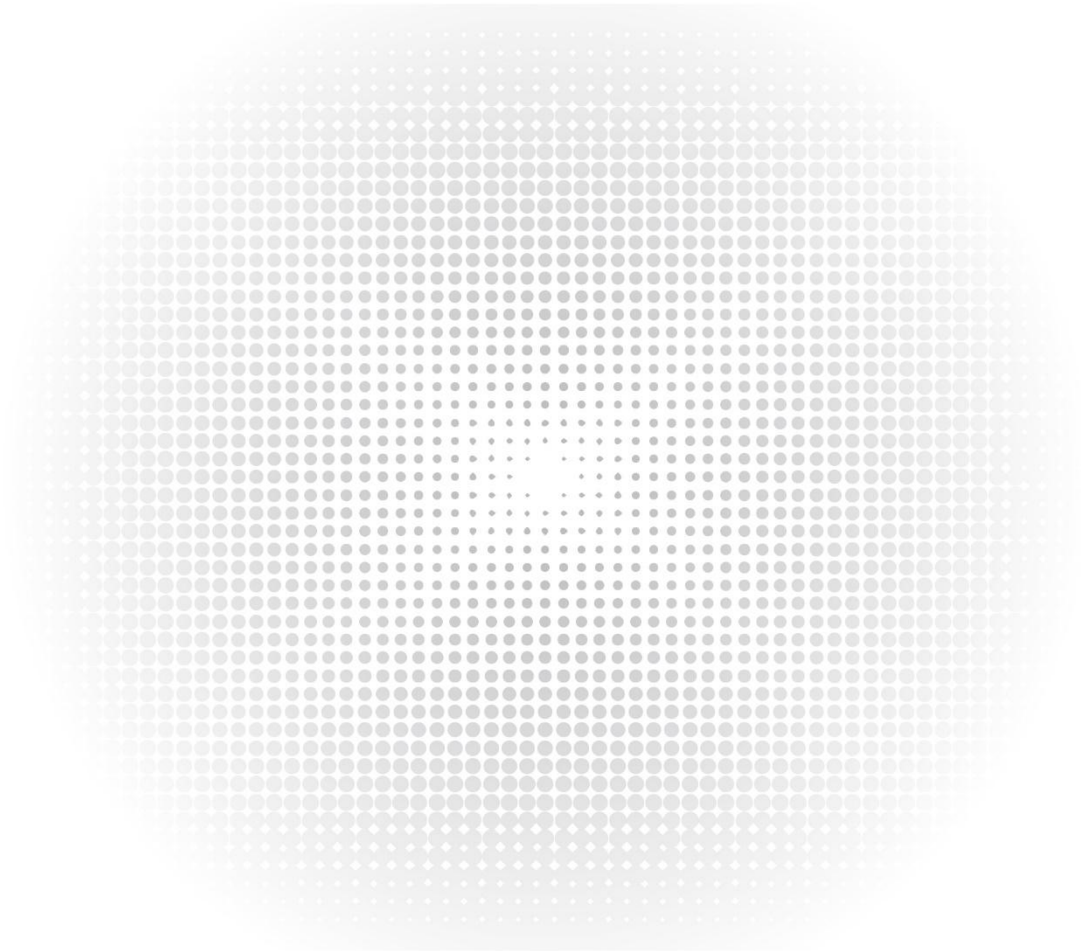
S5850 and S8050 Series Switches Web Management Guide

Models: S5850-24T16S; S5850-32S2Q;
S5850-48S6Q; S5850-48T4Q;
S5850-48S2Q4C; S8050-20Q4C;
S5850-24S2Q



WEB MANAGEMENT GUIDE

Contents

1. Web Login Configuration

Please be noted that this document takes the S5800-8TF12S switch as an example to explain how to perform web configuration.

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through web browser, the switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Management IP/ Route Configuration

Before web network management client can access switch by HTTP, user should configure the management IP and route by CLI on switch.

Command	Purpose
management ip address 10.10.38.2/23	Configure the management IP
management route add gateway 10.10.39.254	Configure the management route

1.1.2 User Configuration

User should add logging user by CLI before access switch by HTTP.

Command	Purpose
username admin password admin	add logging username and password

1.1.3 HTTP Configuration

Switches support to control the HTTP access, only when the HTTP service is enabled can HTTP exchange happen between switch and PC , when the HTTP service is closed, HTTP exchange stops, if you want to open HTTP service, please follow the following steps by CLI on switch:

(1) Use tftp or ftp to copy web image to the flash:
copy mgmt-if tftp://192.168.0.1/webImage.bin flash:/webImage.bin

(2) Load web image:
http server load flash:/webImage.bin

(3) Enable HTTP service for web network management :
service http enable

1.1.4 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

Command	Purpose
service https enable	Enable HTTPS service for web network management

1.1.5 Web Login

After configuration by CLI on switch, you can follow the following steps to login web page:

(1) Open IE browser, input address field with URL (universal resource locator) address of the switch.

(2) Enter username and password which user created with CLI(default is **admin/admin**), the login page is shown as the figure 1.

(3) Enter the main page.

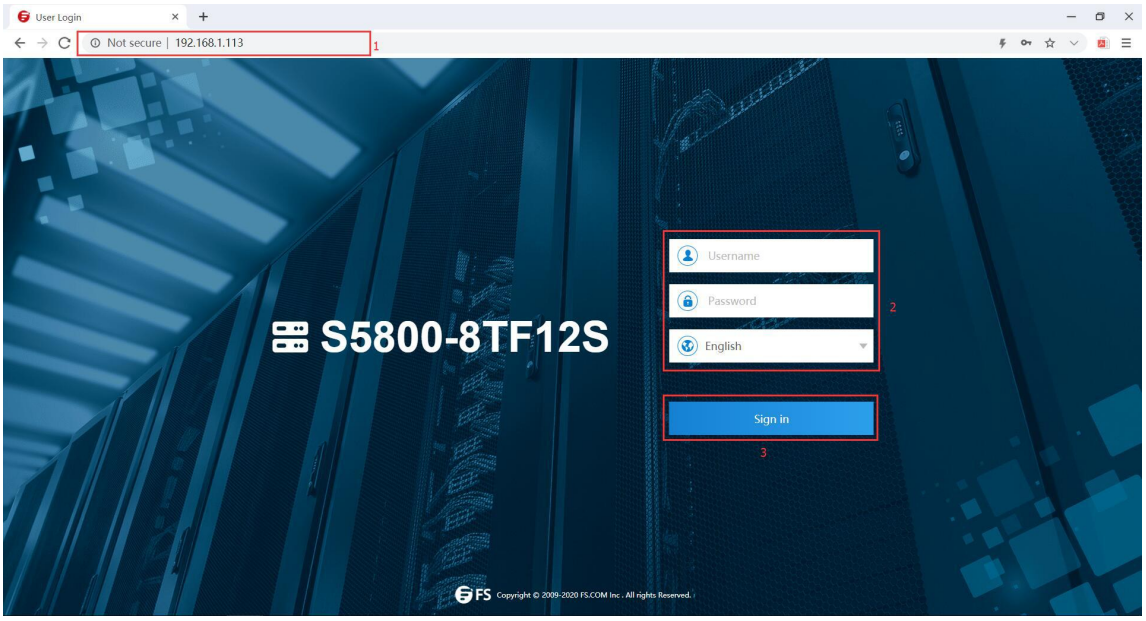


Figure 1 Web login page

1.2 Introduction of Web Interface

The web network management divided four categories: Monitor, Configuration, Maintenance, Network.

The structure of the monitor page is slightly different from that of the other three pages.

(1) Monitor

The Web monitor page appears after login, as shown in figure 2.

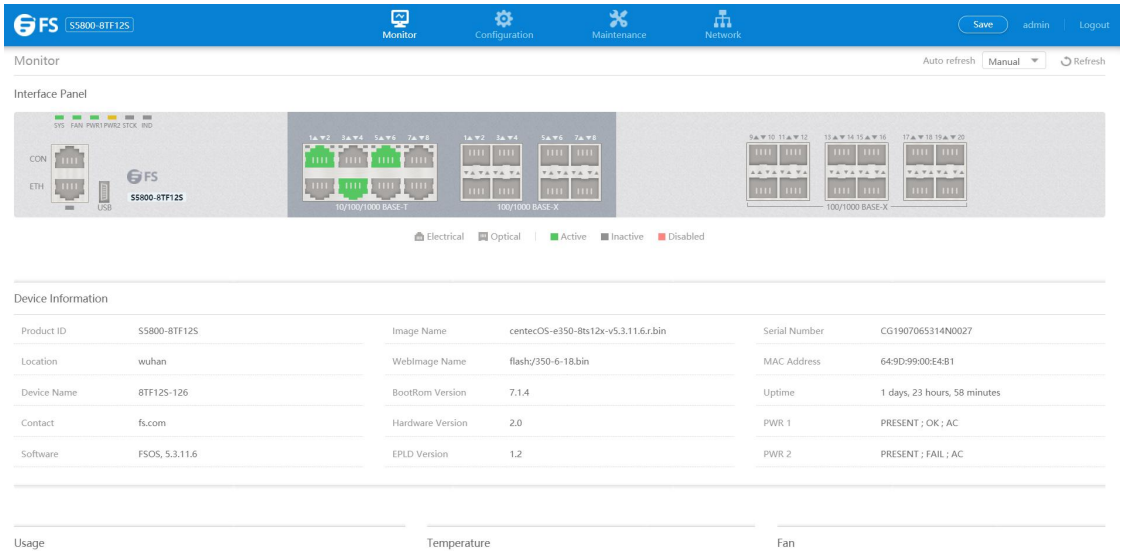


Figure 2 Web monitor page

The whole monitor page consists of the top control bar, the configuration display area and the bottom area.

(2) Configuration

If you click “Configuration” in the top control bar, as shown in figure 3.

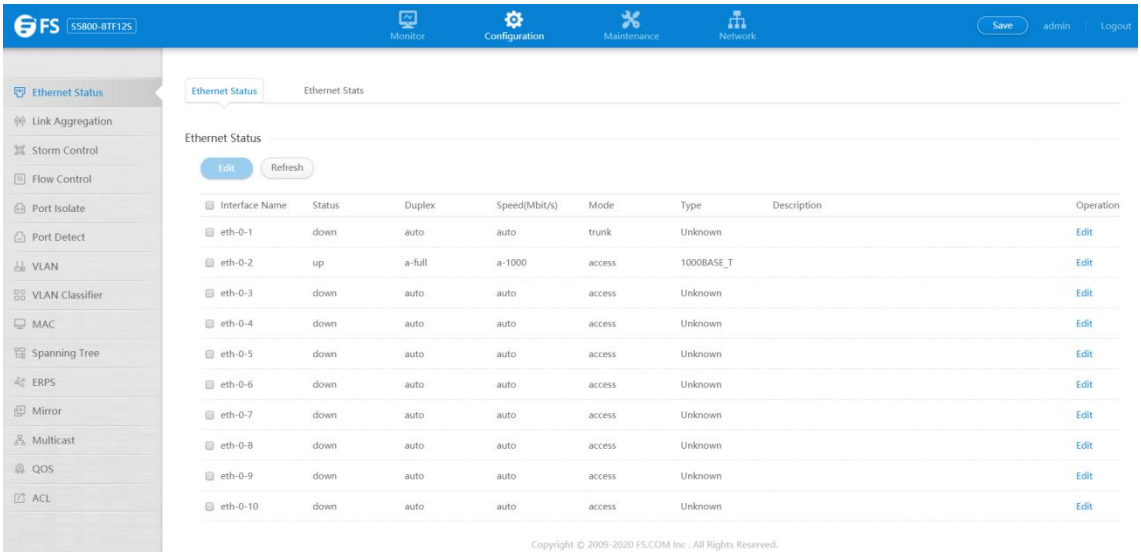


Figure 3 Web configuration page

The whole configuration page consists of the top control bar, the navigation bar, the configuration area and the bottom area.

(3) Maintenance

If you click “Maintenance” in the top control bar, as shown in figure 4.

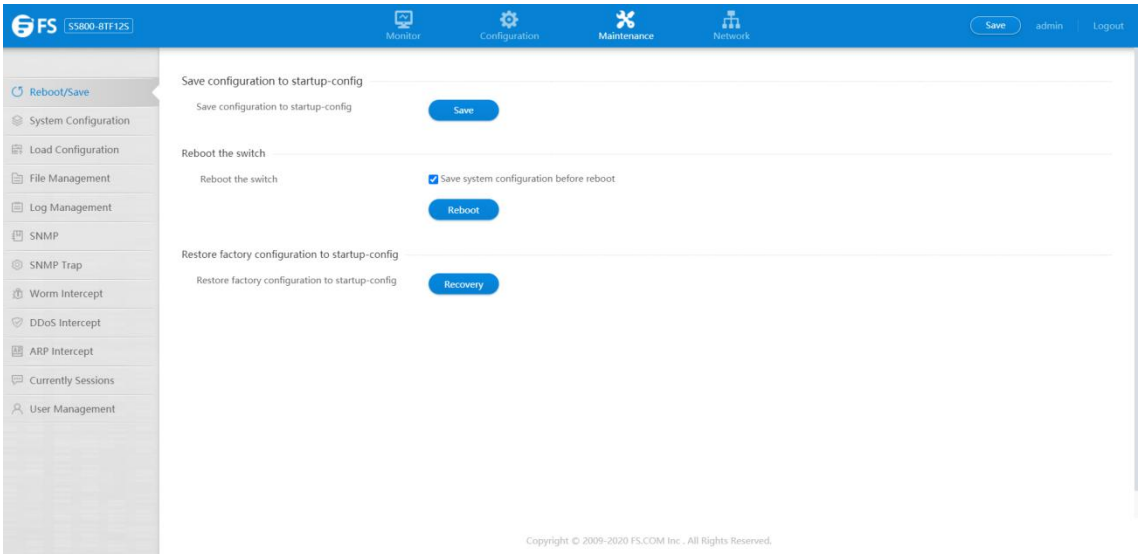


Figure 4 Web maintenance page

The whole maintenance page consists of the top control bar, the navigation bar, the configuration area and the bottom area.

(4) Network

If you click “Network” in the top control bar, as shown in figure 5.

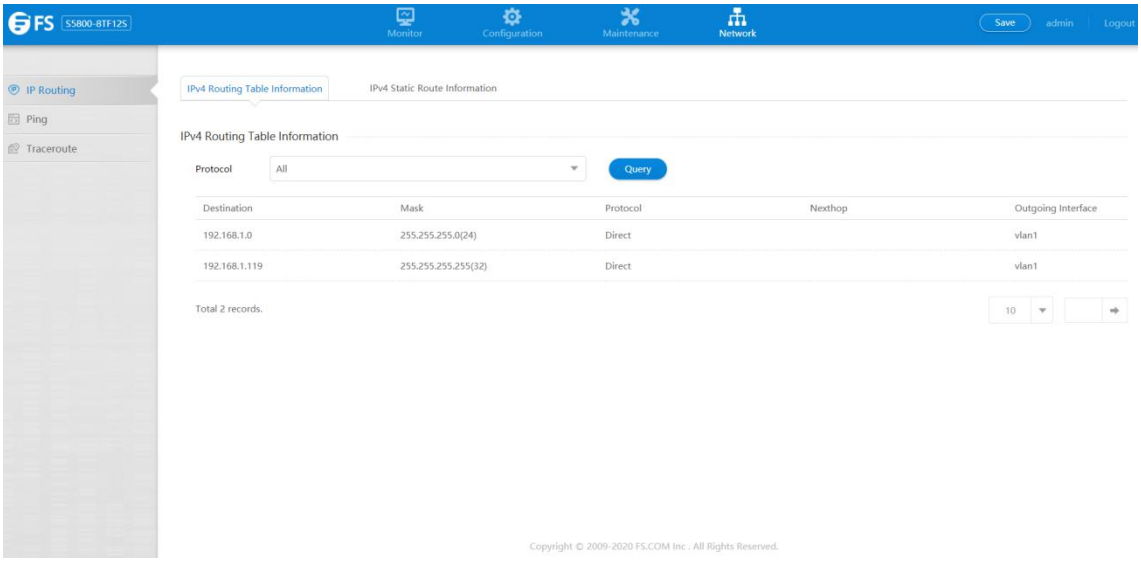


Figure 5 Web network page

The whole network page consists of the top control bar, the navigation bar, the configuration area and the bottom area.

1.2.1 Top Control Bar

Figure 6 Top control bar

- Parameter usage

Item	Description
Monitor	Display interface panel,basic information and monitor of the device
Configuration	Including switch port common configuration and layer-2 protocol, etc
Maintenance	Including switch system configuration and some security configuration, etc
Network	Including IP route configuration, ping and trace route function
Save	Click the Save button will jump to “Maintenance -> Reboot/Save”, then click ”save” button, write the current settings to the configuration file of the device, it is equivalent to the execution of the write command
Username	Display the current web login user
Logout	After you click "logout", you have to enter the username and the password again if you want to continue the web function

1.2.2 Navigation Bar

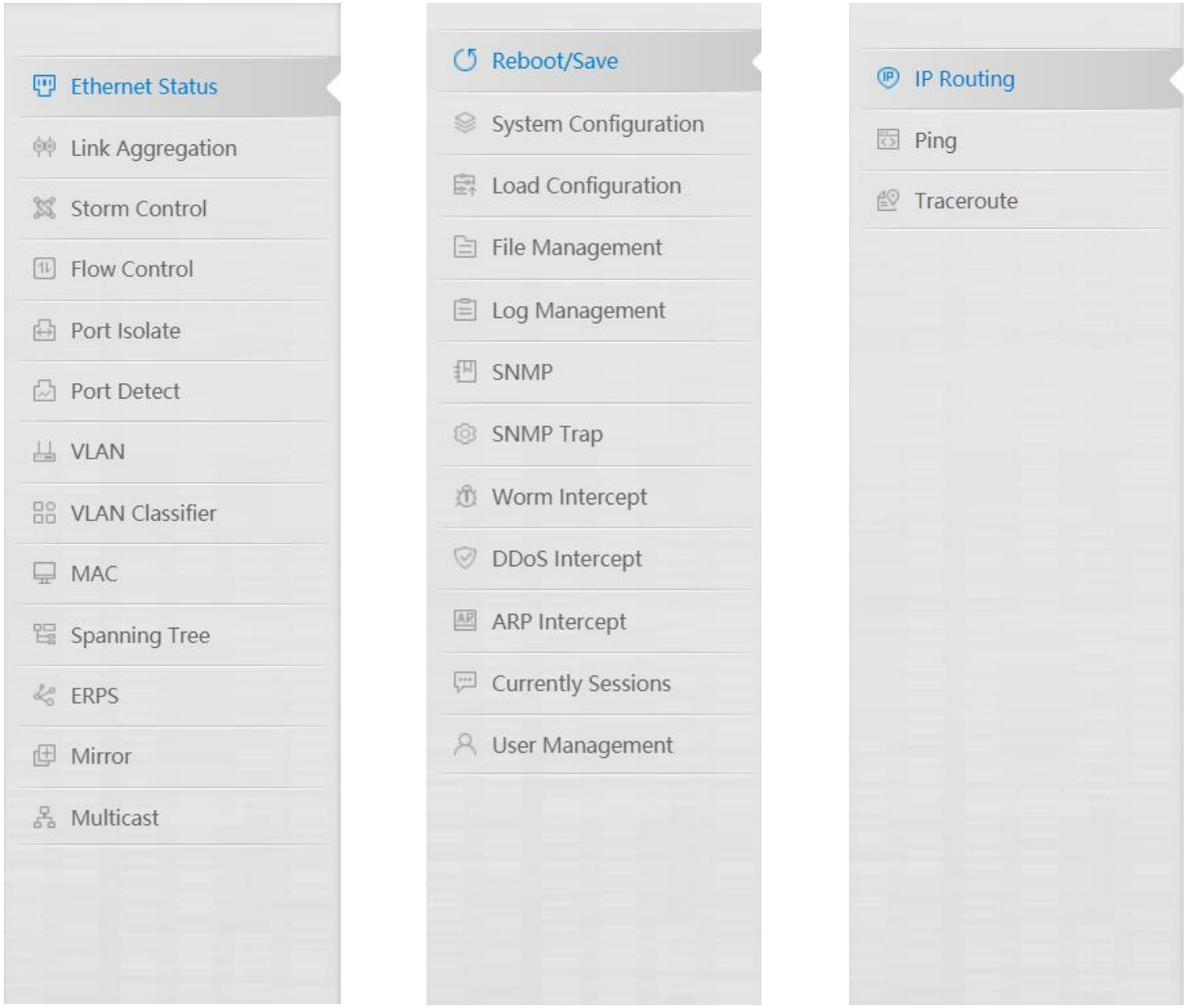


Figure 7 Navigation control bar

For example, to browse the flux of the current port, you have to click “Ethernet Status” and then “Interface State” configure.

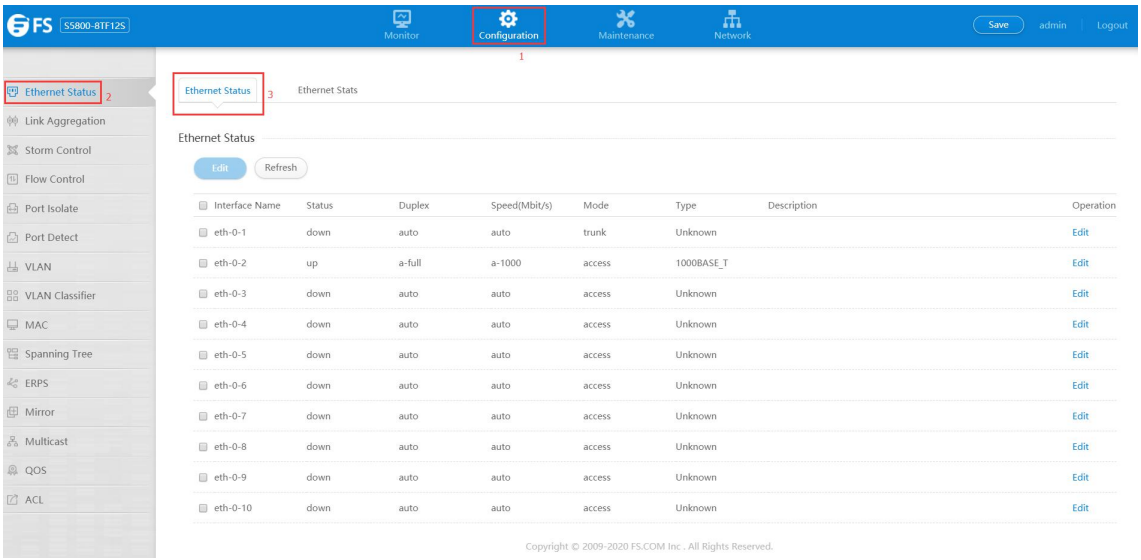


Figure 8 Interface state configure

1.2.3 Configuration Display Area

The configuration display area shows the state and configuration of the device, as shown in figure 9.

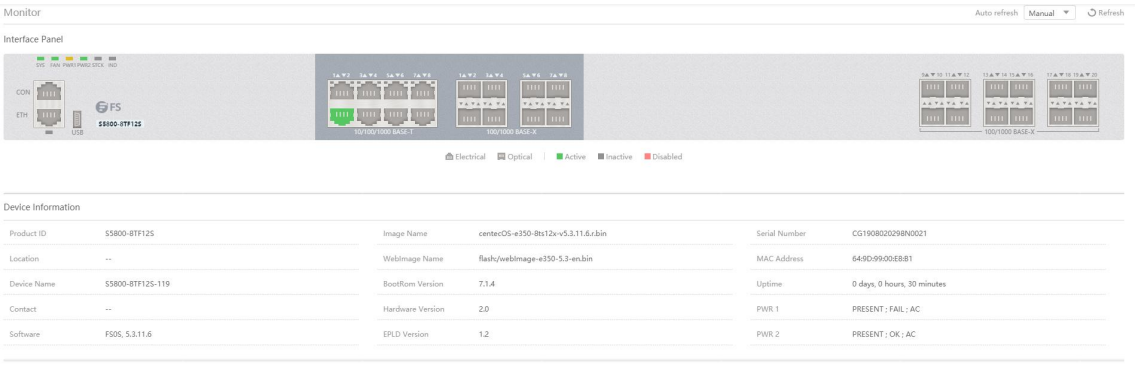


Figure 9 Configuration display area

1.2.4 Bottom Area

The bottom area shows the company copyright information, as shown in figure 10.

Figure 10 Bottom control bar

1.2.5 Configuration Area

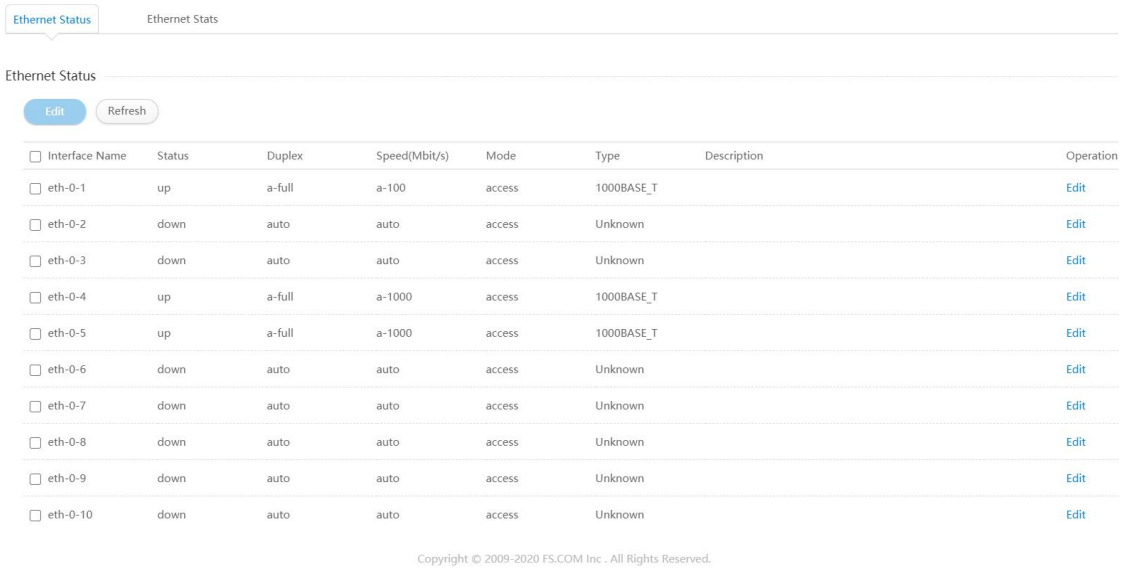


Figure 11 Configuration area

The configuration area is to show the content that is selected in the navigation area, the configuration area always contains one or more buttons, and their functions are listed in the following table.

- Parameter usage

Item	Description
Refresh	Refresh the content shown in the current configuration area
Apply	Apply the modified configuration to the device, the application of the configuration does not mean that the configuration is saved in the configuration file, to save the configuration, you have to click " Save " on the top control bar
New	Creates a list item, for example, you can create a VLAN item or a new user
Network	Including IP route configuration, ping and trace route function
Delete	Deletes an item in the list
Back	Go back to the previous-level configuration page
Edit	Modified configuration to the device

1.3 Device Summary

If you click "Monitor" in the top control bar, the device summary page appears, as shown in figure 12.

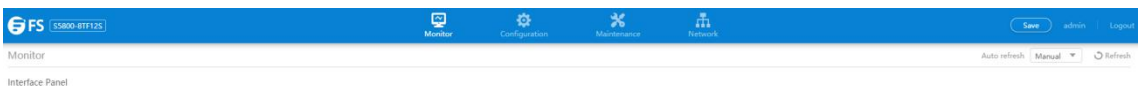


Figure 12 Device summary

This chapter describes all components of logon homepage, including device panel, device information and device monitor.

1.3.1 Interface Panel

Click "Monitor" to check interface panel status on switch, the configuration page is shown as the figure 13.

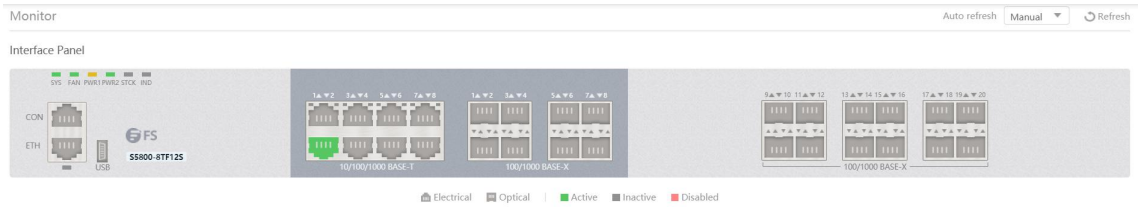


Figure 13 Interface panel

Based on type of the switch connected, the display area of web interface panel can intuitively display information of the various interfaces of this switch, the contents displayed including: Interface amount.
Operating statuses of interfaces: including activated state and interface type.

- Parameter usage

Item	Description
Auto refresh	Refresh the page in specified time

1.3.2 Device Information

Click "Monitor" to check device information status on switch, the configuration page is shown as the figure 14.

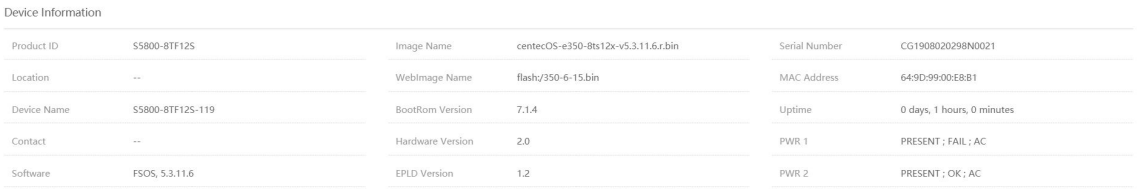


Figure 14 Device information panel

- Parameter usage

Item	Description
Product ID	The hardware product of the switch
Location	Indicate the location of the switch
Device Name	Indicate the host name of the switch
Contact	Indicate the contact of the switch
Software	The software version of the switch
Image Name	The name of the boot image
BootRom Version	Indicate the Boot Rom version of the switch

Item	Description
Hardware Version	Indicate the hardware version of the switch
EPLD Version	Indicate the EPLD version of the switch
Serial Number	Indicate the serial number of the switch
MAC Address	The system mac of the switch
Uptime	Indicate the uptime of the switch
PWR 1	Indicate the current status of power 1
PWR 2	Indicate the current state of power 2

1.3.3 Device Monitor

Click "Monitor" to check device monitor status on switch, the configuration page is shown as the figure 15.

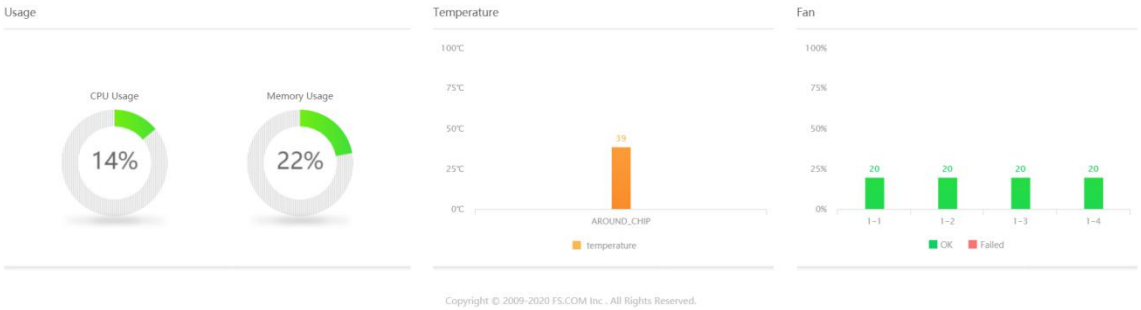


Figure 15 Device summary panel

- Parameter usage

Item	Description
CPU Usage	Indicate the CPU usage of the switch
Memory Usage	Indicate the software memory usage of the switch
Temperature	Indicate the current temperature of the switch
FAN	Specify the fan number and ID
Status	Indicate the current work status of each fan
Speed Rate	Indicate the current work speed rate of the switch

2. Ethernet Status Configuration

If you click "Configuration->Ethernet Status" in the top control bar, the ethernet status configuration list page appears, as shown in figure 1.

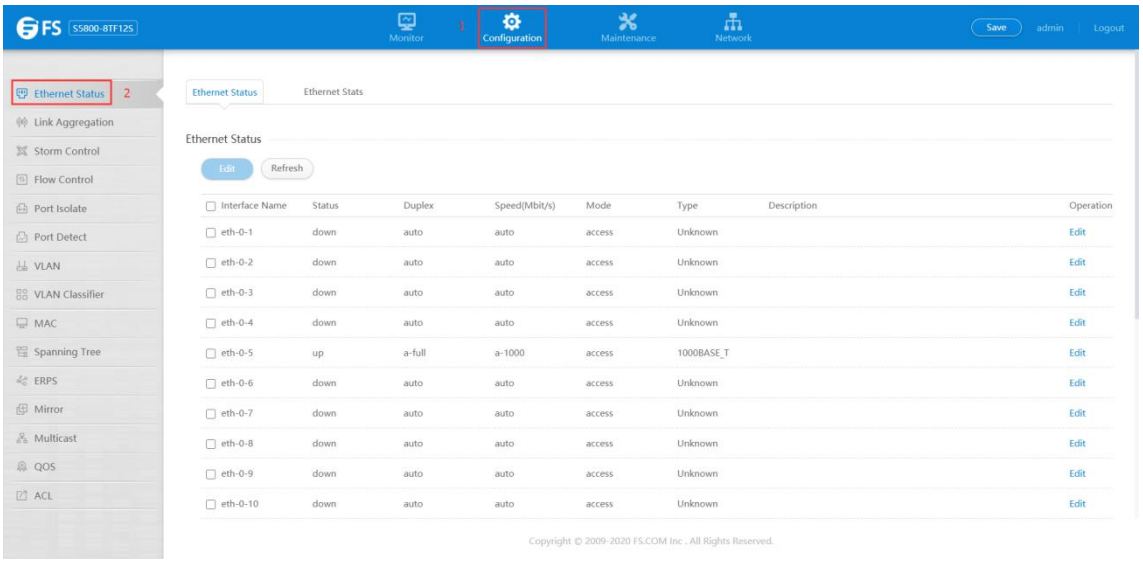


Figure 1 Ethernet status configuration list

This chapter describes the interface configuration function of the switch.

2.1 Ethernet Status

This section mainly describes how to configure and view interface connection.

2.1.1 Basic Information

If you click "Ethernet Status -> Ethernet Status" to check each interface status on switch, the configuration page is shown as the figure 2.

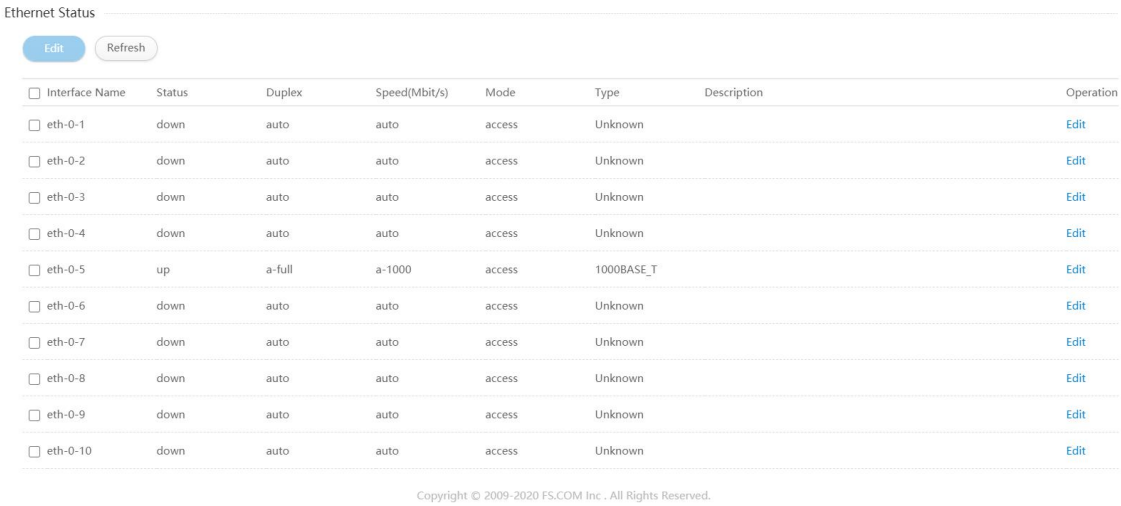


Figure 2 Basic information

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Status	The operating status (up or down) on interface
Duplex	Display the current duplex configuration on the interface
Speed(M bit/s)	Display the current speed configuration on the interface
Mode	Display the switch port mode of interface
Type	Display the media type of interface
Description	Description about the interface
Operation	Display that interface configuration properties can be edited

2.1.2 Interface Attribute Configuration

If you want to modify the configuration to interface attribute, you can follow the following steps:

(1) Please click "Edit" button or select a check box for one or more interfaces and click the "Edit" button.

(2) Select "Up/Down" in the "Admin Status" radio box.

(3) Select "L2 mode/L3 mode" in the "L2/L3 Mode" radio box.

(4) Select "Trunk/Access" in the "Mode" radio box.

(5) Select "Enable/Disable" in the "Jumbo frame" radio box.

(6) Select speed configure in the "Speed" drop-down box.

(7) Enter interface description in the "Description" text box.

(8) After that, click "Apply" to apply all the changes made.

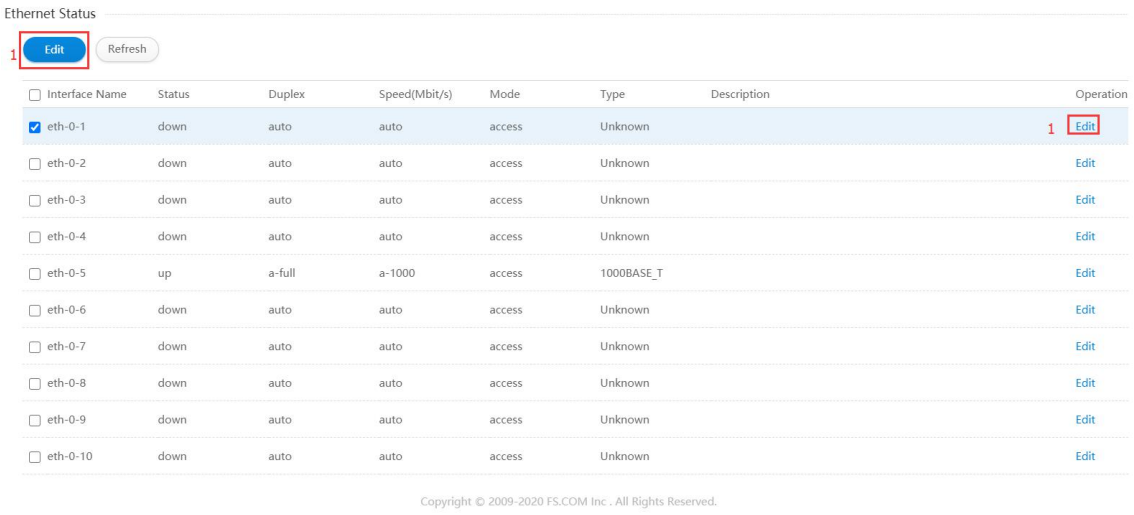


Figure 3 Interface status operation

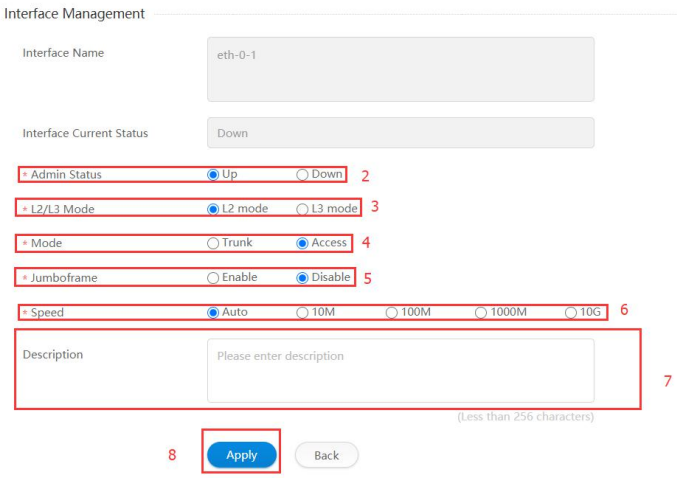


Figure 4 Interface attribute configuration

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Interface Current Status	The Current status (up or down) on interface
Admin Status	The operating status (up or down) on interface
L2/L3 Mode	Display the L2/L3 mode of interface
Mode	Display the switch port mode of interface
Jumboframe	Specific set of machines that you manage and configure
Speed(M bit/s)	Display the current speed configuration on the interface
Description	Description about the interface

2.2 Ethernet Stats

This section mainly describes how to show interface stats.

2.2.1 Basic Information

If you click “Ethernet Status -> Ethernet Stats” to view statistics information for each interface, statistics on interface is accounted after device start up completed, show as the figure 5.

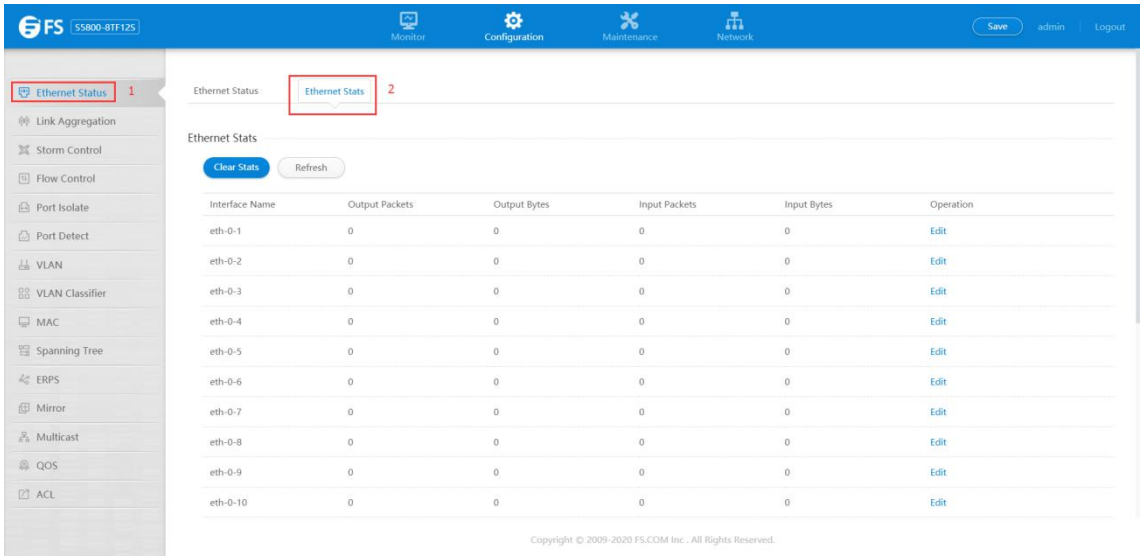


Figure 5 Ethernet stats page

Interface Name	Output Packets	Output Bytes	Input Packets	Input Bytes
eth-0-1	0	0	0	0
eth-0-2	0	0	0	0
eth-0-3	0	0	0	0
eth-0-4	0	0	0	0
eth-0-5	0	0	0	0
eth-0-6	0	0	0	0
eth-0-7	0	0	0	0
eth-0-8	0	0	0	0
eth-0-9	0	0	0	0
eth-0-10	0	0	0	0
eth-0-11	1795	658765	0	0
eth-0-12	0	0	0	0

Figure 6 Statistics on interface

If you want to clear the ethernet stats, please click “Clear Stats” button, shown as the figure 7.

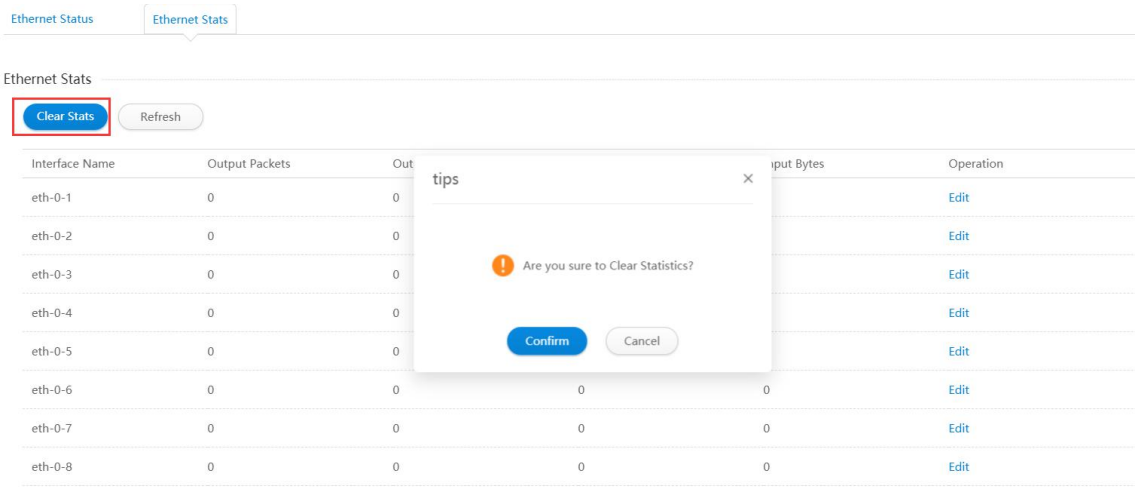


Figure 7 Interface detail clear stats

Choose one interface to enter the interface statistics detail page, shown as the figure 8.

Interface Name:eth-0-4

Item	Statistics
Received Statistics	
Packets Input	0
Bytes Input	0
5 Minute Input Rate(packets/sec)	0
5 Minute Input Rate (bits/sec)	0
Unicast Packet	0
Broadcast Packet	0
Multicast Packet	0
Runts	0
Giants	0
Input Errors	0
CRC	0
Frame	0
Pause	0
Sent Statistics	
Packets Output	0
Bytes Output	0
5 Minute Output Rate(packets/sec)	0
5 Minute Output Rate (bits/sec)	0
Unicast Packet	0
Broadcast Packet	0
Multicast Packet	0
Output Errors	0
Pause	0

Figure 8 Detail statistics on interface

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Output Packets	Total packets sent on this interface
Output Bytes	Total bytes including frame characters sent on this interface
Input Packets	Total packets received on this interface
Input Bytes	Total bytes including frame characters received on this interface
5 Minute Input Rate(packets/sec)	Input rate in 5 minute on this interface(packets/sec)
5 Minute Input Rate(bits/sec)	Input rate in 5 minute on this interface(bits/sec)
Unicast Packets	Total unicast packets received on this interface
Broadcast Packets	Total broadcast packets received on this interface
Multicast Packets	Total multicast packets received on this interface
Runts	Total runts error packets received on this interface
Giants	Total giants packets received on this interface
Input Errors	Total input error packets received on this interface
CRC	Total CRC error packets received on this interface
Frame	Total frame packets received on this interface
Overrun	Total overrun packets received on this interface
Pause	Total pause packets received on this interface
5 Minute Output Rate(packets/sec)	Output rate in 5 minute on this interface(packets/sec)
5 Minute Output Rate(bits/sec)	Output rate in 5 minute on this interface(bits/sec)
Unicast Packet	Total unicast packets transmitted on this interface
Broadcast Packet	Total broadcast packets transmitted on this interface
Multicast Packet	Total multicast packets transmitted on this interface
Under runs	Total under runs packets transmitted on this interface
Output Errors	Total output error packets transmitted on this interface
Pause	Total pause packets transmitted on this interface

3. Link Aggregation Configuration

3.1 Basic Information

If you click "Configuration -> Llink aggregation" in the top control bar, the link aggregation configuration list page appears, as shown in figure 1.

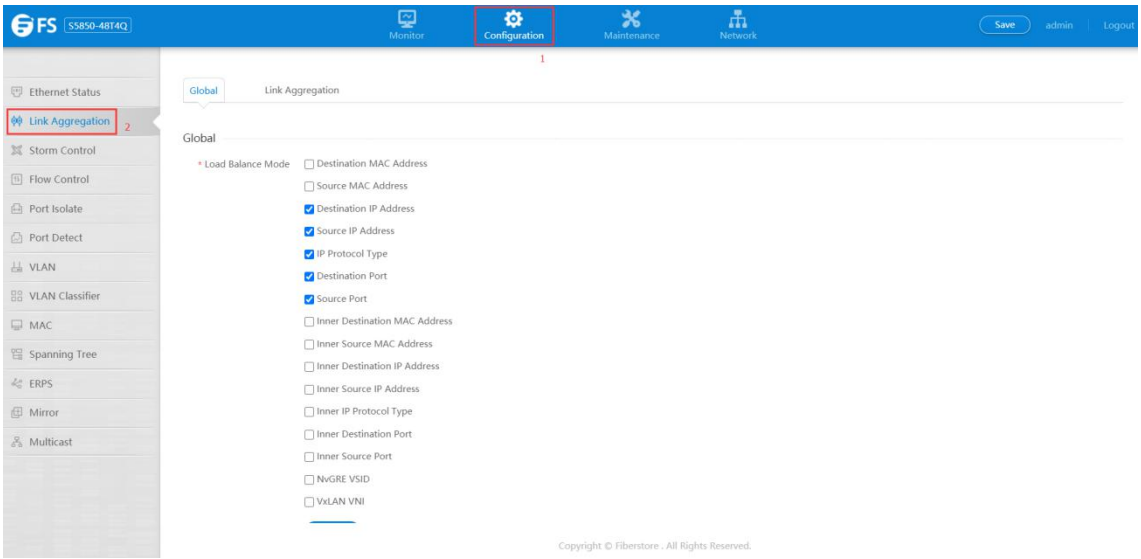


Figure 1 Link aggregation

This chapter describes the link aggregation configuration function and view the link aggregation information of the switch.

3.1.1 Basic Information(S5800-8TF12S)

The link aggregation function of device S5800-8TF12S is different from that of other devices. If you click "Configuration -> Llink aggregation" in the top control bar, the link aggregation configuration list page appears, as shown in figure 2.

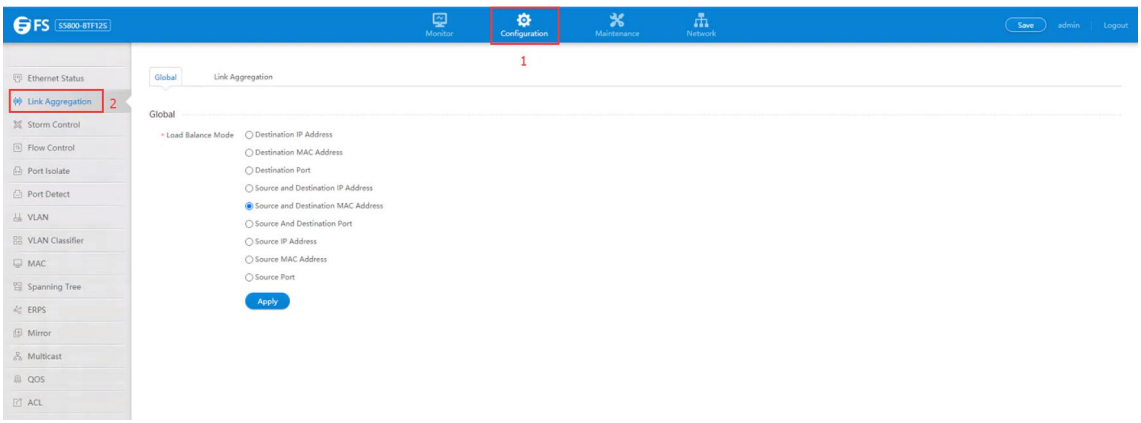


Figure 2 Link aggregation

3.2 Link Aggregation Global Configuration

If you click "Llink aggregation -> Global" in the title bar, the link aggregation global configuration page appears, as shown in figure 3.

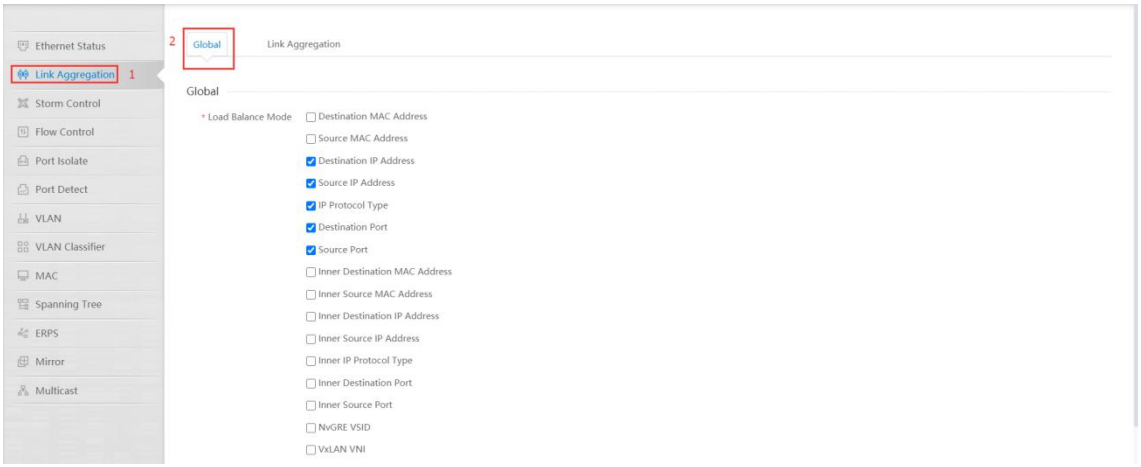


Figure 3 Link Aggregation global configuration information

- Parameter usage

Item	Description
Destination MAC address	Load balancing according to destination MAC
Source MAC address	Load balancing according to source MAC
Destination IP address	Load balancing according to destination IP
Source IP address	Load balancing according to source IP
IP Protocol Type	Load balancing according to IP protocol
Destination Port	Load balancing according to destination port
Source Port	Load balancing according to source port
Inner Destination MAC address	Load balancing according to destination MAC of inner layer message
Inner Source MAC address	Load balancing according to source MAC of inner layer message
Inner Destination IP address	Load balancing according to destination IP of inner layer message
Inner Source IP address	Load balancing according to source IP of inner layer message
Inner IP Protocol Type	Load balancing according to IP protocol of inner layer message
Inner Destination Port	Load balancing according to the destination port of inner layer message
Inner Source Port	Load balancing according to the source port of inner layer message
NvGRE VSID	Load balancing according to Negre's VSID
VxLAN VN	Load balancing according to VSID of Vxlan

If you want to configure the link aggregation global configuration, you can perform the following steps:

(1) You can select the check box in the left column of the load balancing mode you want to configure.

(2) Then click the “Apply ” button to configure the load balancing mode.

The operation is shown in figure 4.

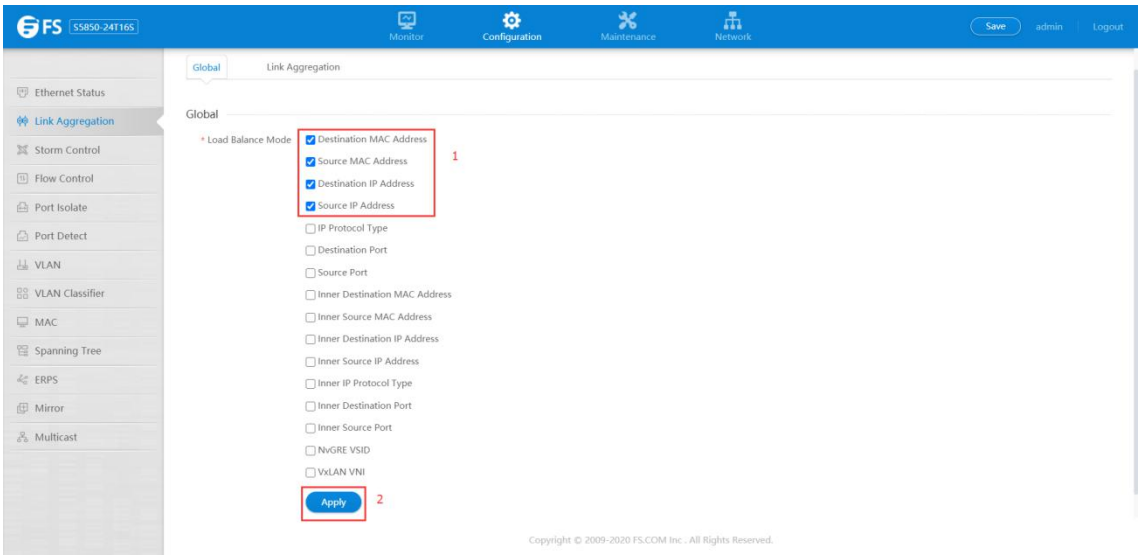


Figure 4 Link Aggregation global configuration

3.2.1 Global Configuration(S5800-8TF12S)

If you click "Llink aggregation -> Global" in the title bar, the link aggregation global configuration page appears, as shown in figure 5.

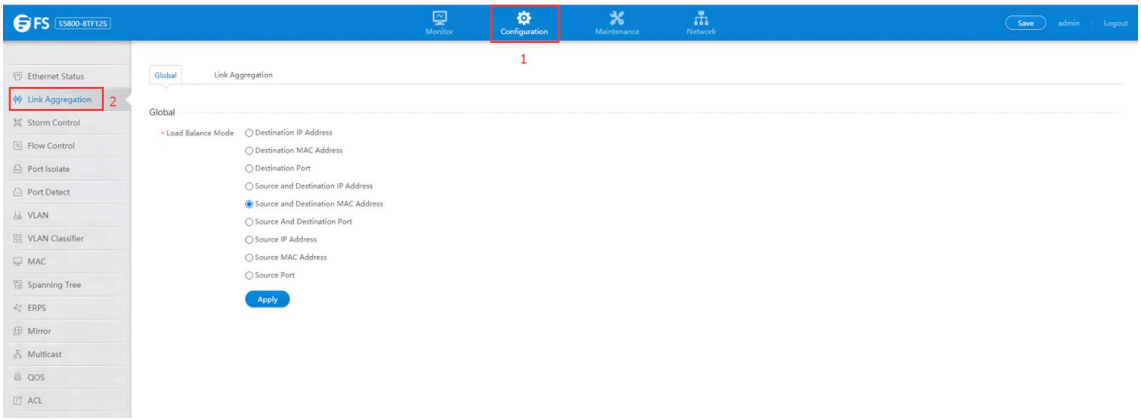


Figure 5 Load balance mode configuration

- Parameter usage

Item	Description
Destination IP address	Load balancing according to destination IP
Destination MAC address	Load balancing according to destination MAC
Destination Port	Load balancing according to destination port

Item	Description
Source and Destination IP address	Load balancing according to source IP address and destination IP address
Source and Destination MAC address	Load balancing according to source MAC address and destination MAC address
Source and Destination Port	Load balancing according to source port and destination port
Source IP address	Load balancing according to source IP
Source MAC address	Load balancing according to source MAC
Source Port	Load balancing according to source port

If you want to configure the link aggregation global configuration, you can perform the following steps:

(1) You can select the radio box in the left column of the load balancing mode you want to configure.

(2) Then click the "Apply " button to configure the load balancing mode.

The operation is shown in figure 6.

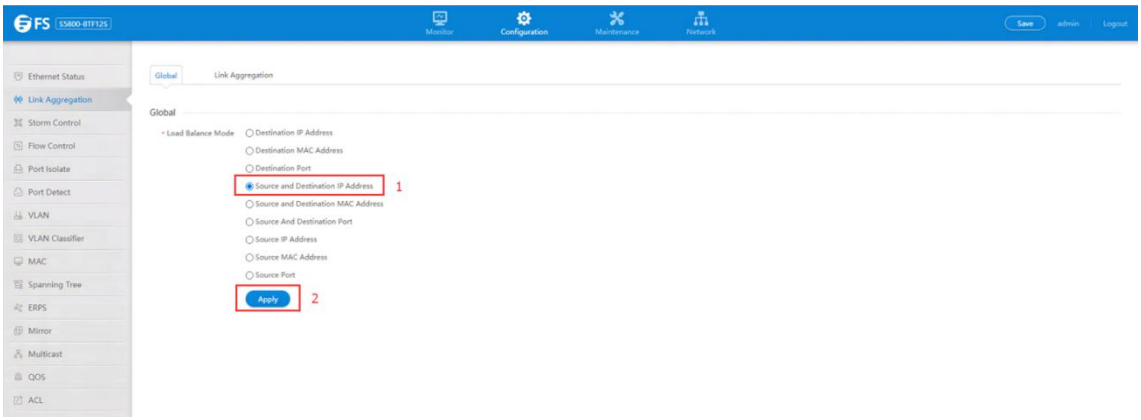


Figure 6 Link Aggregation global configuration

3.3 Link Aggregation Configuration

If you click "Llink aggregation -> Link aggregation" in the title bar, the link aggregation configuration page appears, as shown in figure 7.

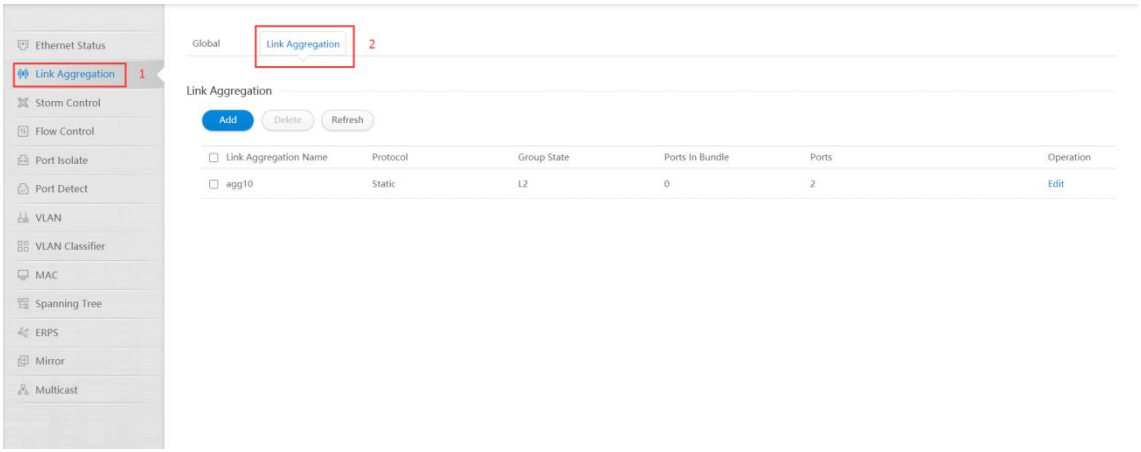


Figure 7 Link aggregation configuration information

- Parameter usage

Item	Description
Link Aggregation Name	Display the name of link aggregation interface
Protocol	Display link aggregation protocol mode
Group State	Display the group state of link aggregation interface
Ports in Bundle	Display the current ports number in bundle
Ports	Display the link aggregation member ports
Operation	Modify the configuration of this link aggregation group

3.3.1 User Configuration Add Link Aggregation

If you click “Add”, you can add link aggregation, as shown in figure 8, and then the link aggregation configuration page appears, as shown in figure 9.

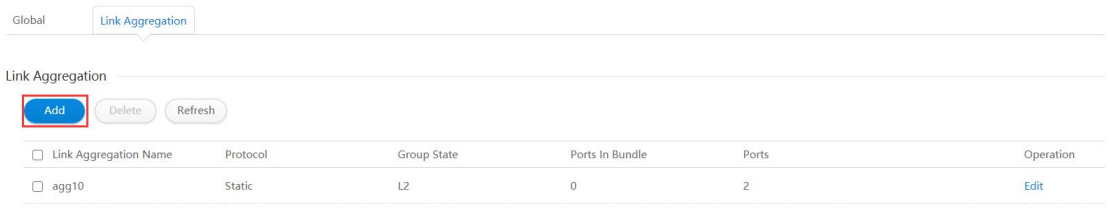


Figure 8 Add link aggregation operation

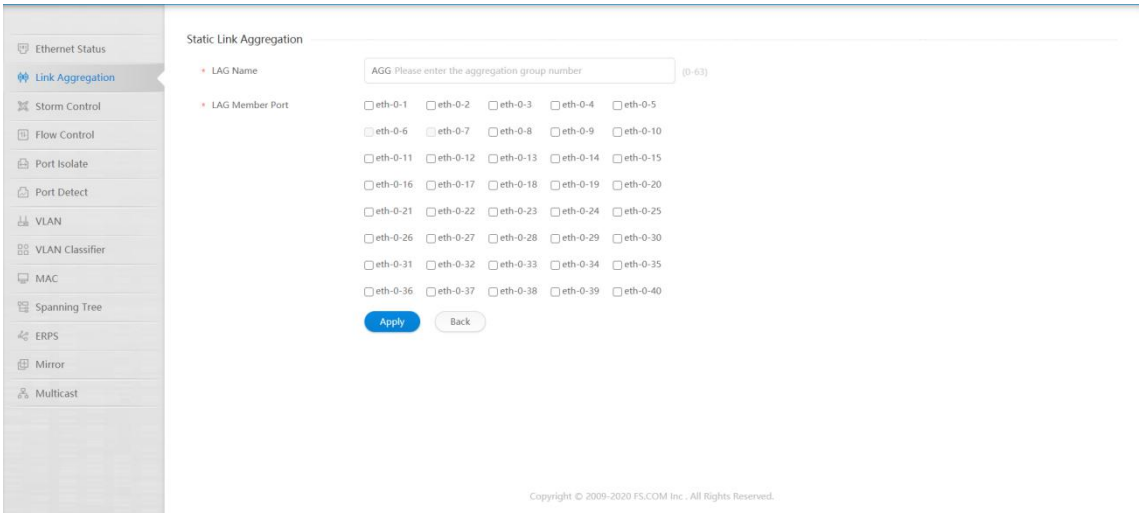


Figure 9 Link aggregation configuration

- Parameter usage

Item	Description
LAG Name	Display the name of link aggregation interface
LAG Member Port	Display the member port of link aggregation interface

If you want to add link aggregation, you can perform the following steps:

(1) Fill LAG name.

(2) Select LAG member port.

(3) Click "Apply" button to apply all the changes made.

The operation is shown in figure 10, and the entry of the link aggregation configuration success table is shown in figure 11.

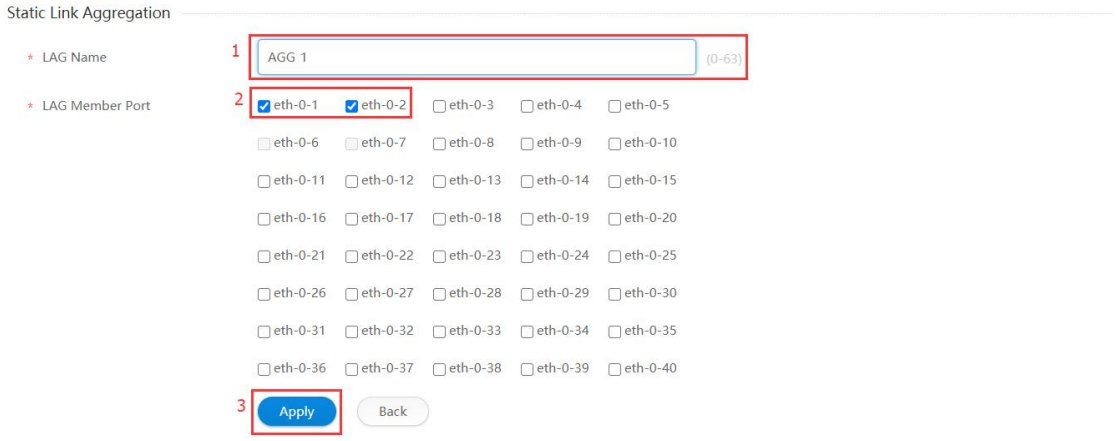


Figure 10 User configuration add link aggregation

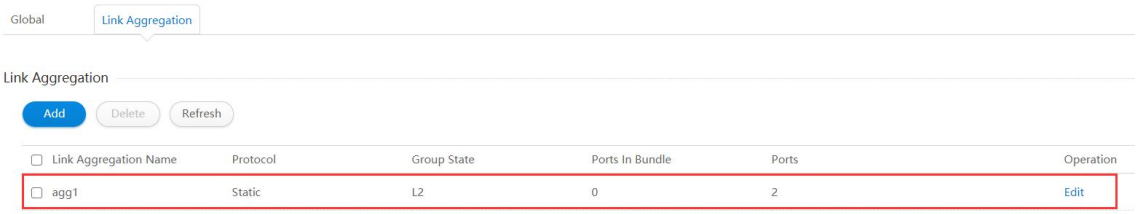


Figure 11 New link aggregation information

3.3.2 User Configuration Edit Link Aggregation

If you click "Edit", you can edit link aggregation, as shown in figure 12, and then the link aggregation configuration page appears, as shown in figure 13.

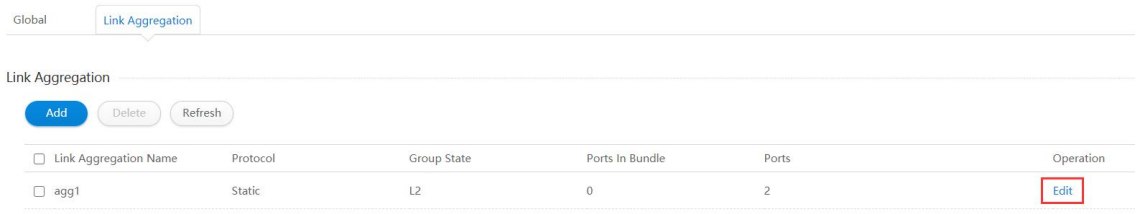


Figure 12 Edit link aggregation operation

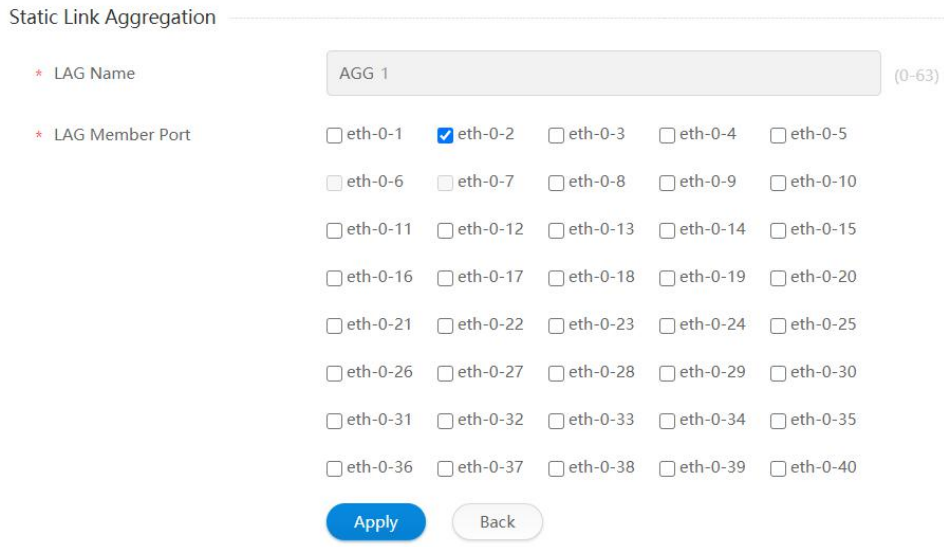


Figure 13 Link aggregation configuration edit

- Parameter usage

Item	Description
LAG Name	Display the name of link aggregation interface
LAG Member Port	Display the member port of link aggregation interface

If you want to edit link aggregation, you can perform the following steps:

(1) Select LAG member port.

(2) Click "Apply" button to apply all the changes made.

The operation is shown in figure 14, and the entry of the link aggregation configuration success table is shown in figure 15.

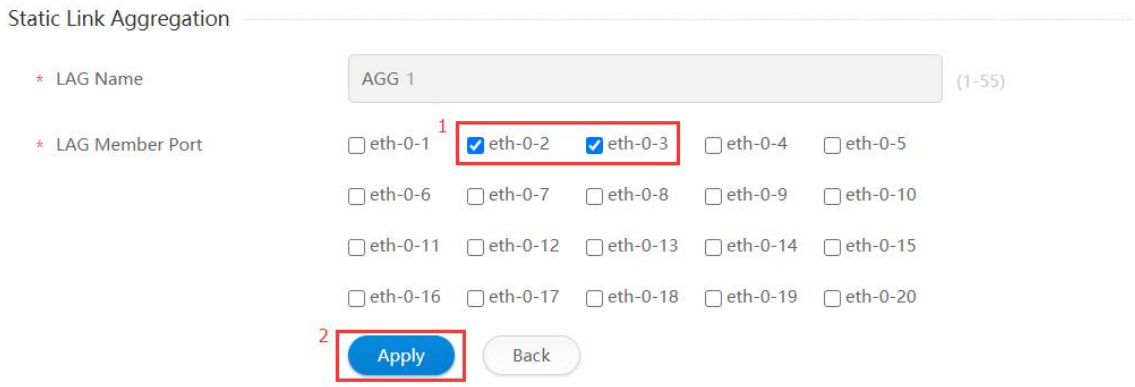


Figure 14 User edit a link aggregation configuration

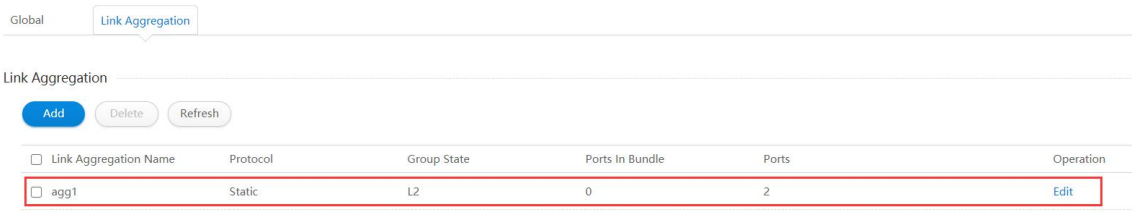


Figure 15 New link aggregation information

3.3.3 Delete A Link Aggregation

If you want to delete the specified link aggregation, you can perform the following steps:

(1) You can select the check box in the left column of the link aggregation you want to delete.

(2) Then click the "Delete " button to delete the link aggregation.

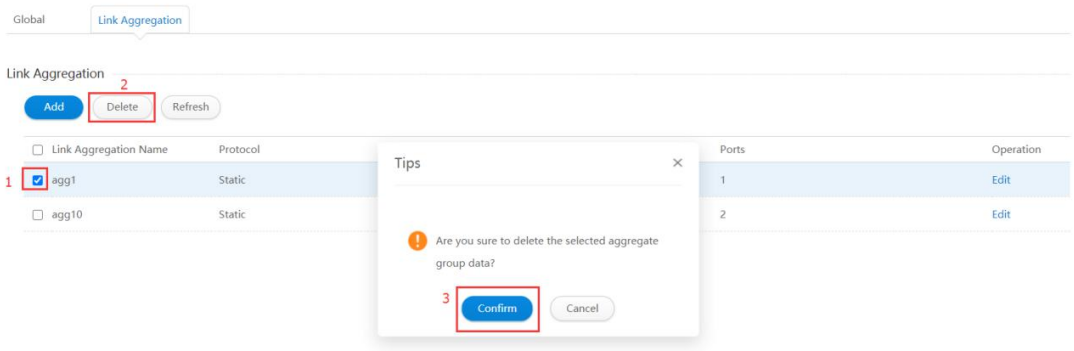


Figure 16 Delete a link aggregation

4. Storm Control

4.1 Storm Control

This section mainly describes how to configure and view interface storm control.

4.1.1 Basic Information

If you click "Configuration -> Storm Control" to check each interface storm control on switch, the configuration page is shown as the figure below.

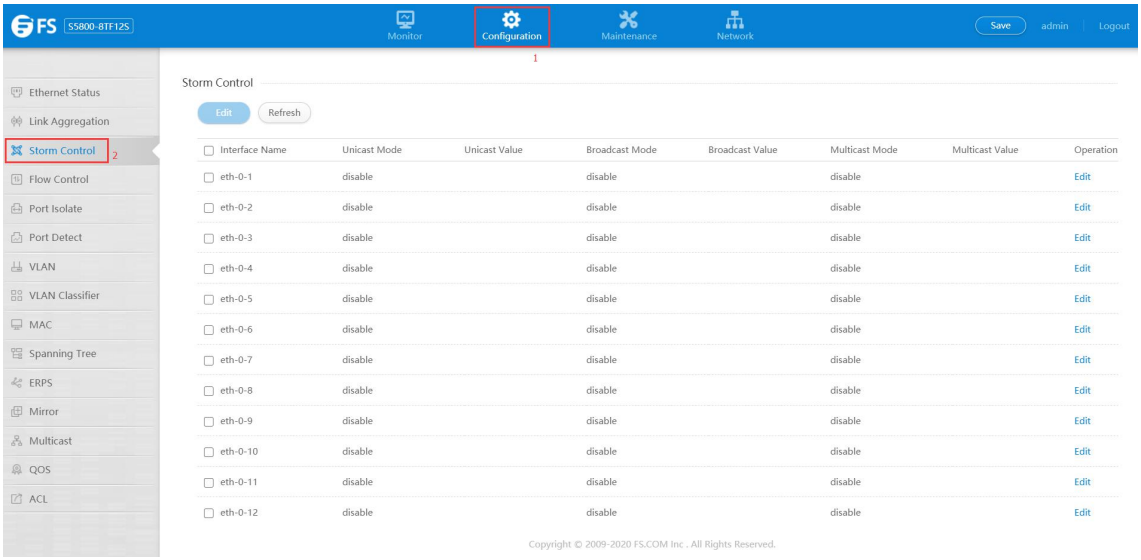


Figure 1 Storm control basic information

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Unicast Mode	Display the unicast storm control mode
Unicast Value	Display the unicast storm control value.Level: 0.00-100.00, PPS: 0-1000000000
Broadcast Mode	Display the broadcast storm control mode
Broadcast Value	Display the broadcast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Multicast Mode	Display the multicast storm control mode
Multicast Value	Display the multicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Operation	Display that interface entries can be edited

4.1.2 Storm Control Attribute Configuration

In the Storm Control basic information page, If you choose one interface, and then click the "Edit" button, the operation is shown in figure 2. and then the interface storm control attribute configuration page appears, as shown in figure 3.

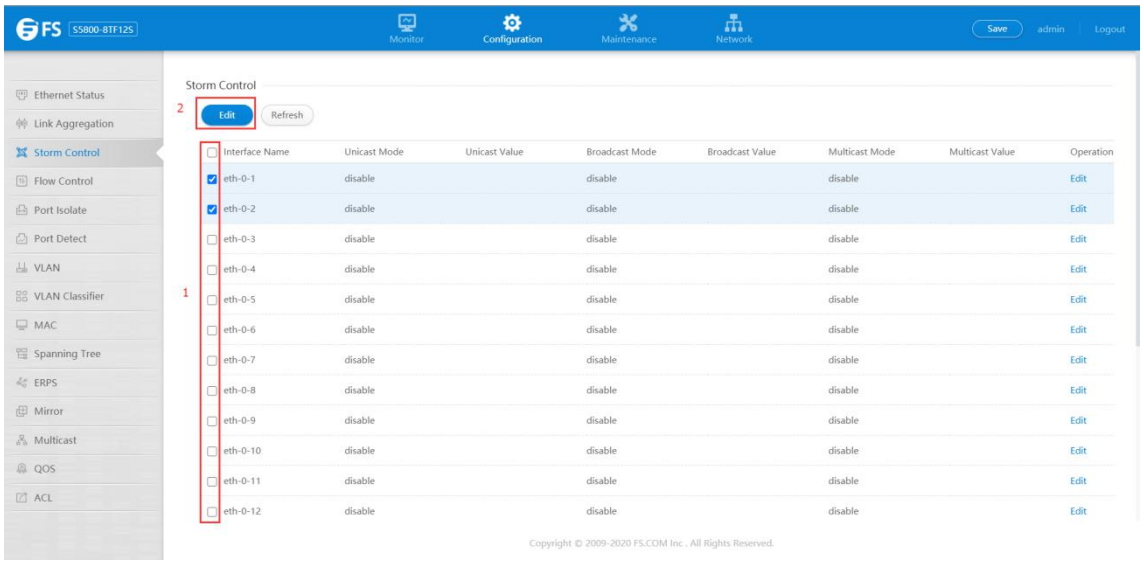


Figure 2 Select the interface

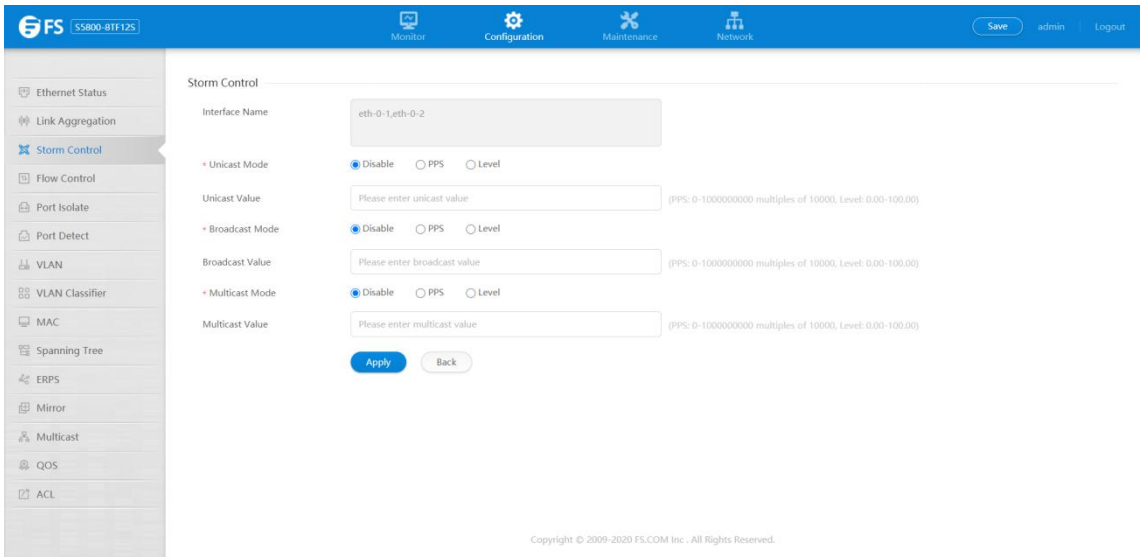


Figure 3 Interface storm control attribute configuration

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Unicast Mode	Enter the unicast storm control mode
Unicast Value	Enter the unicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Broadcast Mode	Enter the broadcast storm control mode
Broadcast Value	Enter the broadcast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Multicast Mode	Enter the multicast storm control mode
Multicast Value	Enter the multicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000

4.1.3 Unknown Unicast Storm Control

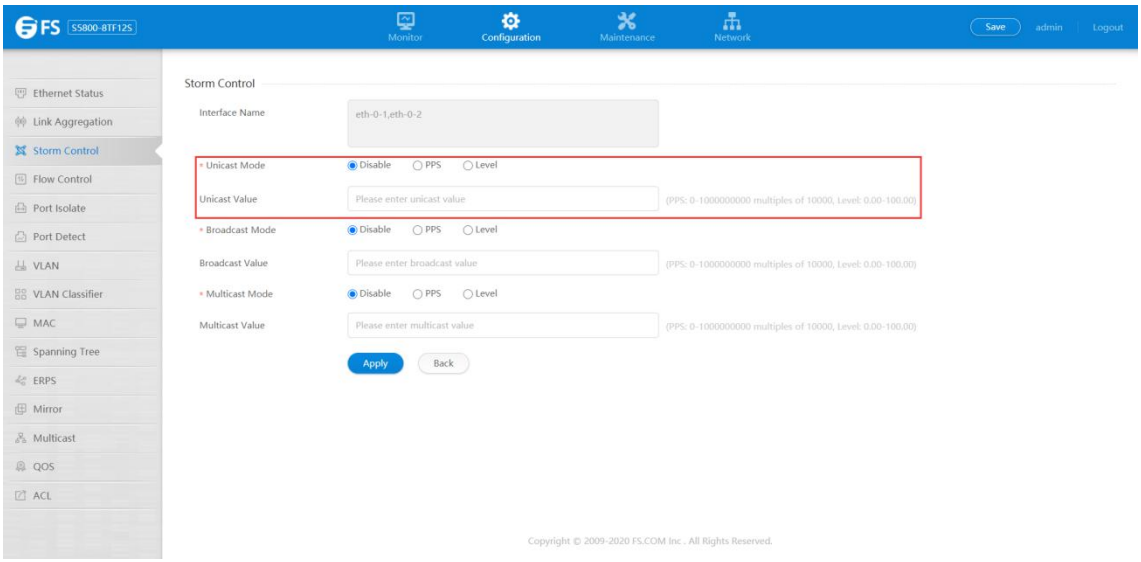


Figure 4 Setting the unknown unicast storm control

Through the radio buttons in the “Unicast Mode” bar, you can choose Disable/PPS/level. When you choose the PPS or level, in the “Unicast Value” bar, you can enter the value of the unicast packets. The legal threshold range for each port is given behind the threshold.Then click apply to apply all the changes made.

4.1.4 Broadcast Storm Control

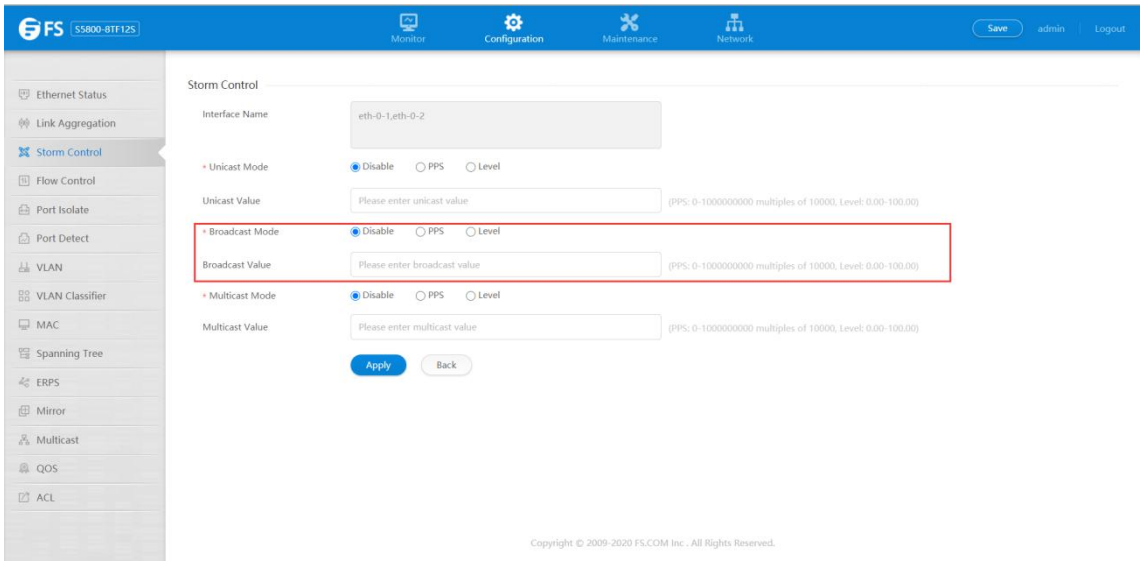


Figure 5 Setting the broadcast storm control

Through the radio buttons in the “Broadcast Mode” bar,you can choose Disable/PPS/level. When you choose the PPS or level, in the “Broadcast Value” bar, you can enter the value of the Broadcast packets. The legal threshold range for each port is given behind the threshold.Then click apply to apply all the changes made.

4.1.5 Multicast Storm Control

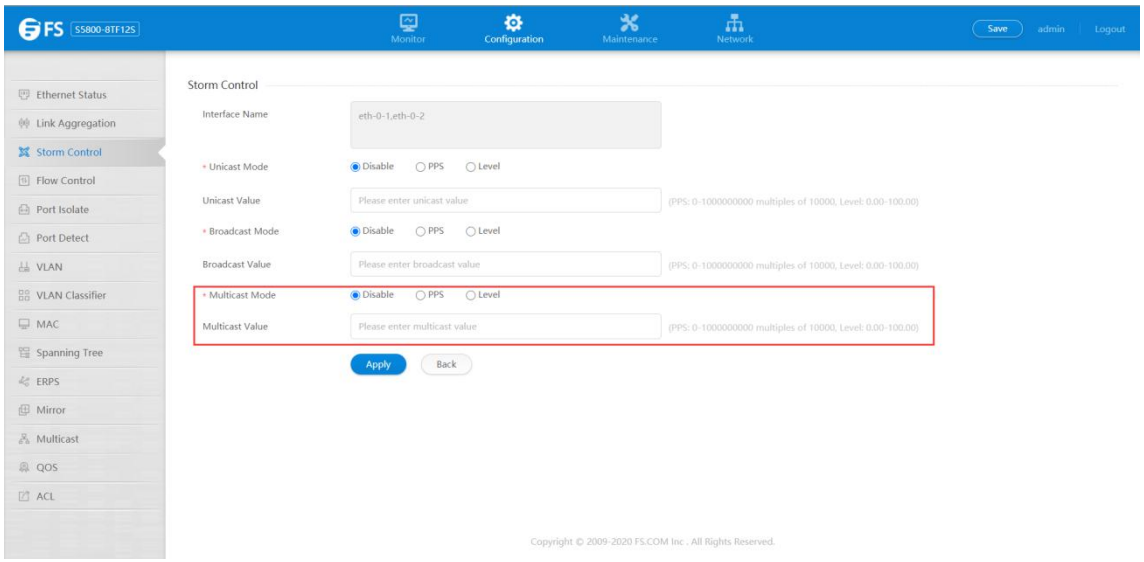


Figure 6 Setting the multicast storm control

Through the radio buttons in the “Multicast Mode” bar, you can choose Disable/PPS/level. When you choose the PPS or level, in the “Multicast Value” bar, you can enter the value of the Multicast packets. The legal threshold range for each port is given behind the threshold.Then click apply to apply all the changes made.

5. Flow Control

If you click “Configuration -> Flow Control” in the top control bar, the flow control page appears, as shown in figure 1.

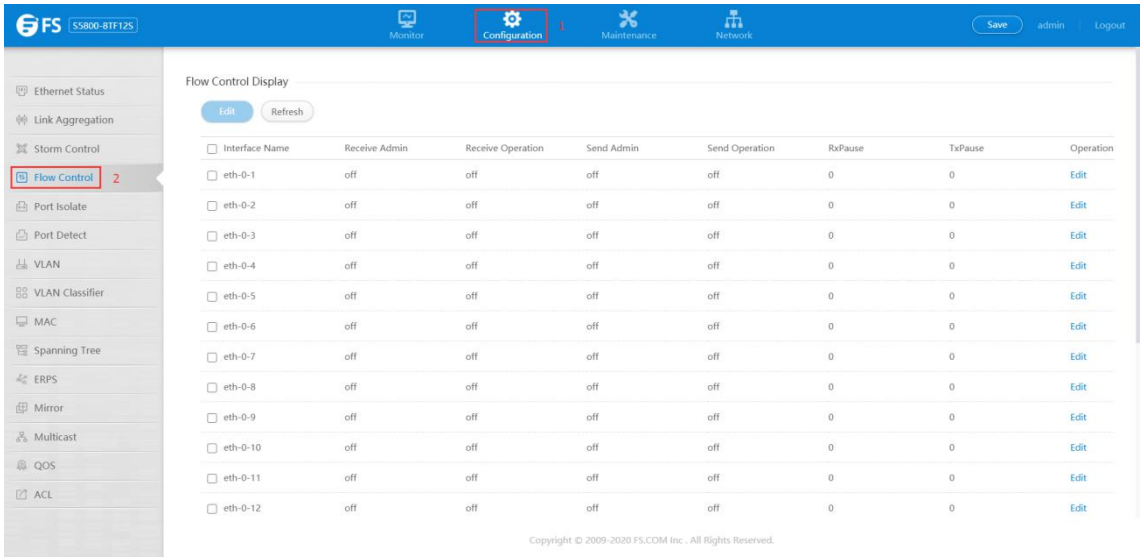


Figure 1 Flow control page

This section mainly describes how to configure and view flow control.

5.1 Flow Control Display

If you click “Configuration -> Flow Control”, the flow control display page appears, as shown in figure 2.

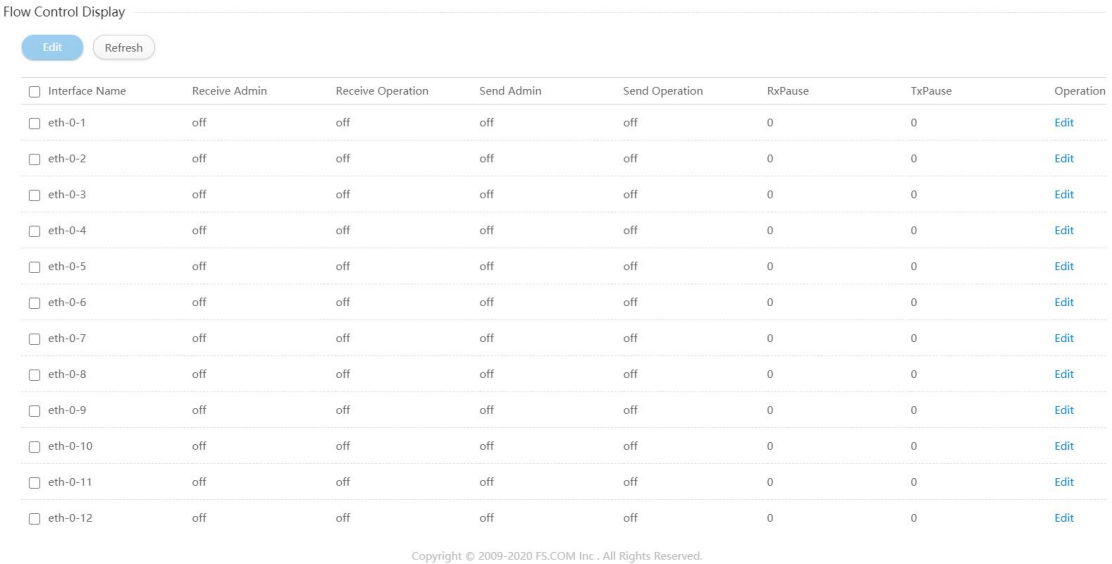


Figure 2 Flow control display

This figure displays all interface name and their receiving and sending status.

- Parameter usage

Item	Description
Interface Name	Display the name of Interface
Receive admin	Display Receive configuration
Receive oper	Display Receiving status
Send admin	Display Send configuration
Send oper	Display Send status
RxPause	Display receive statistics
TxPause	Display Send statistics
Operation	Display that flow control table entries can be edited

5.2 Edit Flow Control

You can choose the check box in the left-hand column of flow control display page, then click "Edit" button, or directly click the "Edit" button in the right-most "Operation" bar, the operation is shown in figure 3, then port configuration page appears, as shown in figure 4.

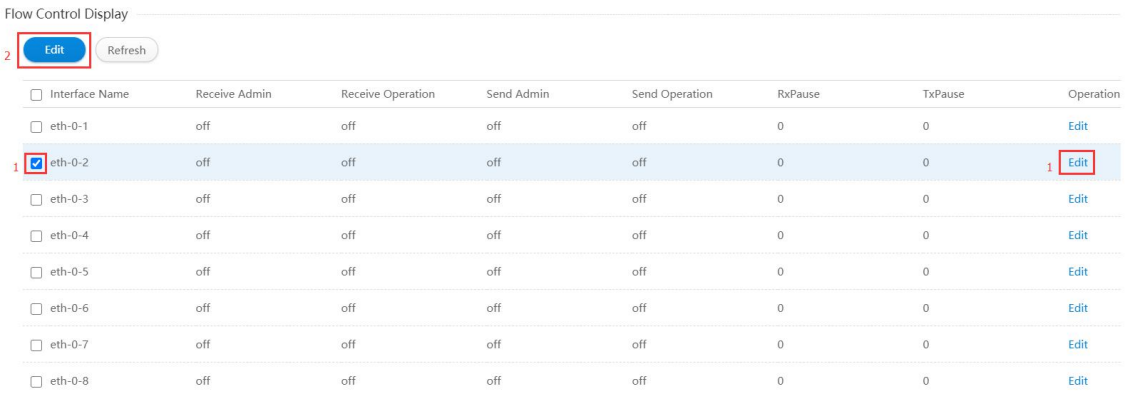


Figure 3 Edit flow control operation

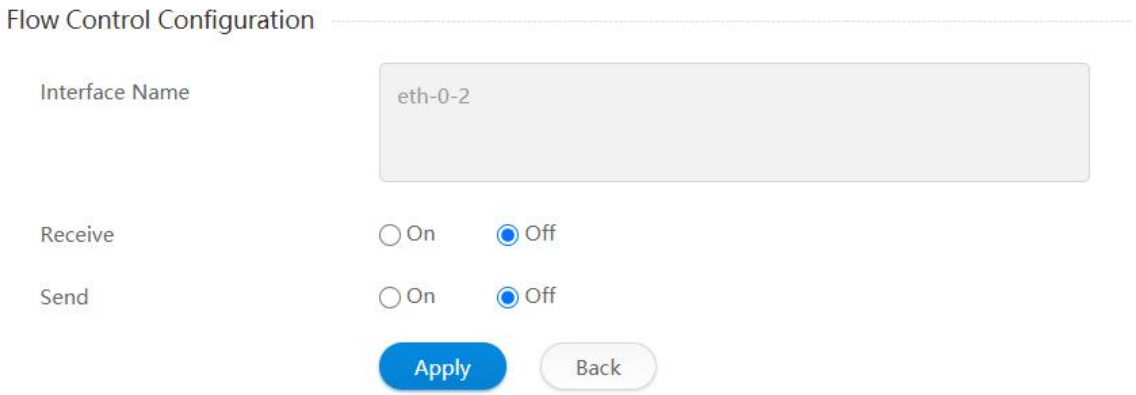


Figure 4 Port configuration list

- Parameter usage

Item	Description
Receive	Receive status of current port flow control
Send	Send status of current port flow control

If you want to modify the sending and receiving status of flow control on the current port, such as enable flow control receive function and disable flow control send function, you can follow the following steps:

(1) Click the "On" button in the line of "Receive" function.

(2) Click the "Down" button in the line of "Send" function.

(3) Click the "Apply" button to modify the sending and receiving status of the current port.

The operation is shown in figure 5, modify the sending and receiving status of flow control on the current port configuration success table entry is shown in figure 6.

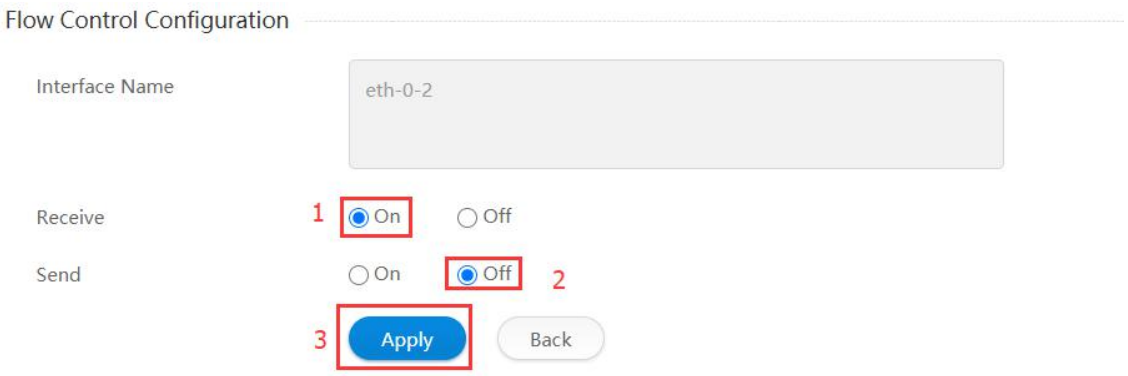


Figure 5 Edit flow control operation

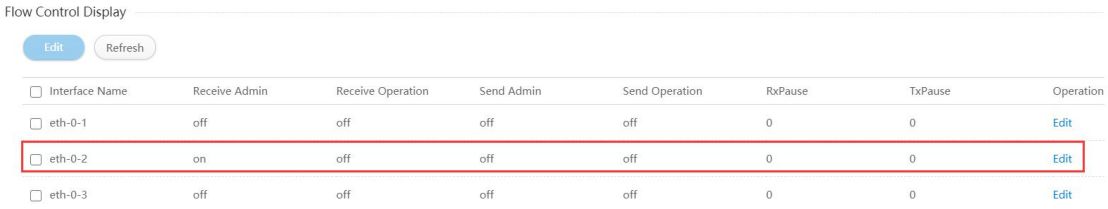


Figure 6 New flow control information

6. Port Isolate

If you click “Configuration->Port Isolate” in the top control bar, the port isolate configuration list page appears, as shown in figure 1.

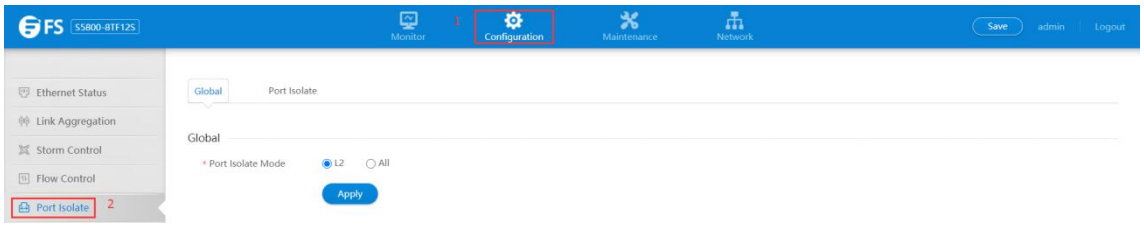


Figure 1 Port isolate configuration list

This chapter describes how to configure port isolation and view port isolation group information.

6.1 Global Configuration

Port isolation provides two modes of operation, layer 2 isolation mode and layer 2 & 3 full isolation mode.

6.1.1 Current Port Isolation Mode

If you click “Port Isolate -> Global” in the title bar, the port isolation mode information page appears, as shown in figure 2.

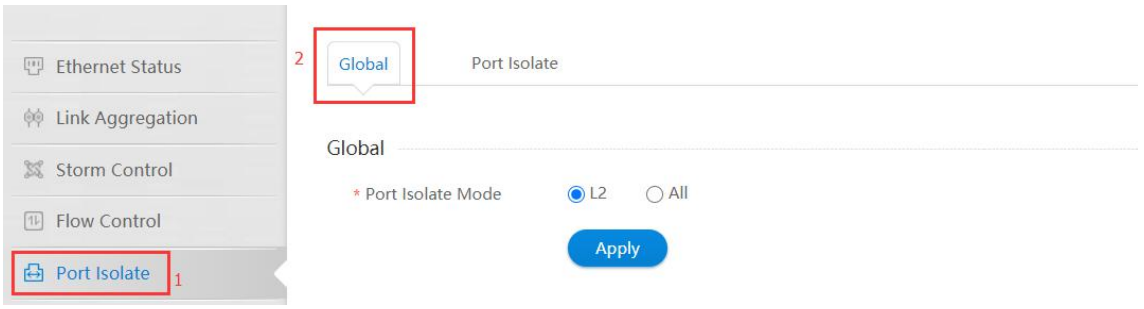


Figure 2 Port isolation mode information

- Parameter usage

Item	Description
Port Isolate Mode	Display the mode of port isolation

If you want to modify the mode of port isolation, please select layer 2 isolation mode or layer 2 & 3 full isolation mode, and then click the “Apply” button, the operation shown in figure 3.

Figure 3 Select the isolation mode

6.2 Port Isolate Configuration

Through the port isolate configuration function, you can add ports to the isolation group, or remove ports from the isolation group, or modify the isolation group that ports join.

6.2.1 Port Isolate Group Information

If you click “Port Isolate -> Port Isolate” in the title bar, the port isolate group information page appears, as shown in figure 4.

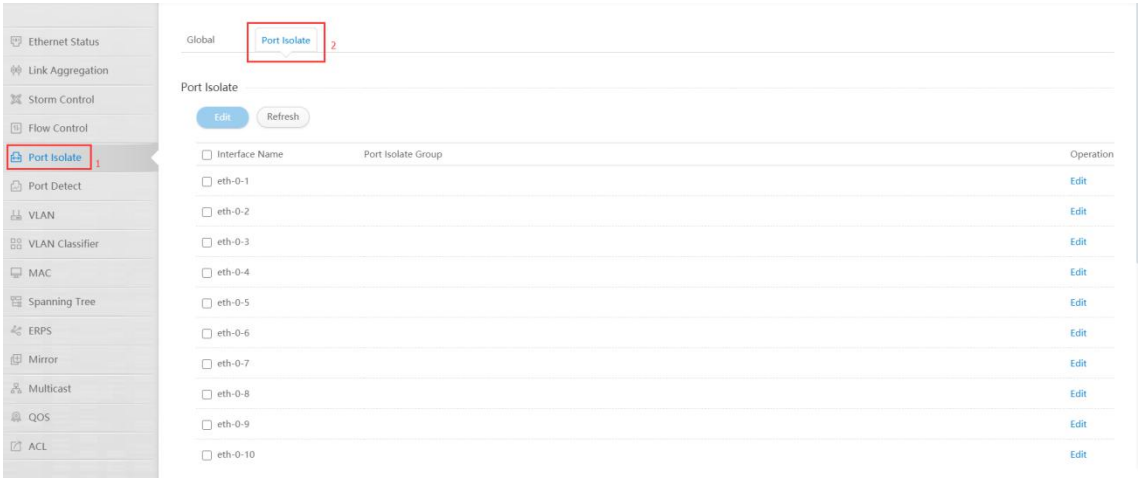


Figure 4 Port isolate group information

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Port Isolate Group	Display Specify the port isolate group

6.2.2 Join the Port Isolation Group

If you first select the port to join the port isolation group, and then click “Edit” button, you can add ports to a port isolation group, the operation is shown in figure 5. And then configure the port to join the isolation group page to appear, as shown in figure 6.

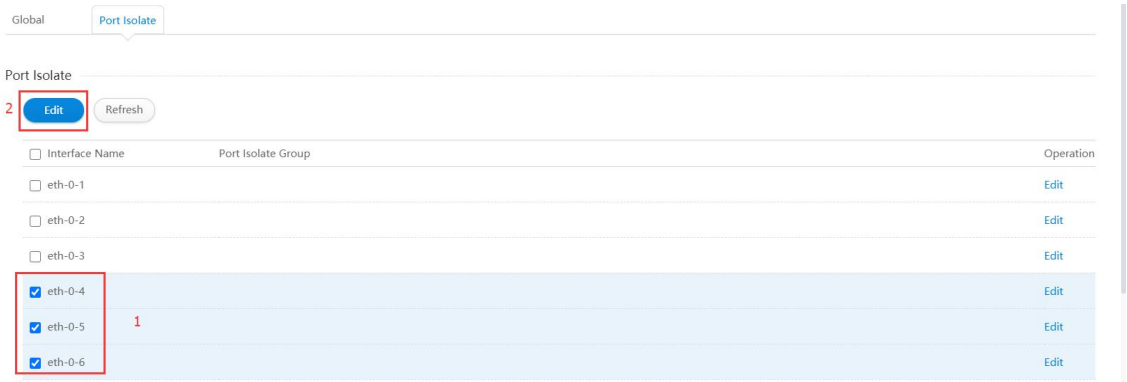


Figure 5 Add port to join the isolation group operation

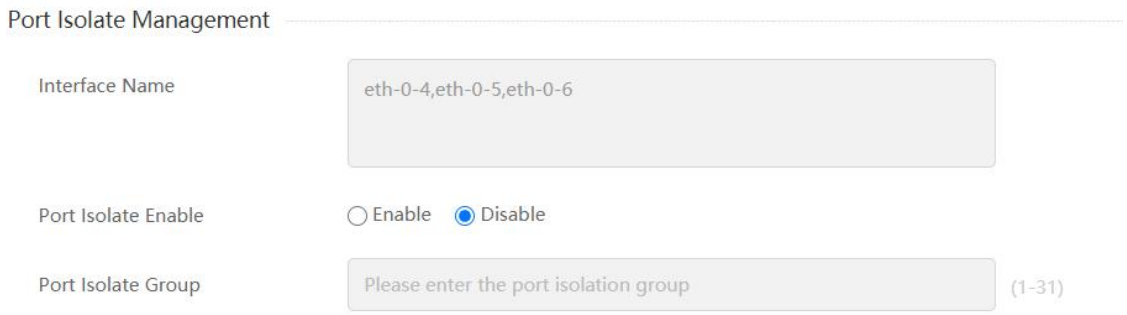


Figure 6 Add port to join the isolation group

-
- Parameter usage

Item	Description
Interface Name	Display the ports to be added to the port isolation group
Port Isolate Enable	Set whether port isolation is enabled
Port Isolate Group	Set the number to join the port isolation group

If you want to add ports to the port isolation group, you can follow the following steps:

(1) Enable port isolate in the "Port Isolate Enable" radio box.

(2) Enter the port isolation group ID in the "Port Isolate Group" textbox.

(3) Click the "Apply" button.

The operation is shown in figure 7, the port successfully joined the isolation group's table entry information is shown in figure 8.

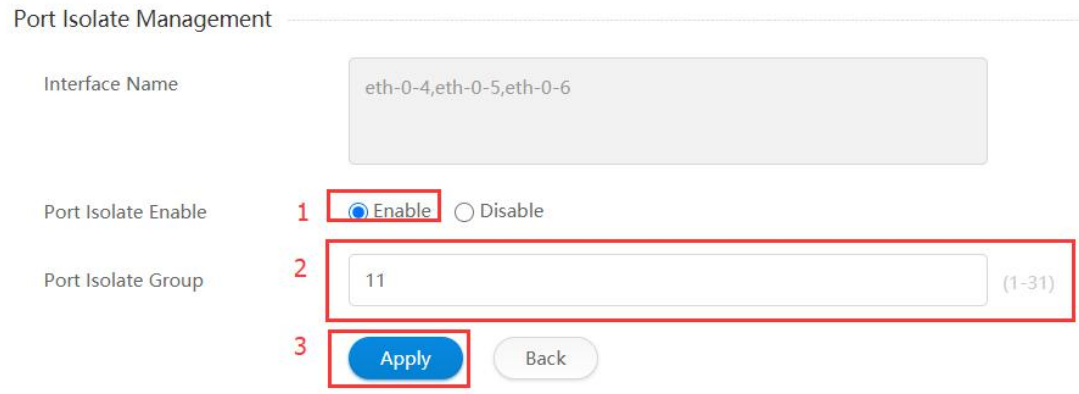


Figure 7 Port join the isolation group operation

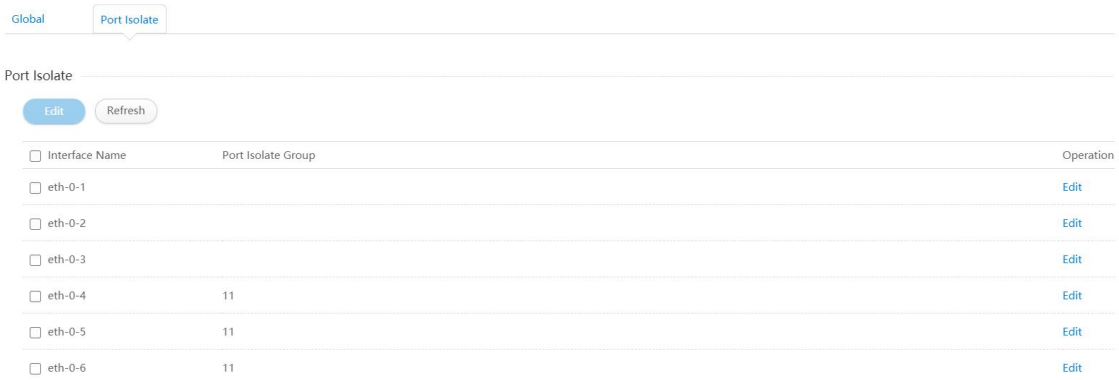


Figure 8 New port isolation group information

6.2.3 Remove the Port Isolation Group

If you select the port of the isolation group first, and then click "Edit" button, you can remove ports from the isolation group, the operation is shown in figure 9. And then the page that configured the port to be removed from the isolation group appears, as shown in figure 10.

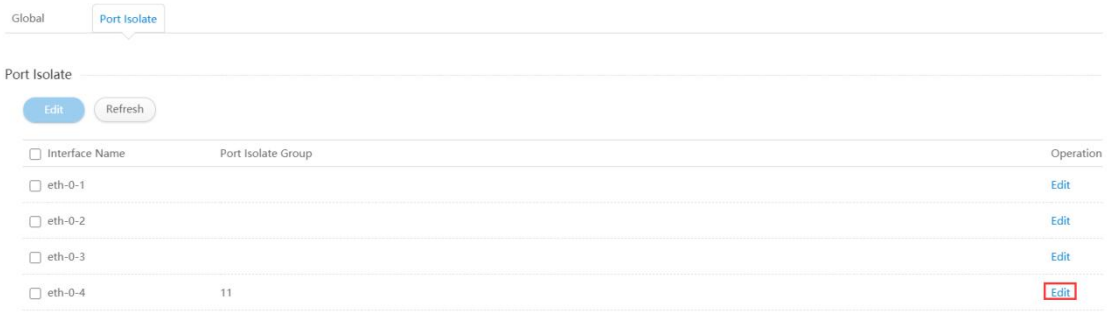


Figure 9 Configure the port to remove the isolation group operation

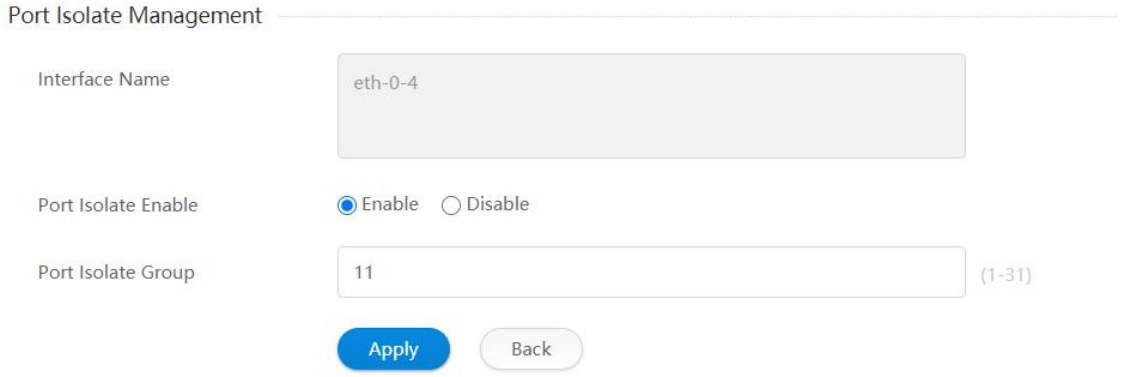


Figure 10 Remove port isolation group information

- Parameter usage

Item	Description
Interface Name	Display the ports on which the isolation group will be removed
Port Isolate Enable	Set whether port isolation is enabled
Port Isolate Group	Set the number to join the port isolation group

If you want to remove ports from the isolation group， you can disable port isolate in the "Port Isolate Enable" radio box, and then click the "Apply" button, the operation is shown in figure 11, the port was successfully removed from the isolation group is shown in figure 12.

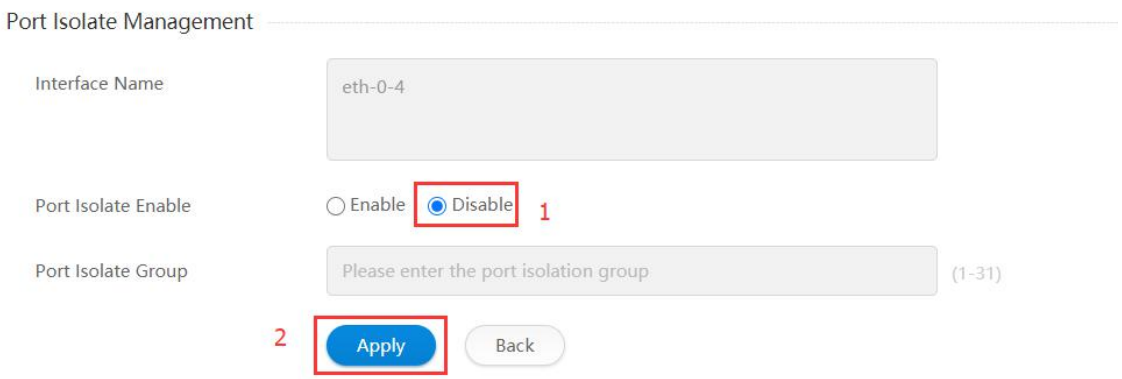


Figure 11 Port removal isolation group operation

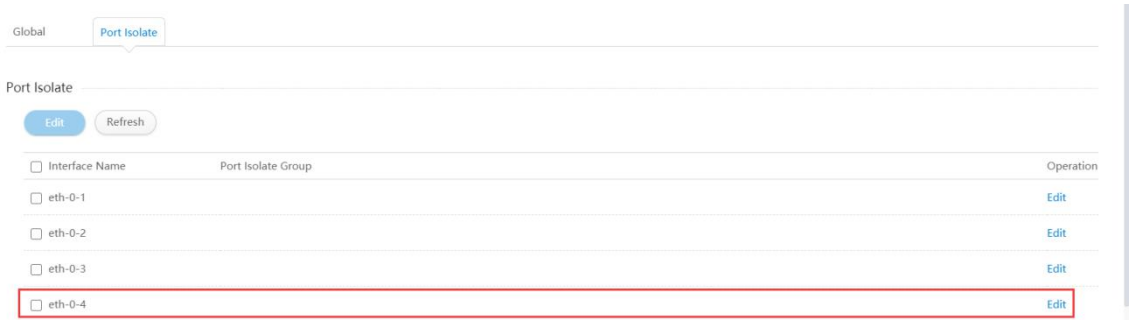


Figure 12 Port isolation group information

6.2.4 Modify the Port Isolation Group

If you select the port of the isolation group first, and then click "Edit" button, you can modify the ports to join the port isolation group, the operation is shown in figure 13. And then the modify port isolation group configuration page appears, as shown in figure 14.

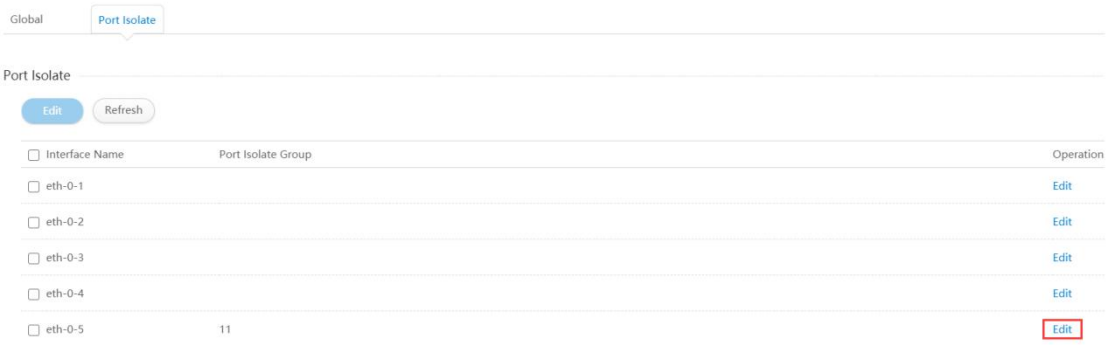


Figure 13 Configure the modify port isolation group operation

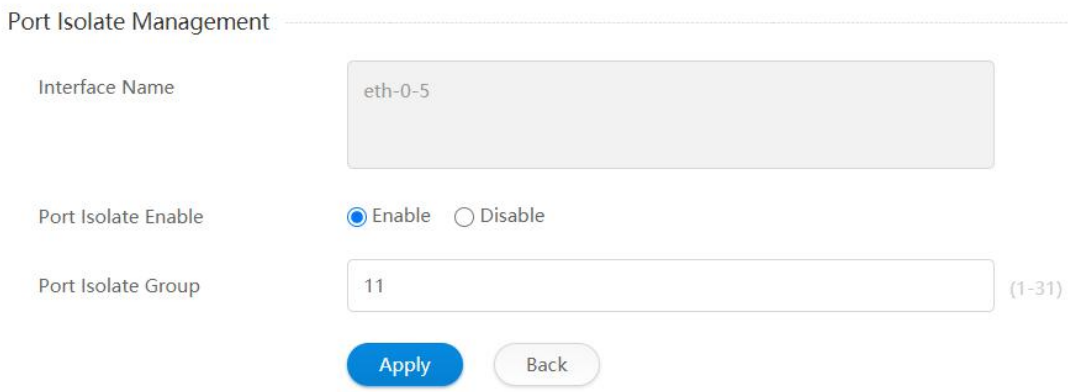


Figure 14 Modify port isolation group information

- Parameter usage

Item	Description
Interface Name	Displays the port to modify the isolation group
Port Isolate Enable	Set whether port isolation is enabled
Port Isolate Group	Set the number to join the port isolation group

If you want to modify the port isolation group id, you can modify the port isolation group id in the "Port Isolate Group" textbox, and then click the "Apply" button to modify port isolation group, the operation is shown in figure 15, the isolation group id of the port was modify successfully is shown in figure 16.

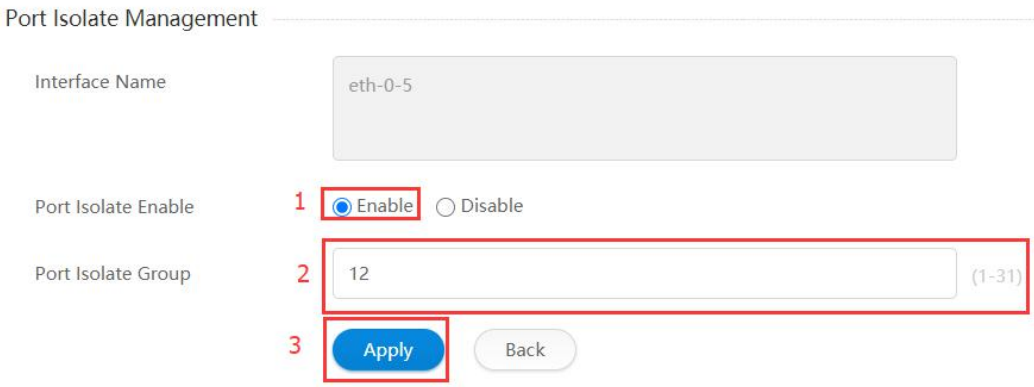


Figure 15 Modify the port isolation group operation

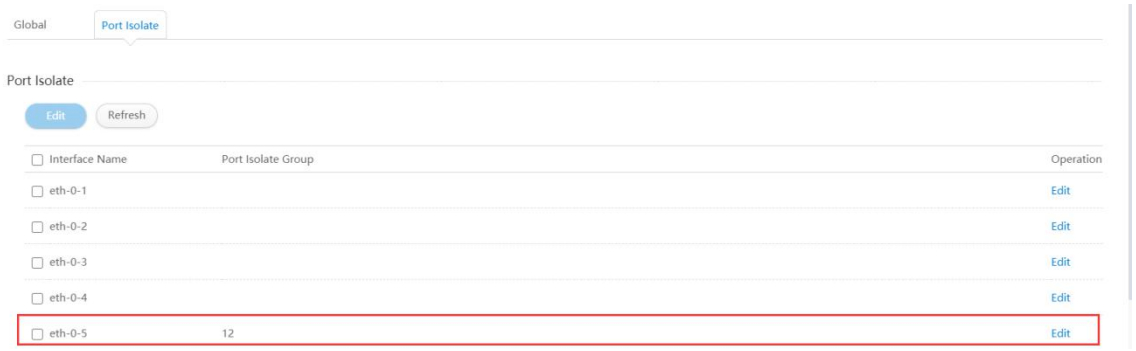


Figure 16 Port isolation group information

6.2.5 Refresh the Port Isolation Group

If you want to refresh the port isolation group configuration information, you can click “Refresh” button. The operation is shown in figure 17.

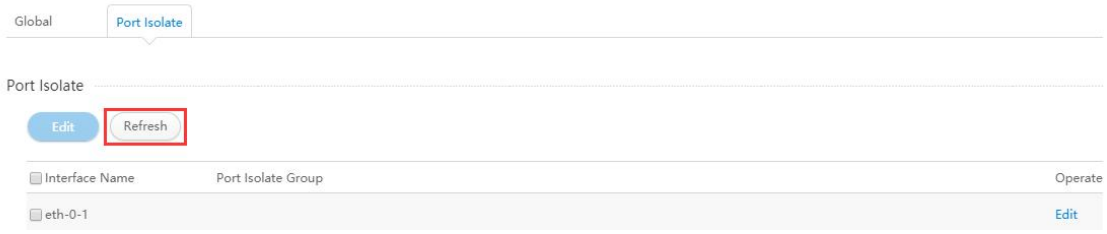


Figure 17 Refresh the port isolation group configuration information

7. Port Detect

If you click “Configuration -> Port Detect” in the top control bar, the port detect page appears, as shown in figure 1.

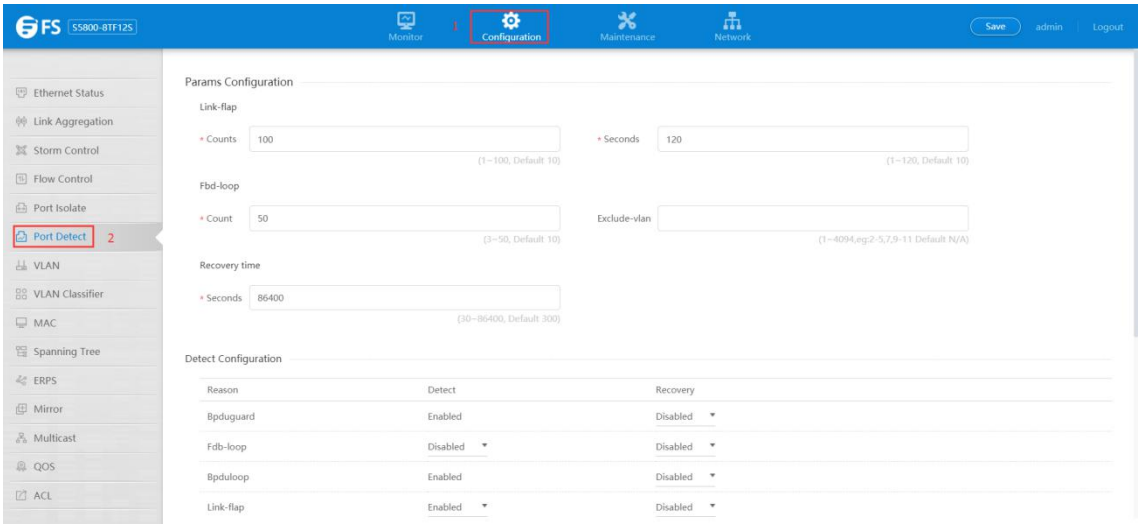


Figure 1 Port detect page

Port detect can detect the link error status of the port.

7.1 Parameter Configuration

7.1.1 Basic Information

If you click “Configuration -> Port Detect”, the parameter configuration list appears, as shown in figure 2.

Figure 2 Parameter configuration list

- Parameter usage

Item	Description
Link-flap	Display Link flapping detection
Counts	Display the number of link flapping detection
Seconds	Display the link flapping detection period in seconds

Item	Description
Fdp-loop	Display FDB for check function
Count	The number of FDB drifts detected during the period
Exclude-vlan	Set the list of VLAN that FDB does not detect
Recovery time	Interval to recover from error state
Seconds	Display the number of intervals to recover from an error state

7.1.2 Modify Parameter Configuration

If you want to modify parameter configuration, you can follow the following steps:

(1) Enter the number of times to modify link flapping detection in the "counts" text box.

(2) Enter the link flapping detection period in the "Seconds" text box.

(3) Enter the number of FDB drifts to be detected during the period in the "Count" text box.

(4) Set the list of VLAN not detected by FDB in the "Exclude-vlan" text box.

(5) Set the number of time intervals to recover from the error state in the "Seconds" text box.

(6) Click the "Apply" button to modify parameter configuration.

NOTE: The items with the asterisk symbol "*" are ones where you must enter values.

The operation is shown in figure 3, modify parameter configuration success table entry is shown in figure 4.

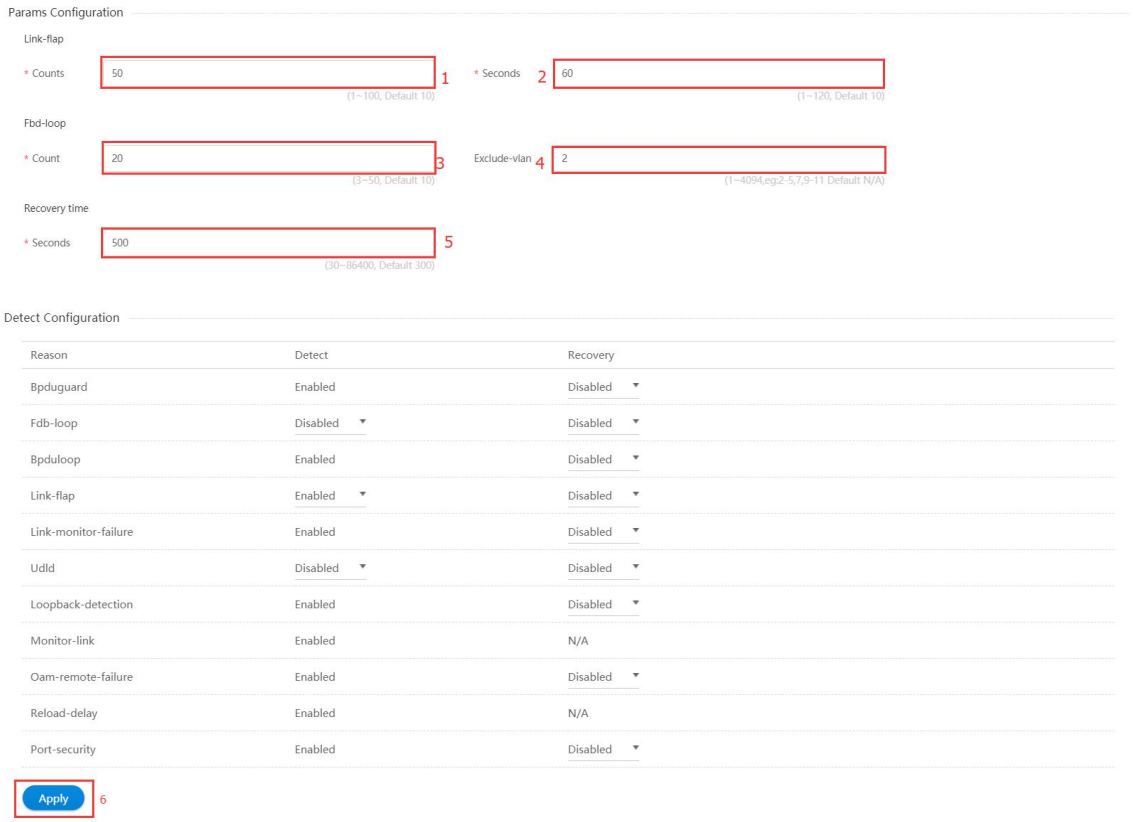


Figure 3 Parameter configuration operation

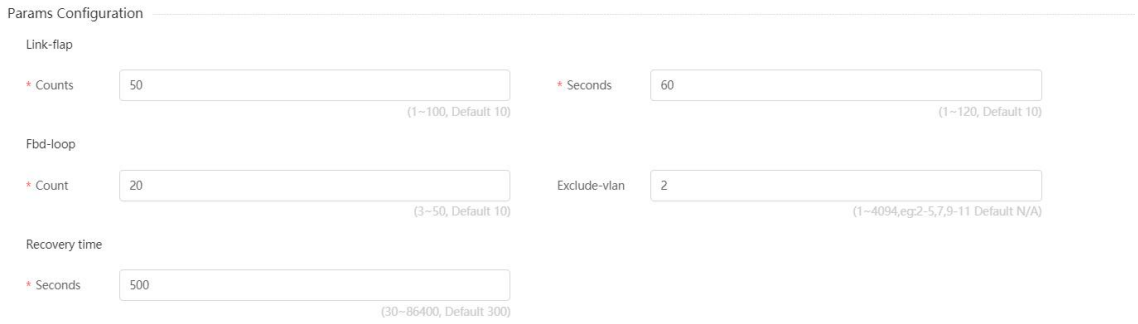


Figure 4 New parameter configuration

7.2 Detect Configuration

If you click "Configuration -> Port Detect", the detect configuration list appears, as shown in figure 5.

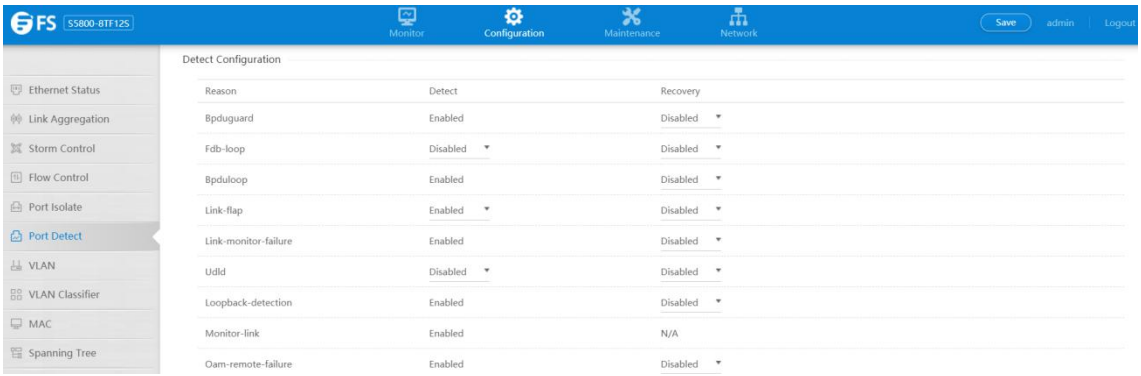


Figure 5 Detect configuration list

You can enable or disable error recovery for specific reasons in this list.

- Parameter usage

Item	Description
Bpduguard	Display Enable recovery from BPDU guard error state
Fdb-loop	Display Enable FDB loop recovery function
bpduloop	Display enable BPDU loopback error status recovery function
link-flap	Display the function of link flapping error recovery
link-monitor-failure	Display enable link monitoring error recovery
udld	Display enable UDLD error recovery function
loopback-detection	Display enable loopback detection error status recovery function
monitor-link	Display enable link monitoring recovery function
oam-remote-failure	Display enable recovery from OAM error
Reload-delay	Display enable reload delay function
Port-security	Display enable port binding error recovery

7.2.1 Modify Error Recovery Function

If you want to modify enable or disable error recovery function, such as enable fdb-loop and link-flap error recovery function, you can follow the following steps:

(1) Select the enable of the drop-down box of the recovery bar corresponding to fdb-loop.

(2) Select the enable of the drop-down box of the recovery bar corresponding to link-flap.

(3) Click the "Apply" button to modify error recovery function.

The operation is shown in figure 6, modify error recovery function success table entry is shown in figure 7.

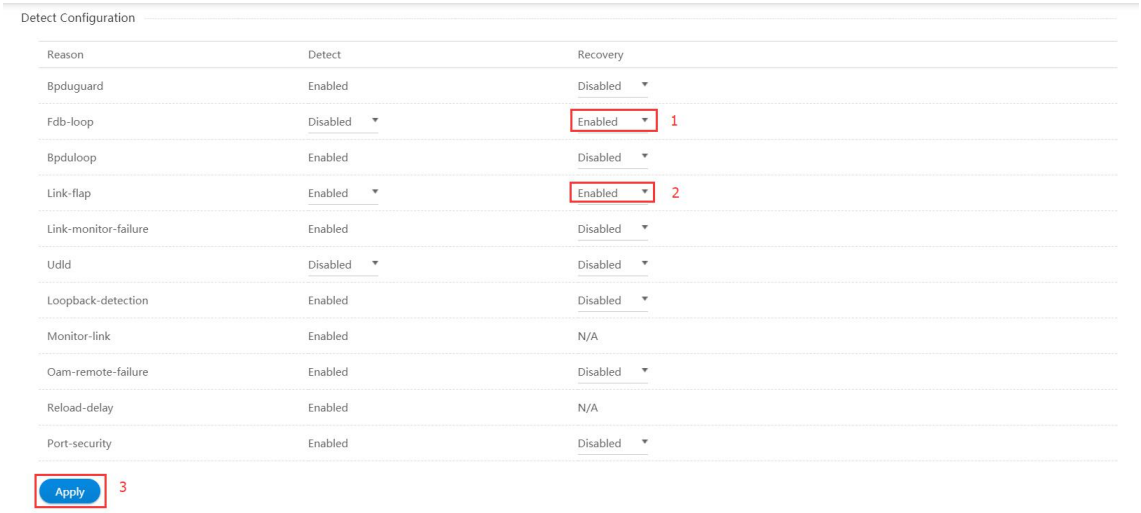


Figure 6 Modify error recovery function operation

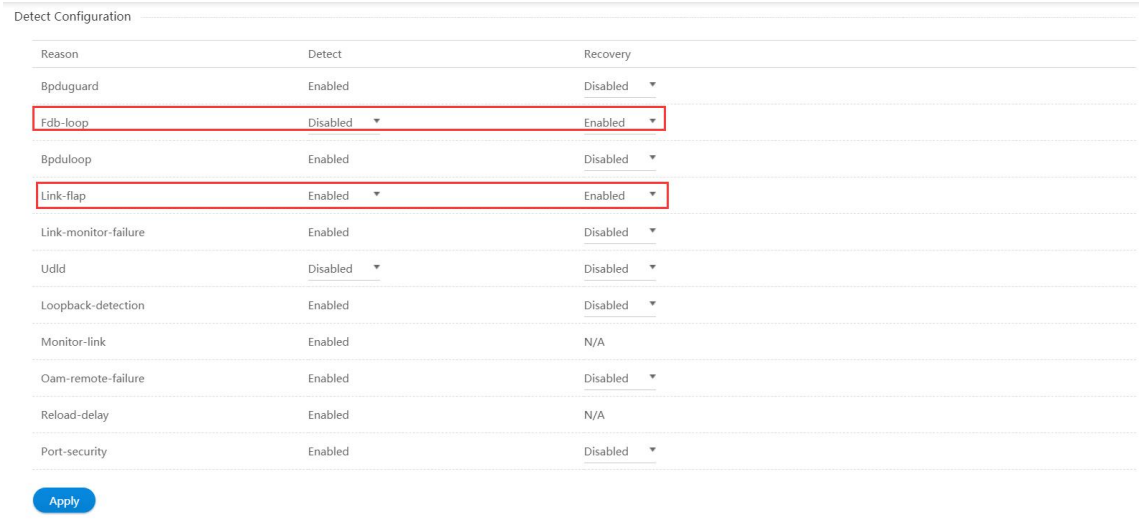


Figure 7 New detect configuration list

8. VLAN

8.1 VLAN

VLAN (Virtual Local Area Network) means logically dividing a LAN (Local Area Network) into many different subsets, and each subset will form its own broadcast domain. In short, VLAN is a telecommunication technology dividing a physical LAN into many broadcast domains. The hosts in VLAN can directly communicate with each other, while VLANs can not directly intercommunicate. Therefore, the broadcast message is limited in a VLAN. The network security is improved.

If you click “Configuration ->VLAN” in the top control bar, the VLAN configuration list page appears, as shown in figure 1.

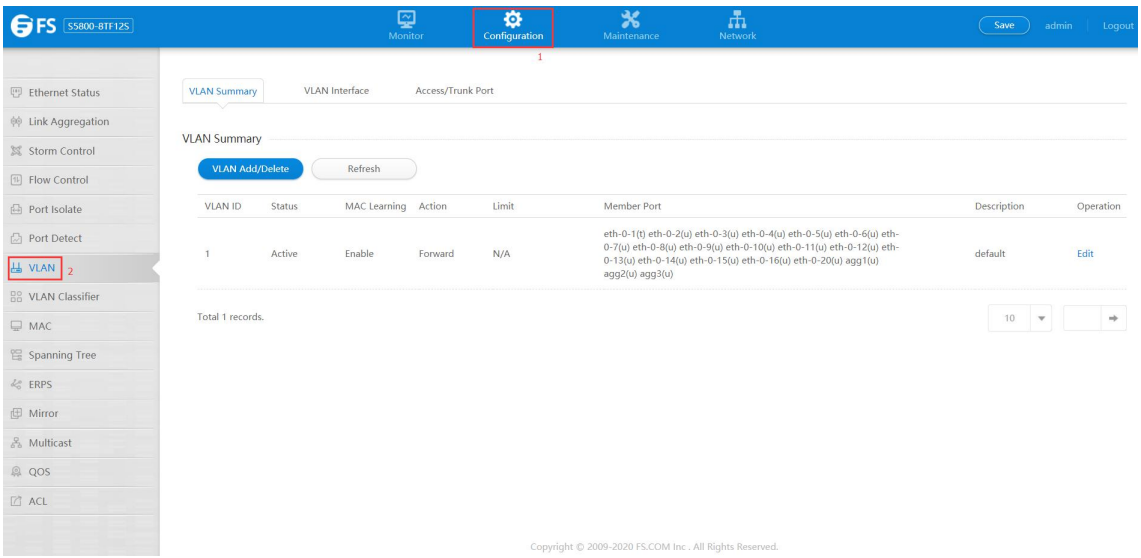


Figure 1 VLAN configuration list

This section describes VLAN configuration function and viewing VLAN information of the switch.

8.1.1 Basic Information

If you click “VLAN > VLAN Summary” in the title bar, the VLAN summary page appears, as shown in figure 2.

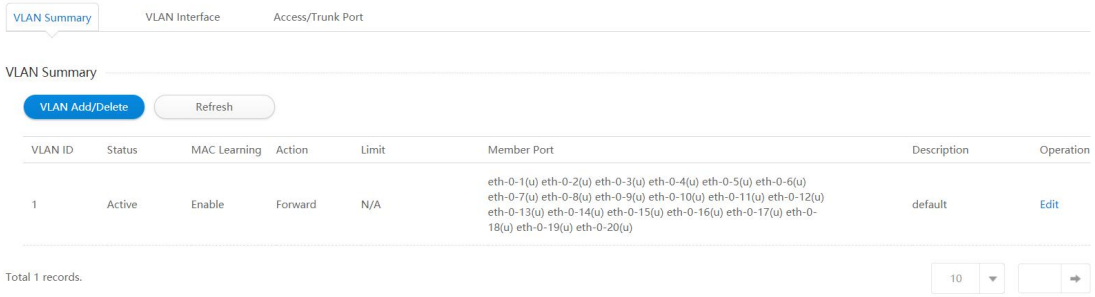


Figure 2 VLAN summary information

- Parameter usage

Item	Description
VLAN ID	Display the number of interface
Status	Display the status of VLAN
Replace DSCP	Display the replace DSCP of VLAN
MAC Learning	Display the MAC learning status of VLAN
Action	Display the action mode of VLAN
Limit	Display the mac-limit maximum of VLAN
Member Port	Display the member port of VLAN
Description	Description about the VLAN
Operate	Display that interface entries can be edited

8.1.2 Add or Delete VLAN

If you click “VLAN add/delete” button, you can add add/delete VLAN , the operation is shown in figure 3. And then the add VLAN & VLAN range settings page appears, as shown in figure 4.

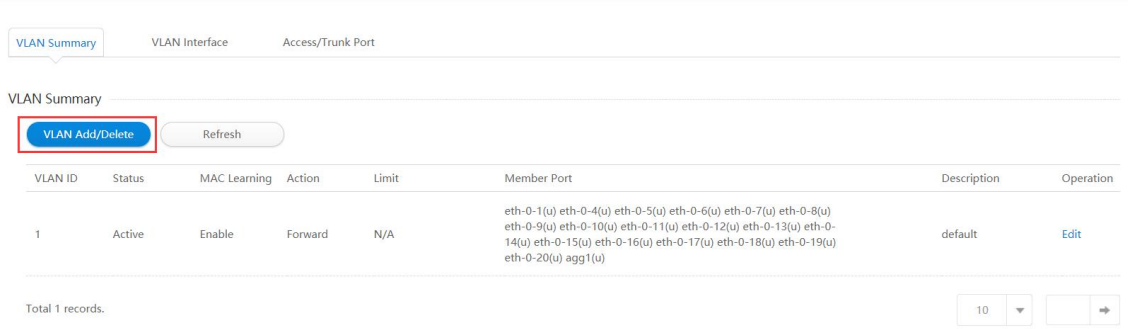


Figure 3 Add or delete VLAN operation

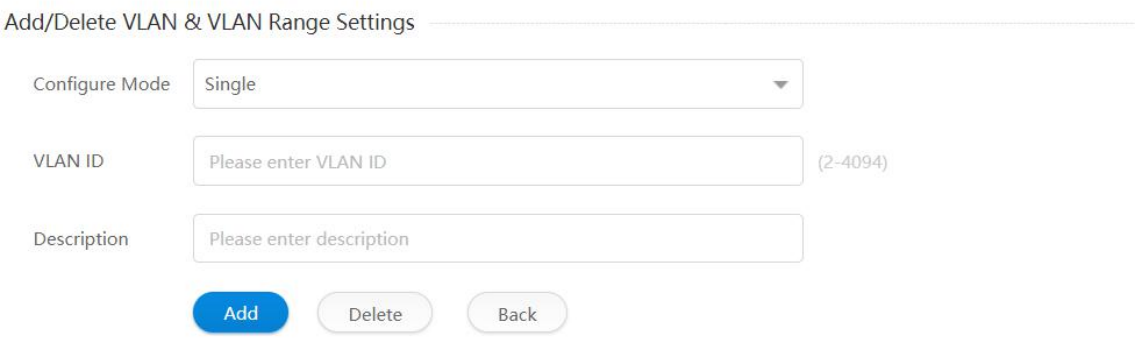


Figure 4 Add/Delete VLAN & VLAN range settings

- Parameter usage

Item	Description
Configure Mode	Display specify VLAN add mode
VLAN ID	Display the number of interface (rang 2-4994)
Description	Description about the VLAN
Operate	Display that interface entries can be edited

If you want to add/delete VLAN, you can follow the following steps:

(1) Select the configure mode.

(2) Enter VLAN ID.

(3) Enter Description.

(4) Click the "Add"/"Delete" button to apply all the changes made.

The operation is shown in figure 5, VLAN configuration success table entry is shown in figure 6.

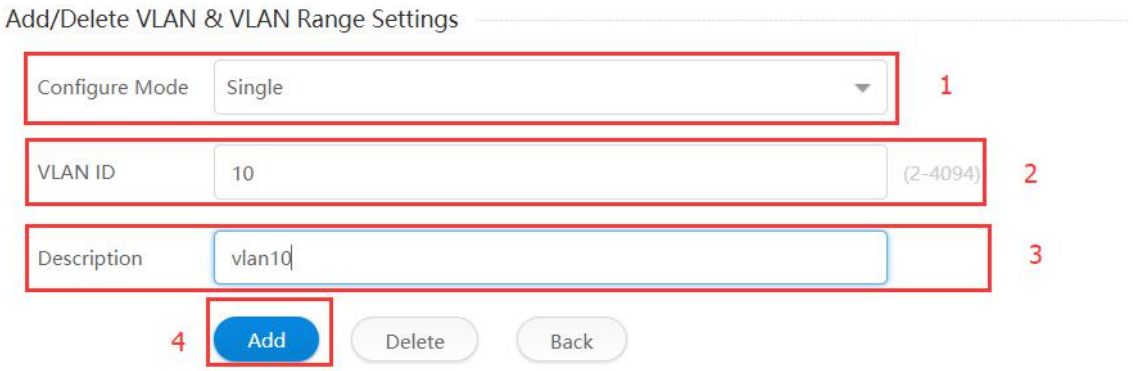


Figure 5 Add VLAN & VLAN range settings configuration

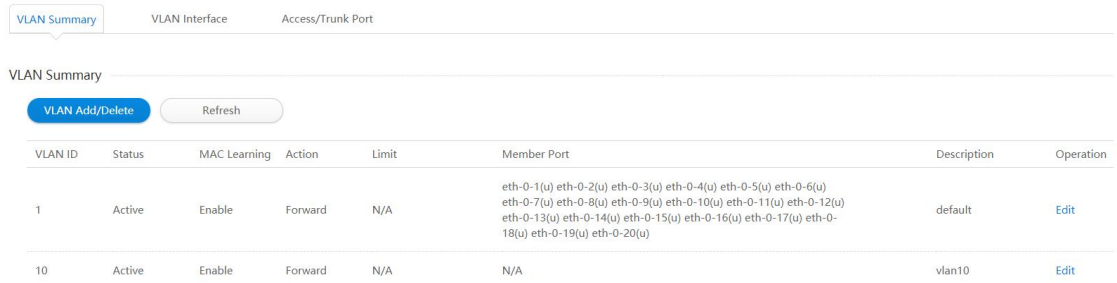


Figure 6 New VLAN information

8.1.3 Modify VLAN

If you want to modify a VLAN, please click "Edit" button, the operation shown in figure 7, VLAN detailed configuration page appears, as shown in figure 8.

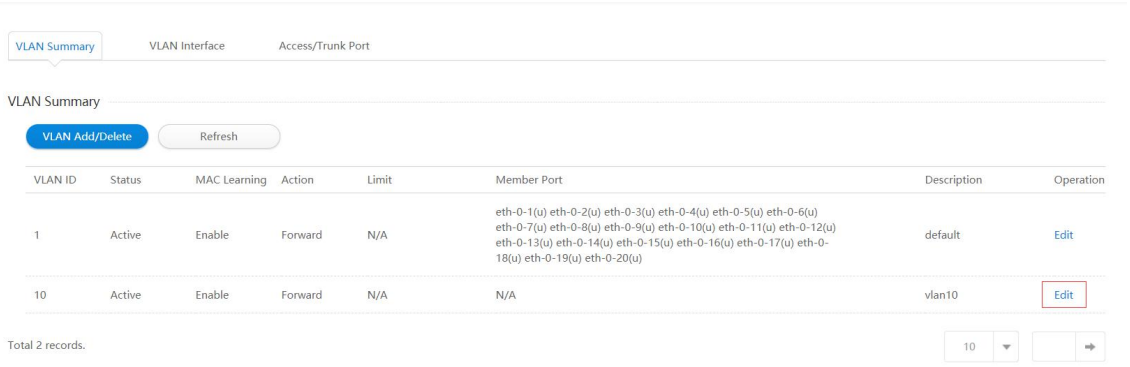


Figure 7 Modify VLAN operation

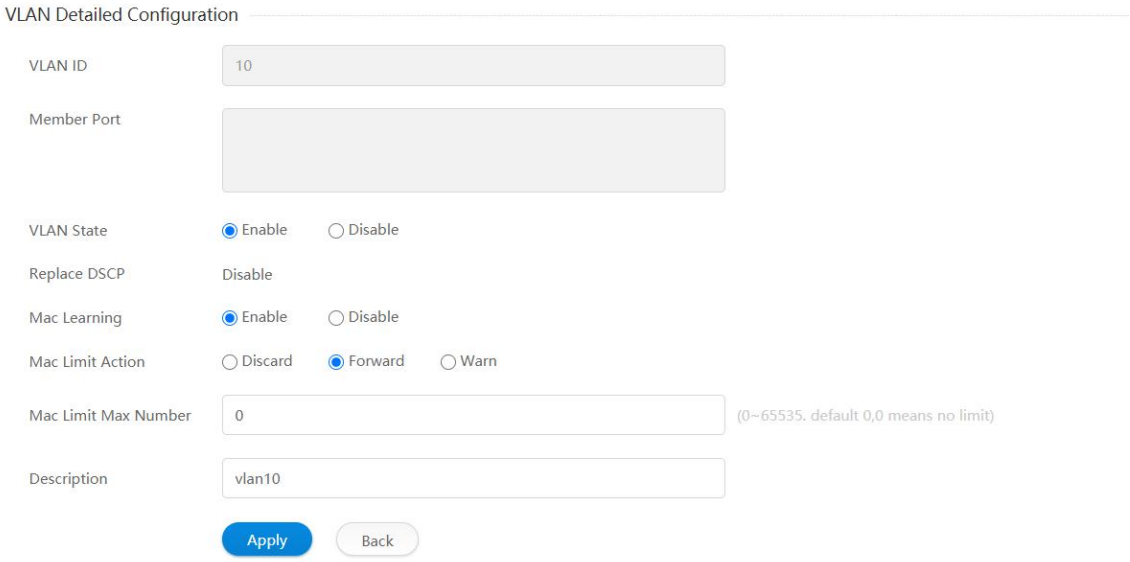


Figure 8 VLAN detailed configuration

- Parameter usage

Item	Description
VLAN ID	Display the number of interface
Member Port	Display the member port of VLAN
VLAN Status	Display the status of VLAN
Replace DSCP	Display the replace DSCP of VLAN
MAC Learning	Display the MAC learning status of VLAN
Mac Limit Action	Display the action mode of VLAN
Mac Limit Max Number	Display the mac-limit maximum of VLAN
Description	Description about the VLAN

If you want to modify a VLAN detail, you can follow the following steps:

(1) Choose VLAN state.

(2) Choose MAC Learning.

(3) Choose Mac Limit Action.

(4) Modify the mac-limit maximum of VLAN.

(5) Modify the description about the VLAN.

(6) Click the “Apply” button to apply all the changes made.

The operation is shown in figure 9.

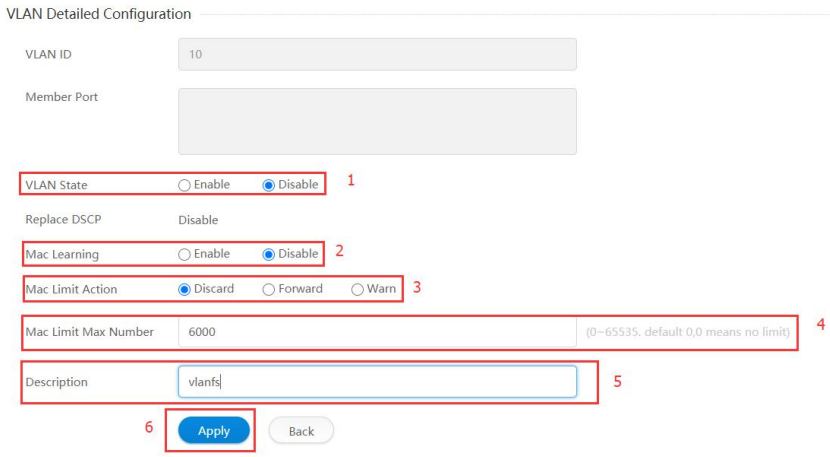


Figure 9 Modify VLAN detailed configuration

8.2 VLAN Interface

VLAN interface: a logical interface with three layers of characteristics, through the configuration of VLANIF interface IP address, VLAN visits.VLAN interfaces can be created and deleted.

Through the VLAN interface configuration function, you can add/modified/delete the VLAN interface on switch.

8.2.1 VLAN Interface Information

If you click “VLAN -> VLAN Interface” in the title bar, the VLAN Interface page appears, as shown in figure 10.

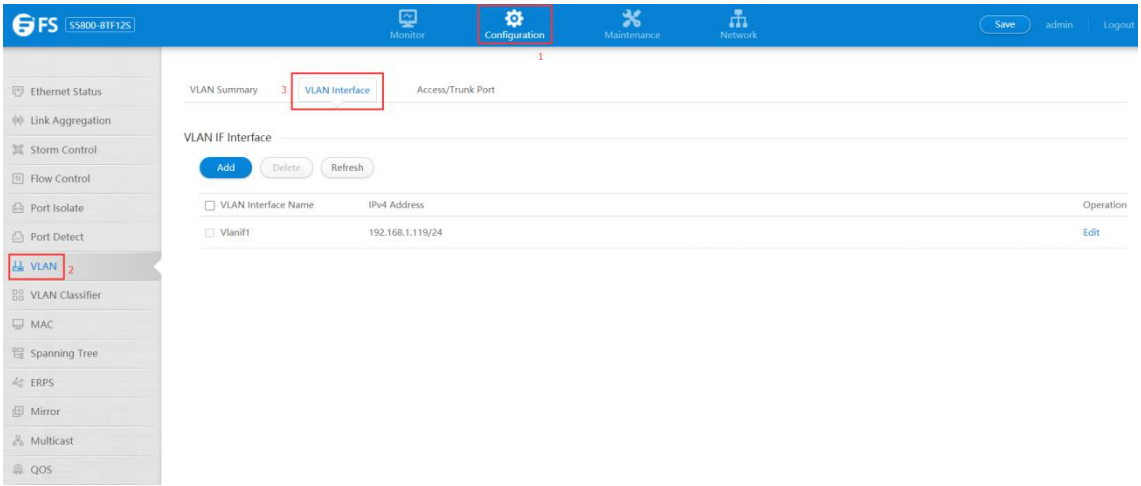


Figure 10 VLAN interface

- Parameter usage

Item	Description
VLAN interface Name	Display Layer 3 VLAN interface name
IPv4 Address	Set the IP address of an interface
Operate	Display that interface entries can be edited

8.2.2 Add VLAN IF

If you click "New" button, you can add a VLAN IF, the operation is shown in figure 11. and then the VLAN Interface Management page appears, as shown in figure 12.

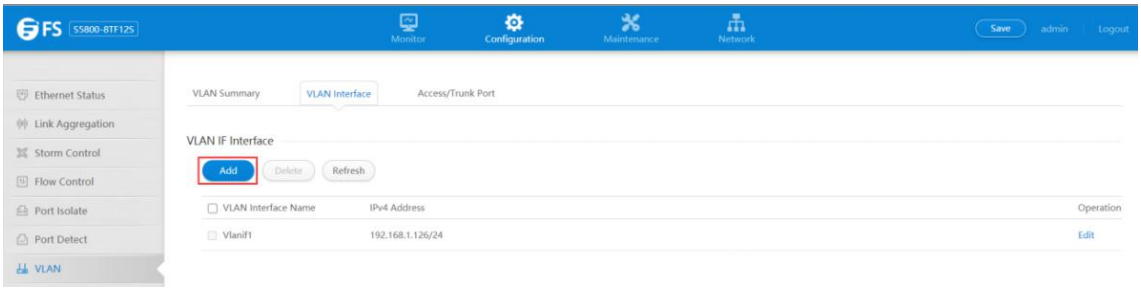


Figure 11 Add VLAN IF operation

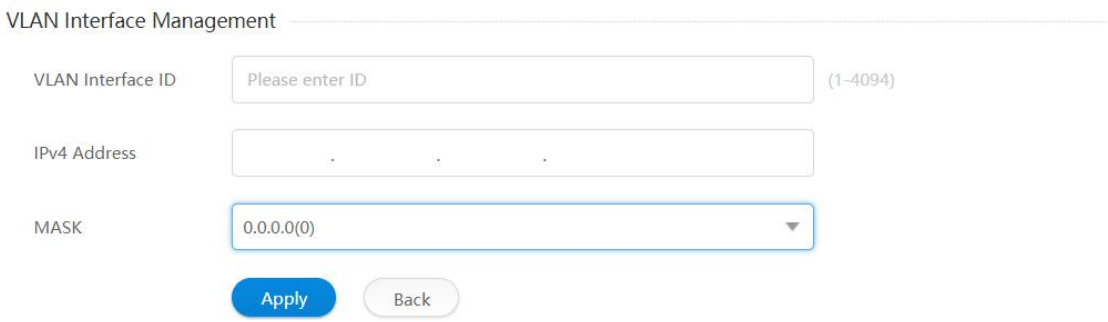


Figure 12 VLAN interface management

- Parameter usage

Item	Description
VLAN interface ID	Display Layer 3 VLAN interface name
IPv4 Address	Set the IP address of an interface
Mask	IP subnet mask

If you want to add the VLAN IF, you can follow the following steps:

(1) Enter a VLAN id in the "VLAN interface ID" textbox, but you should first create a VLAN which you want to use.

(2) Enter IP address in the "IPv4 Address" textbox.

(3) Select the destination address mask in the "mask " dropdown box.

(4) Click the "Apply" button to apply all the changes made.

The operation is shown in figure 13, route configuration success table entry is shown in figure 14.

Figure 13 Add VLAN IF configuration

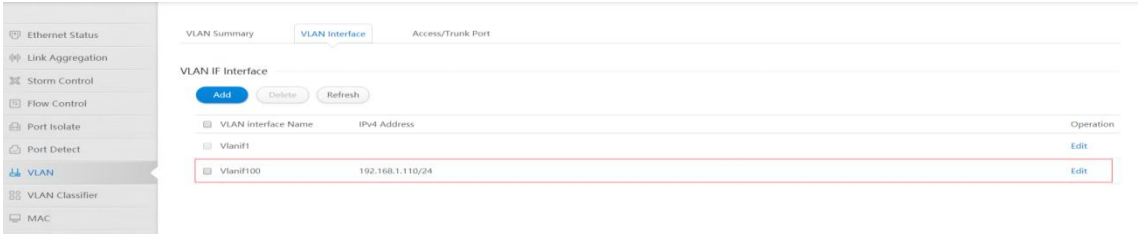


Figure 14 New VLAN IF information

8.2.3 Delete VLAN IF

If you want to delete the specified VLAN IF, you can follow the following steps:

(1) select this specified VLAN IF which you want to delete.

(2) click "Delete" button.

(3) confirm the selected delete VLAN IF and page appears as shown in figure 15, if you click "Confirm" button, you can delete this VLAN IF.

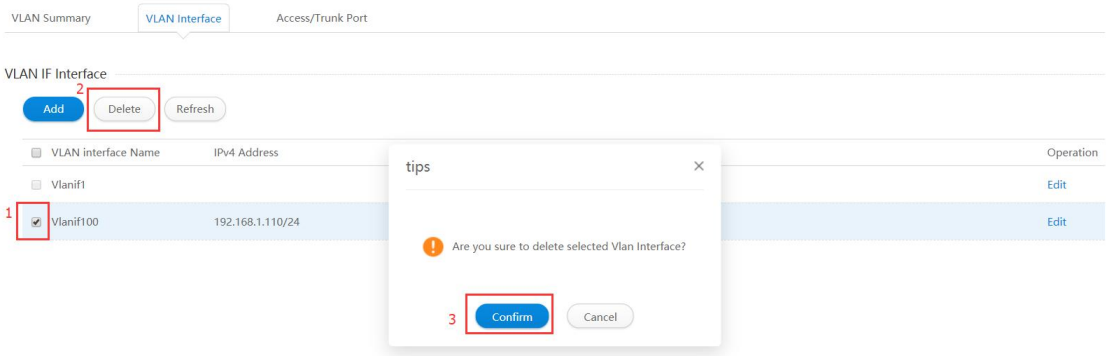


Figure 15 Delete VLAN IF

8.3 Acess/Trunk Port

8.3.1 Acess /Trunk Port Basic Information

If you click "VLAN > Access/Trunk Port" in the title bar, the access/trunk port page appears, as shown in figure 16.

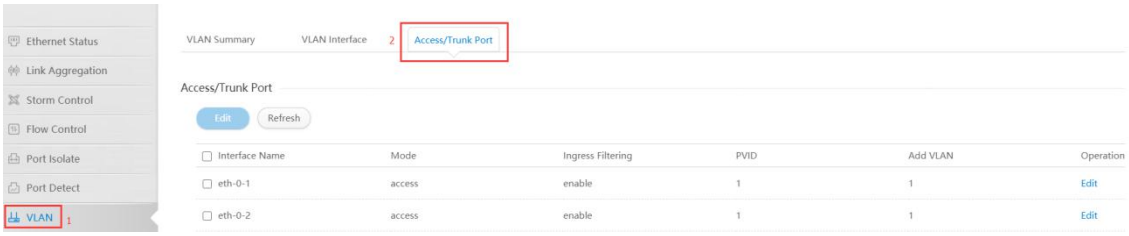


Figure 16 Access/Trunk port information

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Mode	Indicate VLAN membership mode for an interface Access: set the port as an Access VLAN interface. The port transmits tagged or untagged frames on a single VLAN only Trunk: specify an interface as VLAN Trunk interface. A trunk is a direct link between two switches, so the interface transmits tagged frames marked the source VLAN. Note that frames belonging to the interface's default VLAN are also transmitted as untagged frames
Ingress Filtering	Determine how to process the tagged frame, which is not included in this VLAN. (Default: Enable) Ingress filtering only affects tagged frames. If ingress filtering is disabled and the interface receives a tagged frame which is not included in this VLAN, these frames will be flooded to all other ports within this VLAN If ingress filtering is enabled and the interface receives a tagged frame, which is not included in this VLAN, then the frame will be dropped
PVID	Display the native VLAN ID of interface
AddVLAN	If the displayed link type is Trunk, VLAN ID or list is allowed to pass through the interface If the displayed link type is Access, the VLAN ID that the interface belongs to, and the tagged or untagged frames received on the interface will be tagged with the VLAN ID (default: 1)
Operate	Display that interface entries can be edited

8.3.2 Access/Trunk Port Modification

If you want to modify the configuration to specify access/trunk port, please click "Edit" button in the operation bar, or you can follow the following steps:

(1) Select this interface which you want to edit.

(2) Click "Edit" button.

the operation is shown in figure 17. and then the access/trunk port modification page appears, as shown in figure 18.

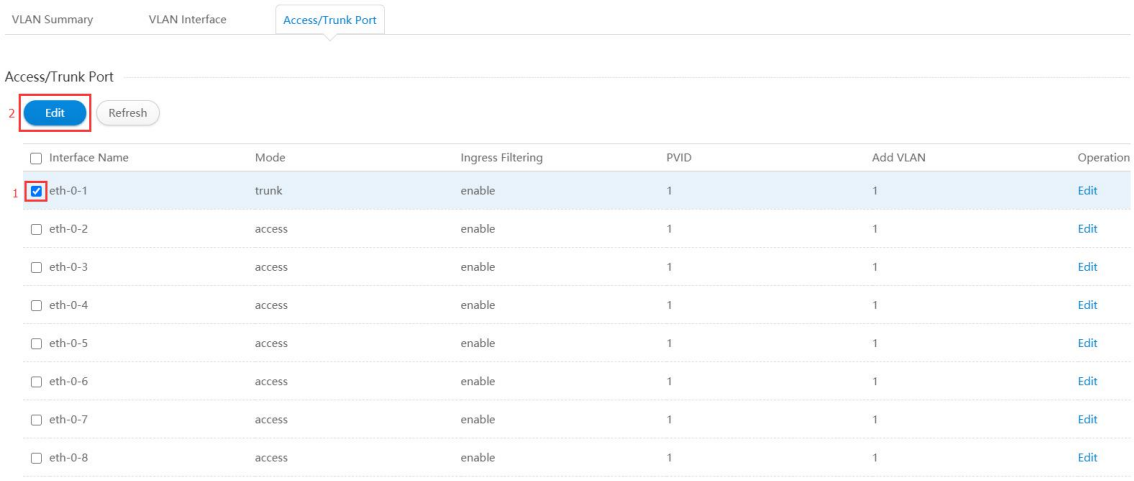


Figure 17 Access/Trunk port edit operation

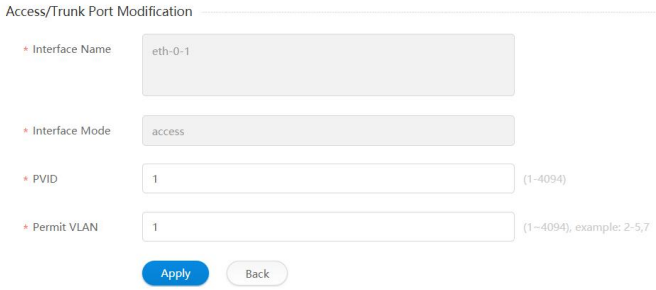


Figure 18 Access/Trunk port modification

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Interface Mode	Indicate VLAN membership mode for an interface Access: set the port as an Access VLAN interface. The port transmits tagged or untagged frames on a single VLAN only Trunk: specify an interface as VLAN Trunk interface. A trunk is a direct link between two switches, so the interface transmits tagged frames marked the source VLAN. Note that frames belonging to the interface's default VLAN are also transmitted as untagged frames
Ingress Filtering	Determine how to process the tagged frame, which is not included in this VLAN. (Default: Enable) Ingress filtering only affects tagged frames. If ingress filtering is disabled and the interface receives a tagged frame which is not included in this VLAN, these frames will be flooded to all other ports within this VLAN If ingress filtering is enabled and the interface receives a tagged frame, which is not included in this VLAN, then the frame will be dropped
PVID	Display the native VLAN ID of interface

Item	Description
Permit VLAN	If the displayed link type is Trunk, VLAN ID or list is allowed to pass through the interface If the displayed link type is Access, the VLAN ID that the interface belongs to, and the tagged or untagged frames received on the interface will be tagged with the VLAN ID (default: 1)
Operate	Display that interface entries can be edited

If you want to modify an access/trunk port, you can follow the following steps:

(1) Modify PVID in the "PVID" textbox.

(2) Modify Permit VLAN in the "Permit VLAN" textbox.

(3) Click the "Apply" button to modify the specify static route.

The operation is shown in figure 19.

Note: When the port mode is trunk, you can select the progress filtering able or disable.

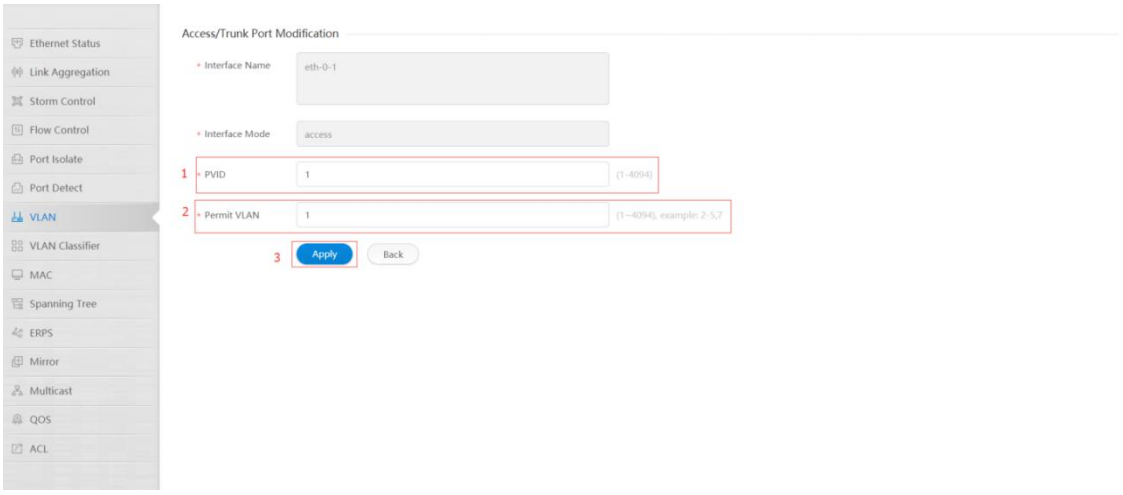


Figure 19 Modify an access/trunk port configuration

9. VLAN Classifier

If you click “Configuration -> VLAN Classifier” in the top control bar, the VLAN classifier configuration page appears, as shown in figure 1.

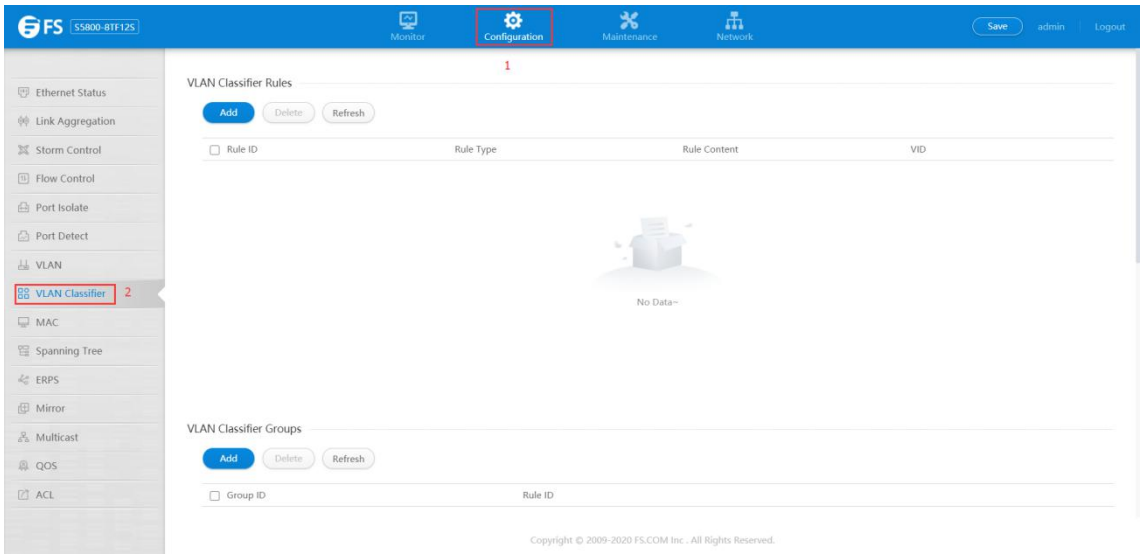


Figure 1 VLAN classifier list

This section mainly describes how to configure and view VLAN classifier.

9.1 VLAN Classifier Rules

If you click “Configuration -> VLAN Classifier”, the VLAN classifier rules list appears, as shown in figure 2.

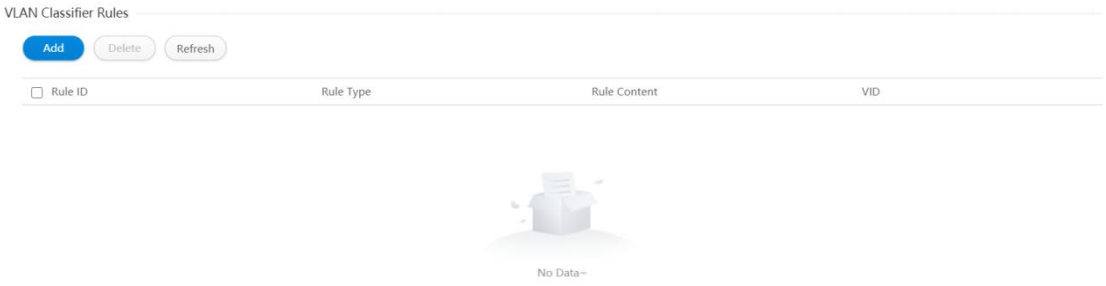


Figure 2 VLAN classifier rules List

- Parameter usage

Item	Description
Rule ID	Display the ID of Rule
Rule Type	Display the Type of Rule, including IP, MAC and protocol
Rule Content	Display the IP address of the current rule
VID	Display the VLAN ID of interface.

9.1.1 Add VLAN Classifier Rules

If you click "Add" in the VLAN classifier rules list, you can add a VLAN classifier rule, the operation is shown in figure 3, then VLAN classifier rule settings page appears, as shown in figure 4.

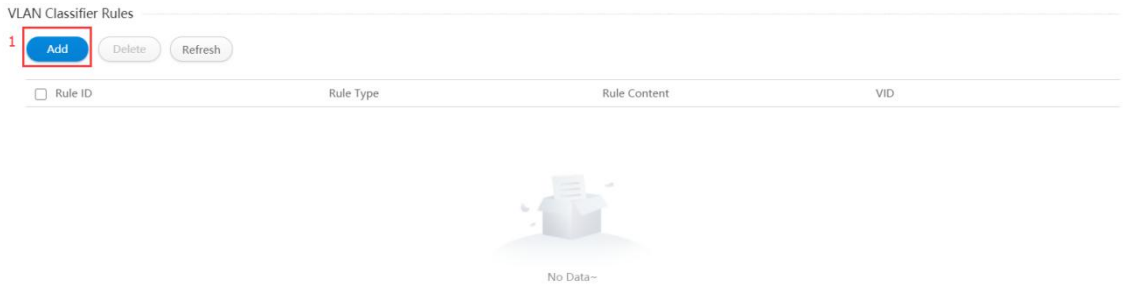


Figure 3 Add VLAN classifier rules operation

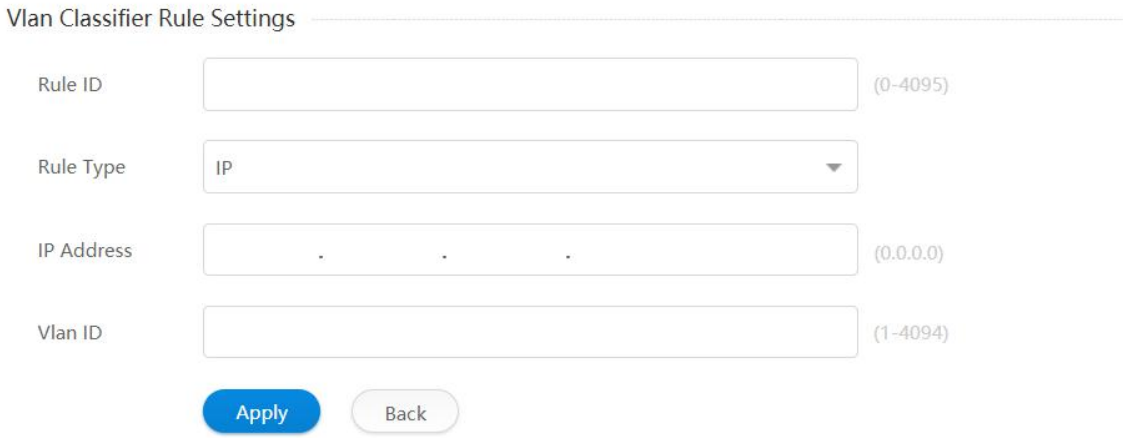


Figure 4 VLAN classifier rule settings list

- Parameter usage

Item	Description
Rule ID	Display the ID of Rule
Rule Type	Display the Type of Rule, including IP, MAC and protocol
IP Address	IP address for which classification rules need to be set
VLAN ID	Display the VLAN ID of interface
IP	IP-based VLAN are classified based on the source IP address of incoming packets
MAC	MAC-based VLAN are classified based on the source MAC address of incoming packets
protocol	Protocol-based VLAN are classified based on Layer 3 protocol type incoming packets

If you want to add a VLAN classifier rule, you can follow the following steps:

(1) Enter a rule ID in the range of 0-4095.

(2) Select IP/ MAC/ protocol from the “Rule Type” drop-down box.

(3) Enter a valid IP address in the “IP Address” text box.

(4) Enter the VLAN ID in the range of 1- 4094.

(5) Click the “Apply” button to add a VLAN classifier rule.

The operation is shown in figure 5, add a VLAN classifier rule configuration success table entry is shown in figure 6.

Figure 5 Add VLAN classifier rule configuration

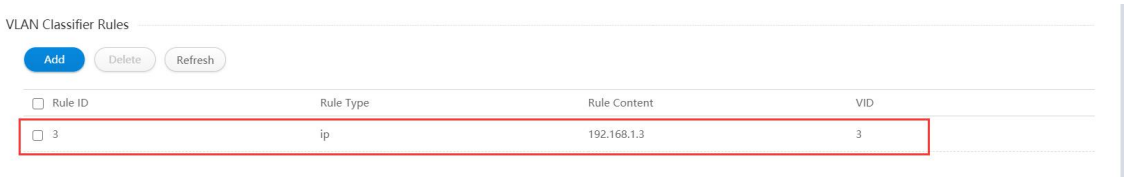


Figure 6 New VLAN classifier rule information

9.1.2 Delete VLAN Classifier Rules

If you want to delete the specified VLAN classifier rule, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified VLAN classifier rule.

(2) Click “Delete” button.

(3) It will appear tips page to note you to confirm the operation, if you click “Confirm” button , it will delete this VLAN classifier rule;

If you click “cancel” button, you will cancel delete this VLAN classifier rule operation, as shown in figure 7.

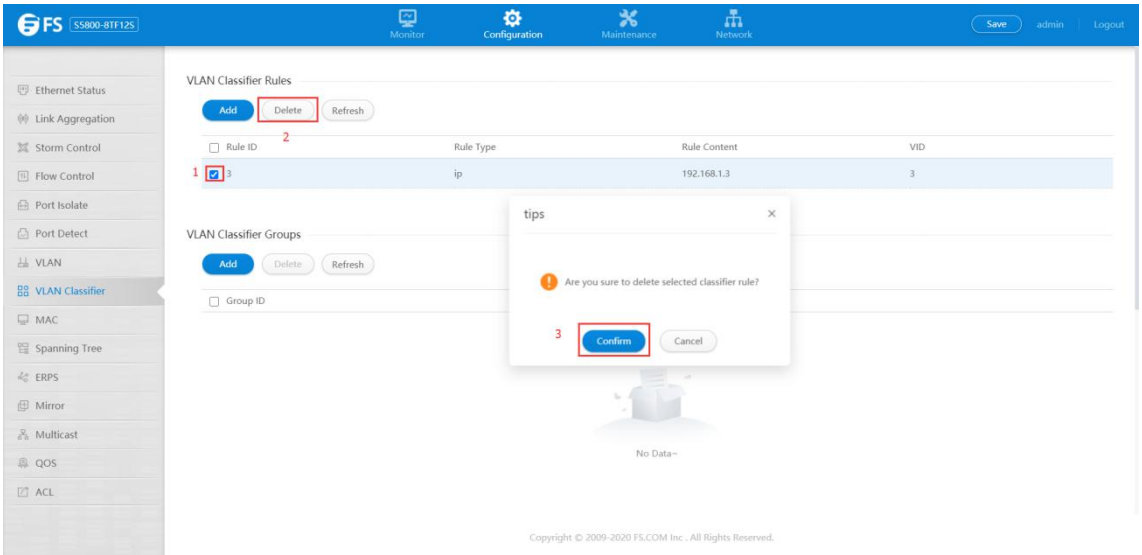


Figure 7 Delete VLAN classifier rule operation

Delete a VLAN classifier rule configuration success table entry is shown in figure 8.

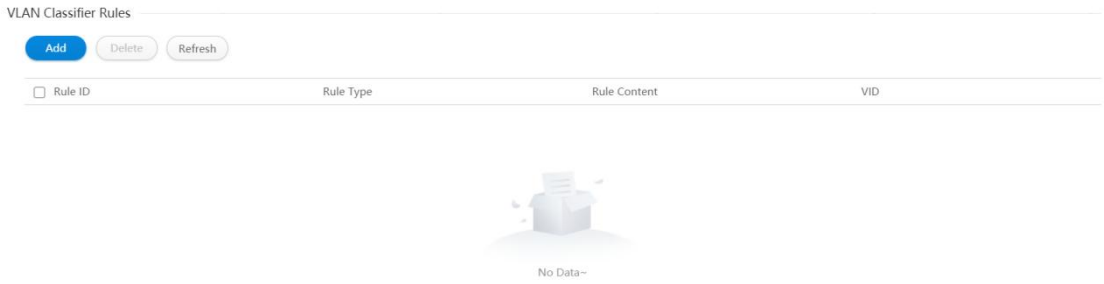


Figure 8 Delete VLAN classifier rule information

9.2 VLAN Classifier Groups

If you click “Configuration -> VLAN Classifier”, the VLAN classifier groups list appears, as shown in figure 9.

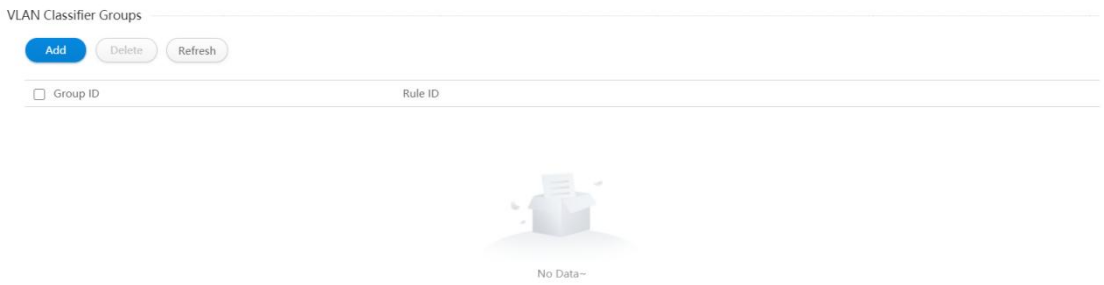


Figure 9 VLAN classifier groups list

9.2.1 Add VLAN Classifier Groups

If you click “Add” in the VLAN classifier groups list, you can add a VLAN classifier group, the operation is shown in figure 10, then the VLAN classifier groups settings page appears, as shown in figure 11.

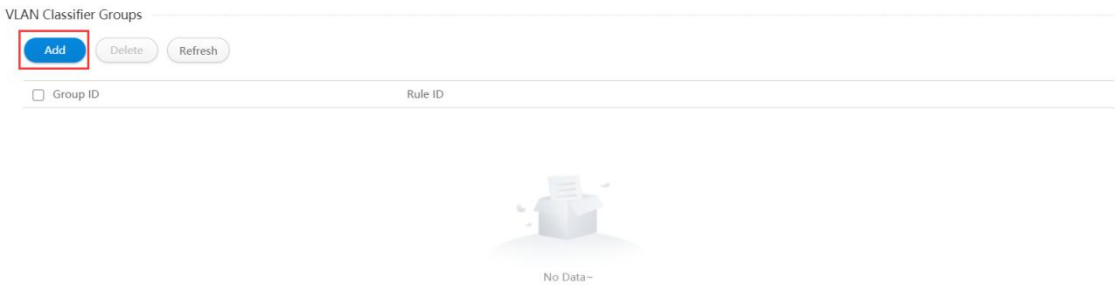


Figure 10 Add VLAN classifier group operation

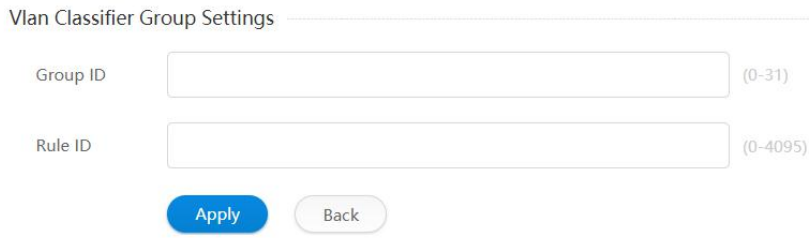


Figure 11 VLAN classifier group settings list

- Parameter usage

Item	Description
Group ID	Set the ID of Group
Rule ID	Set the ID of Group

If you want to add a VLAN classifier group, you can follow the following steps:

(1) Enter a group ID in the range of 0-31.

(2) Enter a rule ID in the range of 0- 4095, the rule ID must exist in the VLAN classifier rules list.

(3) Click the "Apply" button to add a VLAN classifier group.

NOTE: Different types of VLAN classifier rules can be added to the same VLAN classification group.

The operation is shown in figure 12, add a VLAN classifier group configuration success table entry is shown in figure 13.

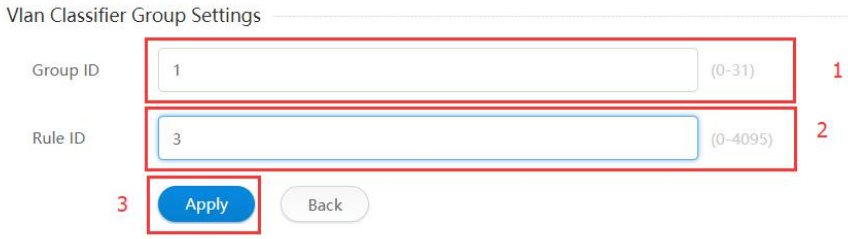


Figure 12 Add VLAN classifier group operation

Figure 13 New VLAN classifier group information

9.2.2 Delete VLAN Classifier Groups

If you want to delete a specified VLAN classifier group, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified VLAN classifier group.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button , it will delete this VLAN classifier group;

If you click "cancel" button, you will cancel delete this VLAN classifier group operation, as shown in figure 14.

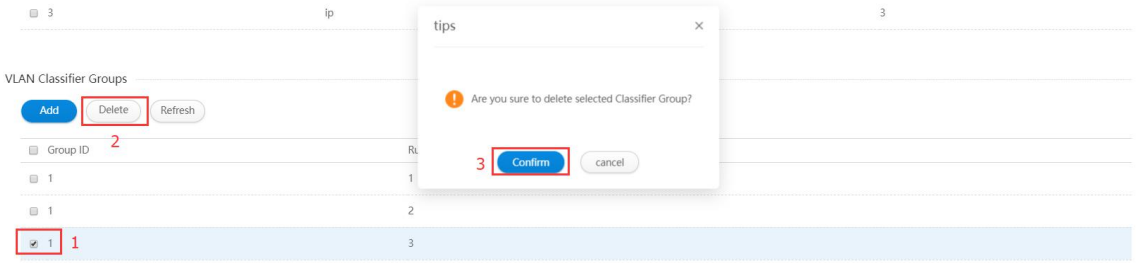


Figure 14 Delete VLAN classifier group operation

Delete a VLAN classifier group configuration success table entry is shown in figure 15.

Figure 15 Delete VLAN classifier group

9.3 VLAN Classifier Usage

If you click "Configuration -> VLAN Classifier", the VLAN classifier usage list appears, as shown in figure below.

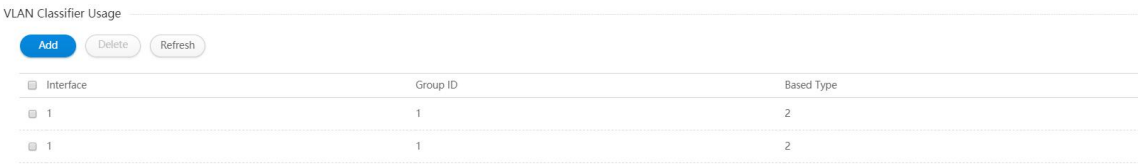


Figure 16 VLAN classifier usage list

9.3.1 Add VLAN Classifier Usage

If you click "Add" in the VLAN classifier usage list, you can add a VLAN classifier usage, the operation is shown in figure 17, then VLAN classifier usage settings page appears, as shown in figure 18.

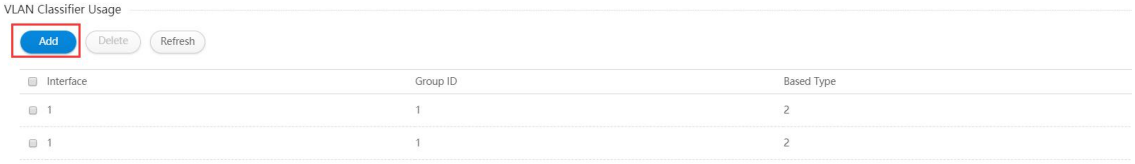


Figure 17 Add VLAN classifier usage operation

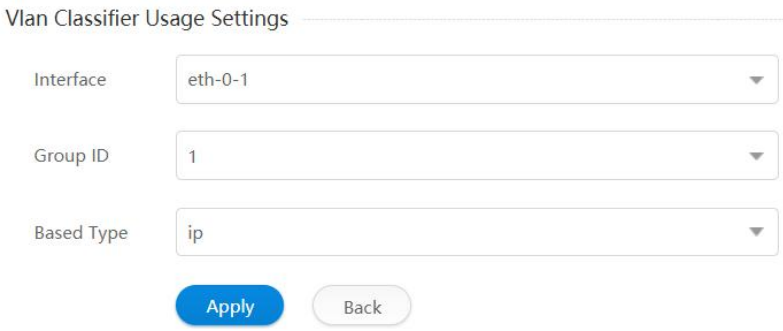


Figure 18 VLAN classifier usage settings list

- Parameter usage

Item	Description
Interface	Select an interface to apply VLAN classification
Group ID	Select a Group ID exist in the VLAN Classifier Groups list
Base Type	Choose what type of interface to base on, including IP mac and protocols

If you want to add a VLAN classifier usage, you can follow the following steps:

(1) Select port from the "Interface" drop-down box.

(2) Select a group ID from the drop-down box, the group ID has been created in the VLAN classifier groups list.

(3) Select IP /MAC/protocol from the "Based Type" drop-down box.

(4) Click the "Apply" button to add a VLAN classifier usage.

The operation is shown in figure 19, add a VLAN classifier usage configuration success table entry is shown in figure 20.

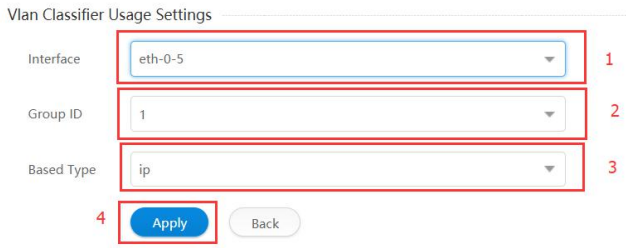


Figure 19 Add VLAN classifier usage operation

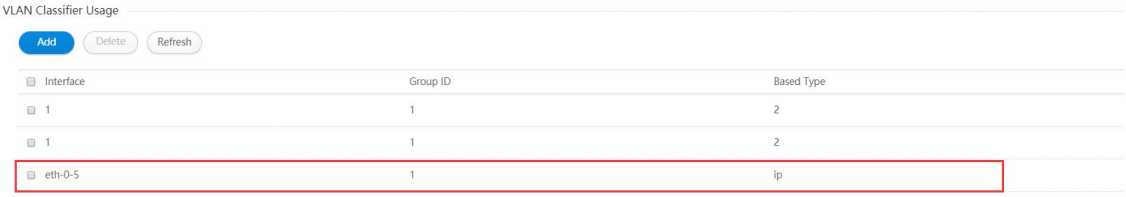


Figure 20 New VLAN classifier usage information

9.3.2 Delete VLAN Classifier Usage

If you want to delete a specified VLAN classifier usage, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified VLAN classifier usage.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button , it will delete this VLAN classifier usage;

If you click "cancel" button, you will cancel delete this VLAN classifier usage operation, as shown in figure 21.

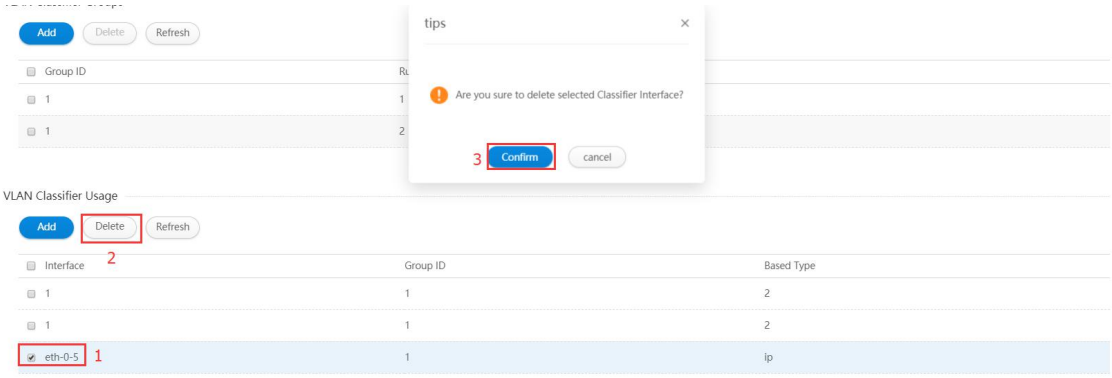


Figure 21 Delete VLAN classifier usage operation

Delete a VLAN classifier usage configuration success table entry is shown in figure 22.

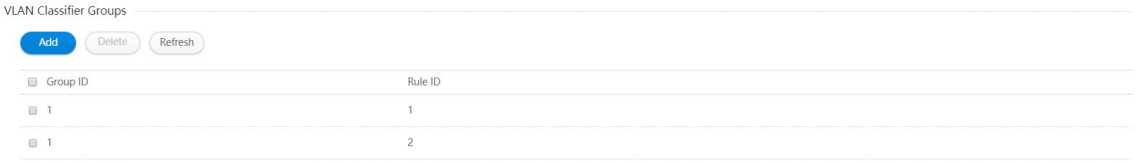


Figure 22 Delete VLAN classifier group

10. MAC

If you click “Configuration->MAC” in the top control bar, the MAC configuration list page appears, as shown in figure 1.

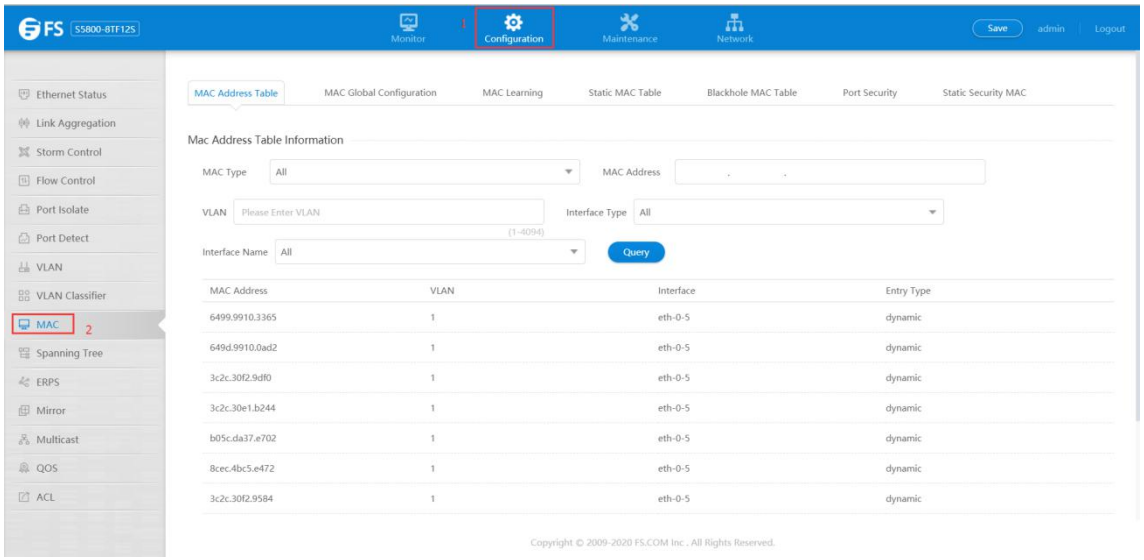


Figure 1 MAC configuration list

Ethernet switch uses information of MAC address list to address and forward the message quickly in link data layer, this article describes the configuring methods of MAC address.

10.1 MAC Address Table

MAC address table allows checking MAC address forwarding table of switch, if switch learns a MAC address and its relevant interface number, it will create an entry in forwarding table, these entries are used in forwarding packets. if the destination address of inbound traffic is in the database, the packets will be directly forwarded to related interface, or they will be forwarded to all interfaces.

If you click “Configuration > MAC > MAC Address Table” page to open the page as shown in following figure 2, which displays the address list information of switch.

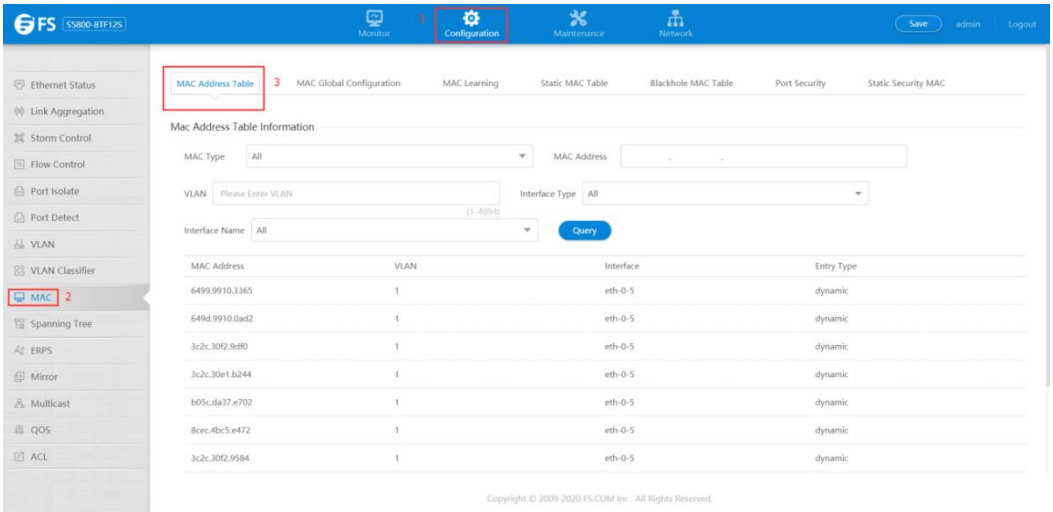


Figure 2 MAC address table page

- Parameter usage

Item	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address
Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC address, which includes Dynamic, Security or

If you want to view MAC address information for a MAC address table, you can follow the following steps:

(1) Select MAC address type in the "MAC type" drop-down box.

(2) Enter the MAC address to be queried in the "MAC address" text box.

(3) Enter the VLAN number to be queried in the "VLAN" text box.

(4) Select interface type in the "Interface type" drop-down box.

(5) Select interface name in the "Interface name" drop-down box.

(6) Click "Query" button, display the MAC address table information.

Figure 3 MAC address table information

10.2 MAC Aging Time

Use MAC aging time to set the remaining time of the learned MAC address in MAC address forwarding table, if exceeds this time, the switch will discard the MAC address forwarding records.

If you click "Configuration > MAC > MAC Global Configuration" page to view the configuration of MAC aging time, as shown in figure 4.

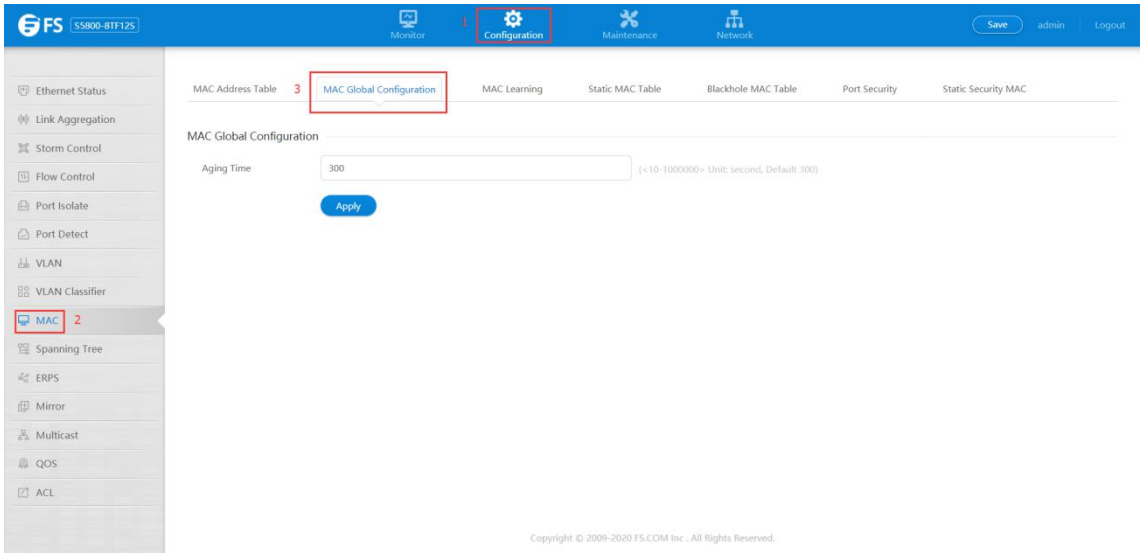


Figure 4 MAC aging time page

- Parameter usage

Item	Description
Aging Time	Enter MAC address aging time(Range:0, 10~1000000 seconds; default: 300 seconds)

If you want to configure MAC aging time, please enter the aging time for mac address in the "Aging time" text box, then click"Apply" button, the operation is shown in figure 5.

Figure 5 MAC aging time configuration

10.3 MAC Learning

If you click "Configuration -> MAC -> MAC Learning" to check each interface MAC learning on switch, the configuration page is shown as the figure 6.

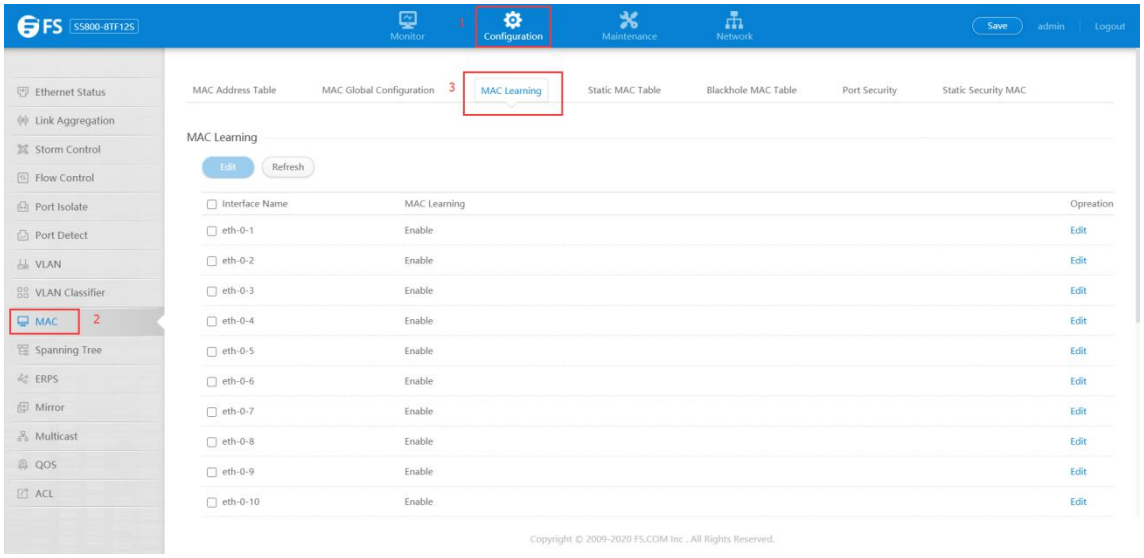


Figure 6 MAC learning page

- Parameter usage

Item	Description
Interface Name	Display the name of interface
MAC Learning	Display the current MAC learning status on interface
Operation	Display that MAC learning status can be edited

If you want to modify the MAC learning, you can follow the following steps:

(1) Click “Configuration -> MAC -> MAC Learning” to enter the basic information page.

(2) Choose one or more interface click “Edit” button to enter the interface attribute configuration page.

(3) Select “Enable/Disable” in the “MAC learning” radio box.

(4) After that, click “Apply” to apply all the changes made.

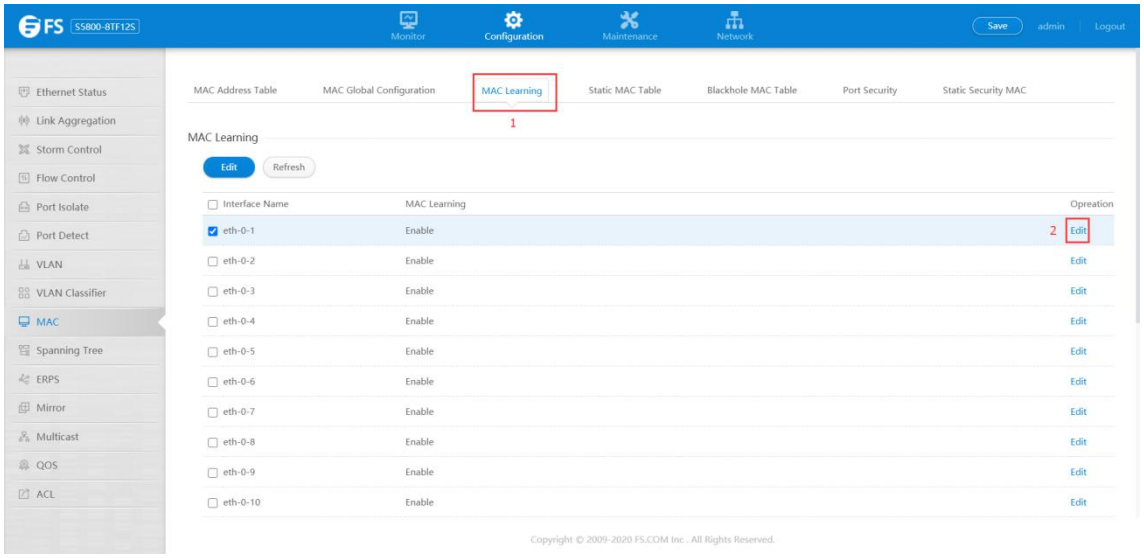


Figure 7 Interface MAC learning configuration

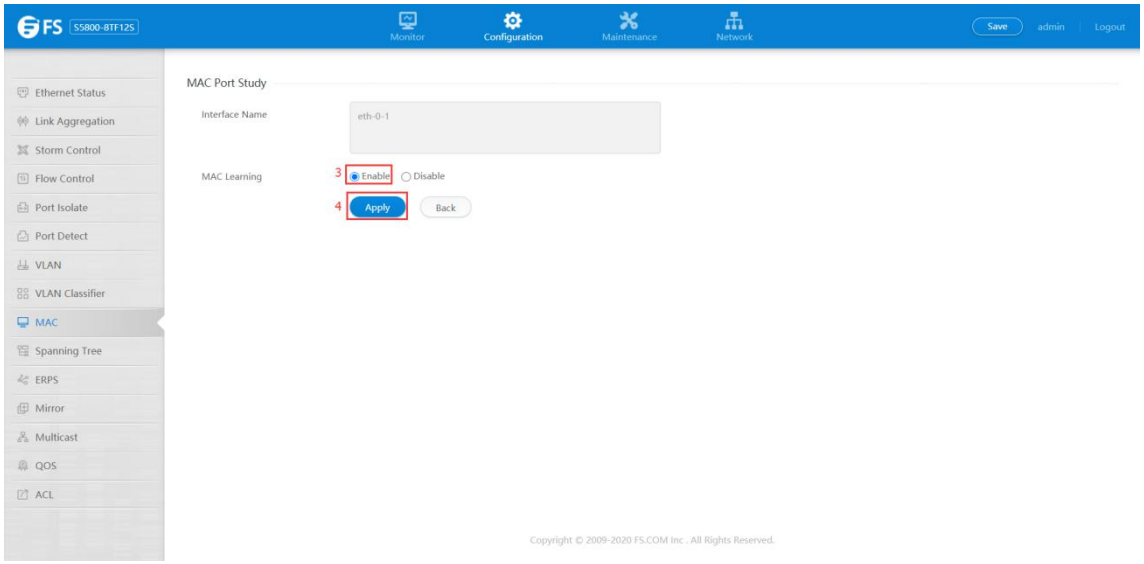


Figure 8 MAC learning configuration

10.4 Static MAC Table

After the MAC address is bound to the assigned interface, the crated static MAC table entry will not be aging in the address table, if the address is discovered by another interface, it will be neglected and not be written into address table, the address will not be learned by other interfaces unless the static address is deleted manually from address table.

If you click "Configuration > MAC > Static MAC Table" page to open the page as shown in following figure 9, which displays the information of static address table of switch.

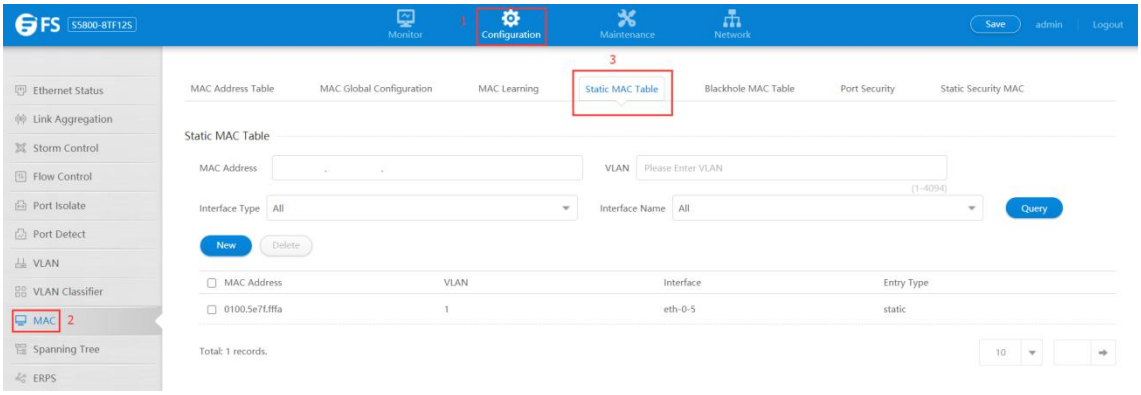


Figure 9 Static MAC table page

- Parameter usage

Item	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address
Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC Static address

If you want to add the static MAC address, you can follow the following steps:

(1) Click "New" button to add a static MAC address, the configuration page is shown as the figure 10.
(2) Enter the MAC address to be added in the "MAC address" text box.
(3) Enter the VLAN number to be added in the "VLAN" text box.
(4) Select interface type in the "Interface type" drop-down box.
(5) Select interface name in the "Interface name" drop-down box.
(6) After that, click "Apply" to apply all the changes made.

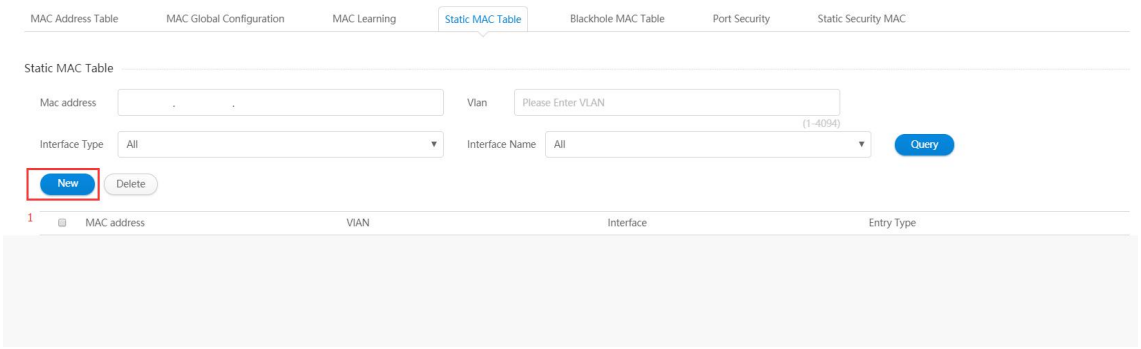


Figure 10 Add static MAC address

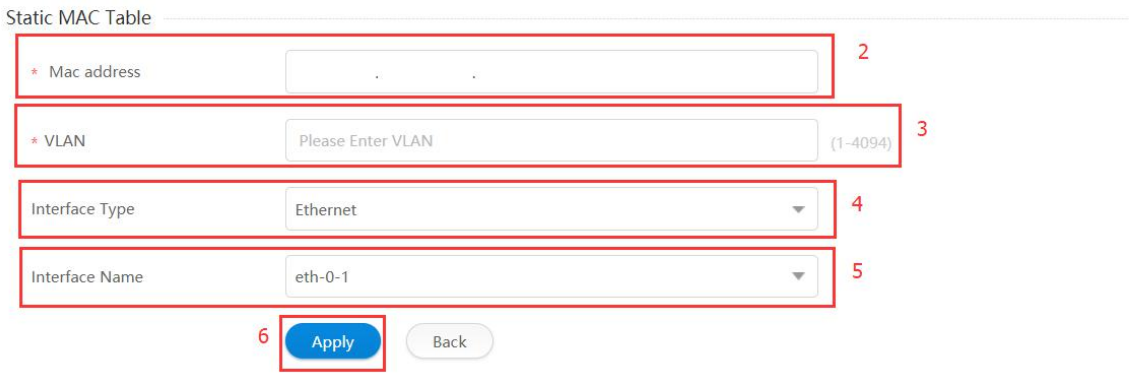


Figure 11 Static MAC address configuration

If you want to delete the static MAC address, you can follow the following steps:

(1) Click "Configuration -> MAC -> Static MAC Table" to enter the basic information page.
(2) Choose the check box in the left-hand column of static MAC to be deleted, then click "Delete" button to delete static MAC entry.
(3) It will appear tips page to note you to confirm the operation, if you click "Apply" button, it will delete the configuration for static MAC address table; if you click "cancel" button, you will cancel the delete configuration operation.

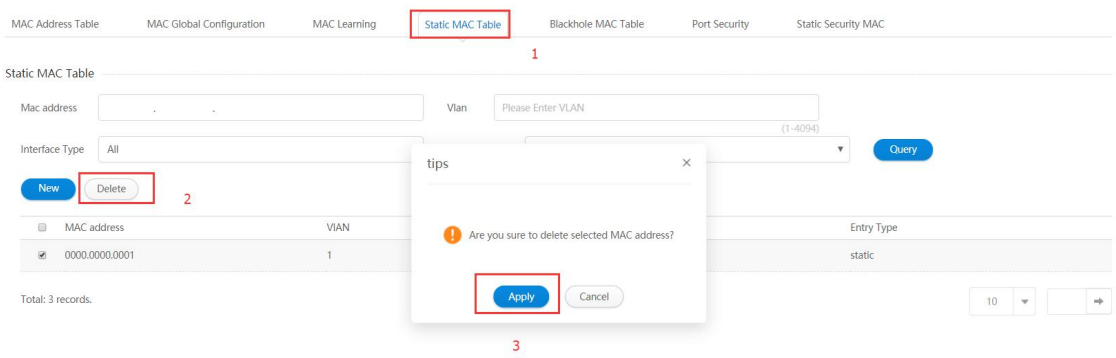


Figure 12 Delete static MAC address

10.5 Blackhole MAC Table

If you click “Configuration > MAC > Blackhole MAC Table” page to open the page as shown in following figure 13, which displays the information of blackhole address table on switch.

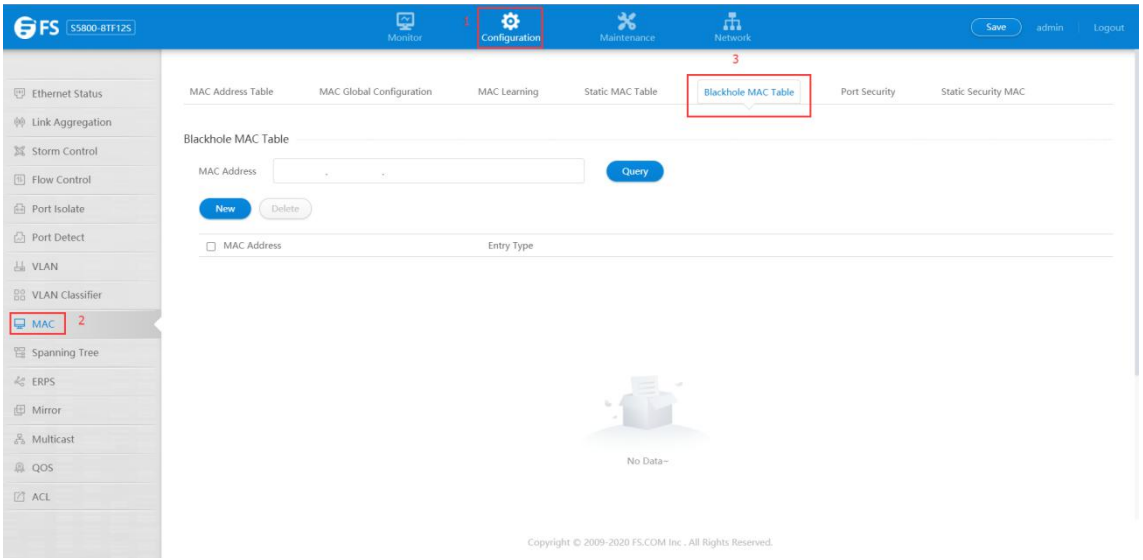


Figure 13 Blackhole MAC table page

- Parameter usage

Item	Description
MAC Address	The Blackhole MAC addresses in the address table
Entry Type	The methods that switch discovers MAC Static address

If you want to add a blackhole MAC adress, you can follow the following steps:

(1) Click “New” button to add a blackhole MAC address, the configuration page is as shown in following figure 14.

(2) Enter the blackhole MAC address information to be added in configuration page.

(3) After that, click “Apply” to apply all the changes made.

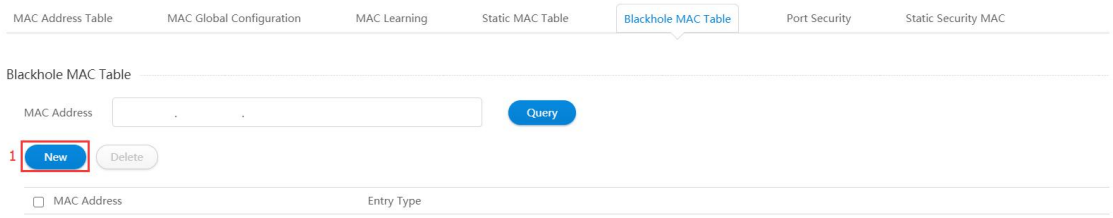


Figure 14 Add blackhole MAC address

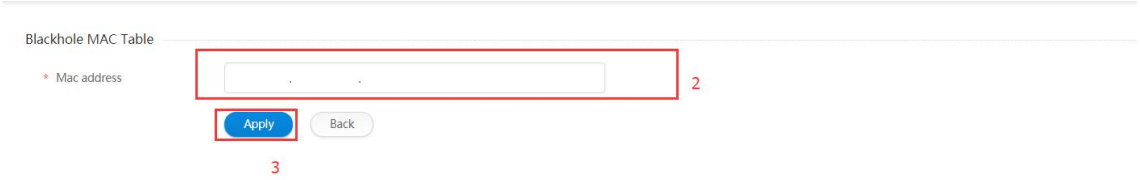


Figure 15 Blackhole MAC address configuration

If you want to delete the blackhole MAC address, you can follow the following steps:

(1) Click "Configuration -> MAC -> Blackhole MAC Table" to enter the basic information page.

(2) Choose the check box in the left-hand column of blackhole MAC to be deleted, then click "Delete" button to delete blackhole MAC entry.

(3) It will appear tips page to note you to confirm the operation, if you click "Apply" button, it will delete the configuration for blackhole MAC address table; if you click "cancel" button, you will cancel the delete configuration operation.

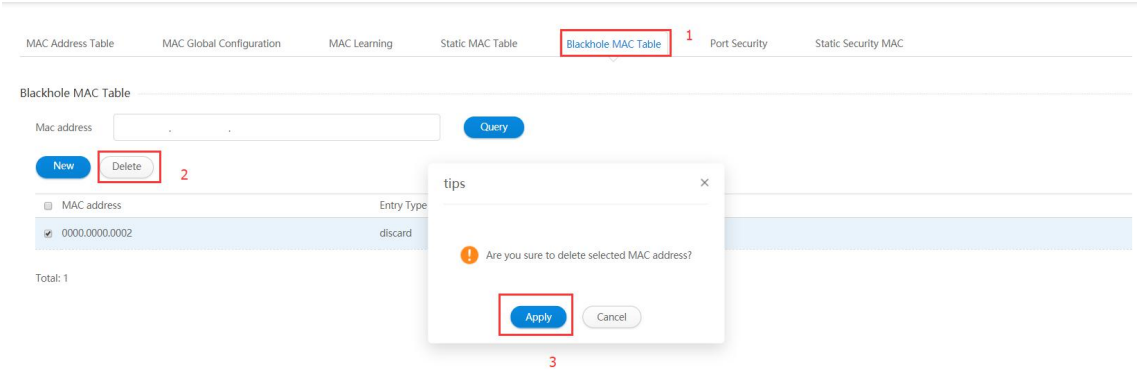


Figure 16 Delete blackhole MAC address

10.6 Port Security

If you click "Service Management -> MAC -> Port Security" to check each interface port security on switch, the configuration page is shown as the figure below 17.

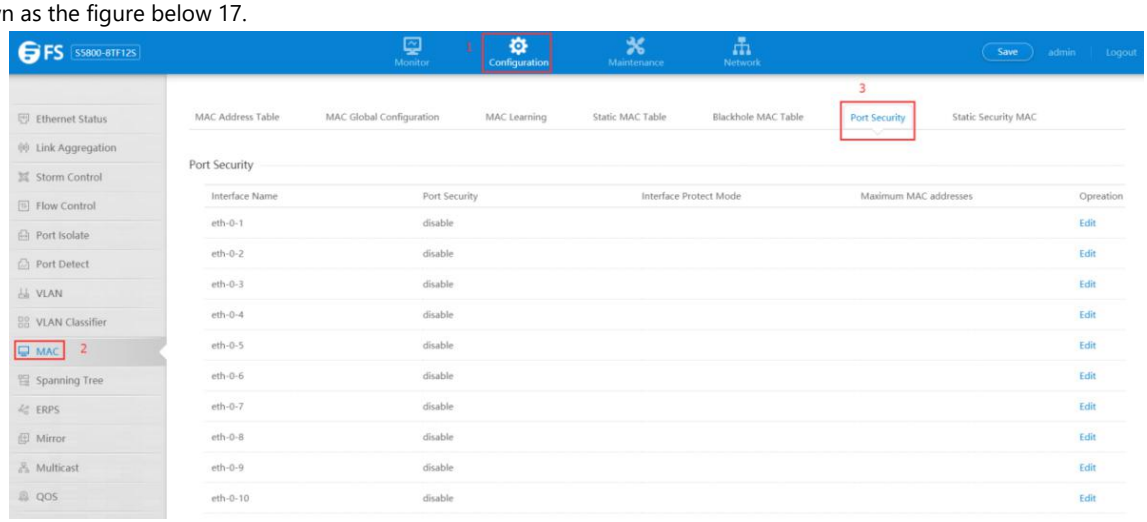


Figure 17 Port security page

- Parameter usage

Item	Description
Interface Name	Display the name of interface
Port Security	Display the current port security status on interface
Interface Protect Mode	Display the current protect mode on interface
Maximum MAC addresses	Display the maximum MAC addresses number on interface
Operation	Display that port security status can be edited

If you want to modify the port security, you can follow the following steps:

(1) Click "Configuration -> MAC -> Port Security" to enter the basic information page.

(2) Choose one interface click "Edit" button to enter the interface attribute configuration page, shown as the figure 18.

(3) Select "Disable/Enable" in the "Port security" radio box.

(4) Select "Protect/Restrict/Shutdown" in the "Interface protect mode" radio box.

(5) Enter max MAC learn in the "Max MAC entries learned" text box.

(6) After that, click "Apply" to apply all the changes made.

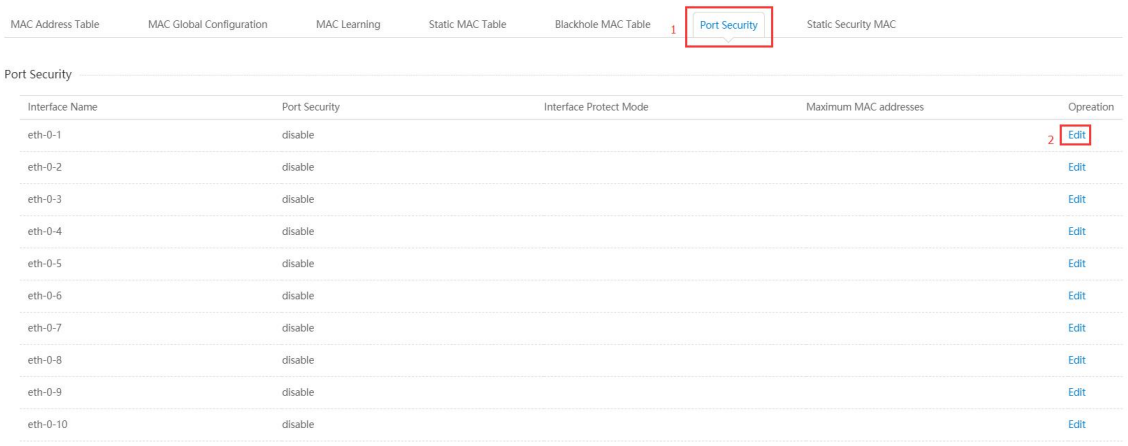


Figure 18 Port security information

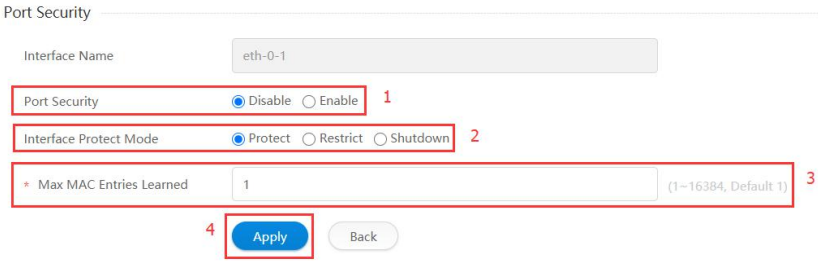


Figure 19 Port security configuration

10.7 Static Security MAC

Static security MAC table lists the information of the static security MAC address among the switch interfaces.

If you click “Configuration > MAC > static security MAC” page to open the page as shown in following figure 20, which displays the information of static security address table of switch.

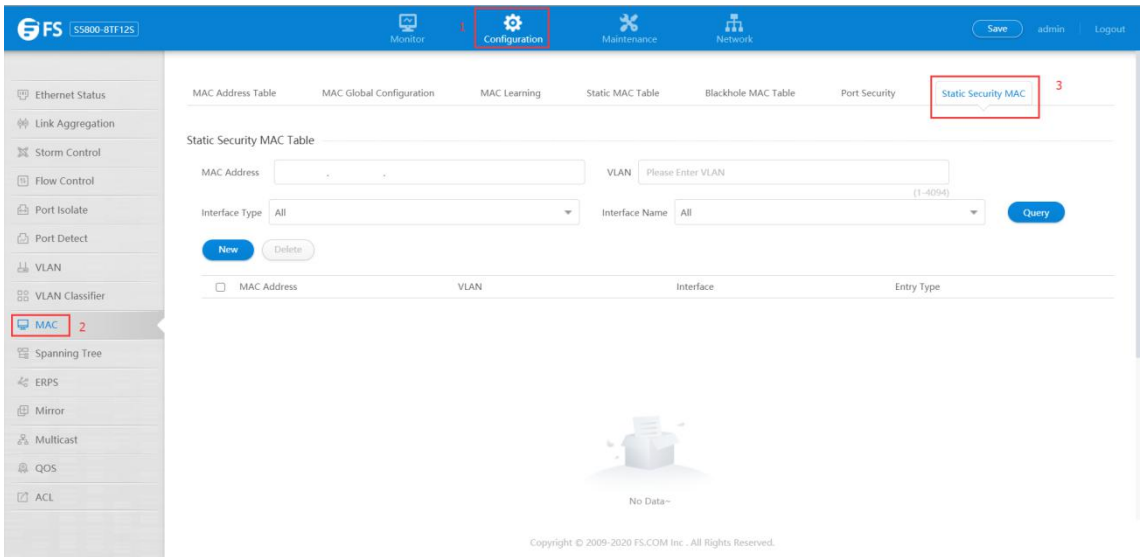


Figure 20 Static security MAC page

- Parameter usage

Item	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address
Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC Static address

If you want to add the static security MAC address, you can follow the following steps:

(1) Click "New" button to add a static MAC address, the configuration page is shown as the figure 21.

(2) Enter the MAC address to be added in the "MAC address" text box.

(3) Enter the VLAN number to be added in the "VLAN" text box.

(4) Select interface type in the "Interface type" drop-down box.

(5) Select interface name in the "Interface name" drop-down box.

(6) After that, click "Apply" to apply all the changes made.

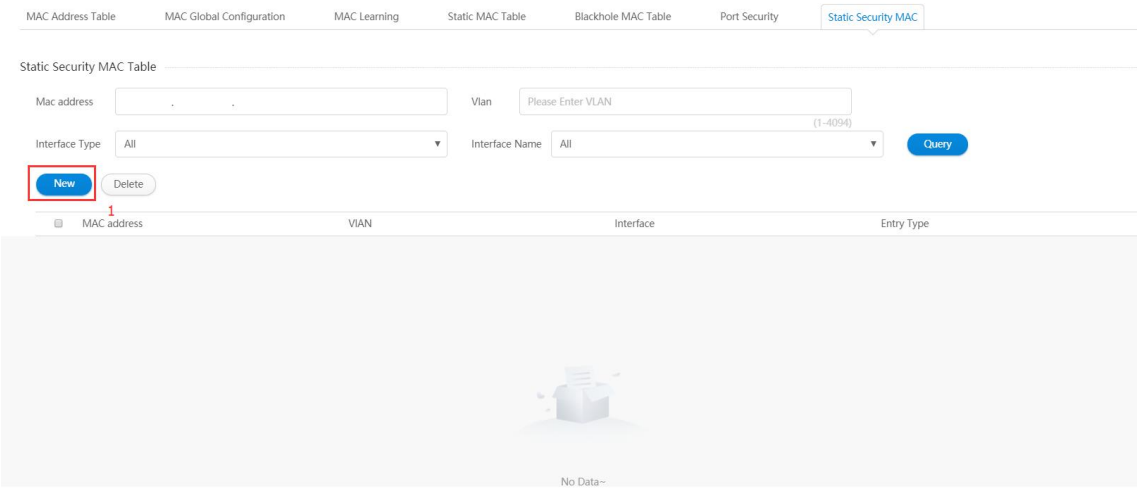


Figure 21 Add static security MAC address

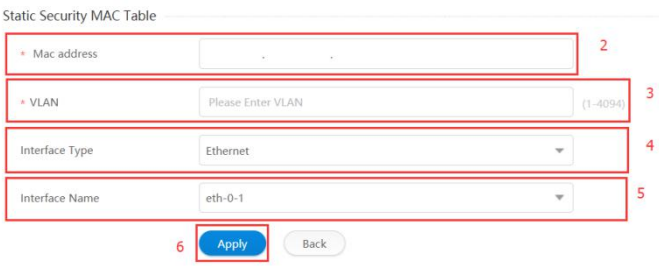


Figure 22 Static security MAC address configuration

If you want to delete the static security MAC address, you can follow the following steps:

(1) Click "Configuration -> MAC -> Static Security MAC Table" to enter the basic information page.

(2) Choose the check box in the left-hand column of static MAC to be deleted, then click “Delete” button to delete static MAC entry.

(3) It will appear tips page to note you to confirm the operation, if you click “Apply” button, it will delete the configuration for static security MAC address table; if you click “cancel” button, you will cancel the delete configuration operation.

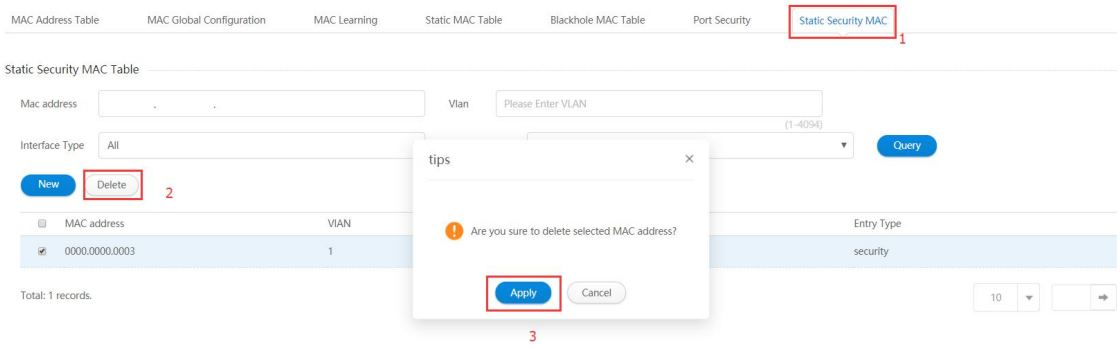


Figure 23 Delete static security MAC address

11. Spanning Tree

Spanning Tree Protocol (STP) is used to decrease link failure in network and provides protection for network by preventing loop circuit. It is easy to generate unconscious loop broadcast storm in complex network construction. It is disabled by default. To enable this function, you must enable STP/RSTP/MSTP function on each switch connected to network. The switch supports three versions of Spanning Tree Protocol: STP, RSTP and MSTP.

If you click "Configuration -> Spanning Tree" the top control bar, the STP configuration page appears, as shown in figure 1.

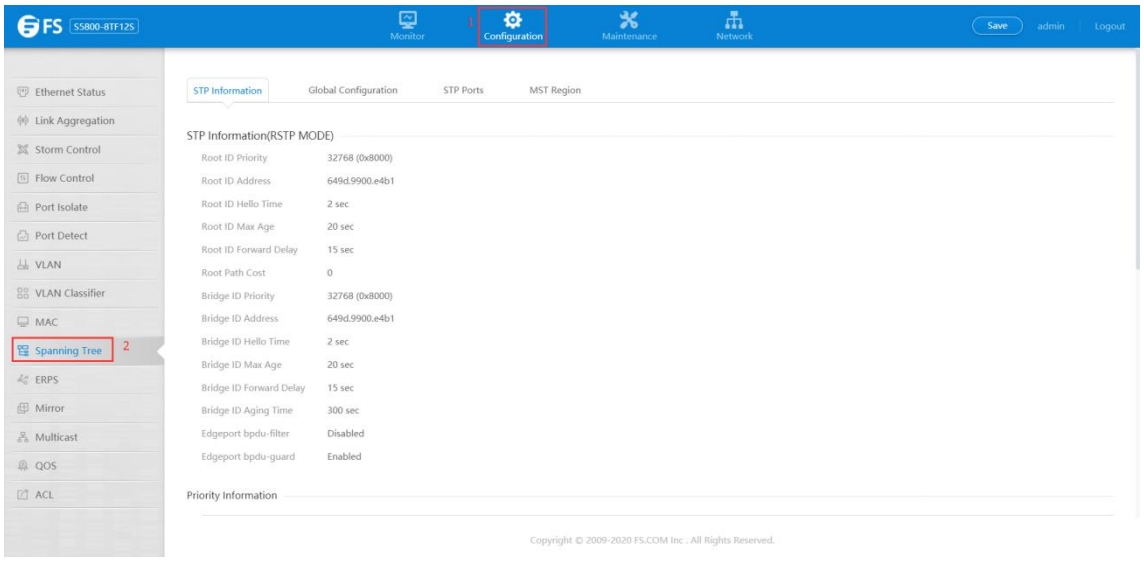


Figure 1 STP information

11.1 STP Information

If you click "Spanning Tree -> STP Information" the top control bar, the STP Information page appears, as shown in figure 2, Priority information is shown in figure 3, and ports information is shown in figure 4.

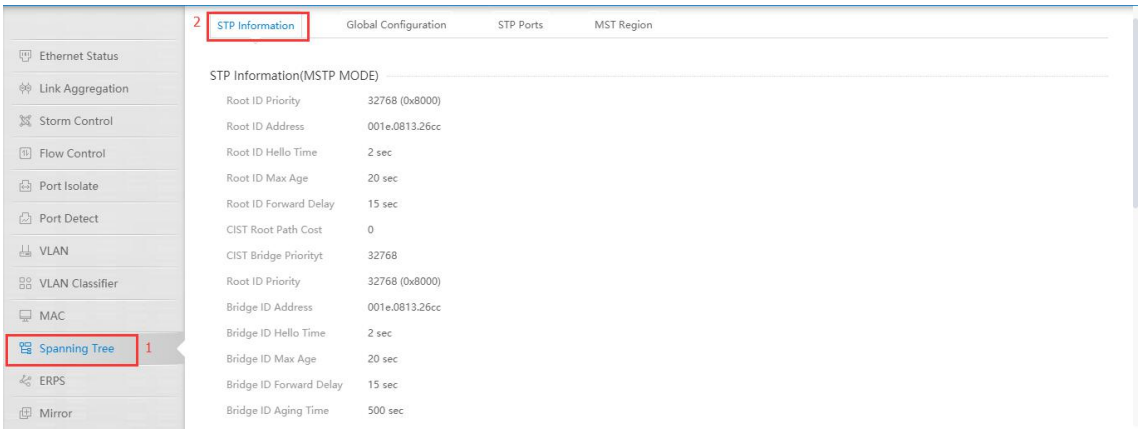


Figure 2 Global information

- Parameter usage

Item	Description
Root ID Priority	Display the priority of the switch which is selected as root
Root ID Address	Display the address of the switch which is selected as root
Root ID Hello Time	Display the hello time interval of the switch which is selected as root
Root ID Max Age	Display the max age of the switch which is selected as root
Root ID Forward Delay	Display the root id forward delay of the switch which is selected as root
CIST Root Path Cost	Display the CIST Root Path Cost
CIST Bridge Priority	Display the CIST Bridge Priority
Bridge ID Priority	Display the bridge ID priority of the switch
Bridge ID Address	Display the bridge ID address of the switch
Bridge ID Hello Time	Display the hello time interval of the switch
Bridge ID Max Age	Display the max age interval of the switch
Bridge ID Forward Delay	Display the forward delay of the switch
Bridge ID Aging Time	Display the of aging time the switch
Edgeport bpdu-filter	Display the enable status of edgeport bpdu-filter
Edgeport bpdu-guard	Display the enable status of edgeport bpdu-guard

Figure 3 Priority information

- Parameter usage

Item	Description
Instance	Display the Instance Id
Path Cost	Display the path cost of the instance
Priority	Display the priority of the instance

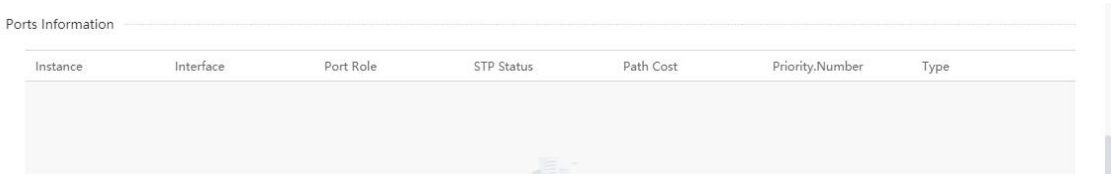


Figure 4 Ports information

- Parameter usage

Item	Description
Instance	Instance number
Interface	Interface number for instance operation
Port Role	Interface status
STP Status	Display this interface's status on the spanning tree
Path Cost	The port's internal path cost in this instance
Priority.Number	The port's internal priority in this instance and port number
Type	Link type

11.2 STP Global

If you click “Spanning Tree -> Global Configuration” in the title bar, the global configuration page appears, as shown in figure 5.

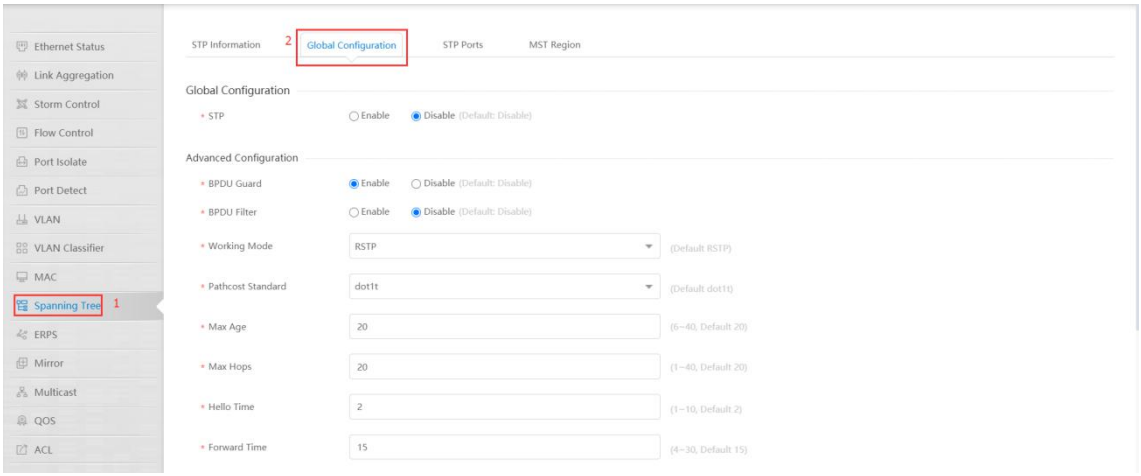


Figure 5 STP global settings

- Parameter usage

Item	Description
STP	Enable or disable STP on this switch(default: disable)
Nexthop	Set specify nexthop IP address
BPDU Guard	Enable or disable bpdu guard in global
BPDU Filter	Enable or disable bpdu filter in global
Working Mode	Specify types of spanning tree adopted on this switch STP: select this parameter to set global spanning tree protocol on switch (STP) RSTP: select this parameter to set global rapid spanning tree protocol on switch (RSTP) MSTP: select this parameter to set global multiple spanning tree protocol on switch (MSTP)

Item	Description
Pathcost Standard	Choose the standard of path cost calculation. The options are as follow: dot1t, dot1d-1998
Max Age	Max-age ensures that the old information will not be endlessly circled within the network's redundant path, and thus stop the valid transmission of the new information. The value is set by the root bridge to confirm that the spanning tree configuration value of the switch accords with the other devices on the bridge LAN. If the value is timeout, while the switch has not received the BPDU packet from root bridge, the switch starts to send its BPDU to all the other switches to ask for becoming the root bridge. If the switch has the minimal bridge identifier, it will become root bridge. User can set the value from 6-40seconds, the default is 20 seconds
Max Hops	Set the device hops among the devices within spanning tree regions before the BPDU packets are discarded by the switch. The number of hop will be reduced one when each packet passes through the switch until the hop count to zero. At this point, the switch will discard the BPDU packet, and interface information in packet will be time-out. Value ranges from 6 to 40, default is 20
Hello Time	Interval for root bridge's broadcast “hello” message.“hello” message is used to detect whether the network topology is normal or not
Forward Time	The setting range is 4-30 seconds (default: 15sec). Each interface on the switch needs to wait double of forward-delay time when the blocked status changes to forwarding status
Instance	Select instance number for the root types needed to configure.
Priority	Bridge priority is used in selecting the root device. The device with the highest priority (the smaller value the higher priority) becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device (note that lower numeric values indicate higher priority) .Default value: 32768; Range: 0~61440; Step Length: 4096

If you want to configure STP global configuration, you can perform the following steps:

(1) Select the configuration items that need to be modified according to the actual needs. The configuration items that do not need to be modified can keep the default value.

(2) Select MSTP in the working mode drop-down box.

(3) After selecting the configuration, you can click "Apply" to complete the configuration.

(4) You can view the configuration in STP information on STP information page.

The operation is shown in figure 6.

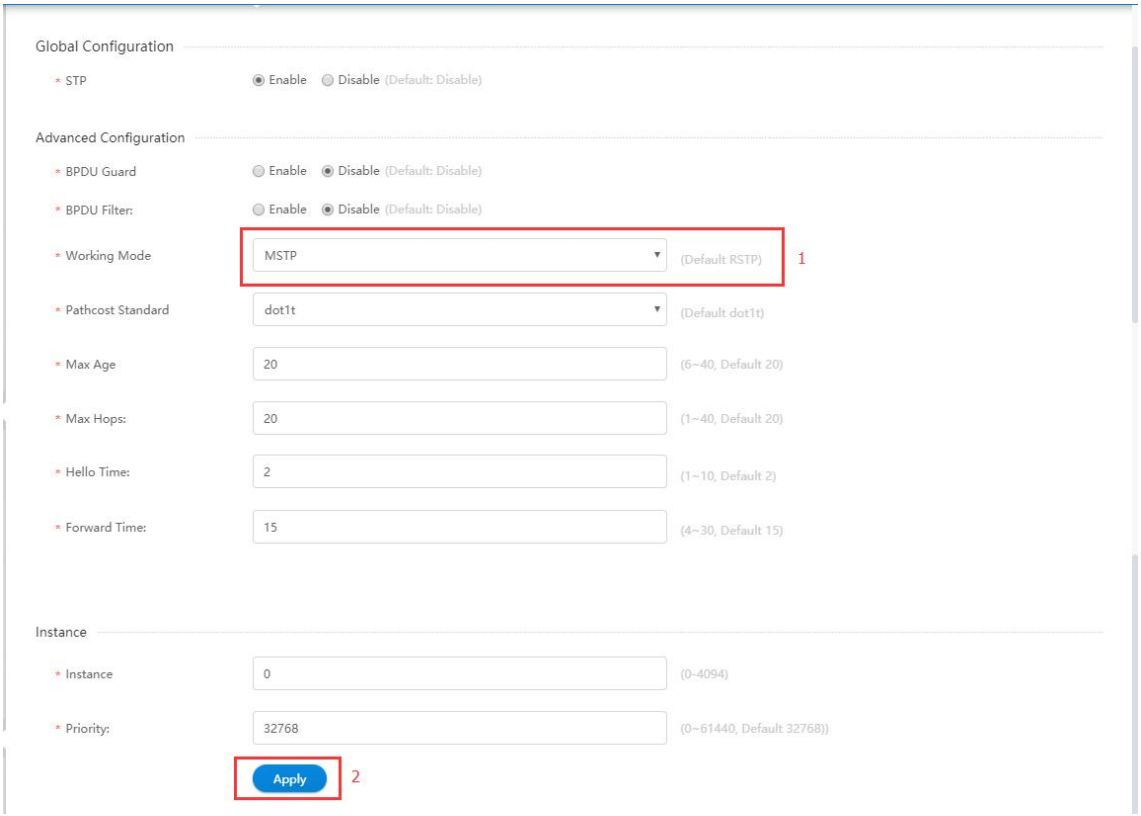


Figure 6 Add STP global configuration

11.3 STP Interface

You can configure properties for a specific interface, including port priority, path cost, protection type, and edge port. For ports of the same media type, different priorities or path overhead can be used to indicate the preferred path. Different link types indicate point-to-point connection or shared media connection, while different edge ports indicate that connected devices can support fast forwarding.

If you click “Spanning Tree -> STP Ports” in the title bar, the STP interface page appears, as shown in figure 7.

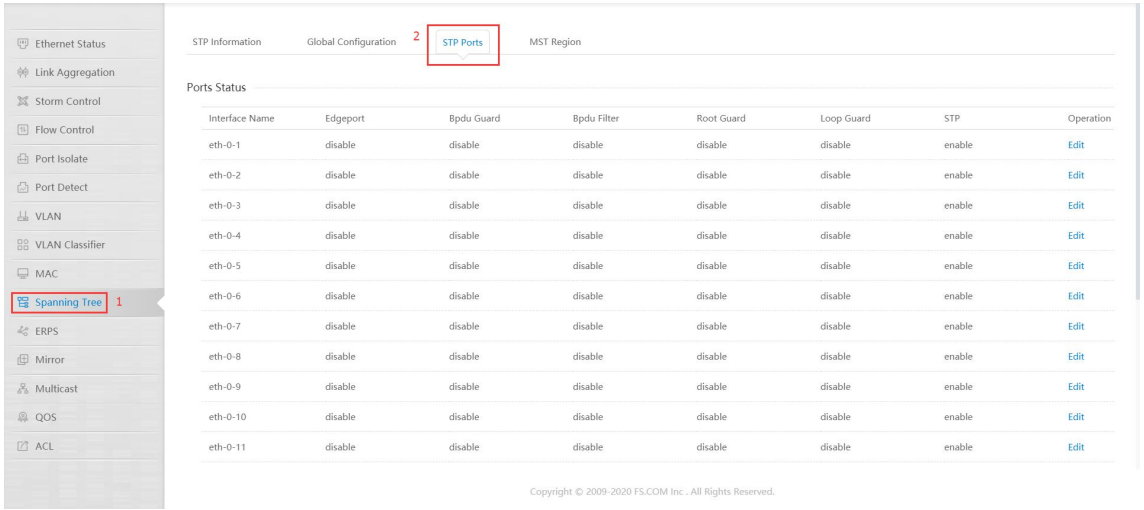


Figure 7 STP interface

- Parameter usage

Item	Description
Interface Name	Interface name
Edgeport	Display this port is enabled edgeport or not
Bpdu Guard	Display this port is enabled bpdu guard or not
Bpdu Filter	Display this port is enabled bpdu filter or not
Root Guard	Display this port is enabled root guard or not
Loop Guard	Display this port is enabled loop guard or not
STP	Display this port is enabled STP or not

If you want to edit the parameters of STP interface "eth-0-1", you can perform the following steps:
Click "Edit" corresponding to "eth-0-1" in the interface list, as shown in figure 8, and the configuration page is shown in figure 9.

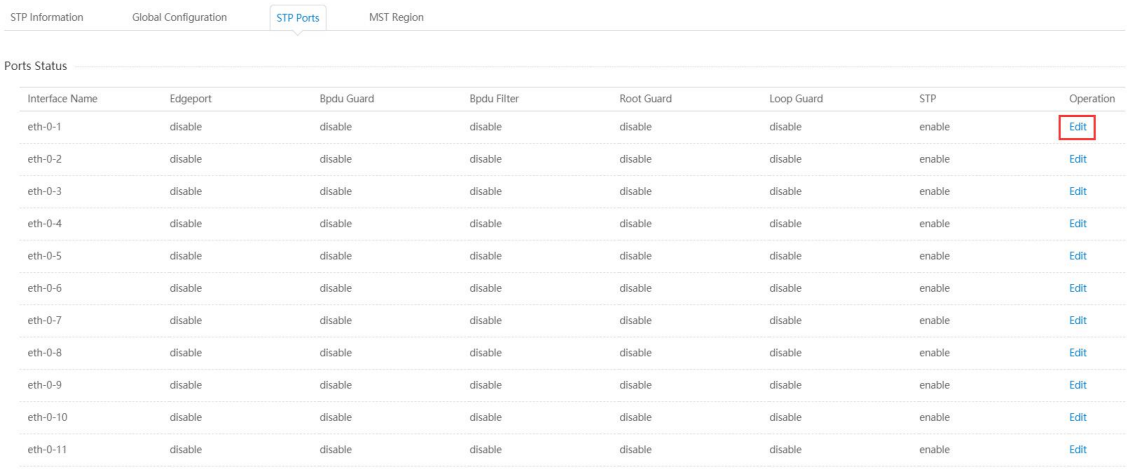


Figure 8 STP Settings based on interface operation

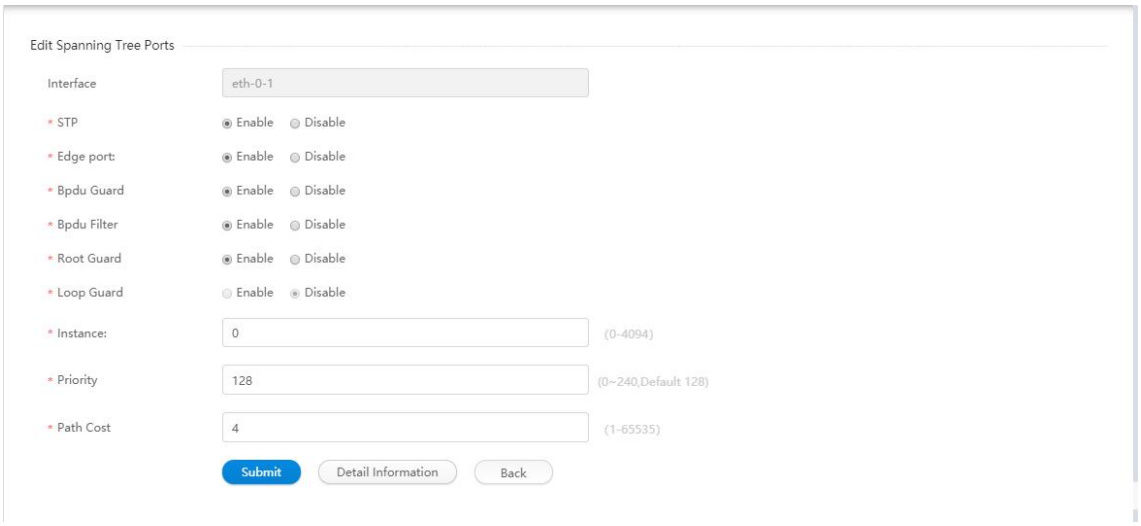


Figure 9 STP settings based on interface

- Parameter usage

Item	Description
Interface	Current configuration interface
STP	Enable or disable STP on port
Edgeport	Set a port as an edgeport and to enable rapid transitions
Bpdu Guard	Enable or disable the BPDU Guard feature on a port
Bpdu Filter	Enable or disable the BPDU Guard Filter on a port
Root Guard	Enable or disable the Root Guard on a port
Loop Guard	Enable or disable the Loop Guard on a port
Instance	Instance id you want to add this port to.
Priority	The port internal priority in this instance
Path Cost	The port internal path cost in this instance

If you want to configure the STP interface, you can perform the following steps:

(1) Select the configuration items that need to be modified according to the actual needs. The configuration items that do not need to be modified can keep the default value.

(2) Use the radio buttons to select "STP", "Edge port" & "Bpdu Guard" as enabled.

(3) Click "Submit" button to apply all the changes made.

The operation is shown in figure 10.

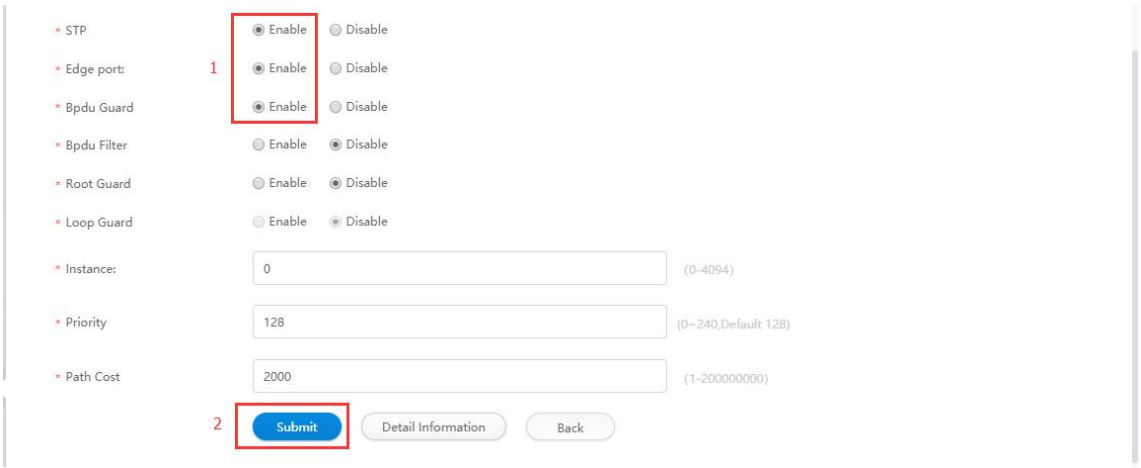


Figure 10 Parameters of editing STP interface

If you want to view the STP interface "eth-0-1" information, you can perform the following steps:

(1) You can click the "Detailed Information" button directly on the page of editing STP interface "eth-0-1",the specified interface detail STP configuration information is shown as the figure below.

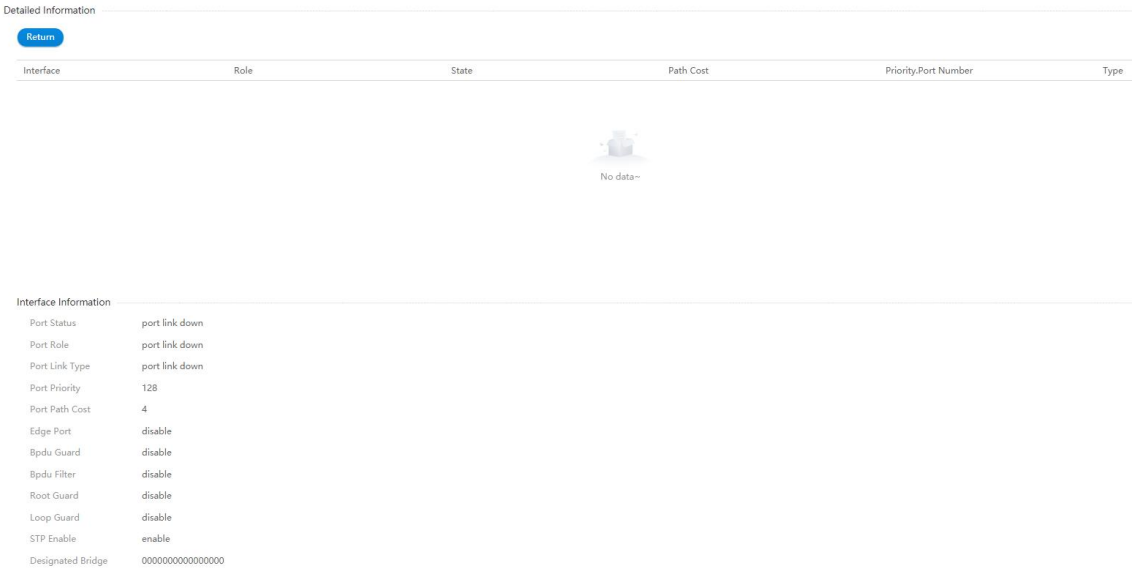


Figure 11 Display STP Interface Details

- Parameter usage

Item	Description
Interface	Instance number
Role	Interface status
State	Display this interface's status on the spanning tree: Discarding: port receives STP configuration messages, but does not forward packets Learning: port does not forward packets, and starts to learn MAC address Forwarding: port forwards packets, and continues learning addresses
Path Cost	This interface's internal path cost
Priority.Number	This interface's internal priority and port number
Type	Link type, point-to-point or shared

- Parameter usage

Item	Description
Port Status	Port status in instance
Port Role	Port role in instance
Port Link Type	Port Link Type in instance
Port Priority	Port internal priority in instance
Port Path Cost	Port internal path cost in instance
Edgeport	Port in instance is enabled edgeport or not
Bpdu Guard	Port in instance is enabled bpdu guard or not
Bpdu Filter	Port in instance is enabled bpdu filter or not

Item	Description
Root Guard	Port in instance is enabled root guard or not
Loop Guard	Port in instance is enabled loop guard or not
STP Enable	Port in instance is enabled stp or not
Designated Bridge	Port's designated bridge in instance

11.4 MST Region

If you click "Spanning Tree -> MST Region" in the title bar, The MST region page appears, as shown in figure 12.

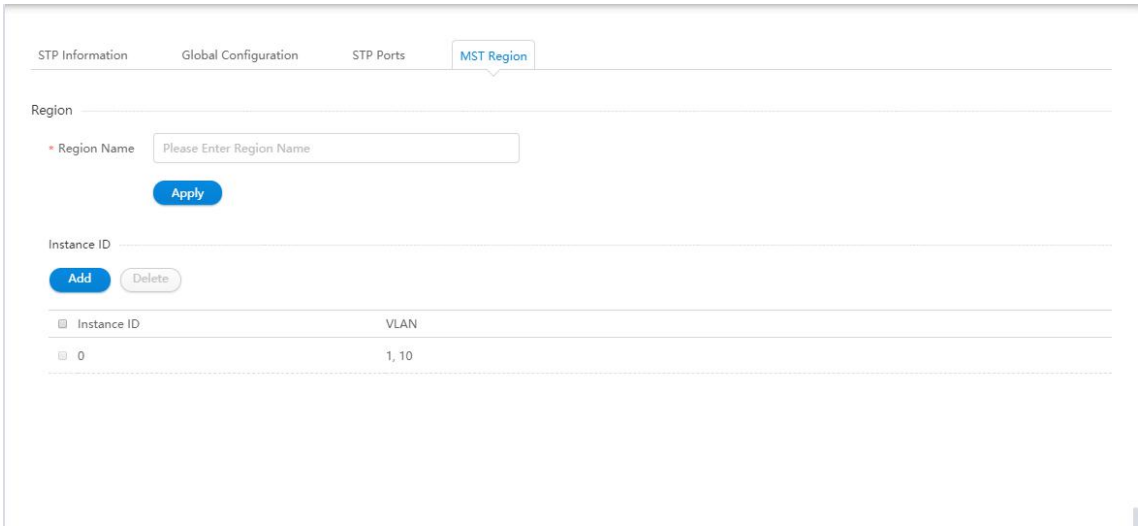


Figure 12 STP Region Information

- Parameter usage

Item	Description
Region Name	Specify MST domain name joined by the switch
Instance ID	Display the MST instance ID currently configured on switch.
VLAN	Display VLAN ID mapped to specified MST instance

If you want to add MSTP instance:, you can perform the following steps:
If you click "Add" , you can add MSTP instance, as shown in figure 13, and then the MSTP instance configuration page appears, as shown in figure 14.

Figure 13 Add CIST operation

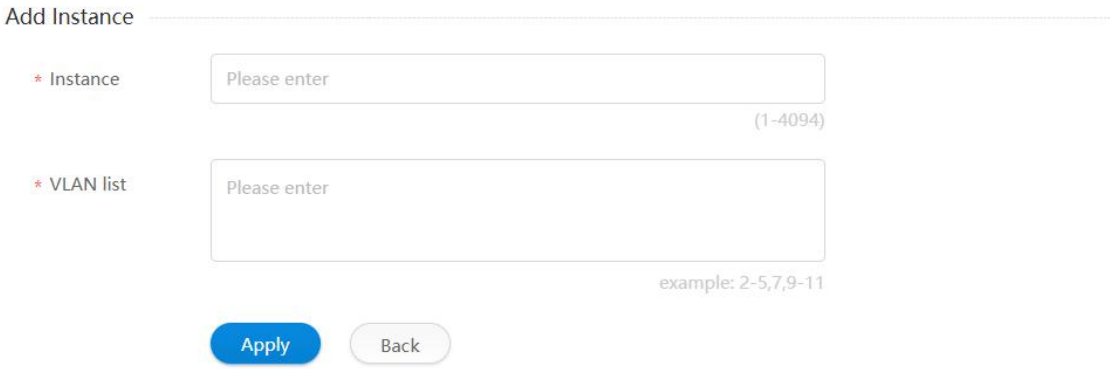


Figure 14 Add CIST

If you want to add CIST, you can perform the following steps:

(1) Select the instance number needed to & in Instance bar, fill in VLAN list.

(2) Click "Apply" button to apply all the changes made.

The operation is shown in figure 15, and the entry of CIST configuration success table is shown in figure 16.

Figure 15 Add CIST configuration

Figure 16 New CIST information

12. ERPS

If you click "Configuration->ERPS" in the top control bar, the ERPS configuration list page appears, as shown in figure 1.

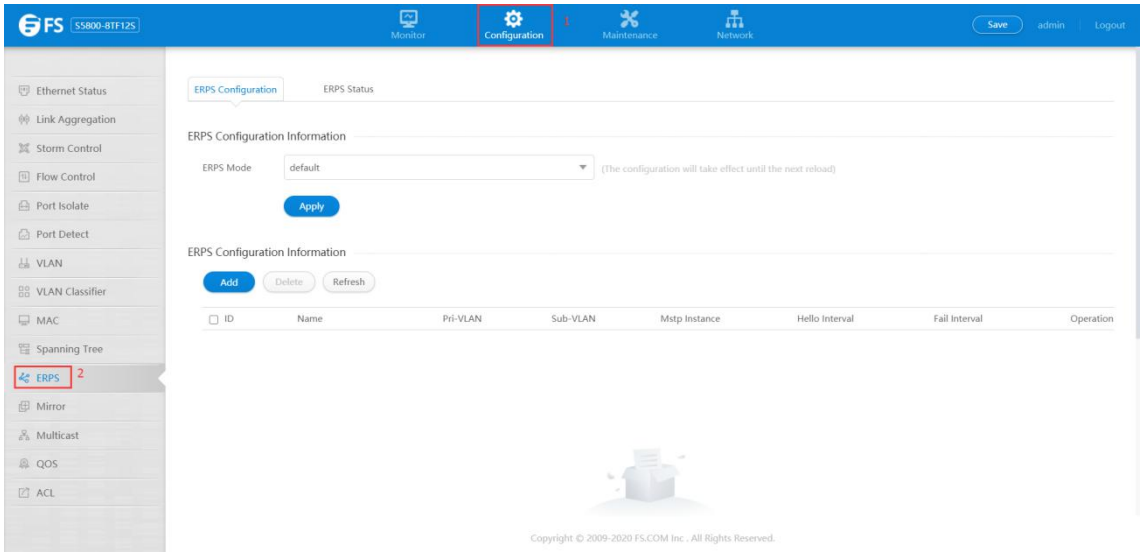


Figure 1 ERPS configuration list

In network planning and practical networking applications, ring network is mostly used to provide high reliability. ERPS technology can improve the availability and durability of Ethernet rings and converge within 50ms of link interruption. This chapter describes the configuration of ERPS.

12.1 ERPS Configuration

With the ERPS configuration feature, you can select the working mode of ERPS, add/remove/modify ERPS domain, and add/remove/modify ERPS ring.

12.1.1 Configure ERPS Mode

If you click "ERPS -> ERPS Configuration" in the title bar, the ERPS mode configuration information page appears, as shown in figure 2, and the ERPS domain configuration information page appears, as shown in figure 4.

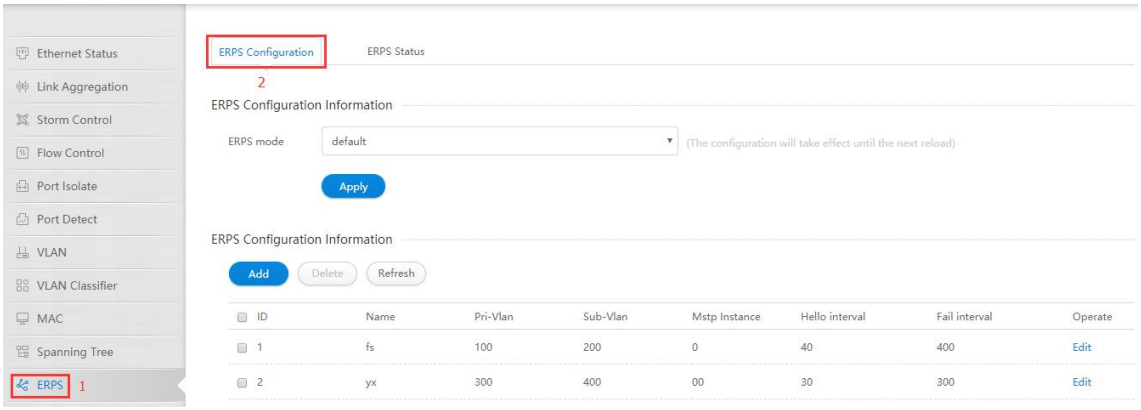


Figure 2 ERPS mode configuration information

- Parameter usage

Item	Description
ERPS mode	Display the working mode of ERPS, which supports RRPP protocol compatibility

If you want to modify the working mode of ERPS, please select the working mode from the "ERPS mode" dropdown box, and then click the "Apply" button, the operation is shown in figure 3.

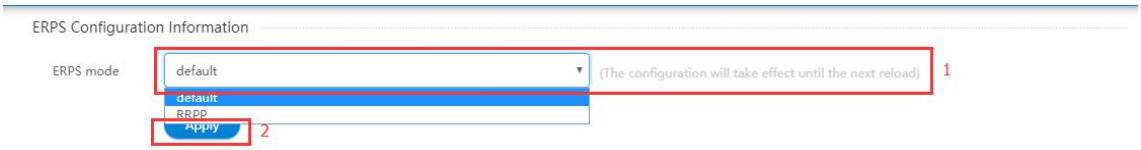


Figure 3 Select the working mode of ERPS

12.1.2 Add the ERPS Domain

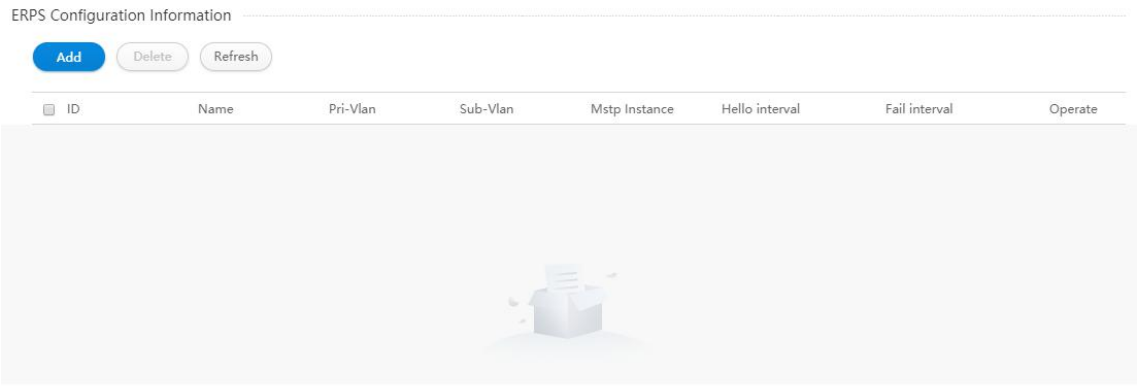


Figure 4 ERPS domain configuration information

- Parameter usage

Item	Description
ID	Display the ERPS domain ID
Name	Display the ERPS domain name
Pri-Vlan	Display the primary control VLAN for ERPS
Sub-Vlan	Display a sub control VLAN for ERPS
Mstp Instance	Display an MSTP instance
Hello interval	Display the Hello message delivery period
Fail interval	Display the Fail message delivery period
Operate	Display that ERPS domain table entries can be edited

If you click "Add" button, you can add an ERPS domain, the operation is shown in figure 5, and then the ERPS domain configuration page appears, as shown in figure 6.

Figure 5 Add ERPS domain operation

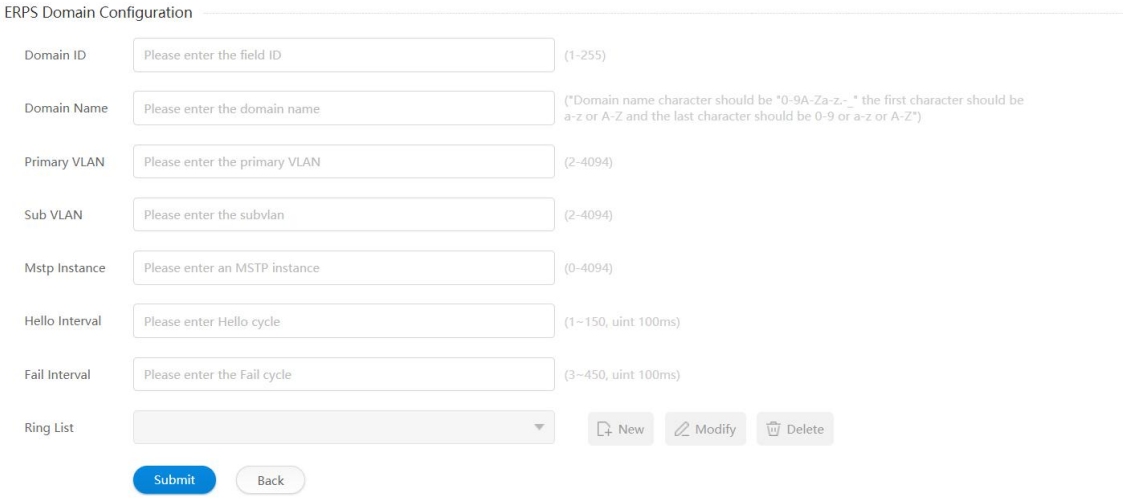


Figure 6 Add ERPS domain

- Parameter usage

Item	Description
ID	Set the ERPS domain ID
Name	Set the ERPS domain name
Pri-Vlan	Set the primary control VLAN for ERPS
Sub-Vlan	Set a sub control VLAN for ERPS
Mstp Instance	Set an MSTP instance
Hello interval	Set the Hello message delivery period
Fail interval	Set the Fail message delivery period
Ring List	Display ERPS ring list information

If you want to add an ERPS domain, you can follow the following steps:

(1) Enter an ERPS domain ID in the “ID” textbox.

(2) Enter an ERPS domain name in the “Name” textbox.

(3) Enter an ERPS primary control VLAN in the “Pri-Vlan” textbox.

(4) Enter an ERPS sub control VLAN in the “Sub-Vlan” textbox.

(5) Enter an MSTP instance in the “Mstp Instance” textbox.

(6) Enter the Hello message delivery period in the “Hello interval” textbox, but the parameters are optional, and if not configured, the default value is 1 second.

(7) Enter the Fail message delivery period in the “Fail interval” textbox, but the parameters are optional, and if not configured, the default value is 3 second.

(8) Click the “Submit” button.

The operation is shown in figure 7, the ERPS domain configured the successful table entry information is shown in figure 8.

Figure 7 Add ERPS domain configuration

Figure 8 New ERPS domain information

12.1.3 Add the ERPS Ring

In the ERPS domain configuration page, if you click "New" button, you can add an ERPS ring, the operation is shown in figure 9, and then the ERPS ring configuration page appears, as shown in figure 10.

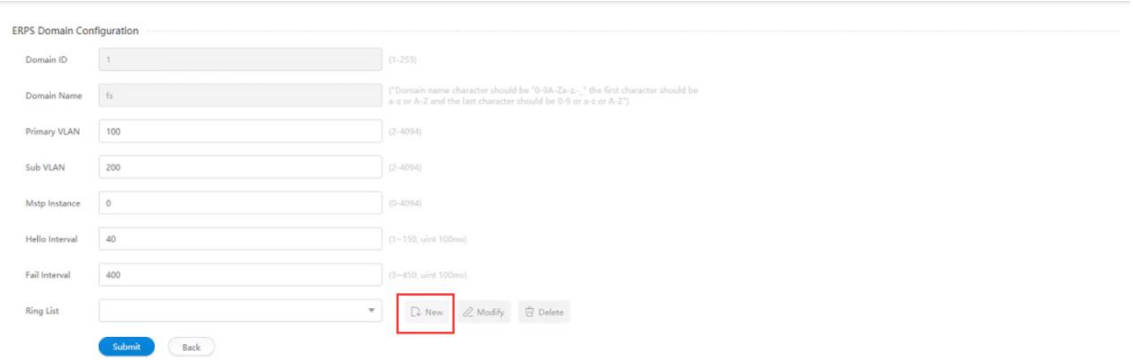


Figure 9 Add ERPS ring operation

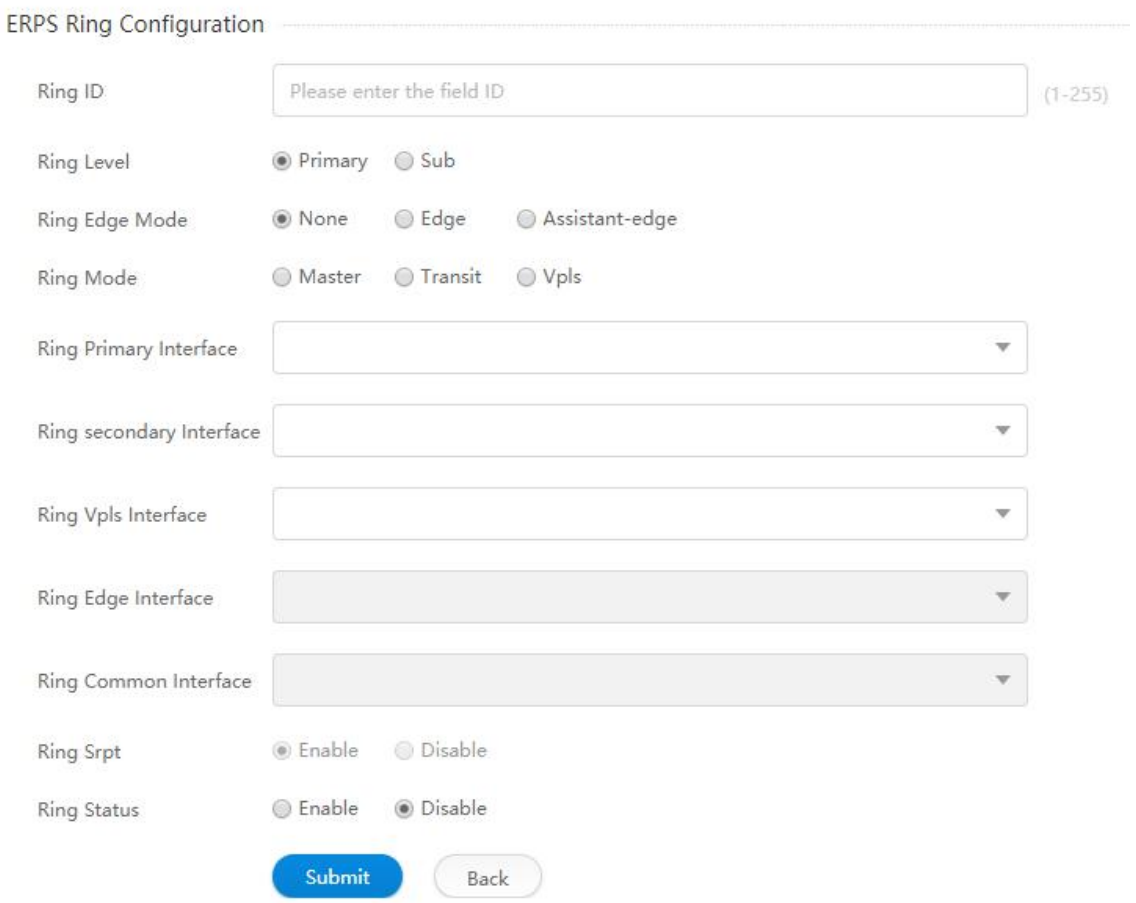


Figure 10 Add ERPS ring

- Parameter usage

Item	Description
Ring ID	Specifies the ERPS ring ID
Ring Level	Specifies that the ERPS ring is the primary ring or sub ring
Ring Edge Mode	Specifies the edge mode of the ERPS ring
Ring Mode	Specifies the node mode for the ERPS ring
Ring Primary Interface	Select the primary interface of the ERPS ring
Ring secondary Interface	Select the secondary interface of the ERPS ring
Ring Vpls Interface	Select the VPLS interface for the ERPS ring
Ring Edge Interface	Select the edge interface of the ERPS ring
Ring Common Interface	Select the common interface of the ERPS ring
Ring Srpt	Enable or disable SRPT message delivery
Ring Status	Enable or disable the ERPS ring

If you want to add a primary ring primary node, you can follow the following steps:

(1) Enter an ERPS ring ID in the "Ring ID" textbox.

(2) Select the ERPS ring is the primary ring in the "Ring Level" radio buttons.

(3) Select the edge mode of the ERPS ring to be none in the "Ring Edge Mode" radio buttons.

(4) Select the node mode of the ERPS ring as master in the "Ring Mode" radio buttons.

(5) Select the primary interface of the ERPS in the "Ring Primary Interface" dropdown box.

(6) Select the secondary interface of the ERPS in the "Ring secondary Interface" dropdown box.

(7) Select the Vpls interface of the ERPS in the "Ring Vpls Interface" dropdown box.

(8) Enable ERPS ring function in the "Ring Status" radio buttons.

(9) Click the "Submit" button.

The operation is shown in figure 11, the ERPS ring configured the successful table entry information is shown in figure 12.

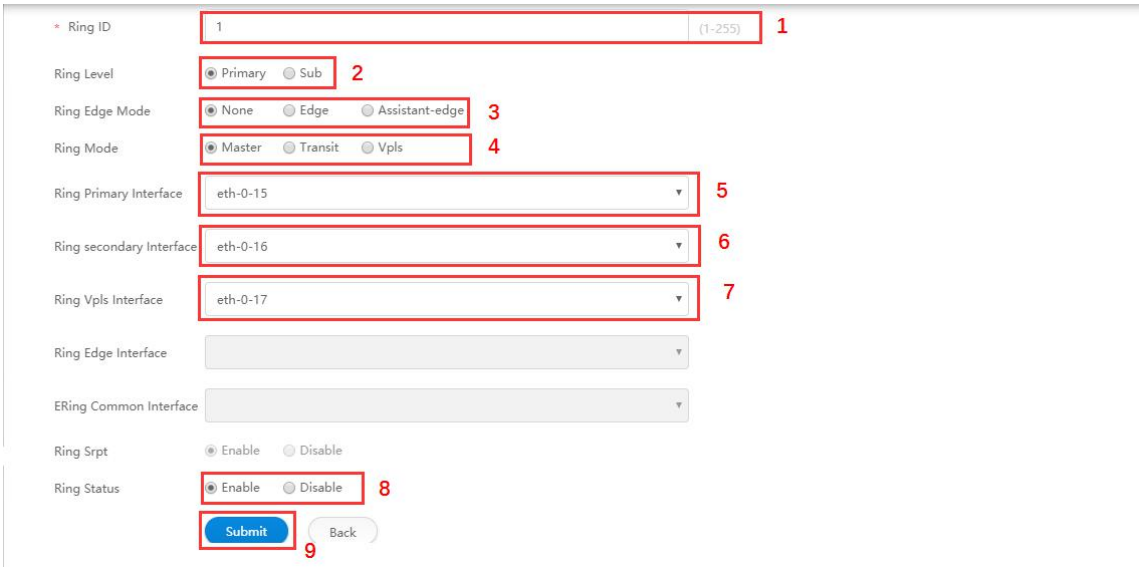


Figure 11 Add ERPS ring configuration

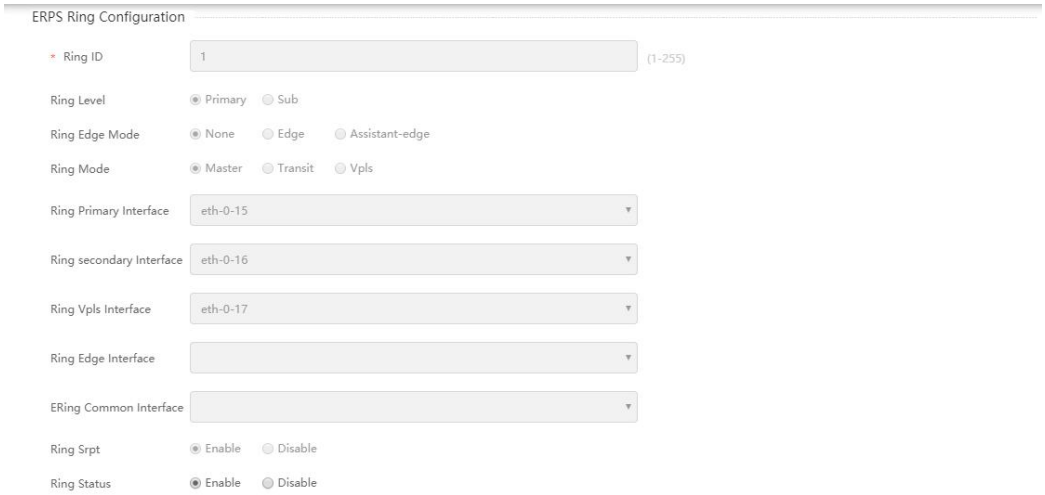


Figure 12 New ERPS ring information

12.1.4 Modify the ERPS Ring

In the ERPS domain configuration page, if you click "Modify" button, you can modify an ERPS ring configuration, the operation is

shown in figure 13, and then the ERPS ring configuration page appears, as shown in figure 14.

Figure 13 Modify ERPS ring operation

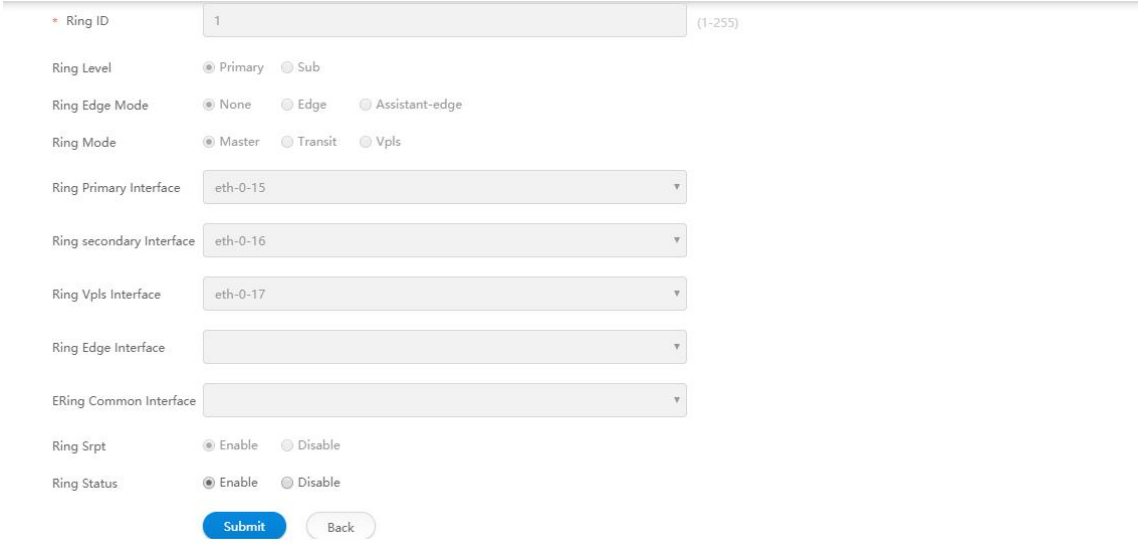


Figure 14 ERPS ring configuration

- Parameter usage

Item	Description
Ring ID	Display the ERPS ring ID
Ring Level	Display the level of the ERPS ring
Ring Edge Mode	Display the edge mode of the ERPS ring
Ring Mode	Display the node mode for the ERPS ring
Ring Primary Interface	Display the primary interface of the ERPS ring
Ring secondary Interface	Display the secondary interface of the ERPS ring
Ring Vpls Interface	Display the VPLS interface for the ERPS ring
Ring Edge Interface	Display the edge interface of the ERPS ring
Item	Description
Ring Common Interface	Display the common interface of the ERPS ring

Ring Srpt	Display the status of ERPS ring SRPT message delivery
Ring Status	Display the status of ERPS ring function

By selecting enable or disable the ERPS ring feature in the "Ring Status" radio buttons, and then click "Submit" button, you can modify the configuration of the ERPS ring, the operation is shown in figure 15.

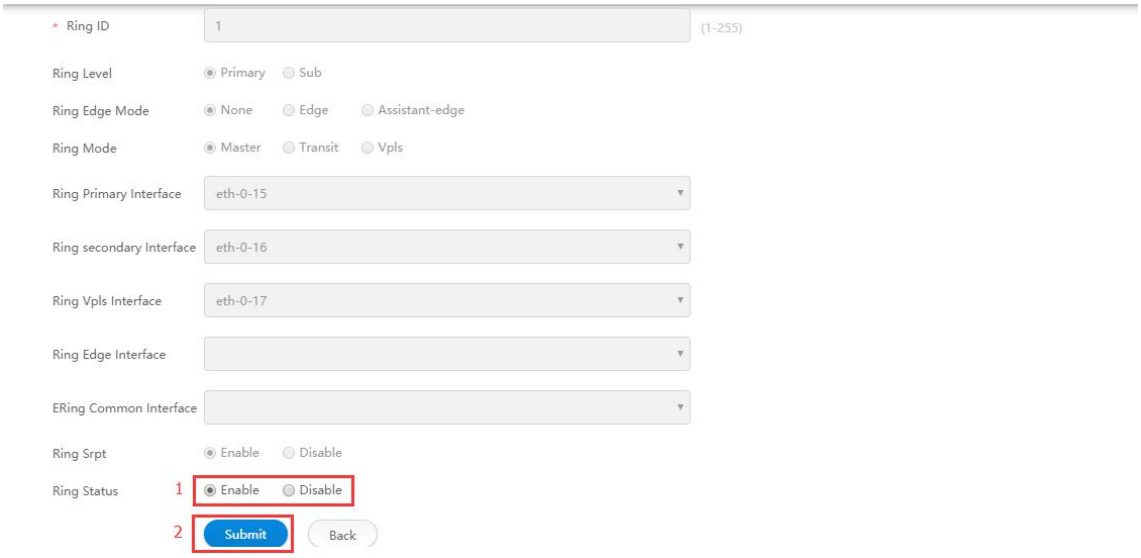


Figure 15 Modify ERPS ring configuration

12.1.5 Remove the ERPS Ring

In the ERPS domain configuration page, if you "Delete" button, you can delete an ERPS ring, the operation is shown in figure 16, and then the delete ERPS ring successful page appears, as shown in figure 17.

Figure 16 Delete ERPS ring operation

Figure 17 ERPS domain configuration

12.1.6 Modify the ERPS Domain

In the ERPS domain information display page, if you click "Edit" button, you can modify an ERPS domain configuration, the operation is shown in figure 18, and then the ERPS domain configuration page appears, as shown in figure 19.

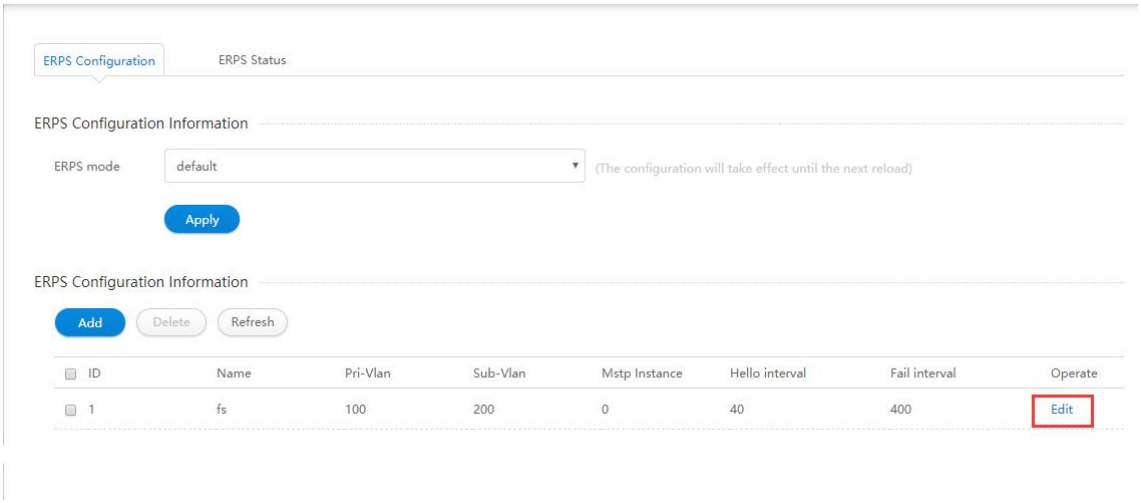


Figure 18 Modify ERPS domain configuration operation

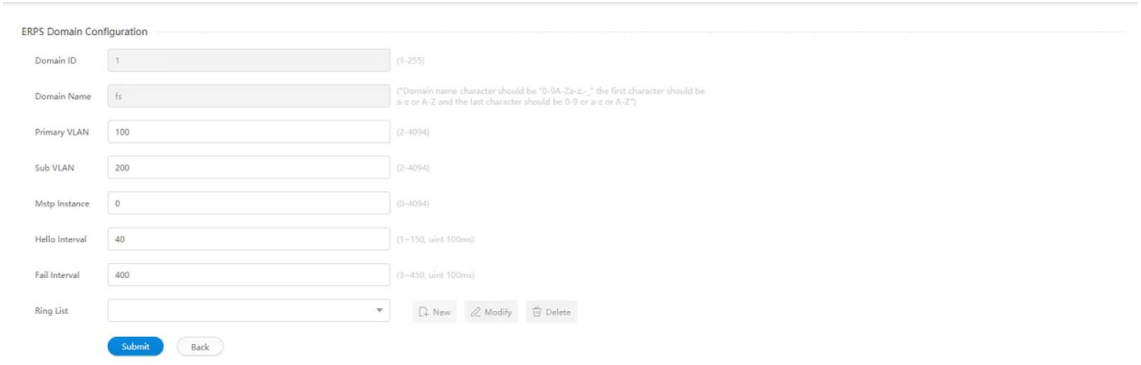


Figure 19 ERPS domain configuration

- Parameter usage

Item	Description
Domain ID	Display the ERPS domain ID
Domain Name	Display the ERPS domain name
Primary Vlan	Set the primary control VLAN for ERPS
Sub Vlan	Set a sub control VLAN for ERPS
Mstp Instance	Set an MSTP instance
Hello interval	Set the Hello message delivery period
Fail interval	Set the Fail message delivery period
Ring List	Display ERPS ring list information

If you want to modify the configuration of the ERPS domain, you can follow the following steps:

(1) Enter an ERPS primary control VLAN in the "Pri-Vlan" textbox.

(2) Enter an ERPS sub control VLAN in the "Sub-Vlan" textbox.

(3) Enter an MSTP instance in the "Mstp Instance" textbox.

(4) Enter the Hello message delivery period in the "Hello interval" textbox, but the parameters are optional, and if not configured, the default value is 1 second.

(5) Enter the Fail message delivery period in the "Fail interval" textbox, but the parameters are optional, and if not configured, the default value is 3 second.

(6) Click the "Submit" button.

The operation is shown in figure 20, the table entry information that ERPS domain successfully modified is shown in figure 21.

Figure 20 Modify ERPS domain configuration

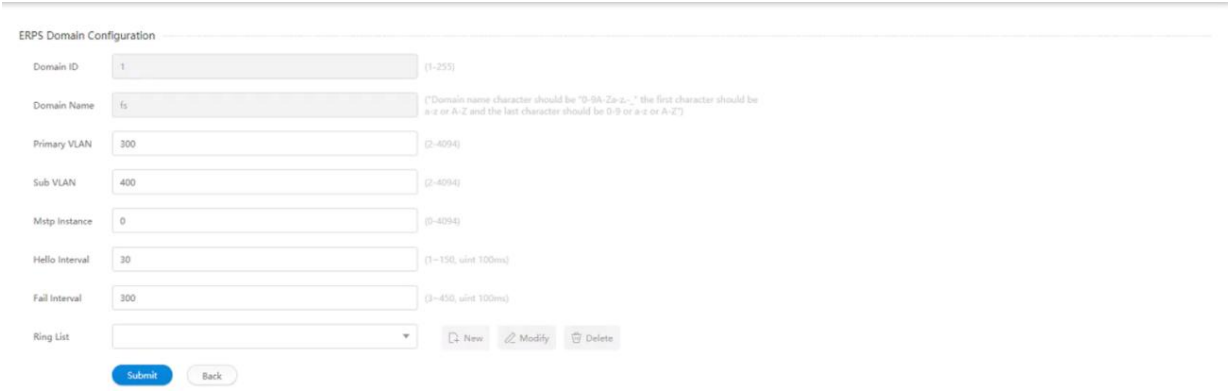


Figure 21 ERPS domain configuration information

12.1.7 Remove the ERPS Domain

If you want to delete the specified ERPS domain, you can follow the following steps:

(1) Select this specified ERPS domain which you want to delete.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, as shown in figure 22, if you click "Confirm" button, it will delete the ERPS domain, the table entry that ERPS domain successfully deleted is shown in figure 23; if you click "Cancel" button, you will cancel the delete operation.

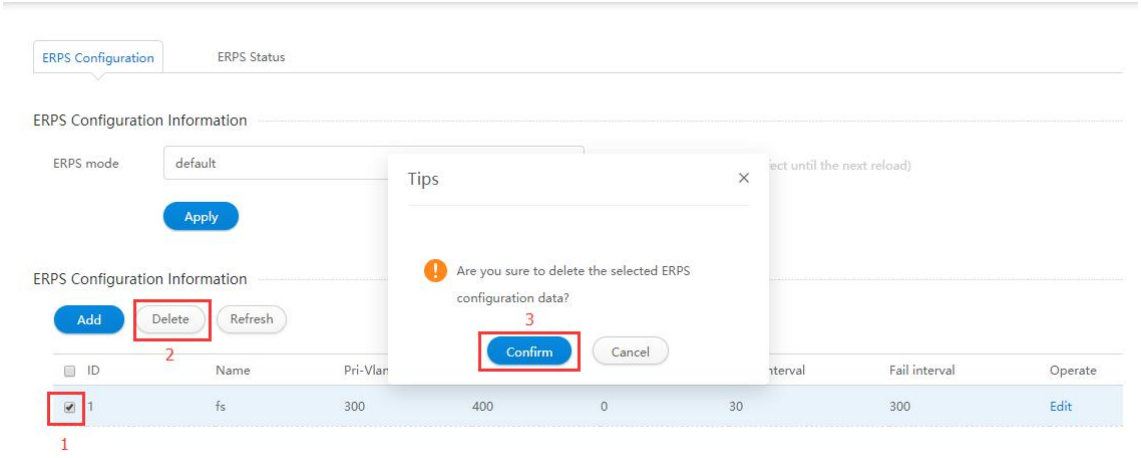


Figure 22 Delete ERPS domain

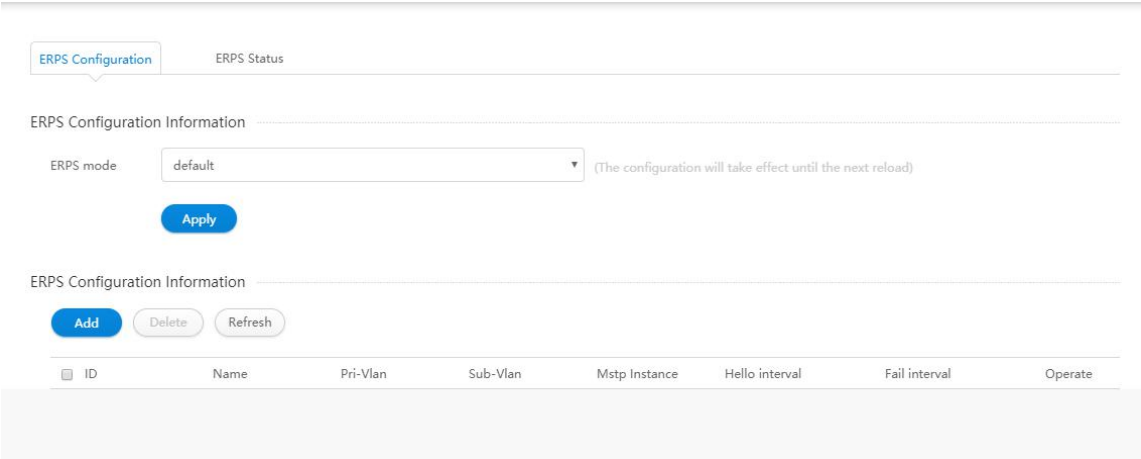


Figure 23 ERPS domain configuration information

12.1.8 Refresh the ERPS Domain

if you want to refresh the ERPS domain configuration information, you can click "Refresh" button. The operation is shown in figure 24.

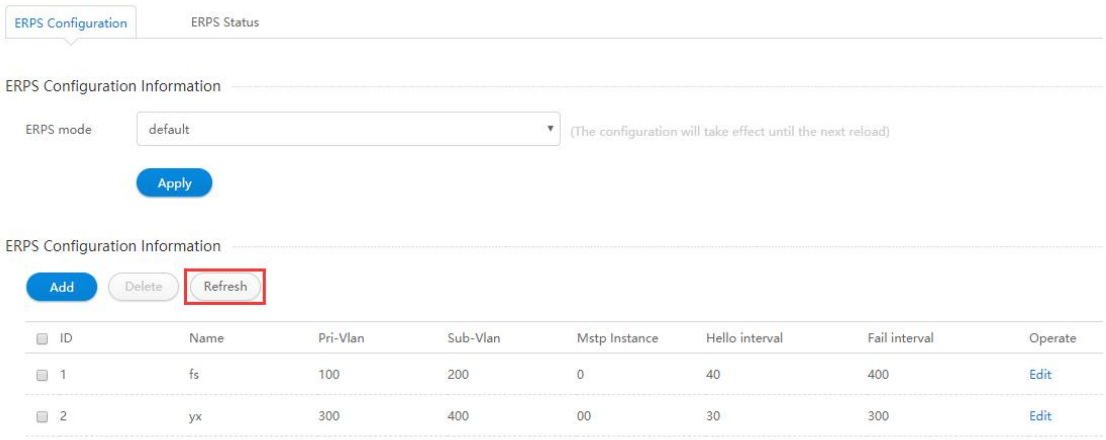


Figure 24 Refresh the ERPS domain configuration information

12.2 ERPS Status

This section describes the state information and statistics of the ERPS domain.

12.2.1 ERPS Status Information

If you click "ERPS -> ERPS Status" in the title bar, the ERPS status information page appears, as shown in figure 25.

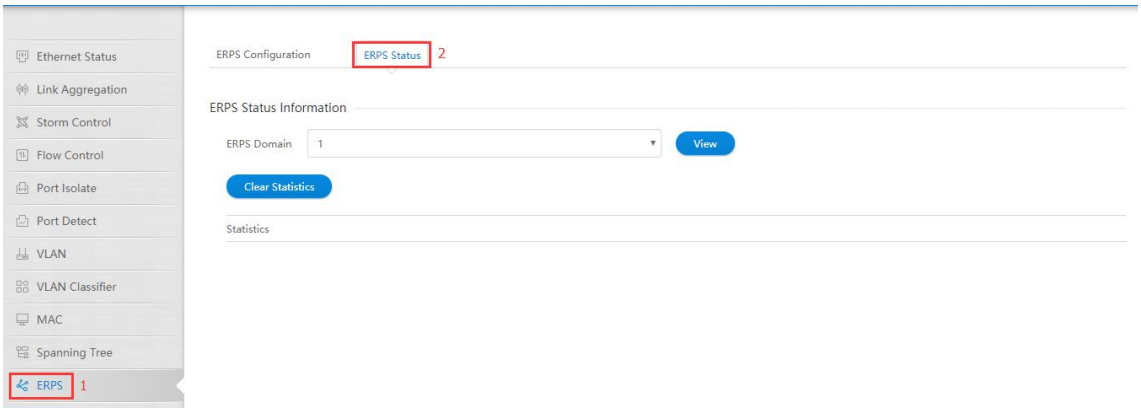


Figure 25 ERPS status information

- Parameter usage

Item	Description
ERPS Domain	Display the domain ID information for the ERPS domain

If you want to view the status of different ERPS domains, please select the ERPS domain ID in the "ERPS Domain" dropdown box, and then click the "View" button, the operation is shown in figure 26, the state information for the ERPS domain is shown in figure

27.

Figure 26 View ERPS status operation

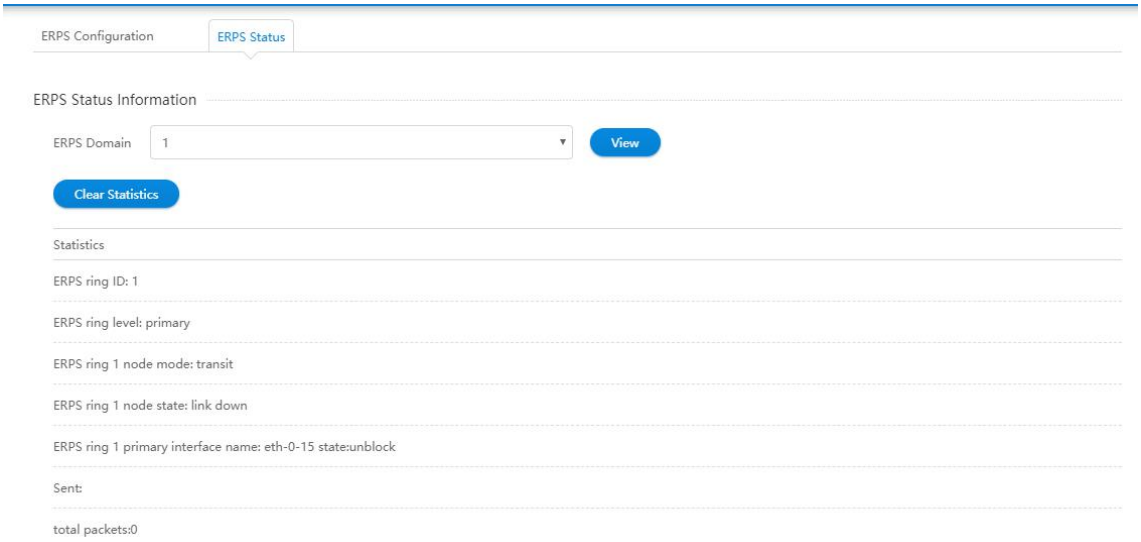


Figure 27 ERPS status information

If you want to clear the ERPS domain's statistics, please click the “Clear Statistics” button, the operation is shown in figure 28.

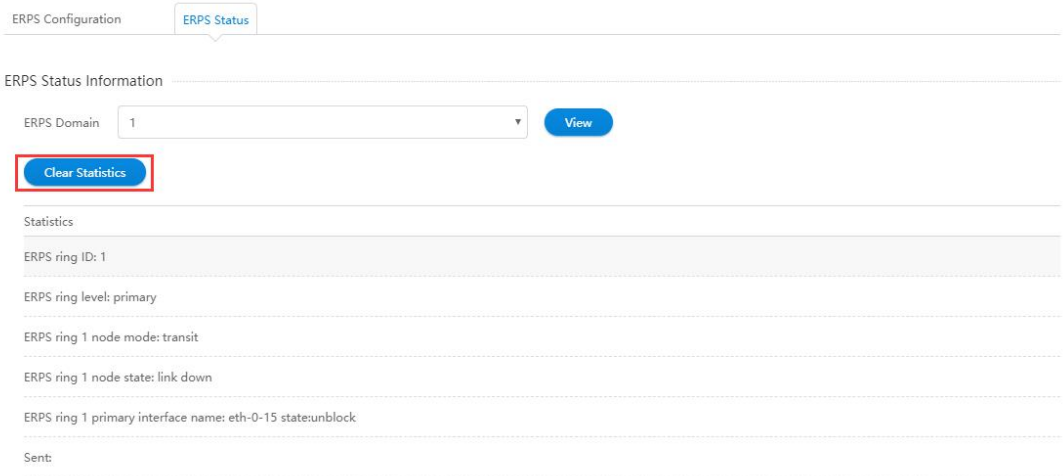


Figure 28 Clear ERPS statistics operation

13. Mirror

If you click “Configuration -> Mirror” in the top control bar, the mirror configuration list page appears, as shown in figure 1.

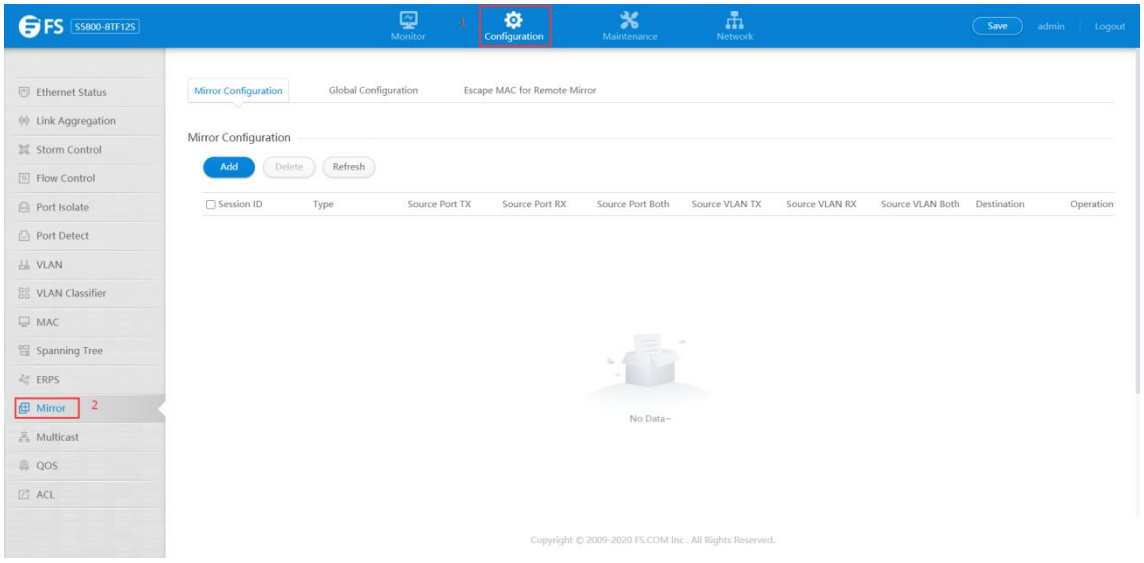


Figure 1 Mirror list

This section mainly describes how to configure and view Mirror.

13.1 Mirror Configuration

If you click “Mirror -> Mirror Configuration” in the title bar, the mirror configuration information page appears, as shown in figure 2.

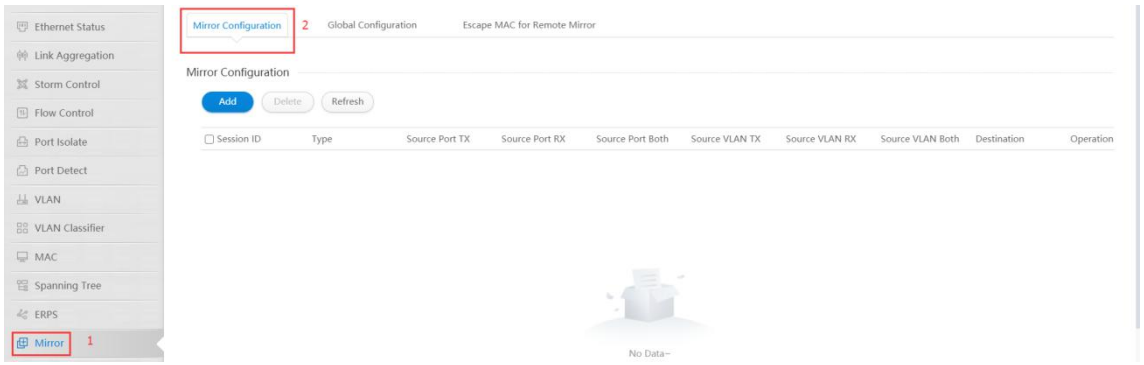


Figure 2 Mirror configuration page

- Parameter usage

Item	Description
Session ID	Display the session ID of mirror
Type	Display the destination type of mirror,including local/Remote port Mirroring
Source PORT TX	Display mirroring of the receiving direction of a port

Item	Description
Source PORT RX	Display mirroring of the sending direction of a port
Source PORT BOTH	Display mirroring of the sending and receiving direction of a port
Source VLAN TX	Display mirroring of the receiving direction of a VLAN
Source VLAN RX	Display mirroring of the sending direction of a VLAN
Source VLAN BOTH	Display mirroring of the sending and receiving direction of a VLAN
Destination	Display mirrored destination port
Operation	Display that mirror configuration table entries can be edited

13.1.1 Add Mirror Sessions

If you click "Add" in the mirror configuration list, you can add a mirror session, the operation is shown in figure 3. then mirror session settings page appears, as shown in figure 4.

Figure 3 Add mirror sessions operation

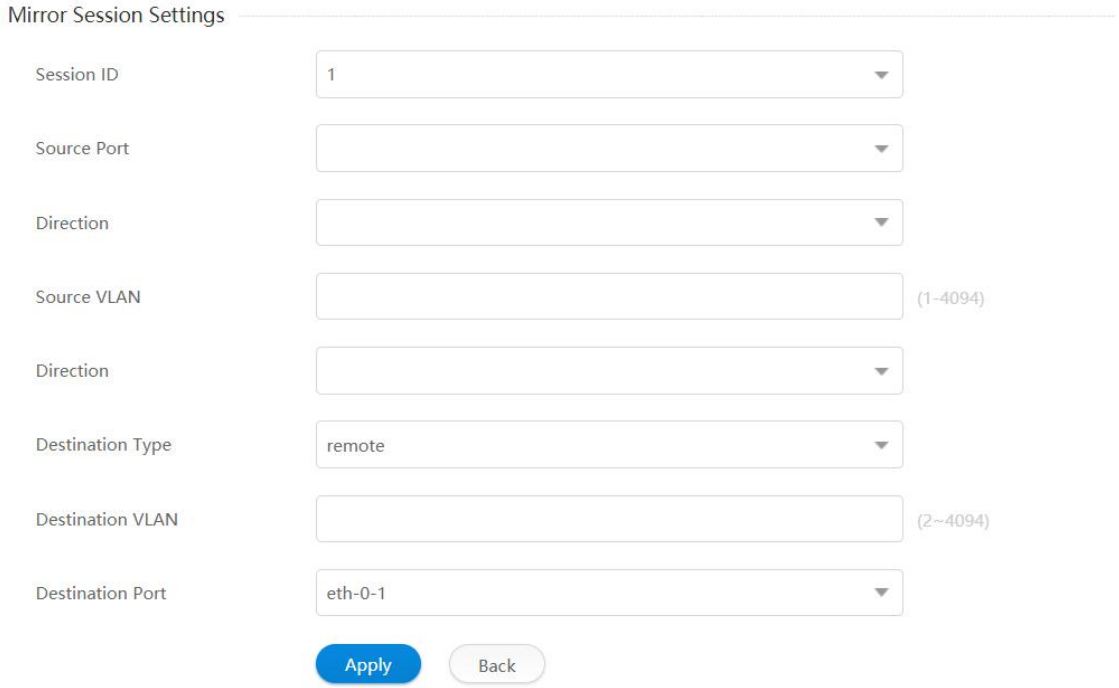


Figure 4 Mirror sessions settings list

- Parameter usage

Item	Description
Session ID	Display the session ID of mirror
Source Port	Display the source port of mirror
Direction	Display the direction of source port
Source VLAN	Display the source vlan of mirror
Direction	Display the direction of source vlan
Direction Type	Display the type of the mirror target (remote or local)
Direction VLAN	Display mirroring target VLAN (remote support only)
Direction port	Display the destination port of mirror

If you want to add a mirror session, you can follow the following steps:

(1) Select a session ID.

(2) Select a source port for configuration mirroring.

(3) Select the direction of source port.

(4) Select the destination type of mirror.

(5) Enter the destination VLAN of mirror.

(6) Select the destination port of mirror.

(7) Click the "Apply" button to add a mirror session.

NOTE:

(1) The items with the asterisk symbol "*" are ones where you must enter values.

(2) A mirroring session is a collection of mirroring sources and a mirroring purpose, for a mirroring session to work, you need to configure a mirroring destination and at least one mirroring source.

The operation is shown in figure 5, add a mirror session configuration success table entry is shown in figure 6.

Figure 5 Add mirror session configuration

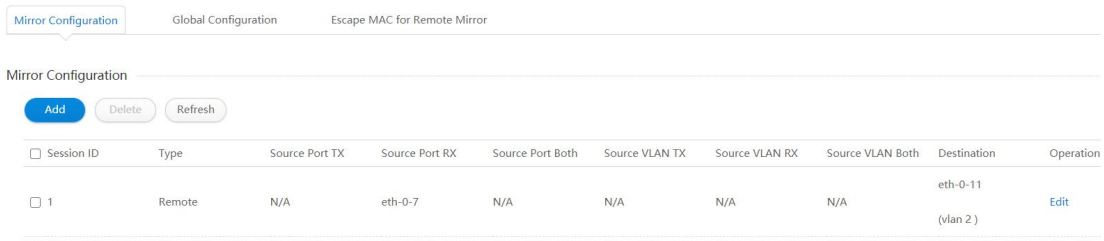


Figure 6 New mirror session information

13.1.2 Modify Mirror

You can click the "Edit" button in the rightmost operation bar to modify the mirror information of the session, this operation is shown in figure 7, and then port mirror configuration page appears, as shown in figure 8.

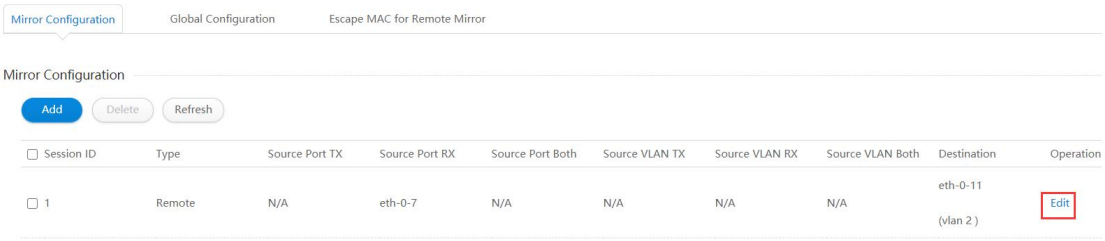


Figure 7 Edit mirror session operation

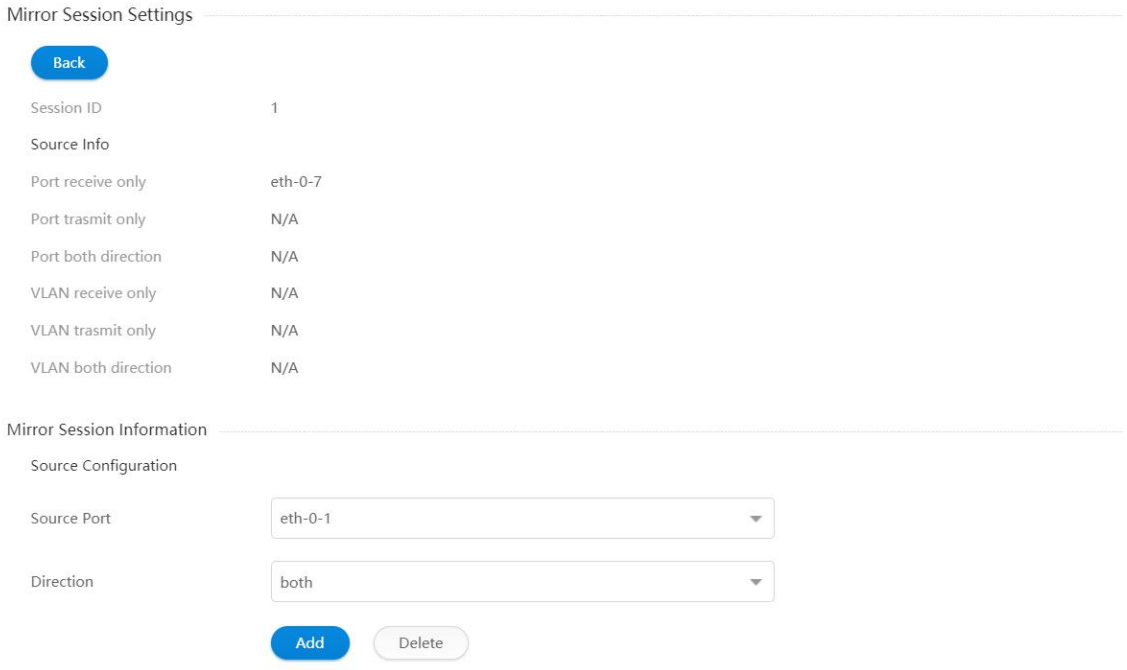


Figure 8 Port mirror configuration page

- Parameter usage

Item	Description
Port receive only	Display port only receive packets
Port transmit only	Display port only transmit packets
Port both direction	Display port both transmit and receive packets
VLAN receive only	Display VLAN only receive packets
VLAN transmit only	Display VLAN only transmit packets
VLAN both direction	Display VLAN both transmit and receive packets

If you want to modify the specified mirror, such as add a source port to receive and send packets in a mirroring session, and then modify the destination port in this mirroring session, you can follow the following steps:

(1) Select a new source port.

(2) Select the direction of receiving and sending packets.

(3) Click the "Add" button to add a source port to the mirroring session.

(4) Select a new destination port.

(5) Click the "Apply" button to modify the destination port in this mirroring session.

NOTE: The items with the asterisk symbol "*" are ones where you must enter values.

The operation is shown in figure 9, modify specified mirror success table entry is shown in figure 10 and figure 11.

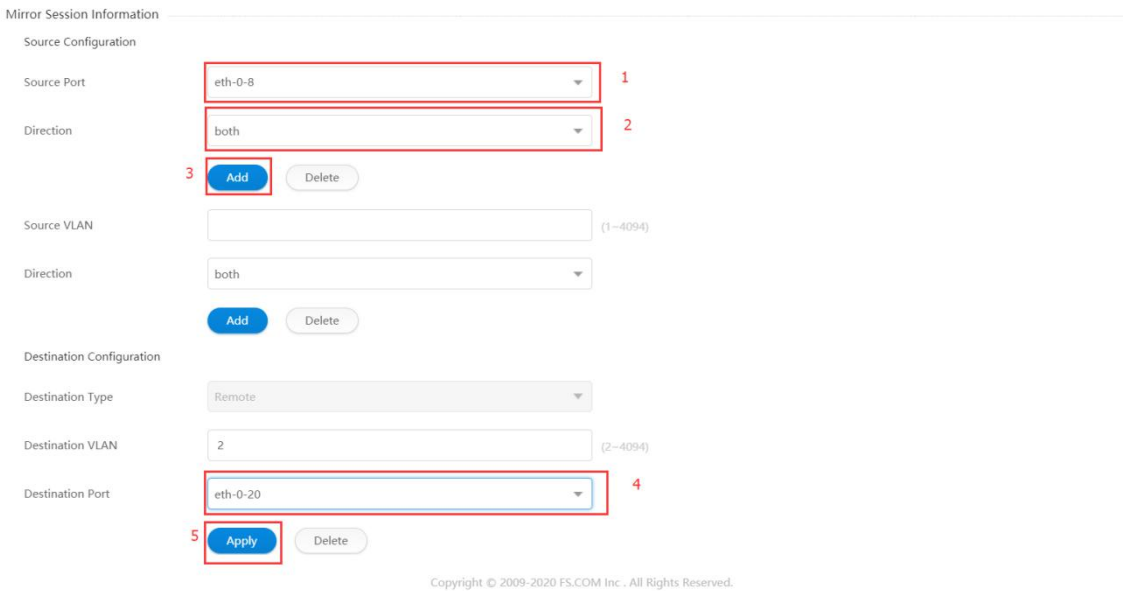


Figure 9 Edit mirror session operation

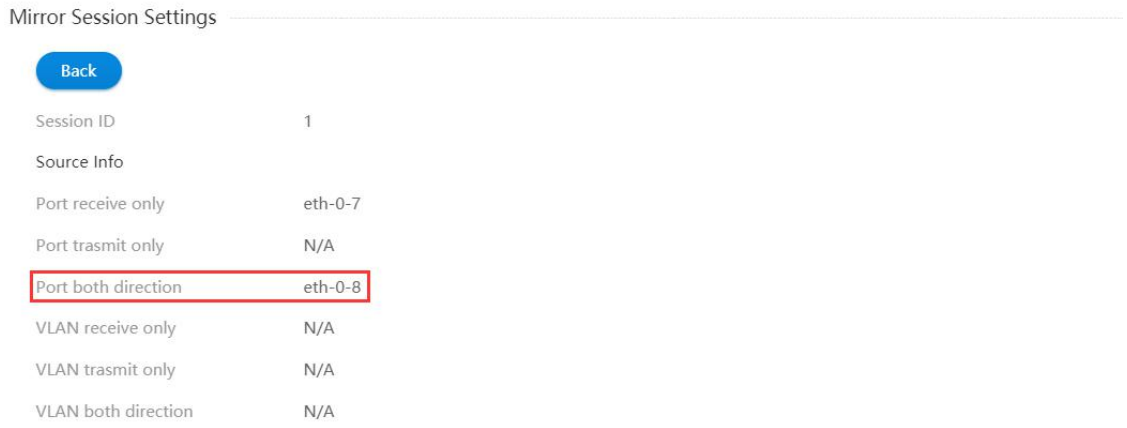


Figure 10 Modified mirroring session information

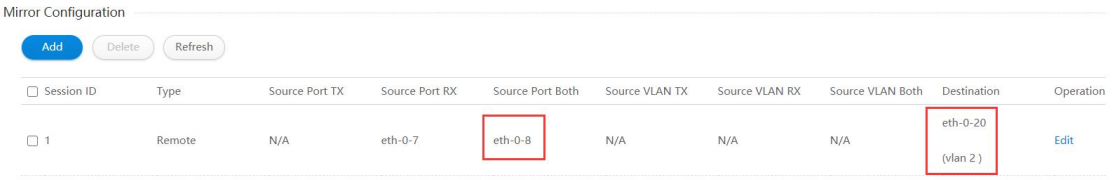


Figure 11 Modified mirroring session information

13.1.3 Delete Mirror

If you want to delete the specified mirror, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified mirror.

(2) Click “Delete” button.

(3) It will appear tips page to note you to confirm the operation, if you click “Confirm” button , it will delete this mirror; if you click “cancel” button, you will cancel delete this mirror operation, as shown in figure 12.

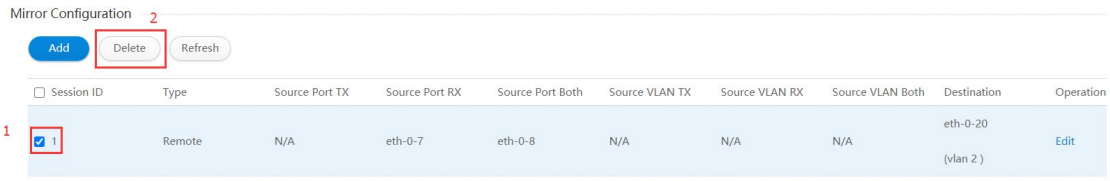


Figure 12 Delete mirror operation

Delete a mirror configuration success table entry is shown in figure 13.

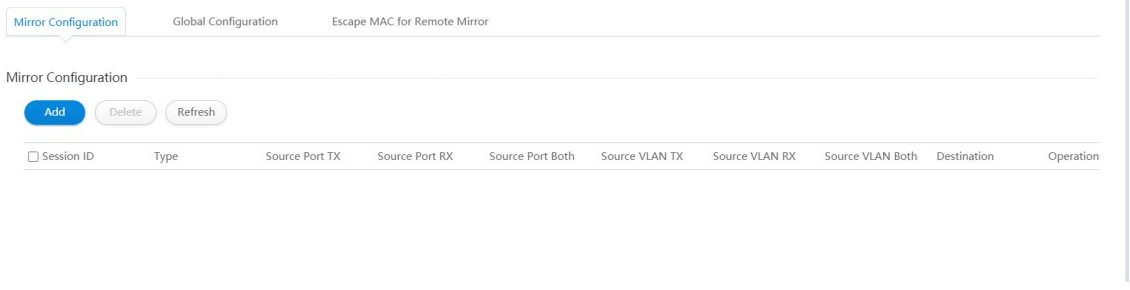


Figure 13 Delete mirror information

13.2 Global Configuration

If you click "Mirror -> Global configuration" in the title bar, the global configuration information page appears, as shown in figure14.

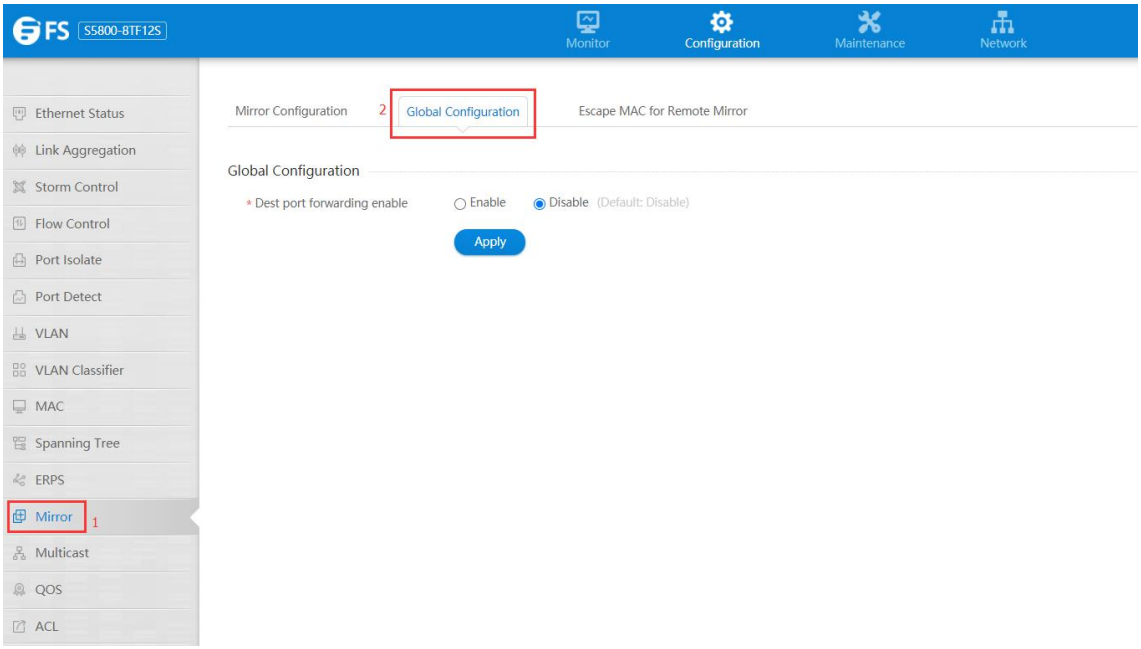


Figure 14 Global configuration list

- Parameter usage

Item	Description
Dest port forwarding enable	Display whether the normal forwarding function of dest port is enabled globally

13.2.1 Configure Destination Port Forwarding Function

If you want to configure destination port forwarding function, such as enable destination port forwarding function, you can click the "Enable" button and then click the "Apply" button.
The operation is shown in figure 15.

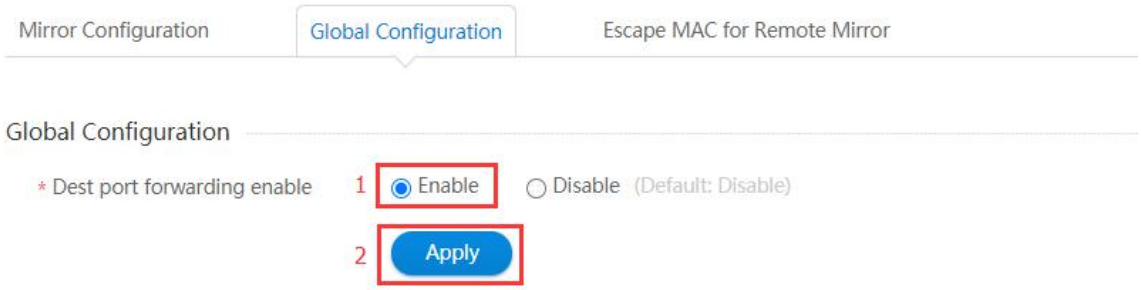


Figure 15 Configure forwarding function operation

13.3 Escape MAC for Remote Mirror

If you click “Mirror -> Escape MAC for Remote Mirror” in the title bar, the escape MAC for remote mirror page appears, as shown in figure16.

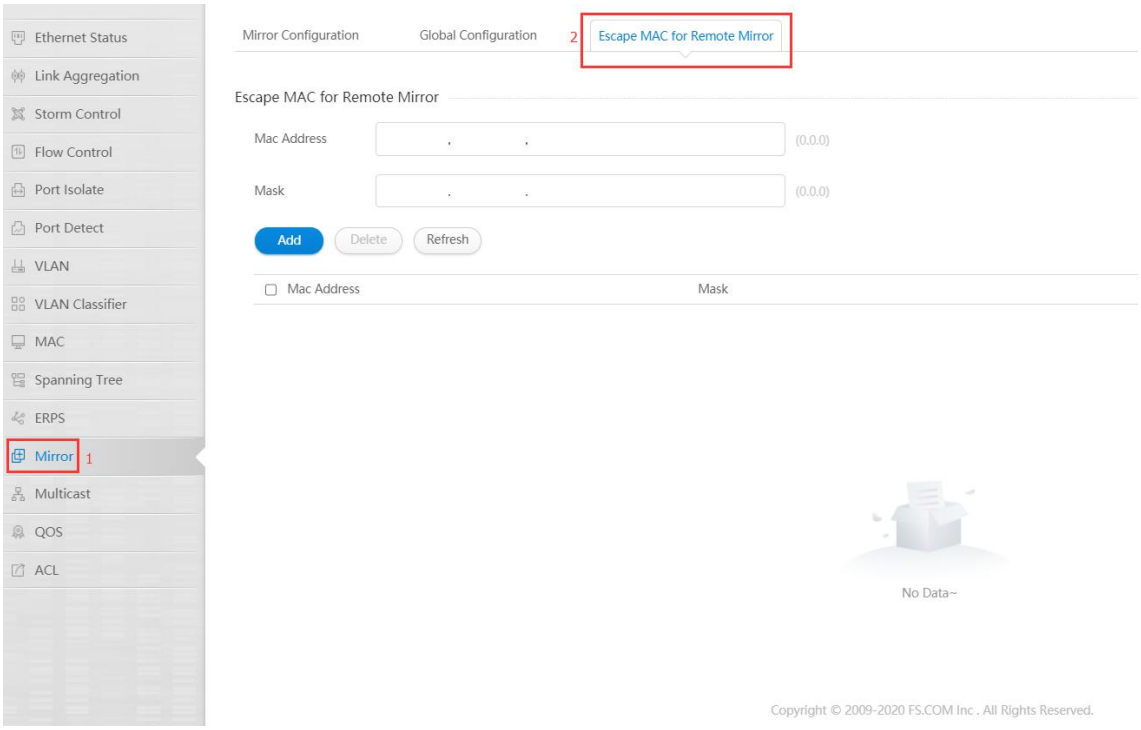


Figure 16 Escape MAC for remote mirror list

- Parameter usage

Item	Description
Mac Address	Displays the Escape MAC address of the remote mirror

13.3.1 Add Escape MAC for Remote Mirror

If you want to add escape MAC for remote mirror, you can follow the following steps:

(1) Enter a valid MAC address.

(2) Enter a valid Mask address.

(3) Click the “Add” button to add escape MAC for remote mirror.

The operation is shown in figure 17, add escape MAC for remote mirror success table entry is shown in figure 18.

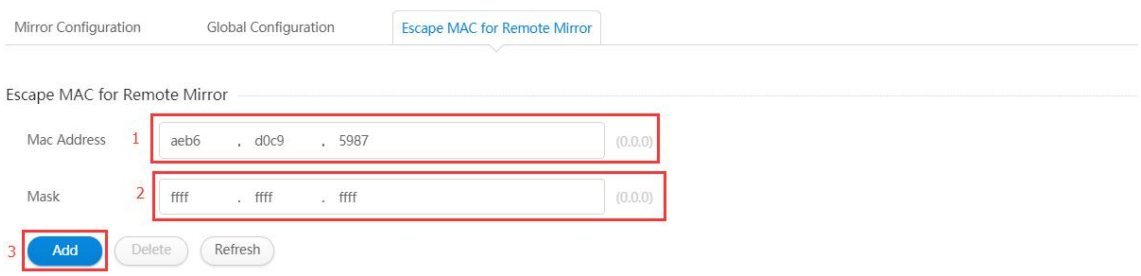


Figure 17 Add escape MAC for remote mirror operation

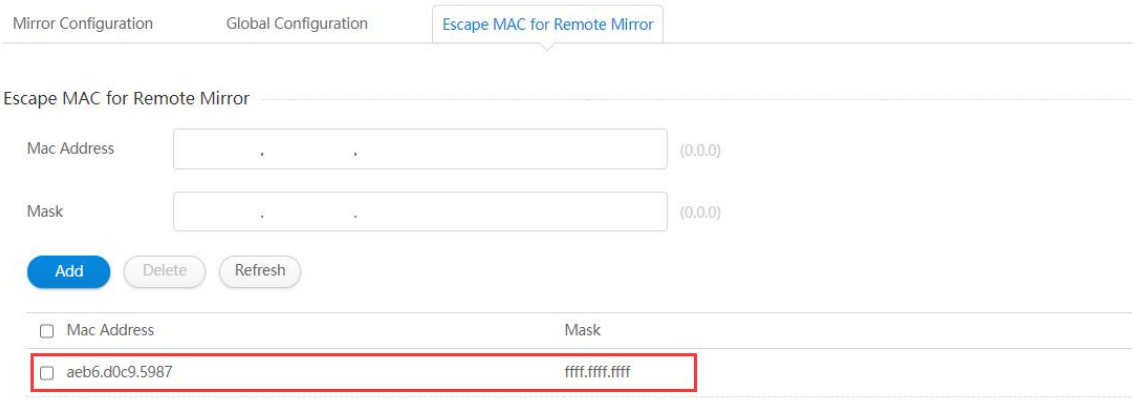


Figure 18 New escape MAC for remote mirror

13.3.2 Delete Escape MAC for Remote Mirror

If you want to delete the specified escape MAC for remote mirror, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified escape MAC for remote mirror.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button , it will delete this escape MAC for remote mirror; if you click "cancel" button, you will cancel delete this escape MAC for remote operation, as shown in figure 19.

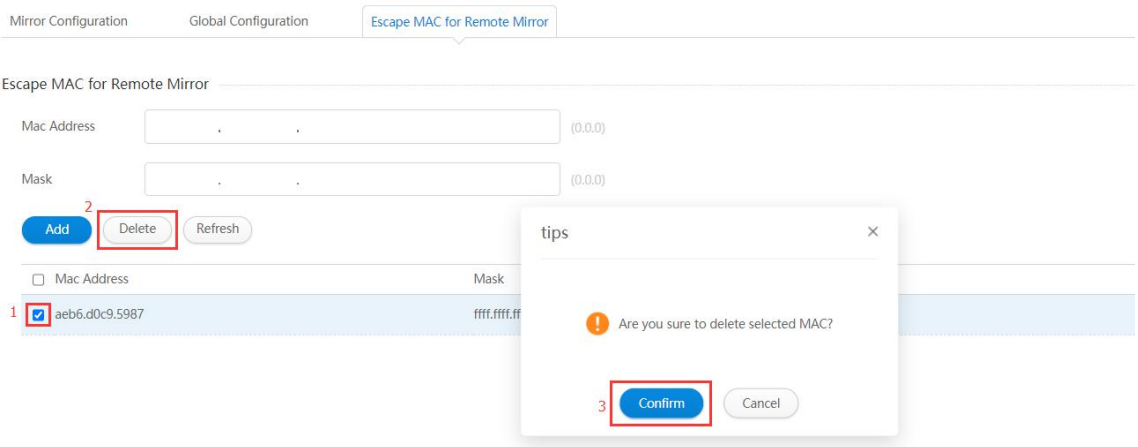


Figure 19 Delete escape MAC for remote mirror operation

Delete escape MAC for remote mirror success table entry is shown in figure 20.

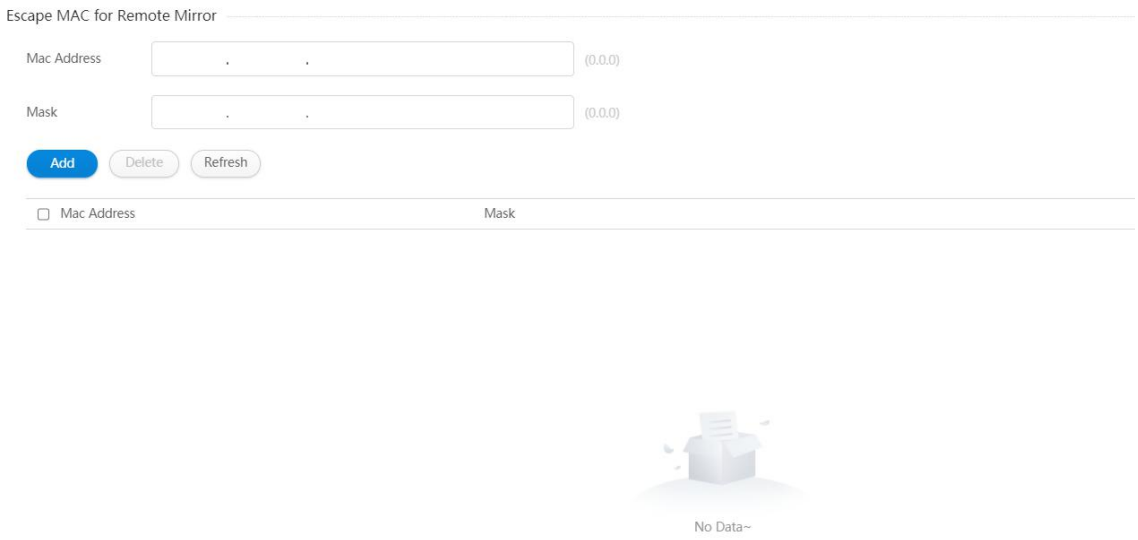


Figure 20 Delete escape MAC for remote mirror

14. Multicast

If you click “Network ->IP Routing” in the top control bar, the multicast configuration list page appears, as shown in figure 1.

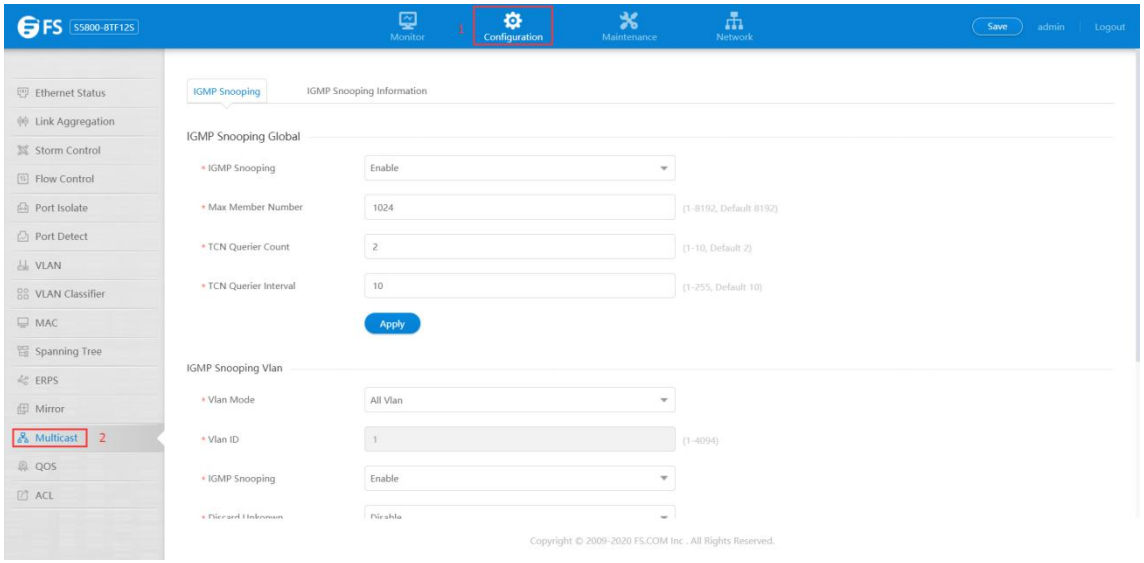


Figure 1 Multicast configuration list

This chapter describes multicast configuration function and viewing multicast information of the device.

14.1 IGMP Snooping

The multicast configuration capabilities include IGMP snooping global configuration and IGMP snooping VLAN configuration.

14.1.1 IGMP Snooping Global Configuration

If you click “Multicast-> IGMP Snooping” in the title bar, the IGMP snooping global configuration page appears, as shown in figure 2.

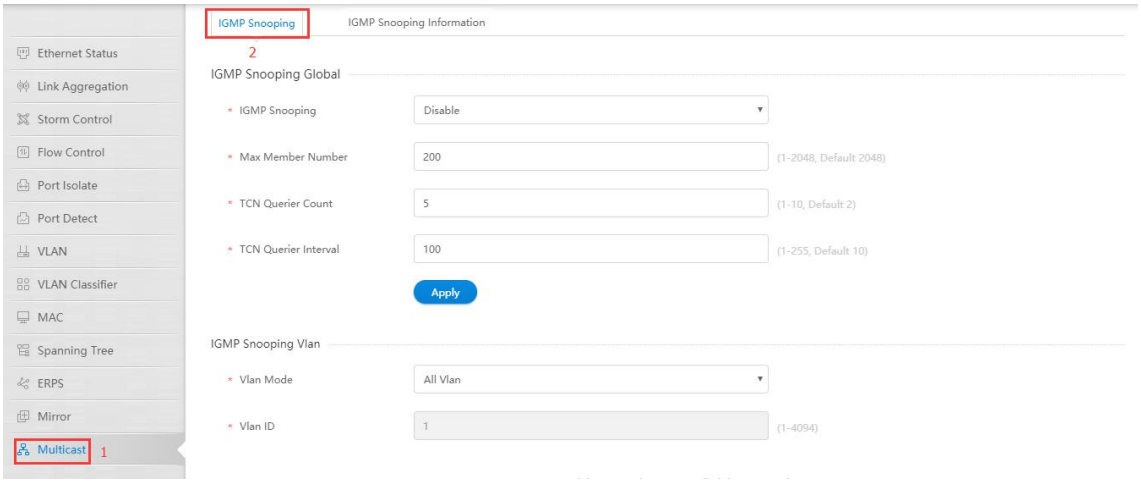


Figure 2 IGMP snooping global configuration

- Parameter usage

Item	Description
IGMP Snooping	Set the IGMP snooping global stats
Max Member Number	Set the IGMP snooping global max member number
TCN Querier Count	Set the IGMP snooping tcn querier count
TCN Querier Interval	Set the IGMP snooping tcn querier interval

If you want to configure parameters of IGMP snooping global, you can follow the following steps:

(1) Select the IGMP snooping global stats in the "IGMP Snooping" dropdown box.

(2) Enter the maximum number of IGMP members in the "Max member number" text box.

(3) Enter tcn querier count in the "TCN Querier Count" textbox.

(4) Enter tcn querier interval in the "TCN Querier Interval" textbox.

(5) Click the "Apply" button.

(6) Click the "Apply" button to confirm configure IGMP snooping global parameters.

The operation is shown in figure 3, IGMP snooping globally configured the successful table entry is shown in figure 4.

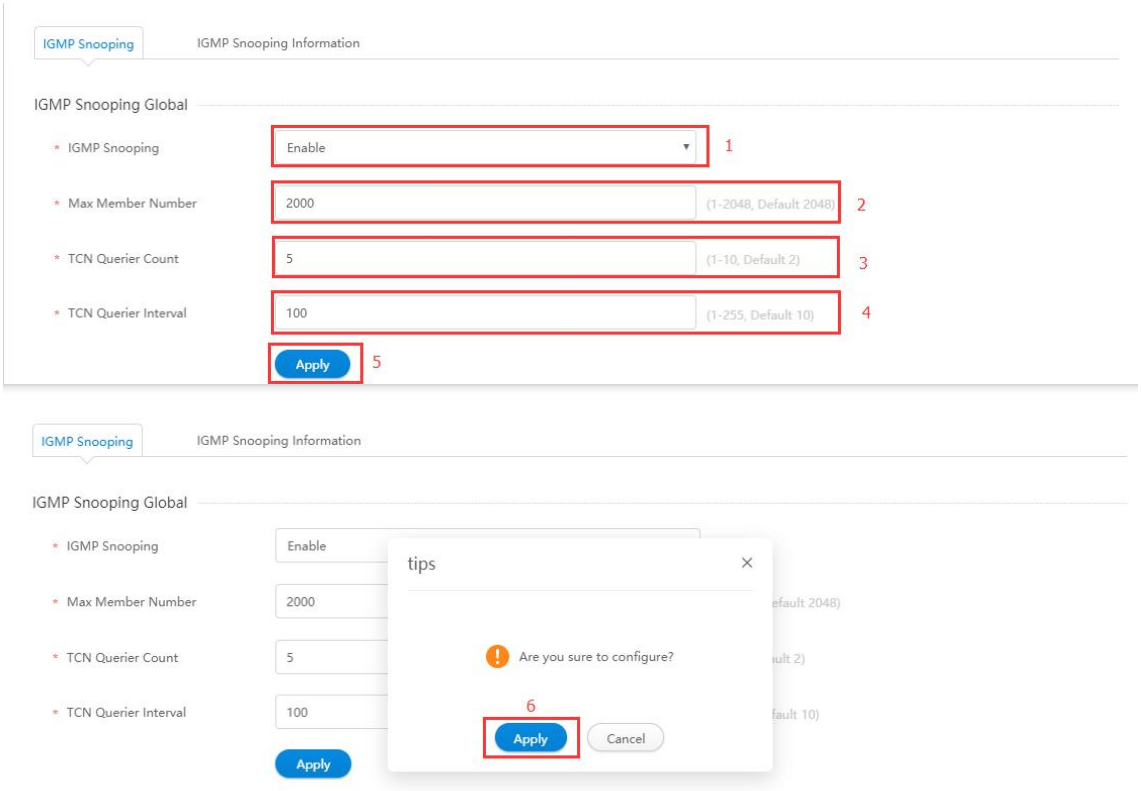


Figure 3 IGMP snooping global configuration operation

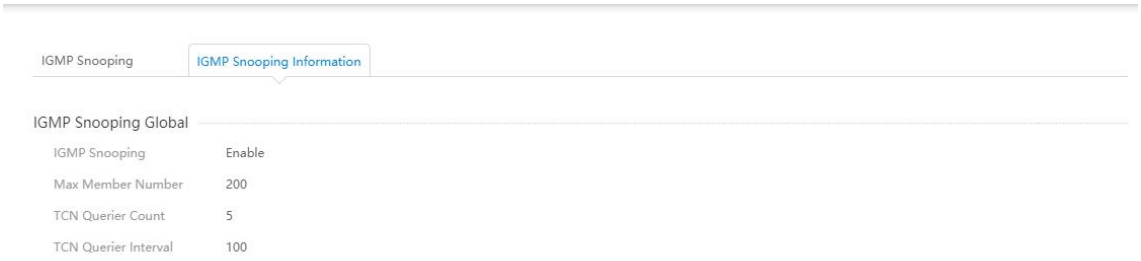


Figure 4 IGMP snooping global configuration information

14.1.2 IGMP Snooping VLAN Configuration

If you click "Multicast-> IGMP Snooping" in the title bar, the IGMP snooping VLAN configuration page appears, as shown in figure 5.

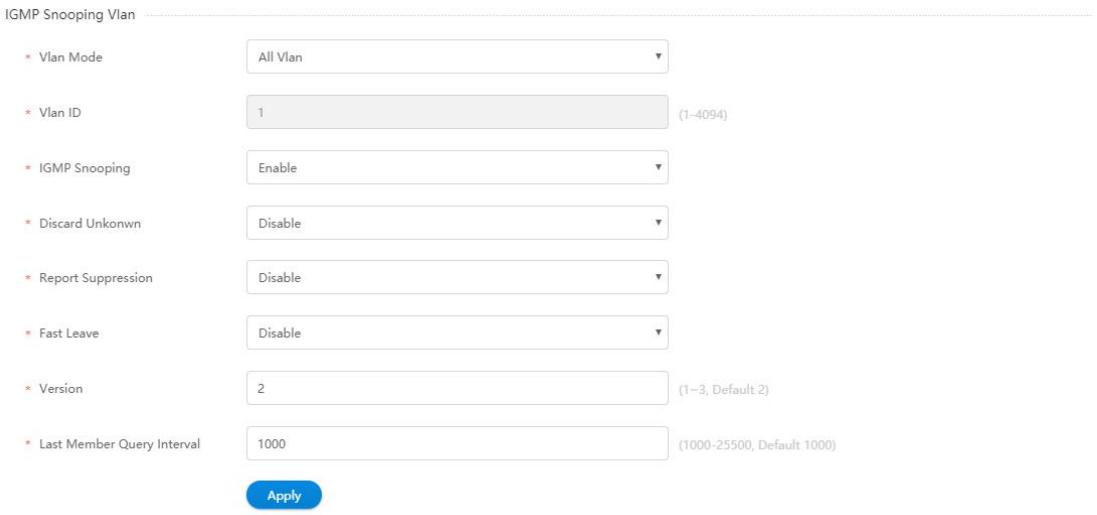


Figure 5 IGMP snooping VLAN configuration

- Parameter usage

Item	Description
Vlan Mode	Set the IGMP snooping VLAN mode(all VLAN or single VLAN)
Vlan ID	Set the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Set the IGMP snooping VLAN stats
Discard Unknown	Set the IGMP snooping VLAN discard unknown stats
Report Suppression	Set the IGMP snooping VLAN report suppression stats
Fast Leave	Set the IGMP snooping VLAN fast leave stats
Version	Set the IGMP snooping VLAN version
Last Member Query Interval	Set the IGMP snooping VLAN last member query interval

If you want to configure parameters of IGMP snooping VLAN, you can follow the following steps:

(1) Select the IGMP snooping VLAN mode in the "Vlan Mode" dropdown box.
(2) Enter the IGMP snooping VLAN id in the "Vlan ID" textbox.
(3) Select the IGMP snooping VLAN state in the "IGMP Snooping" dropdown box.
(4) Select the IGMP snooping discard unknown stat in the "Discard Unknown" dropdown box.
(5) Select the IGMP snooping report suppression stat in the "Report Suppression" dropdown box.
(6) Select the IGMP snooping VLAN fast leave stat in the "Fast Leave" dropdown box.
(7) Enter the IGMP snooping VLAN version in the "Version" textbox.
(8) Enter the IGMP snooping VLAN last member query interval in the "Last Member Query Interval" textbox.
(9) Click the "Apply" button.
(10) Click the "Apply" button to confirm configure IGMP snooping VLAN parameters.

The operation is shown in figure 6, IGMP snooping VLAN configured the successful table entry is shown in figure 7.

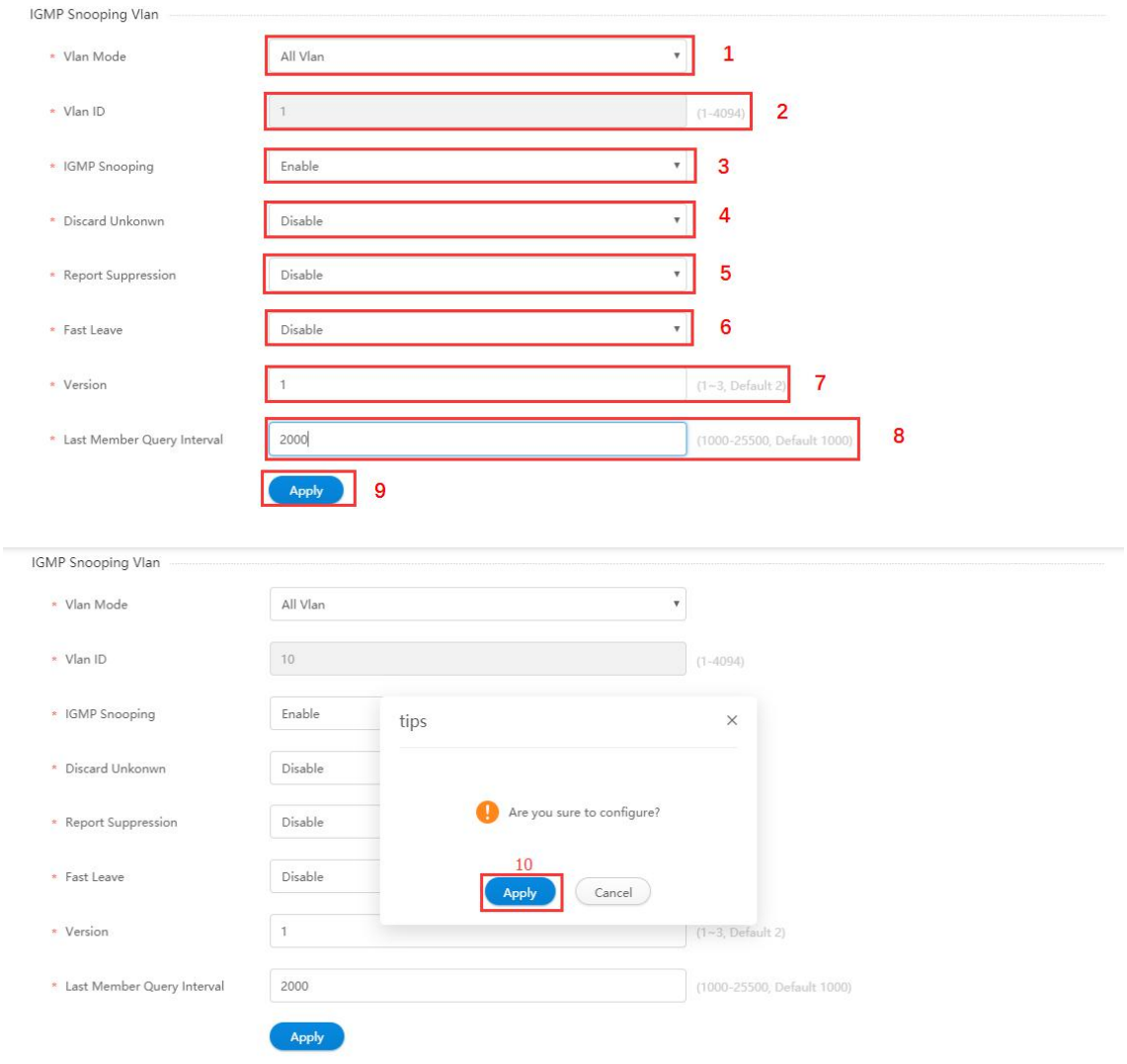


Figure 6 IGMP snooping VLAN configuration operation

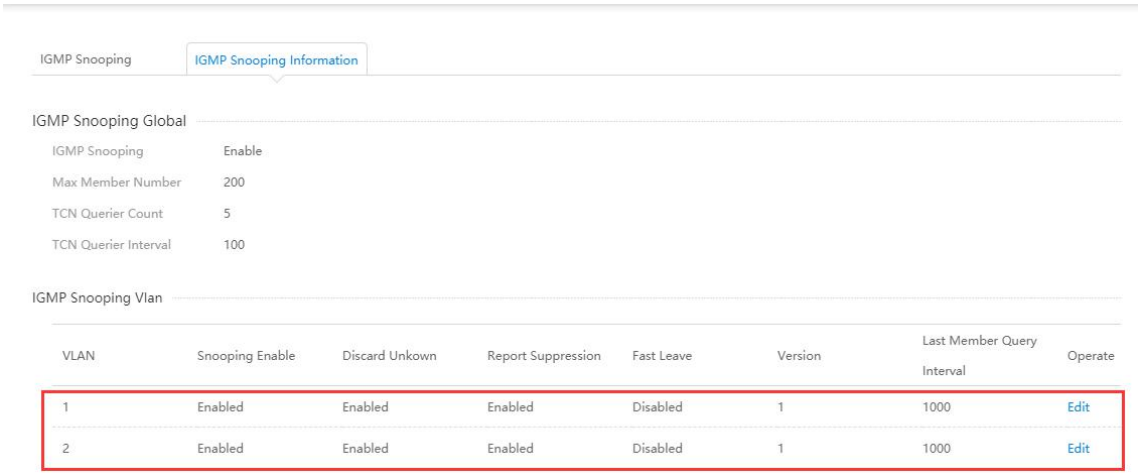


Figure 7 IGMP snooping VLAN configuration information

14.1.3 IGMP Snooping Information

If you click "Multicast-> IGMP Snooping Information" in the title bar, the IGMP snooping global information page, IGMP snooping groups information page and IGMP snooping VLAN information page appears, as shown in figure 8, figure 9 and figure 10.

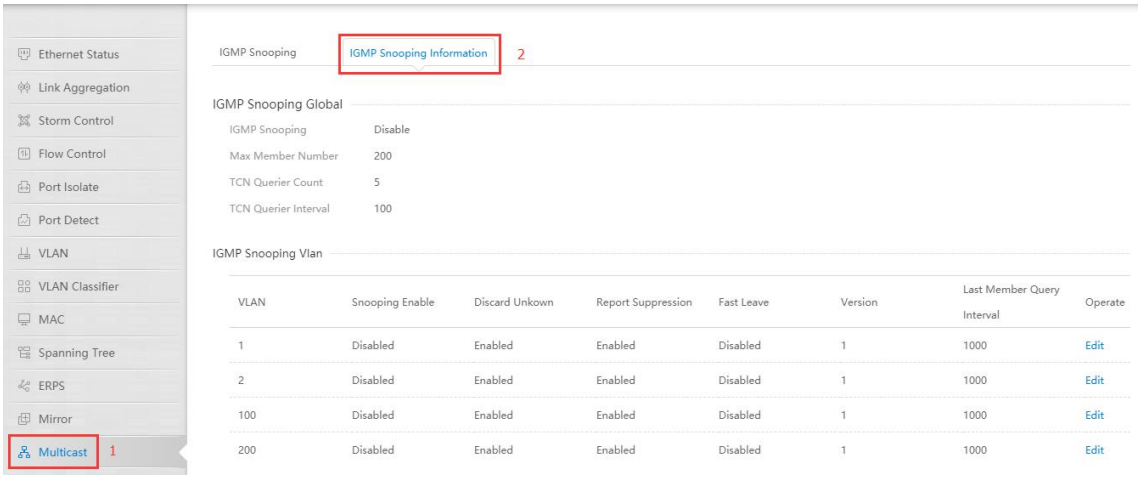


Figure 8 IGMP snooping global information

- Parameter usage

Item	Description
IGMP Snooping	Display the IGMP snooping global stats
Max Member Number	Display the IGMP snooping global max member number
TCN Querier Count	Display the IGMP snooping tcn querier count
TCN Querier Interval	Display the IGMP snooping tcn querier interval

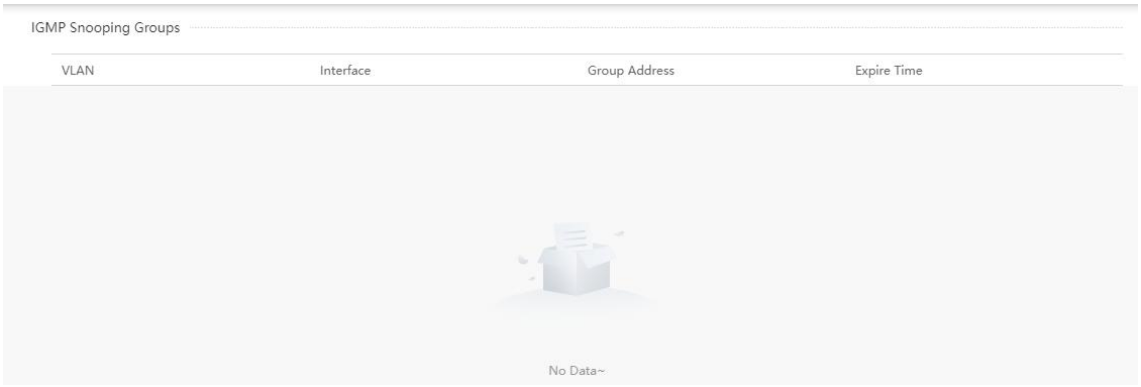


Figure 9 IGMP snooping groups information

- Parameter usage

Item	Description
VLAN	Display the VLAN ID for joining the IGMP snooping group
Interface	Display the VLAN member port that have joined the IGMP snooping group
Group Address	Displays the IGMP snooping group address
Expire Time	Display the expire time for the IGMP snooping group table entry

Figure 10 IGMP snooping VLAN information

- Parameter usage

Item	Description
Vlan Mode	Display the IGMP snooping VLAN mode
Vlan ID	Display the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Display the IGMP snooping VLAN stats
Discard Unknown	Display the IGMP snooping VLAN discasrd unknown stats
Report Suppression	Display the IGMP snooping VLAN report suppression stats
Fast Leave	Display the IGMP snooping VLAN fast leave stats
Version	Display the IGMP snooping VLAN version
Last Member Query Interval	Display the IGMP snooping VLAN last member query interval
Operation	Display that IGMP snooping VLAN table entries can be edited

If you want to modify the configuration to specify IGMP snooping VLAN, please click “Edit” button, the operation shown in figure 11, modify the specified IGMP snooping VLAN page appears, as shown in figure 12.

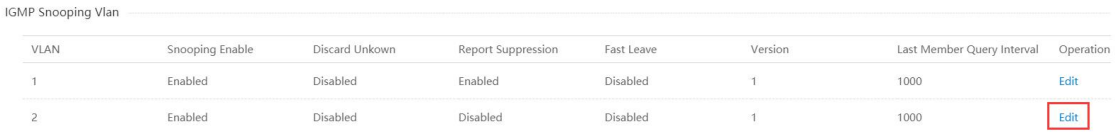


Figure 11 Modify IGMP snooping VLAN operation

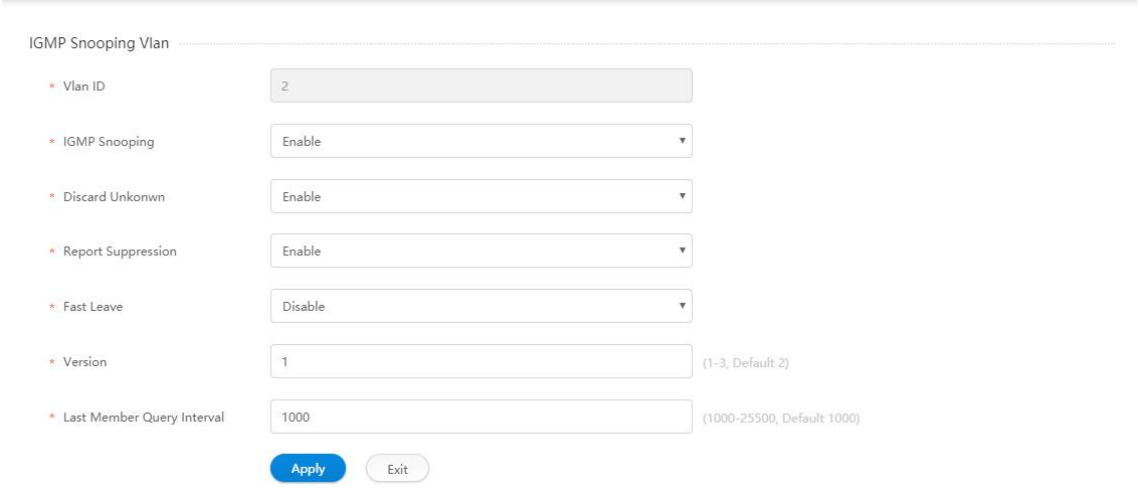


Figure 12 Modify IGMP snooping VLAN

- Parameter usage

Item	Description
Vlan Mode	Display the IGMP snooping VLAN mode(all VLAN or single VLAN)
Vlan ID	Set the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Set the IGMP snooping VLAN stats
Discard Unknown	Set the IGMP snooping VLAN discasrd unknown stats
Report Suppression	Set the IGMP snooping VLAN report suppression stats
Fast Leave	Set the IGMP snooping VLAN fast leave stats
Version	Set the IGMP snooping VLAN version
Last Member Query Interval	Set the IGMP snooping VLAN last member query interval

If you want to modify parameters configuration of IGMP snooping VLAN, you can follow the following steps:

(1) Select the IGMP snooping VLAN stat in the “IGMP Snooping” dropdown box.

(2) Select the IGMP snooping discard unknown stat in the “Discard Unknown” dropdown box.

(3) Select the IGMP snooping report suppression stat in the “Report Suppression” dropdown box.

(4) Select the IGMP snooping VLAN fast leave stat in the “Fast Leave” dropdown box.

(5) Enter the IGMP snooping VLAN version in the “Version” textbox.

(6) Enter the IGMP snooping VLAN last member query interval in the “Last Member Query Interval” textbox.

(7) Click the “Apply” button to configure IGMP snooping VLAN parameters.

(8) Click the “Apply” button to confirm configure IGMP snooping VLAN parameters.

The operation is shown in figure 13.

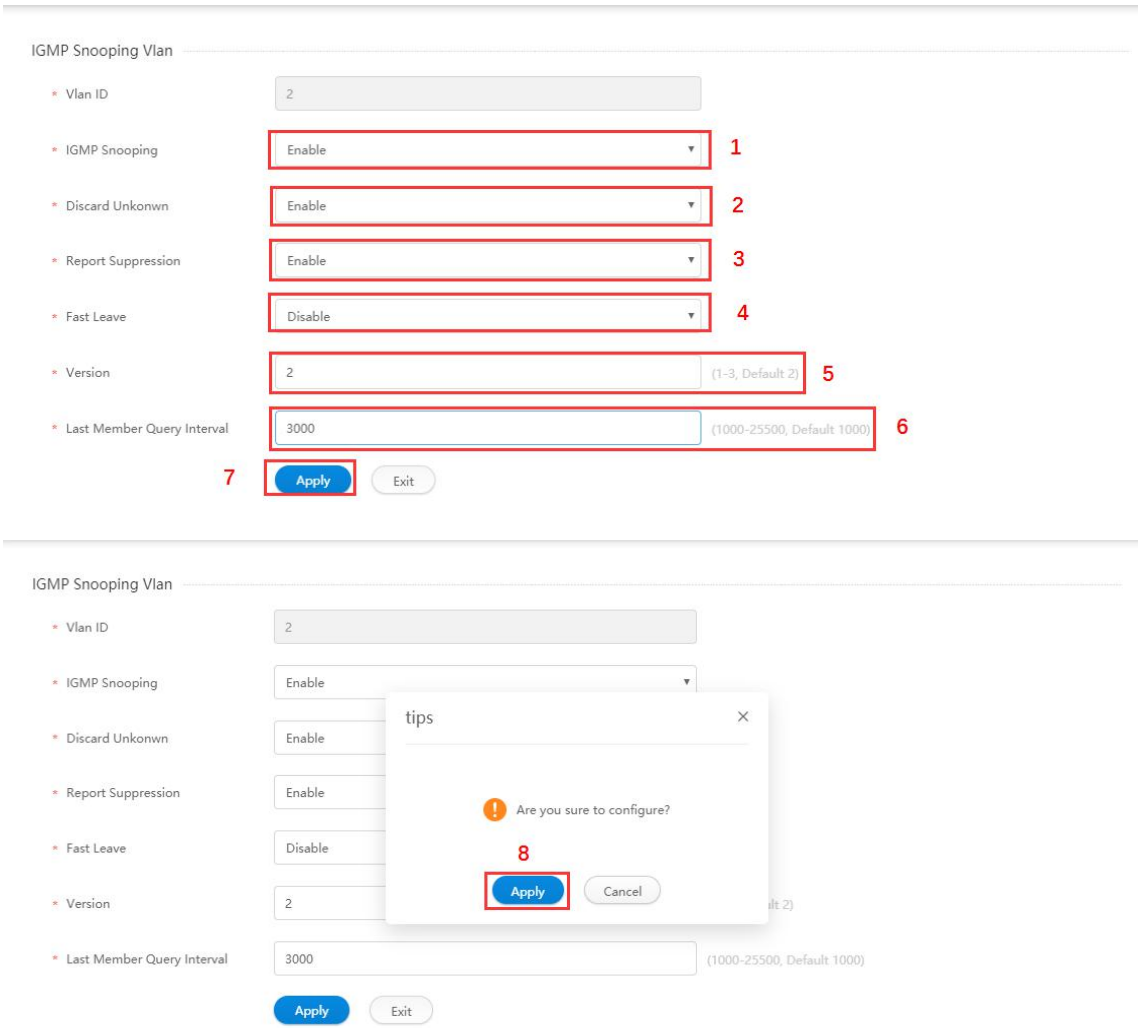


Figure 13 Modify IGMP snooping VLAN

15. QOS

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

If you click “Configuration ->QOS” in the top control bar, the QOS configuration list page appears, as shown in figure 1.

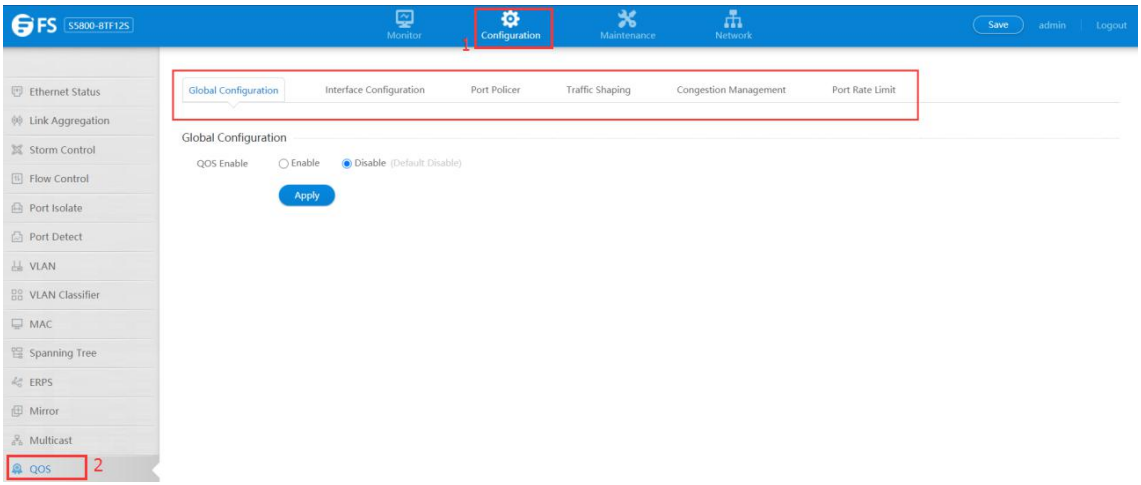


Figure 1 QOS list

15.1 Global Configuration

This section is used to enable or disable QOS global.

15.1.1 Current QOS Status

If you want to check QOS status on switch,you can click “QOS-> Global Configuration” in the title bar, the global configuration page appears, as shown in figure 2.

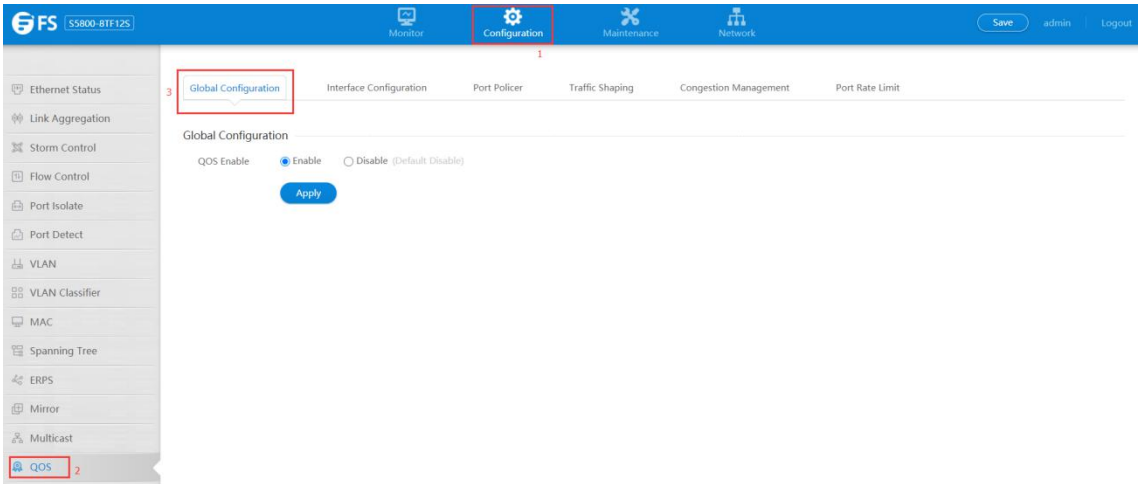


Figure 2 Global configuration

- Parameter usage

Item	Description
Enable	Enable QOS globally
Disable	Disable QOS globally

If you want to change QOS status, please click to turn on or off, after that, click "Apply" to enable or disable QOS globally, the operation is shown in figure 3.

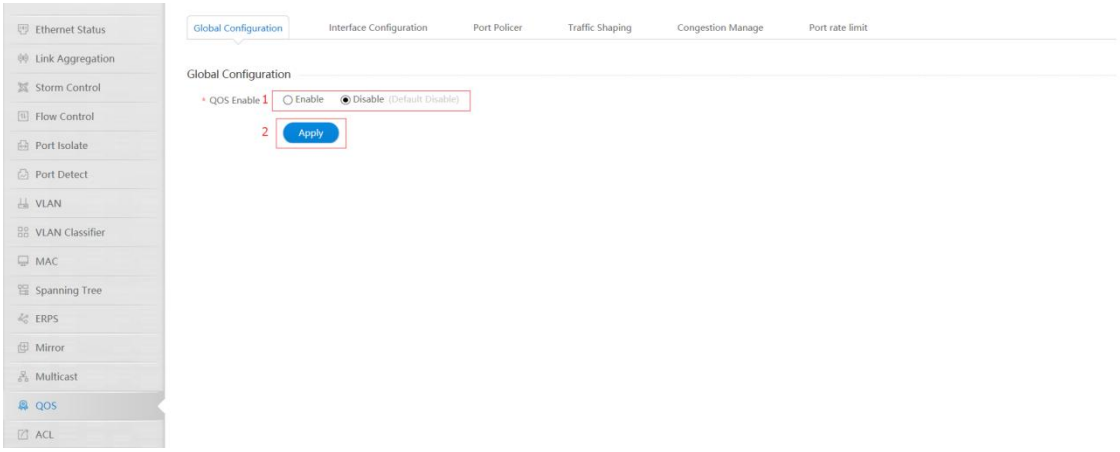


Figure 3 Change QOS status operation

15.2 Interface Configuration

This section mainly describes how to view and configure QOS property on interface.

15.2.1 Interface Configuration View

If you click "QOS -> Interface Configuration" in the title bar, the QOS interface configuration page appears, as shown in figure 4.

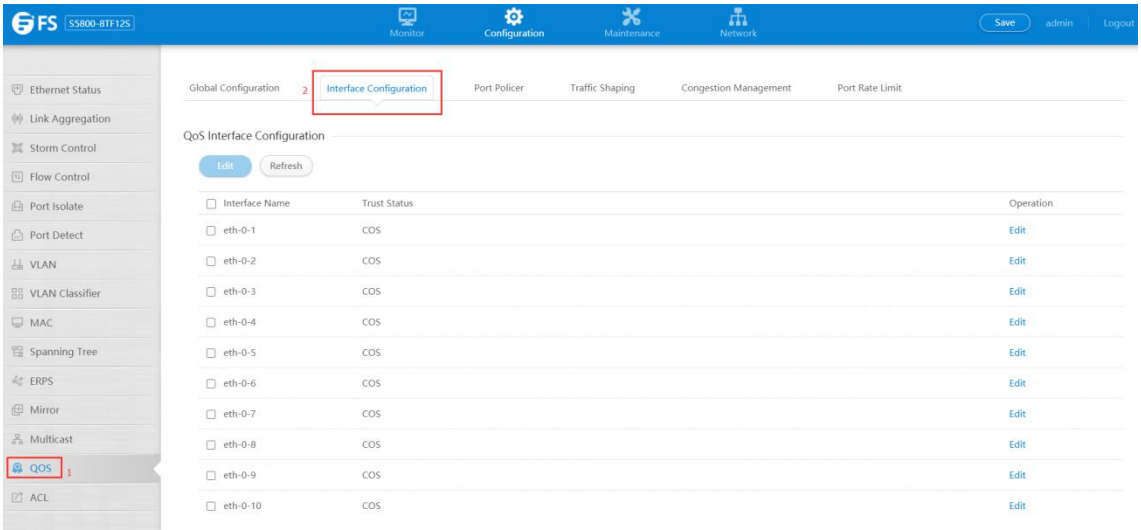


Figure 4 QOS interface configuration

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Replace COS	Display enable or disable replace the cos field in packets on egress
Replace DSCP	Display enable or disable replace the dscp field in packets on egress
Trust Status	Display the trust type on port
Operation	Display that interface entries can be edited

15.2.2 Interface Attribute Configuration

If you want to enter the interface attribute configuration page, you can follow the following steps:

(1) Select this specified Interface which you want to configure.

(2) Click “Edit” button.

The operation is shown in figure 5. and then the interface QOS configuration page appears, as shown in figure 6.

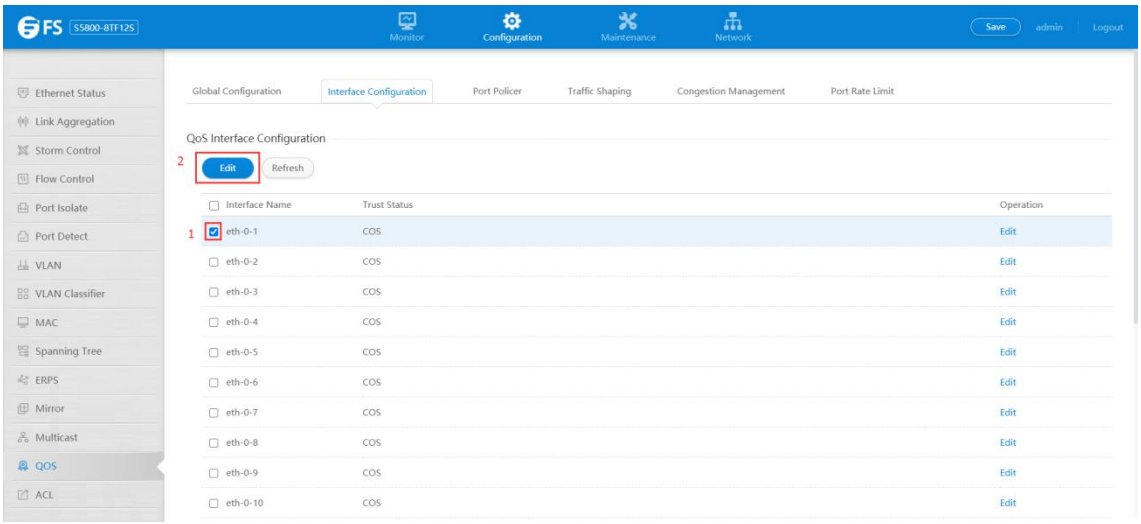


Figure 5 Interface QOS configuration operation

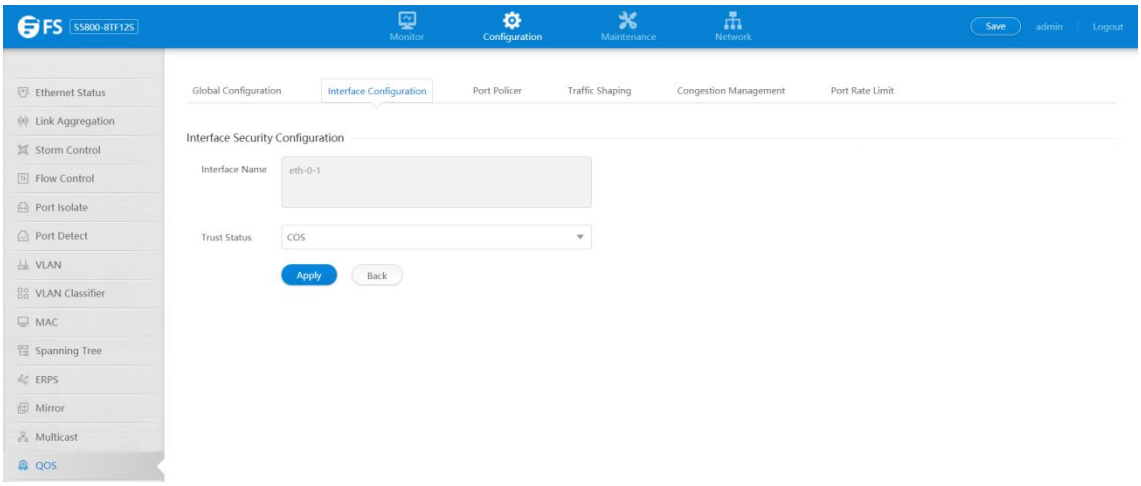


Figure 6 Interface QOS configuration

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Trust	Set trust type on port

If you want to modify the trust status, you can follow the following steps:

(1) Select the Trust type in the "Trust Status" dropdown box.

(2) Click the "Apply" button to apply all the property.

The operation is shown in figure 7, trust status configuration success table entry is shown in figure 8.

Figure 7 Modify the trust status configuration

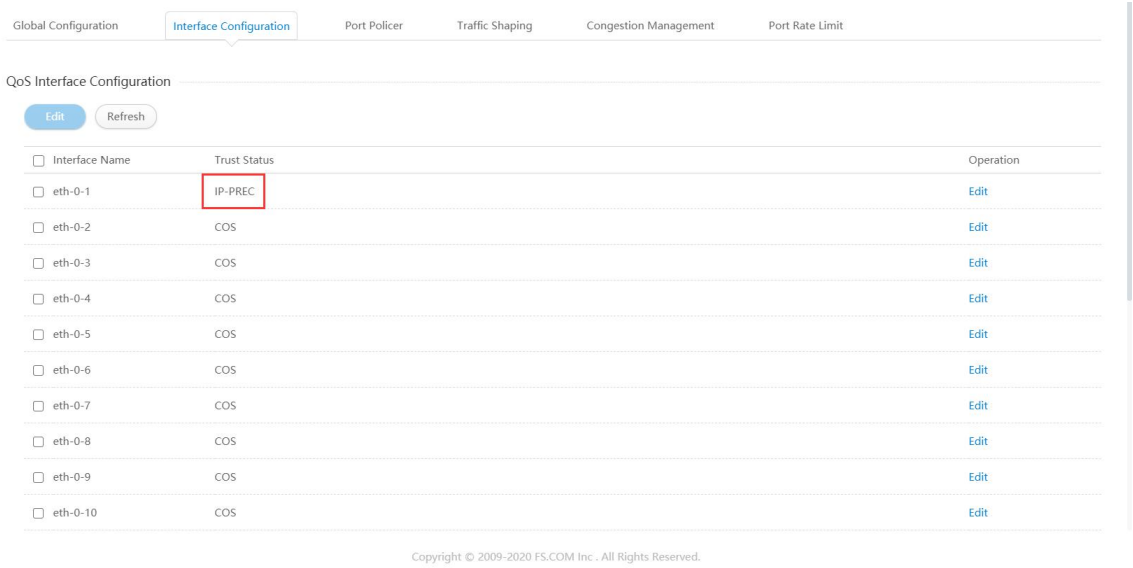


Figure 8 Trust status configuration information

15.3 Port Policer

This section mainly describes how to view and configure port policer for an interface matching all traffic transmitted and received in different direction.

15.3.1 Port Policer View

If you click “QOS -> Port Policer” in the title bar, the QOS port policer configuration page appears, as shown in figure 9.

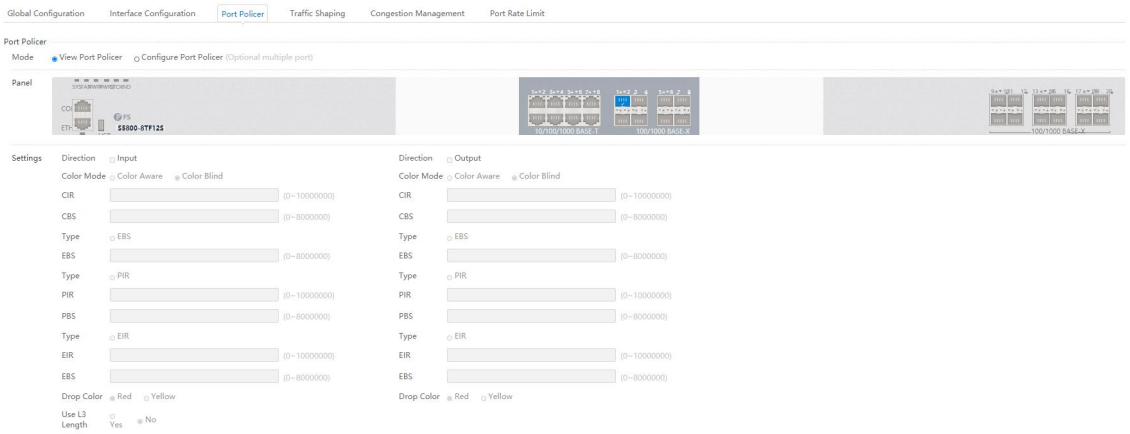


Figure 9 QOS port policer configuration

- Parameter usage

Item	Description
Direction	Choose the direction to limit the traffic entering the interface
Color Mode	Choose color aware or color blind mode policer
CIR	Commit Information Rate with the range of 0 to 10,000,000 kbps
CBS	Commit Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose EBS
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose PIR
PIR	Peak Information Rate with the range of 0 to 10,000,000 kbps
PBS	Peak Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose EIR
EIR	Excess Information Rate with the rang of 0 to 10,000,000 kbps
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes
Drop Color	Drop color configuration includes yellow and red
Use L3 Length	Use layer 3 length for policing

15.3.2 Modify Port Policer

If you want to modify the port policer configuration, please click “Configure Congestion” button, the operation is shown in figure 10. and then the port policer configure page appears, as shown in figure 11.

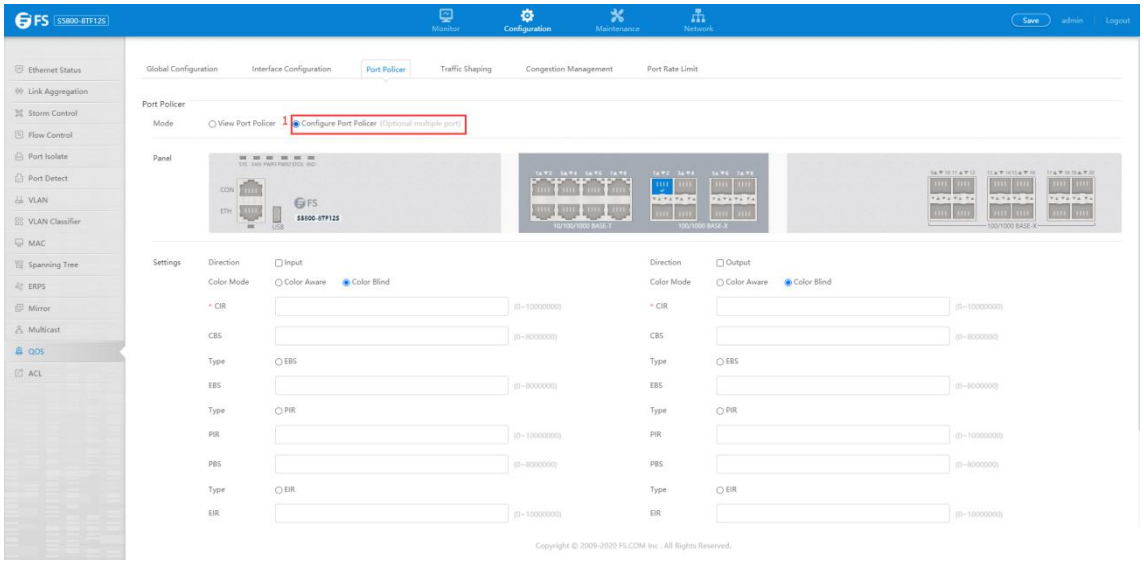


Figure 10 Port policer configure operation

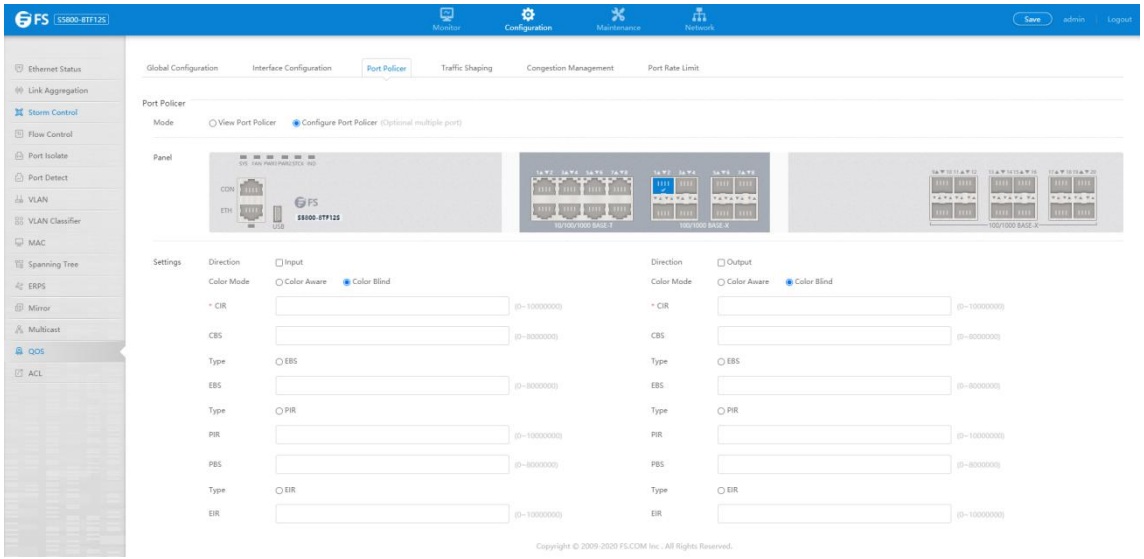


Figure 11 Port policer configure

- Parameter usage

Item	Description
Direction	Choose the direction to limit the traffic entering the interface
Color Mode	Choose color aware or color blind mode policer
CIR	Commit Information Rate with the range of 0 to 10,000,000 kbps
CBS	Commit Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose EBS
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose PIR
PIR	Peak Information Rate with the range of 0 to 10,000,000 kbps

Item	Description
PBS	Peak Burst Size with the range of 0 to 8,000,000 bytes
Type	Choose EIR
EIR	Excess Information Rate with the rang of 0 to 10,000,000 kbps
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes
Drop Color	Drop color configuration includes yellow and red
Use L3 Length	Use layer 3 length for policing

If you want to modify the port policer, you can follow the following steps:

(1) Choose one port to display the configuration information.

(2) Choose the direction to limit the traffic entering the interface.

(3) Choose color aware or color blind mode policer.

(4) Commit Information Rate with the range of 1 to 10,000,000 kbps.

(5) Commit Burst Size with the range of 0 to 16,000 bytes.

(6) Choose type of EBS or PIR or EIR.

(7) Configure parameters of QoS on port.

(8) Choose drop color configuration includes yellow and red.

(9) Choose whether use layer 3 length for policing.

(10) Click the "Apply" button to apply all the property.

The operation is shown in figure 12, port policer configuration success table entry is shown in figure 13.

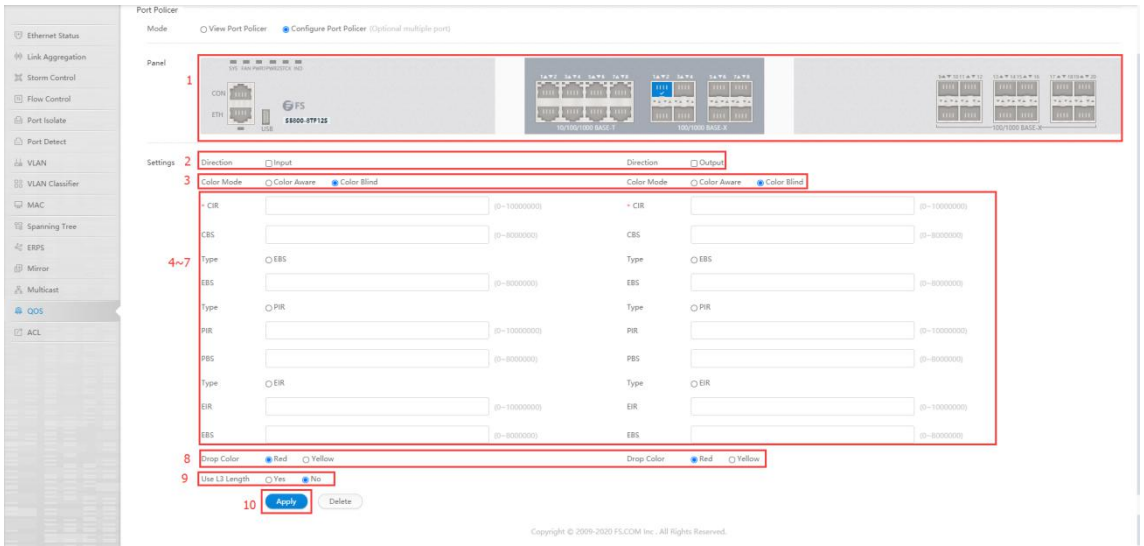


Figure 12 Modify the port policer configuration

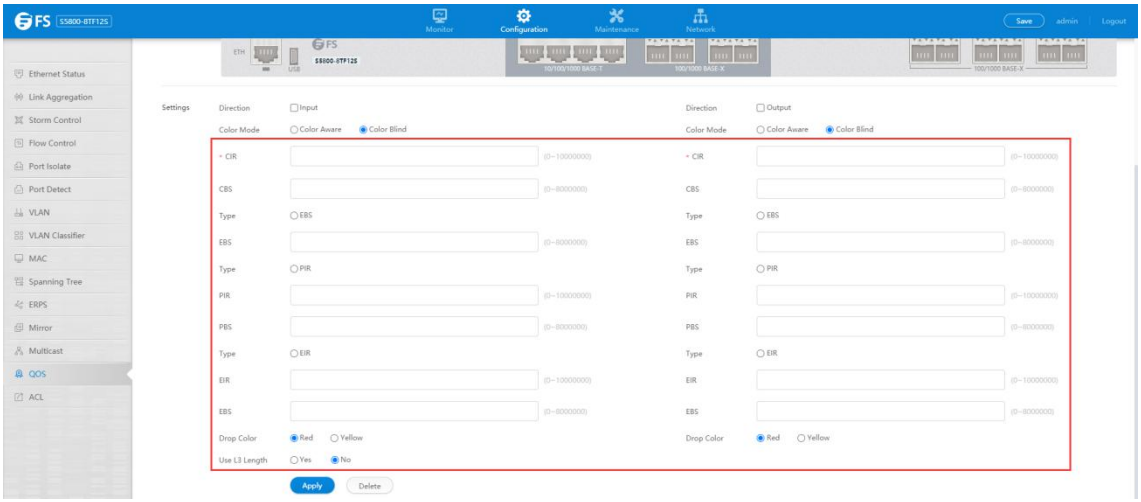


Figure 13 Port policer configuration information

15.4 Traffic Shaping

This section mainly describes how to view and configure shaping for a queue of a port in absolute value mode.

15.4.1 Traffic Shaping View

If you click “QOS ->Traffic Shaping” in the title bar, the QOS traffic shaping configuration page appears, as shown in figure 14.

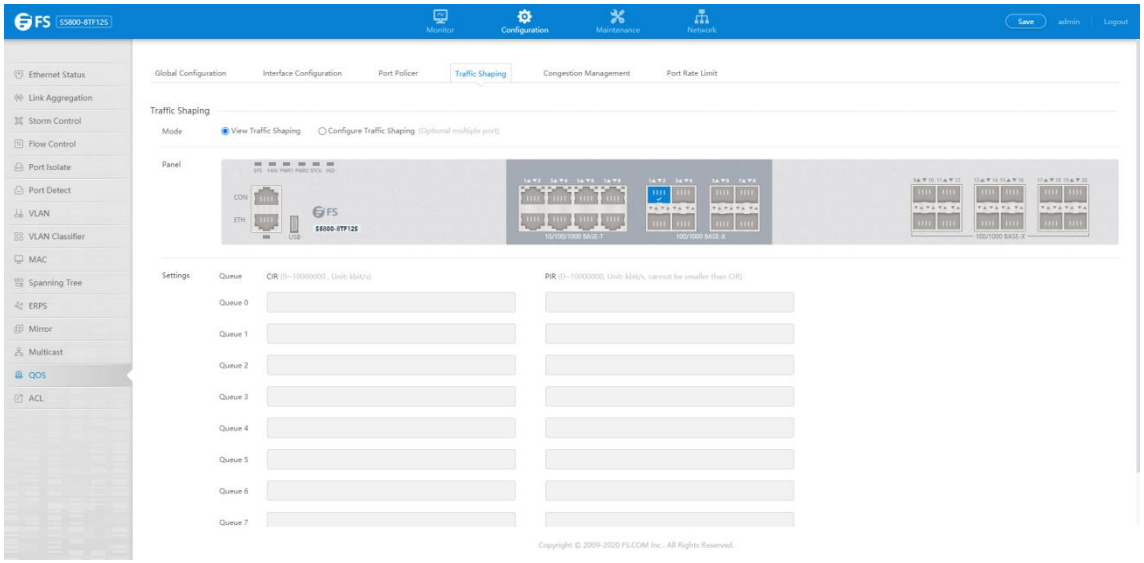


Figure 14 QOS traffic shaping configuration

- Parameter usage

Item	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
CIR	The value for commit information rate with the range of 0 to 10,000,000
PIR	The value for peak information rate with the range of 0 to 10,000,000. If this value is omitted, it will be same as cir

15.4.2 Modify Traffic Shaping

If you want to modify the Traffic Shaping configuration, please click “Configure Congestion” button,the operation is shown in figure 15. And then the traffic shaping configure page appears, as shown in figure 16.

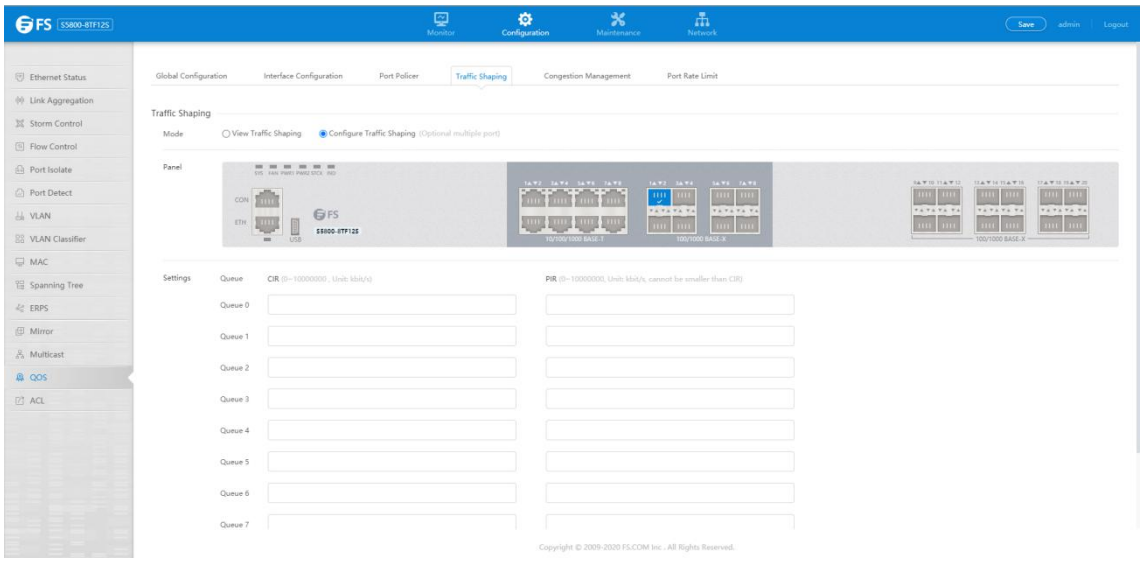


Figure 15 Traffic shaping configure operation

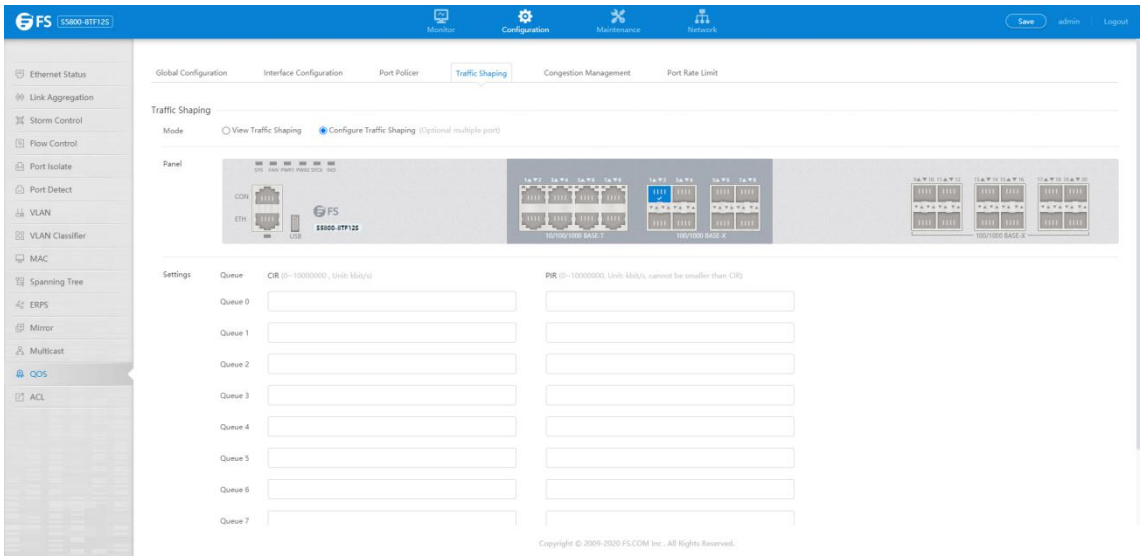


Figure 16 Traffic shaping configure

- Parameter usage

Item	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
CIR	The value for commit information rate with the range of 0 to 10,000,000
PIR	The value for peak information rate with the range of 0 to 10,000,000. If this value is omitted, it will be same as cir

If you want to modify the traffic shaping, you can follow the following steps:

(1) Choose one port to display the configuration information.

(2) Modify Queue Settings.

(3) Click the "Apply" button to apply all the property.

The operation is shown in figure 17, traffic shaping configuration success table entry is shown in figure 18.

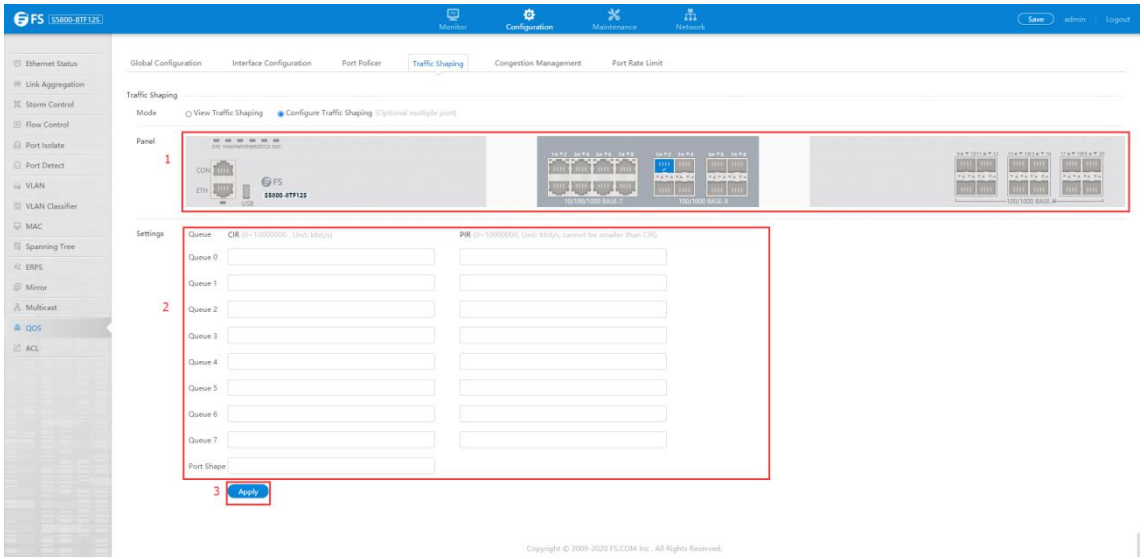


Figure 17 Modify the traffic shaping configuration

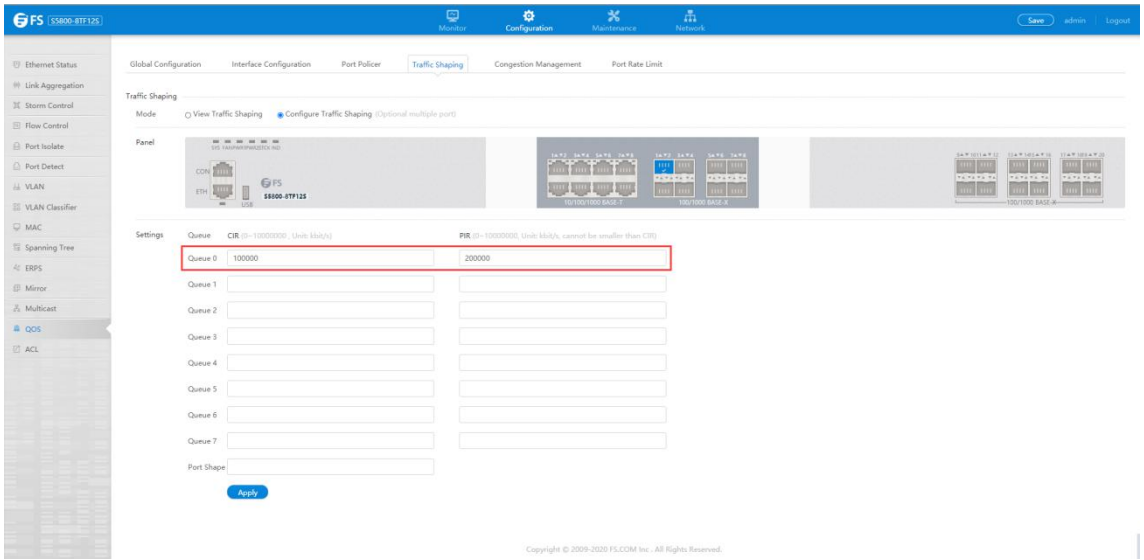


Figure 18 Traffic shaping configuration information

15.5 Congestion Manage

This section mainly describes how to view and configure the WDRR scheduling weight and class for each queue.

15.5.1 Congestion Manage View

If you click "QOS ->Congestion Manage" in the title bar, the QOS congestion manage configuration page appears, as shown in figure 19.

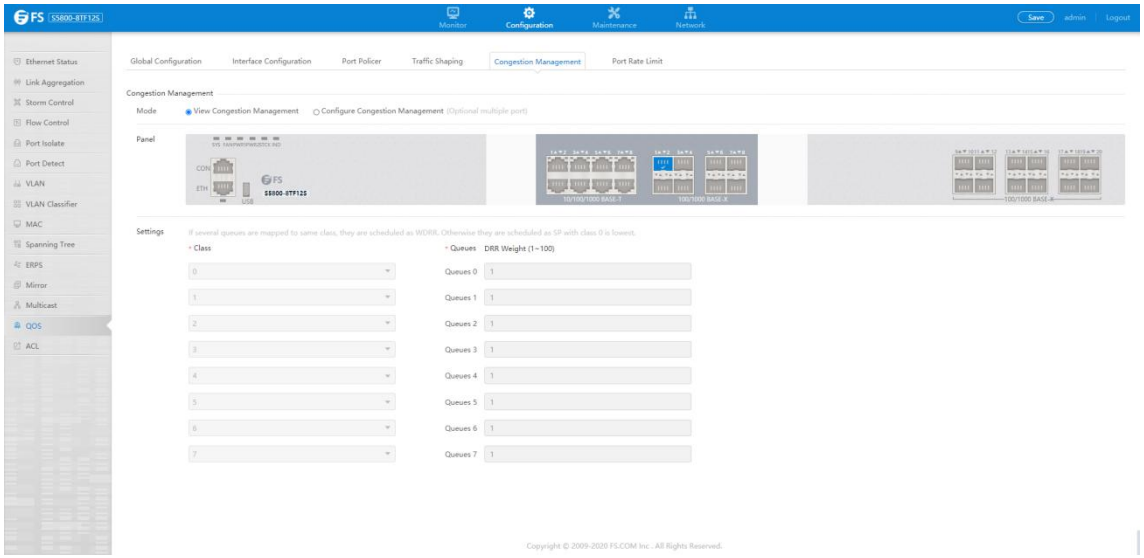


Figure 19 QOS congestion manage configuration

- Parameter usage

Item	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
Class	The class level of queue with the range of 0 to 7
DRR Weight	The value of DRR weight with the range of 1 to 100

15.5.2 Modify Congestion Manage

If you want to modify the congestion manage configuration, please click “Configure Congestion” button,the operation is shown in figure 20. and then the congestion manage configure congestion page appears, as shown in figure 21.

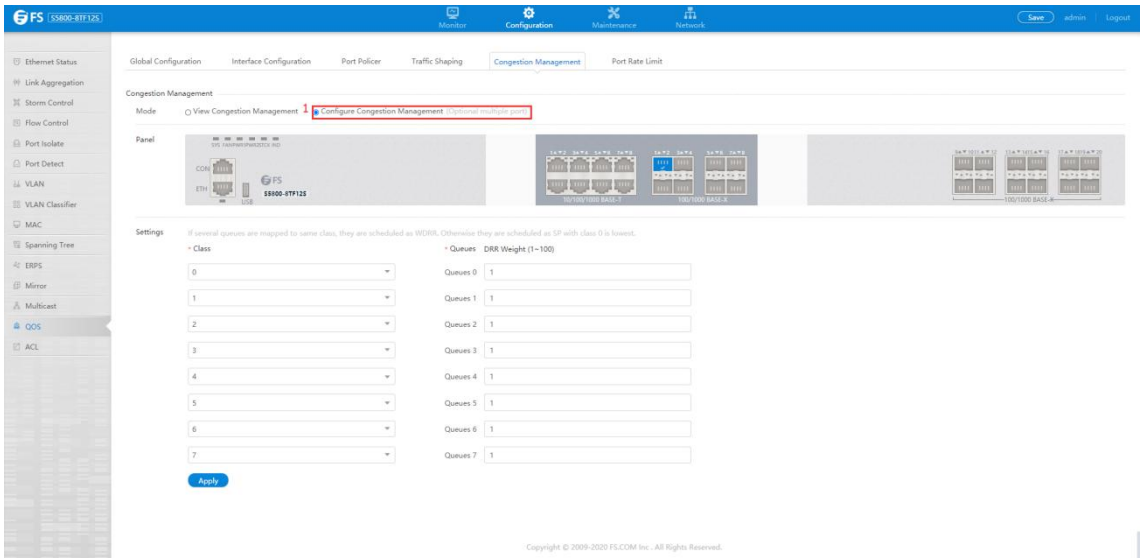


Figure 20 Congestion manage configure operation

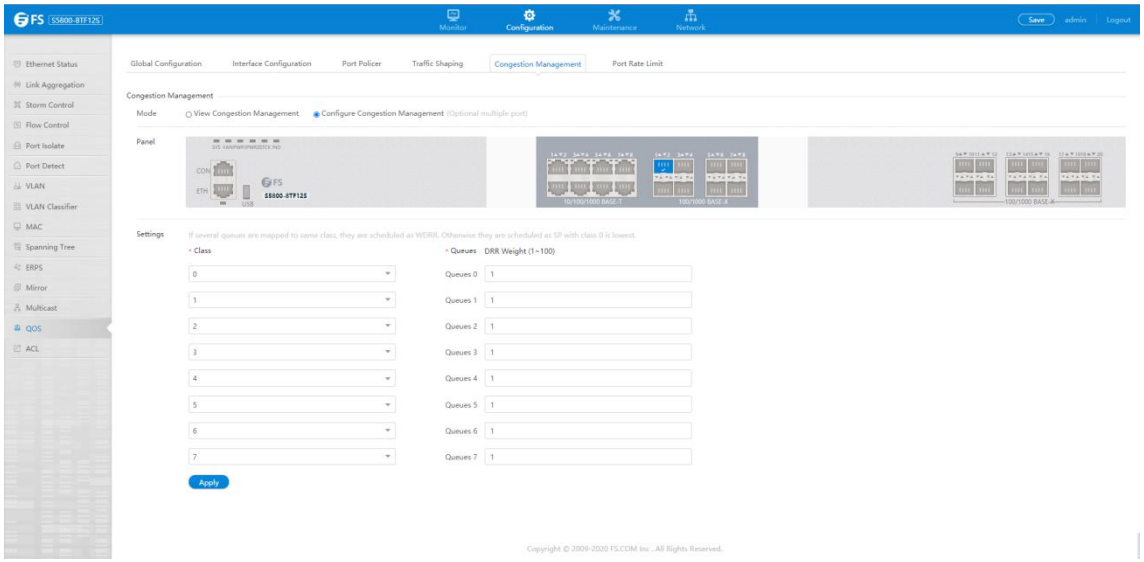


Figure 21 Congestion manage configure

- Parameter usage

Item	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
Class	The class level of queue with the range of 0 to 7
DRR Weight	The value of DRR weight with the range of 1 to 100

If you want to modify the congestion manage, you can follow the following steps:

(1) Choose one port to display the configuration information.

(2) Modify Class Settings.

(3) Modify DRR Weight Settings.

(4) Click the “Apply” button to apply all the property.

The operation is shown in figure 22, congestion manage configuration success table entry is shown in figure 23.

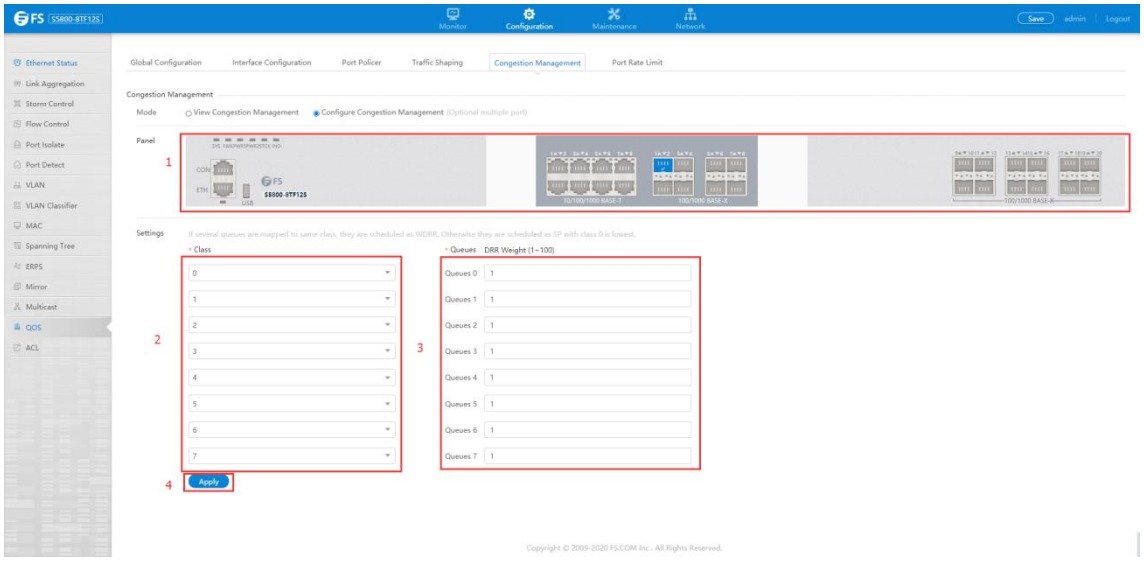


Figure 22 Modify the congestion manage configuration

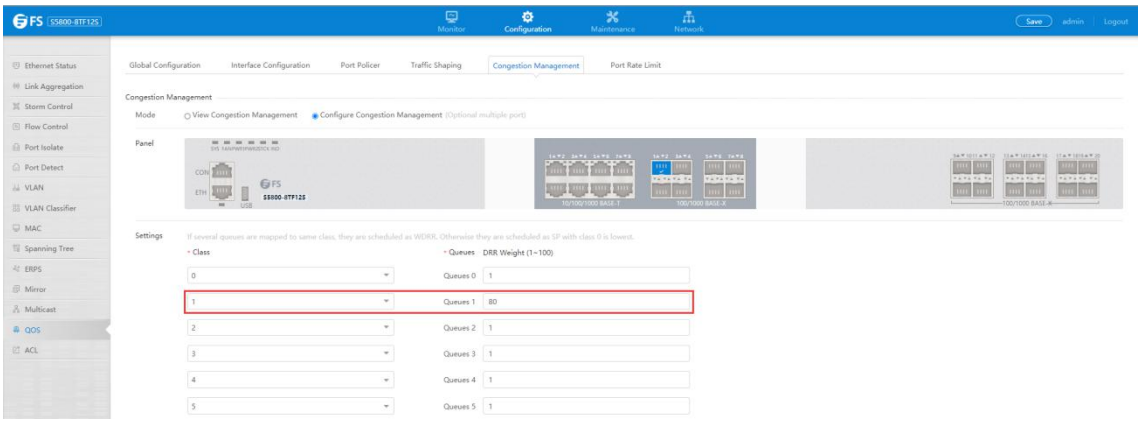


Figure 23 Congestion manage configuration information

15.6 Port Rate Limit

This section mainly describes how to view and configure port rate limit.

15.6.1 Port Rate Limit View

If you click "QOS ->Port rate limit" in the title bar, the port rate limit configuration page appears, as shown in figure 24.

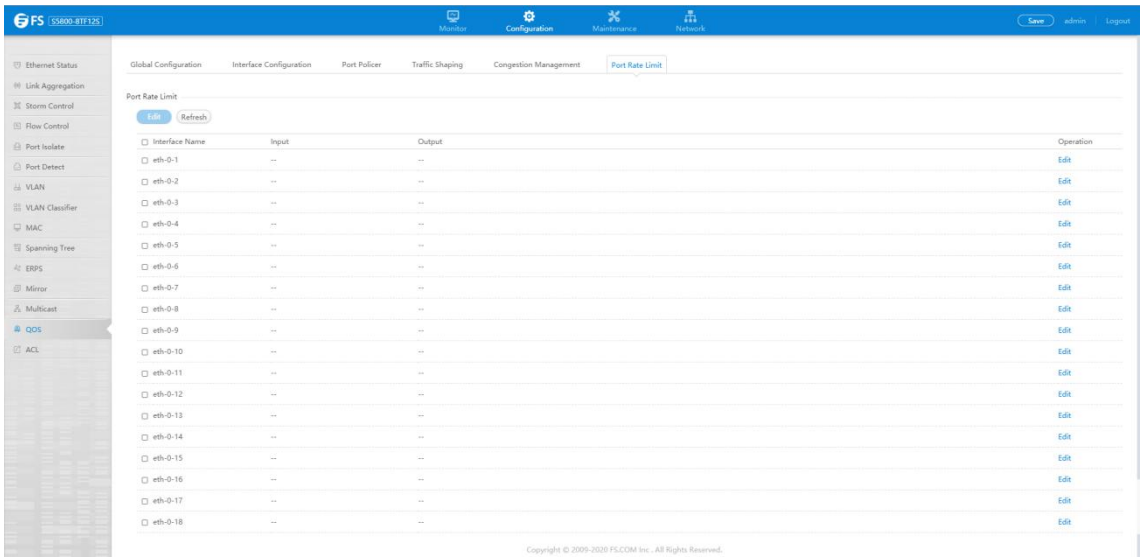


Figure 24 Port rate limit configuration

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Input	Input speed limit, range 8-10 million, unit kbps
Output	Output speed limit, range 8-10 million, unit kbps
Operation	Display that static routing table entries can be edited

15.6.2 Modify Port Rate Limit

Follow the following steps, you can enter the port rate limit configuration page:

(1) Select this specified Interface which you want to configure.

(2) Click “Edit” button.

The operation is shown in figure 25. and then the port rate limit configure page appears, as shown in figure 26.

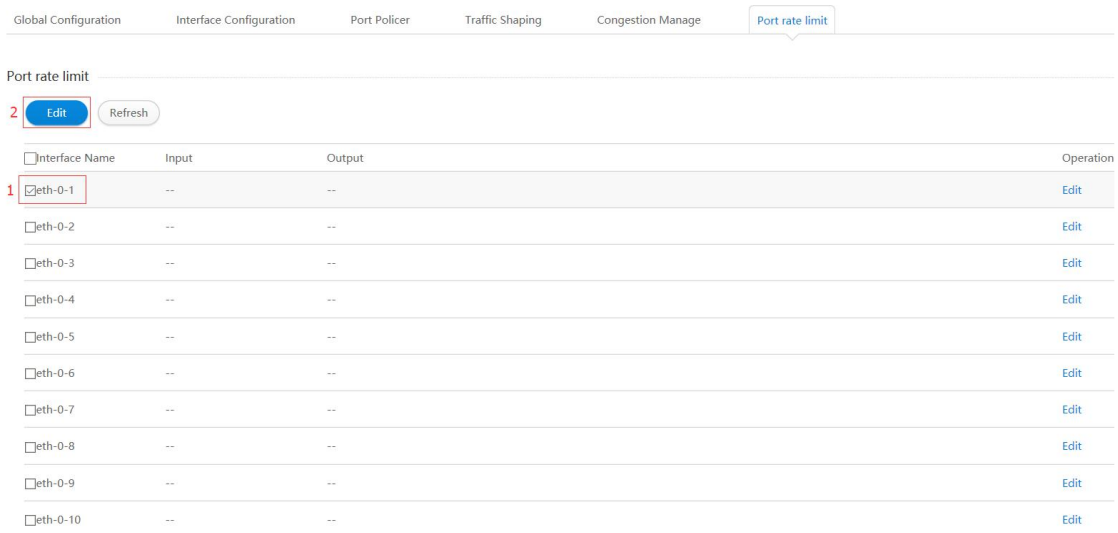


Figure 25 Port rate limit configure operation

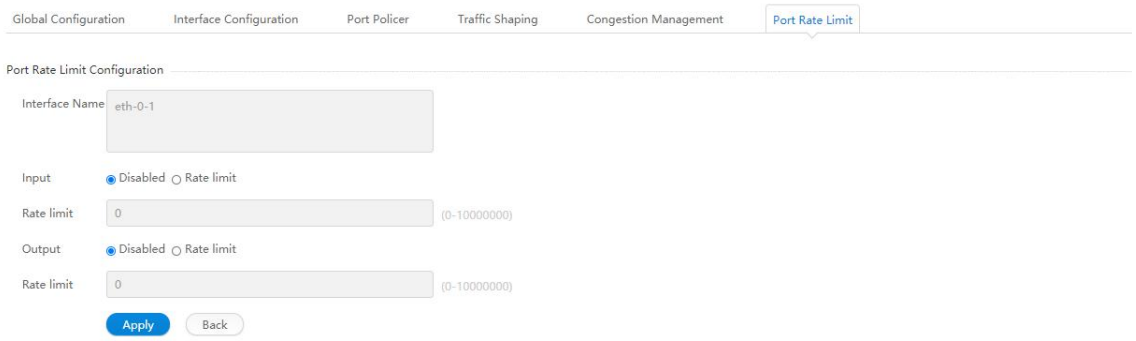


Figure 26 Port rate limit configuration

- Parameter usage

Item	Description
Interface Name	Display the number of interface
Input	Input speed limit, range 8-10 million, unit kbps
Output	Output speed limit, range 8-10 million, unit kbps

If you want to modify the port rate limit, you can follow the following steps:

(1) Choose Disbale or Rate limit in the “Input” radio button.

(2) Enter rate in the “Rate limit” textbox.

(3) Choose Disbale or Rate limit in the “Output” radio button.

(4) Enter rate in the “Rate limit” textbox.

(5) Click the “Apply” button to apply all the property.

The operation is shown in figure 27, port rate limit configuration success table entry is shown in figure 28.

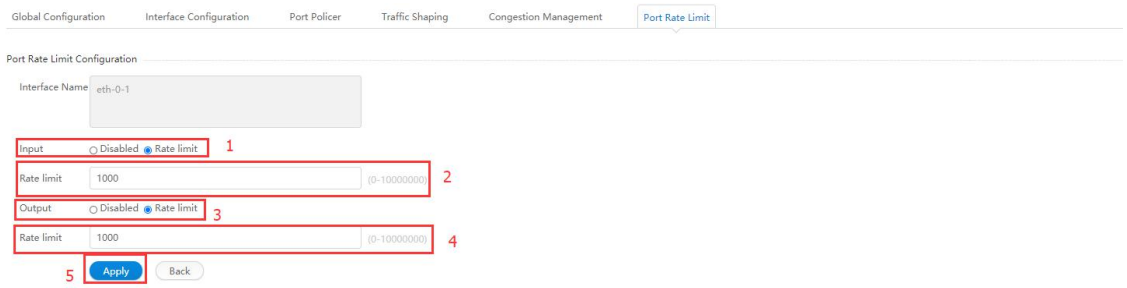


Figure 27 Modify the port rate limit configuration

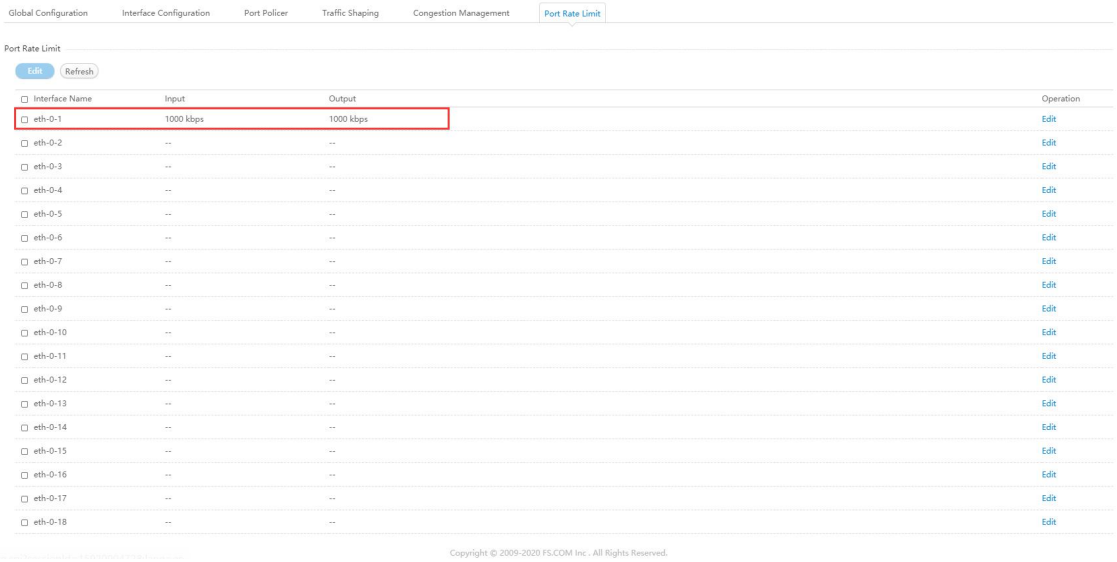


Figure 28 Port rate limit configuration information

16. ACL

If you click “Configuration -> ACL” in the top control bar, the ACL configuration list page appears, as shown in figure 1.

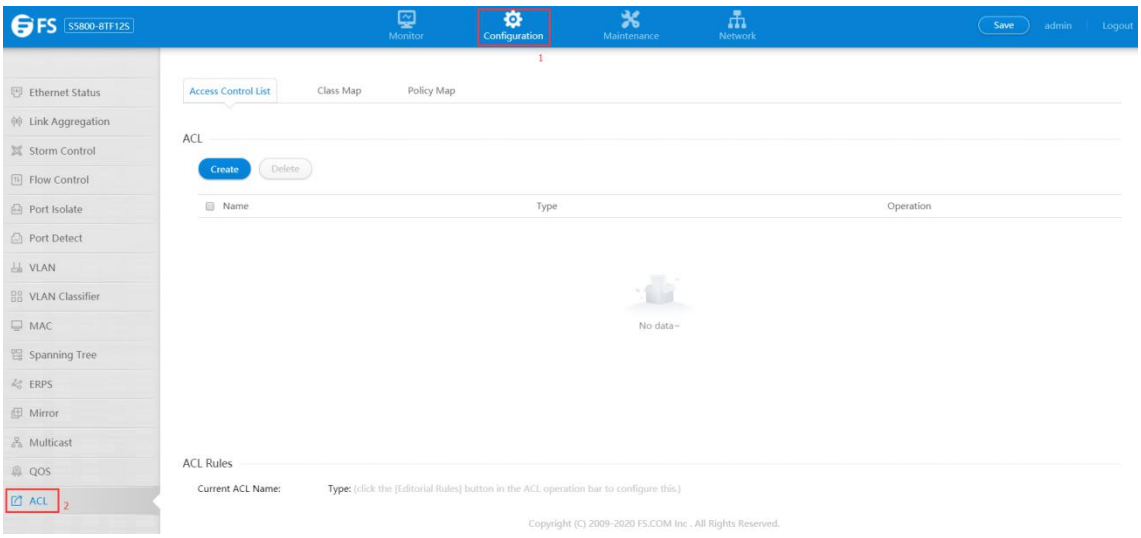


Figure 1 ACL information

16.1 Access Control List

If you click “ACL -> Access Control List” in the top control bar, the access control list configuration list page appears, as shown in figure 2.

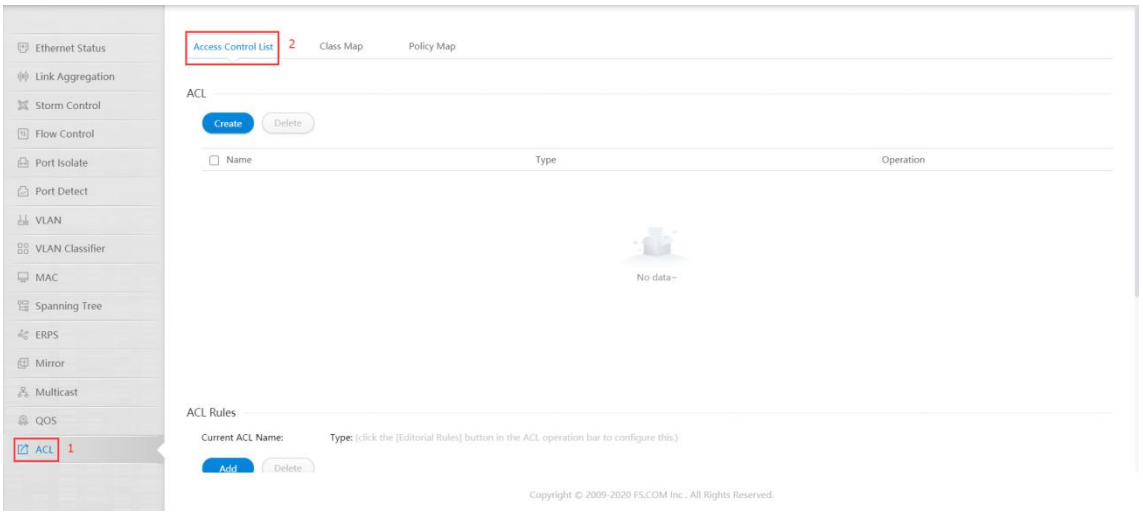


Figure 2 Access control list information

16.1.1 ACL Configuration

ACL provide two basic configuration functions, creating and removing ACL.

If you want to create an ACL, here are the steps:

If you click the “Create” button, you can create ACL. The operation is shown in Figure 3, and then the ACL configuration page appears, as shown in Figure 4.

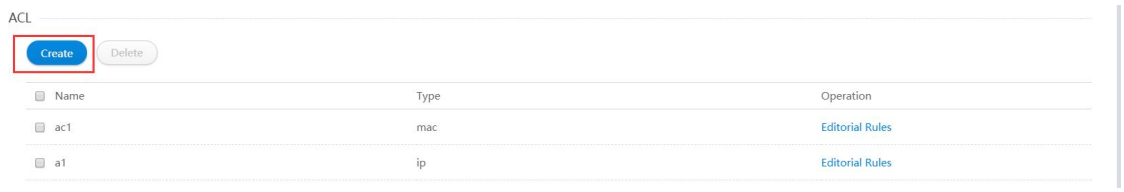


Figure 3 ACL creation process

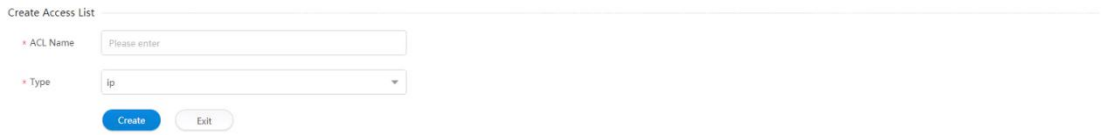


Figure 4 ACL create page

- Parameter usage

Item	Description
ACL Name	Enter the acl name
Type	Select the acl type

If you want to configure ACL, perform the following steps:

(1) In the "ACL name" text box, enter ACL name.

(2) Select the type in the "type " drop-down box.

(3) Click "Create " button.

(4) Confirm the submission configuration and click the "Create " button.

The operation is shown in figure 5, and the ACL configuration success entry is shown in figure 6.

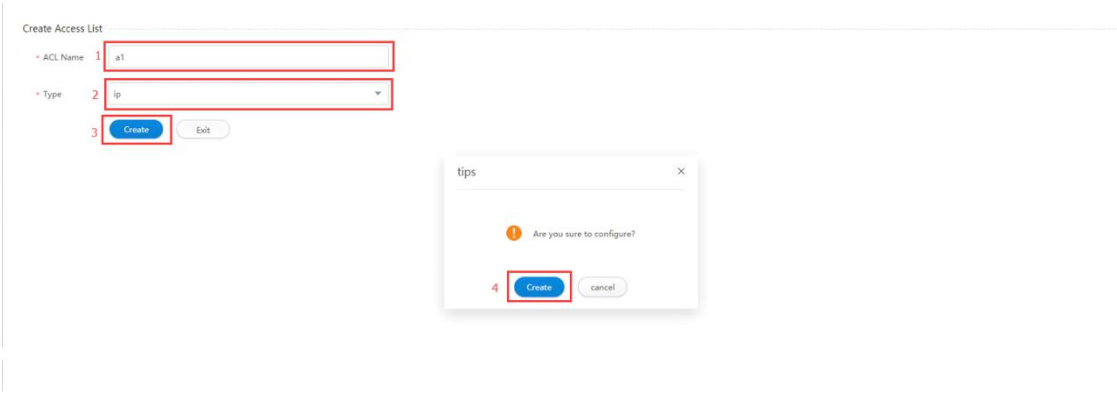


Figure 5 Create ACL configuration

Figure 6 New ACL information

If you want to delete the ACL, here are the steps:

(1) Click the checkbox to select ACL which are need to be deleted as the figure below.

(2) Click "Delete" button.

(3) After clicking "Delete", the page as shown in figure 7 appears, and if you click the "Confirm" button, you can delete it.

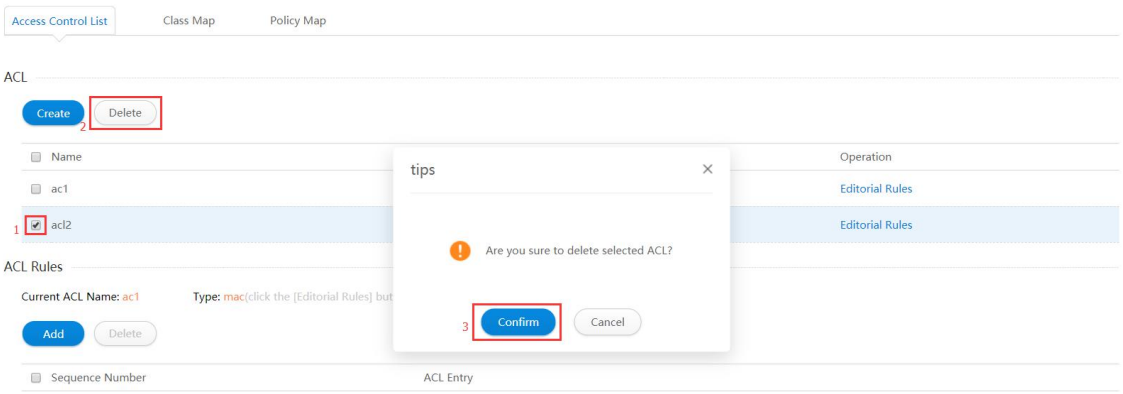


Figure 7 Delete ACL

16.1.2 ACL Rules

ACL rules provides two basic configuration functions: creating and deleting ACL rules.

If you want to create an ACL rules, here are the steps:

Click the blue "Editorial Rules" to select the ACL,choose MAC type as shown in figure 8,choose IP type as shown in figure 9, click "Add" to enter the ACL Rules configuration page, as shown in figure 10. Access different configuration pages depending on the type of ACL selected.The MAC type is shown in figure 11 and the IP type is shown in figure 12.

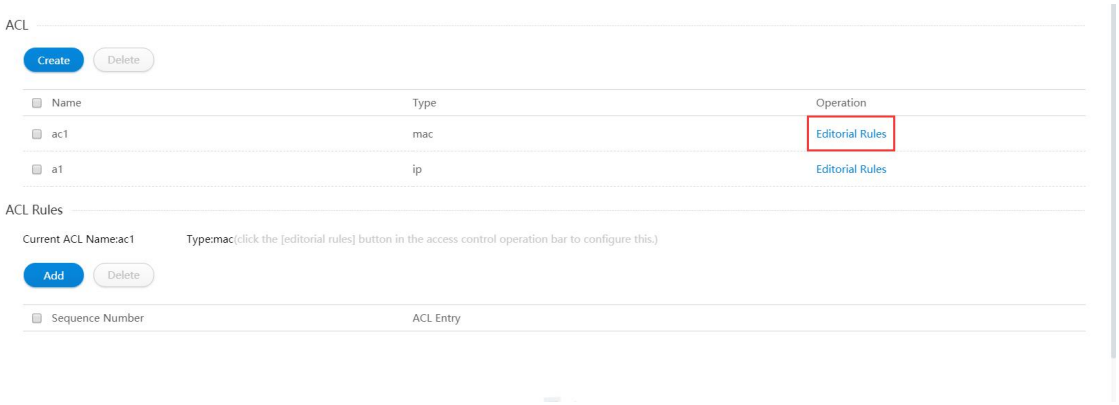


Figure 8 Select MAC type ACL

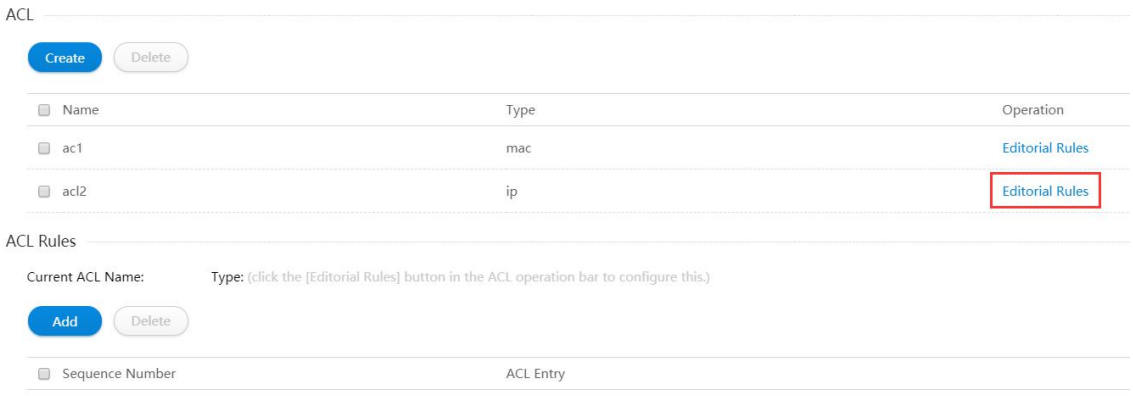


Figure 9 Select IP type ACL

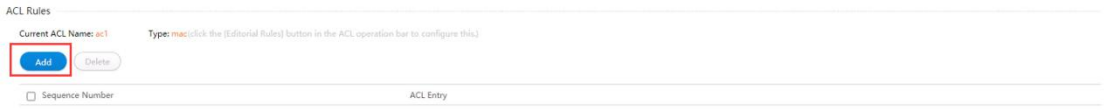


Figure 10 Add ACL operation

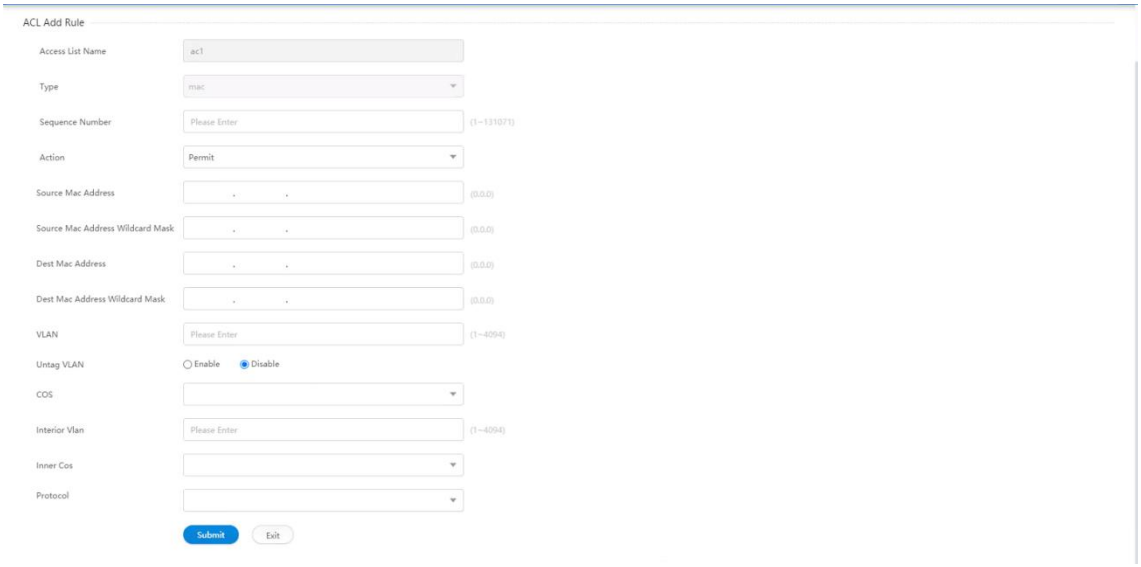


Figure 11 MAC ACL add rule

- Parameter usage

Item	Description
Sequence Number	The serial number of the filter in the MAC ACL. If this field is not displayed, it can be generated automatically
Action	Select the action of mac ACE
Source Mac Address	Enter the source MAC address
Source Mac Address Mask	Enter the source MAC address wildcard bits
Dest Mac Address	Enter the destination MAC address

Item	Description
Dest Mac Address Mask	Enter the destination MAC address wildcard bits
Vlan	Enter VLAN-ID, the range is 1 to 4094
Cos	Enter CoS, the range is 0 to 7
Inner Vlan	Enter Inner VLAN-ID, the range is 1 to 4094
Inner Cos	Enter Inner CoS, the range is 0 to 7
Protocol	Select the protocol type which including ARP, RARP or Ether type
Type	Select the L2 type including ETH2, SNAP, SAP

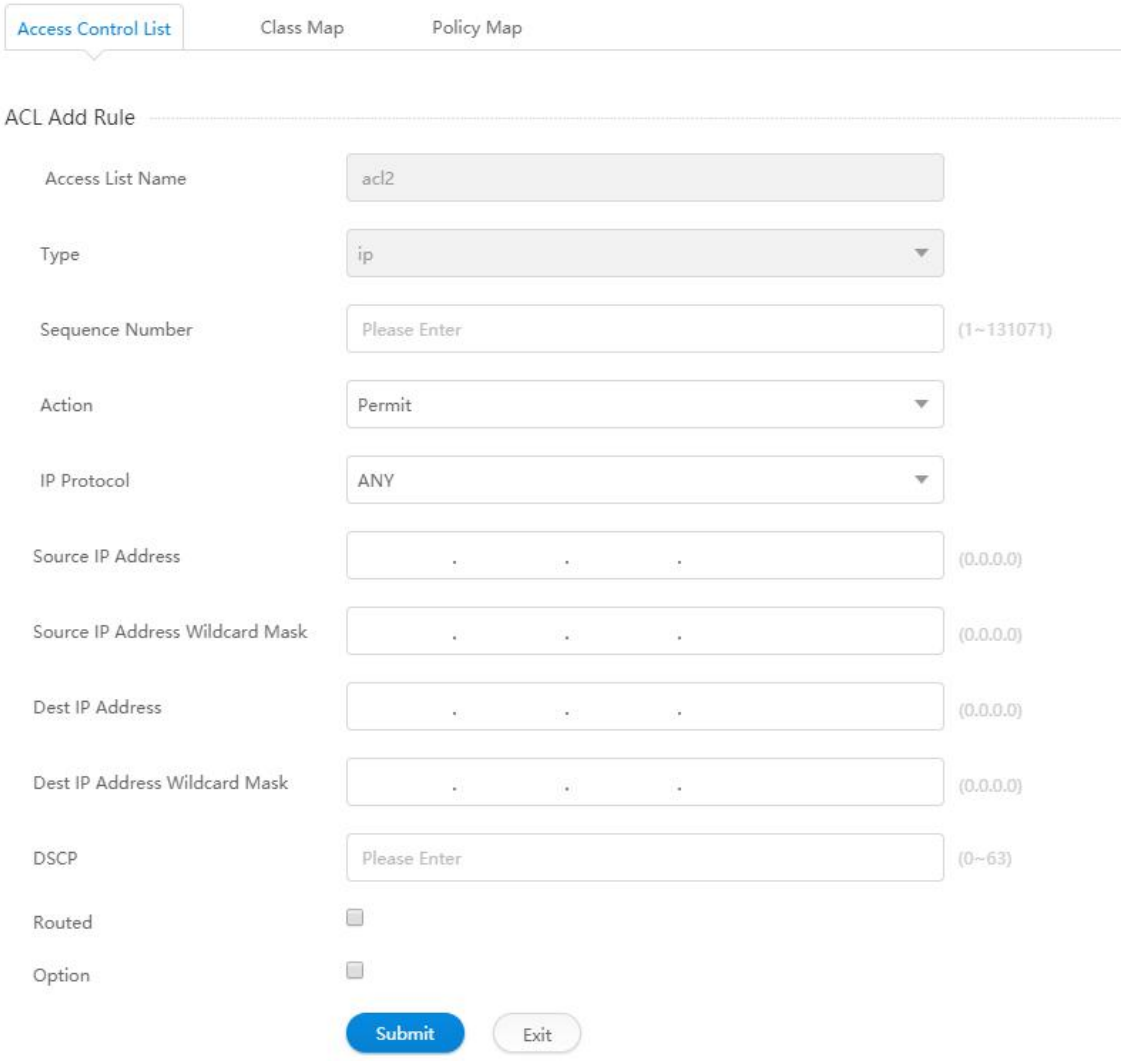


Figure 12 IP ACL add rule

- Parameter usage

Item	Description
Sequence Number	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented
Action	Select the action of IP ACE
IP Protocol	Select IP protocol of IP ACE
IP Protocol Num	Enter IP protocol number, the range is 0 to 255
Source IP Address	Enter the destination MAC address
Source IP Address Mask	Enter the destination MAC address wildcard bits
Dest IP Address	Enter VLAN-ID, the range is 1 to 4094
Dest IP Address Mask	Enter CoS, the range is 0 to 7
Source Port Type	Select source port type
Source Port Num	Enter source port number
Source Port Range	Enter source port range
Dest Port Type	Select destination port type
Dest Port Num	Enter destination port number
Dest Port Range	Enter destination port range
ICMP Type	Enter ICMP type, the range is 1 to 255
ICMP Code	Enter ICMP code, the range is 1 to 255
IGMP Type	Select IGMP type.
DSCP	Enter DSCP
Fragments	Select fragments
Routed	Select routed
option	Select option

The parameters that need to be configured are configured according to the actual requirements, the non-demanding parameters can be left unconfigured.If you want to configure ACL rules, perform the following steps:

(1) Enter VLAN in the “VLAN ” text box.

(2) Select arp in the “Protocol ” drop-down box.

(3) Click the submit to complete the configuration.

The operation is shown in figure 13, and ACL Rules is successfully configured as shown in figure 14.

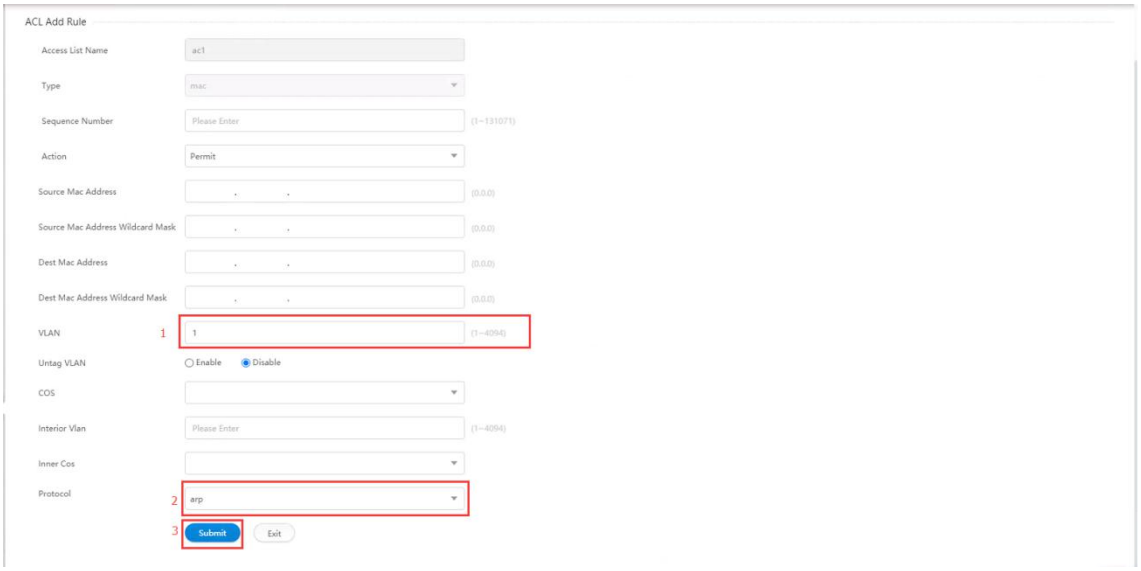


Figure 13 Add ACL rules

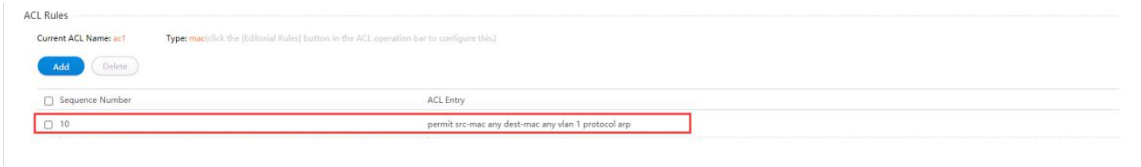


Figure 14 New ACL rules information

If you want to delete the ACL rules, here are the steps:

Click on the blue "Editorial Rules" to select the current ACL, as shown in figure 15.

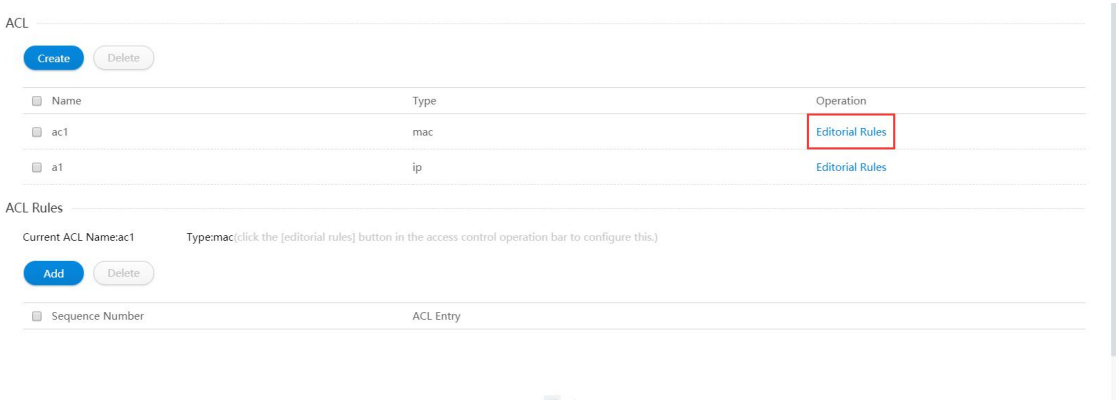


Figure 15 Select current ACL

If you want to delete the configuration, perform the following steps:

(1) Click the checkbox to select ACL rules which are need to be deleted as the figure below.

(2) Click “Delete” button.

(3) After clicking “Delete”, the page as shown in figure 16 appears, and if you click the “Confirm” button, you can delete it.

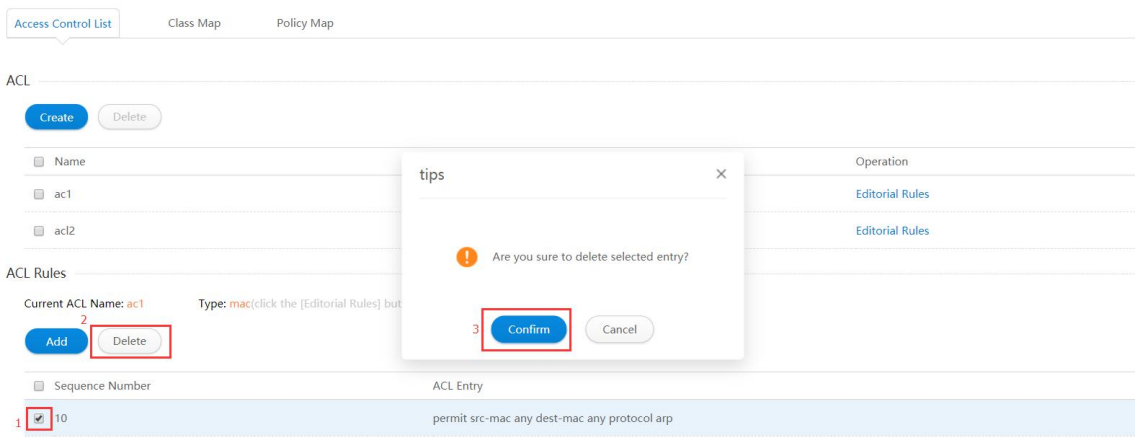


Figure 16 Delete ACL rules

16.2 Class Map

If you click “ACL -> Class Map” in the title bar , the class map page appears, as shown in figure 17.

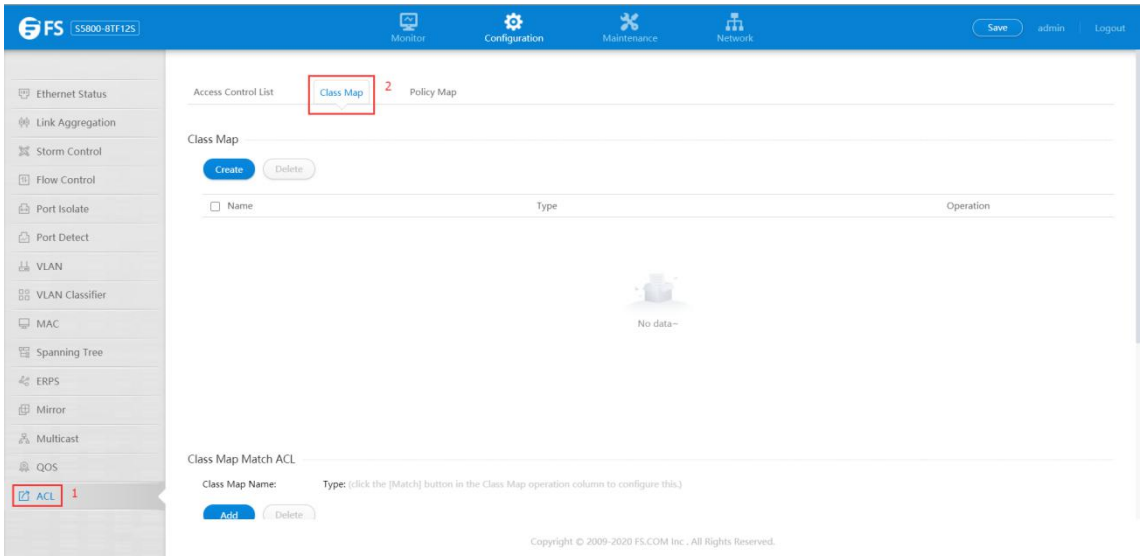


Figure 17 Class map page

16.2.1 Class map

Class map provide two basic configuration functions, creating and removing class map.

If you want to create an class map, here are the steps:

If you click the "Create" button, you can add class map, the operation is shown in figure 18, and then the class map configuration page appears, as shown in figure 19.

Figure 18 Add class map operation

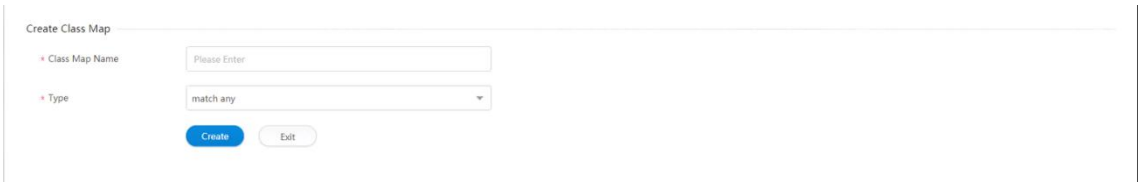


Figure 19 Add class map

- Parameter usage

Item	Description
Class Map Name	Enter the class map name
Type	Select the class map type

If you want to configure class map, perform the following steps:

(1) Enter class map name in the “class map name” text box..

(2) Select the type of create class map in the “type ” drop-down box.

(3) After that, click Create to apply all the changes made.

(4) Click “Create ” button.

(5) Confirm the submission configuration and click the “Create ” button.

The operation is shown in figure 20, and the class map configuration success table entry is shown in figure 21.

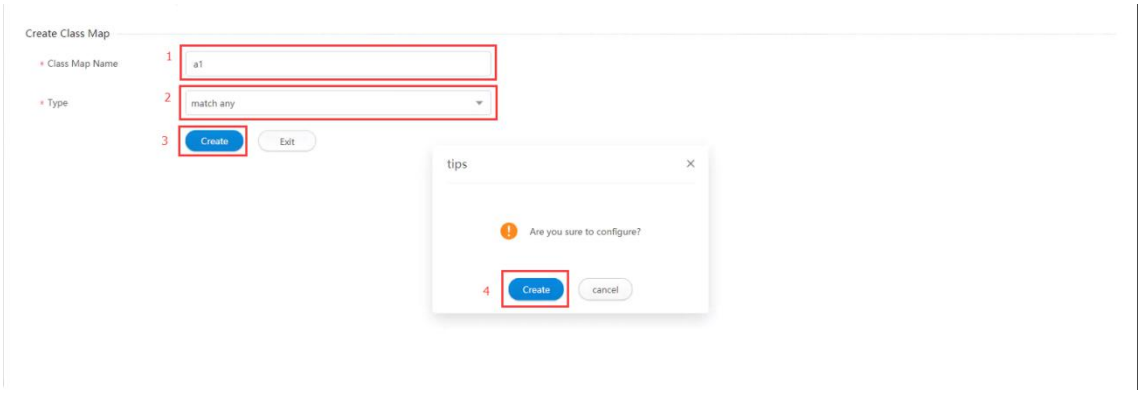


Figure 20 Add class map configuration

Figure 21 New class map

If you want to delete the class map, here are the steps:

(1) Click the checkbox to select class map which are need to be deleted as the figure below.

(2) Click “Delete” button.

(3) After clicking “Delete”, the page as shown in figure 22 appears, and if you click the “Confirm” button, you can delete it.

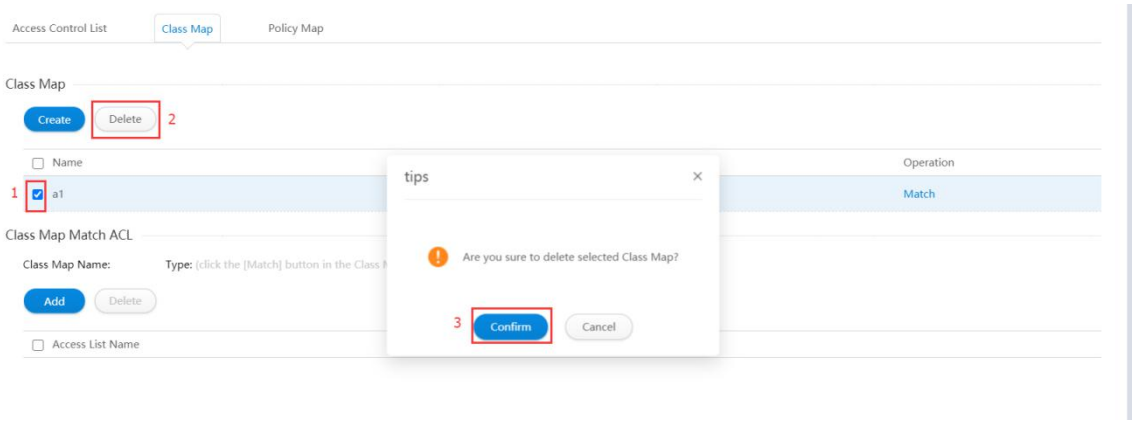


Figure 22 Delete class map

16.2.2 Class Map Match ACL

Class map match ACL provide two basic configuration functions, creating and removing class map match ACL.

If you want to create an class map match ACL, here are the steps:

Click "Match" in blue to select the current class map matching ACL, as shown in figure 23, and click "Add" to enter the class map match ACL configuration page, as shown in figure 24, class map match ACL the configuration page is shown in figure 25.

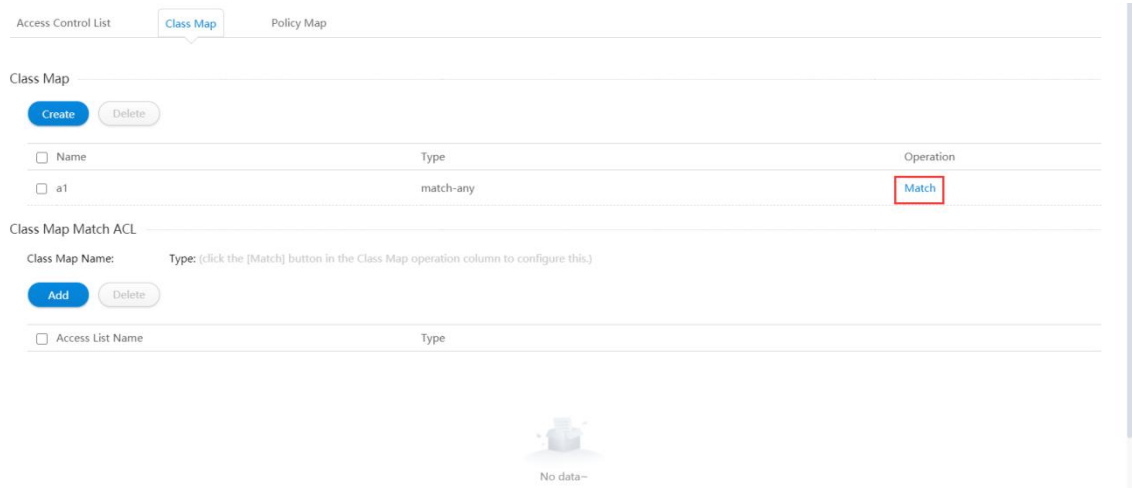


Figure 23 Select current class map

Figure 24 Add class map match ACL

Figure 25 Class map match ACL configuration page

- Parameter usage

Item	Description
Name	acl name
Type	acl type

If you want to configure class map match ACL, perform the following steps:

(1) Click the checkbox to select ACL which are need to be matched to the current Class map.

(2) Click “Submit ” button.

(3) Confirm the submission configuration and click the "Submit " button.

The operation is shown in figure 26, the class map match ACL configuration success table entry is shown in figure 27.

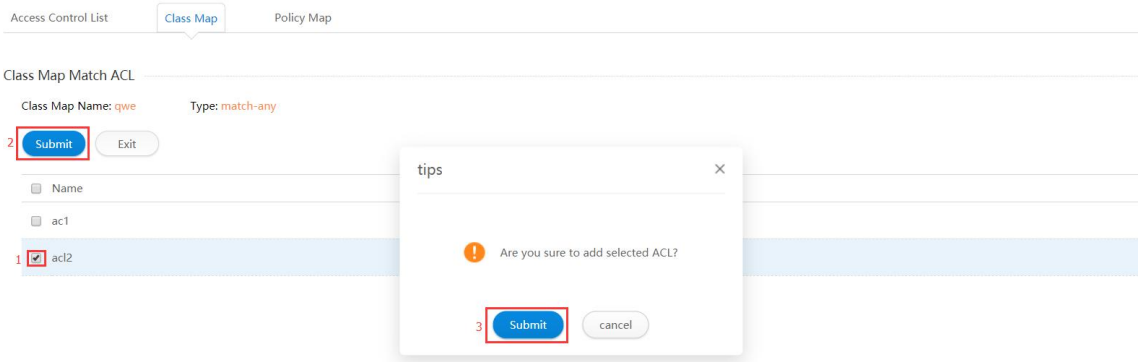


Figure 26 Class map match ACL configuration

Figure 27 New class map match ACL

If you want to delete the class map match ACL, here are the steps:

Click on the blue "Match" and select the current Class map, as shown in figure 28.

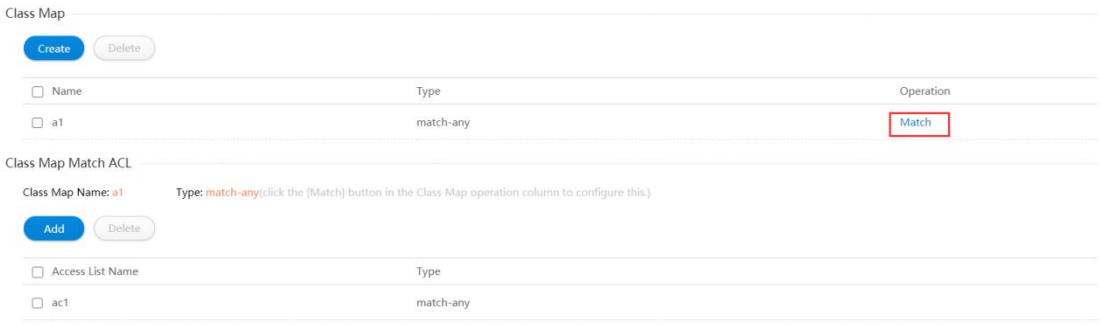


Figure 28 Select current Class map

If you want to delete the configuration, perform the following steps:

(1) Click the checkbox to select class map match ACL which are need to be deleted as the figure below.

(2) Click "Delete" button.

(3) After clicking "Delete", the page as shown in figure 29 appears, and if you click the "Confirm" button, you can delete it.

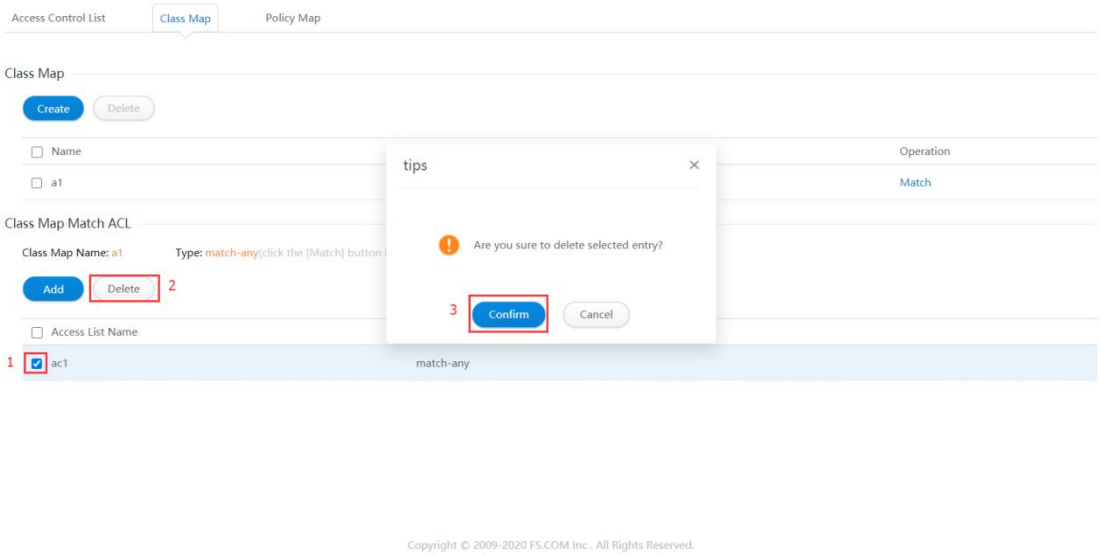


Figure 29 Delete class map match ACL

16.3 Policy Map

If you click "ACL -> Policy Map" in the title bar , the Policy Map page appears, as shown in Figure 30.

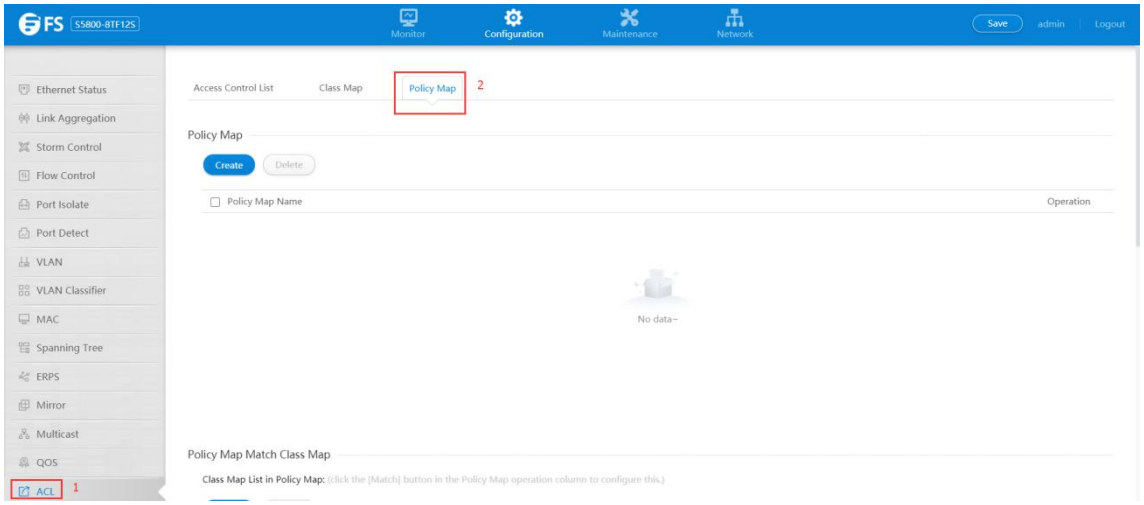


Figure 30 Policy map

16.3.1 Policy Map

Policy map provide two basic configuration functions, creating and removing policy map.

If you want to create an policy map, here are the steps:

If you click the "Create" button, you can add the policy map, the operation is shown in Figure 31, and then the policy map configuration page appears, as shown in Figure 32.

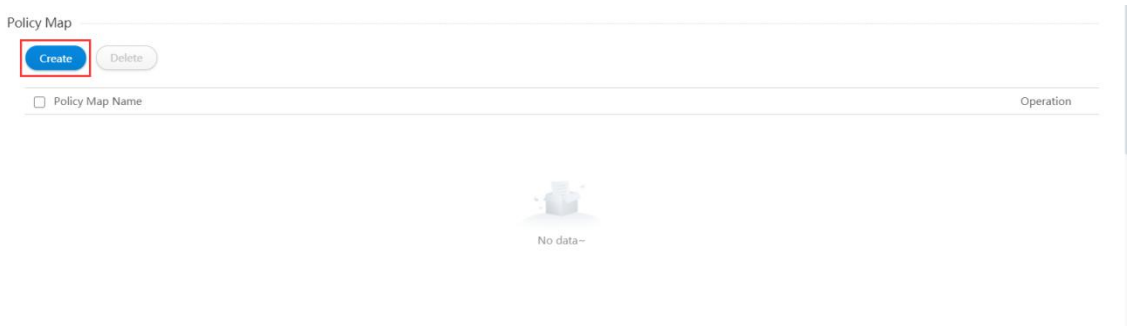


Figure 31 Add policy map operation

Figure 32 Add policy map

- Parameter usage

Item	Description
Policy Map Name	Enter the policy map name

If you want to configure policy map, perform the following steps:

(1) Enter name in the “policy map name” text box

(2) After that, click Create to “Create” all the changes made.

(3) Click “Create ” button.

(4) Confirm the submission configuration and click the “Create ” button.

The operation is shown in figure 33, and the policy map configuration success table entry is shown in figure 34.

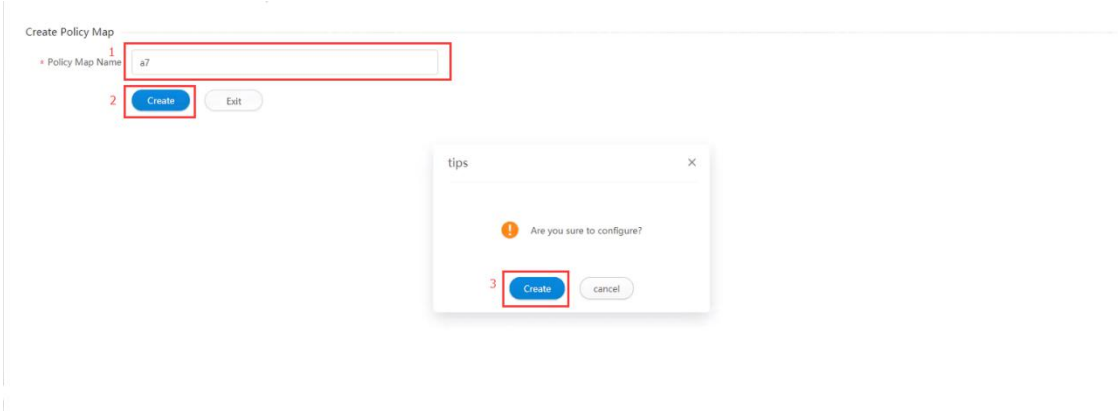


Figure 33 Add policy map configuration

Figure 34 New policy map

If you want to delete the policy map, here are the steps:

(1) Click the checkbox to select policy map which are need to be deleted as the figure below.

(2) Click “Delete” button.

(3) After clicking “Delete”, the page as shown in figure 35 appears, and if you click the “Confirm” button, you can delete it.

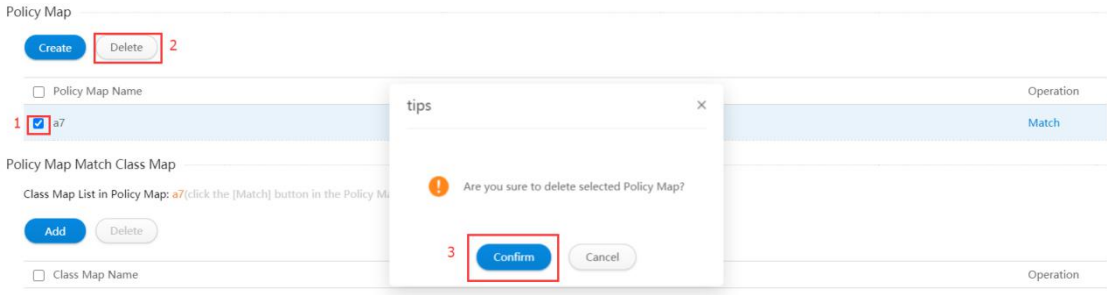


Figure 35 Delete policy map

16.3.2 Policy Map Match Class Map

Policy map match class map provides two basic configuration functions, namely creating and deleting policy map match class map.

If you want to create an policy map match class map, here are the steps:

Click the blue "Matching" to select the current strategy classification, as shown in figure 36, click "Add" to enter the policy map match class map configuration page, as shown in figure 37, policy map match class map configuration page is shown in figure 38.

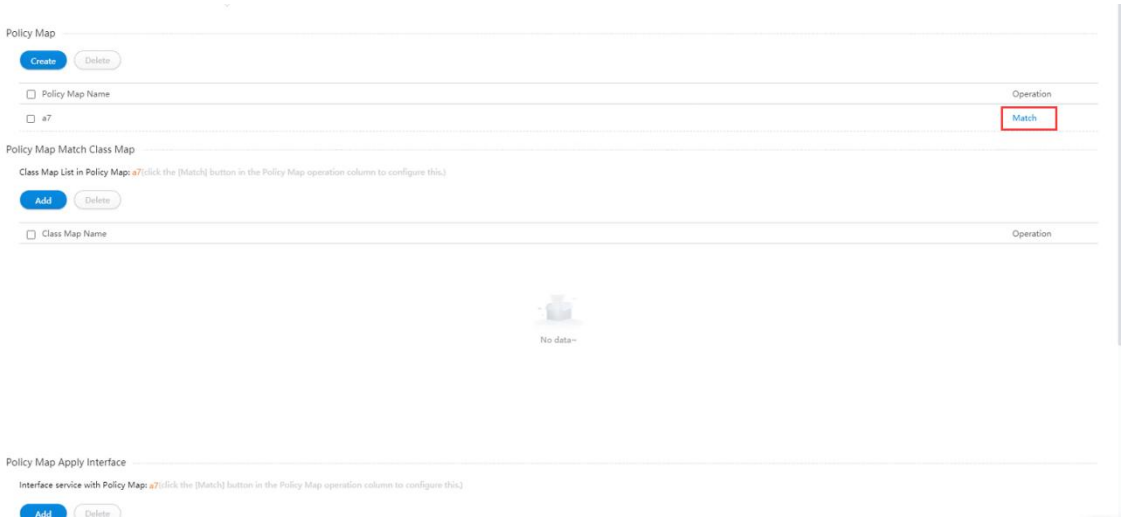


Figure 36 Select policy map

Figure 37 Add button

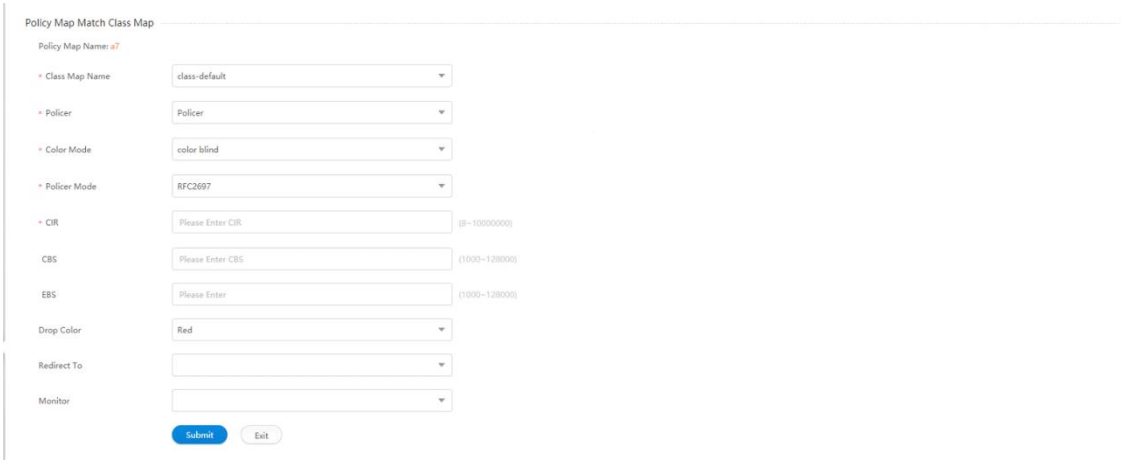


Figure 38 Policy map match class map configuration page

- Parameter usage

Item	Description
Class Map Name	Select the existed class map
Policer	Select the peolicer or not
Color Mode	Select the color mode
Policer Mode	Select the policer mode
CIR	Enter CIR (Commit Information Rate) with the range of 1 to 10,000,000 kbps

Item	Description
CBS	Enter CBS(Commit Burst Size) with the range of 0 to 16,000 bytes
EBS	Enter EBS(Excess Burst Size) with the range of 0 to 16,000 bytes
PIR	Enter PIR(Peak Information Rate) with the range of 1 to 10,000,000 kbps
PBS	Enter PBS (Peak Burst Size) with the range of 0 to 16,000 bytes
Drop color	Select the drop color
Redirect to	Select the redirection interface
Monitor	Select the monitor session

If you want to configure an policy map match class map, here are the steps:

(1) Select name in the “class map name” drop-down box.

(2) Select no police in the “Policer” drop-down box.

(3) Click the “submit ” to complete the configuration, as shown in the figure 39.

(4) Click “Submit ” button.

The operation is shown in figure 39.

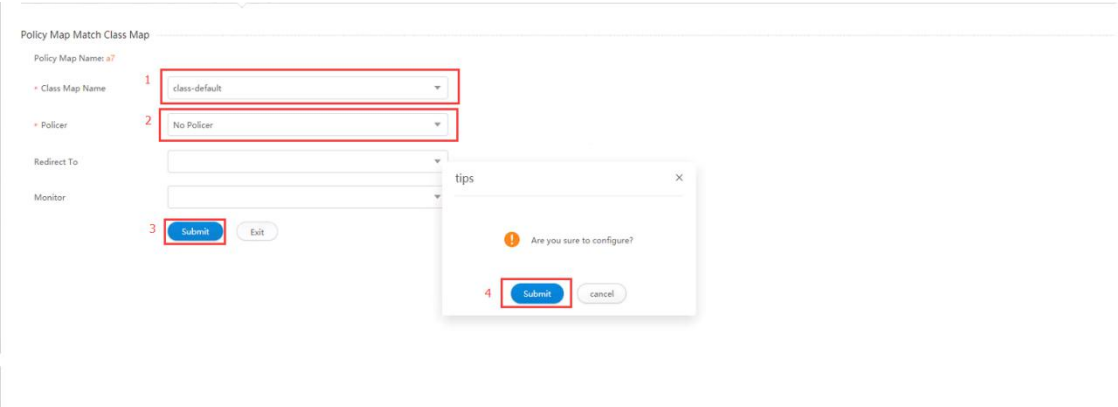


Figure 39 Configuration example

If you want to view the configuration, follow these steps:

(1) Click "Particulars" to view the detailed configuration, the operation process is shown in figure 40, the detailed configuration is shown in figure 41.

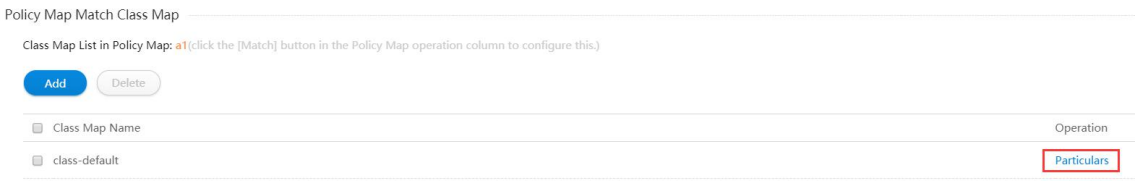


Figure 40 View detailed information process

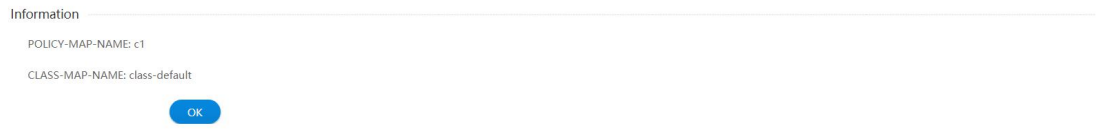


Figure 41 Detailed information

If you want to delete the policy map match class map, here are the steps:

Click the blue "Match" to select the current Strategy classification, as shown in the figure 42.

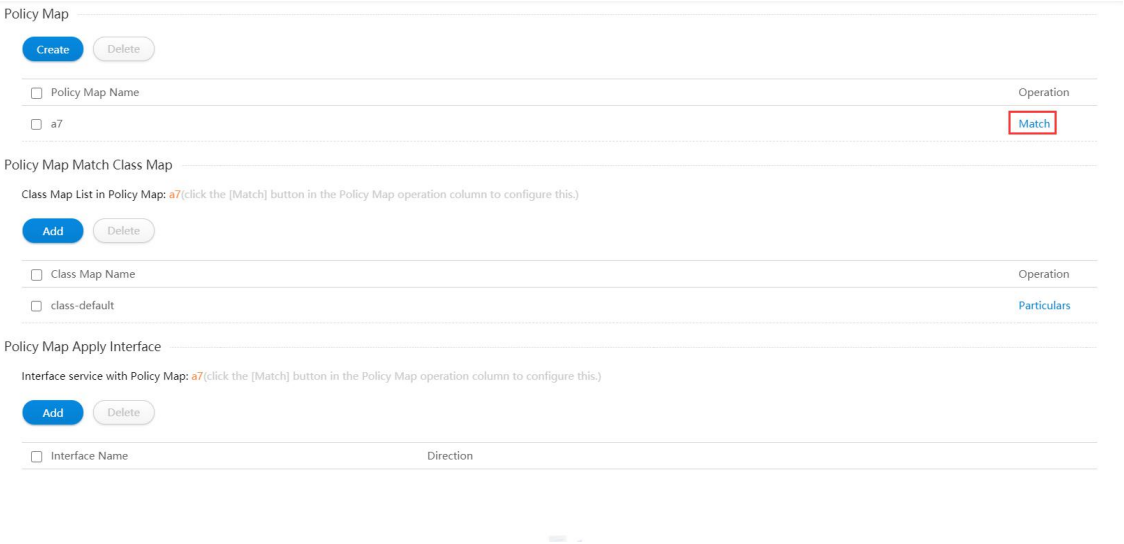


Figure 42 Select policy map

If you want to delete the configuration, perform the following steps:

(1) Click the checkbox to select policy map match class map which are need to be deleted as the figure below.

(2) Click “Delete” button.

(3) After clicking “Delete”, the page as shown in figure 43 appears, and if you click the “Confirm” button, you can delete it.

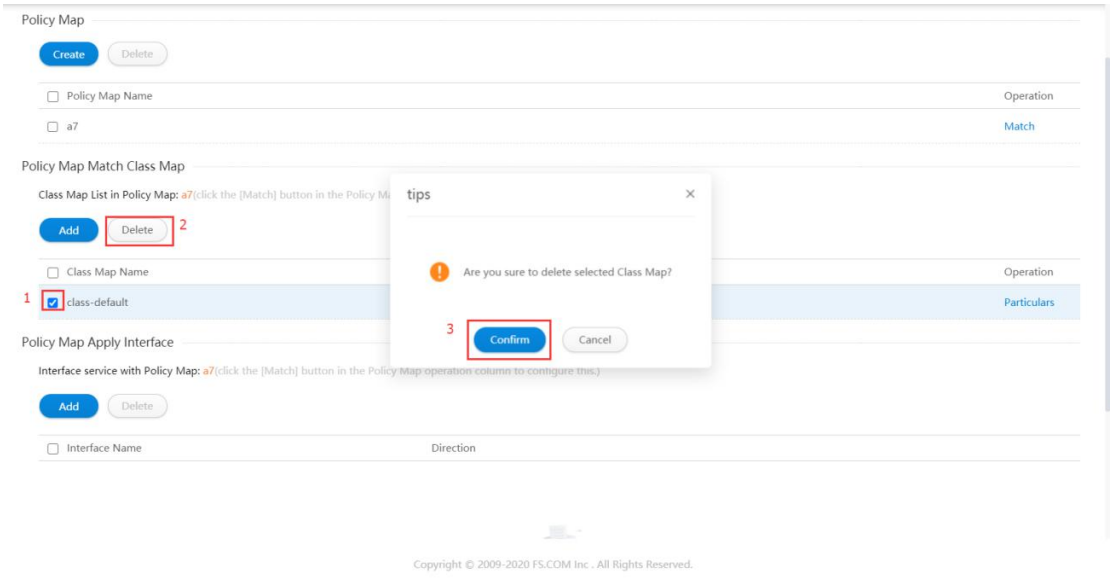


Figure 43 Delete policy map match class map

16.3.3 Policy Map Apply Interface

Policy map apply interface provide two basic configuration functions, creating and removing policy map apply interface.

If you want to create an policy map apply interface, here are the steps:

Click "Match" in blue to select the current policy category, as shown in figure 44, click "Add" to go to the policy map apply interface configuration page, as shown in figure 45, and the class map list in the policy map apply interface configuration page is shown in figure 46.

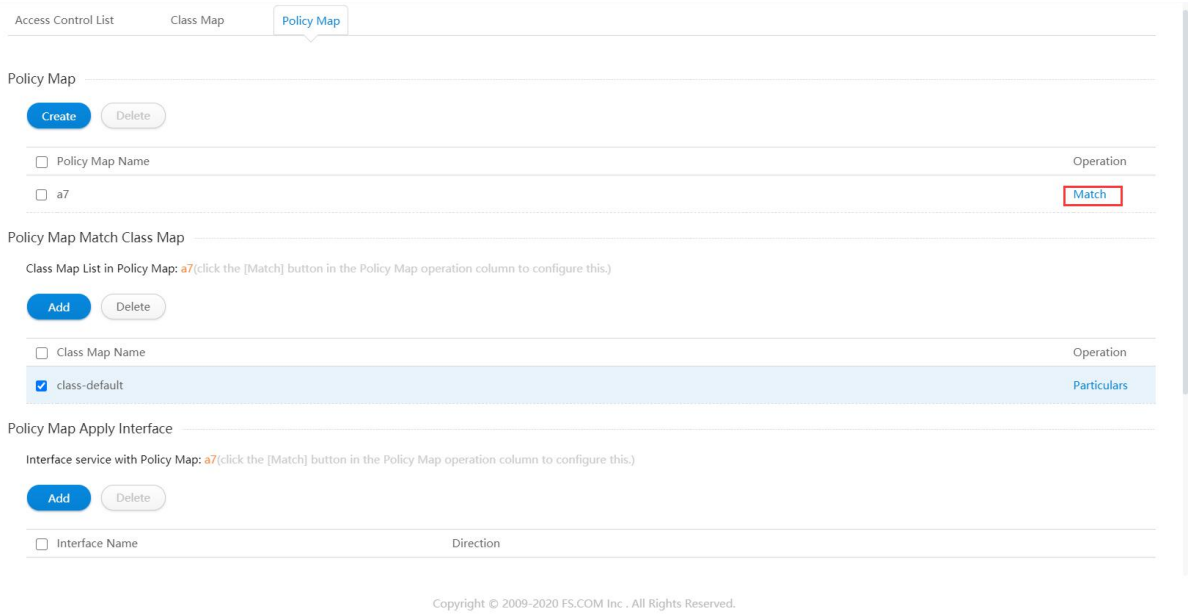


Figure 44 Select policy map

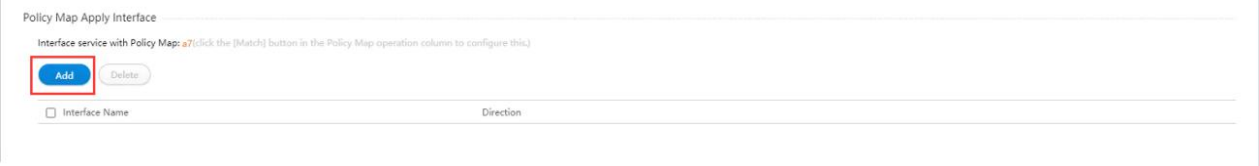


Figure 45 Add policy map apply interface operation

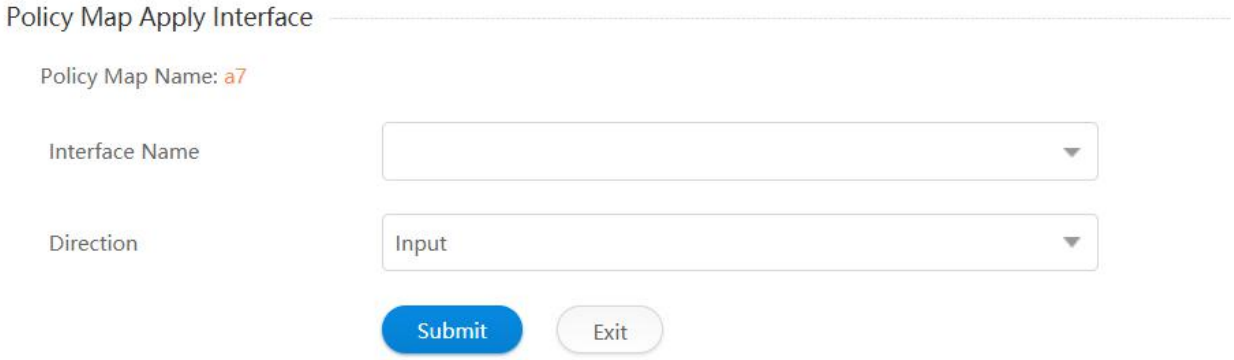


Figure 46 Policy map apply interface configuration page

- Parameter usage

Item	Description
Interface Name	Select the interface name
Direction	Select the direction

If you want to check the configuration policy map apply interface, please perform the following steps:

(1) Select the interface in the “Interface Name” drop-down box.

(2) Select direction in the “Direction” drop-down box.

(3) After that, click “Submit ” to complete the configuration.

The operation is shown in figure 47, the policy map apply interface configuration success table entry is shown in figure 48.

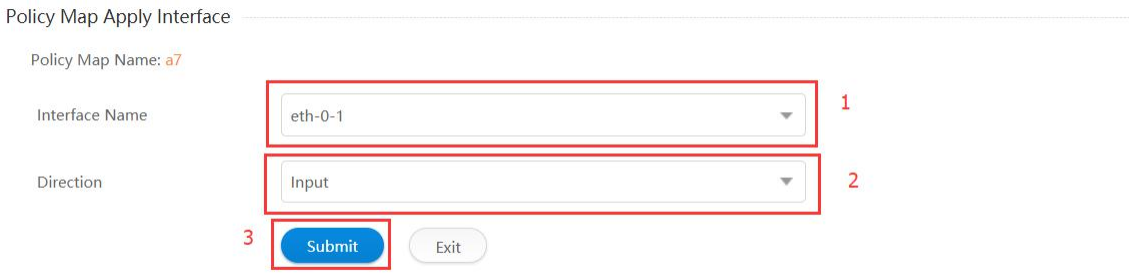


Figure 47 Add policy map apply interface operation

Figure 48 View policy map apply interface

If you want to delete the policy map apply interface, here are the steps:

Click the blue "Match" to select the current Strategy classification, as shown in the figure 49.

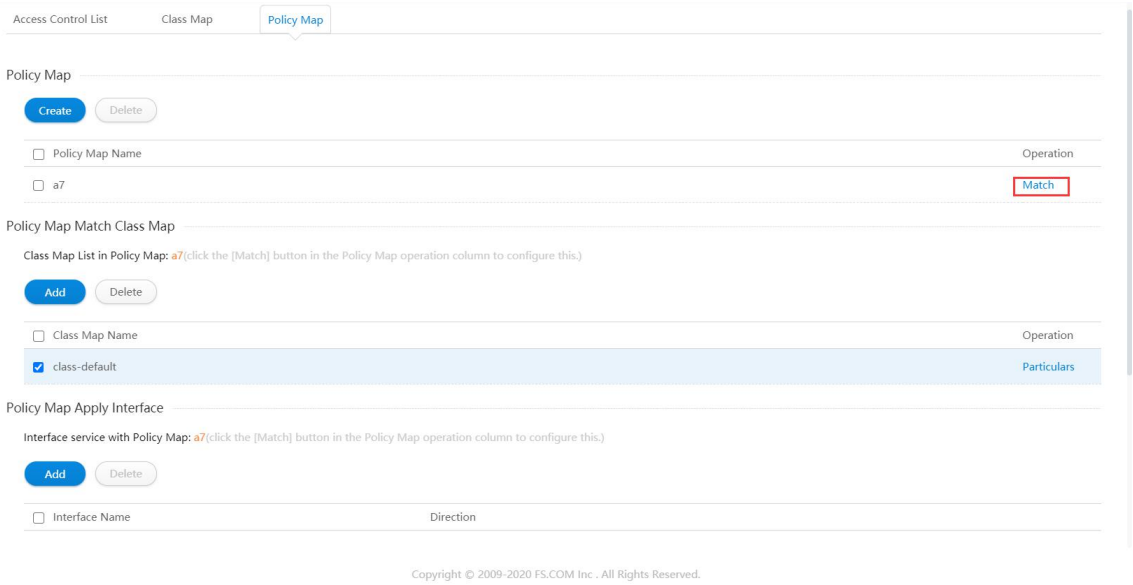


Figure 49 Select policy map

If you want to delete the configuration, perform the following steps:

(1) Click the checkbox to select policy map apply interface which are need to be deleted as the figure below.

(2) Click "Delete" button.

(3) After clicking "Delete", the page as shown in figure 50 appears, and if you click the "Confirm" button, you can delete it.

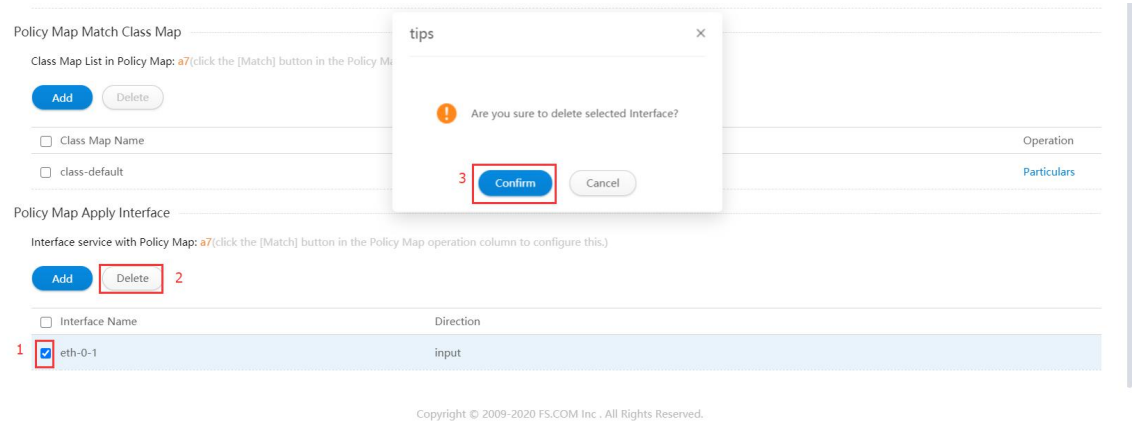


Figure 50 Delete policy map apply interface

17. Reboot/Save

If you want to restart the switch or save the current configuration under the web page, you should click "Maintenance" in the top control bar. Then click "Reboot/Save" in the navigation bar, the correspond page appears.

17.1 Page Overview

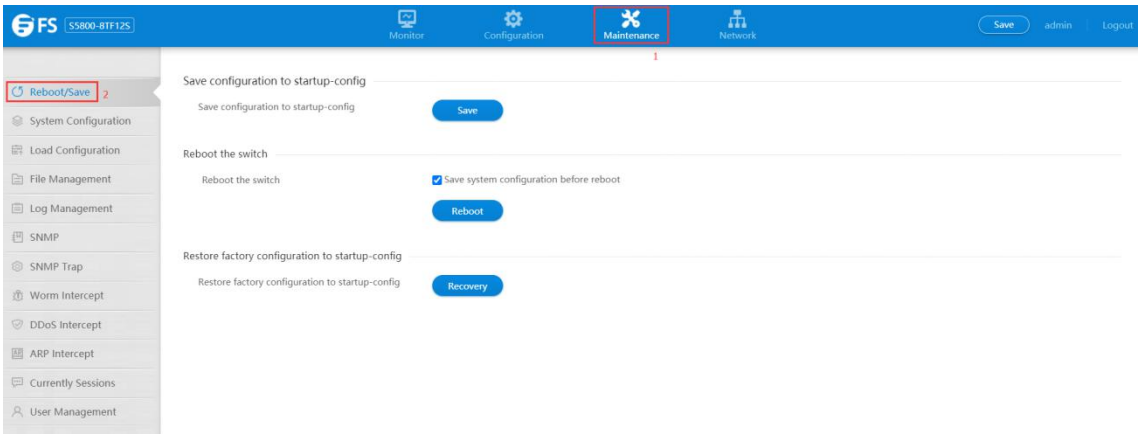


Figure 1 Reboot/Save page

- Parameter usage

Item	Description
Save configuration to startup-config	Save current configuration to startup-config
Save system configuration before reboot	Save current configuration to startup-config before reboot
Restore Factory configuration to startup-config	Restore switch by using startup-config

17.2 Save Configuration

Click "Save" button to save current configuration to startup-config.

Figure 2 Save config

17.3 Reboot Switch

Click "Reboot" button to reboot the switch, but if you want to save the current configuration before reboot, choose "Save system configuration before reboot" at first.

Figure 3 Reboot switch

17.4 Recovery Switch

Click "Recovery" button to recovery switch configuration with startup-config.

Figure 4 Recovery switch

18. System Configuration

If you click “Maintenance -> System Configuration” in the top control bar, the System Configuration list page appears, as shown in figure 1.

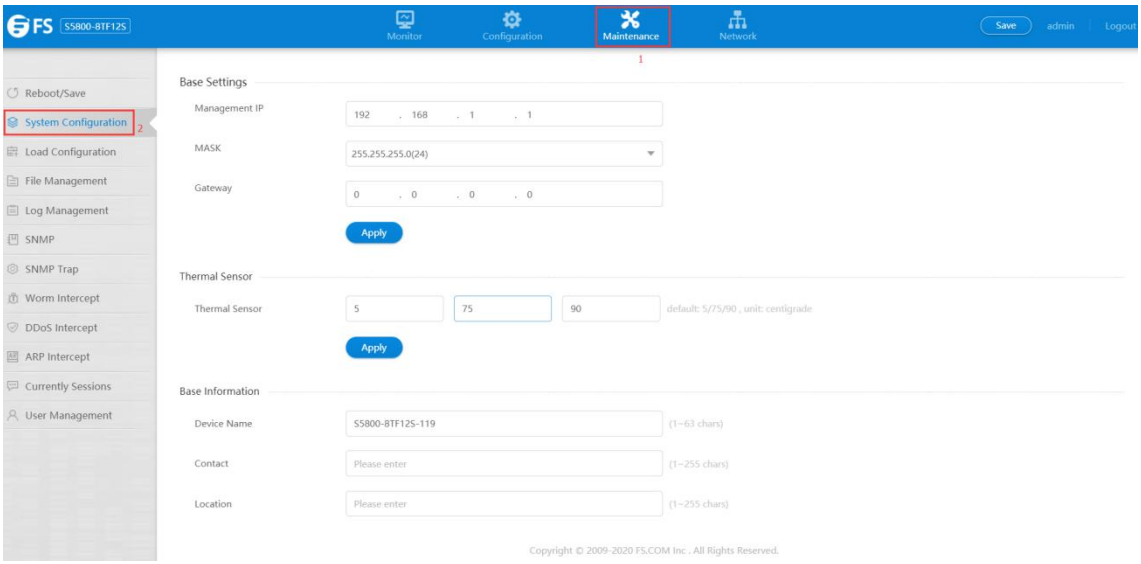


Figure 1 System configuration list

18.1 Base Settings

After you click “System Configuration” button, you will see the first case “base settings”.

If you want to add the IP for this switch, you can follow the following steps:

(1) Enter an IP address in the “Management IP.

(2) Select the destination address mask in the “mask ” dropdown box.

(3) Enter default route IP address in the “Gate Way” textbox.

(4) Click “Apply” button, and a tips popup will appear, as shown in figure 2 and figure 3, then click “Apply” button in tips.

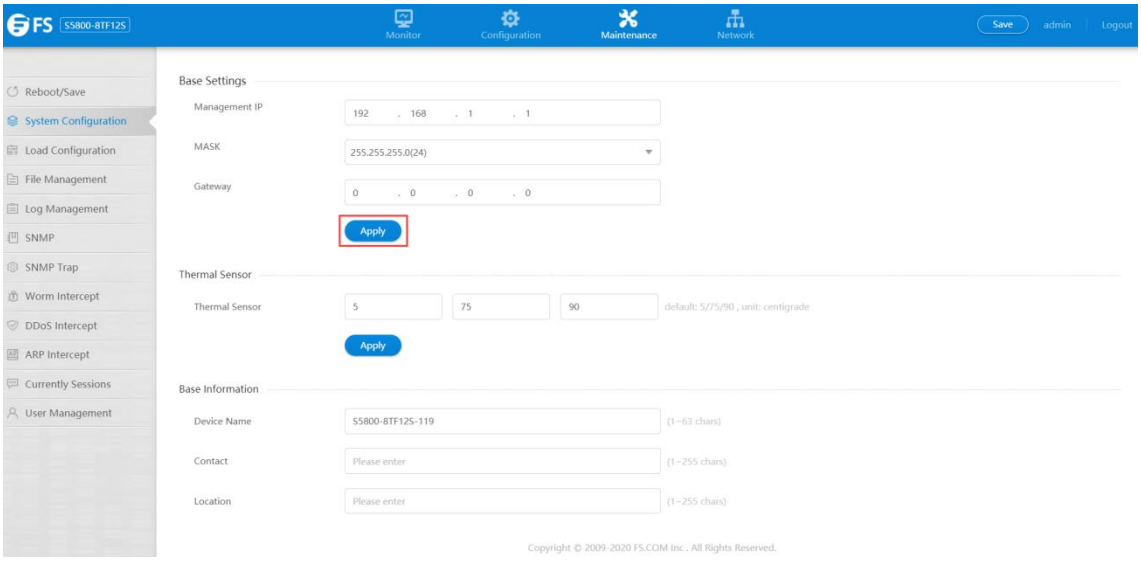


Figure 2 Base settings page

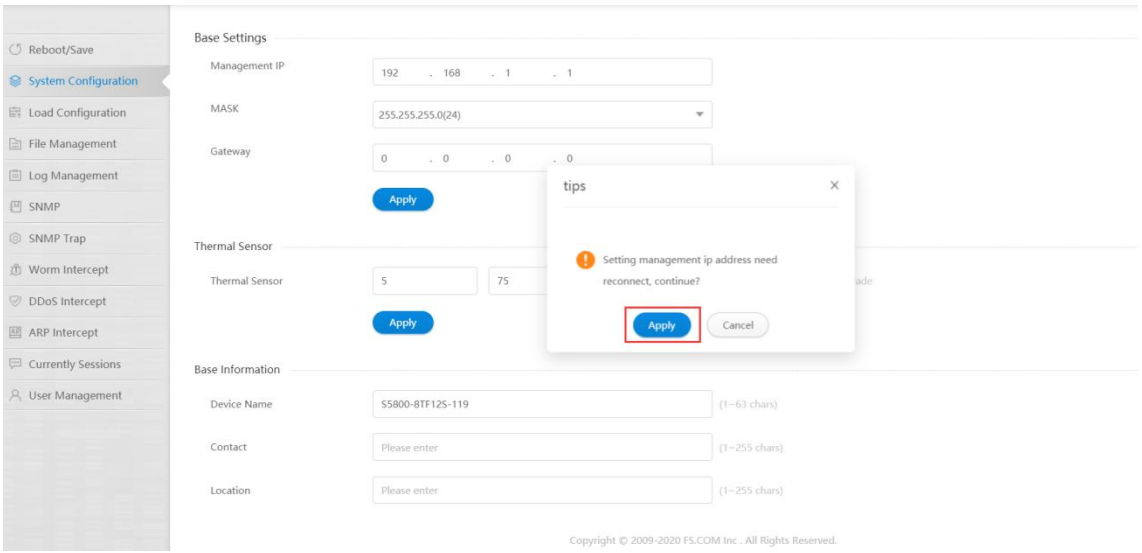


Figure 3 Base settings page

- Parameter usage

Item	Description
Management IP	Manage switch via this IP
Mask	Locate Management IP`s network bits
Gate Way	Defaults route

18.2 Thermal Sensor

After you click “System Configuration” button, you will see the second case “thermal sensor” in this case you can set the threshold of temperature.The boxes from left to right represent the definition of low temperature, medium temperature, and high temperature.

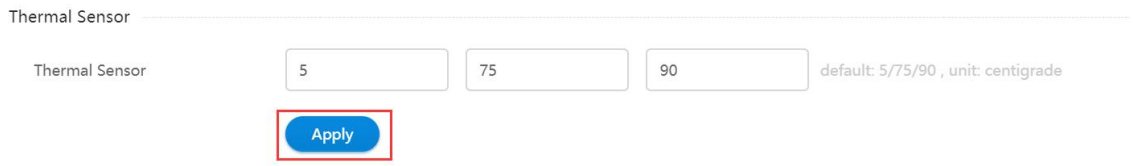


Figure 4 Termal sensor

Notes: From left to right in the table are the low threshold middle threshold and high threshold of the set temperature.

18.3 Base Information

After you click “System Configuration” button, you will see the third case “Base Information”, in this case you can set the switch information to distinguish the switch in network.

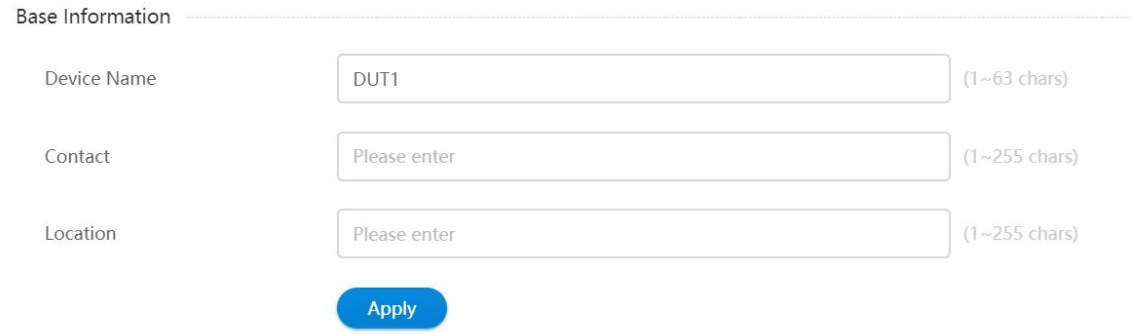


Figure 5 Base information

- Parameter usage

Item	Description
Device Name	Switch hostname
Contact	How to contact this switch in the other words contact is manage IP of this switch or Other information which can visit this switch
Location	Where the switch is

If you want to set the information of this switch, you can follow the following steps:

(1) Enter an device name in the "Management IP.

(2) Enter contact information in the "Contact"

(3) Enter location information in the "Location" textbox.

(4) Click the Apply button.

18.4 Date&Time

After you click "System Configuration" button, you will see the fourth case "Date and Time" in this case you can set time of switch.

Figure 6 Date and time

Example: 12:08:44 17/03/2020

18.5 Time Zone Name

After you click "System Configuration" button, you will see the 5th case "Time Zone Name" in this case you can set the time zone and the offset of time zone.

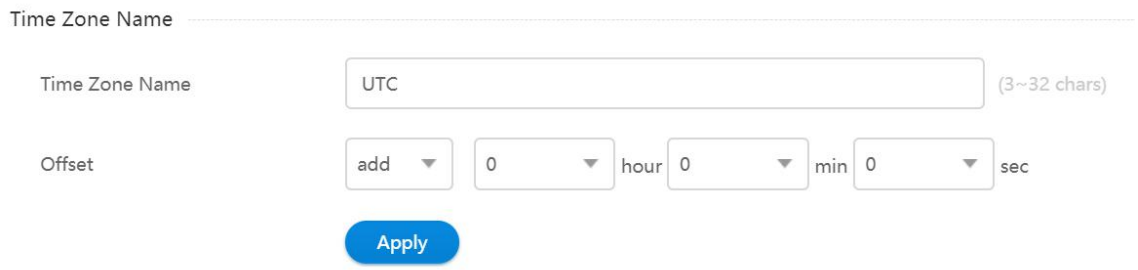


Figure 7 Time zone name

- Parameter usage

Item	Description
Time Zone Name	Time zone
Offset	Offset depends between GMT and Time Zone which your set

If you want to set the time zone name of this switch, you can follow the following steps:

(1) Enter time zone name in the “Time Zone Name.

(2) Select the offset in the “Offset”.

19. Load Configuration

If you click “Maintenance > Load Configuration” in the top control bar, the load configuration list page appears, as shown in figure 1.

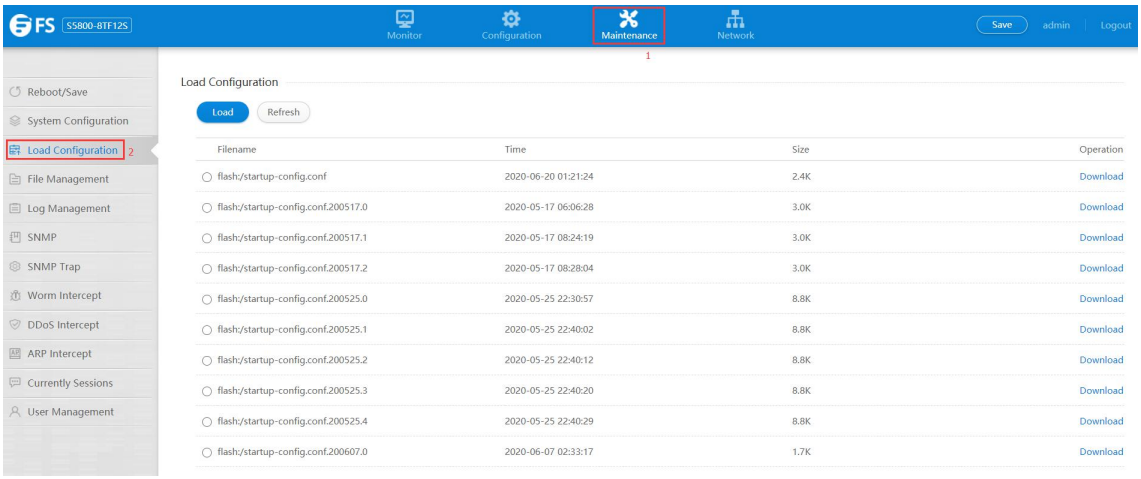


Figure 1 Load configuration list

This chapter describes load the configuration files to the device or download the configuration file to PC as the the backup file.

19.1 Load Configuration

You can load the configuration files from the web to the device and replace the configuration file that is currently being used.

19.1.1 Load the Configuration Files

If you want to load the configuration files to replace the configuration file that is currently being used, you can follow the following steps :

(1) Choose a configuration file which through the file name.

(2) Click “Load” button.

(3) It will appear tips page to note you to confirm the operation, if you click “Loading” button, it will use the configuration as the new configuration of device; if you click “cancel” button, you will cancel the loading configuration operation.

The operation is shown in figure 2.

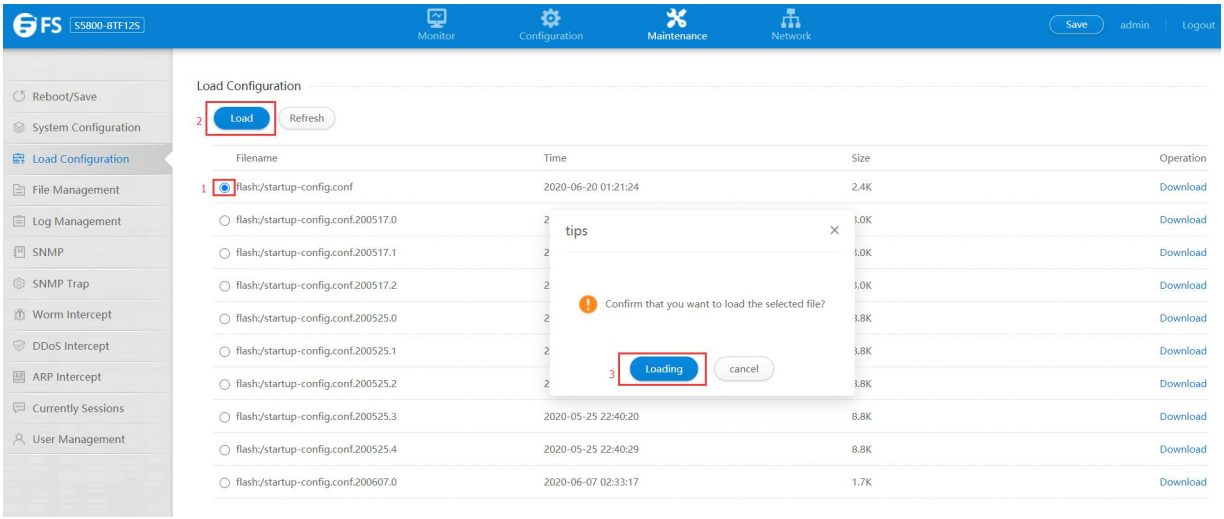


Figure 2 Load configuration operation

- Parameter usage

Item	Description
Filename	Display name of configuration file
Time	Display last modified time of configuration file
Size	Display size of configuration file
Operation	Display that the configuration file can be downloaded

19.1.2 Refresh the Load Configuration Page

If you want to refresh the load configuration page, you can click "Refresh" button. The operation is as shown in Figure 3.

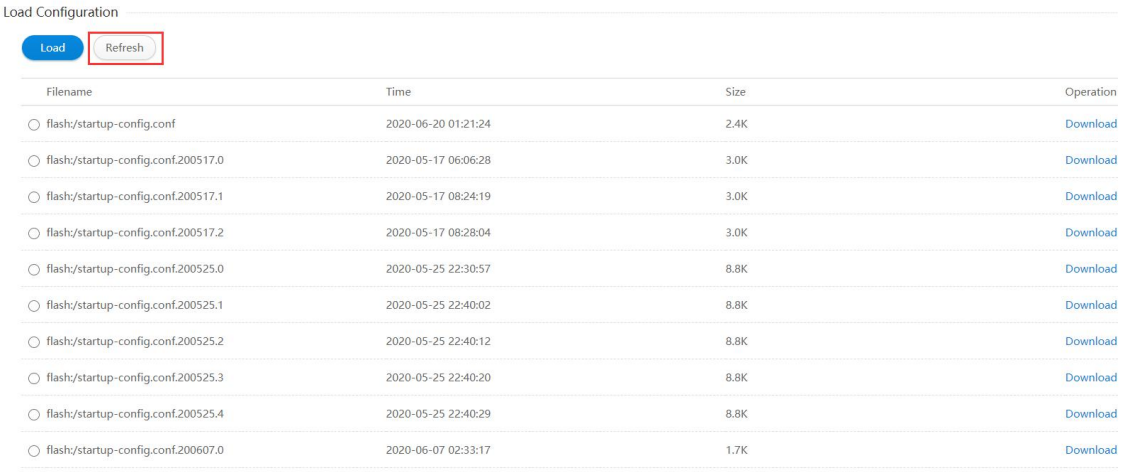


Figure 3 Refresh the load configuration information

19.1.3 Download the Configuration Files

You can download the configuration file and saved in the disk of PC or in the mobile storage device as the backup file and you can also see the configuration file.

To download the configuration file, you can select the configuration file you want to download, and click "Download" button to save the file, the operation is as shown in Figure 4.

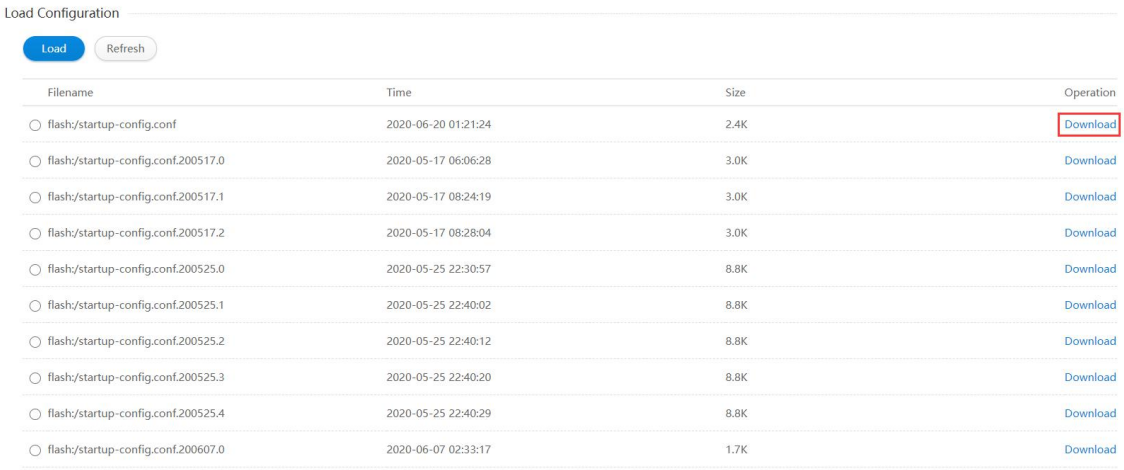


Figure 4 Download configuration file operation

20. File Management

If you click “Maintenance -> File Management” in the top control bar, the file management page appears, as shown in figure 1.

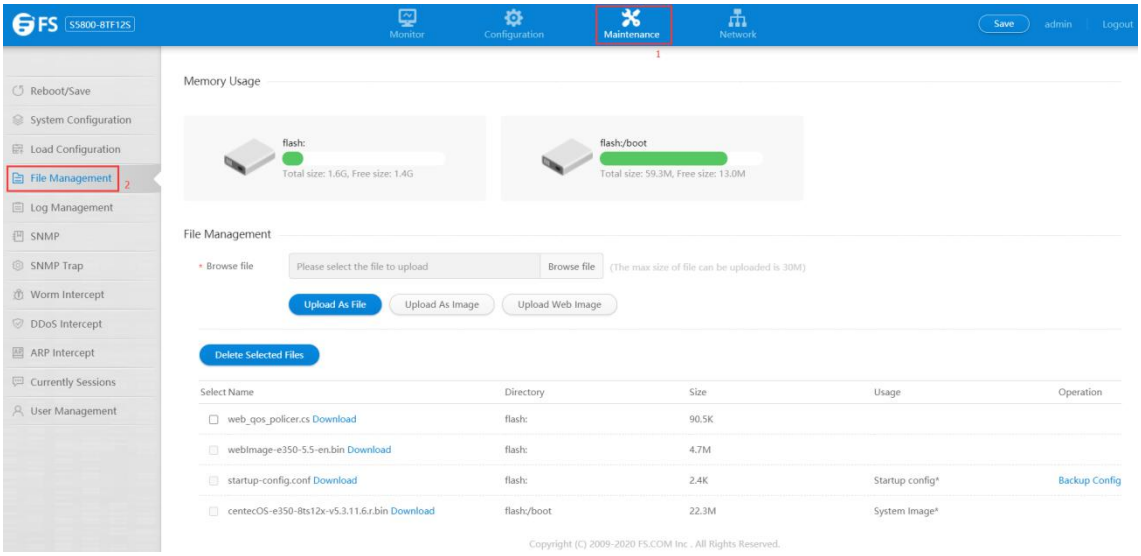


Figure 1 File management

20.1 Memory Usage

Click “Maintenance > File Management” to check memory usage on switch, as shown in figure 2.

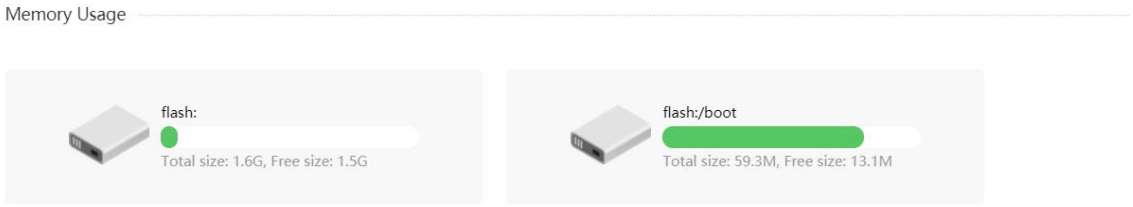


Figure 2 Memory usage

- Parameter usage

Item	Description
flash:	Flash directory at the root of system
flash:/boot	Flash:/boot directory at the root of system

20.2 File Management

Click “Maintenance > File Management” to download or delete system and configuration files of switch, or upload files to switch, the configuration page is as shown in figure 4.

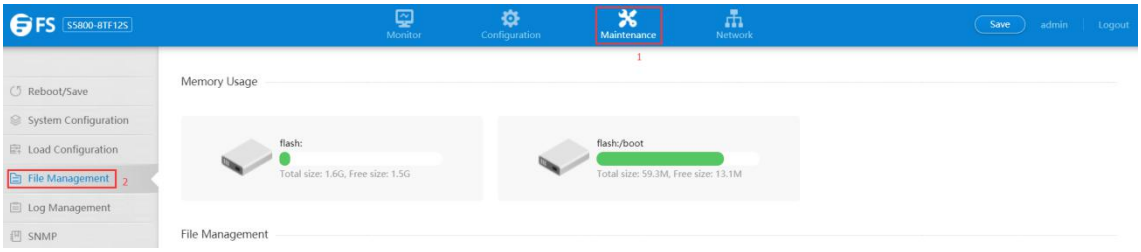


Figure 3 File management

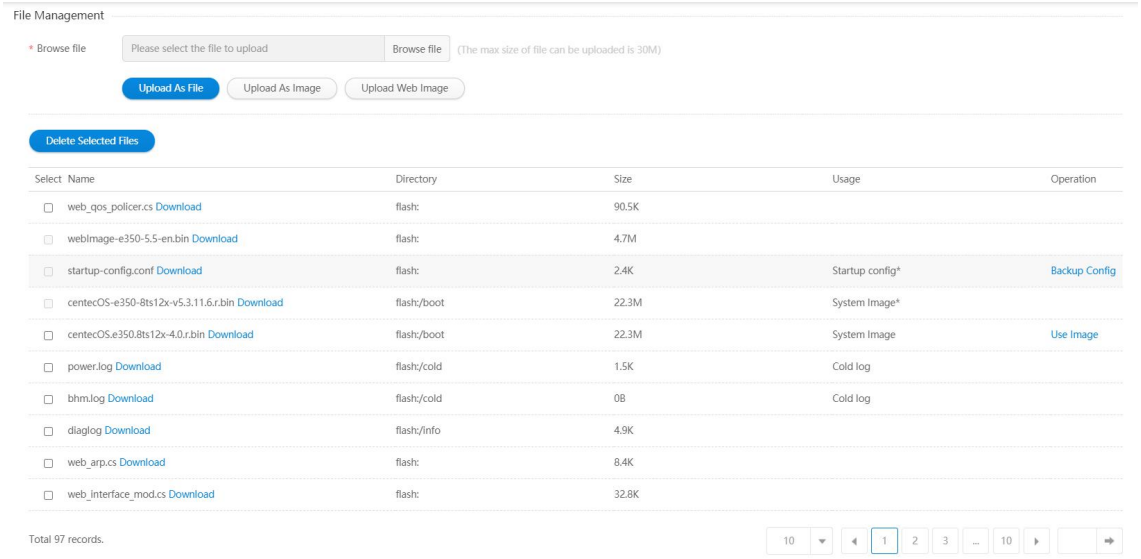


Figure 4 File management

- Parameter usage

Item	Description
File List	File list: shows all files saved on current switch Name: system filename Directory: location of system files Size: size of system files in bytes Usage: description of system files Operation: operation for the special files , include: Use Image: use this file as the next boot image Backup Config: Save running configuration to this file Use Config: use this file as the next start up configuration
Upload As File	Upload the chosen files to Switch
Upload As Image	Upload the chosen files to Switch as a boot image
Delete Selected Files	Select files and delete them from Switch

NOTE: To download a file, just click the name of the file.

If you want to upload file/image/web image , please click “Browse File” button to select the file you need to upload, then click “Upload As File/Upload As Image/Upload Web Image” button, the operation is shown in figure 5.

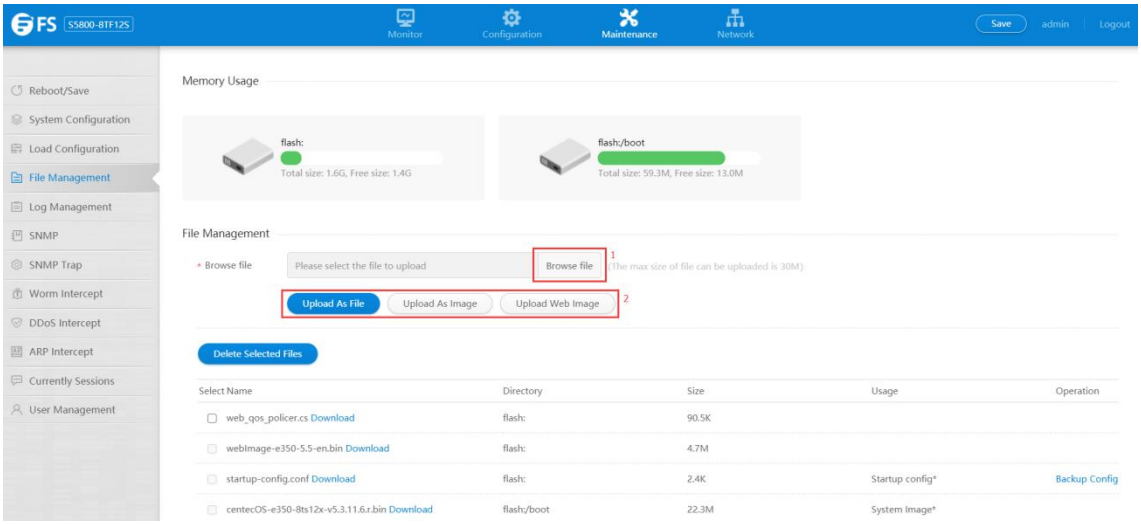


Figure 5 Upload file configuration

If you want to delete files, you can select one or more file check box, click "Delete Selected Files" button to delete the file on switch, the operation is shown in figure 6.

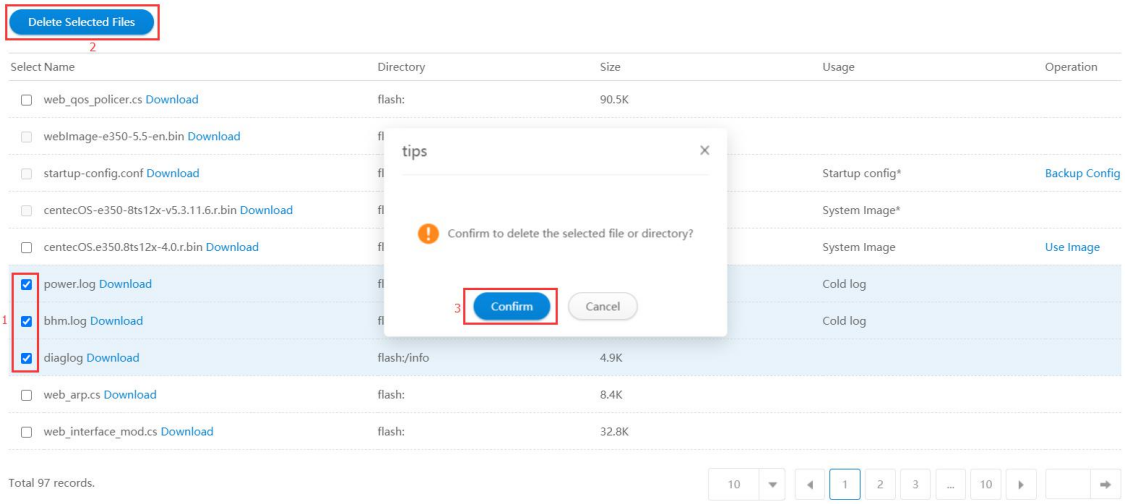


Figure 6 Delete file configuration

If you want to download files , you can click the download button next to the file name to download, the operation is shown in figure 7.

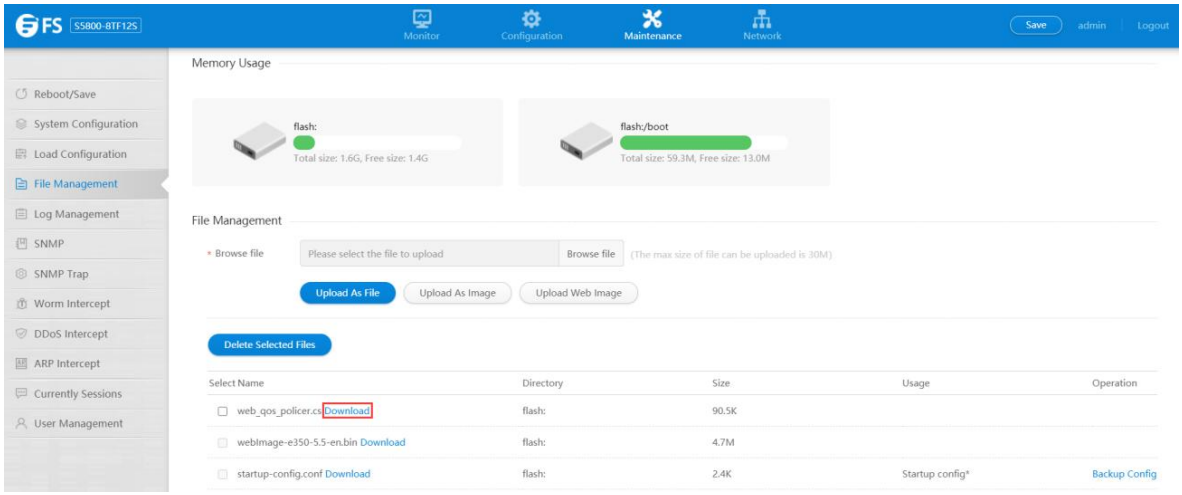


Figure 7 Download file configuration

21. Log Management

If you click “Management->Log Management” in the top control bar, the log management page appears, as shown in figure 1.

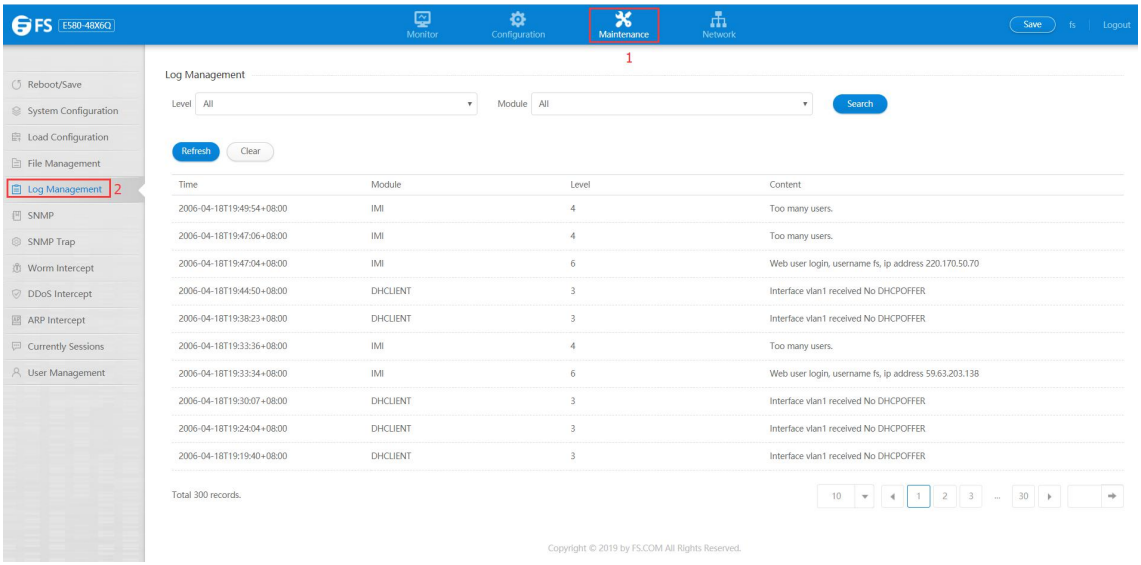


Figure 1 Log management page

This section mainly describes how to search and view log information.

- Parameter usage

Item	Description
Level	Display special log level as condition for search
Module	Display special module creating logs as condition for search
Time	Display the time of log generated
Module	Display Name of the module generating the log
Level	Display Log information level
Content	Display The log content

21.1 Search Log Management

21.1.1 Search Log Information by Level

If you want to search log information for a specified level, you can select the level of the log in the “Level” drop-down box, then click the “Search” button, the operation is shown in figure 2, and the search results are shown in figure 3.

Figure 2 Search log information by level operation

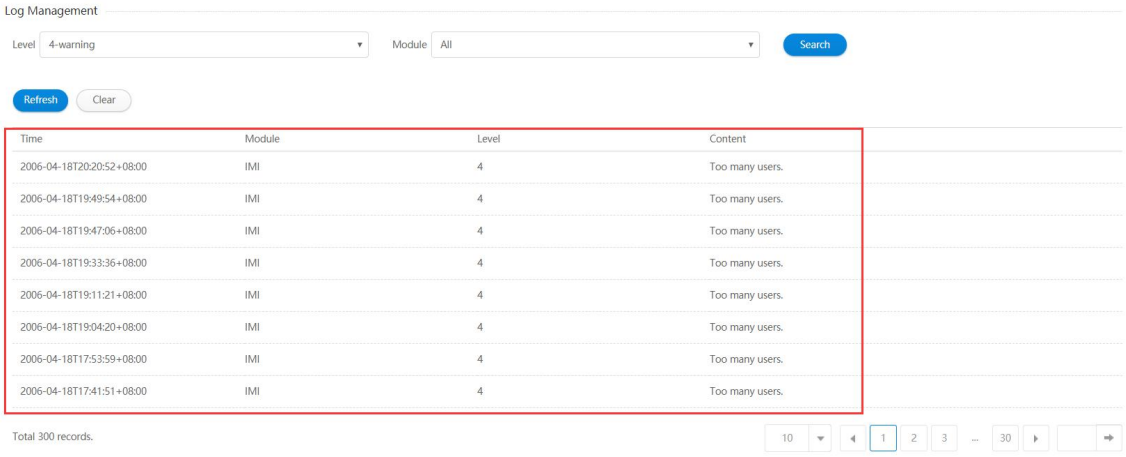


Figure 3 Search results list

21.1.2 Search Log Information by Module

If you want to search log information for a specified module, you can select the module of the log in the "Module" drop-down box, then click the "Search" button, the operation is shown in figure 4, and the search results are shown in figure 5.

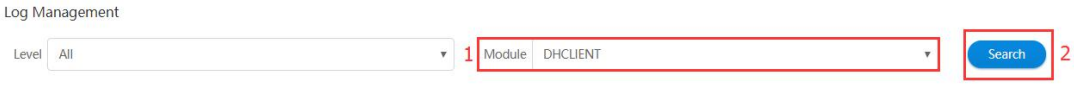


Figure 4 Search log information by module operation

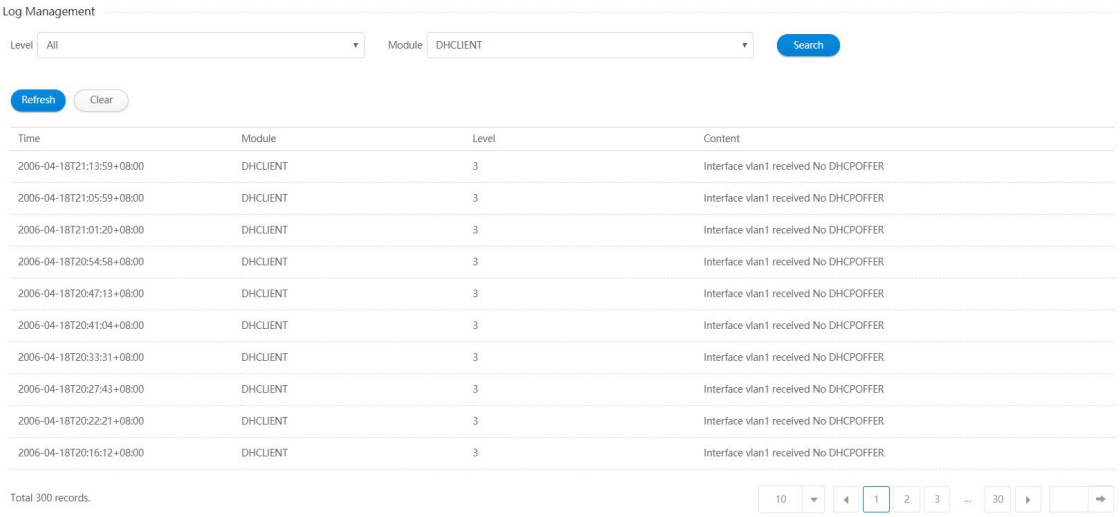


Figure 5 Search results list

21.2 Refresh Log Information

If you want to refresh the logs displayed in the table, you can click "Refresh" button, the operation is shown in figure 6, then the latest log information will be displayed, as shown in figure 7.

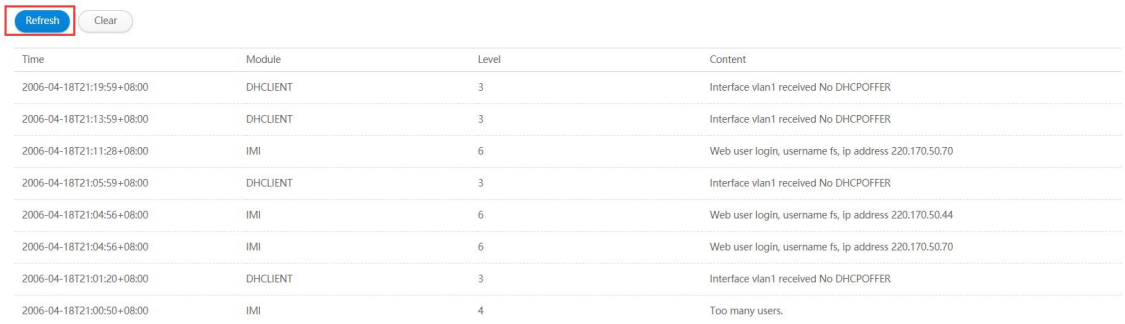


Figure 6 Refresh log information operation

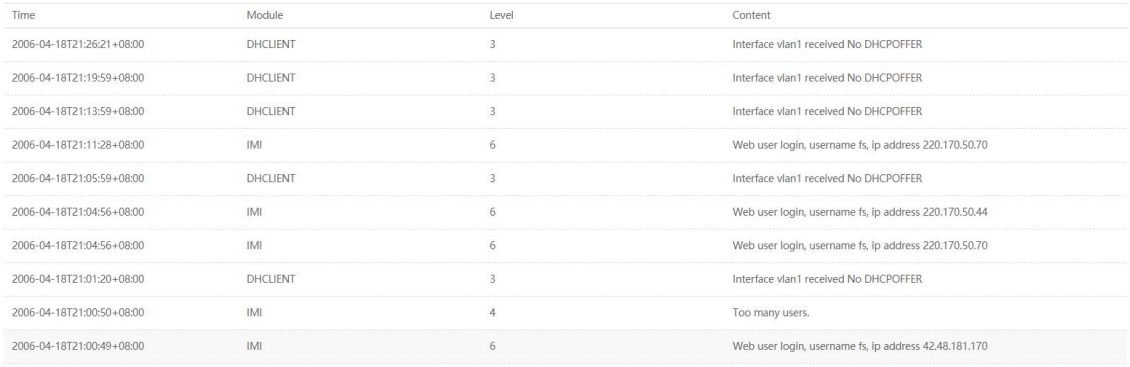


Figure 7 Latest log information list

21.3 Clear Log Information

If you want to clear the logs displayed in the table, you can click “Clear” button, the operation is shown in figure 8, then the cleared log information list will be displayed, as shown in figure 9.

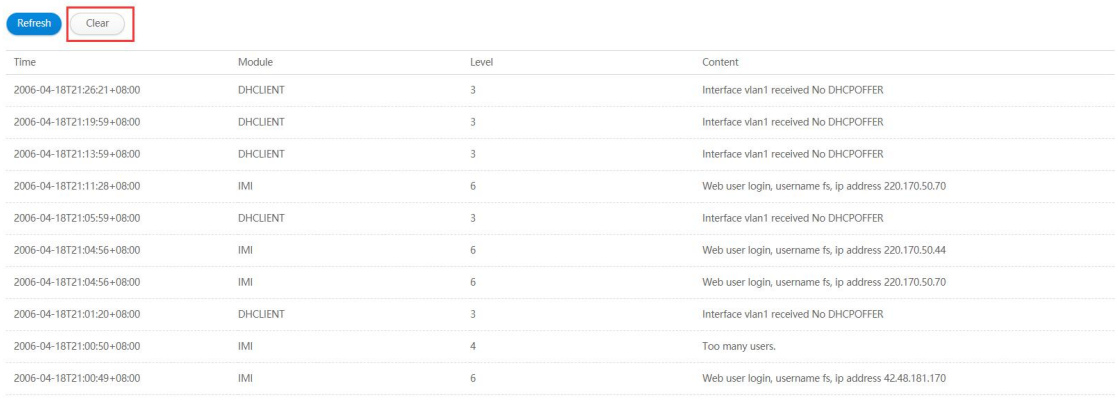


Figure 8 Clear log information operation

Figure 9 New log information list

22. SNMP Configuration

If you want to configure SNMP under the web page, you should click "Maintenance" in the top control bar. Then click "SNMP" in the navigation bar, the SNMP page appears, as shown in figure 1.

22.1 SNMP Basic Configuration

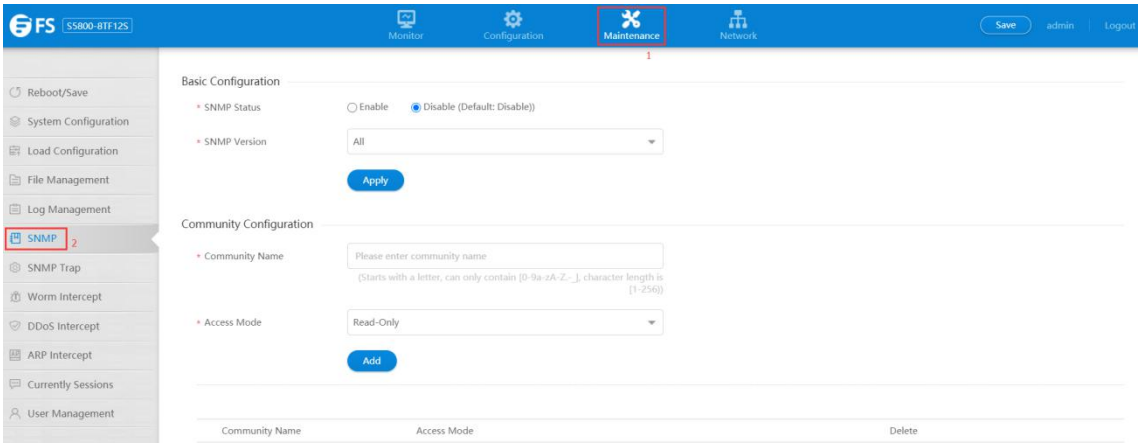


Figure 1 SNMP configuration page

- Parameter usage

Item	Description
SNMP Status	This parameter indicates the SNMP status. It is enabled or disabled
SNMP Version	This parameter indicates the enabled SNMP versions. All of them enable or enable Version 1, Version 2, and Version 3
Group Name	SNMP Group name
Access Mode	Group access mode, read-only or read-write
Delete	Delete the current group

22.1.1 Enable SNMP

As shown, SNMP is disabled by default. If you want to use SNMP, you must enable SNMP at first.

If you want to enable SNMP, you should follow the steps below:

(1) Click "Enable" selection box.

(2) Select the corresponding SNMP version from the drop-down box.

(3) Click "Apply" button.

The operation steps are shown in figure 2.

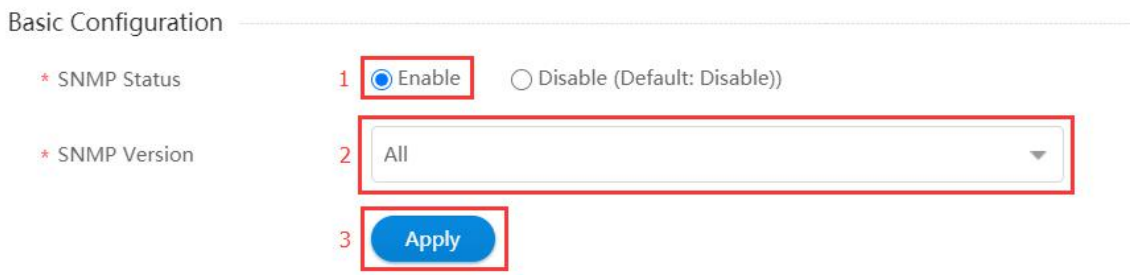


Figure 2 SNMP configuration step

22.2 SNMP Group Configuration

SNMPv1 SNMPv2 uses group name authentication. A group is a basic security mechanism. It is used to implement authentication when an SNMP network administrator accesses the SNMP management agent. SNMP packets with different group names will be discarded. The SNMP group is named by a string and becomes the group name. Different groups can have read-only or read-write access modes. Groups with read-only permissions can only query device information, and groups with read-write permissions can also configure devices.

22.2.1 Add SNMP Group

If you want to add a SNMP group, you should follow the steps below:

(1) Enter the group name. The legal name must start with a letter and can only include 0-9, a-z, A-Z, "_", "-", and the length must be between 1 and 256.

(2) Select the "Access mode" from the drop-down box.

(3) Click "Add" button.

The operation steps are shown in figure 3, and the corresponding results are shown in figure 4.

Figure 3 Add SNMP community step

Figure 4 Add SNMP community result

22.2.2 Delete SNMP Group

If you want to delete an existing group, click the "Delete" behind the group list.

Figure 5 Delete SNMP community

23. SNMP Trap Configuration

TRAP is a mechanism that provides asynchronous reporting from the agent process to the management station. In order to enable the management station to monitor the managed equipment in a timely and effective manner without excessively increasing the communication load on the network, a trap-guided polling process must be used. The agent process is responsible for reporting an abnormal event to the management station when necessary. After receiving the report of the abnormal event, the management station can inquiry the relevant agent in order to obtain more specific information and further analyze the cause of the event.
If you want to configure SNMP trap under the web page, you should click "Maintenance" in the top control bar. Then click "SNMP Trap" in the navigation bar, the SNMP Trap page appears.

23.1 SNMP Trap Basic Configuration

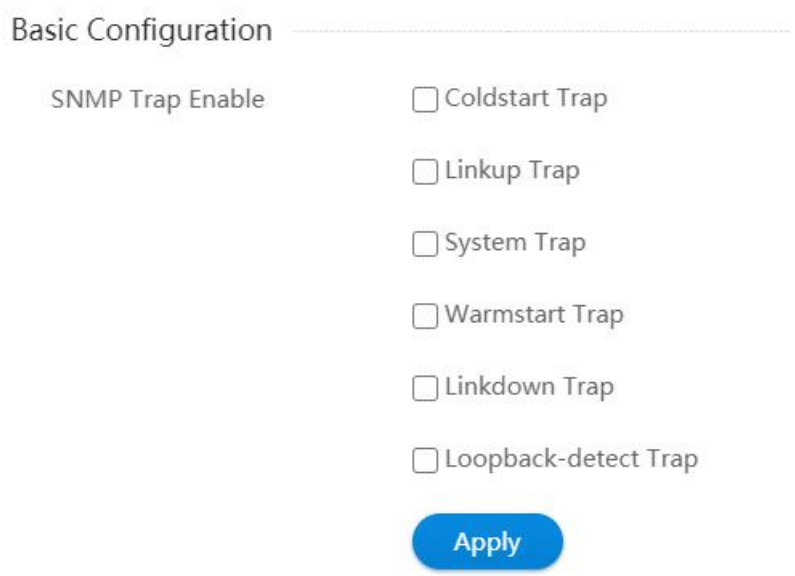


Figure 1 SNMP trap basic configuration page

- Parameter usage

Item	Description
Coldstart Trap	A Coldstart trap signifies that the sending protocol entity is re-initializing itself such that the agent's configuration or the protocol entity implementation may be altered
Linkup Trap	A Linkup trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up
System Trap	A System trap signifies that the protocol has detected a system failure
Warmstart Trap	A Warmstart trap signifies that the sending protocol entity is re-initializing itself such that neither the agent configuration nor the protocol entity implementation is altered
Linkdown Trap	A Linkdown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration
Loopback-detect Trap	A Loopback-detect traps indicate that the protocol has identified loops in the link

23.1.1 Enable SNMP Trap

If you want to enable related SNMP notification types, you should follow the steps below:

(1) Select the notification type you want to enable, and click the checkbox in front of the corresponding type name.

(2) Click the "Apply" button.

The operation is shown in figure 2.

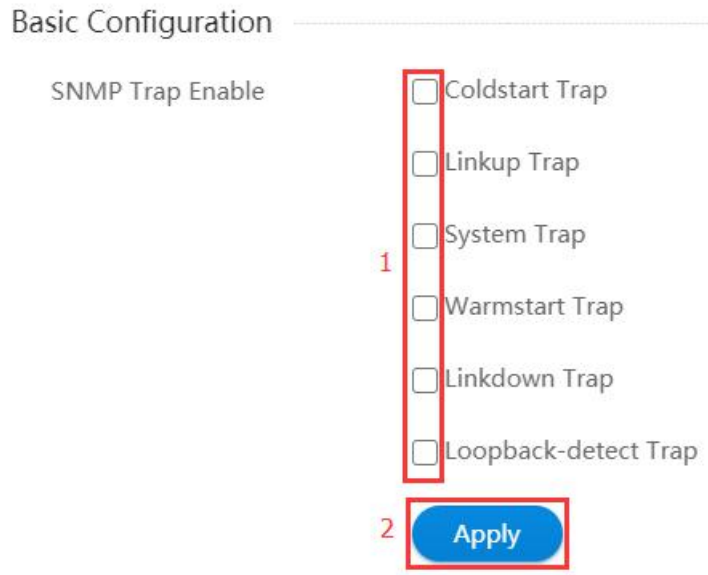


Figure 2 SNMP trap basic configuration steps

23.2 Trap Server Configuration

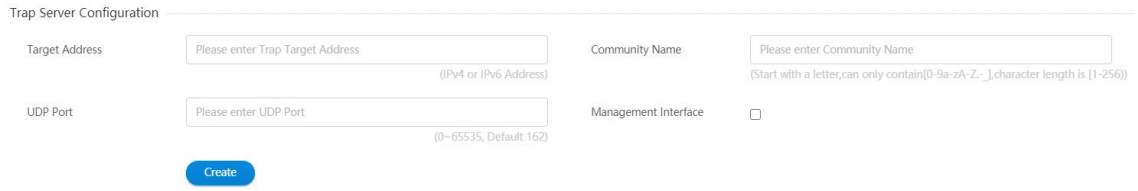


Figure 3 SNMP trap server configuration page

- Parameter usage

Item	Description
Target Address	Destination server address, IPv4 format or IPv6 format
Community Name	SNMP community name
UDP Port	Target server corresponding UDP port number
Management Interface	Whether to forward from the management port

23.2.1 Create Target SNMP Trap Server

If you want to create a target SNMP trap server, you should follow the steps below:

(1) Enter server address. The address must be in IPv4 or IPv6 format.

(2) Enter the name of the community.The legal name must start with a letter and can only include 0-9, a-z, A-Z, "_", "-", and the length must be between 1 and 256.

(3) Enter the UDP port number corresponding to the server.

(4) Select whether to forward through the management port. If not, ignore this step.

(5) Click “Create” button to create SNMP trap server.

The operation steps are shown in figure 4, and the corresponding results are shown in figure 5.

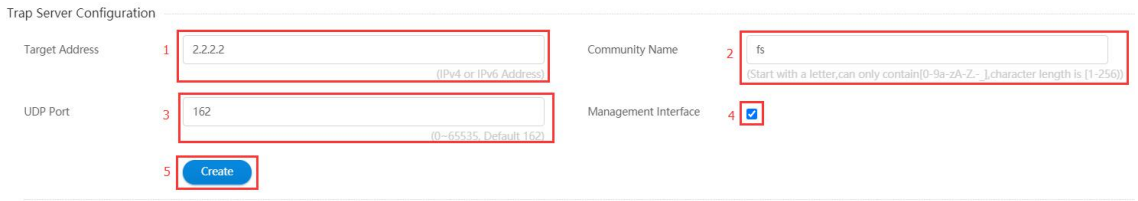


Figure 4 SNMP trap server configuration steps

Figure 5 SNMP trap server configuration result

23.2.2 Delete SNMP Trap Server

If you want to delete an existing target server, click the "Delete" behind the server list.

Figure 6 Delete SNMP trap server

24. Worm Intercept

If you click “Maintenance > Worm Intercept” in the top control bar, the worm intercept list page appears, as shown in figure 1.

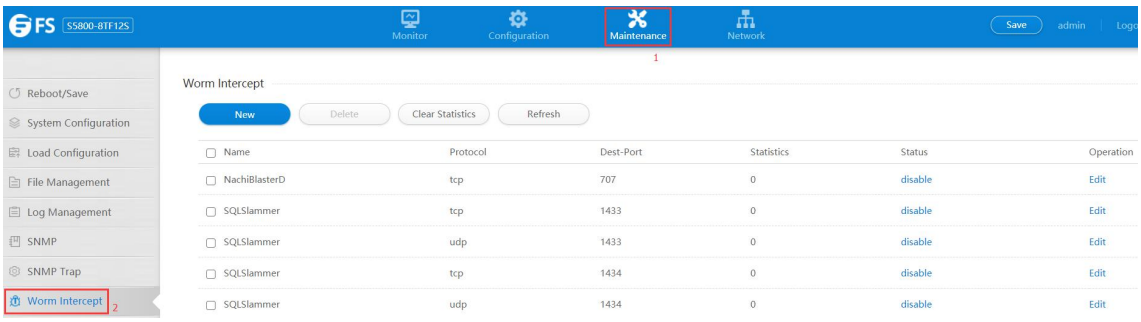


Figure 1 Worm Intercept configuration list

This chapter describes worm intercept function and viewing worm attack protection information of the switch.

24.1 Worm intercept Configuration

The worm intercept page can view worm attack protection information and add/delete rules to prevent worm attack.

24.1.1 Current Worm Intercept Information

The worm intercept information page appears, as shown in figure 2.

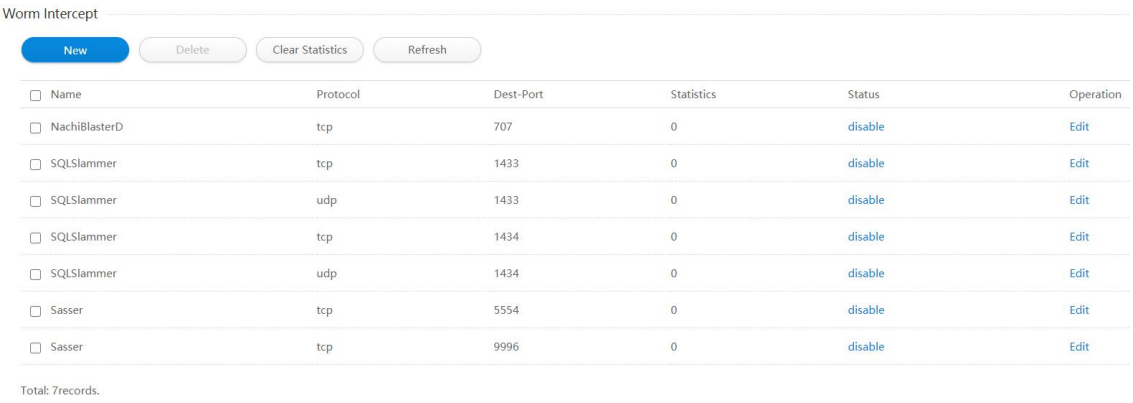


Figure 2 Worm intercept information

- Parameter usage

Item	Description
Name	Display worm attack protection rule name
Protocol	Protect this type of protocol message
Dest-Port	Display destination port of worm attack message
Statisitics	Display statistical value of defense attack message
Status	Whether the protection rule is enabled

24.1.2 Add Worm Intercept Rule

If you click "New" button, you can add a worm attack protection rule, the operation is shown in figure 3. And then the worm attack protection configuration page appears, as shown in figure 4.

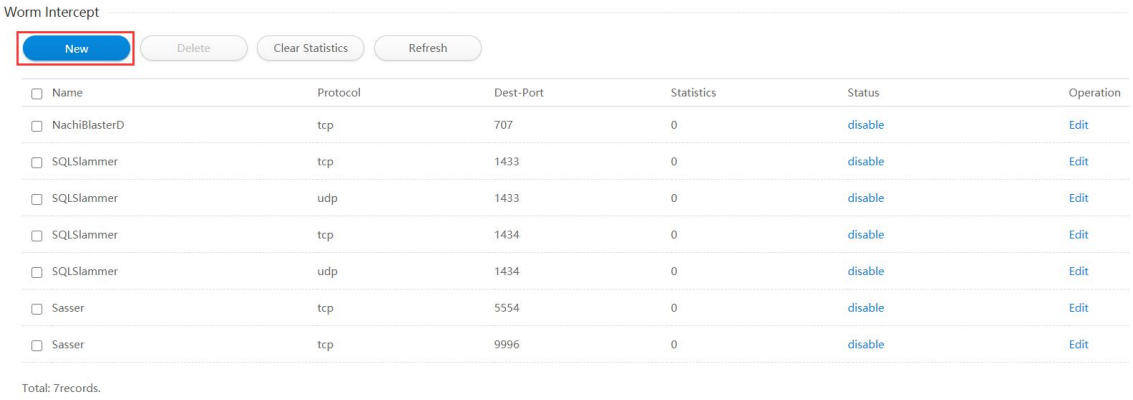


Figure 3 Add worm intercept rule operation

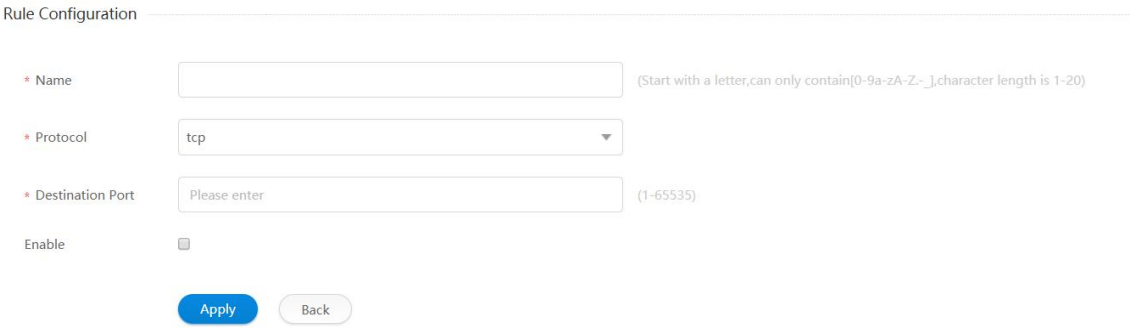


Figure 4 Add worm intercept rule configuration

- Parameter usage

Item	Description
Name	Set worm attack protection name
Protocol	Set Protect protocol type, udp or tcp
Destination Port	Create destination port number of filter message
Enable	Whether to enable this protection rule

If you want to add the worm attack protection rule, you can follow the following steps:

(1) Enter a worm attack protection name in the "Name" textbox, what needs to be noted is the name need to start with a letter, it can only contain [0-9a-zA-Z.-¥], character length is 1-20.

(2) Select protocol type in the "Protocol" dropdown box.

(3) Enter destination port in the "Destination Port" textbox.

(4) Select enable in the "Enable" square box.

(5) Click the "Apply" button to add the new worm attack protection rule.

The operation is shown in figure 5, worm intercept rule will be added to the end of the table is shown in figure 6 and you can also see the total rule numbers at the end of the table. If there are too many rules, you can drag the mouse to pull down the page.

Figure 5 Add worm intercept rule configuration

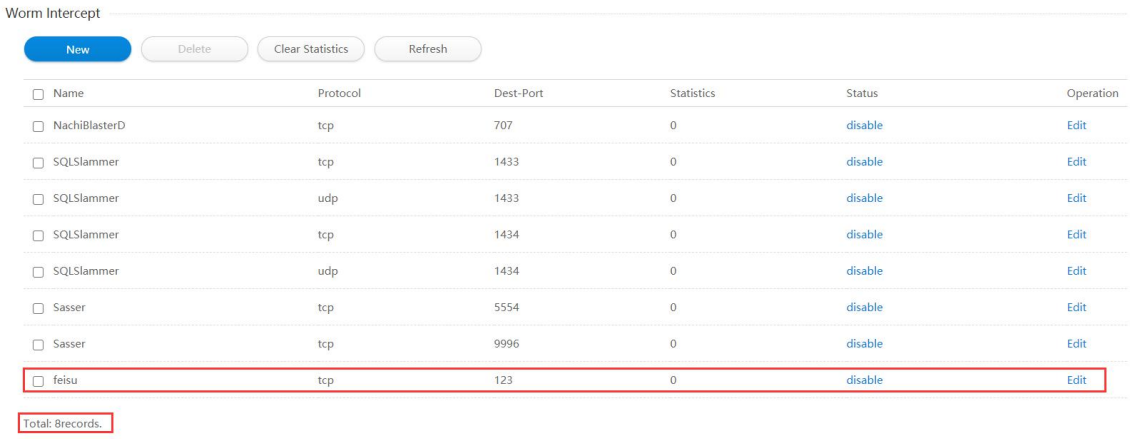


Figure 6 New worm intercept rule information

24.1.3 Delete Worm Intercept Information

If you want to delete the specified worm intercept information, you can follow the following steps:

(1) Select this specified worm attack protection information which you want to delete.

(2) Click "Delete" button.

(3) Confirm to delete the selected worm attack protection information and page appears as shown in figure 7, if you click "Confirm" button, you can delete this worm intercept rule, if you click "cancel" button, you can cancel the operation.

The operation is shown in figure 7.

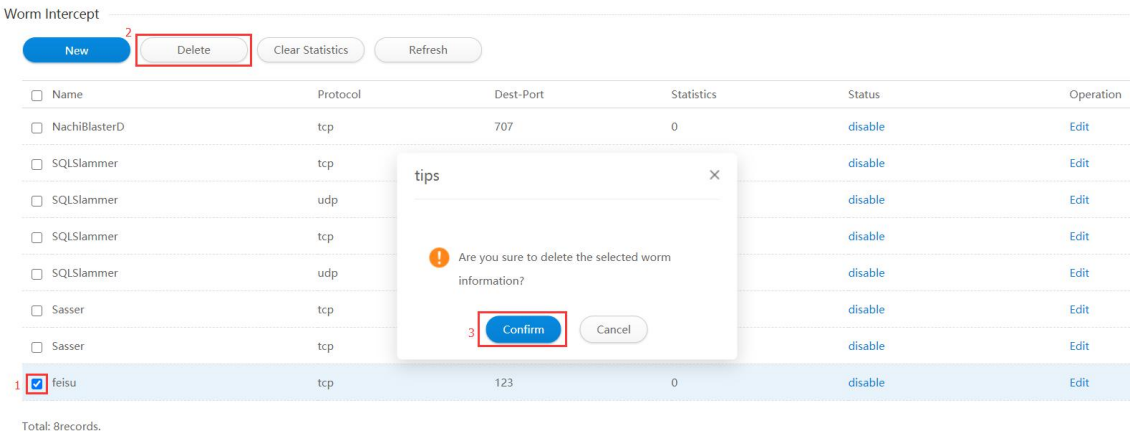


Figure 7 Delete worm intercept information

24.1.4 Clear the Defense Attack Packet Statistics

If you want to clear the specified worm attack protection packet statistics, you can follow the following steps:

(1) Select this specified worm attack protection information which you want to clear statistics.

(2) Click "Clear Statistic" button.

(3) Confirm to clear statistics of the selected worm attack protection information and page appears as shown in figure 8, if you click "Confirm" button, you can delete this worm intercept rule, if you click "cancel" button, you can cancel the operation.

The operation is shown in figure 8.

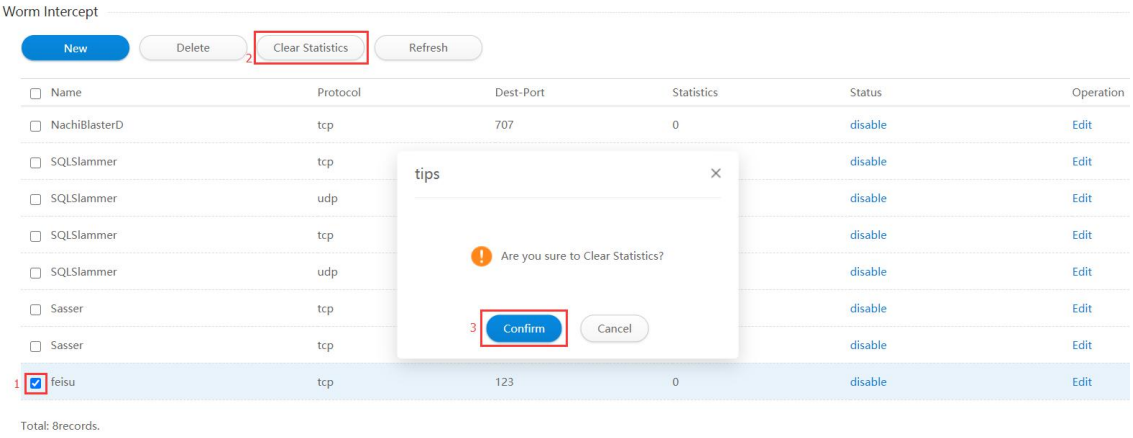


Figure 8 Clear statistics operation

24.1.5 Refresh Worm Intercept Page

If you add/delete worm intercept information or clear statistics but the operation doesn't Immediately effect, please click "Refresh" button to refresh the worm intercept page and the operation is shown in figure 9 .

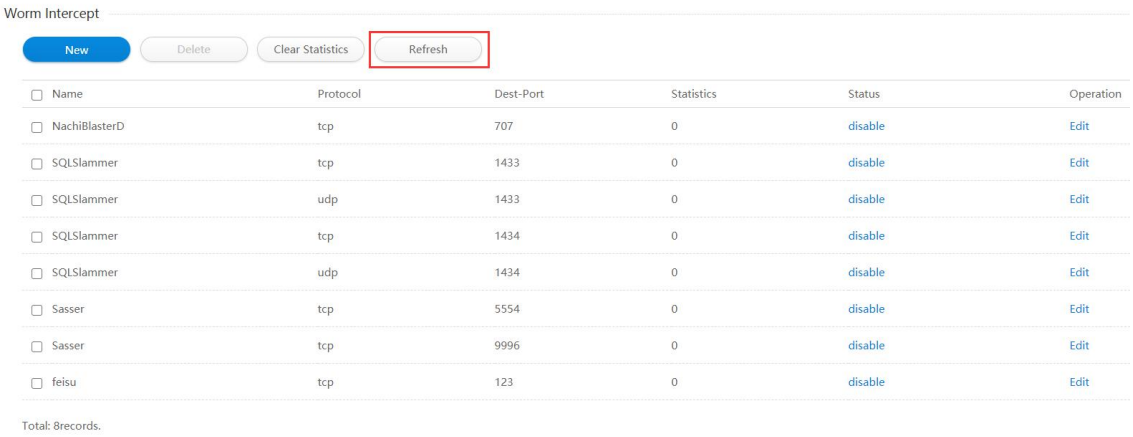


Figure 9 Refresh worm intercept page

25. DDoS Intercept

A DDoS (distributed denial of service attack) refers to multiple attackers in different locations launching attacks on one or several targets simultaneously, or an attacker controls multiple machines in different locations , and use these machines to attack the victims at the same time. Because the attack points are distributed in different places, this type of attack is called a distributed denial of service attack.

In order to prevent DDoS attacks, you can set DDoS interception. DDoS interception settings can limit DDoS attacks according to different types of attacks.

If you want to configure DDoS interception under the web page, you should click "Maintenance" in the top control bar. Then click “DDoS Intercept” in the navigation bar, the DDoS Intercept page appears.

25.1 DDoS Intercept Page

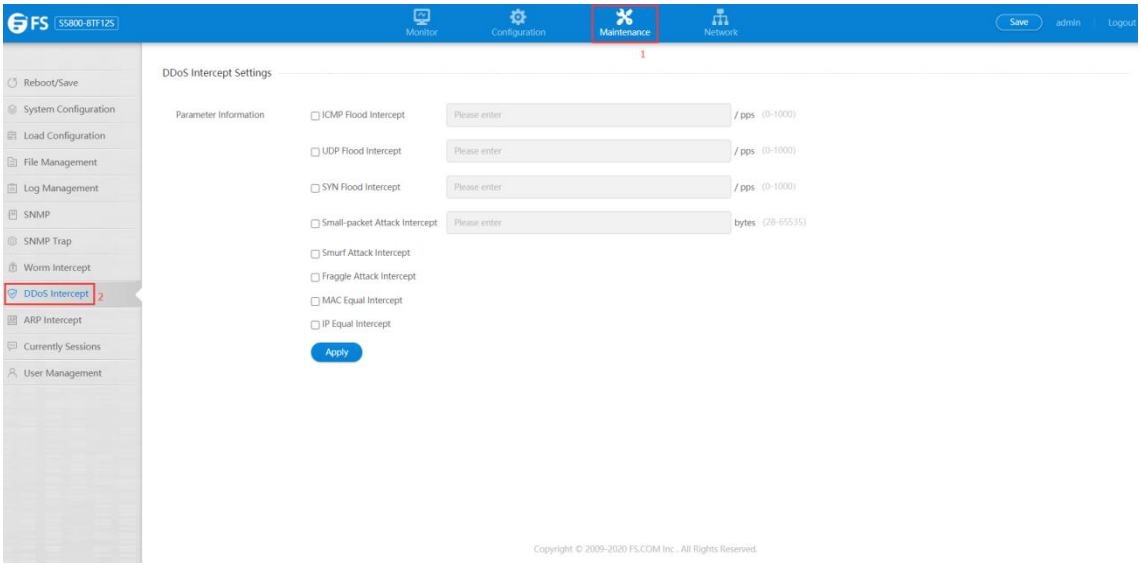


Figure 1 DDoS intercept page

- Parameter usage

Item	Description
ICMP Flood Intercept	ICMP FLOOD attack sends a large number of ping packets to the destination host , consuming host resources. This interception is used to defend against ICMP
UDP Flood Intercept	The UDP Flood attack is to forge a large number of UDP packets to impact the server, resulting in service failure
SYN Flood Intercept	The SYN Flood attack is a vulnerability that uses the TCP three-factor authentication mechanism to send a large number of fake SYN packets, causing
Small-packet Attack Intercept	Small-packet Attack includes UDP and SYN attack,etc. Because most Small-packets are meaningless and are often used for DDoS attacks, they can be intercepted based on Small-packets
Smurf Attack Intercept	The Smurf attack is a virus attack named after the program "Smurf" that originally launched the attack. This attack method uses a combination of IP spoofing and ICMP reply methods to flood the target system with a large number of network transmissions, causing the target system to refuse to serve normal systems

Item	Description
Fraggle Attack Intercept	Fraggle attack is similar to Smurf attack, but it uses UDP reply message instead of ICMP reply
MAC Equal Intercept	The MAC Equal attack is to mimic ARP request packets with both the source and destination MACs as the destination host's MAC, causing the host to constantly consume its own memory and crash
IP Equal Intercept	IP Equal attack is to imitate ICMP Ping packets whose source IP and destination IP are the destination host IP, causing the host to constantly consume its own memory and cause a crash.

The interception of ICMP flood, SYN flood, UDP flood and Small-packet attack is based on setting the PPS (packet per second) threshold to achieve defense functions. Therefore, before using this interception, you need to set a threshold. The threshold range is behind the corresponding textbox.

25.2 DDoS Intercept Setting

If you want to enable one or more of the above interception methods, you should follow the steps below.

(1) Select the interception methods you want to enable, and click the checkbox in front of the corresponding methods name.

(2) If the method is ICMP flood, SYN flood, UDP flood, or Small-packet Attack, you should set the corresponding threshold, and fill in the threshold you want to set in the text edit box after the method name (Note: The range of the threshold is in parentheses after the textbox). If it is not the above four methods, ignore this step.

(3) Click the "Apply" button.

The operation steps are shown in figure 2.

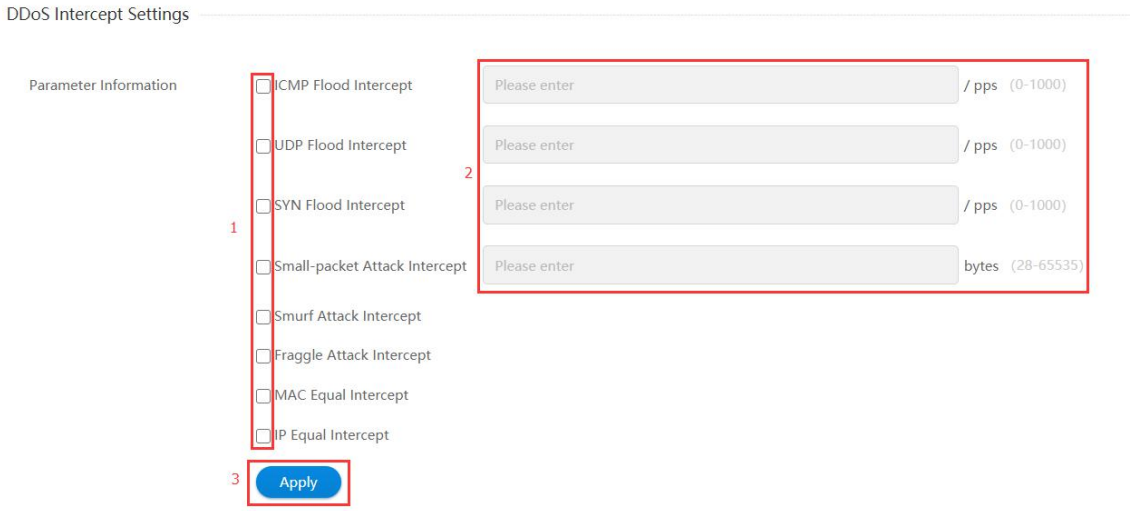


Figure 2 DDoS intercept setting

26. ARP Intercept

If you click “Maintenance ->ARP Intercept” the ARP Intercept configuration list page appears, as shown in figure 1.

If you want to enable and set arp intercept you should follow the steps below:

(1) Select “Arp Intercept” in this page.

(2) Set the threshold of the arp intercept.

(3) Click “Apply” button.

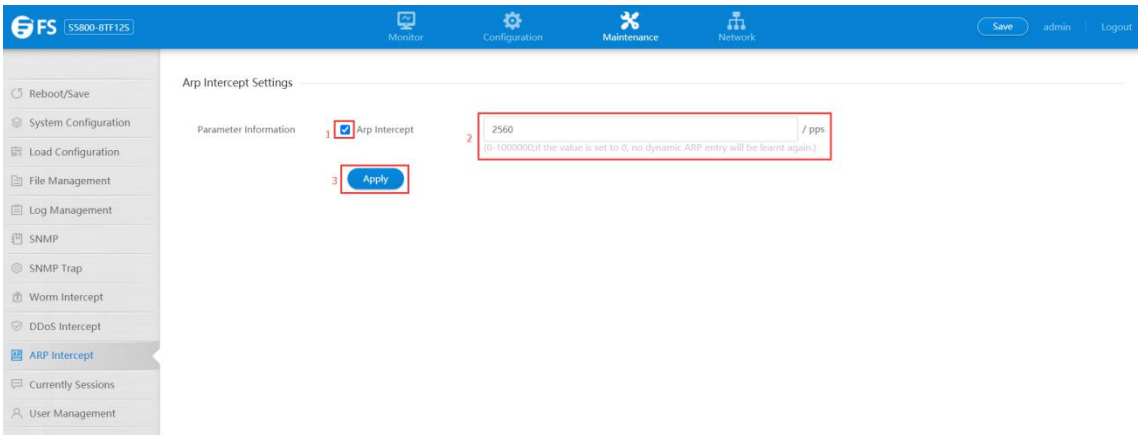


Figure 1 ARP intercept configuration list

- Parameter usage

Item	Description
PPS	Packets per second

NOTE: When you enable Arp Intercept and set threshold of PPS, every IP that exceeds the threshold will be blocked.

27. Currently Sessions

If you click "Maintenance -> Currently Sessions" in the top control bar, the currently session list page appears, as shown in figure 1.

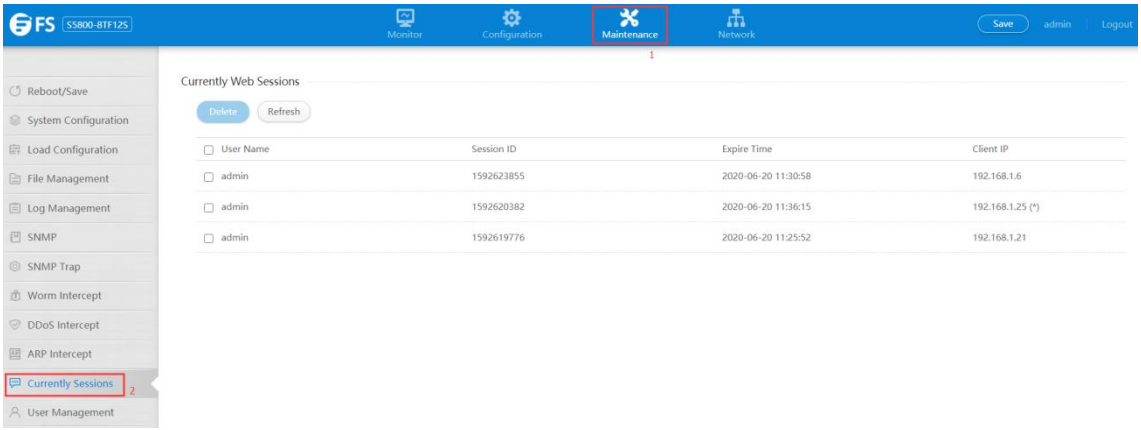


Figure 1 Current sessions list

This chapter describes the users and sessions configuration function of the device. Currently sessions display current web sessions information, and you can delete some sessions.

27.1 Current Sessions Information

Currently sessions display current web sessions information, as shown in figure 2, or you can click "Currently Sessions -> Refresh" button in the title bar, current sessions page will be refreshed and , the operation is shown in figure 3.

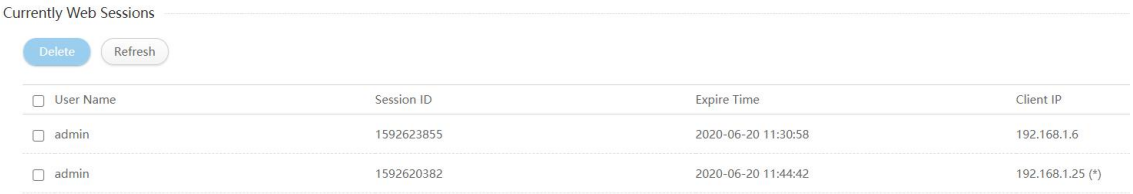


Figure 2 Current sessions information

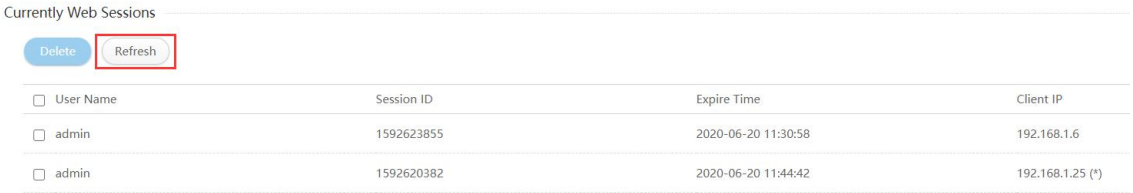


Figure 3 Refresh current sessions information

- Parameter usage

Item	Description
User Name	Display user name
Session ID	Display session id
Expire Time	Display the expire time
Client IP	Display client IP address

27.2 Delete Current Sessions

If you want to delete some sessions, you can follow the following steps:

(1) Choose one or more the sessions which you want to delete.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Delete" button, it will delete the session; if you click "Cancel" button, you will cancel the delete operation.

The operation is shown in figure 4, the result page is shown in figure 5.

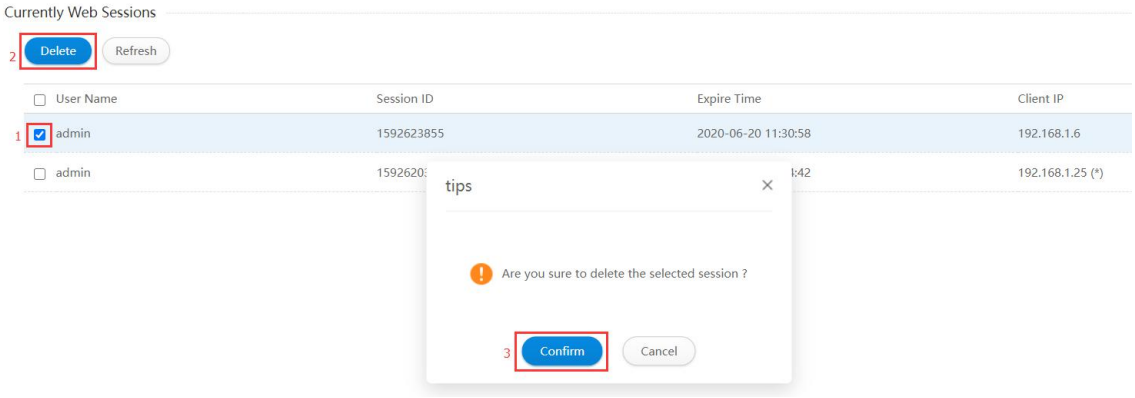


Figure 4 Delete sessions operation

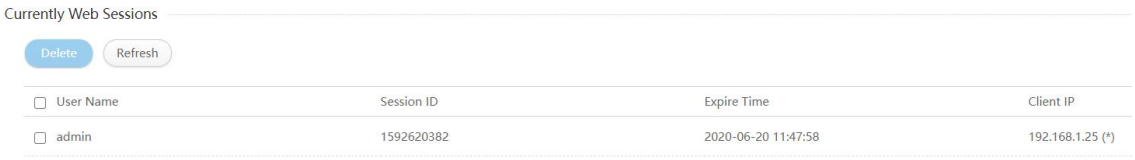


Figure 5 New current sessions information

28. User Management

If you click "Maintenance ->User Management" in the top control bar, the User Management configuration list page appears as shown in figure 1.

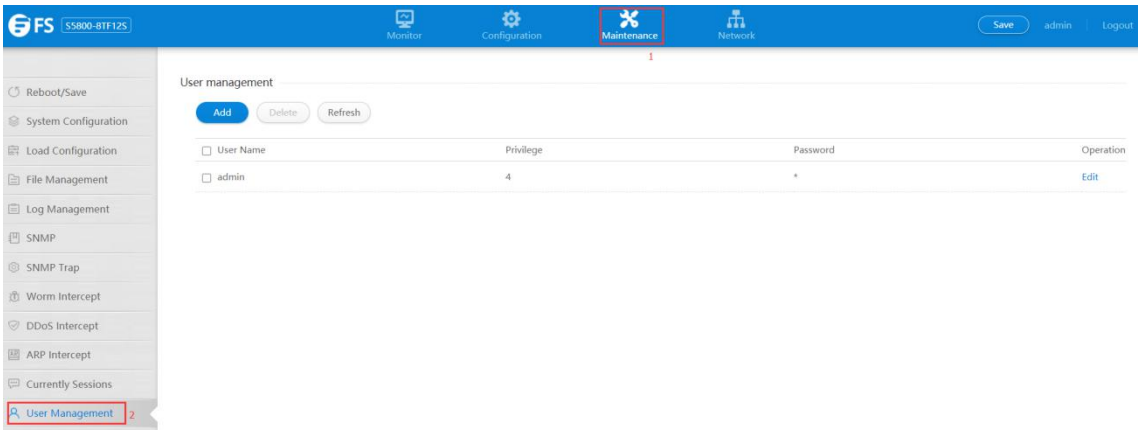


Figure 1 User management configuration list

This chapter describes user management configuration function.

28.1 Add User

If you click " Add" in User Management page you will see figure 2 and figure 3 .

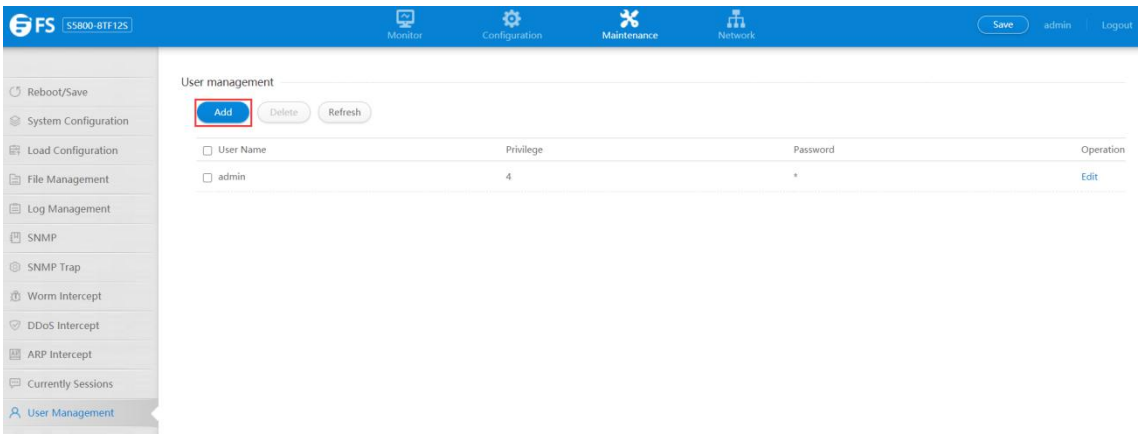


Figure 2 User add page

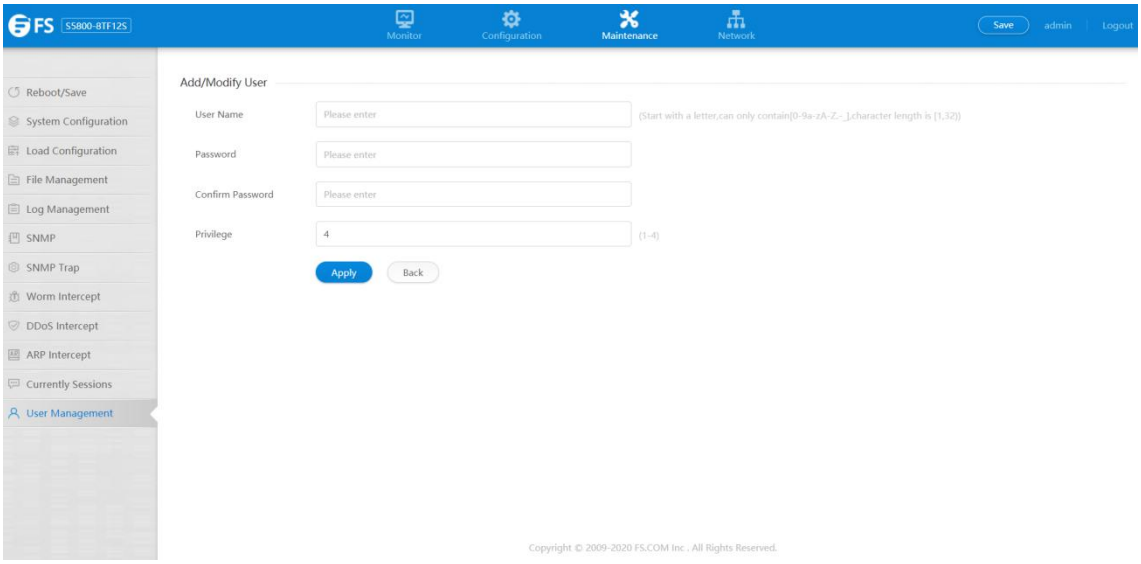


Figure 3 Add/Modify User page

- Parameter usage

Item	Description
User name	user name
Password	user`s password
Confirm password	input Pssword again
Privilege	Privilege of User(1-4)

NOTE:

(1) User Privilege Level 1: You can execute commands for functions such as network diagnostics. Including commands such as ping, tracert, and telnet. The results of executing commands at this level cannot be saved to the configuration file.

(2) User Privilege Level 2: It can execute commands for system maintenance, business fault diagnosis, and other functions. Including commands such as debugging and terminal. The results of executing commands at this level cannot be saved to the configuration file.

(3) User Privilege Level 3: It can execute commands for service configuration, including network-level commands such as routing, to provide network services to users.

(4) User Privilege Level 4: At the highest level, you can run all commands: commands related to the basic operation of the system and functions of the system support module. These commands provide support to the business. Including file system, FTP, TFTP, XModem download, user management commands, level setting commands, etc.

28.2 Edit User

If you click “Edit” after you selected a user in User Management page you will see figure 4 and figure 5.

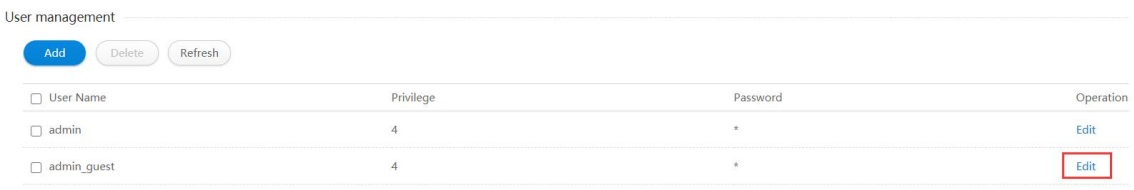


Figure 4 Edit user

Figure 5 Edit user

The corresponding operation steps are the same as those of User Add.

28.3 Delete User

If you click delete after you selected a user in User Management page you will see figure 6.

If you want to delete user, you can follow the following steps:

(1) Select the user by selecting the check box in front of the user name.

(2) Click "Delete" button.

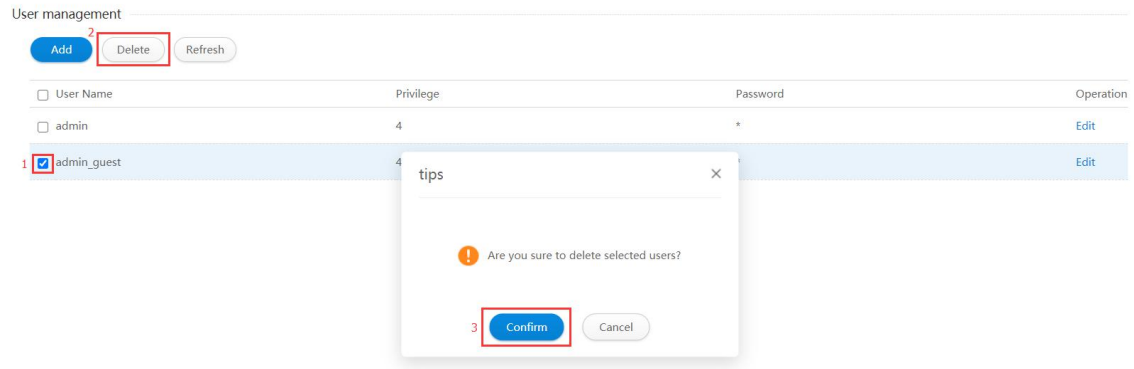


Figure 6 Delete user

28.4 Refresh

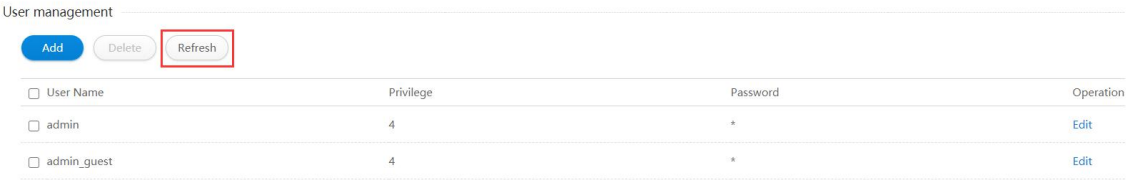


Figure 7 Refresh

NOTE: The refresh button is to refresh the current page.

29. IP Routing

If you click “Network ->IP Routing” in the top control bar, the IP routing configuration list page appears, as shown in figure 1.

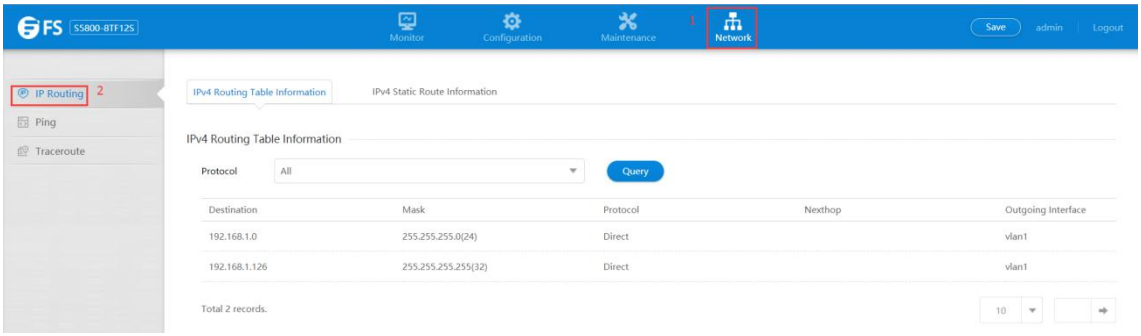


Figure 1 IP routing configuration list

This chapter describes IP static route configuration function and viewing routing information of the device.

29.1 IPv4 Route

By choosing different routing protocols, you can view the protocol routing information you want to know.

29.1.1 Current Routing Information

If you click “IP Routing -> IPv4 Routing table information” in the title bar, the IPv4 routing table information page appears, as shown in figure 2.

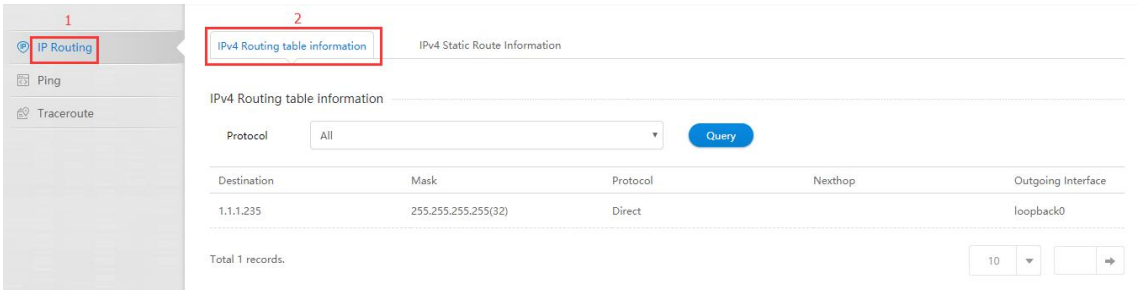


Figure 2 IPv4 routing table information

- Parameter usage

Item	Description
Destination	Display destination IP address of the route
Mask	Display IP address mask of the Destination
Protocol	Display the kind of route
Nexthop	Display nexthop of the route
Outgoing Interface	Display outgoing interface of the route

If you want to view routing information for a protocol, please select the routing protocol from the “Protocol” dropdown box, and

then click the "Query" button, the operation is shown in figure 3.

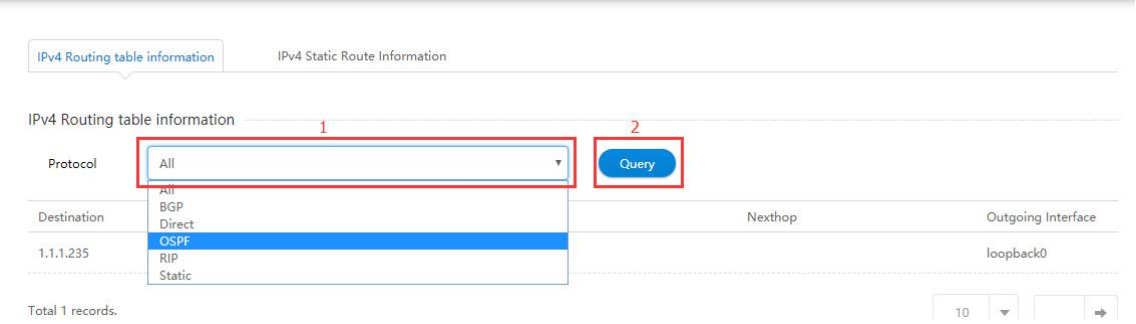


Figure 3 Select the routing protocol

29.2 IPv4 Static

Through the IPv4 static route configuration function, you can add/modified/delete the static route on device.

29.2.1 IPv4 Static Route Information

If you click "IP Routing -> IPv4 Static Route information" in the title bar, the IPv4 static routing information page appears, as shown in figure 4.

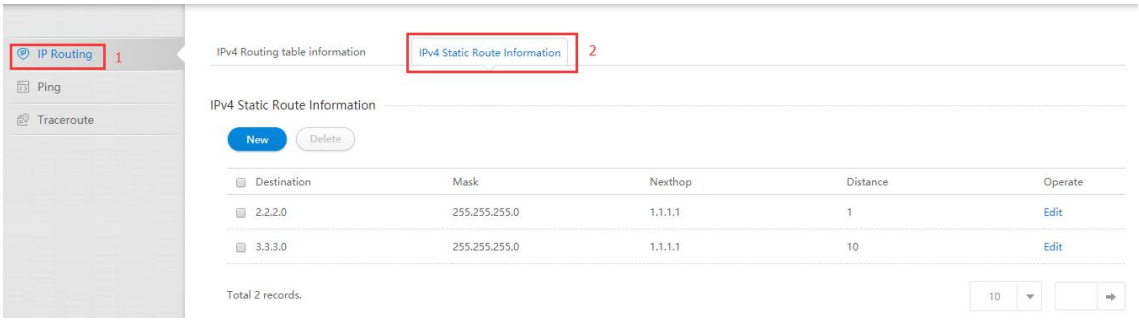


Figure 4 IPv4 static routing information

- Parameter usage

Item	Description
Destination	Display destination IP address of the route
Mask	Display IP address mask of the Destination
Nexthop	Display nexthop of the route
Distance	Display routing distance value
Operate	Display that static routing table entries can be edited

29.2.2 Add IPv4 Static Route

If you click "New" button, you can add a static route, the operation is shown in figure 5, and then the IPv4 static routing configuration page appears, as shown in figure 6.

Figure 5 Add IPv4 static route operation

Figure 6 Add IPv4 static route

- Parameter usage

Item	Description
Destination	Set specify destination IP address
Mask	Set specify IP address mask for destination
Nexthop	Set specify nexthop IP address
Distance	Set specify the distance of the static route(default is 1)

If you want to add the specified static route, you can follow the following steps:

(1) Enter an IP address in the "Destination" textbox, such as the IP address of other network device.

(2) Select the destination address mask in the "mask" dropdown box.

(3) Enter nexthop IP address in the "Nexthop" textbox.

(4) Enter route distance in the "Distance" textbox.

(5) Click the "Apply" button.

The operation is shown in figure 7, routing successfully configured table item information is shown in figure 8.

Figure 7 Add IPv4 static route configuration

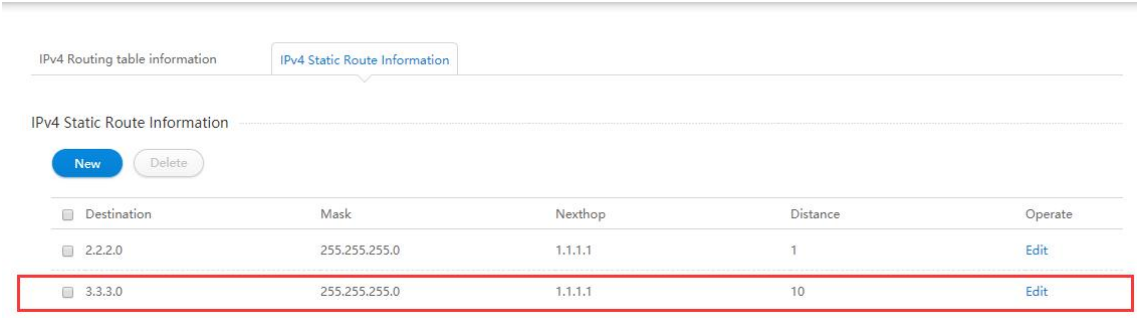


Figure 8 New IPv4 static route information

29.2.3 Delete IPv4 Static Route

If you want to delete the specified static route, you can follow the following steps:

(1) Select this specified static route which you want to delete.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, as shown in figure 9, if you click "Delete" button, it will delete the static route; if you click "Cancel" button, you will cancel the delete operation.

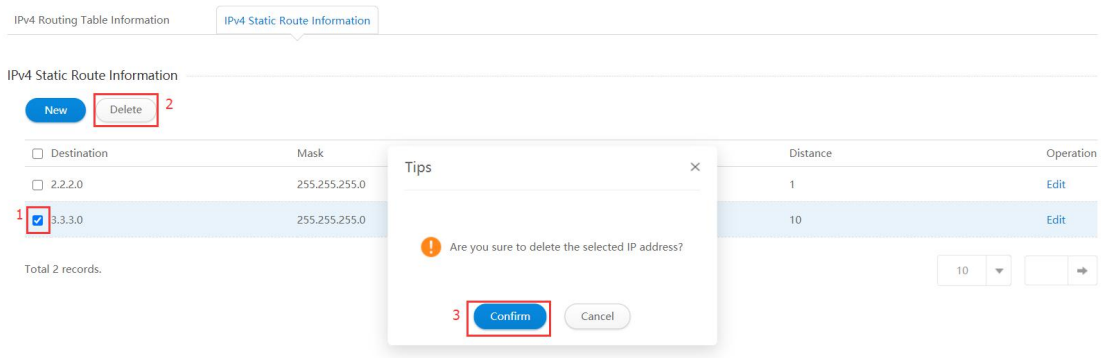


Figure 9 Delete IPv4 static route

29.2.4 Modify IPv4 Static Route

If you want to modify the configuration to specify static routing, please click "Edit" button, the operation is shown in figure 10, modifies the specified static routing page to appear, as shown in figure 11.

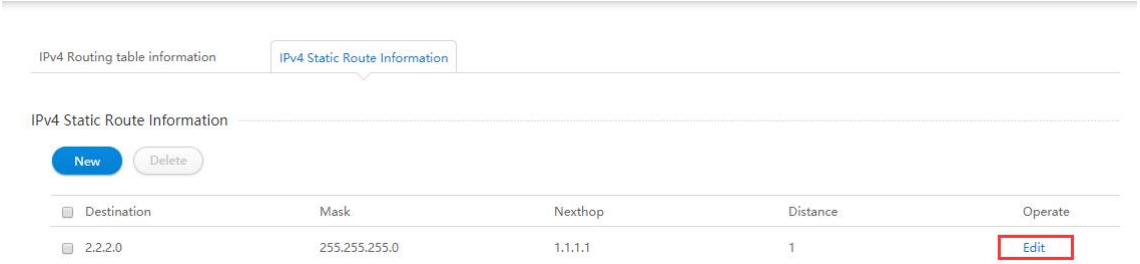


Figure 10 Modify IPv4 static route operation

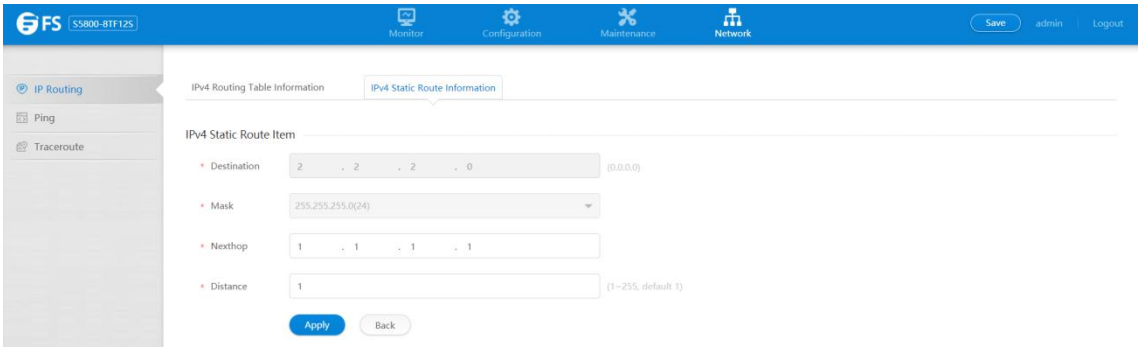


Figure 11 Modify IPv4 static route

- Parameter usage

Item	Description
Destination	Display specify destination IP address
Mask	Display specify IP address mask for destination
Nexthop	Set specify nexthop IP address
Distance	Set specify the distance of the static route(default is 1)

If you want to modify the nexthop and distance of the static route, you can follow the following steps:

(1) Modify nexthop IP address in the “Nexthop” textbox.

(2) Select the destination address mask in the “mask ” dropdown box.

(3) Modify route distance in the “Distance” textbox.

(4) Click the “Apply” button.

The operation is shown in figure 12.

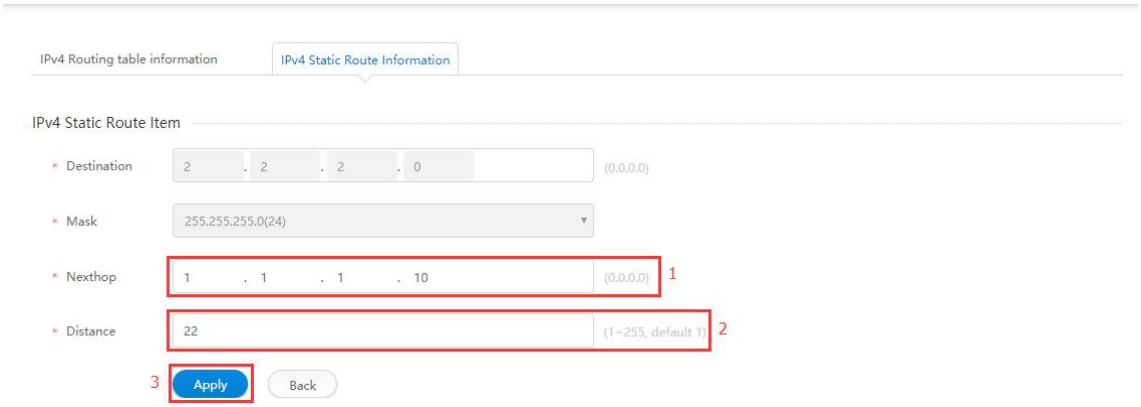


Figure 12 Modify IPv4 static route configuration

30. Ping

Users can take advantage of these features to diagnose and detect network and analyze error information.

If you click "Network-> Ping" in the top control bar, the Ping page appears, as shown in figure 1.

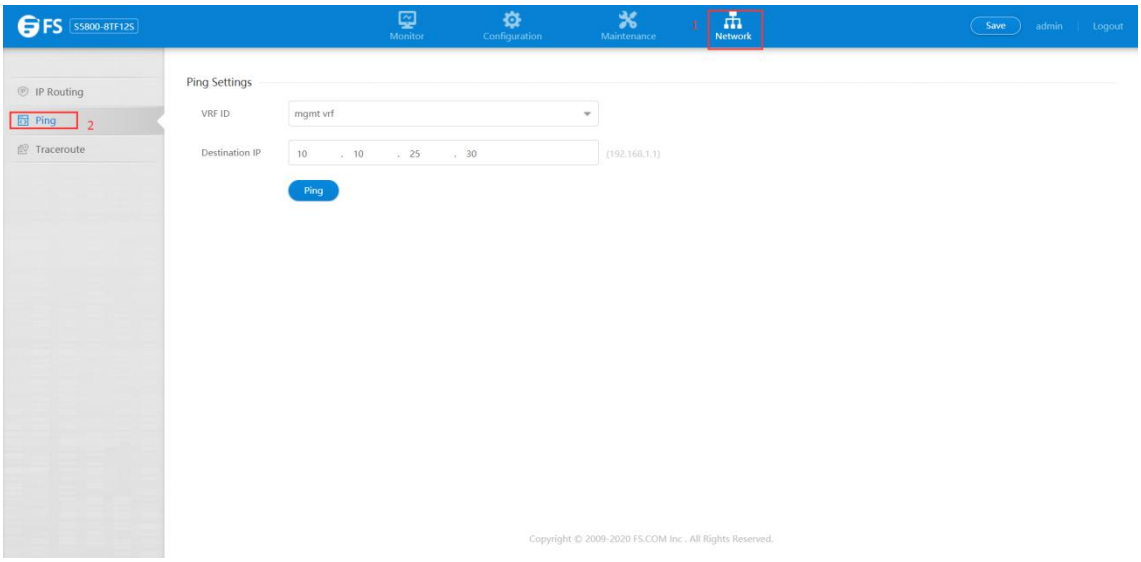


Figure 1 Ping settings

- Parameter usage

Item	Description
VRF ID	Specify ping port. Mgmt VRF means management port and default VRF means VRF1
Destination IP	Destination IP

If you want to implement ping test, you can perform the following steps:

(1) Choose the VRF ID.

(2) Enter target IP address is to be tested in Destination IP.

(3) Click the "Ping " button to test the connection.

The operation is shown in figure 2, implement ping test result is shown in figure 3.

Figure 2 Ping operation process

Figure 3 Implement ping test result

31. Traceroute

31.1 Traceroute

Tracert is a utility program used to confirm the route that IP packet will take to access the target. Tracert determines the route from a host to another host in the network by sending ICMP error packets with time-to-live (TTL) values.

If you click “Network ->Traceroute” in the top control bar, the trace route settings page appears, as shown in figure 1.

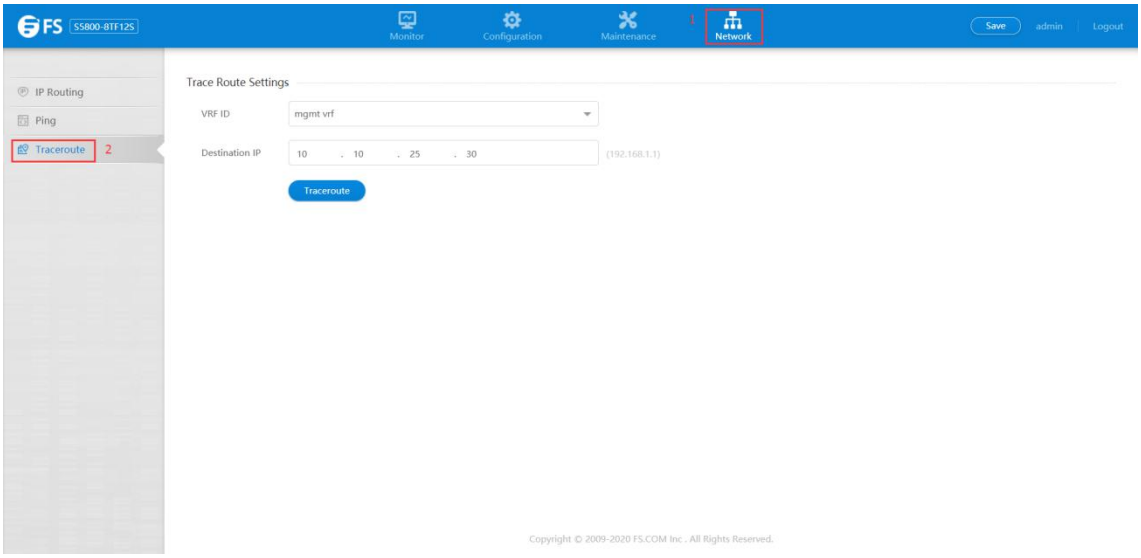


Figure 1 Trace route settings

- Parameter usage

Item	Description
VRF ID	Specify ping port. Mgmt VRF means management port and default VRF means VRF1
Destination IP	Destination IP

31.2 Implement Tracert Ping Test

Through the IPv4 static route configuration function, you can add/modified/delete the static route on switch.

If you want to implement tracert ping test, you can follow the following steps:

(1) Choose the VRF ID.

(2) Enter target IP address is to be tested in Destination IP.

(3) Click Trace Route button to test route from source address to destination address.

(4) The result will display under the configuration panel.

The operation is shown in figure 2, implement tracert ping test result is shown in figure 3.

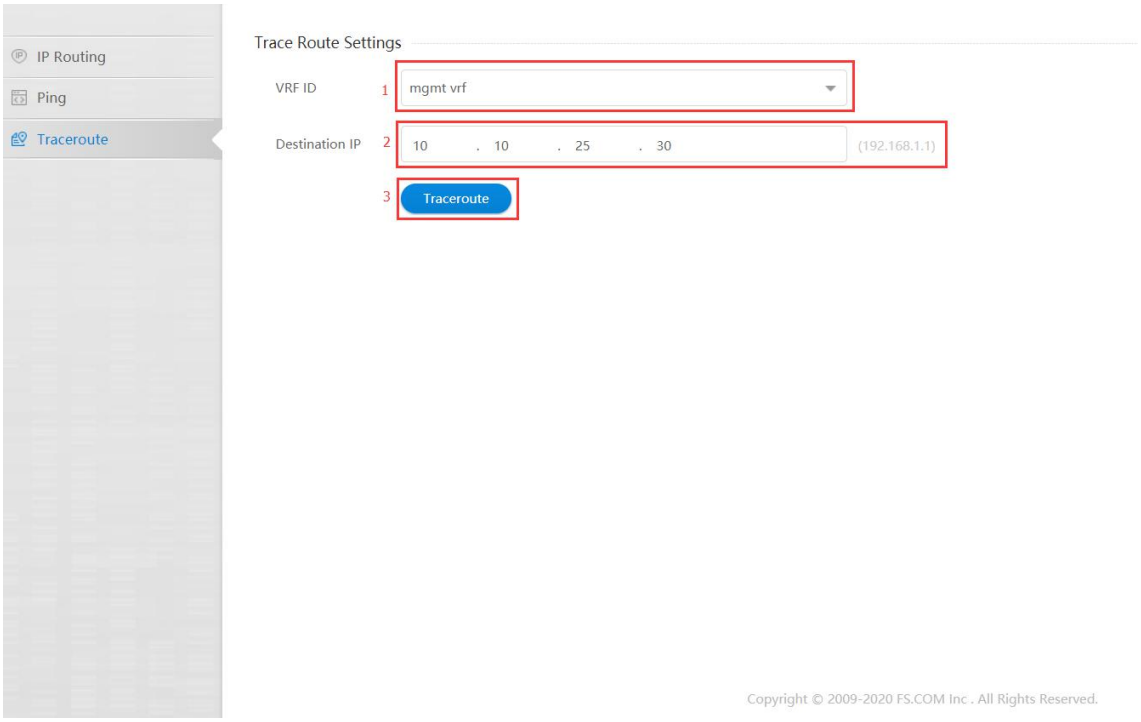


Figure 2 Implement tracert ping test configuration

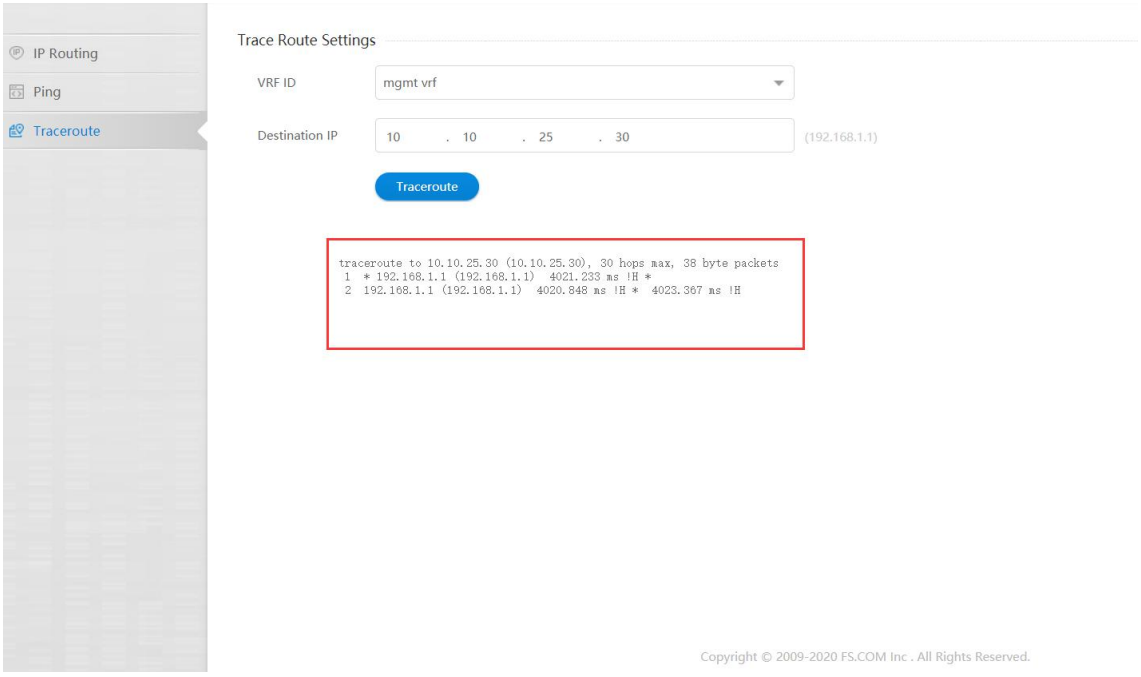


Figure 3 Implement tracert ping test result

32. Virtual Cable Test

If you click “Network->Virtual Cable Test” in the top control bar, the virtual cable test page appears, as shown in figure 1.

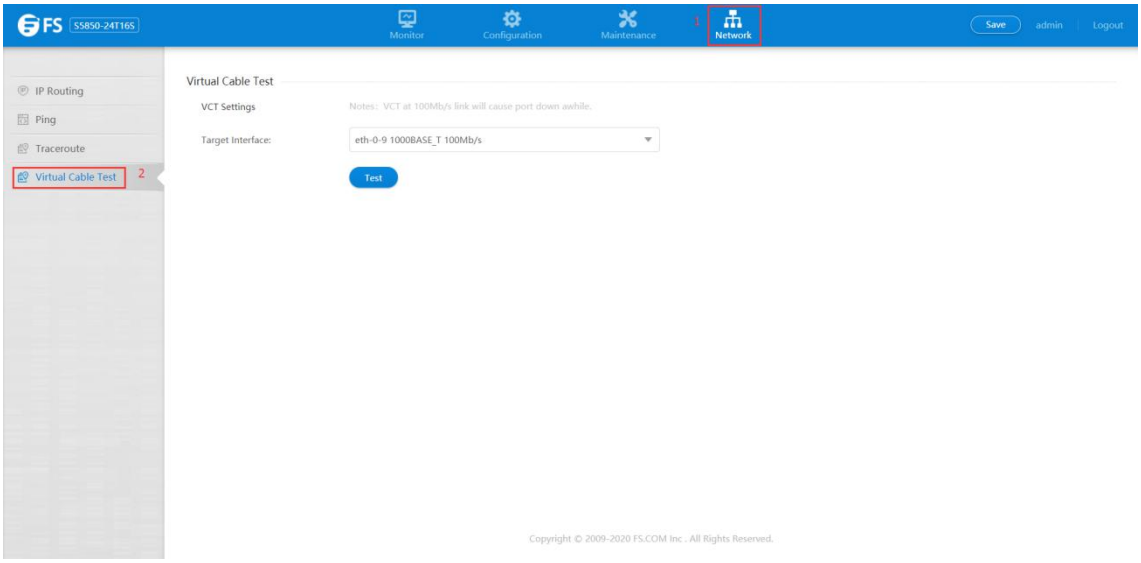


Figure 1 Virtual cable test page

This section mainly describes how to use virtual cable test to detect cable condition and error type.

- Parameter usage

Item	Description
Target Interface	Select the target interface to run VCT

If you want to perform virtual cable detection on a certain port, you can select the port you want to detect from the drop-down box, then click the “Detection” button, the operation is shown in figure 2, and the detection result is shown in figure 3.

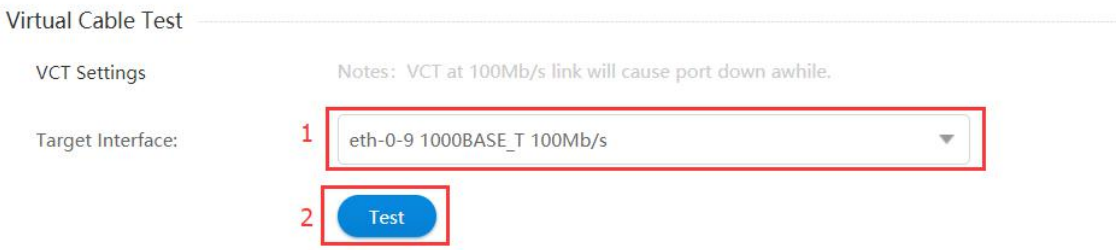


Figure 2 Virtual cable test operation

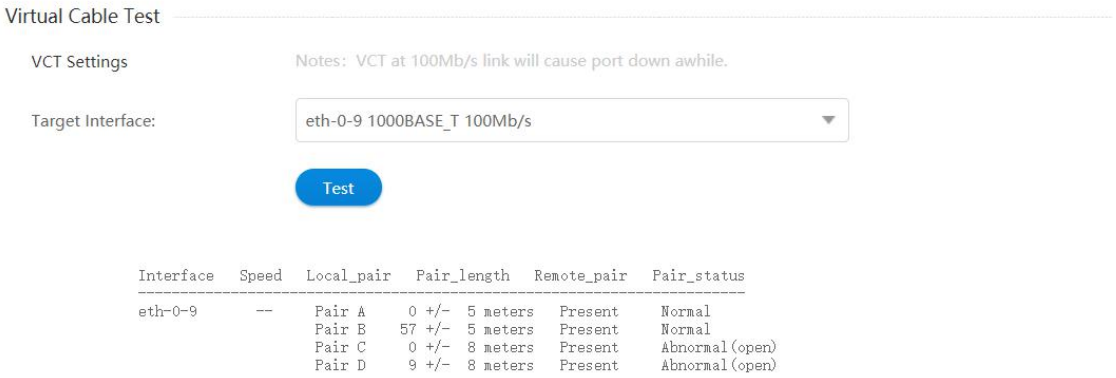


Figure 3 Virtual cable test result

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.