ECS2020 Series

10/28-Port Gigabit Web Smart PoE & Non-PoE Switch

Software Release
v1.0.2.11

Web Management Guide

www.edge-core.com

Web Management Guide

ECS2020-10P

Web-smart Gigabit Ethernet Switch
with 8 10/100/1000BASE-T (RJ-45)
and 2 Gigabit SFP Ports

ECS2020-10T

Web-smart Gigabit Ethernet Switch
with 8 10/100/1000BASE-T (RJ-45) 802.3af/at PoE Ports
and 2 Gigabit SFP Ports

ECS2020-28P

Web-smart Gigabit Ethernet Switch
with 24 10/100/1000BASE-T (RJ-45)
and 4 Gigabit SFP Ports

ECS2020-28T

Web-smart Gigabit Ethernet Switch
with 24 10/100/1000BASE-T (RJ-45) 802.3af/at PoE Ports
and 4 Gigabit SFP Ports

E072021-CS-R04

About This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Related Documentation

This guide focuses on switch software configuration through the Web management interface.

For information on how to manage the switch through the CLI, see the following guide:

CLI Reference Guide

Documentation Notice

This documentation is provided for general information purposes only. If any product feature details in this documentation conflict with the product datasheet, refer to the datasheet for the latest information.

Note: There are 4 devices in this series: ECS2020-10P, ECS2020-10T, ECS2020-28P, and ECS2020-28T.

Note: The PoE function is only applicable to the ECS2020-10P and ECS2020-28P products.

Note: Sections of this document use the ECS2020-10P as an example. The other switch models differ only in panel image, port types, and equipment name but function identically.

Table of Contents

Figures

1 WEB MANAGEMENT LANDING PAGE

1.1 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB

The computer's IP address and the switch IP address must be set to the same subnet (switch default IP address is 192.168.2.10, and the default subnet mask is 255.255.255.0). Run a web browser, and enter http://192.168.2.10 in the address bar. Enter the default user name and password (user name: admin; password: admin), and then click the "Login" button to directly access the web management home page.

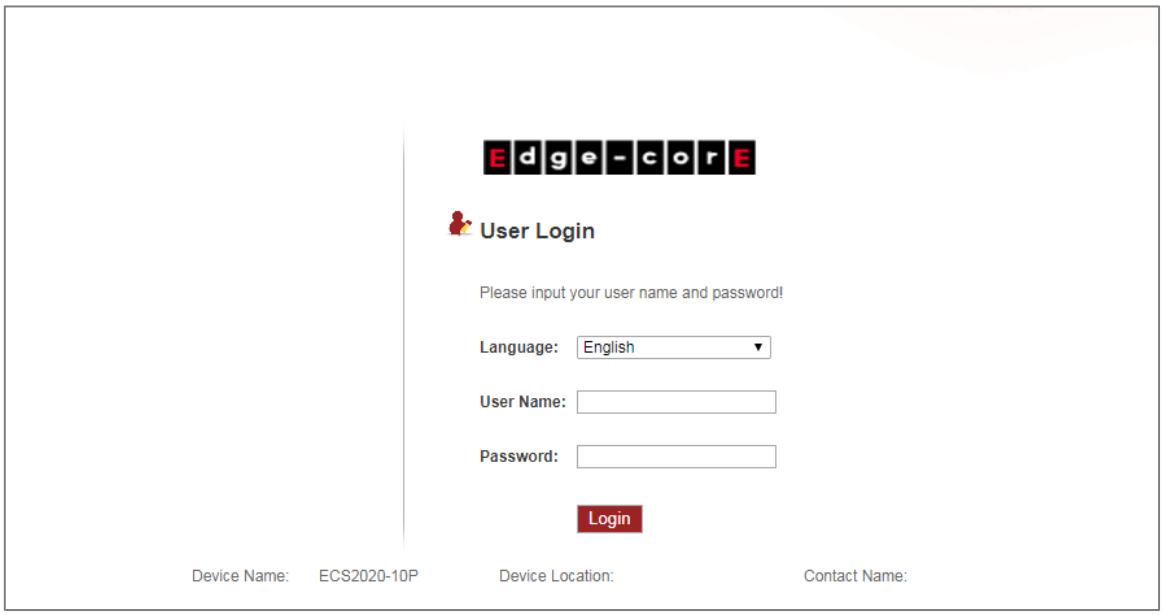


Figure 1-1: The Login Page

After launching successfully, the switch management home page displays:

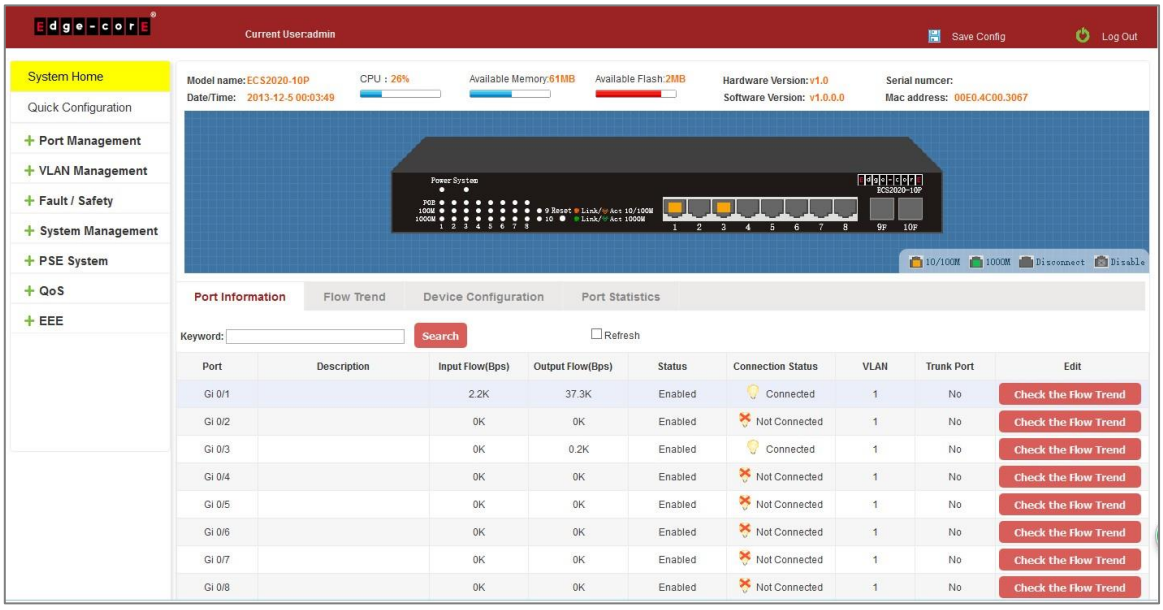


Figure 1-2: Web Management Home Page

2 SYSTEM HOME

2.1 DEVICE PANEL

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

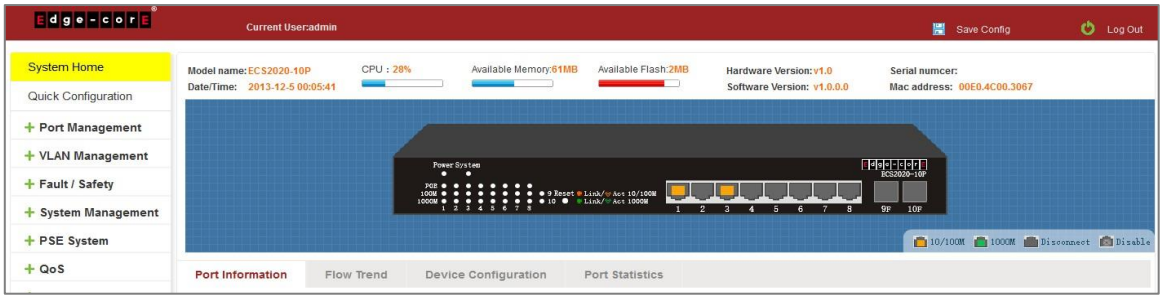


Figure 2-1: Web Device Panel

2. Clicking on a specific port displays the following information.

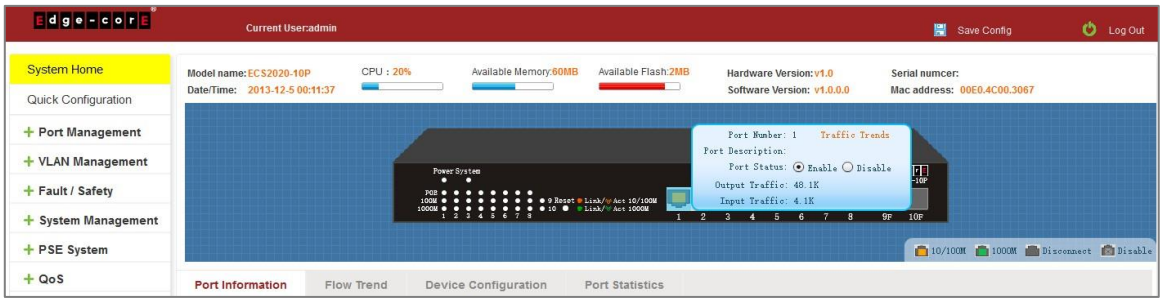


Figure 2-2: View the Port Status

2.2 PORT INFORMATION

The configuration of the ECS2020-10P is as follows: "System Home", "Port Information".

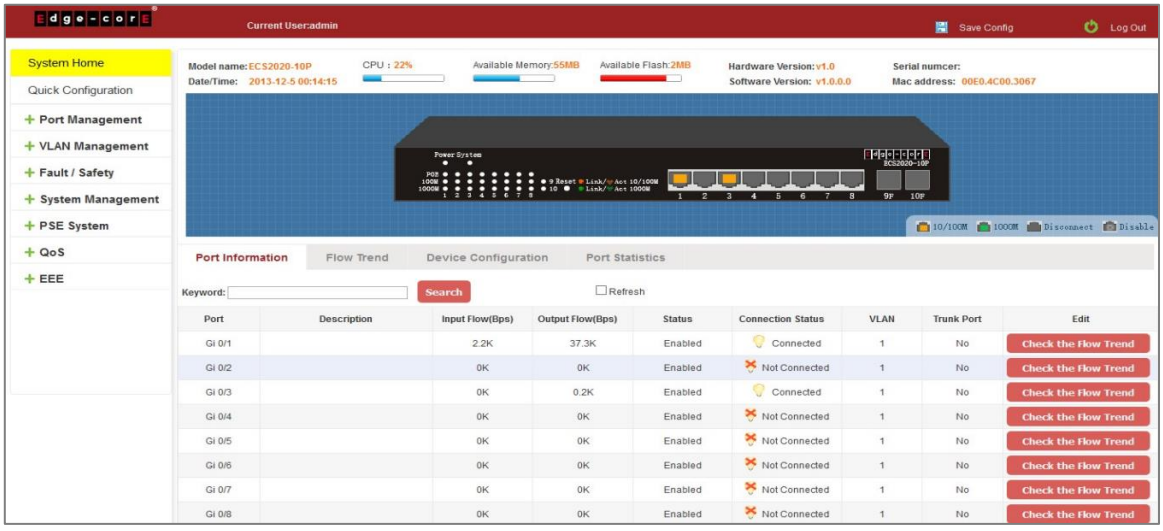


Figure 2-2: Port Information

On the panel, you can see the device port, description, input flow, output flow, state of the port, connection state, VLAN, and trunk status.

2.3 FLOW TREND

Click the device port on the panel port to view the port flow trends.

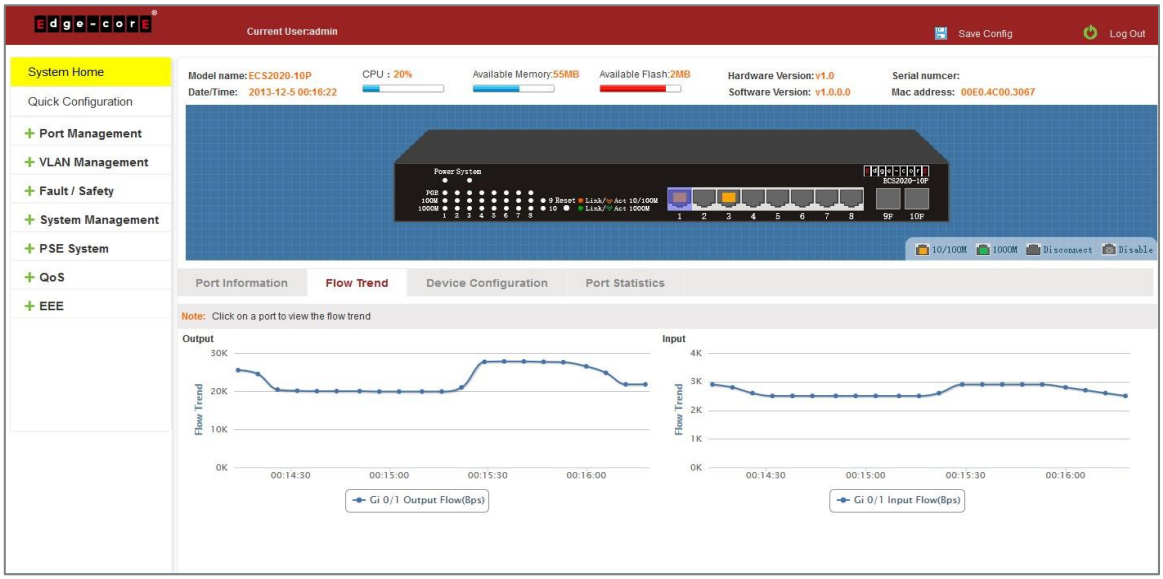


Figure 2-3: View the Flow Trend

2.4 DEVICE CONFIGURATION

Click "Device Configuration" to view and change the configuration of the device.

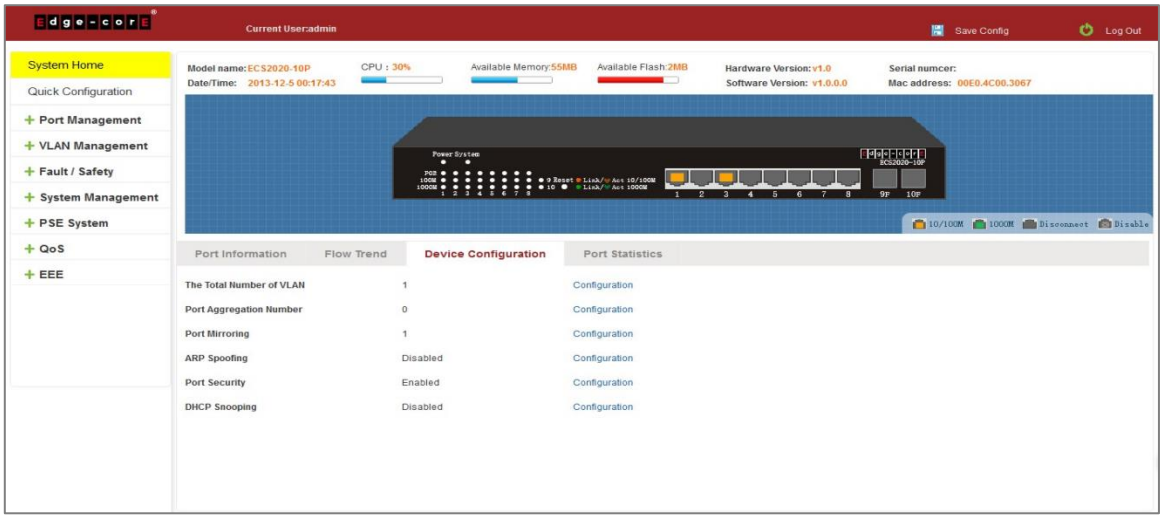


Figure 2-4: Device Configuration

Use "Device configuration" to configure the following modules:

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

2.5 PORT STATISTICS

The Port Statistics page shows the number of bytes received, the number of bytes sent, the number of incomplete packets, the number of large packets, CRC error packets, and the number of conflicts.

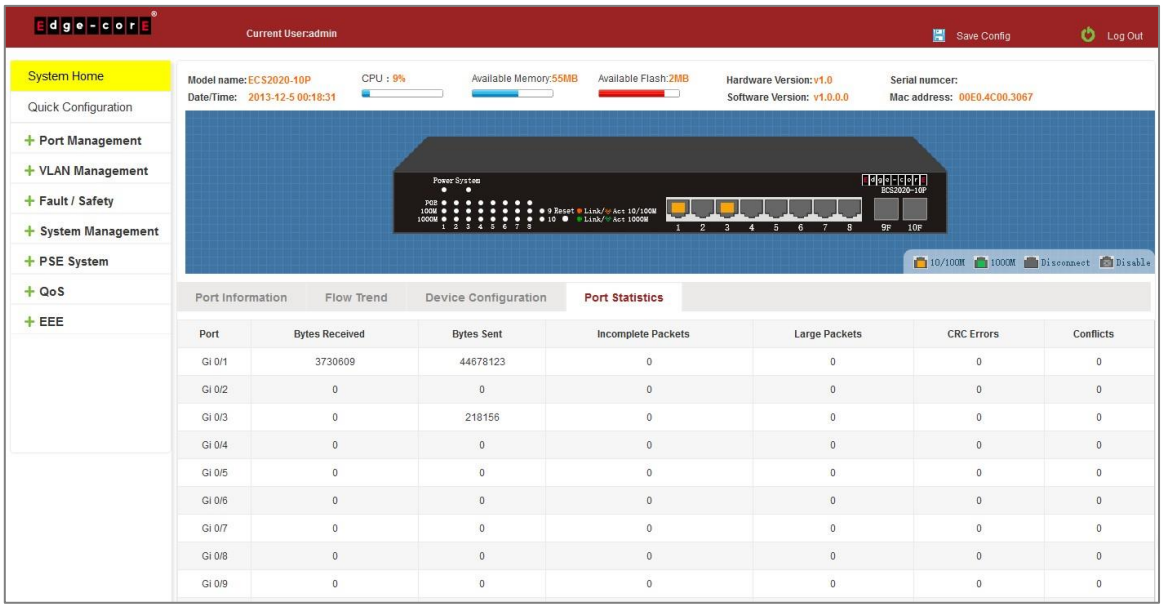


Figure 2-5: View the Port Statistics

3 QUICK CONFIGURATION

Click on "Quick Configuration" to quickly configure commonly used functions, such as a VLANs, trunk ports, port classes, and basic settings.

3.1 BASIC SETTING

Click "Quick Configuration" and then "Basic Settings" to display the System Settings page. The current basic system information and management password can be configured.

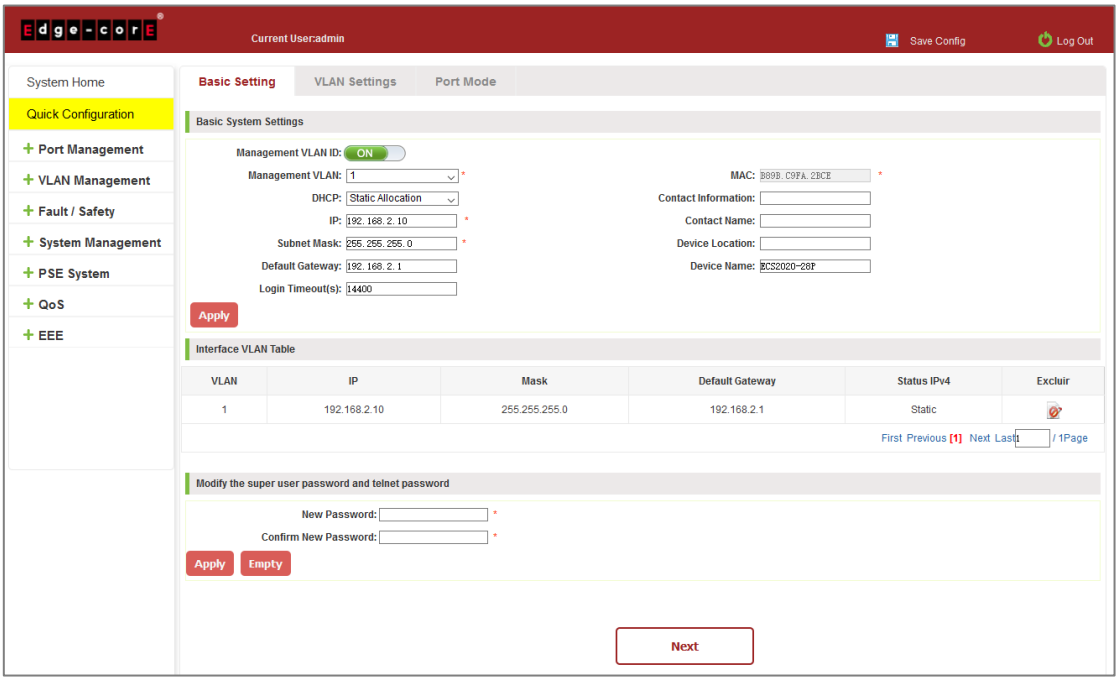


Figure 3-1: Basic Setting

3.2 VLAN SETTINGS

Click "Quick Configuration" and then "VLAN Settings" to access the VLAN configuration page. You can view the current VLAN information, create new VLANs, modify VLANs, delete VLANs, etc. When configuration is completed, click "Next".

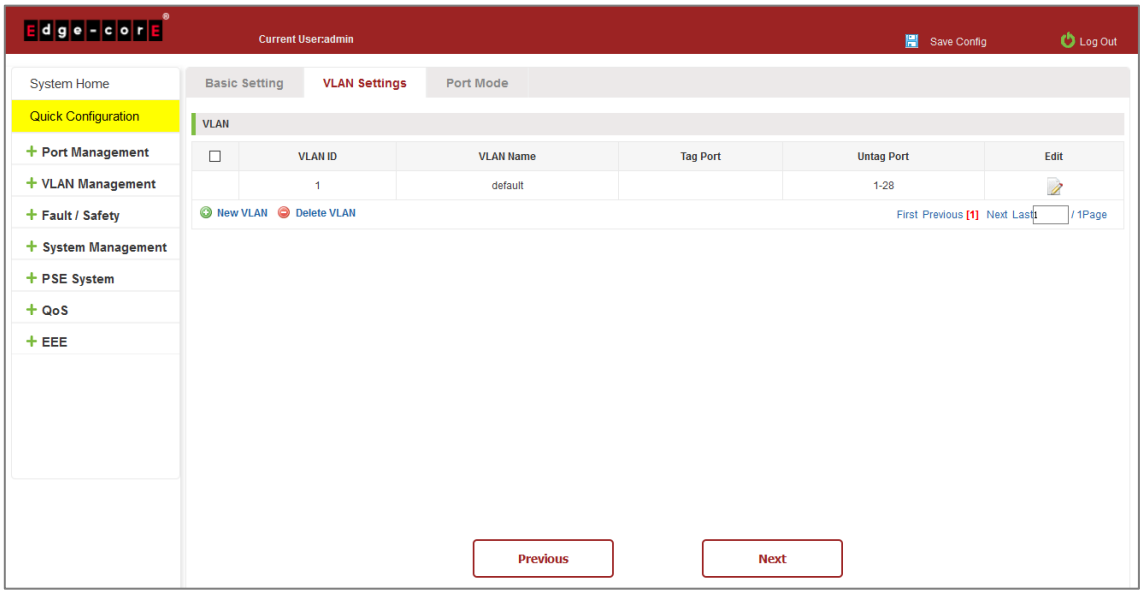


Figure 3-2: VLAN Settings

3.3 PORT MODE

Click "Quick Configuration" and then "Port Mode" to access the port settings page. You can change the port setting to allow VLANs in trunk or hybrid mode (Note: When a port is changed to trunk mode, it will be removed from any previous untagged VLAN). When configuration is complete, click "Complete".

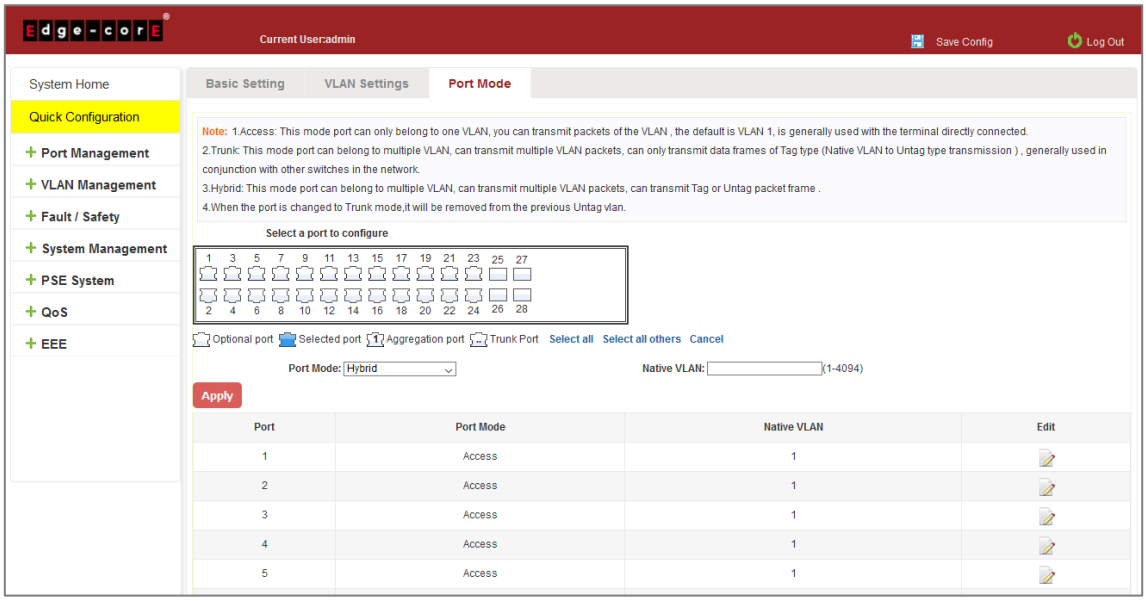


Figure 3-3: Port Mode

4 PORT MANAGEMENT

4.1 BASIC SETTINGS

4.1.1 Check the port configuration

On the navigation bar, click "Port Management" and then "Basic Settings" to view the current configuration of the switch ports:

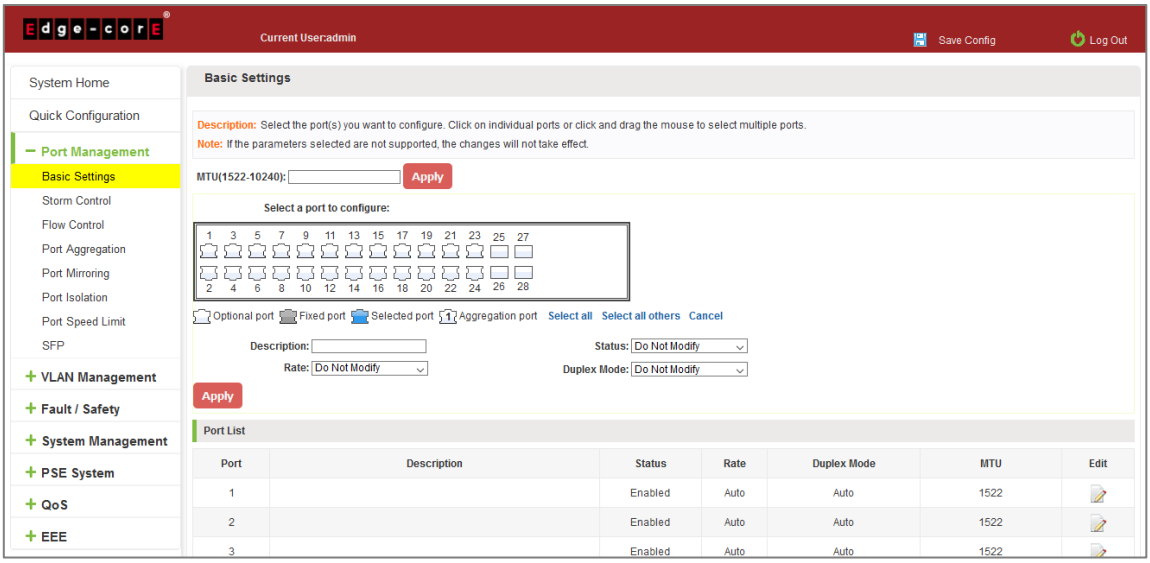


Figure 4-1: Port List Information

The port list attributes show the current switch port configuration information:

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

4.1.2 Configuring port properties

Click the icon to configure the selected port attributes:

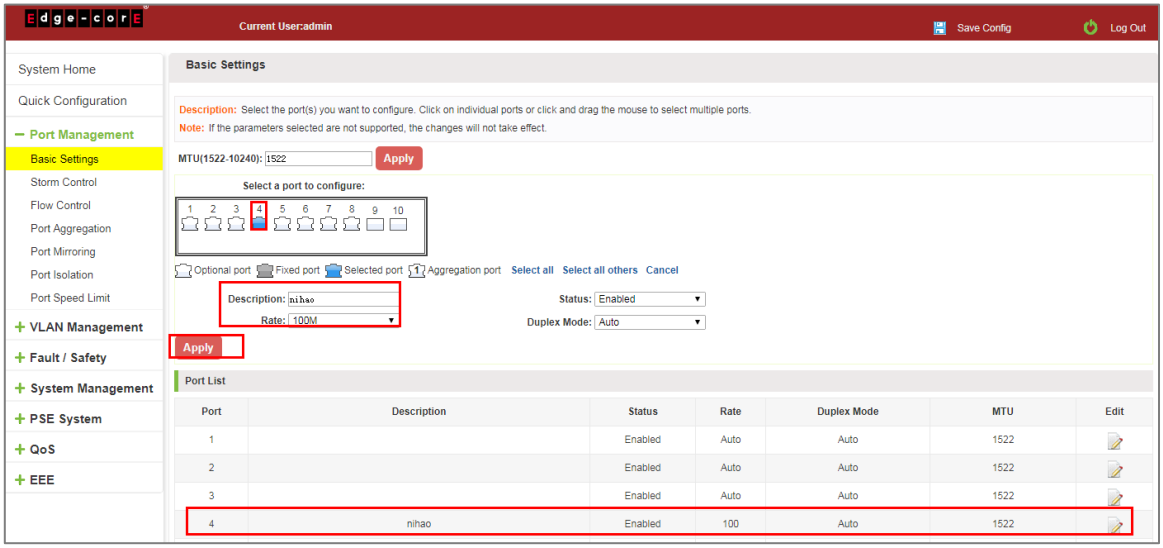


Figure 4-2: Port Properties Configuration

Configure port properties as follows:

Step 1: Click the "Edit" icon .

Step 2: In the Port Properties configuration page, fill/select the value to be configured.

Step 3: Click the "Apply" button to complete the configuration.

4.2 STORM CONTROL

4.2.1 Check the storm control port settings

On the navigation bar, click "Port Management" and then "Storm Control" to view the current switch port storm control information.

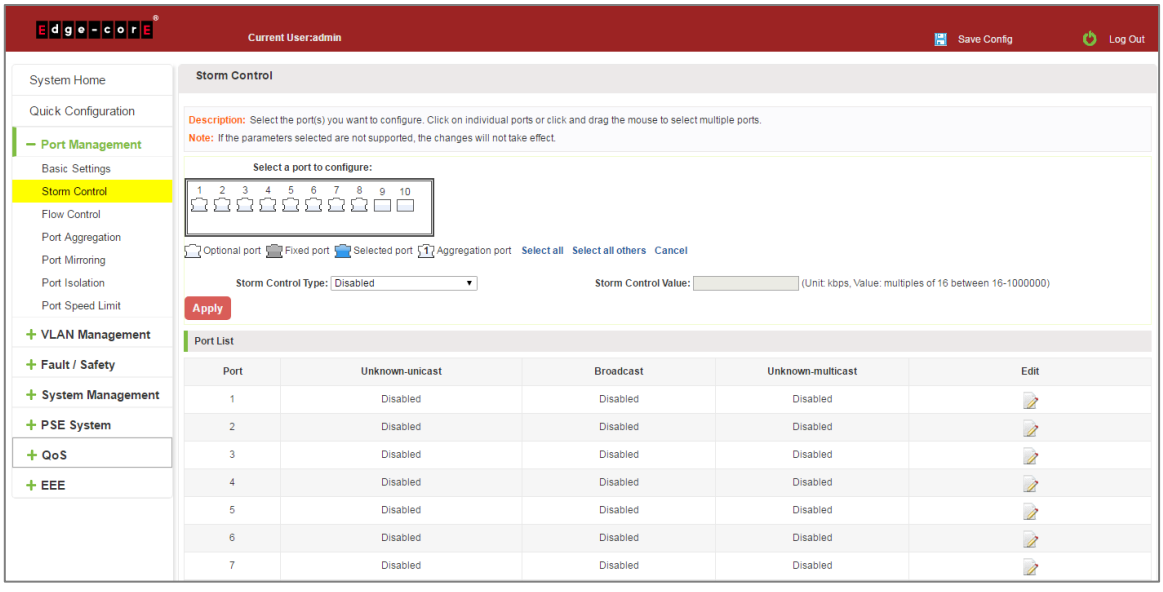


Figure 4-3: Storm Control List Information

The list of ports shows the current storm control property values:

1. Port: The number of the port.
2. Unknown-unicast: Unknown unicast packets control.
3. Broadcast: Broadcast packet control.
4. Unknown-multicast: Multicast packets control.
5. When the control value setting is not a multiple of 16, the system automatically matches the closest multiple of 16.
6. The control values of unknown-unicast, broadcast, and unknown-multicast, can only be a single value.

Clicking the corresponding port on the port panel selects the port to be configured.

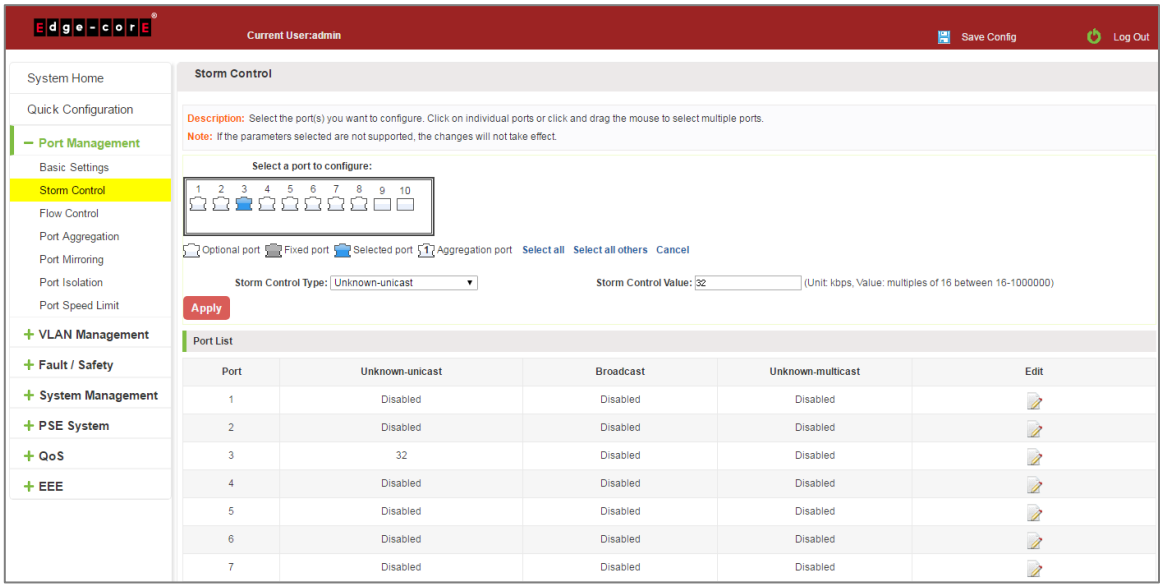


Figure 4-4: Configuring Storm Control Information

You can also select multiple ports for batch settings.

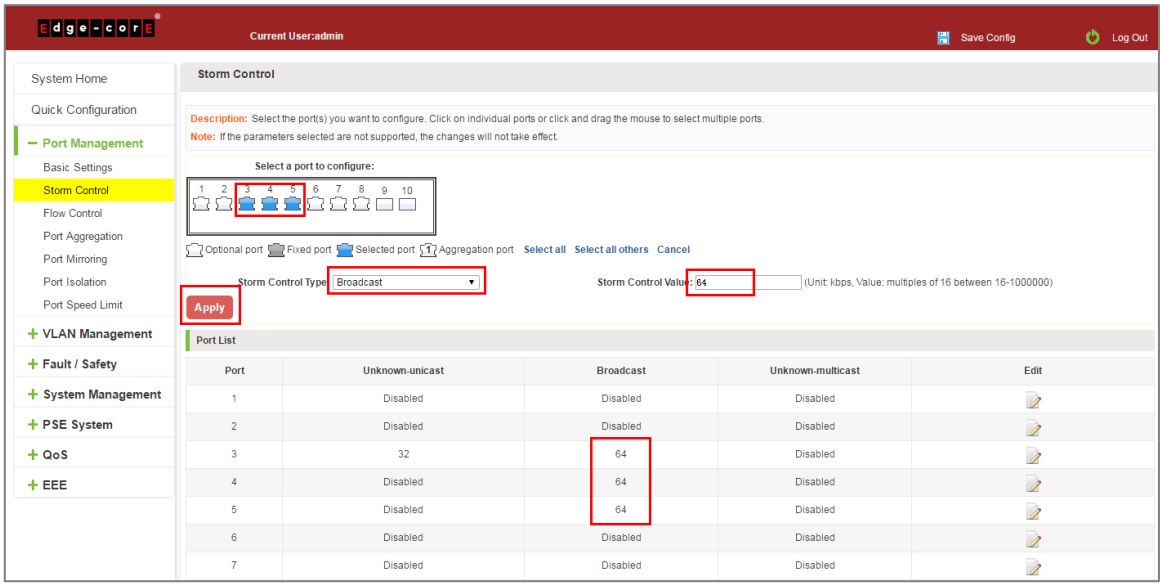


Figure 4-5: Bulk Edit Configuration Information

After selecting the ports in the Storm Control port panel, set the unknown-unicast, unknown-multicast, and broadcast values. For example, set the port 1 unknown-unicast storm control to 1009, and then click "Apply Settings".

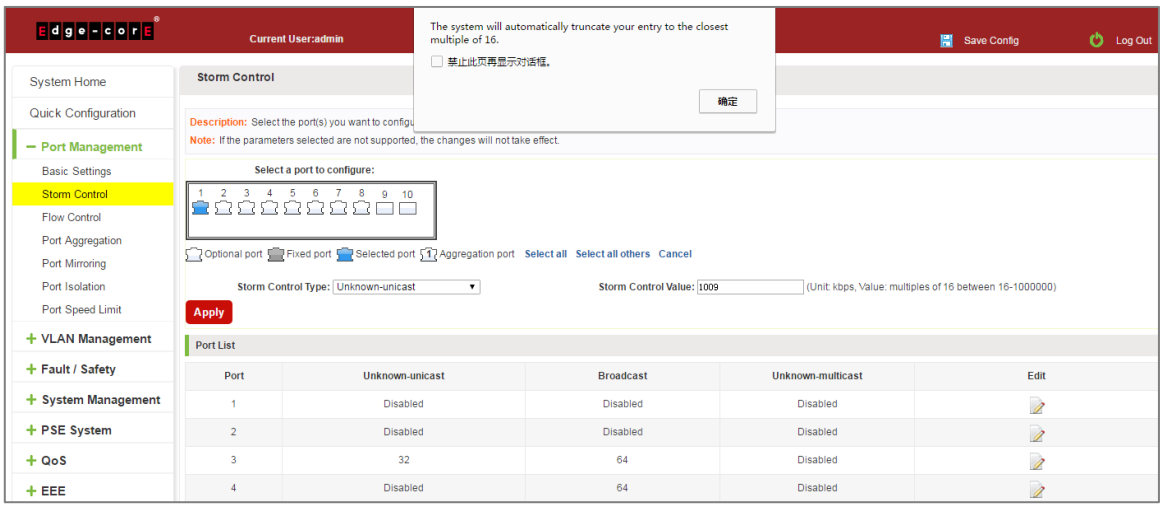


Figure 4-6: Configuring Storm` Control Information

The configuration displays as shown below:

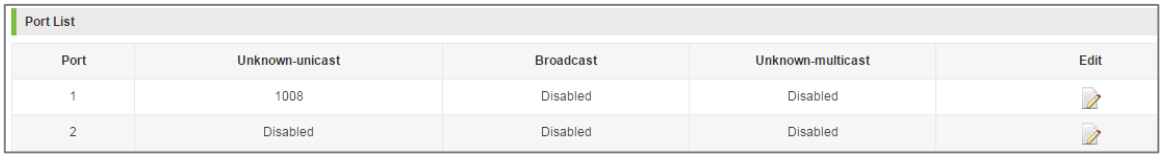


Figure 4-7: Configuration Successfully Storm Control Information Flow Control

4.3 FLOW CONTROL

Click "Port Management" and then "Flow Control" to view the port flow control information on the switch.

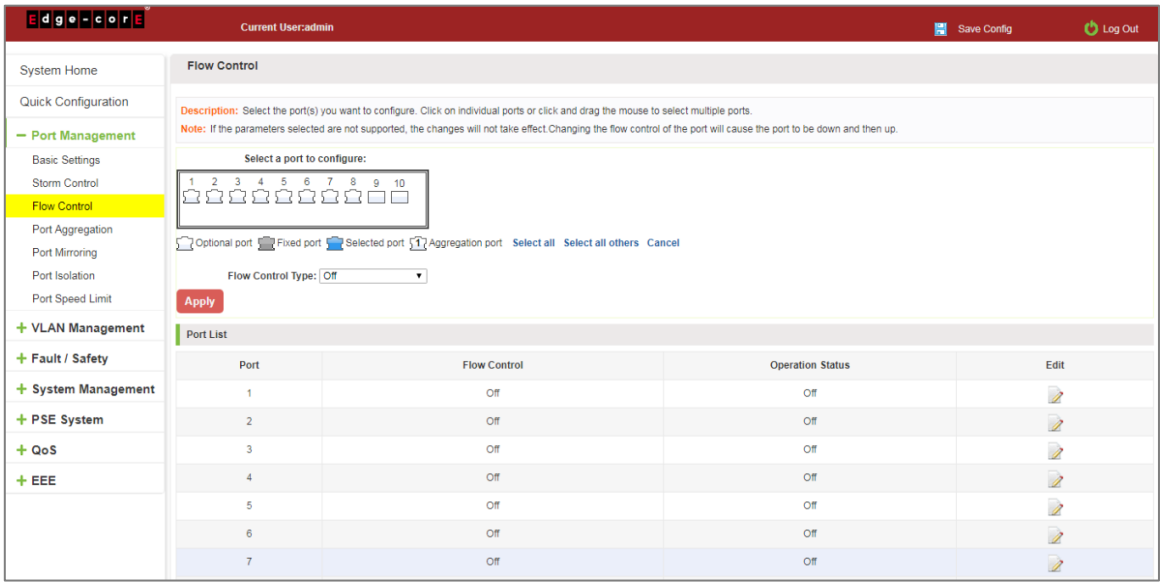


Figure 4-8: Flow Control Information

4.3.1 Configuring flow control

To enable the port flow control function: Select the ports to enable traffic control, and then click "Flow Control". Select "On" and click "Apply".

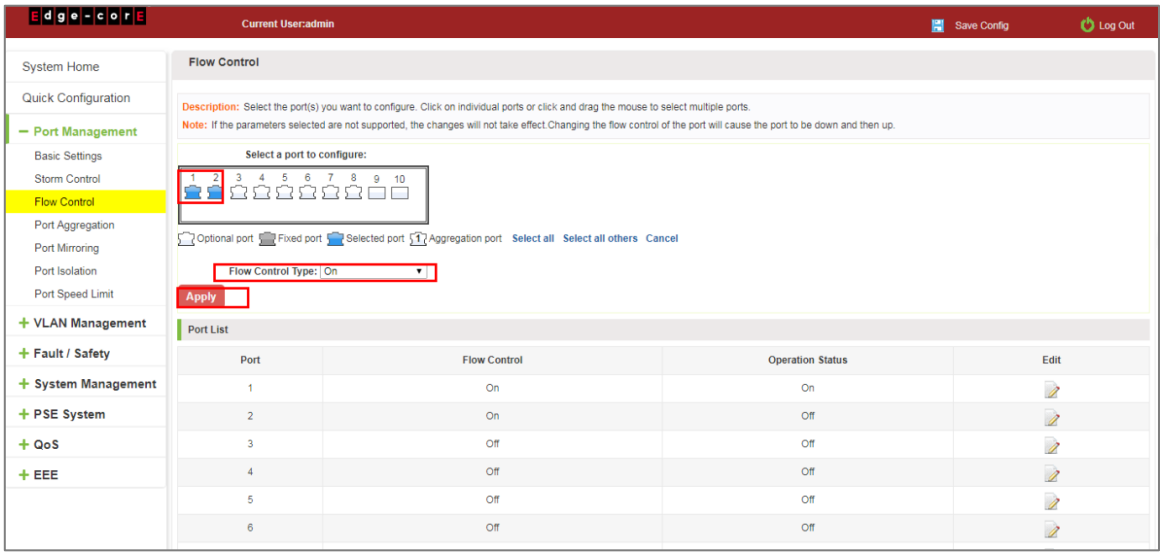


Figure 4-9: Open Port Flow Control Function

To enable port traffic control, follow these steps:

Step 1: Select the port.

Step 2: Set the "Flow control" to “On”.

Step 3: Click "Apply".

View the port list to check that the configuration is successful:

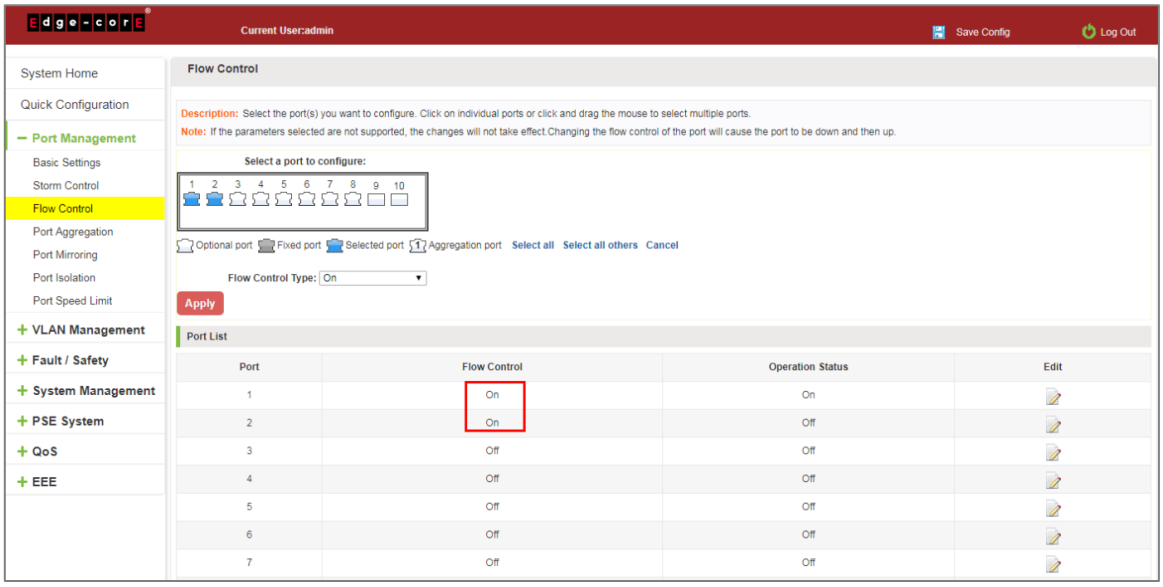


Figure 4-10: Port Flow Control Status

To modify the port flow control function: Click on the port traffic control list corresponding to the rear port of the " " button in the Port Settings page "Flow Control Type" select "Off", "Apply Settings":

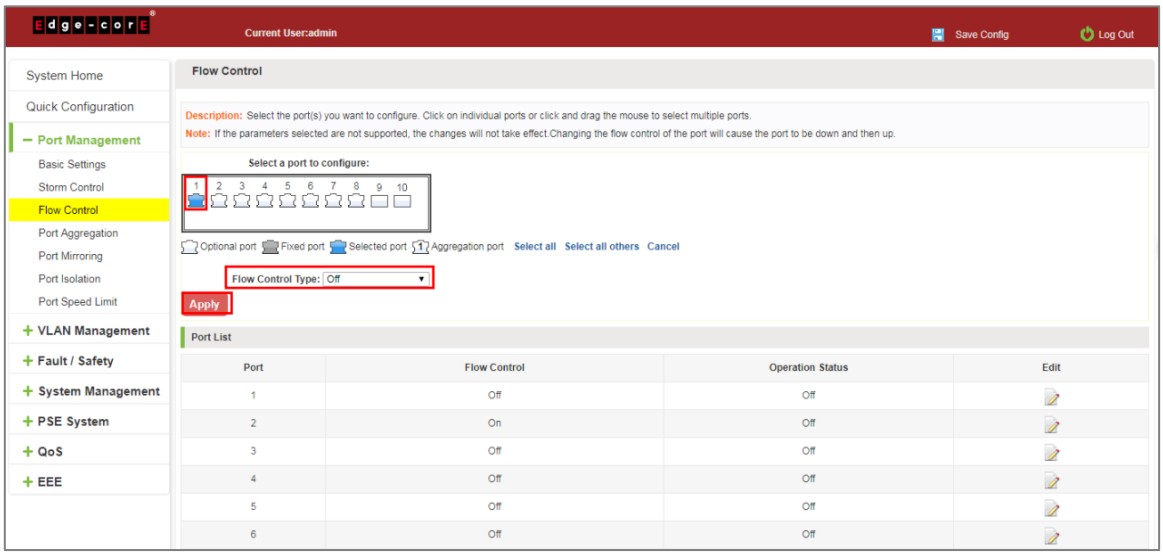


Figure 4-11: Close the Port Flow Control

Close port traffic control, follow these steps:

Step 1: Select the button to the right of the port or directly selected port;

Step 2: In the "Flow Control Type" select off;

Step 3: Click "Apply".

4.4 PORT AGGREGATION

4.4.1 Viewing port aggregation configuration

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

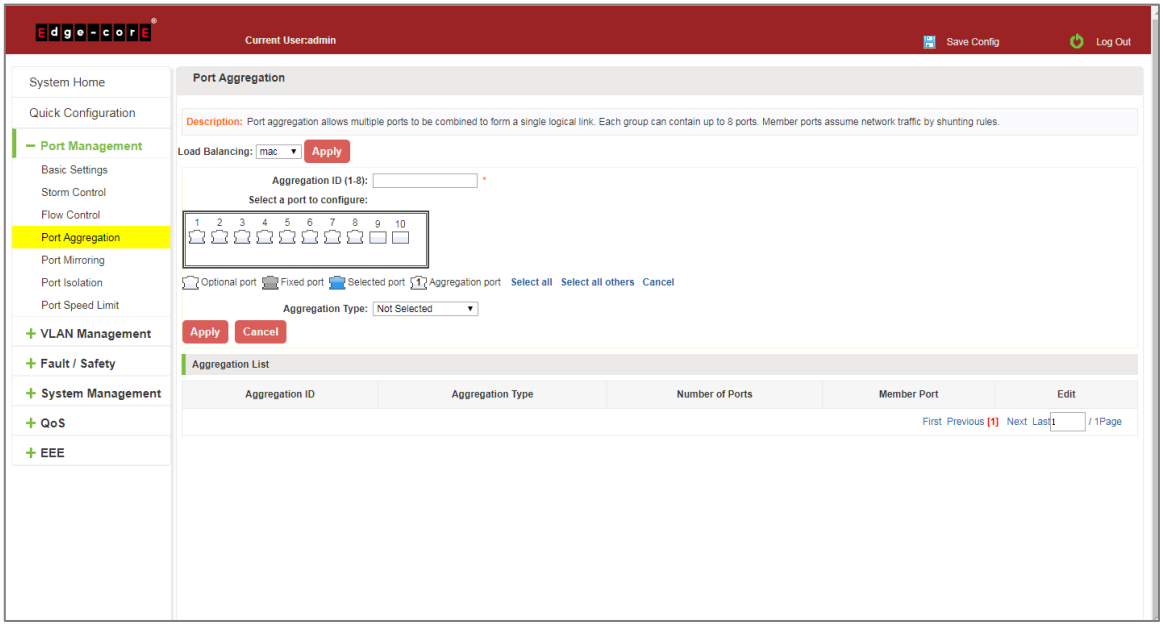


Figure 4-12: Aggregation Port Configuration Information

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.

4.4.2 Add port aggregation

Enter aggregation port number, select the desired aggregation port, select aggregation type, click "Apply".

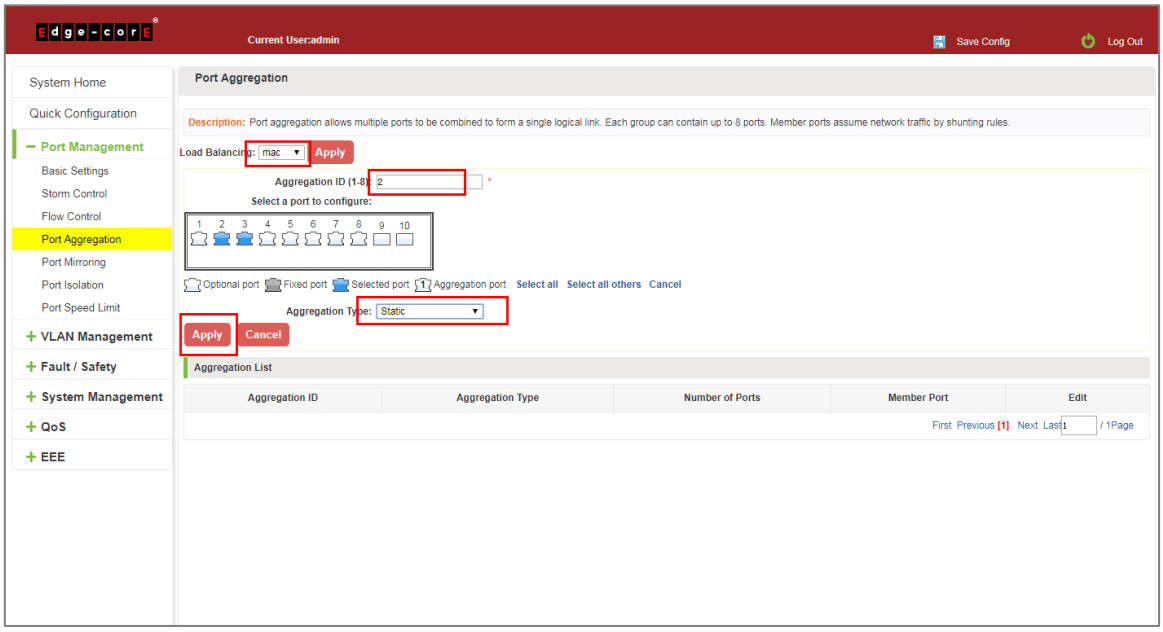


Figure 4-13: Port Aggregation Configuration Area

Increase port aggregation, follow these steps:

Step 1: Select the option to load the shunt in the load balancing list.

Step 2: Enter the number in the "Aggregation number" in.

Step 3: Select the aggregated ports in the panel.

Step 4: Select the aggregation type.

Step 5: Click the "Apply" button to complete the configuration.

4.4.3 Modifying port aggregation

Click on "Aggregation List" in the need to modify the port aggregation right icon in this area to the port aggregation port aggregation group corresponding modification:

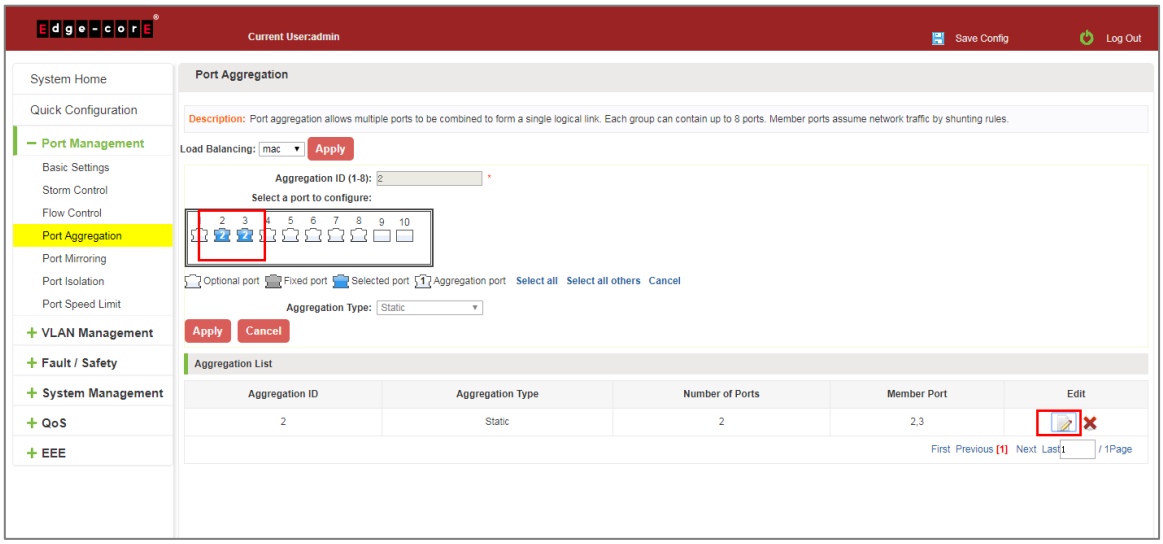


Figure 4-14: To Modify the Port Aggregation

Modify Link Aggregation Procedure:

Step 1: In the "Aggregation List Click to modify the right of the port aggregation,

Step 2: In the port aggregation configuration page to modify the load balancing type and click Next to "Apply".

Step 3: Select the port to be added to the aggregation port.

Step 4: Click the "Apply" button to complete the configuration.

4.5 PORT MIRRORING

4.5.1 Port mirroring configuration

Click "Port Management" "Configuration of Port Mirroring "Port Mirroring" view of the switch:

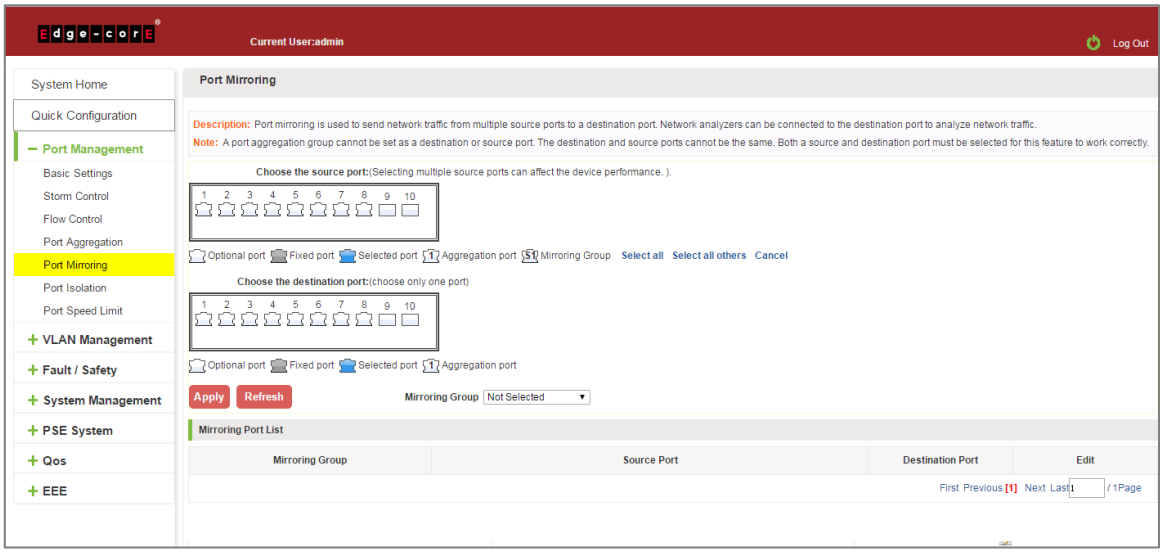


Figure 4-15: Port Mirroring Configuration Information

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.

4.5.2 Add port mirroring group

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

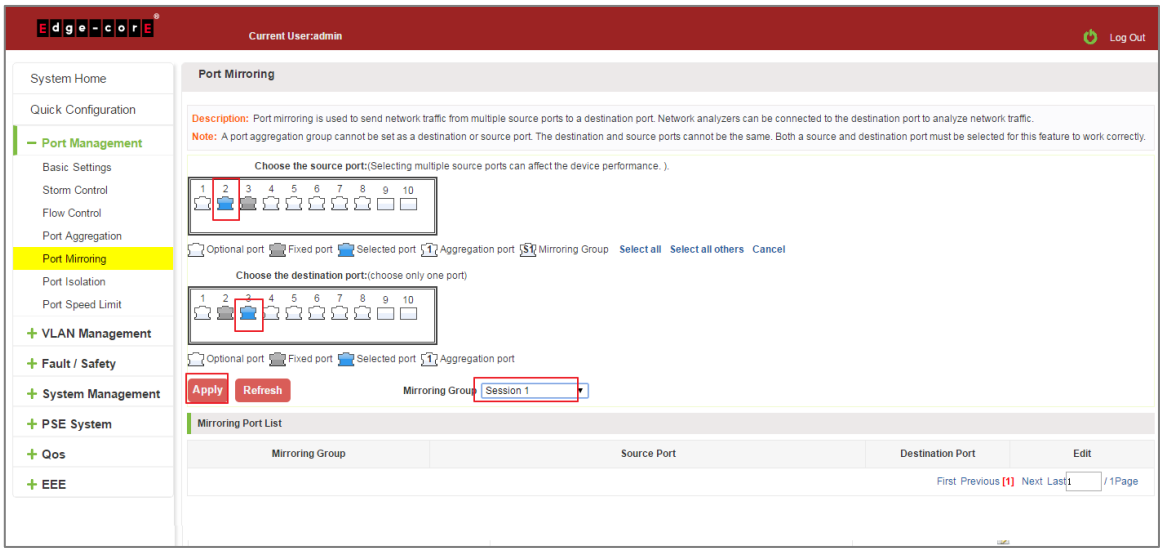


Figure 4-16: Add Port Mirroring Group

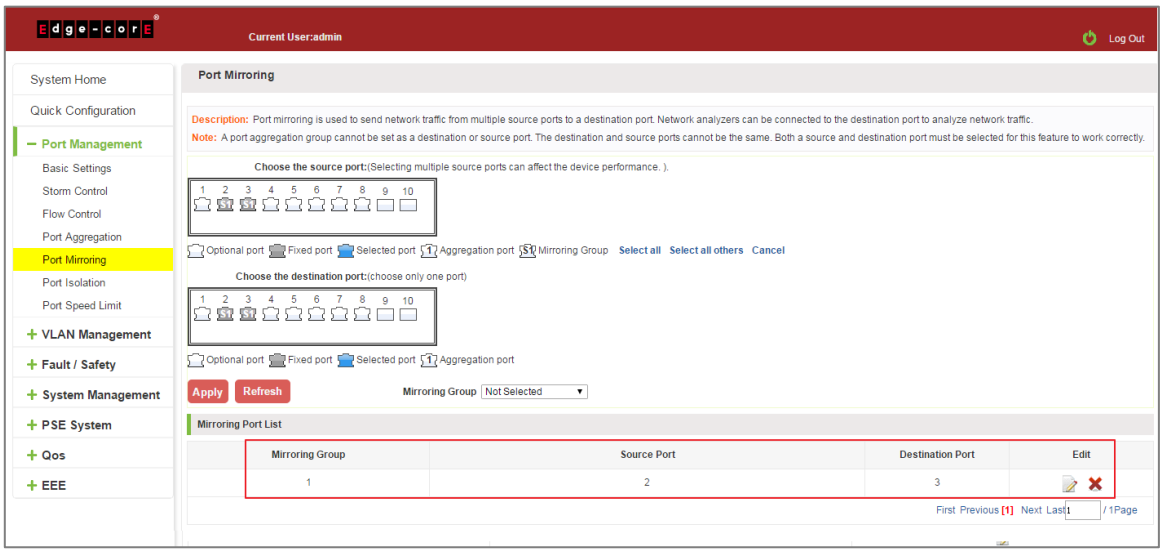


Figure 4-17: Add Port Mirroring Group Results

Port mirroring configuration steps are as follows:

Step 1: Select "Source Port",

Step 2: Select "Destination Port",

Step 3: select mirroring group,

Step 4: 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.

4.5.3 To modify the port mirroring group

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

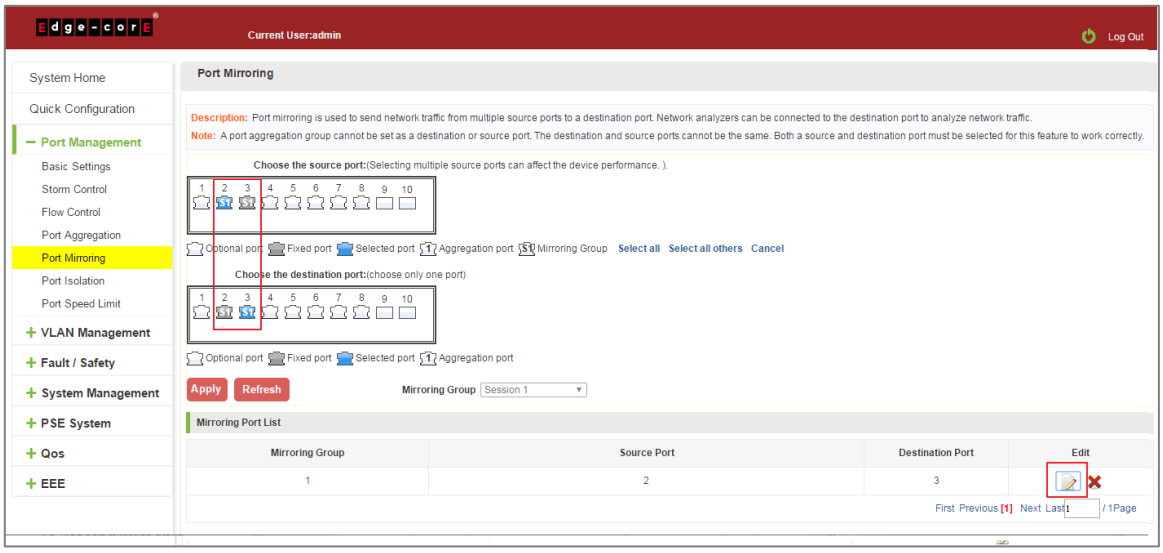


Figure 4-18: To Modify the Port Mirroring Group

Modify the port mirroring configuration steps are as follows:

Step 1: In the image you want to modify the operation of the group column, click on " ";

Step 2: Add or remove the corresponding port in the panel;

Step 3: Click "Apply".

4.5.4 Delete a port mirroring group

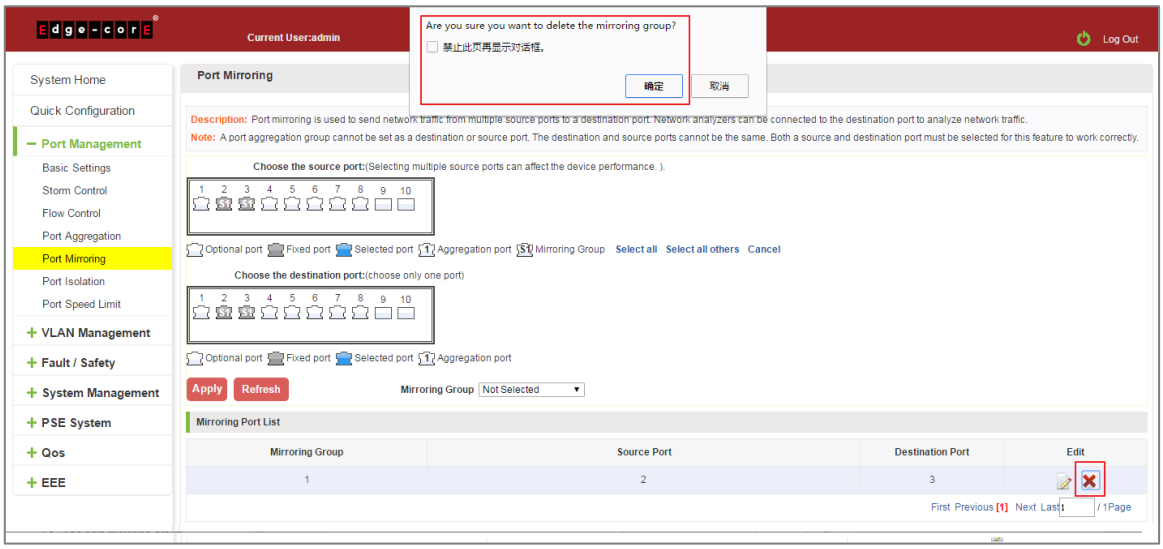


Figure 4-19: Delete Port Mirroring Group

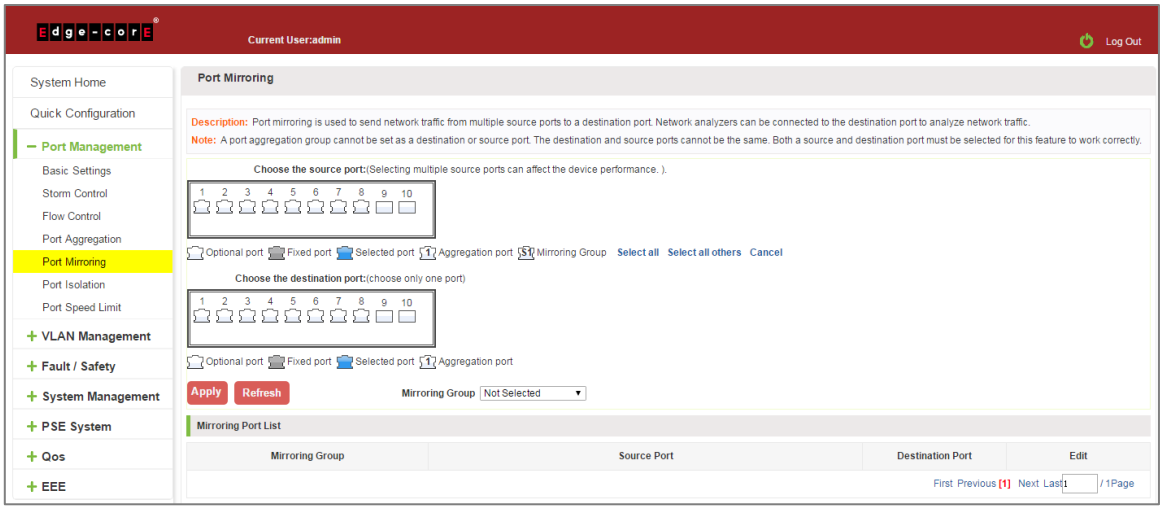


Figure 4-20: Deleted Successfully Port Mirroring

Remove port mirroring configuration steps are as follows:

Step 1: In the image you want to modify the operation of the group column, click " ";

Step 2: In the panel, click Cancel the source port, destination port and then click Cancel;

Step 3: In the panel, click Cancel the source port, destination port and then click Cancel;

Step 4: Click "Apply".

4.6 PORT ISOLATION

4.6.1 Port isolation configuration

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

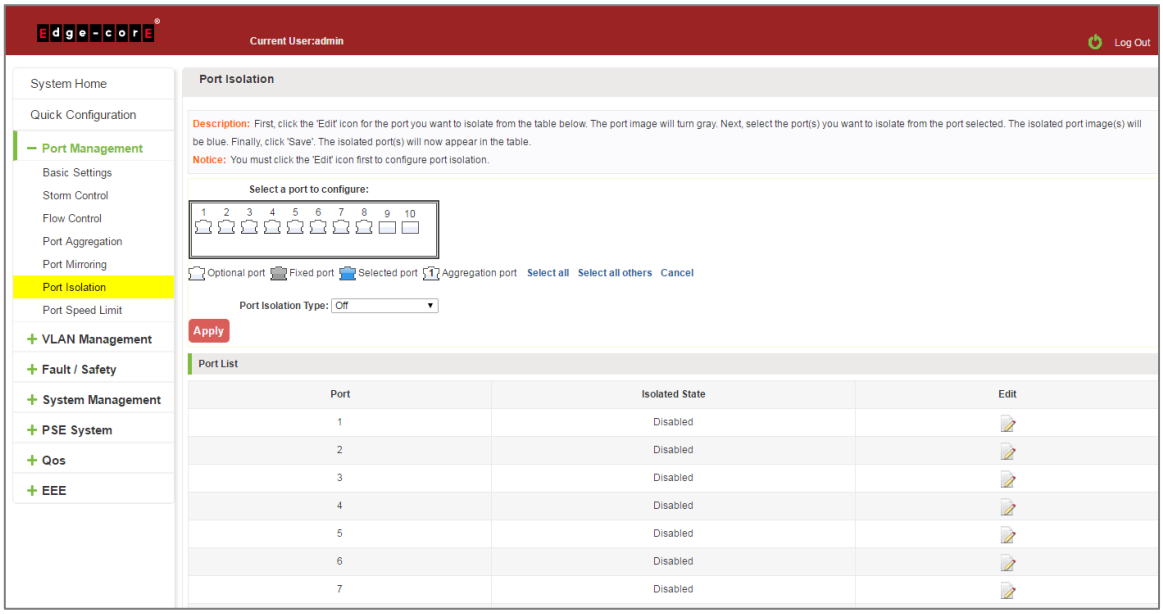


Figure 4-21: Port Isolation Configuration Information

4.6.2 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", "Apply".

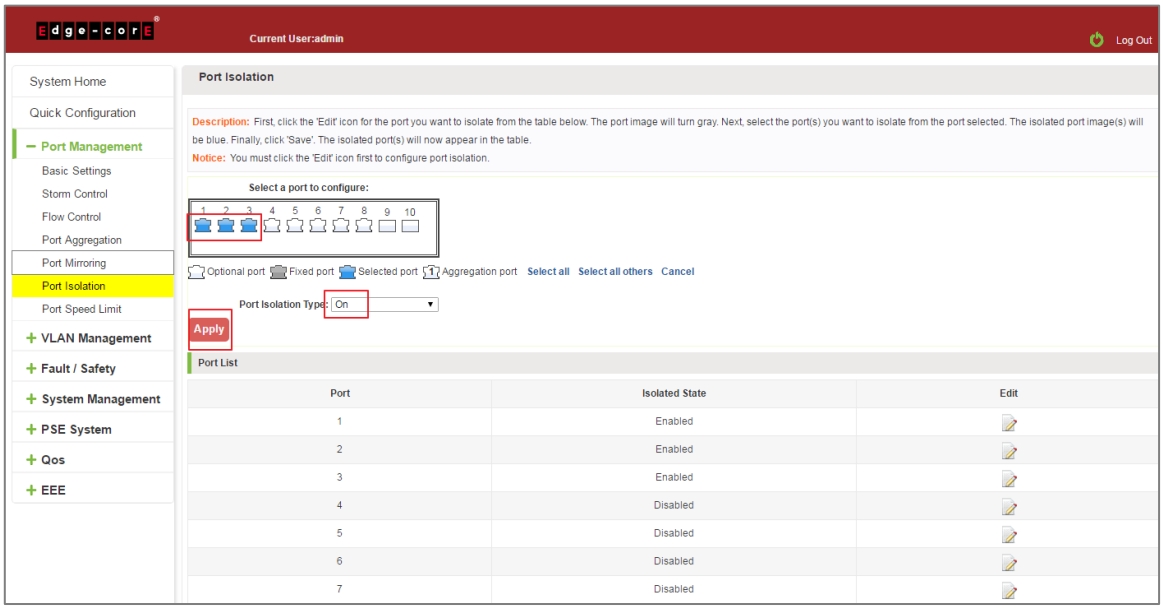


Figure 4-22: Enable Port Isolation Function

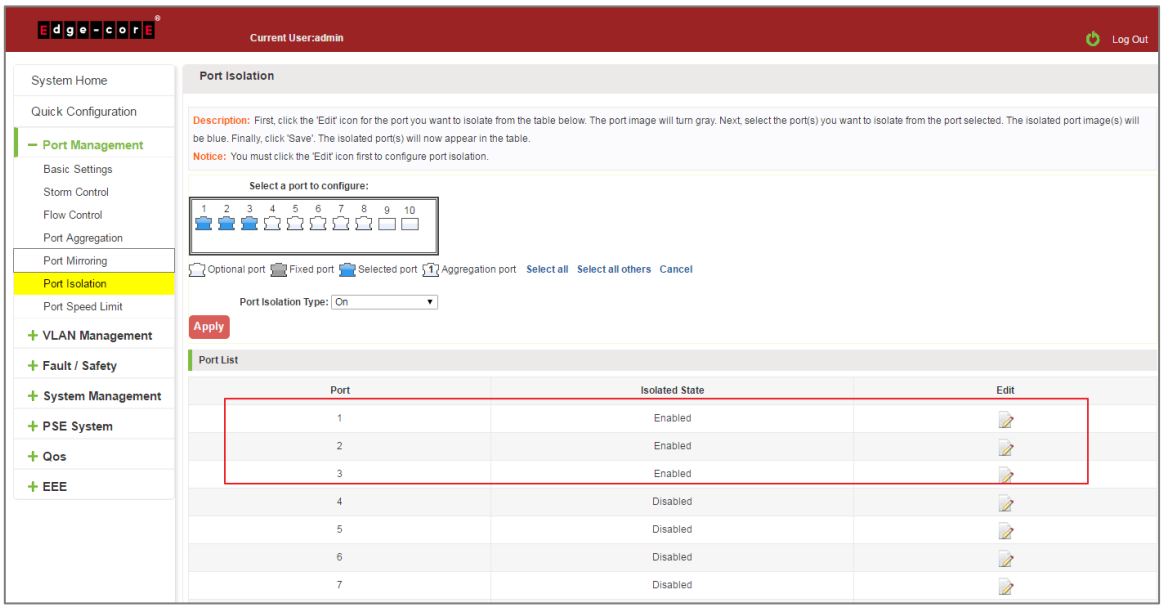


Figure 4-23: Enable Port Isolation Results

4.6.3 Modify the port isolation

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

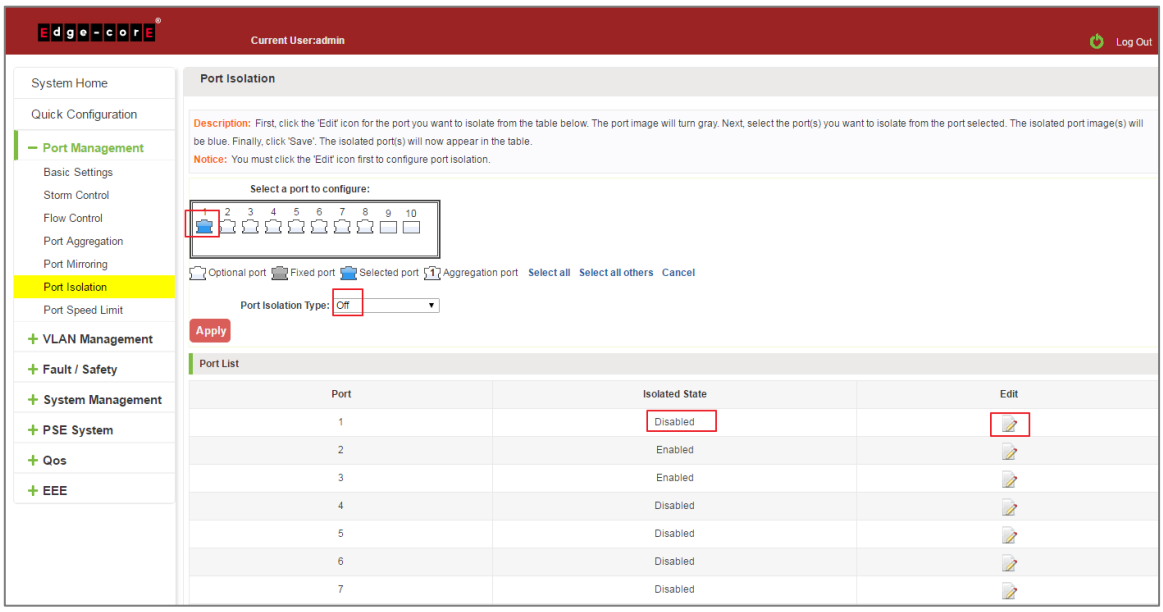


Figure 4-24: To Modify the Port Isolation

4.7 PORT SPEED LIMIT

4.7.1 View port rate limit

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

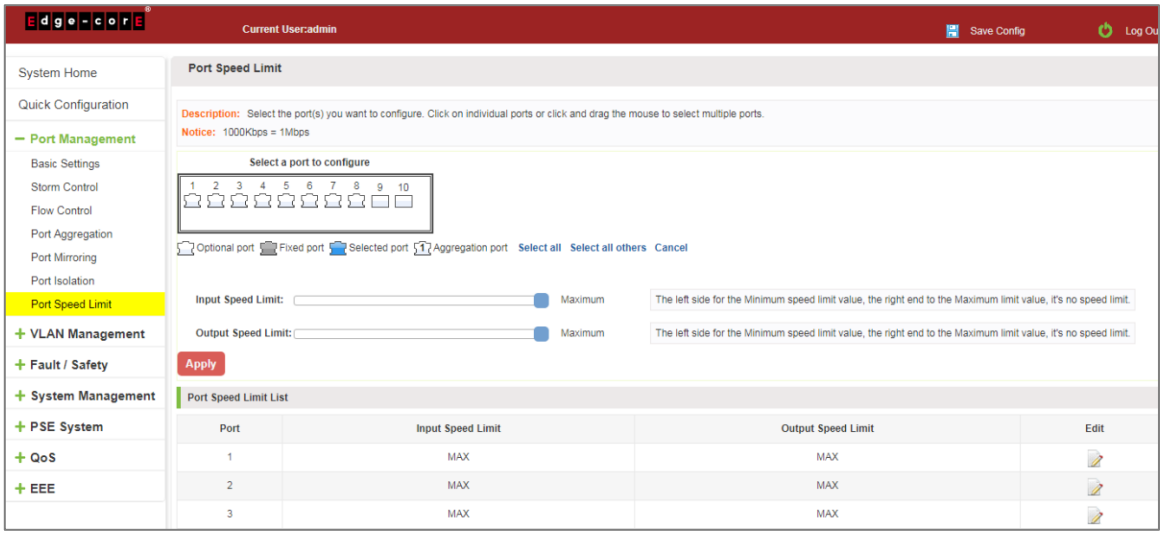


Figure 4-25: View Rate Configuration Information

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;

4.7.2 Configure port access rate

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

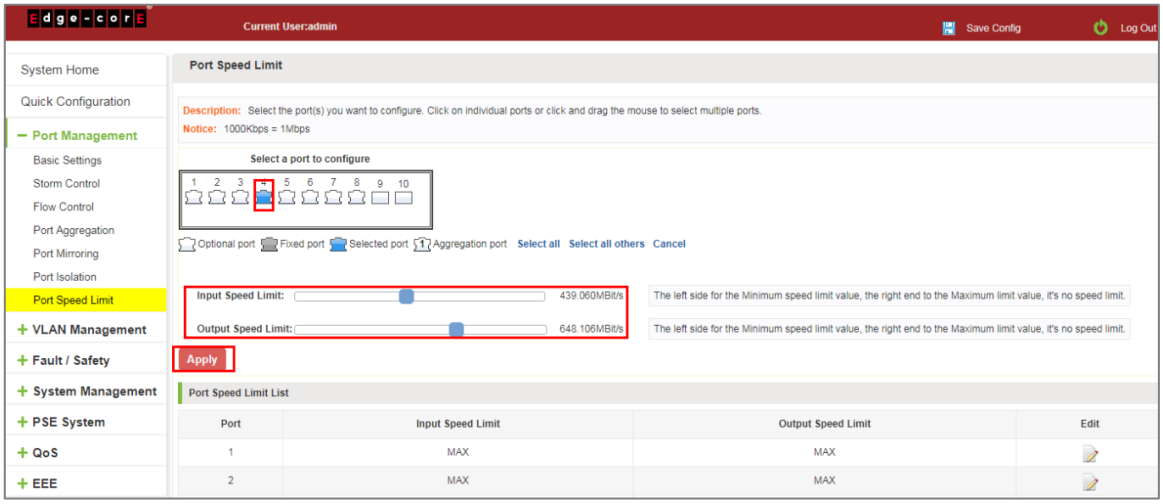


Figure 4-26: Configure Port Rate Limiting Entrance

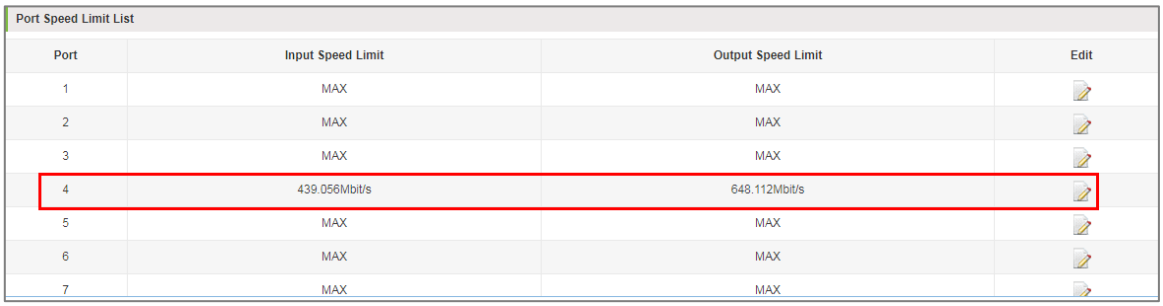


Figure 4-27: Port Entrance Speed Limit Results

Entrance port rate limiting configuration steps are as follows:

Step 1: Click on the right side of the port "  " Icon or select multiple icons;

Step 2: Set rate limiting strip port value;

Step 3: Click the lower right corner "Apply" button to complete the configuration.

4.7.3 Remove the port speed limit

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

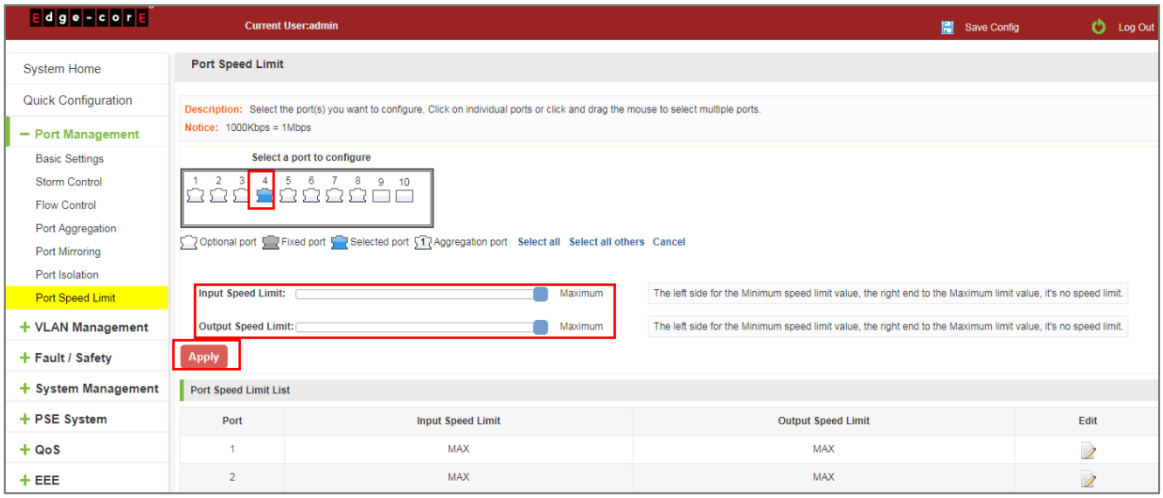


Figure 4-28: Remove the Port Speed Limit

Remove uplink port rate limiting steps are as follows:

Step 1: Click on the right side of the port  icon;

Step 2: In the area of the port rate configuration value rate strip pulled to the far right;

Step 3: Click the "Apply" button to complete the configuration.

4.8 SFP

4.8.1 View SFP Details

Click "Port Management" "SFP" to view the current information on installed SFP transceivers:

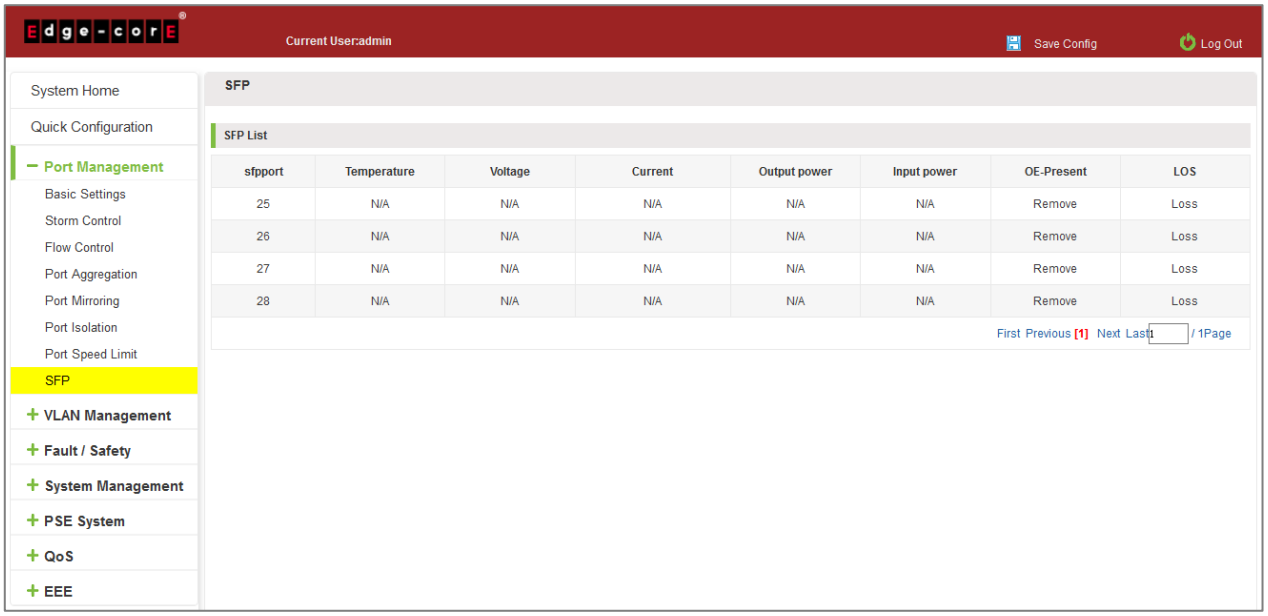


Figure 4-29: View SFP Information

5 VLAN MANAGEMENT

5.1 VLAN MANAGEMENT

5.1.1 Check VLAN configuration information

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

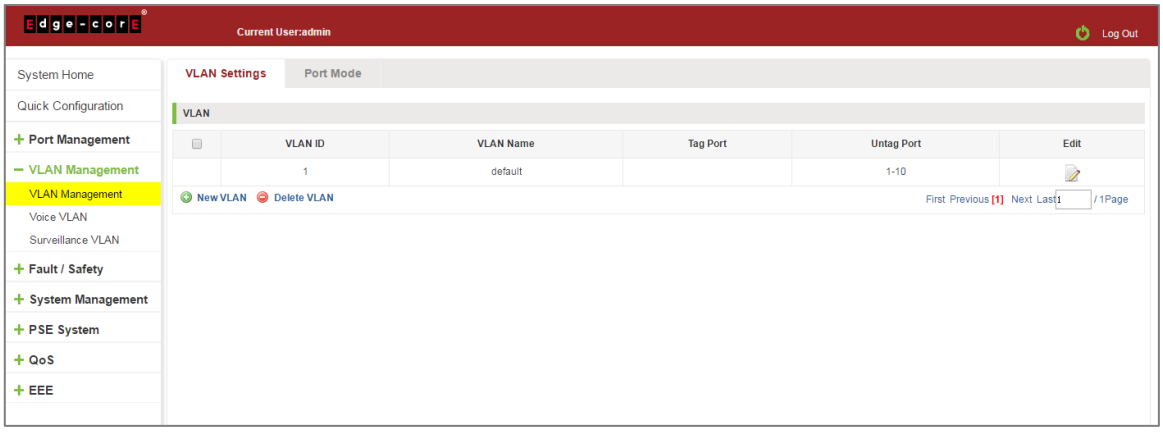


Figure 5-1: VLAN Configuration Information

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

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

5.1.2 Adding a VLAN

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

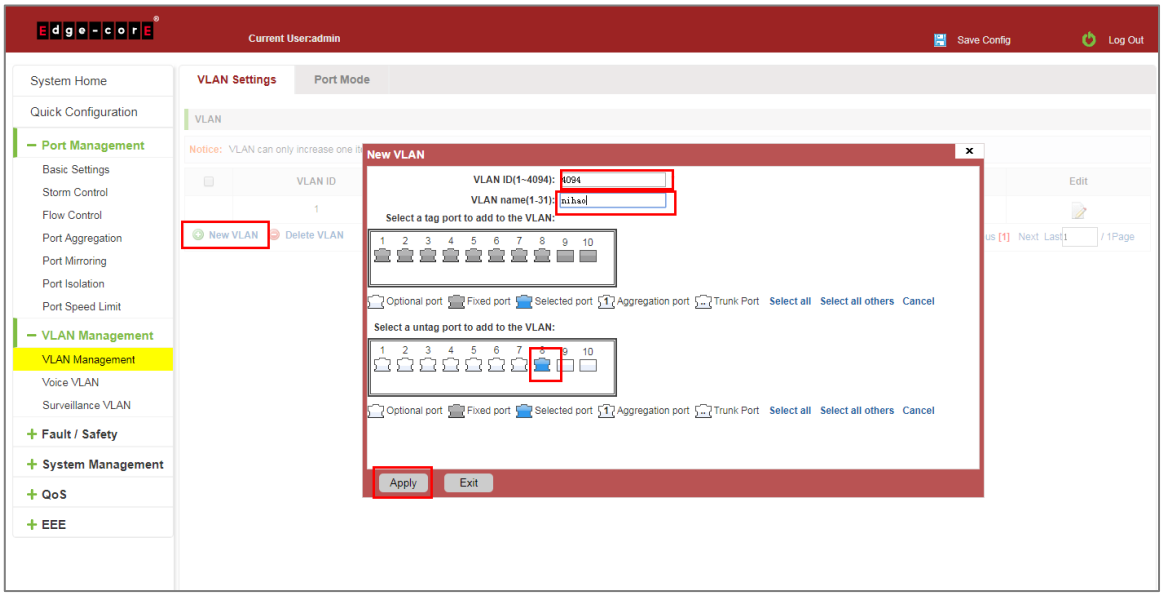


Figure 5-2: Adding a VLAN

Adding a VLAN, follow these steps:

Step 1: Click "New VLAN" connection;

Step 2: Value added VLAN VLAN ID of the page to fill in;

Step 3: Select the ports;

Step 4: Click the lower right corner "Apply" button to complete the configuration.

5.1.3 Remove VLAN

5.1.3.1 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.

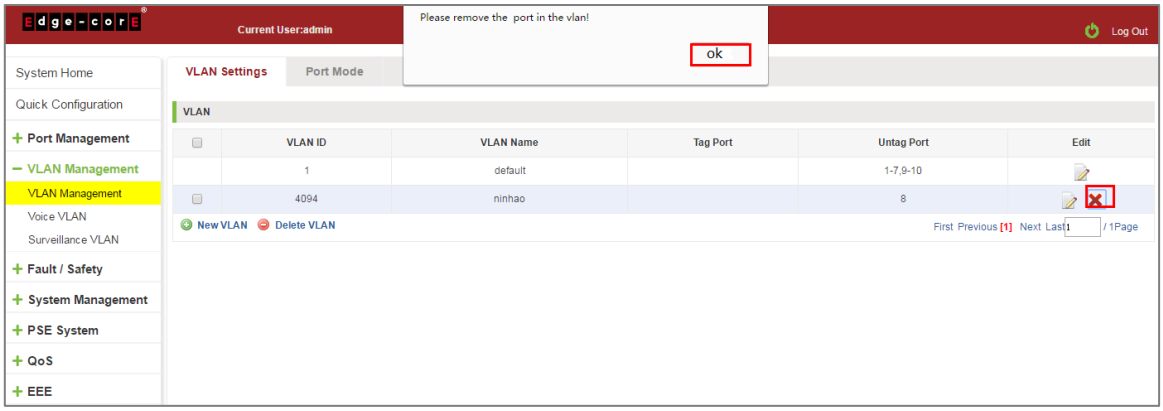


Figure 5-3: Delete a Single VLAN

5.1.3.2 Delete multiple VLAN

First select the VLAN you want to be deleted before the checkbox, then click "Delete VLAN" button to delete the selected VLAN, if the VLANs have some ports the VLAN can not be removed because of there are member ports. The others will be removed.

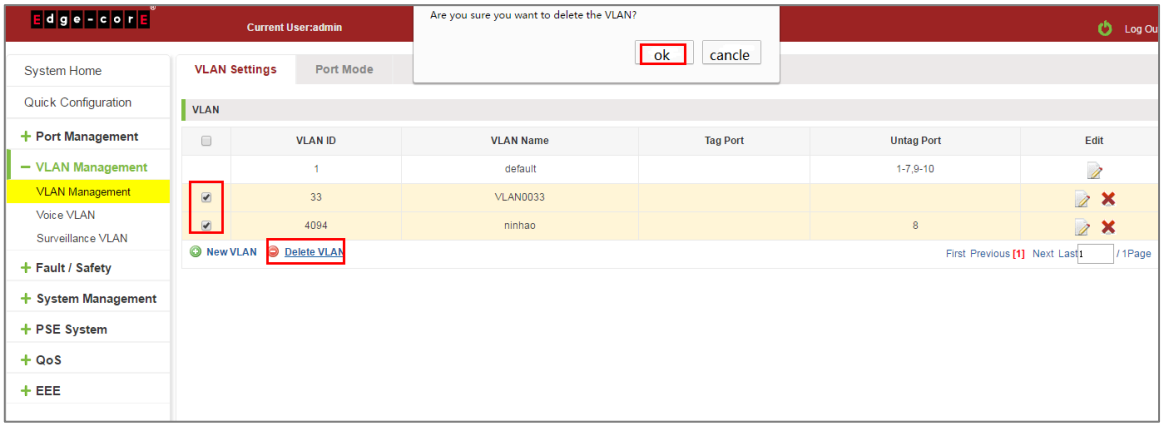


Figure 5-4: Delete Multiple VLAN

Delete multiple VLAN, follow these steps:

Step 1: I want to delete VLAN check box;

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

Step 3: Confirm delete.

5.1.4 Editing VLAN

5.1.4.1 VLAN port to a VLAN

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

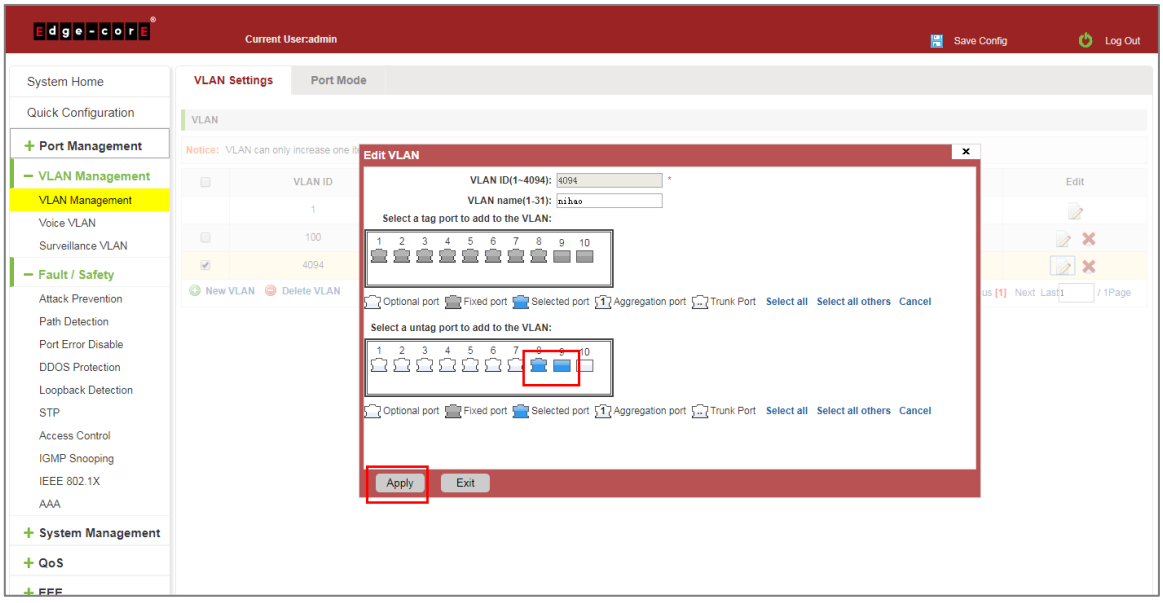


Figure 5-5: Add the Port to the VLAN

Add the port to the VLAN, follow these steps:

Step 1: Click" " "icon.

Step 2: Selected to join the ports in the port panel.

Step 3: Click the lower right corner "Apply" button to complete the configuration.

5.1.4.2 To remove the port from a VLAN

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

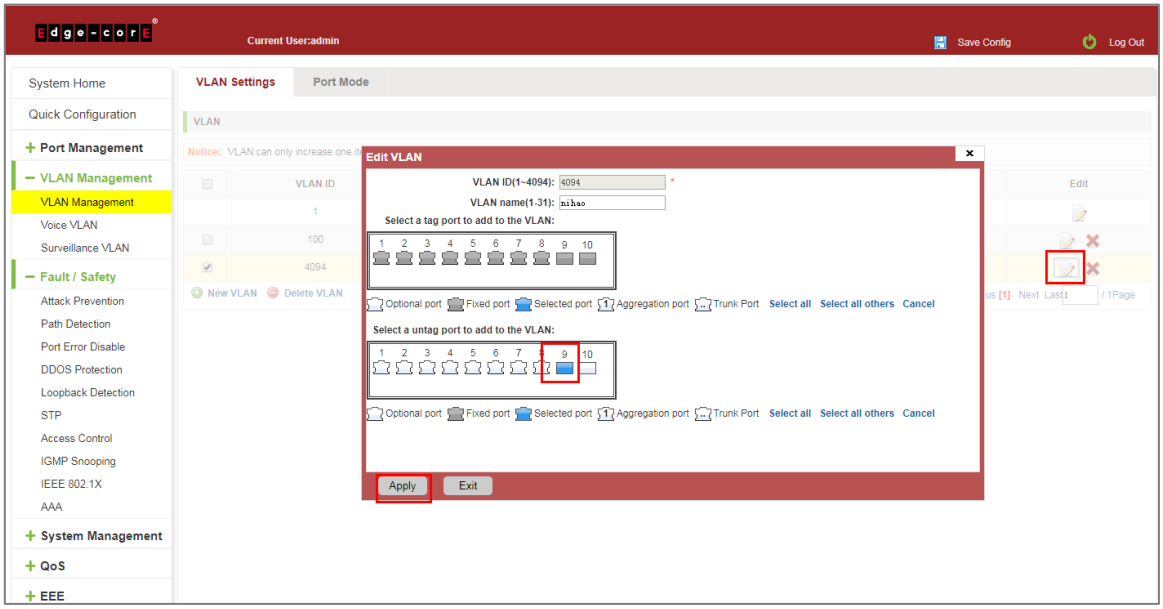


Figure 5-6: To Remove the Port from the VLAN

Procedure to remove the port from VLAN as follows:

Step 1: Click on the icon " ";

Step 2: Remove the port to be removed from the port panel;

Step 3: Click on the lower right corner of the "Apply" button to complete the configuration.

5.1.5 View port mode

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

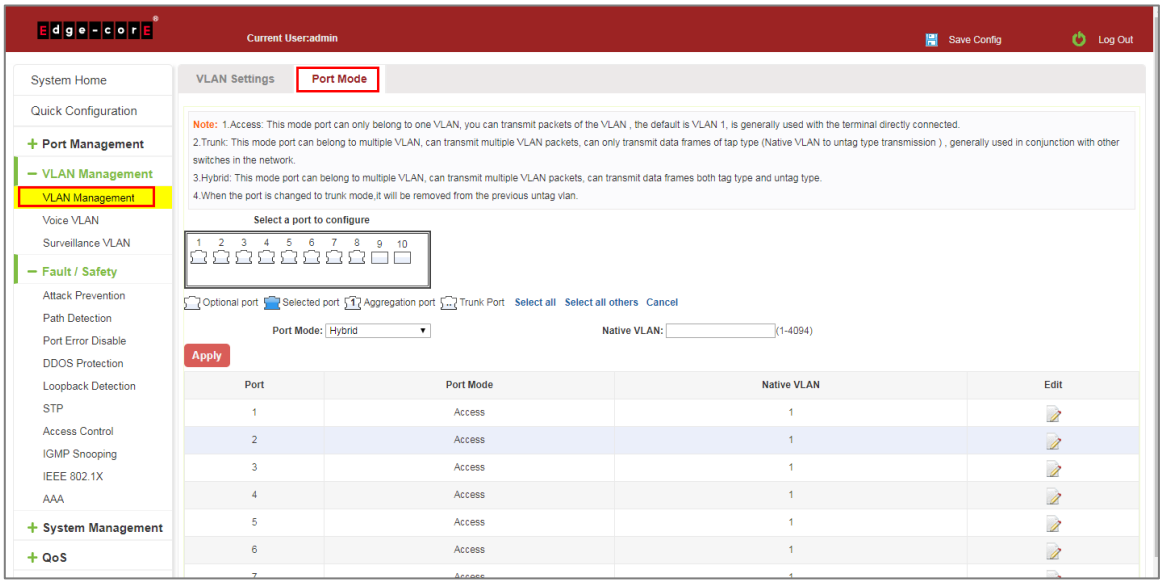


Figure 5-7: View Port Mode Configuration Information

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.

5.1.6 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:

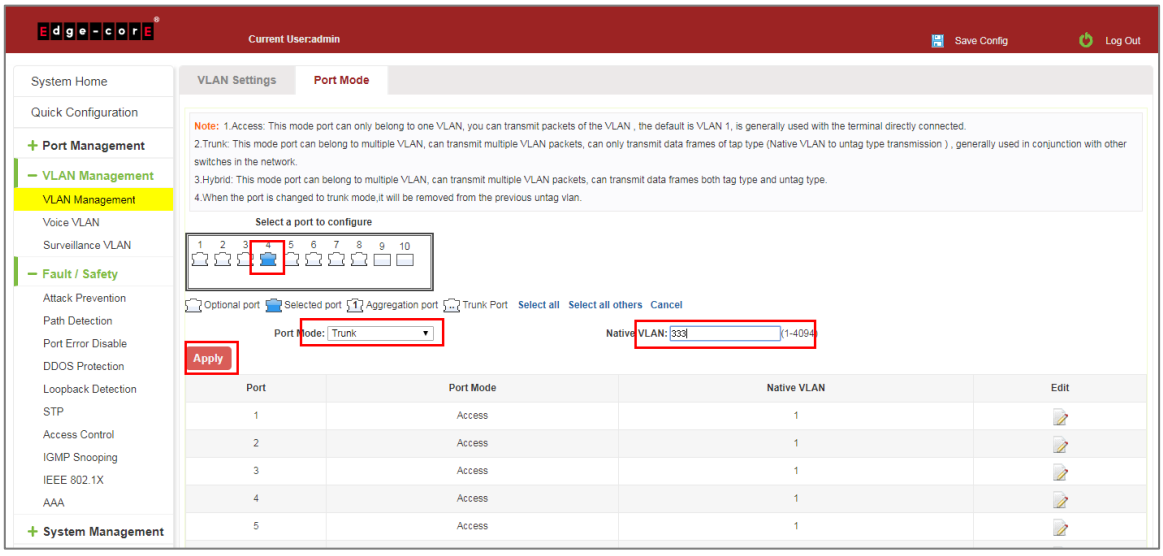


Figure 5-8: Change the Port Mode is Trunk

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

Step 1: Chose one or more ports;

Step 2: Click the port mode list chose the mode is: trunk;

Step 3: Set Native VLAN, the VLAN must be is exist;

Step 4: 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;

Step 5: Click on the lower right corner of the "Apply" button to complete the configuration.

5.1.7 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:

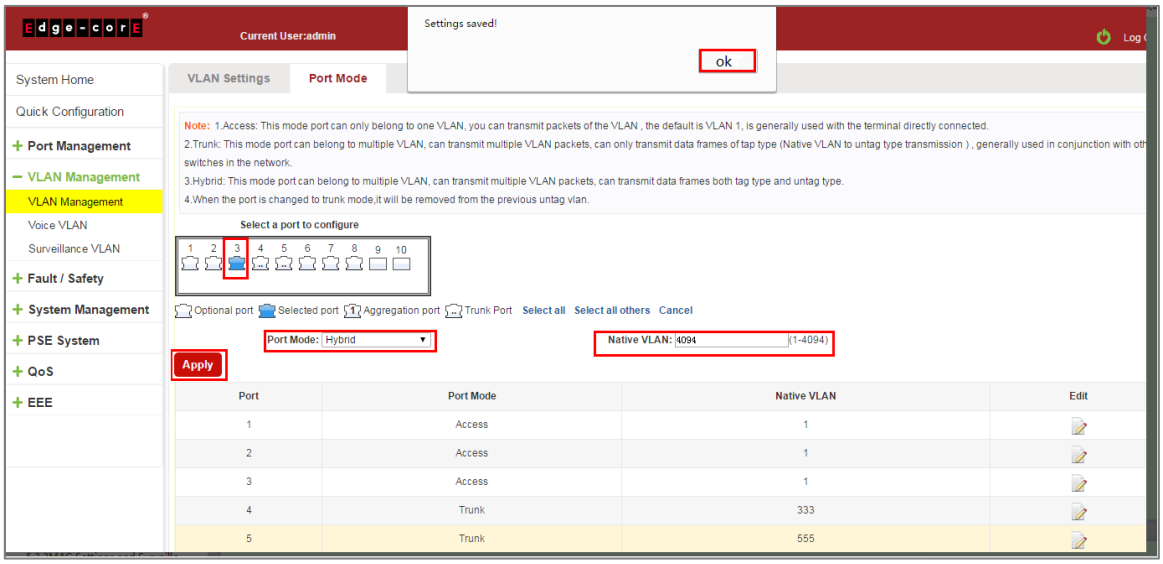


Figure 5-9: Change the Port Mode is Hybrid

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

Step 1: Chose one or more ports;

Step 2: Click the port mode list chose the mode is: hybrid;

Step 3: Set Native VLAN, the VLAN must be is exist;

Step 4: 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;

Step 5: Click on the lower right corner of the "Apply" button to complete the configuration.

5.2 VOICE VLAN

5.2.1 View voice VLAN information

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

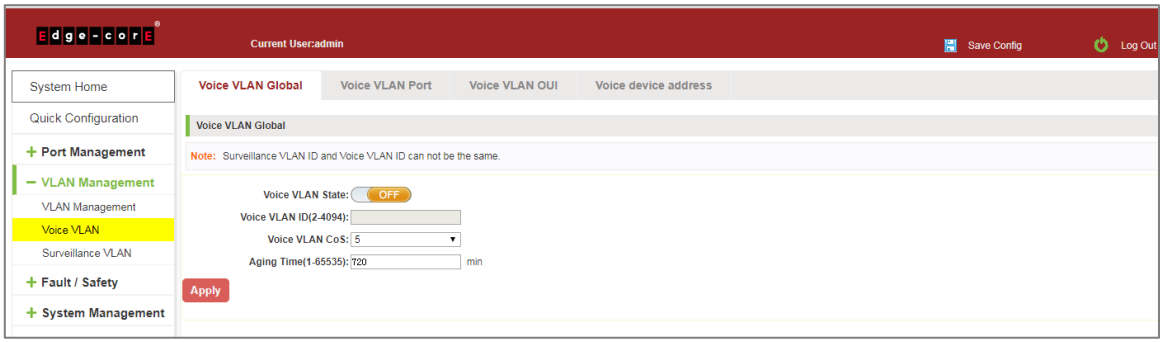


Figure 5-10: View Voice VLAN Information

5.2.2 Configure voice VLAN global

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

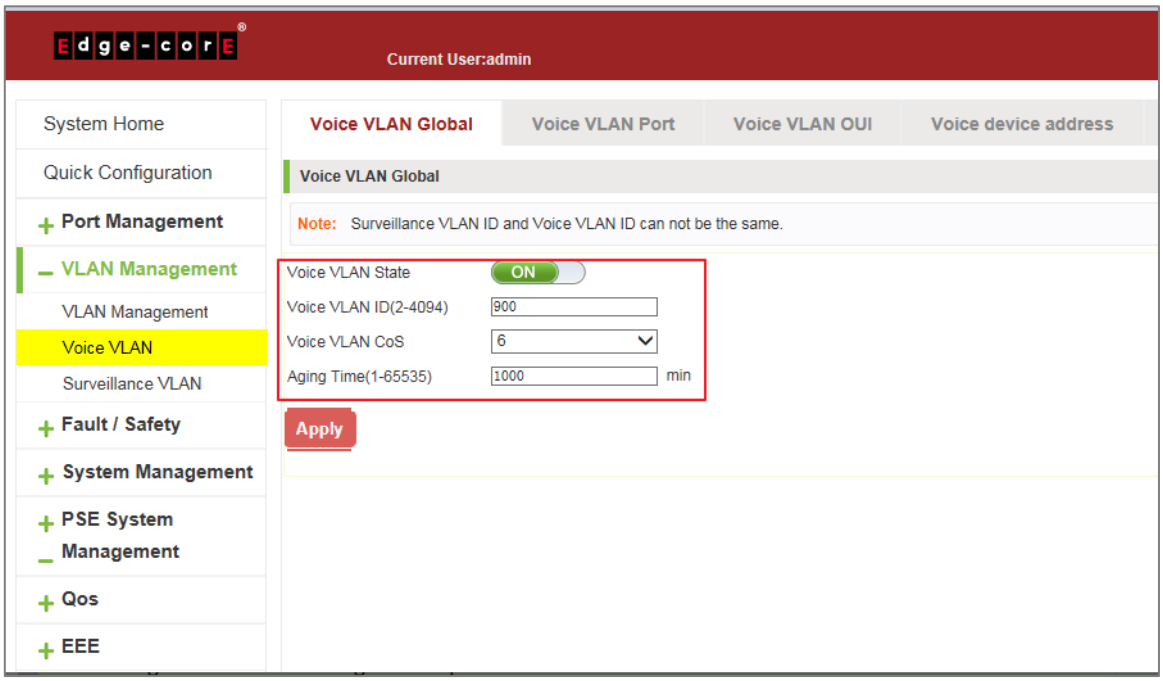


Figure 5-11: View Voice VLAN Information

To configure the voice VLAN global steps as follows:

Step 1: In the voice VLAN state TEXT BOX, click ON the "OFF" to "ON",

Step 2: In the voice VLAN ID text box, enter the ID, such as 900;

Step 3: In the voice VLAN COS text box, choose 6;

Step 4: In the aging time text box, enter aging time, such as 1000;

Step 5: Click "Apply".

5.2.3 Configure voice VLAN port

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

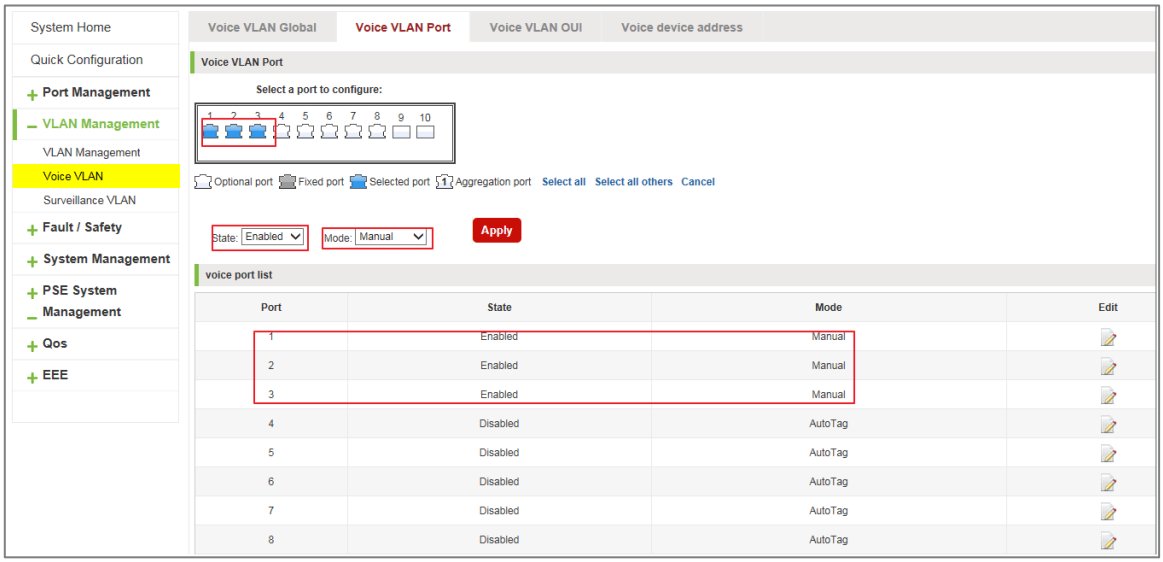


Figure 5-12: Configure Voice VLAN Port

To configure the voice VLAN port steps as follows:

Step 1: Select ports to configure,

Step 2: In the state text box, choose enable;

Step 3: In the mode text box, choose manual;

Step 4: Click "Apply".

5.2.4 Configure voice VLAN OUI

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

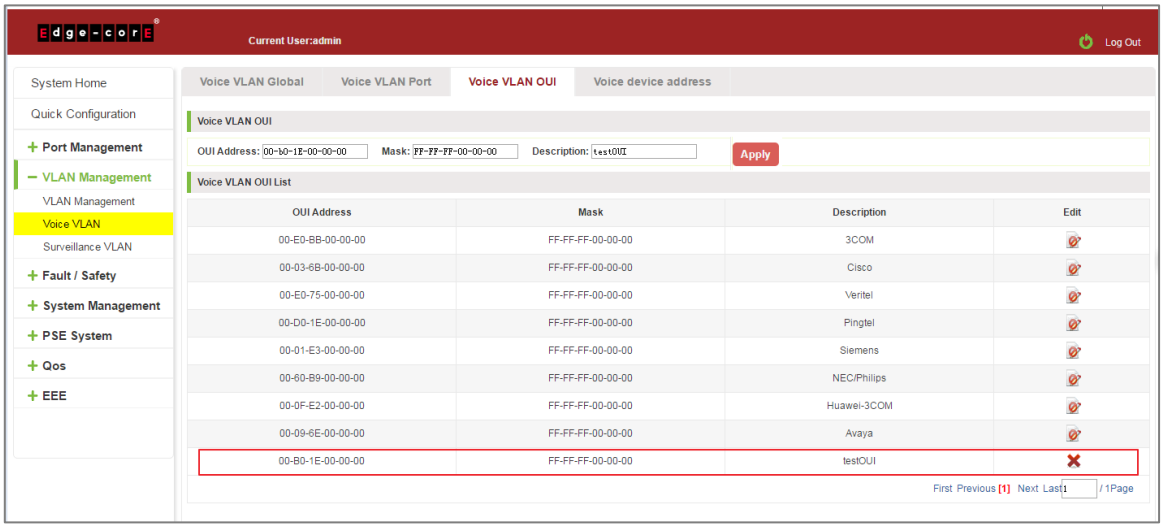


Figure 5-13: Configure Voice VLAN OUI

To configure the voice VLAN OUI steps as follows:

Step 1: In the OUI address text box, enter OUI address, such as 00-b0-1E-00-00-00;

Step 2: In the mask text box, enter the mask, such as FF-FF-FF-00-00-00;

Step 3: In the description text box, enter the description, such as testOUI;

Step 4: Click "Apply".

5.2.5 Voice device address

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

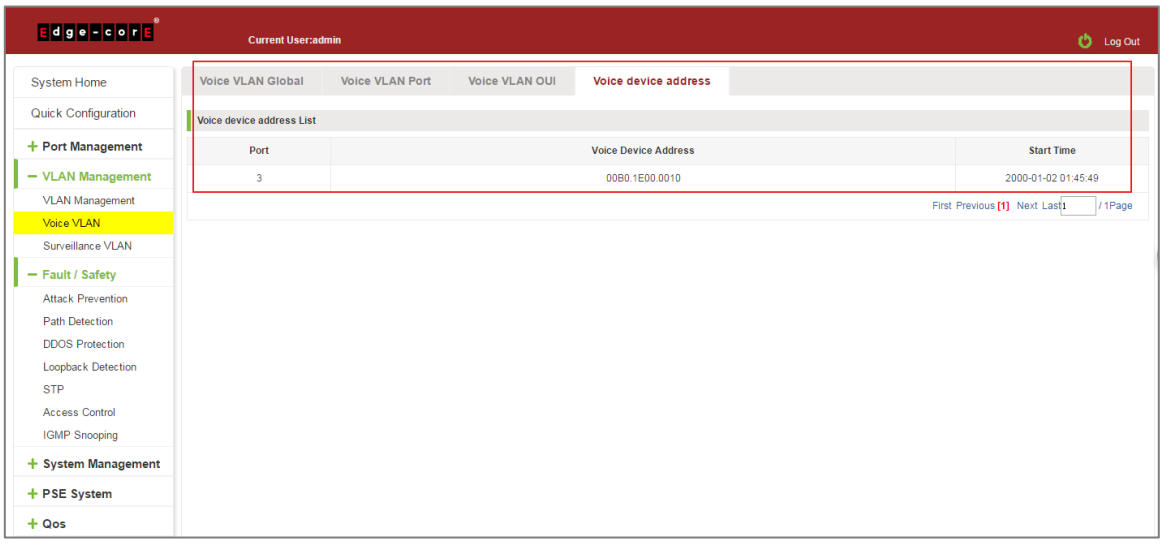


Figure 5-14: Voice VLAN Address

5.3 SURVEILLANCE VLAN

5.3.1 View surveillance VLAN information

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

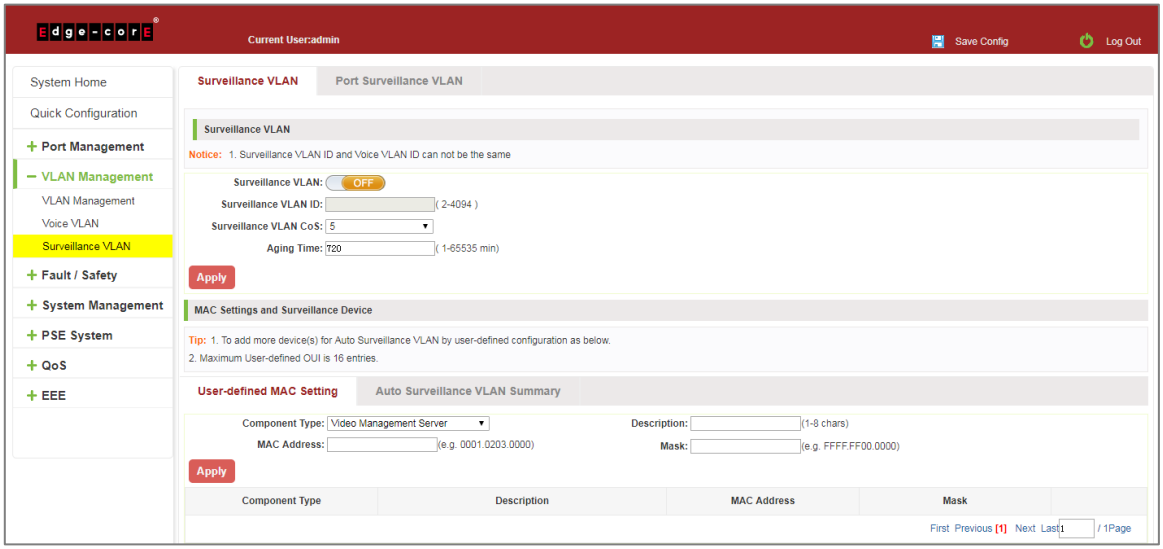


Figure 5-15: Surveillance VLAN Information

5.3.2 Configure surveillance VLAN

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

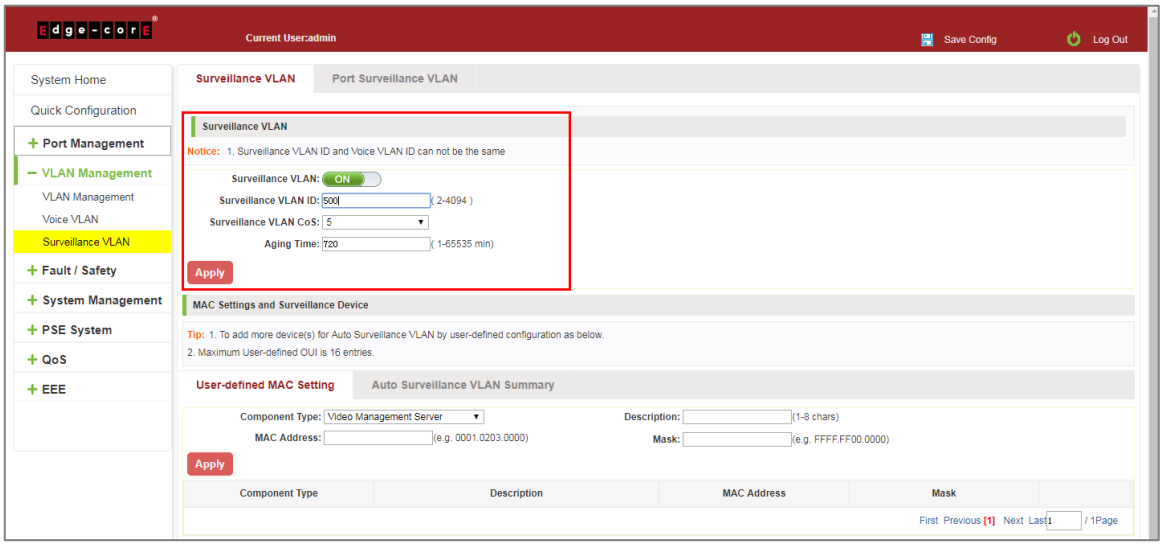


Figure 5-16: Configure Surveillance VLAN

To configure the surveillance VLAN steps as follows:

Step 1: In the surveillance VLAN TEXT BOX, click ON the "OFF" to "ON",

Step 2: In the surveillance VLAN ID text box, enter the ID, such as 500;

Step 3: In the surveillance VLAN COS text box, choose 3;

Step 4: In the aging time text box, enter aging time, such as 500;

Step 5: Click "Apply".

5.3.3 MAC settings and surveillance device

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

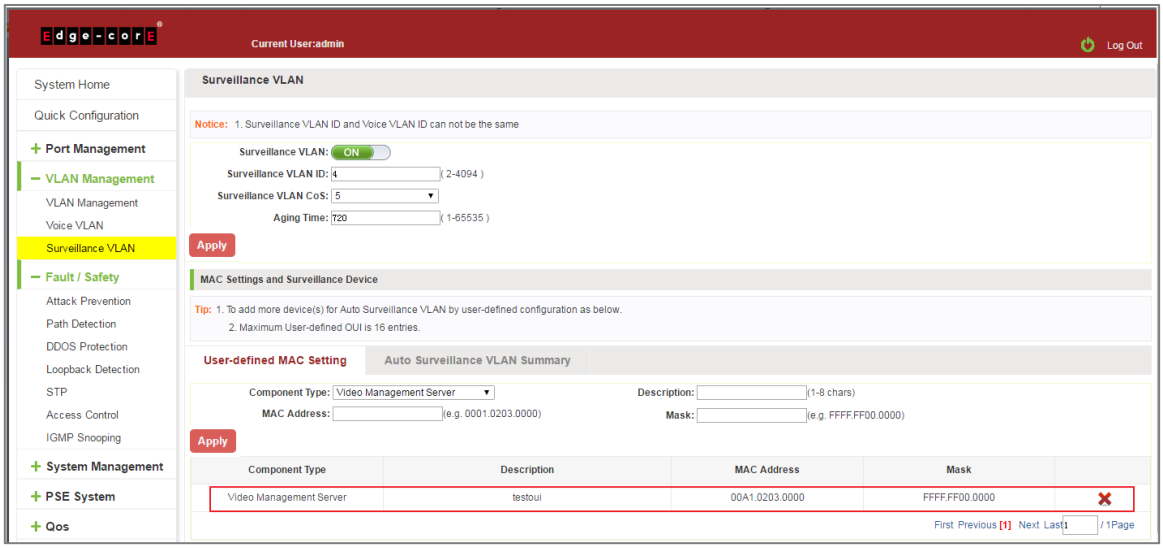


Figure 5-17: Configure the User-defined MAC Settings

To configure the surveillance VLAN steps as follows:

Step 1: In the component type EXT BOX, choose video management server;

Step 2: In the description text box, enter testOUI;

Step 3: In the MAC address text box, enter MAC address, such as 00A1.0203.0000.

Step 4: In the mask text box, enter the mask, such as FFFF.F000.000,

Step 5: Click "Apply".

5.3.4 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:

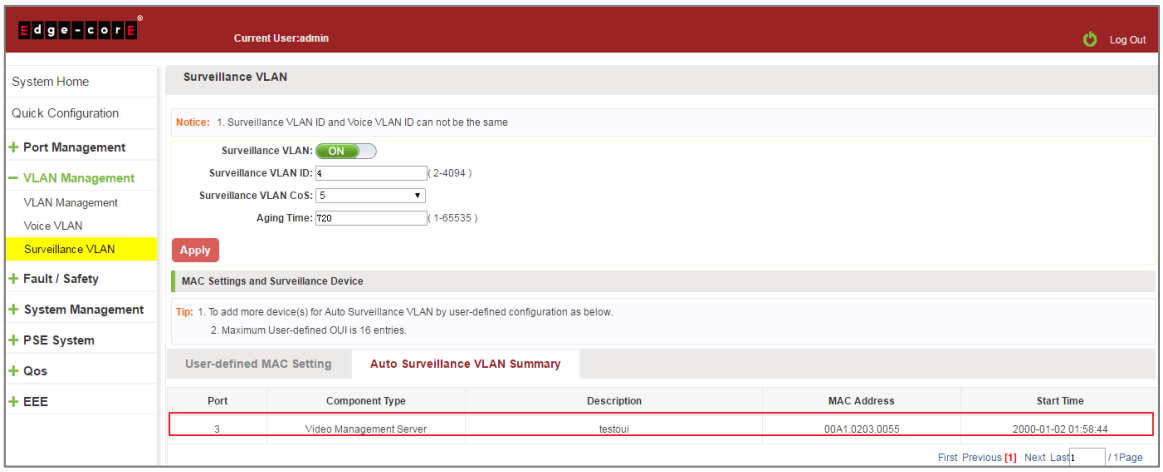


Figure 5-18: Configure the User-defined MAC Settings

5.4 ONVIF

5.4.1 View ONVIF Information

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

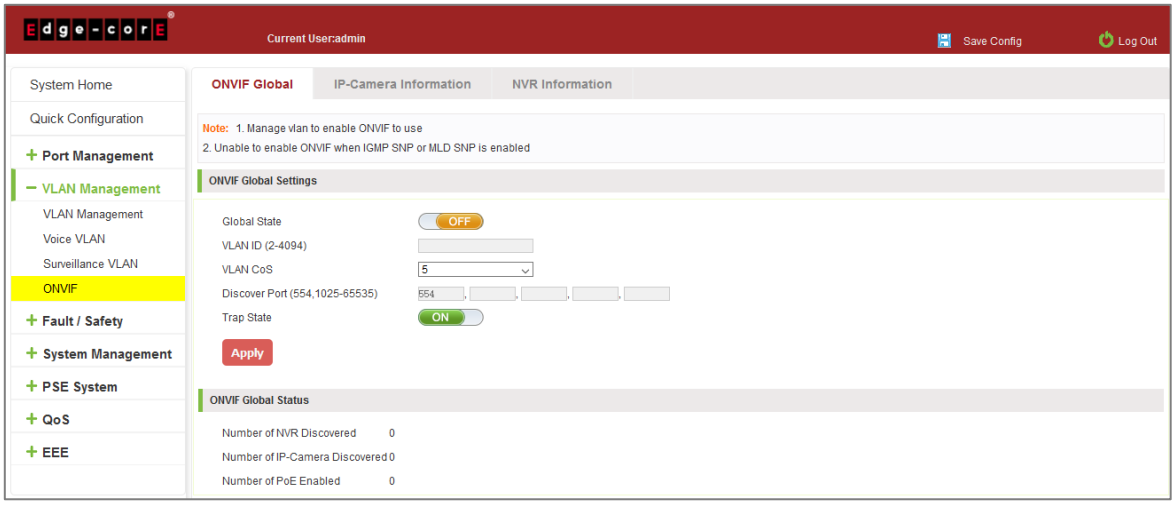


Figure 5-19: ONVIF Information

To configure ONVIF, follow these steps:

Step 1: Turn off the IGMP and MLD functions.

Step 2: Enable the Management VLAN. (Confirm that the switch management IP address is in the same segment as the IP cameras and NVRs.)

Step 3: Configure the ONVIF VLAN ID.

Step 4: Configure the port number used by the ONVIF protocol. The default is 554.

Step 5: Set the ONVIF Global State to “ON.”

Step 6: Click "Apply".

5.4.2 View IP-Camera Information

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

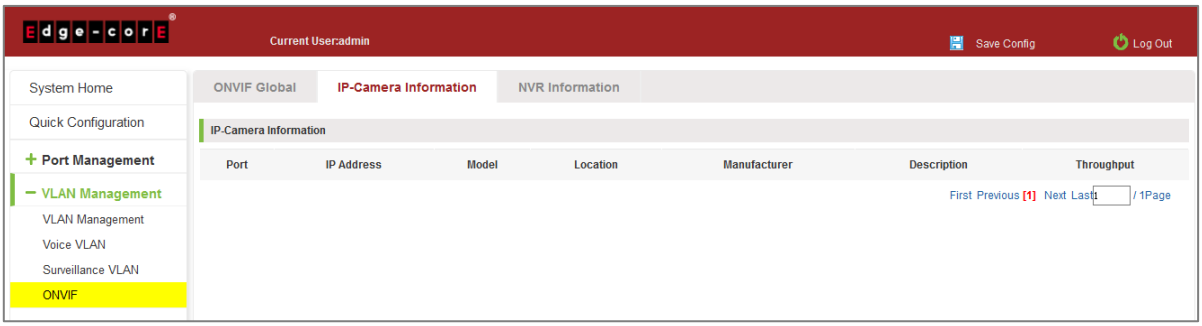


Figure 5-20: IP-Camera Information

5.4.3 View NVR Information

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

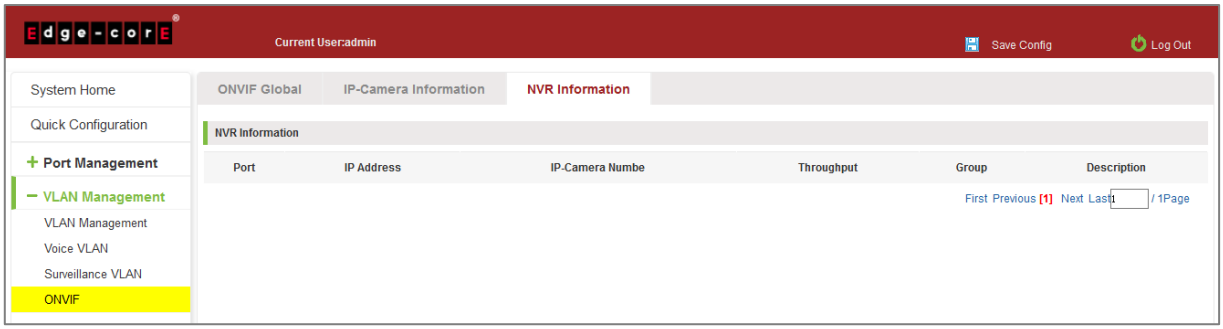


Figure 5-21: NVR Information

6 FAULT/SAFETY

6.1 ATTACK PREVENTION

6.1.1 ARP snooping

6.1.1.1 View ARP configuration

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

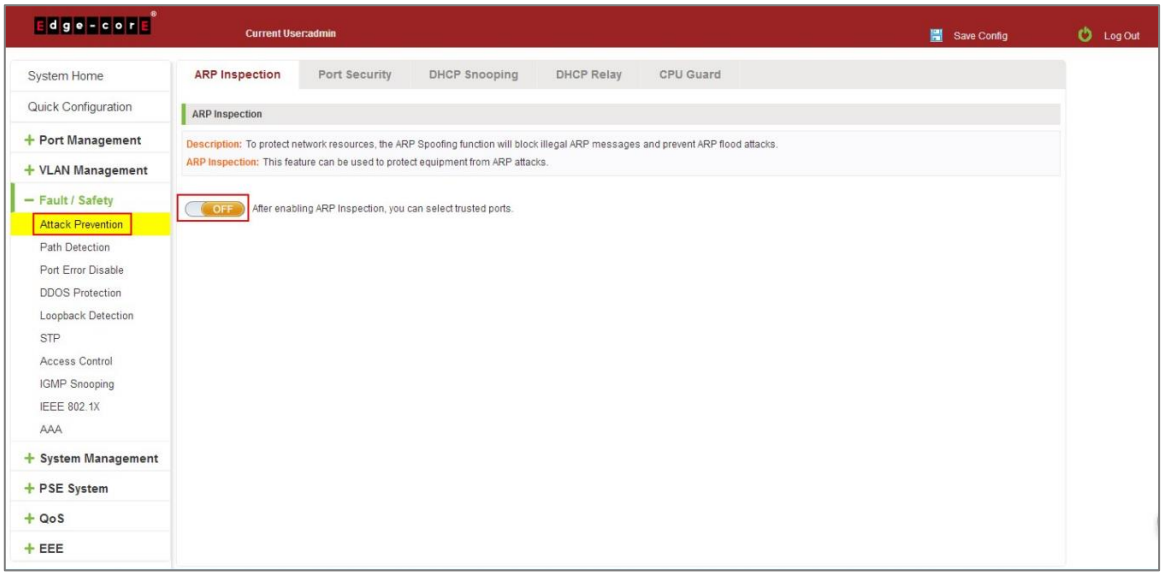


Figure 6-1: View Port ARP Inspection Information

6.1.1.2 ARP inspection function

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

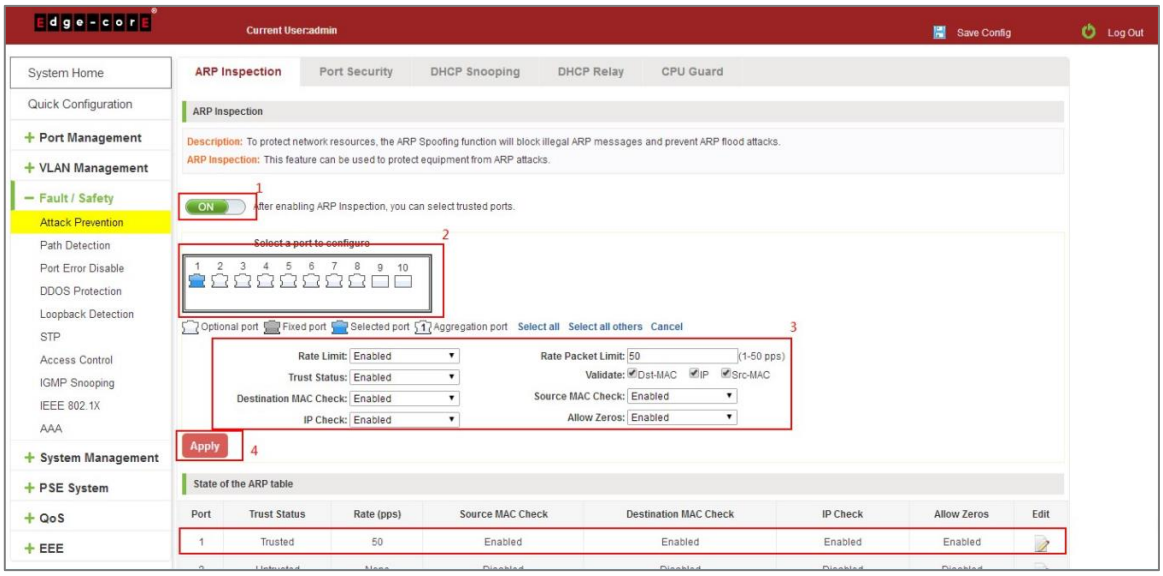


Figure 6-2: ARP Inspection Configuration

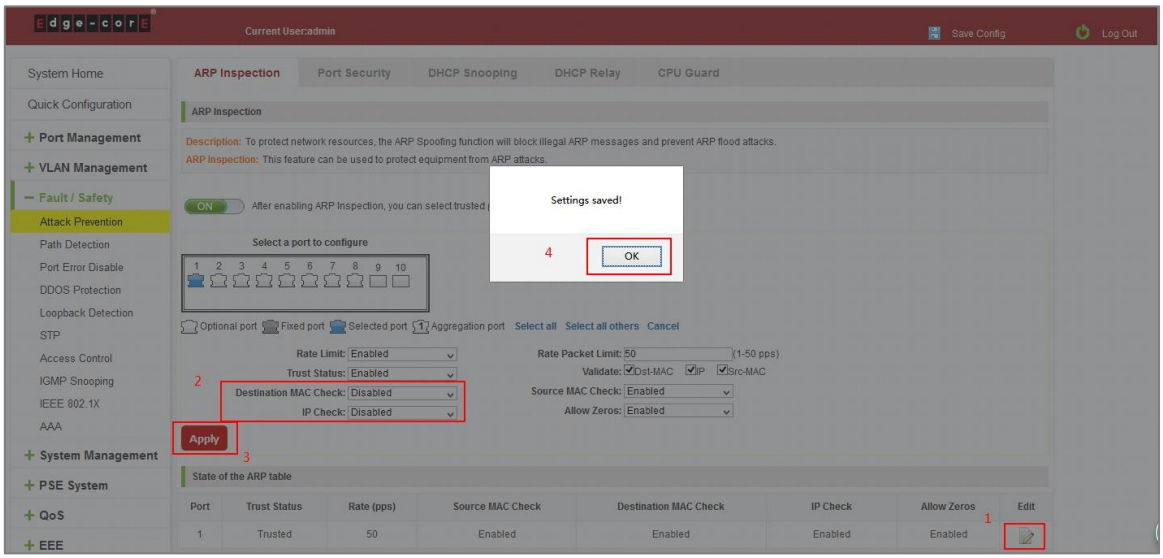


Figure 6-3: Change ARP Inspection Configure

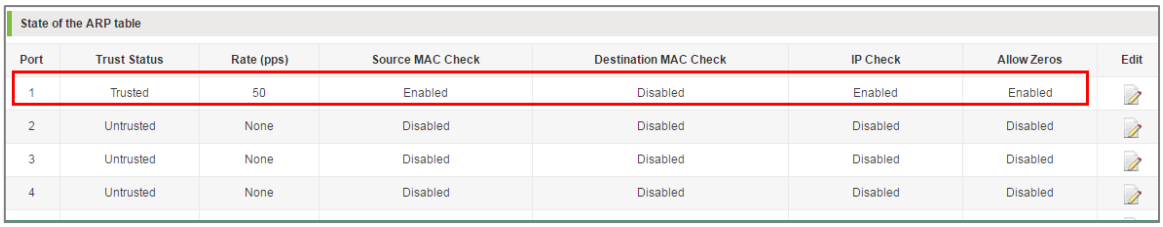


Figure 6-4: Change ARP Inspection Configure Success

6.1.1.3 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.

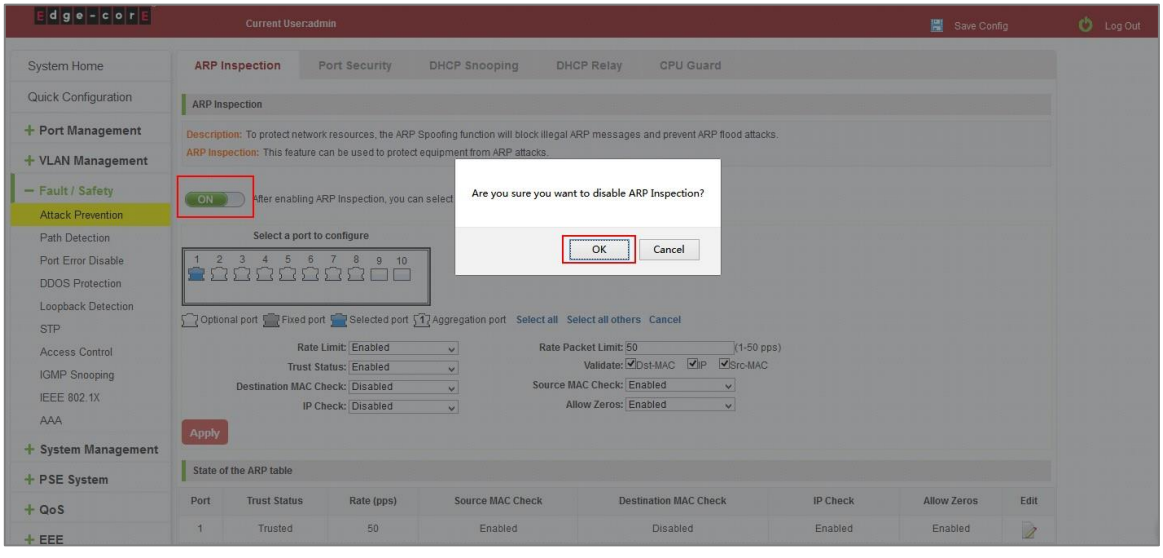


Figure 6-5: Disable ARP Inspection Function

6.1.2 Port security

6.1.2.1 Configuration port security

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

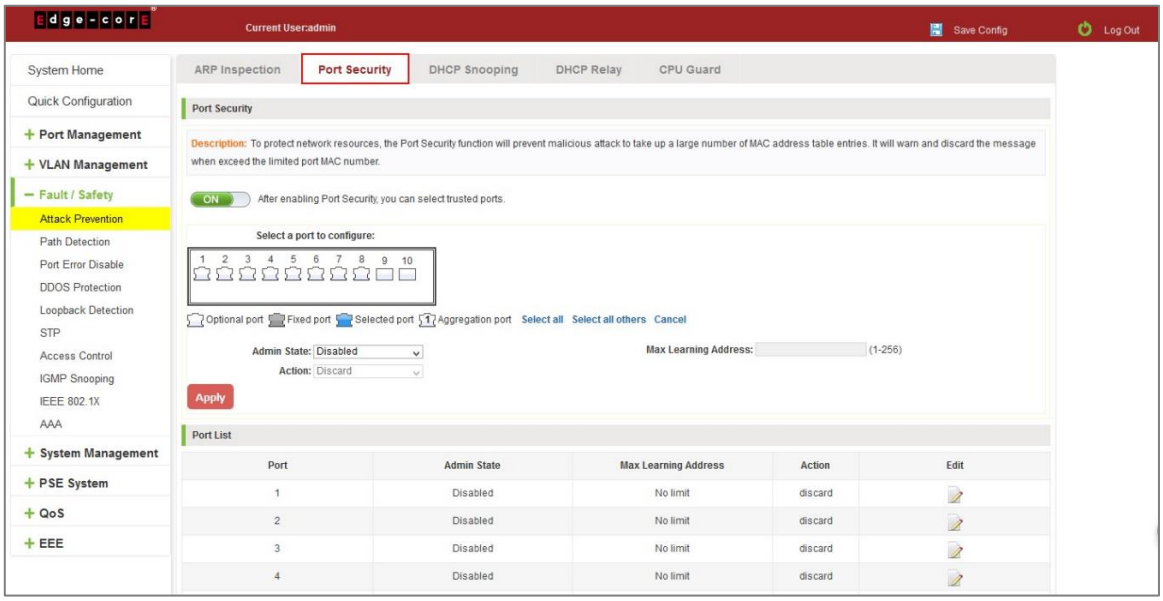


Figure 6-6: Port security configuration

In the configuration page, selected one or more ports, enable the admin state and configure the port max learning address. Then, click "Save" button.

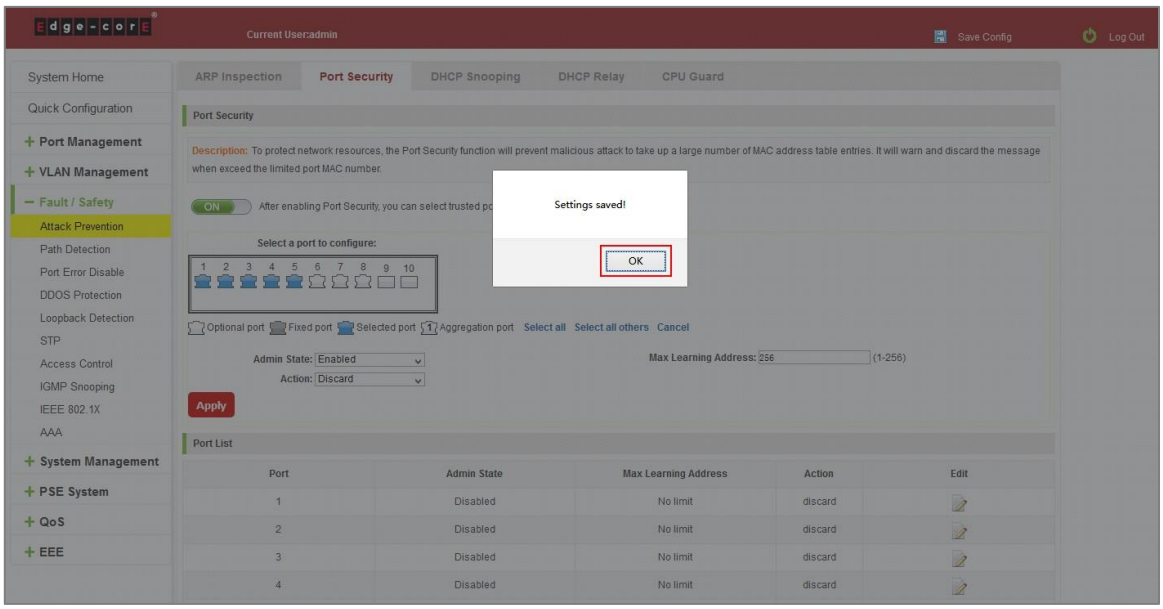


Figure 6-7: Port Security Manual Configuration

6.1.2.2 Change port security status

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

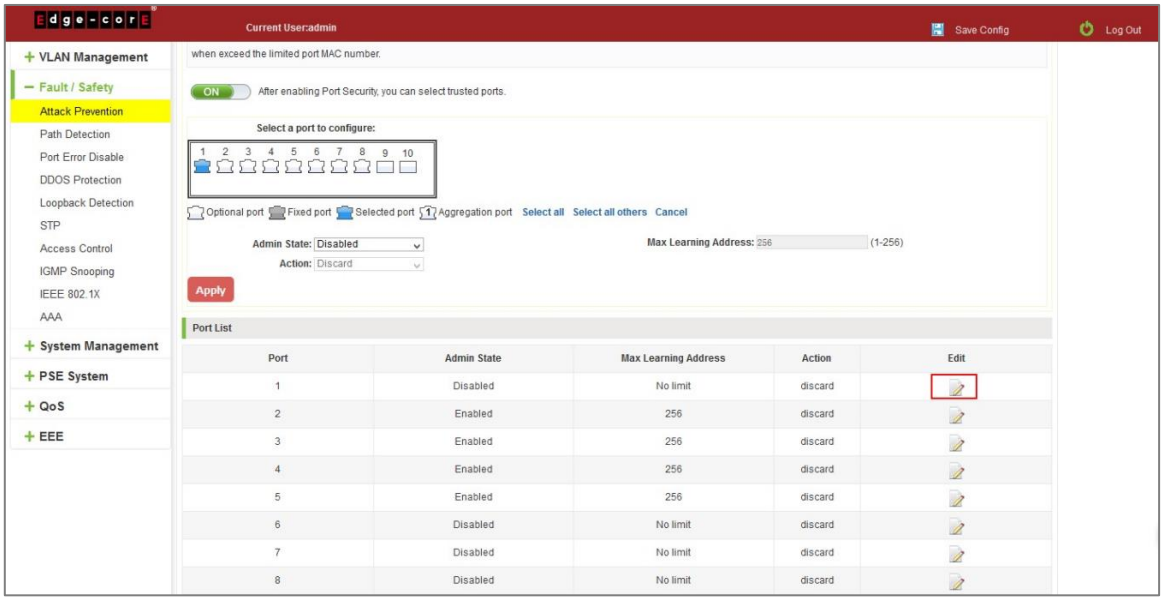


Figure 6-8: Change Port Security Status

6.1.3 DHCP snooping

6.1.3.1 View DHCP snooping configuration

Click the "Fault/Safety" "Attack Prevention" "DHCP Snooping", the configuration information show the anti DHCP attack:

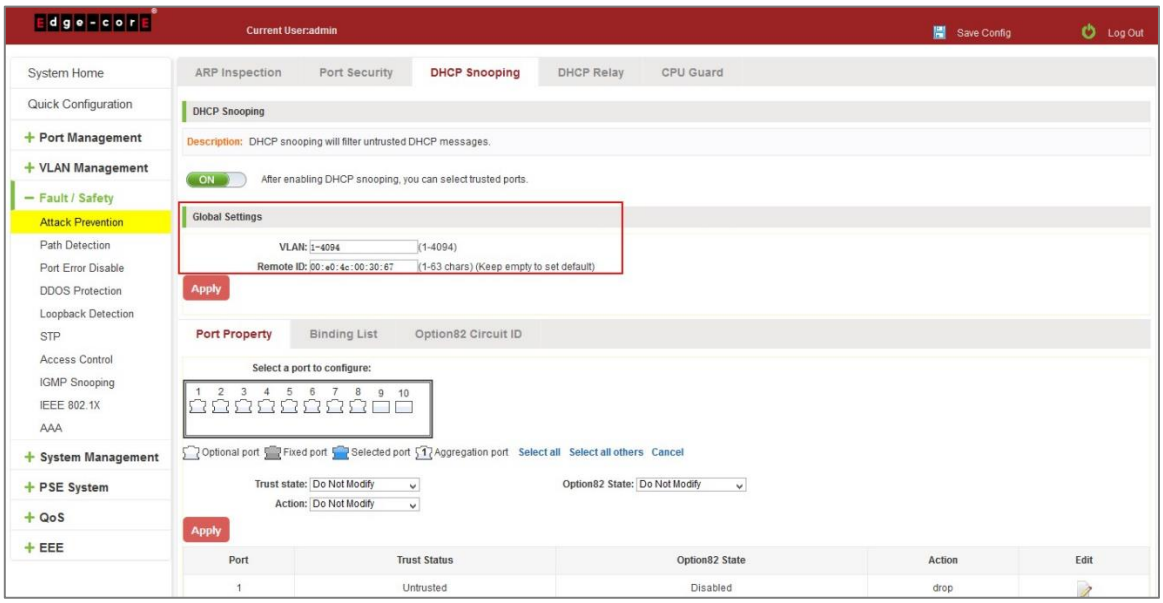


Figure 6-9: View Anti DHCP Snooping Configuration Information

Display refresh configuration information.

6.1.3.2 Open DHCP snooping function

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

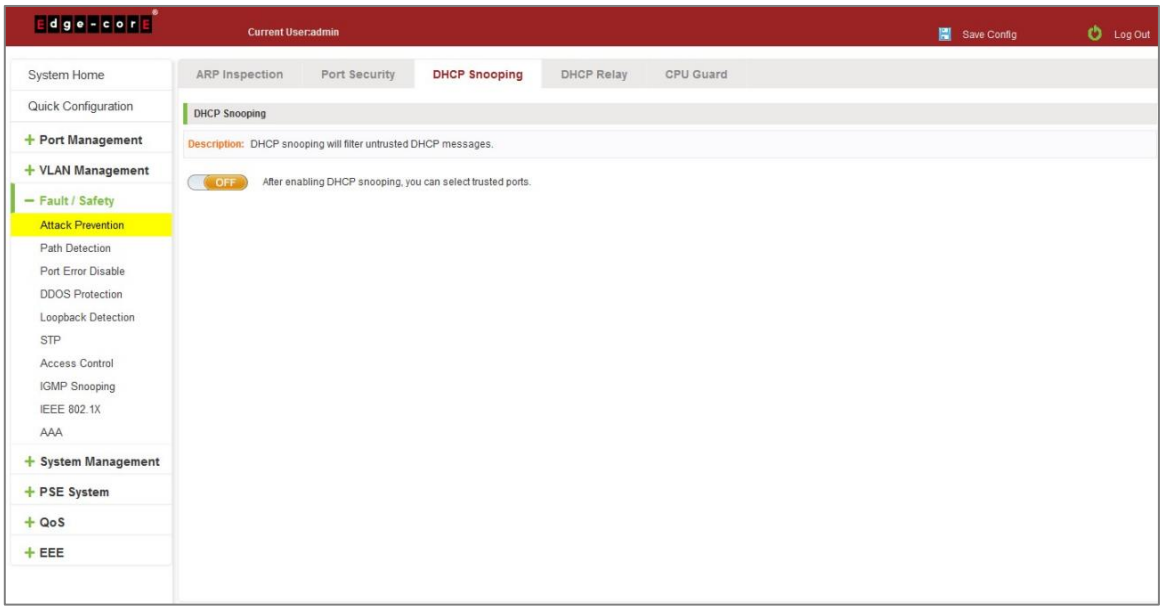


Figure 6-10: Activation of DHCP Snooping Function

6.1.3.3 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.

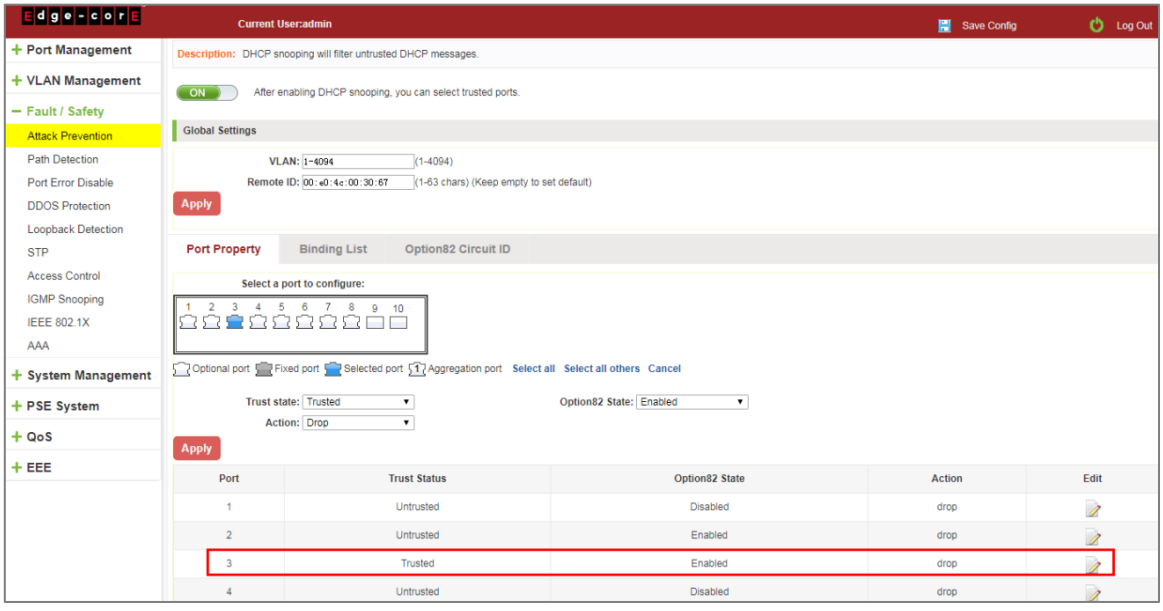


Figure 6-11: Disable Anti-Illegal DHCP Server Functions and Enable Option 82

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.

6.1.3.4 The trusted port gets the IP address

Click "Binding List" to view the list information.

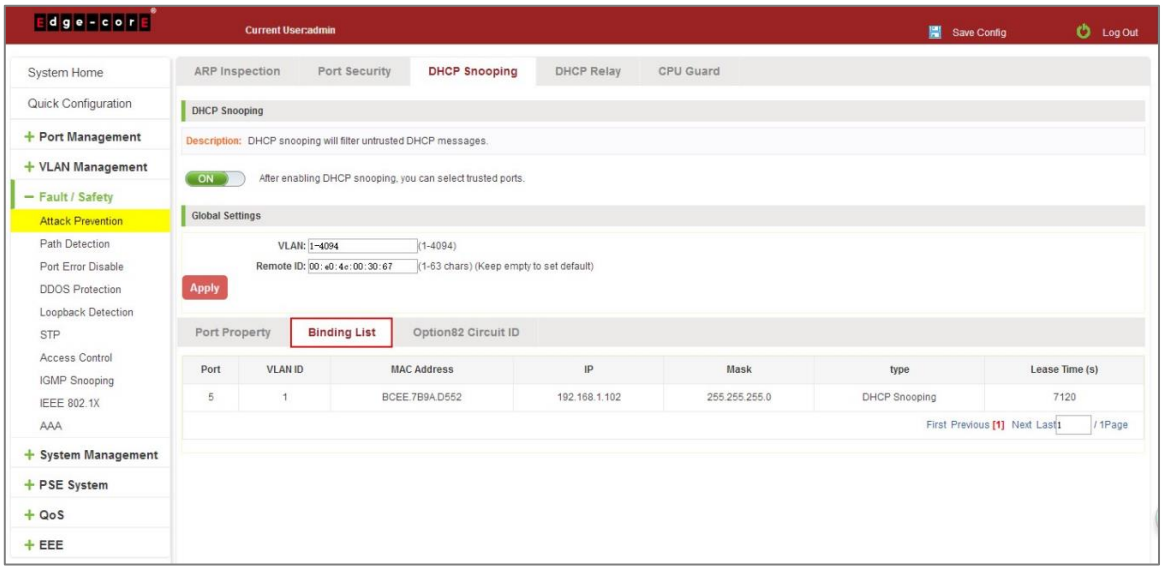


Figure 6-12: View the IP Address that the Trusted Port Gets

6.1.3.5 Configure CID information

Click the "Option82 Circuit ID" button, configure the CID information:

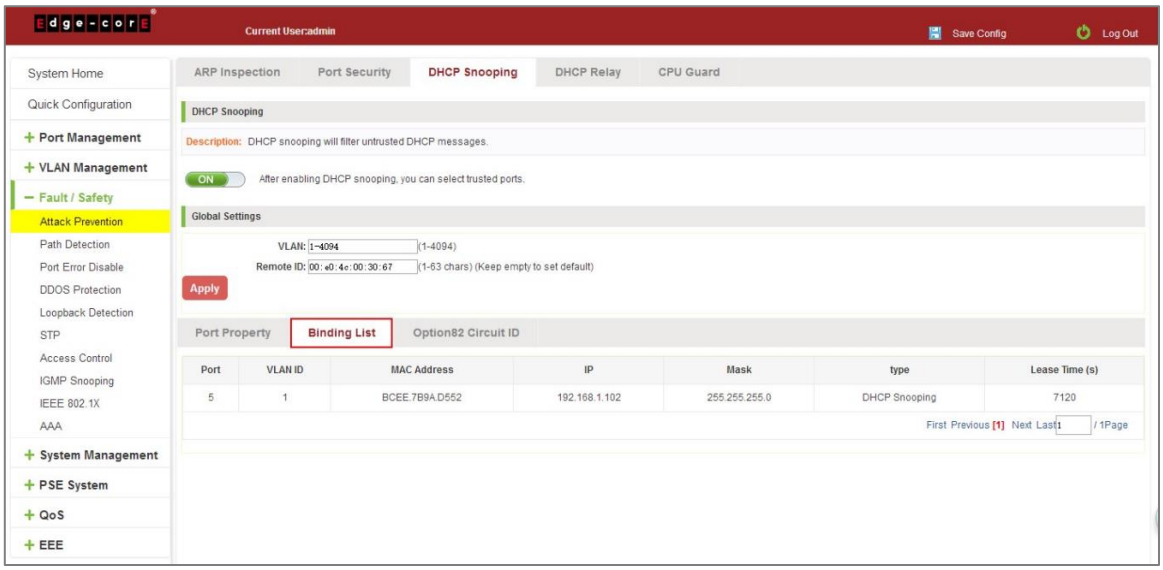


Figure 6-13: CID Information

6.1.3.6 Off DHCP snooping function

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

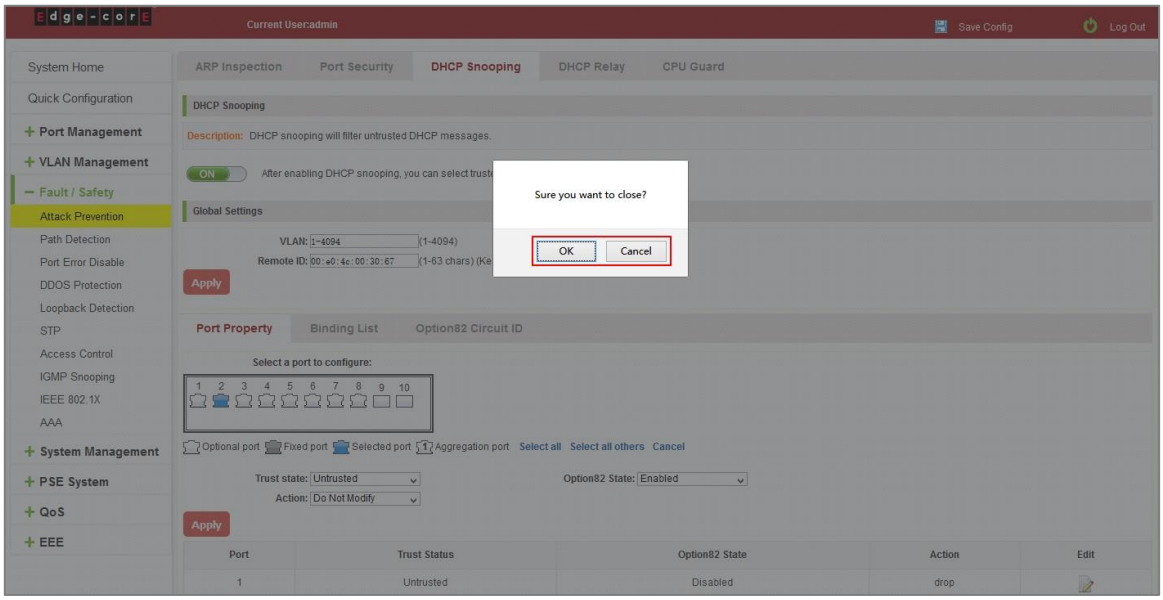


Figure 6-14: Off DHCP Snooping Function

6.1.4 CPU Guard

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

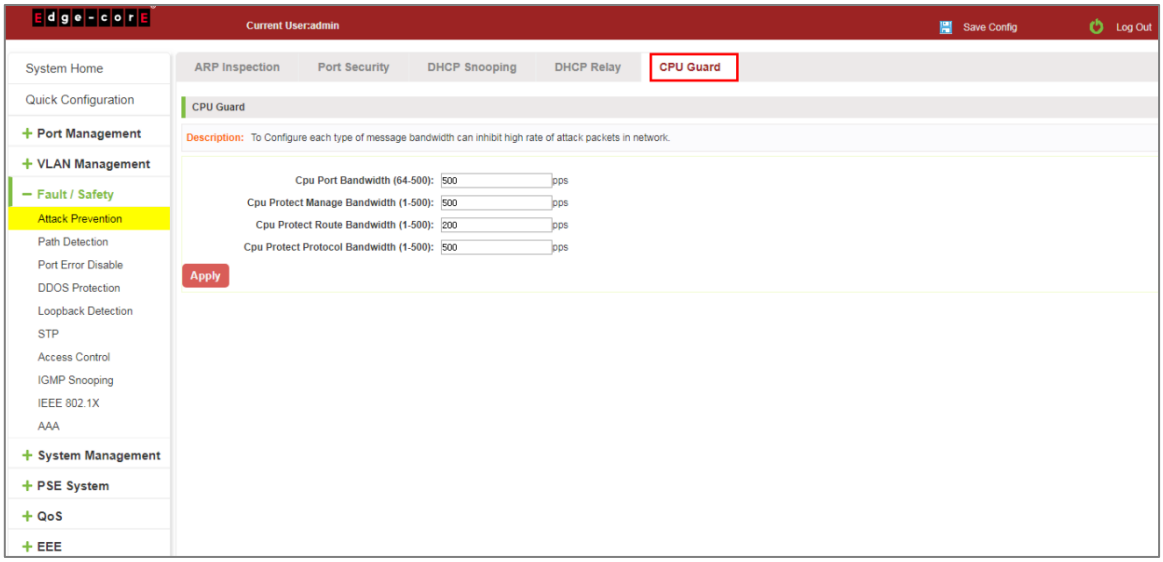


Figure 6-15: CPU Guard Information

Change CPU guard configuration:

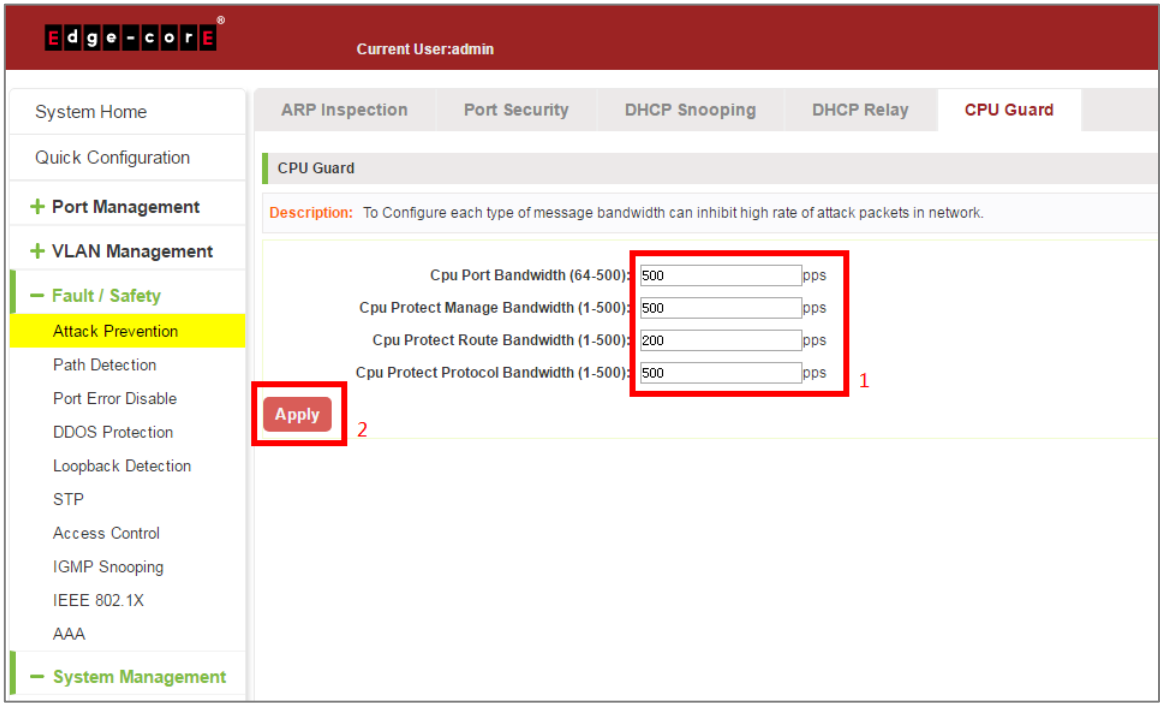


Figure 6-16: Change CPU Guard Configuration

6.2 PATH DETECTION

6.2.1 Path/Tracert detection

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

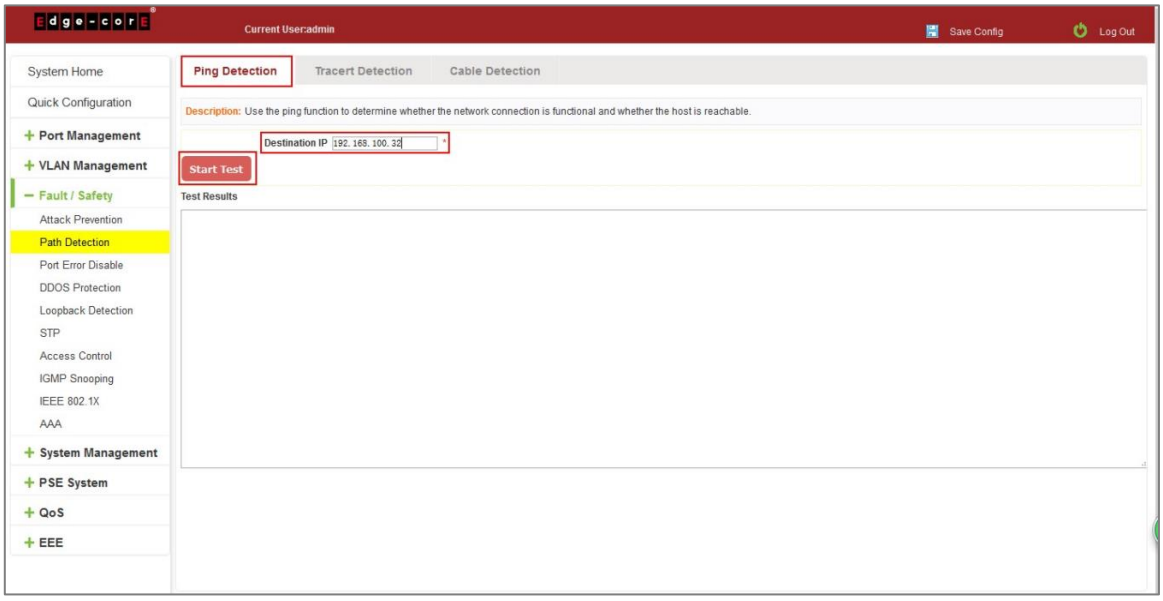


Figure 6-17: Path Detection Information

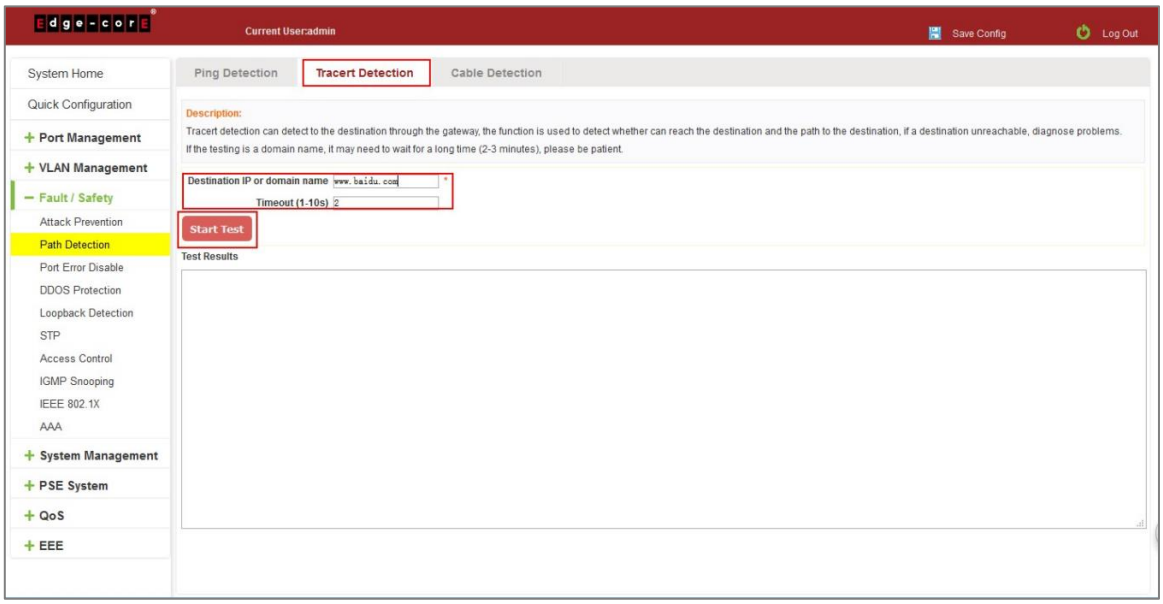


Figure 6-18: Tracert Detection Information

6.2.2 Cable detection

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

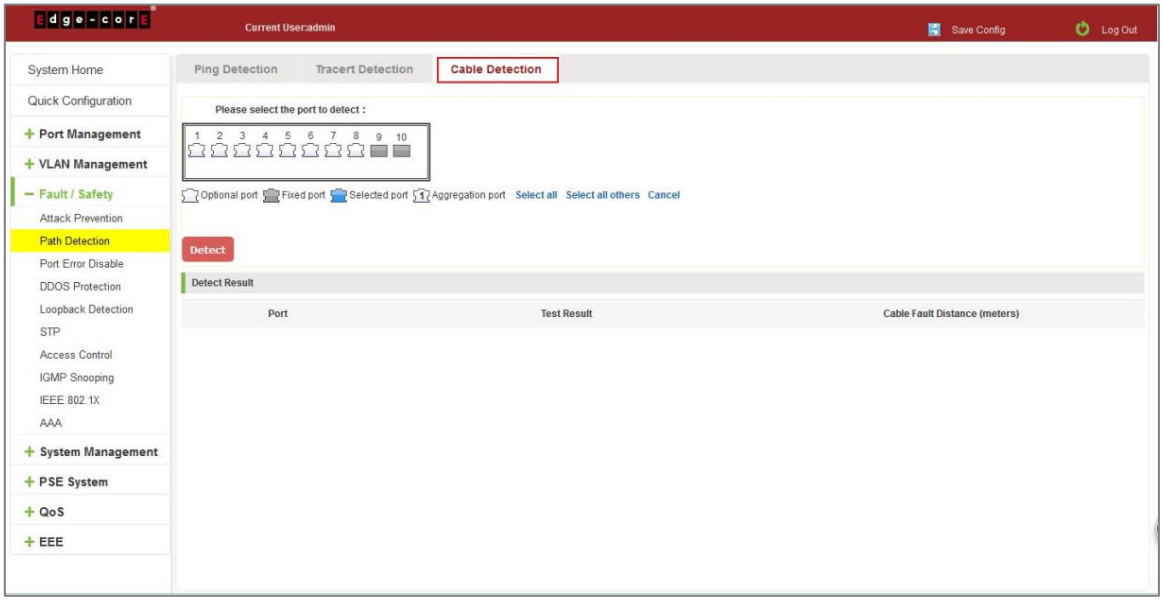


Figure 6-19: Cable Detection Information

The cable detection only selected one port:

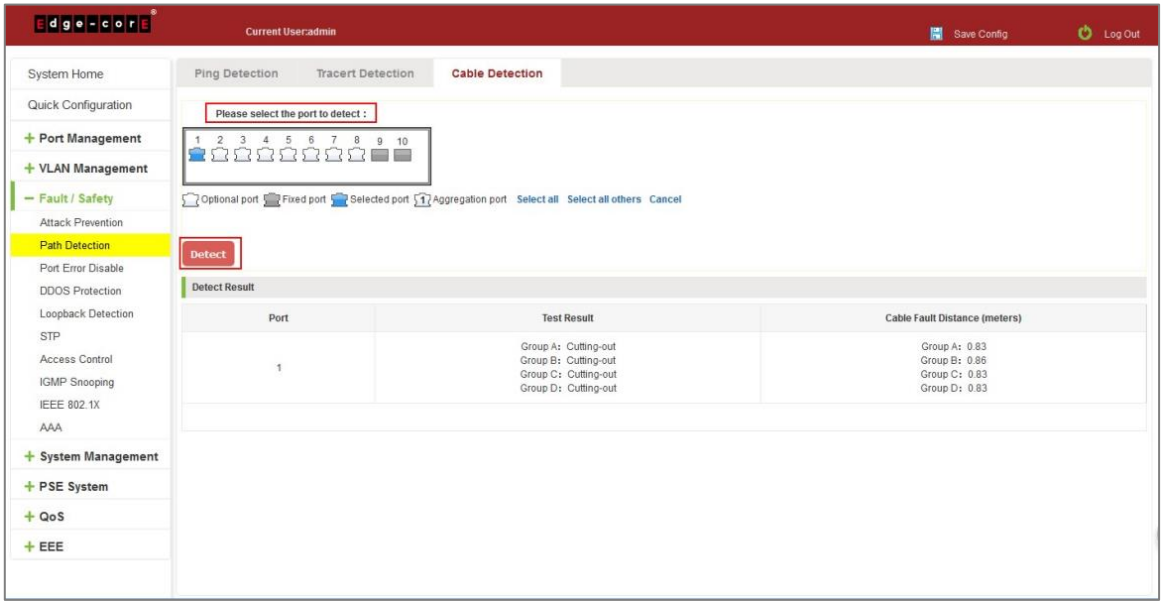


Figure 6-20: Port Cable Detection Result

6.3 PORT ERROR DISABLE

Collect port disable information, and can set the port auto recovery time.

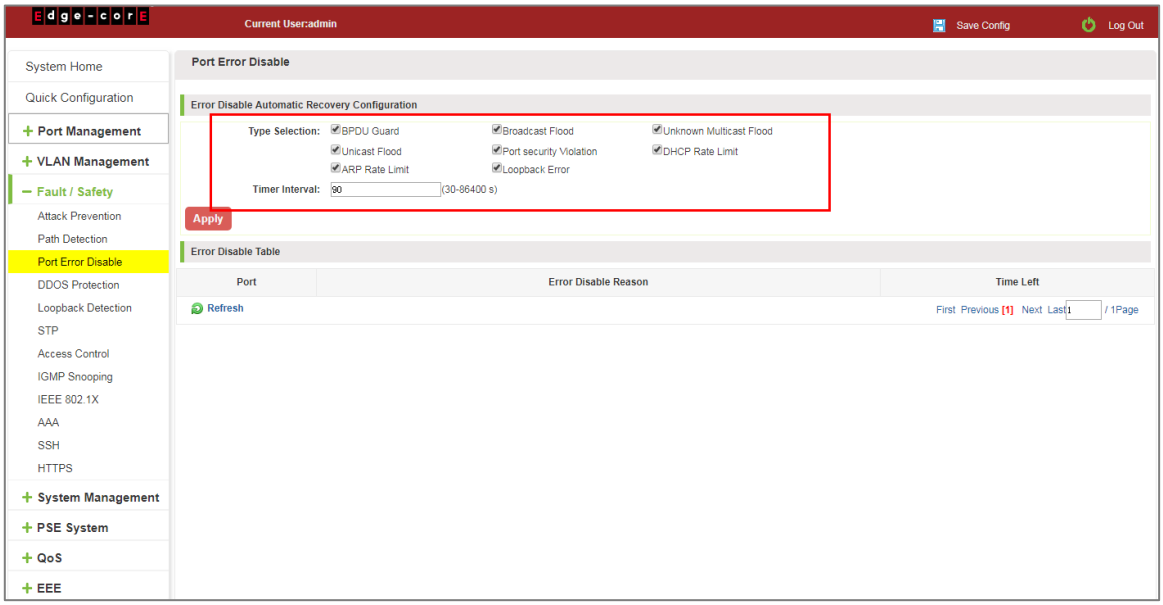


Figure 6-21: Error Disable Automatic Recovery Configuration

6.4 DDOS PROTECTION

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

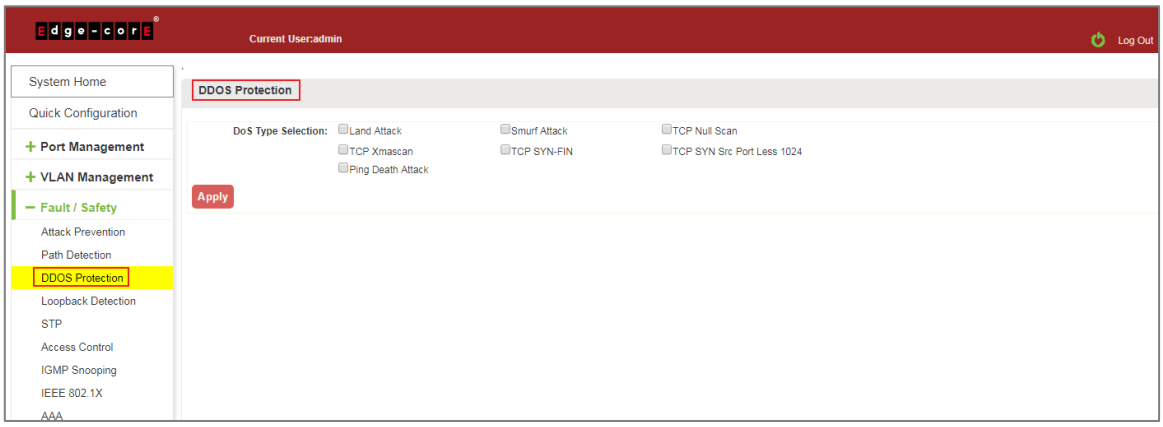


Figure 6-22: DDOS Protection Information

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

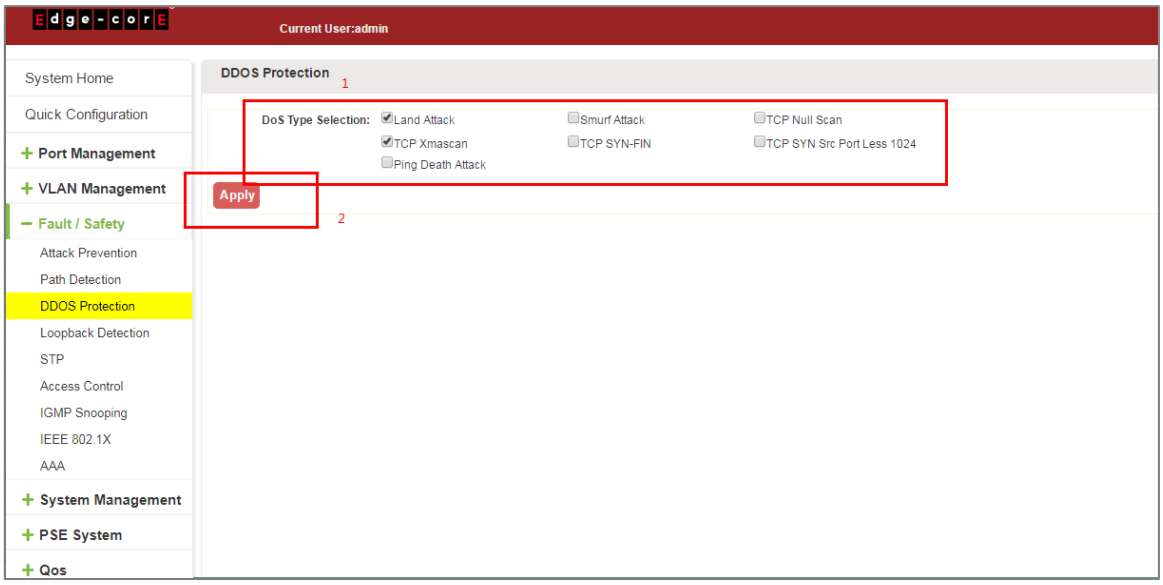


Figure 6-23: Selected DoS Type

6.5 LOOP DETECTION

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

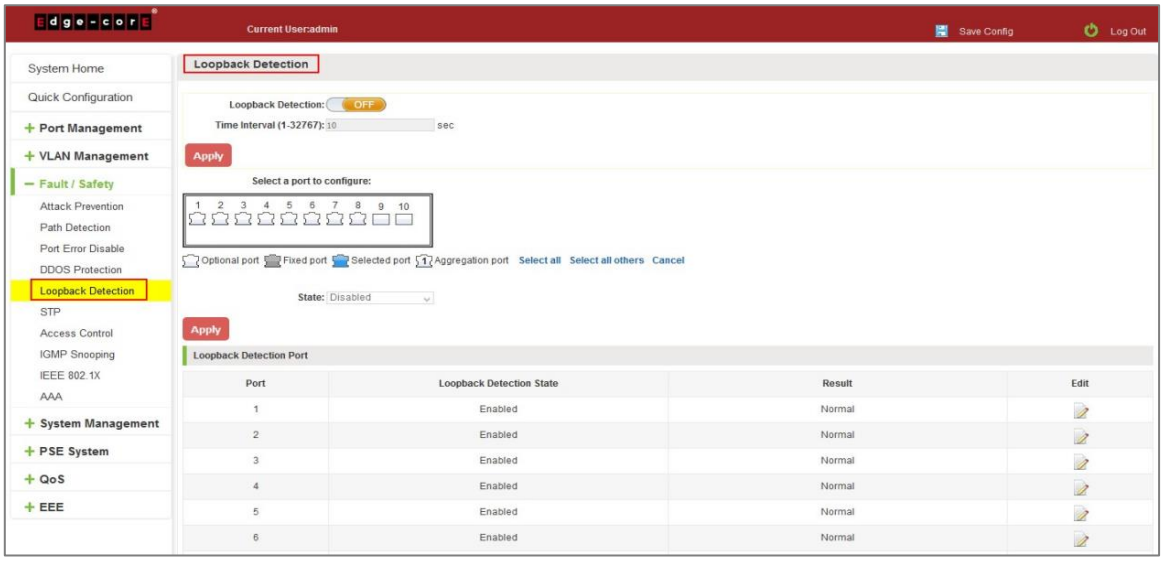


Figure 6-24: View Loopback Detection Configuration Information

6.5.1 Enable loopback detection

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

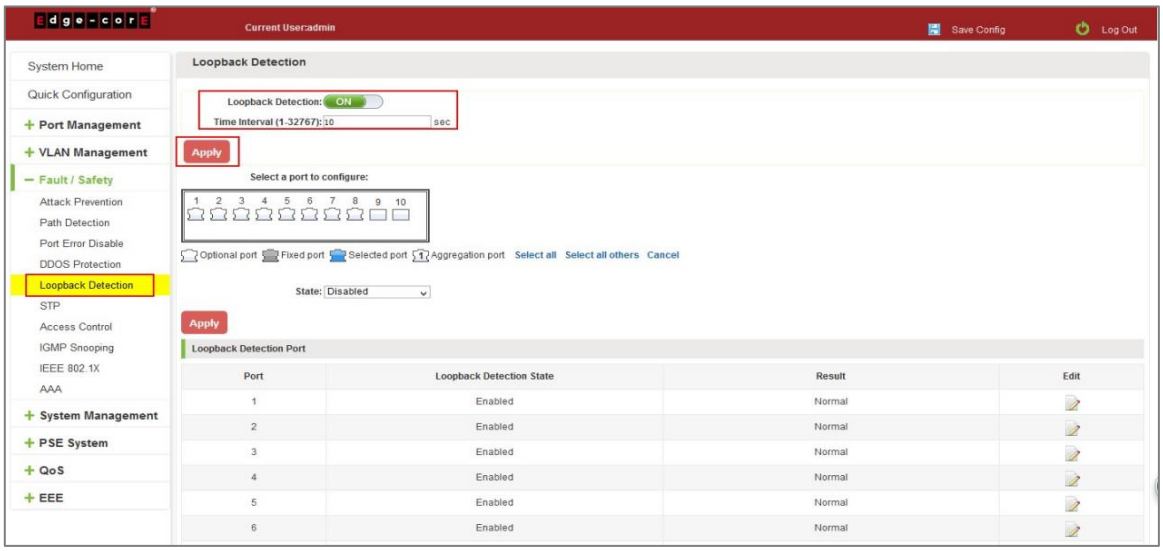


Figure 6-25: Enable Loopback Detection

6.5.2 Choose the port to configure

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

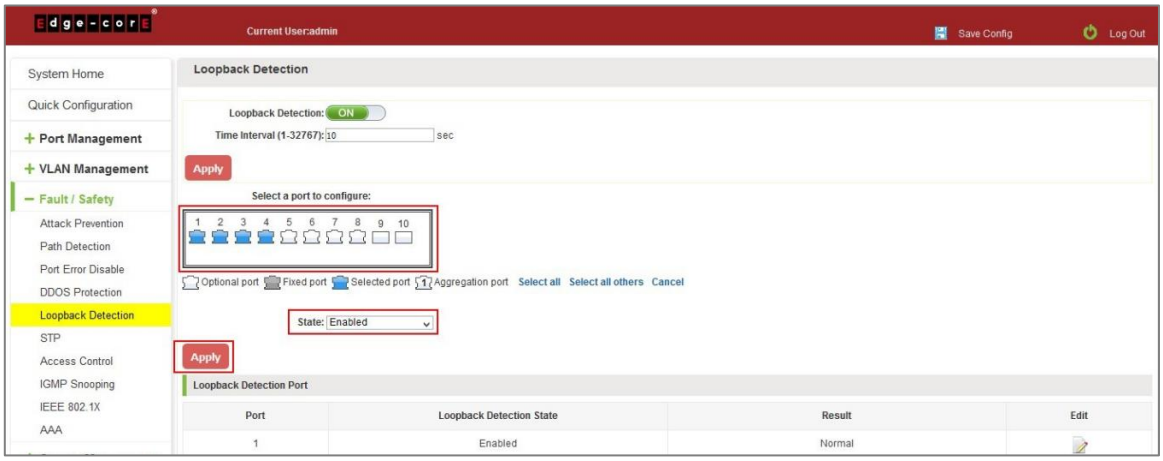


Figure 6-26: Configure Ports Parameter

Click "Edit" button, change the port status:

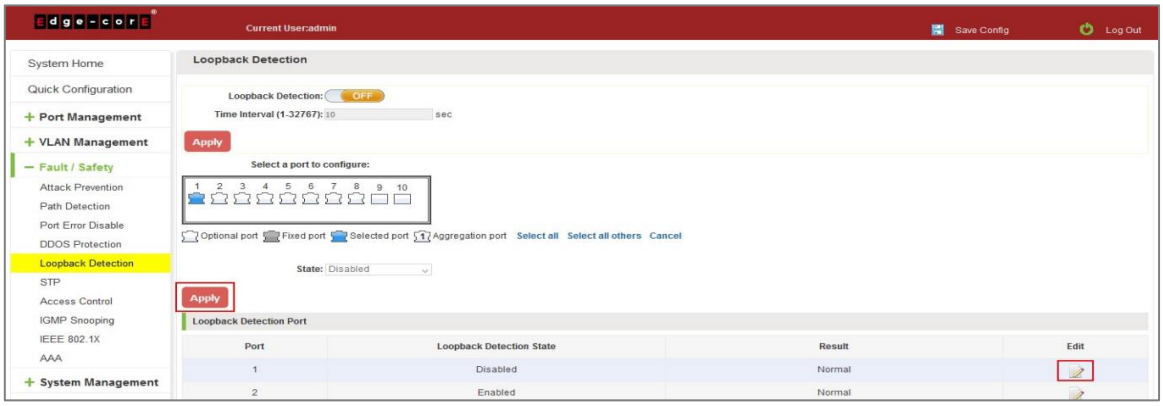


Figure 6-27: Change the Port Configure

6.6 STP

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

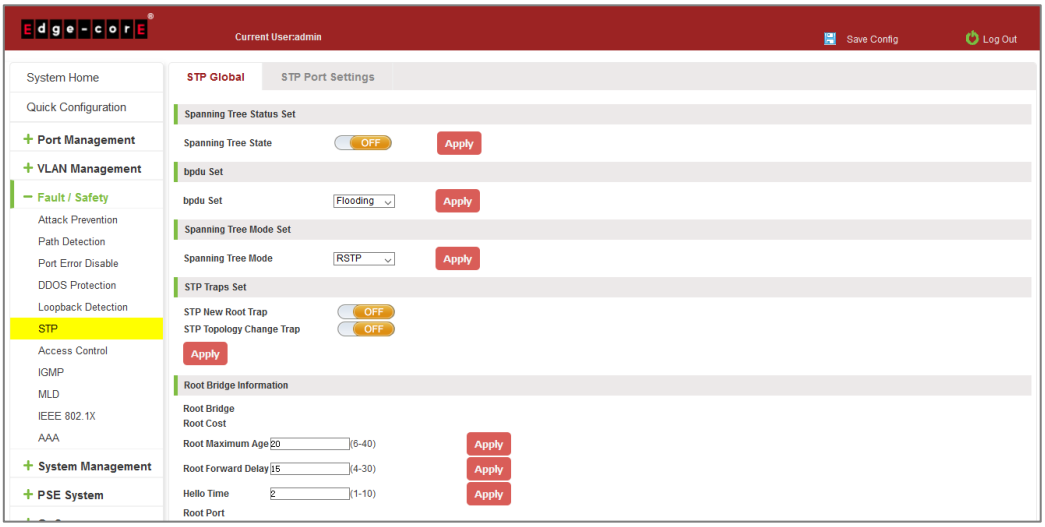


Figure 6-28: STP Global View

6.6.1 Enable STP function

Enable STP global state and configuration mode and traps.

Notice:

1. When the loopback detection and STP functions are mutually exclusive.
2. LLDP PDU flooding enabled prevents executing mSTP enable.

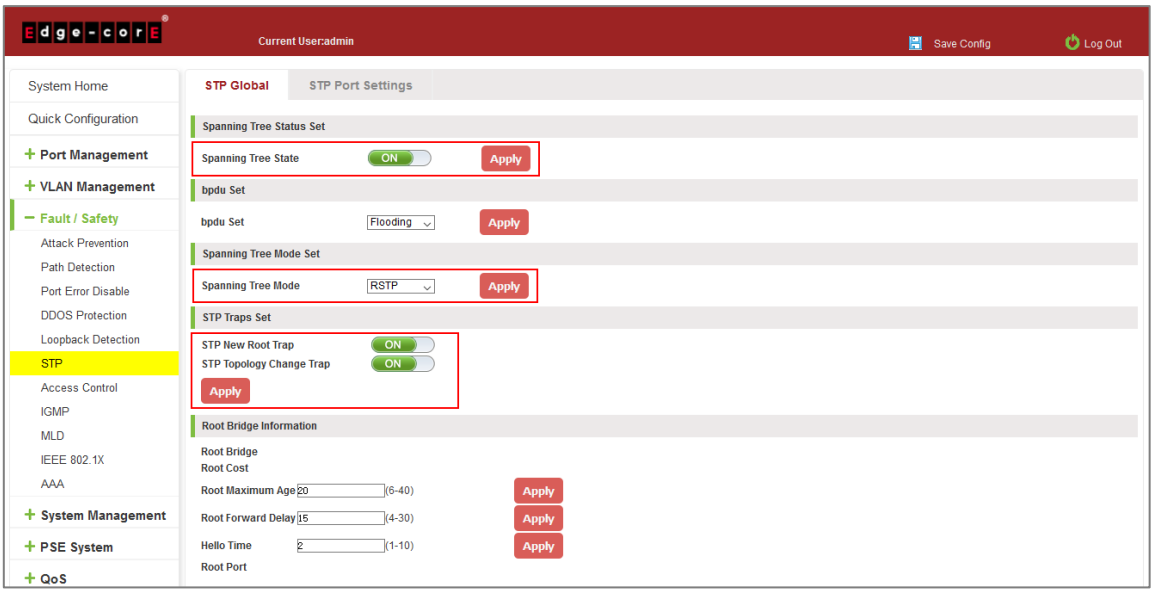


Figure 6-29: Enable STP Change Mode and Traps

6.6.2 STP port settings

Selected port to configuration STP.

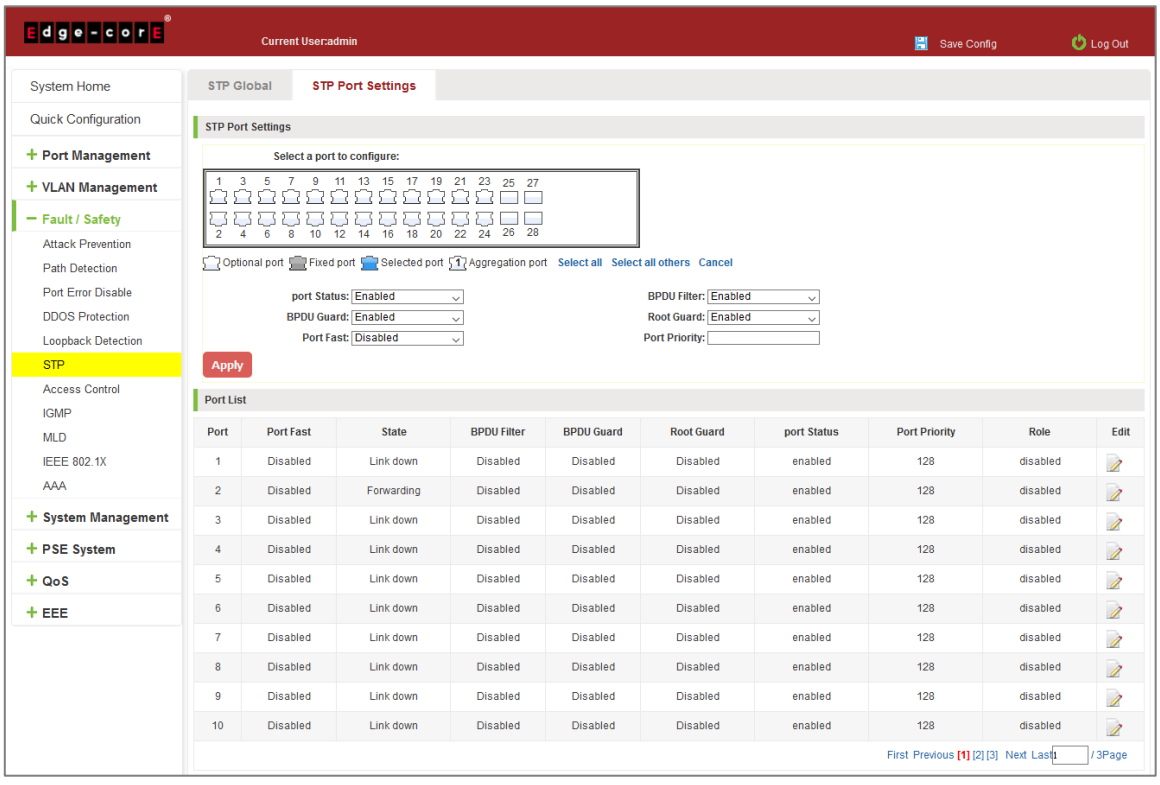


Figure 6-30: Selected Port to Configuration STP

6.7 ACCESS CONTROL

6.7.1 ACL access control list

6.7.1.1 View access control list

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

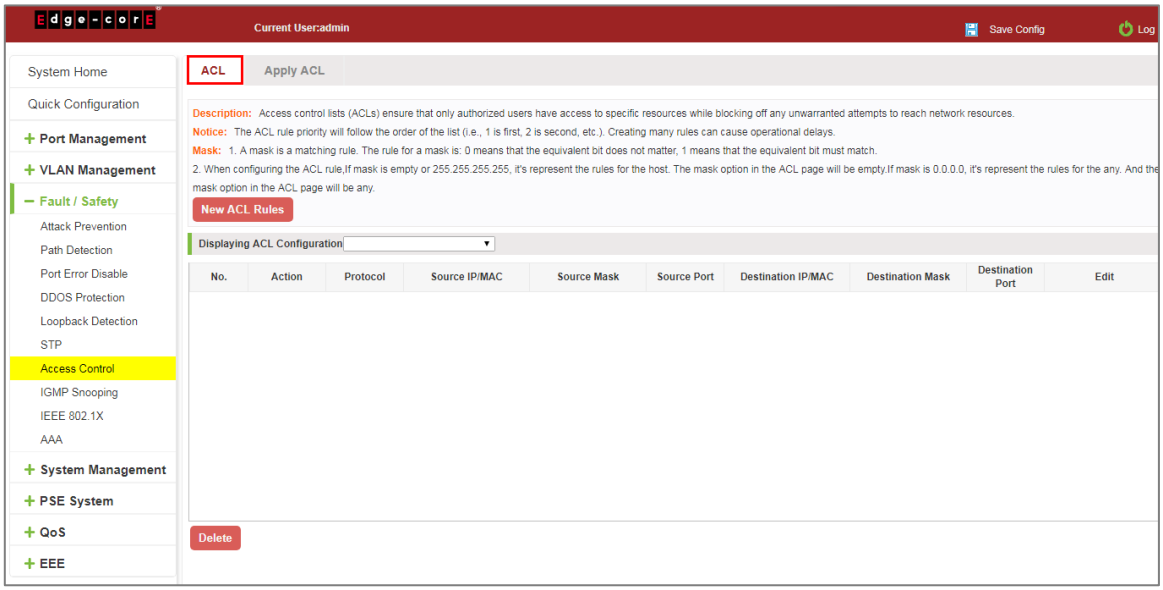


Figure 6-31: Access Control List

6.7.1.2 Increased access rules

1. INCREASE THE STANDARD IP ACCESS RULES

Click "New ACL Rules", 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:

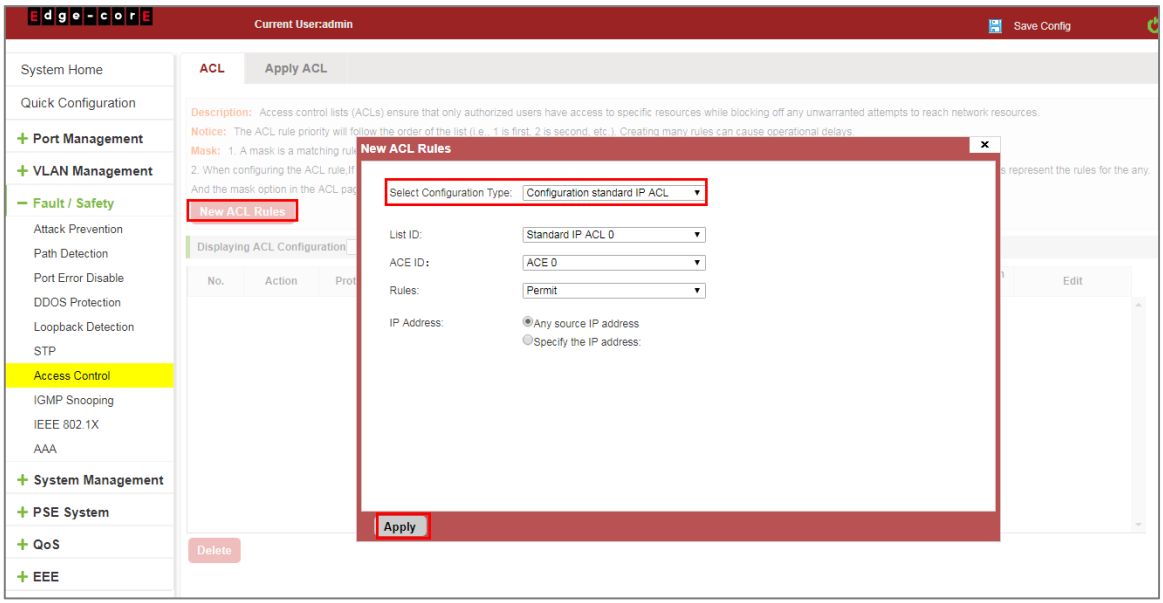


Figure 6-32: Configuration Standard IP Access Control List

2. INCREASE THE EXTENDED IP ACCESS RULE

Click "New ACL Rules", in the pop-up dialog box, select "Configuration Expand IP ACL", 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:

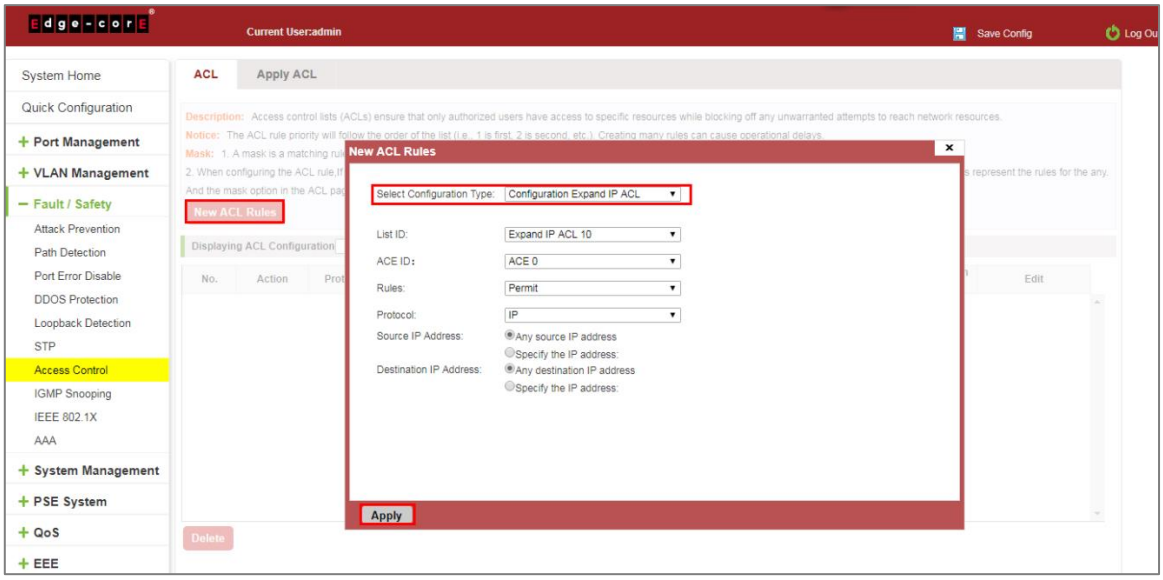


Figure 6-33: Configuration Standard IP Access Control List

3. INCREASING EXPAND MAC ACCESS RULES

Click "New ACL rules", select "Configuration Expand MAC ACL" in the pop-up window, in list ID: 20，ACE ID: 0, Rules "Deny", Source MAC address: 0088.9999.999A. Destination MAC address is the random MAC. MAC protocol type: 0x0086. After the configuration is complete, click "Apply":

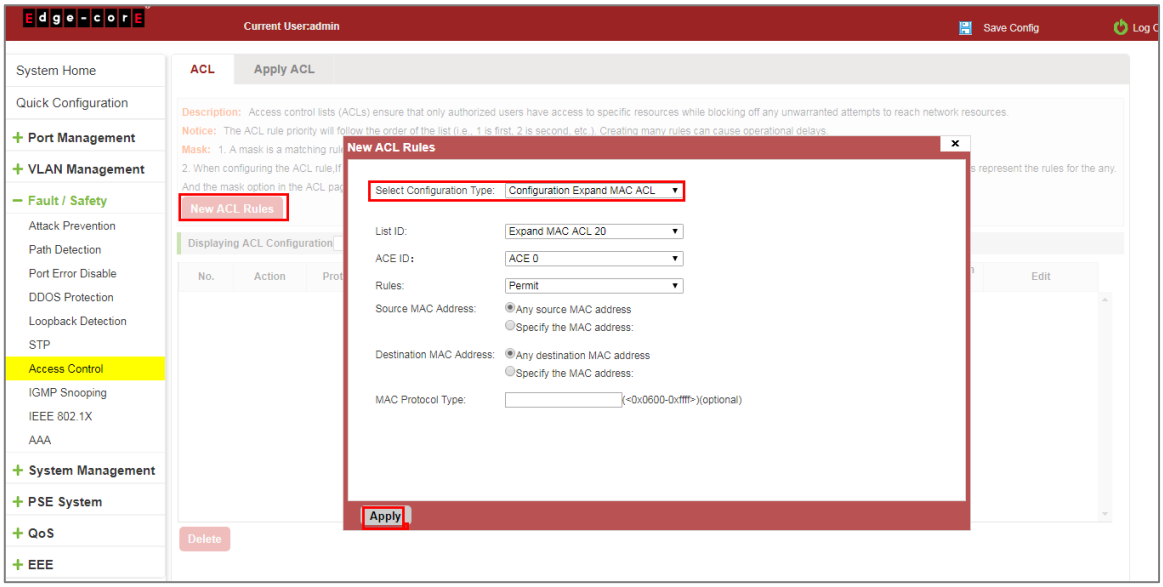


Figure 6-34: Configuration Extended MAC Access Control List

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.

6.7.1.3 Modify configuration

Rules for modifying port applications

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

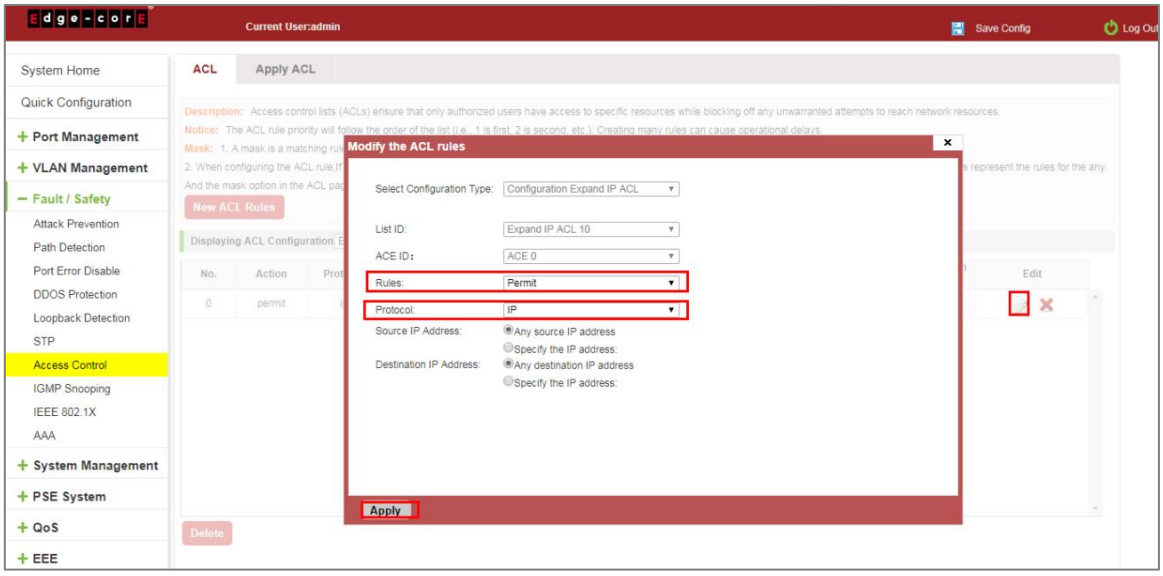


Figure 6-35: To Modify the ACL Rule

Configuration instructions

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

6.7.1.4 Delete rule

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

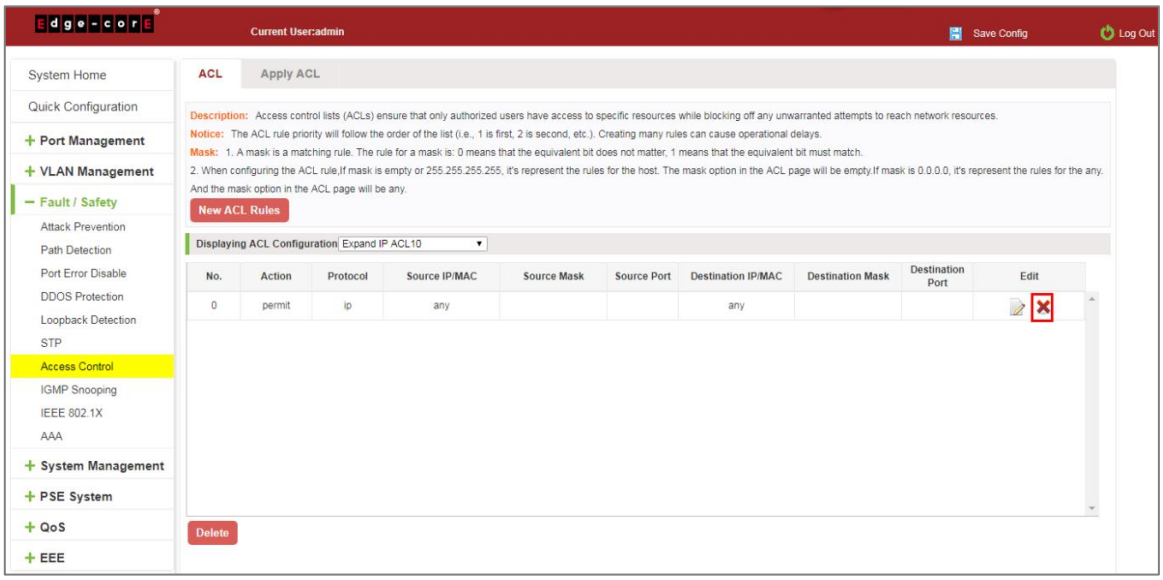


Figure 6-36: Delete Rules

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

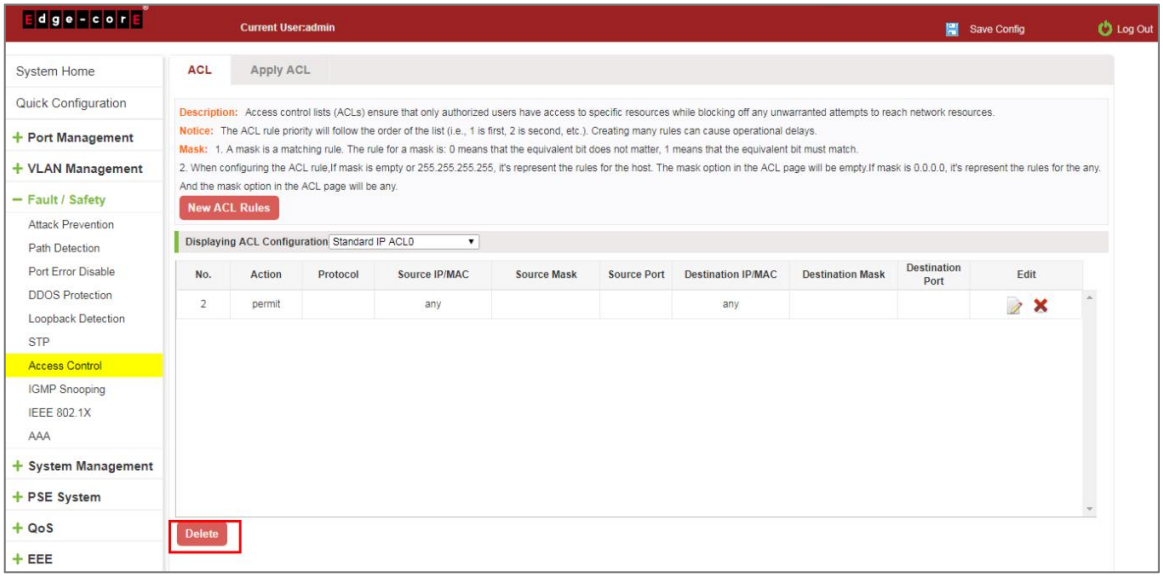


Figure 6-37: Delete ACL Rules

Configuration instructions

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

6.7.2 Application ACL

6.7.2.1 View application ACL

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

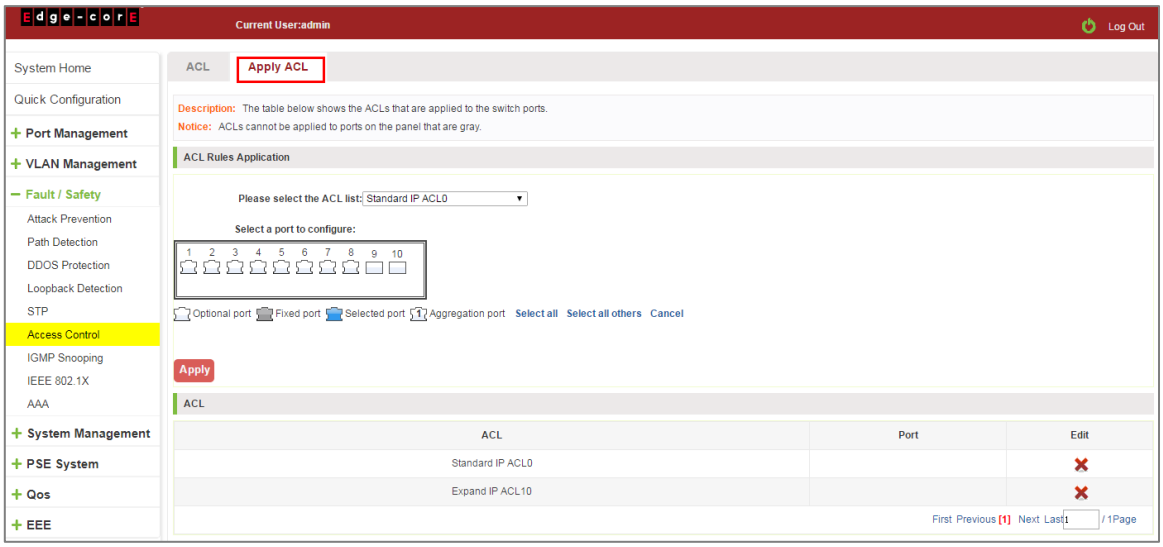


Figure 6-38: View Application ACL Rules

6.7.2.2 Increased application ACL

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

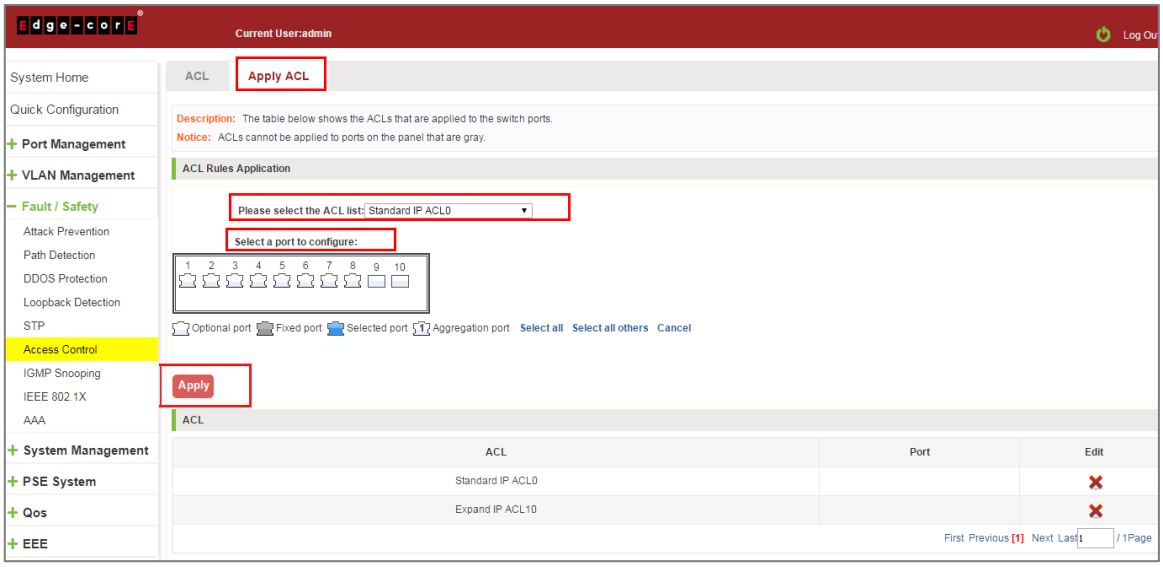


Figure 6-39: Add Applications ACL

6.7.2.3 Delete application ACL

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

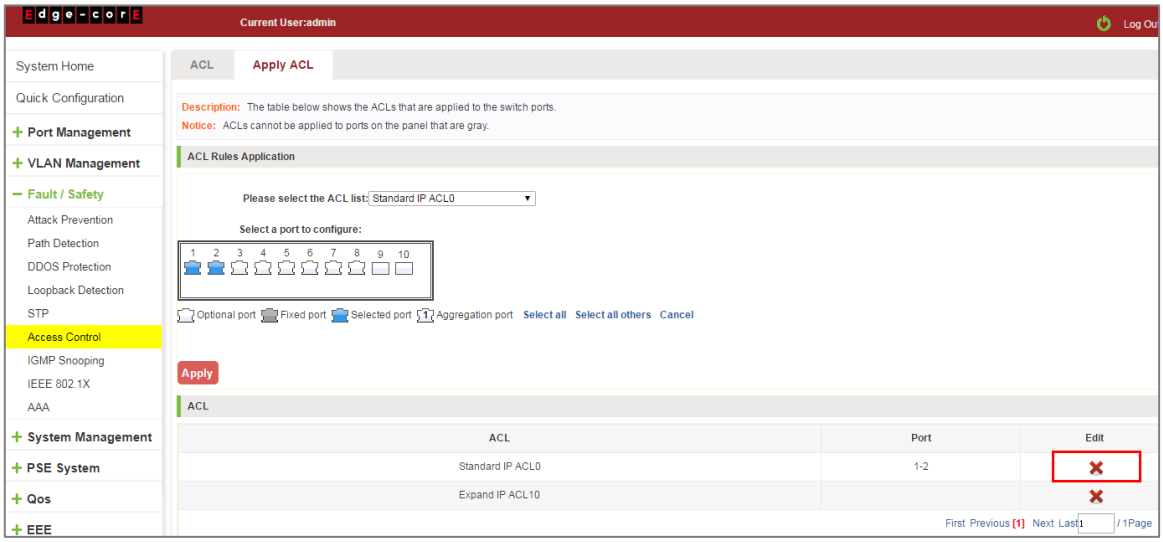


Figure 6-40: Delete Application ACL

6.8 IGMP SNOOPING

6.8.1 View IGMP snooping configuration

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

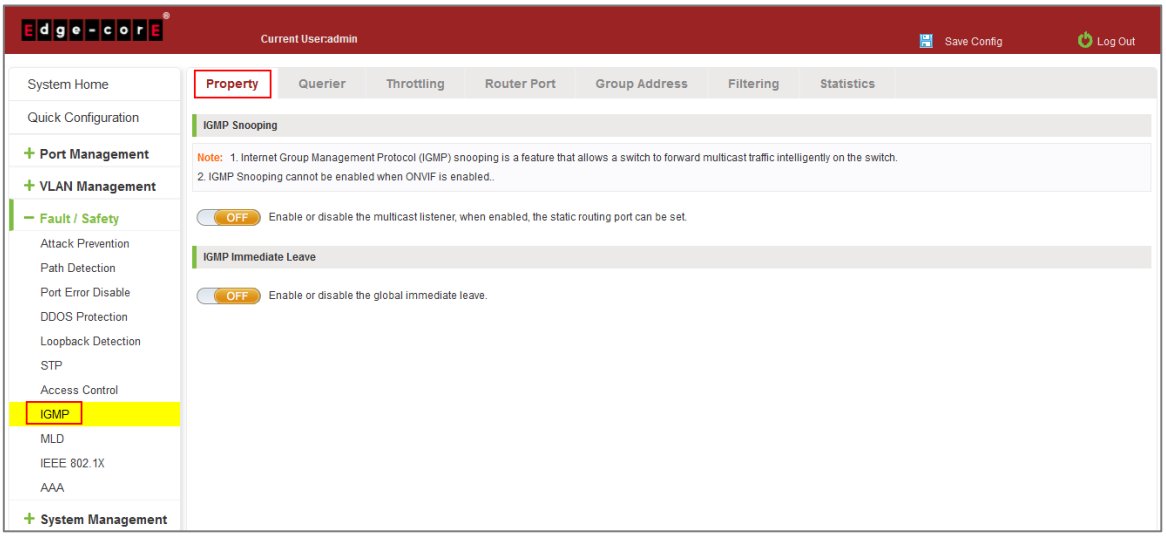


Figure 6-41: View Snooping IGMP Configuration Information

6.8.2 Action multicast listener function

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

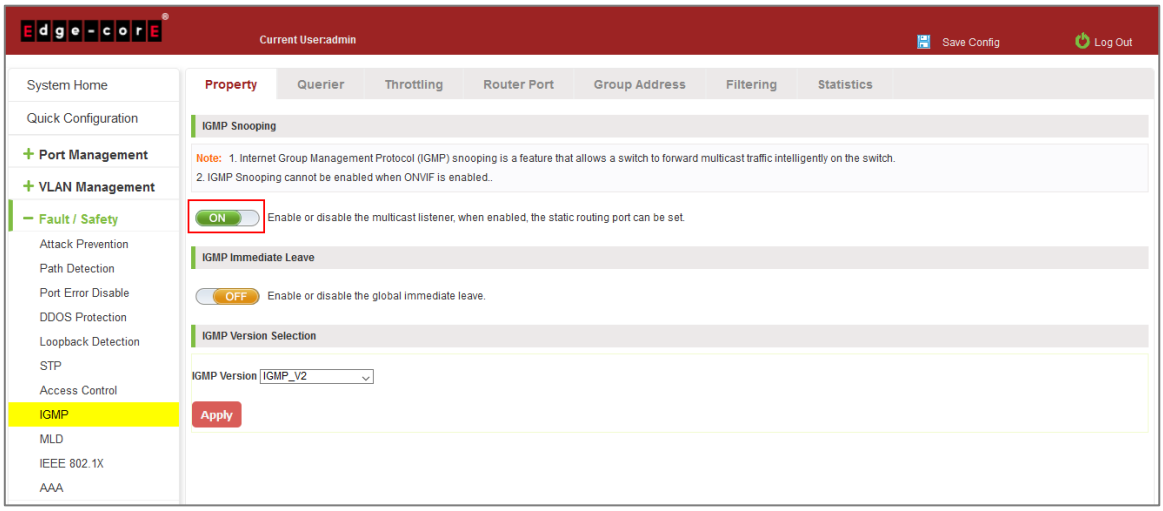


Figure 6-42: Open Multicast Listener Configuration

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.

6.8.3 Disable multicast listener function

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

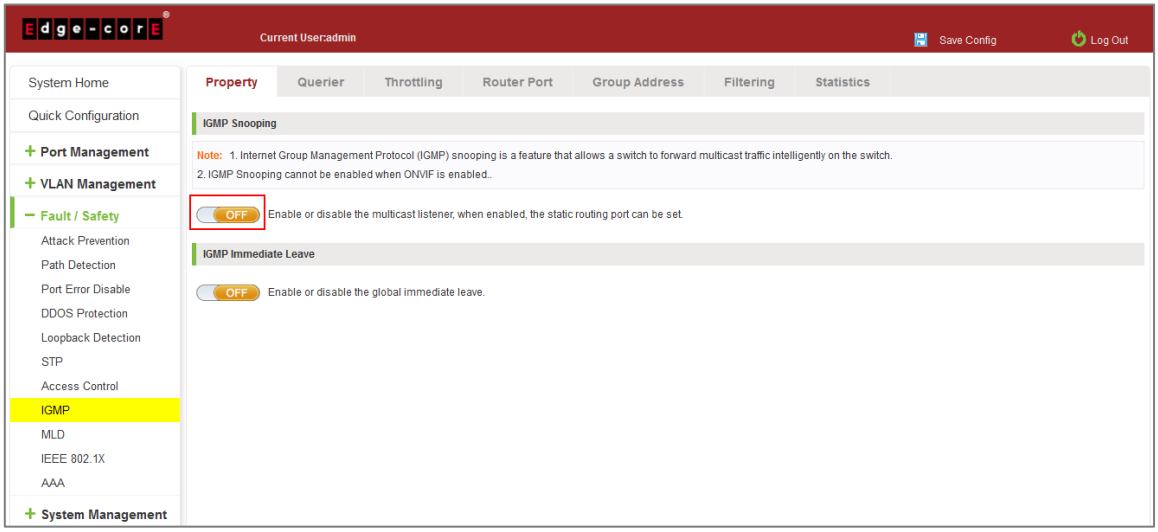


Figure 6-43: Closed Multicast Listener Function Operation

6.8.4 Configuration multicast routing

Click the "Fault/Safety" "IGMP" “RouterPort,” select the VLAN, click "Router Port Add" button, to configure the multicast routing in the port panel:

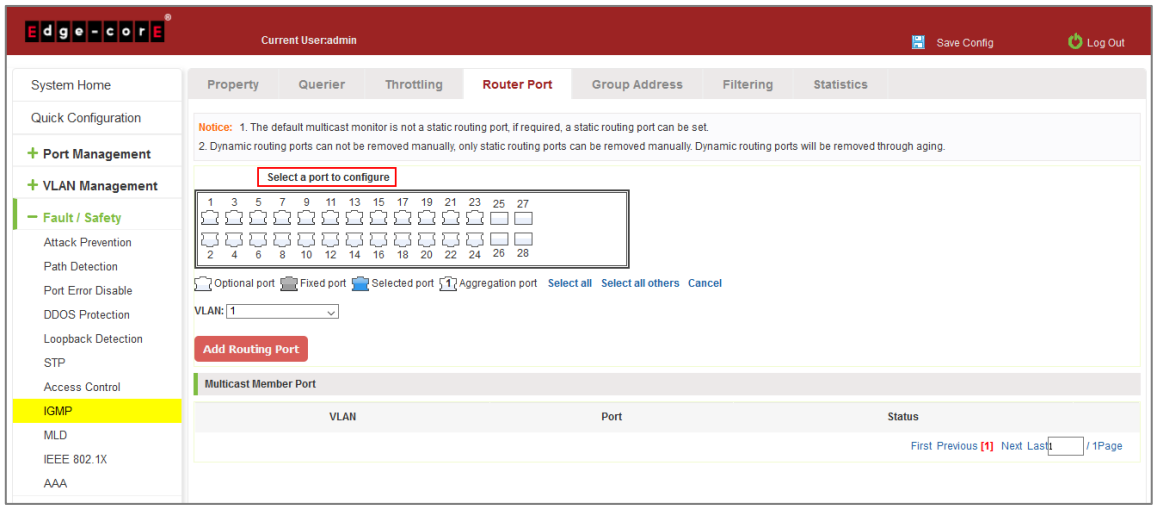


Figure 6-44: Configuration of Multicast Routing

Multicast routing configuration steps are as follows:

Step 1: In the port panel to select multicast listener routing port;

Step 2: Select VLAN;

Step 3: Click on the "Add Router Port" button to complete the configuration.

6.8.5 IGMP Version

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

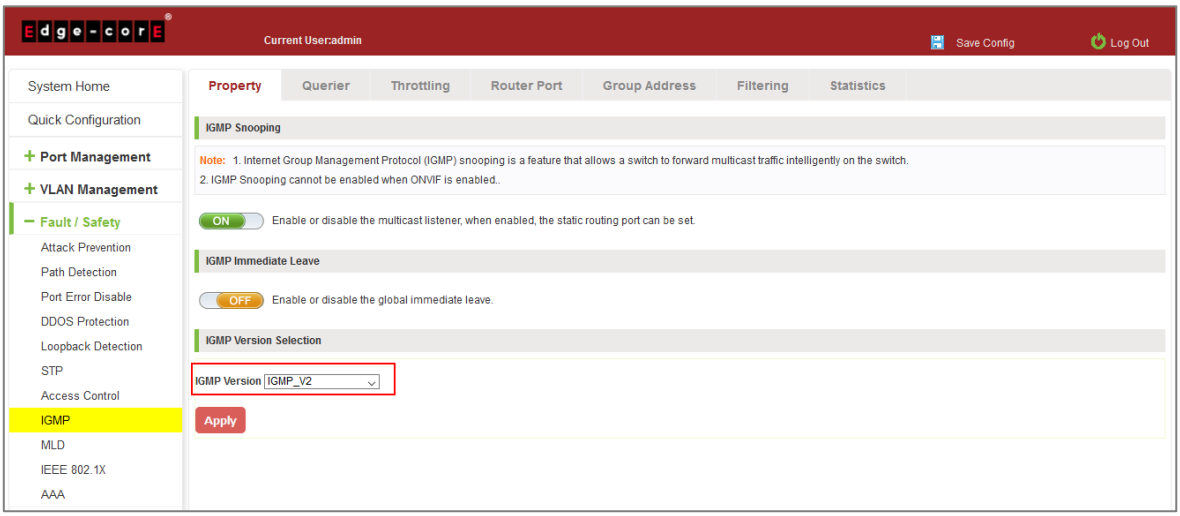


Figure 6-45: Configuration IGMP Version

IGMP version configuration steps are as follows:

Step 1: Select the required version number;

Step 2: Click the "Apply" button to complete the configuration.

6.8.6 IGMP Querier

Click the "Fault/Safety" "IGMP" “Querier,” set the IGMP Querier:

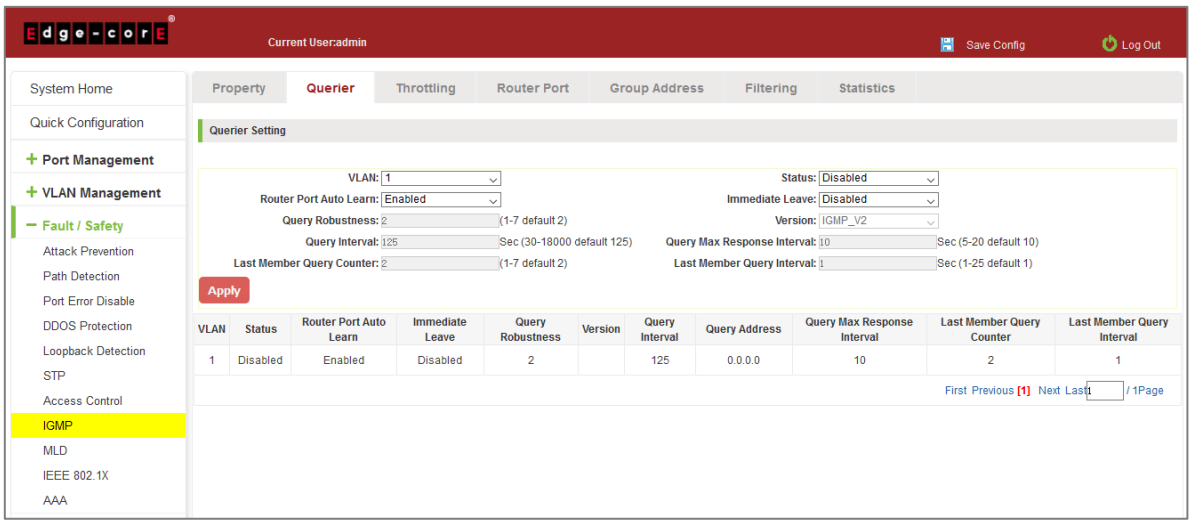


Figure 6-46: Configuration IGMP Querier

6.8.7 IGMP Group Address

Click the "Fault/Safety" "IGMP" “Group Address,” set the IGMP Group Address:

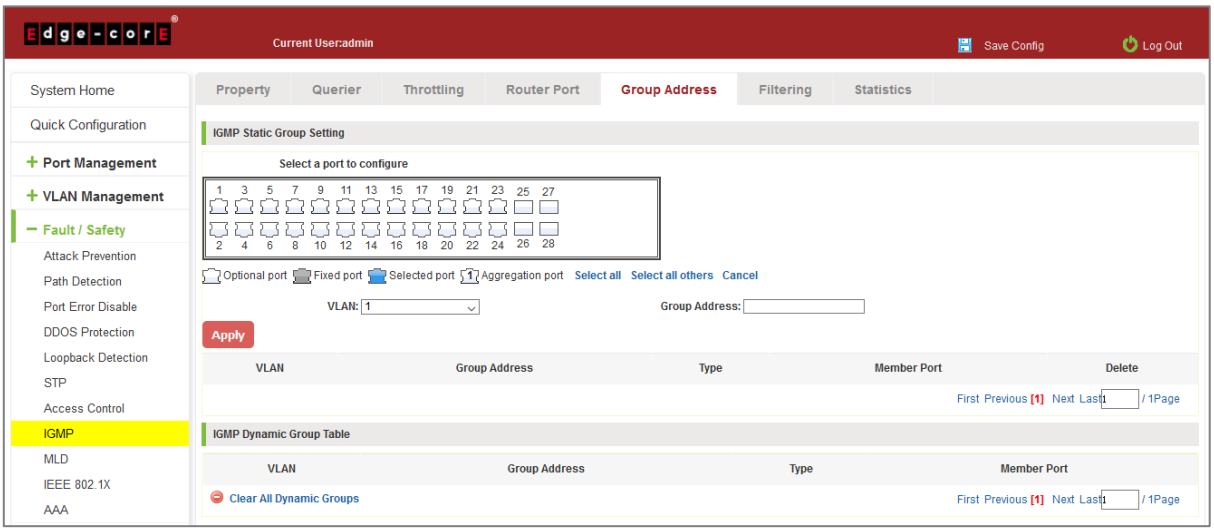


Figure 6-47: Configuration IGMP Group Address

6.8.8 IGMP Throttling

Click the "Fault/Safety" "IGMP" “Throttling,” to configure IGMP throttling:

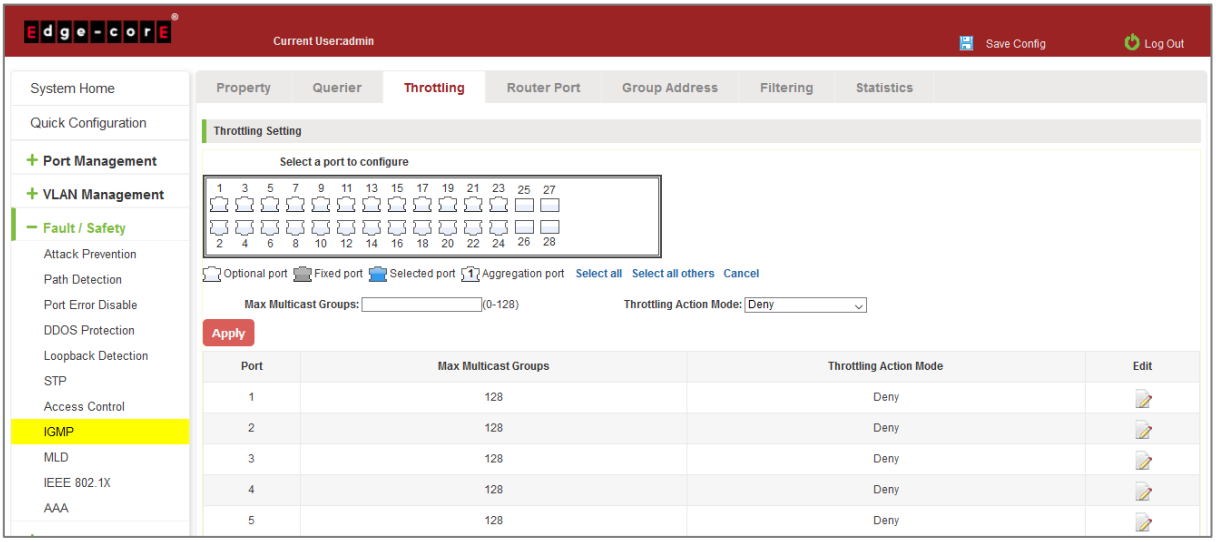


Figure 6-48: Configuration IGMP Throttling

6.8.9 IGMP Filtering

Click the "Fault/Safety" "IGMP" “Filtering,” to configure IGMP filtering:

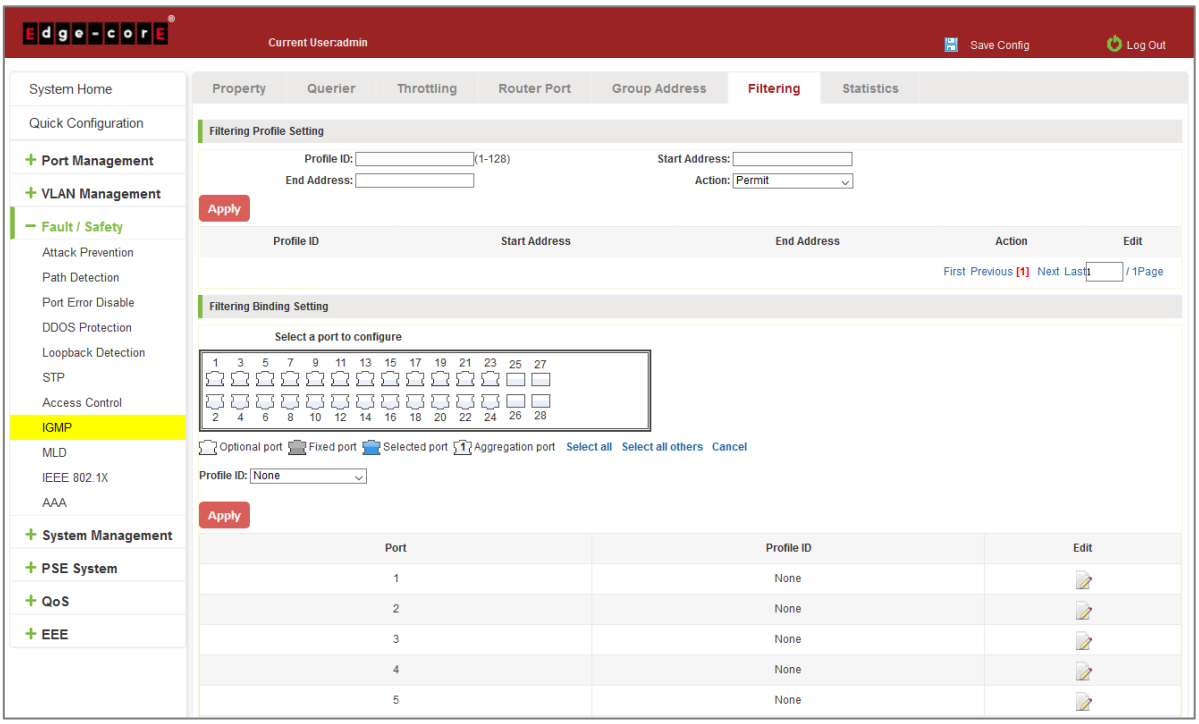


Figure 6-49: Configuration IGMP Filtering

6.8.10 IGMP Statistics

Click the "Fault/Safety" "IGMP" “Statistics,” to view IGMP statistics:

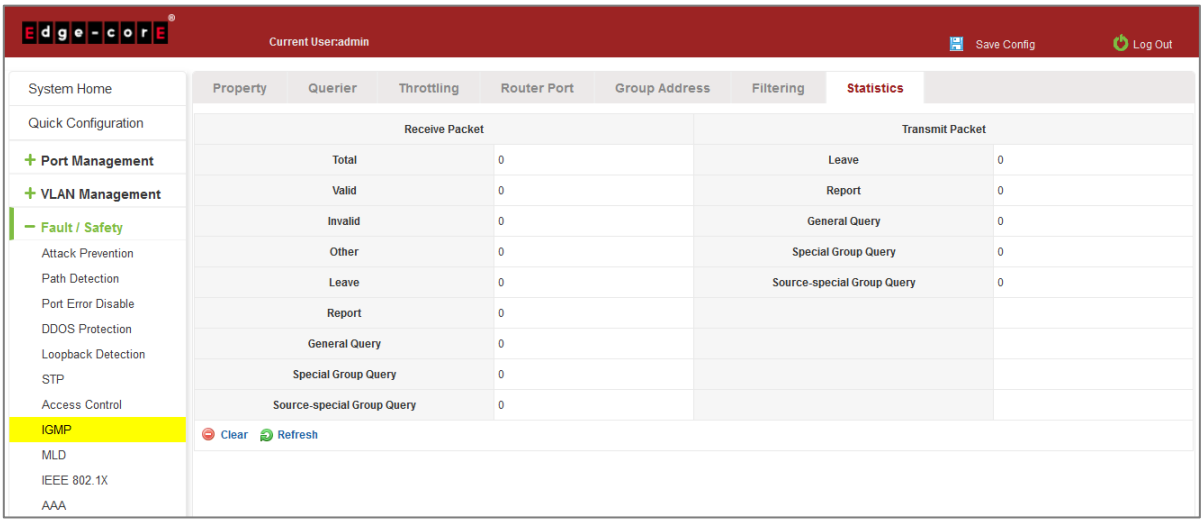


Figure 6-50: Configuration IGMP Statistics

6.9 MLD

6.9.1 View MLD configuration

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

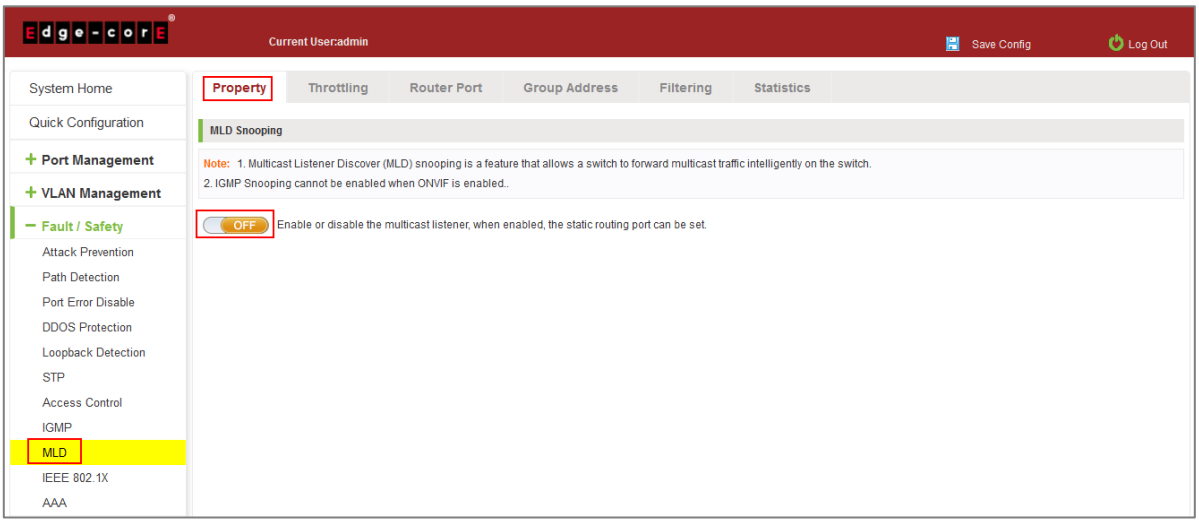


Figure 6-51: View MLD Configuration Information

6.9.2 Active multicast listener function

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

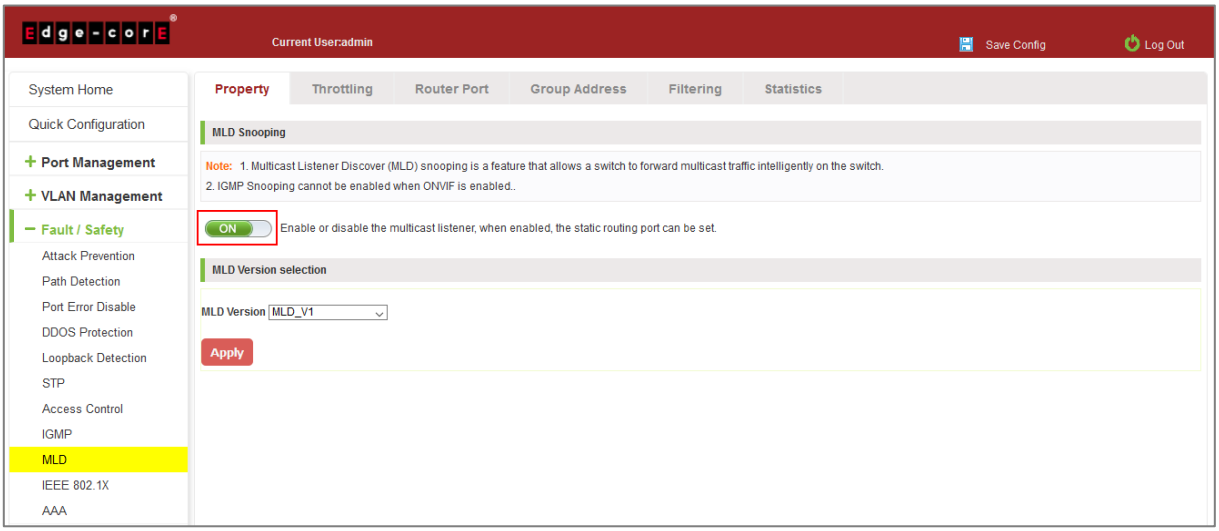


Figure 6-52: Open Multicast Listener Configuration

The default multicast listener (MLD) did not open;

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

The default version of V1 - MLD.

6.9.3 Disable multicast listener function

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

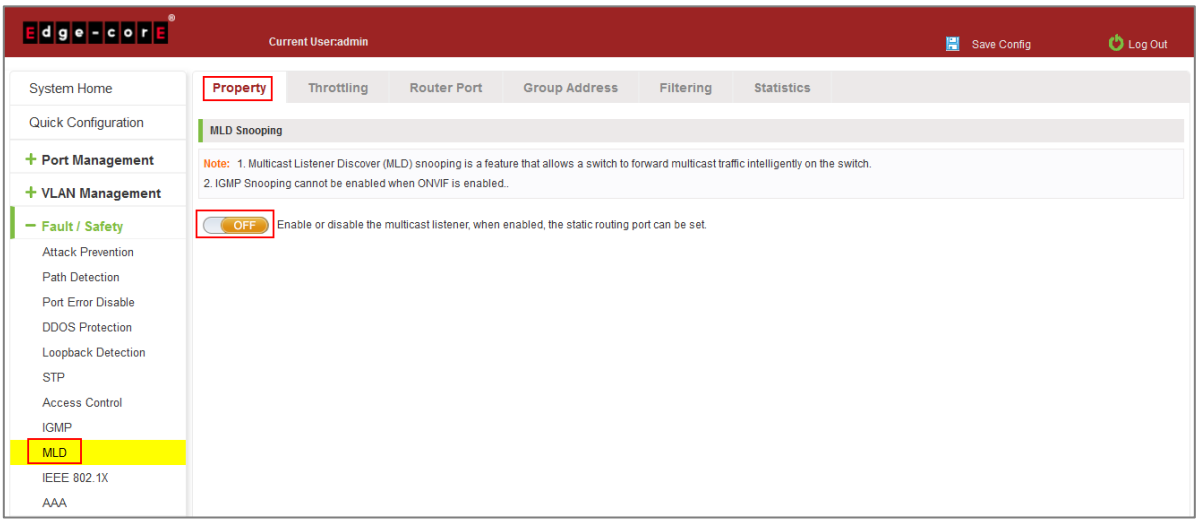


Figure 6-53: Closed Multicast Listener Function Operation

6.9.4 Configuration multicast routing

Click the "Fault/Safety" "MLD" “Router Port,” Select VLAN, click "Add Routing Port" button, to configure the multicast routing in the port panel:

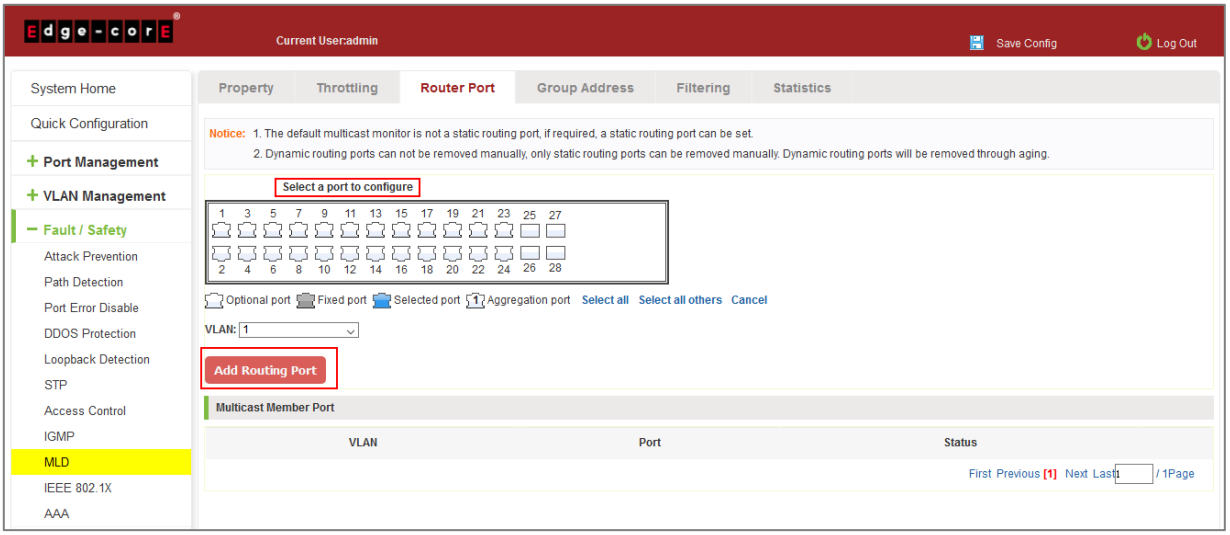


Figure 6-54: Configuration of Multicast Routing

Multicast routing configuration steps are as follows:

Step 1: In the port panel to select multicast listener routing port;

Step 2: Select VLAN;

Step 3: Click on the "Add Routing Port" button to complete the configuration.

6.9.5 Configuration MLD Group Address

Click the "Fault/Safety" "MLD" “Group Address,” Select a port, select VLAN, and enter the group address:

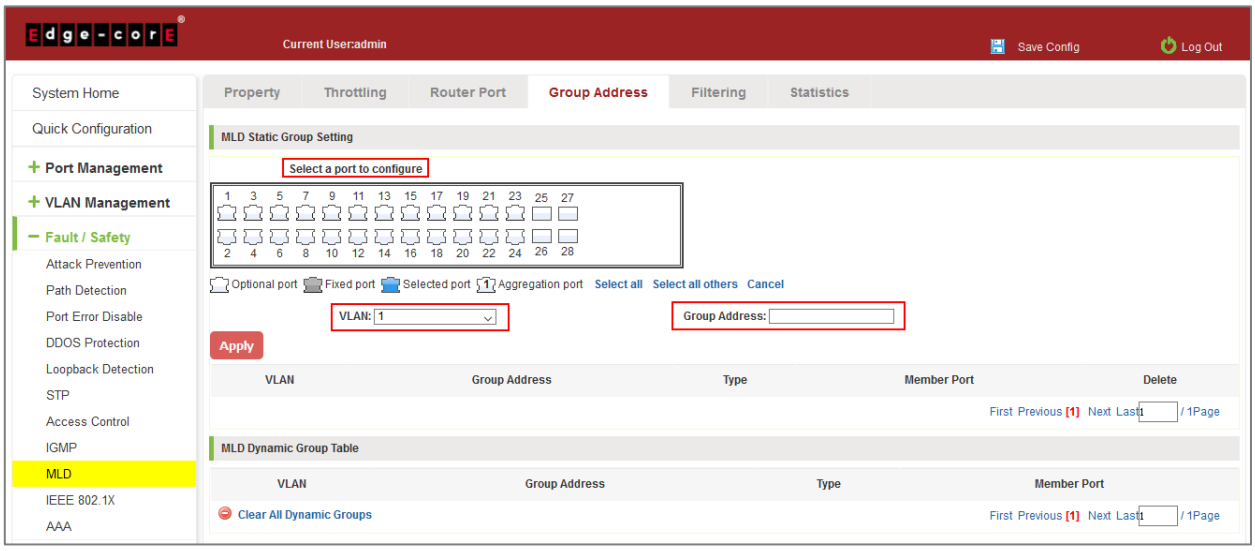


Figure 6-55: Configuration of MLD Group Address

6.9.6 Configuration MLD Throttling

Click the "Fault/Safety" "MLD" “Throttling,” Select a port, enter the maximum number of groups, and set the action mode:

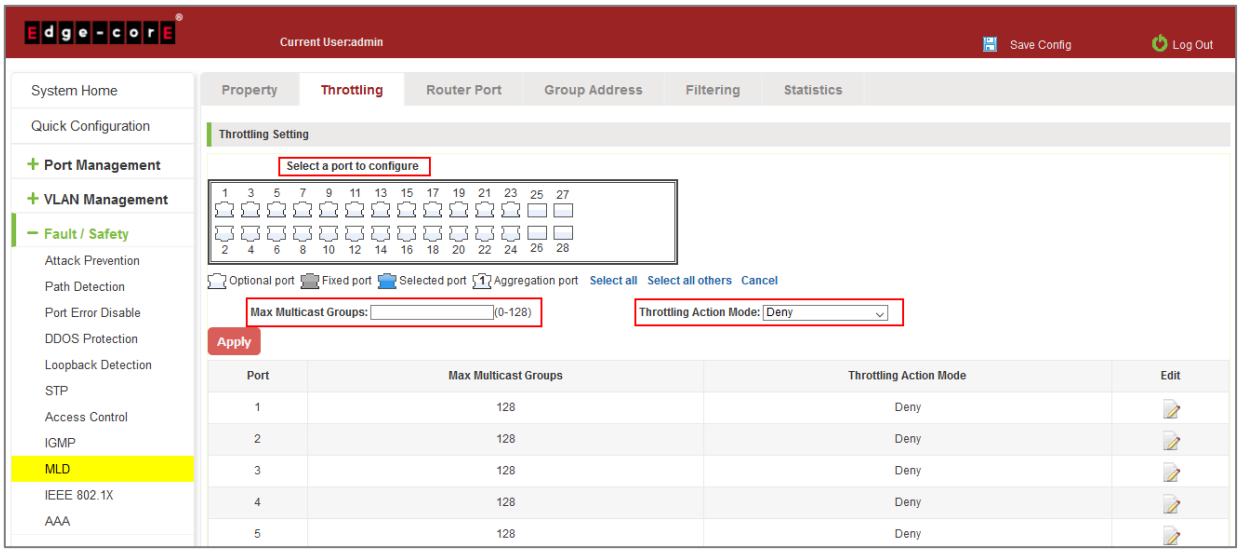


Figure 6-56: Configuration of MLD Throttling

6.9.7 Configuration MLD Filtering

Click the "Fault/Safety" "MLD" “Filtering,” set a profile ID, address range, and action to create a profile. Select a port, and profile ID to apply, then click Apply:

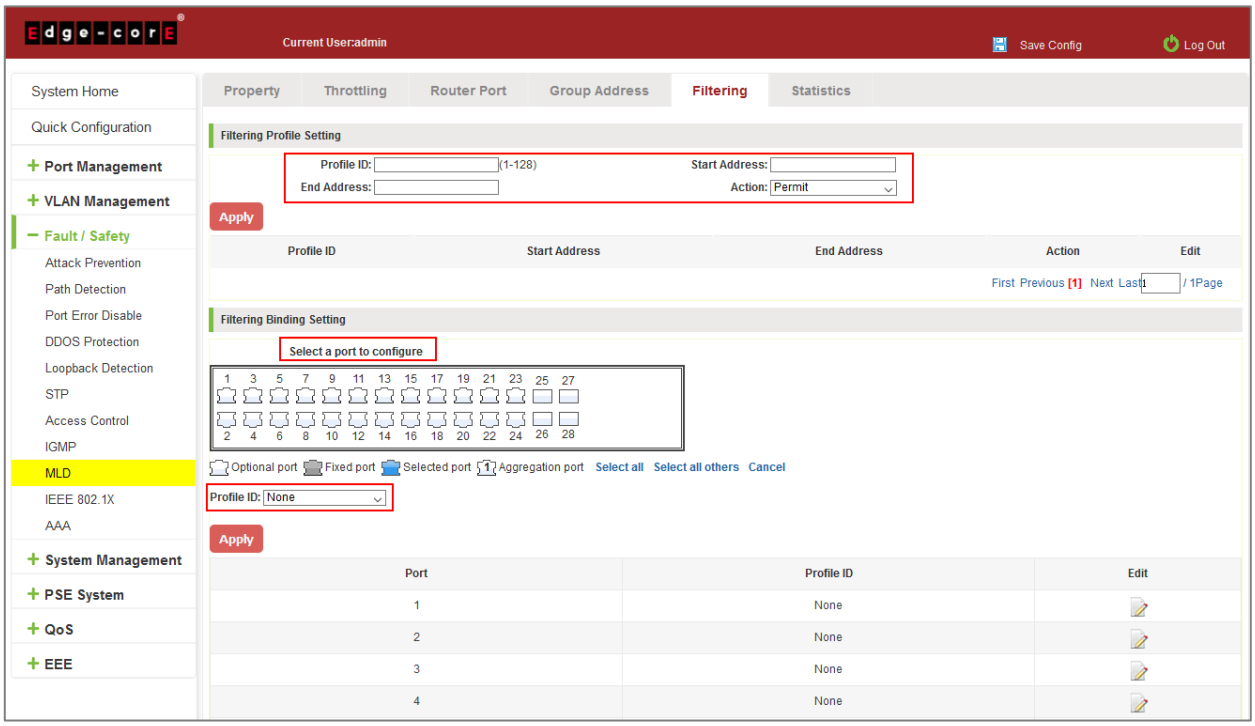


Figure 6-57: Configuration of MLD Filtering

6.9.8 Configuration MLD Statistics

Click the "Fault/Safety" "MLD" “Statistics,” to view the MLD statistics:

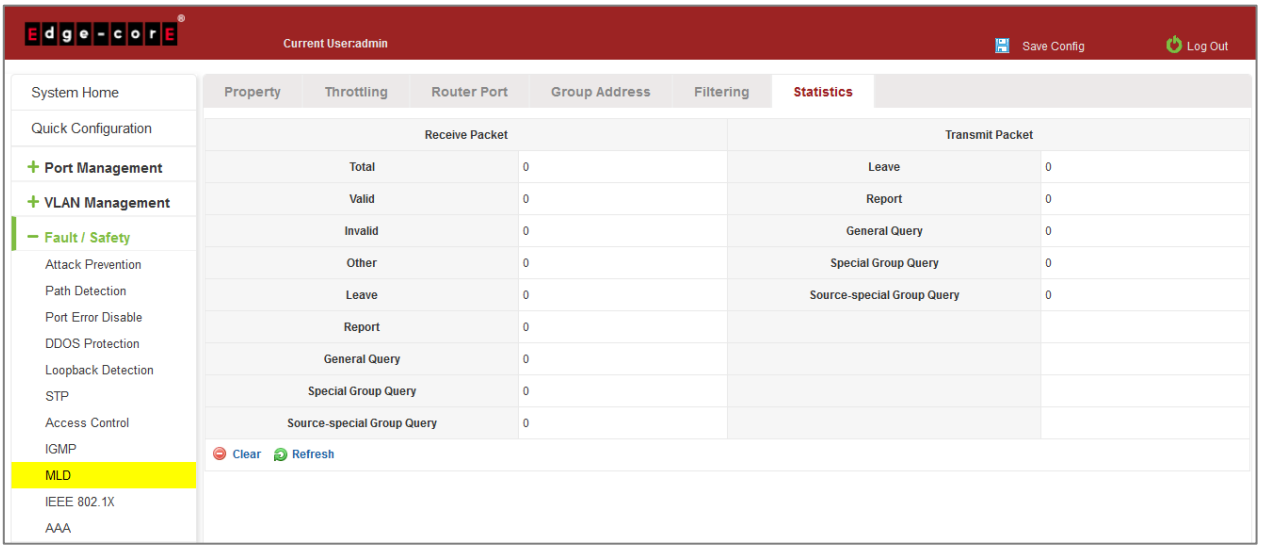


Figure 6-58: Configuration of MLD Statistics

6.10 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"

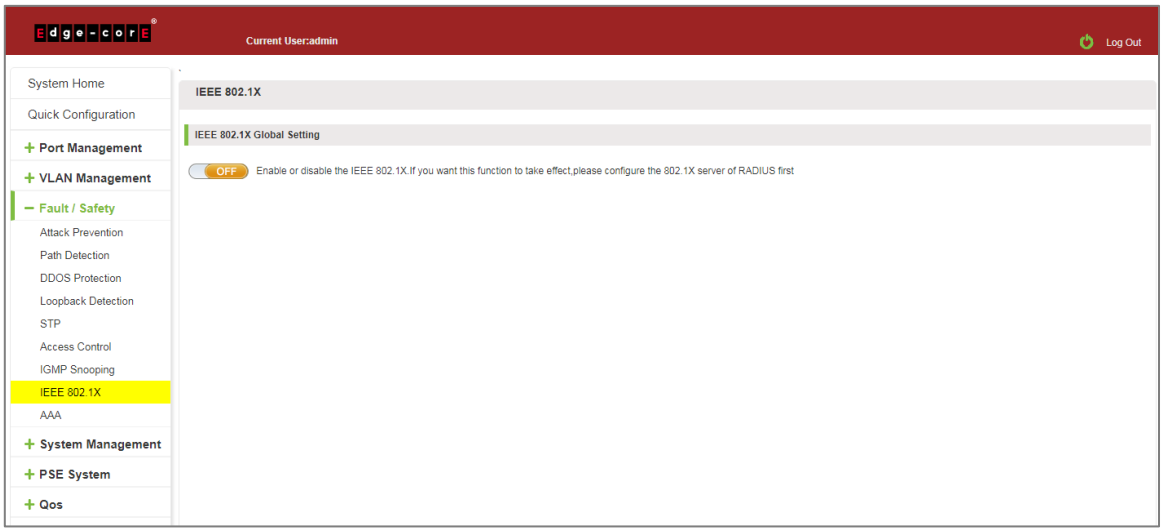


Figure 6-59: IEEE 802.1X

Click to Open.

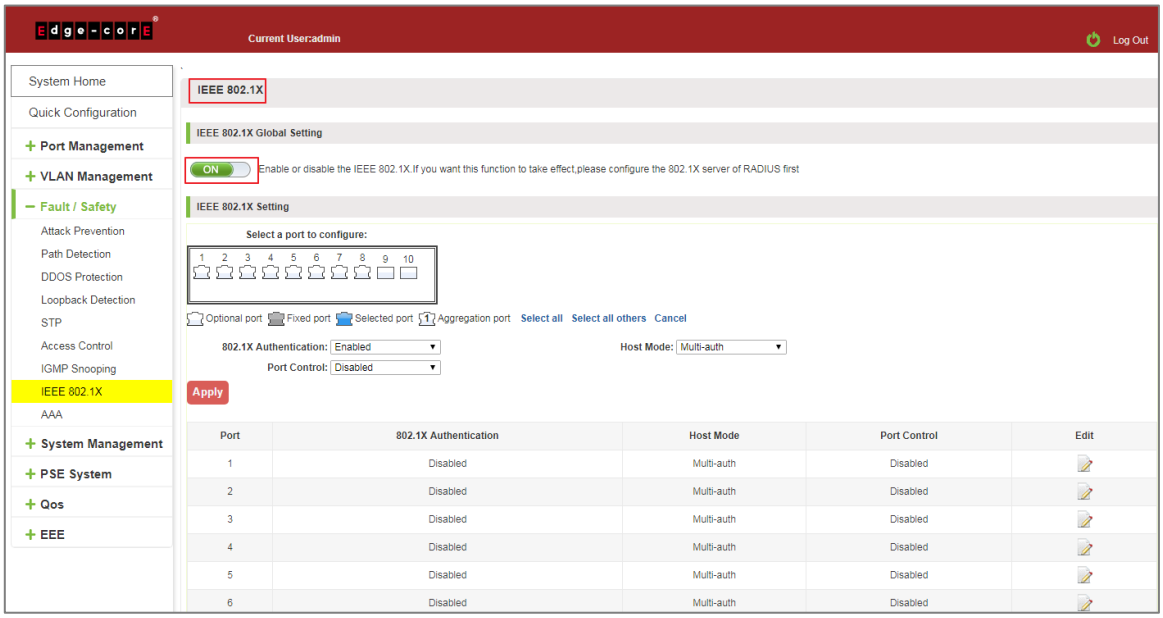


Figure 6-60: Enable IEEE 802.1X

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

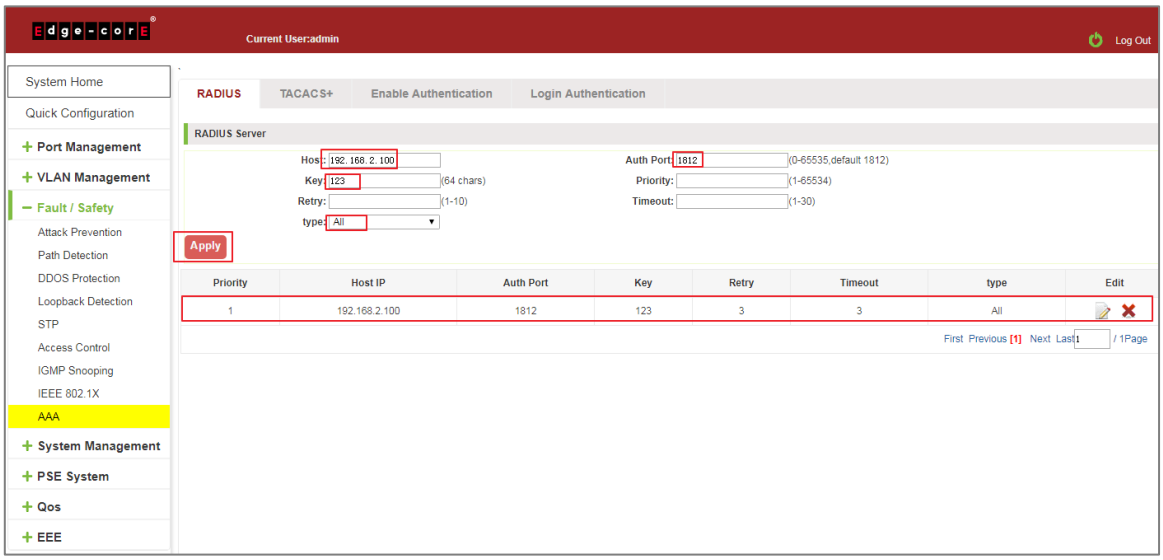


Figure 6-61: Configuration Radius

Switch enable 802.1X port Gi 0/2, Port Control: auto, Host Mode: multi-auth

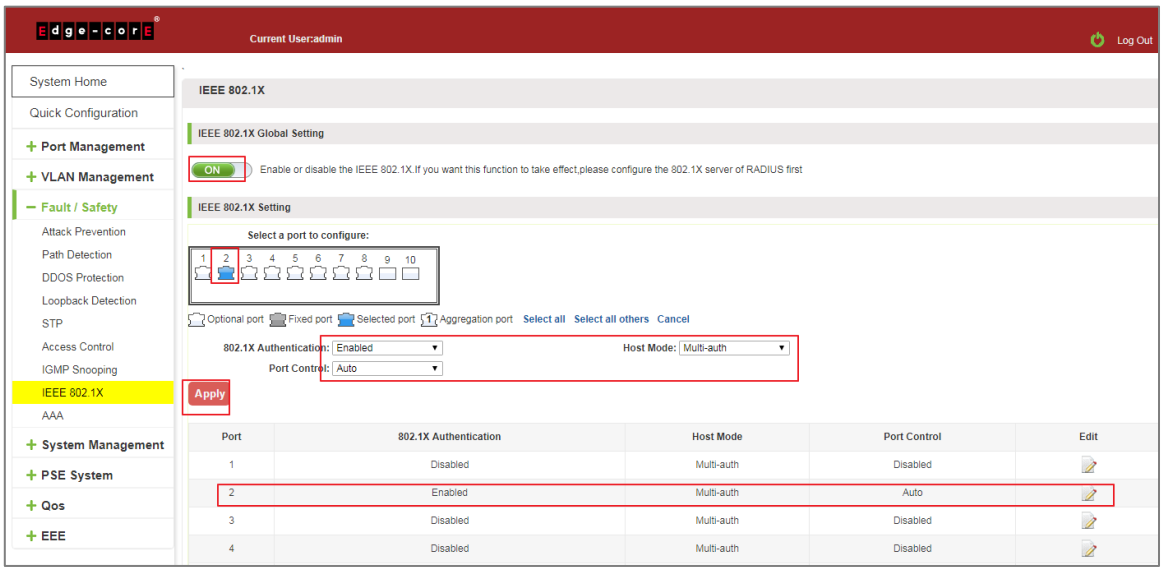


Figure 6-62: Configuration IEEE802.1X

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-unauth: 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 can not be forwarded, must also have passed authentication.

6.11 AAA

6.11.1 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

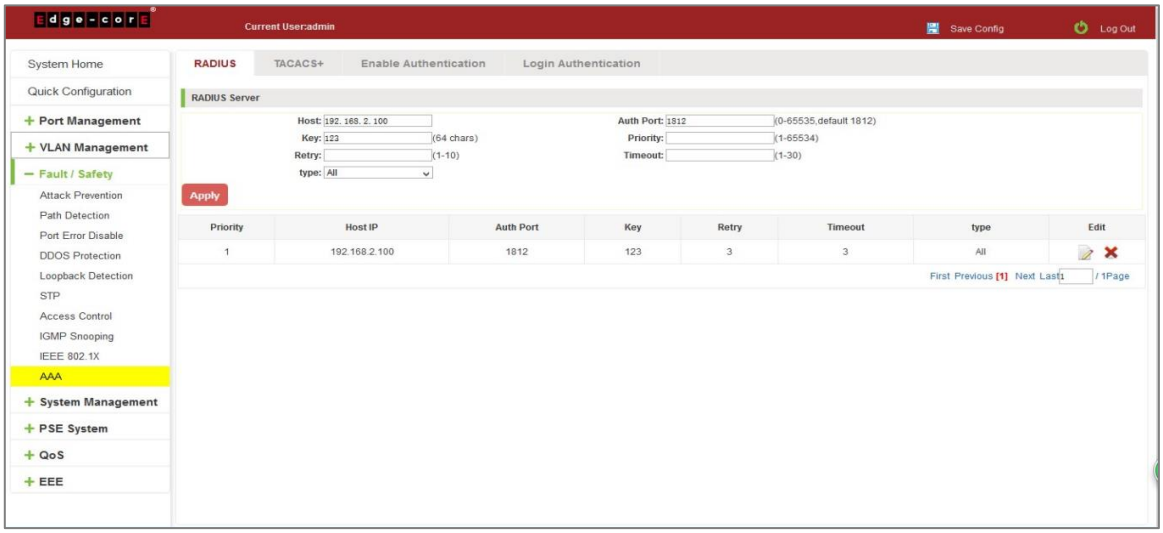


Figure 6-63: Configuration Radius

Switch config Method List: Name: test, Method 1: RADIUS, click "Apply".

Switch config Enable Authentication: Console: ECS2020, Telnet: ECS2020, SSH: ECS2020, click "Apply".

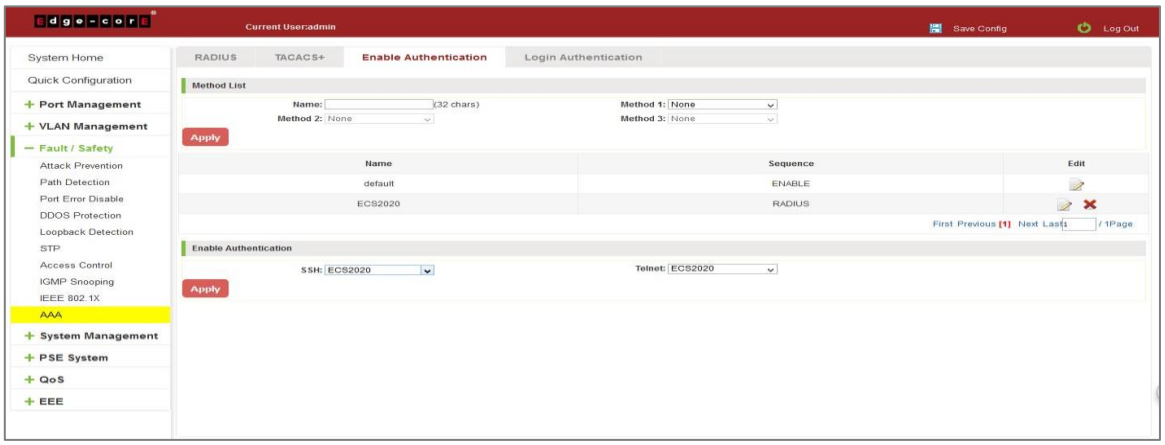


Figure 6-64: Configuration Enable Authentication

Switch config Method List: Name: ECS2020, Method 1: RADIUS, click "Save".

Switch config Enable Authentication: Console: ECS2020, Telnet: ECS2020, SSH: ECS2020, click "Save".

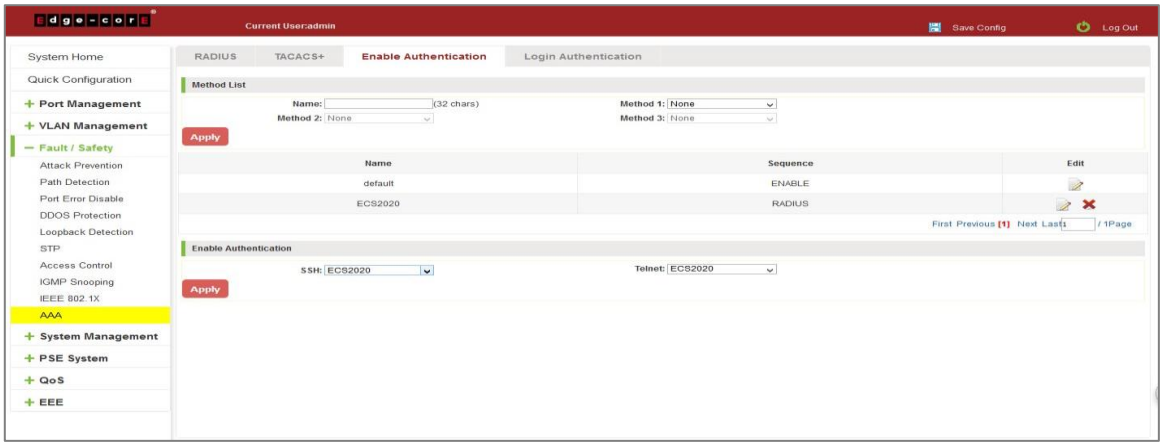


Figure 6-65: Configuration Login Authentication

TIPS:

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

6.11.2 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

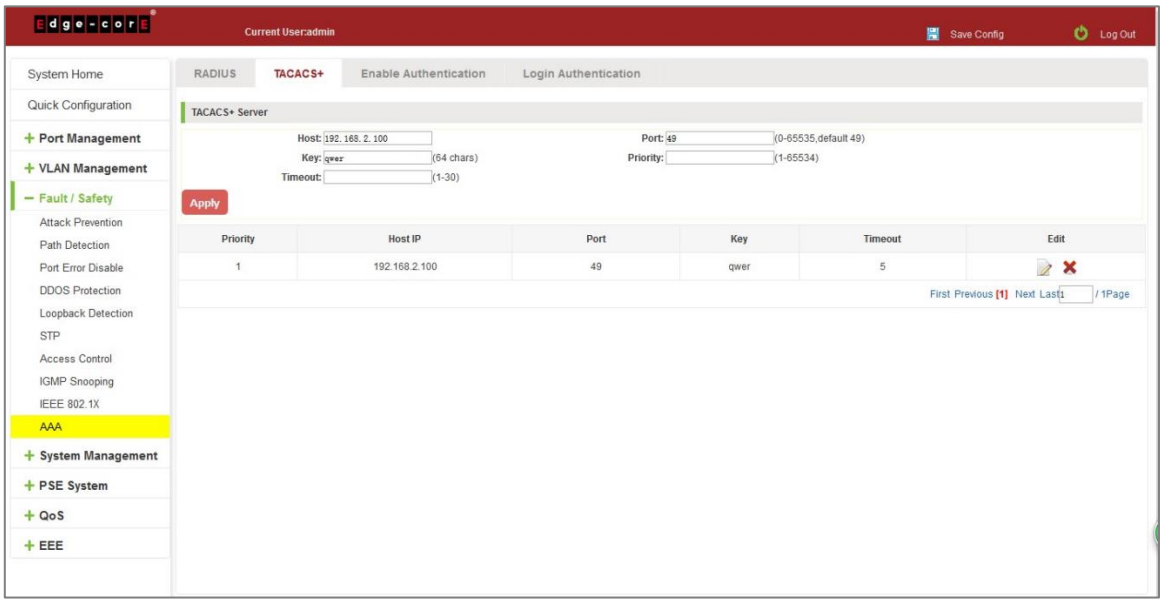


Figure 6-66: Configuration TACACS+

Switch config Method List: Name: ECS2020, Method 1: TACACS+, click "Save".

Switch config Enable Authentication: Console: ECS2020, Telnet: ECS2020, SSH: ECS2020, click "Save".

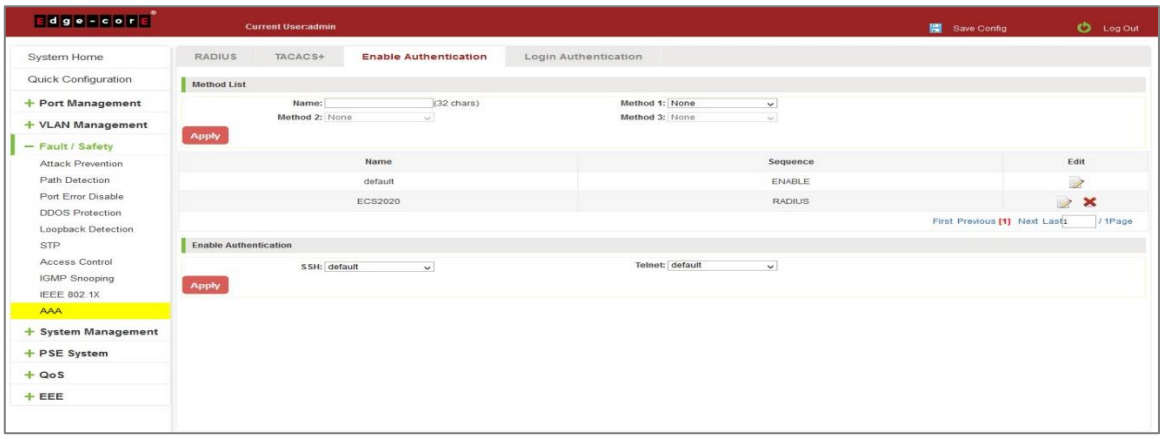


Figure 6-67: Configuration Enable Authentication

Switch config Method List: Name: ECS2020, Method 1: TACACS+, click "Apply".

Switch config Enable Authentication: Console: ECS2020, Telnet: ECS2020, SSH: ECS2020, click "Apply".

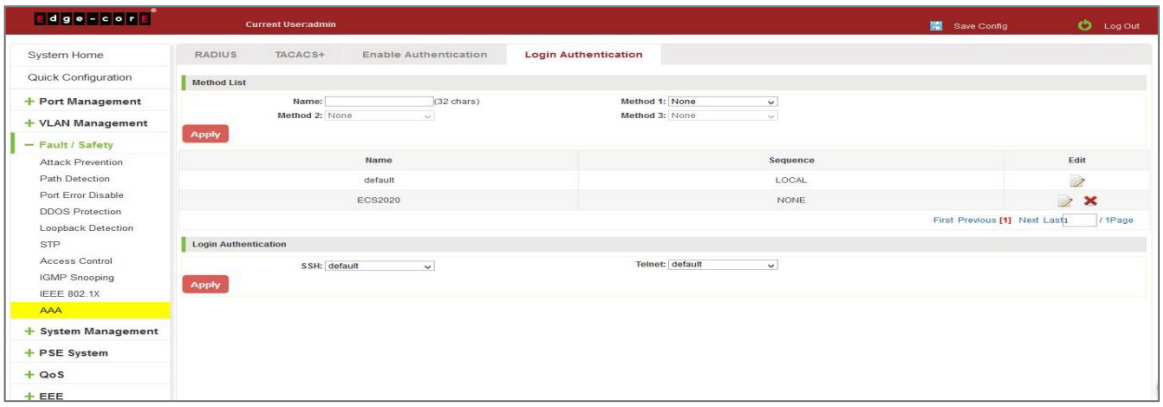


Figure 6-68: Configuration Login Authentication

You can successfully open AAA TACACS+ function

PC input right user name and password, PC can console, telnet and SSH switch

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

7 SYSTEM MANAGEMENT

7.1 SYSTEM SETTINGS

7.1.1 Interfaces VLAN

7.1.1.1 Configuration basic system settings

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

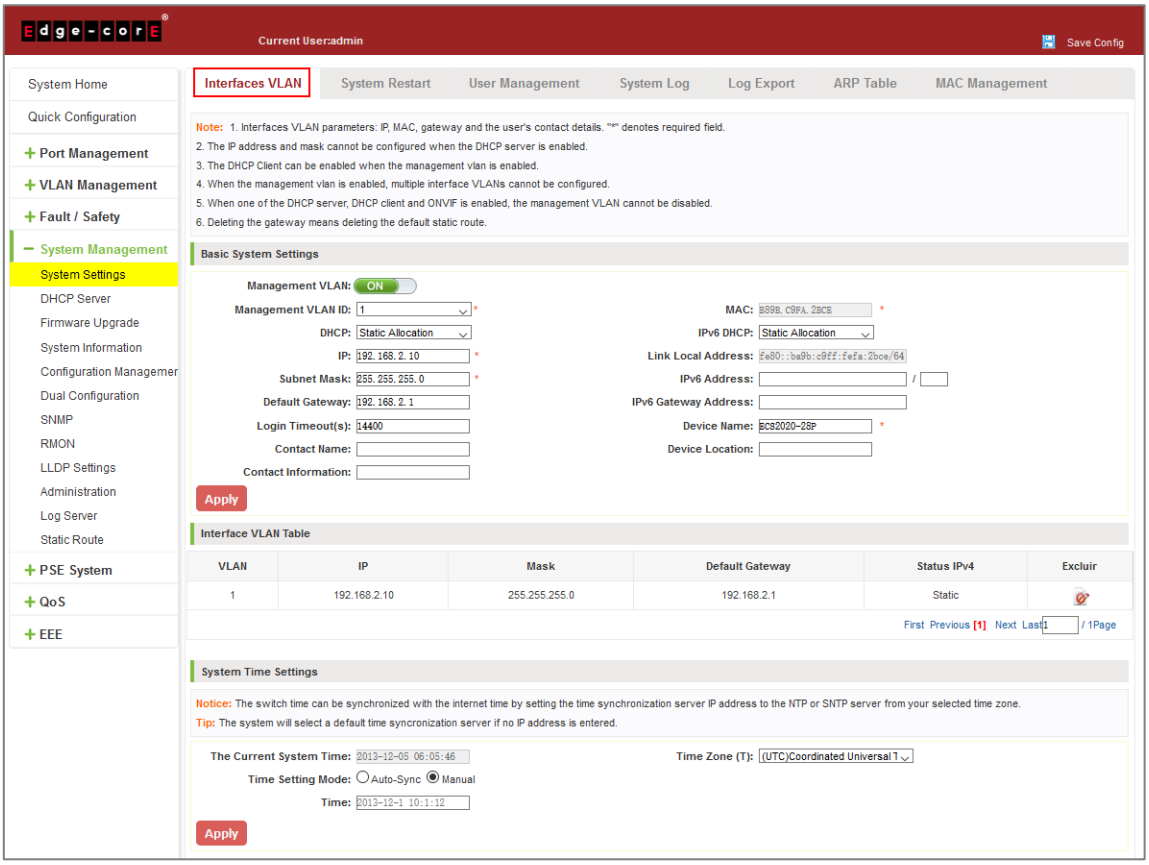


Figure 7-1: Basic System Settings

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" button to complete the configuration

7.1.1.2 System time synchronization

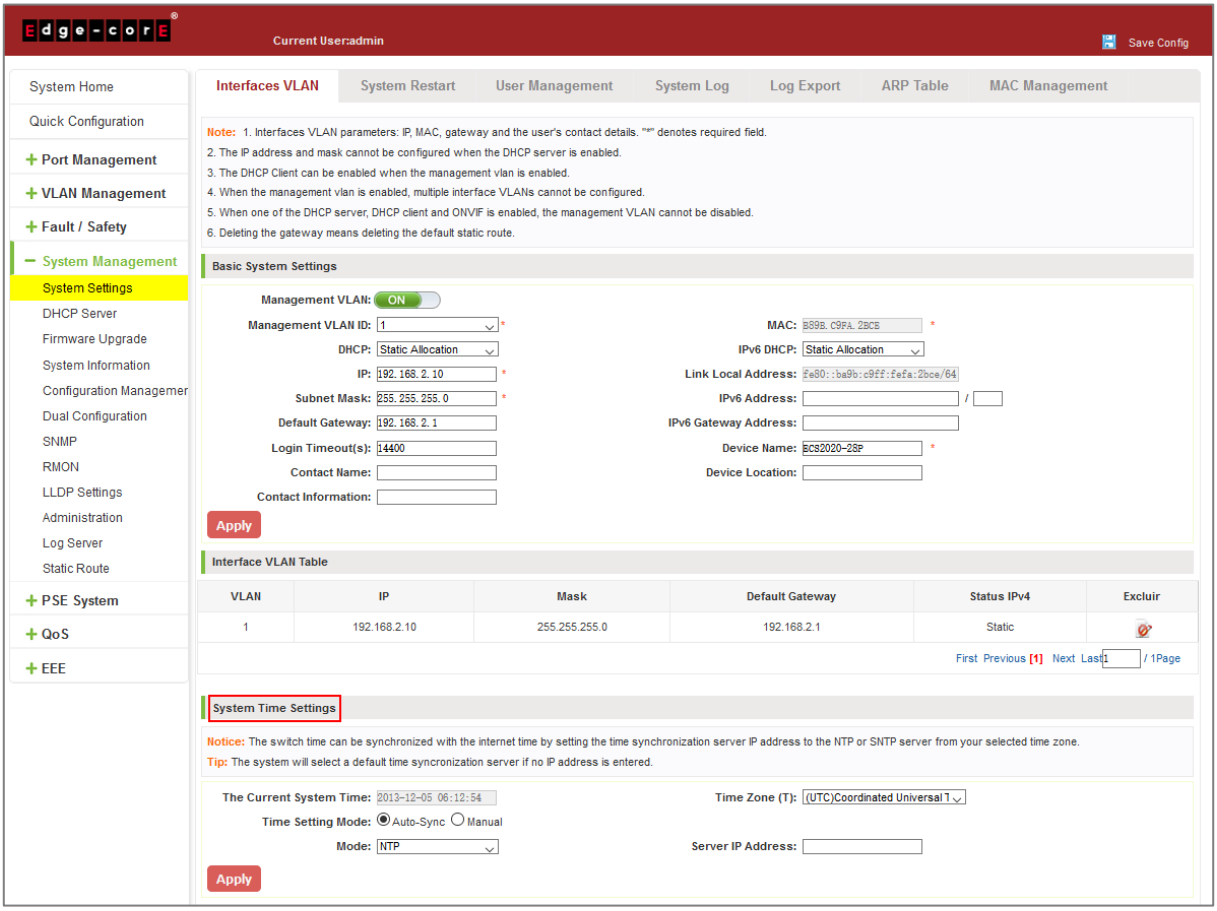
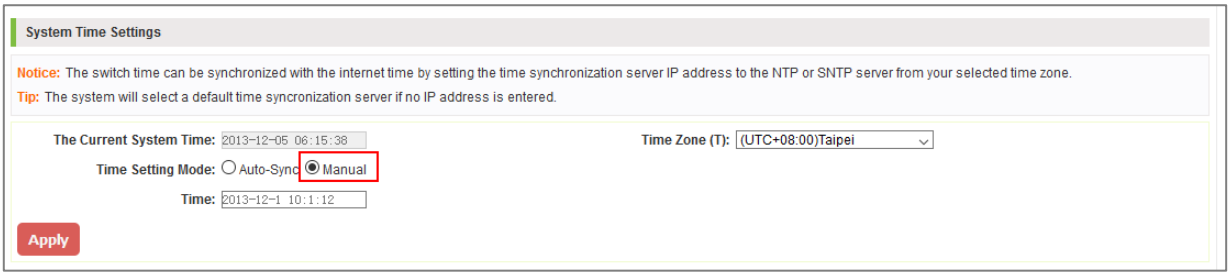


Figure 7-2: System Time Synchronization

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.



7.1.2 System restart

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

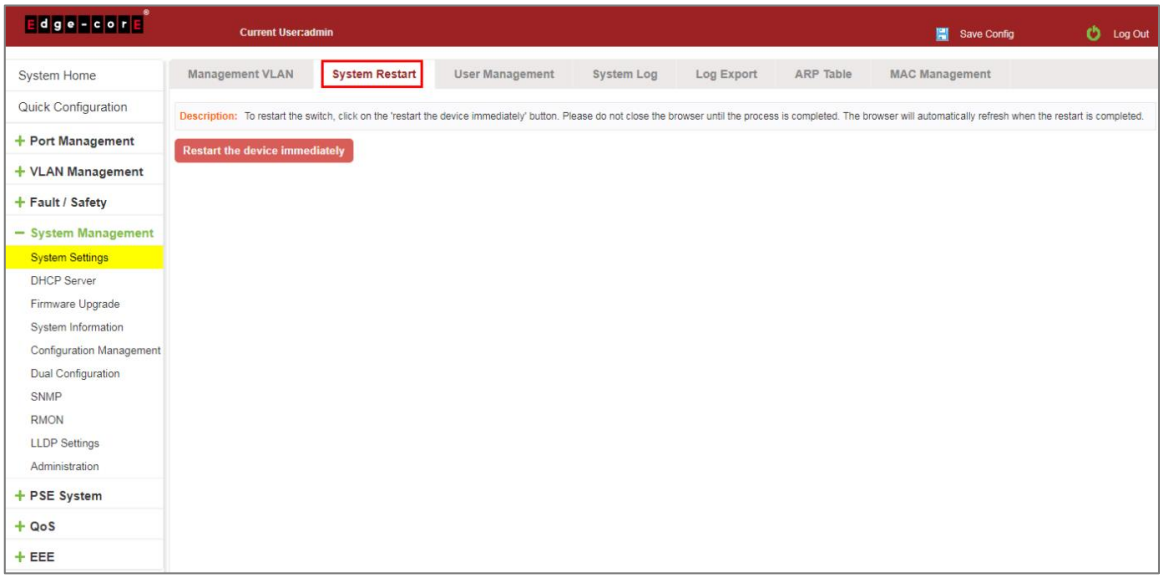


Figure 7-3: System Restart

Restart the device, follow these steps:

Step 1: Click on "Restart the device immediately" button;

Step 2: Click OK in the box that pops up "OK" button;

Step 3: Prompted to save the current configuration, depending on your need to select "OK" or "Cancel";

Step 4: After the restart the progress bar moves to 100%, reboot the device.

7.1.3 User Management

Click on the navigation bar "System Management" "System Settings" "User Management" to modify the super user password and telnet password:

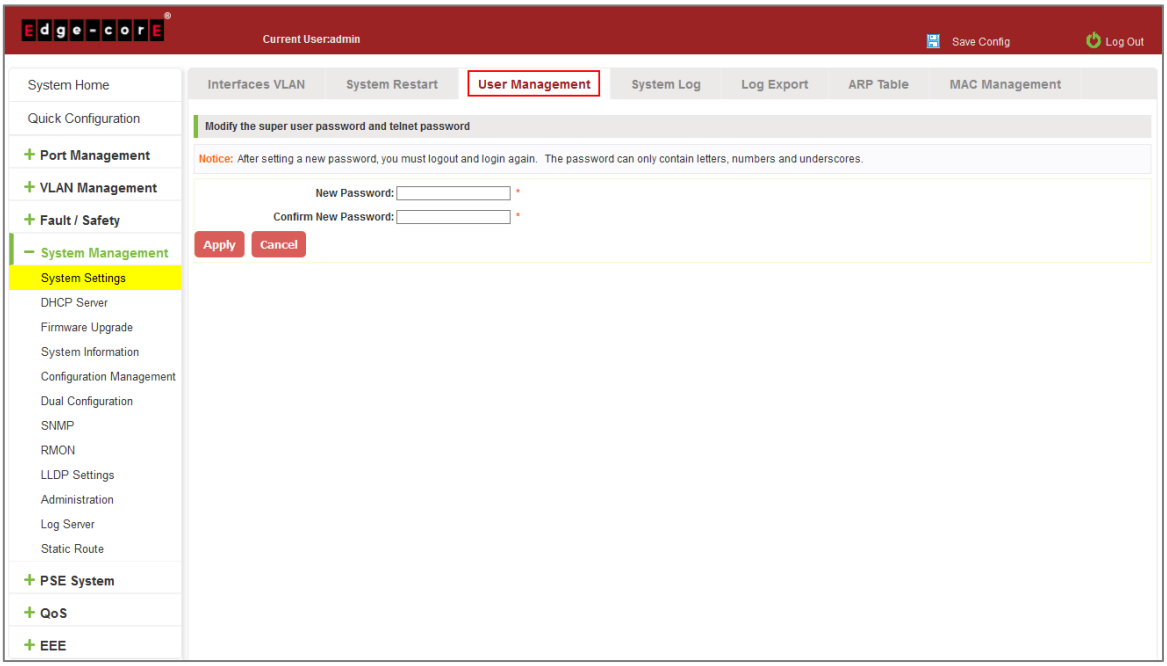


Figure 7-4: Change Password

To change the password follow these steps:

Step 1: Enter the new password: admin;

Step 2: Confirm new password: admin;

Step 3: Click the "Apply" button;

Step 4: Pop-up dialog box, click "OK" button.

7.1.4 System log

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

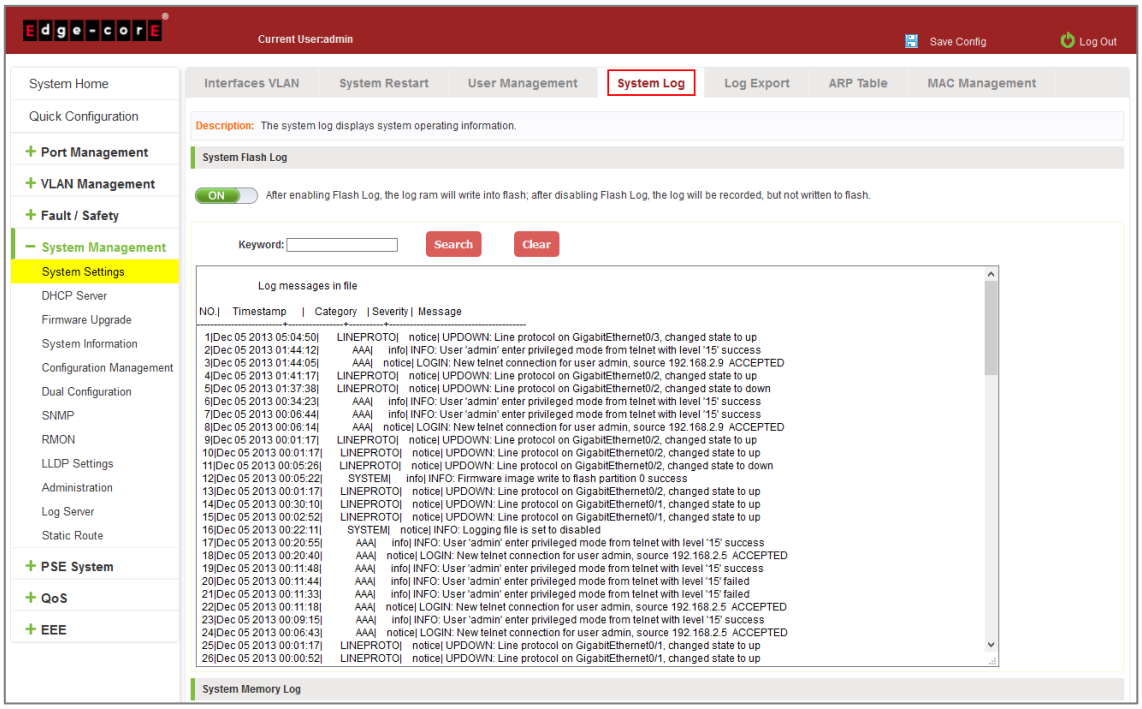


Figure 7-5: System Log

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

7.1.5 Log export

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

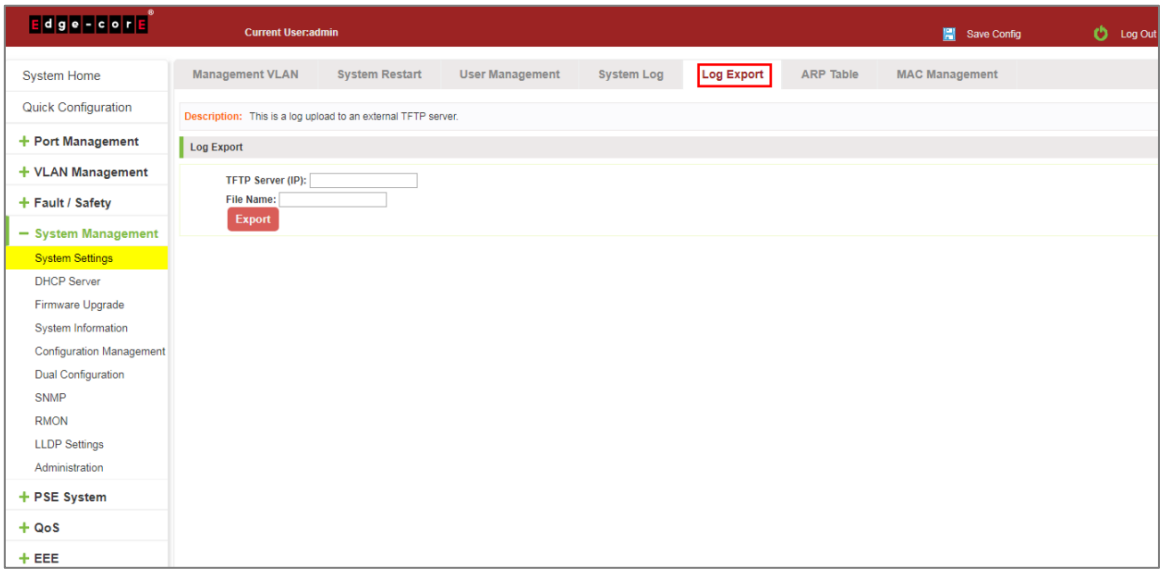


Figure 7-6: Log Export

7.1.6 ARP table

Click on the navigation bar "System Management" "System Settings" "ARP Table" to enter the ARP entry interface, you can view the ARP information:

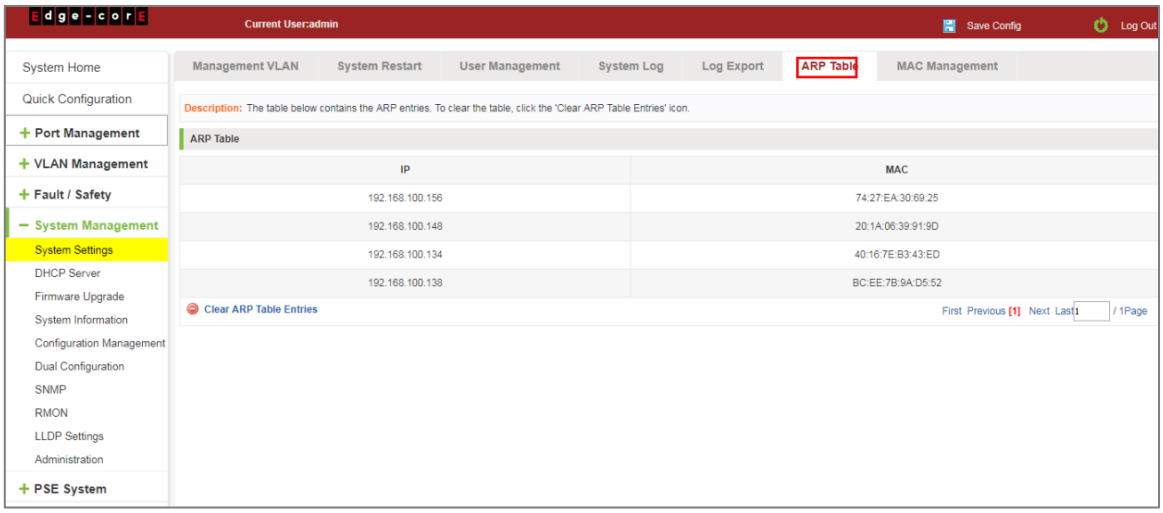


Figure 7-7: ARP Message

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

7.1.7 MAC management

7.1.7.1 MAC address lookup

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

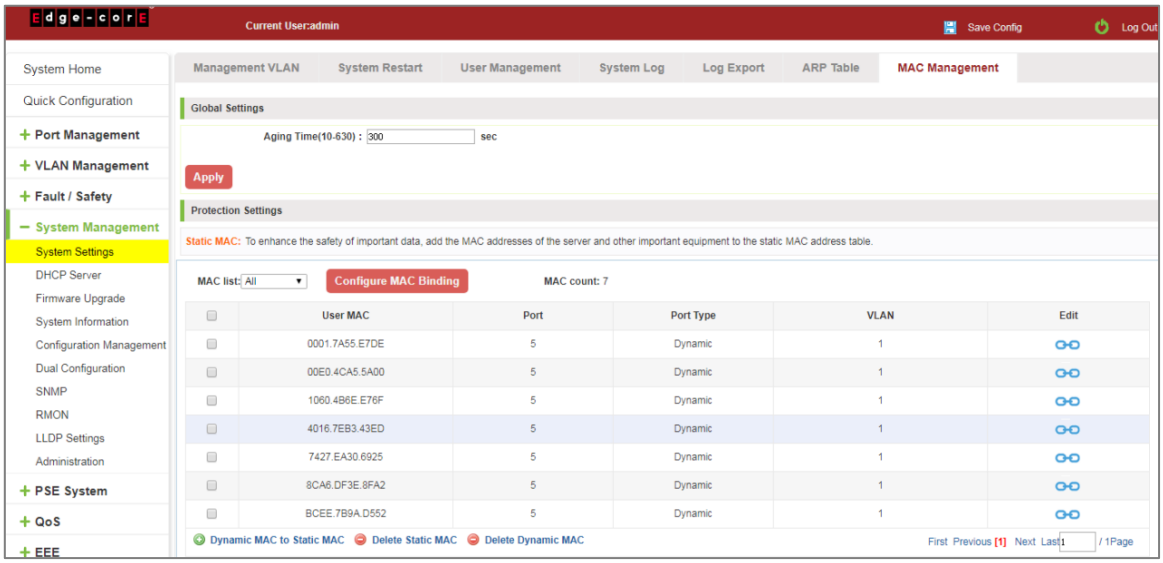


Figure 7-8: MAC address Lookup Display

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

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

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

7.1.7.2 Add a static MAC address type

1. Use manual binding MAC address
   Click the "Configure MAC Binding" After, you can configure a static MAC address type in the MAC address configuration area:

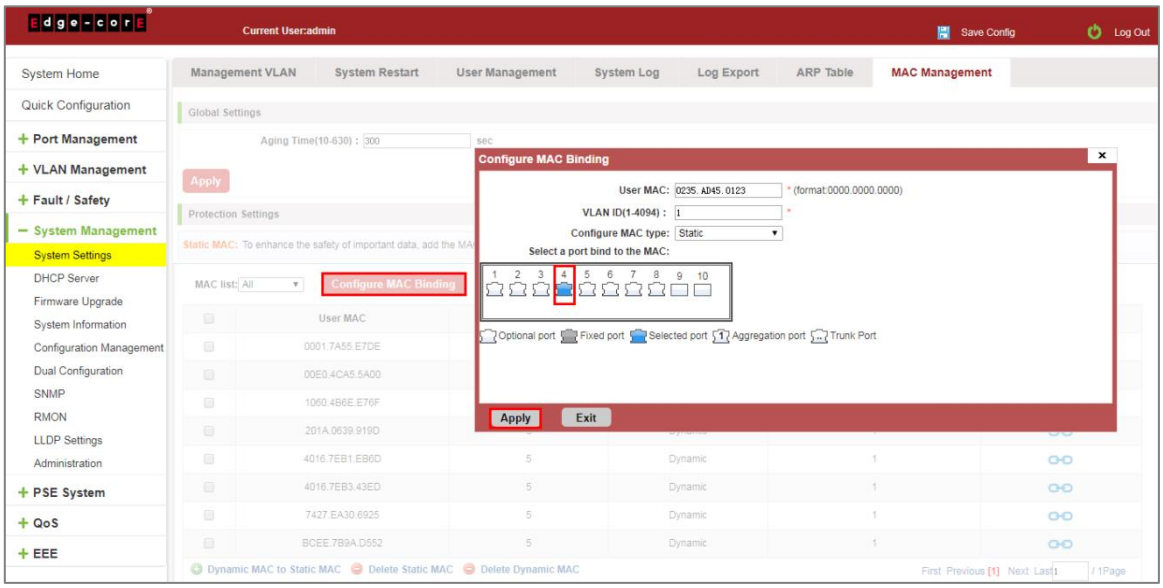


Figure 7-9: MAC Addresses Statically Bound Static Configuration

Statically typed MAC address configuration steps are as follows:

Step 1: Click the "Configure MAC Binding" button;

Step 2: In the "User MAC" text box to enter the MAC address, such as 0001.7A4F.74D2;

Step 3: In the "VLAN ID" text box to enter the VLAN ID, such as 1;

Step 4: Select ports in the port panel;

Step 5: Click on "Apply" to complete the configuration.

2. Use"  " button binding static MAC address

In the MAC address list, select the MAC address to be bound, click on the left "  " button, to achieve binding:

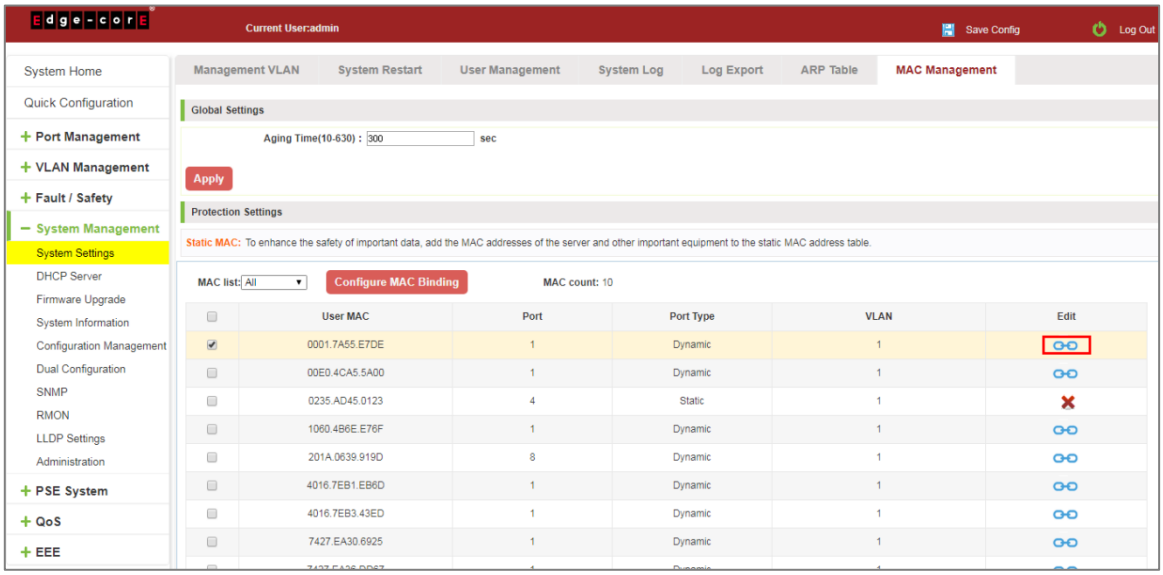


Figure 7-10: MAC Address of the Static Binding Configuration

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

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

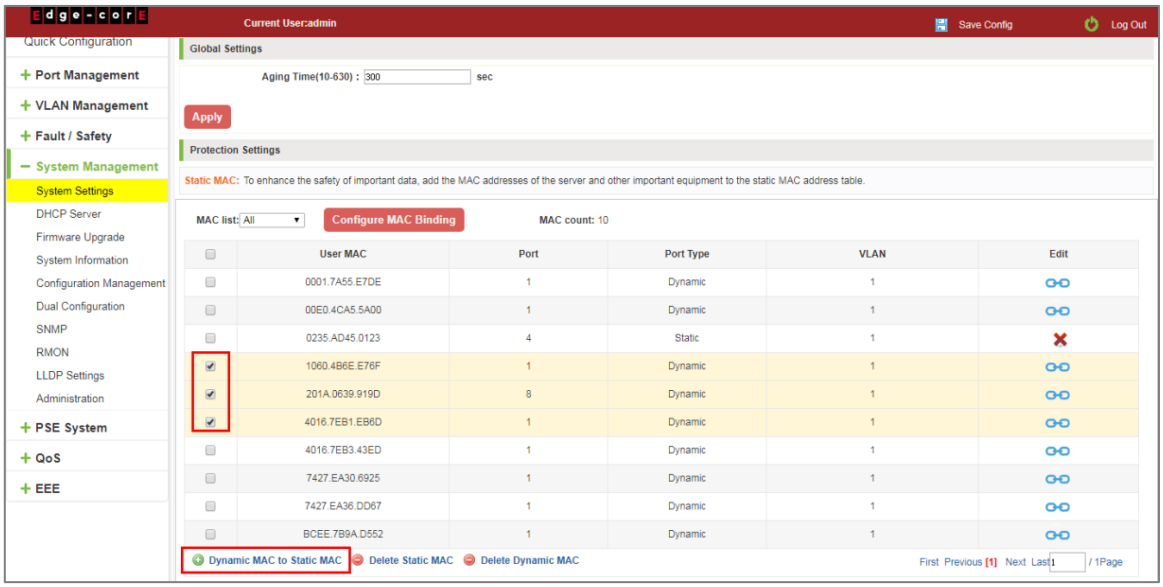


Figure 7-11: Batch-MAC Binding Configuration

7.1.7.3 Remove the static MAC address type

1. Single MAC records are deleted

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

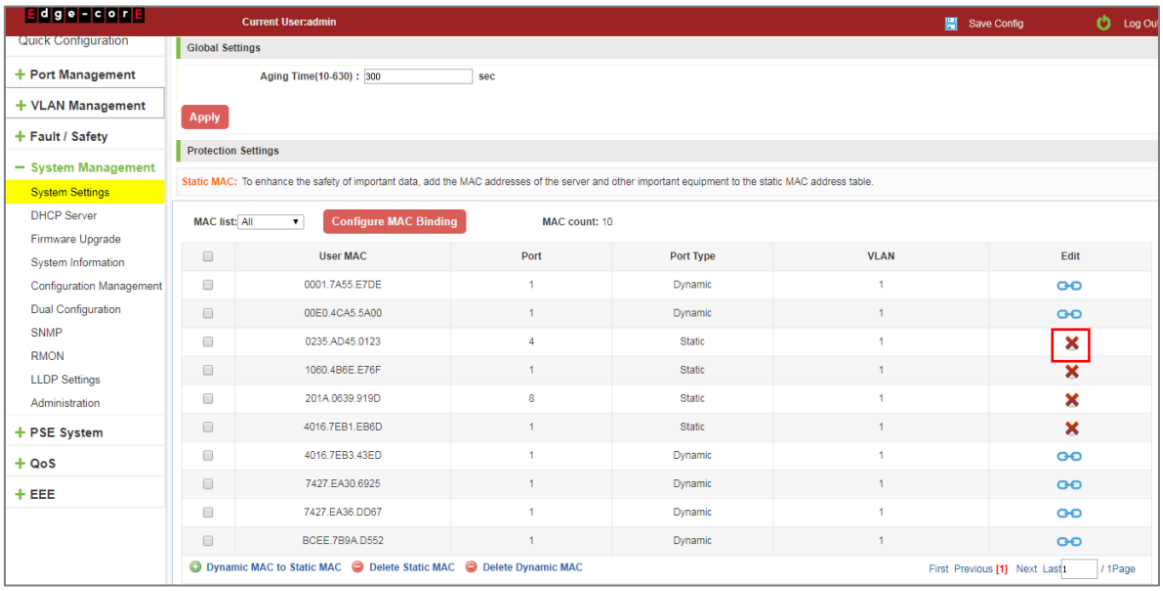


Figure 7-12: MAC Address Deletion

Remove MAC address configuration steps are as follows:

Step 1: To delete the selected MAC address;

Step 2: Click " ✖ " button to delete the configuration.

2. Batch delete a static MAC address

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

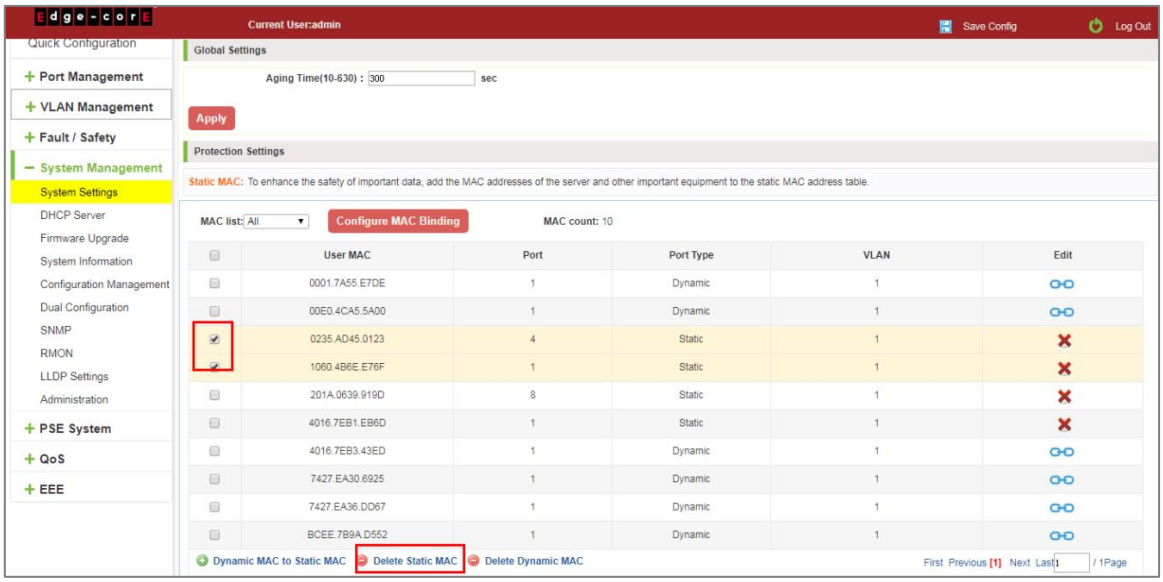


Figure 7-13: MAC Address Batch Deletion

3. Delete all dynamic MAC address

In the MAC address list, click "Delete Dynamic MAC" button to clear all dynamic mac address:

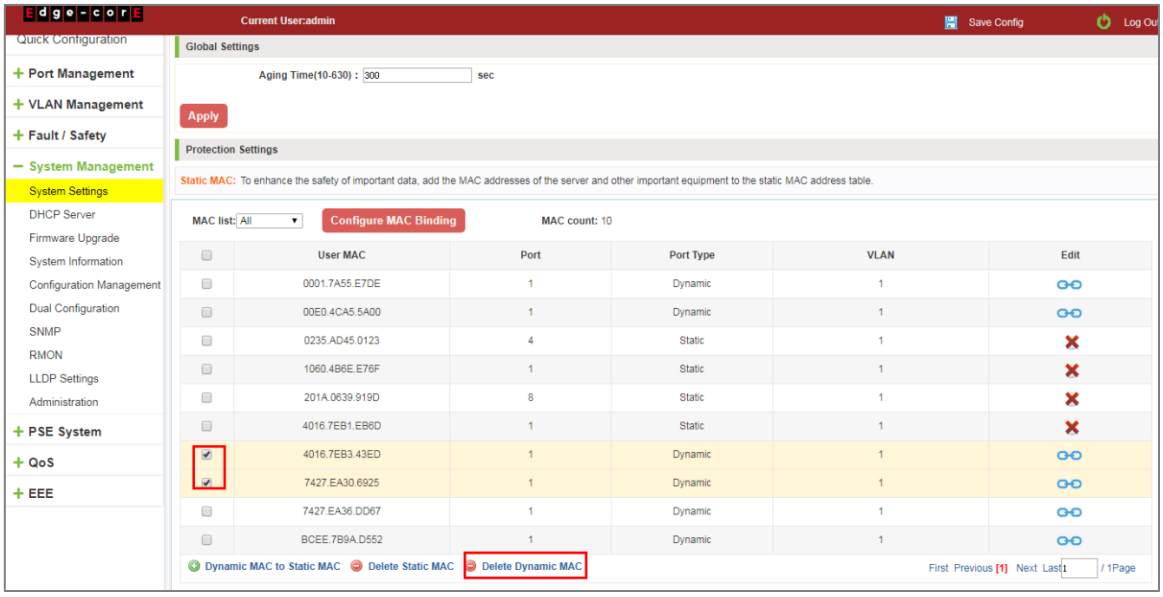


Figure 7-14: Clear All Dynamic MAC Address

7.2 DHCP SERVER

7.2.1 DHCP server info

Click the "System Management" "DHCP Server" to view the DHCP Server configuration:

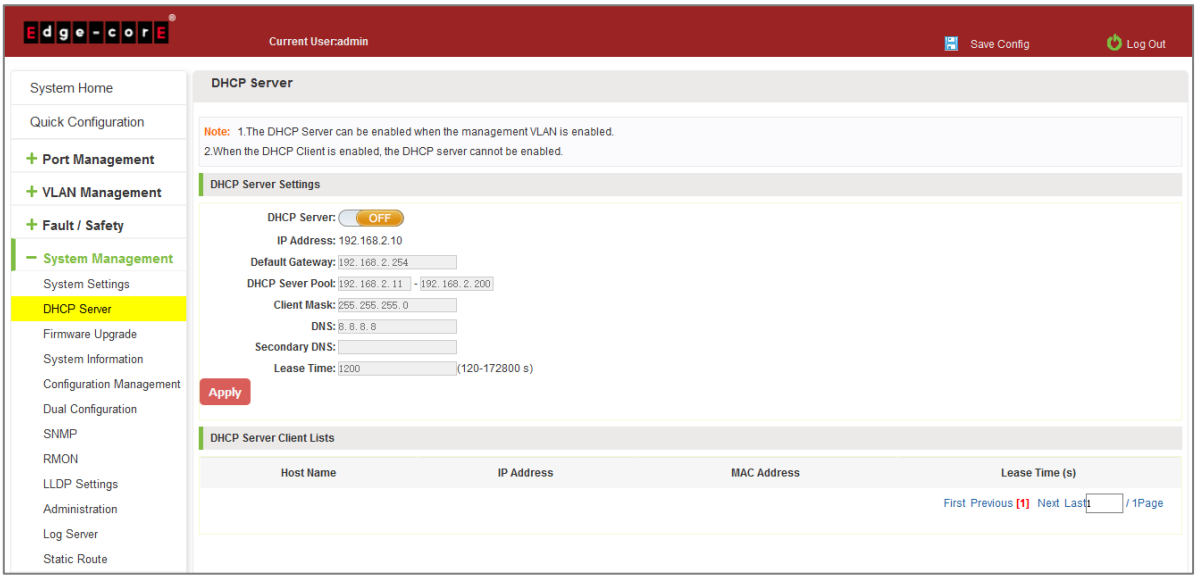


Figure 7-15: DHCP Server Info

7.2.2 Enable the DHCP server

Enable the DHCP server, address pool IP range and device IP must be the same network segment IP:

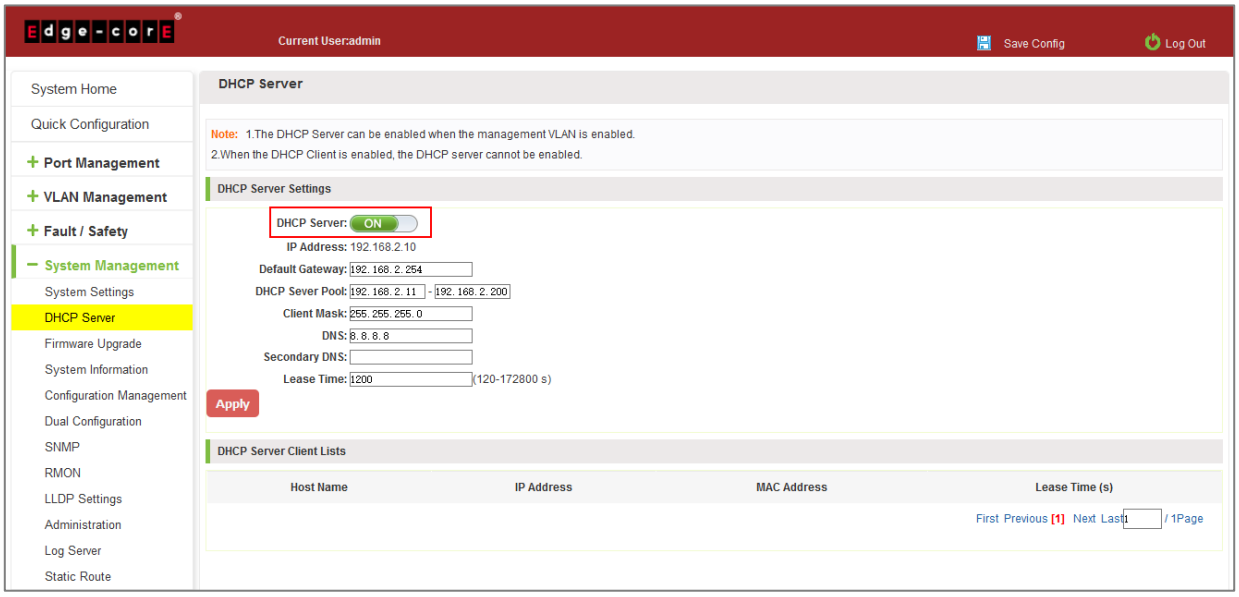


Figure 7-16: Enable DHCP Server

When the host and the device are connected directly, the IP assigned to the DHCP server will be displayed in the DHCP server client list.

7.3 SYSTEM UPGRADE

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

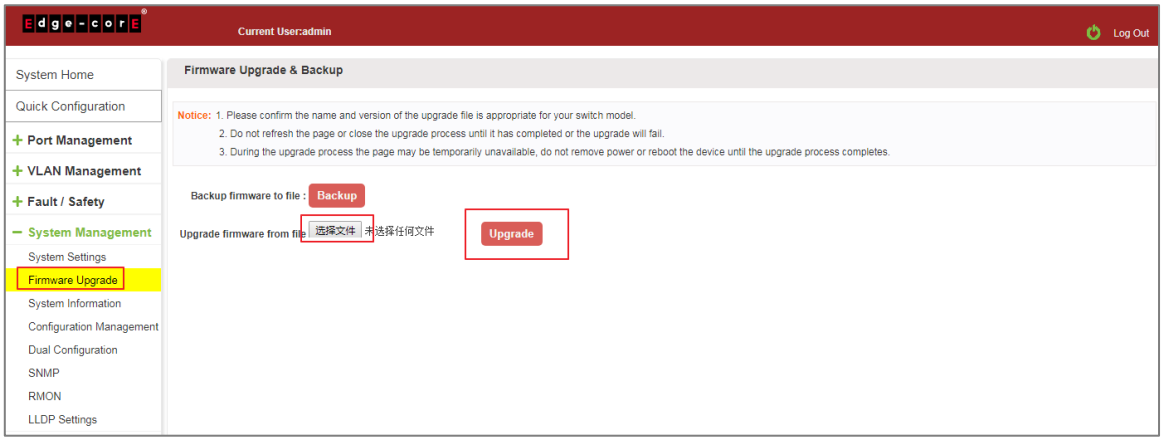


Figure 7-17: Switch System Upgrade

Switch system upgrade steps are as follows:

Step 1: Click "Choose File" button to select the switch upgrade file;

Step 2: Click the "Upgrade" button switch to start the upgrade new software;

Step 3: When the upgrade progress bar is at 100%, the switch will automatically reboot, completion of the upgrade is completed.

7.4 SYSTEM INFORMATION

7.4.1 Memory information

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

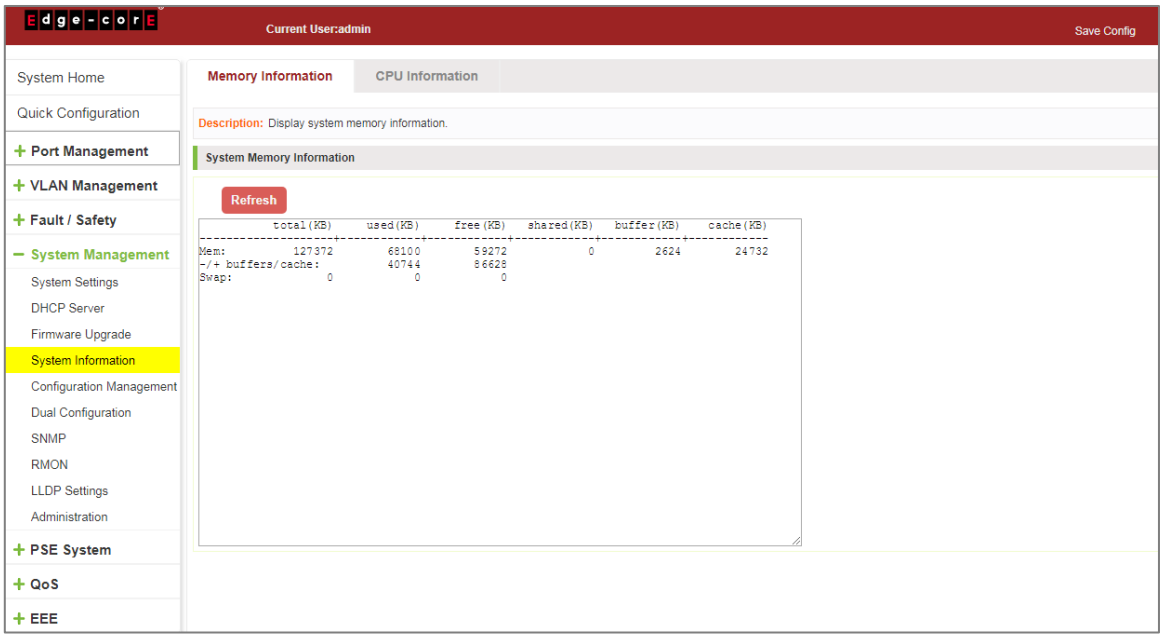


Figure 7-18: System Memory Information

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

7.4.2 CPU information

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

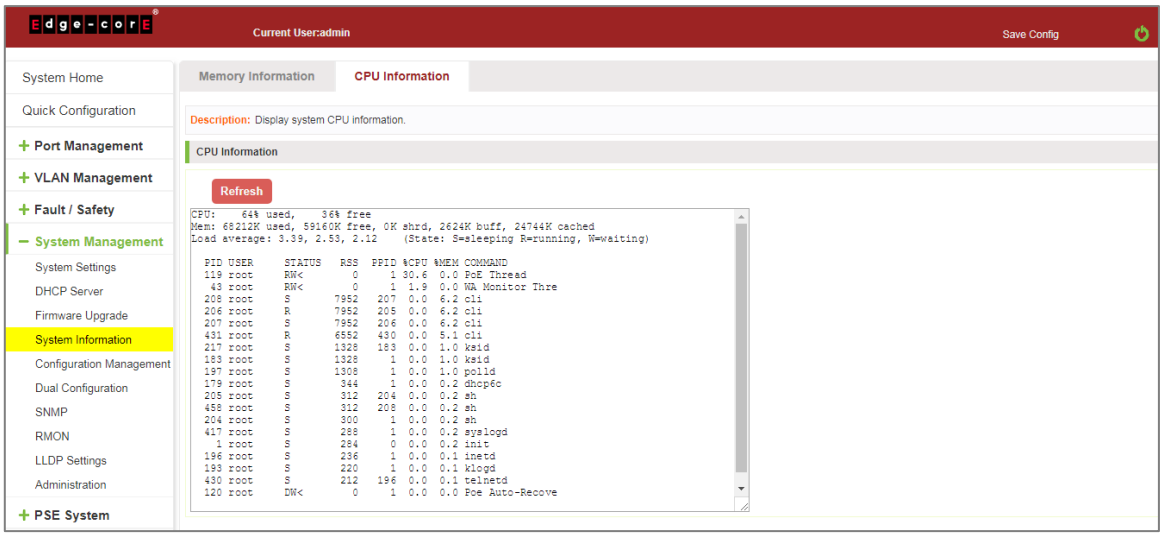


Figure 7-19: CPU Information

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.

7.5 CONFIGURATION MANAGEMENT

7.5.1 Configuration management

1. To see the current configuration

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

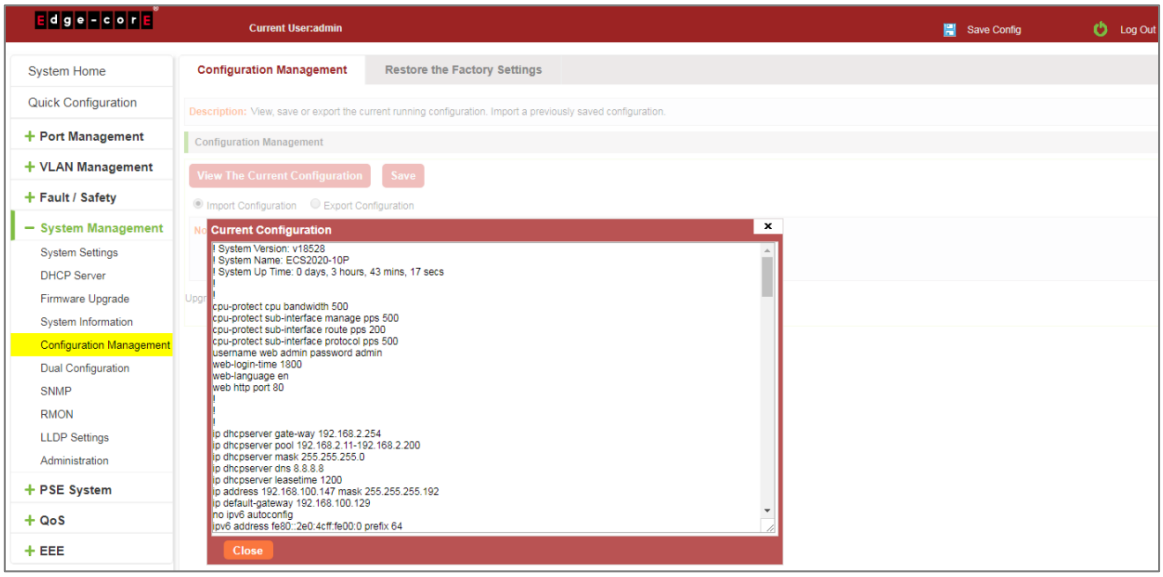


Figure 7-20: View the Current Configuration

2. Save the current configuration

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

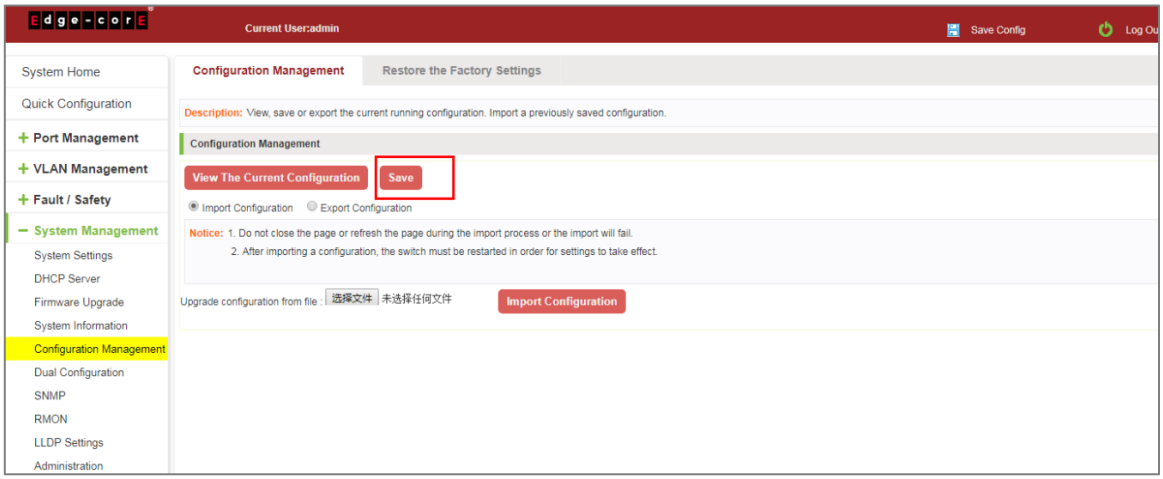


Figure 7-21: To Save the Current Configuration

3. The configuration

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

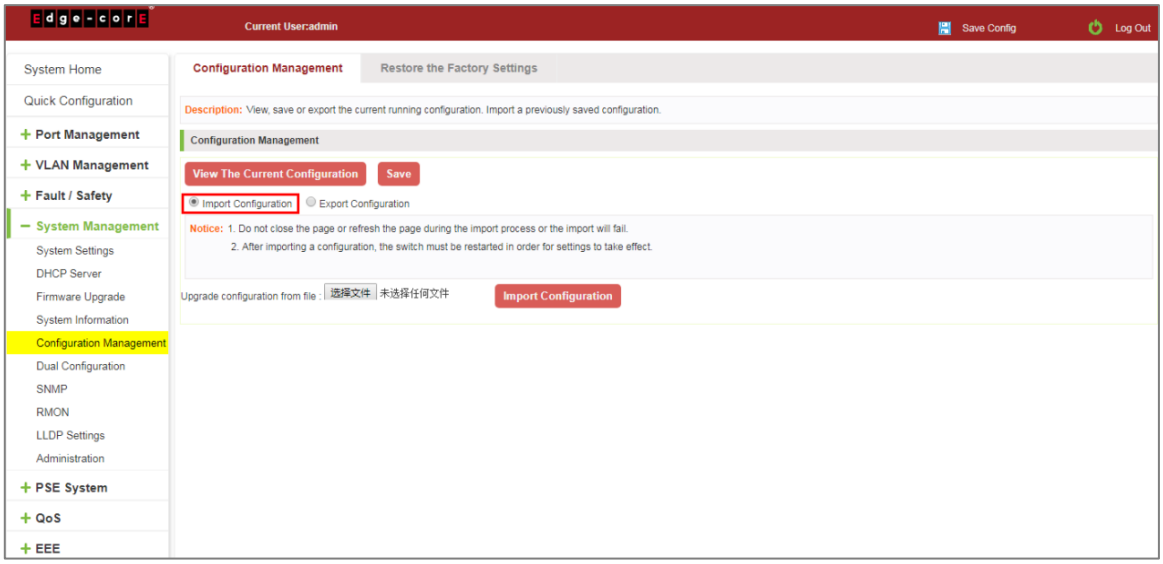


Figure 7-22: Imported Configuration

Import the configuration steps are as follows:

Step 1: Select the "Import Configuration";

Step 2: Click "Choose File" button to find you want to import the configuration File;

Step 3: Click on "Import Configuration" button;

Step 4: Confirm the restart.

4. Export configuration

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

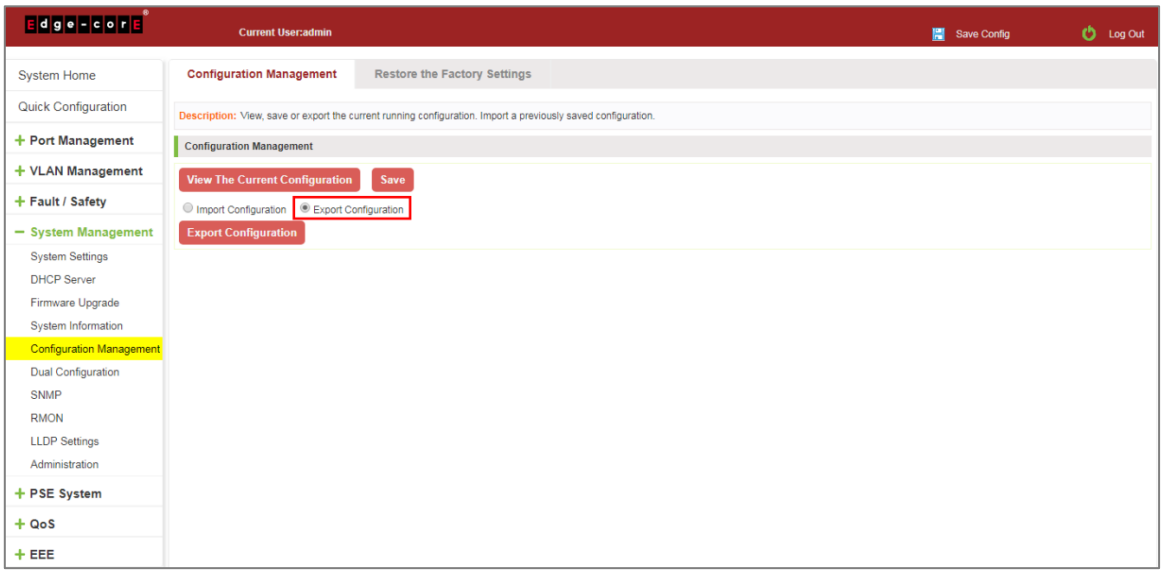


Figure 7-23: Export Configuration

7.5.2 Restore factory settings

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

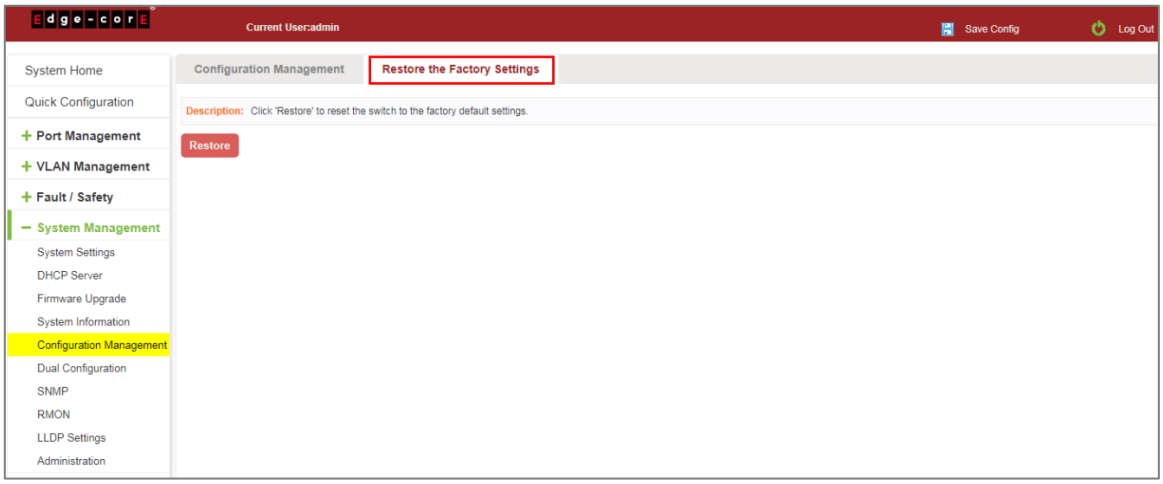


Figure 7-24: Restore Factory Settings

Factory default operation steps are as follows:

Step 1: Click the "Restore the Factory Settings" button;

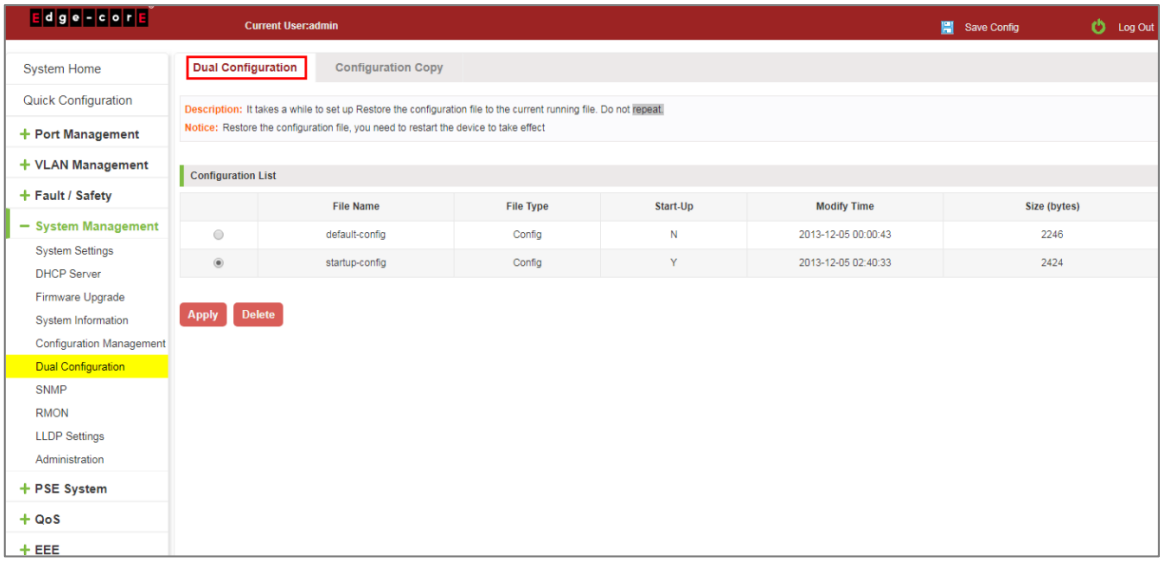
Step 2: In the pop-up confirmation box, click the "OK" button;

Step 3: After the completion of the reset switch, wait for equipment to restart, switch back to factory default configuration.

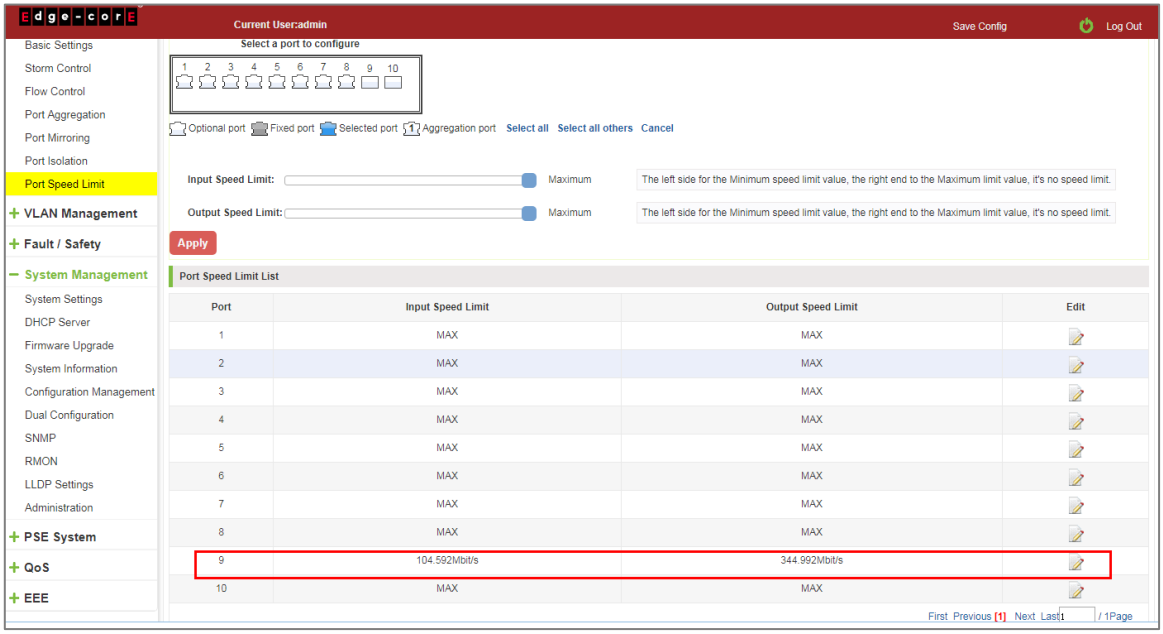
7.6 DUAL CONFIGURATION

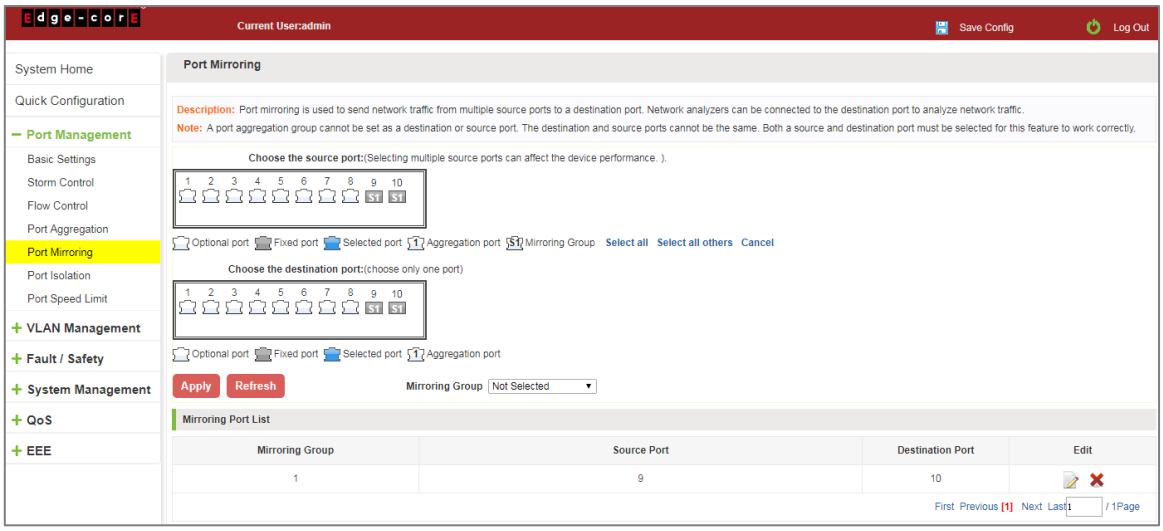
7.6.1 Backup and restore the current configuration file

Click on "System Management" "Dual Configuration".

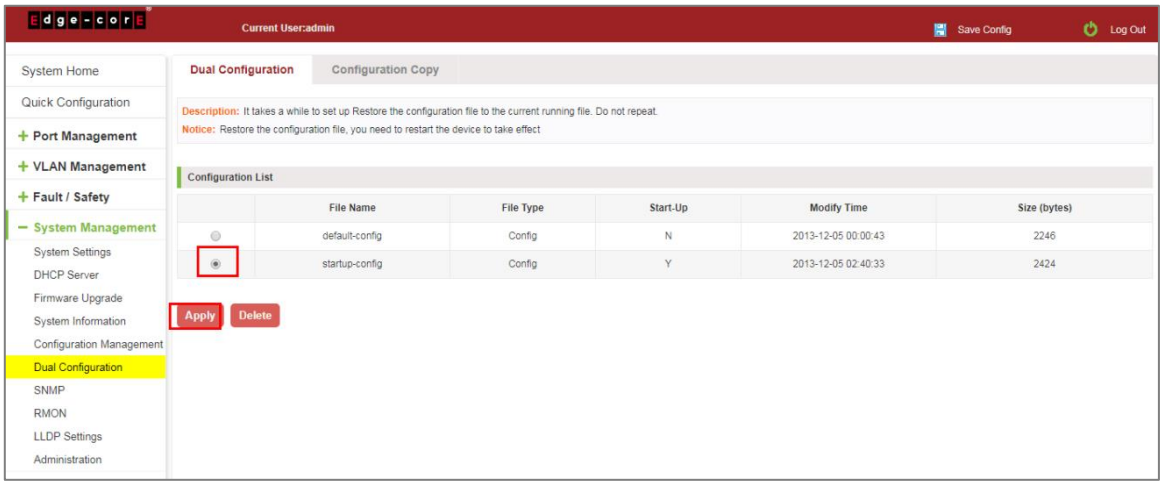


1. Configure some functions, such as: IP address, port speed limit, port mirroring and other functions.

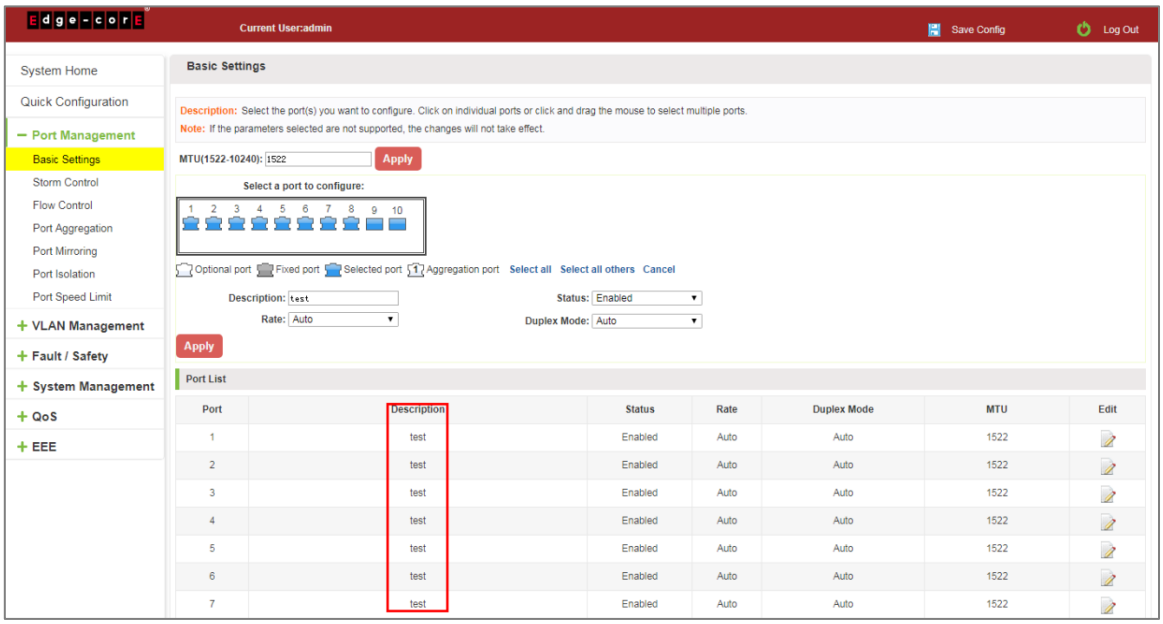




2. Click on the "System Management" "Dual configuration". To configure the switch backup the current running profile.



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



4. Click on the "Apply"/"Delete". The configuration file is applied, the system will set the parameters to run at system startup; can also delete the configuration file.

7.6.2 Configuration Copy

Back up the running-config file to the startup-config file or backup-config file.

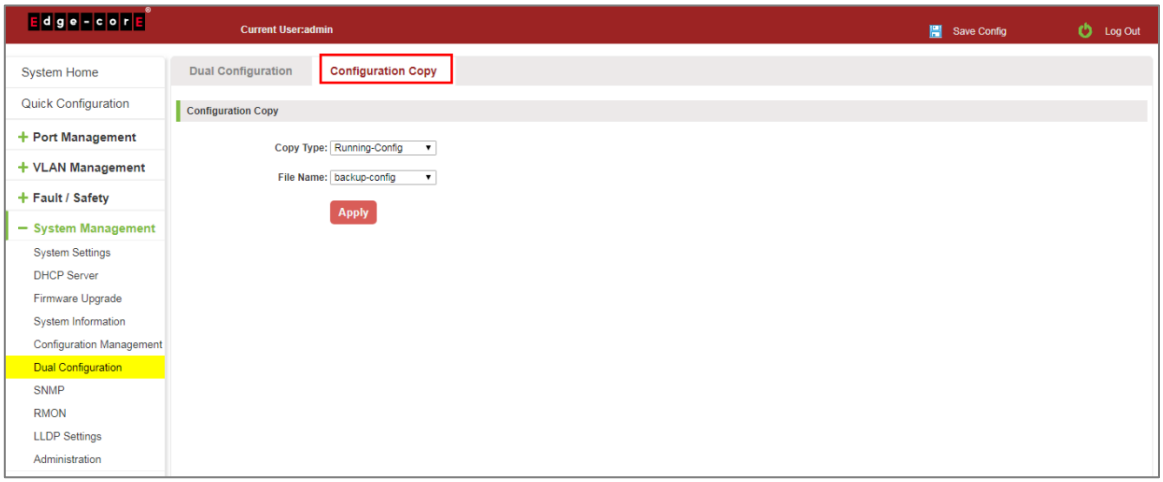


Figure 7-25: Configuration copy

7.7 SNMP

7.7.1 Check the SNMP

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

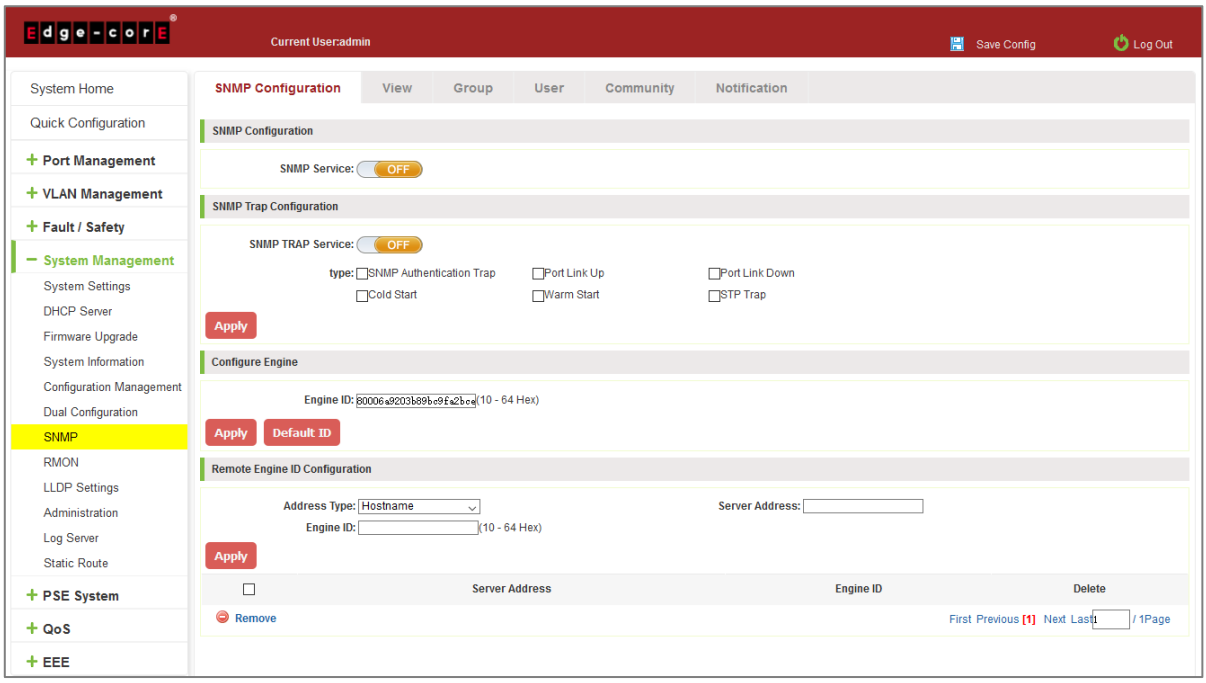


Figure 7-26: View the SNMP Configuration Information

By default, SNMP is not open;

For SNMP monitoring software and switches, the SNMP version must be consistent. Inconsistencies can lead to communication failure.

7.7.2 Activate the SNMP

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

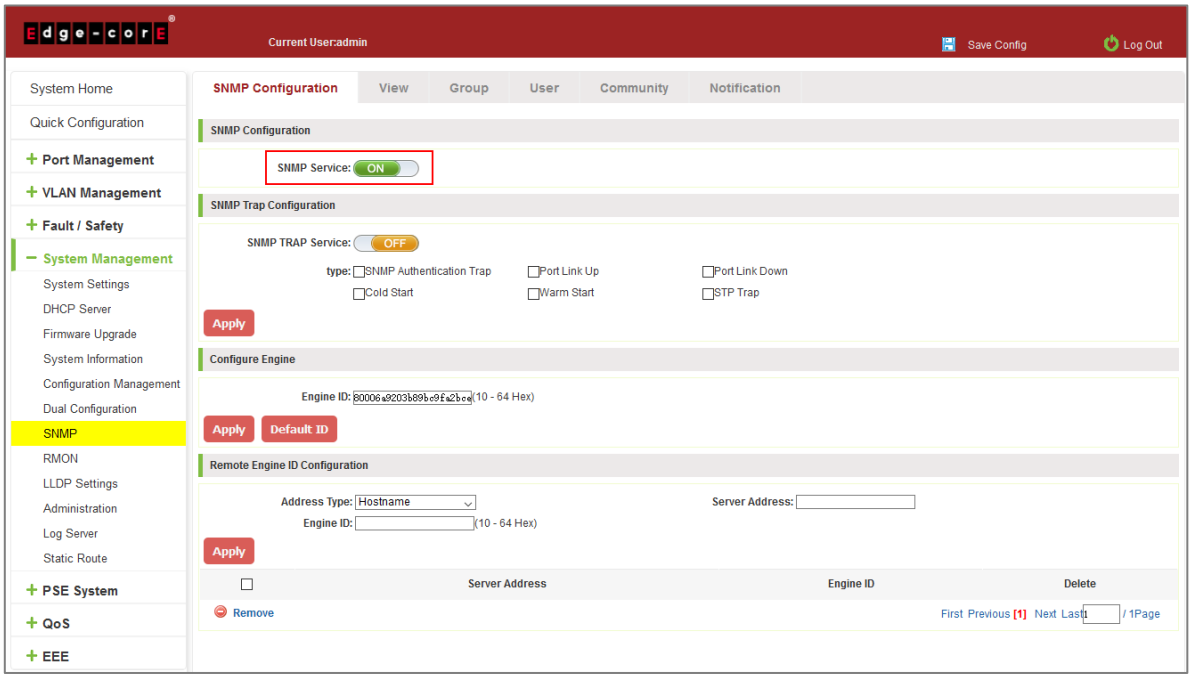


Figure 7-27: Activation SNMP Function

7.7.3 To disable the SNMP

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

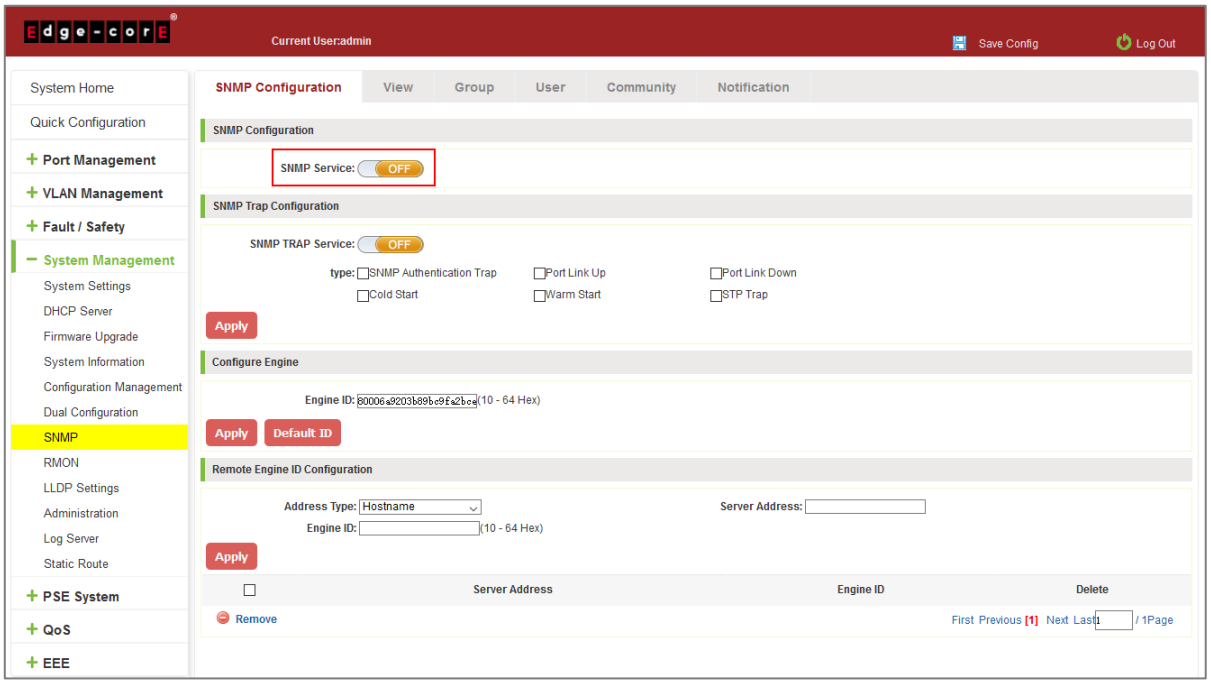


Figure 7-28: Disable the SNMP Function

7.7.4 Activate the TRAP

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

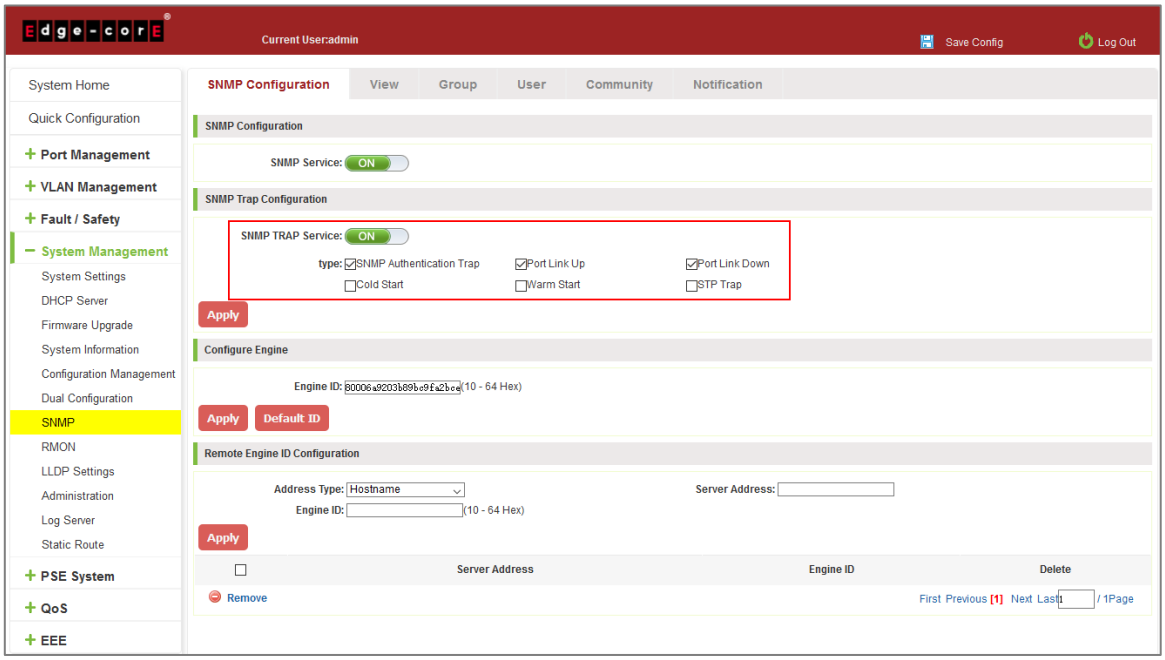


Figure 7-29: Activation Function of the TRAP

To activate TRAP functions, follow these steps:

Step 1: Select the "ON" option.

Step 2: Select the trap types you want to enable.

Step 3: Click the "Apply" button to complete the configuration.

7.7.5 Disable the TRAP

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

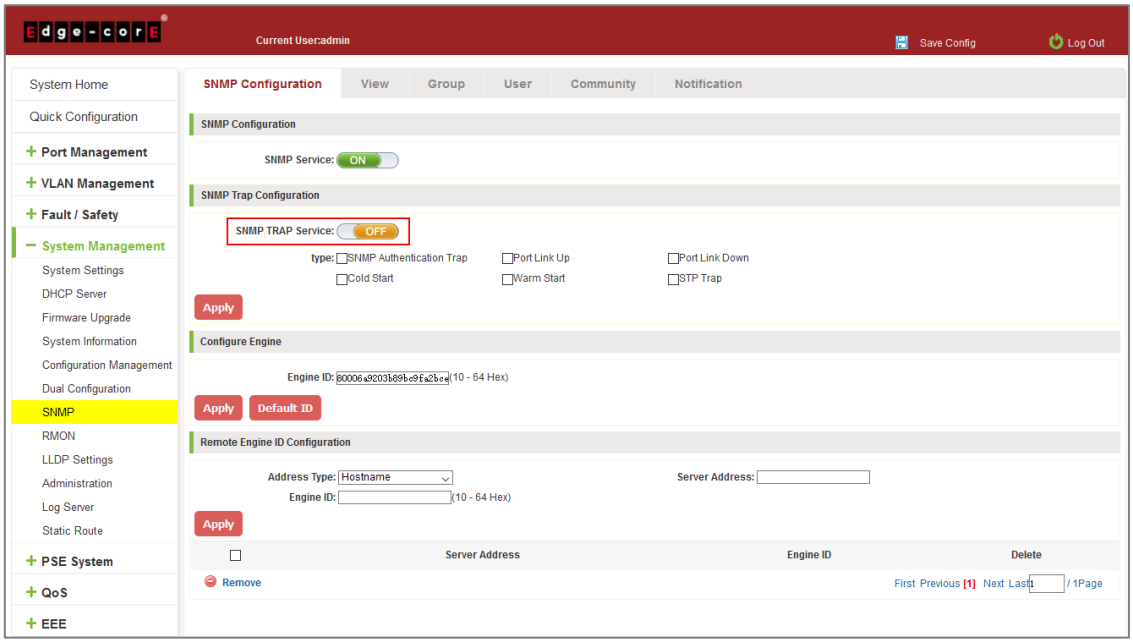


Figure 7-30: Disable TRAP Function

7.7.6 Configure the SNMP Engine ID

After open SNMP, select the Engine ID, enter a valid ID or click the “Default ID” button.

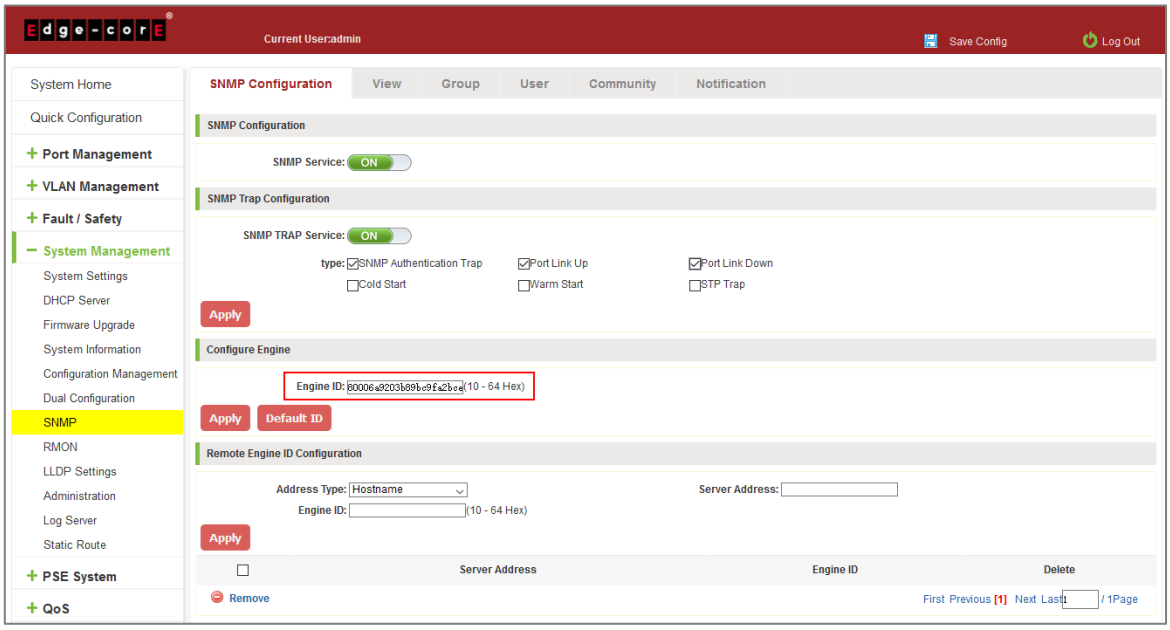


Figure 7-31: Engine ID Configuration

To configure the Engine ID, follow these steps:

Step 1: Select the "ON" option.

Step 2: Enter a valid ID number. Specify an engine ID by entering 10 to 64 hexadecimal characters. Alternatively, click the “Default ID” button to restore and use the default ID.

Step 3: Click the "Apply" button to complete the configuration.

7.7.7 Configure the Remote Engine ID

After open SNMP, select the Remote Engine ID configuration.

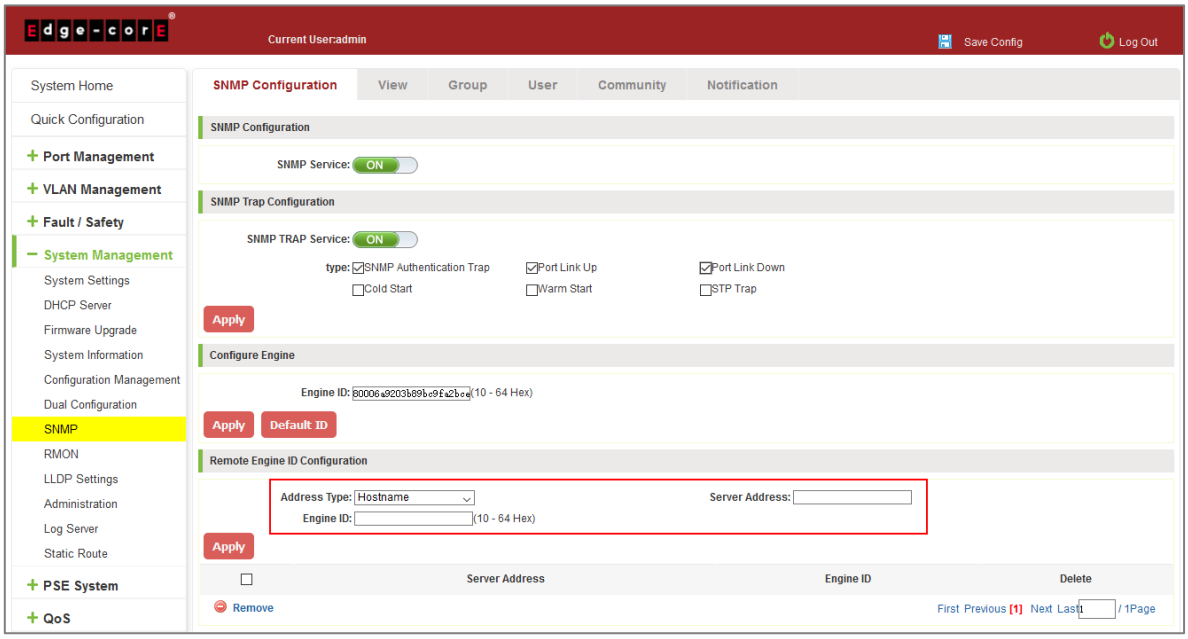


Figure 7-32: Remote Engine ID Configuration

To configure the Remote Engine ID, follow these steps:

Step 1: Enter the IPv4, IPv6, or hostname of the remote SNMP engine.

Step 2: Specify the remote engine ID by entering 10 to 64 hexadecimal characters.

Step 3: Click the "Apply" button to complete the configuration.

7.7.8 Configure SNMP Views

Click "System Management" "SNMP" “View,” to configure SNMP views.

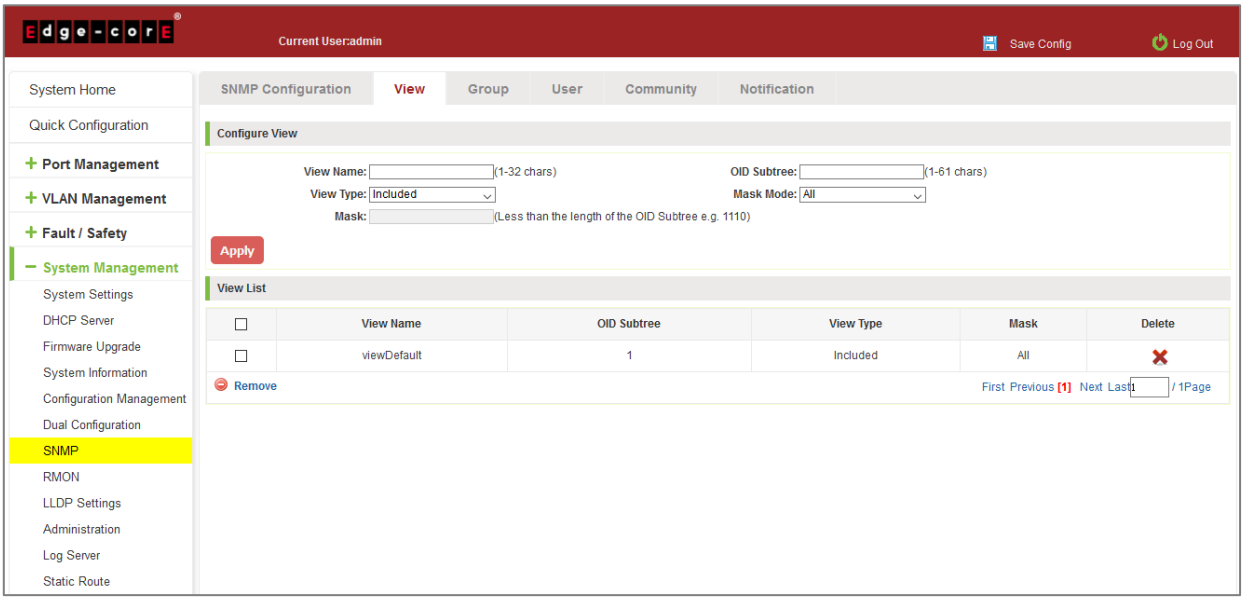


Figure 7-33: Remote Engine ID Configuration

To configure an SNMP view, follow these steps:

Step 1: Enter a name of up to 32 characters for the view.

Step 2: Specify the MIB OID subtree and mask mode.

Step 3: Specify the view type; included or excluded.

Step 4: Click the "Apply" button to complete the configuration.

7.7.9 Configure SNMP Groups

Click "System Management" "SNMP" “Group,” to configure SNMP user groups.

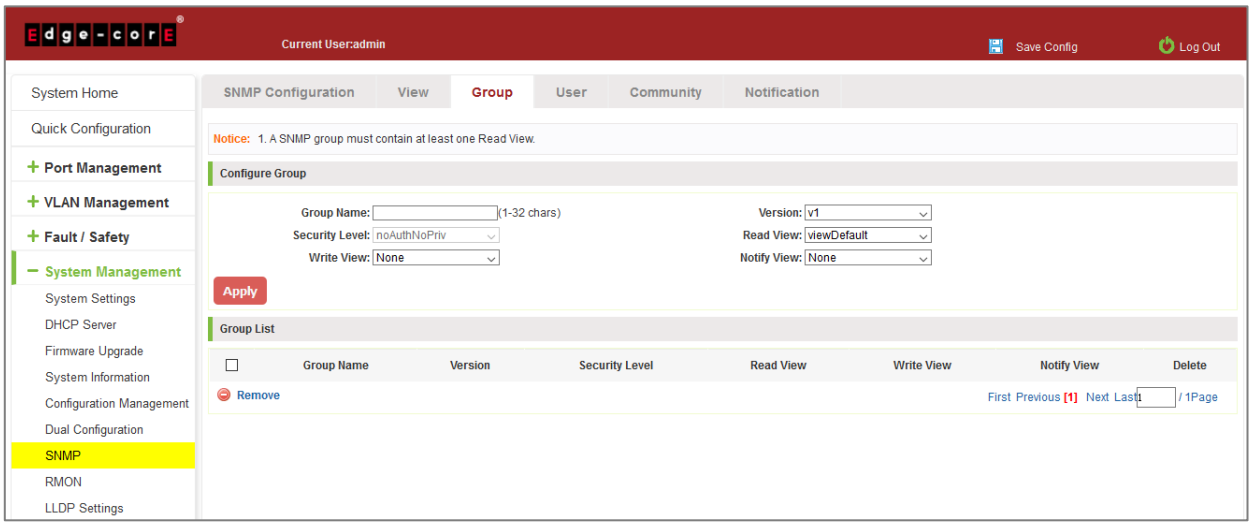


Figure 7-34: SNMP Group Configuration

To configure an SNMP user group, follow these steps:

Step 1: Enter a name of up to 32 characters for the group.

Step 2: Specify the SNMP version for the group.

Step 3: Specify the security level for SNMPv3 users.

Step 4: Select read, write, and notify views for the group.

Step 5: Click the "Apply" button to complete the configuration.

7.7.10 Configure SNMP Users

Click "System Management" "SNMP" “User,” to configure SNMP users.

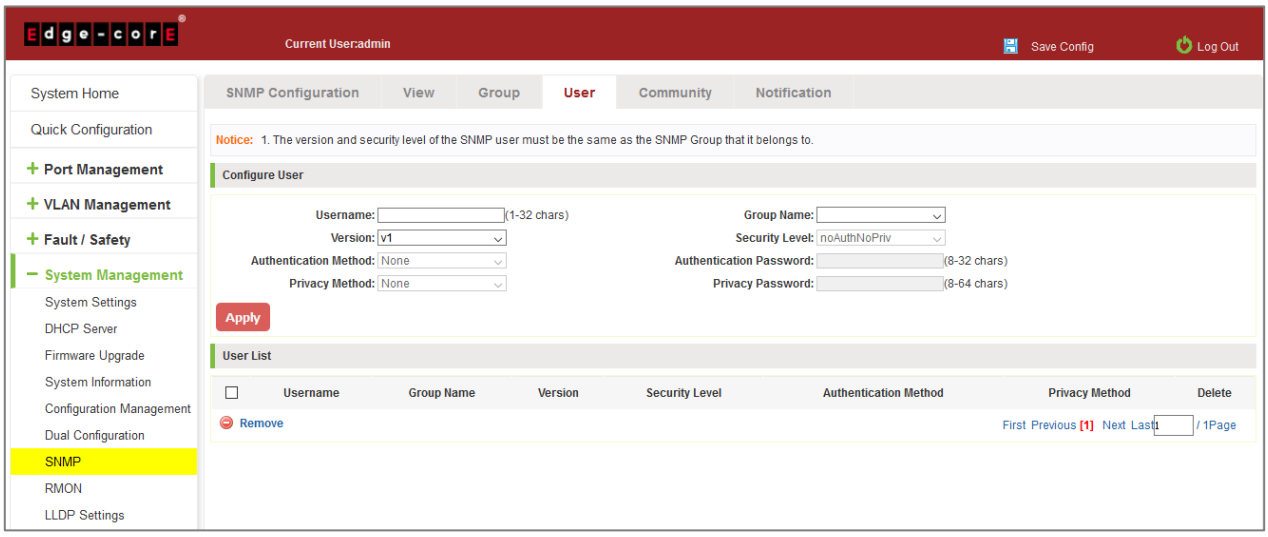


Figure 7-35: SNMP User Configuration

To configure an SNMP user, follow these steps:

Step 1: Enter a name of up to 32 characters for the user.

Step 2: Assign the user to a configured SNMP group.

Step 3: Specify the SNMP version for the user.

Step 4: Specify the security level for SNMPv3 users and configure the authentication and privacy settings.

Step 5: Click the "Apply" button to complete the configuration.

7.7.11 Configure SNMP Communities

Click "System Management" "SNMP" “Community,” to configure SNMP community settings.

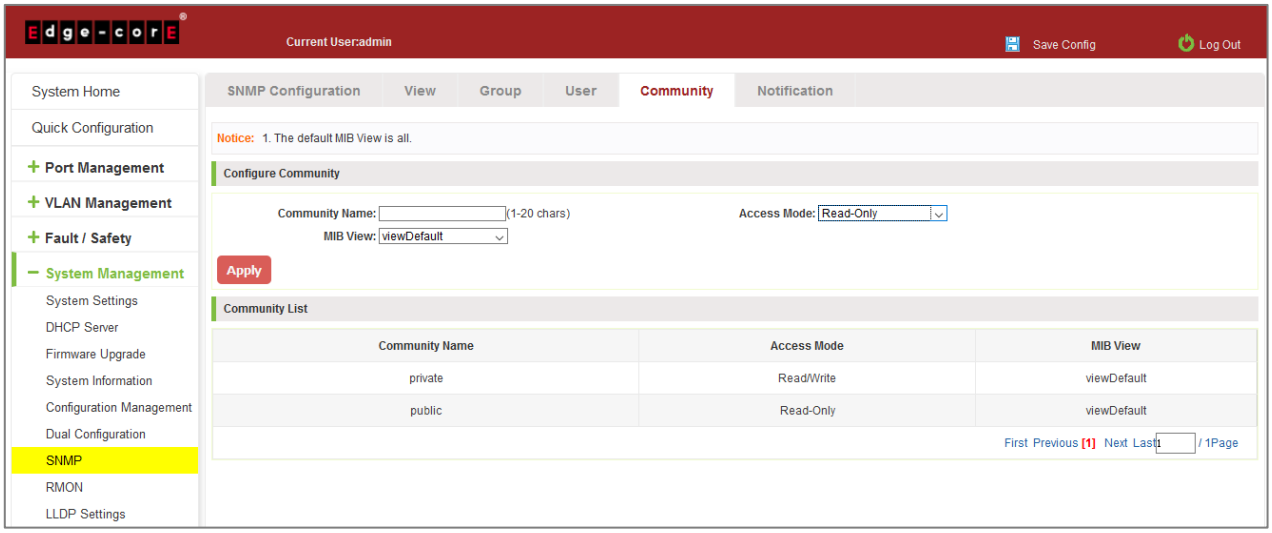


Figure 7-36: SNMP Community Configuration

To configure an SNMP community name, follow these steps:

Step 1: Enter a name of up to 20 characters for the community.

Step 2: Specify the community access mode: Read-Only or Read/write.

Step 3: Specify the MIB View for the community.

Step 4: Click the "Apply" button to complete the configuration.

7.7.12 Configure SNMP Notifications

Click "System Management" "SNMP" “Notification,” to configure SNMP notification settings.

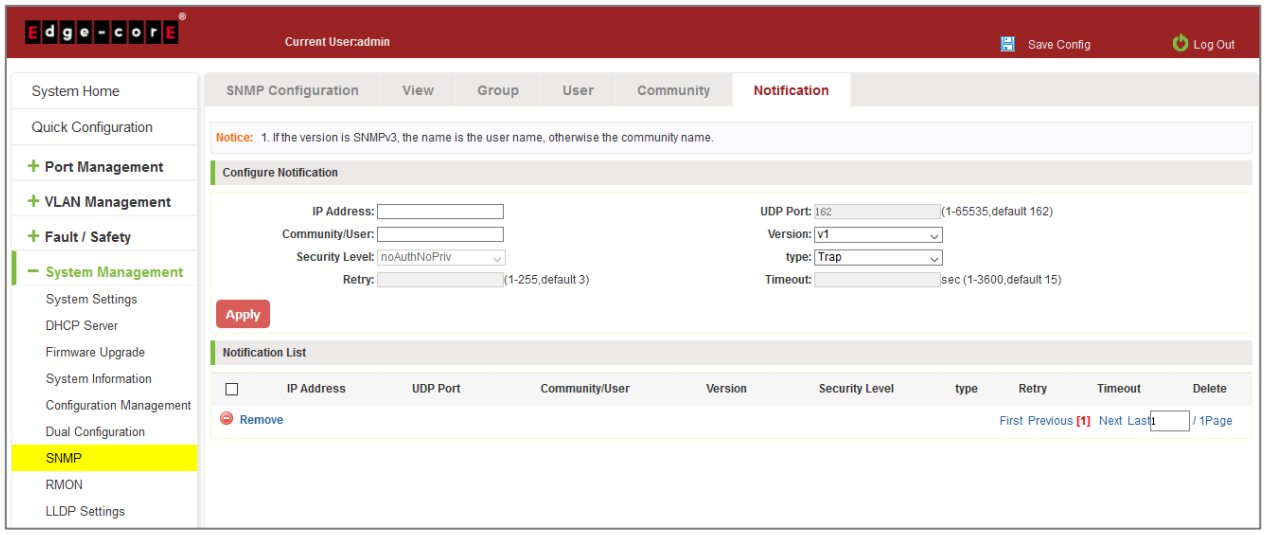


Figure 7-37: SNMP Notification Configuration

To configure SNMP notifications, follow these steps:

Step 1: Enter the IP address of the notification receiver.

Step 2: Specify the community for SNMPv1/v2c users, or the user name for SNMPv3 users.

Step 3: Specify the SNMP version, the notification type, and security level as appropriate.

Step 4: Click the "Apply" button to complete the configuration.

7.8 RMON

7.8.1 View ROMN configure information

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

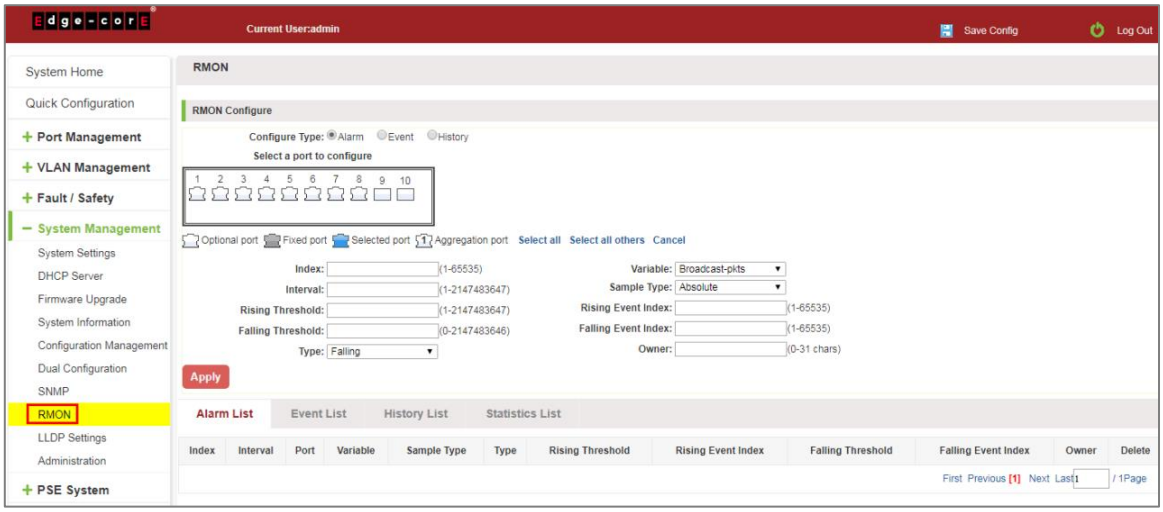


Figure 7-38: View RMON Configure Information

7.8.2 Configure ROMN type

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

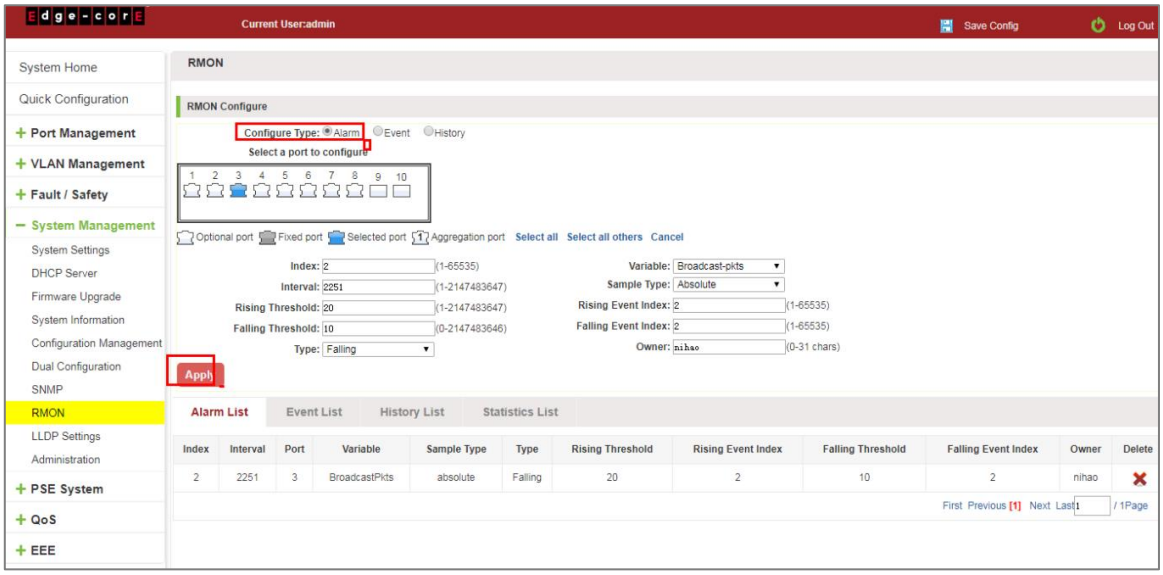


Figure 7-39: Configure ROMN Type

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

7.8.3 Change RMON type

On the RMON 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".

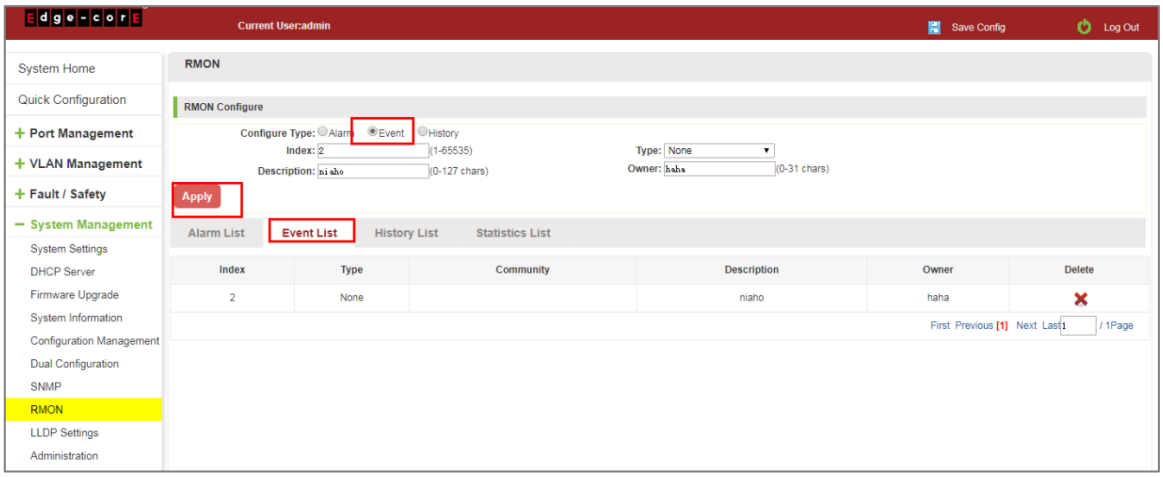


Figure 7-40: Change ROMN Type is Event

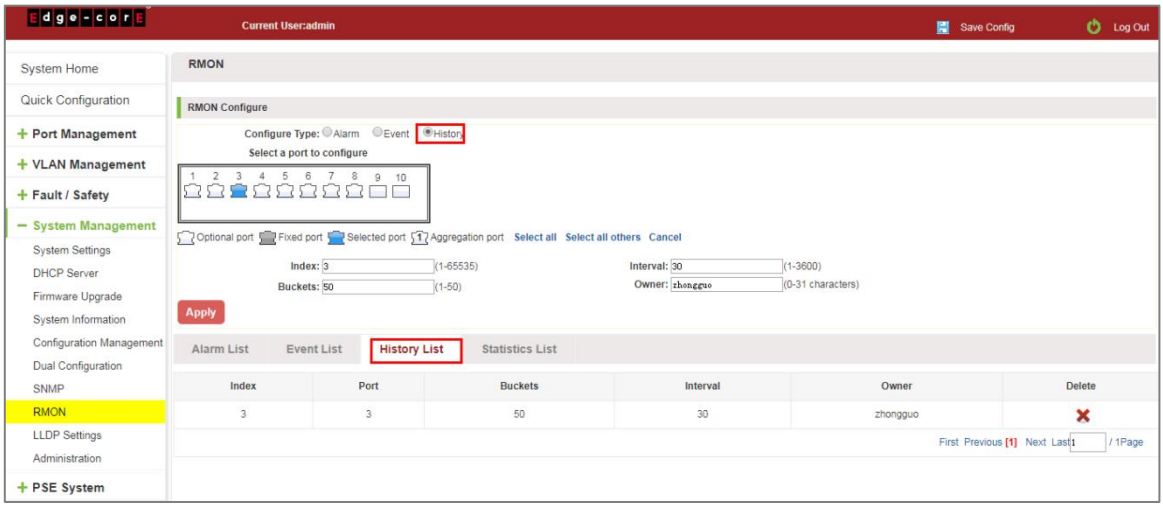


Figure 7-41: Change ROMN Type is History

When the parameters configure is ok, click the Statistics List. We can choose the port to view the information.

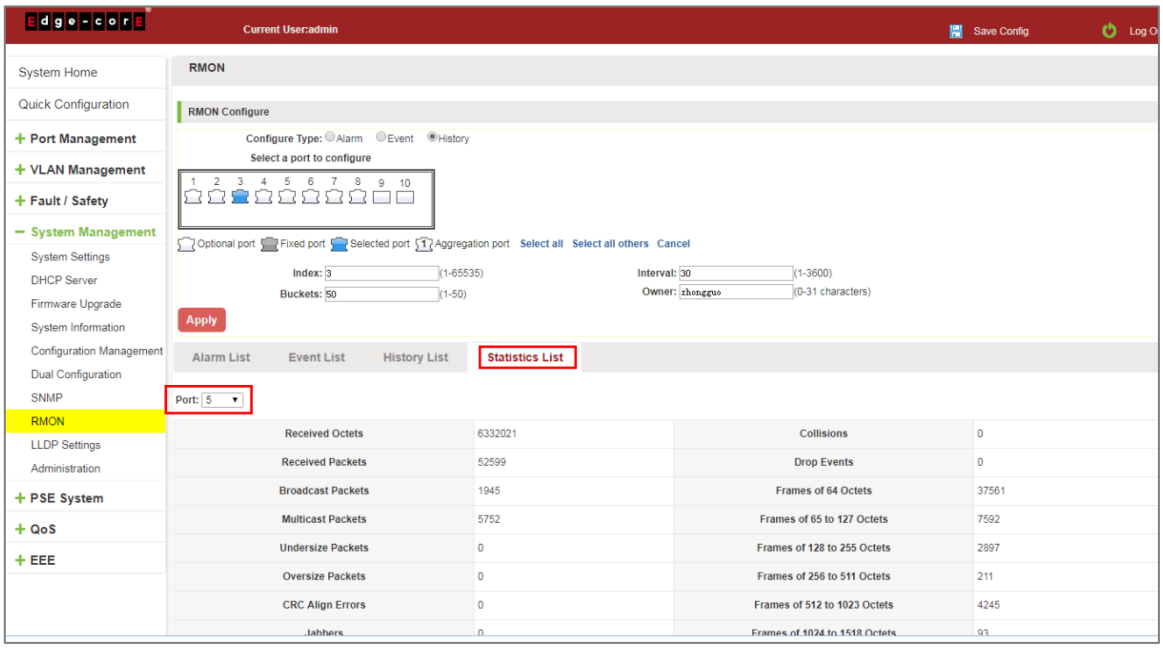


Figure 7-42: View the Port Configure Information

7.8.4 Delete the configured rule

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

Figure 7-43: Delete the Alarm List Rule

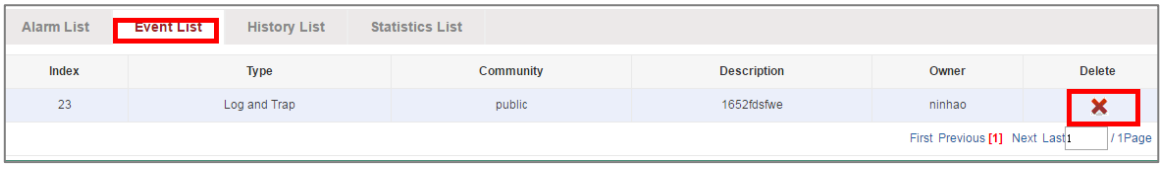


Figure 7-44: Delete the Event List Rule

Figure 7-45: Delete the History List Rule

7.9 LLDP SETTINGS

7.9.1 LLDP Settings Information

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

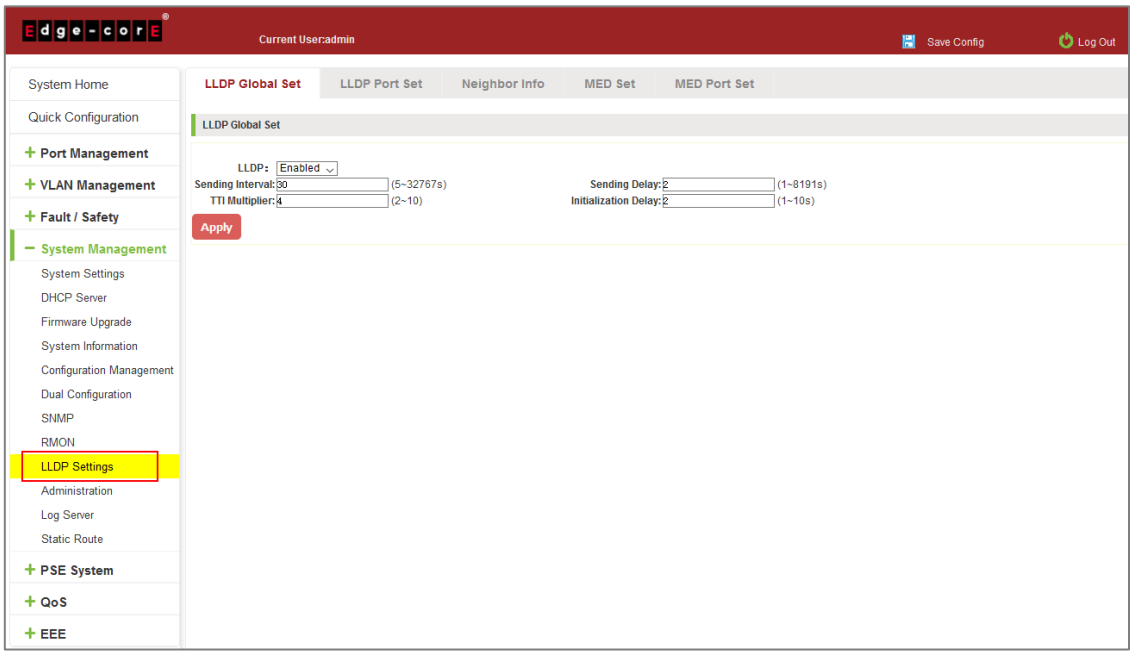


Figure 7-46: View LLDP Settings Information

7.9.2 LLDP Port Settings

Configuration of the LLDP port properties:

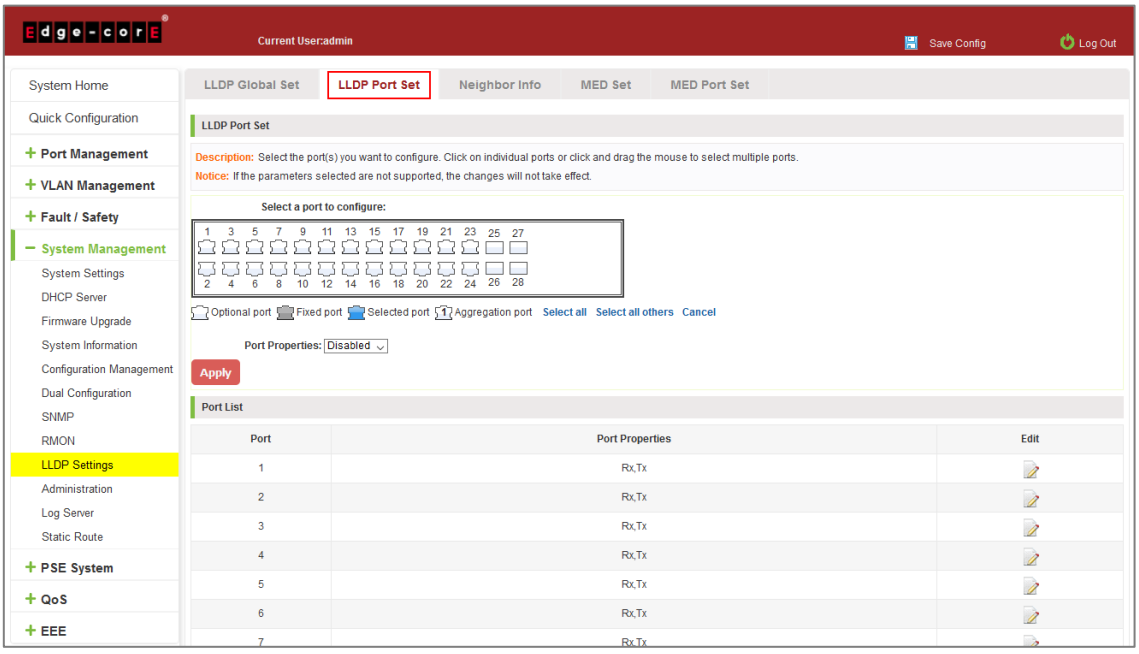


Figure 7-47: LLDP Port Properties

7.9.3 Neighbor info

When the LLDP function is enabled, the neighbor information is recorded when a neighbor device is found. Notice: you should be configuration the Peer device on CLI, on the port of the peer device that is connected to the DUT: LLDP tlv-select sys-name sys-cap.

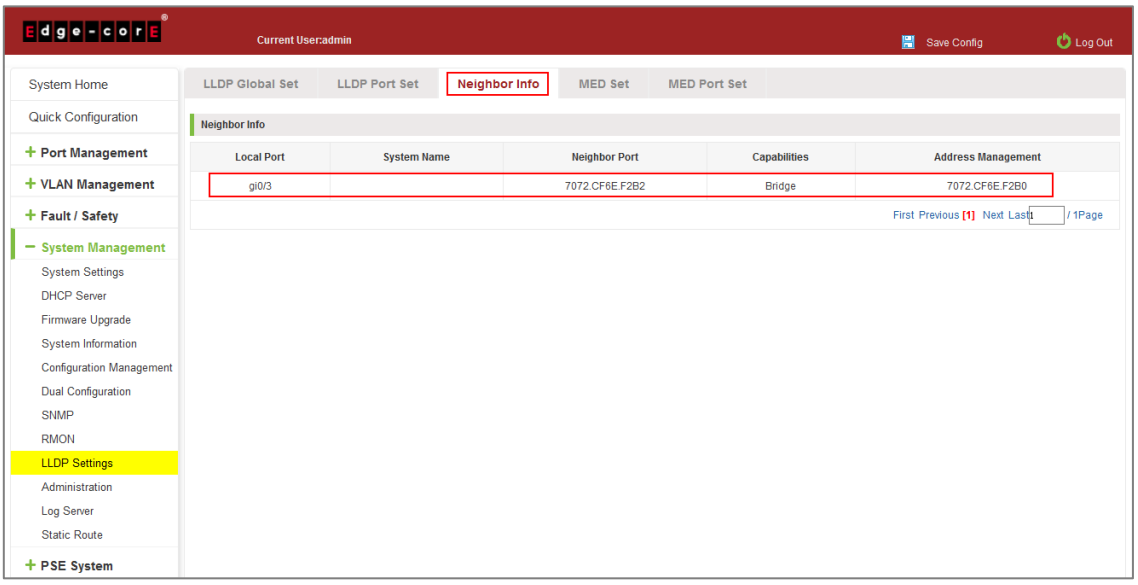


Figure 7-48: LLDP Neighbor Info

7.9.4 MED Set

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches.

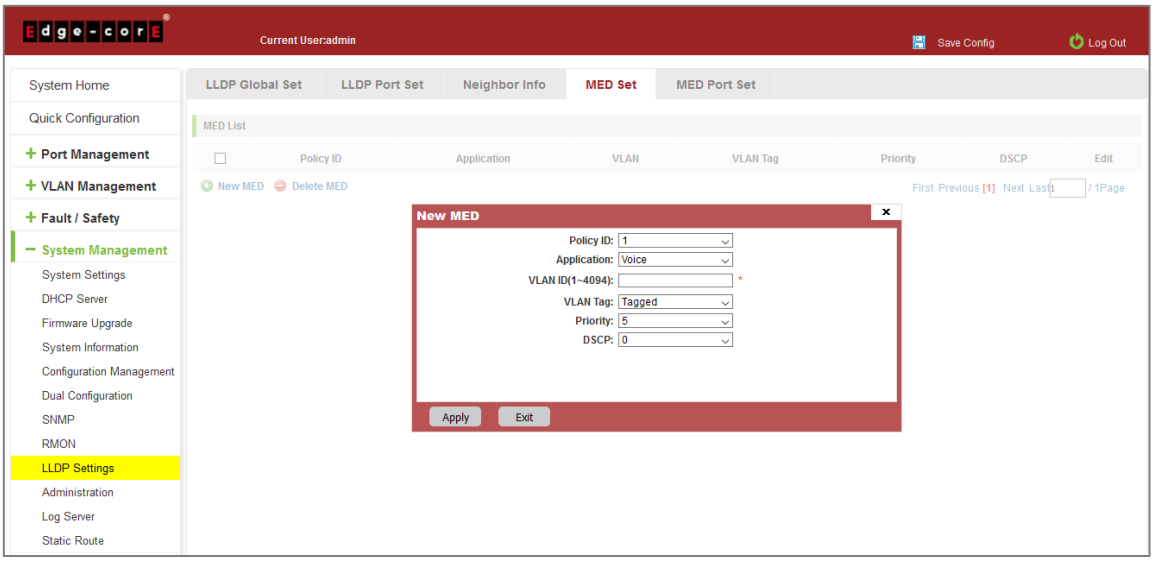


Figure 7-49: LLDP MED Set

To configure a new MED, follow these steps:

Step 1: Click "New MED."

Step 2: Enter the details of the MED.

Step 3: Click the "Apply" button to complete the configuration.

7.9.5 MED Port Set

Configuration of the LLDP-MED Port Properties:

.

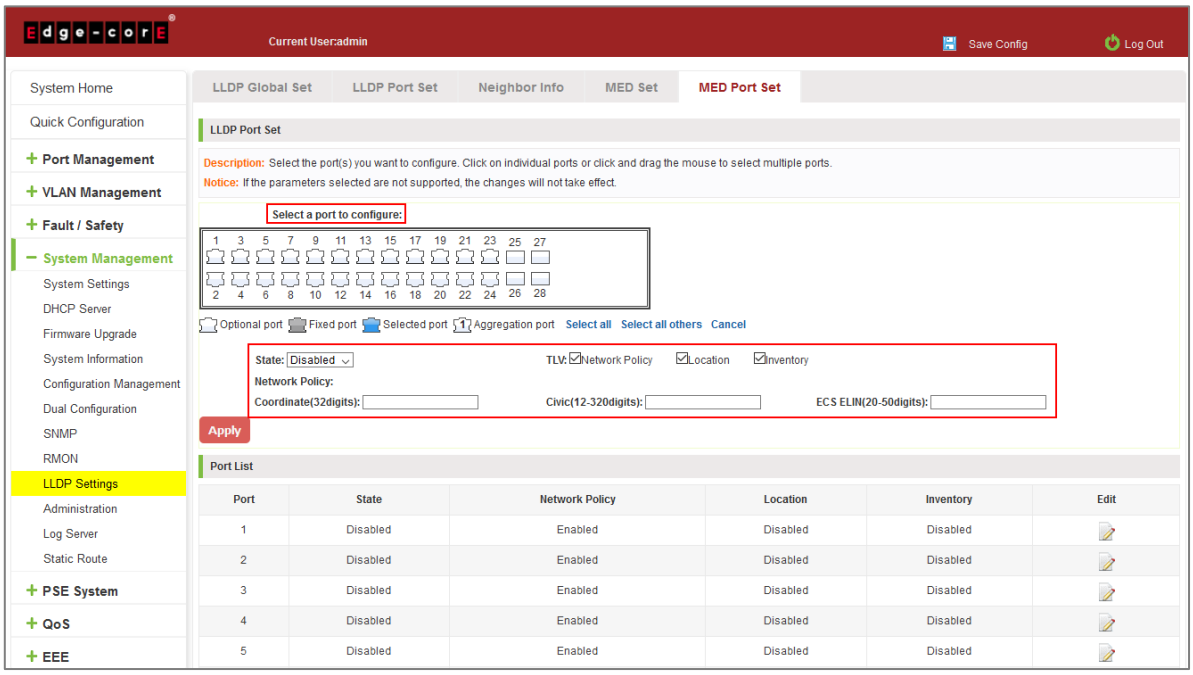


Figure 7-50: LLDP MED Port Set

To configure MED port settings, follow these steps:

Step 1: Select a port to configure it.

Step 2: Set the status to “Enabled.”

Step 3: Enable TLVs and configure the details where required.

Step 4: Click the "Apply" button to complete the configuration.

7.10 ADMINISTRATION

7.10.1 Telnet Information

Click on the "System Management" "Administration, "Administration Settings" can view the Telnet settings information. This feature is turned off by default.

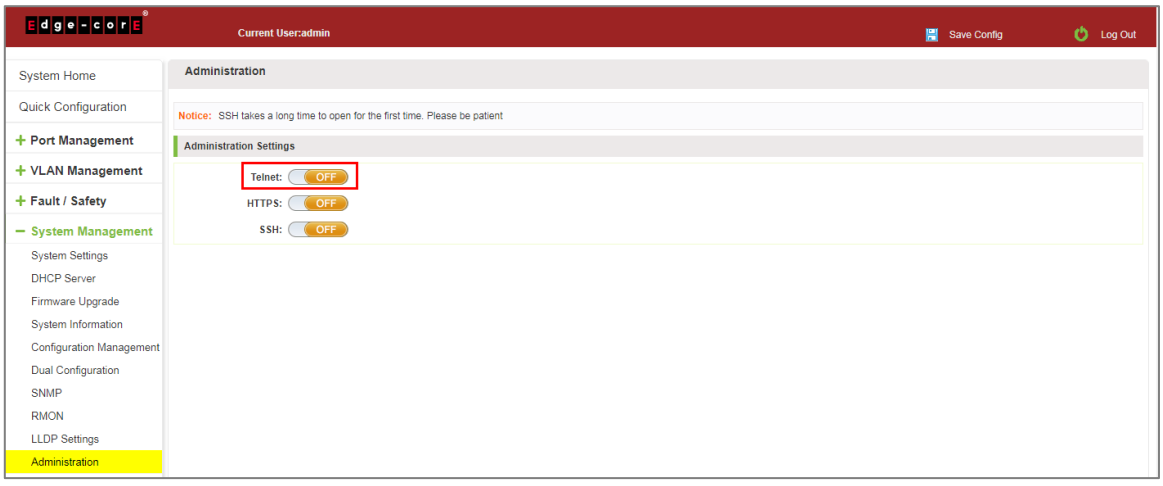


Figure 7-51: Telnet Information

7.10.2 Enable Telnet

Click on the button " 

" and apply. To enable Telnet, and the user can connect to the device via telnet.

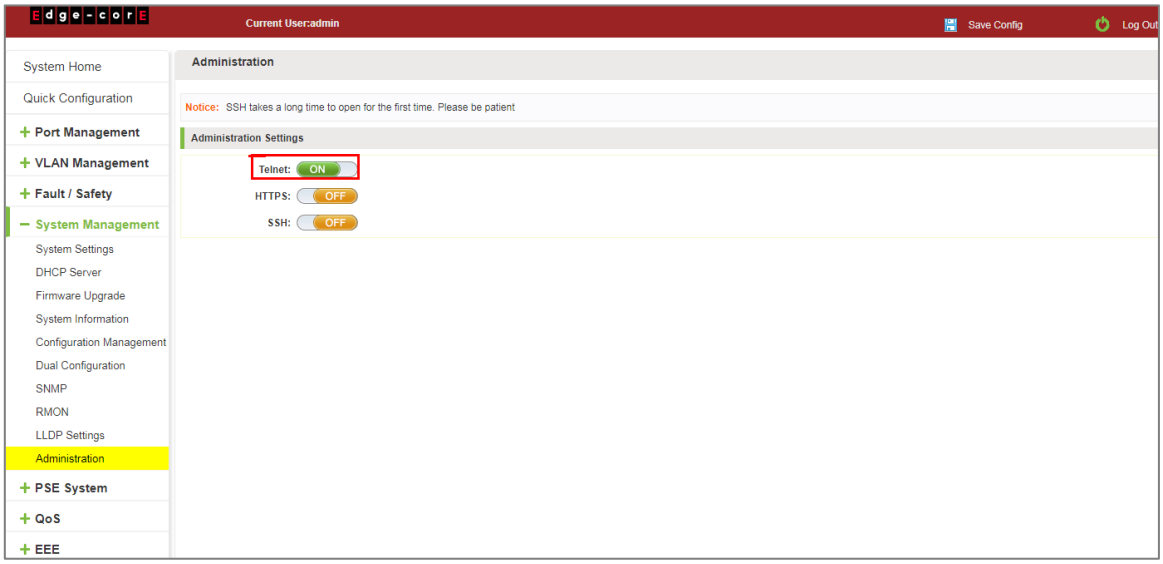


Figure 7-52: Enable Telnet

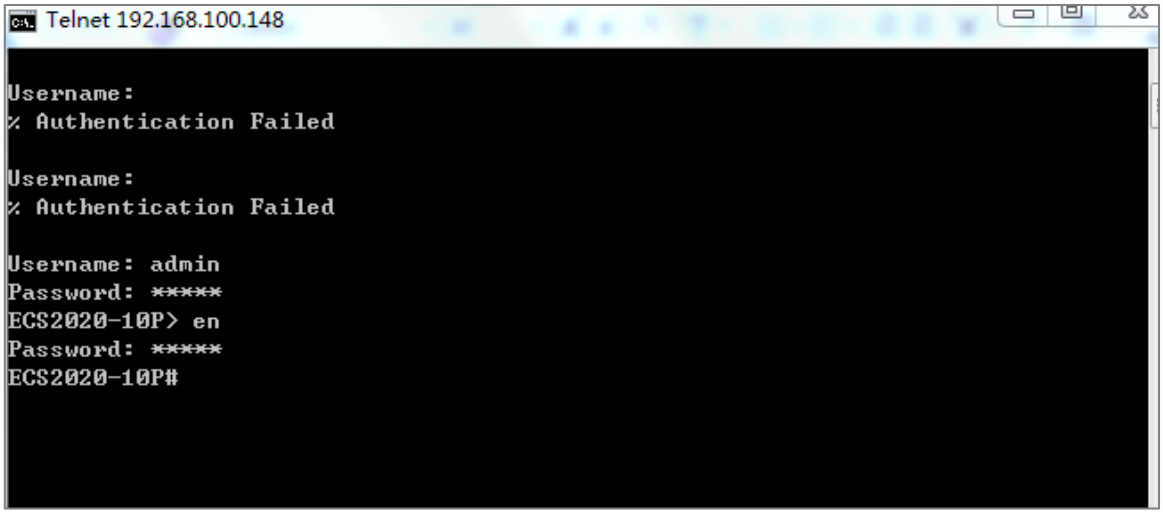


Figure 7-53: Telnet Login

7.10.3 HTTPS

Enable HTTPS function, users can manage the device through HTTPS.

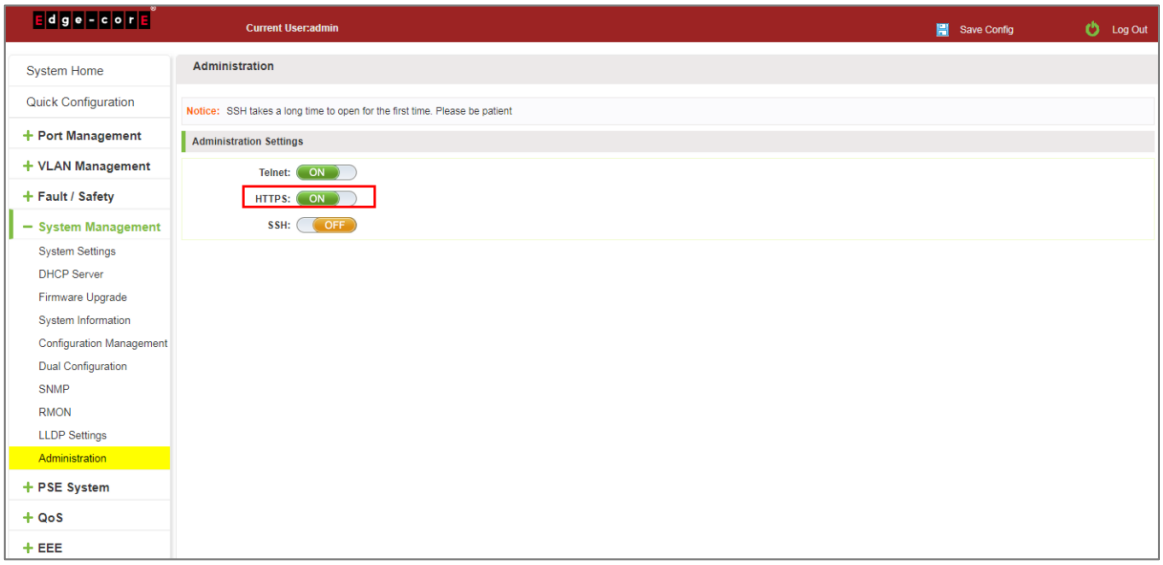


Figure 7-54: Enable HTTPS

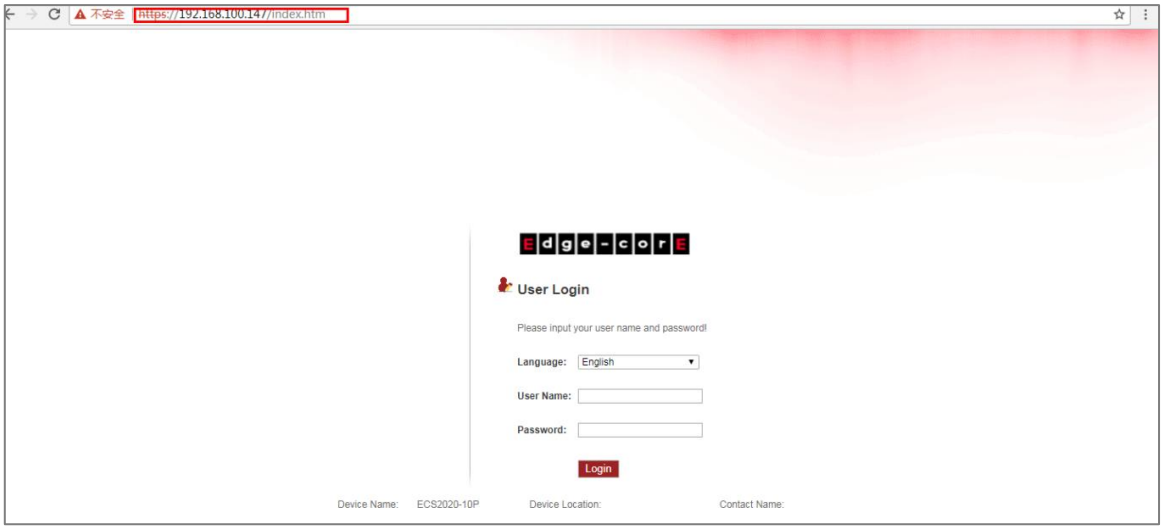


Figure 7-55: HTTPS login

7.10.4 SSH

Enable SSH function and SSH takes a long time to open for the first time.

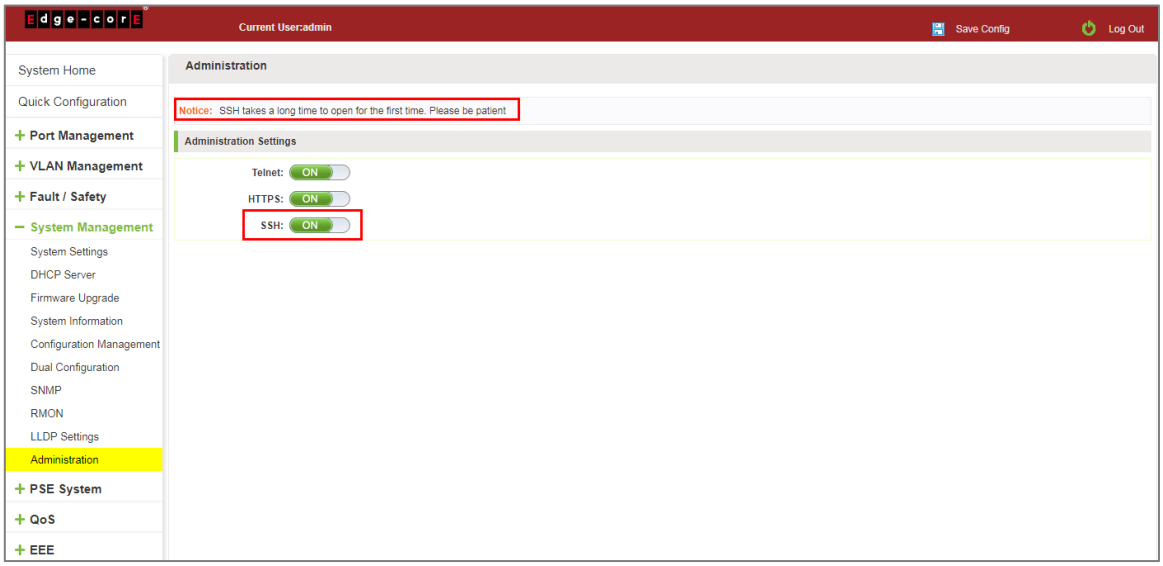
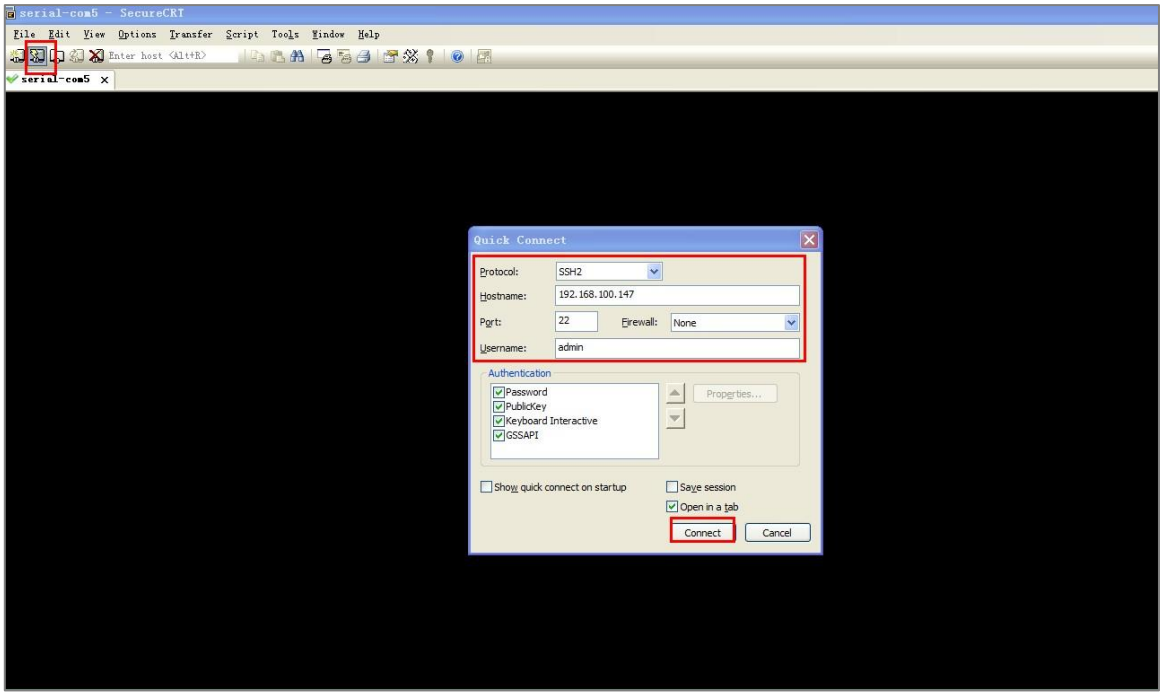


Figure 7-56: Enable SSH



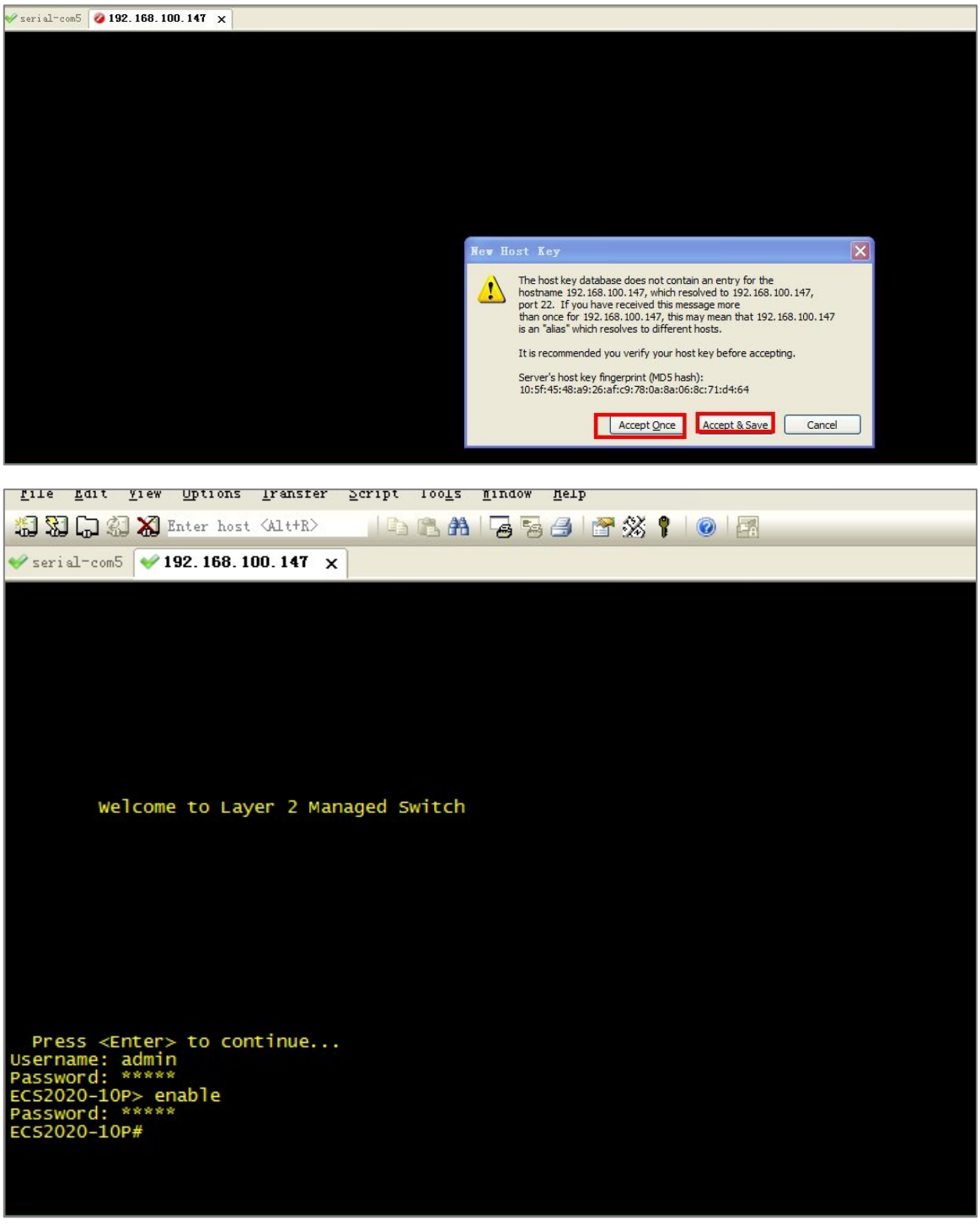


Figure 7-57: Use SSH2 Login

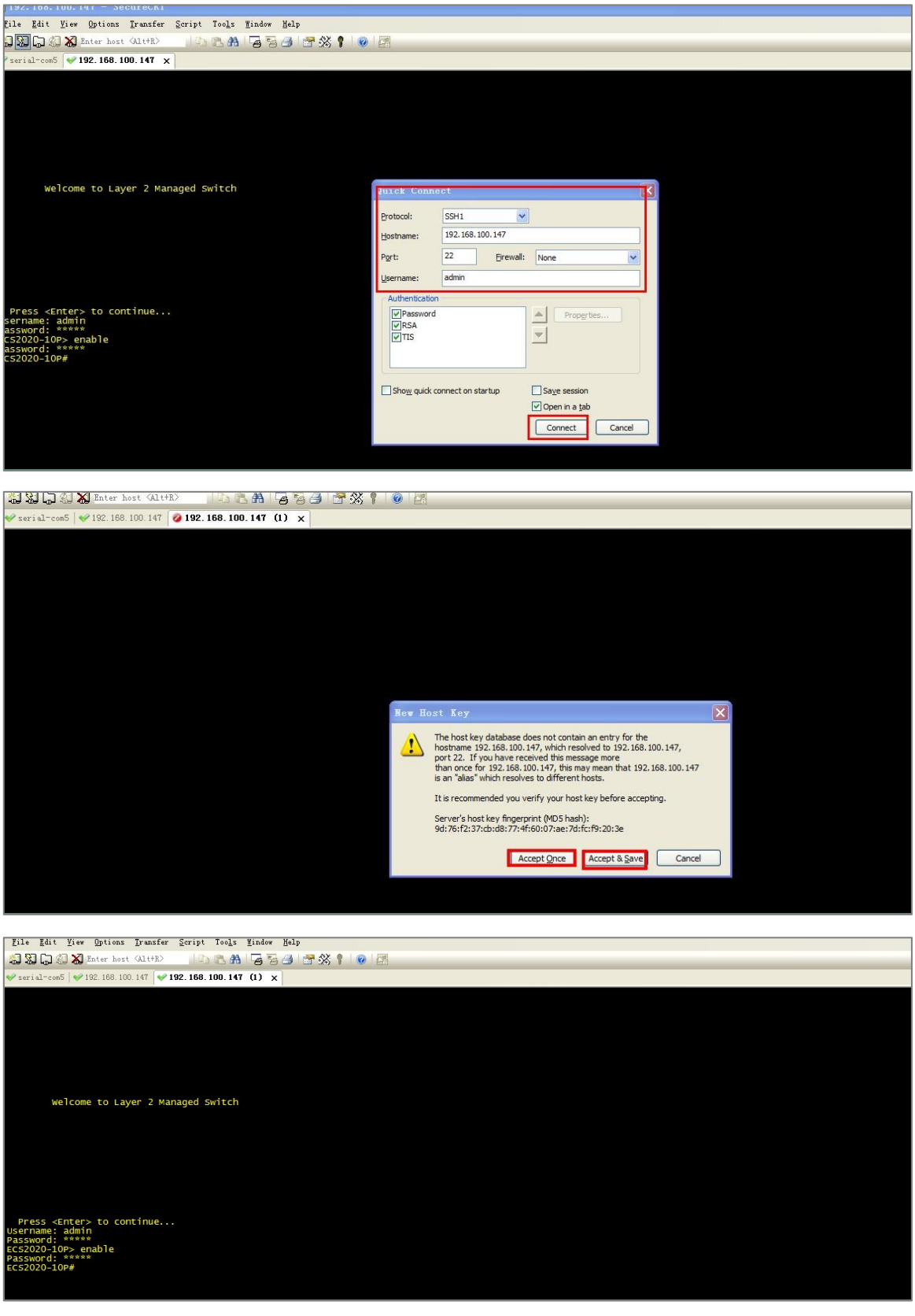


Figure 7-58: Use SSH1 Login

7.11 LOG SERVER

Click on "System Management" "Log Server" to configure a Syslog server.

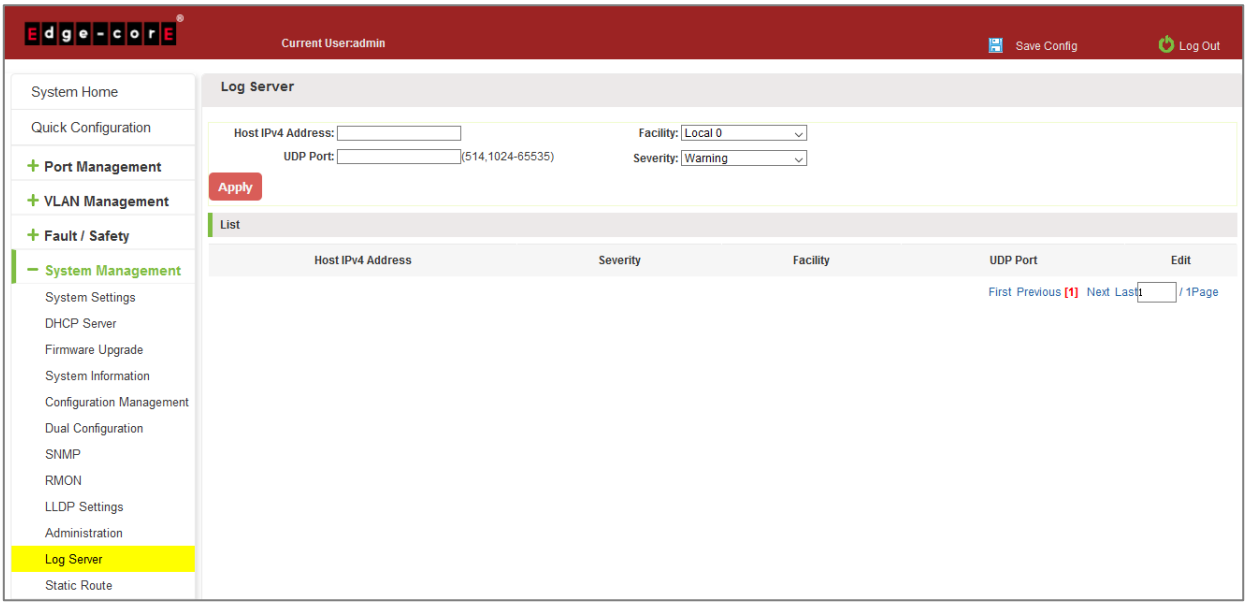


Figure 7-59: Log Server

To configure Log Server settings, follow these steps:

Step 1: Enter the IPv4 address of the Syslog server.

Step 2: Specify the UDP port number for the Syslog server.

Step 3: Specify the Facility and severity level of log messages to send to the server.

Step 4: Click the "Apply" button to complete the configuration.

7.12 STATIC ROUTE

Click on "System Management" "Static Route" to configure static routes.

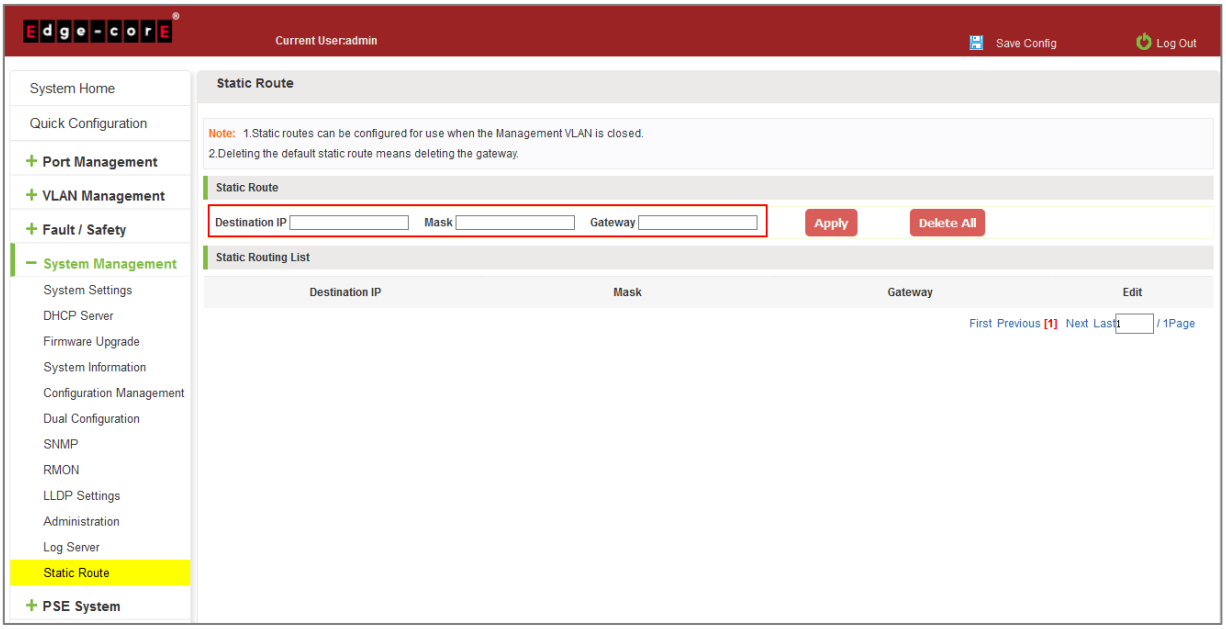


Figure 7-60: Static Route

To add a static route, follow these steps:

Step 1: Specify the destination IP address and mask for the subnet route.

Step 2: Specify the gateway to reach the destination subnet.

Step 3: Click the "Apply" button to complete the configuration.

8 PSE SYSTEM MANAGEMENT

8.1 PSE SYSTEM CONFIGURATION

8.1.1 View the PSE system configuration

Click on the navigation bar "PSE System Management" "PSE System Configuration" to view the PSE system information of the current switch, click "Refresh" button, display refresh configuration information:

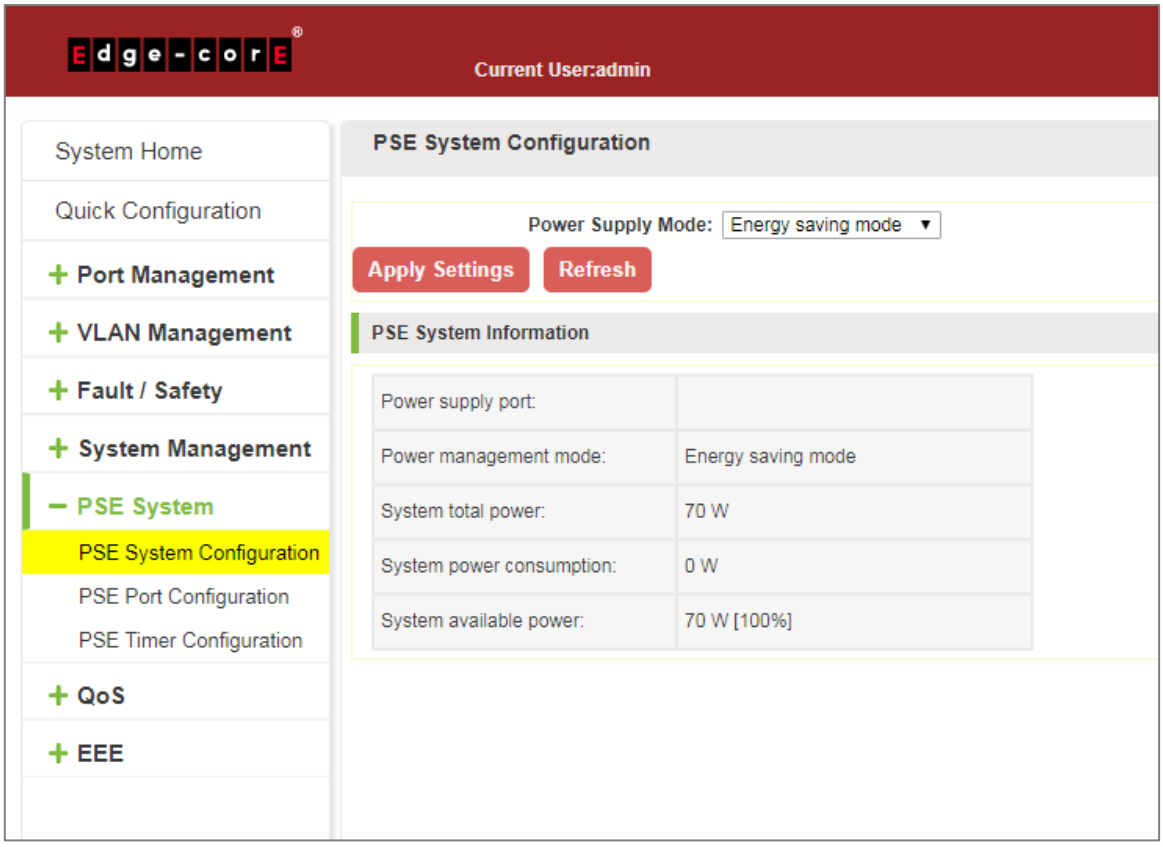


Figure 8-1: View the PSE System Information

8.1.2 Configure power supply mode

8.1.2.1 Configure power supply mode to automatic

Click on the navigation bar "PSE System Management" "PSE System Configuration" to configure power supply mode to automatic mode

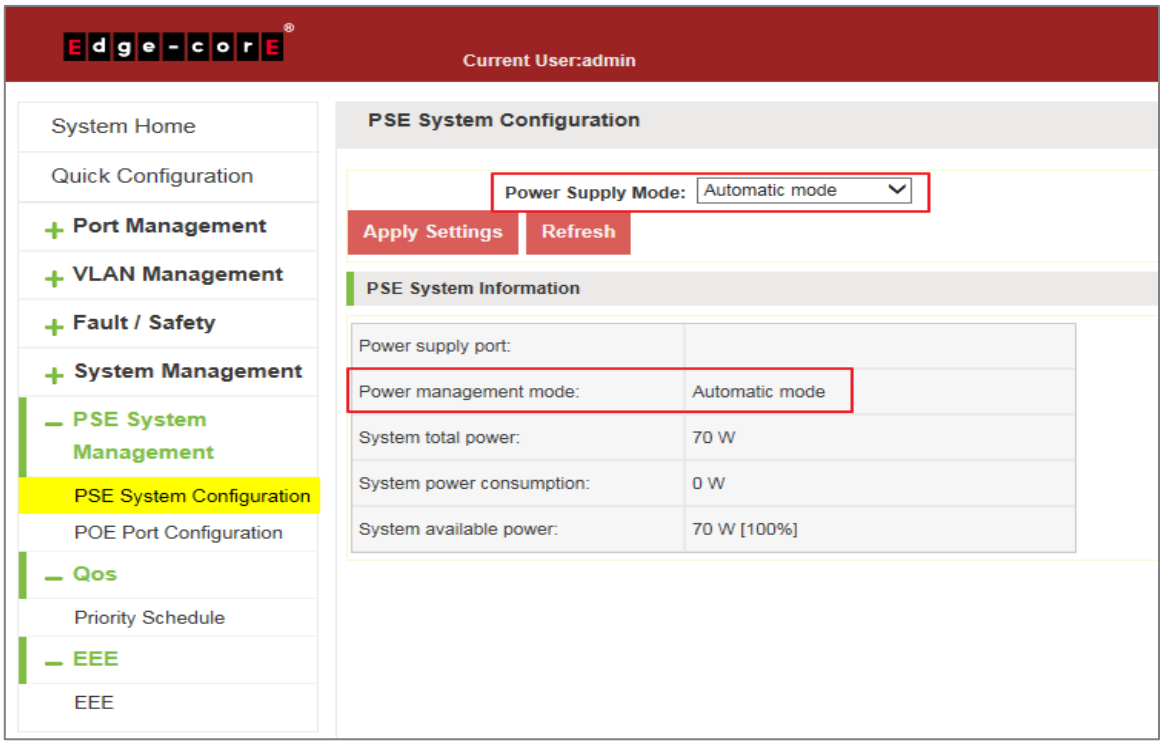


Figure 8-2: Automatic Mode

To configure the switch PSE System steps as follows:

Step 1: In the power supply mode, choose automatic mode;

Step 2: Click on "Apply Settings" button to complete the configuration

8.1.2.2 Configure power supply mode to static

Click on the navigation bar "PSE System Management" "PSE System Configuration" to configure power supply mode to static mode

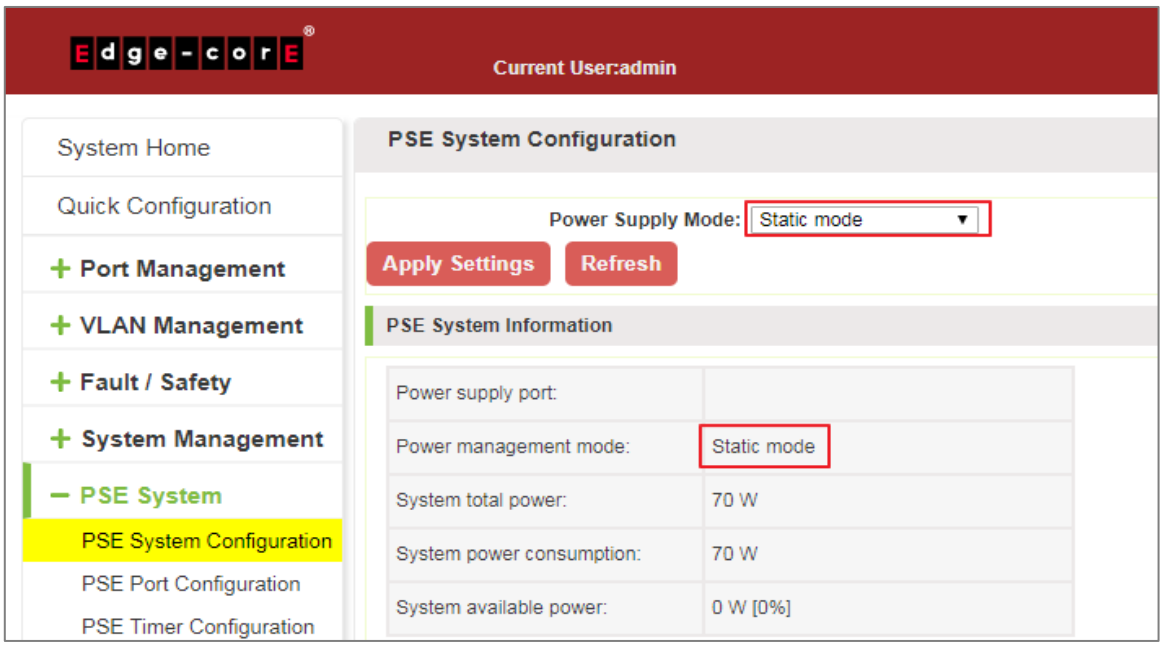


Figure 8-3: Static Mode

To configure the switch PSE System steps as follows:

Step 1: In the power supply mode, choose static mode;

Step 2: Click on "Apply Settings" button to complete the configuration.

8.1.2.3 Configure power supply mode to energy saving

Click on the navigation bar "PSE System Management" "PSE System Configuration" to configure power supply mode to energy saving mode

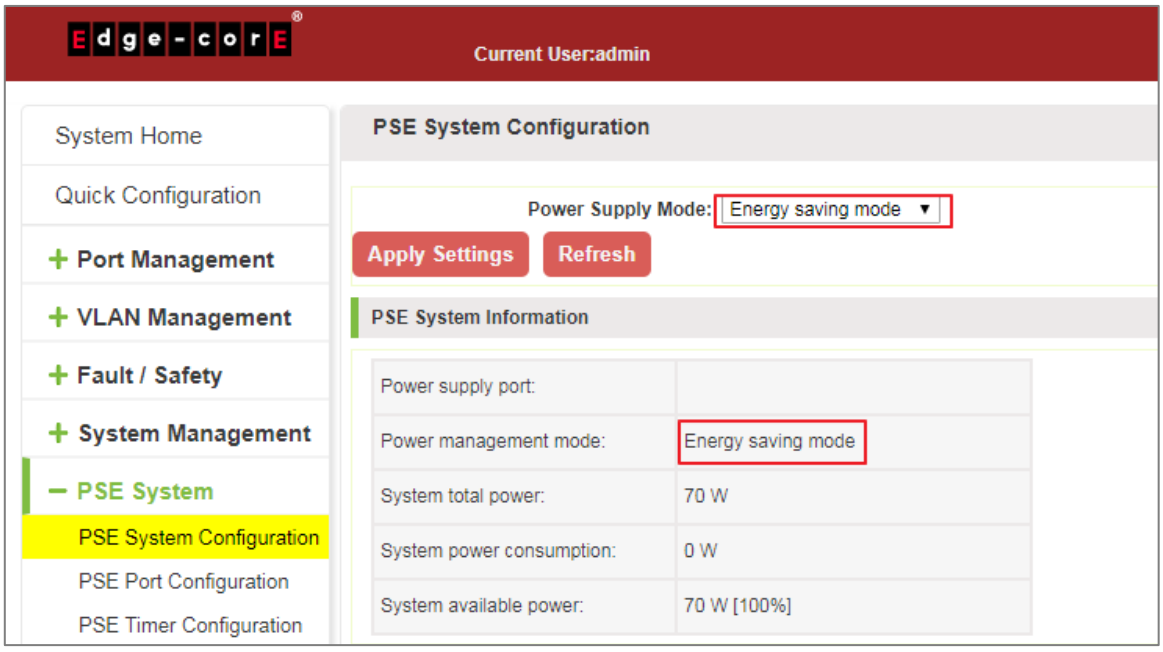


Figure 8-4: Energy Saving Mode

To configure the switch PSE System steps as follows:

Step 1: In the power supply mode, choose energy saving mode;

Step 2: Click on "Apply Settings" button to complete the configuration

8.2 POE PORT CONFIGURATION

Click the "PSE System Management" "POE Port Configuration" to configure the POE port on the switch:

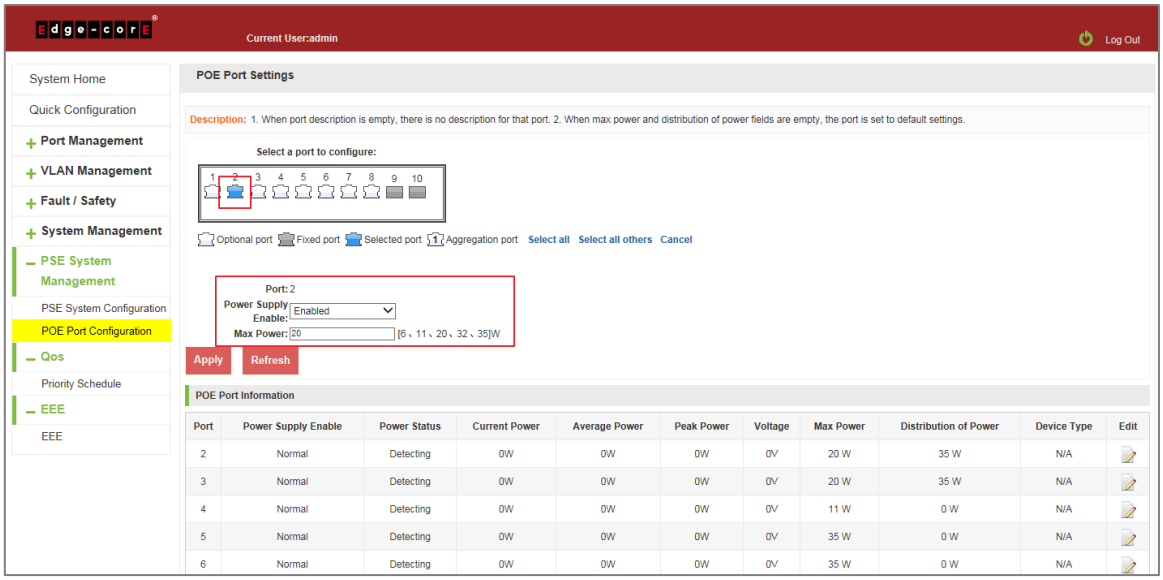


Figure 8-5: PoE Port Configuration

PoE Port configuration steps are as follows:

Step 1: Select a port to configure;

Step 2: In the power supply enable, choose enable.

Step 3: In the max power text, choose 20.

8.2.1 Editing POE port

Click on the " " icon can be configured selected port:

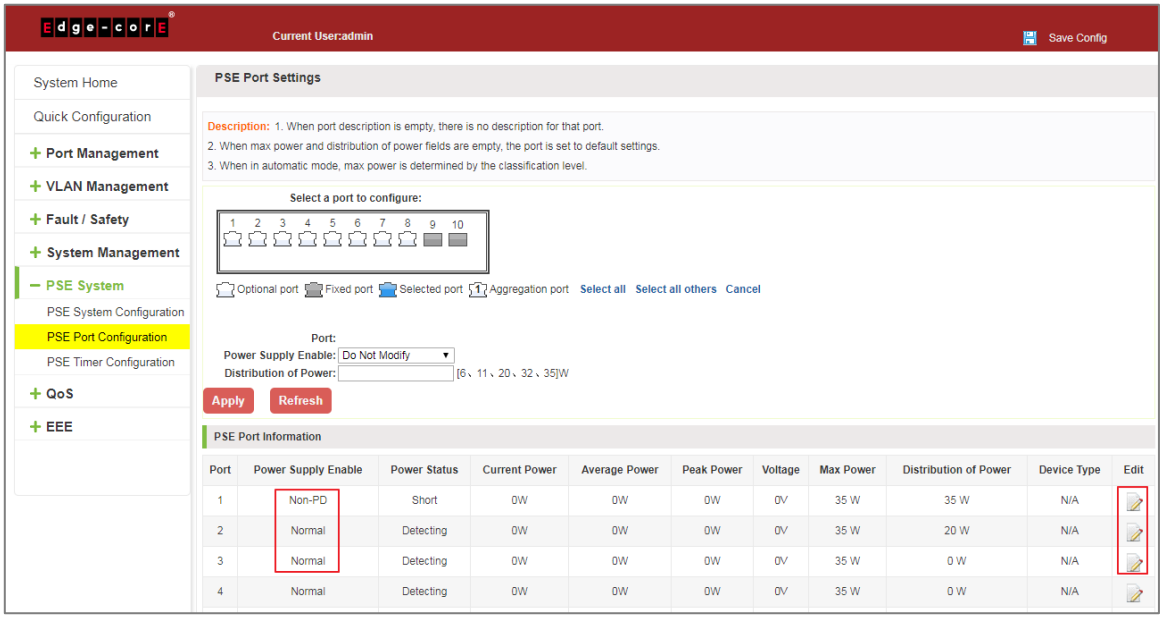


Figure 8-6: Edit the PoE Port

Modify POE port settings follow these steps:

Step 1: Select port and Click" "icon.

Step 2: In the power supply enable, choose disable.

8.3 POE TIMER CONFIGURATION

Click the "PSE System Management" "PoE Timer Configuration" to configure the PoE port absolute and periodic time on the switch:

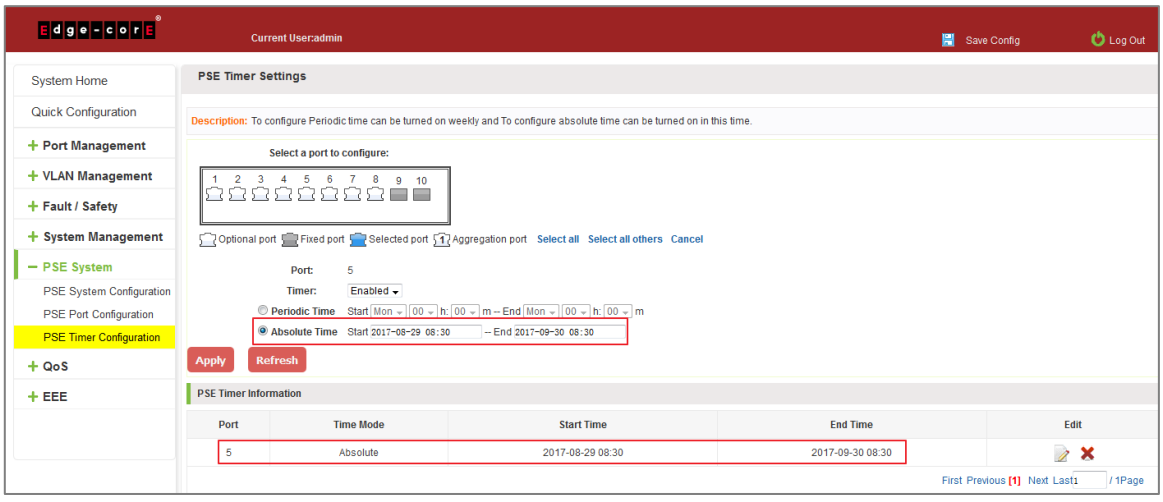


Figure 8-7: PoE Timer Absolute Time Configuration

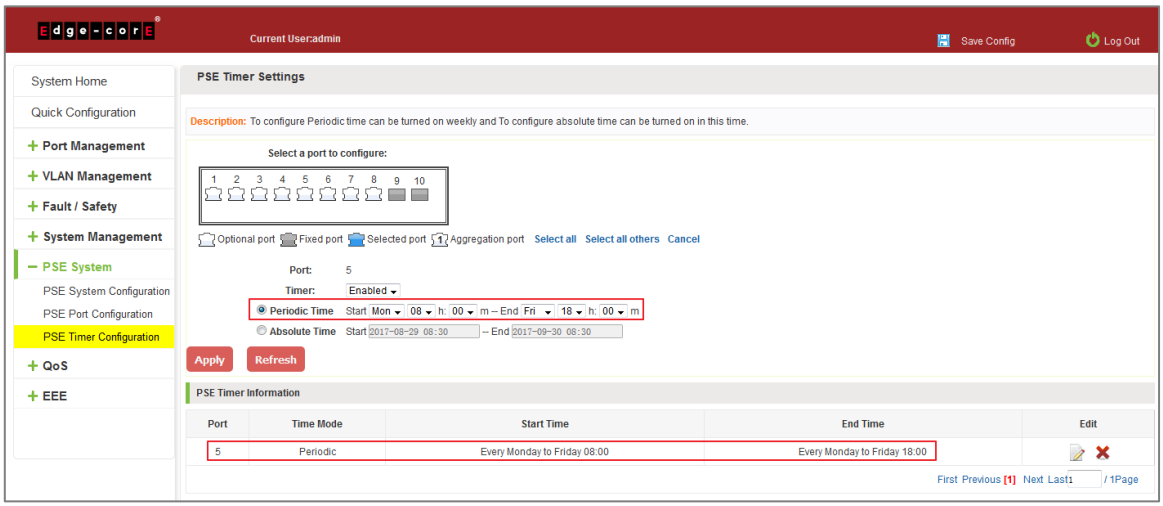


Figure 8-8: PoE Timer Periodic Time Configuration

PoE Port configuration steps are as follows:

Step 1: Select a port to configure;

Step 2: In the timer, choose enable

Step 3: Configure absolute time start time 2017-8-29 08:30 end time 2017-9-30 08:30

Step 4: Configure periodic time start time Every Monday to Friday 08:00 end time Every Monday to Friday 18:00.

9 QOS

9.1 PRIORITY SCHEDULE

9.1.1 View the priority schedule

Click on the "QoS" "Priority Schedule", can view the device priority schedule:

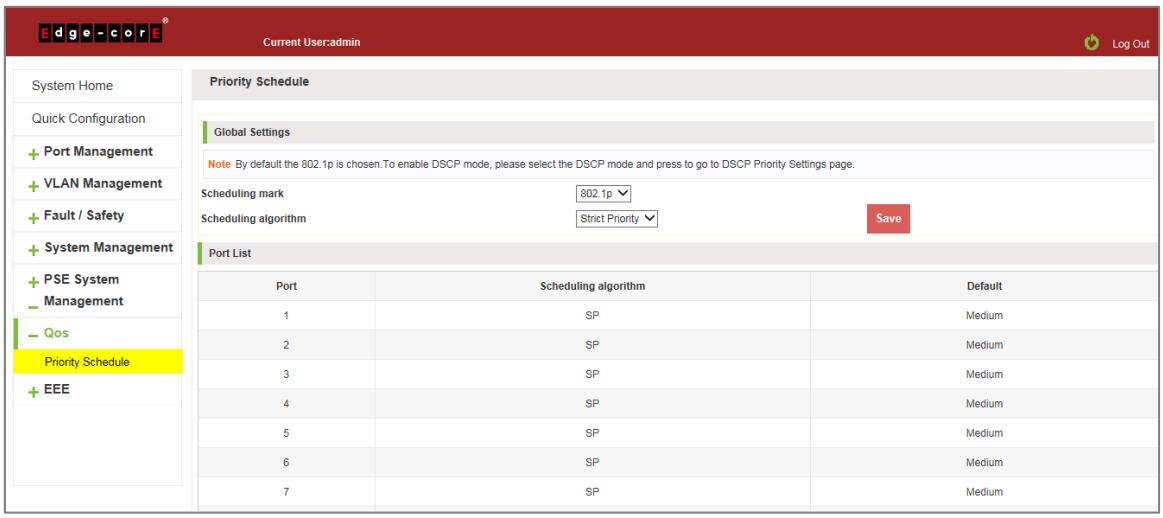


Figure 9-1: Priority Schedule

9.1.2 The configuration global settings of SP

9.1.2.1 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.

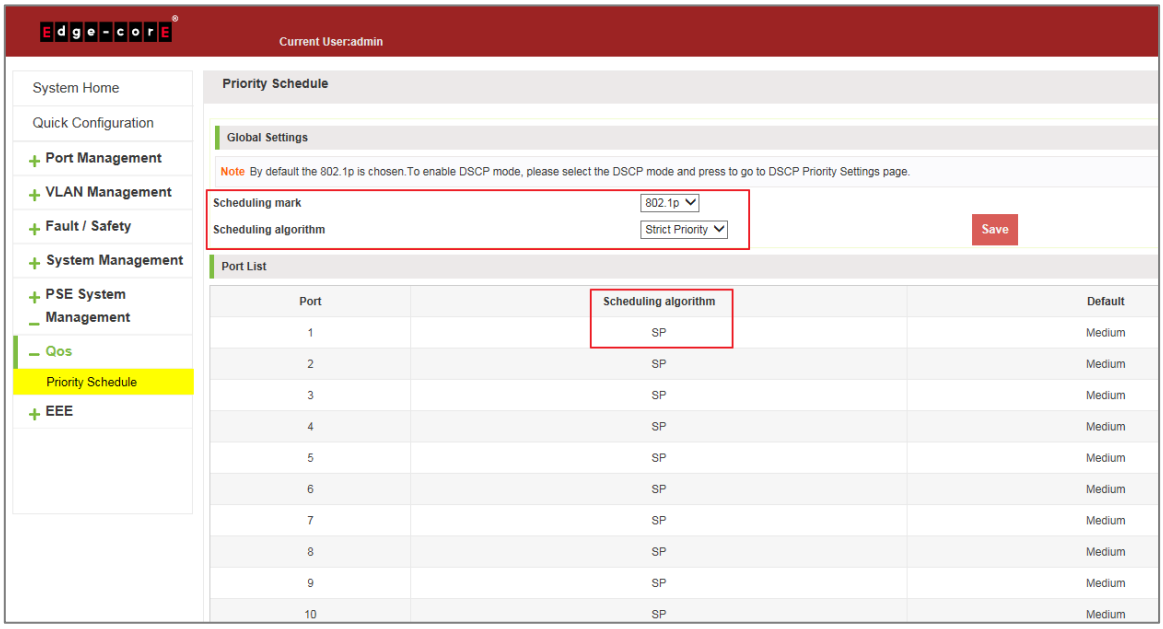


Figure 9-2: Global Settings in 802.1p and SP

9.1.2.2 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.

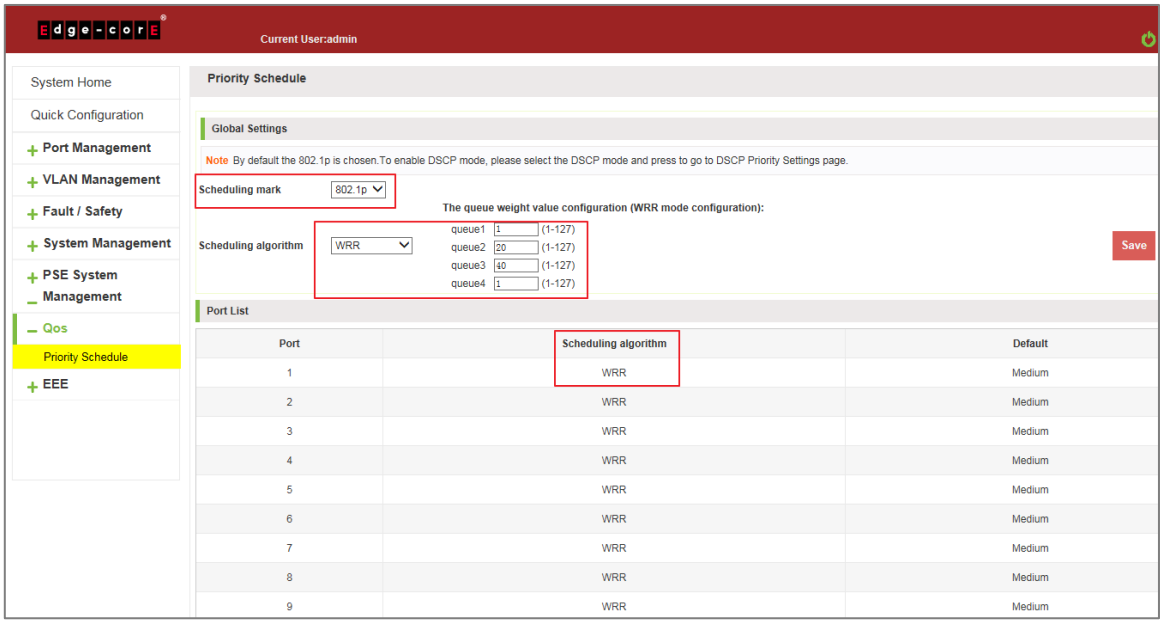


Figure 9-3: Global Settings in 802.1p and WRR

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose 802.1p;

Step 2: In the Scheduling algorithm, choose WRR,

Step 3: In queue1 text box, enter the weight value, such as 1;

Step 4: In queue2 text box, enter the weight value, such as 20;

Step 5: In queue3 text box, enter the weight value, such as 40;

Step 6: In queue4 text box, enter the weight value, such as 1.

9.1.2.3 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.

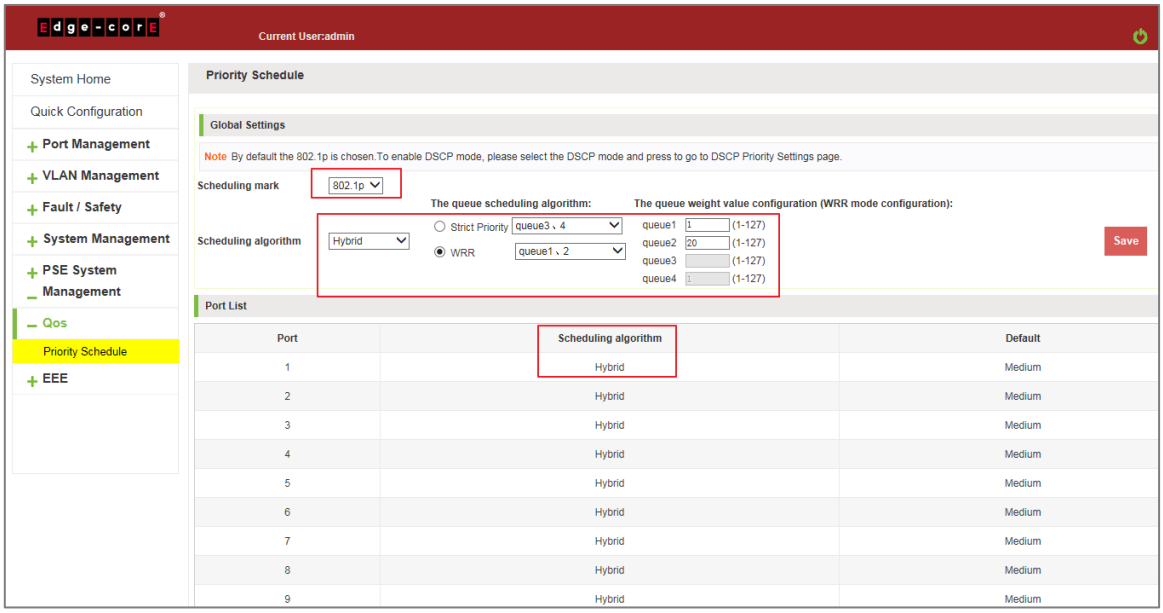


Figure 9-4: Global Settings in 802.1p and Hybrid

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose 802.1p;

Step 2: In the Scheduling algorithm, choose hybrid,

Step 3: In strict priority text box, choose the queue3,4;

Step 4: In WRR text box, choose the queue 1,2;

Step 5: In queue1 text box, enter the weight value, such as 1;

Step 6: In queue2 text box, enter the weight value, such as 20.

9.1.3 The configuration global settings of DSCP

9.1.3.1 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.

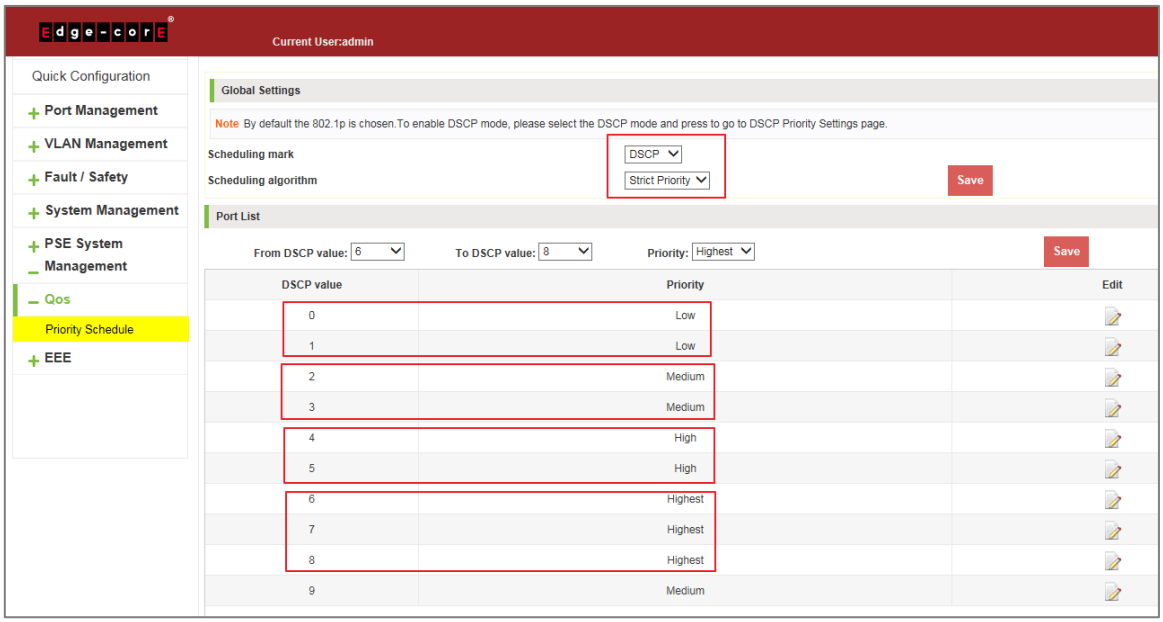


Figure 9-5: Global Settings in DSCP and SP

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose DSCP;

Step 2: In the Scheduling algorithm, choose strict priority,

Step 3: In from DSCP value text box, choose 0 and in to DSCP value text box, choose 1 and in priority text box, choose low;

Step 4: In from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose medium;

Step 5: In from DSCP value text box, choose 4 and in to DSCP value text box, choose 5 and in priority text box, choose high;

Step 6: In from DSCP value text box, choose 6 and in to DSCP value text box, choose 8 and in priority text box, choose highest.

9.1.3.2 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.

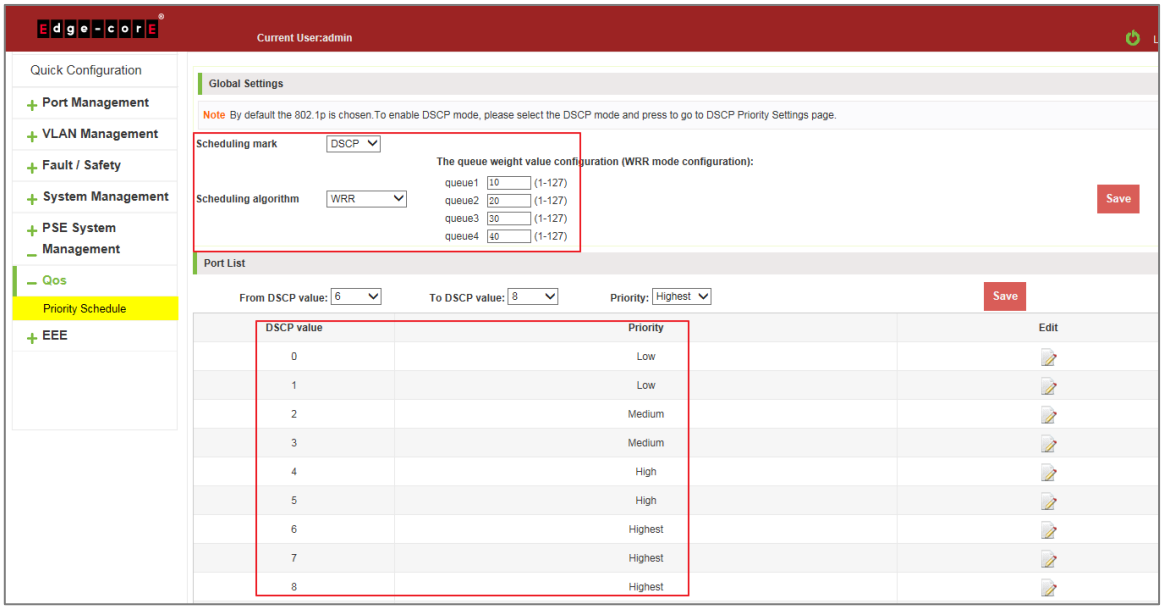


Figure 9-6: Global Settings in DSCP and WRR

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose DSCP;

Step 2: In the Scheduling algorithm, choose WRR,

Step 3: In queue1 text box, enter the weight value, such as 10;

Step 4: In queue2 text box, enter the weight value, such as 20;

Step 5: In queue3 text box, enter the weight value, such as 30;

Step 6: In queue4 text box, enter the weight value, such as 40.

9.1.3.3 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.

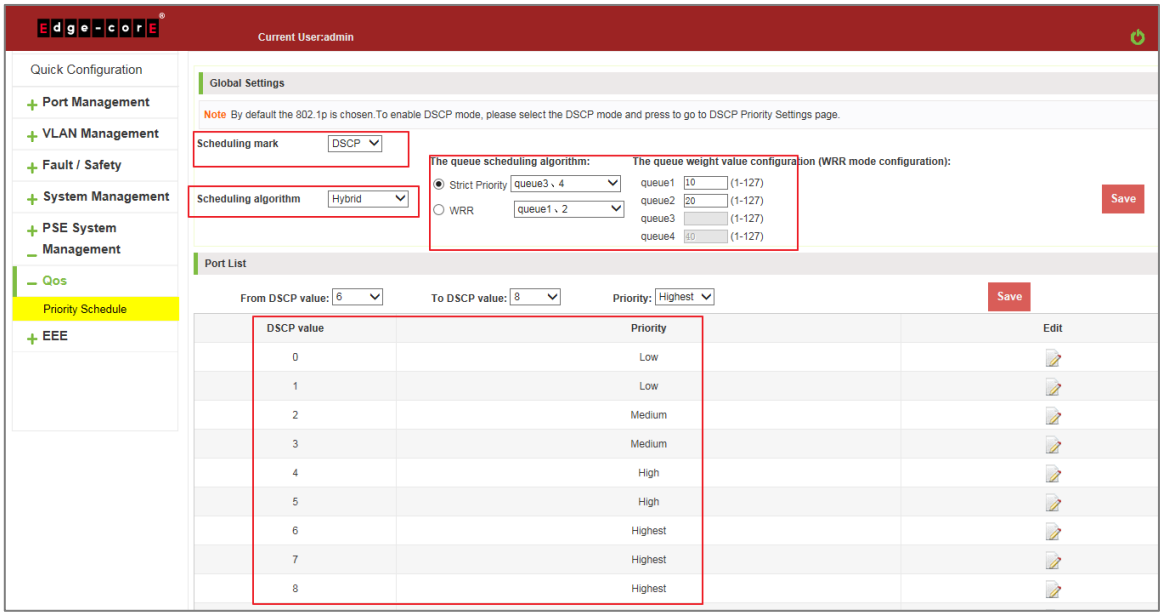


Figure 9-7: Global Settings in DSCP and HYBRID

Priority schedule steps are as follows:

Step 1: In scheduling mark, choose DSCP;

Step 2: In the Scheduling algorithm, choose hybrid;

Step 3: In strict priority text box, choose the queue3,4;

Step 4: In WRR text box, choose the queue 1,2;

Step 5: In queue1 text box, enter the weight value, such as 10;

Step 6: In queue2 text box, enter the weight value, such as 20.

9.1.4 Editing the DSCP values

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

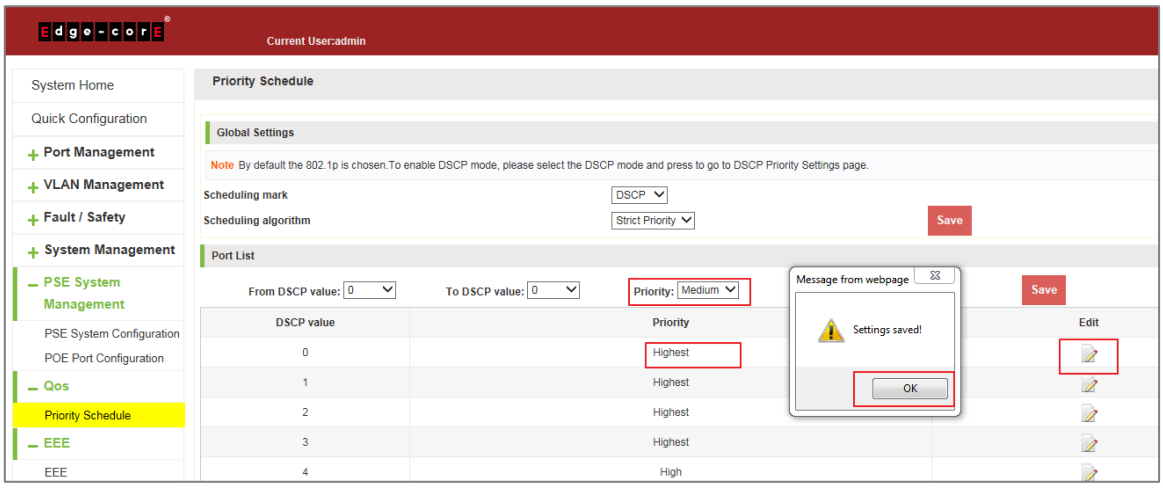


Figure 9-8: Add the Port to the VLAN

Modify DSCP values follow these steps:

Step 1: Select DSCP values and Click" "icon;

Step 2: In the priority text box, choose medium;

Step 3: Click on the save;

Step 4: Click OK.

10 EEE

10.1 EEE

10.1.1 802.3AZ EEE settings

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

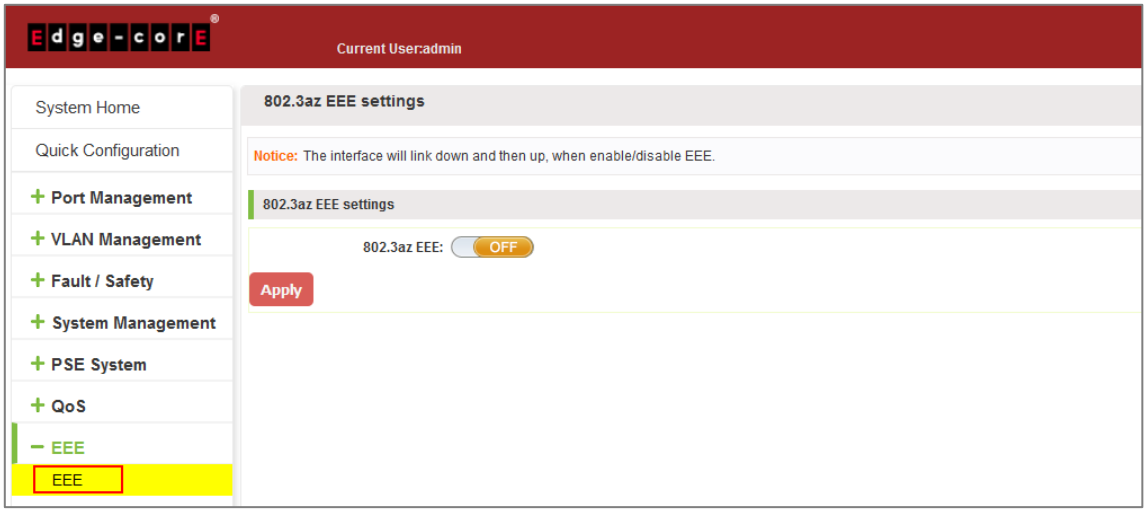


Figure 10-1: View the 802.3az EEE Settings

10.1.2 Active the EEE

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

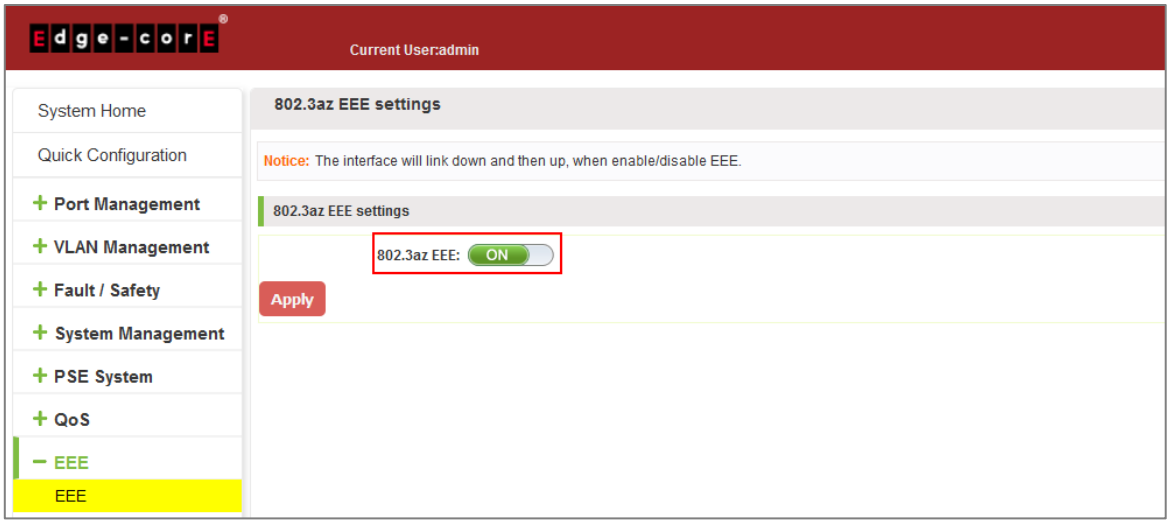


Figure 10-2: Active the 802.3az EEE Settings