



EKSELANS BY ITS

USER MANUAL

SWG 24 L2

334200

Switch Ethernet Layer2. 24 ports x GB
Ethernet + 4 x SFP. 1Gbps

V01

TABLE OF CONTENTS

| | |
|---|----|
| Introduction..... | 7 |
| Description..... | 7 |
| Main characteristics..... | 7 |
| Package contents..... | 7 |
| WEB MANAGEMENT LANDING PAGE..... | 8 |
| Log in to the switch management page WEB..... | 8 |
| System home..... | 9 |
| Device panel..... | 9 |
| Port information..... | 10 |
| Flow trend..... | 11 |
| Device configuration..... | 12 |
| Port statistics..... | 13 |
| Quick configuration..... | 14 |
| VLAN setting..... | 14 |
| PORT MODE..... | 15 |
| BASIC SETTING..... | 15 |
| Port Management..... | 16 |
| Basic Settings..... | 16 |
| Check the port configuration..... | 16 |
| Configuring Port Properties..... | 17 |
| Storm Control..... | 18 |
| Check the port settings Storm..... | 18 |
| FLOW CONTROL..... | 21 |
| Configuring Flow Control..... | 21 |
| Port Aggregation..... | 23 |
| Viewing Port Aggregation Configuration..... | 23 |
| Add port aggregation..... | 24 |
| Modifying port aggregation..... | 24 |
| Port Mirroring..... | 25 |
| Port Mirroring Configuration..... | 25 |

| | |
|---|----|
| Add port mirroring group..... | 26 |
| To modify the port mirroring group..... | 27 |
| Delete a port mirroring group..... | 28 |
| Port ISOLATION..... | 29 |
| Port ISOLATION Configuration..... | 29 |
| Configuring port isolation..... | 29 |
| Modify the port isolation..... | 30 |
| Port speed limit..... | 31 |
| View port rate limit..... | 31 |
| Configure port access rate..... | 32 |
| Remove the port speed limit..... | 33 |
| Vlan management..... | 34 |
| VLAN management..... | 34 |
| Check VLAN configuration information..... | 34 |
| Adding a VLAN..... | 35 |
| Remove VLAN..... | 36 |
| VLAN PORT TO A VLAN..... | 37 |
| TO REMOVE THE PORT FROM A VLAN..... | 38 |
| View port MODE..... | 39 |
| CHANGE THE PORT MODE IS TRUNK..... | 40 |
| Change the port mode is hybrid..... | 41 |
| Voice VLAN..... | 42 |
| View voice VLAN information..... | 42 |
| Configure voice VLAN global..... | 42 |
| Configure voice VLAN port..... | 43 |
| Configure voice VLAN OUI..... | 44 |
| Voice device address..... | 44 |
| Surveillance VLAN..... | 45 |
| View surveillance VLAN information..... | 45 |
| Configure surveillance VLAN..... | 45 |
| MAC Settings and Surveillance Device..... | 46 |
| MAC Settings and Surveillance Device..... | 46 |
| ONVIF..... | 47 |
| View ONVIF..... | 47 |
| View IP-Camera information..... | 50 |
| View Nvr information information..... | 51 |
| Fault / safety..... | 51 |

| | |
|---|----|
| ATTACK PREVENTION..... | 51 |
| VIEW ARP CONFIGURATION..... | 51 |
| ARP INSPECTION FUNCTION..... | 52 |
| DISABLE ARP INSPECTION FUNCTION..... | 53 |
| CONFIGURATION PORT SECURITY..... | 54 |
| CHANGE PORT SECURITY STATUS..... | 55 |
| VIEW DHCP snooping CONFIGURATION..... | 56 |
| OPEN DHCP snooping FUNCTION..... | 56 |
| SET THE PORT TO DHCP SNOOPING TRUSTED PORT..... | 57 |
| Configure CID information..... | 58 |
| OFF DHCP snooping FUNCTION..... | 58 |
| CPU GUARD..... | 59 |
| Path detection..... | 60 |
| Path /Tracert detection..... | 60 |
| Cable Detection..... | 61 |
| DDOS PROTECTION..... | 62 |
| Loop detection..... | 63 |
| Choose the port to configure..... | 63 |
| STP..... | 65 |
| ENABLE STP function..... | 65 |
| ENABLE LOOPBACK DETECTION..... | 66 |
| STP PORT SETTINGS..... | 66 |
| Access control..... | 67 |
| VIEW ACCESS CONTROL LIST..... | 67 |
| INCREASE THE STANDARD IP ACCESS RULES..... | 68 |
| INCREASE THE EXTENDED IP ACCESS RULE..... | 68 |
| INCREASING EXPAND MAC ACCESS RULES..... | 69 |
| MODIFY CONFIGURATION..... | 70 |
| DELETE RULE..... | 70 |
| VIEW APPLICATION ACL..... | 72 |
| INCREASED APPLICATION ACL..... | 72 |
| IGMP Snooping..... | 74 |
| VIEW IGMP SNOOPING CONFIGURATION..... | 74 |
| ACTION MULTICAST LISTENER FUNCTION..... | 75 |
| DISABLE MULTICAST LISTENNER FUNCTION..... | 75 |
| CONFIGURATION MULTICAST ROUTING..... | 76 |
| IGMP VERSION..... | 77 |

| | |
|--|-----|
| VIEW MLD CONFIGURATION..... | 77 |
| ACTIVE MULTICAST LISTENER FUNCTION..... | 78 |
| DISABLE MULTICAST LISTENER FUNCTION..... | 78 |
| CONFIGURATION MULTICAST ROUTING..... | 79 |
| IEEE 802.1X..... | 80 |
| AAA..... | 83 |
| RADIUS..... | 83 |
| TACACS+..... | 85 |
| System management..... | 87 |
| System settings..... | 87 |
| CONFIGURATION BASIC SYSTEM SETTINGS..... | 87 |
| SYSTEM TIME SYNCHRONIZATION..... | 88 |
| System restart..... | 89 |
| Change PassWord..... | 90 |
| System Log..... | 91 |
| Log Export..... | 91 |
| ARP table..... | 92 |
| MAC management..... | 92 |
| DHCP server..... | 97 |
| Firmware Upgrade..... | 98 |
| System information..... | 99 |
| Memory information..... | 99 |
| CPU INFORMATION..... | 100 |
| Configuration management..... | 101 |
| Configuration management..... | 101 |
| Restore factory Settings..... | 104 |
| Dual Configuration..... | 105 |
| SNMP..... | 110 |
| RMON..... | 117 |
| LLDP Settings..... | 121 |
| LLDP settings..... | 121 |
| NEIGHBOR INFO..... | 122 |
| Administration..... | 122 |
| TELNET..... | 122 |
| Static Route..... | 124 |
| QOS..... | 126 |
| Priority Schedule..... | 126 |

| | |
|---------------------------|-----|
| EEE..... | 134 |
| EEE..... | 134 |
| 802.3AZ EEE SETTINGS..... | 134 |

Introduction.

Description.

Switch Ethernet Layer2. 24 ports x GB Ethernet + 4 x SFP. 1Gbps.

Main characteristics.

- 24 Port 10/100/1000Mbps + 4 SFP port.
- Layer 2+ function for an efficient routing.
- Standard IEEE802.3, 802.3u, 802.3ab, 802.3x.
- VLAN management, IGMP snooping, MACs admin, port mirroring.
- Web management interface, SSH, TELNET, SNMP.
- 1U / Rack 19".
- Multi-cast facilities (companies, hotels, hospitals, SoHo).
- Suitable product to include in GPON by EK, EK CAST, EK HOTEL or Wi-Fi by EK installations.

Package contents.

- Rack Mounting Kit.
- Power cord.
- Four adhesive rubber feet.
- Documentation.

WEB MANAGEMENT LANDING PAGE.

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 192.168.2.10, the default subnet mask of 255.255.255.0). Run WEB browser, in the address bar enter http://192.168.2.10. Enter, enter the user name and password (default user name:admin; password: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:

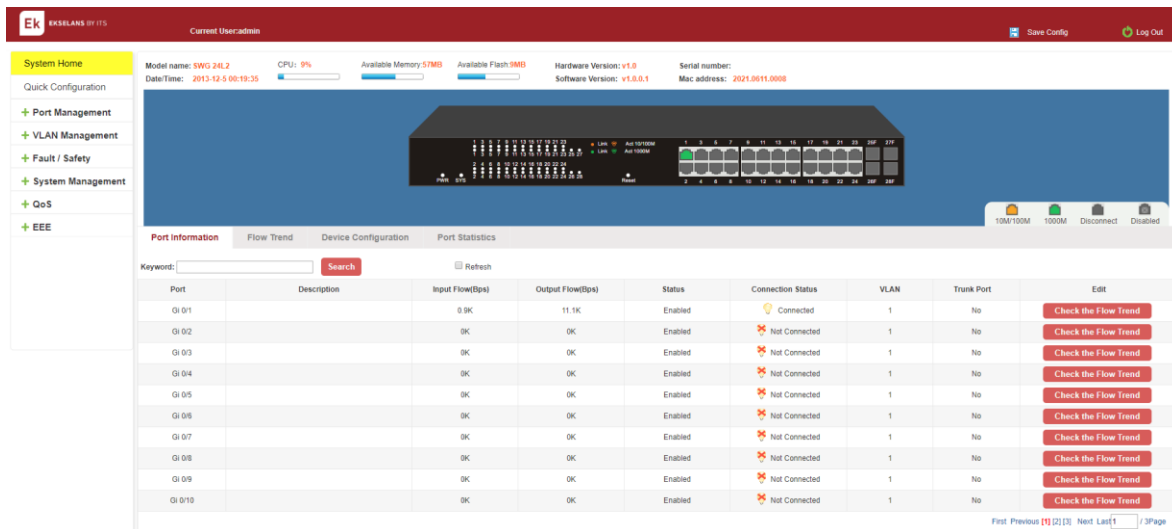


Figure 1-2: switch WEB management page Home.

System home.

Device panel.

Through the HTTP page, a quick understanding of the operation of the device, panel information, port information, such as the general network of common management information.

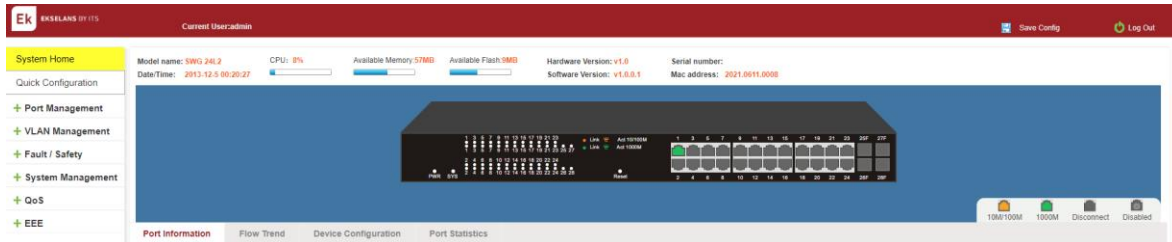


Figure 2-1: Device Panel.

Click on the specific port, you can see the following information.

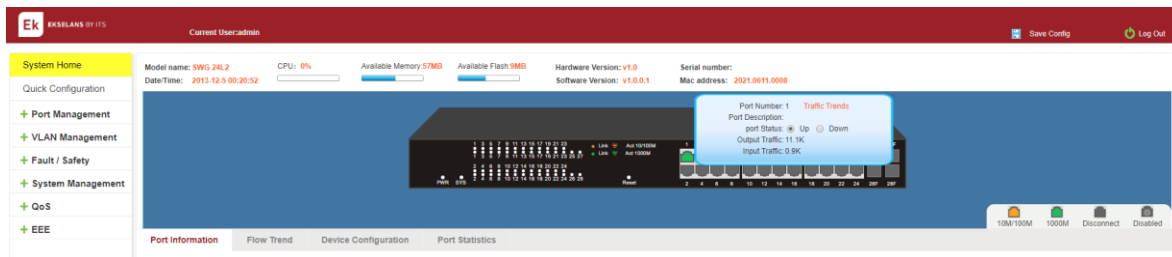


Figure 2-2: View the port status.

Port information.

The configuration of the SWG 24L2-10P is as follows: "System Home", "Port Information".

The screenshot shows the 'Port Information' page in the SWG 24L2-10P web interface. At the top, there is a navigation menu with options like 'System Home', 'Quick Configuration', 'Port Management', 'VLAN Management', 'Fault / Safety', 'System Management', 'CoS', and 'EEE'. The main content area displays a network switch image and a table of port information. The table has columns for Port, Description, Input Flow(Bps), Output Flow(Bps), Status, Connection Status, VLAN, Trunk Port, and Edit. The ports listed are Gi 0/1 through Gi 0/10. Port Gi 0/1 is 'Connected', while all other ports are 'Not Connected'. Each row has a 'Check the Flow Trend' button in the Edit column.

| Port | Description | Input Flow(Bps) | Output Flow(Bps) | Status | Connection Status | VLAN | Trunk Port | Edit |
|---------|-------------|-----------------|------------------|---------|-------------------|------|------------|----------------------|
| Gi 0/1 | | 0.9K | 11.1K | Enabled | Connected | 1 | No | Check the Flow Trend |
| Gi 0/2 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/3 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/4 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/5 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/6 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/7 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/8 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/9 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |
| Gi 0/10 | | 0K | 0K | Enabled | Not Connected | 1 | No | Check the Flow Trend |

Figure 2-3: Port Information.

On the panel you seen the device port, description, input flow, output flow, state of the port, connection state, the VLAN, whether trunk.

Flow trend.

Use the mouse to click the device port on the panel port, can view the port Flow trends.

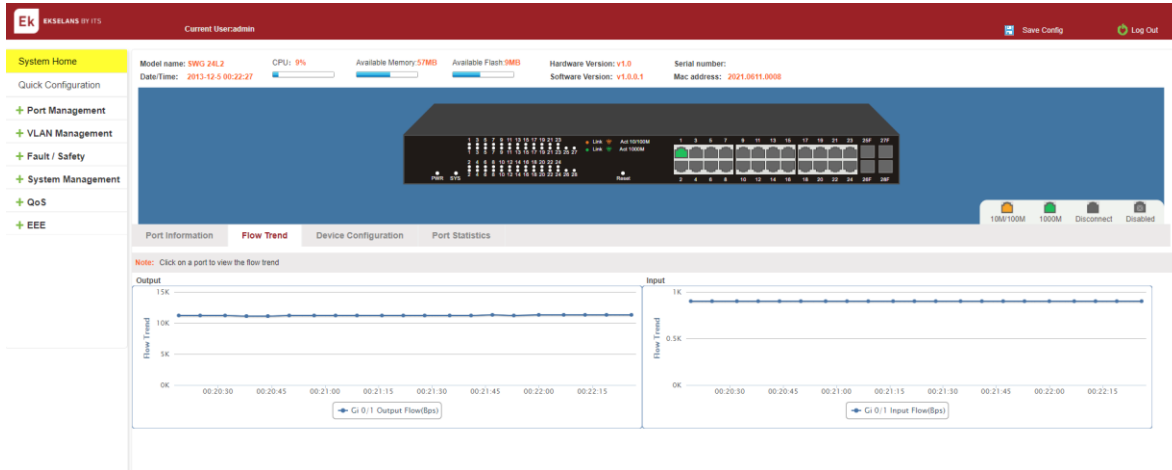


Figure 2-4 View the Flow Trend.

Device configuration.

With the HTTP page, click "Device Configuration" to view and change the configuration of the device.

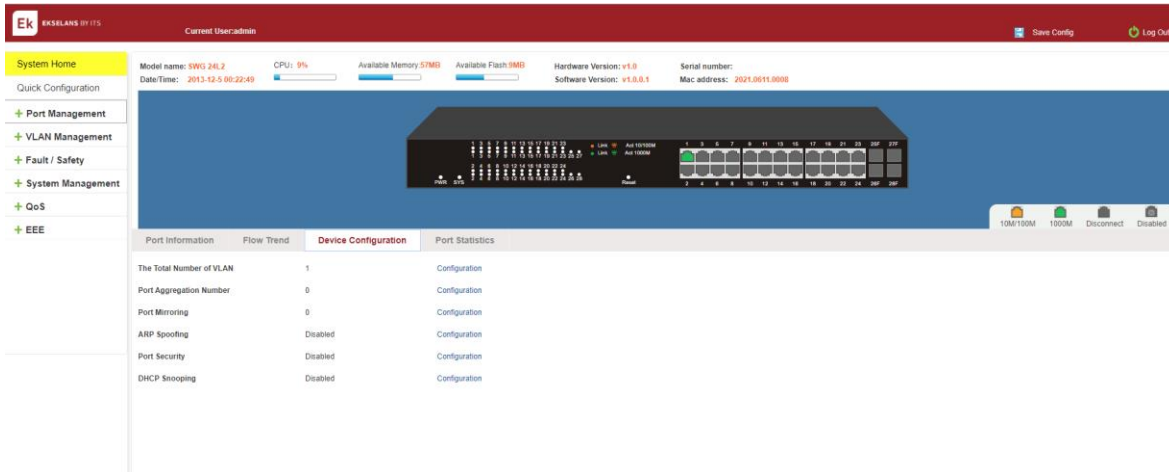


Figure 2-5: Device Configuration.

"Device configuration" can quickly configure the following modules:

- 1 Total number of VLAN.
- 2 Port Aggregation Number.
- 3 Port Mirroring.
- 4 ARP Spoofing.
- 5 Port Security.
- 6 DHCP Snooping.

Port statistics.

Through the HTTP page, the user can quickly understand the number of bytes received, the number of bytes sent, the number of incomplete packets, the number of large packets, CRC error packets, the number of conflicts.

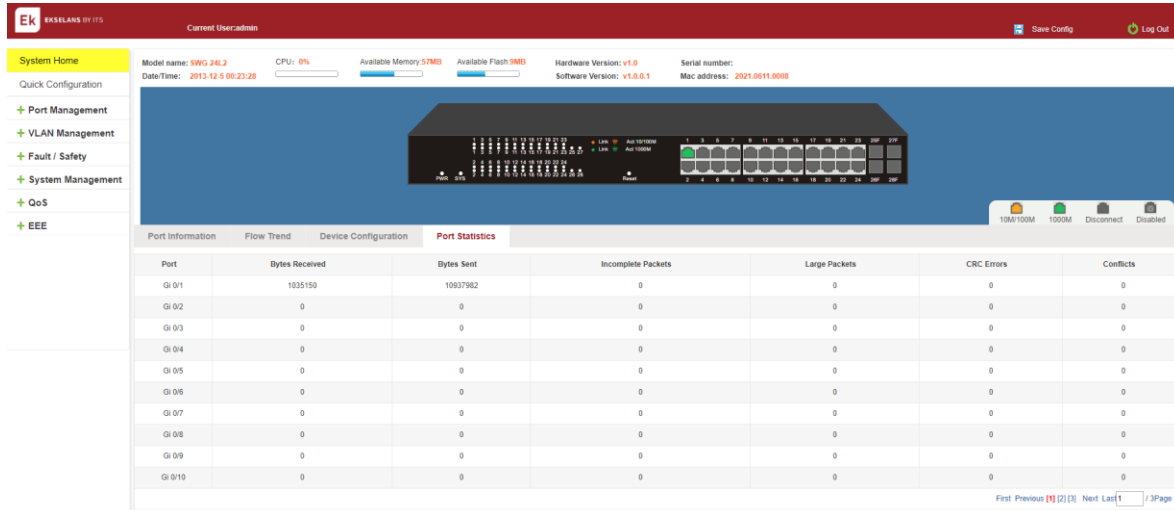


Figure 2-6: View the port Statistics.

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 and others. According to the steps, the configurations of step by step, also can choose configuration.

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.

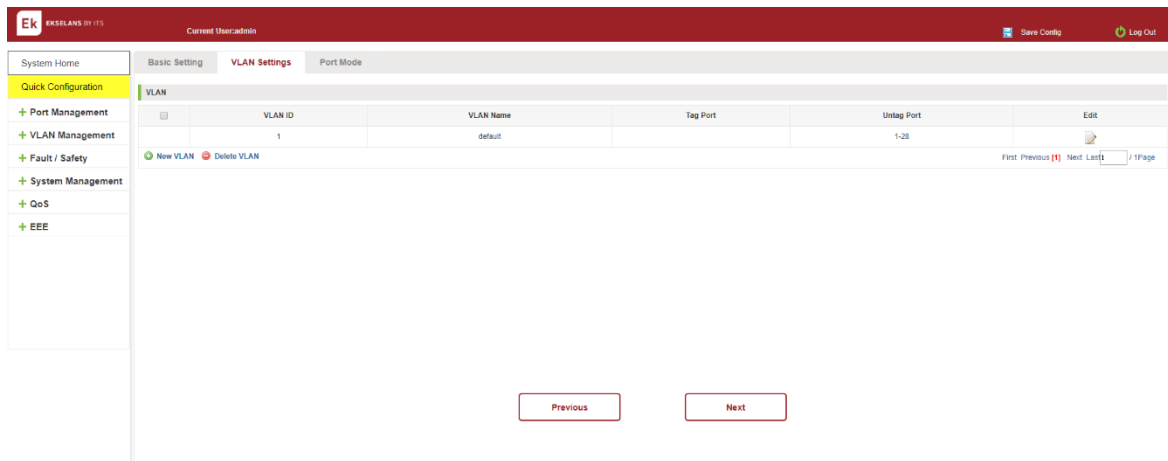


Figure 3-1: VLAN Setting.

PORT MODE.

Click on "Quick Configuration" "Port Mode" into the port mode configuration settings page. You can change the port mode and allowed some vlans on trunk or hybrid mode, notice:When the port is changed to trunk mode,it will be removed from the previous untag vlan.

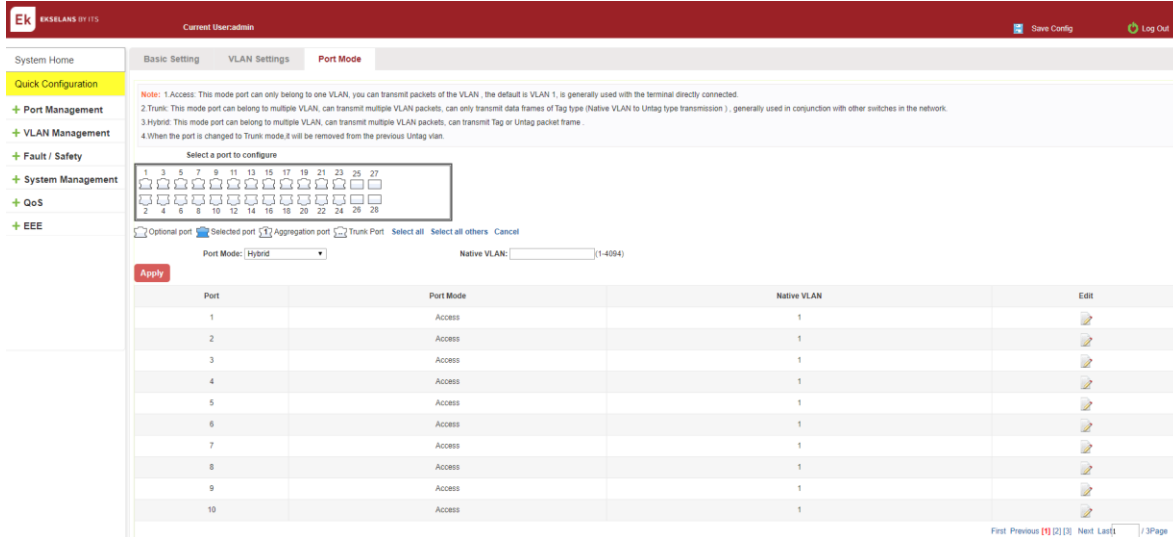


Figure 3-2: Trunk Port Setting.

BASIC SETTING.

Click "Quick Configuration" "Basic Setting" into the quick Configuration of equipment information system Settings page. Can the current equipment basic information system and manage password configured.

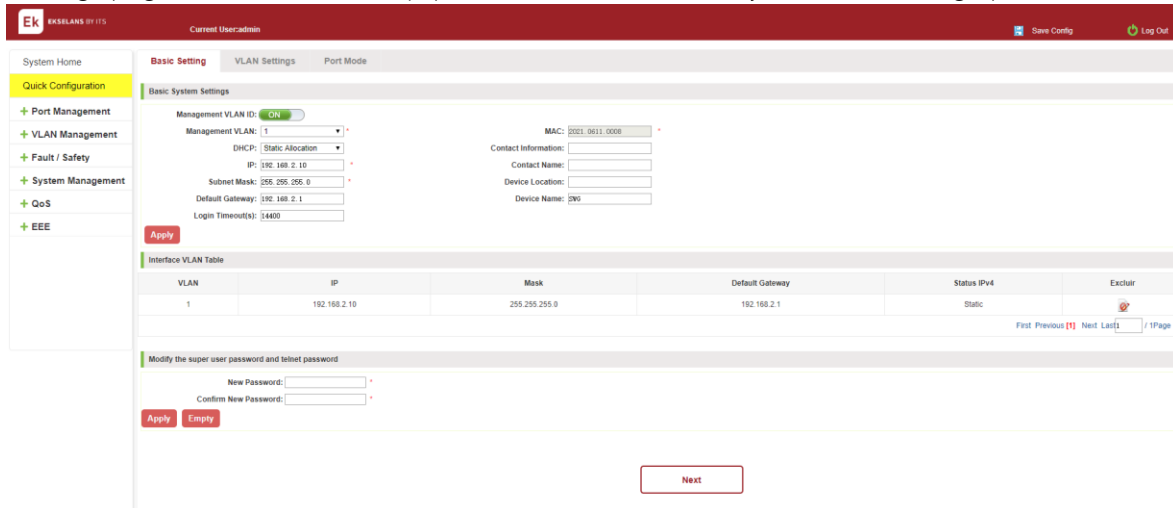


Figure 3-3: other settings.

Port Management.

Basic Settings.

Check the port configuration.

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

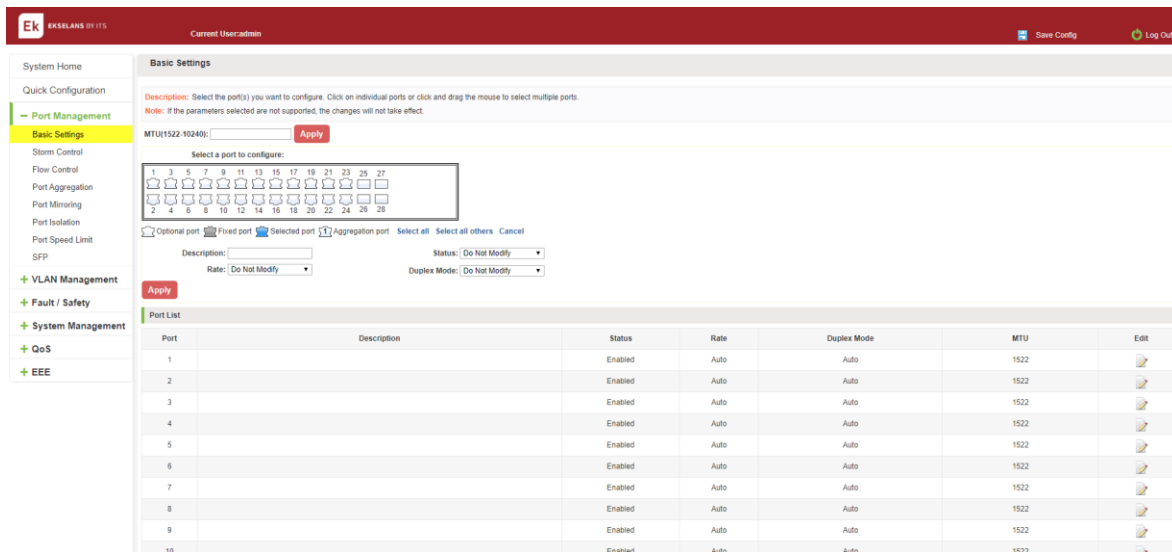


Figure 4-1: Port list information.

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.

Configuring Port Properties.

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

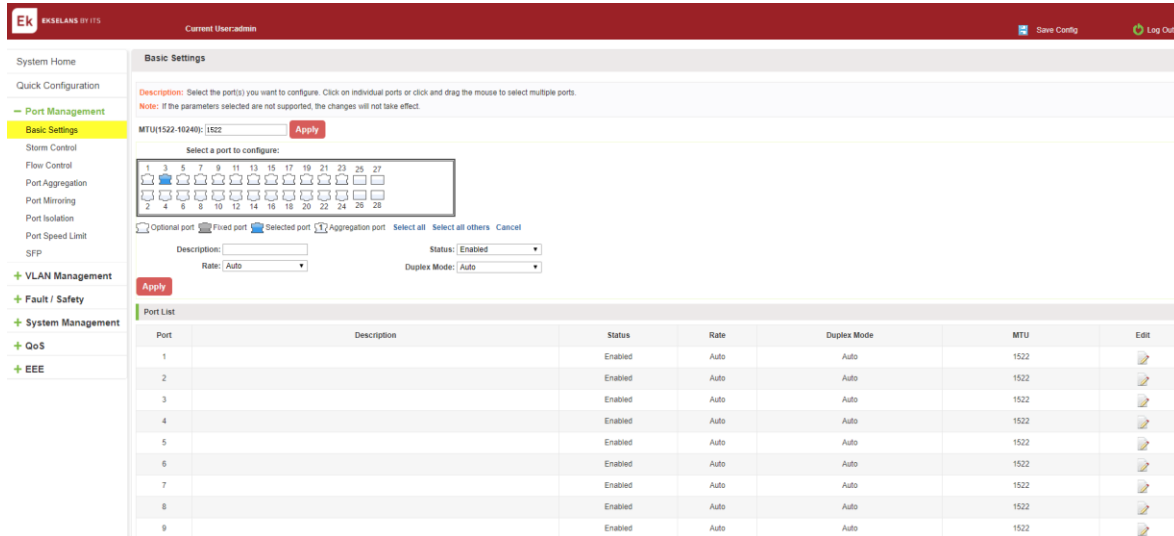


Figure 4-2: Port Properties configuration of FIG.

To configure port properties as follows:

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

Storm Control.

Check the port settings Storm.

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

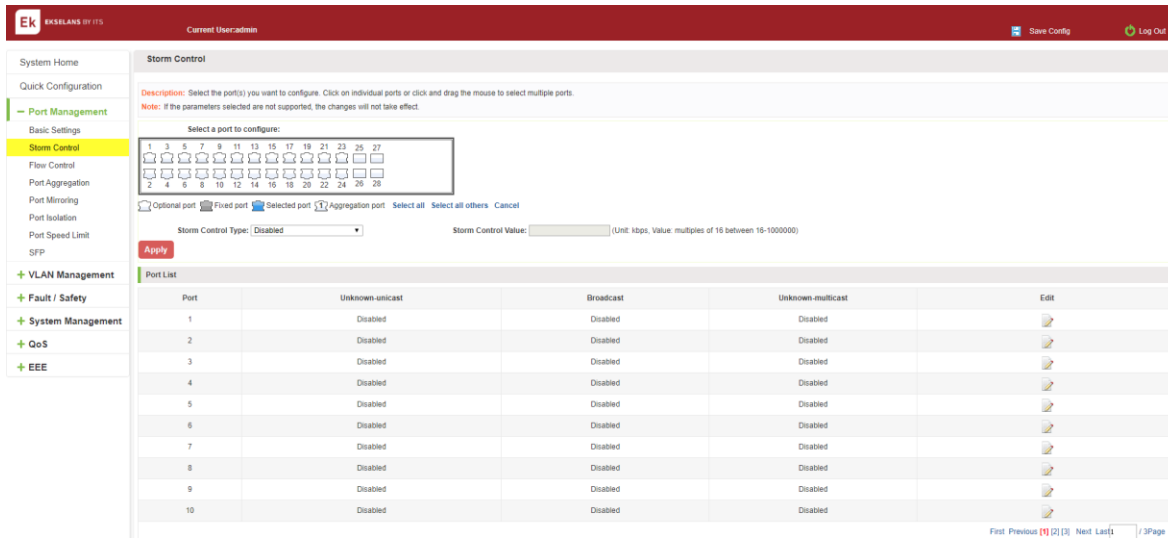


Figure 4-3: Storm Control List information.

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 16, the system automatically matches similar multiples of 16.
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.

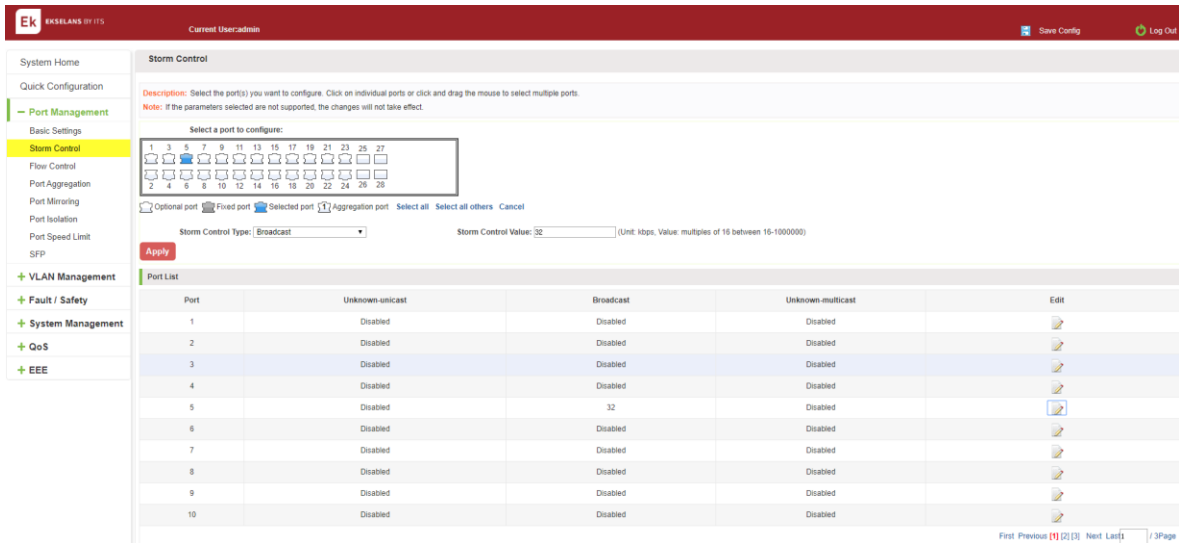


Figure 4-3: Configuring Storm Control information.

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

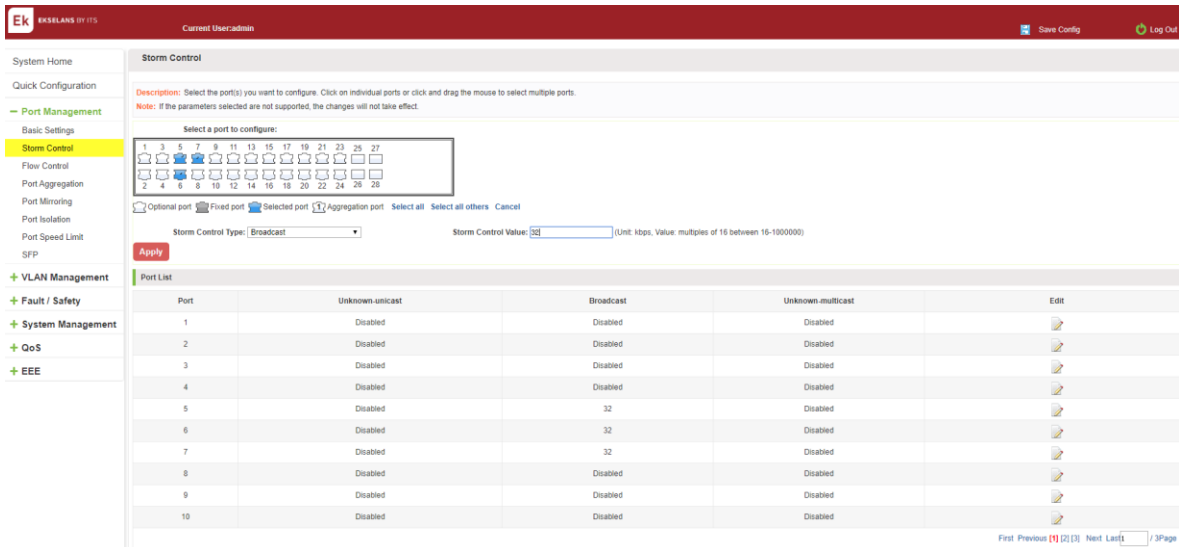


Figure 4-4: Bulk edit configuration information.

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 1009. Click Apply Settings.

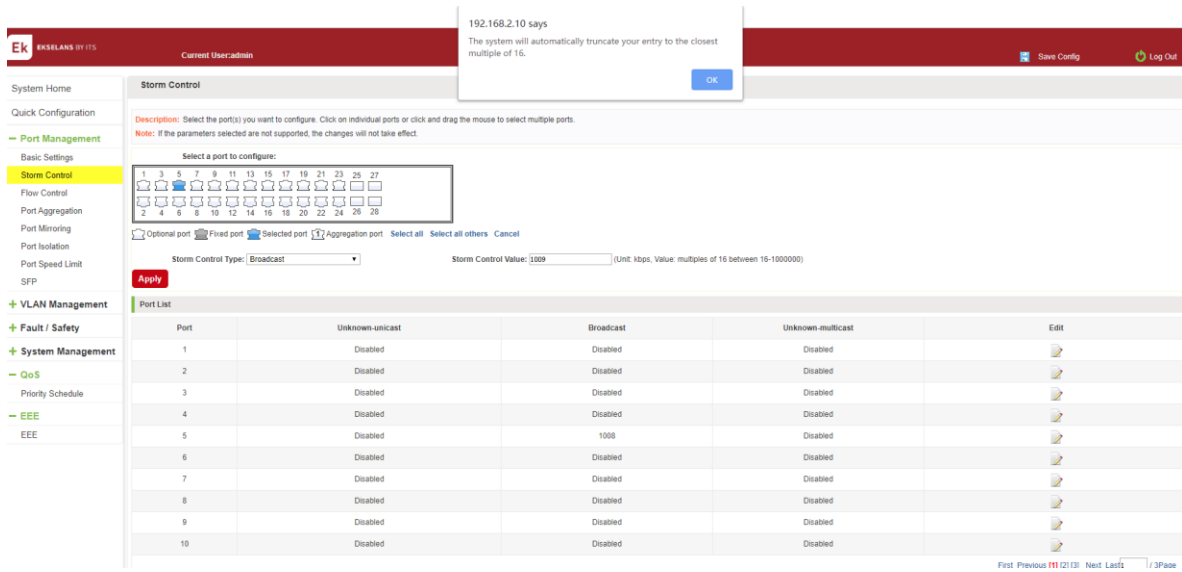


Figure 4-5: Configuring Storm Control information.

After the configuration, as shown below:

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

Figure 4-6: Configuration successfully Storm Control information flow control.

FLOW CONTROL.

Click "Port Management" "Flow Control" view of the switch:

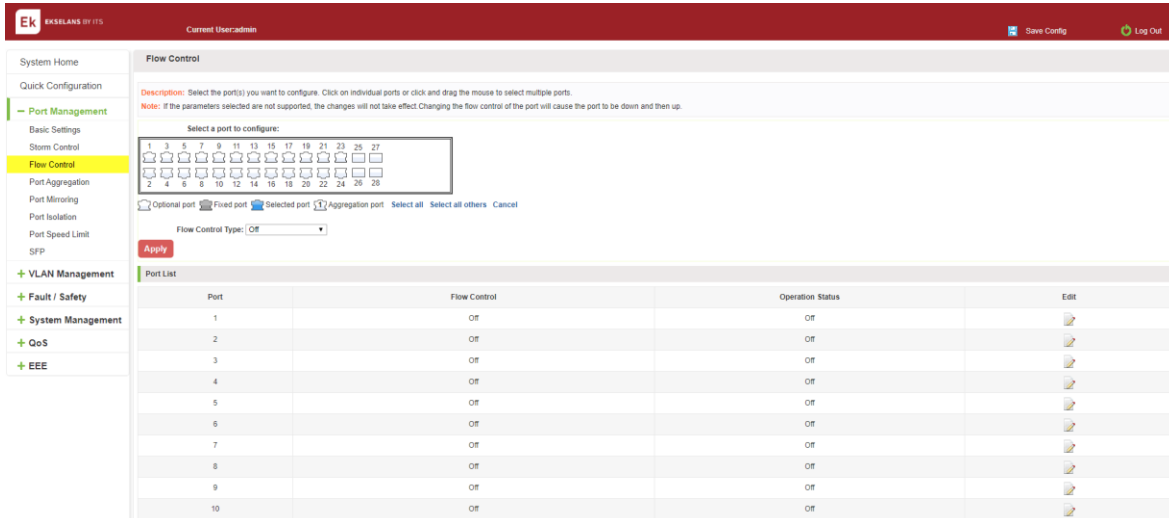


Figure 4-7: Flow Control Information.

Configuring Flow Control.

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

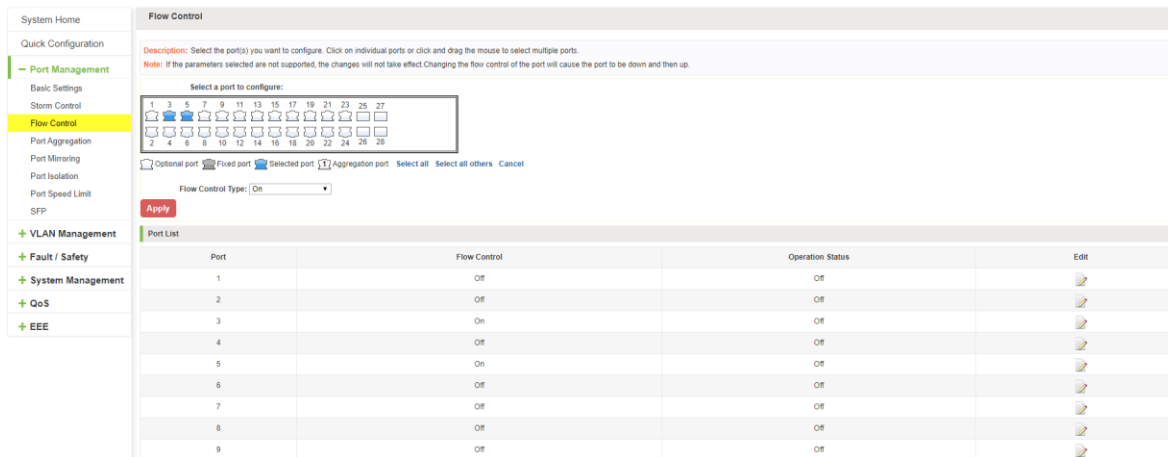


Figure 4-8: Open port flow control function.

Open port traffic control, follow these steps:

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

View Configuration list to display configuration is successful:

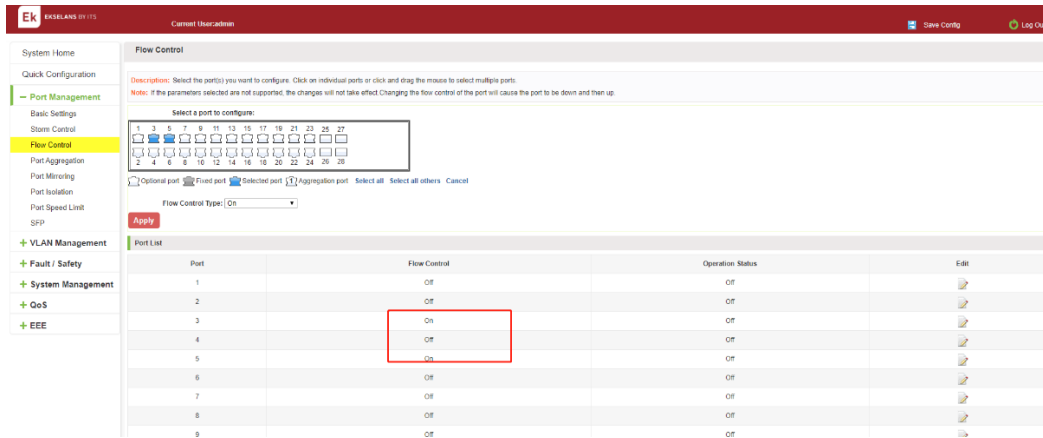


Figure 4-9: Port flow control status.

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

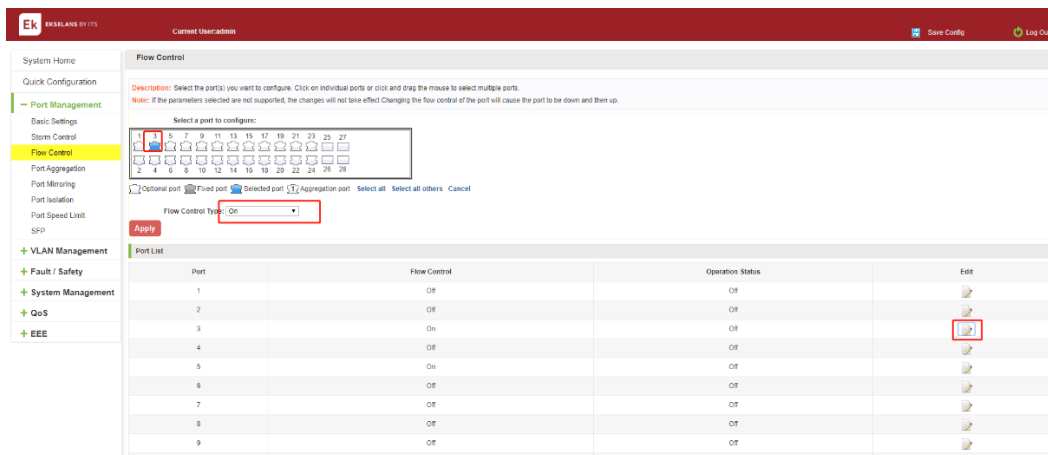


Figure 4-10: Close the port flow control.

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 "Apply".

Port Aggregation.

Viewing Port Aggregation Configuration.

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

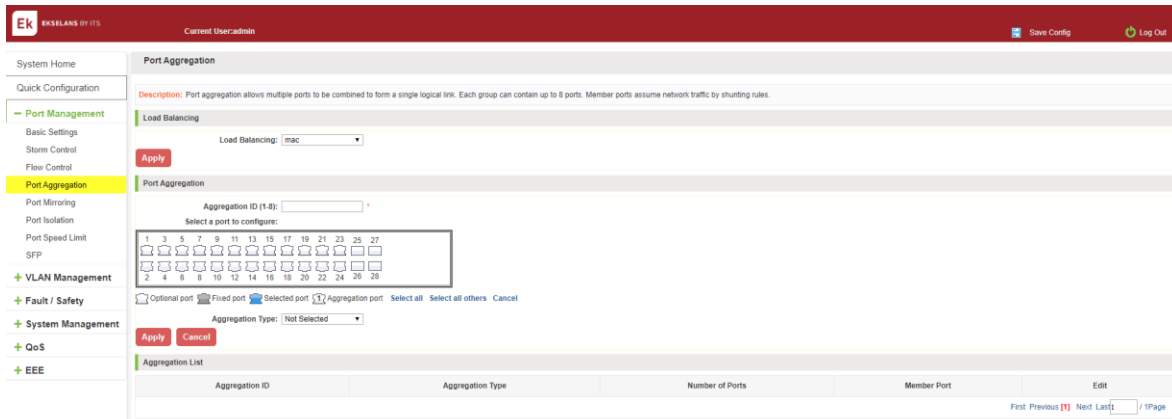


Figure 4-12: Aggregation port configuration information.

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.

Add port aggregation.

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

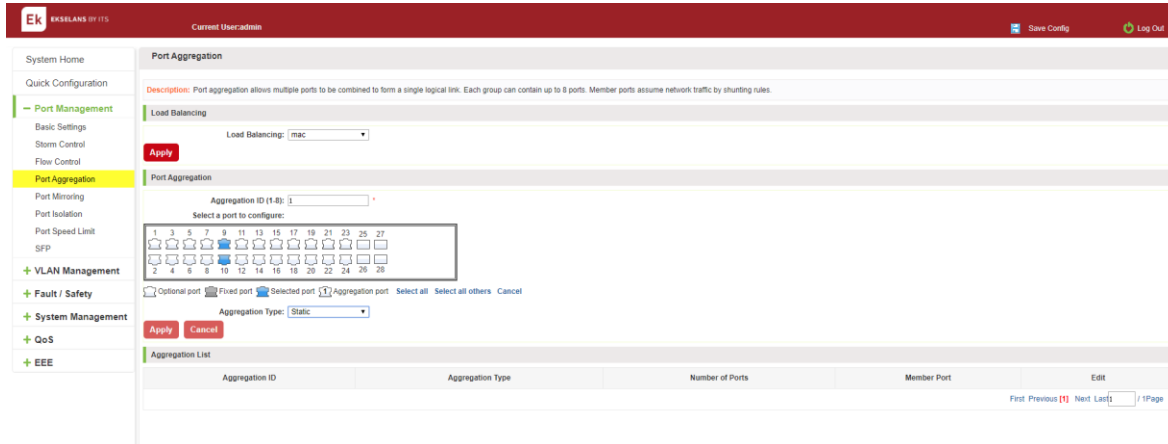


Figure 4-13: Port Aggregation Configuration area.

Increase port aggregation, follow these steps:

Step1: Select the option to load the shunt in the load balancing list. Step2: Enter the number in the "Aggregation number" in. Step3: Select the aggregated ports in the panel. Step4: Select the aggregation type. Step5: Click the "Apply" button to complete the configuration.

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:

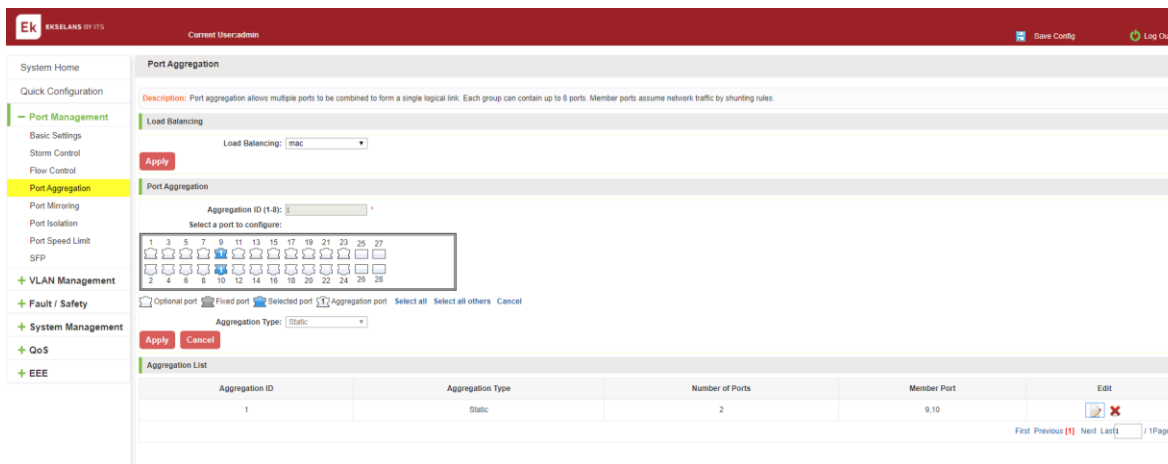


Figure 4-14: To modify the port aggregation.

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 "Apply". step3: Select the port to be added to the aggregation port. step4: Click the "Apply" button to complete the configuration.

Port Mirroring.

Port Mirroring Configuration.

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

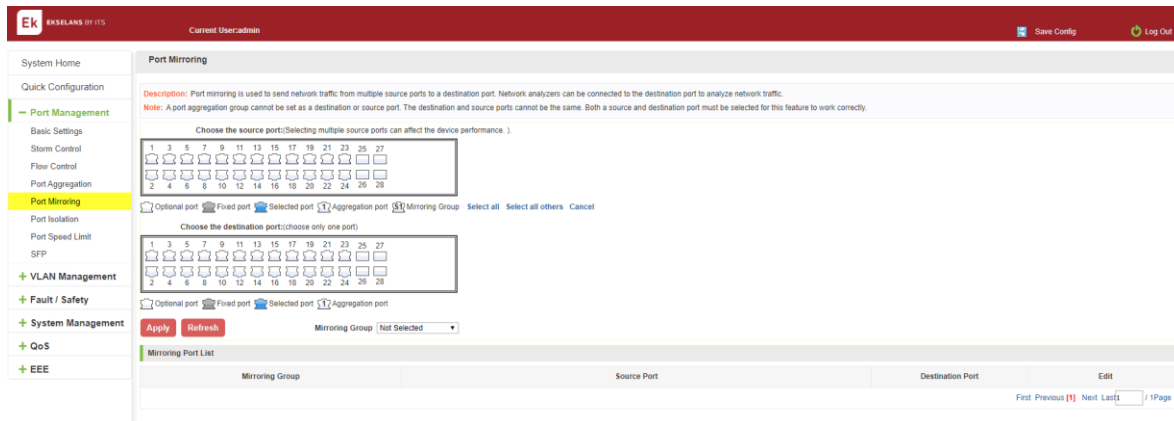


Figure 4-15: Port mirroring configuration information.

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.

Add port mirroring group.

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

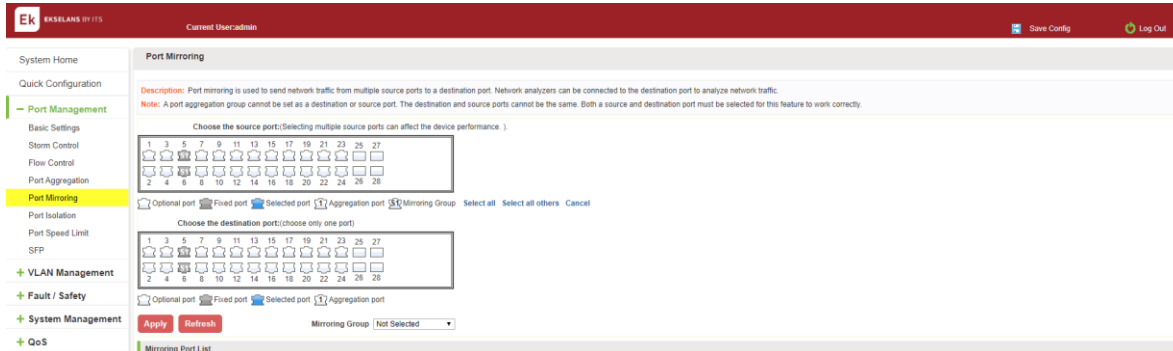


Figure 4-16: Add port mirroring group.

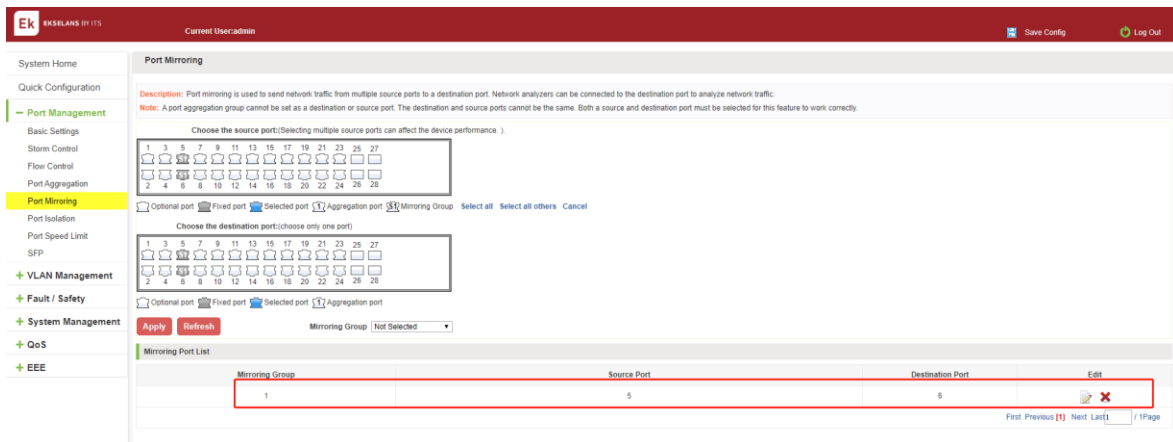


Figure 04-17: Add port mirroring group results.

Port mirroring configuration steps are as follows:

- Step1: Select "Source Port", Step2: Select "Destination Port", Step3: select mirroring group, Step4, Click"Apply".

Configuration instructions:

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

To modify the port mirroring group.

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

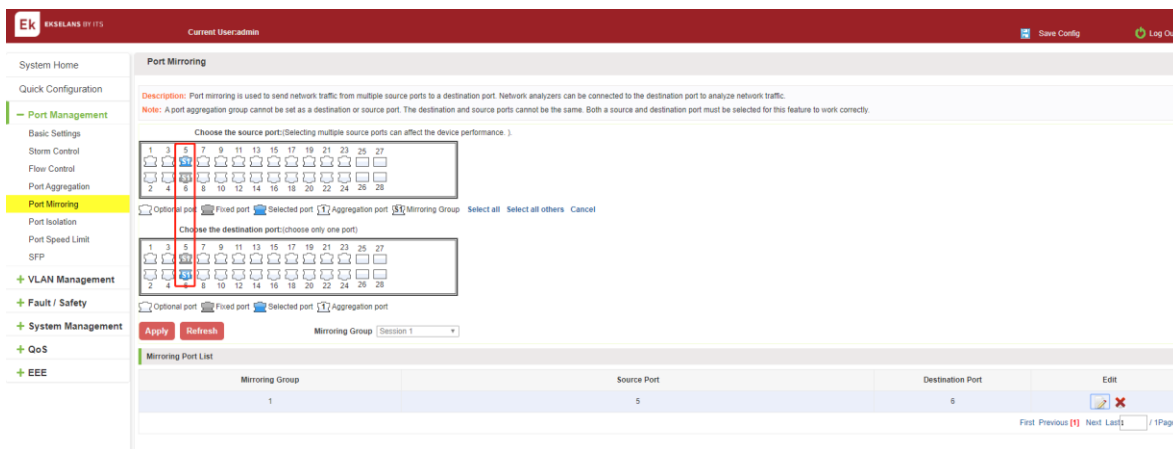


Figure 4-18: To modify the port mirroring group.

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 "Apply".

Delete a port mirroring group.

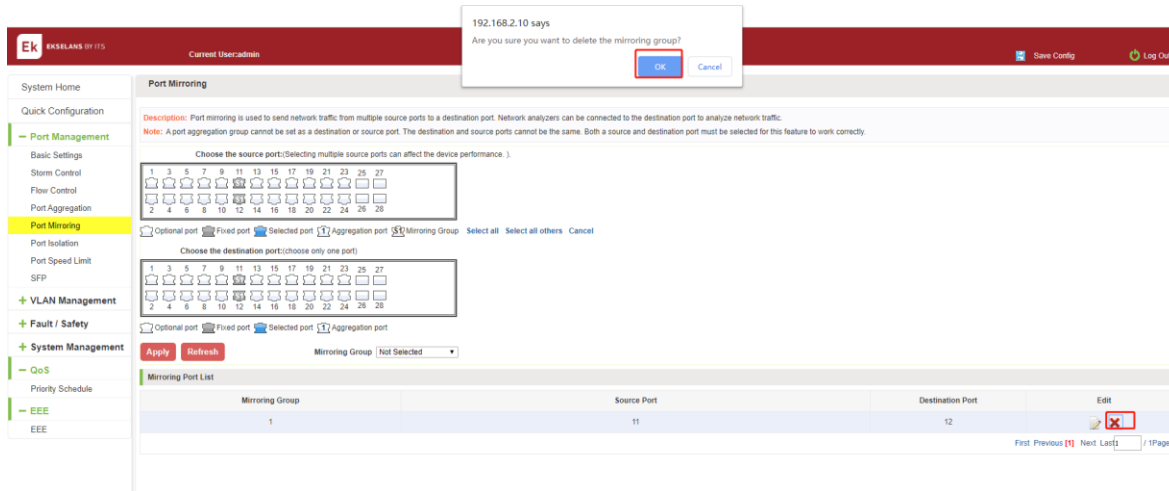


Figure 4-19: Delete port mirroring group.

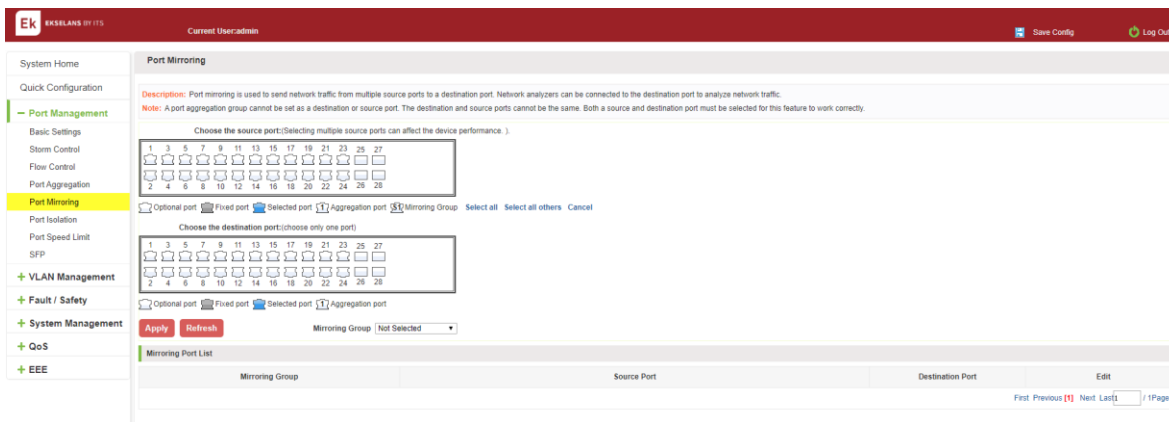


Figure 4-20: Deleted successfully port mirroring.

Remove port mirroring configuration steps are as follows:

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

Port ISOLATION.

Port ISOLATION Configuration.

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

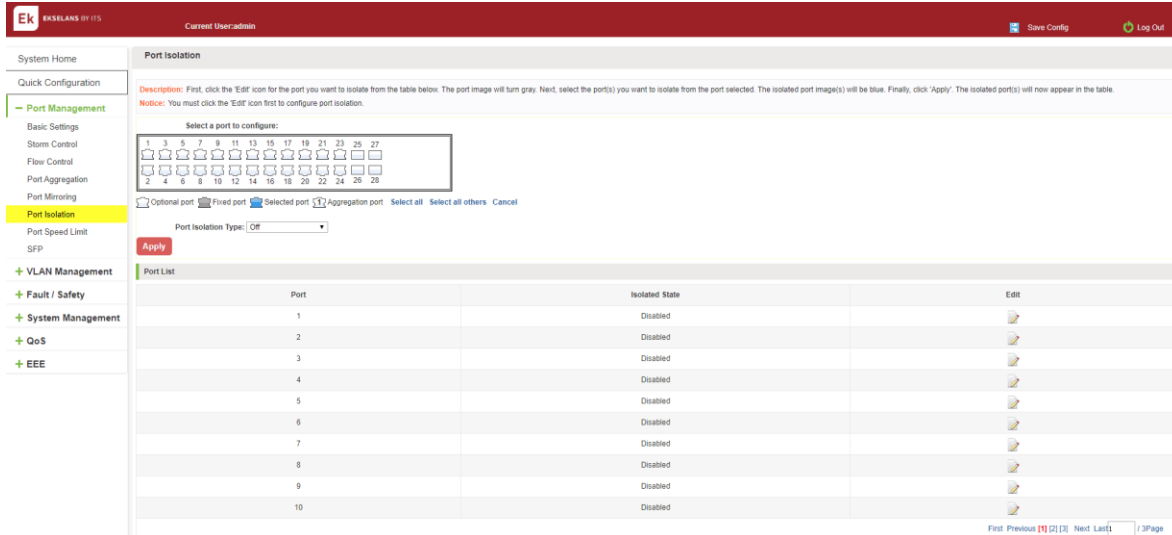


Figure 4-21: Port Isolation configuration information.

Configuring port isolation.

Open Port Isolation function: select the port on which you want to open port isolation, click the "port isolation type" Select "On", "Apple":

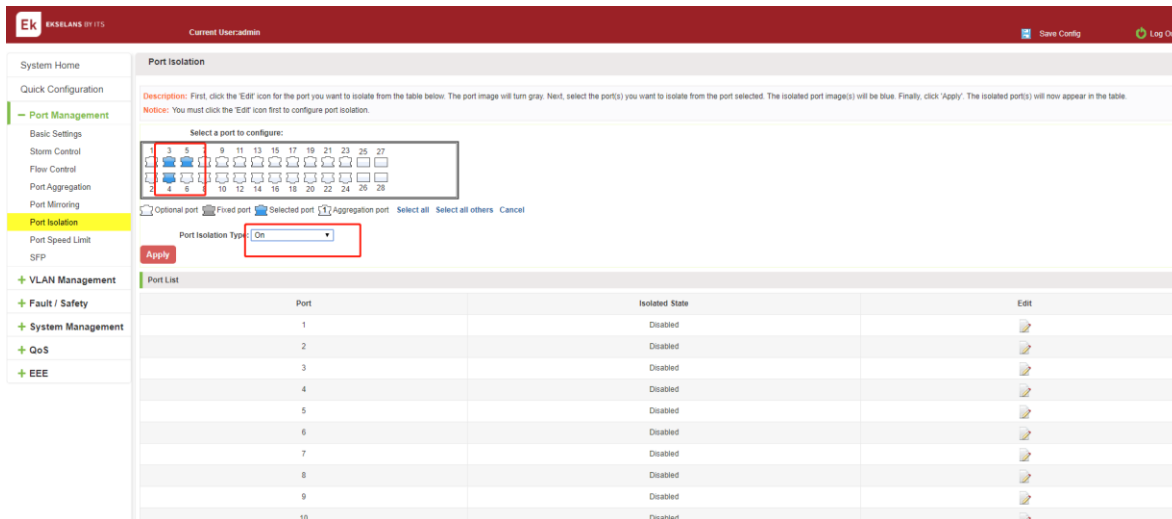


Figure 4-22: enable port isolation function.

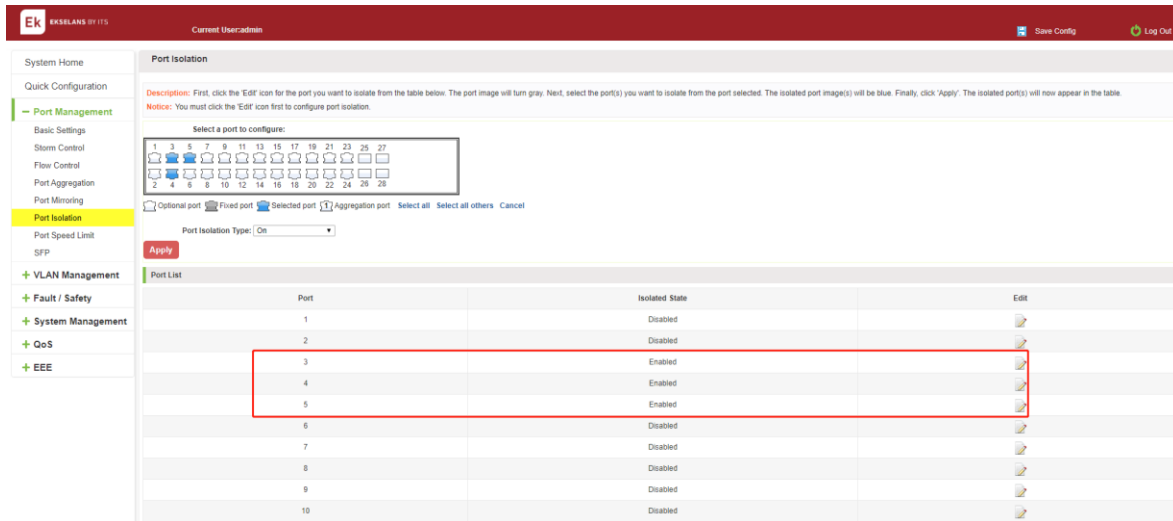


Figure 04-23: enable port isolation results.

Modify the port isolation.

Select the port to modify, click on the action bar " " button. Modify the corresponding port isolation.

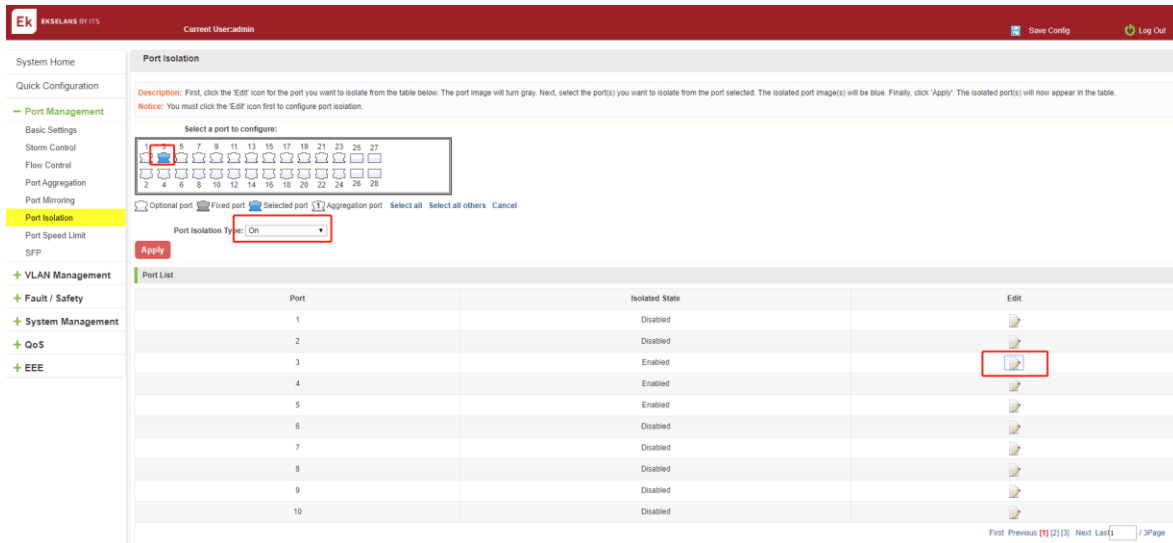


Figure 4-24: To modify the port isolation.

Port speed limit.

View port rate limit.

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

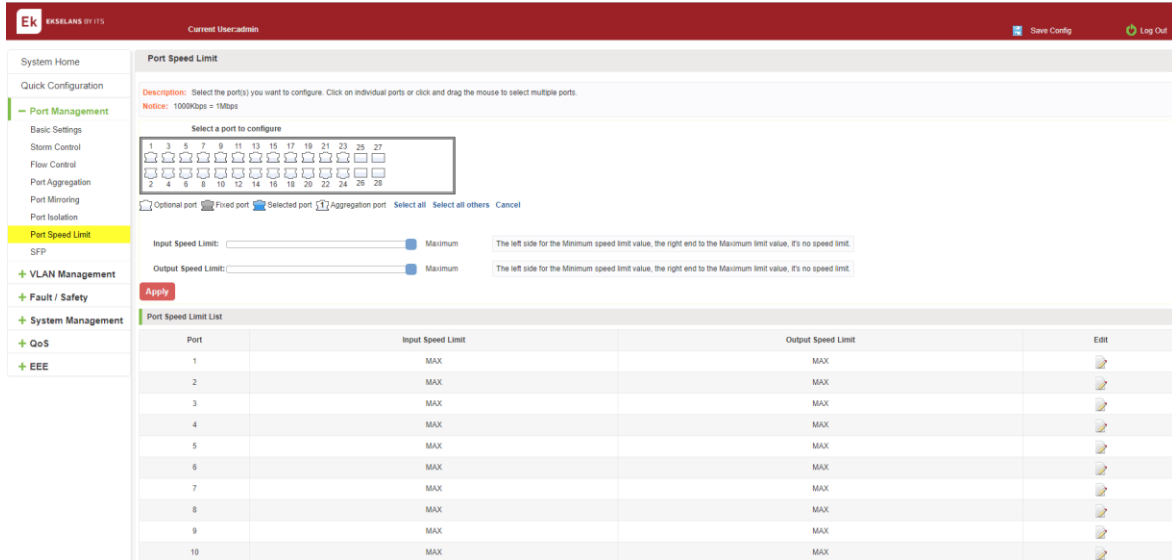


Figure 4-25: View Rate Configuration information.

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.

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.

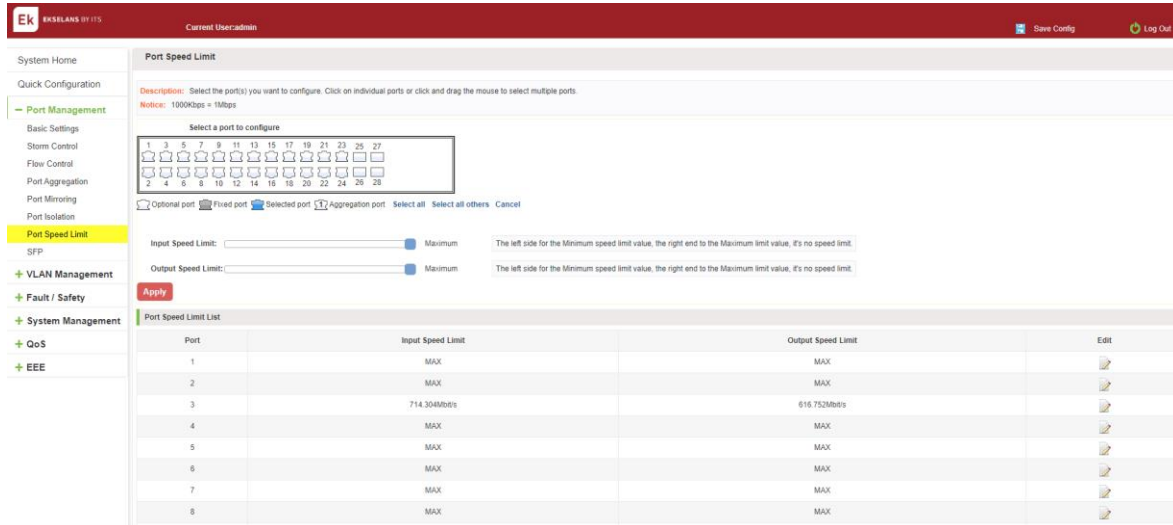



Figure 4-26 Configure port rate limiting entrance.

| Port | Input Speed Limit | Output Speed Limit | Edit |
|------|-------------------|--------------------|------|
| 1 | MAX | MAX | |
| 2 | MAX | MAX | |
| 3 | 714.304Mbit/s | 616.752Mbit/s | |
| 4 | MAX | MAX | |
| 5 | MAX | MAX | |
| 6 | MAX | MAX | |
| 7 | MAX | MAX | |
| 8 | MAX | MAX | |
| 9 | MAX | MAX | |
| 10 | MAX | MAX | |

Figure 4-27: Port entrance speed limit results.

Entrance port rate limiting configuration steps are as follows:

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

Remove the port speed limit.

Click the need to remove the limit on the right port icon " " in the configuration area of the port rate value pull bar to the far right, "Apply" to complete the operation.

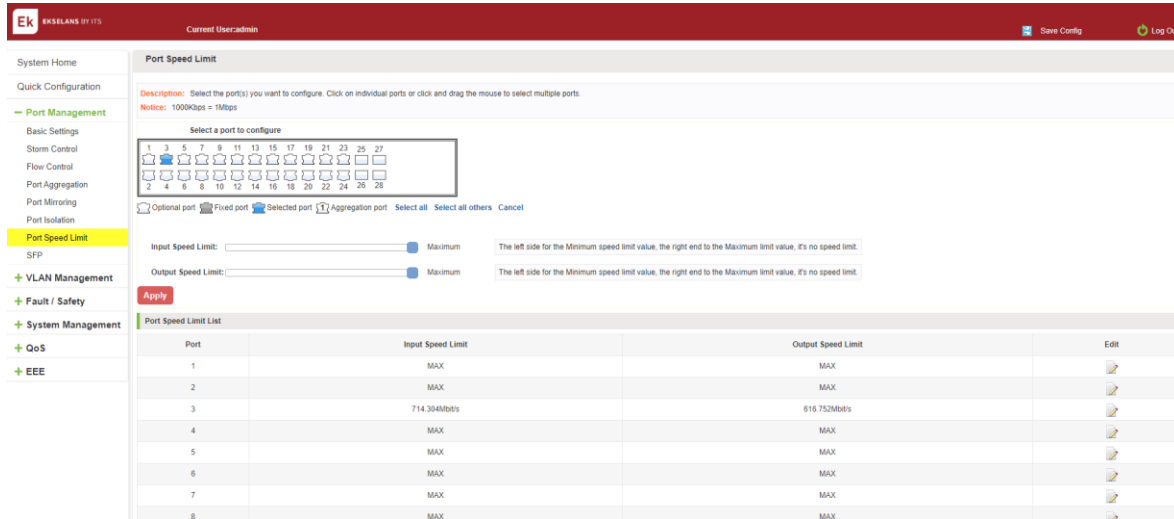


Figure 4-28: Remove the port speed limit.

Remove uplink port rate limiting steps are as follows:

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

Vlan management.

VLAN management.

Check VLAN configuration information.

Click on the navigation bar "VLAN Management" "VLAN management" "VLAN Settings" to view the switch configured:

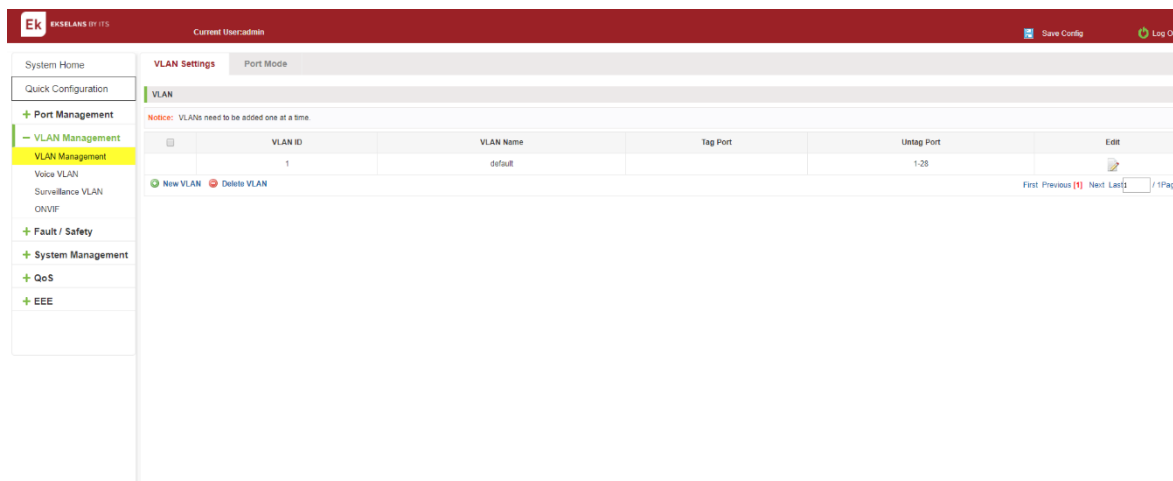


Figure 5-1: VLAN configuration information.

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

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

Adding a VLAN.

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

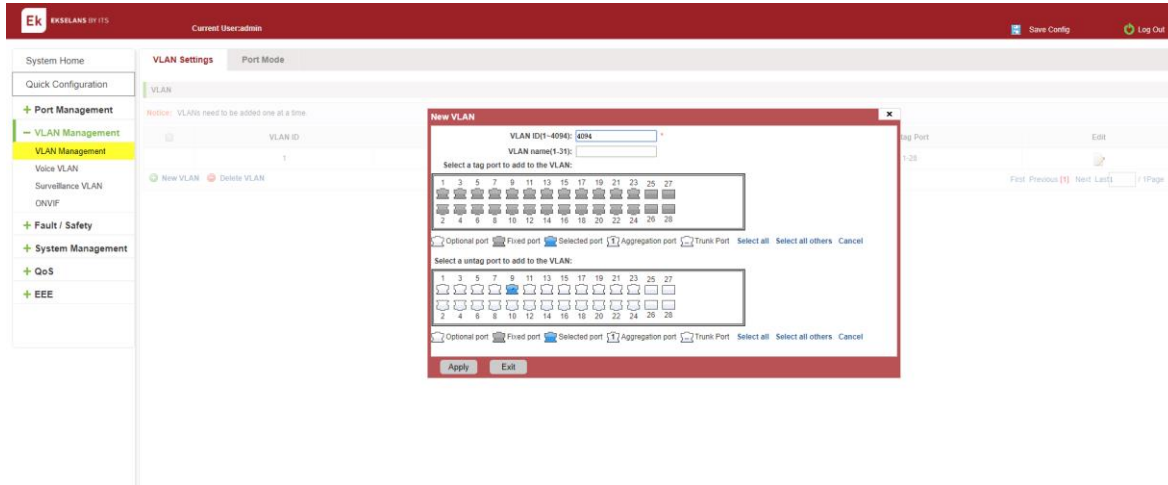


Figure 5-2: Adding a VLAN.

Adding a VLAN, follow these steps:

Step1: Click "NEW vlan" connection; step2: Value added VLAN VLAN ID of the page to fill in; step3: Select the ports; step4: Click the lower right corner "Apply" button to complete the configuration.

Remove VLAN.

- SINGLE VLAN delete:

To delete the selected VLAN, click the "X" button to delete the selected VLAN,if the VLAN do not have ports ,You can directly delete the VLAN;if the VLAN have some ports,you must be remove the ports in the VLAN firstly and then you can delete the selected VLAN.

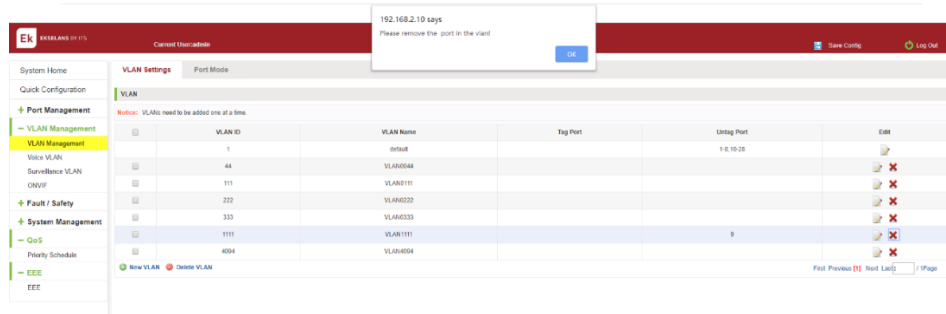


Figure 5-3: Delete a single VLAN.

- 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,if the VLANs have some ports the VLAN can not be removed because of there are member ports.The others will be removed.

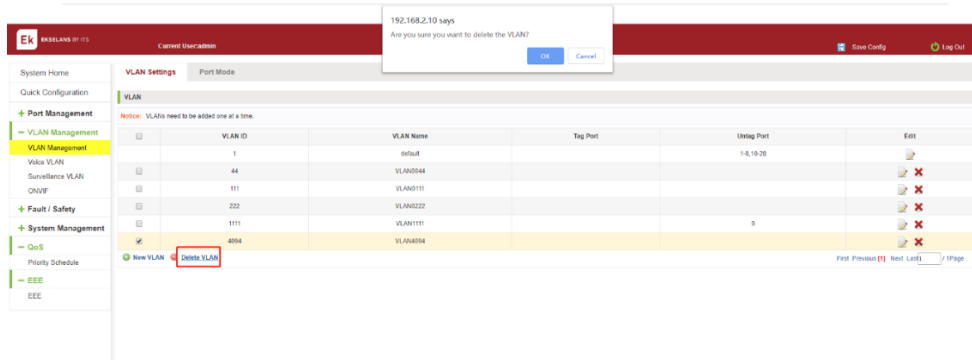


Figure 5-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

- 1 Step1:I want to delete VLAN check box;
- 2 Setp2:Click on the bottom left "Delete VLAN" connection;
- 3 Step3:Confirm delete.

VLAN PORT TO A VLAN.

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

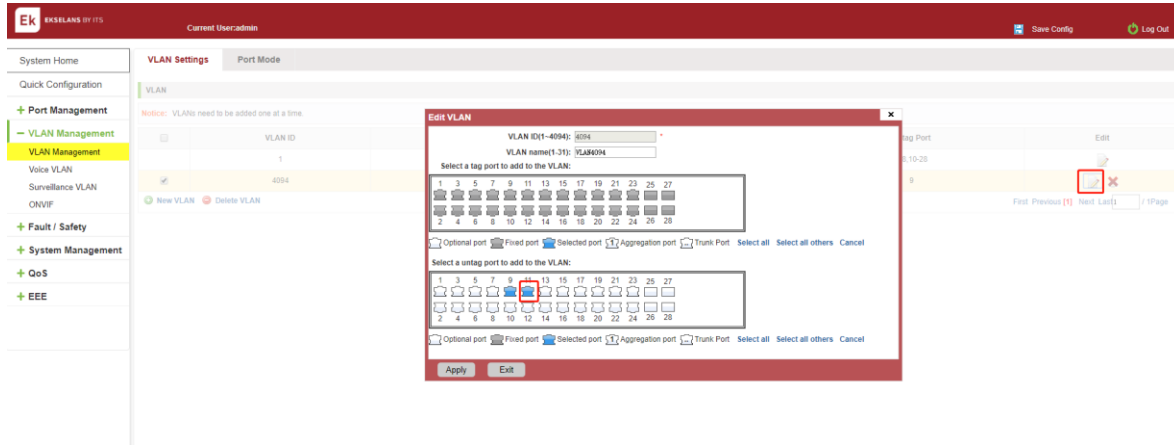



Figure 5-5: Add the port to the VLAN

Add the port to the VLAN, follow these steps:

1. Step1: Click"  "icon.
2. step2: Selected to join the ports in the port panel.
3. step3: Click the lower right corner "Apply" button to complete the configuration.

TO REMOVE THE PORT FROM A VLAN.

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

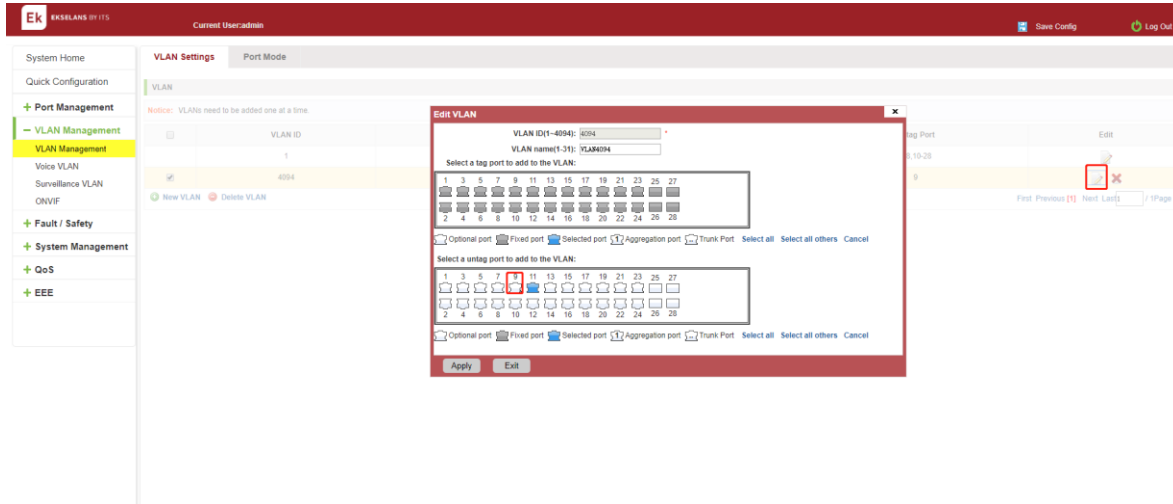


Figure 5-6: To remove the port from the VLAN.

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 "Apply" button to complete the configuration.

View port MODE.

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

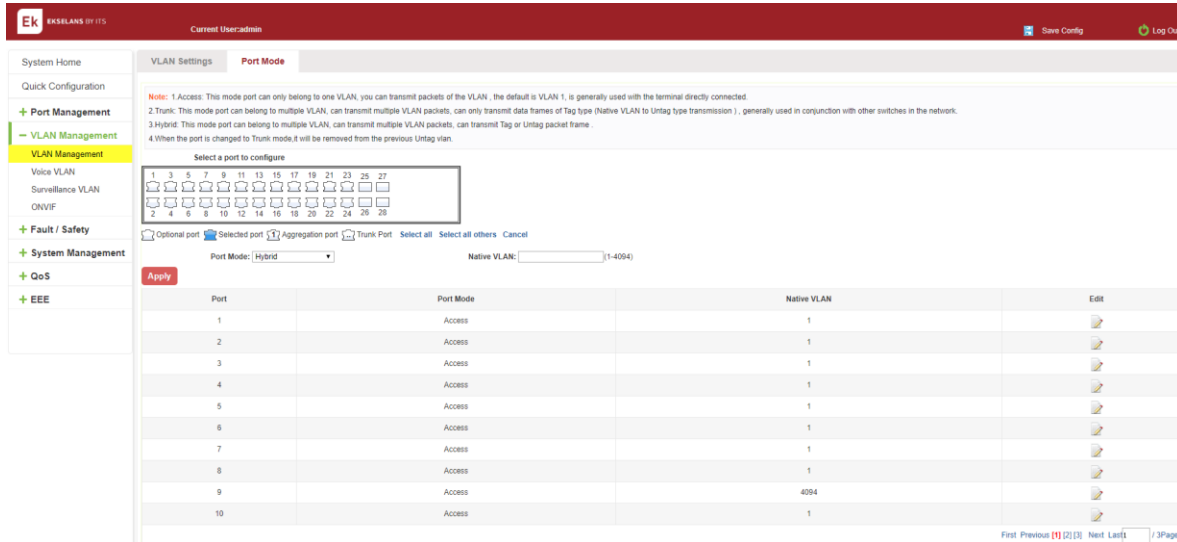


Figure 5-7: View port mode configuration information.

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

- 1 The port name: display port number used.
- 2 The Native VLAN: display native VLAN.
- 3 the allowed VLAN: The VLAN allows the display message can be through VLAN.
- 4 The default port is 1 VLAN native VLAN.
- 5 The default port mode is access.

CHANGE THE PORT MODE IS TRUNK.

Select the port you want to change the mode and click the "port mode " list, you can set the port mode is trunk:

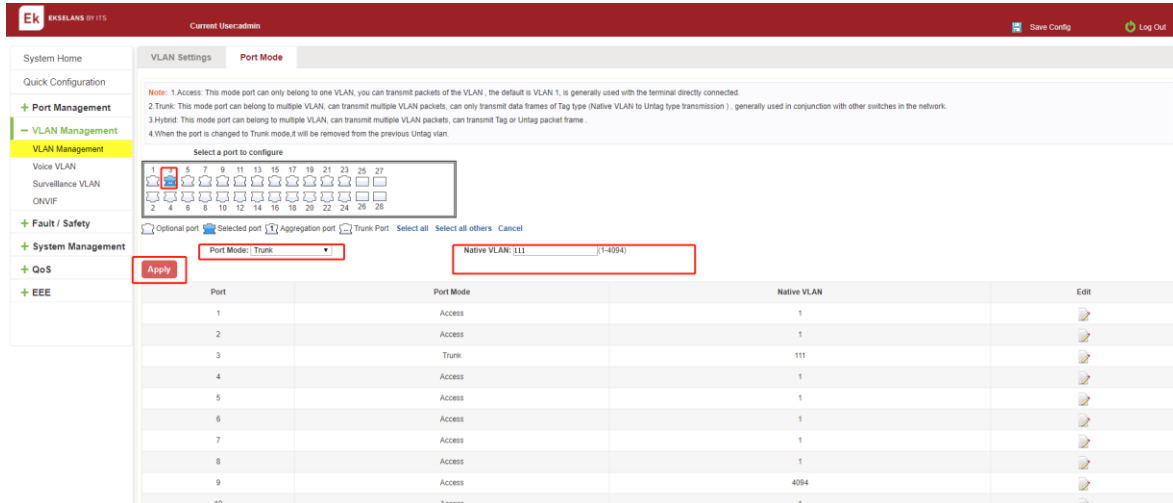


Figure 5-8: Change the port mode is trunk.

The steps to set port mode is trunk are as follows :

Step1:Chose one or more ports; step2:Click the port mode list chose the mode is :trunk; step3:Set Native VLAN, the VLAN must be is exist; step4:Set by allowing the VLAN number, the default allowed VLAN is empty if you want to allowed the native VLAN ,you must be configure allowed the native vlan; step5:Click on the lower right corner of the "Apply" button to complete the configuration.

Change the port mode is hybrid.

Select the port you want to change the mode and click the "port mode " list, you can set the port mode is hybrid.

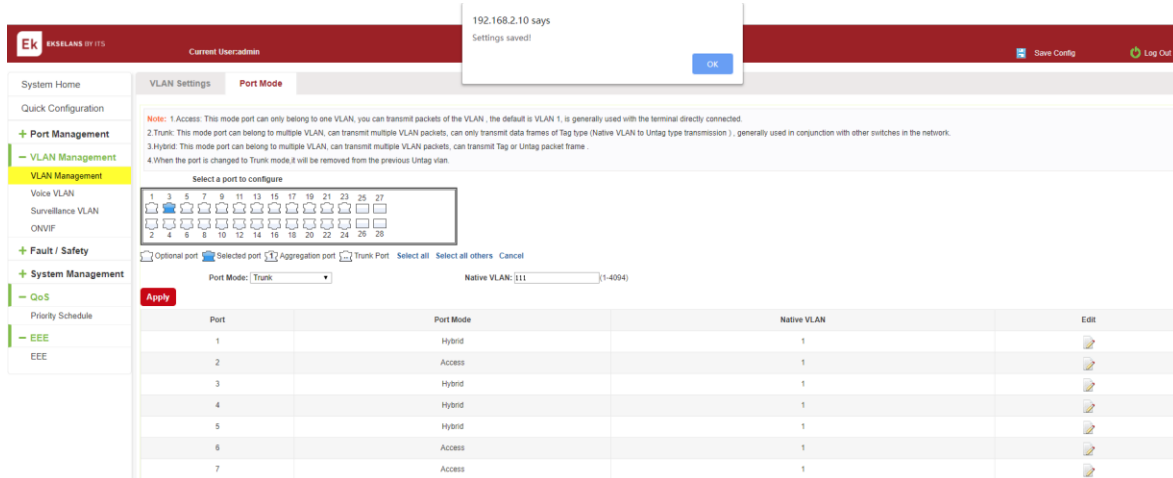


Figure 5-9: Change the port mode is hybrid.

The steps to set port mode is hybrid are as follows :

Step1:Chose one or more ports ; step2:Click the port mode list chose the mode is :hybrid; step3: Set Native VLAN,the VLAN must be is exist; step4:Set by allowing the VLAN number ,the default allowed VLAN 1,if you want to allowed the native VLAN ,you must be configure allowed the native vlan; step5: Click on the lower right corner of the "Apply" button to complete the configuration.

Voice VLAN.

View voice VLAN information

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to view the switch configured:

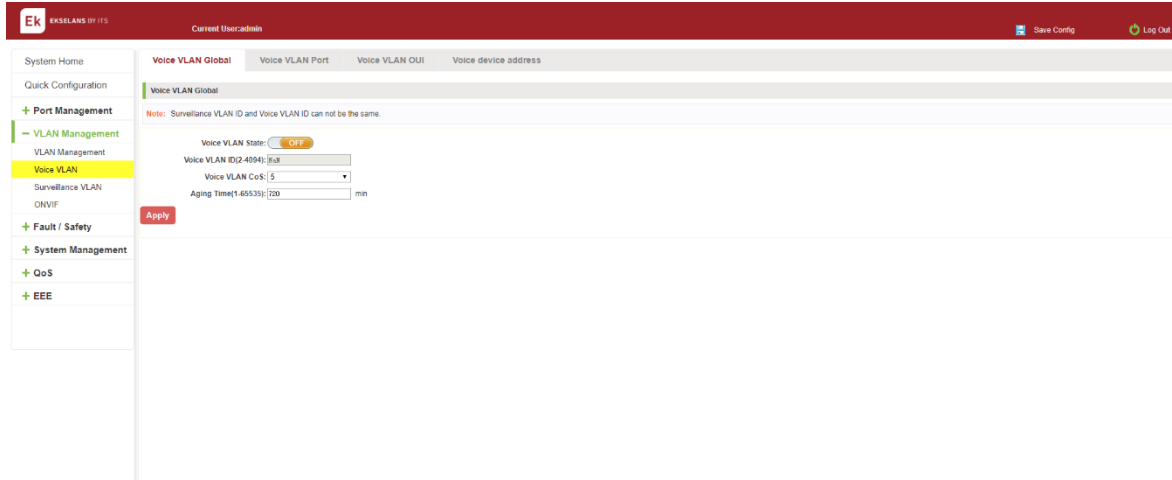


Figure 5-10: view voice VLAN information.

Configure voice VLAN global.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to configure the voice VLAN;

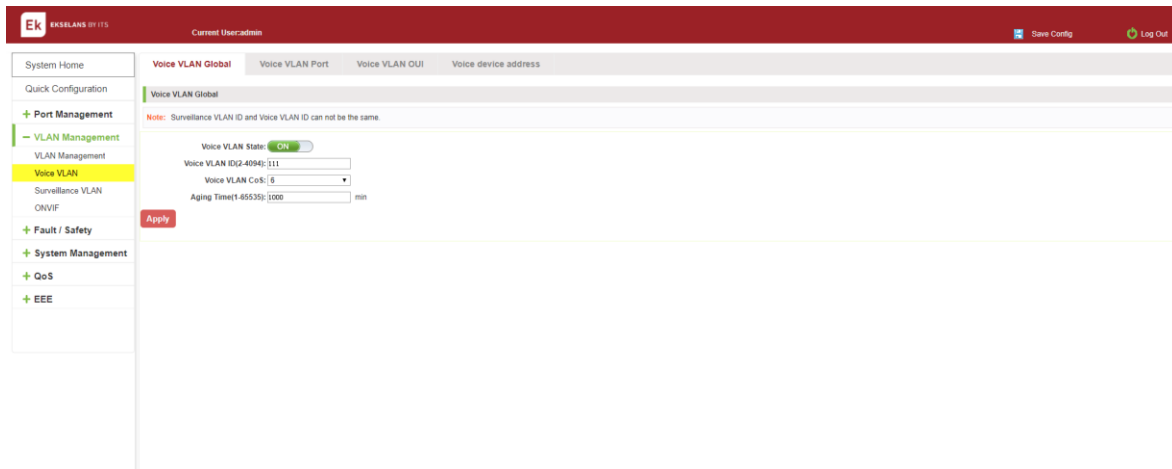


Figure 5-11: view voice VLAN information.

To configure the voice VLAN global steps as follows:

Step1:in the voice VLAN state TEXT BOX, click ON the "OFF" to "ON", Step2:in the voice VLAN ID text box, enter the ID, such as 111; step3: in the voice VLAN COS text box, choose 6; step 4:in the aging time text box, enter aging time, such as 1000; step5: click on Apply.

Configure voice VLAN port.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN port" to configure the voice VLAN port;

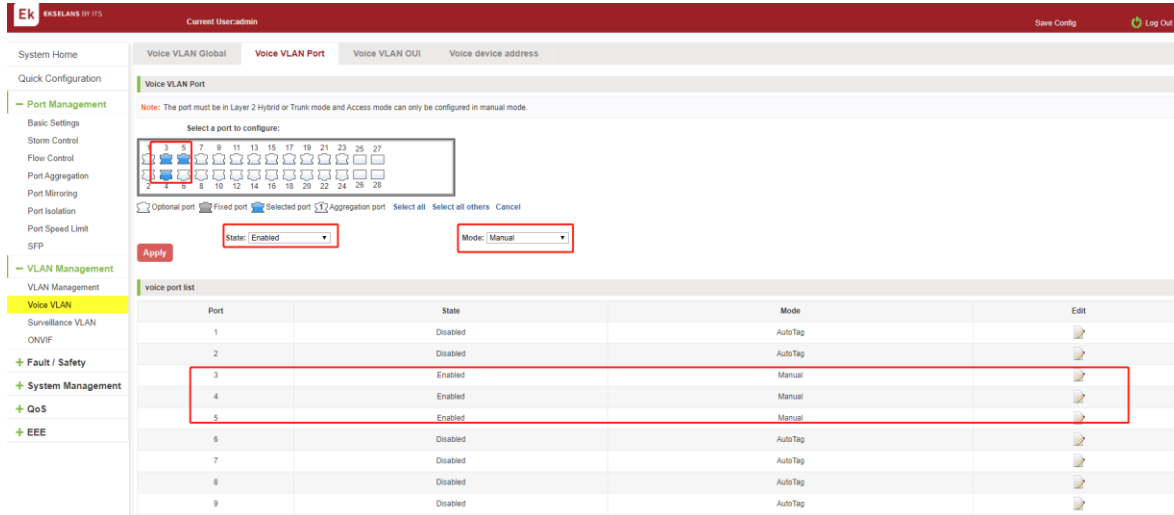


Figure 5-12: configure voice VLAN port.

To configure the voice VLAN port steps as follows:

Step1: select ports to configure, step2:in the state text box, choose enable step 3: in the mode text box, choose manual. step 3:click on Apply.

Configure voice VLAN OUI.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN OUI" to configure the voice VLAN OUI;

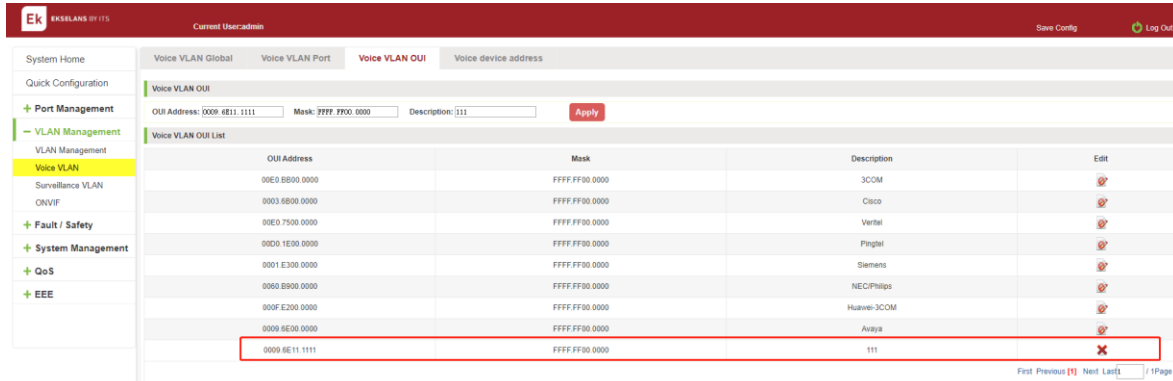


Figure 5-13: configure voice VLAN OUI.

To configure the voice VLAN OUI steps as follows:

Step1: In the OUI address text box, enter OUI address, such as 0009.6E11.1111.

Step2: In the mask text box, enter the mask, such as FFFF.FF00.0000; step 3: in the description text box, enter the description, such as testOUI; step 4: click Apply;

Voice device address.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice device address" to view the voice device:

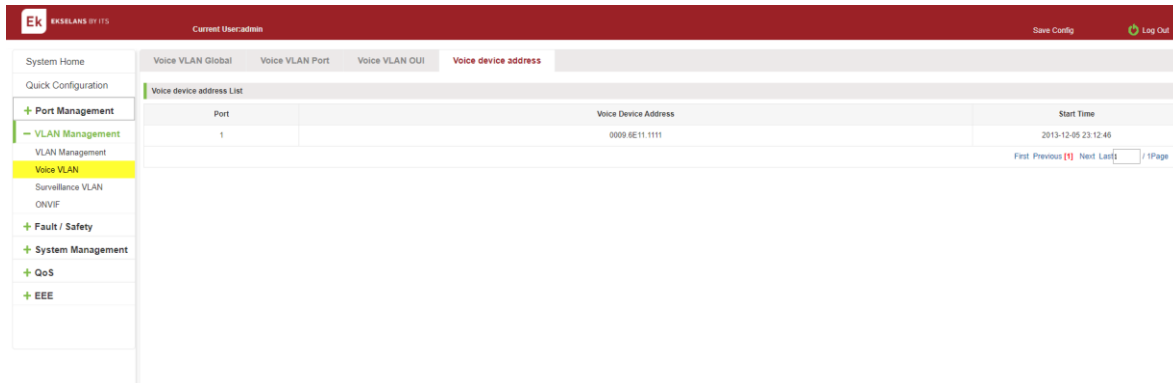


Figure 5-14: VOICE VLAN address.

Surveillance VLAN.

View surveillance VLAN information.

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

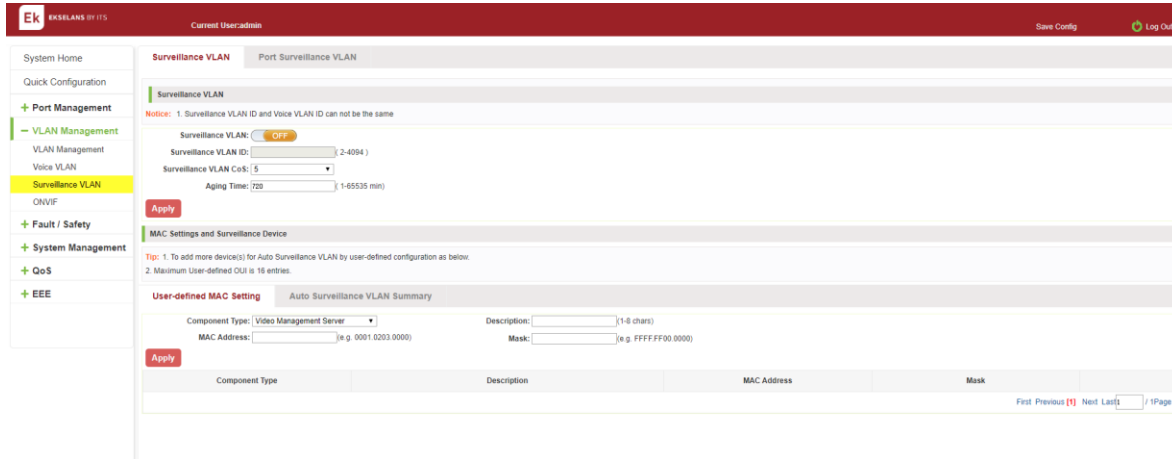


Figure 5-15: surveillance VLAN information.

Configure surveillance VLAN.

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

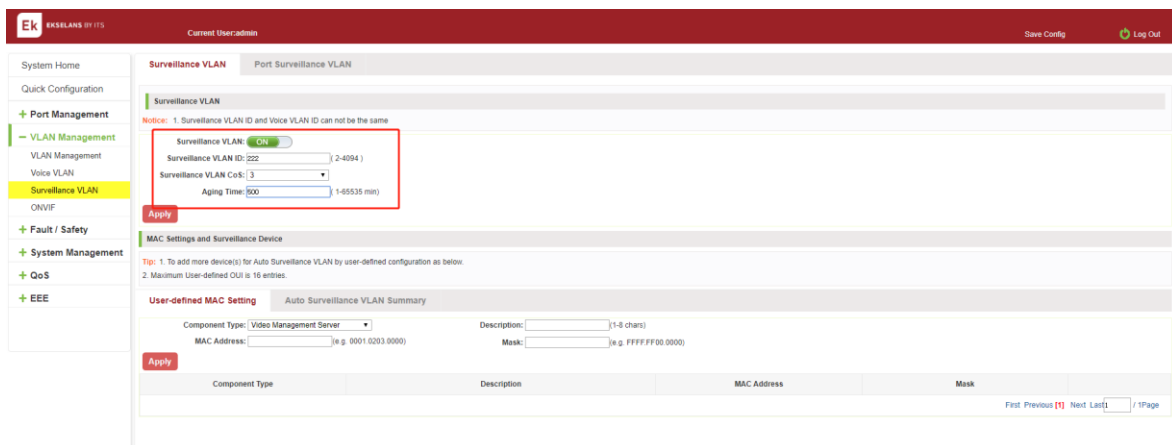


Figure 5-16: configure surveillance VLAN.

To configure the surveillance VLAN steps as follows:

Step1:in the surveillance VLAN TEXT BOX, click ON the "OFF" to "ON", Step2:in the surveillance VLAN ID text box, enter the ID, such as 222; step3: in the surveillance VLAN COS text box, choose 3; step 4:in the aging time text box, enter aging time, such as 500; step5: click on Apply.

MAC Settings and Surveillance Device.

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

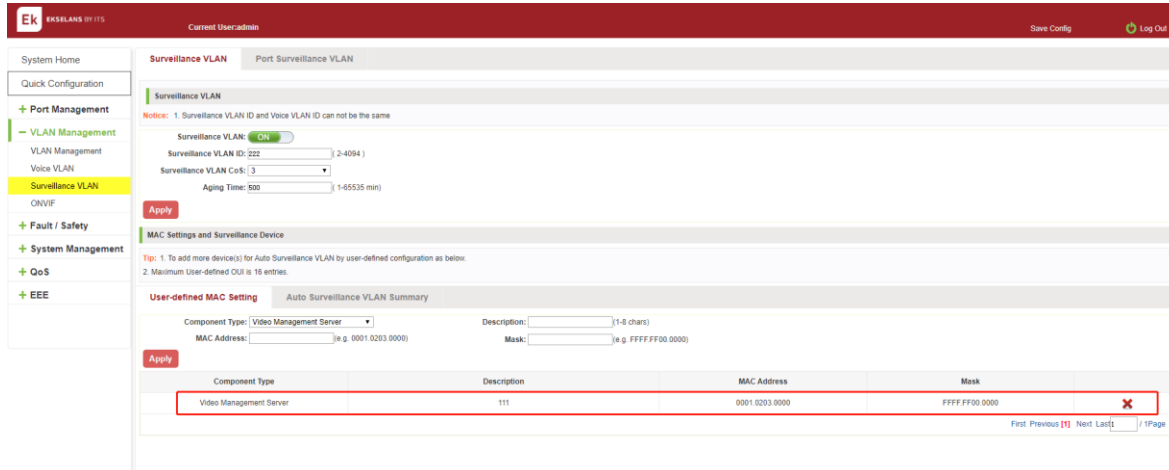


Figure 5-17: configure the user-defined mac settings.

To configure the surveillance VLAN steps as follows:

- Step1:in the component type EXT BOX, choose video management server;
- Step2: in the description text box, enter testOUI;
- step 3: in the mac address text box, enter mac address such as 0001.0203.0000.
- step4: in the mask text box ,enter the mask ,such as FFFF.FF00.0000,step 5:click on Apply;

MAC Settings and Surveillance Device.

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" " MAC Settings and Surveillance Device" to view the information:

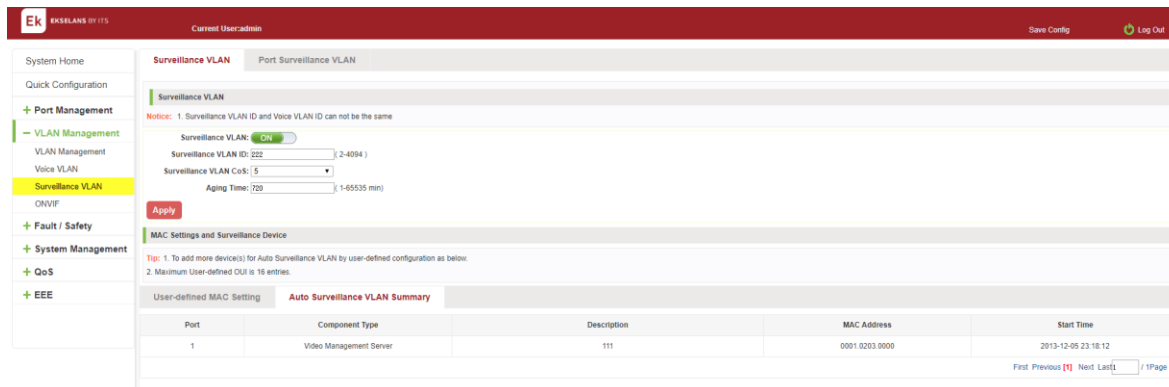


Figure 5-18: configure the user-defined mac settings.

ONVIF.

View ONVIF.

Click on the navigation bar "VLAN Management" "ONVIF" " ONVIF Global" to view the switch configured:

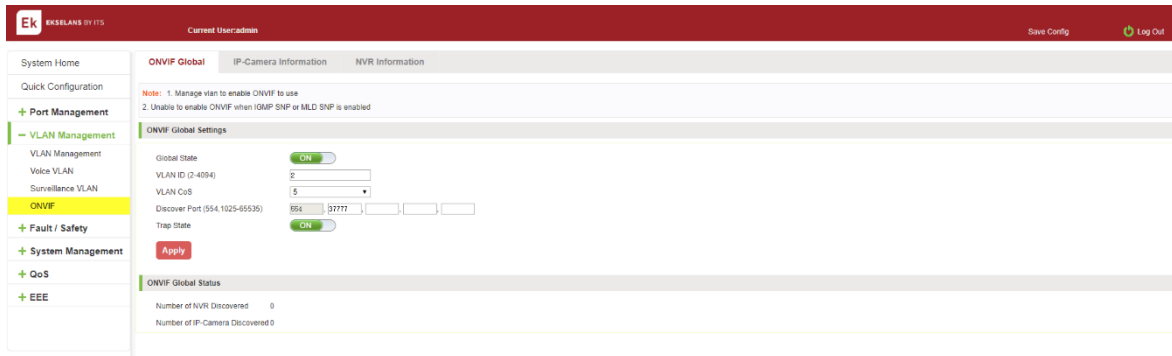


Figure 5-19: ONVIF information.

To configure the ONVIF steps as follows:

Step1: Turn off IGMP and MLD functions

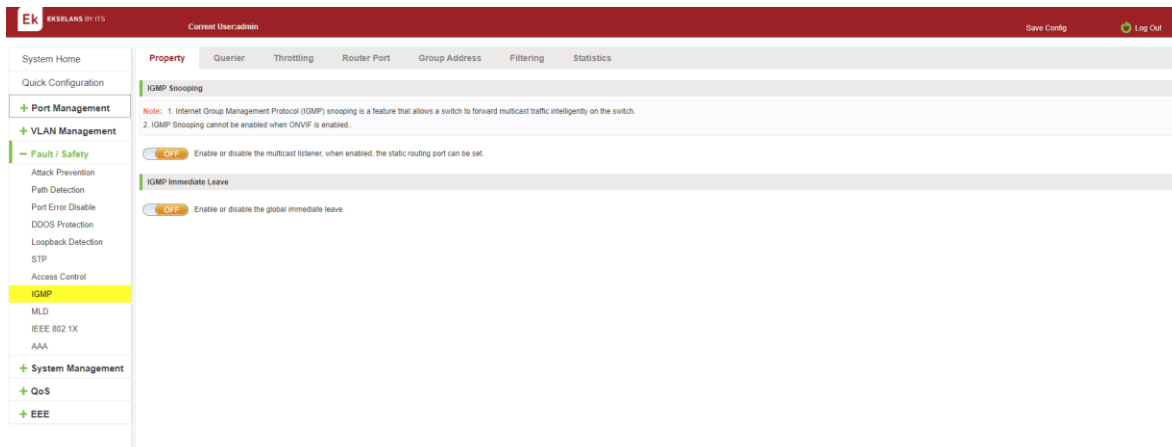


Figure 5-20: igmp.

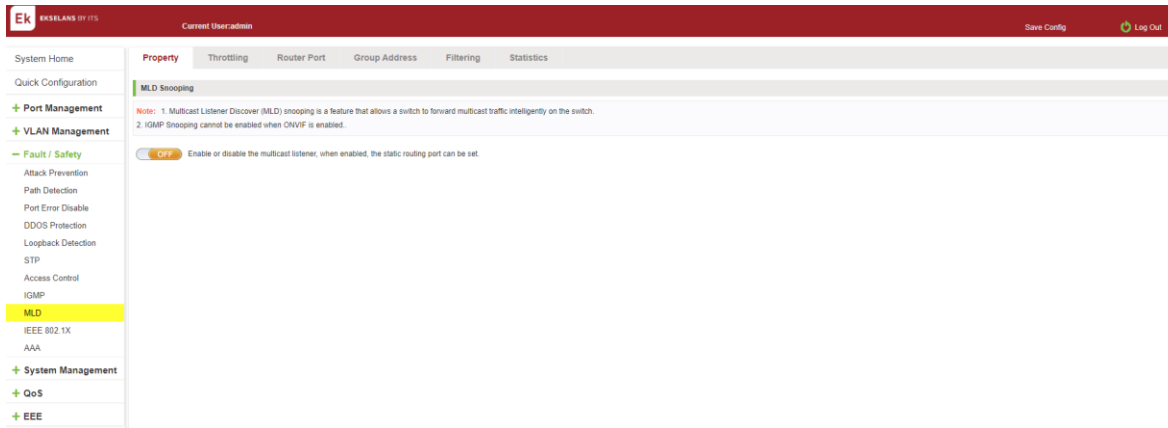


Figure 5-21: mld.

Step2: Enable Management VLAN.

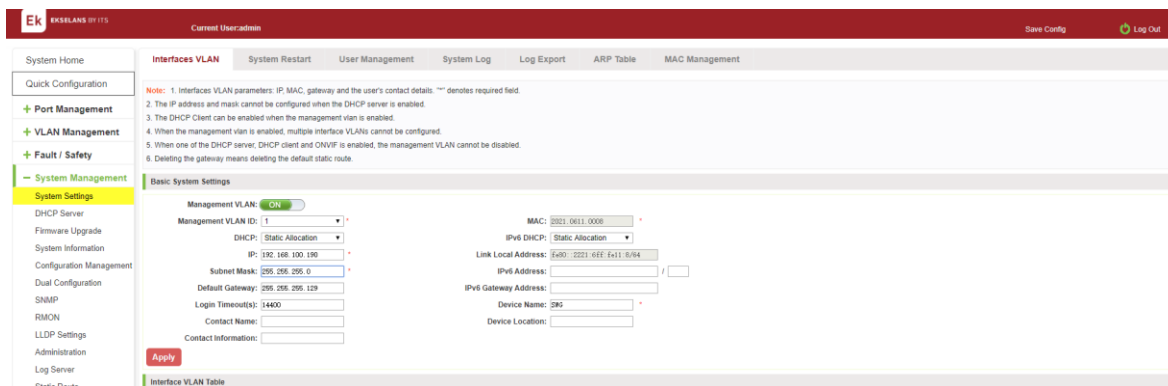


Figure 5-22: management vlan.

Step3: Confirm that the IP address segment of switch management address is the same as that of IPC and NVR.

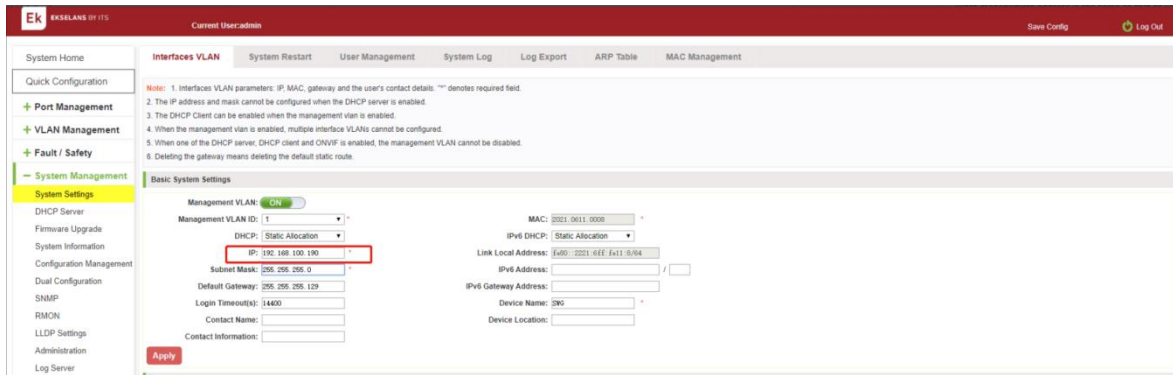


Figure 5-23: management vlan.

| ONVIF Global IP-Camera Information NVR Information | | | | |
|---|-----------------|----------------|---------------|--------------|
| IP-Camera Information | | | | |
| Port | IP Address | Model | Location | Manufacturer |
| 3 | 192.168.100.253 | IPC-HFW4631M-1 | country/china | Dahua |
| 4 | 192.168.100.251 | IPC-HFW4631M-1 | country/china | Dahua |

Figure 5-24: ip-camera information.

| ONVIF Global IP-Camera Information NVR Information | | |
|---|-----------------|-----------------|
| NVR Information | | |
| Port | IP Address | IP-Camera Numbe |
| 2 | 192.168.100.250 | 2 |

Figure 5-25: nvr information.

Step4: Configure the VLAN ID



Figure 5-26: onvif global.

Step5: Configure the port number used by the onvif protocol, The default is 554.



View IP-Camera information.

Click on the navigation bar "VLAN Management" "ONVIF" "IP-Camera Information" to view the IP-Camera information:

| Port | IP Address | Model | Location | Manufacturer | Traffic | Description | Throughput |
|------|-----------------|-----------------|---------------|--------------|----------|-------------|------------|
| 3 | 192.168.100.253 | IPC-HFW4631M-H1 | country/china | Dahua | 948.00M | | 4.00M |
| 4 | 192.168.100.251 | IPC-HFW4631M-H1 | country/china | Dahua | 1072.00M | | 4.00M |

First Previous 1 Next Last 1 / 1Page

Figure 5-27: IP-Camera information.

View Nvr information information.

Click on the navigation bar "VLAN Management" "ONVIF" " NVR infromation" to view the switch NVR information:

| Port | IP Address | IP-Camera Numbe | Throughput | Group | Description |
|------|-----------------|-----------------|------------|-------|-------------|
| 2 | 192.168.100.250 | 2 | 8.00M | 1 | |

Navigation: First Previous (1) Next Last / 1Page

Figure 5-28: NVR information.

Fault / safety.

ATTACK PREVENTION.

VIEW ARP CONFIGURATION.

Click the "Fault/Safety" "Attack Prevention" "ARP Inspection" to check the current switches has been configured for ARP information, this feature is turned off by default.

ARP Inspection

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

OFF After enabling ARP inspection, you can select trusted ports.

Figure 6-1: View port ARP Inspection information.

ARP INSPECTION FUNCTION.

In the ARP Inspection configuration, enable this function and then selected a port to configure some parameters .Click the "Apply" button to complete the configuration.

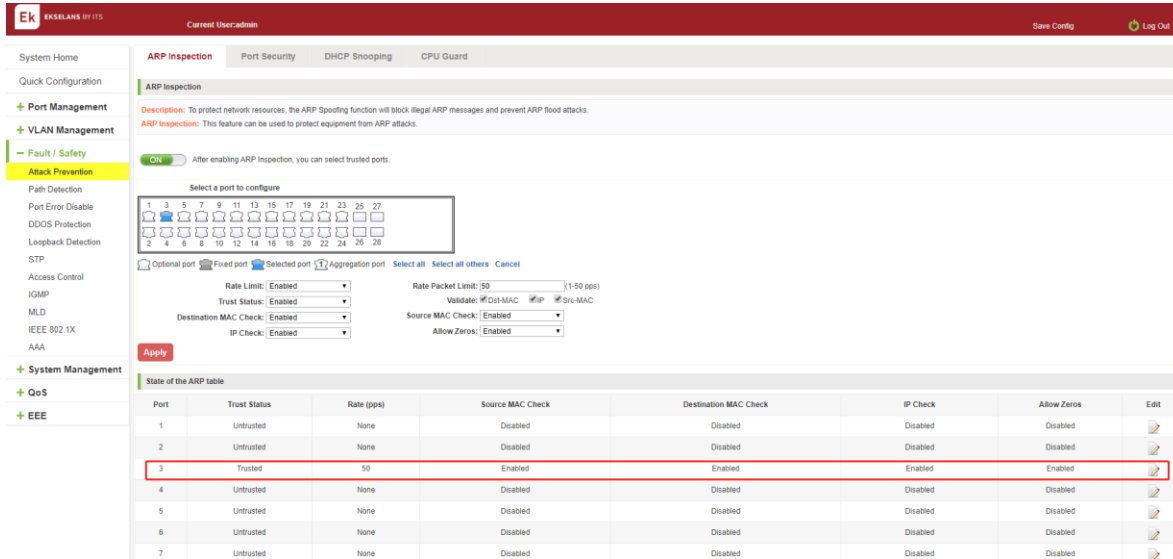


Figure 6-2: ARP Inspection configuration.

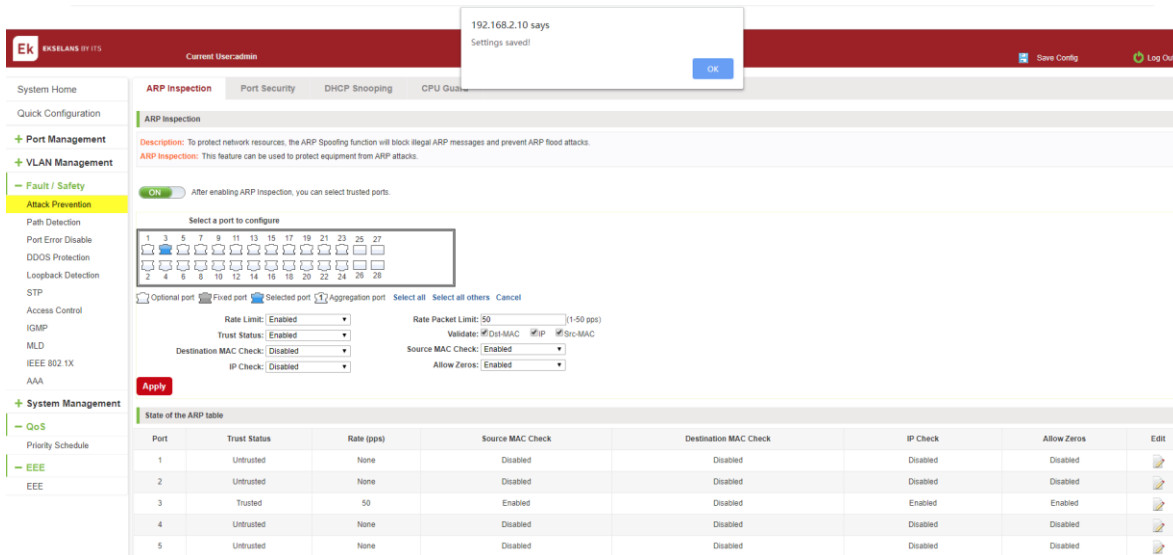


Figure 6-3: Change ARP Inspection configure.

| Port | Trust Status | Rate (pps) | Source MAC Check | Destination MAC Check | IP Check | Allow Zeros | Edit |
|------|--------------|------------|------------------|-----------------------|----------|-------------|------|
| 1 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 2 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 3 | Trusted | 50 | Enabled | Disabled | Enabled | Enabled | |
| 4 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 5 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 6 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 7 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 8 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 9 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |
| 10 | Untrusted | None | Disabled | Disabled | Disabled | Disabled | |

Figure 6-4: Change ARP Inspection configure success.

DISABLE ARP INSPECTION FUNCTION.

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

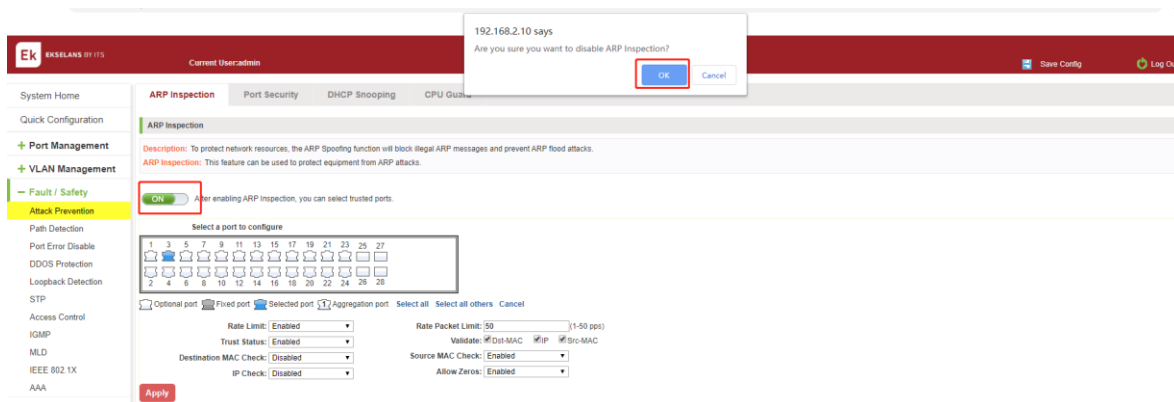


Figure 6-5: Disable ARP Inspection function.

CONFIGURATION PORT SECURITY.

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

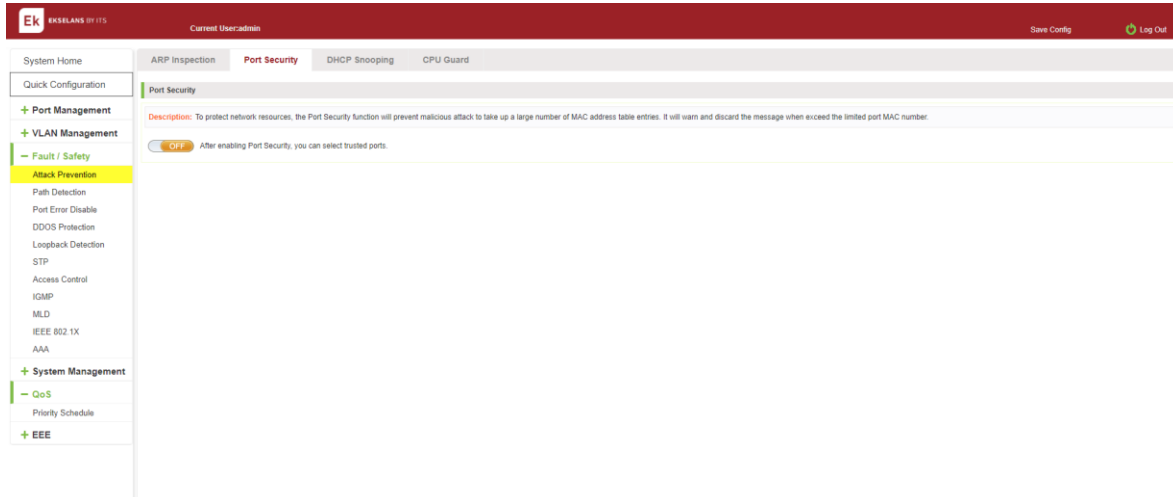


Figure 6-6: Port security configuration.

In the configuration pag, selected one or more ports, enable the admin state and configure the port max learning address. Finally click "Apply" button.

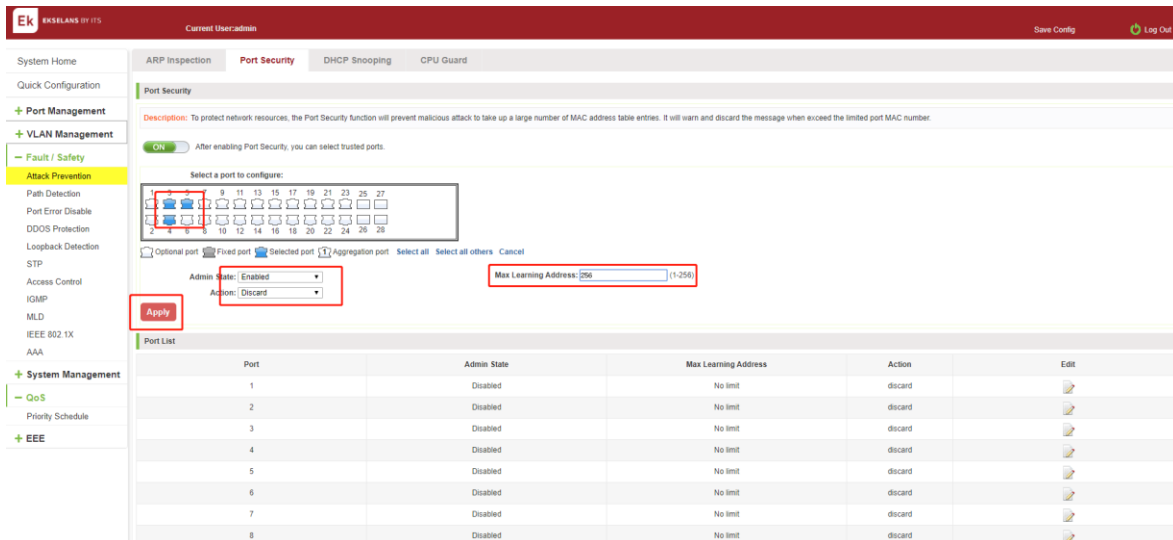


Figure 6-7: Port security manual configuration.

CHANGE PORT SECURITY STATUS.

In the port list, select the port to edit, change some parameters or disable the port security and click the button of "Apply".

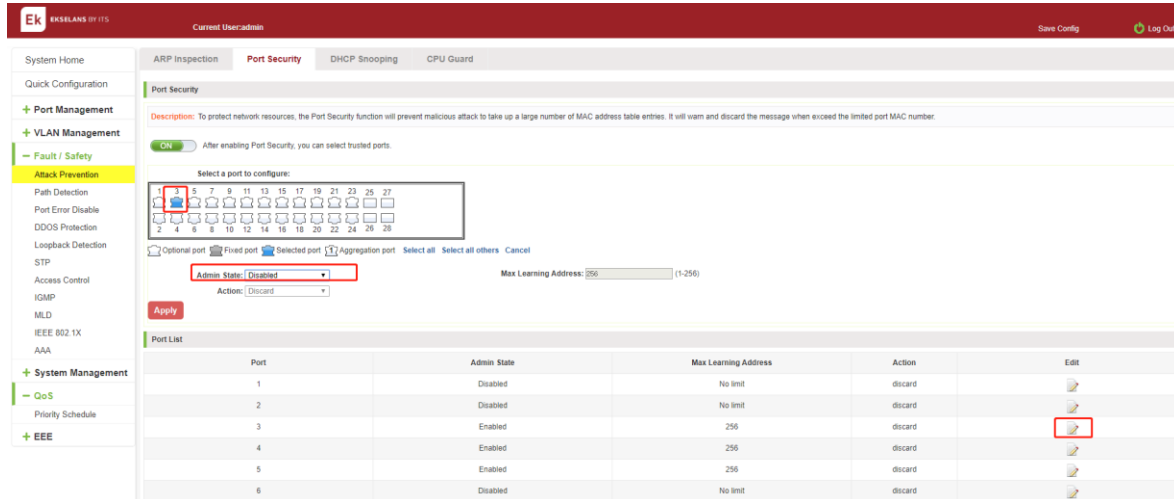


Figure 6-8: Change port security status.

VIEW DHCP snooping CONFIGURATION.

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

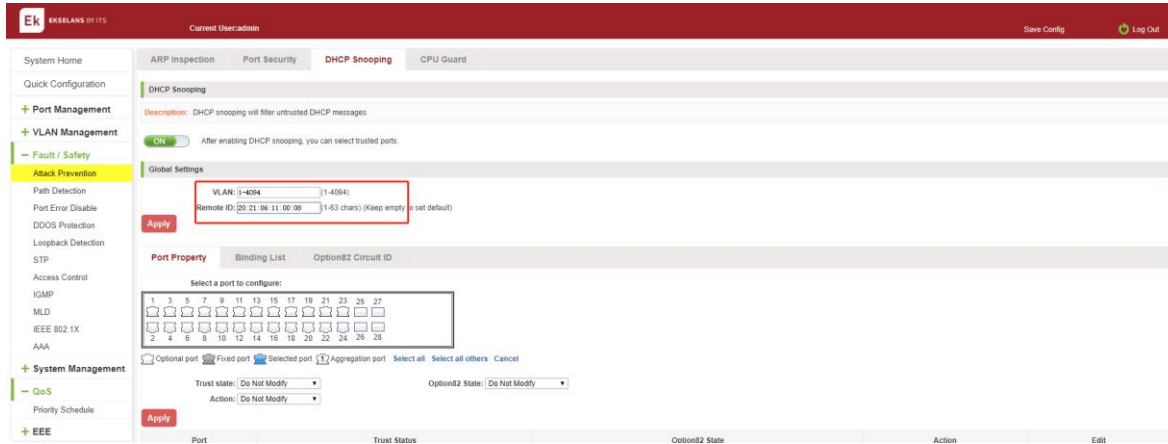


Figure 6-g: View anti DHCP snooping configuration information.

Display refresh configuration information.

OPEN DHCP snooping FUNCTION.

Click on a "Fault/Safety" "DHCP Snooping" click the button



to open the DHCP snooping:

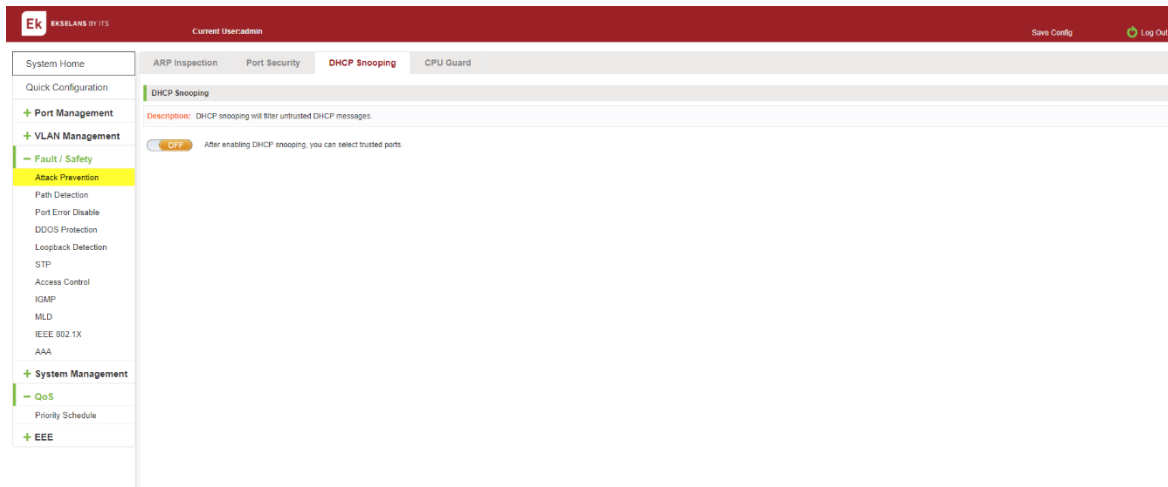


Figure 6-10: Activation of DHCP snooping function.

SET THE PORT TO DHCP SNOOPING TRUSTED PORT.

In the trusted port list, select the port that needs to be disabled to prevent DHCP attacks, and click the "Apply" button and enable option82 function

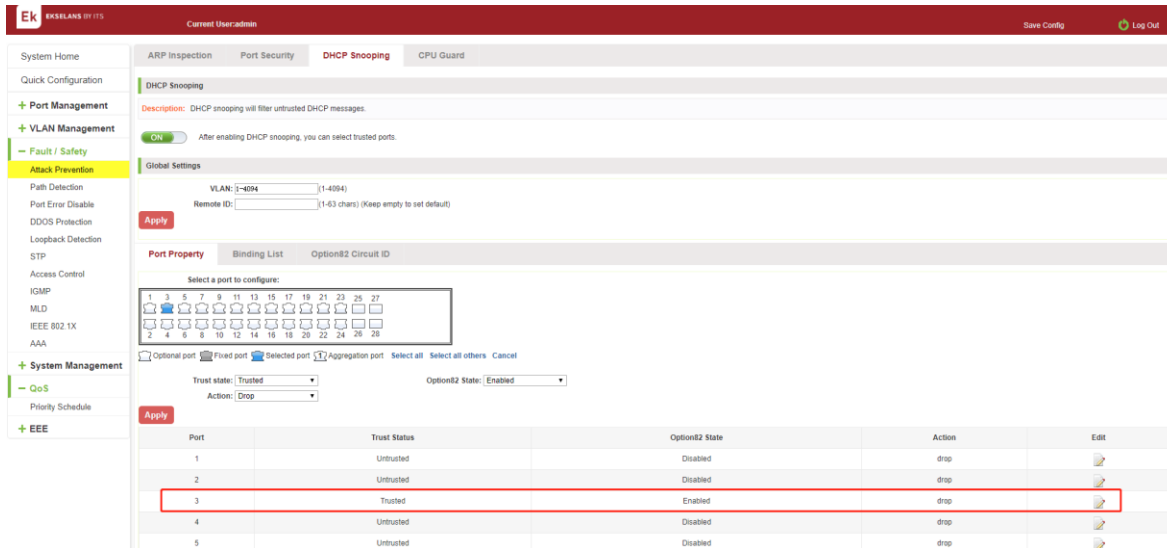


Figure 6-11: Disable anti-illegal DHCP server functions and enable option 82.

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.

Configure CID information.

Click the "option82 circuit id" button, configure the CID information:



Figure 6-12: CID information.

OFF DHCP snooping FUNCTION.

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

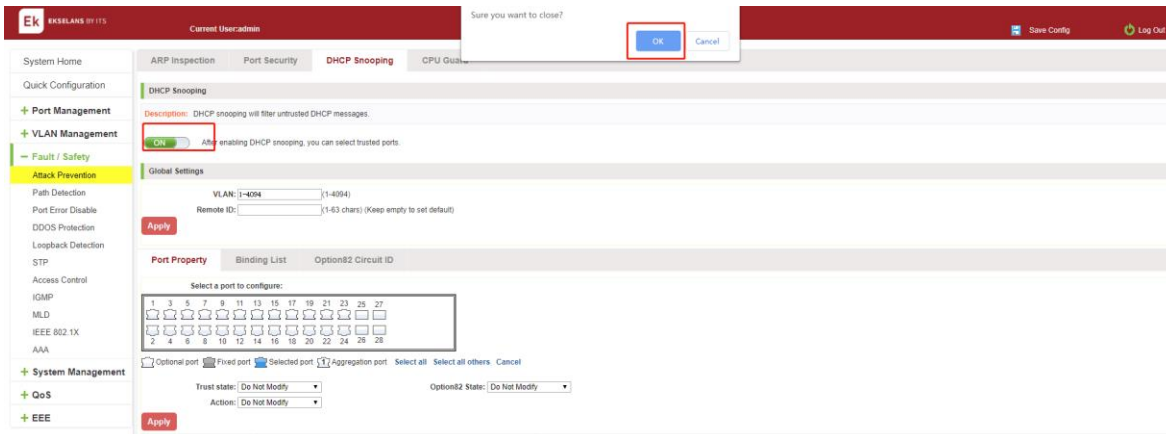


Figure 6-13: Off DHCP snooping function.

CPU GUARD.

Click the "Fault/Safety" "Attack prevention" "CPU Guard", the configuration information show the CPU guard.

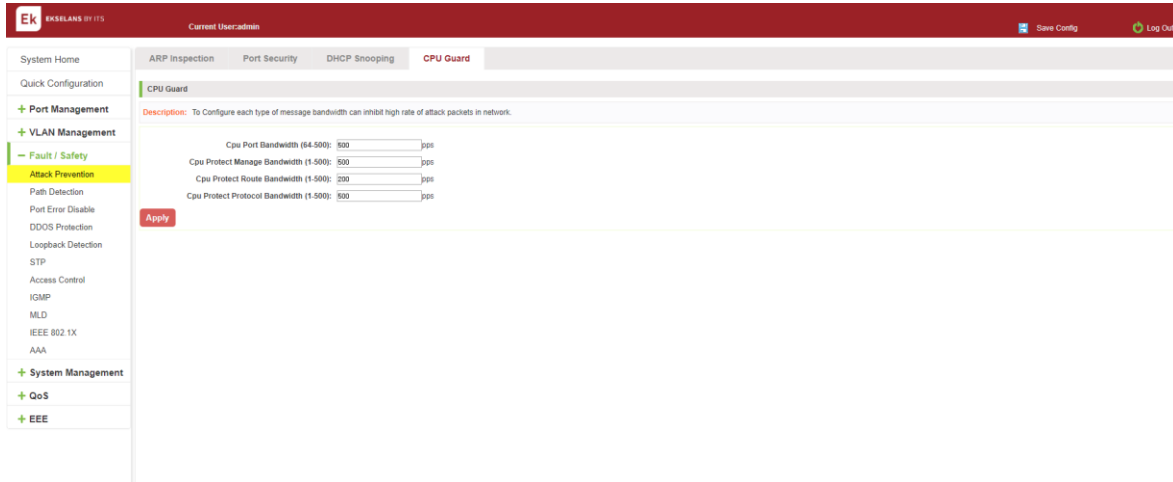


Figure 6-14: CPU Guard information.

Change CPU guard configuration:

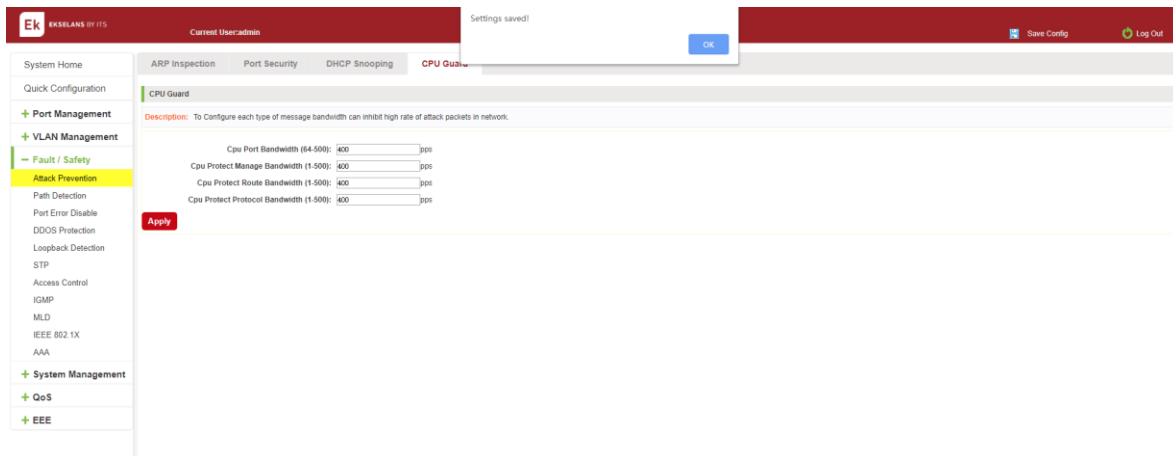


Figure 6-15: Change CPU Guard configuration.

Path detection.

Path /Tracert detection.

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

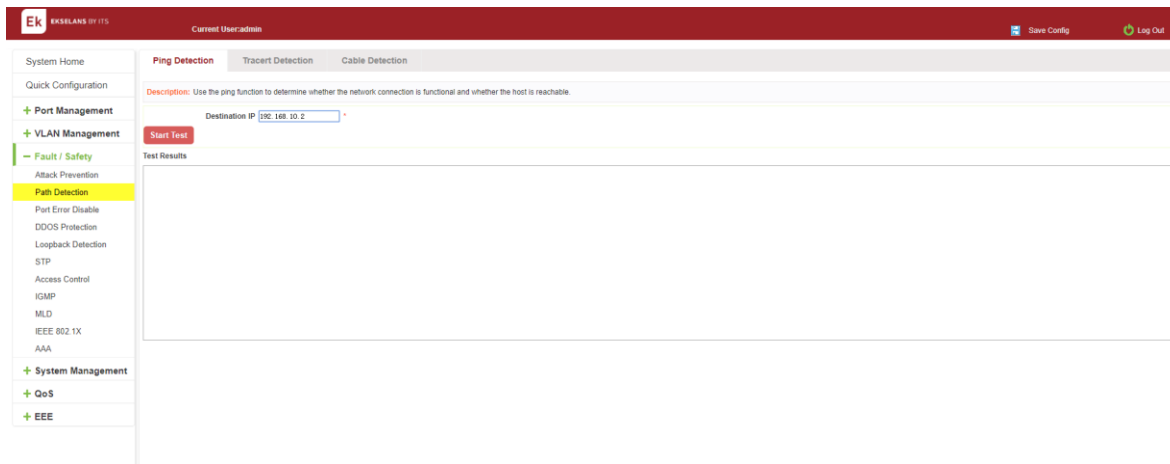


Figure 6-16: Path detection information.

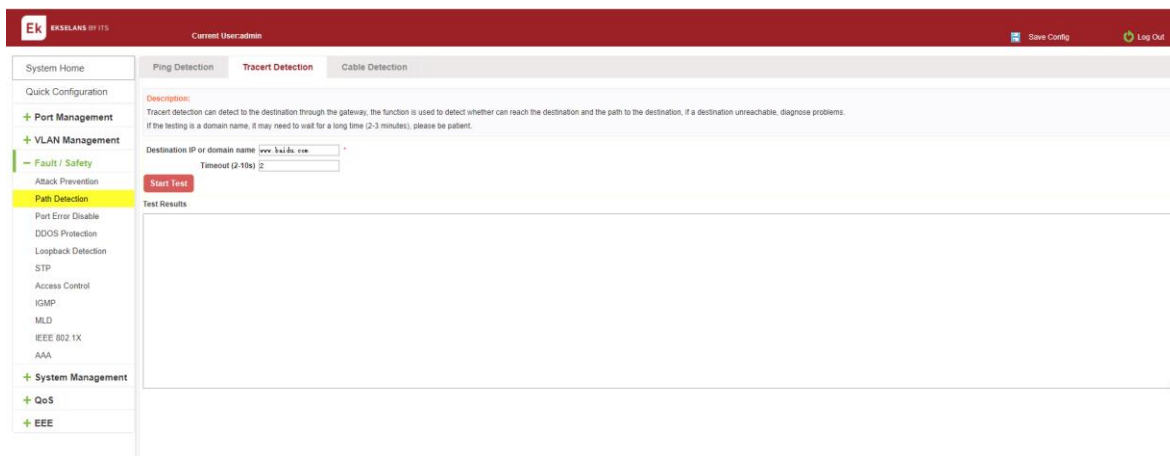


Figure 6-17: Tracert detection information.

Cable Detection.

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

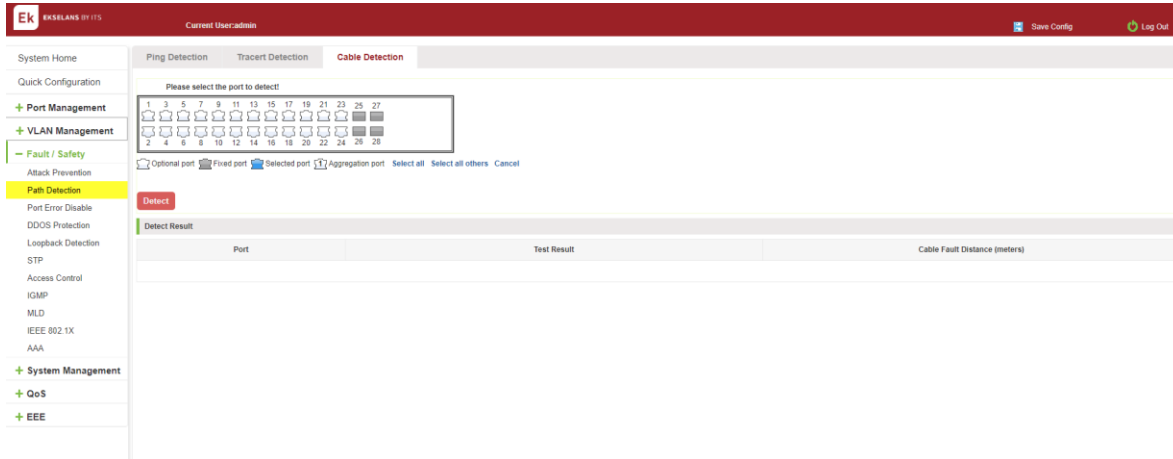


Figure 6-18: Cable detection information.

The cable detection only selected one port:

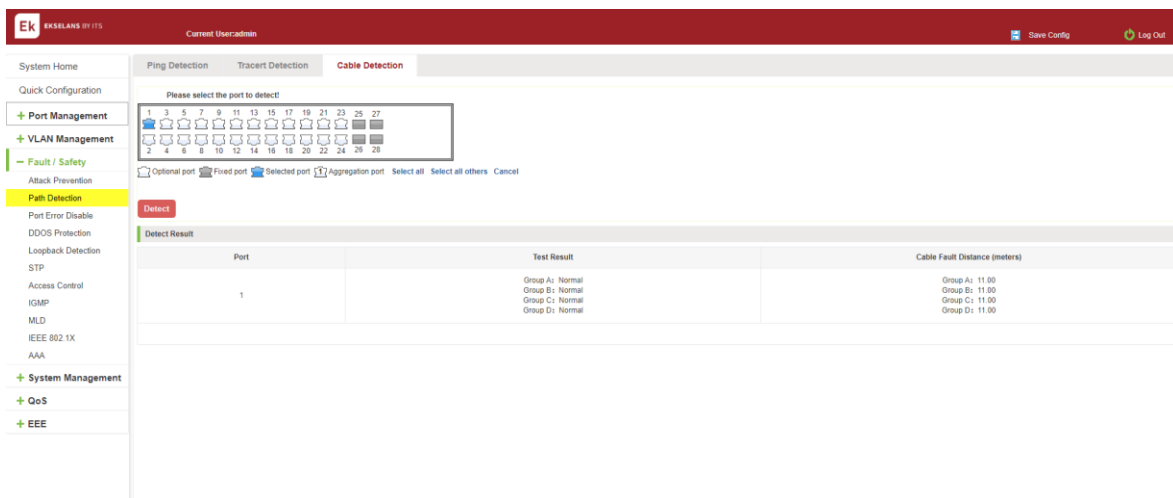


Figure 6-19: Port cable detection result.

DDOS PROTECTION.

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

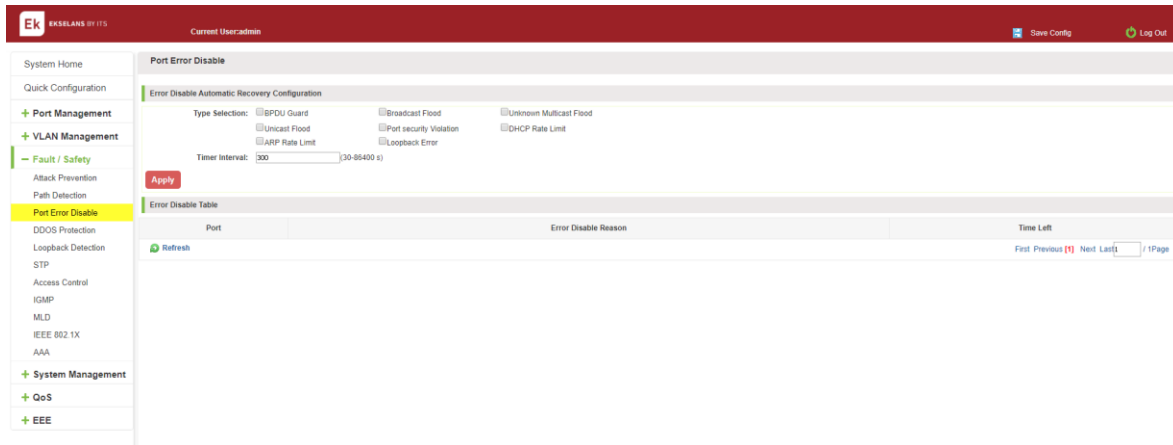


Figure 6-20: DDOS Protection information.

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

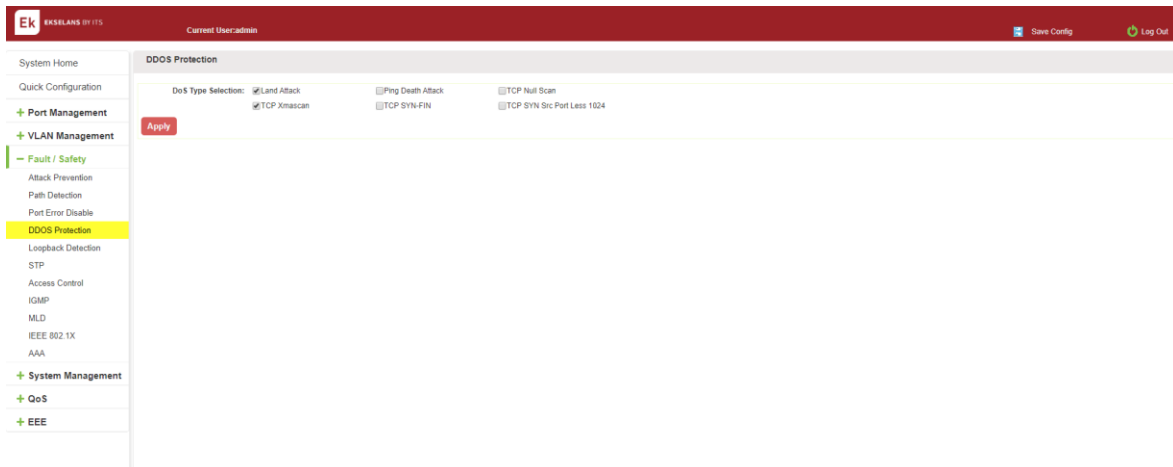


Figure 6-21: selected dos type.

Loop detection

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

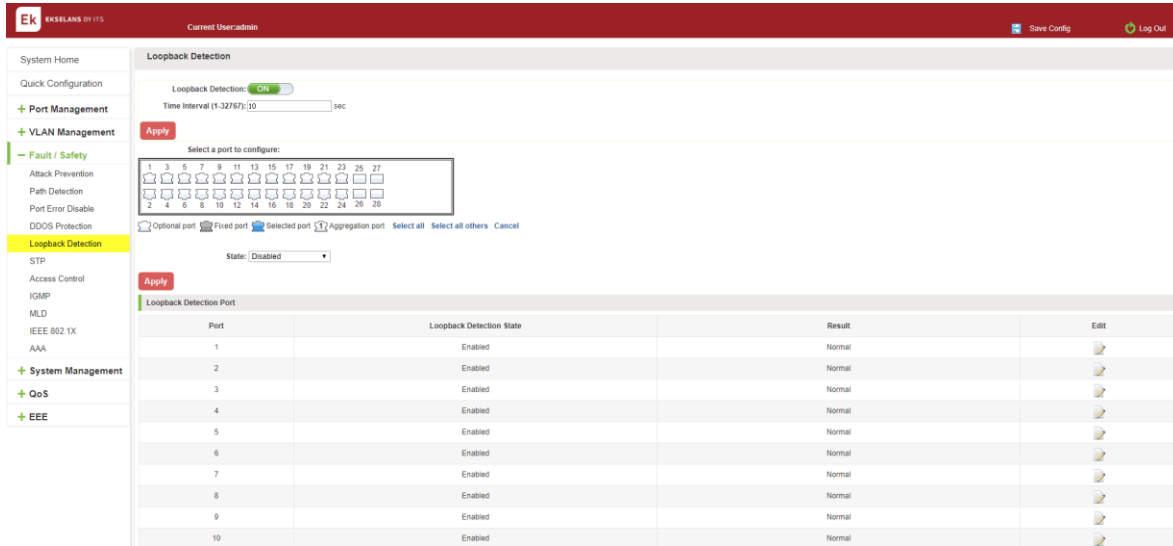


Figure 6-22: View loopback detection configuration information.

Choose the port to configure.

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

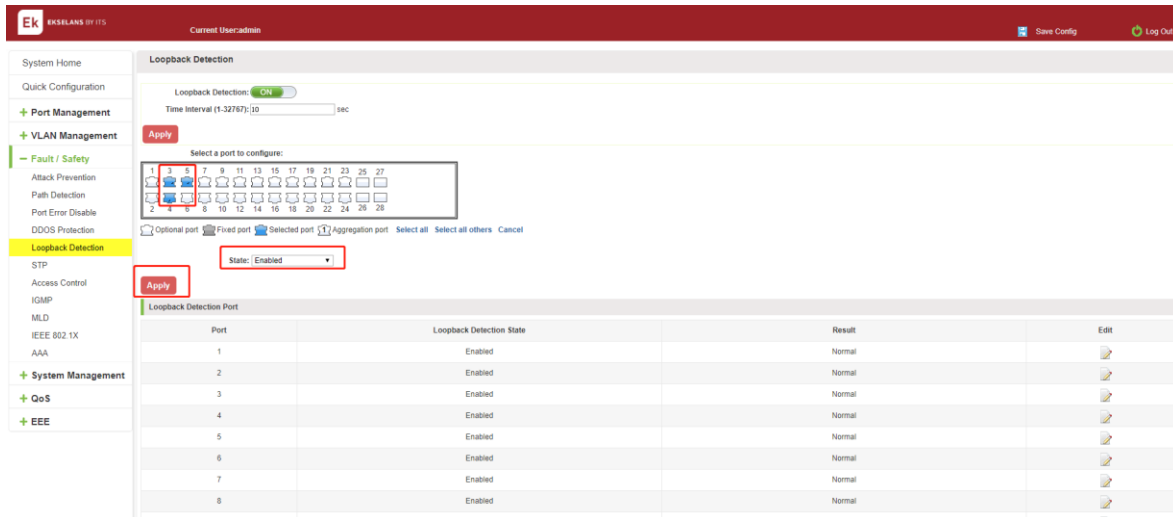


Figure 6-24: configure ports parameter.

Click "Edit" button, change the port status:

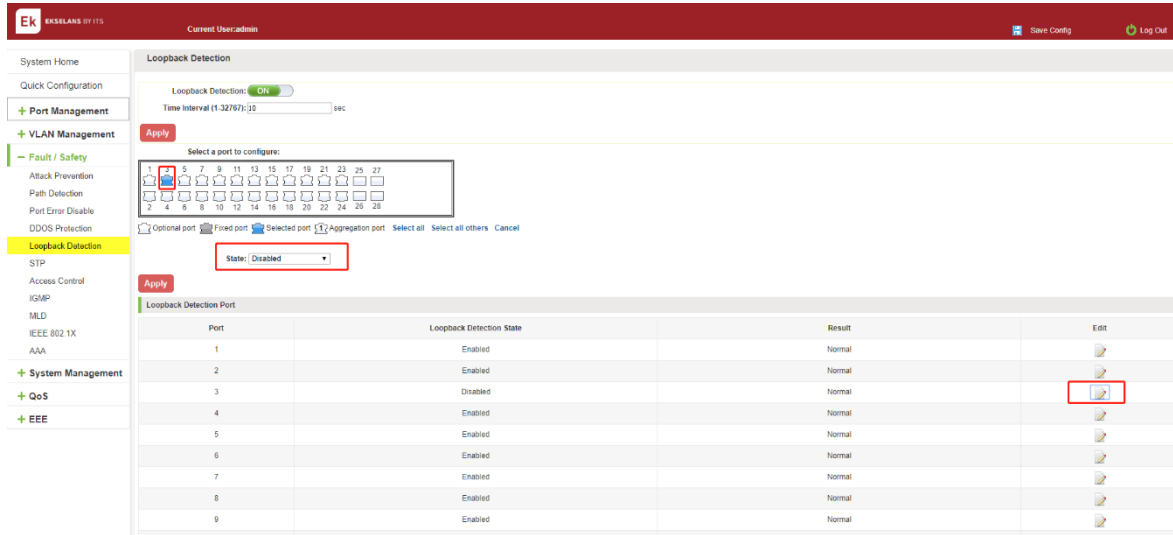


Figure 6-25: change the port configure.

STP.

Click the "Fault/Safety" "STP" "STP Global" can view the current STP global configuration:

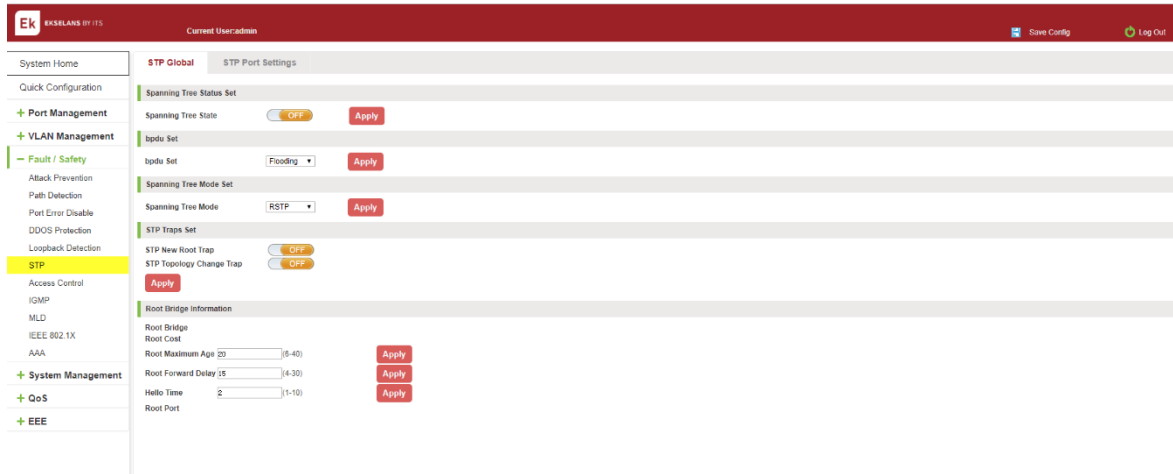


Figure 6-26: STP Global view.

ENABLE STP function.

Enable STP global state and configuration mode and traps.

Notice:

- 1When the loopback detection and STP functions are mutually exclusive.
- 2LLDP PDU Flooding enabled prevents executing mstp enable.

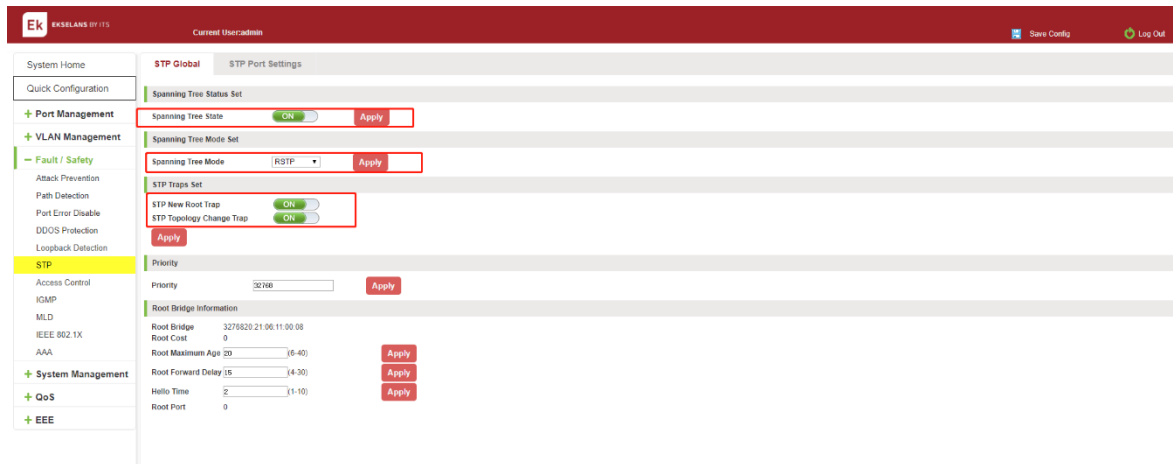
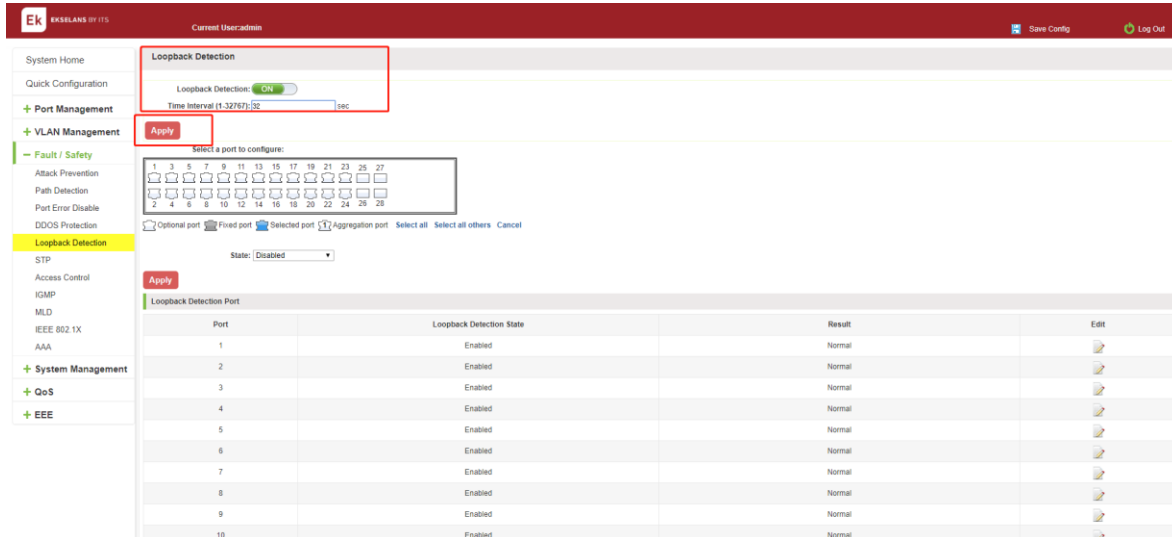


Figure 6-27: enable STP change mode and traps.

ENABLE LOOPBACK DETECTION.

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



STP PORT SETTINGS.

Selected port to configuration STP.

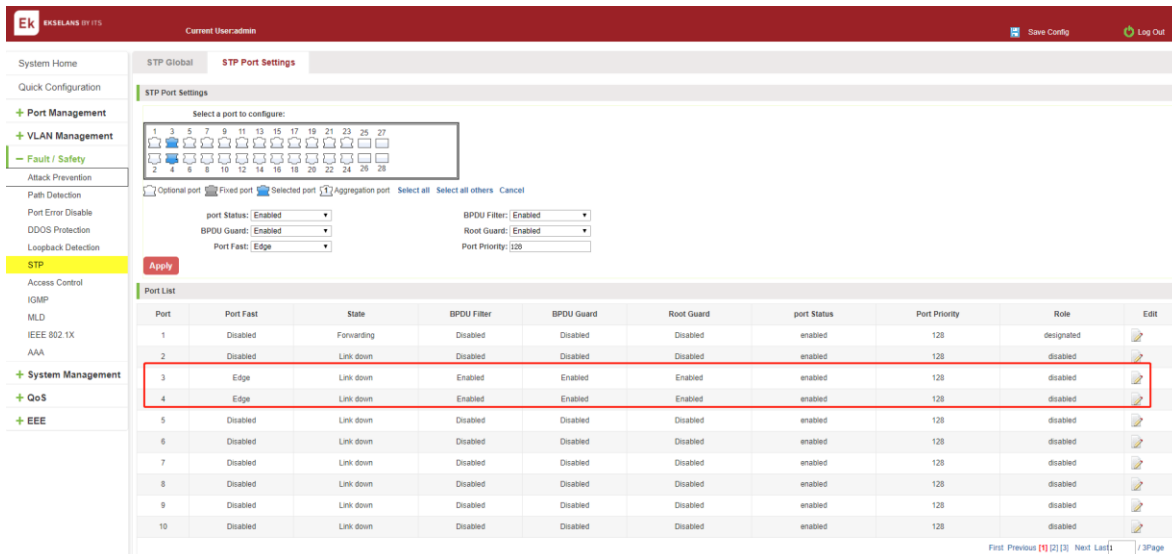


Figure 6-28: selected port to configuration STP.

Access control

VIEW ACCESS CONTROL LIST.

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

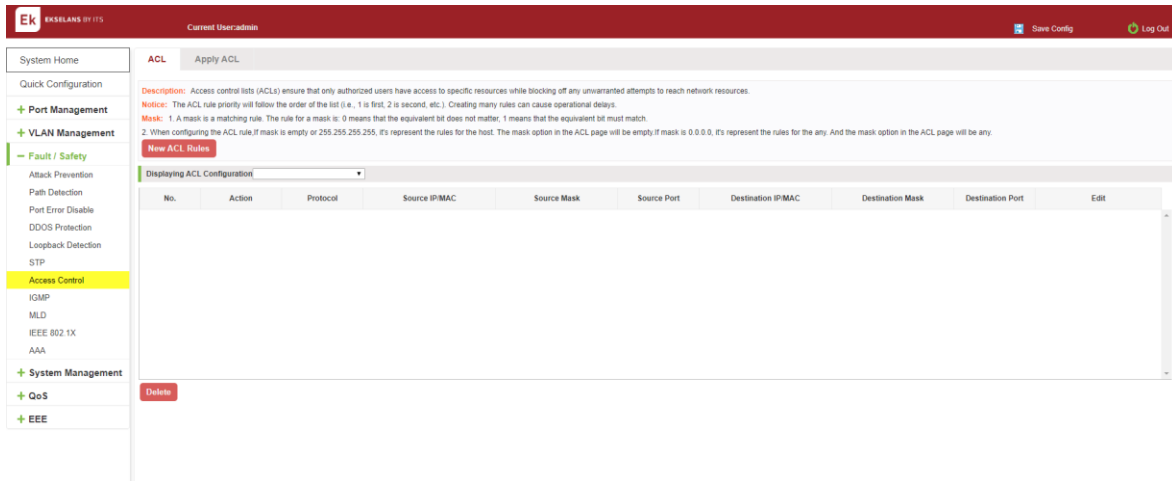


Figure 6-29: Access control list.

INCREASE THE STANDARD IP ACCESS RULES.

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

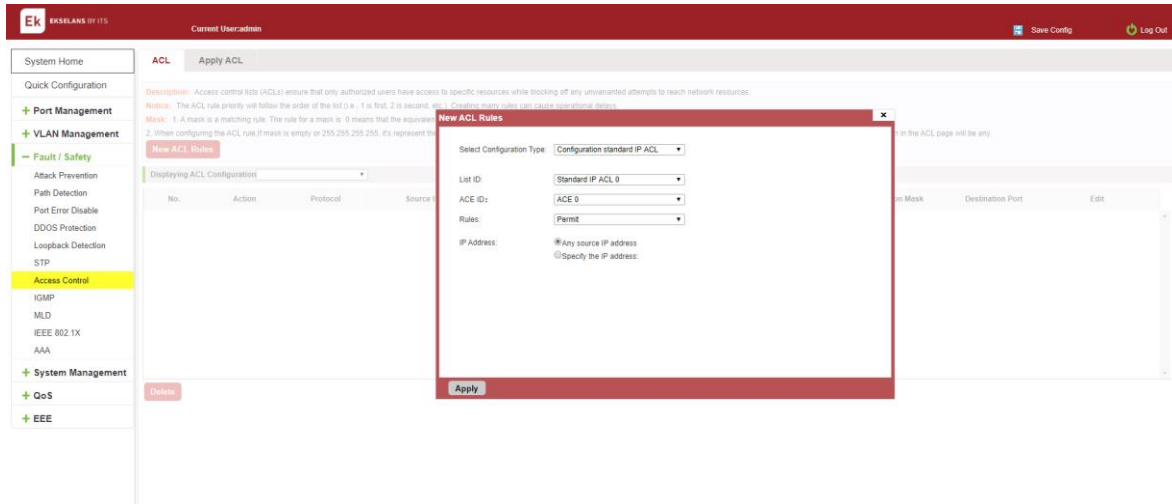


Figure 6-30: Configuration standard IP access control list.

INCREASE THE EXTENDED IP ACCESS RULE.

Click "ACL rules New", in the pop-up dialog box, select "Expand IPV4 ACL Configuration", in the list of ACE, ID:0 ID:10, rules for "Permit". Agreement: TCP, source IP address: any source IP address; purpose IP address: any destination IP address, click "Apply" to complete the new:

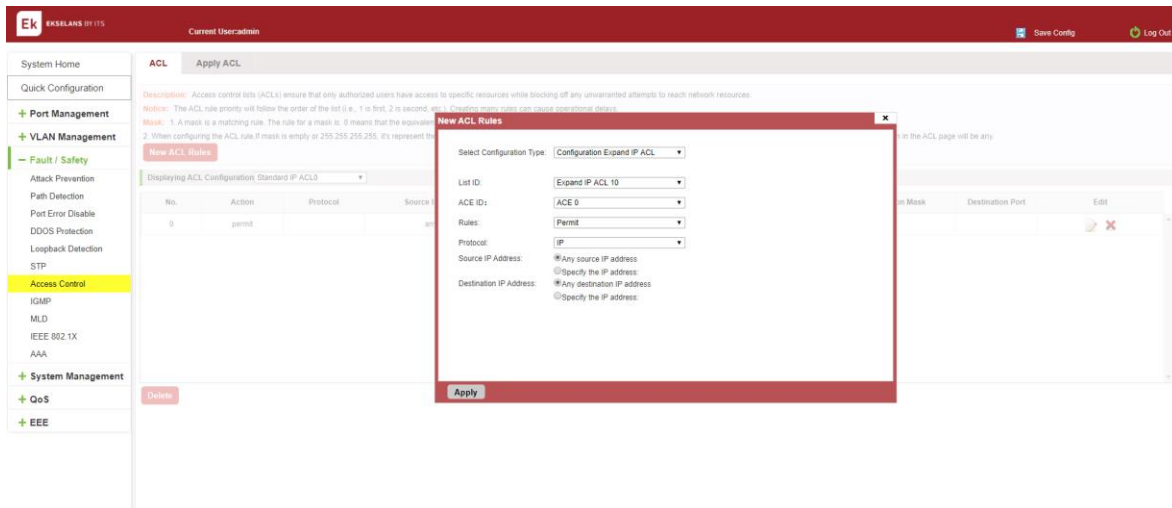


Figure 6-31: Configuration standard IP access control list.

INCREASING EXPAND MAC ACCESS RULES.

Click "New ACL rules", select "Configuration Expand MAC ACL" in the pop-up window, in list ID : 20 , ACE ID : 0, Rules "Deny"、Source MAC address : 0088.9999.999A

Destination MAC address is the random MAC。MAC protocol type : 0x0086。After the configuration is complete, click "Apply" :

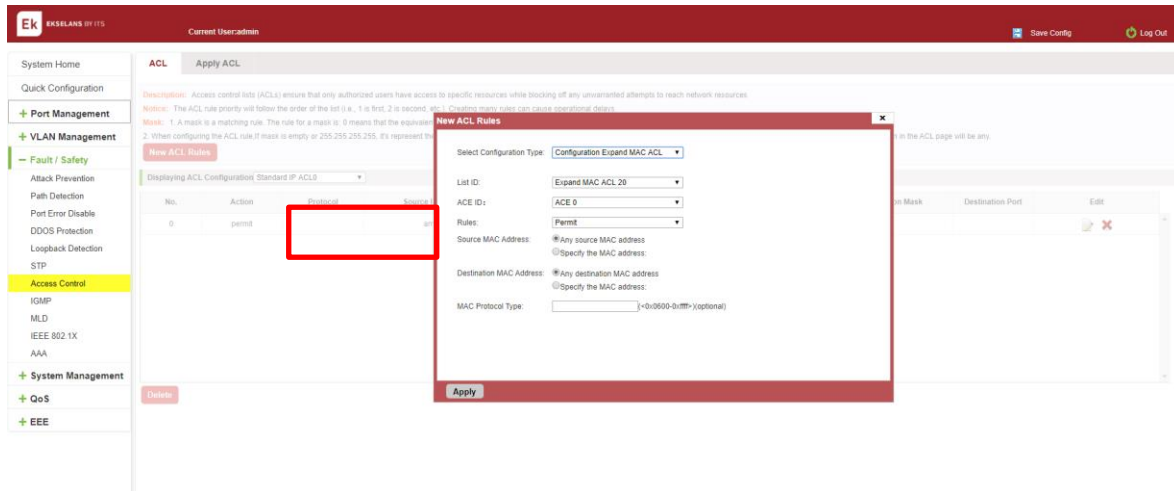


Figure 6-32: Configuration extended MAC access control list.

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.

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 "Apply":

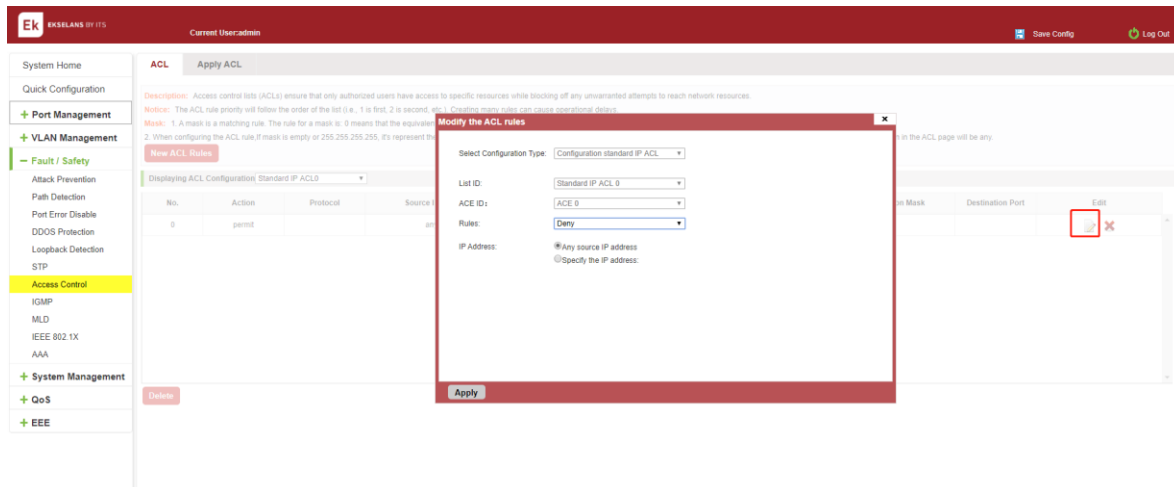


Figure 6-33: To modify the ACL rule.

Configuration instructions

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

DELETE RULE.

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

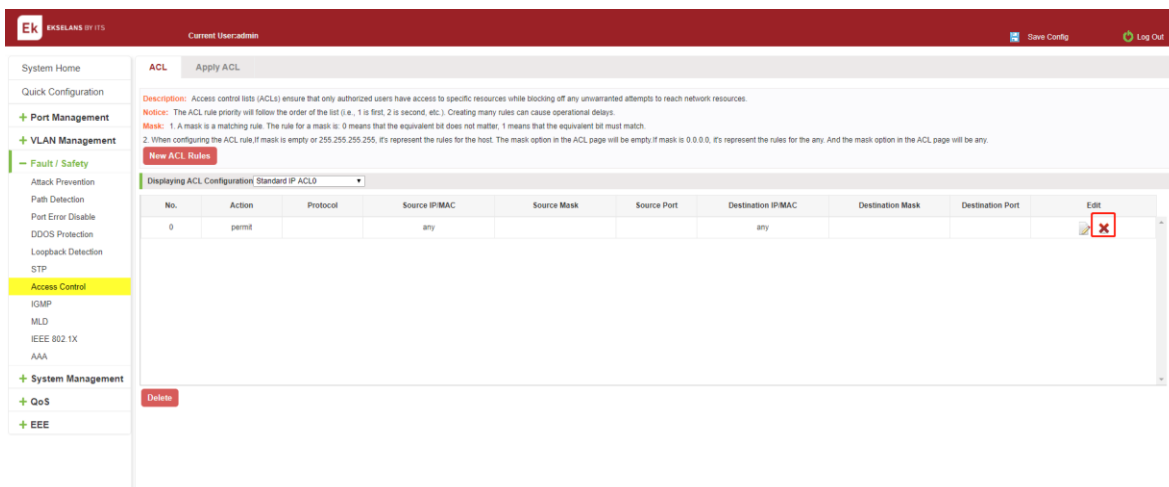


Figure 6-34: Delete rules.

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

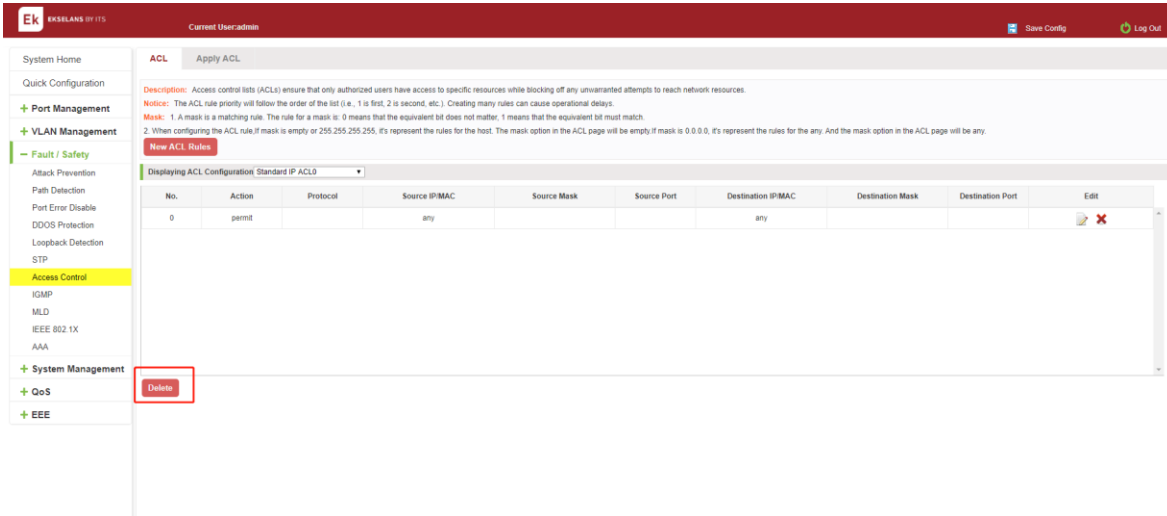


Figure 6-35: Delete ACL rules.

Configuration instructions.

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

VIEW APPLICATION ACL.

"Apply"->"Access Control"->"Fault/Safety" ACL:

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

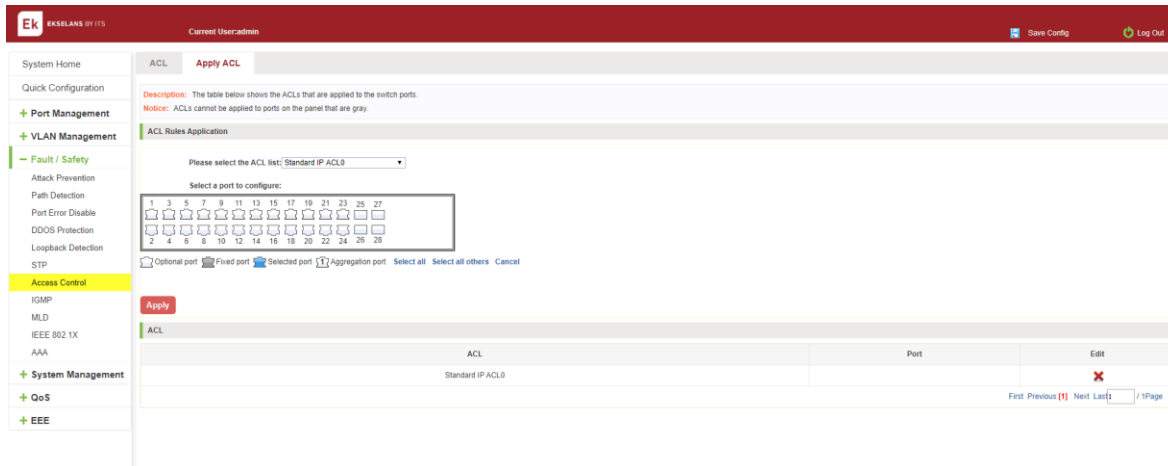


Figure 6-36: View application ACL rules.

INCREASED APPLICATION ACL.

"Apply":

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

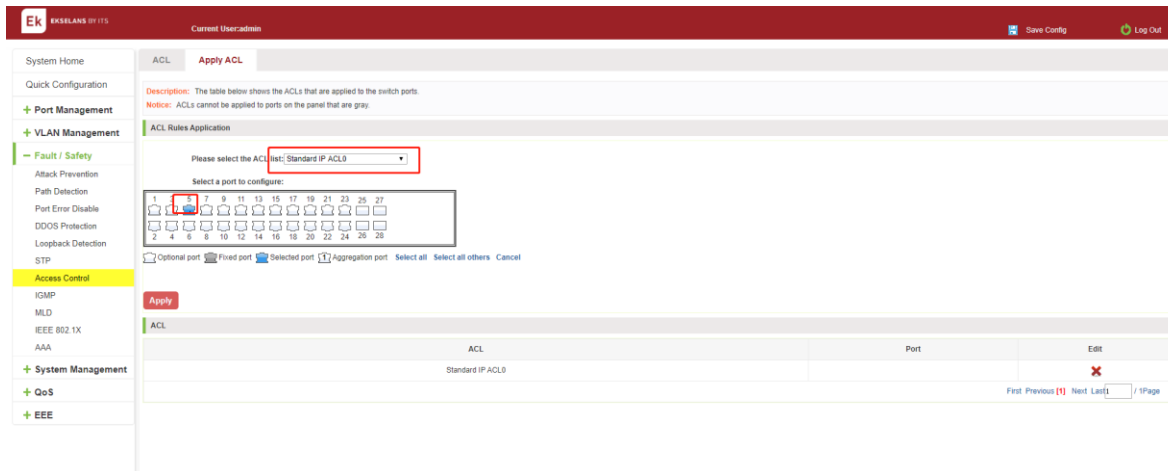


Figure 6-37: Add applications ACL.

DELETE APPLICATION ACL.

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

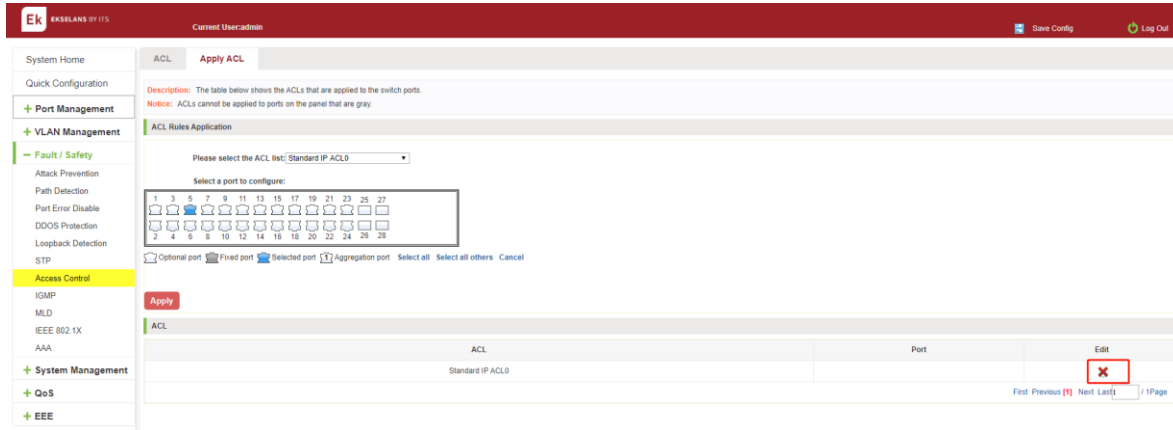


Figure 6-38: Delete application ACL.

IGMP Snooping.

VIEW IGMP SNOOPING CONFIGURATION.

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

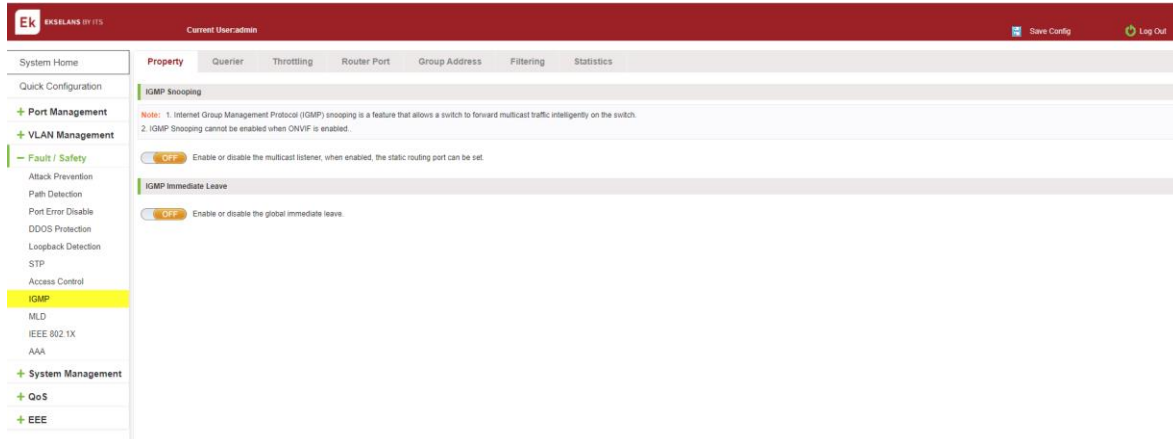


Figure 6-39: View Snooping IGMP configuration information.

ACTION MULTICAST LISTENER FUNCTION.

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

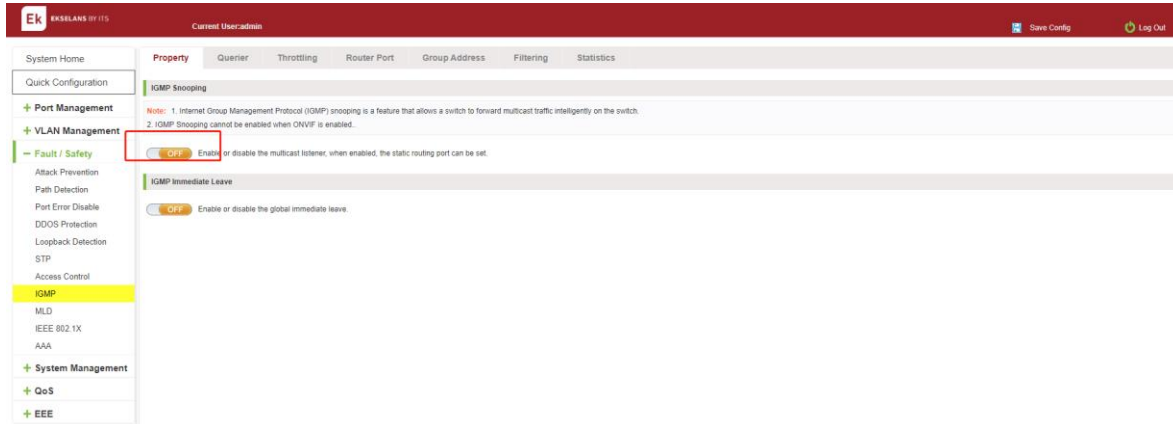


Figure 6-40: Open multicast listener configuration.

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.

DISABLE MULTICAST LISTENNER FUNCTION.

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

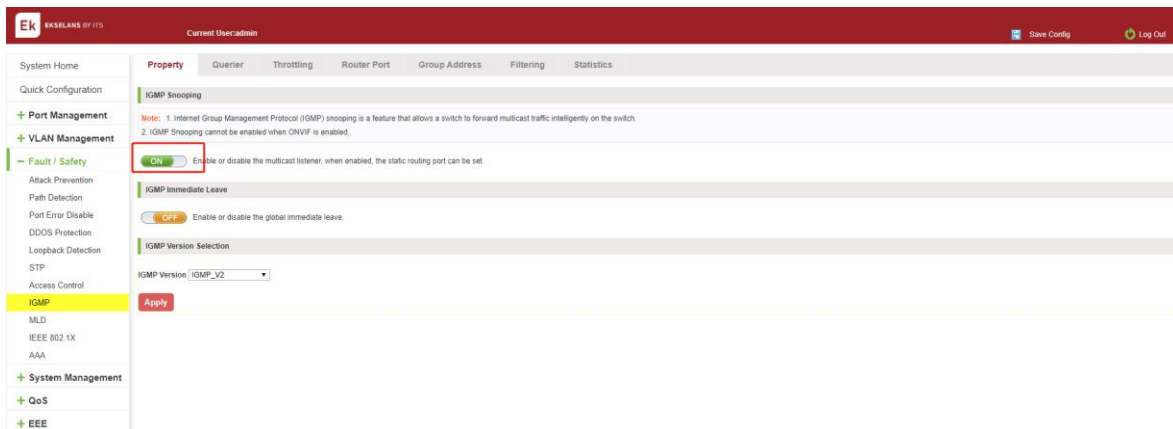


Figure 6-41: Closed multicast listener function operation.

CONFIGURATION MULTICAST ROUTING.

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

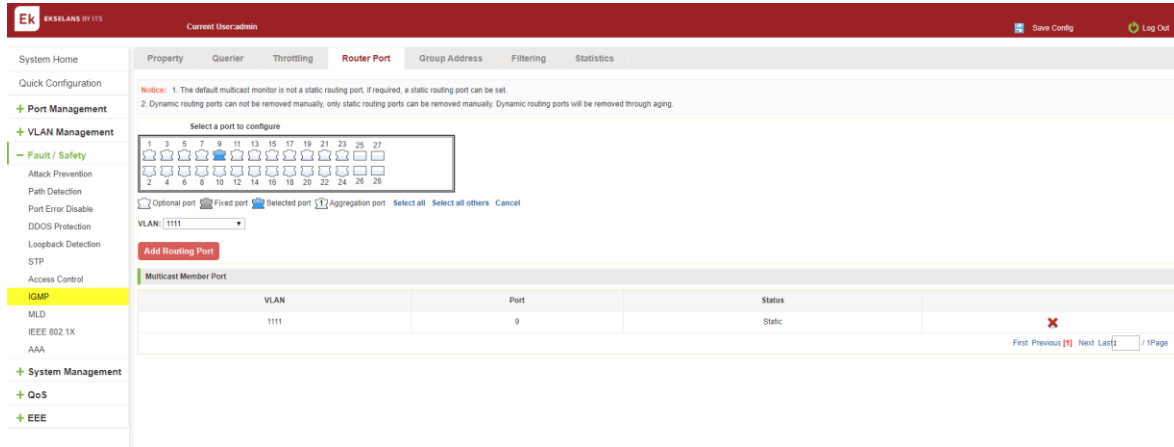


Figure 6-42: Configuration of multicast routing.

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.

IGMP VERSION.

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

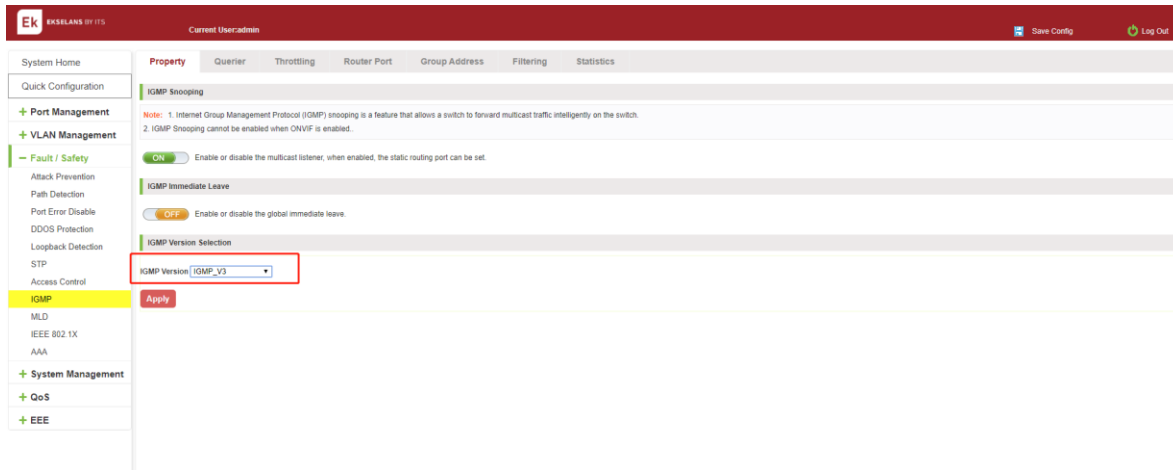


Figure 6-43: Configuration IGMP version.

IGMP version configuration steps are as follows:

Step1: Select the required version number.

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

VIEW MLD CONFIGURATION.

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

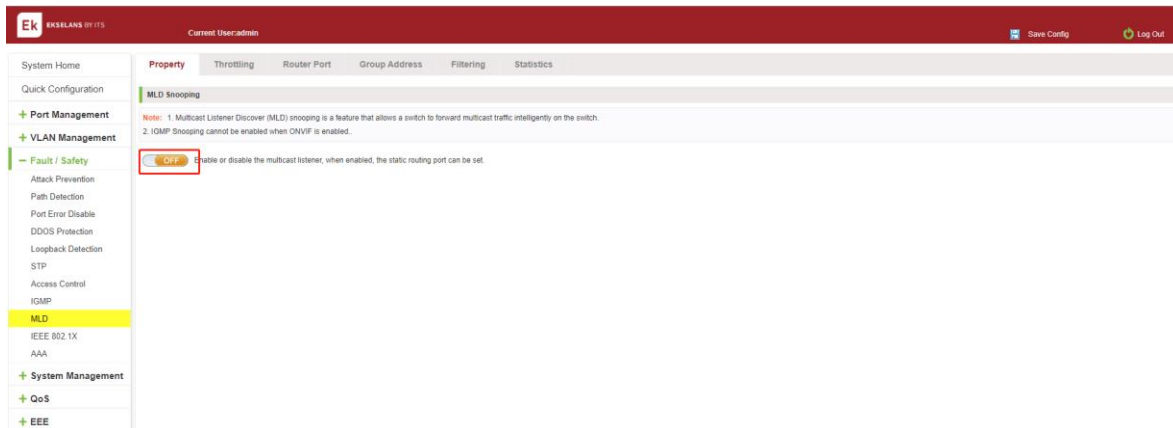


Figure 6-44: View MLD configuration information.

ACTIVE MULTICAST LISTENER FUNCTION.

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

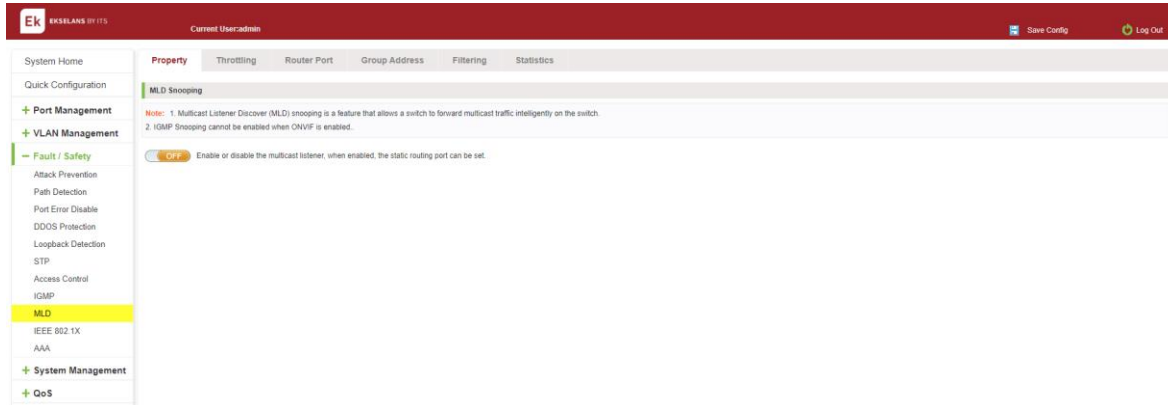


Figure 6-45: Open multicast listener configuration.

The default multicast listener (MLD) did not open.

The default on multicast listener (MLD), all VLAN are open.

The default version of V1 - MLD.

DISABLE MULTICAST LISTENER FUNCTION.

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

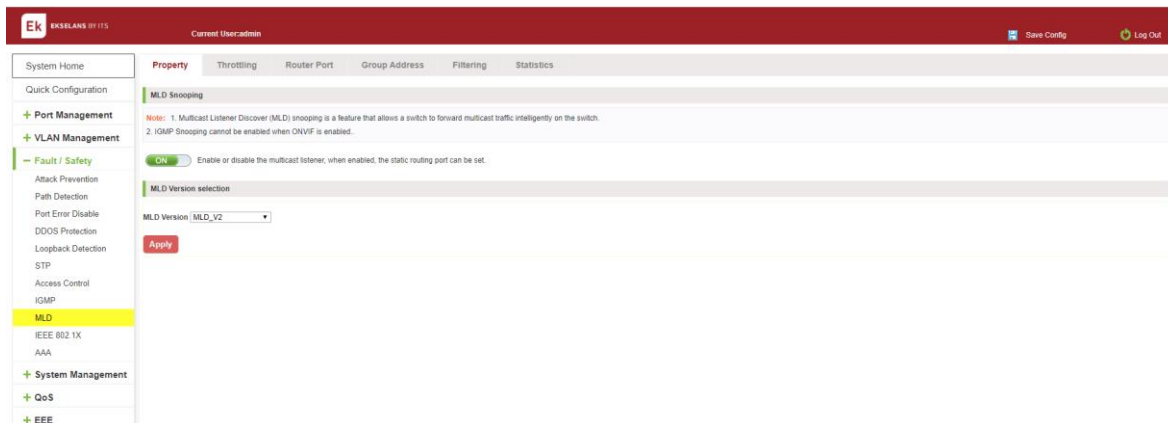


Figure 6-46: Closed multicast listener function operation.

CONFIGURATION MULTICAST ROUTING.

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

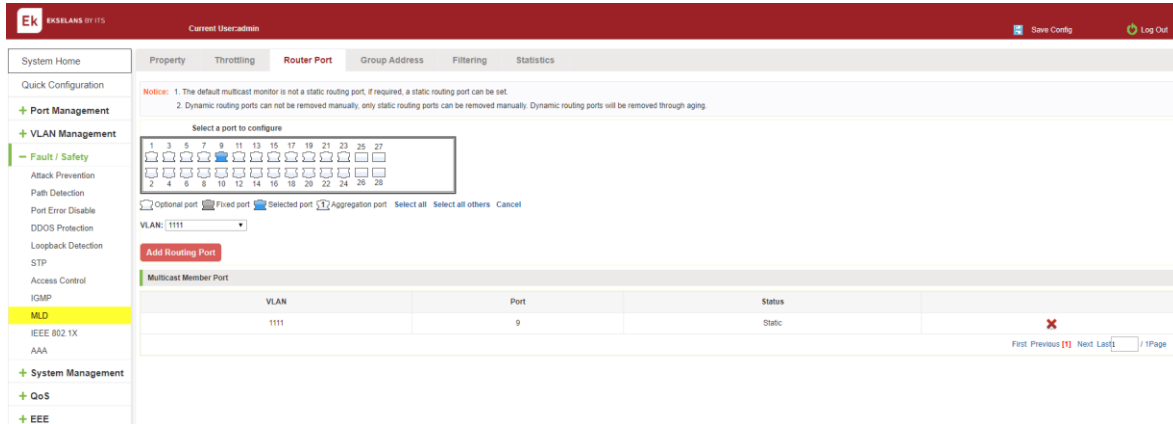


Figure 6-47: Configuration of multicast routing.

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.

IEEE 802.1X.

IEEE 802.1X is a port-based authentication protocol, is a method and strategy for authenticating users.

Configure the PC 192.168.2.145, and connect with switch by Gi 0/2

Configure the radius sever 192.168.2.100, and connect with switch by Gi 0/1

Click ON "Fault / safety" "IEEE 802.1X".

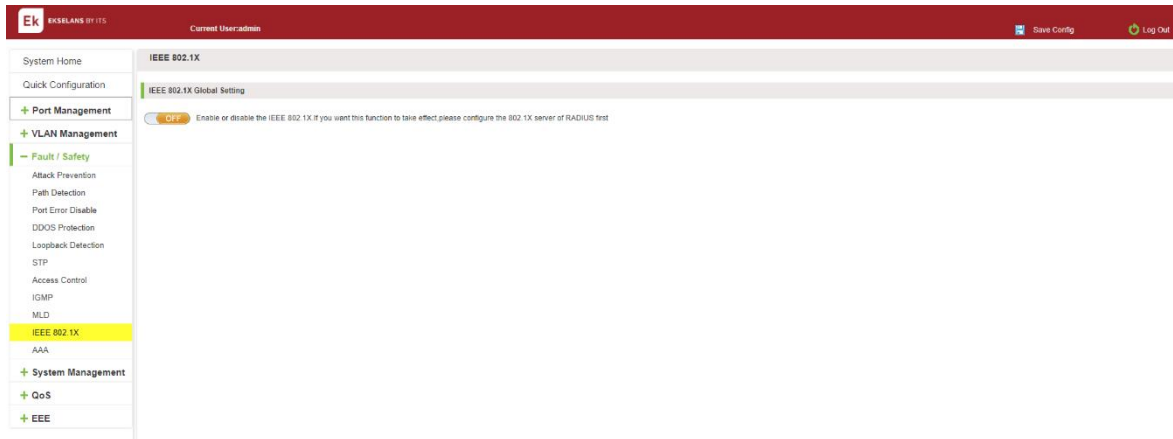


Figure 6-48: IEEE 802.1X.

Click to OPEN.

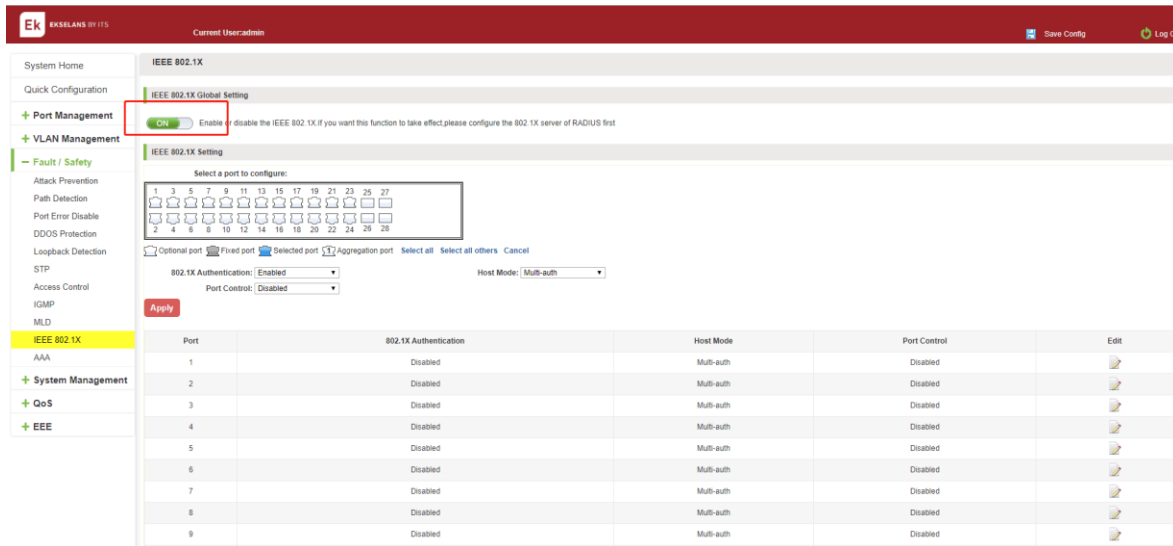
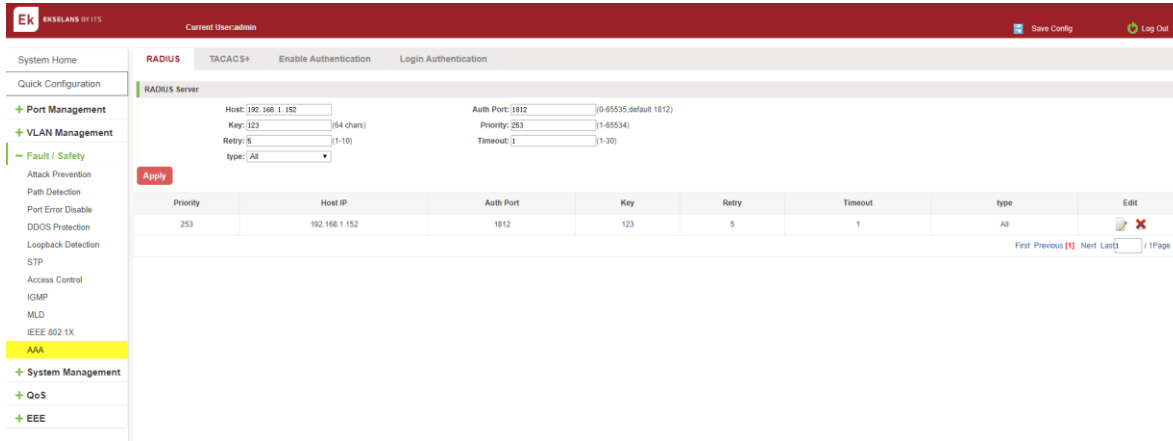


Figure 6-49: Enable IEEE 802.1X.

Switch config AAA RADIUS server address:192.168.1.152, Auth Port: 1812, Key:123, type: all.



Switch enable 802.1X port Gi 0/9, Port Control: auto, Host Mode: multi-auth.

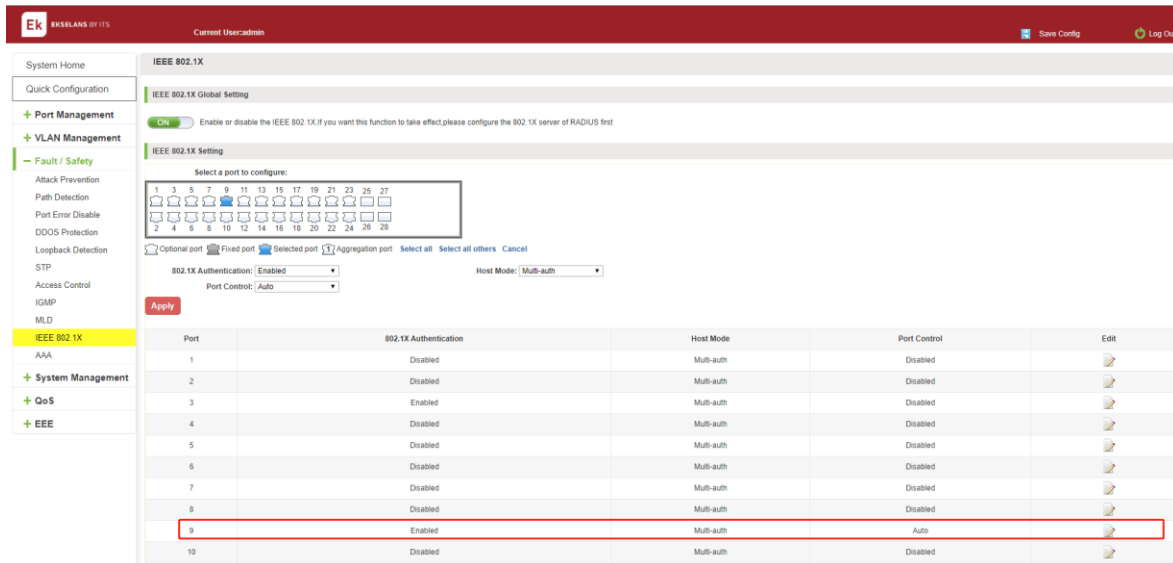


Figure 6-51: configuration IEEE802.1X.

Tips: The IEEE802.1x function is used with the AAA function.

Auto: It indicates that the initial state of the port is unauthorized. It only allows EAPOL packets to be sent and received. It does not allow users to access network resources. If the authentication passes, the port switches to the authorized state, allowing the user to access the network resources. This is also the most common case.

Force-auth: Indicates that the port is always authorized, allowing users to access network resources without authorization.

Force-unit: Indicates that the port is always in an unauthorized state and does not allow the user to authenticate. The device does not provide authentication services to clients that pass through the port.

Single host: This port can only connect to a host, through authentication can be forwarded for data packets.

Multi-auth: This port can be connected to the following switches, including a host through the certification, other hosts can be forwarded data packets.

Multi-host: This port can be connected to the following switches, including a host through the certification, other host data packets cannot be forwarded, must also have passed authentication.

AAA.

RADIUS.

Enabled and logged in can use radius authentication.

Configure the PC 192.168.2.145 and connect with switch by Gi 0/2.

Configure the radius sever 192.168.2.100 and connect with switch by Gi 0/1.

Click ON "Fault / safety" "AAA" "RADIUS".

Switch config AAA RADIUS server address:192.168.2.100, Auth Port:1812, Key:123, type: all.

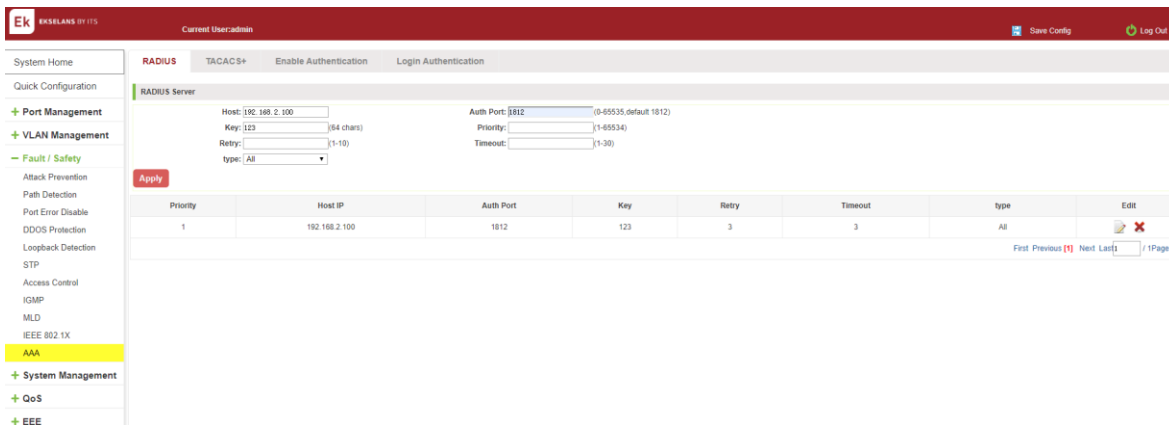


Figure 6-52: configuration radius.

Switch config Method List: Name: test, Method1: RADIUS, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2 Click Apply.

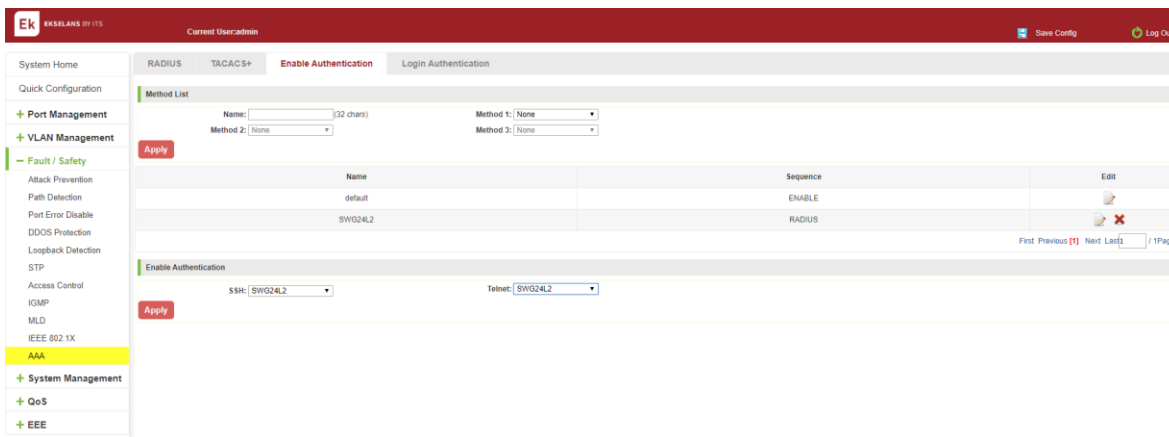


Figure 6-53: configuration enable authentication

Switch config Method List: Name: SWG24L2, Method 1: RADIUS, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.

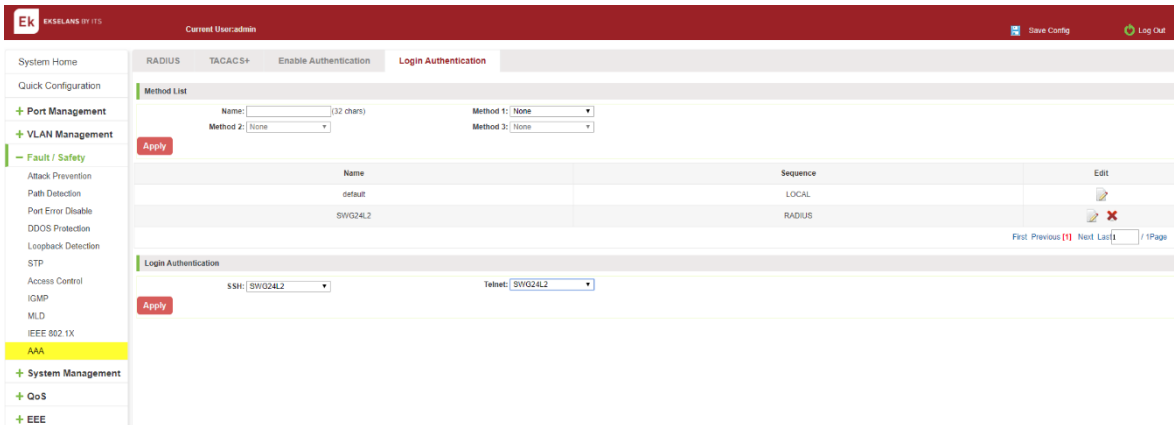


Figure 6-54: configuration login authentication.

TIPS:

1. PC input right username and password, PC can console, telnet and ssh switch
2. PC input right password, user can join "# mode".

TACACS+.

Enable and Login can use TACACS+ authentication.

Configure the PC 192.168.2.145 and connect with switch by Gi 0/2.

Configure the TACACS+ sever 192.168.2.100 and connect with switch by Gi 0/1.

Click ON "Fault / safety" "AAA" "TACACS+".

Switch config AAA TACACS+ server address:192.168.2.100, Auth Port:49, Key: qwer.

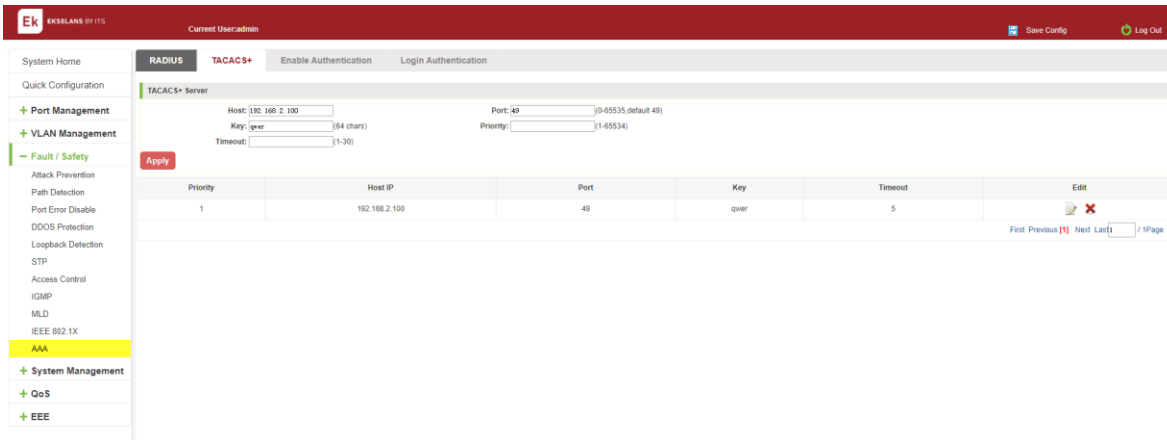


Figure 6-55: configuration TACACS+.

Switch config Method List: Name: SWG24L2, Method 1: TACACS+ Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.

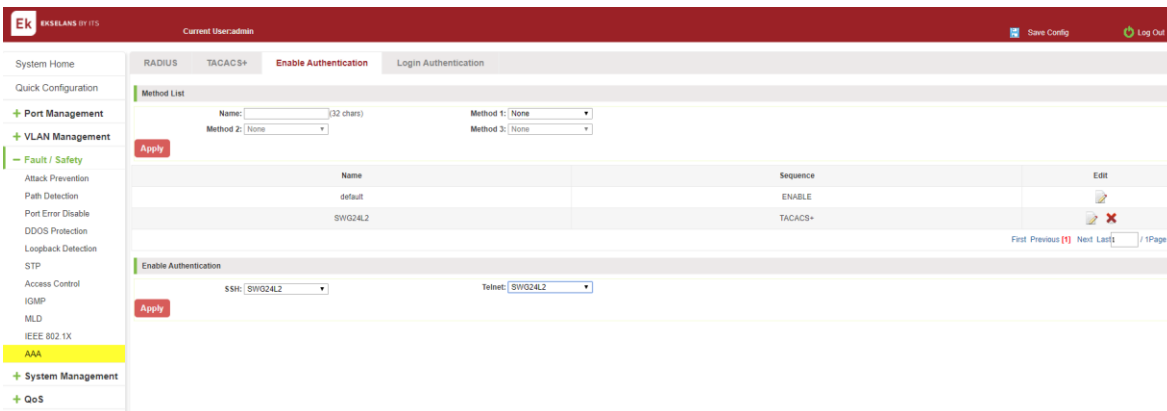


Figure 6-56: configuration enable authentication.

Switch config Method List: Name: SWG24L2, Method 1: TACACS+, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.

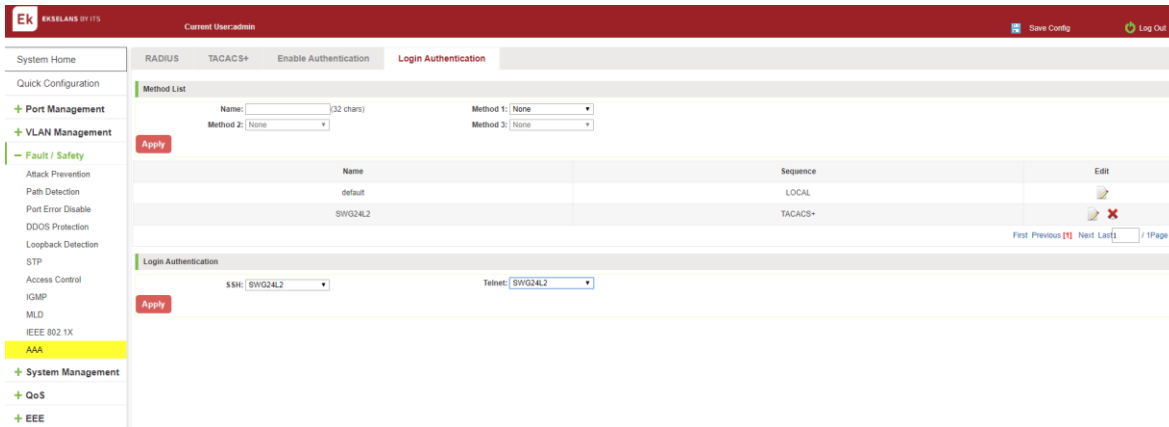


Figure 6-57: configuration login authentication.

You can successfully open AAA TACACS+ function.

PC input right username and password, PC can console, telnet and ssh switch.

PC input right password, user can join "# mode".

System management.

System settings

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:

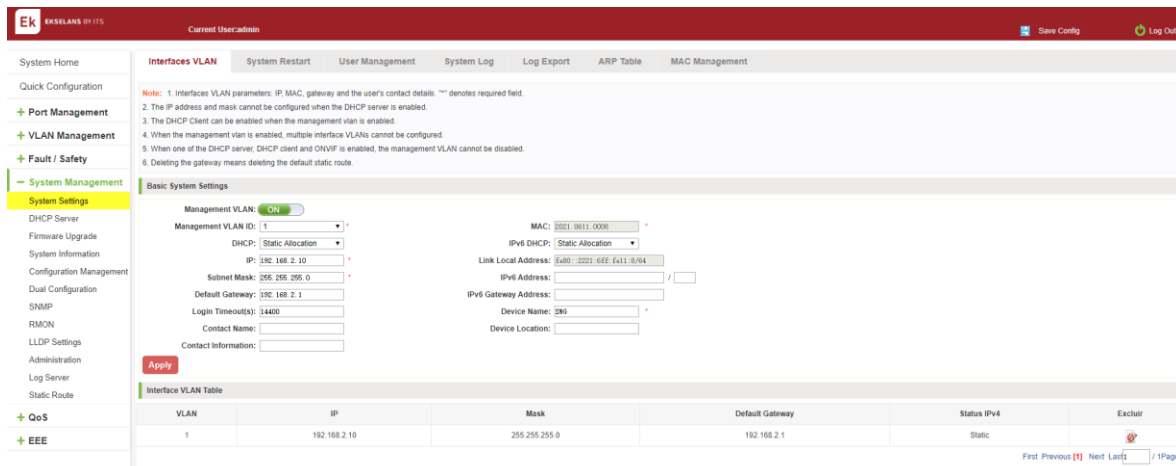


Figure 7-1: basic system settings.

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 192.168.2.10
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 192.168.2.1.
5. In the **Device Location** text box, enter the **Device Location**, such as China.
6. In the **Contact Name** text box, enter the **Contact Name**, such as john.
7. In the **Contact Information** text box, enter **Contact Information**, such as 12345678900.
8. Click on "Apply Settings" button to complete the configuration.

SYSTEM TIME SYNCHRONIZATION.

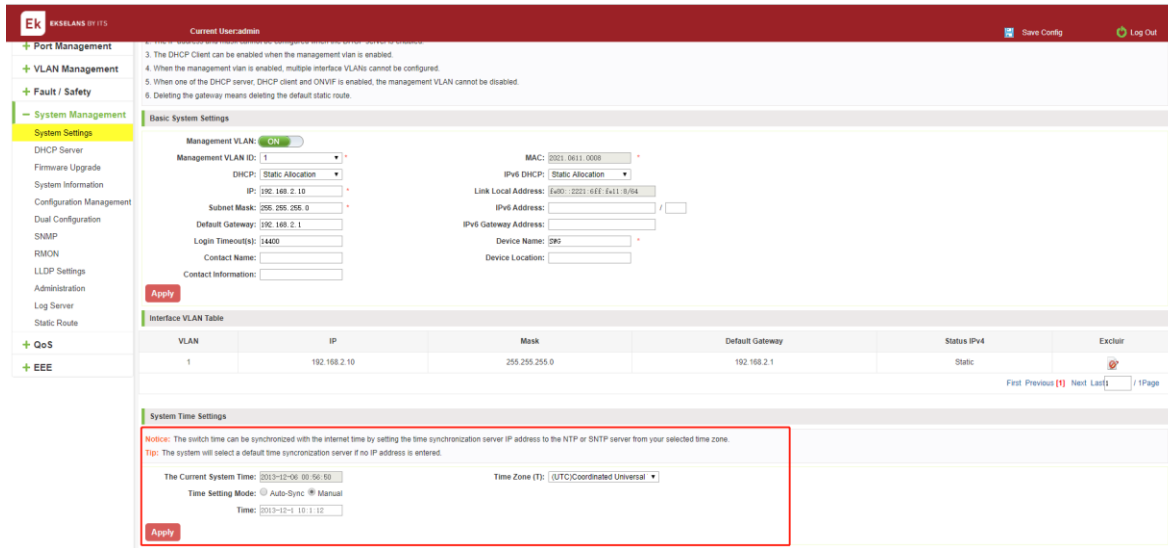


Figure 7-2: System time synchronization.

To configuration system time, You can select NTP or SNTP, enter SNTP/NTP Server IP Address such as 203.117.180.36(local SNTP/NTP servers or internet SNTP/NTP servers), in the Time Zone (T) text box, you can choose any time zone you want, such as UTC+08:00

The user can manually configure the device system time.

System restart.

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

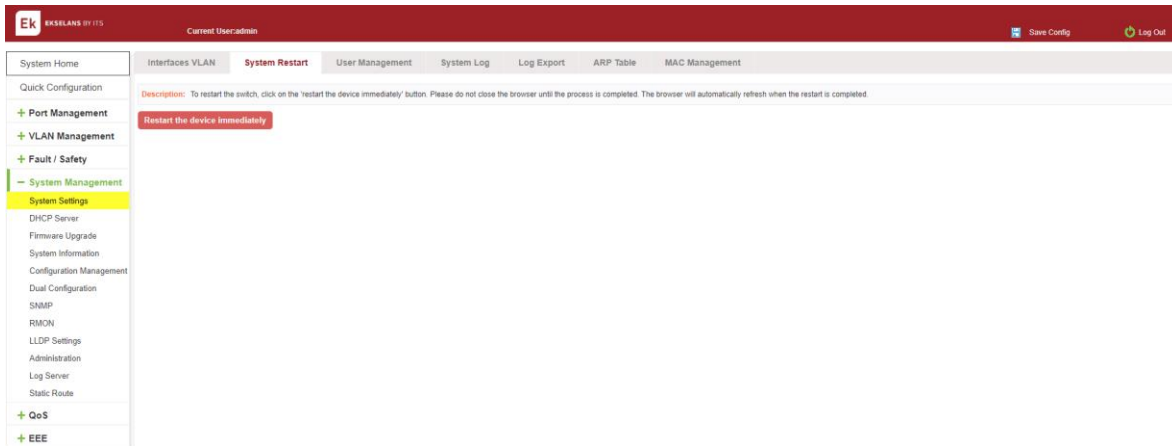


Figure 7-6: System Restart

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 Apply 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.

Change PassWord.

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

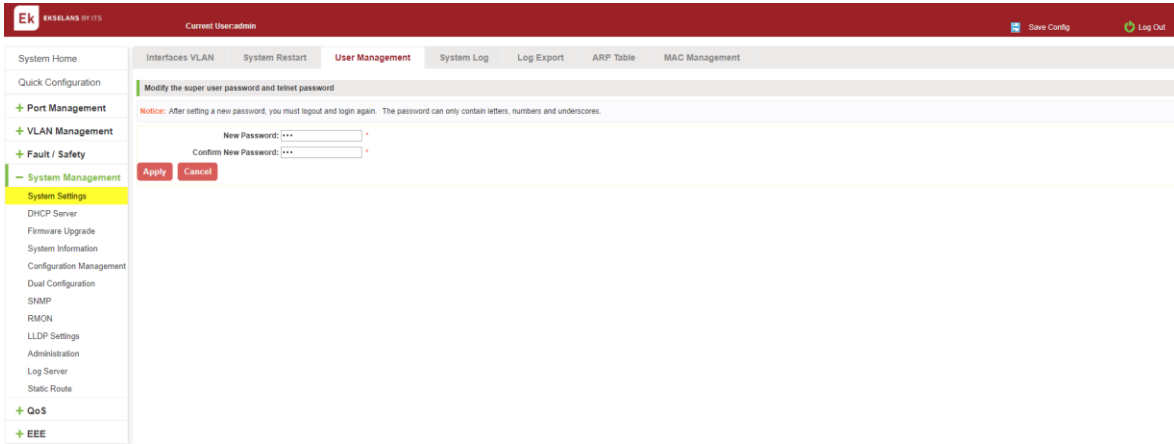


Figure 7-7: change password.

Change password follow these steps:

Step1: Enter the new password: admin.

Step2: Confirm new password: admin.

Step3: Click the "Apply" button.

Step5: Pop-up dialog box, click "OK" button.

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:

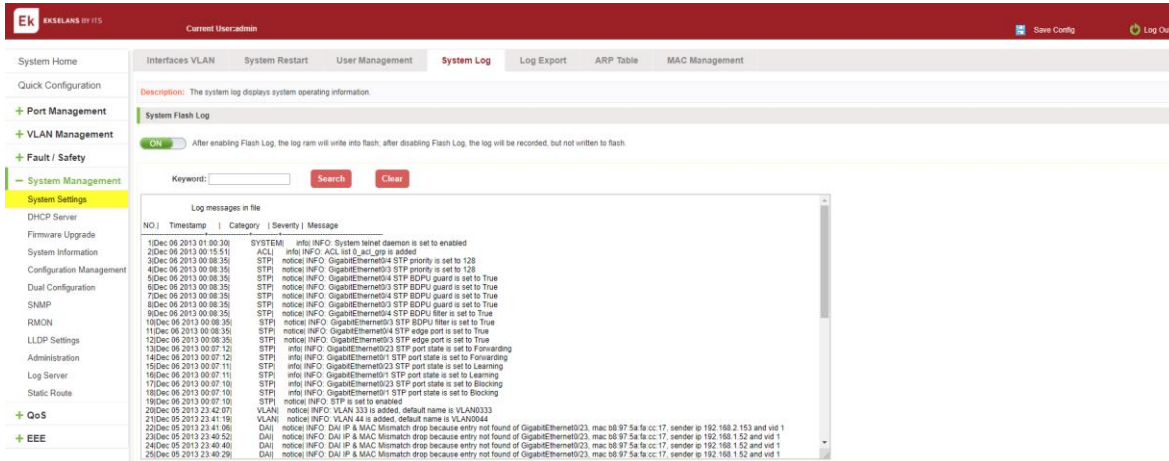


Figure 7-8: system log.

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.

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.

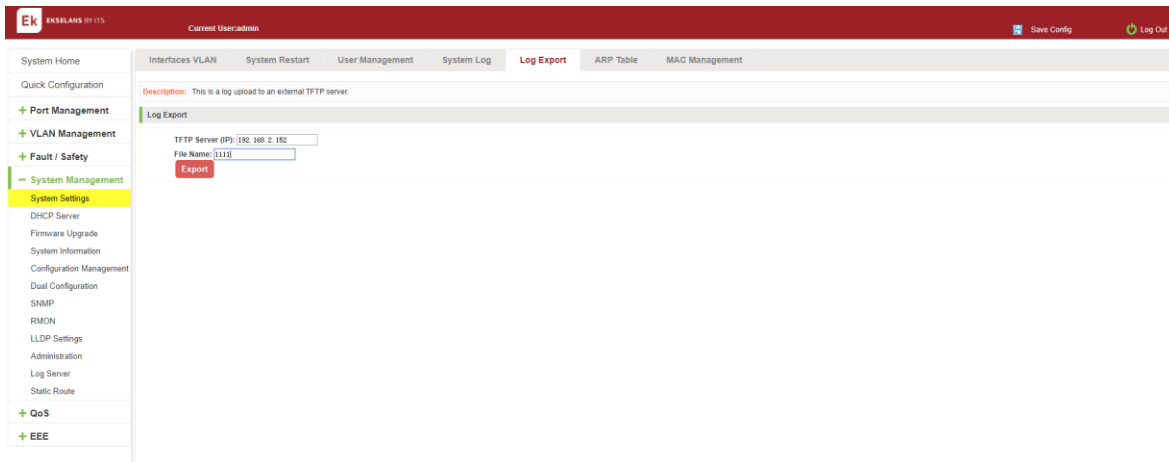


Figure 7-9: Log Export.

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:

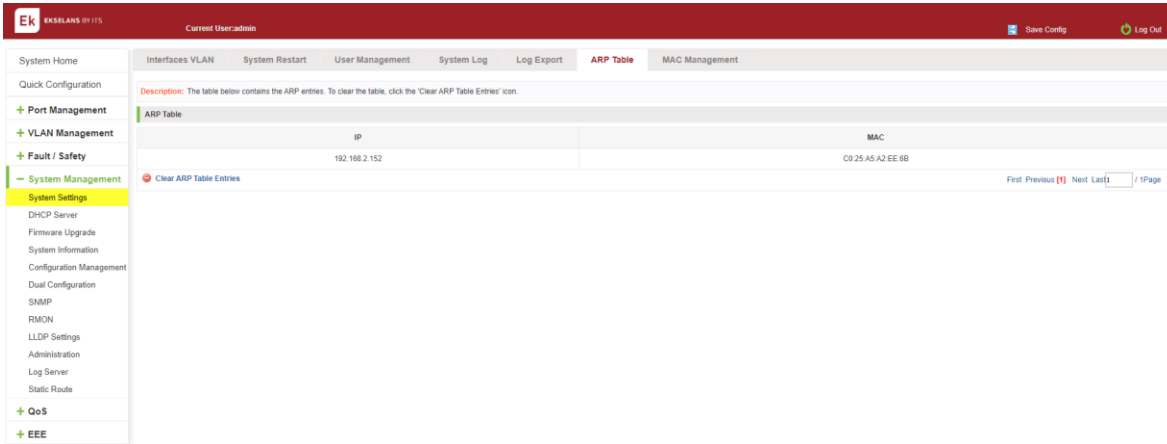


Figure 7-10: ARP message

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

MAC management.

MAC ADDRESS LOOKUP

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

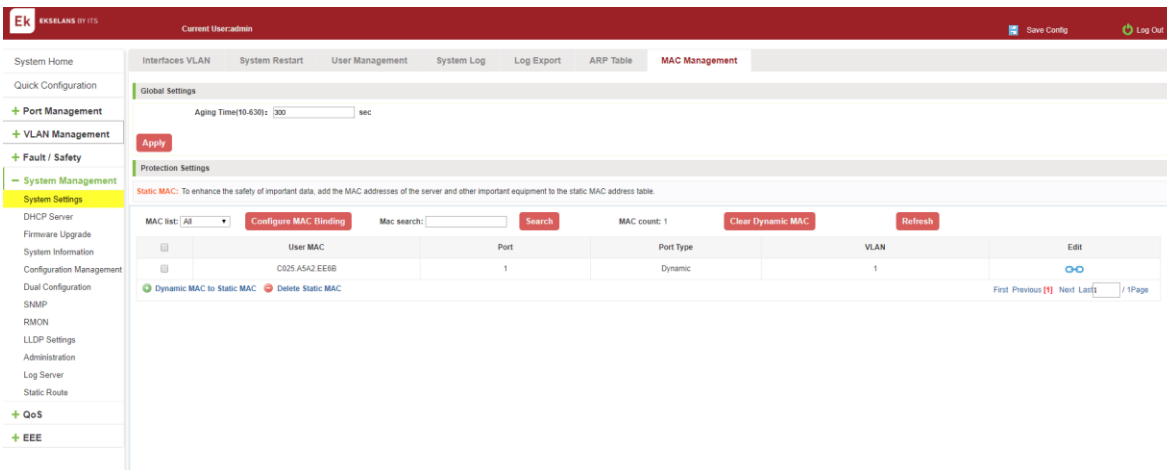


Figure 7-11: MAC address lookup display.

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.

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:

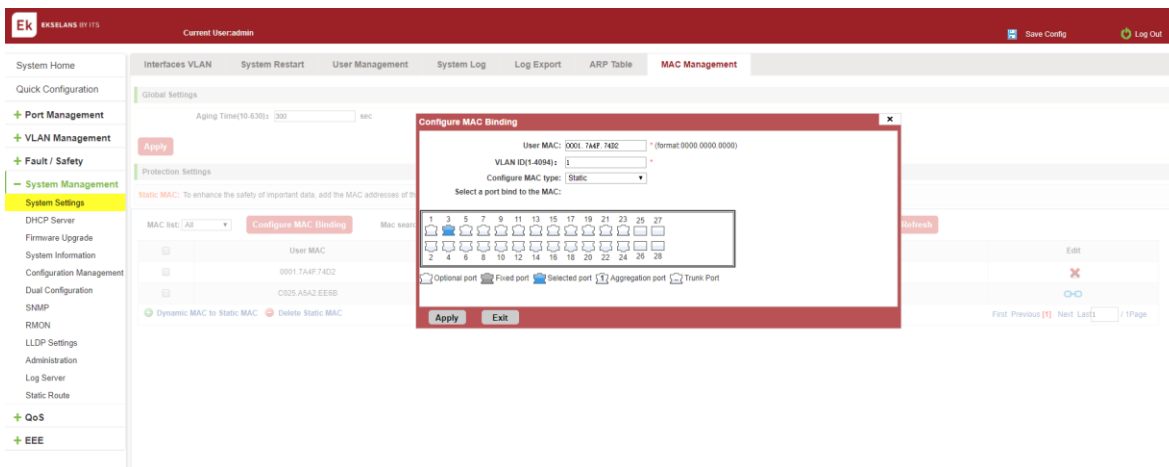



Figure 7-12: MAC addresses statically bound static configuration.

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 "Apply" to complete the configuration.

- 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:

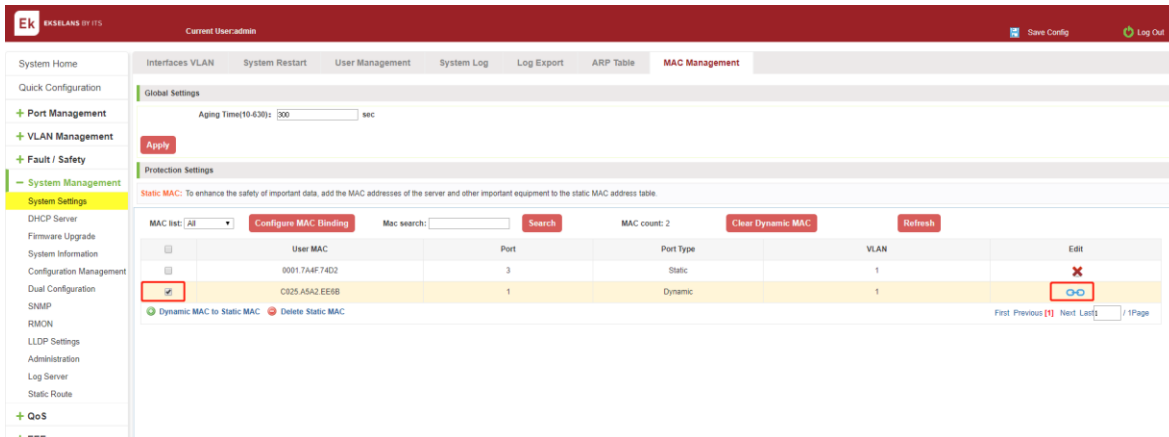


Figure 7-13: MAC address of the static binding configuration.

- 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:

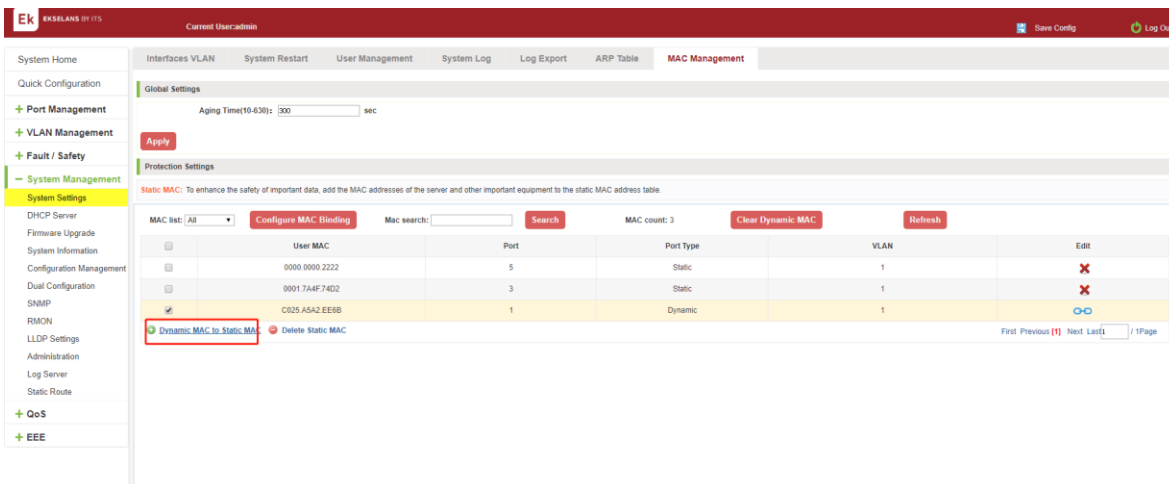


Figure 7-14: Batch-MAC binding configuration.

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:

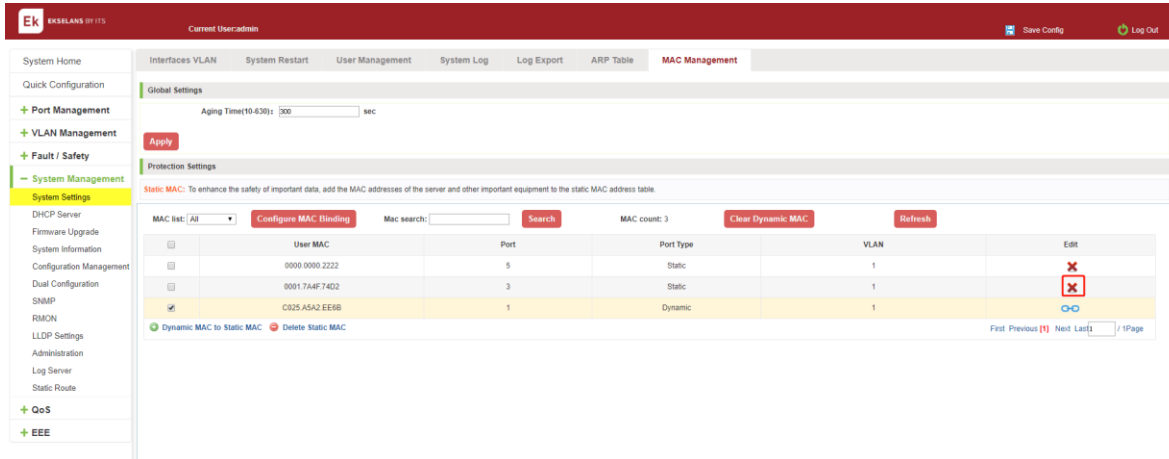


Figure 7-15: MAC address deletion.

Remove MAC address configuration steps are as follows:

Step1: To delete the selected MAC address.

step2: Click " X " button to delete the configuration.

1. 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:

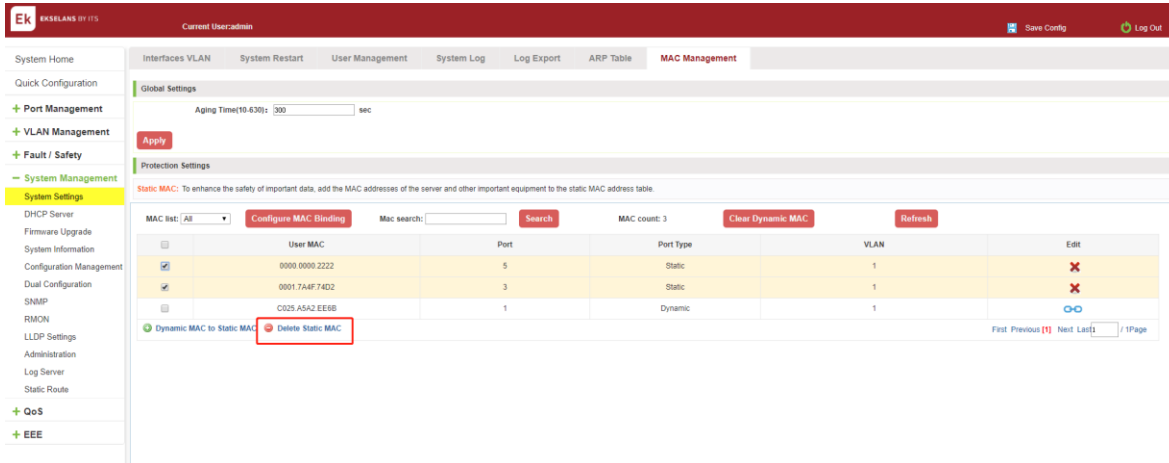


Figure 7-16: MAC address batch deletion deletion.

DHCP server.

Click on the navigation bar "System Management" "DHCP Server" to configure the switch dhcp server:

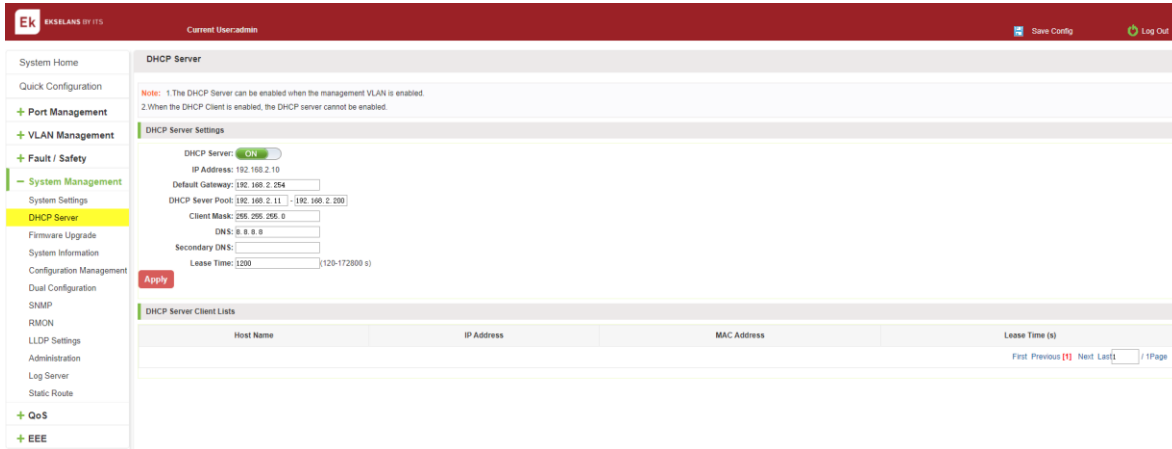


Figure 7-5: DHCP server.

DHCP server configuration, follow these steps:

Step1: In the DHCP server, choose to enable.

Step2: In the DHCP client range, configure the server IP.

Firmware Upgrade.

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

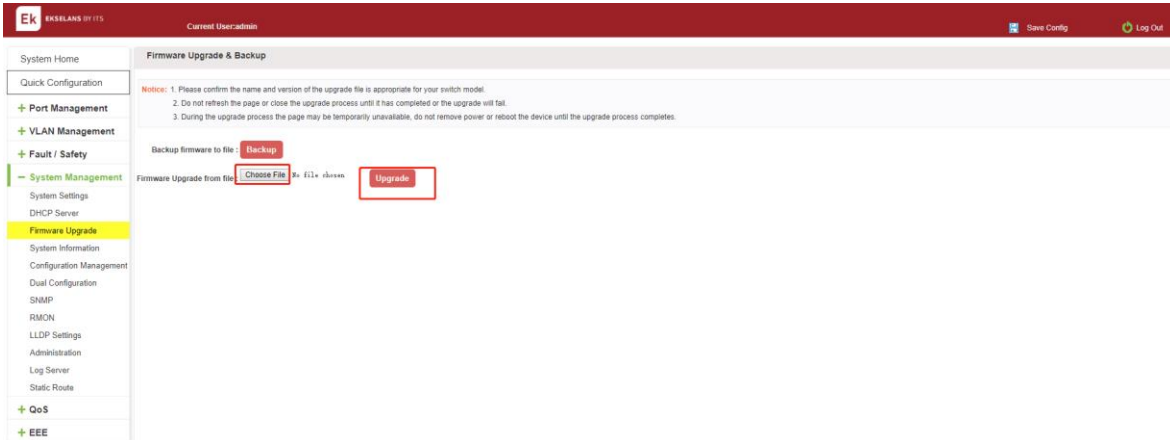


Figure 7-17: Switch System Upgrade.

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.

System information.

Memory information.

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

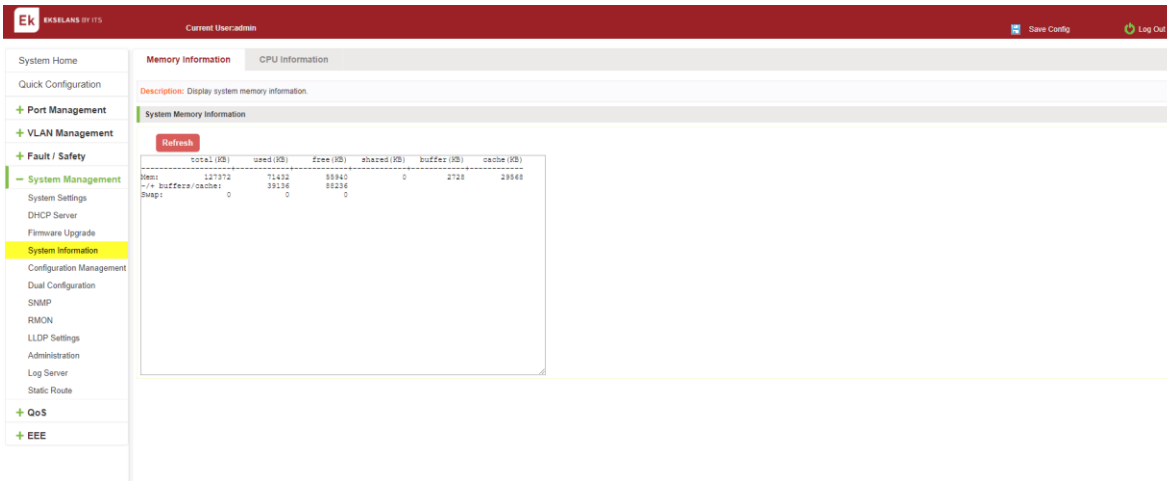


Figure 7-18: System memory information.

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.

CPU INFORMATION.

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

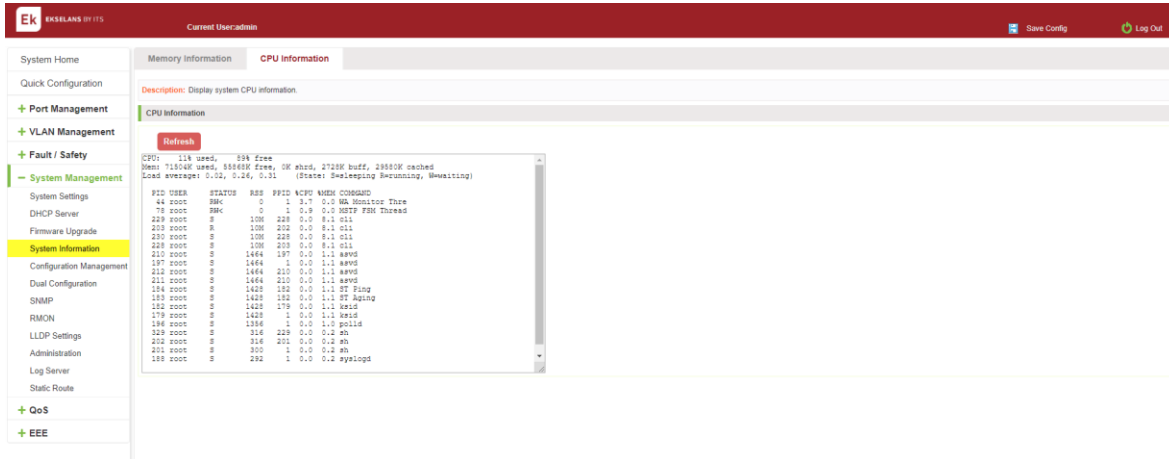


Figure 7-19: CPU information.

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.

Configuration management.

Configuration management.

To see the current configuration.

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

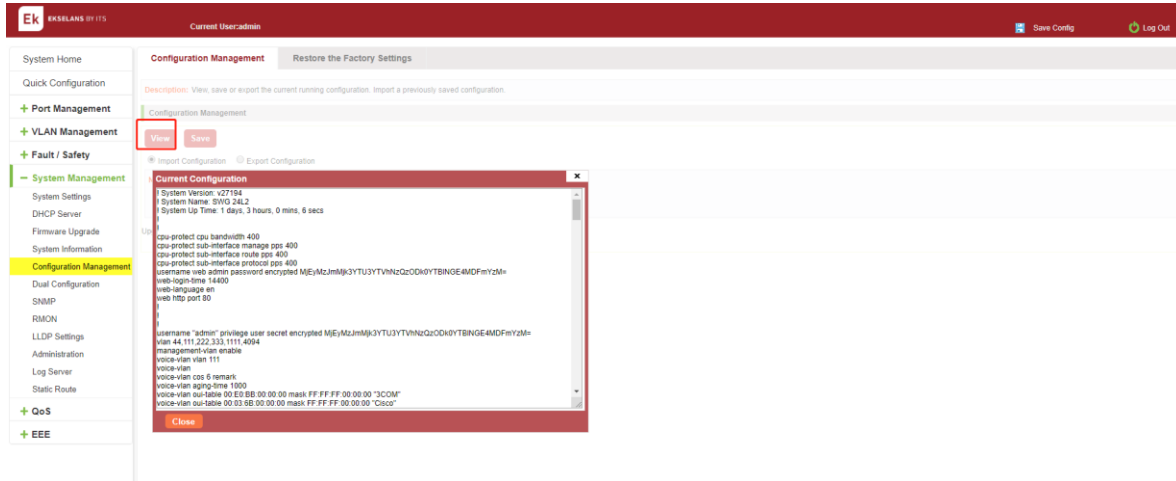


Figure 7-20: View the current configuration.

Apply the current configuration.

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

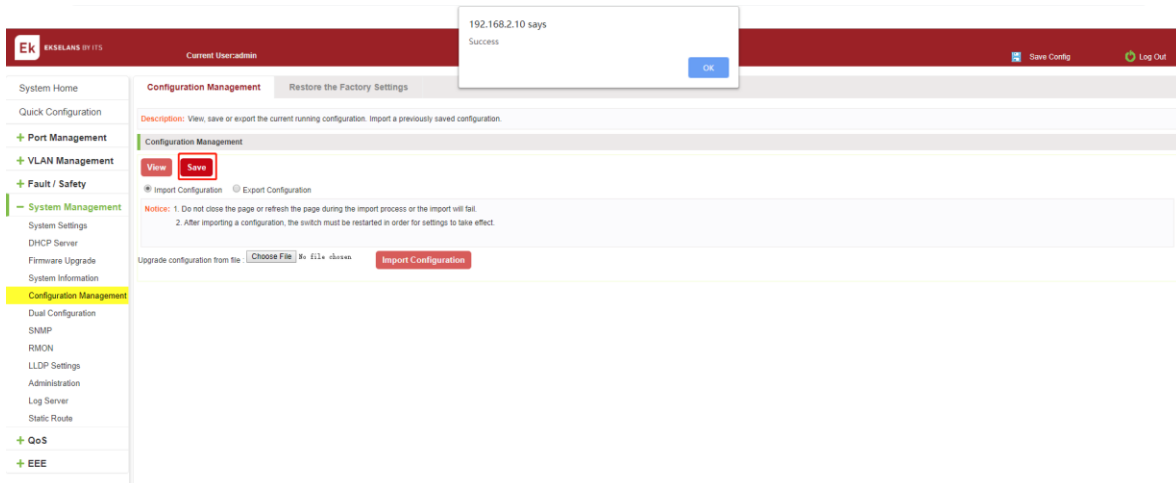


Figure 7-21: To Apply the current configuration.

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:

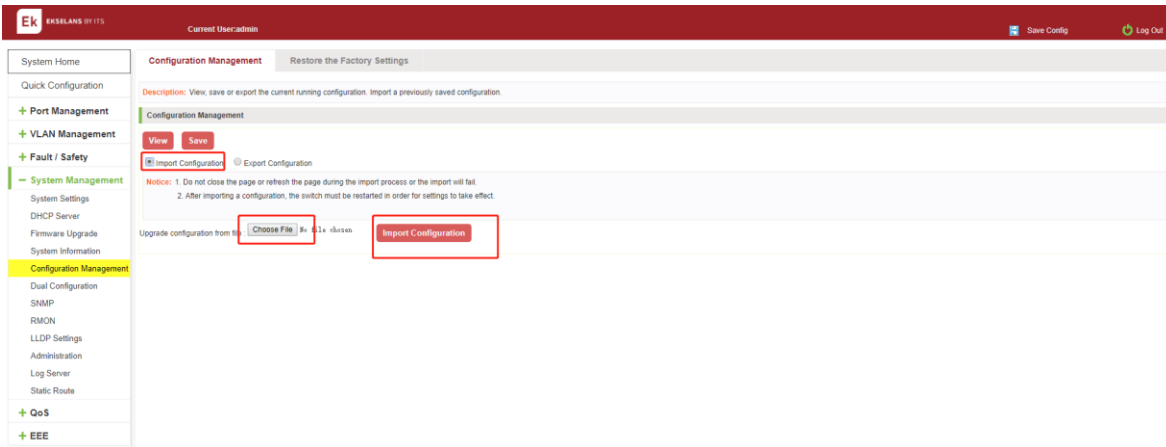


Figure 7-22: Imported configuration.

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.

Export configuration.

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

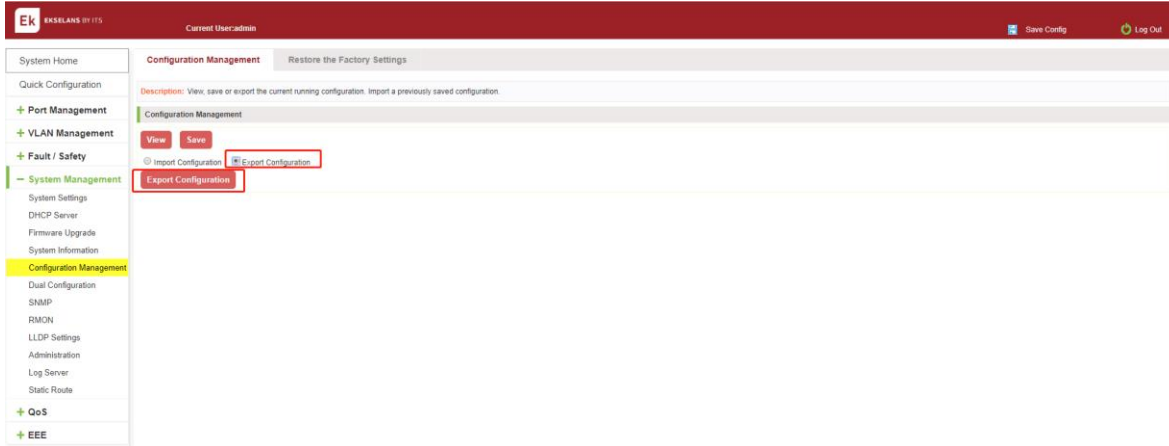


Figure 7-23: Export configuration.

Restore factory Settings.

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

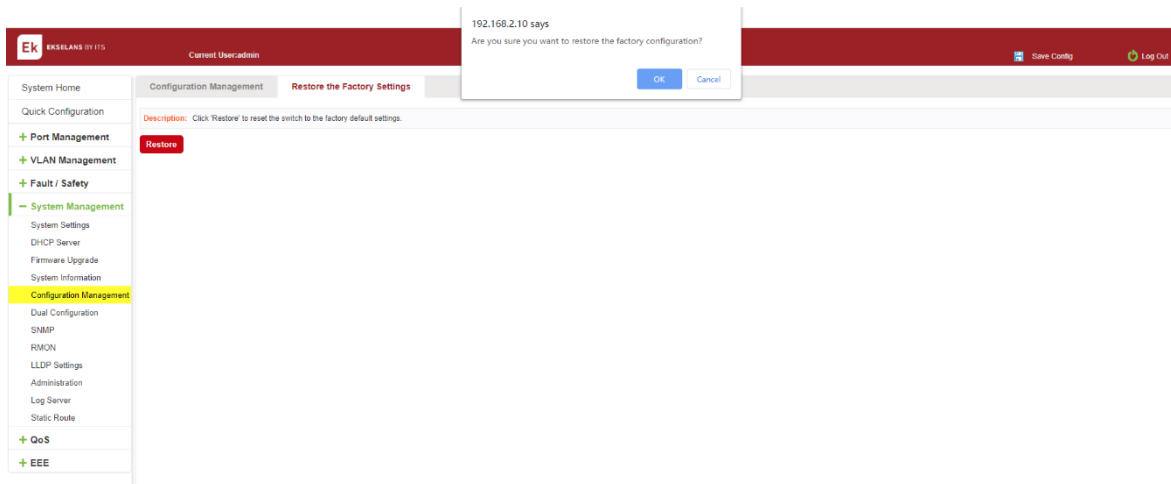


Figure 7-24: Restore factory Settings.

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.

Dual Configuration.

BACK UP AND RESTORE THE CURRENT CONFIGURATION FILE.

1. Click on "System Management" "Dual Configuration".

| File Name | File Type | Start-Up | Modify Time | Size (bytes) |
|----------------|-----------|----------|---------------------|--------------|
| default-config | Config | N | 2013-12-05 00:00:49 | 2915 |
| startup-config | Config | Y | 2013-12-06 03:01:26 | 5267 |

2. Configure some functions, such as: IP address, port speed limit, port mirroring and other functions.

The screenshot shows the 'Port Speed Limit' configuration page. The left sidebar contains a navigation menu with 'Port Speed Limit' highlighted. The main content area includes a description, a notice, and a 'Select a port to configure' section with a grid of 28 ports. Below this are sliders for 'Input Speed Limit' (set to 714.304Mbit/s) and 'Output Speed Limit' (set to 615.752Mbit/s). At the bottom, there is a 'Port Speed Limit List' table.

| Port | Input Speed Limit | Output Speed Limit | Edit |
|------|-------------------|--------------------|------|
| 1 | MAX | MAX | |
| 2 | MAX | MAX | |
| 3 | 714.304Mbit/s | 615.752Mbit/s | |
| 4 | MAX | MAX | |
| 5 | MAX | MAX | |
| 6 | MAX | MAX | |
| 7 | MAX | MAX | |

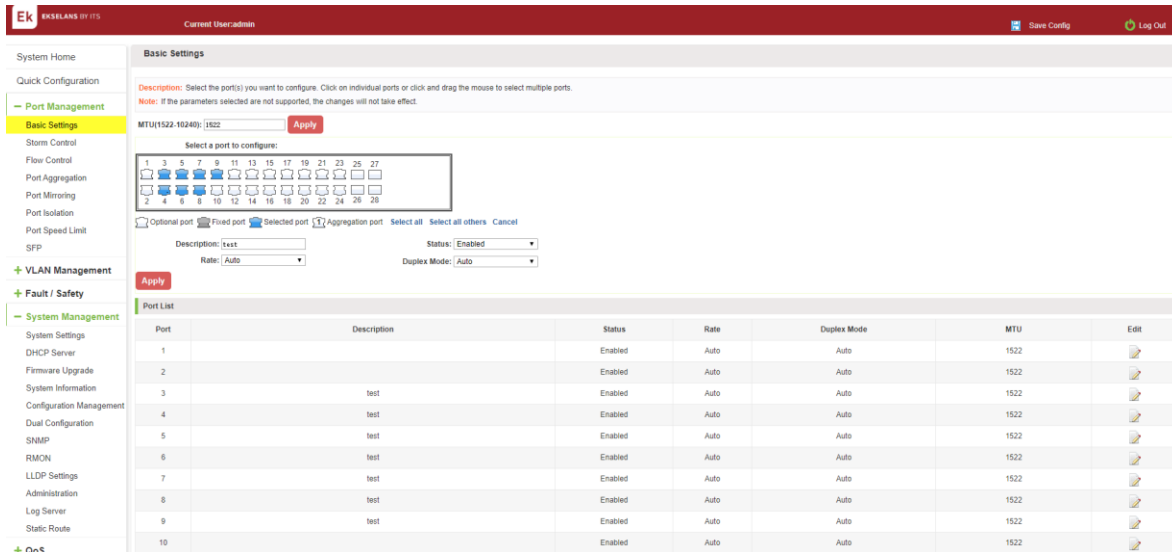
The screenshot shows the 'Port Mirroring' configuration page. The left sidebar has 'Port Mirroring' highlighted. The main content area includes a description, a note, and two sections for selecting source and destination ports. Below these are 'Apply' and 'Refresh' buttons, and a 'Mirroring Group' dropdown menu. At the bottom, there is a 'Mirroring Port List' table.

| Mirroring Group | Source Port | Destination Port | Edit |
|-----------------|-------------|------------------|------|
| 1 | 7 | 8 | |

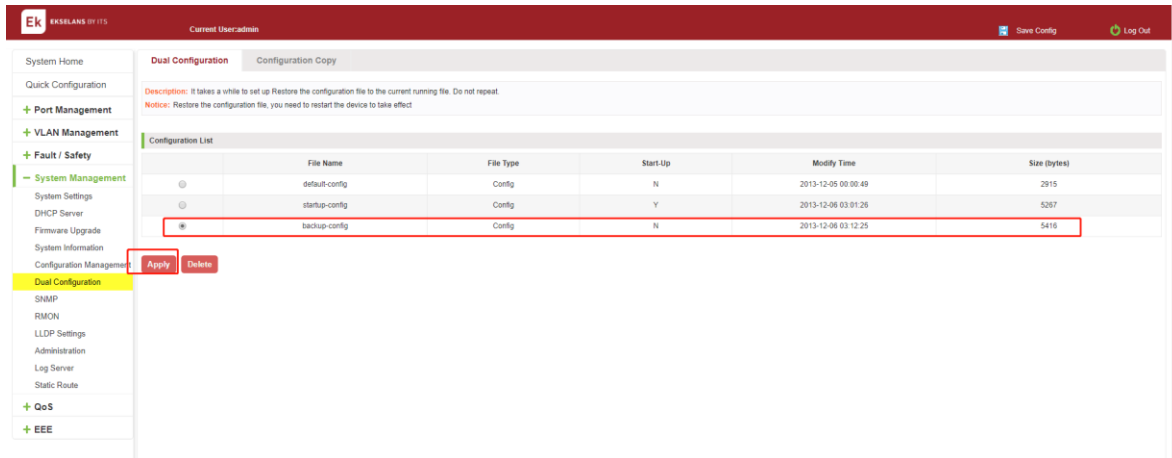
- Click on the "System Management" "Dual configuration" To configure the switch Back up the current running profile.

The screenshot shows the 'Dual Configuration' page. The left sidebar has 'Dual Configuration' highlighted. The main content area shows a 'Configuration Copy' section with a 'Copy Type' dropdown set to 'Running-Config' and a 'File Name' dropdown set to 'backup-config'. An 'Apply' button is visible below these options.

4. Based on step 1, add or remove the function configuration. such as: port description.



5. Click on the "Dual configuration" and restore the configuration file to the current running file.



The switch should restore the configuration to the current running file for the previous backup (Restore to the configuration of step 4).

BACK UP AND RESTORE THE STARTUP CONFIGURATION FILE.

1. Configure some functions, such as MAC: IP address, port speed limit, port mirroring and other functions.

The screenshot shows the 'Basic System Settings' page. The 'Management VLAN' is set to 'ON'. The 'Management VLAN ID' is 1. The DHCP is set to 'Static Allocation'. The IP is 192.168.2.100, and the Subnet Mask is 255.255.255.0. The Default Gateway is 192.168.2.129. The Login Timeout(s) is 14400. The Contact Name and Contact Information fields are empty. The MAC is 0021.0011.0009. The IPv6 DHCP is set to 'Static Allocation'. The Link Local Address is fe80::221:6ff:fa11:8/64. The IPv6 Address and IPv6 Gateway Address fields are empty. The Device Name is SWG and the Device Location is empty. An 'Apply' button is visible at the bottom left.

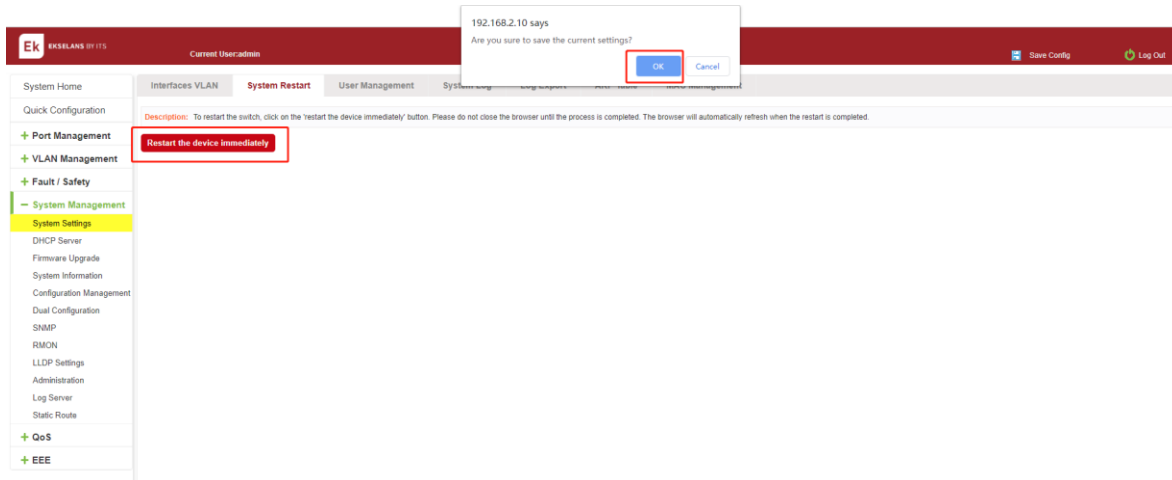
The screenshot shows the 'Port Speed Limit' page. The description states: 'Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.' The notice says: '1000Kbps = 1Mbps'. A grid of 28 port icons is shown, with ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, and 27 selected. Below the grid, there are sliders for 'Input Speed Limit' (set to 714.304Mbps) and 'Output Speed Limit' (set to 616.752Mbps). A 'Port Speed Limit List' table is shown below:

| Port | Input Speed Limit | Output Speed Limit | Edit |
|------|-------------------|--------------------|--------|
| 1 | MAX | MAX | [Edit] |
| 2 | MAX | MAX | [Edit] |
| 3 | 714.304Mbps | 616.752Mbps | [Edit] |
| 4 | MAX | MAX | [Edit] |
| 5 | MAX | MAX | [Edit] |
| 6 | MAX | MAX | [Edit] |
| 7 | MAX | MAX | [Edit] |

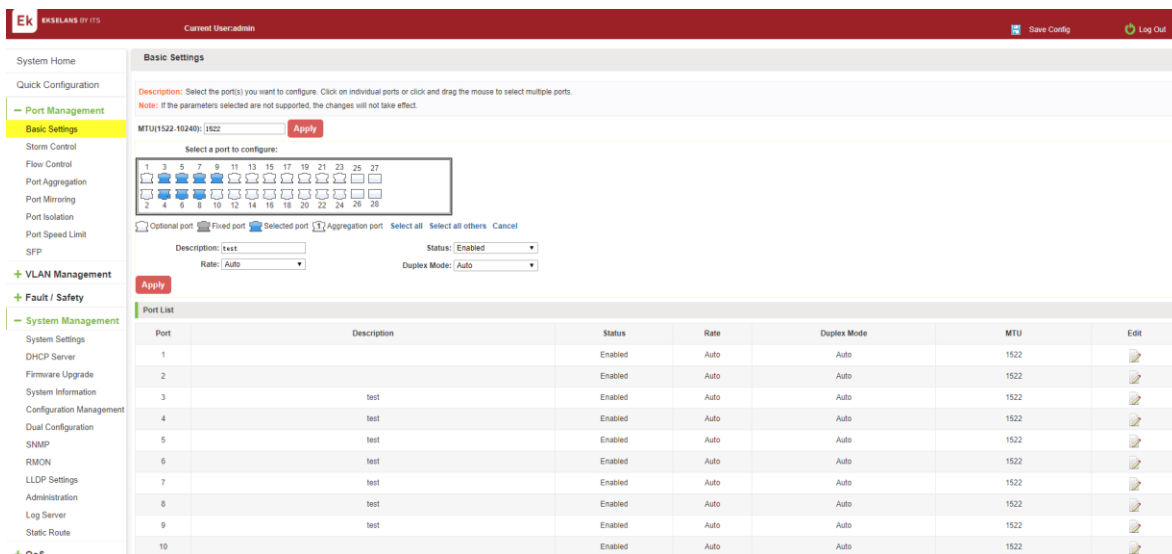
The screenshot shows the 'Port Mirroring' page. The description states: 'Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.' The note says: 'A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.' A grid of 28 port icons is shown, with ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, and 27 selected. Below the grid, there are sliders for 'Input Speed Limit' (set to 714.304Mbps) and 'Output Speed Limit' (set to 616.752Mbps). A 'Mirroring Group' dropdown is set to 'Not Selected'. A 'Mirroring Port List' table is shown below:

| Mirroring Group | Source Port | Destination Port | Edit |
|-----------------|-------------|------------------|--------|
| 1 | 7 | 8 | [Edit] |

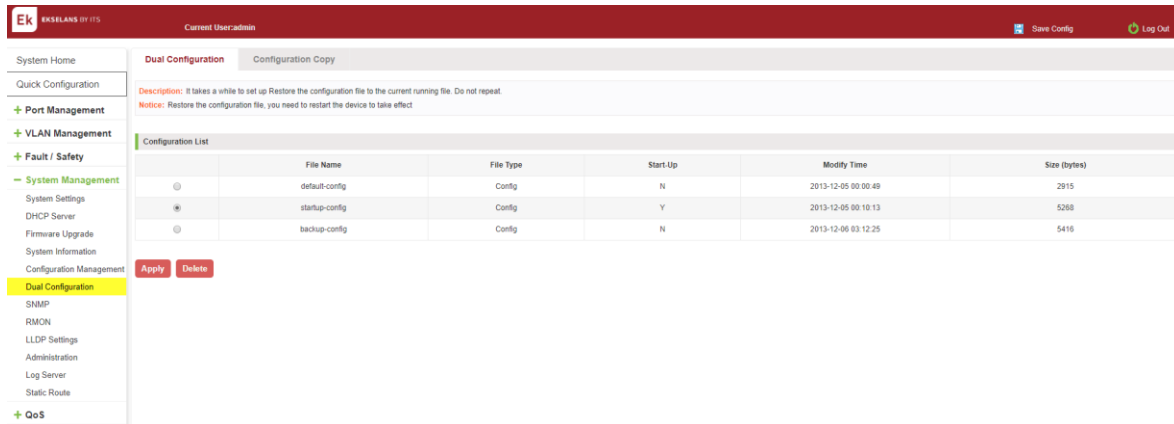
2. Apply the current configuration (You can use GUI settings, or you can use CLI commands).



3. On the basis of step 1, add or remove the function configuration. Such as: port description.



- Click on the "Dual configuration" click the "Restore the configuration file to the start-up file".



- Reboot the device

SNMP.

Check the SNMP.

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

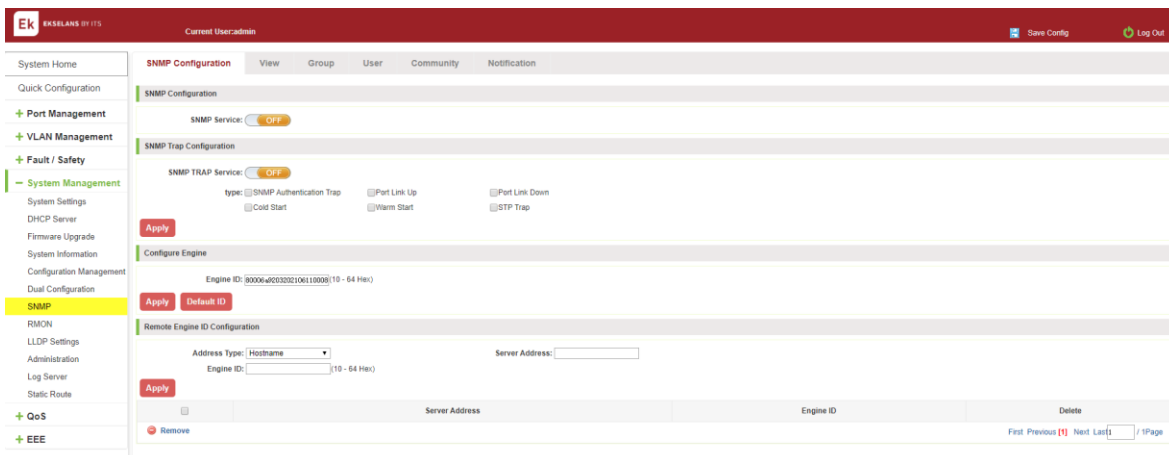


Figure 7-25: View the SNMP configuration information.

By default, SNMP is not open.

SNMP monitoring software and switches the SNMP version is consistent, if inconsistencies can lead to communication failure.

Activate the SNMP.

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

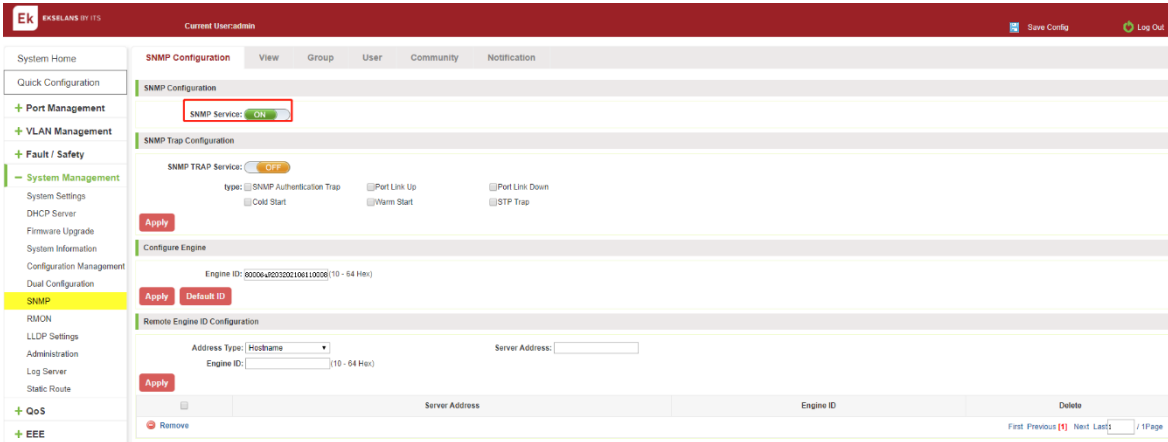


Figure 7-26: Activation SNMP function.

Activation function SNMP configuration steps are as follows:

Step1: Choose open SNMP options.

Step2: Click "OK" button to complete the configuration.

To disable the SNMP.

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

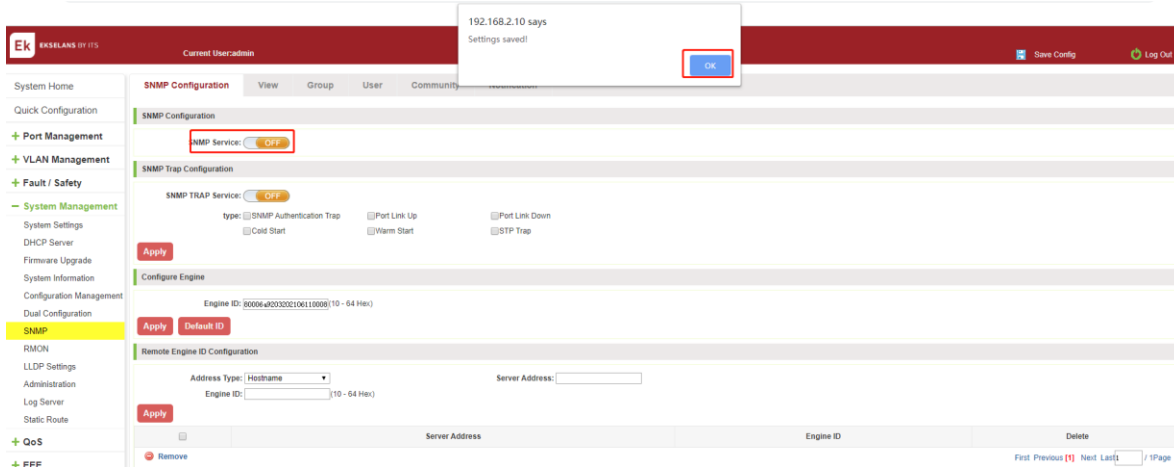


Figure 7-27: Disable the SNMP function.

Disable the SNMP function configuration steps are as follows:

Step1: Choose close SNMP options.

Step2: Click "OK" button to complete the configuration.

Activate the TRAP.

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

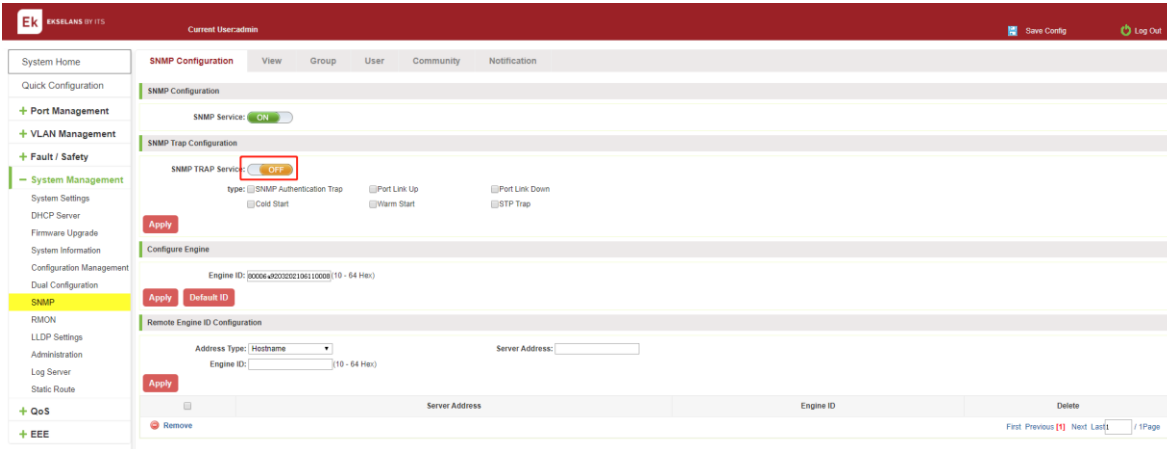


Figure 7-28: Activation function of the TRAP.

Activate the TRAP function configuration steps are as follows:

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

Disable the TRAP.

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

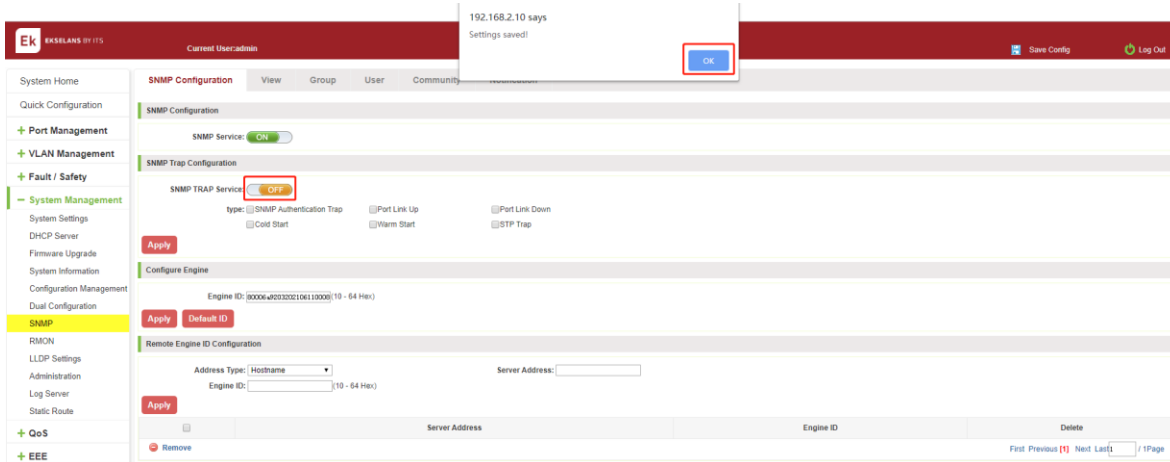


Figure 7-29: Disable TRAP function.

Disable the TRAP function configuration steps are as follows:

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

Step2: Click "OK" button to complete the configuration.

CHANGE community.

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

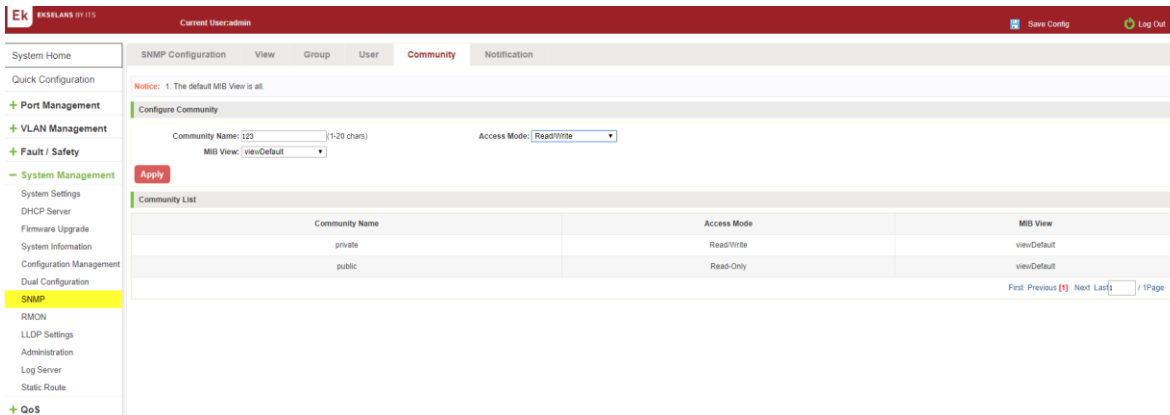


Figure 7-30: Change community.

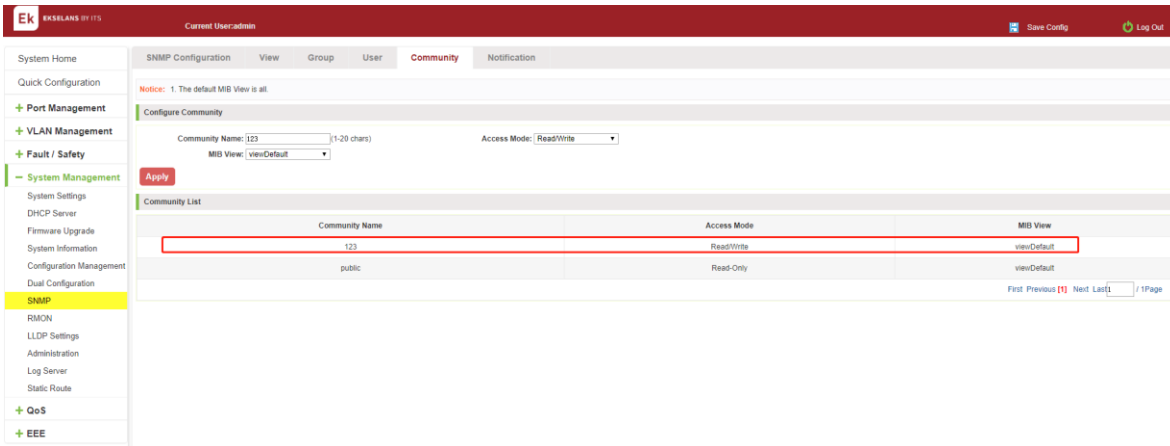


Figure 7-31: Community results.

Change community configuration steps are as follows:

Step1: In the community's name dialog box input: the 123.

Step2: Select "Read/Write" permissions.

Step3: Click on "Apply" button, complete the configuration.

Added the SNMP TRAP service host.

Click on the "System Management" "SNMP" "Notification", in the host IP text box input: 192.168.2.150, TRAP community name: 123, SNMP version choice: v1, click the "Apply" button, complete the configuration:

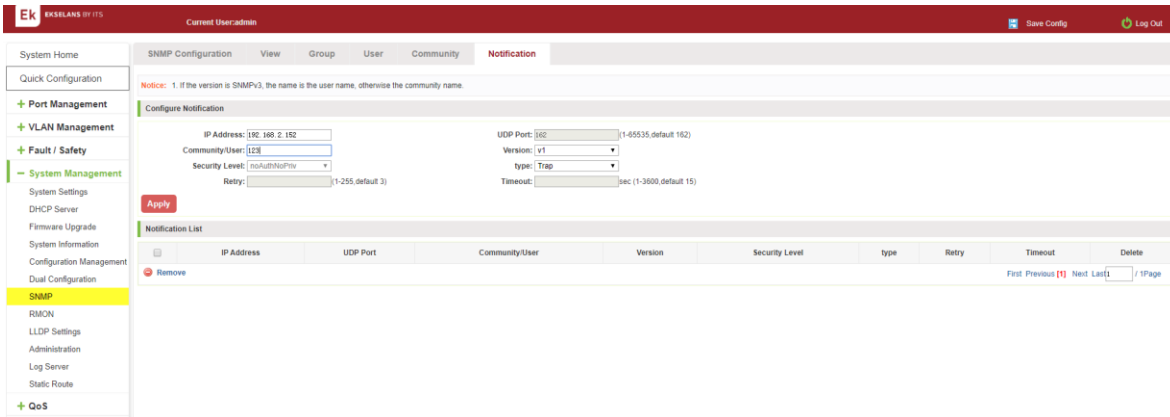


Figure 7-32: Increases the SNMP TRAP service host.




Figure 7-33: SNMP TRAP service host.

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

- Step1: In the host IP dialog box input: 192.168.2.150.
- Step2: In TRAP community name dialog input: 123.
- Step3: Select the SNMP version: v1.
- Step4: Click on "Apply" button, complete the configuration.

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

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:

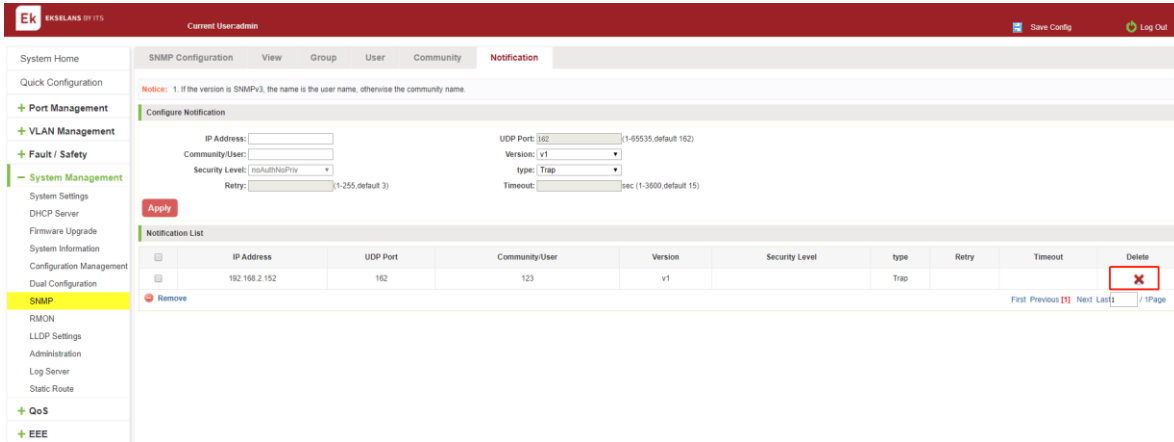


Figure 7-34: Delete community.

RMON.

View ROMN configure information.

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

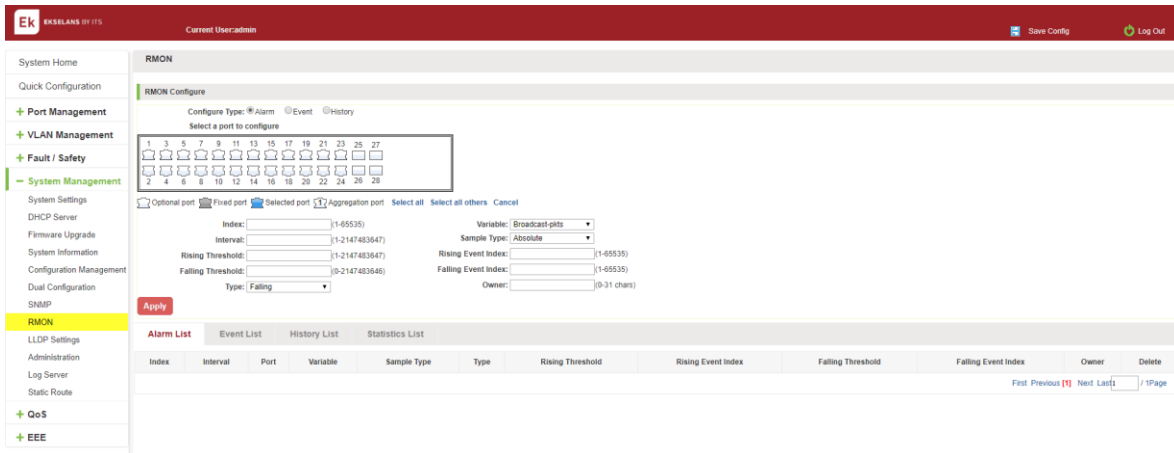


Figure 7-35: View RMON configure information.

Configure ROMN type.

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

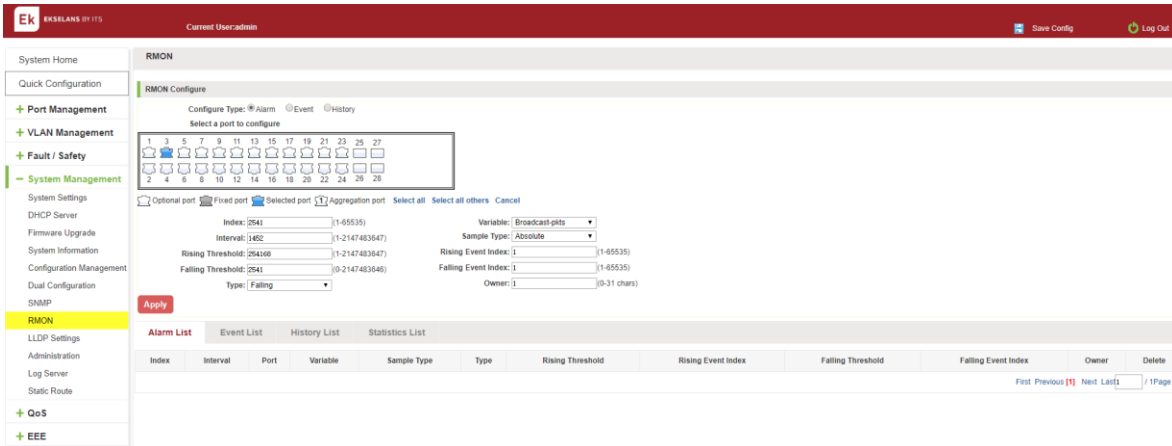


Figure 7-36: configure ROMN type.

Notice: Parameters There are some special rules in the configuration. The EVENT should be created first. Please note the prompts in the configuration. ex: Rising Threshold is greater than Falling Threshold.

Change ROMN type.

On the ROMN configure page, click the type "Event" or "History" and setting parameters. Be careful the parameter of Community should be exit in SNMP Community name. Configure ok after clicking "Apply".

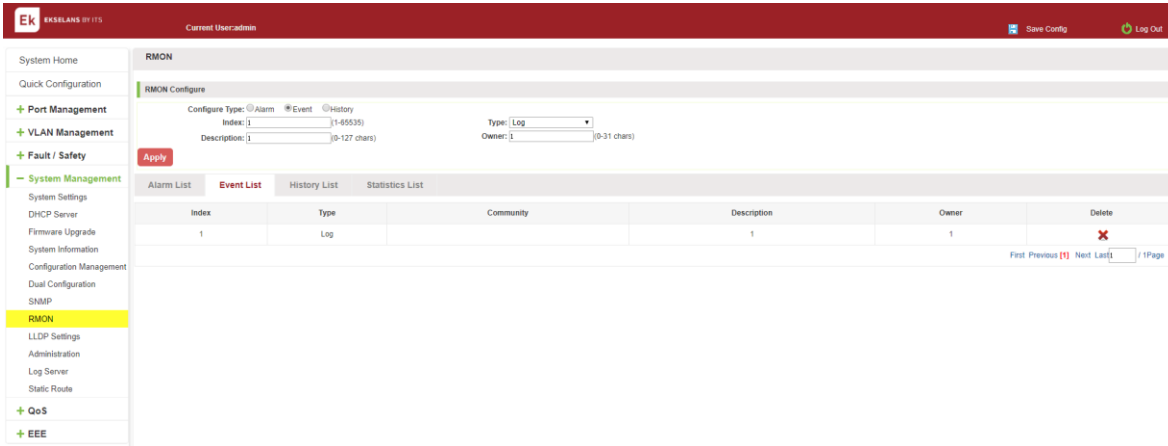


Figure 7-37 Change ROMN type is Event.

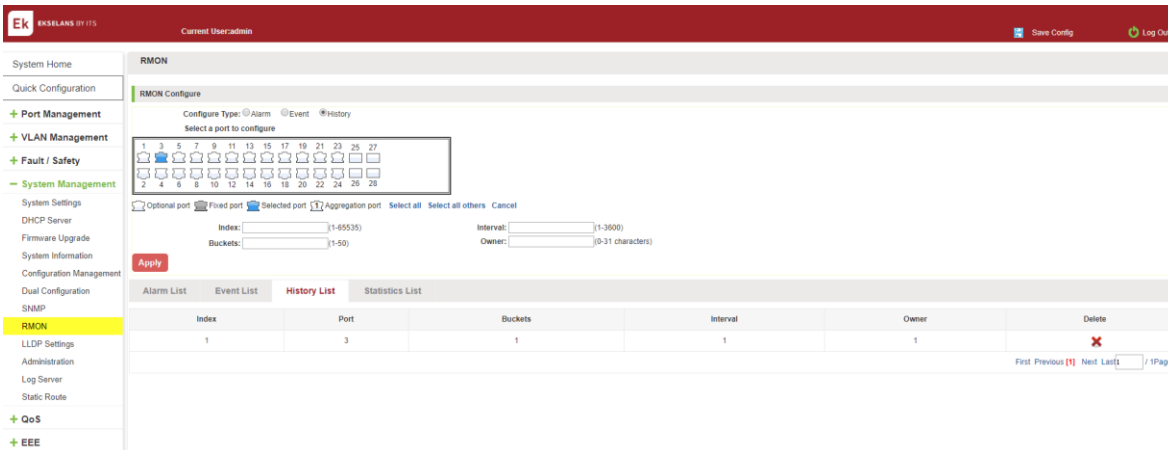


Figure 7-38: Change ROMN type is History.

When the parameters configure is ok, click the [Statistics List](#) .We can choose the port to view the information.

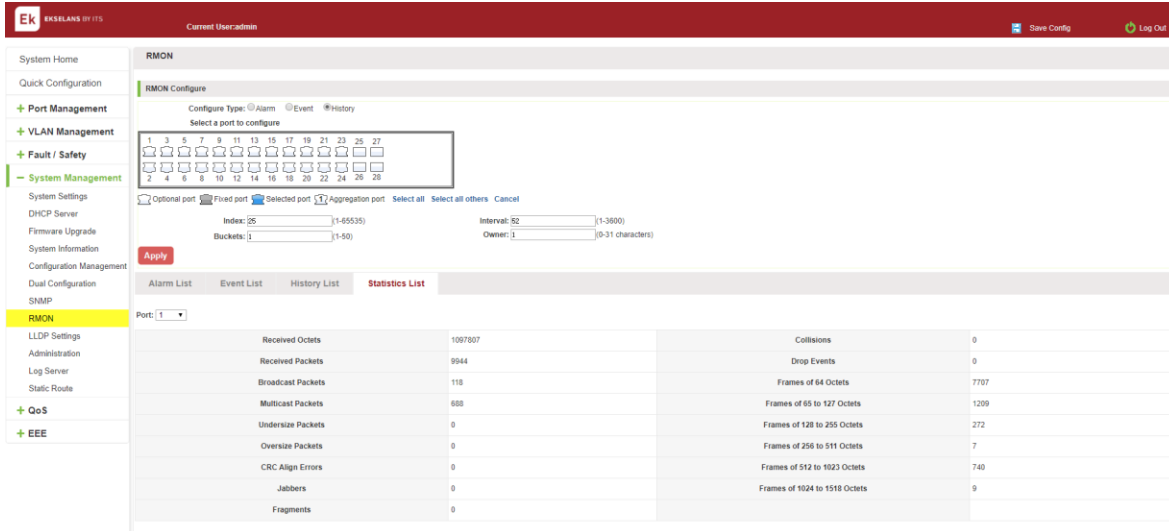


Figure 7-39: View the port configure information.

Delete the configured rule.

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



Figure 7-40: Delete the Alarm list rule.

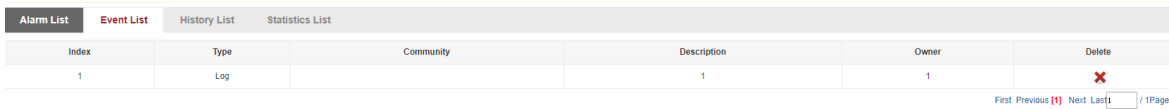


Figure 7-41: Delete the Event list rule.

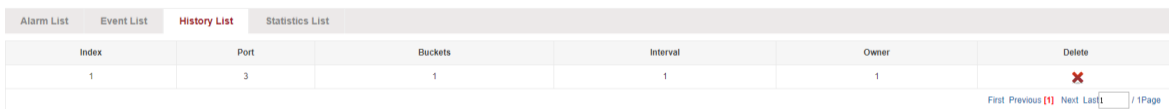


Figure 7-42: Delete the History list rule.

LLDP Settings.

LLDP settings.

Click on the "System Management" "LLDP Settings", "LLDP Settings" can view the lldp settings information. The default mode is Global settings, and this feature is turned off by default.

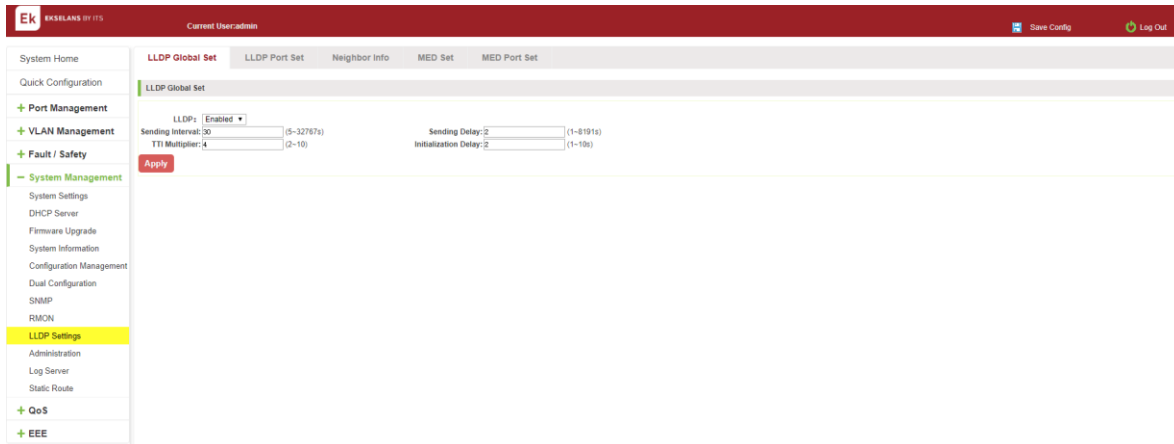


Figure 7-43: view LLDP settings information.

ENABLE LLDP SETTINGS.

Click the drop-down menu to select enable and configuration parameters. Finally click "Apply" button.

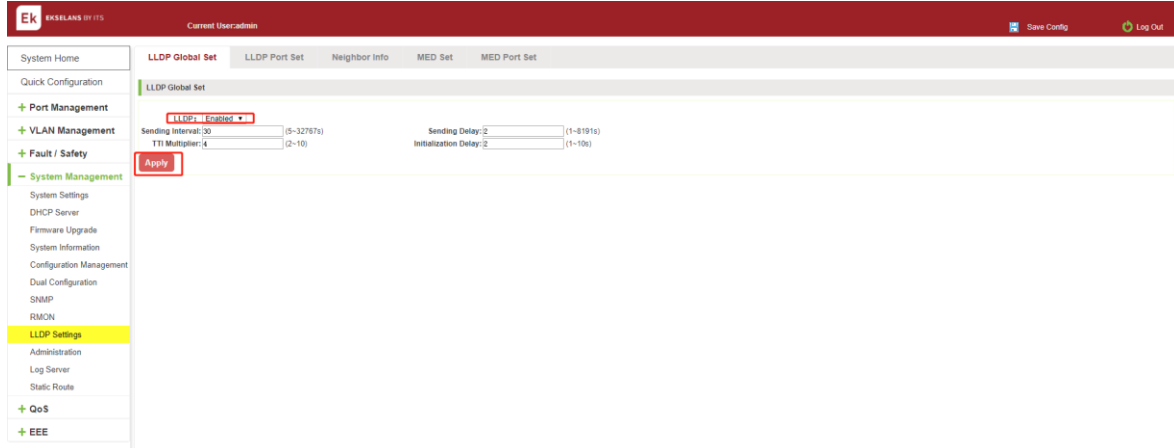


Figure 7-44: Enable LLDP settings.

NEIGHBOR INFO.

When the LLDP function is enabled, the neighbour information is recorded when a neighbour device is found.

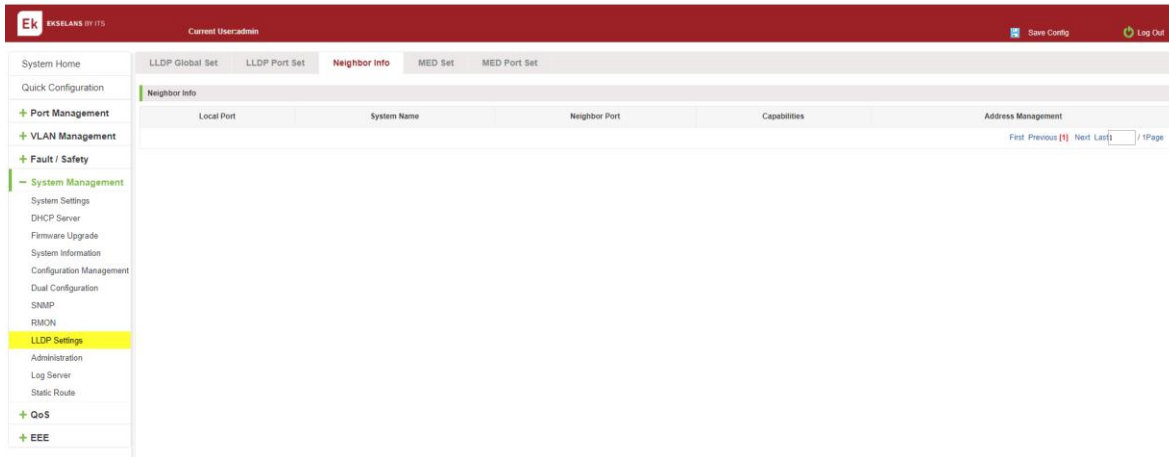


Figure 7-45: Neighbour Info.

Administration.

TELNET.

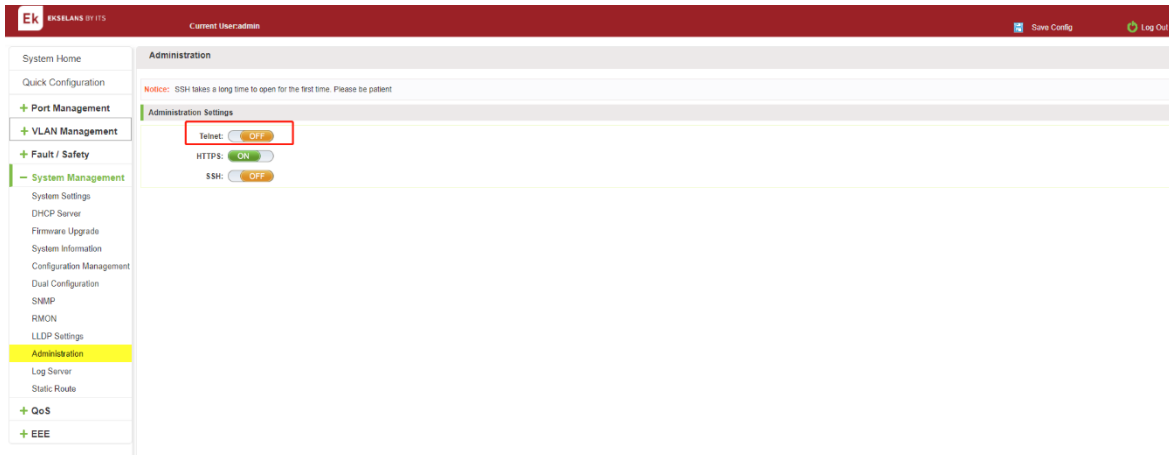


Figure 7-3: telnet.

After you turn on telnet, you can telnet the device to manage the device.

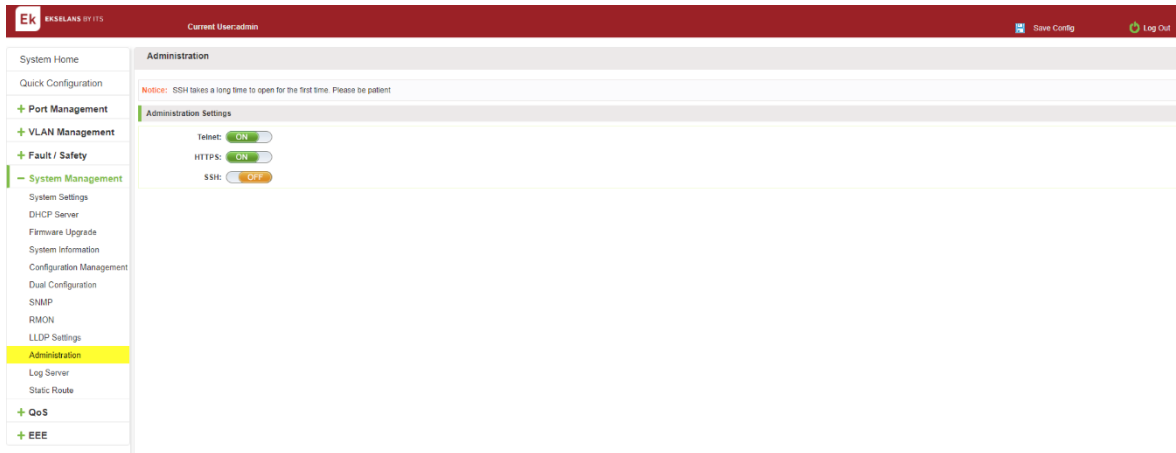


Figure 7-4: enable telnet.

Static Route.

Click on the "System Management" "Static Route"

Step1, Turn off switch management VLAN.

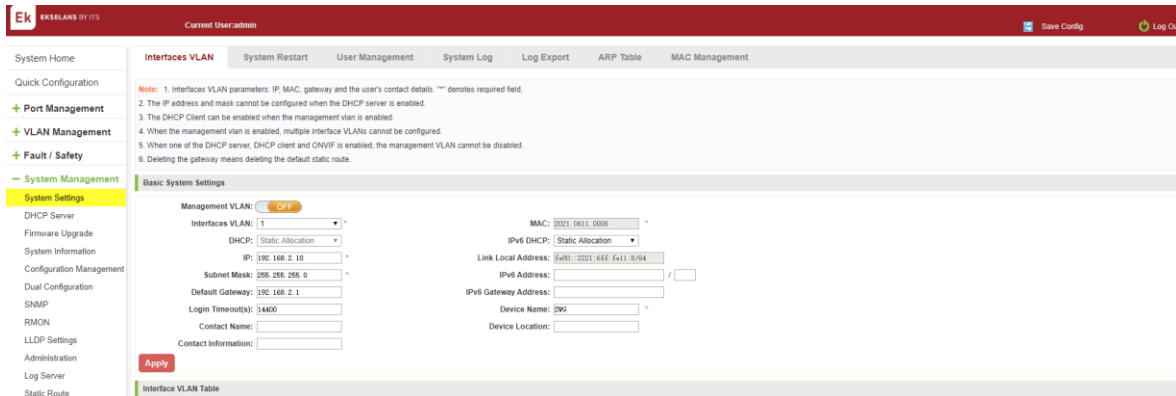


Figure 7-46: Static Route.

Step 2, Modify the IP address of interface vlan1 to 10.1.1.1/24.

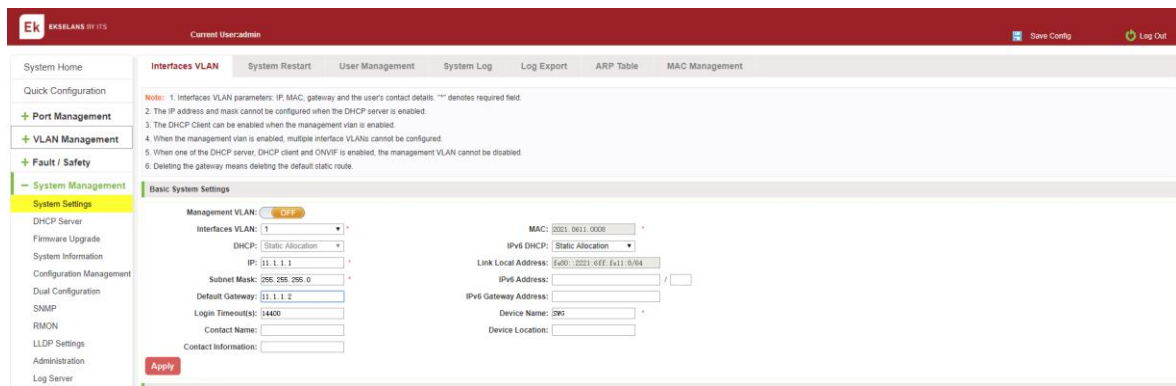


Figure 7-47: Static Route.

Step 3 Modify the IP address of interface vlan10 to 192.168.100.160/25.

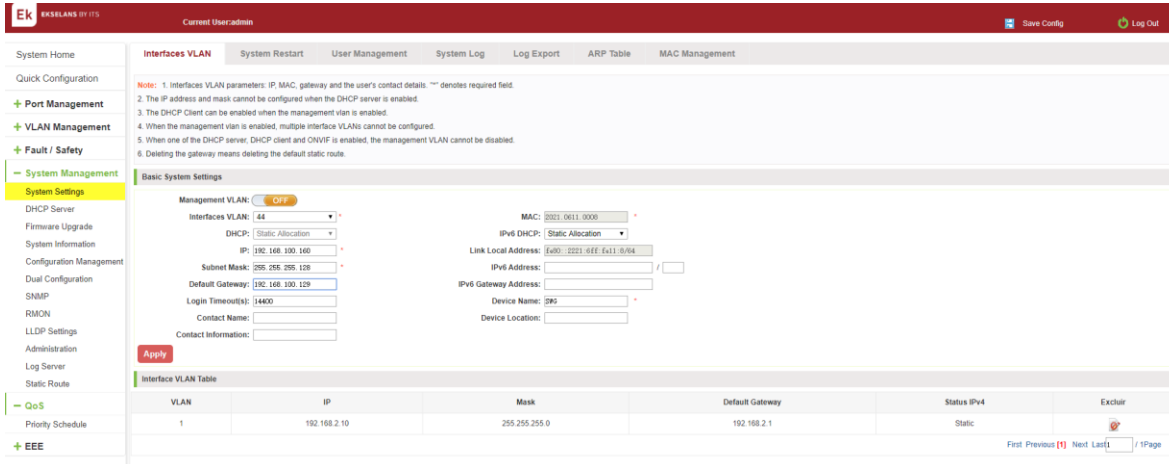


Figure 7-48: Static Route.

Step 4, The gateway with static route 192.168.100.0/25 added is 192.168.100.129.

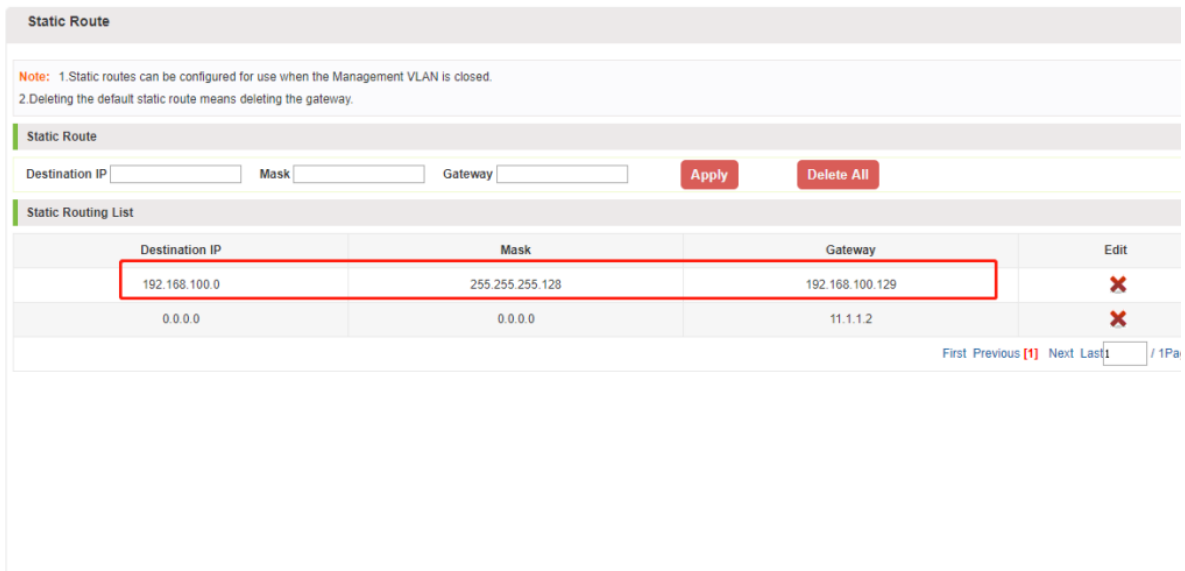


Figure 7-49: Static Route.

QOS.

Priority Schedule.

View the priority schedule.

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

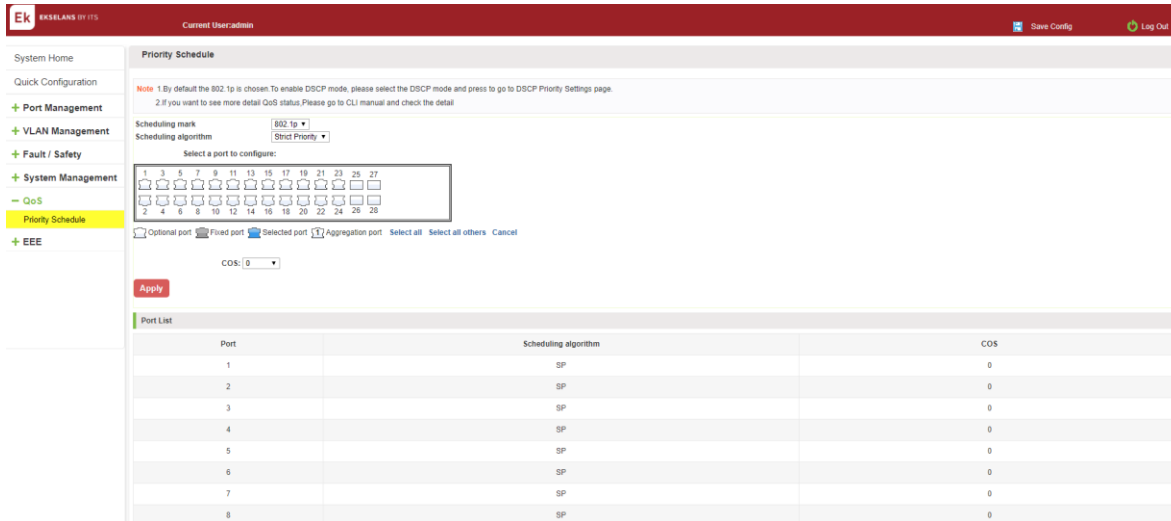


Figure 8-1: priority schedule.

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP.

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

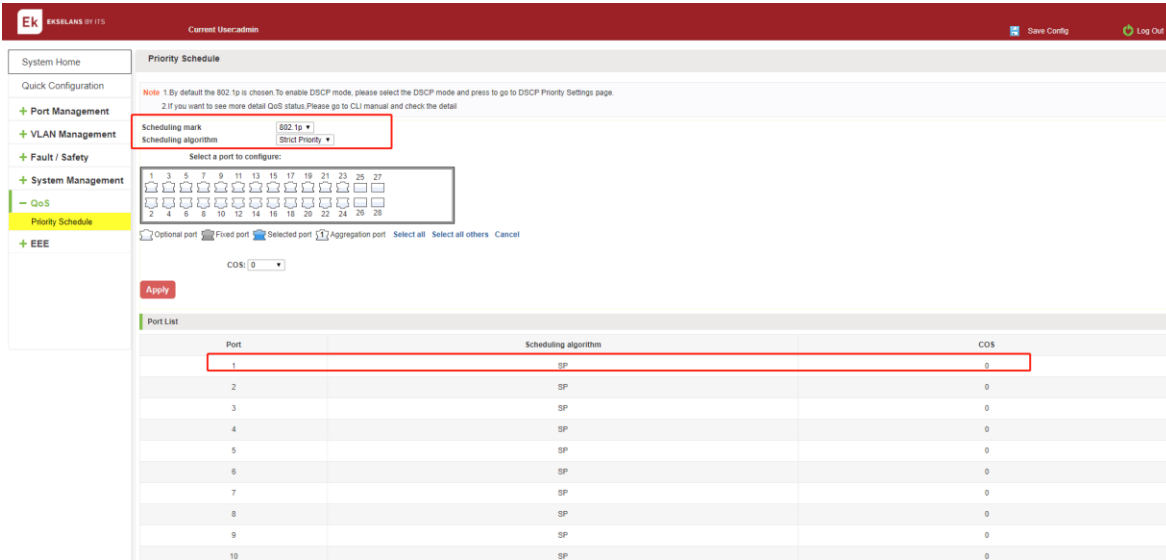


Figure 8-2: global settings in 802.1p and SP.

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP ADD WRR.

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

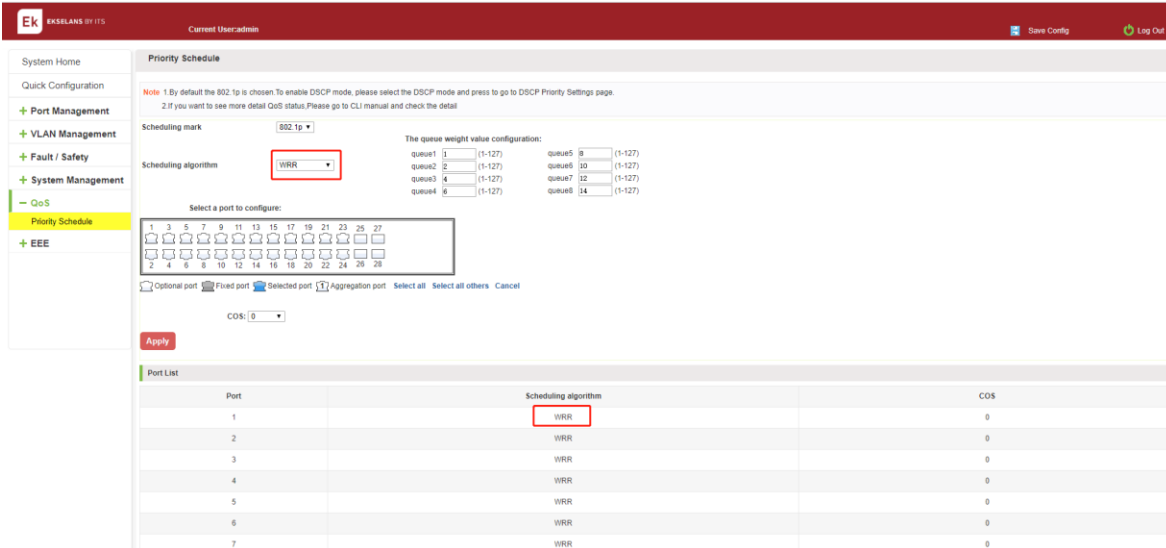


Figure 8-3: global settings in 802.1p and WRR.

Priority schedule steps are as follows:

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

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P AND HYBRID.

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

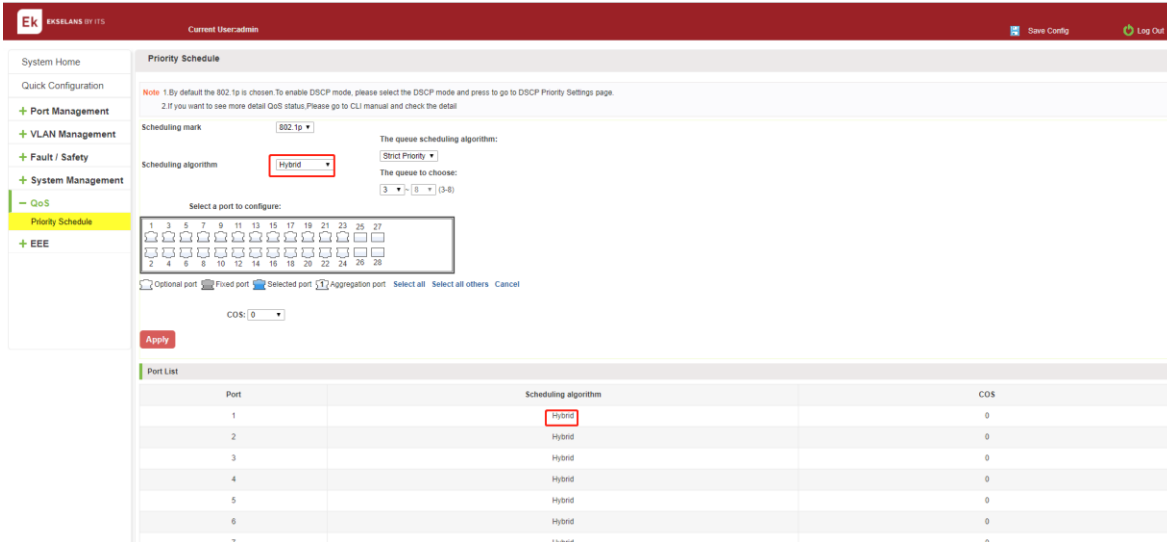


Figure 8-4: global settings in 802.1p and hybrid.

Priority schedule steps are as follows:

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

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND SP.

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

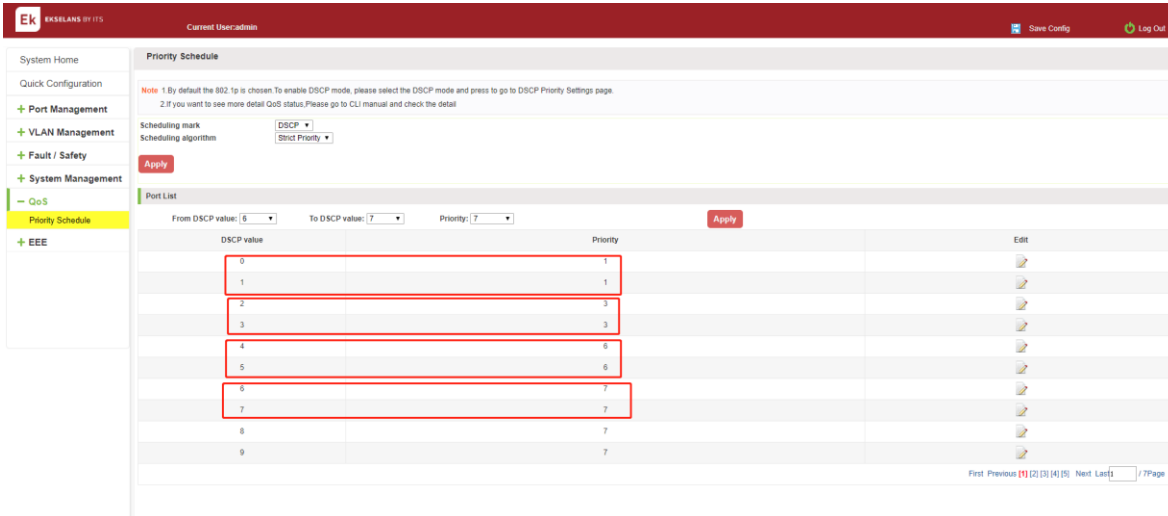


Figure 8-5: global settings in DSCP and SP.

Priority schedule steps are as follows:

- Step1: in scheduling mark, choose DSCP; step2:in the Scheduling algorithm, choose strict priority.
- Step3:in from DSCP value text box, choose 0 and in to DSCP value text box, choose 1 and in priority text box, choose 1.
- Step4:in from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose 3.
- Step5:in from DSCP value text box, choose 4 and in to DSCP value text box, choose 5 and in priority text box, choose 6.
- Step6:in from DSCP value text box, choose 6 and in to DSCP value text box, choose 8 and in priority text box, choose 7.

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND WRR.

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

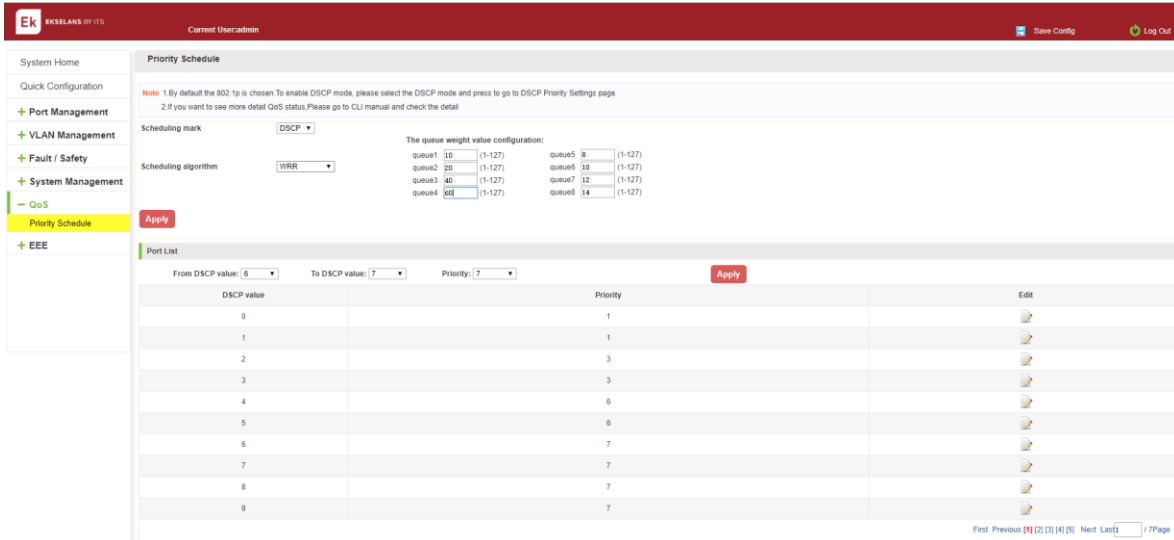


Figure 8-6: global settings in DSCP and WRR.

Priority schedule steps are as follows:

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

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND HYBRID.

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

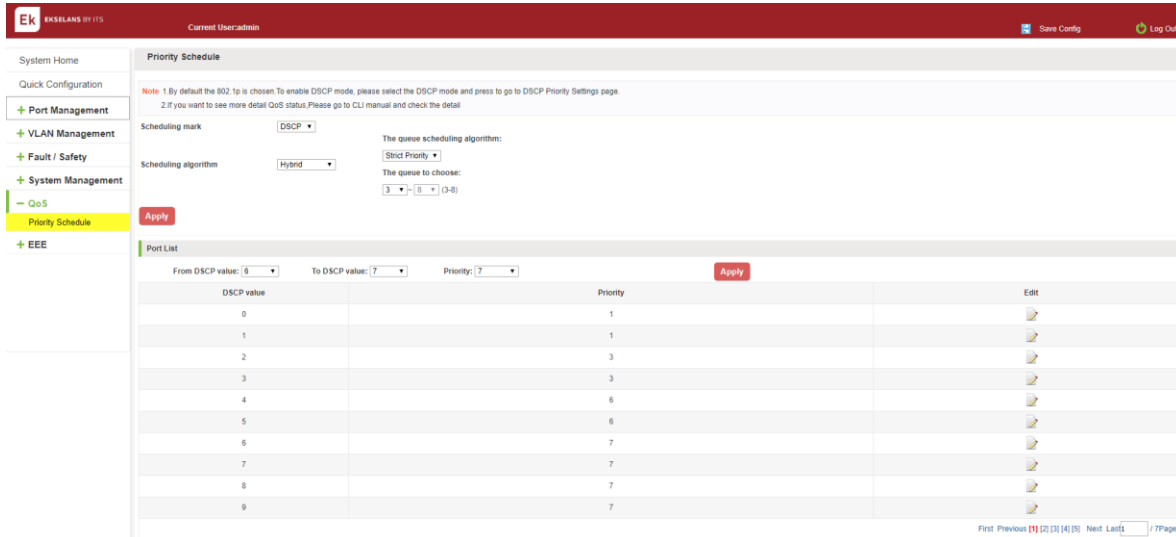


Figure 8-7: global settings in DSCP and HYBRID:

Priority schedule steps are as follows:

- Step1: in scheduling mark, choose DSCP.
- Step2: in the Scheduling algorithm, choose hybrid.
- Step3: in strict priority text box, choose the queue 3,4.
- Step4: in WRR text box, choose the queue 1,2.
- Step5: in queue1 text box, enter the weight value, such as 10.
- Step6: in queue2 text box, enter the weight value, such as 20.

Editing the DSCP values.

Click on the "🔧" icon to modify DSCP values:

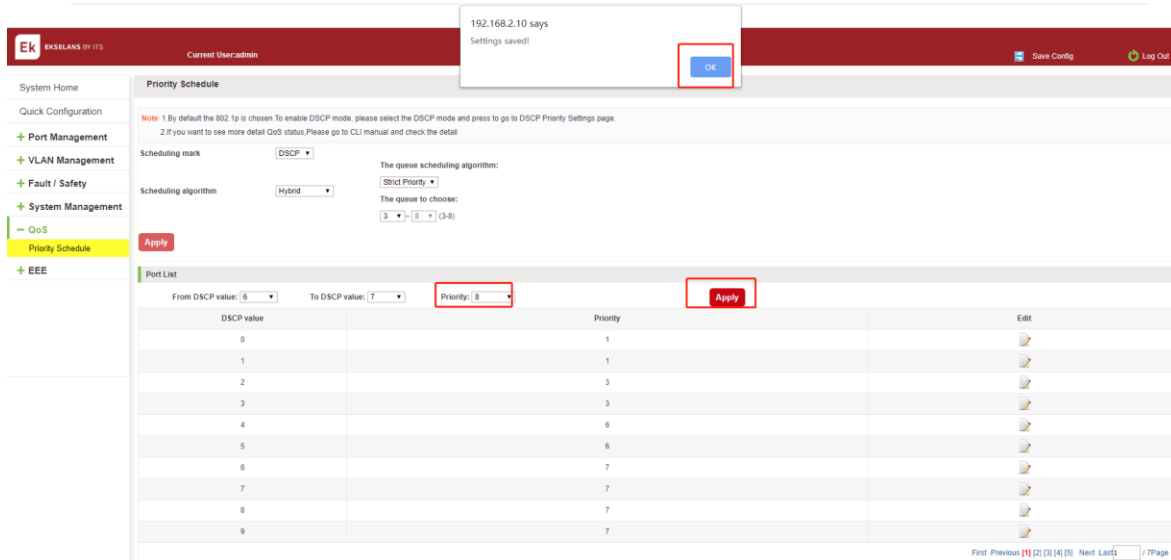


Figure 8-8: Add the port to the VLAN.

Modify DSCP values follow these steps:

- Step1: select DSCP values and Click "🔧" icon.
- Step 2: In the priority text box, choose medium.
- Step3: Click on the Apply.
- Step 4: click OK.

EEE.

EEE.

802.3AZ EEE SETTINGS.

Click on the "EEE" "EEE" "802.3az EEE settings", you can view the EEE information:



Figure 9-1: view the 802.3az EEE settings.

ACTIVE THE EEE.

Click ON the "EEE" "EEE" "802.3az EEE settings", choose the 802.3az EEE, click ON the "OFF" to "ON", click Apply:



Figure 9-2: active the 802.3az EEE settings.