



ECS2020 Series

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

Software Release  
v1.0.0.0

Web Management  
Guide

[www.edge-core.com](http://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

- 
-  There are 4 devices in this series: ECS2020-10P, ECS2020-10T, ECS2020-28P, and ECS2020-28T.
  -  The PoE function is only applicable to the ECS2020-10P and ECS2020-28P products.
  -  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

<b>1</b>	<b>WEB MANAGEMENT LANDING PAGE</b>	<b>10</b>
1.1	LOG IN TO THE SWITCH MANAGEMENT PAGE WEB	10
<b>2</b>	<b>SYSTEM HOME</b>	<b>11</b>
2.1	DEVICE PANEL	11
2.2	PORT INFORMATION	11
2.3	FLOW TREND	12
2.4	DEVICE CONFIGURATION	12
2.5	PORT STATISTICS	13
<b>3</b>	<b>QUICK CONFIGURATION</b>	<b>14</b>
3.1	BASIC SETTING	14
3.2	VLAN SETTINGS	14
3.3	PORT MODE	15
3.4	SNMP CONFIGURATION	15
<b>4</b>	<b>PORT MANAGEMENT</b>	<b>16</b>
4.1	BASIC SETTINGS	16
4.1.1	<i>Viewing the port configuration</i>	16
4.1.2	<i>Configuring port properties</i>	16
4.2	STORM CONTROL	17
4.2.1	<i>Viewing the storm control port settings</i>	17
4.3	FLOW CONTROL	19
4.3.1	<i>Configuring flow control</i>	19
4.4	PORT AGGREGATION	21
4.4.1	<i>Viewing the port aggregation configuration</i>	21
4.4.2	<i>Configuring a port aggregation group</i>	22
4.4.3	<i>Modifying port aggregation</i>	23
4.5	PORT MIRRORING	23
4.5.1	<i>Port mirroring configuration</i>	23
4.5.2	<i>Adding a port mirroring group</i>	24
4.5.3	<i>Modifying a port mirroring group</i>	25
4.5.4	<i>Deleting a port mirroring group</i>	26
4.6	PORT ISOLATION	27
4.6.1	<i>Port isolation configuration</i>	27

4.6.2	Configuring port isolation .....	27
4.6.3	Modify the port isolation.....	28
4.7	PORT SPEED LIMIT.....	29
4.7.1	View port rate limit .....	29
4.7.2	Configuring the port access rate .....	29
4.7.3	Removing the port speed limits.....	30
<b>5</b>	<b>VLAN MANAGEMENT .....</b>	<b>32</b>
5.1	VLAN MANAGEMENT .....	32
5.1.1	Showing the VLAN configuration .....	32
5.1.2	Adding a VLAN .....	33
5.1.3	Removing VLAN.....	33
5.1.4	Editing a VLAN.....	34
5.1.5	Viewing the VLAN port mode .....	35
5.1.6	Changing the port mode to trunk.....	36
5.1.7	Changing the port mode to hybrid .....	37
5.2	VOICE VLAN .....	37
5.2.1	View voice VLAN information.....	37
5.2.2	Configure voice VLAN global.....	38
5.2.3	Configuring a voice VLAN port .....	38
5.2.4	Configure voice VLAN OUI.....	39
5.2.5	Voice device address .....	40
5.3	SURVEILLANCE VLAN .....	41
5.3.1	Showing the surveillance VLAN information .....	41
5.3.2	Configuring a surveillance VLAN .....	41
5.3.3	MAC settings and the surveillance devices .....	42
<b>6</b>	<b>FAULT/SAFETY .....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1	ATTACK PREVENTION .....	43
6.1.1	ARP snooping .....	43
6.1.2	Port security .....	45
6.1.3	DHCP snooping.....	46
6.1.4	CPU Guard.....	49
6.2	PATH DETECTION .....	50
6.2.1	Path/Tracert detection.....	50
6.2.2	Cable detection .....	51
6.3	PORT ERROR DISABLE .....	52

6.4	DDOS PROTECTION .....	53
6.5	LOOP DETECTION .....	54
6.5.1	<i>Enabling loopback detection</i> .....	54
6.5.2	<i>Enabling/Disabling loopback detection on specified ports</i> .....	55
6.6	STP .....	56
6.6.1	<i>Enabling STP</i> .....	56
6.6.2	<i>STP port settings</i> .....	57
6.7	ACCESS CONTROL .....	57
6.7.1	<i>ACL access control list</i> .....	57
6.7.2	<i>Applying ACLs</i> .....	61
6.8	IGMP SNOOPING .....	63
6.8.1	<i>Viewing IGMP snooping configuration</i> .....	63
6.8.2	<i>MLD</i> .....	66
6.9	IEEE 802.1X .....	68
6.9.1	<i>AAA radius configuration</i> .....	69
6.9.2	<i>Configuring IEEE802.1X parameters</i> .....	69
6.10	AAA RADIUS .....	70
6.10.1	<i>Configuring RADIUS</i> .....	70
6.10.2	<i>TACACS+</i> .....	72
<b>7</b>	<b>SYSTEM MANAGEMENT .....</b>	<b>75</b>
7.1	SYSTEM SETTINGS .....	75
7.1.1	<i>Management VLAN</i> .....	75
7.1.2	<i>System restart</i> .....	76
7.1.3	<i>User management</i> .....	77
7.1.4	<i>System log</i> .....	78
7.1.5	<i>Log export</i> .....	78
7.1.6	<i>ARP table</i> .....	79
7.1.7	<i>MAC management</i> .....	79
7.2	DHCP SERVER .....	84
7.2.1	<i>DHCP server info</i> .....	84
7.2.2	<i>Enabling the DHCP server</i> .....	84
7.3	SYSTEM UPGRADE .....	85
7.4	SYSTEM INFORMATION .....	85
7.4.1	<i>Memory information</i> .....	85

7.4.2	CPU information.....	86
7.5	CONFIGURATION MANAGEMENT.....	86
7.5.1	Configuration management.....	86
7.5.2	Restore the factory default settings.....	88
7.6	DUAL CONFIGURATION .....	89
7.6.1	To Backup and restore the current configuration file .....	89
7.6.2	Configuration Copy.....	90
7.7	SNMP .....	91
7.7.1	Viewing the SNMP Configuration.....	91
7.7.2	Enabling SNMP.....	91
7.7.3	Disabling SNMP.....	92
7.7.4	Enabling SNMP TRAPs.....	92
7.7.5	Disabling SNMP TRAPs.....	93
7.7.6	Modifying the Community name and permissions.....	93
7.7.7	Adding an SNMP TRAP service host .....	94
7.7.8	Deleting an SNMP TRAP service host .....	94
7.8	RMON .....	95
7.8.1	Viewing the RMON configuration .....	95
7.8.2	Configuring an RMON Alarm .....	95
7.8.3	Modifying an RMON event or history .....	96
7.8.4	Deleting an RMON rule .....	97
7.9	LLDP SETTINGS.....	98
7.9.1	Viewing LLDP settings .....	98
7.9.2	Enabling LLDP settings .....	98
7.9.3	LLDP port set .....	99
7.9.4	Neighbor info .....	99
7.10	ADMINISTRATION.....	100
7.10.1	Viewing the Telnet, HTTPS and SSH settings.....	100
7.10.2	Enabling Telnet.....	100
7.10.3	Enabling HTTPS.....	101
7.10.4	Enabling SSH.....	102
<b>8</b>	<b>PSE SYSTEM MANAGEMENT .....</b>	<b>106</b>
8.1	PSE SYSTEM CONFIGURATION.....	106
8.1.1	Viewing the PSE system configuration .....	106
8.1.2	Configuring power supply mode .....	106

8.2	POE PORT CONFIGURATION.....	108
8.2.1	<i>Modifying a POE port.....</i>	109
8.3	POE TIMER CONFIGURATION .....	109
<b>9</b>	<b>QOS.....</b>	<b>111</b>
9.1	PRIORITY SCHEDULE .....	111
9.1.1	<i>Viewing the QOS priority schedule.....</i>	111
9.1.2	<i>Configuring 802.1P QoS .....</i>	111
9.1.3	<i>Configuring DSCP QoS.....</i>	113
9.1.4	<i>Editing the QoS values.....</i>	115
<b>10</b>	<b>EEE.....</b>	<b>116</b>
10.1	VIEWING THE 802.3AZ EEE SETTINGS .....	116
10.2	ENABLING 802.3AZ EEE.....	116

# 1 WEB MANAGEMENT – LOGIN

## 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). Using a web browser enter <http://192.168.2.10> in the address bar. Wait for the User Login page to appear and then enter the default user name and password (user name: admin; password: admin). Click the “Login” button to directly access the web management home page.

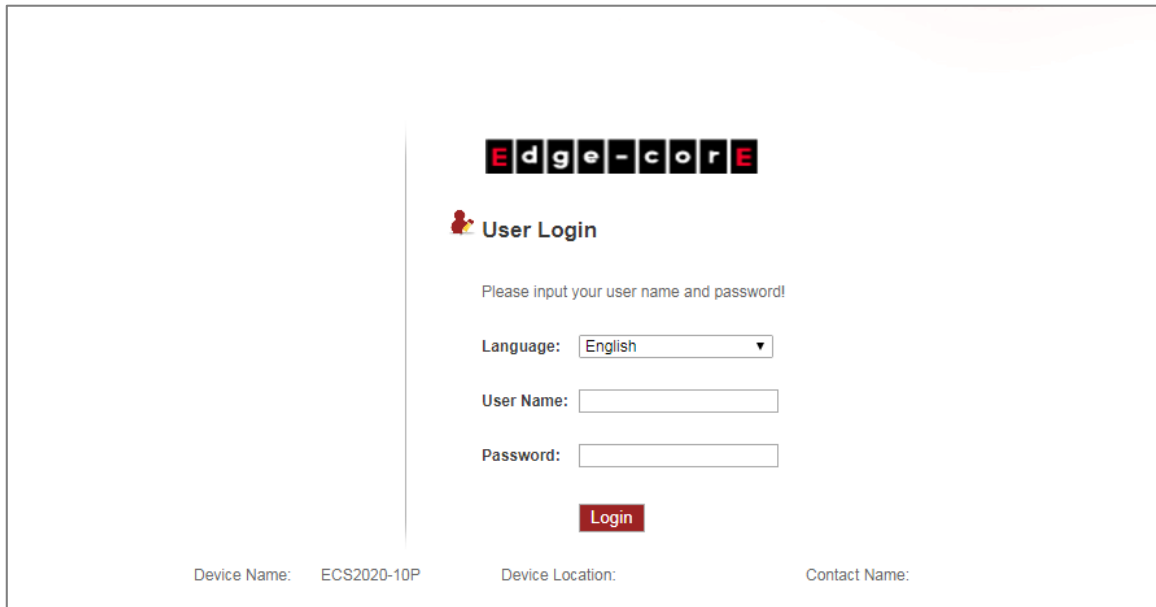


Figure 1-1: The Login Page

After launching successfully, the switch management home page displays:

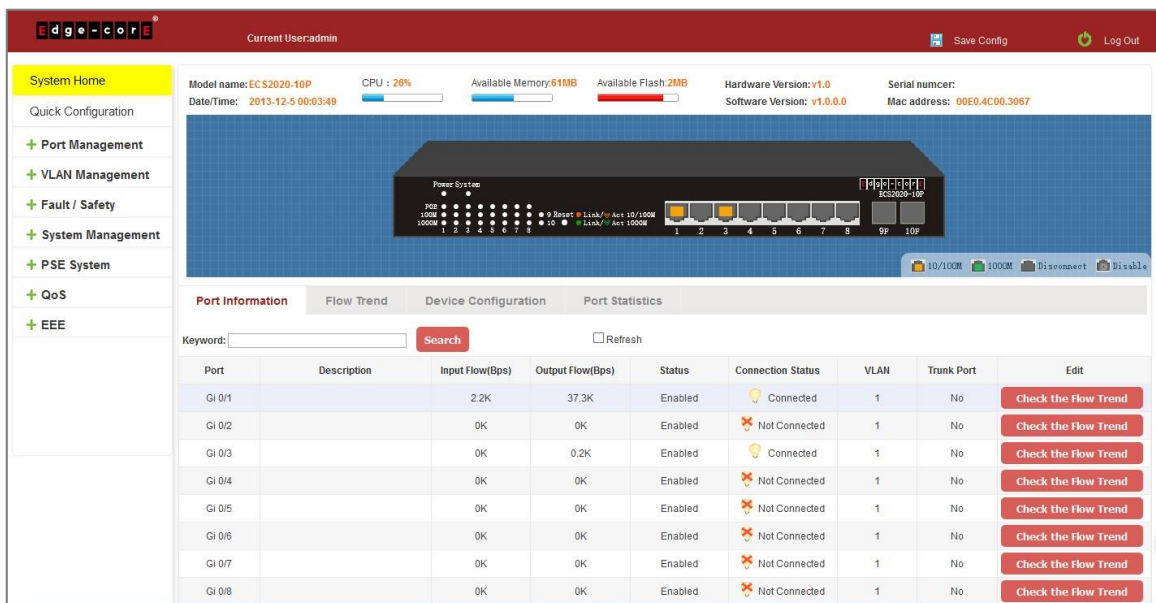


Figure 1-1: Web Management Home Page

## 2 SYSTEM HOME

### 2.1 DEVICE PANEL

1. Use the system home page to get a quick understanding of the device operating state, panel information, port status and general network management information.

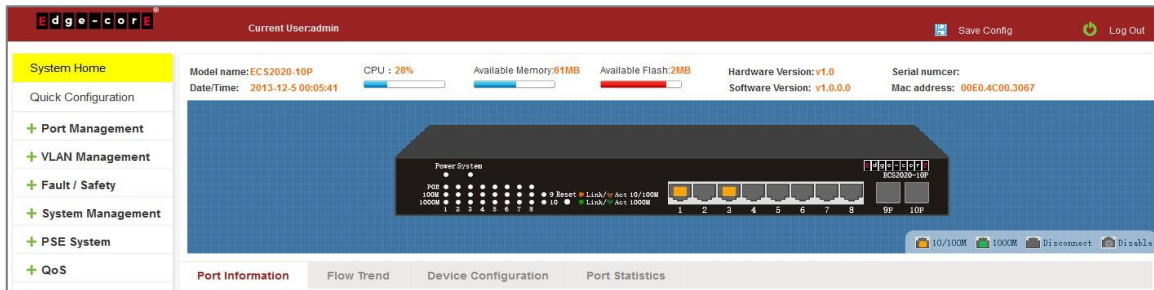


Figure 2-1 Web View of the Switch Front Panel

2. Clicking on a specific port displays the pop-up window shown in the screenshot below and it is possible to use the Enable/Disable radio buttons to administratively shutdown or bring up the port.

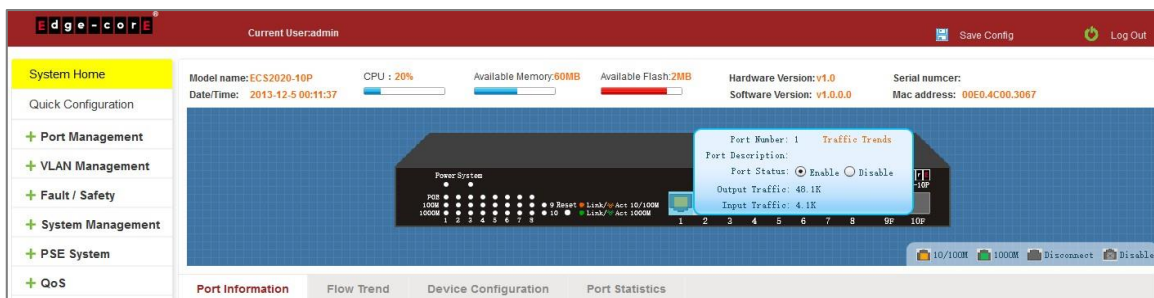


Figure 2-2 Port Pop-Up

### 2.2 PORT INFORMATION

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

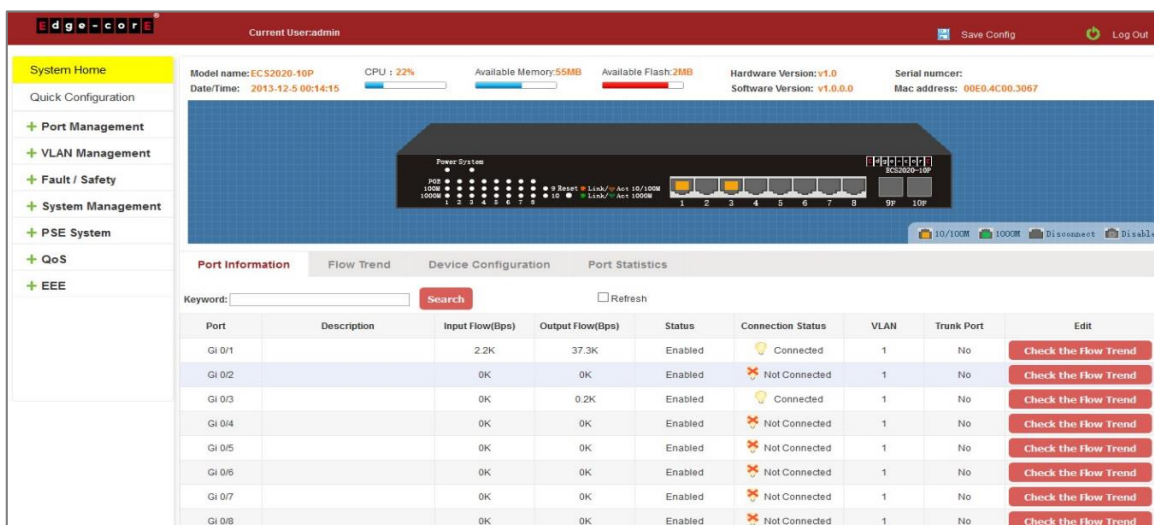


Figure 2-3 Port Information

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.

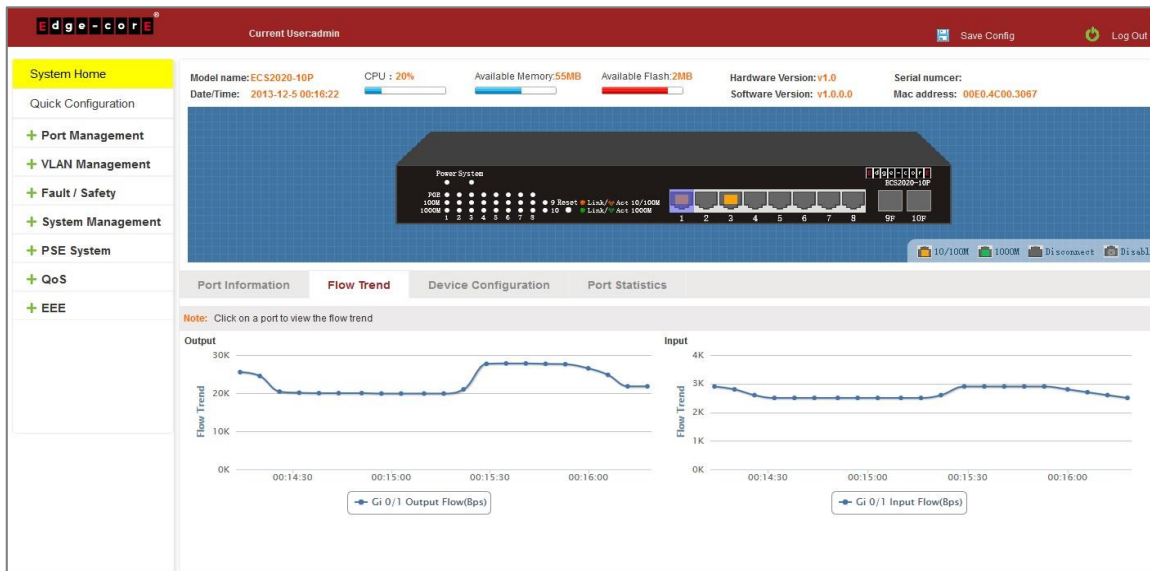


Figure 2-4 Viewing the Flow Trend

## 2.4 DEVICE CONFIGURATION

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

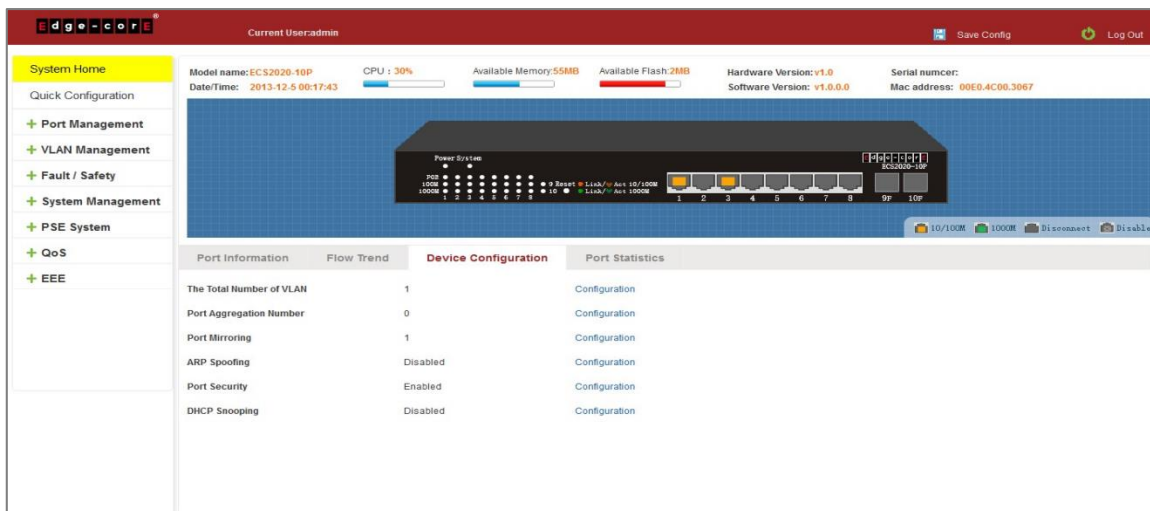


Figure 2-5 Device Configuration

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.

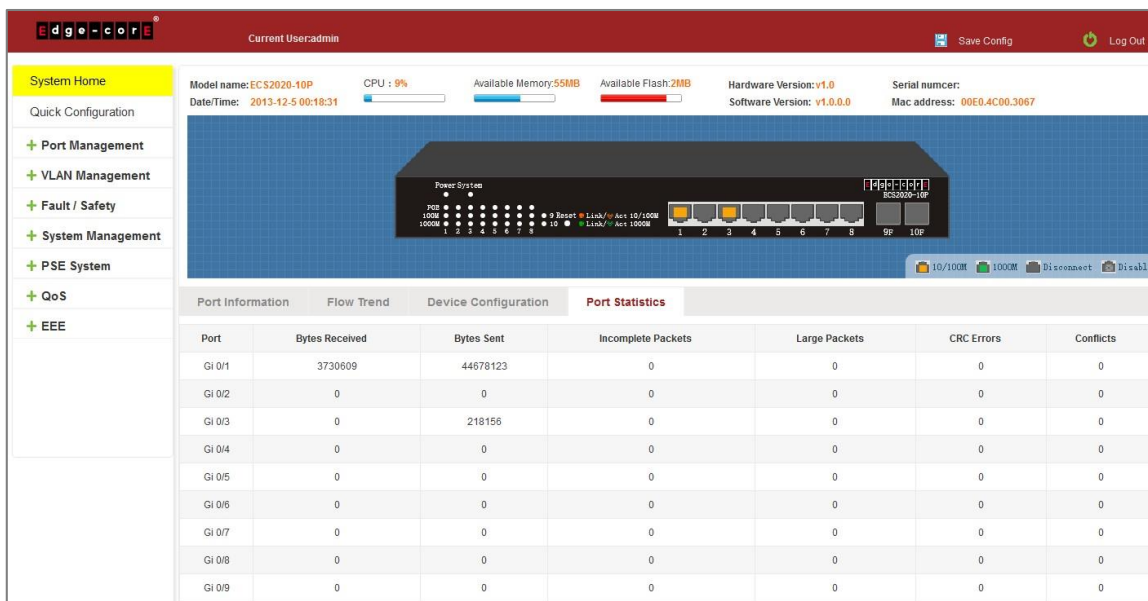


Figure 2-6 Viewing Port Statistics

### 3 QUICK CONFIGURATION

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

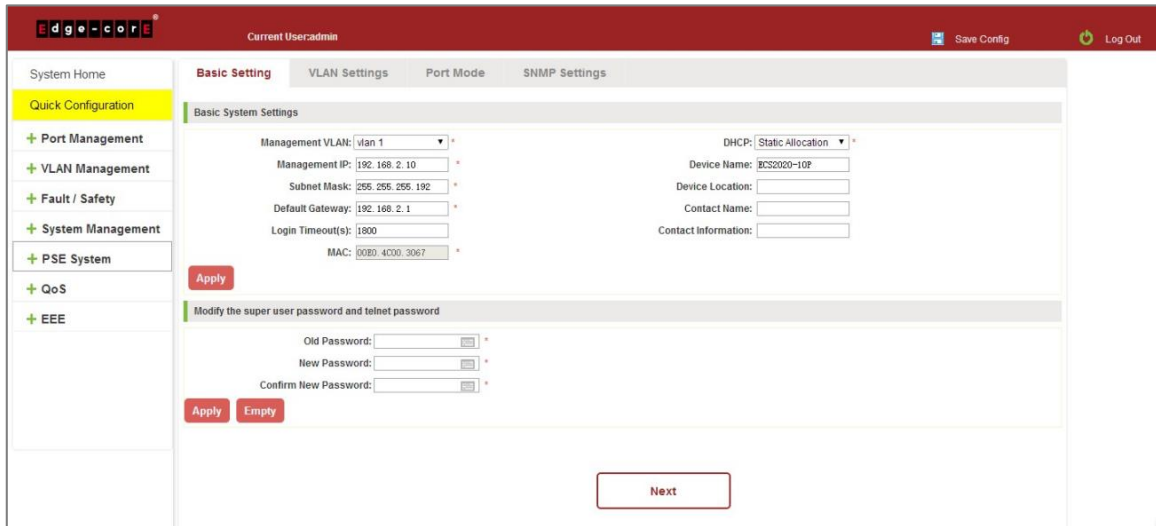


Figure 3-1: Basic Setting

#### 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".

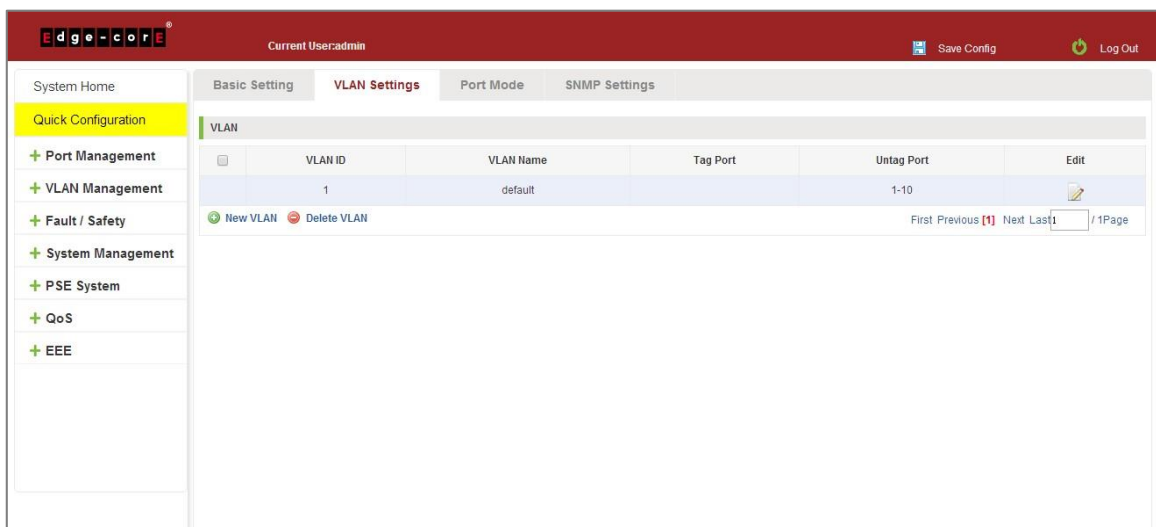


Figure 3-2: VLAN Settings

### 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 "Next".

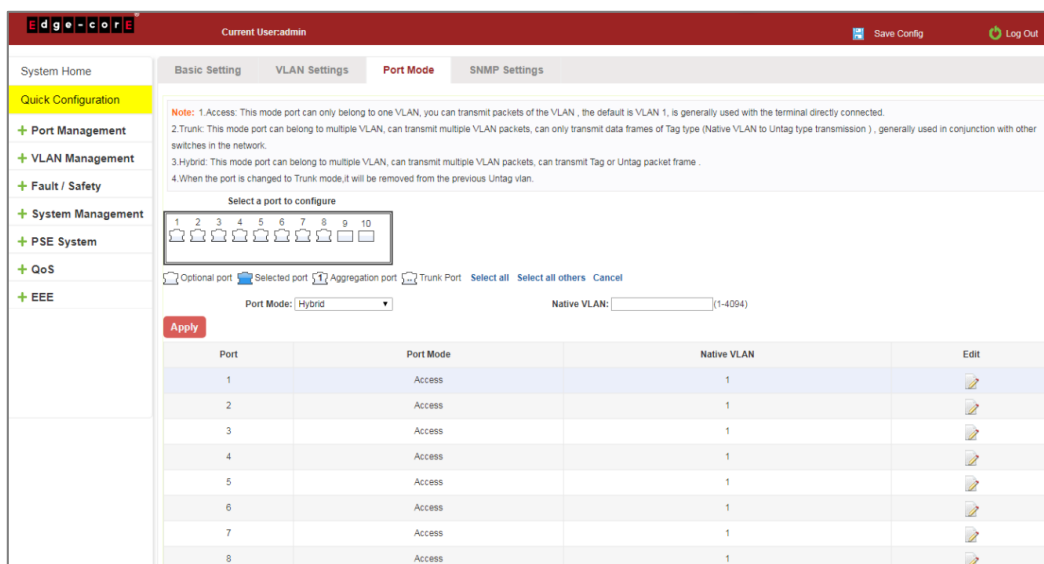


Figure 3-3: Port Mode

### 3.4 SNMP CONFIGURATION

Click "Quick Configuration" and then "SNMP Settings" to access the SNMP Settings page. You can configure SNMP settings, such as enable/disable SNMP and SNMP TRAP services, etc. When configuration is complete, click "Next".

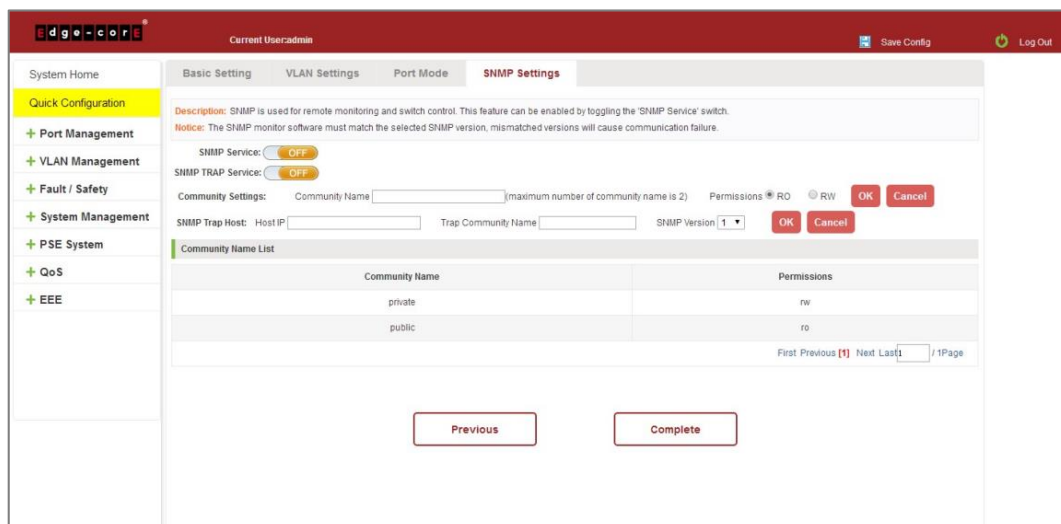


Figure 3-4: SNMP Settings

## 4 PORT MANAGEMENT

### 4.1 BASIC SETTINGS

#### 4.1.1 Viewing the port configuration

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

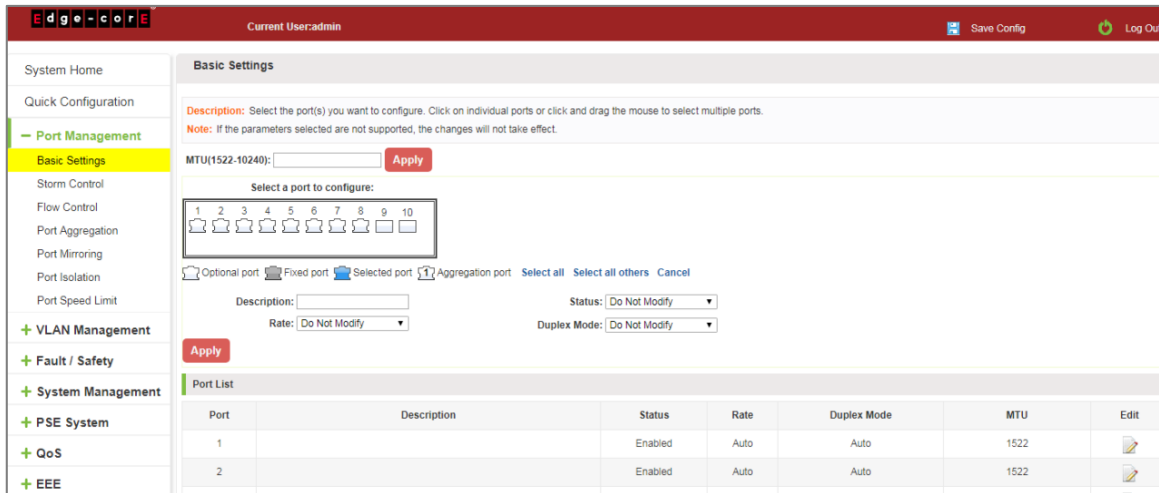


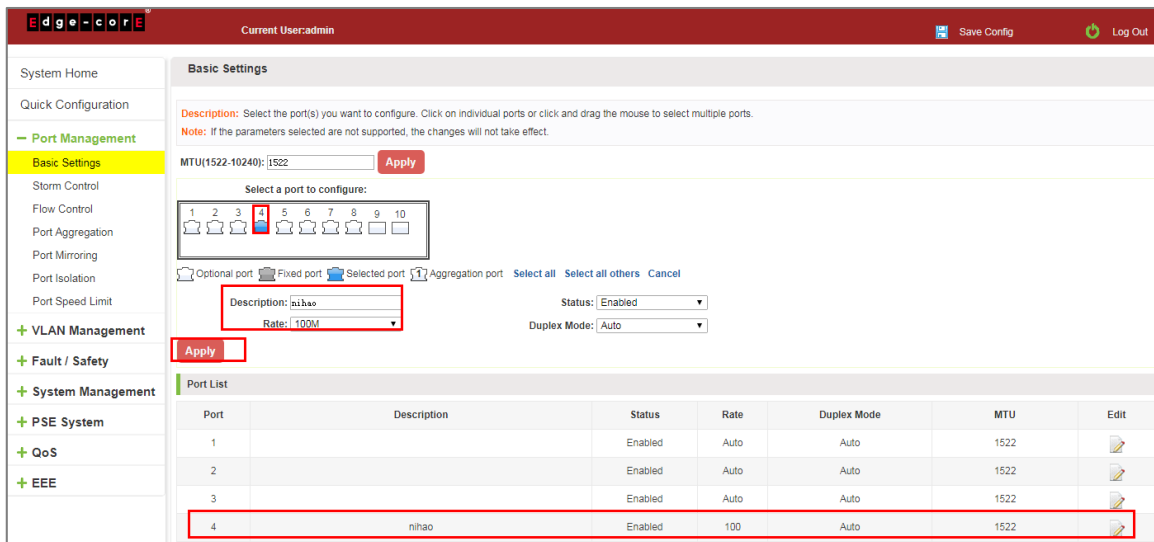
Figure 4-1: Viewing the Port List Data

The port list attributes show the current switch port configuration:

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**

To configure port properties:

Step 1: Click the edit icon

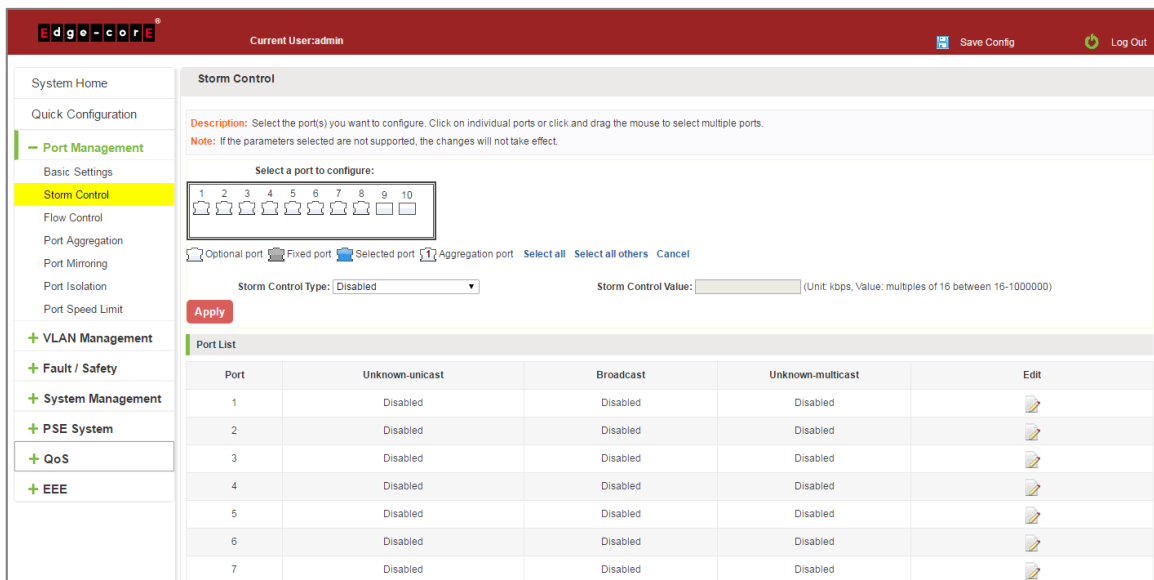
Step 2: In the Port Properties configuration page, fill or select the value to be configured.

Step 3: Click Apply

## 4.2 STORM CONTROL

### 4.2.1 Viewing the storm control port settings

Click "Port Management" and then "Storm Control" to view the current switch port storm control information.



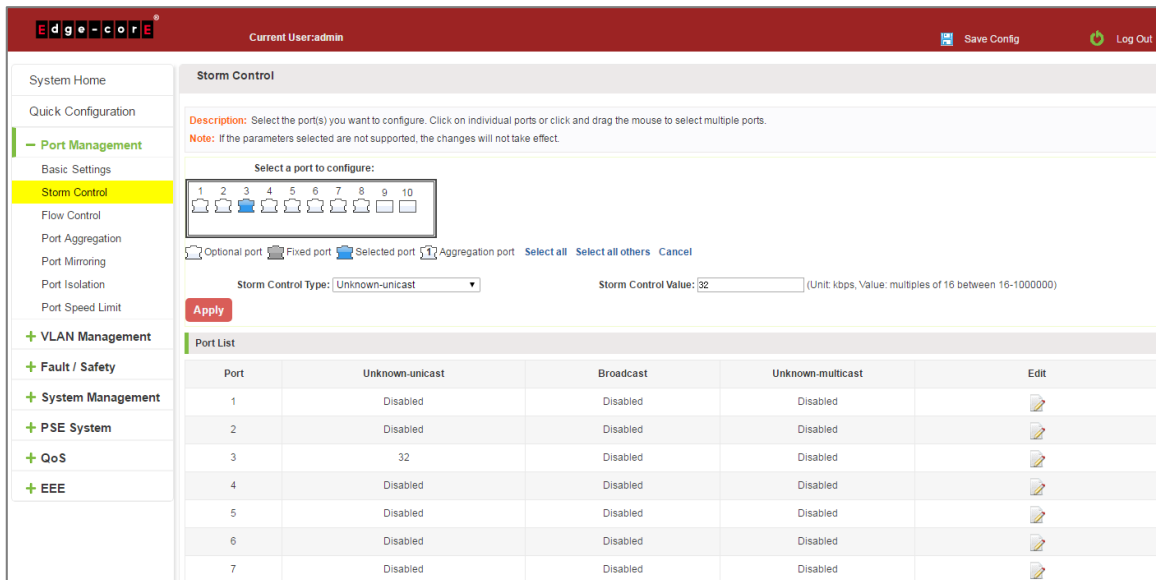
**Figure 4-3: Viewing the Storm Control List**

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

1. Port: The number of the port.

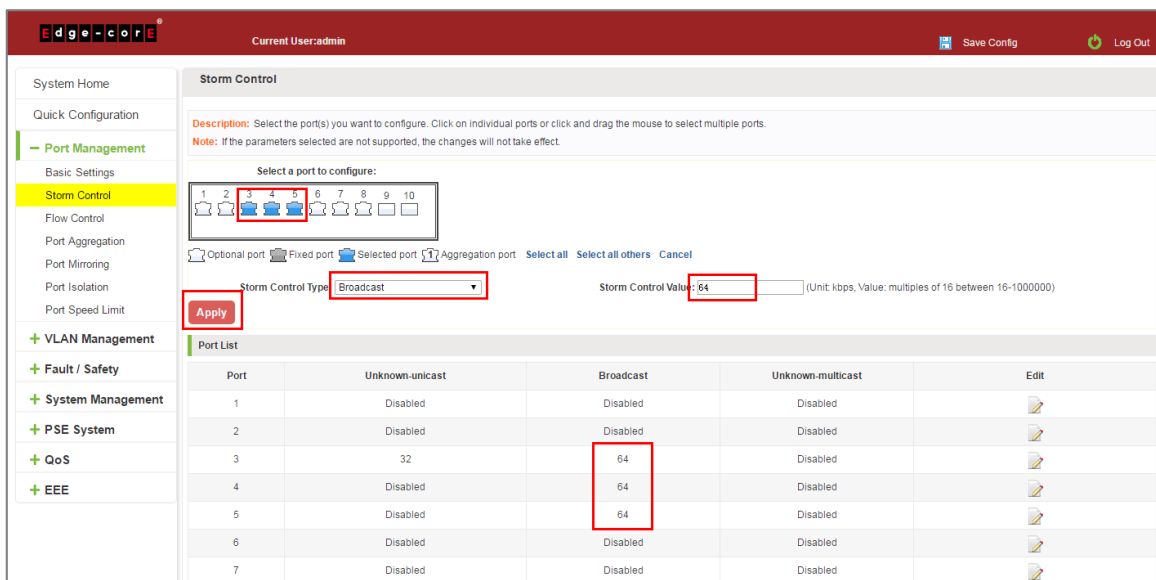
2. Unknown-unicast: Unknown unicast packets control.
3. Broadcast: Broadcast packet control.
4. Unknown-multicast: Multicast packets control.
5. When the control value setting is not a multiple of 16, the system automatically matches the closest multiple of 16.
6. The control values of unknown-unicast,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

Clicking the corresponding port on the port panel view selects the port(s) 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**

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.

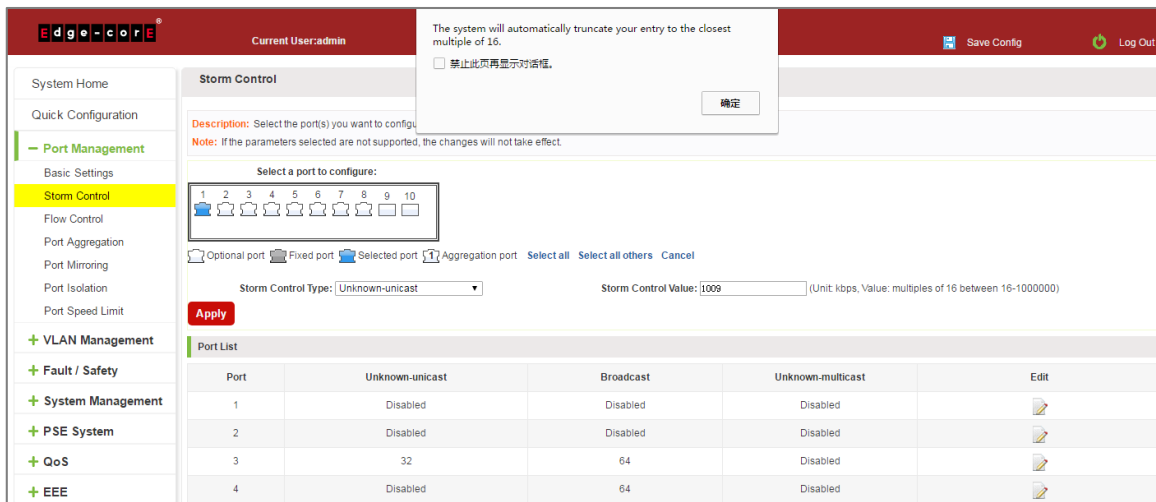


Figure 4-6: Configuring Storm Control Information

The configuration displays as shown below:

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	1008	Disabled	Disabled	
2	Disabled	Disabled	Disabled	

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.

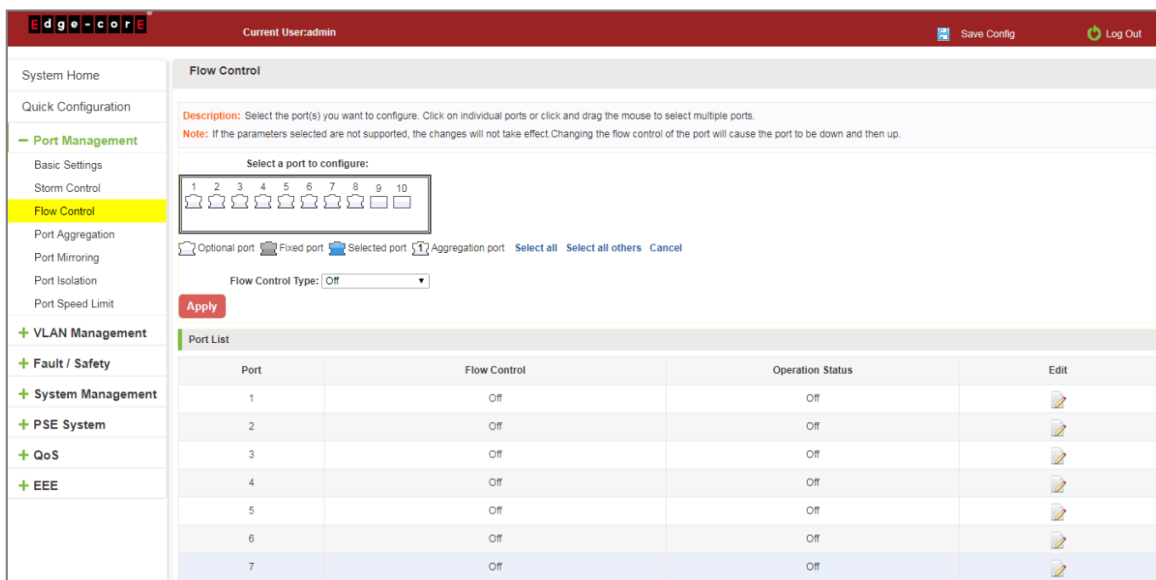
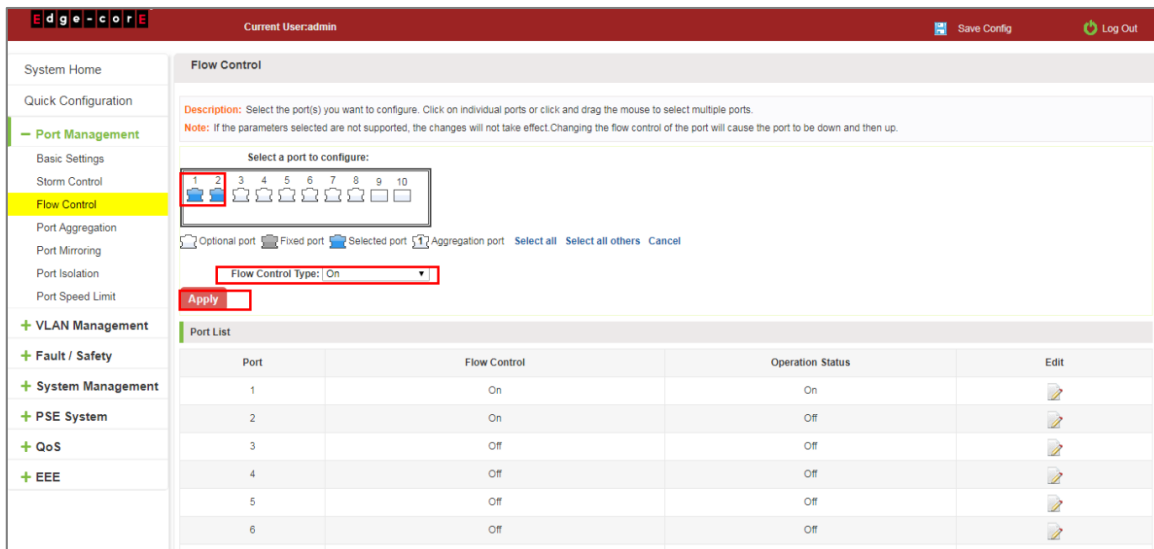


Figure 4-8: Flow Control Information

#### 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" in the Flow Control Type pull down menu and click Apply.



**Figure 4-9: Open Port Flow Control Function**

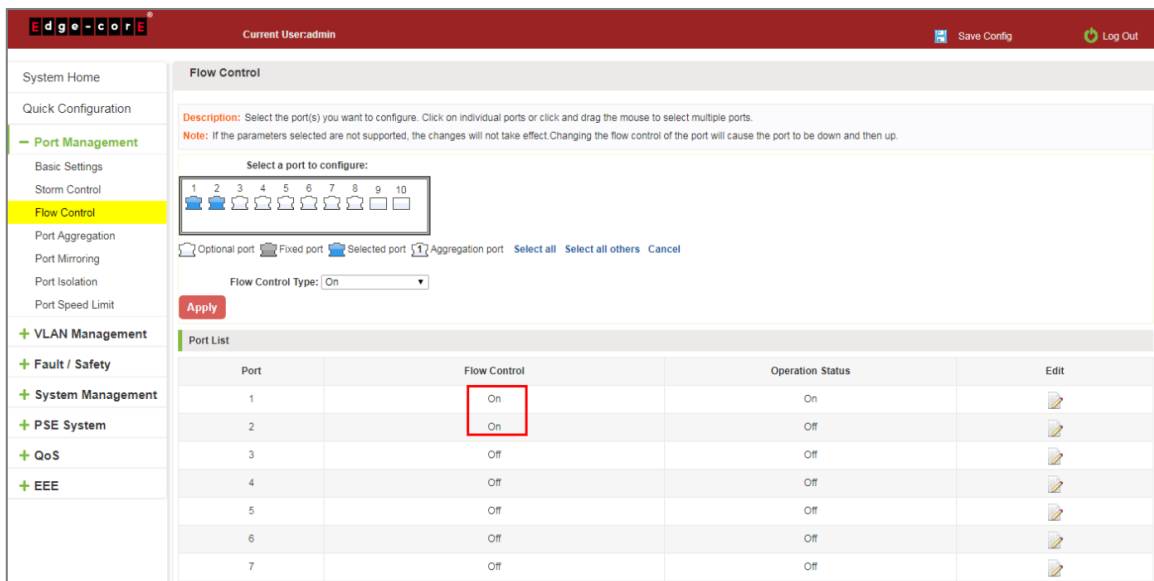
To enable port traffic control:

Step 1: Select the port.

Step 2: Set the Flow control Type 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's flow control function: click the button in the Edit column of the port list.



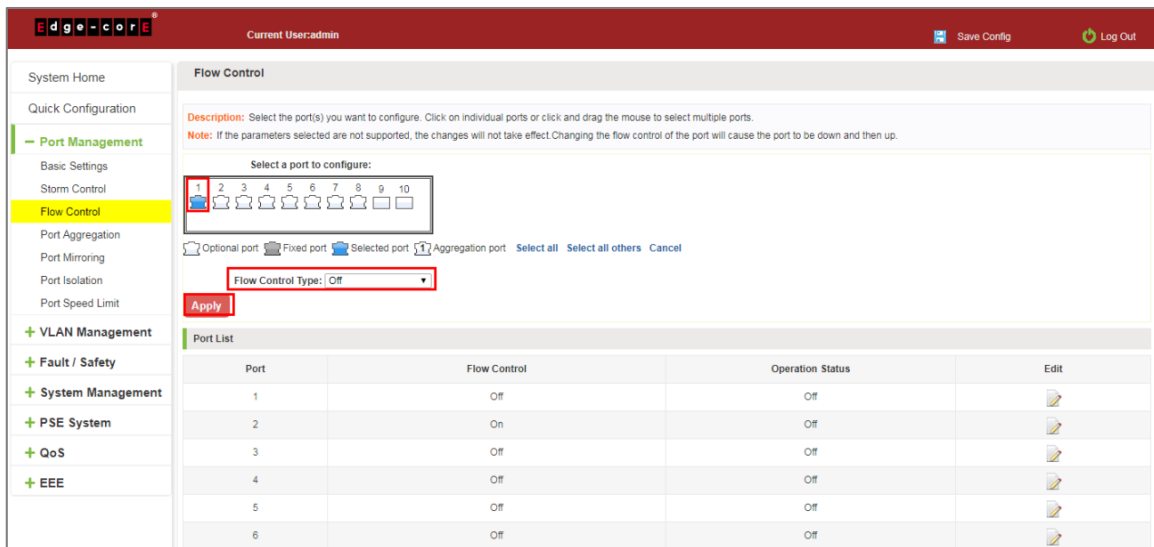


Figure 4-11: Close the Port Flow Control

To turn off port flow control:

Step 1: Select a port by clicking on the desired port in the "Select a port to configure:" port panel view.

Step 2: Set the Flow Control Type drop down menu to Off.

Step 3: Click Apply.

## 4.4 PORT AGGREGATION

### 4.4.1 Viewing the port aggregation configuration

Click "Port Management"->"Port Aggregation" to view the current port aggregation configuration.

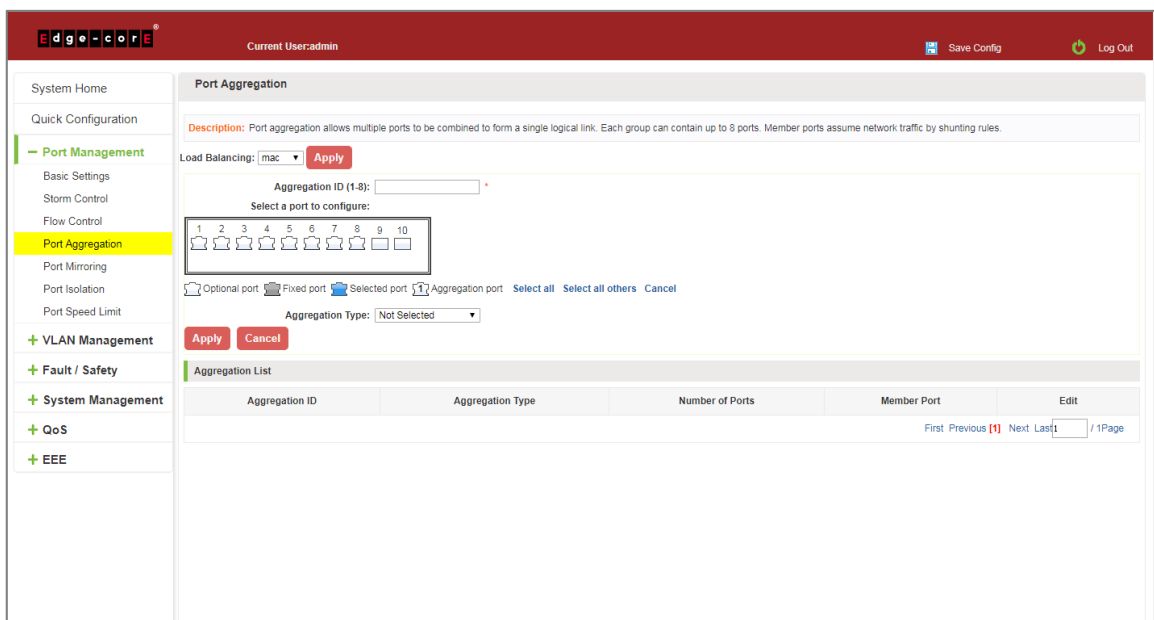


Figure 4-12: Port Aggregation Configuration

The port aggregation list shows the current port configuration:

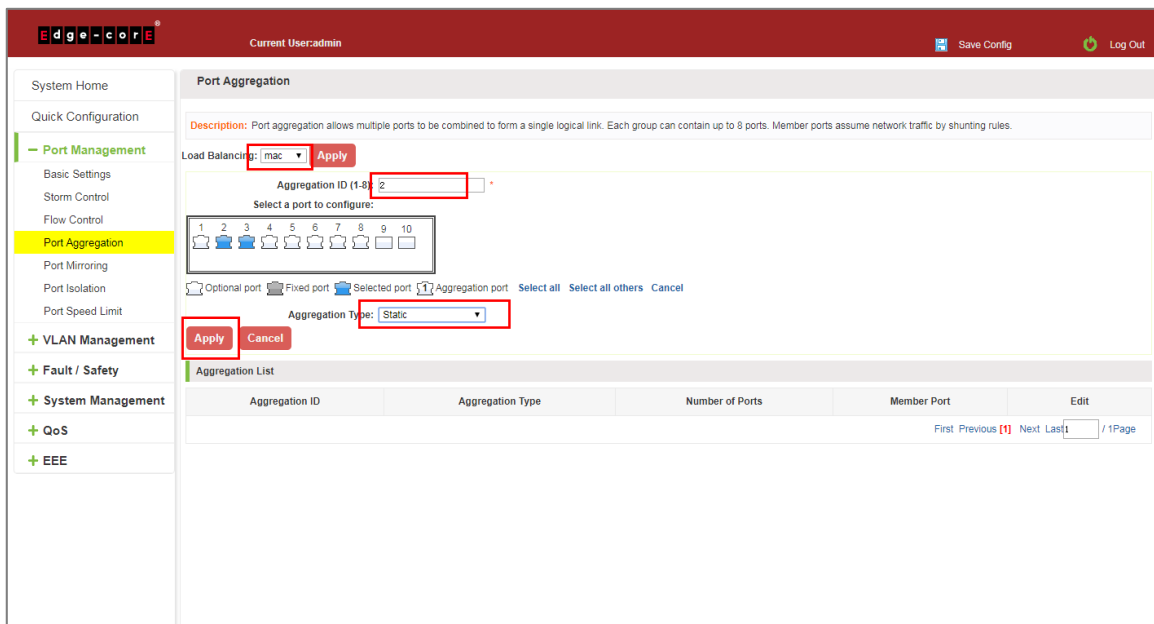
1. **Aggregation number:** The link aggregation group number value.
2. **Load Balancing:** Displays the current link aggregation group load balancing condition.
3. **Aggregate types:** Displays the port aggregation protocol.
4. **Member ports:** The number of ports in the link aggregation group by displaying the current port link aggregation group members.

Configuring aggregated ports can bind a maximum of eight member ports together, and transfer data among members of the group using network traffic shunt rules.

The port members of a port aggregation group must ensure that their port speed, duplex and port states agree otherwise the configuration will fail when using the Apply button.

#### 4.4.2 Configuring a port aggregation group

1. In the Aggregation ID field enter an aggregation ID from 1 to 8.
2. Select the desired ports to be aggregated in the port window.
3. Select the aggregation type.
4. Click Apply.




**Figure 4-13: Port Aggregation Configuration Area**

To add more ports to the aggregated logical:

- Step 1: Select the “load the shunt” option in the Load Balancing drop down menu.
- Step 2: Enter the aggregation ID number in the "Aggregation ID" field.
- Step 3: Select the ports to be aggregated in the port window.
- Step 4: Select the aggregation type in the “Aggregation Type” drop down menu.
- Step 5: Click Apply.

### 4.4.3 Modifying port aggregation

In the Aggregation List click on the  icon under Edit that corresponds to the Aggregation group that needs to be modified:

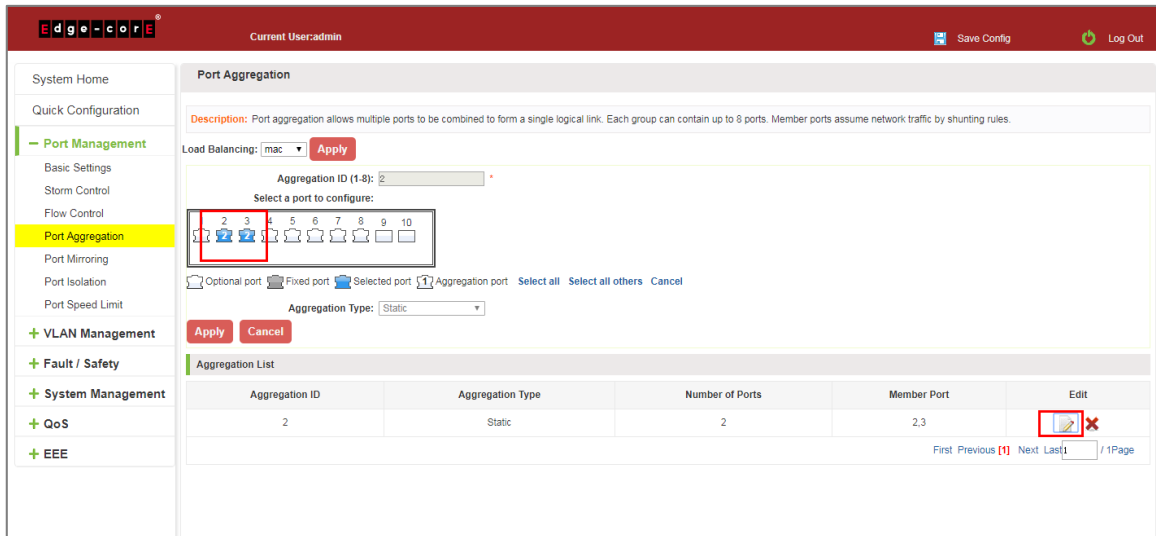


Figure 4-14: Modifying the Port Aggregation

Modify Link Aggregation Procedure:

Step 1: In the Aggregation List, click the Edit icon on the right that corresponds to the Aggregation group.

Step 2: In the port aggregation configuration page modify the load balancing type.

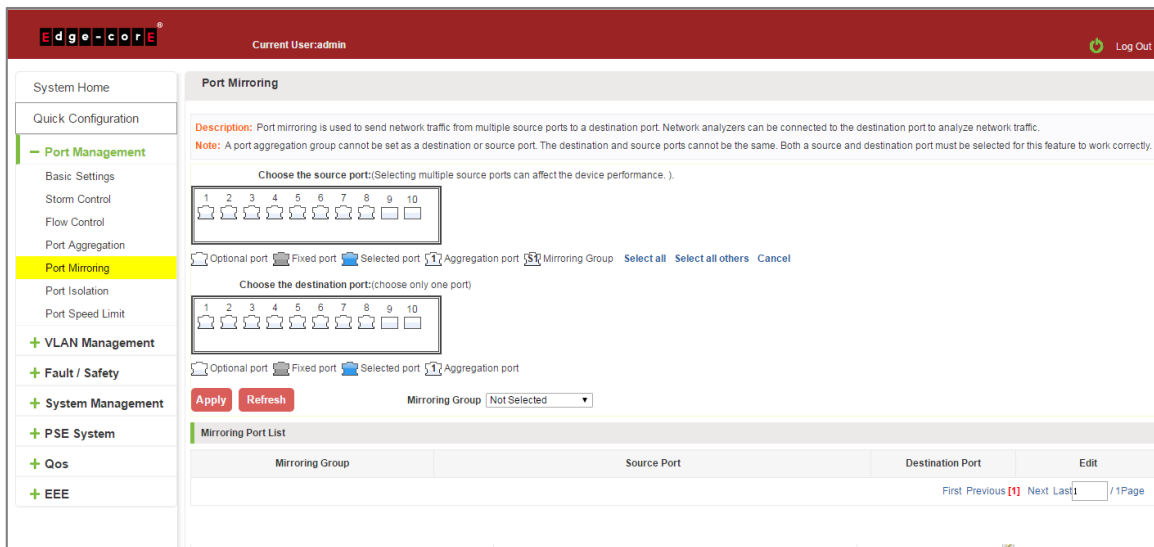
Step 3: To add a port to the aggregation group select it.

Step 4: Click Apply.

## 4.5 PORT MIRRORING

### 4.5.1 Port mirroring configuration

Click "Port Management" - "Port Mirroring"






**Figure 4-15: Port Mirroring Configuration Information**

The Mirroring Port List at the bottom of the page shows the current port mirroring configuration.

**Mirroring group:** This is the ID that identifies the port mirroring (1-7).

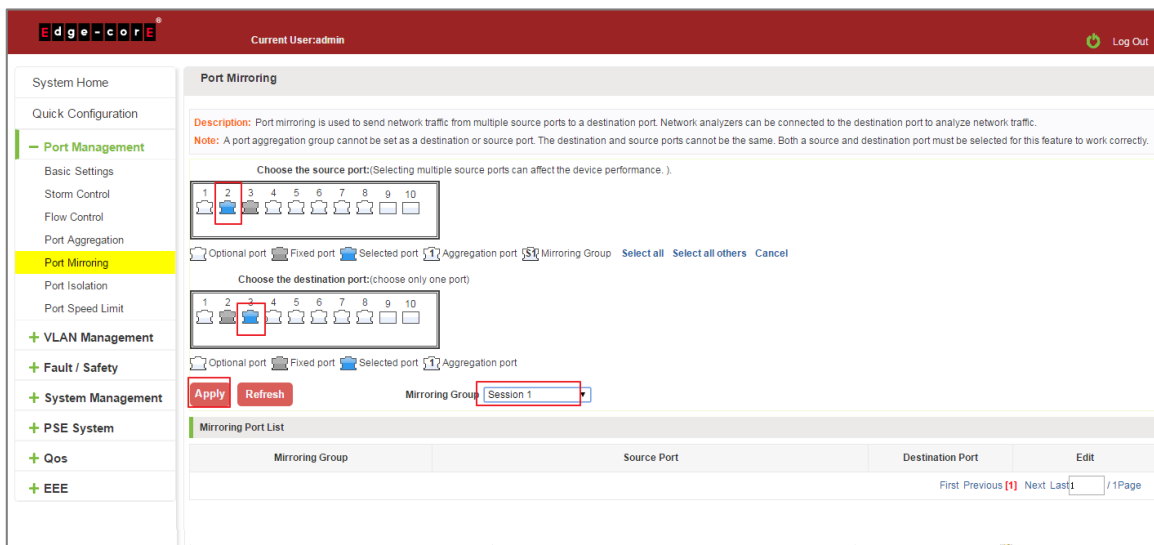
**Source Port:** The port selected to forward its traffic to another port.

**Destination port:** The port which receives the forwarded traffic from the configured source port.

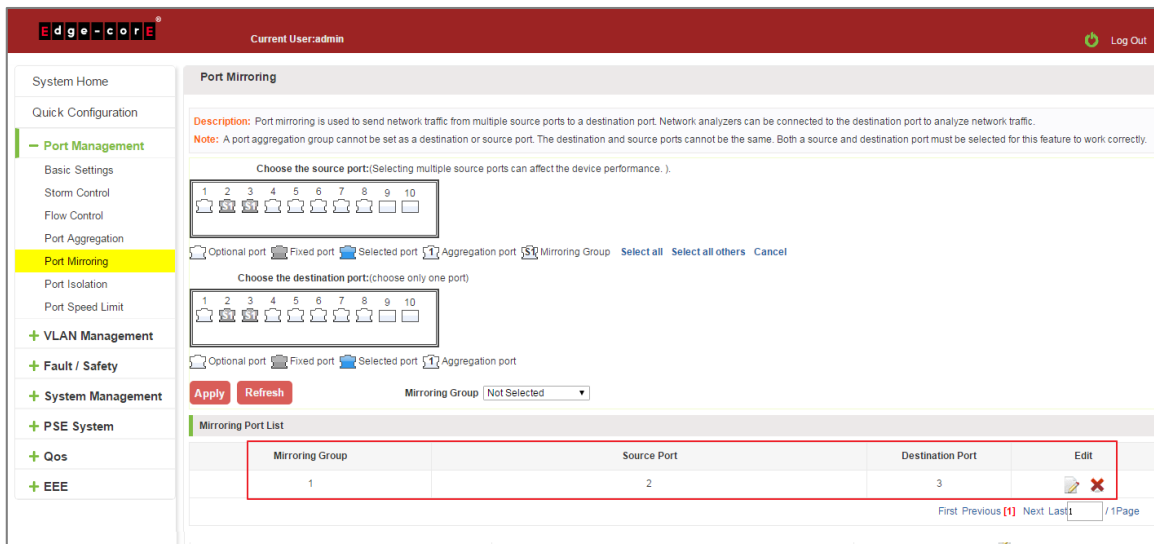
- 
-  **Note 1:** A Port aggregation port cannot be used as either a destination port or a source port.
  -  **Note 2:** The destination port and source port cannot be the same port.
  -  **Note 3:** A group mirroring group can have only one destination port.
- 

#### 4.5.2 Adding a port mirroring group

Select the source and destination ports in the appropriate windows, select the mirroring group session ID and then click Apply.



**Figure 4-16: Adding a Port Mirroring Group**



**Figure 4-17: Adding a Port Mirroring Group Results**

Port mirroring configuration steps:

Step 1: Select a Source Port.

Step 2: Select a Destination Port.


Step 3: Select a Mirroring Group.

Step 4: Click Apply.

Configuration Notes:

1. A maximum of 7 mirroring groups can be configured.
2. Aggregated ports are shown as gray in the panel – these cannot be configured for port mirroring.
3. Additionally, ports already being used for port mirroring are also displayed as gray (grey ports are unavailable when configuring a new port mirroring).

### 4.5.3 Modifying a port mirroring group

Select the group to modify, click the  icon under the Edit field in the Mirroring Port List and make the modifications.

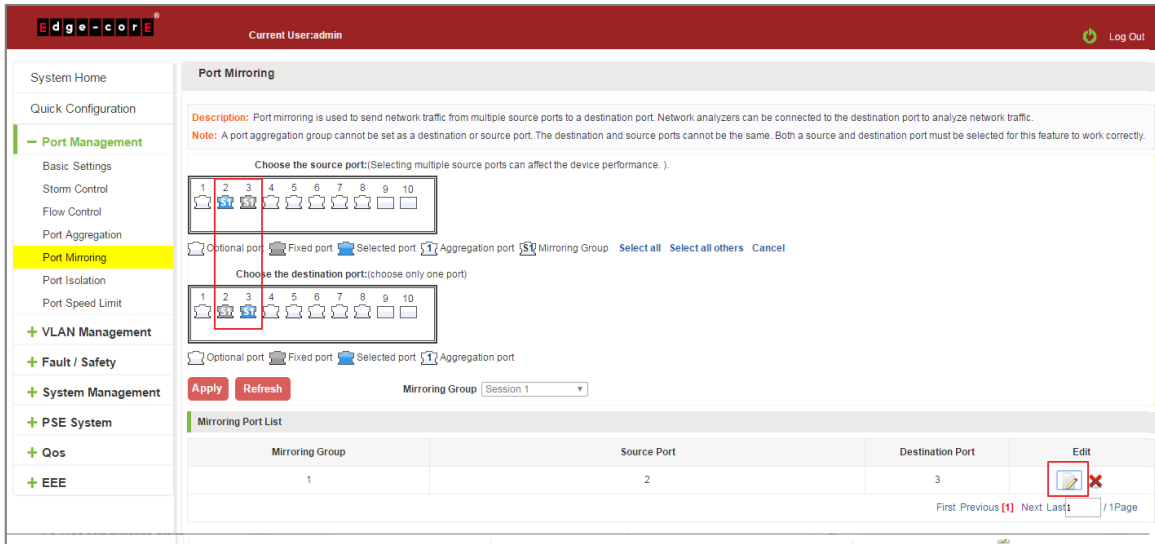



Figure 4-18: Modifying the Port Mirroring Group

To Modify the port mirroring configuration:

- Step 1: Click the  icon in the Mirroring Port List.
- Step 2: Add or remove the ports required in the configuration panel.
- Step 3: Click Apply.

#### 4.5.4 Deleting a port mirroring group

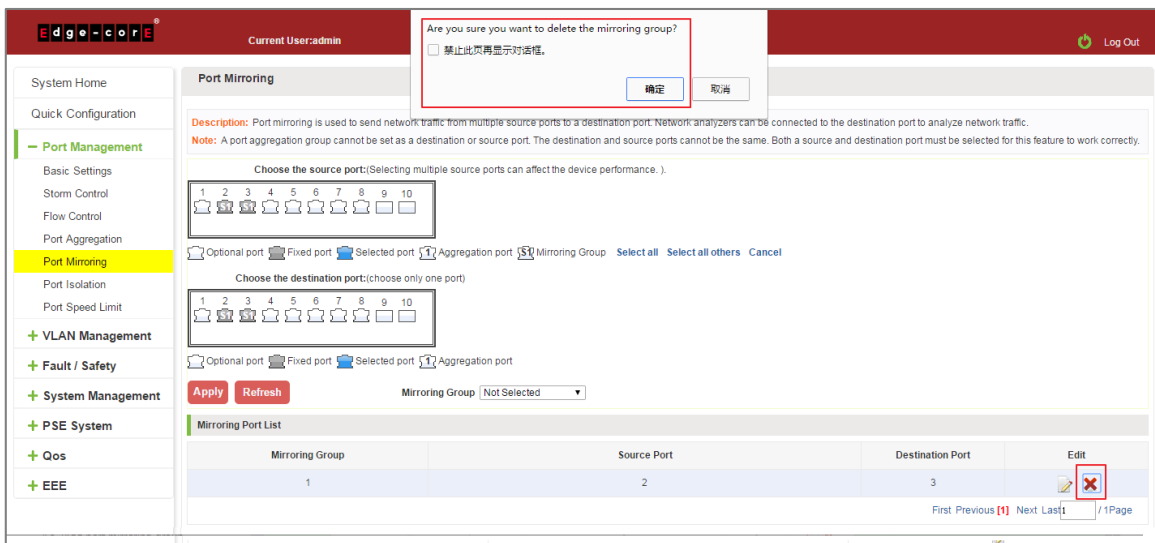


Figure 4-19: Deleting a Port Mirroring Group

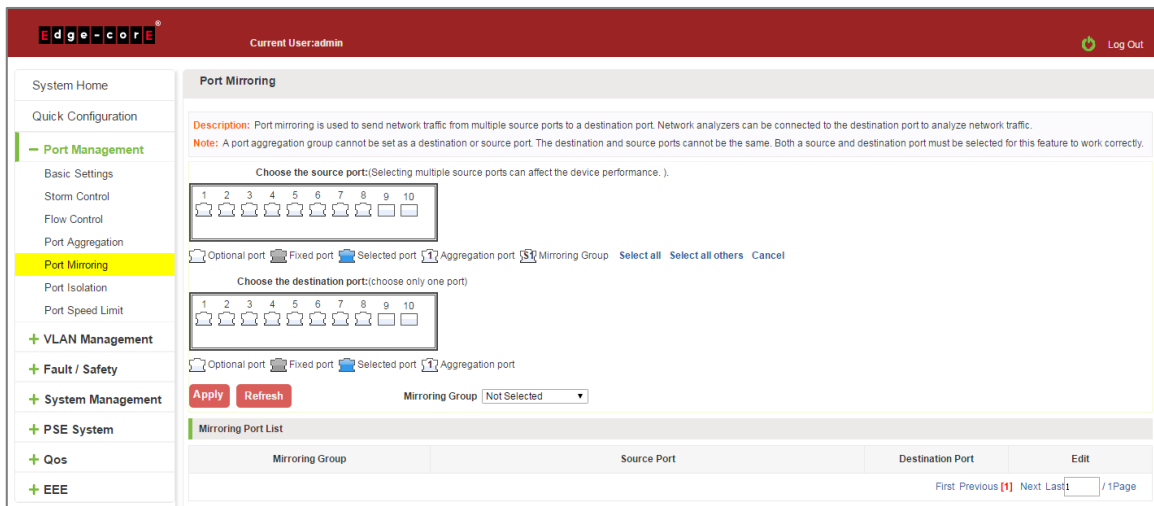



Figure 4-20: A Successfully Deleted Port Mirroring group

To remove a port mirroring configuration:

Step 1: Click the  icon in the appropriate Mirroring Port List row.

Step 2: In the new 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" - "Port Isolation"

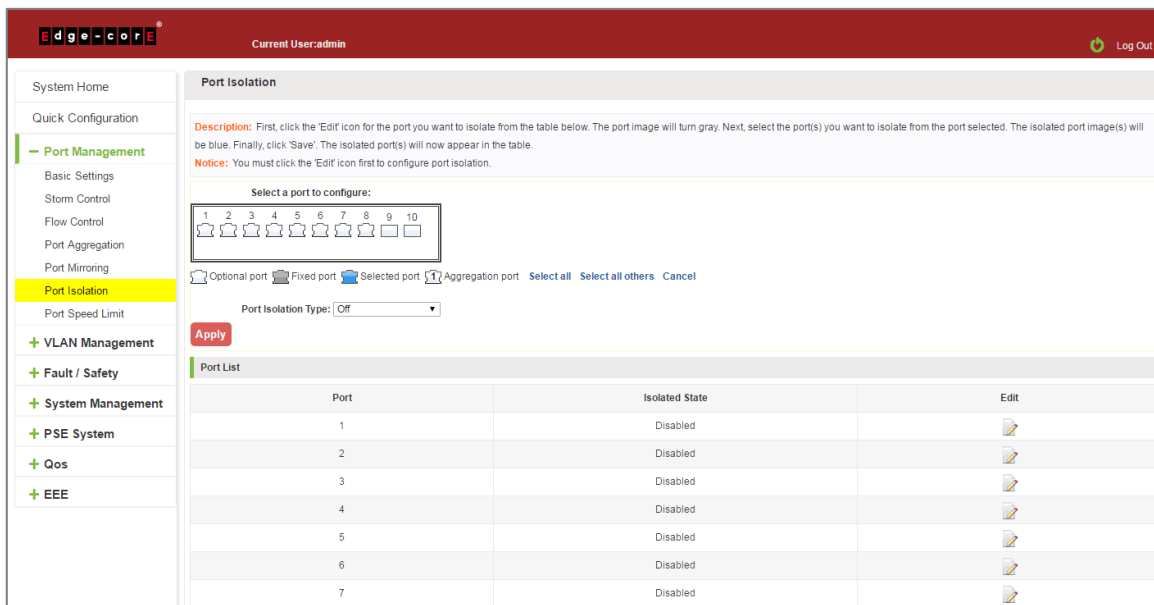
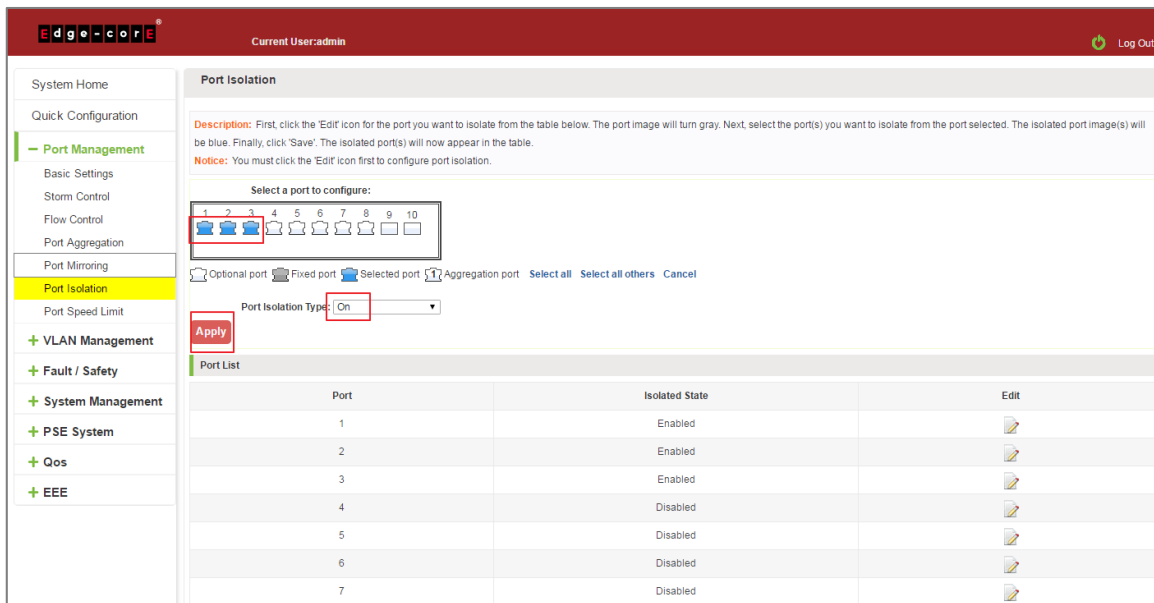


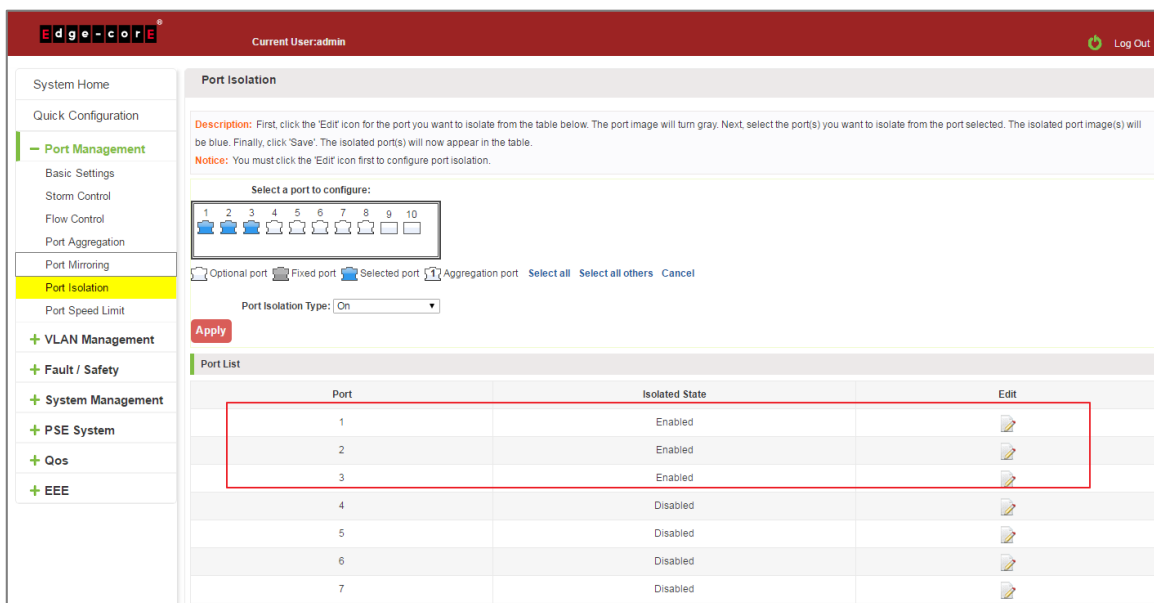
Figure 4-21: Viewing Port Isolation Configuration

### 4.6.2 Configuring port isolation

Select the port(s) to configure port isolation on, then set the Port Isolation Type to On, finally click Apply.



**Figure 4-22: Enabling the Port Isolation Function**



**Figure 4-23: Enabling Port Isolation Results**

### 4.6.3 Modify the port isolation

In the Port List select the port to modify and click the icon under the Edit column. Make the modifications to the port isolation configuration.



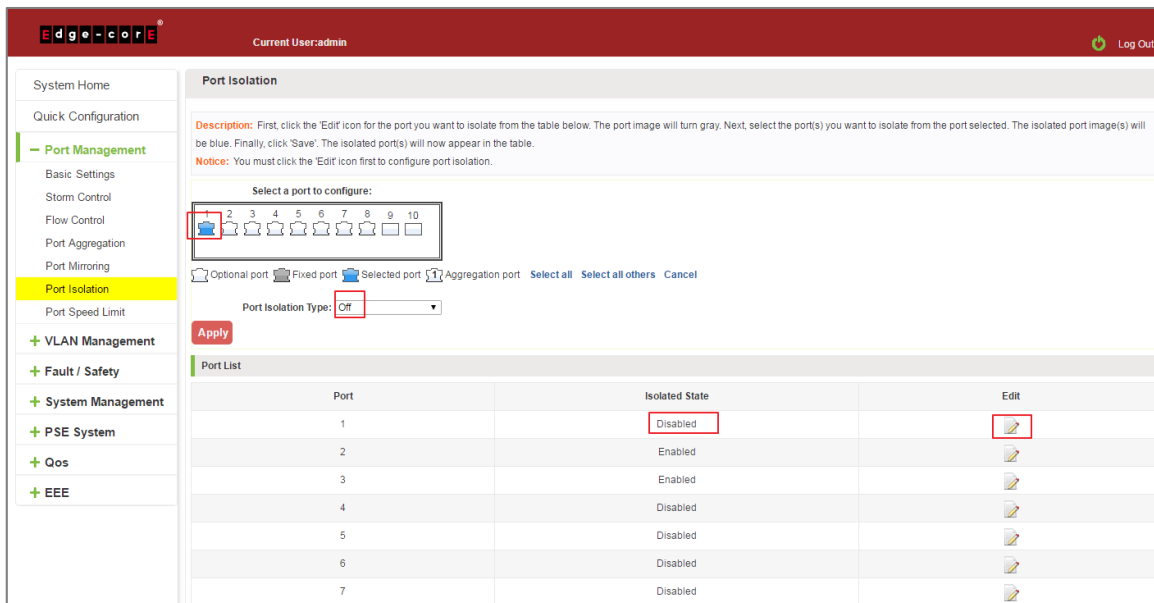


Figure 4-24: Modifying the Port Isolation configuration

## 4.7 PORT SPEED LIMIT

### 4.7.1 View port rate limit

Click "Port Management" - "Port Speed Limit" to view the currently configured port speeds.

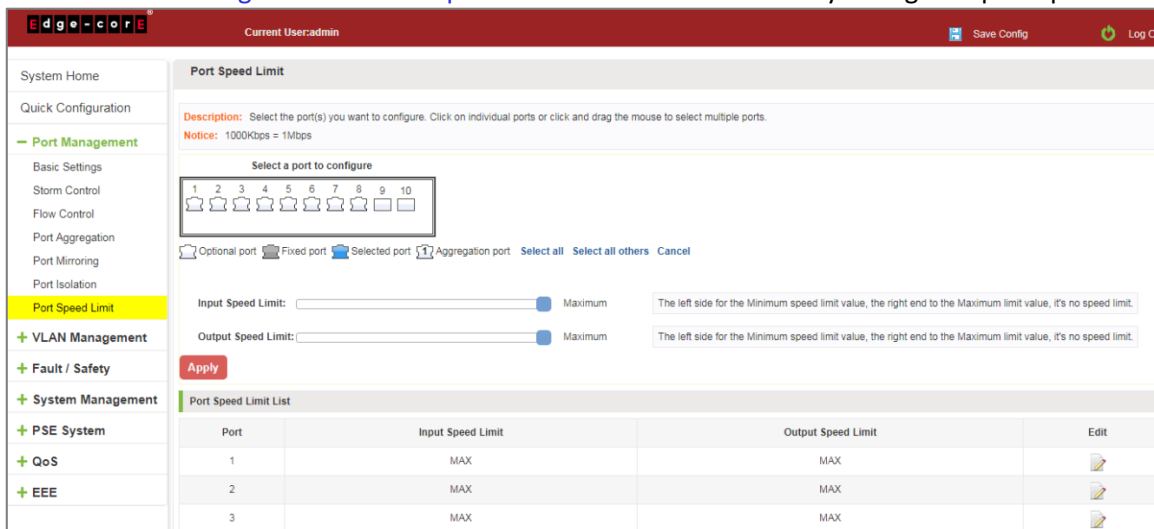


Figure 4-25: Viewing the port speed configuration

The port speed limit list shows the current speed limits for each port.

**Port:** The number of the port;

**Input limit:** uplink port speed;

**Output speed:** port downstream rate;

### 4.7.2 Configuring the port access rate

In the port panel view click the port to select it and then set the speed limit value by dragging the Input and Output Speed Limit bars.

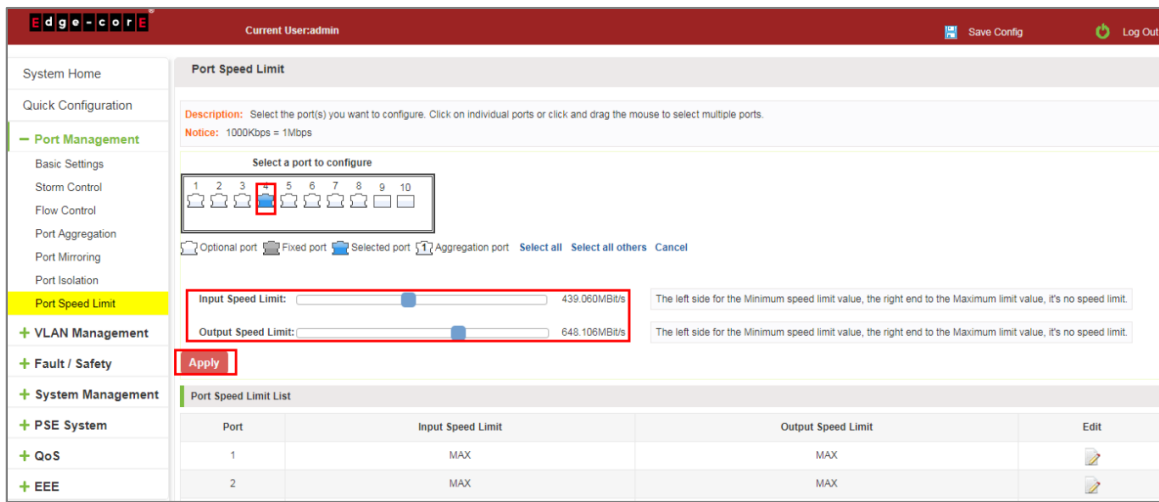


Figure 4-26: Configuring the Port Speed Limits

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	
2	MAX	MAX	
3	MAX	MAX	
4	439.056Mbit/s	648.112Mbit/s	
5	MAX	MAX	
6	MAX	MAX	
7	MAX	MAX	

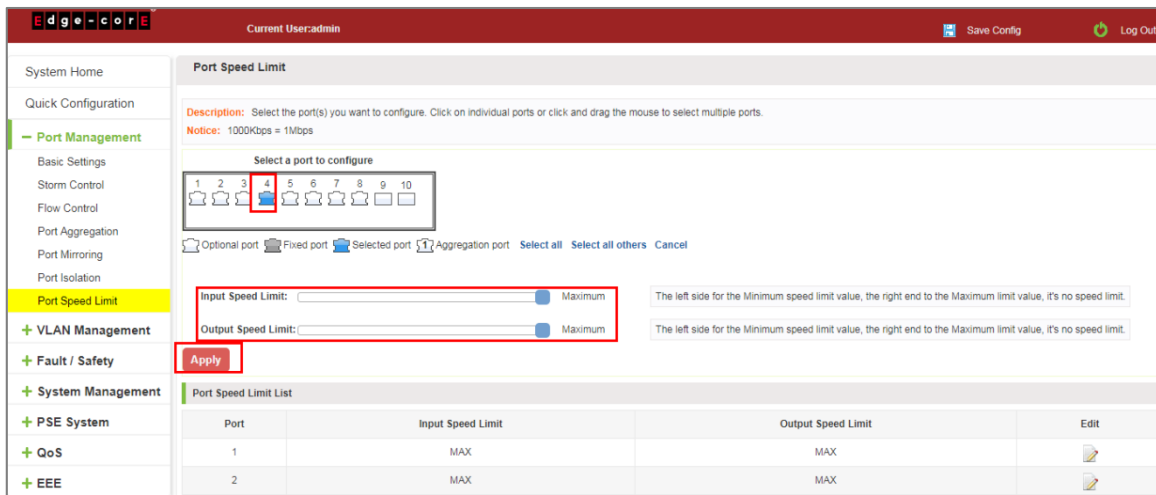
Figure 4-27: Port Speed Limits Configured

To configure Port Speed Limits:

- Step 1: Click the port icon or select multiple port icons;
- Step 2: Set the input and output speed limits for the port or ports selected;
- Step 3: Click Apply button.

### 4.7.3 Removing the port speed limits

Select the port or ports to remove the speed limits from. Slide the Input and Output speed limit controls all the way to the right and then click Apply.



**Figure 4-28: Removing the Port Speed Limits**

To remove port speed limits:

Step 1: In the port list click on the port's icon under the Edit column.

Step 2: Slide the input and output speed limit controls all the way to the right.

Step 3: Click Apply.

## 5 VLAN MANAGEMENT

### 5.1 VLAN MANAGEMENT

#### 5.1.1 Showing the VLAN configuration

Click "VLAN Management" "VLAN Management" to view the VLAN settings:

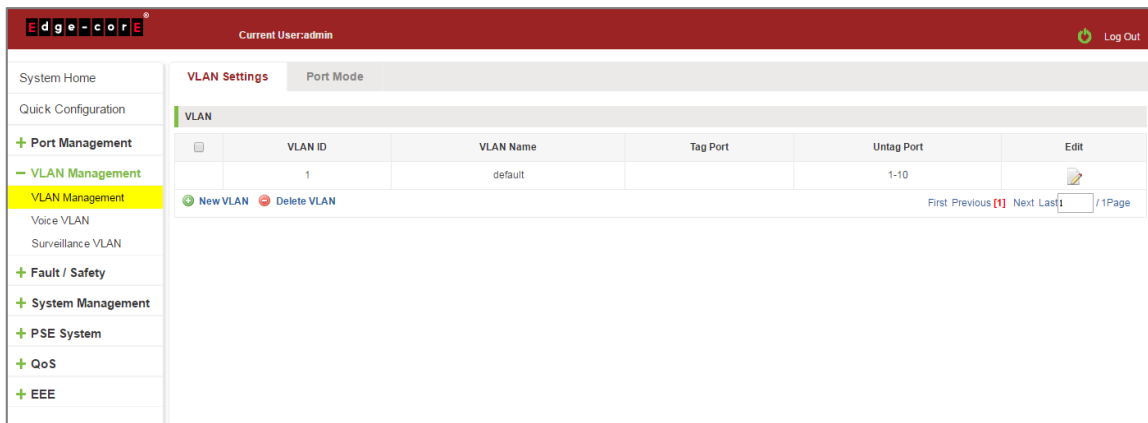


Figure 5-1: VLAN Configuration Information

VLAN Settings Tab: shows the currently configured VLANs. The fields are:

- **VLAN ID:** The VLAN ID that identifies the particular VLAN.
- **VLAN Name:** The configured name of the VLAN.
- **VLAN IP address:** Displays the switch's management IP;
- **Tag Port:** The VLAN's port members that are set to tag the MAC layer with VLAN tags.
- **Untag Port:** Ports that are members of the VLAN – no tagging.

By default, all ports belong to VLAN 1.

## 5.1.2 Adding a VLAN

Click the New VLAN button to add a new VLAN.

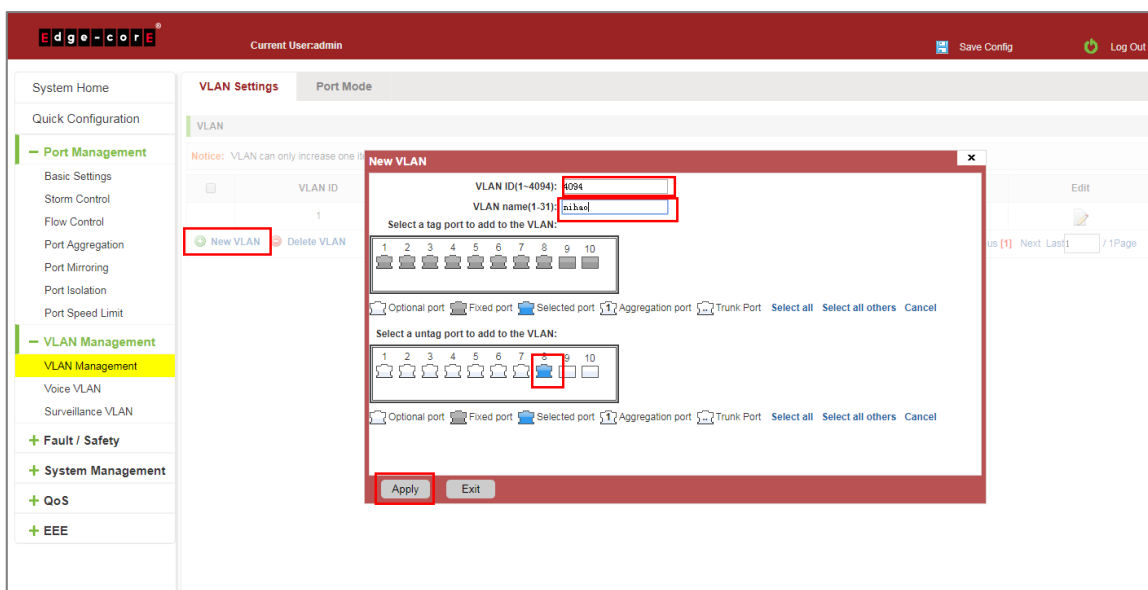


Figure 5-2: Adding a VLAN

To add a VLAN:

Step 1: Click New VLAN.

Step 2: Input a VLAN ID (1 to 4094) and a VLAN name (1 to 31 characters).

Step 3: Select the ports to add as members of the VLAN

Step 4: Click Apply.

## 5.1.3 Removing VLAN

### 5.1.3.1 Single VLAN delete

To delete a single VLAN all the port members must be deleted first. Once the VLAN has no port members click the red X on the far right side of the VLAN list to delete the VLAN.

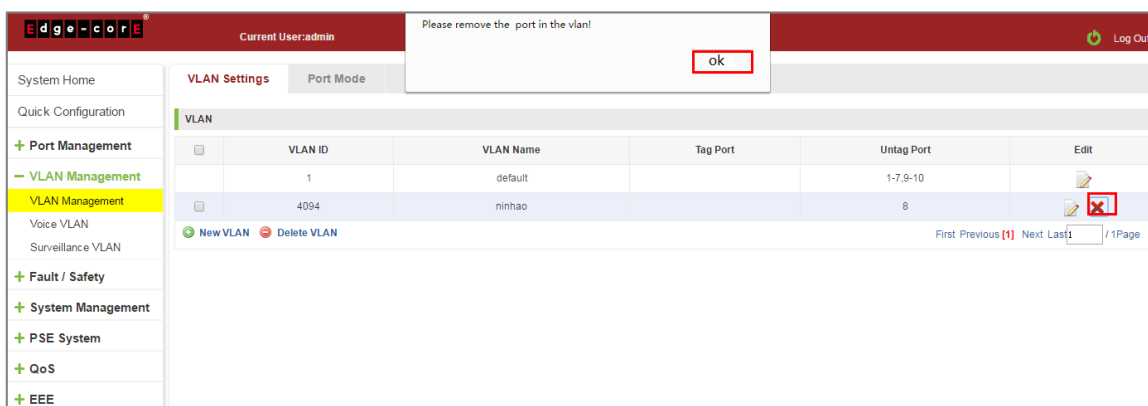


Figure 5-5-3: Deleting a Single VLAN

### 5.1.3.2 Deleting multiple VLANs

In the VLAN list check the checkbox next to the VLANs to be deleted in the box(s) on the left. Click the Delete VLAN button to delete the selected VLAN(s). Note that any VLANs that still have member ports will not be deleted.

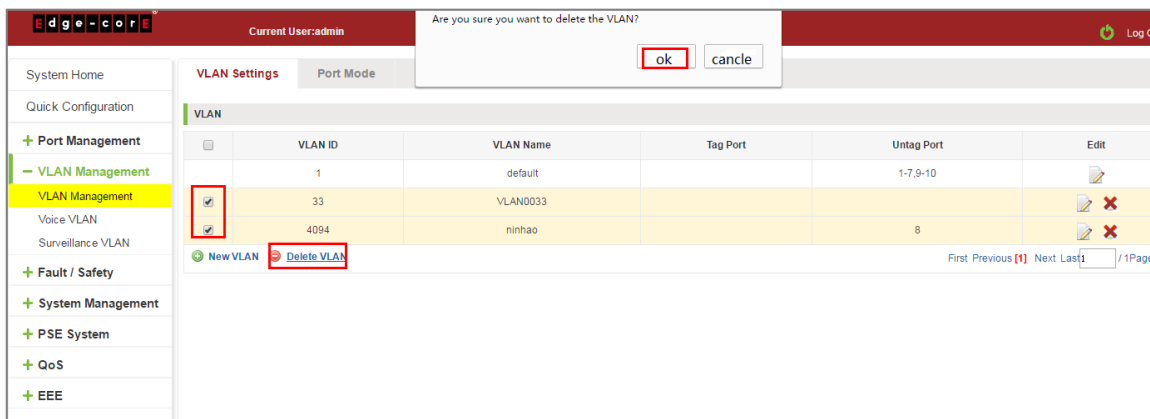


Figure 5-4: Deleting Multiple VLAN

To delete multiple VLANs:

Step 1: Check the checkbox next to the VLAN ID in the VLAN list. (you can check multiple VLANs if needed)

Step 2: Click the Delete VLAN button.

Step 3: Click OK in the confirmation window to delete the VLAN(s).

### 5.1.4 Editing a VLAN

#### 5.1.4.1 Adding a port(s) to a VLAN

In the edit VLAN window click on the port panel view ports to select them as members of the VLAN.

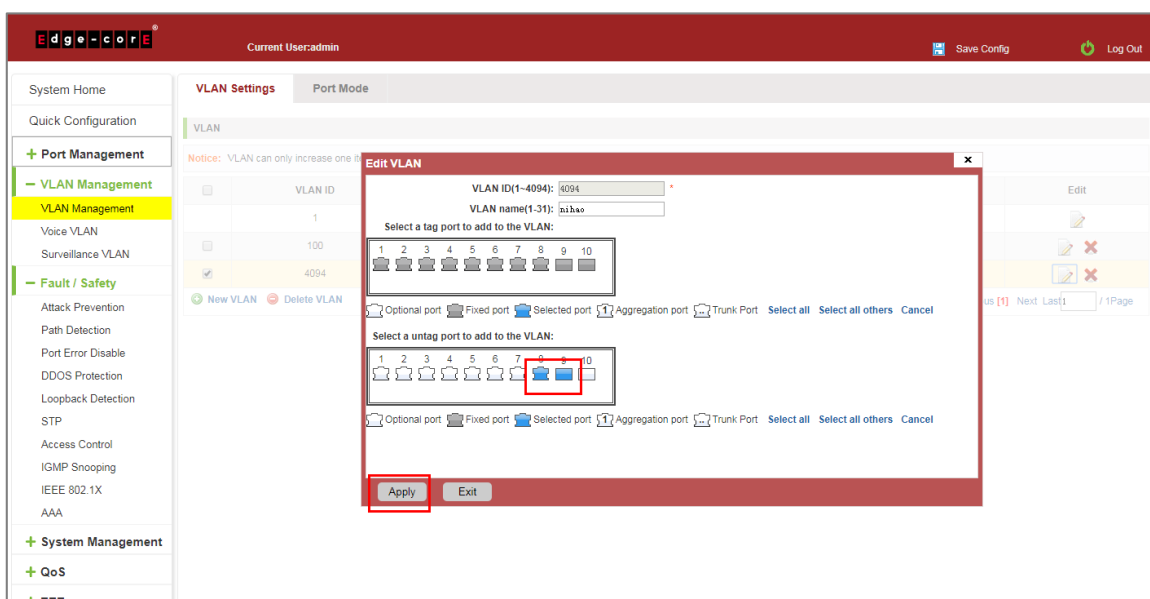



Figure 5-5: Adding a Port(s) to a VLAN

To add a port(s) to a VLAN:

Step 1: Click  icon under the edit column in the VLAN list view.

Step 2: In the port panel windows select the tagged or untagged ports to add to the VLAN.

Step 3: Click Apply.

### 5.1.4.2 Removing a port(s) from a VLAN

In the Edit VLAN window click on the existing port members to deselect them from the VLAN and then click the Apply button.

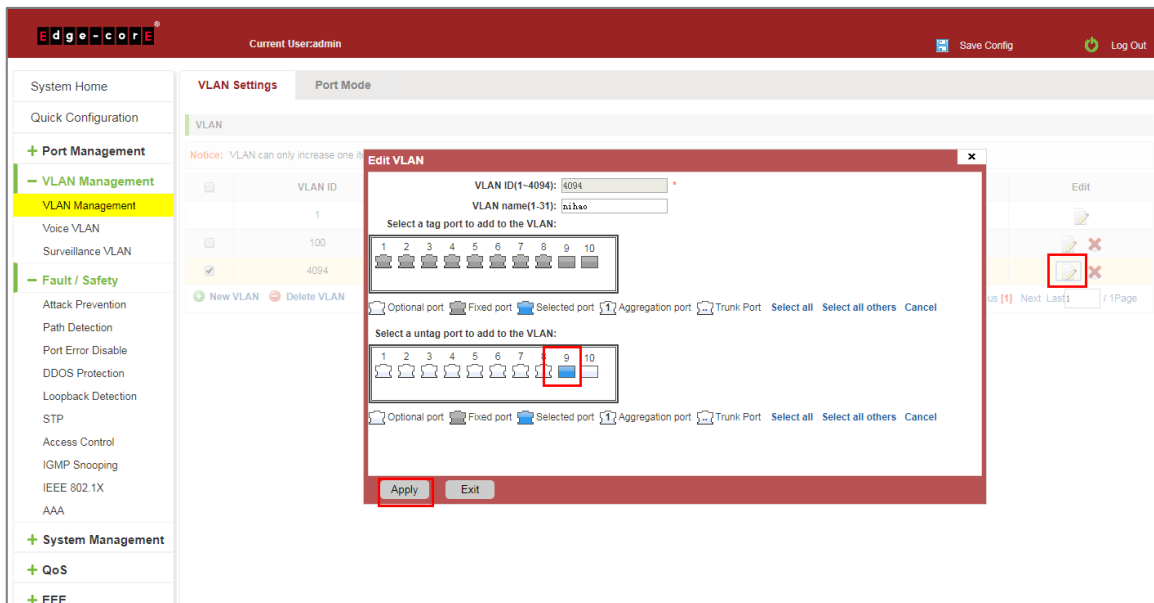



Figure 5-6: Removing a Port(s) from a VLAN

To remove a port(s) from a VLAN:

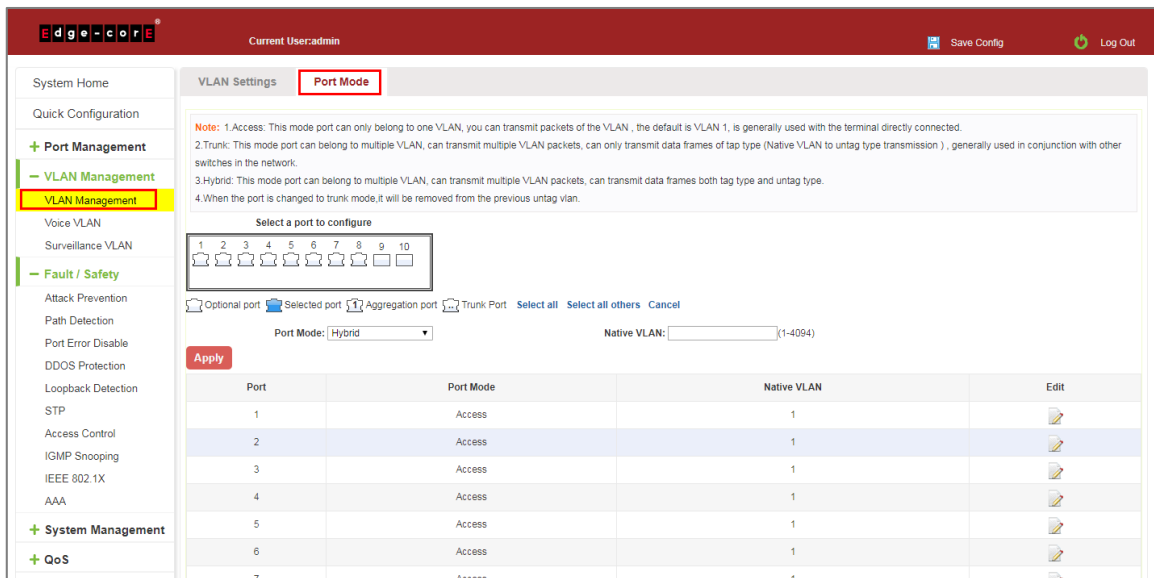
Step 1: Click the  icon.

Step 2: Click the untagged or tagged ports to deselect them from the VLAN.

Step 3: Click Apply.

### 5.1.5 Viewing the VLAN port mode

Click [Port Management - VLAN Management- Port Mode](#) to view the configured VLAN port mode.



**Figure 5-7: Viewing the VLAN Port Mode**

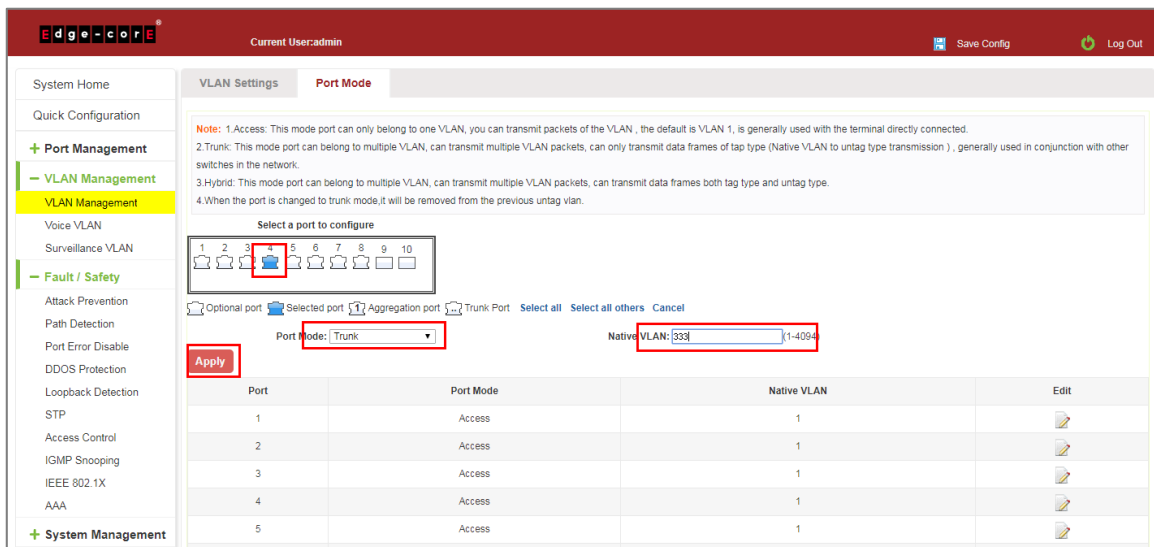
The following is displayed in the Port Mode list:

- Port Number
- The Native VLAN the port is a member of.
- Port Mode (Trunk, Hybrid or Access)

The default setting for all ports: Native VLAN set to 1 and Port Mode set to Access.

### 5.1.6 Changing the port mode to trunk

Select the port and click the Port Mode drop down menu and set it to Trunk, then click Apply.



**Figure 5-8: Change the Port Mode is Trunk**

Setting the Port Mode steps:

Step 1: Select one or more ports in the port panel.

Step 2: Click the Port Mode drop down menu and change the mode to: Trunk.



Step 3: Set the Native VLAN; the VLAN ID must be configured.

Step 4: Click Apply.

### 5.1.7 Changing the port mode to hybrid

Select the port and click the Port Mode drop down menu setting it to Hybrid, then click Apply

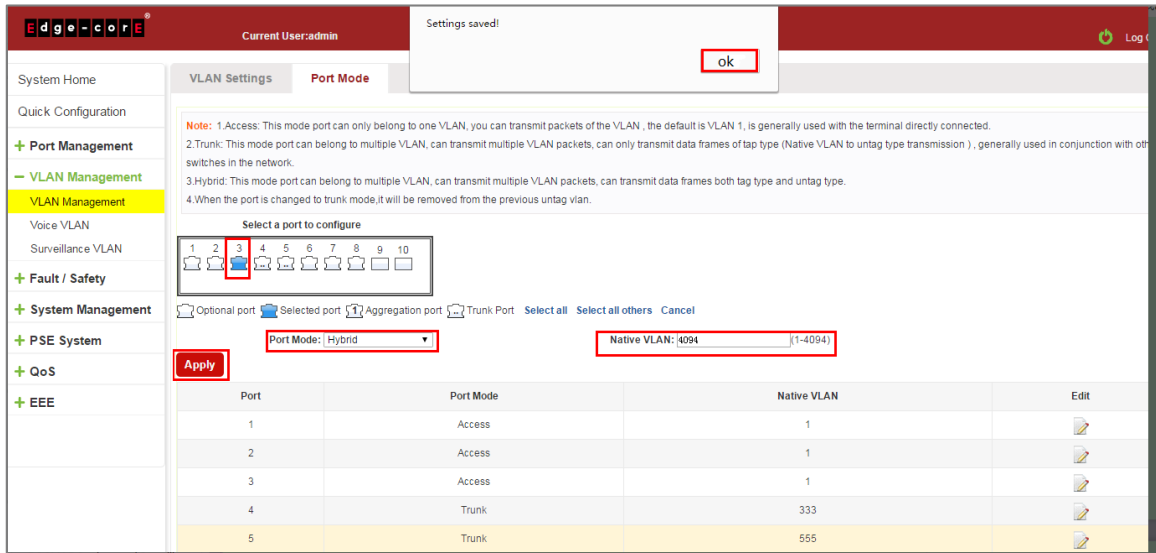


Figure 5-9: Change the Port Mode is Hybrid

To set the Port Mode as hybrid:

Step 1: Select one or more ports in the port panel.

Step 2: Click the port mode list and change the mode to: Hybrid.

Step 3: Set the Native VLAN; the VLAN ID must be configured.

Step 4: Click Apply.

## 5.2 VOICE VLAN

### 5.2.1 View voice VLAN information

Click "VLAN Management" "Voice VLAN" "Voice VLAN Global" to view the switch voice VLAN configuration.

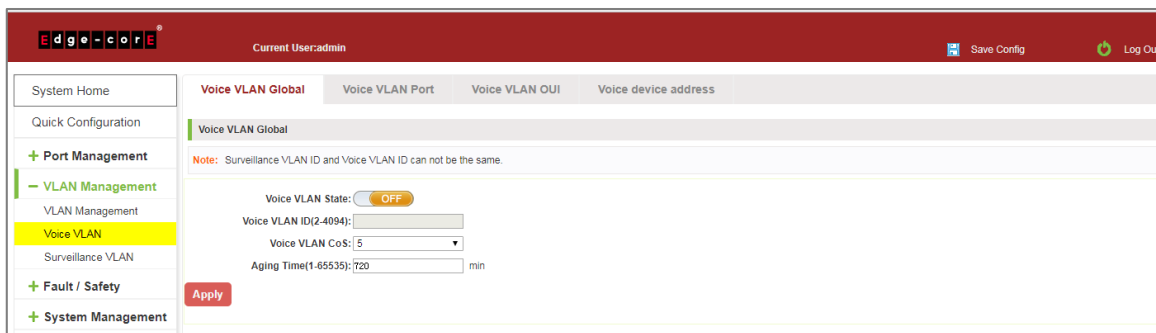


Figure 5-10: View Voice VLAN Information

## 5.2.2 Configure voice VLAN global

Click "VLAN Management" "Voice VLAN" "Voice VLAN Global" to configure the voice VLAN.

The screenshot displays the Edge-core network management interface. The top header shows the logo and the current user as 'admin'. The left sidebar contains a navigation menu with categories like 'Port Management', 'VLAN Management', 'Fault / Safety', 'System Management', 'PSE System Management', 'Qos', and 'EEE'. The 'Voice VLAN' option under 'VLAN Management' is highlighted. The main content area shows the 'Voice VLAN Global' configuration page. It includes a note: 'Surveillance VLAN ID and Voice VLAN ID can not be the same.' Below the note, there are four configuration fields: 'Voice VLAN State' (a toggle switch set to 'ON'), 'Voice VLAN ID(2-4094)' (a text box containing '900'), 'Voice VLAN CoS' (a dropdown menu set to '6'), and 'Aging Time(1-65535)' (a text box containing '1000' with 'min' as a unit). A red box highlights these four fields. Below the fields is a red 'Apply' button.

Figure 5-11: View Voice VLAN Information

To configure the voice VLAN global:

Step 1: Next to Voice VLAN State click the OFF slider to ON.

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

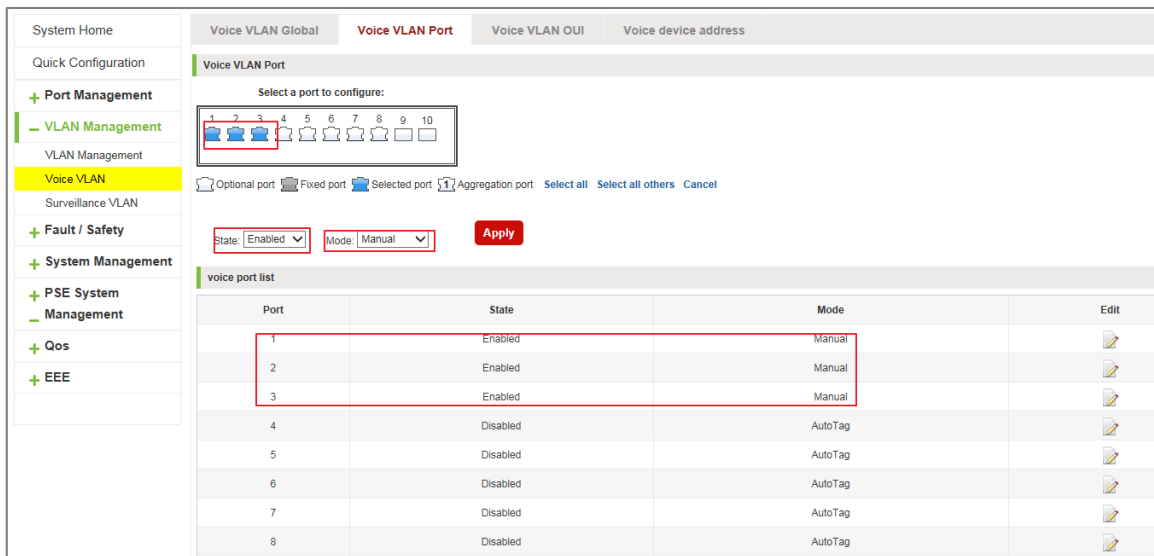
Step 3: In the voice VLAN CoS text box, choose 6;

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

Step 5: Click Apply.

## 5.2.3 Configuring a voice VLAN port

Click "VLAN Management" "Voice VLAN" "Voice VLAN port" to configure a voice VLAN port;



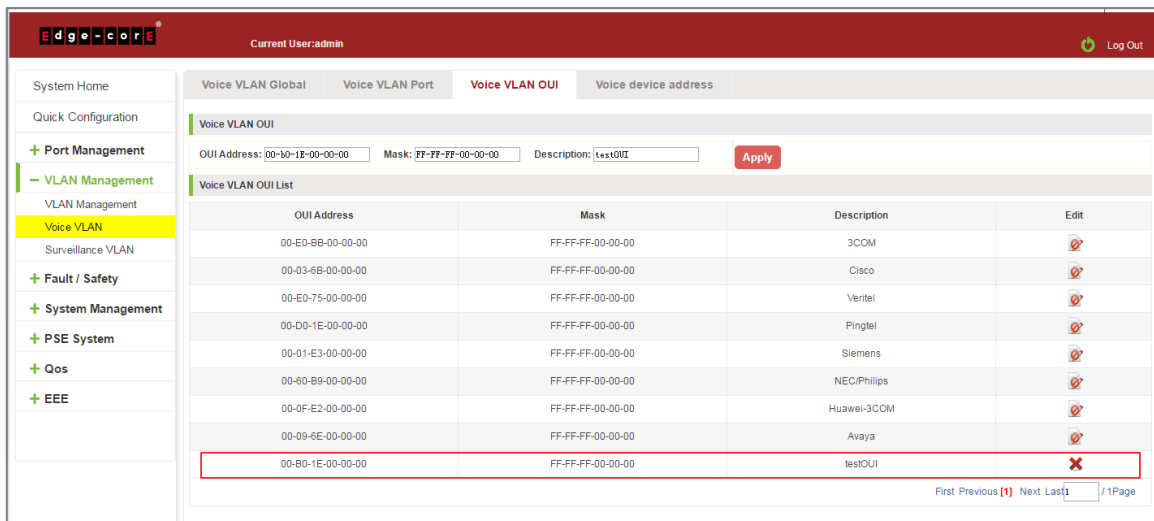
**Figure 5-12: Configure Voice VLAN Port**

To configure a voice VLAN port(s):

- 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 "VLAN Management" "Voice VLAN" "Voice VLAN OUI" to configure a voice VLAN OUI.



**Figure 5-13: Configure Voice VLAN OUI**

To configure a voice VLAN OUI:

- 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 "VLAN Management" "Voice VLAN" "Voice Device Address" to view the Voice Device Address.

The screenshot shows the Edgeworks network management interface. The top navigation bar includes the Edgeworks logo, the user name 'Current User:admin', and a 'Log Out' button. The main content area is divided into a sidebar and a main panel. The sidebar contains a tree view with categories: System Home, Quick Configuration, Port Management, VLAN Management (expanded), Voice VLAN (highlighted), Surveillance VLAN, Fault / Safety, System Management, PSE System, and Qos. The main panel has tabs for 'Voice VLAN Global', 'Voice VLAN Port', 'Voice VLAN OUI', and 'Voice device address'. The 'Voice device address' tab is active, displaying a table titled 'Voice device address List'. The table has three columns: 'Port', 'Voice Device Address', and 'Start Time'. A single row is visible with the following data: Port: 3, Voice Device Address: 0060.1E00.0010, Start Time: 2000-01-02 01:45:49. Below the table is a pagination control showing 'First Previous [1] Next Last 1 / 1 Page'.

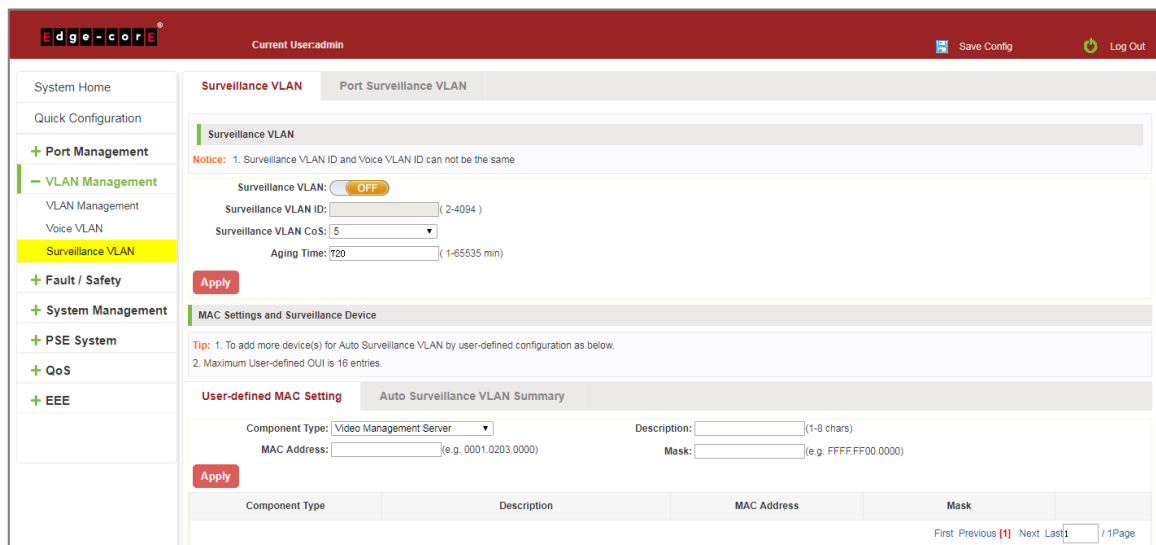
Port	Voice Device Address	Start Time
3	0060.1E00.0010	2000-01-02 01:45:49

Figure 5-14: Voice VLAN Address

## 5.3 SURVEILLANCE VLAN

### 5.3.1 Showing the surveillance VLAN information

Click "VLAN Management" "Surveillance VLAN" "Surveillance VLAN" to show the Surveillance VLAN information.

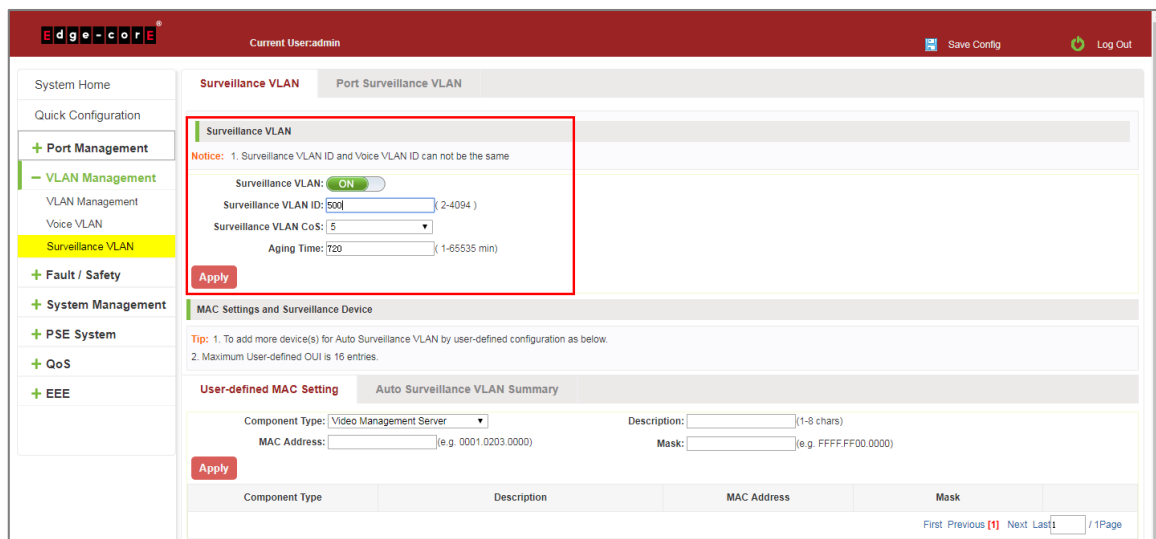


The screenshot displays the 'Surveillance VLAN' configuration page in the Edgeworks web interface. The page title is 'Surveillance VLAN' and the sub-tab is 'Port Surveillance VLAN'. The 'Surveillance VLAN' toggle is currently set to 'OFF'. The 'Surveillance VLAN ID' is set to 500, 'Surveillance VLAN CoS' is set to 5, and 'Aging Time' is set to 720 minutes. The 'User-defined MAC Setting' section is also visible, showing a dropdown for 'Component Type' set to 'Video Management Server'.

Figure 5-15: Showing the Surveillance VLAN Information

### 5.3.2 Configuring a surveillance VLAN

Click "VLAN Management" "Surveillance VLAN" "Surveillance VLAN" to configure a Surveillance VLAN.



The screenshot displays the 'Surveillance VLAN' configuration page in the Edgeworks web interface. The 'Surveillance VLAN' toggle is currently set to 'ON'. The 'Surveillance VLAN ID' is set to 500, 'Surveillance VLAN CoS' is set to 5, and 'Aging Time' is set to 720 minutes. The 'User-defined MAC Setting' section is also visible, showing a dropdown for 'Component Type' set to 'Video Management Server'.

Figure 5-16: Configure Surveillance VLAN

To configure a surveillance:

Step 1: In the surveillance VLAN TEXT BOX, click the ON/OFF" to "ON" (green).

Step 2: In the surveillance VLAN ID text box, enter an ID for the Surveillance VLAN for example, 500.

Step 3: In the Surveillance VLAN CoS text box, select for example, 3.

Step 4: In the aging time text box, enter the aging time in minutes (1 to 65535), for example, 500.

Step 5: Click Apply.

### 5.3.3 MAC settings and the surveillance devices

Click "VLAN Management" "Surveillance VLAN" "Surveillance VLAN" "MAC Settings and Surveillance Device" to configure the User-defined MAC settings.

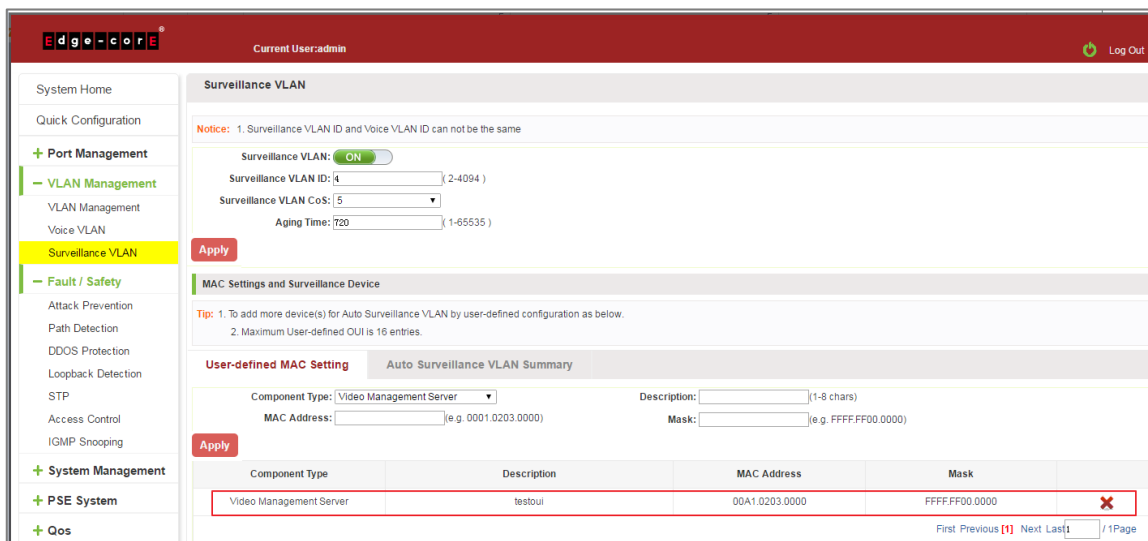


Figure 5-17: Configuring the User-defined MAC Settings

To configure the surveillance VLAN:

Step 1: From the component type drop down menu, choose video management server;

Step 2: In the description text box, enter type "testOUI" without the quotation marks.

Step 3: In the MAC address text box, enter the required MAC address, for example 00A1.0203.0000.

Step 4: In the mask text box, enter the required mask, for example FFFF F000 000.

Step 5: Click Apply.

## 6 FAULT/SAFETY

### 6.1 ATTACK PREVENTION

#### 6.1.1 ARP snooping

##### 6.1.1.1 Showing the ARP Inspection configuration

Click "Fault/Safety" "Attack Prevention" "ARP Inspection" to view the ARP Inspection configuration, this feature is turned off by default.

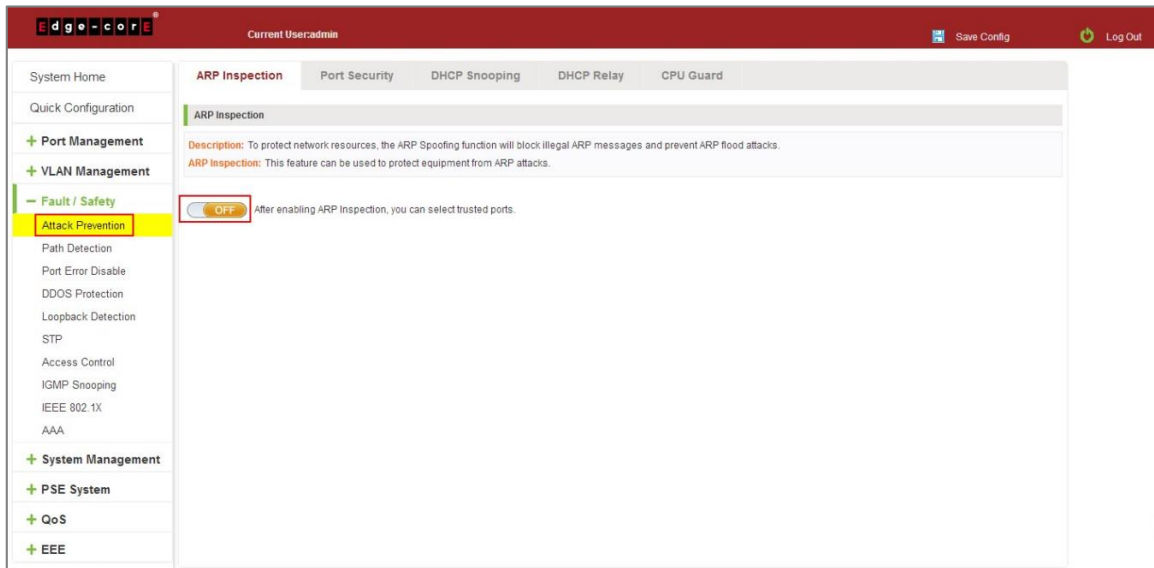


Figure 6-1: Showing the Port ARP Inspection configuration

##### 6.1.1.2 ARP inspection function

In the ARP Inspection configuration, click the ON/Off switch to enable this function and then select a port to apply the ARP inspection. Select the ARP inspection parameters in the fields below the Port window and then click Apply.

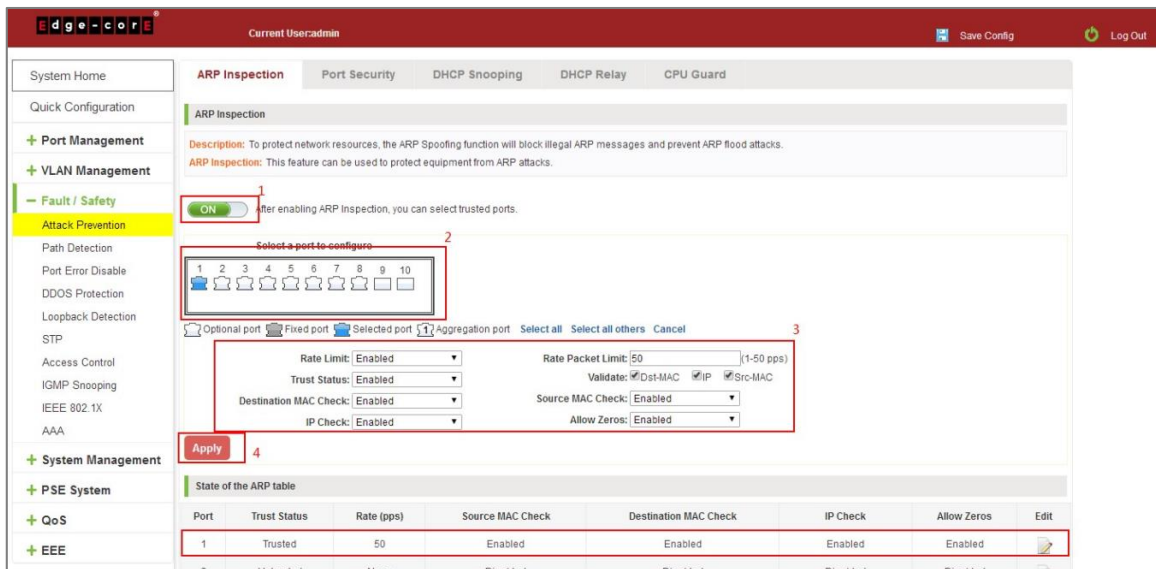


Figure 6-2: Configuring ARP Inspection

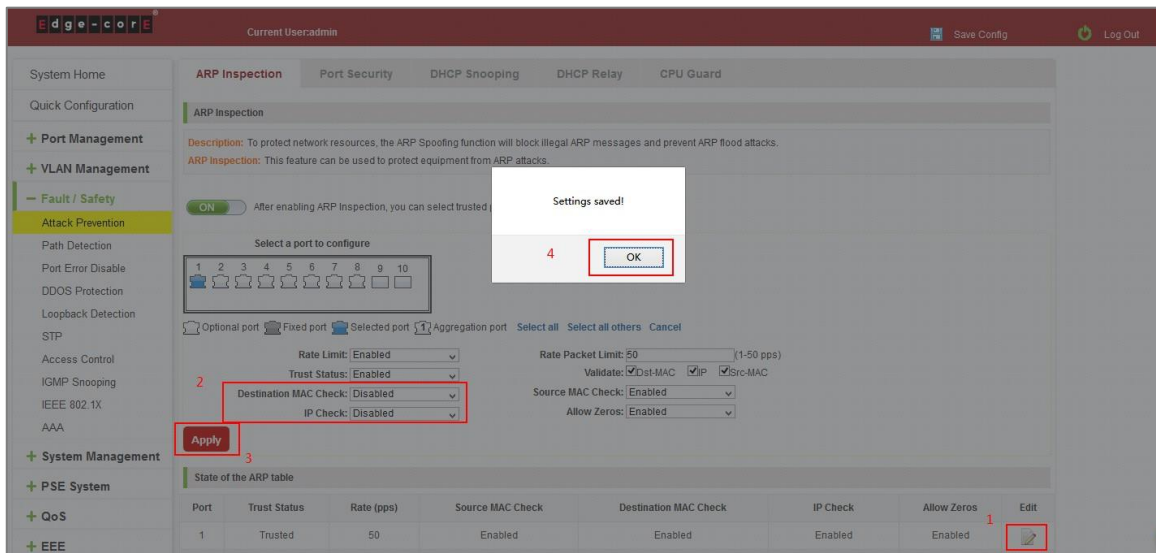


Figure 6-3: Saving the ARP Inspection configuration

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Trusted	50	Enabled	Disabled	Enabled	Enabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
4	Untrusted	None	Disabled	Disabled	Disabled	Disabled	

Figure 6-4: Successful configuration of ARP Inspection

### 6.1.1.3 Disabling ARP Inspection

In the ARP Inspection configuration table (State of the ARP table), click the edit icon. In the ARP inspection configuration panel click the ON/OFF button to the OFF position. Click OK in the confirmation window to disable ARP Inspection from the associated port.



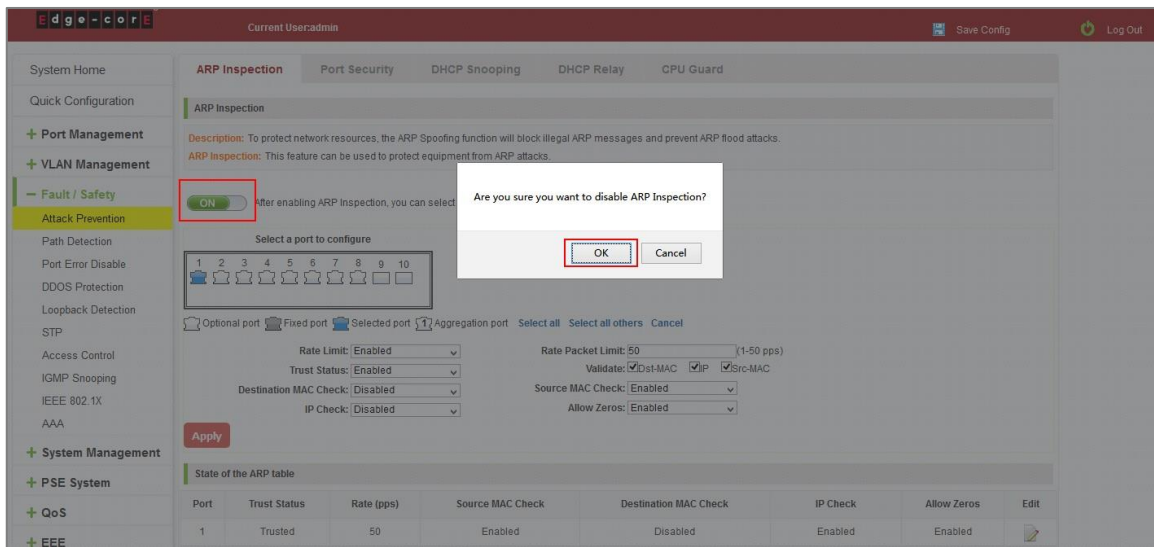


Figure 6-5: Disabling ARP Inspection

## 6.1.2 Port security

### 6.1.2.1 Configuring port security

To configure port security click "Fault/Safety" "Attack prevention" "Port Security".

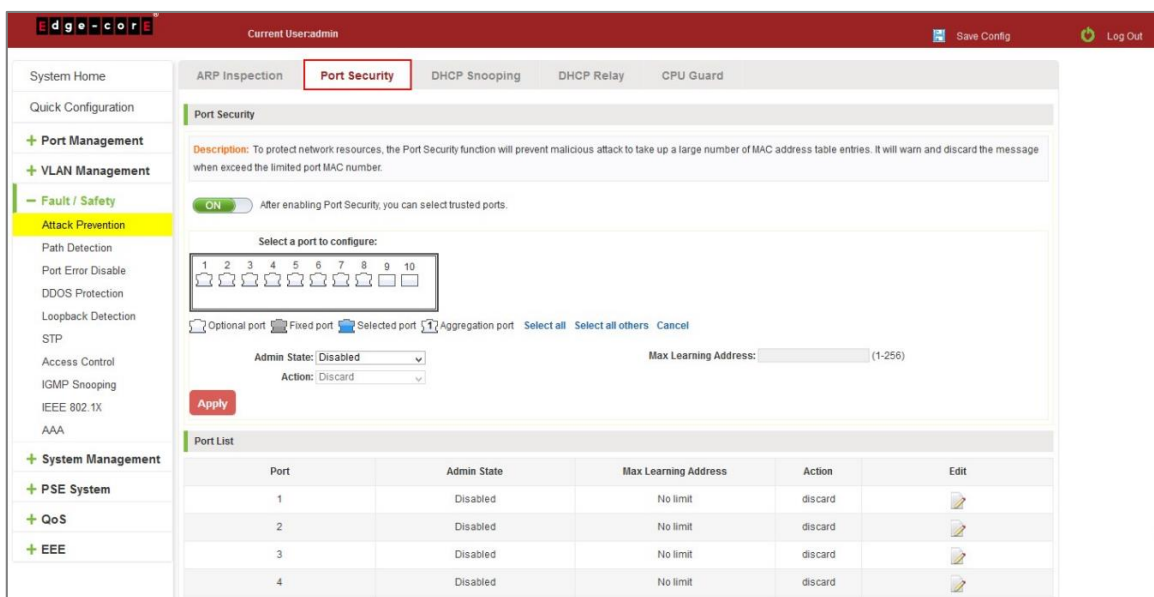


Figure 6-6: Configuring port security

In the configuration page, select one or more ports, enable the admin state, configure the port max learning address (1 to 256) and click Apply.

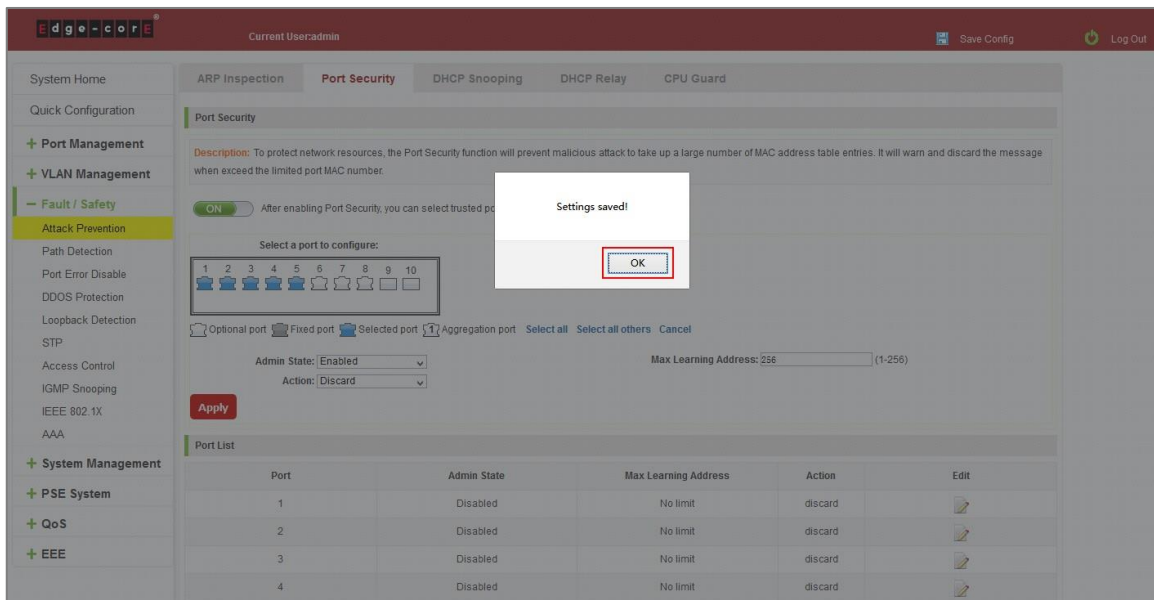


Figure 6-7: Port Security Manual Configuration

### 6.1.2.2 Modifying port security

In the port list, select the port to edit and change the configured security parameters for the port (for example, disabling the port security Admin State) and click Apply.

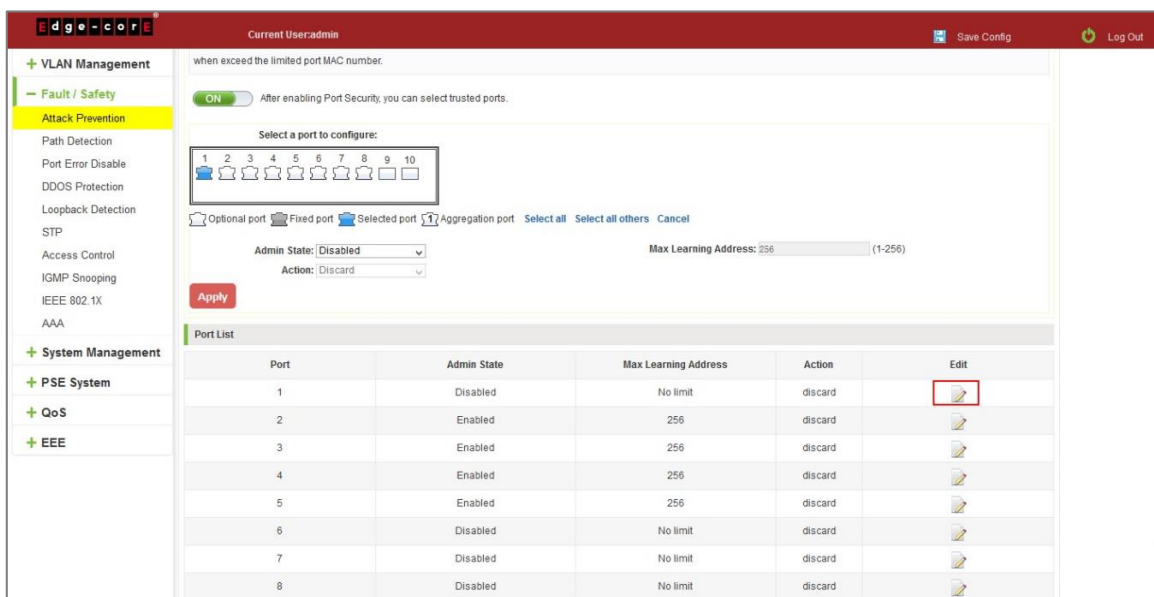


Figure 6-8: Modifying the port security configuration

## 6.1.3 DHCP snooping

### 6.1.3.1 Viewing DHCP snooping configuration

To show the DHCP snooping configuration click "Fault/Safety" "Attack Prevention" "DHCP Snooping". DHCP Snooping is used to detect and prevent rogue DHCP servers from offering IP addresses to the network clients.

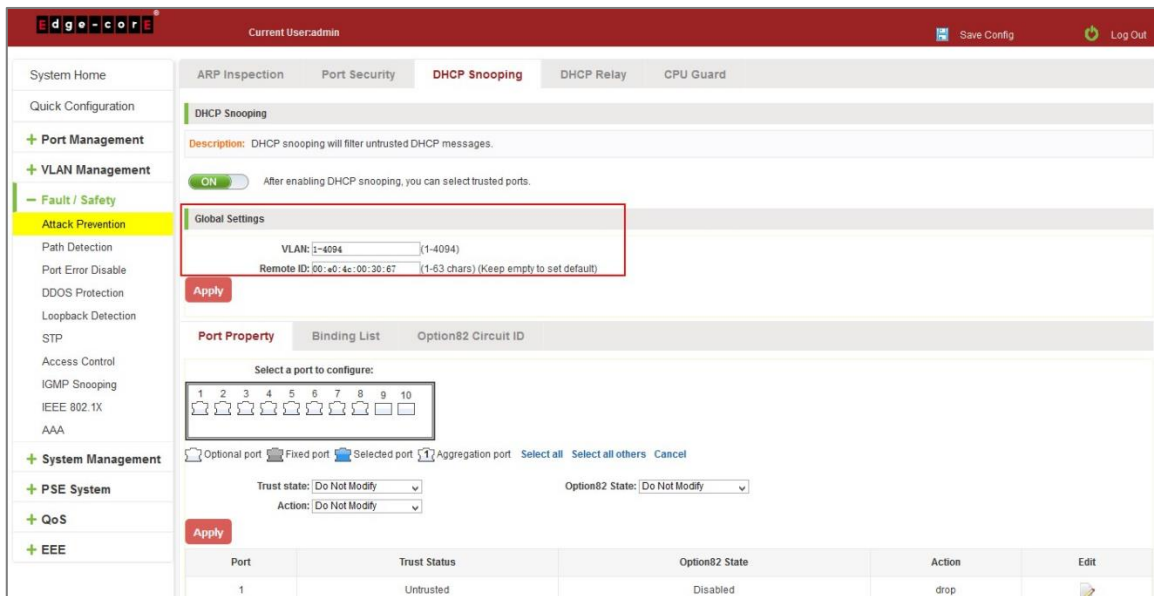


Figure 6-9: Viewing DHCP Snooping Configuration

### 6.1.3.2 Enabling DHCP snooping

Click "Fault/Safety" "Attack Prevention" "DHCP Snooping" "Port Property" and then click the ON/OFF slider to turn on DHCP snooping.

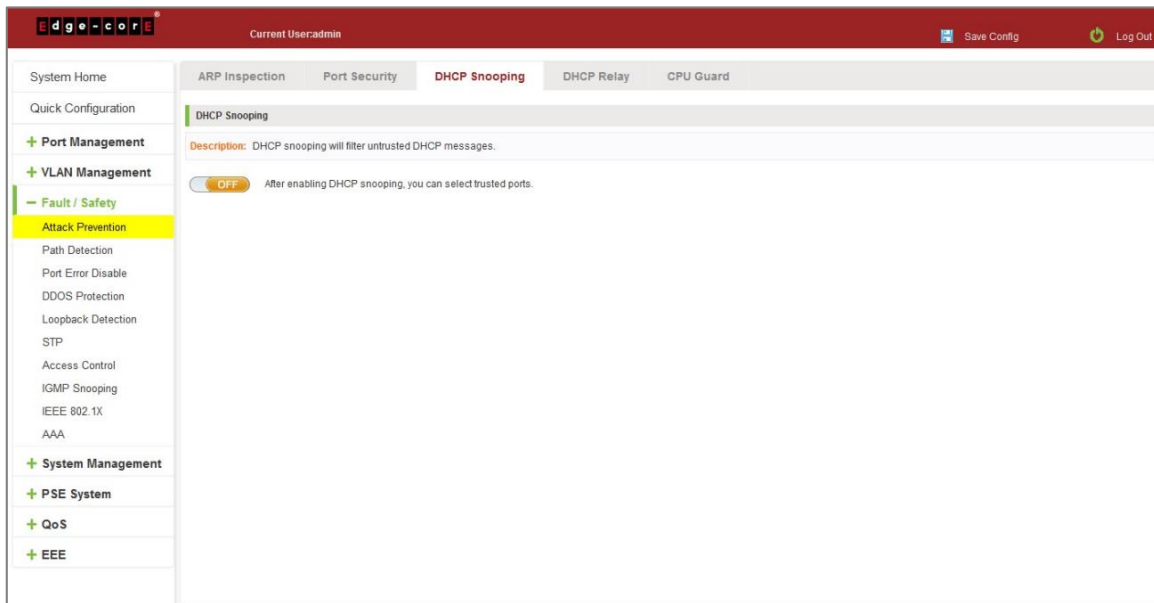
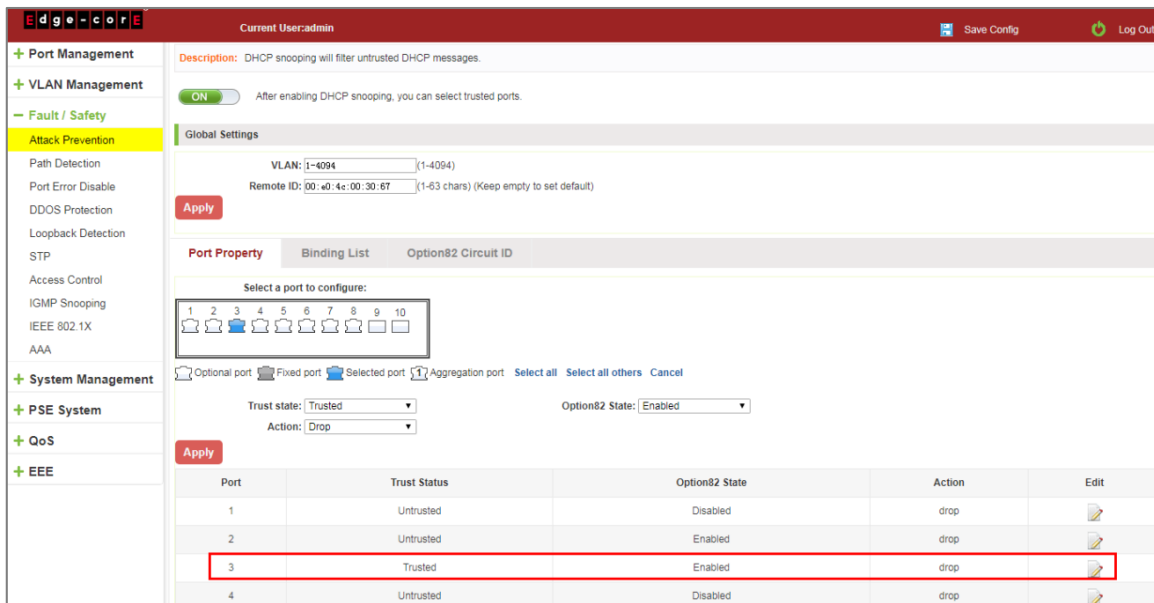


Figure 6-10: Enabling DHCP Snooping

### 6.1.3.3 Configuring DHCP snooping trusted ports

Select the ports to be trusted and change the Trust state to Trusted, enable option82 and the Action parameter and then click Apply.



**Figure 6-11: Disabling Rogue DHCP Server Functions on a DHCP Port and Enabling Option 82**

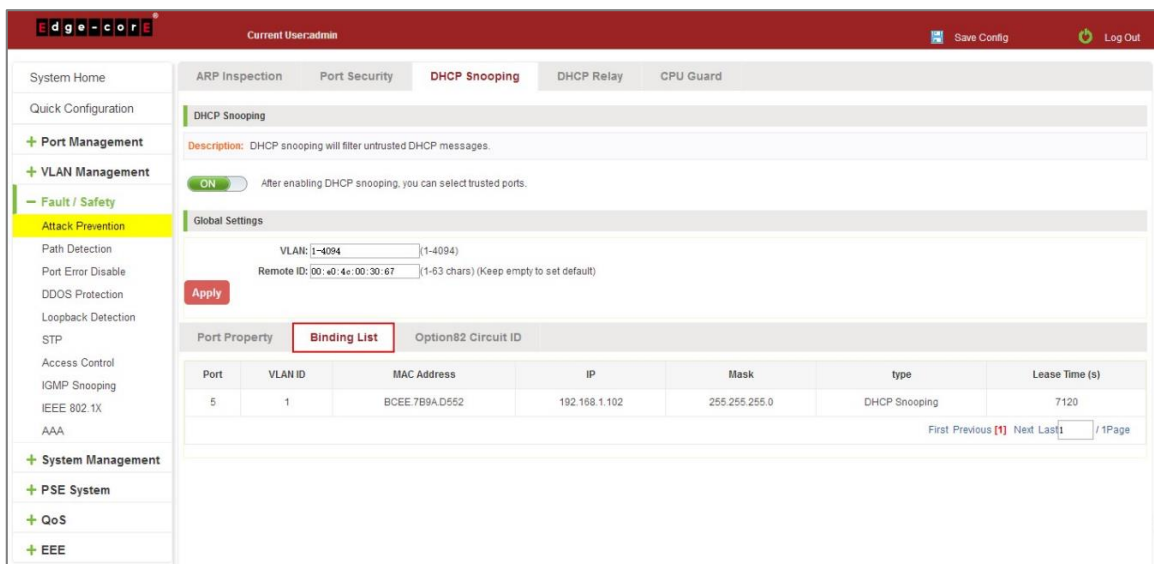
When a DHCP server is connected to an access port set the Trust Status in DHCP Snooping to Trusted.

Access ports not hosting a valid DHCP server should have their Trust Status set to Untrusted.

Configure Option82 if your DHCP server supports the option to restrict the number of IP addresses that can be assigned to the port.

#### 6.1.3.4 Viewing the DHCP Snooping Binding Table

Click the Binding List tab to view a list of the IP addresses assigned to a port.



**Figure 6-12: Viewing the Binding List of a Port.**

#### 6.1.3.5 Configuring Option82 CID information

Click the Option82 Circuit ID tab to configure the CID information.

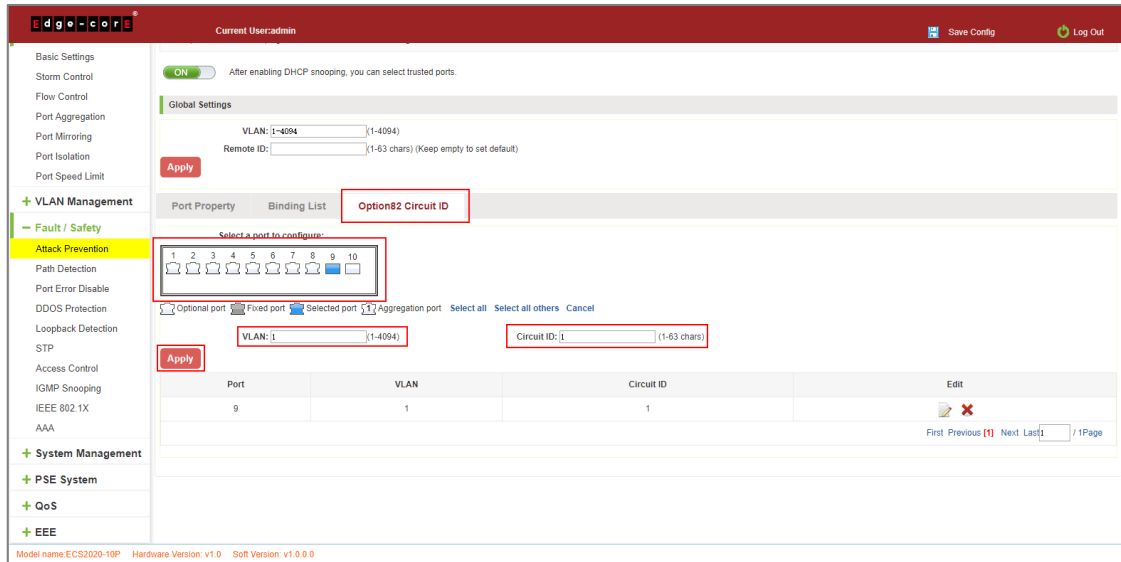


Figure 6-13: CID Information

### 6.1.3.6 Disabling the DHCP snooping function

On the DHCP Snooping Page under Attack Prevention click the ON/OFF slider and click OK in the confirmation window. The sliding switch should now display OFF.

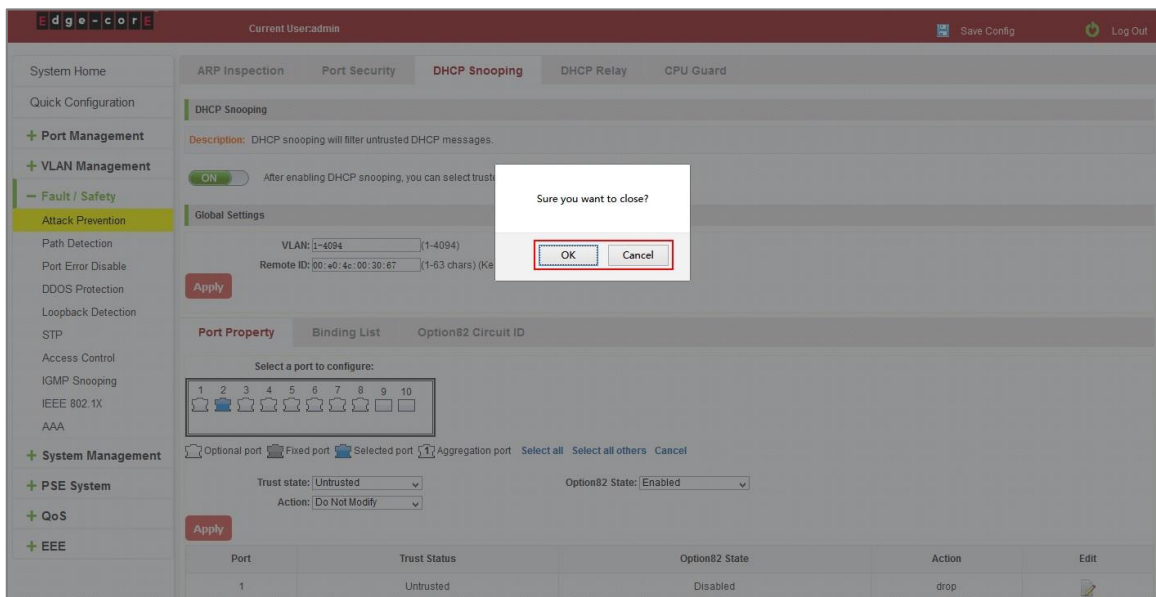


Figure 6-14: Disabling DHCP Snooping

### 6.1.4 CPU Guard

Click "Fault/Safety" "Attack prevention" "CPU Guard" to view the CPU guard settings.

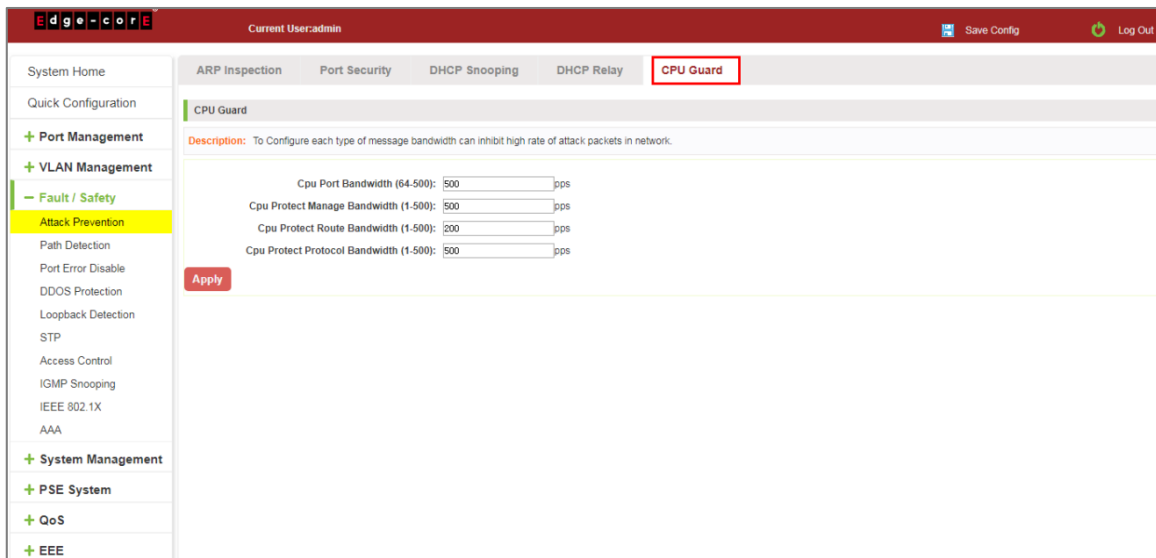


Figure 6-15: Viewing the CPU Guard Configuration

### 6.1.4.1 Modifying the CPU guard configuration

Set the packet per second rate for each of the traffic types and then click Apply.

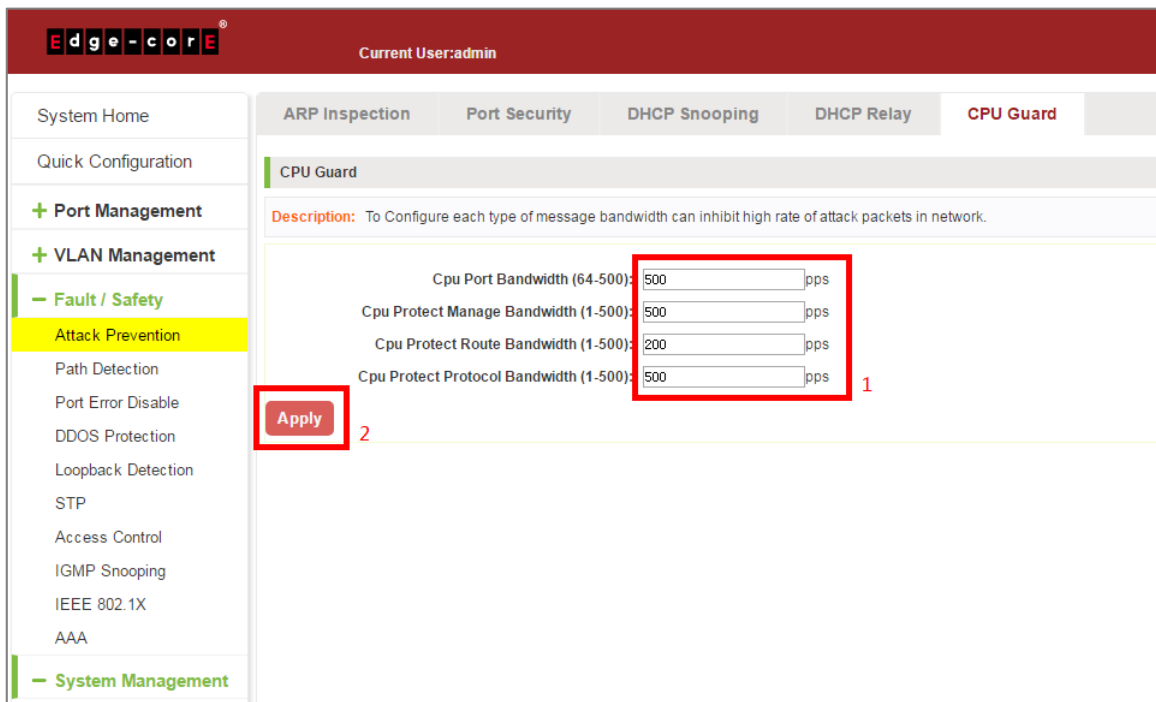


Figure 6-16: Modifying the CPU Guard Configuration

## 6.2 PATH DETECTION

### 6.2.1 Path/Tracert detection

Click "Fault/Safety" "Path Detection" "Ping Detection" or "Tracert Detection" to send pings to specified hosts or trace the network route to a specified host.

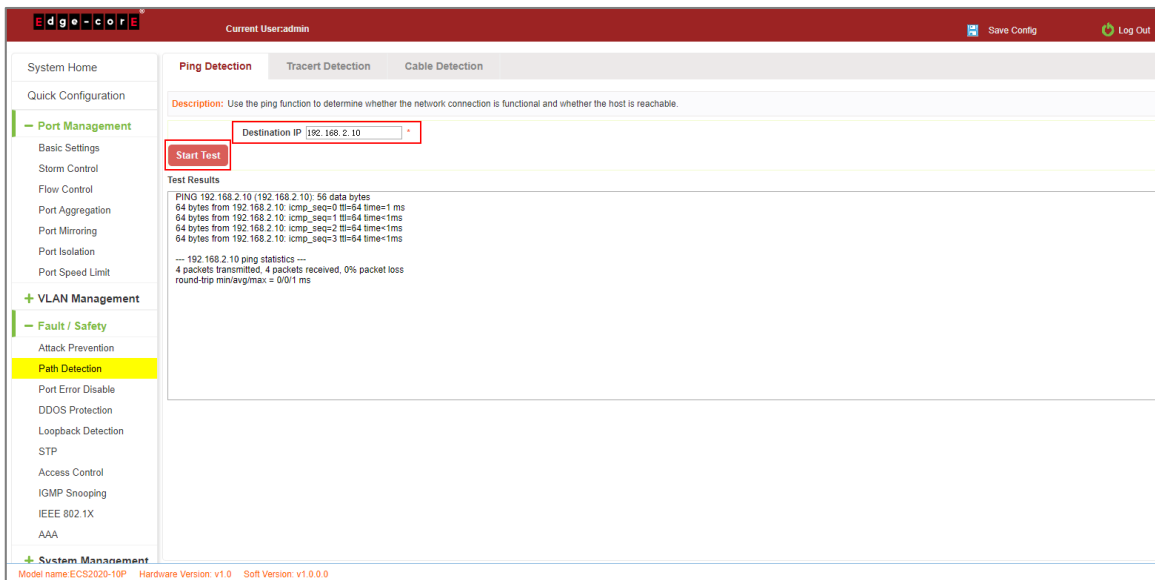


Figure 6-17: Ping Testing

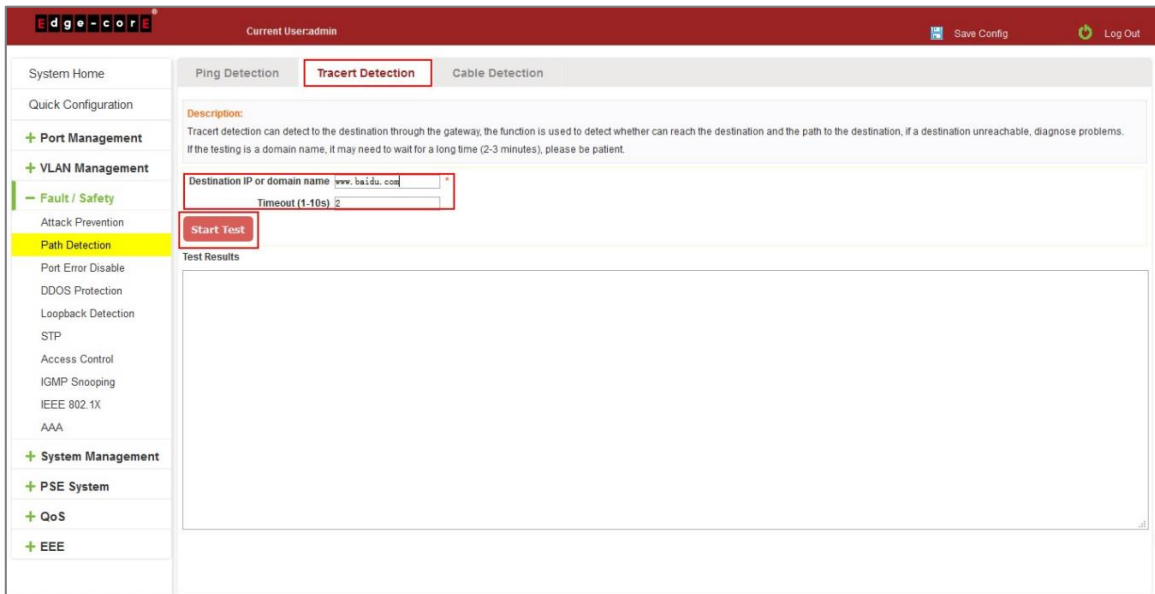


Figure 6-18: Trace Route Test

## 6.2.2 Cable detection

Click "Fault/Safety" "Path Detection" "Cable Detection" to view Cable Detection tests:

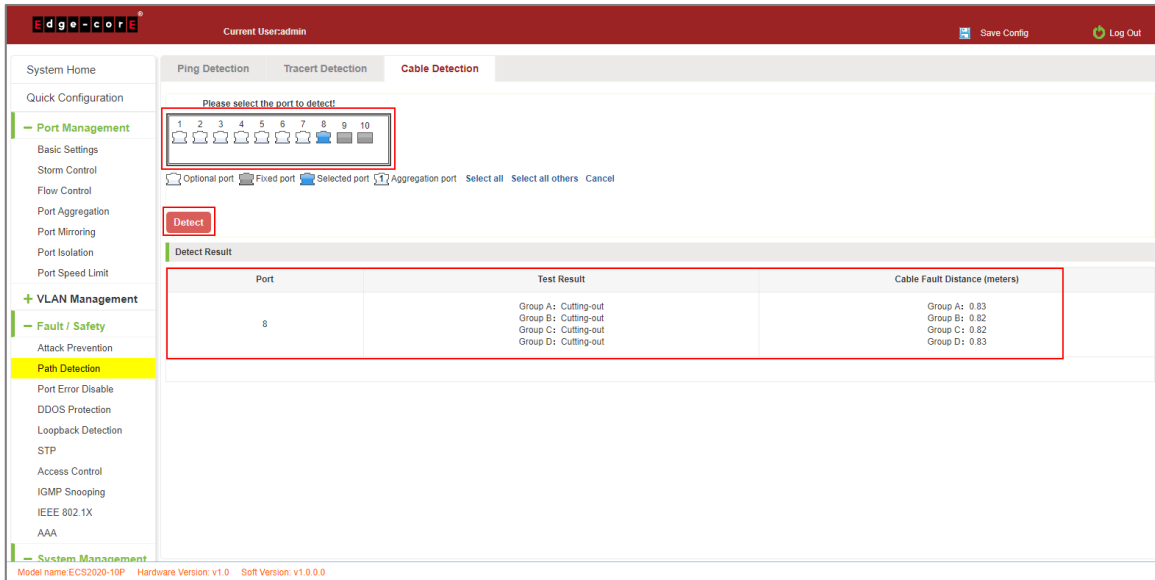


Figure 6-19: Cable Detection Test

Only one cable (port) can be selected for the test and then click the Detect button.

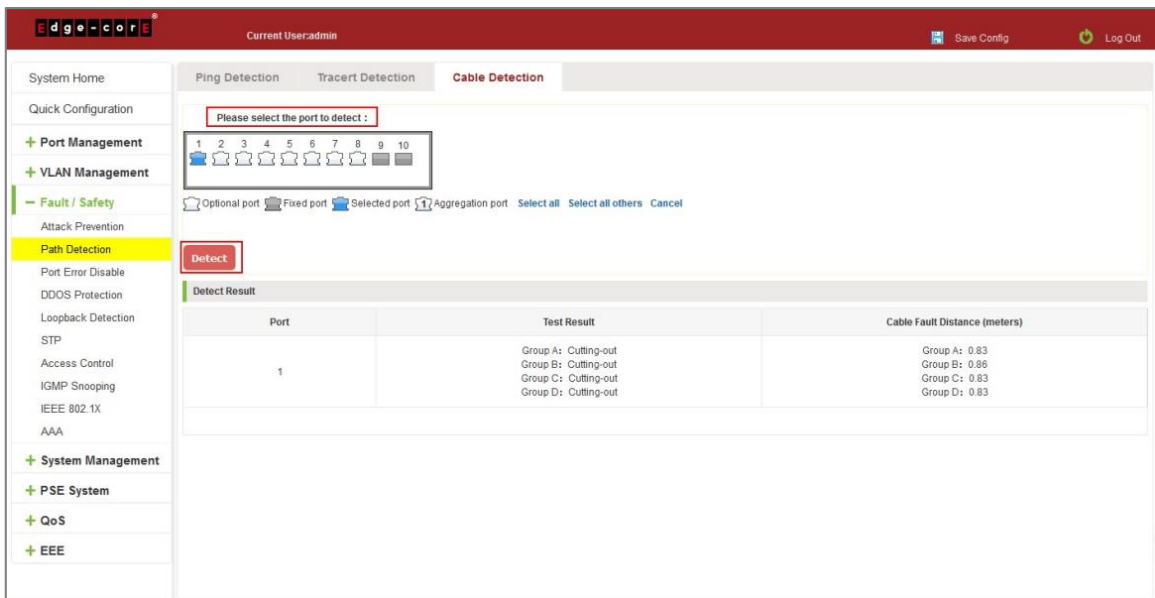


Figure 6-20: Port Cable Detection Test Result

### 6.3 PORT ERROR DISABLE

Use "Fault Safety" "Port Error Disable" to collect port disable information and set the port auto recovery time.



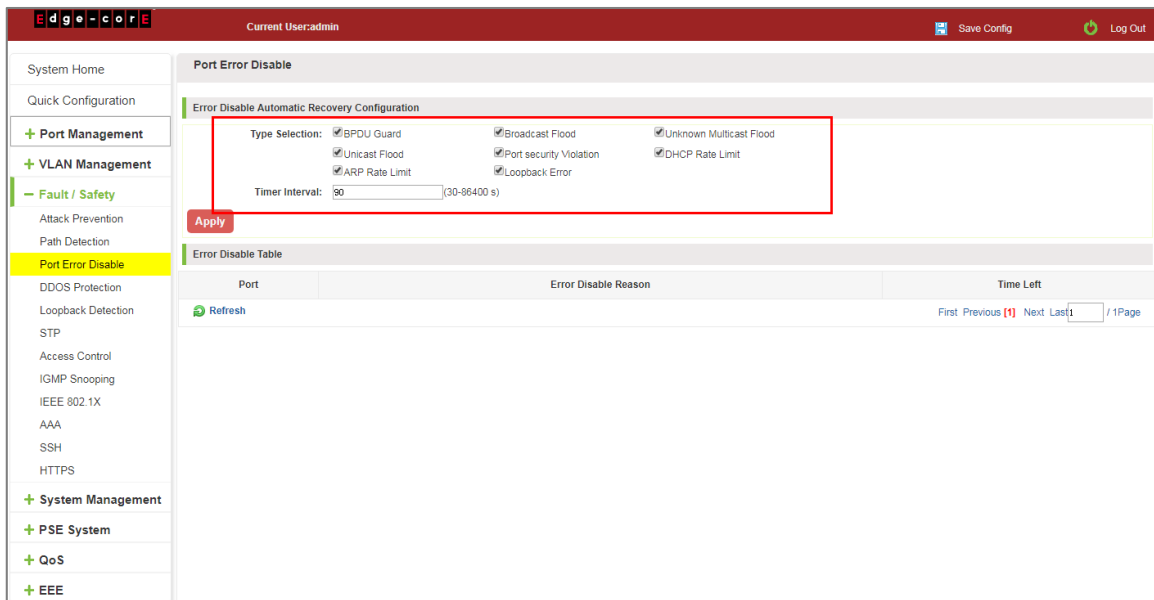


Figure 6-21: Configuring Error Disable Automatic Recovery

## 6.4 DDOS PROTECTION

Click "Fault/Safety" "DDOS Protection" to view DDOS protection configuration.

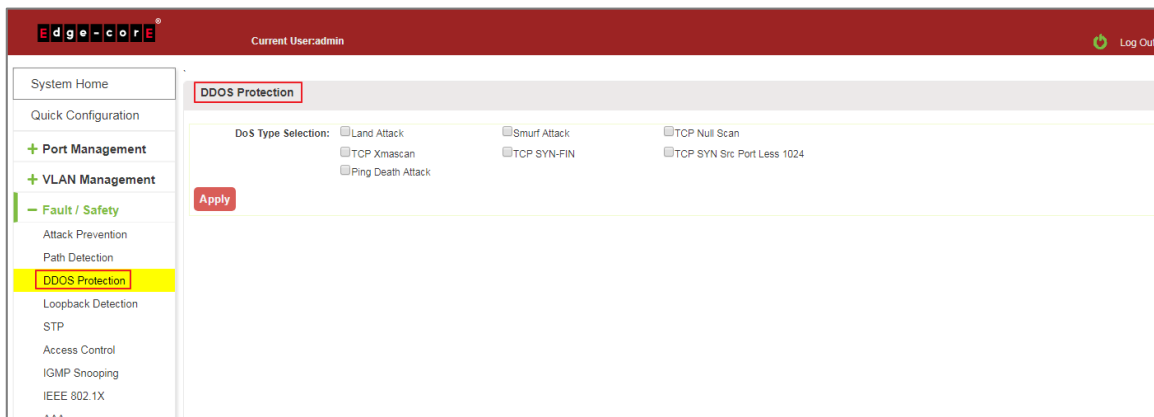


Figure 6-22: Configuring DDOS Protection

To prevent different types of DoS attacks from multiple computers select the DoS type(s) to configure and then click Apply.

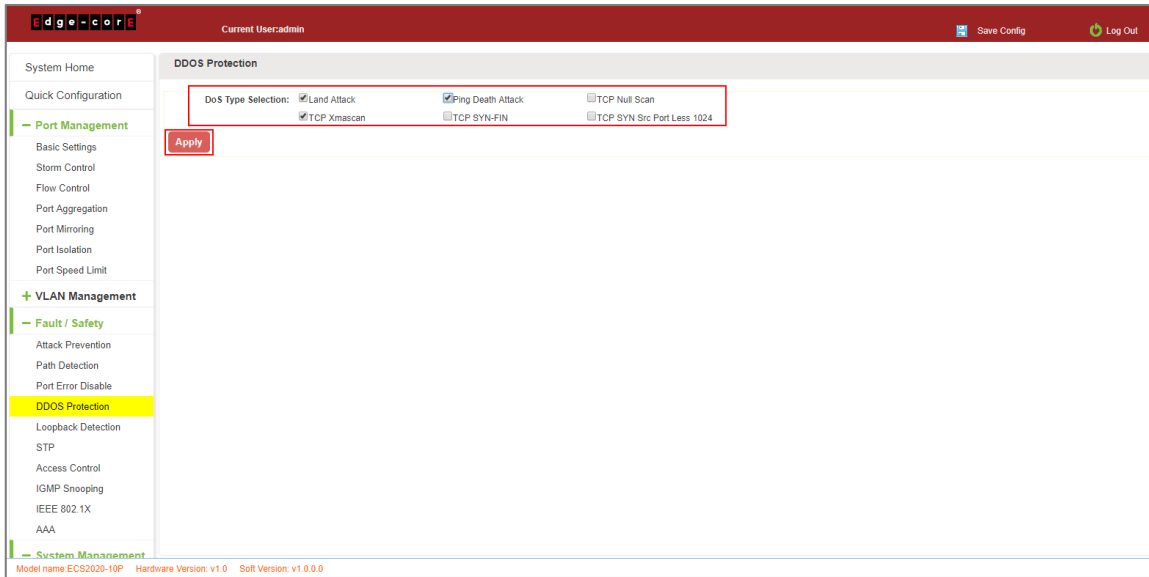


Figure 6-23: Selecting the DoS Types to Prevent

## 6.5 LOOP DETECTION

Click "Fault/Safety" "Loop Detection" to view the current loopback detection configuration.

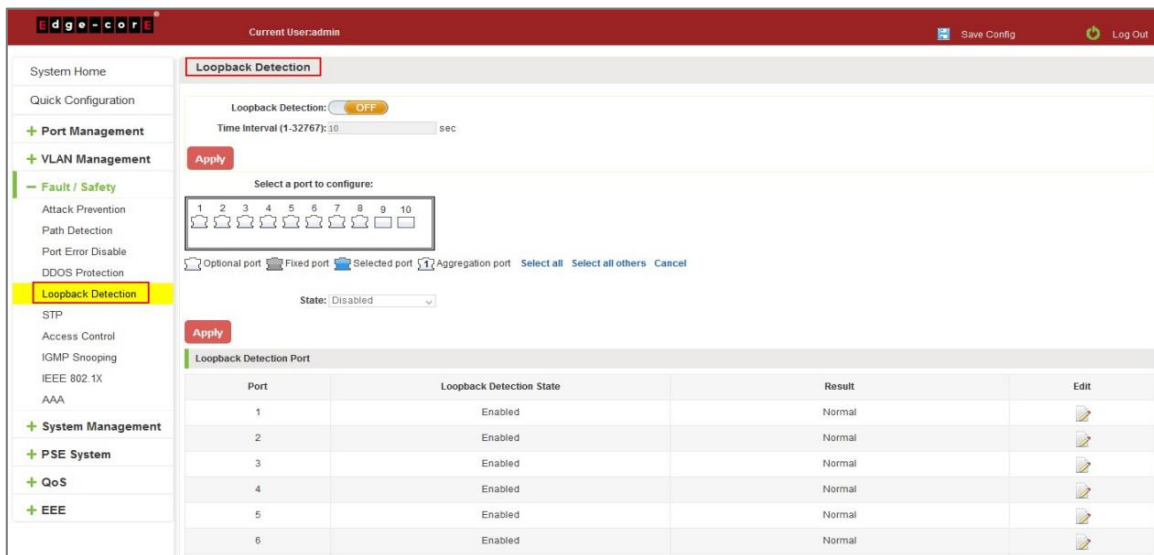


Figure 6-24: Viewing Loopback Detection Configuration

### 6.5.1 Enabling loopback detection

Click the ON/OFF slider to ON and then configure the time interval (1 to 32767 seconds) between sending loopback detection packets and click Apply. Select the ports to enable loopback detection on, then change the State to Enable and click Apply.

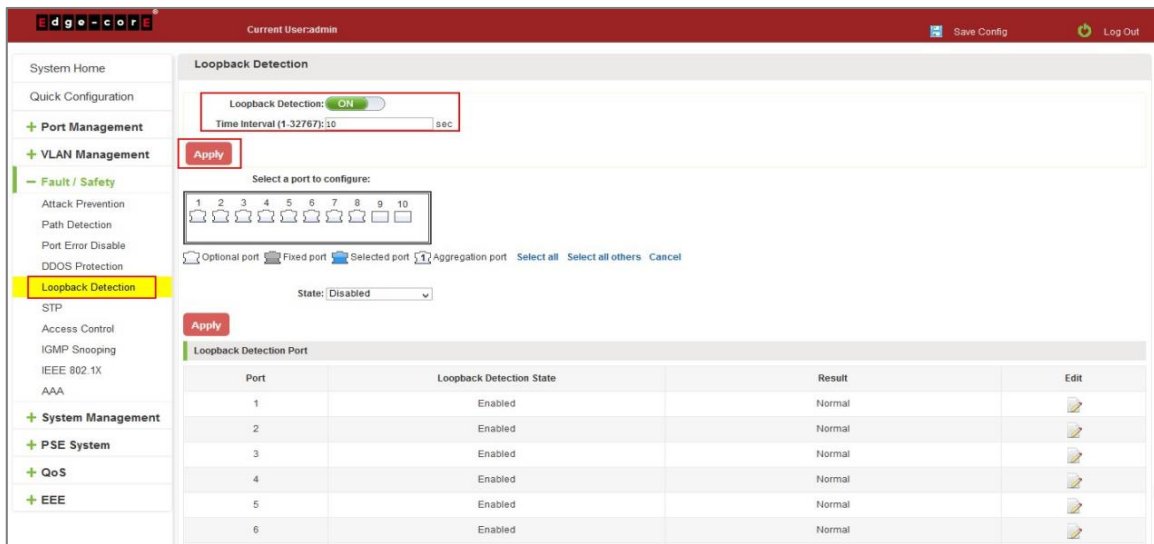


Figure 6-25: Enabling Loopback Detection

## 6.5.2 Enabling/Disabling loopback detection on specified ports

In the port panel select one or more ports to enable or disable the loopback detection state. Change the state to disabled or enabled in the State drop down menu and click Apply.

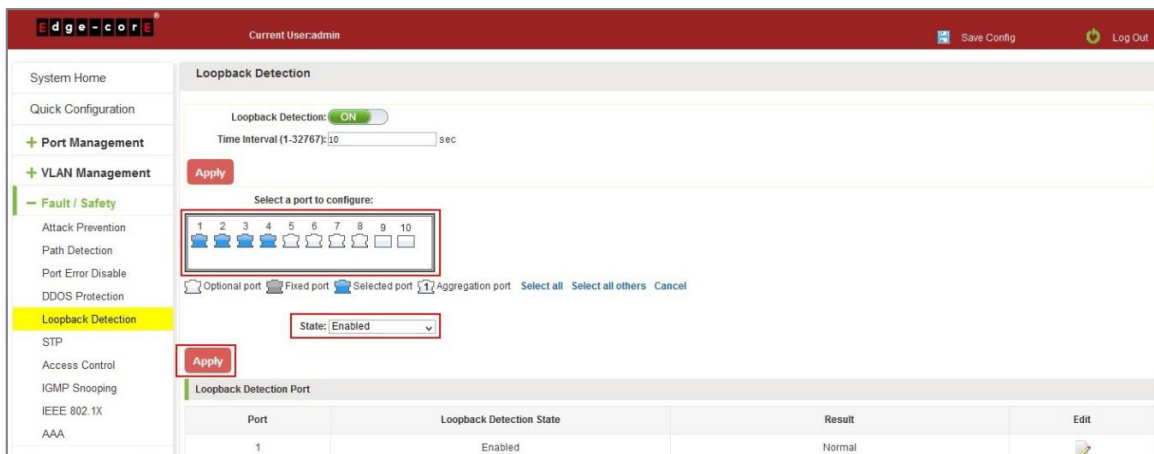


Figure 6-26: Configuring Ports Parameter

To edit ports individually click the "Edit" icon in the edit column of the Loopback Detection Port list. Then change the port state to either enabled or disabled.

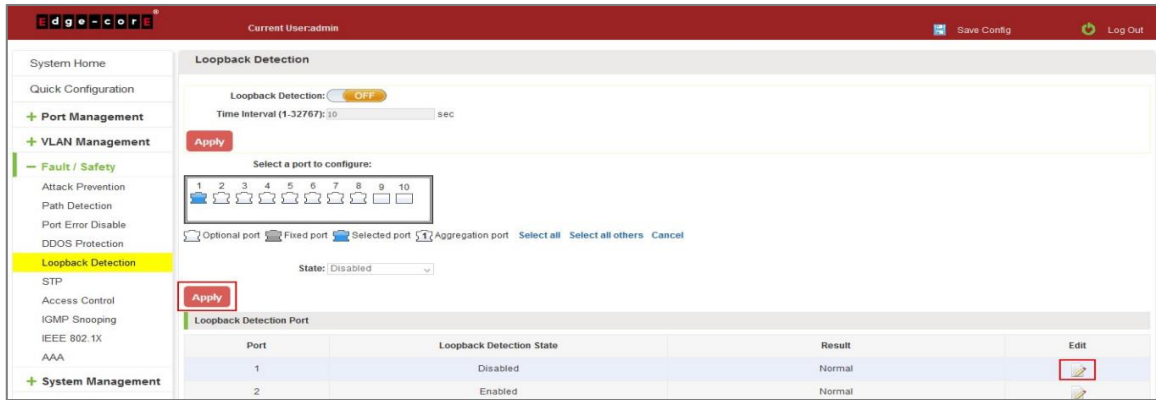


Figure 6-27: Editing Port Loopback Detection

## 6.6 STP

Click "Fault/Safety" "STP" "STP Global" to view the STP global configuration.

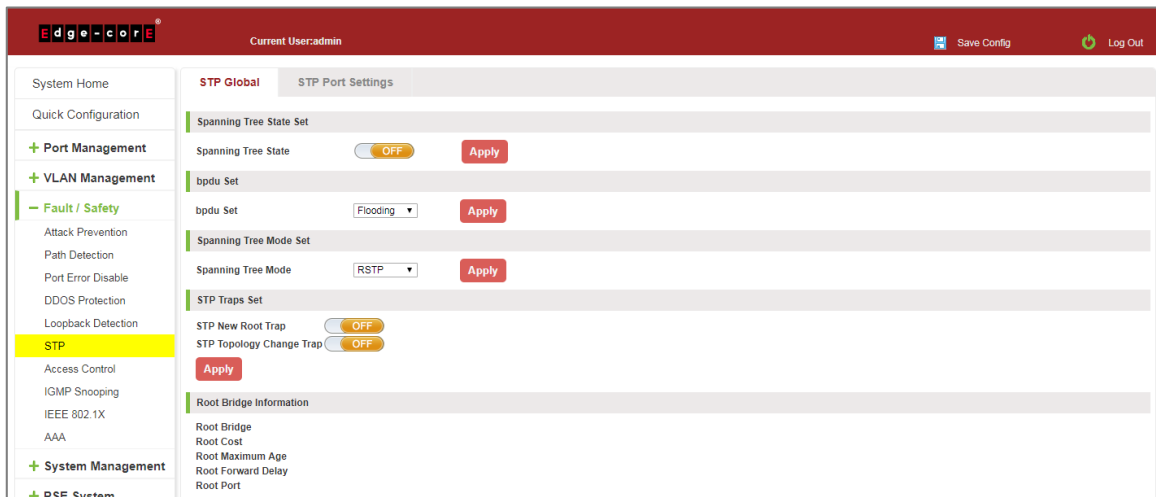


Figure 6-28: STP Global View

### 6.6.1 Enabling STP

1. Click the Spanning Tree State ON/OFF of slider to ON and then Click Apply to enable the STP global state.
2. In the Spanning Tree Mode drop down menu select the STP algorithm desired, for example RSTP and click Apply.
3. Under STP Traps Set use the ON/OFF sliders to turn on or off traps for STP New Root set or Topology Change.

Once the trap buttons are set correctly click Apply.

#### Note:

1. Loopback detection and STP functions are mutually exclusive.
2. If LLDP PDU flooding is enabled, mSTP cannot be enabled.

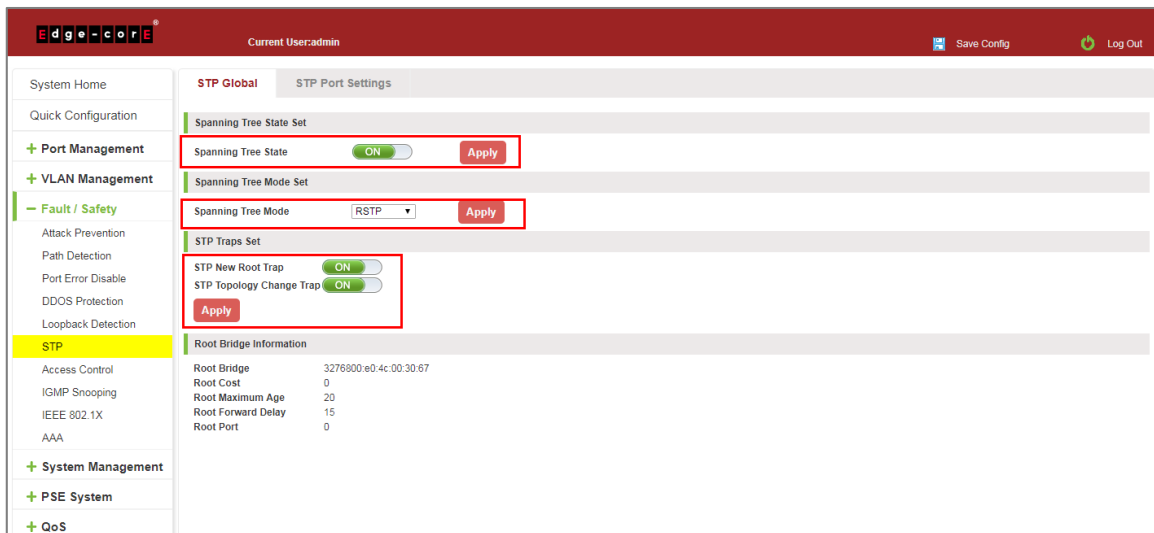


Figure 6-29: Enabling STP and Configuring the STP Mode and Traps

## 6.6.2 STP port settings

Click "Fault/Safety" "STP" "STP Port Settings" to view the STP port configuration.

Select the port(s) in the port panel view and then select the STP settings in the pulldown menus below the port panel to configure the port STP settings and click Apply.

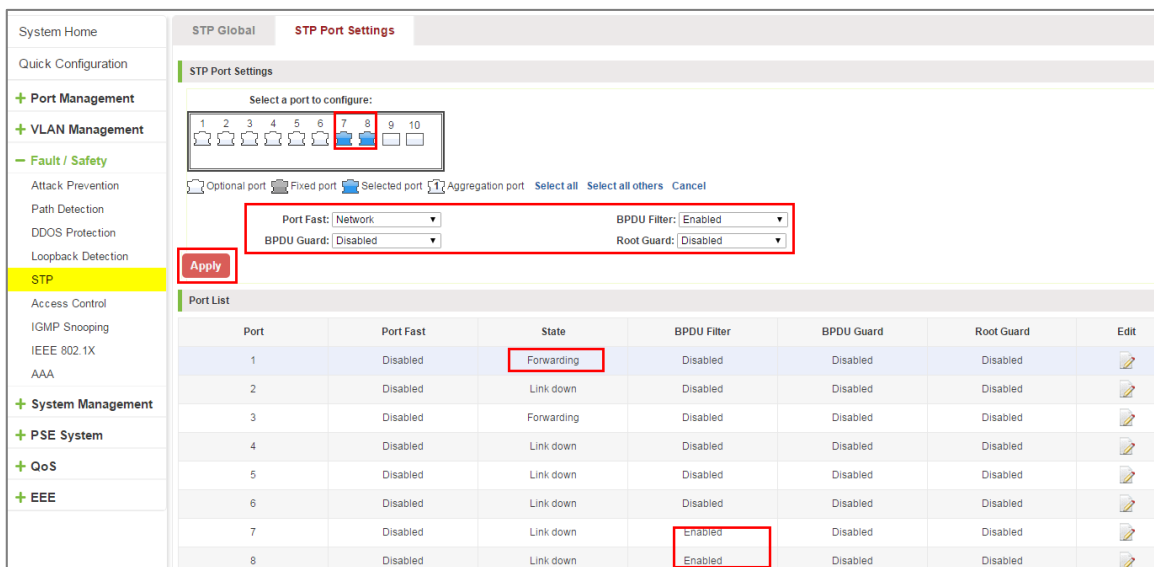


Figure 6-30: Port STP Configuration

## 6.7 ACCESS CONTROL

### 6.7.1 ACL access control list

#### 6.7.1.1 View access control list

Click "Fault/Safety" "Access Control" to view the ACL configuration.

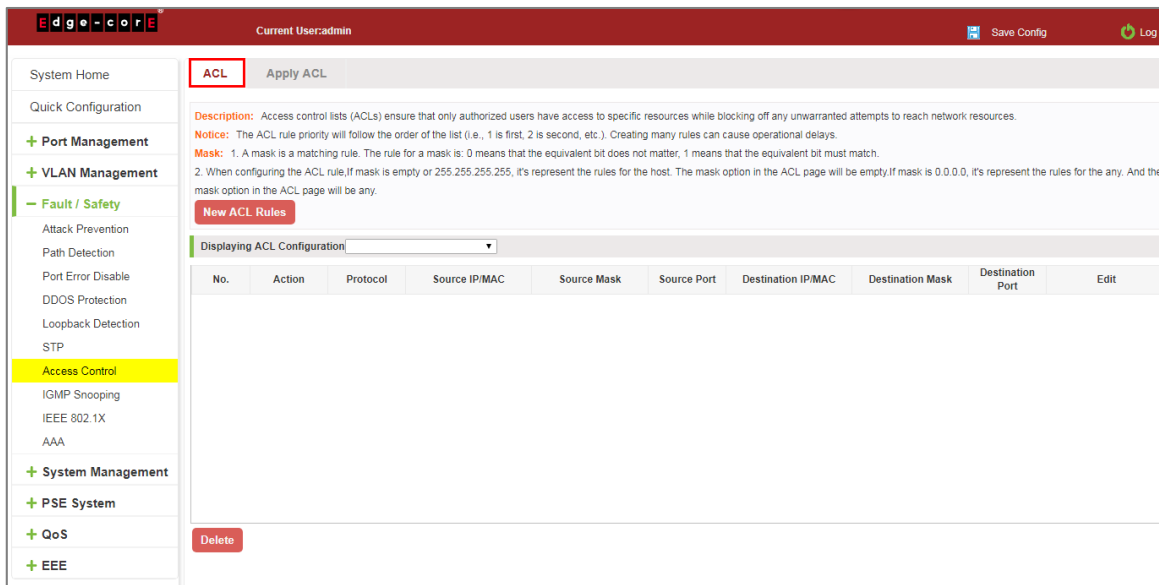


Figure 6-31: Access Control List

### 6.7.1.2 Add access rules

#### ADDING STANDARD IP ACCESS RULES

Click "New ACL Rules" and in the pop-up dialog box:

1. List ID: Select "Standard IPV4 ACL Configuration"
2. ACE ID: Select ACE 0.
3. Rules: Permit/Deny
4. IP address: Select "Any source IP address"
5. Click Apply to add the new rule:

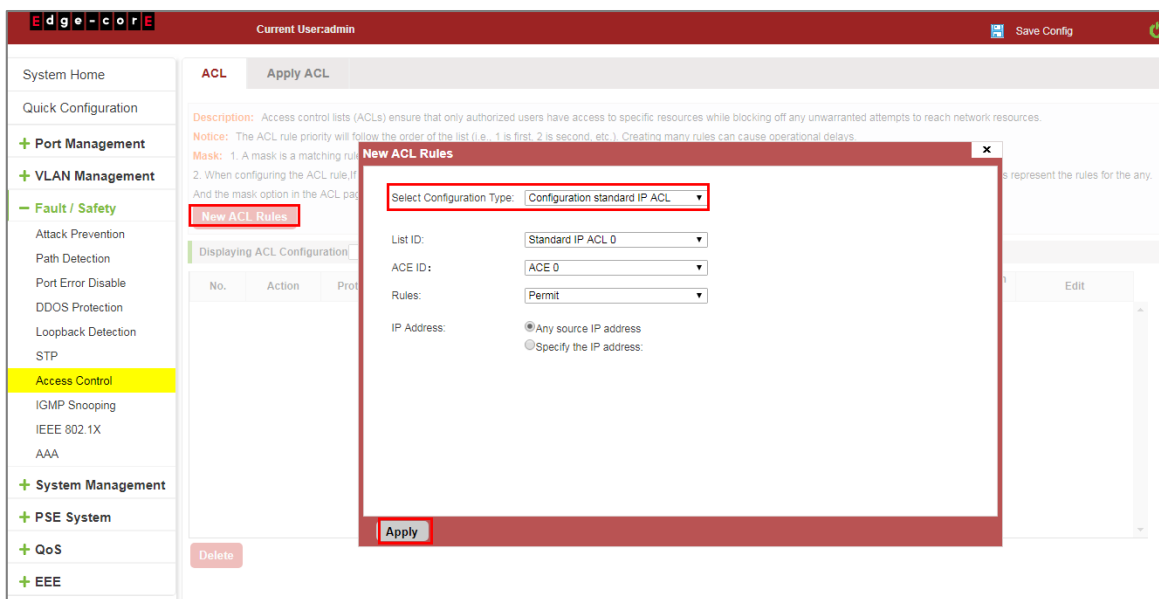


Figure 6-32: Configuring Standard IP Access Control Lists

#### ADDING AN EXPANDED IP ACCESS RULE

Click "New ACL Rules" and in the pop-up dialog box:

1. List ID: Select "Expand IP ACL "
2. ACE ID: Select ACE 0.
3. Rules: Permit/Deny
4. Protocol: IP
5. Source IP address: Select "Any source IP address"
6. Destination IP address: Select "Any destination IP address"
7. Click Apply to add the new rule:

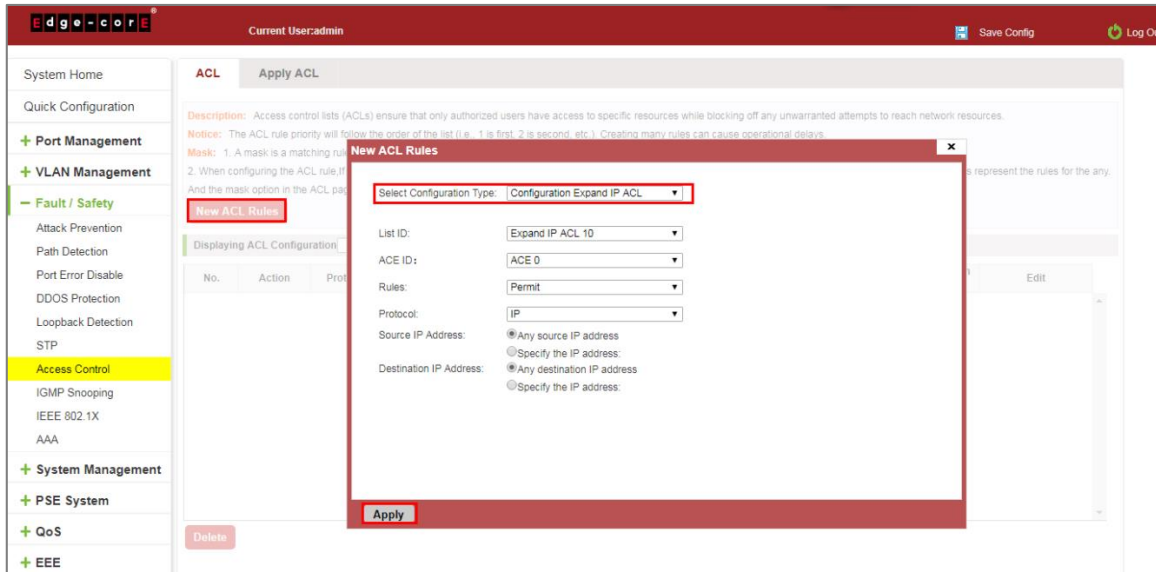


Figure 6-33: Configuring an Expanded IP Access Control List

## 8. ADDING AN EXPAND MAC ACCESS RULES

Click "New ACL Rules" and in the pop-up dialog box:

1. List ID: Select " Expand MAC ACL"
2. ACE ID: Select ACE 0.
3. Rules: Permit/Deny
4. Source IP address: Select "Any source IP address"
5. Destination IP address: Select "Any destination IP address"
6. Click Apply to add the new rule:

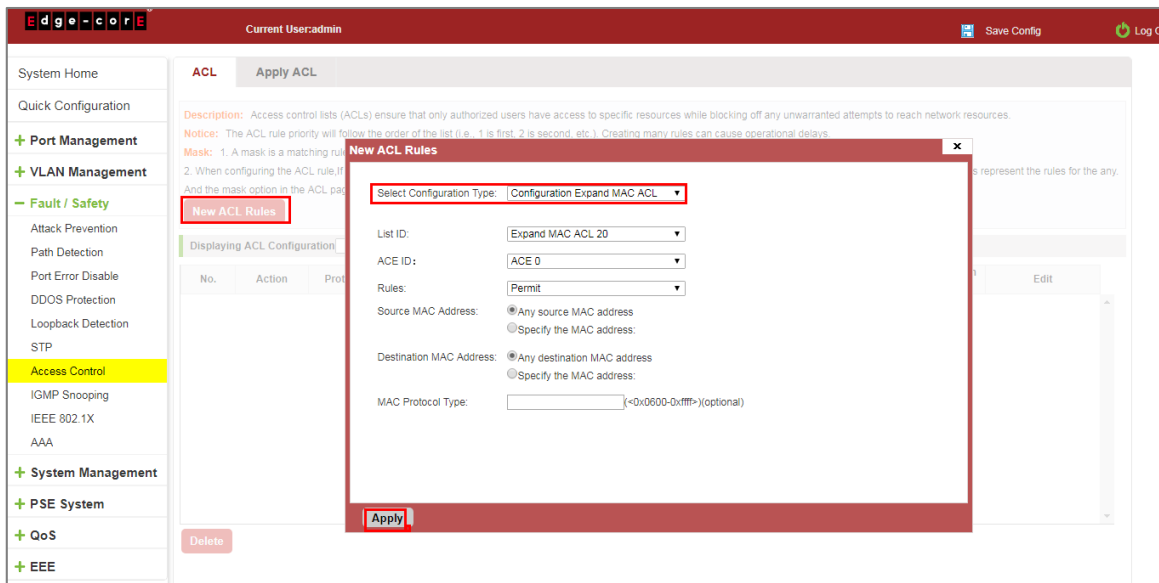


Figure 6-34: Configuring an Extended MAC Access Control List

**Note 1:** ACE ID is an optional rule and not required: the default is 0.

**Note 2:** For extended IP protocol access control lists, type: TCP, UDP, or IP.

### 6.7.1.3 Modifying the ACL configuration

To modify the rules select the rules to be replaced, click "  " to enter the ACL rules page.

Once on the ACL rules page modify the following:

Rules: Permit or Deny

Protocol: Select the required protocol

Source or Destination IP Address: Select Any IP address or Specify the IP address and input a specific address.

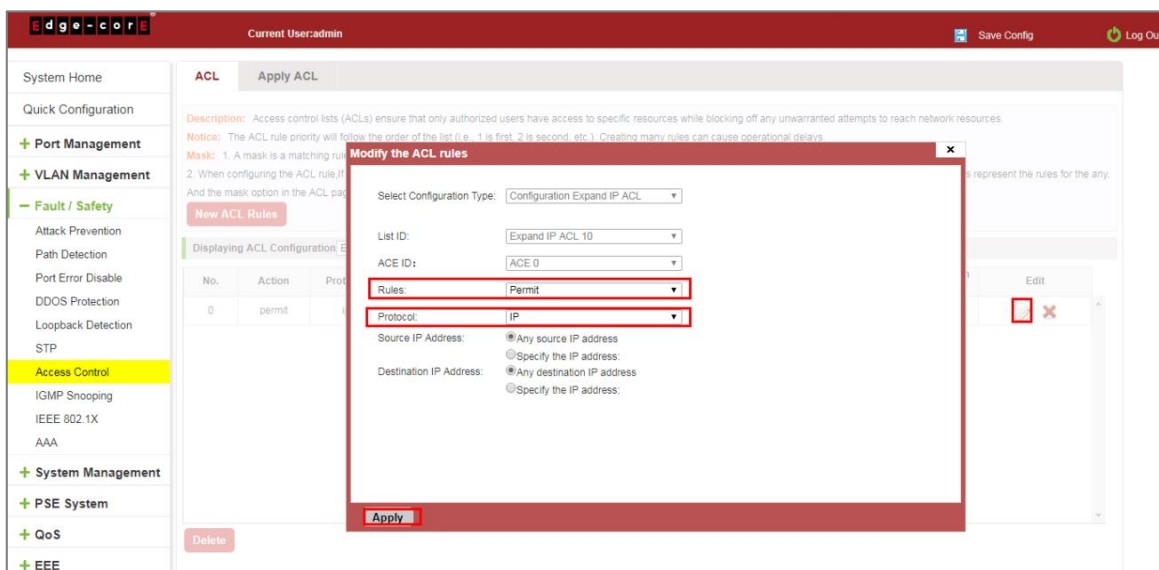


Figure 6-35: Modifying ACL rules



### 6.7.1.4 Delete an ACL rule

To delete an ACL rule, select the ACL configuration type in the pull down list at the top and then click the red **X** in the ACL Rules list to delete it.

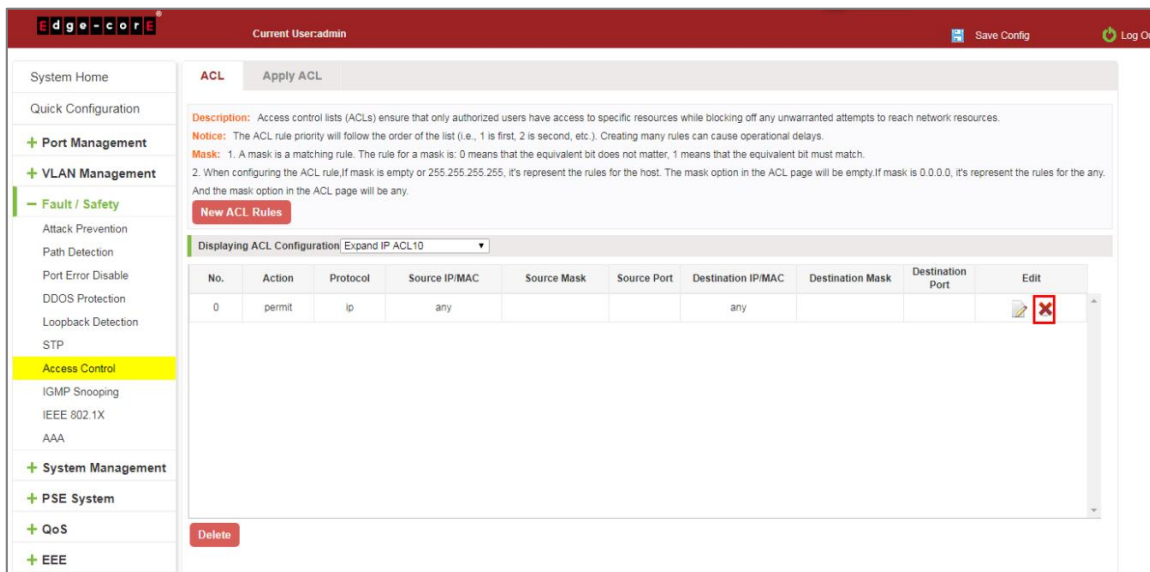


Figure 6-36: Deleting ACL Rules

To remove all the ACE rules of a specified ACL configuration, click the "Delete" button at the bottom of the ACL rules list.

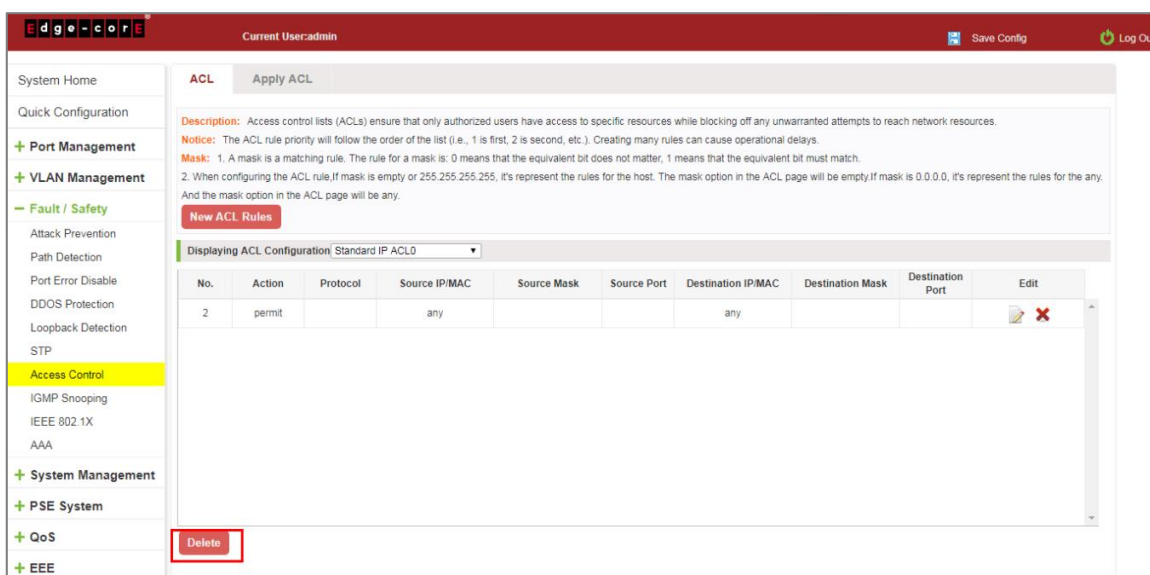


Figure 6-37: Deleting all ACL Rules of a specified ACL configuration type

## 6.7.2 Applying ACLs

### 6.7.2.1 View applied ACLs

Click "Fault/Safety" "Access Control" "Apply ACL" to view a list of ACLs applied to the switch ports.

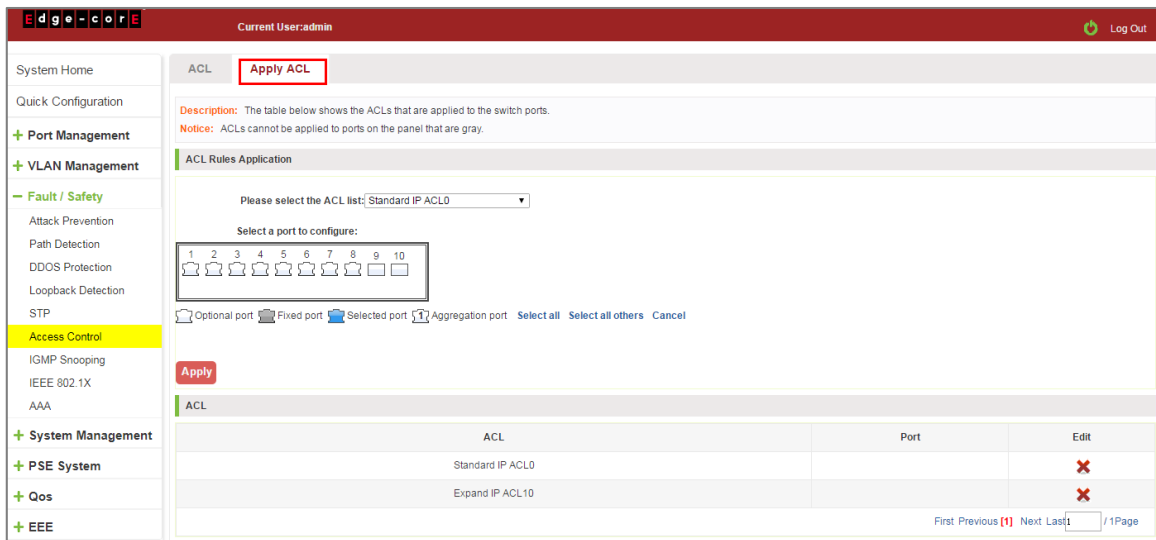


Figure 6-38: View Application ACL Rules

### 6.7.2.2 Apply ACLs to Specified Ports

1. Select the ACL rules from the Please select the ACL List drop down menu.
2. Select the specified ports to apply the ACL rule on.
3. Click Apply.

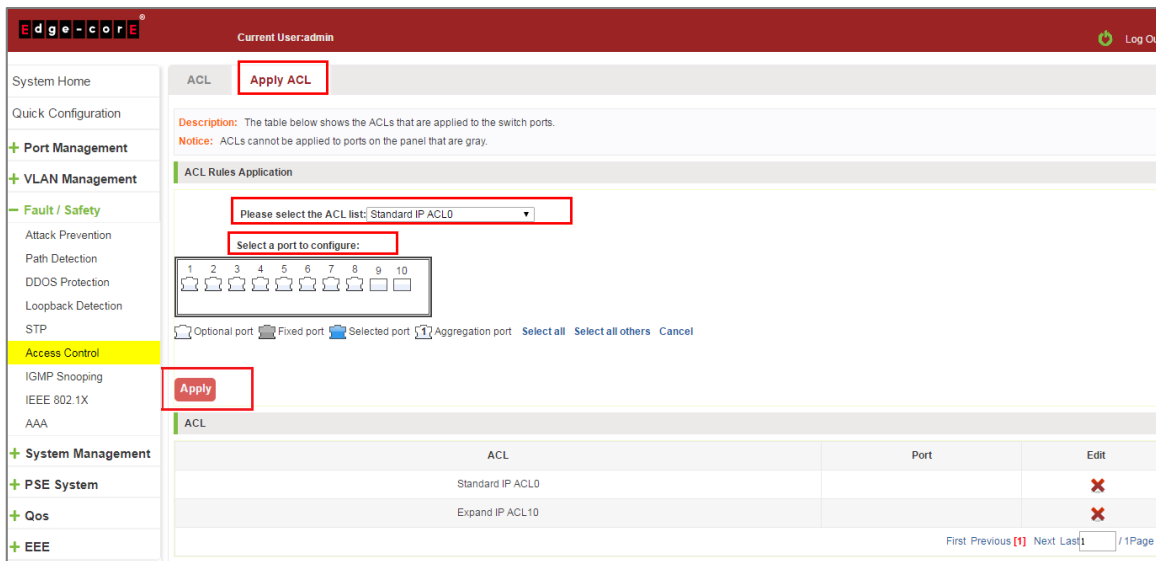


Figure 6-39: Applying ACL Rules to Specified Ports

### 6.7.2.3 Delete ACLs Applied to a Specified Port(s)

1. Select the ports to delete the applied ACL rule on.
2. Find the ACL rule in the ACL list at the bottom of the page and click the red X under the Edit column to delete the rule from the port(s).

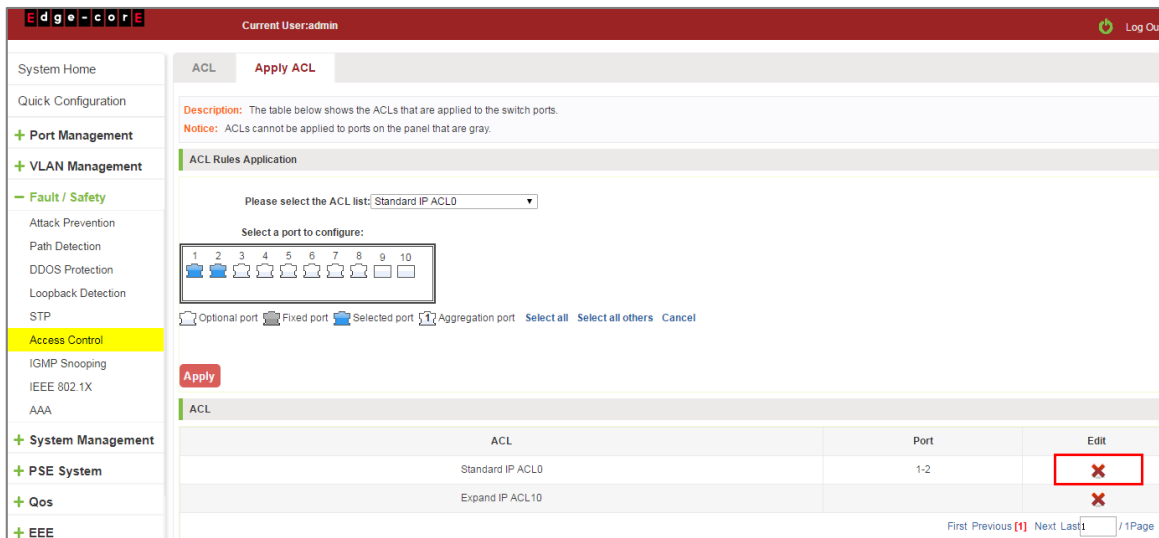


Figure 6-40: Delete Application ACL

## 6.8 IGMP SNOOPING

### 6.8.1 Viewing IGMP snooping configuration

Click "Fault/Safety" "IGMP Snooping" to view the configured multicast monitoring information.

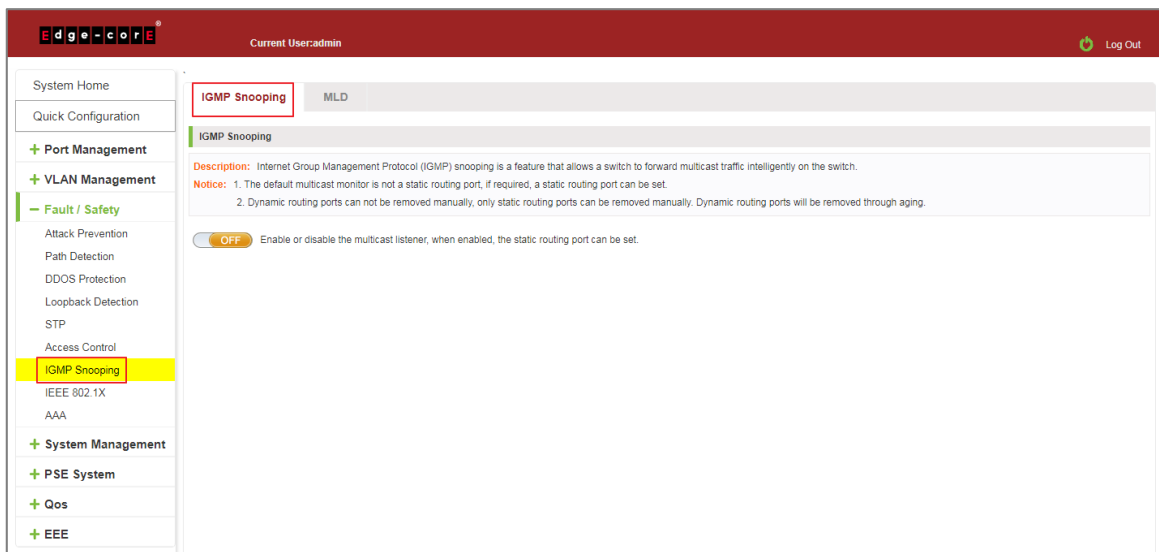


Figure 6-41: Viewing the IGMP Snooping Configuration

#### 6.8.1.1 Enabling IGMP Snooping

Click "Fault/Safety" "IGMP Snooping" and click the OFF slider to ON to enable IGMP snooping.

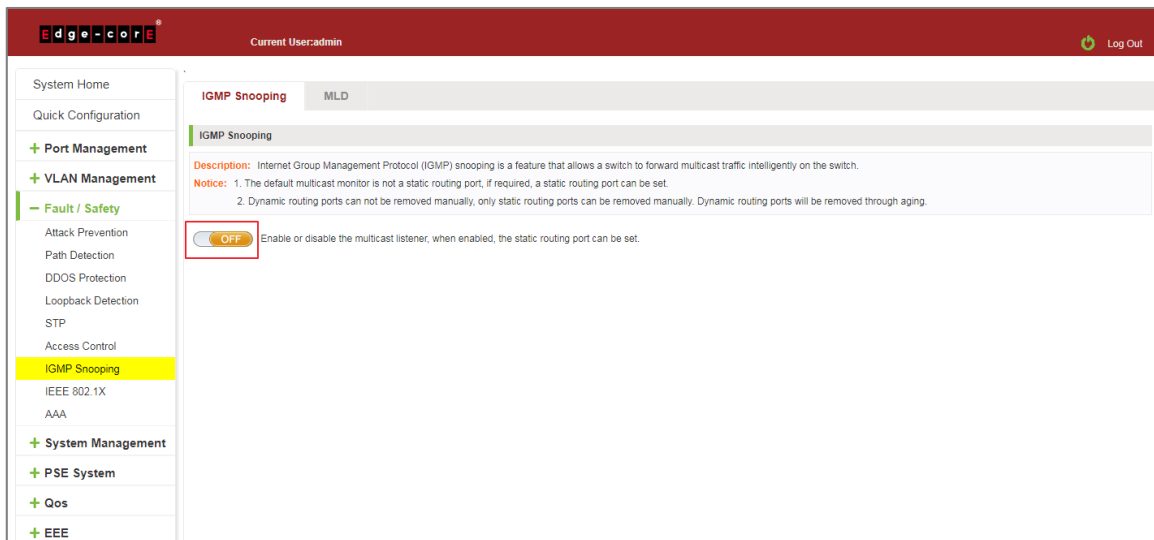





Figure 6-42: Viewing the Multicast Listener Configuration

-  **Note 1:** IGMP Snooping is disabled by default.
-  **Note 2:** IGMP snooping VLANs are all open by default.
-  **Note 3:** The switch uses IGMP v2 as default.

### 6.8.1.2 Disabling IGMP Snooping

Click "Fault/Safety" "IGMP Snooping" and click the "ON/OFF" slider to "OFF" to disable IGMP snooping.

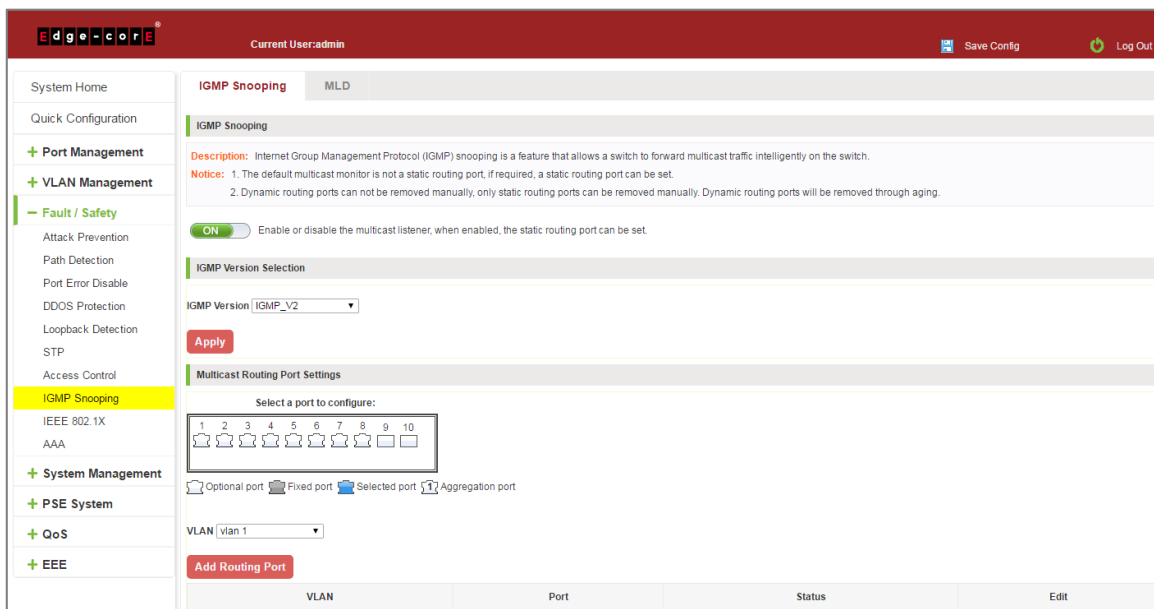


Figure 6-43: Disabling IGMP Snooping

### 6.8.1.3 Configuring multicast routing

1. From the VLAN drop down menu select the desired VLAN
2. Click the Add Router Port button, to launch the Multicast Routing Port Settings panel.

3. In the port panel select the port(s) to apply multicast routing on.
4. Select the VLAN ID number from the drop down menu.
5. Click the Add Routing Port button to complete the configuration.

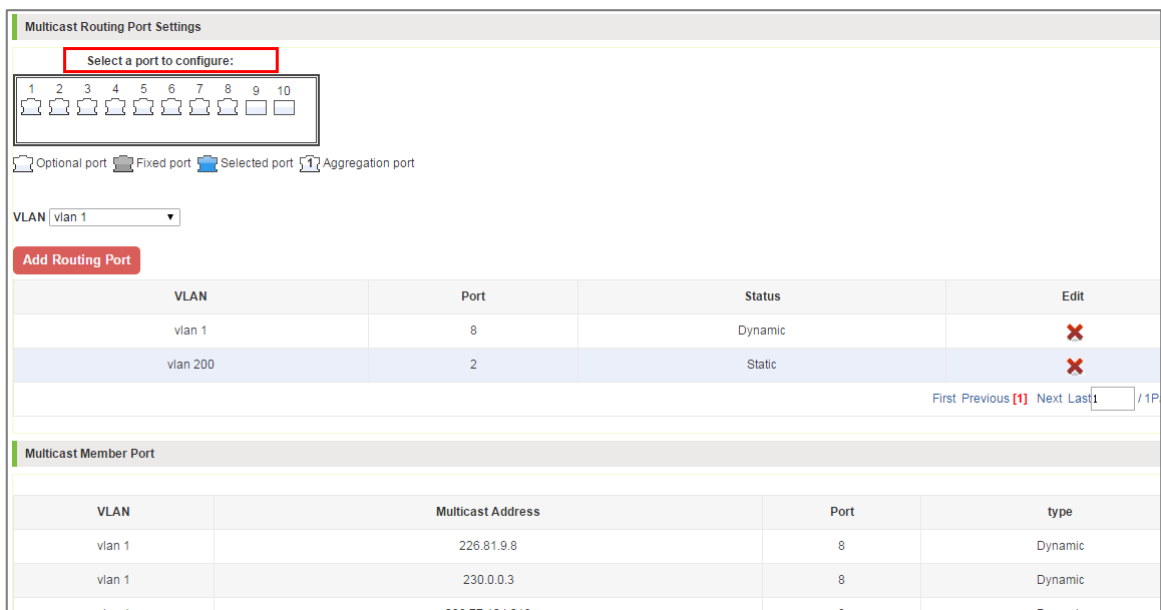


Figure 6-44: Configuring Multicast Routing

### 6.8.1.4 Configuring the IGMP Version

Click "Fault/Safety" "IGMP Snooping", to access the IGMP version page.

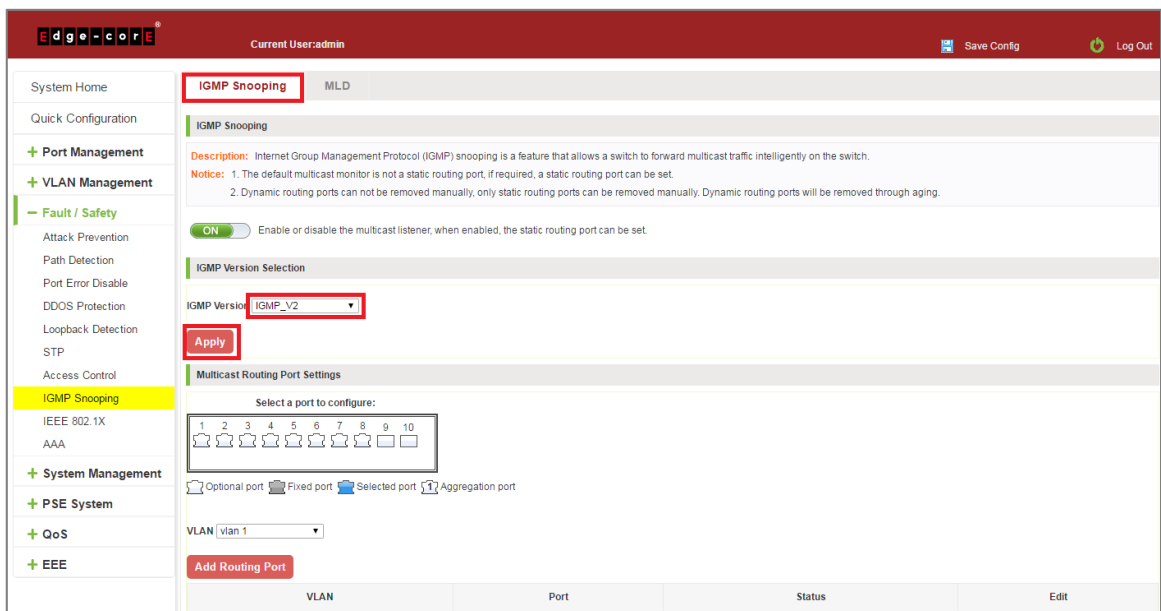


Figure 6-45: Configuring IGMP Version

To configure the IGMP version:

Step 1: Select the required version from the IGMP Version drop down menu.

Step 2: Click Apply.

## 6.8.2 MLD

### 6.8.2.1 Viewing the MLD configuration

Click "Fault/Safety" "IGMP Snooping" "MLD" to view the configured multicast monitoring data.

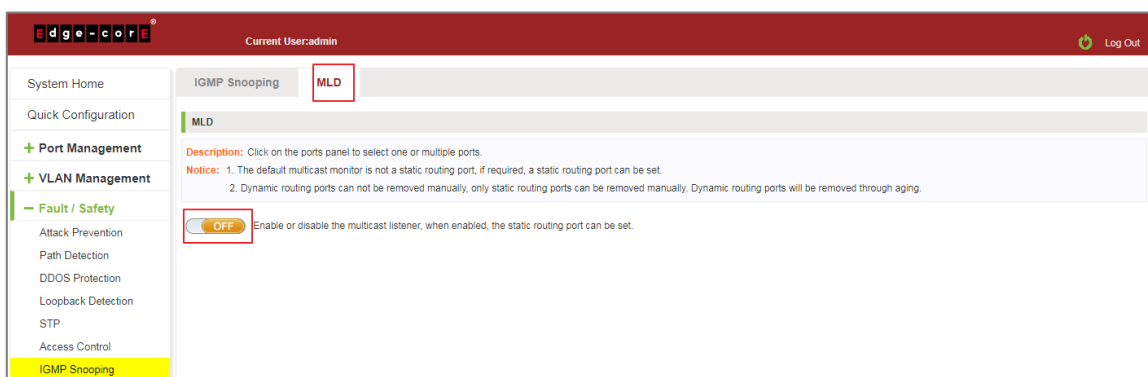


Figure 6-46: Viewing the MLD Configuration

### 6.8.2.2 Enabling the multicast listener function

Click "Fault/Safety" "IGMP Snooping" "MLD", and then click the OFF slider to ON to enable the multicast monitoring function.

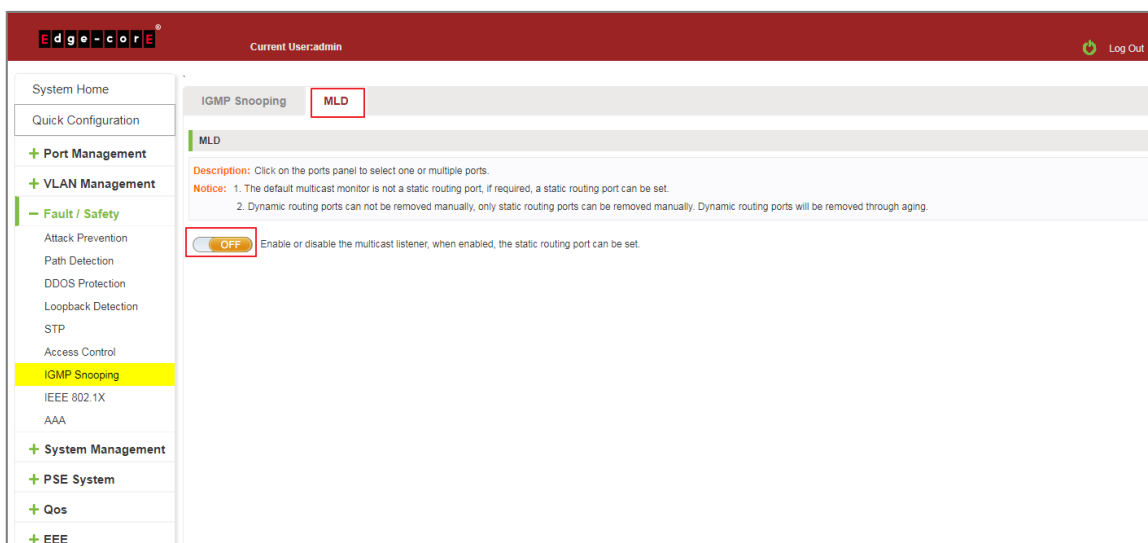


Figure 6-47: Enabling Multicast Listener (MLD)



**Note 1:** By default, MLD is set to OFF.



**Note 2:** For MLD all VLANs are open by default.



**Note 3:** MLD uses version 1 by default.

### 6.8.2.3 Disabling the multicast listener function

Click "Fault/Safety" "IGMP Snooping" "MLD" and then click the "ON/OFF" slider to "OFF" to disable the multicast monitoring function.

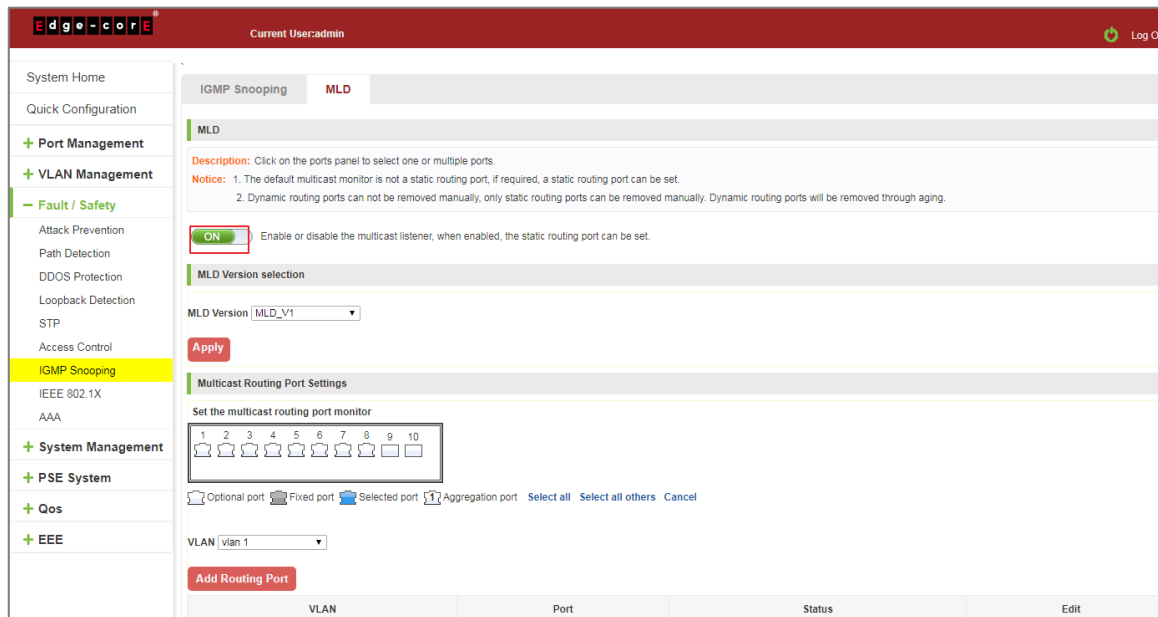


Figure 6-48: Disabling the Multicast Listener Function

### 6.8.2.4 Configuring multicast routing

1. In the MLD window select a VLAN from the VLAN drop down menu
2. Click the Add Router Port button, to open the port multicast listening configuration panel.
3. In the port configuration panel select the multicast listener routing port(s).
4. Select the VLAN ID from the VLAN drop down menu.
5. Click the Add Router Port button to configure the multicast routing.

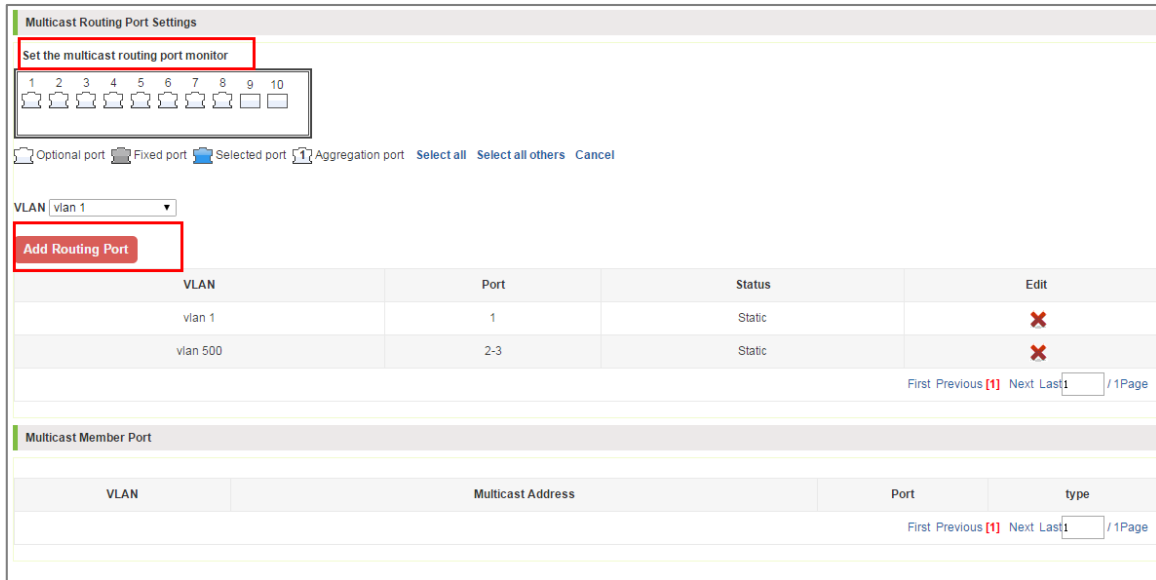


Figure 6-49: Configuring Multicast Routing

## 6.9 IEEE 802.1X

IEEE 802.1X is a port-based authentication protocol used for authenticating clients.

Click "Fault/Safety" "IEEE 802.1X"

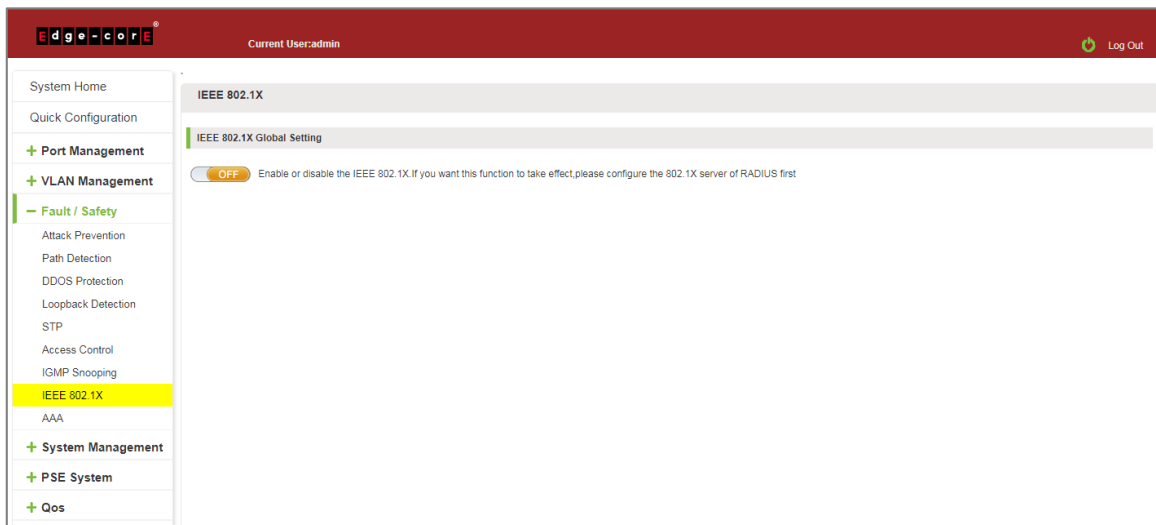


Figure 6-50: IEEE 802.1X

Click the OFF slider to ON to enable IEEE802.1X.



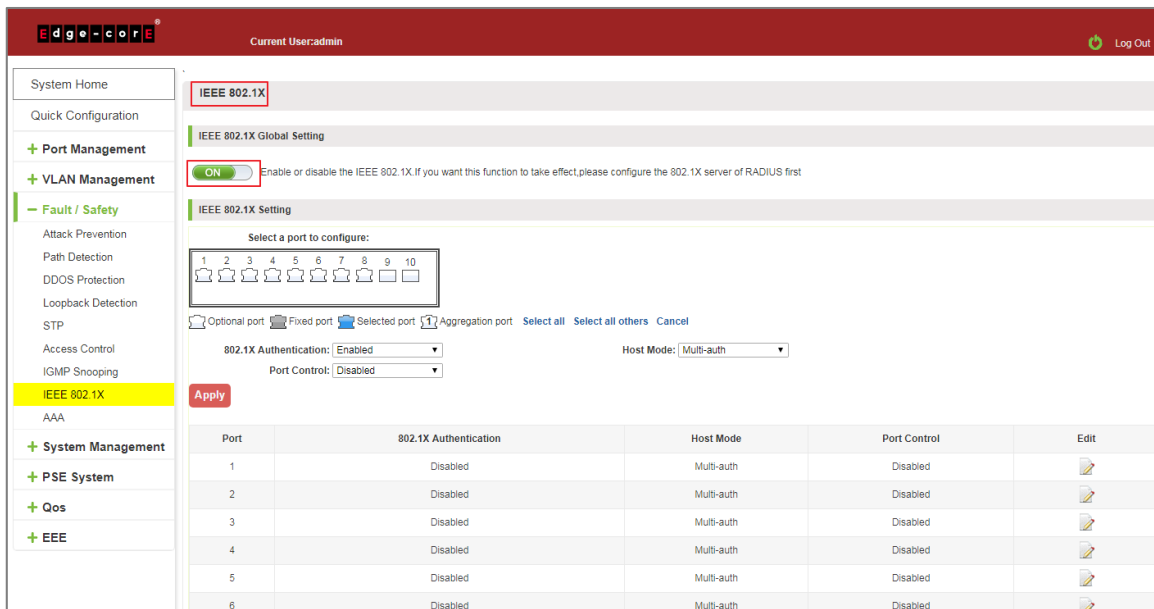


Figure 6-51: Enabling IEEE 802.1X

### 6.9.1 AAA radius configuration

Click "Fault/Safety" "AAA"

In the AAA configuration page enter the AAA RADIUS server IP address, the Authentication Port and Key values and then for Type select All. Click Apply to configure the AAA RADIUS configuration.

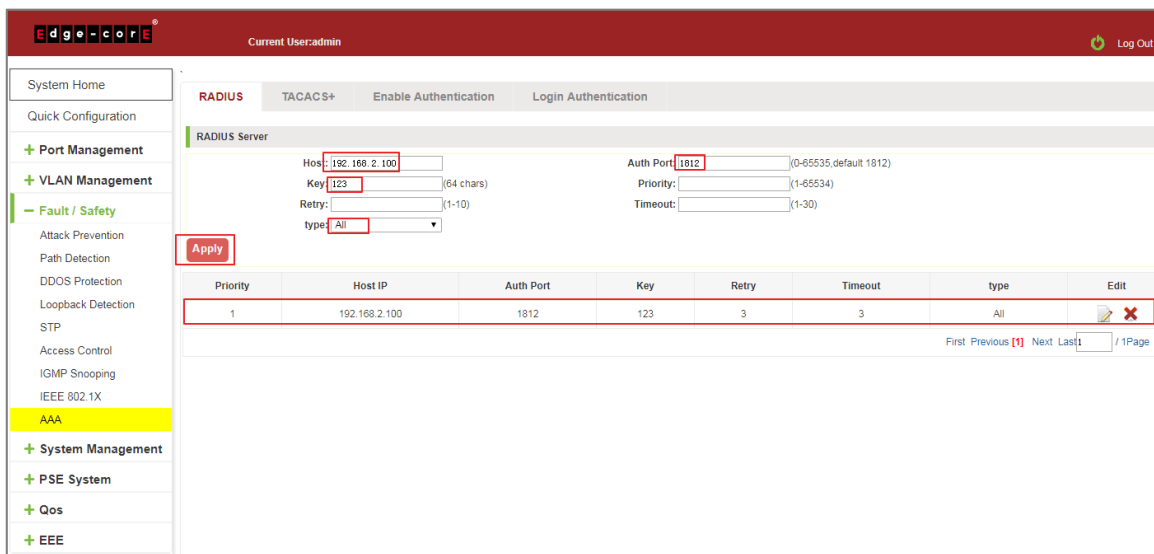


Figure 6-52: Configuring Radius for IEEE802.1X

### 6.9.2 Configuring IEEE802.1X parameters

In the port panel select the port(s) to apply the 802.1X settings on.

Set the following in the 802.1X parameter area:

1. 802.1X Authentication: Enabled
2. Port Control: Auto

3. Host Mode: Multi-auth
4. Click Apply

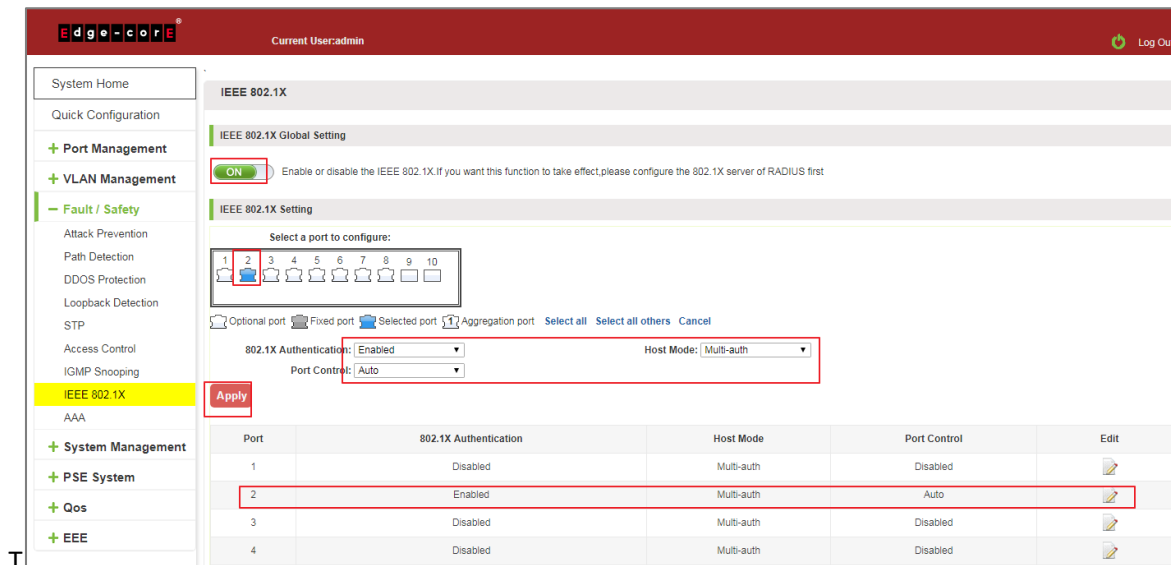


Figure 6-53: Configuration IEEE802.1X



**Note:** IEEE802.1x protocol is used with the AAA function.

**Auto:** 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.

**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 single host, until authentication is complete it can only forward authentication frames.

**Multi-auth:** When a port is connected to another hub/switch all the connecting hosts on the connected hub/switch can be authenticated individually.

**Multi-host:** This port can be connected to multiple hosts, once a single host has passed its client authentication all other hosts on the port can pass traffic.

## 6.10 AAA RADIUS

### 6.10.1 Configuring RADIUS

Click "Fault/Safety" "AAA" "RADIUS"

In the RADIUS configuration page enter the RADIUS server IP address, the Authentication Port and Key values and then for Type select All. Click Apply to configure the AAA RADIUS configuration.

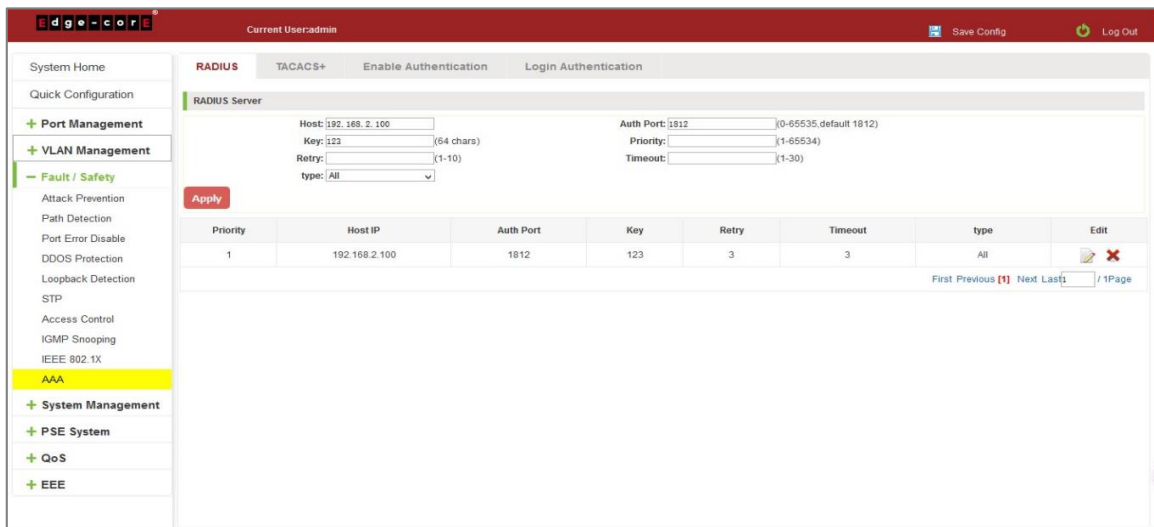


Figure 6-54: Configuring RADIUS

### 6.10.1.1 Configuring RADIUS Authentication

Click the [Enable Authentication](#) tab.

1. Input a name for the authenticating host, for example ECS2020
2. In the Method 1 drop down menu select RADIUS
3. Click Apply
4. In the Enable Authentication parameters select the following drop down menu items:  
**SSH: ECS2020, Telnet: ECS2020**
5. Click Apply.

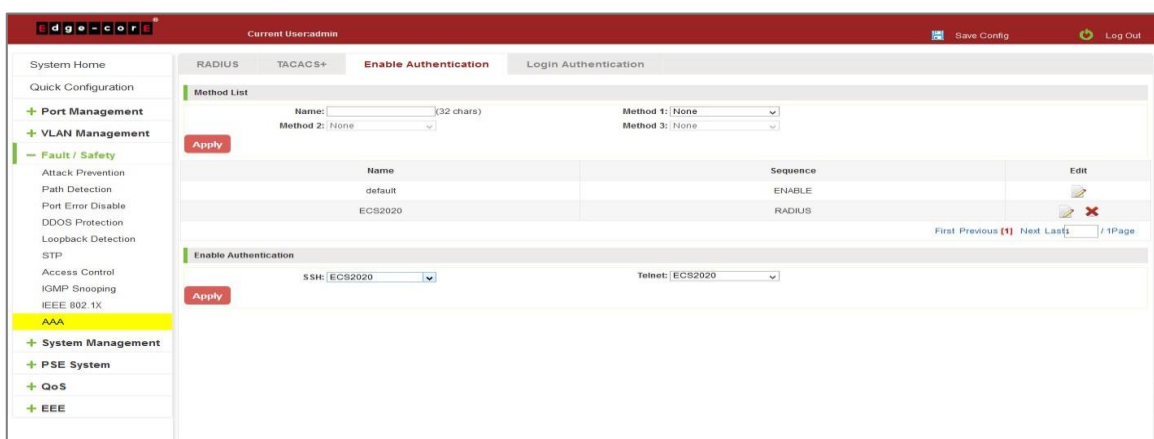
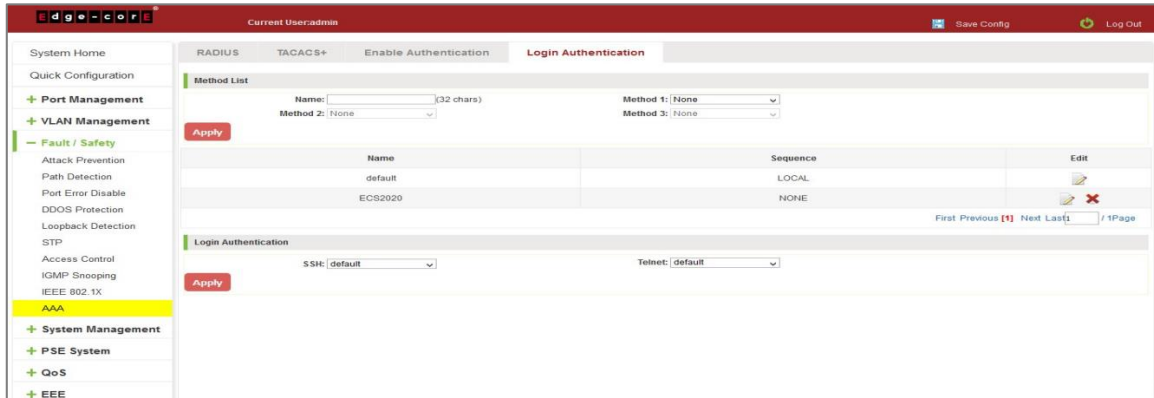


Figure 6-55: Enabling Authentication

### 6.10.1.2 Configuring RADIUS Login Authentication

Click the [Login Authentication](#) tab.

1. Input a name for the authenticating host, for example ECS2020
2. In the Method 1 drop down menu select RADIUS
3. Click Apply
4. In the Enable Authentication parameters select the following drop down menu items:  
**SSH: ECS2020, Telnet: ECS2020**
5. Click Apply.



**Figure 6-56: Configuring RADIUS Login Authentication**

**NOTE:**

To successfully authenticate with the AAA TACACS+ function, using a PC input the correct user name and password through either telnet or SSH connection to the switch.

**6.10.2 TACACS+**

Click "[Fault/Safety](#)" "[AAA](#)" "[TACACS+](#)"

To configure a TACACS+ server:

1. Input the TACACS+ server IP address in the host field.
2. Input the TCP port to use (default is 49).
3. Input a key in the Key field.
4. Click Apply.

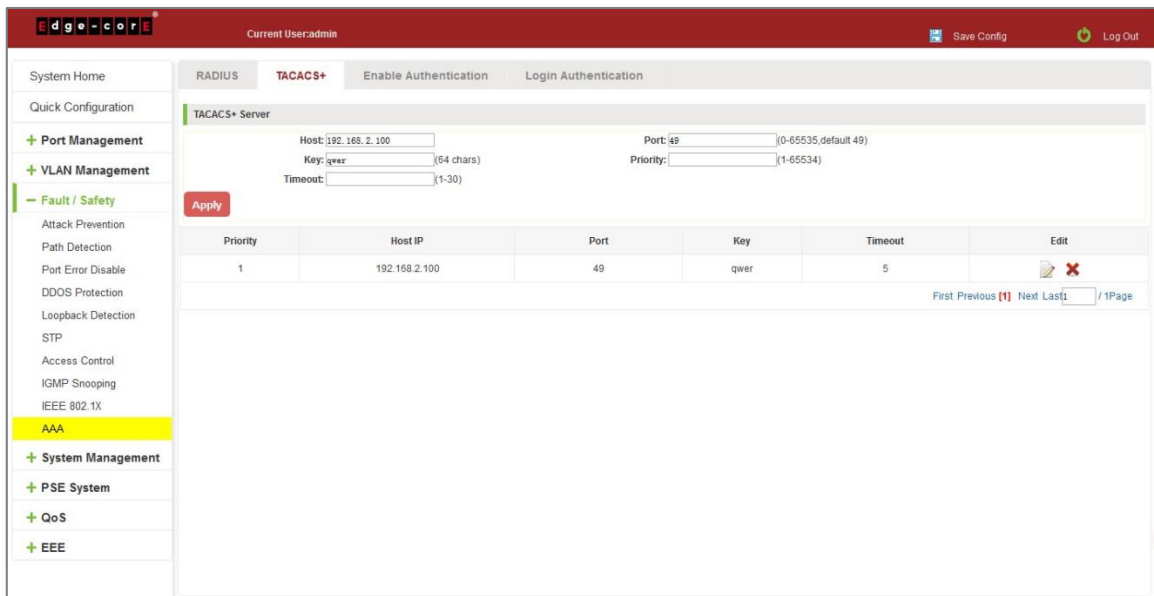


Figure 6-57: Configuring TACACS+

### 6.10.2.1 Configuring TACACS+ Authentication

Click the [Enable Authentication](#) tab:

1. Input a name for the authenticating host, for example ECS2020.
2. In the Method 1 drop down menu select RADIUS.
3. Click Apply.
4. In the Enable Authentication parameters select the following drop down menu items:  
**SSH: ECS2020, Telnet: ECS2020**
5. Click Apply.

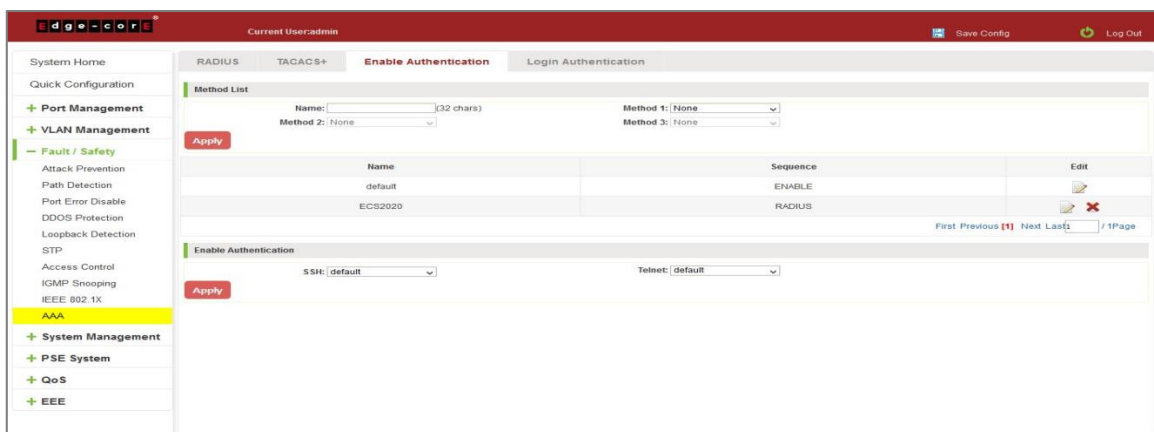


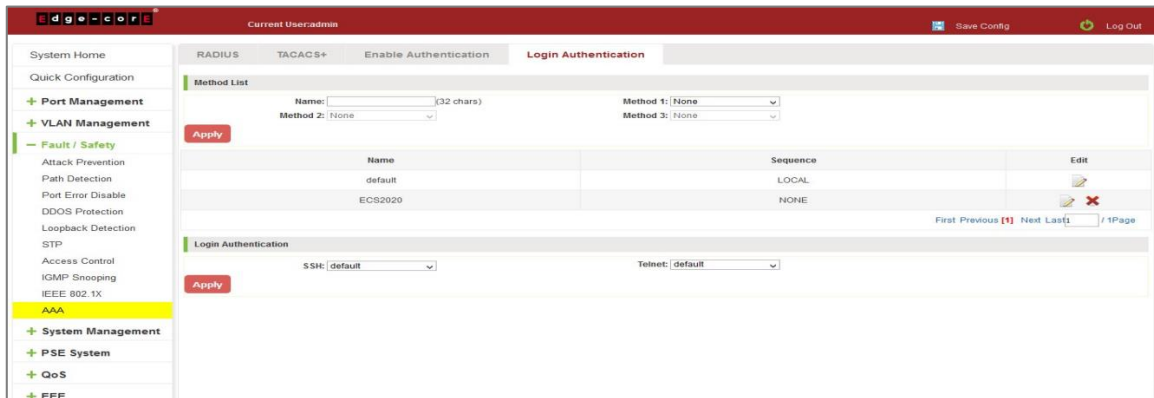
Figure 6-58: Configuring TACACS+ Authentication

### 6.10.2.2 Configuring TACACS+ Login Authentication

Click the [Login Authentication](#) tab:

1. Input a name for the authenticating host, for example ECS2020.

2. In the Method 1 drop down menu select TACACS+.
3. Click Apply.
4. In the Enable Authentication parameters select the following drop down menu items:  
**SSH: ECS2020, Telnet: ECS2020**
5. Click Apply.



**Figure 6-59: Configuring TACACS+ Login Authentication**



**NOTE:** To successfully authenticate with the AAA TACACS+ function, using a PC input the correct user name and password through either telnet or SSH connection to the switch.

## 7 SYSTEM MANAGEMENT

### 7.1 SYSTEM SETTINGS

#### 7.1.1 Management VLAN

##### 7.1.1.1 Configuring basic system settings

Click "System Management" "System Settings" "Management VLAN" to view the management IP address of the current switch configuration.

The screenshot displays the Edge-Core switch management interface. The top navigation bar shows 'Current User: admin' and a 'Save Config' button. The left sidebar contains a menu with 'System Management' selected, and 'System Settings' highlighted. The main content area is titled 'Management VLAN' and contains the following sections:

- Description:** 1. Management VLAN parameters: IP, MAC, gateway and the user's contact details. "\*" denotes required field. 2. The IP address and mask cannot be configured when the DHCP server is enabled.
- Basic System Settings:** Fields for Management VLAN (vlan 1), DHCP (Static Allocation), Management IP (192.168.100.147), Subnet Mask (255.255.255.192), Default Gateway (192.168.100.129), Login Timeout (1800), Contact Name (joesa), MAC (00E0.4C00.0000), IPv6 DHCP (Static Allocation), IPv6 Address (fe80::2a0:4c00:fe00:0 / 64), IPv6 Gateway Address, Device Name (ECS2020-10P), Device Location (china), and Contact Information (12345678900).
- System Time Settings:** Includes a notice about time synchronization, a tip about default server selection, and fields for 'The Current System Time' (2013-12-05 00:57:15), 'Time Setting Mode' (Auto-Sync or Manual), and 'Time Zone (T)' (UTC/Coordinated Universal).

Figure 7-1: Basic System Settings

To configure the switch Basic System Settings: In the DHCP text box, choose static allocation

1. In the Management IP text box, enter an IP address for the switch, for example 192.168.2.10.
2. In the Subnet Mask text box, enter a subnet mask, for example 255.255.255.0.
3. In the Gateway Address text box enter a gateway address, for example 192.168.2.1.
4. In the Device Location text box, enter a Device Location, for example "RnD Comms Equipment Room".
5. In the Contact Name text box, enter a Contact Name, for example "Zhang San".
6. In the Contact Information text box, enter the Contact's Information, for example their extension x3358.
7. Click Apply



**Note:** For the switch management VLAN switch the default VLAN ID is 1.

### 7.1.1.2 System time synchronization

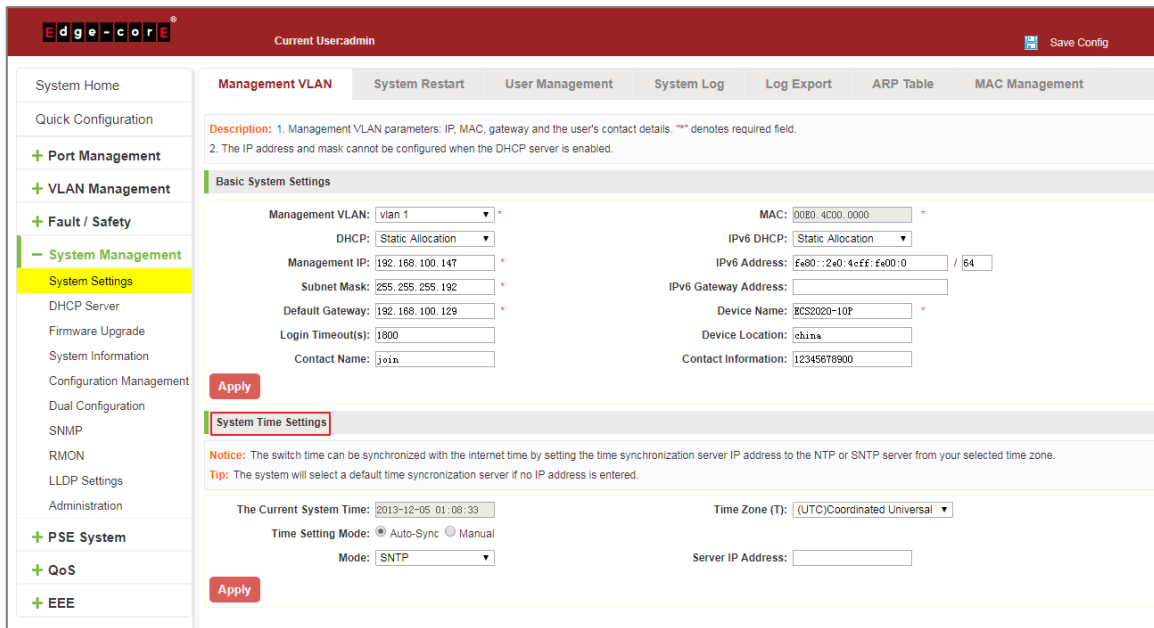
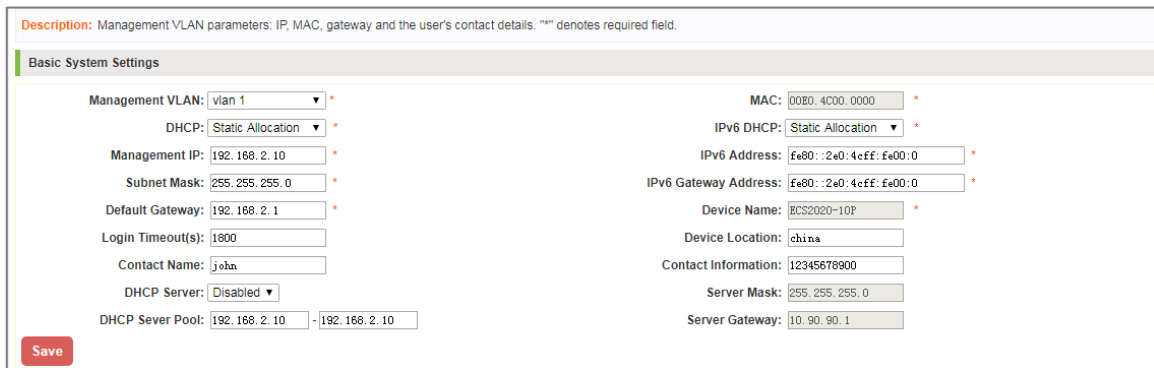


Figure 7-2: System Time Synchronization

To configure the system time, select NTP or SNTP and 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 the time zone for your location, for example the time zone for South Africa is UTC+02:00.

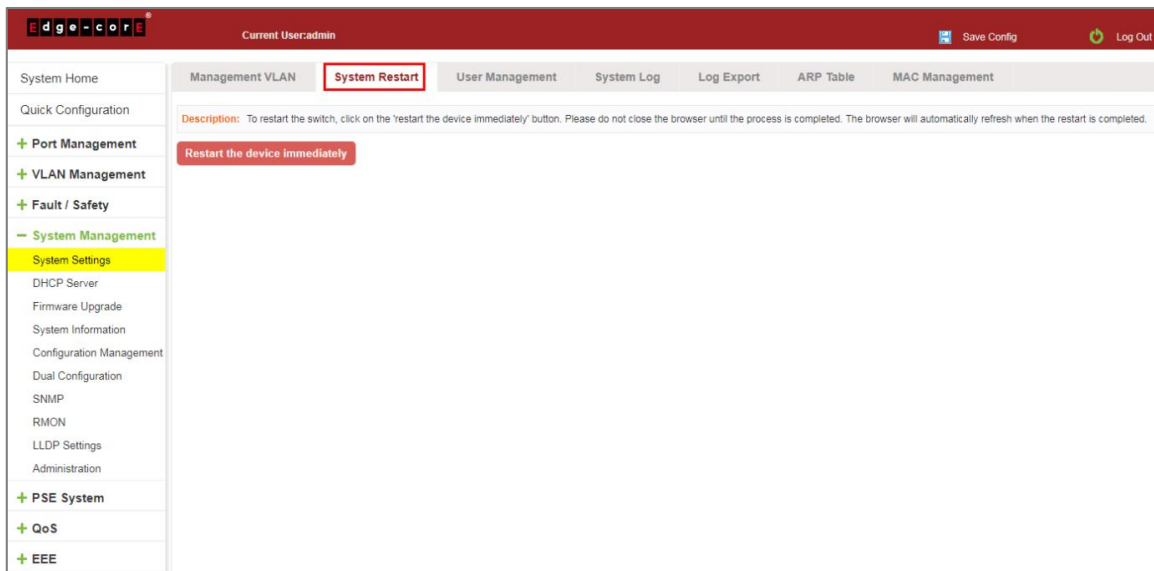
The device system time can also be manually configured.



### 7.1.2 System restart

Click "System Management" "System Settings" "System Restart" to reboot the switch.





**Figure 7-3: System Restart**

To Restart the device:

Step 1: Click the Restart the device immediately button.

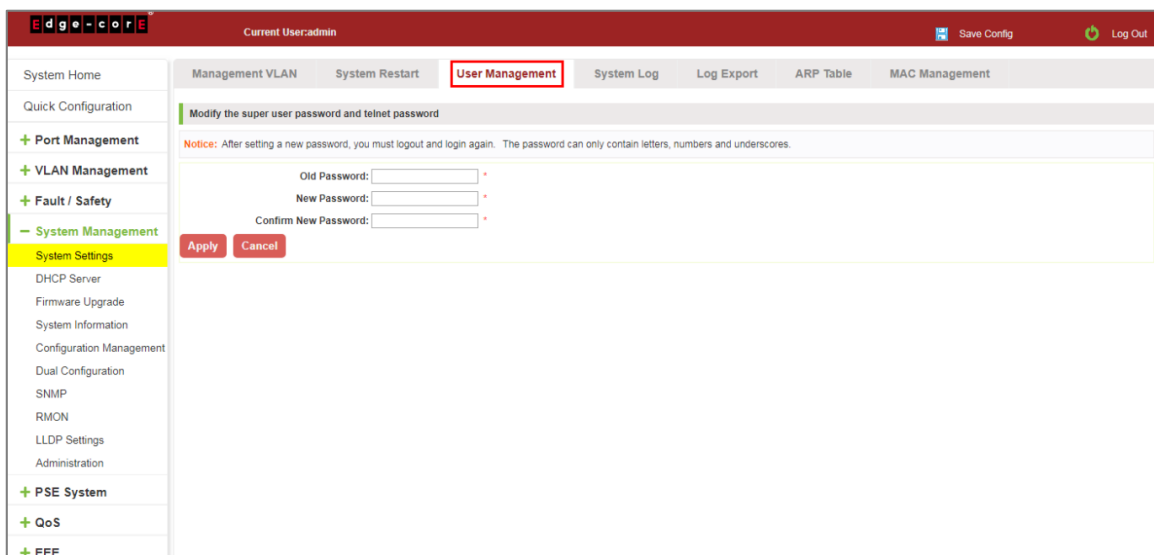
Step 2: Click OK in the dialog box that appears.

Step 3: As needed select OK or Cancel at the prompt to save the current configuration.

Step 4: After the restart once the progress bar moves to 100% the switch will be rebooted.

### 7.1.3 User management

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



**Figure 7-4: Change Password**

To change the password:

Step 1: Enter the old password: for example, password.

Step 2: Enter the new password: for example, abcd123.

Step 3: Confirm new password: for example, abcd123.

Step 4: Click the Apply button;

Step 5: In the dialog box, click the "OK" button.

### 7.1.4 System log

Click "System Management" "System Settings" "System Log" to enter the log management interface. The log management interface allows log queries using the search feature and all the logs can be cleared.

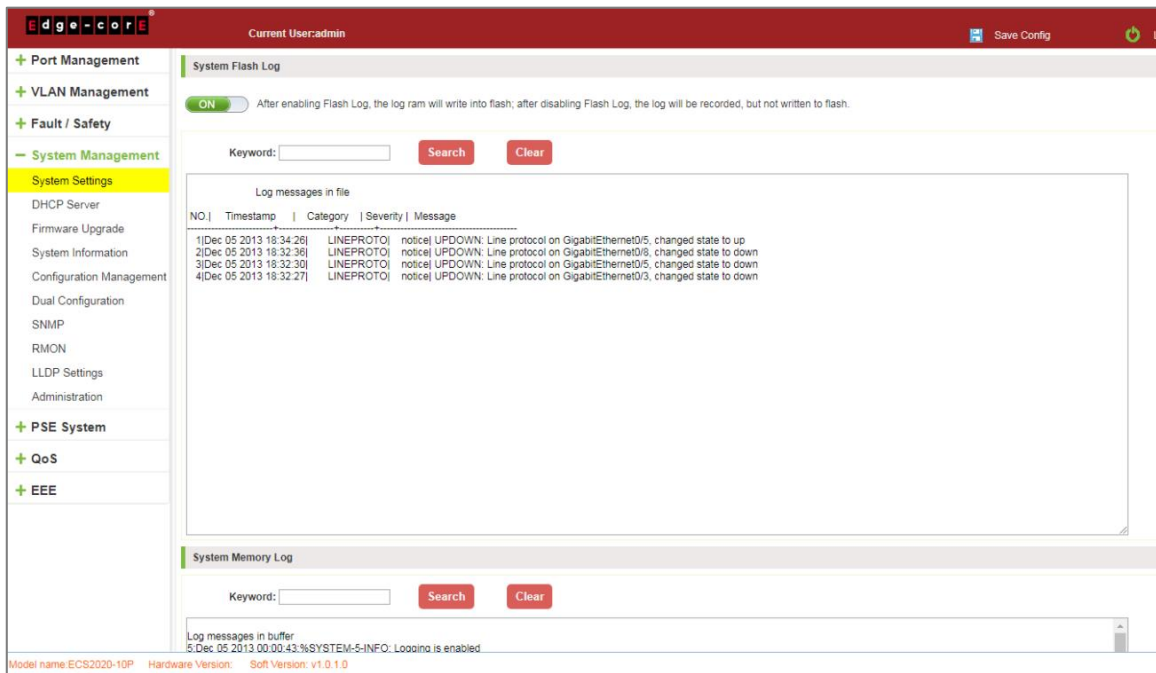


Figure 7-5: System Log

**Note:** The Log management system WEB page shows the same logs as using the show logging command from the CLI. Click the "Clear" button to clear the current log records in the switch.

### 7.1.5 Log export

Click "System Management" "System Settings" "Log Export" to export the switch log information. A TFTP server needs to be configured to export the log information.

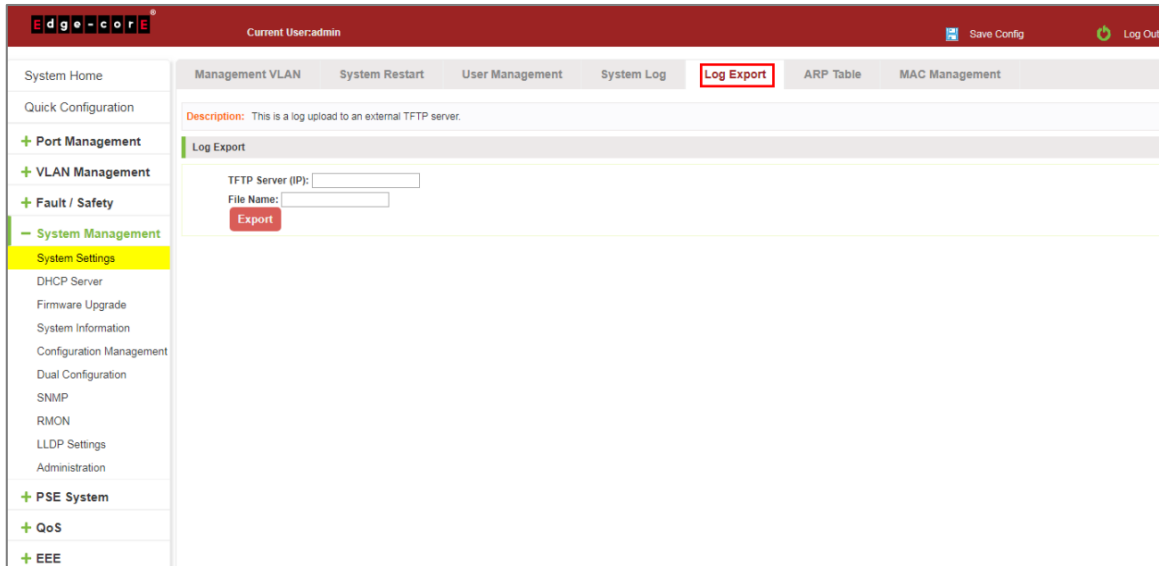


Figure 7-6: Log Export

## 7.1.6 ARP table

Click "System Management" "System Settings" "ARP Table" to view the current ARP table of the switch.

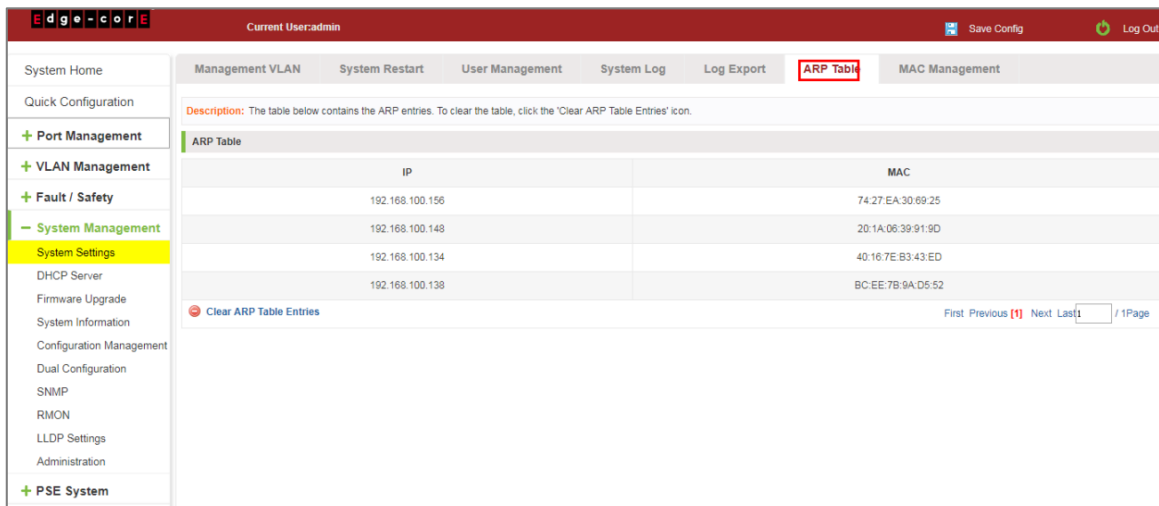


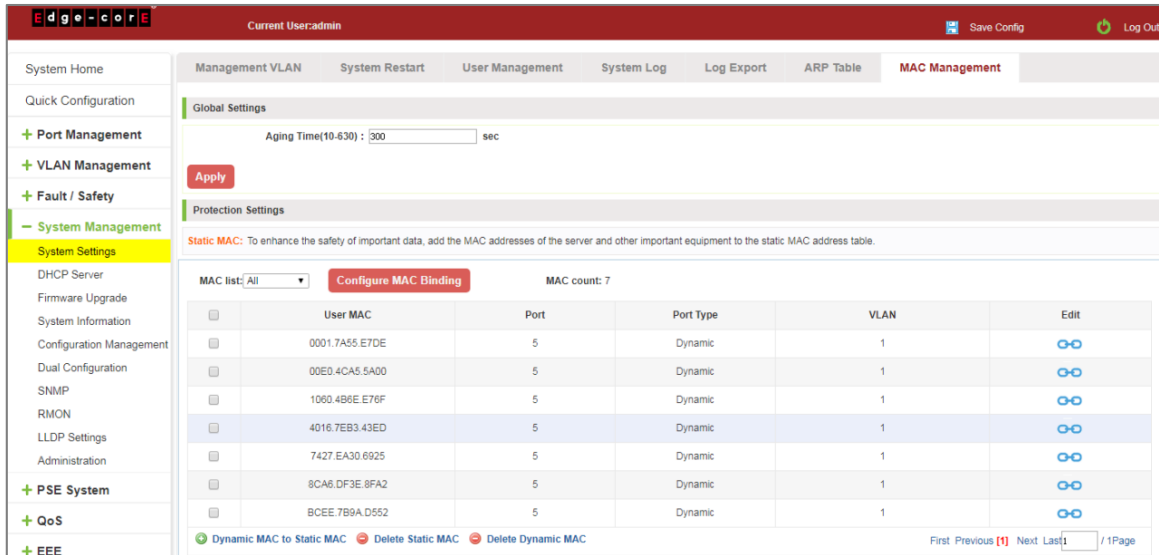
Figure 7-7: ARP Table

Click the Clear ARP Table Entries button to clear the switch's ARP table.

## 7.1.7 MAC management

### 7.1.7.1 MAC address lookup

Click "System Management" "System Settings" "MAC Management" to view and query the switch MAC address information.



**Figure 7-8: MAC address Lookup Display**

The MAC address list shows the current switch port learned MAC addresses:

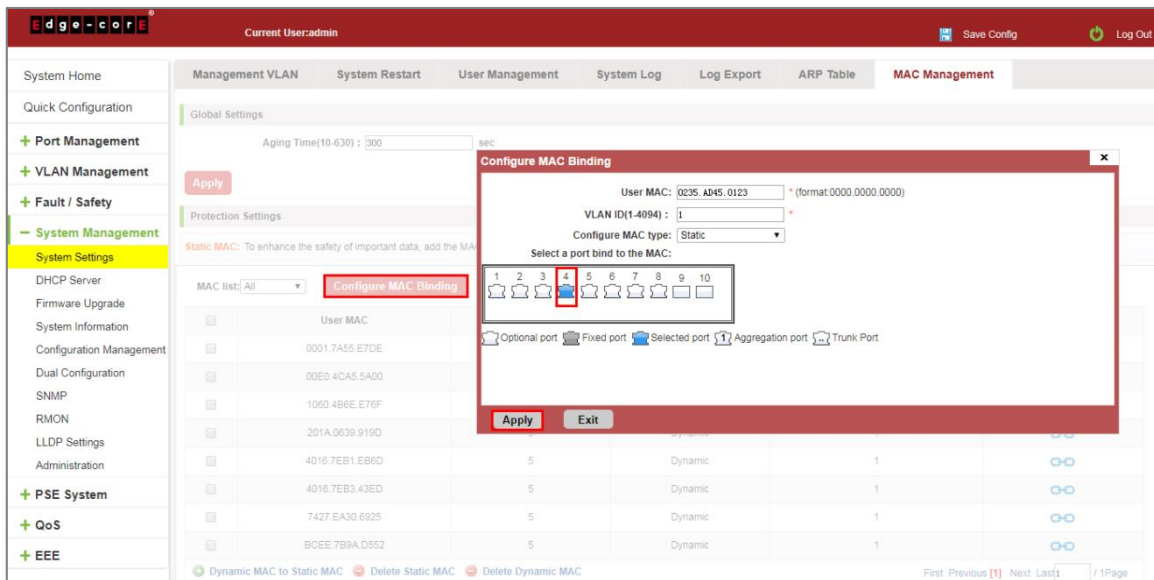
- **User MAC:** MAC address of the connected device
- **Port:** Switch port connected to the device MAC address;
- **Port Type:** How the MAC was configured on the port: Learned (Dynamic) Configured (Static)
- **VLAN:** The VLAN ID for the port within which the device connected.

You can query the MAC address type according to the type of MAC address (All/static/dynamic) using the drop-down menu **MAC list**.

### 7.1.7.2 Add a static MAC address type

1. To manually bind a MAC address:

Click "Configure MAC Binding" and follow the steps below to configured a MAC address manually.



**Figure 7-9: MAC Addresses Statically Bound Static Configuration**

Configuring a MAC address manually:


Step 1: Click the Configure MAC Binding button.


Step 2: In the "User MAC" text box enter the MAC address, for example B861.6FA8.C187

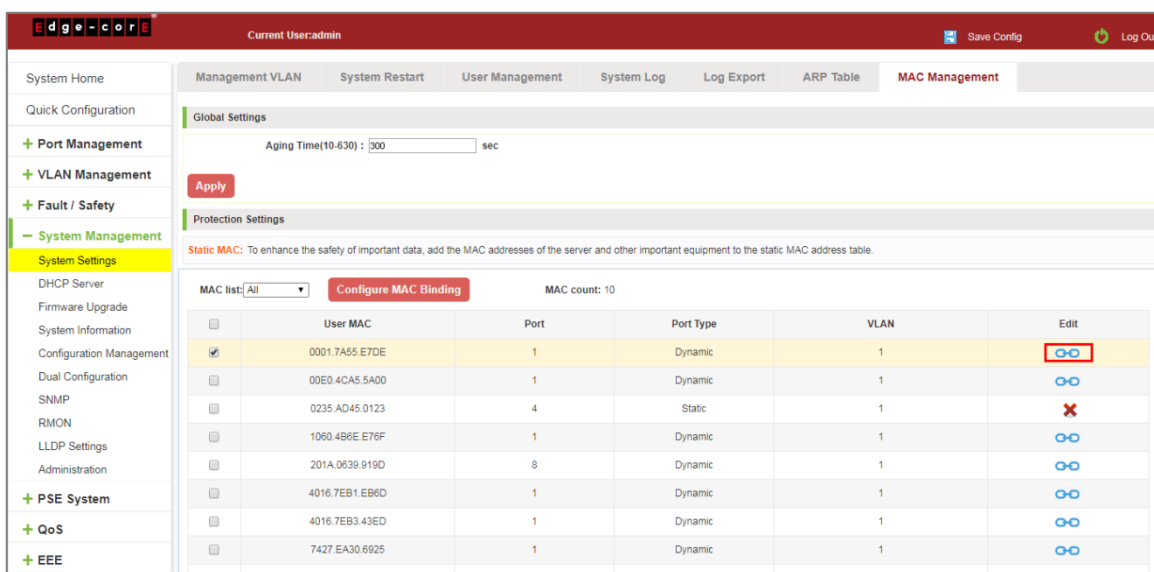
Step 3: In the VLAN ID text box enter the VLAN ID, for example the default VLAN ID 1.

Step 4: Select the port in the port panel to bind the MAC address to.

Step 5: Click Apply.

2. Use the  icon to edit a MAC address binding.

In the MAC address list, find the MAC address and click the  icon to edit the Port and VLAN as necessary. Then click check the checkbox next to the User MAC address and click the Configure MAC Binding button statically configure the MAC address to the port and VLAN configured.



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

3. Using the Dynamic MAC to Static MAC button to bulk link dynamic MAC address and bind them as a static MAC address.
  1. In the MAC address list check the checkbox next to the Dynamic MAC address to be bound as a static MAC.
  2. Click the Dynamic MAC to Static MAC button to bind the dynamic MAC address as a static address.

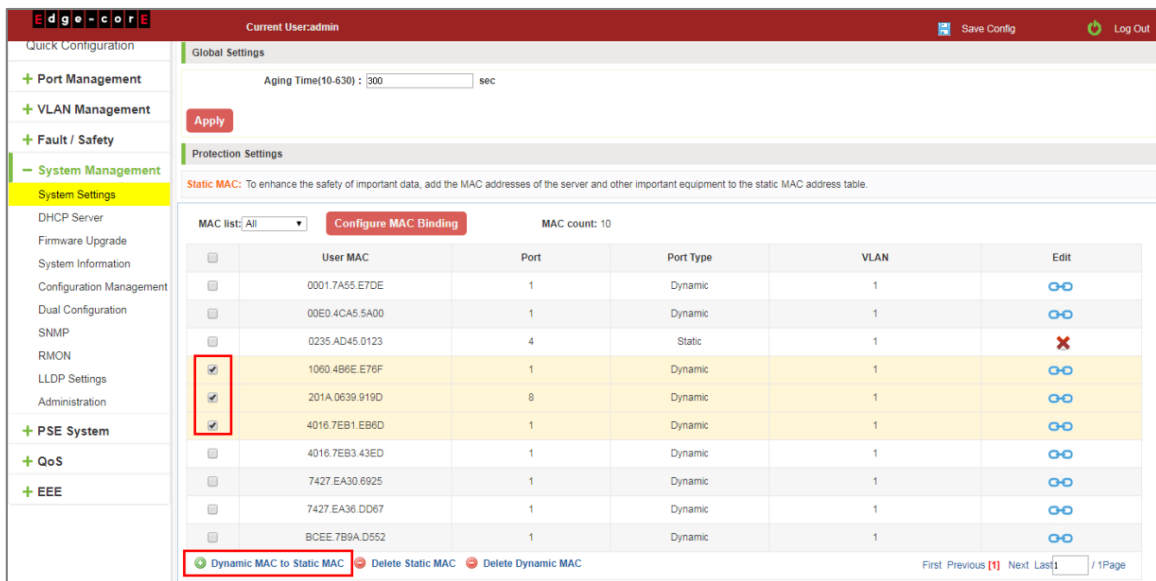


Figure 7-11: Batch-MAC Binding Dynamic Address as Static

### 7.1.7.3 Batch Deleting static MAC addresses

1. In the MAC address list check the checkbox next to the Static MAC address(es) to be deleted.
2. Click the Delete Static MAC button to delete the MAC address(es).

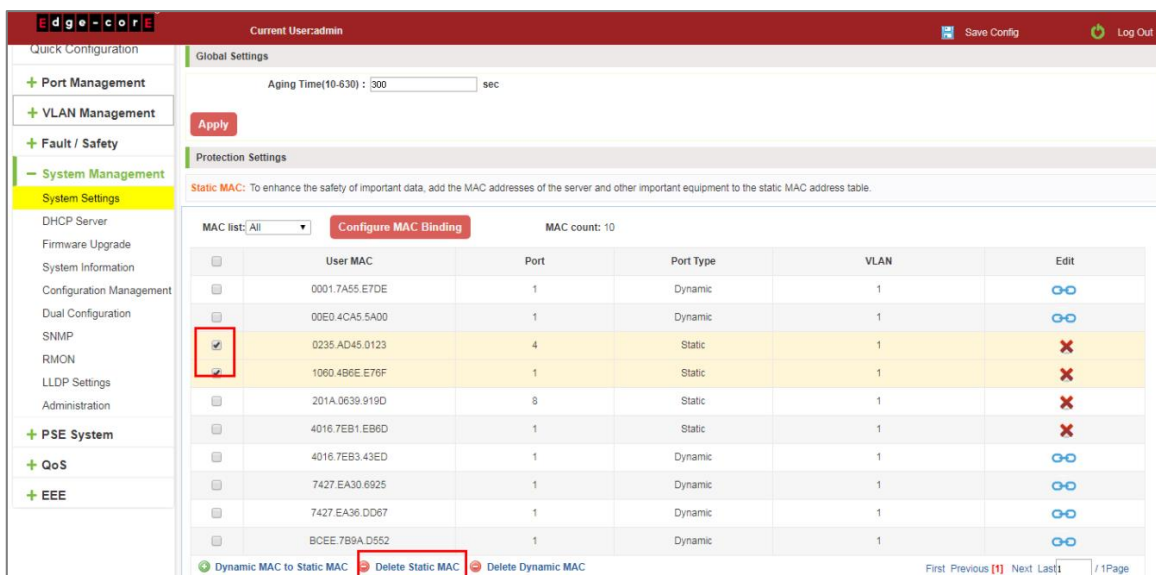


Figure 7-12: Batch MAC Address Deletion

### 7.1.7.4 Delete a single static MAC address

To delete a single static MAC address:

Step 1: In the MAC address list find the static MAC address binding to delete.

Step 2: Click the **X** icon under the Edit column to delete the MAC address binding from the MAC list.

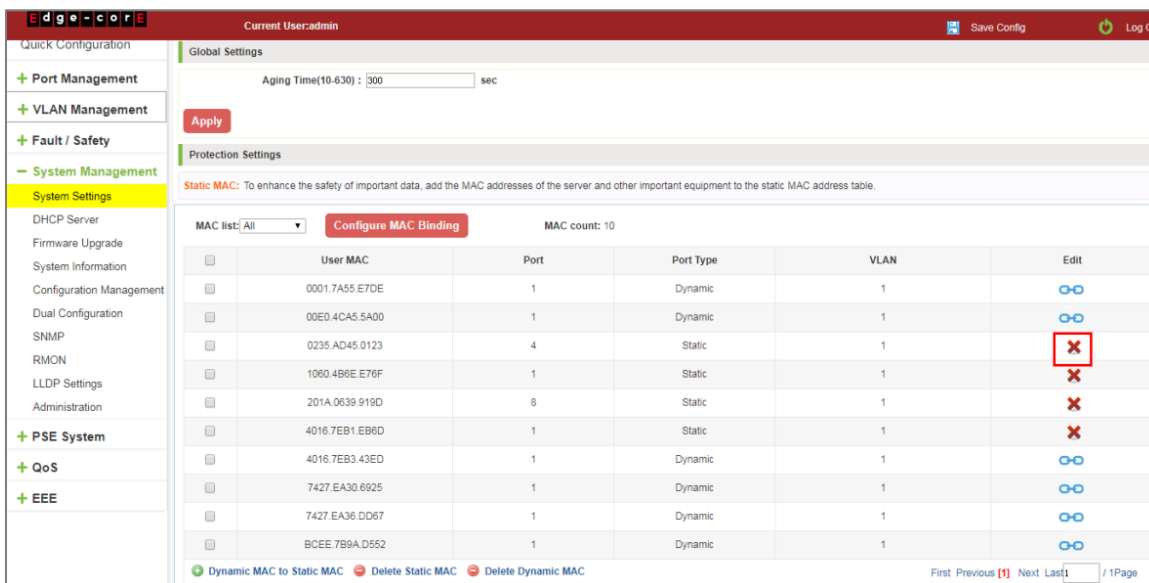


Figure 7-13: MAC Address Deletion

### 7.1.7.5 Delete all dynamic MAC address

In the MAC address list, click the Delete Dynamic MAC button to clear all dynamic MAC addresses bindings from the MAC list.

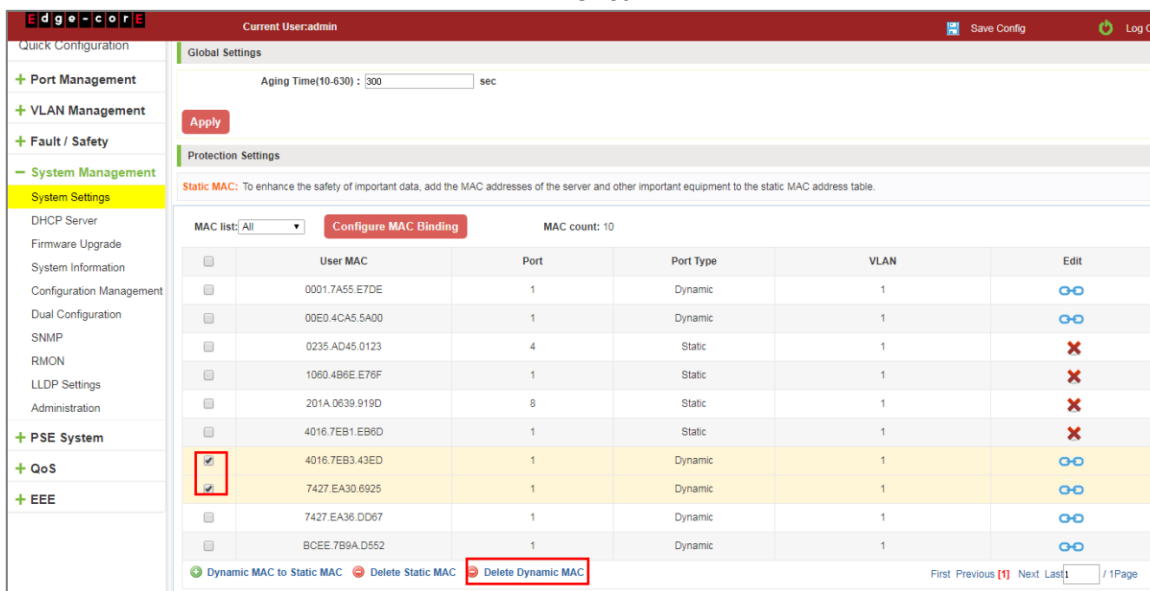


Figure 7-14: Clear All Dynamic MAC Address

## 7.2 DHCP SERVER

### 7.2.1 DHCP server info

Click "System Management" "DHCP Server" to view and enable the DHCP Server configuration.

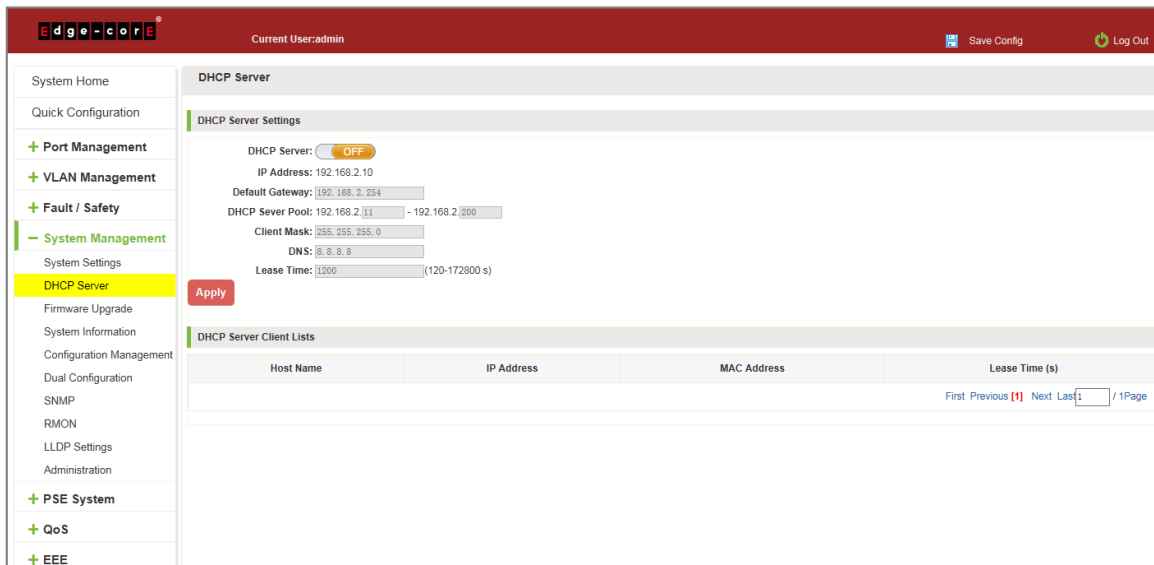


Figure 7-15: Viewing the DHCP Server Configuration

### 7.2.2 Enabling the DHCP server

To enable the DHCP server, the DHCP IP address pool range and switch device IP must be within the same network segment.

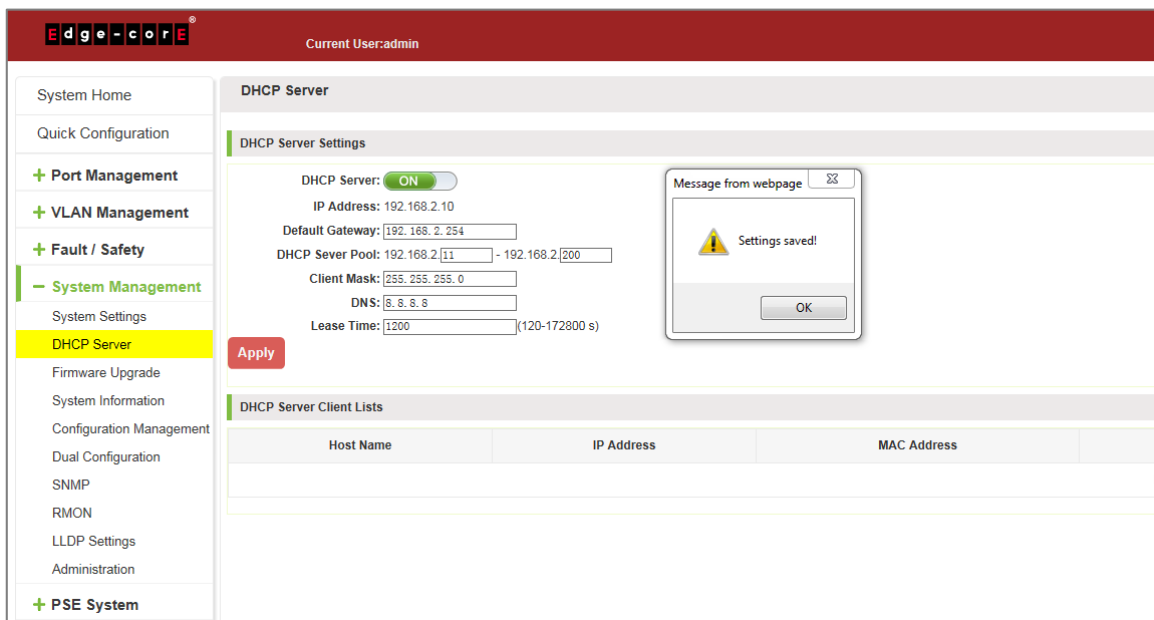


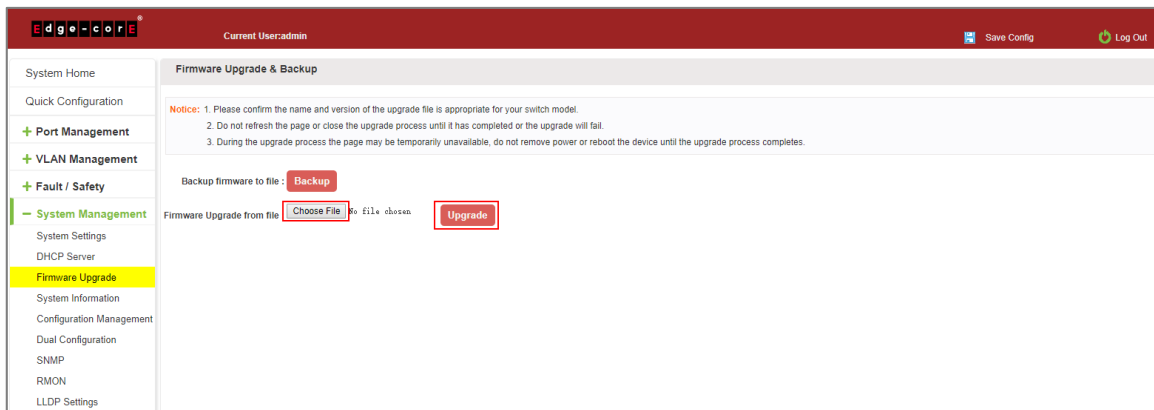
Figure 7-16: Enabling the DHCP Server

When a host client connects to the switch's network segment and sends DHCP requests, the IP assigned to the client from the switch's DHCP server will be displayed in the DHCP server client list.



## 7.3 SYSTEM UPGRADE

Click "System Management" "Firmware Upgrade" to upgrade the switch's firmware.



**Figure 7-17: Upgrading the Switch Firmware**

To upgrade the firmware:

Step 1: Click the Choose File button to select a switch upgrade file.

Step 2: Click the Upgrade button switch to execute the new firmware upgrade.

Step 3: When the upgrade progress bar is at 100%, the switch will automatically reboot. When the switch finishes rebooting the firmware upgrade is completed.

## 7.4 SYSTEM INFORMATION

### 7.4.1 Memory information

Click "System Management" "System Information" "Memory Information" to view the current memory allocation of the switch.

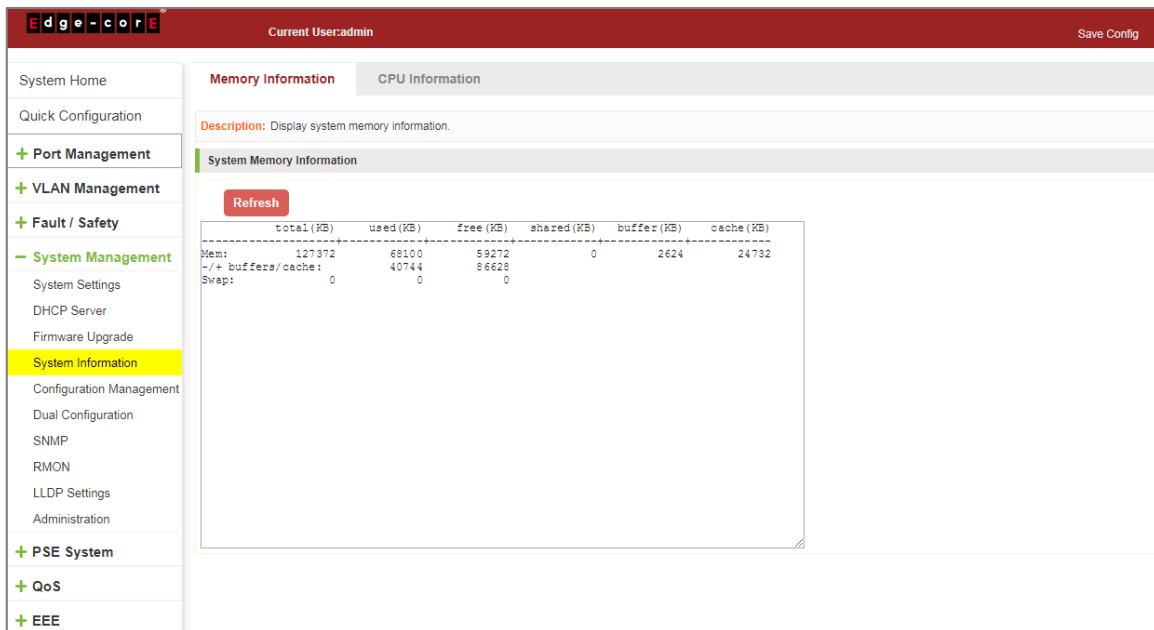


Figure 7-18: Viewing the System Memory Information

Click the Refresh button to update the memory allocation.

## 7.4.2 CPU information

Click "System Management" "System Information" "CPU Information" to view the details of the current process execution queue of the switch.

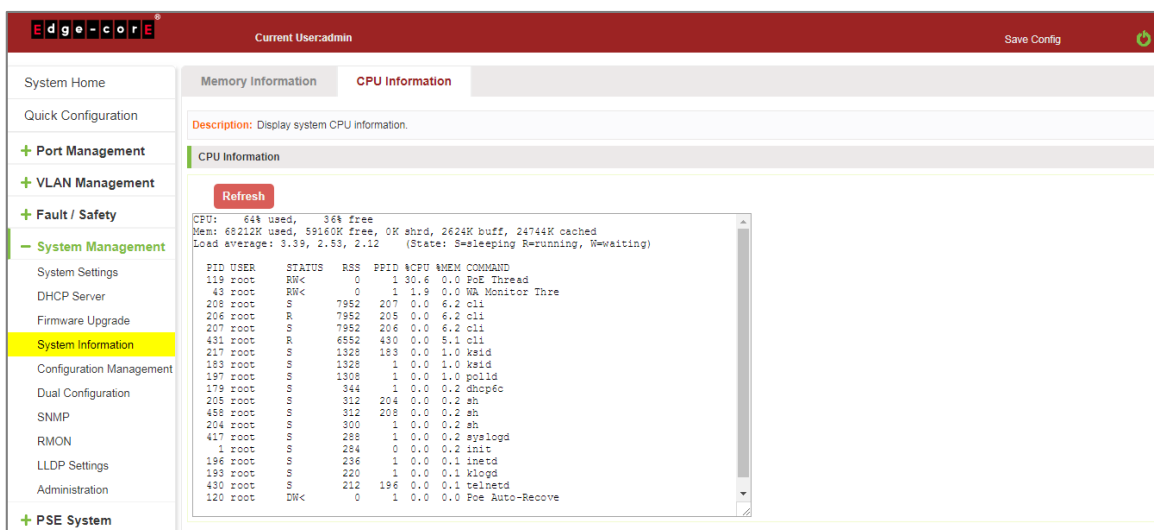


Figure 7-19: Viewing the CPU Information

To refresh the process execution queue, click the Refresh button.

## 7.5 CONFIGURATION MANAGEMENT

### 7.5.1 Configuration management

1. To view the switch's current configuration:

Click "System Management" "Configuration Management" "Configuration Management", and click the View The Current Configuration button.

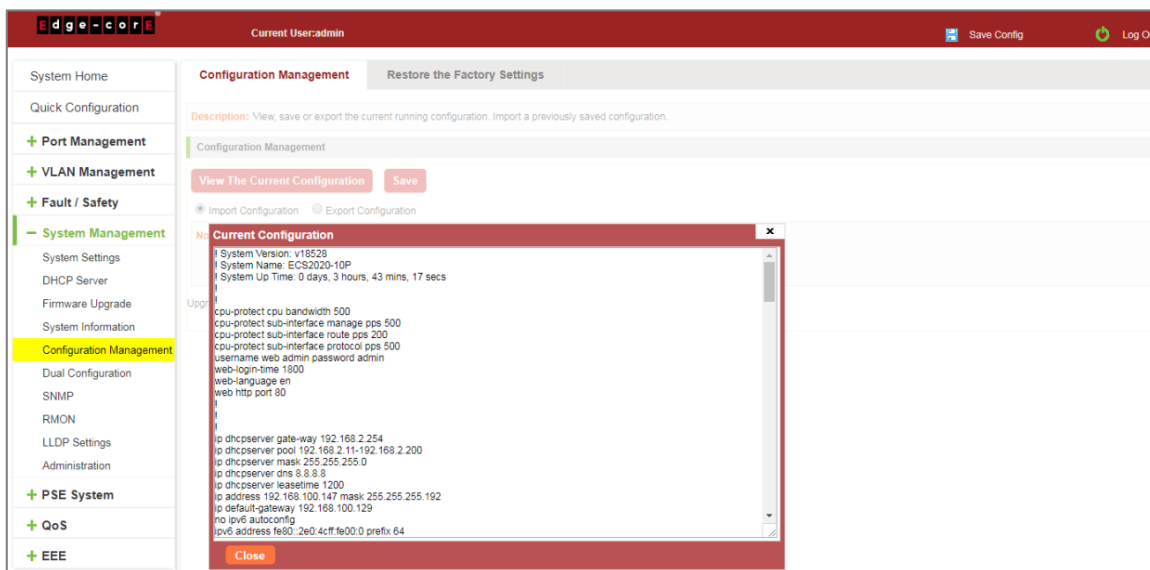


Figure 7-20: Viewing the Current Configuration

2. To save the current configuration of the switch:

Click "System Management" "Configuration Management" "Configuration Management", and then click the Save button, the running configuration of the switch will be saved to the startup configuration file.

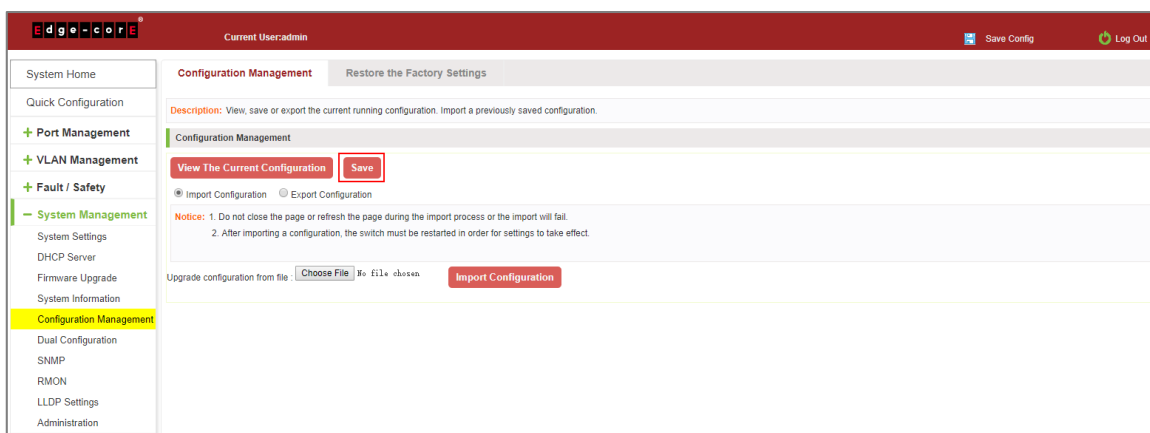


Figure 7-21: Saving the Current Configuration

3. To import a new switch configuration file:

Click "System Management" "Configuration Management" "Configuration Management"

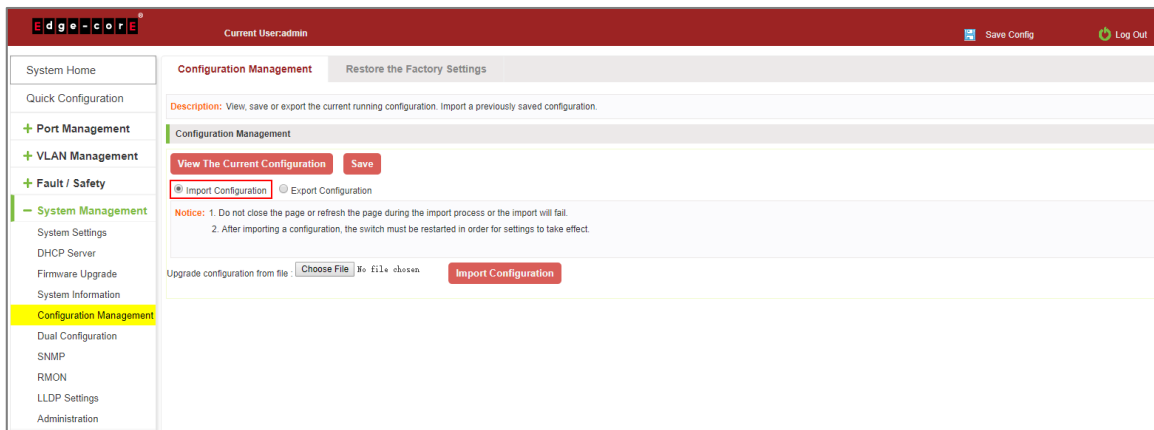


Figure 7-22: Importing a Configuration

To import a configuration file:

Step 1: Select the Configuration Management tab.

Step 2: Click the "Choose File" button to select the configuration file to be imported from the switch's file system.

Step 3: Click the Import Configuration button.

Step 4: In the restart confirmation dialog box, click to confirm the restart.

4. To export the current configuration file from the switch:

Select the Export Configuration radio button in the "System Management" "Configuration Management" "Configuration Management" tab and then click the Export Configuration button.

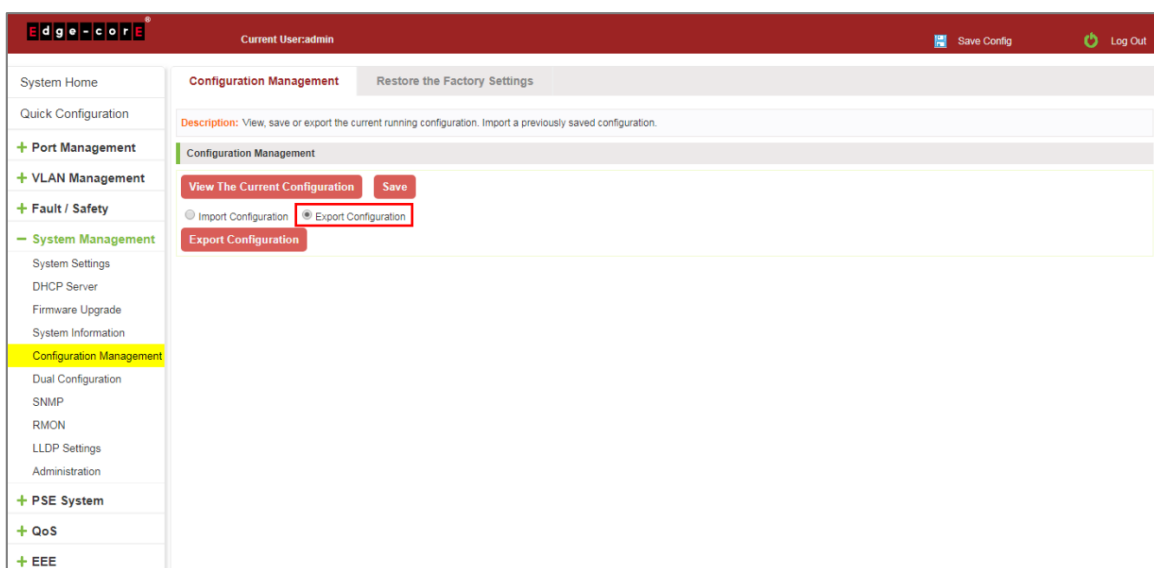
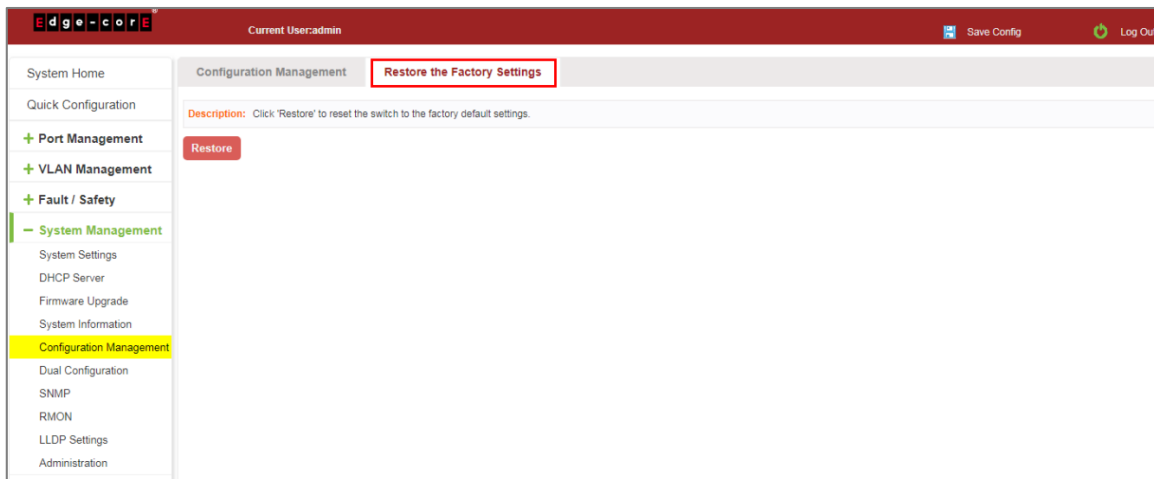


Figure 7-23: Exporting the Configuration

### 7.5.2 Restore the factory default settings

Click "System Management" "Configuration Management" "Restore the Factory Settings" to restore the switch to the default factory settings.



**Figure 7-24: Restoring the Factory Settings**

To restore the switch to factory default settings:

Step 1: Select the "Restore the Factory Settings" tab under "System Management" "Configuration Management".

Step 2: Click the Restore button and click OK in the pop-up confirmation box.

Step 3: After the switch reboots it will be restored to the factory default settings.


## 7.6 DUAL CONFIGURATION

### 7.6.1 To Backup and restore the current configuration file

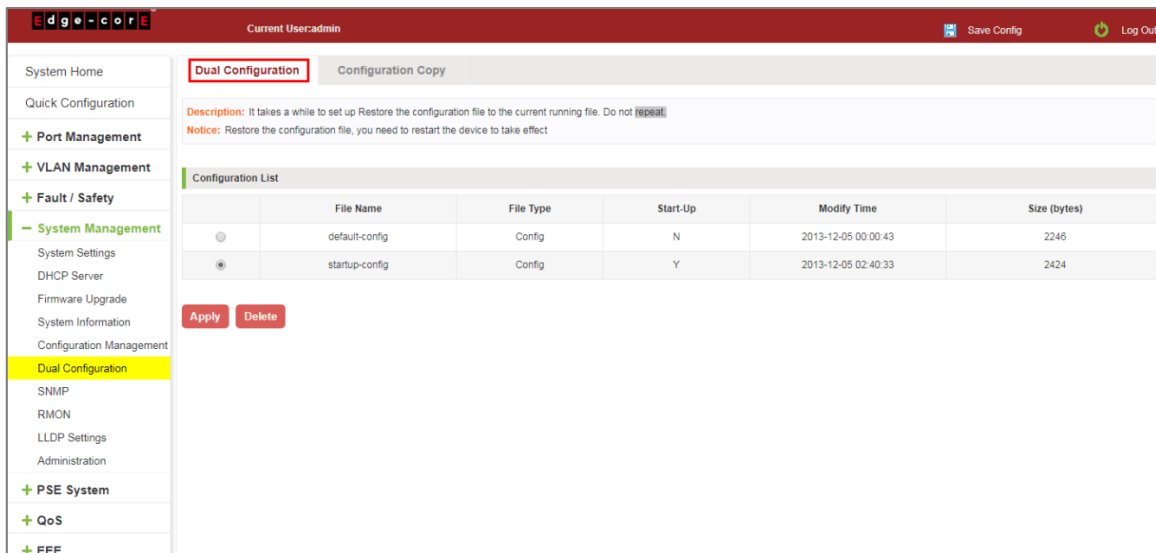
The system maintains two configuration files: "default-config" and "startup-config". Further a backup configuration file can also be created. You can use the dual configuration page to apply any current running configuration settings to any to the startup and backup configuration files and set any of the three files as the startup configuration file.

Click "System Management" "Dual Configuration".

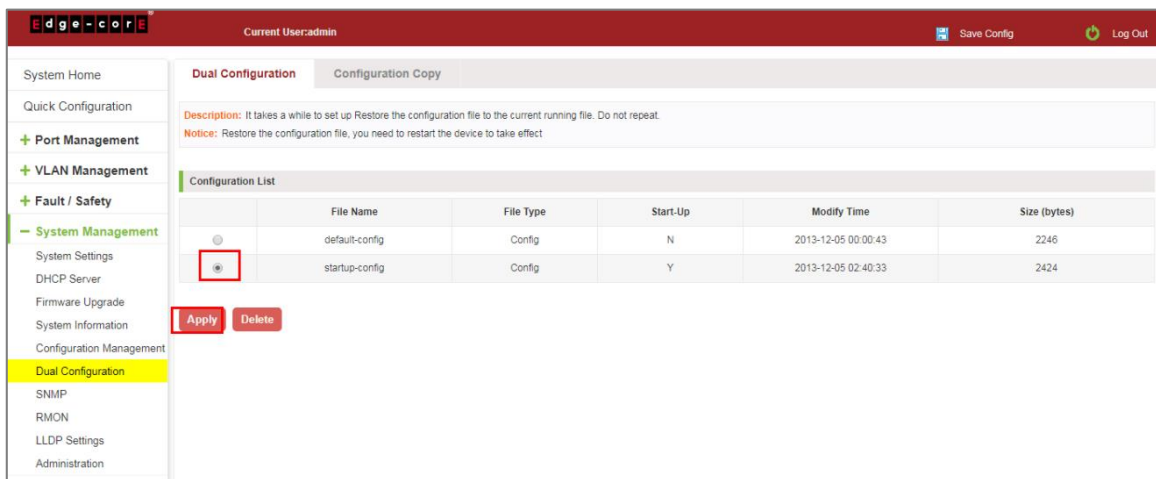
---

 Note: Use the Configuration Copy tab to create a "backup-config" file if it does not exist on the file system.

---




1. Click the radio button in the left column and then click apply to set the file as the Start-Up configuration file (Start-Up flag is set to Y).



2. Further, when the Apply button is clicked, the system will update the selected file with the current running configuration settings. Use the "Delete" button to delete the backup configuration file if it has been created.

---


 **Note:** The "default-config" configuration file will not be updated with the current running parameters.

---

## 7.6.2 Configuration Copy

Use the "Configuration Copy" tab to copy the running configuration to either the "startup-config" file or "backup-config" file.

---

 **Note:** If the "backup-config" file does not exist a new file will be created.

---

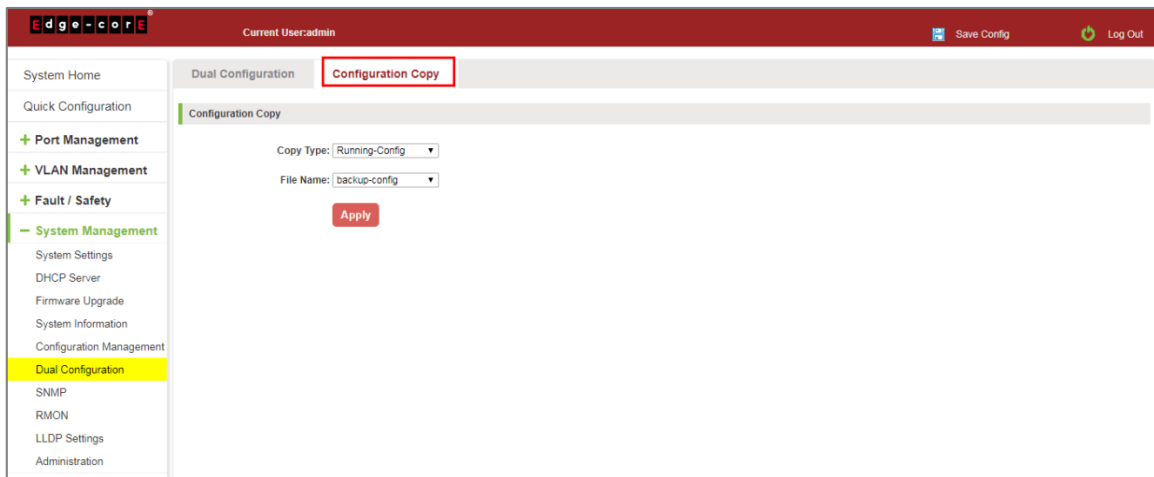


Figure 7-25: Saving the Running-Config

## 7.7 SNMP

### 7.7.1 Viewing the SNMP Configuration

Click "System Management" "SNMP" to view the SNMP configuration.

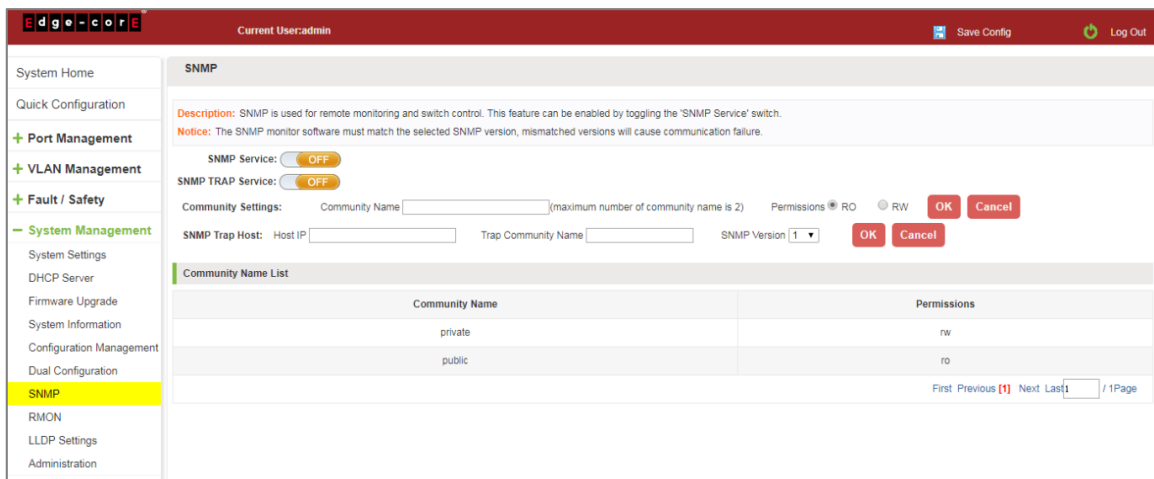


Figure 7-26: Viewing the SNMP Configuration Information



**Note 1:** By default SNMP is disabled.



**Note 2:** The SNMP version used by external SNMP monitoring software used and the switch must be the identical.

### 7.7.2 Enabling SNMP

Click "System Management" "SNMP", and then click the SNMP service OFF slider and wait for the pop-up dialog box and Click "OK". The SNMP Service slider should change to ON.

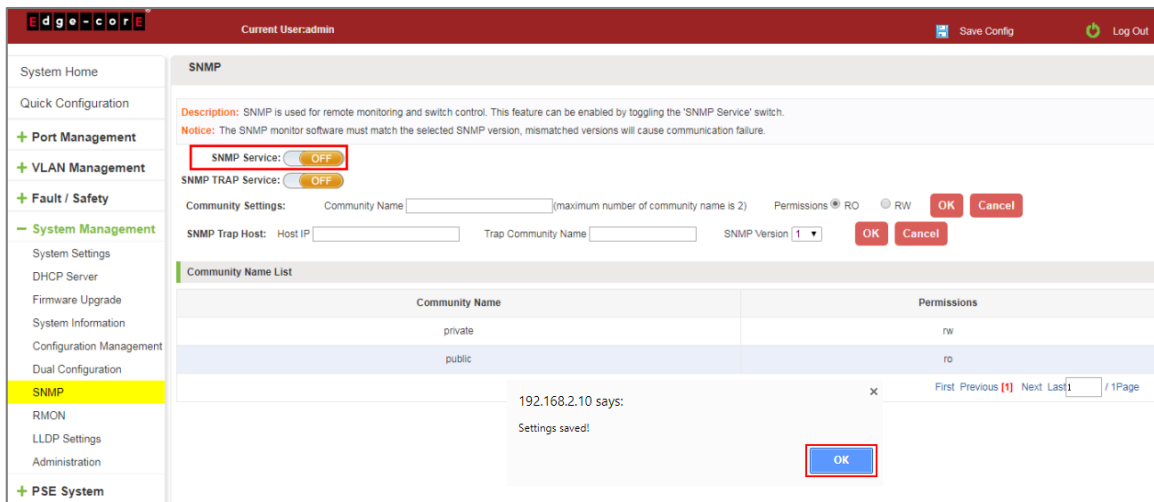


Figure 7-27: Activation SNMP Function

### 7.7.3 Disabling SNMP

Click "System Management" "SNMP", and then click the SNMP service button ON and wait for the pop-up dialog box and Click OK. The SNMP Service slider will change to OFF.

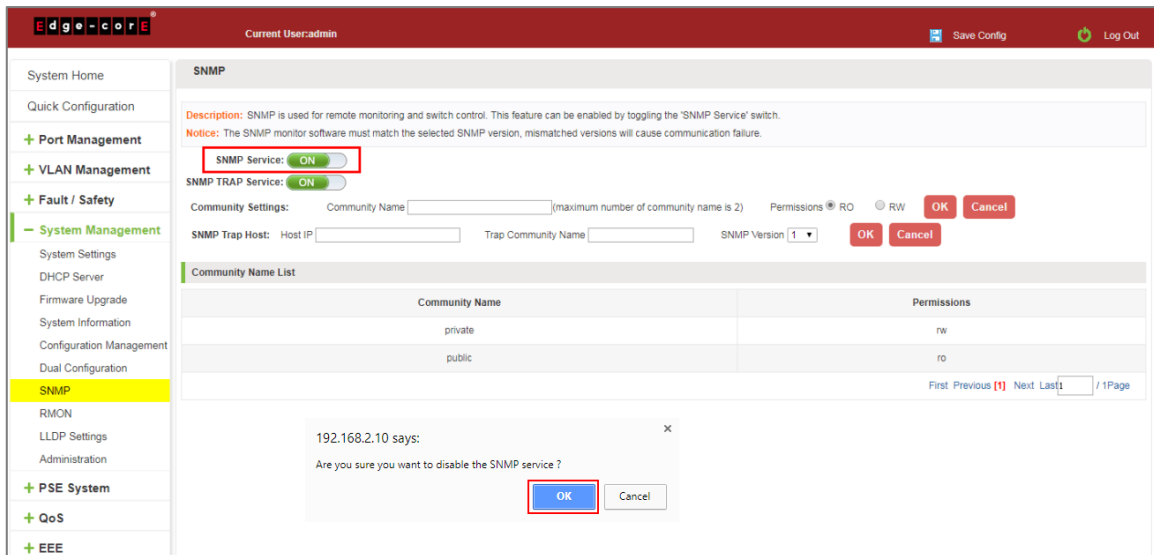


Figure 7-28: Disable the SNMP Function

### 7.7.4 Enabling SNMP TRAPS

With SNMP enabled, click the OFF slider next to SNMP TRAP service and click OK in the confirmation box. the SNMP TRAP Service slider will change to ON.



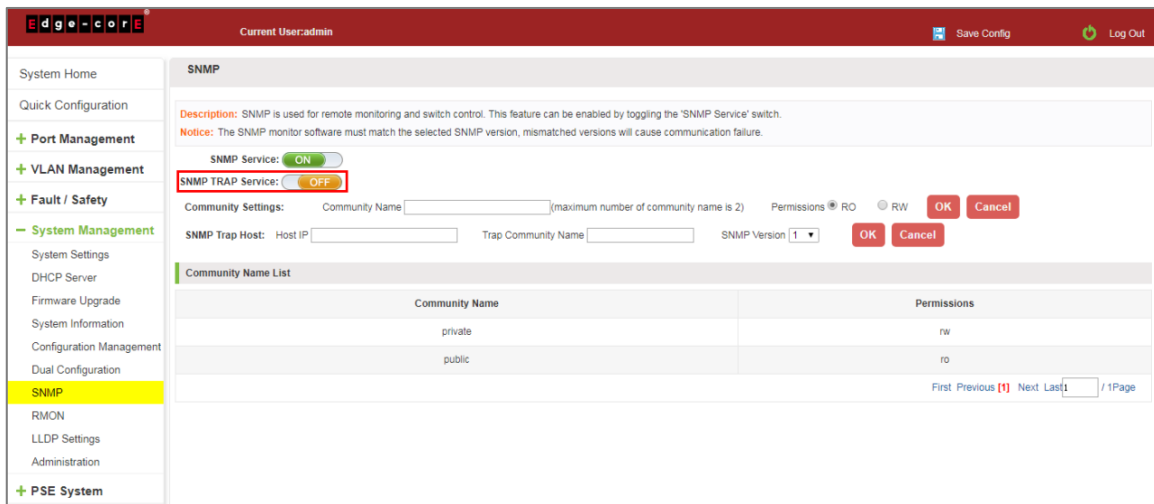


Figure 7-29: Enabling TRAPs

### 7.7.5 Disabling SNMP TRAPs

Click the ON slider next to SNMP TRAP service and click OK in the confirmation box – the SNMP TRAP Service slider will change to OFF .

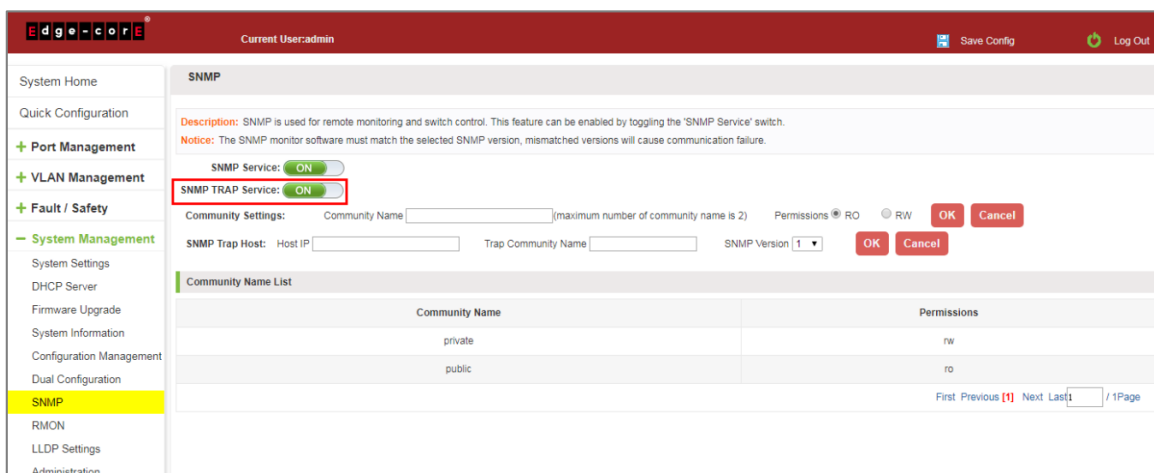


Figure 7-30: Disabling TRAPs

### 7.7.6 Modifying the Community name and permissions

Click "System Management" "SNMP", and in the community name text box input the community name for example: *public*. Then in the radio buttons next to Permissions, select either: *RO* – Read Only or *RW* – Read and Write and finally click the OK button to complete the configuration.

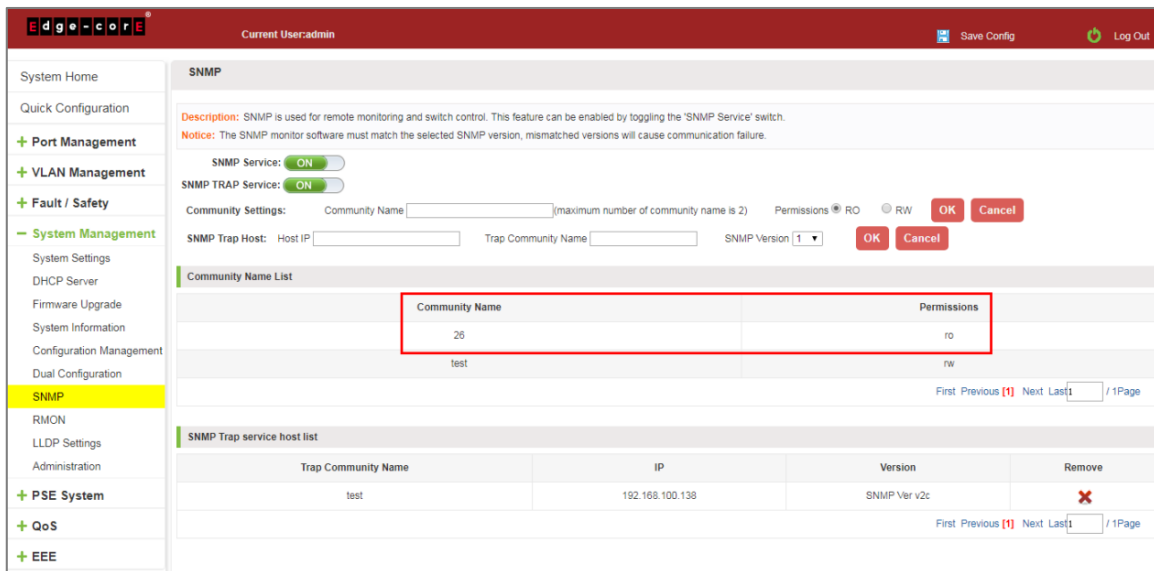



Figure 7-31: Modifying the Community Name and Permissions

### 7.7.7 Adding an SNMP TRAP service host

Click "System Management" "SNMP" and in the **SNMP Trap Host - Host IP** text box input for example: *192.168.100.150*, **TRAP Community Name:** *pub*, **SNMP Version:** *2C* then click the **OK** button to complete the configuration.

 **Note:** these are example settings – make sure to use the IP and SNMP settings of your SNMP Management Software.

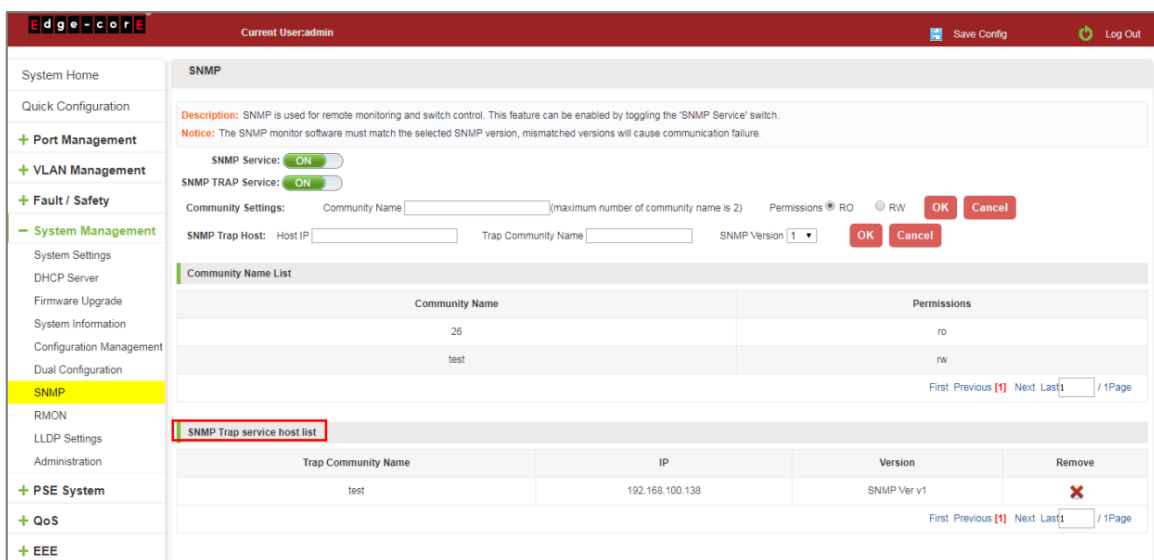



Figure 7-32: Adding an SNMP TRAP Service Host

### 7.7.8 Deleting an SNMP TRAP service host

To delete a configured SNMP Trap Service Host, click "System Management" "SNMP" and in the SNMP TRAP service host list click the  icon and then click **OK** in the confirmation box to delete the host.

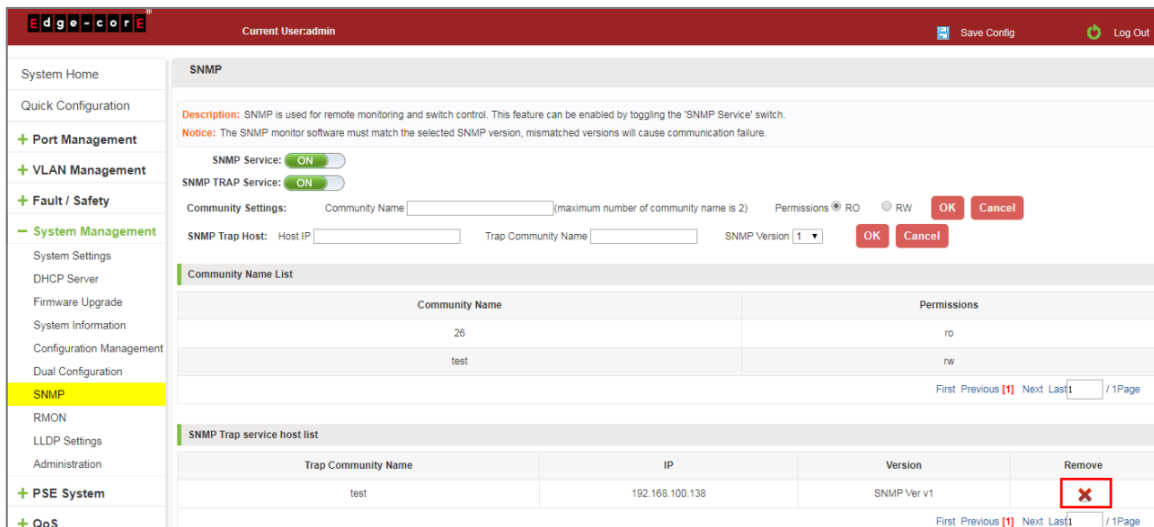


Figure 7-33: Deleting an SNMP Trap Service Host

## 7.8 RMON

### 7.8.1 Viewing the RMON configuration

Click "System Management" "RMON", to view the RMON configuration.

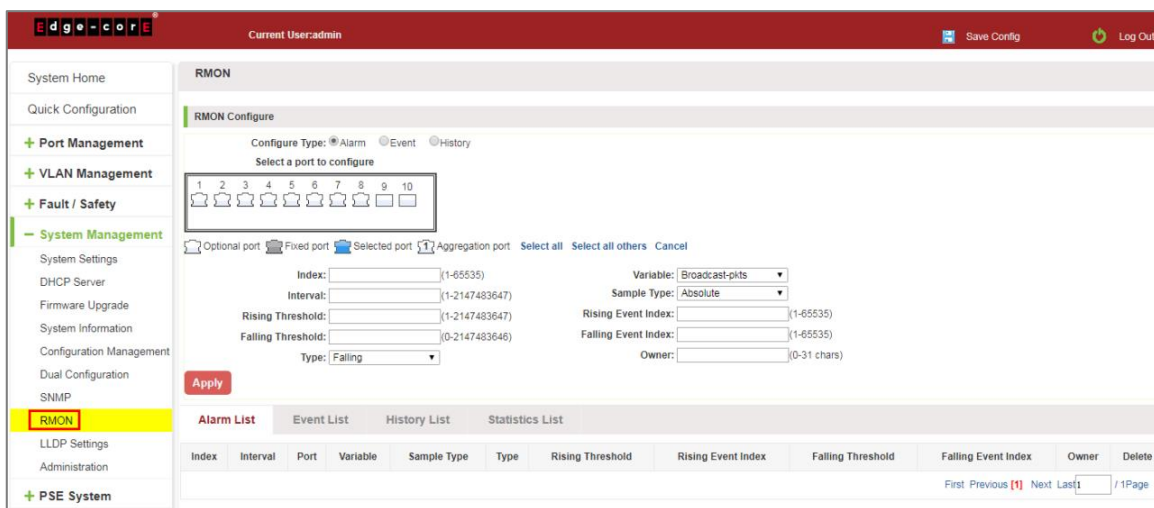


Figure 7-34: Viewing the RMON Configuration

### 7.8.2 Configuring an RMON Alarm

To configure an RMON Alarm select the port(s) to be configured and then use the example settings in Figure 7-35: Configuring an RMON Alarm and click the Apply button.

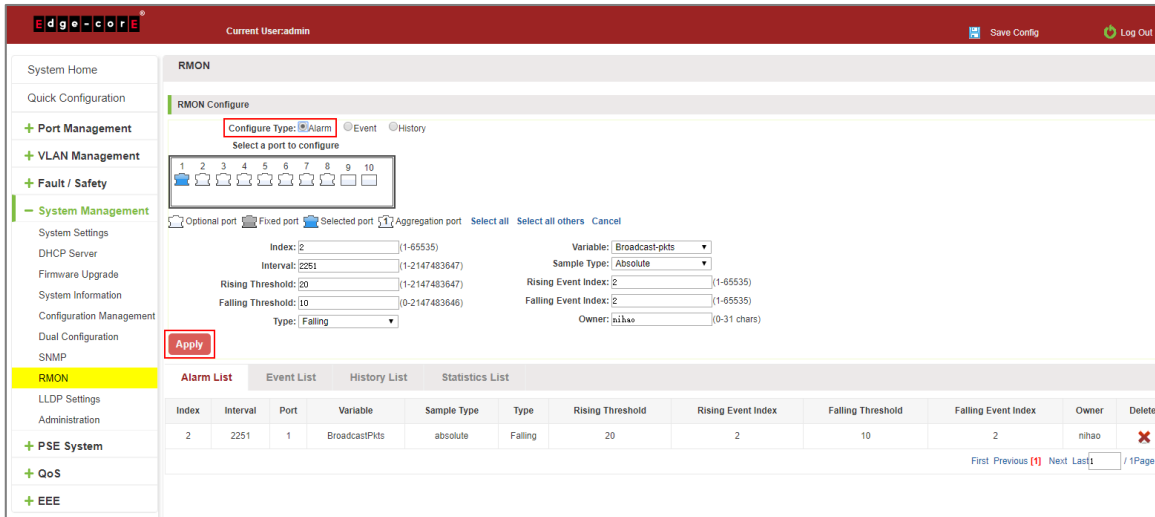


Figure 7-35: Configuring an RMON Alarm

**Note 1:** To configure the RMON Alarm Rising and Falling Event Index the EVENTS should be configured first using the Event Radio button next to Configure Type at the top of the page.

**Note 2:** The Rising Threshold must be greater than the Falling Threshold.

### 7.8.3 Modifying an RMON event or history

Click either the Event or History radio button in the RMON configuration page and set the configuration accordingly. Make sure the Community parameter matches the existing SNMP Community name. Click Apply after making any changes.

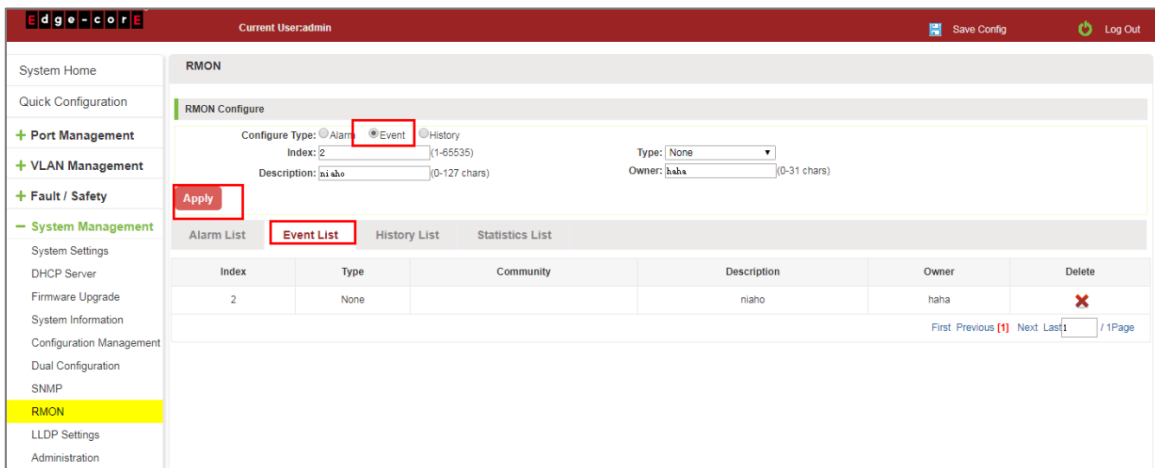


Figure 7-36: Modifying an RMON Event

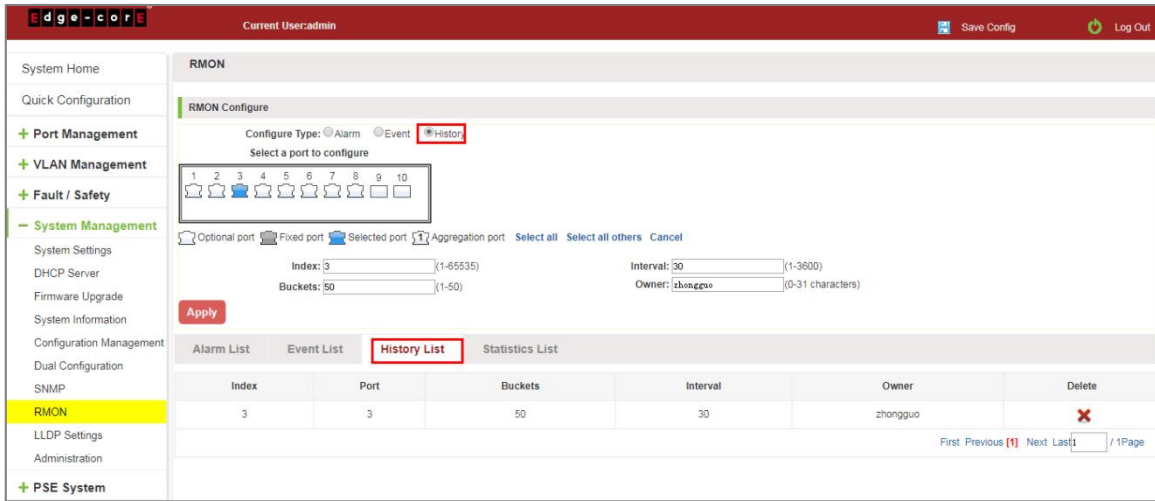


Figure 7-37: Modifying an RMON History Configuration

When the RMON configuration is completed, click the Statistics List and choose a port to view its associated RMON statistics.

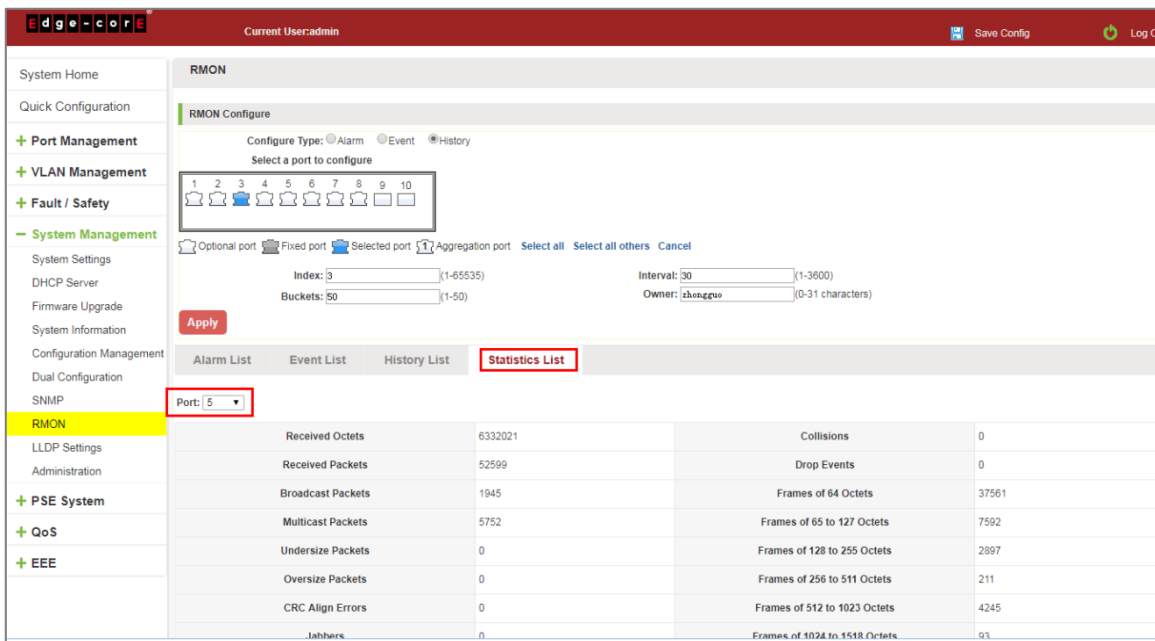



Figure 7-38: Viewing Port RMON Statistics

### 7.8.4 Deleting an RMON rule

Select the Configure Type: Alarm, Event or History and then the entry you want to delete. Click the  icon on the right to delete the rule entry.

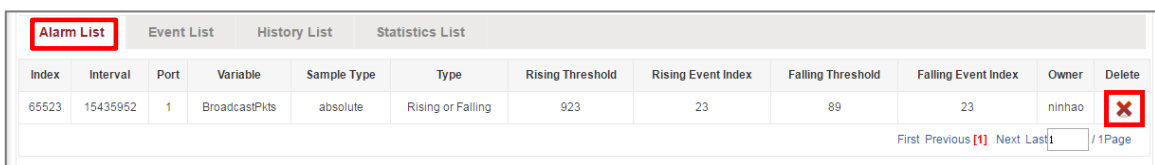


Figure 7-39: Deleting an Alarm List Rule

Alarm List	Event List	History List	Statistics List			
Index	Type	Community	Description	Owner	Delete	
23	Log and Trap	public	1652fdfswe	ninhao		

First Previous [1] Next Last 1 / 1Page

Figure 7-40: Deleting an Event List Rule

Alarm List	Event List	History List	Statistics List			
Index	Port	Buckets	Interval	Owner	Delete	
23	1	50	3500	ninghm		

First Previous [1] Next Last 1 / 1Page

Figure 7-41: Deleting an History List Rule

## 7.9 LLDP SETTINGS

### 7.9.1 Viewing LLDP settings

Click "System Management" "LLDP Settings" to view the LLDP settings. The LLDP Global Set is disabled by default.

Figure 7-42: Viewing the LLDP Configuration

### 7.9.2 Enabling LLDP settings

In the LLDP Global Set tab click the drop down menu next to LLDP: and select enable. Then make any changes to the Global Set parameters and click Apply.

To modify the switch action when receiving LLDP PDUs use the LLDP PDU Set drop down menu to select either flooding, bridging or filtering.

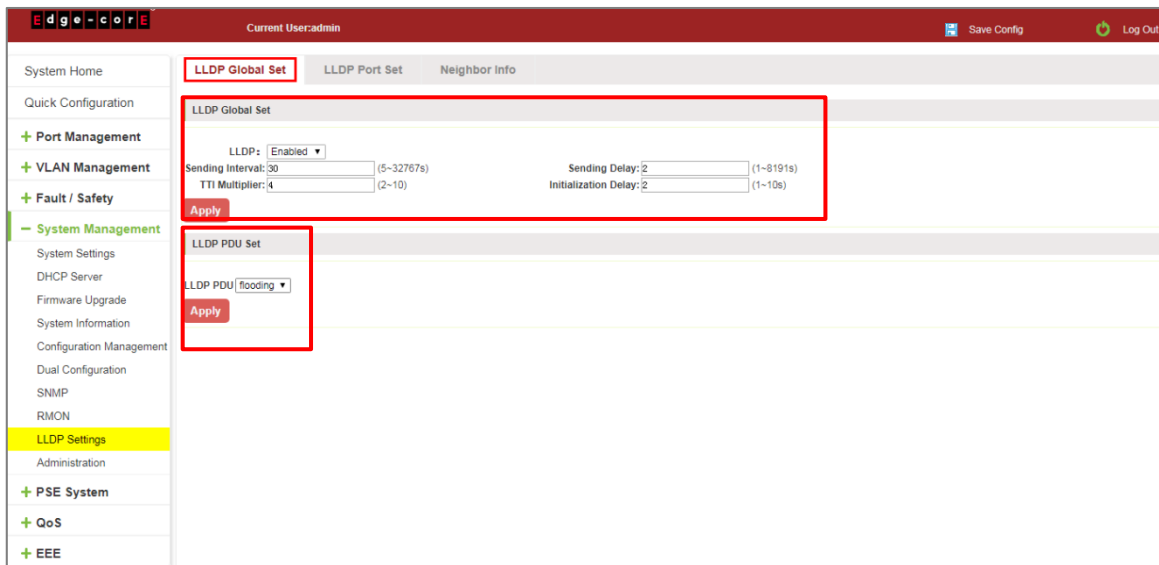


Figure 7-43: Enabling LLDP

### 7.9.3 LLDP port set

Select the LLDP Port Set tab to modify the individual LLDP port behavior to either Disabled, RX, TX or RX,TX.

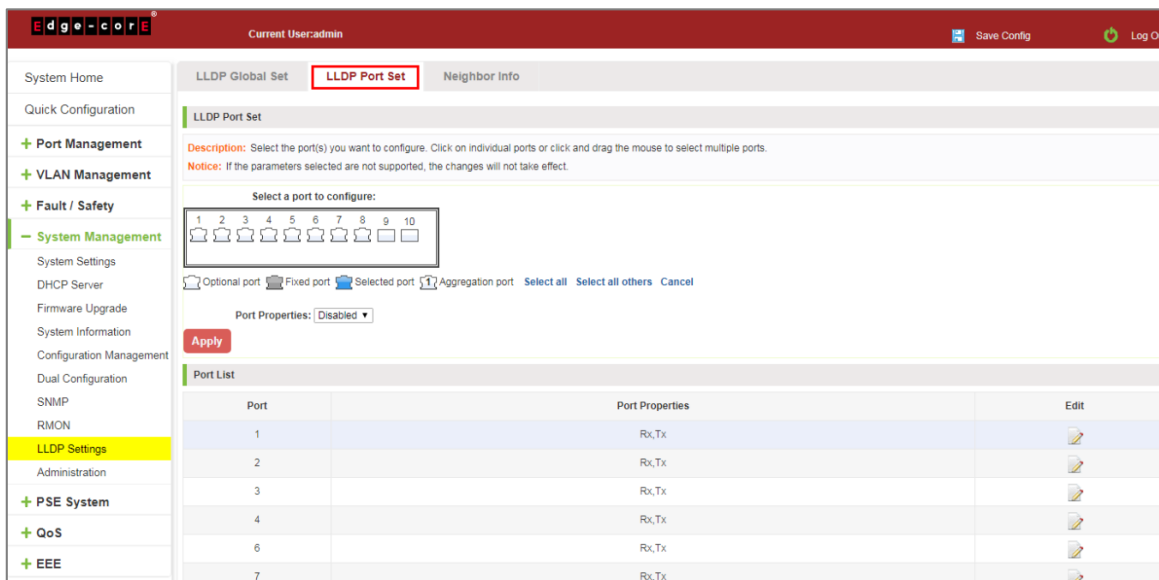


Figure 7-44: Setting the LLDP port properties

### 7.9.4 Neighbor info

When the LLDP function is enabled, neighbor information will be recorded when a neighbor device is found.

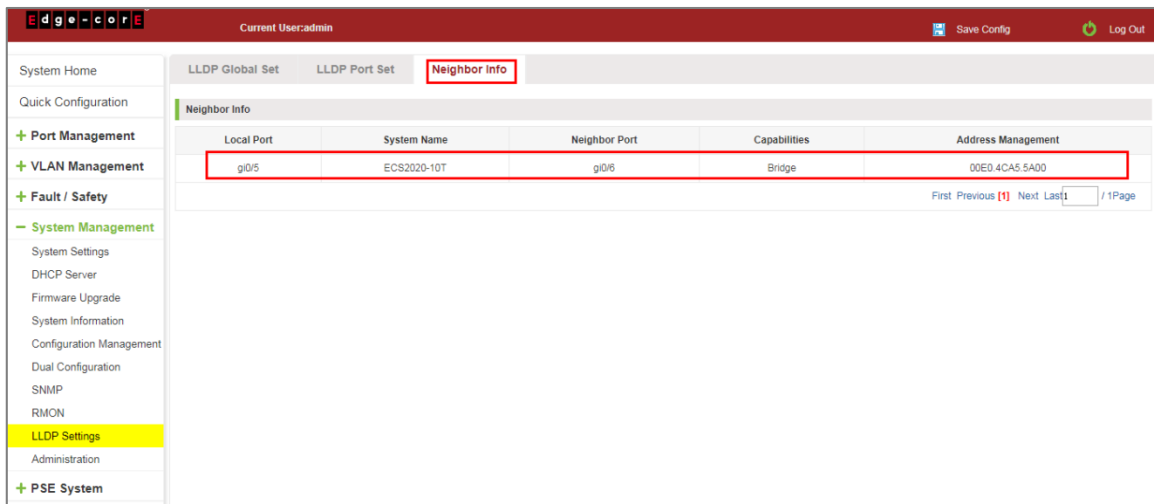


Figure 7-45: Viewing LLDP Neighbors

## 7.10 ADMINISTRATION

### 7.10.1 Viewing the Telnet, HTTPS and SSH settings

Click "System Management" "Administration, "Administration Settings" to view the settings. Telnet is enabled by default and HTTPS is enabled by default and SSH is disabled by default.

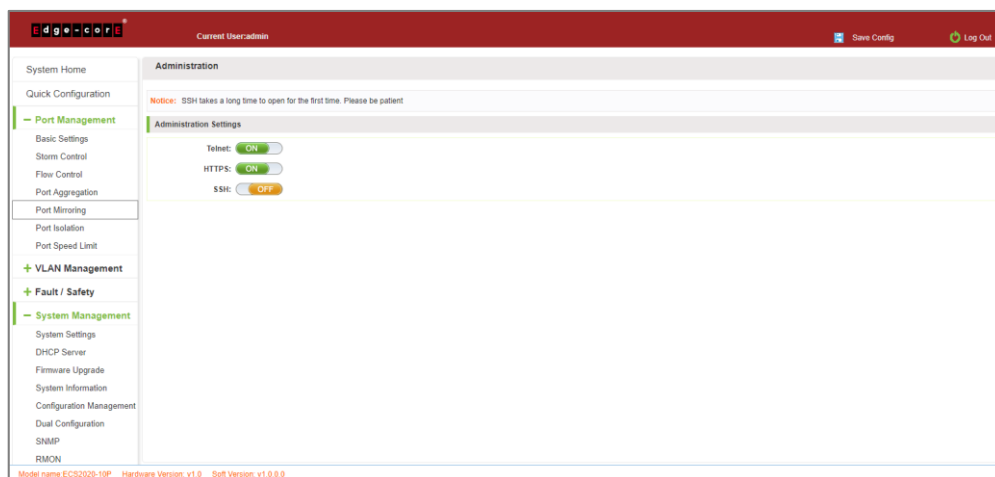


Figure 7-46: Viewing the Telnet, HTTPS, and SSH Settings

### 7.10.2 Enabling Telnet

Click the OFF slider next to Telnet: and click OK in the pop-up confirmation box to enable the Telnet.



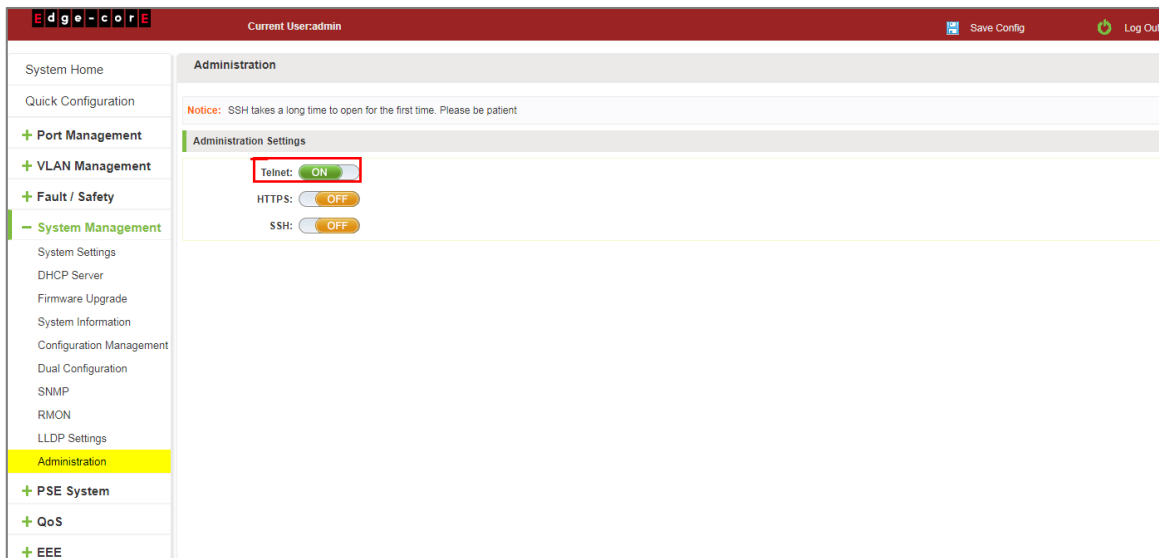


Figure 7-47: Enabling Telnet

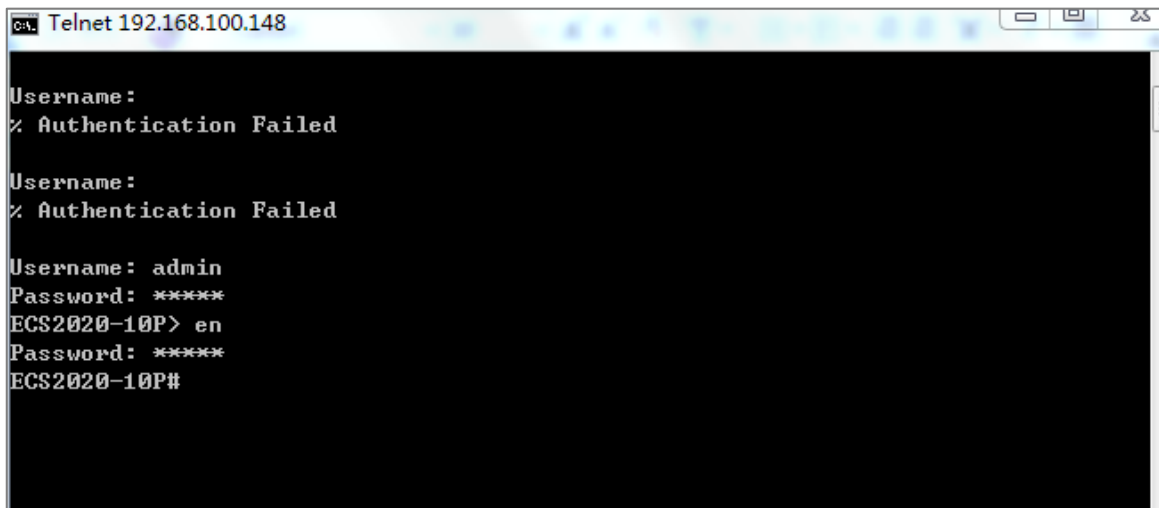


Figure 7-48: Telnet Login

### 7.10.3 Enabling HTTPS

Click the OFF slider next to HTTPS: and click OK in the pop-up confirmation box to enable the HTTPS. Once enabled a user can login to the Web Browser Management interface using HTTPS protocol.

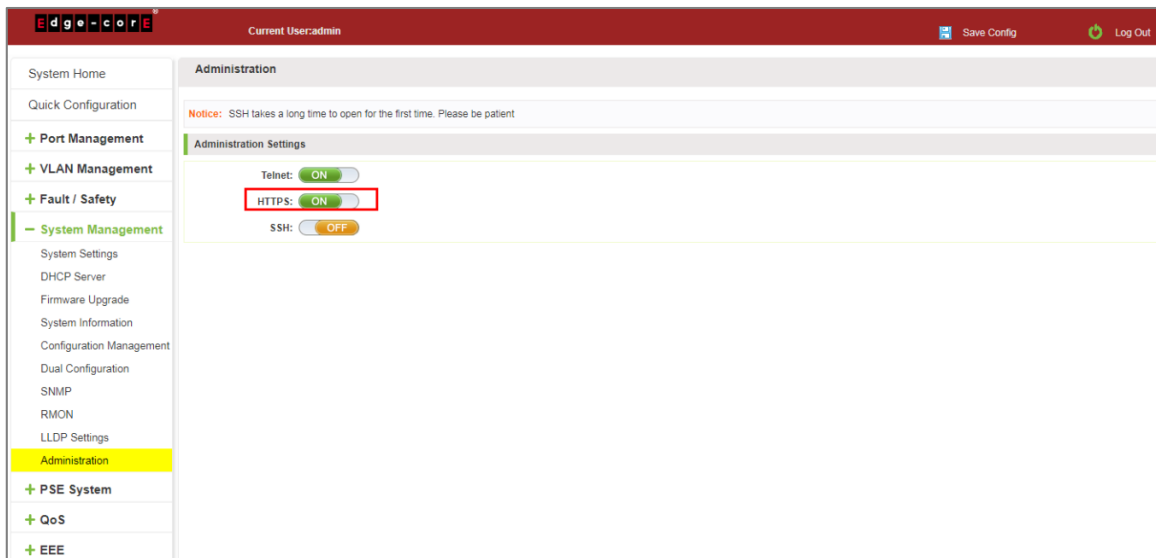


Figure 7-49: Enabling HTTPS

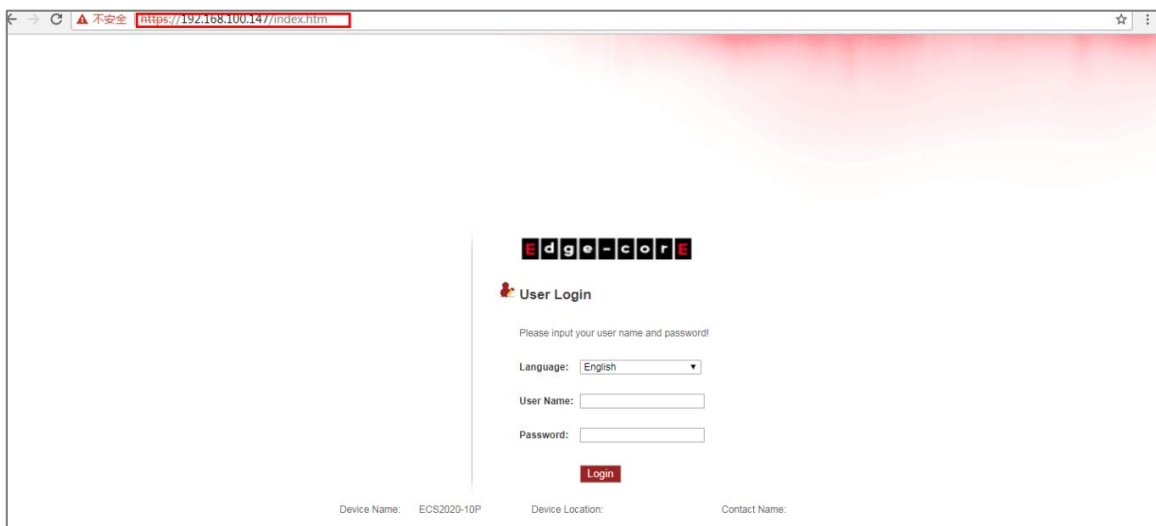


Figure 7-50: HTTPS login

#### 7.10.4 Enabling SSH

Next to SSH: on the Administration Settings page click the OFF sliding button once. The first time enabling the SSH function may take approximately one minute before the interface responds. Ignore any warnings from your browser and wait for the confirmation box.

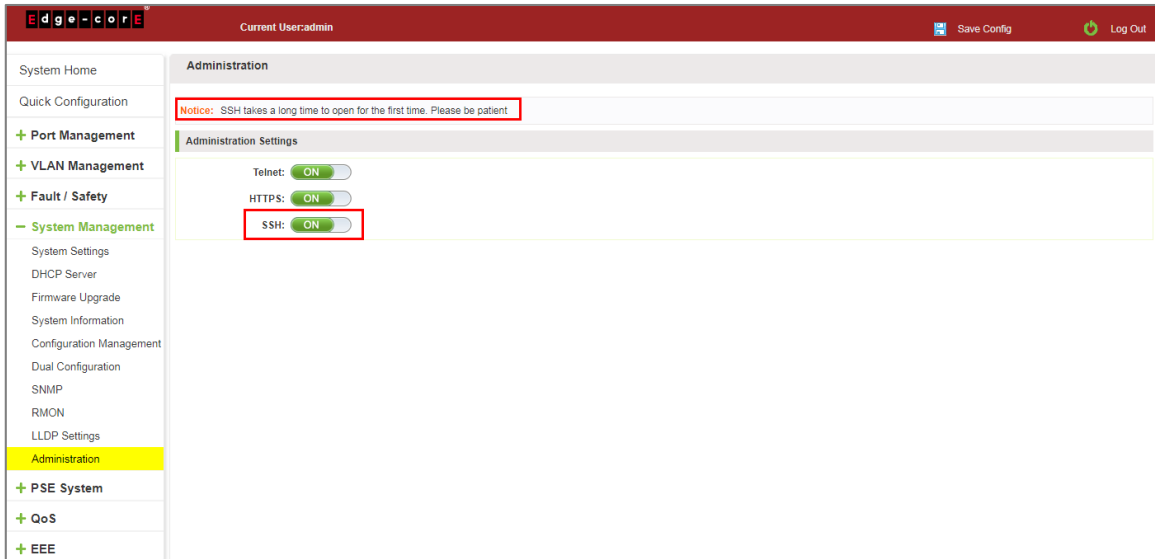
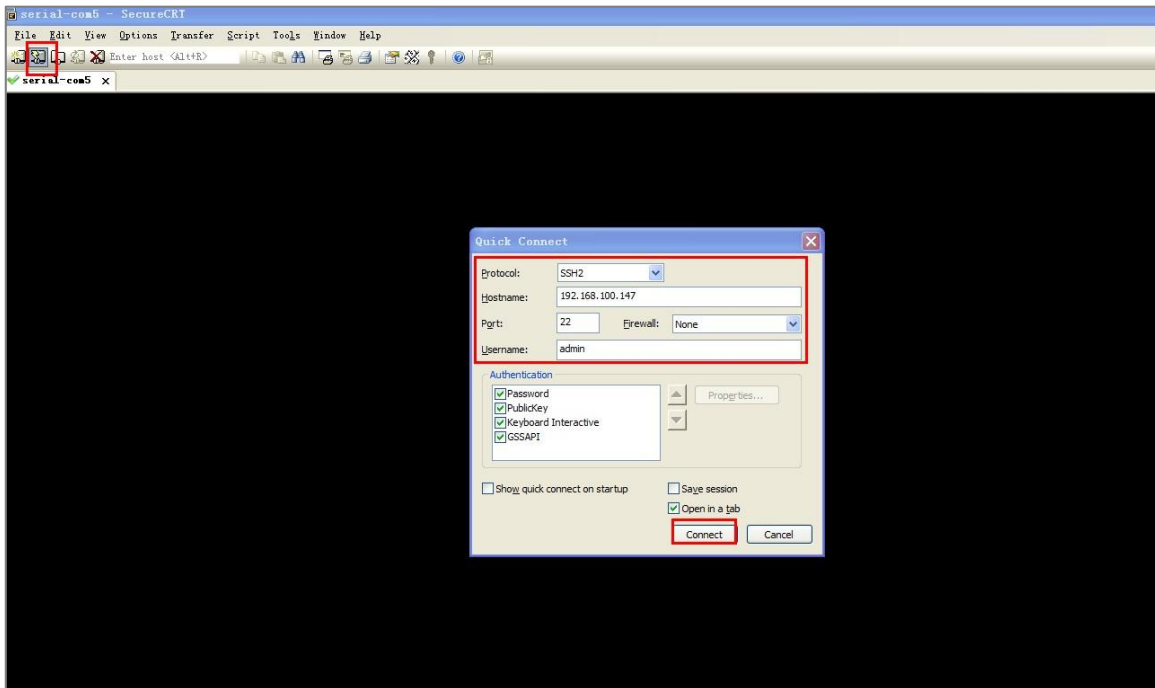


Figure 7-51: Enabling SSH



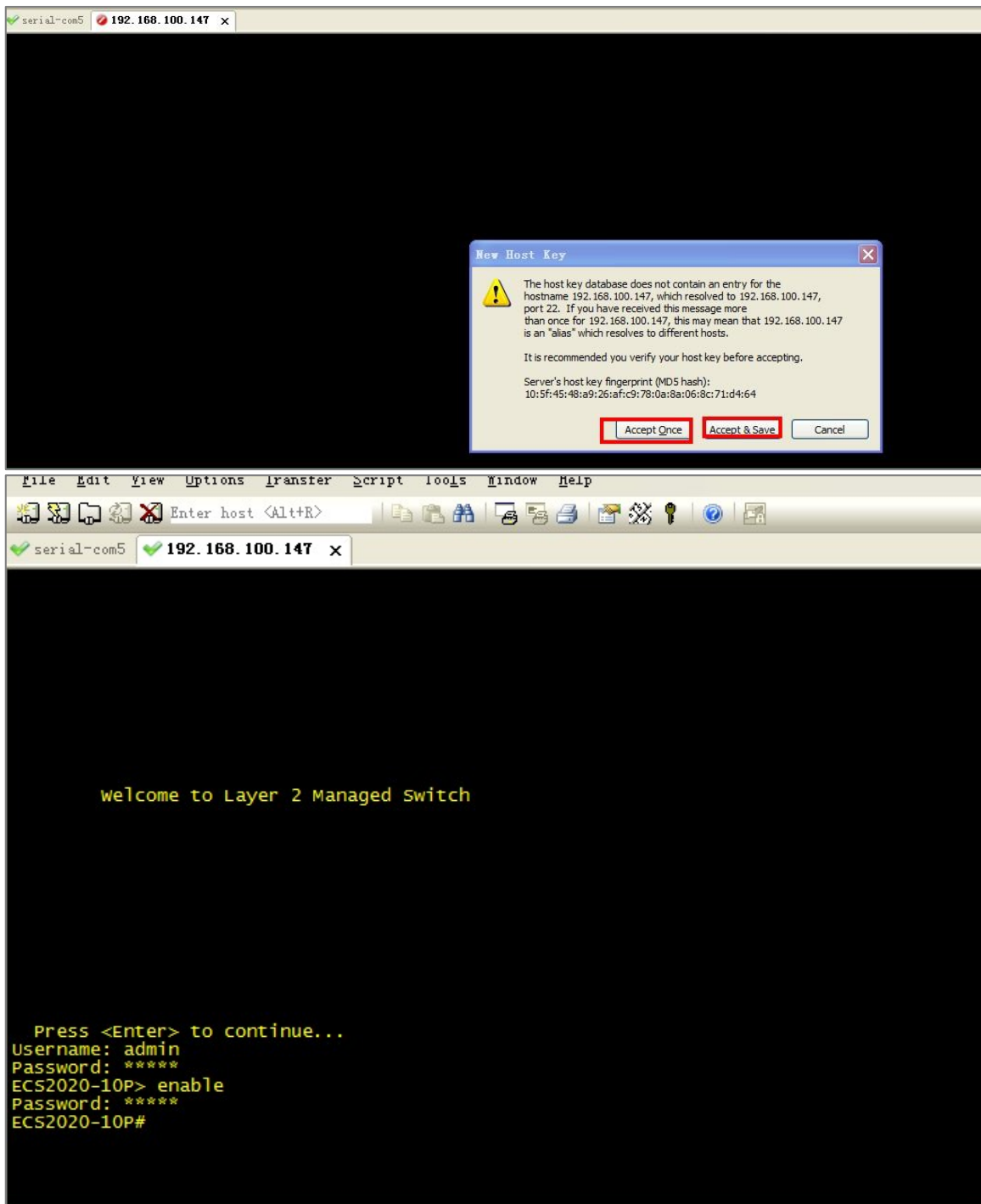


Figure 7-52: Using SSH to Login to the Switch

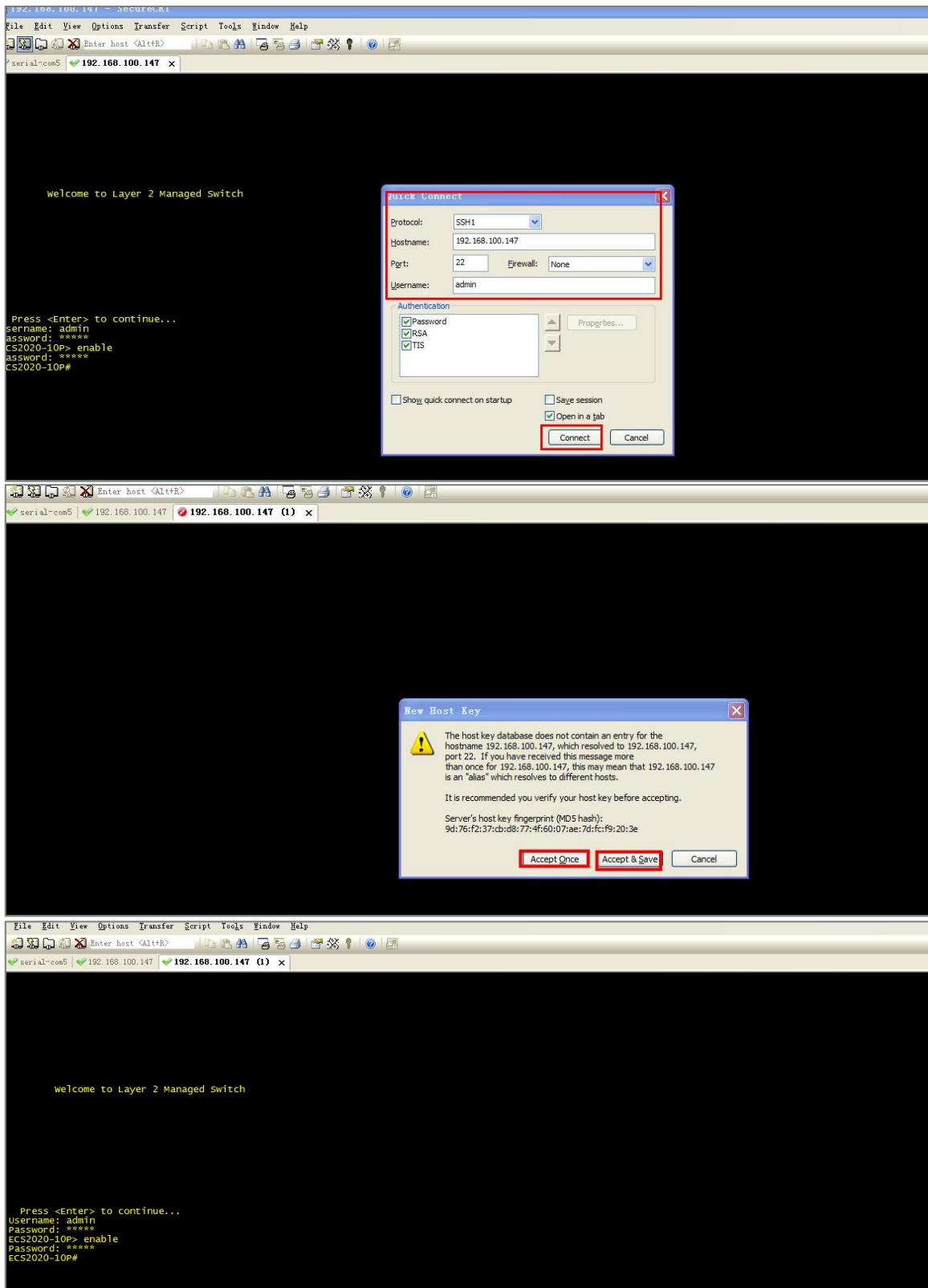


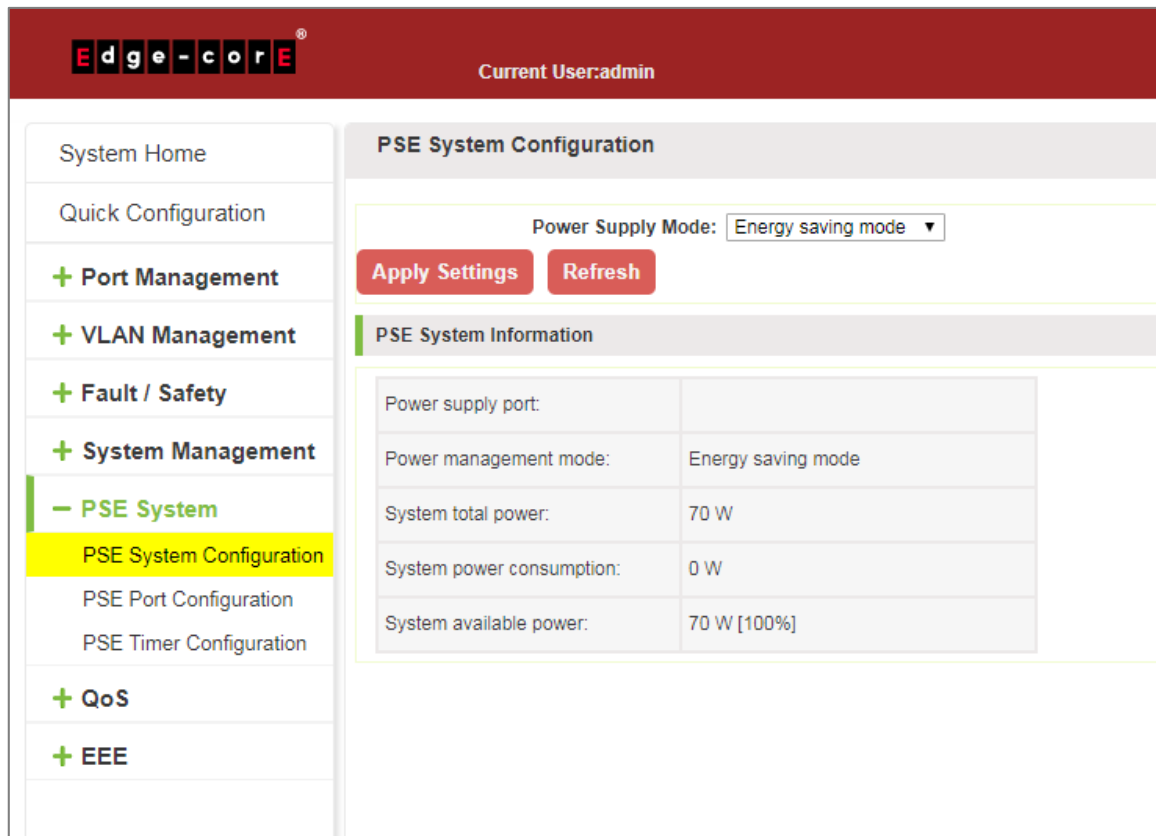
Figure 7-53: SSH1 Login

## 8 PSE SYSTEM MANAGEMENT

### 8.1 PSE SYSTEM CONFIGURATION

#### 8.1.1 Viewing the PSE system configuration

Click "PSE System Management" "PSE System Configuration" to view the PSE system configuration. Click the "Refresh" button update the display with the latest configuration.



The screenshot shows the Edge-core web interface for PSE System Configuration. The top header displays the Edge-core logo and the current user as 'admin'. The left navigation menu includes options like System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety, System Management, PSE System (expanded), PSE System Configuration (highlighted), PSE Port Configuration, PSE Timer Configuration, QoS, and EEE. The main content area is titled 'PSE System Configuration' and features a 'Power Supply Mode' dropdown menu currently set to 'Energy saving mode'. Below the dropdown are 'Apply Settings' and 'Refresh' buttons. A section titled 'PSE System Information' contains a table with the following data:

PSE System Information	
Power supply port:	
Power management mode:	Energy saving mode
System total power:	70 W
System power consumption:	0 W
System available power:	70 W [100%]

Figure 8-1: Viewing the PSE System Configuration

#### 8.1.2 Configuring power supply mode

The power supply mode can be one of 3 modes either: Automatic, Static or Energy Saving mode. To set the power supply mode click "PSE System Management" "PSE System Configuration" and then next to Power Supply Mode use the pull down menu and select either Automatic, Static or Energy Savings Mode. Finally click the Apply Settings button.

The screenshot shows the Edge-core PSE System Configuration interface. The top navigation bar includes the Edge-core logo and the text "Current User:admin". On the left, a sidebar menu lists various configuration options, with "PSE System Configuration" highlighted in yellow. The main content area is titled "PSE System Configuration" and features a dropdown menu for "Power Supply Mode" set to "Automatic mode". Below this are "Apply Settings" and "Refresh" buttons. A section titled "PSE System Information" contains a table with the following data:

Power supply port:	
Power management mode:	Automatic mode
System total power:	70 W
System power consumption:	0 W
System available power:	70 W [100%]

Figure 8-2: Configuring the Power Supply to Automatic Mode

The screenshot shows the Edge-core PSE System Configuration interface with the "Power Supply Mode" dropdown menu set to "Static mode". The "Apply Settings" and "Refresh" buttons are visible. The "PSE System Information" table now displays the following data:

Power supply port:	
Power management mode:	Static mode
System total power:	70 W
System power consumption:	70 W
System available power:	0 W [0%]

Figure 8-3: Configuring the Power Supply to Static Mode

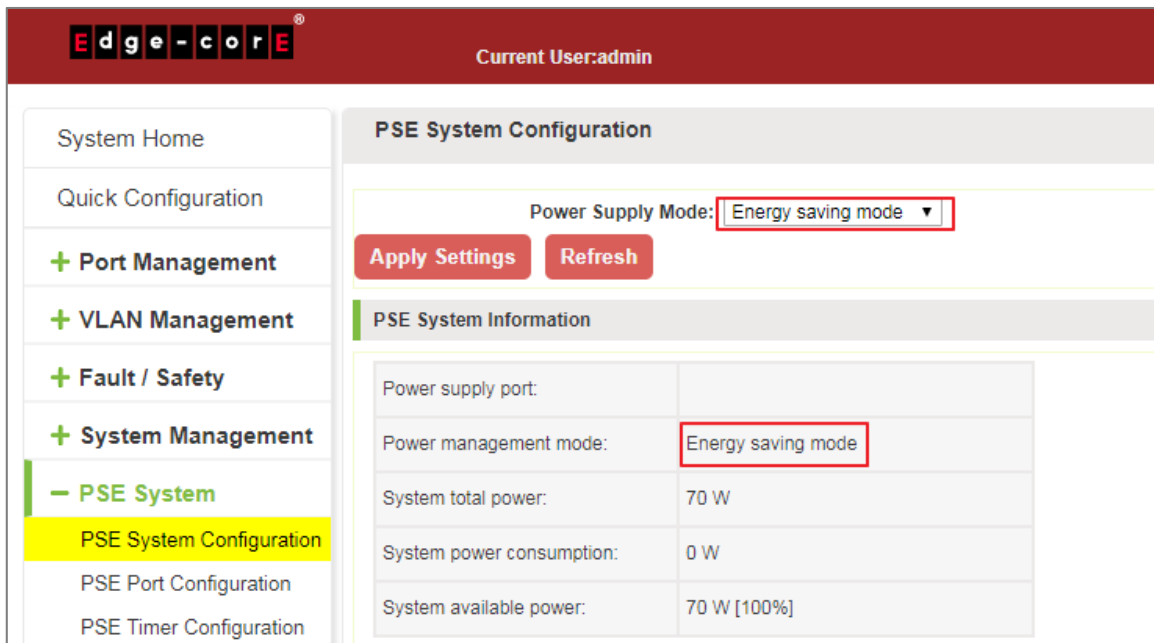


Figure 8-4: Configuring the Power Supply to Energy Saving Mode

## 8.2 POE PORT CONFIGURATION

Click "PSE System Management" "POE Port Configuration" to configure the power allocation on individual POE ports.

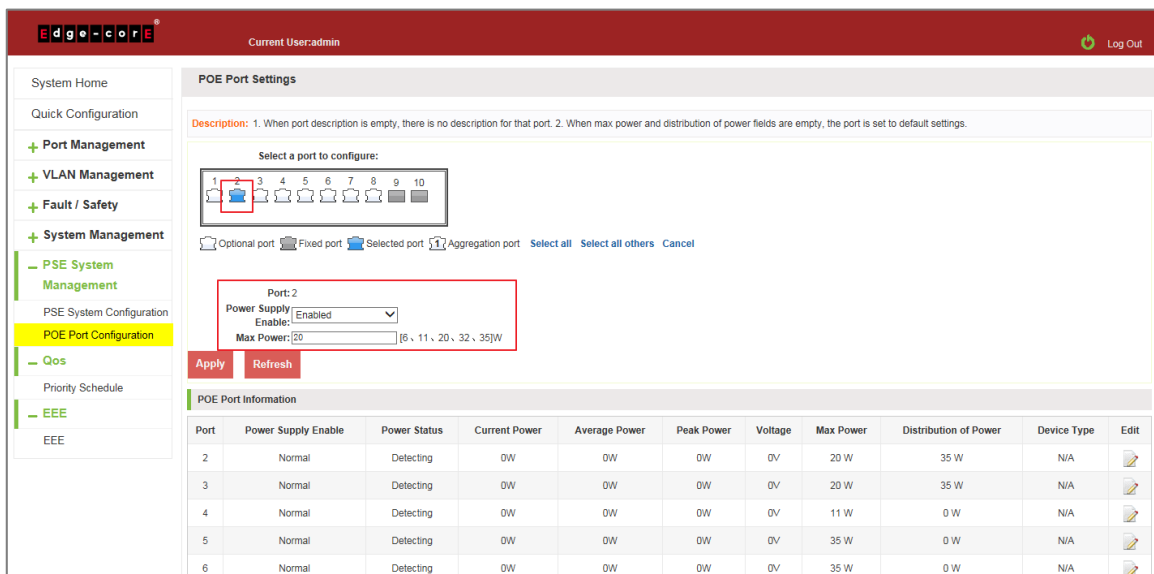


Figure 8-5: Port PoE Power Allocation

To configure the power allocation on individual PoE Ports:


Step 1: Click a port to select it in the port selection panel

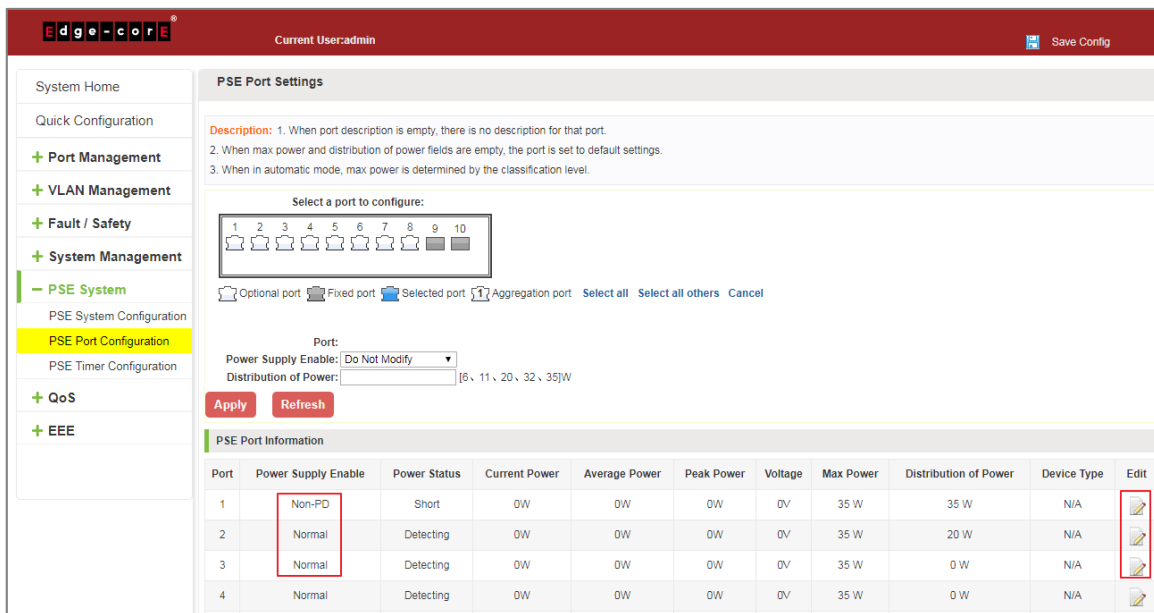
Step 2: In the power supply enable pull down menu, select "Enabled".

Step 3: In the Max Power pull down menu, select 6, 11, 20, 32 or 35 watts depending on the Powered Device (PD) requirement and the total available switch power.



## 8.2.1 Modifying a POE port

In the PSE Power Information list Click the  icon to re-configure the port's PSE power allocation and disable or enable the power the port's power supply.







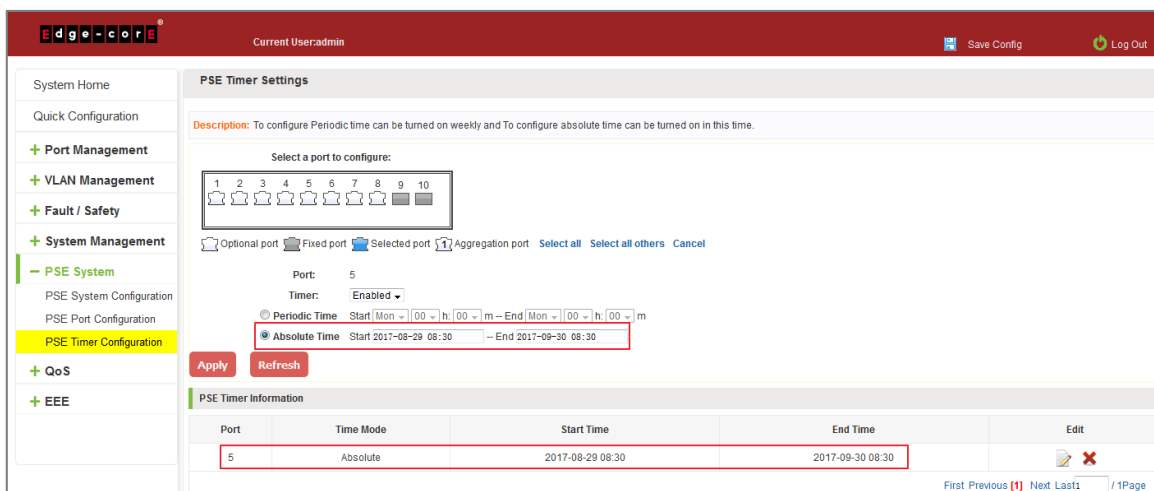
Port	Power Supply Enable	Power Status	Current Power	Average Power	Peak Power	Voltage	Max Power	Distribution of Power	Device Type	Edit
1	Non-PD	Short	0W	0W	0W	0V	35 W	35 W	N/A	
2	Normal	Detecting	0W	0W	0W	0V	35 W	20 W	N/A	
3	Normal	Detecting	0W	0W	0W	0V	35 W	0 W	N/A	
4	Normal	Detecting	0W	0W	0W	0V	35 W	0 W	N/A	

Figure 8-6: Modifying the Port PoE Configuration

## 8.3 POE TIMER CONFIGURATION

Click "PSE System Management" "PoE Timer Configuration" to configure the individual port's automatic PoE power ON/OFF schedule. The on and off times can be set either using a single absolute time period or a repeating periodic schedule.




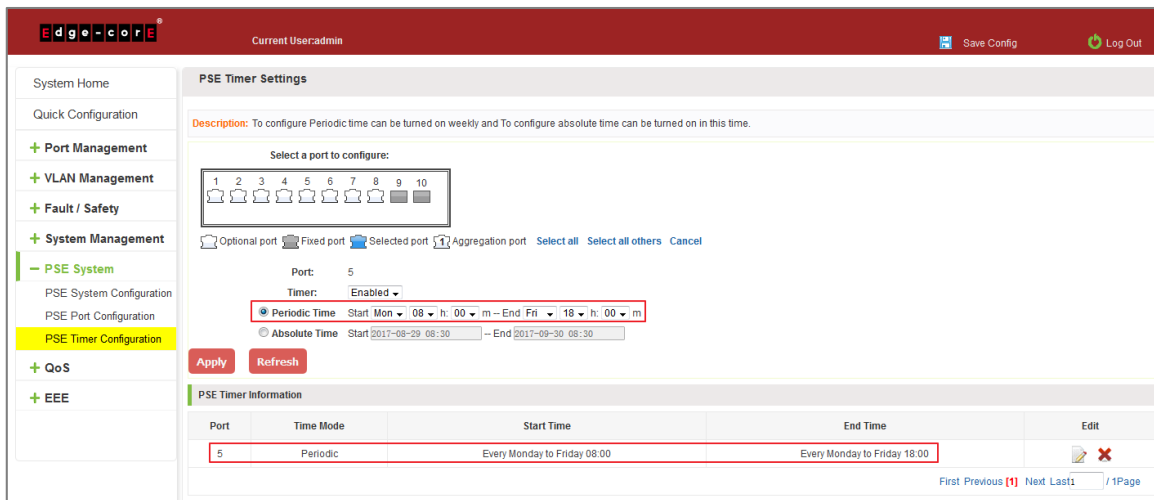
Port	Time Mode	Start Time	End Time	Edit
5	Absolute	2017-08-29 08:30	2017-09-30 08:30	

Figure 8-7: PoE Timer Absolute Time Configuration



**Figure 8-8: PoE Timer Periodic Time Configuration**

To configure the PoE timers:

Step 1: Select a port(s) in the port panel view to configure.

Step 2: In the Timer pull down menu, select enable.

Step 3: Configure absolute time selecting from the calendar and time configuration window a start time YYYY-MM-DD HH:MM to an end time YYYY-MM-DD HH:MM.

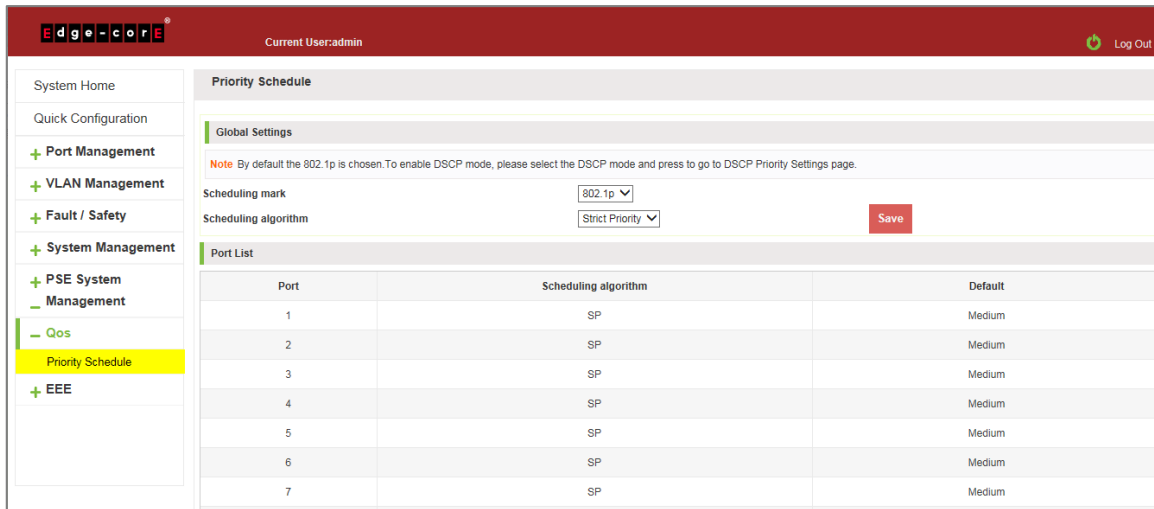
Step 4: -or- Configure a repeating periodic start time Day (M-S) Hour/Min to end time Day (M-S) Hour/Min using the pull down menus.

## 9 QOS

### 9.1 PRIORITY SCHEDULE

#### 9.1.1 Viewing the QOS priority schedule

Click "QoS" "Priority Schedule" to view the port priority schedule.



The screenshot shows the Edge-core network management interface. The top navigation bar includes the logo, the current user 'Useradmin', and a 'Log Out' button. The left sidebar contains a menu with options: System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety, System Management, PSE System Management, QoS (highlighted), Priority Schedule (highlighted), and EEE. The main content area is titled 'Priority Schedule' and contains the following sections:

- Global Settings:** A note states, 'By default the 802.1p is chosen. To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.'
- Scheduling mark:** A dropdown menu is set to '802.1p'.
- Scheduling algorithm:** A dropdown menu is set to 'Strict Priority', with a 'Save' button to its right.
- Port List:** A table with three columns: Port, Scheduling algorithm, and Default.

Port	Scheduling algorithm	Default
1	SP	Medium
2	SP	Medium
3	SP	Medium
4	SP	Medium
5	SP	Medium
6	SP	Medium
7	SP	Medium

Figure 9-9-1: Priority Schedule

#### 9.1.2 Configuring 802.1P QoS

##### 9.1.2.1 Configuring 802.1P Strict Priority QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select 802.1p. In the Scheduling algorithm pull down menu select Strict Priority. Select the port(s) to apply the QoS algorithm CoS to in the port panel view and then select the Class of Service using the COS: pull down menu (0-7) to be applied to the selected ports. Finally click Apply to configure the 802.1p Hybrid QoS COS on the selected ports (repeat with a new COS for the other ports until done).

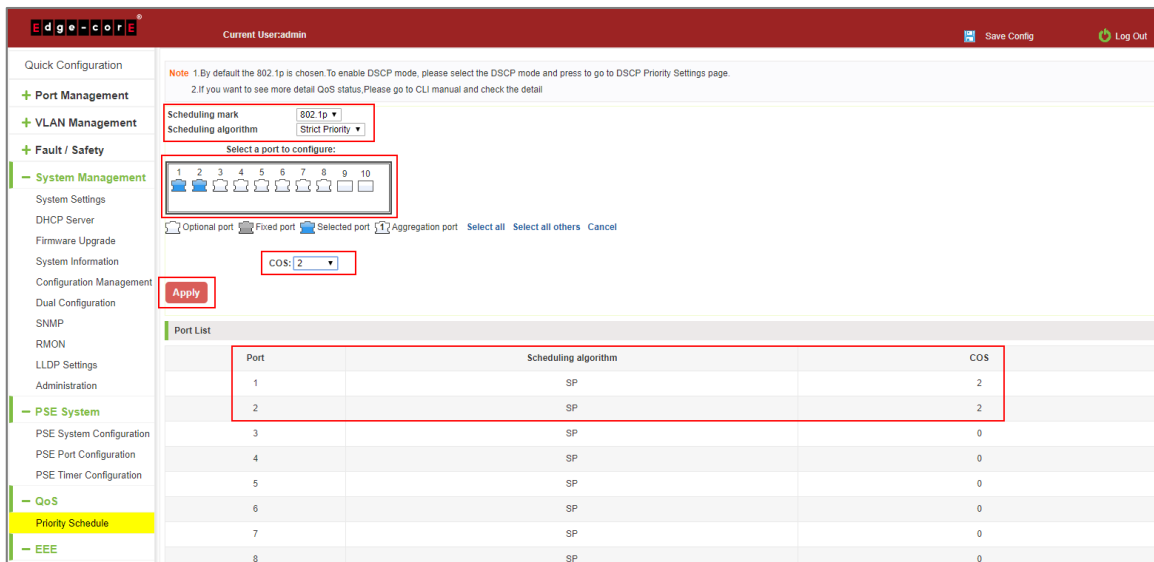


Figure 9-2: Configuring 802.1p Strict Priority QoS

### 9.1.2.2 Configuring 802.1P WRR QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select 802.1p. In the Scheduling algorithm pull down menu select WRR. Adjust the queue weights for queues 1 to 8 in the eight Queue Weight Value Configuration boxes. Select the port(s) to apply the QoS algorithm CoS to in the port panel view and then select the Class of Service using the COS: pull down menu (0-7) to be applied to the selected ports. Finally click Apply to configure the 802.1p Hybrid QoS COS on the selected ports (repeat with a new COS for the other ports until done).

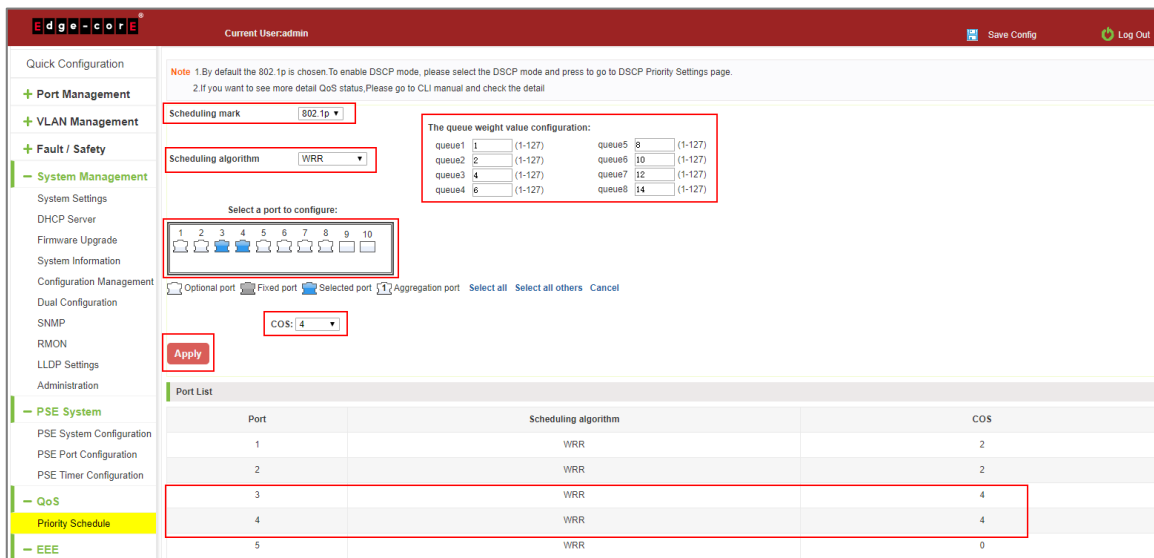


Figure 9-3: Configuring 802.1p WRR QoS

### 9.1.2.3 Configuring 802.1P Hybrid QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select 802.1p. In the Scheduling algorithm pull down menu select Hybrid. Select WRR in the Queue Scheduling Algorithm pull down menu with the queues 1 to 7 selected below and then adjust the queue weight values in the Queue's 1 to 8 input boxes. Select

the port(s) to apply the QoS algorithm CoS to in the port panel view and then select the Class of Service using the COS: pull down menu (0-7) to be applied to the selected ports. Finally click Apply to configure the 802.1p Hybrid QoS COS on the selected Settings ports (repeat with a new COS for the other ports until done).

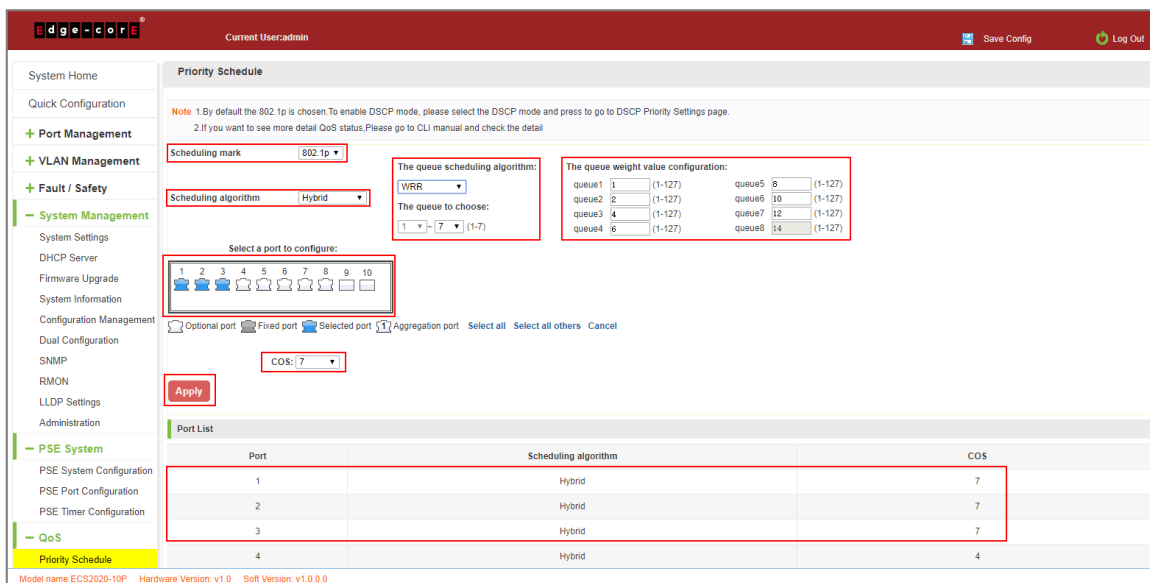


Figure 9-4: Configuring 802.1p Hybrid QoS

### 9.1.3 Configuring DSCP QoS

#### 9.1.3.1 Configuring DSCP Strict Priority QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select DSCP. In the Scheduling algorithm pull down menu select Strict Priority. Click Apply and then adjust the priority of the DSCP values using the DSCP value from (0-63) and to (0-63) pull down menus selecting the required priority (1-8) for the range. Click Apply and repeat until all DSCP values have the required priorities.

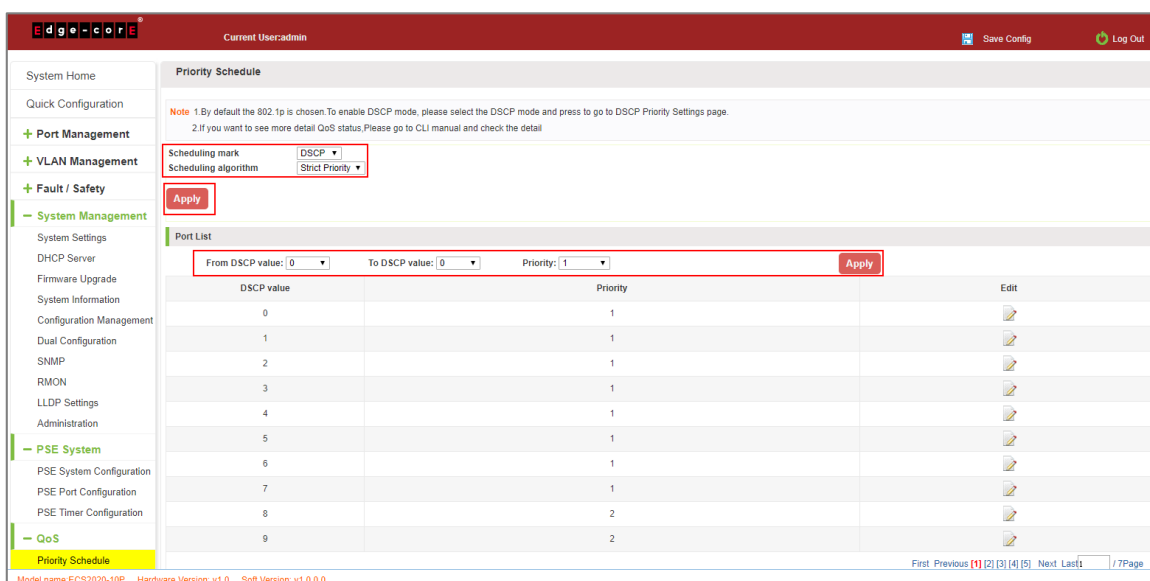


Figure 9-5: Configuring DSCP Strict Priority QoS

### 9.1.3.2 Configuring DSCP WRR QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select DSCP. In the Scheduling algorithm pull down menu select WRR. Adjust the queue weights for queues 1 to 8 in the eight Queue Weight Value Configuration boxes and click Apply. Then adjust the priority of the DSCP values using the DSCP value from (0-63) and to (0-63) pull down menus selecting the required priority (1-8) for the range. Click Apply and repeat until all DSCP values have the required priorities.

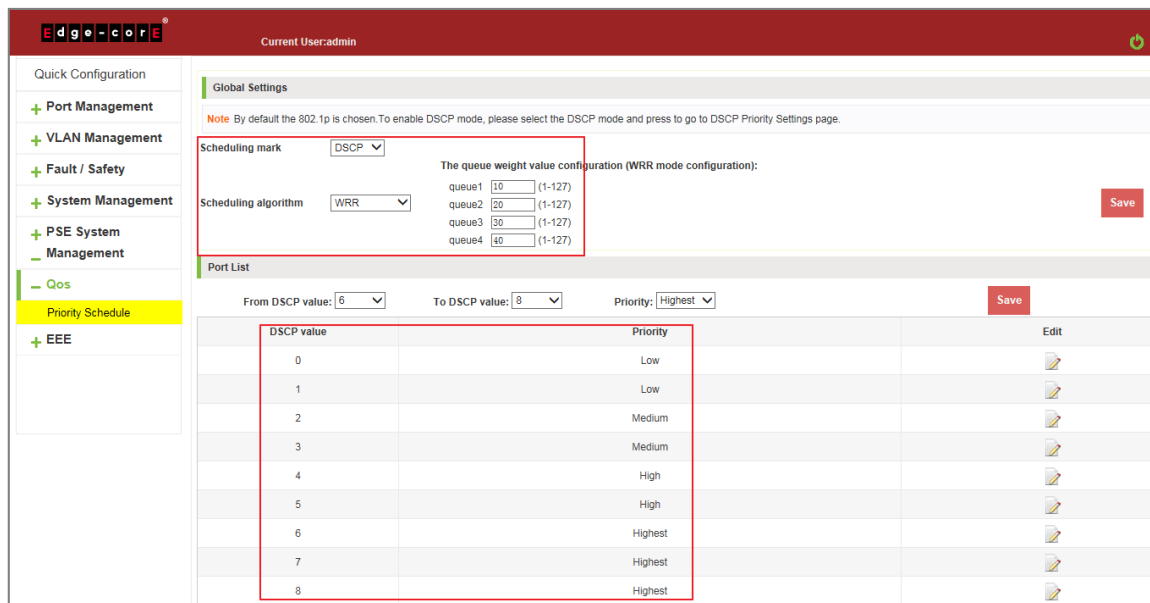


Figure 9-6: Configuring DSCP WRR QoS

### 9.1.3.3 Configuring DSCP Hybrid QoS

Click "QoS" "Priority Schedule" and in the scheduling mark pull down menu select DSCP. In the Scheduling algorithm pull down menu select Hybrid. Select WRR in the Queue Scheduling Algorithm pull down menu with the queues 1 to 7 to selected below and then adjust the queue weight values in the Queue's 1 to 8 input boxes. Click Apply and after adjust the priority of the DSCP values using the DSCP value from (0-63) and to (0-63) pull down menus selecting the required priority (1-8) for the range. Click Apply and repeat until all DSCP values have the required priorities.

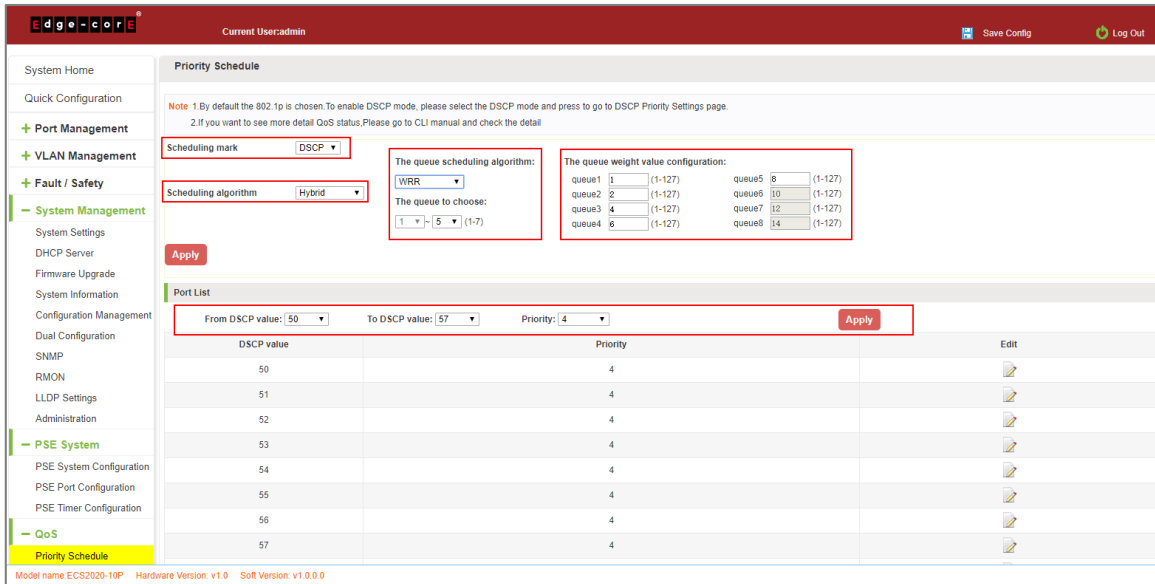


Figure 9-7: Configuring DSCP Hybrid QoS

### 9.1.4 Editing the QoS values

Click the icon to modify the QoS values:

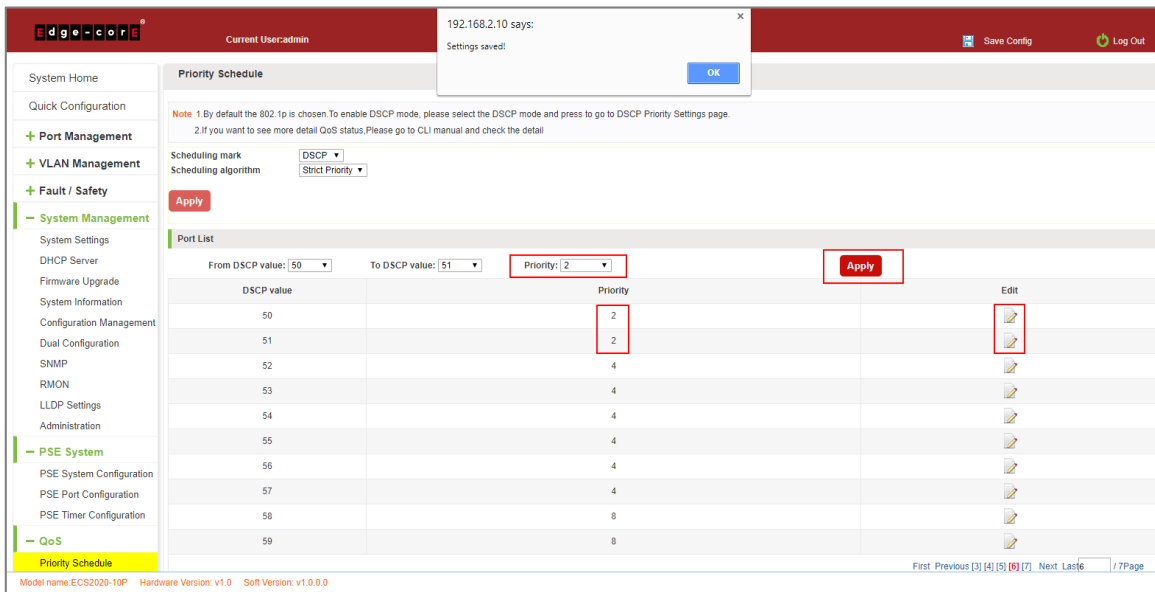


Figure 9-8: Modifying QoS parameters

## 10 EEE

### 10.1 VIEWING THE 802.3AZ EEE SETTINGS

Click "EEE" "EEE" to view the EEE ON/OFF status.

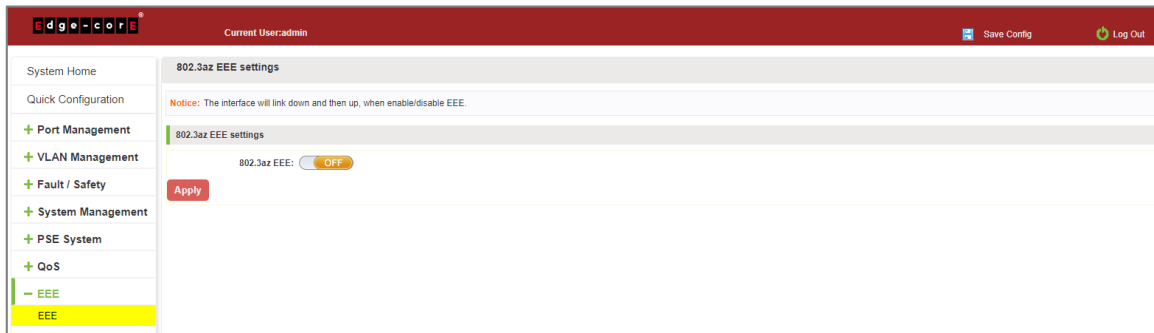


Figure 10-1: Viewing the 802.3az EEE ON/OFF Status

### 10.2 ENABLING 802.3AZ EEE

Click "EEE" "EEE and click the "OFF" slider once and wait for it to turn to green "ON" then click Apply.

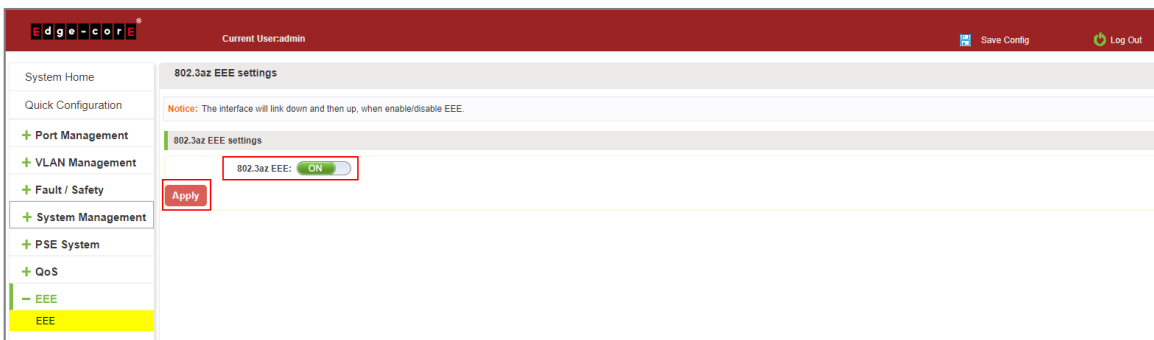


Figure 10-2: Enabling 802.3az EEE





