

LevelOne

GES-2451

HW: ver 3

28-Port Web Smart Gigabit Switch

User Manual

1 WEB MANAGEMENT LANDING PAGE	5
1.1 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB.....	5
2 QUICK CONFIGURATION	6
2.1 VLAN SETTING.....	6
2.2 TRUNK PORT SETTING.....	7
2.3 SNMP CONFIGURATION	7
2.4 THE OTHER SETTINGS.....	8
3 PORT MANAGEMENT.....	8
3.1 BASIC SETTINGS.....	8
3.1.1 <i>Check the port configuration</i>	8
3.1.2 <i>Configuring Port Properties</i>	9
3.2 STORM CONTROL	9
3.2.1 <i>Check the port settings Storm</i>	9
3.3 FLOW CONTROL.....	12
3.3.1 <i>Configuring Flow Control.</i>	13
3.4 PORT AGGREGATION	14
3.4.1 <i>Viewing Port Aggregation Configuration</i>	14
3.4.2 <i>Add port aggregation</i>	15
3.4.3 <i>Modifying port aggregation</i>	15
3.6 PORT MIRRORING.....	16
3.6.1 <i>Port Mirroring Configuration</i>	16
3.6.2 <i>Add port mirroring group</i>	16
3.6.3 <i>To modify the port mirroring group</i>	17
3.6.4 <i>Delete a port mirroring group</i>	18
3.7 PORT SPEED.....	19
3.7.1 <i>View port rate limiting</i>	19
3.7.2 <i>Configure port access rate</i>	20
3.4.4 <i>Remove the port speed limit</i>	21
4 VLAN MANAGEMENT.....	22
4.1 VLAN MANAGEMENT.....	22
4.1.1 <i>Check VLAN configuration information</i>	22
4.1.2 <i>Adding a VLAN</i>	23
4.1.3 <i>Remove VLAN</i>	23
4.1.4 <i>Editing VLAN</i>	24
4.1.4.1 <i>Port to a VLAN</i>	24
4.1.4.2 <i>To remove the port from a VLAN</i>	24
4.1.5 <i>View TRUNK port settings</i>	25
4.1.6 <i>increased TRUNK</i>	25
4.1.7 <i>delete TRUNK port</i>	26
4.1.7.1 <i>Delete a single trunk port</i>	26
4.1.7.2 <i>Multiple trunk ports simultaneously deleted</i>	26
5 FAULT / SAFETY	27
5.1 ATTACK PREVENTION.....	27
5.1.1 <i>ARP SNOOFING</i>	27
5.1.1.1 <i>View ARP configuration</i>	27
5.1.1.2 <i>ARP spoofing function</i>	27

5.1.1.3 Disable ARP anti cheat function	28
5.1.1.4 Delete IP+MAC	29
5.1.2 port security	29
5.1.2.1 Configuration port security	29
5.1.2.2 Enable the function	29
5.1.2.3 Change port security configuration	30
5.1.3 anti DHCP attack	30
5.1.3.1 view anti DHCP attack configuration	30
5.1.3.2 Open anti DHCP attack function	31
5.1.3.3 Sets the port to DHCP non trusted port	31
5.1.3.4 Off anti DHCP attack function	32
5.2 PATH DETECTION	33
5.3 LOOP DETECTION	33
5.3.1 to change the spanning tree mode	34
5.3.2 Close spanning tree function	34
5.4 ACCESS CONTROL	34
5.4.1 ACL access control list	34
5.4.1.1 view access control list	34
5.4.1.2 Increased access rules	35
5.4.1.3 Modify configuration	37
5.4.1.4 Delete rule	37
5.4.2 application ACL	38
5.4.2.1 View application ACL	38
5.4.2.2 Increased application ACL	38
5.4.2.3 Delete application ACL	39
5.5 IGMP SNOOPING	39
5.5.1 View IGMP Snooping configuration	39
5.5.2 active multicast listener function	40
5.5.3 disable multicast listener function	40
5.5.4 configuration multicast routing	41
5.5.5 IGMP version	41
6 SYSTEM MANAGEMENT	42
6.1 SYSTEM SETTINGS	42
6.1.1 management vlan	42
6.1.1.1 configuration Basic System Settings	42
6.1.2 System restart	43
6.1.3 change password	44
6.1.4 System Log	44
6.1.5 Log Export	45
6.1.6 ARP table	45
6.1.7 MAC management	46
6.1.7.1 MAC address lookup	46
6.1.7.2 Add a static MAC address type	47
6.1.7.3 Remove the static MAC address type	48
6.2 SYSTEM UPGRADE	49
6.3 SYSTEM INFORMATION	49
6.3.1 Memory information	49
6.3.2 CPU INFORMATION	50
6.4 CONFIGURATION MANAGEMENT	51
6.4.1 Configuration management	51

<i>6.4.2 Restore factory Settings</i>	52
6.5 SNMP	53
<i>6.5.1 Check the SNMP</i>	53
<i>6.5.2 Activate the SNMP</i>	53
<i>6.5.3 To disable the SNMP</i>	54
<i>6.5.4 Activate the TRAP.....</i>	55
<i>6.5.5 Disable the TRAP</i>	55
<i>6.5.6 Increase of community.....</i>	55
<i>6.5.7 Delete the community name</i>	56
<i>6.5.8 Added the SNMP TRAP service host</i>	56
<i>6.5.9 Delete the SNMP TRAP service host</i>	57
6.6 SYSTEM DIAGNOSTICS	57
6.7 THE WEB CONSOLE	58

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

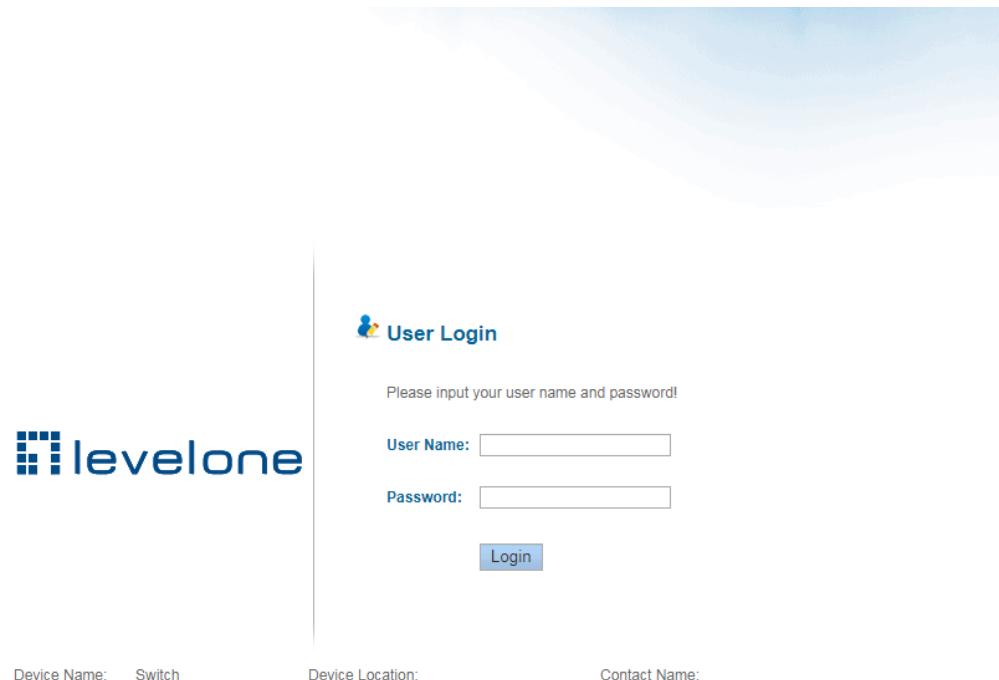


Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:

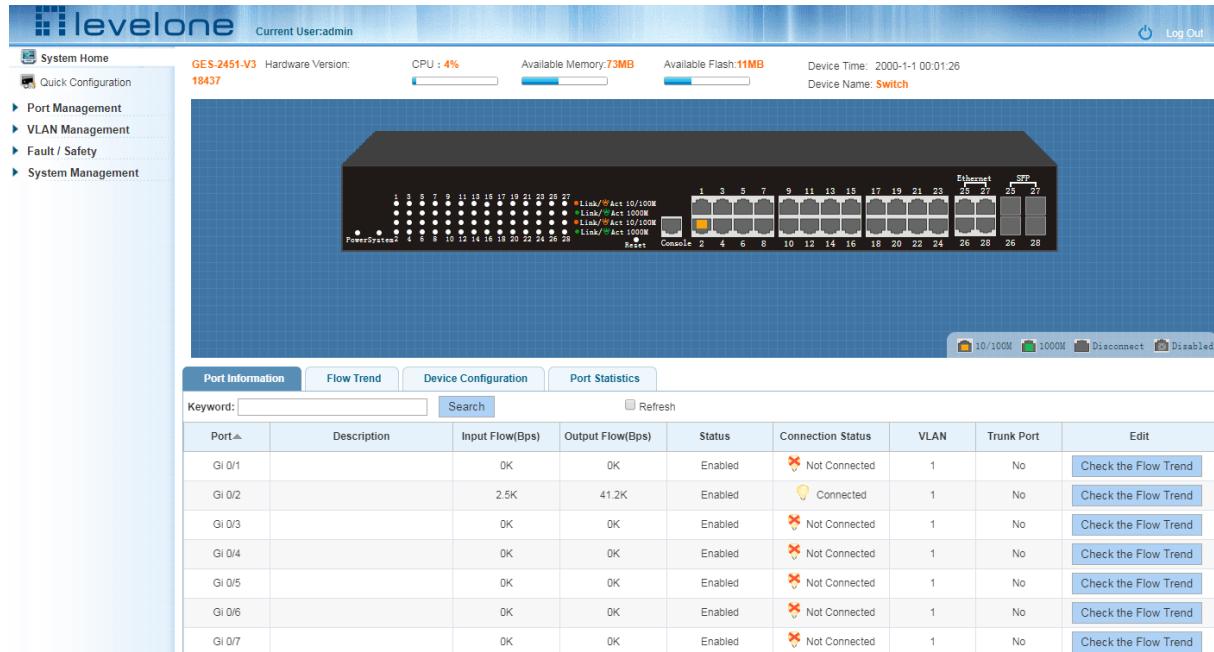


Figure 1-2: switch WEB management page Home

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".

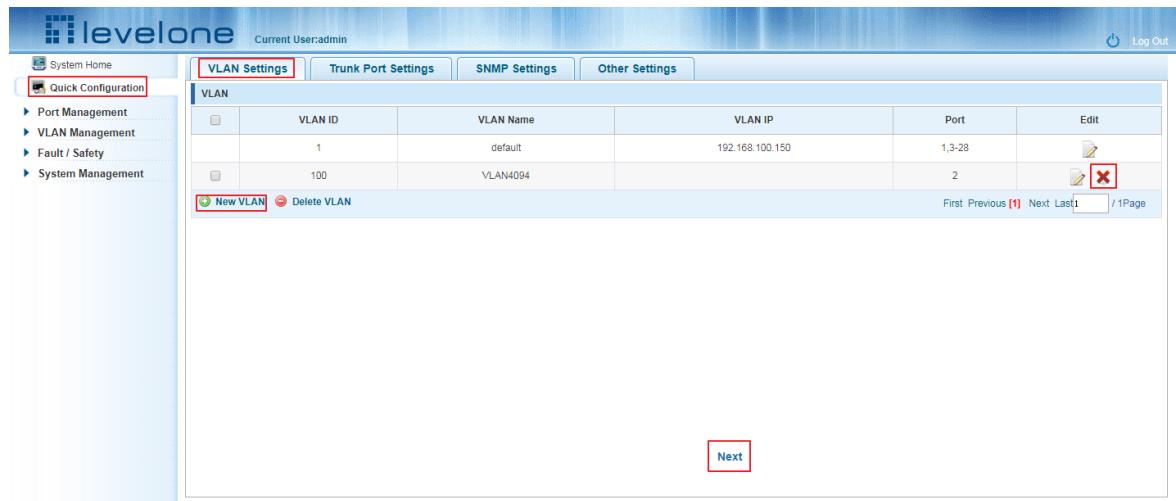


Figure 2-1: VLAN Setting

2.2 TRUNK PORT SETTING

Click on "Quick Configuration" "Trunk Port Settings" into the Trunk of Quick Configuration Settings page. Trunk can view the current equipment configuration information, and according to the demand of new Trunk, modify Trunk, delete the Trunk opening operation, such as after configuration is complete, click "Next" to enter the Port Class Settings page. Or click on "Previous" back to the VLAN Settings page.

The screenshot shows the 'Trunk Port List' section of the 'Trunk Port Settings' page. The table has columns for Port (7-12), Native VLAN (all set to 1), and Allowed VLAN (all set to 1,100). Each row has an 'Edit' button with a pencil icon and a red X icon. At the bottom left is a 'New Trunk Port List' button, and at the bottom right are navigation links: First, Previous [1], Next, Last, and /1Page.

Port	Native VLAN	Allowed VLAN	Edit
7	1	1,100	
8	1	1,100	
9	1	1,100	
10	1	1,100	
11	1	1,100	
12	1	1,100	

Figure 2-2: Trunk Port Setting

2.3 SNMP CONFIGURATION

Click on "Quick Configuration" "SNMP Settings" into the Quick Configuration of the SNMP Settings page. Can configure SNMP function on the current equipment, such as open/close function of SNMP, configure SNMP TRAP services, etc. Configuration is complete, click "Next" to enter POE Settings page. Or click on "Previous" back to the Trunk port Settings page.

The screenshot shows the 'Community Name List' section of the 'SNMP Settings' page. It includes fields for Community Name (private, public), Permissions (rw, ro), and Remove buttons. At the bottom left is a 'Community Name List' button, and at the bottom right are navigation links: First, Previous [1], Next, Last, and /1Page.

Community Name	Permissions	Remove
private	rw	
public	ro	

Figure 2-3: SNMP Setting

2.4 THE OTHER SETTINGS

Click "Quick Configuration" "Other Settings" into the quick Configuration of equipment information system Settings page. Can the current equipment basic information system and manage password configured. End of the configuration is Complete, click on "Complete" rapid configuration, or click the "Previous" back to the SNMP Settings page.

The screenshot shows the 'Other Settings' page of the LevelOne web interface. It includes fields for Management VLAN (Vlan 1), Management IP (192.168.100.150), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), Login Timeout(s) (1800), and MAC (E405.0FAB.871A). A 'Device Name' field is set to 'Switch'. Below these are sections for modifying the super user password (Old Password, New Password, Confirm New Password) with 'Save' and 'Empty' buttons. At the bottom right are 'Previous' and 'Complete' buttons, with 'Complete' highlighted by a red box.

Figure 2-4: other settings

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:

The screenshot shows the 'Basic Settings' page under 'Port Management'. It features a port selection grid where ports can be individually selected or multiple ports can be selected using the mouse. Below the grid are fields for 'Description', 'Status' (set to 'Do Not Modify'), 'Rate' (set to 'Do Not Modify'), and 'Duplex Mode' (set to 'Do Not Modify'). A 'Save' button is located at the bottom left. To the left of the main form is a sidebar with navigation links for System Home, Quick Configuration, Port Management (selected), Basic Settings, VLAN Management, Fault / Safety, and System Management. A note at the top states: 'Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.' and 'Note: If the parameters selected are not supported, the changes will not take effect.'

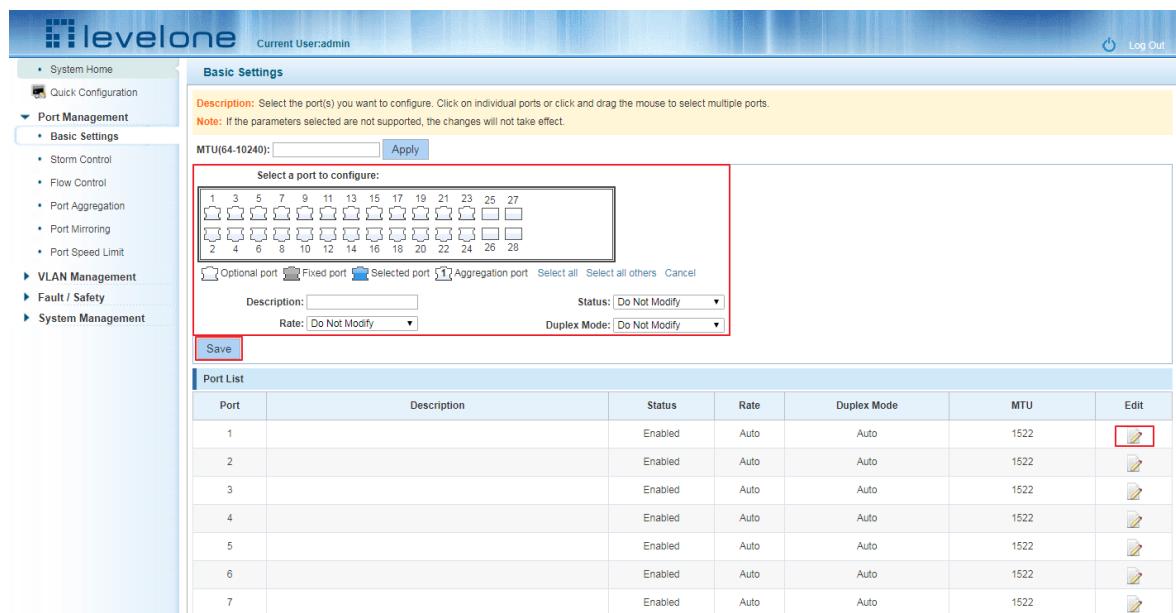
Figure 3-1: Port list information

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:



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	

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

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:

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](#)

Storm Control Type:

Save

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

Port List

Port	Unicast	Broadcast	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	

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.Uncast: 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.

Port	Unicast	Broadcast	Multicast	Edit
1	Disabled	54640	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	

Figure 3-4: Configuring Storm Control information

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

Port	Unicast	Broadcast	Multicast	Edit
1	Disabled	54640	Disabled	
2	Disabled	Disabled	Disabled	
3	Disabled	53440	Disabled	
4	Disabled	Disabled	Disabled	
5	Disabled	53440	Disabled	
6	Disabled	Disabled	Disabled	
7	Disabled	53440	Disabled	
8	Disabled	Disabled	Disabled	
9	Disabled	53440	Disabled	

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.

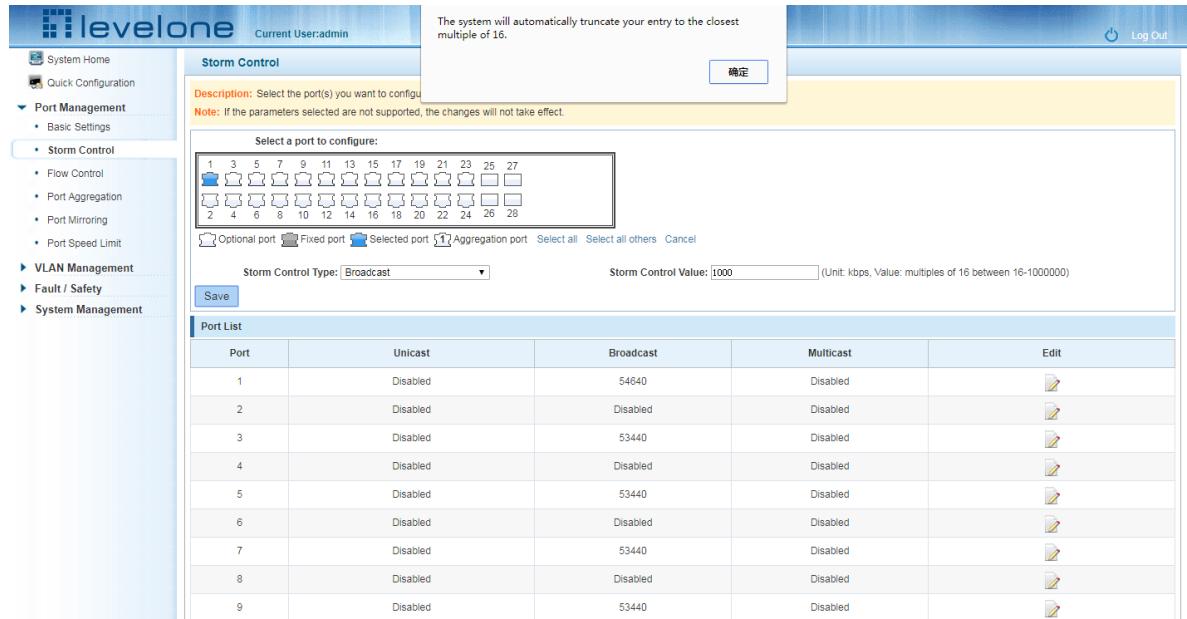


Figure 3-6: Configuring Storm Control information

After the configuration, as shown below:

Port List					
Port	Unicast	Broadcast	Multicast	Edit	
1	Disabled	1008	Disabled		
2	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:

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

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":

Port	Flow Control	Edit
1	On	
2	Off	
3	Off	

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	Flow Control	Edit
1	On	
2	Off	
3	On	

Figure 3-10: Port flow control status

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

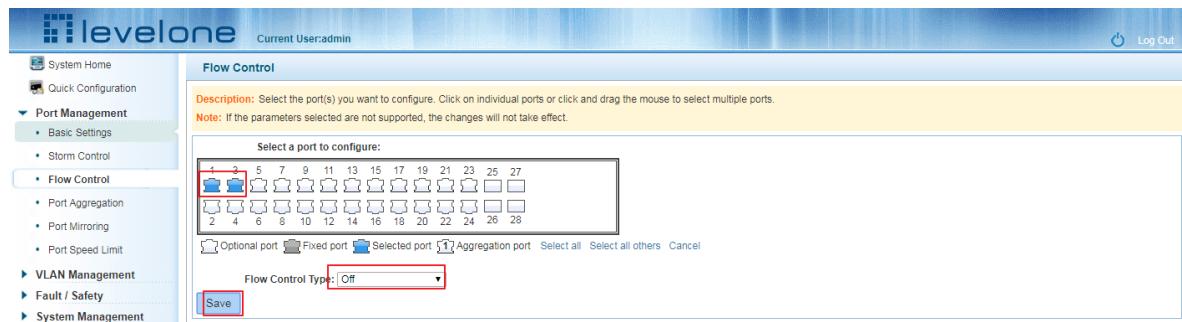


Figure 3-11: Close the port flow control

Close port traffic control, follow these steps:

Step1:Select the button to the right of the port or directly selected port;step2:In the "Flow control type" select Off;step3:Click "Save".

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:

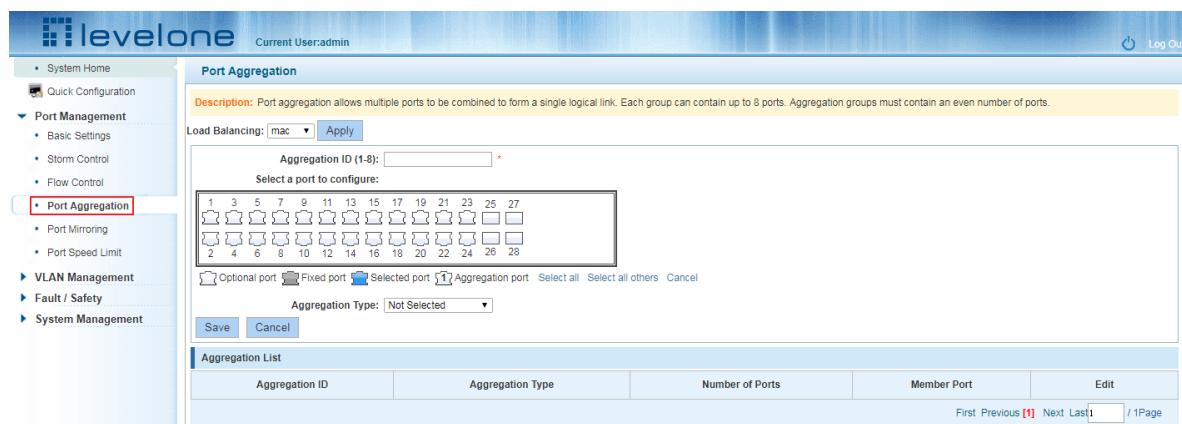


Figure 3-12: Aggregation port configuration information

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"

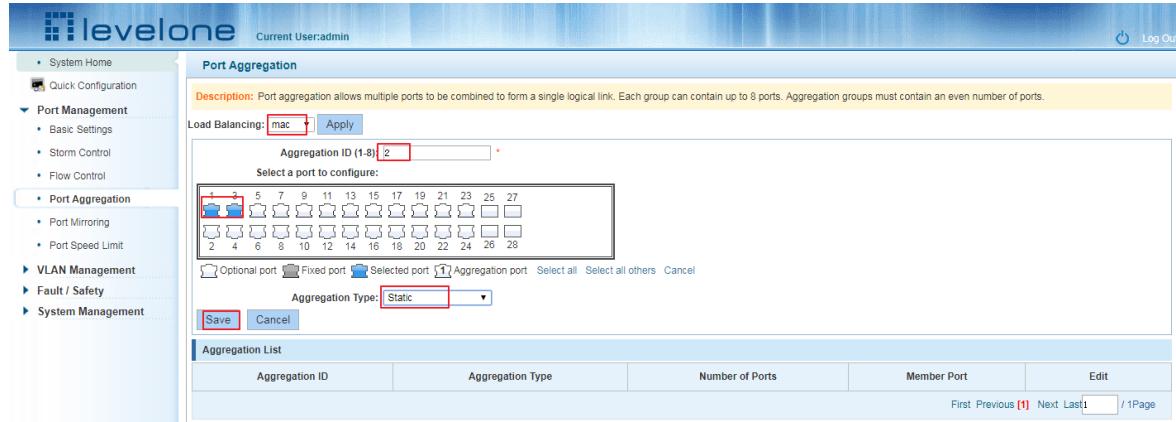


Figure 3-13: Port Aggregation Configuration area

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:

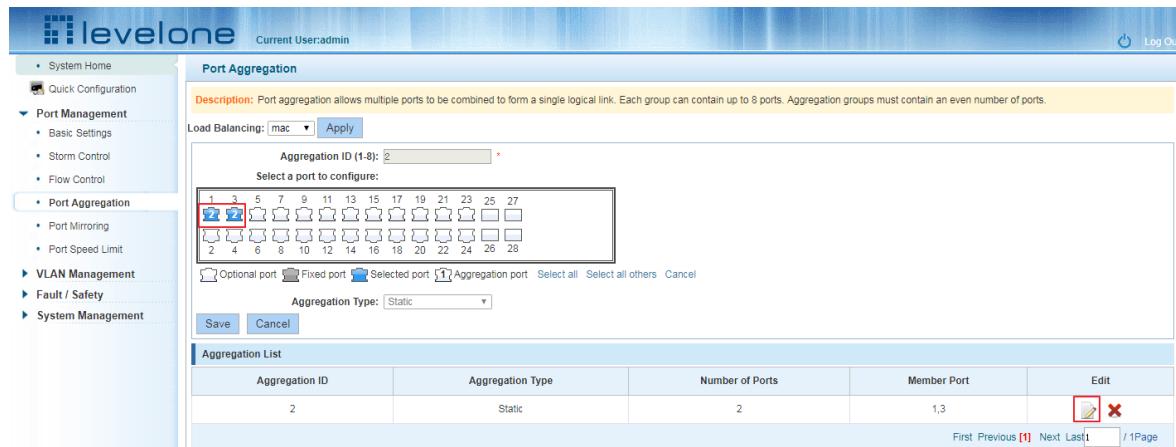


Figure 3-14: To modify the port aggregation

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.

3.6 PORT MIRRORING

3.6.1 PORT MIRRORING CONFIGURATION

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

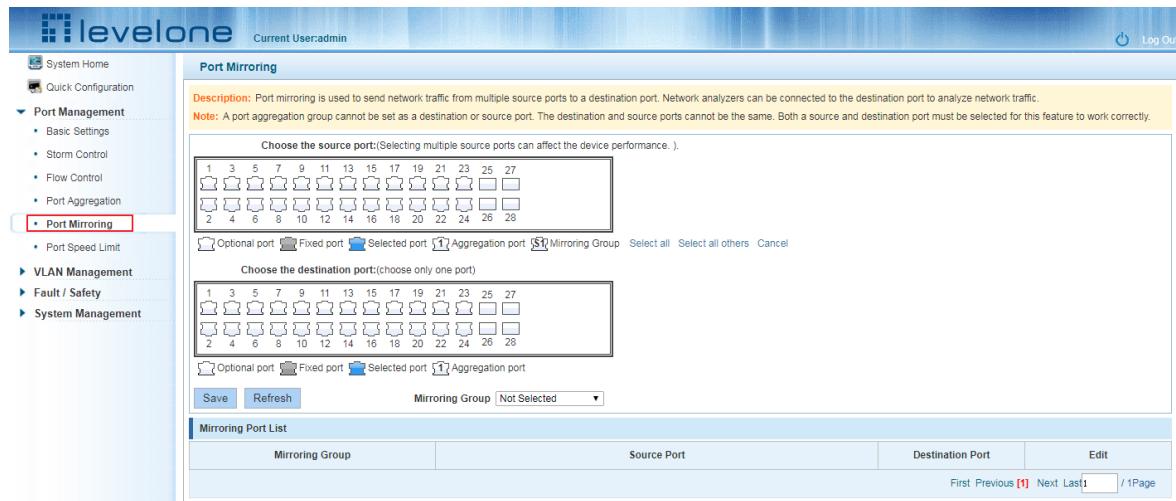


Figure 3-15: Port mirroring configuration information

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.

3.6.2 ADD PORT MIRRORING GROUP

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

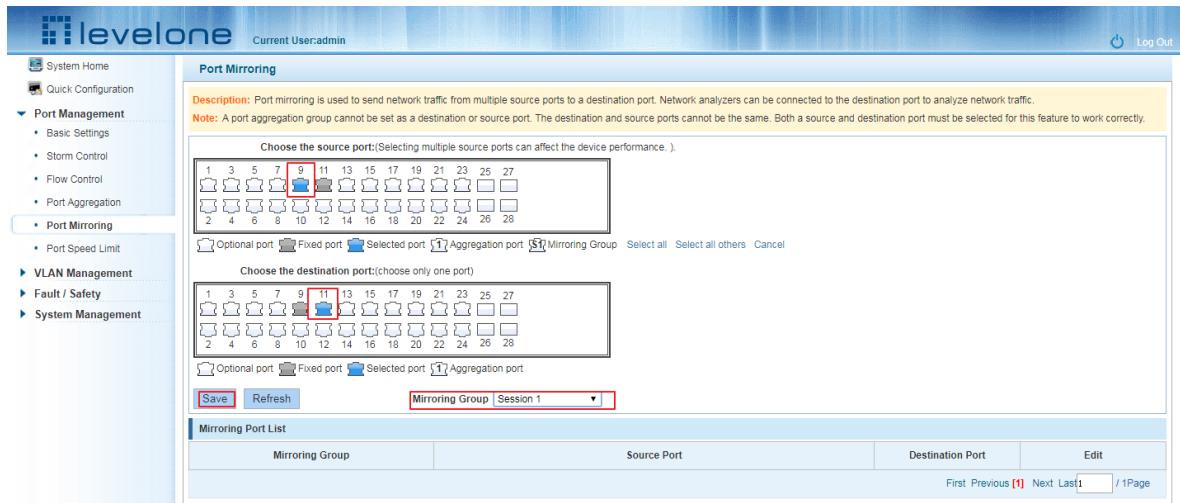


Figure 3-16: Add port mirroring group

Mirroring Group	Source Port	Destination Port	Edit
1	9	11	

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.
- 4.Aggregated port mirroring can not be configured are shown in gray in the panel.
- 5.Has been selected port mirroring port, displayed in the faceplate is gray.

3.6.3 TO MODIFY THE PORT MIRRORING GROUP

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

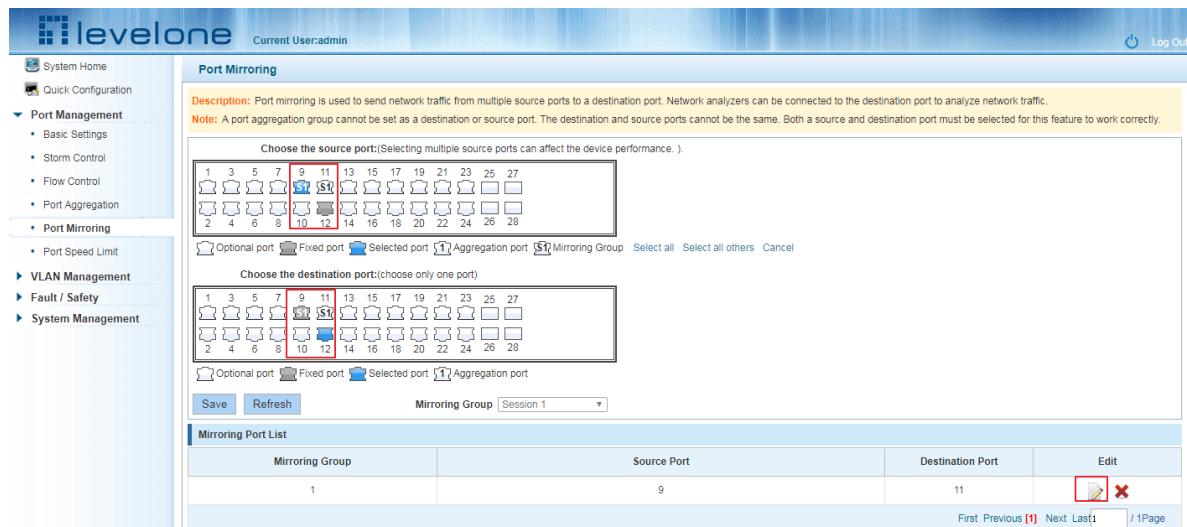


Figure 3-18: To modify the port mirroring group

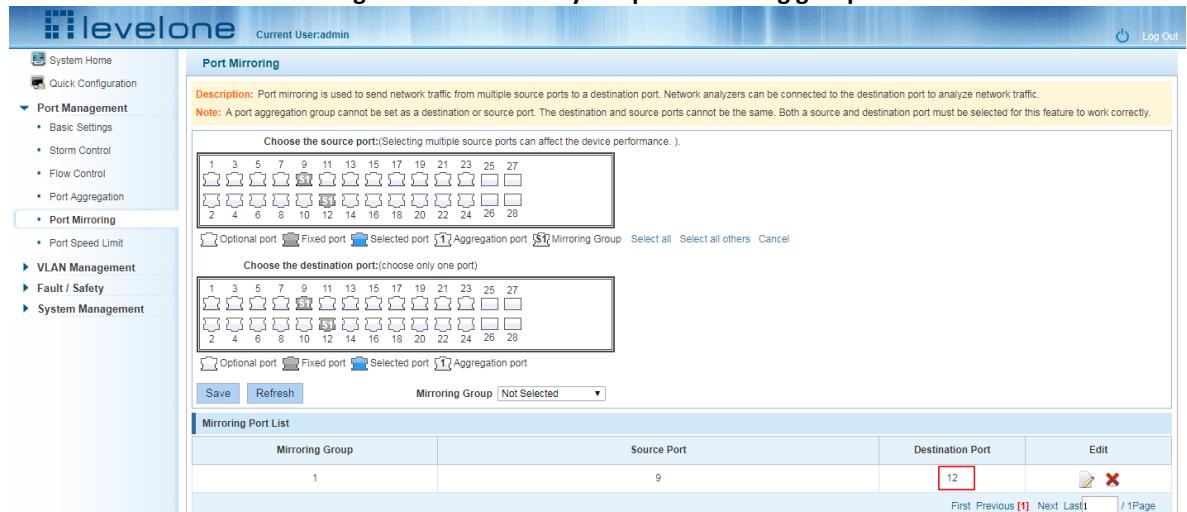


Figure 3-19: Modify successful port mirroring group

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"

3.6.4 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)

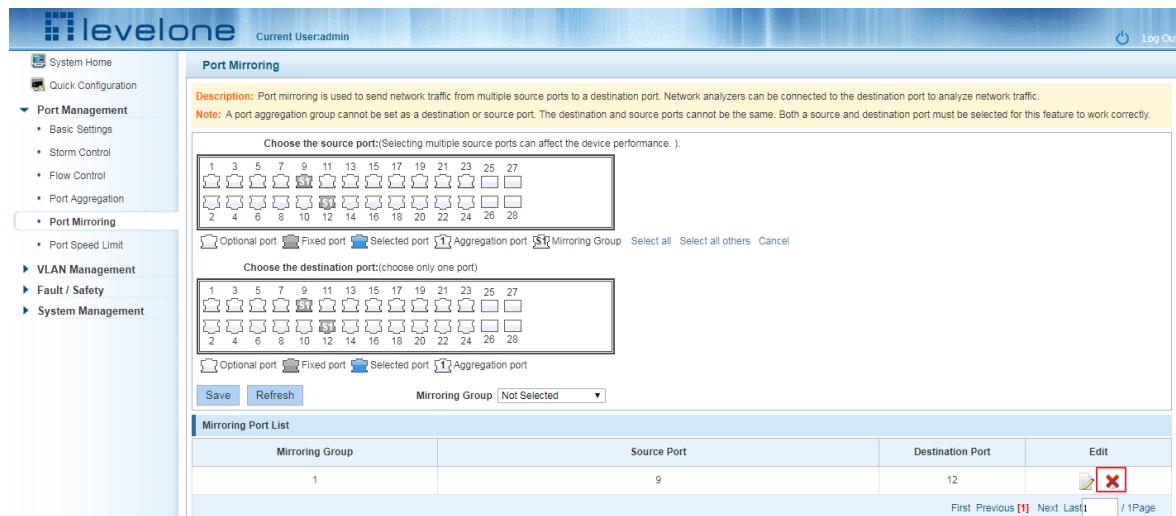


Figure 3-20: Delete port mirroring group

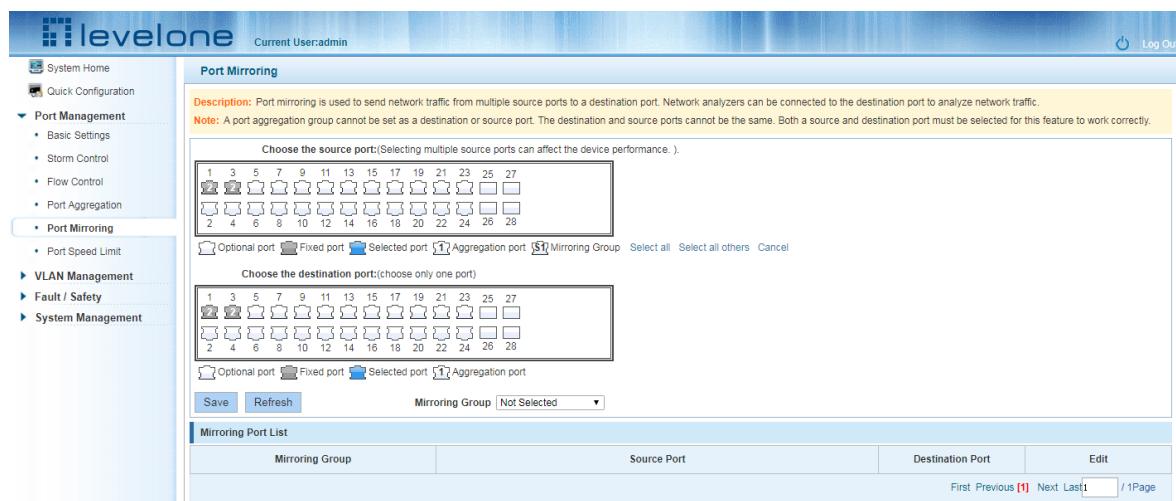


Figure 3-21: Deleted successfully port mirroring

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"

3.7 PORT SPEED

3.7.1 VIEW PORT RATE LIMITING

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

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	

Figure 3-22: 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	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	

Figure 3-23 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	MAX	MAX	
6	MAX	MAX	
7	MAX	MAX	
8	MAX	MAX	
9	306.672Mbit/s	480.864Mbit/s	
10	MAX	MAX	

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

Figure 3-24: 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.

3.4.4 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.

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	320.608Mbit/s	522.672Mbit/s	

Figure 3-25: Remove the port 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		

Figure 3-26: Remove the port speed limit results

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:

VLAN ID	VLAN Name	VLAN IP	Port	Edit
1	default	192.168.100.150	4-26 Ag2	
100	VLAN0100		2.7-12	

Figure 4-1: VLAN configuration information

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

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:

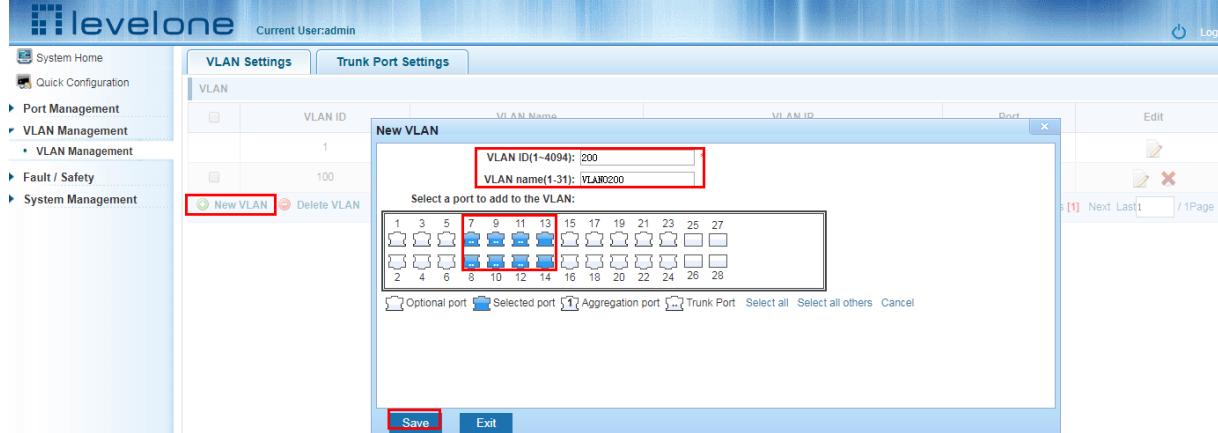


Figure 4-2: Adding a VLAN

Adding a VLAN, follow these steps:

Step1:Click "NEW vlan" connection;

step2:Value added VLAN VLAN ID of the page to fill in;

step3:Click the lower right corner "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:

VLAN Settings					
VLAN					
	VLAN ID	VLAN Name	VLAN IP	Port	Edit
	1	default	192.168.100.150	4-12,15-26,Ag2	
	100	VLAN100		2,7-12	
	200	VLAN200		7-14	

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:

VLAN Settings					
Trunk Port Settings					
VLAN					
	VLAN ID	VLAN Name	VLAN IP	Port	Edit
	1	default	192.168.100.150	4-12,15-26,Ag2	
<input checked="" type="checkbox"/>	100	VLAN100		2,7-12	
<input checked="" type="checkbox"/>	200	VLAN200		7-14	

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

Figure 4-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

Step1:I 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 Port to a VLAN

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

VLAN Settings					
Trunk Port Settings					
VLAN					
	VLAN ID	VLAN Name	VLAN ID	Port	Edit
	1				
<input checked="" type="checkbox"/>	100				
	200				

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

Edit VLAN

VLAN ID(1~4094): *

VLAN name(1~31):

Select the ports to modify the VLAN:

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

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

Save **Exit**

Figure 4-5: Add 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:

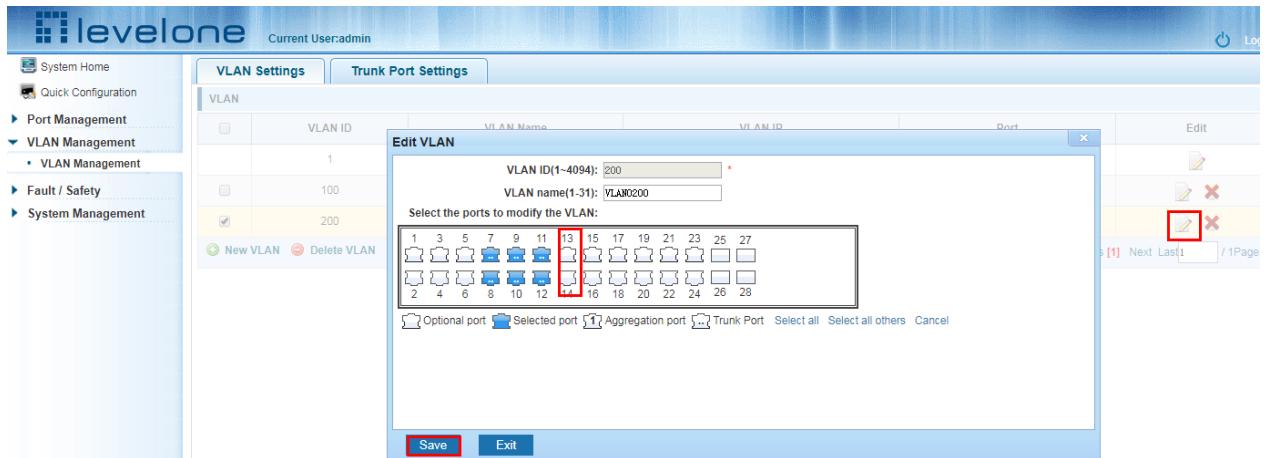


Figure 4-6: To remove the port from the VLAN.

Procedure to remove the port from VLAN as follows:

Step1:Click on the icon “” ;

step2:Remove the port to be removed from the port panel;

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

4.1.5 VIEW TRUNK PORT SETTINGS

Click on the "Vlan Management" "TRUNK Port settings" view switches has been configured trunk port information:

	Port	Native VLAN	Allowed VLAN	Edit
	3	1		

Figure 4-7: View trunk configuration information

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

- 1.The port name: display port number used;
- 2.The Native VLAN's native VLAN: display port;
- 3.The VLAN allows the display message can be through vlan;
- 4.The default port is 1 VLAN native vlan,

4.1.6 INCREASED TRUNK

Click the "Trunk Port List New" button, can be carried out to increase the configuration of the trunk port:

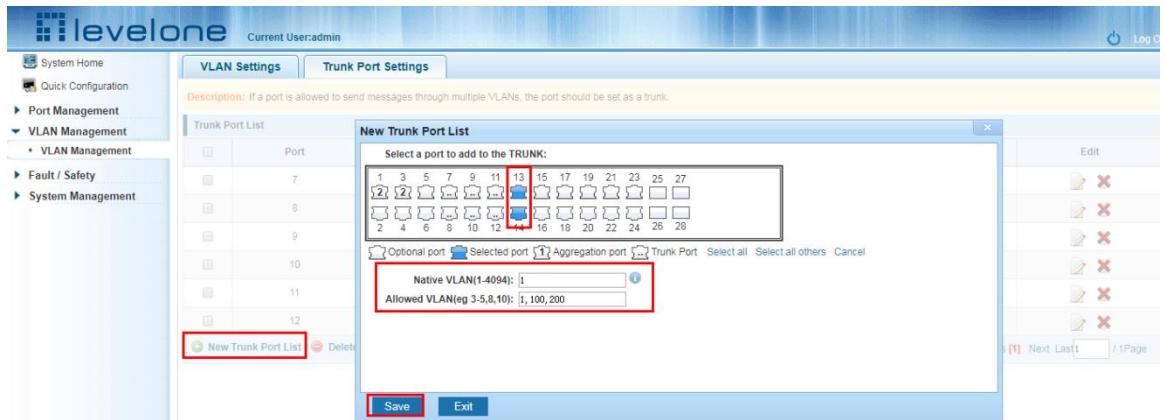


Figure 4-8: Trunk

The steps to increase trunk are as follows :

Step1:Click on the "new trunk port list" button;

step2:Select the port to be set on the port panel;

step3:Set local VLAN;step3:Set local VLAN;

step4:Set by allowing the VLAN number;

step5:Click on the lower right corner of the "application" button to complete the configuration.

4.1.7 DELETE TRUNK PORT

4.1.7.1 Delete a single trunk port

Selected to remove the trunk port, click the "X" button, you can delete the selected trunk. port:

Trunk Port List				
	Port	Native VLAN	Allowed VLAN	Edit
	9	1	1,100,200	
	10	1	1,100,200	

Figure 4-9: Delete a single trunk port

4.1.7.2 Multiple trunk ports simultaneously deleted

First selected to need to be removed before the trunk port of the "√" check box, click "Trunk Port Delete" connection, you can delete the selected trunk port:

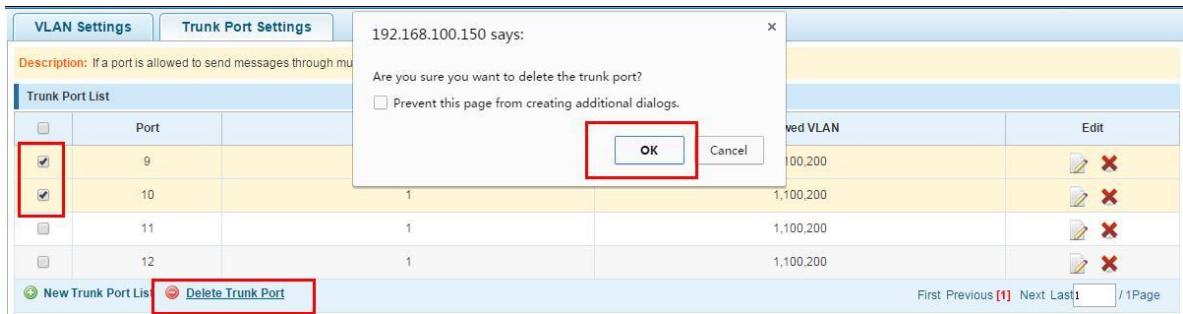


Figure 4-10: Delete multiple trunk ports

The procedure for removing multiple trunk ports is as follows:

Step1:select the check box to delete the trunk port;step2:Click on the lower left corner of the "Trunk Port Delete" button;step3: Confirm complete delete。

5 FAULT / SAFETY

5.1 ATTACK PREVENTION

5.1.1 ARP SNOOFING

5.1.1.1 View ARP configuration

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



Figure 5-1: View port ARP configuration information

5.1.1.2 ARP spoofing function

In the ARP spoofing configuration , input IP and mac ,then click the "Save" button to complete the configuration prevent ARP deception .

Figure 5-2: ARP spoofing configuration

The screenshot shows the 'ARP Spoofing' configuration page. At the top, there are three tabs: 'ARP Spoofing' (selected), 'Port Security', and 'DHCP Snooping'. Below the tabs, under 'Protection status', there is a description: 'To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.' A green 'ON' button is highlighted with a red box. Under 'Protection Settings', there is a note about 'Protection Settings' and 'IP+MAC' binding. A table at the bottom lists an entry with IP 192.168.100.55 and MAC 4016.A1B1.3355. A 'Save' button is visible.

The screenshot shows the 'ARP spoofing status table'. It displays a single row with the IP 192.168.100.55 and MAC 4016.A1B1.3355. The table includes columns for IP, MAC, and Edit. A delete icon (cross) is shown next to the MAC column. A note at the bottom says 'Delete choose IP + MAC'. Navigation links like 'First', 'Previous', 'Next', 'Last', and '1 / 1Page' are at the bottom right.

Figure 5-3: ARP spoofing status table

5.1.1.3 Disable ARP anti cheat function

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

The screenshot shows the 'ARP Spoofing' configuration page. The 'ON' button is highlighted with a red box. A confirmation dialog box is overlaid, asking 'Sure you want to close the ARP attack prevention function?' with an 'OK' button highlighted with a red box. The background page shows the same configuration options as Figure 5-2.

Figure 5-4: Disable ARP spoofing function

5.1.1.4 Delete IP+MAC

The screenshot shows the 'ARP Spoofing' configuration page. At the top, there are tabs for 'ARP Spoofing', 'Port Security', and 'DHCP Snooping'. The 'ARP Spoofing' tab is active. Below the tabs, there is a 'Protection status' section with a green 'ON' button. A yellow 'Description' box states: 'To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.' In the 'Protection Settings' section, there is a note: 'Protection Settings: This feature can be used to protect equipment from ARP attacks.' Another note says: 'IP+MAC: To prevent the distribution of static IP address users against ARP deception or attack, an IP can only bind a MAC, a MAC can bind multiple IP.' Below these notes, there is a table with two rows. The first row has an empty checkbox, the IP '192.168.100.55', and the MAC '4015.7819.1740'. The second row has a checked checkbox, the IP '192.168.100.55', and the MAC '4015.7819.1740'. To the right of the table is an 'Edit' button and a red-bordered 'Delete' button. At the bottom of the table area, there are navigation links: 'First', 'Previous [1]', 'Next', 'Last [1]', and '/ 1Page'.

Figure 5-5: Delete IP+MAC

5.1.2 PORT SECURITY

5.1.2.1 Configuration port security

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

The screenshot shows the 'Port Security' configuration page. At the top, there are tabs for 'ARP Spoofing', 'Port Security' (which is highlighted with a red border), and 'DHCP Snooping'. The 'Port Security' tab is active. A yellow 'Description' box states: 'To protect network resources, the Port Security function will prevent malicious attack to take up a large number of MAC address table entries. It will warn and discard the message when exceed the limited port MAC number.' Below the description, there is a section titled 'Select a port to configure:' with a grid of 27 numbered ports (1-27). Below the grid are buttons for 'Optional port', 'Fixed port', 'Selected port', 'Aggregation port', 'Select all', 'Select all others', and 'Cancel'. There is also a dropdown for 'Admin State' set to 'Disabled' and a 'Max Learning Address' input field set to '(1-256)'. A 'Save' button is at the bottom left. Below this is a 'Port List' table with three entries:

Port	Admin State	Max Learning Address	Edit
1	Disabled	No limit	
2	Disabled	No limit	
3	Disabled	No limit	

Figure 5-6: Port security configuration

5.1.2.2 Enable the function

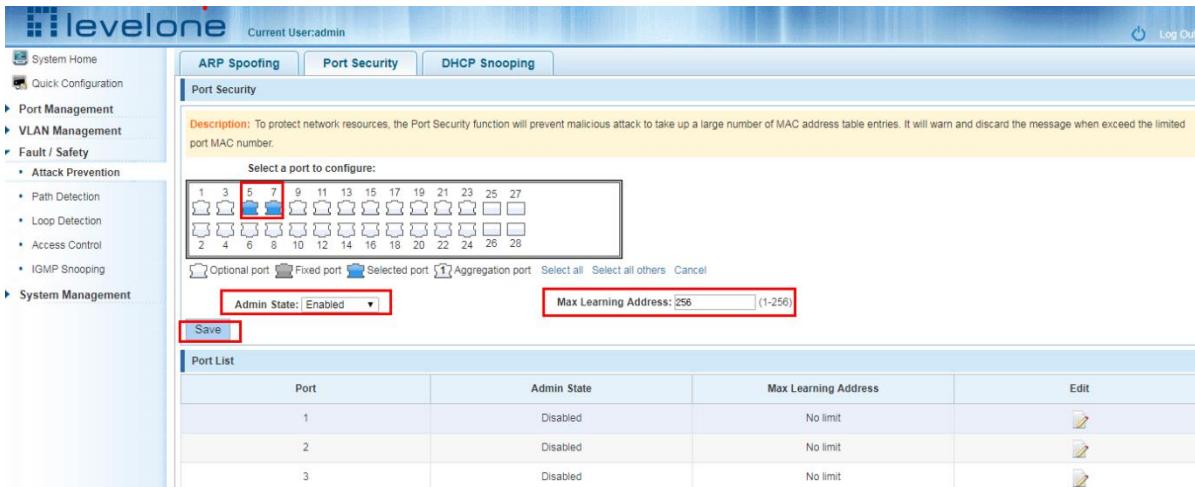


Figure 5-7: Enable the Port security

5.1.2.3 Change port security configuration

In the port list, select the port you want to edit, you can change the port state and the max learning address numbers :

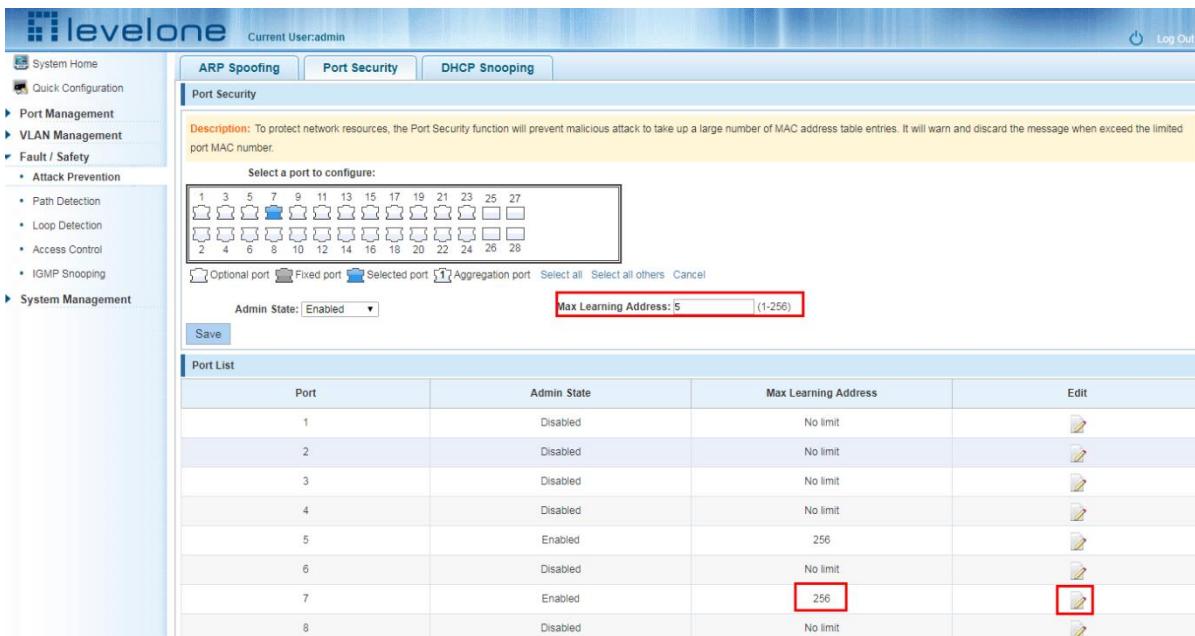


Figure 5-8: Change port max learning address

5.1.3 ANTI DHCP ATTACK

5.1.3.1 view anti DHCP attack configuration

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

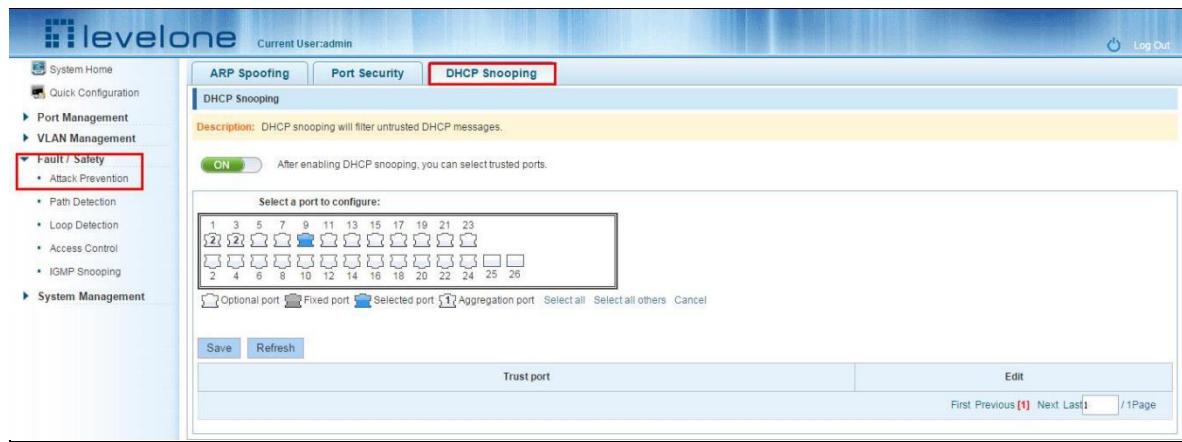


Figure 5-9: View anti DHCP attack configuration information

Click "Refresh" button, display refresh configuration information.

5.1.3.2 Open anti DHCP attack function

Click on a "Fault/Safety" "DHCP Snooping" click the button to open the anti DHCP attack:



Figure 5-10: Activation of anti DHCP attack function

5.1.3.3 Sets the port to DHCP non trusted port

In the trusted port list, select the port that needs to be disabled to prevent DHCP attacks, and click the "" button to disable the function:

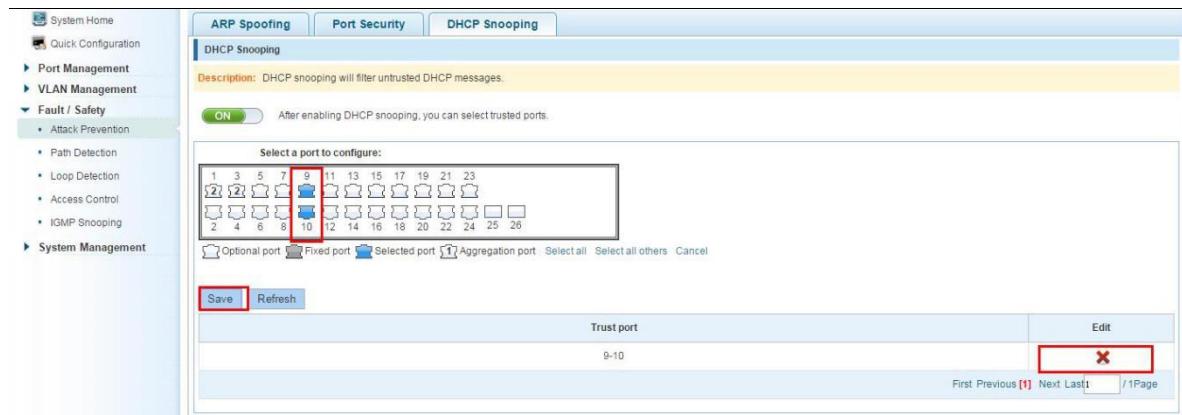


Figure 5-11: Disable anti illegal DHCP server functions

The activation of anti DHCP attack function, is the port setting for trust status;
Disable - preventing DHCP attack, is set to a non trusted state port.

5.1.3.4 Off anti DHCP attack function

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

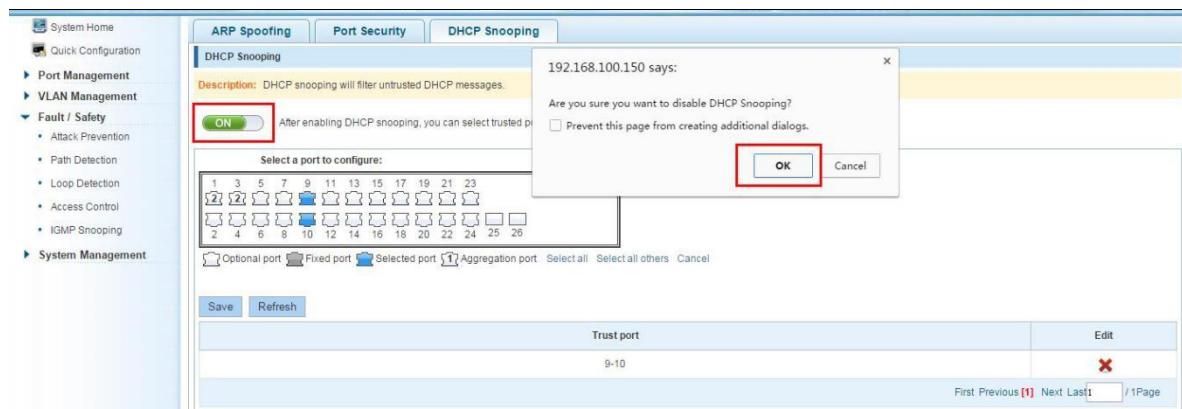


Figure 5-12: Off anti DHCP attack function

5.2 PATH DETECTION

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

The screenshot shows the LevelOne network management interface. The left sidebar has a tree structure with nodes like System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety (with Attack Prevention, Path Detection, Loop Detection, Access Control, IGMP Snooping), and System Management. The main content area has tabs for 'Path Detection' (selected) and 'Tracert Detection'. A yellow header bar says 'Description: Use the ping function to determine whether the network connection is functional and whether the host is reachable.' Below it is a form with 'Destination IP [192.168.100.1]' and a 'Start Test' button. A large empty box labeled 'Test Results' follows.

Figure 5-13: Path detection information

This screenshot shows the 'Tracert Detection' configuration page. The left sidebar is identical to Figure 5-13. The main content area has tabs for 'Path Detection' and 'Tracert Detection' (selected). A yellow header bar says 'Description: Tracert detection can detect to the destination through the gateway, the function is used to detect whether can reach the destination and the path to the destination, if a destination unreachable, diagnose problems. If the testing is a domain name, it may need to wait for a long time (2-3 minutes), please be patient.' Below it is a form with 'Destination IP or domain name [www.baidu.com]' and 'Timeout (1-10s) [10]'. A 'Start Test' button is present, along with a large empty 'Test Results' box.

Figure 5-14: Tracert detection information

5.3 LOOP DETECTION

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

This screenshot shows the 'Loop Detection' configuration page. The left sidebar includes a 'Loop Detection' node under the Fault / Safety category. The main content area has a tab for 'Loop Detection'. A yellow header bar says 'Description: Open the STP loop, not only can avoid the loop caused by the broadcast storm problem, and can provide link redundancy backup. Notice: If the user PC on the device to open the feature will lead to user PC1~2 minutes delay, so it is recommended only to open the STP loop in non access devices.' Below it is a form with 'The spanning tree state: [Enabled]' and a 'Save' button. A large empty 'Test Results' box is at the bottom.

Figure 5-15: View spanning tree configuration information

When the detected loop occurs when the port opened, after the port UP will automatically eliminate the loop.

5.3.1 TO CHANGE THE SPANNING TREE MODE

Click the button on the page, change the spanning-tree mode .click the "save" button to close the spanning tree:

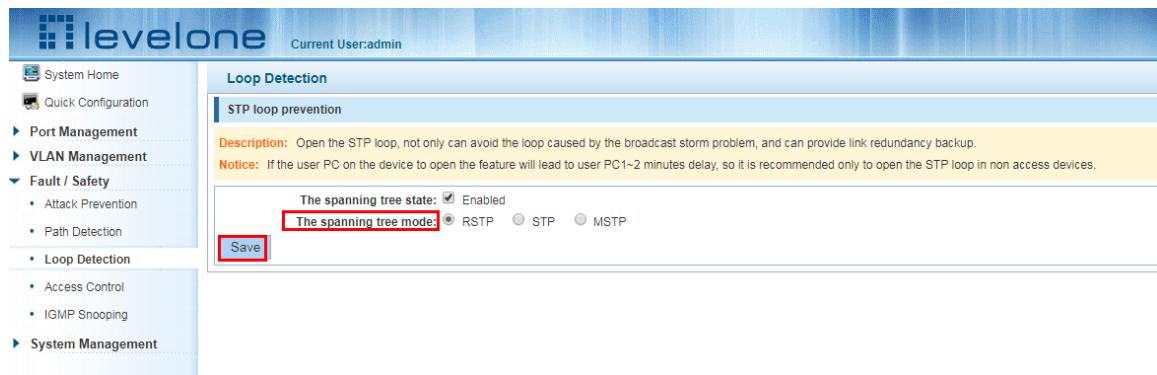


Figure 5-16: Changing the spanning tree pattern

5.3.2 CLOSE SPANNING TREE FUNCTION

Click the button on the page, click the "save" button to close the spanning tree:

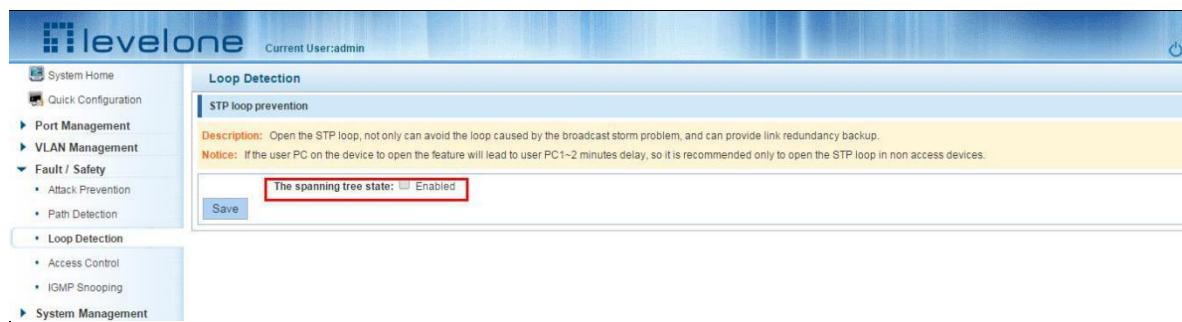


Figure 5-17: close the spanning tree pattern

5.4 ACCESS CONTROL

5.4.1 ACL ACCESS CONTROL LIST

5.4.1.1 view access control list

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

Figure 5-18: Access control list

5.4.1.2 Increased access rules

1. Increase the standard IP access rules

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

Figure 5-19 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 "Save" to complete the new:

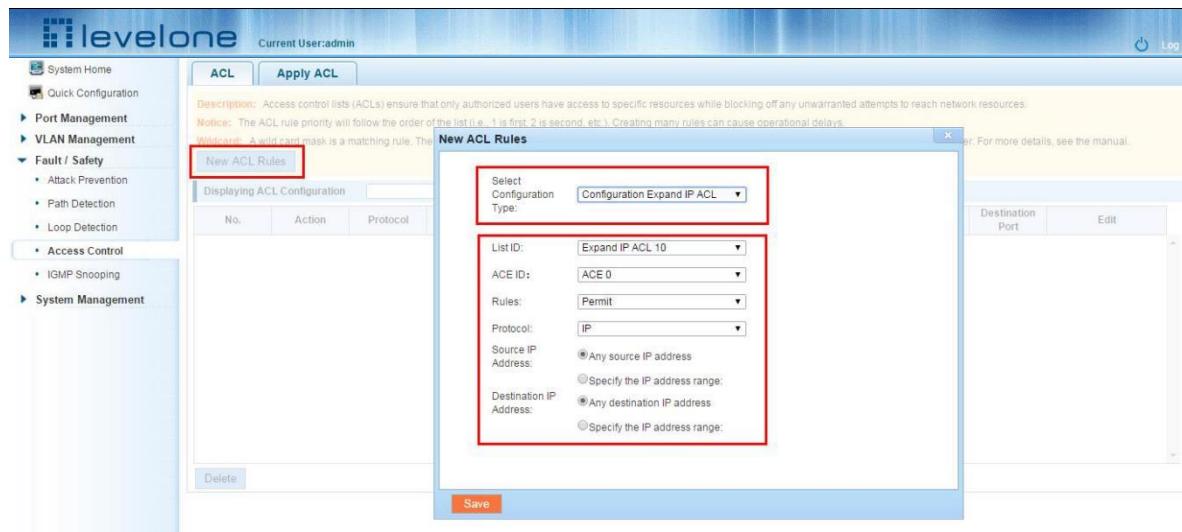


Figure 5-20: Configuration standard IP access control list

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 "Save" :

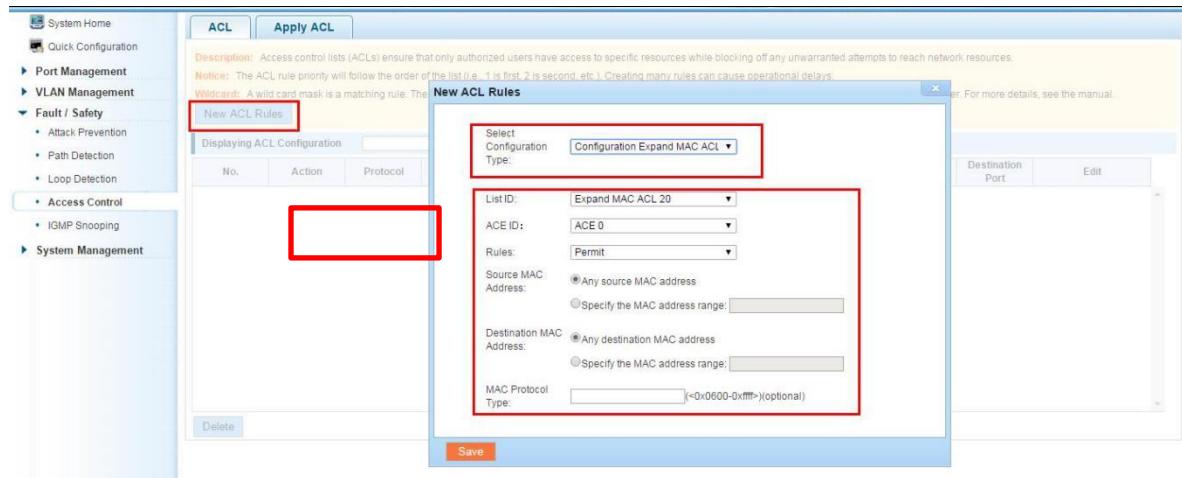


Figure 5-21: Configuration extended MAC access control list

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

5.4.1.3 Modify configuration

Rules for modifying port applications

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

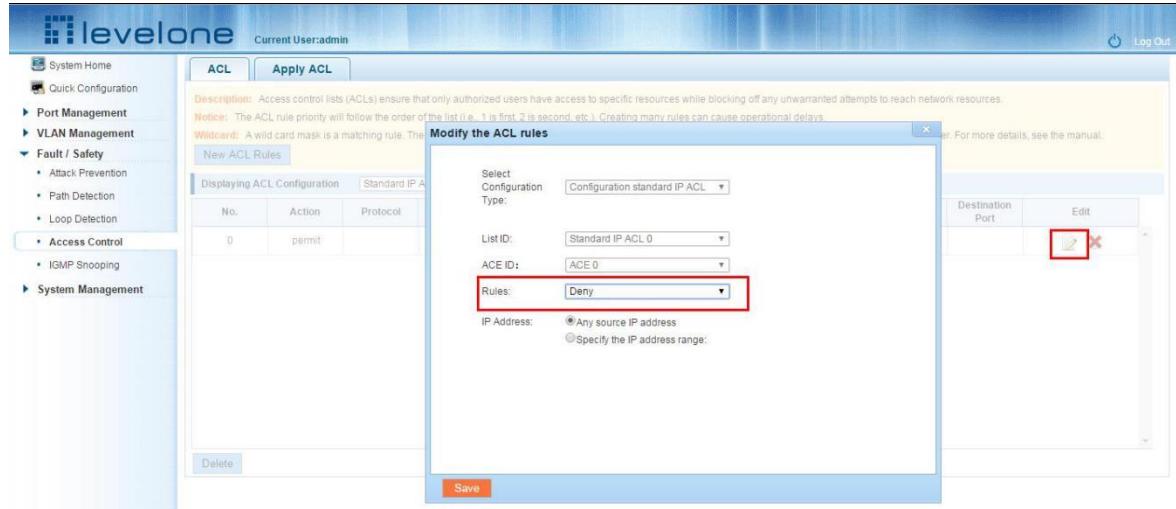


Figure 5-22: To modify the ACL rule

Configuration instructions

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

5.4.1.4 Delete rule

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

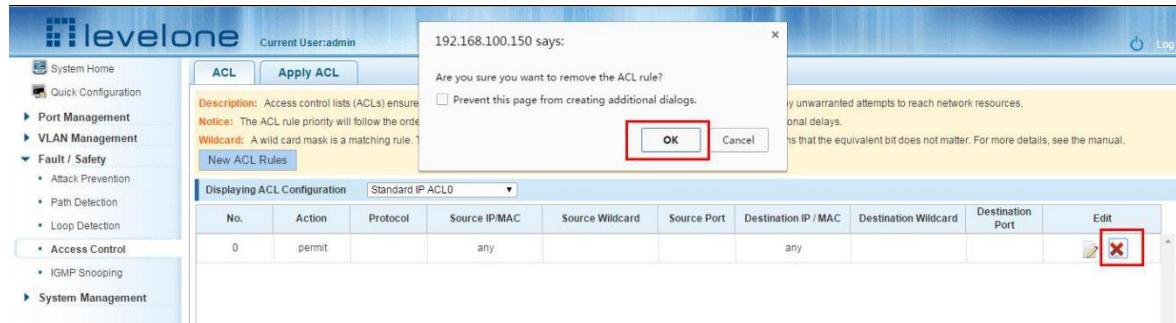


Figure 5-23: Delete rules

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

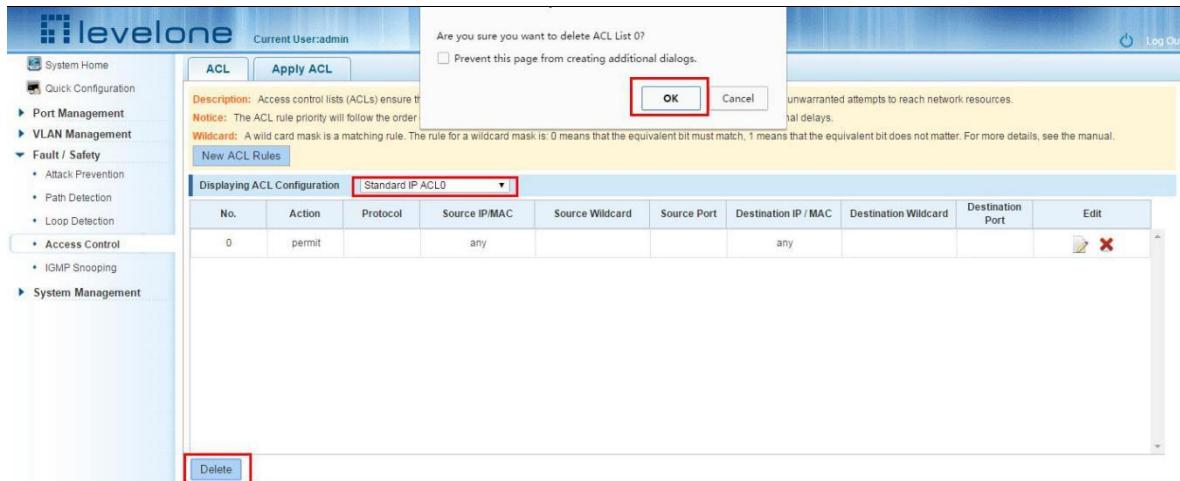


Figure 5-24: Delete ACL rules

Configuration instructions

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

5.4.2 APPLICATION ACL

5.4.2.1 View application ACL

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

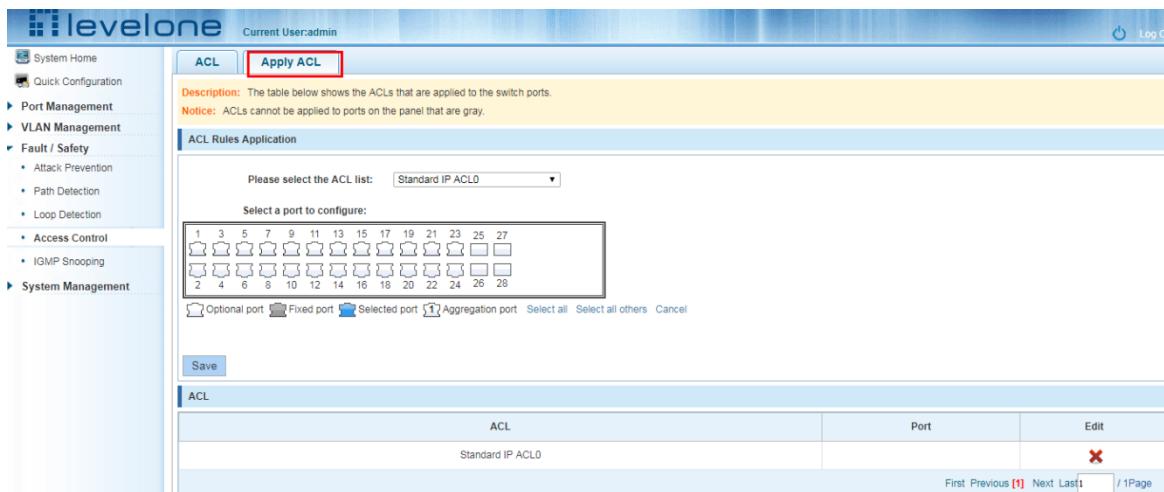


Figure 5-25: View application ACL rules

5.4.2.2 Increased application ACL

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

The screenshot shows the 'ACL Rules Application' section. It includes a dropdown menu for 'Please select the ACL list:' set to 'Standard IP ACL0'. Below it is a grid of 28 ports (1-28) with checkboxes. Ports 5 and 7 have their checkboxes selected and are highlighted with a red box. At the bottom of the grid are buttons for 'Optional port', 'Fixed port', 'Selected port' (highlighted with a red box), 'Aggregation port', 'Select all', 'Select all others', and 'Cancel'. A 'Save' button is also highlighted with a red box.

Figure 5-26: Add applications ACL

5.4.2.3 Delete application ACL

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

The screenshot shows a confirmation dialog box asking 'Are you sure you want to remove the ACL rule?' with 'ok' and 'cancel' buttons, where 'ok' is highlighted with a red box. Below the dialog is the 'ACL Rules Application' section with the same interface as Figure 5-26. At the bottom of the main interface is a table:

ACL	Port	Edit
Standard IP ACL0	5,7	

Below the table are buttons for 'First', 'Previous [1]', 'Next', 'Last', and '1/1Page'.

Figure 5-27: Delete application ACL

5.5 IGMP SNOOPING

5.5.1 VIEW IGMP SNOOPING CONFIGURATION

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

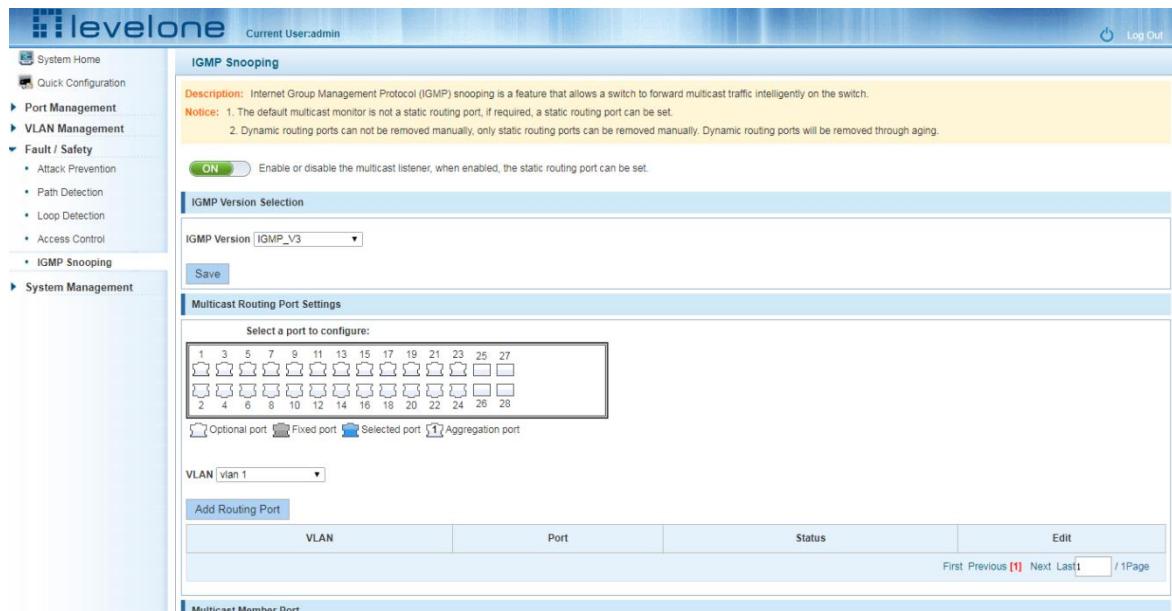


Figure 5-28: View Snooping IGMP configuration information

5.5.2 ACTIVE MULTICAST LISTENER FUNCTION

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



Figure 5-29: Open multicast listener configuration

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

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

The default version of V2 - IGMP.

5.5.3 DISABLE MULTICAST LISTENER FUNCTION

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

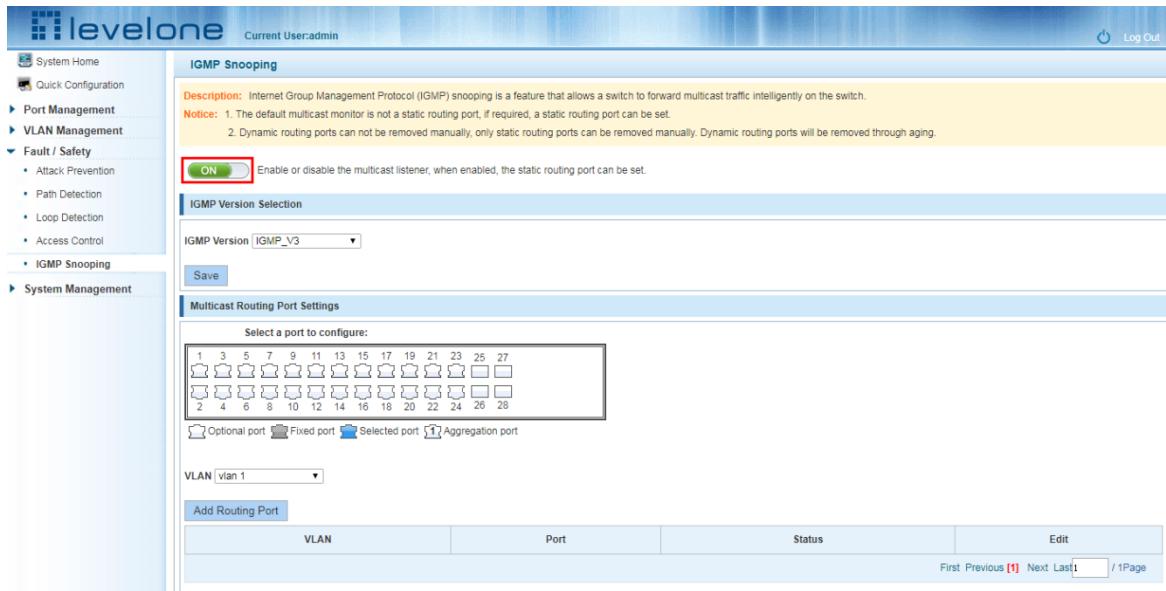


Figure 5-30: Closed multicast listener function operation

5.5.4 CONFIGURATION MULTICAST ROUTING

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

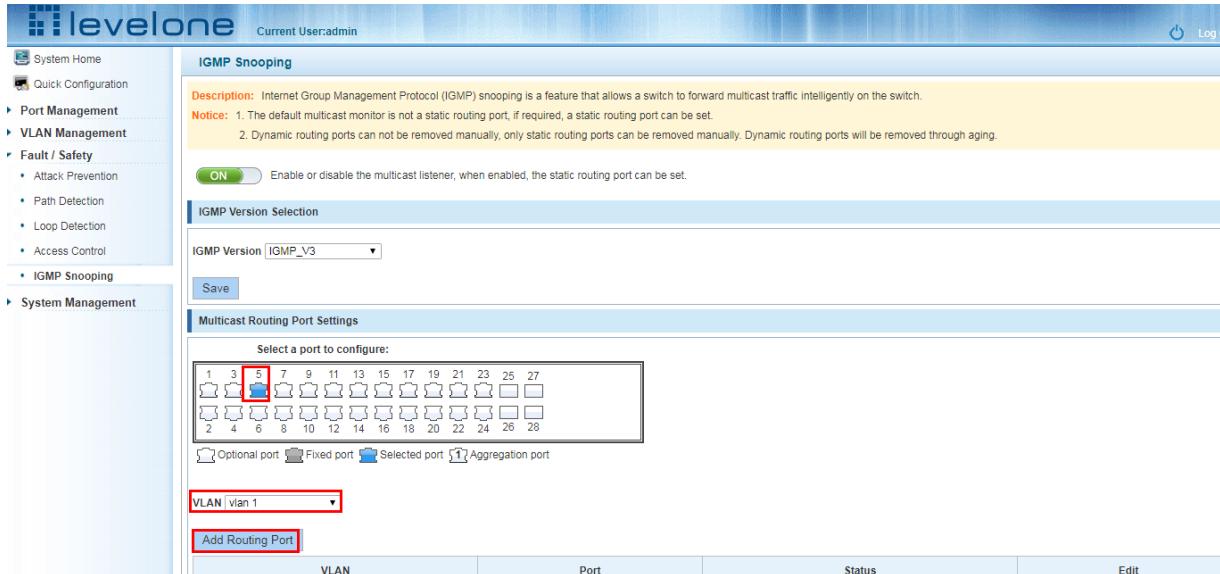


Figure 5-31: Configuration of multicast routing

Multicast routing configuration steps are as follows:

Step1:In the port panel to select multicast listener routing port;

step2:Select vlan;

Step3:Click on the "Add Router Port" button to complete the configuration.

5.5.5 IGMP VERSION

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

The screenshot shows the 'IGMP Snooping' configuration page. In the 'IGMP Version Selection' section, the 'IGMP Version' dropdown is set to 'IGMP_V3'. In the 'Multicast Routing Port Settings' section, there is a grid of ports numbered 1 to 28. Port 1 is highlighted as a 'Selected port'. Below the grid, there are icons for 'Optional port', 'Fixed port', 'Selected port', and 'Aggregation port'. A 'VLAN' dropdown menu is open, showing 'vlan 1'.

Figure 5-32: Configuration IGMP version

IGMP version configuration steps are as follows:

Step1:Select the required version number;

step2:Click the "Save" button to complete the configuration.

6 SYSTEM MANAGEMENT

6.1 SYSTEM SETTINGS

6.1.1 MANAGEMENT VLAN

6.1.1.1 configuration Basic System Settings

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

The screenshot shows the 'Basic System Settings' page under 'Management VLAN'. It includes fields for Management VLAN (set to 'vlan 1'), DHCP (set to 'Static Allocation'), Management IP (192.168.100.150), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), MAC (00B0.4C00.0000), Device Name (Switch), Device Location, Contact Name, and Login Timeout (1800).

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 192.168.100.52
3. In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.0
4. In the Gateway Address text box to enter the gateway address, such as 192.168.100.1
5. In the Device Name text box ,enter the Device Name ,such as dx
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 john
8. In the Contact Information text box ,enter Contact Information ,such as 12345678900
9. Click on "Save Settings" button to complete the configuration

6.1.1.2 SYSTEM TIME SYNCHRONIZATION

The screenshot shows the 'Basic System Settings' and 'System time synchronization' sections of the web interface. The 'Basic System Settings' section contains fields for Management VLAN (vlan 1), MAC (00B0.4C00.0000), Device Name (Switch), Device Location, Contact Name, and Contact Information. The 'System time synchronization' section shows the current system time (2000-01-01 00:09:58) and an SNTP server IP address field. A red box highlights the 'Synchronize' button at the bottom.

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.

6.1.2 SYSTEM RESTART

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

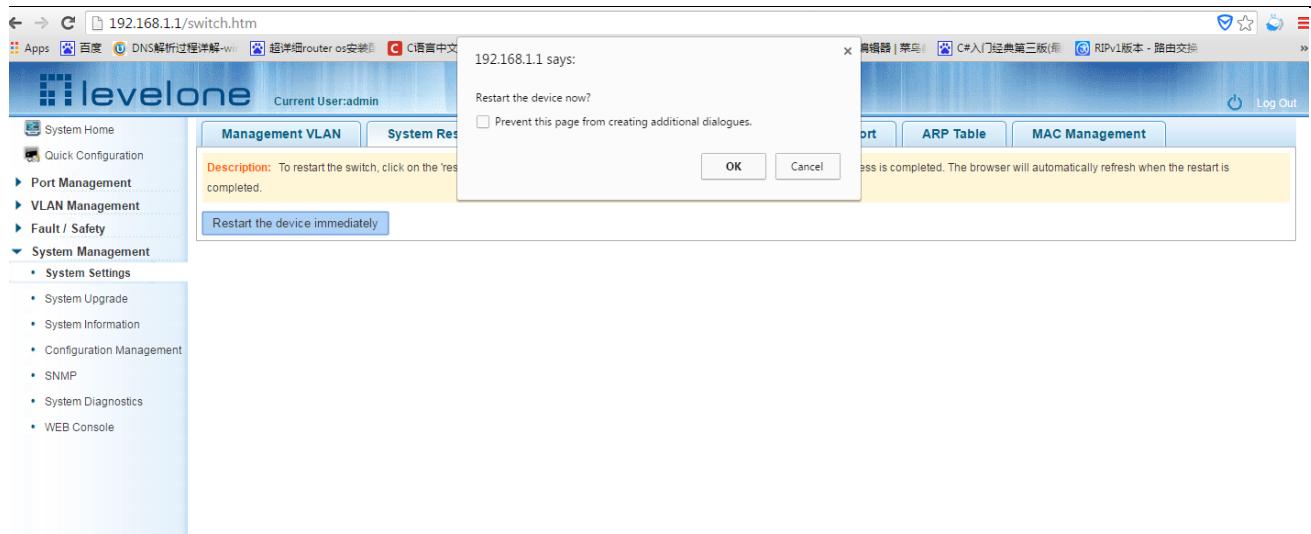


Figure 6-3: System Restart

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 CHANGE PASSWORD

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

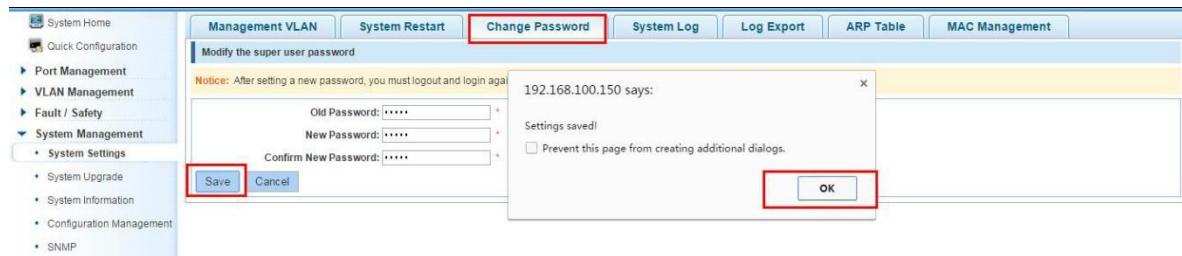


Figure 6-4: change password

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

6.1.4 SYSTEM LOG

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

Figure 6-5: system log

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

6.1.5 LOG EXPORT

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

Figure 6-6: 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:

IP	MAC
192.168.1.51	40:16:7E:B1:EB:6D

Figure 6-7: ARP message

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

6.1.7 MAC MANAGEMENT

6.1.7.1 MAC address lookup

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

User MAC	Port	Port Type	VLAN	Edit
0001.7A55.E7DE	1	Dynamic	1	
1060.4B6E.E76F	1	Dynamic	1	
1C1C.0248.AAB6	1	Dynamic	1	
4016.7EB1.EB6D	1	Dynamic	1	
7427.EA30.6925	1	Dynamic	1	
7427.EA36.DD67	1	Dynamic	1	
80C1.6EDF.AF7A	1	Dynamic	1	
BCEE.7B9A.D4FE	1	Dynamic	1	
BCEE.7B9A.D552	1	Dynamic	1	

Figure 6-8: MAC address lookup display

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

- 1.User MAC: MAC address of the switch that currently exists is displayed;
- 2.Port: Displays the source port number of the MAC address;
- 3.Port Type: There are two types of dynamic and static;
- 4.VLAN: VLAN ID display value.

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

6.1.7.2 Add a static MAC address type

1.Use manual binding MAC address

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

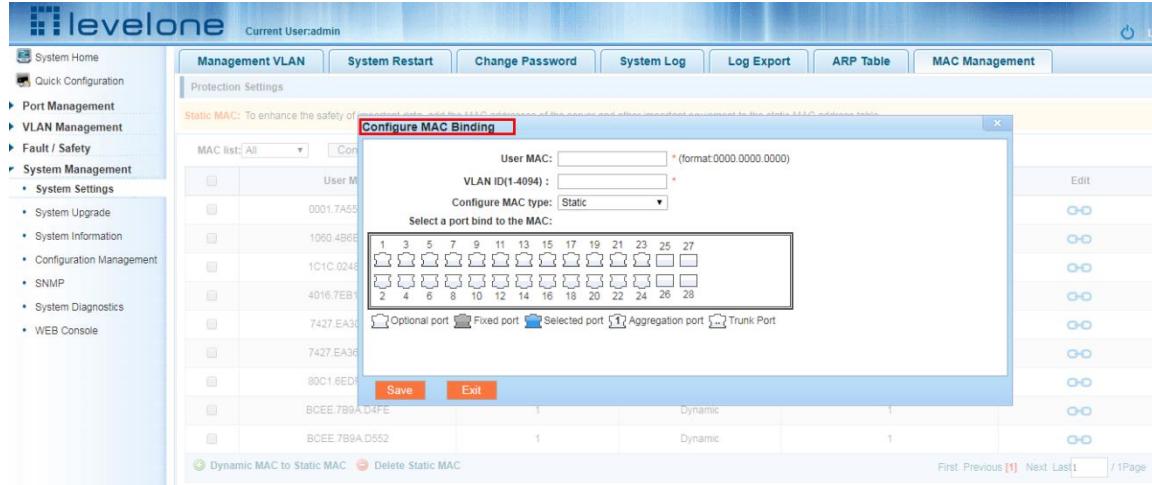


Figure 6-9: MAC addresses statically bound static configuration

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;

step5:Click on "save"to complete the configuration.

2.Use “” Button binding static MAC address

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

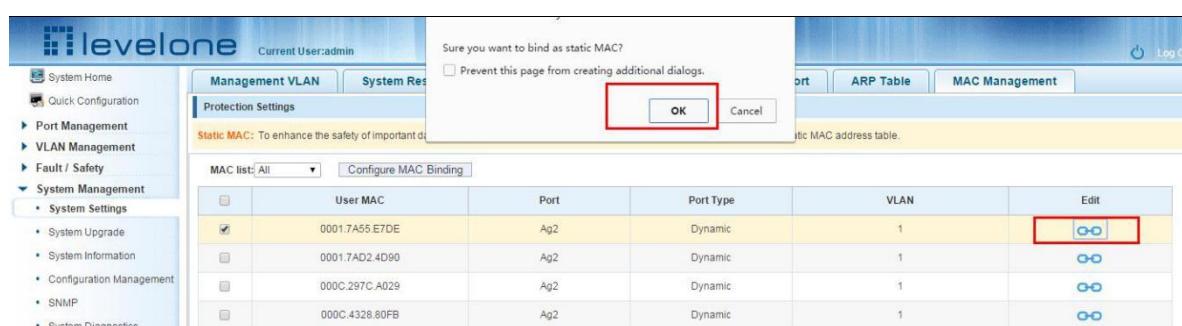


Figure 6-10: MAC address of the static binding configuration

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

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

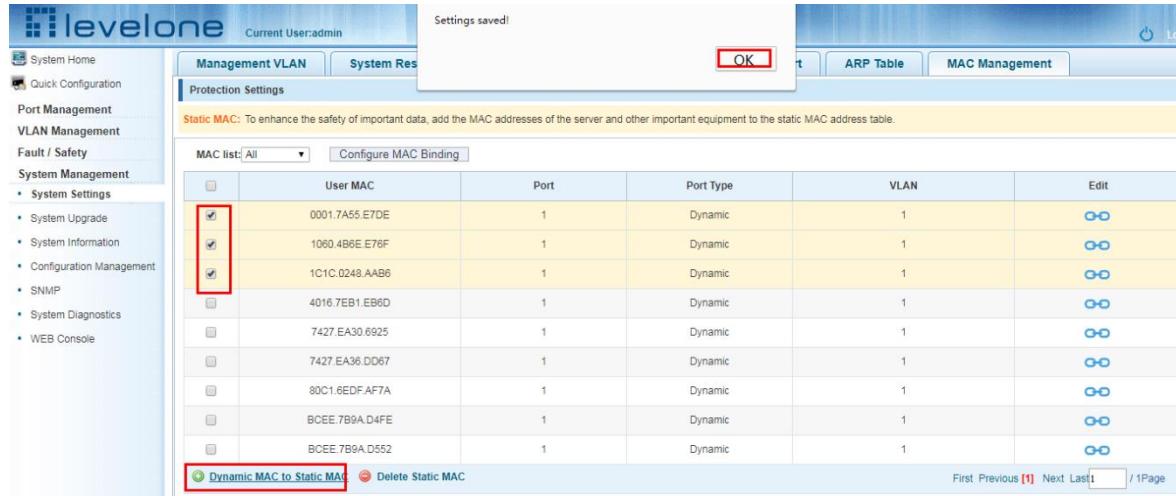


Figure 6-11: Batch-MAC binding configuration

6.1.7.3 Remove the static MAC address type

1. Single MAC records are deleted

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

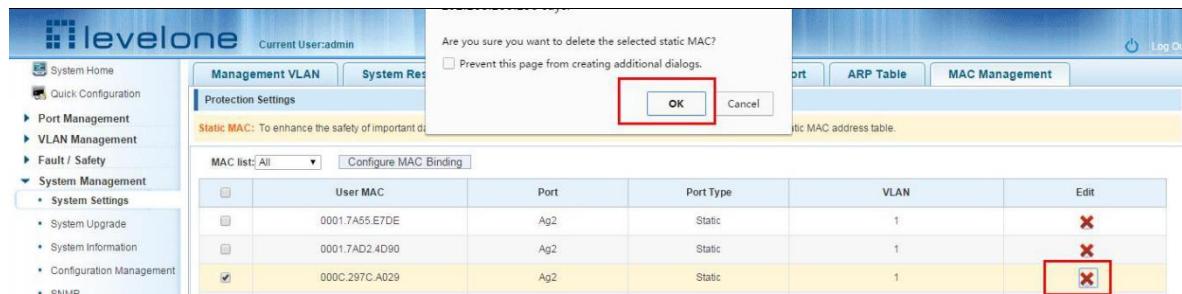


Figure 6-12: MAC address deletion

Remove MAC address configuration steps are as follows:

Step1:To delete the selected MAC address;

step2:Click "X" button to delete the configuration

2. Batch delete a static MAC address

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

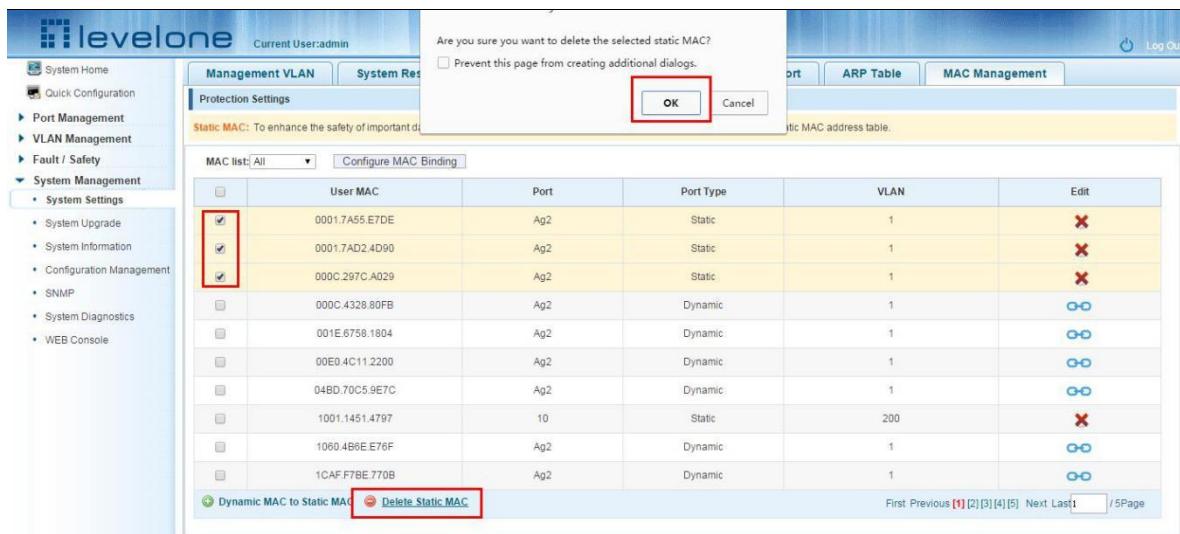


Figure 6-13: MAC address batch deletion

6.2 SYSTEM UPGRADE

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

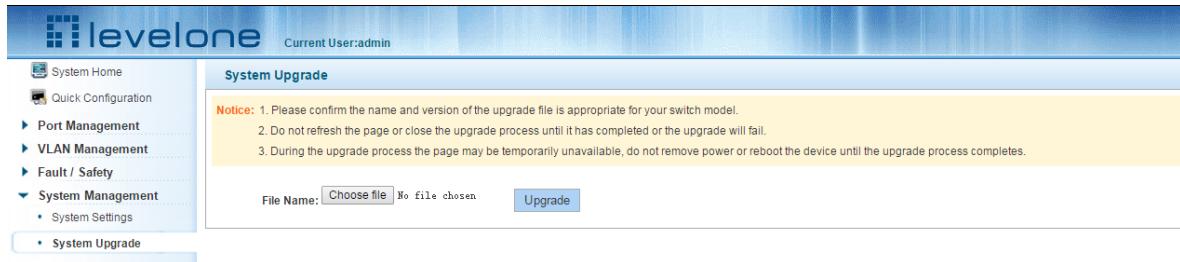


Figure 6-14: Switch System Upgrade

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 MEMORY INFORMATION

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

Memory Information

CPU Information

Description: Display system memory information.

System Memory Information

	total (KB)	used (KB)	free (KB)	shared (KB)	buffer (KB)	cache (KB)
Mem:	127384	54640	72744	0	1708	22272
-/+ buffers/cache:		30660	96724			
Swap:	0	0	0			

Figure 6-15: System memory information

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

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:

Memory Information

CPU Information

Description: Display system CPU information.

CPU Information

	PID	USER	STATUS	RSS	PPID	%CPU	%MEM	COMMAND
CPU:	47	root	RN<	0	1	3.8	0.0	WA Monitor Thre
	571	root	S	6240	570	0.0	4.8	cli
	573	root	S	6240	572	0.0	4.8	cli
	572	root	S	6240	571	0.0	4.8	cli
	196	root	S	1328	1	0.0	1.0	ksuid
	203	root	S	1328	196	0.0	1.0	ksuid
	212	root	R	1300	1	0.0	1.0	polld
	192	root	S	340	1	0.0	0.2	dhcpc6c
	570	root	S	304	569	0.0	0.2	sh
	576	root	S	304	573	0.0	0.2	sh
	569	root	S	296	1	0.0	0.2	sh
	202	root	S	292	1	0.0	0.2	syslogd
	1	root	S	280	0	0.0	0.2	init
	208	root	S	220	1	0.0	0.1	klogd
	211	root	S	208	1	0.0	0.1	inetd
	79	root	RN<	0	1	0.0	0.0	MSTP FSM Thread
	61	root	SW<	0	1	0.0	0.0	Port Statistics
	64	root	SW<	0	1	0.0	0.0	Rev ACL Rate Ch
	63	root	SW<	0	1	0.0	0.0	L2 Routine Thre

Figure 6-16: 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.

6.4 CONFIGURATION MANAGEMENT

6.4.1 CONFIGURATION MANAGEMENT

1. To see the current configuration

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

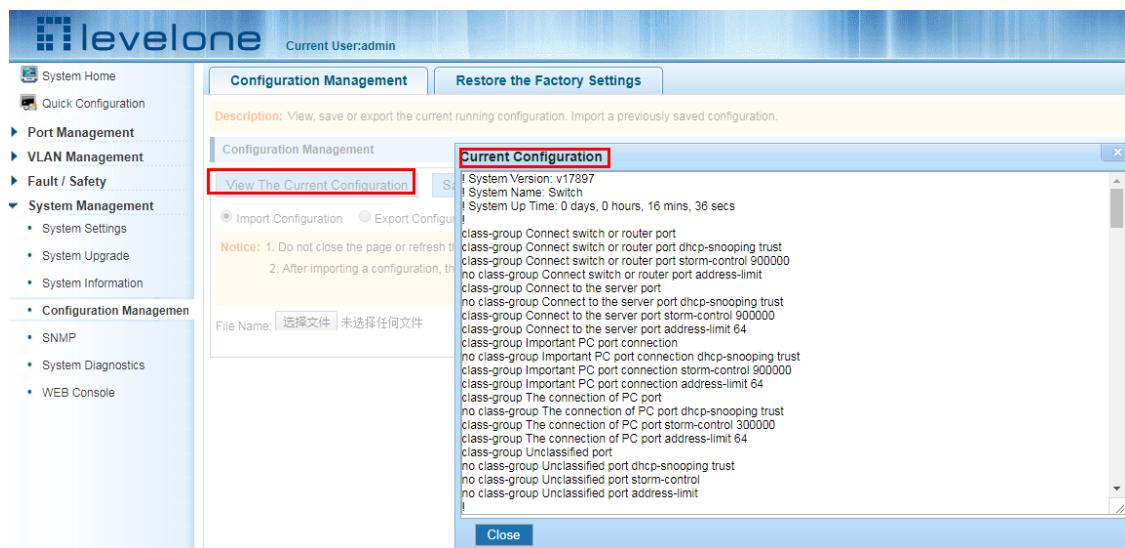


Figure 6-17: View the current configuration

2. Save the current configuration

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

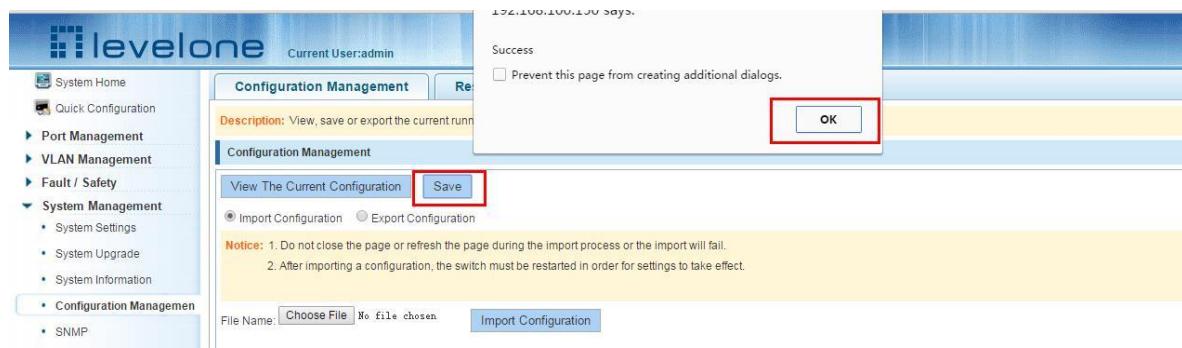


Figure 6-18: To save the current configuration

3. The configuration

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



Figure 6-19: Imported configuration

Import the configuration steps are as follows:

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

4. Export configuration

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



Figure 6-20: Export configuration

6.4.2 RESTORE FACTORY SETTINGS

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

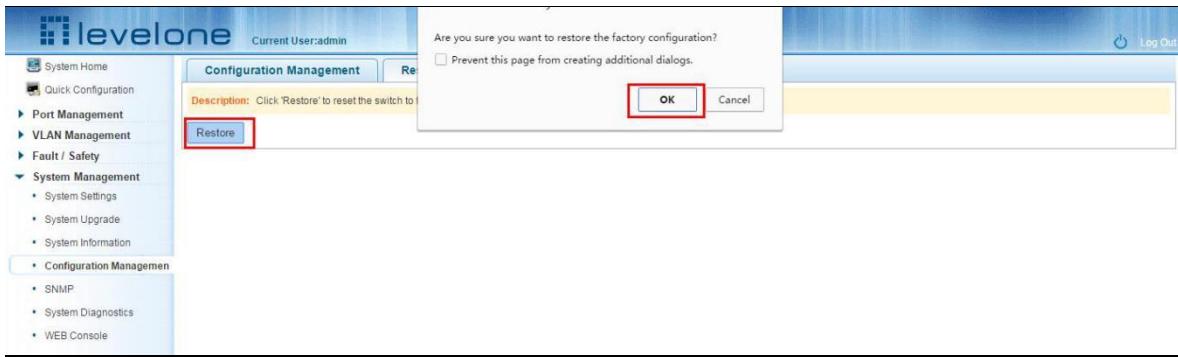


Figure 6-21: Restore factory Settings

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.

6.5 SNMP

6.5.1 CHECK THE SNMP

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

Community Name	Permissions	Remove
private	RW	X
public	RO	X

Figure 6-22: 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.

6.5.2 ACTIVATE THE SNMP

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

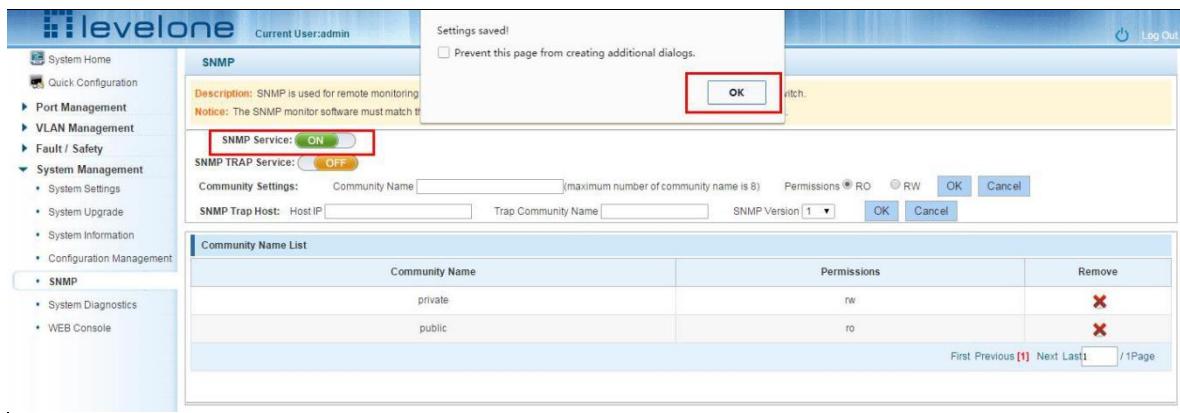


Figure 6-23: Activation SNMP function

Activation function SNMP configuration steps are as follows:

Step1:Choose open SNMP options;

step2:Click "OK" button to complete the configuration.

6.5.3 TO DISABLE THE SNMP

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

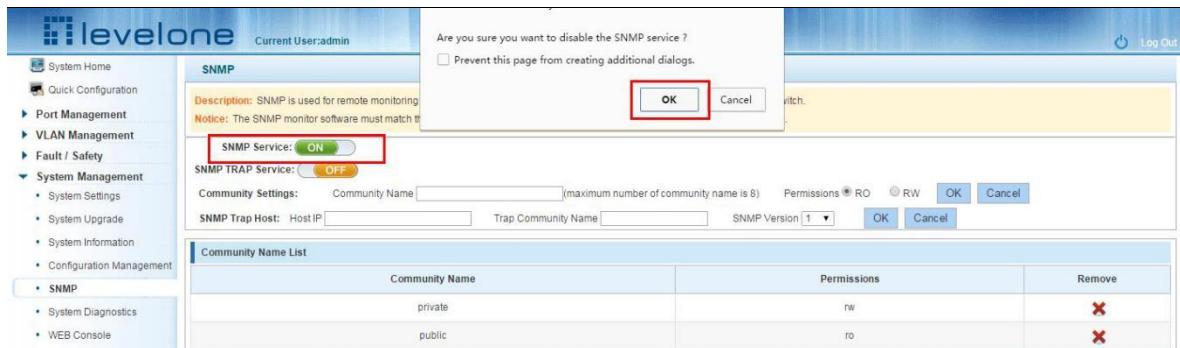


Figure 6-24: Disable the SNMP function

Disable the SNMP function configuration steps are as follows:

Step1:Choose close SNMP options;

step2:Click "OK" button to complete the configuration.

6.5.4 ACTIVATE THE TRAP

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

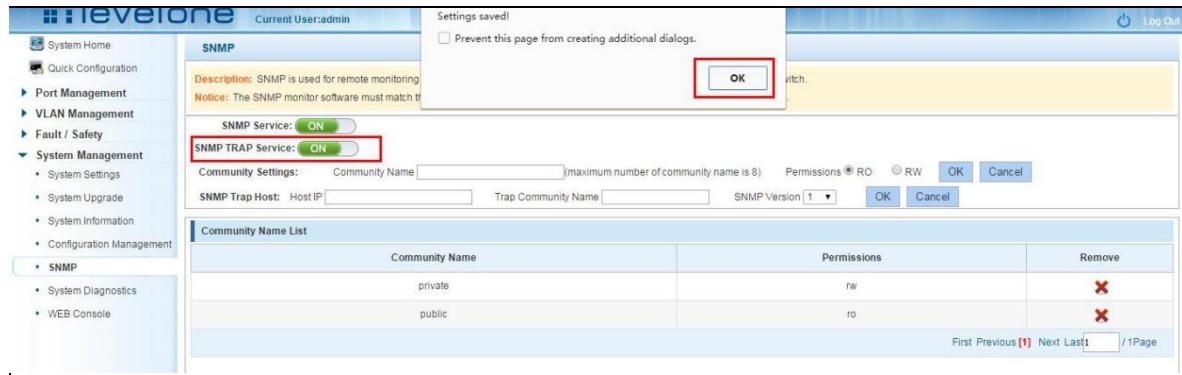


Figure 6-25: Activation function of the TRAP

Activate the TRAP function configuration steps are as follows:

Step1:Select "ON" option;

step2:Click "OK" button to complete the configuration.

6.5.5 DISABLE THE TRAP

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

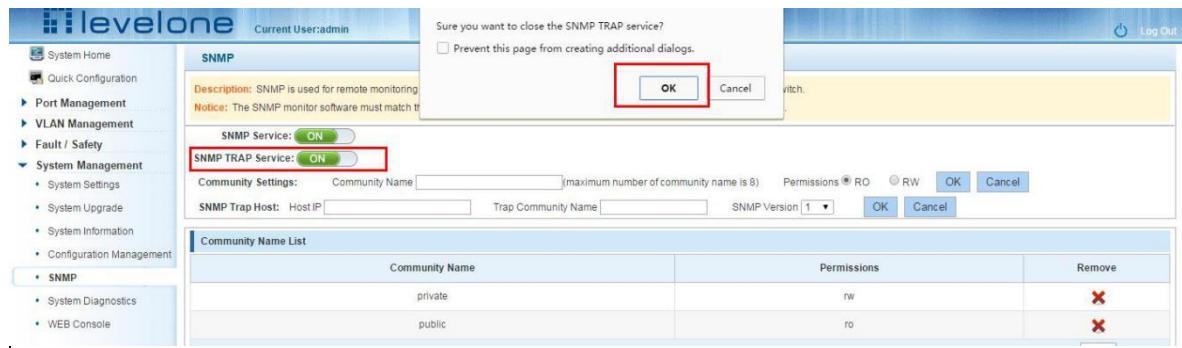


Figure 6-26: Disable TRAP function

Disable the TRAP function configuration steps are as follows:

Step1: Select "ON" to "OFF" option;

step2:Click "OK" button to complete the configuration.

6.5.6 INCREASE OF COMMUNITY

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

SNMP

Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMP Service' switch.
Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communication failure.

SNMP Service: ON

SNMP TRAP Service: ON

Community Settings: Community Name: (maximum number of community name is 8) Permissions: RO RW OK Cancel

SNMP Trap Host: Host IP: Trap Community Name: SNMP Version: OK Cancel

Figure 6-27: Increase community

Community Name	Permissions	Remove
private	rw	<input type="button"/>
pub	ro	<input type="button"/>
public	ro	<input type="button"/>

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

Figure 6-28: Community results

Increase community configuration steps are as follows:

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

step2: Select "RO" permissions;

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

6.5.7 DELETE THE COMMUNITY NAME

Click on the "System Management" "SNMP", in the community list choose need to delete the object, click “” finish configuration:

Community Name	Permissions	Remove
private	rw	<input type="button"/>
pub	ro	
public	ro	

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

Figure 6-29: Delete community

6.5.8 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:

System Home
Quick Configuration
Port Management
VLAN Management
Fault / Safety
System Management
System Settings
System Upgrade
Guidelines Information

SNMP

Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMP Service' switch.
Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communication failure.

SNMP Service: **ON**
SNMP TRAP Service: **ON**

Community Settings: Community Name: (maximum number of community name is 8) Permissions: RO RW OK Cancel

SNMP Trap Host: Host IP: 192.168.100.83 Trap Community Name: pub SNMP Version: 1 OK Cancel

Figure 6-30: Increases the SNMP TRAP service host

Trap Community Name	IP	Version	Remove
pub	192.168.100.83	SNMP Ver v2c	

First Previous [1] Next Last 1 / 1 Page

Figure 6-31: SNMP TRAP service host

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

- Step1: In the host IP dialog box input: 192.168.100.83;
- Step2: In TRAP community name dialog input: public;
- Step3: Select the SNMP version: V2C;
- Step4: Click on "OK" button, complete the configuration.

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

6.5.9 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:

Trap Community Name	IP	Version	Remove
pub	192.168.100.83	SNMP Ver v2c	

First Previous [1] Next Last 1 / 1 Page

Figure 6-32: Delete community

6.6 SYSTEM DIAGNOSTICS

Click on the "System Management" "System Diagnostics", can collect the equipment failure information.

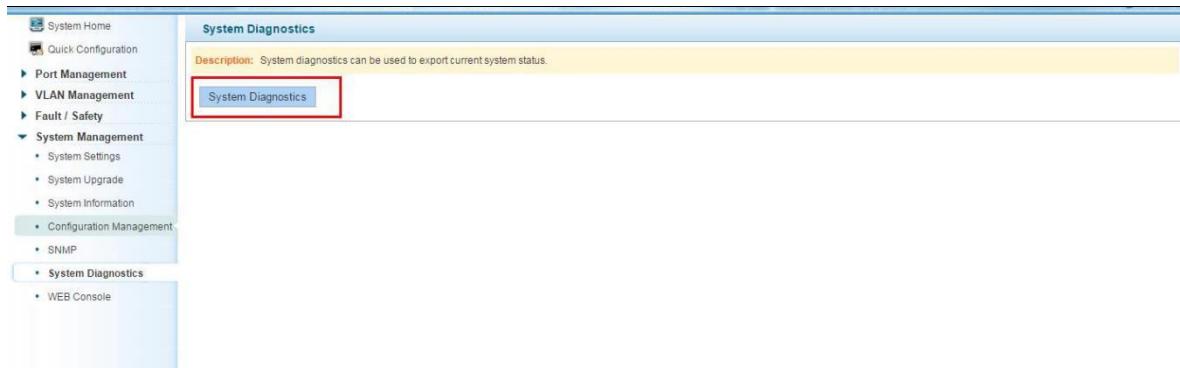


Figure 6-33: Key fault collection

6.7 THE WEB CONSOLE

Click on the "System Management" "WEB Console", can enter commands for operating equipment.

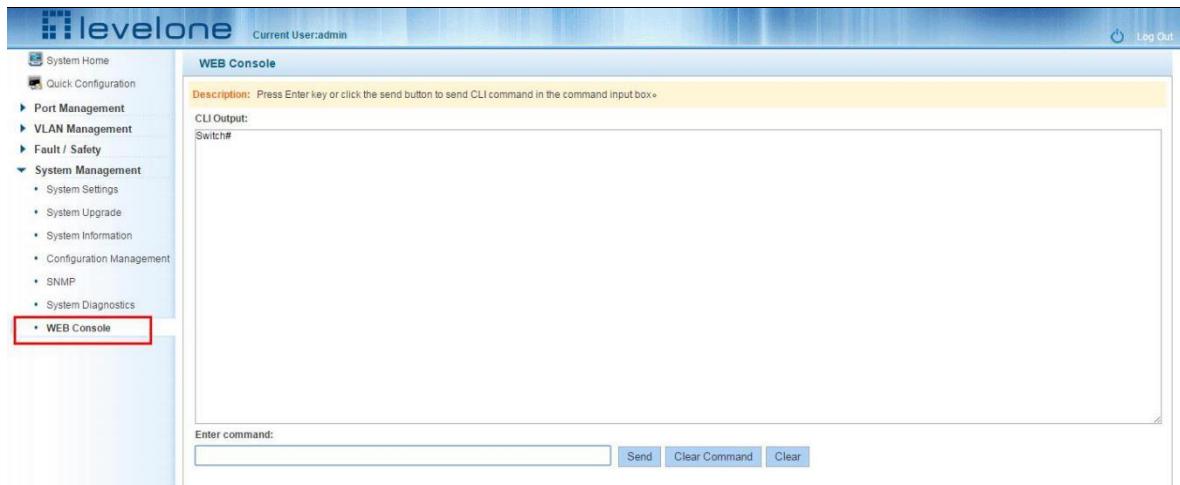


Figure 6-34: Web console

Input in the input box legal name, such as: the show version click on the Send button, Send the Command, if the input error Command, click on the button to Clear the Command to remove the current haven't Send orders, Clear the contents of the orders after click the Clear button.

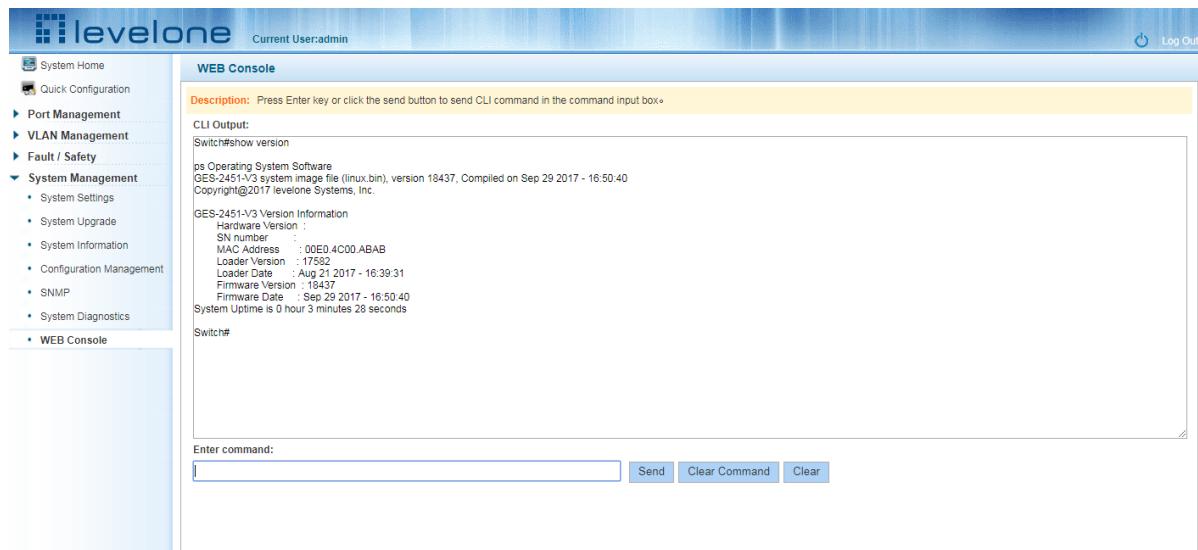


Figure 6-35: Web console operation