



## Web Configuration Manual

## TABLE OF CONTENTS

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

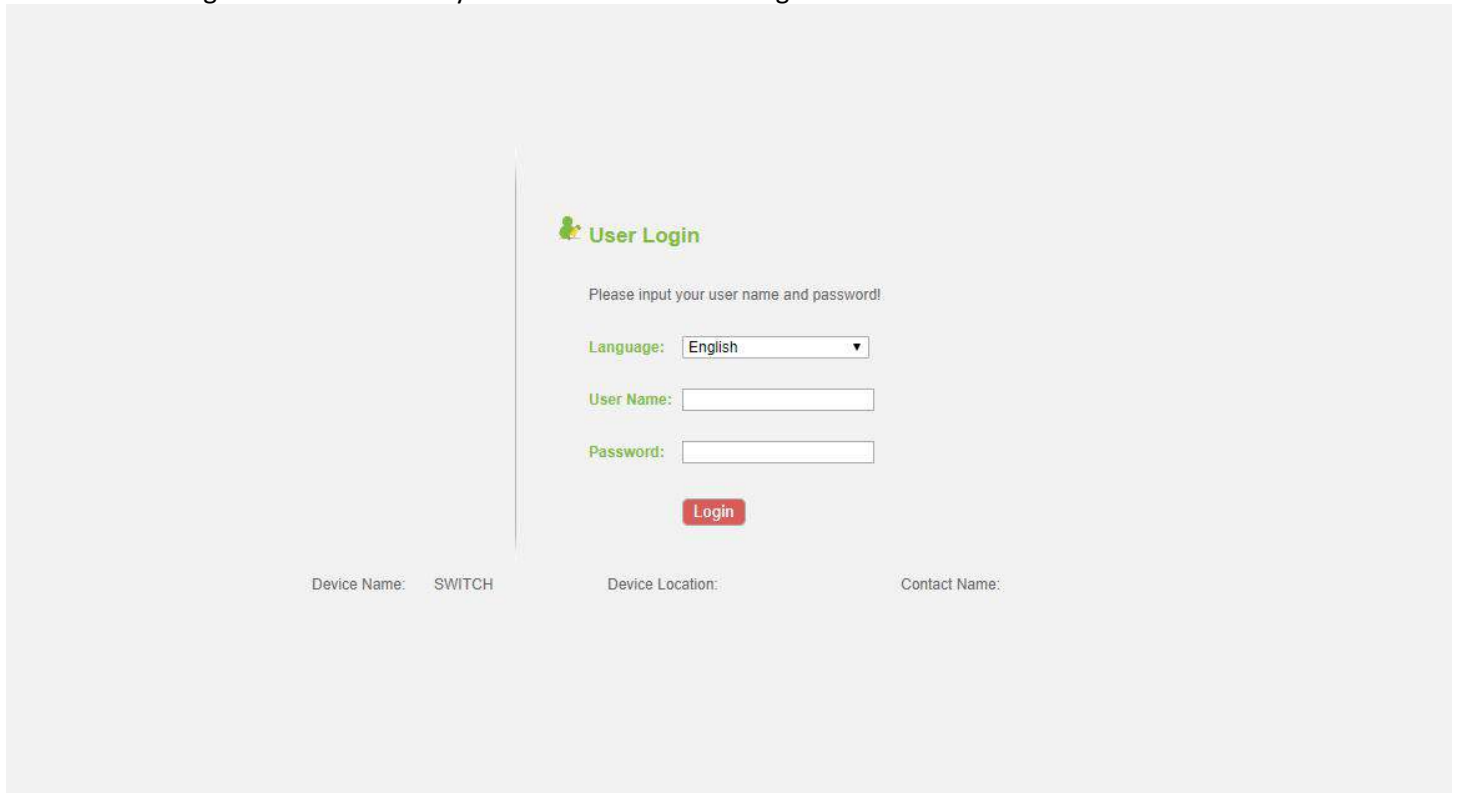
4.2 VOICE VLAN.....	27
4.2.1 VIEW THE VOICE VLAN CONFIGURATION.....	27
4.2.2 ENABLE THE VOICE VLAN.....	27
4.2.3 CONFIGURE THE VOICE VLAN PORT.....	28
4.2.4 VOICE VLAN OUI TABLE.....	29
4.2.5 view the voice vlan device.....	30
4.3 SURVEILLANCE VLAN.....	30
4.3.1 VIEW THE surveillance VLAN CONFIGURATION.....	30
4.3.2 configure surveillance VLAN.....	31
4.3.3 MAC Settings and Surveillance Device.....	32
4.3.4 PROT SURVEILLANCE VLAN.....	32
4.3.5 ATUO SURVEILLANCE VLAN SUMMARY.....	34
<b>5 FAULT / SAFETY.....</b>	<b>42</b>
5.1 ATTACK PREVENTION.....	42
5.1.1 ARP INSPECTION.....	42
5.1.1.1 VIEW ARP CONFIGURATION.....	42
5.1.1.2 ARP INSPECTION FUNCTION.....	43
5.1.1.3 DISABLE ARP INSPECTION CHEAT FUNCTION.....	43
5.1.1.4 TO MODIFY THE PORT ATTRIBUTE.....	44
5.1.2 port security.....	45
5.1.2.1 CONFIGURATION PORT SECURITY.....	45
5.1.2.2 MODIFY CONFIGURATION.....	45
5.1.3 anti DHCP attack.....	45
5.1.3.1 VIEW ANTI DHCP ATTACK CONFIGURATION.....	45
5.1.3.2 OPEN ANTO DHCP ATTACK FUNCTION.....	46
5.1.3.3 SETSTHE PORT TO DHCP NON TRUSED PORT.....	46
5.1.3.4 Off ANTI DHCP ATTACK FUNCTION.....	47
5.2 PATH DETECTION.....	48
5.2.1 path Detection.....	48
5.2.2 Tracert Detection.....	48

5.2.3 Cable Detection.....	49
5.3 DDOS PROTECTION.....	50
5.4 LOOPBACK DETECTION.....	51
5.4.1 ENABLE LOOPBACK DETECTION.....	51
5.4.2 choose the port to configure.....	51

## 1 WEB MANAGEMENT LANDING PAGE

### 1.1 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB

Configuration computer's IP address and the switch must be set to the same subnet (switch default IP address is 192.168.1.1, the default subnet mask of 255.255.255.0). Run WEB browser, in the address bar enter http://192.168.1.1 Enter, enter the 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:

Login

Device Name: SWITCH      Device Location:      Contact Name:

Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:

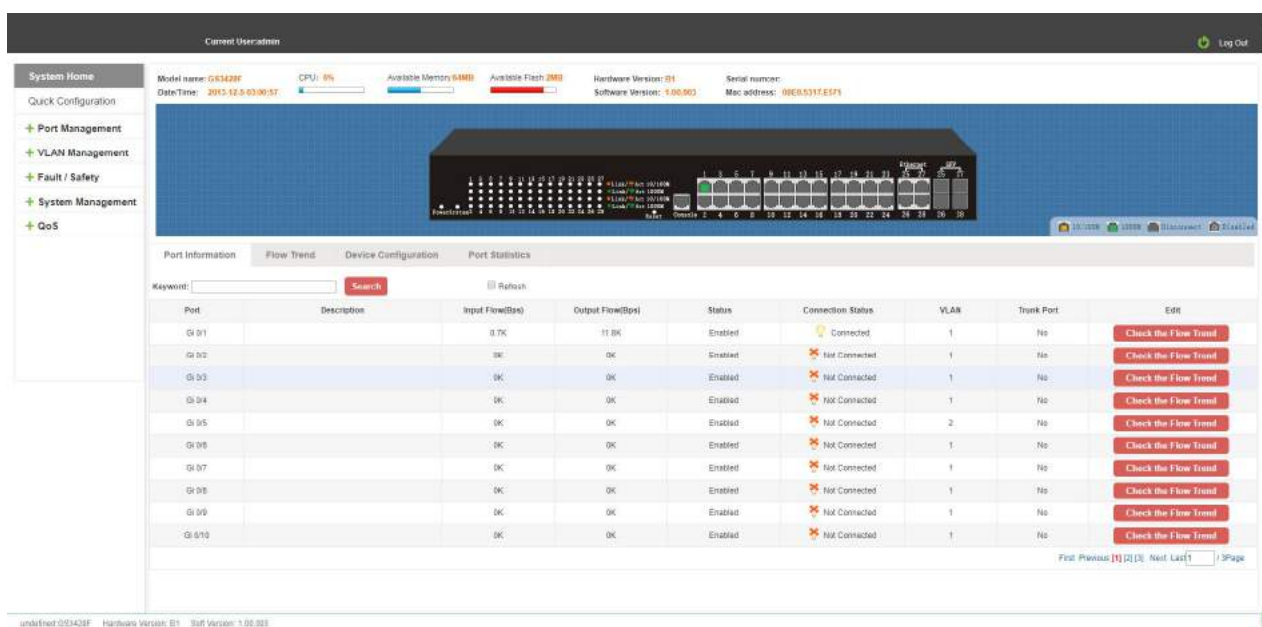


Figure 1-2: switch WEB management page Home

## 2 QUICK CONFIGURATION

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

### 2.1 VLAN SETTING

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



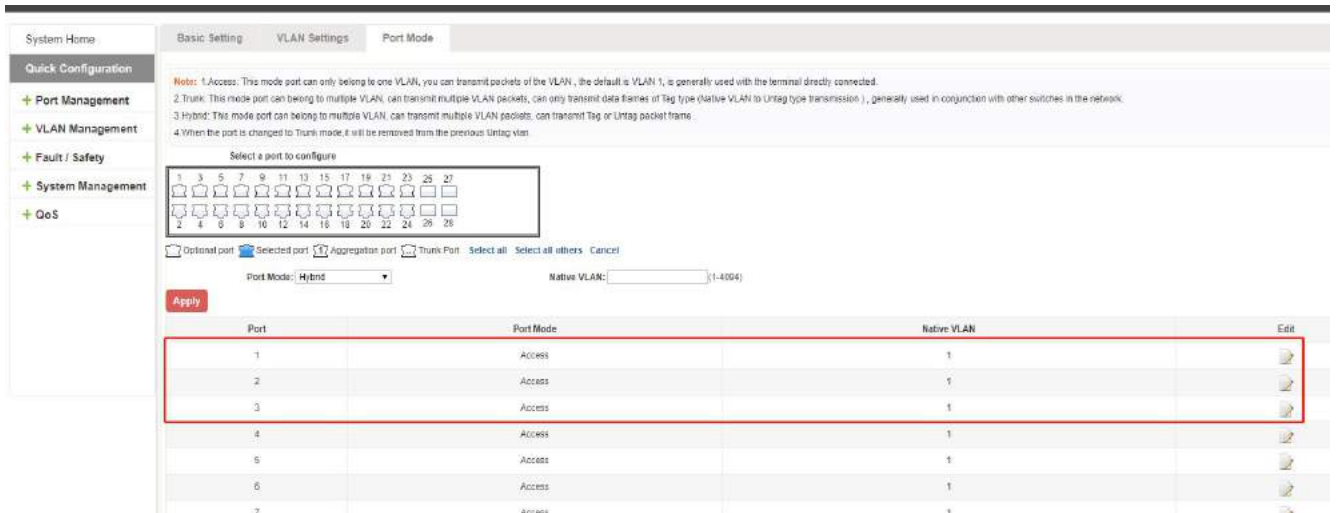
Figure 2-1: VLAN Setting

## 2.2 MODE

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

Notice:

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



System Home Basic Setting VLAN Settings Port Mode

Quick Configuration

Port Management

VLAN Management

Fault / Safety

System Management

QoS

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

Optional port Selected port Aggregation port Trunk Port Select all Select all others Cancel

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	

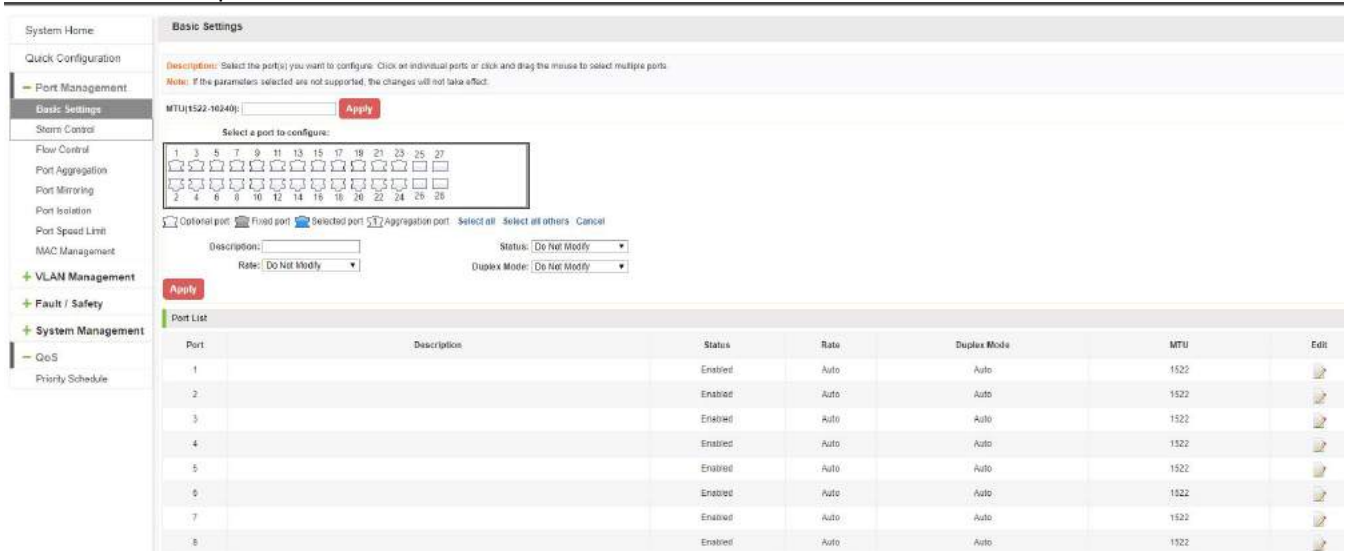
Figure 2-2: Port mode Setting

## 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:



**Basic Settings**

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):

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

☐ Optional port ☐ Fixed port ☒ Selected port ☐ Aggregation port

Description:  Status:

Rate:  Duplex Mode:

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	

**Figure 3-1: Port list information**

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

- 1.Port: The number of the port;
- 2.Port Description: Displays the contents of the switch port description;
- 3.Port Status: switch port status information, on / off;
- 4.Port Rate: Displays the switch port speed configuration, auto-negotiation / 10/100/1000;
- 5.Working Mode: Displays the switch port configuration duplex, auto-negotiation / full / half duplex;
- 6.MTU: Indicates the port is the maximum length of the packet;



### 3.1.2 CONFIGURING PORT PROPERTIES

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

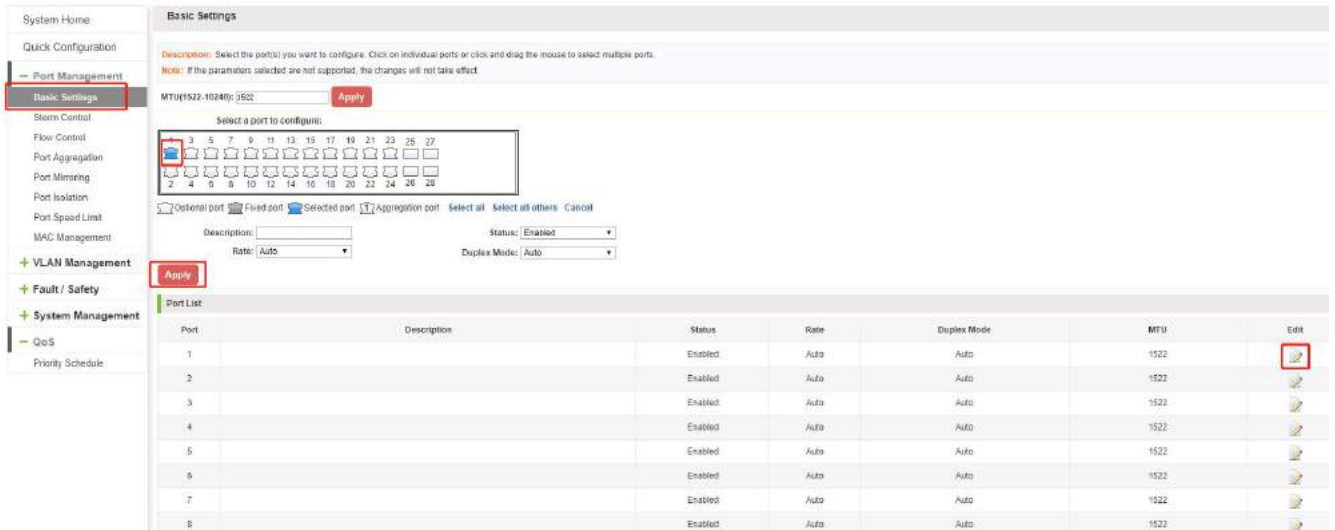



Figure 3-2: Port Properties configuration of FIG.

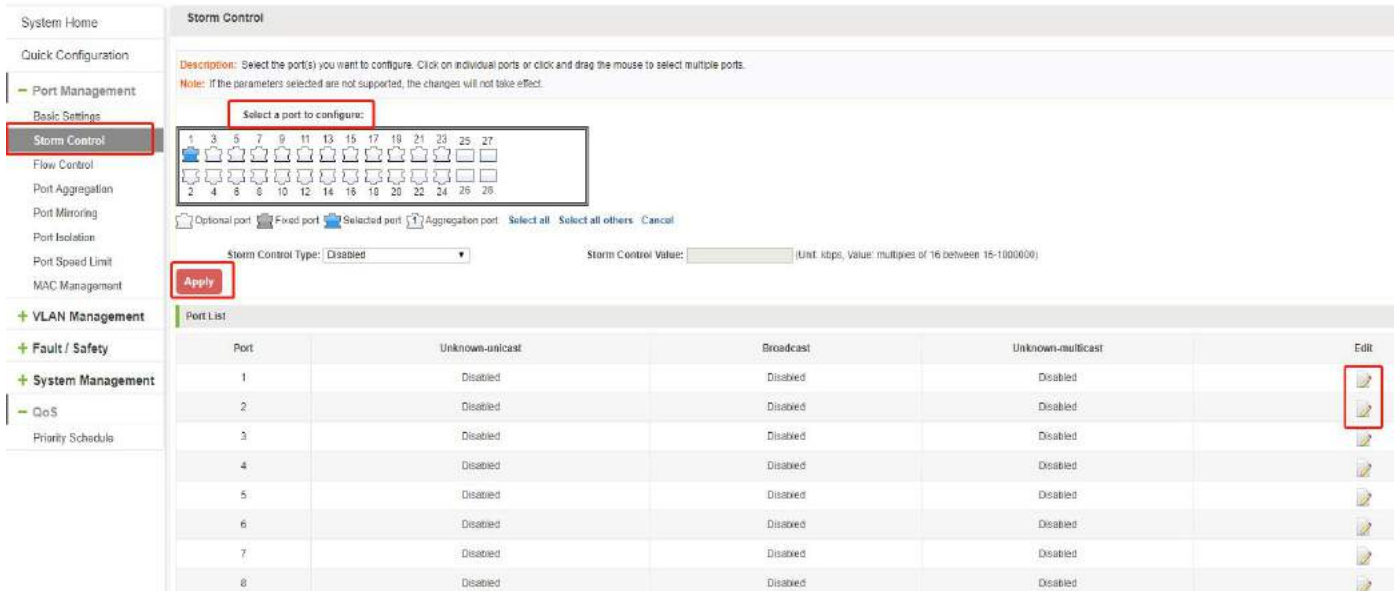
To configure port properties as follows:

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



**Storm Control Configuration Panel:**









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:

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

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

Apply

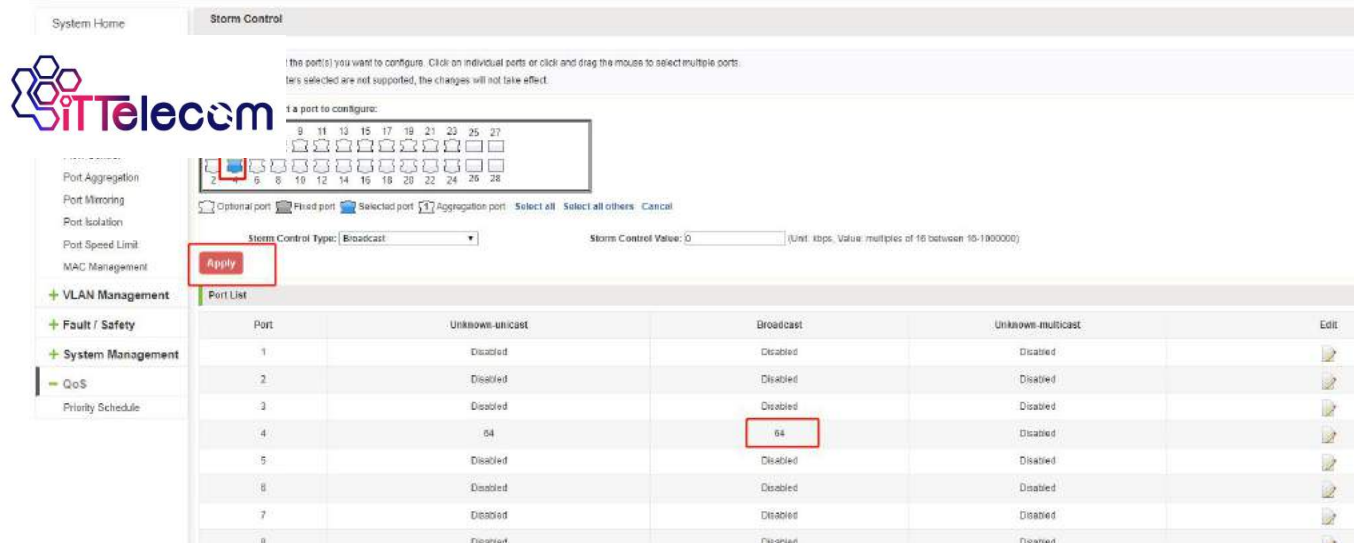
Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	
2	Disabled	Disabled	Disabled	
3	Disabled	Disabled	Disabled	
4	Disabled	Disabled	Disabled	
5	Disabled	Disabled	Disabled	
6	Disabled	Disabled	Disabled	
7	Disabled	Disabled	Disabled	
8	Disabled	Disabled	Disabled	

**Figure 3-3: Storm Control List information**

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

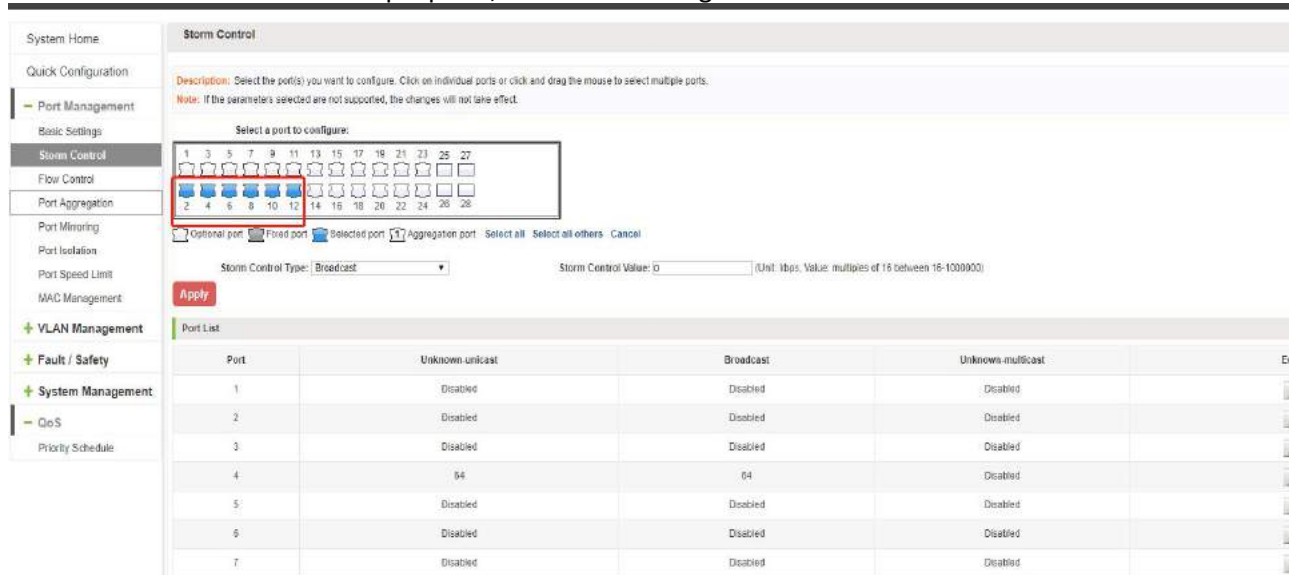
- 1.Port: The number of the port
- 2.Unicast: unknown unicast packets control
- 3.Broadcast: Broadcast packet control
- 4.Multicast: multicast packets control prompt
- 5.When set the control value is not a multiple of 64, the system automatically matches similar multiples of 64.
- 6.Control value unicast, broadcast, multicast, while only a single value for the control.

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



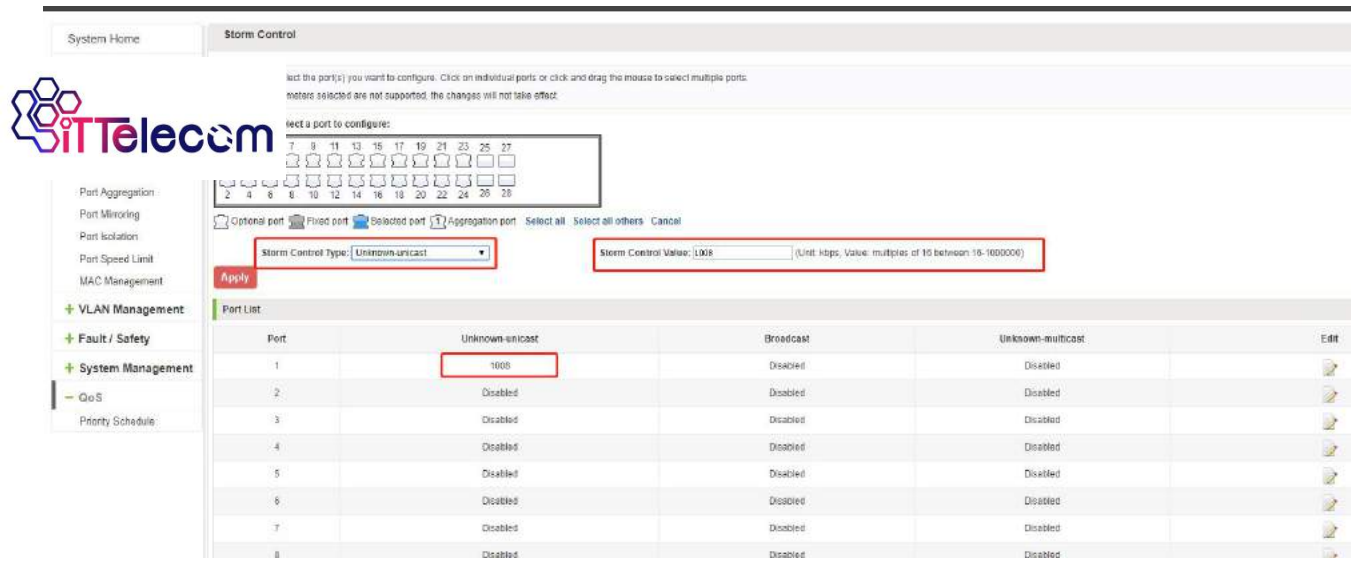
**Figure 3-4: Configuring Storm Control information**

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



**Figure 3-5: Bulk edit configuration information**

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



**Figure 3-6: Configuring Storm Control information**

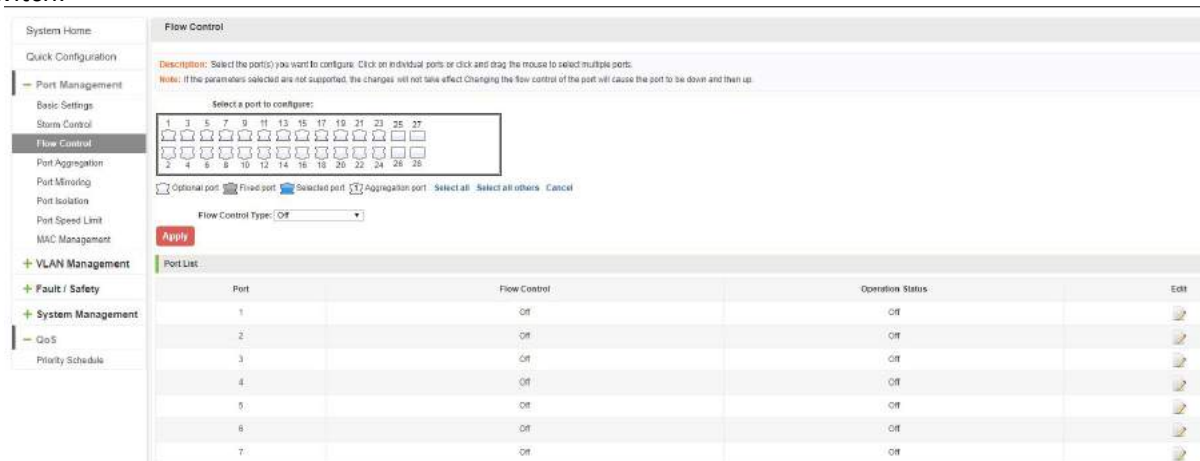
After the configuration, as shown below:

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	1000	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	

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

### 3.3 FLOW CONTROL

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



**Figure 3-8: Flow Control Information**

### 3.3.1 CONFIGURING FLOW CONTROL

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

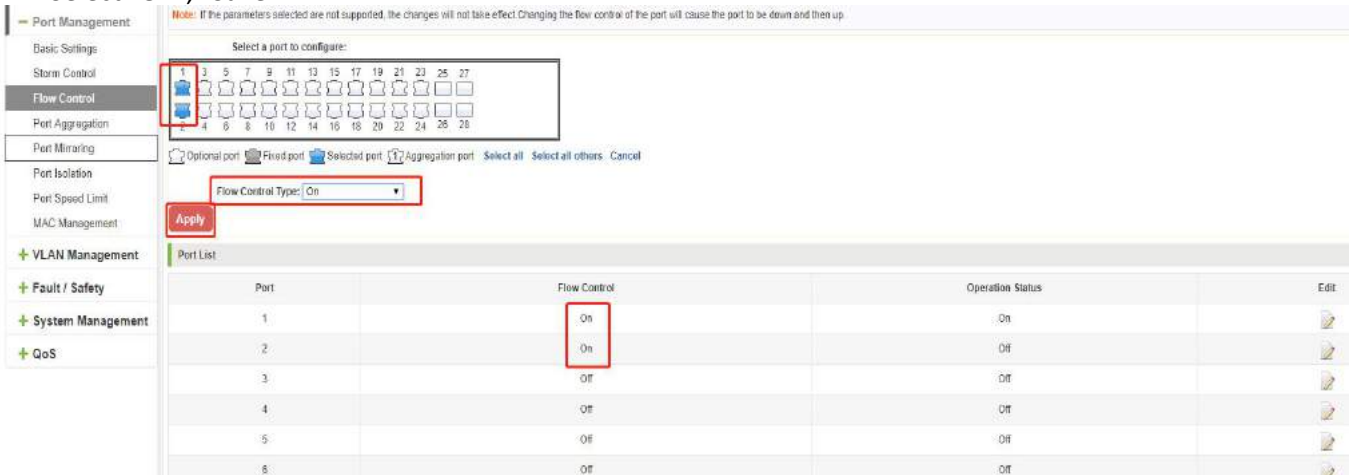


Figure 3-9: Open port flow control function

Open port traffic control, follow these steps:

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

View Configuration list to display configuration is successful:





Port List			
Port	Flow Control	Operation Status	Edit
1	On	On	
2	On	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	

Figure 3-10: Port flow control status

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

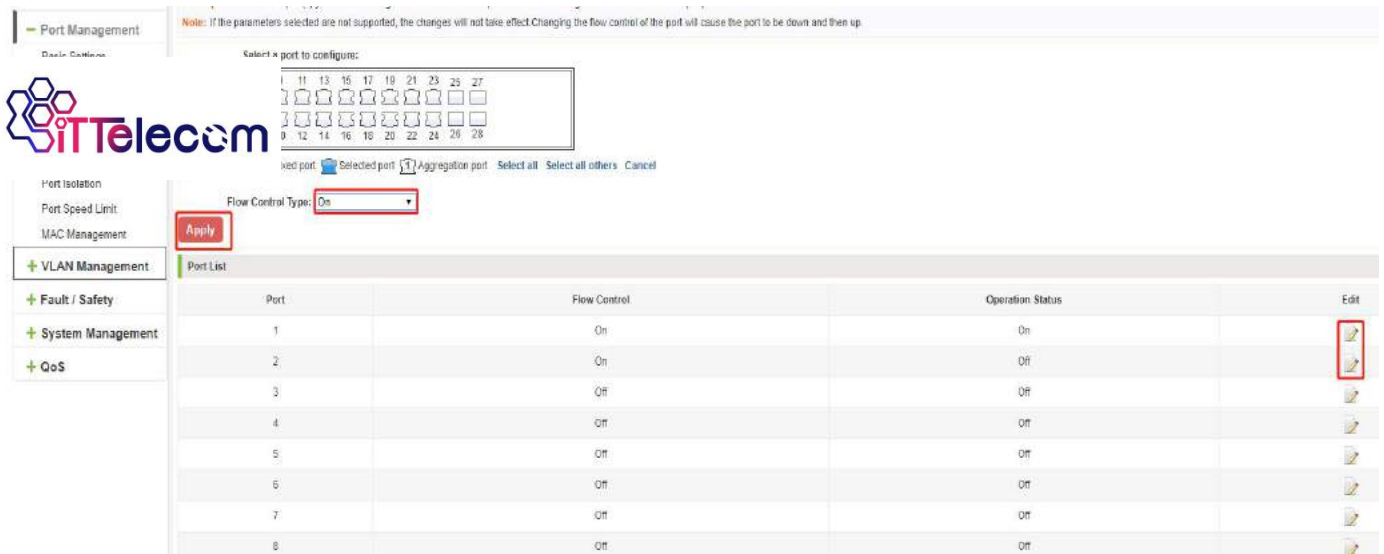


Figure 3-11: Close the port flow control

### 3.4 PORT AGGREGATION

#### 3.4.1 VIEWING PORT AGGREGATION CONFIGURATION

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

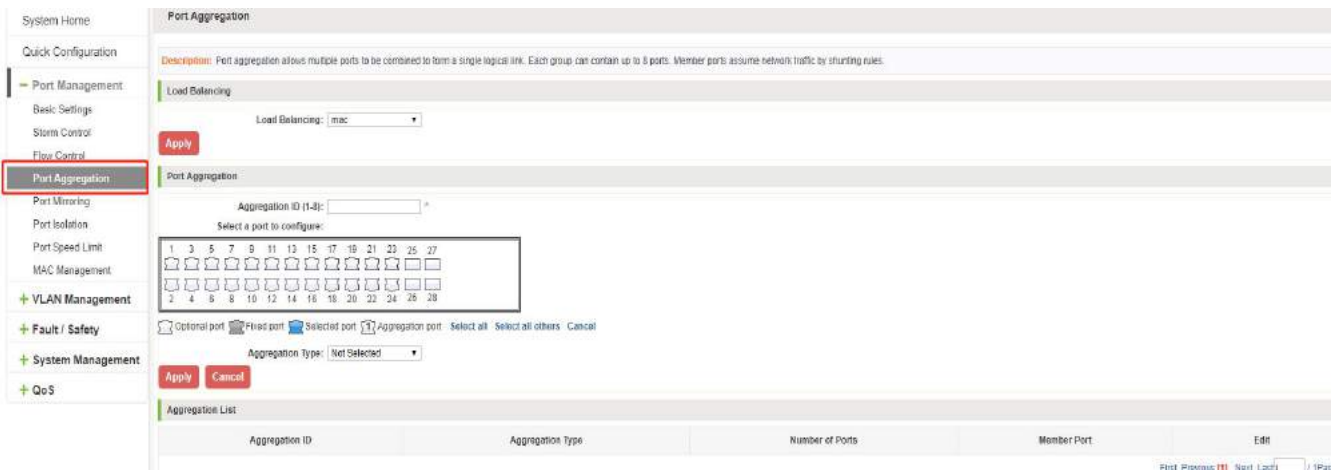


Figure 3-12: Aggregation port configuration information

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

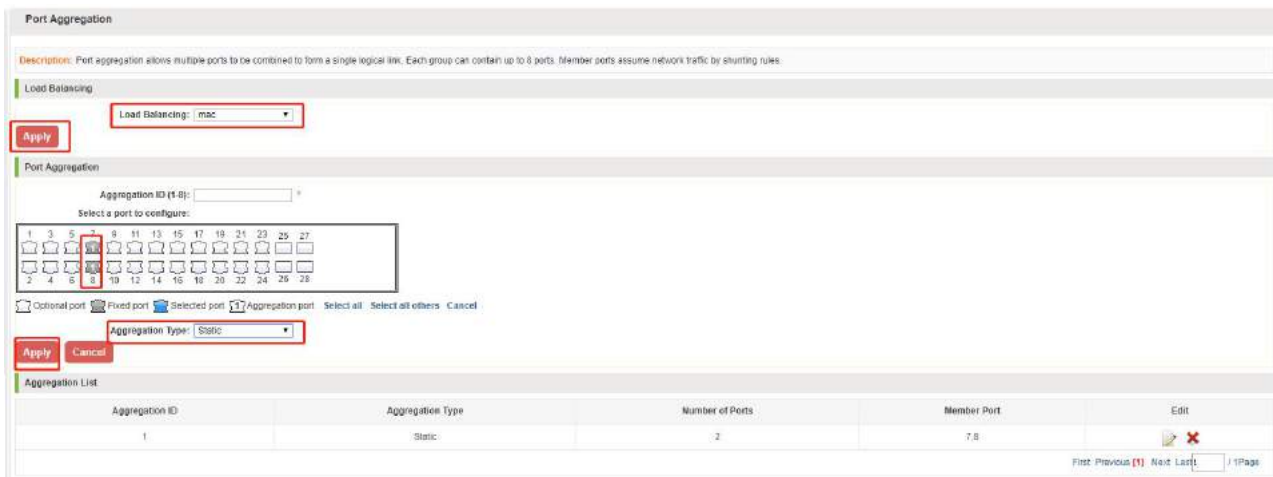
1. Aggregation number: display link aggregation group number value;
2. Load Balancing: Displays the current link aggregation group load balancing judgment condition;
3. Aggregate types: Displays whether to use a polymerization port LACP protocol;
4. Member ports quantity: Displays the number of ports in the link aggregation group contains a total of member port: Displays the current port link aggregation group member prompt

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

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

### 3.4.2 ADD PORT AGGREGATION

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



**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:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Aggregation Type: Static

**Aggregation List**

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Static	2	7.8	

First Previous 1 Next Last 1 / 1 Page

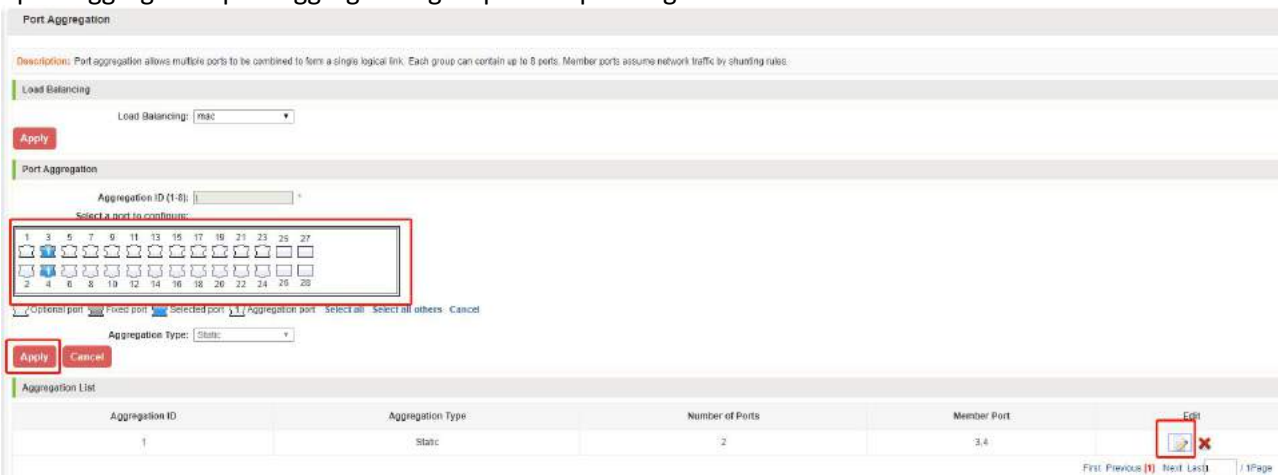
Figure 3-13: Port Aggregation Configuration area

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 "Save" 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:



**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:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Aggregation Type: Static

**Aggregation List**

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Static	2	3.4	

First Previous 1 Next Last 1 / 1 Page

**Figure 3-14: To modify the port aggregation**

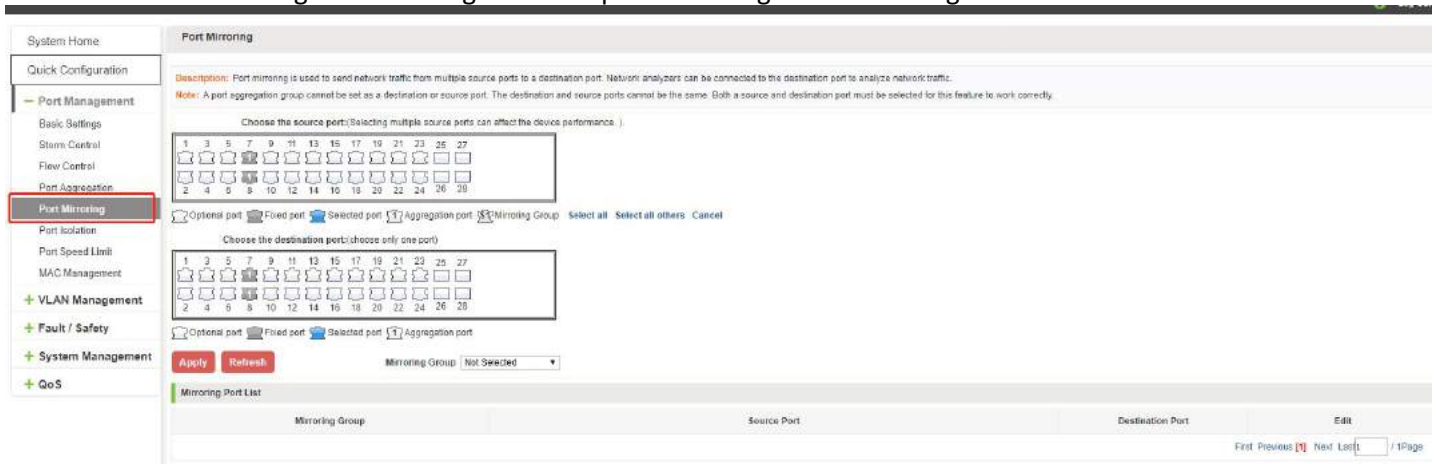
Modify Link Aggregation Procedure:

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 "Save" button to complete the configuration.

## 3.5 PORT MIRRORING

### 3.5.1 PORT MIRRORING CONFIGURATION

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



**Figure 3-15: Port mirroring configuration information**

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

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

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

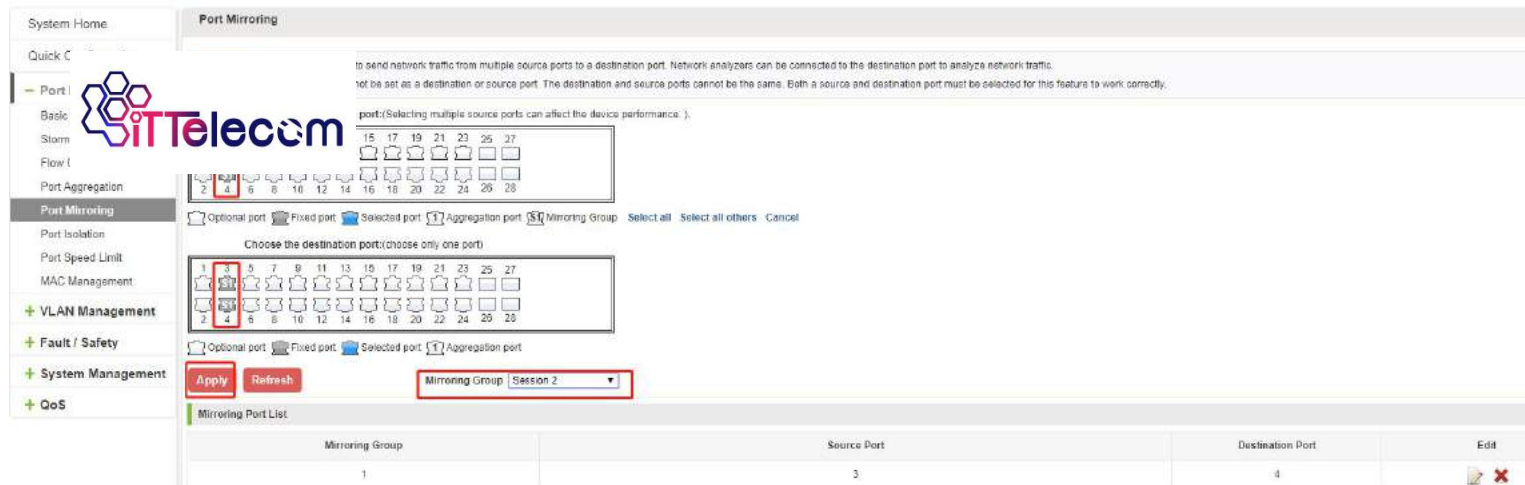
Destination port: mirror data sent to the destination port.

- 1.Port aggregation port can not be used as the destination port and source port;
- 2.Destination port and source port can not be the same;
- 3.Same group mirroring group can have only one destination port.

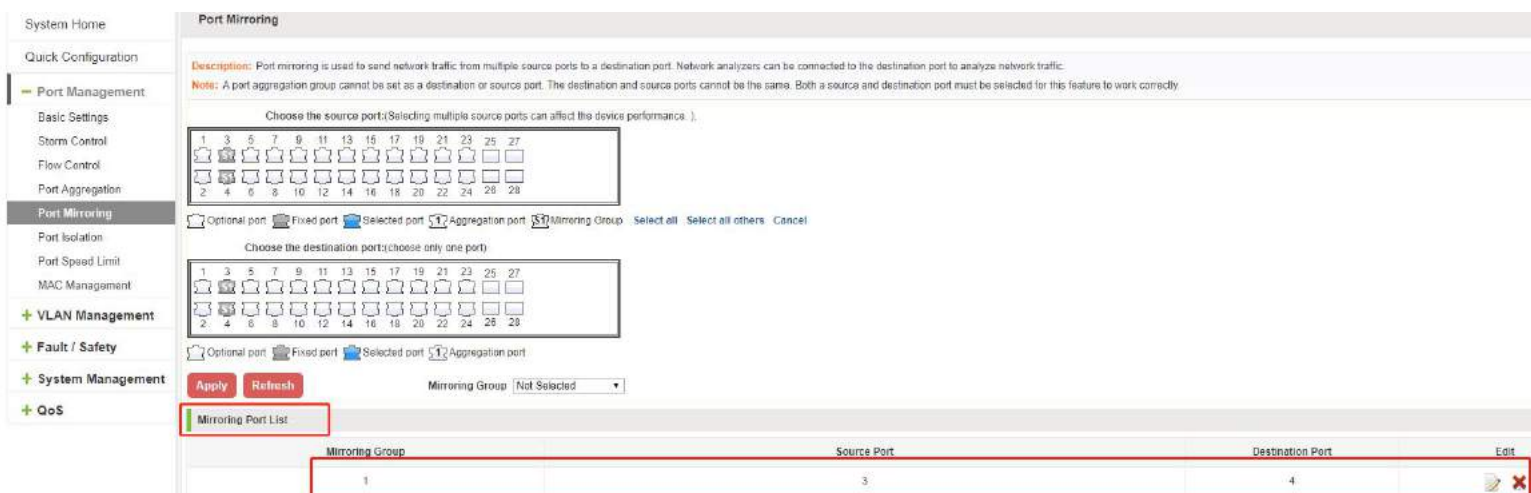
### 3.5.2 ADD PORT MIRRORING GROUP

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





**Figure 3-16: Add port mirroring group**



**Figure 3-17: Add port mirroring group results**

Port mirroring configuration steps are as follows:

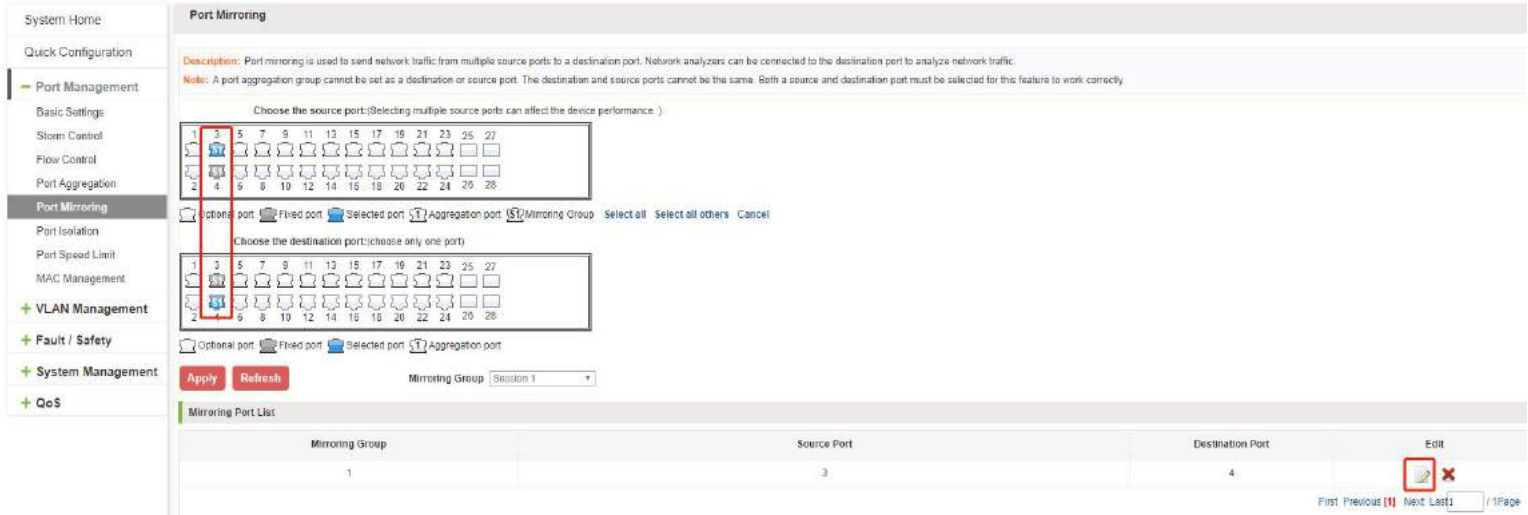
Step1:Select "Source Port",step2:Select "Destination Port",step3: select mirroring group ,step4,Click"Save".

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.



**Figure 3-18: To modify the port mirroring group**

**Figure 3-19: Modify successful port mirroring group**

Modify the port mirroring configuration steps are as follows:

- 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 "Save"

Quick (

Port

Basic

Storm

Flow Control

Port Aggregation

Port Mirroring

Port Isolation

Port Speed Limit

MAC Management

+ VLAN Management

+ Fault / Safety

+ System Management

+ QoS



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, or 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.

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

15

17

19

21

23

25

27

2

4

6

8

10

12

14

16

18

20

22

24

26

28

☐ Optional port ☒ Fixed port ☒ Selected port ☒ Aggregation port ☒ Mirroring Group [Select all](#) [Select all others](#) [Cancel](#)

Choose the destination port:(choose only one port!)

1

3

5

7

9

11

13

15

17

19

21

23

25

27

2

4

6

8

10

12

14

16

18

20

22

24

26

28

☐ Optional port ☒ Fixed port ☒ Selected port ☒ Aggregation port

[Apply](#) [Refresh](#)

Mirroring Group Session 2

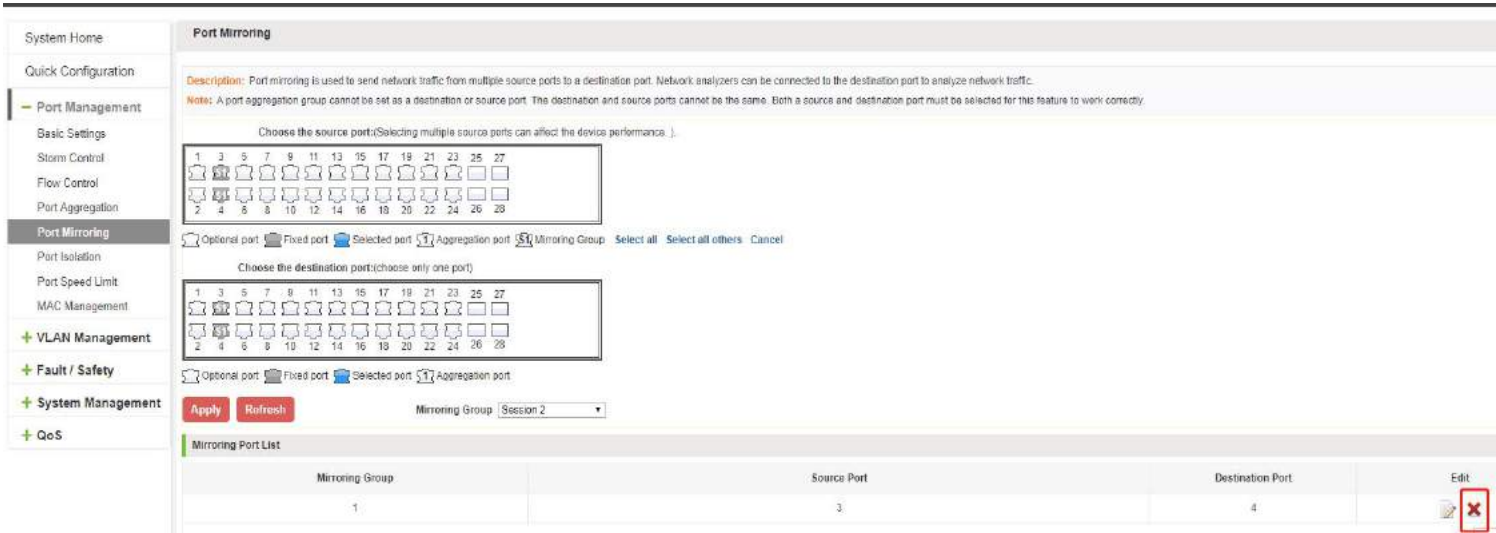
Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	3	4	

First Previous **1** Next Last

### 3.5.4 DELETE A PORT MIRRORING GROUP

Remove some ports from multiple source ports and save them.



**Figure 3-20: Delete a port mirroring group**

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

**Figure 3-21: Delete port mirroring group**

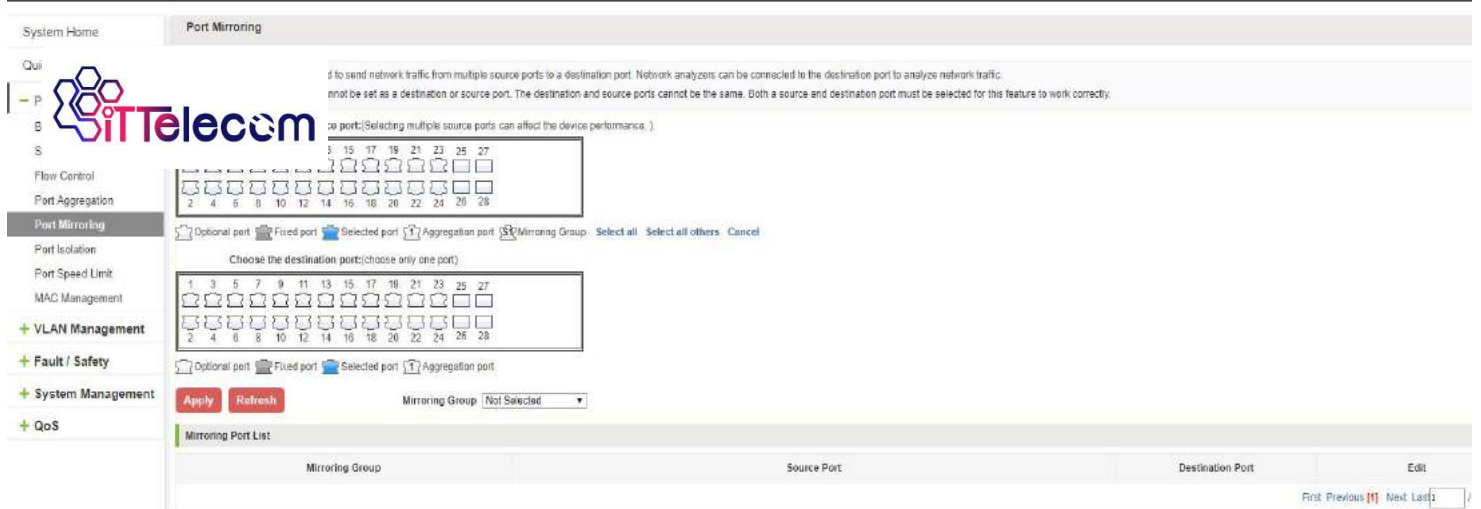


Figure 3-22: Deleted successfully port mirroring

Remove port mirroring configuration steps are as follows:

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

## 3.6 PORT ISOLATION

### 3.6.1 VIEW PROT ISOLATION

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

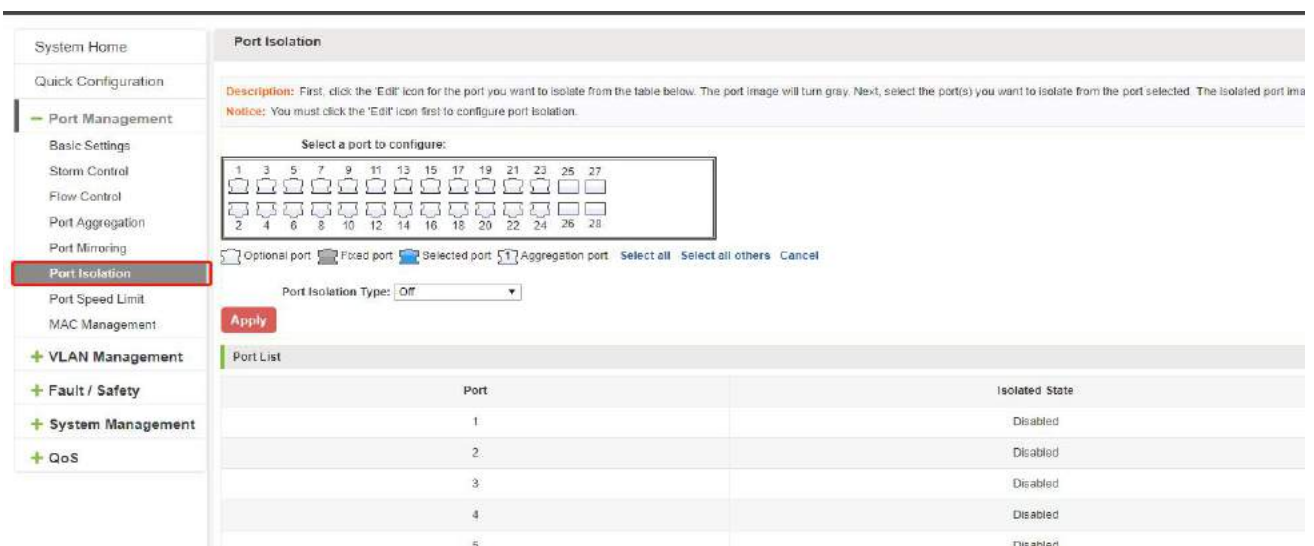


Figure 3-23: View the port isolation

### 3.6.2 CONFIGURE THE PROT ISOLATION

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

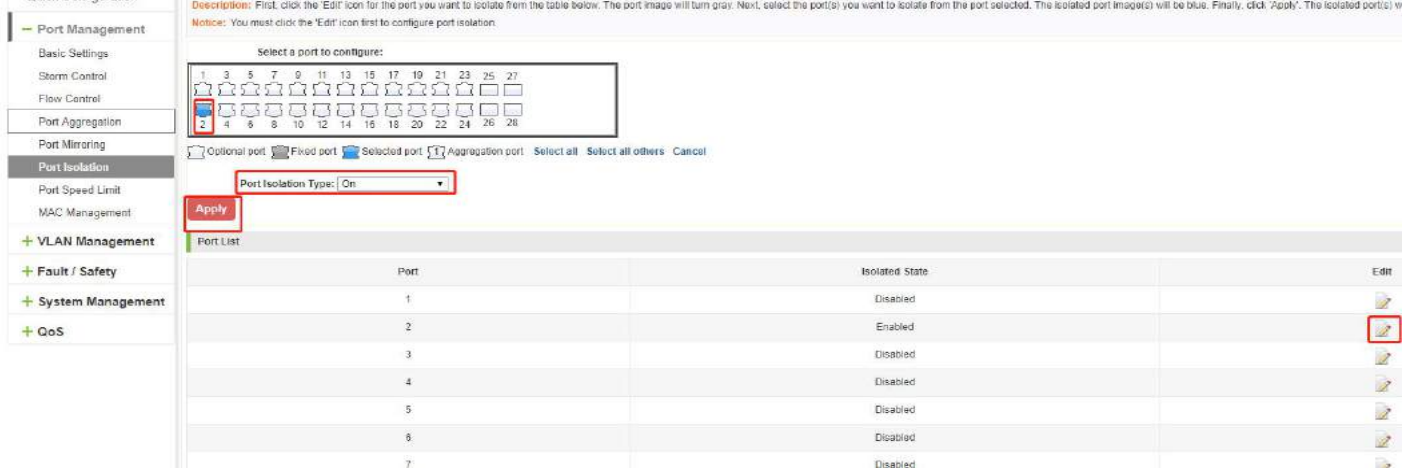


Figure 3-24: Configure the port isolation

### 3.6.3 EDIT THE PORT ISOLATION

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

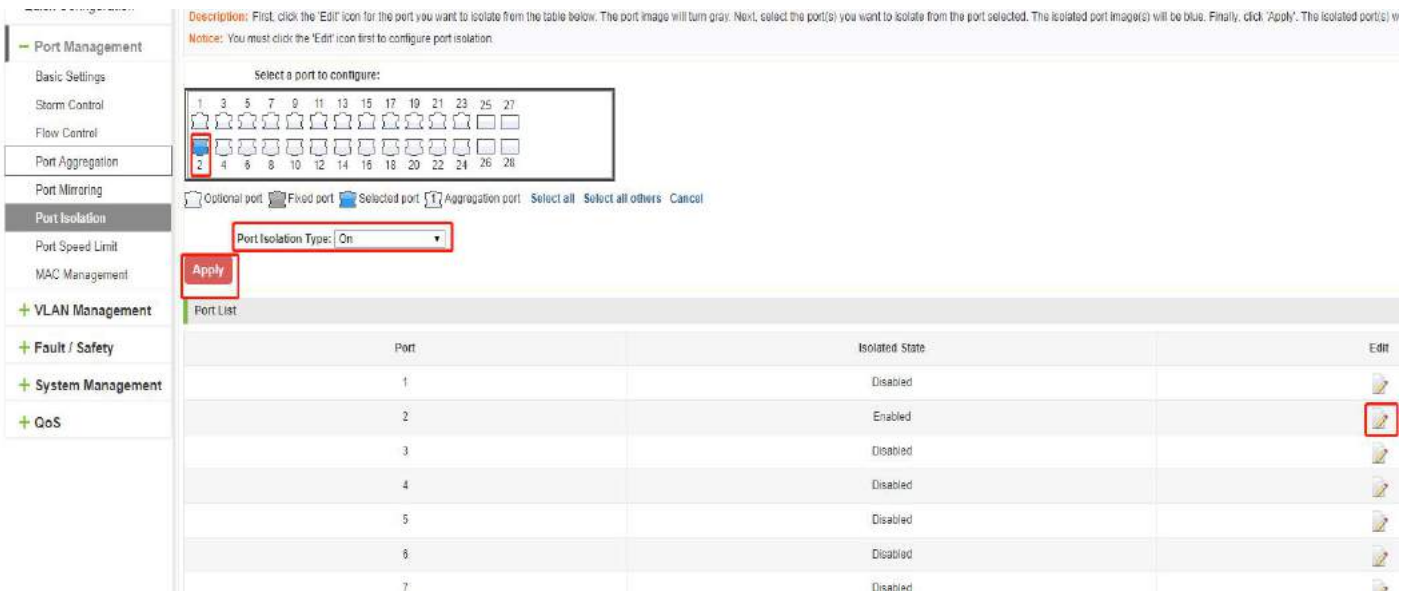
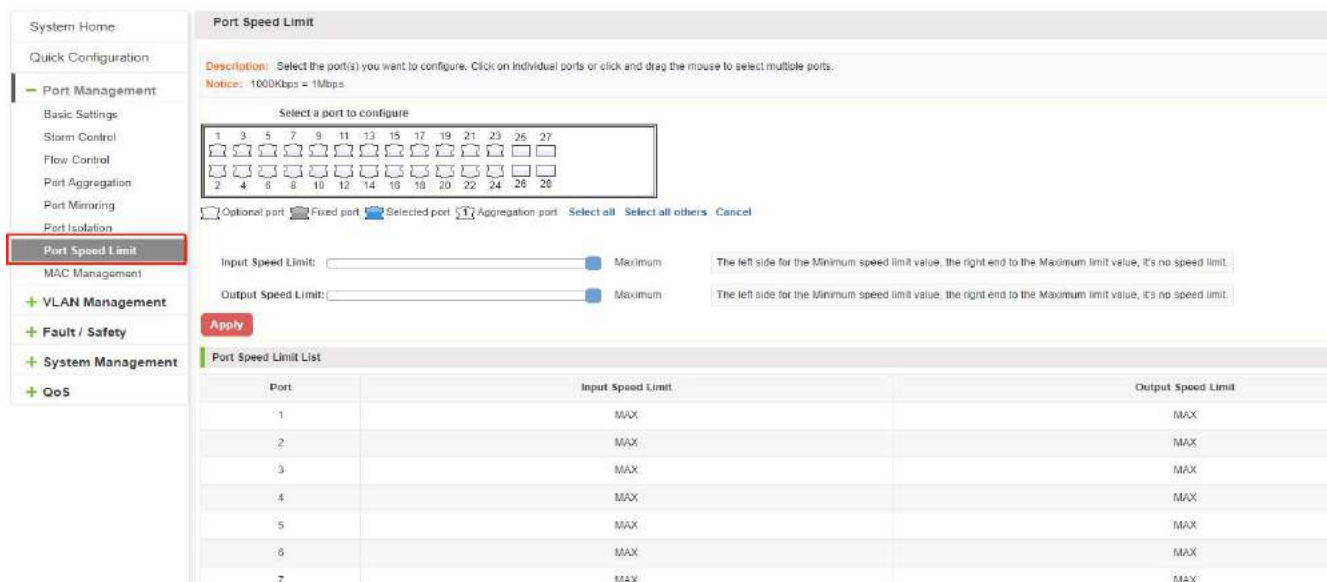


Figure 3-25: Edit the port isolation

## 3.7 PORT SPEED LIMIT

### 3.7.1 VIEW PORT RATE LIMITING

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



**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

Select a port to configure

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Input Speed Limit:  Maximum  
 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
1	MAX	MAX
2	MAX	MAX
3	MAX	MAX
4	MAX	MAX
5	MAX	MAX
6	MAX	MAX
7	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;

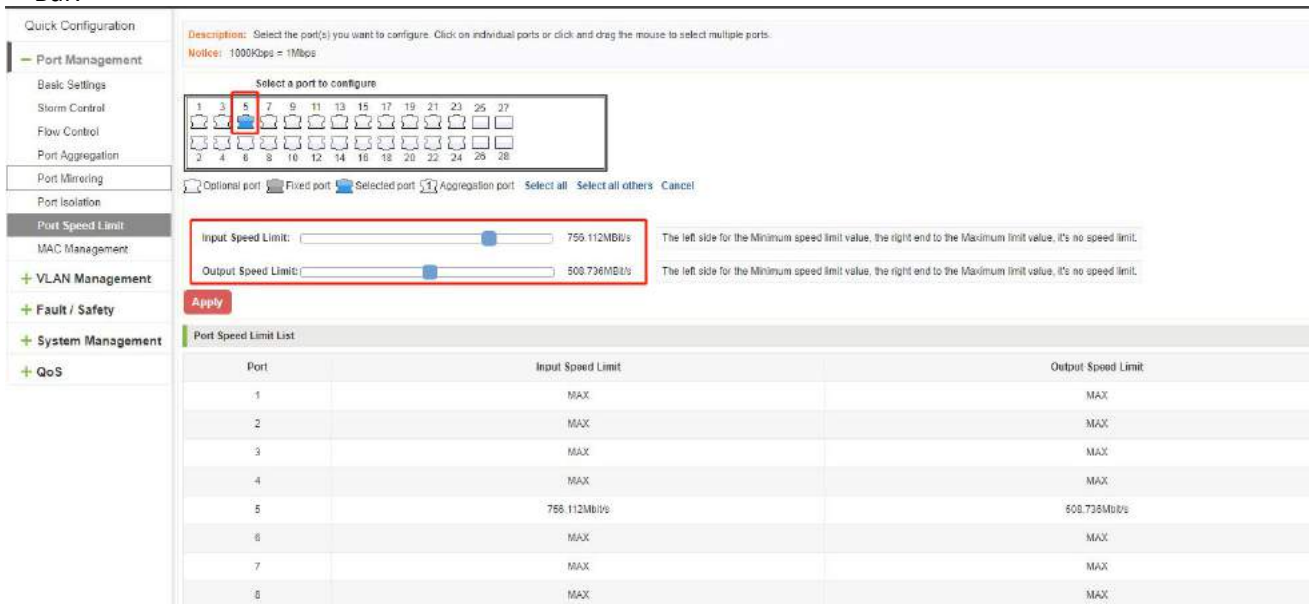
Input limit: uplink port speed;

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 List**

Port	Input Speed Limit	Output Speed Limit
1	MAX	MAX
2	MAX	MAX
3	MAX	MAX
4	MAX	MAX
5	755.112MB/s	500.736MB/s
6	MAX	MAX
7	MAX	MAX
8	MAX	MAX


Figure 3-27 Configure port rate limiting entrance



Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	
2	MAX	MAX	
3	MAX	MAX	
4	MAX	MAX	
5	755.112MB/s	500.736MB/s	
6	MAX	MAX	
7	MAX	MAX	

Figure 3-28: Port entrance speed limit results

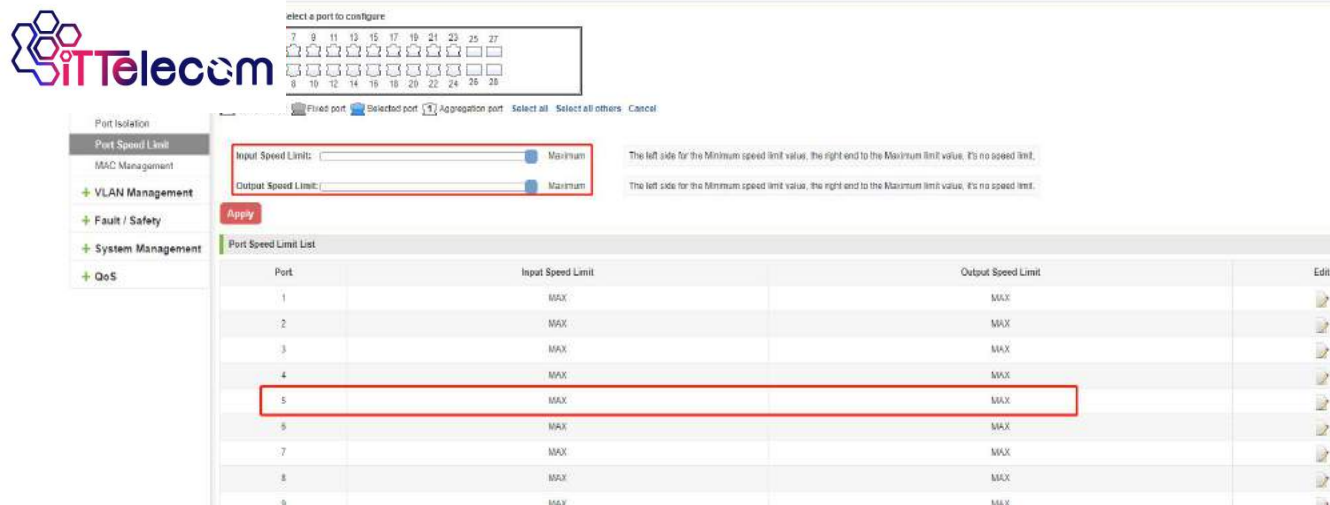
Entrance port rate limiting configuration steps are as follows:

- 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 "Save" 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, "Save" to complete the operation.





**Figure 3-29: Remove the port speed limit**

Remove uplink port rate limiting steps are as follows:

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

## 4 VLAN MANAGEMENT

### 4.1 VLAN MANAGEMENT

#### 4.1.1 CHECK VLAN CONFIGURATION INFORMATION

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



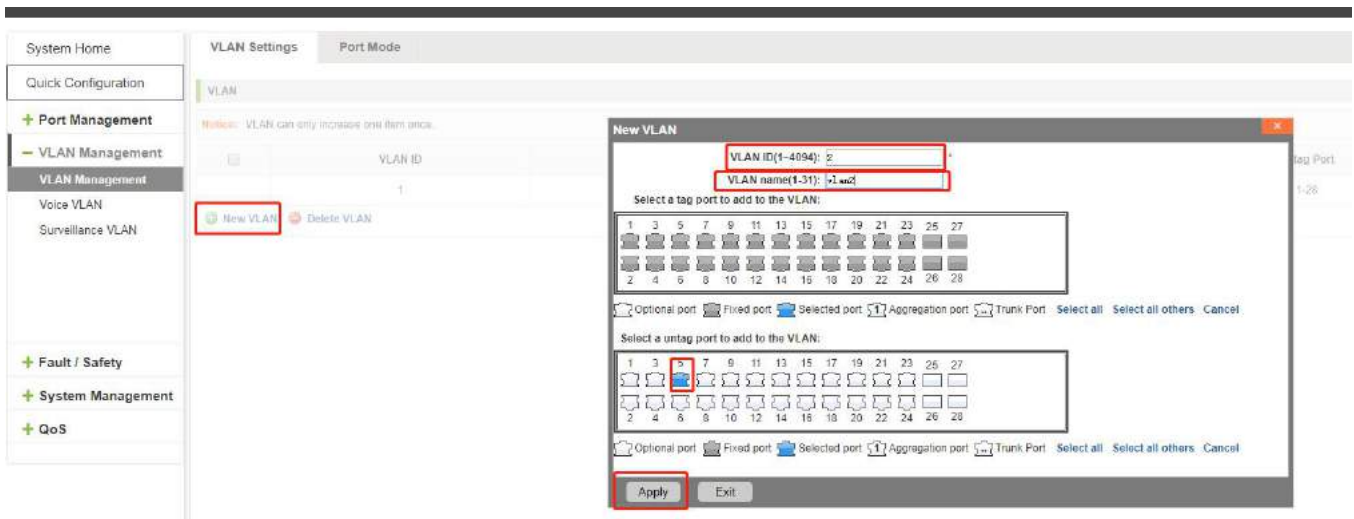
**Figure 4-1: VLAN configuration information**

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

- 1.VLAN ID: VLAN ID value is displayed;
- 2.VLAN Name: The name of the VLAN, the default VLAN ID to name;
- 3.VLAN IP address: Displays the switch's management IP;
- 4.Port: Displays the port VLAN that exist.
- 5.By default, all ports belong to VLAN 1.

#### 4.1.2 ADDING A VLAN

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



**Figure 4-2: Adding a VLAN**

Adding a VLAN, follow these steps:

Step1:Click "NEW vlan" connection;

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

step3:Click the "Save" 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.

## + Port Management

## - VLAN Management

## VLAN Management

## Voice VLAN

## Surveillance VLAN

Notice: VLAN can only increase one item once.

<input type="checkbox"/>	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
<input type="checkbox"/>	1	default		1-4/5-20	
<input checked="" type="checkbox"/>	2	vlan2		5	

New VLAN Delete VLAN

First Previous [1] Next Last

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.

System Home

Quick Configuration

+ Port Management

- VLAN Management

VLAN Management

Voice VLAN

Surveillance VLAN

VLAN Settings

Port Mode

VLAN

Notice: VLAN can only increase one item once.

<input type="checkbox"/>	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
<input type="checkbox"/>	1	default		1-4/5-20	
<input checked="" type="checkbox"/>	2	vlan2		5	
<input checked="" type="checkbox"/>	3	vlan3			

New VLAN Delete VLAN

First Previous [1] Next Last

Figure 4-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

Step1: Select you want to delete VLAN check box;

Step2: Click on the bottom left "Delete VLAN" connection;

Step3: Confirm delete.

#### 4.1.4 EDITING VLAN

##### 4.1.4.1 CHANGE PORT TO A VLAN

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

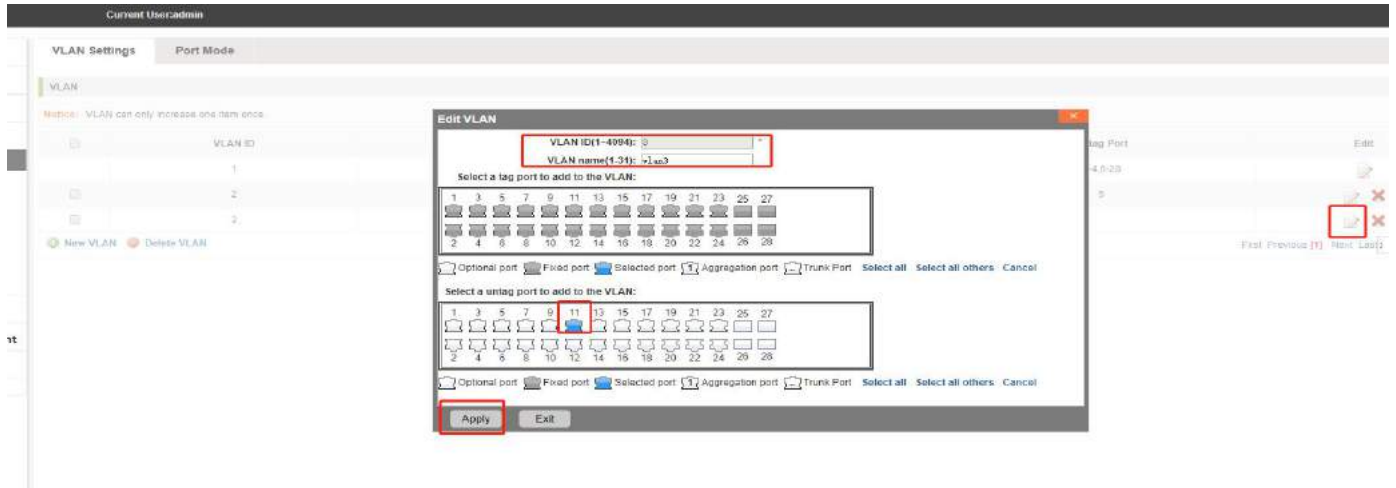


Figure 4-5: Change the port to the VLAN

Add the port to the VLAN, follow these steps:

Step1: Click " " icon.

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

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

##### 4.1.4.2 TO REMOVE THE PORT FROM A VLAN

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

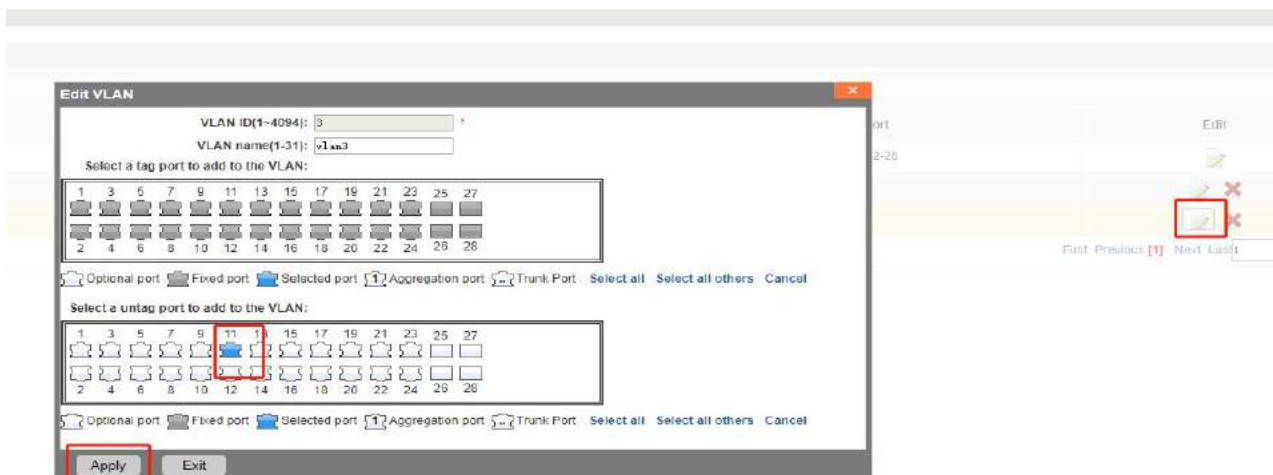



Figure 4-6: To remove the port from the VLAN.

Procedure to remove the port from VLAN as follows:

Step1:Click on the icon “”;

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

step3:Click on the lower right corner of the "Save" 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:

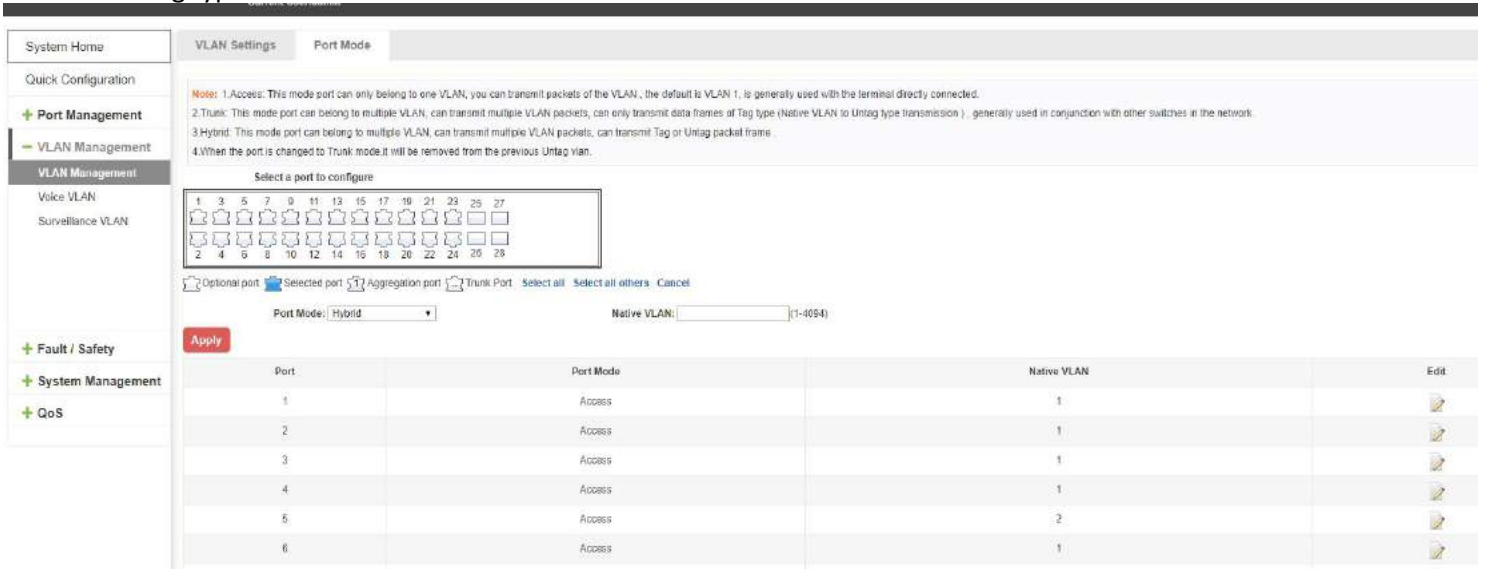
Notice:

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.









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

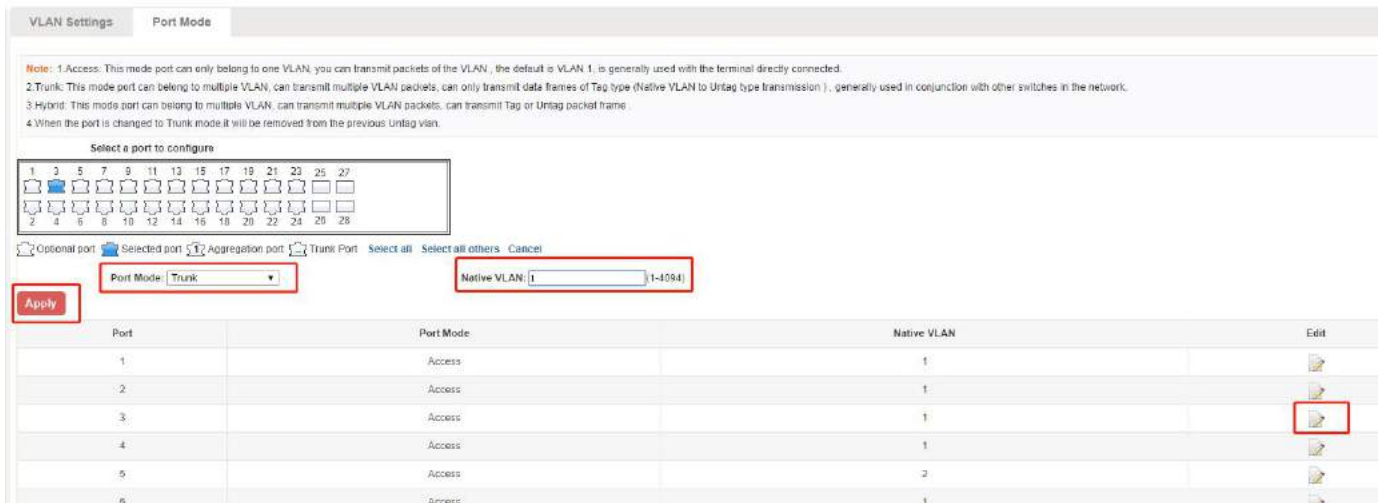
Displayed in the port mode list is the property value of the port configuration of the current switch:

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.

Select a port to configure

Optional port Selected port Aggregation port Trunk Port Select all Select all others Cancel

Port Mode: Trunk Native VLAN: 1 (1-4094)

Apply

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.

Select a port to configure

Optional port Selected port Aggregation port Trunk Port Select all Select all others Cancel

Port Mode: Access Native VLAN: 1 (1-4094)

Apply

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:



System Home

Quick Configuration

+ Port Management

- VLAN Management

VLAN Management

**Voice VLAN**

Surveillance VLAN

Voice VLAN Global

Voice VLAN Port

Voice VLAN OUI

Voice device address

Voice VLAN Global

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

Voice VLAN State:

Voice VLAN ID(2-4094):

Voice VLAN CoS:

Aging Time(1-65535):  min

Apply

Figure 4-10: View the voice vlan configuration

### 4.2.2 ENABLE THE VOICE VLAN

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



System Home

Quick Configuration

+ Port Management

- VLAN Management

VLAN Management

**Voice VLAN**

Surveillance VLAN

Voice VLAN Global

Voice VLAN Port

Voice VLAN OUI

Voice device address

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

Apply

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.

System Home

Quick Configuration

+ Port Management

- VLAN Management

VLAN Management

**Voice VLAN**

Surveillance VLAN

Voice VLAN Global

Voice VLAN Port

Voice VLAN OUI

Voice device address

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:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

State: Enabled Mode: AutoUntag

Apply

voice port list

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”.



mode and Access mode can only be configured in manual mode.

1 3 5 7 9 11 13 15 17 19 21 23 25 27  
2 4 6 8 10 12 14 16 18 20 22 24 26 28

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

State: Enabled Mode: AutoUntag

Apply

voice port list

Port	State	Mode	Edit
1	Disabled	Auto Tag	
2	Disabled	AutoUntag	
3	Disabled	Auto Tag	
4	Disabled	Auto Tag	

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 Global Voice VLAN Port Voice VLAN OUI Voice device address

Voice VLAN OUI

OUI Address: 0000.0000.0000 Mask: 0000.0000.0000 Description: 0 chars Apply

Voice VLAN OUI List

OUI Address	Mask	Description	Edit
00E0.BD00.0000	FFFF.FF00.0000	3COM	
0003.5B00.0000	FFFF.FF00.0000	Cisco	
00E0.7500.0000	FFFF.FF00.0000	Vertel	
00D0.1E00.0000	FFFF.FF00.0000	Pingtel	
0001.E300.0000	FFFF.FF00.0000	Siemens	
0080.B900.0000	FFFF.FF00.0000	NEC/Philips	
000F.E200.0000	FFFF.FF00.0000	Huawei-3COM	
0009.8E00.0000	FFFF.FF00.0000	Avaya	

First Previous 11 Next Last

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.

Voice VLAN Global

Voice VLAN Port

Voice VLAN OUI

Voice device address



MAC:

Description:

Apply

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.B000.0000	FFFF.FF00.0000	NEC/Philips
000F.E200.0000	FFFF.FF00.0000	Huawei-3COM
0009.0E00.0000	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:

Voice VLAN Global

Voice VLAN Port

Voice VLAN OUI

Voice device address

Voice device address List

Port	Voice Device Address	Start Time

[First](#)
[Previous](#)
[Next](#)
[Last](#)
/ 1Page

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

System Home | Surveillance VLAN | Port Surveillance VLAN

**VLAN**

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

Surveillance VLAN: ☐ OFF

Surveillance VLAN ID:  (2-4094)

Surveillance VLAN CoS:  (1-8)

Aging Time:  (1-65535 min)

**Apply**

**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.

User-defined MAC Setting | Auto Surveillance VLAN Summary

Component Type:  Description:  (1-8 chars)

MAC Address:  (e.g. 0001.0203.0000) Mask:  (e.g. FFFF.FF00.0000)

**Apply**

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 .

System Home | Quick Configuration | Port Management | VLAN Management | Surveillance VLAN

**Surveillance VLAN**

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

Surveillance VLAN: ☐ ON

Surveillance VLAN ID:  (2-4094)

Surveillance VLAN CoS:  (1-8)

Aging Time:  (1-65535 min)

**Apply**

**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.

User-defined MAC Setting | Auto Surveillance VLAN Summary

Component Type:  Description:  (1-8 chars)

MAC Address:  (e.g. 0001.0203.0000) Mask:  (e.g. FFFF.FF00.0000)

**Apply**

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 .



**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:

Surveillance VLAN

Port Surveillance VLAN

id or Trunk mode and Access mode can only be configured in manual mode.

ire:

5 17 19 21 23 25 27

2 4 6 8 10 12 14 16 18 20 22 24 26 28

Optional port

Fixed port

Selected port

Aggregation port

Select all

Select all others

Cancel

Status: Do Not Modify

Mode: Do Not Modify

Apply

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 :

Surveillance VLAN

Port Surveillance VLAN

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:

1 3 5 7 9 11 13 15 17 19 21 23 25 27

2 4 6 8 10 12 14 16 18 20 22 24 26 28

Optional port

Fixed port

Selected port

Aggregation port

Select all

Select all others

Cancel

Status: Do Not Modify

Mode: Auto

Apply

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

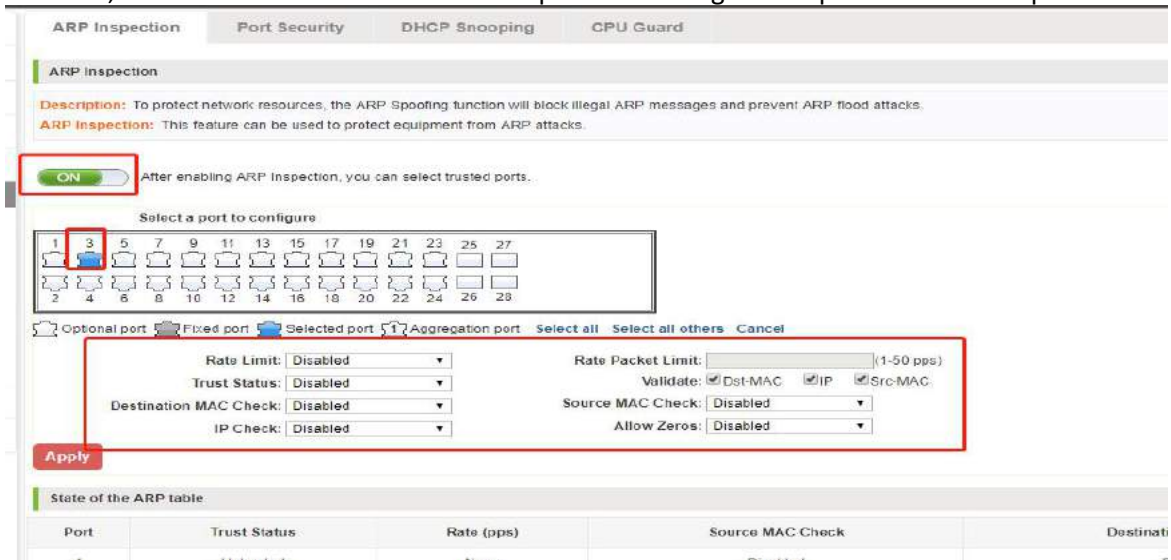
Click the "Fault/Safety" "Attack Prevention" "ARP Inspection" to check the current switches has been configured for ARP information:

Figure 5-1: View port ARP configuration information



### 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 "Save" 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.

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

Select a port to configure

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Rate Limit: Disabled Rate Packet Limit: (1-50 pps)

Trust Status: Disabled Validate: ☒ Dst-MAC ☒ IP ☒ Src-MAC

Destination MAC Check: Disabled Source MAC Check: Disabled

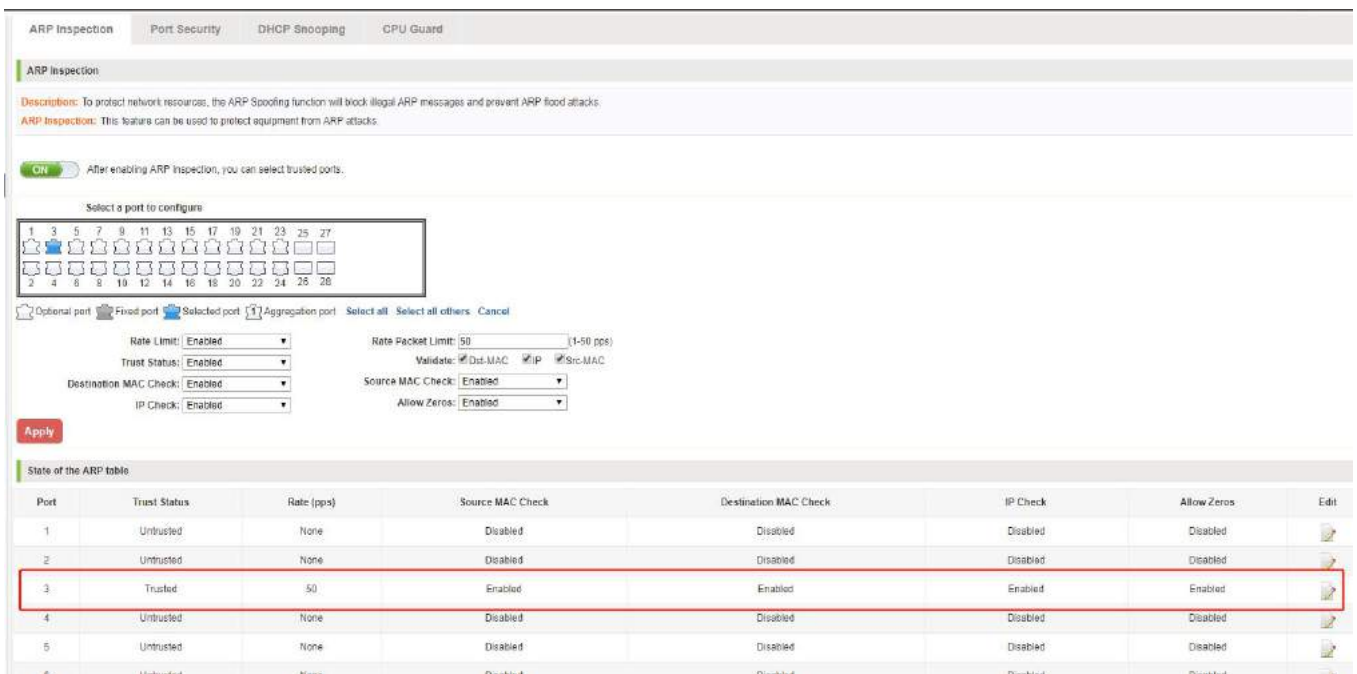
IP Check: Disabled Allow Zeros: Disabled

**Apply**

**State of the ARP table**

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Destination
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 5-2: 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.

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

Select a port to configure

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Rate Limit: Enabled Rate Packet Limit: 50 (1-50 pps)

Trust Status: Enabled Validate: ☒ Dst-MAC ☒ IP ☒ Src-MAC

Destination MAC Check: Enabled Source MAC Check: Enabled

IP Check: Enabled Allow Zeros: Enabled

**Apply**

**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.

resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks. be used to protect equipment from ARP attacks.

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

Select a port to configure

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Rate Limit: Enabled Rate Packet Limit: 50 (1-50 pps)

Trust Status: Enabled Validate: ☒ Dst-MAC ☒ IP ☒ Src-MAC

Destination MAC Check: Enabled Source MAC Check: Enabled

IP Check: Enabled Allow Zeros: Enabled

**Apply**

State of the ARP table

Figure 5-4: Disable ARP spoofing function

### 5.1.1.4 TO MODIFY THE PORT ATTRIBUTE

ARP Inspection Port Security DHCP Snooping CPU Guard

**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

1	3	5	7	9	11	12	13	15	17	19	21	23	25	27
2	4	6	8	10	14	16	18	20	22	24	26	28		

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Rate Limit: Enabled Rate Packet Limit: 50 (1-50 pps)

Trust Status: Enabled Validate: ☒ Dst-MAC ☒ IP ☒ Src-MAC

Destination MAC Check: Enabled Source MAC Check: Enabled

IP Check: Enabled Allow Zeros: Enabled

**Apply**

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:

Current User:admin

System Home	Ping Detection	Tracert Detection	Cable Detection
-------------	----------------	-------------------	-----------------

Quick Configuration

- + Port Management
- + VLAN Management
- Fault / Safety
  - Attack Prevention
  - Path Detection**
  - DDOS Protection
  - Loopback Detection
  - STP
  - Access Control
  - IGMP
  - MLD
- + System Management
- + QoS

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

Destination IP

**Start Test**

**Test Results**

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:

System Home	Ping Detection	Tracert Detection	Cable Detection
-------------	----------------	-------------------	-----------------

Quick Configuration

- + Port Management
- + VLAN Management
- Fault / Safety
  - Attack Prevention
  - Path Detection**
  - DDOS Protection
  - Loopback Detection
  - STP
  - Access Control
  - IGMP
  - MLD
- + System Management
- + QoS

**Description:** Tracert detection can detect to the destination through the gateway, the function is used to detect whether can reach the destination and the time. 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

Timeout (2-10s)

**Start Test**

**Test Results**

Figure 5-13: Tracert detection information

### 5.2.3 CABLE DETECTION

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

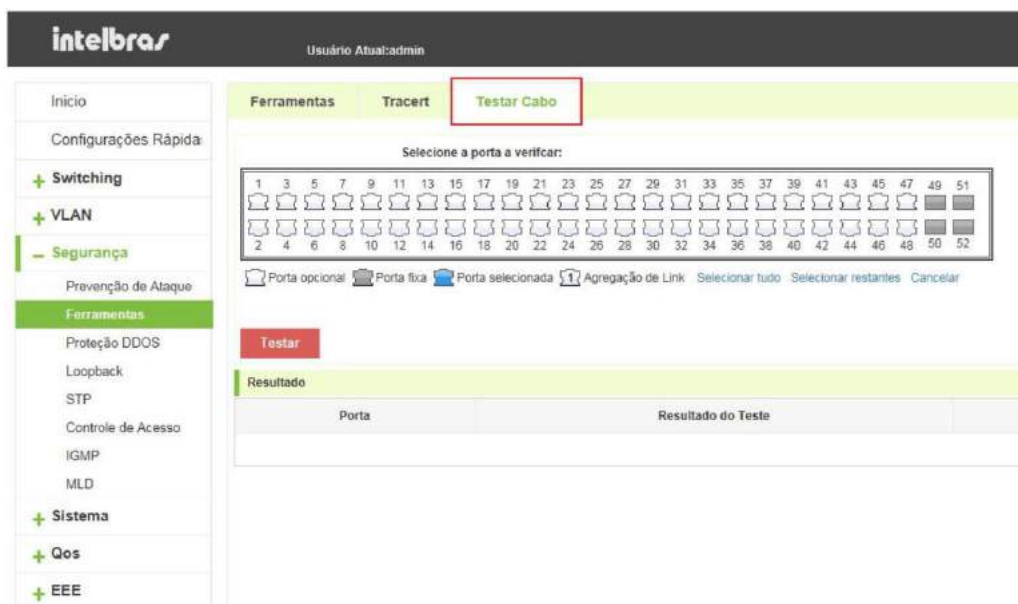


Figure 5-14: Cable detection information

The cable detection only selected one port:

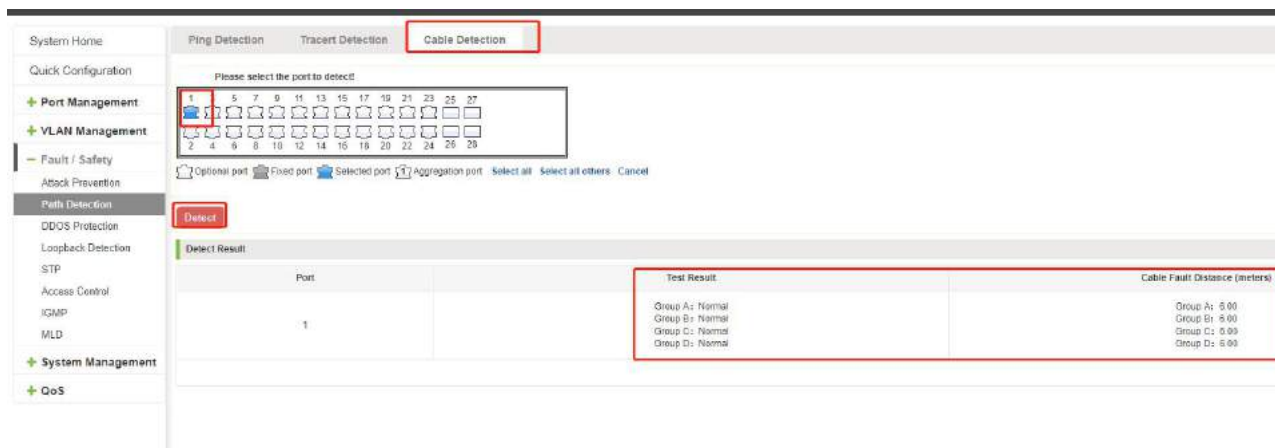


Figure 5-15: Port cable detection result

### 5.3 DDOS PROTECTION

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



Figure 5-16: DDOS Protection information

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

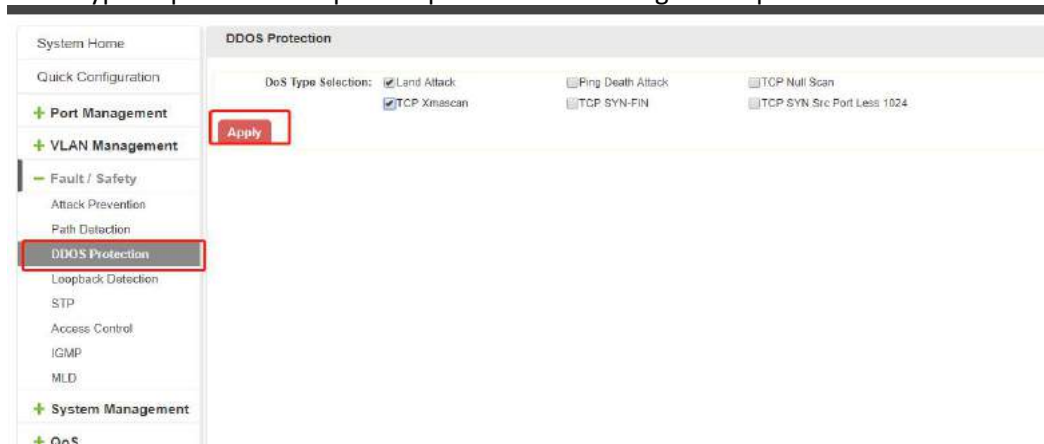


Figure 5-17: selected dos type

## 5.4 LOOPBACK DETECTION

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

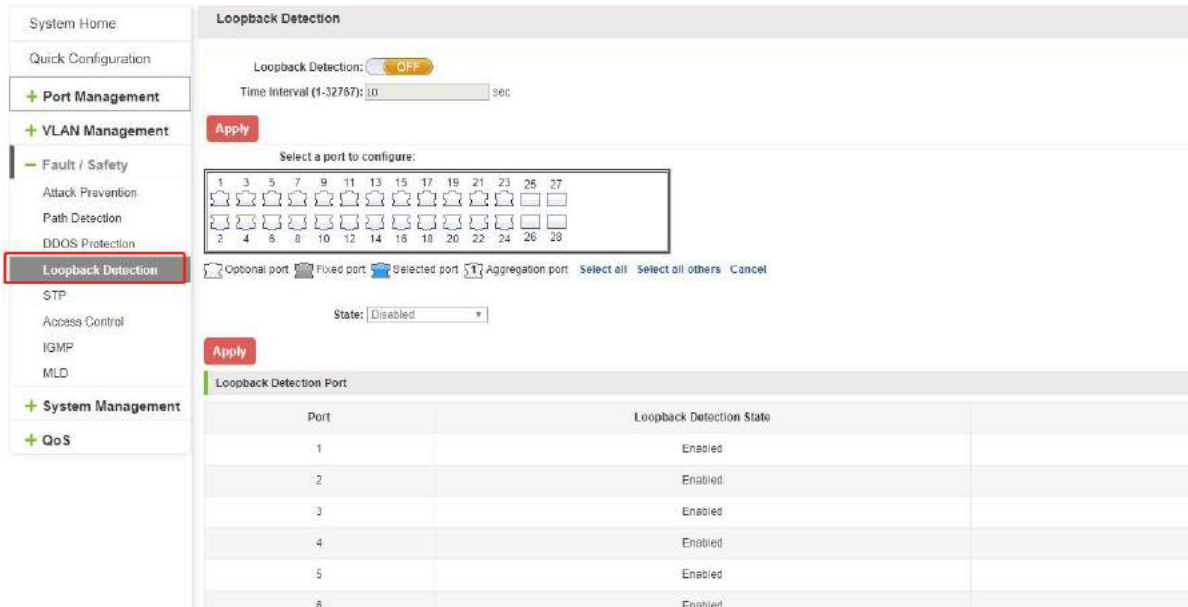


Figure 5-18: View loopback detection configuration information

### 5.4.1 ENABLE LOOPBACK DETECTION

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

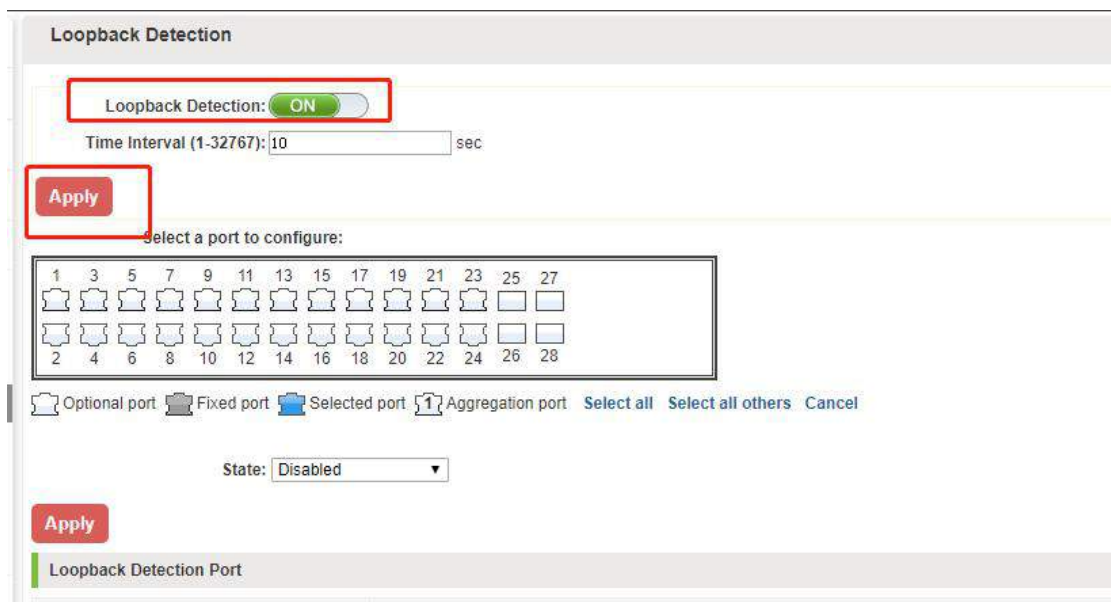


Figure 5-19: enable loopback detection

### 5.4.2 CHOOSE THE PORT TO CONFIGURE

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

Loopback Detection

Loopback Detection: **ON**

Time Interval (1-32767): 10 sec

**Apply**

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port **Selected port** Aggregation port Select all Select all others Cancel

State: Enabled

**Apply**

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

**Apply**

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Optional port Fixed port **Selected port** Aggregation port Select all Select all others Cancel

State: Disabled

**Apply**

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**