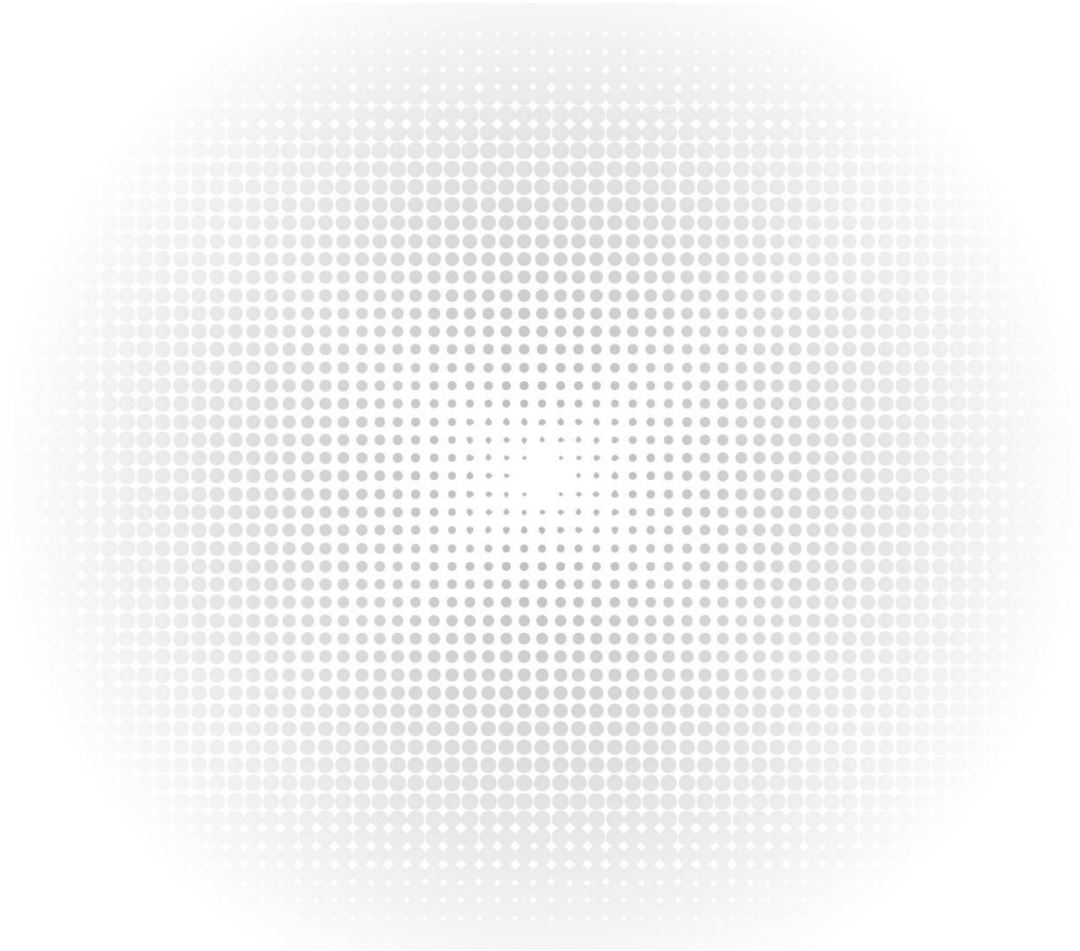
S2800S Series Switches Web Configuration Guide

Models: S2800S-8T2F-P; S2800S-8T; S2800S-24T4F-P; S2800S-24T2F; S2800S-48T4F



CONFIGURATION GUIDE

Contents

1. Web Management Landing Page

1.1 Log in to the Switch Management Page WEB

Configuration computer's IP address and the switch must be set to the same subnet (switch default IP address is 192.168.1.1, the default subnet mask of 255.255.255.0). Run WEB browser, in the address bar enter http: //192.168.1.1. Enter, enter the username and password (default username: admin; password: admin), click "Login" button or directly enter the WEB management.

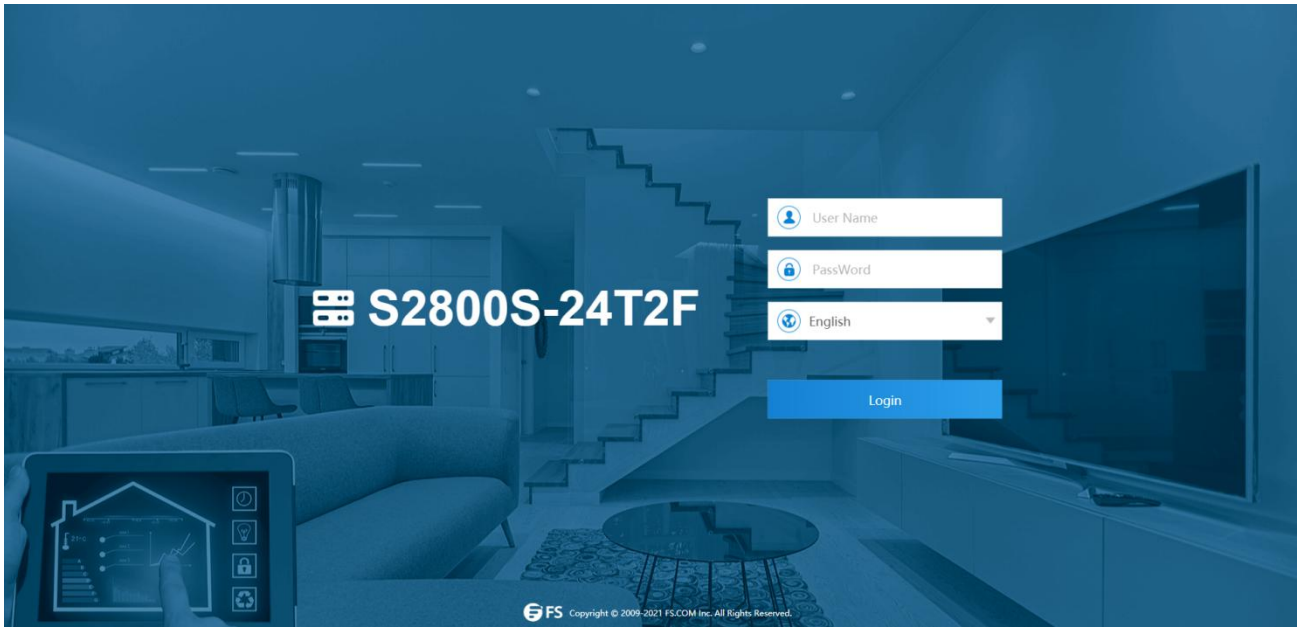


Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:

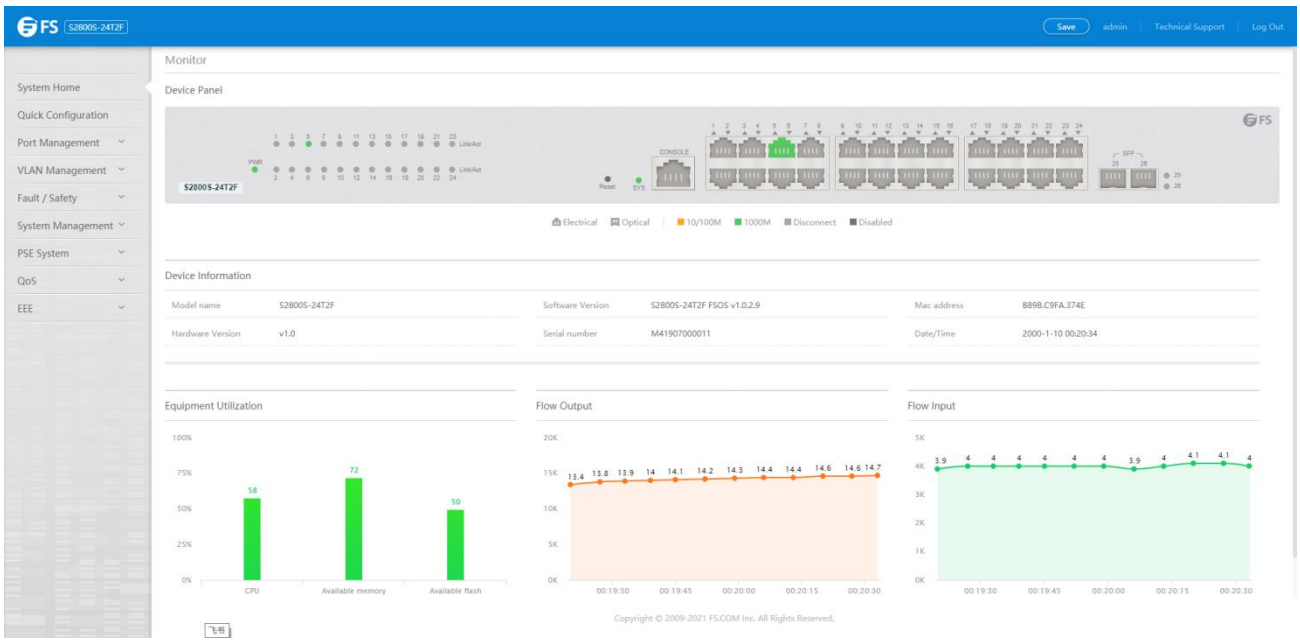


Figure 1-2: Switch WEB management page Home

2. System Home

2.1 Device Panel

1. Through the HTTP page, a quick understanding of the operation of the device, panel information, port information, such as the general network of common management information.

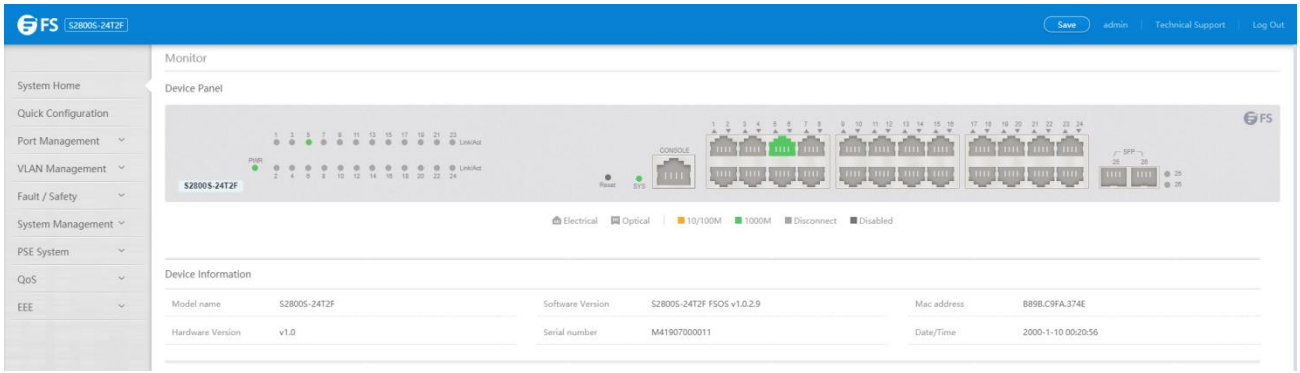


Figure 2-1: Device panel

2. Click on the specific port, you can see the following information.

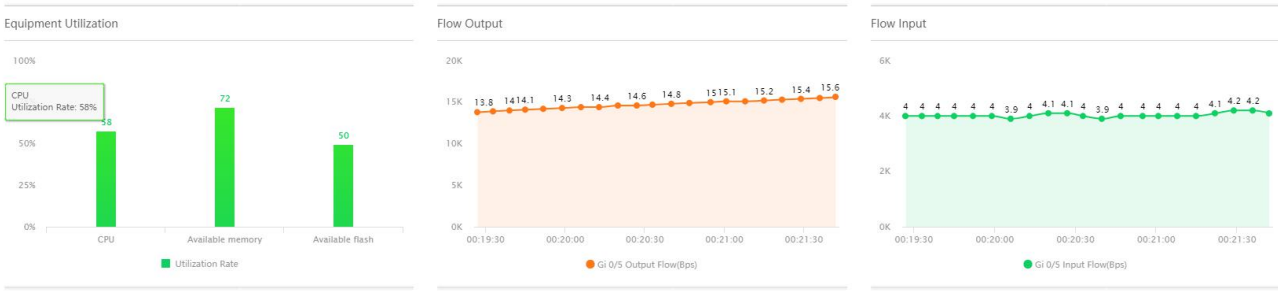


Figure 2-2: View the port status

2.2 Port Information

The configuration of the S2800S-24T2F is as follows: “System Home”, “Port Information”

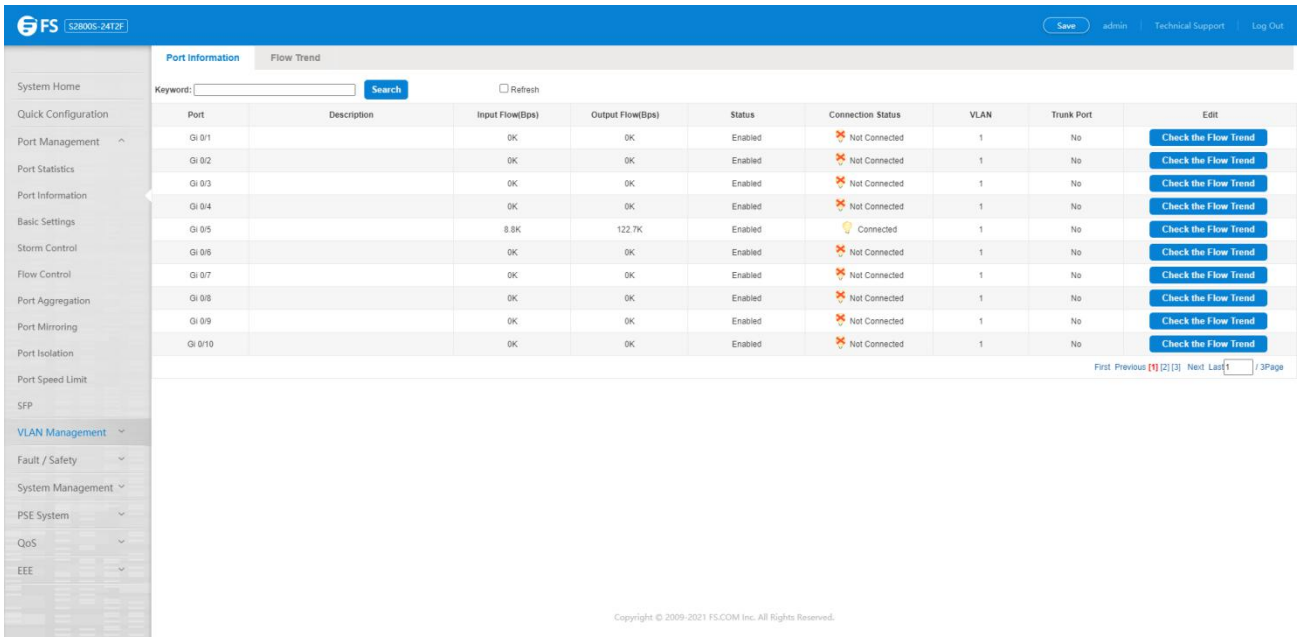


Figure 2-3: Port Information

2.3 Flow Trend

Click the check flow trend on the panel port with the mouse to view the port flow trend.

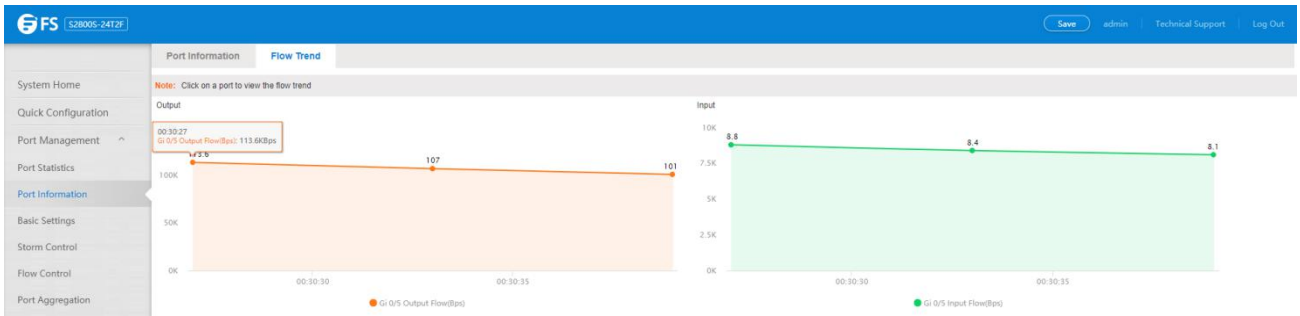


Figure 2-4: View the flow trend

2.4 Port Statistics

Through the HTTP page, the user can quickly understand the number of bytes received, the number of bytes sent, the number of incomplete packets, the number of large packets, CRC error packets, the number of conflicts.

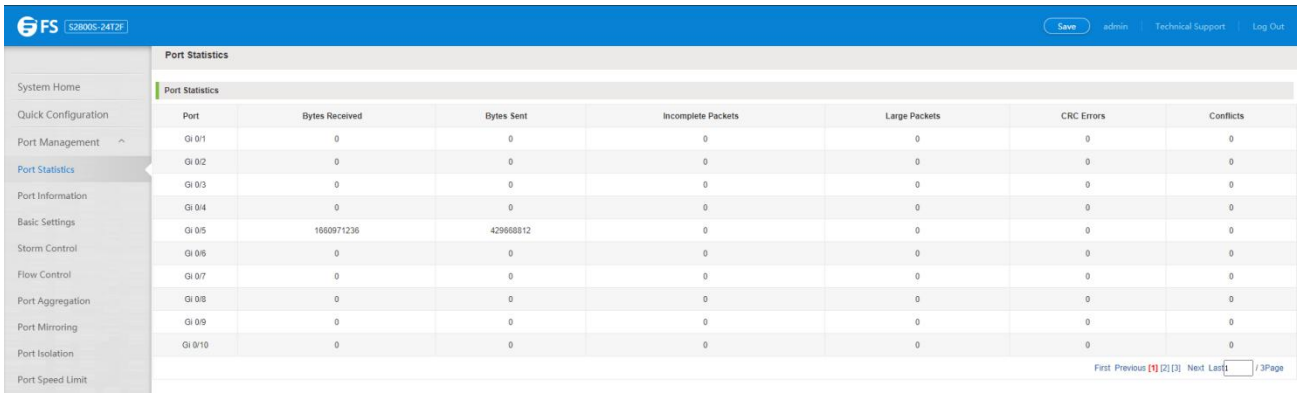


Figure 2-5: View the port Statistics

3. Quick Configuration

The quick configuration consists of four chapters. Click "Quick Configuration" to quickly configure common functions of the device, such as VLAN, trunk port, port category, etc. According to Steps, Step by Step configuration, you can also choose configuration.

3.1 VLAN Settings

Click on "Quick Configuration" "VLAN Settings" into the Quick Configuration of VLAN Configuration page. Can view the current equipment VLAN information, according to the demand of new VLAN, modify VLAN, delete VLAN, etc. after the completion of the configuration, click "Next".

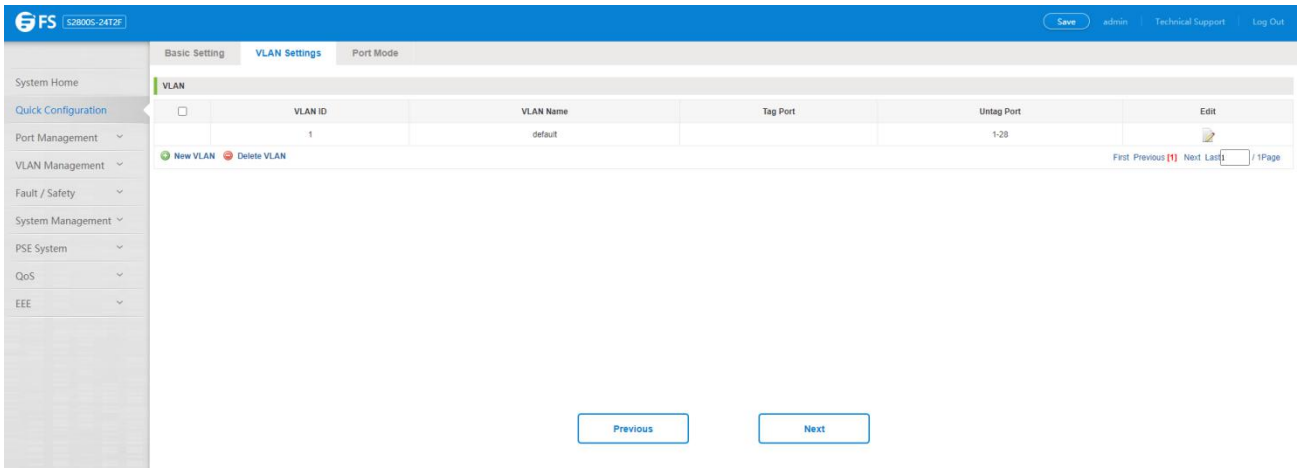


Figure 3-1: VLAN Setting

3.2 Port Mode

Click on "Quick Configuration" "Port Mode" into the port mode configuration settings page. You can change the port mode and allowed some VLANs on trunk or hybrid mode, notice: When the port is changed to trunk mode, it will be removed from the previous untagged VLAN, such as after configuration is complete, click "Next" to enter the Port Class Settings page. Or click on "Previous" back to the VLAN Settings page.

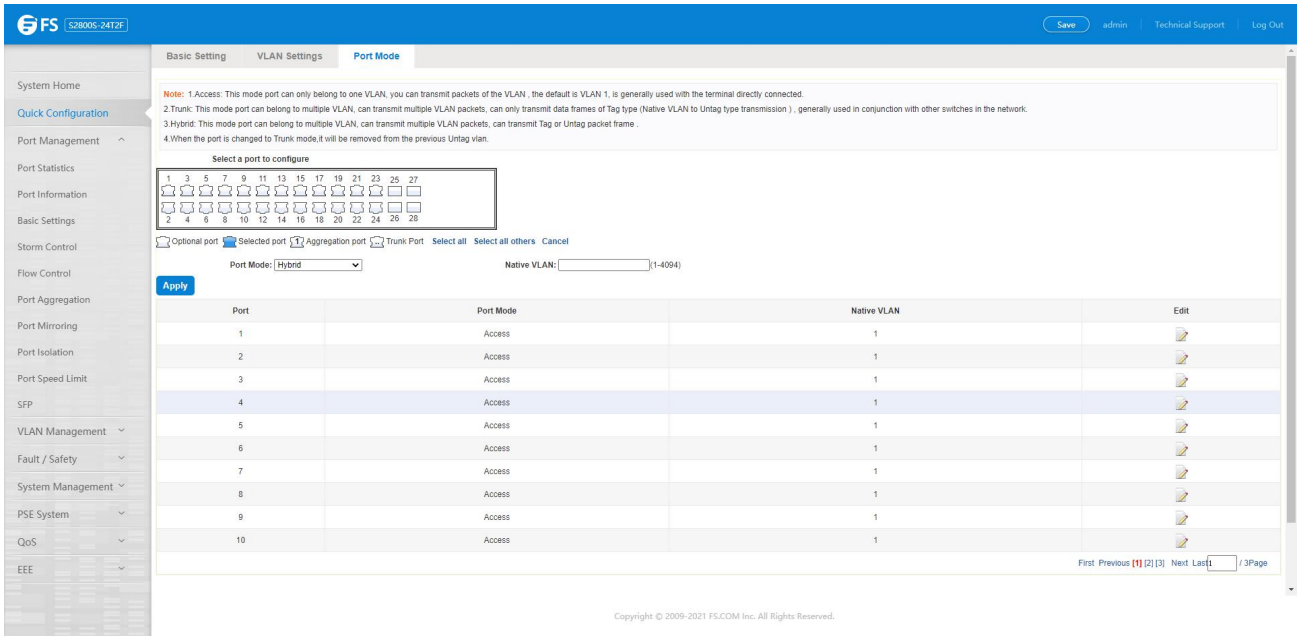


Figure 3-2: Trunk port setting

3.3 Basic Settings

Click "Quick Configuration" "Basic Settings" into the quick Configuration of equipment information system Settings page. Can the current equipment basic information system and manage password configured. End of the configuration is complete, click on "Complete" rapid configuration.

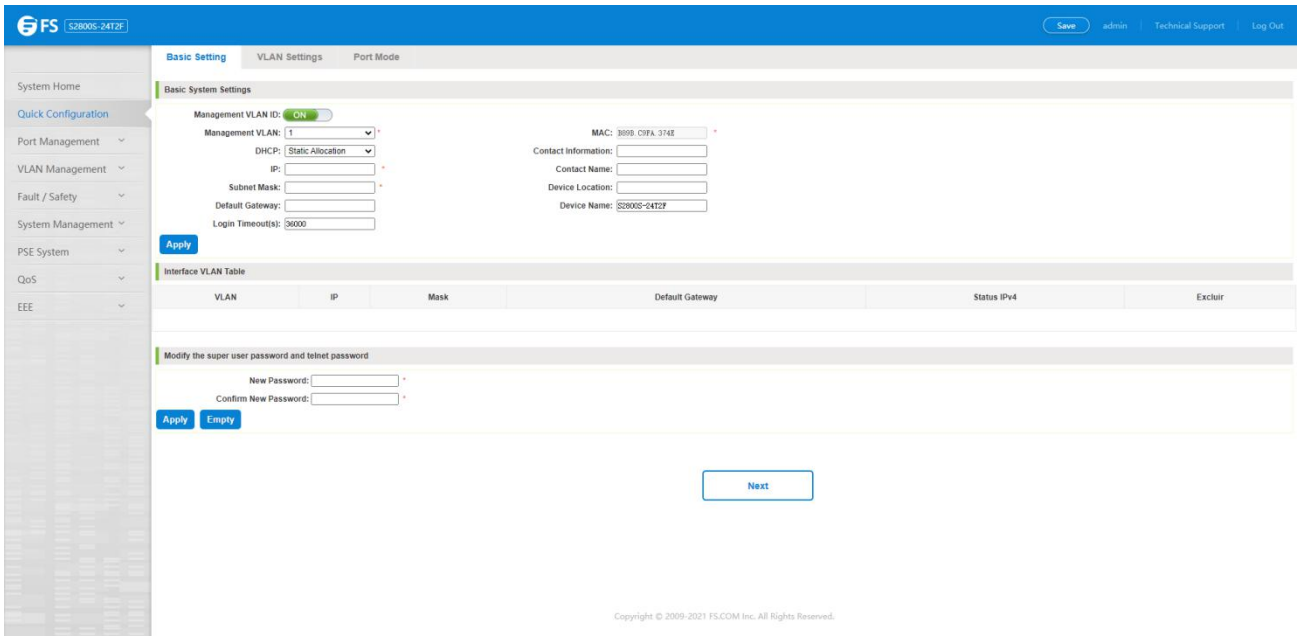


Figure 3-3: Basic settings

4. Port Management

4.1 Basic Settings

4.1.1 Check the Port Configuration

Click on the navigation bar "Port Management" "Basic Settings" to view the current configuration of the switch ports:

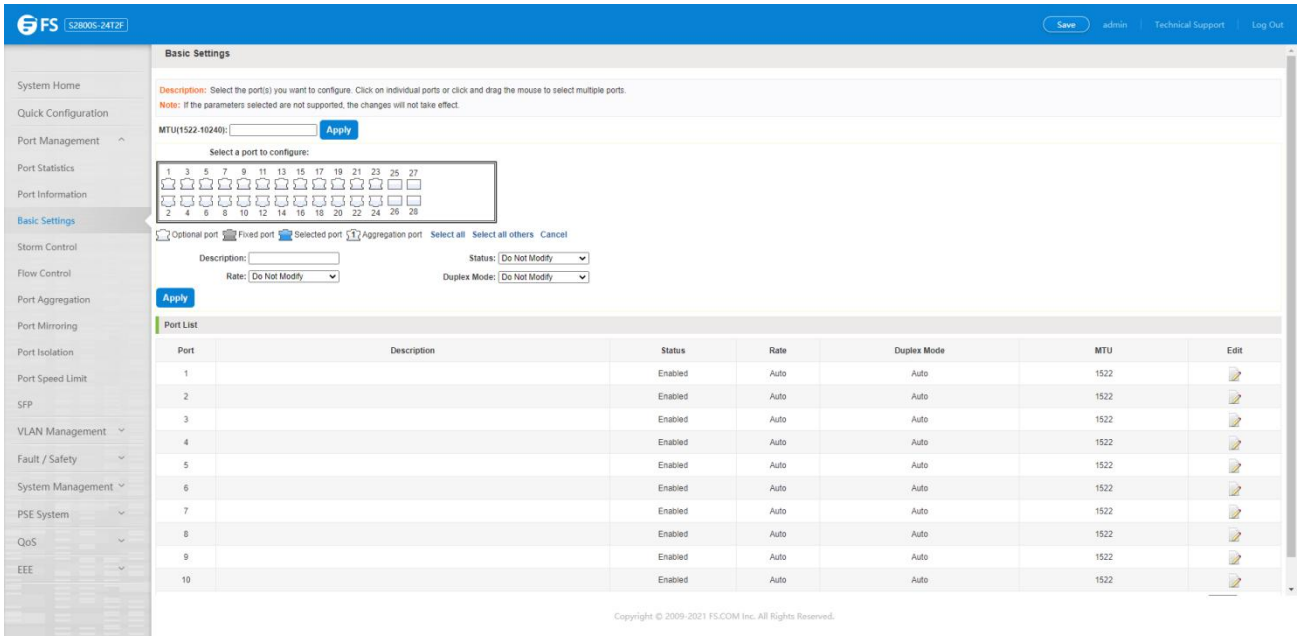


Figure 4-1: Port list information

In the port list attribute, which shows the current switch port configuration information:

1. Port: The number of the port.

2. Port Description: Displays the contents of the switch port description.

3. Port Status: Switch port status information, on/off.

4. Port Rate: Displays the switch port speed configuration, auto-negotiation /10/100/1000.

5. Working Mode: Displays the switch port configuration duplex, auto-negotiation /full/half duplex.

6. MTU: Indicates the port is the maximum length of the packet.

4.1.2 Configuring Port Properties

 After the icon, you can configure the selected port attributes:

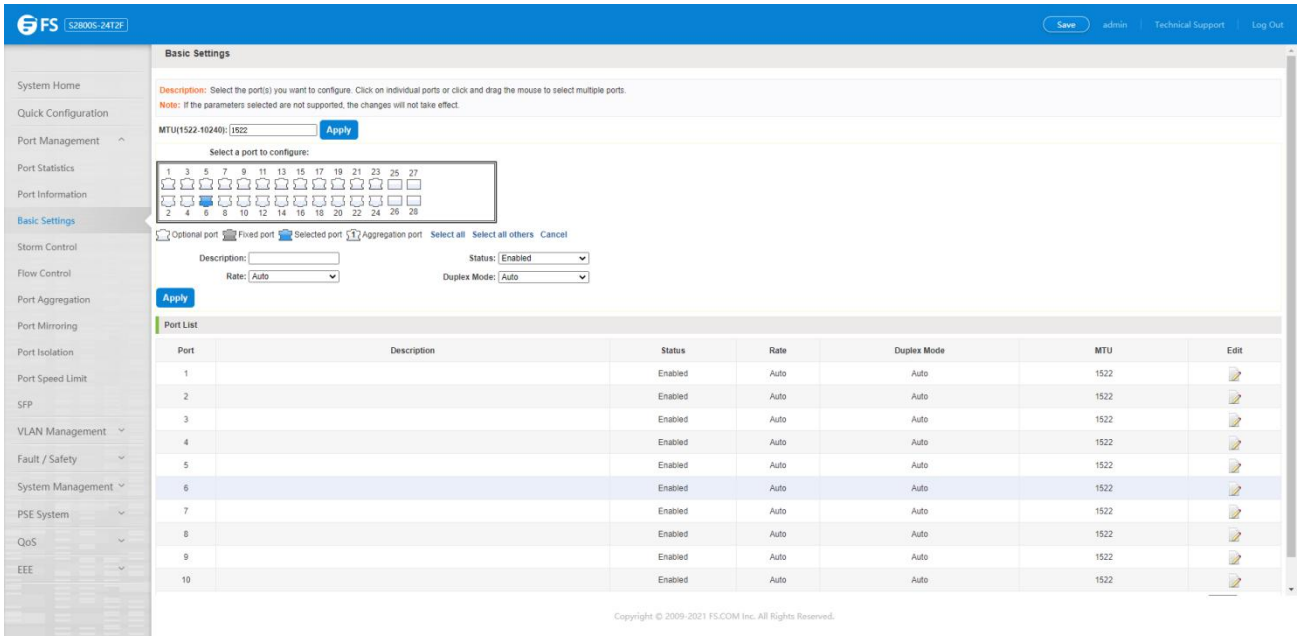


Figure 4-2: Port properties configuration of FIG.

To configure port properties as follows:

Step 1: Click the "Edit" icon ;

Step 2: In the Port Properties configuration page Fill / select the value to be configured.

Step 3: Click the "Save" button to complete the configuration.

4.2 Storm Control

4.2.1 Check the Port Settings Storm

Click on the navigation bar "Port Management" "Storm Control" to view the current switch port storm control information:

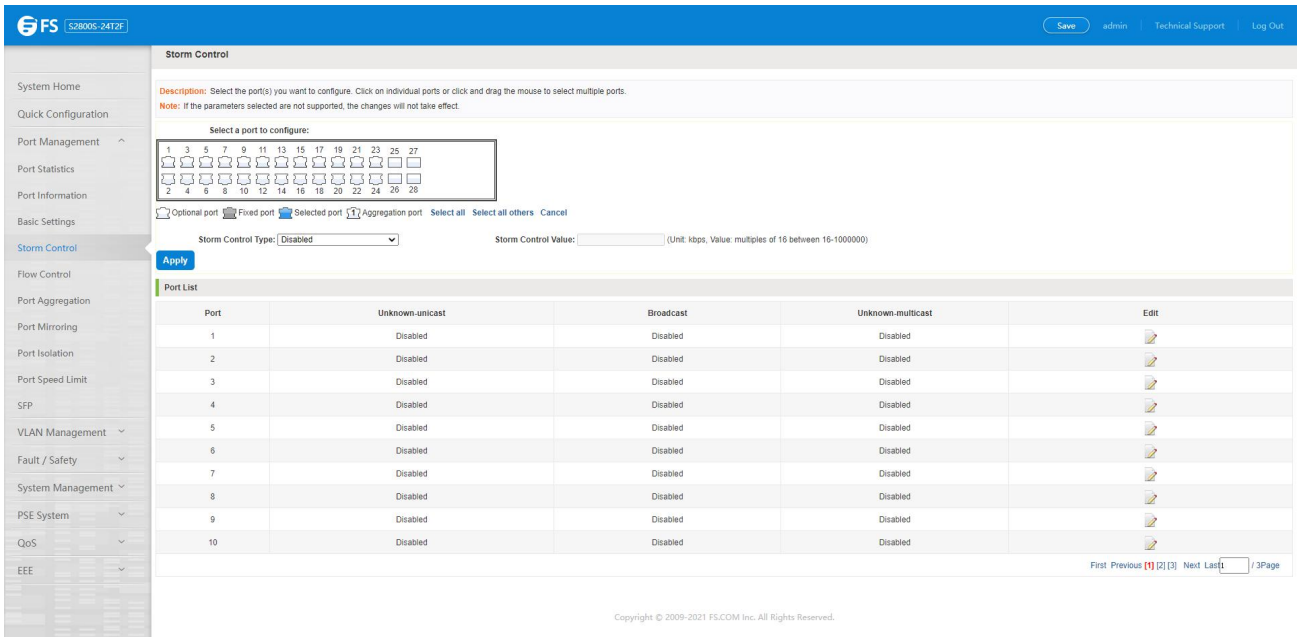


Figure 4-3: Storm control list information

In the list of ports which shows the property values of the current storm control switch:

1. Port: The number of the port.

2. Unicast: Unknown unicast packets control.

3. Broadcast: Broadcast packet control.

4. Multicast: Multicast packets control prompt.

5. When set the control value is not a multiple of 16, the system automatically matches similar multiples of 16.

6. Control value unicast, broadcast, multicast, while only a single value for the control.

By clicking on the port panel " " corresponding port", select the port to be controlled.

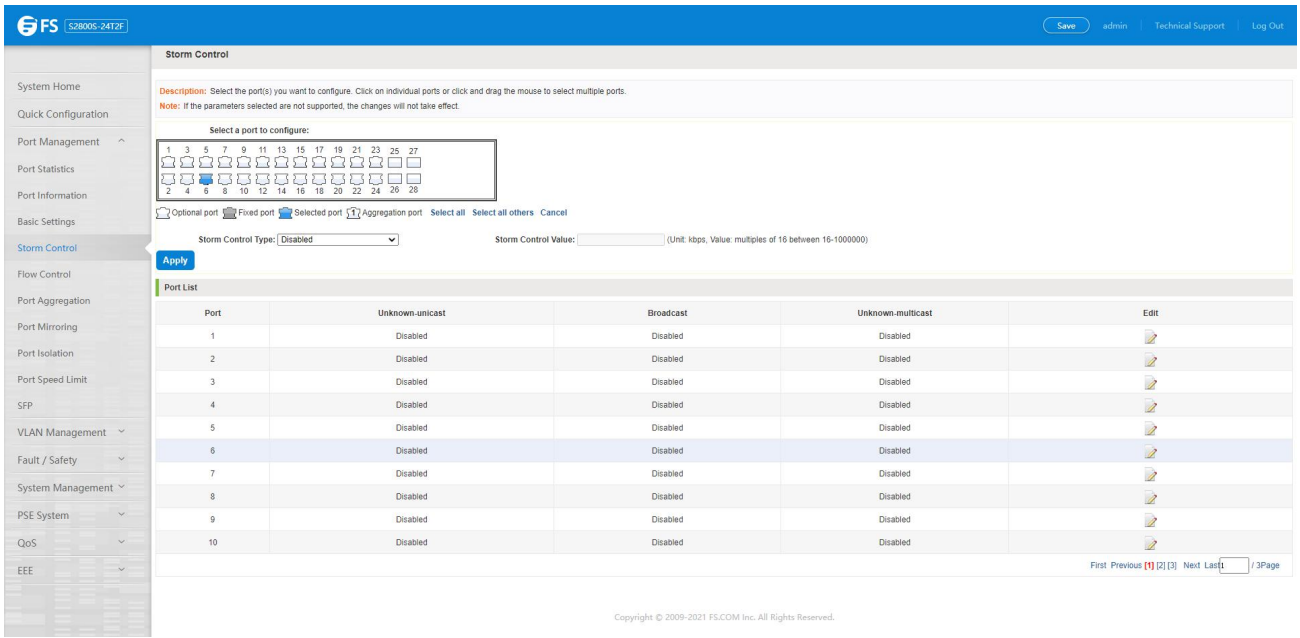


Figure 4-4: Configuring storm control information

After You can also select multiple ports, and batch editing.

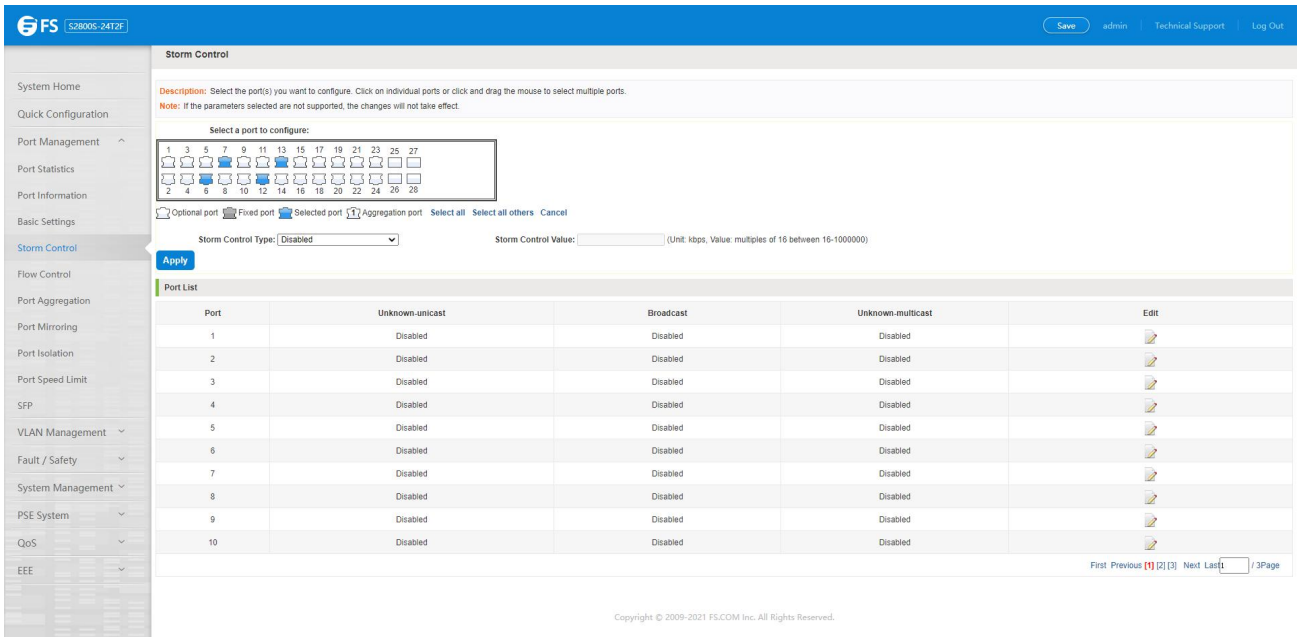


Figure 4-5: Bulk edit configuration information

After the selected ports in the Storm Control category, set the Unknown-unicast, Unknown-multicast, broadcast value, such as setting the port number 1 Unknown-unicast storm control is 1009. Click Save Settings.

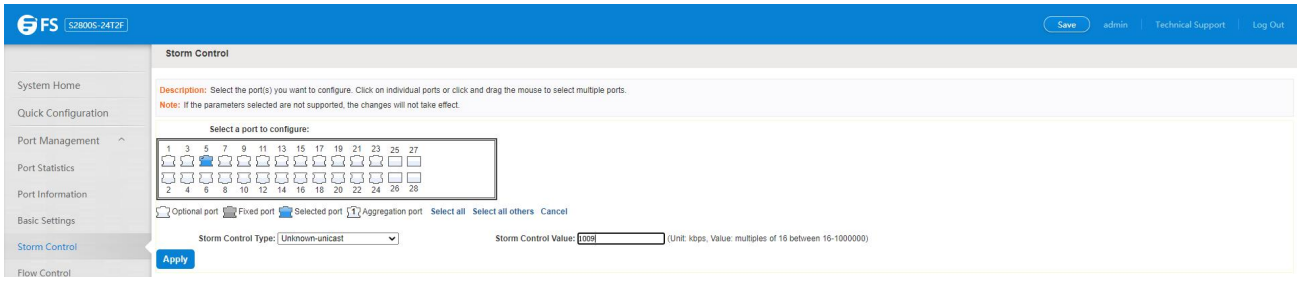


Figure 4-6: Configuring storm control information

After the configuration, as shown below:

Figure 4-7: Configuration successfully storm control information flow control

4.3 Flow Control

Click "Port Management" "Flow Control" view of the switch:

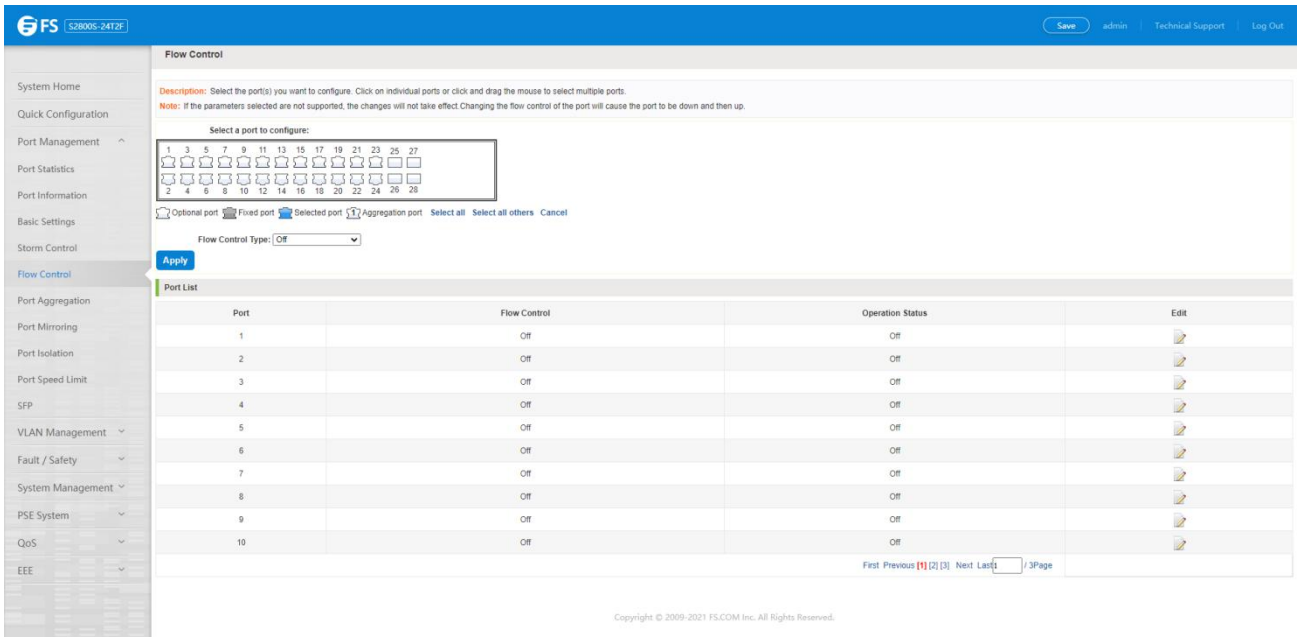


Figure 4-8: Flow control information

4.3.1 Configuring Flow Control

Open port flow control function: Select to open port traffic control, click the "Flow control type" a Select "On", "Save":

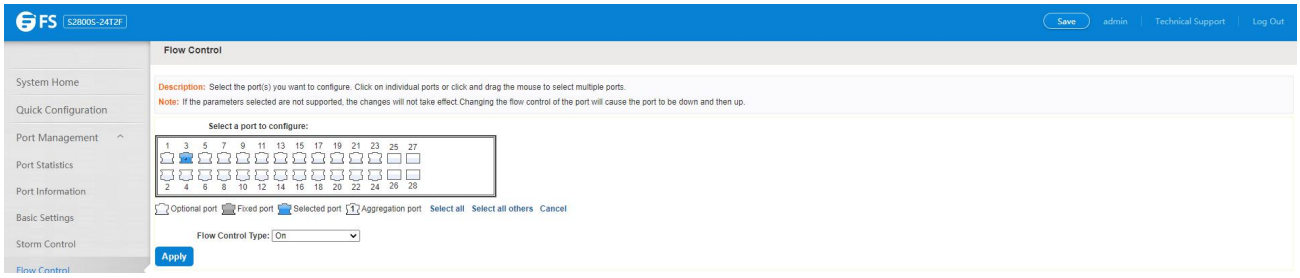


Figure 4-9: Open port flow control function

Open port traffic control, follow these Steps:

Step 1: Select Open port traffic control;

Step 2: Select Open in "Flow control type" on;

Step 3: Click "Save".

View configuration list to display configuration is successful:

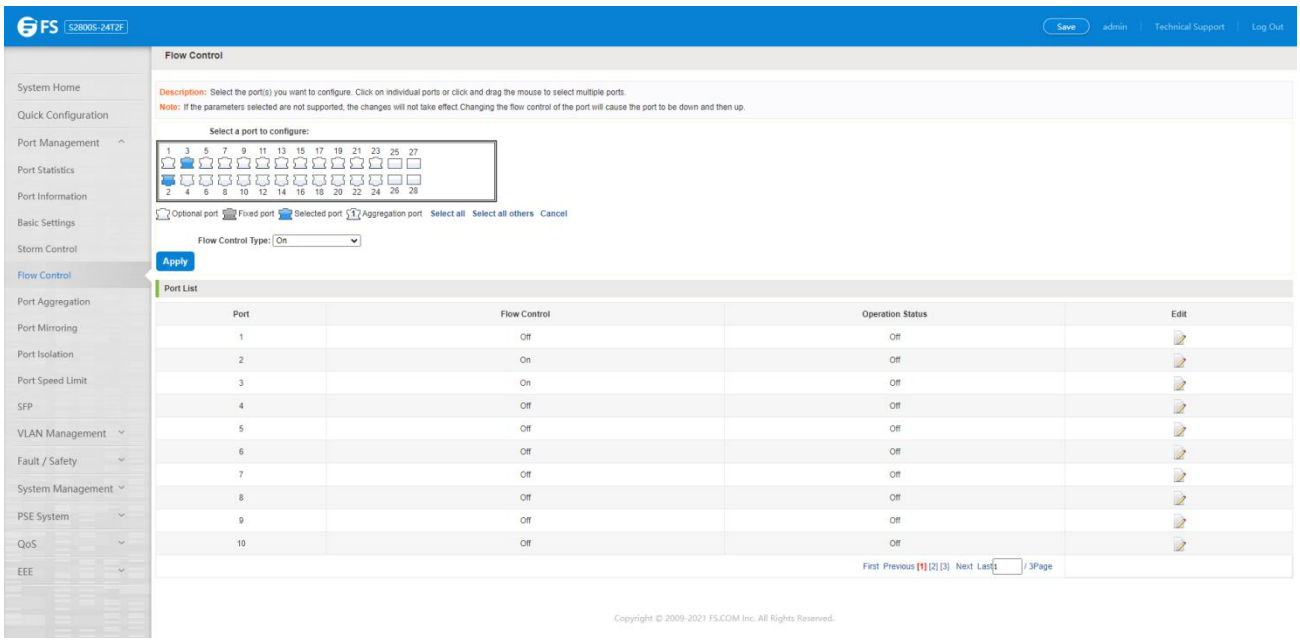


Figure 4-10: Port flow control status

Modify the Port Flow Control Function: Click on port traffic control list corresponding to the rear port of the "  " button in the Port Settings page "Flow control type" select "Off", "Save Settings":

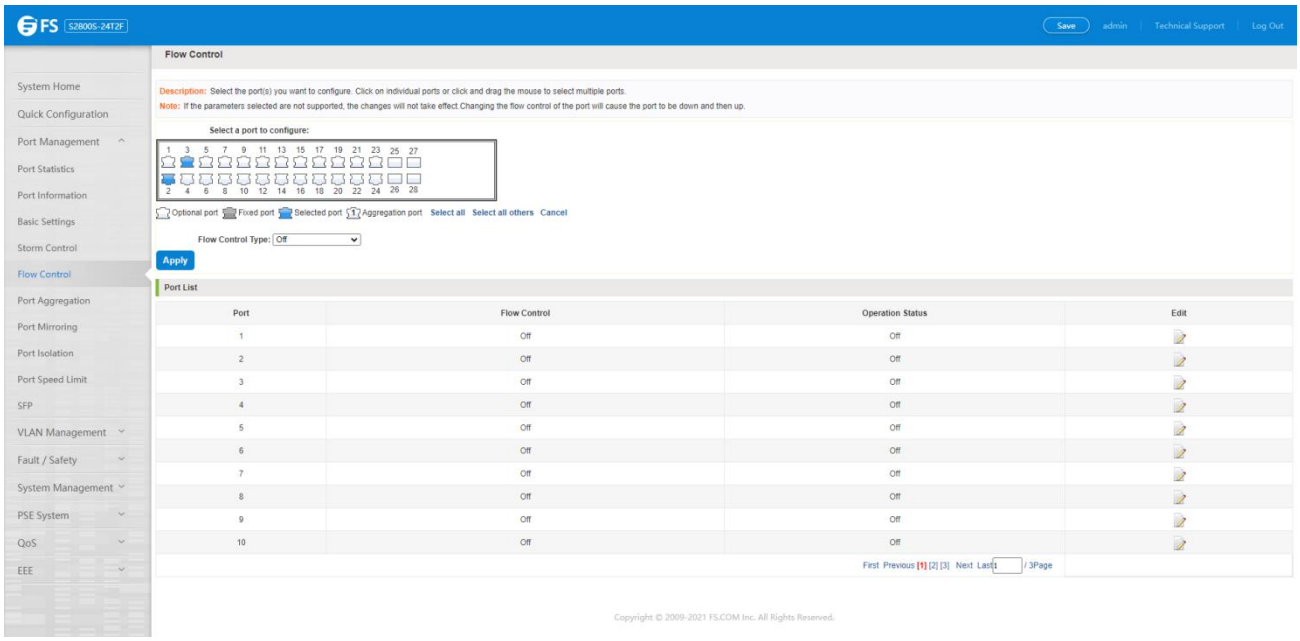


Figure 4-11: Close the port flow control

Close port traffic control, follow these Steps:

Step 1: Select the button to the right of the port or directly selected port;

Step 2: In the "Flow control type" select Off;

Step 3: Click "Save".

4.4 Port Aggregation

4.4.1 Viewing Port Aggregation Configuration

Click "Port Management" "Port Aggregation" to view the current switch configured port aggregation information:

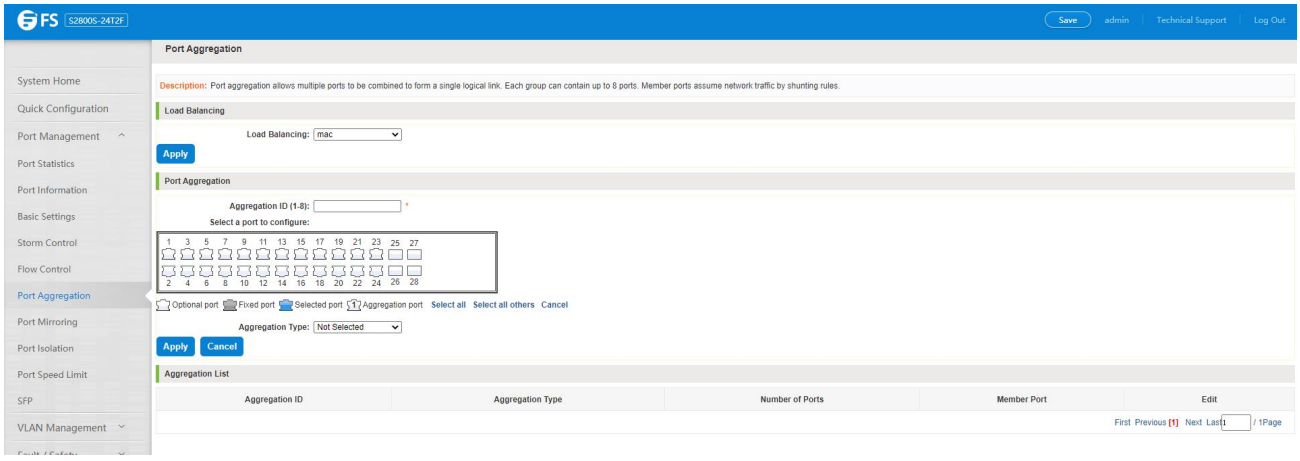


Figure 4-12: Aggregation port configuration information

In the port aggregation list which shows the current switch port configuration information for the polymerization properties:

1. Aggregation Number: Display link aggregation group number value.

2. Load Balancing: Displays the current link aggregation group load balancing judgment condition.

3. Aggregate Types: Displays whether to use a polymerization port LACP protocol.

4. Member Ports Quantity: Displays the number of ports in the link aggregation group contains a total of member port: Displays the current port link aggregation group member prompt.

5. Each aggregate port can bind up to eight member ports, port to transfer data among members of the network traffic through the shunt rules.

6. Port aggregation group must ensure that the port speed, duplex, port state agreement, or cannot ATTACH after configuration.

4.4.2 Add Port Aggregation

Enter aggregation port number, select the desired aggregation port, select aggregation type, click "Save".

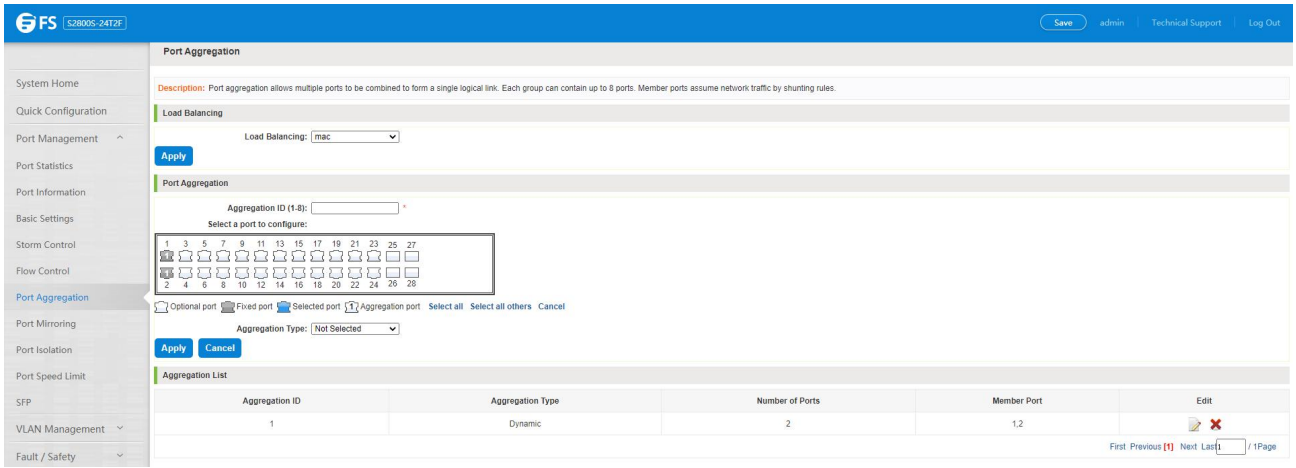


Figure 4-13: Port aggregation configuration area

Increase port aggregation, follow these Steps:

Step 1: Select the option to load the shunt in the load balancing list;

Step 2: Enter the number in the "Aggregation Number" in;

Step 3: Select the aggregated ports in the panel;

Step 4: Select the aggregation type;

Step 5: Click the "Save" button to complete the configuration.

4.4.3 Modifying Port Aggregation

Click on "Aggregation List" in the need to modify the port aggregation right icon in this area to the port aggregation port aggregation group corresponding modification:

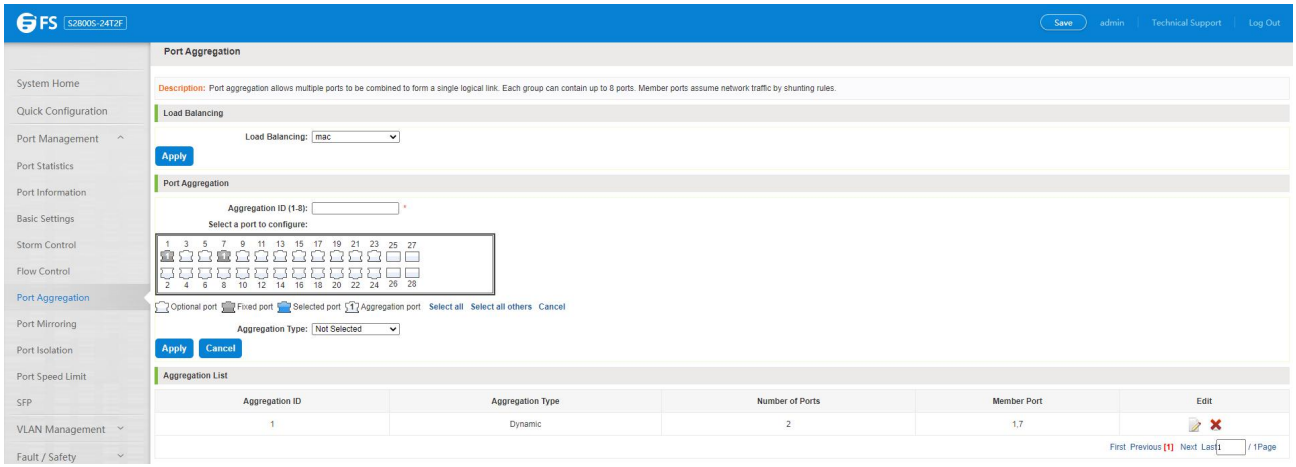


Figure 4-14: To modify the port aggregation

Modify Link Aggregation Procedure:

Step 1: In the "Aggregation List Click to modify the right of the port aggregation;

Step 2: In the port aggregation configuration page to modify the load balancing type and click Next to “Save”;

Step 3: Select the port to be added to the aggregation port;

Step 4: Click the "Save" button to complete the configuration.

4.5 Port Mirroring

4.5.1 Port Mirroring Configuration

Click "Port Management" "configuration of port mirroring "Port Mirroring" view of the switch:

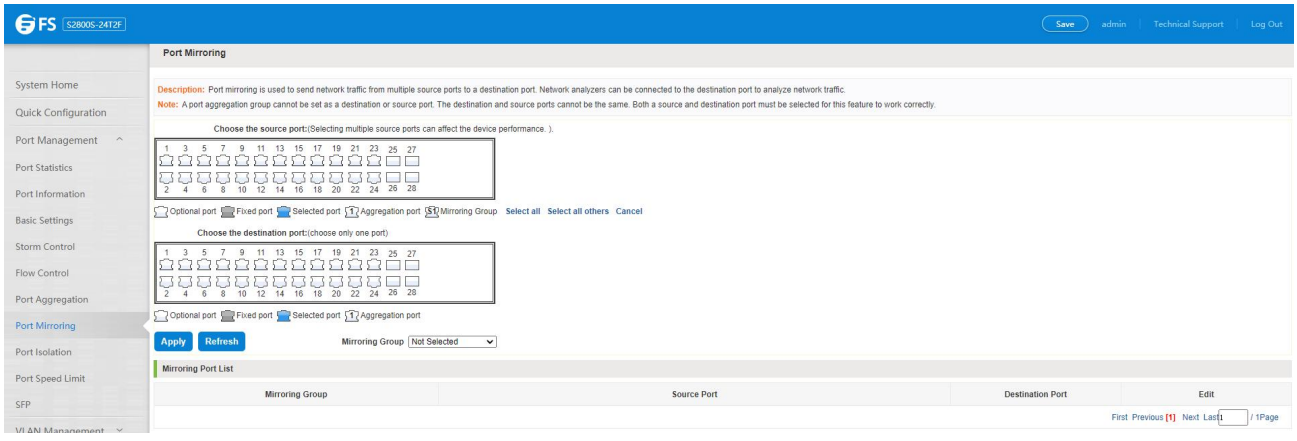


Figure 4-15: Port mirroring configuration information

In the Port Mirroring is a property list which shows the configuration of the current mirror switch:

Mirroring Group: Mirroring group ID, can be configured up to seven mirroring group;

Source Port: The port forwarding on the source data is mirrored to the destination port;

Destination Port: Mirror data sent to the destination port.

1. Port aggregation port cannot be used as the destination port and source port.

2. Destination port and source port cannot be the same.

3. Same group mirroring group can have only one destination port.

4.5.2 Add Port Mirroring Group

On the panel, select "Source Port" and "Destination Port" add port mirroring group.

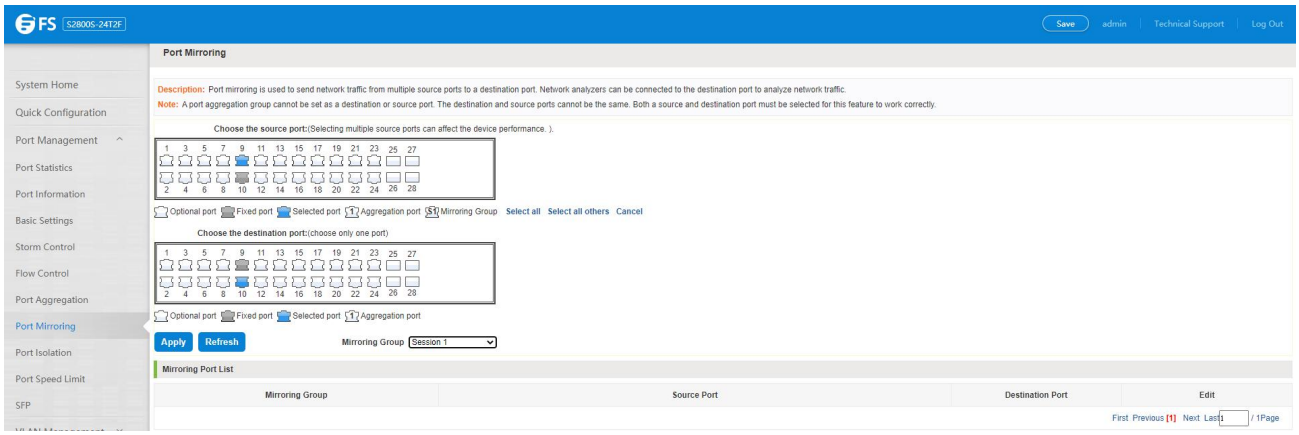


Figure 4-16: Add port mirroring group

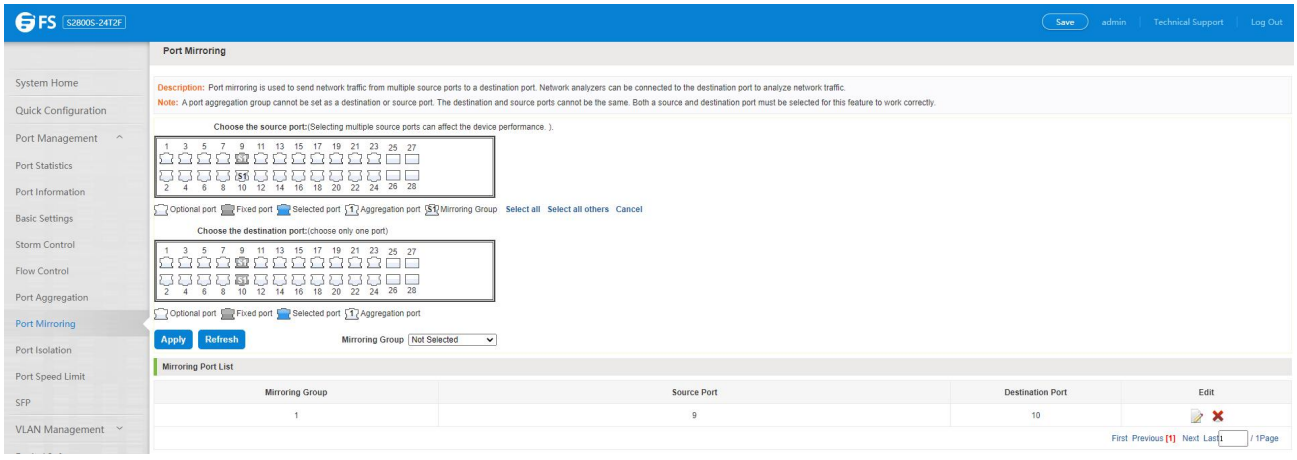


Figure 4-17: Add port mirroring group results

Port mirroring configuration steps are as follows:

Step 1: Select “Source Port”;

Step 2: Select “Destination Port”;

Step 3: Select “Mirroring Group”;

Step 4: Click “Save”.

Configuration instructions:

1. On the switch can be configured 7 mirroring group.

2. Aggregated port mirroring cannot be configured are shown in gray in the panel.

3. Has been selected port mirroring port, displayed in the faceplate is gray.

4. Aggregated port mirroring cannot be configured are shown in gray in the panel.

5. Has been selected port mirroring port, displayed in the faceplate is gray.

4.5.3 To Modify the Port Mirroring Group

Select the group to modify, click on the action bar "  " button. Modify the corresponding mirroring group.

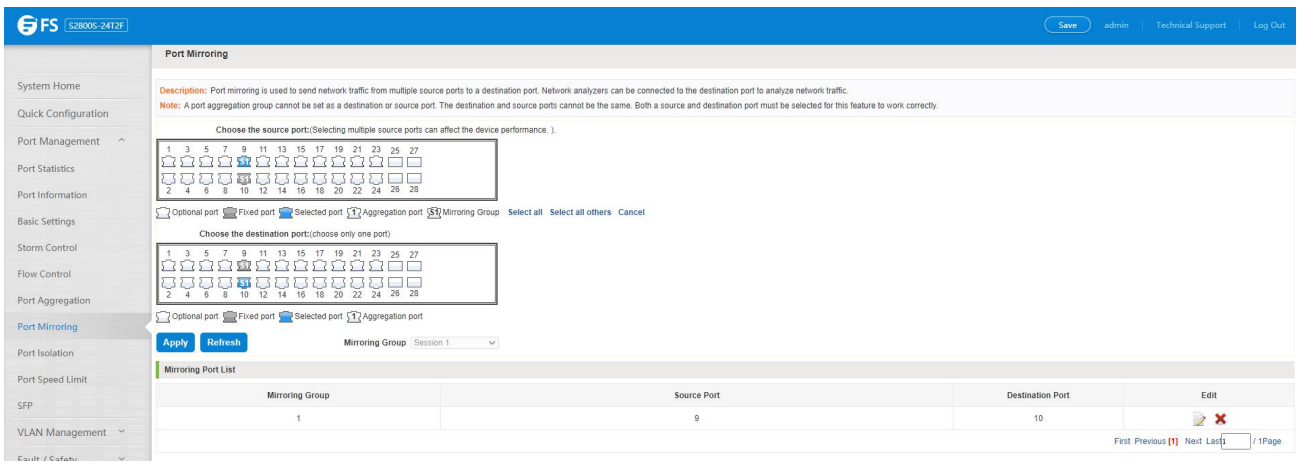


Figure 4-18: To modify the port mirroring group

Modify the port mirroring configuration Steps are as follows:

Step 1: In the image you want to modify the operation of the group column, click on “  ”;

Step 2: Add or remove the corresponding port in the panel;

Step 3: Click "Save".

4.5.4 Delete a Port Mirroring Group

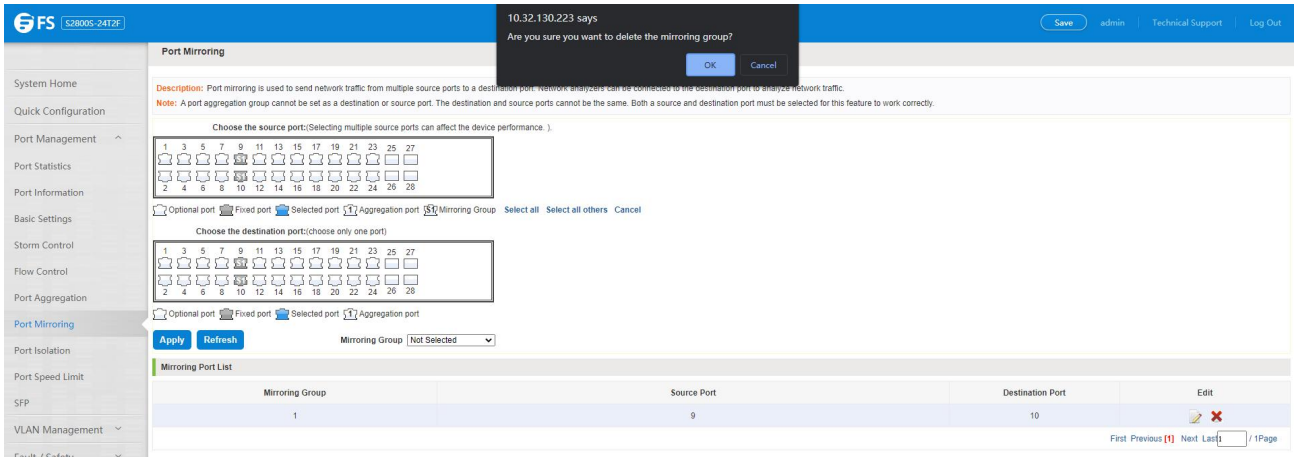


Figure 4-19: Delete port mirroring group

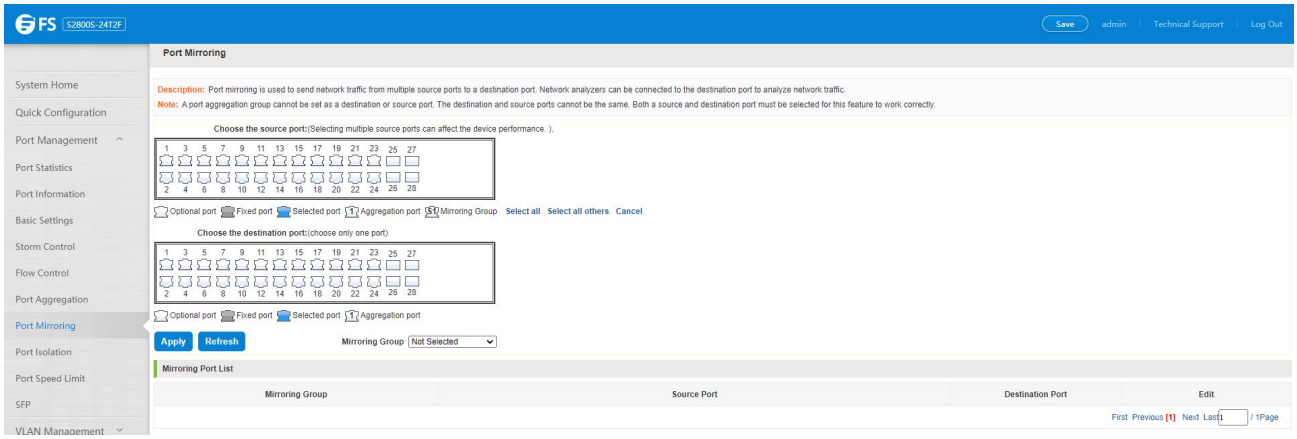


Figure 4-20: Deleted successfully port mirroring

Remove port mirroring configuration Steps are as follows:

Step 1: In the image you want to modify the operation of the group column, click “ ” ;

Step 2: In the panel, click Cancel the source port, destination port and then click Cancel;

Step 3: In the panel, click Cancel the source port, destination port and then click Cancel;

Step 4: Click "Save".

4.6 Port Isolation

4.6.1 Port Isolation Configuration

Click "Port Management" "Configuration of Port Mirroring "Port Isolation" view of the switch:

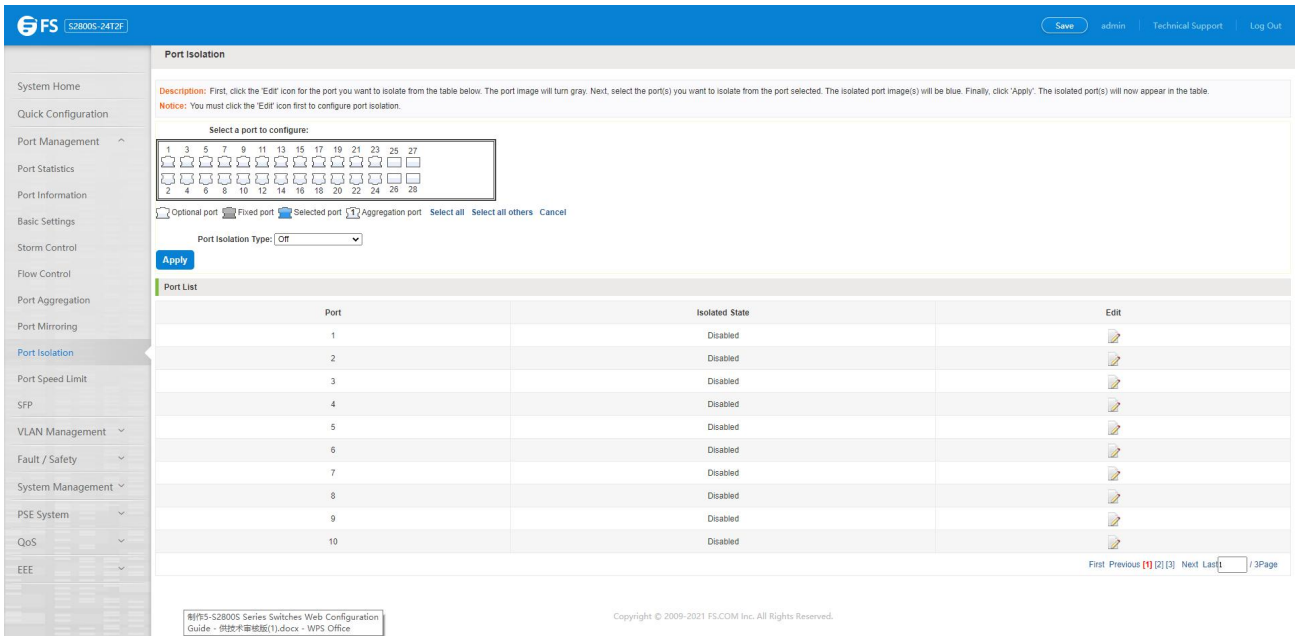


Figure 4-21: Port Isolation configuration information

4.6.2 Configuring Port Isolation

Open Port Isolation Function: select the port on which you want to open port isolation, click the "port isolation type", select "On", "Save":

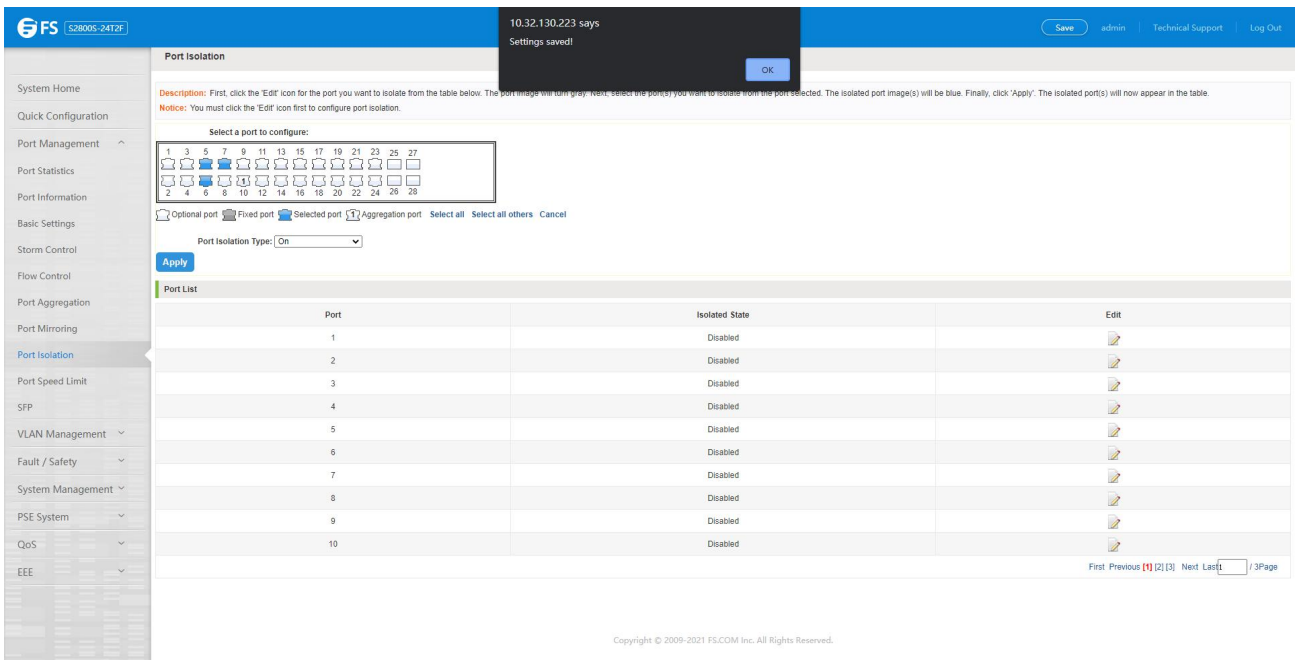


Figure 4-22: Enable port isolation function

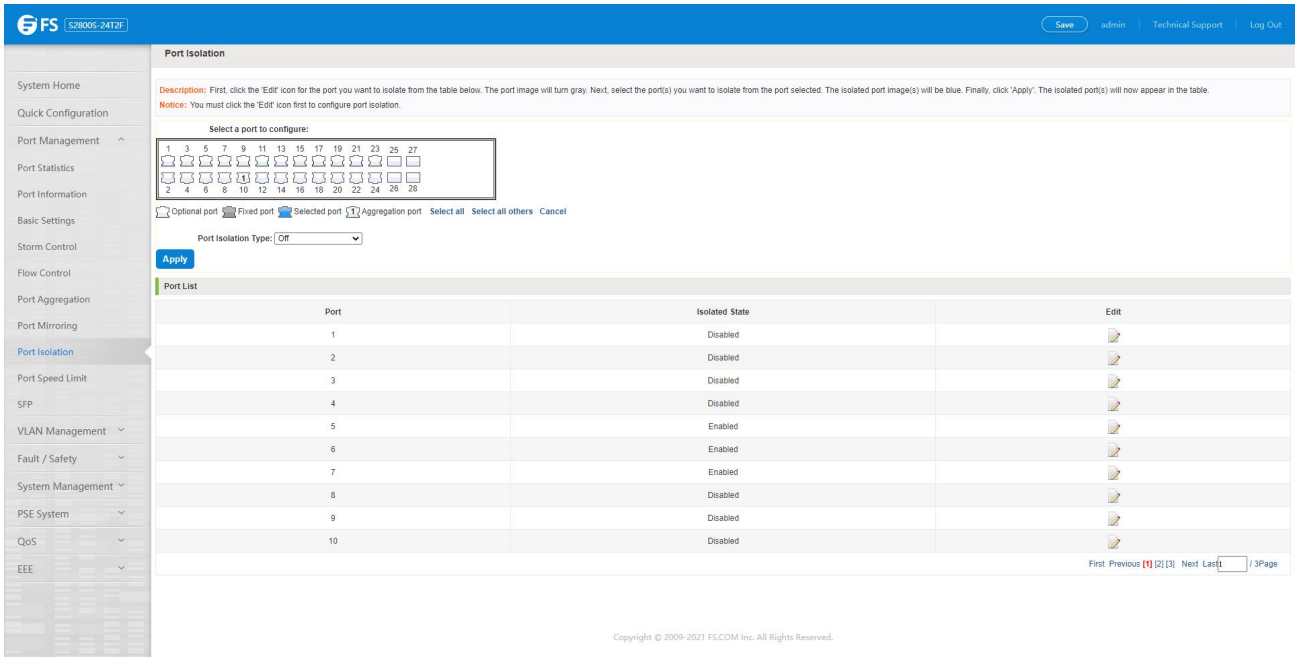


Figure 4-23: Enable port isolation results

4.6.3 Modify the Port Isolation

Select the port to modify, click on the action bar "  " button. Modify the corresponding port isolation.

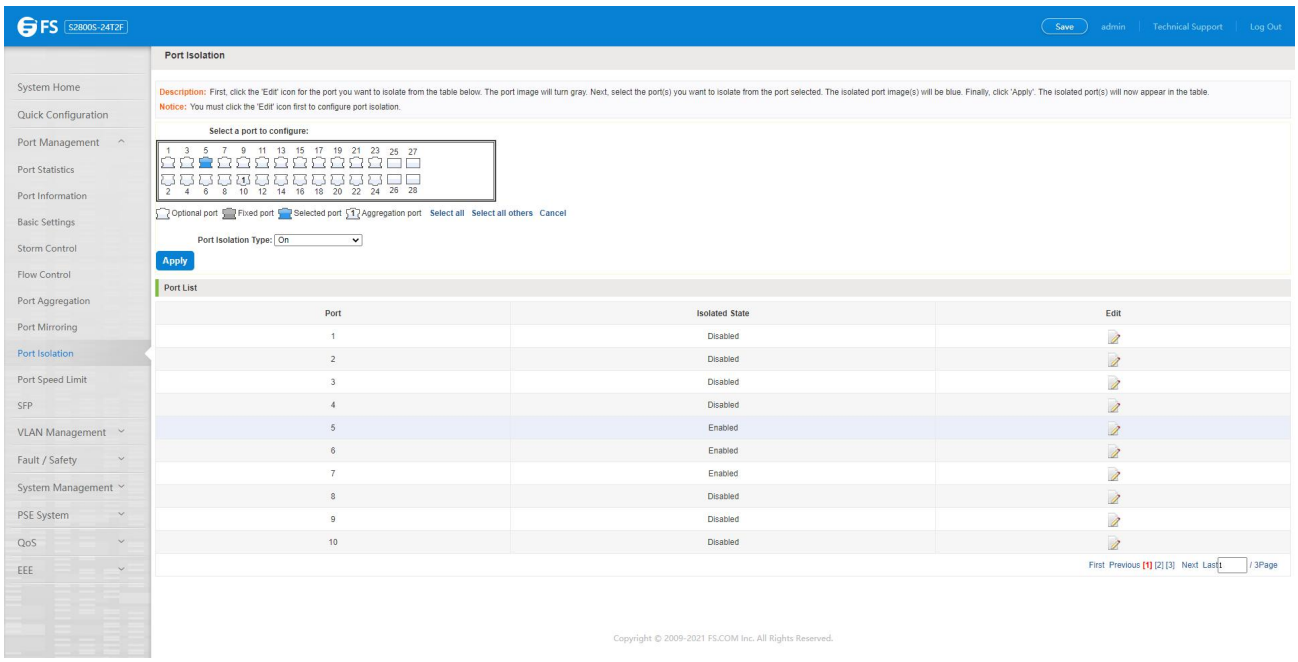


Figure 4-24: To modify the port isolation

4.7 Port Speed Limit

4.7.1 View Port Rate Limit

Click "Port Management" "Port Speed Limit" switch to view the current port speed configured information:

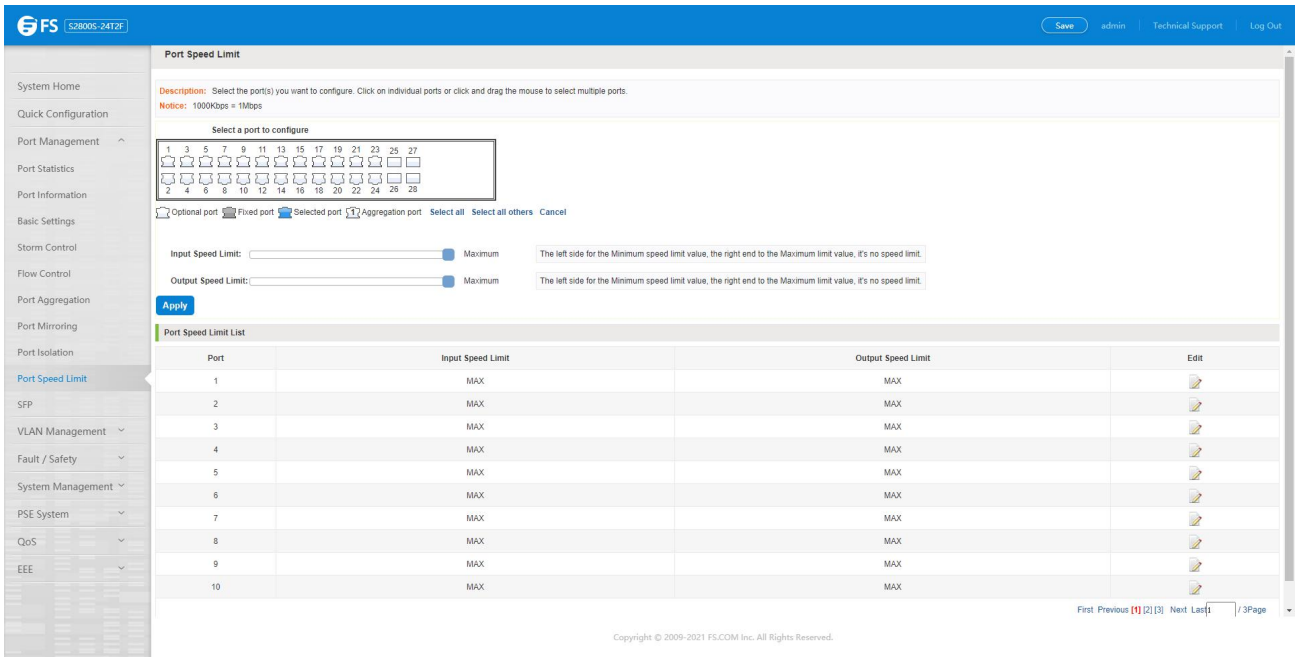


Figure 4-25: View rate configuration information

In the port speed list which shows the current speed limit switch attribute configuration information:

Port: The number of the port;

Input Limit: Uplink port speed;

Output Speed: Port downstream rate;

4.7.2 Configure Port Access Rate

Select the panel to set the speed limit of the port, set the rate limit value by dragging the speed bar.

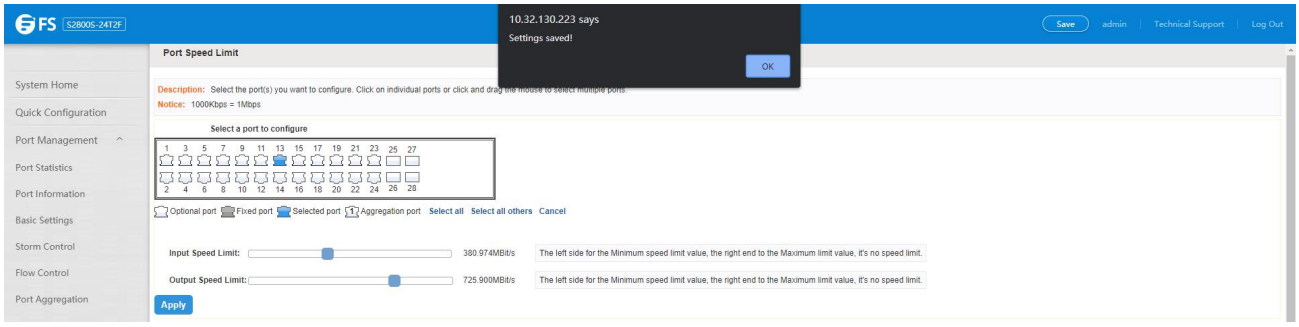


Figure 4-26: Configure port rate limiting entrance

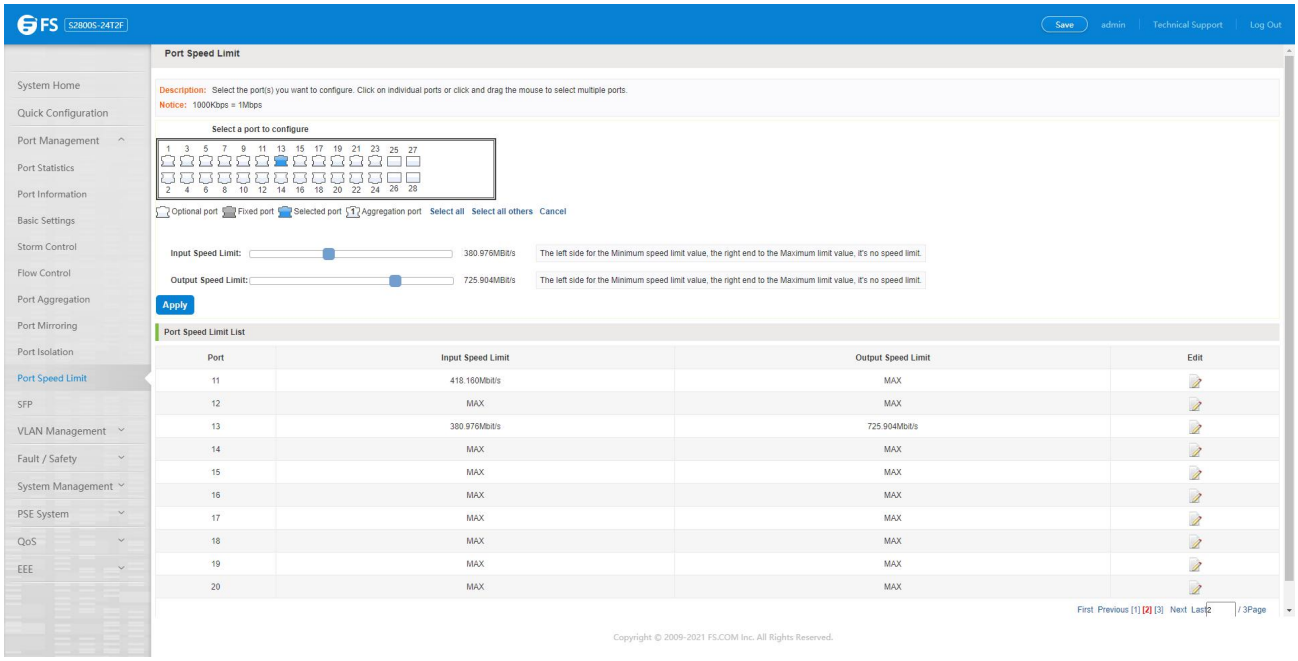


Figure 4-27: Port entrance speed limit results

Entrance port rate limiting configuration Steps are as follows:

Step 1: Click on the right side of the port "  " Icon or select multiple icons;

Step 2: Set rate limiting strip port value;

Step 3: Click the lower right corner "Save" button to complete the configuration.

4.7.3 Remove the Port Speed Limit

Click the need to remove the limit on the right port icon " in the configuration area of the port rate value pull bar to the far right, "Save" to complete the operation.

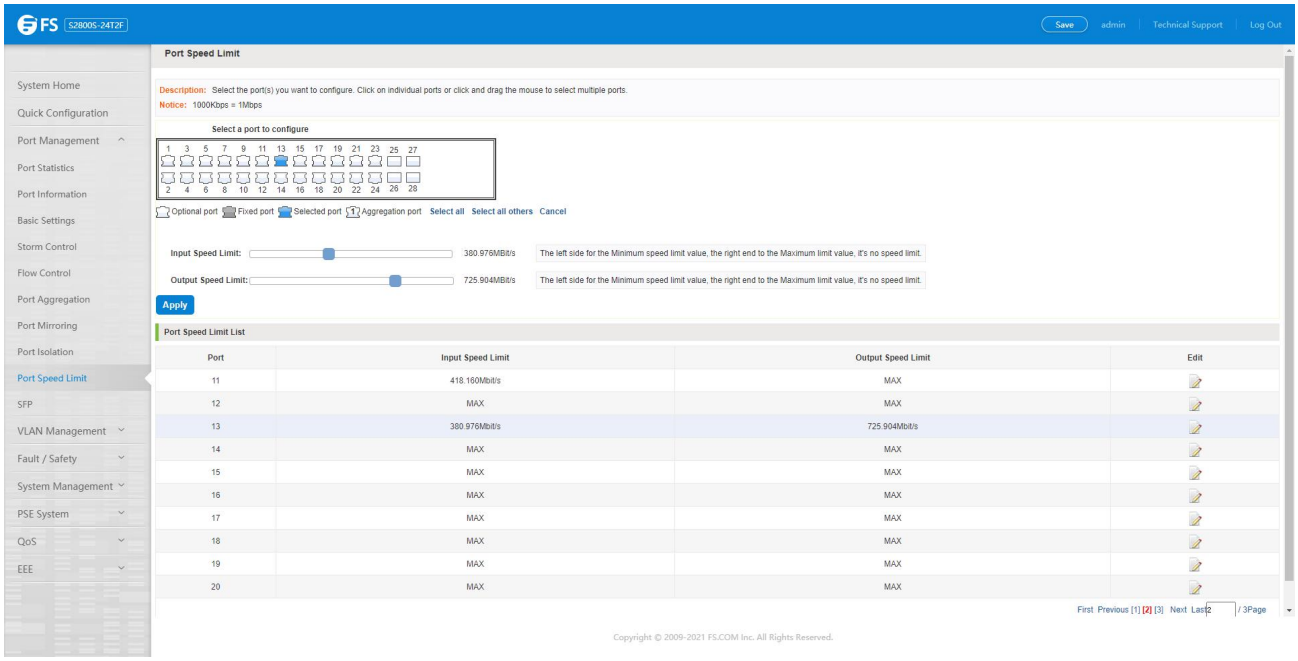


Figure 4-28: Remove the port speed limit

Remove uplink port rate limiting Steps are as follows:

Step 1: Click on the right side of the port  icon;

Step 2: In the area of the port rate configuration value rate strip pulled to the far right;

Step 3: Click the "Save" button to complete the configuration.

5. VLAN management

5.1 VLAN management

5.1.1 Check VLAN Configuration Information

Click on the navigation bar "VLAN Management" "VLAN management" "VLAN Settings" to view the switch configured:

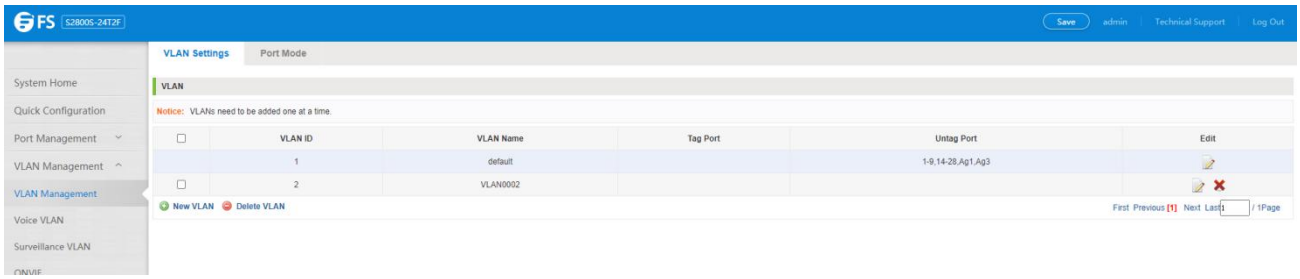


Figure 5-1: VLAN configuration information

In the VLAN list which shows the properties of the configuration information of the current switch VLAN ID:

1. VLAN ID: VLAN ID value is displayed.

2. VLAN Name: The name of the VLAN, the default VLAN ID to name.

3. VLAN IP Address: Displays the switch's management IP.

4. Port: Displays the port VLAN that exist.

5. By default, all ports belong to VLAN 1.

5.1.2 Adding a VLAN

Click "NEW VLAN" button, you can increase the VLAN configurations:

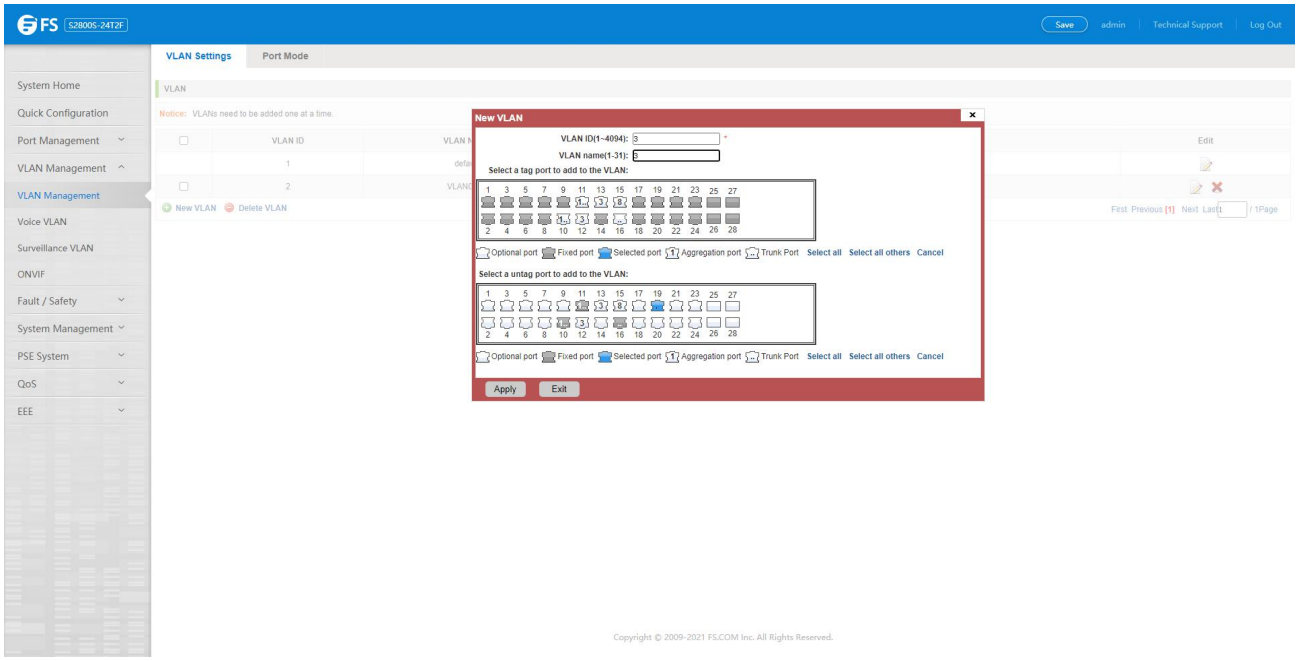


Figure 5-2: Adding a VLAN

Adding a VLAN, follow these Steps:

Step 1: Click "NEW VLAN" connection;

Step 2: Value added VLAN VLAN ID of the page to fill in;

Step 3: Select the ports;

Step 4: Click the lower right corner "Save" button to complete the configuration.

5.1.3 Remove VLAN

5.1.3.1 Single VLAN Delete

To delete the selected VLAN, click the "X" button to delete the selected VLAN, if the VLAN do not have ports, you can directly delete the VLAN; if the VLAN have some ports, you must remove the ports in the VLAN firstly and then you can delete the selected VLAN.

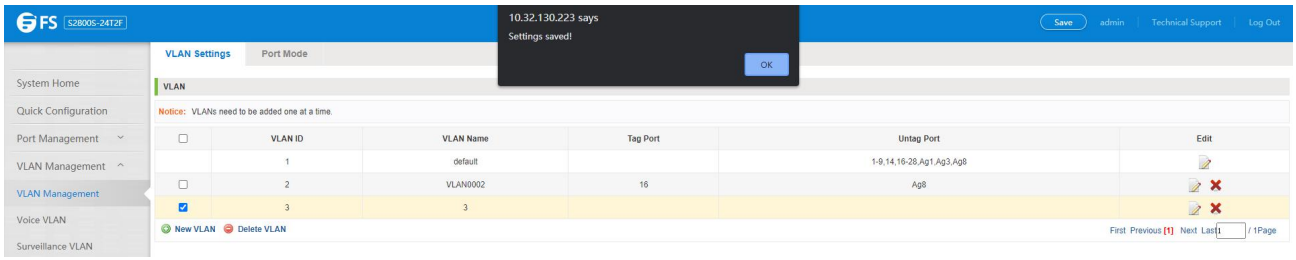


Figure 5-3: Delete a single VLAN

5.1.3.2 Delete Multiple VLAN

First select the VLAN you want to be deleted before the "checkbox, then click" "Delete VLAN" button to delete the selected VLAN, if the VLANs have some ports the VLAN cannot be removed because of there are member ports. The others will be removed.

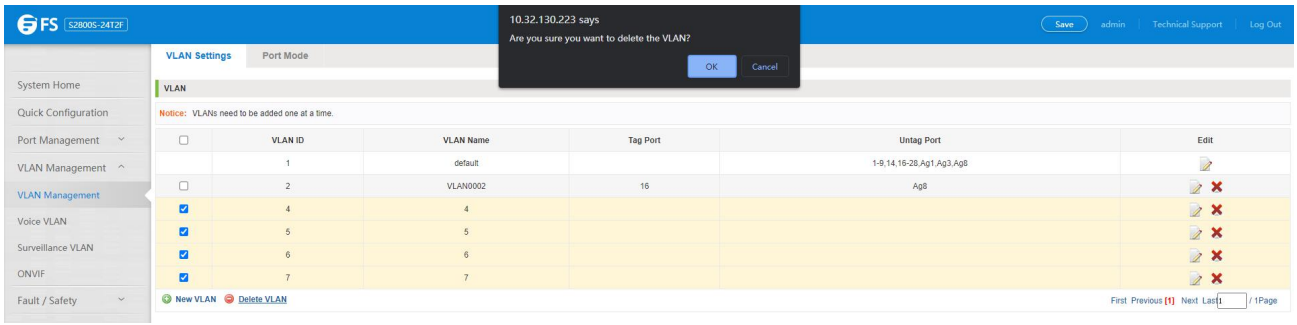


Figure 5-4: Delete multiple VLAN

Delete multiple VLAN, follow these Steps:

Step 1: I want to delete VLAN check box;

setp2: Click on the bottom left "Delete VLAN" connection;

Step 3: Confirm delete.

5.1.4 Editing VLAN

5.1.4.1 VLAN Port to a VLAN

Click on the icon can be added to the selected port in the VLAN:

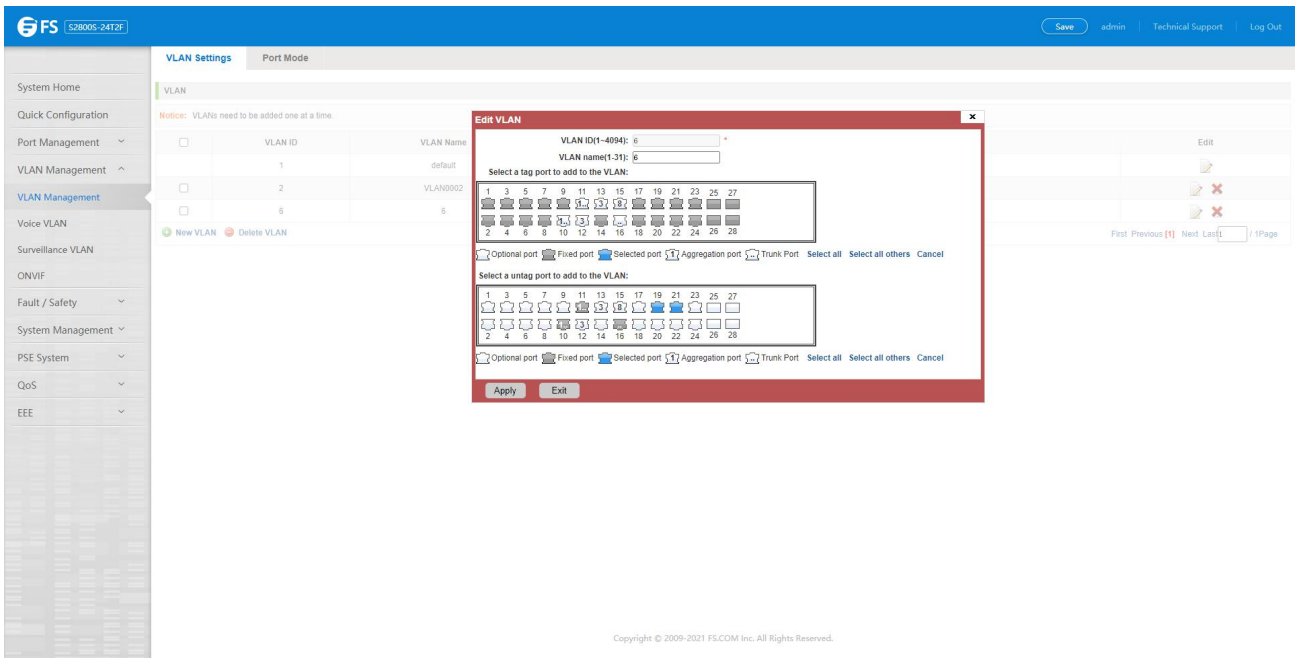


Figure 5-5: Add the port to the VLAN

Add the port to the VLAN, follow these Steps:

Step 1: Click " " icon;

Step 2: Selected to join the ports in the port pane;

Step 3: Click the lower right corner "Save" button to complete the configuration.

5.1.4.2 to Remove the Port From a VLAN

Click on the icon, you can remove the port from this VLAN:

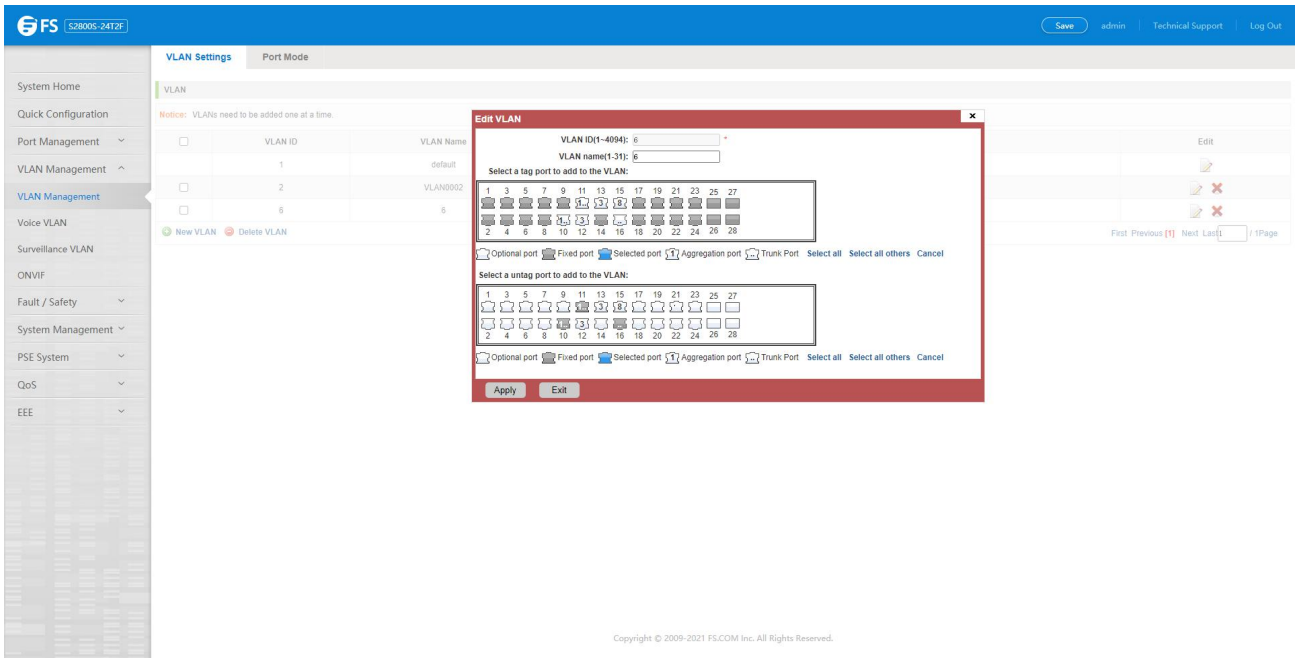


Figure 5-6: To remove the port from the VLAN

Procedure to remove the port from VLAN as follows:

Step 1: Click on the icon " ";

Step 2: Remove the port to be removed from the port panel;

Step 3: Click on the lower right corner of the "Save" button to complete the configuration.

5.1.5 View Port Mode

Click on the "VLAN Management" "Port Mode" view switches has been configured port mode information:

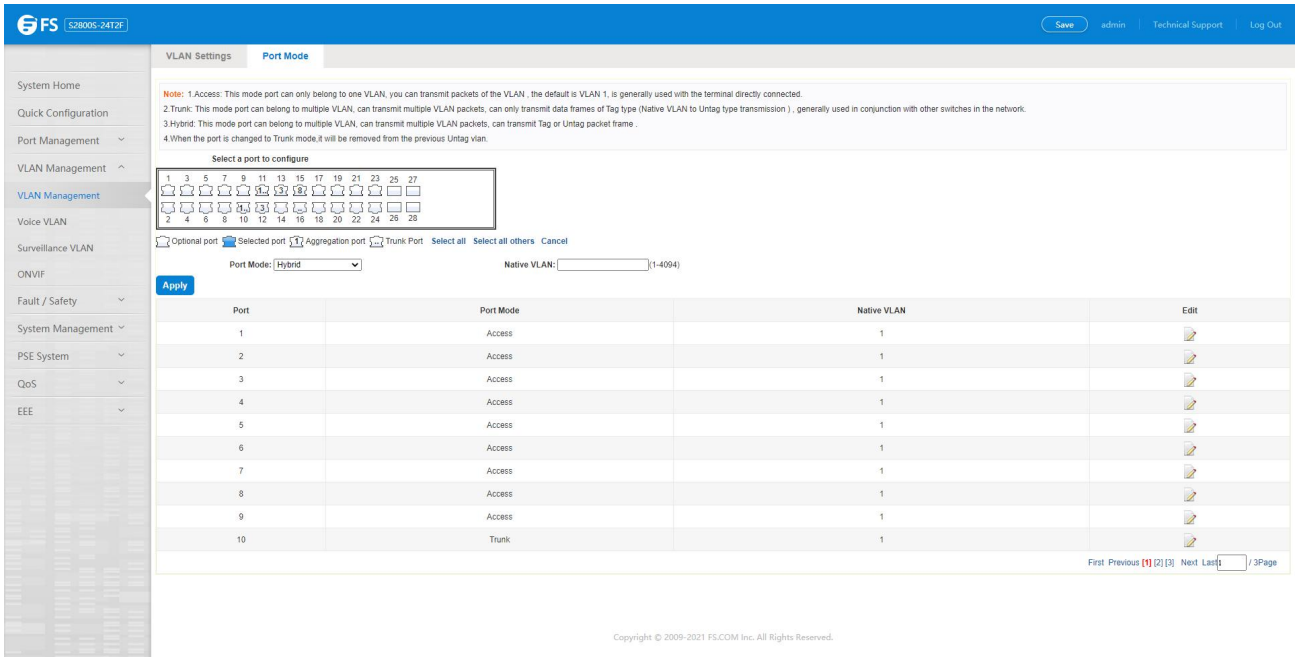


Figure 5-7: View port mode configuration information

Displayed in the port mode list is the property value of the port configuration of the current switch:

1. The Port Name: Display port number used.

2. The Native VLAN: Display native VLAN.

3. The Allowed VLAN: The VLAN allows the display message can be through VLAN.

4. The default port is 1 VLAN native VLAN.

5. The default port mode is access.

5.1.6 Change the Port Mode is Trunk

Select the port you want to change the mode and click the "port mode" list, you can set the port mode is trunk:

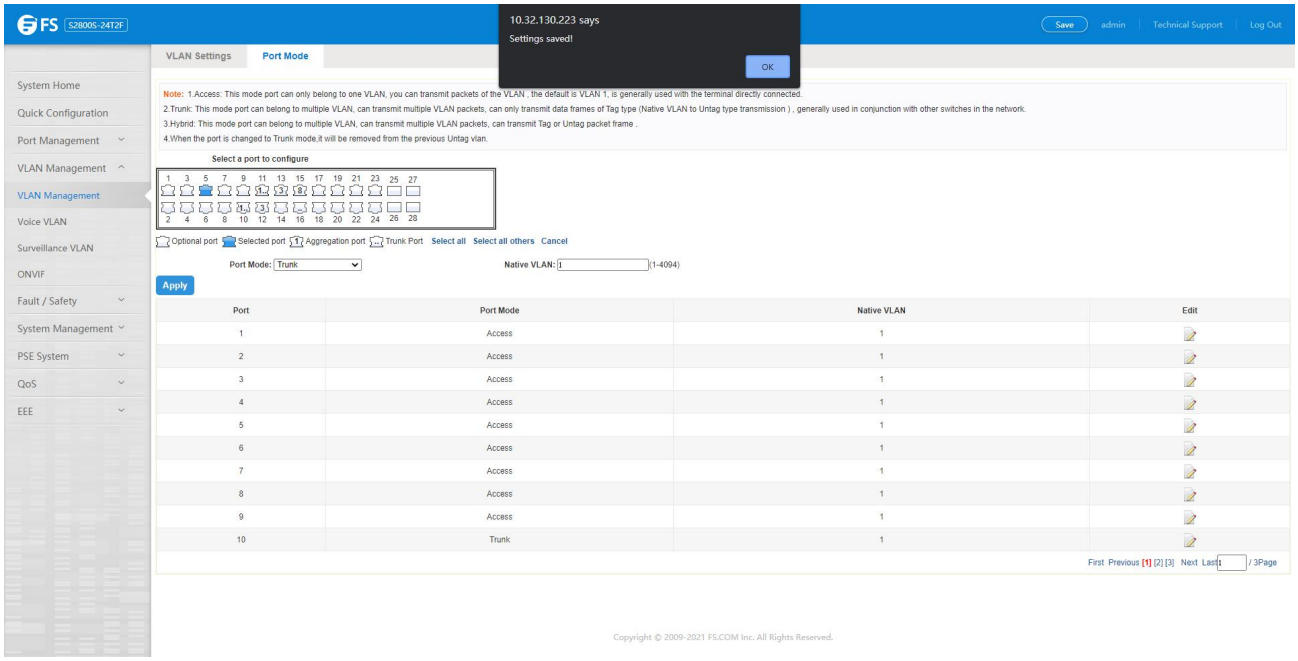


Figure 5-8: Change the port mode is trunk

The Steps to set port mode is trunk are as follows:

Step 1: Chose one or more ports;

Step 2: Click the port mode list chose the mode is: trunk;

Step 3: Set Native VLAN, the VLAN must be is exist;

Step 4: Set by allowing the VLAN number, the default allowed VLAN is empty, if you want to allow the native VLAN, you must be configure allowed the native VLAN;

Step 5: Click on the lower right corner of the "Save" button to complete the configuration.

5.1.7 Change the Port Mode is Hybrid

Select the port you want to change the mode and click the "port mode " list, you can set the port mode is hybrid:

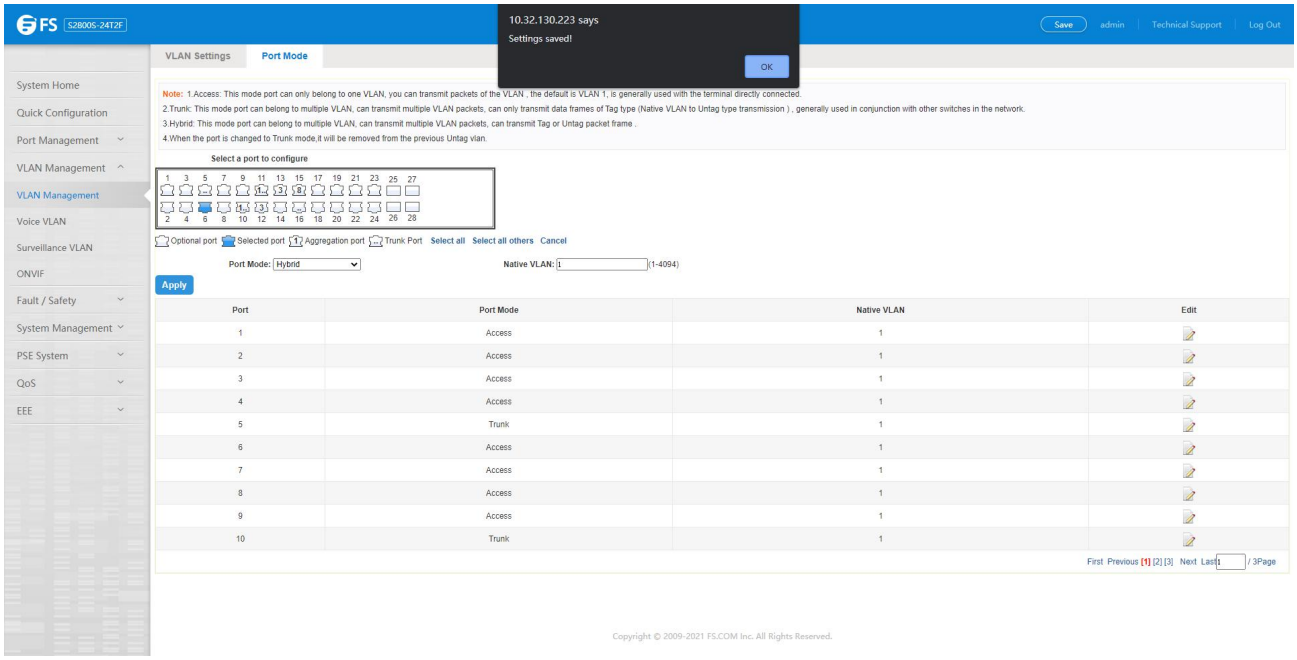


Figure 5-9: Change the port mode is hybrid

The steps to set port mode is hybrid are as follows:

Step 1: Chose one or more ports;

Step 2: Click the port mode list chose the mode is: hybrid;

Step 3: Set Native VLAN, the VLAN must be is exist;

Step 4: Set by allowing the VLAN number, the default allowed VLAN 1, if you want to allow the native VLAN, you must be configure allowed the native VLAN;

Step 5: Click on the lower right corner of the "Save" button to complete the configuration.

5.2 Voice VLAN

5.2.1 View Voice VLAN Information

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to view the switch configured:

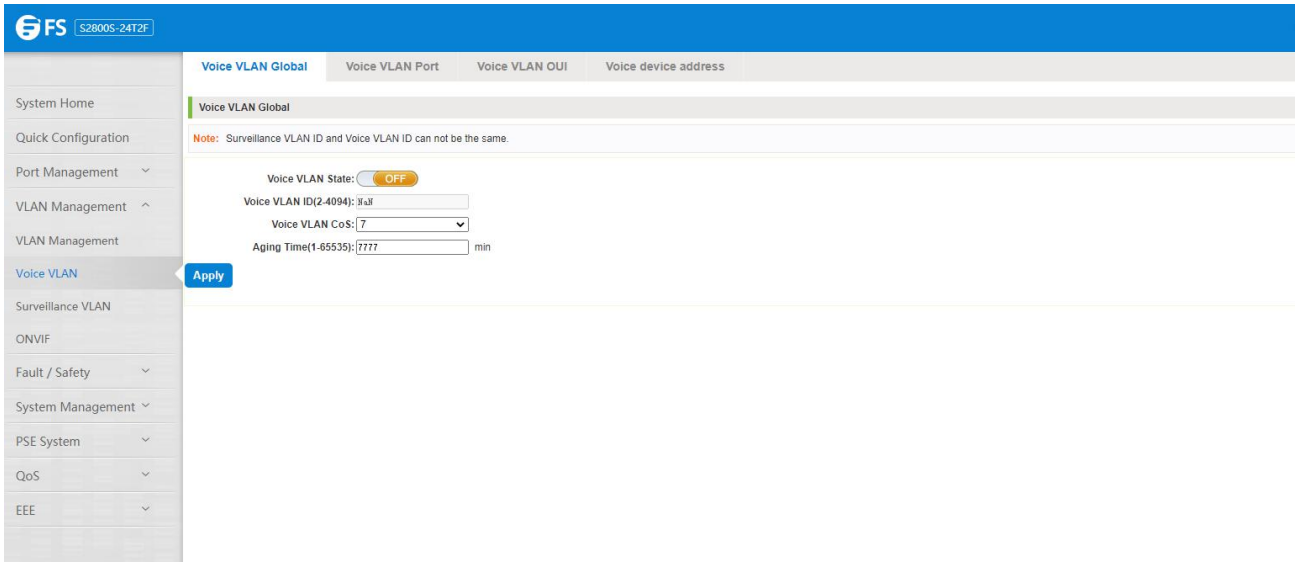


Figure 5-10: View voice VLAN information

5.2.2 Configure Voice VLAN global

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to configure the voice VLAN;

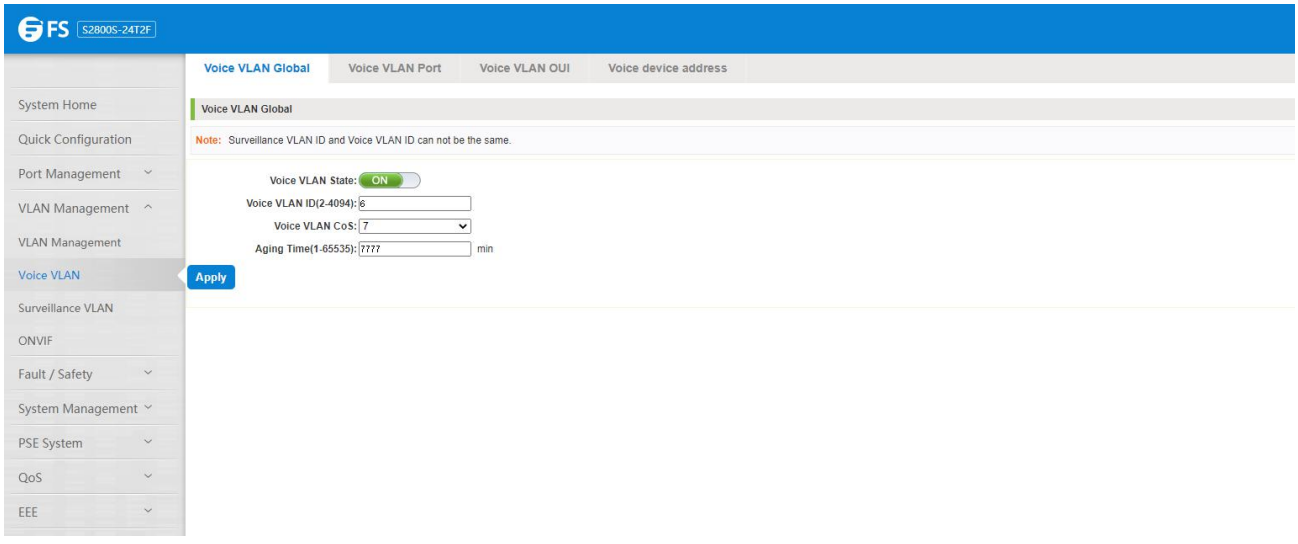


Figure 5-11: view voice VLAN information

To configure the voice VLAN global Steps as follows:

Step 1: In the voice VLAN state TEXT BOX, click ON the "OFF" to "ON";

Step 2: In the voice VLAN ID text box, enter the ID, such as 900;

Step 3: In the voice VLAN COS text box, choose 6;

Step 4: In the aging time text box, enter aging time, such as 1000;

Step 5: Click on save.

5.2.3 Configure Voice VLAN Port

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN port" to configure the voice VLAN port;

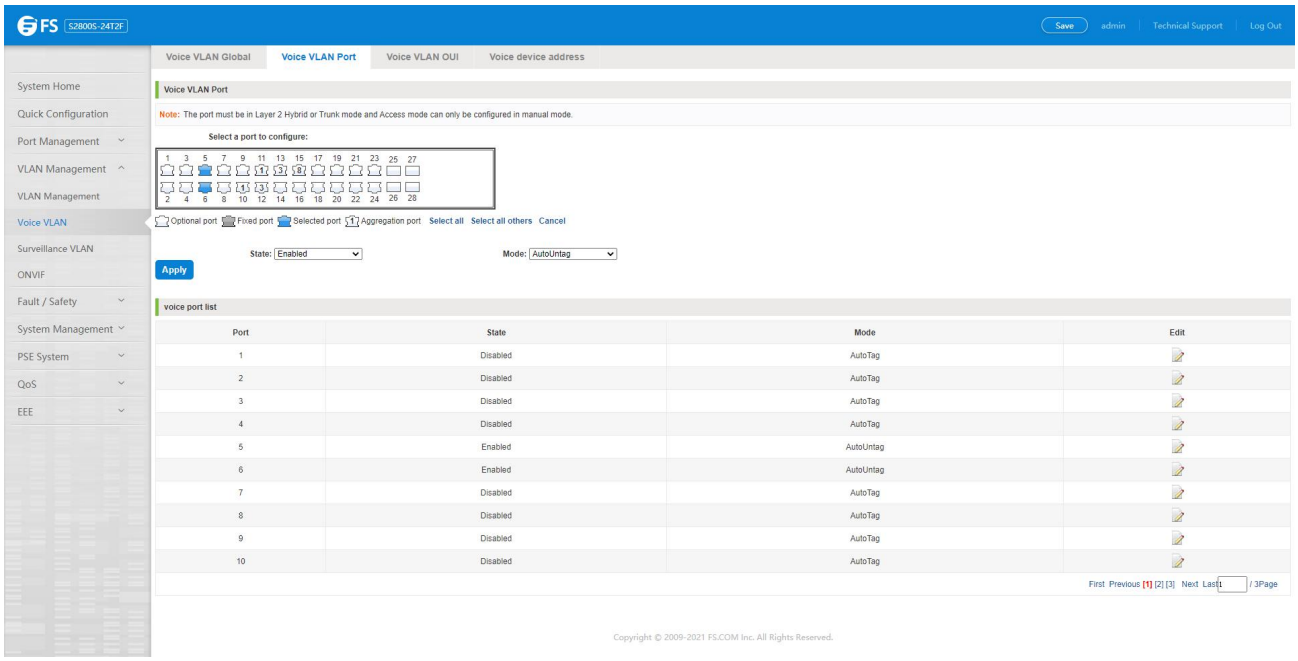


Figure 5-12: Configure voice VLAN port

To configure the voice VLAN port steps as follows:

Step 1: Select ports to configure;

Step 2: In the state text box, choose enable;

Step 3: In the mode text box, choose manual;

Step 4: Click on save.

5.2.4 Configure Voice VLAN OUI

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN OUI" to configure the voice VLAN OUI.

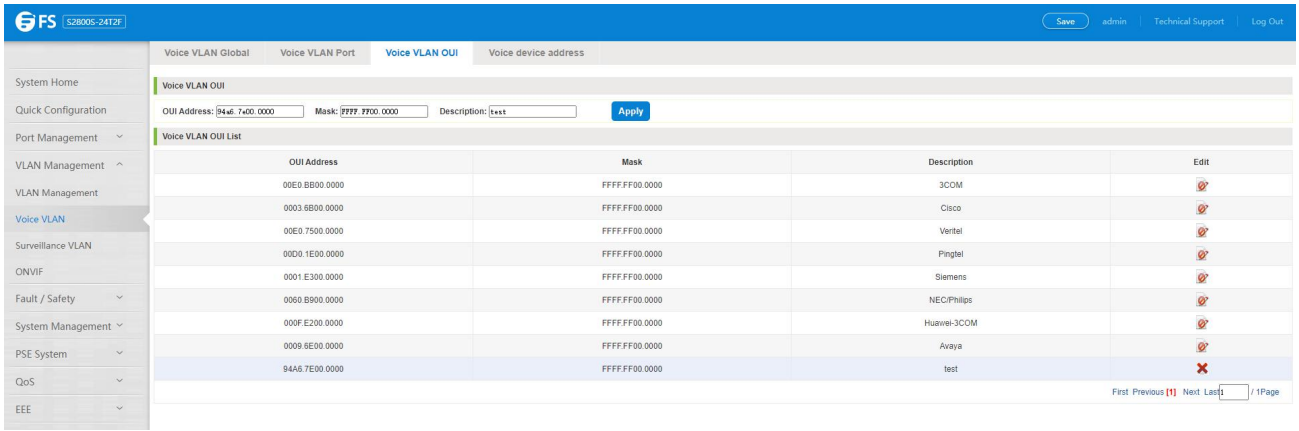


Figure 5-13: Configure Voice VLAN OUI

To configure the voice VLAN OUI Steps as follows:

Step 1: In the OUI address text box, enter OUI address, such as 00-b0-1E-00-00-00;

Step 2: In the mask text box, enter the mask, such as FF-FF-FF-00-00-00;

Step 3: In the description text box, enter the description, such as test OUI;

Step 4: Click save.

5.2.5 Voice Device Address

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice device address" to view the voice device:

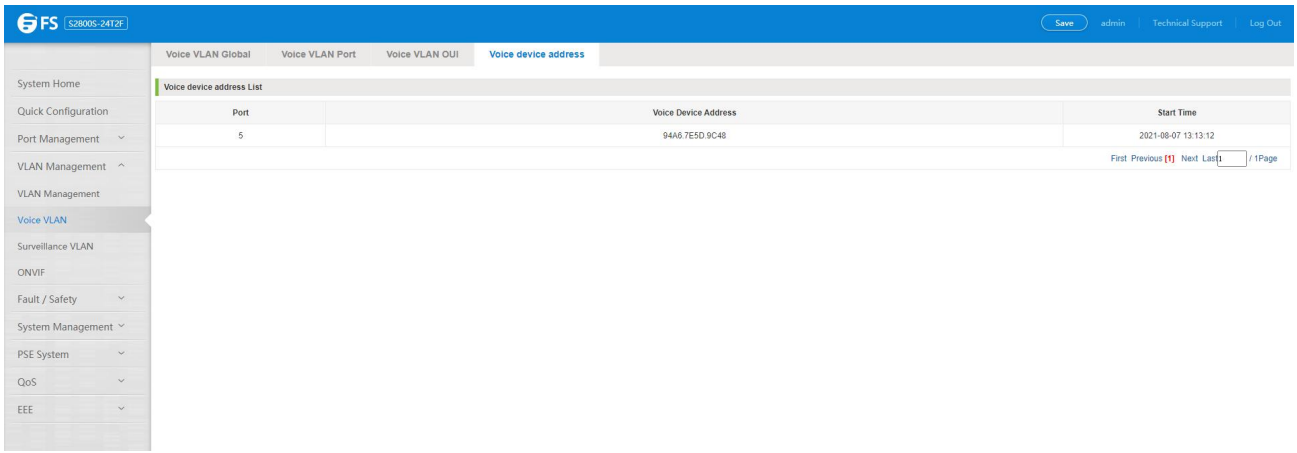


Figure 5-14: Voice device address

5.3 Surveillance VLAN

5.3.1 View Surveillance VLAN Information

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" to view the switch configured:

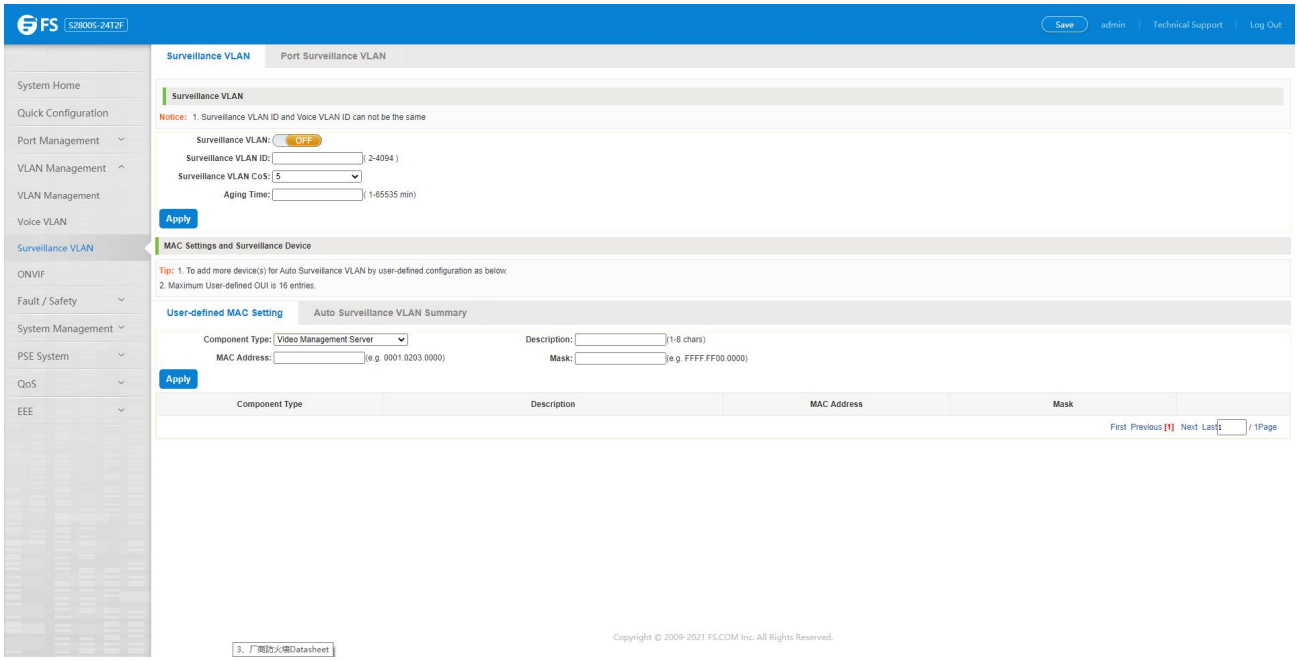


Figure 5-15: Surveillance VLAN information

5.3.2 Configure Surveillance VLAN

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" to configure the switch surveillance VLAN.

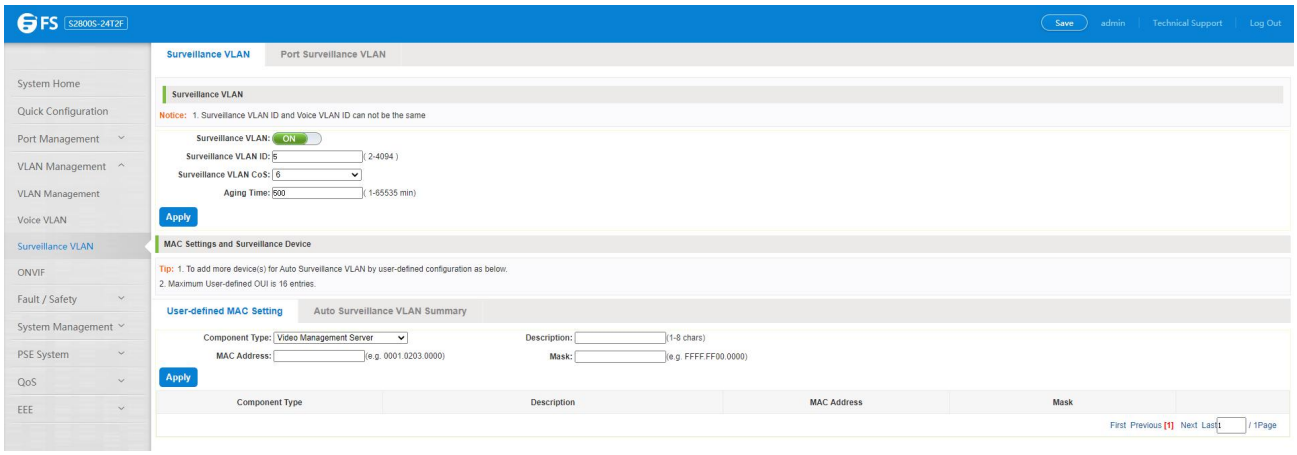


Figure 5-16: Configure Surveillance VLAN

To configure the surveillance VLAN Steps as follows:

Step 1: In the surveillance VLAN TEXT BOX, click ON the "OFF" to "ON".

Step 2: In the surveillance VLAN ID text box, enter the ID, such as 500;

Step 3: In the surveillance VLAN COS text box, choose 3;

Step 4: In the aging time text box, enter aging time, such as 500;

Step 5: Click on save.

5.3.3 MAC Settings and Surveillance Device

Click on the navigation bar "VLAN Management" "surveillance VLAN" "surveillance VLAN" "MAC Settings and Surveillance Device" to configure the user-defined mac settings.

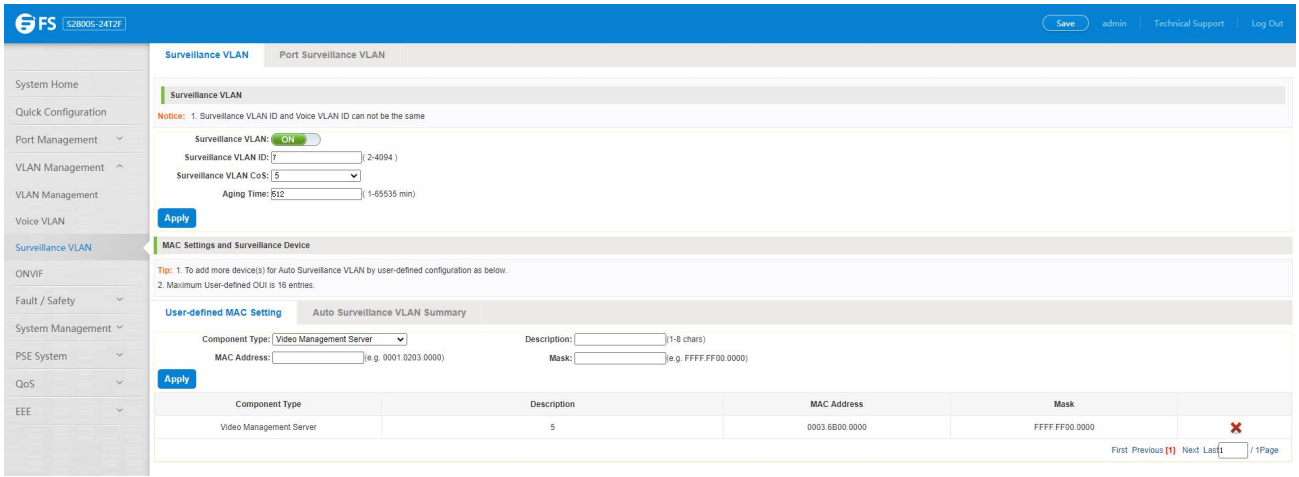


Figure 5-17: Configure the user-defined mac settings

To configure the surveillance VLAN Steps as follows:

Step 1: In the component type EXT BOX, choose video management server;

Step 2: In the description text box, enter test OUI;

Step 3: In the mac address text box, enter mac address, such as 00A1.0203.0000;

Step 4: In the mask text box, enter the mask, such as FFFF.F000.000;

Step 5: Click on save.

5.3.4 MAC Settings and Surveillance Device

Click on the navigation bar "VLAN Management" "surveillance VLAN" "surveillance VLAN" "MAC Settings and Surveillance Device" to view the information:

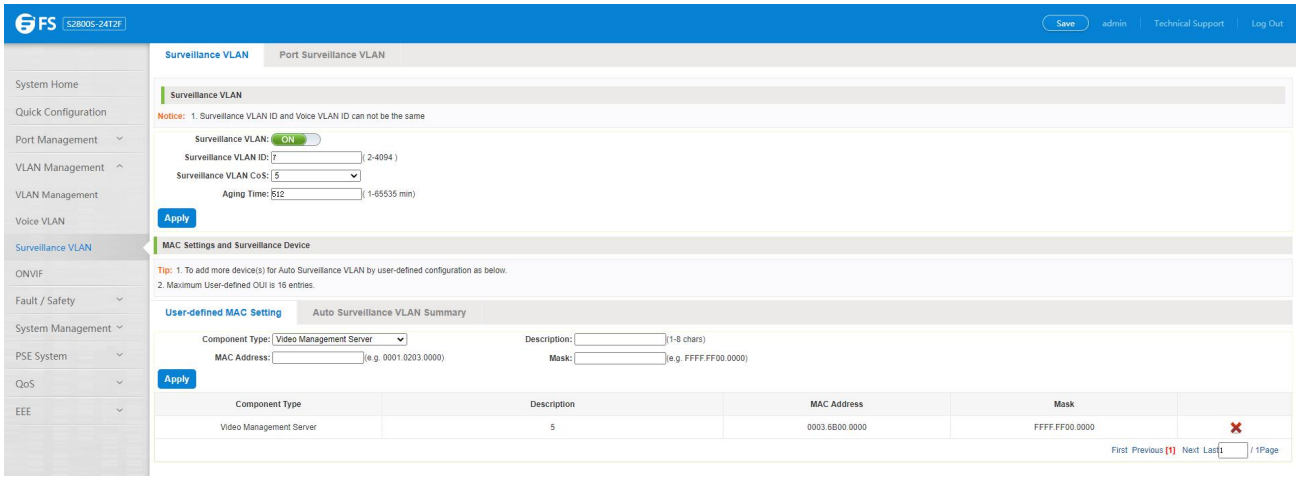


Figure 5-18: Configure the user-defined mac settings

5.4 ONVIF

5.4.1 View ONVIF

Click on the navigation bar "VLAN Management" "ONVIF" "ONVIF Global" to view the switch configured:

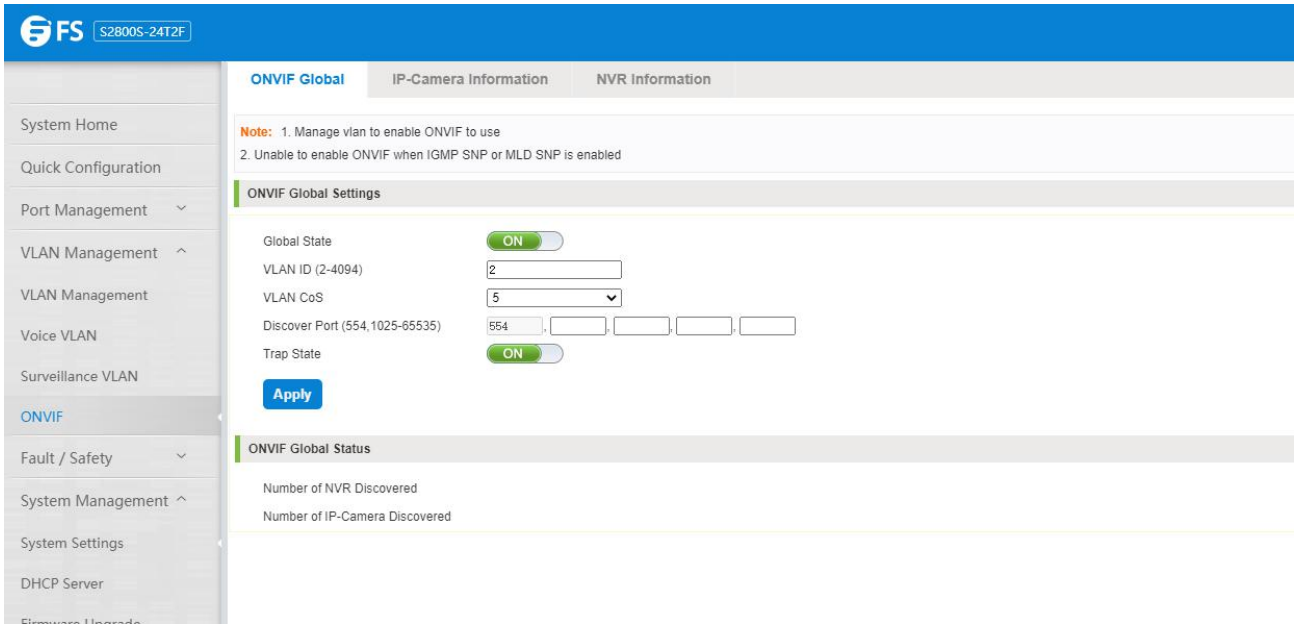


Figure 5-19: ONVIF information

To configure the ONVIF Steps as follows:

Step 1: Turn off IGMP and MLD functions;

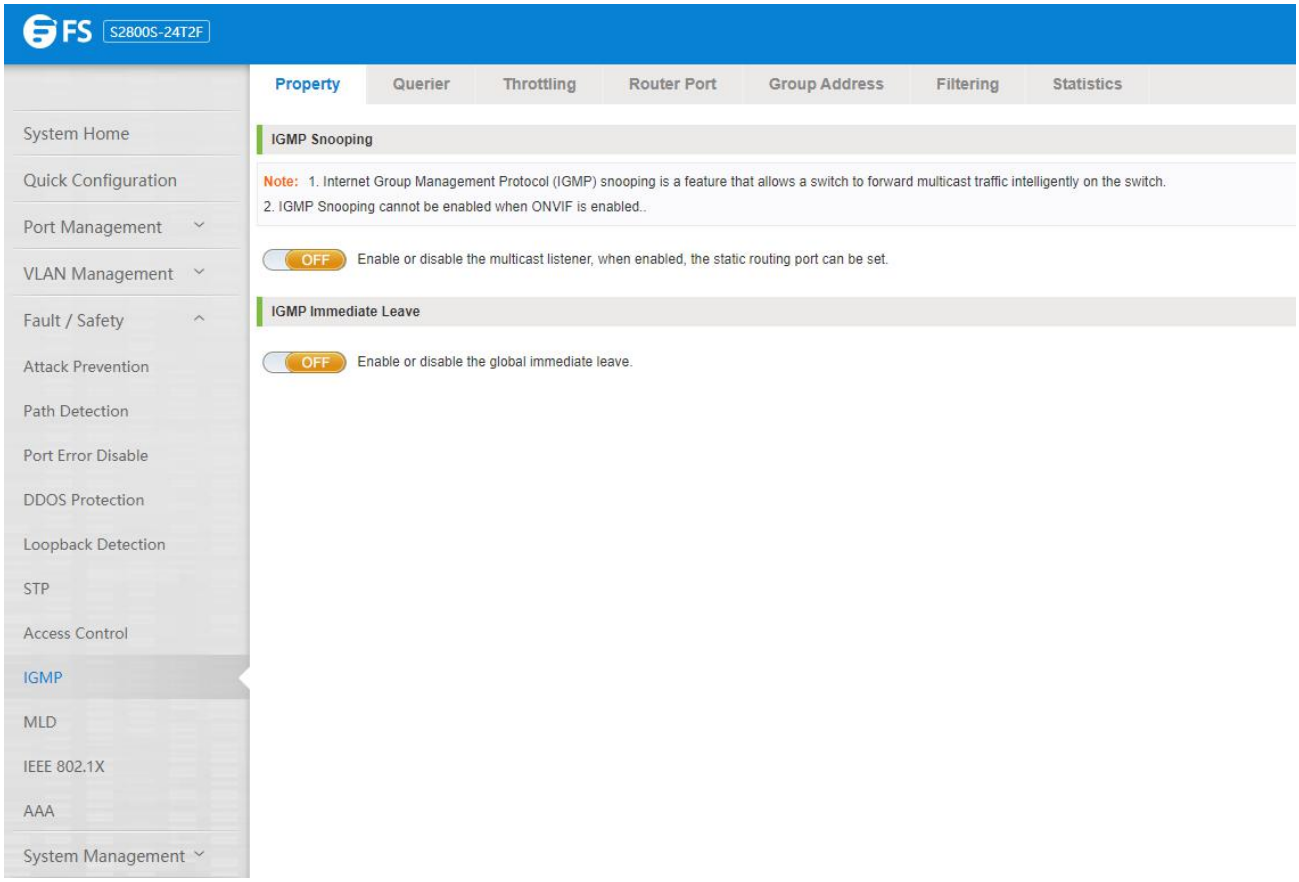


Figure 5-20: Turn off IGMP

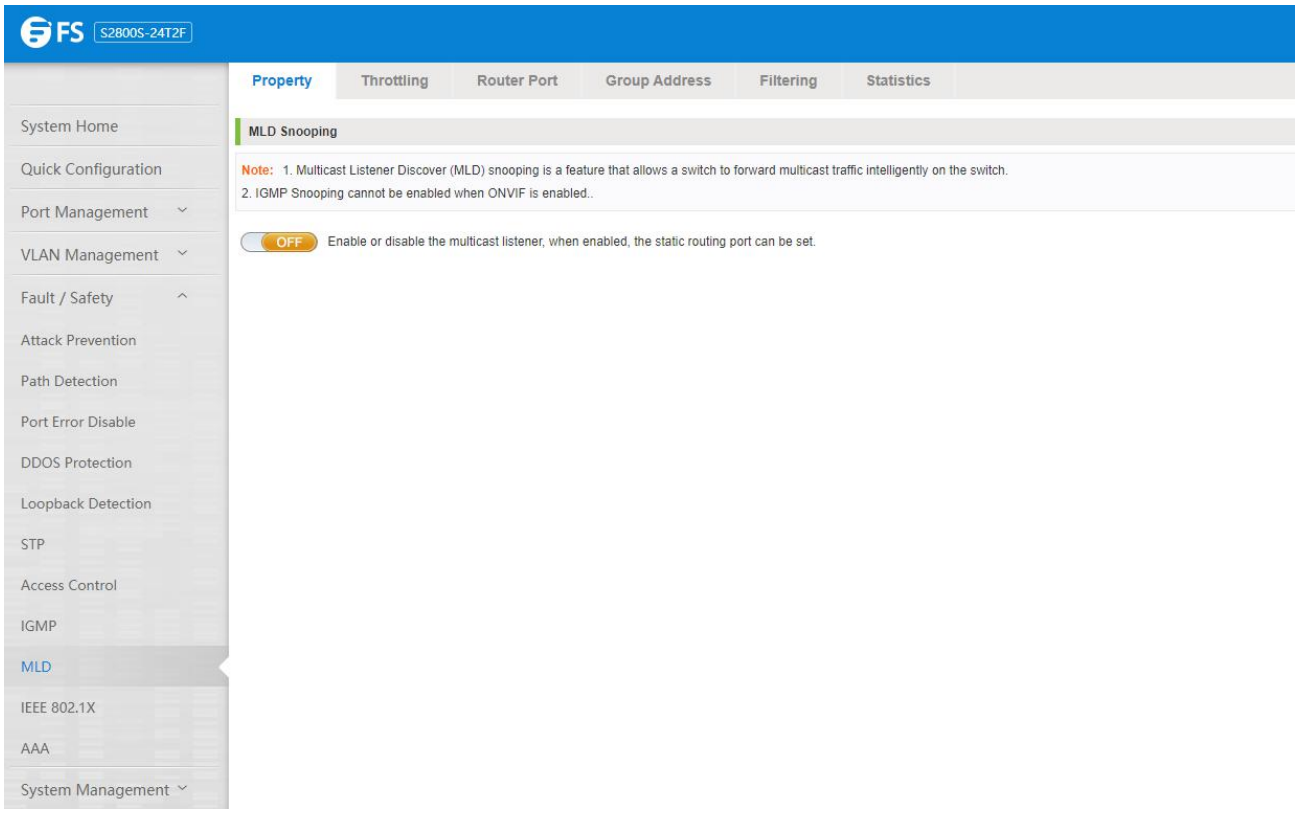


Figure 5-21: Turn off MLD

Step 2: Enable management VLAN;

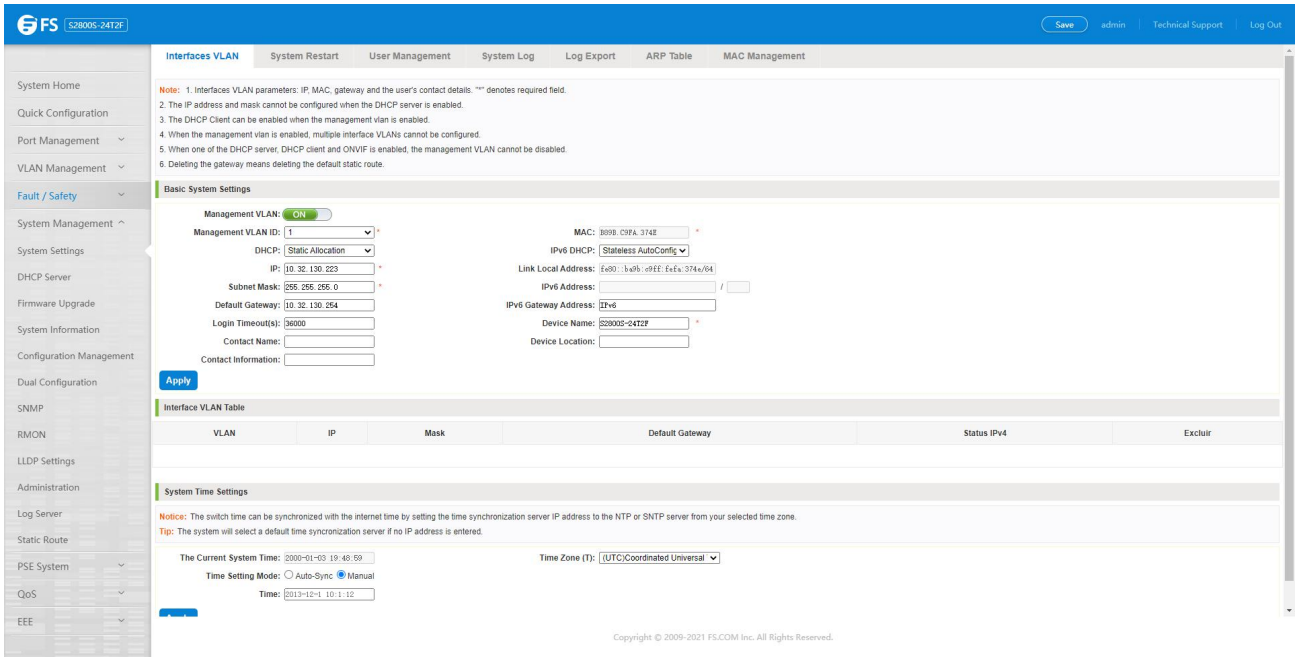


Figure 5-22: Enable management VLAN

Step 3: Confirm that the IP address segment of switch management address is the same as that of IPC and NVR;

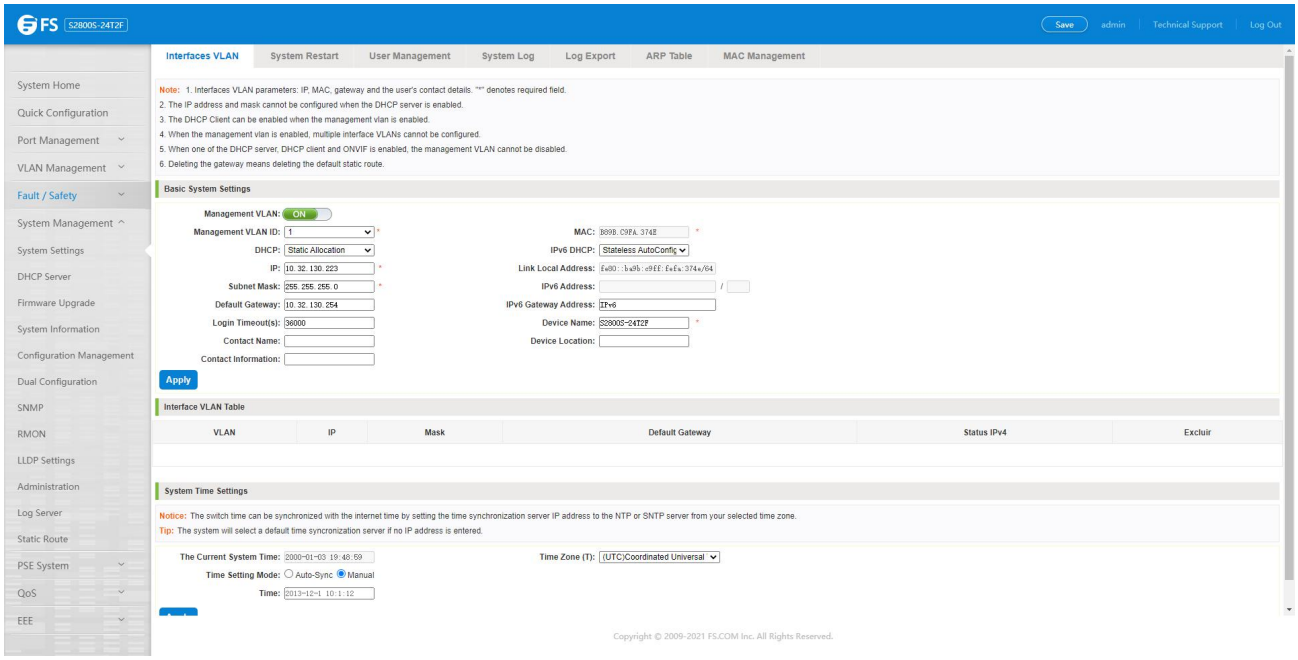


Figure 5-23: Configure IP address

Step 4: Configure the VLAN ID;

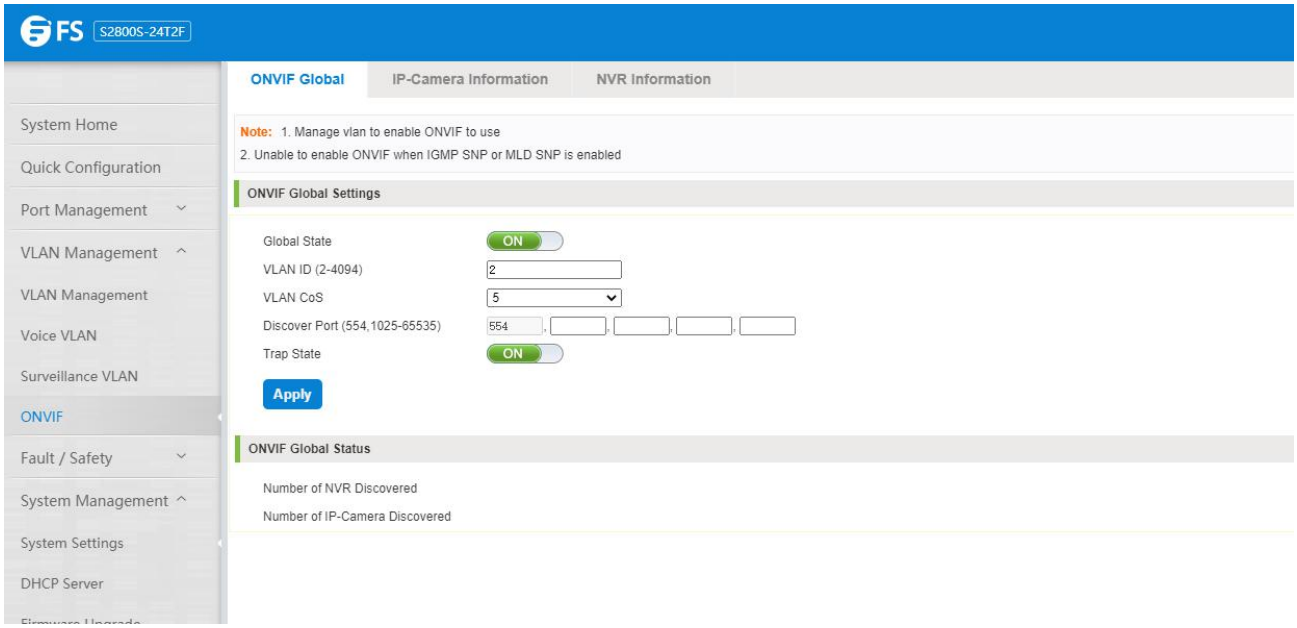


Figure 5-24: Configure the VLAN ID

Step 5: Configure the port number used by the ONVIF protocol, The default is 554.

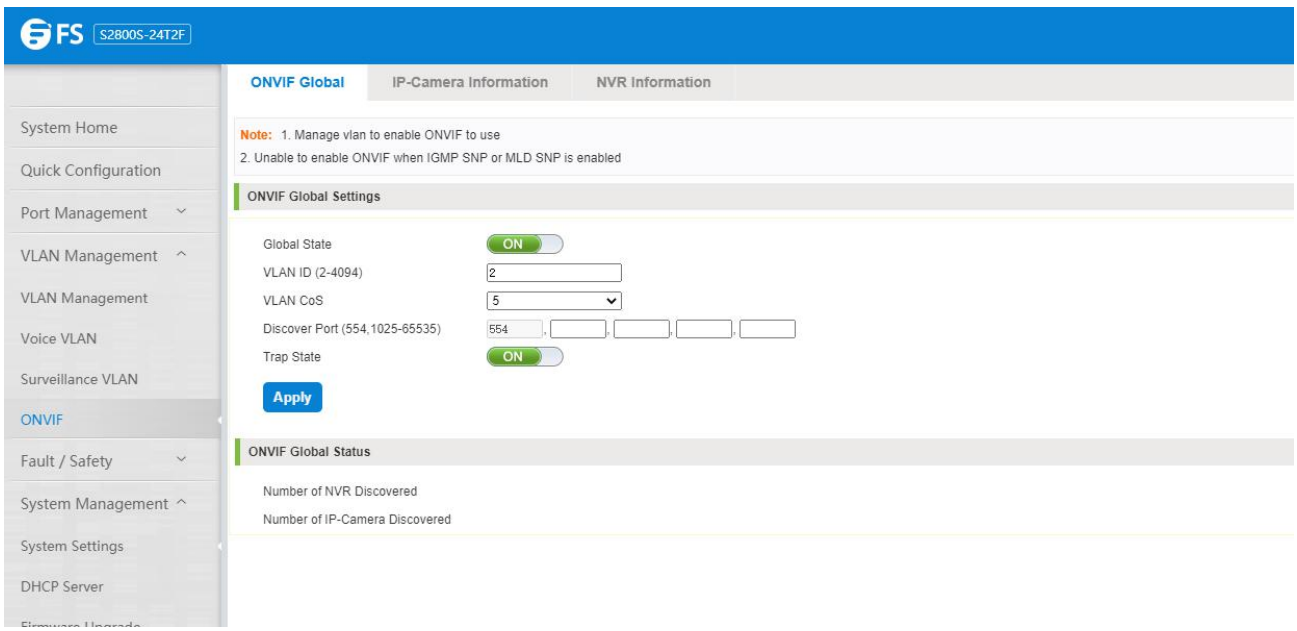


Figure 5-25: Configure the port number

5.4.2 View IP-Camera Information

Click on the navigation bar "VLAN Management" "ONVIF" " IP-Camera Information" to view the IP-Camera information:

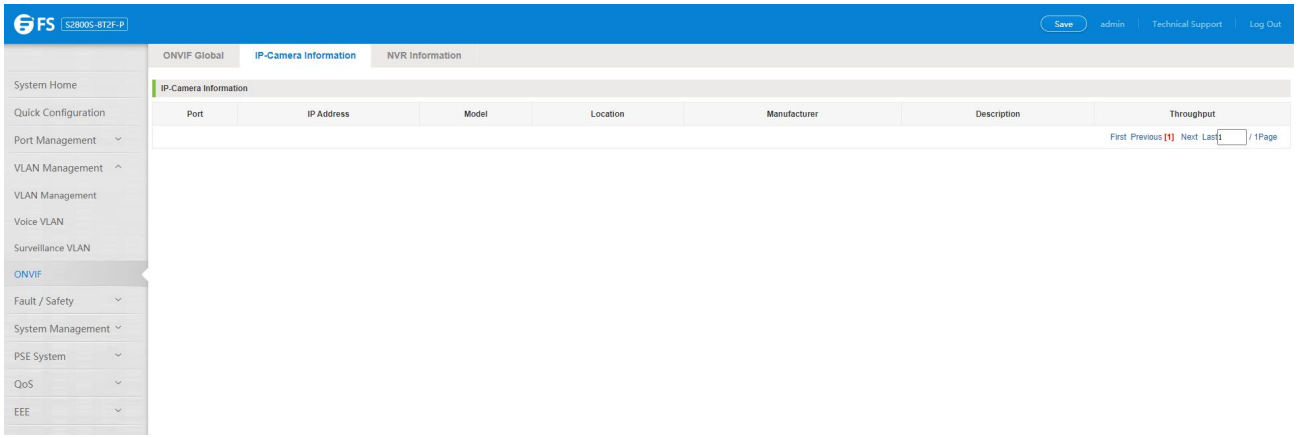


Figure 5-26: IP-Camera information

5.4.3 View NVR Information

Click on the navigation bar "VLAN Management" "ONVIF" " NVR information" to view the switch NVR information:

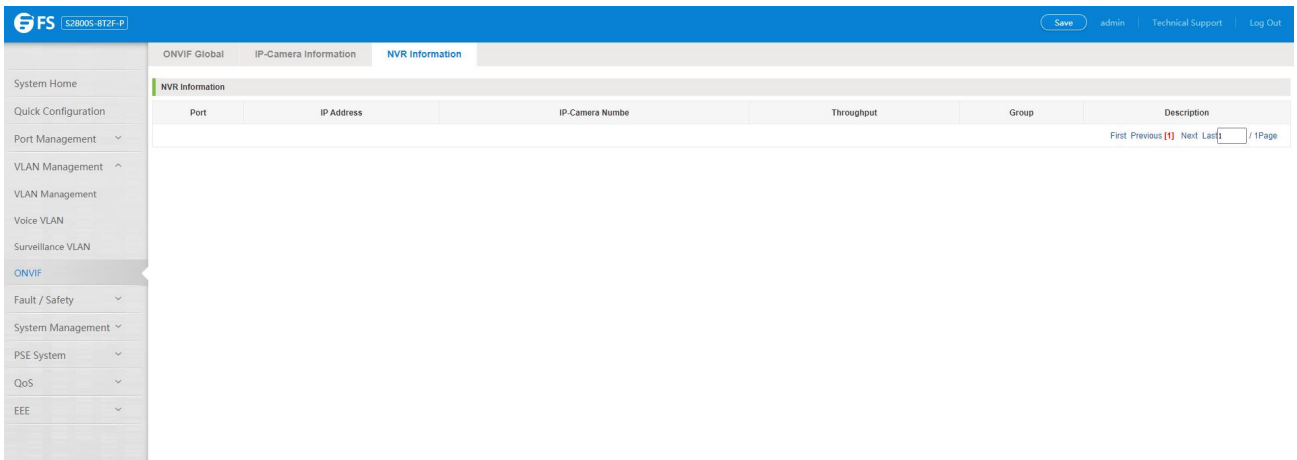


Figure 5-27: NVR information

6. Fault / Safety

6.1 Attack Prevention

6.1.1 ARP Spoofing

6.1.1.1 View ARP Configuration

Click the "Fault/Safety" “Attack Prevention” "ARP Inspection“ to check the current switches has been configured for ARP information, this feature is turned off by default .

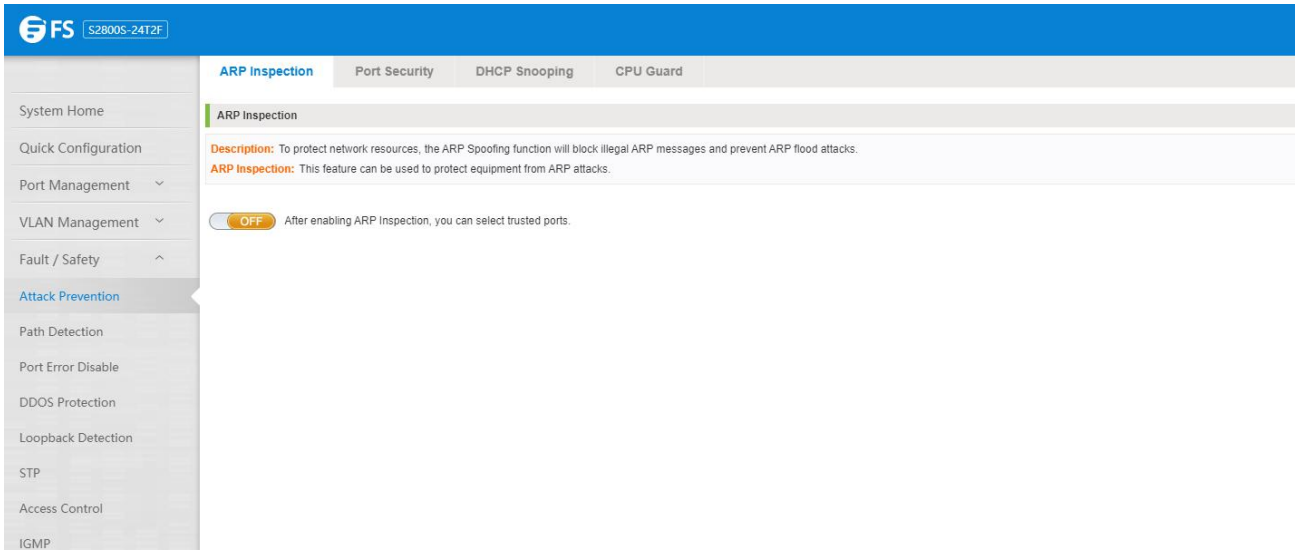


Figure 6-1: View port ARP Inspection information

6.1.1.2 ARP Inspection Function

In the ARP Inspection configuration, enable this function and then selected a port to configure some parameters. Click the "Save" button to complete the configuration.

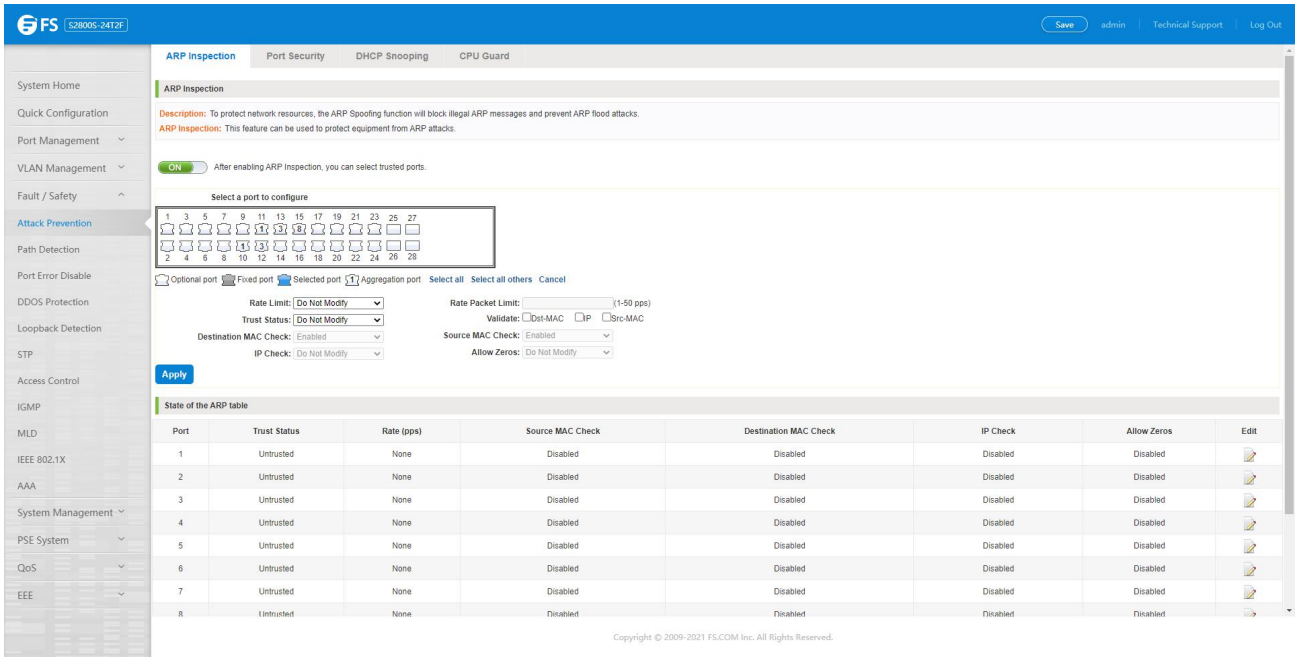


Figure 6-2: ARP Inspection configuration

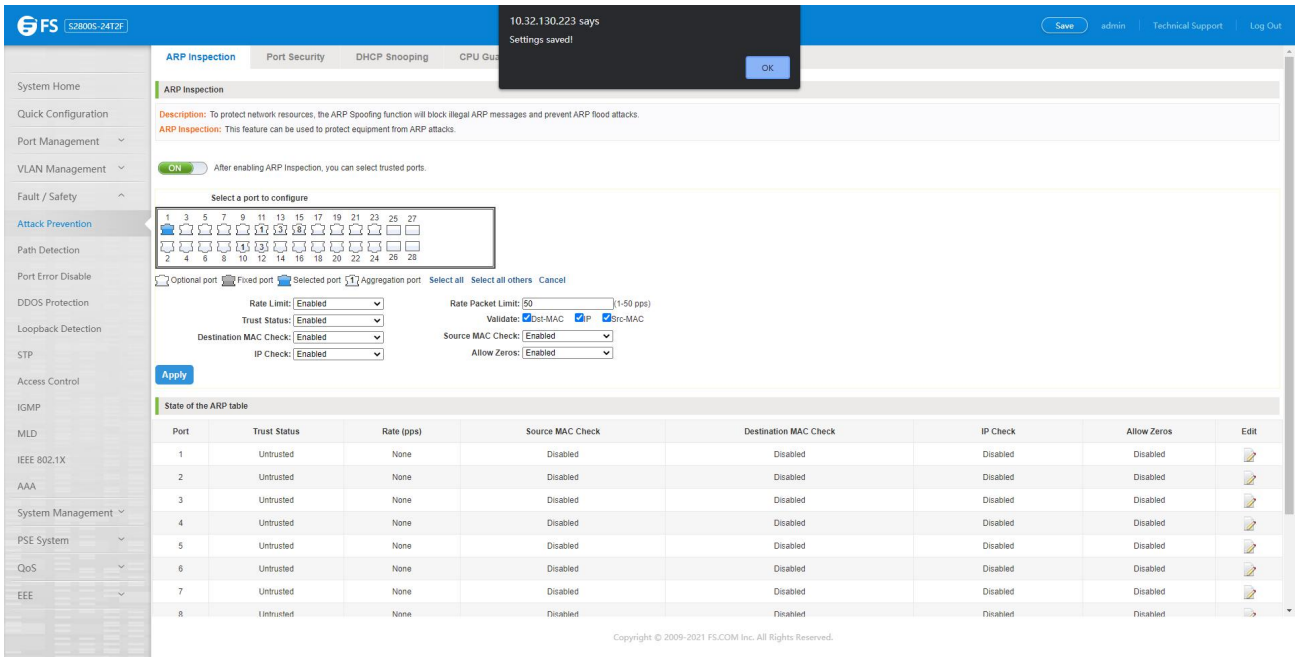
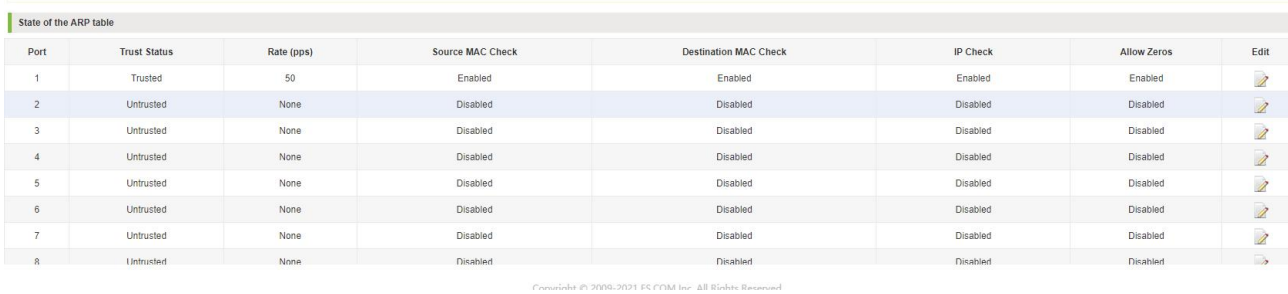


Figure 6-3: Change ARP Inspection configure


State of the ARP table

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Trusted	50	Enabled	Enabled	Enabled	Enabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
4	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
5	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
6	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
7	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
8	Untrusted	None	Disabled	Disabled	Disabled	Disabled	

Figure 6-4: Change ARP Inspection configure success

6.1.1.3 Disable ARP Inspection Function

In the ARP Inspection configuration table, click the button from on to off to disable the ARP Inspection and then click the "OK" button to complete the configuration.

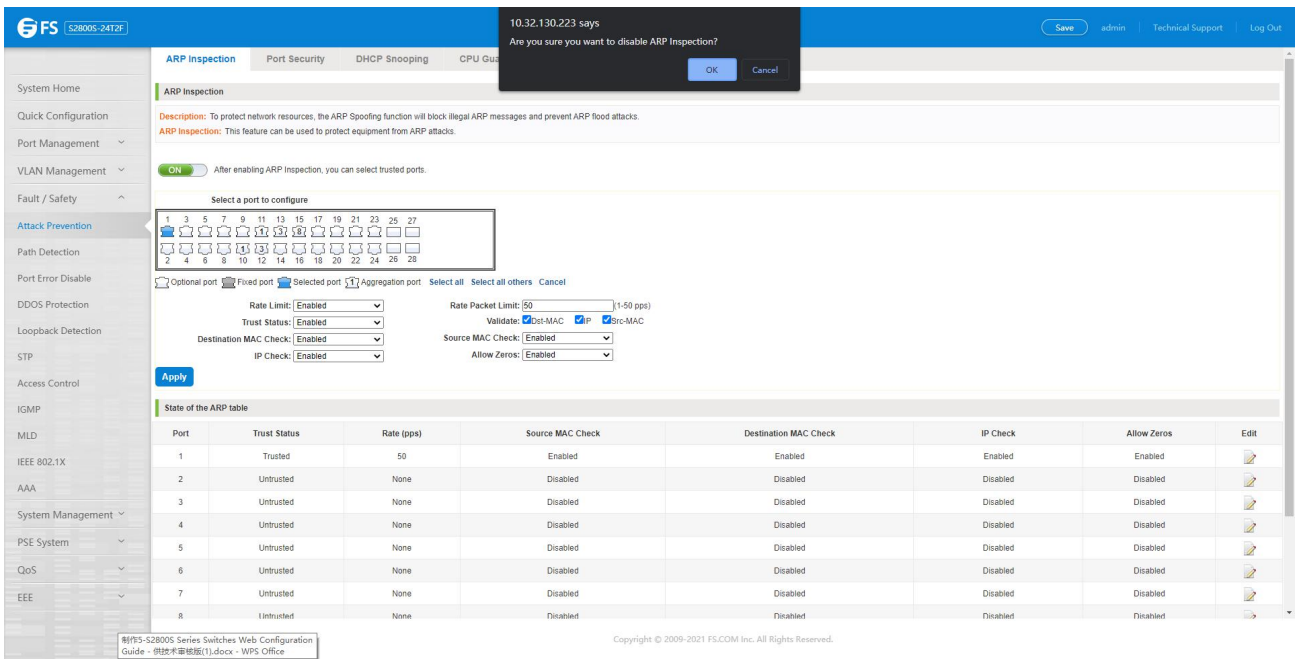


Figure 6-5: Disable ARP Inspection function

6.1.2 Port Security

6.1.2.1 Port Security Configuration

Click the "Fault/Safety" "Attack prevention" "Port Security", configure the switch port security:

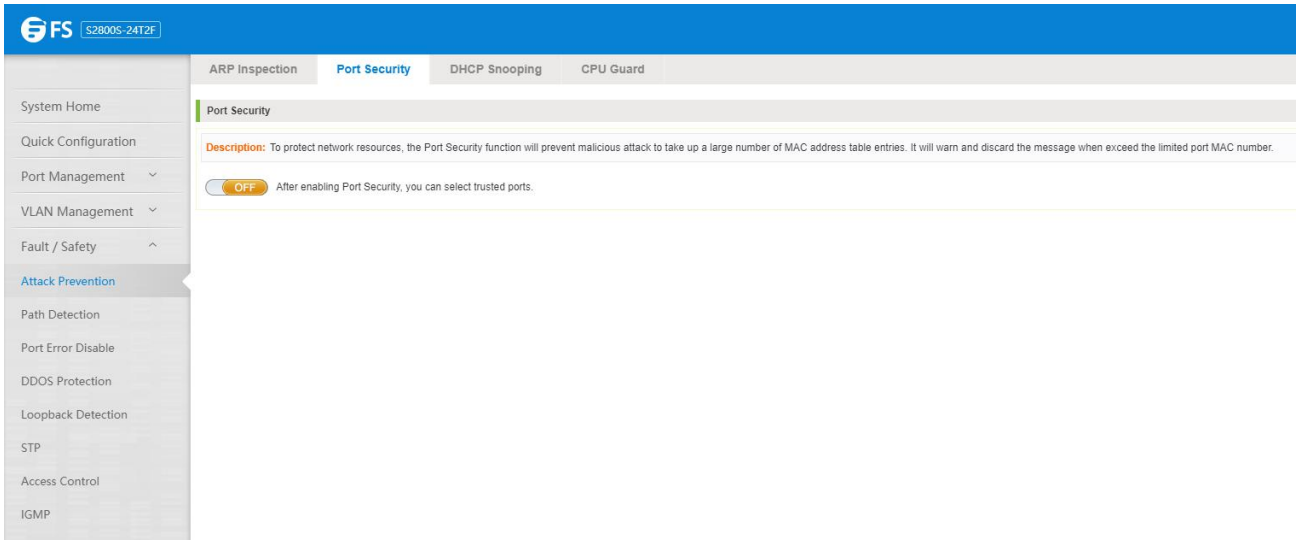


Figure 6-6: Port security configuration

In the configuration page, selected one or more ports, enable the admin state and configure the port max learning address. Finally, click "Save" button.

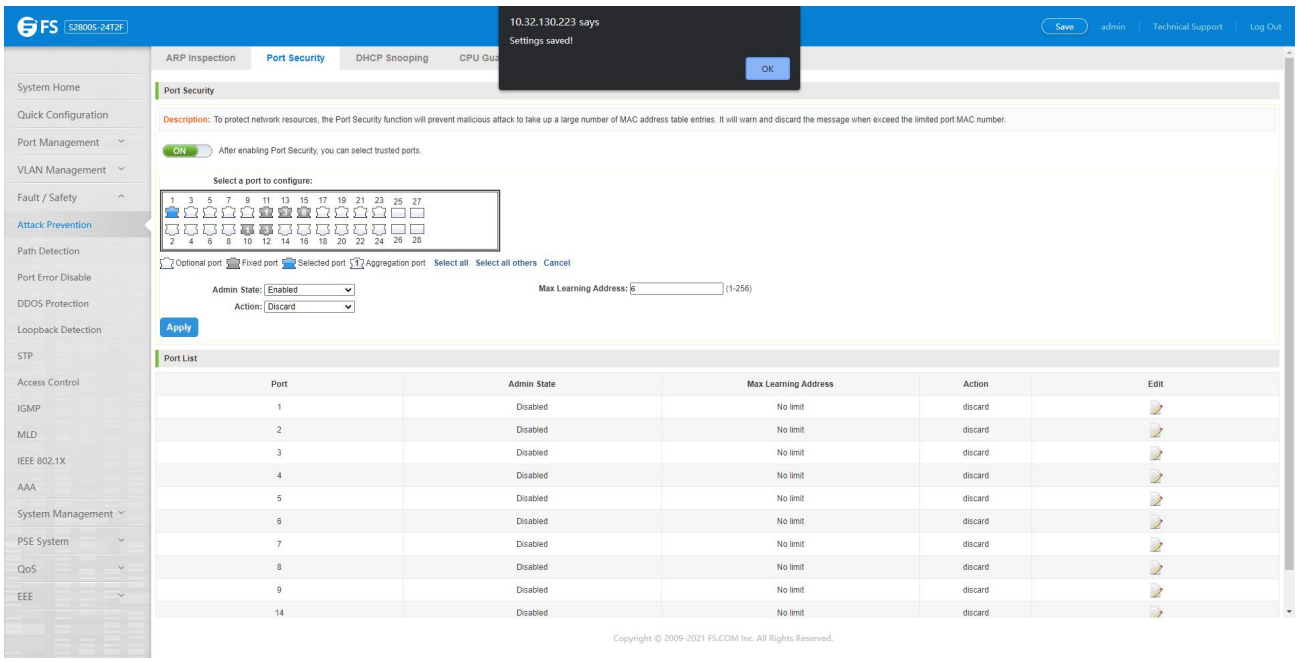


Figure 6-7: Port security manual configuration

6.1.2.2 Change Port Security Status

In the port list, select the port to edit, change some parameters or disable the port security and click the button of "Save".

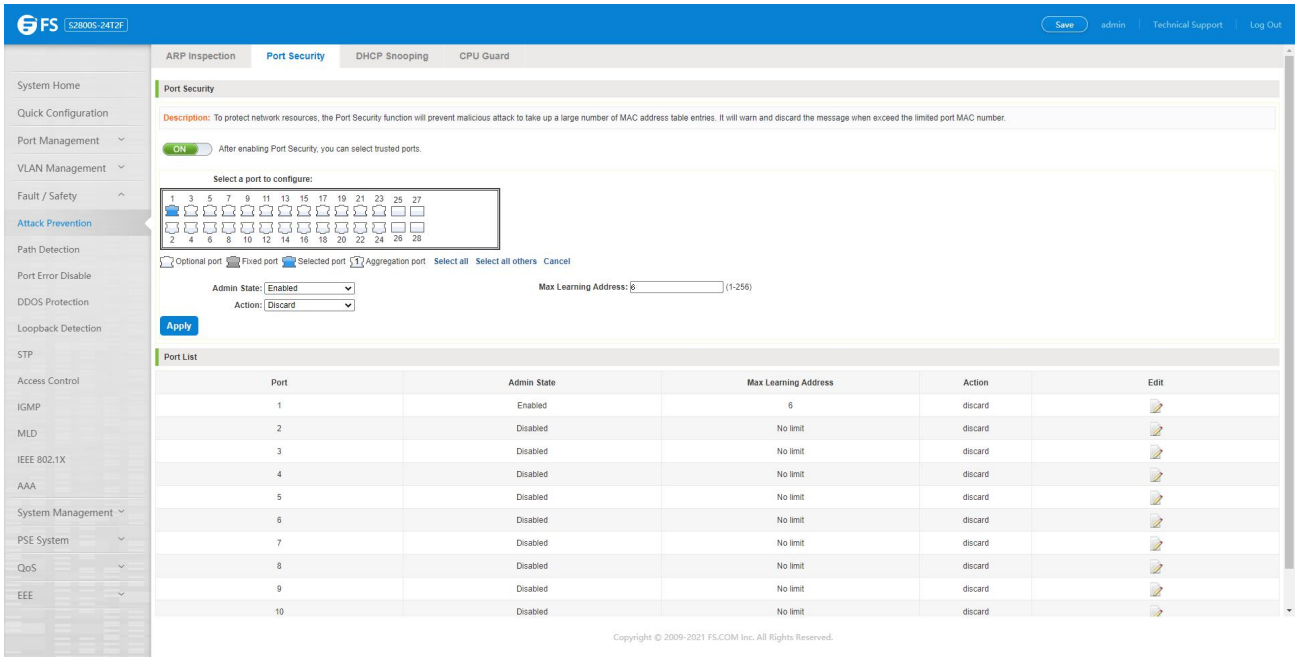


Figure 6-8: Change port security status

6.1.3 DHCP Snooping

6.1.3.1 View DHCP Snooping Configuration

Click the "Fault/Safety" "Attack prevention" "DHCP snooping", the configuration information show the anti DHCP attack:

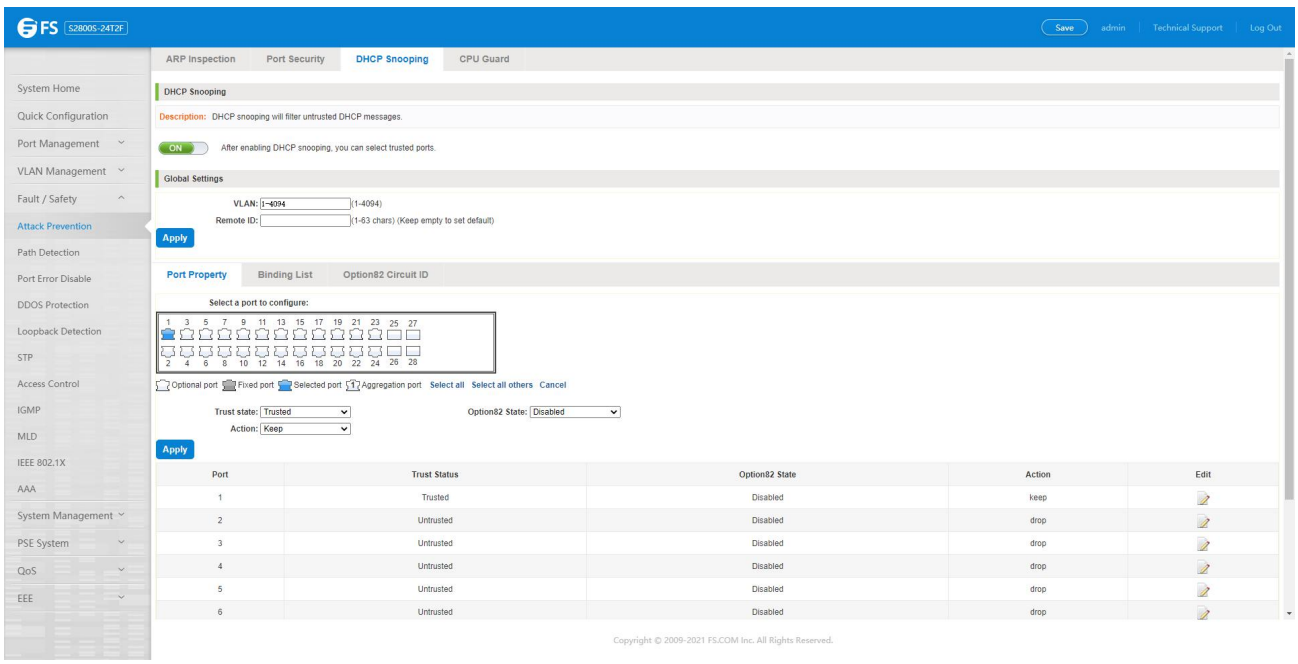


Figure 6-9: View anti DHCP snooping configuration information

Display refresh configuration information.

6.1.3.2 Open DHCP Snooping Function

Click on a "Fault/Safety" "DHCP Snooping" click the button 

to open the DHCP snooping:

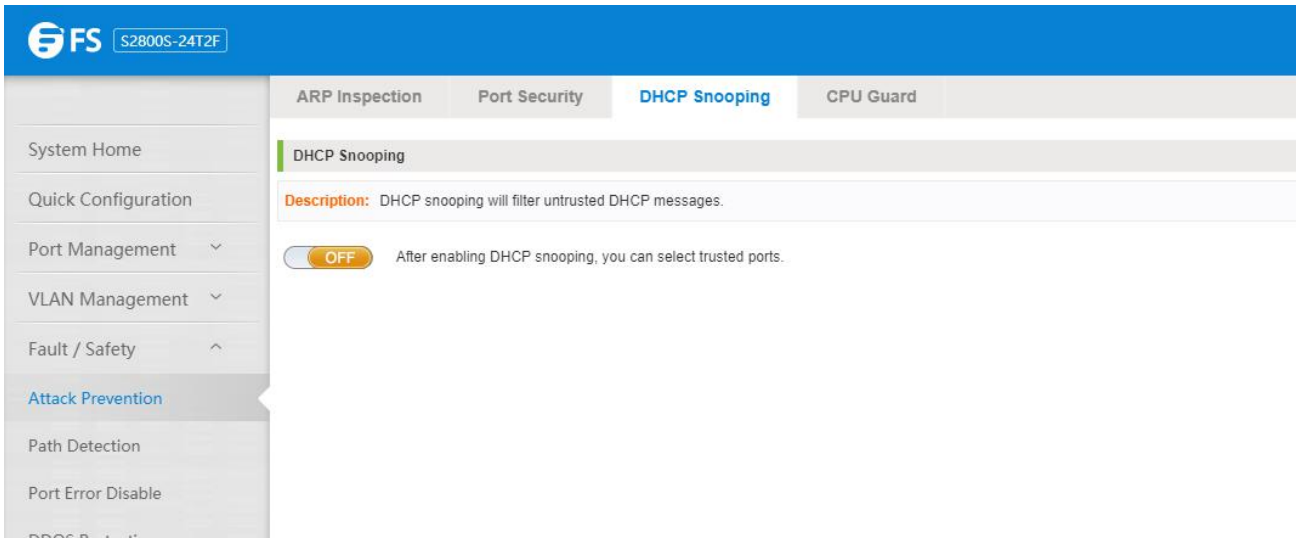


Figure 6-10: Activation of DHCP snooping function

6.1.3.3 Set the Port to DHCP Snooping Trusted Port

In the trusted port list, select the port that needs to be disabled to prevent DHCP attacks, and click the "Save" button and enable option82 function.

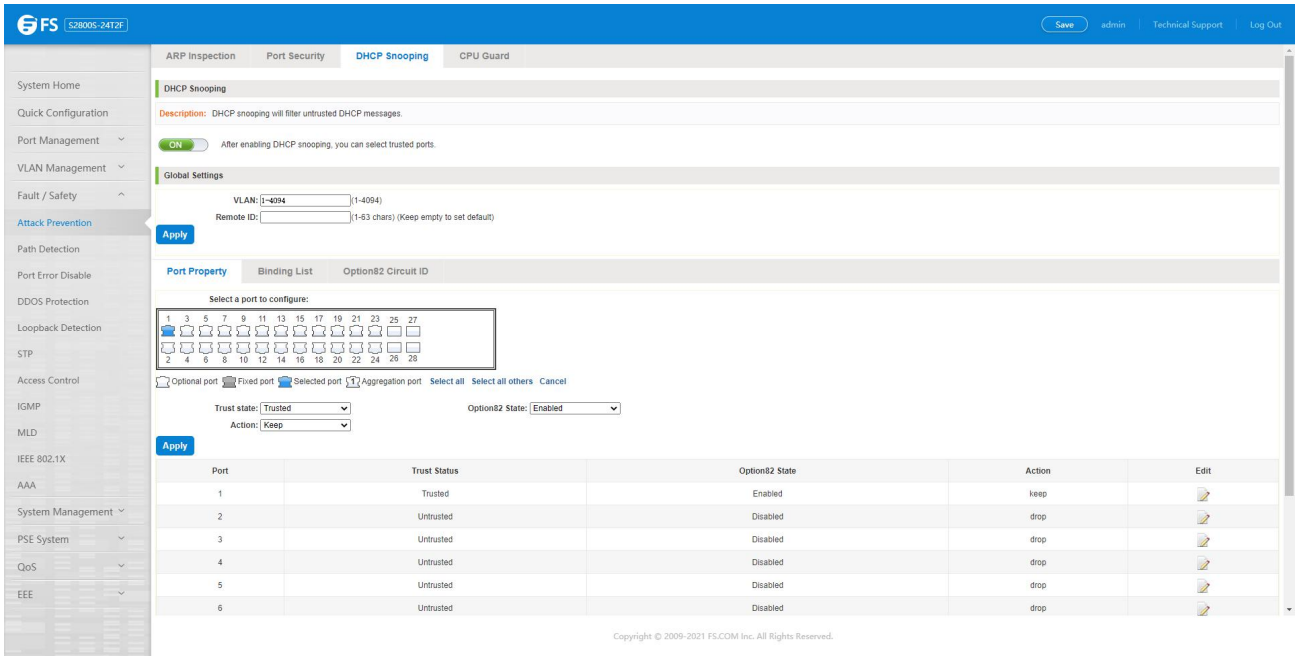


Figure 6-11: Disable anti illegal DHCP server functions and enable option 82

The activation of anti DHCP attack function, is the port setting for trust status;

Disable - preventing DHCP attack, is set to a non-trusted state port.

6.1.3.4 Configure CID Information

Click the "Option82 Circuit Id" button, configure the CID information:

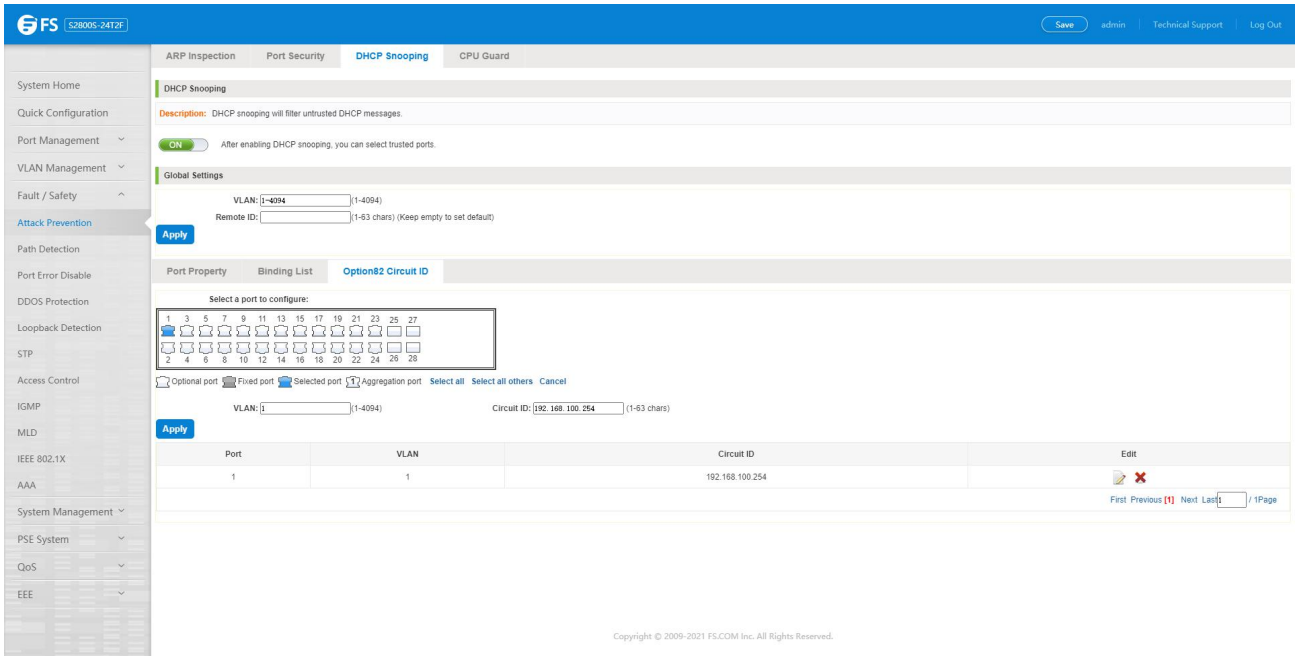


Figure 6-12: CID information

6.1.3.5 Off DHCP Snooping Function

Click the "ON" button, will prevent the DHCP attack function off:

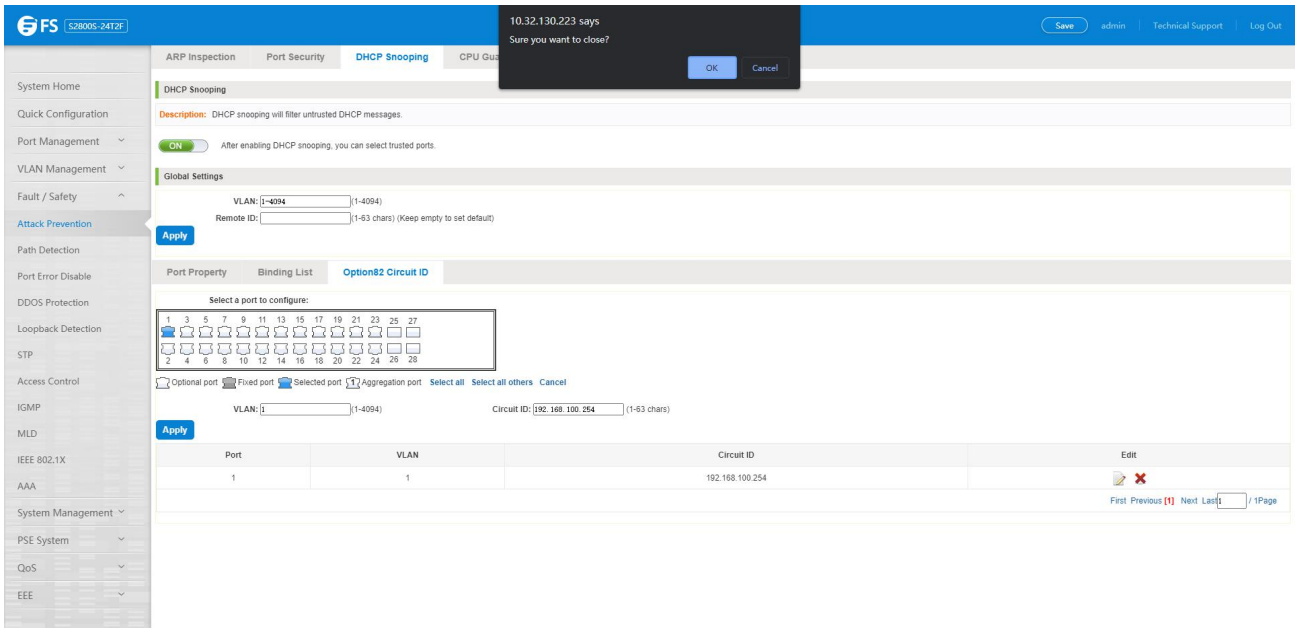


Figure 6-13: Off DHCP snooping function

6.1.4 CPU Guard

Click the "Fault/Safety" "Attack prevention" "CPU Guard", the configuration information show the CPU guard.

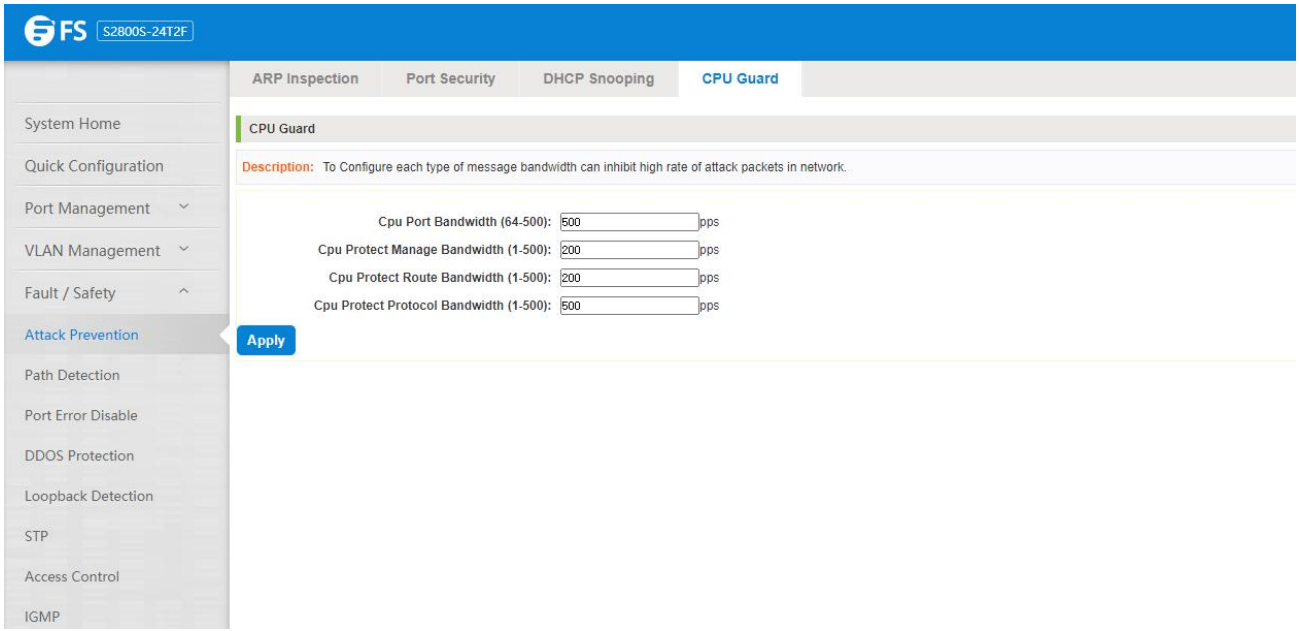


Figure 6-14: CPU Guard information

Change CPU guard configuration:

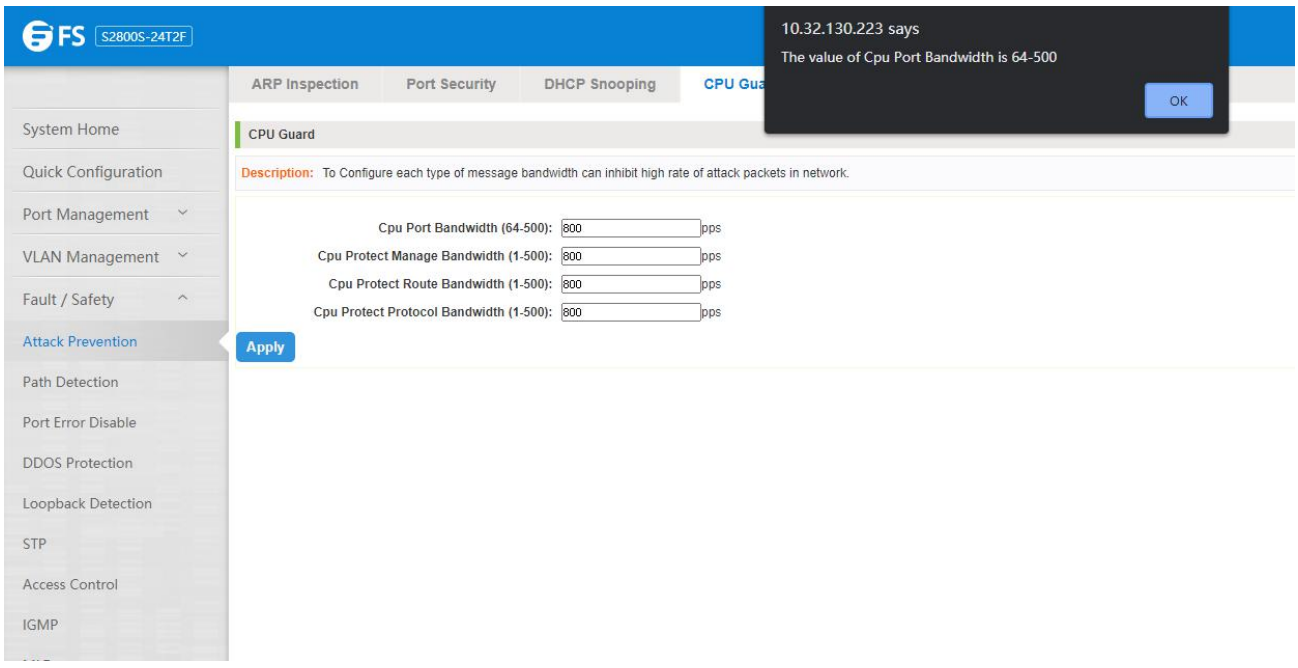


Figure 6-15: Change CPU Guard configuration

6.2 Path Detection

6.2.1 Path Detection

Click the "Fault/Safety" "Path Detection" or “Tracert detection” can view the Path Detection configuration:

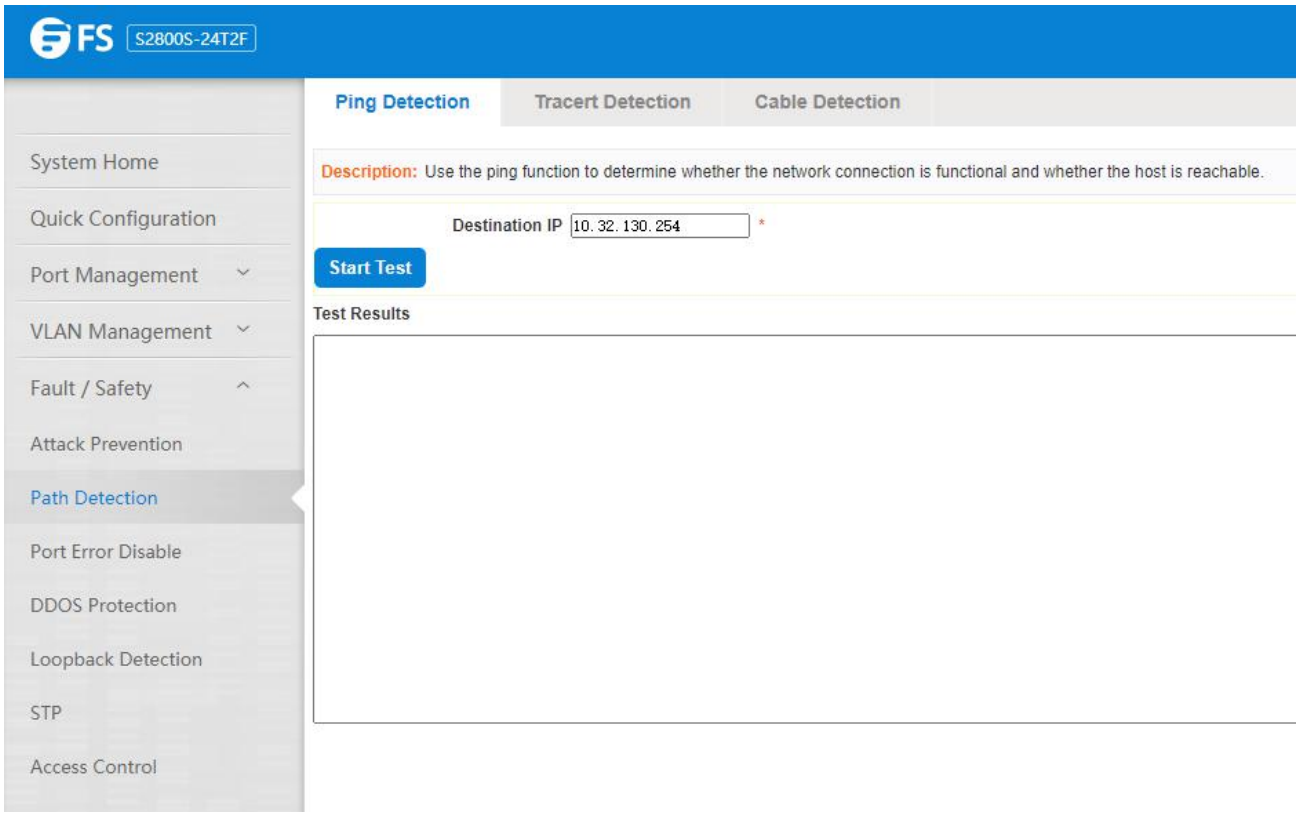


Figure 6-16: Path detection information

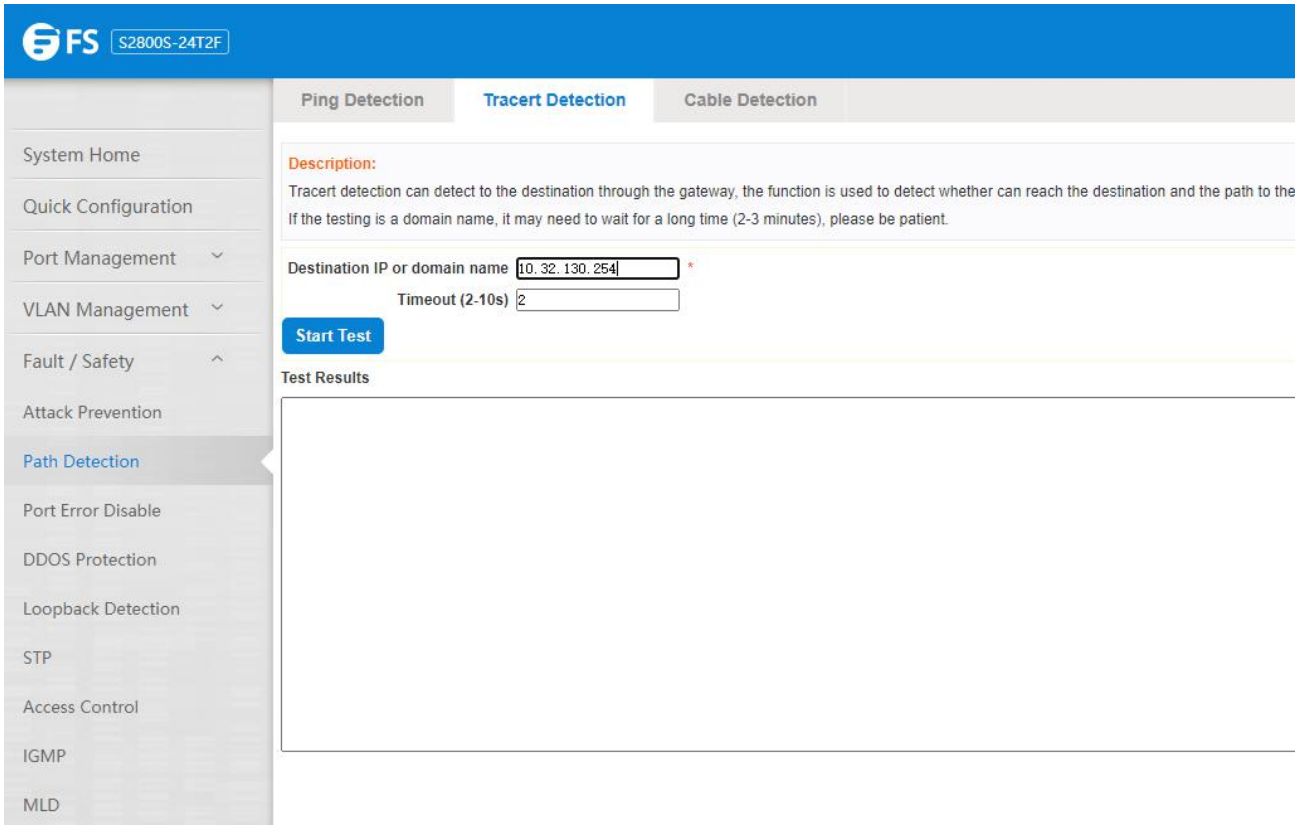


Figure 6-17: Tracert detection information

6.2.2 Cable Detection

Click the "Fault/Safety" "Path Detection" “Cable Detection” can view the Cable Detection configuration:

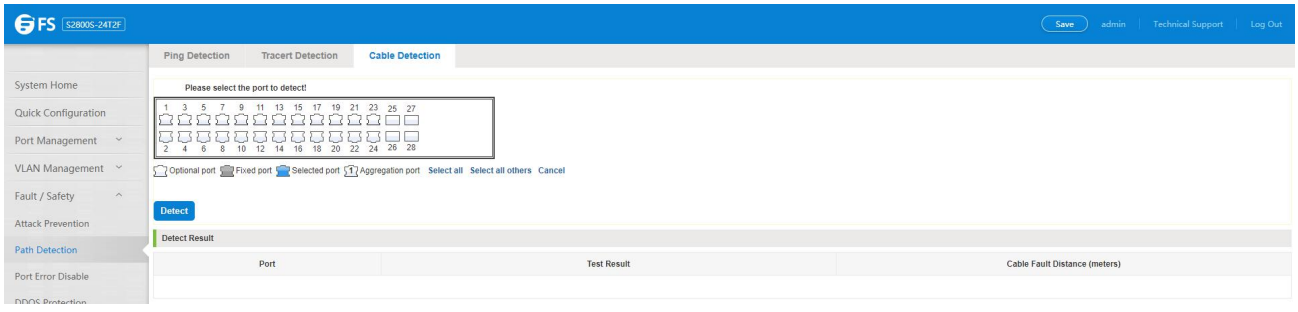


Figure 6-18: Cable detection information

The cable detection only selected one port:

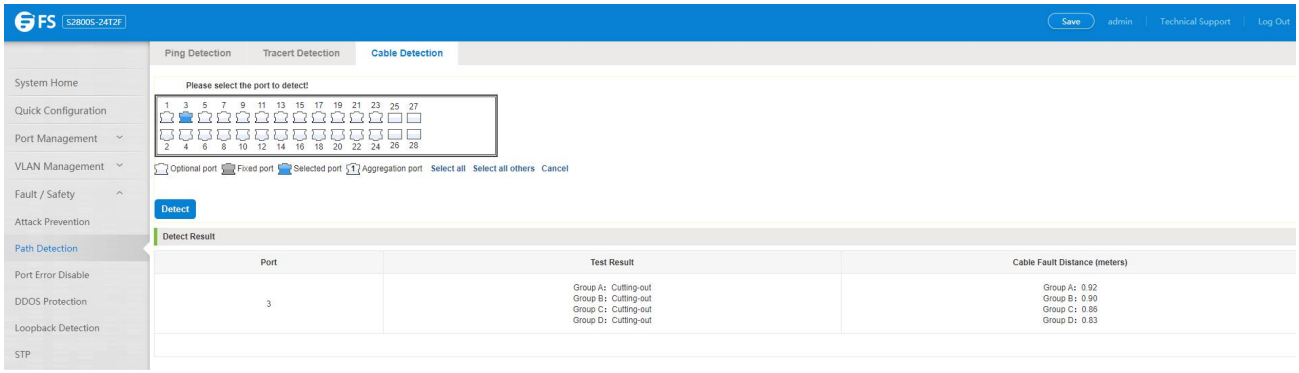


Figure 6-19: Port cable detection result

6.3 DDoS Protection

Click the "Fault/Safety" "DDoS Protection" can view the DDoS protection configuration:

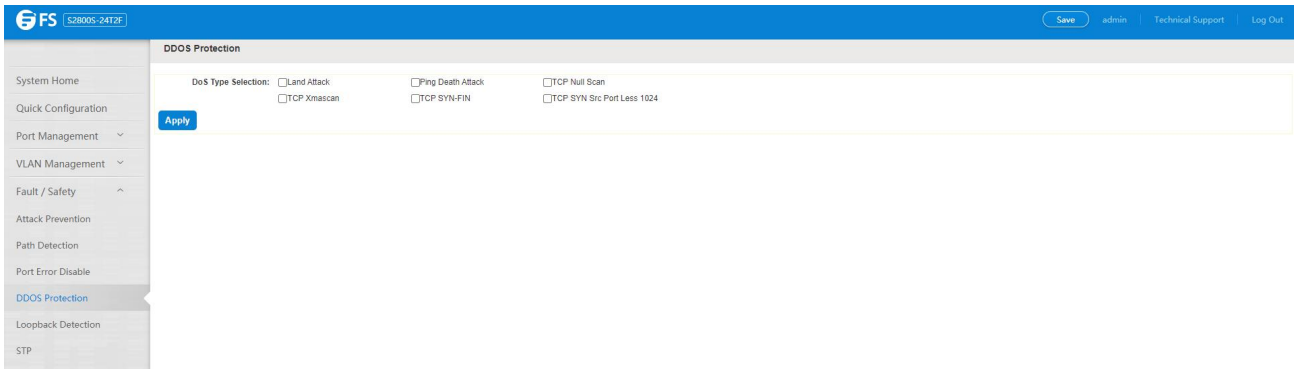


Figure 6-20: DDoS Protection information

Selected dos type to prevent multiple computers from sending attack packets.

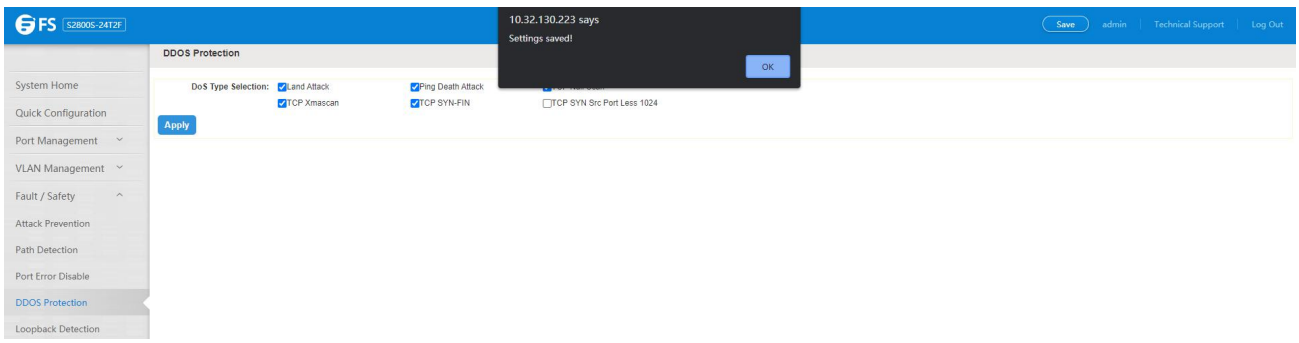


Figure 6-21: Selected dos type

6.4 Loop Detection

Click the "Fault/Safety" "loop detection" can view the current loop detection configuration:

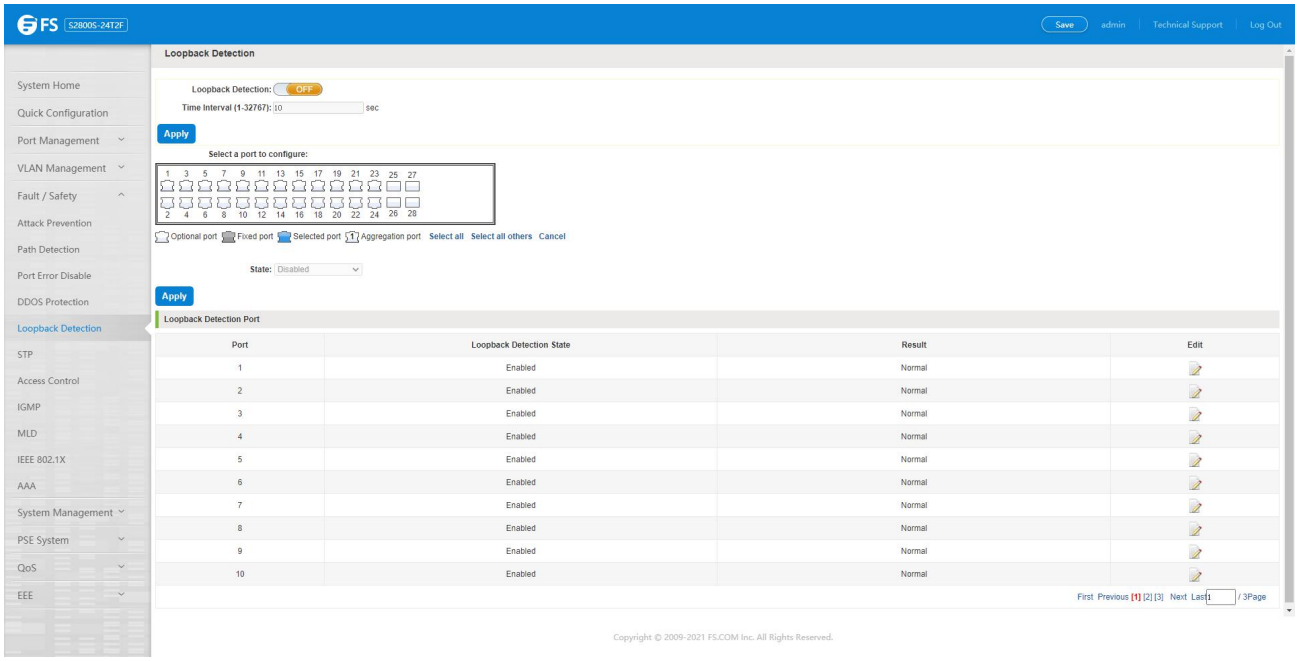


Figure 6-22: View loopback detection configuration information

6.4.1 Enable Loopback Detection

Enable the loopback detection and configuration some parameters, click "Save" button:

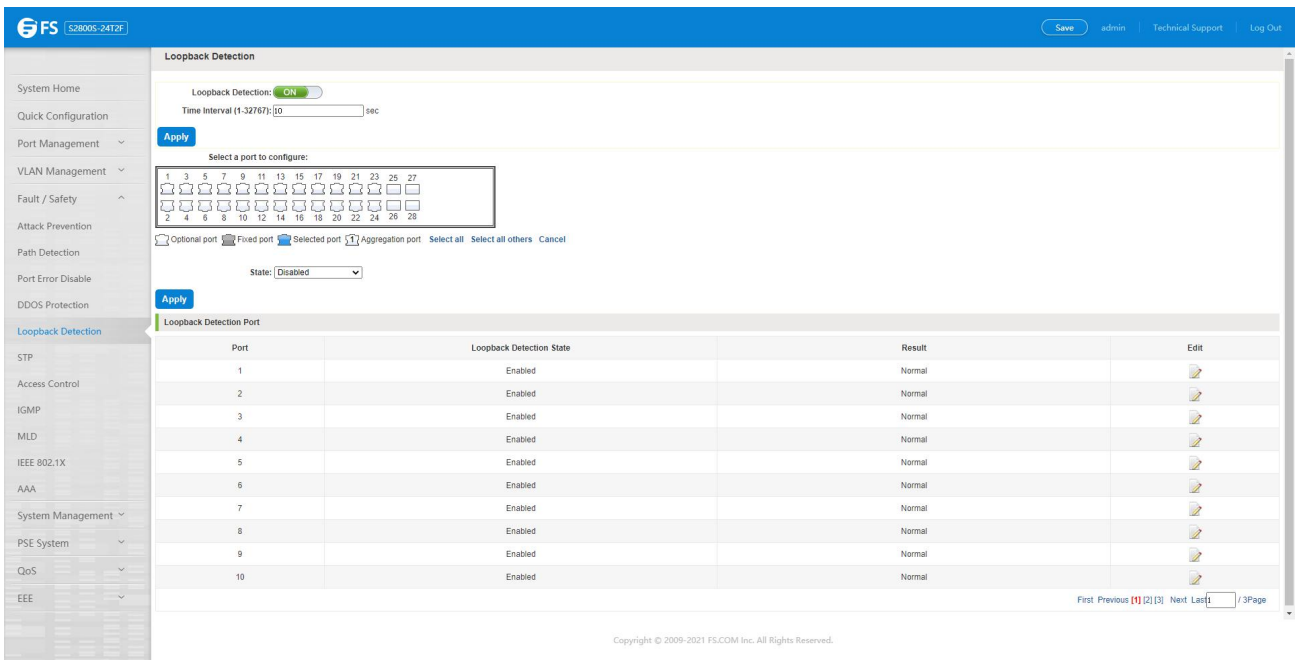


Figure 6-23: Enable loopback detection

6.4.2 Choose the Port to Configure

Select one or more ports to change the loopback detection status:

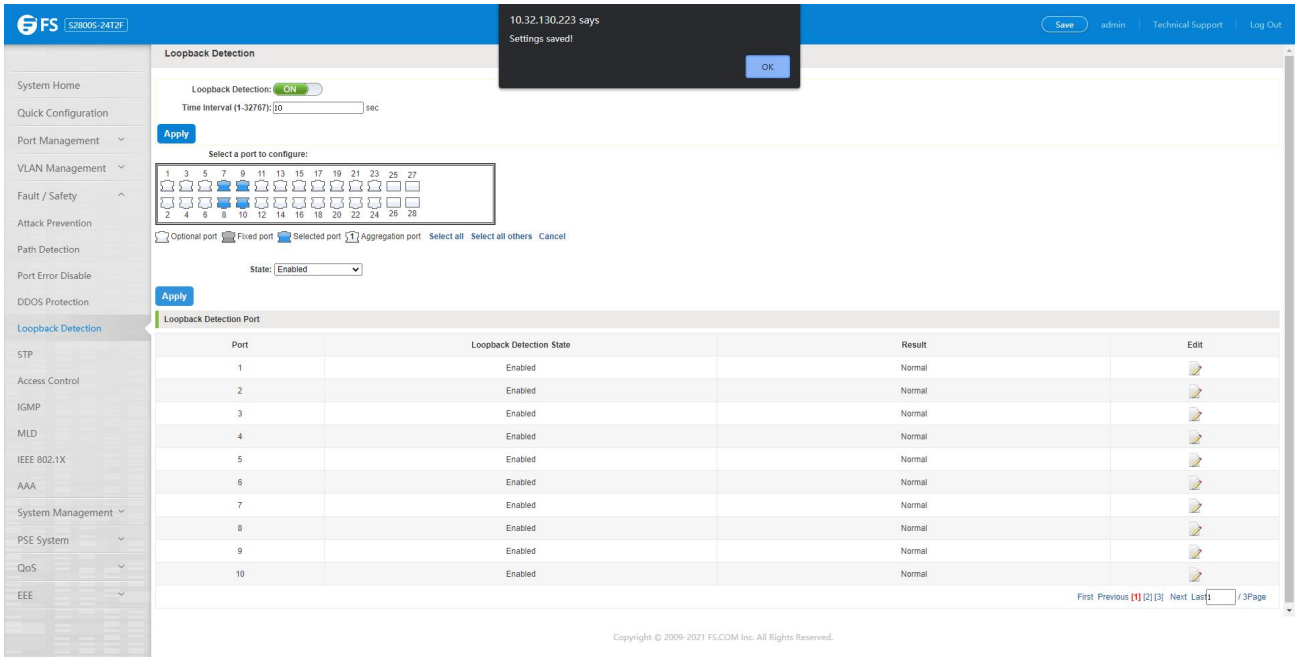


Figure 6-24: Configure ports parameter

Click “Edit” button, change the port status:

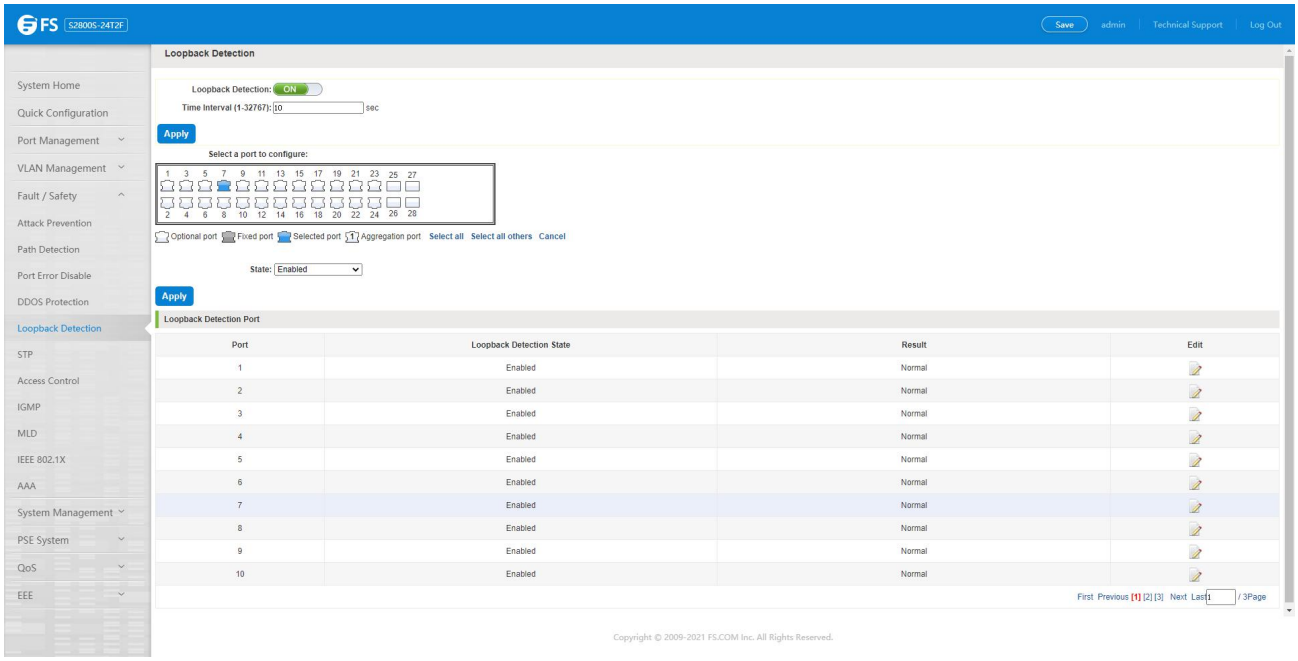


Figure 6-25: Change the port configure

6.5 STP

Click the "Fault/Safety" "STP" “STP Global” can view the current STP global configuration:

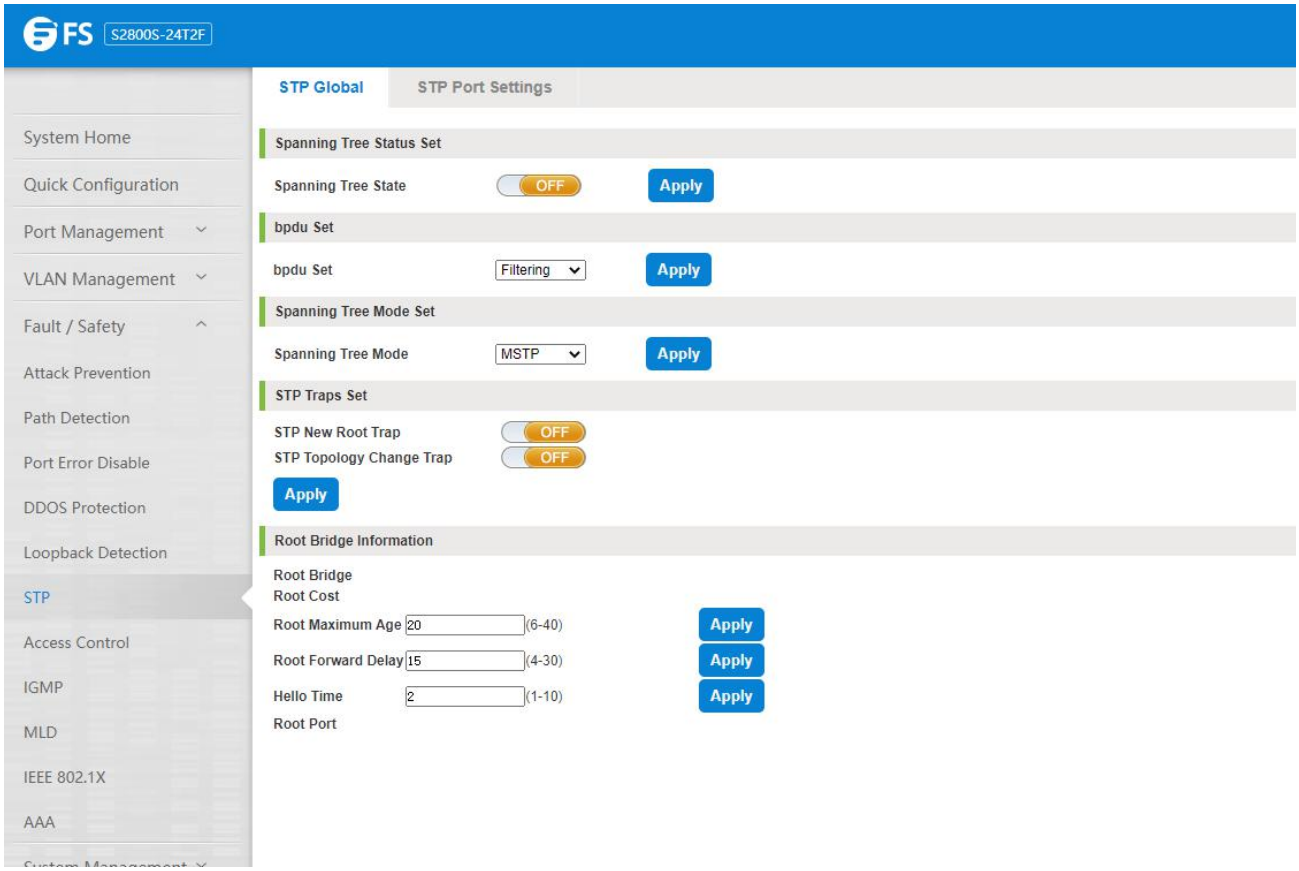


Figure 6-26: STP Global view

6.5.1 Enable STP Function

Enable STP global state and configuration mode and traps.

Notice:

1. When the loopback detection and STP functions are mutually exclusive.

2. LLDP PDU Flooding enabled prevents executing MSTP enable.

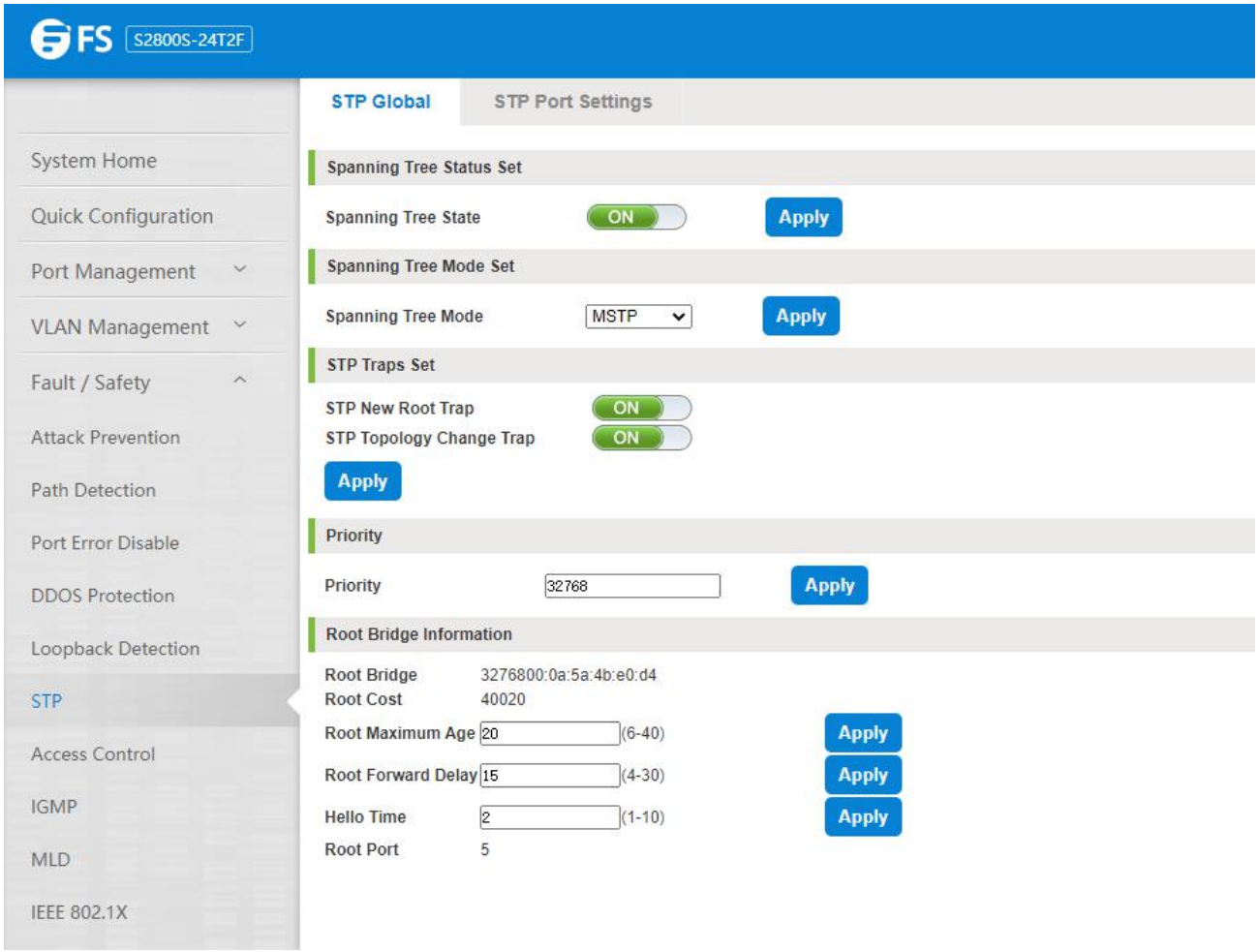


Figure 6-27: Enable STP change mode and traps

6.5.2 STP Port Settings

Selected port to configuration STP.

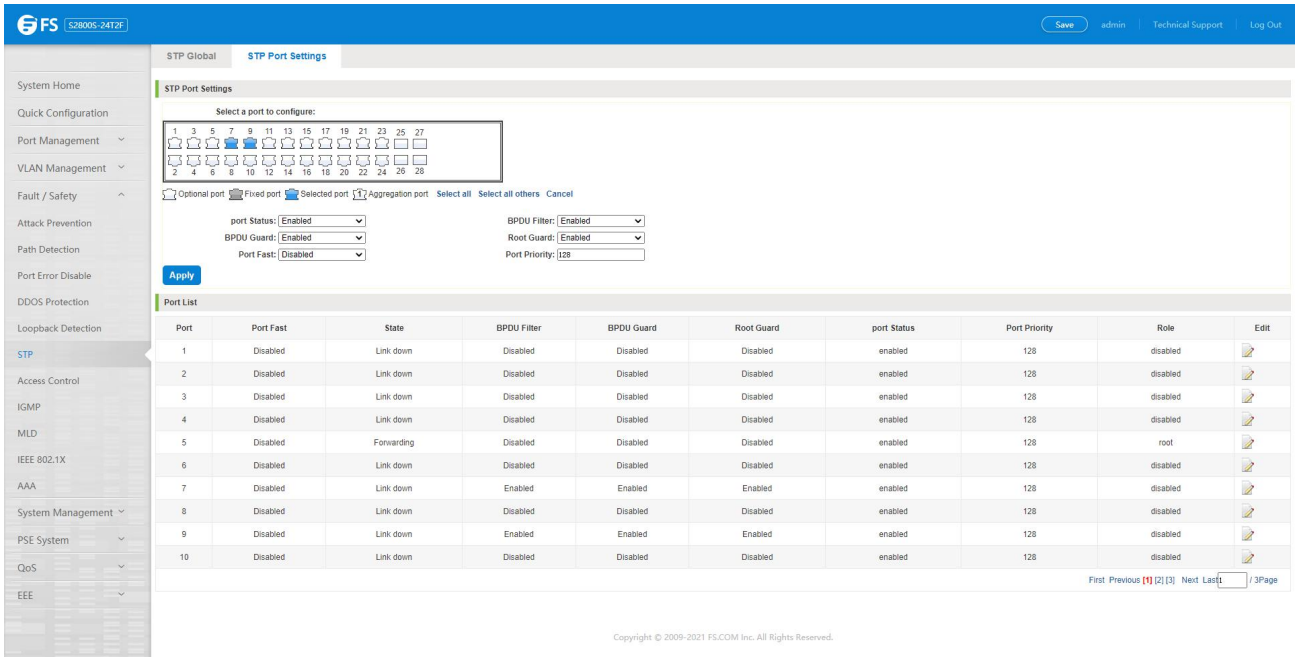


Figure 6-28: Selected port to configuration STP

6.6 Access Control

6.6.1 ACL Access Control List

6.6.1.1 View Access Control List

Click the "Fault/Safety" "Access Control" you can view the configuration information of the access control list:

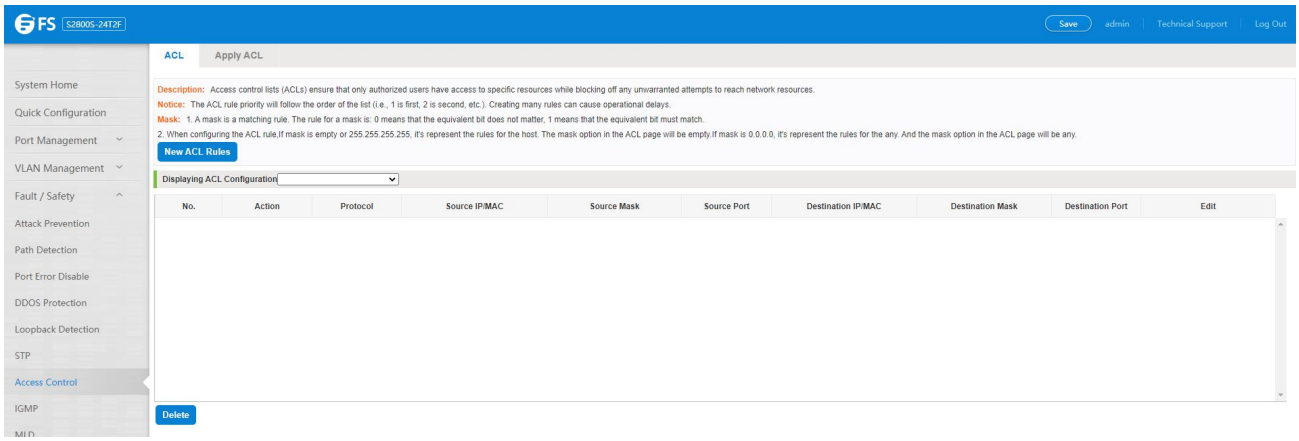


Figure 6-29: Access control list

6.6.1.2 Increased Access Rules

1. Increase the standard IP Access Rules

Click "ACL Rules New", in the pop-up dialog box, select "Standard IPV4 ACL Configuration", in the list of ID: 0, ID: 0 ACE, rules to allow. IP address is: any source IP address. Click "Save" to complete the new rules:

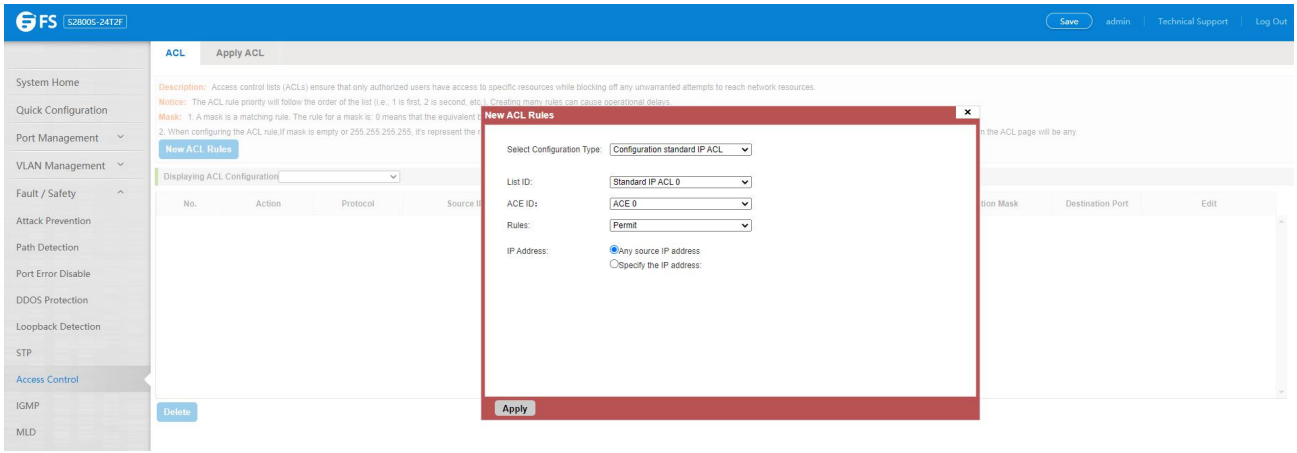


Figure 6-30: Configuration standard IP access control list

2. Increase the Extended IP Access Rules

Click "ACL Rules New", in the pop-up dialog box, select "Expand IPV4 ACL Configuration", in the list of ACE, ID: 0 ID: 10, rules for "Permit". Agreement: TCP, source IP address: any source IP address; purpose IP address: any destination IP address, click "Save" to complete the new:

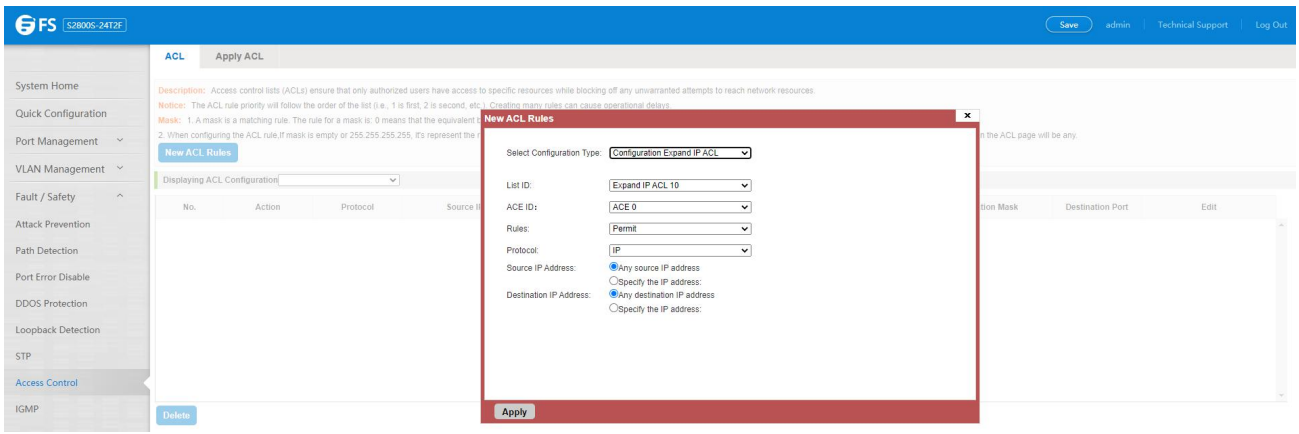


Figure 6-31: Configuration standard IP access control list

3. Increase Expand MAC Access Rules

Click "New ACL Rules" , select "Configuration Expand MAC ACL" in the pop-up window, in list ID: 20,ACE ID: 0,Rules "Deny"、Source MAC address: 0088.9999.999A

Destination MAC address is the random MAC。MAC protocol type: 0x0086. After the configuration is complete, click "Save":

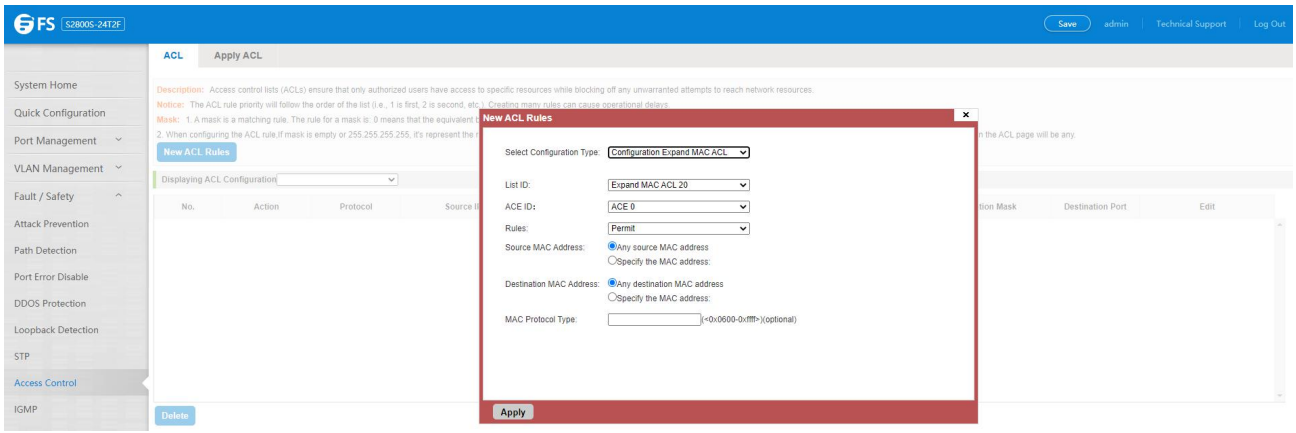


Figure 6-32: Configuration extended MAC access control list

Configuration instructions:

ACE ID is an optional rule. Do not fill: the default is 0;

The extended IP protocol access control list, type: TCP, UDP, IP.

6.6.1.3 Modify Configuration

Rules for modifying port applications

Select the rules to be replaced, click " ", enter the modified ACL rules page, the rules are: "Deny", click "Save":

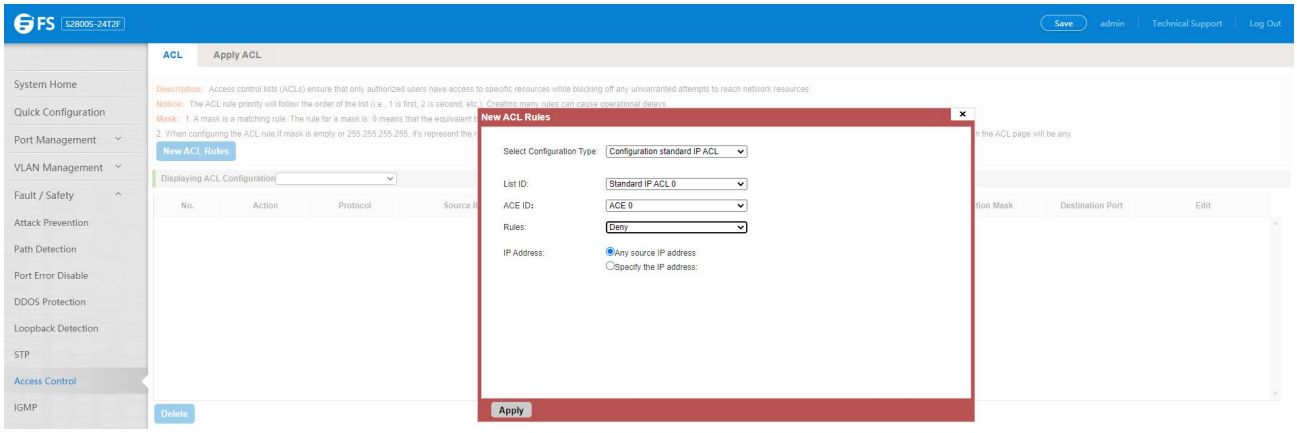


Figure 6-33: To modify the ACL rule

Configuration instructions

The modified extended MAC and extended IP for the same operation.

6.6.1.4 Delete Rule

To delete the rule, click "X" to delete the current list of ACE under a ACL rule:

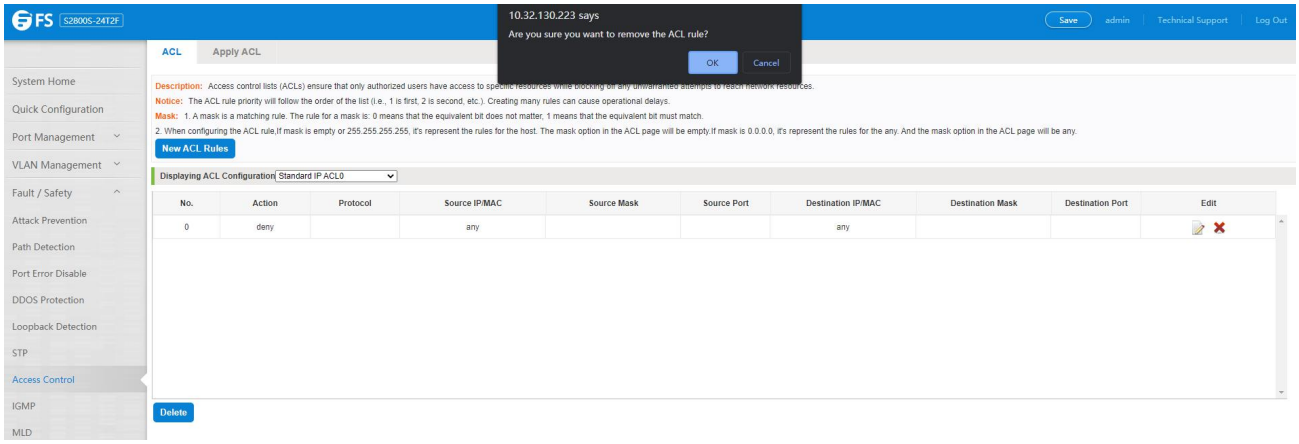


Figure 6-34: Delete rules

Remove all of the ACE rule table under ACL, click "Delete":

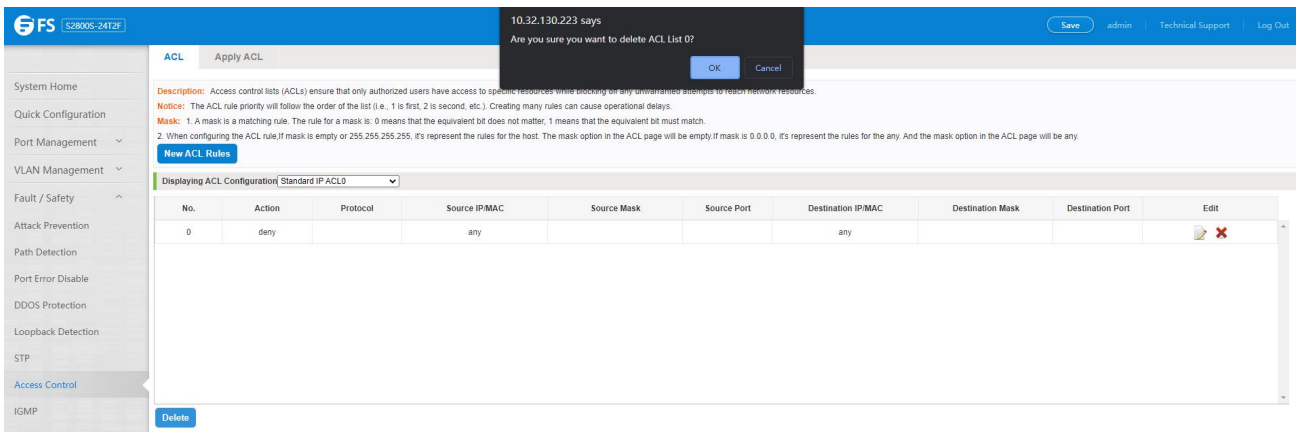


Figure 6-35: Delete ACL rules

Configuration instructions

Delete - after the success of the kneeling in port configuration table deleted together.

6.6.2 Application ACL

6.6.2.1 View Application ACL

The configuration information and click on the "Fault/Safety" "Access Control" "Apply ACL" can view access control using ACL:

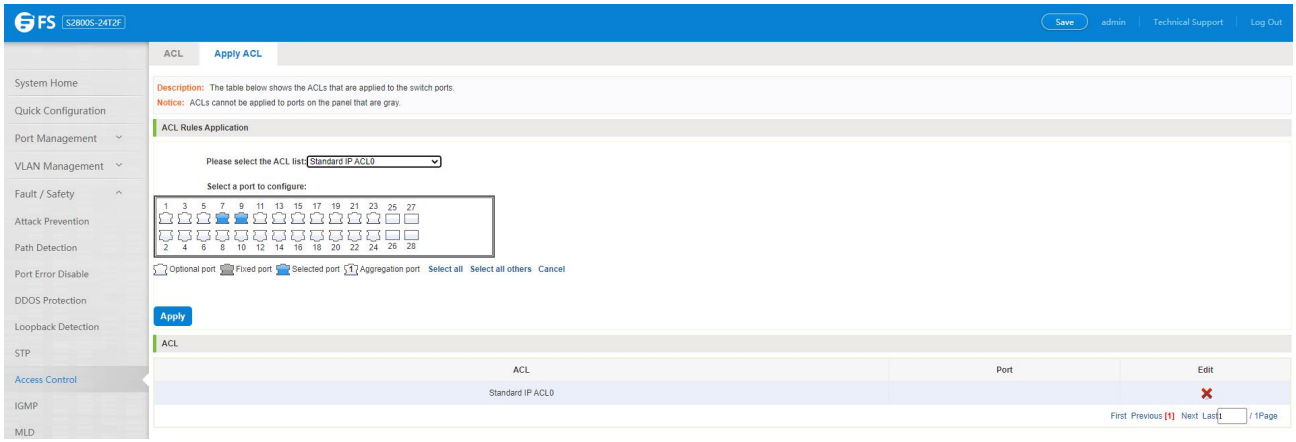


Figure 6-36: View application ACL rules

6.6.2.2 Increased Application ACL

Select the rules that need to be applied, then select the port of application, click "Save" to complete the configuration:

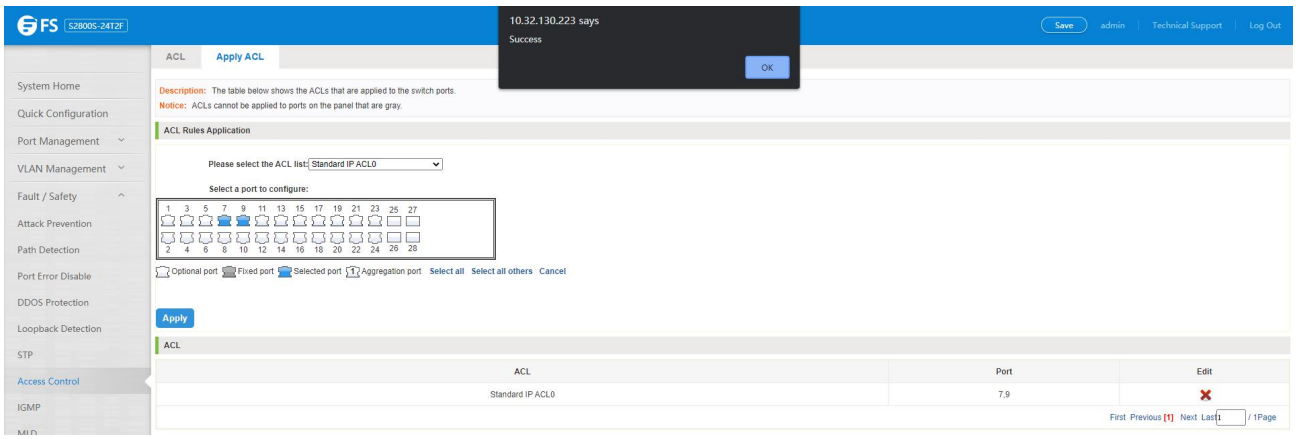


Figure 6-37: Add applications ACL

6.6.2.3 Delete Application ACL

Click to delete the application rule on the right side, cancel the application of the rules in the port:

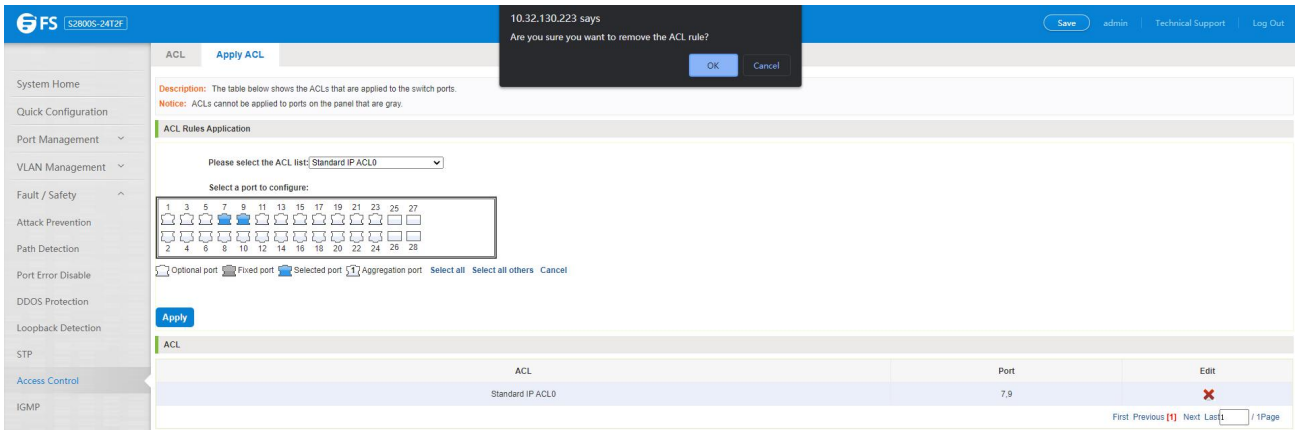


Figure 6-38: Delete application ACL

6.7 IGMP Snooping

6.7.1 IGMP Snooping

6.7.1.1 View IGMP Snooping Configuration

Click the "Fault/Safety" "IGMP Snooping" to check the current switch configured multicast monitoring information:

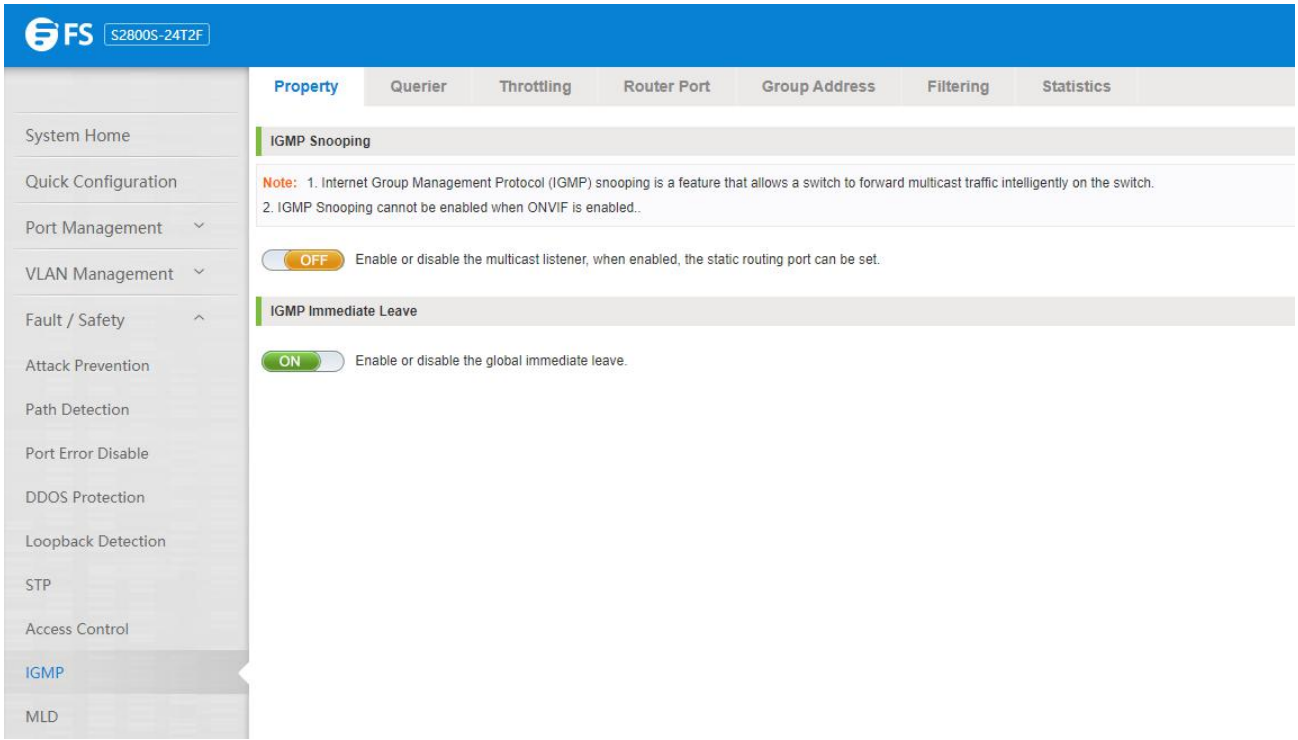


Figure 6-39: View snooping IGMP configuration information

6.7.1.2 Action Multicast Listener Function

Click the "Fault/Safety" "IGMP Snooping", click "OFF" button to activate the multicast monitoring function:

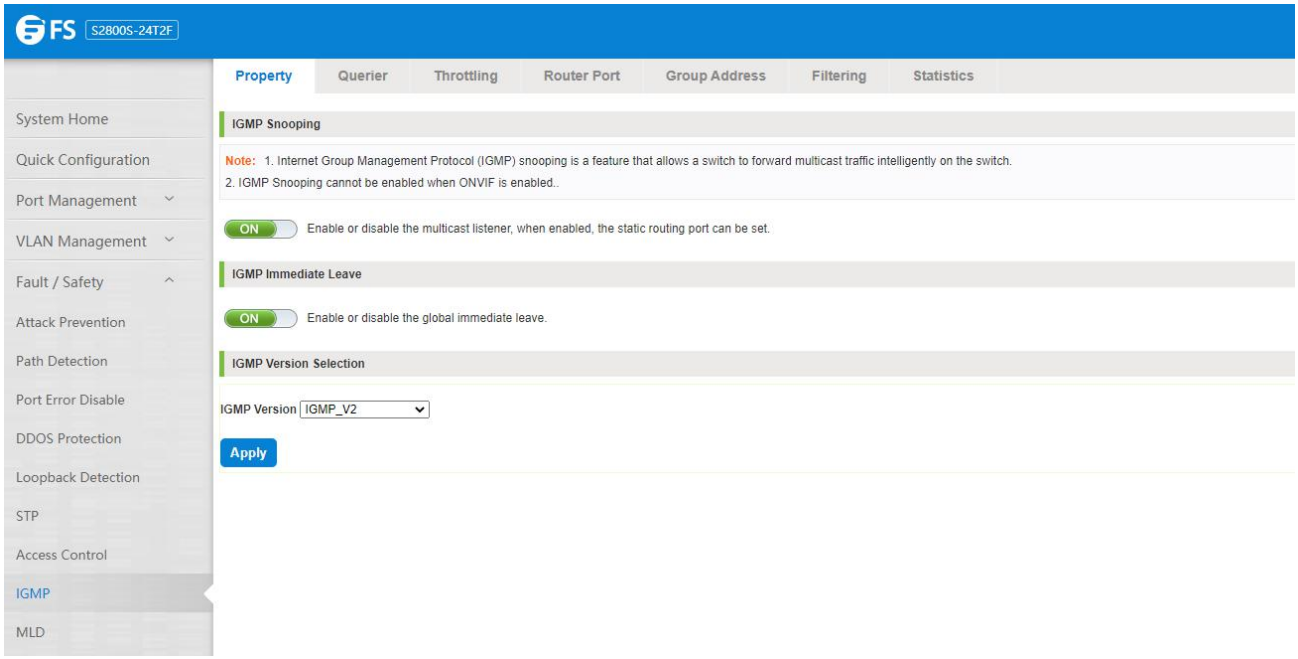


Figure 6-40: Open multicast listener configuration

The default multicast listener (IGMP Snooping) did not open;

The default on multicast listener (IGMP Snooping), all VLAN are open;

The default version of V2 - IGMP.

6.7.1.3 Disable Multicast Listener Function

Click the "Fault/Safety" "IGMP Snooping", click "ON" button to disable multicast monitoring function:

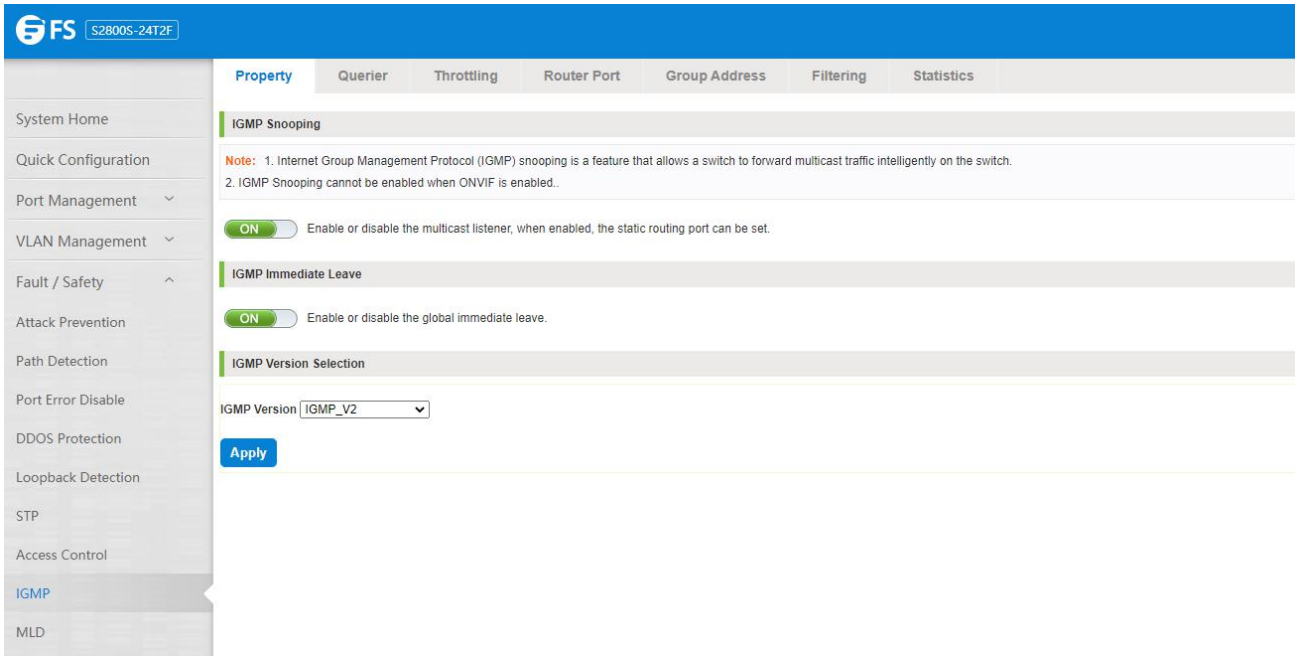


Figure 6-41: Closed multicast listener function operation

6.7.1.4 Configuration Multicast Routing

Select VLAN, click "Router Port Add" button, to configure the multicast routing in the port panel:

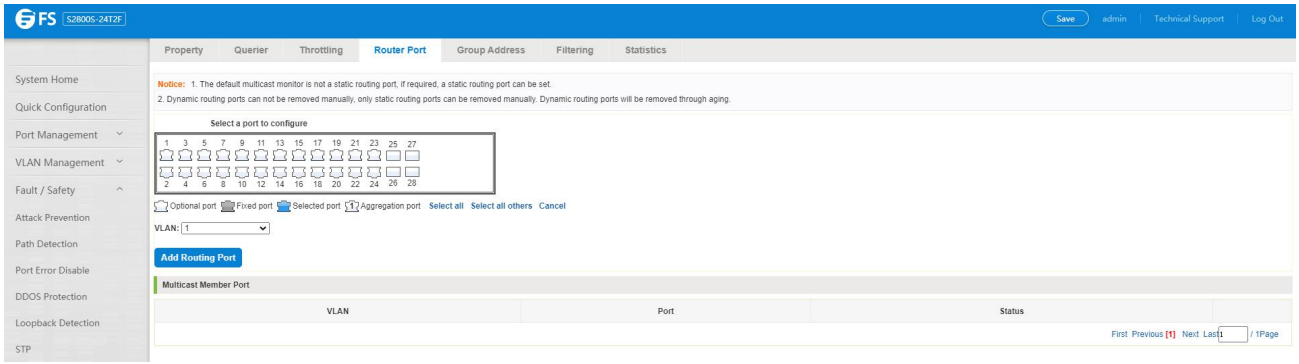


Figure 6-42: Configuration of multicast routing

Multicast routing configuration Steps are as follows:

Step 1: In the port panel to select multicast listener routing port;

Step 2: Select VLAN;

Step 3: Click on the "Add Router Port" button to complete the configuration.

6.7.1.5 IGMP Version

Click the "Fault/Safety" "IGMP Snooping", set the IGMP version of the page:

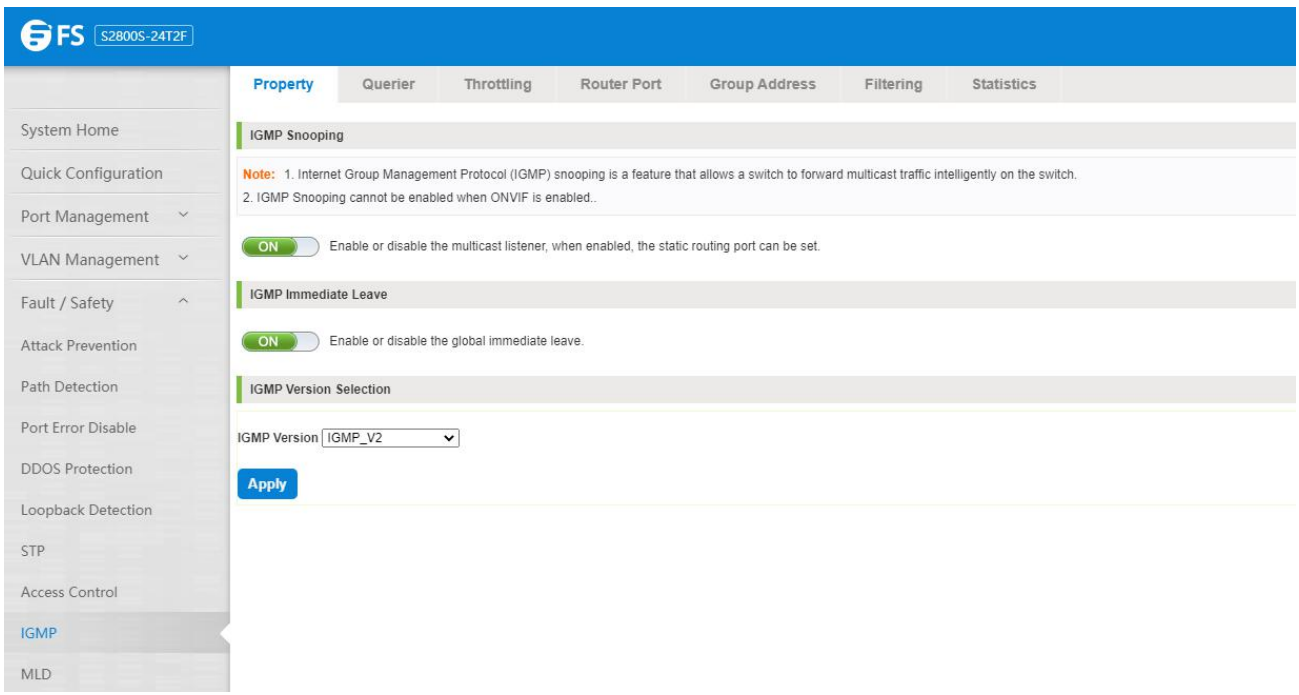


Figure 6-43: Configuration IGMP version

IGMP version configuration Steps are as follows:

Step 1: Select the required version number;

Step 2: Click the "Save" button to complete the configuration.

6.7.2 MLD

6.7.2.1 View MLD Configuration

Click the "Fault/Safety" to check the current switch configured multicast monitoring information:

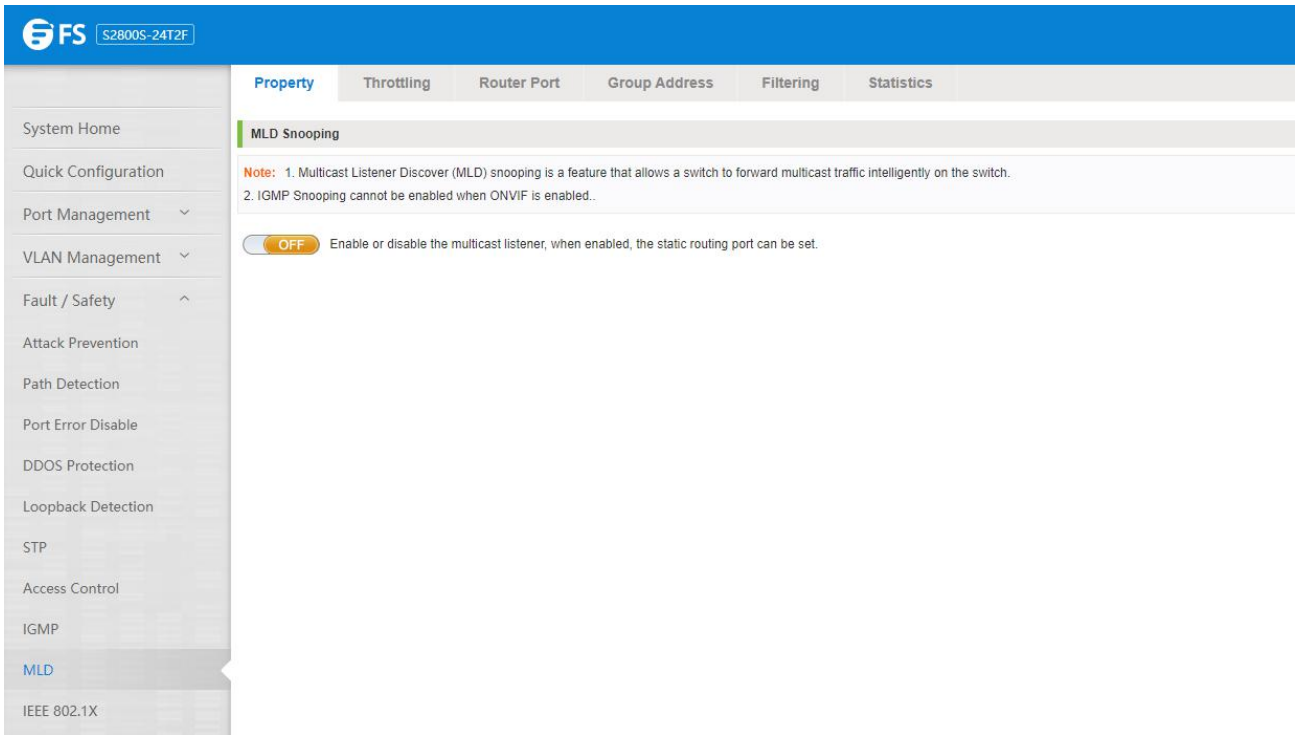


Figure 6-44: View MLD configuration information

6.7.2.2 Active Multicast Listener Function

Click the "Fault/Safety" "MLD", click "OFF" button to activate the multicast monitoring function:

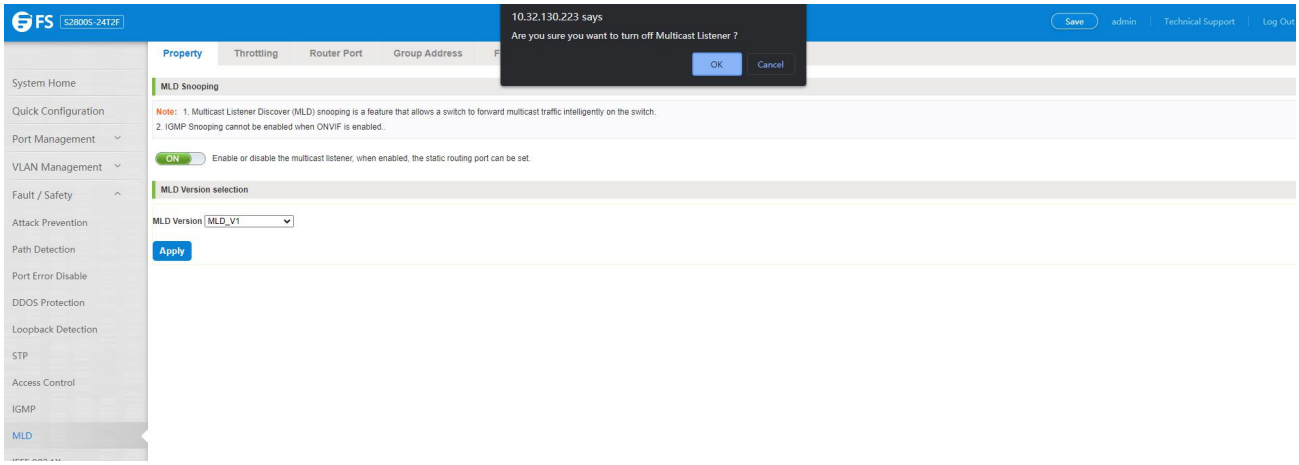


Figure 6-45: Open multicast listener configuration

The default multicast listener (MLD), did not open;

The default on multicast listener (MLD), all VLAN are open;

The default version of V1 - MLD.

6.7.2.3 Disable Multicast Listener Function

Click the "Fault/Safety" "IGMP Snooping", click "ON" button to disable multicast monitoring function:

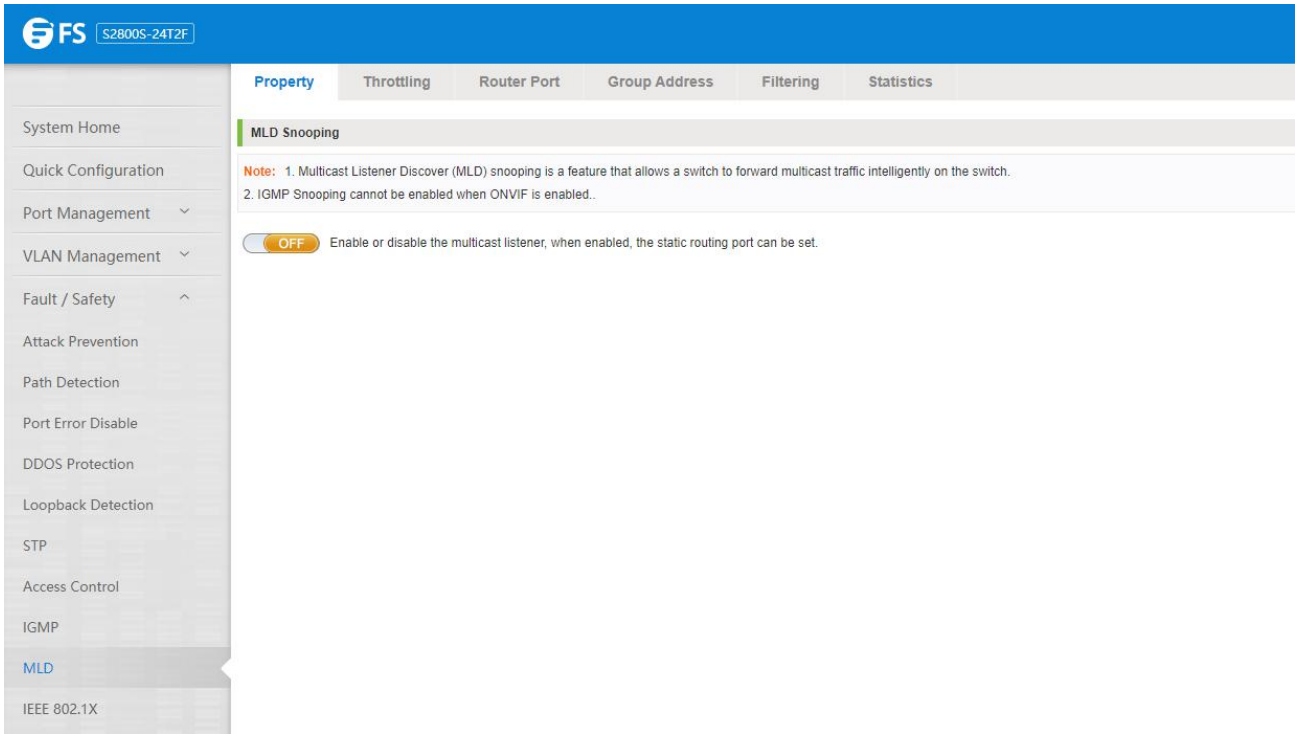


Figure 6-46: Closed multicast listener function operation**6.7.2.4 Configuration Multicast Routing**

Select VLAN, click "Router Port Add" button, to configure the multicast routing in the port panel:

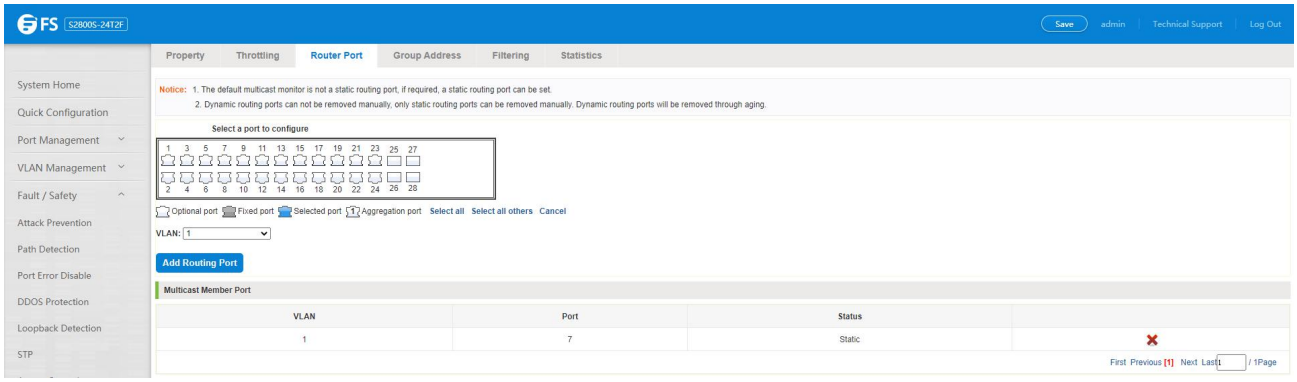


Figure 6-47: Configuration of multicast routing

Multicast routing configuration Steps are as follows:

Step 1: In the port panel to select multicast listener routing port;

Step 2: Select VLAN;

Step 3: Click on the "Add Router Port" button to complete the configuration.

6.8 IEEE 802.1X

IEEE 802.1X is a port-based authentication protocol, is a method and strategy for authenticating users.

Configure the PC 10.32.130.253, and connect with switch by Gi 0/2.

Configure the radius sever 10.32.130.254, and connect with switch by Gi 0/1.

Click ON “Fault/Safety" "IEEE 802.1X".

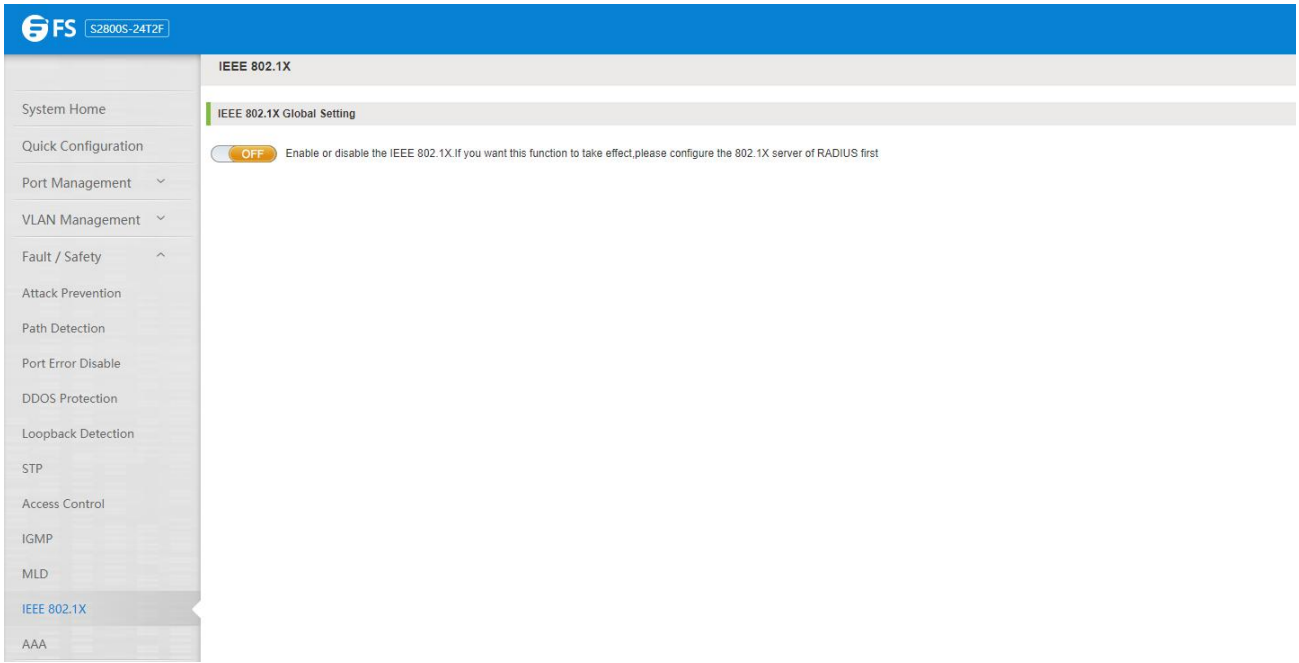


Figure 6-48: IEEE 802.1X

Click to OPEN

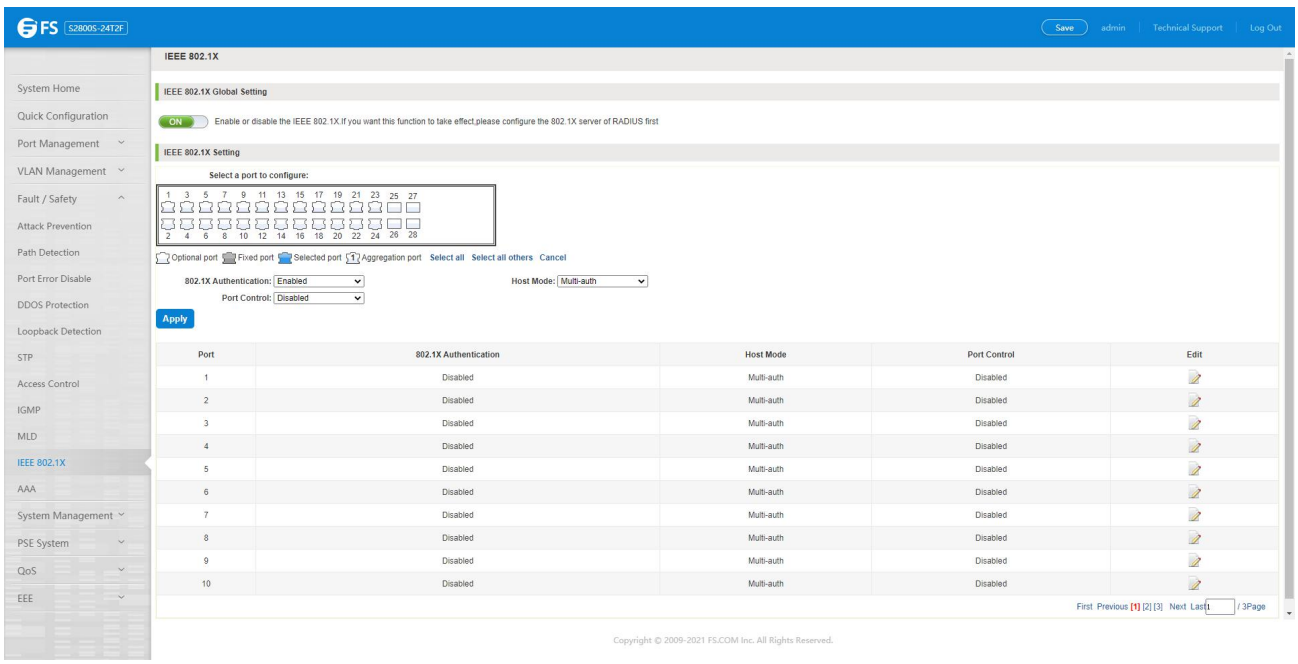


Figure 6-49: Enable IEEE 802.1X

Switch Configuration AAA RADIUS Server Address: 10.32.130.254

Auth Port: 1812

Key: 123

type: all

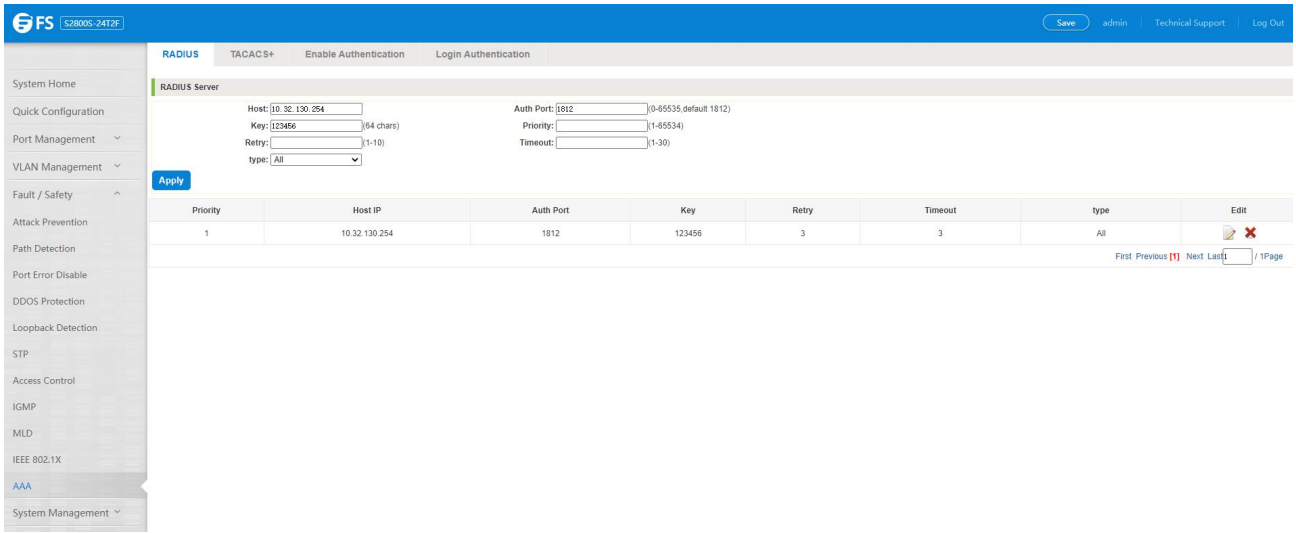


Figure 6-50: Configuration radius

Switch Enable 802.1X port Gi 0/2

Port Control: auto

Host Mode: multi-auth

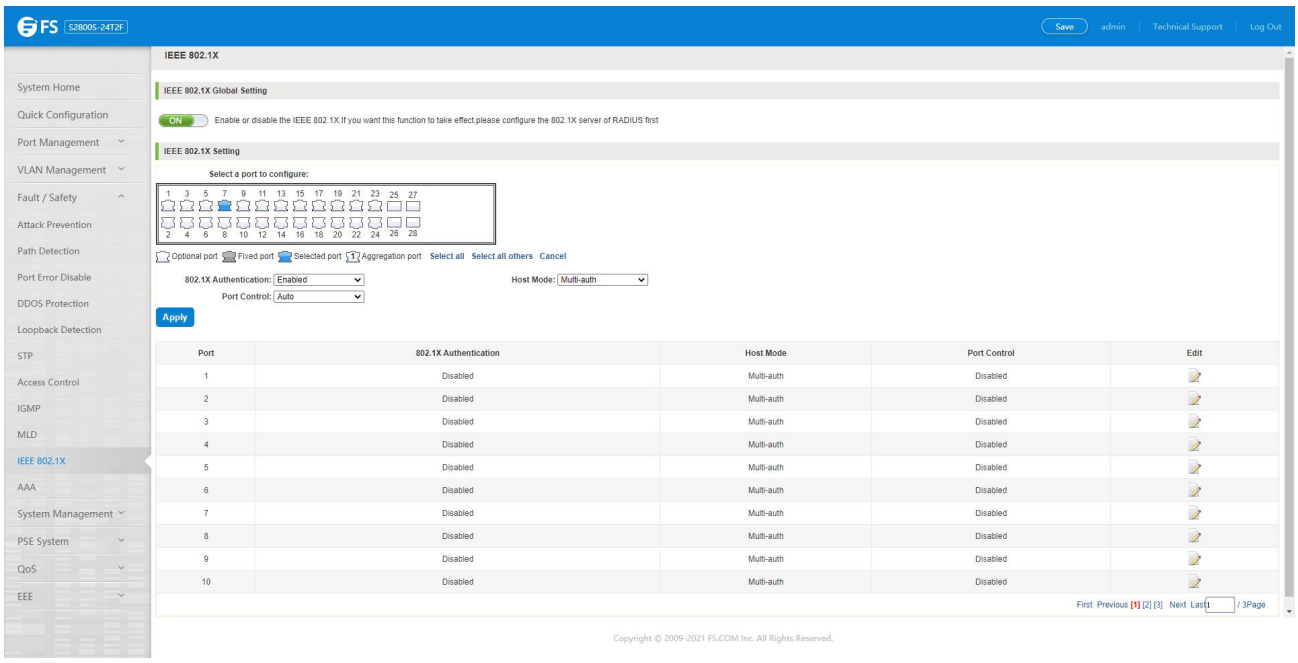


Figure 6-51: Configuration IEEE802.1X

Tips: The IEEE802.1x function is used with the AAA function.

Auto: It indicates that the initial state of the port is unauthorized. It only allows EAPOL packets to be sent and received. It does not allow users to access network resources. If the authentication passes, the port switches to the authorized state, allowing the user to access the network resources. This is also the most common case.

Force-auth: Indicates that the port is always authorized, allowing users to access network resources without authorization.

Force-unauth: Indicates that the port is always in an unauthorized state and does not allow the user to authenticate. The device does not provide authentication services to clients that pass through the port.

Single-host: This port can only connect to a host, through authentication can be forwarded for data packets.

Multi-auth: This port can be connected to the following switches, including a host through the certification, other hosts can be forwarded data packets.

Multi-host: This port can be connected to the following switches, including a host through the certification, other host data packets can not be forwarded, must also have passed authentication.

6.9 AAA

6.9.1 RADIUS

Enabled and logged in can use radius authentication

Configure the PC 10.32.130.253., and connect with switch by Gi 0/2

Configure the radius sever 10.32.130.254, and connect with switch by Gi 0/1

Click ON “Fault / safety" "AAA" “RADIUS”

Switch Configuration AAA RADIUS server address: 10.32.130.254,

Auth Port: 1812

Key: 123

type: all

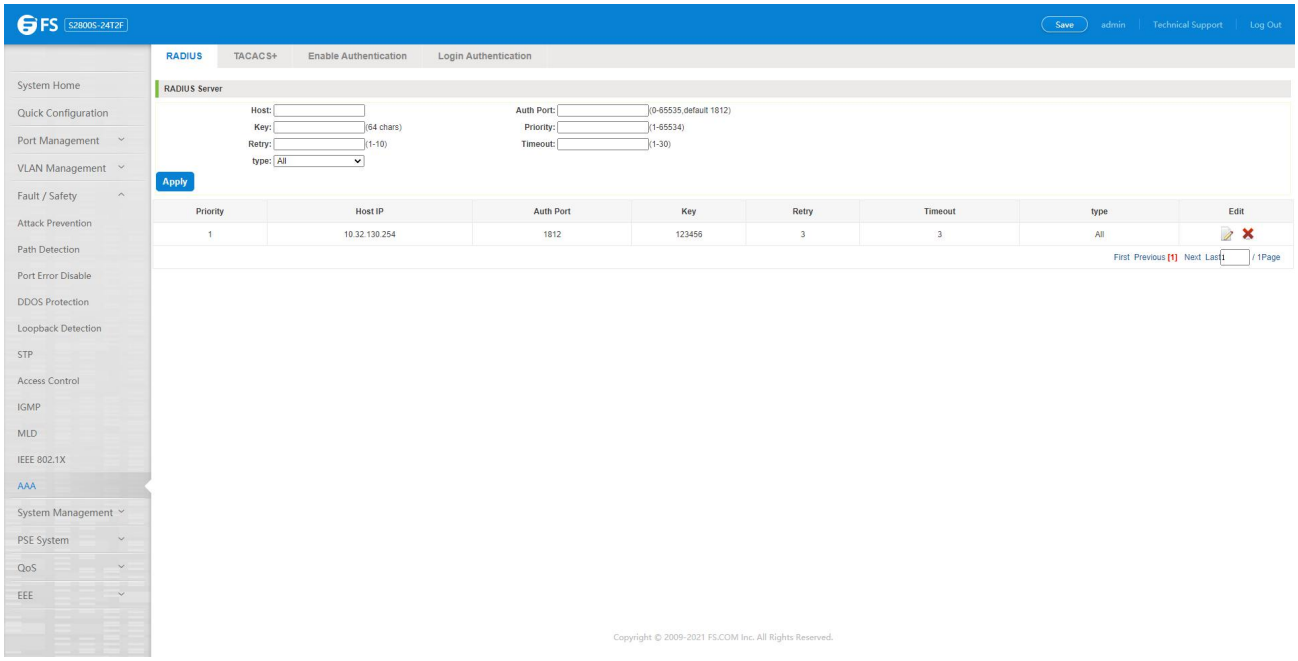


Figure 6-52: Configuration radius

Switch Config Method List:

Name: test

Method 1: RADIUS

Click save.

Switch Config Enable Authentication:

Console: S2800S

Telnet: S2800S

SSH: S2800S

Click save.

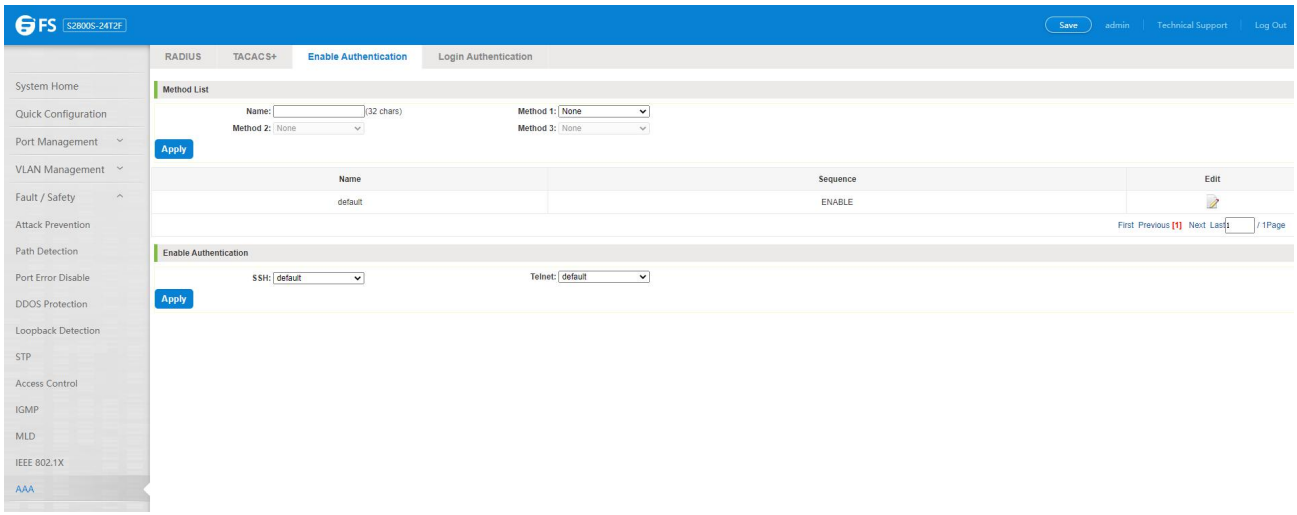


Figure 6-53: configuration enable authentication

Switch Config Method List:

Name: S2800S

Method 1: RADIUS

Click save.

Switch Config Enable Authentication:

Console: S2800S

Telnet: S2800S

SSH: S2800S

Click save.

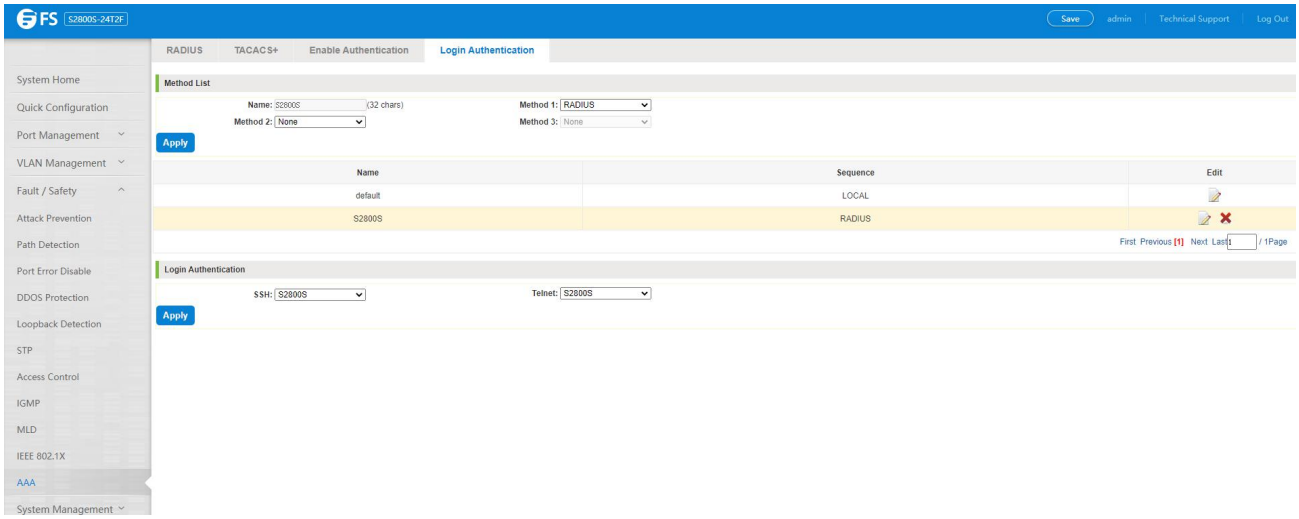


Figure 6-54: Configuration login authentication

TIPS:

1. PC input right username and password, PC can console, telnet and SSH switch

2. PC input right password, user can join "# mode"

7. System Management

7.1 System Settings

7.1.1 Management VLAN

7.1.1.1 Configuration Basic System Settings

Click on the navigation bar "System Management" "System Settings" " Management VLAN" to view the management address of the current switch configuration information:

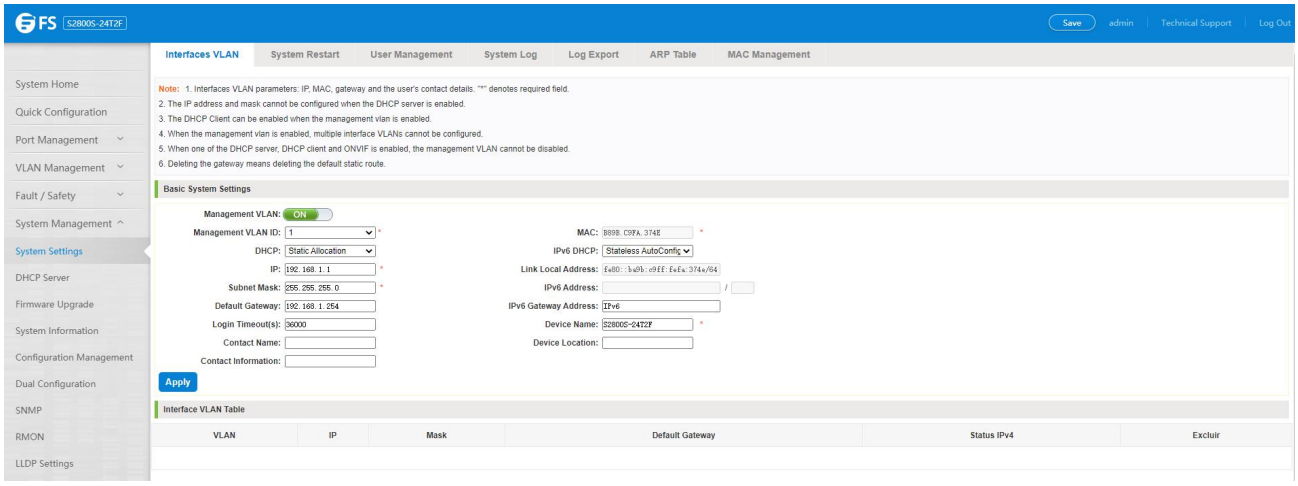


Figure 7-1: Basic system settings

To configure the switch Basic System Settings as follows:

Management VLAN: switch management VLAN ID, the default is 1

1. In the DHCP text box, choose static allocation.
2. In the Management IP text box, enter the IP address, such as 192.168.1.1.
3. In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.0.
4. In the Gateway Address text box to enter the gateway address, such as 192.168.1.254.
5. In the Device Location text box, enter the Device Location.
6. In the Contact Name text box, enter the Contact Name, such as john.
7. In the Contact Information text box, enter Contact Information, such as 12345678900.
8. Click on "Save Settings" button to complete the configuration.

7.1.1.2 System Time Synchronization

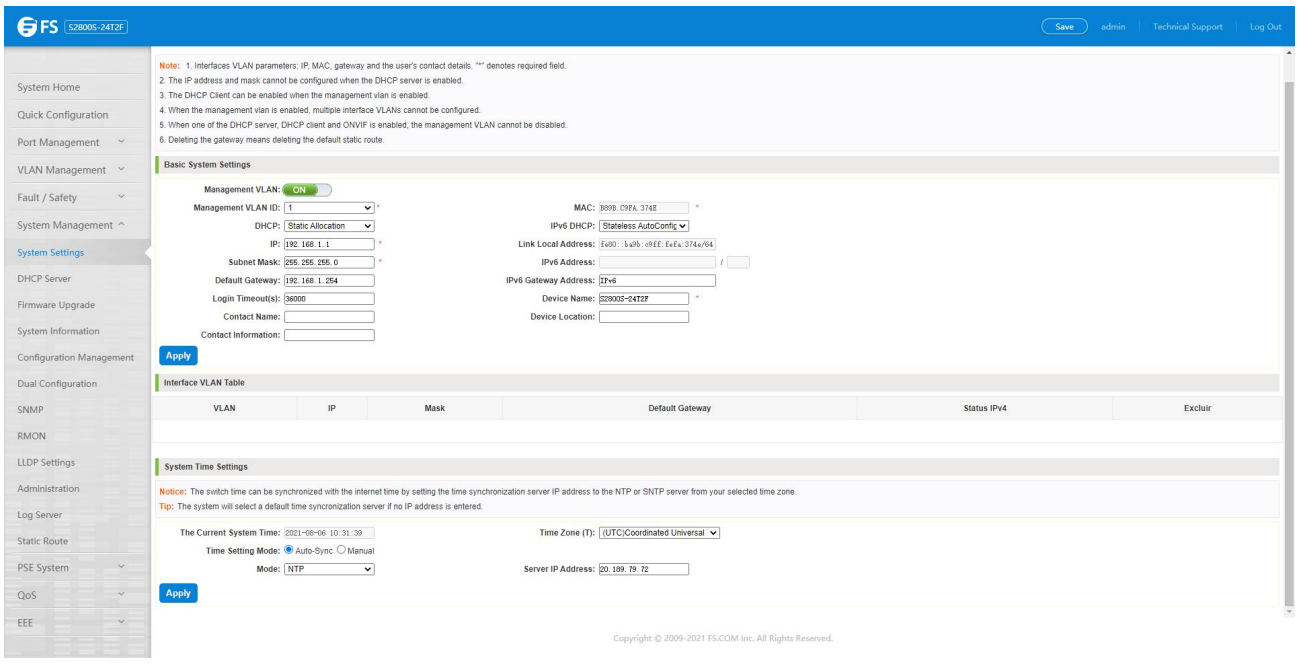
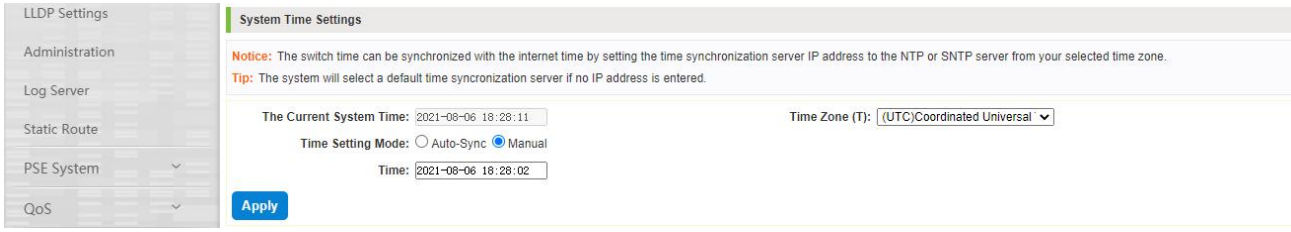


Figure 7-2: System time synchronization

To configuration system time, You can select NTP or SNTP, enter SNTP/NTP Server IP Address such as 20.189.79.72 (local SNTP/NTP servers or internet SNTP/NTP servers), in the Time Zone (T) text box, you can choose any time zone you want, such as UTC+08: 00.

The user can manually configure the device system time.



7.1.1.3 Telnet

After enabling telnet, you can telnet to manage the device

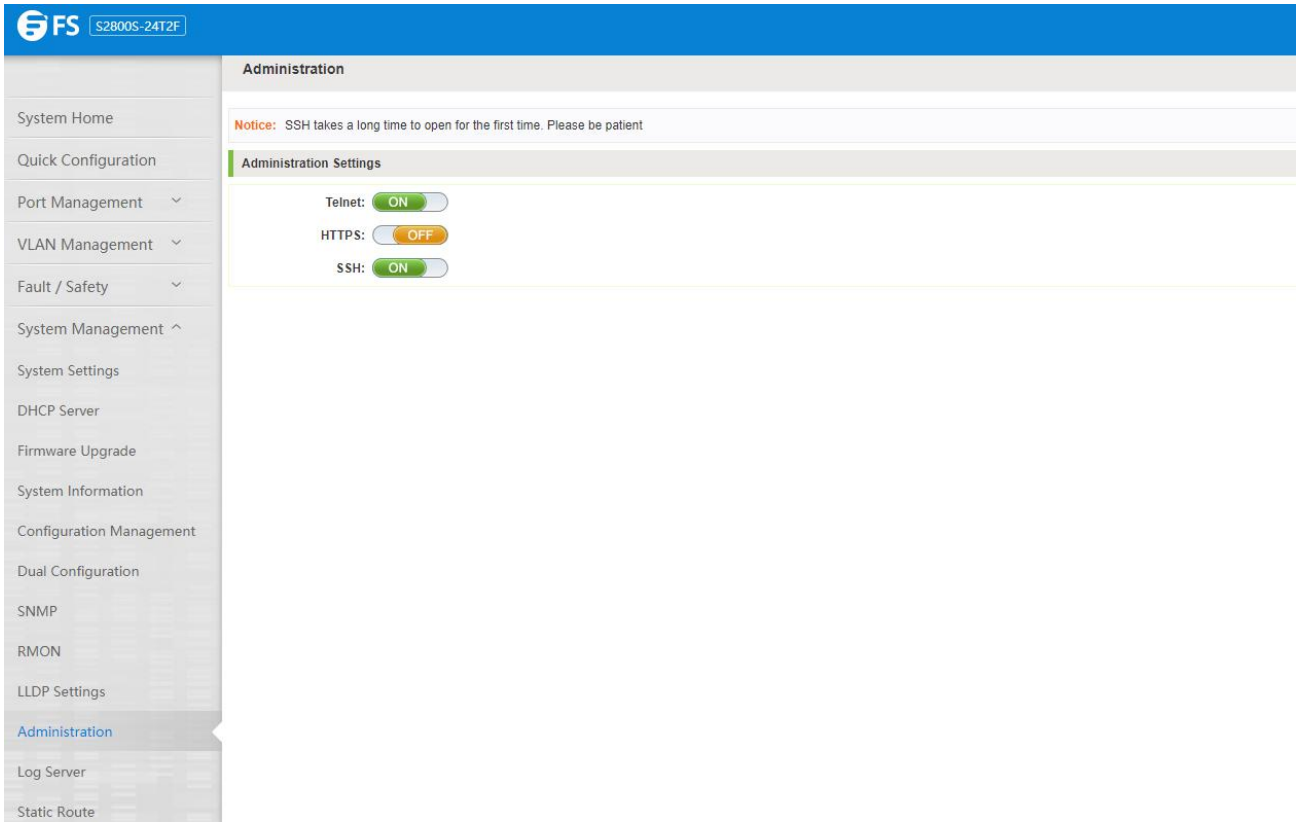


Figure 7-3: Telnet

7.1.1.4 SSH

After enabling SSH, you can use SSH to manage the device more securely

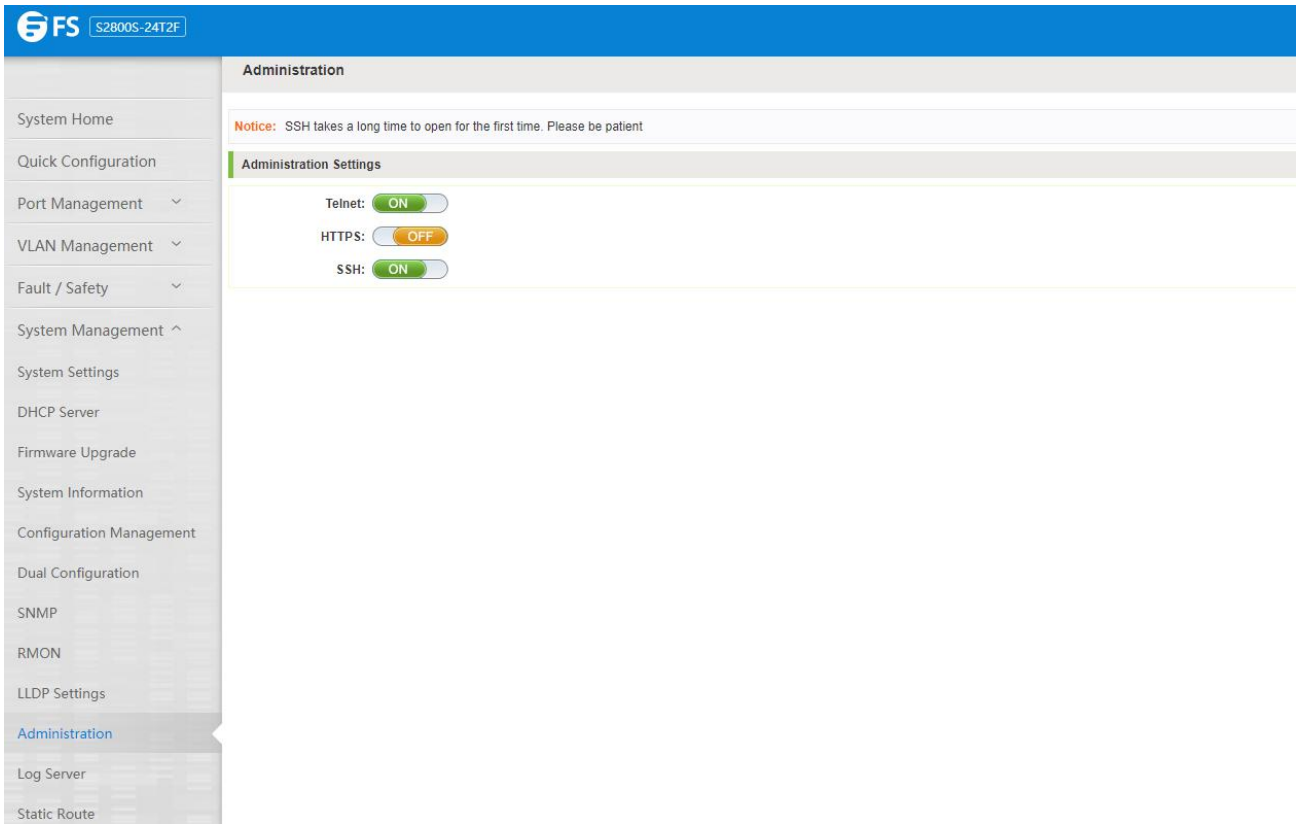


Figure 7-4: SSH

7.1.1.5 DHCP Server

Click on the navigation bar "System Management" "System Settings" "DHCP Server" to configure the switch DHCP server:

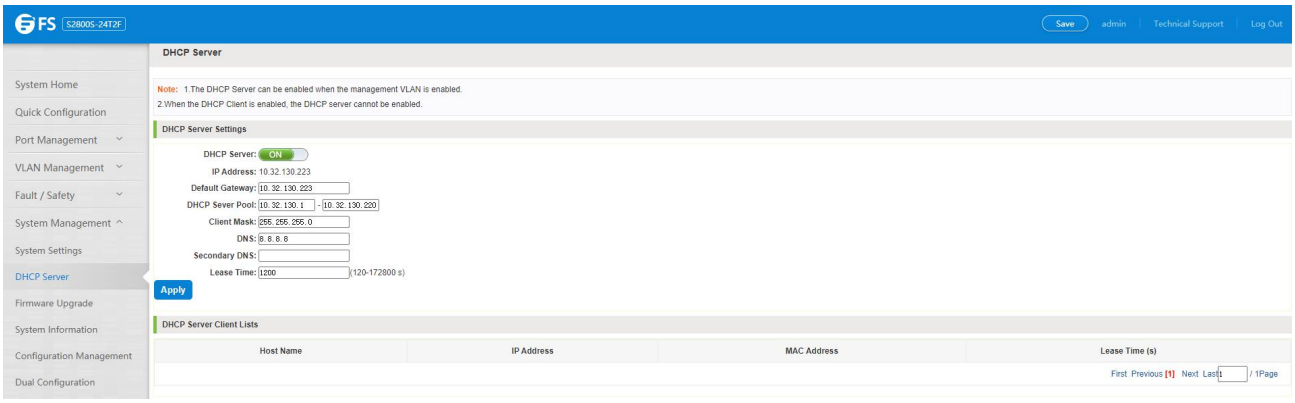


Figure 7-5: DHCP Server

DHCP server configuration, follow these Steps:

Step 1: In the DHCP server, choose enable;

Step 2: In the DHCP client range, configure the server IP.

7.1.2 System Restart

Click on the navigation bar "System Management" "System Settings" "System Restart" to reboot the switch:

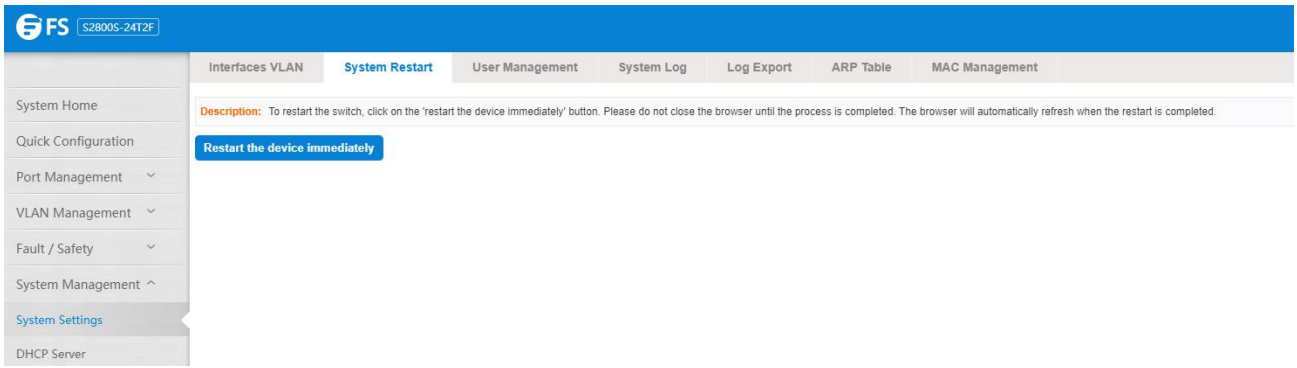


Figure 7-6: System Restart

Restart the device, follow these Steps:

Step 1: Click on "Restart the device immediately" button;

Step 2: Click OK in the box that pops up "OK" button;

Step 3: Prompted to save the current configuration, depending on your need to select "OK" or "Cancel";

Step 4: After the restart the progress bar moves to 100%, reboot the device.

7.1.3 User Management

Click on the navigation bar "System Settings" "User Management" to modify the super user password:

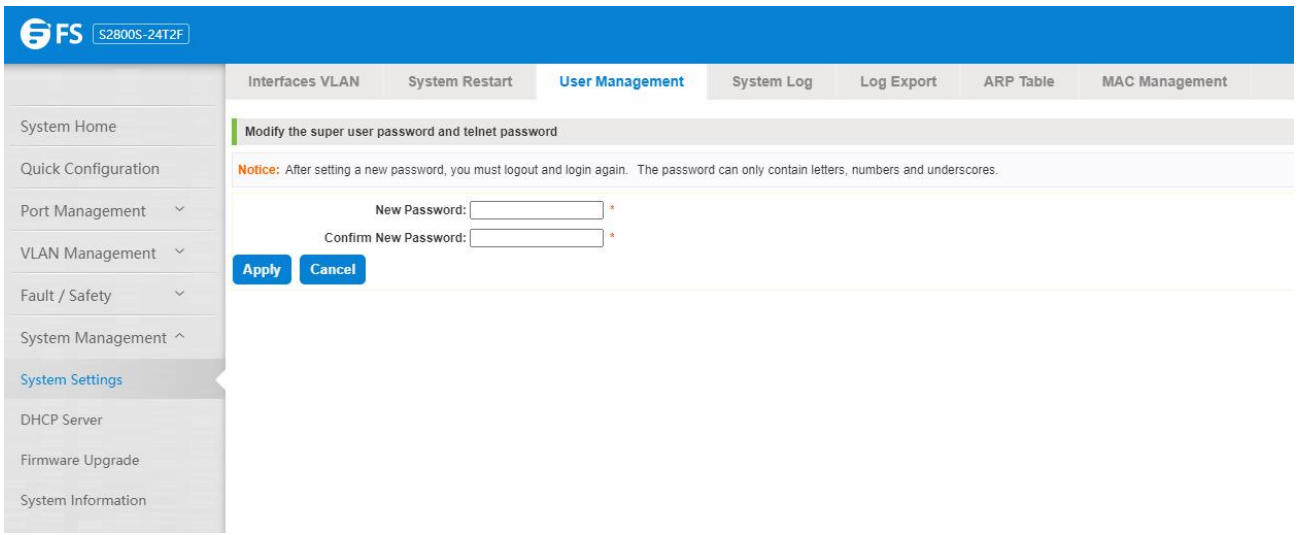


Figure 7-7: Change Password

Change password follow these Steps:

Step 1: Enter the old password: password;

Step 2: Enter the new password: admin;

Step 3: Confirm new password: admin;

Step 4: Click the "Save" button;

Step 5: Pop-up dialog box, click "OK" button.

7.1.4 System Log

Click on the navigation bar "System Management" "System Settings" "System Log" to enter the log management interface, you can query the system log, clear the log:

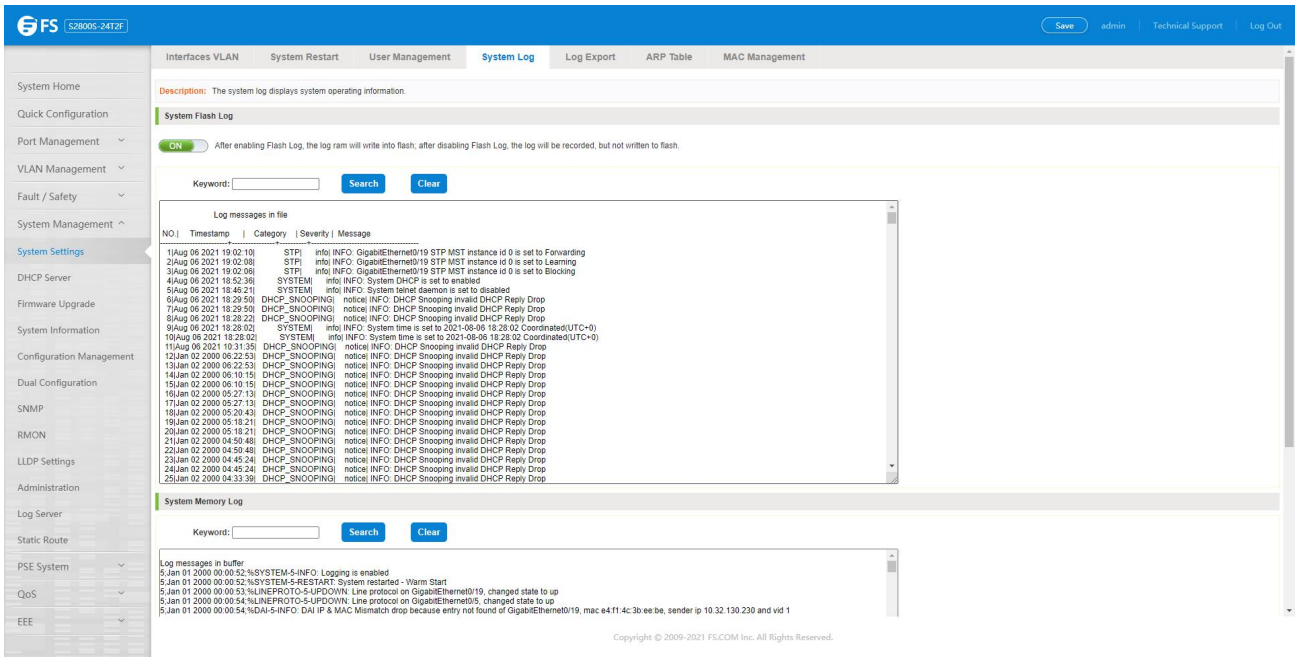


Figure 7-8: System log

Log management system WEB page to view the contents of the command line is consistent with the results of the command show logging; Click "Clear" button to clear the current log information switch.

7.1.5 Log Export

Click on the navigation bar "System Management" "System Settings" "Log Export" to export log information into the interface, you can export the log information through TFTP Server.

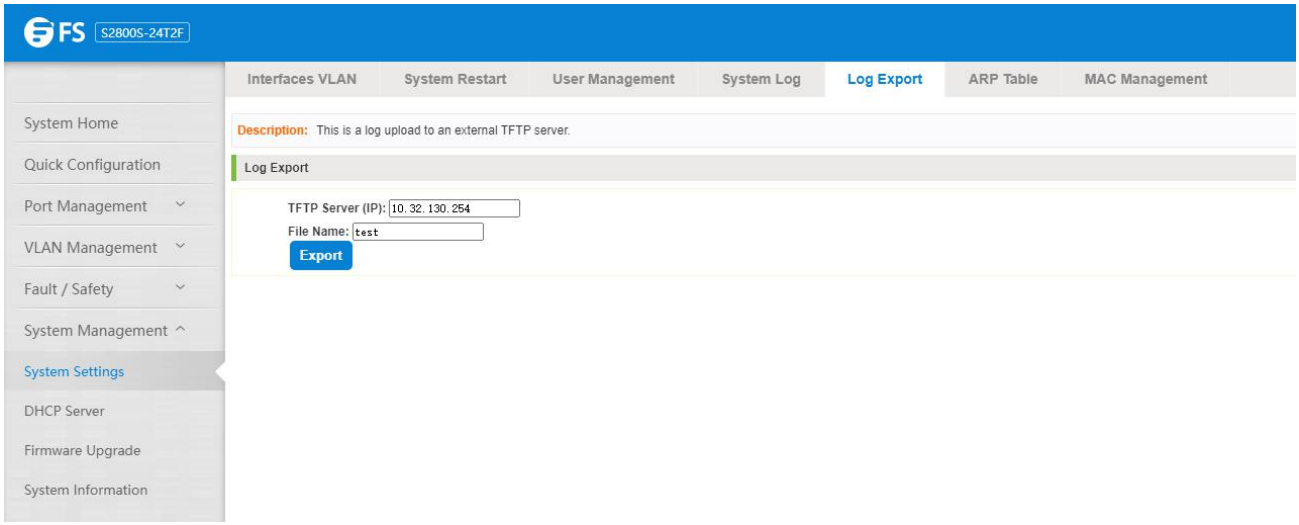


Figure 7-9: Log export

7.1.6 ARP Table

Click on the navigation bar "System Management" "System Settings" "ARP Table" to enter the ARP entry interface, you can view the ARP information:

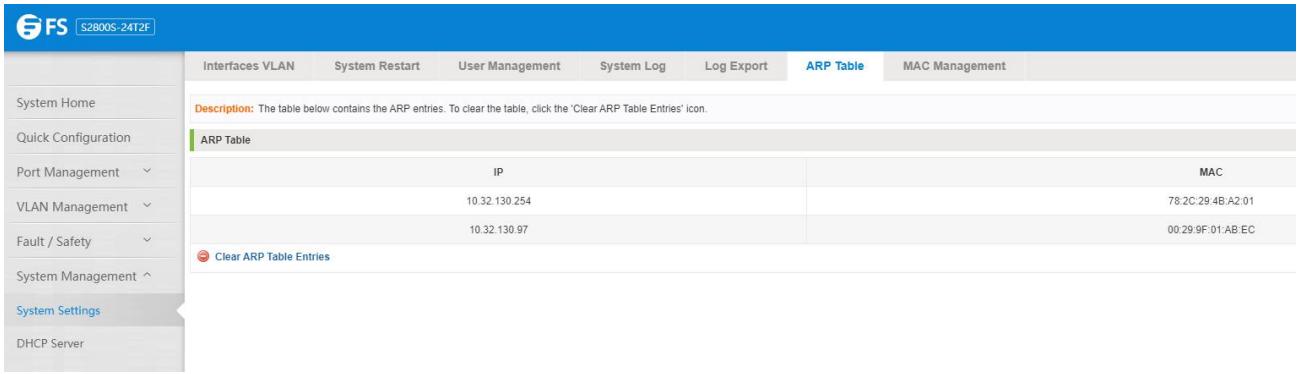


Figure 7-10: ARP message

Click "Clear ARP table entries" button to clear the display ARP information.

7.1.7 MAC Management

7.1.7.1 MAC Address Lookup

Click the "System Management" "System Settings" "MAC Management" can switch MAC address information query:

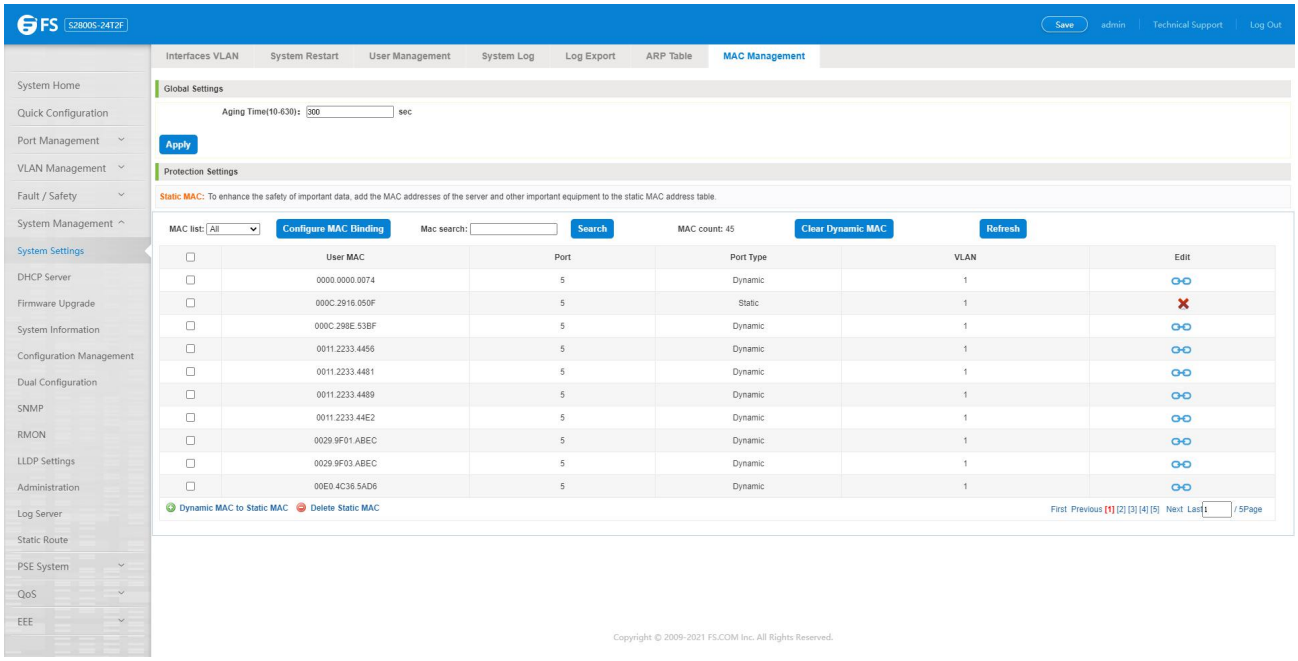


Figure 7-11: MAC address lookup display

In the MAC address list which shows the current switch port to learn MAC addresses:

1. User MAC: MAC address of the switch that currently exists is displayed.

2. Port: Displays the source port number of the MAC address.

3. Port Type: There are two types of dynamic and static.

4. VLAN: VLAN ID display value.

You can query the MAC address type: according to the type of query MAC address, type in the MAC address MAC check list next to the drop-down box Select: All / static / dynamic.

7.1.7.2 Add a Static MAC Address Type

1. Use manual binding MAC address.

Click the "Configure MAC Binding" After, you can configure a static MAC address type in the MAC address configuration area:

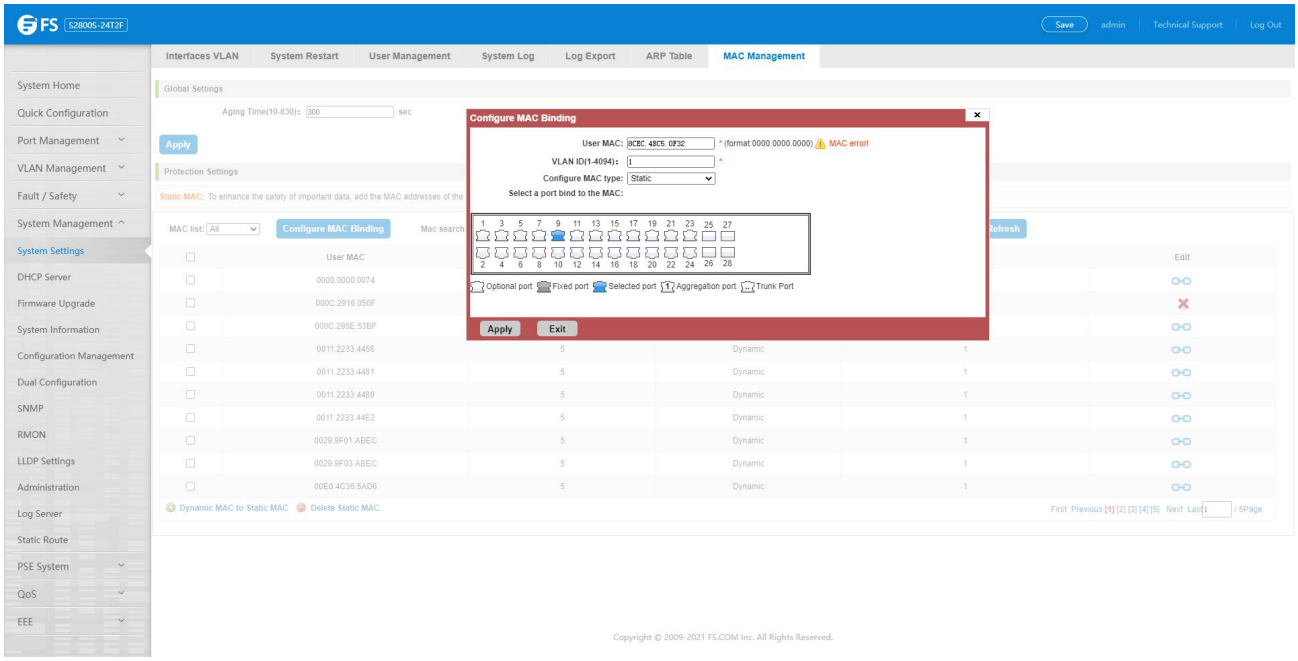


Figure 7-12: MAC addresses statically bound static configuration

Statically typed MAC address configuration Steps are as follows:

Step 1: Click the "Configure MAC Binding" button;

Step 2: In the "User MAC" text box to enter the MAC address, such as 0001.7A4F.74D2;

Step 3: In the "VLAN ID" text box to enter the VLAN ID, such as 1;

Step 4: Select ports in the port panel;

Step 5: Click on "save" to complete the configuration.

2. Use" " Button binding static MAC address.

In the MAC address list, select the MAC address to be bound, click on the left " " Button, to achieve binding:

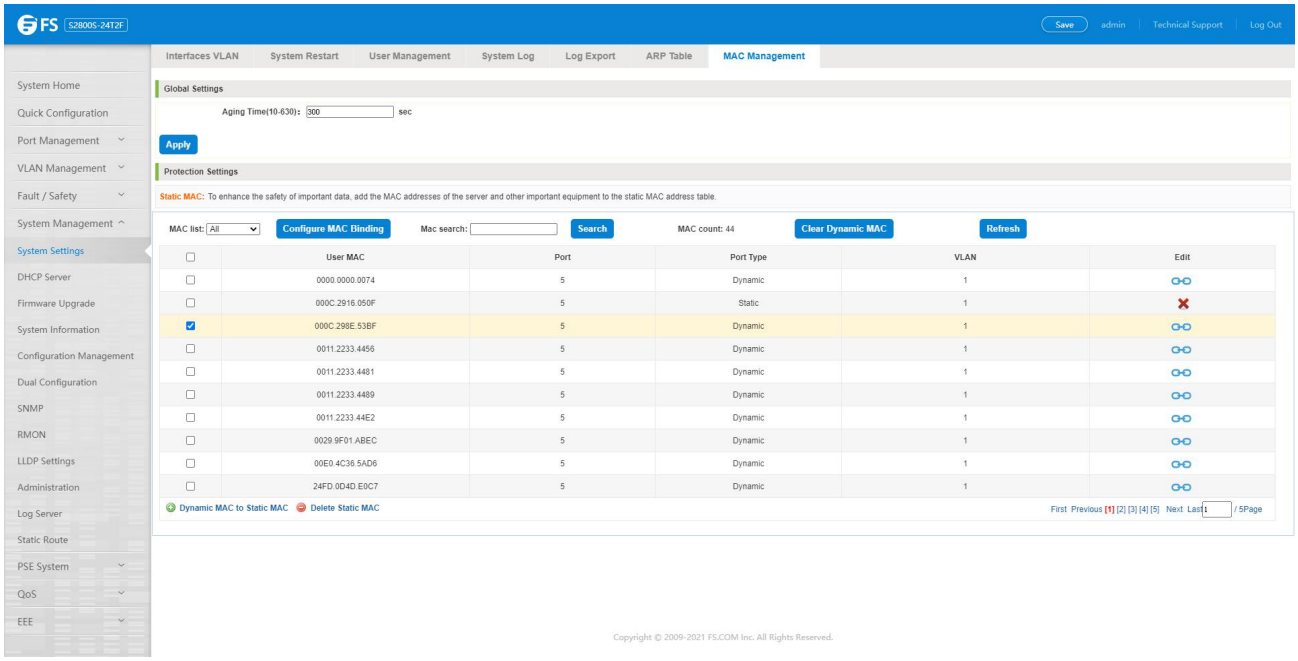


Figure 7-13: MAC address of the static binding configuration

3. Using the "Dynamic MAC to Static MAC" link Bulk Bind static MAC.

In the MAC address list by checking the front of the column you want to bind, "√" check box, click on the "Dynamic MAC to Static MAC" button to complete the configuration:

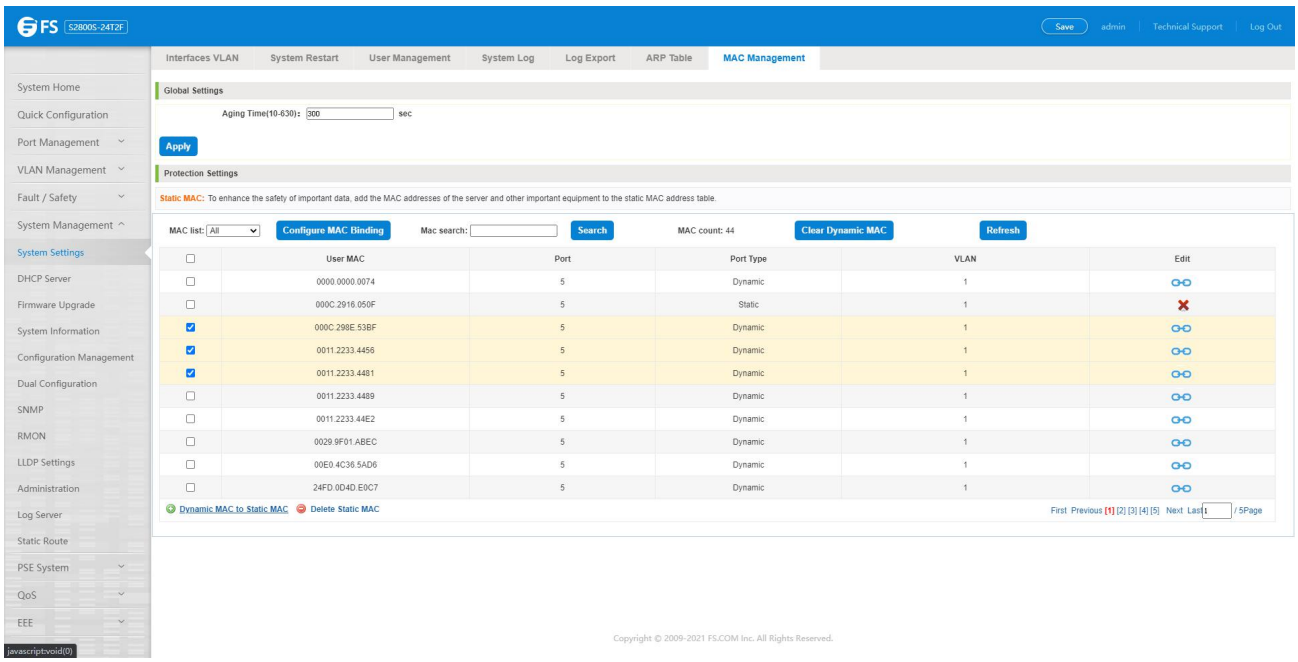


Figure 7-14: Batch-MAC binding configuration

7.1.7.3 Remove the Static MAC Address Type

1. Single MAC records are deleted

Select the need to delete the MAC address, click the "X" button to delete a static MAC address type:

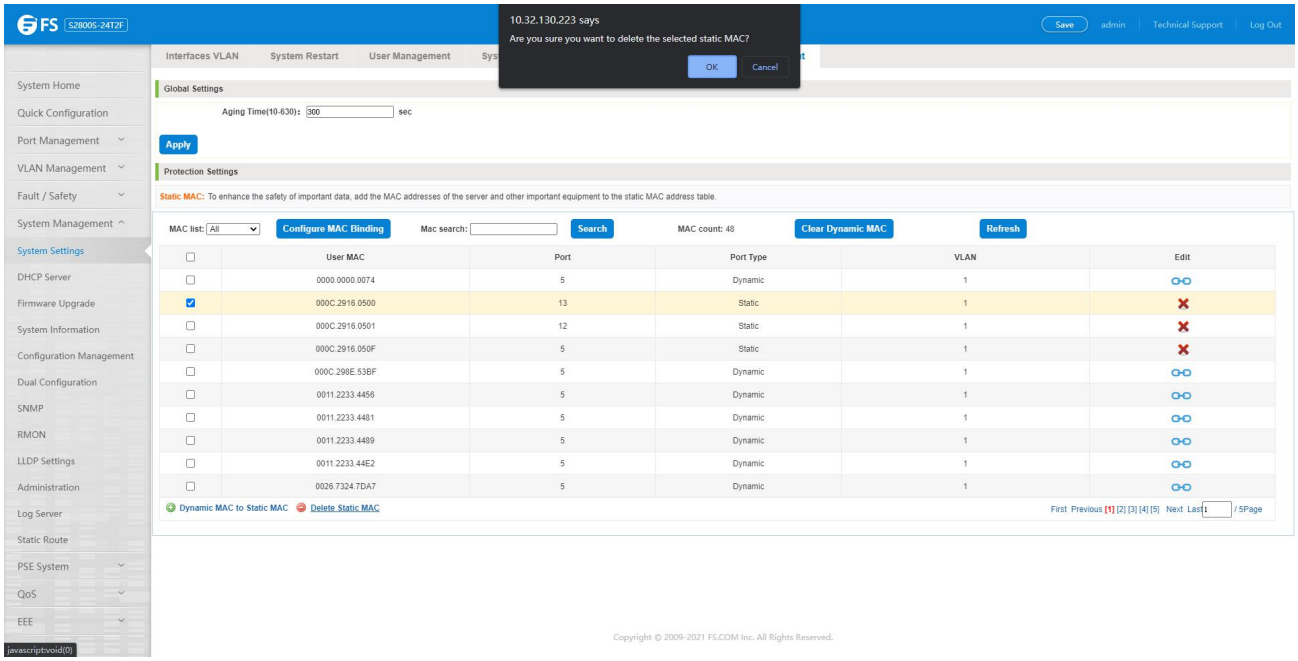


Figure 7-15: MAC address deletion

Remove MAC address configuration Steps are as follows:

Step 1: To delete the selected MAC address;

Step 2: Click" ✖ " button to delete the configuration.

2. Batch delete a static MAC address

In the MAC address list by checking the front of the column you want to bind, "√" check box, click "Delete Static MAC" button:

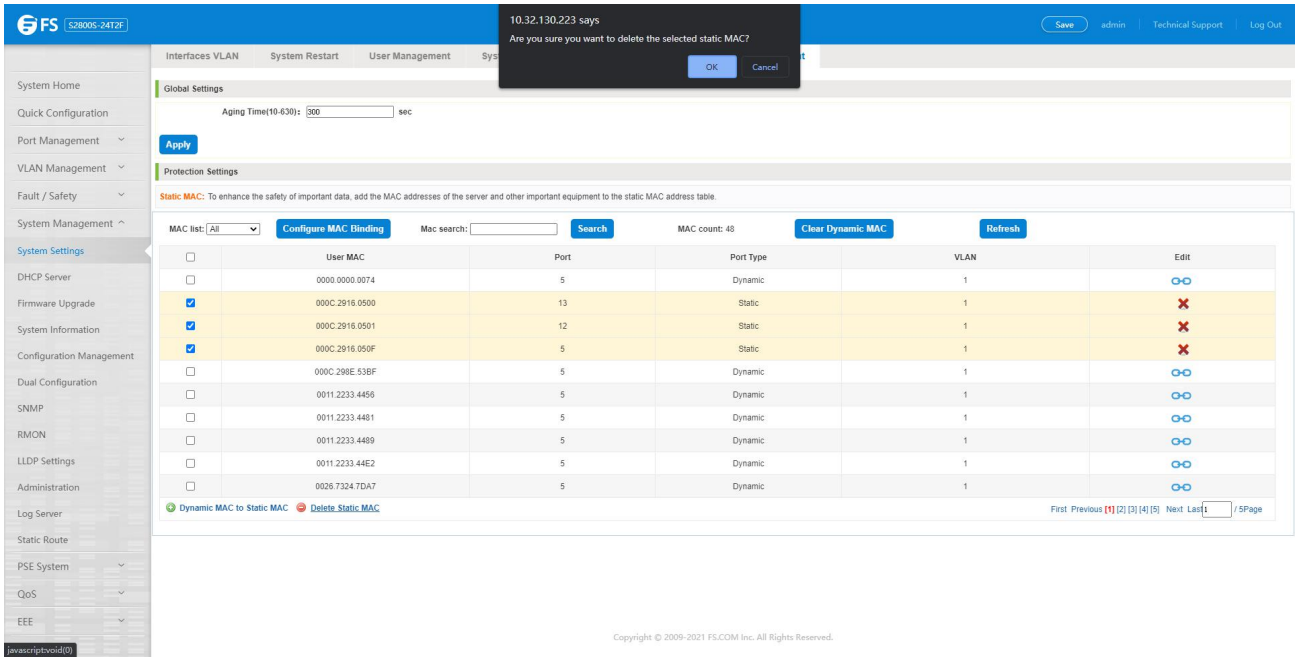


Figure 7-16: MAC address batch deletion

7.2 System Upgrade

Click the "System Management" "System Upgrade" to upgrade the software on the switch:

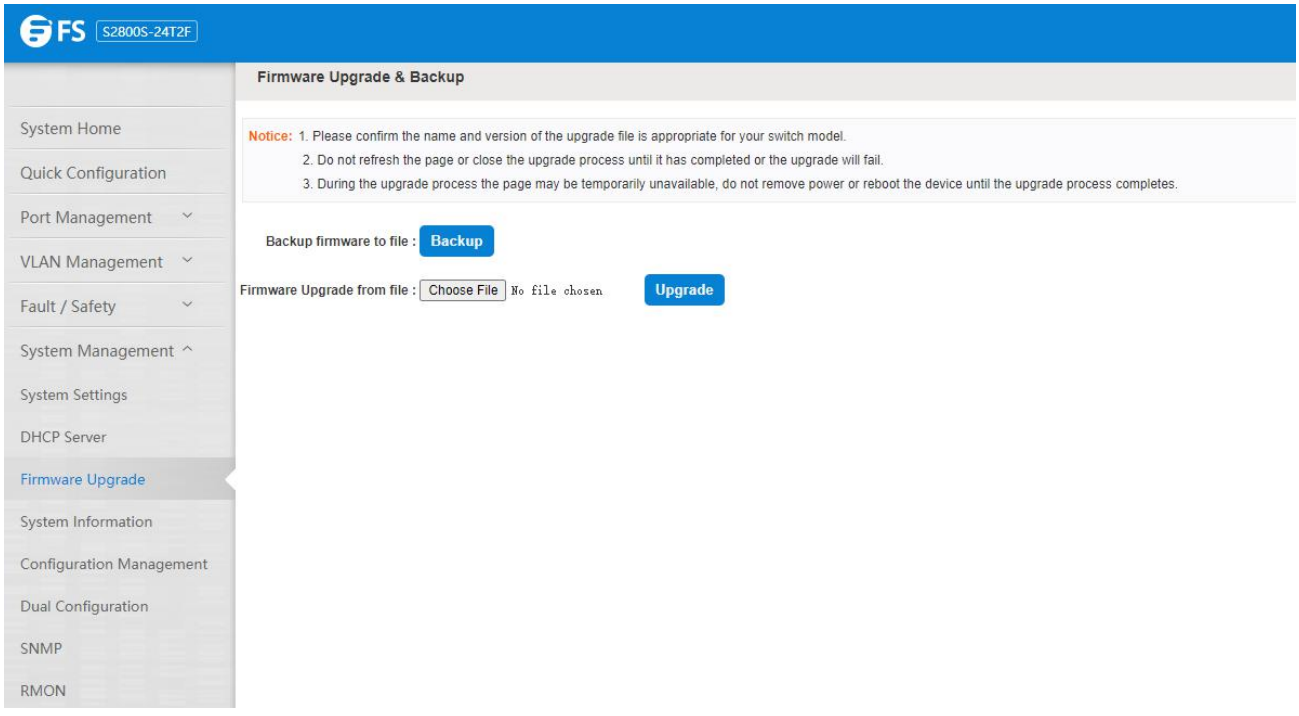


Figure 7-17: Switch System Upgrade

Switch system upgrade Steps are as follows:

Step 1: Click "Choose File" button to select the switch upgrade file;

Step 2: Click the "Upgrade" button switch to start the upgrade new software;

Step 3: When the upgrade progress bar is at 100%, the switch will automatically reboot, completion of the upgrade is completed.

7.3 System information

7.3.1 Memory Information

Click on the "System Management" "System Information" "of" the Memory Information into the Memory Information interface, can view the System Memory Information:

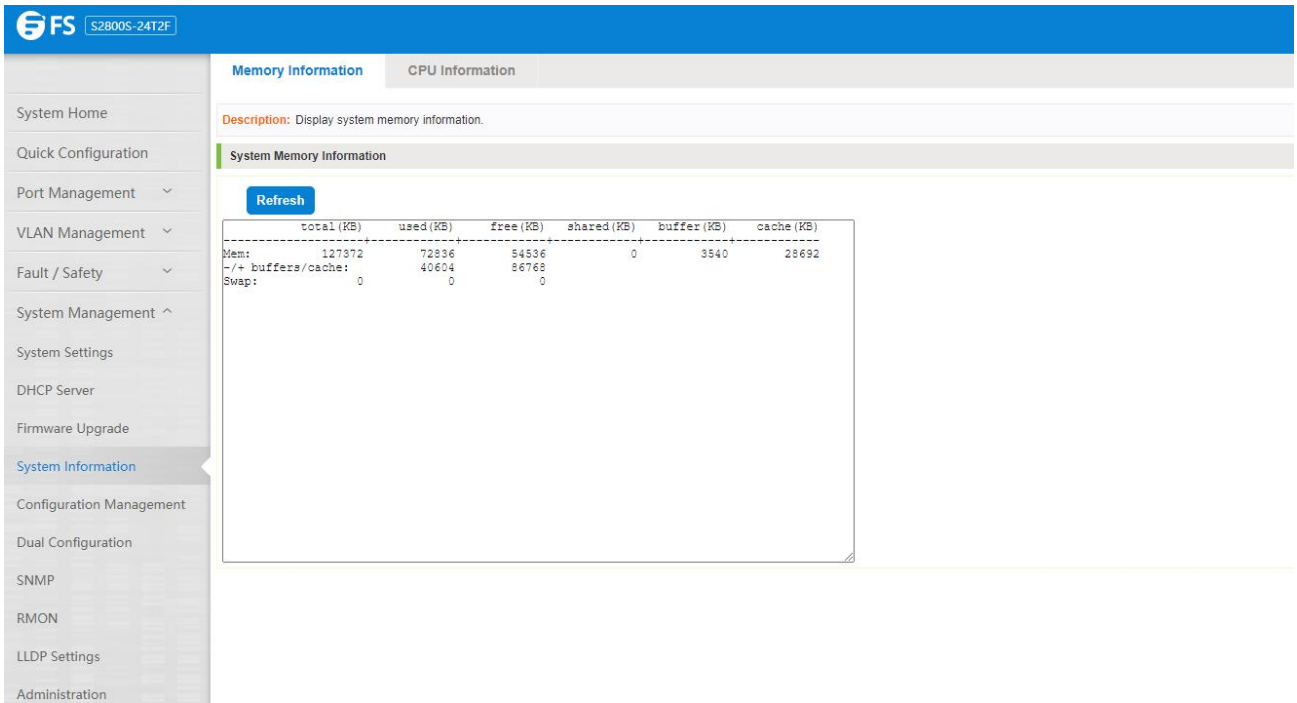


Figure 7-18: System memory information

See the WEB page of memory information content consistent with the results show the memory command line; Click on the "Clear" button to Clear the current switches in the memory information; Click on the "Refresh" button to Refresh the current switches in the memory information.

7.3.2 CPU Information

Click on the "System Management" "System Information" "CPU Information" to enter the CPU Information interface, can view the System task Information:

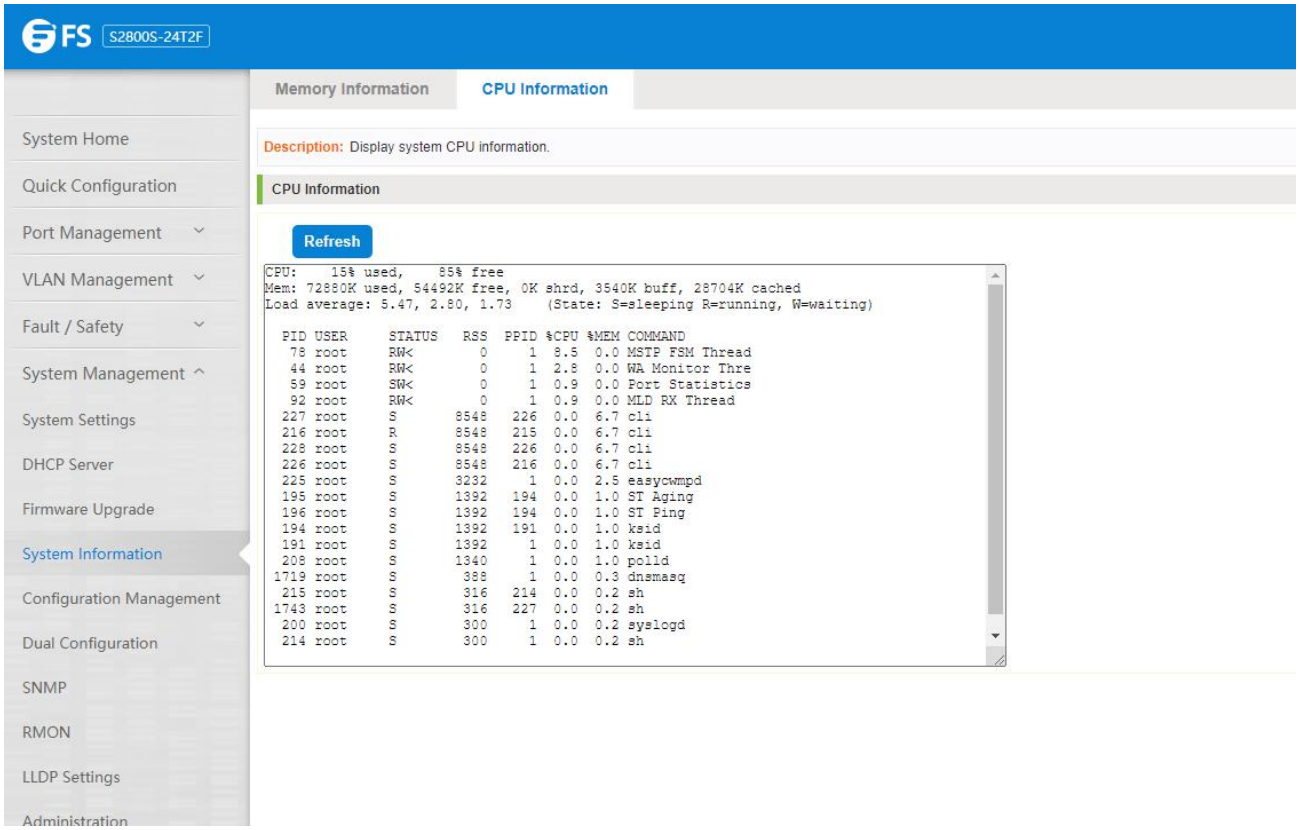


Figure 7-19: CPU information

WEB pages to the content of the system task view consistent with the results show the CPU commands command line; Click on the "Clear" button to remove the current switches in the system; Click on the "Refresh" button to Refresh the current switches in the system task.

7.4 Configuration Management

7.4.1 Configuration Management

1. To See the Current Configuration

Click on "System Management" "Configuration Management" "Configuration Management", and click the button "View", View the current Configuration information:

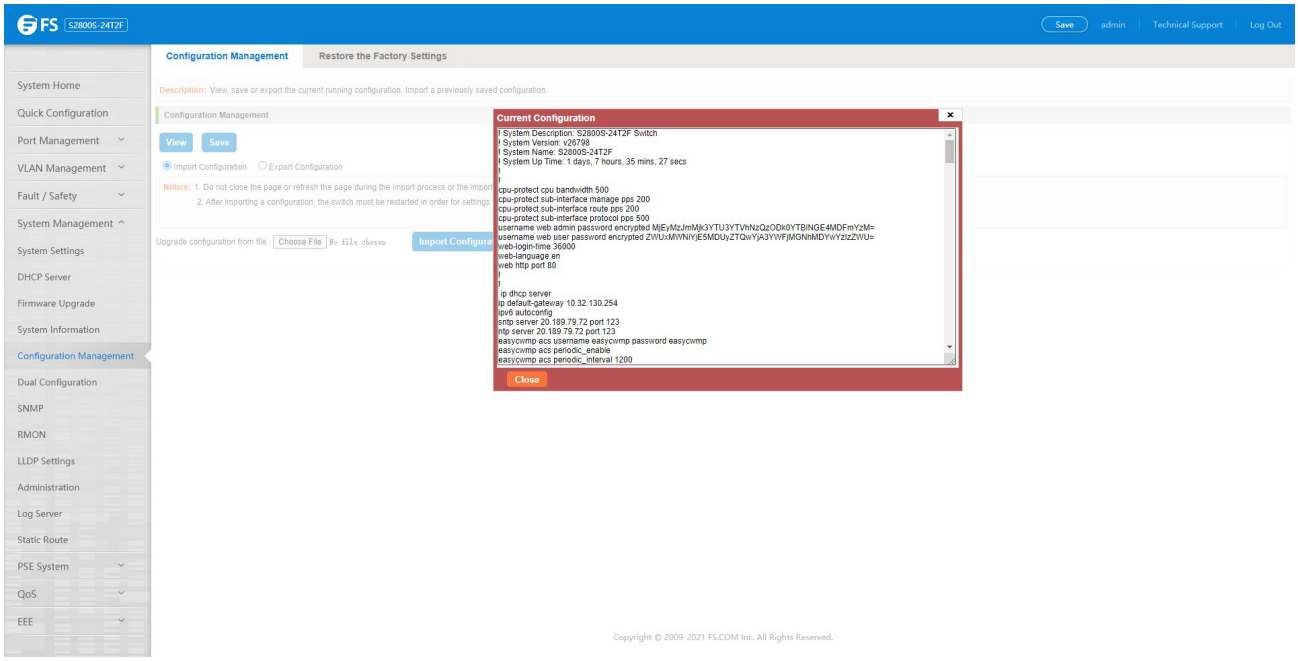


Figure 7-20: View the Current Configuration

2. Save the Current Configuration

Click on the "System Management" "Configuration Management" "Configuration Management", click "Save" button, the running - the content of the config files saved to the start up --config file:

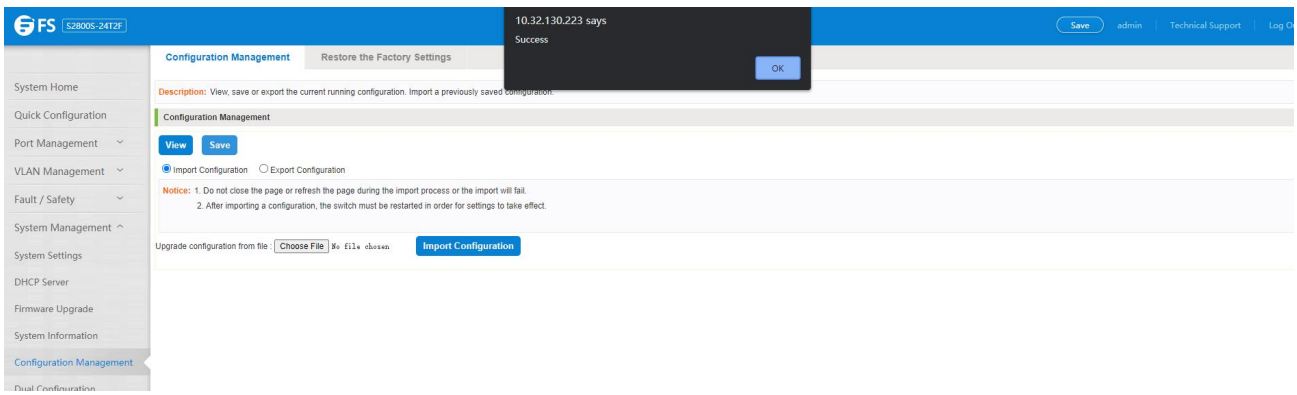


Figure 7-21: To save the current configuration

3. The configuration

Click on the "System Management" "Configuration Management" "Configuration Management", select "Import Configuration", click "Choose File" button to find Configuration File to Import, click the "Import Configuration" button, complete the Configuration Import:

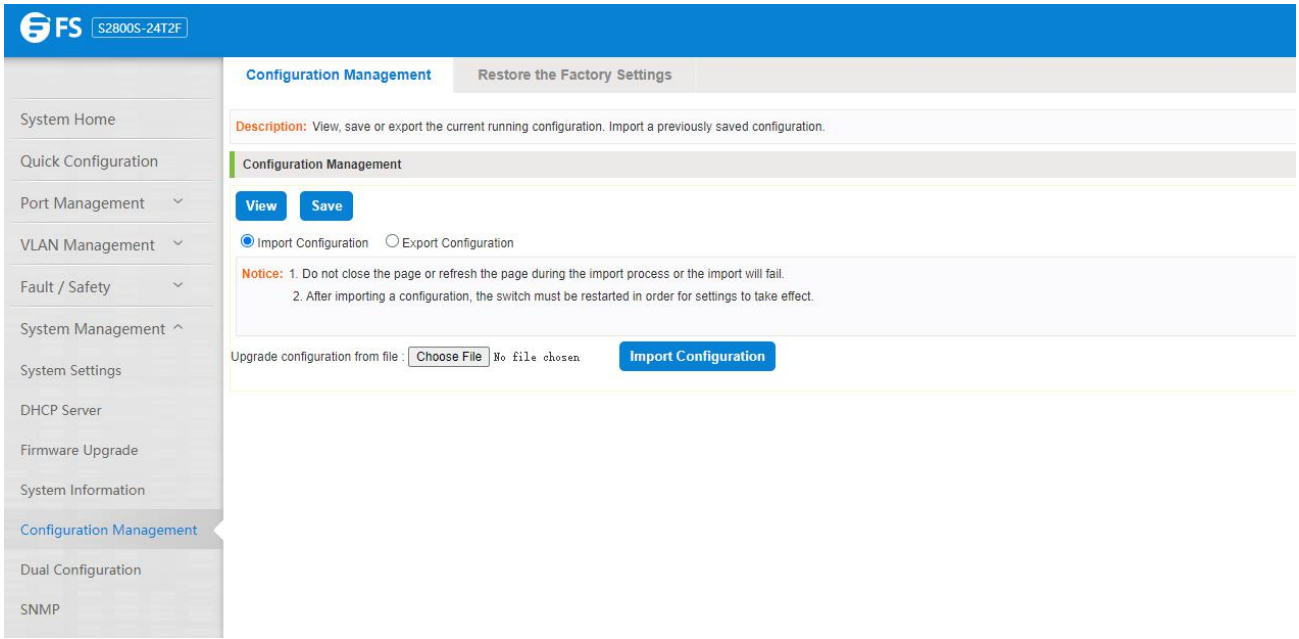


Figure 7-22: Imported Configuration

Import the configuration Steps are as follows:

Step 1: Select the "Import Configuration";

Step 2: Click "Choose File" button to find you want to import the configuration file;

Step 3: Click on "Import Configuration" button;

Step 4: Confirm the restart.

4. Export configuration

Click on the "System Management" "Configuration Management" "Configuration Management", select "Export Configuration", Export Configuration.

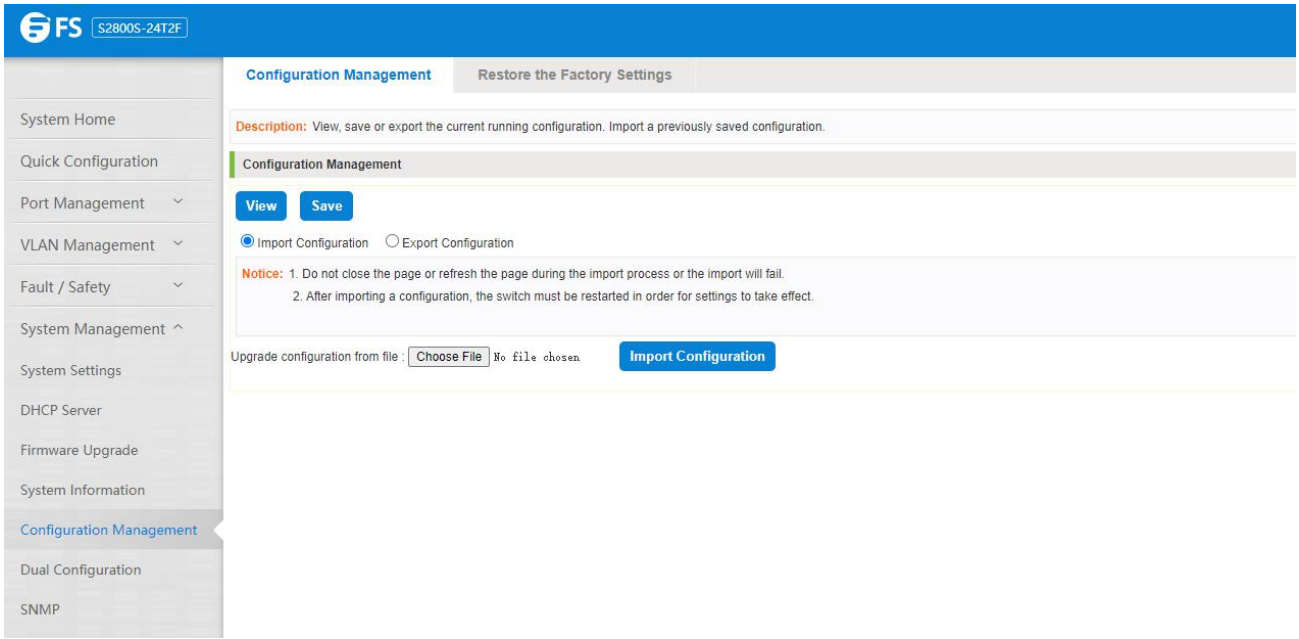


Figure 7-23: Export configuration

7.4.2 Restore Factory Settings

Click on the "System Management" "Configuration Management" "Restore the Factory Settings" to switch to Restore the Factory Configuration actions:

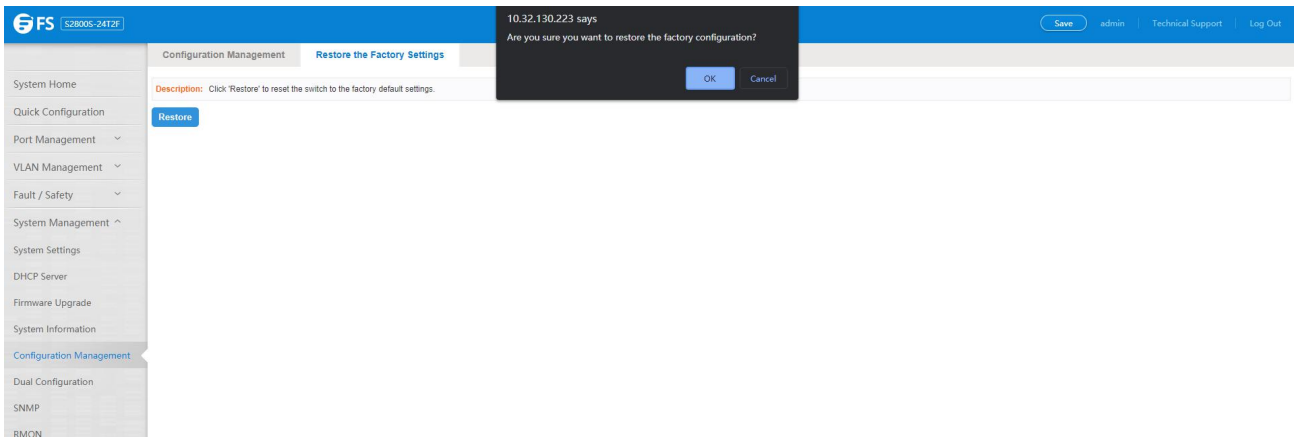


Figure 7-24: Restore factory Settings

Factory default operation Steps are as follows:

Step 1: Click the "Restore the Factory Settings" button;

Step 2: In the pop-up confirmation box, click the "OK" button;

Step 3: After the completion of the reset switch, wait for equipment to restart, switch back to factory default configuration.

7.5 SNMP

7.5.1 Check the SNMP

Click on the "System Management" "SNMP", you can view the SNMP configured information:

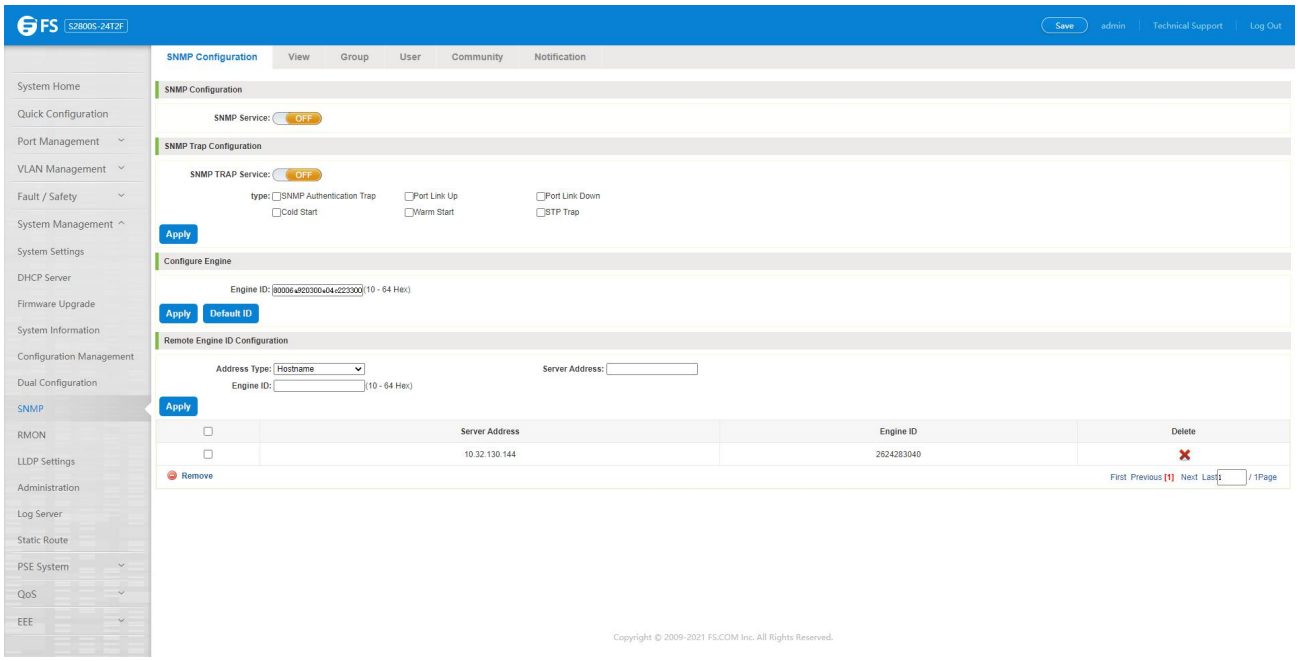


Figure 7-25: View the SNMP configuration information

By default, SNMP is not open;

SNMP monitoring software and switches the SNMP version is consistent, if inconsistencies can lead to communication failure.

7.5.2 Activate the SNMP

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "OFF" to "ON", click OK:

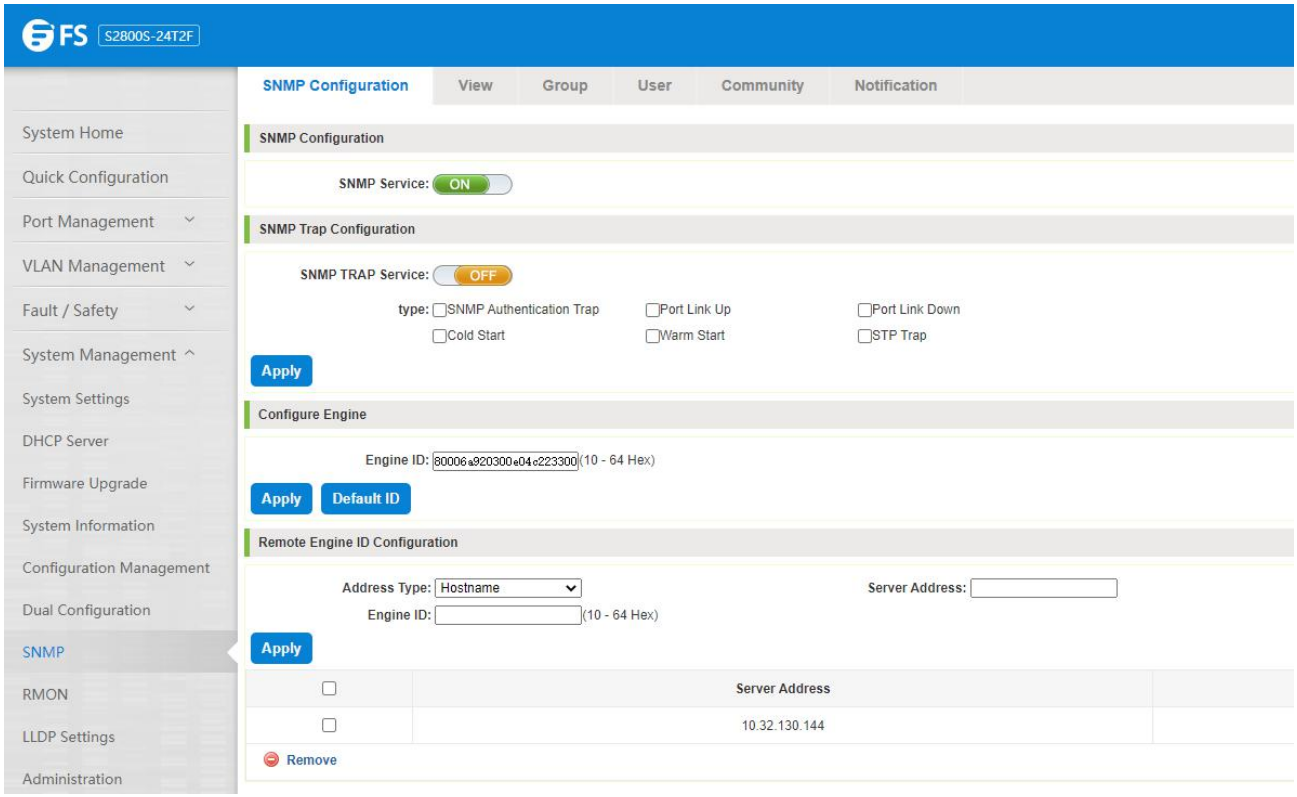


Figure 7-26: Activation SNMP function

Activation function SNMP configuration steps are as follows:

Step 1: Choose open SNMP options;

Step 2: Click "OK" button to complete the configuration.

7.5.3 to Disable the SNMP

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "ON" to "OFF", complete the configuration:

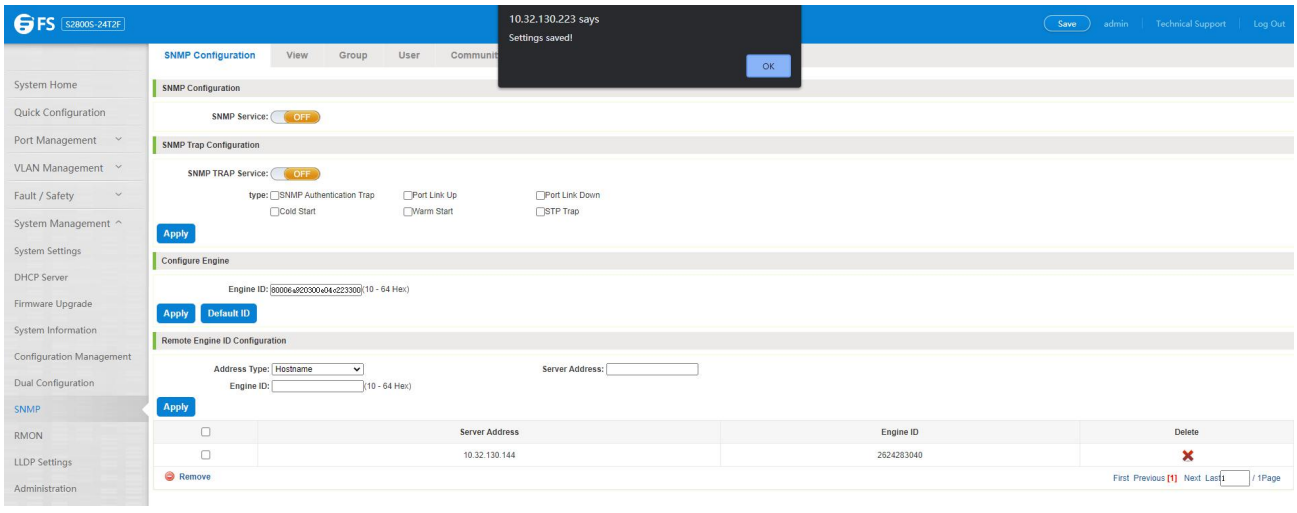


Figure 7-27: Disable the SNMP function

Disable the SNMP function configuration Steps are as follows:

Step 1: Choose close SNMP options;

Step 2: Click "OK" button to complete the configuration.

7.5.4 Activate the TRAP

After open the SNMP, select the SNMP TRAP service, click ON the "OFF" to "ON", click ok:

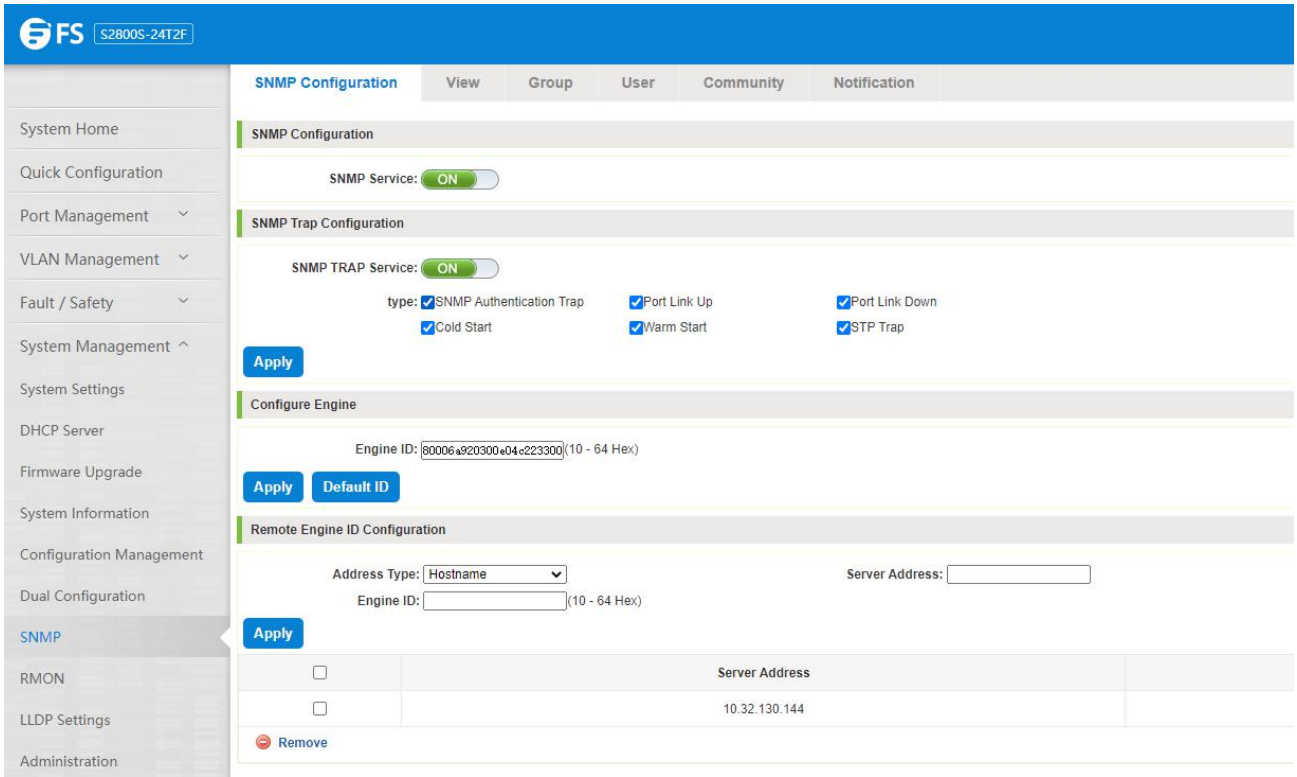


Figure 7-28: Activation function of the TRAP

Activate the TRAP function configuration Steps are as follows:

Step 1: Select "ON" option;

Step 2: Click "OK" button to complete the configuration.

7.5.5 Disable the TRAP

Choose the SNMP TRAP service, click ON the "ON" to "OFF", click "OK", complete the configuration:

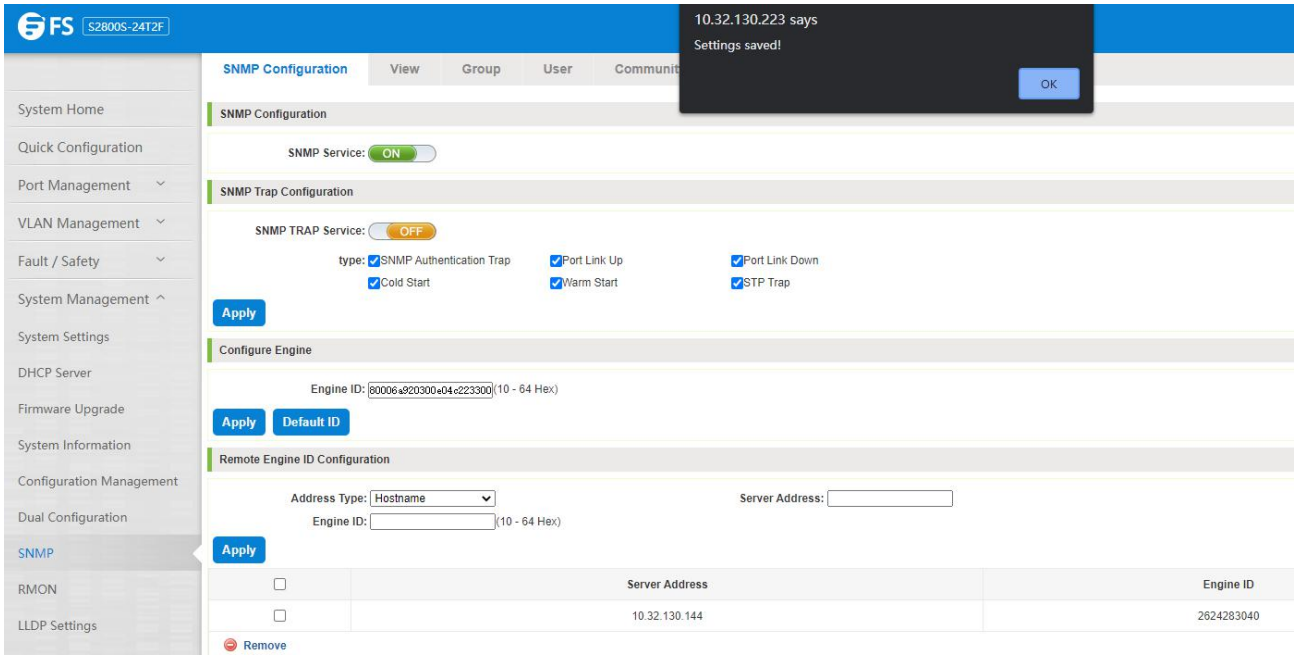


Figure 7-29: Disable TRAP function

Disable the TRAP function configuration steps are as follows:

Step 1: Select "ON" to "OFF" option;

Step 2: Click "OK" button to complete the configuration.

7.5.6 Change Community

Click on the "System Management" "SNMP", in the community name text box input: public, permissions choice: read and write, click the "OK" button, complete the configuration:

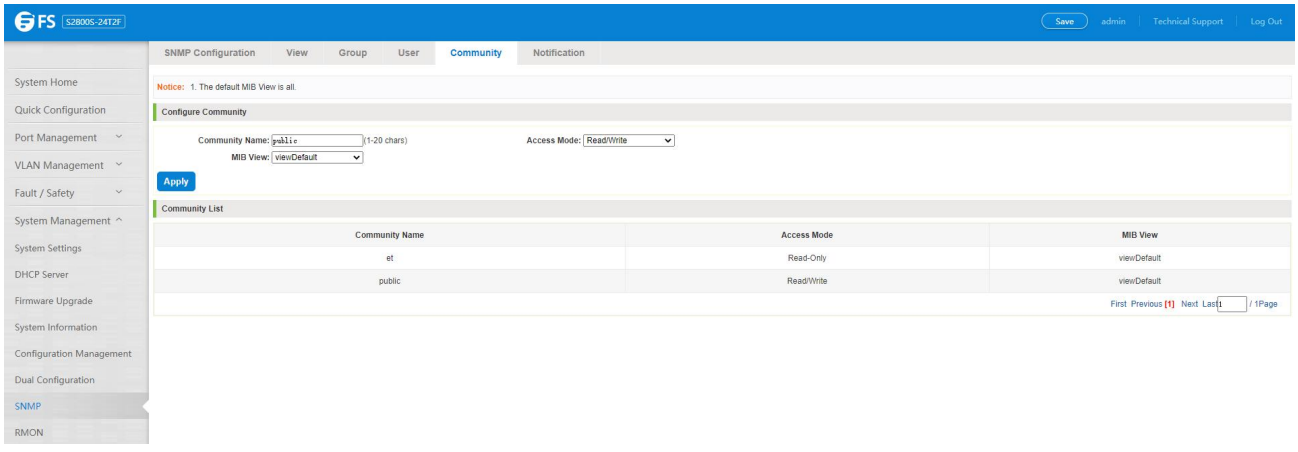


Figure 7-30: Change Community

Change community configuration Steps are as follows:

Step 1: In the community name dialog box input: the public;

Step 2: Select "RW" permissions;

Step 3: Click on "OK" button, complete the configuration.

7.5.7 Added the SNMP TRAP Service Host

Click on the "System Management" "SNMP", in the host IP text box input: 10.32.130.254, TRAP community name: public, SNMP version choice: 2C, click the "OK" button, complete the configuration:

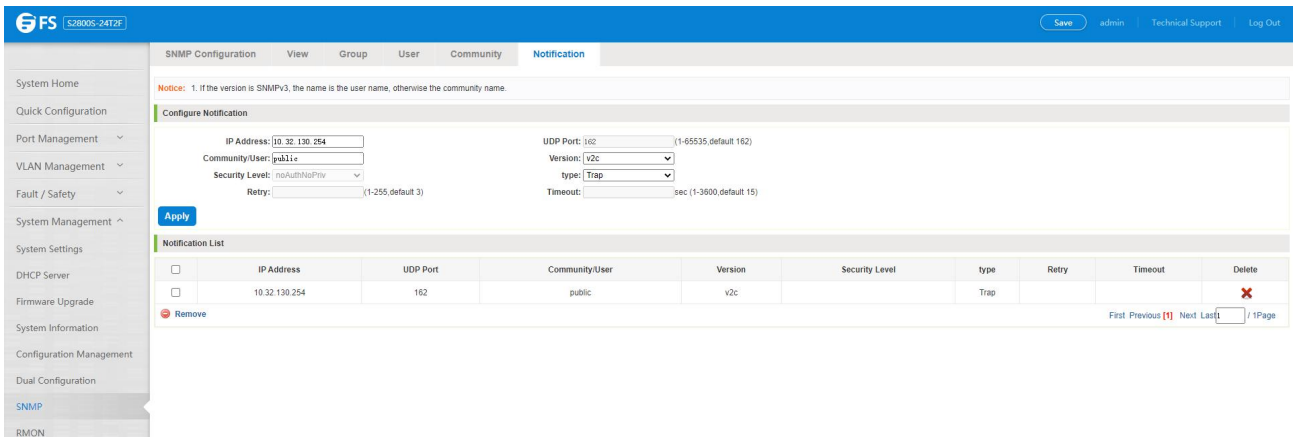


Figure 7-31: Increases the SNMP TRAP service host

Increase the SNMP TRAP service host configuration Steps are as follows:

Step 1: In the host IP dialog box input: 10.32.130.254;

Step 2: In TRAP community name dialog input: public ;

Step 3: Select the SNMP version: 2C;

Step 4: Click on "OK" button, complete the configuration.

When an SNMP closed, hide the SNMP TRAP service host list.

7.5.8 Delete the SNMP TRAP service host

Click on the "System Management" "SNMP", in the SNMP TRAP service host list need to delete the object, click  "finish" configuration:

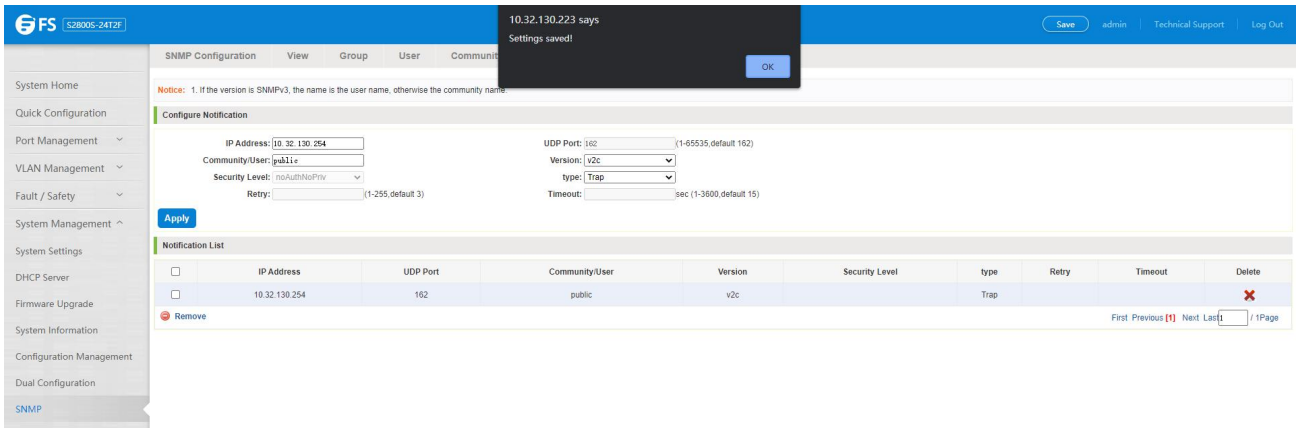


Figure 7-32: Delete community

7.6 RMON

7.6.1 View RMON Configure Information

Click on the "System Management" "RMON", can view RMON configure information.

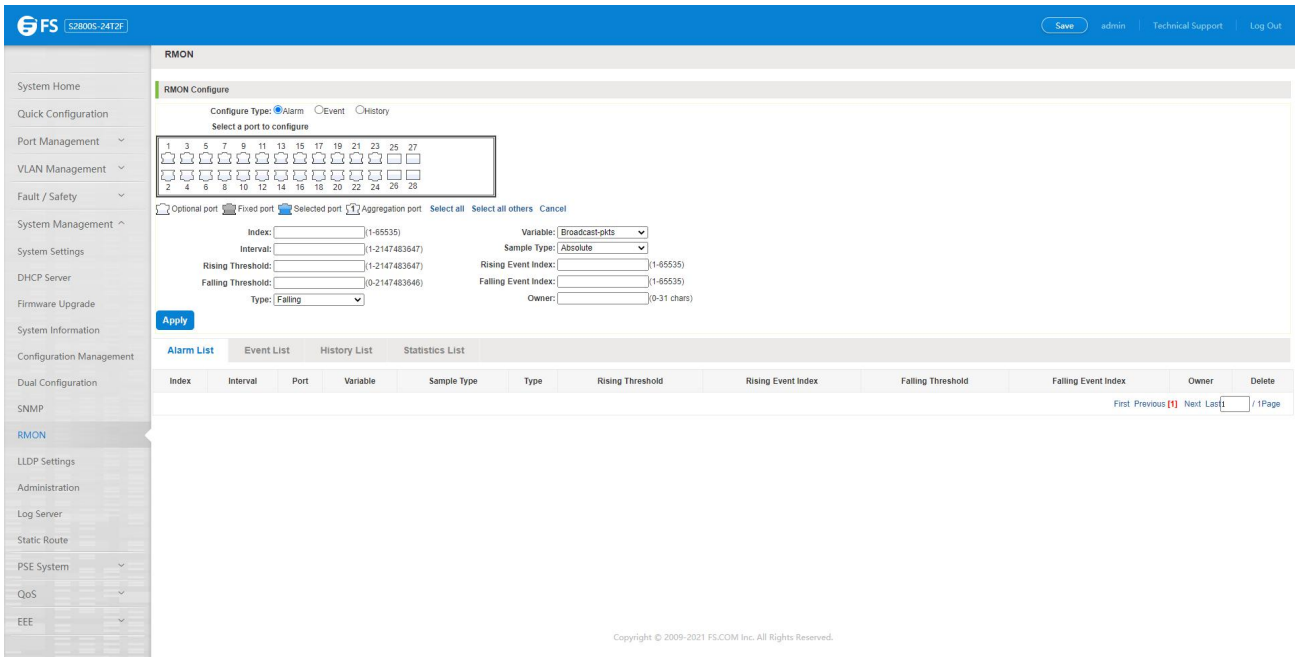


Figure 7-33: View RMON configure information

7.6.2 Configure RMON Type

Configure RMON type: Alarm, selected one port to configure and setting parameters and click “Save” button.

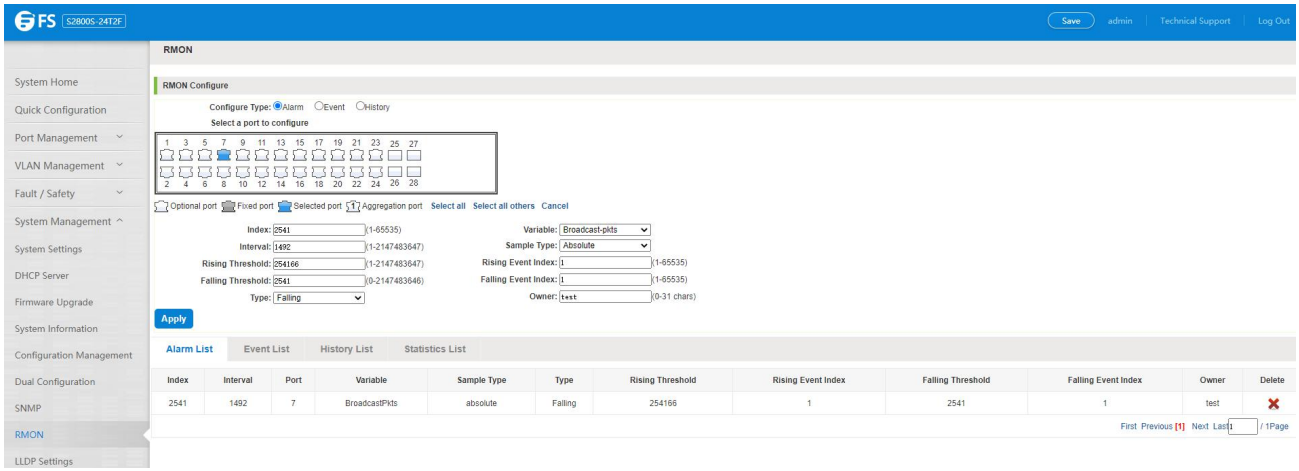


Figure 7-34: Configure RMON Type

Notice: Parameters There are some special rules in the configuration. The EVENT should be created first. Please note the prompts in the configuration. eg: Rising Threshold is greater than Falling Threshold.

7.6.3 Change RMON Type

On the RMON configure page, click the type “Event” or “History” and setting parameters. Be careful the parameter of Community should be exit in SNMP Community name. Configure OK after clicking “Save”.

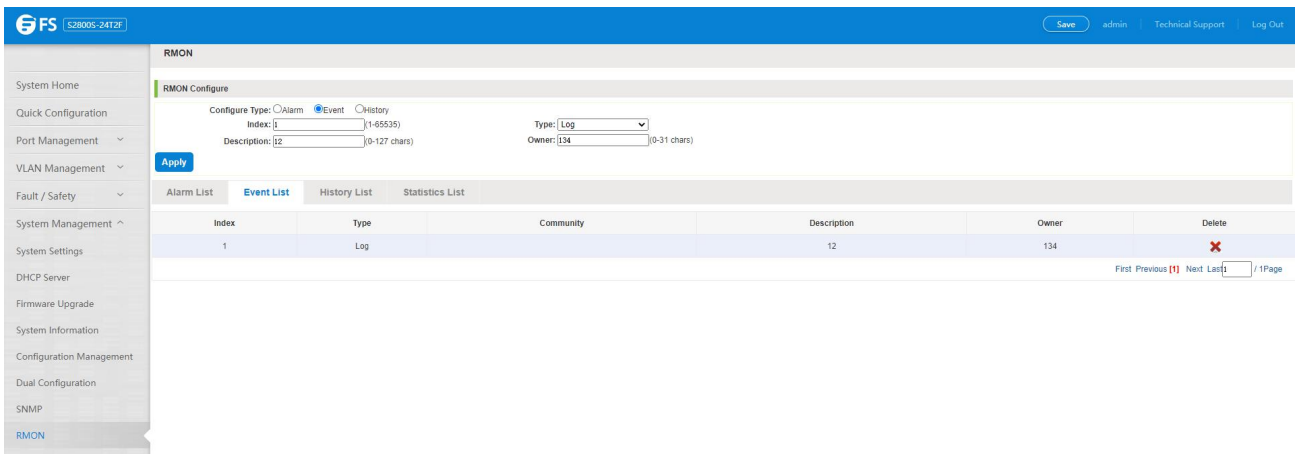


Figure 7-35 Change RMON Type is Event

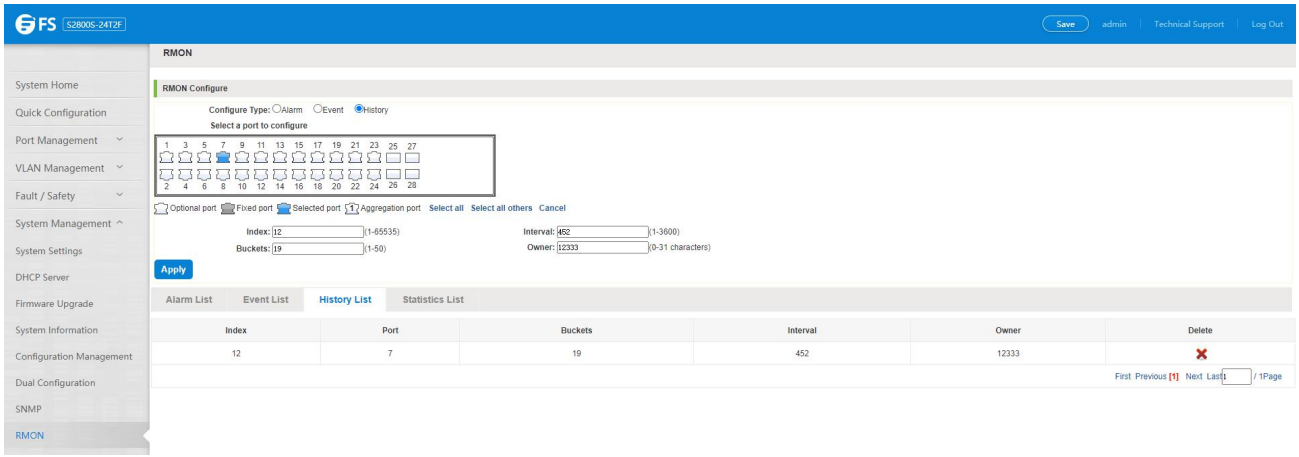


Figure 7-36: Change RMON type is History

When the parameters configure is OK, click the Statistics List .We can choose the port to view the information.

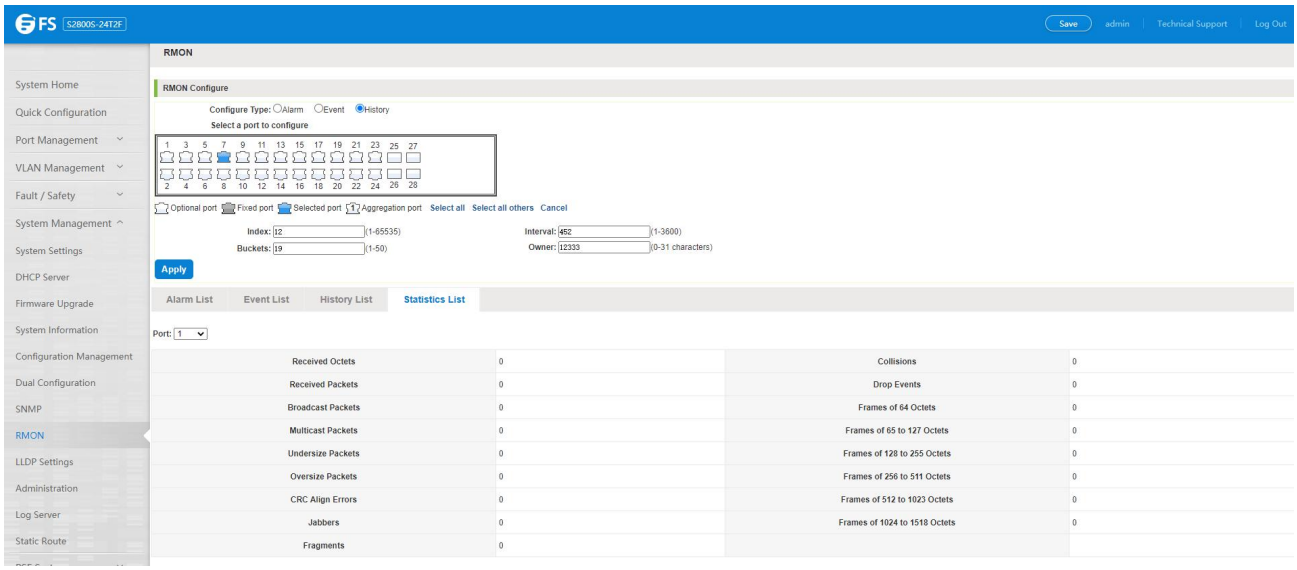


Figure 7-37: View the port configure information

7.6.4 Delete the Configured Rule

Select the entry you want to delete and click Fork to delete the unwanted configuration

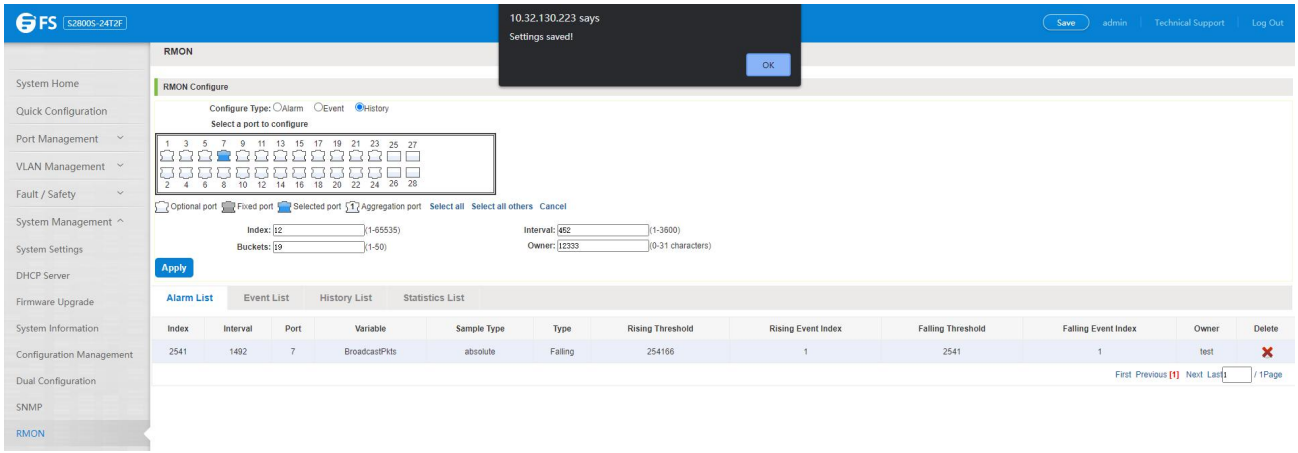


Figure 7-38: Delete the Alarm list rule

7.7 LLDP Settings

7.7.1 LLDP Settings

Click on the "System Management" "LLDP Settings", ”LLDP Settings” can view the LLDP settings information. The default mode is Global settings and this feature is turned off by default.

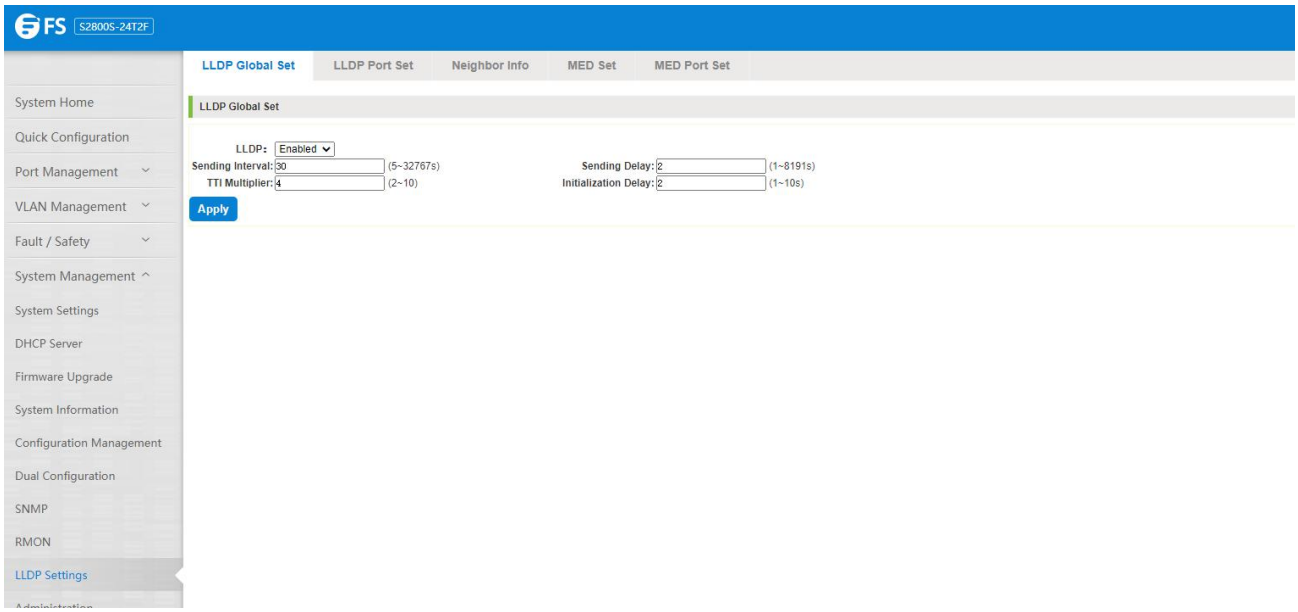


Figure 7-39: View LLDP Settings Information

7.7.2 Enable LLDP Settings

Click the drop-down menu to select enable and configuration parameters. Finally click “Apply” button.

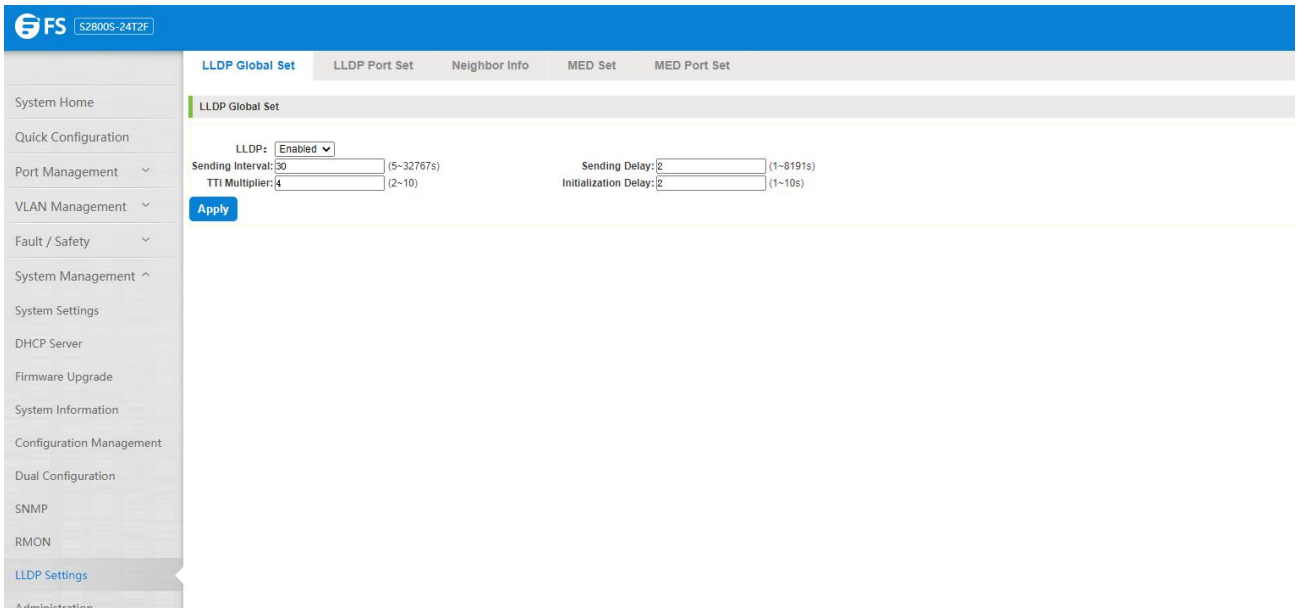


Figure 7-40: Enable LLDP settings

7.7.3 Neighbor Info

When the LLDP function is enabled, the neighbor information is recorded when a neighbor device is found.

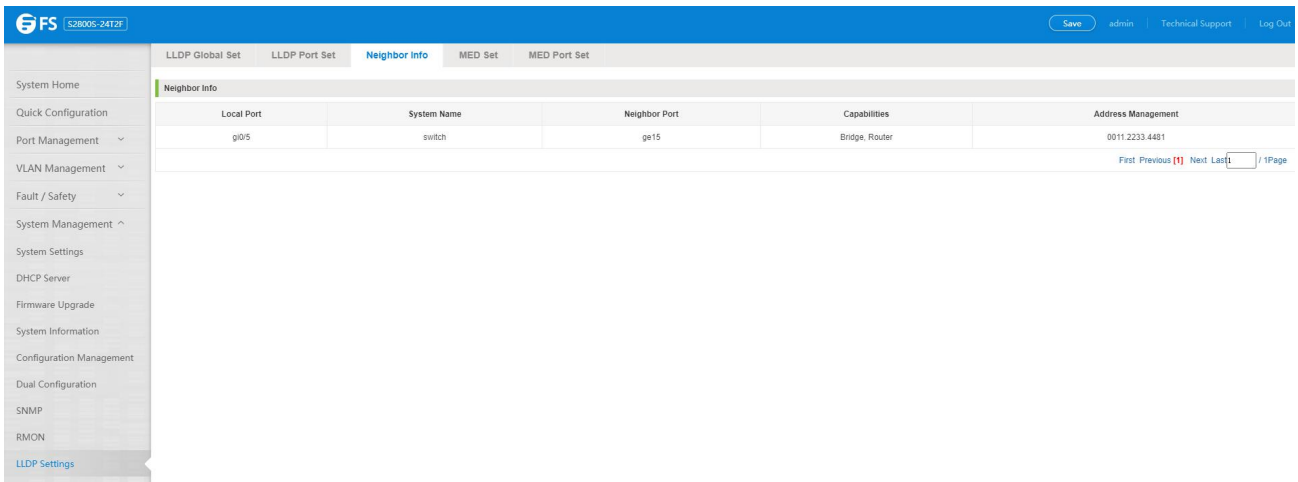


Figure 7-41: Neighbor Info

7.8 Static Route

Click on the "System Management" "Static Route"

Step 1: Turn off switch management VLAN;

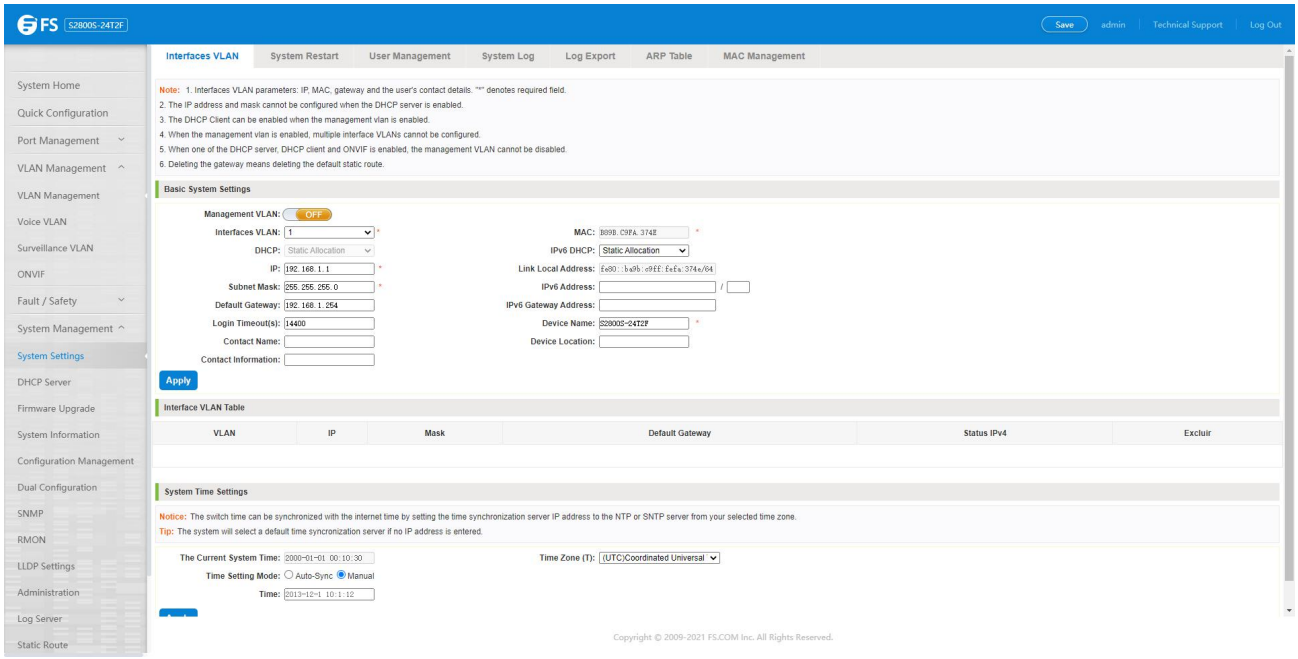


Figure 7-42: Static Route

Step 2: Modify the IP address of interface VLAN1 to 192.168.1.1/24;

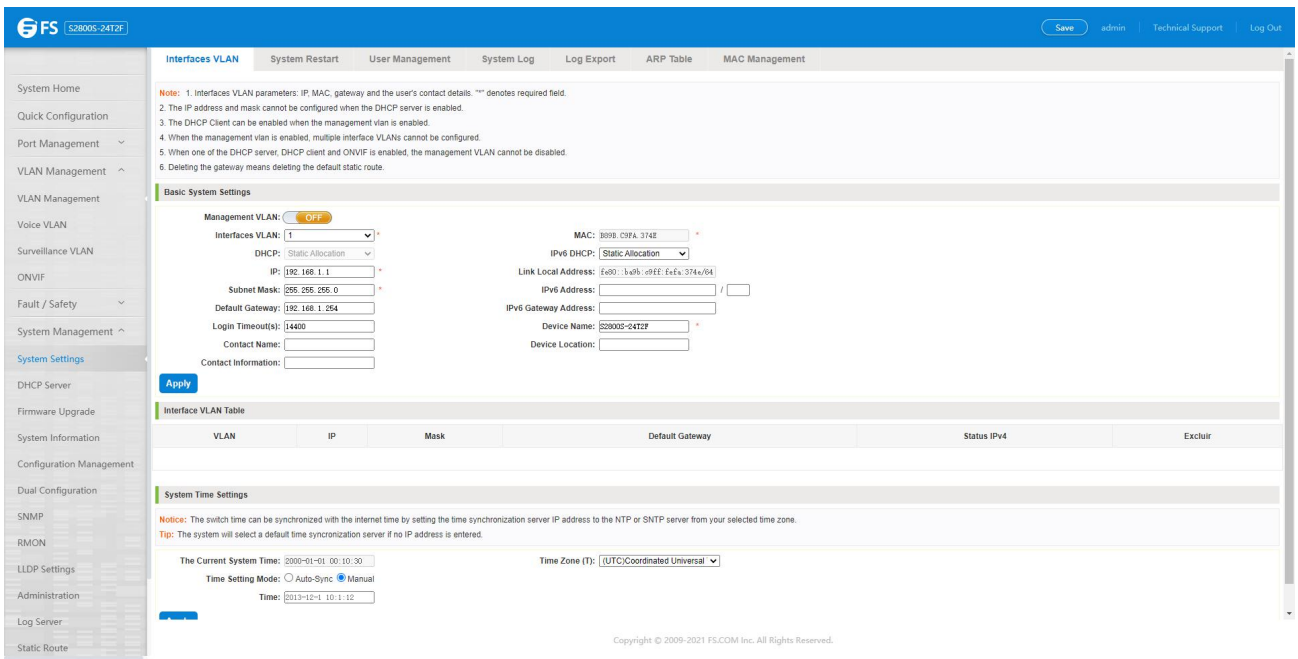


Figure 7-43: Static Route

Step 3: The gateway with static route 192.168.2.0/25 added is 192.168.1.254.

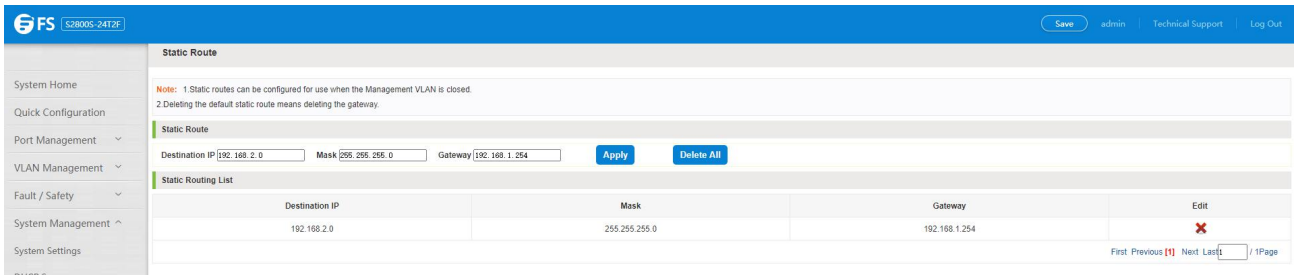


Figure 7-44: Static Route

8. PSE System Management

8.1 PSE System Configuration

8.1.1 View the PSE System Configuration

Click on the navigation bar "PSE System Management" "PSE System Configuration" to view the PSE system information of the current switch, Click "Refresh" button, display refresh configuration information:

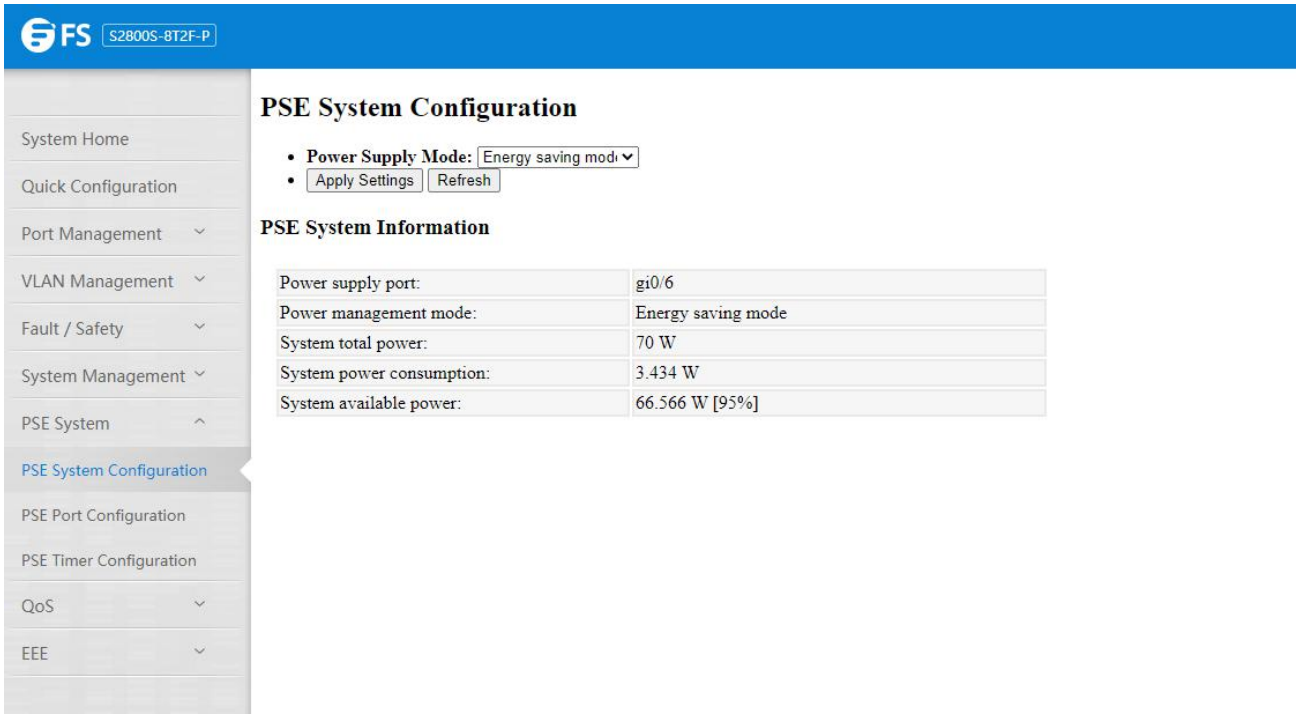


Figure 8-1: View the PSE System Information

8.1.2 Configure Power Supply Mode

8.1.2.1 Configure Power Supply Mode to Automatic

Click on the navigation bar "PSE System Management" "PSE System Configuration" to configure power supply mode to automatic mode

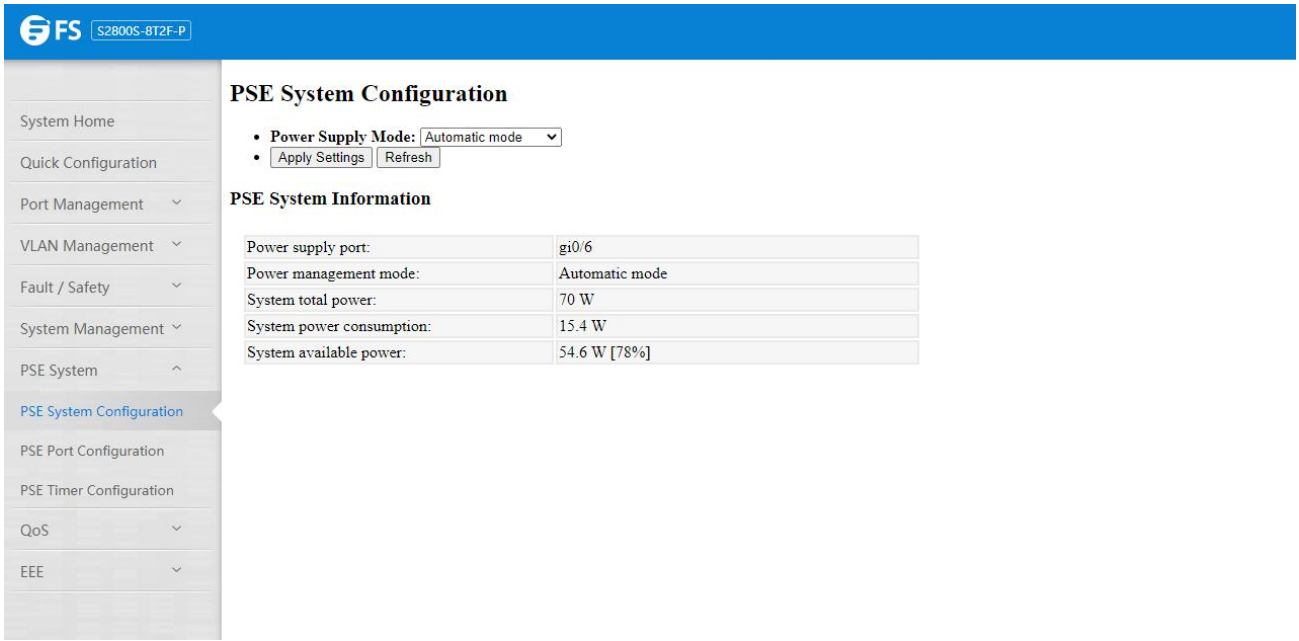


Figure 8-2: Automatic Mode

To configure the switch PSE System steps as follows:

Step 1: In the power supply mode, choose automatic mode;

Step 2: Click on "Apply Settings" button to complete the configuration.

8.1.2.2 Configure Power Supply Mode to Static

Click on the navigation bar " PSE System Management" "PSE System configuration" to configure power supply mode to static mode

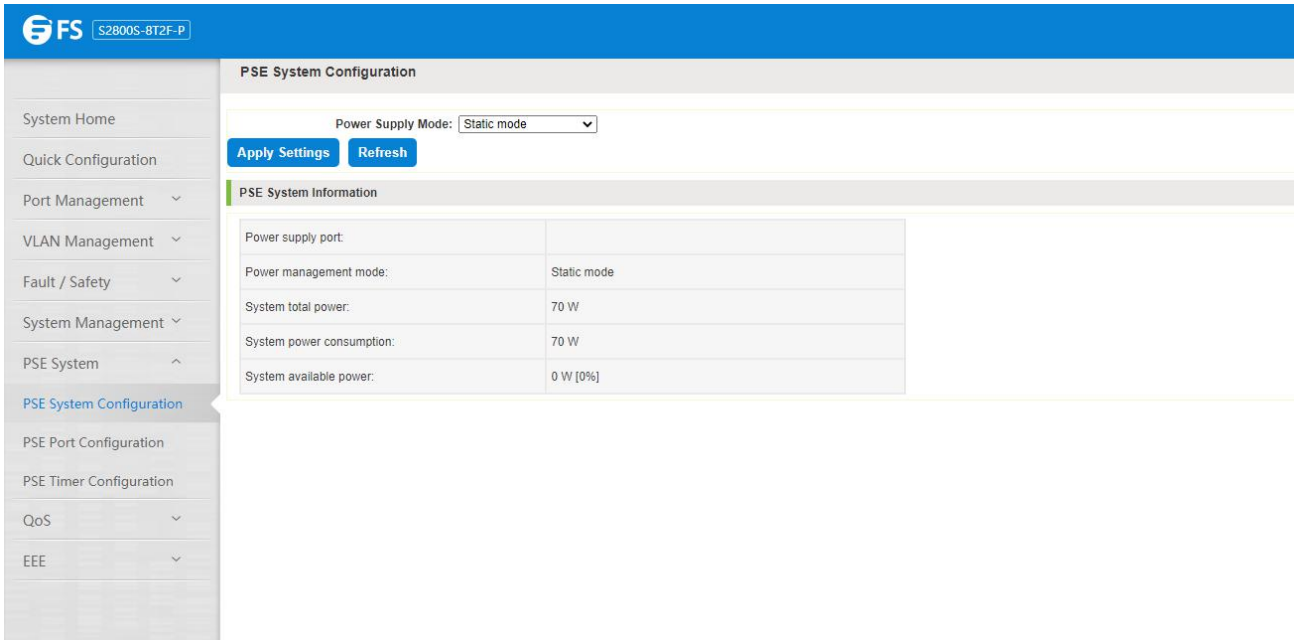


Figure 8-3: Static Mode

To configure the switch PSE System steps as follows:

Step 1: In the power supply mode, choose static mode;

Step 2: Click on "Apply Settings" button to complete the configuration.

8.1.2.3 Configure Power Supply Mode to Energy Saving

Click on the navigation bar " PSE System Management" "PSE System Configuration" to configure power supply mode to energy saving mode

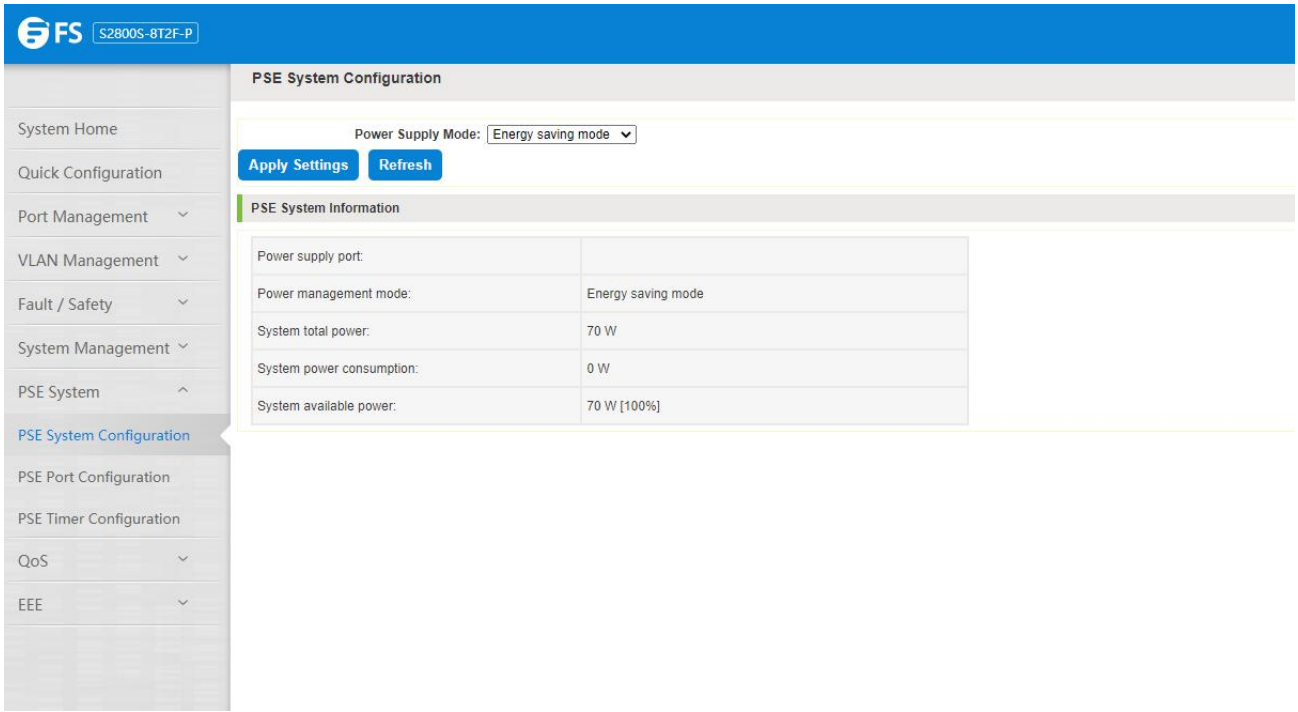


Figure 8-4: Energy saving mode

To configure the switch PSE System Steps as follows:

Step 1: In the power supply mode, choose energy saving mode;

Step 2: Click on "Apply Settings" button to complete the configuration.

8.2 PoE Port Configuration

Click the " PSE System Management" "PoE Port Configuration" to configure the PoE port on the switch:

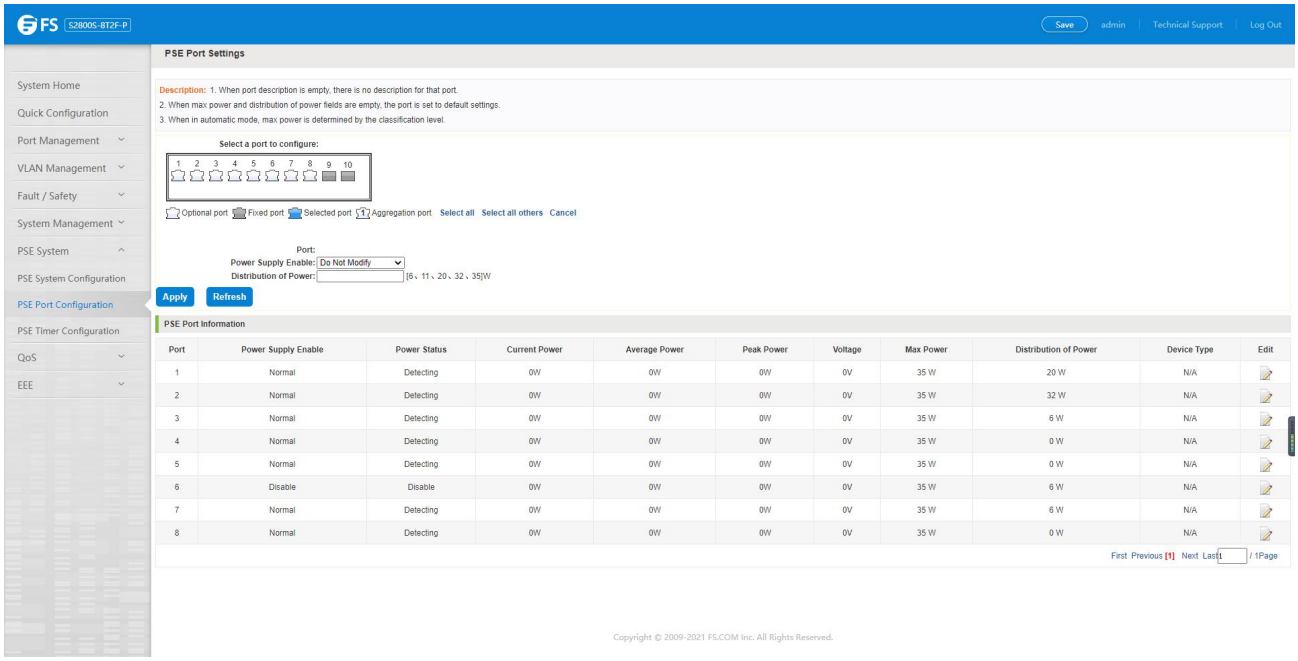


Figure 8-5: PoE Port Configuration

POE Port configuration steps are as follows:

Step 1: Select a port to configure;

Step 2: In the power supply enable, choose enable;

Step 3: In the max power text, choose 20.

8.2.1 Editing PoE Port

Click on the " " icon can be configured selected port:

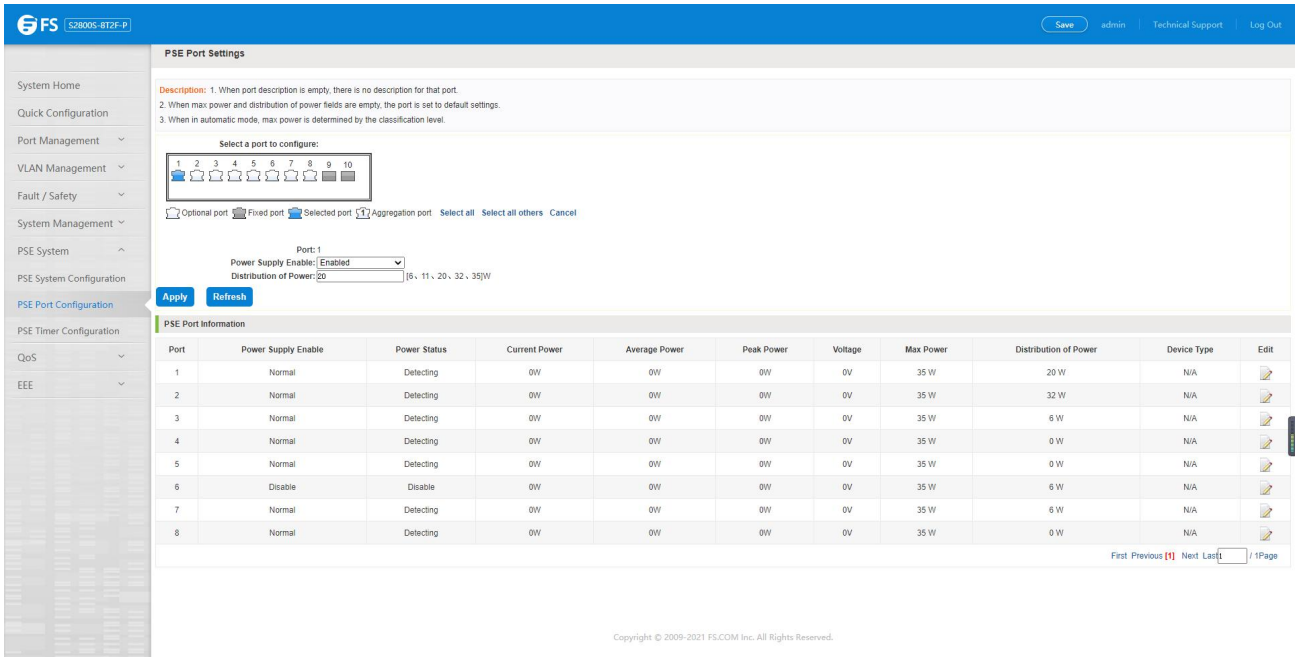


Figure 8-6: Editing PoE Port

Modify PoE port settings follow these steps:

Step 1: Select port and Click" " "icon;

Step 2: In the power supply enable, choose disable.

8.3 PoE Timer Configuration

Click the " PSE System Management" "PoE Timer Configuration" to configure the POE port absolute and periodic time on the switch:

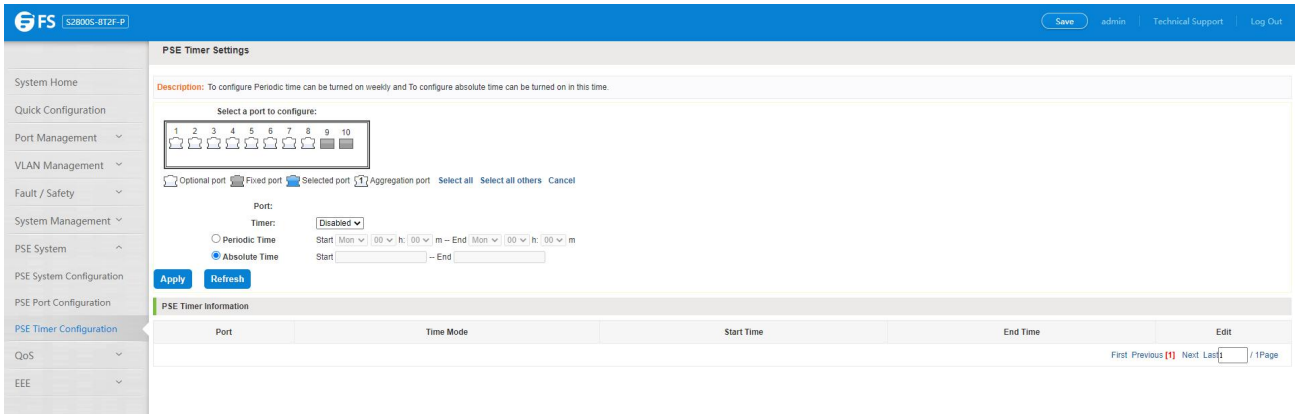


Figure 8-7: PoE timer absolute time configuration

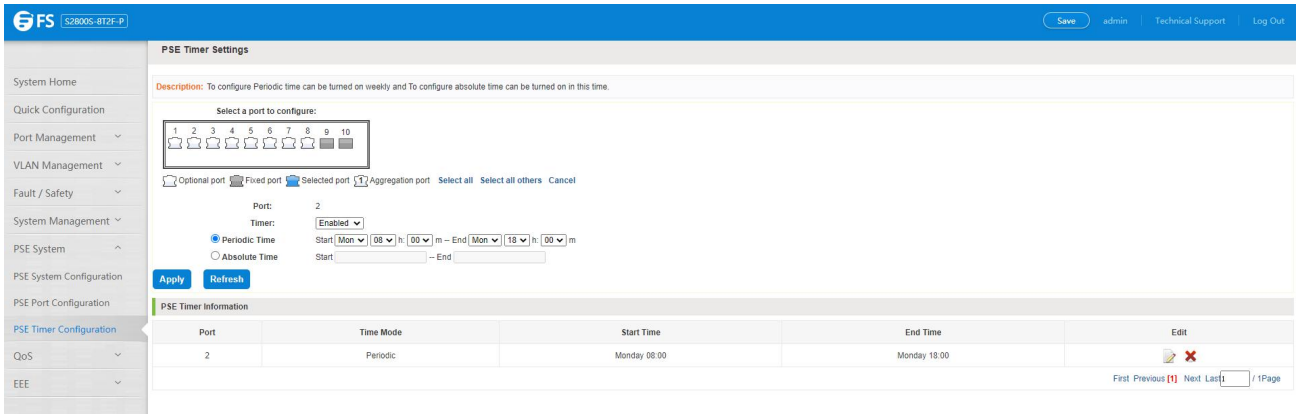


Figure 8-7: PoE timer periodic time configuration

PoE Port configuration Steps are as follows:

Step 1: Select a port to configure;

Step 2: In the timer, choose enable;

Step 3: configure absolute time start time 2017-07-25 08: 30 end time 2017-07-28 08: 30;

Step 4: configure periodic time start time Every Monday to Friday 08: 00 end time Every Monday to Friday 18: 00.

9. QoS

9.1 Priority Schedule

9.1.1 View the Priority Schedule

Click on the "QoS" "Priority Schedule", can view the device priority schedule:

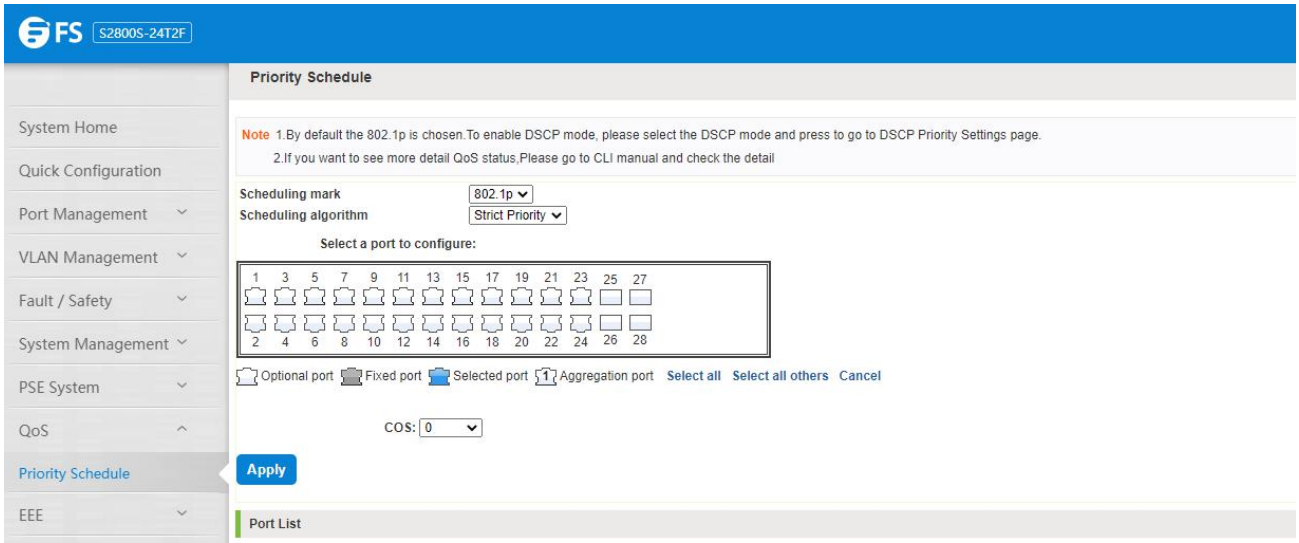


Figure 9-1: Priority Schedule

9.1.2 The Configuration Global Settings of SP

9.1.2.1 The Configuration Global Settings of 802.1P SP

Click on "QOS" "Priority Schedule" “Global Settings”, in scheduling mark, choose 802.1p, in the Scheduling algorithm, choose strict priority.

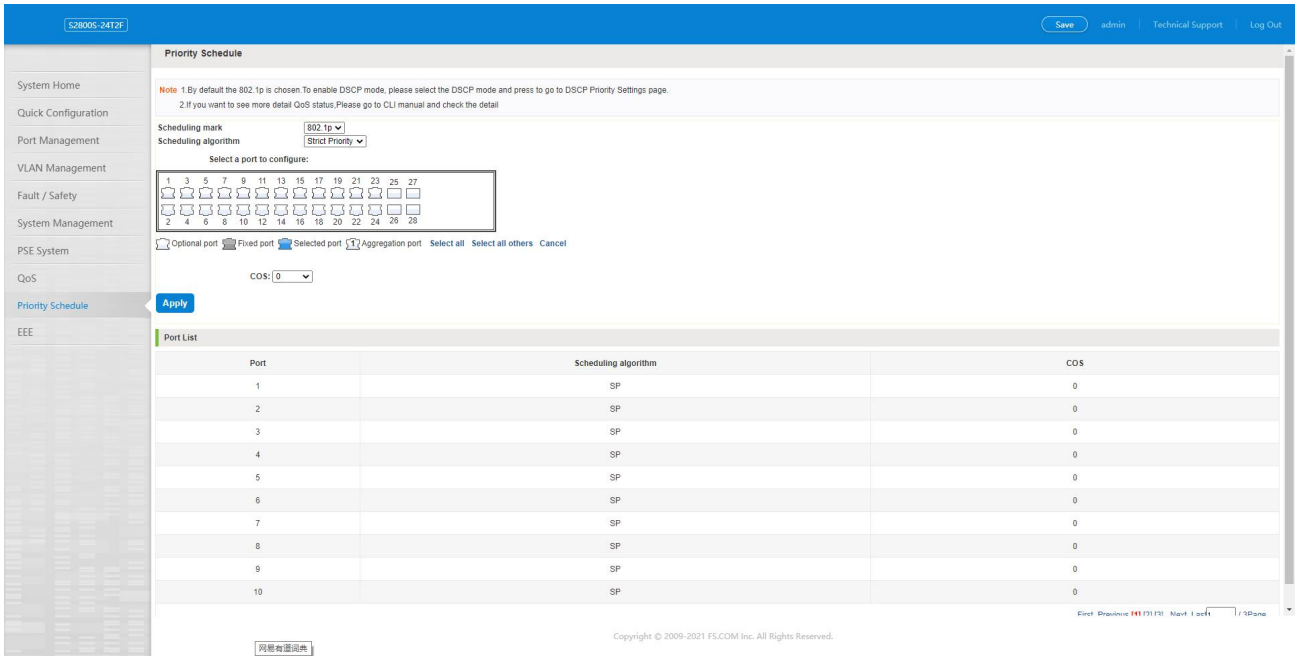


Figure 9-2: Global settings in 802.1p and SP

9.1.2.2 The Configuration Global Settings of 802.1p SP and WRR

Click on "QoS" "Priority Schedule" “Global Settings”, in scheduling mark, choose 802.1p, in the Scheduling algorithm, choose WRR.

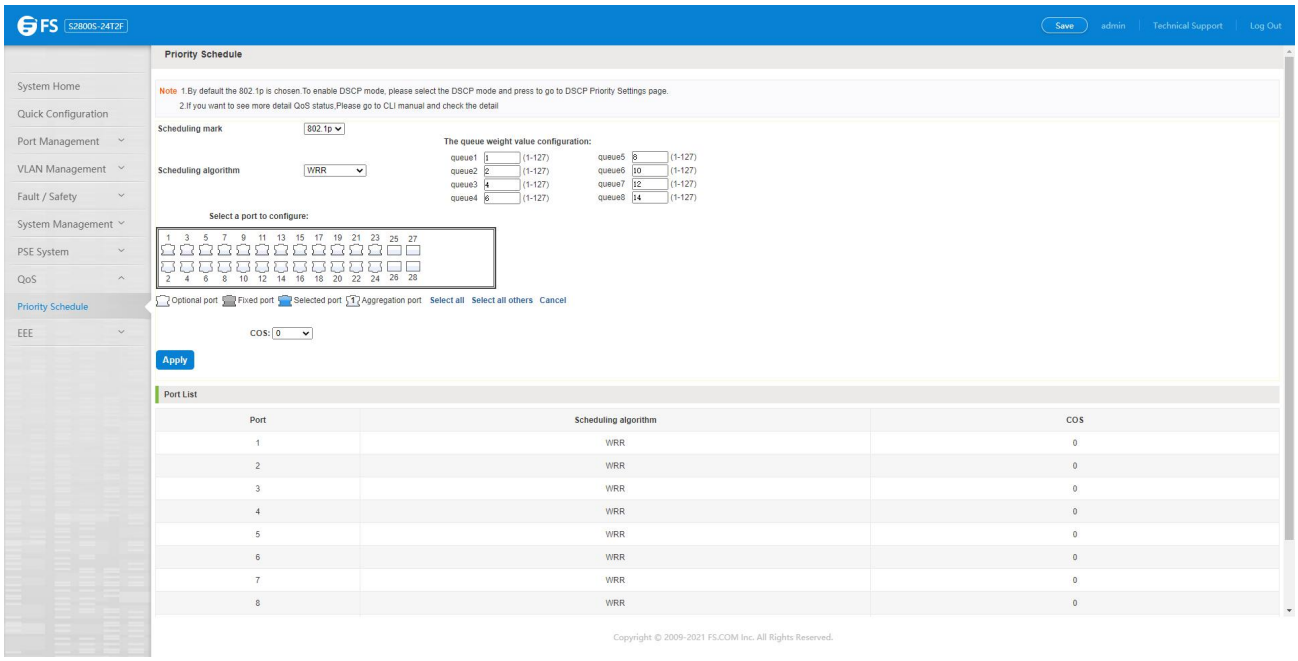


Figure 9-3: Global settings in 802.1p and WRR

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose 802.1p;

Step 2: In the Scheduling algorithm, choose WRR;

Step 3: In queue1 text box, enter the weight value, such as 1;

Step 4: In queue2 text box, enter the weight value, such as 20;

Step 5: In queue3 text box, enter the weight value, such as 40;

Step 6: In queue4 text box, enter the weight value, such as 1.

9.1.2.3 The Configuration Global Settings of 802.1p and Hybrid

Click on "QoS" "Priority Schedule" “Global Settings”, in scheduling mark, choose 802.1p, in the scheduling algorithm, choose hybrid.

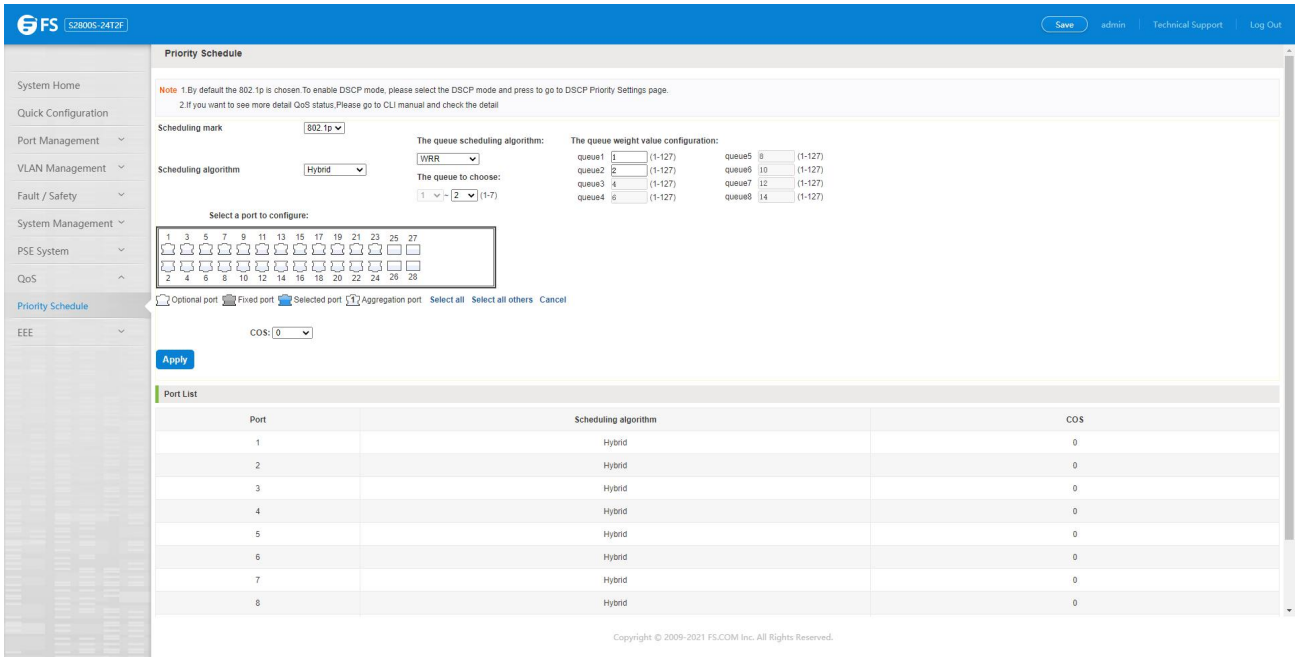


Figure 9-4: Global settings in 802.1p and hybrid

Priority schedule steps are as follows:

Step 1: in scheduling mark, choose 802.1p;

Step 2: in the Scheduling algorithm, choose hybrid;

Step 3: in strict priority text box, choose the queue 3,4;

Step 4: in WRR text box, choose the queue 1, 2;

Step 5: in queue1 text box, enter the weight value, such as 1;

Step 6: in queue2 text box, enter the weight value, such as 20.

9.1.3 The Configuration Global Settings of DSCP

9.1.3.1 The Configuration Global Settings of DSCP and SP

Click on "QoS" "Priority Schedule" “Global Settings”, in scheduling mark, choose DSCP, in the Scheduling algorithm, choose strict priority.

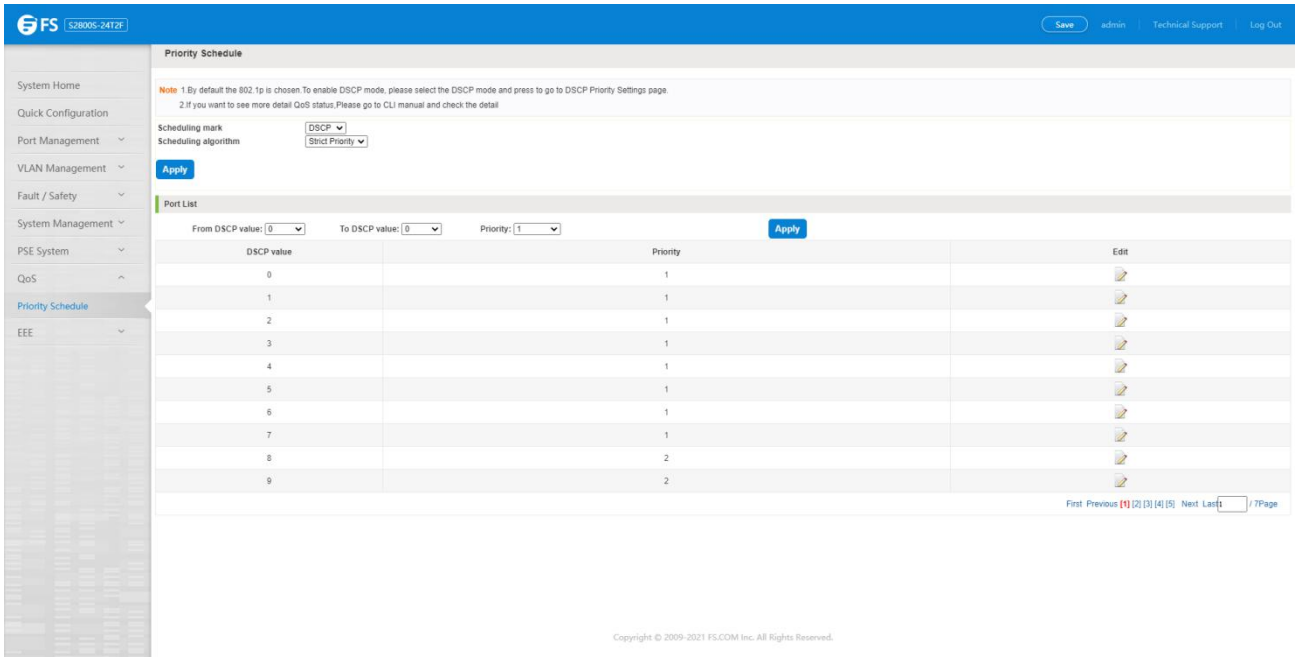


Figure 9-5: Global settings in DSCP and SP

Priority schedule Steps are as follows:

Step 1: In scheduling mark, choose DSCP;

Step 2: In the Scheduling algorithm, choose strict priority;

Step 3: In from DSCP value text box, choose 0 and in to DSCP value text box, choose 1 and in priority text box, choose low;

Step 4: In from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose medium;

Step 5: In from DSCP value text box, choose 4 and in to DSCP value text box, choose 5 and in priority text box, choose high;

Step 6: In from DSCP value text box, choose 6 and in to DSCP value text box, choose 8 and in priority text box, choose highest.

9.1.3.2 The Configuration Global Settings of DSCP and WRR

Click on "QoS" "Priority Schedule" “Global Settings”, in scheduling mark, choose DSCP, in the Scheduling algorithm, choose strict priority.

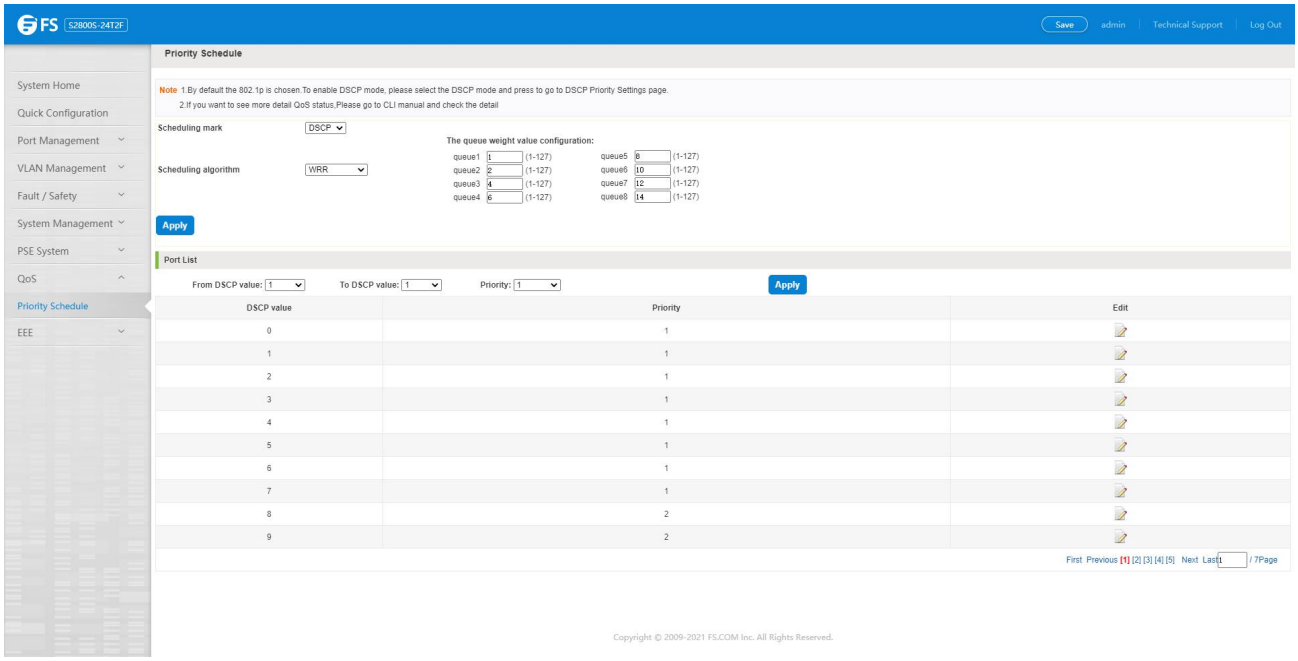


Figure 9-6: Global settings in DSCP and WRR

Priority schedule Steps are as follows:

Step 1: in scheduling mark, choose DSCP;

Step 2: in the Scheduling algorithm, choose WRR;

Step 3: in queue1 text box, enter the weight value, such as 10;

Step 4: in queue2 text box, enter the weight value, such as 20;

Step 5: in queue3 text box, enter the weight value, such as 30;

Step 6: in queue4 text box, enter the weight value, such as 40.

9.1.3.3 The Configuration Global Settings of DSCP and Hybrid

Click on "QoS" "Priority Schedule" “Global Settings”, in scheduling mark, choose DSCP, in the Scheduling algorithm, choose hybrid.

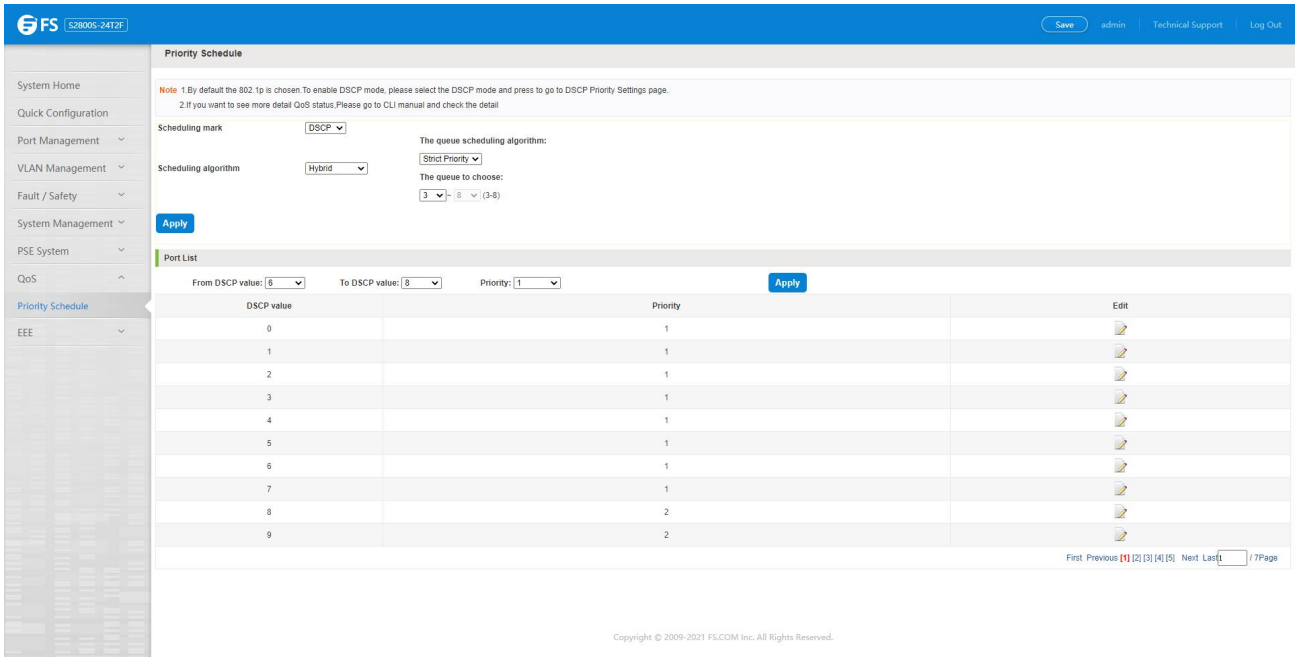


Figure 9-7: Global settings in DSCP and HYBRID

Priority schedule Steps are as follows:

Step 1: In scheduling mark, choose DSCP;

Step 2: In the Scheduling algorithm, choose hybrid ;

Step 3: In strict priority text box, choose the queue 3,4;

Step 4: In WRR text box, choose the queue 1,2;

Step 5: In queue1 text box, enter the weight value, such as 10;

Step 6: In queue2 text box, enter the weight value, such as 20.

9.1.4 Editing the DSCP Values

Click on the " " icon to modify DSCP values:

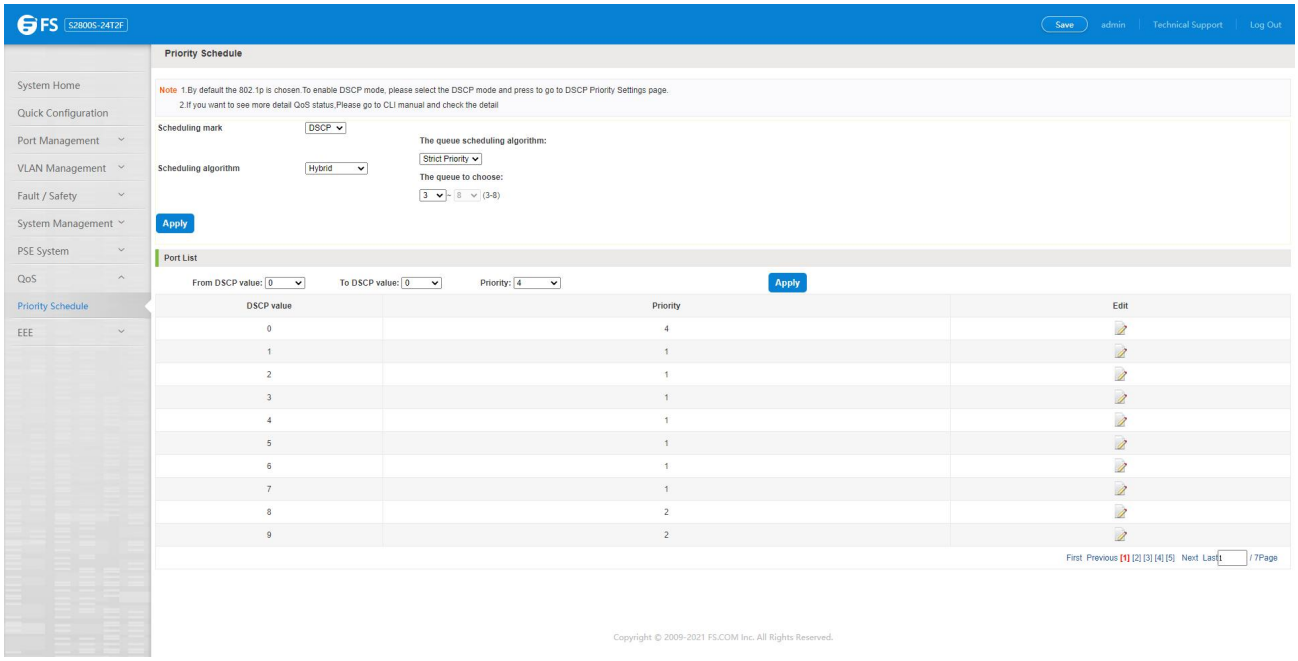


Figure 9-8: Add the port to the VLAN

Modify DSCP values follow these Steps:

Step 1: Select DSCP values and click"  "icon;

Step 2: In the priority text box, choose medium;

Step 3: Click on the save;

Step 4: Click OK.

10. EEE

10.1 EEE

10.1.1 802.3az EEE Settings

Click on the "EEE" "EEE" “802.3az EEE settings”, you can view the EEE information:

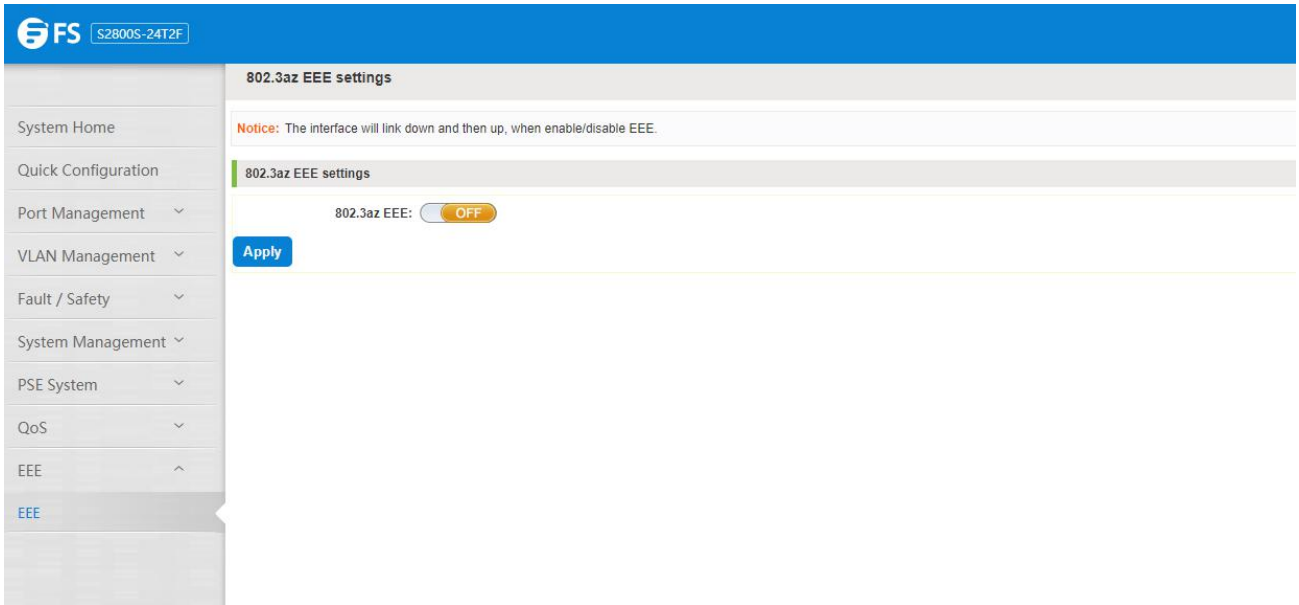


Figure 10-1: View the 802.3az EEE settings

10.1.2 Active the EEE

Click ON the "EEE “ "EEE" "802.3az EEE Settings”, choose the 802.3az EEE, click ON the "OFF" to "ON", click save:

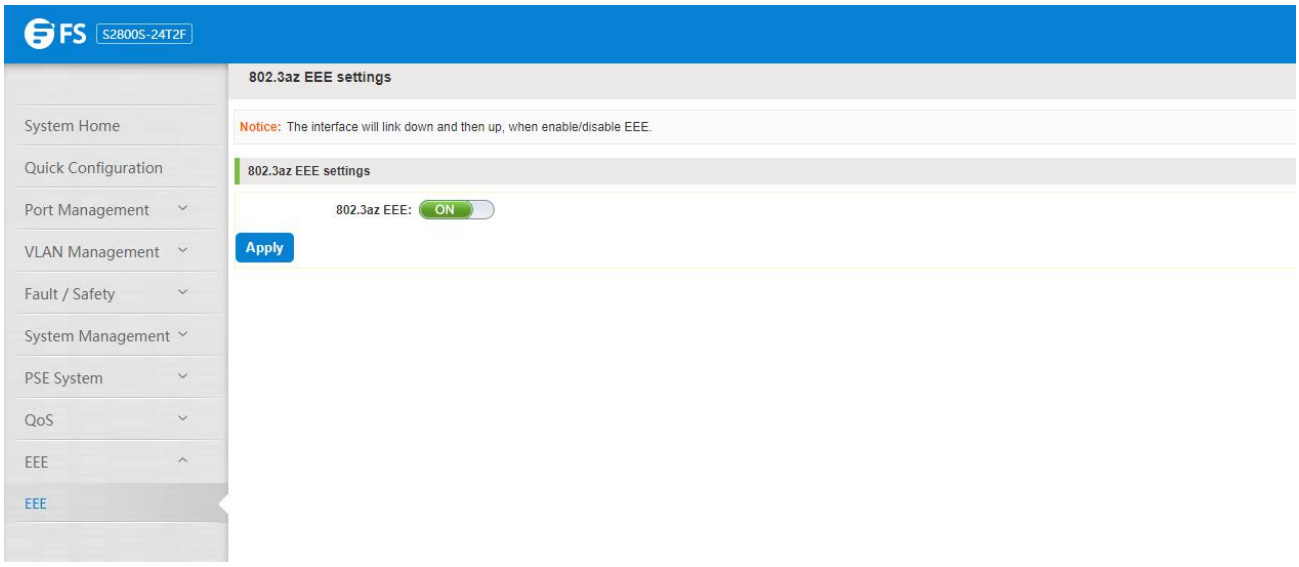


Figure 10-2: Active the 802.3az EEE settings

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.