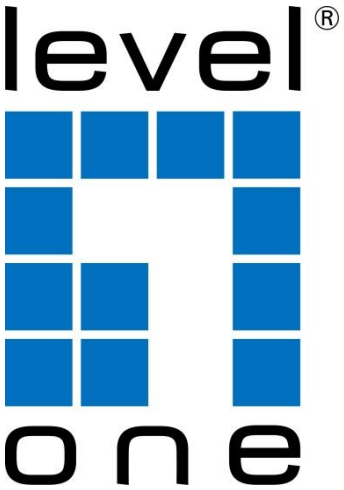


LevelOne

User Manual

GES-2451

26-Port Web Smart Gigabit Switch

TABLE OF CONTENTS

1 WEB MANAGEMENT LANDING PAGE

1.1 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB

Configuration computer's IP address and the switch must be set to the same subnet (switch default IP address is 192.168.1.1, 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

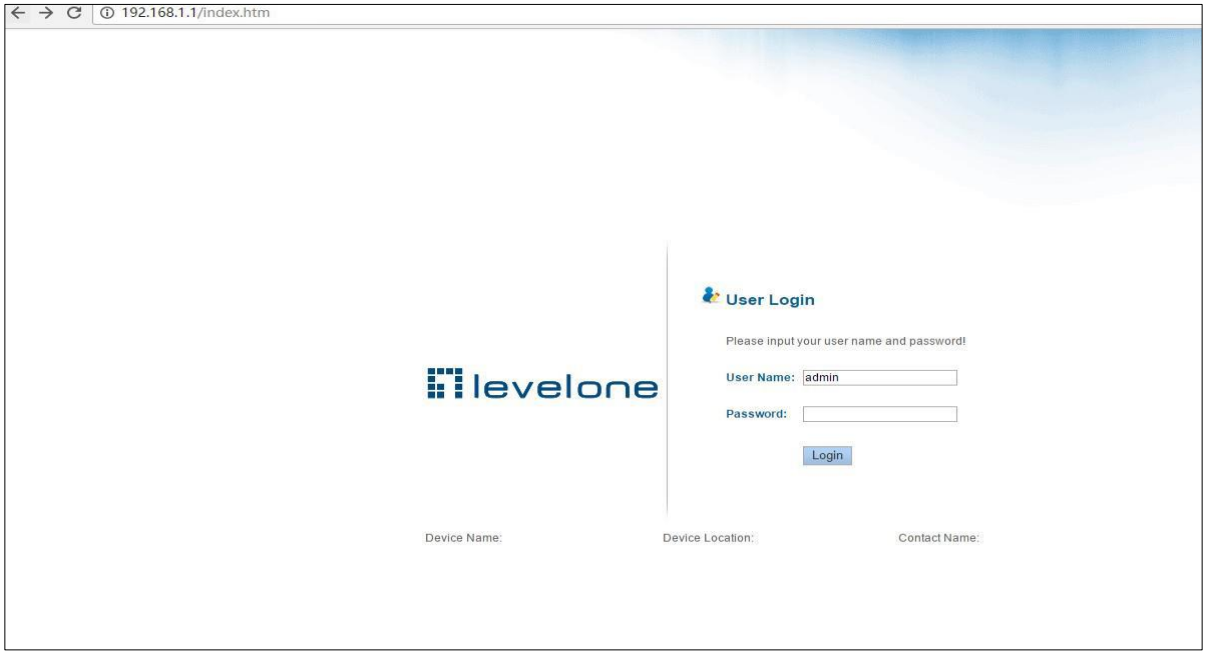


Figure 1-1: The login page WEB

After landing successfully, the switch management page WEB page:

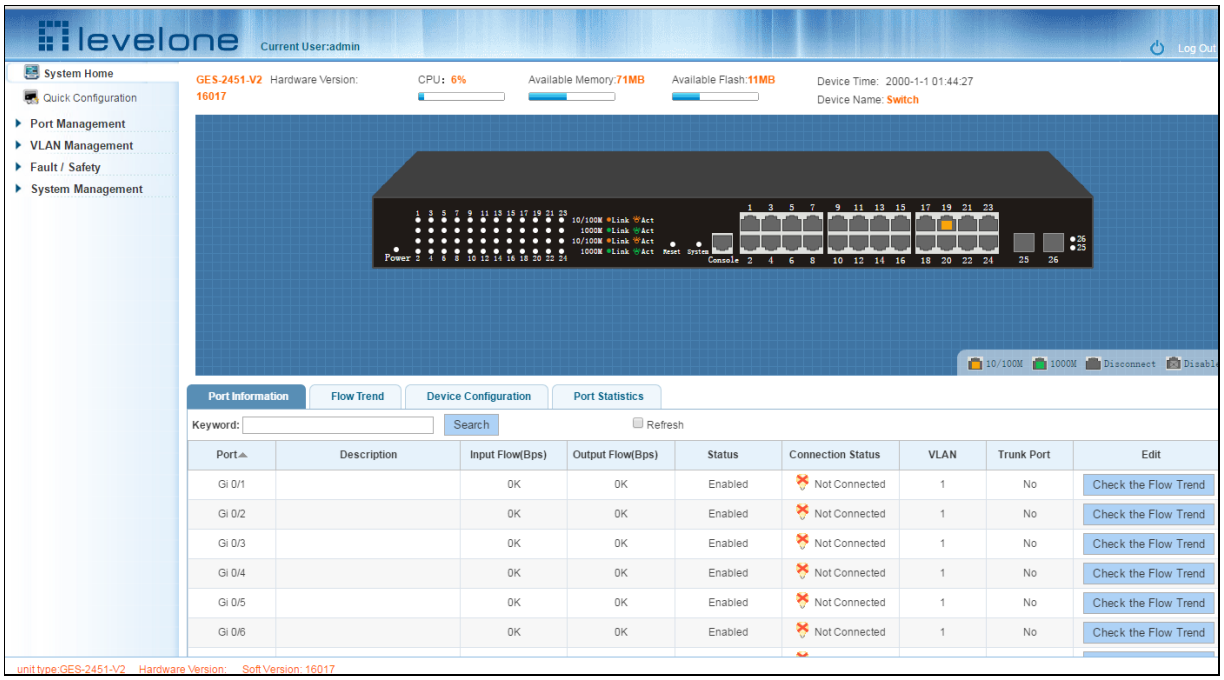


Figure 1-2: switch WEB management page Home

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".

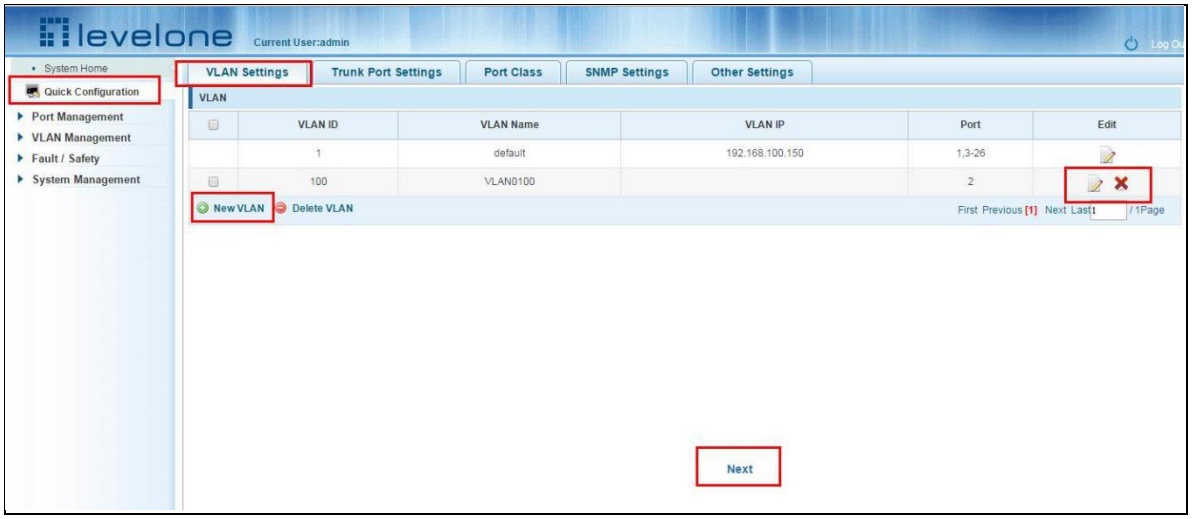


Figure 2-1: VLAN Setting

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.

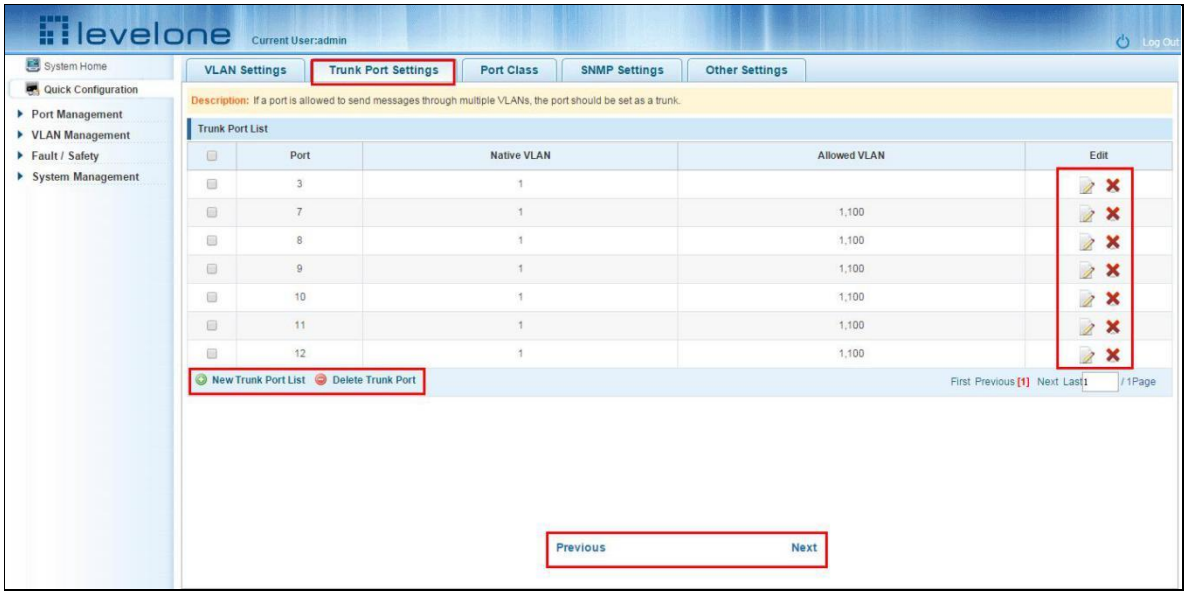


Figure 2-2: Trunk Port Setting

2.3 PORT CLASS

Click on "Quick Configuration" "Port Class" into the Port Class of Quick Configuration Settings page. can view the current equipment configuration information, and according to the demand of new a classification of port , modify port class, configure port class such as after configuration is complete, click "Next" to enter the SNMP Settings page. Or click on "Previous" back to the TRUNK Port Settings page.

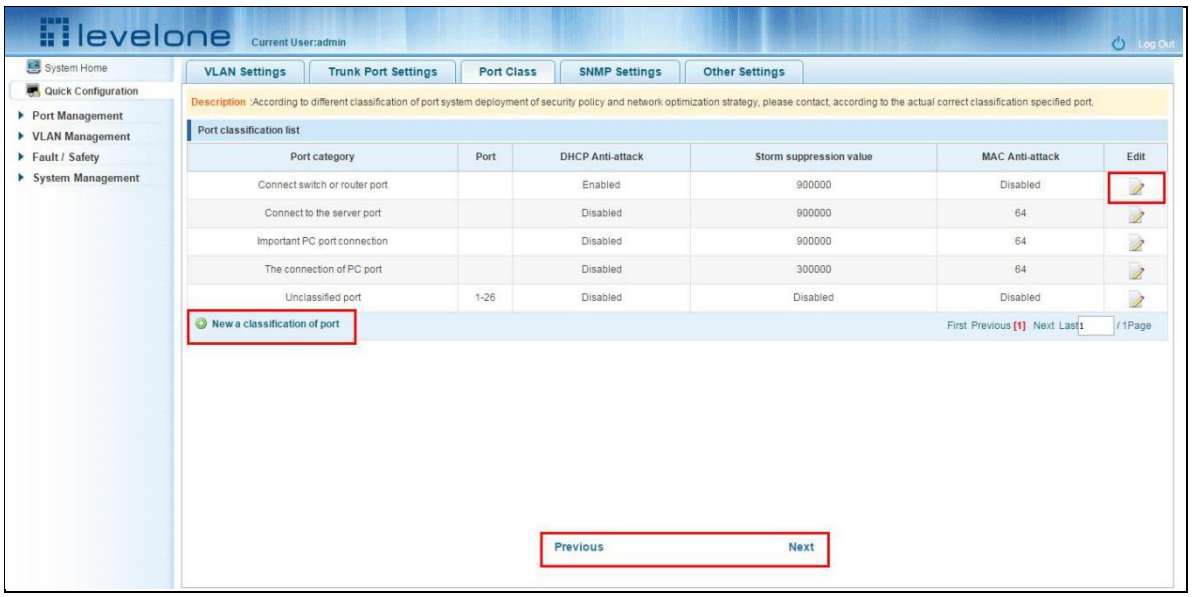


Figure 2-3: Port Class

2.4 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.

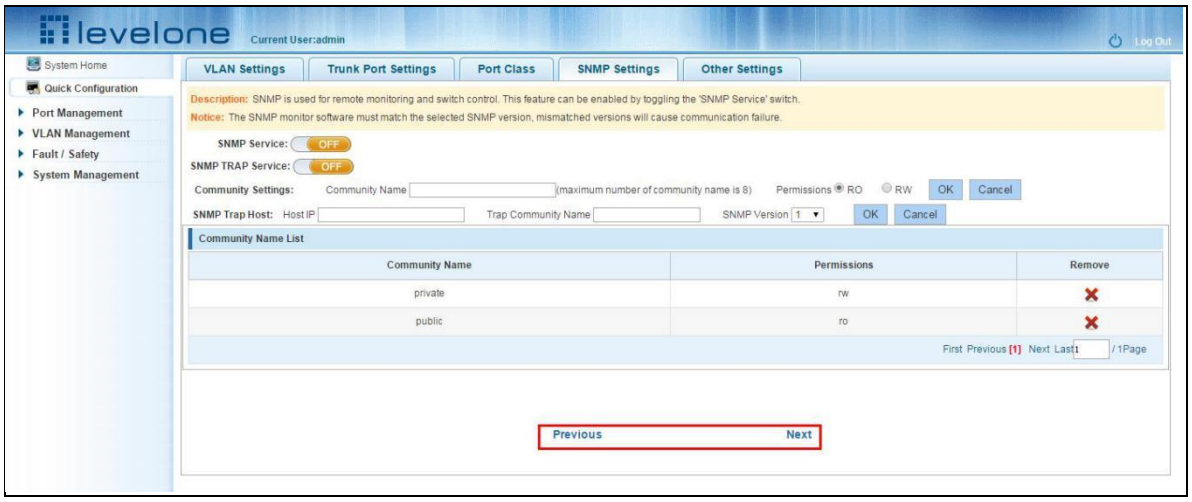


Figure 2-4: SNMP Setting

2.5 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.

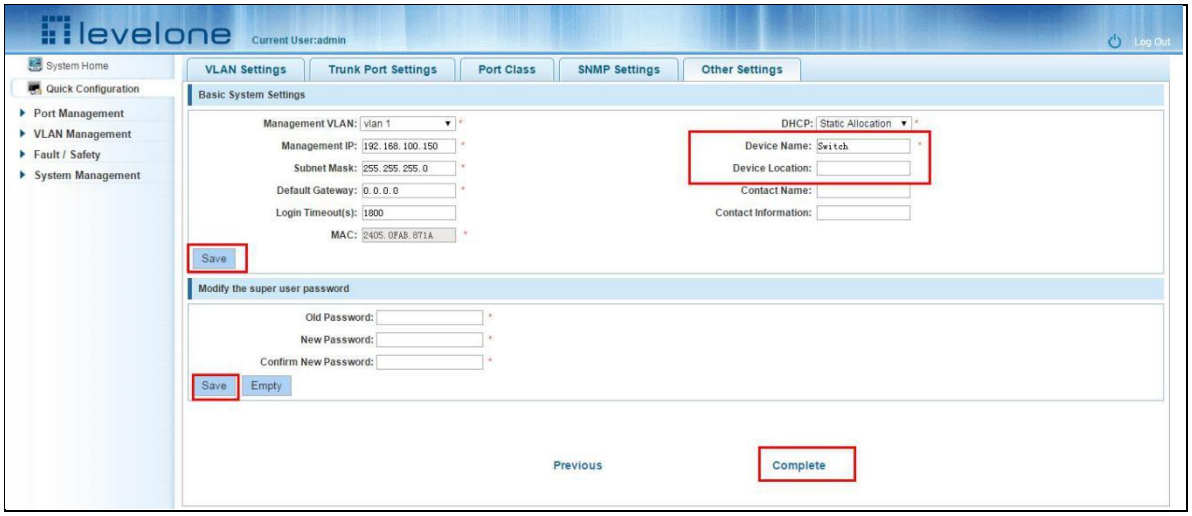


Figure 2-5: other settings

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:

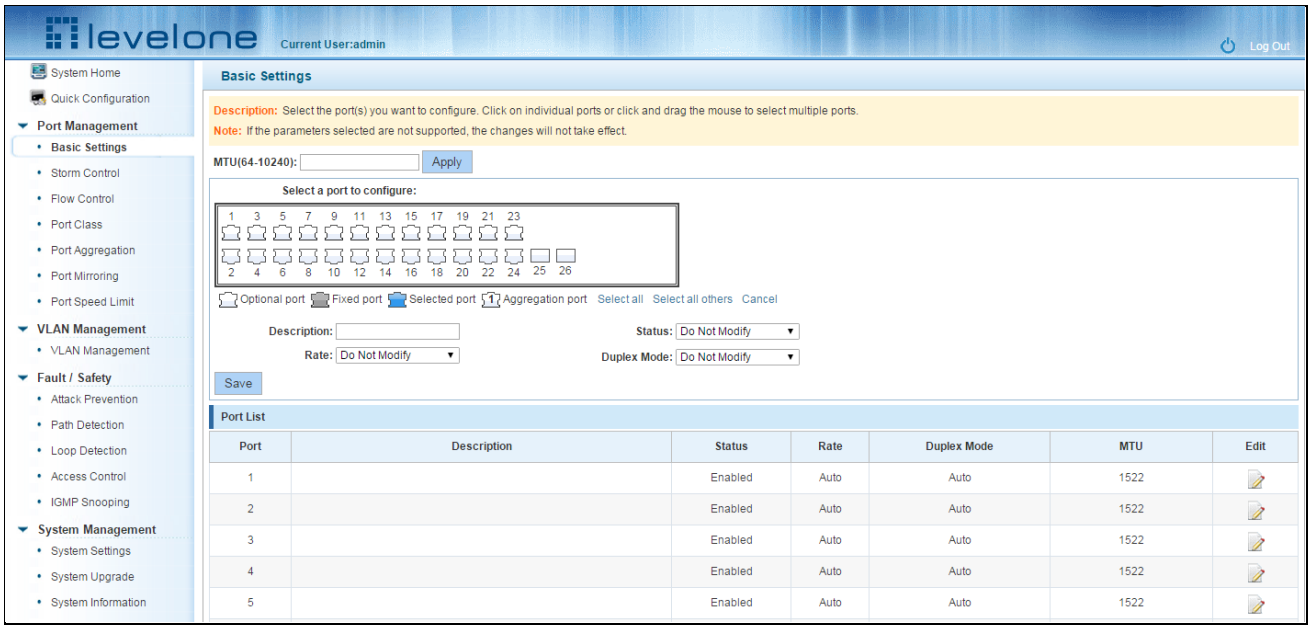


Figure 3-1: Port list information

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:

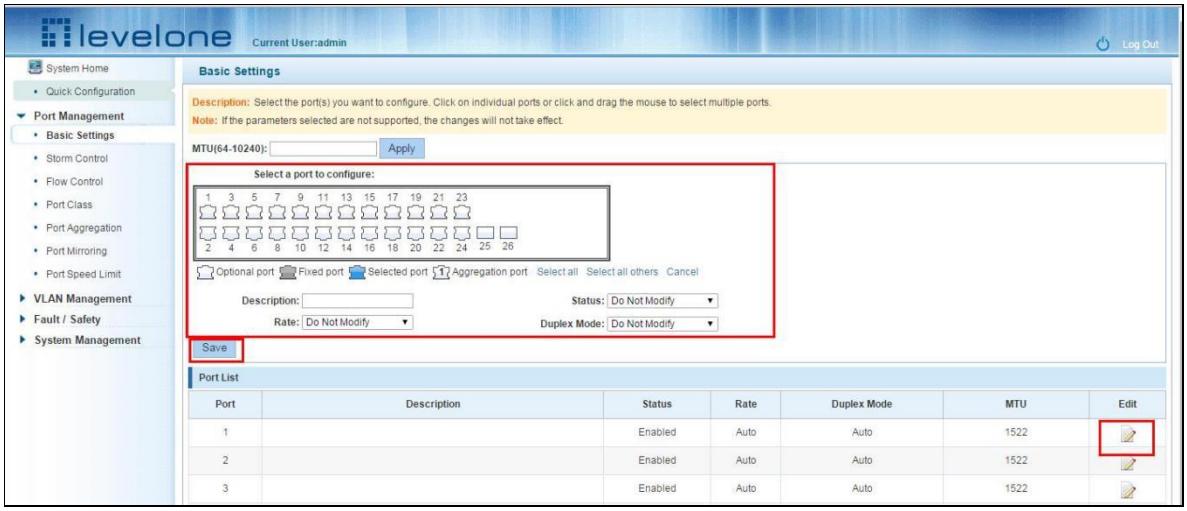


Figure 3-2: Port Properties configuration of FIG.

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:

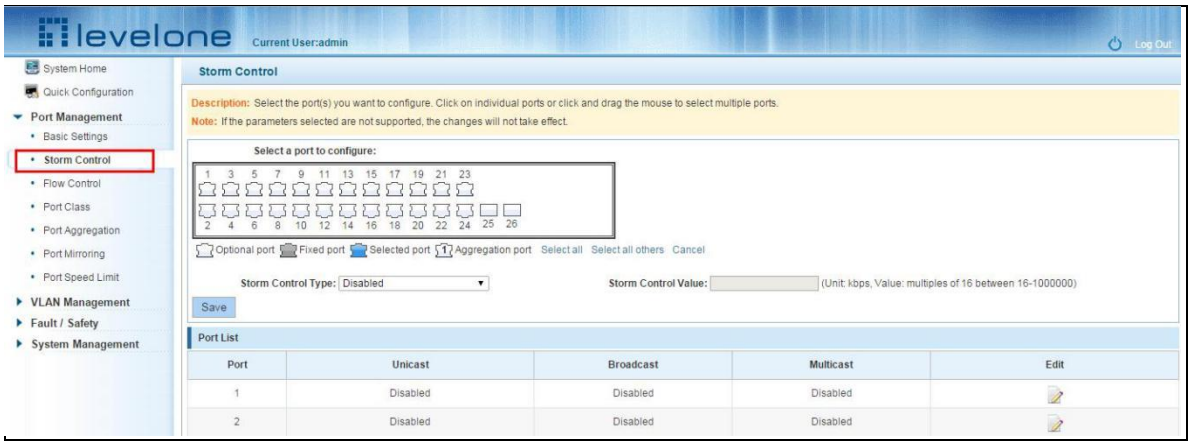


Figure 3-3: Storm Control List information

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.

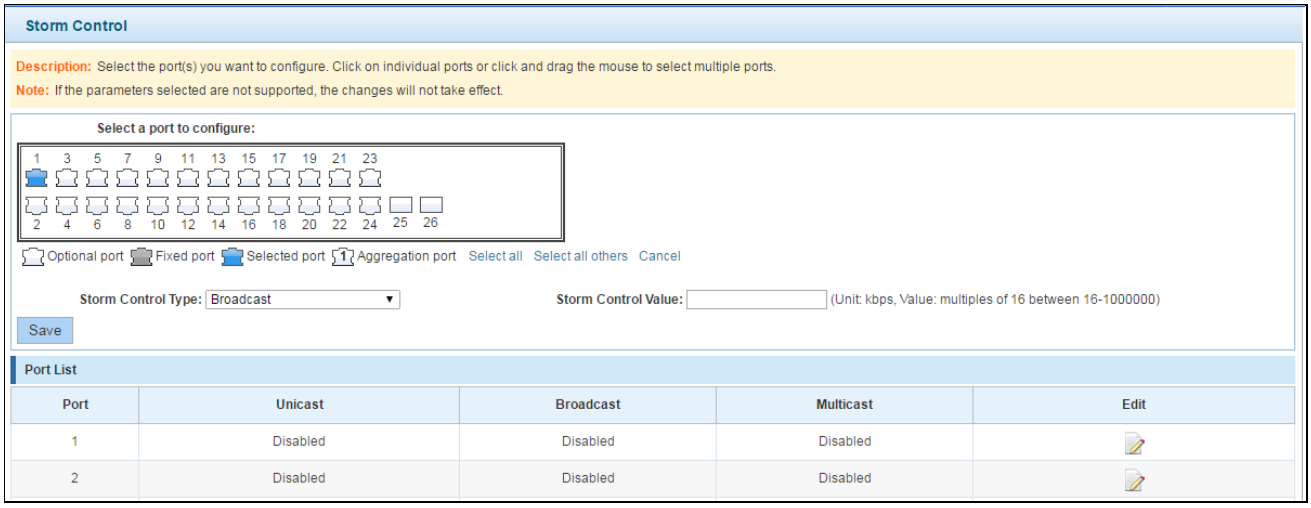


Figure 3-4: Configuring Storm Control information

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

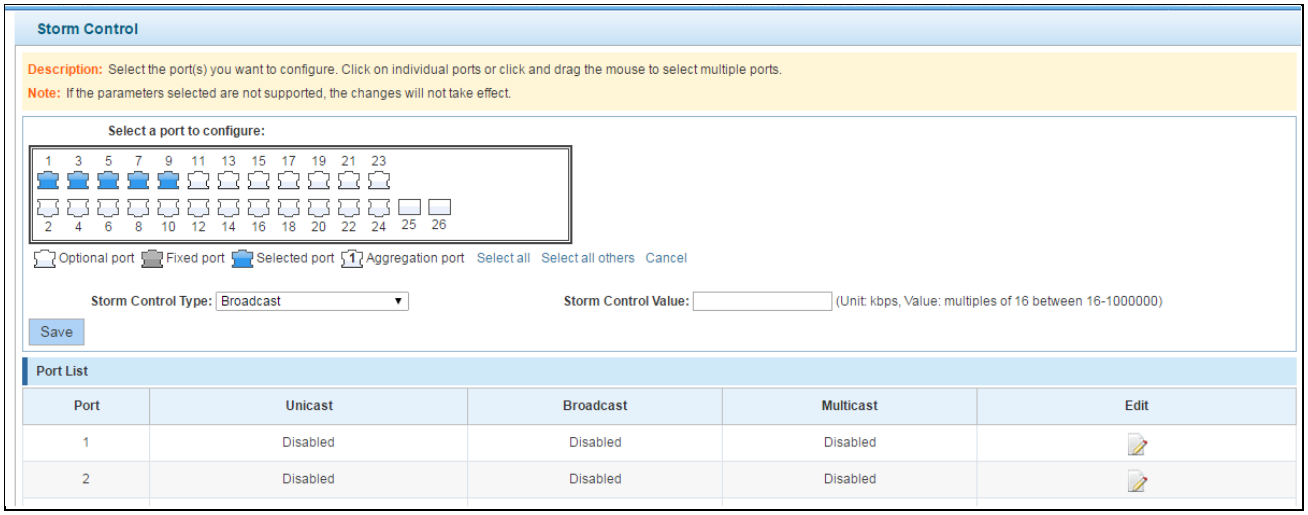


Figure 3-5: Bulk edit configuration information

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.

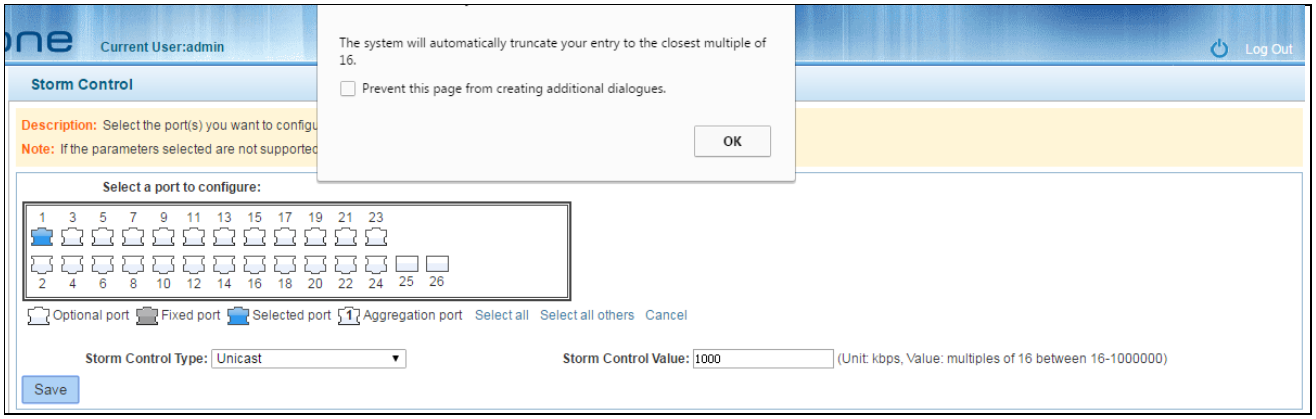
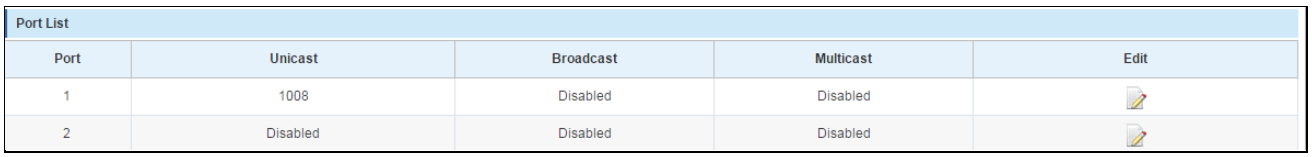


Figure 3-6: Configuring Storm Control information

After the configuration, as shown below:



Port List

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

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

3.3 VIEWING TRAFFIC CONTROL LIST

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

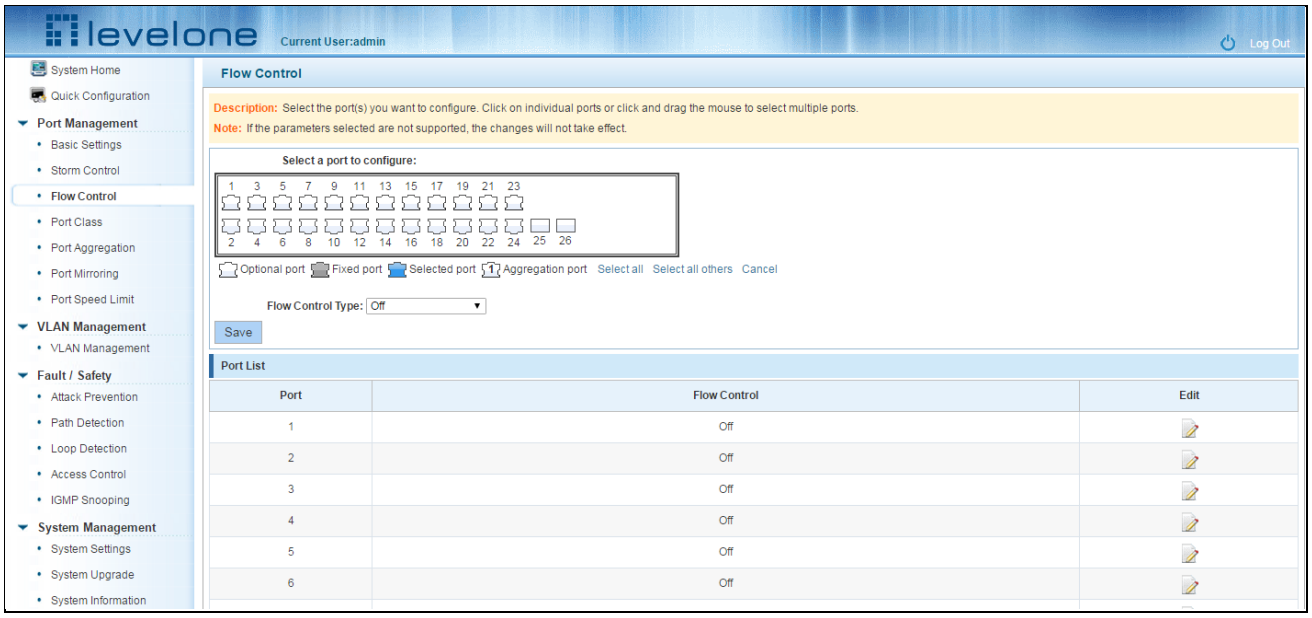


Figure 3-8: Flow Control Information

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":

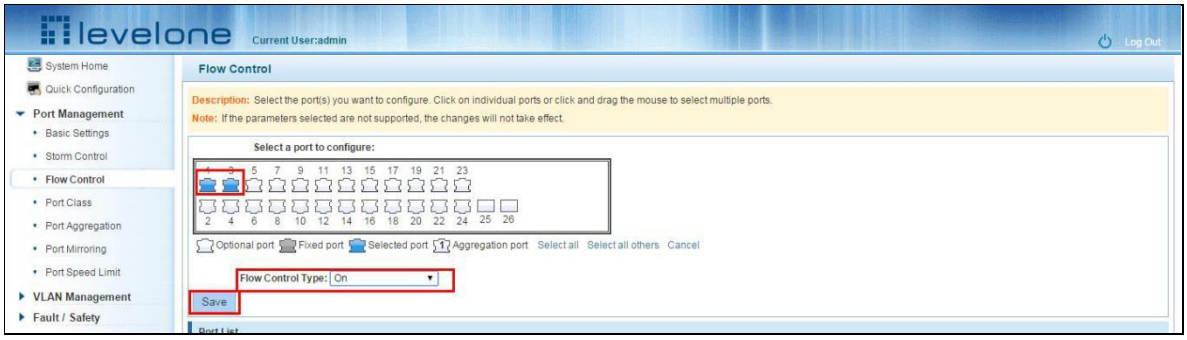
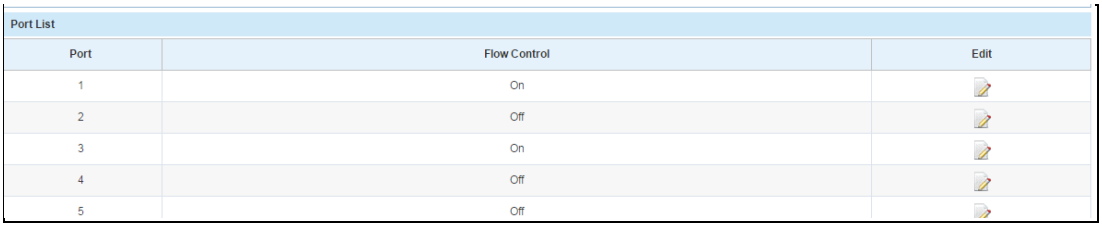


Figure 3-9: Open port flow control function

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	Edit
1	On	
2	Off	
3	On	
4	Off	
5	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":

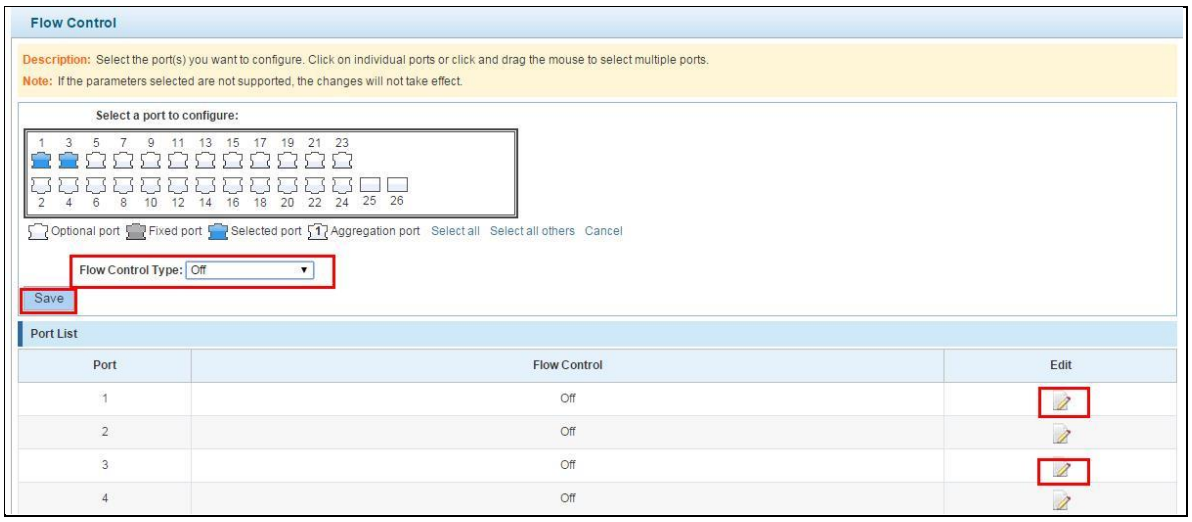


Figure 3-11: Close the port flow control

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 CLASS

3.4.1 VIEWING PORT CLASS

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

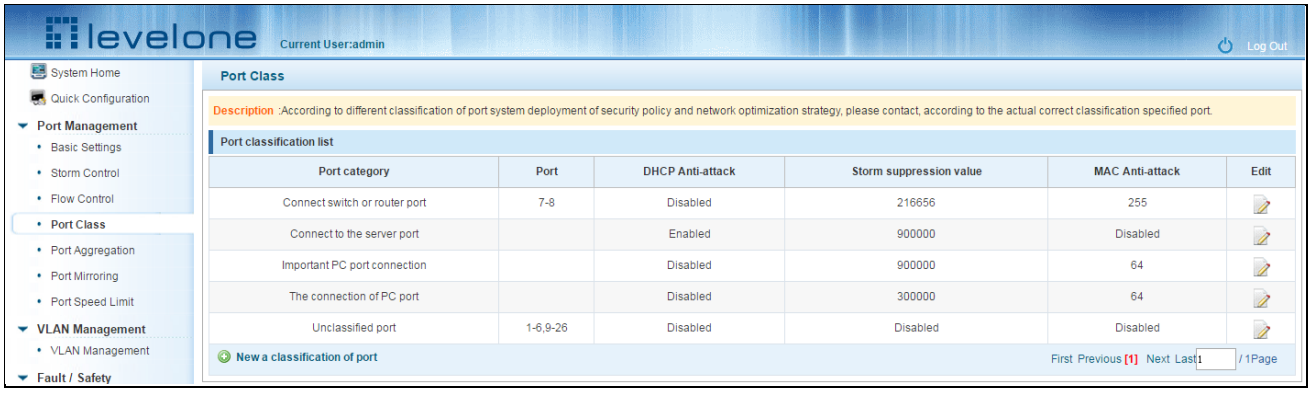


Figure 3-12: port class configuration information

3.4.2 MODIFYING PORT CLASS

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

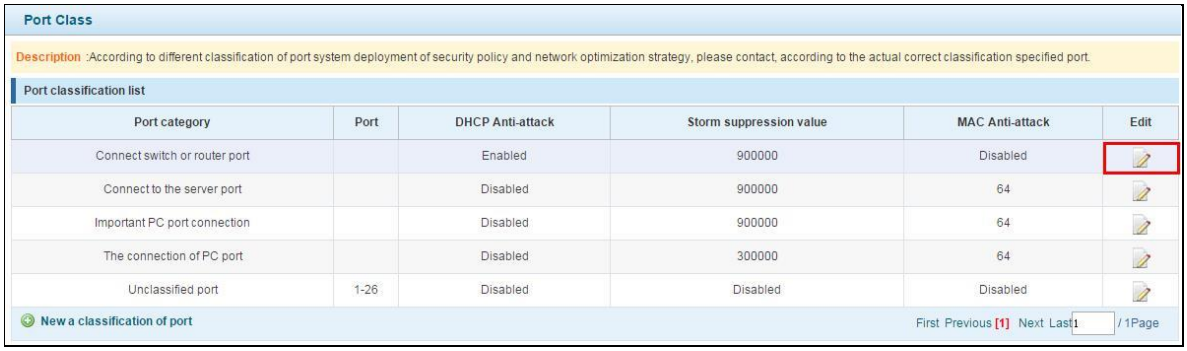


Figure 3-13: to modify port class information

3.4.3 CONFIGURE ANTI-ATTACK

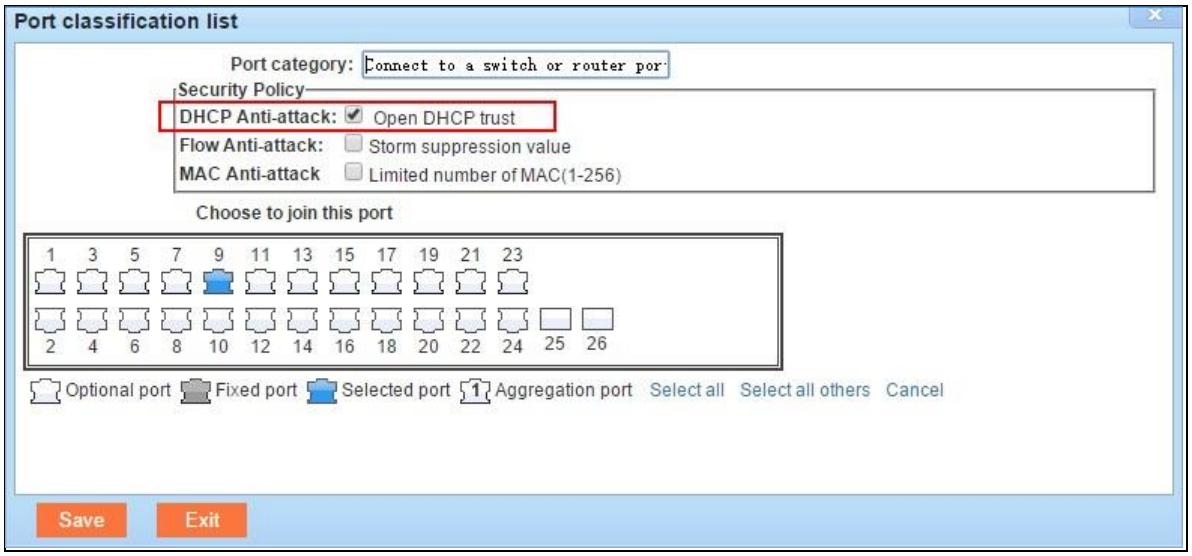


Figure 3-14: to configure port DHCP anti-attack

Open port traffic control, follow these steps:

Step1:Select Open port DHCP anti-attack,step2:Select Open in "Flow control type" on;step3:Click "Save".

View Configuration list to display configuration is successful:

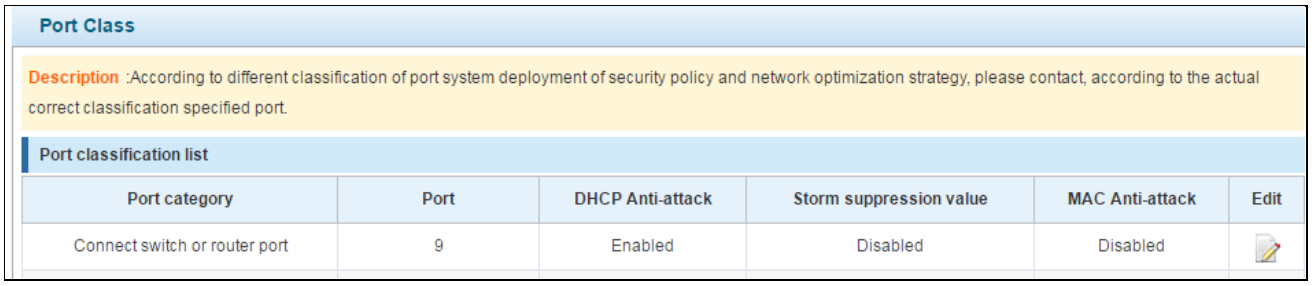


Figure 3-15: port DHCP anti-attack status

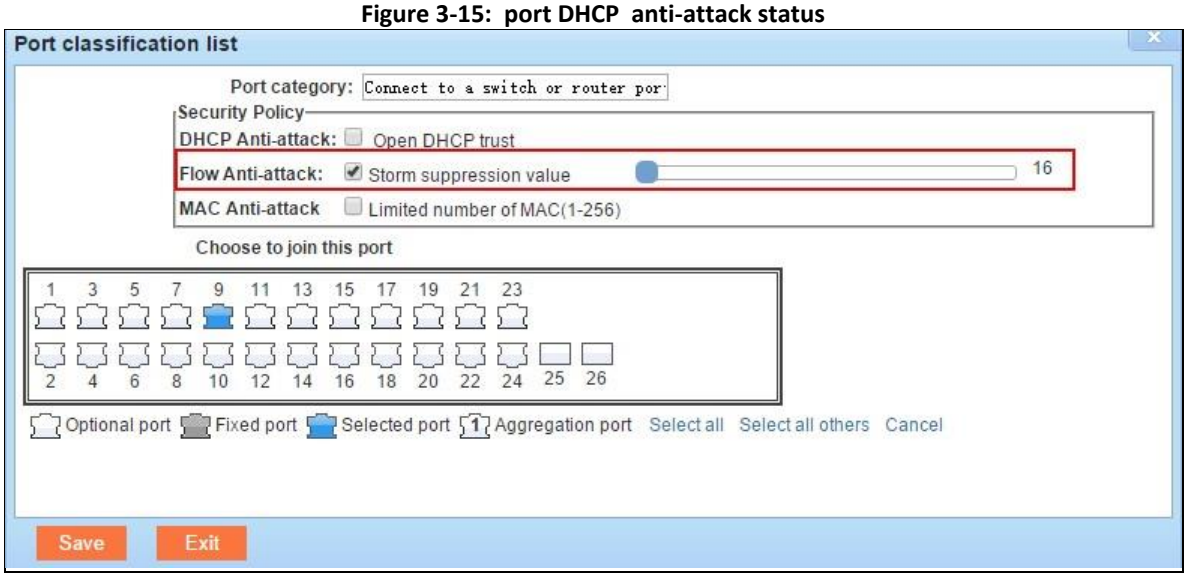


Figure 3-16:to configure Flow anti-attack

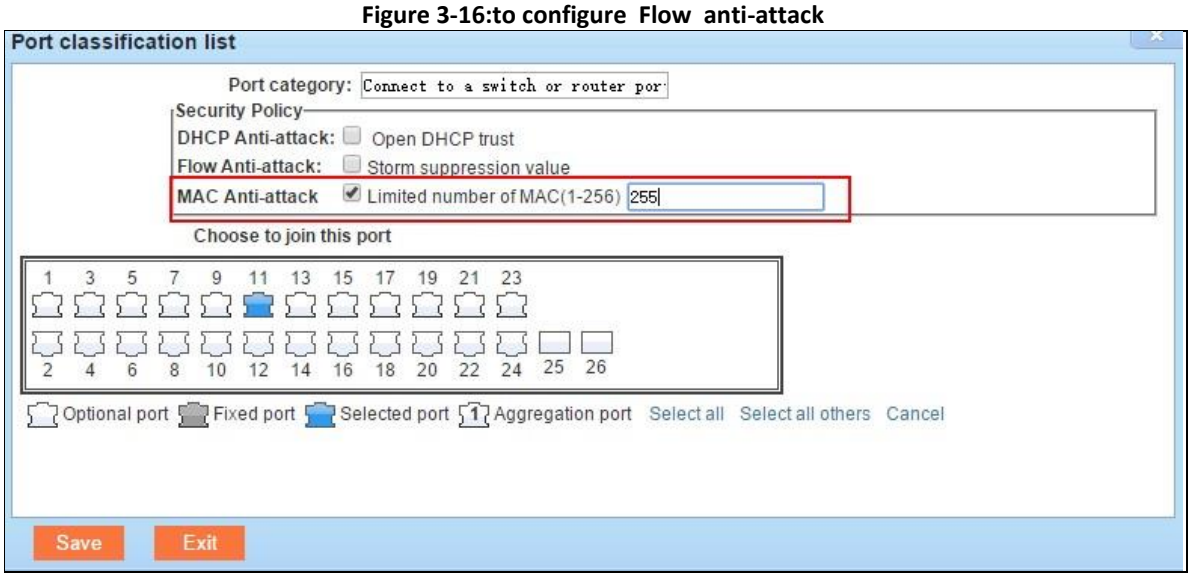


Figure 3-17:to configure MAC anti-attack

3.5 PORT AGGREGATION

3.5.1 VIEWING PORT AGGREGATION CONFIGURATION

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

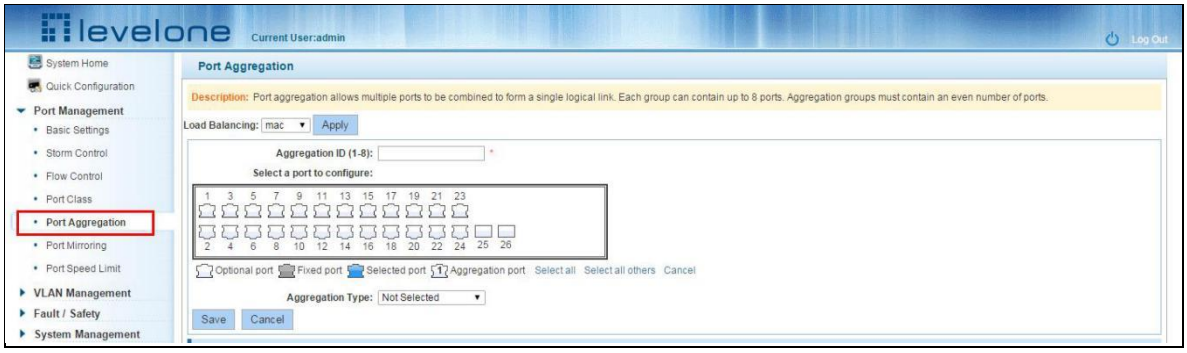


Figure 3-18: Aggregation port configuration information

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.

3.5.2 ADD PORT AGGREGATION

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

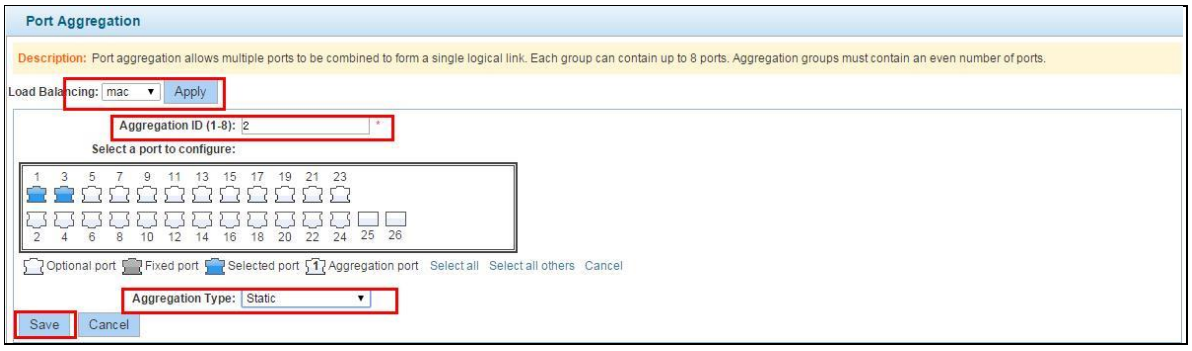


Figure 3-19: Port Aggregation Configuration area

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.

3.5.3 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:

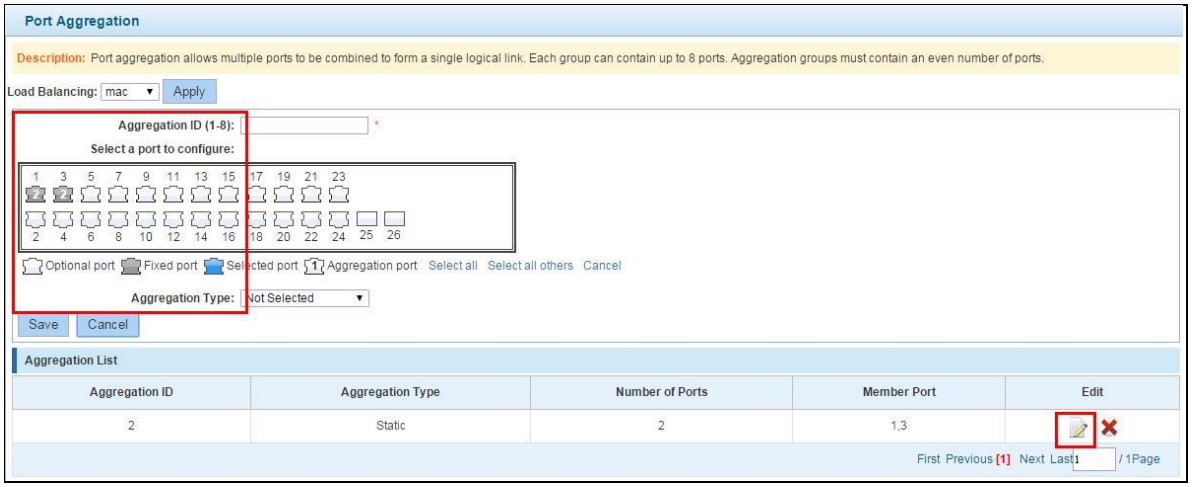


Figure 3-20: To modify the port aggregation

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:

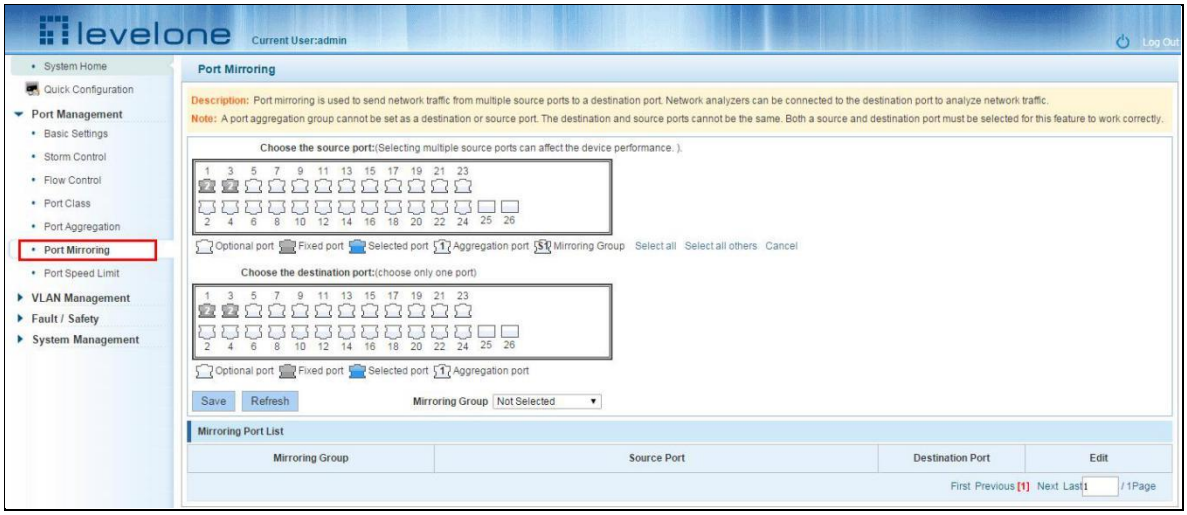


Figure 3-21: Port mirroring configuration information

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.

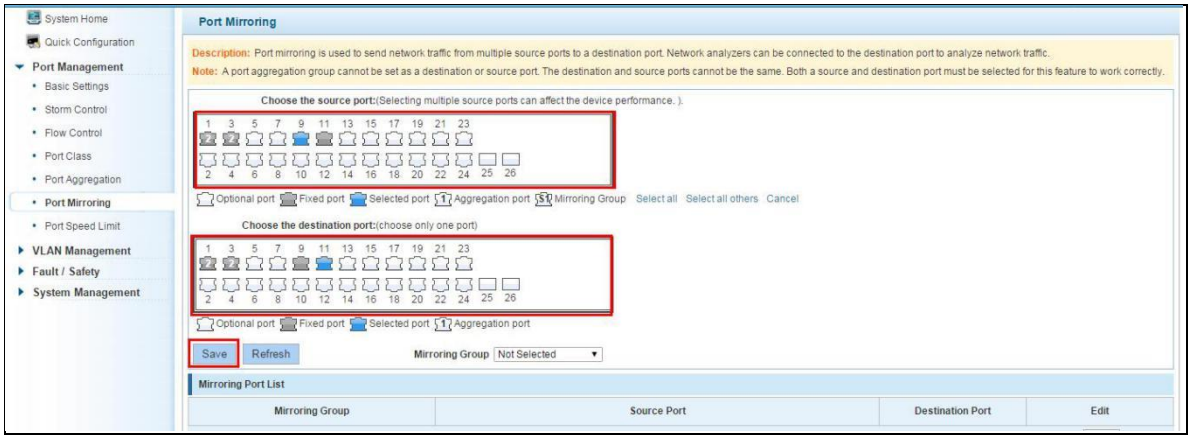


Figure 3-22: Add port mirroring group

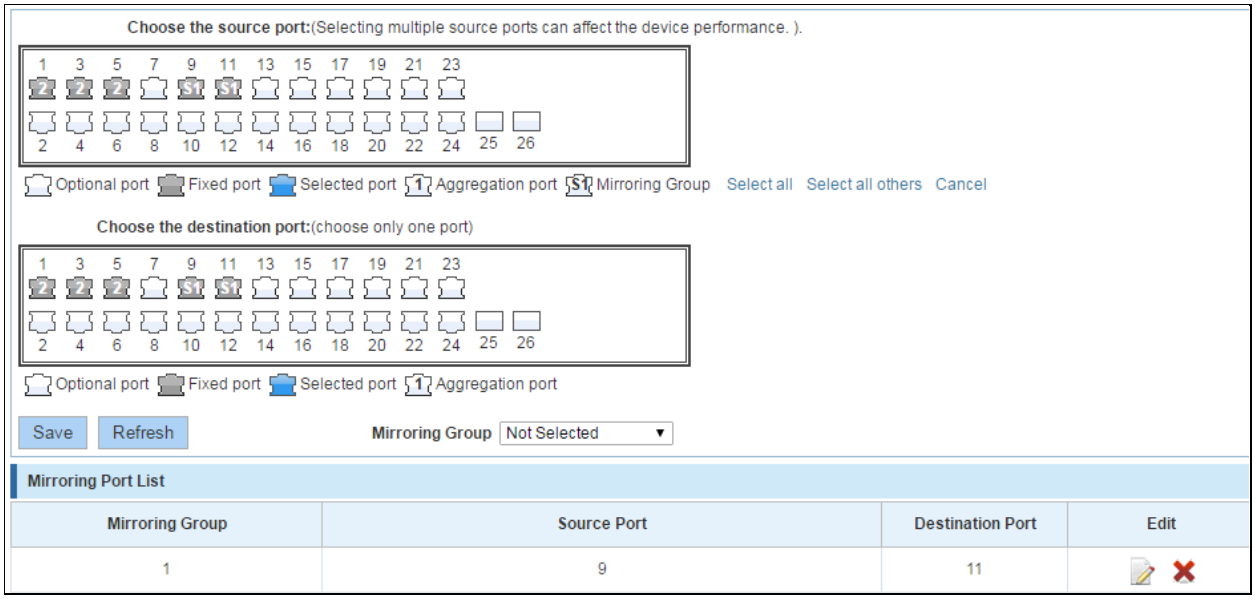


Figure 3-13: Add port mirroring group results

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.

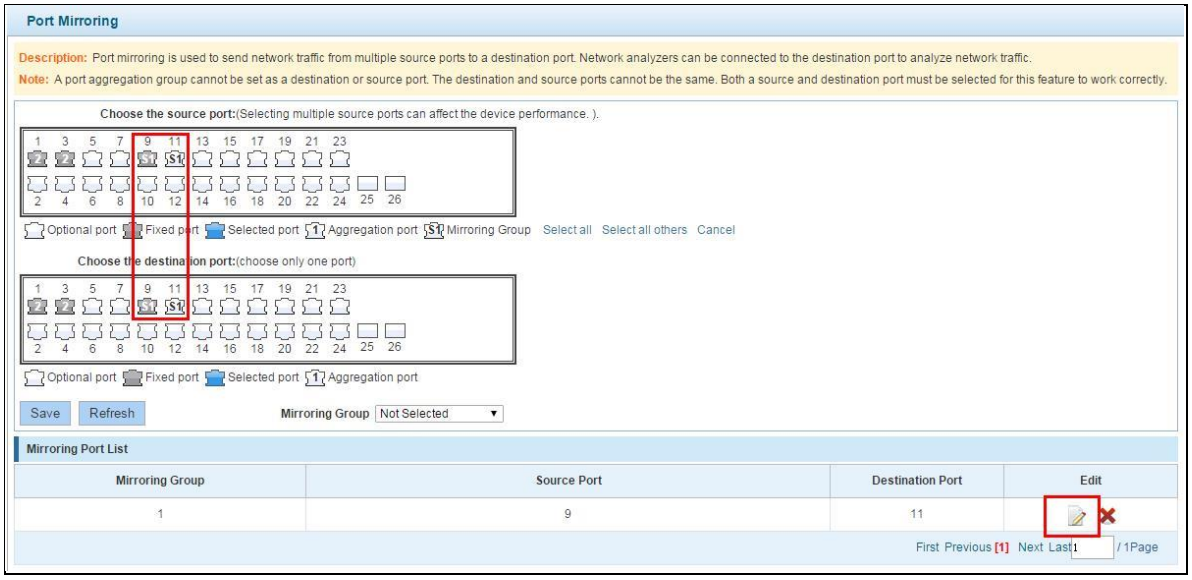


Figure 3-23: To modify the port mirroring group

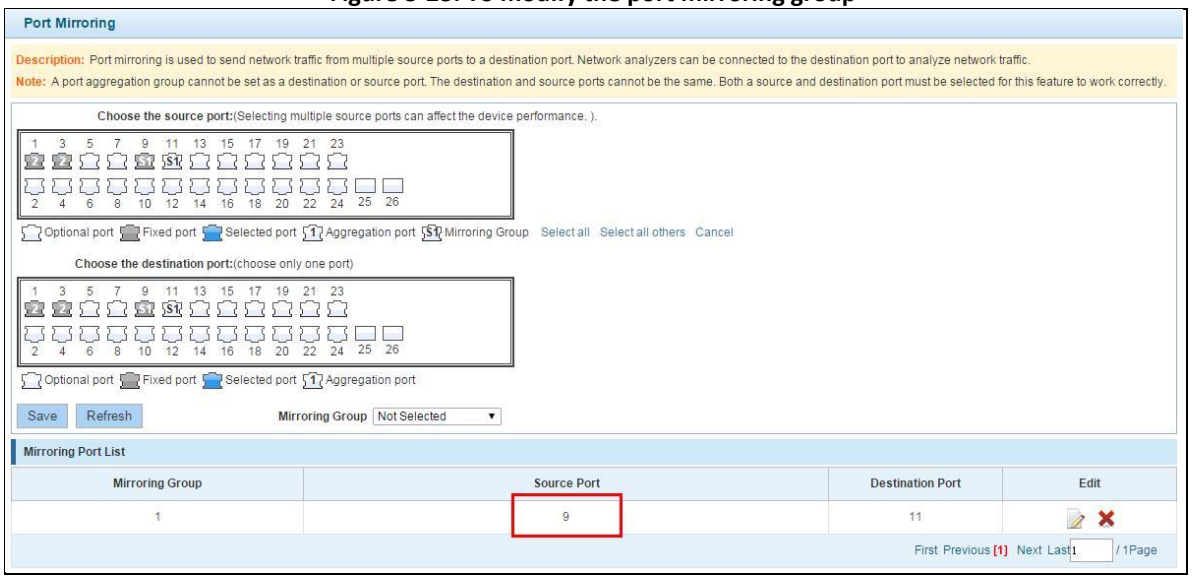


Figure 3-14: Modify successful port mirroring group

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)

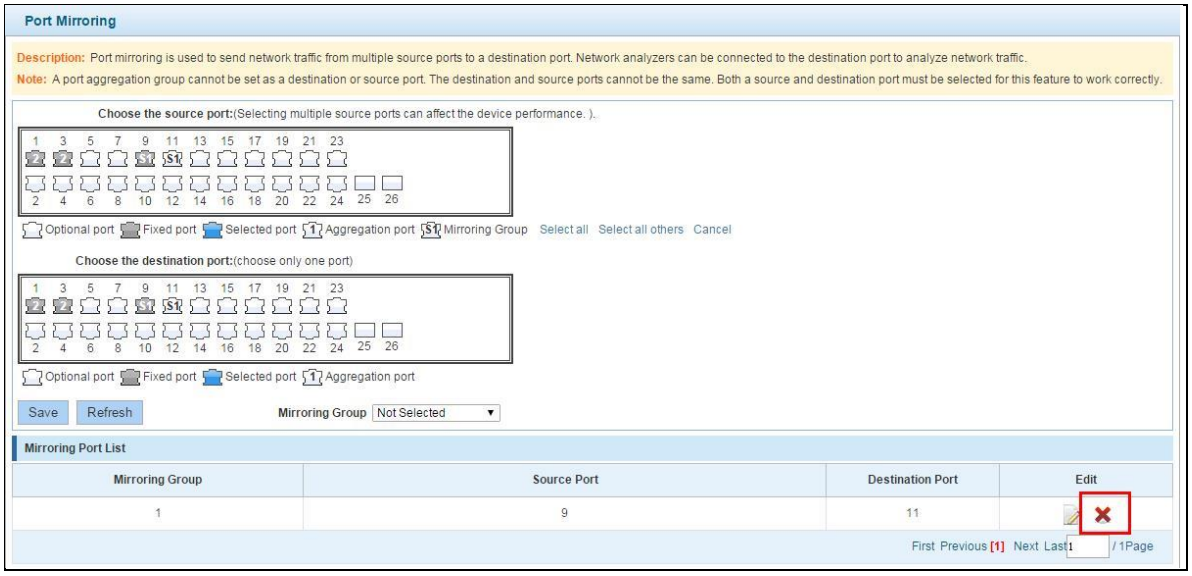


Figure 3-24: Delete port mirroring group

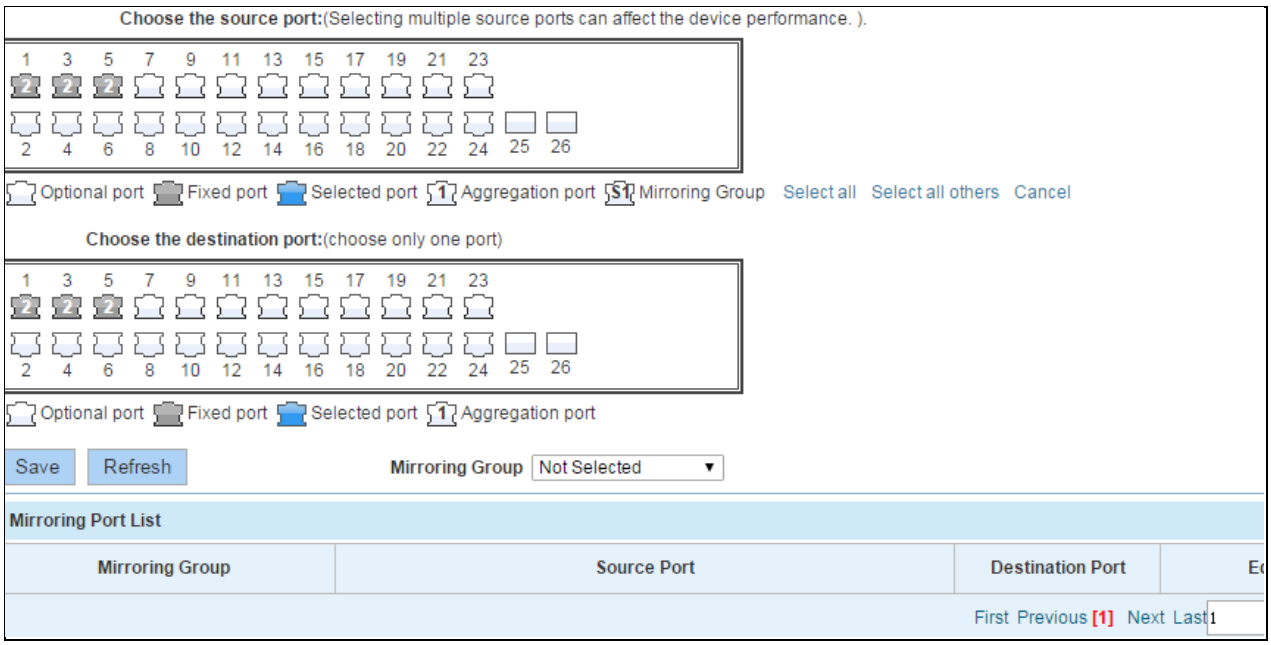


Figure 3-25: Deleted successfully port mirroring

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:

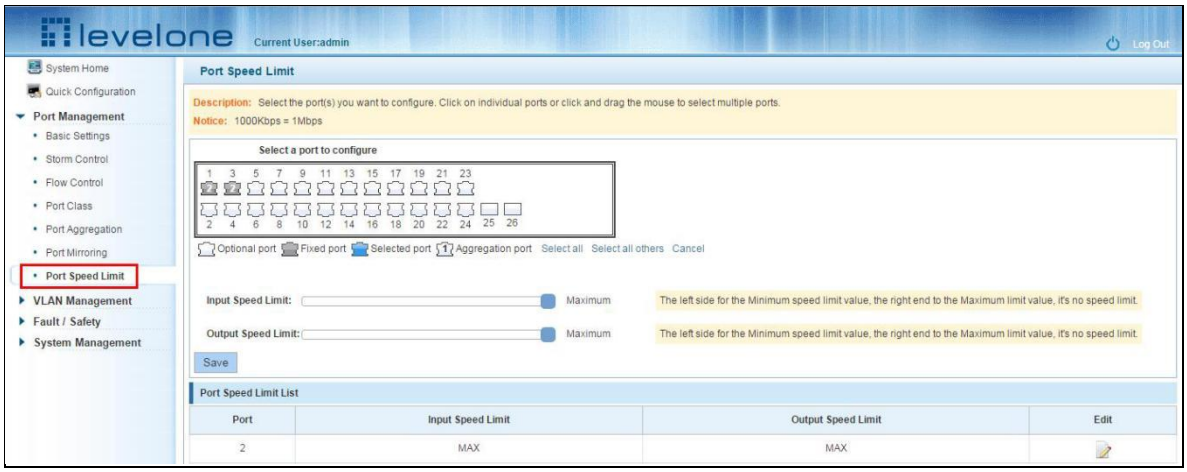


Figure 3-26: View Rate Configuration information

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

Port: The number of the port;

Input limit: uplink port speed;

Output speed: port downstream rate;

3.7.2 CONFIGURE PORT ACCESS RATE

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

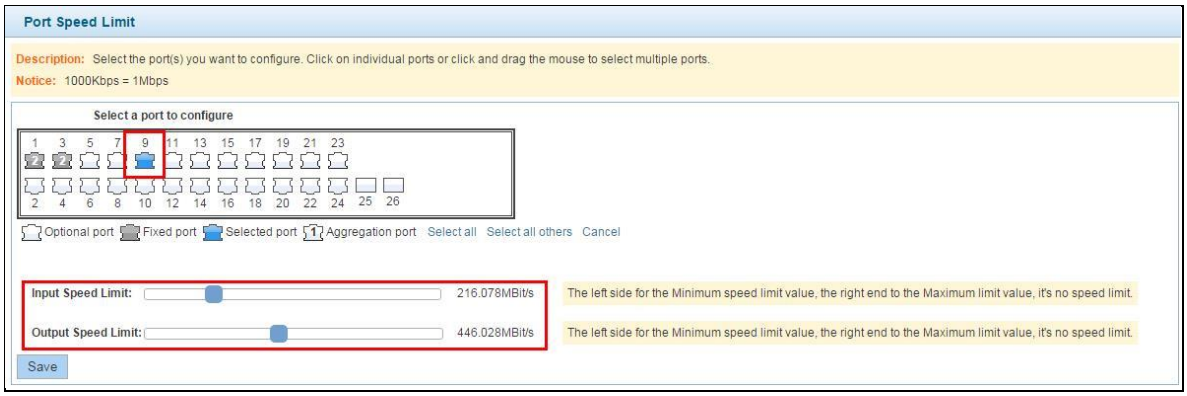


Figure 3-27 Configure port rate limiting entrance

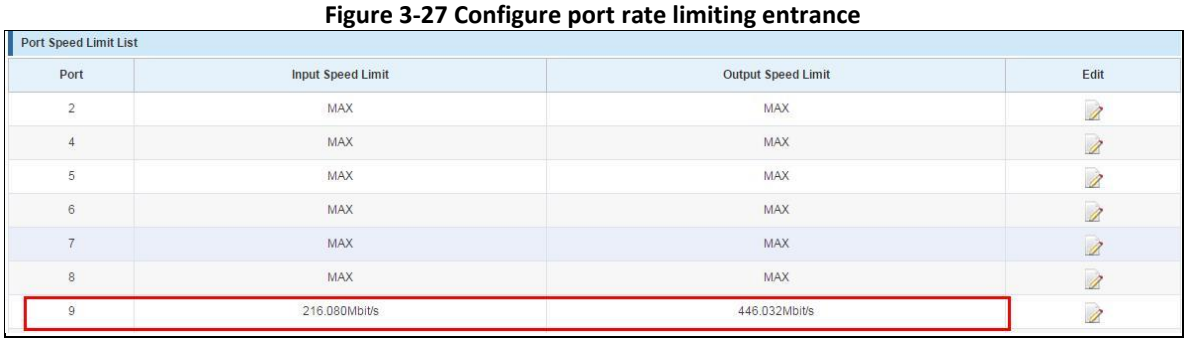


Figure 3-28: Port entrance speed limit results

Entrance port rate limiting configuration steps are as follows:

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

3.2.2 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.

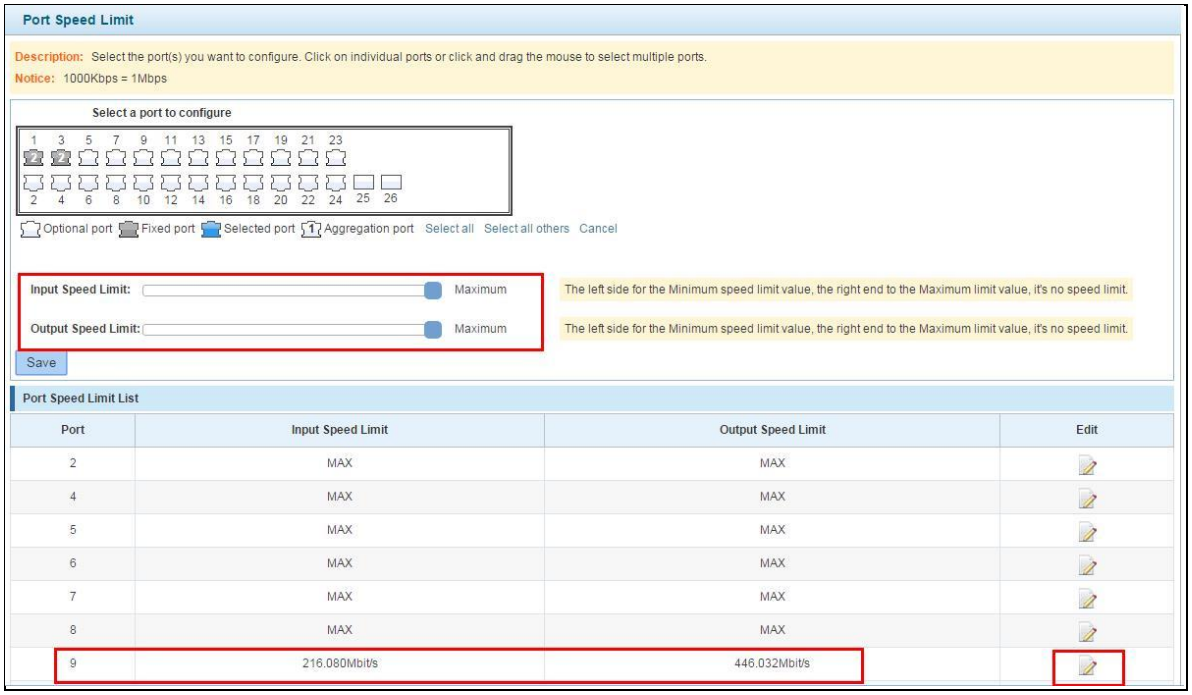


Figure 3-29: Remove the port speed limit

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 VLAND:

1.VLAN ID: VLAN ID value is displayed;

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

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

4.Port: Displays the port VLAN that exist.

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

4.1.2 ADDING A VLAN

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

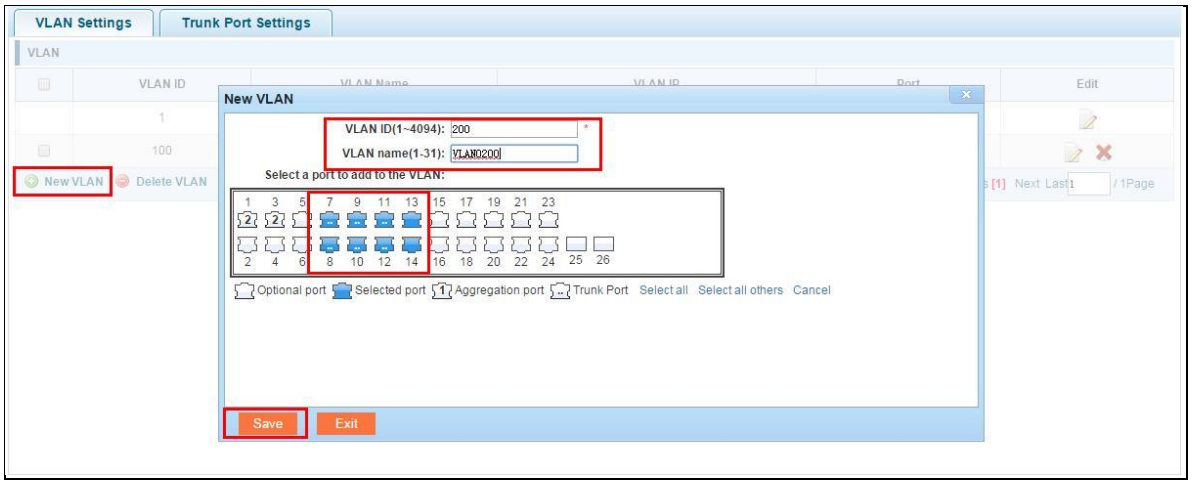


Figure 4-2: Adding a VLAN

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:

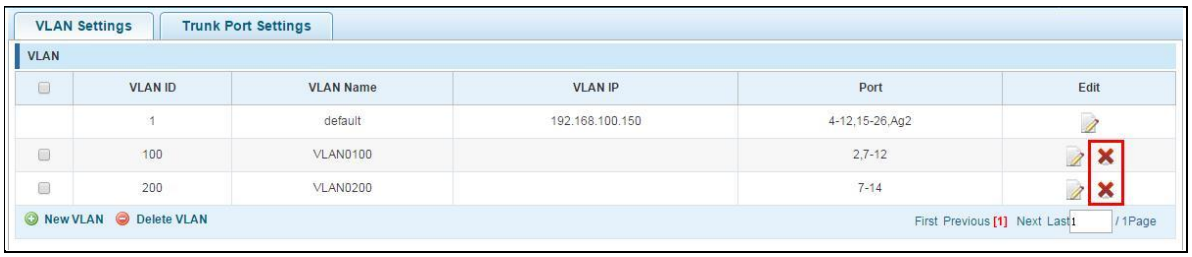


Figure 4-3: Delete a single VLAN

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:

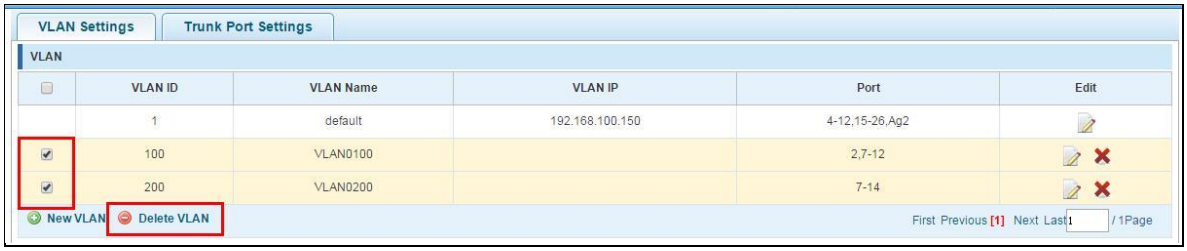


Figure 4-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

Step1:I want to delete VLAN check box;setp2:Click on the bottom left "Delete VLAN" connection;step3:Confirm delete.

4.1.4 EDITING VLAN

4.1.4.1 Port to a VLAN

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

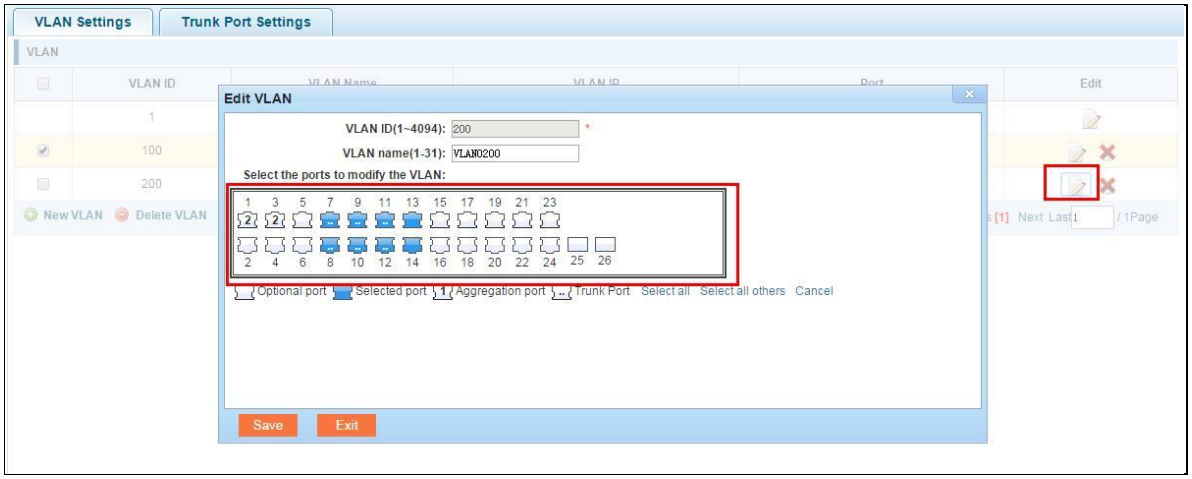


Figure 4-5: Add the port to the VLAN

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:

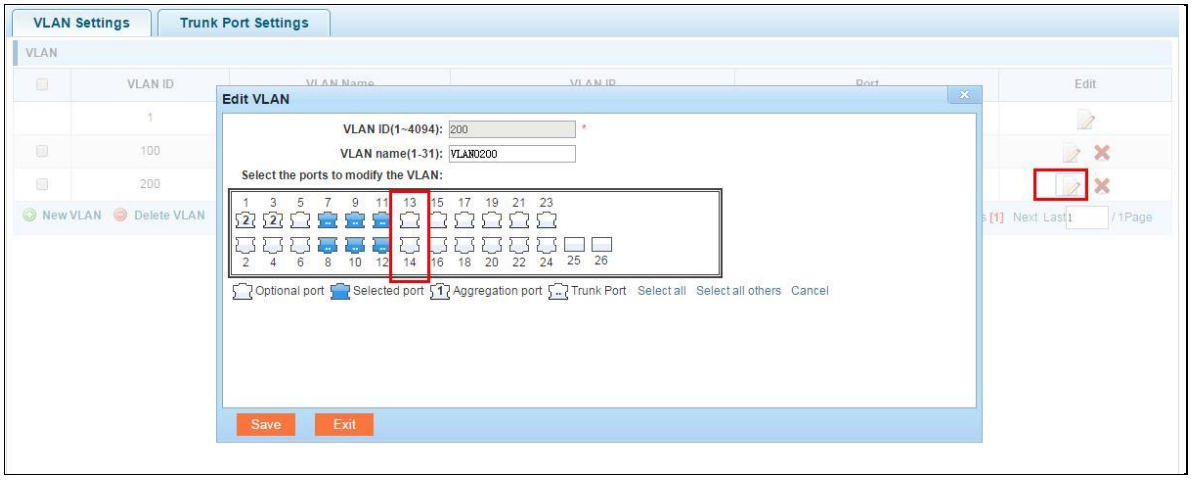


Figure 4-6: To remove the port from the VLAN.

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:

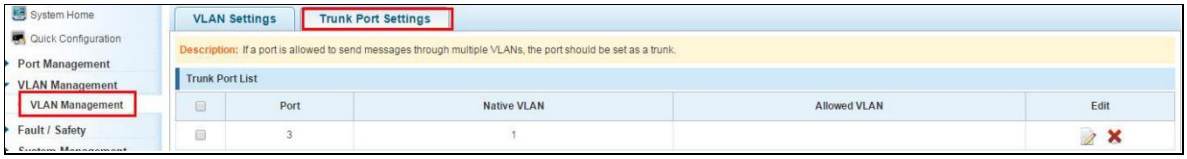


Figure 4-7: View trunk configuration information

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:

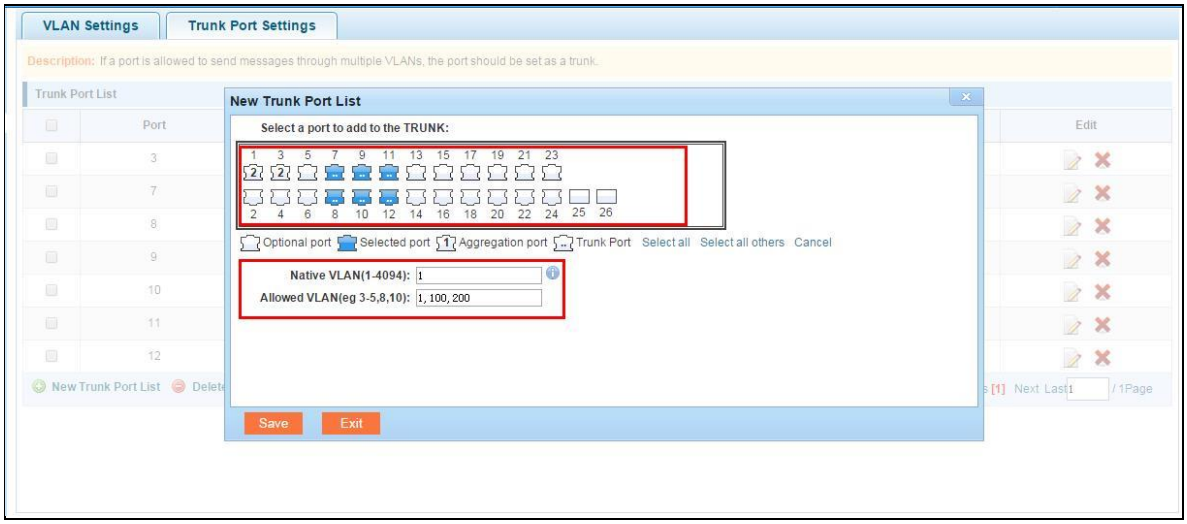


Figure 4-8: Trunk

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:

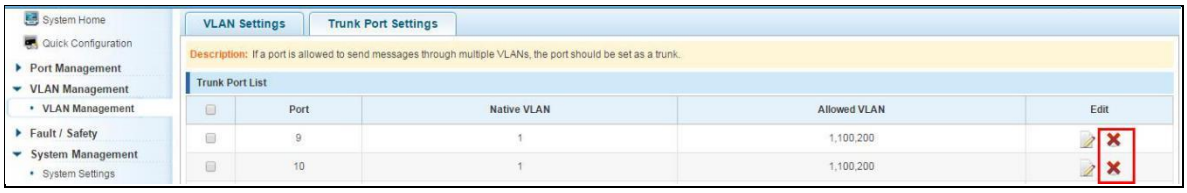


Figure 4-9: Delete a single trunk port

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:

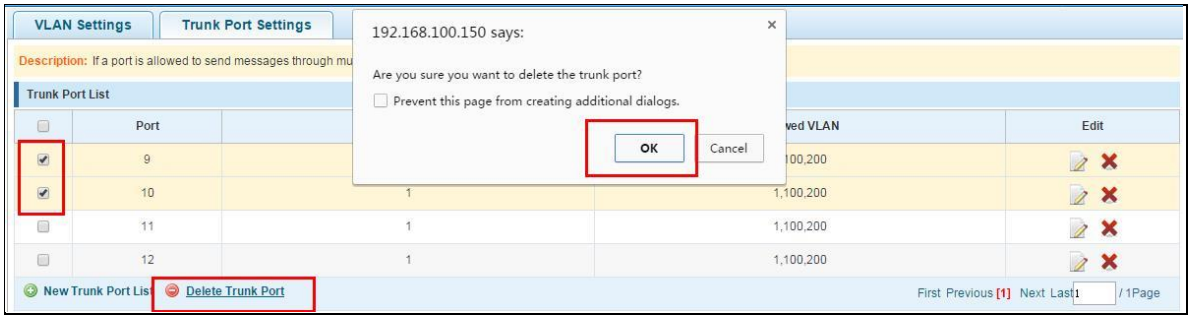


Figure 4-10: Delete multiple trunk ports

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

5.1.1ARP 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

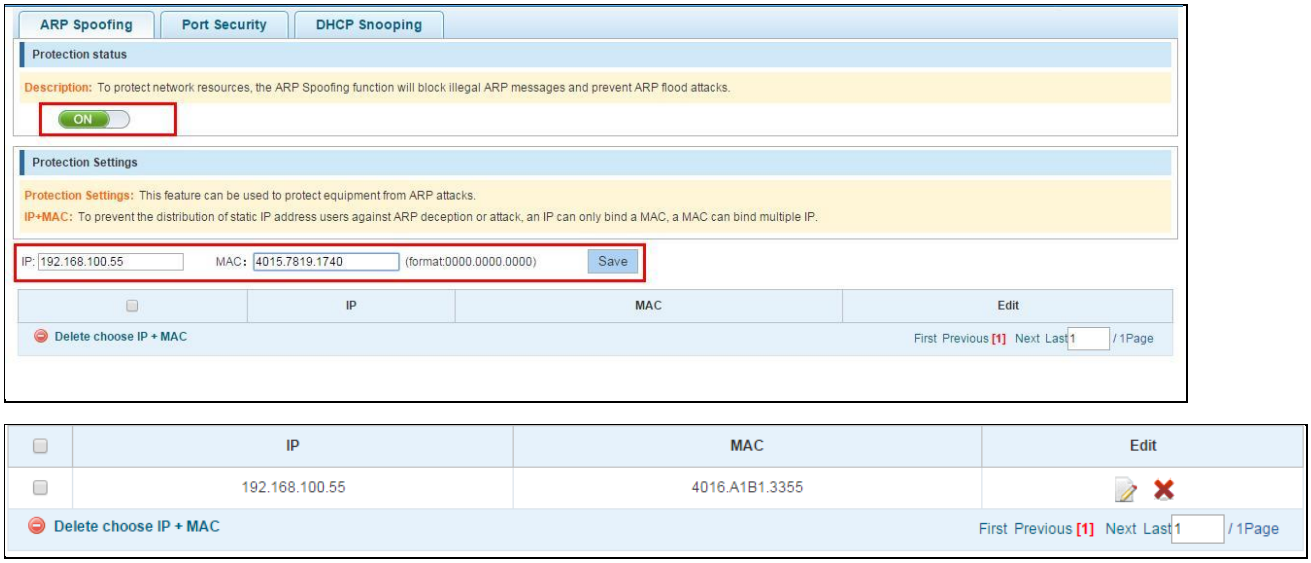


Figure 5-3: ARP spoofing status table

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.

.

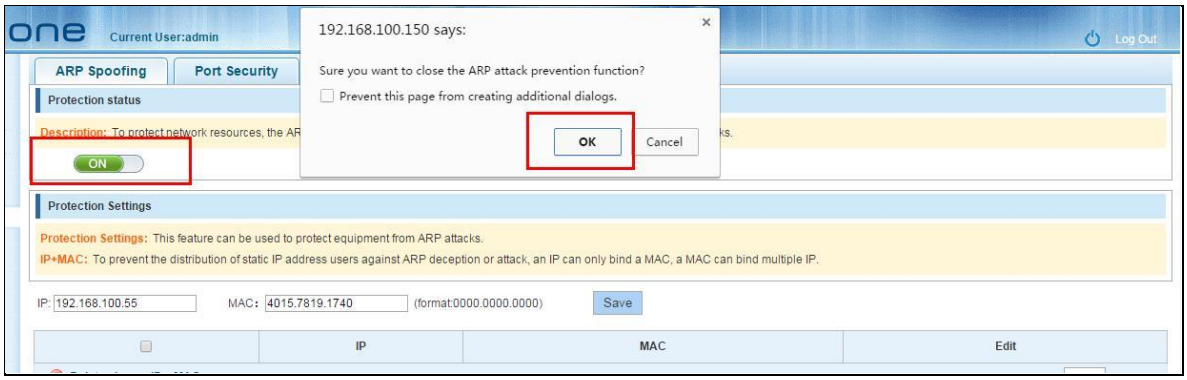


Figure 5-4: Disable ARP spoofing function

5.1.1.4 Delete IP+MAC

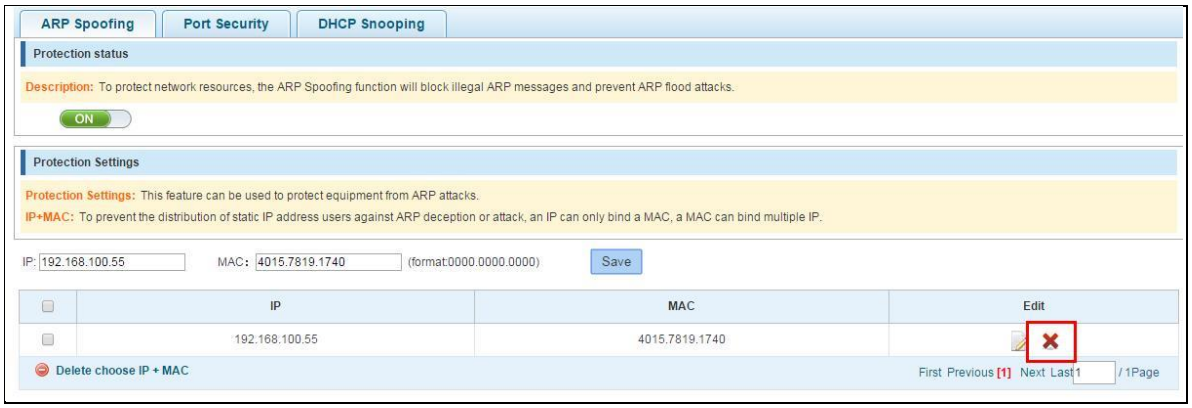


Figure 5-5: Delete IP+MAC

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:

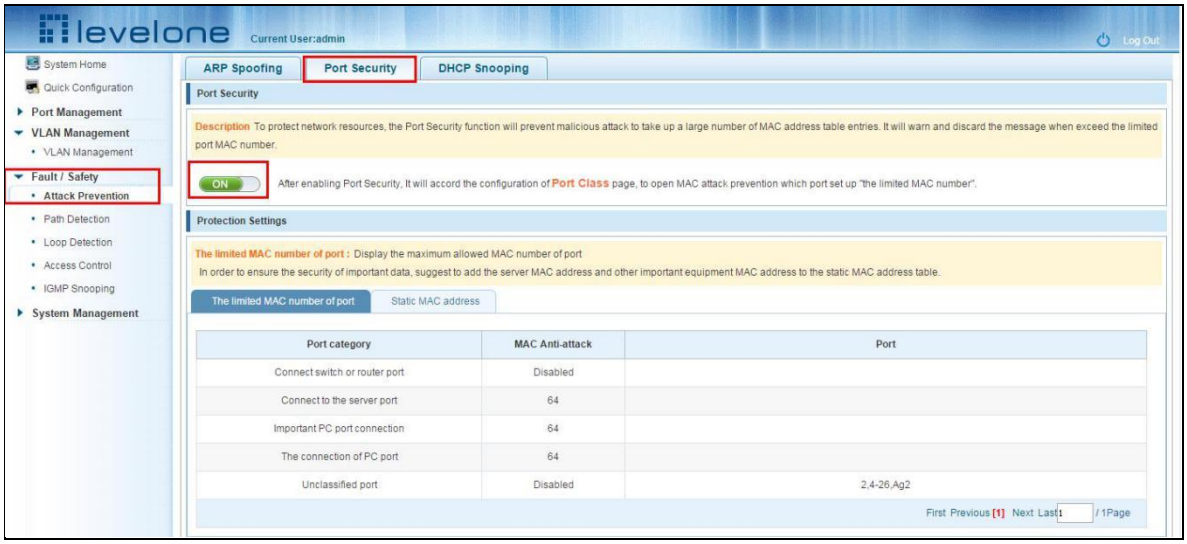


Figure 5-6: Port security configuration

5.1.2.2 Manual configuration

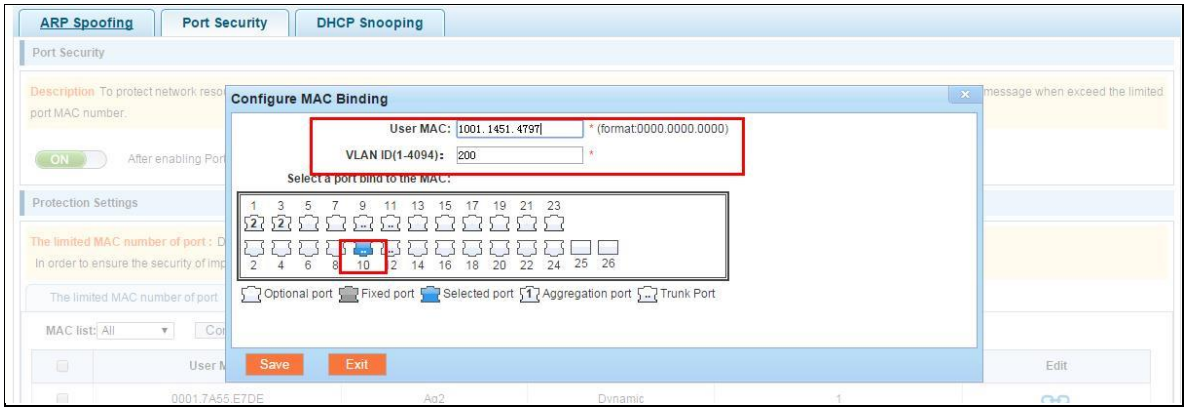


Figure 5-7: Port security manual configuration

5.1.2.3 Cancel port security binding configuration

In the binding list, select the IP address, MAC, and port to which you want to cancel the binding "X":

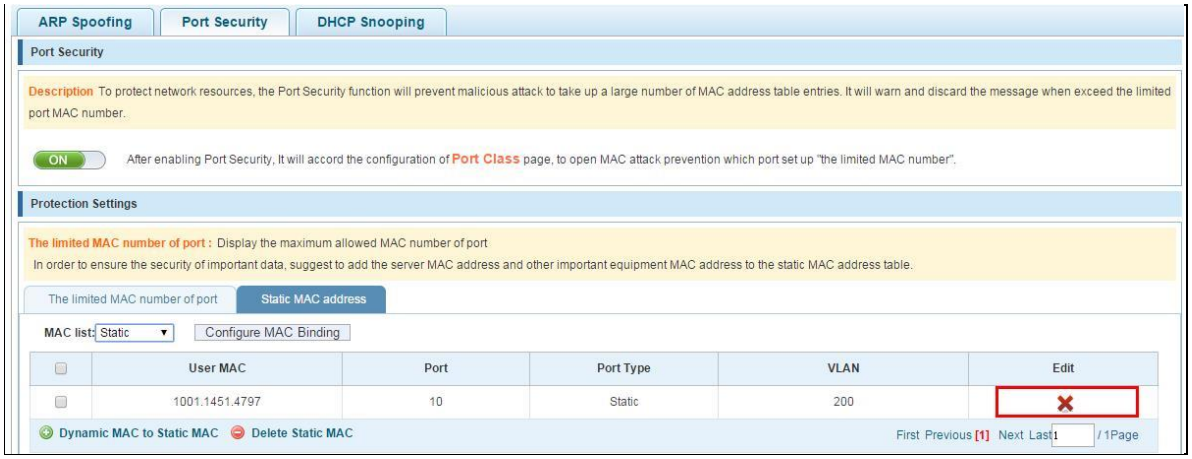


Figure 5-8: Cancel port security bound

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:

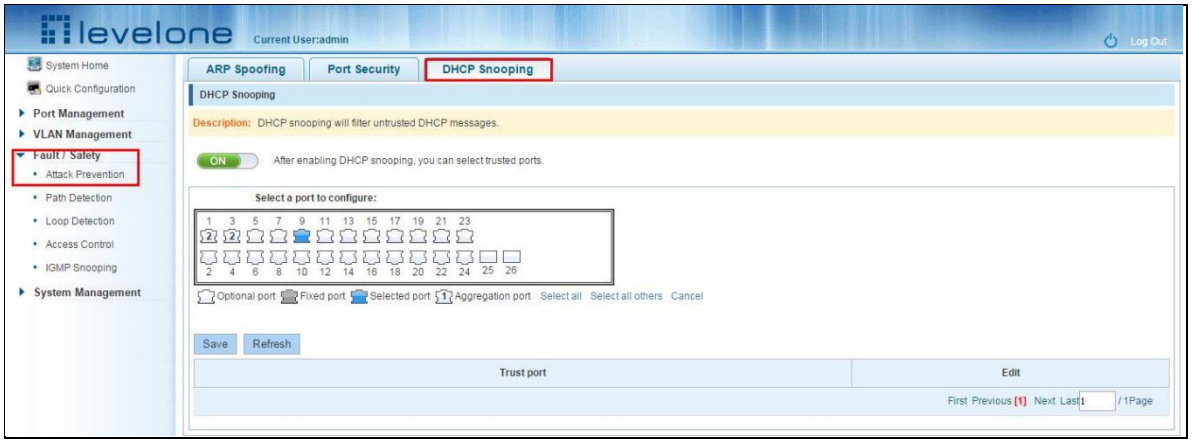


Figure 5-9: View anti DHCP attack configuration information

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:

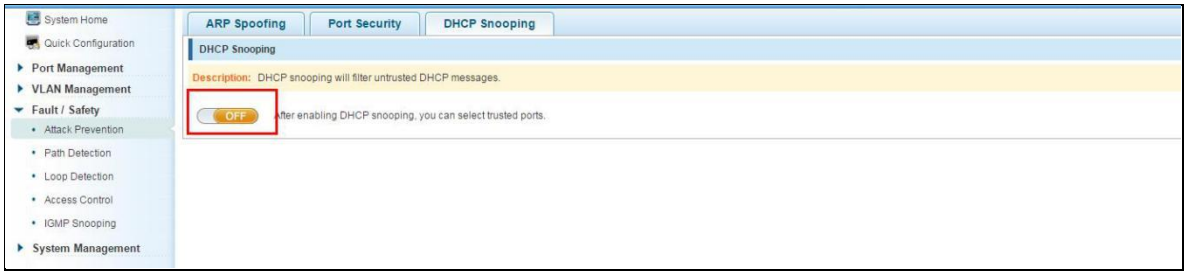


Figure 5-10: Activation of anti DHCP attack function

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:

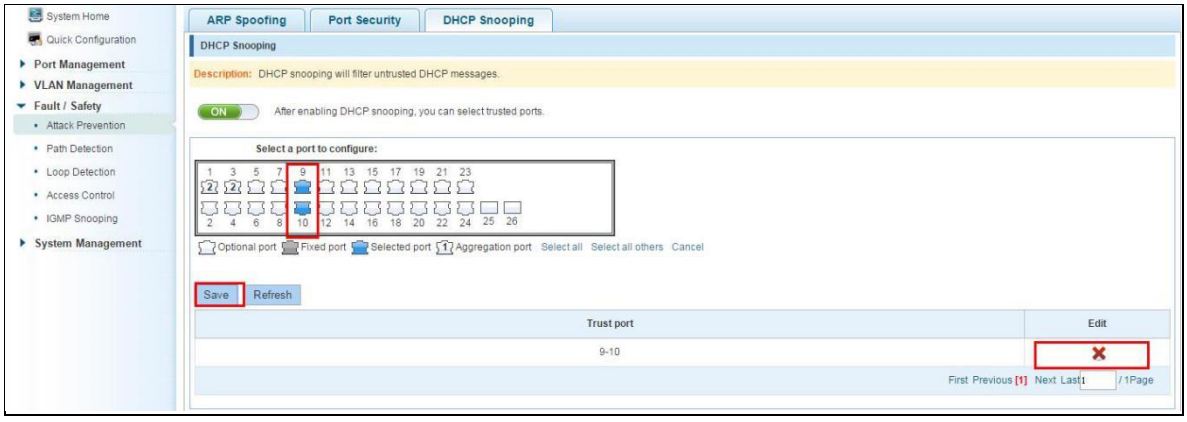


Figure 5-11: Disable anti illegal DHCP server functions

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:

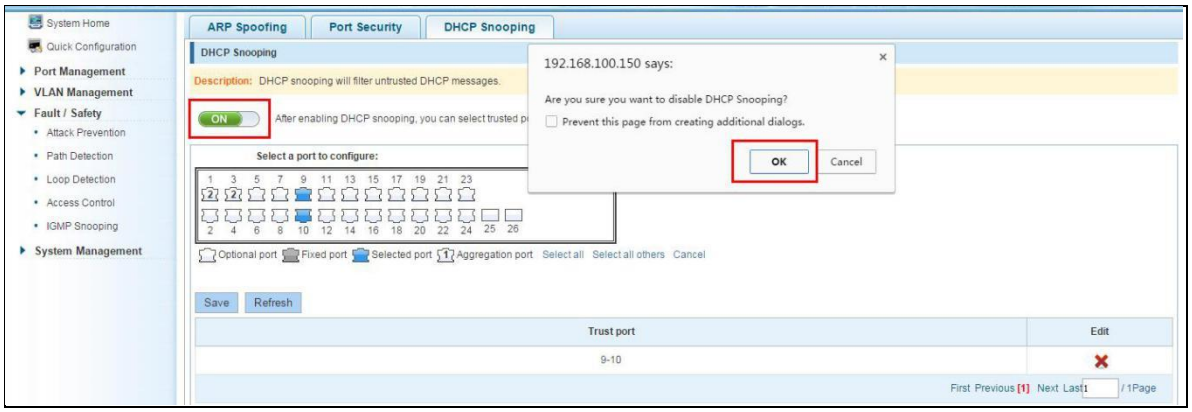


Figure 5-12: Off anti DHCP attack function

5.2 PATH DETECTION

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

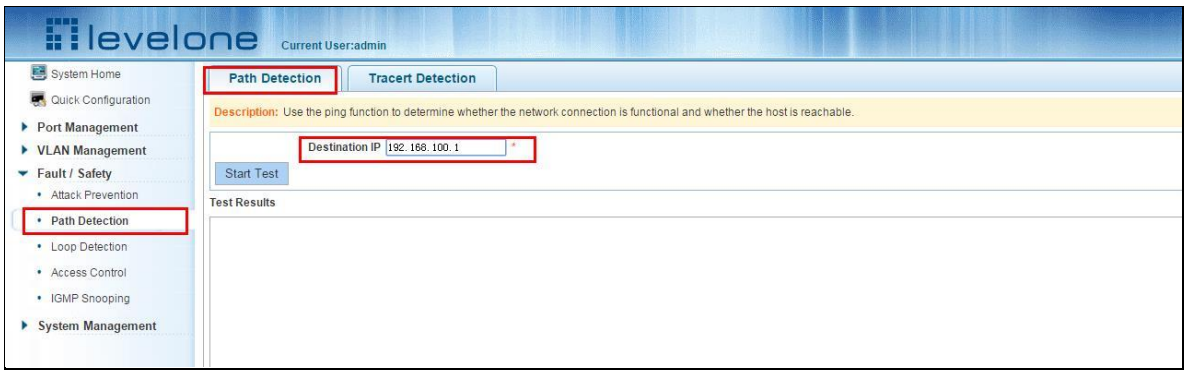


Figure 5-13: Path detection information

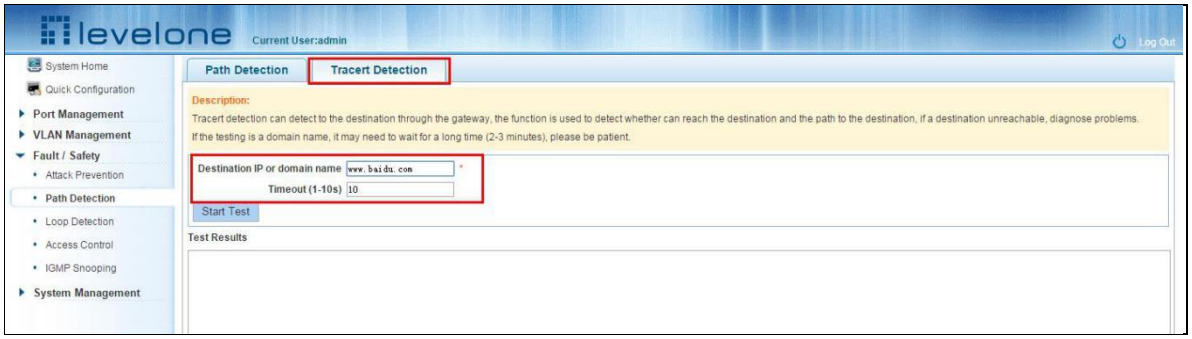


Figure 5-14: Tracert detection information

5.3 LOOP DETECTION

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

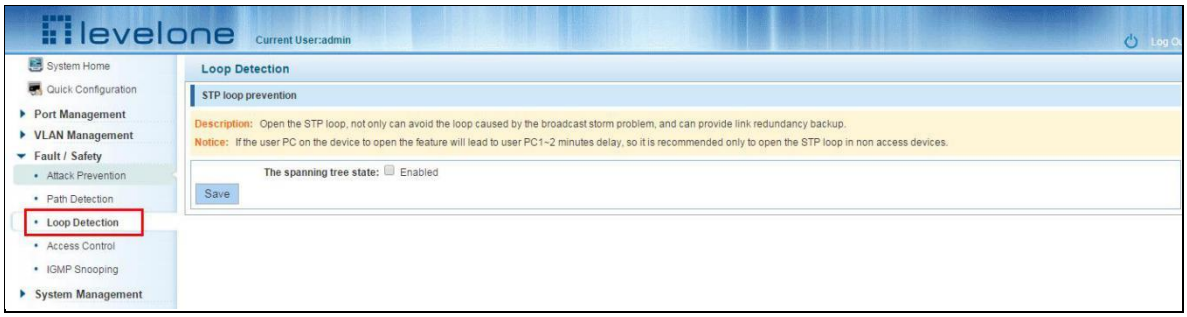


Figure 5-15: View spanning tree configuration information

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 MODEL

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:

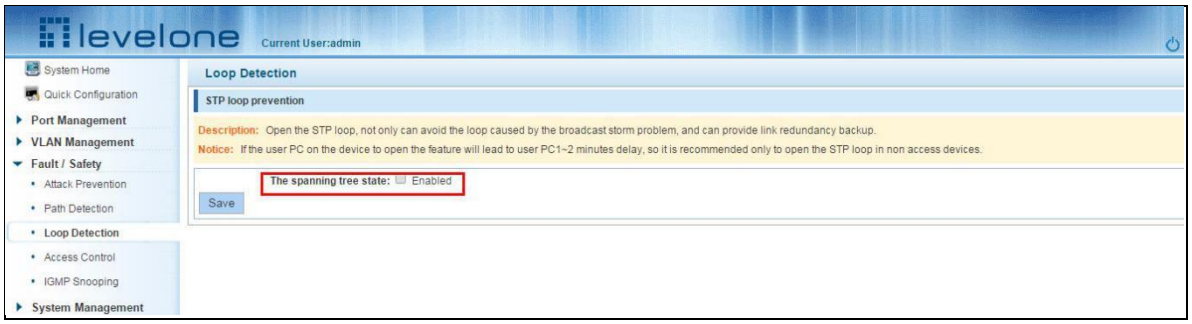


Figure 5-17: close the spanning tree pattern

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:

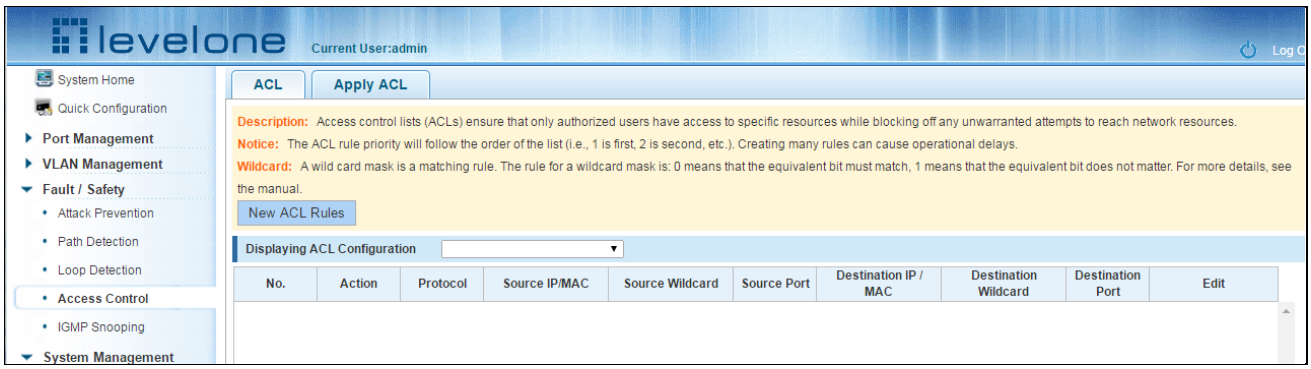


Figure 5-18: Access control list

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:

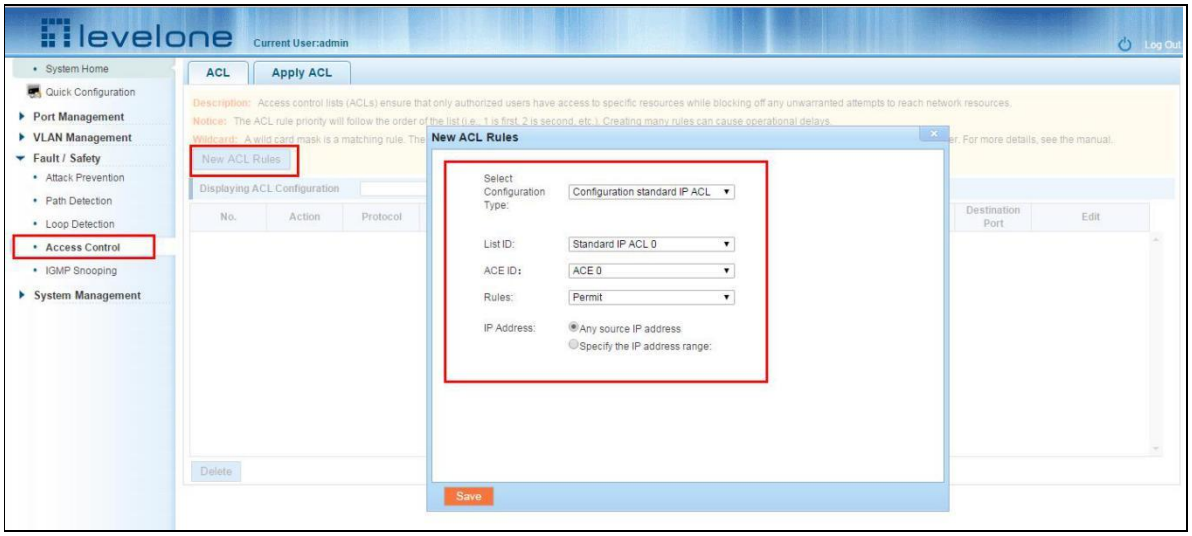


Figure 5-:19 Configuration standard IP access control list

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:

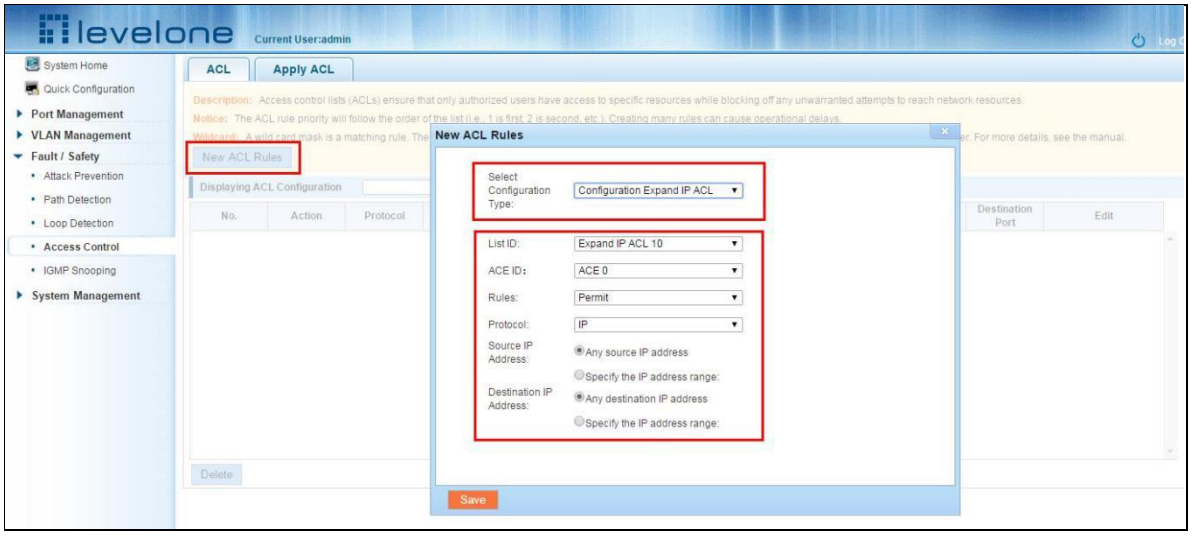


Figure 5-20: Configuration standard IP access control list

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"：

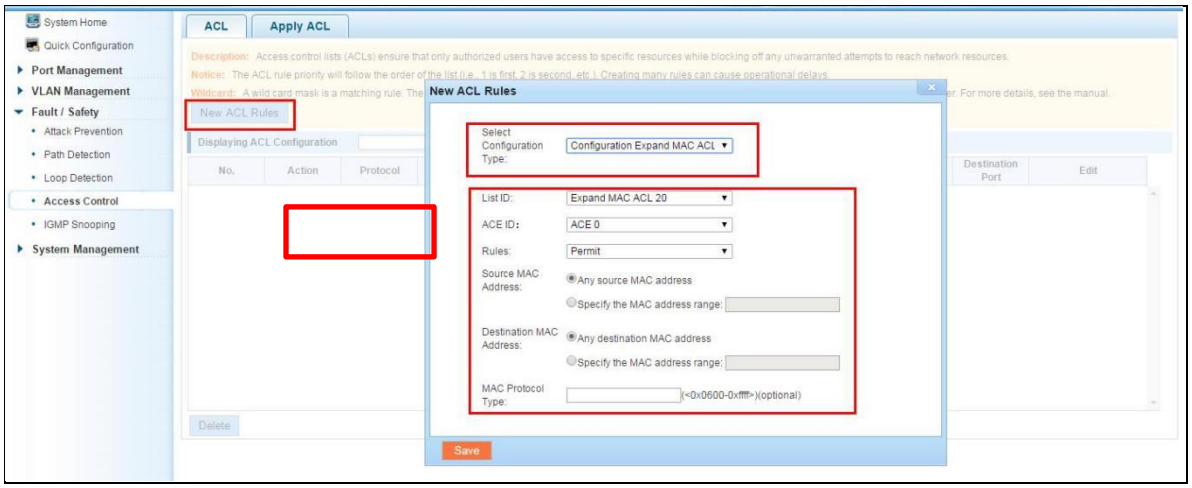


Figure 5-21: Configuration extended MAC access control list

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":

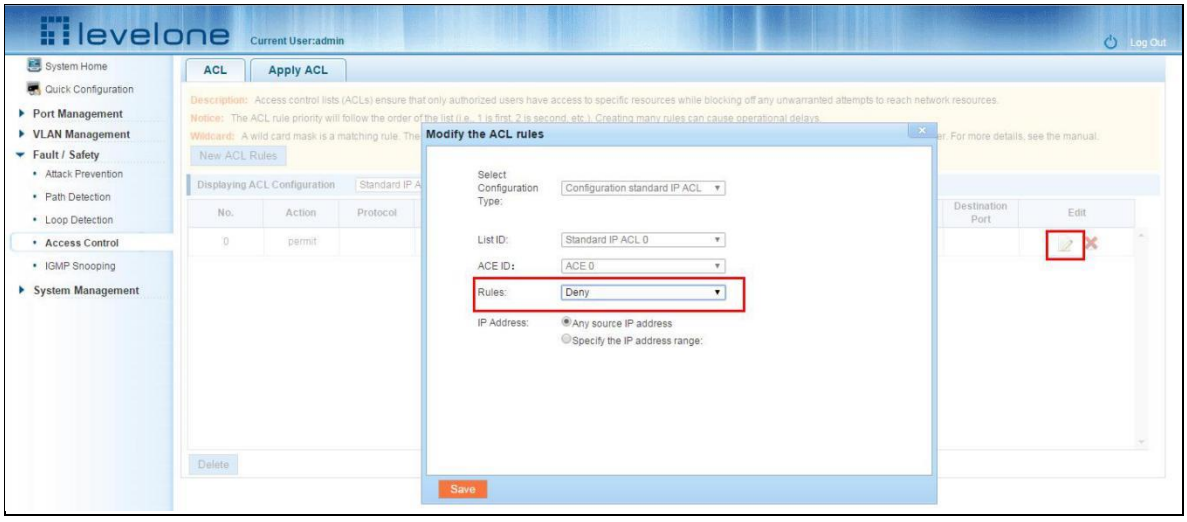


Figure 5-22: To modify the ACL rule

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:

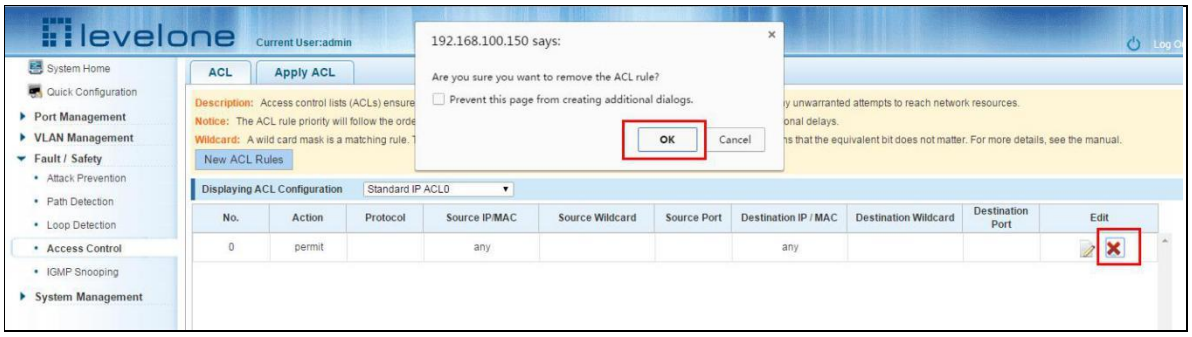


Figure 5-23: Delete rules

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

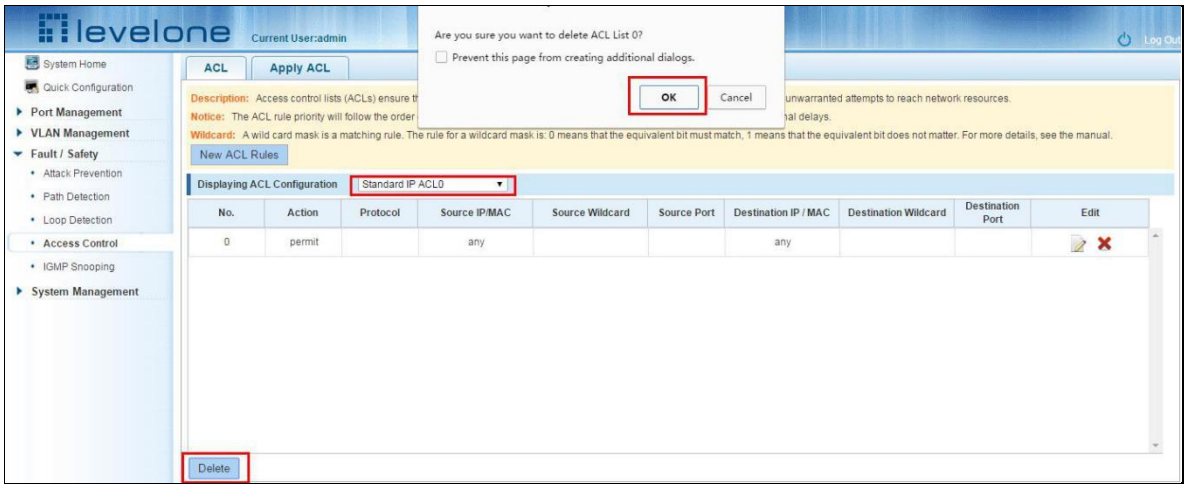


Figure 5-24: Delete ACL rules

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:

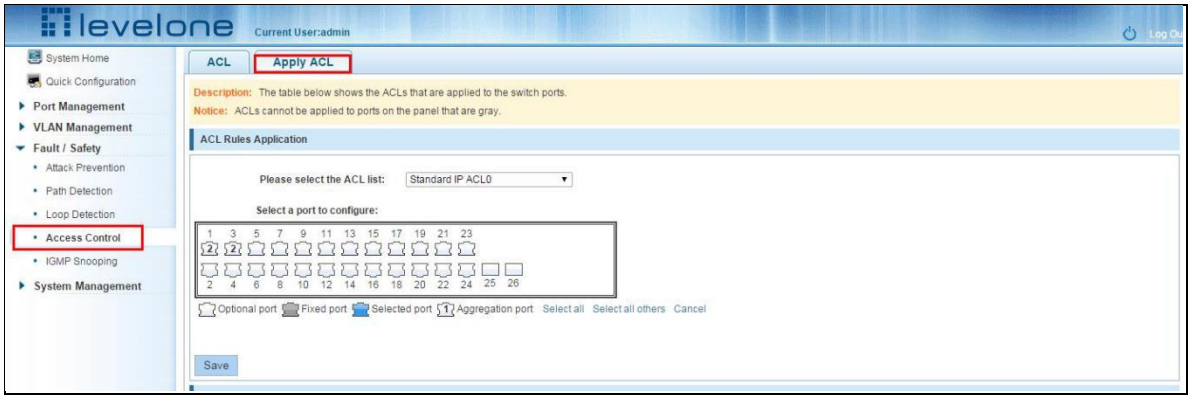


Figure 5-25: View application ACL rules

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:

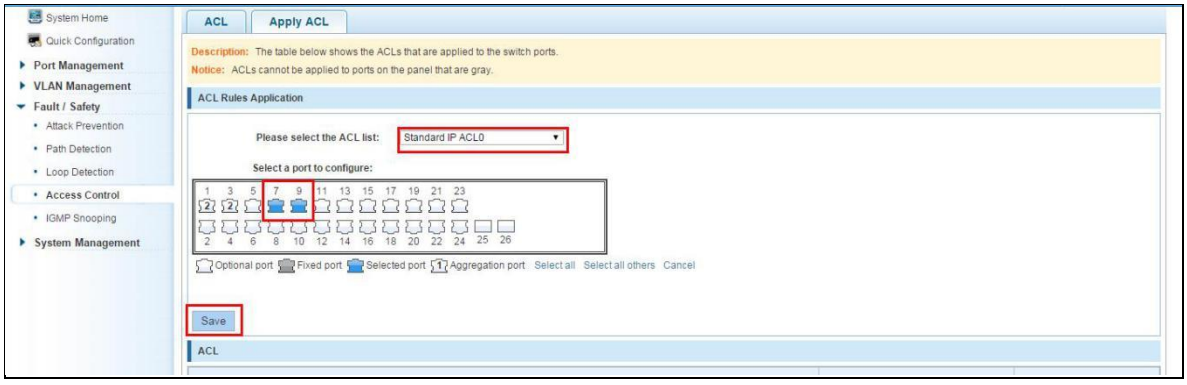


Figure 5-26: Add applications ACL

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:

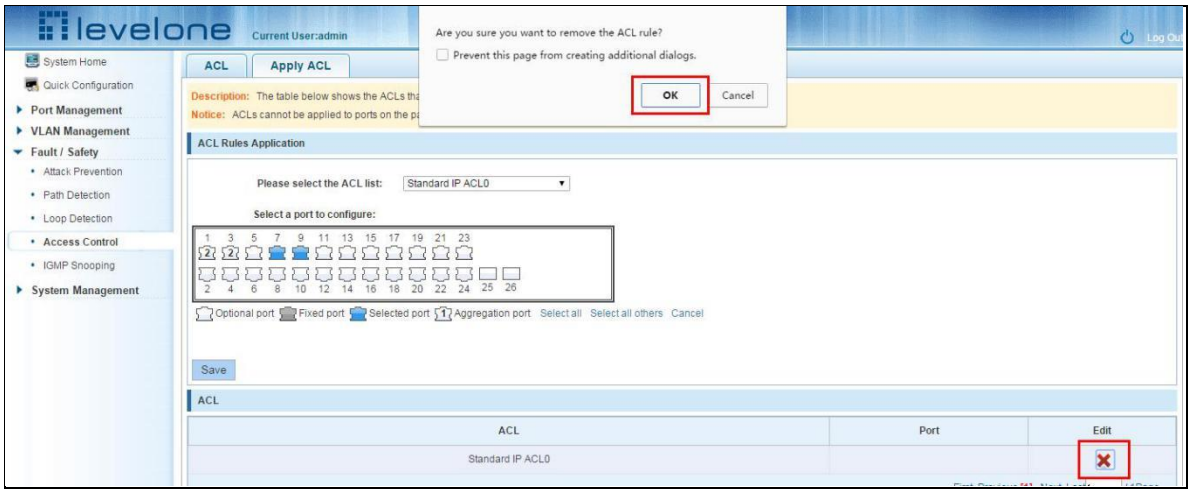


Figure 5-27: Delete application ACL

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:

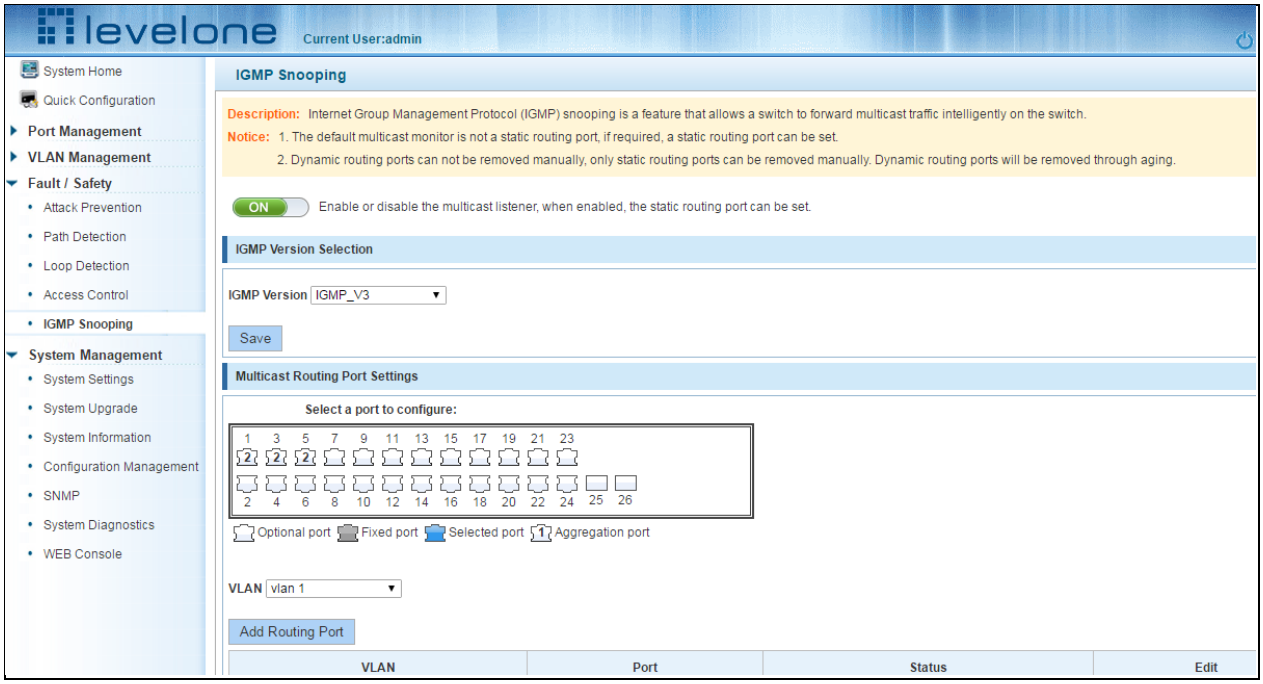


Figure 5-28: View Snooping IGMP configuration information

5.5.2 ACTIVE MULTICAST LISTENER FUNCTION

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

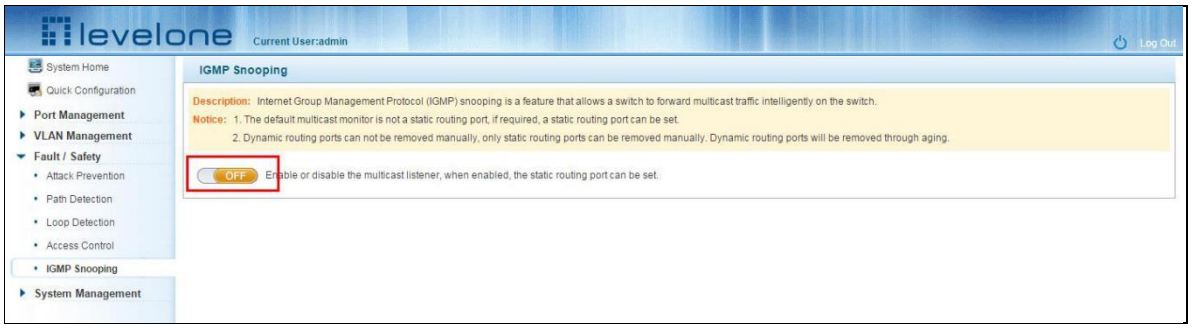


Figure 5-29: Open multicast listener configuration

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:

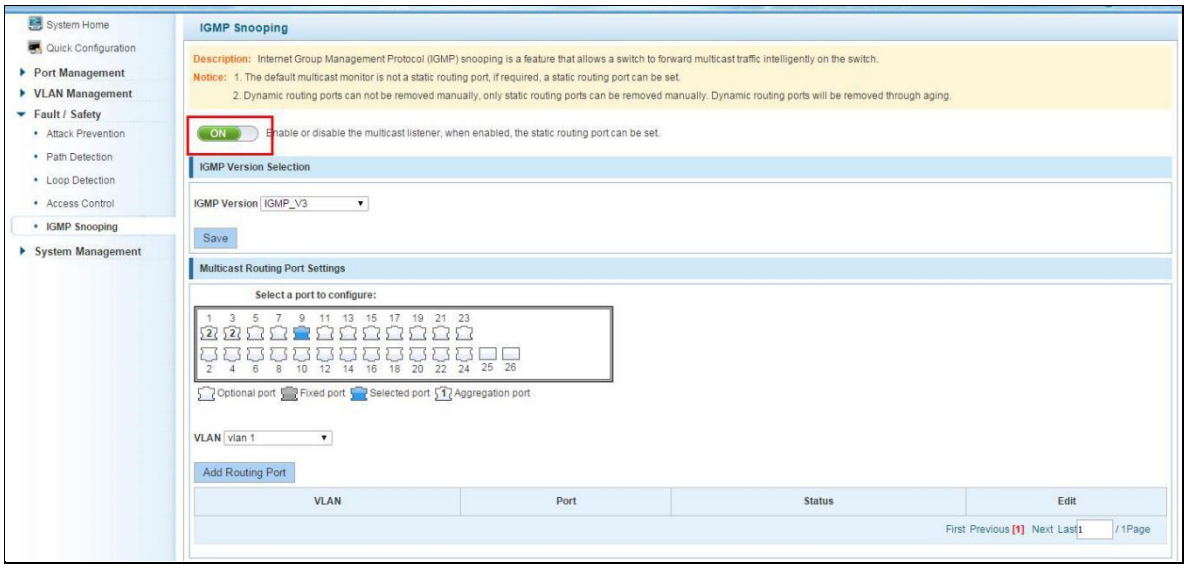


Figure 5-30: Closed multicast listener function operation

5.5.4 CONFIGURATION MULTICAST ROUTING

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

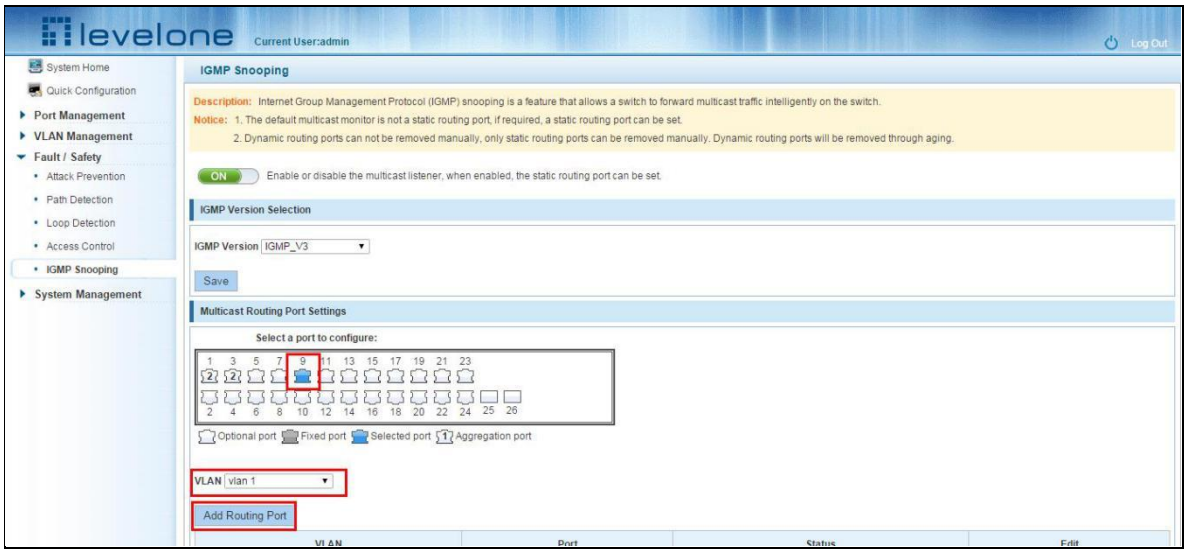


Figure 5-31: Configuration of multicast routing

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:

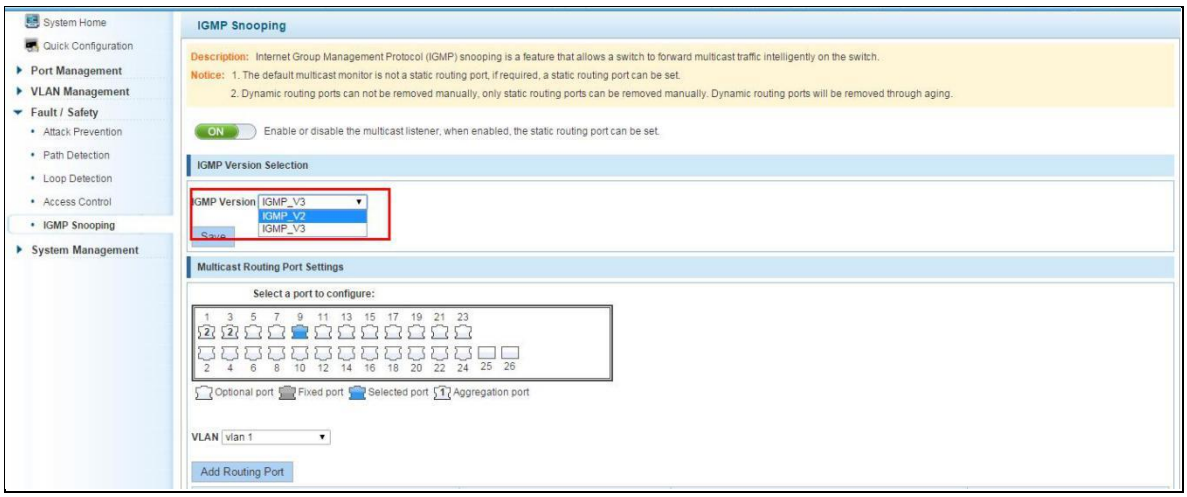


Figure 5-32: Configuration IGMP version

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:

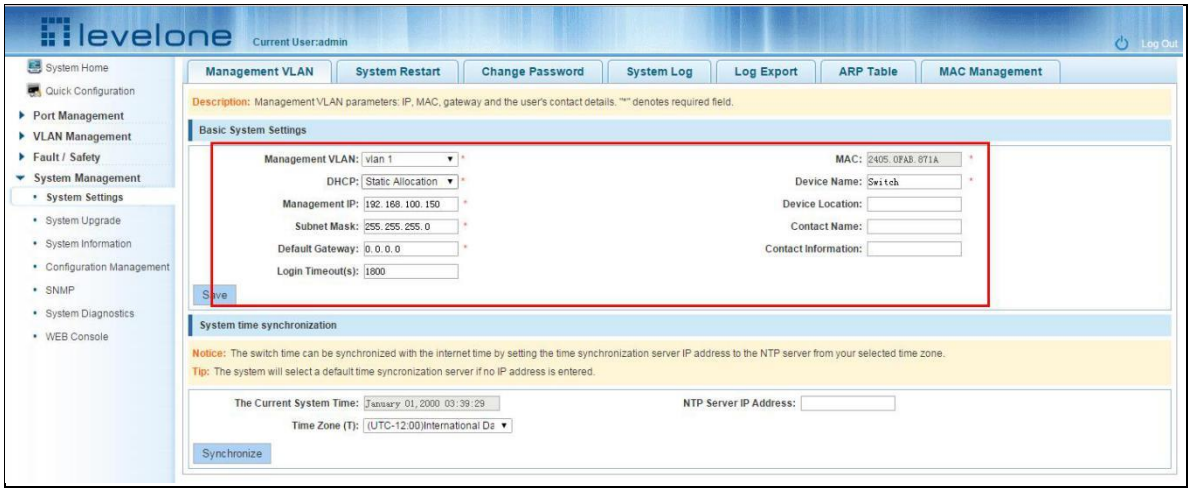


Figure 6-1: basic system settings

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

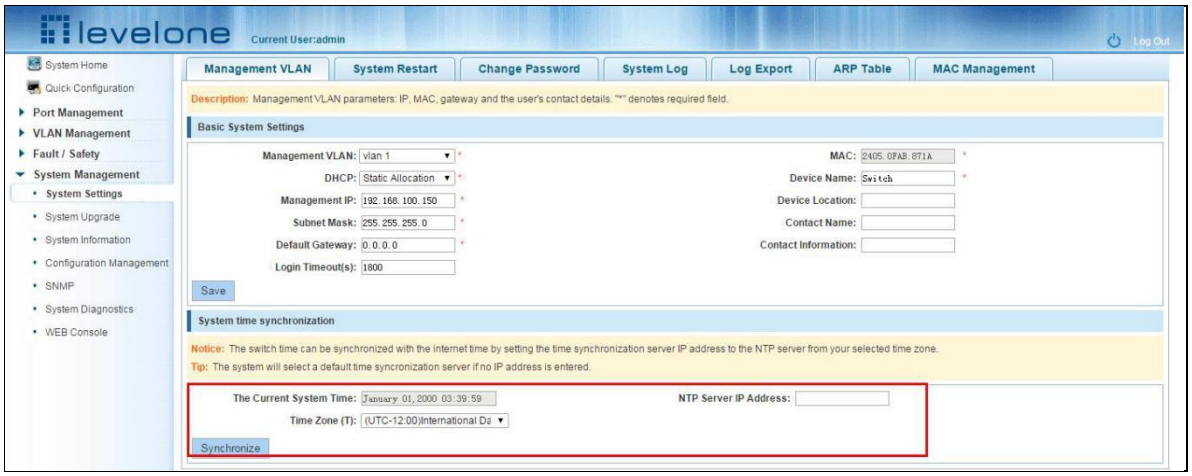


Figure 6-2: System time synchronization

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:

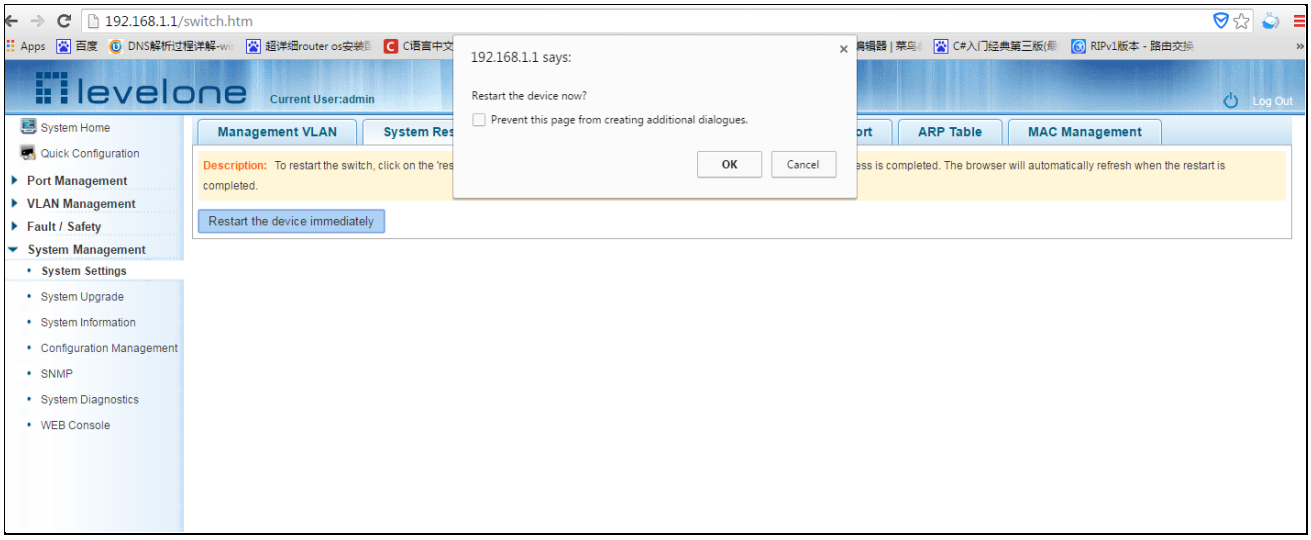


Figure 6-3: System Restart

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:

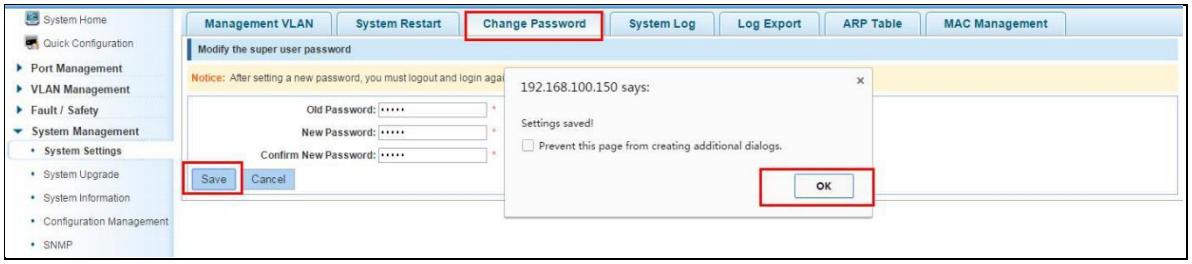


Figure 6-4: change password

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:

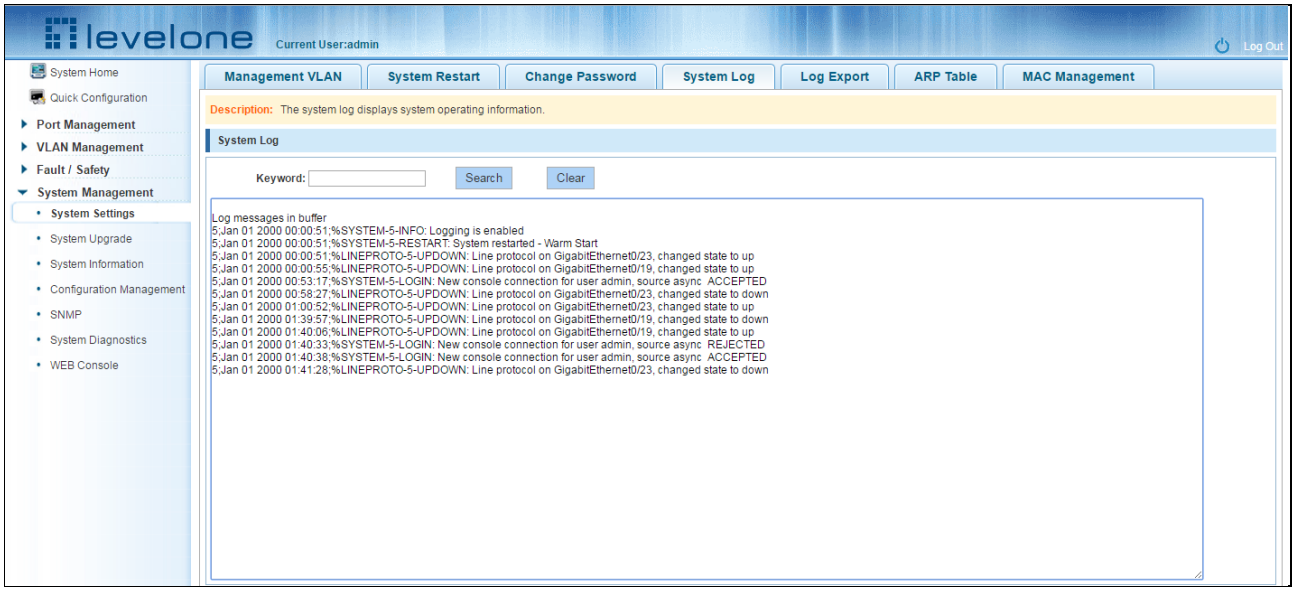


Figure 6-5: system log

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.

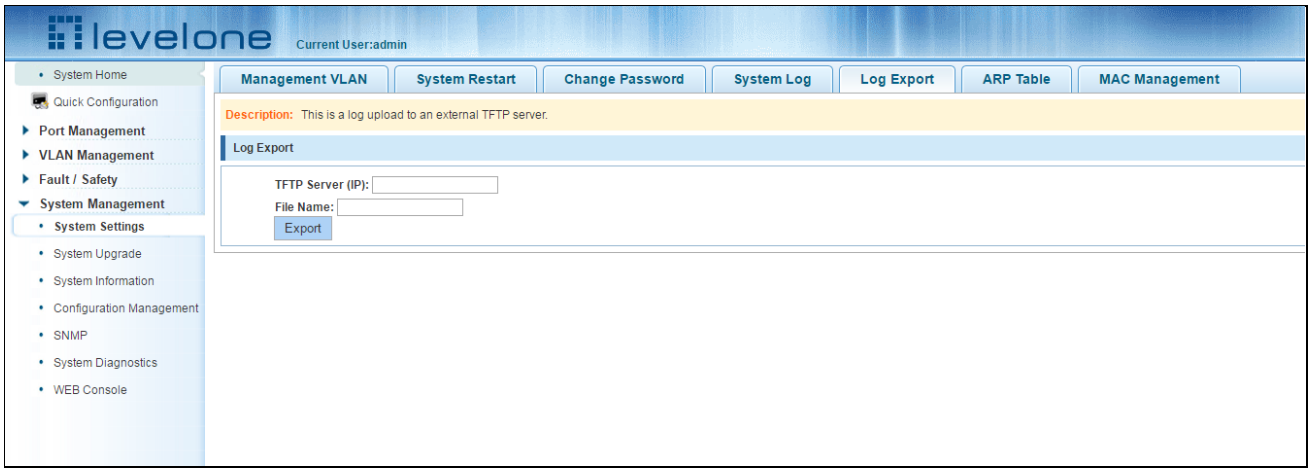


Figure 6-6: Log Export

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:

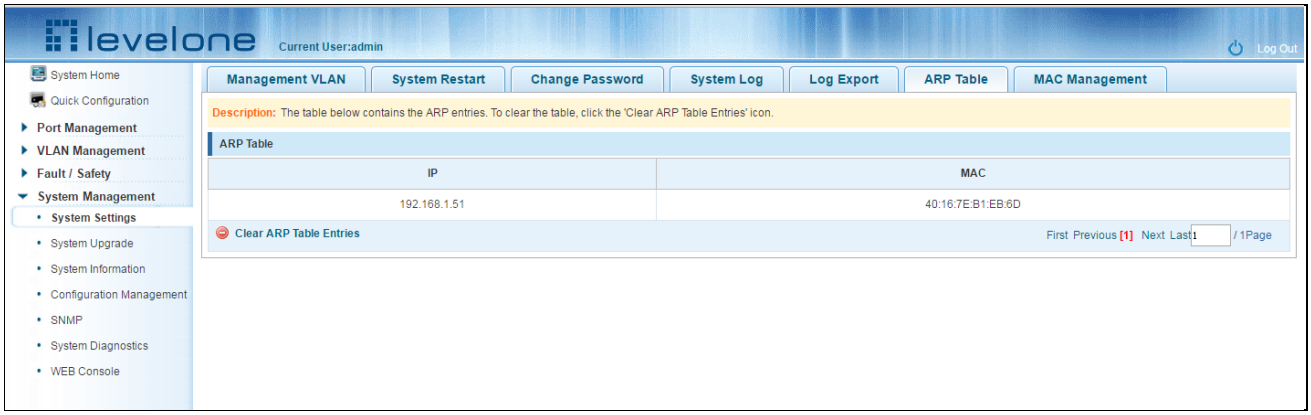


Figure 6-7: ARP message

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:

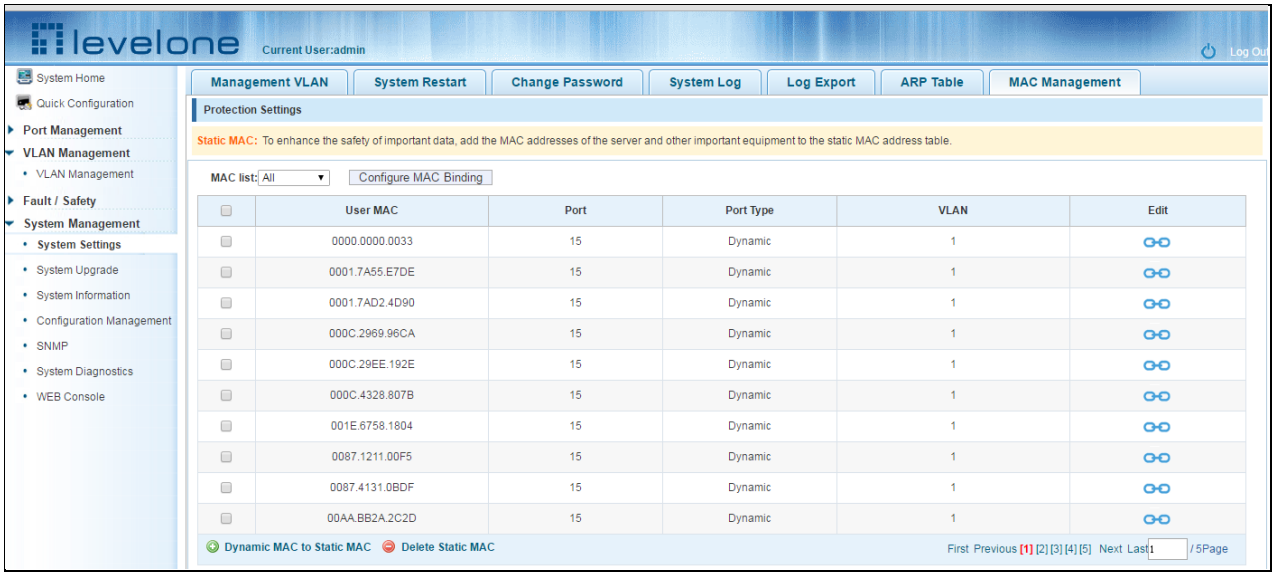


Figure 6-8: MAC address lookup display

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:

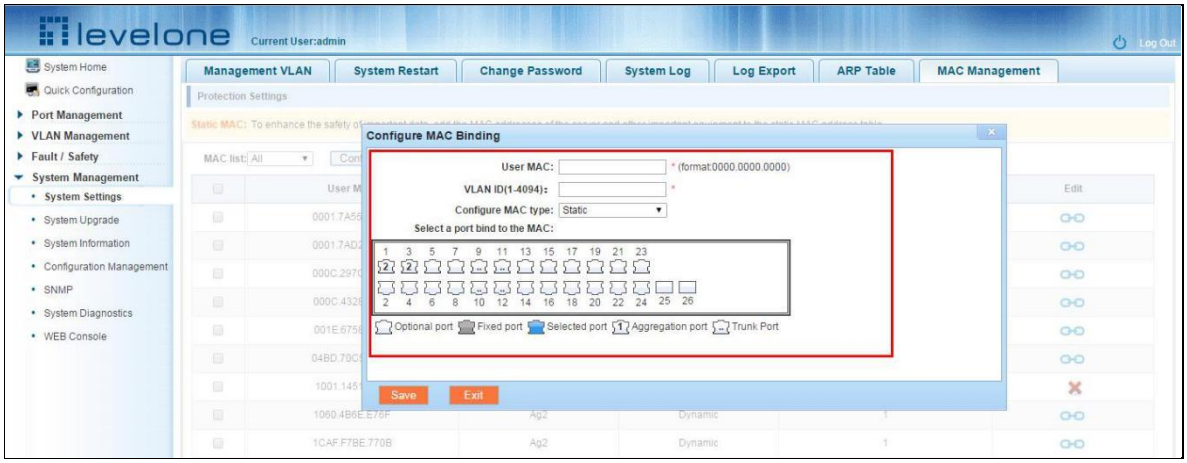


Figure 6-9: MAC addresses statically bound static configuration

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;step4: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:

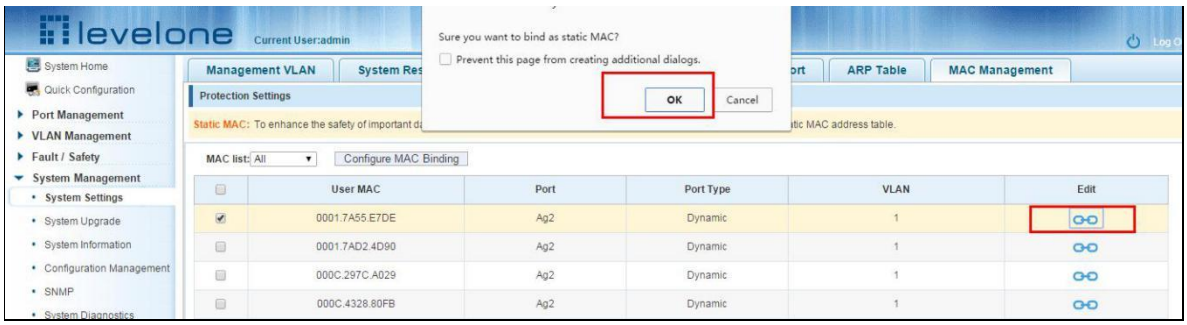


Figure 6-10: MAC address of the static binding configuration

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:

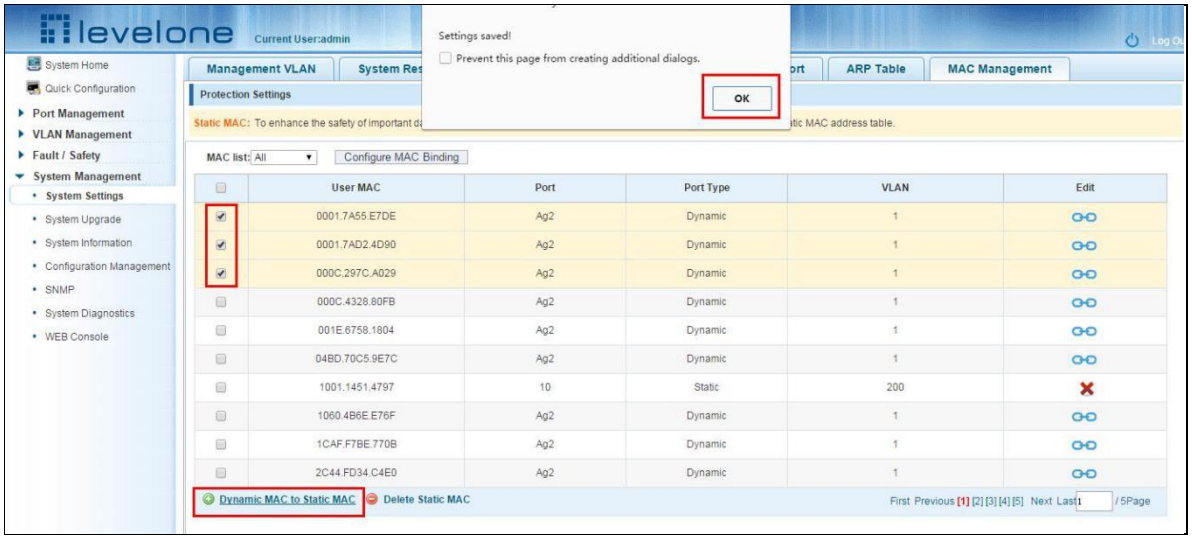


Figure 6-11: Batch-MAC binding configuration

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:

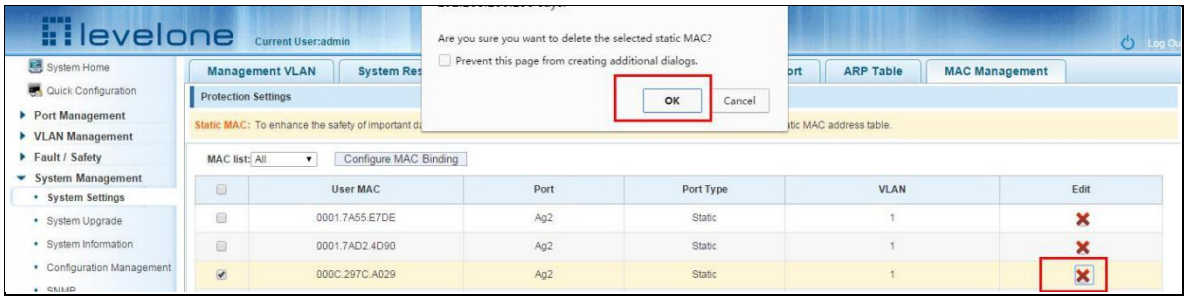


Figure 6-12: MAC address deletion

Remove MAC address configuration steps are as follows:

Step1:To delete the selected MAC address,step2:Click“ ✖ ” 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:

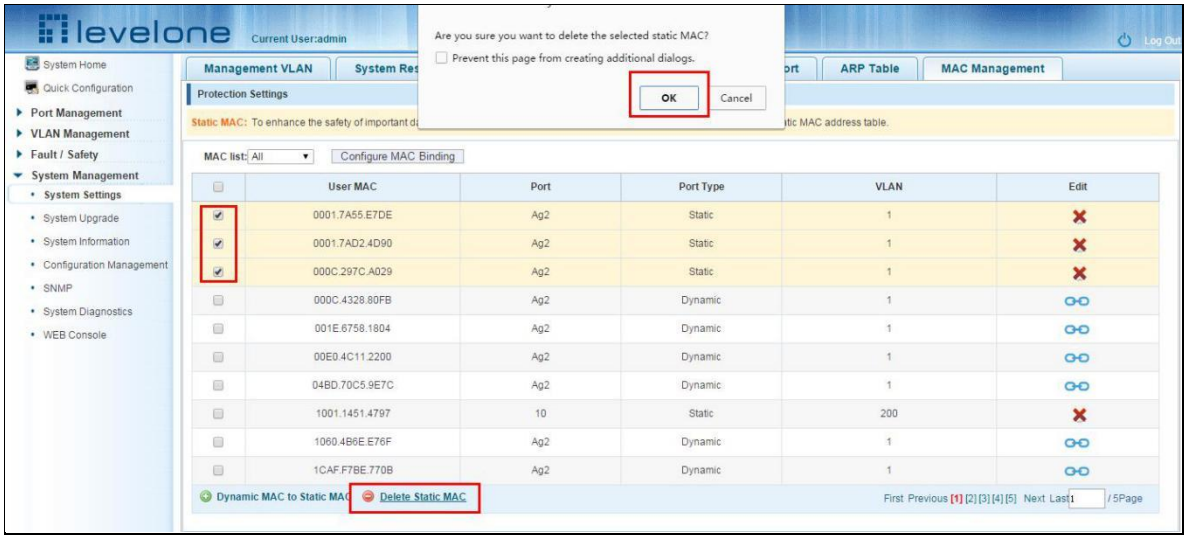


Figure 6-13: MAC address batch deletion deletion

6.2 SYSTEM UPGRADE

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

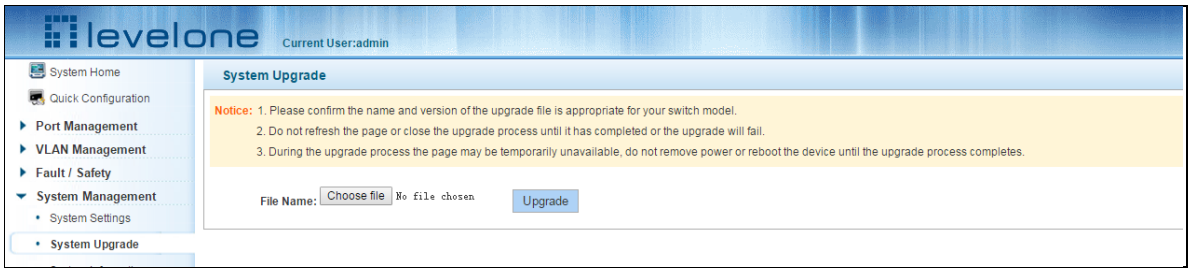


Figure 6-14: Switch System Upgrade

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:

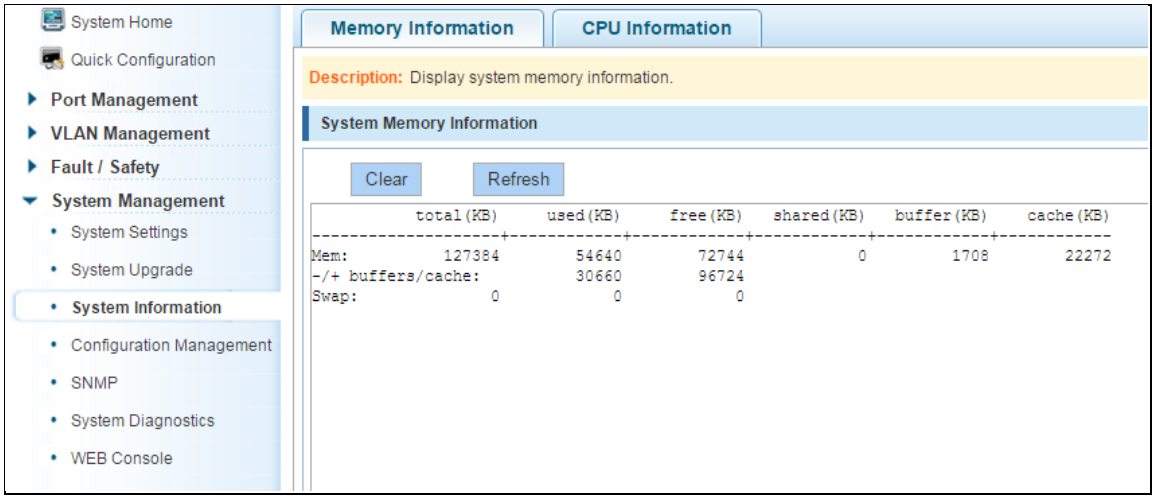


Figure 6-15: System memory information

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:

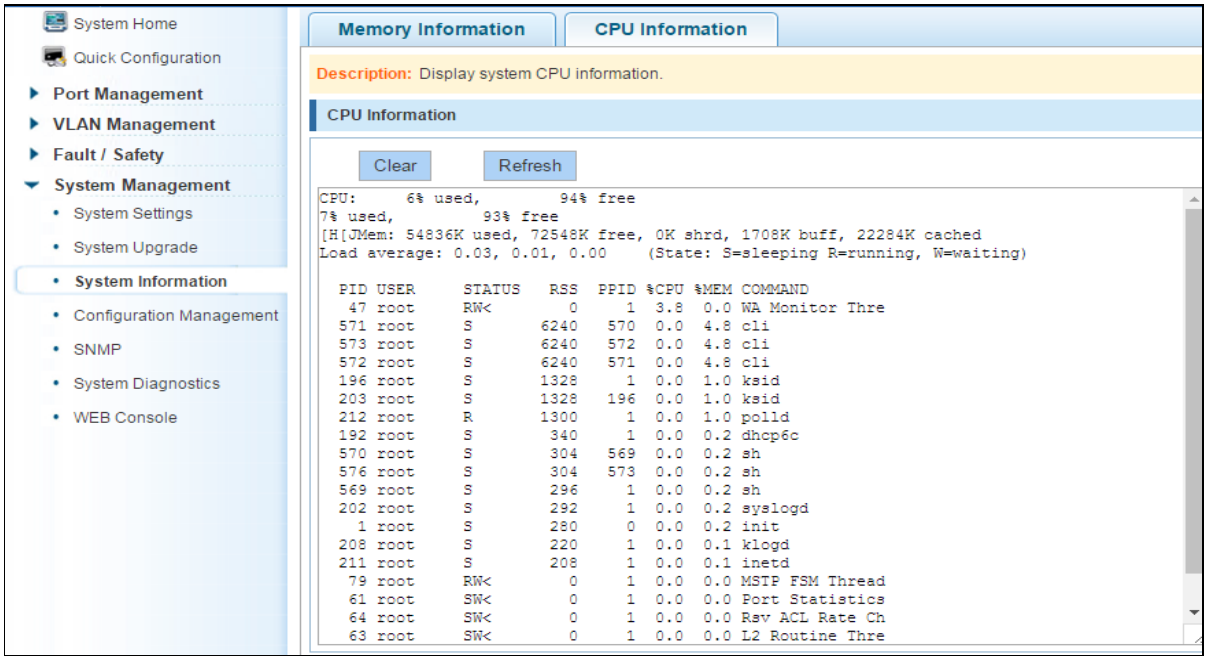


Figure 6-16: CPU information

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:

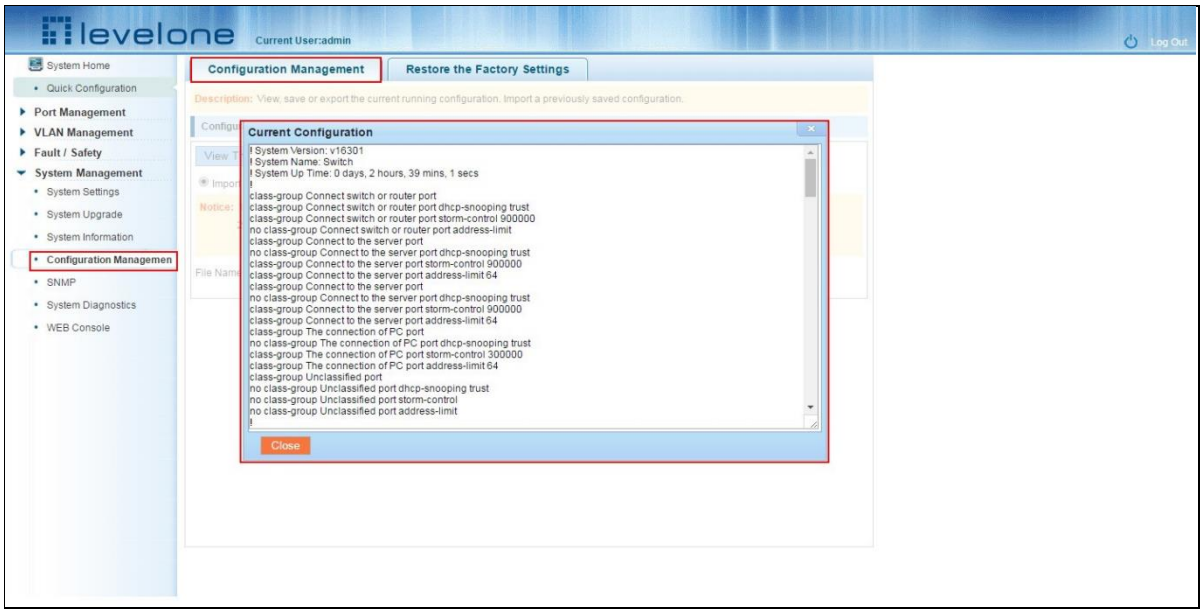


Figure 6-17: View the current configuration

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:

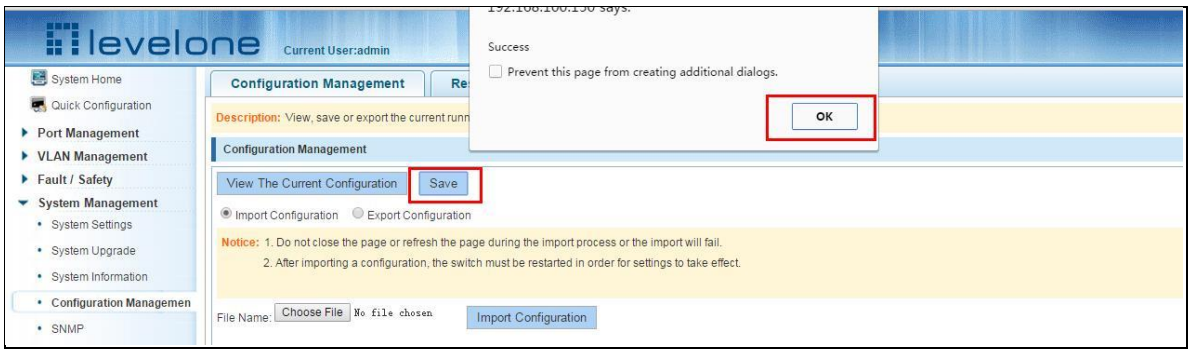


Figure 6-18: To save the current configuration

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:

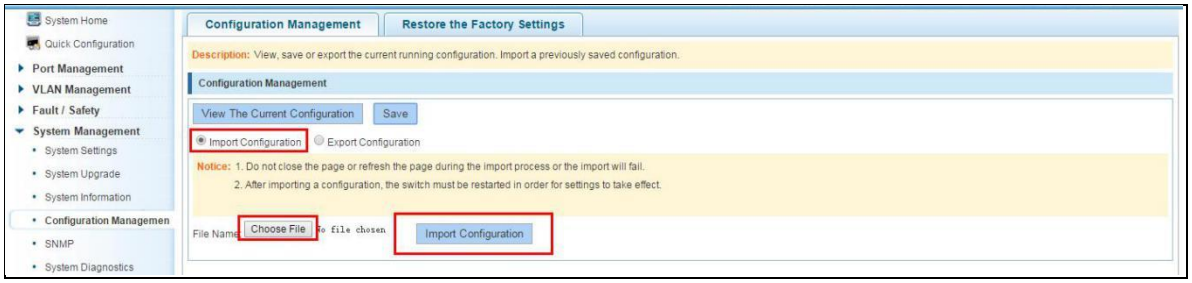


Figure 6-19: Imported configuration

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.

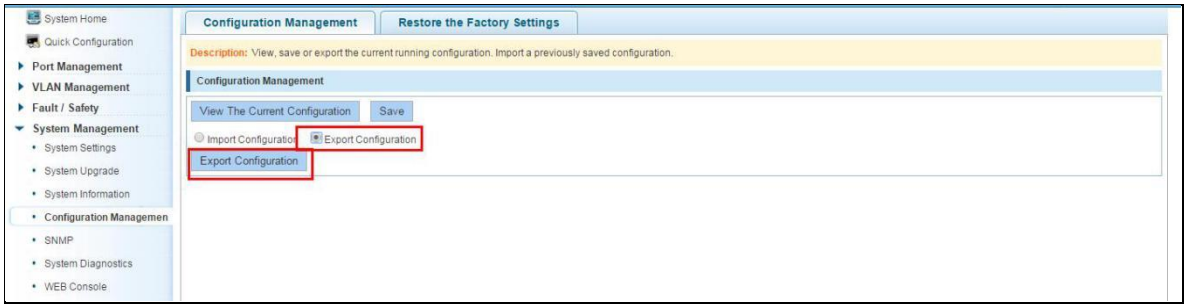


Figure 6-20: Export configuration

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:

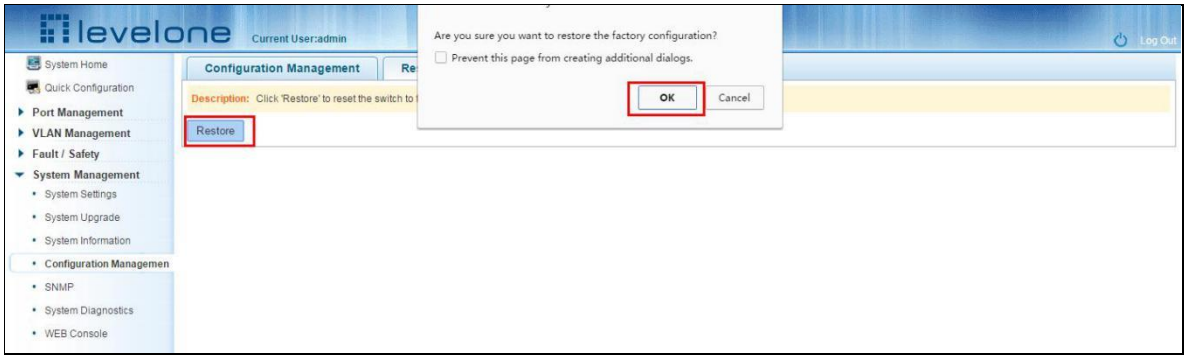


Figure 6-21: Restore factory Settings

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:

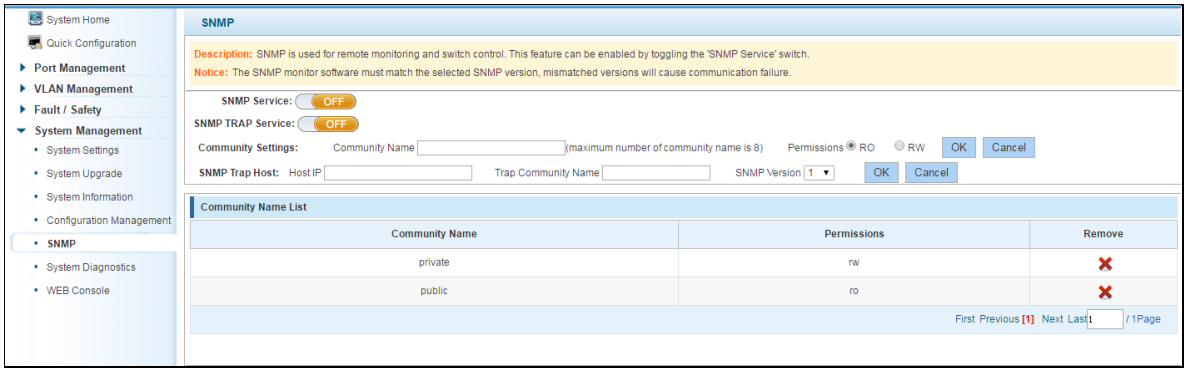


Figure 6-22: View the SNMP configuration information

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:

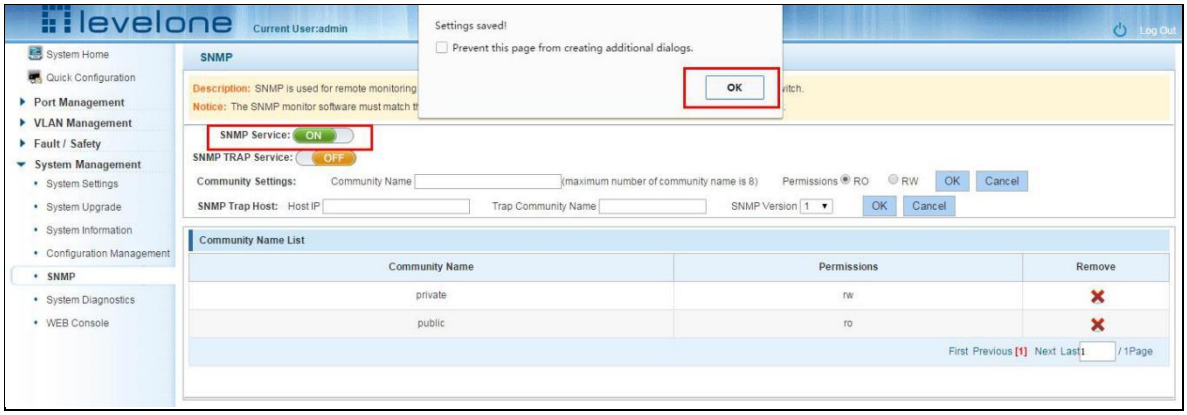


Figure 6-23: Activation SNMP function

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:

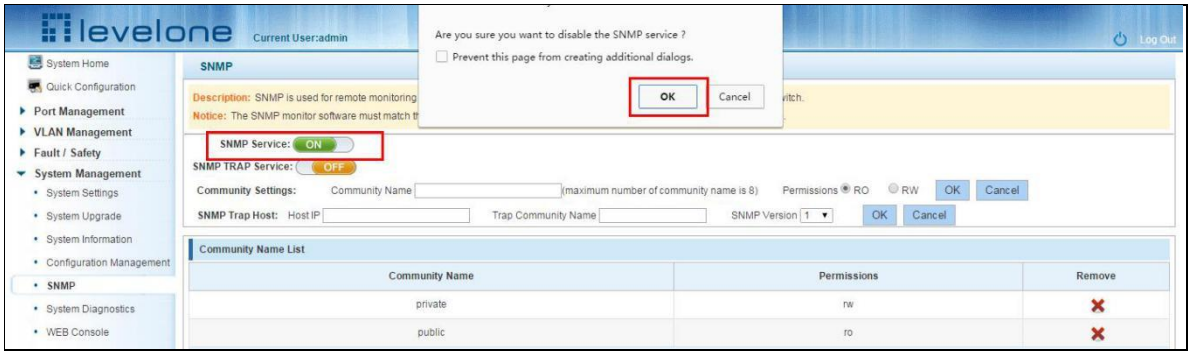


Figure 6-24: Disable the SNMP function

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:

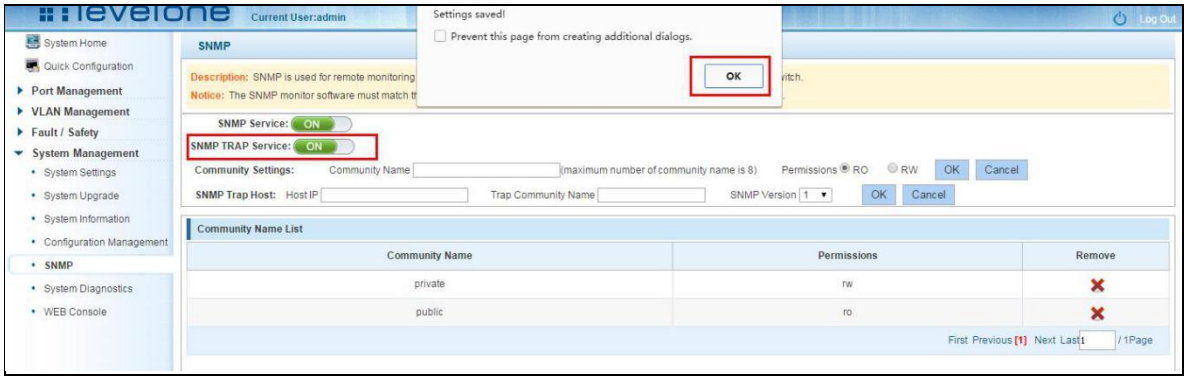


Figure 6-25: Activation function of the TRAP

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:

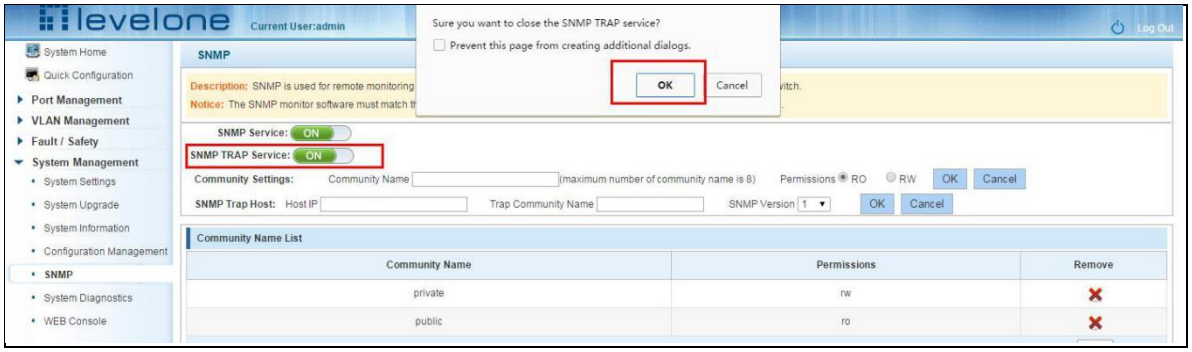


Figure 6-26: Disable TRAP function

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:

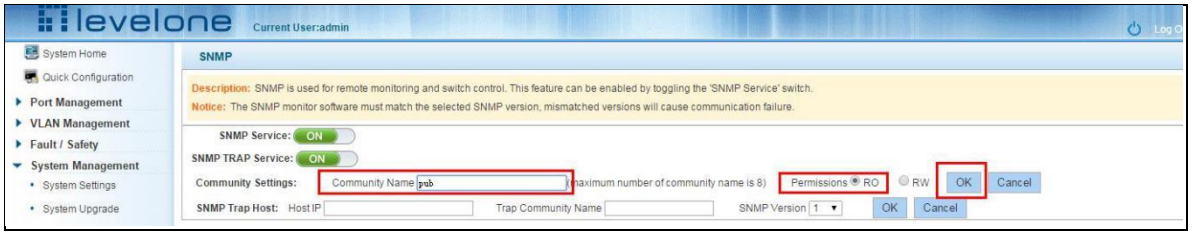


Figure 6-27: Increase community

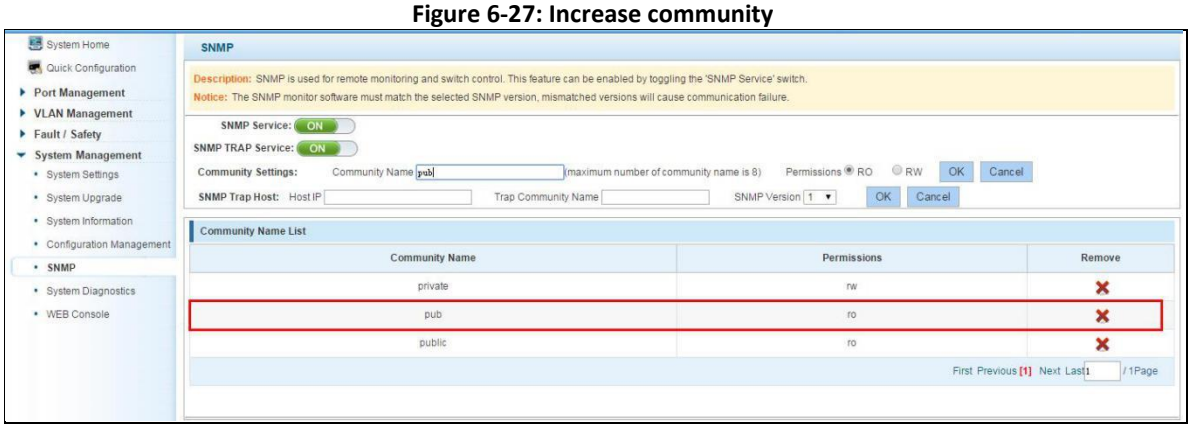


Figure 6-28: Community results

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:

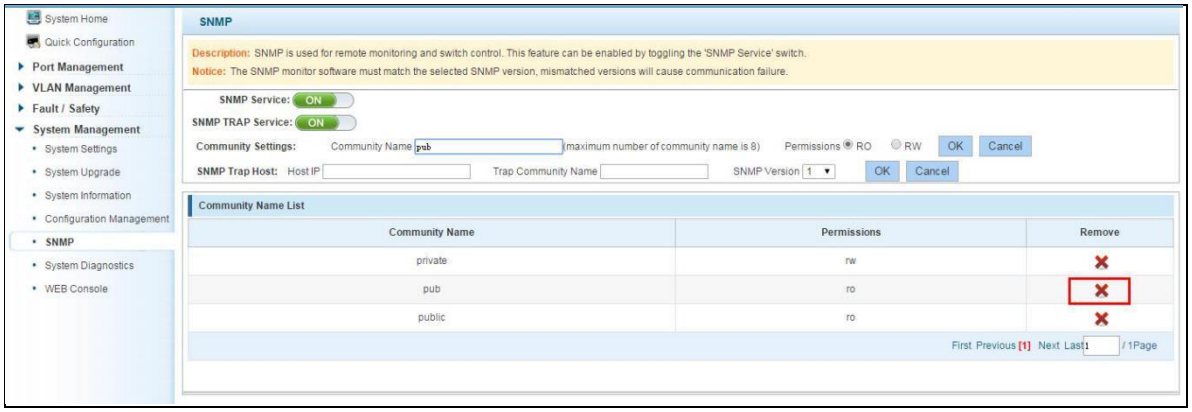


Figure 6-29: Delete community

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:

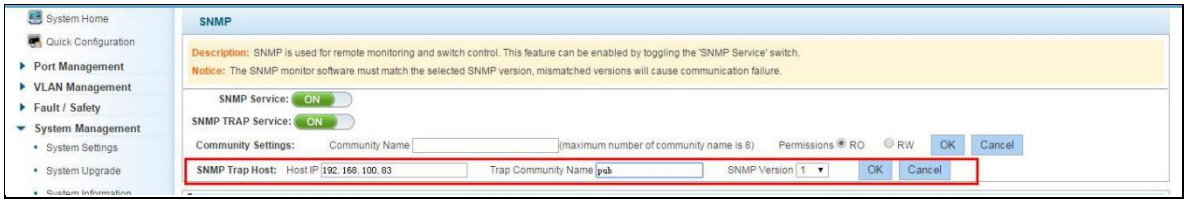


Figure 6-30: Increases the SNMP TRAP service host

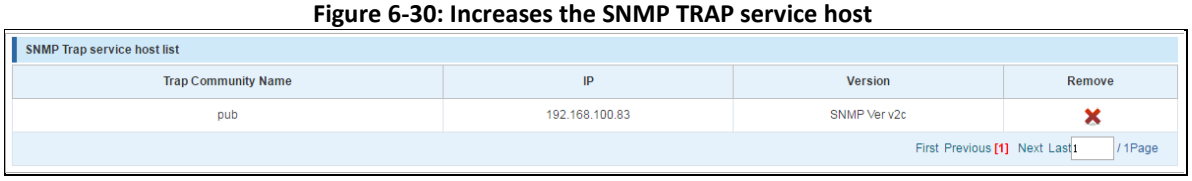


Figure 6-31: SNMP TRAP service host

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:

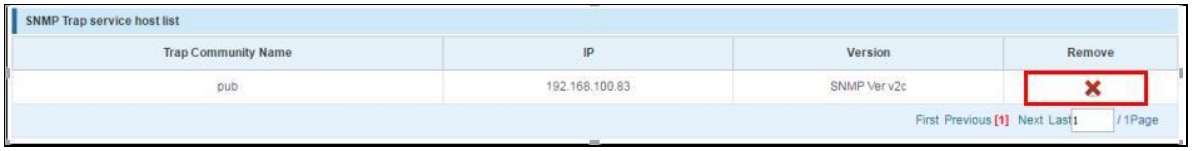


Figure 6-32: Delete community

6.6 SYSTEM DIAGNOSTICS

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

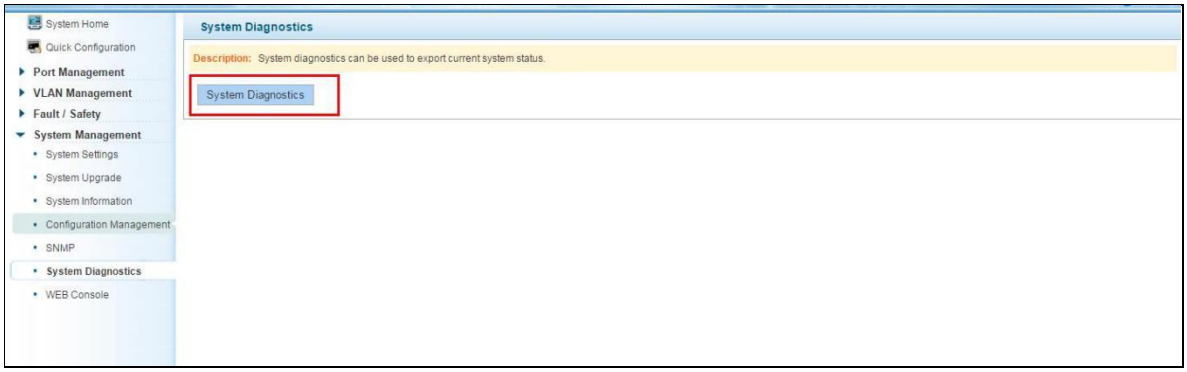


Figure 6-33: Key fault collection

6.7 THE WEB CONSOLE

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

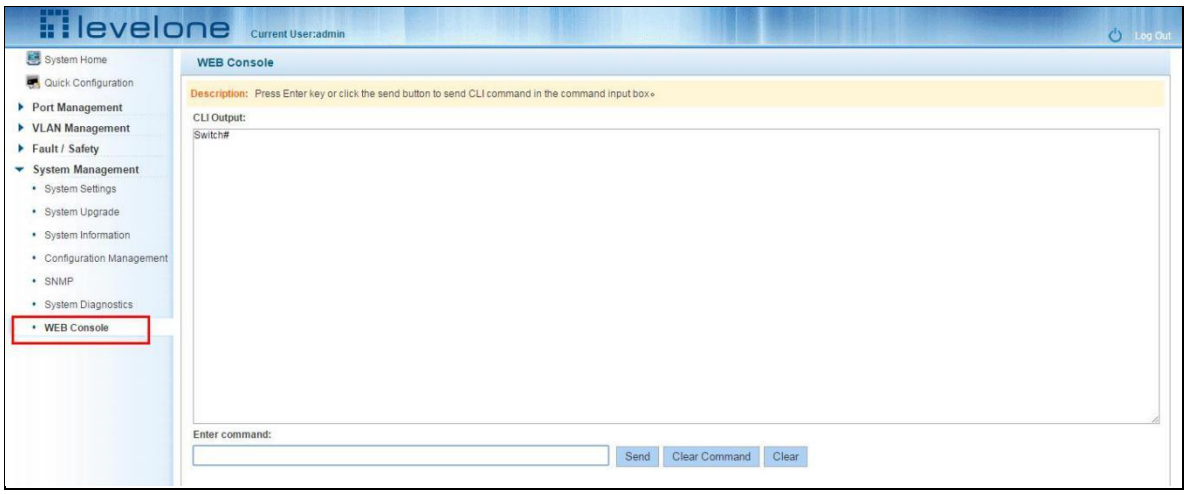


Figure 6-34: Web console

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.

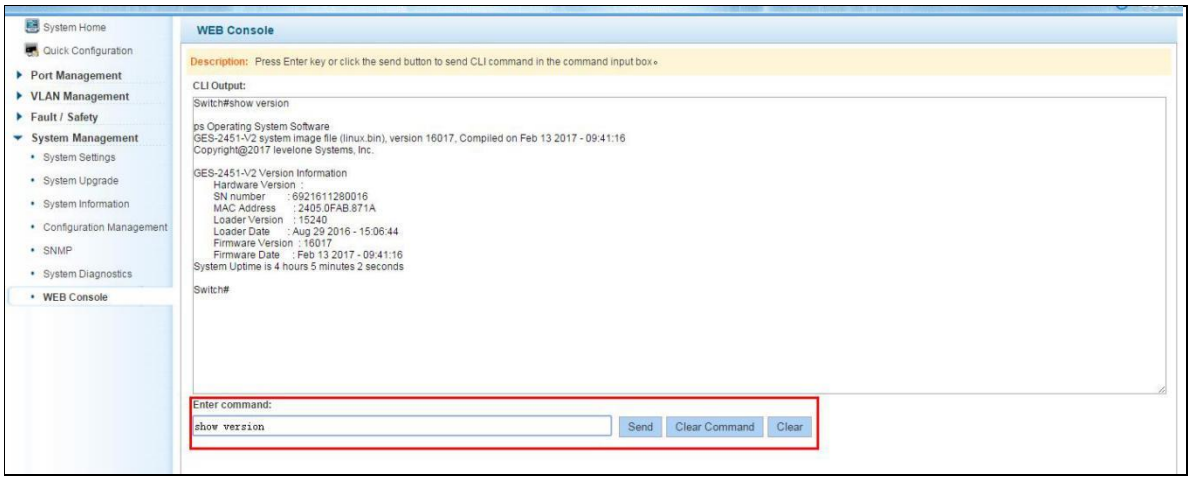


Figure 6-35: Web console operation