ORIGO

L2 Switch Series

OS2312L/OS2320L/OS2328L

User Manual

Foreword

Manual Introduction

This manual primarily covers the web operation methods for the Light Management Series switches. We have endeavored to group each system function within the same chapter. This way, when you need to use a specific function, you can simply refer to the corresponding chapter. For functions that overlap and cannot be grouped together, this manual will explicitly indicate their separate locations.

We hope this manual proves helpful in your work!

Target Audience

This manual is primarily intended for the following personnel:

Software Testing Engineers

Field Maintenance Engineers

System Maintenance Engineers

This manual specifies

Format Conventions

Format	Instruction
Song font	The main text content adopts
Black font	Title format
Kaiti font	Warnings, cautions, instructions, and similar content shall be presented using
Courier new font	Formatting indicates screen output information. Additionally, user input from the terminal interspersed within the screen output is displayed in bold font.

Icon Symbol Conventions

Format	Note
 Note:	Supplementary or emphatic explanation of the preceding content.
 Attention:	Indicates important considerations during the installation or use of equipment, which are critical for ensuring proper installation and operation.
 Warning:	Prohibited operations or operations that must be performed according to specified procedures must be followed; failure to do so may result in personal injury or equipment damage.

Introduction

Device WEB Management is a network management software designed for individual devices. It provides a visual configuration method for service functions, helping operators and maintenance personnel quickly complete device configuration, view current configuration information for various service functions, and understand the device's current operational status.

Device WEB Management utilizes browsers such as Edge, Firefox, or Chrome to manage network devices like routers or switches. It is primarily used to simplify device configuration and enhance product usability.

Device WEB Management comprises two components: the WEB server and the WEB client. The WEB server is integrated into the device to receive and process requests from the client, returning results to the client. The WEB client typically refers to web browsers such as Edge, Firefox, Chrome, etc.

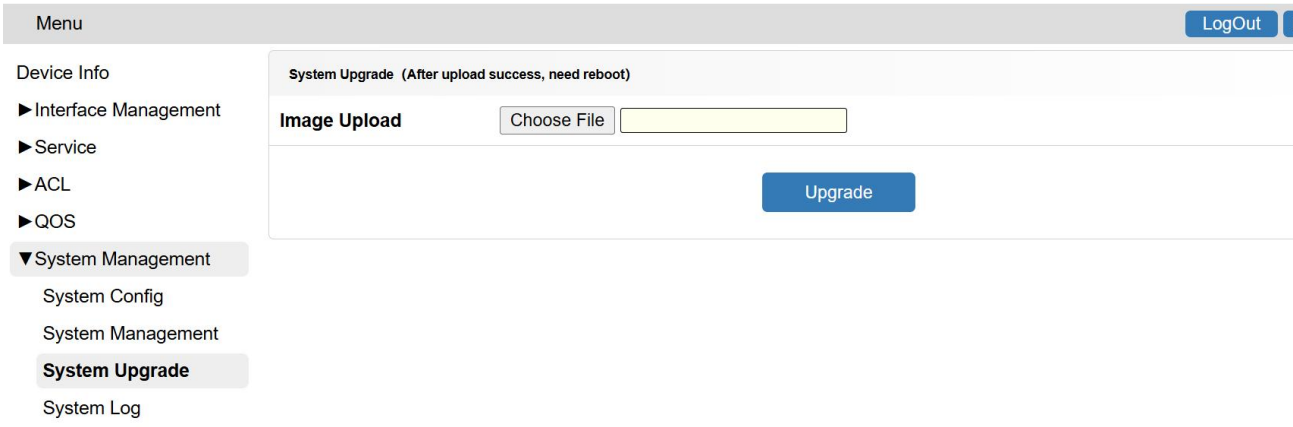
1 Download Device WEB Package and Device Upgrade

1.1 Download the device WEB package

First, download the device's WEB package (full_xx.bin) and save it to a local folder.

1.2 Equipment Upgrades

After logging into the device using a web browser, perform the device upgrade on the “System Management” > “System Upgrade” page. For details, refer to Section 8.3.



1.3 Restore factory settings

To restore the device to its default settings, press and hold the “reset” button on the device panel for 5 seconds. Release the button when all power port LEDs turn orange.

2 WEB Login

2.1 Web Login

Open your web browser (currently supports Chrome/Firefox/360/Edge, but IE is not recommended), enter the switch management address, and access the login page (as shown in Figure 2-1). The default switch IP address is 192.168.1.1, the default subnet mask is 255.255.255.0, and the default gateway is 192.168.1.254.

Figure 2- 1

2.2 User Account and Password Configuration

The user account and password for WEB management must be configured on the System Management - System Configuration page. The default username is admin, and the default password is admin. See Figure 2-2.

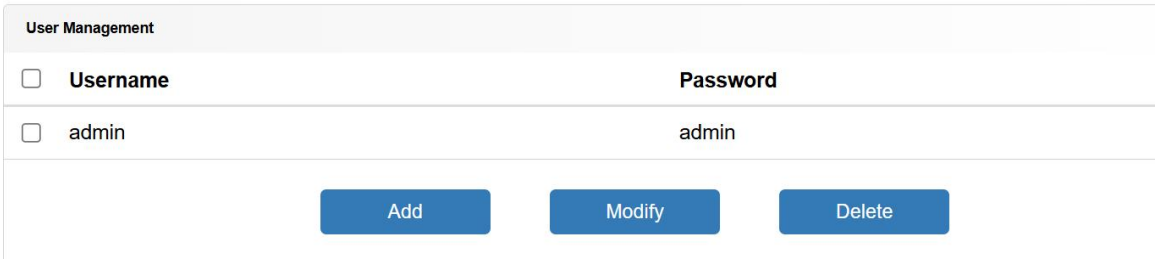


Figure 2- 2

2.3 Managing Network Port IP Addresses and Gateway Configuration

Before managing the switch via the web interface, users can configure the IP address and gateway address of the management network port through the “System Management” > “System Config” page.

For example: Configure IP address: 10.10.38.10, Subnet mask: 255.255.255.0, Default gateway: 10.10.38.254. Click “Modify” then “Confirm” (as shown in Figure 2-3). Save the configuration and reboot for changes to take effect.

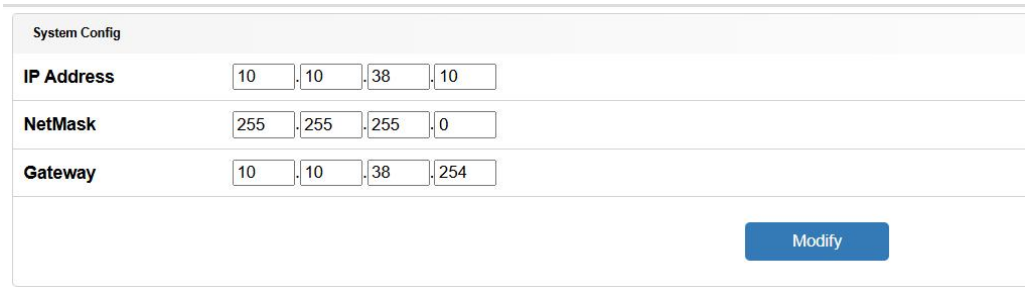


Figure 2-3

Attention:

- The default IP address is 192.168.1.1, the default subnet mask is 255.255.255.0, and the default gateway is 192.168.1.254.

2.4 Error Messages

When a user enters an incorrect username or password, they cannot successfully log in to the operating interface. At this point, the interface will display a corresponding prompt (as shown in Figure 2-4). After five consecutive incorrect username or password entries, the system enters a silent period, displaying a prompt (as shown in Figure 2-5).

Figure 2- 4

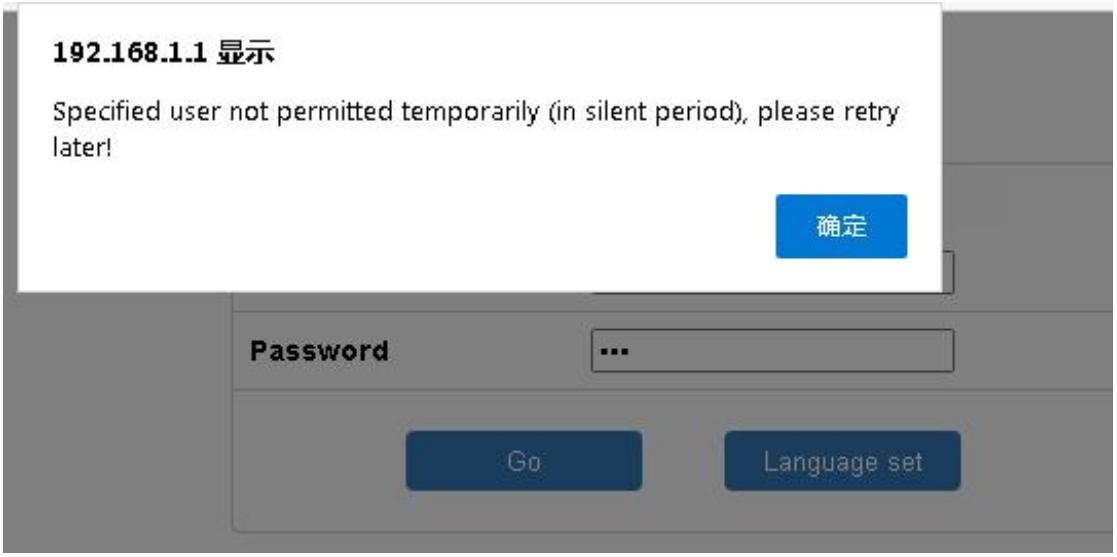


Figure 2-5

Warning:

- Entering an incorrect username or password five times will trigger a 15-minute lockout period. You must wait until the lockout period ends before attempting to log in again.

2.5 Language Settings

Clicking “Language Settings” on the login interface will automatically redirect you to the page for configuring the login language mode. You can choose to log in using either Chinese or English mode (as shown in Figure 2-6), with Chinese being the default.

After successful login, users can access the language settings page via the “Language” button in the upper-right corner of the operation interface (as shown in Figure 2-7).

Figure 2- 6

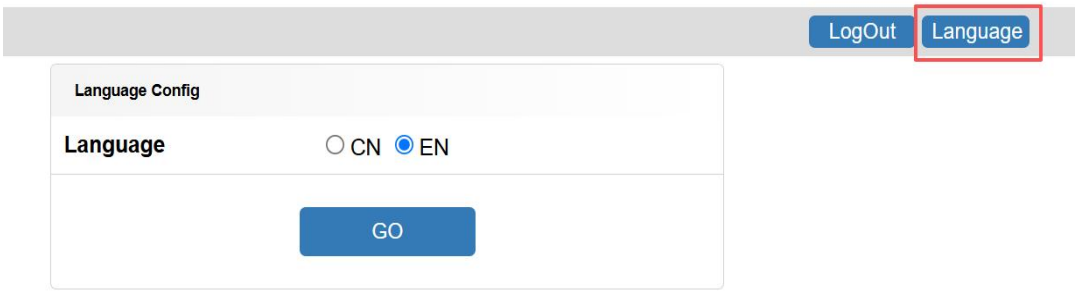


Figure 2- 7

2.6 Log Out

After completing device configuration, users can exit the operation interface by clicking the “Logout” button.

The “Logout” button is located in the upper-right corner of the operation page (as shown in Figure 2-8).

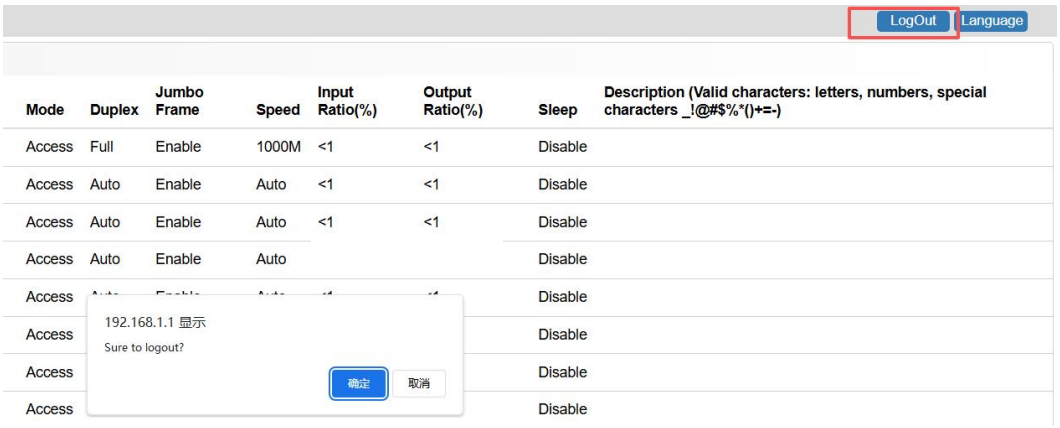

LogOut
Language
Mode
Duplex
Jumbo Frame
Speed
Input Ratio(%)
Output Ratio(%)
Sleep
Description (Valid characters: letters, numbers, special characters _!@#$%*()+=-)
Access Full Enable 1000M <1 <1 Disable
Access Auto Enable Auto <1 <1 Disable
Access Auto Enable Auto <1 <1 Disable
Access Auto Enable Auto Disable
Access Disable
Access Disable
Access Disable
Access Disable
192.168.1.1 显示
Sure to logout?
确定
取消

Figure 2- 8

3 Equipment Overview

3.1 Device Info

View device information through the “Device Info” interface, which displays the device panel, model, software version, MAC/IP address, and other details for the current device (as shown in Figure 3-1).

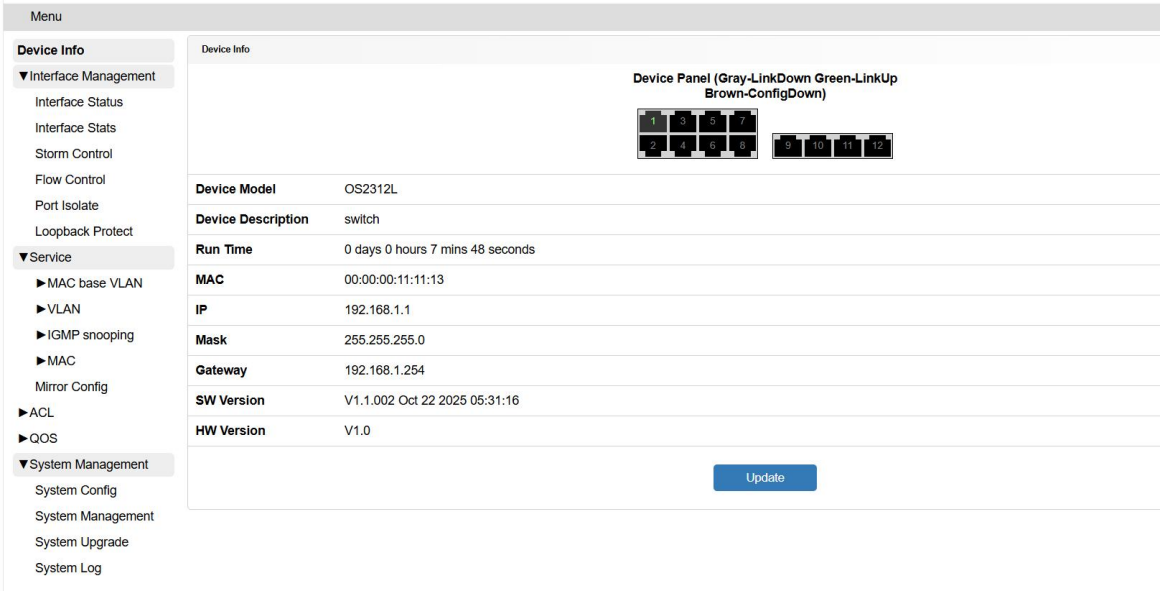


Figure 3- 1

Parameter Description

Parameter Item	Note
Device Info	Display the port numbers and their arrangement on the device panel.
Device Model	Display device model number
Device Description	Users can customize this in “System Configuration”; the default display is switch.
Run Time	Display restart to current runtime

MAC	MAC address information of the device
IP	The device's current IP address information
Mask	The device's current subnet mask information
Gateway	The device's current default gateway information
SW Version	Software version and build time of the current image
HW Version	Current device hardware version information
SN	Equipment Serial Number

4 Interface Management

4.1 Interface Status

4.1.1 Overview

The Interface Status page is the interface for displaying port information and modifying port configurations. Ports support configuration of speed, duplex, mode, jumbo frames, and more. When a port status is “Up,” it will function normally with a properly connected cable. When a port status is “Down,” the port will not function regardless of whether a cable is connected.

4.1.2 Enter the Interface Status

Select “Interface Status” under “Interface Management” in the menu bar to access the Interface Status page (as shown in Figure 4-1).

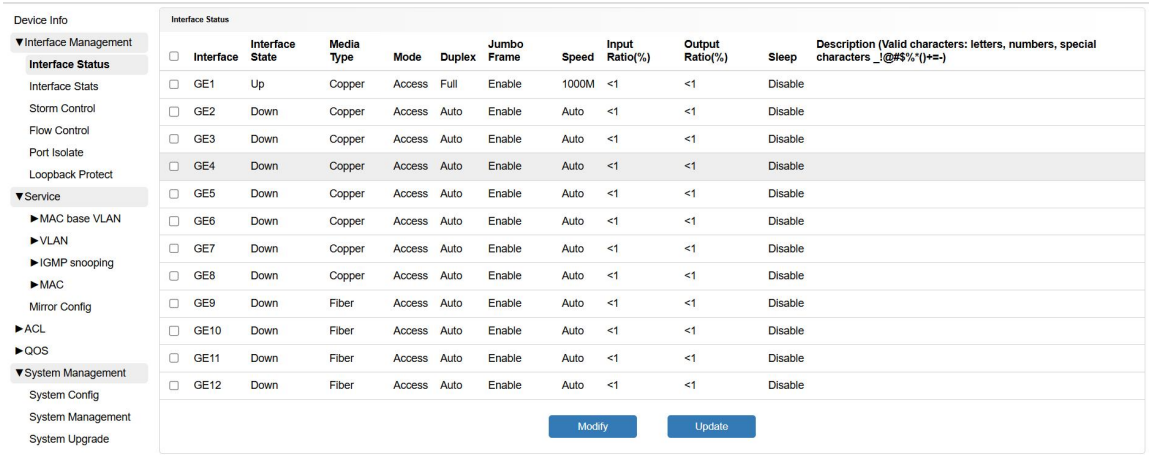


Figure 4- 1

4.1.3 Configure Interface Status

On the Port Status page, select the ports and click the “Modify” button at the bottom of the page. This will pop up the port configuration dialog box, which can be configured according to user requirements and the specific support capabilities of the device (as shown in Figure 4-2). GE1-GE8 are electrical ports, arranged in an upper single-down dual configuration. GE9-GE12 are optical ports, oriented from left to right. For details, refer to the device panel diagram in the Device Overview.。

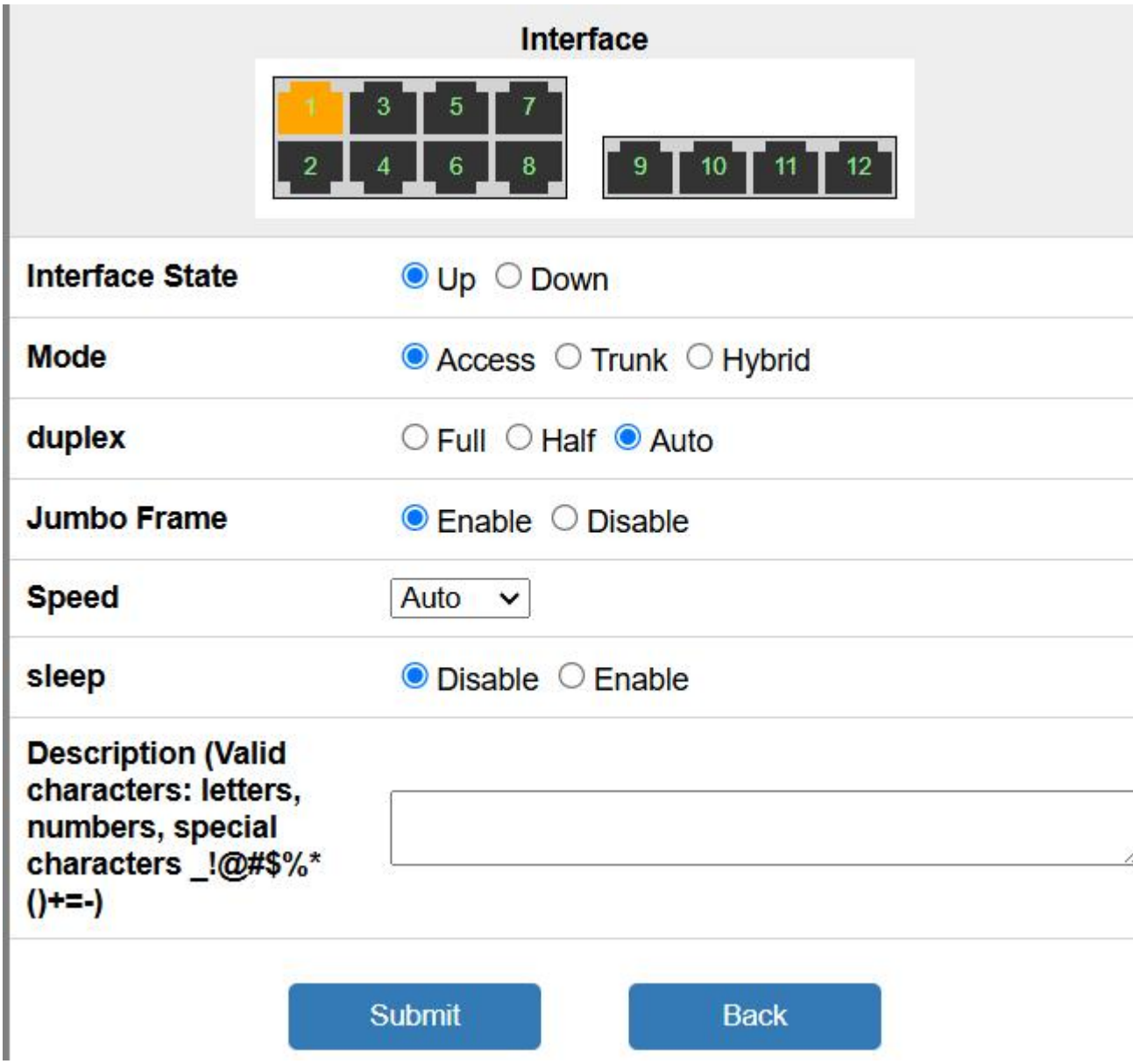


Figure 4- 2

Parameter Description

Parameter Item	Note
Interface	Display Port Name
Interface State	Includes the two states Up and Down
Media Type	Includes the two states: Copper and Fiber
Mode	Includes three port types: Access, Trunk, and Hybrid.
Duplex	Includes three types: Full, Half, and Auto.
Jumbo Frame	Enable Jumbo Frame functionality (Enabling this allows the port to

	transmit packets ranging from 1519 to 9600 bytes)
Speed	Includes 10M, 100M, and 1000M speeds
Input Ratio	Inbound Port Rate Share
Ouput Ratio	Outbound Port Rate Proportion
Sleep	The switch enters low-power mode, with only electrical ports supported—optical ports are not supported. This mode is activated only when the port is down.
Description	Port description information, supports up to 32 characters

Attention:

- This page displays the actual negotiated results. For example, if the speed is configured as auto and the negotiated rate is 1000M, the page will show 1000M.

4.2 Interface Stats

4.2.1 Overview

Count the number of packets received and transmitted by each port.

4.2.2 Enter Interface Stats

Select “Interface Stats” under “Interface Management” to access the interface (as shown in Figure 4-3).

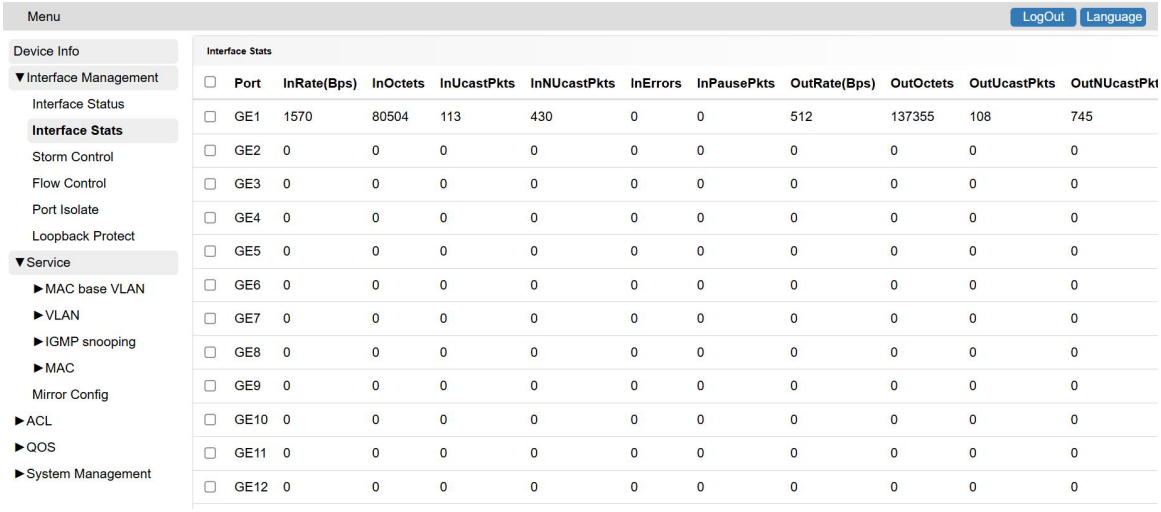


Figure 4- 3

Click the “Update “button at the bottom of the port statistics page to refresh the port statistics data. You can also clear the port statistics data using the “Clear ":button, provided that you have selected the corresponding port(s) (as shown in Figure 4-4).

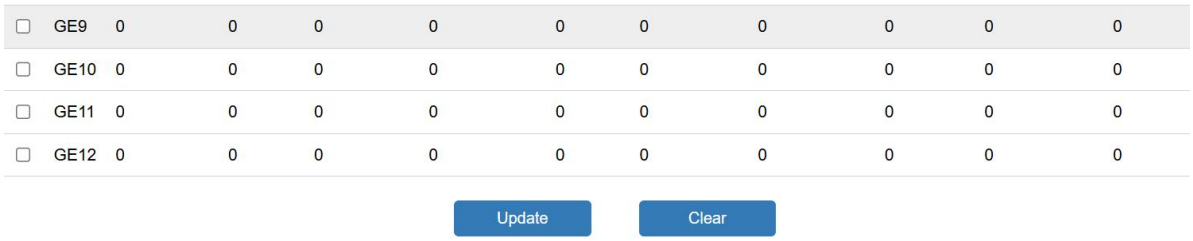


Figure 4- 4

Parameter Description

Parameter Item	Note
Port	Display Port Name
InRate(Bps)	Receive message rate, units Bps
InOctets	Number of bytes received, including error frames and jumbo frames
InUcastPkts	Number of valid unicast packets received, including jumbo frames; excluding error frames
InNUcastPkts	Number of valid non-unicast packets received, including jumbo frames; excluding error frames
InErrors	Received error frames, including error frames and jumbo frames
InPausePkts	Number of Pause frames received by the port
OutRate(Bps)	Data transmission rate, in bits per second (bps)
OutOctests	Number of bytes sent
OutUcastPkts	Number of unicast packets sent
OutNUcastPkts	Number of non-unicast packets sent
OutPausePkts	Number of Pause Frame Messages Sent by the Port

4.3 Storm Control

4.3.1 Overview

Storm control refers to limiting the maximum broadcast, unknown unicast, unknown multicast, and known multicast traffic received on a designated interface. This prevents flooding from consuming excessive switch resources and ensures normal service operation.

Storm control can be implemented using one of the following two methods:

Percent Mode

Packets per Second (PPS) Mode

PPS: An acronym for Packets per second, referring to the number of packets transmitted per second, i.e., the packet rate.

4.3.2 Enter the Storm Control

Select “Storm Control” under “Interface Management” to access the Storm Control page, which primarily enables rate limiting for specific types of packets (as shown in Figure 4-7).

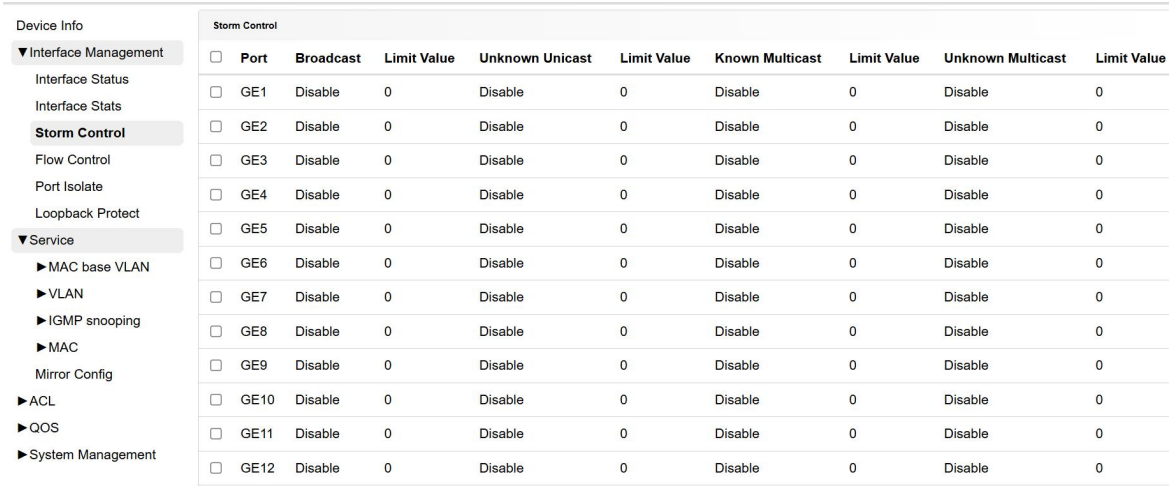


Figure 4- 7

4.3.3 Configuring Storm Control

On the Storm Control page, select the port to configure and click the “Modify” button at the bottom of the page. This will pop up a dialog box for configuring port storm control. Within this dialog box, you can choose to restrict broadcast, unknown unicast, and multicast packets. You can also configure the storm control mode to be based on packet count or port bandwidth percentage (as shown in Figure 4-8).

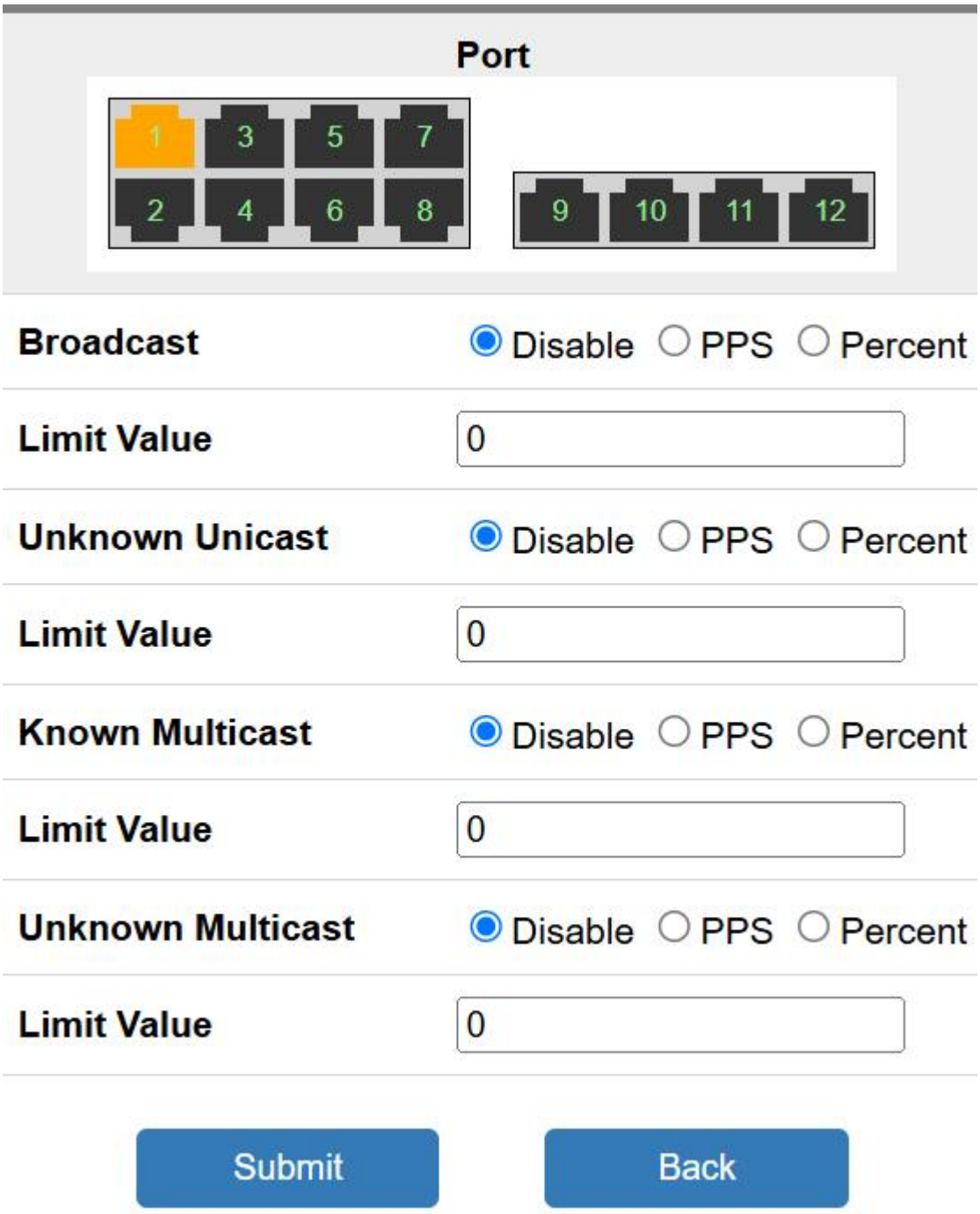


Figure 4- 8

Parameter Description

Parameter Item	Note
Disable	Disable this function
PPS	Messages per second

Percent	Percentage of port line speed, range: 0-100
Broadcast	Destination address: FF-FF-FF-FF-FF-FF
Unknown Unicast	The destination address is not present in the FDB table entry.
Known Multicast	When used in conjunction with IGMP snooping, this destination address exists in the multicast MAC table.
Unknown Multicast	When used in conjunction with IGMP snooping, the destination address is not present in the multicast MAC table.

4.4 Flow Control

4.4.1 Overview

Flow control is enabled on directly connected Ethernet ports, allowing congested nodes at the opposite end to suspend link operations during congestion to regulate traffic rates. When a local device detects any congestion locally, it can send a suspend frame to notify the link partner or remote device that congestion has occurred. Immediately upon receiving the suspend frame, the remote device ceases sending any packets, thereby preventing packet loss during congestion. On auto-negotiated links, the local flow control capability can be communicated to the other end through link disconnections/reconnections.

4.4.2 Enter the Flow Control

Select “Flow Control” under “Interface Management” to access the flow control page (as shown in Figure 4-9).。

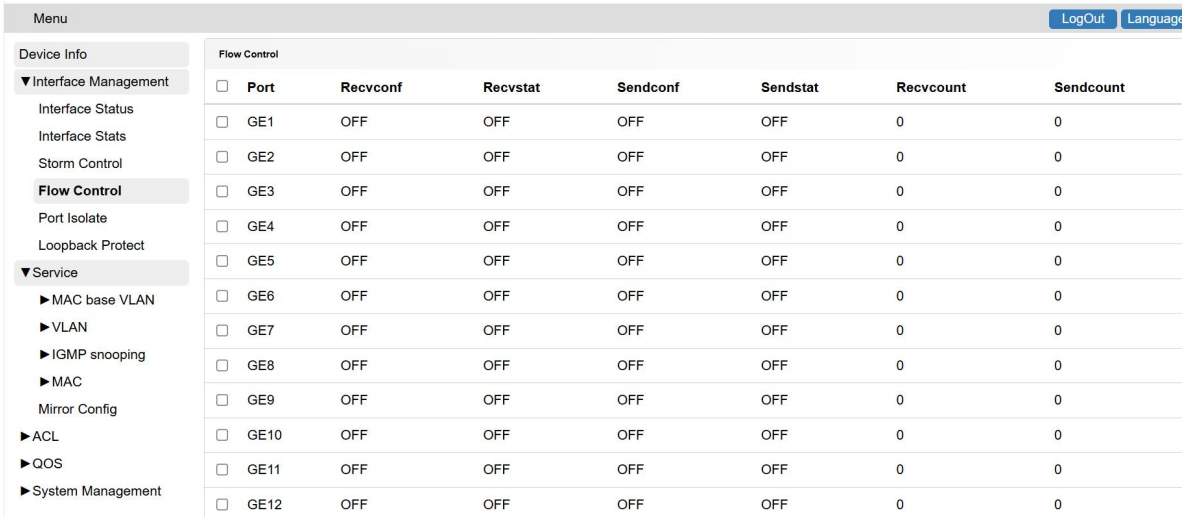


Figure 4- 9

Attention:

- Flow control is only effective on full-duplex links.

4.4.3 Configuring Flow Control

On the Flow Control page, select the port you wish to configure. Click the “Modify” button at the bottom of the page to open the port flow control configuration dialog. You can choose to enable flow control for either the receive direction or the transmit direction (as shown in Figure 4-10).

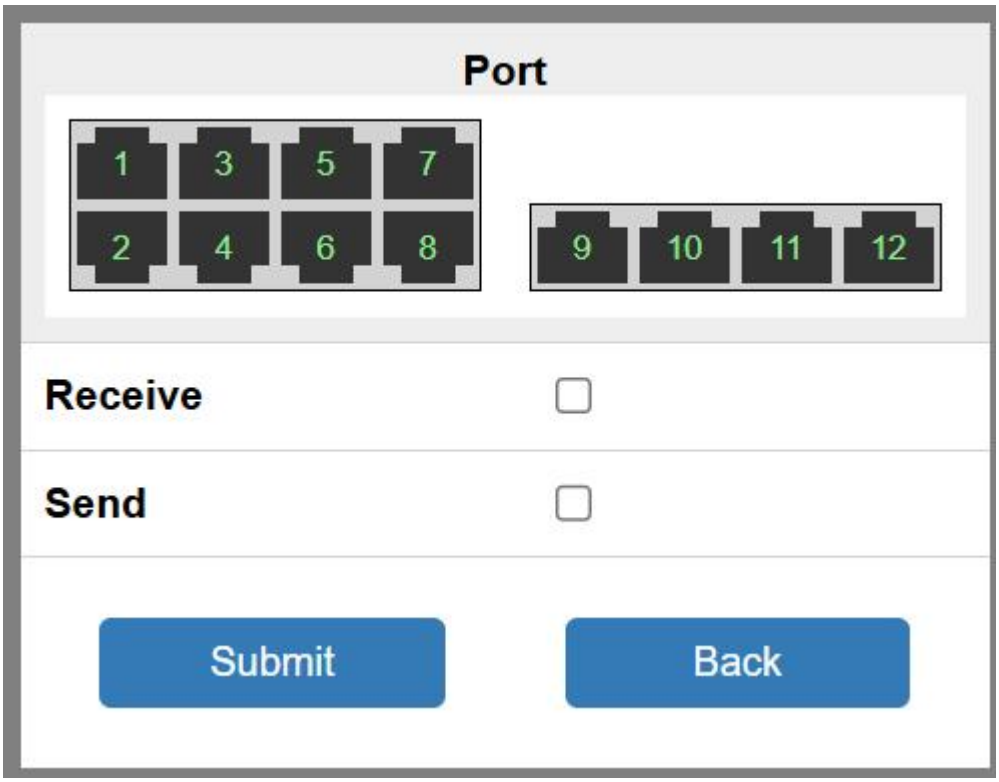


Figure 4- 10

Parameter Description

Parameter Item	Note
Recvconf	User-configured receive direction enable/disable status
Recvstat	Actual receiving direction activation/deactivation status
Sendconf	User-configured send direction enable/disable status

Sendstat	Actual transmission direction enable/disable status
Recvcount	Number of Pause frames received
Sendcount	Number of Pause frames sent

4.5 Port Isolate

4.5.1 Overview

The Port-Isolated feature enables isolation between ports within the same VLAN. Simply adding ports to an isolation group achieves Layer 2 data isolation among ports within that group. This enhances network security, provides flexible networking solutions, and simultaneously conserves significant VLAN resources.

4.5.2 Enter the Port Isolate

Select “Port Isolate” under “Port Management” to access the port isolate page (as shown in Figure 4-11).

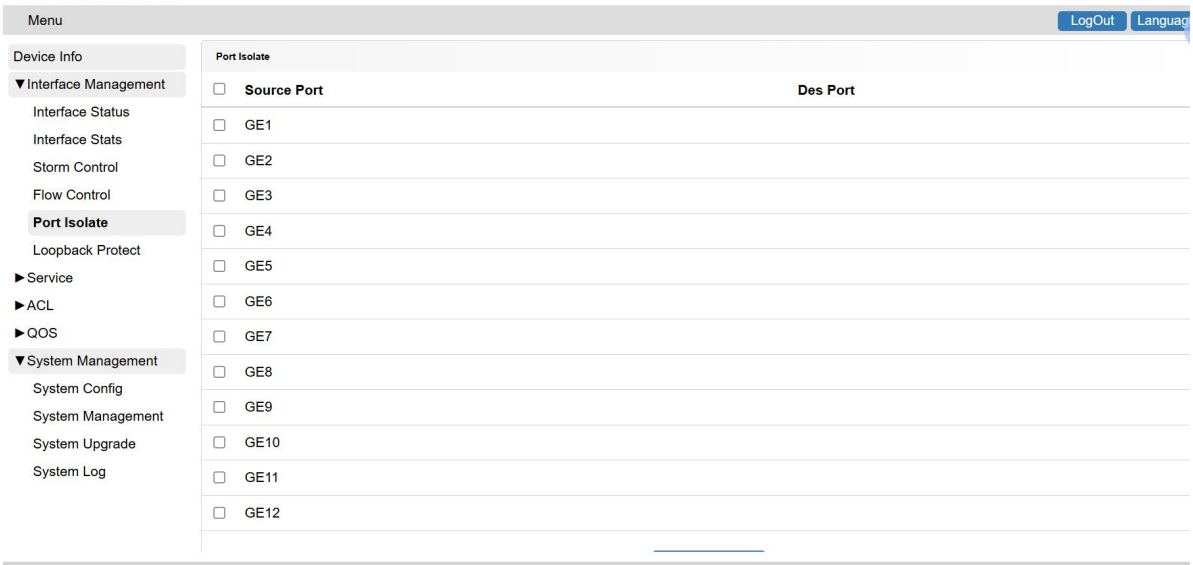


Figure 4- 11

4.5.3 Configuring Port Isolate

On the Port Isolate page, select the source port to configure. Click the “Modify” button at the bottom of the page to open the port isolation configuration dialog. Select the destination ports to isolate, then click the “Submit” button to save the configuration. By default, the destination port field is empty, allowing communication between all ports. (As shown in Figure 5-12) To configure isolation between port 3 and ports 11-12, this setting prevents port 3 from communicating with ports 11-12, while ports 11-12 can still communicate with port 3. This constitutes unidirectional isolation.

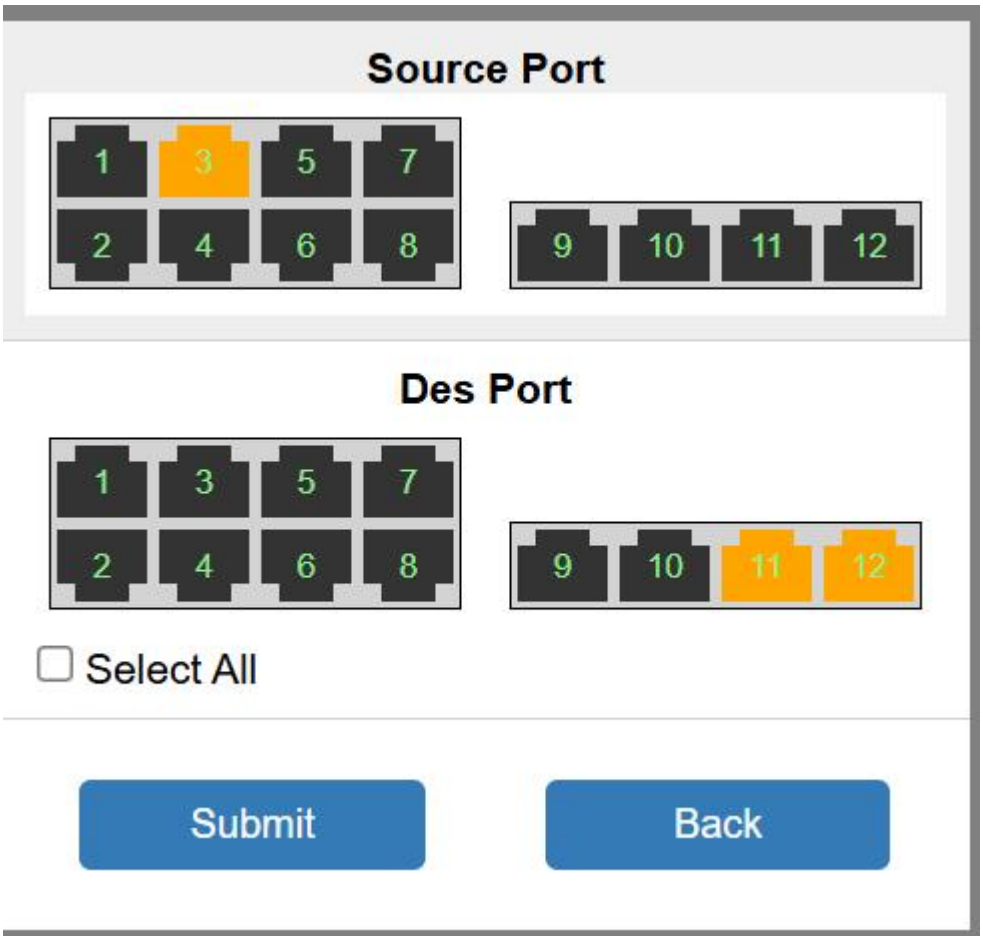


Figure 4- 12

Attention:

- The system supports unidirectional isolation. If bidirectional isolation is required, it can be achieved by configuring two unidirectional isolation settings.

Parameter Description

Parameter Item	Note
Source Port	Port for incoming packets corresponding to the isolation function

Des Port	Port for outgoing traffic corresponding to the isolation function

4.6 Loopback Protect

4.6.1 Overview

Loops in a network cause devices to repeatedly transmit broadcast, multicast, and unknown unicast messages, leading to wasted network resources and potentially causing network paralysis. To promptly detect loops in Layer 2 networks and prevent severe impacts on the entire network, loopback protection is provided. This feature alerts users to inspect network connections and configurations when a loop occurs, and can place the affected interface into a controlled state.

Loopback Detection technology periodically sends detection packets from a port to check whether the packets return to the device (without requiring the sending and receiving ports to be the same). This determines whether a loop exists on the port, the network segment connected to the device, the device itself, or between device ports. Upon detecting a loop, the port is processed to enter a controlled state, minimizing the impact of the loop on the device and the entire network.

4.6.2 Enter the Loopback Protect

Under the “Interface Management” menu, select “Loopback Protection” to access the Loopback Protection page (as shown in Figure 4-13).

On this page, you can enable or disable the loopback protection feature. The feature is enabled by default, with a default recovery time of 6 seconds. When enabled, each port sends a broadcast packet with type 0x8899 every 2 seconds. If any port on the device receives this packet, it blocks that port for 6 seconds. If no further packets are received after 6 seconds, the port is set to forward.

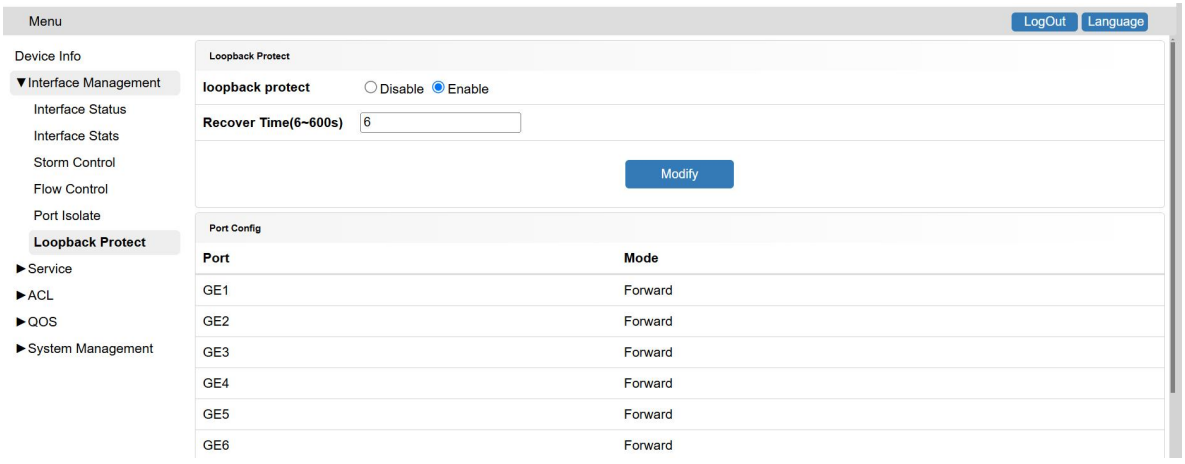


Figure 4- 13

4.6.3 Refresh Port Status

Click the “ Update ” button at the bottom of the page to refresh the current forwarding status of the controlled port (as shown in Figure 4-14).

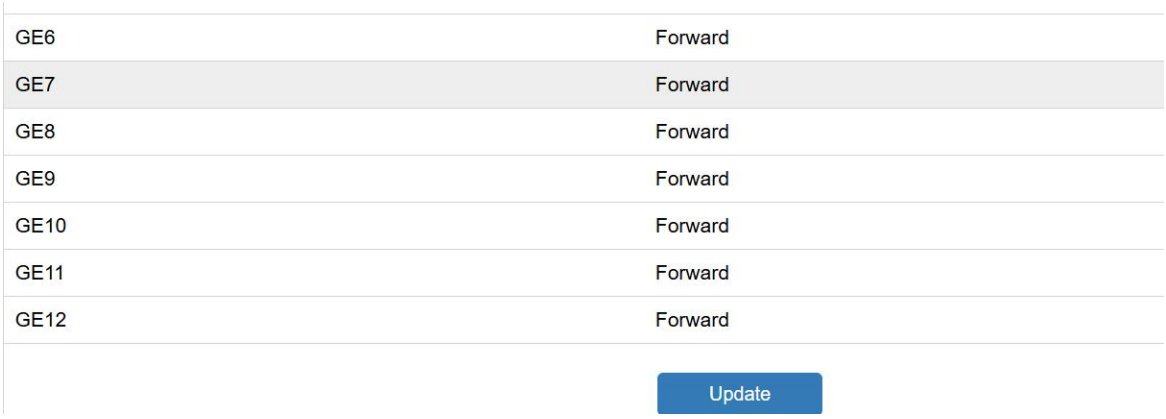


Figure 4- 14

Parameter Description

Parameter Item	Note
Enable	Enable loopback protection globally
Disable	Disable loopback protection globally
Recover Time	The time for the controlled port to automatically recover to its normal state after detecting a loopback, with a range of 6 to 600 seconds.
Mode	Forward: Normal data transmission and reception Block: Only permits transmission and reception of loopback protocol packets

5 Service

5.1 MAC base VLAN

MAC base VLAN divides VLANs based on the source MAC address of the packet. After configuring the MAC base VLAN, if the port receives an untag packet and the source mac address of the packet matches a mac base vlan entry, the device adds a VLAN tag to the packet, and its VLAN ID is the VLAN ID in the matching entry.

When the user's physical location changes, as long as the user's MAC address does not change, there is no need to reconfigure the VLAN to which the port connecting the user belongs.

Click the menu bar-"Service"-"MAC base VLAN" to enter. (See Figure 5-1)

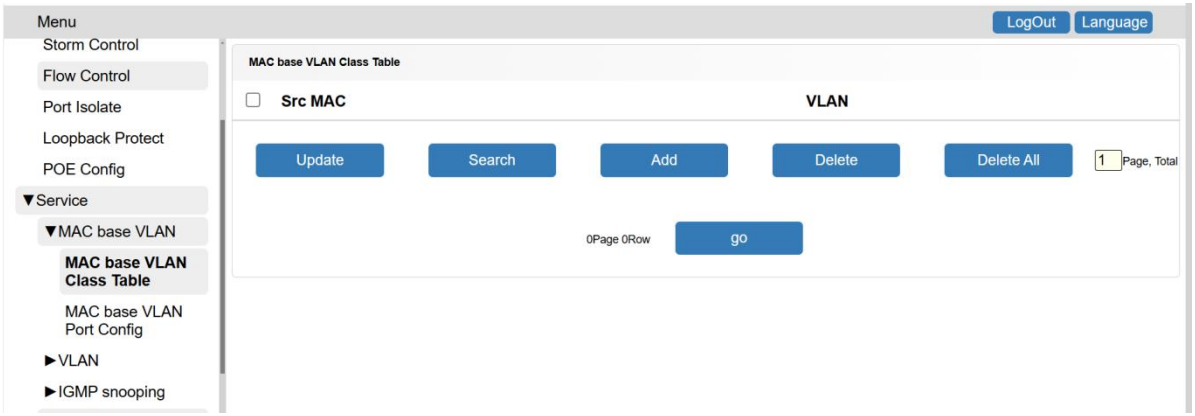


Figure 5-1

5.1.1 MAC base VLAN Class Table

Used to configure MAC base VLAN table entries, with a maximum specification of 64 entries.

If the MAC is configured as 00.00.00.11.11, the VLAN is set to 10, as shown in Figure 5-2.

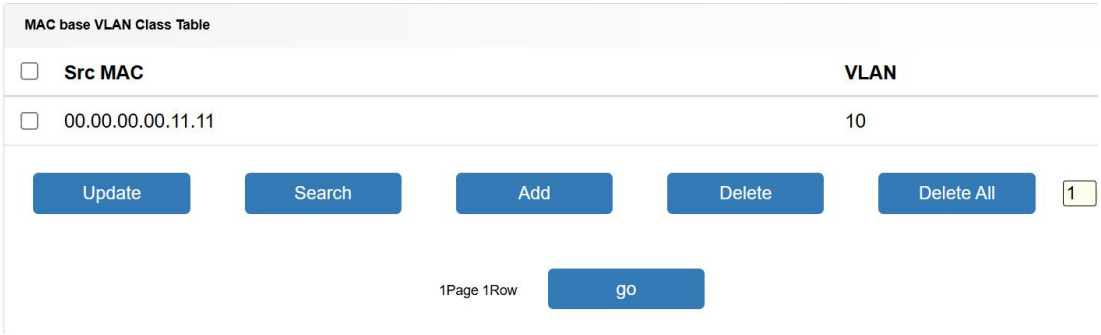


Figure 5-2

Parameter Item	Note

Src MAC	Message source MAC address
VLAN	VLAN ID added after matching MAC base VLAN

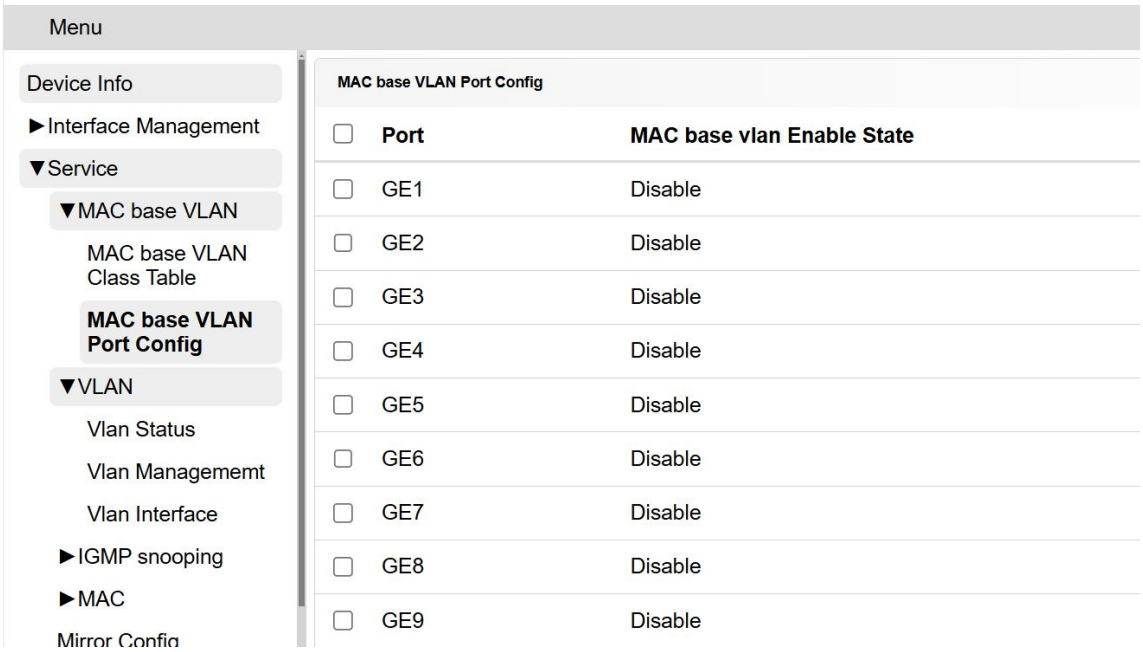
Attention:

- Ports that enable MAC base VLAN functionality need to add matching table entries for VLANs, otherwise packets from that VLAN cannot be forwarded and packets with matching source MAC addresses will be discarded.

5.1.2 MAC base VLAN Port Config

Used to configure the MAC base VLAN enable status for ports, with all ports set to Disabled by default. The port must be a Hybrid port to enable MAC base VLAN.

Check the port, click "Modify", and select "Enable" to enable the MAC base VLAN function of the port (as shown in Figure 5-3).



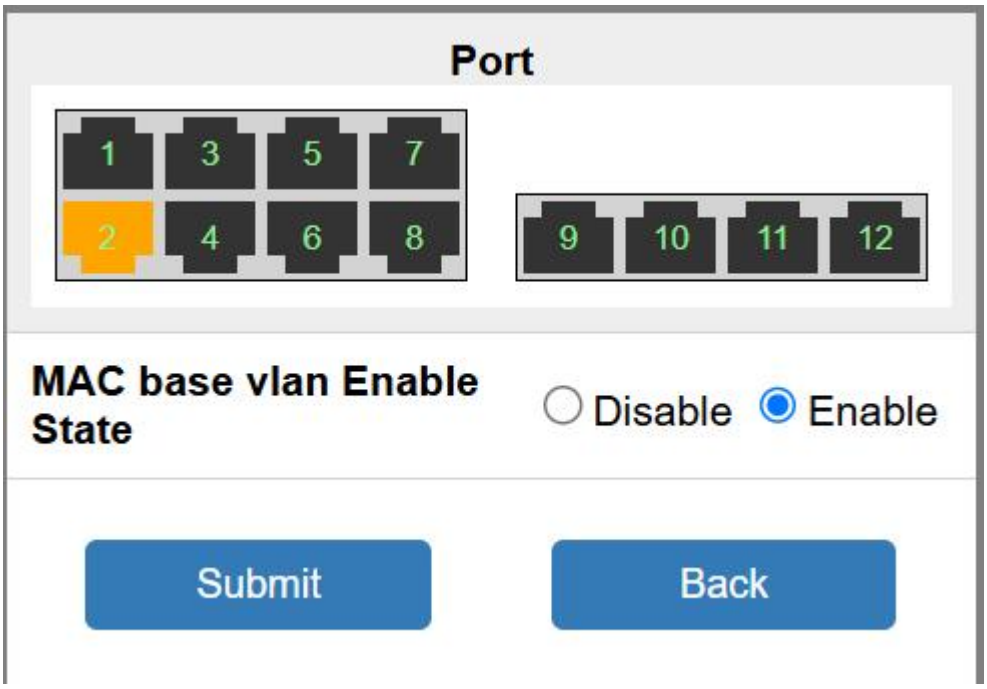


Figure 5-3

Parameter Item	Note
Port	Port ID
MAC base vlan Enable State	Disable: Disable port MAC base VLAN function, default state Enable: Enable port MAC base VLAN function

5.2 VLAN

A VLAN (Virtual Local Area Network) is a network logically segmented into separate broadcast domains, enabling packet exchange only between ports designated for the same VLAN. Each VLAN is treated as a logical network; packets destined for ports outside the same VLAN must be forwarded via routing.

VLANs are described using the following terminology:

VID: VLAN ID

LAN: Local Area Network

VLAN: Virtual Local Area Network

PVID: Port VLAN ID, which determines the VLAN tagging applied to frames transmitted or received by the port

Tagged Frame: A frame carrying a 4-byte VLAN tag, as shown below:

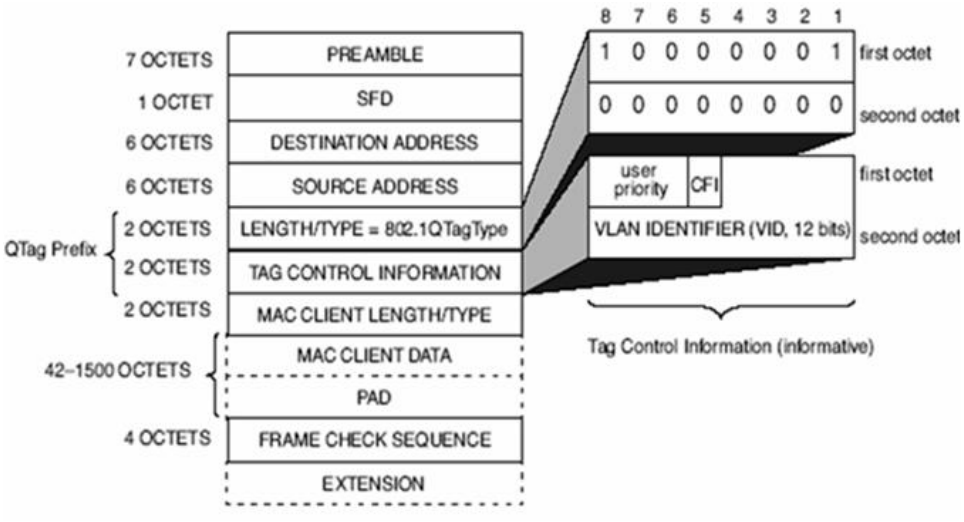


Figure 5-4 Tagged Frame

Trunk Link: Both tagged and untagged frames can be transmitted over this link. A trunk allows multiple VLANs to be forwarded over the link, as illustrated in the diagram below:

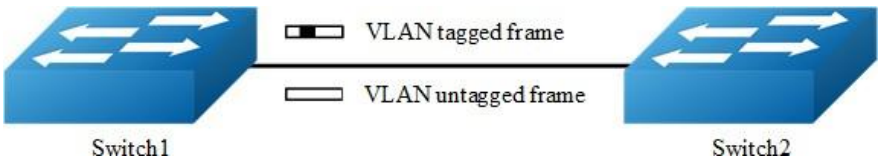


Figure 5-5 Trunk Link

Access Link: Only frames without a TAG or with a PVID TAG can traverse the ACCESS link. The Access link can only connect to the network edge, i.e., workstations, as shown in the diagram below:

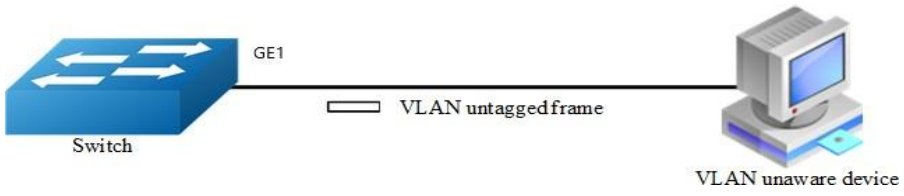


Figure 5-6 Access Link

Hybrid Link: Both tagged and untagged frames can be transmitted over this link. Users can manually designate which VLANs are tagged and which are untagged, as illustrated in the diagram below:

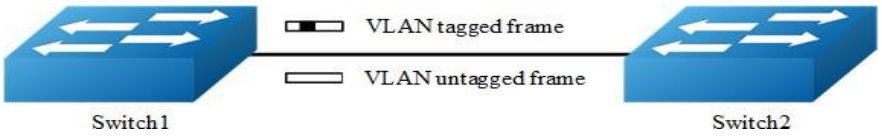


Figure 5-7

5.2.1 VLAN Staus

To view which member ports belong to a VLAN, by default all ports are in VLAN 1 (as shown in Figure 5-8).

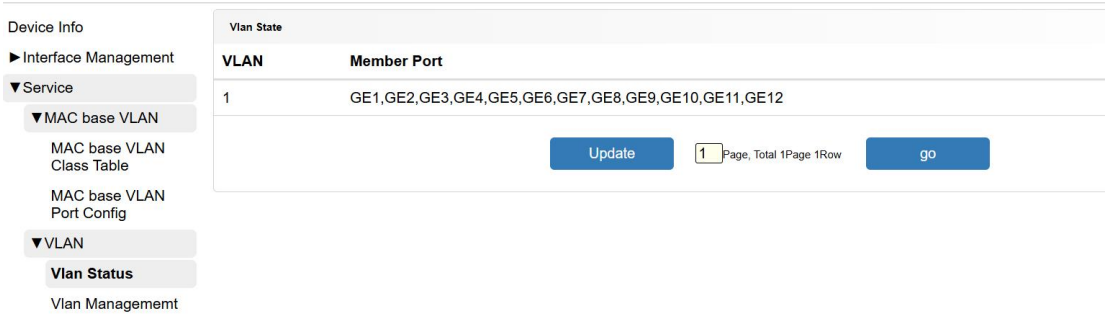


Figure 5-8

Parameter Description

Parameter Item	Note
VLAN	Display VLAN ID
Member Port	Display the port members that have joined this VLAN

5.2.2 VLAN Management

Used to add or delete VLANs, with specifications supporting up to 128 VLANs. You can perform “Add” and “Delete” operations on relevant VLANs.

Configuration

(As shown in Figure 5-9) To add VLANs 2-128, click “Add”.

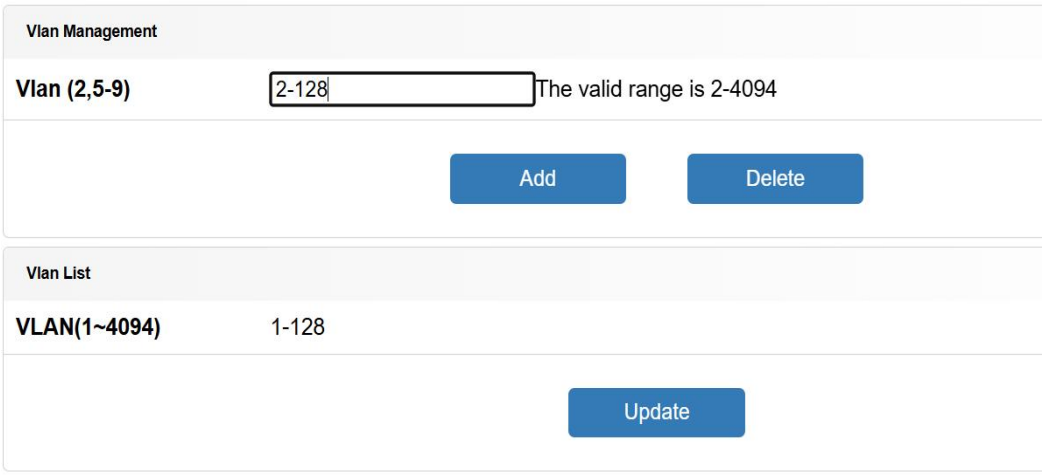


Figure 5-9

（(As shown in Figure 5-10) To delete VLAN 10-20, add VLAN 10-20 and click “Delete.”

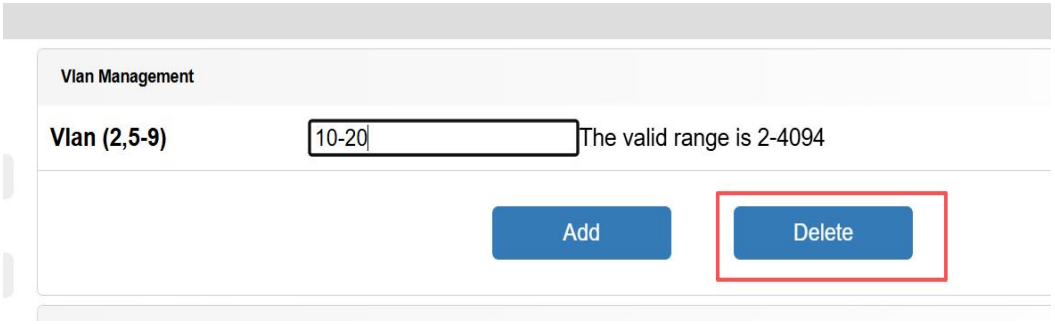


Figure 5-10

Attention:

- VLAN 1 cannot be created or deleted as it is the default VLAN.

5.2.3 Vlan Interface

Used to configure port PVID and allow VLANs/untag VLANs. Default is Access mode with PVID=1. Click “Service ” > ‘VLAN’ > “VLAN Interface” to access the page (as shown in Figure 5-11).

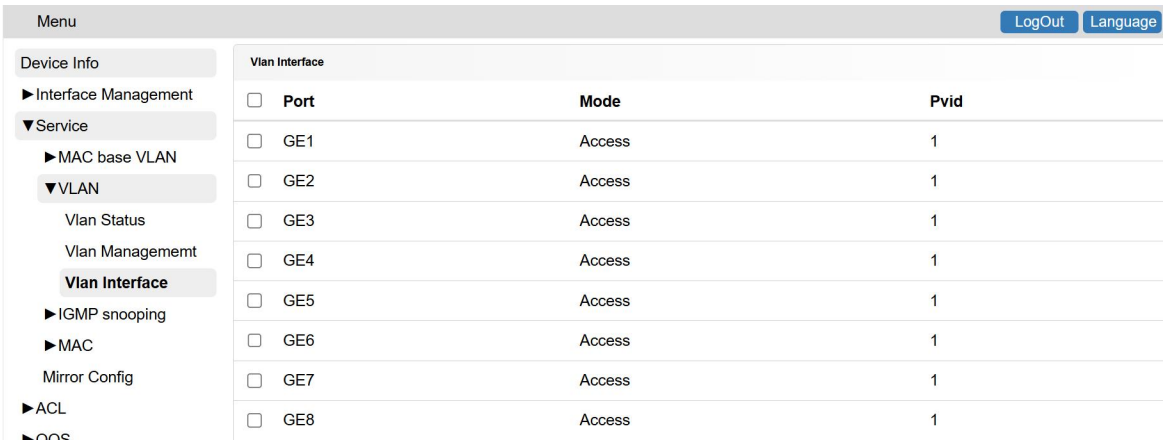


Figure 5-11

You can configure the port Pvid and add multiple VLANs to the port by selecting the port and clicking "Modify." Click "Submit" to apply the changes (as shown in Figure 5-12). By default, configuring ports other than VLAN1 requires creating that VLAN first.

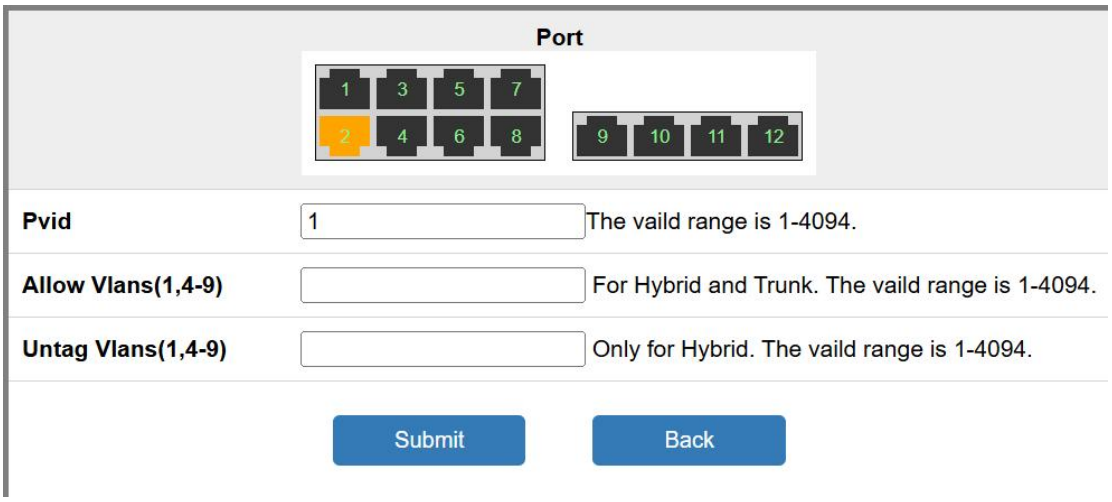


Figure 5-12

Parameter Description

Parameter Item	Note
Port	Select the configured port
Mode	Consistent with the pattern of port status
Pvid	Set the default VLAN for this port. The VLAN must already be created.
Vlans	Configure Trunk or Hybrid ports to permit specific VLANs.
UntagVlans	Configuring Hybrid Port Direction Requires Unlabeled VLANs

Note: To modify the VLAN mode of a port, click “Interface Management” → “Interface Status” → select the port → “Modify” (as shown in Figure 5-13).

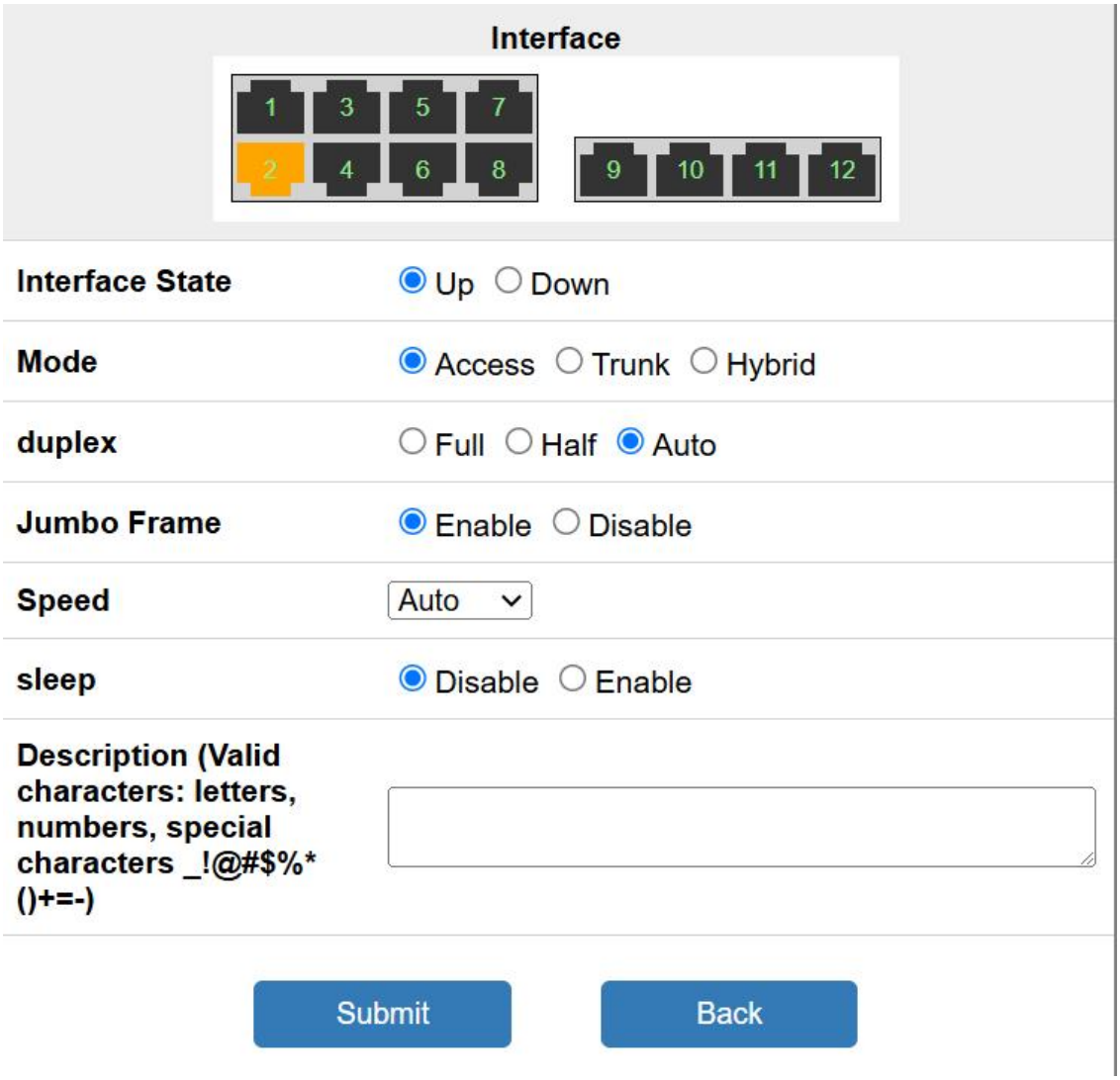


Figure 5-13

Configuration Example:

1. Configure GE1 as Access Port 2.

First create VLAN 2, modify GE1 Access Port's PVID to 2, then click “Submit” to apply the changes. (As shown in Figure 5-14)

Access ports receive untagged frames or frames with PVID tags, and transmit frames without tags.

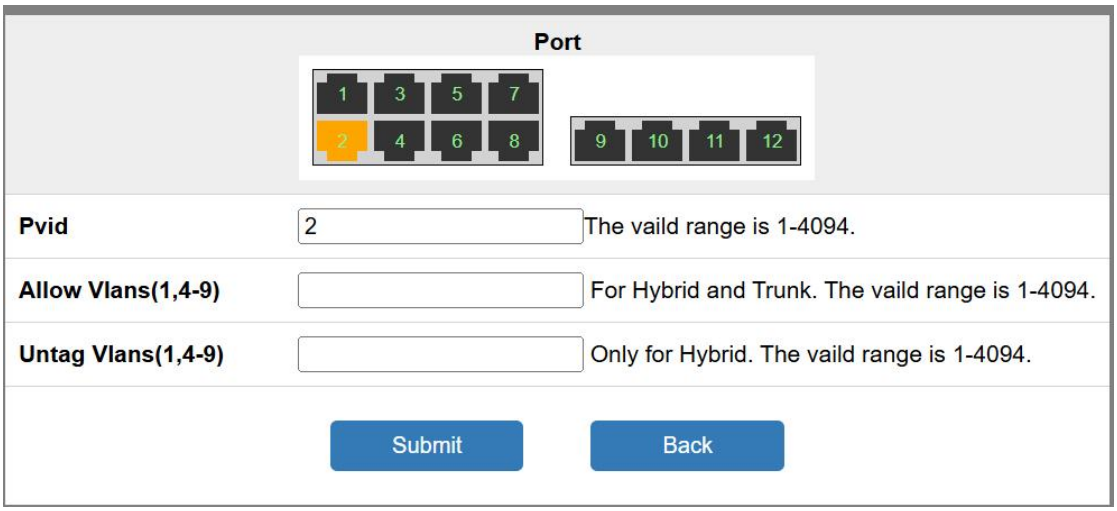


Figure 5-14

2.Configure GE4 as a trunk port, allowing VLANs 10-20.

First create VLANs 10-20. Configure GE4 trunk port with Pvid=1, allowing VLANs 10-20 to pass through. Click “Submit” to apply the changes. (As shown in Figure 5-15)

Trunk ports can receive both tagged and untagged frames, and transmit both untagged and tagged frames. If a port receives an untagged frame, it assigns the port's PVID as the VLAN ID to that frame. If a frame's VID matches the port's PVID, the frame is transmitted with its VLAN tag stripped.

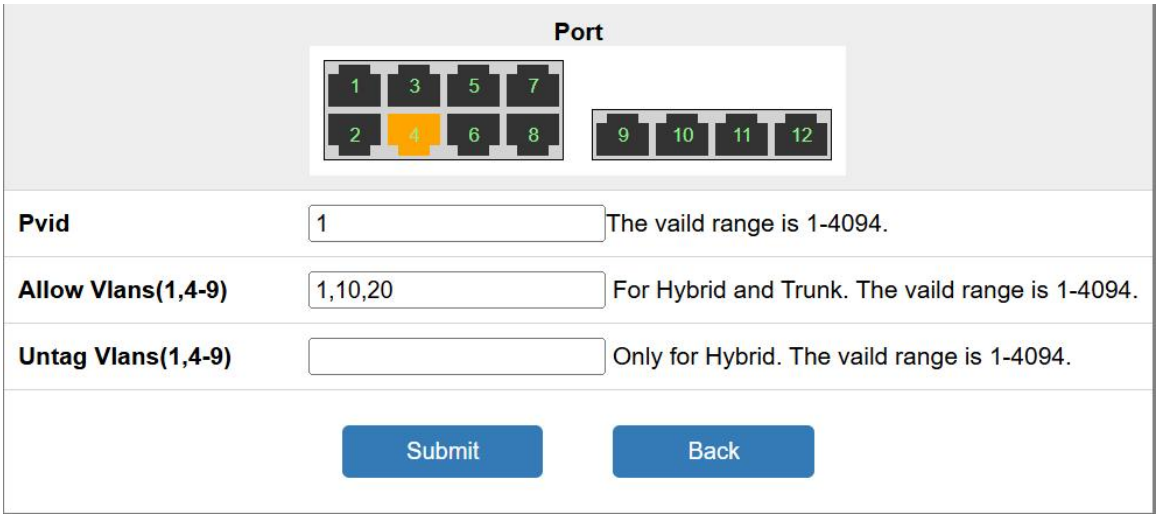


Figure 5-15

3.Configure GE10 ports as hybrid ports, transmitting tagged frames on vlan 10-14 and 16-20, and untagged frames on vlan 15.

First, create VLANs 10-20. Configure the GE10 Hybrid port with Pvid=1, allowing VLANs 10-20 to pass through. The untagged VLAN is 15. Click “Submit” to apply the changes. (As shown in Figure 5-16)

Hybrid ports can receive tagged and untagged frames, and transmit both untagged and tagged frames. If a port receives an untagged frame, it assigns the port's PVID as the VLAN ID. When transmitting frames, hybrid ports determine whether the VLAN is tagged or untagged. If untagged, it strips the VLAN information before transmission; if tagged, it sends the frame directly.

By default, hybrid ports transmit tagged frames with the PVID. This behavior can be modified to send

untagged frames by stripping the PVID.

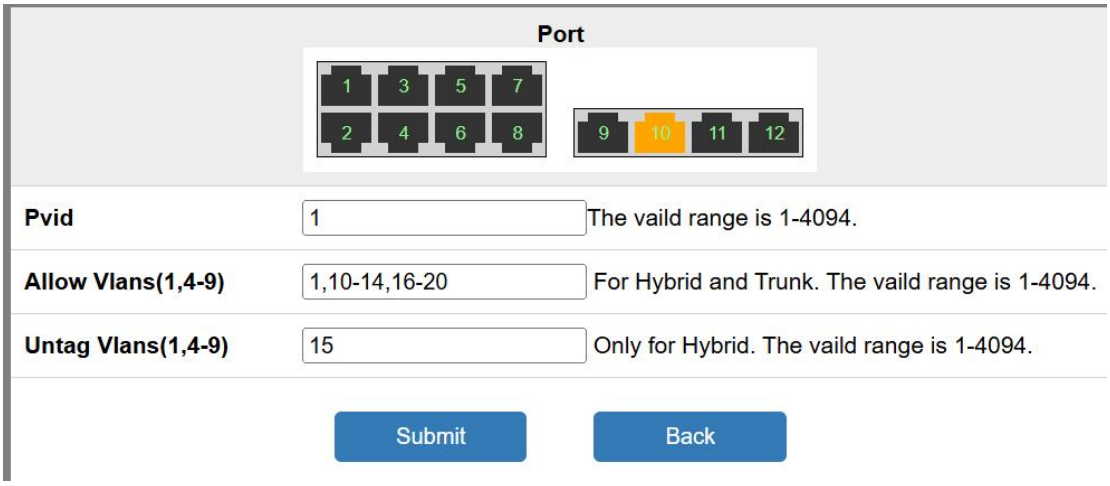


Figure 5-16

5.3 MAC

The MAC address table contains address information for forwarding traffic between switch ports. The table includes the following address types:

Dynamic addresses: Learned by the interface from source MAC addresses in packets; entries can be aged.

Static Address: Manually configured by the user. Entries do not age and are preserved after a reboot.

Navigate to the MAC Address Table by clicking the menu bar > “Service ” > ‘MAC’ > “MAC Address Table”. (As shown in Figure 5-17)

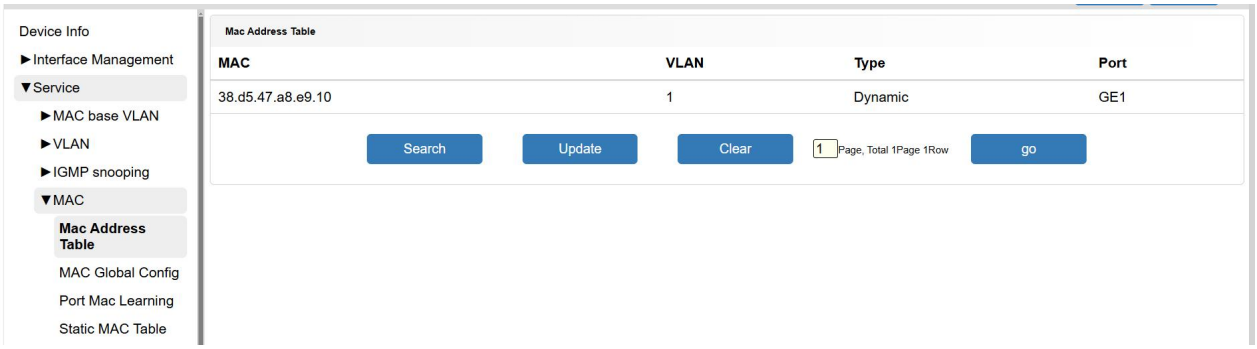


Figure 5-17

5.3.1 MAC Address Table

Used to view the MAC address table entries learned by the current device. The specification supports up to 8,256 entries (as shown in Figure 5-18).

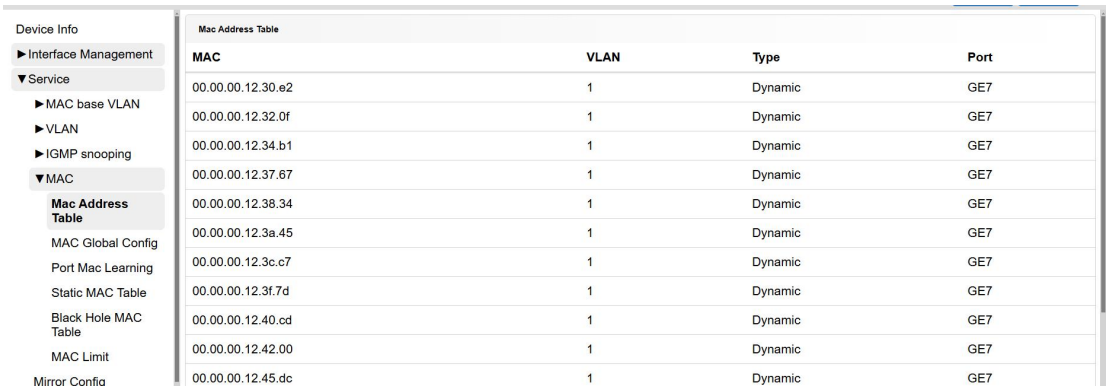


Figure 5-18

Parameter Description

Parameter Item	Note
MAC	MAC address
VLAN	VLAN ID
Type	MAC table entries, including dynamic and static
Port	Port information corresponding to MAC table entries

5.3.2 MAC Global Config

Used to configure the dynamic MAC address aging time. The default aging time is 300 seconds, with a valid range of 0-100000. A value of 0 indicates no aging. (As shown in Figure 5-19) To configure an aging time of 450 seconds, click “Modify” to deploy the configuration.

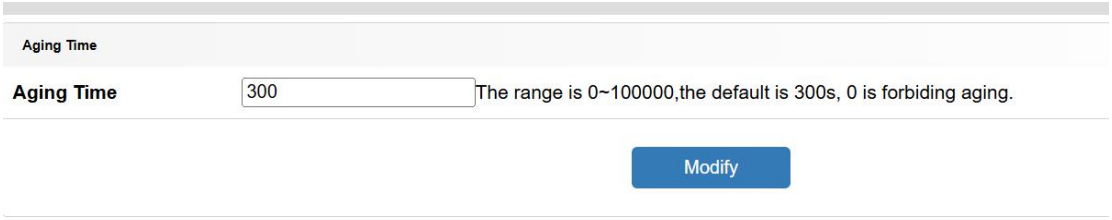


Figure 5-19

5.3.3 Port Mac Learning

Used to enable or disable MAC address learning, determine the behavior of new MAC addresses when

port MAC learning is disabled, and specify the behavior of new MAC addresses when the MAC learning capacity is full while port MAC learning is enabled. (See Figures 5-20 and 5-21)

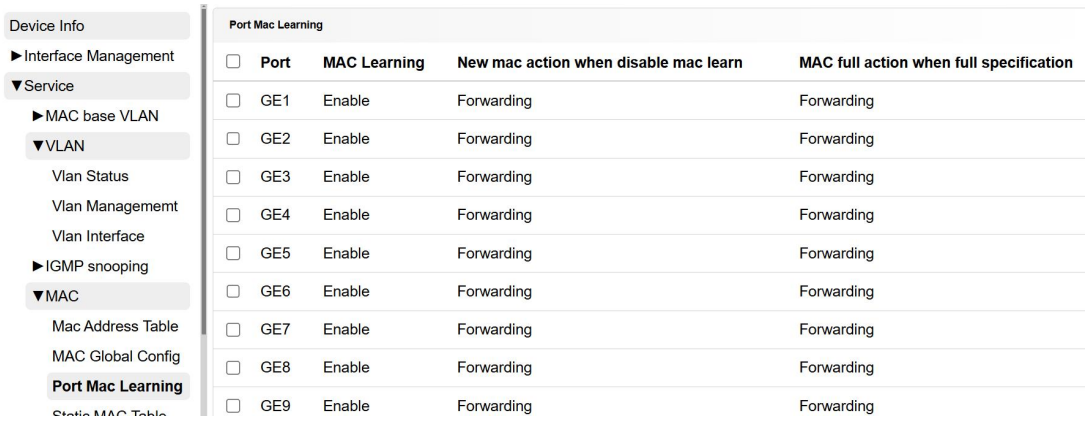


Figure 5-20

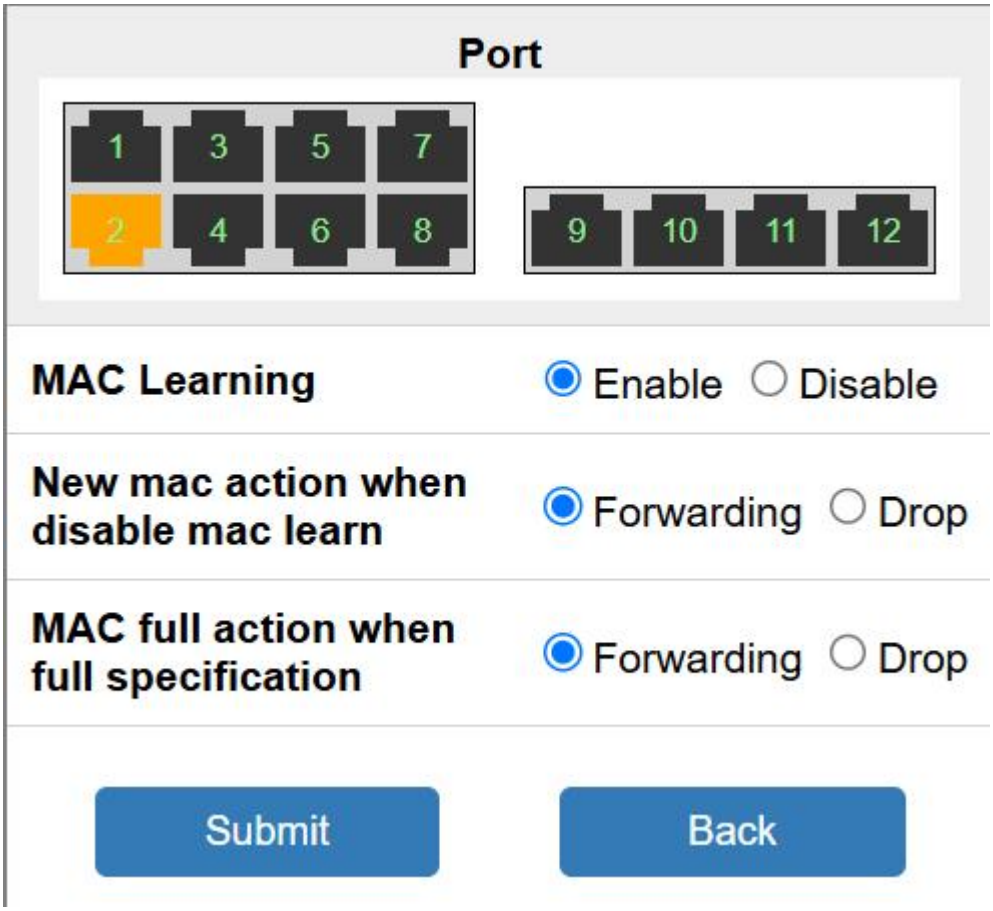


Figure 5-21

Parameter Description

Parameter Item	Note
Port	Physical port
MAC Learning	Port MAC learning status, including Enable and Disable

New mac action when disable mac learn	Disabling MAC learning suppresses forwarding of new MAC addresses, including both Forwarding and Drop actions. This behavior only takes effect when MAC learning is disabled.
MAC full action When full specification	Enable MAC learning. When a port reaches its maximum MAC address capacity, MAC addresses exceeding the limit will be handled as follows: Forwarding and dropping.

5.3.4 Static MAC Table

Used for manually adding static MAC address table entries. (As shown in Figure 5-22) The specification supports configuration of up to 64 entries.

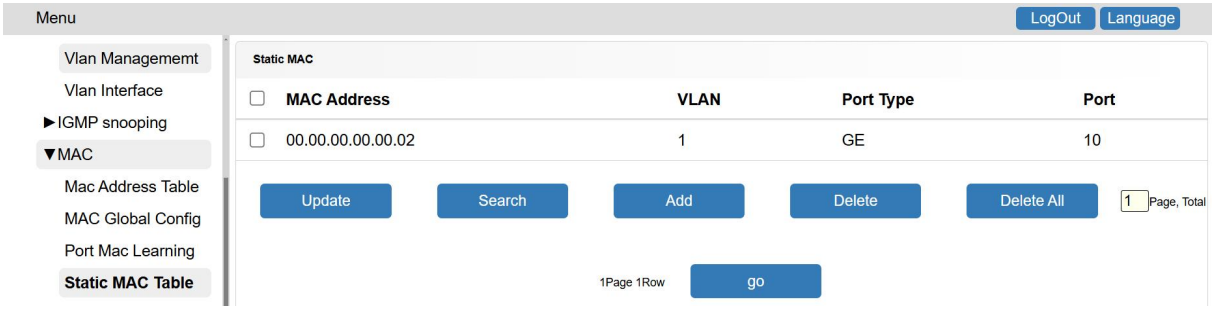


Figure 5-22

Parameter Description

Parameter Item	Note
MAC Address	The MAC address corresponding to a static MAC table entry only supports configuration of a unicast address.
VLAN	VLAN ID
Port Type	Port Type
Port	Port ID

Attention:

- Static MAC addresses share resources with the FDB and are constrained by the total resource limit. Static MAC addresses can override dynamic FDB entries.

5.3.5 Black Hole MAC Table

Used for manually adding black hole MAC address table entries, (as shown in Figure 5-23) the specification supports configuring up to 64 entries. When the device receives a packet with a destination MAC or source MAC address matching a black hole MAC address, it is discarded immediately.

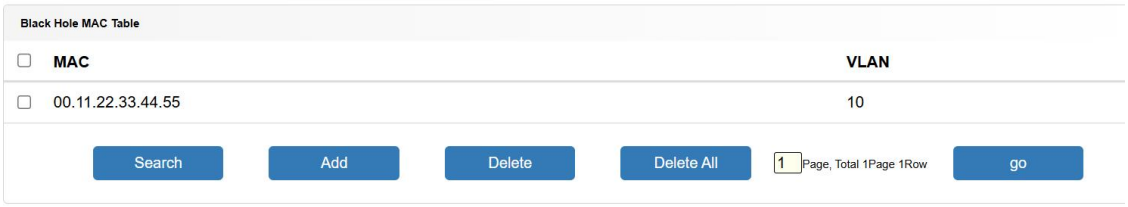


Figure 5-23

Parameter Item	Note
MAC	The MAC address corresponding to the black hole MAC supports only unicast addresses.
VLAN	VLAN address corresponding to the MAC address of the black hole

Attention:

- Black hole MAC and FDB tables share the same resources, with specifications constrained by total resource limits
- Black hole MAC addresses can override dynamic FDB tables
- Black hole MAC and FDB tables share the same resources, with specifications constrained by total resource limits

5.3.6 MAC Limit

MAC address learning limit per port. The default status is Disabled. A learning count of 0 indicates no restriction. (As shown in Figure 5-24)

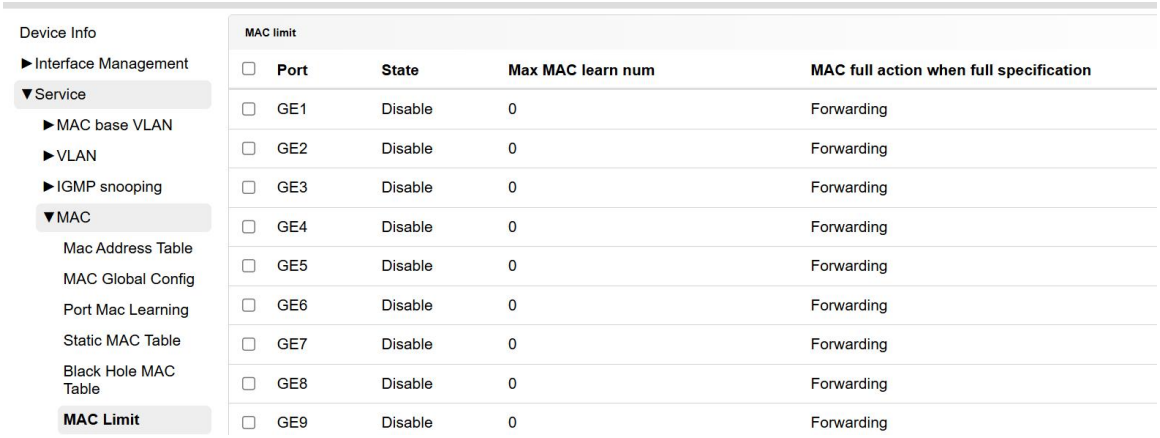


Figure 5-24

Configure the maximum MAC address learning count for Port 1 to 100. Check GE1, click “Modify” to enable the feature, configure the maximum MAC address learning count to 100, then click “Submit” to apply the changes (as shown in Figure 5-25). Port 1 can only learn up to 100 MAC addresses.

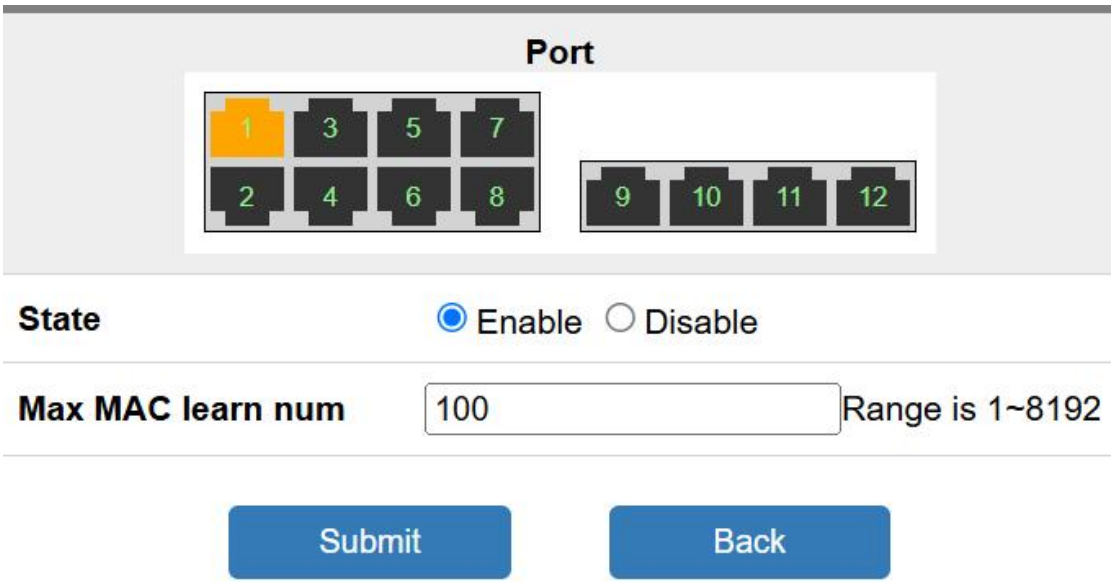


Figure 5-25

Parameter Description

Parameter Item	Note
Port	Display port information
State	Is address restriction enabled for this port?
Max MAC Learn num	Maximum MAC address learning count for this port after enabling address restriction
MAC full action when full specification	After learning the maximum MAC address specification, other MAC forwarding actions

5.4 Mirror Config

Through the mirroring function, users can duplicate packets from a device port and send them out through another port on the device. By connecting a tester or other packet collection device to this port, users can capture and analyze the original packets. The mirroring function does not affect the original network traffic on the switch.

The mirror source refers to the original network traffic being monitored. Source port: A port requiring monitoring or analysis, supporting only physical ports. The mirror destination specifies the port where traffic replicated via mirroring is to be delivered. Supports configuring mirroring for either receive direction, transmit direction, or both simultaneously. Access via Menu Bar > “Service” > “Mirror Config” (as shown in Figure 5-26).

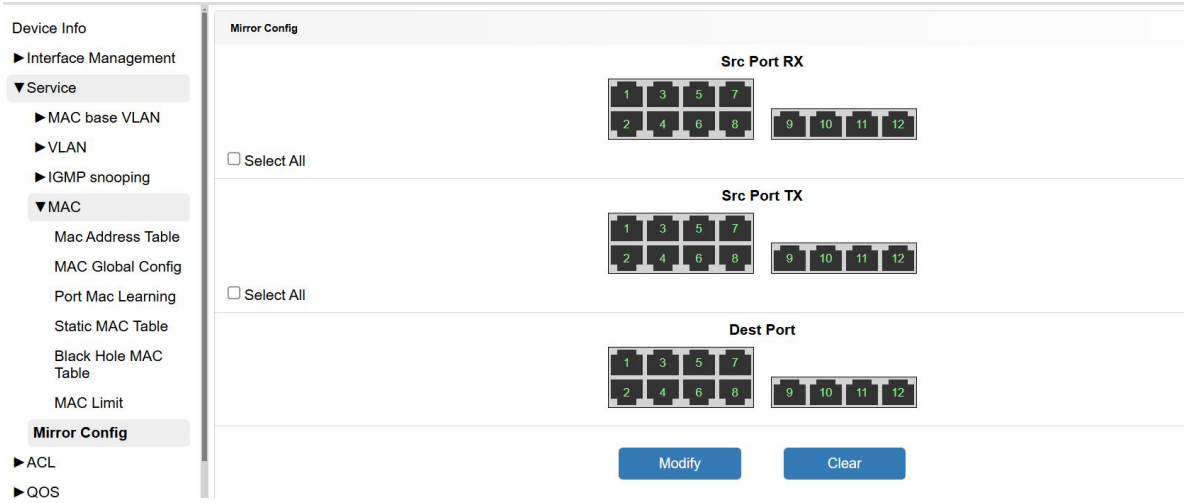


Figure 5-26

5.4.1 Mirror Configuration

Configure the mirroring function with source port 1 for receive direction, port 2 for transmit direction, and port 3 for both receive and transmit directions. Set the destination port to 12. Click “Modify” to successfully deploy the configuration. (As shown in Figure 5-27) Packets from the source port can be captured at the destination port.

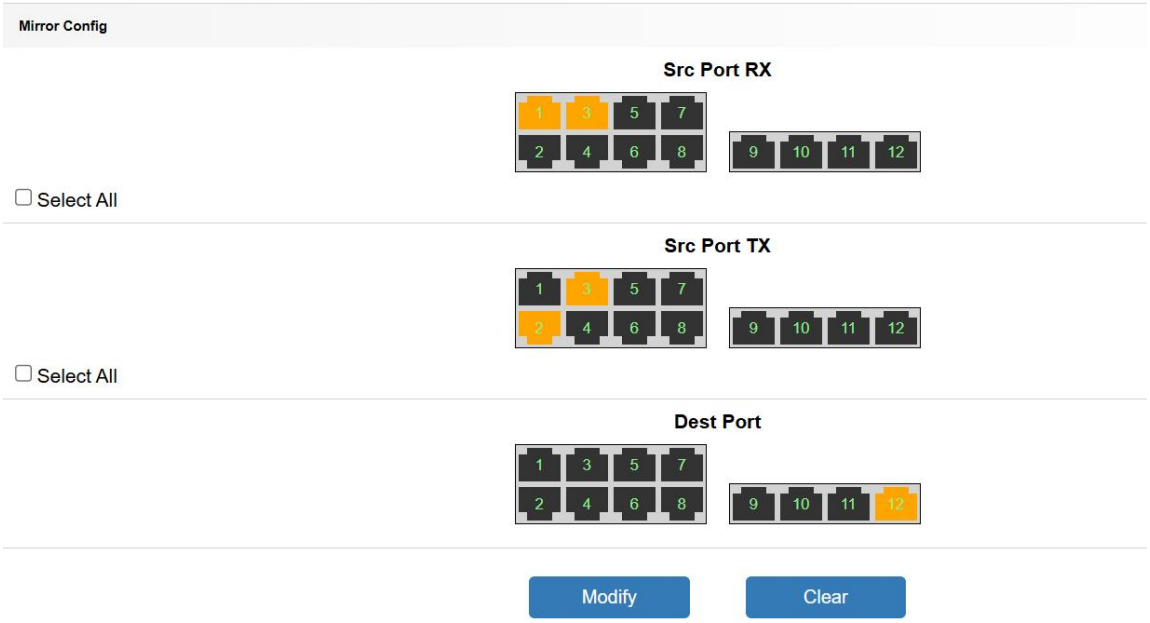


Figure 5-27

Click “Clear” to delete the configuration. (As shown in Figure 5-28)

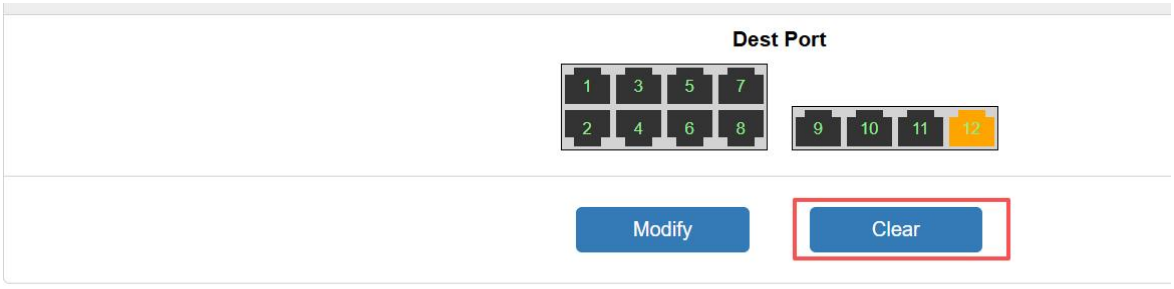


Figure 5-28

Attention:

- Configuration deployment must include the destination port; otherwise, deployment will fail.
- The destination port cannot be configured to match the source port.

5.5 IGMP snooping

Layer 2 switches use IGMP Snooping to control multicast traffic flooding, ensuring multicast traffic is forwarded only to interfaces associated with IP multicast devices. As the name implies, IGMP Snooping (Internet Group Management Protocol Snooping) requires LAN switches to monitor IGMP transmissions between hosts and routers, tracking multicast group member ports. Click the menu bar > “Service ” > “IGMP Snooping” to access the page (as shown in Figure 5-29).

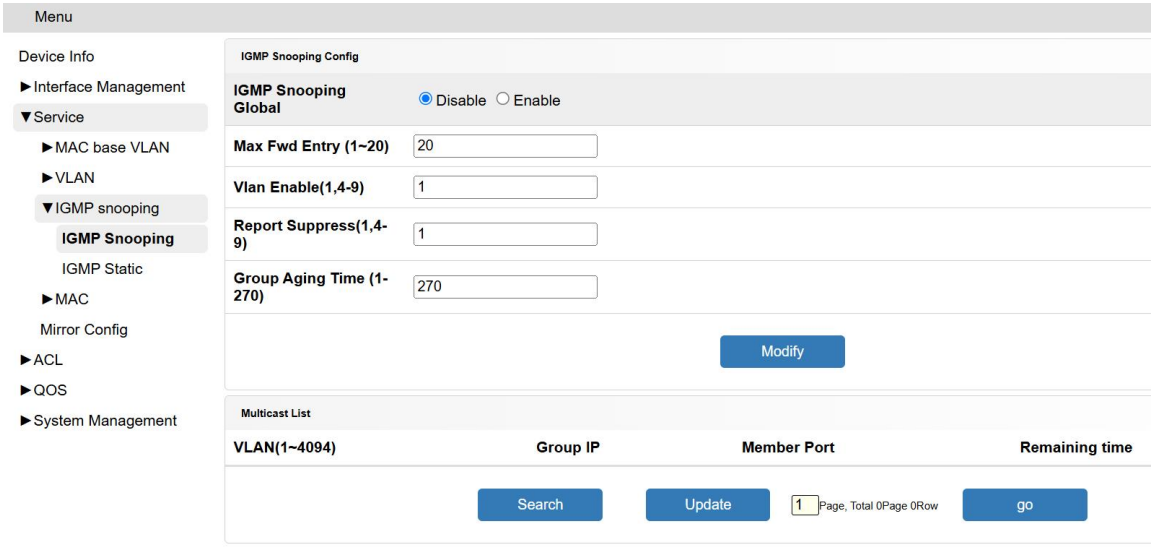


Figure 5-29

5.5.1 IGMP Snooping Configuration

IGMP Snooping configuration must be enabled both globally and per VLAN. When IGMP Snooping is disabled globally, enabling it only at the VLAN level will be ineffective. When IGMP Snooping is enabled globally, it can be selectively disabled on specific VLANs. (As shown in Figure 5-30) Enable IGMP Snooping for VLAN 1.

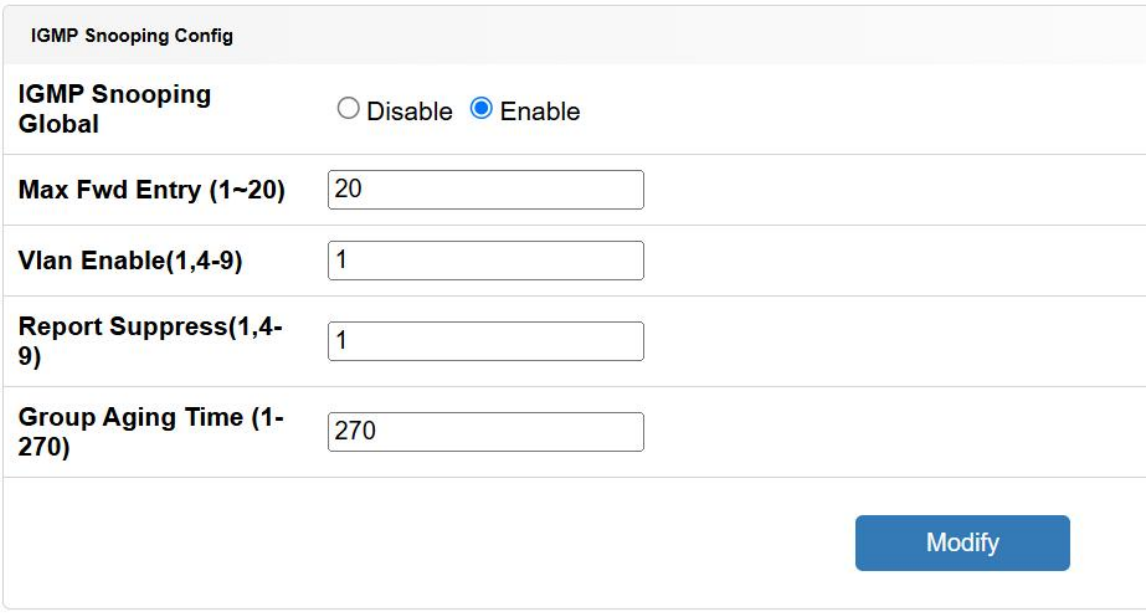


Figure 5-30

Parameter Description

Parameter Item	Note
IGMP Snooping Global	IGMP Snooping Global Mode: Enable or Disable
Max Fwd Entry	Limit the maximum number of multicast entries learned dynamically
VLAN Enable	Select the VLAN and enable IGMP snooping, provided that the VLAN exists.
Report Suppress	Select a VLAN to enable packet suppression, provided that the VLAN exists.
Group Aging Time	Configure the multicast aging time, which can be modified before the multicast group is created.

Multicast List

Used to record dynamic multicast entries, supporting IGMP versions 1-3 (as shown in Figure 5-31). The maximum specification supports 20 entries. When static multicast entries exist, these 20 entries will be shared with the static multicast entries. To prevent the use of protocol multicast addresses, reserved addresses 224.0.0.1–224.0.0.255 are restricted from being learned into the dynamic multicast table. IGMP v3 only supports learning multicast entries and does not support source address filtering. When IGMP snooping receives an IGMP leave message, it immediately removes the port from the multicast group.

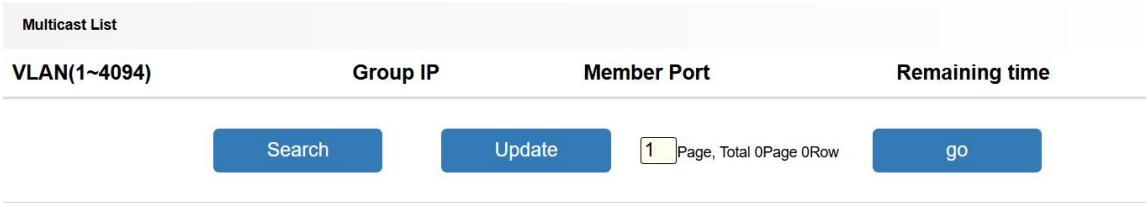


Figure5-31

Parameter Description

Parameter Item	Note
VLAN	Multicast Table Entries VLAN
IP	Multicast IP address
Port	Multicast Member Port

Supports search, refresh, and page navigation functions. To filter table entries, click “Search,” enter the criteria, then click “Submit” to locate entries. (As shown in Figure 5-32).

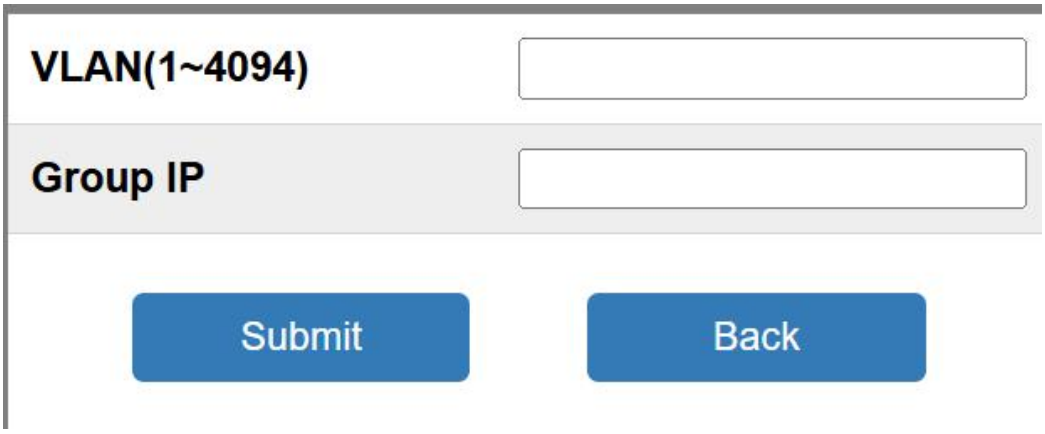


Figure5-32

5.5.2 IGMP Static

To configure static IGMP multicast entries, click the menu bar > “Service Management” > “IGMP Snooping” > “IGMP Static ” to enter (as shown in Figure 5-33).

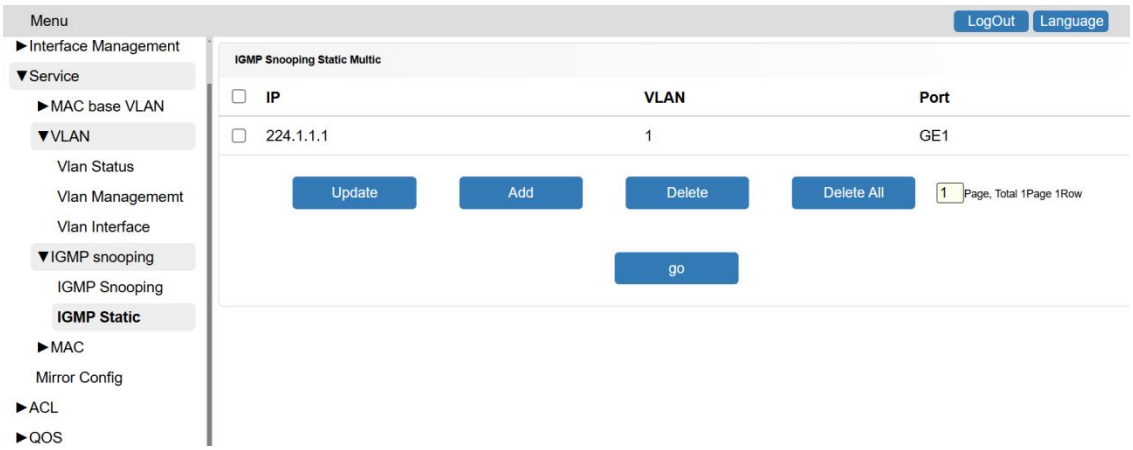


Figure 5-33

Used to configure static multicast entries. These entries are directly pushed to the hardware forwarding table, thus eliminating the need to enable IGMP Snooping. A maximum of 10 static multicast entries can be configured. The reserved addresses 224.0.0.1–224.0.0.255 do not support static multicast entry configuration. When both static and dynamic entries exist for the same port, static multicast entries take precedence. When the group address and VLAN are identical, they constitute a single entry. As shown in Figure 6-34, this configuration occupies two entries.

This page allows configuration of “Update,” “Add,” “Delete,” “Delete All,” and “Page Jump” (as shown in Figure 5-34).

Figure 5-34

Parameter Description

Parameter Item	Note
IP	Multicast IP addresses, reserved addresses: 224.0.0.1–224.0.0.255
VLAN	Multicast Vlan
Port	Multicast Member Port

Attention:

- Static and dynamic IGMP multicast entries share the same resources, with specifications constrained by total resource limitations.

6 ACL

Access Control Lists (ACLs) are primarily used to implement flow identification and access control functions. To filter packets, network devices require a set of matching rules to identify the packets that need filtering. Only after identifying specific packets can they allow or deny the corresponding packets based on predefined policies. ACLs classify packets using a series of matching conditions, which can include the packet's source address, destination address, port number, and so on.

Below is a brief introduction to terms and concepts related to ACLs:

Access Control Entry (ACE): Each ACE includes an action element (allow or deny) and a set of filtering elements based on criteria such as source address, destination address, etc.

MAC ACL: MAC ACLs can filter packets based on MAC source address (MAC-SA) and MAC destination address (MAC-DA). MAC addresses can be configured with masks or set to specific host MACs. MAC ACLs can also filter packets based on other Layer 2 fields, such as L2 type and L2 type mask.

IPv4 ACL: IPv4 ACLs can filter packets based on IP source address (IP-SA) and IP destination address (IP-DA). IP addresses can be configured with masks or set to specific host IP addresses. IPv4 ACLs can also filter packets based on other fields, such as TCP port, UDP port, etc.

6.1 ACL Rule

Used to configure MAC access control lists and ACL access control lists. After configuration, the entry activation function must be enabled on the “Port ACL” page for the settings to take effect.

MAC Access Control List: For example, configure to drop packets with a source MAC address of 0000.0000.1111 (as shown in Figure 6-1).

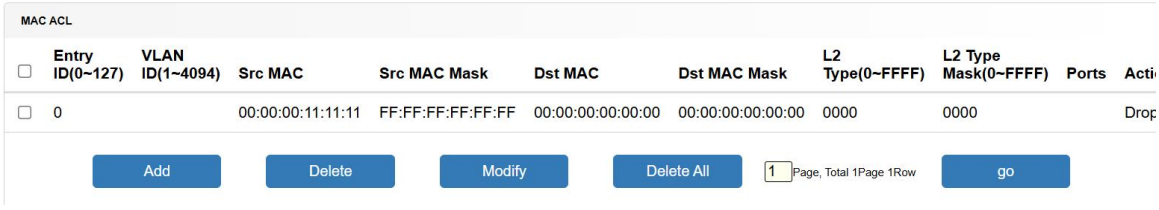


Figure6-1

IP Access Control List: For example, configure to drop packets originating from the source IP address 1.1.1.1/24 (as shown in Figure 6-2).。

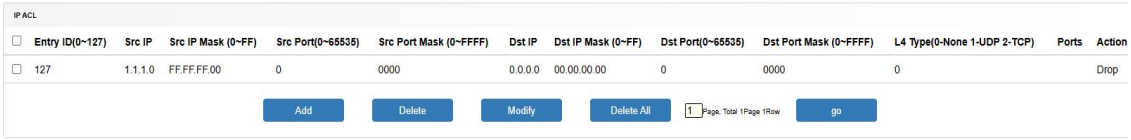


Figure 6-2

Parameter Description

MAC ACL Rules Page

Parameter Item	Note
Entry ID	Supports 0-127 table entries, with no duplicate entries allowed. Entries 0-63 form one group, and entries 64-127 form another group. Both groups operate in parallel with parallel priority, where lower numbers within each group indicate higher priority.
VLAN ID	VLAN frame
Src MAC	Source MAC Address
Src MAC Mask	Source MAC address mask, such as 0xff indicating all bits are valid, or 0x0f indicating only the lower 4 bits are valid.
Dst MAC	Destination MAC Address
L2 Type	Layer 2 Message Type
L2 Type Mask	Layer 2 type mask for packets, such as 0xff indicating all bits are valid, and 0x0f indicating only the lower 4 bits are valid.
Port	Physical Port for Messages
Action	After matching, perform the discard or allow action.

IP Access Control List Rules Page

Parameter Item	Note
Entry ID	Supports 0-127 table entries, with no duplicate entries allowed. Entries 0-63 form one group, and entries 64-127 form another group. Both groups operate in parallel with parallel priority, where lower numbers within each group indicate higher priority.
Src IP	Source IP Address of the Packet
Src IP Mask	Source IP address mask in the packet, 1 indicates valid, 0 indicates invalid
Src Port	Source Port
Src Port Mask	Source Port Mask

Dst IP	Destination IP Address
Dst IP Mask	Destination IP address mask in the packet; 1 indicates valid, 0 indicates invalid.
Dst Port	Destination Port
Dst Port Mask	Destination Port Mask
L4 Type	Four-layer types: 1. UDP 2. TCP
Port	Physical Port for Messages
Action	After matching, perform the discard or allow action.

6.2 Port ACL

Used to configure ACL rules for the activation port. The port is disabled by default (as shown in Figure 6-3). Check the port and click “Modify” to activate MAC ACL or IPv4 ACL (as shown in Figure 6-4).

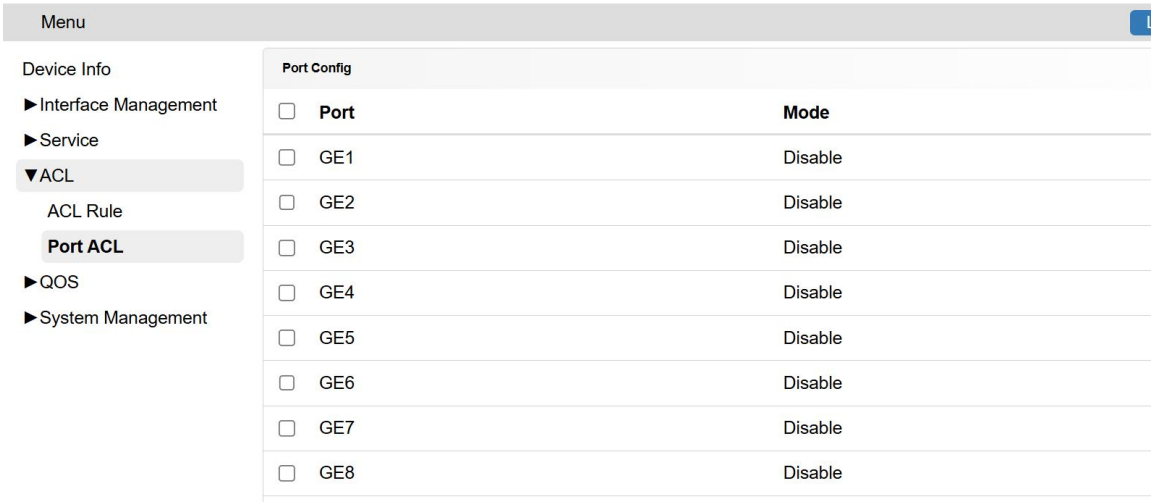


Figure 6-3

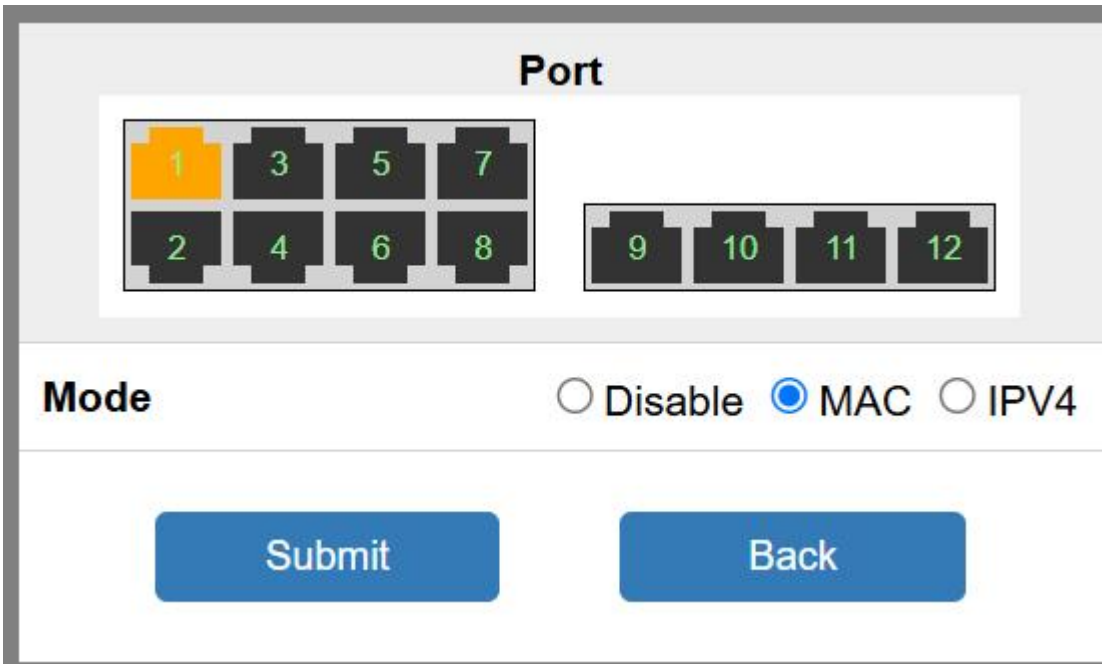


Figure 6-4

Parameter Description

Parameter Item	Note
Port	Select ports where ACL rules apply
Mode	1. Disable: ACL is not enabled on this port. 2. MAC: ACL is enabled on this port with MAC matching mode selected. 3. IPV4: ACL is enabled on this port with IP matching mode selected.

7 QoS

Quality of Service (QoS) is a concept prevalent in any scenario involving a service provider-consumer relationship. It evaluates the provider's ability to meet customer service requirements. This assessment is typically not a precise score but focuses on analyzing under what conditions service is satisfactory and where deficiencies exist, enabling targeted improvements. Within the Internet, QoS evaluates a network's capability to deliver packets. Given the diverse services networks provide, QoS assessments can be based on different aspects. Typically, QoS refers to evaluating a network's ability to support core requirements during packet delivery, such as delay, delay jitter, and packet loss rate. QoS serves as a network security mechanism and a technical solution for addressing issues like network delay and congestion. Under normal circumstances, QoS is unnecessary for applications with no strict time constraints, such as web services or email configurations. However, it becomes essential for mission-critical and multimedia applications. During network overload or congestion, QoS ensures vital traffic avoids delays or discards while maintaining overall network efficiency.

7.1 Domain Mapping

In QoS processing, the switch maps all traffic to internal priority handling. Based on this priority, the system performs a series of processing steps on the packets. During flow classification, QoS uses configurable mapping tables to assign packets. The internal priority consists of 6 bits mapped from CoS and DSCP values, with these tables containing CoS-Priority-Color and DSCP-Priority-Color mappings. During traffic policing, QoS assigns packets a new priority and color, such as based on Class-Map. Each QoS domain exhibits distinct behaviors described above.

Class of Service (CoS) is the field determining packet priority at Layer 2 of the network. QoS distinguishes traffic with varying priorities by setting different CoS values. Layer 2 802.1Q packets can carry a 2-byte VLAN tag, with the upper 3 bits reserved for user-specified priority. Other packet types cannot carry VLAN tags. CoS has 3 bits, with values ranging from 0 to 7.

Differential Service Code Point (DSCP) uses 6 bits to distinguish packet priority in Layer 3 networks. DSCP values range from 0 to 63, as shown on the page.

The Domain Mapping page configures the correspondence between queues, mapping methods, priorities, and colors (as shown in Figure 7-1).

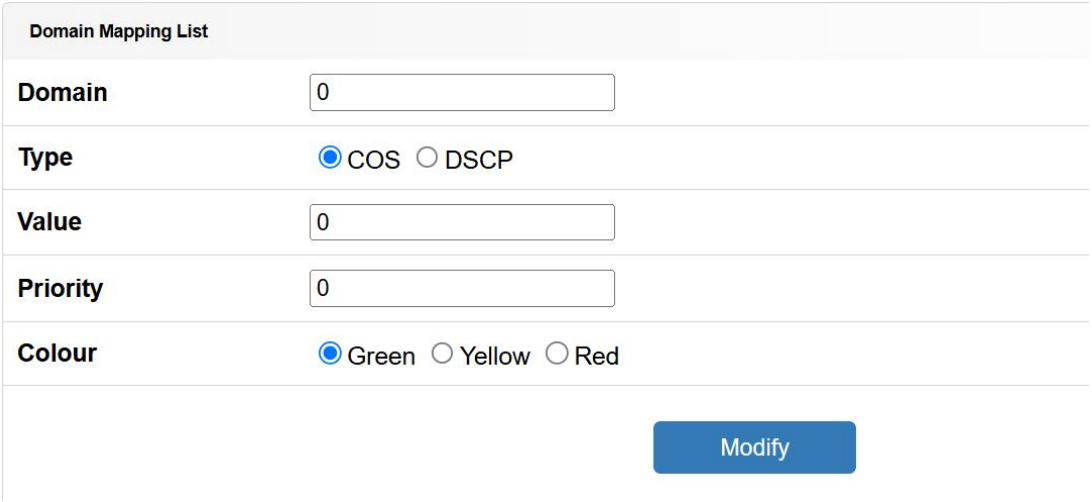


Figure 7-1

Domain Mapping table

Domain	Type	Value	Priority	Colour
0	COS	0	0	Green
0	COS	1	1	Green
0	COS	2	2	Green
0	COS	3	3	Green
0	COS	4	4	Green
0	COS	5	5	Green
0	COS	6	6	Green
0	COS	7	7	Green
0	DSCP	0	0	Green
0	DSCP	1	0	Green
0	DSCP	2	0	Green
0	DSCP	3	0	Green
0	DSCP	4	0	Green
0	DSCP	5	0	Green
0	DSCP	6	0	Green
0	DSCP	7	0	Green

Figure 7-2

Parameter Description

Parameter Item	Note
Domain	Internal Priority Mapping Table of the Switch. ID Number: 0-7
Type	Check the COS/DSCP field in the packet
Value	The COS field corresponds to values from 0 to 7, while the DSCP field corresponds to values from 0 to 63.
Priority	The message-specified field corresponds to the priority in the Domain table, with a range of 0-7.

Colour	There are three colors: green, yellow, and red, each representing a different forwarding method.

7.2 Port Config

Used to configure port mapping relationships, with the default type being COS (as shown in Figure 7-3). Supports COS, DSCP, and Default configuration methods (as shown in Figure 7-4).

Port Config

Port	Domain ID	Type
GE1	0	COS
GE2	0	COS
GE3	0	COS
GE4	0	COS
GE5	0	COS
GE6	0	COS
GE7	0	COS
GE8	0	COS
GE9	0	COS
GE10	0	COS
GE11	0	COS
GE12	0	COS

Figure 7-3

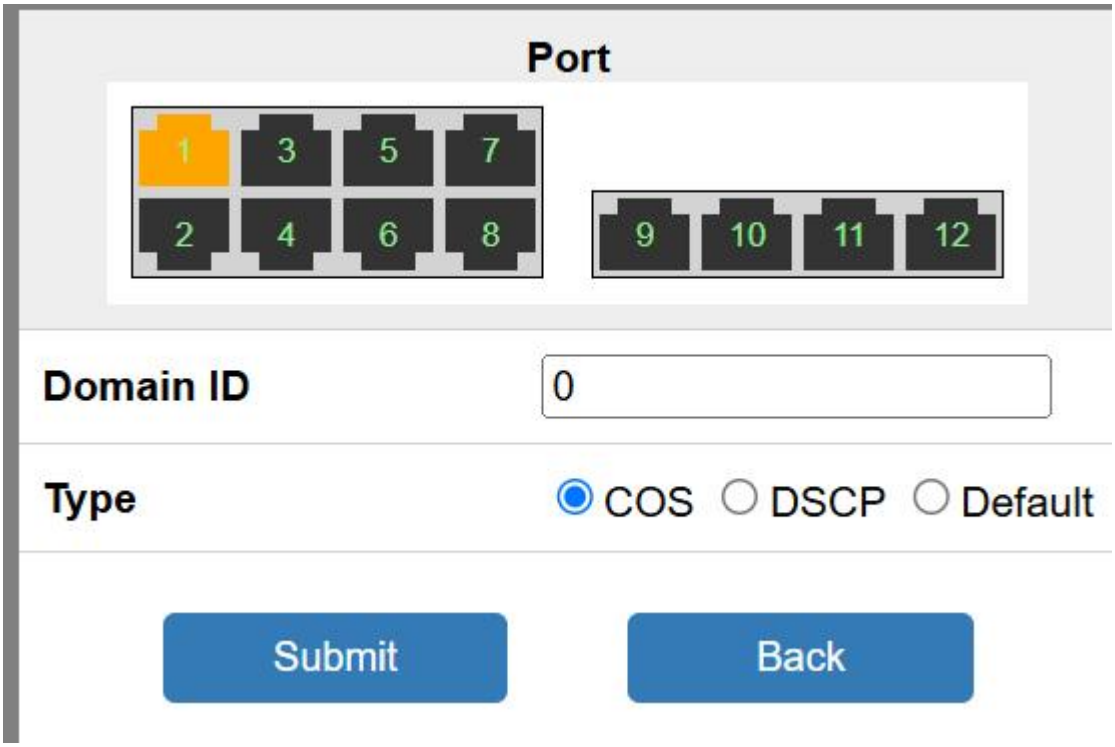


Figure 7-4

Parameter Description

Parameter Item	Note
Port	Select the configured port
Doamin ID	Internal Priority Mapping Table of the Switch. ID Number: 0-7
Type	1. COS: Inspect the COS field in packets to route them into different queues for congestion management. 2. DSCP: Inspect the DSCP field in the IP header to route packets into different queues for congestion management. 3. Default: Do not enable QoS functionality.

7.3 Port Policy

Used to configure port rate limiting functionality, which is disabled by default (as shown in Figure 7-5) (as shown in Figure 7-6). Configuration takes effect at the ingress. Colorblind mode does not detect packet color, with the limited rate being approximately CIR+EIR. Color-sensitive mode first determines packet color, then decides whether to forward it, and sets the limited rate accordingly.

Figure7-5

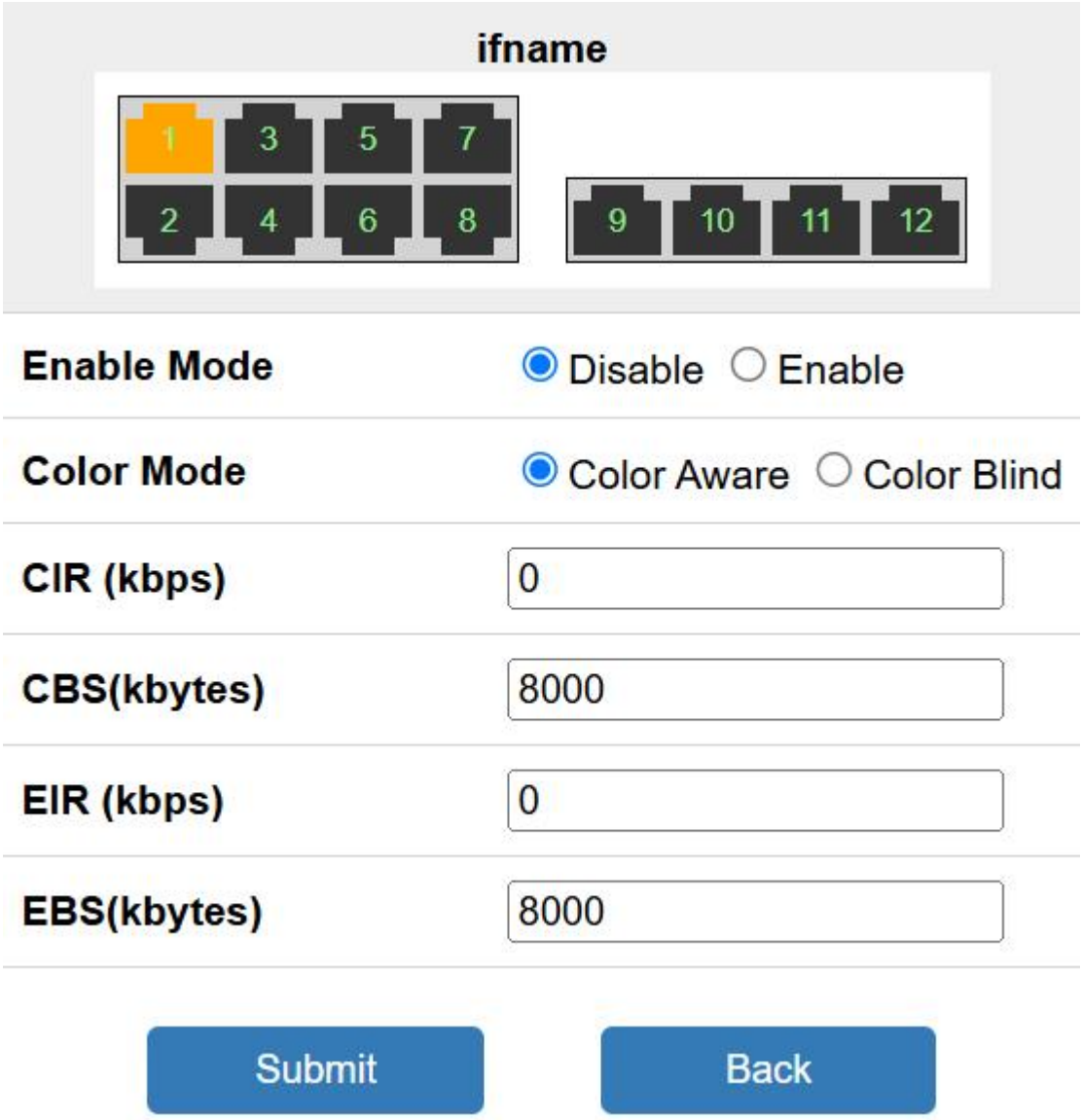


Figure 7-6

Parameter Description

Parameter Item	Note
Enable Mode	Turn On/Off
Color Mode	Color_Aware Color Sensitive, Color_Blind Color Blind
CIR	Committed information rate, unit: kbps. Must be entered as a multiple of 8. Range: 0-4,190,000.
CBS	Commitment to sudden size changes, range: 0-8000
EIR	Excess information rate, in kbps. Must be entered as a multiple of 8. Range: 0-4,190,000
EBS	Overrange sudden size, range: 0-8000

7.4 QOS Congestion

Used to configure port queue scheduling methods and weights, (as shown in Figure 7-7) and (as shown in Figure 7-8);

QOS Congestion

ifname	Q0 Mode	WDRR Weight	Q1 Mode	WDRR Weight	Q2 Mode	WDRR Weight	Q3 Mode	WDRR Weight	Q4 Mode	WDRR Weight	Q5 Mode	WDRR Weight	Q6 Mode	WDRR Weight	Q7 Mode	WDRR Weight
GE1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE2	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE3	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE4	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE5	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE6	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE7	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE8	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE9	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1
GE10	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1	WDRR	1

Figure7-7

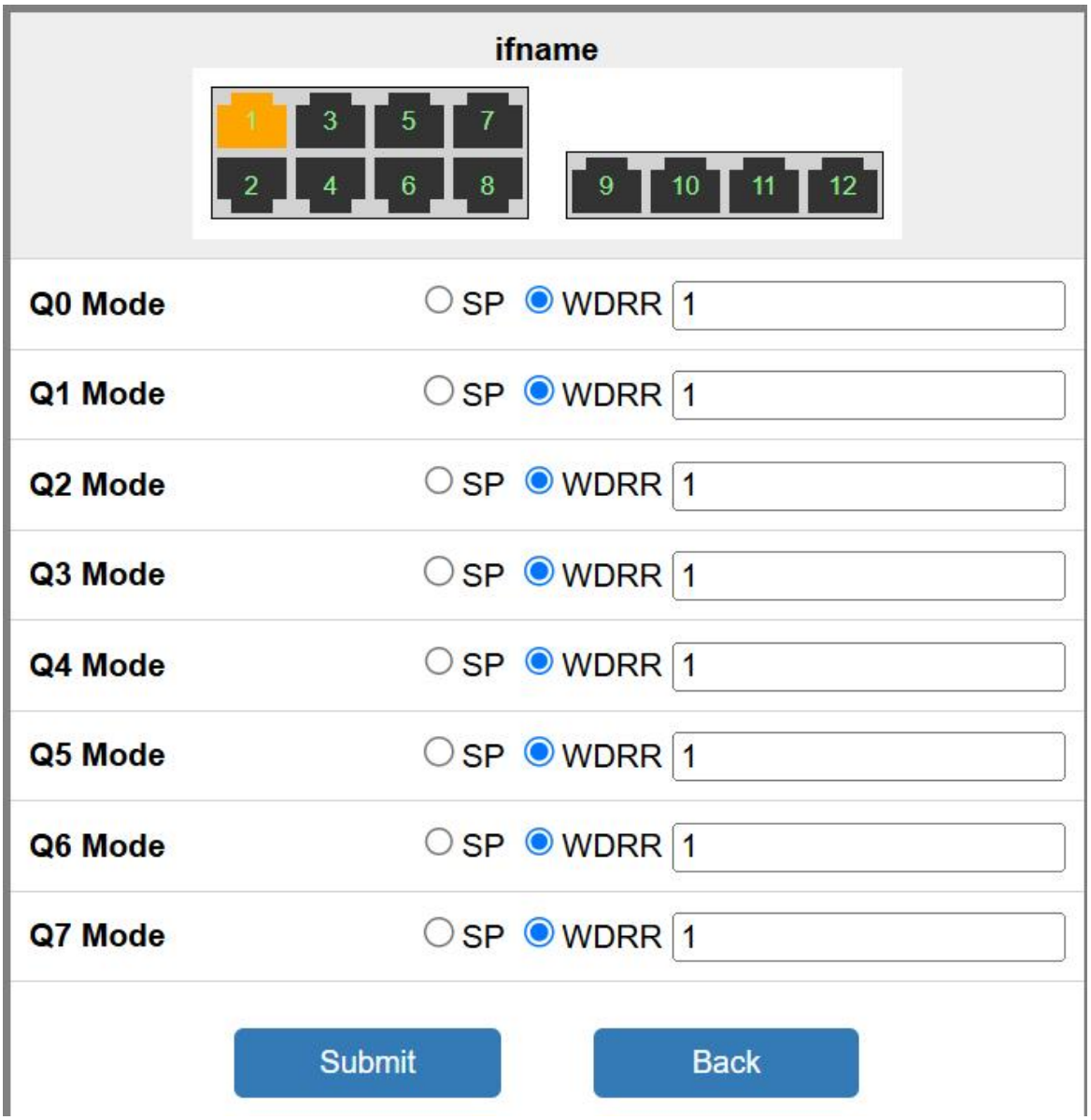


Figure7-8

Parameter Description

Parameter Item	Note
Queue	Each port has 8 queues, with different modes and weights selected for each port.
SP	Strict priority, default weight is only 1 SP mode has higher priority than WDRR. If multiple SP modes exist, the queue with the higher number has higher priority.
WDRR	Weighted average, supporting weight configuration, calculated as a weighted average among multiple WDRRs.

7.5 Port Shaping

All traffic passing through the switch's physical interfaces can be shaped. Traffic exceeding the shaping rate is buffered, but if the buffer becomes full, subsequent packets are dropped until space is freed. Note: Configuration takes effect on the output port.

The following example demonstrates how to configure physical interface-based traffic shaping. In this example, the forwarding rate on the GE1 port will eventually converge to 1000kbps (as shown in Figure 7-9).

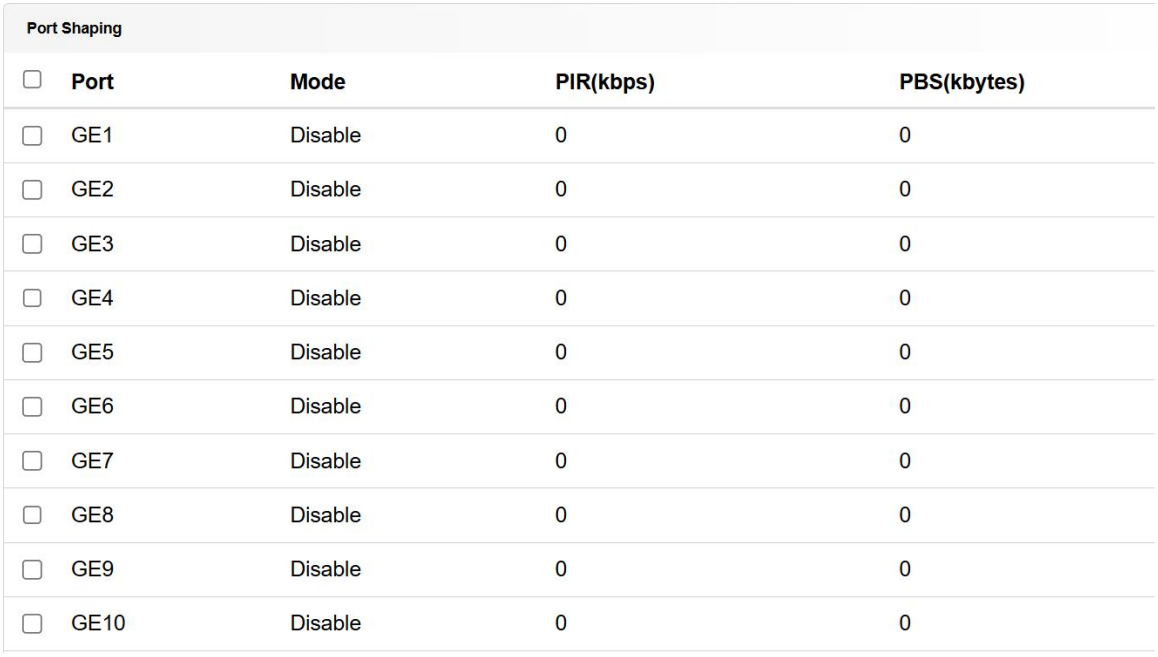


Figure 7-9

Parameter Description

Parameter Item	Instruction
Port	Select the configured port
Mode	Enable or disable this feature
PIR	Peak information rate, range: 0-4,190,000
PBS	Peak burst size, range: 1–2000

7.6 Queue Shaping

Traffic can be shaped as it passes through queues in the outgoing direction of a switch. Traffic exceeding the shaping rate is buffered, but if the buffer becomes full, subsequent packets are discarded until space is freed. The following example demonstrates how to configure traffic shaping on an outbound queue. In this example (as shown in Figure 7-10), queue shaping is configured for queue 2 on the GE3 port; packets will be discarded when the flow rate in queue 2 exceeds 1000 kbps.

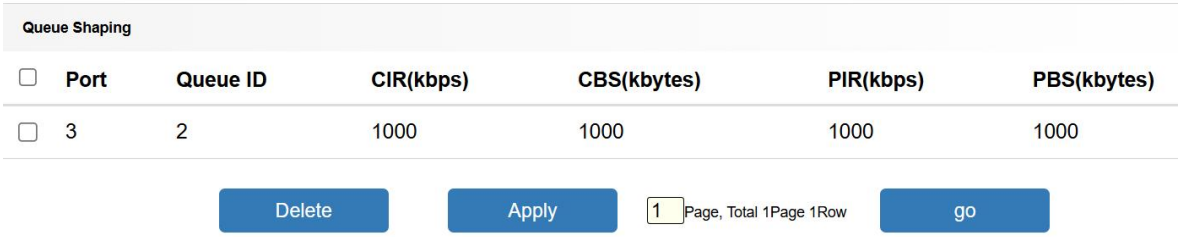


Figure 7-10

Parameter Description

Parameter Item	Note
Port	Select the port number for configuration
Queue ID	A port has 8 queues, with ID numbers ranging from 0 to 7.
CIR	Committed information rate, range: 0-4,190,000
CBS	Commitment to sudden size changes, range: 1-2000
PIR	Peak information rate, range: 0–4,190,000
PBS	Peak burst size, range: 1–2000

8 System Managment

8.1 System Config

This page enables users to configure device management settings, including “System Config” “Device Description” “Web Page Aging time,” “User Management” functions. Navigate to this page by clicking the menu bar, then “System Management,” followed by “System Config” (as shown in Figure 8-1).;

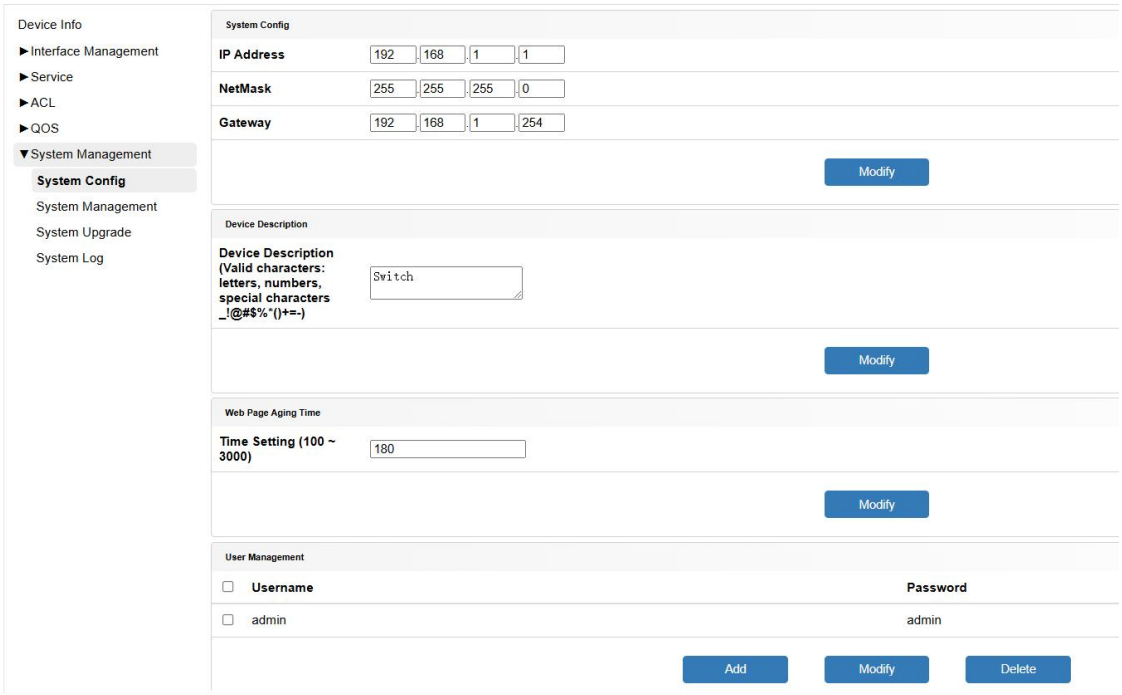


Figure 8- 1

8.1.1 System Config

This page is used to modify the IP address, NetMask, and Gateway for logging into the management device. For example, to change the IP address to 10.10.38.10, click “Modify” for the changes to take effect. (As shown in Figure 8-2). The default IP address is 192.168.1.1, the subnet mask is 24 bits, and the default gateway is 192.168.1.254.;

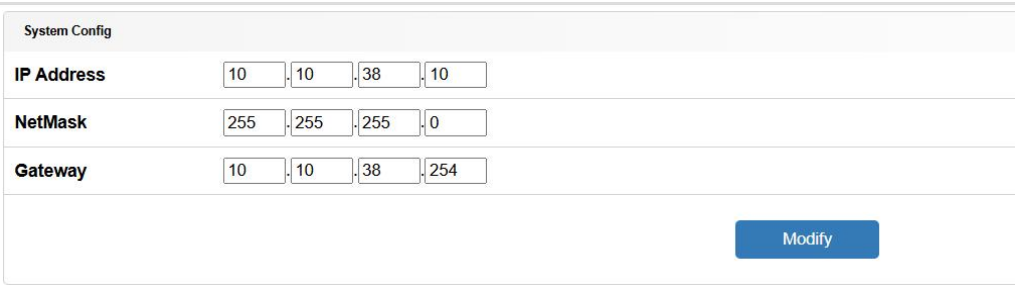


Figure 8-2

Attention:

- The IP address and subnet mask must match; the default gateway supports both empty and zero values.

8.1.2 Device Description

Used to modify the device description. After successful modification, you can navigate to the "Device Info" page to verify if the configuration was successful. Valid characters include letters, numbers, and special characters _!@#$%*()+=-, with a length supported between 1 and 32 characters. The default display is switch (as shown in Figure 8-3).

Figure 8-3

8.1.3 Web Page Aging Time

Used to configure the user page access timeout, with a configurable range of 100-3000 seconds (as shown in Figure 8-4). The default value is 180 seconds;

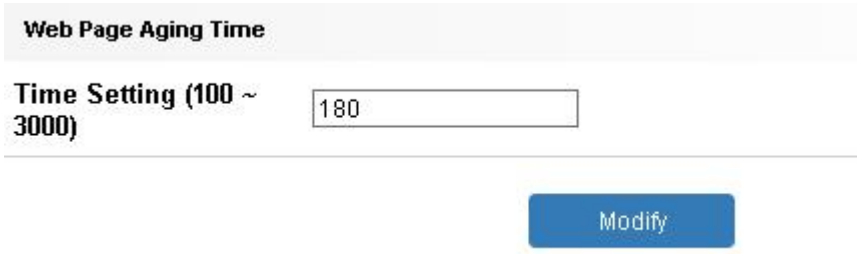


Figure 8-4

8.1.4 User Management

Used to configure the username and password for logged-in users. The default username and password are both admin. Supports configuring up to five usernames and passwords, with lengths ranging from 5 to 64 characters. Allows configuration of alphanumeric characters and underscores (as shown in Figure 8-5)；

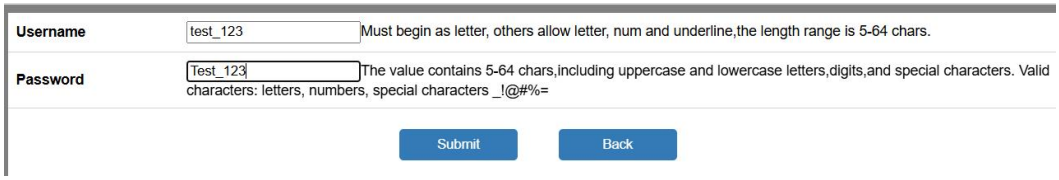


Figure 8-5

8.2 System Management

This page is used to save configurations, download configurations, upload configurations, reboot devices, and restore factory settings. Navigate to it by clicking the menu bar > “System Management” > “System Management” (as shown in Figure 8-6).；

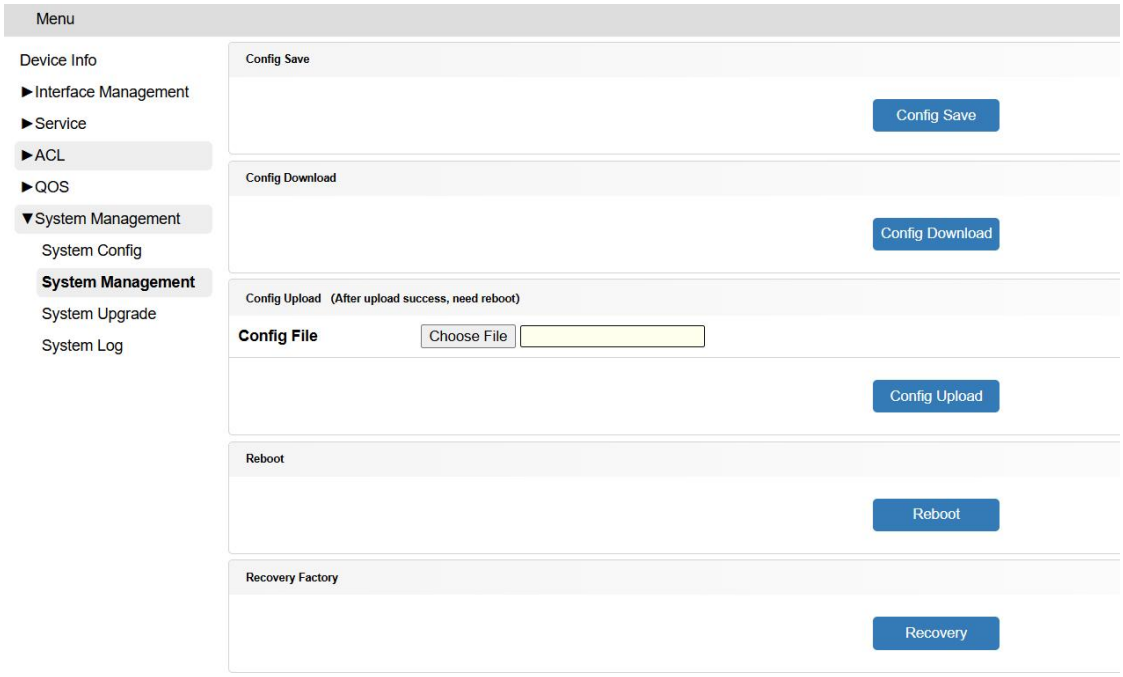
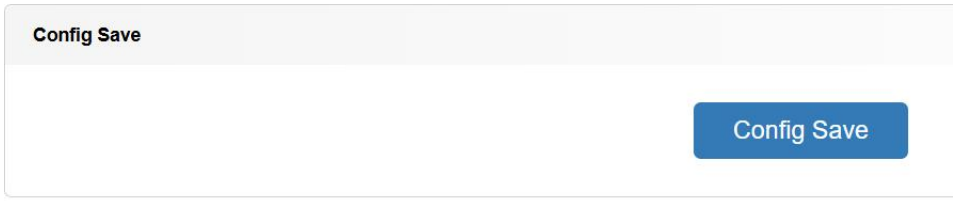


Figure 8-6

8.2.1 Config Save

The user saves the configuration by clicking “Config save” followed by ‘Sure’ (as shown in Figure 8-7). Upon successful completion, a prompt stating “Save start-config Successfully” will appear.；



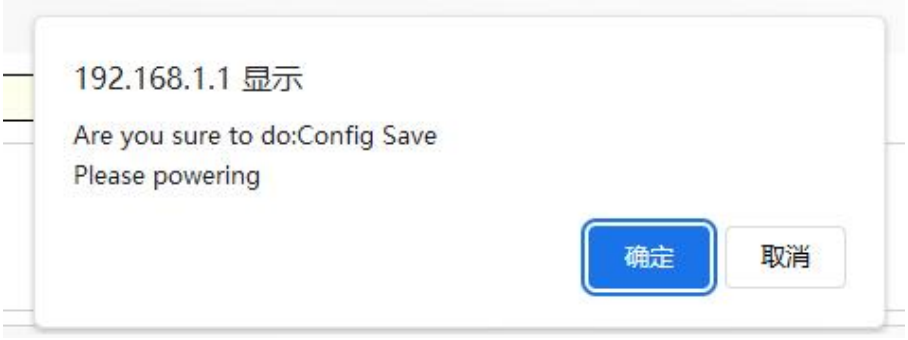


Figure 8-7

Attention:

- Do not power cycle during configuration saving, otherwise the settings will revert to default upon restart.

8.2.2 Reboot

To perform a soft restart on the device, click “Reboot” followed by “Sure” (as shown in Figure 8-8). During the restart process, all LED indicators will turn green.;

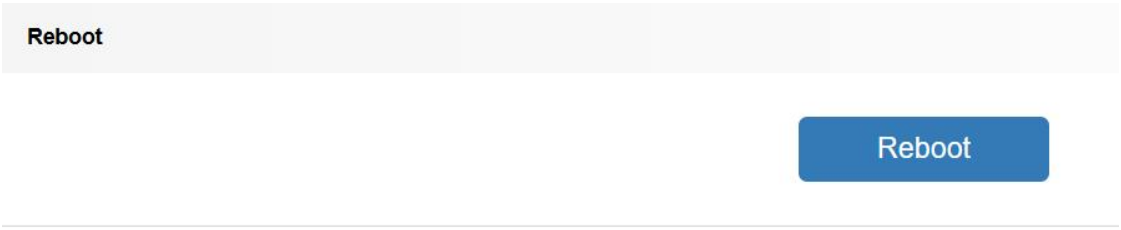


Figure 8-8

8.2.3 Recovery Factory

To restore the device to its default configuration, click “Recovery Factory” followed by “Sure” (as shown in Figure 8-9). Upon completion, all settings will revert to their default values.

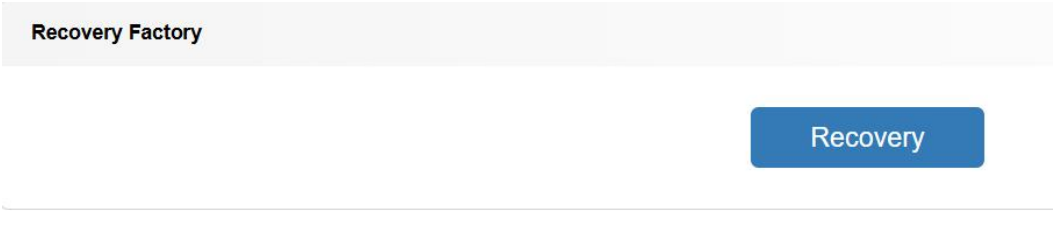


Figure 8-9

8.2.4 Config Download

To export the device configuration, click the “Config Download” button (as shown in Figure 8-10). The configuration file is named startup-config.conf.

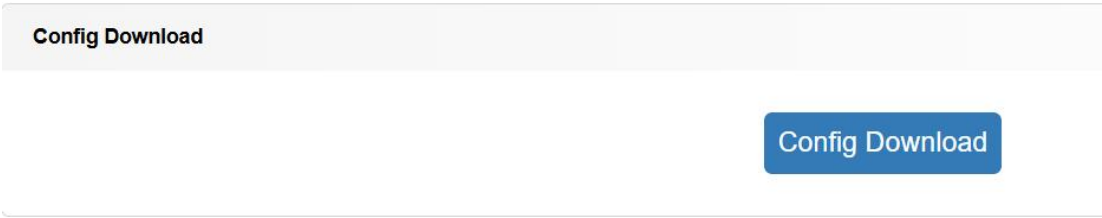


Figure 8-10

Attention:

- The exported configuration is the startup file, not the currently running configuration. To back up the current running configuration, save the configuration before proceeding with the backup.

8.2.5 Config Upload

If users need to import configuration files to the device, they can click the "Config Upload" button (as shown in Figure 8-11). After successful upload, the device must be restarted for the changes to take effect.

Figure 8-11

Attention:

- Configuration files cannot be imported between different models.

8.3 System Upgrade

To upgrade to the new host file, click Menu Bar > System Management > System Upgrade (as shown in Figure 8-12).

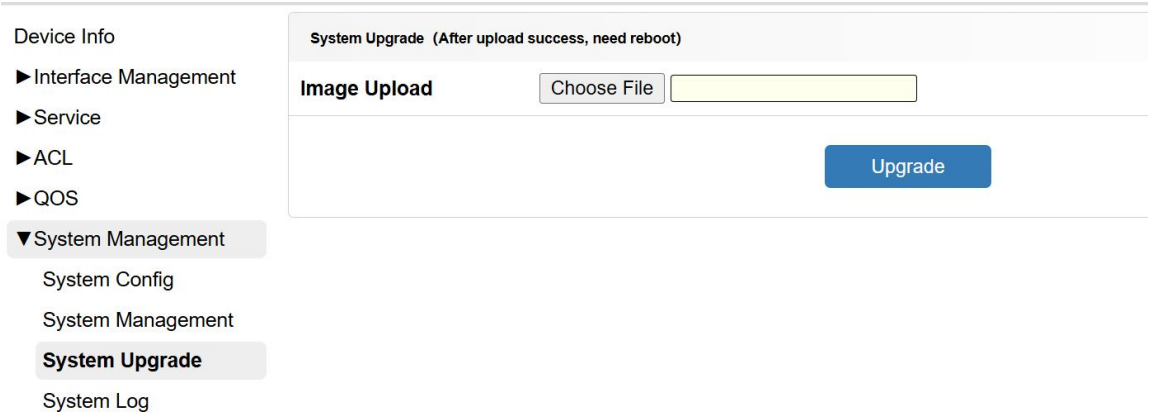


Figure 8-12

8.3.1 System Upgrade

Click Browse to select the host file to update, then click “Upgrade” and click “Sure” (as shown in Figure 8-13).

Figure 8-13

Attention:

- The selected file must be the corresponding version upgrade package for the device, with a file size range of 780K to 1024KB and a .bin file extension.

8.4 System Log

8.4.1 System Log

Used to display device system log information, download logs, and clear system logs. The specification for system logs is 50 entries, and old log information will be overwritten by new logs if it exceeds the specification. Startup, upgrade, and soft restart will automatically synchronize log information to flash.

Click on the menu bar - System Management - System Upgrade to enter (as shown in Figure 8-14);

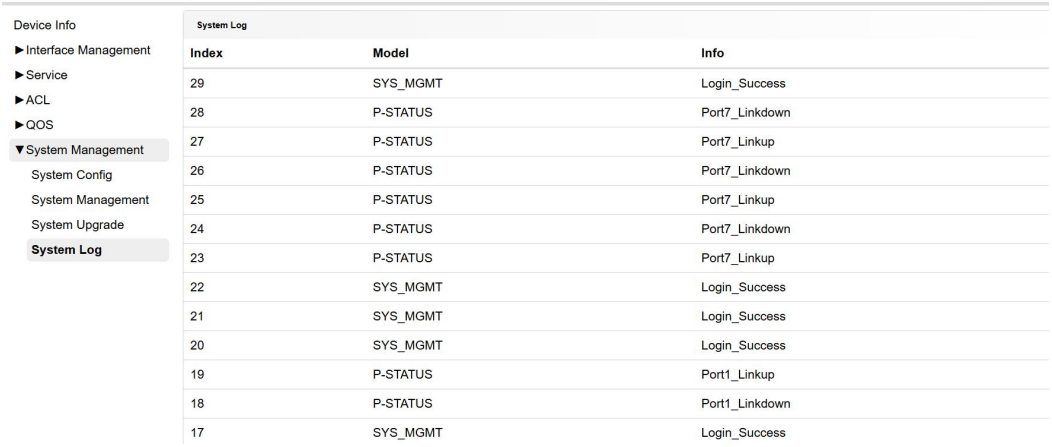


Figure 8-14

Clicking on 'Log Download' will automatically synchronize the log information to Flash before downloading. The downloaded system logs will be named 'log. txt'.

Clicking 'Clear' will delete the log information in the flash.