
Web Configuration Manual

TABLE OF CONTENTS

1 WEB MANAGEMENT LANDING PAGE.....	1
1.1 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB.....	1
2 QUICK CONFIGURATION.....	2
2.1 VLAN SETTING.....	2
2.2 MODE.....	3
2.3 SNMP CONFIGURATION.....	4
2.4 THE OTHER SETTINGS.....	4
3 PORT MANAGEMENT.....	5
3.1 BASIC SETTINGS.....	5
3.1.1 Check the port configuration.....	5
3.1.2 Configuring Port Properties.....	6
3.2 STORM CONTROL.....	7
3.2.1 Check the port settings Storm.....	7
3.3 FLOW CONTROL.....	9
3.3.1 Configuring Flow Control.....	10
3.4 PORT AGGREGATION.....	11
3.4.1 Viewing Port Aggregation Configuration.....	11
3.4.2 Add port aggregation.....	12
3.4.3 Modifying port aggregation.....	12
3.5 PORT MIRRORING.....	13
3.5.1 Port Mirroring Configuration.....	13
3.5.2 Add port mirroring group.....	13
3.5.3 To modify the port mirroring group.....	15
3.5.4 Delete a port mirroring group.....	16
3.6 PORT ISOLATION.....	17
3.6.1 VIEW PROT ISOLATION.....	17
3.6.2 CONFIGURE THE PROT ISOLATION.....	18
3.6.3 EDIT THE PORT ISOLATION.....	18
3.7 PORT SPEED LIMIT.....	19
3.7.1 View port rate limiting.....	19
3.7.2 Configure port access rate.....	20
3.7.3 Remove the port speed limit.....	20
4 VLAN MANAGEMENT.....	21
4.1 VLAN MANAGEMENT.....	21
4.1.1 Check VLAN configuration information.....	21
4.1.2 Adding a VLAN.....	22
4.1.3 Remove VLAN.....	22
4.1.3.1 SINGLE VLAN DELETE.....	22
4.1.3.2 DELETE MULTIPLE VLAN.....	23
4.1.4 Editing VLAN.....	24
4.1.4.1 CHANGE PORT TO A VLAN.....	24
4.1.4.2 TO REMOVE THE PORT FROM A VLAN.....	24
4.1.5 View port mode.....	25
4.1.6 change the port mode is trunk.....	26
4.1.7 CHANGE THE PORT MODE IS ACCESS.....	26

4.2 VOICE VLAN.....	27
4.2.1 VIEW THE VOICE VLAN CONFIGURATION.....	27
4.2.2 ENABLE THE VOICE VLAN.....	27
4.2.3 CONFIGURE THE VOICE VLAN PORT.....	28
4.2.4 VOICE VLAN OUI TABLE.....	29
4.2.5 view the voice vlan device.....	30
4.3 SURVEILLANCE VLAN.....	30
4.3.1 VIEW THE surveillance VLAN CONFIGURATION.....	30
4.3.2 configure surveillance VLAN.....	31
4.3.3 MAC Settings and Surveillance Device.....	32
4.3.4 PROT SURVEILLANCE VLAN.....	32
4.3.5 ATUO SURVEILLACE VLAN SUMMARY.....	34
4.4 MAC VLAN.....	34
4.4.1 VIEW THE MAC VLAN INFORMATION.....	34
4.4.2 CONFIGURE THE MAC VLAN ADDRESS.....	34
4.3.3 CONFIGURE MAC VLAN PORT.....	35
4.5 GUEST VLAN.....	36
4.5.1 VIEW THE GUEST VLAN INFORMATION.....	36
4.5.2 ENABLE THE GUEST VLAN.....	36
4.5.3 CONFIGURE GUEST VLAN PORT.....	37
4.6 PROTOCOL VLAN.....	37
4.6.1 VIEW THE PROTOCOL VLAN INFORMATION.....	37
4.6.2 ADD PROTOCOL GROUP.....	38
4.6.3 DELETE PROTOCOL GROUP.....	38
4.6.4 NEW GROUP BINDING.....	39
4.6.5 DELETE GROUP BINGDING.....	39
4.7 MVR.....	40
4.7.1 MVR INFORMATION.....	40
4.7.2 ENABLE MVR.....	40
4.7.3 SETTINGS MVR PORT.....	41
4.7.4 MVR GROUP ADDRESS.....	41
5 FAULT / SAFETY.....	42
5.1 ATTACK PREVENTION.....	42
5.1.1 ARP INSPECTION.....	42
5.1.1.1 VIEW ARP CONFIGURATION.....	42
5.1.1.2 ARP INSPECTION FUNCTION.....	43
5.1.1.3 DISABLE ARP INSPECTION CHEAT FUNCTION.....	43
5.1.1.4 TO MODIFY THE PORT ATTRIBUTE.....	44
5.1.2 port security.....	45
5.1.2.1 CONFIGURATION PORT SECURITY.....	45
5.1.2.2 MODIFY CONFIGURATION.....	45
5.1.3 anti DHCP attack.....	45
5.1.3.1 VIEW ANTI DHCP ATTACK CONFIGURATION.....	45
5.1.3.2 OPEN ANTO DHCP ATTACK FUNCTION.....	46
5.1.3.3 SETSTHE PORT TO DHCP NON TRUSED PORT.....	46
5.1.3.4 Off ANTI DHCP ATTACK FUNCTION.....	47
5.2 PATH DETECTION.....	48
5.2.1 path Detection.....	48
5.2.2 Tracert Detection.....	48

5.2.3 Cable Detection.....	49
5.3 DDOS PROTECTION.....	50
5.4 LOOPBACK DETECTION.....	51
5.4.1 ENABLE LOOPBACK DETECTION.....	51
5.4.2 choose the port to configure.....	51
5.5 STP.....	52
5.5.1 STP GLOBAL.....	52
5.5.1.1 VIEW THE STP GLOBAL INFORMATION.....	52
5.5.1.2 ENABLE THE STP GLOBAL INFORMATION.....	53
5.5.1.3 STP PORT SETTINGS.....	53
5.6 ACCESS CONTROL.....	54
5.6.1 ACL access control list.....	54
5.6.1.1 VIEW ACCESS CONTROL LIST.....	54
5.6.1.2 INCREASED ACCESS RULES.....	55
5.6.1.3 MODIFY CONFIGURATION.....	56
5.6.1.4 DELETE RULE.....	57
5.6.2 application ACL.....	58
5.6.2.1 VIEW APPLICATION ACL.....	58
5.6.2.2 INCREASED APPLICATION ACL.....	58
5.6.2.3 DELETE APPLICATION ACL.....	59
5.7 IGMP.....	60
5.7.1 VIEW IGMP CONFIGURATION.....	60
5.7.2 ACTIVE MULTICAST LISTENER FUNCTION.....	60
5.7.3 VIEW AND CONFIGURE ROUTER PORT.....	61
5.7.4 GROUP ADDRESS.....	61
5.7.5 FILTERING PROFILE.....	61
5.7.6 IGMP STATISTICS.....	62
5.7.7 DISABLE MULTICAST LISTENER FUNCTION.....	63
5.8 MLD.....	63
5.8.1 View MLD configuration.....	63
5.8.2 ACTIVE MULTICAST LISTENER FUNCTION.....	64
5.8.3 VIEW AND CONFIGURE ROUTER PORT.....	64
5.8.4 GROUP ADDRESS.....	65
5.8.5 FILTERING PROFILE.....	65
5.8.6 MLD STATISTICS.....	66
5.8.7 disable multicast listener function.....	67
6 SYSTEM MANAGEMENT.....	67
6.1 SYSTEM SETTINGS.....	67
6.1.1 management vlan.....	67
6.1.1.1 configuration Basic System Settings.....	67
6.1.1.2 System time synchronization.....	69
6.1.1.3 DHCPv6 client.....	69
6.1.1.4 IPv6 HTTPS.....	69
6.1.2 System restart.....	70
6.1.3 change password.....	70
6.1.4 System Log.....	71
6.1.5 Log Export.....	71
6.1.6 ARP table.....	72
6.1.7 MAC management.....	72
6.1.7.1 MAC address lookup.....	72

6.1.7.2 Add a static MAC address type.....	73
6.1.7.3 Remove the static MAC address type.....	75
6.2 SYSTEM UPGRADE.....	76
6.3 SYSTEM INFORMATION.....	77
6.3.1 System Log.....	77
6.3.2 CPU INFORMATION.....	77
6.5 CONFIGURATION MANAGEMENT.....	79
6.5.1 Configuration management.....	79
6.5.2 Restore factory Settings.....	81
6.6 SNMP.....	82
6.6.1 Check the SNMP.....	82
6.6.2 Activate the SNMP.....	83
6.6.3 To disable the SNMP.....	83
6.6.4 Activate the TRAP.....	84
6.6.5 Disable the TRAP.....	84
6.6.6 CHANGE of community.....	84
6.6.7 Added the SNMP TRAP service host.....	85
6.6.8 Delete the SNMP TRAP service host.....	86
6.7 RMON.....	87
6.7.1 view ROMN configure information.....	87
6.7.2 configure ROMN type.....	87
6.7.3 change ROMN type.....	88
6.7.4 Delete the configured rule.....	89
7 QOS.....	90
7.1 PRIORITY SCHEDULE.....	90
7.1.1 view the priority schedule.....	90
7.1.2 The configuration global settings OF SP.....	90
7.1.2.1 THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP.....	90
7.1.2.2 THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP ADD WRR.....	90
7.1.3 The configuration global settings OF DSCP.....	92
7.1.3.1 THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND SP.....	92
7.1.3.2 THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND WRR.....	93
7.1.4 Editing the DSCP values.....	95
8 EEE.....	97
8.1 EEE.....	97
8.2 ENABLE 802.3AZ EEE SETTINGS.....	97

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 192.168.1.200, the default subnet mask of 255.255.255.0). Run WEB browser, in the address bar enter http://192.168.1.200 Enter, enter the user name and password -admin/admin, click "Login" button or directly enter into the WEB management



Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:

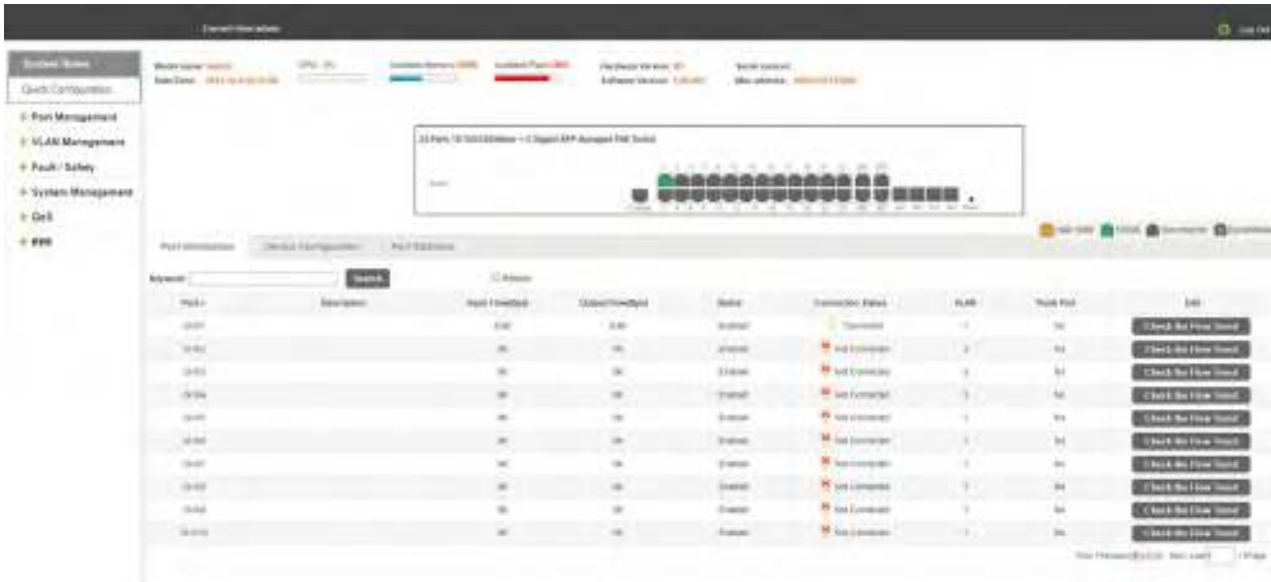


Figure 1-2: switch WEB management page Home

2 QUICK CONFIGURATION

The quick configuration contains five chapters. Click on "Quick Configuration", can quickly to Configuration of the device commonly used functions, such as a VLAN, Trunk port ,port class ,SNMP and others. According to the steps, the configurations of step by step, also can choose configuration.

2.1 VLAN SETTING

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 2-1: VLAN Setting

2.2 MODE

Click on the "Quick Configuration" "port mode" view switches has been configured trunk port information:

Notice:

- 1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected;
- 2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of tap type (Native VLAN to untag type transmission) , generally used in conjunction with other switches in the network;
- 3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit data frames both tag type and untag type;
- 4.When a trunk or hybrid port mode , it will only allow the default Native VLAN through with untag types of data frames.

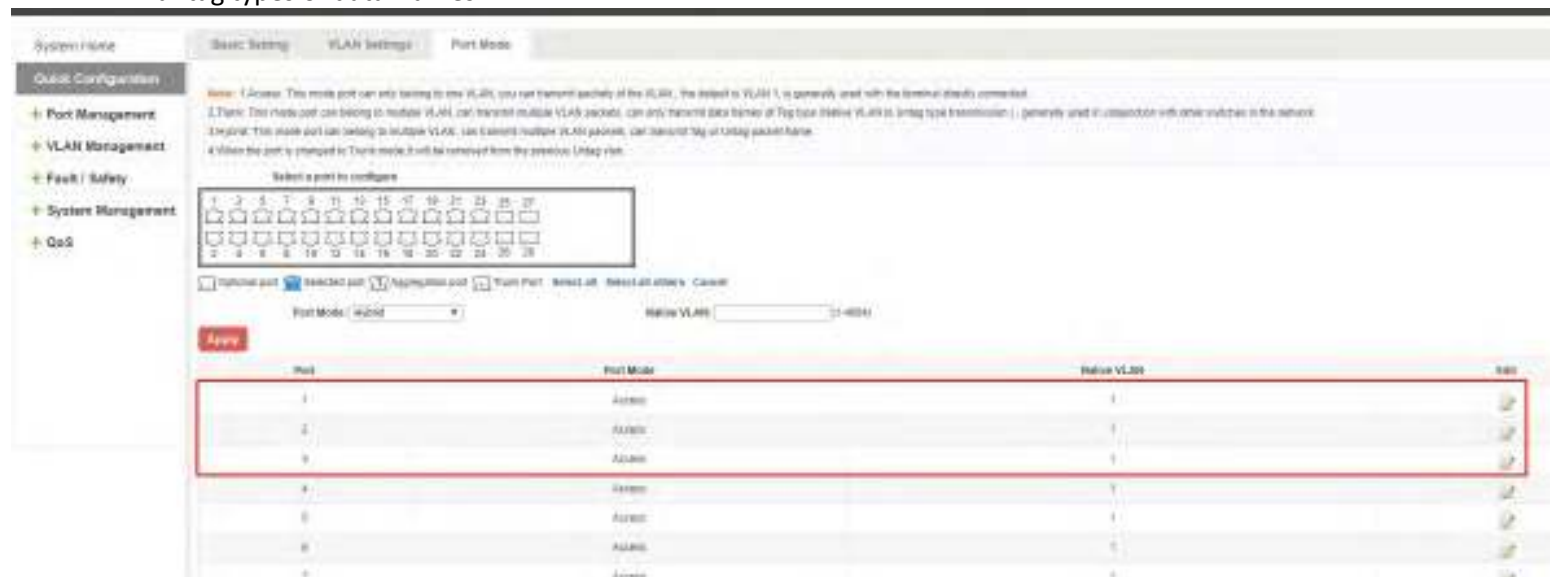


Figure 2-2: Port mode Setting

3 PORT MANAGEMENT

3.1 BASIC SETTINGS

3.1.1 CHECK THE PORT CONFIGURATION

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

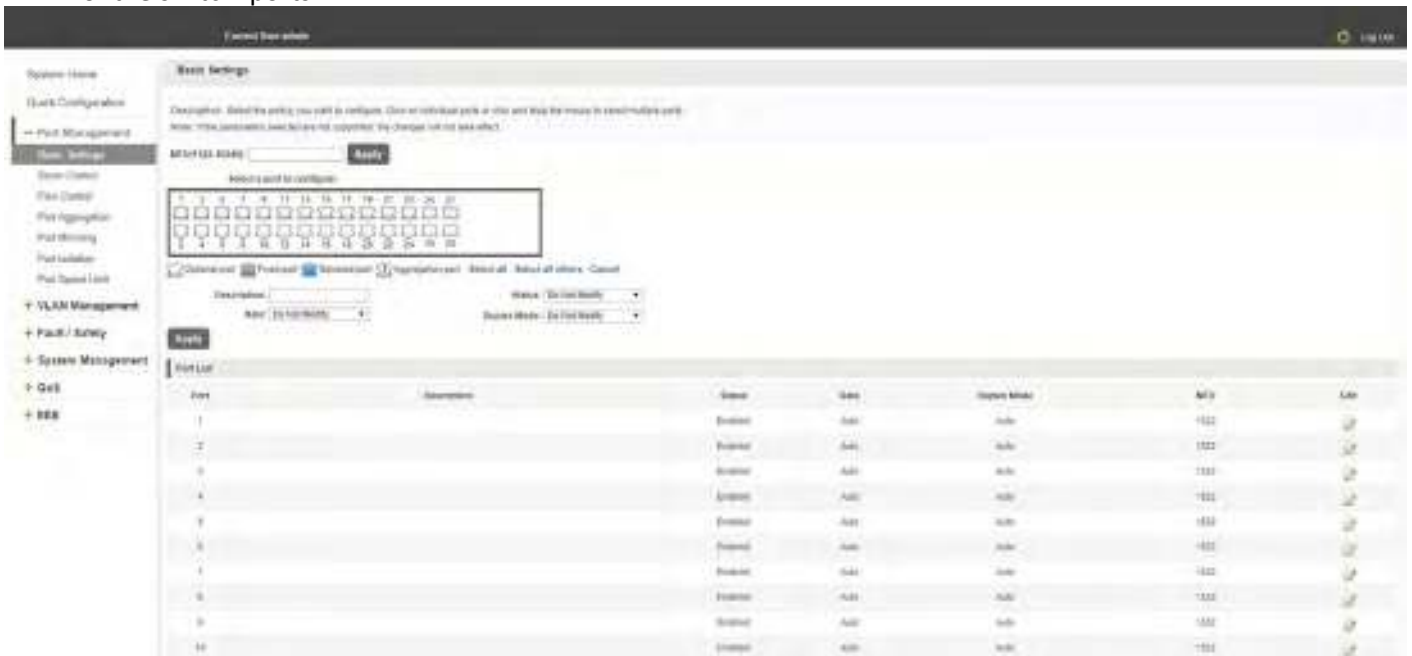


Figure 3-1: Port list information

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;

3.1.2 CONFIGURING PORT PROPERTIES

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

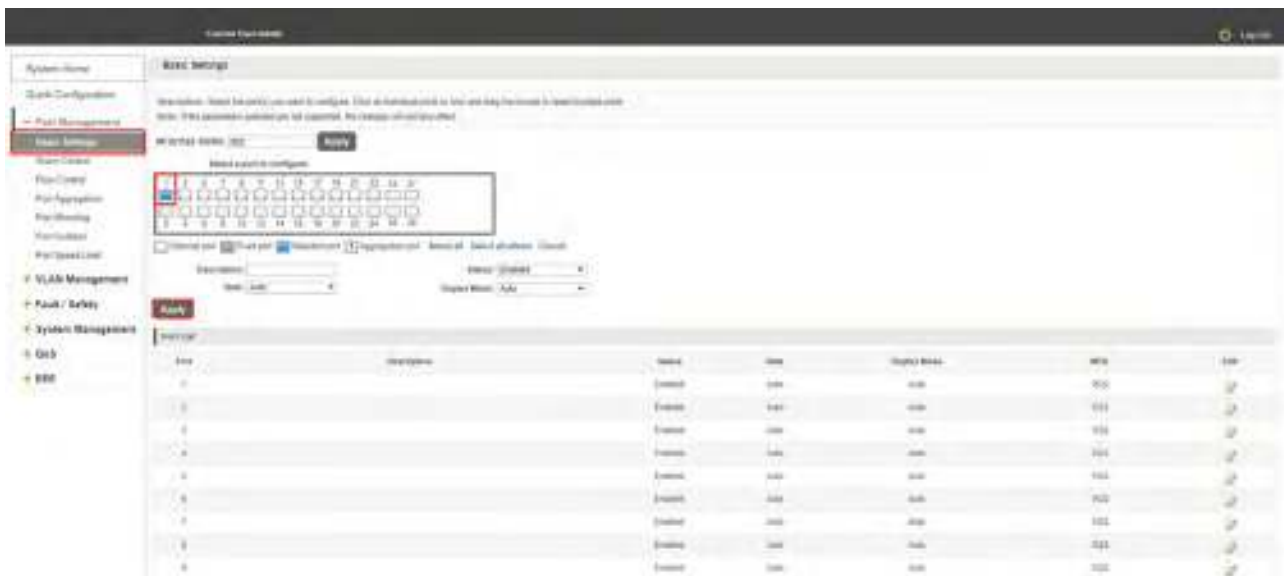


Figure 3-2: Port Properties configuration of FIG.

To configure port properties as follows:

Step1:Click the "Edit" icon ,step2:In the Port Properties configuration page Fill / select the value to be configured,step3:Click the "Apply" button to complete the configuration.

3.2 STORM CONTROL

3.2.1 CHECK THE PORT SETTINGS STORM

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



Figure 3-3: 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 64, the system automatically matches similar multiples of 64.
 - 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.

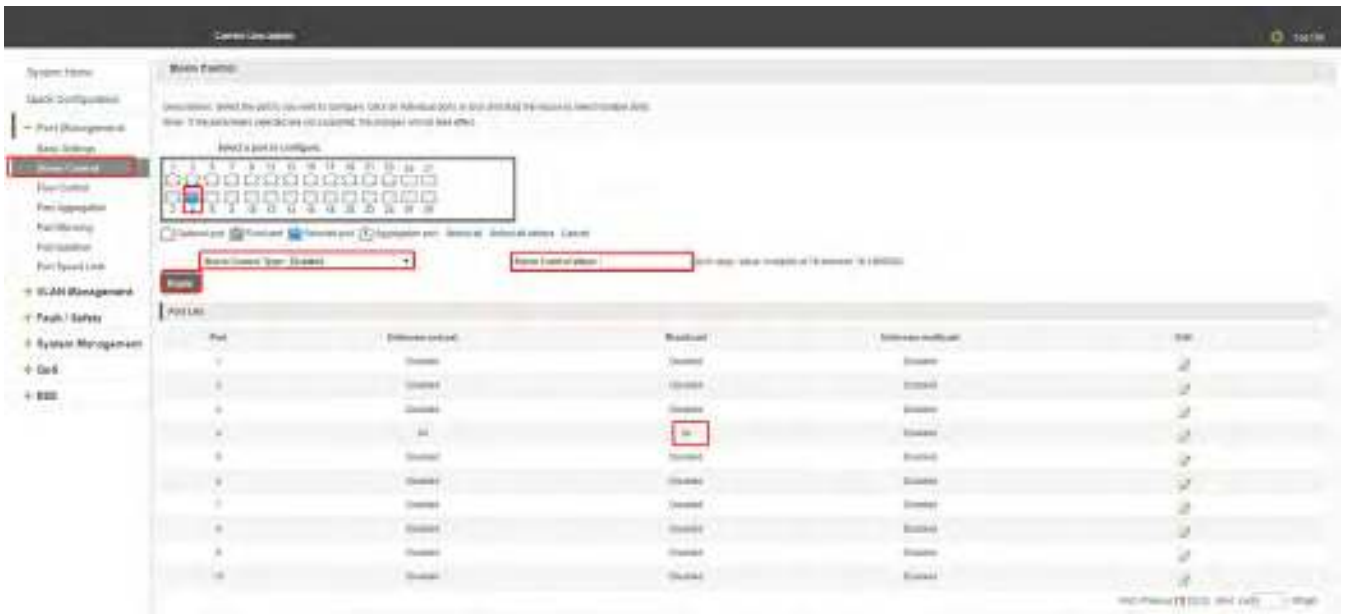


Figure 3-4: Configuring Storm Control information

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



Figure 3-5: Bulk edit configuration information

After the selected ports in the Storm Control category, set the unicast, multicast, broadcast value, such as setting the port number 1 unicast storm control is 1008,. Click Save Settings.

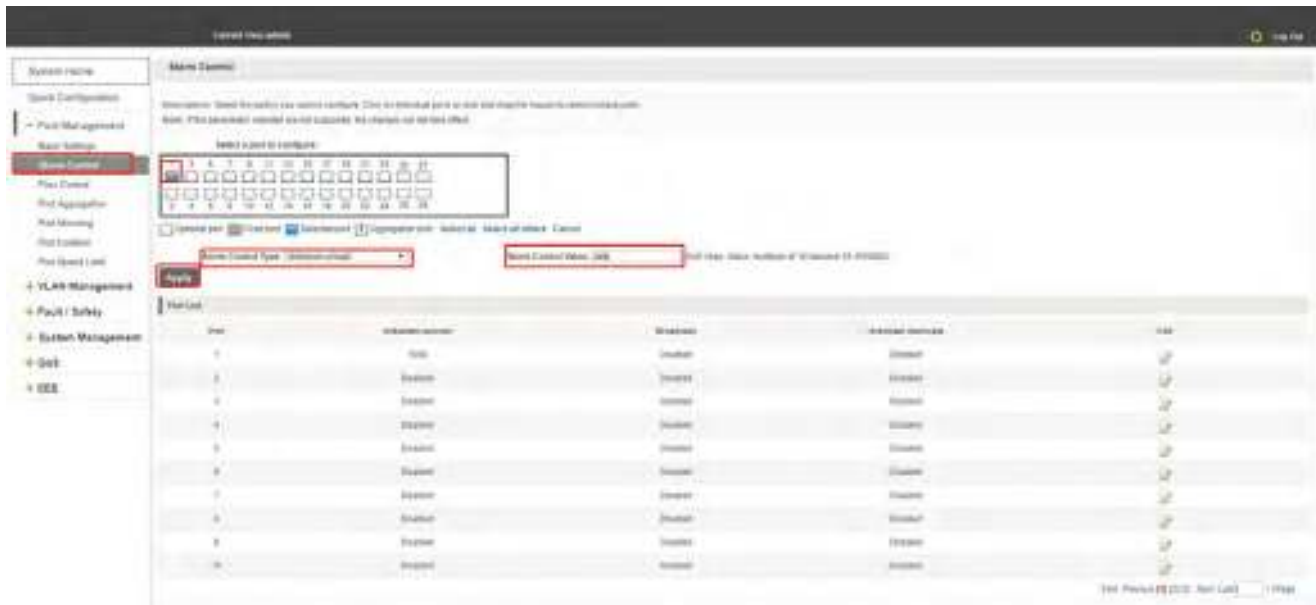


Figure 3-6: Configuring Storm Control information

After the configuration, as shown below:

Port	Storm Control Type	Storm Control Mode	Storm Control Action	Rate
1	Storm	Storm	Storm	100
2	Storm	Storm	Storm	100
3	Storm	Storm	Storm	100
4	Storm	Storm	Storm	100
5	Storm	Storm	Storm	100
6	Storm	Storm	Storm	100
7	Storm	Storm	Storm	100
8	Storm	Storm	Storm	100
9	Storm	Storm	Storm	100
10	Storm	Storm	Storm	100
11	Storm	Storm	Storm	100
12	Storm	Storm	Storm	100
13	Storm	Storm	Storm	100
14	Storm	Storm	Storm	100
15	Storm	Storm	Storm	100
16	Storm	Storm	Storm	100
17	Storm	Storm	Storm	100
18	Storm	Storm	Storm	100
19	Storm	Storm	Storm	100
20	Storm	Storm	Storm	100
21	Storm	Storm	Storm	100
22	Storm	Storm	Storm	100
23	Storm	Storm	Storm	100
24	Storm	Storm	Storm	100

Figure 3-7: Configuration successfully Storm Control information flow control

3.3 FLOW CONTROL

Click "Port Management" "configuration information flow control "Flow Control" view of the switch:

Figure 3-8: Flow Control Information

3.3.1 CONFIGURING FLOW CONTROL

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

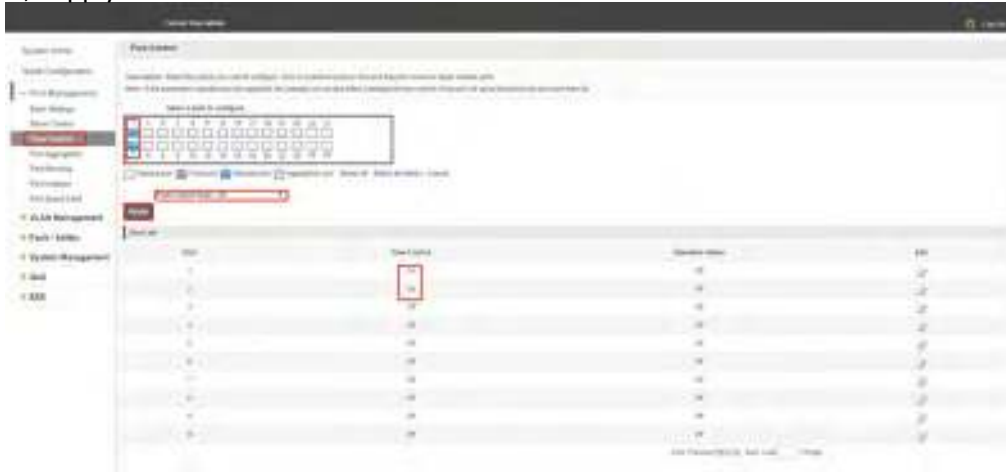


Figure 3-9: Open port flow control function

Open port traffic control, follow these steps:

Step1:Select Open port traffic control;step2:Select Open in "Flow control type" on;step3:Click "Apply".

View Configuration list to display configuration is successful:

Port	Flow Control	Flow Control Type	Flow Control Status
1	On	On	On
2	On	On	On
3	On	On	On
4	On	On	On
5	On	On	On
6	On	On	On
7	On	On	On
8	On	On	On
9	On	On	On
10	On	On	On

Figure 3-10: 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":

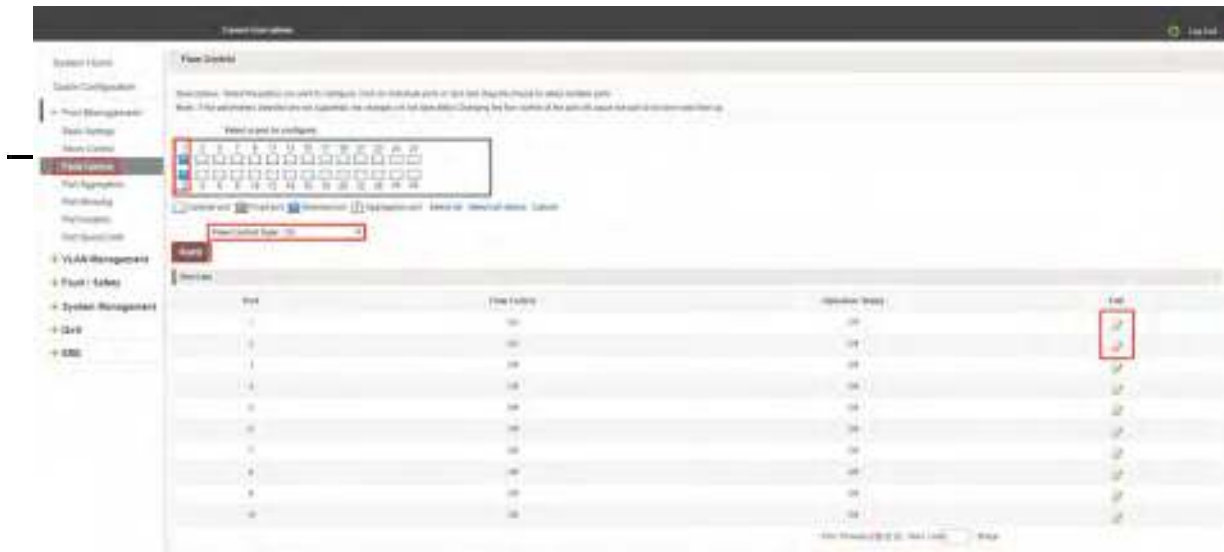


Figure 3-11: Close the port flow control

3.4 PORT AGGREGATION

3.4.1 VIEWING PORT AGGREGATION CONFIGURATION

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



Figure 3-12: 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 can not ATTACH after configuration.

3.4.2 ADD PORT AGGREGATION

Enter aggregation port number, select the desired aggregation port, select aggregation type, click "Apply"



Figure 3-13: Port Aggregation Configuration area

Increase port aggregation, follow these steps:

Step1: Select the option to load the shunt in the load balancing list.
step2: Enter the number in the "Aggregation number" in.
step3: Select the aggregated ports in the panel.
step4: Select the aggregation type.
step5: Click the "Apply" button to complete the configuration.

3.4.3 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 3-14: To modify the port aggregation

Modify Link Aggregation Procedure:

Step1:In the "Aggregation List Click to modify the right of the port aggregation,step2:In the port aggregation configuration page to modify the load balancing type and click Next to "Save".step3:Select the port to be added to the aggregation port.step4:Click the "Apply" button to complete the configuration.

3.5 PORT MIRRORING

3.5.1 PORT MIRRORING CONFIGURATION

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



Figure 3-15: 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 can not be used as the destination port and source port;
- 2.Destination port and source port can not be the same;
- 3.Same group mirroring group can have only one destination port.

3.5.2 ADD PORT MIRRORING GROUP

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



Figure 3-16: Add port mirroring group

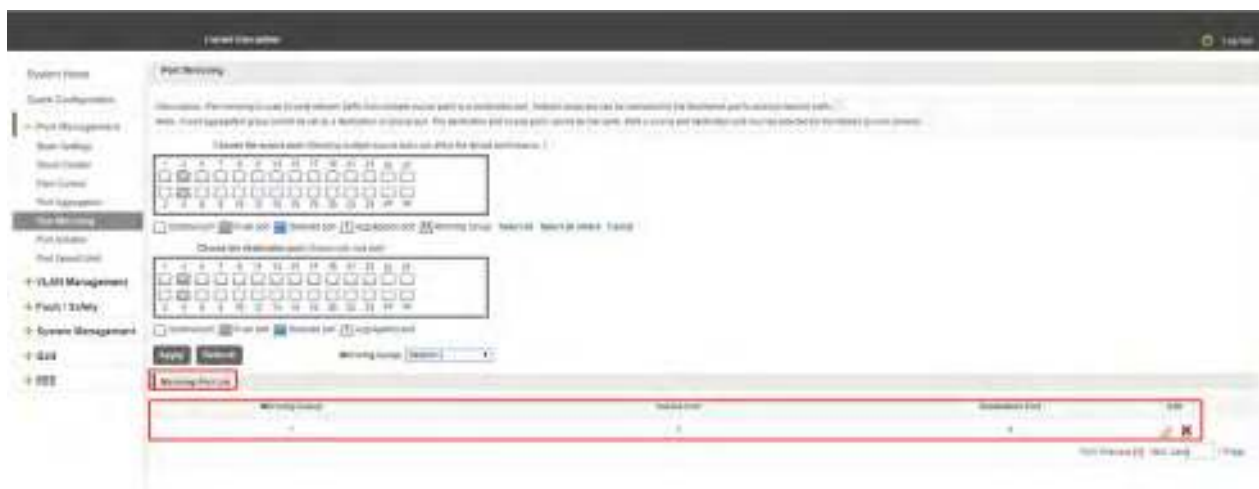


Figure 3-17: Add port mirroring group results

Port mirroring configuration steps are as follows:

Step1:Select "Source Port",step2:Select "Destination Port",step3: select mirroring group ,step4,Click"Apply".

Configuration instructions:

- 1.On the switch can be configured 7 mirroring group.
- 2.Aggregated port mirroring can not be configured are shown in gray in the panel.
- 3.Has been selected port mirroring port, displayed in the faceplate is gray.

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



20

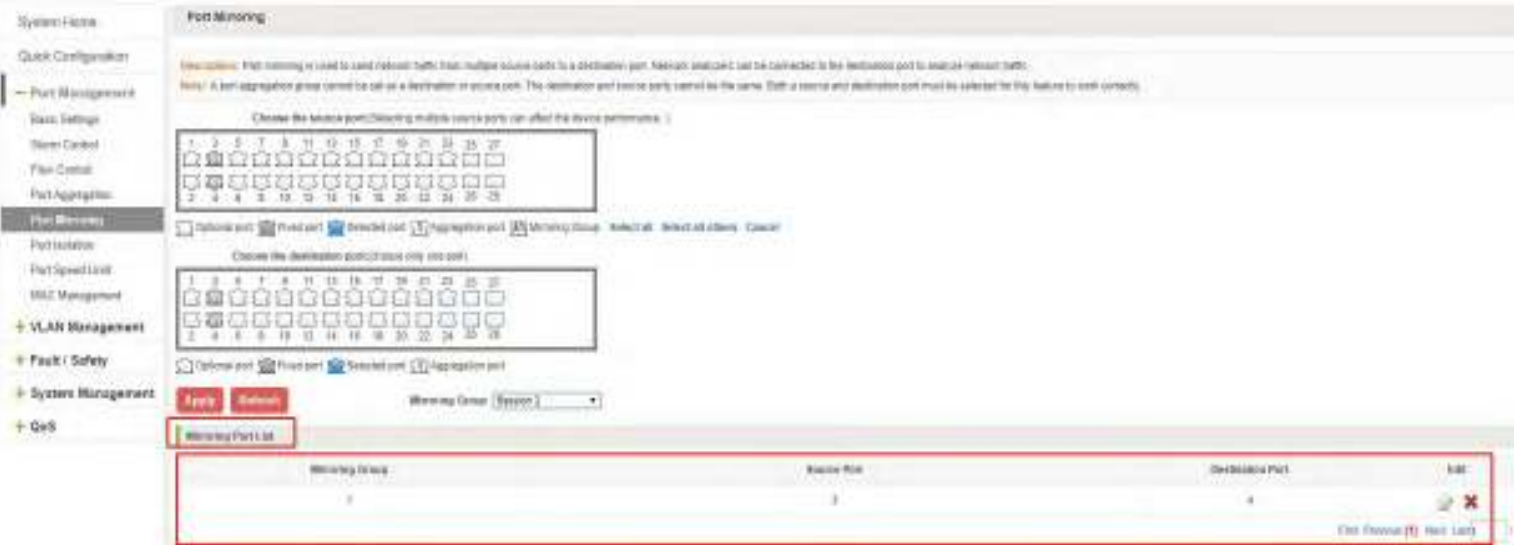


Figure 3-19: Modify successful port mirroring group
 Modify the port mirroring configuration steps are as follows:

3.5.4 DELETE A PORT MIRRORING GROUP

Remove some ports from multiple source ports and save them.

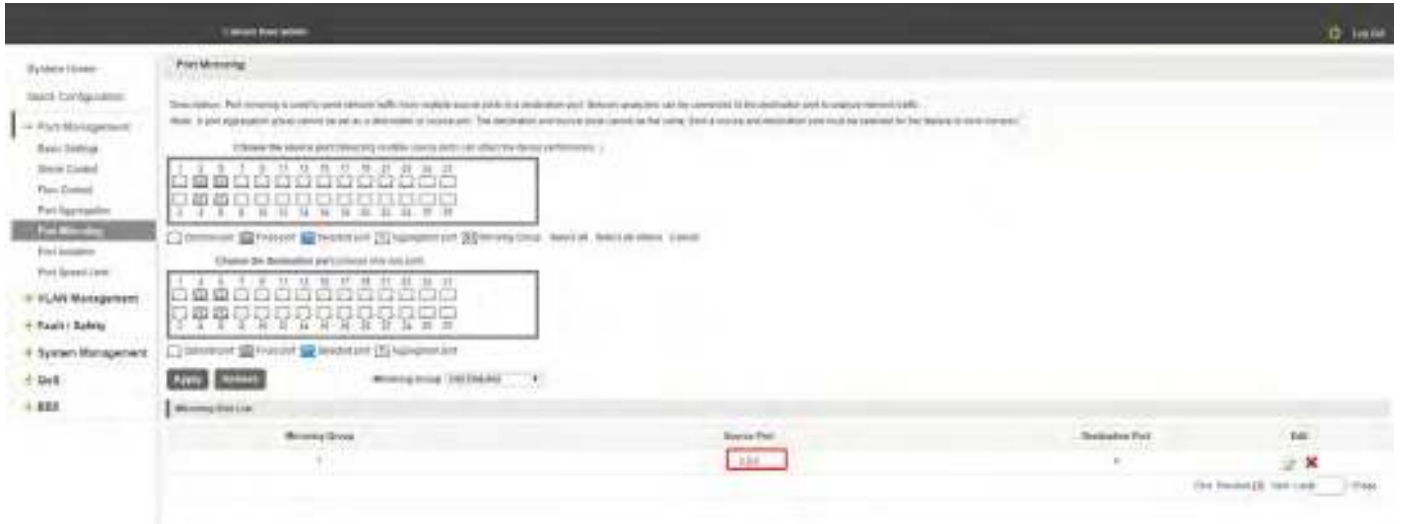


Figure 3-20: Delete a port mirroring group

Remove the current port mirroring, click the " " button in the action bar, click on the source port and destination port, respectively cancel the currently selected port, and click Save. (Note: The current version supports only one port mirroring group)

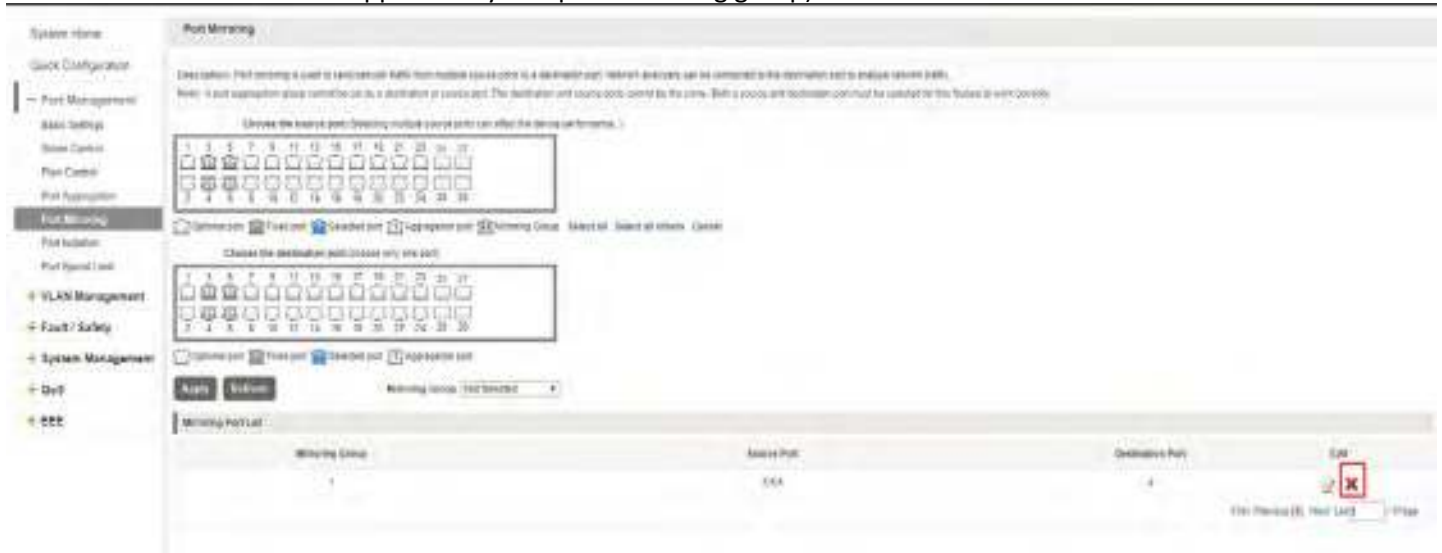


Figure 3-21: Delete port mirroring group

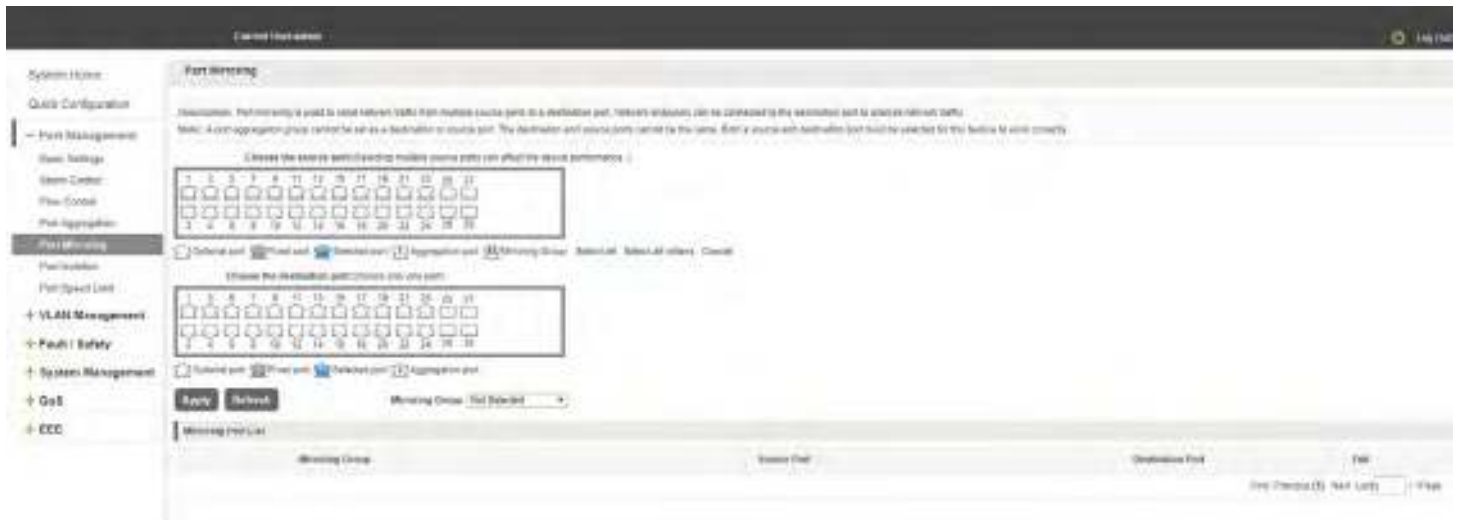


Figure 3-22: Deleted successfully port mirroring

Remove port mirroring configuration steps are as follows:

Step1:In the image you want to modify the operation of the group column, click “”; step2:In the panel, click Cancel the source port, destination port and then click Cancel;step3:In the panel, click Cancel the source port, destination port and then click Cancel;step4:Click "Apply"

3.6 PORT ISOLATION

3.6.1 VIEW PROT ISOLATION

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

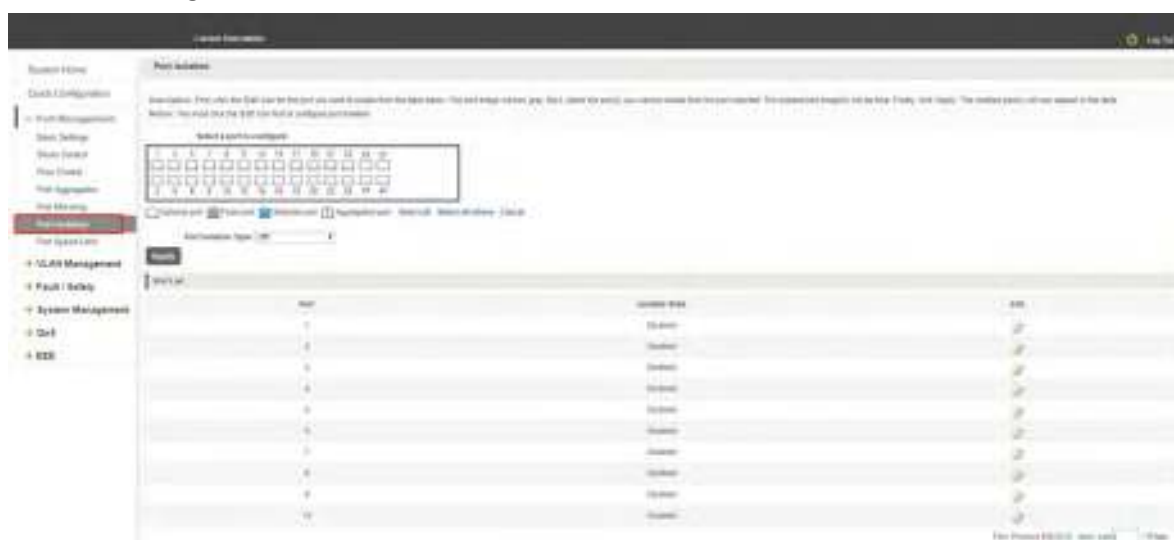


Figure 3-23: View the port isolation

3.6.2 CONFIGURE THE PROT ISOLATION

Select the port(s) you want to isolate from each other. Click the port isolation type button “ON”, then click “Apply”. We can view the port you configure ok.

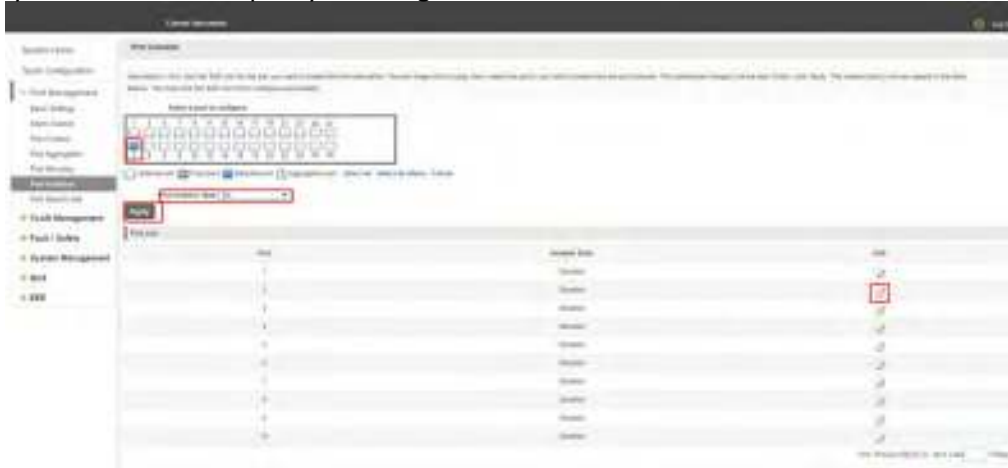


Figure 3-24: Configure the port isolation

3.6.3 EDIT THE PORT ISOLATION

Click “Edit”, you can change the port isolation type then click the button “Apply”.

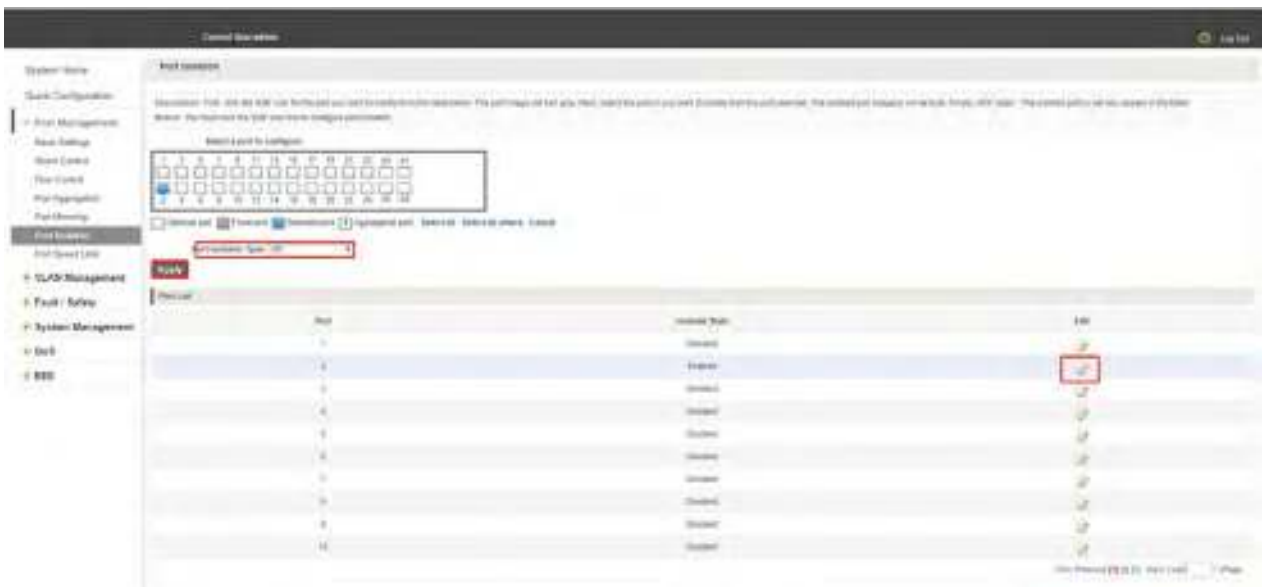


Figure 3-25: Edit the port isolation

3.7 PORT SPEED LIMIT

3.7.1 VIEW PORT RATE LIMITING

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

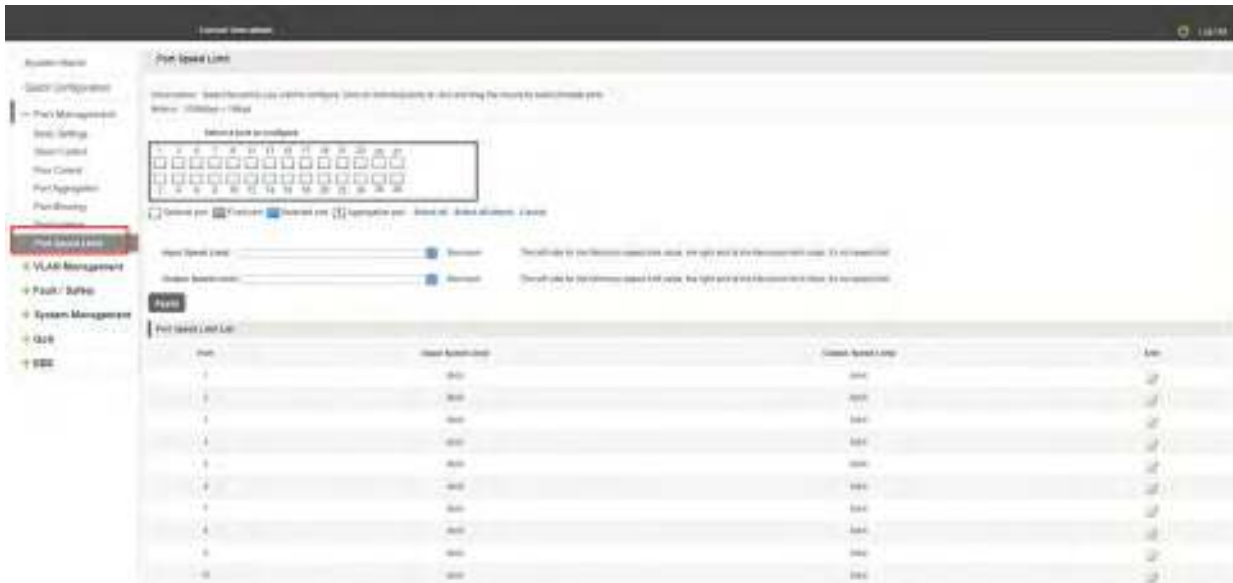


Figure 3-26: View Rate Configuration information

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;

3.7.2 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.

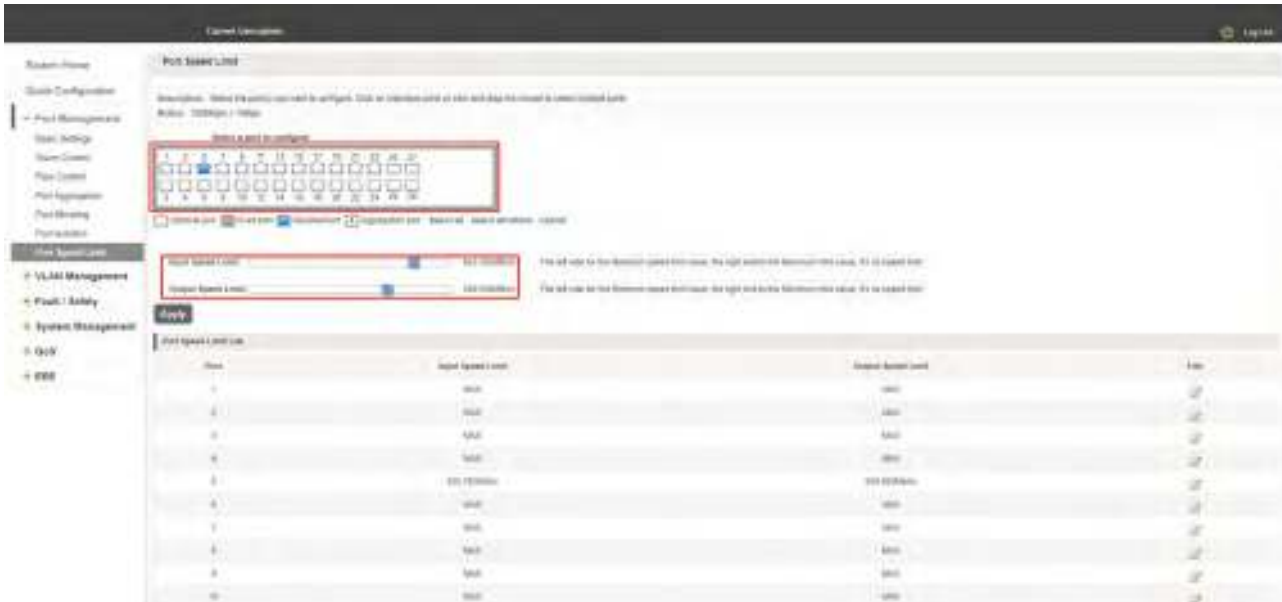


Figure 3-27 Configure port rate limiting entrance



Figure 3-28: Port entrance speed limit results

Entrance port rate limiting configuration steps are as follows:

- Step1: Click on the right side of the port “🔌” Icon or select multiple icons;
- step2:Set rate limiting strip port value;
- step3:Click the lower right corner "Apply" button to complete the configuration.

3.7.3 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, "Apply" to complete the operation.

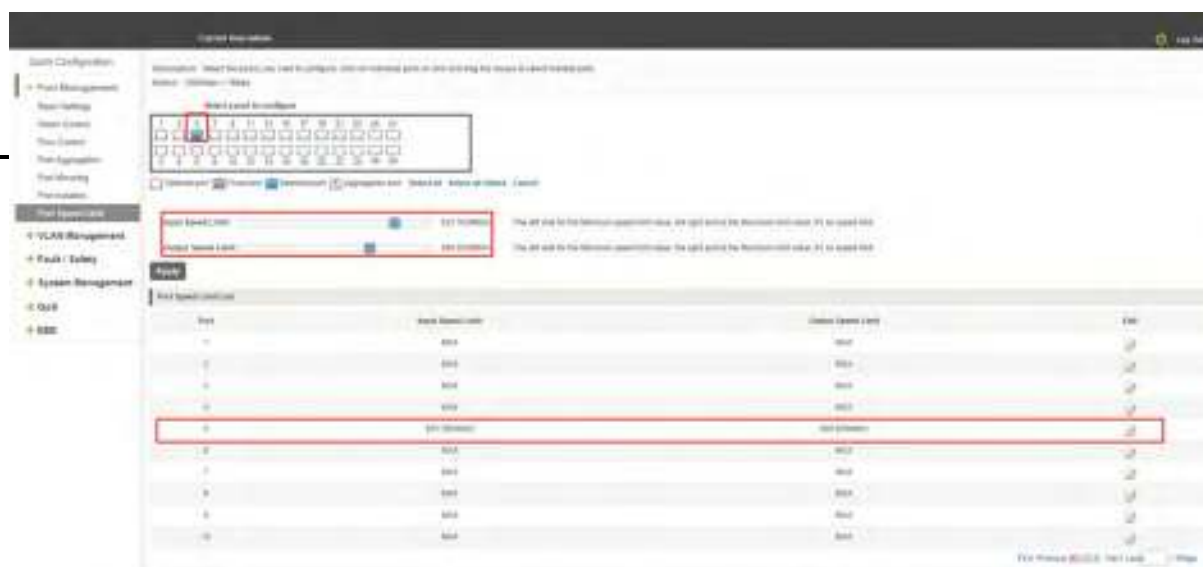


Figure 3-29: Remove the port speed limit

Remove uplink port rate limiting steps are as follows:

Step1: Click on the right side of the port  icon; step2: In the area of the port rate configuration value rate strip pulled to the far right; step3: Click the "Apply" button to complete the configuration.

4 VLAN MANAGEMENT

4.1 VLAN MANAGEMENT

4.1.1 CHECK VLAN CONFIGURATION INFORMATION

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



Figure 4-1: VLAN configuration information

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

- 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.

4.1.2 ADDING A VLAN

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



Figure 4-2: Adding a VLAN

Adding a VLAN, follow these steps:

Step1:Click "NEW vlan" connection;

step2:Value added VLAN ID of the page to fill in and select a tag or untag port to add to the VLAN:

step3:Click the "Apply" button to complete the configuration.

4.1.3 REMOVE VLAN

4.1.3.1 SINGLE VLAN DELETE

To delete the selected VLAN, click the "X" button to delete the selected VLAN, if the vlan have port please remove the port from the vlan fist.



Figure 4-3: Delete a single VLAN

4.1.3.2 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; notice: if the vlan have port please remove the port from the vlan first else the system will be delete the vlan have no ports.

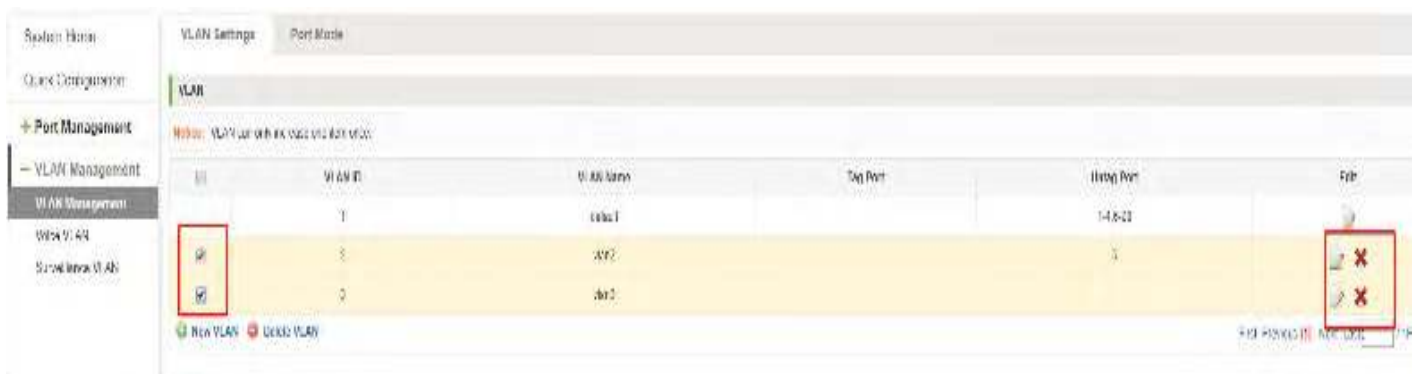


Figure 4-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

- Step1: Select you want to delete VLAN check box;
- Step2: Click on the bottom left "Delete VLAN" connection;
- Step3: Confirm delete.

4.1.4 EDITING VLAN

4.1.4.1 CHANGE PORT TO A VLAN

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

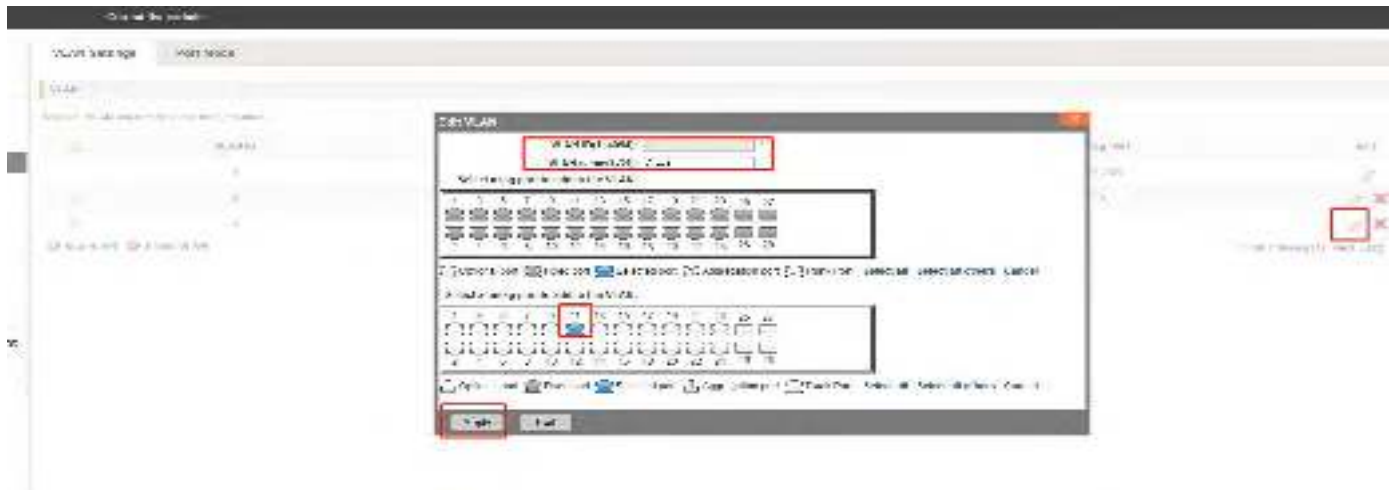


Figure 4-5: Change the port to the VLAN

Add the port to the VLAN, follow these steps:

Step1: Click "🔍" icon.

step2: Selected to join the ports in the port panel.

step3: Click the lower right corner "Apply" button to complete the configuration.

4.1.4.2 TO REMOVE THE PORT FROM A VLAN

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

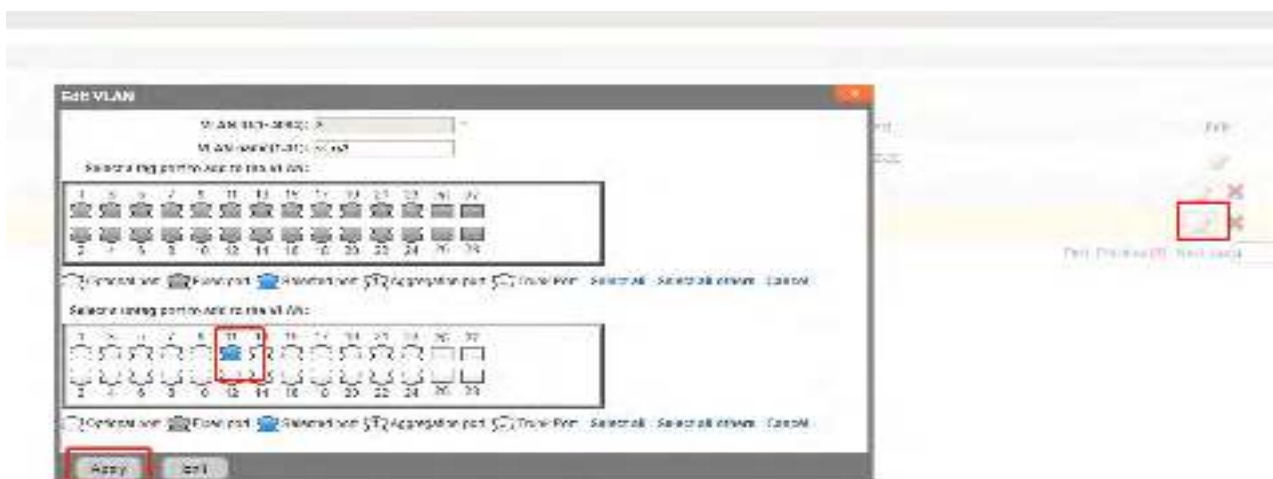


Figure 4-6: To remove the port from the VLAN.

Procedure to remove the port from VLAN as follows:

Step1:Click on the icon “ ”;

step2:Remove the port to the vlan on the port panel;

step3:Click on the lower right corner of the "Apply" button to complete the configuration;

4.1.5 VIEW PORT MODE

Click on the "Vlan Management" "port mode" view switches has been configured trunk port information:

Notice:

1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected;

2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of tap type (Native VLAN to untag type transmission) , generally used in conjunction with other switches in the network;

3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit data frames both tag type and untag type;

4.When a trunk or hybrid port mode , it will only allow the default Native VLAN through with untag types of data frames.



Figure 4-7: View port mode information

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

1.the port default mode is hybrid;

2.The native default is vlan 1;

4.1.6 CHANGE THE PORT MODE IS TRUNK

Select one or more ports you want to change the mode :



Figure 4-8: Trunk

The steps to change the port mode as follows:

Step1:Select one or more ports to configure;

step2:Change the port mode from hybrid to trunk;

step3:Set this port native VLAN that you have created;

step4:Click the “Save”,complete the change.

4.1.7 CHANGE THE PORT MODE IS ACCESS

Select one or more ports you want to change the mode :

Notice:When you want to create a new vlan ,the port mode is access can not be set up tag.



Figure 4-9: Change the port mode is access

4.2 VOICE VLAN

4.2.1 VIEW THE VOICE VLAN CONFIGURATION

Click the “VLAN Management” “Voice VLAN”, you can view the voice vlan global information:

The screenshot shows a web interface for configuring Voice VLAN. On the left is a sidebar menu with the following items: 'System Home', 'Quick Configuration', '+ Port Management', '- VLAN Management', 'VLAN Management', 'Voice VLAN' (highlighted with a red box), and 'Surveillance VLAN'. The main content area has a top navigation bar with four tabs: 'Voice VLAN Global' (selected), 'Voice VLAN Port', 'Voice VLAN OUI', and 'Voice device address'. Below the tabs, the 'Voice VLAN Global' section contains a note: 'Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.' The configuration fields are: 'Voice VLAN State' with a toggle switch set to 'OFF', 'Voice VLAN ID(2-4094):' with an empty text box, 'Voice VLAN CoS:' with a dropdown menu showing '5', and 'Aging Time(1-65535):' with a text box containing '20' and a 'min' unit label. A red 'Apply' button is located at the bottom left of the configuration area.

Figure 4-10: View the voice vlan configuration

4.2.2 ENABLE THE VOICE VLAN

Click the button “” turn ON, enable the voice vlan and input a existed vlan. Last click “Save” button. Voice VLAN ID and Surveillance VLAN ID can not be the same.



Figure 4-11: Enable the voice vlan

4.2.3 CONFIGURE THE VOICE VLAN PORT

Click the “VLAN Management”→“Voice VLAN”→“Voice vlan port ”Configuration the voice vlan port you should select the port mode is trunk or hybrid ,the port join in the voice vlan mode type can be untag or tag or manual.



Figure 4-12: Enable voice vlan on port

When you want to change port mode or state add to VLAN ,we can click “Edit”button,change the port state or mode ,when you complete configuration,click “Save”.

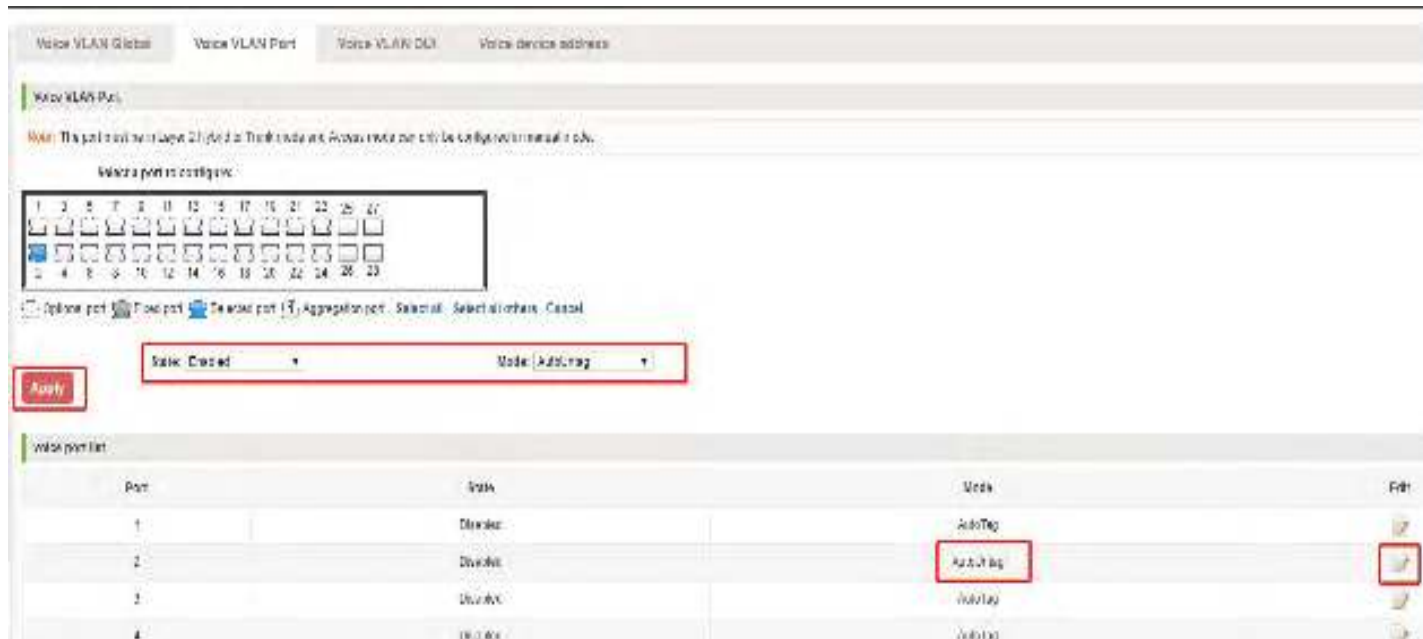


Figure 4-13: Edit port state or mode

4.2.4 VOICE VLAN OUI TABLE

Click the “VLAN Management”→“Voice VLAN”→“Voice vlan OUI” we can view the default voice vlan oui table:



Figure 4-14: Voice vlan OUI table

Add the oui entry,enter valid address and mask,click “Save”:

Notice:

- 1.The max entry is 16.;
- 2.The oui address valid only for unicast addresses;
- 3.The mask can be all F, but 0 cannot be in front of F.



Figure 4-17: View the surveillance vlan device

4.3.2 CONFIGURE SURVEILLANCE VLAN

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



Figure 4-18: configure surveillance VLAN

To configure the surveillance VLAN steps as follows:

- Step1:in the surveillance VLAN TEXT BOX ,click ON the "OFF" to "ON",
- Step2:in the surveillance VLAN ID text box,enter the ID,such as 5;
- step3:in the surveillance VLAN COS text box,choose 5(default is 5);
- step 4:in the aging time text box,enter aging time ,such as 500(default is 720min);
- step 5:click on save;

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

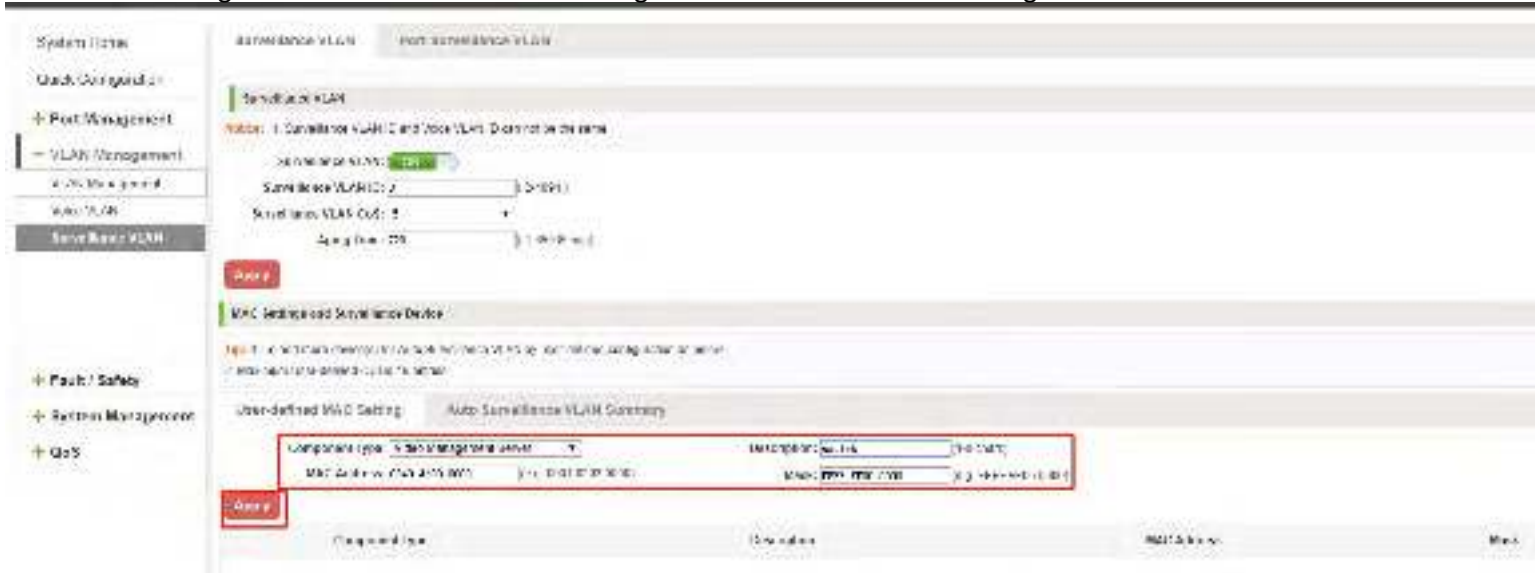


Figure 4-19: configure the user-defined mac settings

To configure the surveillance VLAN steps as follows:

Step1:in the component type EXT BOX,choose video management server ;

Step2:in the description text box ,enter guest;

step 3: in the mac address text box,enter mac address ,such as 0402.0011.3120;

step4 : in the mask text box ,enter the mask ,such as FFFF.F000.000;

step 5:click on save;

4.3.4 PROT SURVEILLANCE VLAN

Click on the navigation bar "VLAN Management" "surveillance VLAN" "Port Surveillance VLAN" to view the information:



Figure 4-20: view the port surveillance vlan information

Configuration the port surveillance vlan ,set the port stats and mode :

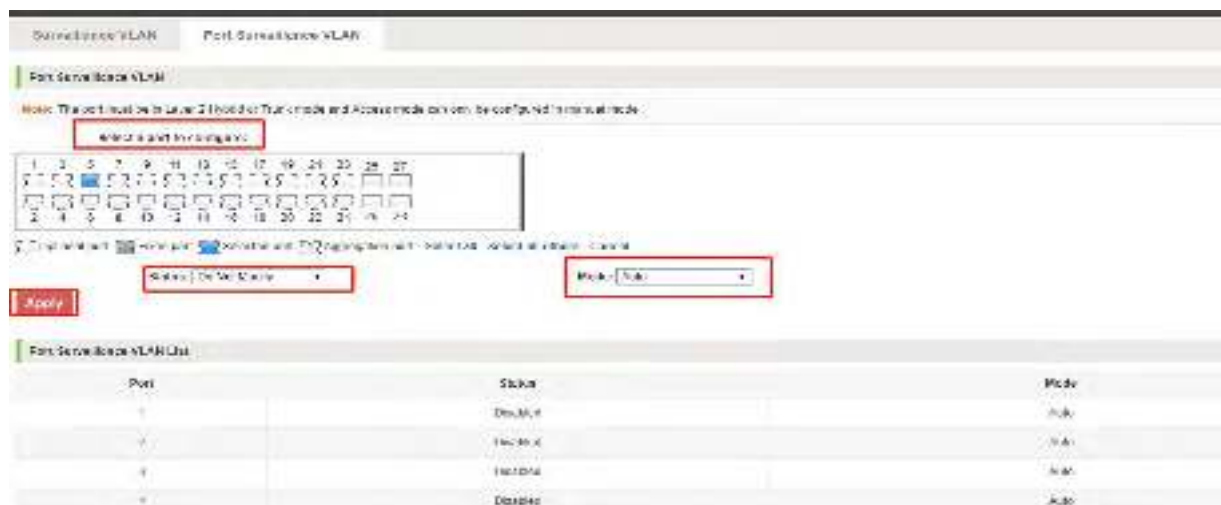


Figure 4-21: configure the port surveillance vlan

5 FAULT / SAFETY

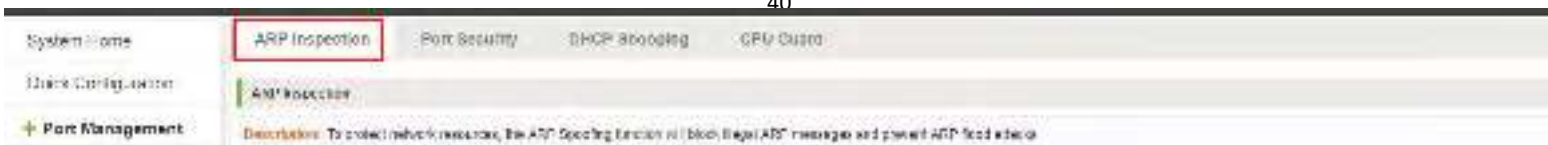
5.1 ATTACK PREVENTION

5.1.1 ARP INSPECTION

5.1.1.1 VIEW ARP CONFIGURATION

Click the "Fault/Safety" "Attack Prevention" "ARP Inspection" to check the current switches has been configured for ARP information:

Figure 5-1: View port ARP configuration information



5.1.1.2 ARP INSPECTION FUNCTION

In the ARP inspection configuration , select a or multiple ports set up the rate limit、trust status、Rate Packet Limit、Validate、Destination MAC Check、Source MAC Check、IP Check、Allow Zeros ,then click the "Apply" button to complete the configuration prevent ARP deception .

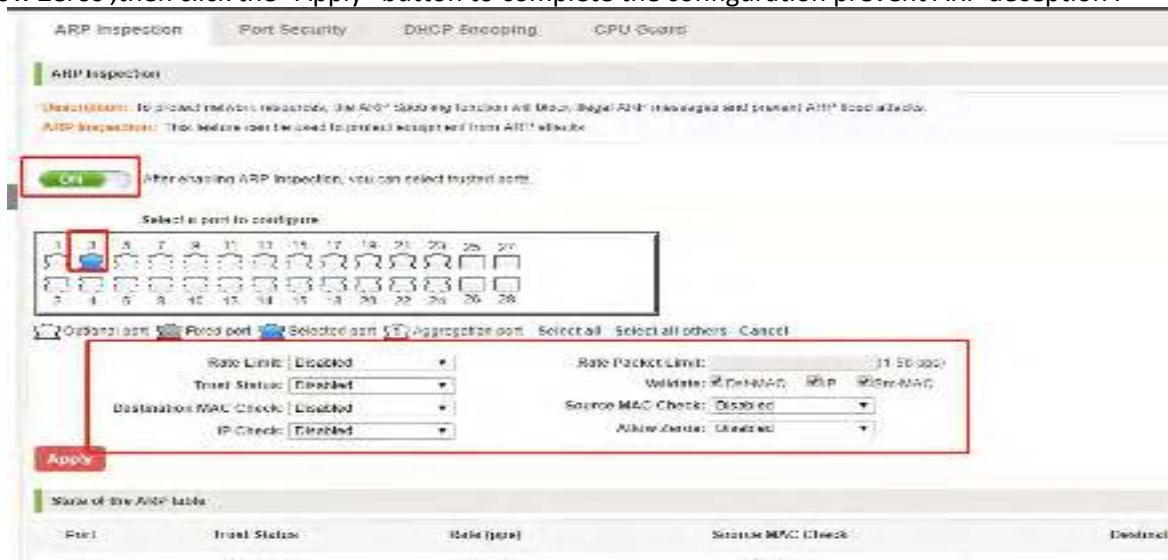


Figure 5-2: ARP inspection configuration



Figure 5-3: ARP inspection status table

5.1.1.3DISABLE ARP INSPECTION CHEAT 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.

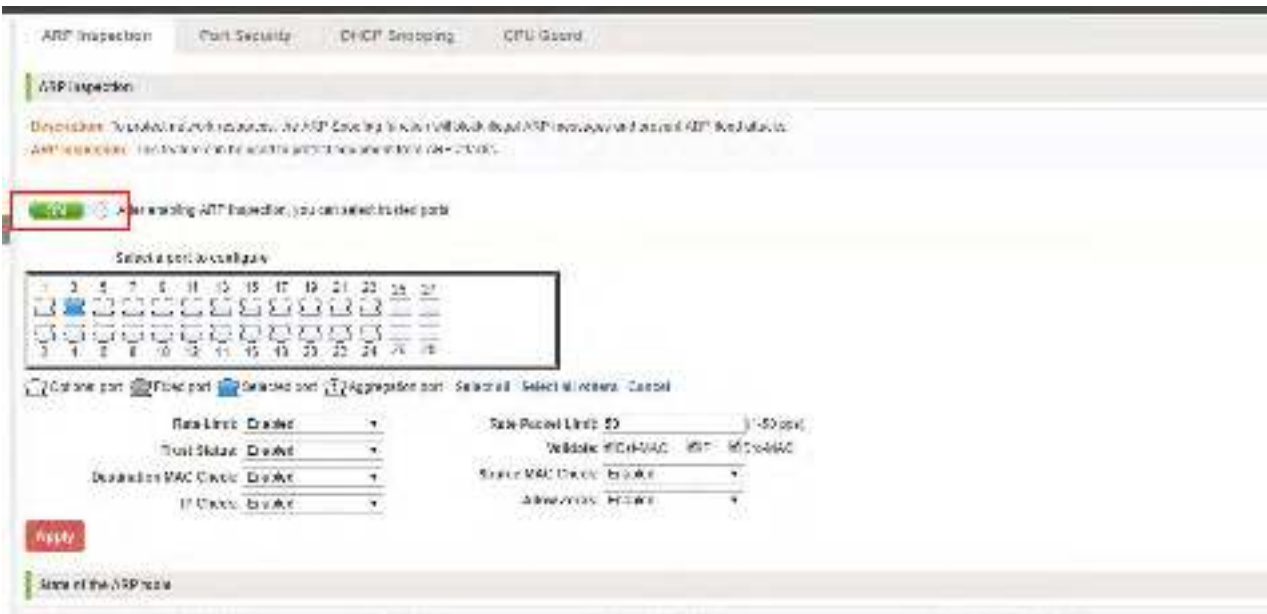


Figure 5-4: Disable ARP spoofing function

5.1.1.4 TO MODIFY THE PORT ATTRIBUTE

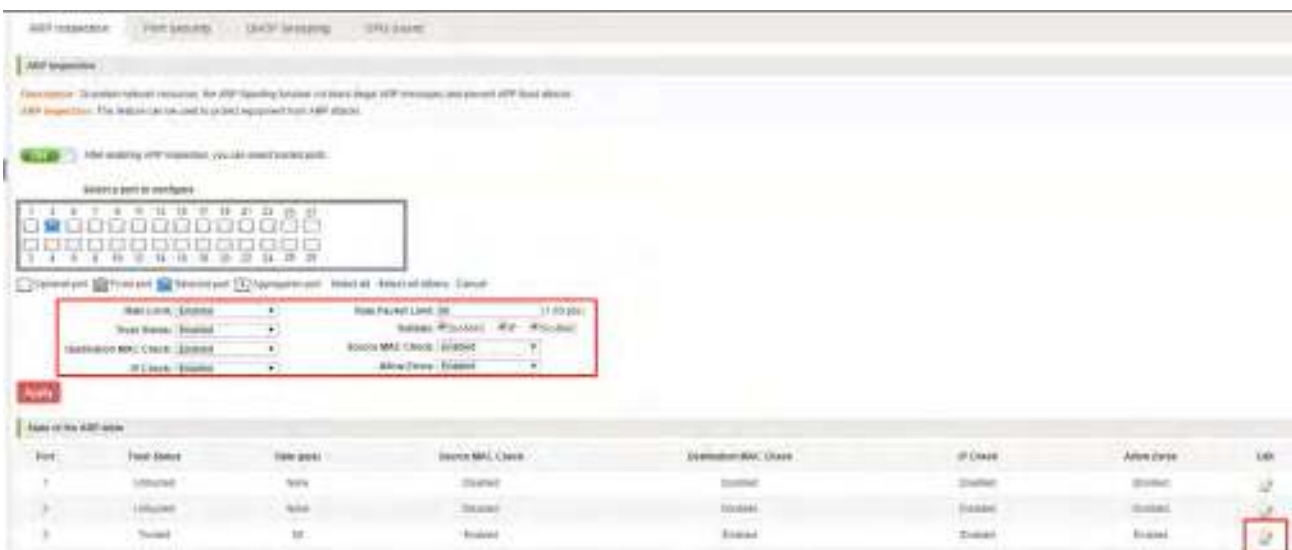


Figure 5-5: To modify the port attribute

5.2 PATH DETECTION

5.2.1 PATH DETECTION

Click the "Fault/Safety" "path Detection" can view the ipv4 or ipv6 Path Detection configuration:



Figure 5-12: Path detection information

5.2.2 TRACERT DETECTION

Click the "Fault/Safety" "Tracert Detection" can view the ipv4 or ipv6 Tracert Detection" Tracert Detection configuration:

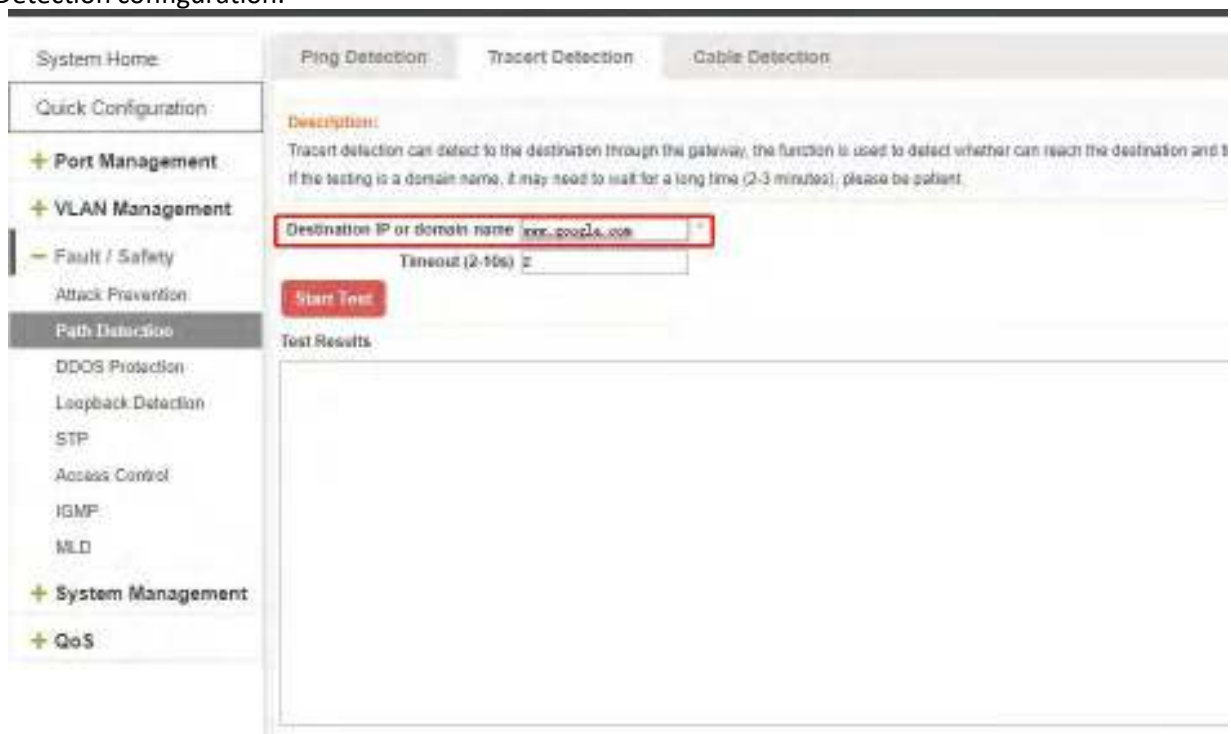


Figure 5-13: Tracert detection information

5.2.3 CABLE DETECTION

Click the "Fault/Safety" "path Detection" "Cable Detection" can view the Cable Detection configuration:



Figure 5-14: Cable detection information

The cable detection only selected one port:



Figure 5-15: Port cable detection result

5.3 DDOS PROTECTION

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



Figure 5-16: DDOS Protection information

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



Figure 5-17: selected dos type

5.4 LOOPBACK DETECTION

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

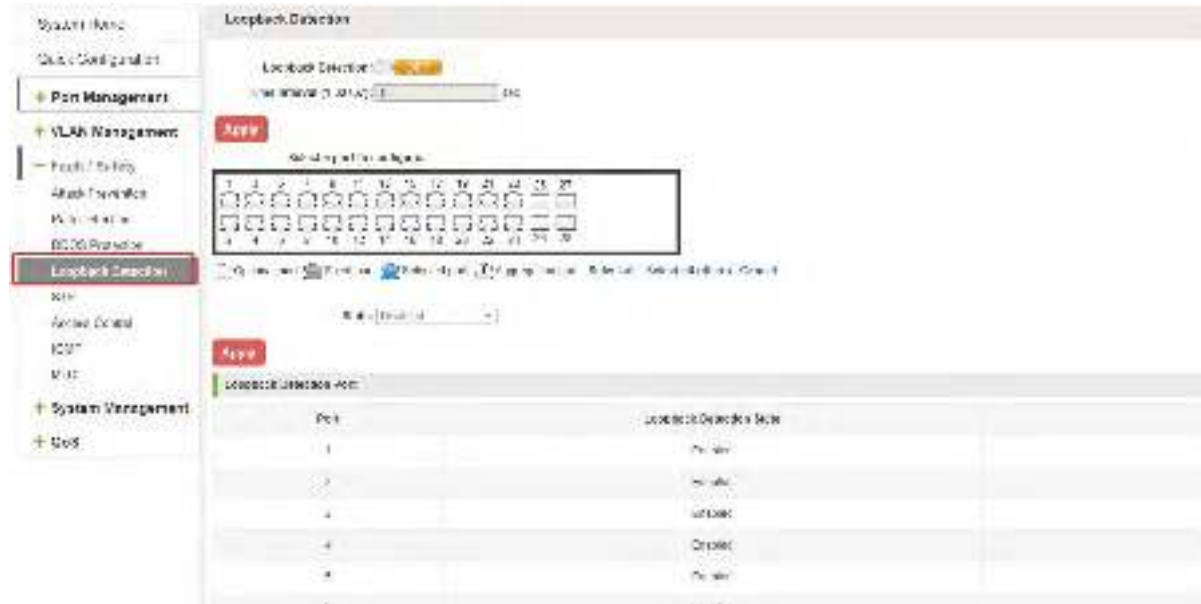


Figure 5-18: View loopback detection configuration information

5.4.1 ENABLE LOOPBACK DETECTION

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



Figure 5-19: enable loopback detection

5.4.2 CHOOSE THE PORT TO CONFIGURE

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



Figure 5-20: configure ports parameter

Click "Edit" button, change the port status:



Figure 5-21: change the port configure

5.5 STP

5.5.1 STP GLOBAL

5.5.1.1VIEW THE STP GLOBAL INFORMATION

Click the "Fault/Safety" "STP" you can view the configuration information of the STP Global:



Figure 5-22: STP global information

5.5.1.2ENABLE THE STP GLOBAL INFORMATION

Enable stp global and set up the stp mode and stp traps .You can view the root bridge information on the page .Notice:LLDP PDU flooding enable prevents executing mstp enable.



Figure 5-23: Change STP global status

5.5.1.3STP PORT SETTINGS

Select a port to configure the status eg:network、 disable、 edge

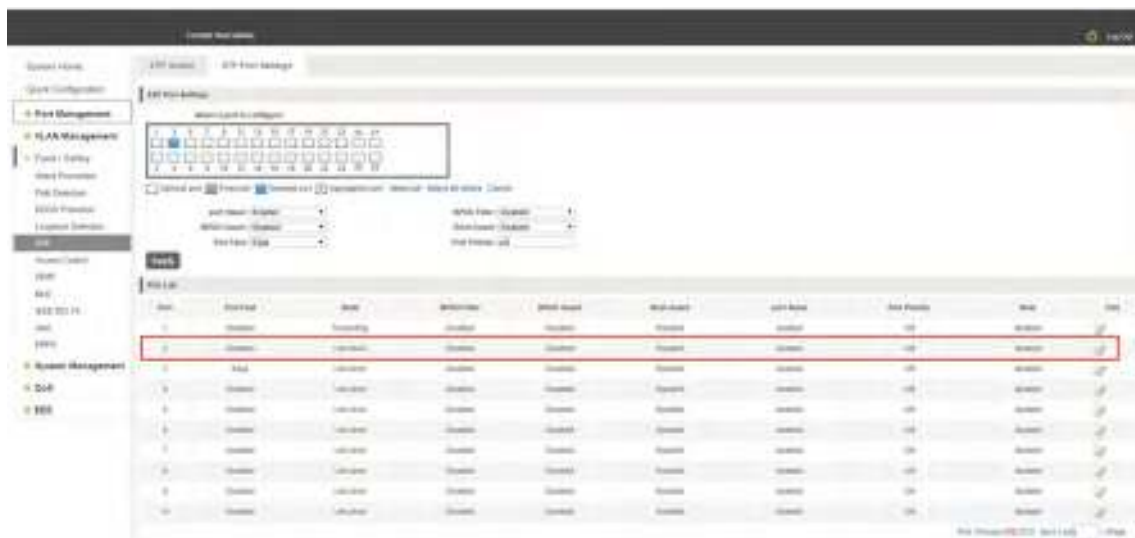


Figure 5-24: STP Port settings

5.6 ACCESS CONTROL

5.6.1 ACL ACCESS CONTROL LIST

5.6.1.1VIEW ACCESS CONTROL LIST

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



Figure 5-25: Access control list

5.6.1.2 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 "Apply" to complete the new rules:



Figure 5-:26 Configuration standard IP access control list

2. Increase the extended IP access rule

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 "Apply" to complete the new:



Figure 5-27: Configuration standard IP access control list

3. Increasing 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 "Apply":



Figure 5-28: 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

5.6.1.3MODIFY CONFIGURATION

Rules for modifying port applications

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

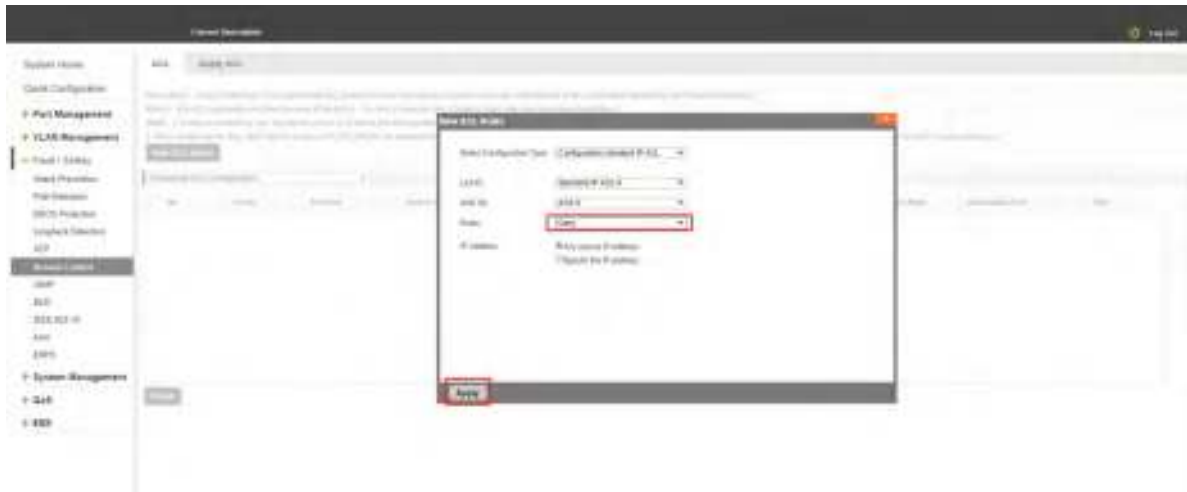


Figure 5-29: To modify the ACL rule

Configuration instructions

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

5.6.1.4DELETE RULE

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



Figure 5-30: Delete rules

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



Figure 5-31: Delete ACL rules

Configuration instructions:

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

5.6.2 APPLICATION ACL

5.6.2.1VIEW APPLICATION ACL

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



Figure 5-32: View application ACL rules

5.6.2.2INCREASED APPLICATION ACL

5.7 IGMP

5.7.1 VIEW IGMP CONFIGURATION

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



Figure 5-35: View Snooping IGMP configuration information

5.7.2 ACTIVE MULTICAST LISTENER FUNCTION

Click the "Fault/Safety" "IGMP Snooping", click "Off" button to activate the multicast monitoring function and you can choose the IGMP version :



Figure 5-36: 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 V3 - IGMP.

5.7.3 VIEW AND CONFIGURE ROUTER PORT

Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

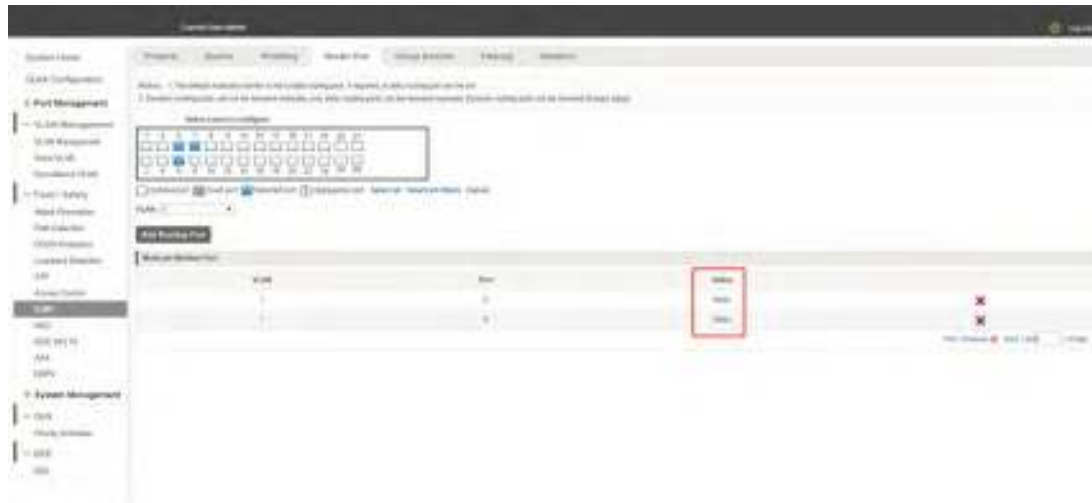


Figure 5-37: configure router port

5.7.4 GROUP ADDRESS

In this page you can configuration static group address and view the dynamic groups,Statically configured multicast groups can not be deleted,Dynamic multicast groups can be deleted:



Figure 5-38: Group address

5.7.5 FILTERING PROFILE

On the IGMP filter page, you can set up a section of multicast that is allowed or denied. And the application rules on the corresponding ports.You can also edit or delete rules by clicking the Edit button or the delete button:

Notice: If the rule has been applied to the port, if you want to delete the rule, you need to remove the rule from the port before you do so, otherwise you won't be able to delete it successfully:

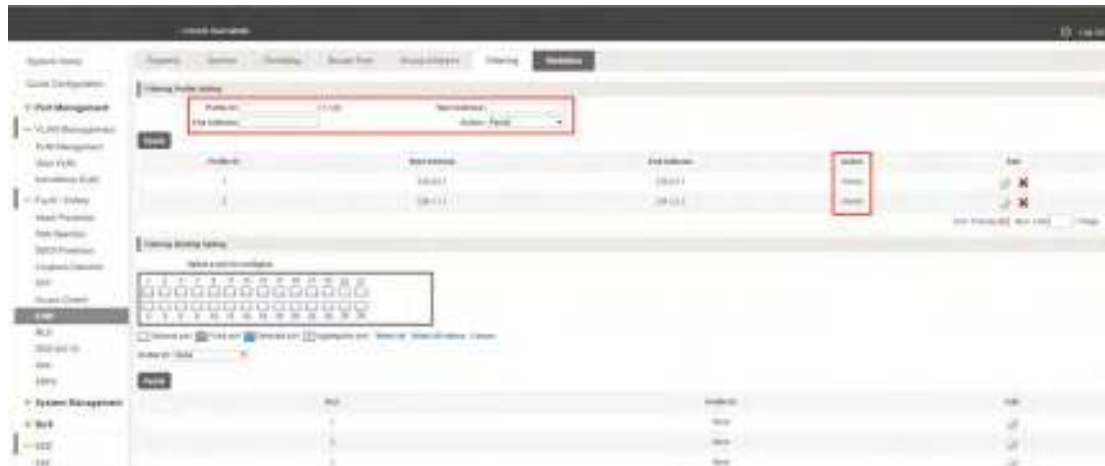


Figure 5-39: Configure filtering profile

When the above set rules are bound on the port, the port receives the multicast in the rule and processes it according to the corresponding action:

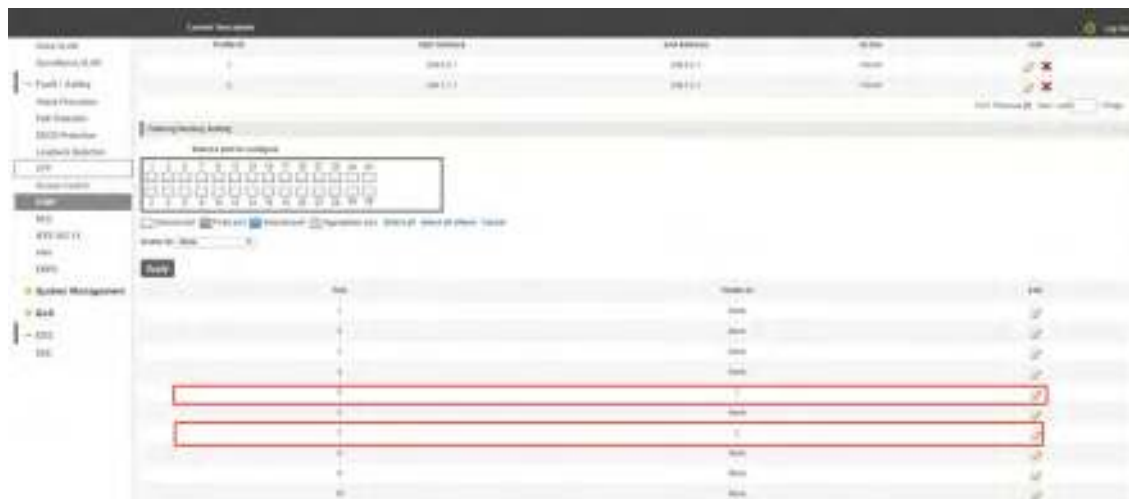


Figure 5-40: Filtering binding

5.7.6 IGMP STATISTICS

On the IGMP statistics page, you can look at the changes in the number of messages received by the current device in the IGMP type:



Figure 5-41: IGMP Statistics

5.7.7 DISABLE MULTICAST LISTENER FUNCTION

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



Figure 5-42: Closed multicast listener function operation

5.8 MLD

5.8.1 VIEW MLD CONFIGURATION

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



Figure 5-43: View MLD configuration information

5.8.2 ACTIVE MULTICAST LISTENER FUNCTION

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



Figure 5-44: 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.

5.8.3 VIEW AND CONFIGURE ROUTER PORT

Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.



Figure 5-45: configure router port

5.8.4 GROUP ADDRESS

In this page you can configuration static group address and view the dynamic groups,Statically configured multicast groups can not be deleted,Dynamic multicast groups can be deleted:



Figure 5-46: Group address

5.8.5 FILTERING PROFILE

On the MLD filter page, you can set up a section of multicast that is allowed or denied. And the application rules on the corresponding ports,You can also edit or delete rules by clicking the Edit button or the delete button:

Notice:If the rule has been applied to the port, if you want to delete the rule, you need to remove the rule from the port before you do so, otherwise you won't be able to delete it successfully

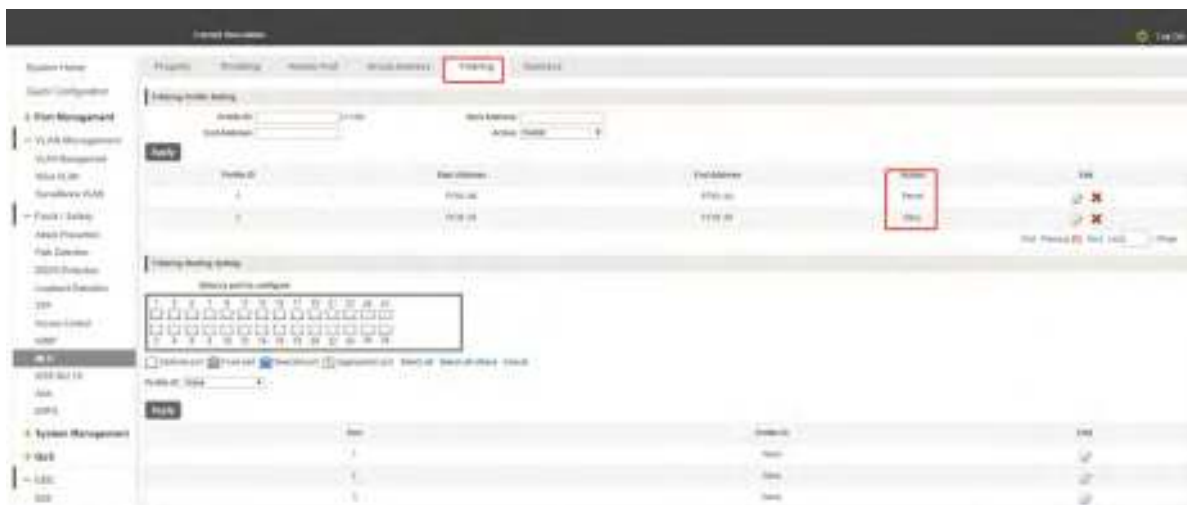


Figure 5-47: Configure filtering profile

When the above set rules are bound on the port, the port receives the multicast in the rule and processes it according to the corresponding action:



Figure 5-48: Filtering binding

5.8.6 MLD STATISTICS

On the MLD statistics page, you can look at the changes in the number of messages received by the current device in the MLD type:

5.9 IEEE 802.1X

5.9.1 VIEW IEEE802.1X CONFIGURATION

Click the "Fault/Safety" "IEEE 802.1X", Click the "Close" button to activate the 802.1X authentication function:



Figure 5-51: View 802.1x configuration information

5.9.2 PORT ENABLE 802.1X CONFIGURATION

Notice: If you want the 802.1x function to take effect, you need to configure the radius server separately in the AAA configuration page

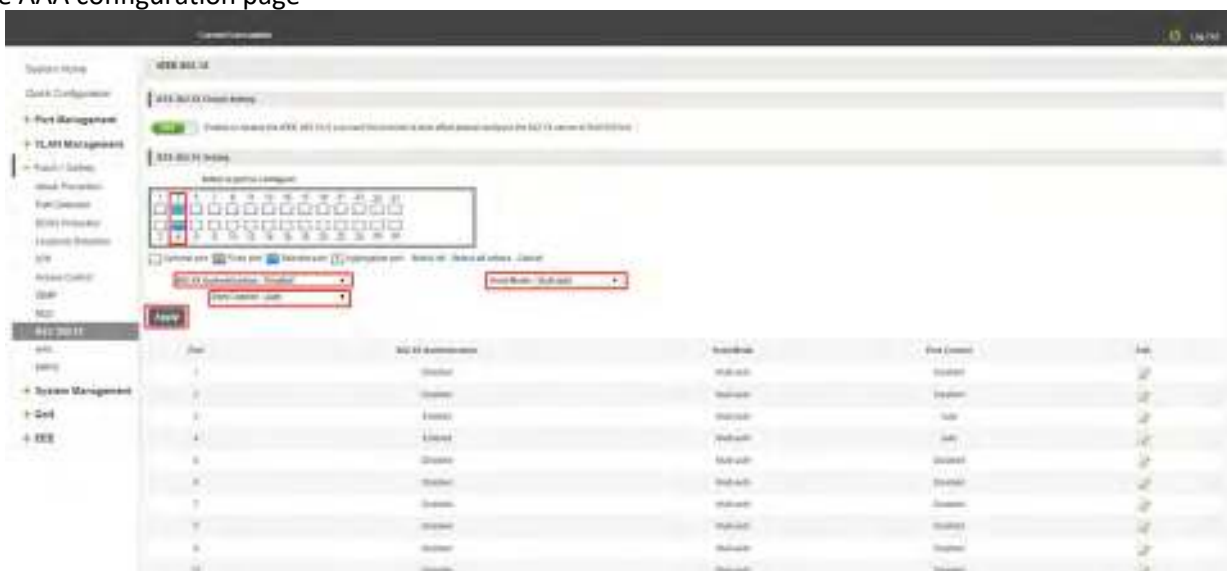


Figure 5-52: Port enable 802.1x function operation

5.10 AAA

5.9.1 VIEW AAA CONFIGURATION



Figure 5-53: View AAA configuration information

5.9.2 ENABLE RADIUS CONFIGURATION

Notice: The current device supports mac authentication function, just add the mac address you need to authenticate in the "key" field.



Figure 5-54: Radius server configuration

5.10 ERPS

5.10.1 VIEW ERPS CONFIGURATION



Figure 5-55: View ERPS configuration information

5.10.2 CREAT ERPS RING



Figure 5-56: Enable an erps ring

5.10.3 Enable erps port

Notice: The erps port must be in trunk mode, otherwise it cannot be successfully enabled.

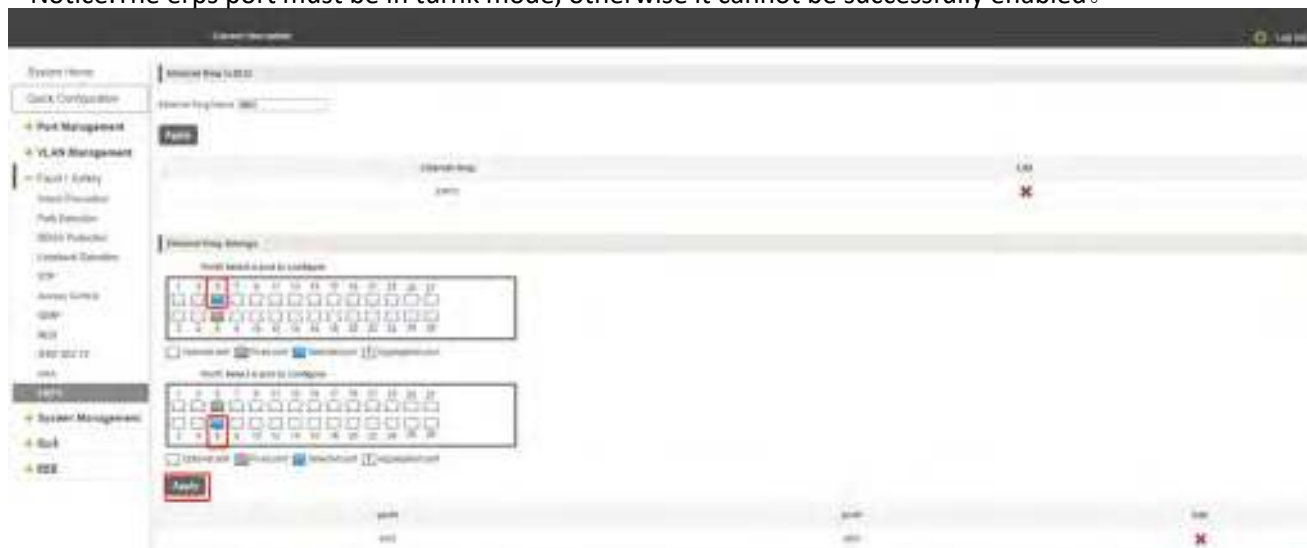


Figure 5-56: Port added erps ring

5.10.4 Erps ring parameter configuration

Notice:

1. In networking, only one switch is the master node, and the other switches are ordinary nodes, otherwise the ERPS function will not take effect.
2. After the configuration is complete, you need to enable the ERPS ring
3. During the test, the port on the ring must be added to the data vlan, otherwise the data may not be forwarded normally.

At the same time, for ports other than the ports on the ring, when specifying a VLAN, do not assign the control VLAN to it, otherwise the data may not be forwarded normally.



Figure 5-56: Port added erps ring



Figure 6-1: 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 192.168.100.147
3. In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.192
4. In the Gateway Address text box to enter the gateway address, such as 192.168.100.129
5. In the Device Name text box ,enter the Device Name ,such as internet device
6. In the Device Location text box ,enter the Device Location ,such as china
7. In the Contact Name text box ,enter the Contact Name ,such as miss
8. In the Contact Information text box ,enter Contact Information ,such as 18542154730
9. Click on "Save Settings" button to complete the configuration

6 SYSTEM MANAGEMENT

6.1 SYSTEM SETTINGS

6.1.1 MANAGEMENT VLAN

6.1.1.1configuration 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:

6.1.1.2 System time synchronization



Figure 6-2: System time synchronization

To configuration system time,in the NTP Server IP Address text box,enter NTP Server IP Address such as 202.118.1.81(local NTP servers or internet NTP servers),in the Time Zone (T) text box,you can choose any time zone you want,such as UTC+08:00.

6.1.1.3 DHCPv6 client



Figure 6-3: DHCPv6 client

To enable DHCPv6 client,click dynamic allocation,If the environment has dhcpv6 server ,the device will get a ipv6 address,and the address will display in ipv6 address input box,however,the address can't be change by Manual modification.

6.1.1.4 IPv6 HTTPS

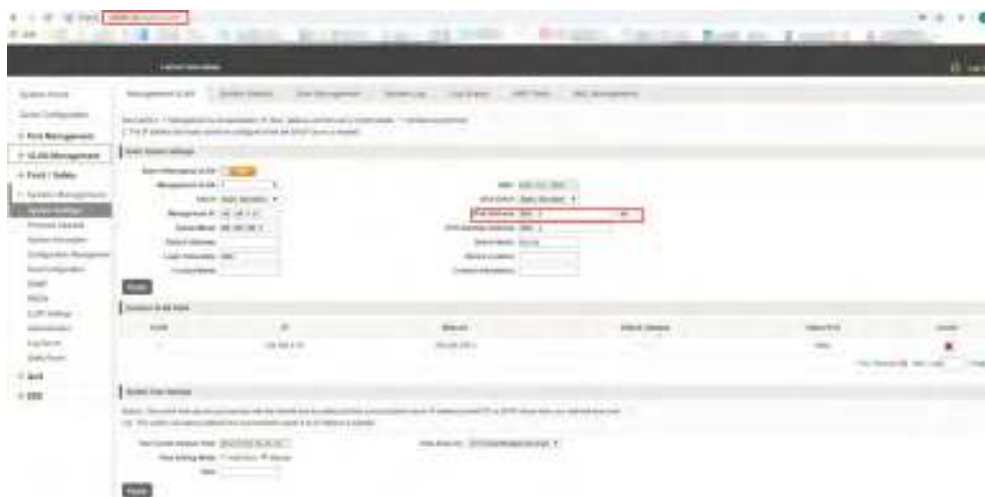


Figure 6-4: IPv6 HTTP

6.1.2 SYSTEM RESTART

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



Figure 6-5: System Restart

Restart the device, follow these steps: step1:Click on "Restart the device immediately" button,step2:Click OK in the box that pops up "OK" button,step3:Prompted to save the current configuration, depending on your need to select "OK" or "Cancel",step4:After the restart the progress bar moves to 100%, reboot the device.

6.1.3 USER MANAGEMENT

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



Figure 6-6: change password

Change password follow these steps:

step1:Enter the old password: password;

step2:Enter the new password: admin;

step3:Confirm new password: admin,

step4:Click the "Apply" button;

step5:Pop-up dialog box, click "OK" button.

6.1.4 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:

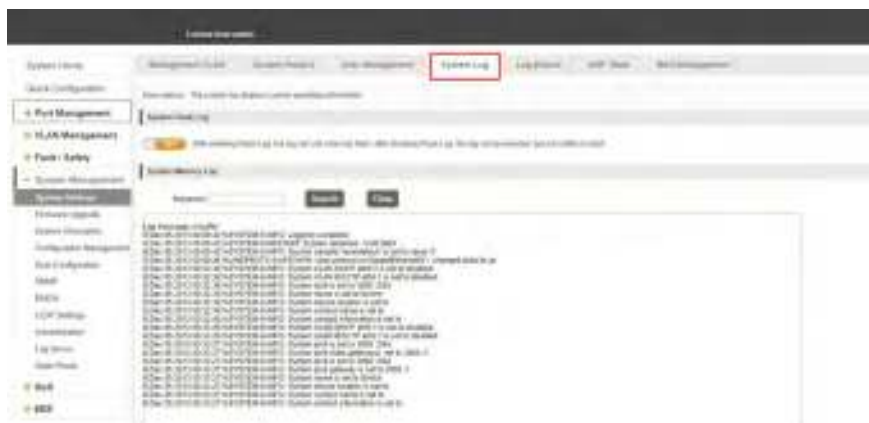


Figure 6-7: system log

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.

6.1.5 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 6-8: Log Export

6.1.6 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 6-9: ARP message

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

6.1.7 MAC MANAGEMENT

6.1.7.1 MAC address lookup

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

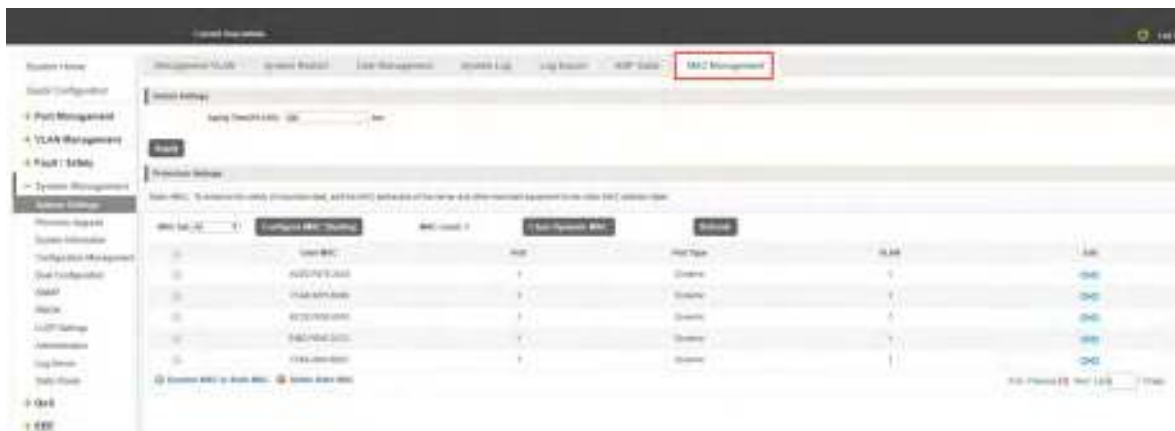


Figure 6-10: MAC address lookup display

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.

6.1.7.2 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 6-11: MAC addresses statically bound static configuration

Statically typed MAC address configuration steps are as follows:

step1:Click the "Configure MAC Binding" button;step2:In the "User MAC" text box to enter the MAC address, such as 0001.7A4F.74D2;step3:In the "VLAN ID" text box to enter the VLAN ID, such as 1;step4:Select ports in the port panel;step4:Click on "Apply"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:

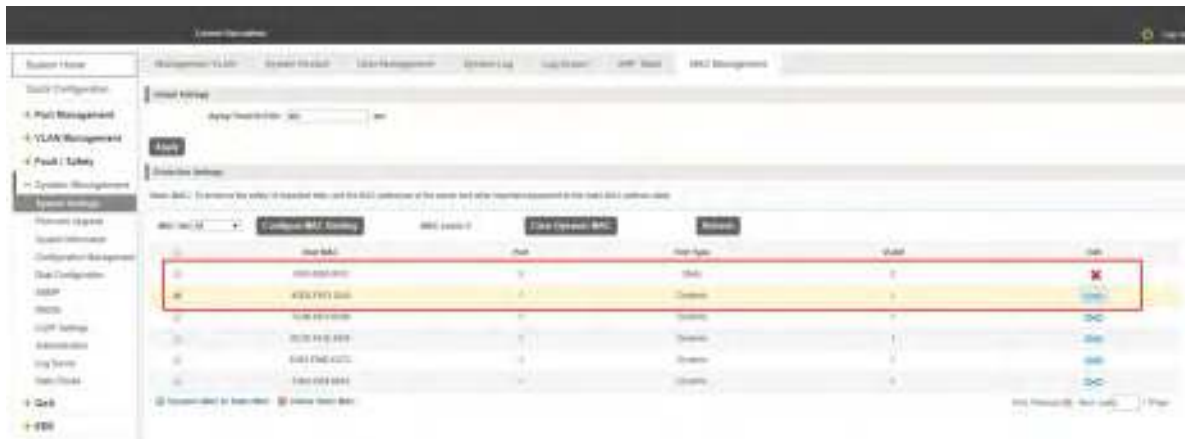


Figure 6-12: MAC address of the static binding configuration

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 6-13: Batch-MAC binding configuration

6.1.7.3 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:

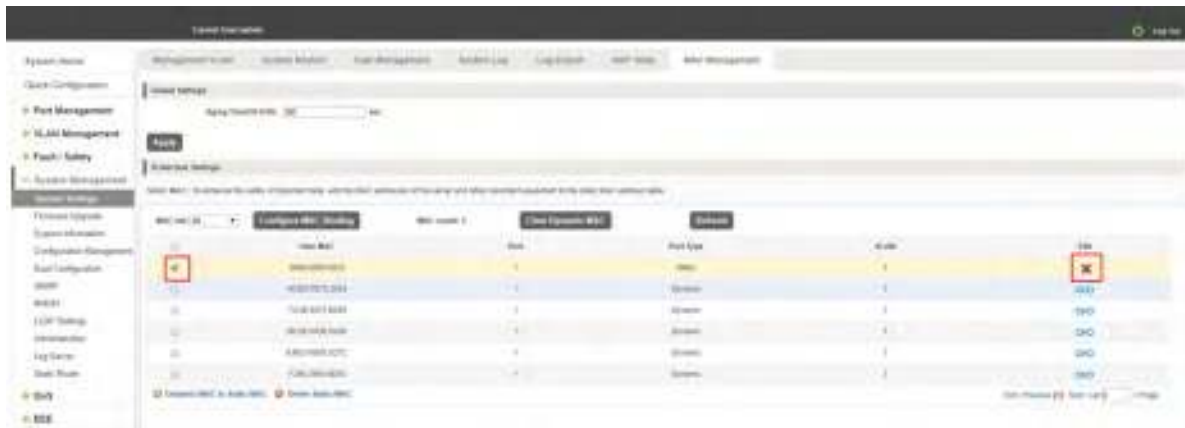


Figure 6-14: MAC address deletion

Remove MAC address configuration steps are as follows:

Step1: To delete the selected MAC address, step2: Click "X" 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:

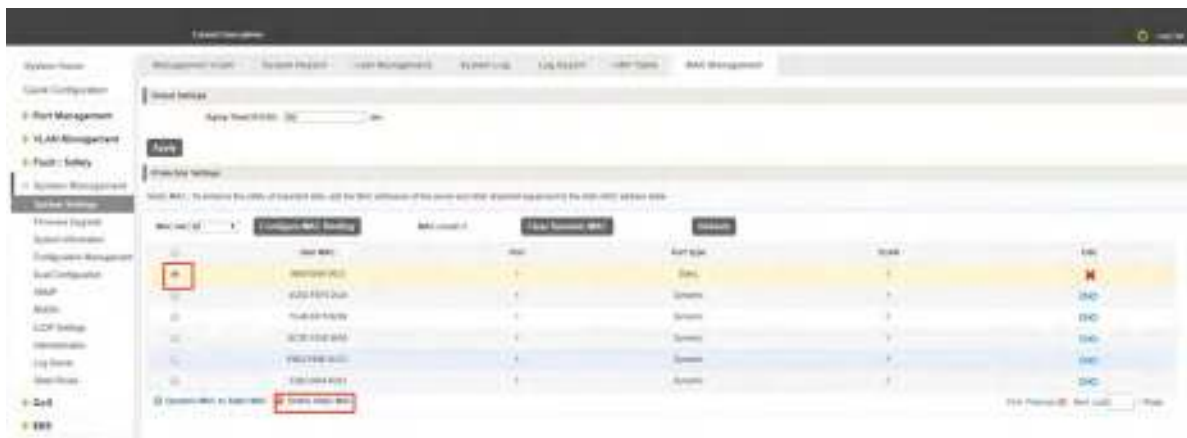


Figure 6-15: MAC address batch deletion deletion

6.2 SYSTEM UPGRADE

Click the "System Management" "Firmware Upgrade" to backup firmware to file or upgrade the software on the switch:



Figure 6-16: Switch System backup firmware to file and Upgrade firmware

Switch backup firmware to file as follows:

Step1:Click"Backup"button waiting the system download the firmware completed.

Switch system upgrade steps are as follows:

Step1:Click "Choose File" button to select the switch upgrade file;

step2:Click the "Upgrade" button switch to start the upgrade new software;

step3:When the upgrade progress bar is at 100%, the switch will automatically reboot, completion of the upgrade is completed.

6.3 SYSTEM INFORMATION

6.3.1 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 6-17: 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.

6.3.2 CPU INFORMATION

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



Figure 6-18: 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.

6.5 CONFIGURATION MANAGEMENT

6.5.1 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 6-22: 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 startup --config file:



Figure 6-23: 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 6-24: Imported configuration

Import the configuration steps are as follows:

Step1:Select the "Import Configuration";step2:Click "Choose File" button to find you want to import the configuration File;step3:Click on "Import Configuration" button;step4:Confirm the restart.

4. Export configuration

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



Figure 6-25: Export configuration

6.5.2 RESTORE FACTORY SETTINGS

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



Figure 6-26: Restore factory Settings

Factory default operation steps are as follows:

Step1:Click the "Restore the Factory Settings" button,step2:In the pop-up confirmation box, click the "OK" button,step3:After the completion of the reset switch, wait for equipment to restart, switch back to factory default configuration.

6.6 SNMP

6.6.1 CHECK THE SNMP

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



Figure 6-27: 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.

6.6.2 ACTIVATE THE SNMP

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "OFF" to "ON", and the ipv6 SNMP will be enable too ;click ok:



Figure 6-28: Activation SNMP function

Activation function SNMP configuration steps are as follows:

Step1:Choose open SNMP options;step2:Click "OK" button to complete the configuration.

6.6.3 TO DISABLE THE SNMP

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "ON" to "OFF",and the ipv6 SNMP will be disable too ; complete the configuration:



Figure 6-29: Disable the SNMP function

Disable the SNMP function configuration steps are as follows:

Step1:Choose close SNMP options;step2:Click "OK" button to complete the configuration.

6.6.4 ACTIVATE THE TRAP

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



Figure 6-30: Activation function of the TRAP

Activate the TRAP function configuration steps are as follows:

Step1:Select "ON" option;step2:Click "OK" button to complete the configuration.

6.6.5 DISABLE THE TRAP

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



Figure 6-31: Disable TRAP function

Disable the TRAP function configuration steps are as follows:

Step1: Select "ON" to "OFF" option.step2:Click "OK" button to complete the configuration.

6.6.6 CHANGE OF COMMUNITY

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

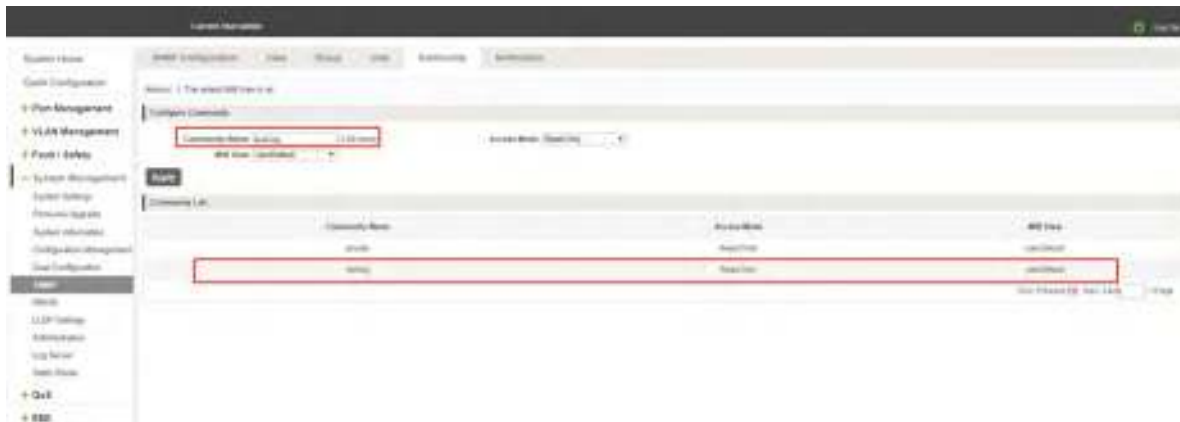


Figure 6-32: Increase community

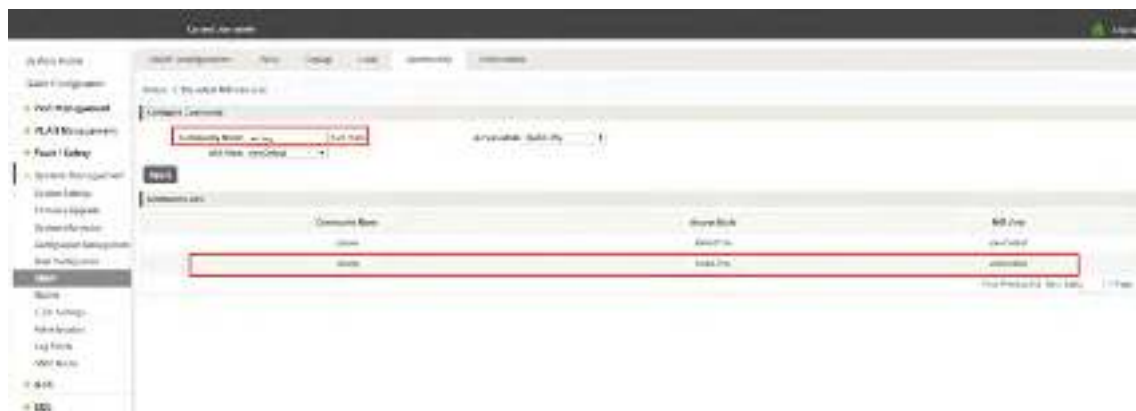


Figure 6-33: Community results

Change community configuration steps are as follows:

Step1:In the community name dialog box input:testing;

step2:Select "RO" permissions;

step3:Click on "OK" button, complete the configuration.

6.6.7 ADDED THE SNMP TRAP SERVICE HOST

Click on the "System Management" "SNMP", in the host IP text box input: 192.168.100.83, TRAP community name: public, SNMP version choice: V2C, click the "OK" button, complete the configuration:



Figure 6-34: Increases the SNMP TRAP service host



Figure 6-35: SNMP TRAP service host

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

Step1:In the host IP dialog box input: 192.168.100.40;

step2:In TRAP community name dialog input: testing;

step3:Select the SNMP version: V1;

step4:Click on "OK" button, complete the configuration.

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

6.6.8 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 6-36: Delete community

6.7 Administration

6.7.1 CHECK THE Administration

Click on the "System Management" "Administration", you can view the telnet,https,ssh configured information:



Figure 6-37: View the Administration configuration information



Figure 6-38: telnet,https,ssh configuration

6.8 LOG SERVER

6.8.1 CHECK THE LOG SERVER

Click on the "System Management" "Log Server", you can view the log server configured information:



Figure 6-39: View the Log server configuration information

6.8.2 Log server configured

Click on the "System Management" "Log Server", you can view the log server configured information,Enter the ip address of the log server in the "host ipv4 address", enter the port number bind to the log server when it is running in the udp port, and set the log level in the Severity selection:

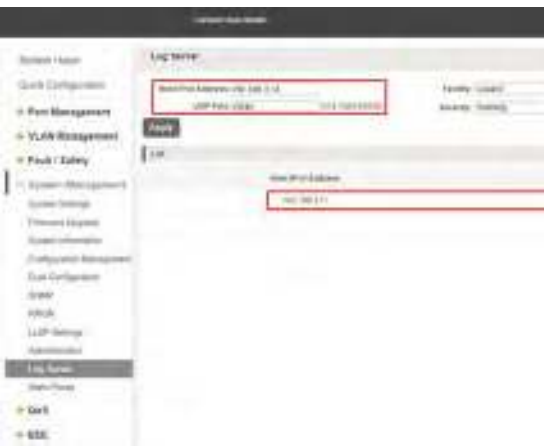


Figure 6-40: Log server configuration

6.8 STATIC ROUTE

6.8.1 CHECK THE STATIC ROUTE

Click on the "System Management" "Static route", you can view the static route configured information:



Figure 6-41: View the static route

6.8.1

Click on the "System Management" "Static route", Configure the ip address of the destination network segment in the "Destination IP" option, and configure the ip address of the next hop in the "Gateway" option:

Note: The static routing of this device only supports ipv4 static routing, and the device has the corresponding IP address of the next hop network segment.

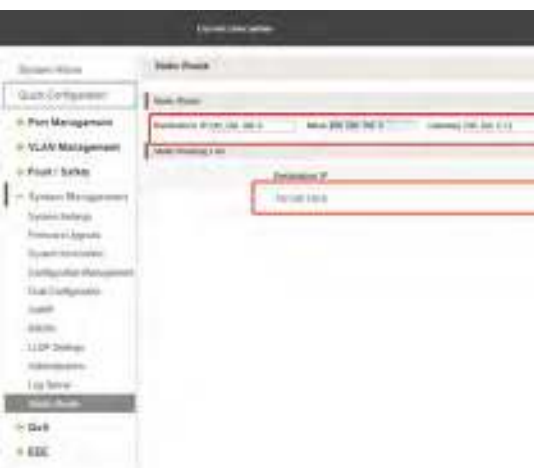


Figure 6-42: static route configuration

6.7 RMON

6.7.1 VIEW ROMN CONFIGURE INFORMATION

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



Figure 6-37: View RMON configure information

6.7.2 CONFIGURE ROMN TYPE

Configure ROMN type : Alarm,selected one port to configure and setting parameters and click "Save" button.



Figure 6-38: configure ROMN type

Notice:Parameters There are some special rules in the configuration. Please note the prompts in the configuration.eg:Rising Threshold is greater than Falling Threshold.

6.7.3 CHANGE ROMN TYPE

On the romn 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”.

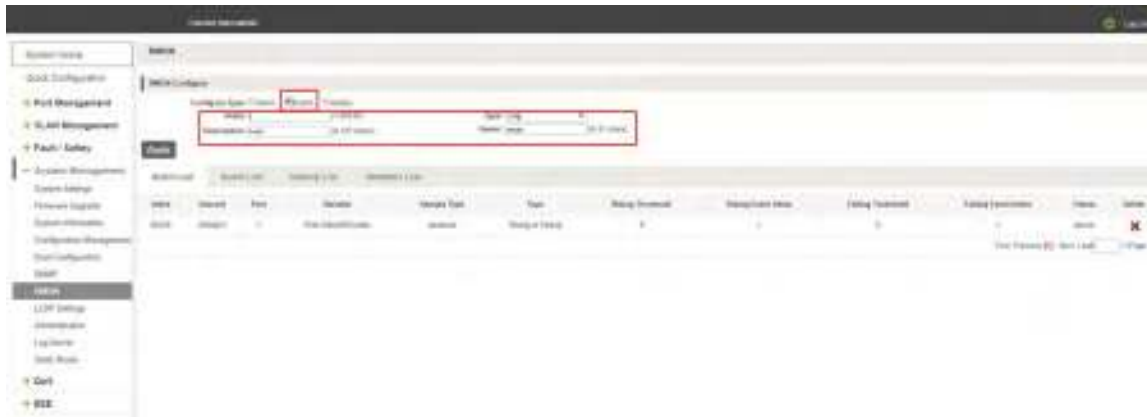


Figure 6-39: Change ROMN type is Event



Figure 6-40: Change ROMN type is History

When the parameters are configured ,click the Statistics List .We can choose the port to view the information .



Figure 6-41: View the port configure information

6.7.4 DELETE THE CONFIGURED RULE

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



Figure 6-42: Delete the Alarm list rule



Figure 6-43: Delete the Event list rule



Figure 6-44: Delete the History list rule

7 QOS

7.1 PRIORITY SCHEDULE

7.1.1 VIEW THE PRIORITY SCHEDULE

Click on the "QOS" "priority schedule", can view the device priority schedule:



Figure7-1: priority schedule

7.1.2 THE CONFIGURATION GLOBAL SETTINGS OF SP

7.1.2.1THE 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.

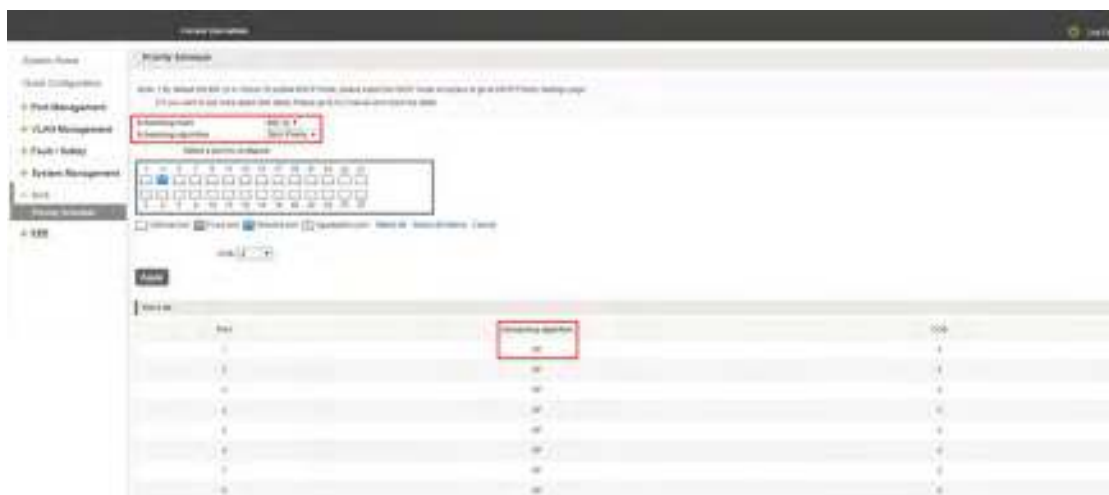


Figure 7-2: global settings in 802.1p and SP

7.1.2.2THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP ADD WRR

Click on "QOS" "priority schedule" "global settings ", in scheduling mark , choose 802.1p,in the Scheduling algorithm,choose WRR.

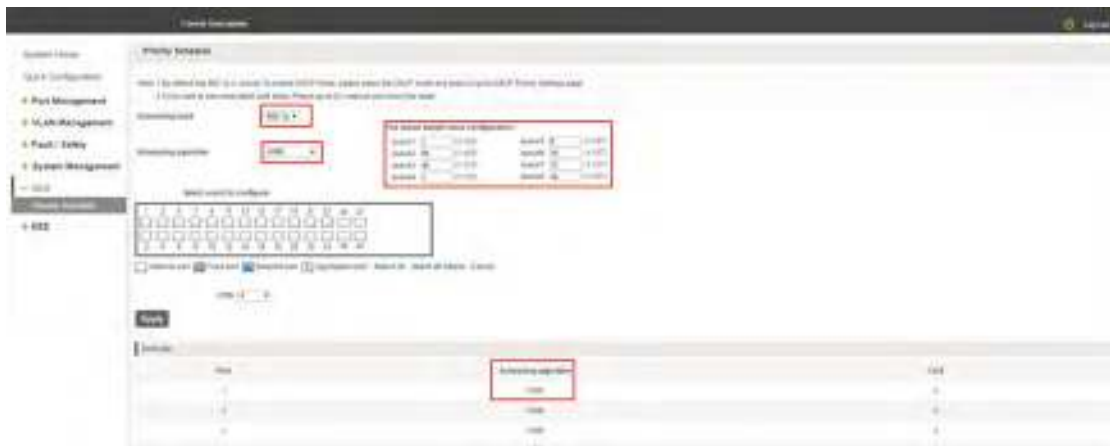


Figure 7-3: global settings in 802.1p and WRR

Priority schedule steps are as follows:

Step1: in scheduling mark , choose 802.1p;step2:in the Scheduling algorithm,choose WRR ,step3:in queue1 text box, enter the weight value ,such as 1;step4:in queue2 text box, enter the weight value ,such as 20;step5:in queue3 text box, enter the weight value ,such as 40;Step6:in queue4 text box, enter the weight value ,such as 1;

Step1: in scheduling mark , choose 802.1p;step2:in the Scheduling algorithm,choose hybrid ,step3:in strict priority text box, choose the queue3,4;step4:in WRR text box, choose the queue 1,2 ;step5:in queue1 text box, enter the weight value ,such as 1;Step6:in queue2 text box, enter the weight value ,such as 20;

7.1.3 THE CONFIGURATION GLOBAL SETTINGS OF DSCP

7.1.3.1THE 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 7-6: global settings in DSCP and SP

Priority schedule steps are as follows:

- Step1: in scheduling mark , choose DSCP;step2:in the Scheduling algorithm,choose strict priority,
- step3:in from DSCP value text box, choose 0 and in to DSCP value text box, choose 1 and in priority text box, choose low ;
- step4:in from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose medium;
- step5:in from DSCP value text box, choose 4 and in to DSCP value text box, choose 5 and in priority text box, choose high;
- step6:in from DSCP value text box, choose 6 and in to DSCP value text box, choose 8 and in priority text box, choose highest;

7.1.3.2THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND WRR

Click on "QOS" "priority schedule" "global settings ", in scheduling mark , choose DSCP,in the Scheduling algorithm,choose WRR .

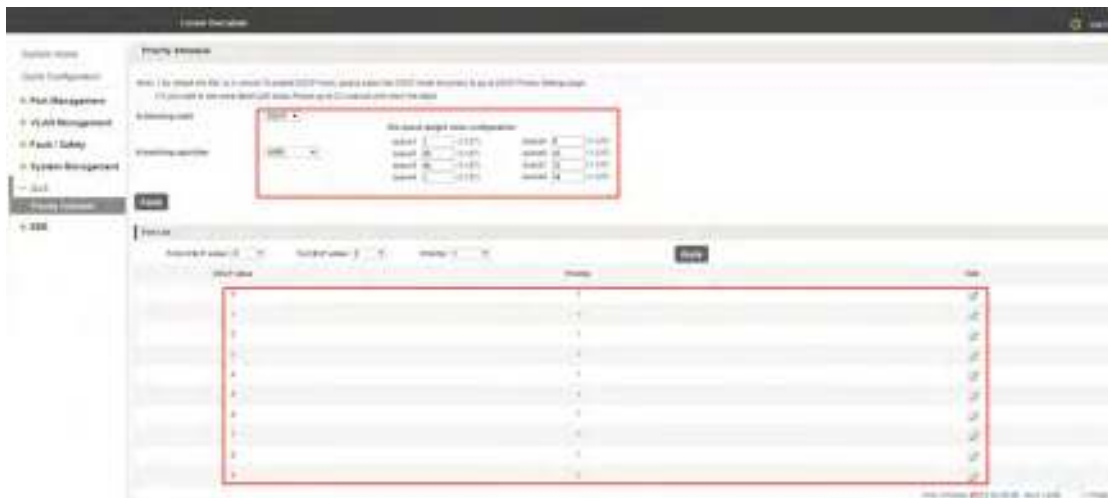


Figure 7-7: global settings in DSCP and WRR

Priority schedule steps are as follows:

Step1: in scheduling mark , choose DSCP ;step2:in the Scheduling algorithm,choose WRR ,step3:in queue1 text box, enter the weight value ,such as 10;step4:in queue2 text box, enter the weight value ,such as 20;step5:in queue3 text box, enter the weight value ,such as 30;Step6:in queue4 text box, enter the weight value ,such as 40;

Figure 7-10: Add the port to the VLAN

Modify DSCP values follow these steps:

- Step1:select DSCP values and Click“”icon;
- step 2:In the priority text box,choose medium;
- step3;click on the apply;
- step 4:click OK.

8 EEE

8.1 EEE

Click “EEE”. View the EEE configuration details. Function is turned off by default.



Figure 8-1 EEE information

8.2 ENABLE 802.3AZ EEE SETTINGS

Enable 802.3az and click  change the status. Finally save the configure.



Figure 8-2 Enable 802.3az EEE