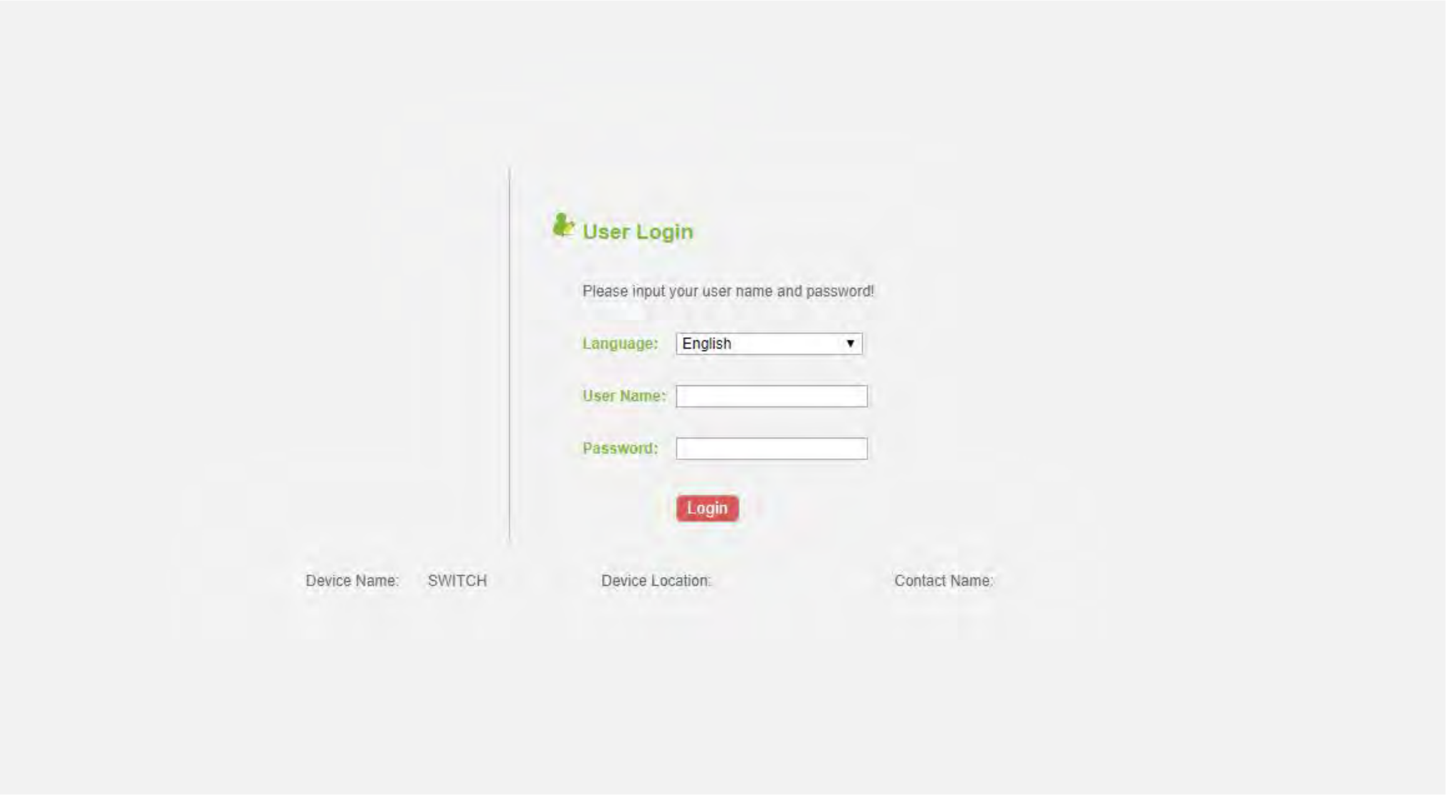
Web Configuration Manual

TABLE OF 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 192.168.1.200, 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



User Login

Please input your user name and password!

Language: English

User Name:

Password:

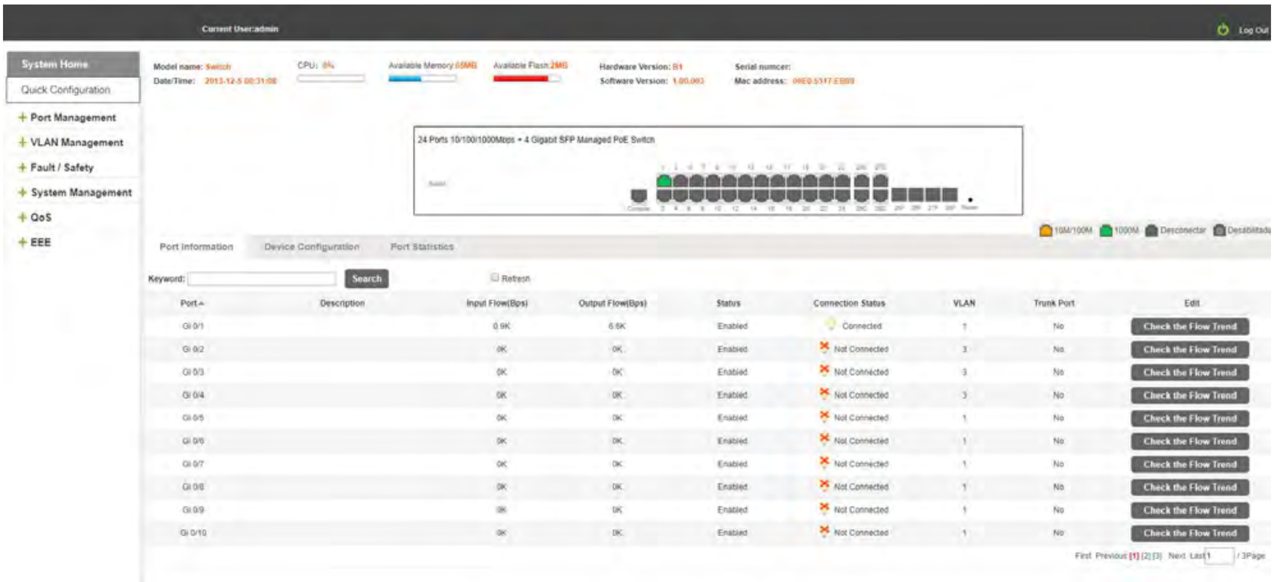
Device Name: SWITCH

Device Location:

Contact Name:

Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:



Model name: Switch
Date/Time: 2013-12-5 00:31:08
CPU: 0%
Available Memory:65MB
Available Flash:2MB
Hardware Version: B1
Software Version: 1.00.003
Serial numcer:
Mac address: 00E0.5317.EB88

Keyword:

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Status	Connection Status	VLAN	Trunk Port	Edit
Gi 0/1		0.9K	6.6K	Enabled	Connected	1	No	Check the Flow Trend
Gi 0/2		0K	0K	Enabled	✗ Not Connected	3	No	Check the Flow Trend
Gi 0/3		0K	0K	Enabled	✗ Not Connected	3	No	Check the Flow Trend
Gi 0/4		0K	0K	Enabled	✗ Not Connected	3	No	Check the Flow Trend
Gi 0/5		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/6		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/7		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/8		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/9		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/10		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend

First Previous [1] [2] [3] Next Last 1 / 3Page

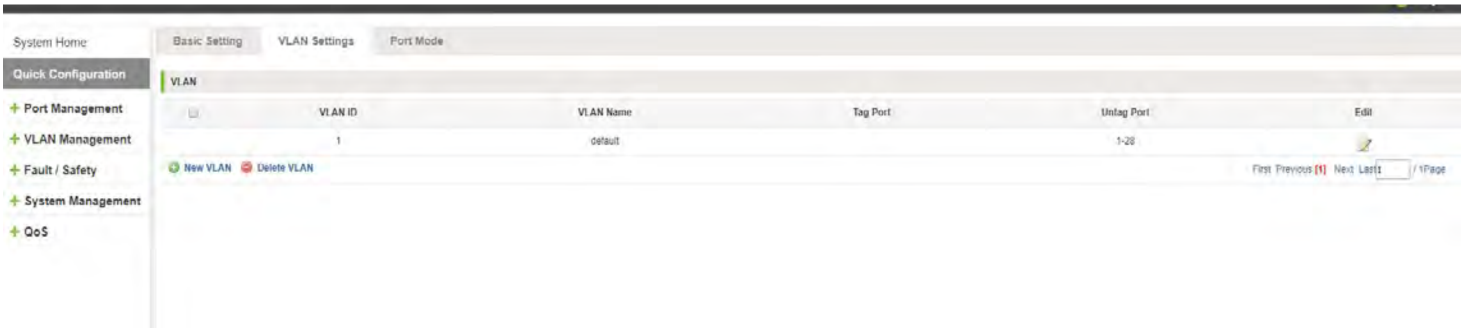
Figure 1-2: switch WEB management page Home

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".



□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-28	✎

First Previous [1] Next Last 1 / 1Page

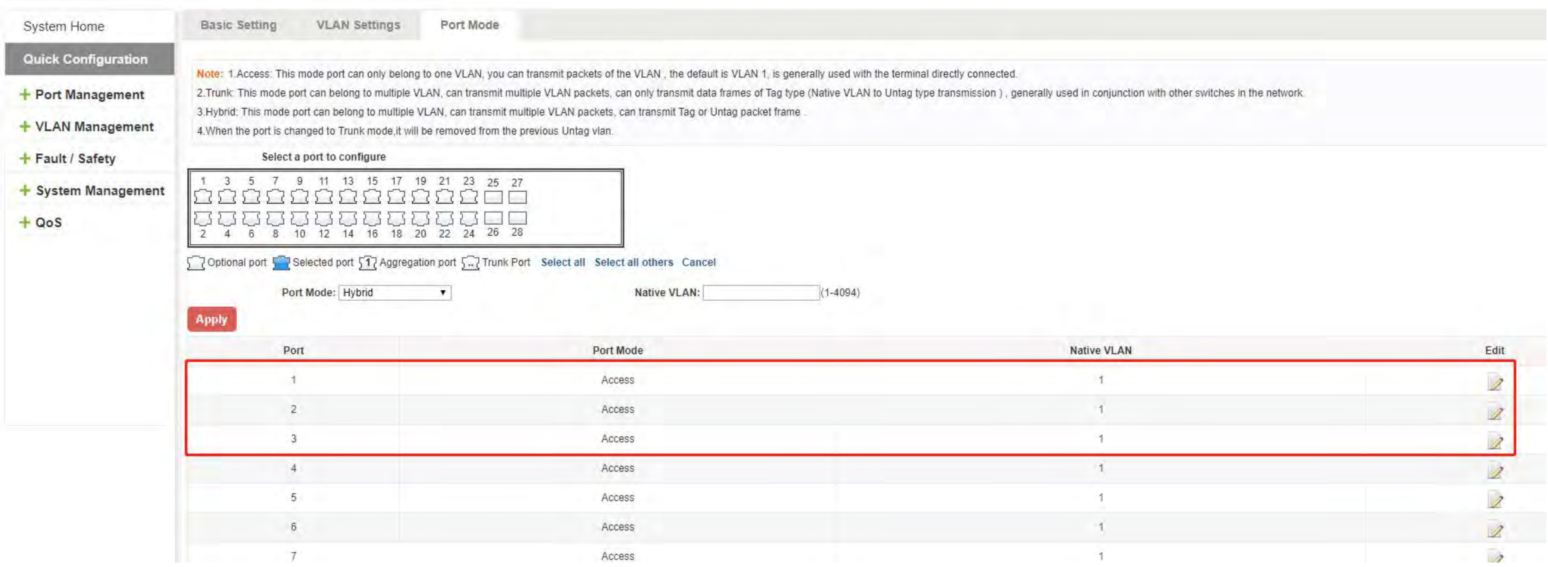
Figure 2-1: VLAN Setting

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.



Note: 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 Tag 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 Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Select a port to configure

Port Mode: Hybrid ▾ Native VLAN: (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Access	1	✎
2	Access	1	✎
3	Access	1	✎
4	Access	1	✎
5	Access	1	✎
6	Access	1	✎
7	Access	1	✎

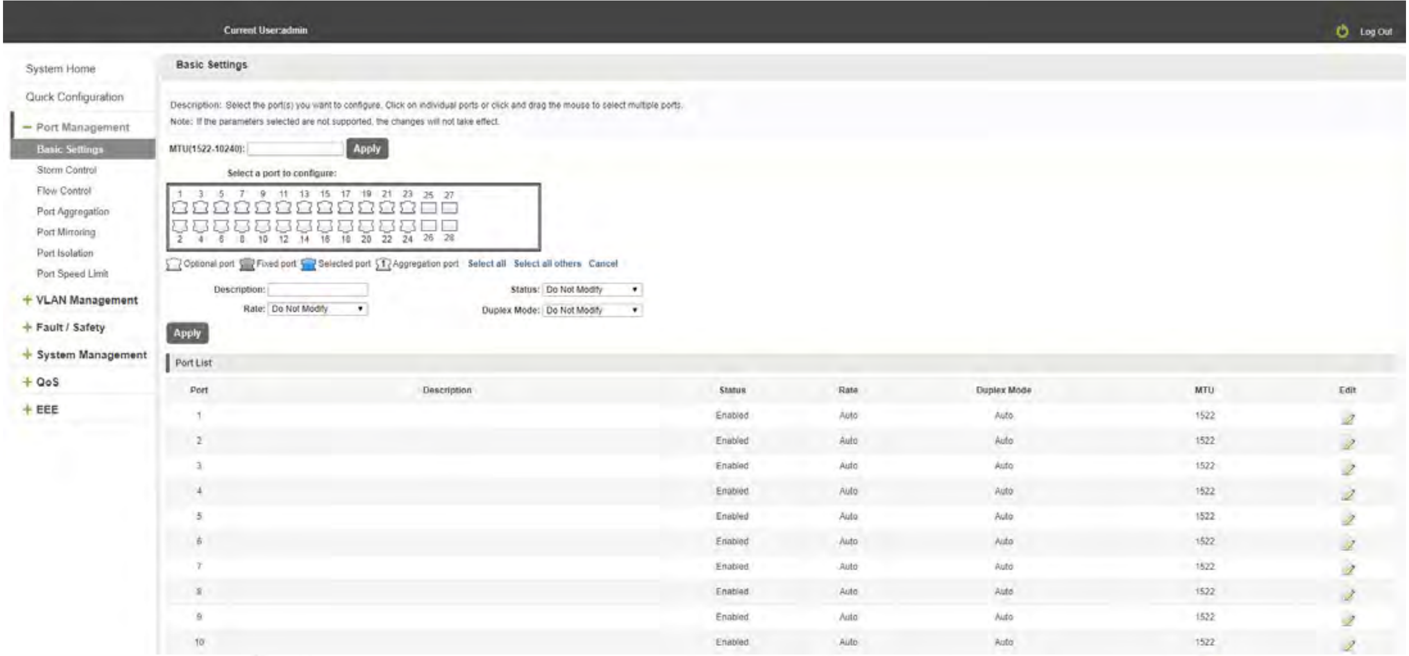
Figure 2-2: Port mode Setting

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:



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.

MTU(1522-10240):

Description:

Rate: Do Not Modify

Status: Do Not Modify

Duplex Mode: Do Not Modify

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	✎
2		Enabled	Auto	Auto	1522	✎
3		Enabled	Auto	Auto	1522	✎
4		Enabled	Auto	Auto	1522	✎
5		Enabled	Auto	Auto	1522	✎
6		Enabled	Auto	Auto	1522	✎
7		Enabled	Auto	Auto	1522	✎
8		Enabled	Auto	Auto	1522	✎
9		Enabled	Auto	Auto	1522	✎
10		Enabled	Auto	Auto	1522	✎

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;

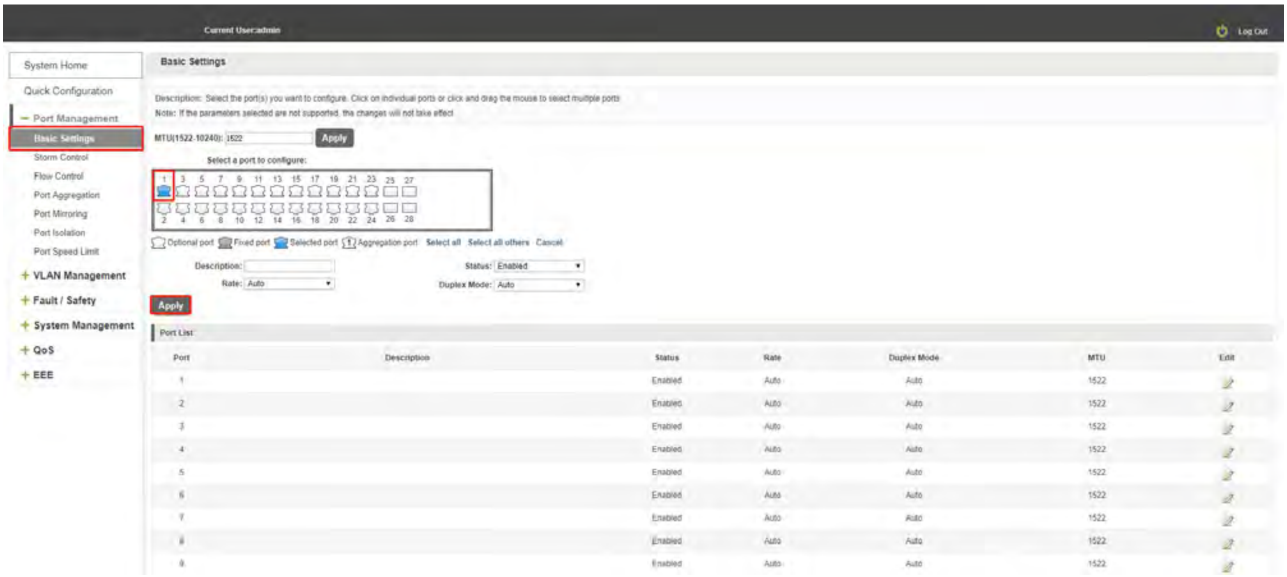
4.Port Rate: Displays the switch port speed configuration, auto-negotiation / 10/100/1000;

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:



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports

Note: If the parameters selected are not supported, the changes will not take effect

MTU(1522-10240): 1522 Apply

Select a port to configure:

Description:

Status: Enabled

Rate: Auto

Duplex Mode: Auto

Apply

Port List

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	✎
2		Enabled	Auto	Auto	1522	✎
3		Enabled	Auto	Auto	1522	✎
4		Enabled	Auto	Auto	1522	✎
5		Enabled	Auto	Auto	1522	✎
6		Enabled	Auto	Auto	1522	✎
7		Enabled	Auto	Auto	1522	✎
8		Enabled	Auto	Auto	1522	✎
9		Enabled	Auto	Auto	1522	✎

Figure 3-2: Port Properties configuration of FIG.

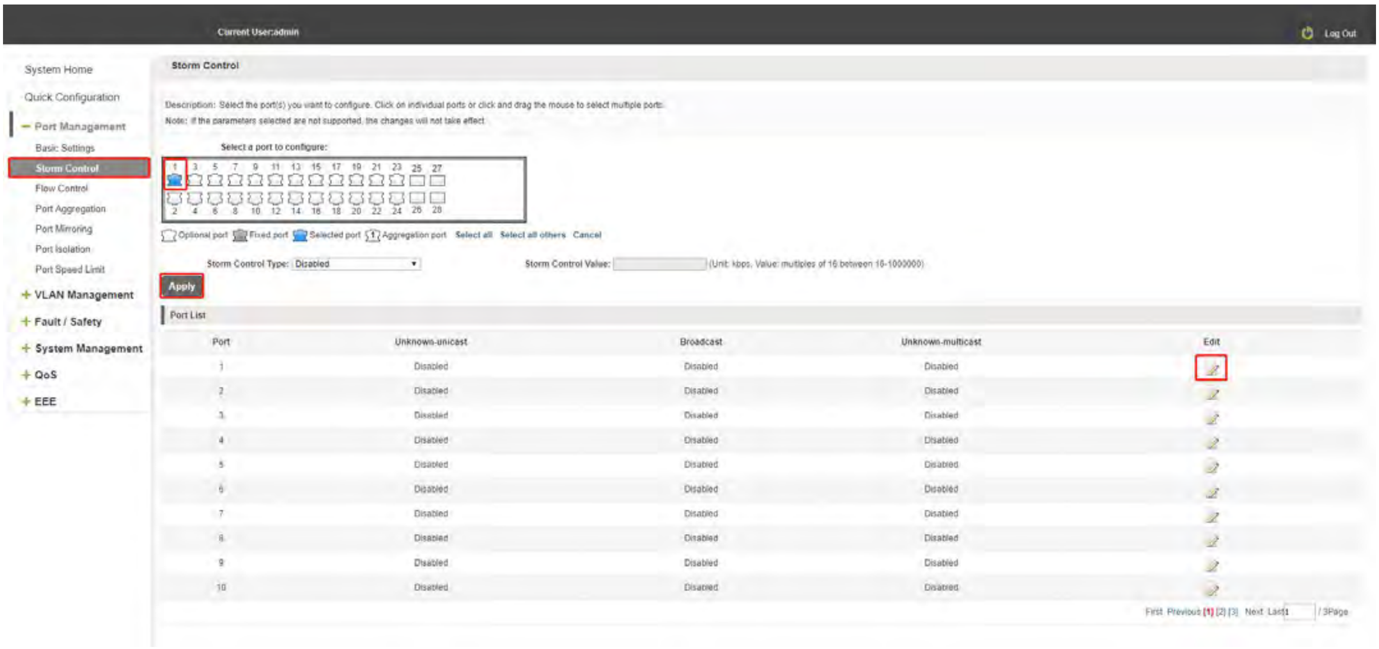
To configure port properties as follows:

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:



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.

Storm Control Type: Disabled

Storm Control Value: (Unit: kbps, Value: multiples of 16 between 16-1000000)

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	Disabled	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

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

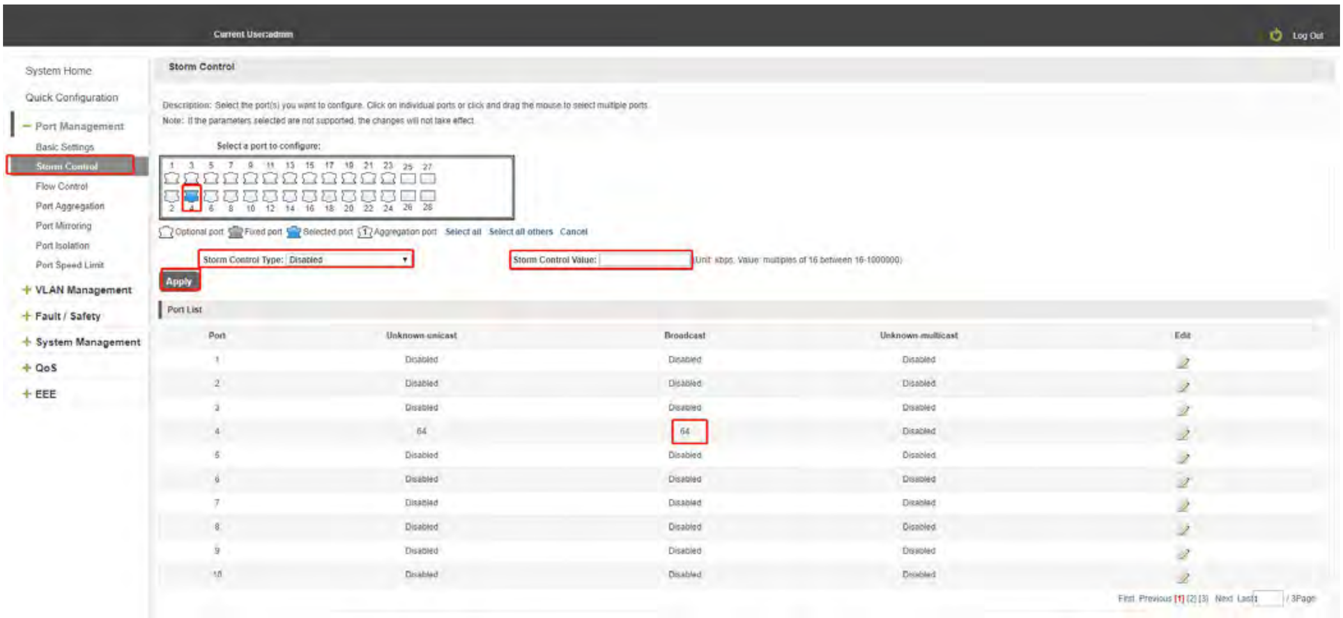
3.Broadcast: Broadcast packet control

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.



Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect

Select a port to configure:

Storm Control Type: Disabled ▾

Storm Control Value: (Unit: kbps, Value: multiples of 16 between 16-1000000)

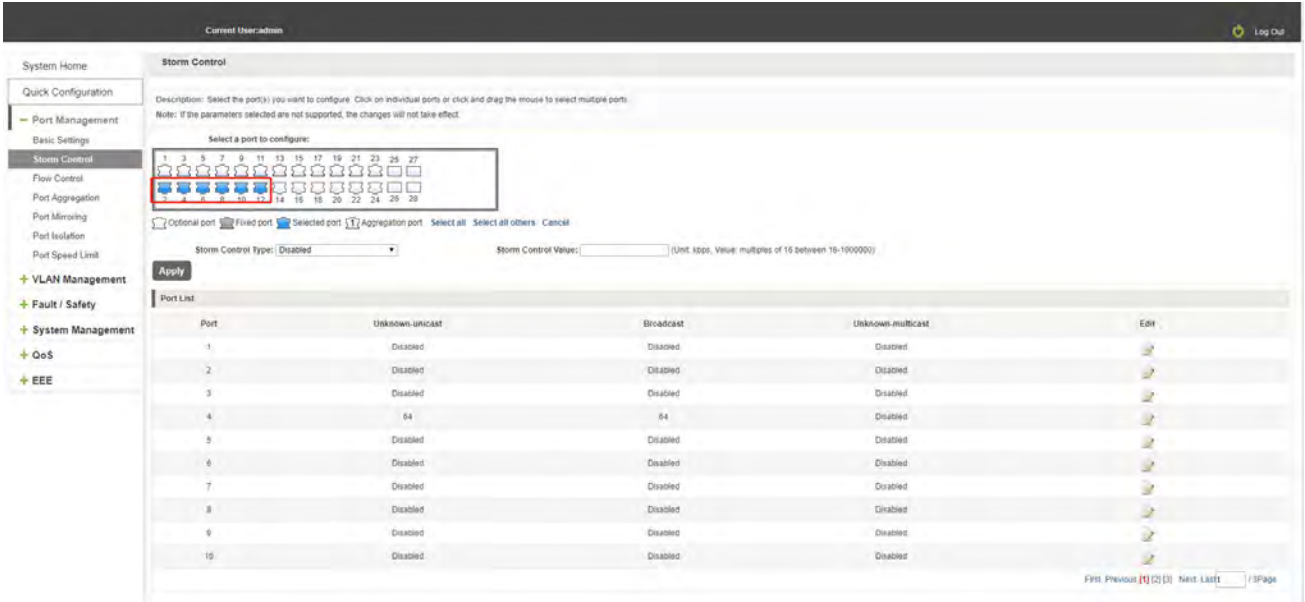
Port List

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	64	64	Disabled	✎
5	Disabled	Disabled	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 3-4: Configuring Storm Control information

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



Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect

Select a port to configure:

Storm Control Type: Disabled ▾

Storm Control Value: (Unit: kbps, Value: multiples of 16 between 16-1000000)

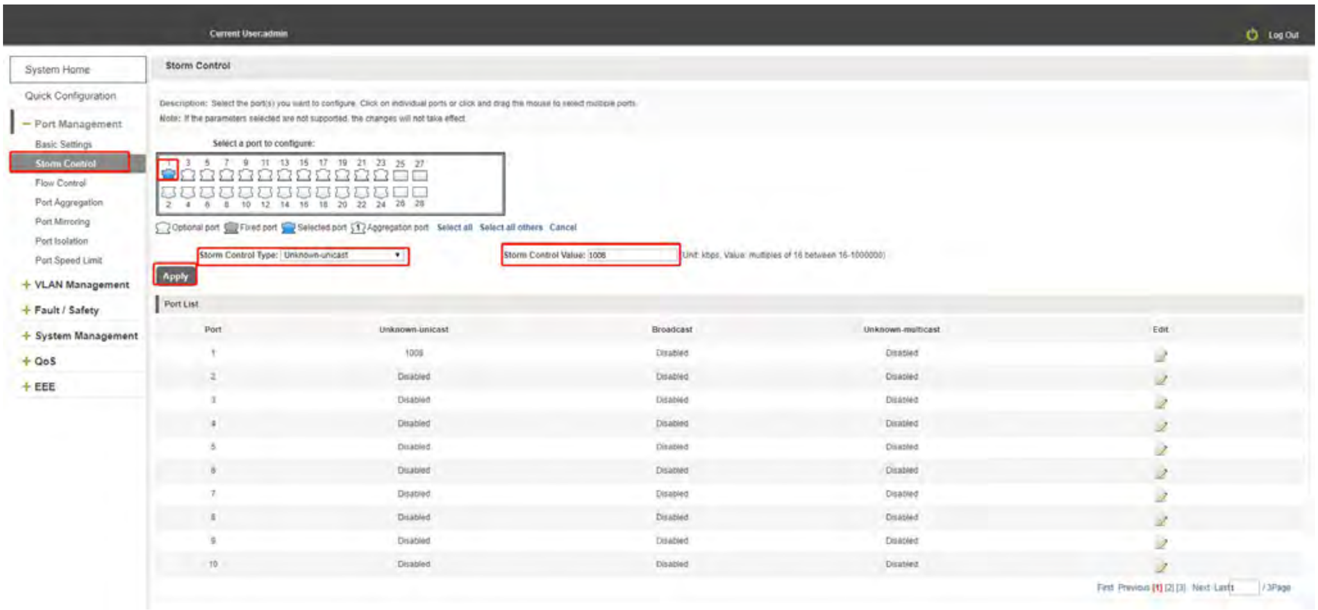
Port List

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	64	64	Disabled	✎
5	Disabled	Disabled	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

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.



Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect

Select a port to configure:

Storm Control Type: Unknown-unicast

Storm Control Value: 1008 Unit: kbps, Value: multiples of 16 between 16-1000000)

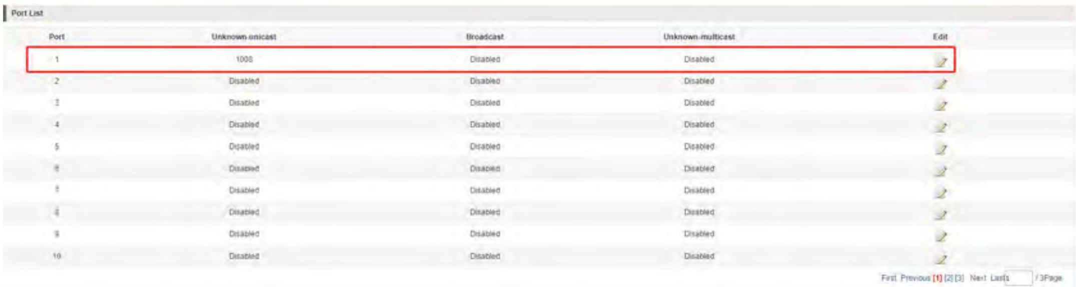
Port List

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	1008	Disabled	Disabled	
2	Disabled	Disabled	Disabled	
3	Disabled	Disabled	Disabled	
4	Disabled	Disabled	Disabled	
5	Disabled	Disabled	Disabled	
6	Disabled	Disabled	Disabled	
7	Disabled	Disabled	Disabled	
8	Disabled	Disabled	Disabled	
9	Disabled	Disabled	Disabled	
10	Disabled	Disabled	Disabled	

First Previous [1] [2] [3] Next Last 1 /3Page

Figure 3-6: Configuring Storm Control information

After the configuration, as shown below:



Port List

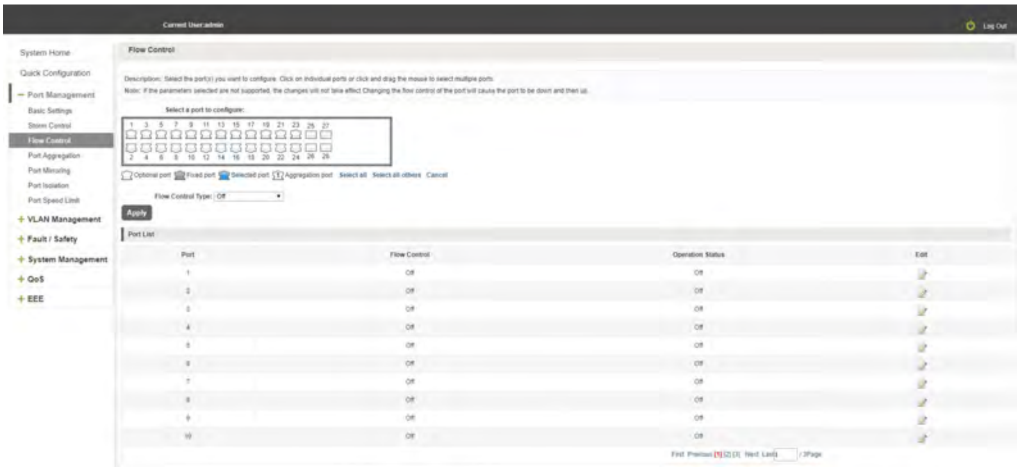
Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	1008	Disabled	Disabled	
2	Disabled	Disabled	Disabled	
3	Disabled	Disabled	Disabled	
4	Disabled	Disabled	Disabled	
5	Disabled	Disabled	Disabled	
6	Disabled	Disabled	Disabled	
7	Disabled	Disabled	Disabled	
8	Disabled	Disabled	Disabled	
9	Disabled	Disabled	Disabled	
10	Disabled	Disabled	Disabled	

First Previous [1] [2] [3] Next Last 1 /3Page

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:



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

Flow Control Type: Off

Port List

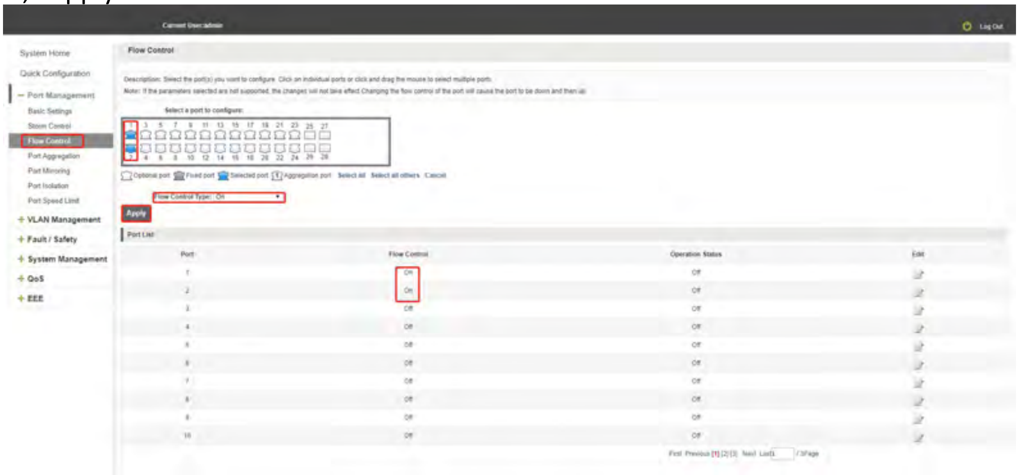
Port	Flow Control	Operation Status	Edit
1	Off	Off	
2	Off	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	
7	Off	Off	
8	Off	Off	
9	Off	Off	
10	Off	Off	

First Previous [1] [2] [3] Next Last 1 /3Page

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":



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect. Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

Flow Control Type: On

Port List

Port	Flow Control	Operation Status	Edit
1	On	Off	
2	On	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	
7	Off	Off	
8	Off	Off	
9	Off	Off	
10	Off	Off	

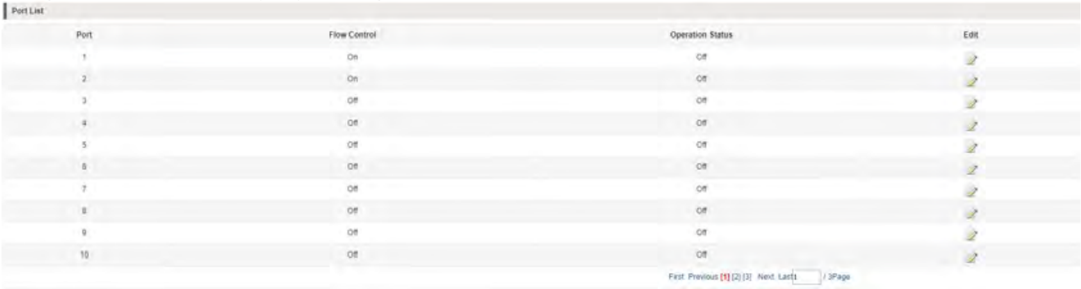
First Previous [1] [2] [3] Next Last 1 /3Page

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:



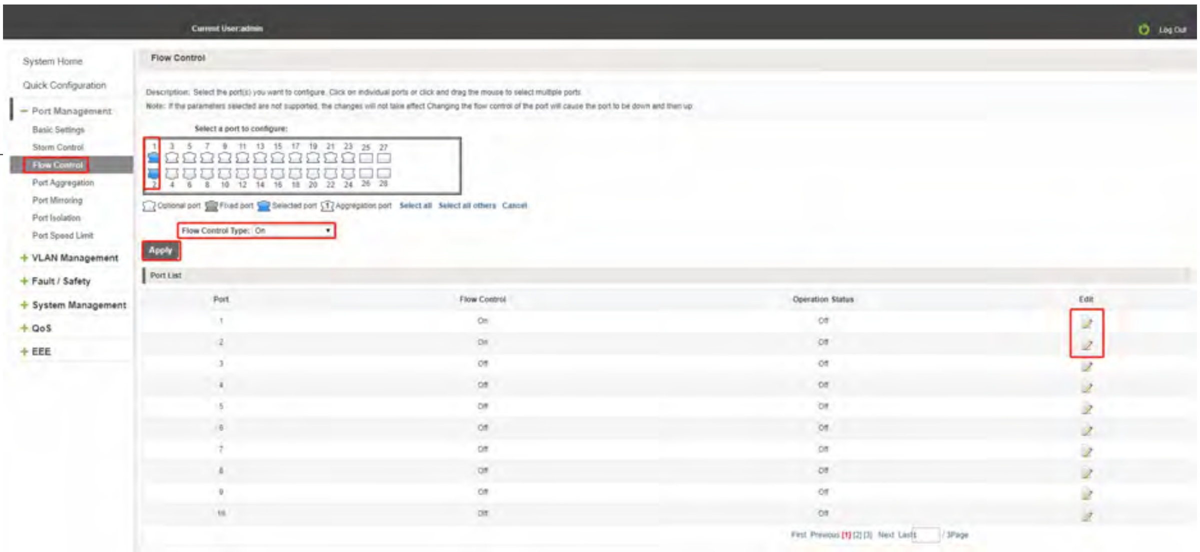
Port List

Port	Flow Control	Operation Status	Edit
1	On	Off	
2	On	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	
7	Off	Off	
8	Off	Off	
9	Off	Off	
10	Off	Off	

First Previous [1] [2] [3] Next Last 1 /3Page

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":



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect Changing the flow control of the port will cause the port to be down and then up

Select a port to configure:

Flow Control Type: On

Port List

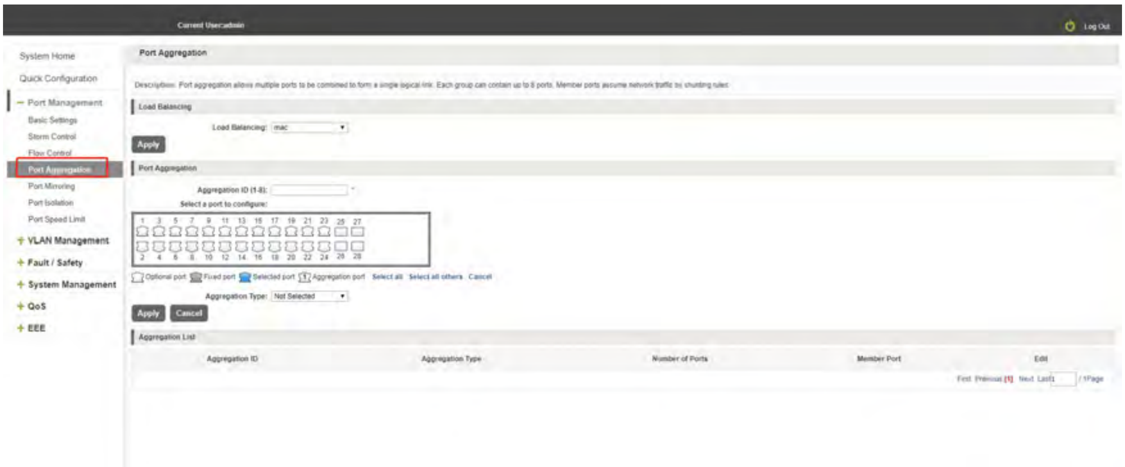
Port	Flow Control	Operation Status	Edit
1	On	Off	✎
2	On	Off	✎
3	Off	Off	✎
4	Off	Off	✎
5	Off	Off	✎
6	Off	Off	✎
7	Off	Off	✎
8	Off	Off	✎
9	Off	Off	✎
10	Off	Off	✎

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**:**



Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8):

Select a port to configure:

Aggregation Type: Not Selected

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit

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;

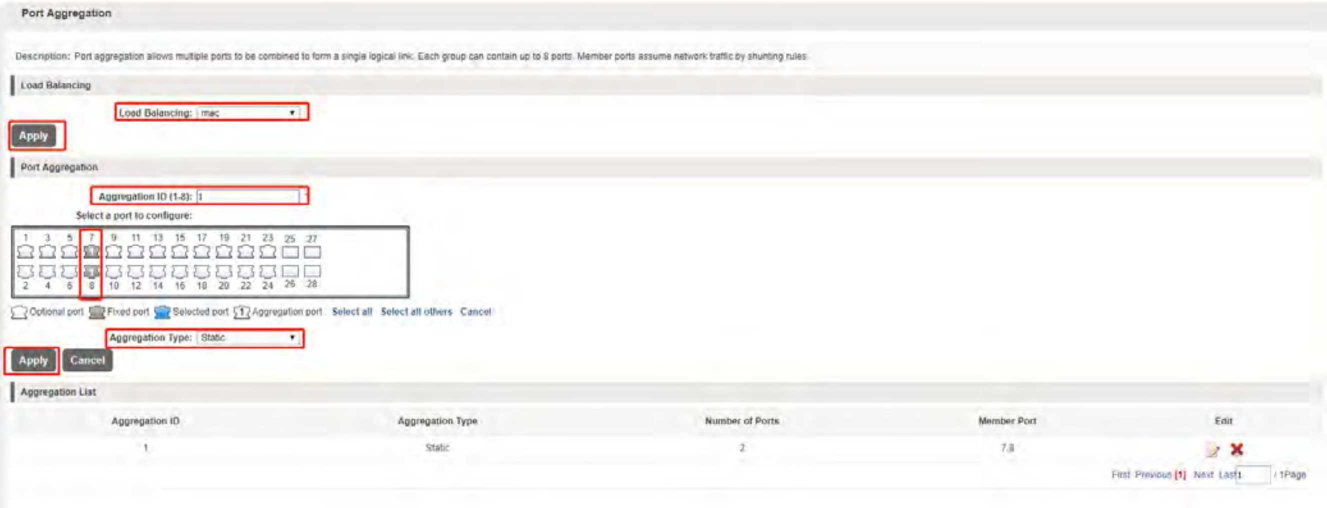
4.Member ports quantity: Displays the number of ports in the link aggregation group contains a total of member port: Displays the current port link aggregation group member prompt

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"



Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules.

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8): 1

Select a port to configure:

Aggregation Type: Static

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Static	2	7,8	

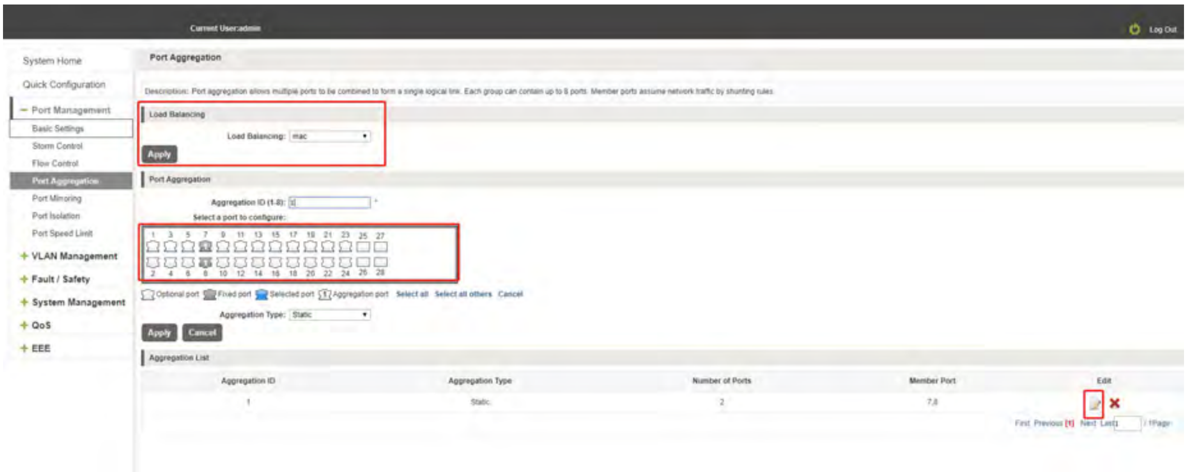
Figure 3-13: Port Aggregation Configuration area

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**:**



Current User:admin

Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules.

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8): 1

Select a port to configure:

Aggregation Type: Static

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Static	2	7,8	

Figure 3-14: To modify the port aggregation

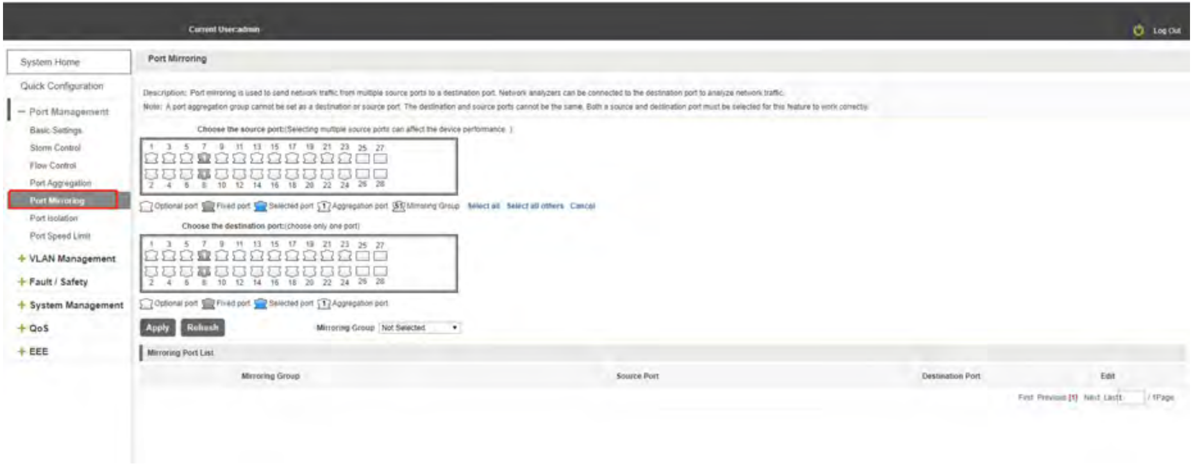
Modify Link Aggregation Procedure:

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:



Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Group	Source Port	Destination Port	Edit

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.

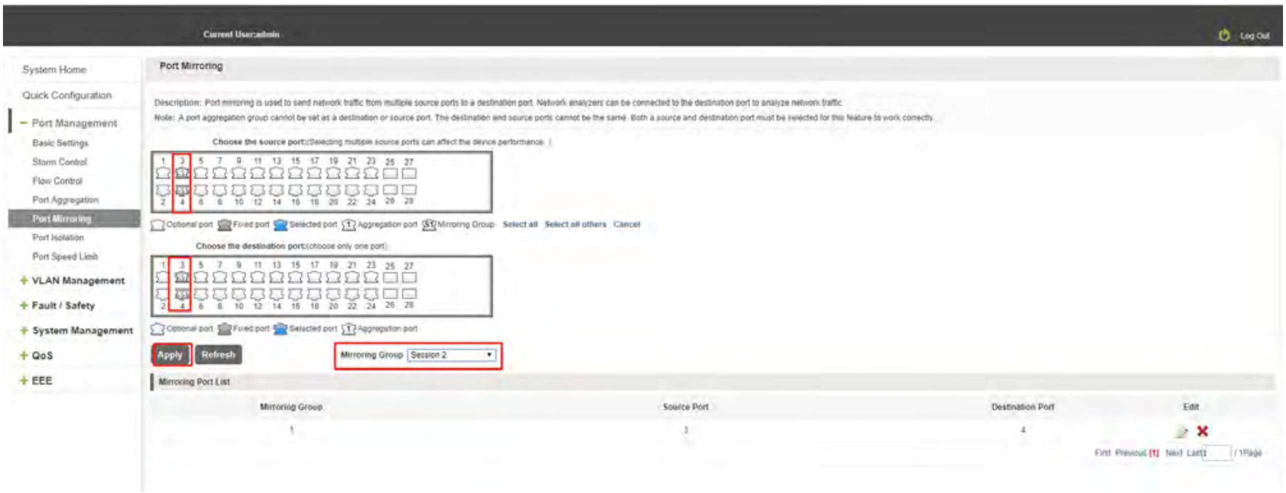
1.Port aggregation port can not be used as the destination port and source port;

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.



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

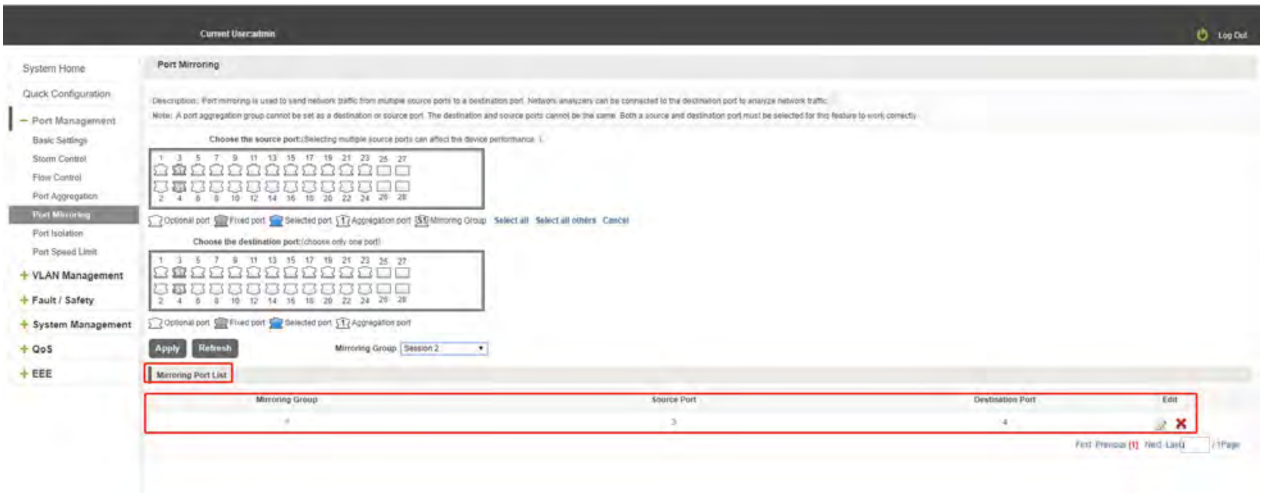
Choose the destination port:(choose only one port)

Mirroring Group: Session 2

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	3	4	

Figure 3-16: Add port mirroring group



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Mirroring Group: Session 2

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	3	4	

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:

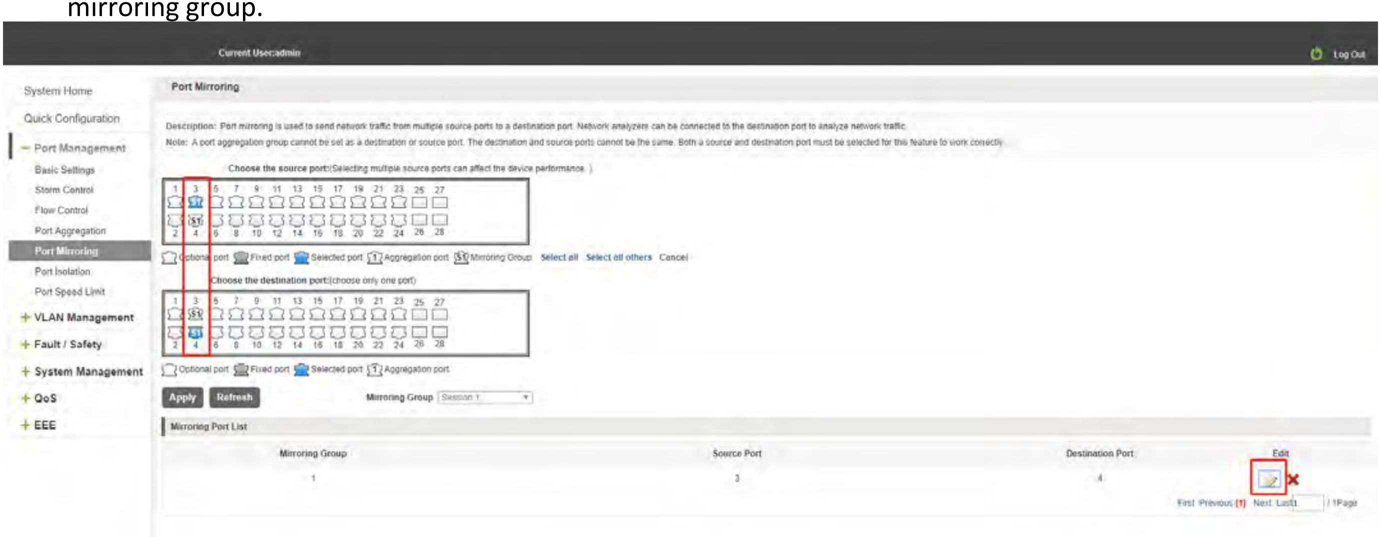
1.On the switch can be configured 7 mirroring group.

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.

3.5.3 TO MODIFY THE PORT MIRRORING GROUP

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



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

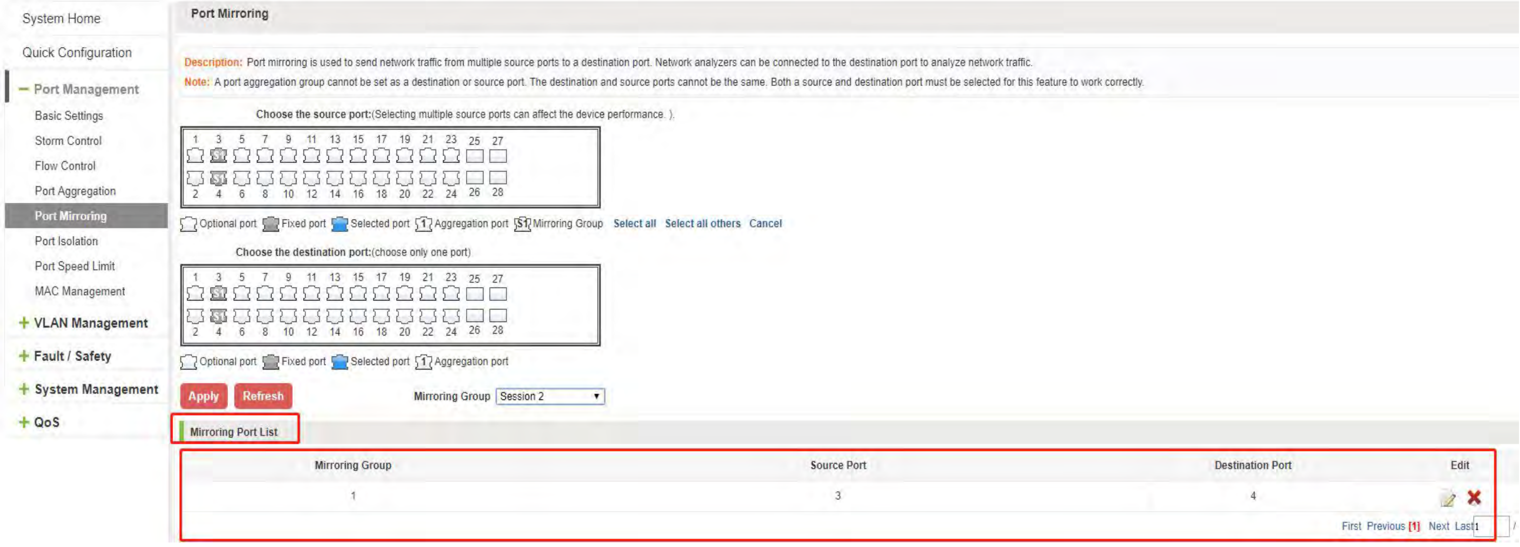
Mirroring Group: Session 1

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	3	4	✗

Figure 3-18: To modify the port mirroring group

Step1:In the image you want to modify the operation of the group column, click on “ ”; step2:Add or remove the corresponding port in the panel;,step3:Click "Apply"



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Session 2

Mirroring Group	Source Port	Destination Port	Edit
1	3	4	

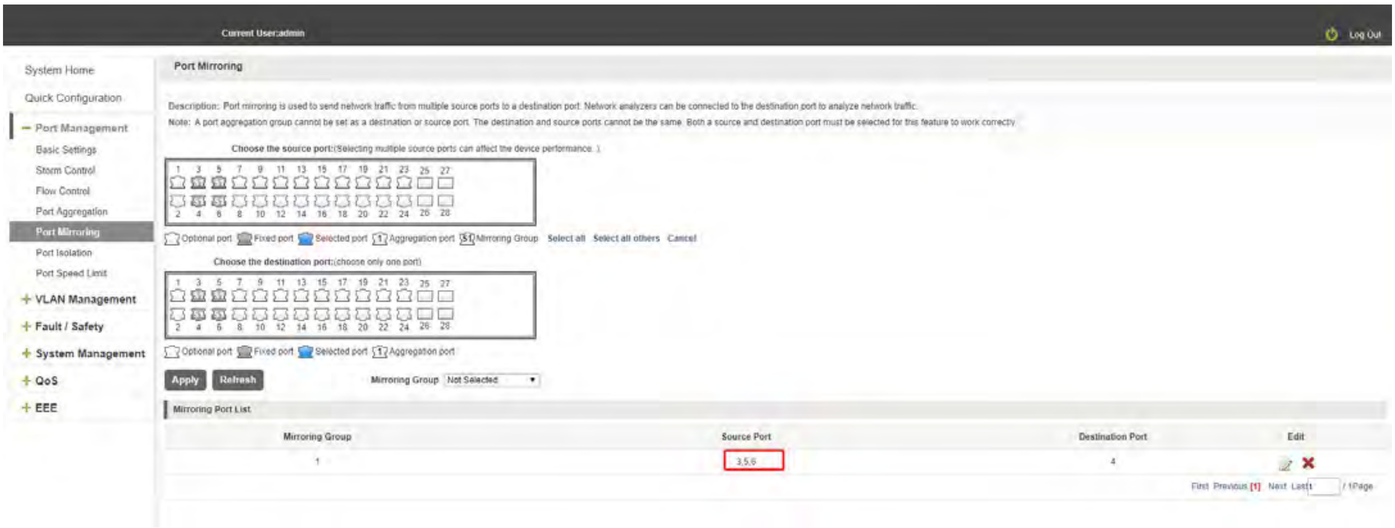
First Previous [1] Next Last 1 /

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.



Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

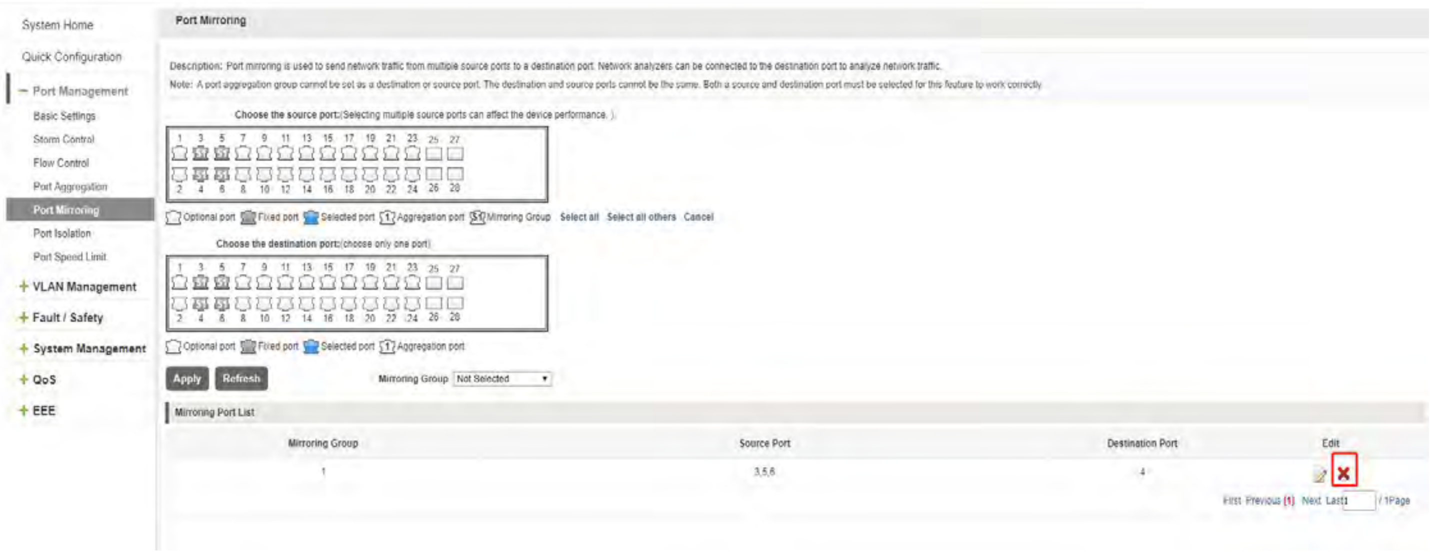
Mirroring Group: Not Selected

Mirroring Group	Source Port	Destination Port	Edit
1	3,5,6	4	

First Previous [1] Next Last 1 /1Page

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)



Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

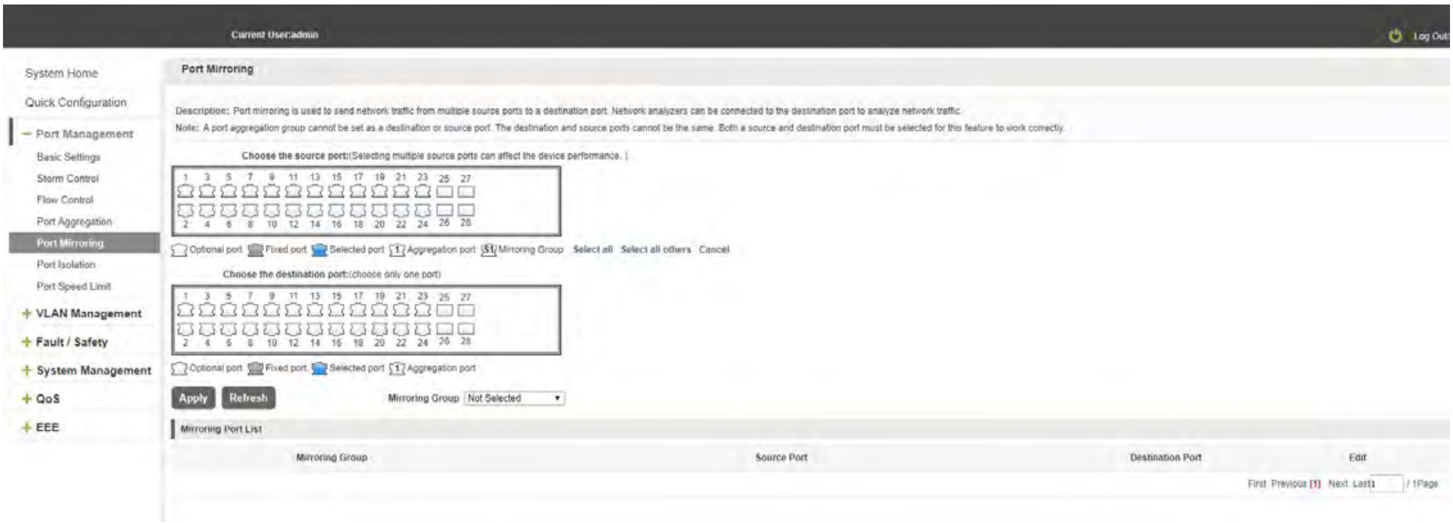
Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Group	Source Port	Destination Port	Edit
1	3,5,6	4	

First Previous [1] Next Last 1 /1Page

Figure 3-21: Delete port mirroring group



Current User:admin

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit

First Previous [1] Next Last 1 / 1Page

Figure 3-22: Deleted successfully port mirroring

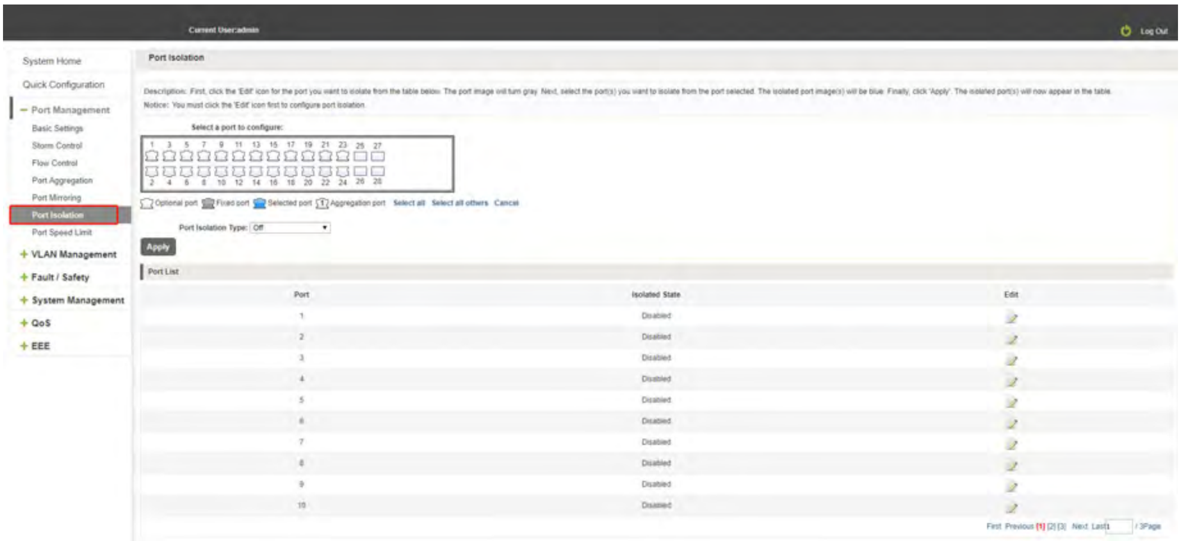
Remove port mirroring configuration steps are as follows:

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:



Current User:admin

Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: Off

Port List

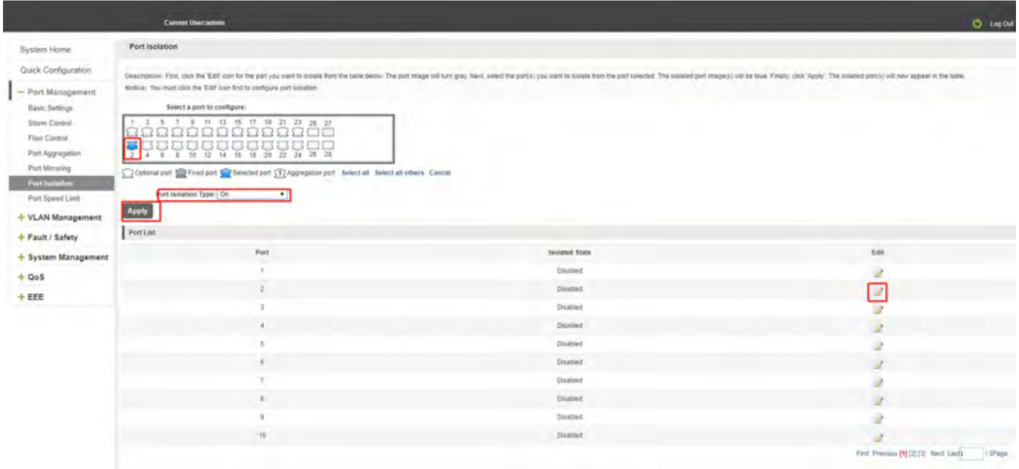
Port	Isolated State	Edit
1	Disabled	✎
2	Disabled	✎
3	Disabled	✎
4	Disabled	✎
5	Disabled	✎
6	Disabled	✎
7	Disabled	✎
8	Disabled	✎
9	Disabled	✎
10	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

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",lat click "Apply".We can view the port you configure ok.



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: On

Port List

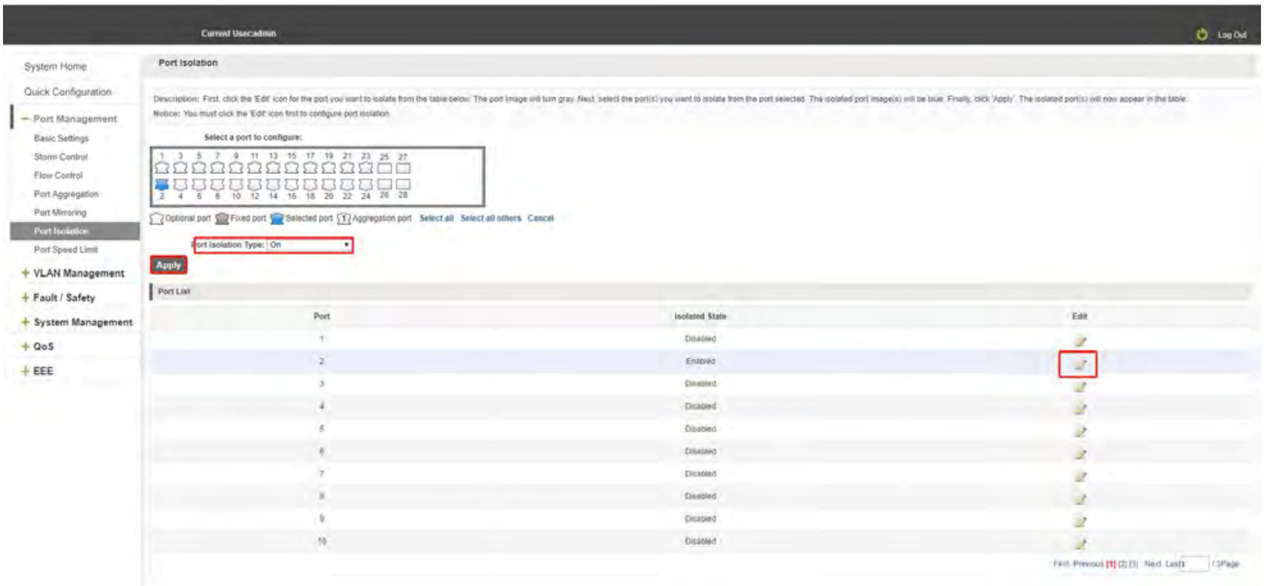
Port	Isolated State	Edit
1	Disabled	
2	Disabled	
3	Disabled	
4	Disabled	
5	Disabled	
6	Disabled	
7	Disabled	
8	Disabled	
9	Disabled	
10	Disabled	

First Previous [1] [2] [3] Next Last[1] /3Page

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".



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: On

Port List

Port	Isolated State	Edit
1	Disabled	
2	Enabled	
3	Disabled	
4	Disabled	
5	Disabled	
6	Disabled	
7	Disabled	
8	Disabled	
9	Disabled	
10	Disabled	

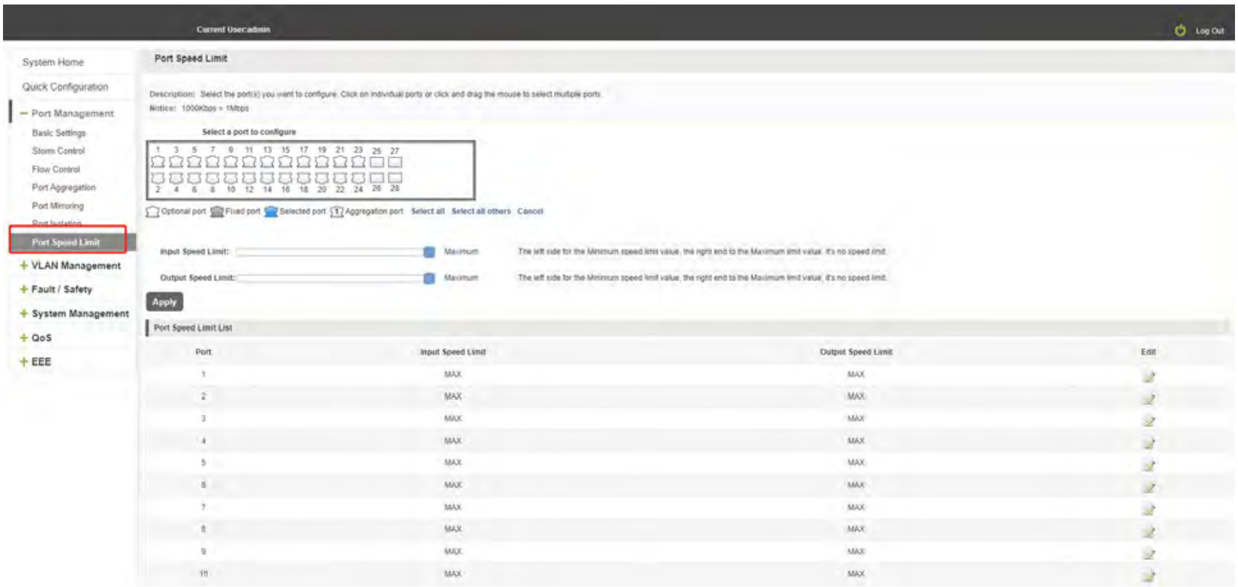
First Previous [1] [2] [3] Next Last[1] /3Page

Figure 3-25: Edit the port isolation

3.7 PORT SPEED LIMT

3.7.1 VIEW PORT RATE LIMITING

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



Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Input Speed Limit: Maximum The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: Maximum The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	MAX	MAX	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎
9	MAX	MAX	✎
10	MAX	MAX	✎

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;

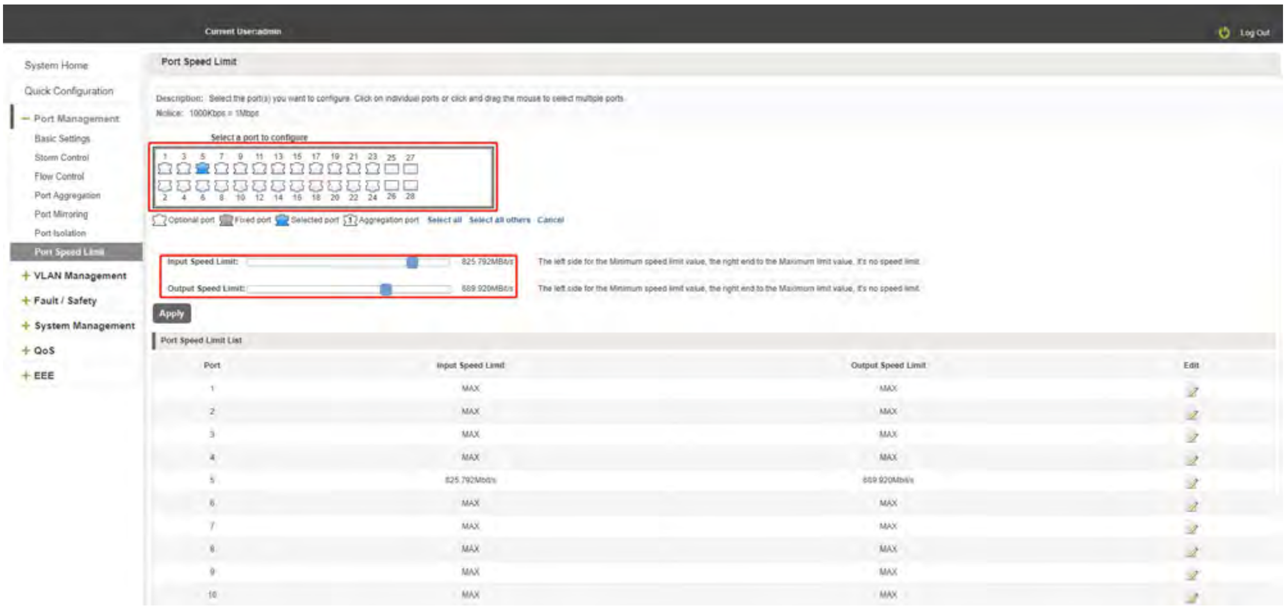
Input limit: uplink port speed;

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.



Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Notice: 1000Kbps = 1Mbps

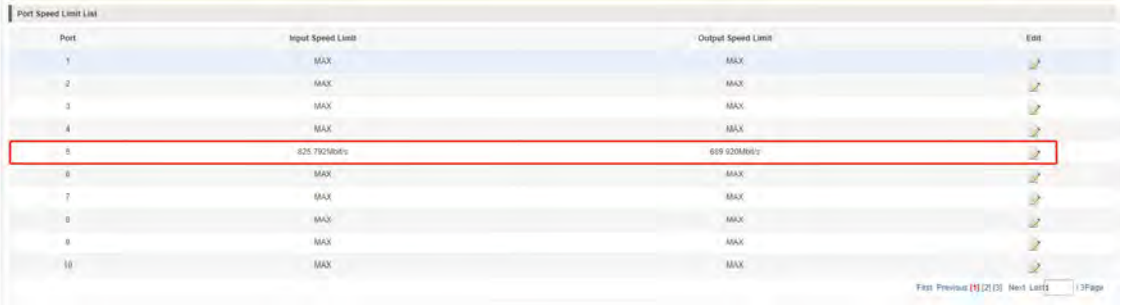
Input Speed Limit: 825.792MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value. It's no speed limit.

Output Speed Limit: 689.920MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value. It's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	MAX	MAX	✎
4	MAX	MAX	✎
5	825.792Mbit/s	689.920Mbit/s	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎
9	MAX	MAX	✎
10	MAX	MAX	✎

Figure 3-27 Configure port rate limiting entrance



Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	MAX	MAX	✎
4	MAX	MAX	✎
5	825.792Mbit/s	689.920Mbit/s	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎
9	MAX	MAX	✎
10	MAX	MAX	✎

Figure 3-28: Port entrance speed limit results

Entrance port rate limiting configuration steps are as follows:

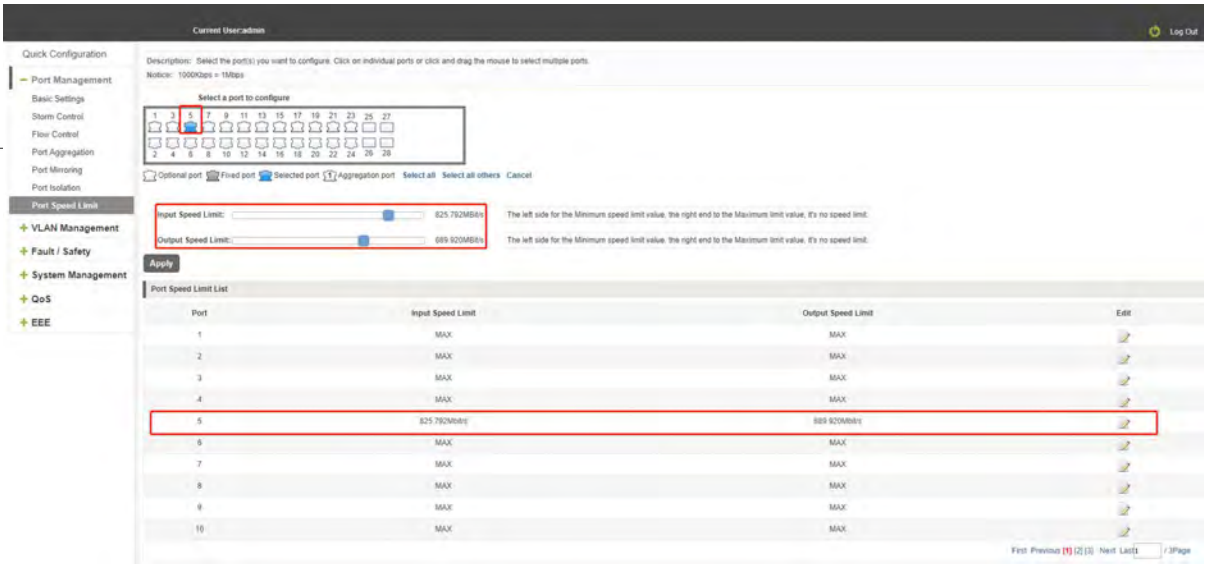
Step1： Click on the right side of the port “ ” Icon or select multiple icons;

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.



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Notice: 1000Kbps = 1Mbps

Input Speed Limit: 825.792MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: 689.920MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	
2	MAX	MAX	
3	MAX	MAX	
4	MAX	MAX	
5	825.792Mbit/s	689.920Mbit/s	
6	MAX	MAX	
7	MAX	MAX	
8	MAX	MAX	
9	MAX	MAX	
10	MAX	MAX	

Figure 3-29: Remove the port speed limit

Remove uplink port rate limiting steps are as follows:

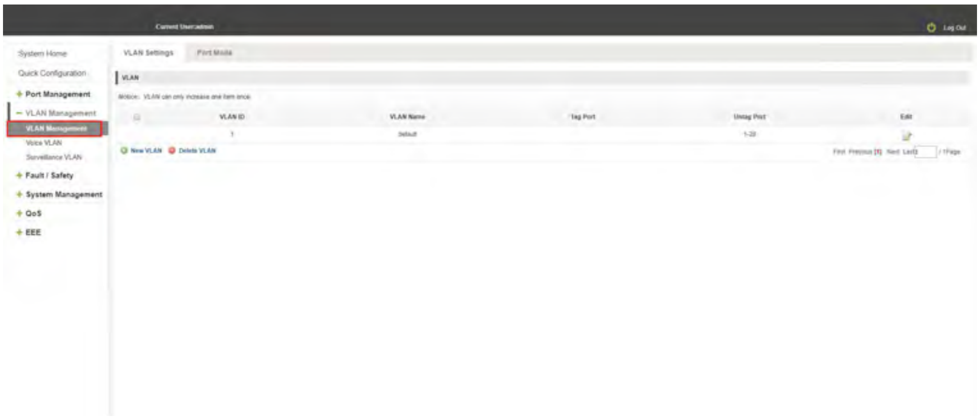
Step1:Click on the right side of the port icon； step2： In the area of the port rate configuration value rate strip pulled to the far right;step3： Click the "Apply" button to complete the configuration.

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:



VLAN

Notice: VLAN can only increase one item once.

□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-28	

Figure 4-1: VLAN configuration information

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

1.VLAN ID: VLAN ID value is displayed;

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

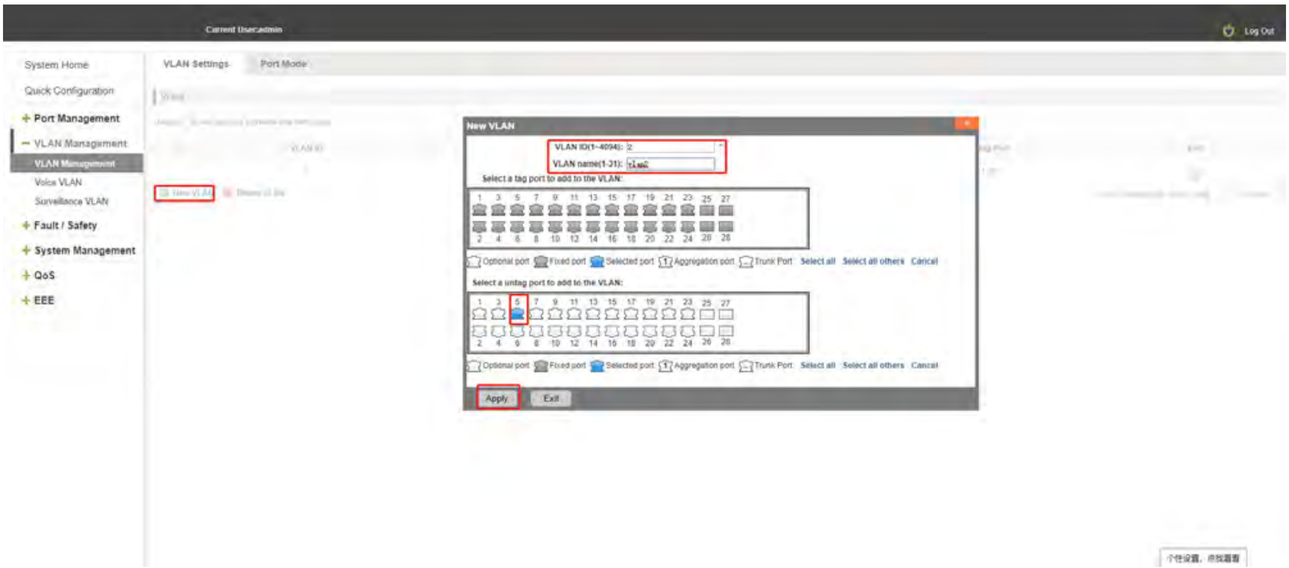
3.VLAN IP address: Displays the switch's management IP;

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:



New VLAN

VLAN ID(1~4094): 2

VLAN name(1-31): vlan2

Figure 4-2: Adding a VLAN

Adding a VLAN, follow these steps:

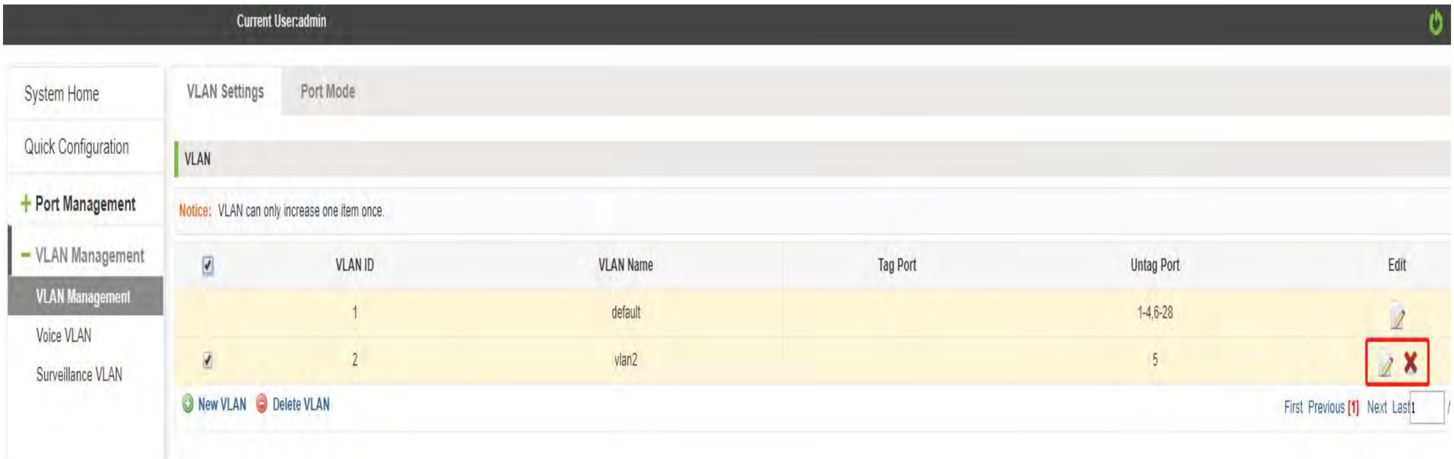
Step1:Click "NEW vlan" connection;

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.



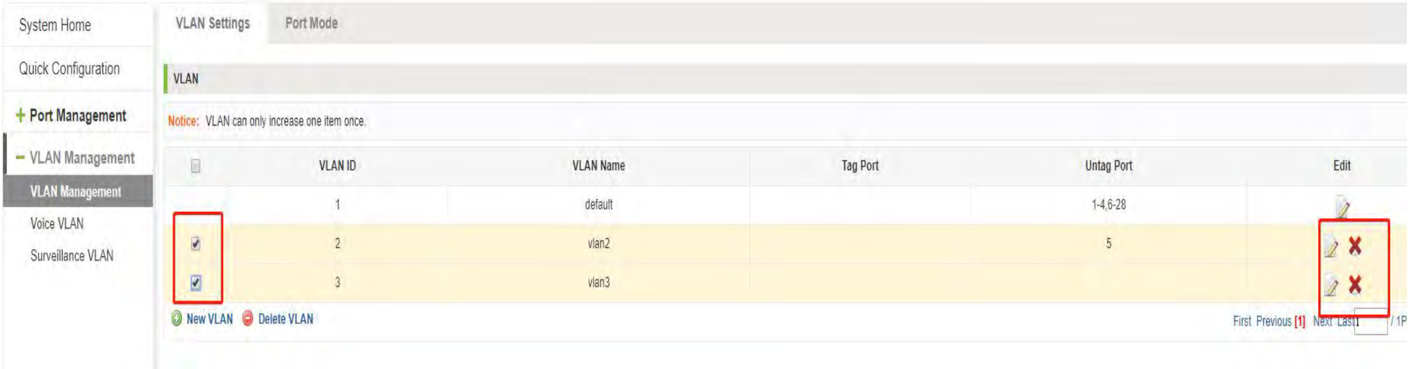
Notice: VLAN can only increase one item once.

☑	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-4,6-28	
☑	2	vlan2		5	

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.



Notice: VLAN can only increase one item once.

☐	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-4,6-28	
☑	2	vlan2		5	
☑	3	vlan3			

Figure 4-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

Step1:Select you want to delete VLAN check box;

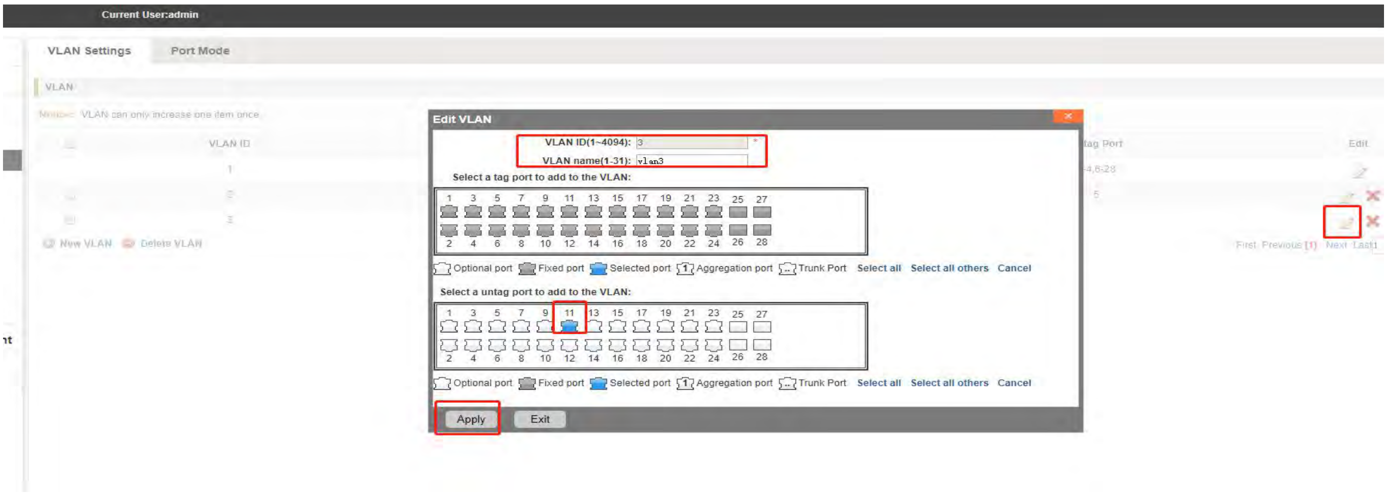
setp2:Click on the bottom left "Delete VLAN" connection;

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:


Current User:admin

Edit VLAN

VLAN ID(1~4094): 3

VLAN name(1-31): vlan3

Select a tag port to add to the VLAN:

Select a untag port to add to the VLAN:

Figure 4-5: Change the port to the VLAN

Add the port to the VLAN, follow these steps:

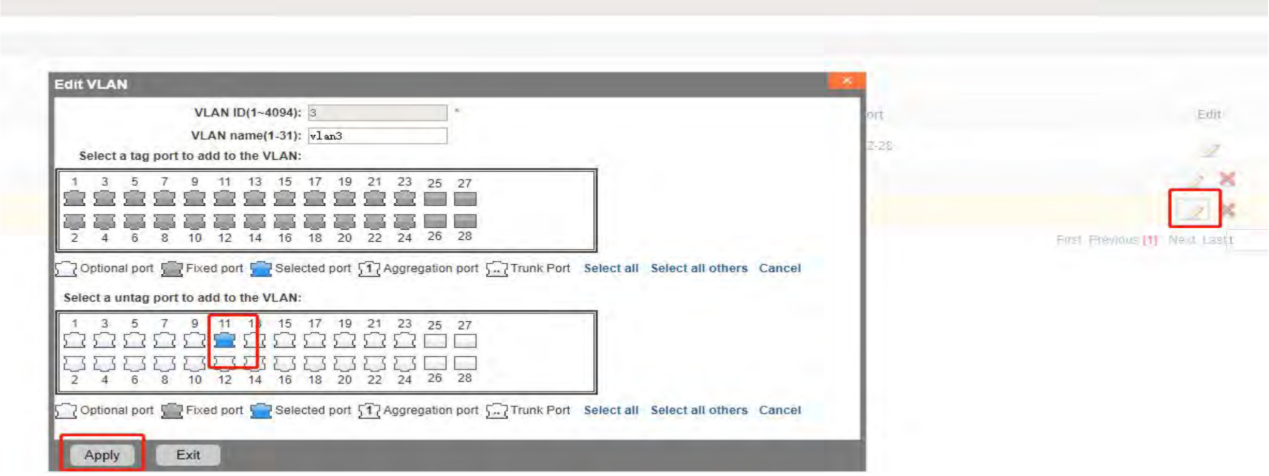
Step1:Click“ ✎ ”icon.

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:


Edit VLAN

VLAN ID(1~4094): 3

VLAN name(1-31): vlan3

Select a tag port to add to the VLAN:

Select a untag port to add to the 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;

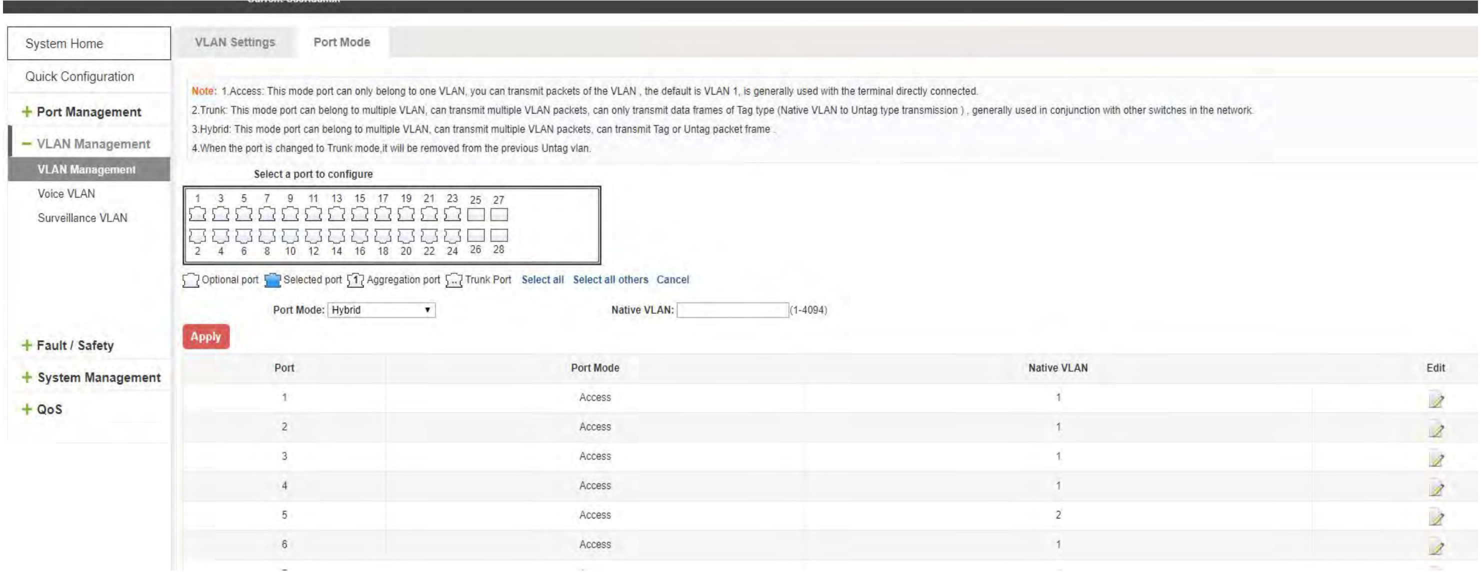
4.1.5 VIEW PORT MODE

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.



Note: 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 Tag 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 Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Select a port to configure

Port Mode: Hybrid ▾   Native VLAN: (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Access	1	✎
2	Access	1	✎
3	Access	1	✎
4	Access	1	✎
5	Access	2	✎
6	Access	1	✎

Figure 4-7: View port mode information

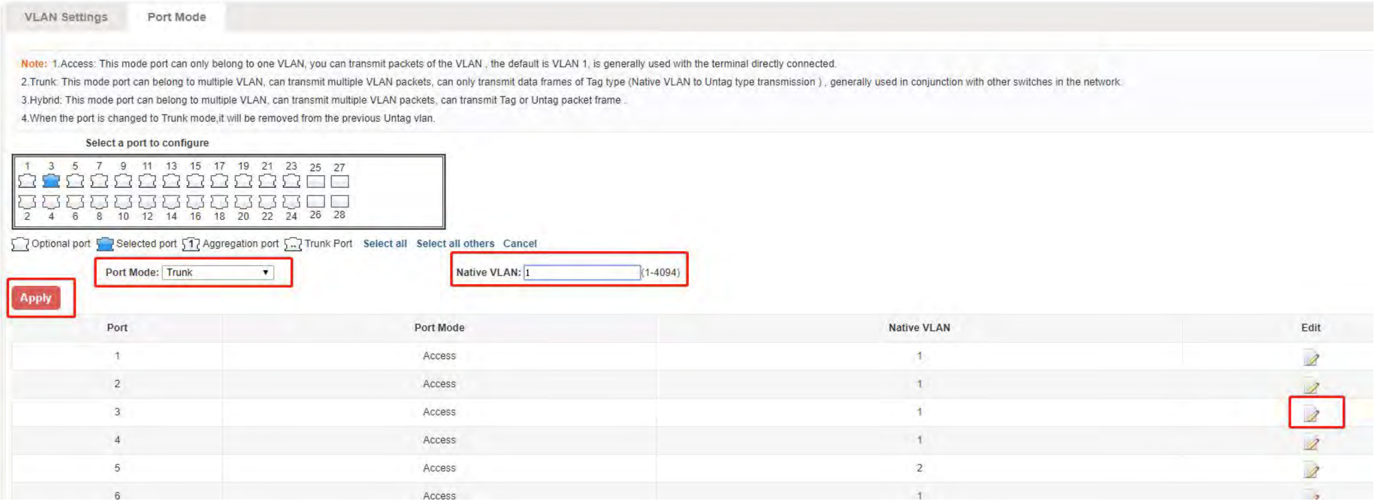
Displayed in the port mode list is the property value of the port configuration of the current switch:

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 :



Note: 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 Tag 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 Tag or Untag packet frame .

4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Port Mode: Trunk

Native VLAN: 1 (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	
5	Access	2	
6	Access	1	

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;

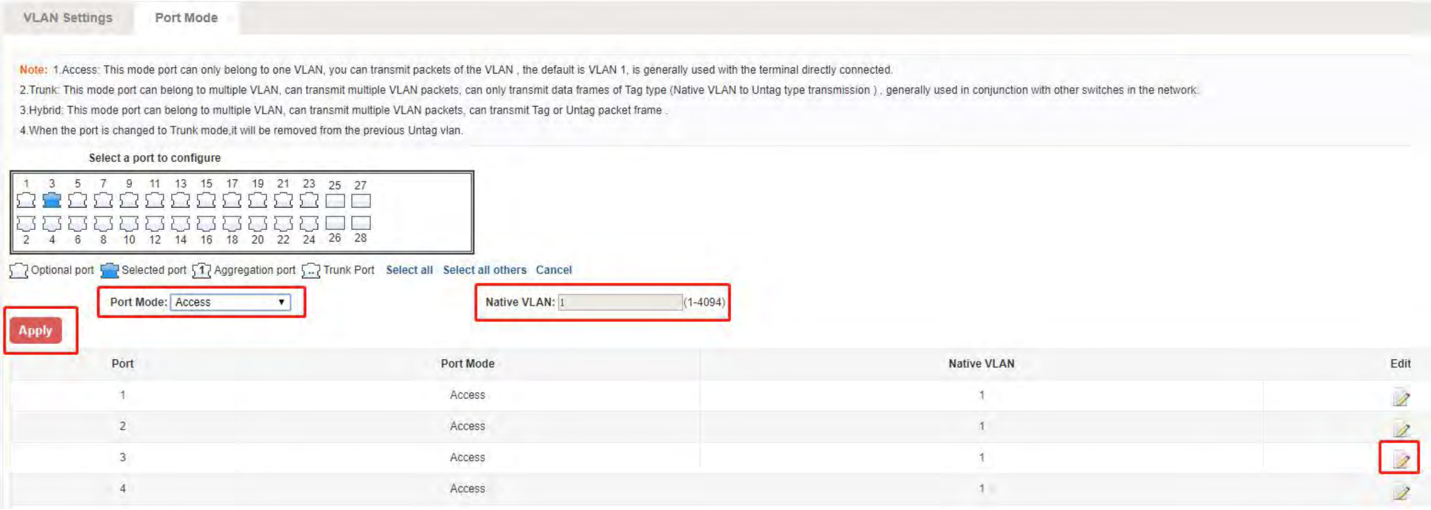
step3:Set this port native VLAN that you have created;

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.



Note: 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 Tag 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 Tag or Untag packet frame .

4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Port Mode: Access

Native VLAN: 1 (1-4094)

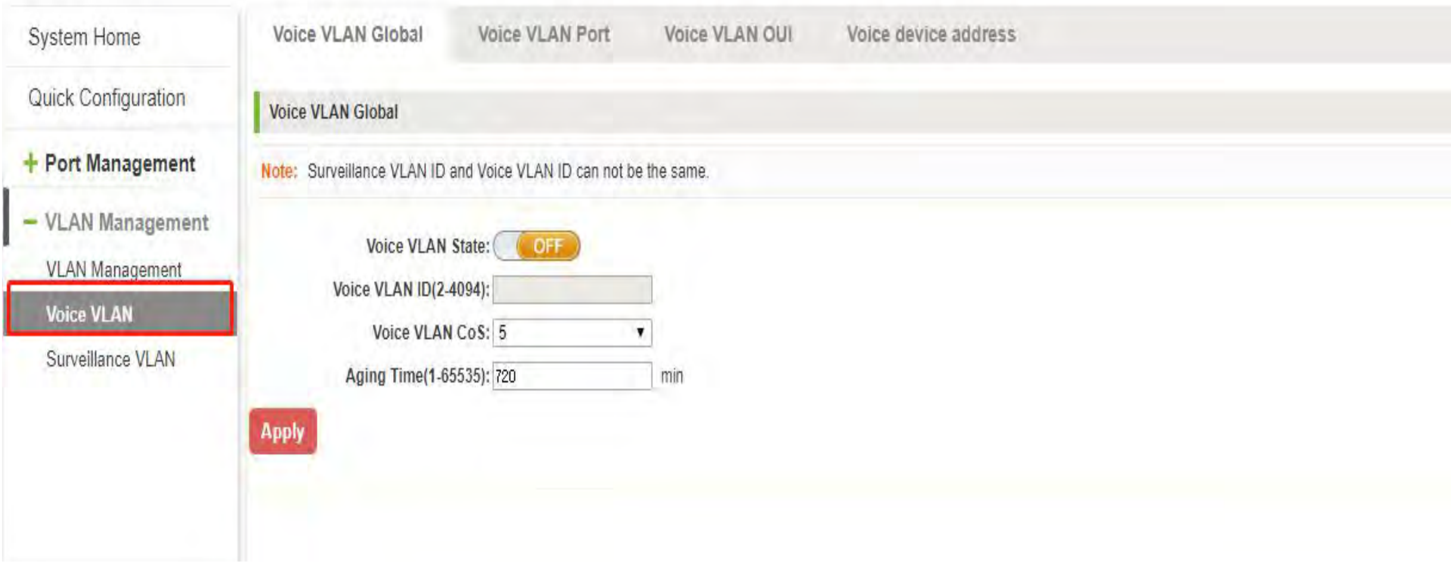
Port	Port Mode	Native VLAN	Edit
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	

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:



Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.

Voice VLAN State: OFF

Voice VLAN ID(2-4094):

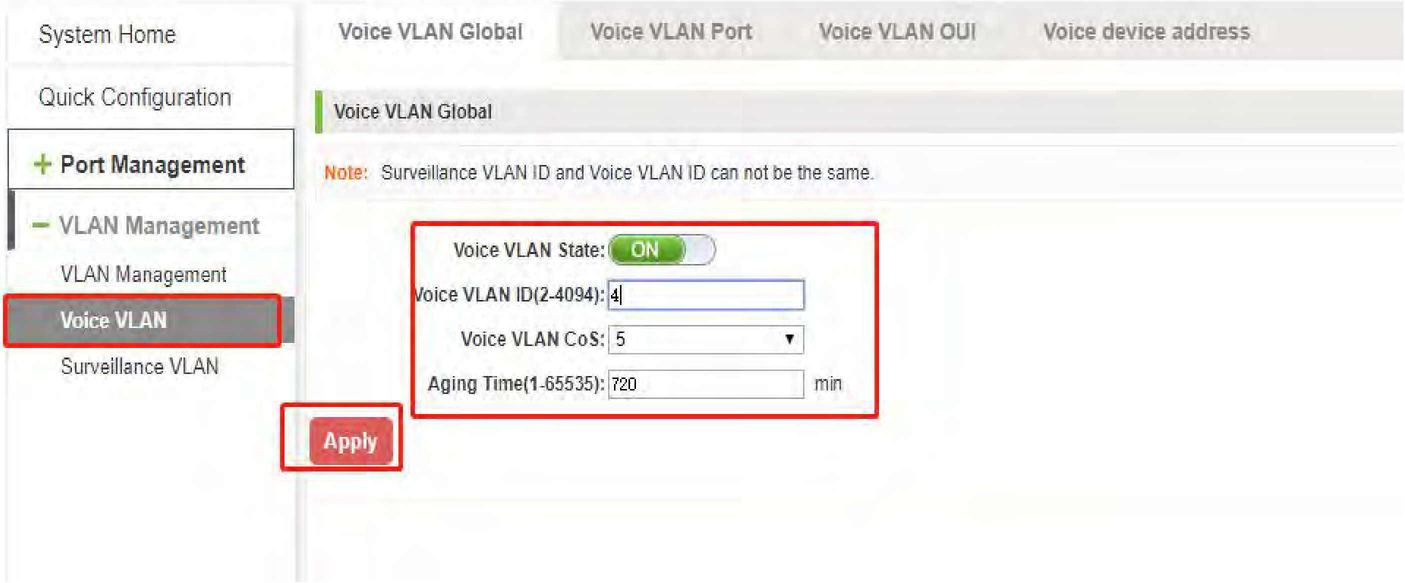
Voice VLAN CoS: 5

Aging Time(1-65535): 720 min

Figure 4-10: View the voice vlan configuration

4.2.2 ENABLE THE VOICE VLAN

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



Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.

Voice VLAN State: ON

Voice VLAN ID(2-4094): 4

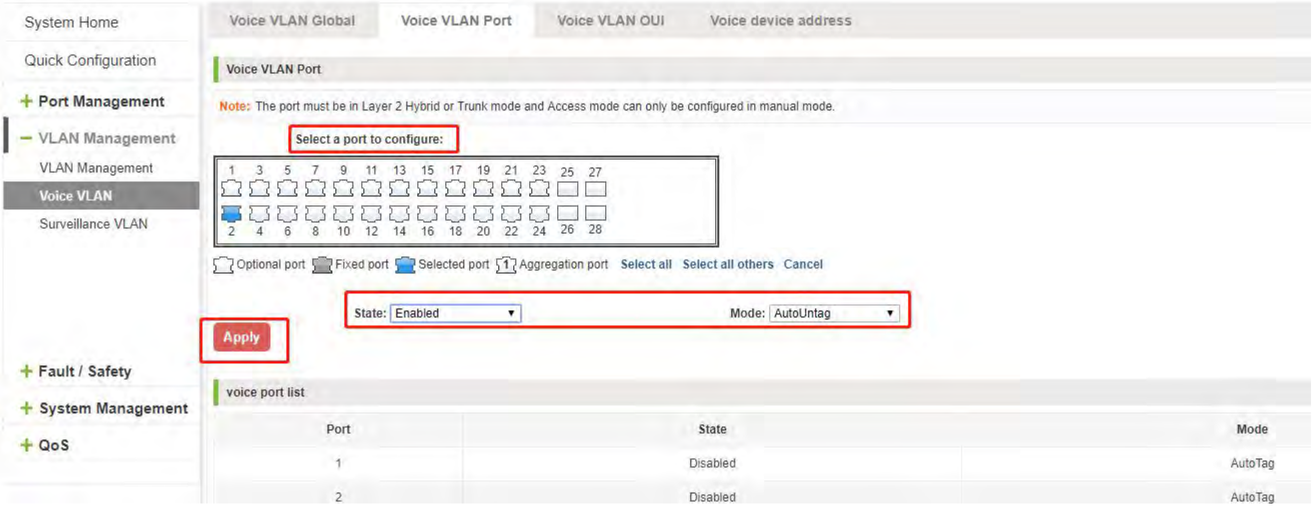
Voice VLAN CoS: 5

Aging Time(1-65535): 720 min

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.



Note: The port must be in Layer 2 Hybrid or Trunk mode and Access mode can only be configured in manual mode.

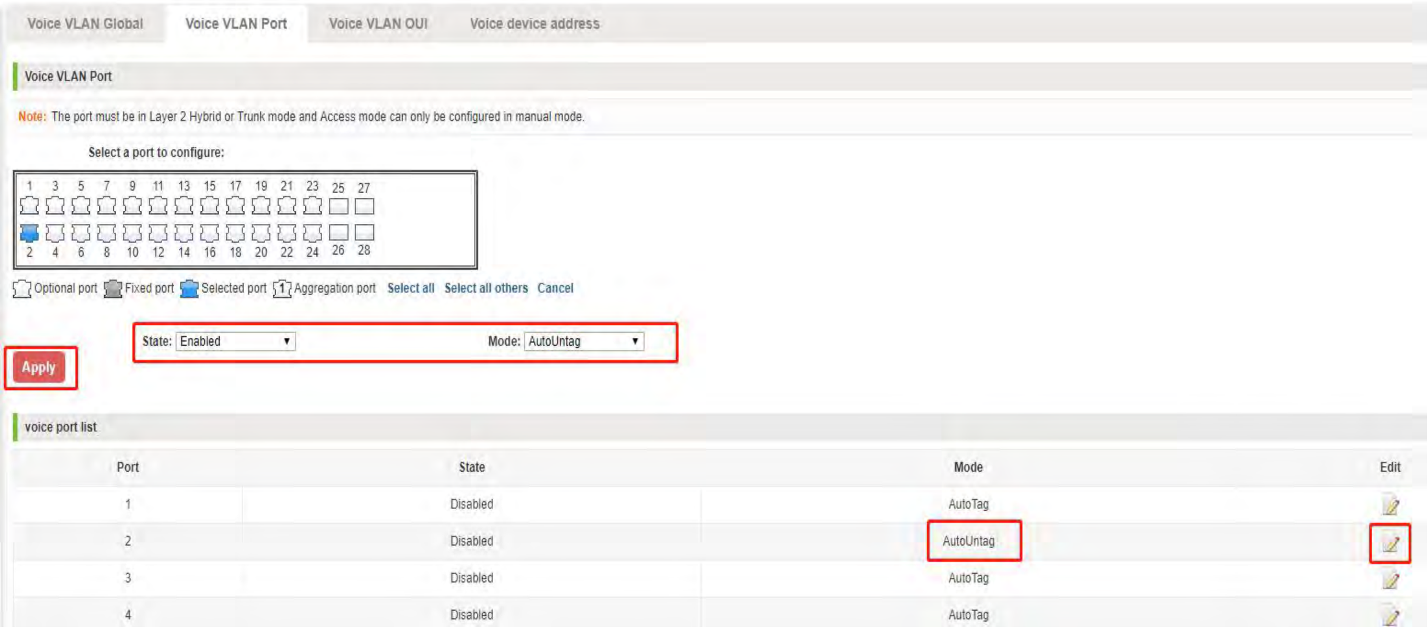
State: Enabled

Mode: AutoUntag

Port	State	Mode
1	Disabled	AutoTag
2	Disabled	AutoTag

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”.



Voice VLAN Port

Note: The port must be in Layer 2 Hybrid or Trunk mode and Access mode can only be configured in manual mode.

Select a port to configure:

State: Enabled

Mode: AutoUntag

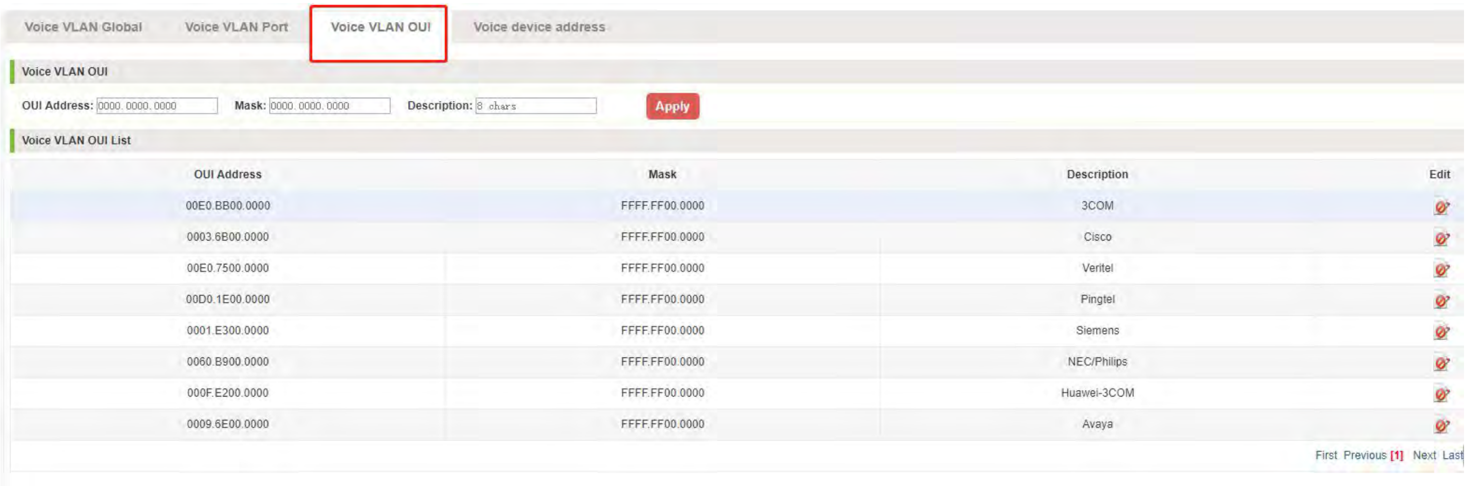
voice port list

Port	State	Mode	Edit
1	Disabled	AutoTag	
2	Disabled	AutoUntag	
3	Disabled	AutoTag	
4	Disabled	AutoTag	

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:



Voice VLAN OUI

OUI Address: 0000.0000.0000 Mask: 0000.0000.0000 Description: 8 chars

Voice VLAN OUI List

OUI Address	Mask	Description	Edit
00E0.BB00.0000	FFFF.FF00.0000	3COM	
0003.6B00.0000	FFFF.FF00.0000	Cisco	
00E0.7500.0000	FFFF.FF00.0000	Veritel	
00D0.1E00.0000	FFFF.FF00.0000	Pingtel	
0001.E300.0000	FFFF.FF00.0000	Siemens	
0060.B900.0000	FFFF.FF00.0000	NEC/Philips	
000F.E200.0000	FFFF.FF00.0000	Huawei-3COM	
0009.6E00.0000	FFFF.FF00.0000	Avaya	

Figure 4-14: Voice vlan OUI table

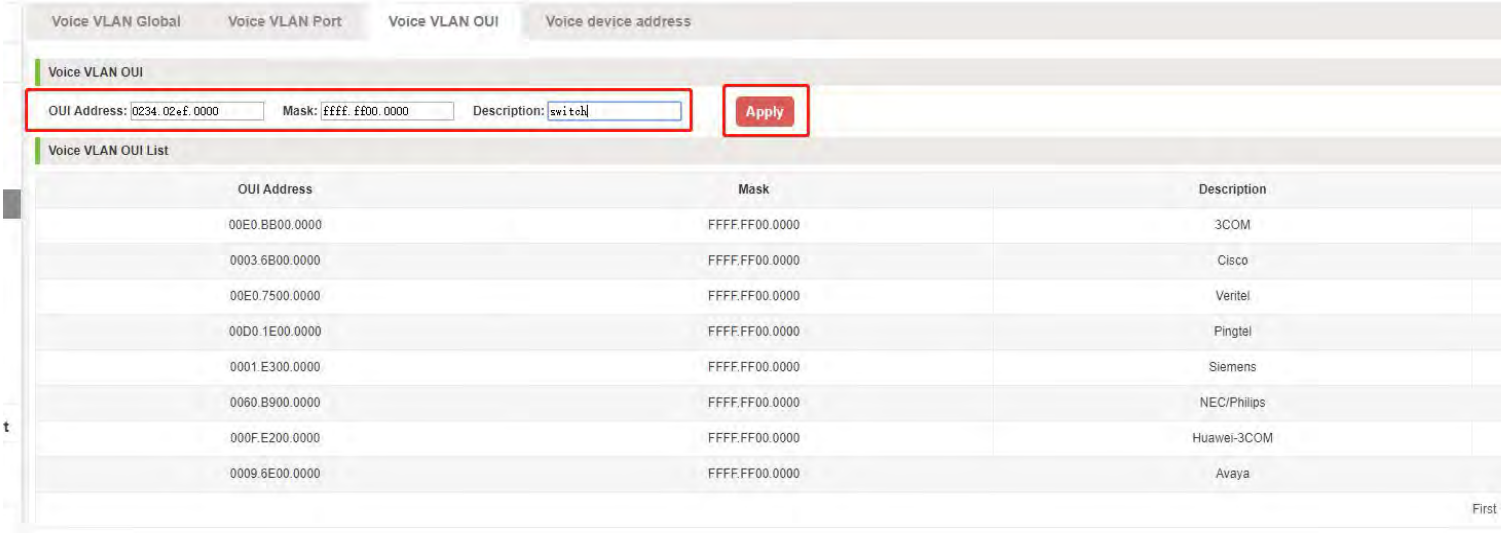
Add the oui entry,enter valid address and mask,click “Save”:

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.



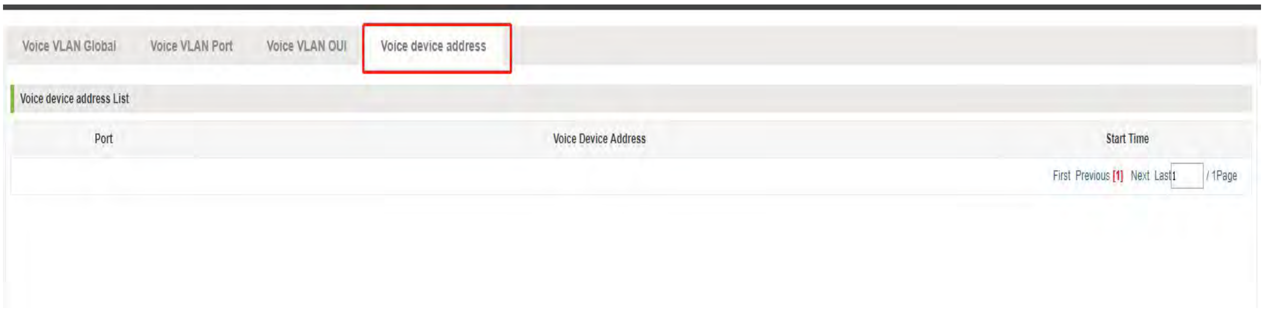
OUI Address: 0234.02ef.0000 Mask: ffff.ff00.0000 Description: switch

OUI Address	Mask	Description
00E0.BB00.0000	FFFF.FF00.0000	3COM
0003.6B00.0000	FFFF.FF00.0000	Cisco
00E0.7500.0000	FFFF.FF00.0000	Veritel
00D0.1E00.0000	FFFF.FF00.0000	Pingtel
0001.E300.0000	FFFF.FF00.0000	Siemens
0060.B900.0000	FFFF.FF00.0000	NEC/Philips
000F.E200.0000	FFFF.FF00.0000	Huawei-3COM
0009.6E00.0000	FFFF.FF00.0000	Avaya

Figure 4-15: Add Voice vlan OUI entry

4.2.5 VIEW THE VOICE VLAN DEVICE

When the device receives the oui entry from the port on which the voice VLAN is opened, the device is displayed in the list:



Port	Voice Device Address	Start Time

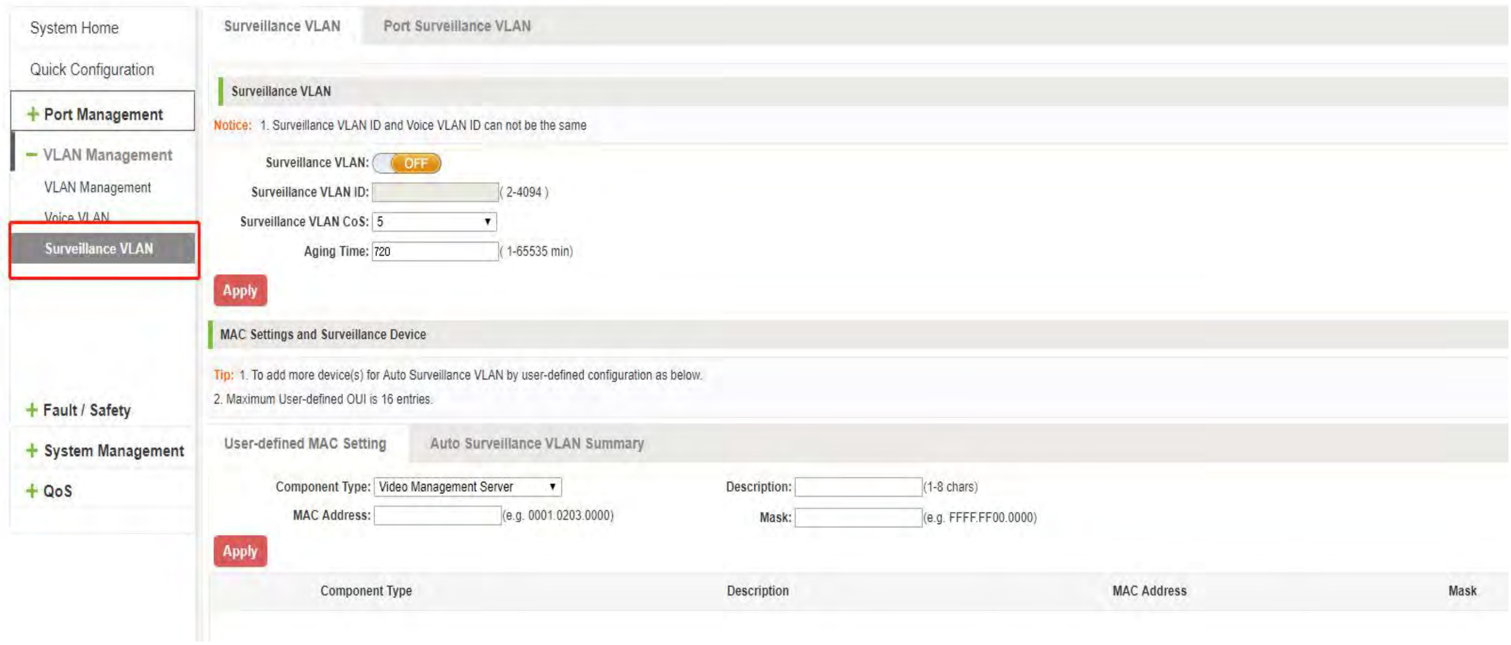
Figure 4-16: View the voice vlan device

4.3 SURVEILLANCE VLAN

4.3.1 VIEW THE SURVEILLANCE VLAN CONFIGURATION

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

Notice:Surveillance VLAN ID and Voice VLAN ID can not be the same



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: OFF

Surveillance VLAN ID: (2-4094)

Surveillance VLAN CoS: 5

Aging Time: 720 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

Component Type: Video Management Server

Description: (1-8 chars)

MAC Address: (e.g. 0001.0203.0000)

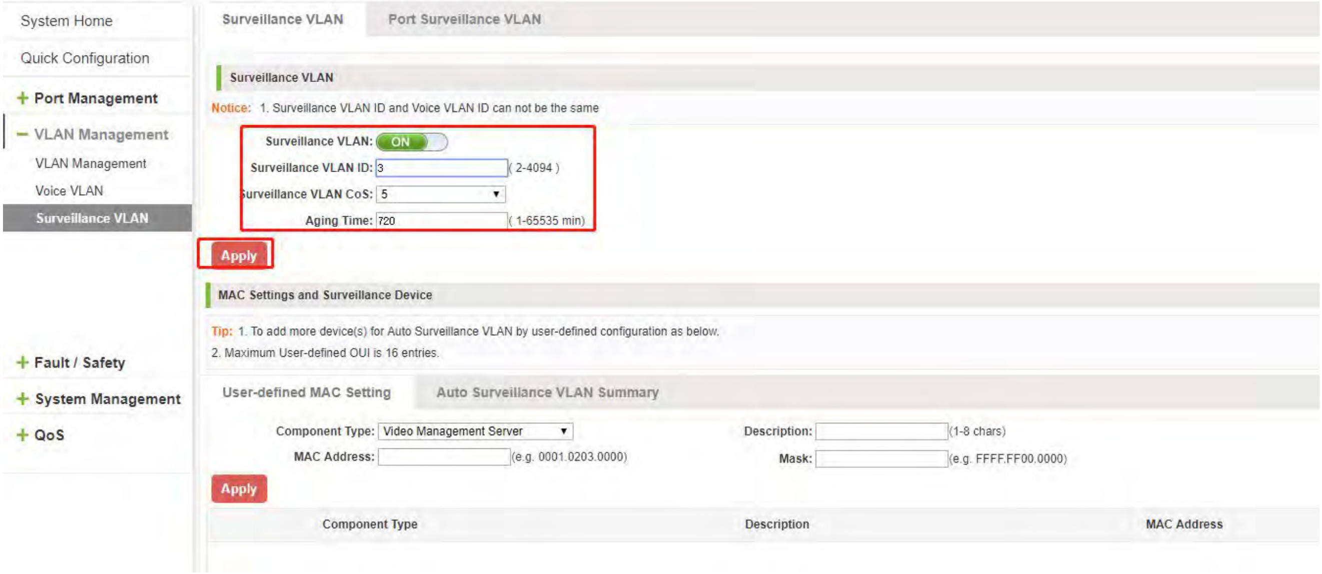
Mask: (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address	Mask

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 .



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: ON

Surveillance VLAN ID: 3 (2-4094)

Surveillance VLAN CoS: 5

Aging Time: 720 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

Component Type: Video Management Server

Description: (1-8 chars)

MAC Address: (e.g. 0001.0203.0000)

Mask: (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address

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;

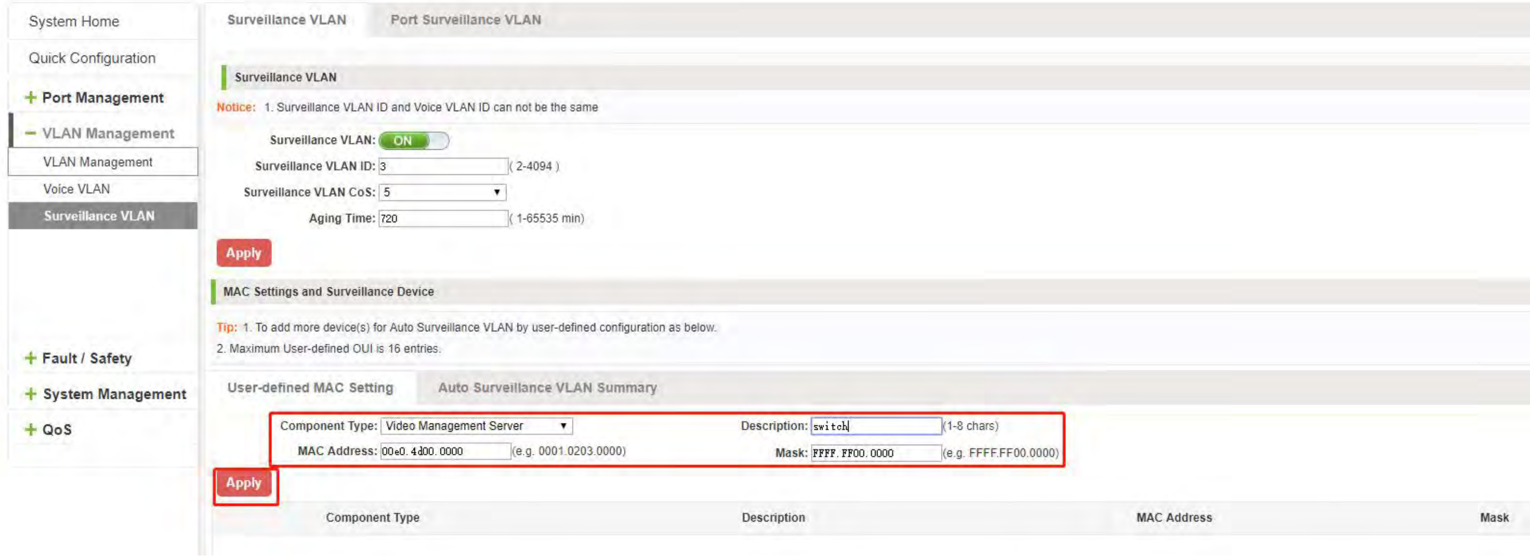
step3:in the surveillance VLAN COS text box,choose 5(default is 5);

step 4:in the aging time text box,enter aging time ,such as 500(default is 720min);

step 5:click on save;

4.3.3 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 .



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: ON

Surveillance VLAN ID: 3 (2-4094)

Surveillance VLAN CoS: 5

Aging Time: 720 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

Component Type: Video Management Server

Description: switch (1-8 chars)

MAC Address: 00e0.4d00.0000 (e.g. 0001.0203.0000)

Mask: FFFF.FF00.0000 (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address	Mask

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;

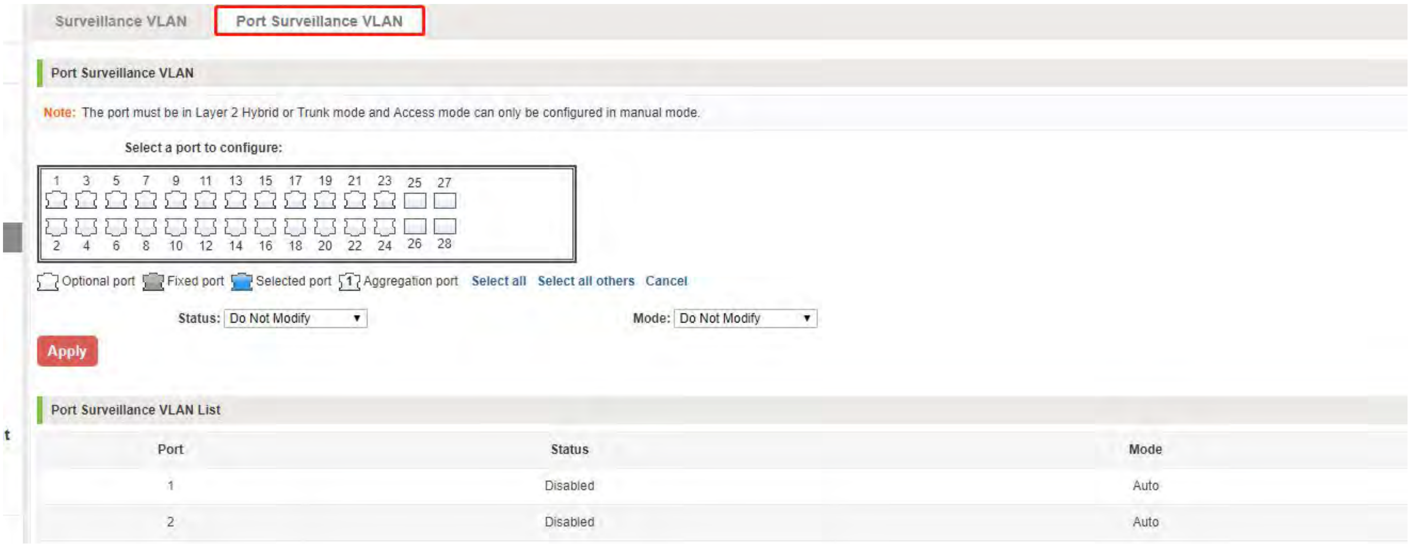
step 3: in the mac address text box,enter mac address ,such as 0402.0011.3120;

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:



Port Surveillance VLAN

Note: The port must be in Layer 2 Hybrid or Trunk mode and Access mode can only be configured in manual mode.

Select a port to configure:

Status: Do Not Modify

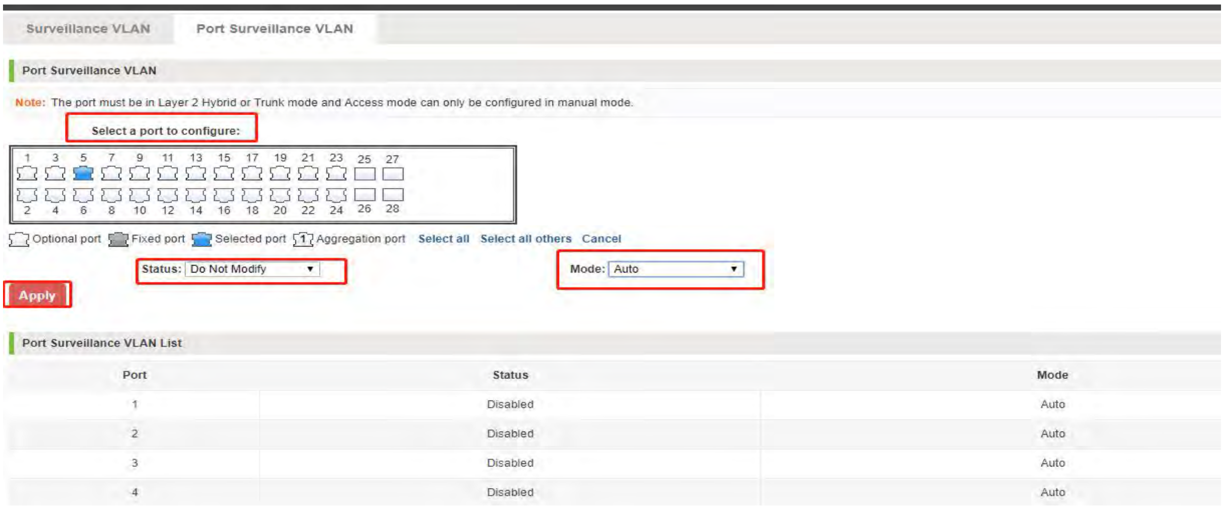
Mode: Do Not Modify

Port Surveillance VLAN List

Port	Status	Mode
1	Disabled	Auto
2	Disabled	Auto

Figure 4-20: view the port surveillance vlan information

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



Port Surveillance VLAN

Note: The port must be in Layer 2 Hybrid or Trunk mode and Access mode can only be configured in manual mode.

Select a port to configure:

Status: Do Not Modify

Mode: Auto

Port Surveillance VLAN List

Port	Status	Mode
1	Disabled	Auto
2	Disabled	Auto
3	Disabled	Auto
4	Disabled	Auto

Figure 4-21: configure the port surveillance vlan

5 FAULT / SAFETY

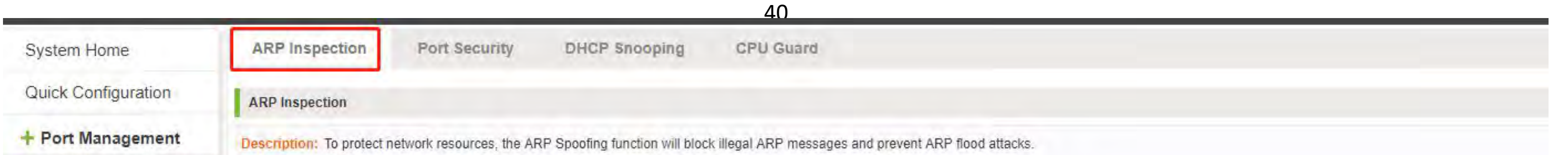
5.1 ATTACK PREVENTION

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:

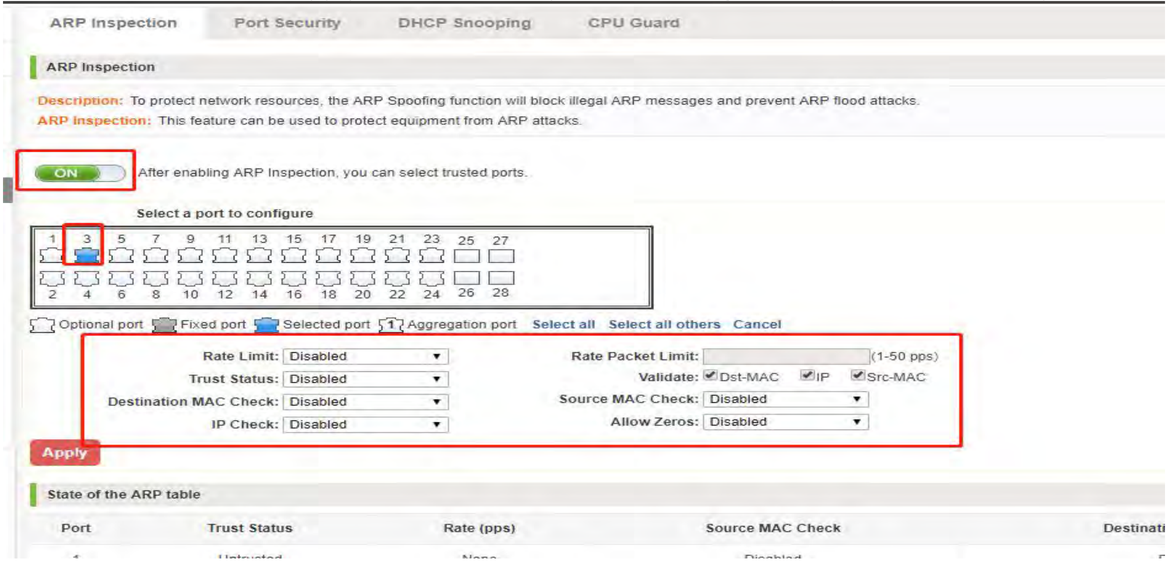
Figure 5-1: View port ARP configuration information



Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.

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 .



ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
ARP Inspection: This feature can be used to protect equipment from ARP attacks.

After enabling ARP Inspection, you can select trusted ports.

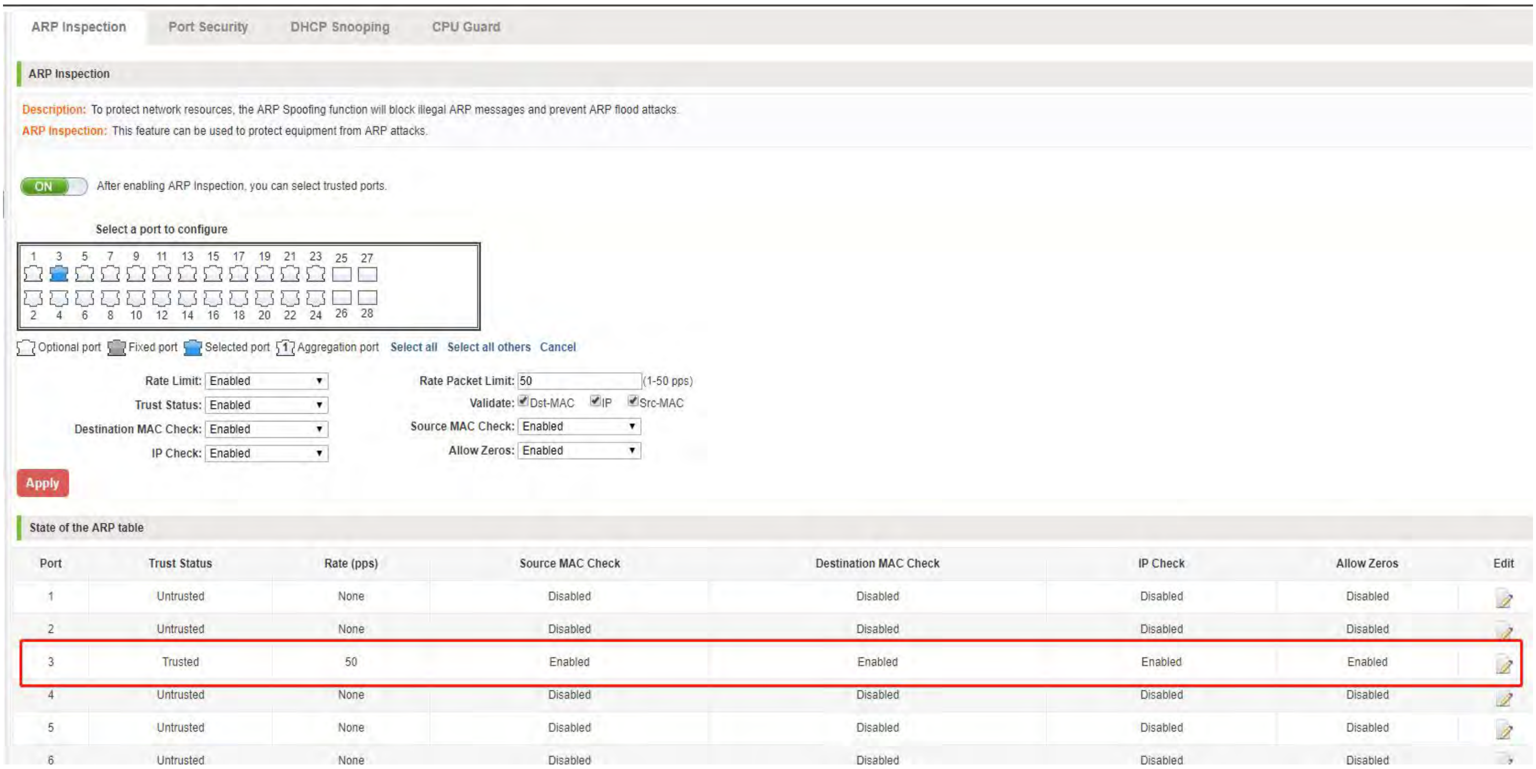
Select a port to configure

Rate Limit: Disabled
Trust Status: Disabled
Destination MAC Check: Disabled
IP Check: Disabled
Rate Packet Limit: (1-50 pps)
Validate: ☑Dst-MAC ☑IP ☑Src-MAC
Source MAC Check: Disabled
Allow Zeros: Disabled

State of the ARP table

Port	Trust Status	Rate (pps)	Source MAC Check	Destinati

Figure 5-2: ARP inspection configuration



ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
ARP Inspection: This feature can be used to protect equipment from ARP attacks.

After enabling ARP Inspection, you can select trusted ports.

Select a port to configure

Rate Limit: Enabled
Trust Status: Enabled
Destination MAC Check: Enabled
IP Check: Enabled
Rate Packet Limit: 50 (1-50 pps)
Validate: ☑Dst-MAC ☑IP ☑Src-MAC
Source MAC Check: Enabled
Allow Zeros: Enabled

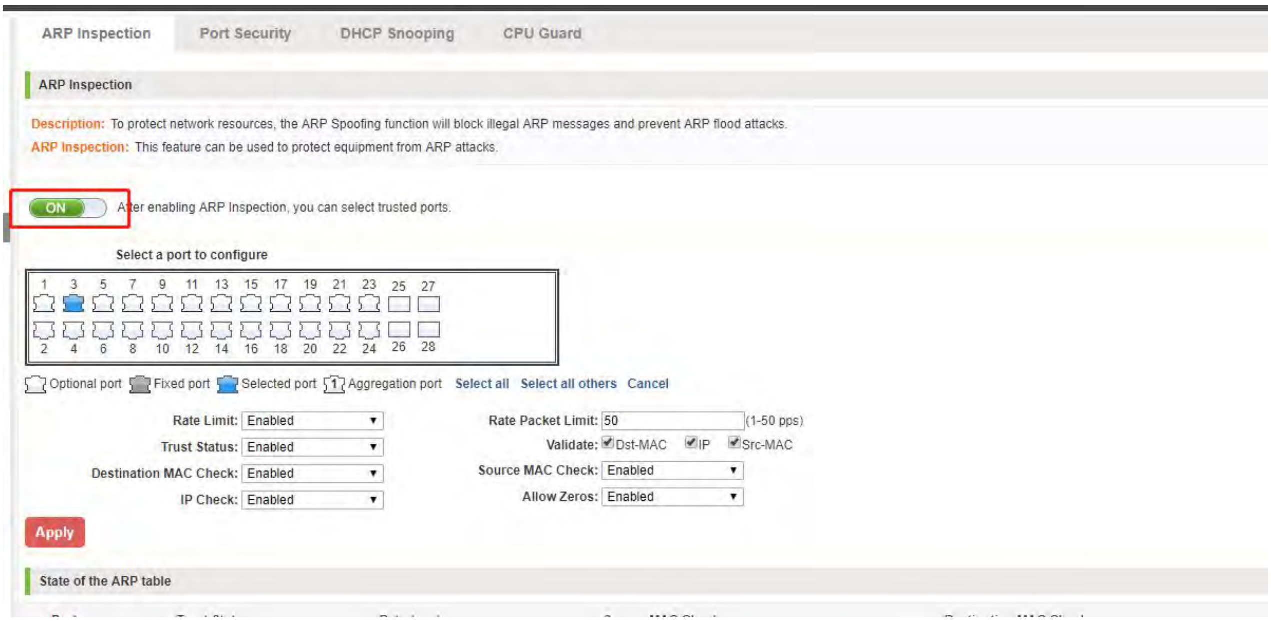
State of the ARP table

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

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.



ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.

ARP Inspection: This feature can be used to protect equipment from ARP attacks.

ON After enabling ARP Inspection, you can select trusted ports.

Select a port to configure

Optional port, Fixed port, Selected port, Aggregation port

Rate Limit: Enabled

Trust Status: Enabled

Destination MAC Check: Enabled

IP Check: Enabled

Rate Packet Limit: 50 (1-50 pps)

Validate: ☑Dst-MAC ☑IP ☑Src-MAC

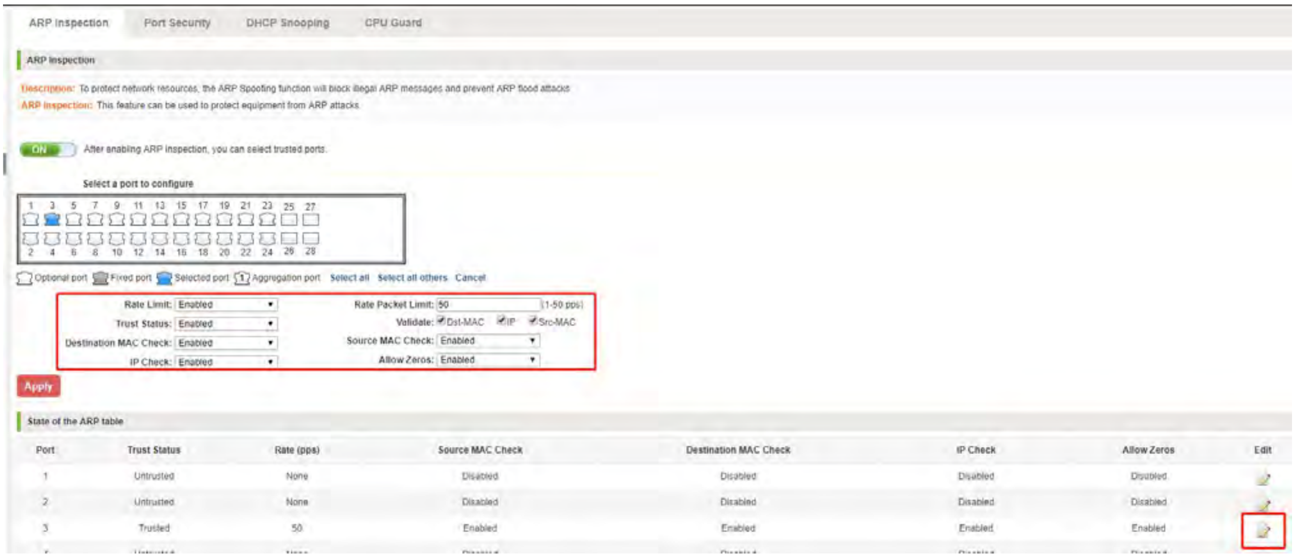
Source MAC Check: Enabled

Allow Zeros: Enabled

State of the ARP table

Figure 5-4: Disable ARP spoofing function

5.1.1.4TO MODIFY THE PORT ATTRIBUTE



ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.

ARP Inspection: This feature can be used to protect equipment from ARP attacks.

ON After enabling ARP Inspection, you can select trusted ports.

Select a port to configure

Optional port, Fixed port, Selected port, Aggregation port

Rate Limit: Enabled

Trust Status: Enabled

Destination MAC Check: Enabled

IP Check: Enabled

Rate Packet Limit: 50 (1-50 pps)

Validate: ☑Dst-MAC ☑IP ☑Src-MAC

Source MAC Check: Enabled

Allow Zeros: Enabled

State of the ARP table

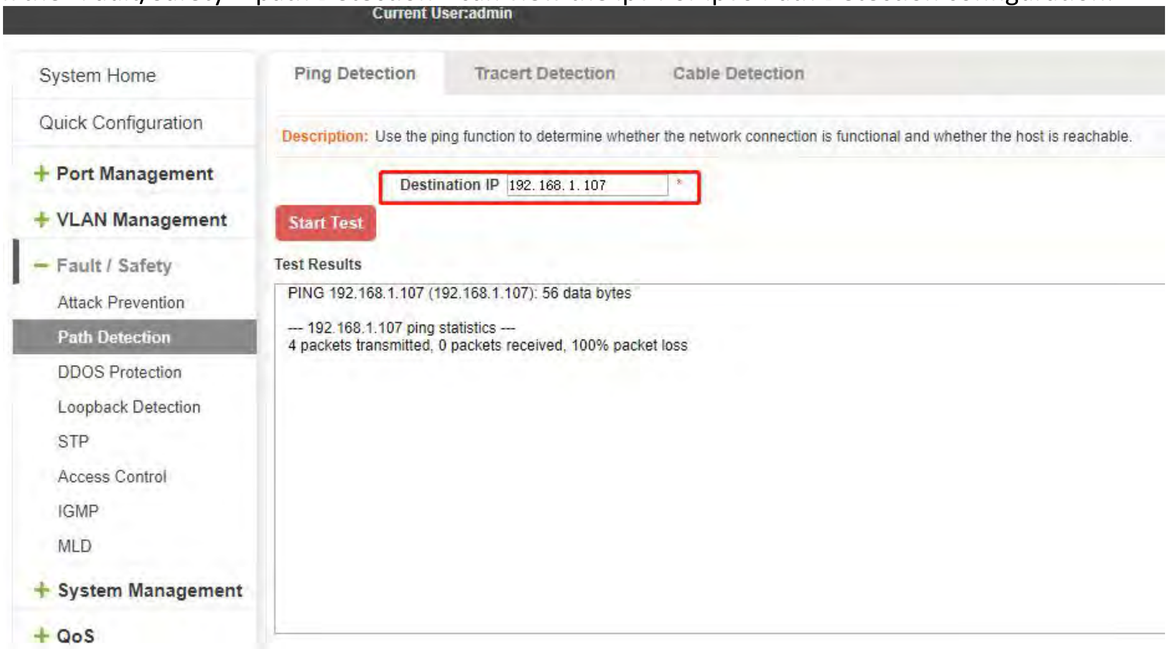
Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Trusted	50	Enabled	Enabled	Enabled	Enabled	

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:



Description: Use the ping function to determine whether the network connection is functional and whether the host is reachable.

Destination IP 192. 168. 1. 107 *

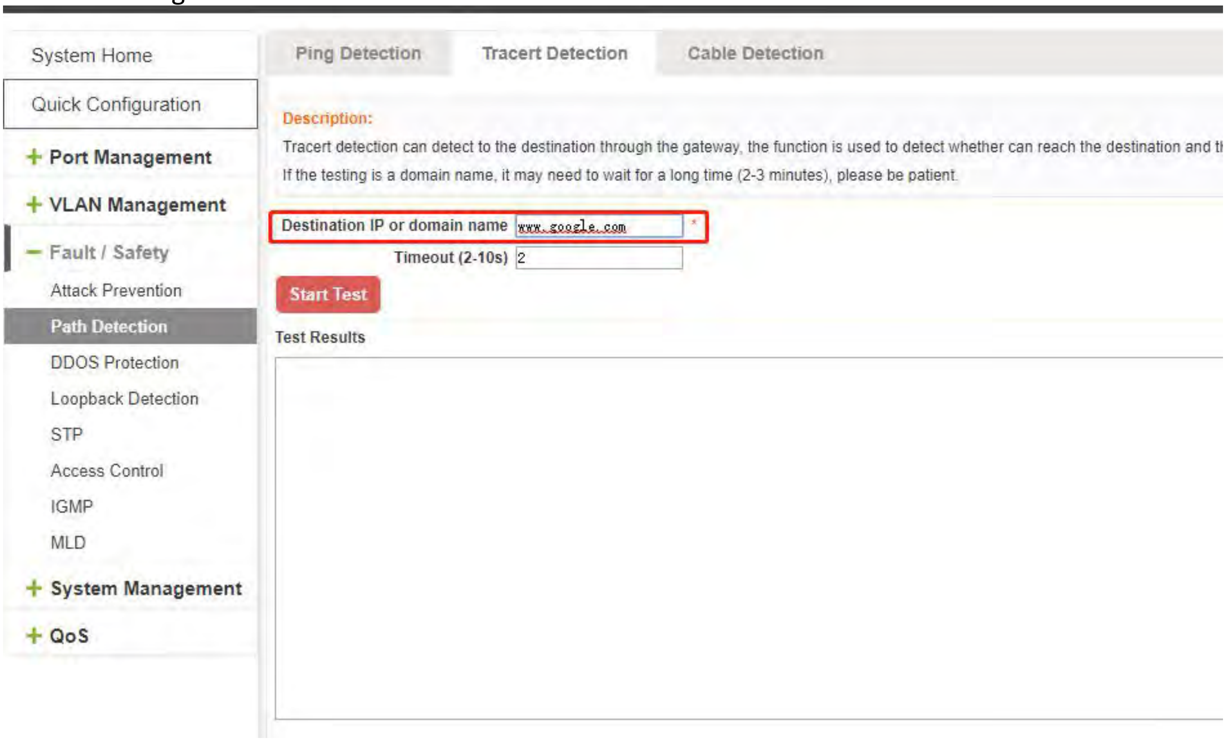
```
PING 192.168.1.107 (192.168.1.107): 56 data bytes

--- 192.168.1.107 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

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:



Description:

Tracert detection can detect to the destination through the gateway, the function is used to detect whether can reach the destination and tl

If the testing is a domain name, it may need to wait for a long time (2-3 minutes), please be patient.

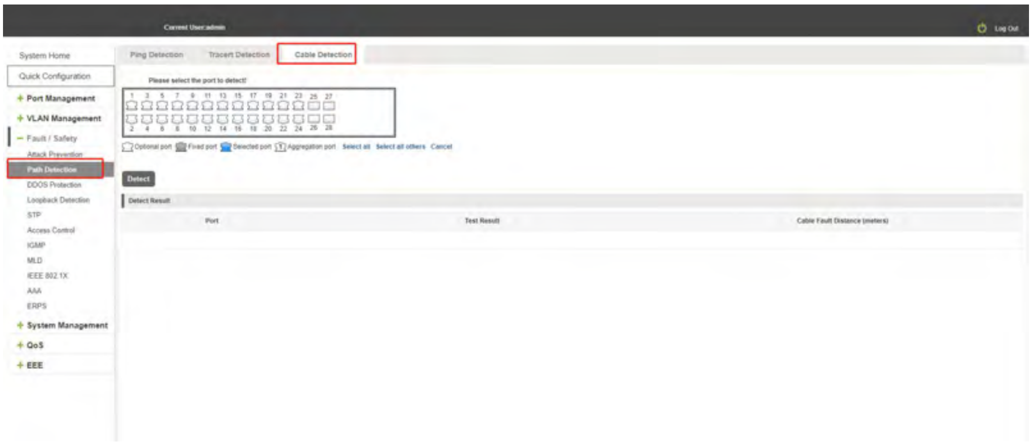
Destination IP or domain name www.google.com *

Timeout (2-10s) 2

Figure 5-13: Tracert detection information

5.2.3 CABLE DETECTION

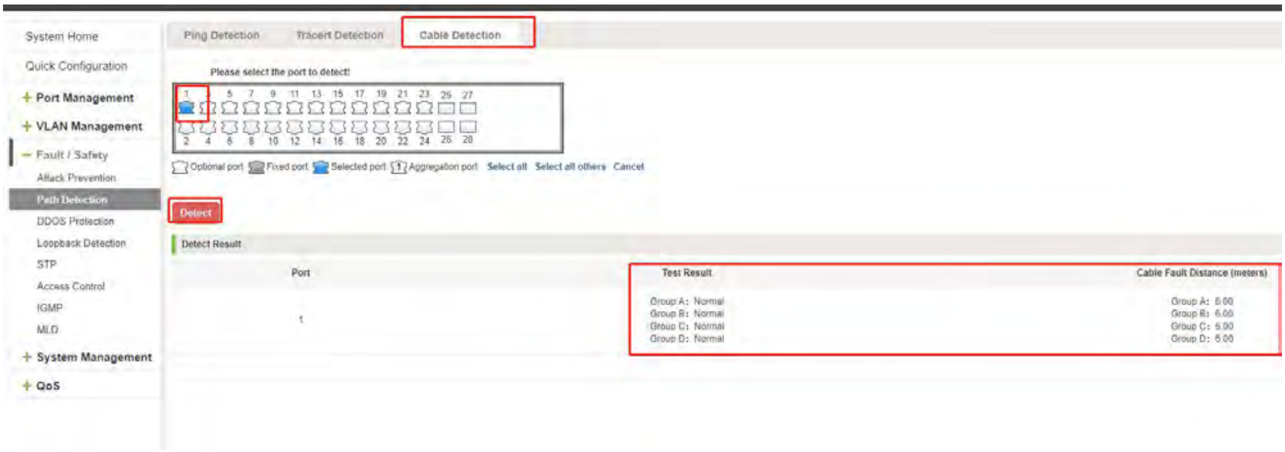
Click the "Fault/Safety" "path Detection" “Cable Detection” can view the Cable Detection configuration:



Port	Test Result	Cable Fault Distance (meters)

Figure 5-14: Cable detection information

The cable detection only selected one port:

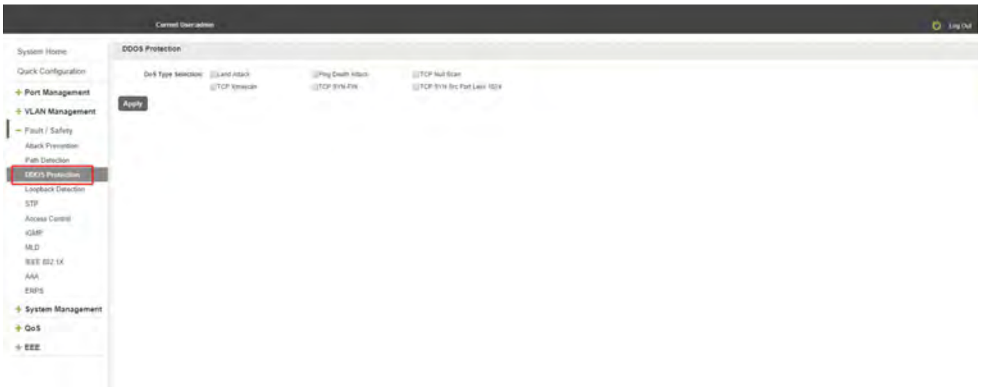


Port	Test Result	Cable Fault Distance (meters)
1	Group A: Normal Group B: Normal Group C: Normal Group D: Normal	Group A: 6.00 Group B: 6.00 Group C: 6.00 Group D: 6.00

Figure 5-15: Port cable detection result

5.3 DDOS PROTECTION

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

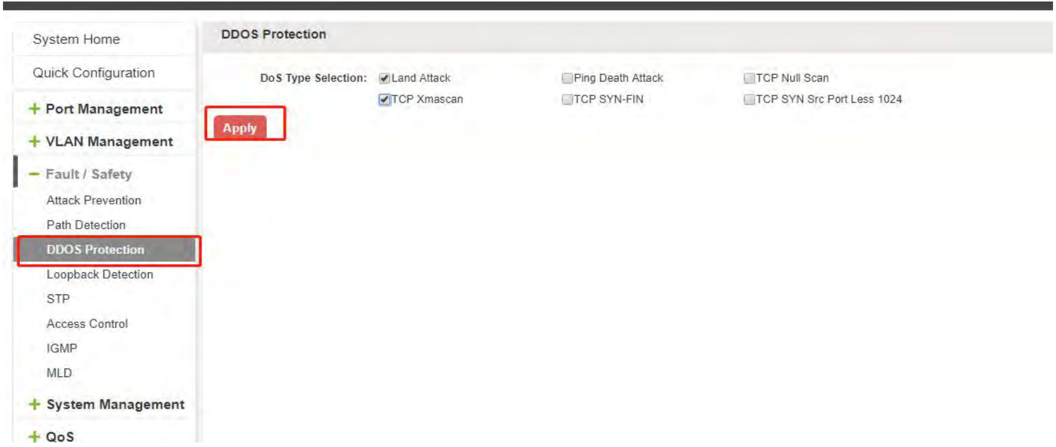


DDOS Protection

DoS Type Selection: □Land Attack □Ping Death Attack □TCP Null Scan
□TCP Xmascan □TCP SYN-FIN □TCP SYN Src Port Less 1024

Figure 5-16: DDOS Protection information

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



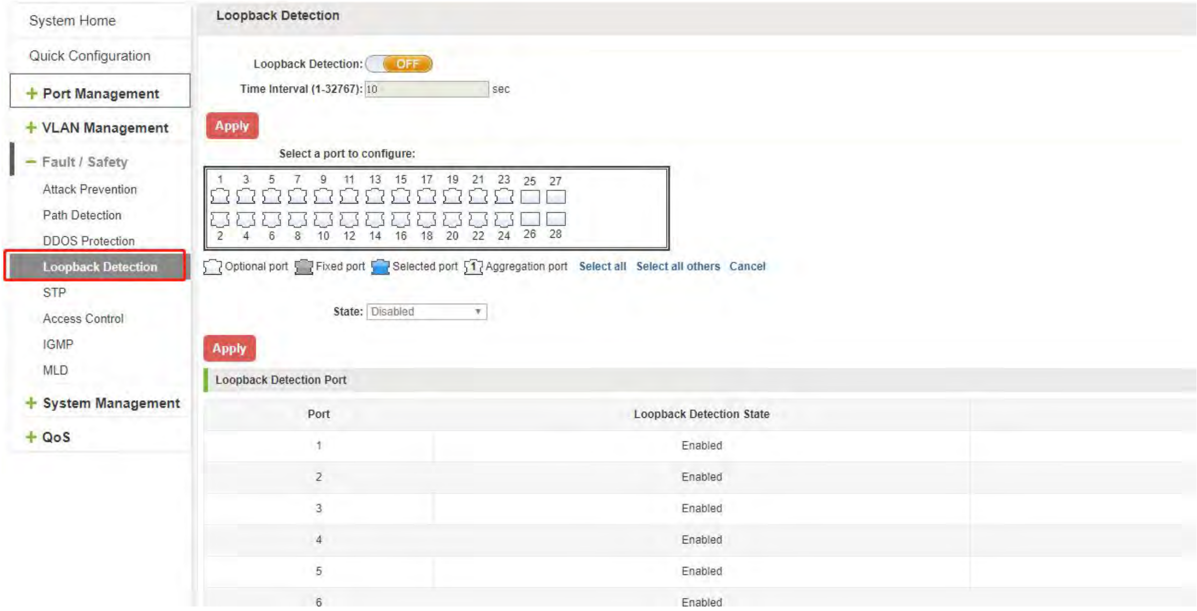
DDOS Protection

DoS Type Selection: ☑Land Attack □Ping Death Attack □TCP Null Scan
☑TCP Xmascan □TCP SYN-FIN □TCP SYN Src Port Less 1024

Figure 5-17: selected dos type

5.4 LOOPBACK DETECTION

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



Loopback Detection

Loopback Detection: OFF

Time Interval (1-32767): 10 sec

Select a port to configure:

State: Disabled

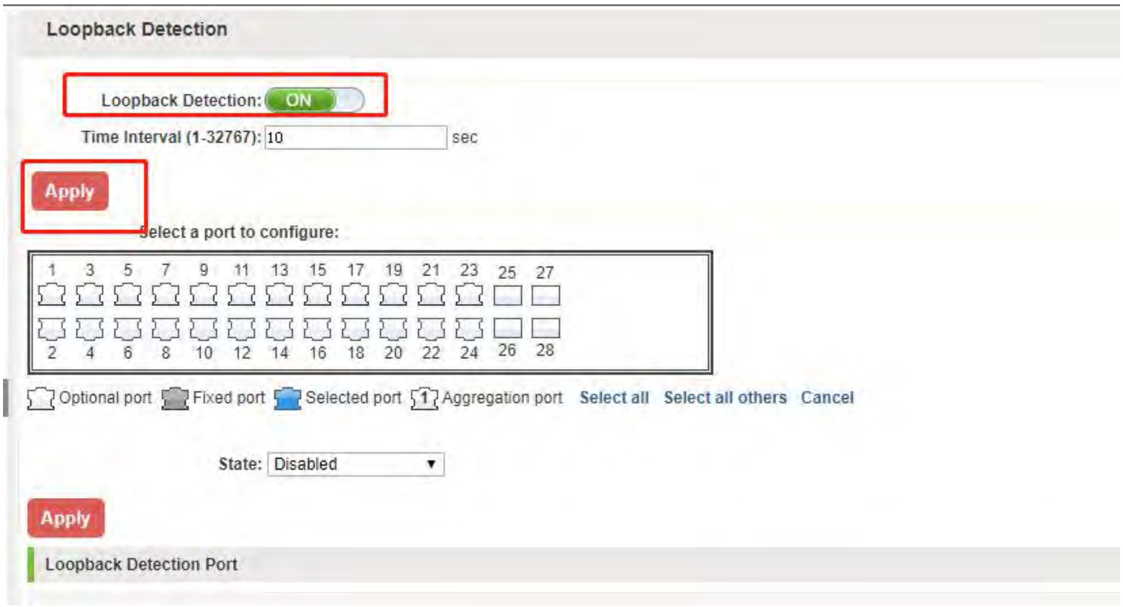
Loopback Detection Port

Port	Loopback Detection State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled

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:



Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

Select a port to configure:

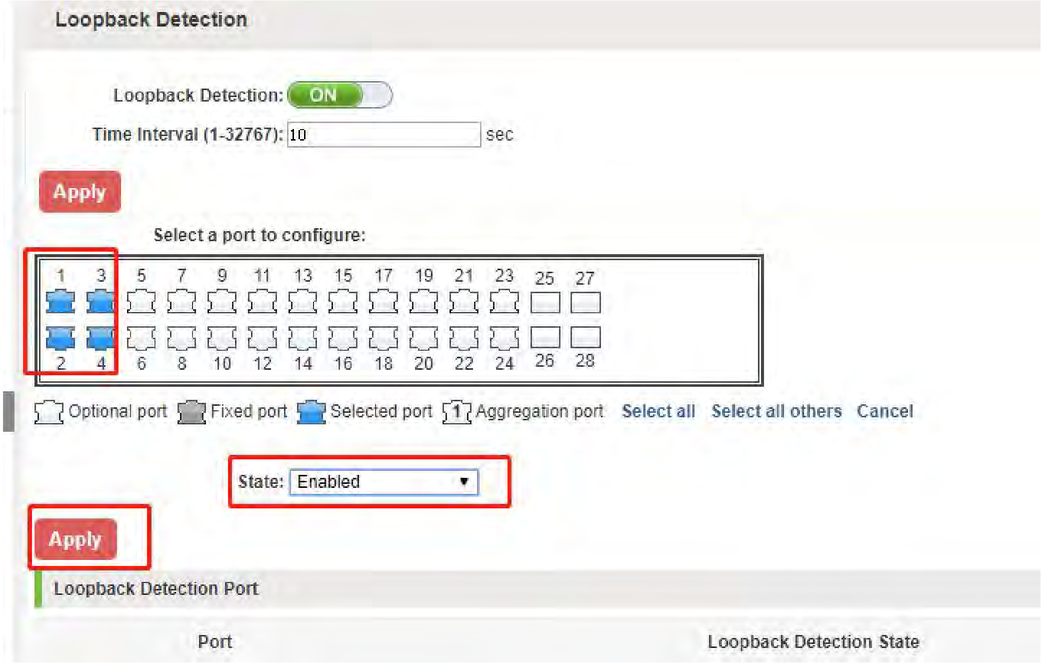
State: Disabled

Loopback Detection Port

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:


Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

Select a port to configure:

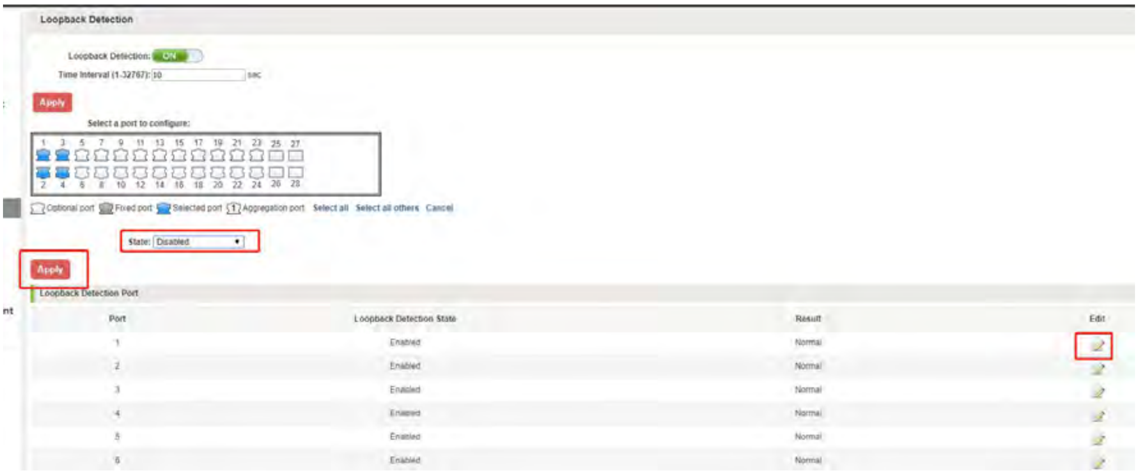
State: Enabled

Loopback Detection Port

Port	Loopback Detection State

Figure 5-20: configure ports parameter

Click “Edit”button,change the port status:


Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

Select a port to configure:

State: Disabled

Loopback Detection Port

Port	Loopback Detection State	Result	Edit
1	Enabled	Normal	
2	Enabled	Normal	
3	Enabled	Normal	
4	Enabled	Normal	
5	Enabled	Normal	
6	Enabled	Normal	

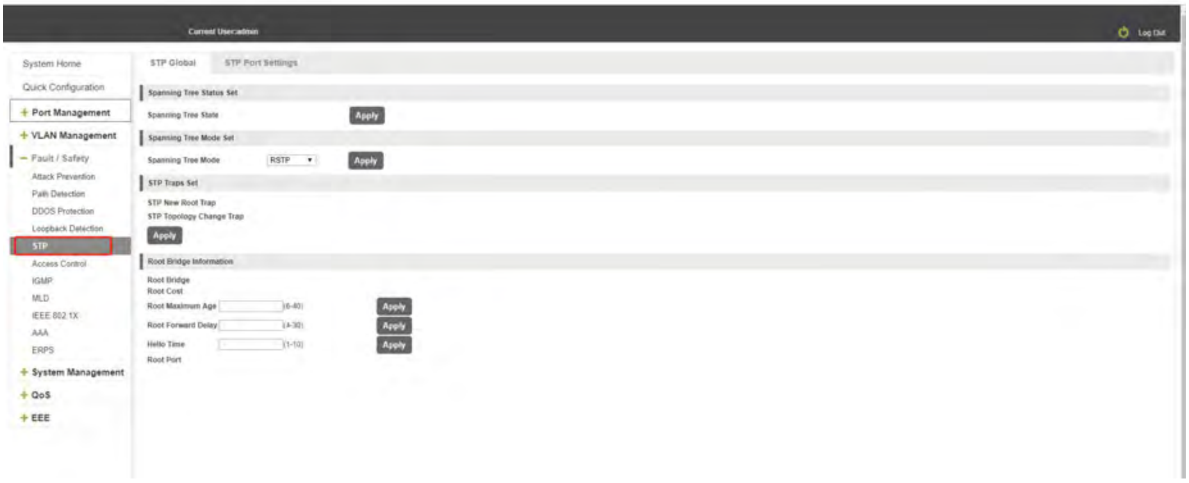
Figure 5-21: change the port configure

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:



Spanning Tree State

Spanning Tree Mode: RSTP

Root Maximum Age (6-40)

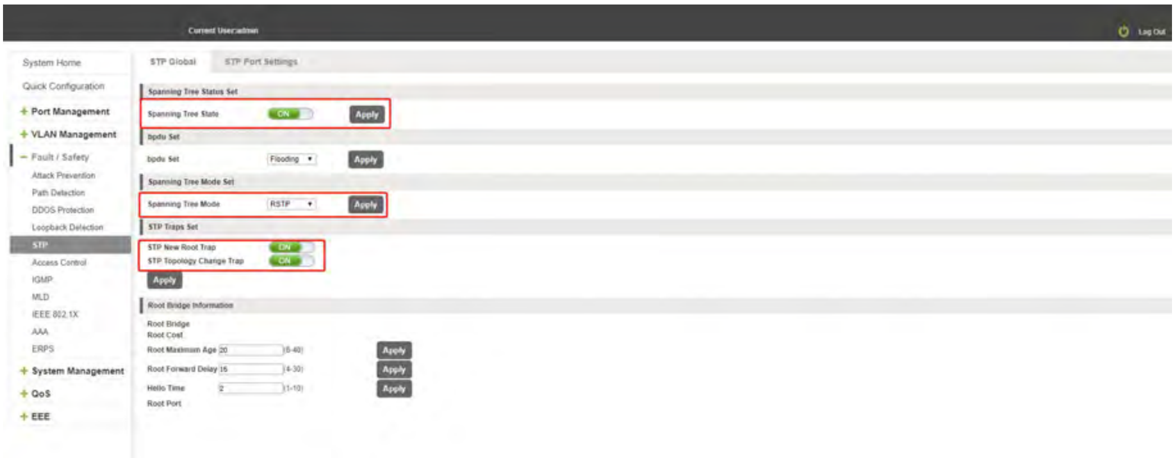
Root Forward Delay (4-30)

Hello Time (1-10)

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.



Spanning Tree State: ON

bpdu Set: Flooding

Spanning Tree Mode: RSTP

STP New Root Trap: ON

STP Topology Change Trap: ON

Root Maximum Age: 20 (6-40)

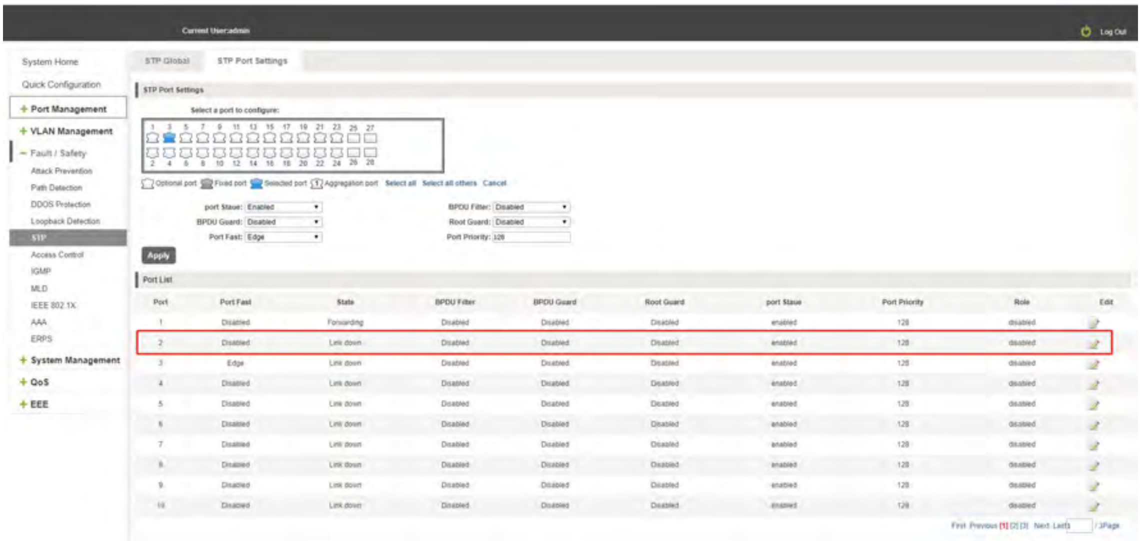
Root Forward Delay: 15 (4-30)

Hello Time: 2 (1-10)

Figure 5-23: Change STP global status

5.5.1.3STP PORT SETTINGS

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



STP Port Settings

port Staue: Enabled
BPDU Guard: Disabled
Port Fast: Edge
BPDU Filter: Disabled
Root Guard: Disabled
Port Priority: 128

Port List

Port	Port Fast	State	BPDU Filter	BPDU Guard	Root Guard	port Staue	Port Priority	Role	Edit
1	Disabled	Forwarding	Disabled	Disabled	Disabled	enabled	128	disabled	
2	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
3	Edge	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
4	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
5	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
6	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
7	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
8	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
9	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	
10	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	

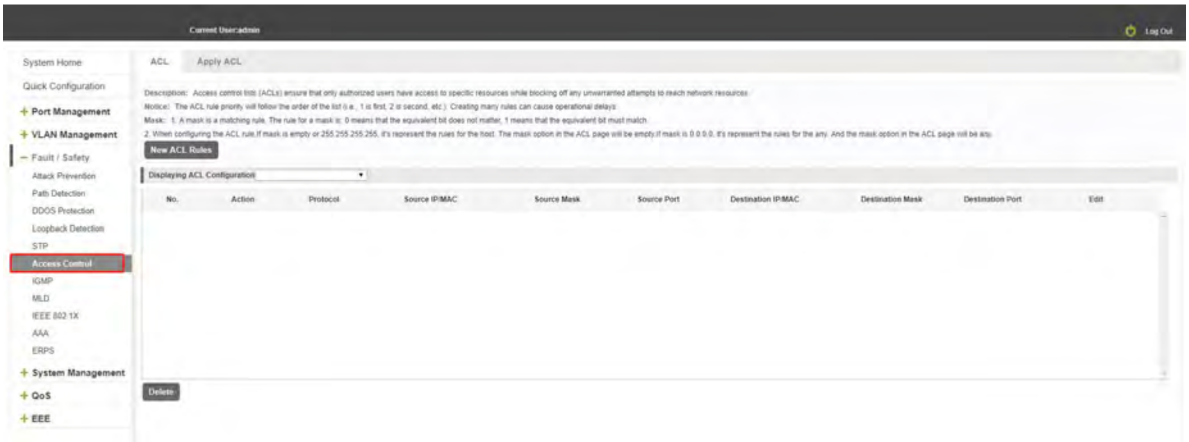
Figure 5-24: STP Port settings

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:



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.

Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter, 1 means that the equivalent bit must match.

2. When configuring the ACL rule,If mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.If mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

Displaying ACL Configuration

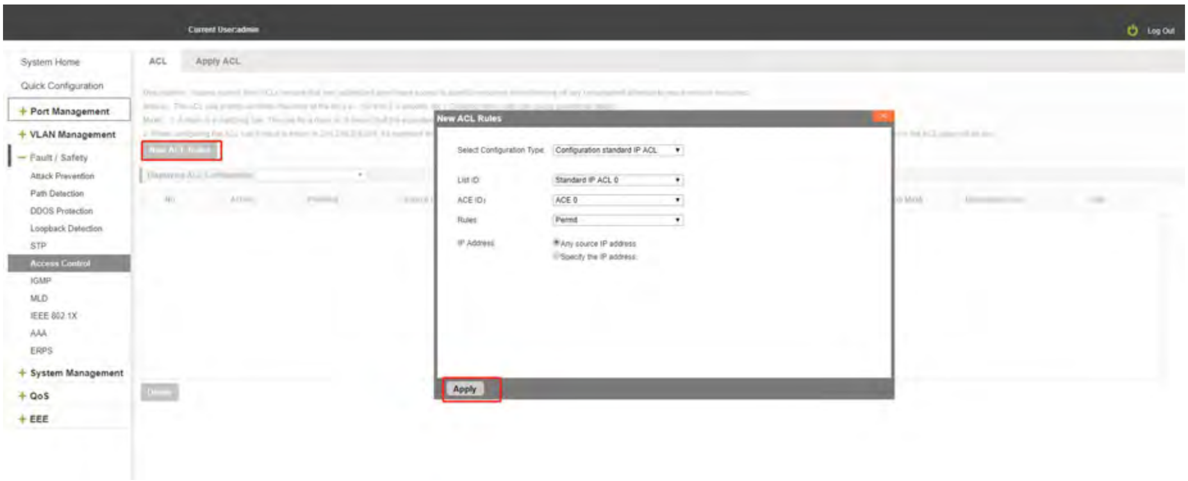
No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit

Figure 5-25: Access control list

5.6.1.2INCREASED 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:



New ACL Rules

Select Configuration Type: Configuration standard IP ACL

List ID: Standard IP ACL 0

ACE ID: ACE 0

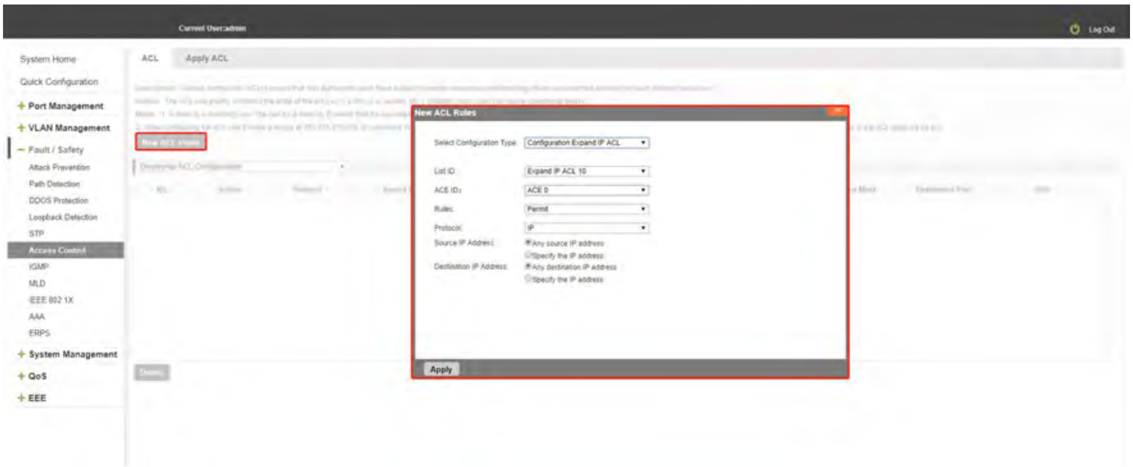
Rules: Permit

IP Address: ● Any source IP address ○ Specify the IP address

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:



New ACL Rules

Select Configuration Type: Configuration Expand IP ACL

List ID: Expand IP ACL 10

ACE ID: ACE 0

Rules: Permit

Protocol: IP

Source IP Address: ● Any source IP address ○ Specify the IP address

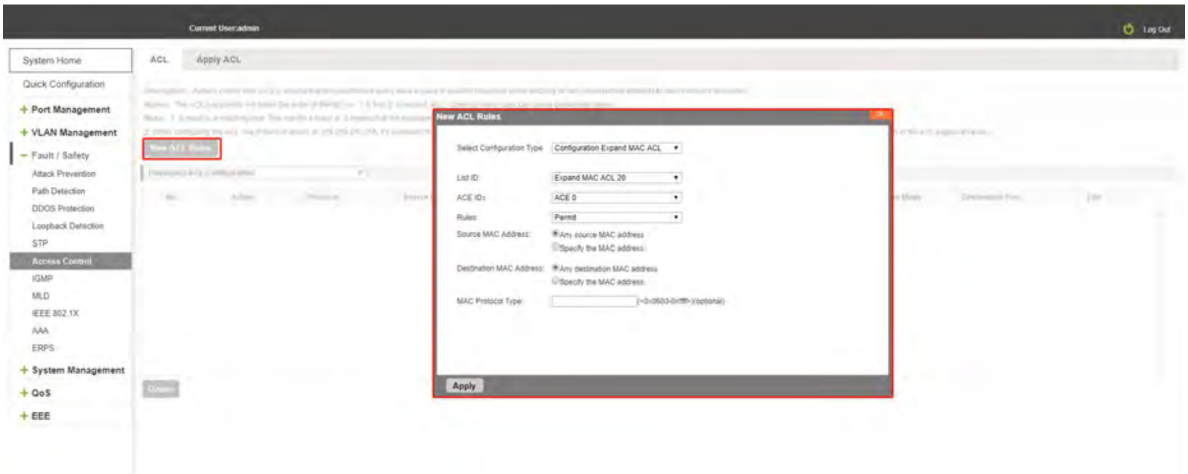
Destination IP Address: ● Any destination IP address ○ Specify the IP address

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 After the configuration is complete, click "Apply"：



Select Configuration Type: Configuration Expand MAC ACL

List ID: Expand MAC ACL 20

ACE IDs: ACE 0

Rules: Permit

Source MAC Address: ● Any source MAC address ○ Specify the MAC address

Destination MAC Address: ● Any destination MAC address ○ Specify the MAC address

MAC Protocol Type: (<0x0600-0xffff>)(optional)

Figure 5-28: Configuration extended MAC access control list

Configuration instructions:

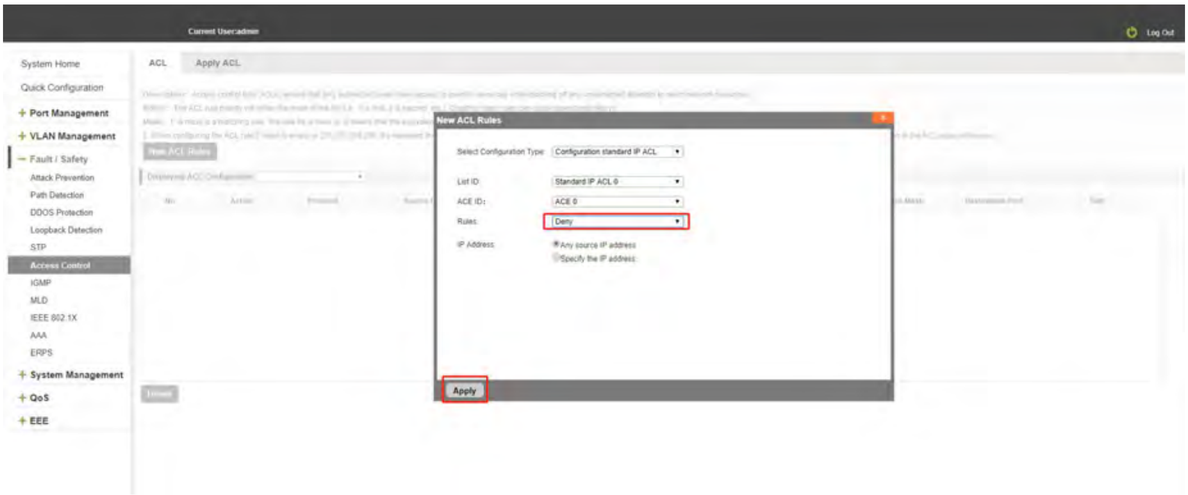
ACE ID is an optional rule. Do not fill: the default is 0;

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":



New ACL Rules

Select Configuration Type: Configuration standard IP ACL

List ID: Standard IP ACL 0

ACE ID: ACE 0

Rules: Deny

IP Address: ● Any source IP address ○ Specify the IP address

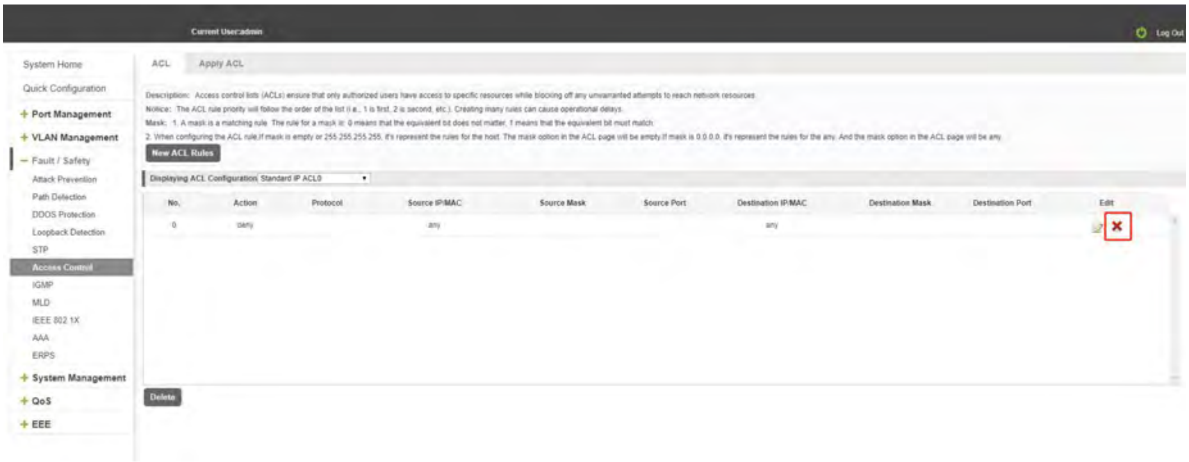
Figure 5-29: To modify the ACL rule

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:



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.

Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter, 1 means that the equivalent bit must match.

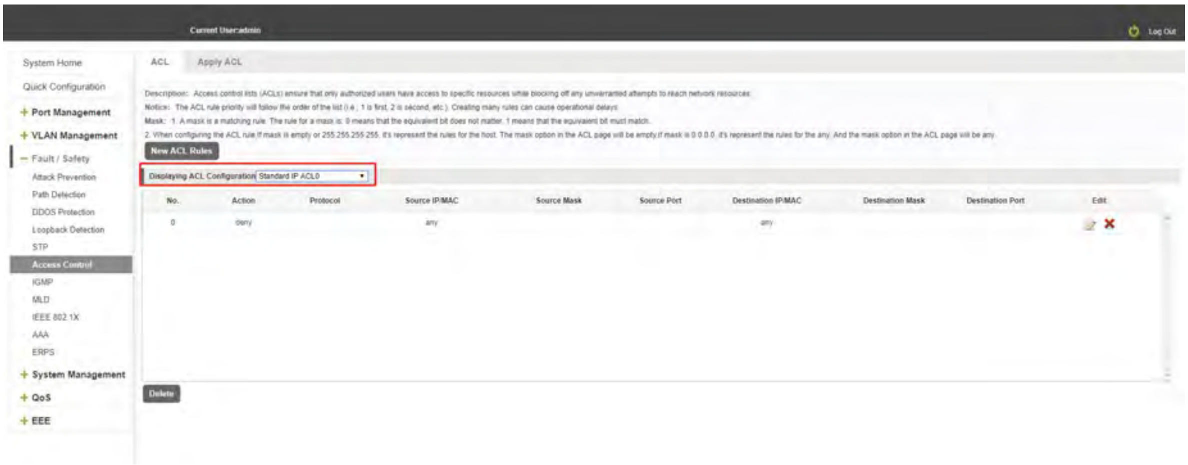
2. When configuring the ACL rule,If mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.If mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

Displaying ACL Configuration: Standard IP ACL0

No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit
0	deny		any			any			✕

Figure 5-30: Delete rules

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



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.
Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.
Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter. 1 means that the equivalent bit must match.
2. When configuring the ACL rule if mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.if mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

Displaying ACL Configuration: Standard IP ACL0

No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit
0	deny		any			any			✗

Figure 5-31: Delete ACL rules

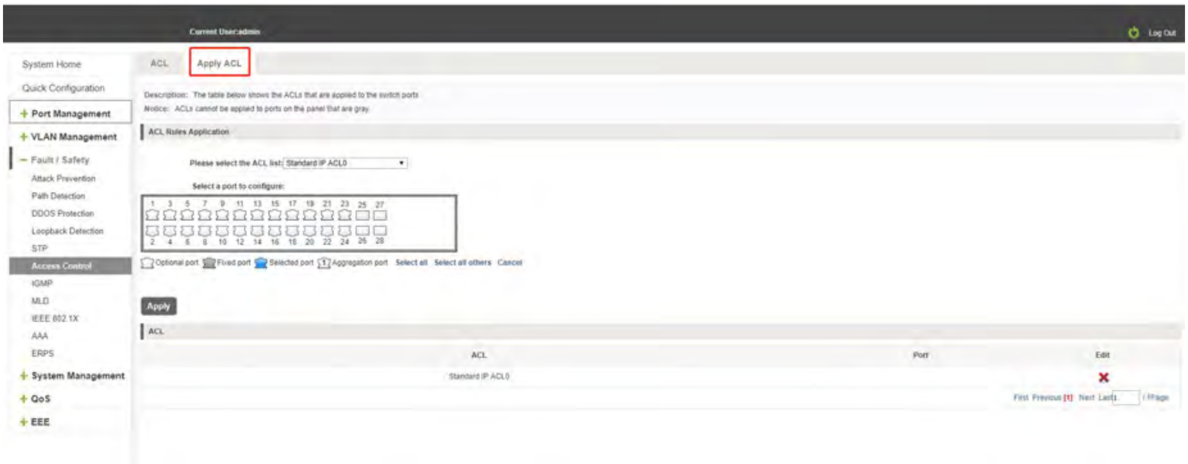
Configuration instructions:

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:



Description: The table below shows the ACLs that are applied to the switch ports
Notice: ACLs cannot be applied to ports on the panel that are gray

ACL Rules Application

Please select the ACL list: Standard IP ACL0

Select a port to configure:

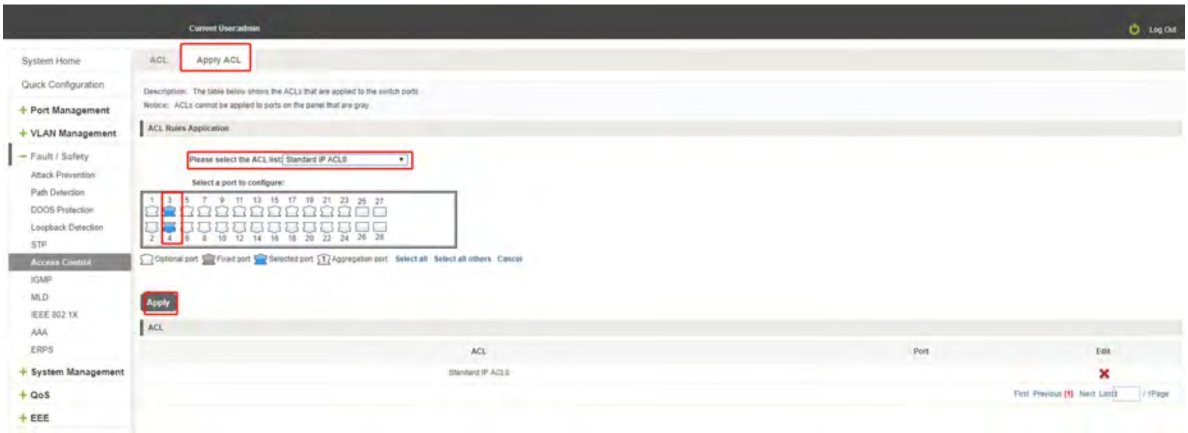
ACL

ACL	Port	Edit
Standard IP ACL0		✗

Figure 5-32: View application ACL rules

5.6.2.2INCREASED APPLICATION ACL

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



Description: The table below shows the ACLs that are applied to the switch ports

Notice: ACLs cannot be applied to ports on the panel that are gray

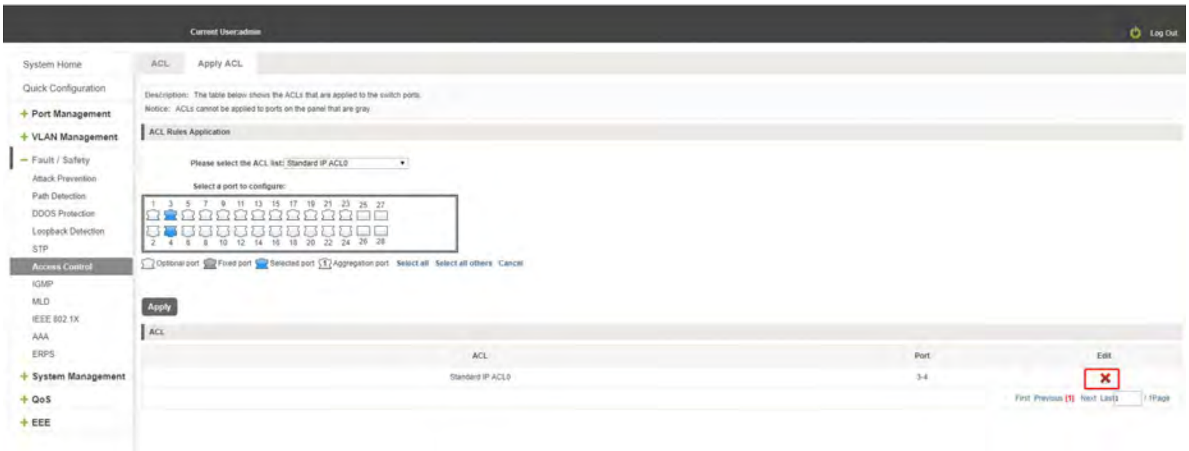
Please select the ACL list: Standard IP ACL0

ACL	Port	Edit
Standard IP ACL0		✕

Figure 5-33: Add applications ACL

5.6.2.3DELETE APPLICATION ACL

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



Description: The table below shows the ACLs that are applied to the switch ports

Notice: ACLs cannot be applied to ports on the panel that are gray

Please select the ACL list: Standard IP ACL0

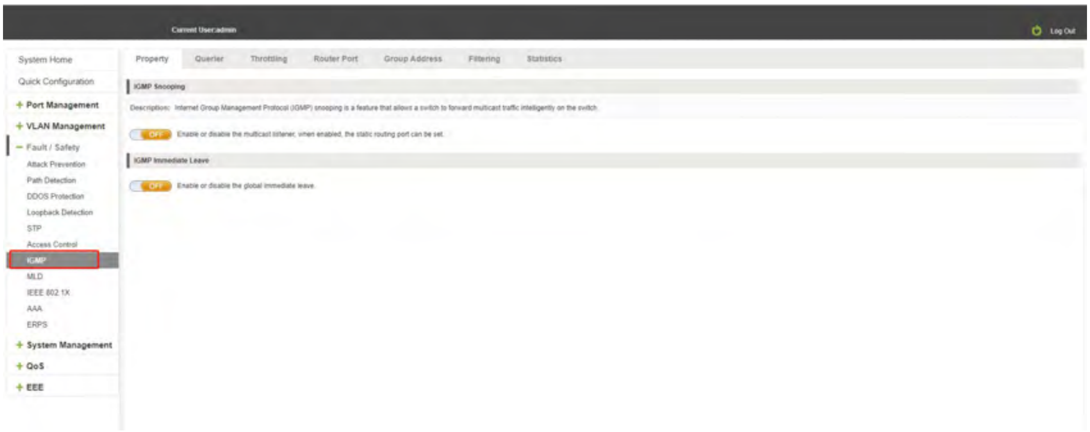
ACL	Port	Edit
Standard IP ACL0	3-4	✕

Figure 5-34: Delete 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:



Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

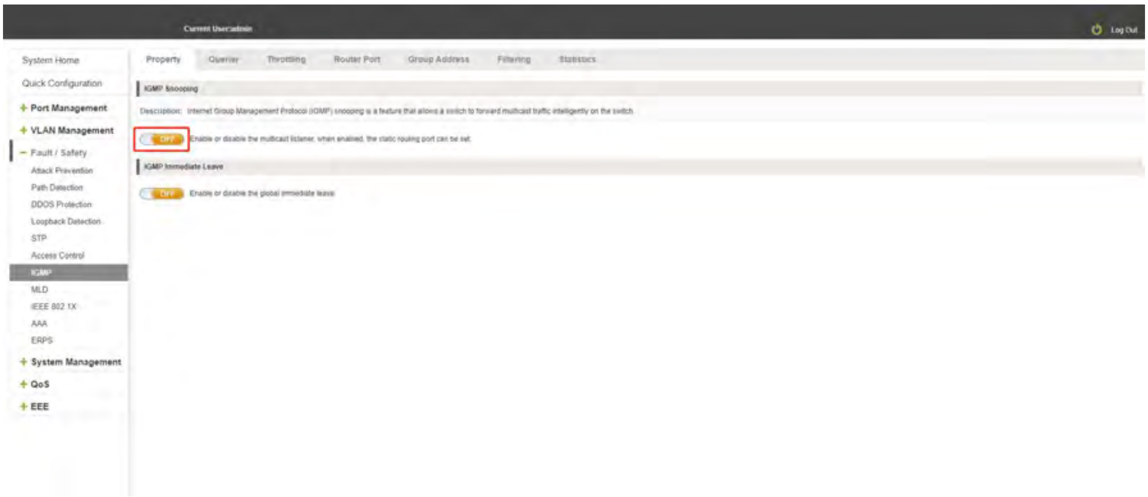
OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

OFF Enable or disable the global immediate leave.

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 :



Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

OFF Enable or disable the global immediate leave.

Figure 5-36: Open multicast listener configuration

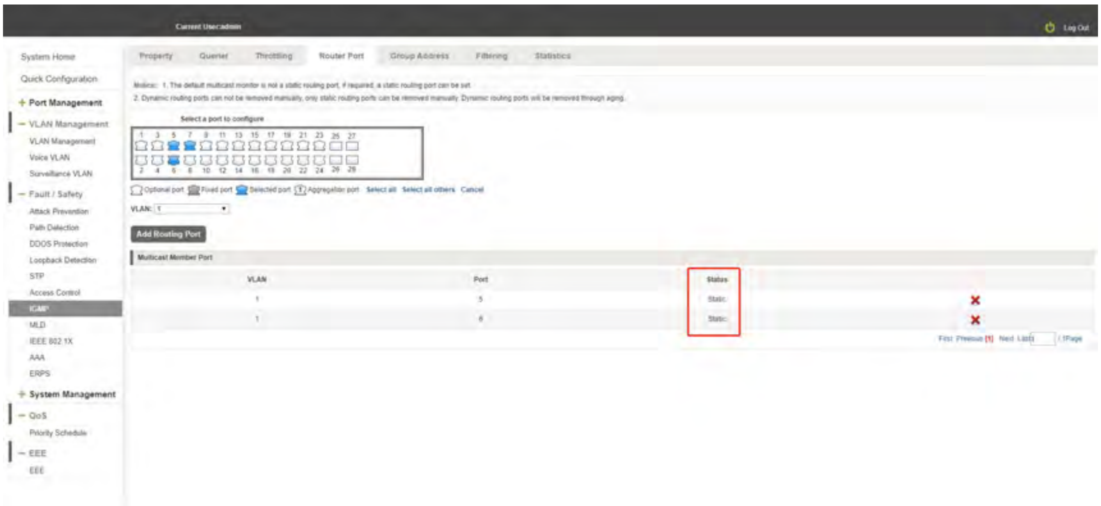
The default multicast listener (IGMP Snooping) did not open;

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.



Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

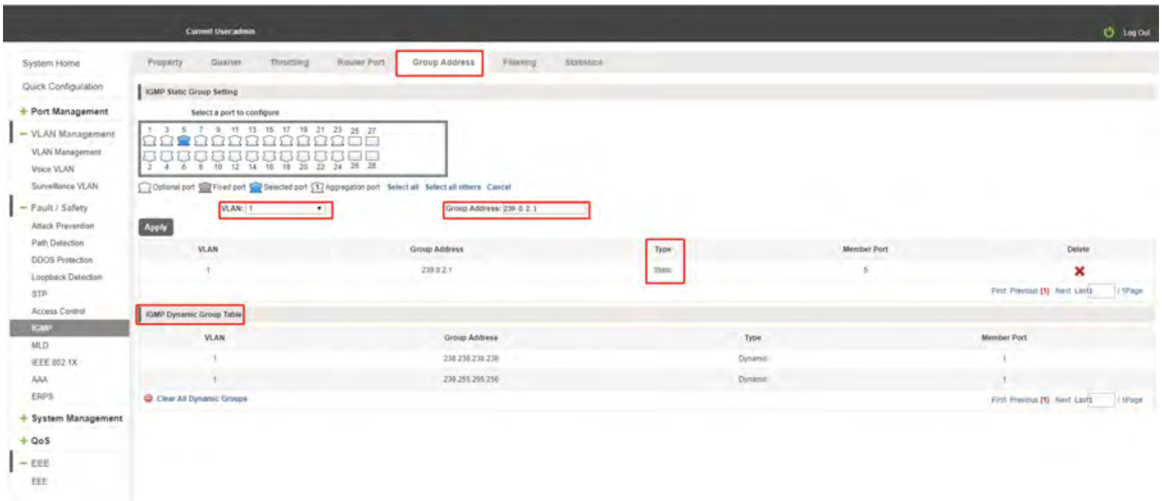
VLAN: 1

VLAN	Port	Status	
1	5	Static	✖
1	6	Static	✖

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:



VLAN: 1

Group Address: 239.0.2.1

VLAN	Group Address	Type	Member Port	Delete
1	239.0.2.1	Static	5	✖

IGMP Dynamic Group Table

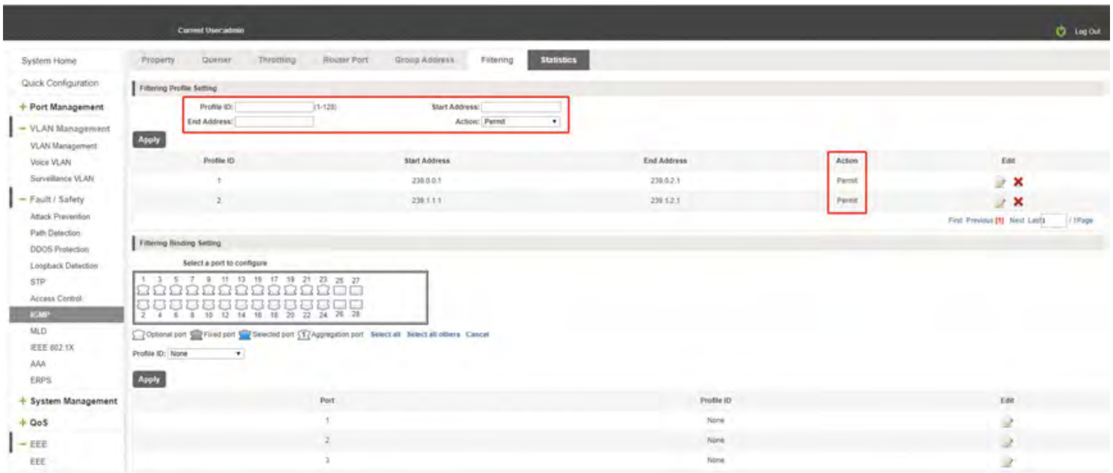
VLAN	Group Address	Type	Member Port
1	238.238.238.238	Dynamic	1
1	239.255.255.250	Dynamic	1

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:



Filtering Profile Setting

Profile ID: (1-128)   Start Address:
End Address: Action: Permit

Profile ID	Start Address	End Address	Action	Edit
1	239.0.0.1	239.0.2.1	Permit	
2	239.1.1.1	239.1.2.1	Permit	

Filtering Binding Setting

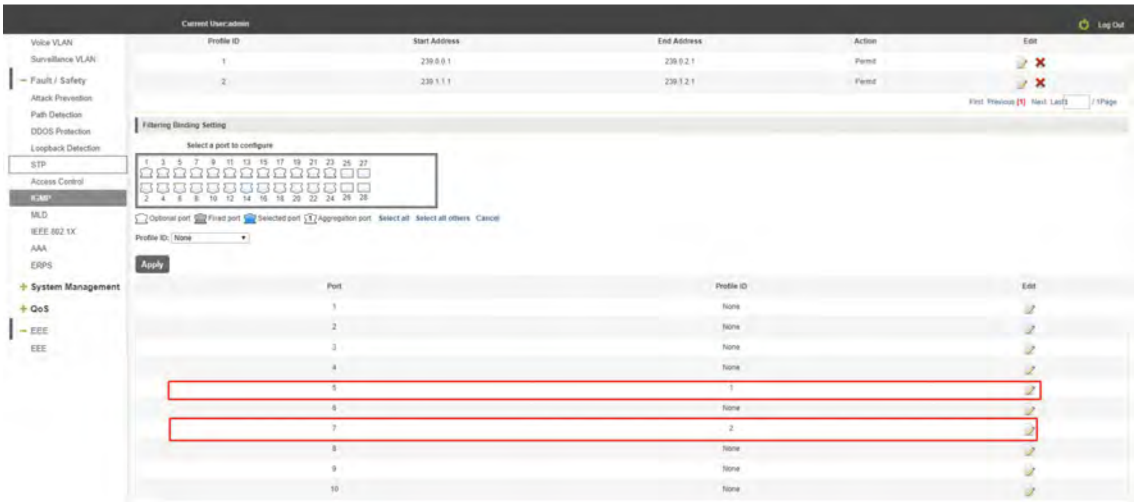
Select a port to configure

Profile ID: None

Port	Profile ID	Edit
1	None	
2	None	
3	None	

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:



Profile ID	Start Address	End Address	Action	Edit
1	239.0.0.1	239.0.2.1	Permit	
2	239.1.1.1	239.1.2.1	Permit	

Filtering Binding Setting

Select a port to configure

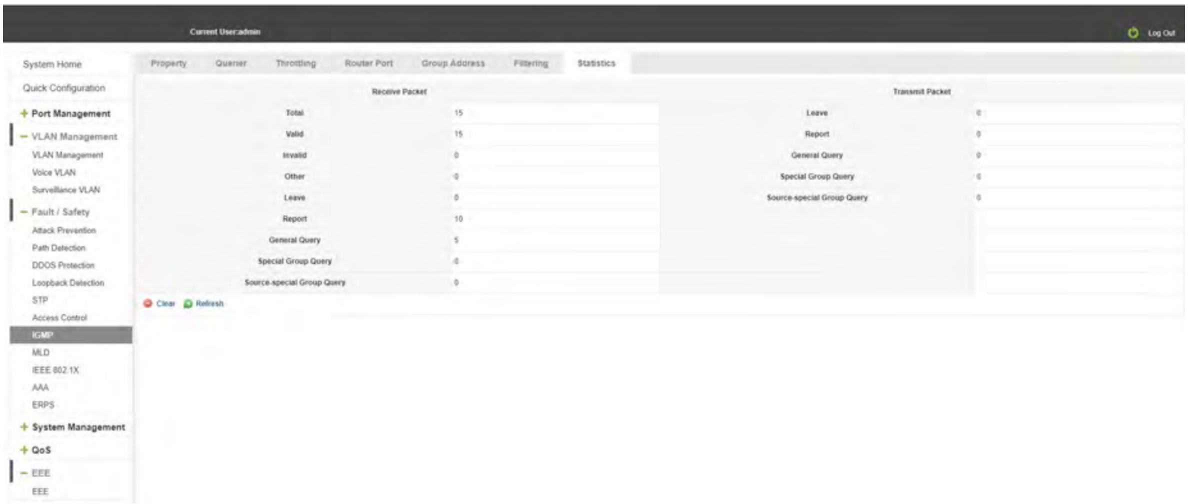
Profile ID: None

Port	Profile ID	Edit
1	None	
2	None	
3	None	
4	None	
5	1	
6	None	
7	2	
8	None	
9	None	
10	None	

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:

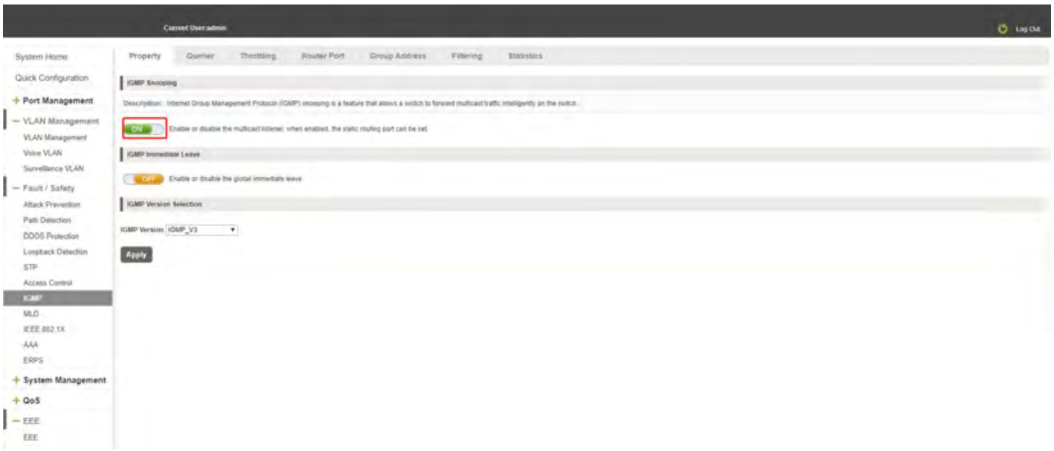


Receive Packet		Transmit Packet	
Total	15	Leave	0
Valid	15	Report	0
Invalid	0	General Query	0
Other	0	Special Group Query	0
Leave	0	Source-special Group Query	0
Report	10		
General Query	5		
Special Group Query	0		
Source-special Group Query	0		

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:



IGMP Snooping

Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

ON Enable or disable the multicast listener, when enabled, the static routing port can be set

IGMP Immediate Leave

OFF Enable or disable the global immediate leave

IGMP Version Selection

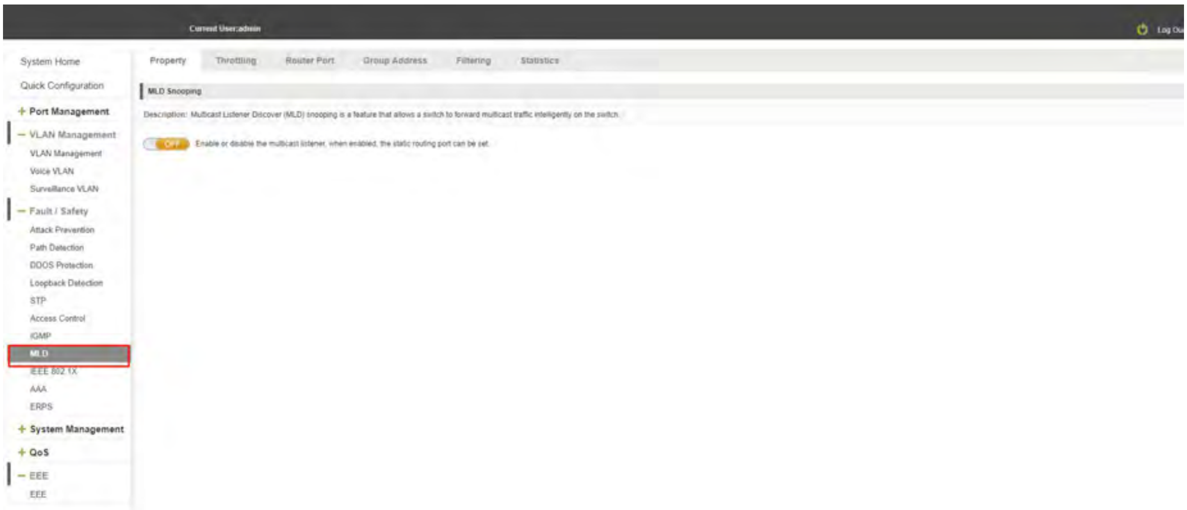
IGMP Version: IGMP_V3

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:



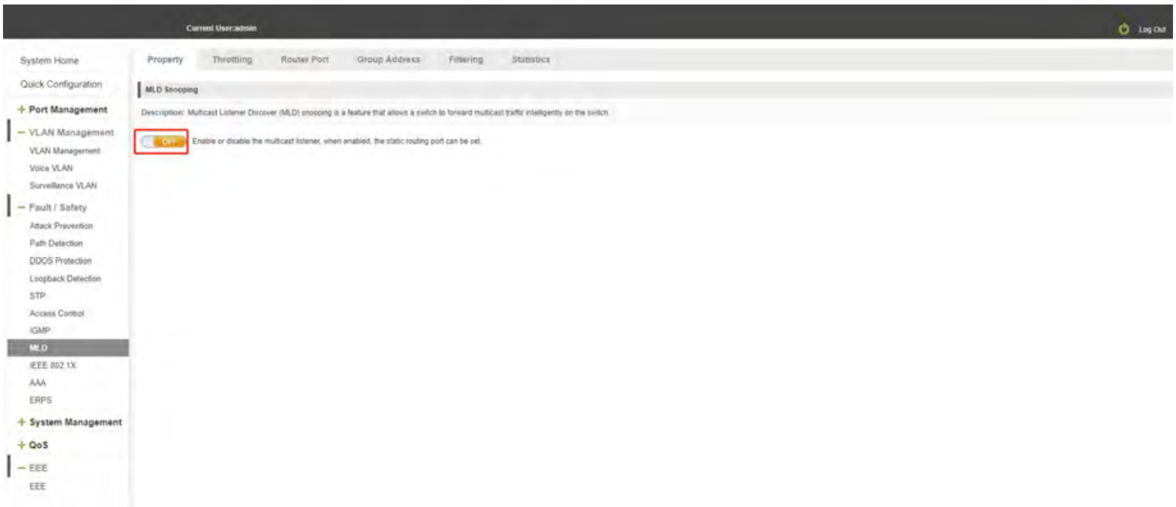
Description: Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

Enable or disable the multicast listener, when enabled, the static routing port can be set.

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:



Description: Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

Enable or disable the multicast listener, when enabled, the static routing port can be set.

Figure 5-44: Open multicast listener configuration

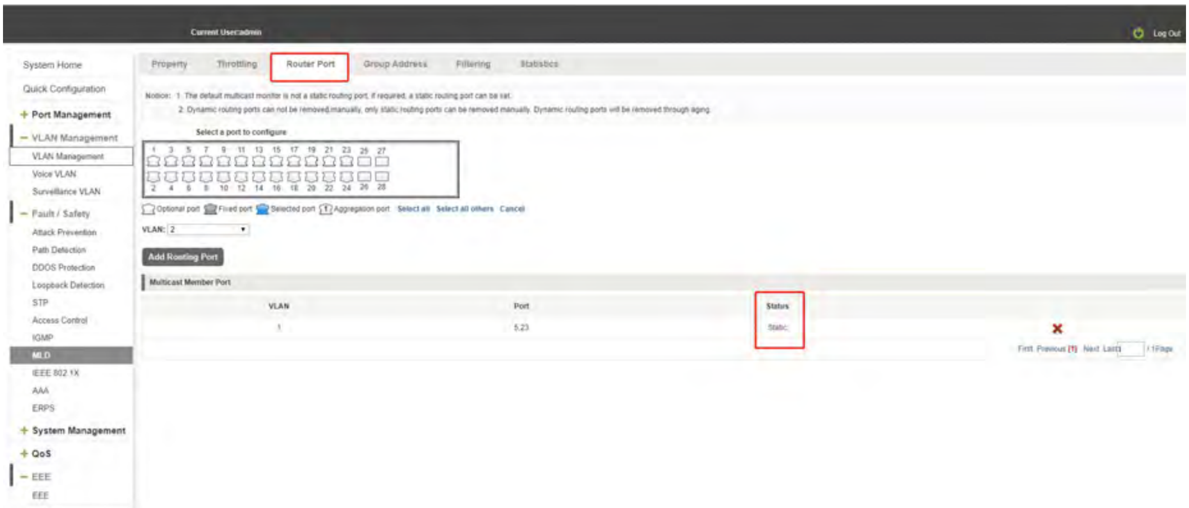
The default multicast listener (MLD) did not open;

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.



Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

VLAN: 2

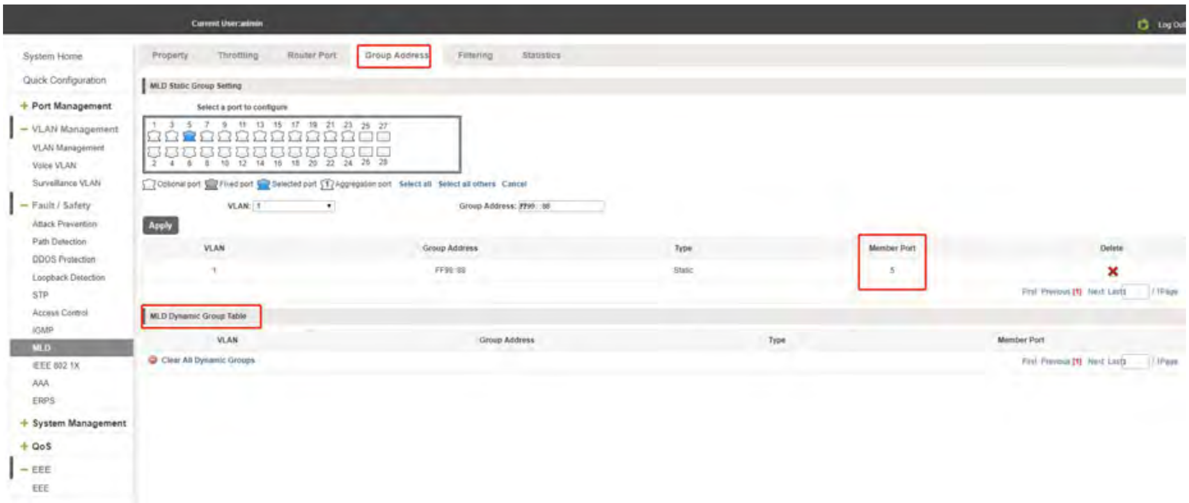
Multicast Member Port

VLAN	Port	Status	
1	5,23	Static	✗

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:



MLD Static Group Setting

VLAN: 1   Group Address: FF99::88

VLAN	Group Address	Type	Member Port	Delete
1	FF99::88	Static	5	✗

MLD Dynamic Group Table

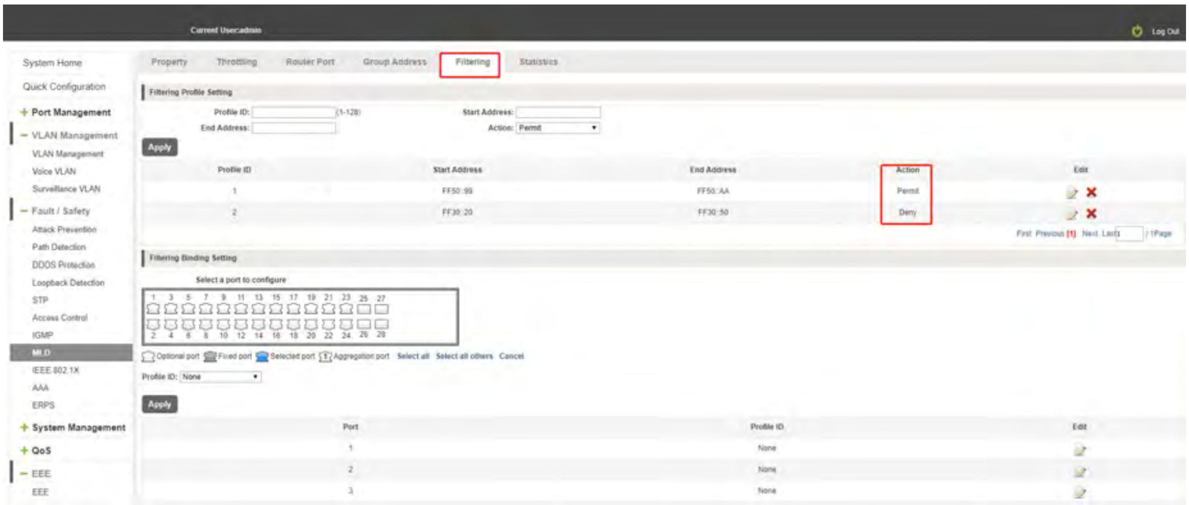
VLAN	Group Address	Type	Member Port

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



Filtering Profile Setting

Profile ID: (1-128) Start Address:
End Address: Action: Permit

Profile ID	Start Address	End Address	Action	Edit
1	FF50::99	FF50::AA	Permit	
2	FF30::20	FF30::50	Deny	

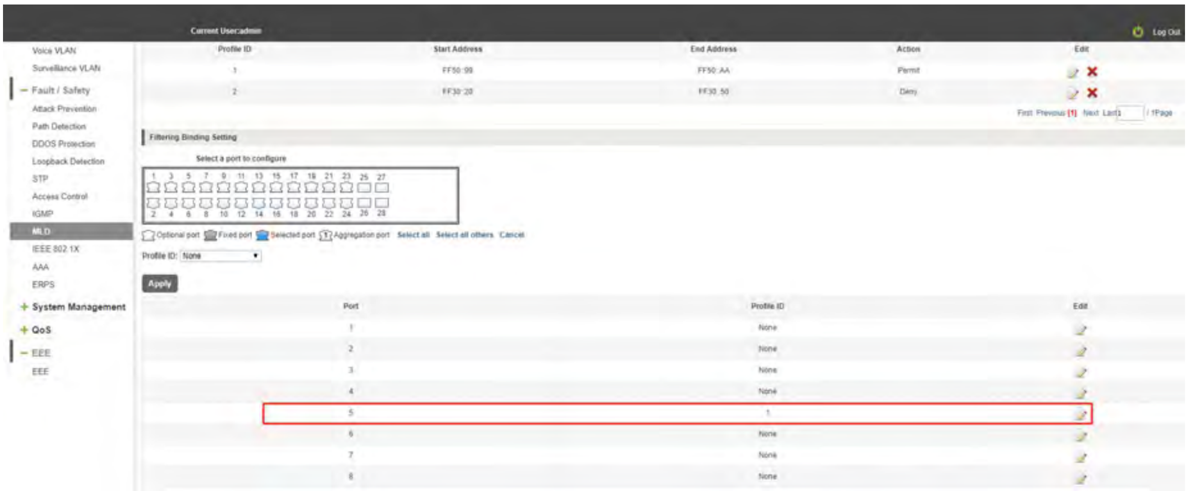
Filtering Binding Setting

Profile ID: None

Port	Profile ID	Edit
1	None	
2	None	
3	None	

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:



Profile ID	Start Address	End Address	Action	Edit
1	FF50::99	FF50::AA	Permit	
2	FF30::20	FF30::50	Deny	

Filtering Binding Setting

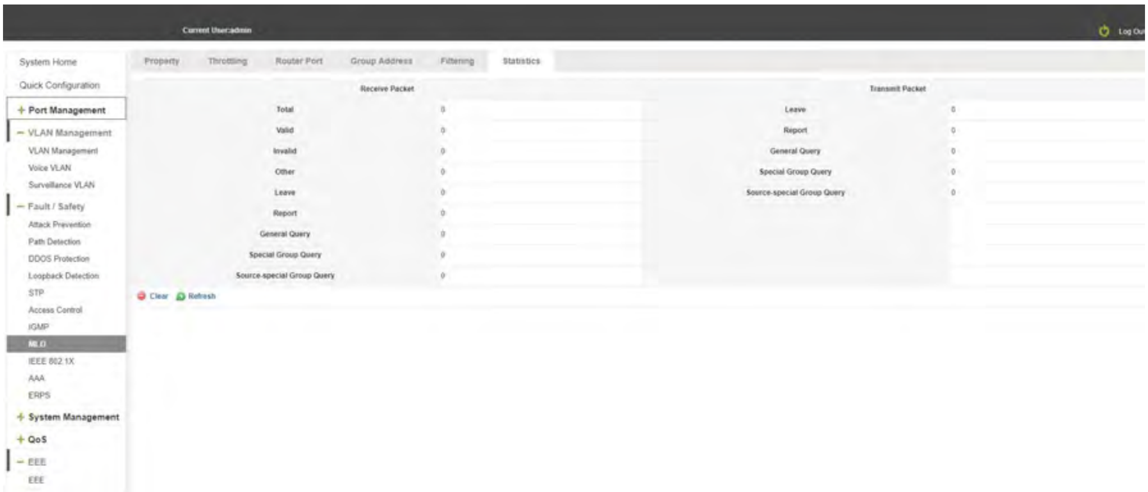
Profile ID: None

Port	Profile ID	Edit
1	None	
2	None	
3	None	
4	None	
5	1	
6	None	
7	None	
8	None	

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:

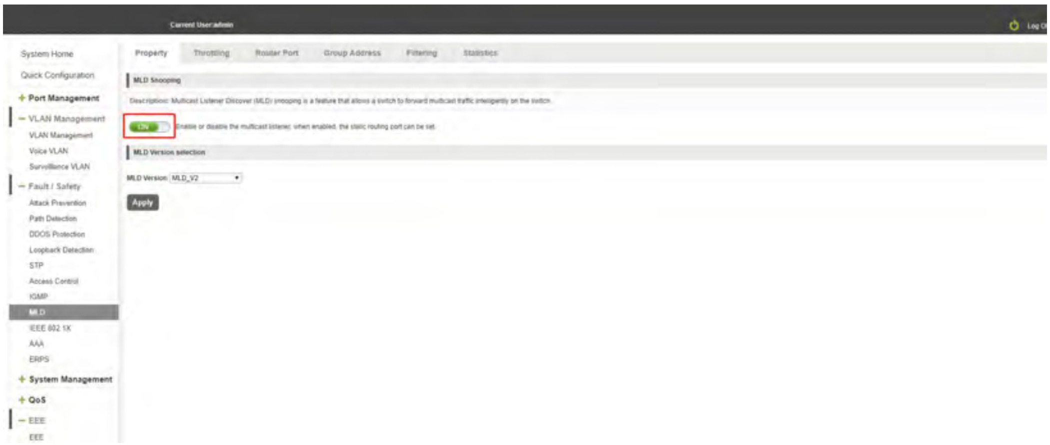


Receive Packet		Transmit Packet	
Total	0	Leave	0
Valid	0	Report	0
Invalid	0	General Query	0
Other	0	Special Group Query	0
Leave	0	Source-special Group Query	0
Report	0		
General Query	0		
Special Group Query	0		
Source-special Group Query	0		

Figure 5-49: MLD Statistics

5.8.7 DISABLE MULTICAST LISTENER FUNCTION

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



MLD Snooping

Description: Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

MLD Version selection

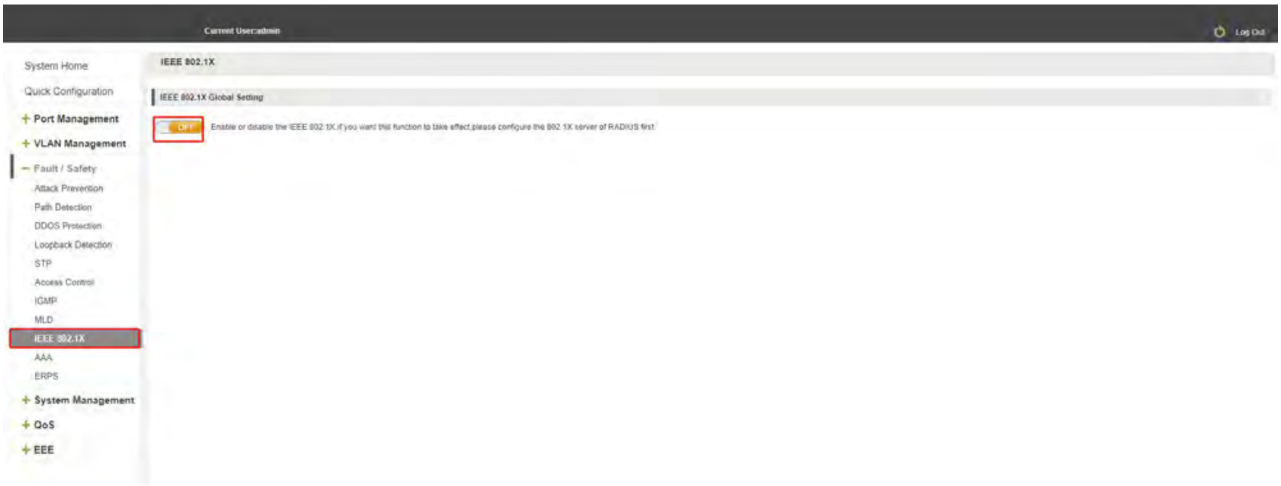
MLD Version: MLD_V2

Figure 5-50: Closed multicast listener function operation

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:

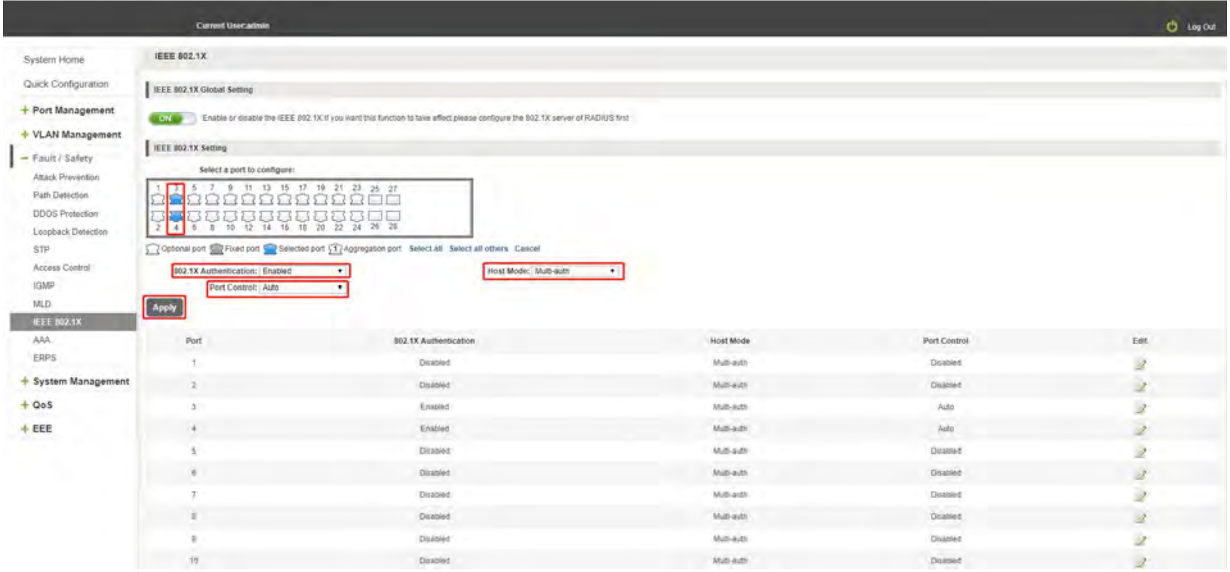


Enable or disable the IEEE 802.1X.If you want this function to take effect,please configure the 802.1X server of RADIUS first

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



Enable or disable the IEEE 802.1X.If you want this function to take effect,please configure the 802.1X server of RADIUS first

802.1X Authentication: Enabled

Port Control: Auto

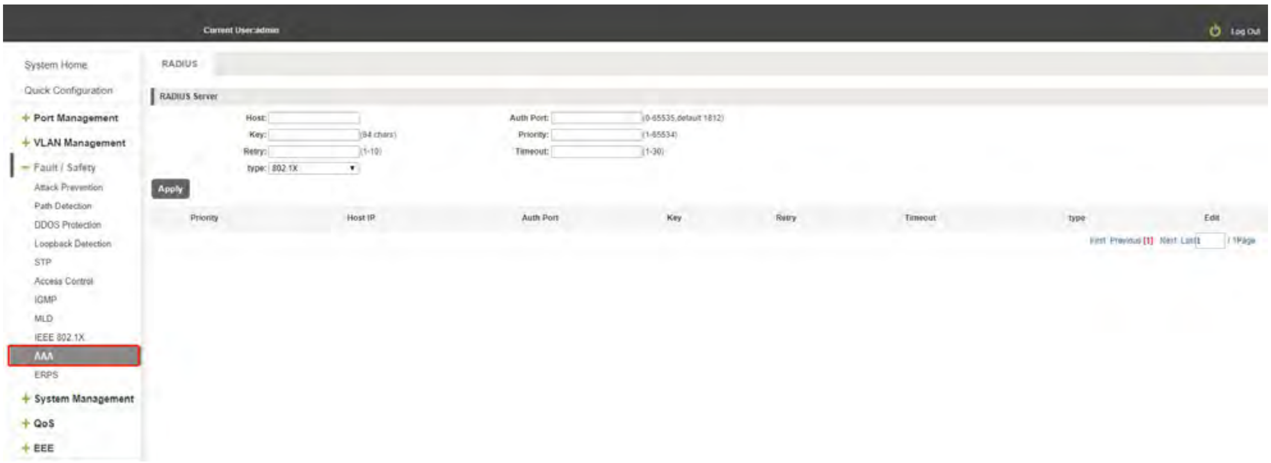
Host Mode: Multi-auth

Port	802.1X Authentication	Host Mode	Port Control	Edit
1	Disabled	Multi-auth	Disabled	
2	Disabled	Multi-auth	Disabled	
3	Enabled	Multi-auth	Auto	
4	Enabled	Multi-auth	Auto	
5	Disabled	Multi-auth	Disabled	
6	Disabled	Multi-auth	Disabled	
7	Disabled	Multi-auth	Disabled	
8	Disabled	Multi-auth	Disabled	
9	Disabled	Multi-auth	Disabled	
10	Disabled	Multi-auth	Disabled	

Figure 5-52: Port enable 802.1x function operation

5.10 AAA

5.9.1 VIEW AAA CONFIGURATION



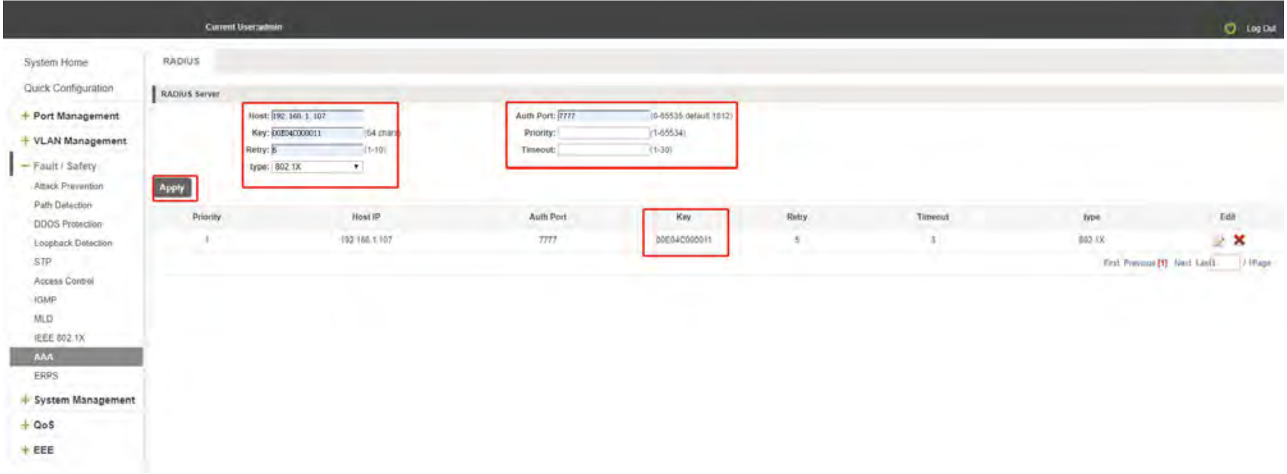
Host:
Key: (64 chars)
Retry: (1-10)
type: 802.1X
Auth Port: (0-65535,default 1812)
Priority: (1-65534)
Timeout: (1-30)

Priority	Host IP	Auth Port	Key	Retry	Timeout	type	Edit

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.



Host: 192.168.1.107
Key: 00E04C000011 (64 chars)
Retry: 5 (1-10)
type: 802.1X
Auth Port: 7777 (0-65535,default 1812)
Priority: (1-65534)
Timeout: (1-30)

Priority	Host IP	Auth Port	Key	Retry	Timeout	type	Edit
1	192.168.1.107	7777	00E04C000011	5	3	802.1X	✎ ✖

Figure 5-54: Radius server configuration

5.10 ERPS

5.10.1 VIEW ERPS CONFIGURATION

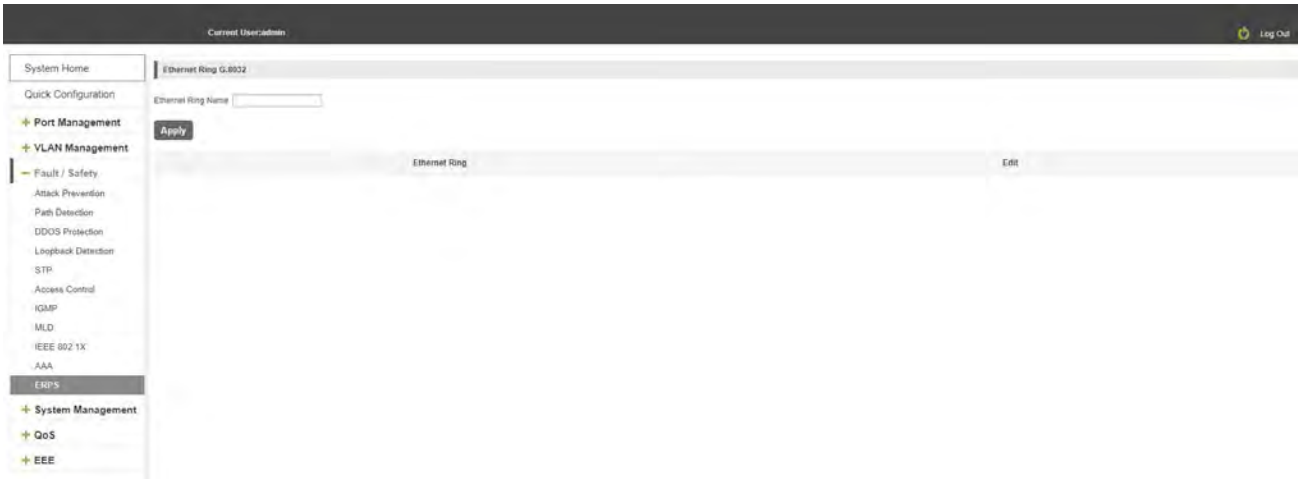
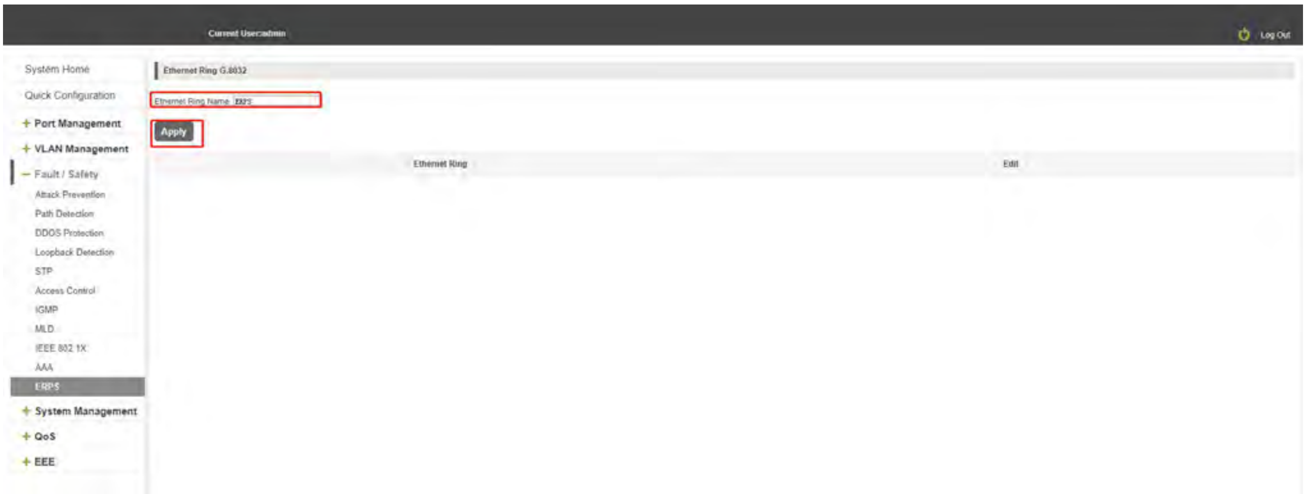


Figure 5-55: View ERPS configuration information

5.10.2 CREAT ERPS RING

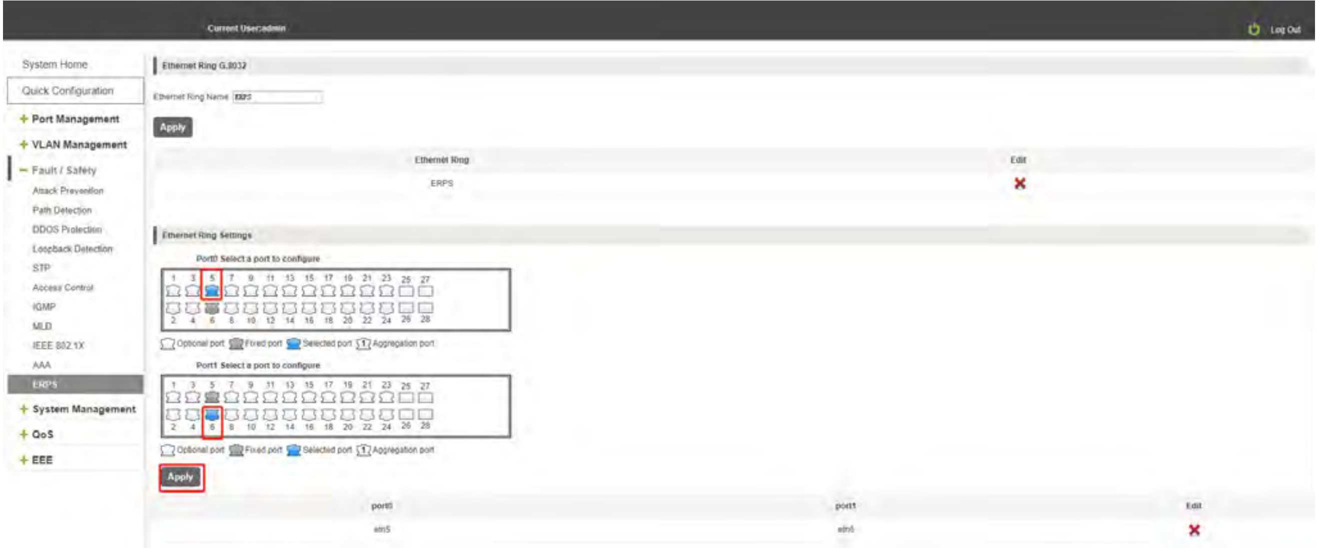


Ethernet Ring Name ERPS

Figure 5-56: Enable an erps ring

5.10.3 Enable erps port

Notice:The erps port must be in turnk mode, otherwise it cannot be successfully enabled。



Ethernet Ring G.8032

Ethernet Ring Name: ERPS

Ethernet Ring	Edit
ERPS	✖

Ethernet Ring Settings

Port0 Select a port to configure

Port1 Select a port to configure

port0	port1	Edit
eth5	eth6	✖

Figure 5-56: Port added erps ring

5.10.4 Erps ring parameter configuration

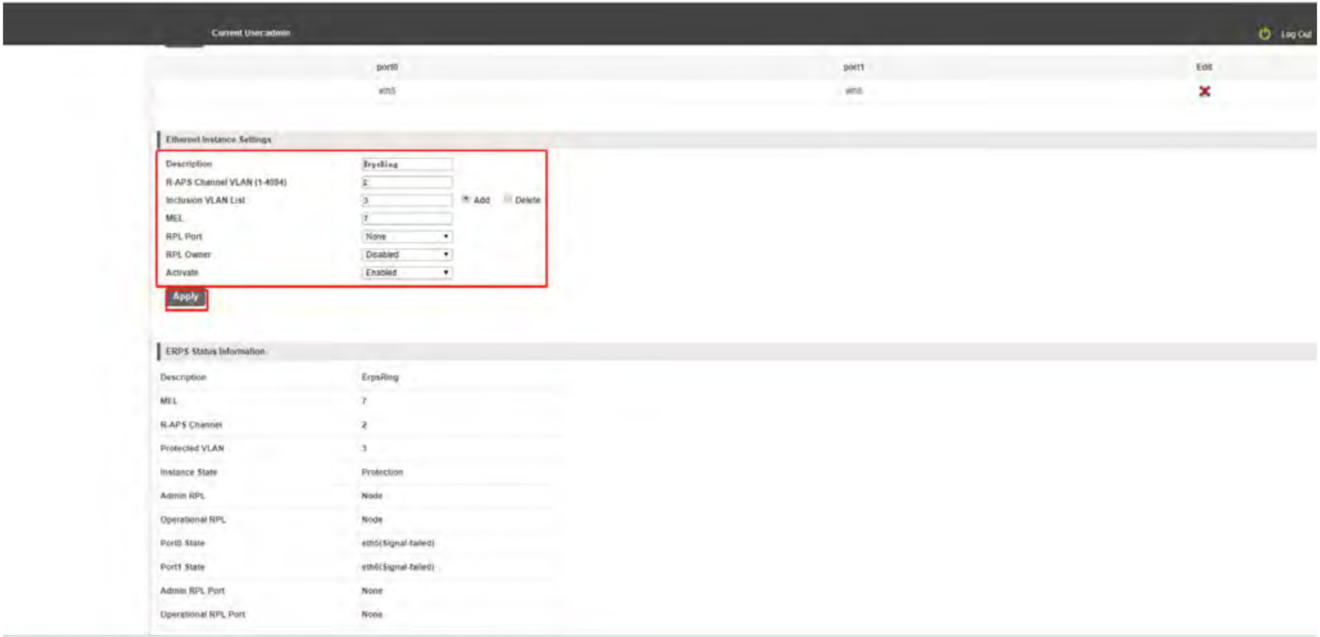
Notice:

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.



port0	port1	Edit
eth5	eth6	✖

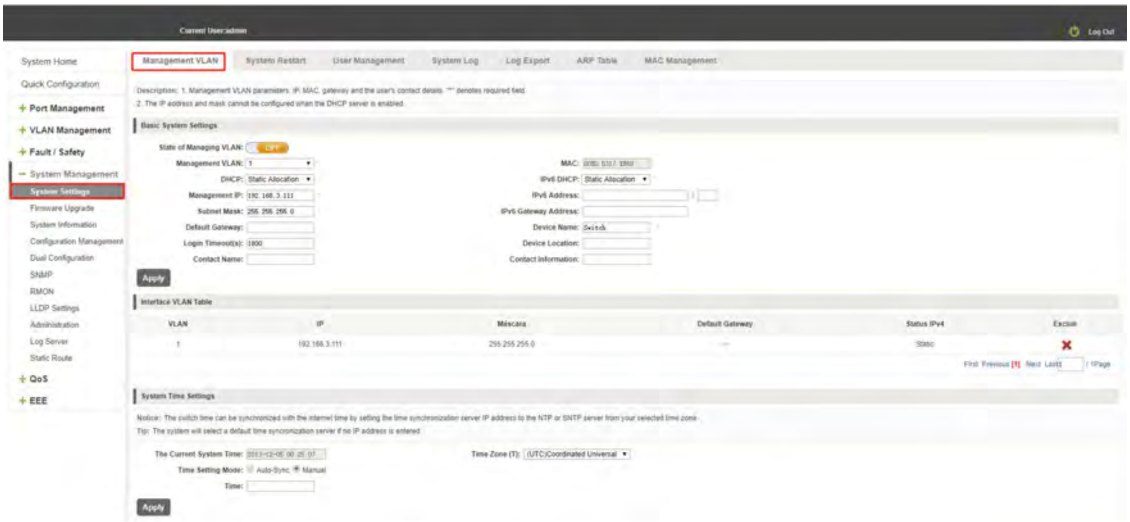
Ethernet Instance Settings

Description	ErpsRing
R-APS Channel VLAN (1-4094)	2
Inclusion VLAN List	3 ● Add ○ Delete
MEL	7
RPL Port	None
RPL Owner	Disabled
Activate	Enabled

ERPS Status Information

Description	ErpsRing
MEL	7
R-APS Channel	2
Protected VLAN	3
Instance State	Protection
Admin RPL	Node
Operational RPL	Node
Port0 State	eth5(Signal-failed)
Port1 State	eth6(Signal-failed)
Admin RPL Port	None
Operational RPL Port	None

Figure 5-56: Port added erps ring



Description: 1. Management VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.

2. The IP address and mask cannot be configured when the DHCP server is enabled.

Basic System Settings

State of Managing VLAN: OFF

Management VLAN: 1

DHCP: Static Allocation

Management IP: 192.168.3.111

Subnet Mask: 255.255.255.0

Default Gateway:

Login Timeout(s): 1800

Contact Name:

MAC:

IPv6 DHCP: Static Allocation

IPv6 Address:

IPv6 Gateway Address:

Device Name: Switch

Device Location:

Contact Information:

Interface VLAN Table

VLAN	IP	Máscara	Default Gateway	Status IPv4	Exclude
1	192.168.3.111	255.255.255.0	---	Static	✖

First Previous [1] Next Last / 1Page

System Time Settings

Notice: The switch time can be synchronized with the internet time by setting the time synchronization server IP address to the NTP or SNTP server from your selected time zone

Tip: The system will select a default time syncronization server if no IP address is entered

The Current System Time: 2013-12-05 00:25:07

Time Zone (T): (UTC)Coordinated Universal

Time Setting Mode: ○ Auto-Sync ● Manual

Time:

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

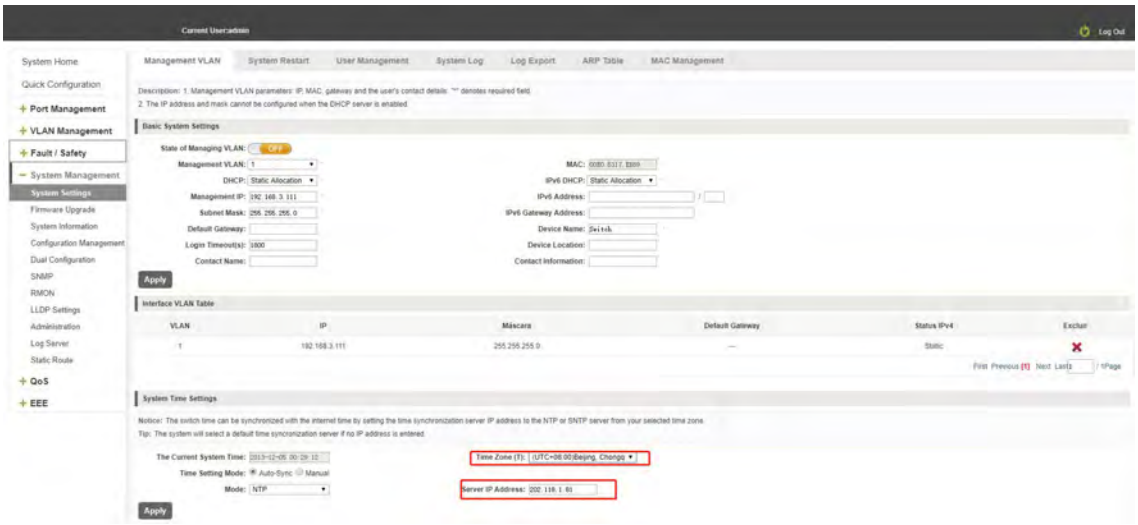
6.1 SYSTEM SETTINGS

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:

6.1.1.2System time synchronization



Description: 1. Management VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.

Basic System Settings

State of Managing VLAN: OFF
Management VLAN: 1
DHCP: Static Allocation
Management IP: 192.168.3.111
Subnet Mask: 255.255.255.0
Default Gateway:
Login Timeout(s): 1800
Contact Name:
MAC: 0080.8317.E889
IPv6 DHCP: Static Allocation
IPv6 Address: /
IPv6 Gateway Address:
Device Name: Switch
Device Location:
Contact Information:

Interface VLAN Table

VLAN	IP	Máscara	Default Gateway	Status IPv4	Excluir
1	192.168.3.111	255.255.255.0	—	Static	✕

First Previous [1] Next Last 1 / 1Page

System Time Settings

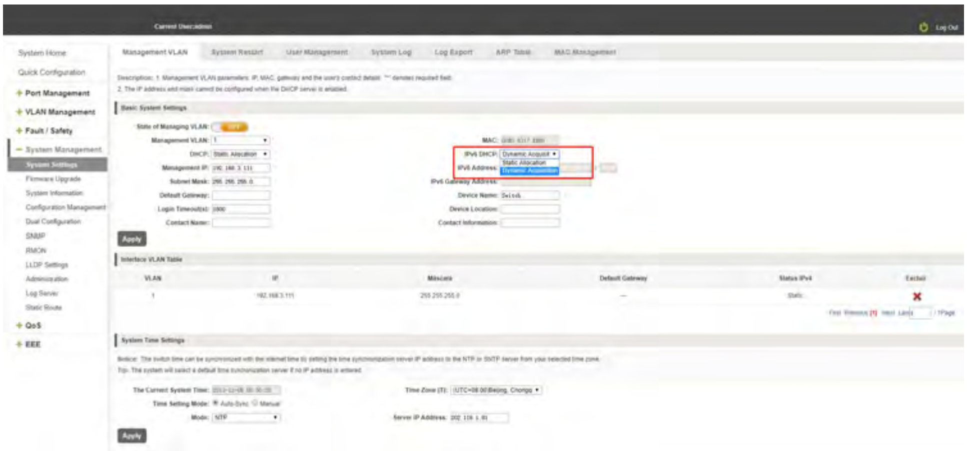
Notice: The switch time can be synchronized with the internet time by setting the time synchronization server IP address to the NTP or SNTP server from your selected time zone.
Tip: The system will select a default time syncronization server if no IP address is entered.

The Current System Time: 2013-12-05 00:29:12
Time Setting Mode: ● Auto-Sync ○ Manual
Mode: NTP
Time Zone (T): (UTC+08:00)Beijing, Chongq
Server IP Address: 202.118.1.81

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.

6.1.1.3DHCPv6 client



Description: 1. Management VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.

Basic System Settings

State of Managing VLAN: OFF
Management VLAN: 1
DHCP: Static Allocation
Management IP: 192.168.3.111
Subnet Mask: 255.255.255.0
Default Gateway:
Login Timeout(s): 1800
Contact Name:
MAC: 0080.8317.E889
IPv6 DHCP: Dynamic Acquisit
IPv6 Address:
IPv6 Gateway Address:
Device Name: Switch
Device Location:
Contact Information:

Interface VLAN Table

VLAN	IP	Máscara	Default Gateway	Status IPv4	Excluir
1	192.168.3.111	255.255.255.0	—	Static	✕

First Previous [1] Next Last 1 / 1Page

System Time Settings

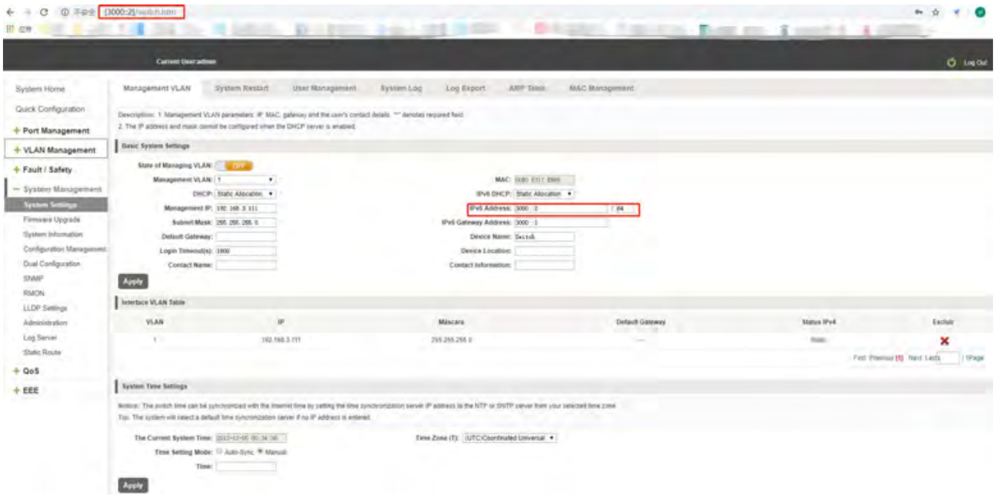
Notice: The switch time can be synchronized with the internet time by setting the time synchronization server IP address to the NTP or SNTP server from your selected time zone.
Tip: The system will select a default time syncronization server if no IP address is entered.

The Current System Time: 2013-12-05 00:30:05
Time Setting Mode: ● Auto-Sync ○ Manual
Mode: NTP
Time Zone (T): (UTC+08:00)Beijing, Chongq
Server IP Address: 202.118.1.81

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.

6.1.1.4IPv6 HTTPS



Description: 1. Management VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.

Basic System Settings

State of Managing VLAN: OFF
Management VLAN: 1
DHCP: Static Allocation
Management IP: 192.168.3.111
Subnet Mask: 255.255.255.0
Default Gateway:
Login Timeout(s): 1800
Contact Name:
MAC: 0080:E717:E800
IPv6 DHCP: Static Allocation
IPv6 Address: 3000::2 / 64
IPv6 Gateway Address: 3000::1
Device Name: Switch
Device Location:
Contact Information:

Interface VLAN Table

VLAN	IP	Máscara	Default Gateway	Status IPv4	Excluir
1	192.168.3.111	255.255.255.0	---	Static	✗

System Time Settings

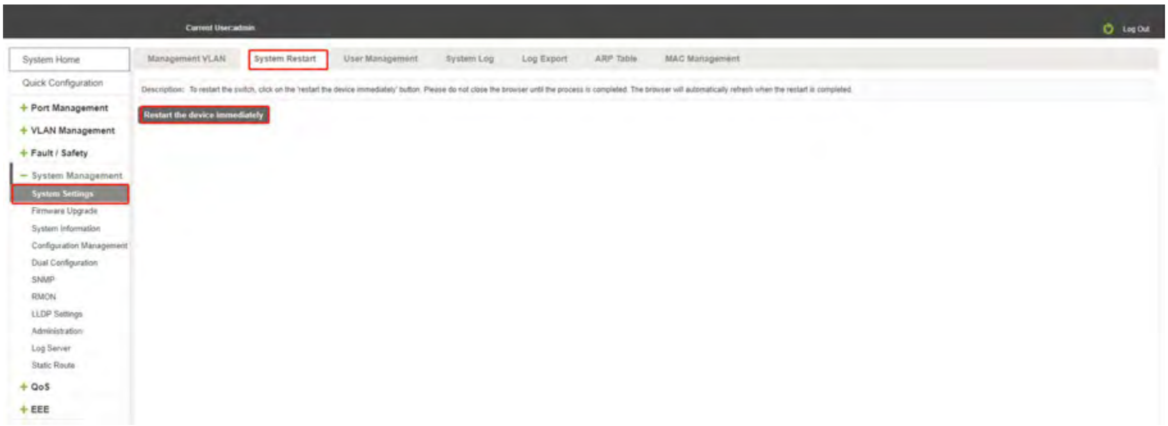
Notice: The switch time can be synchronized with the Internet time by setting the time synchronization server IP address to the NTP or SNTP server from your selected time zone.
Tip: The system will select a default time synchronization server if no IP address is entered.

The Current System Time: 2013-12-05 00:34:56
Time Zone (T): (UTC)Coordinated Universal
Time Setting Mode: □ Auto-Sync ● Manual
Time:

Figure 6-4: IPv6 HTTPS

6.1.2 SYSTEM RESTAR

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



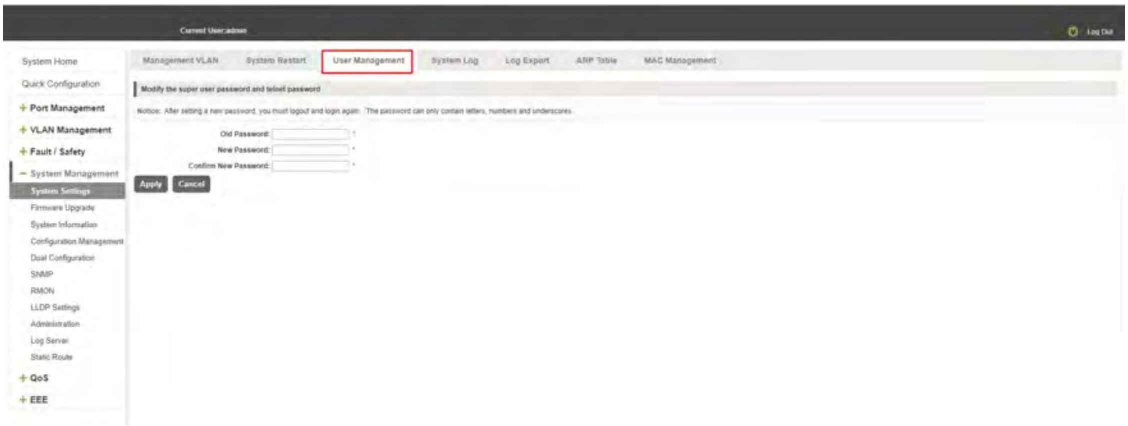
Description: To restart the switch, click on the 'restart the device immediately' button. Please do not close the browser until the process is completed. The browser will automatically refresh when the restart is completed.

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:



Modify the super user password and telnet password

Notice: After setting a new password, you must logout and login again. The password can only contain letters, numbers and underscores.

Old Password: *

New Password: *

Confirm New Password: *

Figure 6-6: change password

Change password follow these steps:

step1:Enter the old password: password;

step2:Enter the new password: admin;

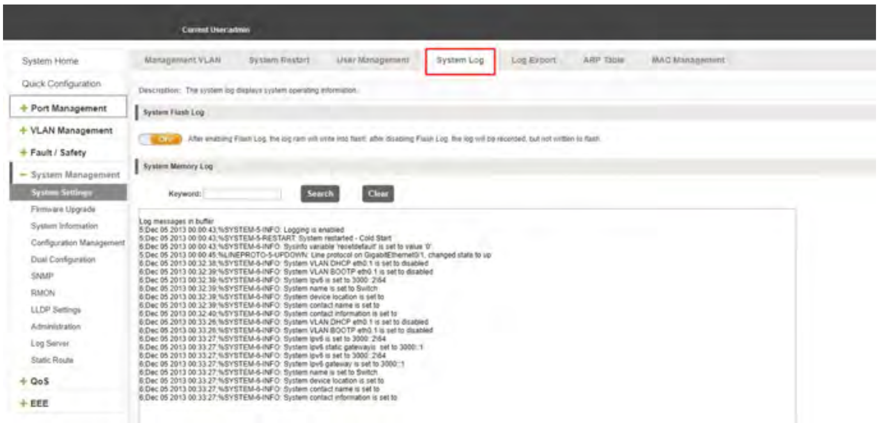
step3:Confirm new password: admin,

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:



Description: The system log displays system operating information.

System Flash Log

OFF After enabling Flash Log, the log ram will write into flash; after disabling Flash Log, the log will be recorded, but not written to flash.

System Memory Log

Keyword:

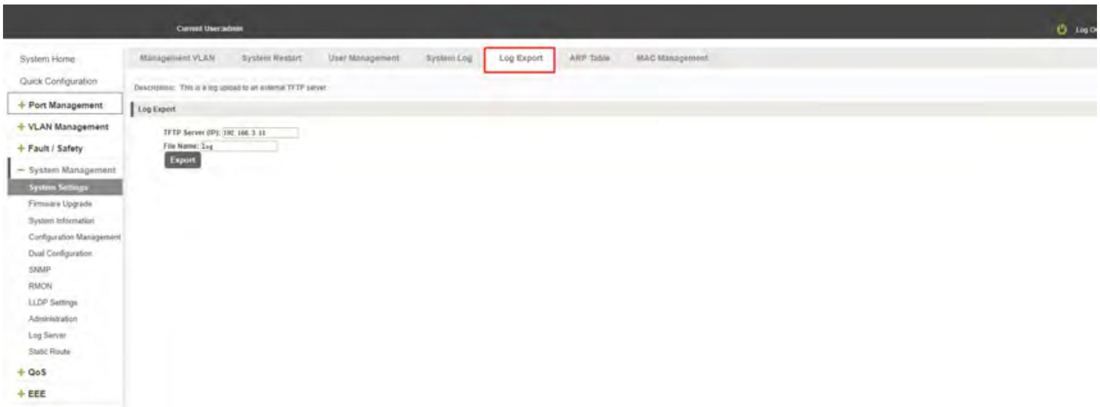
```
Log messages in buffer
5;Dec 05 2013 00:00:43;%SYSTEM-5-INFO: Logging is enabled
5;Dec 05 2013 00:00:43;%SYSTEM-5-RESTART: System restarted - Cold Start
6;Dec 05 2013 00:00:43;%SYSTEM-6-INFO: Sysinfo variable 'resetdefault' is set to value '0'
5;Dec 05 2013 00:00:45;%LINEPROTO-5-UPDOWN: Line protocol on GigabitEthernet0/1, changed state to up
6;Dec 05 2013 00:32:38;%SYSTEM-6-INFO: System VLAN DHCP eth0.1 is set to disabled
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System VLAN BOOTP eth0.1 is set to disabled
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System name is set to Switch
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System device location is set to
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System contact name is set to
6;Dec 05 2013 00:32:40;%SYSTEM-6-INFO: System contact information is set to
6;Dec 05 2013 00:33:26;%SYSTEM-6-INFO: System VLAN DHCP eth0.1 is set to disabled
6;Dec 05 2013 00:33:26;%SYSTEM-6-INFO: System VLAN BOOTP eth0.1 is set to disabled
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 static gatewayis  set to 3000::1
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 gateway is set to 3000::1
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System name is set to Switch
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System device location is set to
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System contact name is set to
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System contact information is set to
```

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.



Description: This is a log upload to an external TFTP server

Log Export

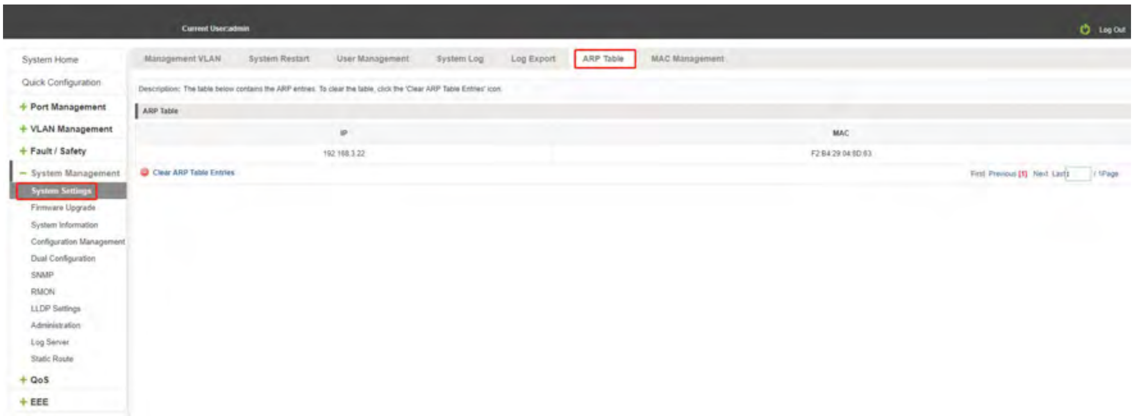
TFTP Server (IP): 192.168.3.11

File Name: log

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:



Description: The table below contains the ARP entries. To clear the table, click the 'Clear ARP Table Entries' icon.

ARP Table

IP	MAC
192.168.3.22	F2:B4:29:04:8D:63

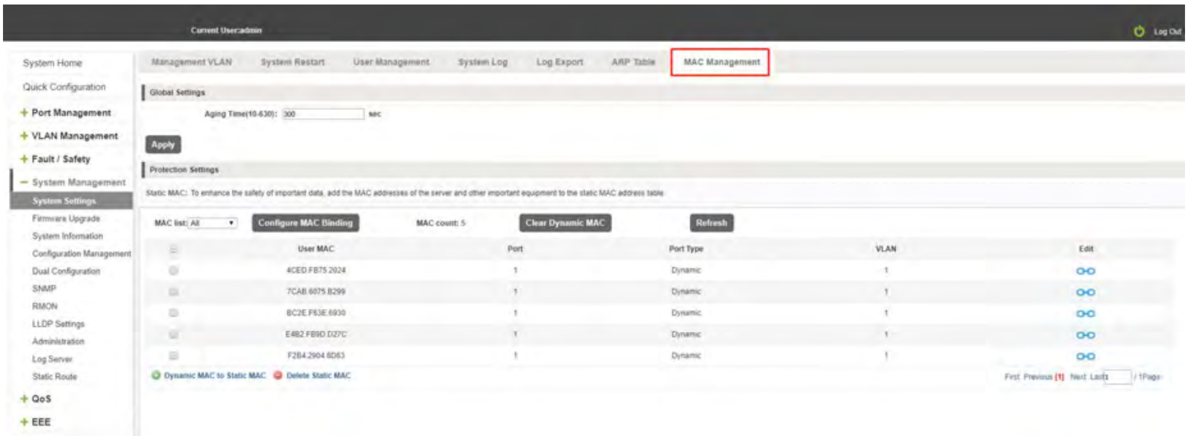
Figure 6-9: ARP message

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

6.1.7 MAC MANAGEMENT

6.1.7.1MAC address lookup

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



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table

MAC list: All

MAC count: 5

	User MAC	Port	Port Type	VLAN	Edit
□	4CED.FB75.2024	1	Dynamic	1	
□	7CAB.6075.B299	1	Dynamic	1	
□	BC2E.F63E.6930	1	Dynamic	1	
□	E4B2.FB9D.D27C	1	Dynamic	1	
□	F2B4.2904.6D63	1	Dynamic	1	

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;

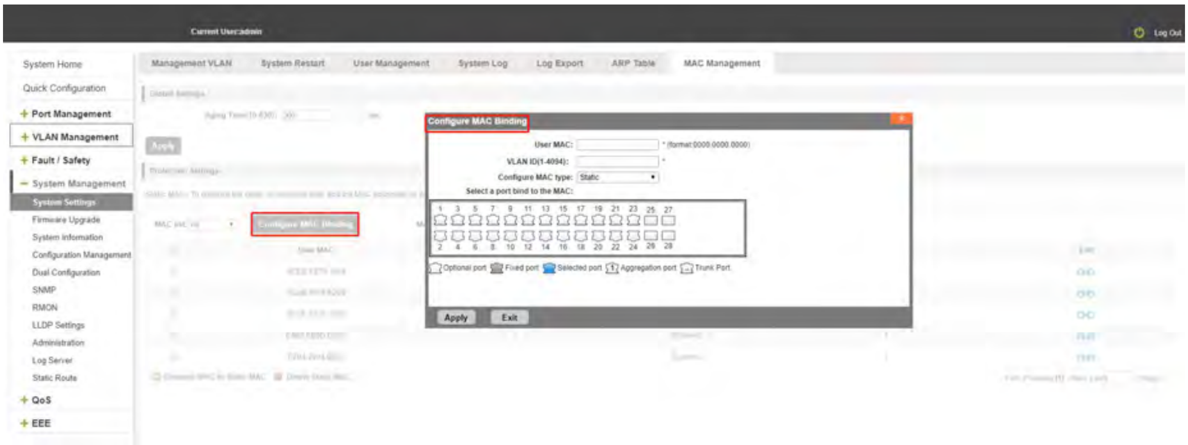
3.Port Type: There are two types of dynamic and static;

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.

6.1.7.2Add 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:



Configure MAC Binding

User MAC: * (format:0000.0000.0000)

VLAN ID(1-4094): *

Configure MAC type: Static

Select a port bind to the MAC:

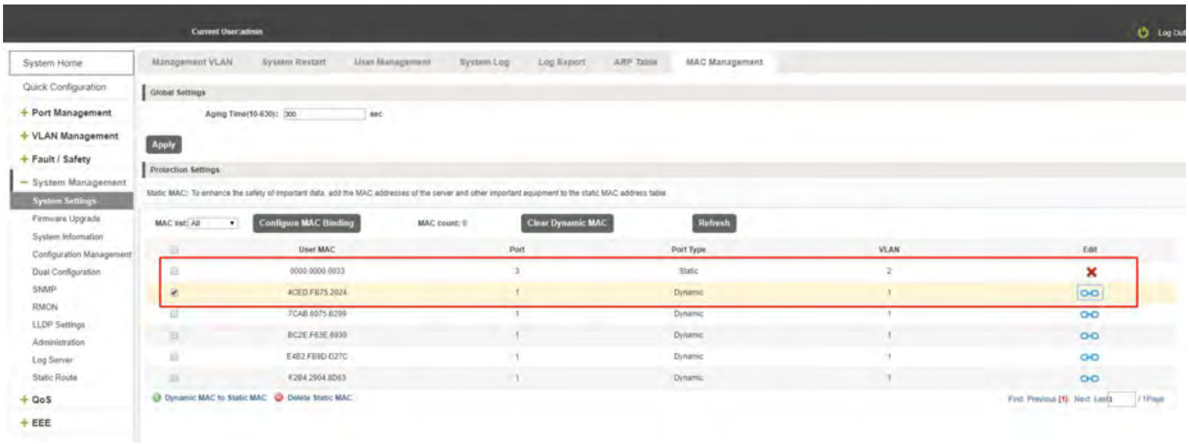
Figure 6-11: MAC addresses statically bound static configuration

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:



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table

MAC list: All

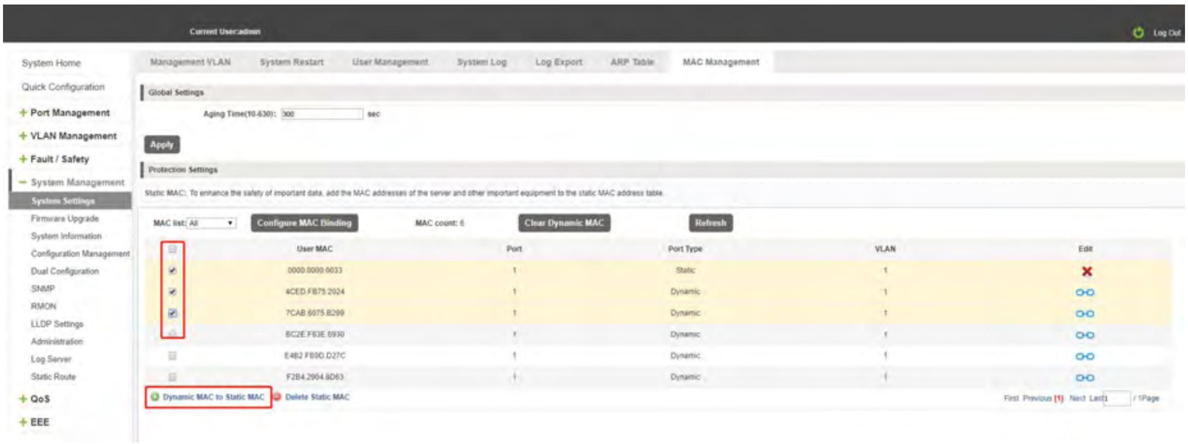
MAC count: 6

□	User MAC	Port	Port Type	VLAN	Edit
□	0000.0000.0033	3	Static	2	✕
☑	4CED.FB75.2024	1	Dynamic	1	🔗
□	7CAB.6075.B299	1	Dynamic	1	🔗
□	BC2E.F63E.6930	1	Dynamic	1	🔗
□	E4B2.FB9D.D27C	1	Dynamic	1	🔗
□	F2B4.2904.8D63	1	Dynamic	1	🔗

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:



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table

MAC list: All

MAC count: 6

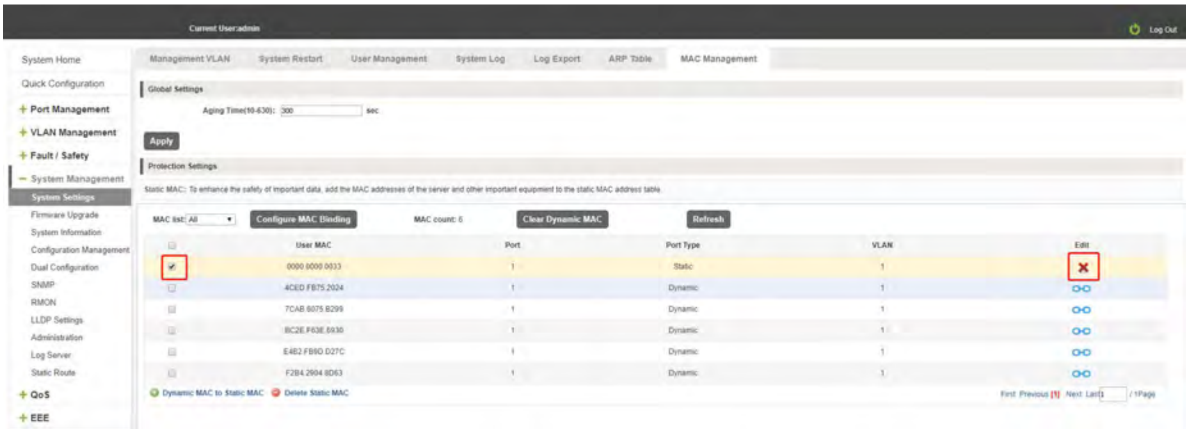
□	User MAC	Port	Port Type	VLAN	Edit
☑	0000.0000.0033	1	Static	1	✕
☑	4CED.FB75.2024	1	Dynamic	1	🔗
☑	7CAB.6075.B299	1	Dynamic	1	🔗
□	BC2E.F63E.6930	1	Dynamic	1	🔗
□	E4B2.FB9D.D27C	1	Dynamic	1	🔗
□	F2B4.2904.8D63	1	Dynamic	1	🔗

Figure 6-13: Batch-MAC binding configuration

6.1.7.3Remove 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:



Aging Time(10-630): 300 sec

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All

MAC count: 6

□	User MAC	Port	Port Type	VLAN	Edit
☑	0000.0000.0033	1	Static	1	✖
□	4CED.FB75.2024	1	Dynamic	1	⚯
□	7CAB.6075.B299	1	Dynamic	1	⚯
□	BC2E.F63E.6930	1	Dynamic	1	⚯
□	E4B2.FB9D.D27C	1	Dynamic	1	⚯
□	F2B4.2904.8D63	1	Dynamic	1	⚯

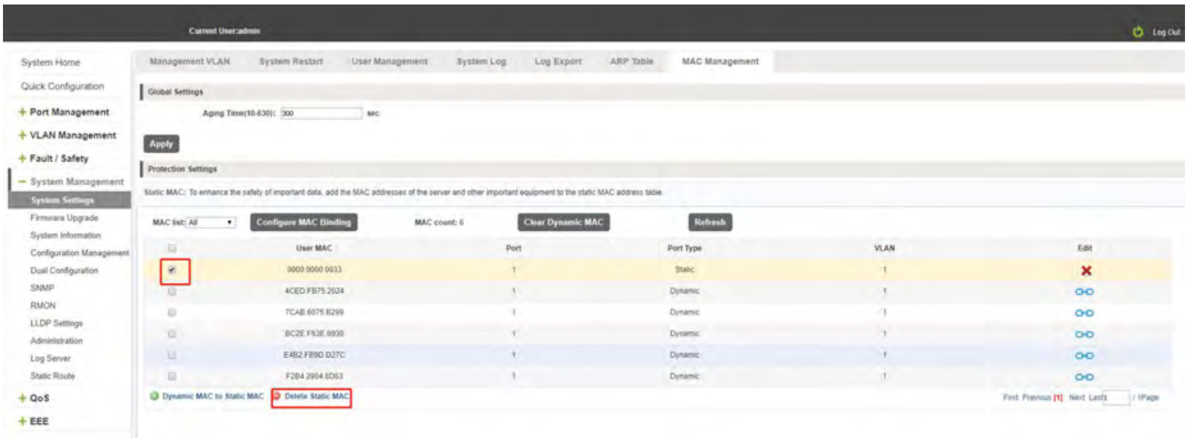
Figure 6-14: MAC address deletion

Remove MAC address configuration steps are as follows:

Step1:To delete the selected MAC address,step2: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:



Aging Time(10-630): 300 sec

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All

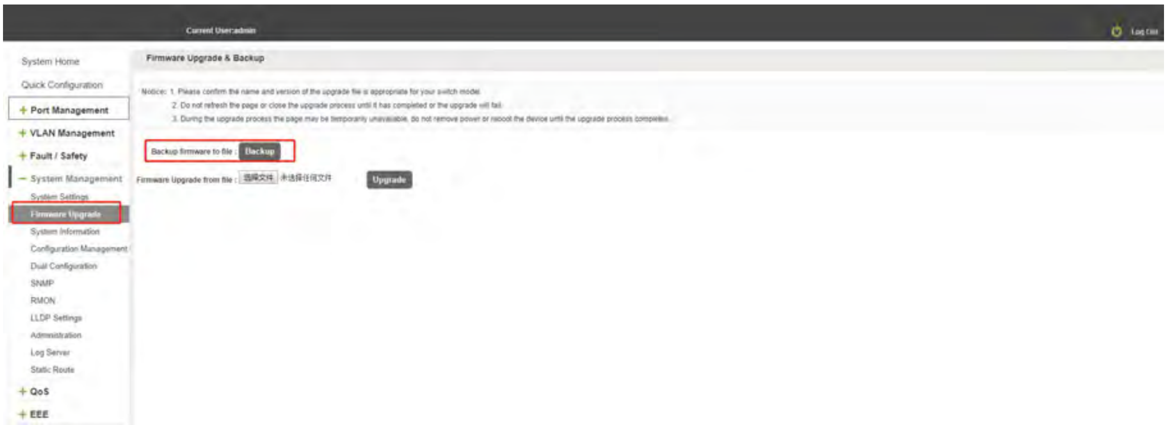
MAC count: 6

□	User MAC	Port	Port Type	VLAN	Edit
☑	0000.0000.0033	1	Static	1	✗
□	4CED.FB75.2024	1	Dynamic	1	⚭
□	7CAB.6075.B299	1	Dynamic	1	⚭
□	BC2E.F53E.6930	1	Dynamic	1	⚭
□	E4B2.FB9D.D27C	1	Dynamic	1	⚭
□	F2B4.2904.6D63	1	Dynamic	1	⚭

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:



Firmware Upgrade & Backup

Notice: 1. Please confirm the name and version of the upgrade file is appropriate for your switch model.
2. Do not refresh the page or close the upgrade process until it has completed or the upgrade will fail.
3. During the upgrade process the page may be temporarily unavailable, do not remove power or reboot the device until the upgrade process completes.

Backup firmware to file : Backup

Firmware Upgrade from file : 选择文件 未选择任何文件

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;

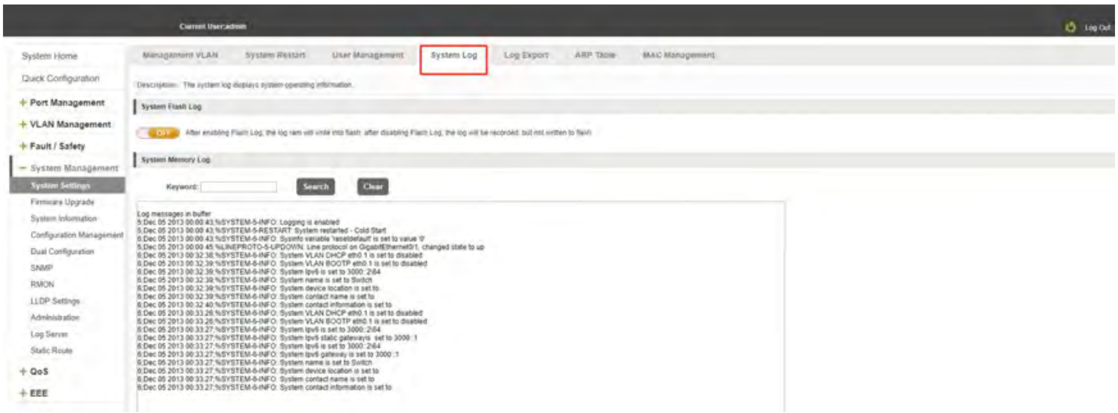
step2:Click the "Upgrade" button switch to start the upgrade new software;

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:



Description: The system log displays system operating information.

After enabling Flash Log, the log ram will write into flash; after disabling Flash Log, the log will be recorded, but not written to flash

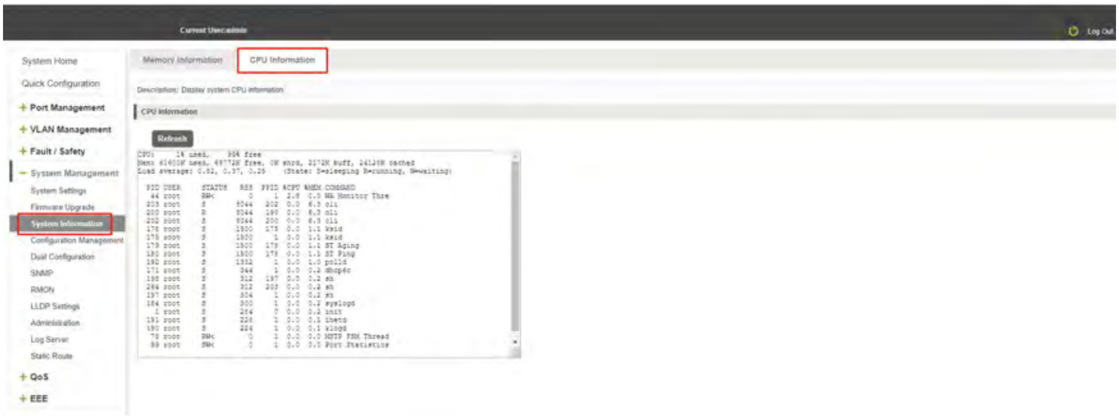
```
Log messages in buffer
5;Dec 05 2013 00:00:43;%SYSTEM-5-INFO: Logging is enabled
5;Dec 05 2013 00:00:43;%SYSTEM-5-RESTART: System restarted - Cold Start
6;Dec 05 2013 00:00:43;%SYSTEM-6-INFO: Sysinfo variable 'resetdefault' is set to value '0'
5;Dec 05 2013 00:00:45;%LINEPROTO-5-UPDOWN: Line protocol on GigabitEthernet0/1, changed state to up
6;Dec 05 2013 00:32:38;%SYSTEM-6-INFO: System VLAN DHCP eth0.1 is set to disabled
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System VLAN BOOTP eth0.1 is set to disabled
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System name is set to Switch
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System device location is set to
6;Dec 05 2013 00:32:39;%SYSTEM-6-INFO: System contact name is set to
6;Dec 05 2013 00:32:40;%SYSTEM-6-INFO: System contact information is set to
6;Dec 05 2013 00:33:26;%SYSTEM-6-INFO: System VLAN DHCP eth0.1 is set to disabled
6;Dec 05 2013 00:33:26;%SYSTEM-6-INFO: System VLAN BOOTP eth0.1 is set to disabled
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 static gateways  set to 3000::1
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 is set to 3000::2/64
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System Ipv6 gateway is set to 3000::1
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System name is set to Switch
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System device location is set to
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System contact name is set to
6;Dec 05 2013 00:33:27;%SYSTEM-6-INFO: System contact information is set to
```

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:



Description: Display system CPU information

CPU Information

```
CPU:     1% used,    99% free
Mem: 61400K used, 48772K free, 0K shrd, 2172K buff, 14128K cached
Load average: 0.52, 0.37, 0.25    (State: S=sleeping R=running, W=waiting)

  PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
   44 root     RW<        0     1  2.8  0.0 ML Monitor Thre
  203 root     S       8044   202  0.0  6.3 cli
  200 root     R       8044   199  0.0  6.3 cli
  202 root     S       8044   200  0.0  6.3 cli
  176 root     S       1500   175  0.0  1.1 ksid
  175 root     S       1500     1  0.0  1.1 ksid
  179 root     S       1500   178  0.0  1.1 ST Aging
  180 root     S       1500   178  0.0  1.1 ST Ping
  192 root     S       1332     1  0.0  1.0 polld
  171 root     S        344     1  0.0  0.2 dhcp6c
  198 root     S        312   197  0.0  0.2 sh
  264 root     S        312   203  0.0  0.2 sh
  197 root     S        304     1  0.0  0.2 sh
  184 root     S        300     1  0.0  0.2 syslogd
    1 root     S        254     0  0.0  0.2 init
  191 root     S        228     1  0.0  0.1 inetd
  190 root     S        224     1  0.0  0.1 klogd
   78 root     RW<        0     1  0.0  0.0 MSTP FSM Thread
   89 root     RW<        0     1  0.0  0.0 Port Statistics
```

Figure 6-18: CPU information

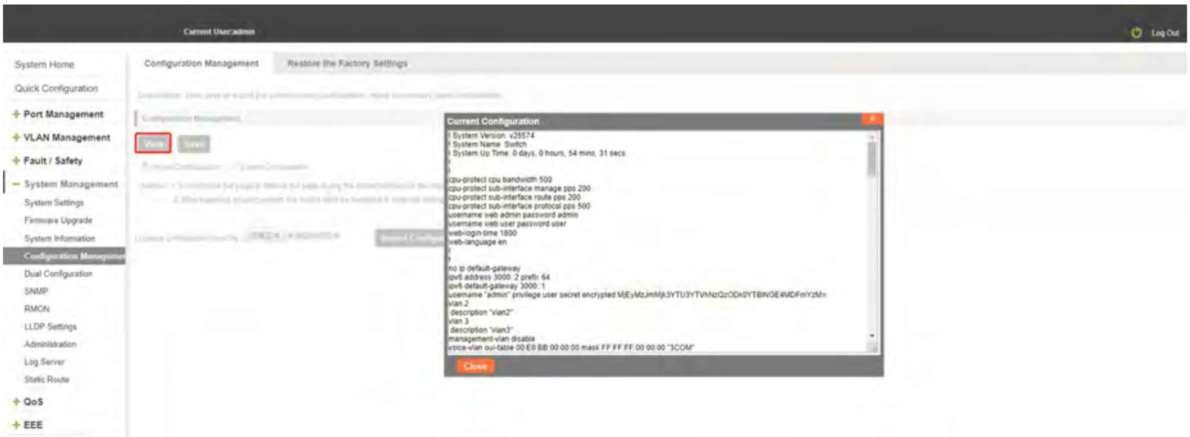
WEB pages to the content of the system task view consistent with the results show the CPU commands command line;click on the "Clear" button to remove the current switches in the system;Click on the "Refresh" button to Refresh the current switches in the system task.

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:

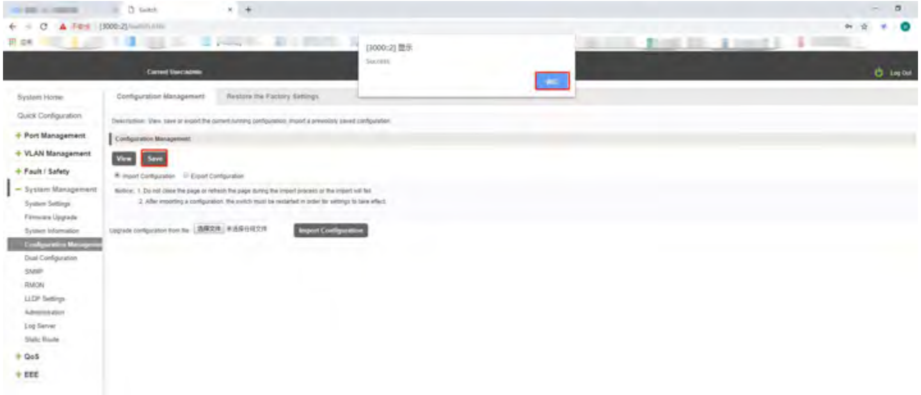


```
! System Version: v25574
! System Name: Switch
! System Up Time: 0 days, 0 hours, 54 mins, 31 secs
!
!
cpu-protect cpu bandwidth 500
cpu-protect sub-interface manage pps 200
cpu-protect sub-interface route pps 200
cpu-protect sub-interface protocol pps 500
username web admin password admin
username web user password user
web-login-time 1800
web-language en
!
!
no ip default-gateway
ipv6 address 3000::2 prefix 64
ipv6 default-gateway 3000::1
username "admin" privilege user secret encrypted MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMx
vlan 2
 description "vlan2"
vlan 3
 description "vlan3"
management-vlan disable
voice-vlan oui-table 00:E0:BB:00:00:00 mask FF:FF:FF:00:00:00 "3COM"
```

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:



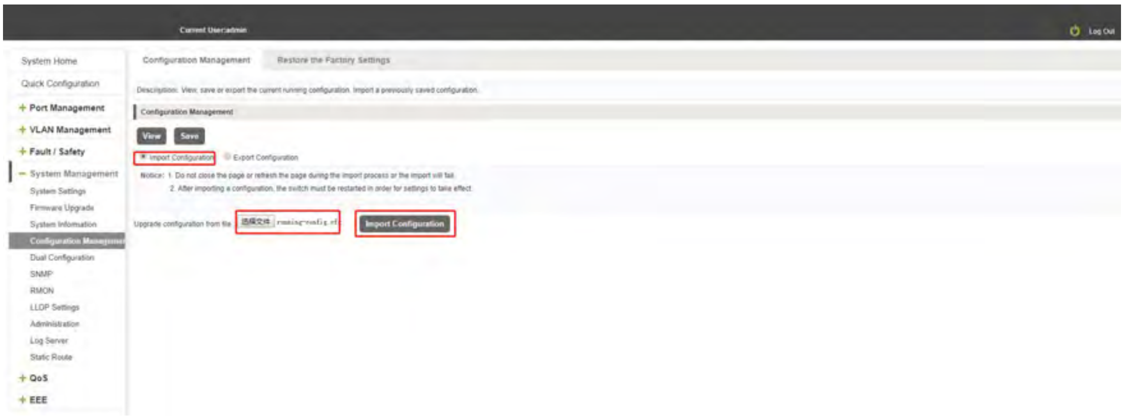
Description: View, save or export the current running configuration, import a previously saved configuration.

Notice: 1. Do not close the page or refresh the page during the import process or the import will fail.
2. After importing a configuration, the switch must be restarted in order for settings to take effect.

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:



Description: View, save or export the current running configuration. Import a previously saved configuration.

Configuration Management

● Import Configuration ○ Export Configuration

Notice: 1. Do not close the page or refresh the page during the import process or the import will fail.
2. After importing a configuration, the switch must be restarted in order for settings to take effect.

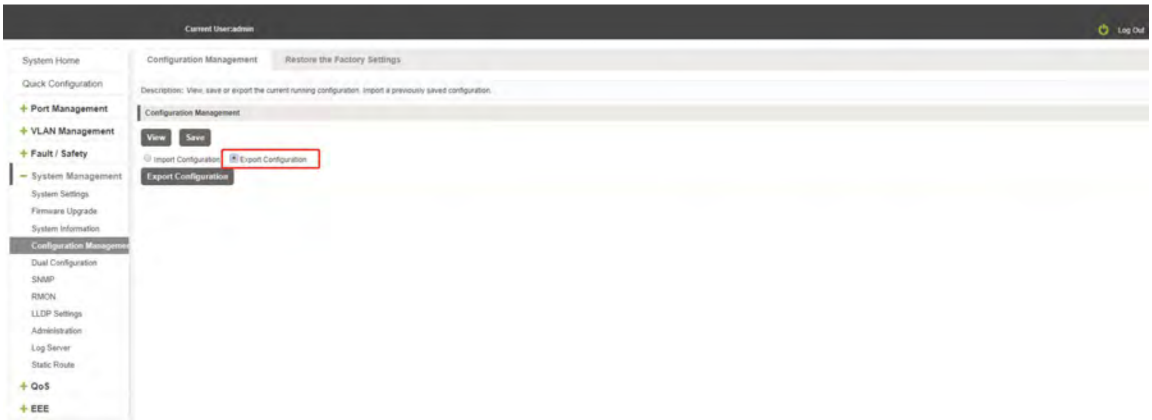
Upgrade configuration from file 选择文件 running-config.cf

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.



Description: View, save or export the current running configuration. Import a previously saved configuration.

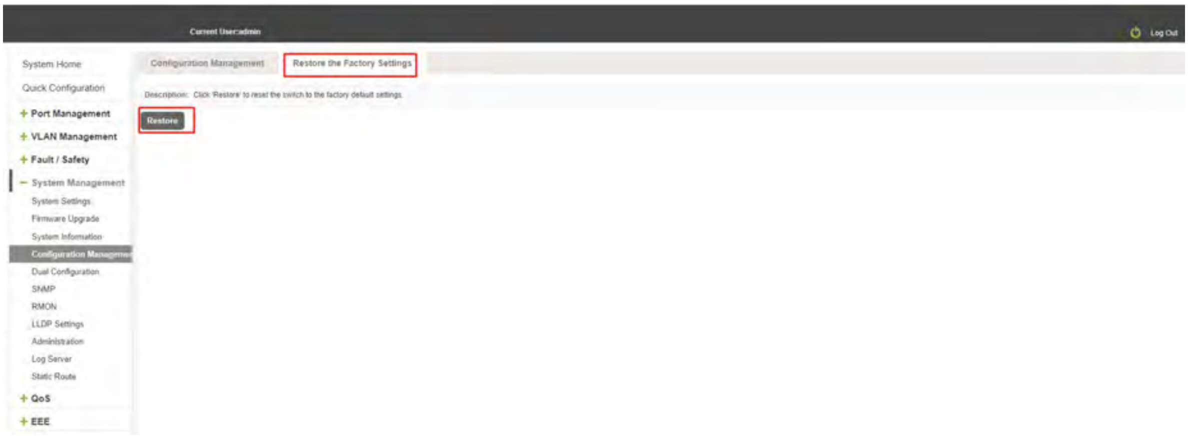
Configuration Management

○ Import 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:



Description: Click 'Restore' to reset the switch to the factory default settings.

Figure 6-26: Restore factory Settings

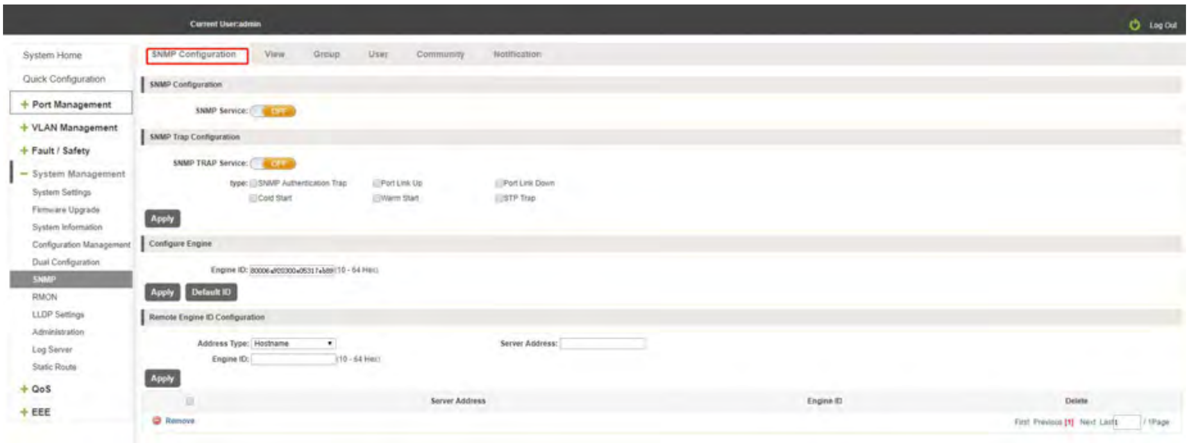
Factory default operation steps are as follows:

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:



SNMP Configuration

SNMP Service: OFF

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a903000e05317eb89 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname

Server Address:

Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

1 / 1Page

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:

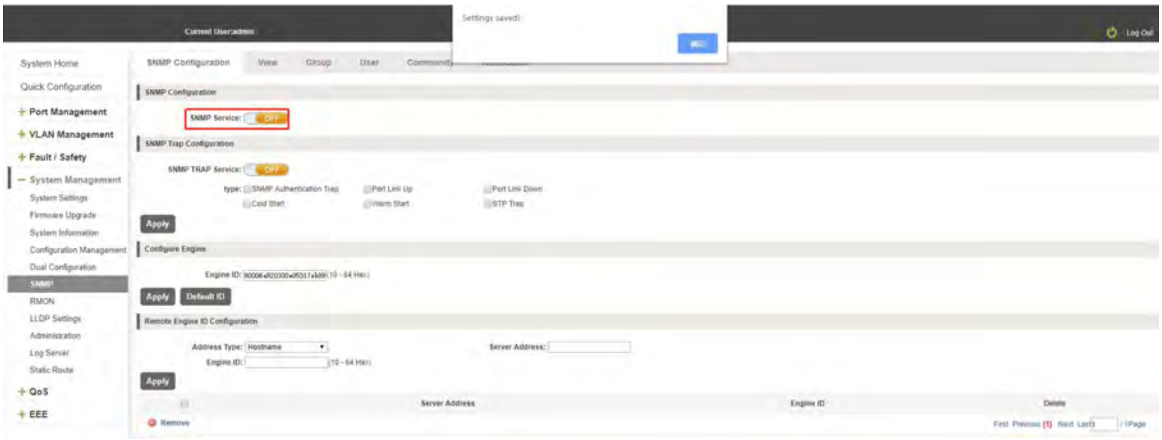


Figure 6-28: Activation SNMP function

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:

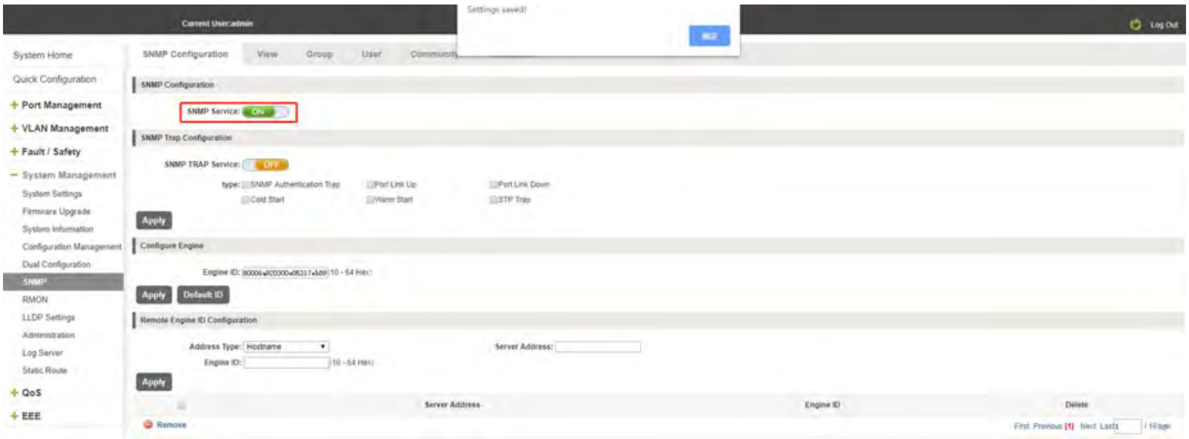


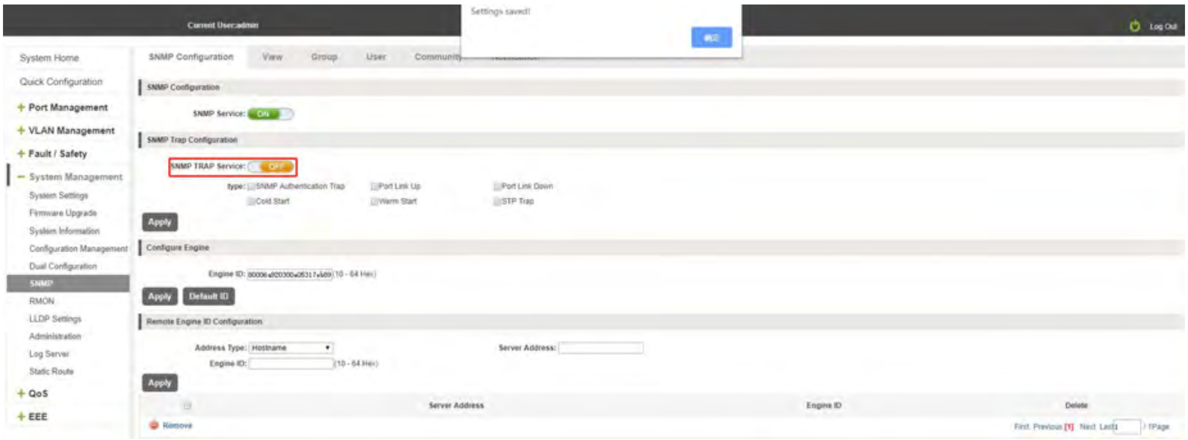
Figure 6-29: Disable the SNMP function

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:



Settings saved!

SNMP Configuration

SNMP Service: ON

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a920300a05317ab89 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname ▾ Server Address:
Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

First Previous [1] Next Last 1 / 1Page

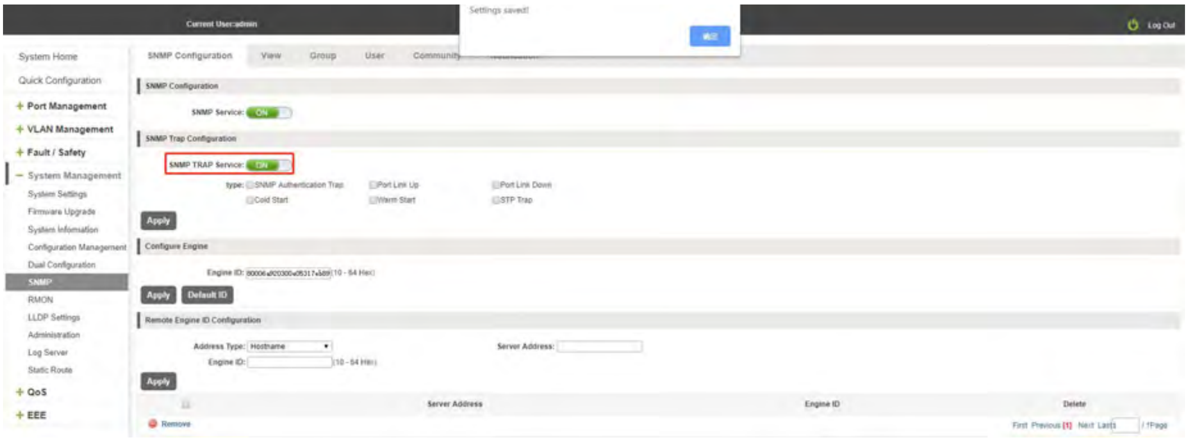
Figure 6-30: Activation function of the TRAP

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:



Settings saved!

SNMP Configuration

SNMP Service: ON

SNMP Trap Configuration

SNMP TRAP Service: ON

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a920300a05317ab89 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname ▾ Server Address:
Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

First Previous [1] Next Last 1 / 1Page

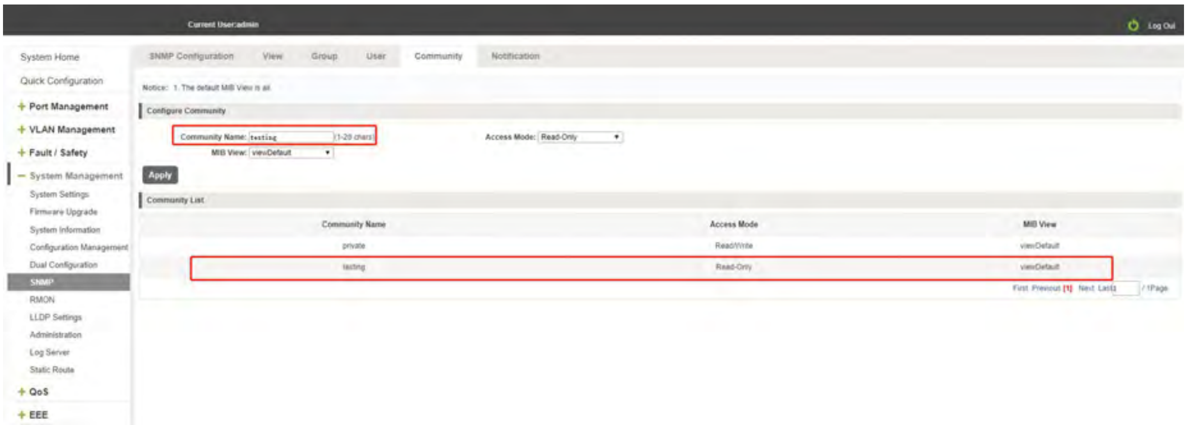
Figure 6-31: Disable TRAP function

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:



Notice: 1. The default MIB View is all.

Configure Community

Community Name: testing (1-20 chars)

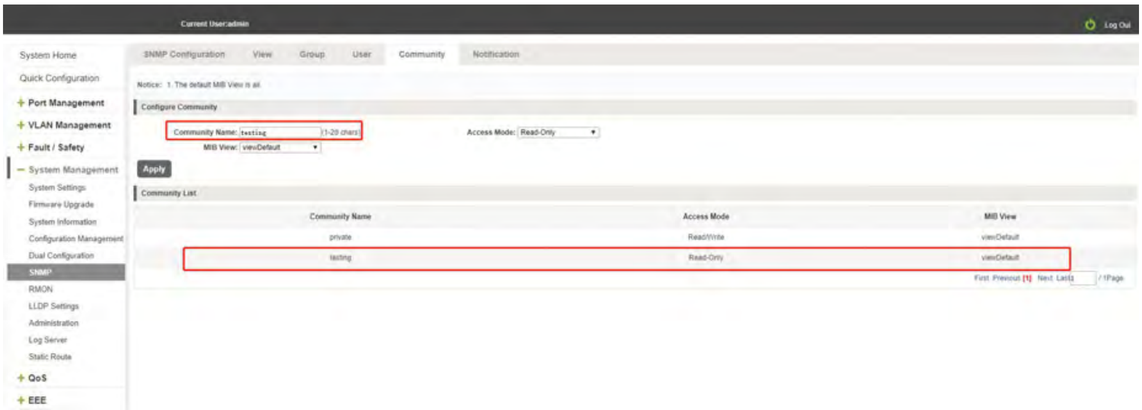
Access Mode: Read-Only

MIB View: viewDefault

Community List

Community Name	Access Mode	MIB View
private	Read/Write	viewDefault
testing	Read-Only	viewDefault

Figure 6-32: Increase community



Notice: 1. The default MIB View is all.

Configure Community

Community Name: testing (1-20 chars)

Access Mode: Read-Only

MIB View: viewDefault

Community List

Community Name	Access Mode	MIB View
private	Read/Write	viewDefault
testing	Read-Only	viewDefault

Figure 6-33: Community results

Change community configuration steps are as follows:

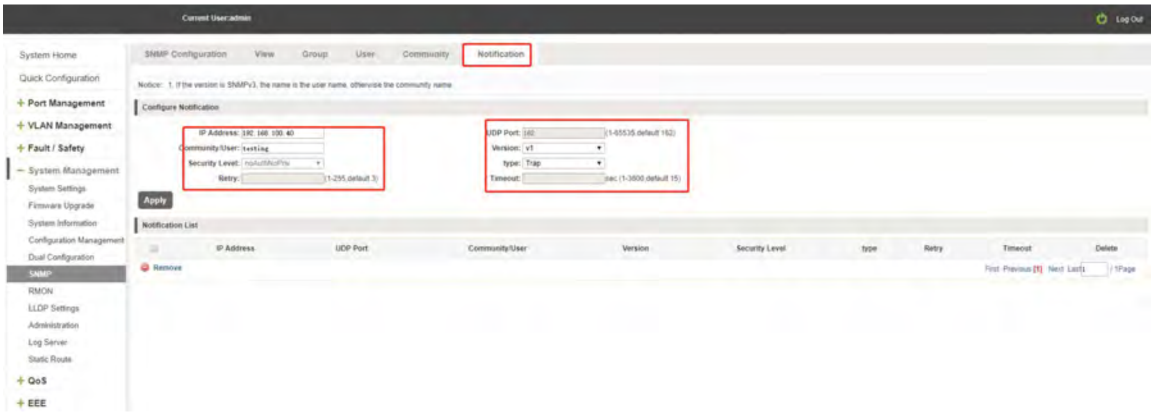
Step1:In the community name dialog box input:testing;

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:



Notice: 1. If the version is SNMPv3, the name is the user name, otherwise the community name

Configure Notification

IP Address: 192.168.100.40

Community/User: testing

Security Level: noAuthNoPriv

Retry: (1-255,default 3)

UDP Port: 162 (1-65535,default 162)

Version: v1

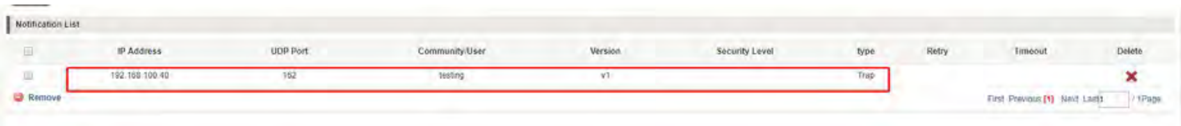
type: Trap

Timeout: sec (1-3600,default 15)

Notification List

□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete

Figure 6-34: Increases the SNMP TRAP service host



Notification List

□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete
□	192.168.100.40	162	testing	v1		Trap			✖

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;

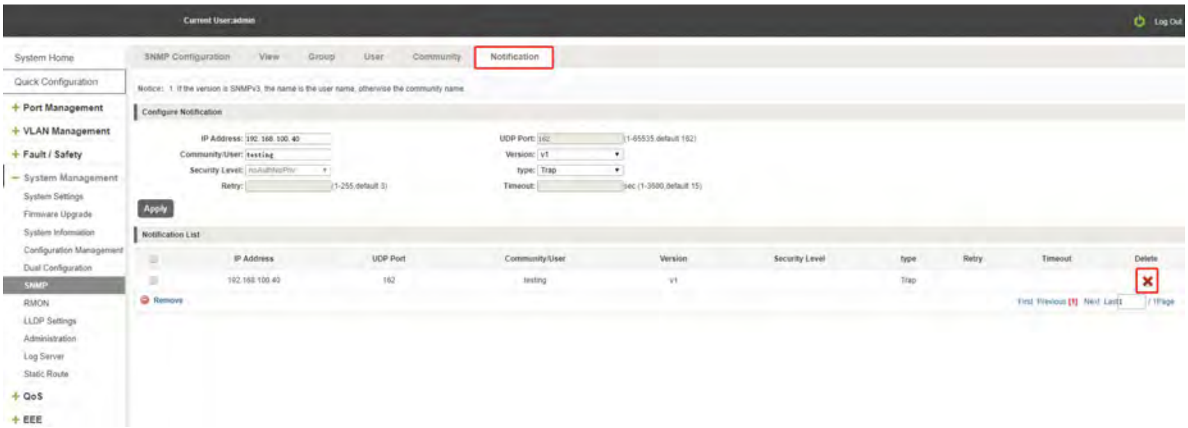
step3:Select the SNMP version: V1;

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:



Notice: 1. If the version is SNMPv3, the name is the user name, otherwise the community name

Configure Notification

IP Address: 192.168.100.40

Community/User: testing

Security Level: noAuthNoPriv

Retry: (1-255,default 3)

UDP Port: 162 (1-65535,default 162)

Version: v1

type: Trap

Timeout: sec (1-3600,default 15)

Notification List

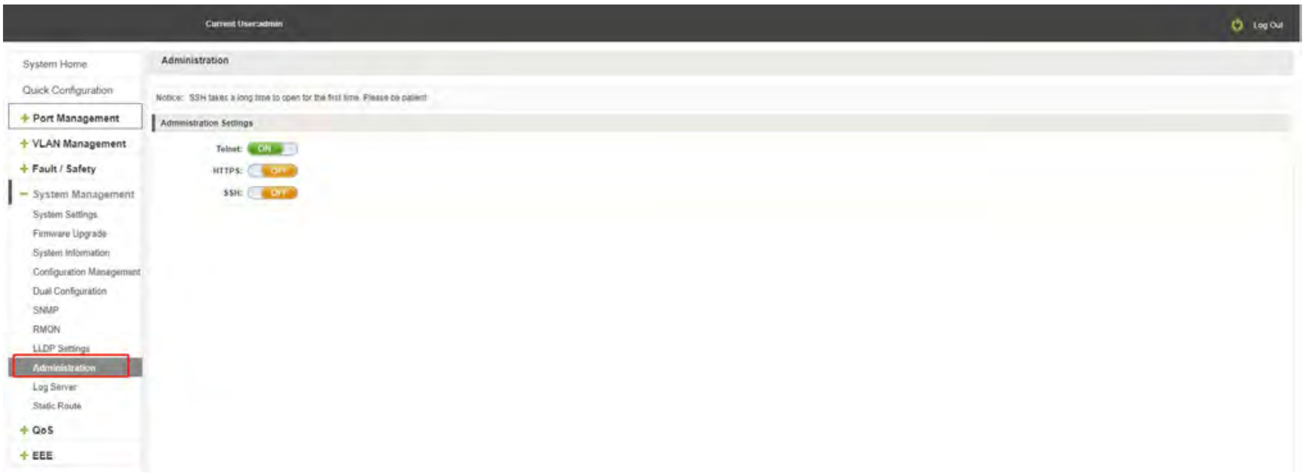
□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete
□	192.168.100.40	162	testing	v1		Trap			☒

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:



Notice: SSH takes a long time to open for the first time. Please be patient

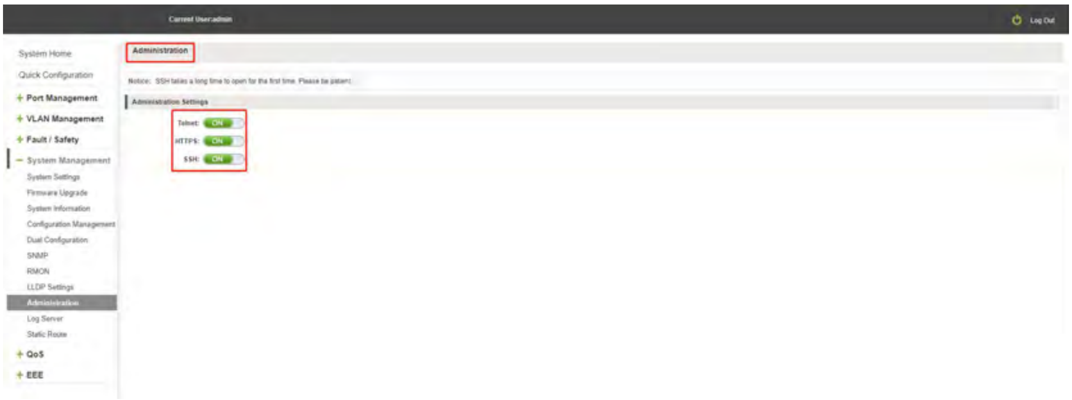
Administration Settings

Telnet: ON

HTTPS: OFF

SSH: OFF

Figure 6-37: View the Adminstration configuration information



Notice: SSH takes a long time to open for the first time. Please be patient

Administration Settings

Telnet: ON

HTTPS: ON

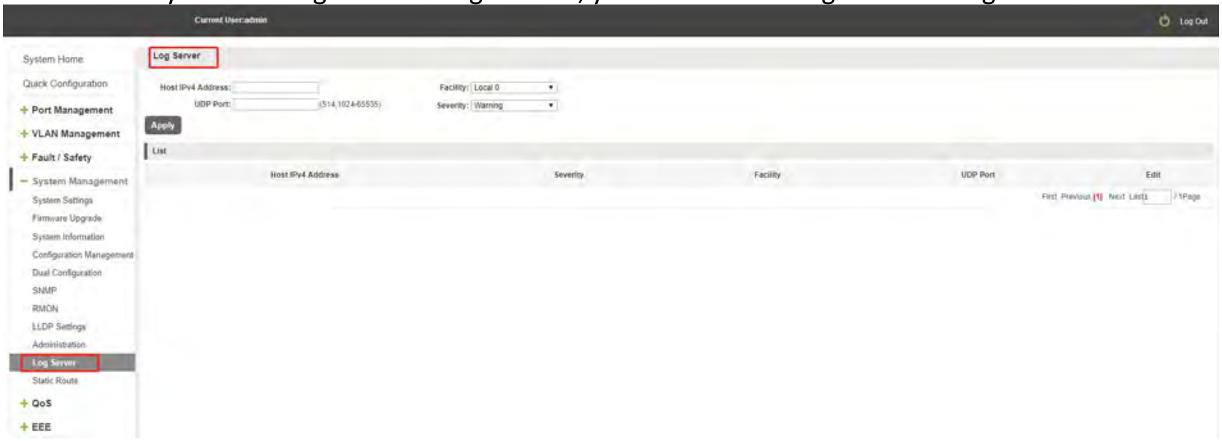
SSH: ON

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:



Host IPv4 Address:

UDP Port: (514,1024-65535)

Facility: Local 0

Severity: Warning

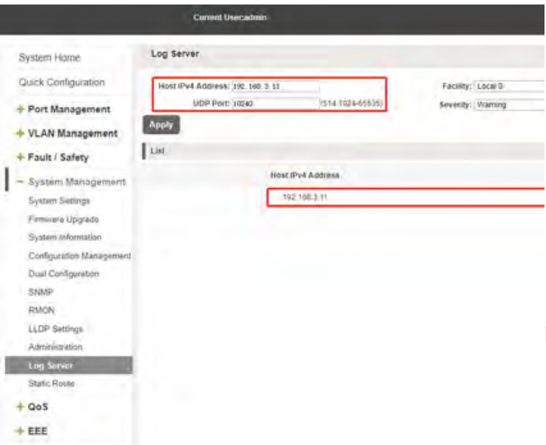
List

Host IPv4 Address	Severity	Facility	UDP Port	Edit

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:



Host IPv4 Address: 192. 168. 3. 11
UDP Port: 10240 (514 1024-65535)
Facility: Local 0
Severity: Warning

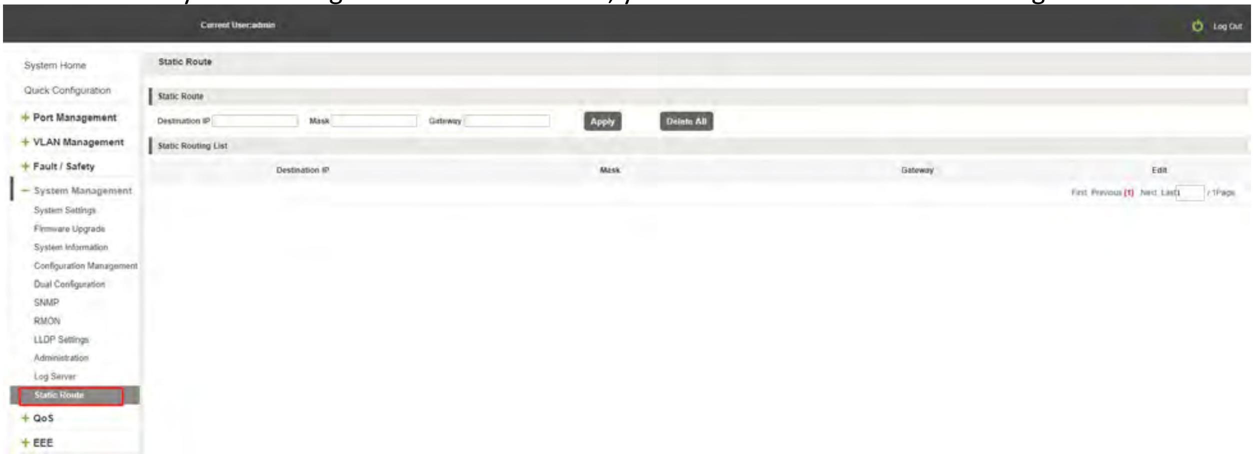
Host IPv4 Address
192.168.3.11

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:



Destination IP
Mask
Gateway

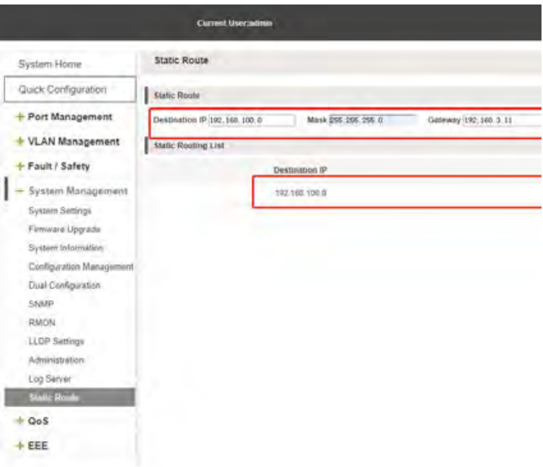
Destination IP	Mask	Gateway	Edit

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.



Destination IP 192. 168. 100. 0 Mask 255. 255. 255. 0 Gateway 192. 168. 3. 11

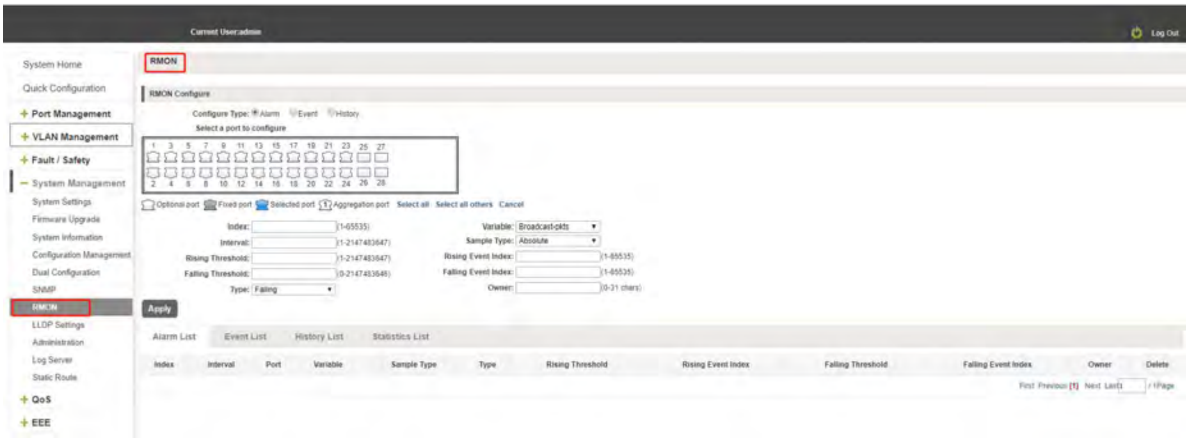
Destination IP
192.168.100.0

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.



Configure Type: ● Alarm ○ Event ○ History

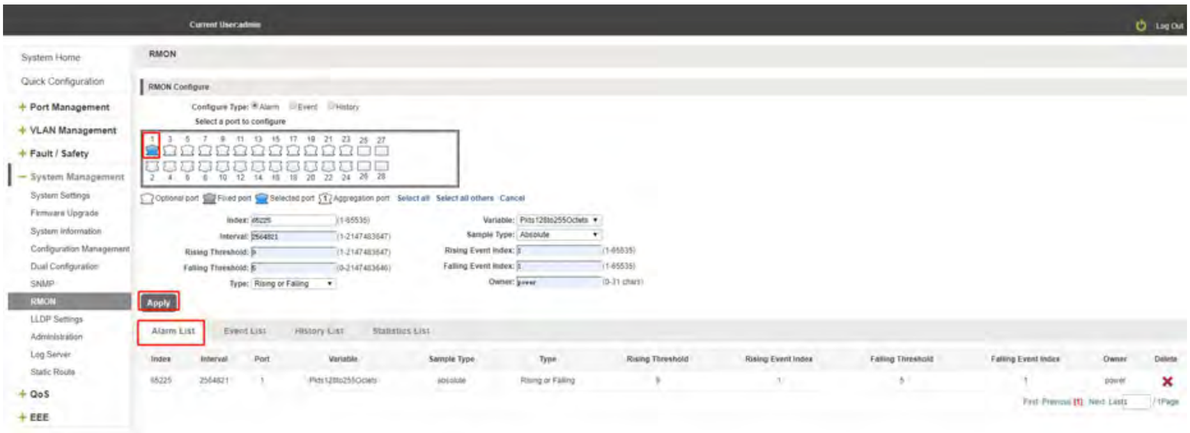
Index:		(1-65535)	Variable:	Broadcast-pkts	
Interval:		(1-2147483647)	Sample Type:	Absolute	
Rising Threshold:		(1-2147483647)	Rising Event Index:		(1-65535)
Falling Threshold:		(0-2147483646)	Falling Event Index:		(1-65535)
Type:	Falling		Owner:		(0-31 chars)

Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete

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.



Configure Type: ● Alarm ○ Event ○ History

Index:	65225	(1-65535)	Variable:	Pkts128to255Octets	
Interval:	2564821	(1-2147483647)	Sample Type:	Absolute	
Rising Threshold:	9	(1-2147483647)	Rising Event Index:	1	(1-65535)
Falling Threshold:	5	(0-2147483646)	Falling Event Index:	1	(1-65535)
Type:	Rising or Falling		Owner:	power	(0-31 chars)

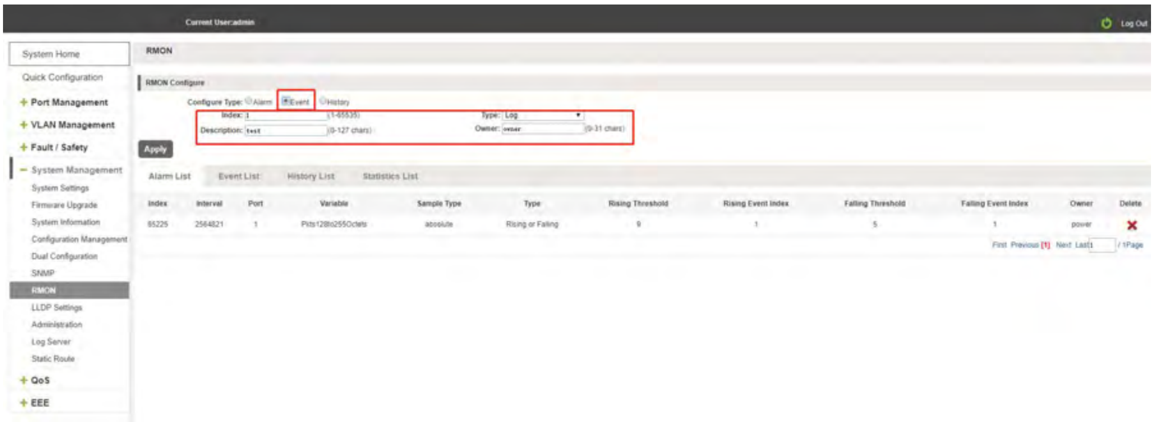
Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete
65225	2564821	1	Pkts128to255Octets	absolute	Rising or Falling	9	1	5	1	power	✕

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”.

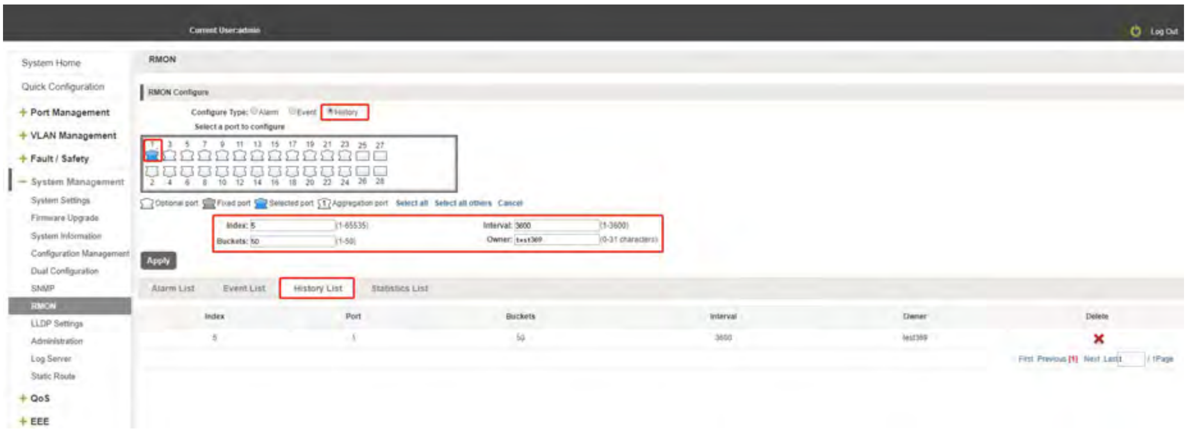


Configure Type: ○ Alarm ● Event ○ History

Index: 1 (1-65535)
Type: Log
Description: test (0-127 chars)
Owner: owner (0-31 chars)

Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete
65225	2564821	1	Pkts128to255Octets	absolute	Rising or Falling	9	1	5	1	power	✗

Figure 6-39: Change ROMN type is Event



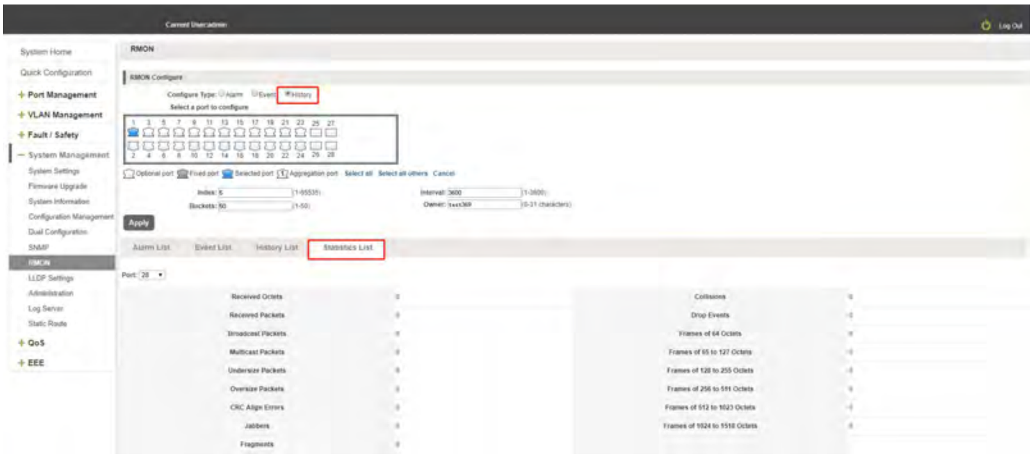
Configure Type: ○ Alarm ○ Event ● History

Index: 5 (1-65535)
Interval: 3600 (1-3600)
Buckets: 50 (1-50)
Owner: test369 (0-31 characters)

Index	Port	Buckets	Interval	Owner	Delete
5	1	50	3600	test369	✗

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 .



Configure Type: ○ Alarm ○ Event ● History

Select a port to configure

Index: 5 (1-65535)

Buckets: 50 (1-50)

Interval: 3600 (1-3600)

Owner: test369 (0-31 characters)

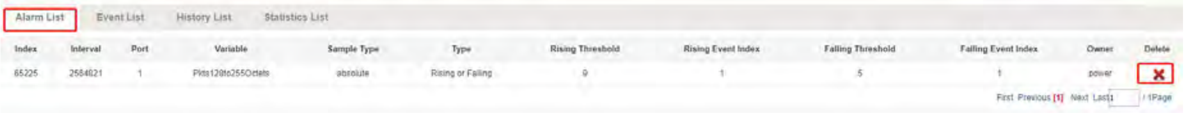
Port: 28

Received Octets	0	Collisions	0
Received Packets	0	Drop Events	0
Broadcast Packets	0	Frames of 64 Octets	0
Multicast Packets	0	Frames of 65 to 127 Octets	0
Undersize Packets	0	Frames of 128 to 255 Octets	0
Oversize Packets	0	Frames of 256 to 511 Octets	0
CRC Align Errors	0	Frames of 512 to 1023 Octets	0
Jabbers	0	Frames of 1024 to 1518 Octets	0
Fragments	0		

Figure 6-41: View the port configure information

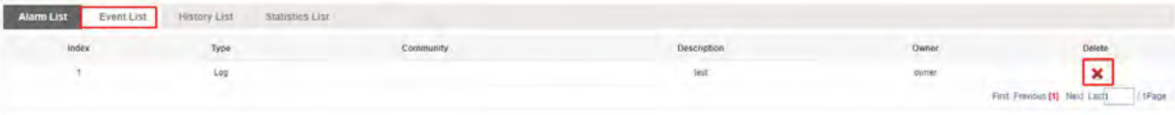
6.7.4 DELETE THE CONFIGURED RULE

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



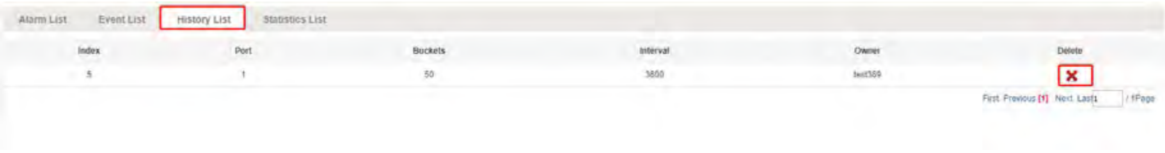
Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete
65225	2584021	1	Pkts128to255Octets	absolute	Rising or Falling	9	1	5	1	power	✗

Figure 6-42: Delete the Alarm list rule



Index	Type	Community	Description	Owner	Delete
1	Log		test	owner	✗

Figure 6-43: Delete the Event list rule



Index	Port	Buckets	Interval	Owner	Delete
5	1	50	3600	test369	✗

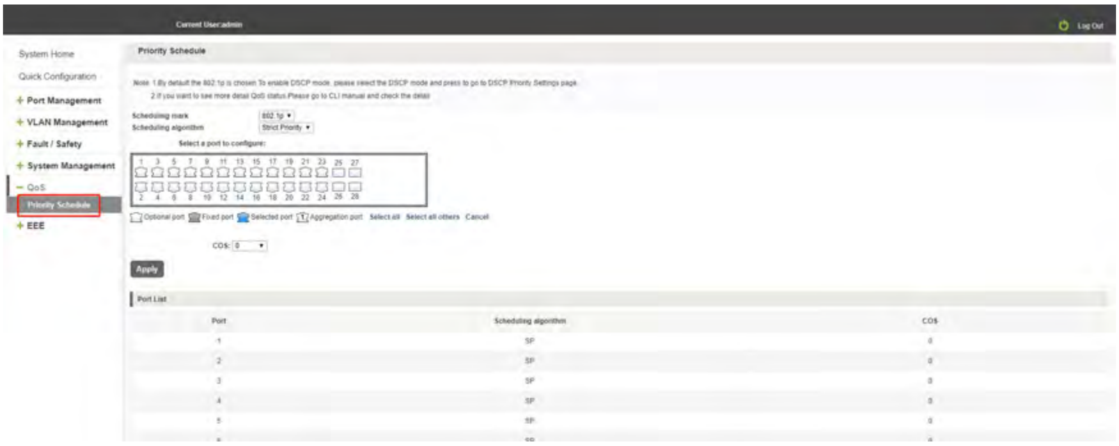
Figure 6-44: Delete the History list rule

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:



Priority Schedule

Note: 1.By default the 802.1p is chosen To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page
2.If you want to see more detail QoS status Please go to CLI manual and check the detail

Scheduling mark: 802.1p
Scheduling algorithm: Strict Priority

Select a port to configure:

COS: 0

Port List

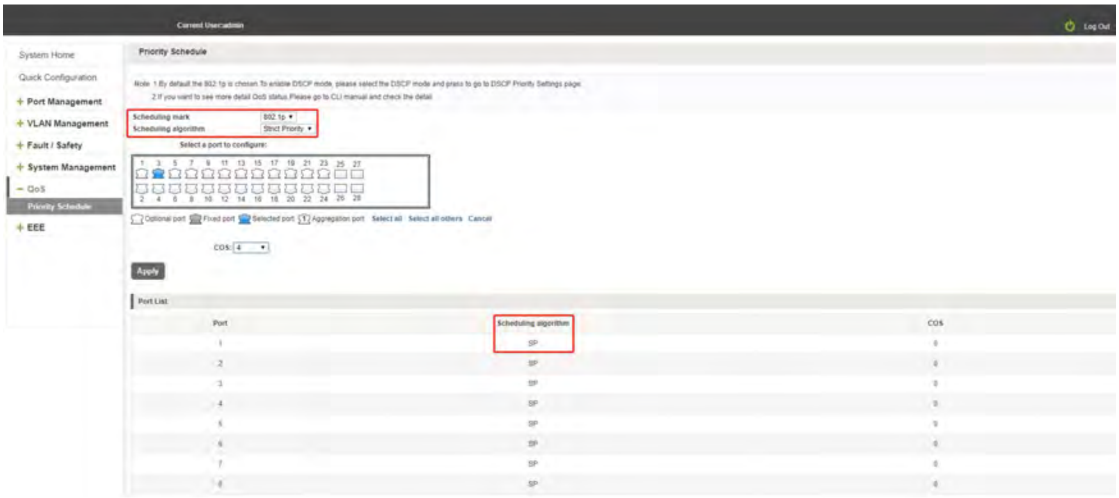
Port	Scheduling algorithm	COS
1	SP	0
2	SP	0
3	SP	0
4	SP	0
5	SP	0
6	SP	0

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.



Priority Schedule

Note: 1.By default the 802.1p is chosen To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page
2.If you want to see more detail QoS status Please go to CLI manual and check the detail

Scheduling mark: 802.1p
Scheduling algorithm: Strict Priority

Select a port to configure:

COS: 4

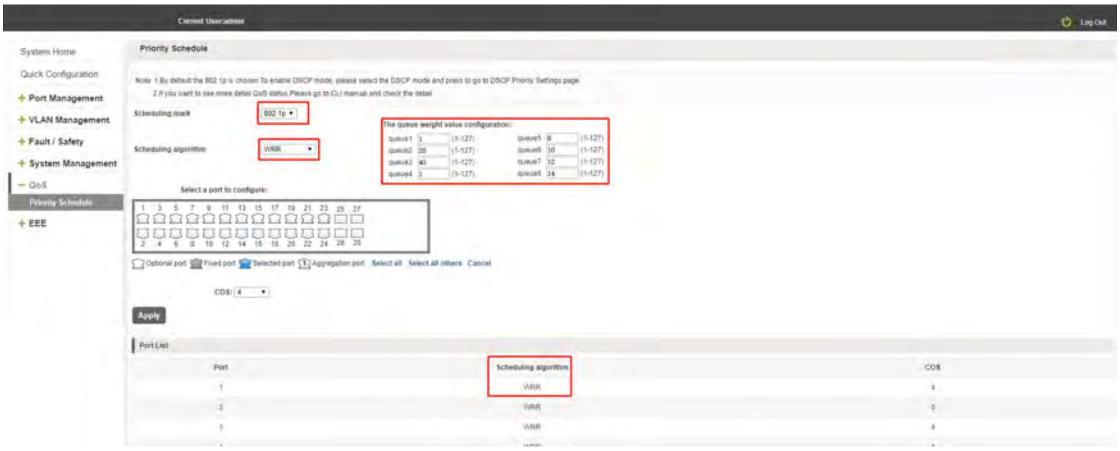
Port List

Port	Scheduling algorithm	COS
1	SP	0
2	SP	4
3	SP	0
4	SP	0
5	SP	0
6	SP	0
7	SP	0
8	SP	4

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.



Priority Schedule

Note: 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status.Please go to CLI manual and check the detail

Scheduling mark: 802.1p

Scheduling algorithm: WRR

The queue weight value configuration:

queue1	1	(1-127)	queue5	8	(1-127)
queue2	20	(1-127)	queue6	10	(1-127)
queue3	40	(1-127)	queue7	12	(1-127)
queue4	1	(1-127)	queue8	14	(1-127)

COS: 4

Port List

Port	Scheduling algorithm	COS
1	WRR	4
2	WRR	0
3	WRR	4

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

Priority schedule steps are as follows:

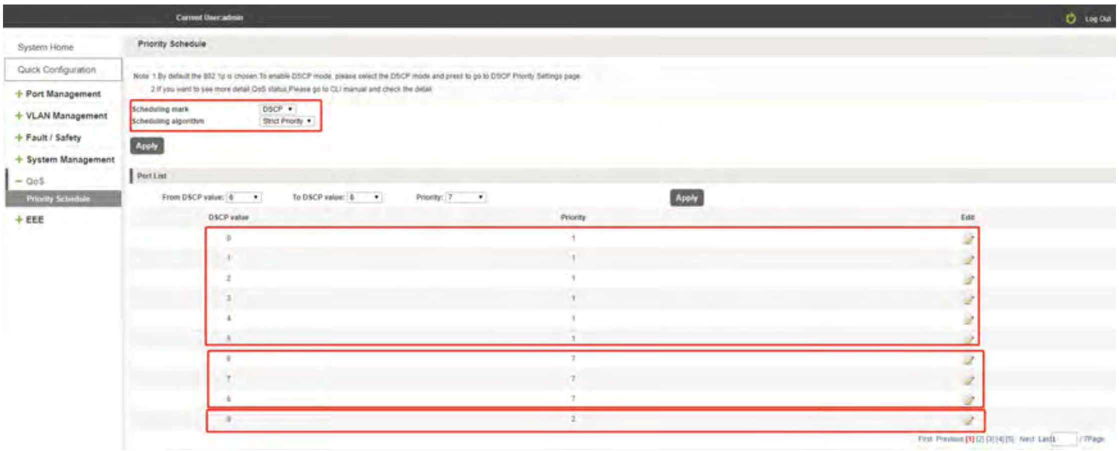
Step1: in scheduling mark , choose 802.1p;step2:in the Scheduling algorithm,choose WRR ,step3:in queue1 text box, enter the weight value ,such as 1;step4:in queue2 text box, enter the weight value ,such as 20;step5:in queue3 text box, enter the weight value ,such as 40;Step6:in queue4 text box, enter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



Priority Schedule

Note 1 By default the 802.1p is chosen To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page
2 If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP
Scheduling algorithm: Strict Priority

Port List

From DSCP value: 6 To DSCP value: 8 Priority: 7

DSCP value	Priority	Edit
0	1	✎
1	1	✎
2	1	✎
3	1	✎
4	1	✎
5	1	✎
6	7	✎
7	7	✎
8	7	✎
9	2	✎

First Previous [1] [2] [3] [4] [5] Next Last 1 /7Page

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 ;

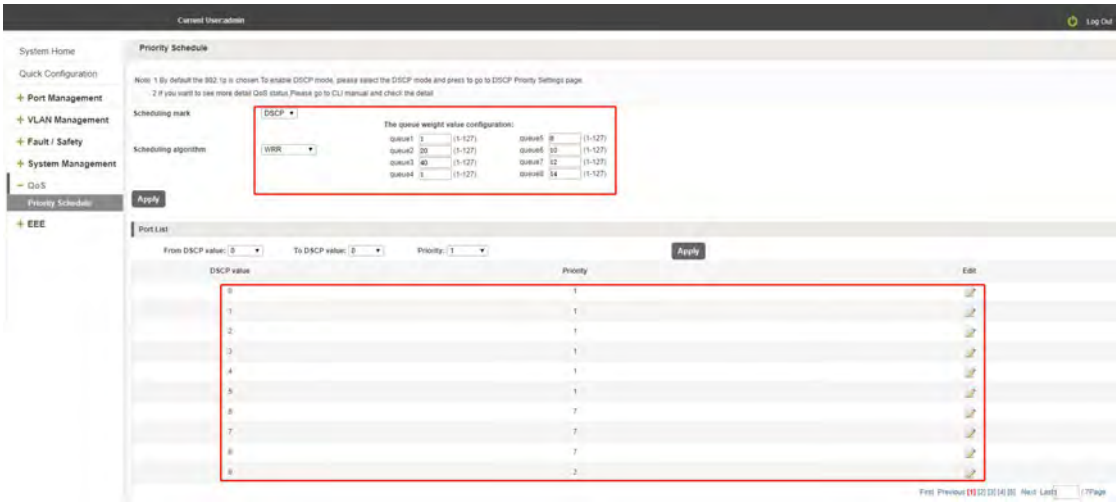
step4:in from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose medium;

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 .



Priority Schedule

Note: 1 By default the 802.1p is chosen To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page
2 If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP

Scheduling algorithm: WRR

The queue weight value configuration:

queue1	1	(1-127)	queue5	8	(1-127)
queue2	20	(1-127)	queue6	10	(1-127)
queue3	40	(1-127)	queue7	12	(1-127)
queue4	1	(1-127)	queue8	14	(1-127)

Apply

Port List

From DSCP value: 0 To DSCP value: 0 Priority: 1 Apply

DSCP value	Priority	Edit
0	1	✎
1	1	✎
2	1	✎
3	1	✎
4	1	✎
5	1	✎
6	7	✎
7	7	✎
8	7	✎
9	2	✎

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;

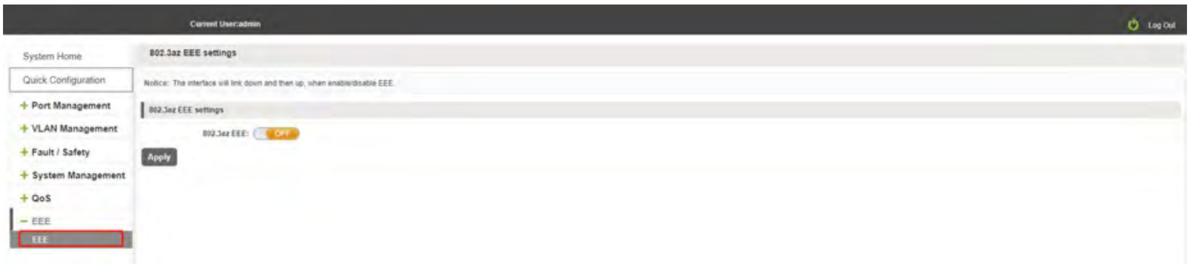
step3;click on the apply;

step 4:click OK.

8 EEE

8.1 EEE

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



802.3az EEE settings

Notice: The interface will link down and then up, when enable/disable EEE.

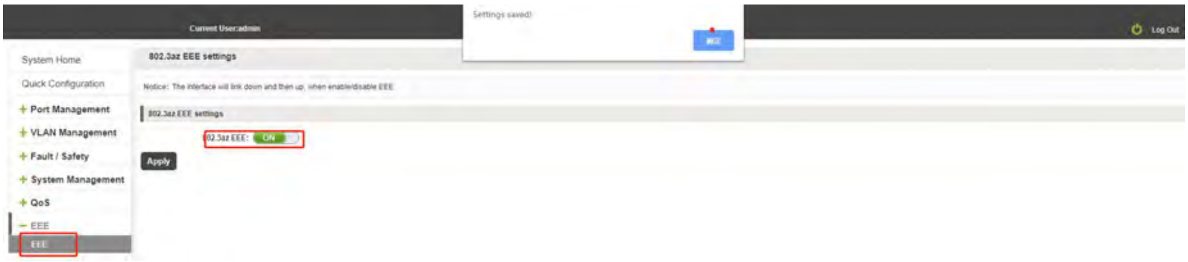
802.3az EEE settings

802.3az EEE: OFF

Figure 8-1 EEE information

8.2 ENABLE 802.3AZ EEE SETTINGS

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



Settings saved!

802.3az EEE settings

Notice: The interface will link down and then up, when enable/disable EEE

802.3az EEE settings

802.3az EEE: ON

Figure 8-2 Enable 802.3az EEE