PDS-208G

Web Configuration Manual

Version 2.4

Microsemi
One Enterprise Aliso Viejo, CA 92656 USA

Disclaimer

The instruction made according to existing information. The contents may change if products upgraded or other unpredictable reason. The web reserved the right to modify instruction without prior notice and prompt.

The manual is for user instruction. Web try to make all contents correct and reliable, but can't assume none of mistake and no message missing. Even so web don't make any express or hint guarantee.

TABLE OF CONTENTS

PREFACE

This manual will guide you in detail how the device management page WEB local management.

1.1 OVERVIEW

Microsemi's PDS-208G PoE switch offers optimal and cost effective solution for connected lighting applications. It allows PoE capable LED fixtures and other IP terminals to receive power, along with data, over standard Ethernet cables.

The PDS-208G is a 240 W fan less switch, designed to be deployed in the ceiling.

The switch has 8 PoE ports and 2 uplink ports, all ports supporting 10/100/1000-Mbps (Gigabit Ethernet).

The switch can provide full power of 30W per port for all 8 ports simultaneously, In extra power mode, any specific port can go up to 72W.

The 240W high-speed switch offers secured Layer 2 management capabilities and remote web management.

The switch offer high energy efficacy performance, specifically supporting "Green PoE" – offering savings of 50% of the cable losses by proving 30W of power over 4-pairs while any other switch will use only 2-pairs resulting in double losses over the Ethernet cables due to the higher current level.

1.2 INTENDED AUDIENCE

This documentation is intended for:

- Network planner
- Technical support and maintenance personnel
- Network Management

1.3 CONVENTIONS

Switch mentioned in this manual, unless otherwise specified, refer to PDS-208G switches. This document only PDS-208G switch as an example.

1.4 CHAPTERS CONTENT

Chapter 1: Introduction Configuration Guide. Help readers quickly grasp the structure of the book, to understand the book conventions, more effective use of this manual.

Chapter 2: WEB MANAGEMENT LANDING PAGE. Landing preparations WEB page guides you switch WEB MANAGEMENT LANDING PAGE.

Chapter 3: WEB management page introduction. This chapter will take you quickly become familiar with WEB management page.

Chapter 4: Quick Configuration. This chapter describes the device management via flash configuration.

Chapter 5: Port Management. This chapter describes some common settings for the port.

Chapter 6: vlan management. This chapter describes the management vlan configuration.

Chapter 7: Fault / safety. This chapter describes the security configuration management, such as: port security, and access control.

Chapter 8: System Management. Guide you through the switching system management through the WEB page, such as software upgrades, configuration file management.

Chapter 9: PoE system management. Guide you through the POE switching power supply management through WEB page.

Appendix - Default switch Configuration: Default some key features of the switch configuration information.

Switches Terminology Appendix: switches glossary .

2 WEB MANAGEMENT LANDING PAGE

2.1 PREPARATIONS

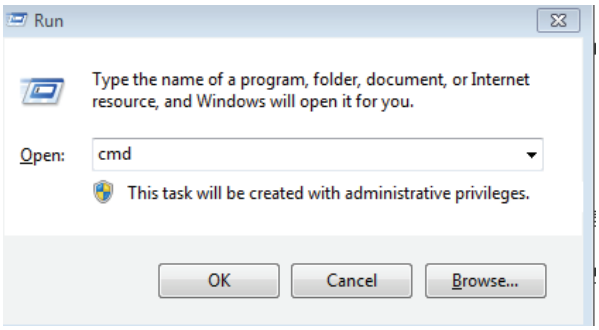
2.1.1 SETTING THE COMPUTER'S IP ADDRESS

- IP address management computer's IP address and the switch must be set to the same subnet (switch default IP address is 192.168.0.50, the default subnet mask of 255.255.255.0).
- IP address management need to manually configure the computer.
- By default, all ports belong vlan1, so any management host access ports can be used to configure switch management.

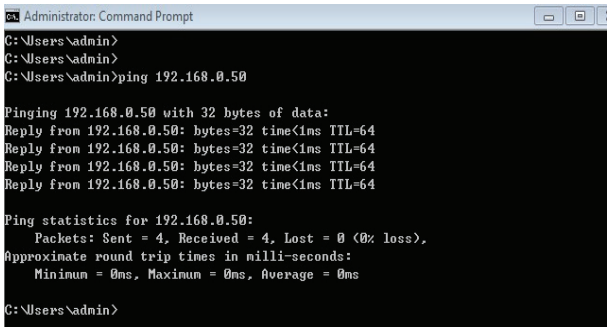
2.2 VERIFY NETWORK CONNECTIVITY BETWEEN THE SWITCH AND COMPUTER MANAGEMENT

Claim management computer and switch between network connectivity, follow these steps:

1. Enter the windows key + R keyboard, enter the "Run" box "cmd", click "OK".



2. Enter the "ping 192.168.0.50", Enter. If a response is returned from the exchange side, the network connectivity; otherwise, check the network connection.



2.3 LOG IN TO THE SWITCH MANAGEMENT PAGE WEB

Run WEB browser, in the address bar enter http://192.168.0.50. Enter, enter the user name and password (default is admin, password is case-sensitive), click "Login" button or directly enter into the WEB management

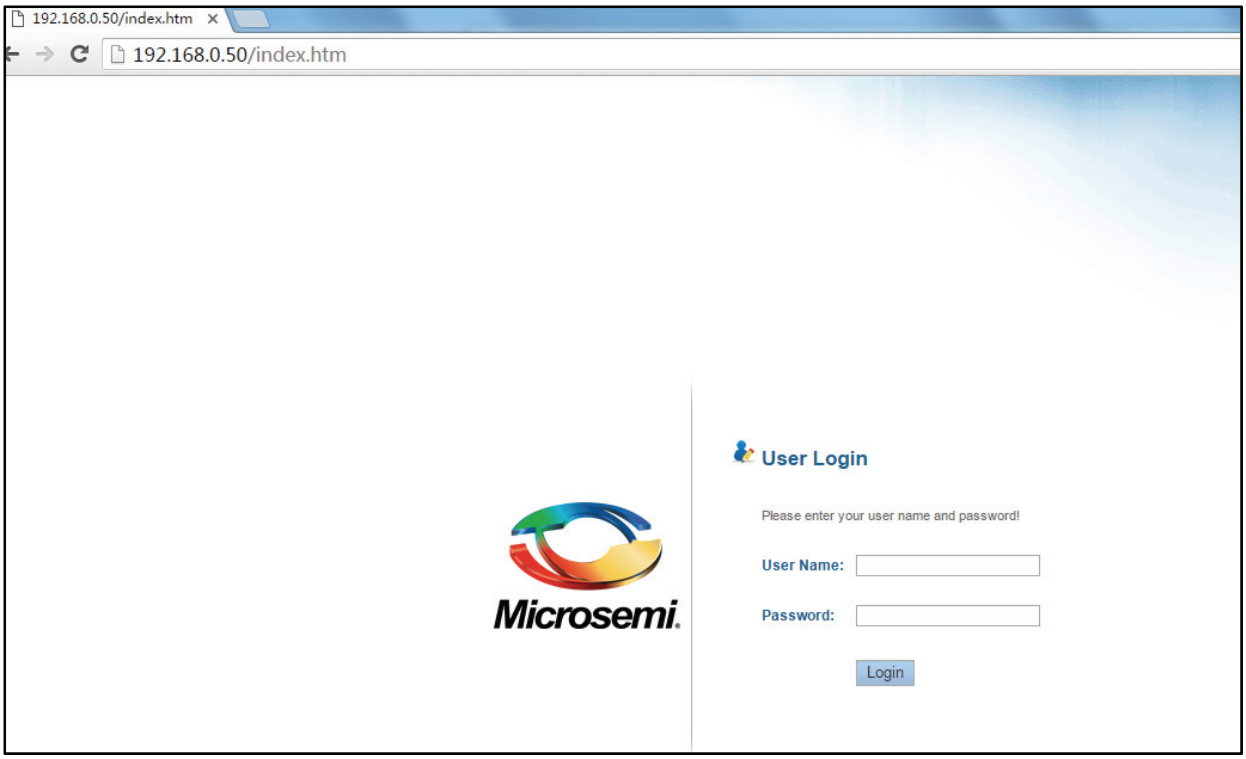


Figure 2-1: The login page WEB

After landing successfully, the switch management page WEB page:

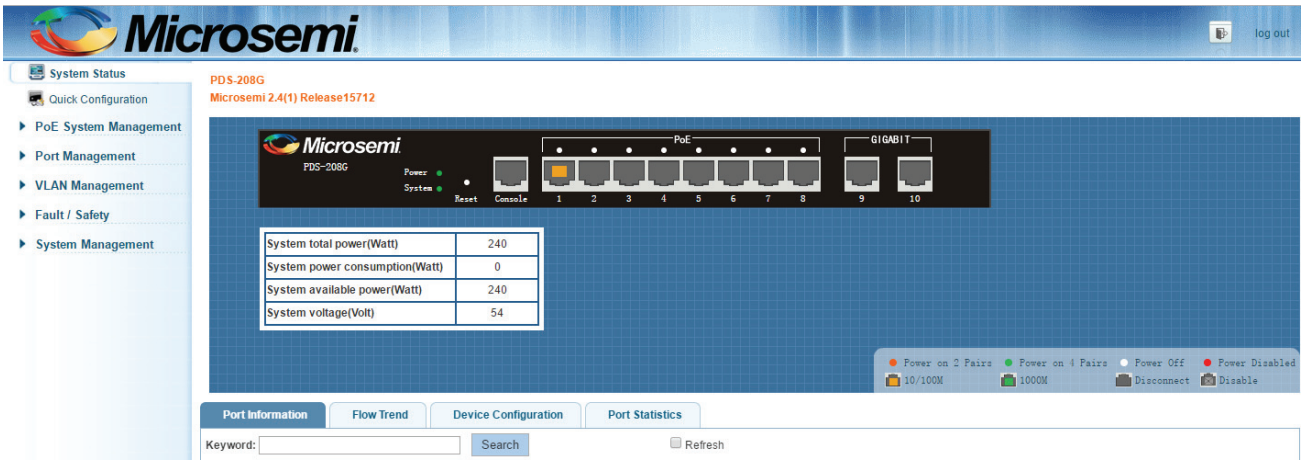


Figure 2-2: switch WEB management page Home

This document applies to PDS-208G switches, WEB interface functions configuration steps and consistent manner, so that here only one of a device described as an example.

We recommend using IE 8 and above browsers

2.4 ADDRESS CONFIGURATION MANAGEMENT

2.4.1 CHECK THE IP ADDRESS MANAGEMENT

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

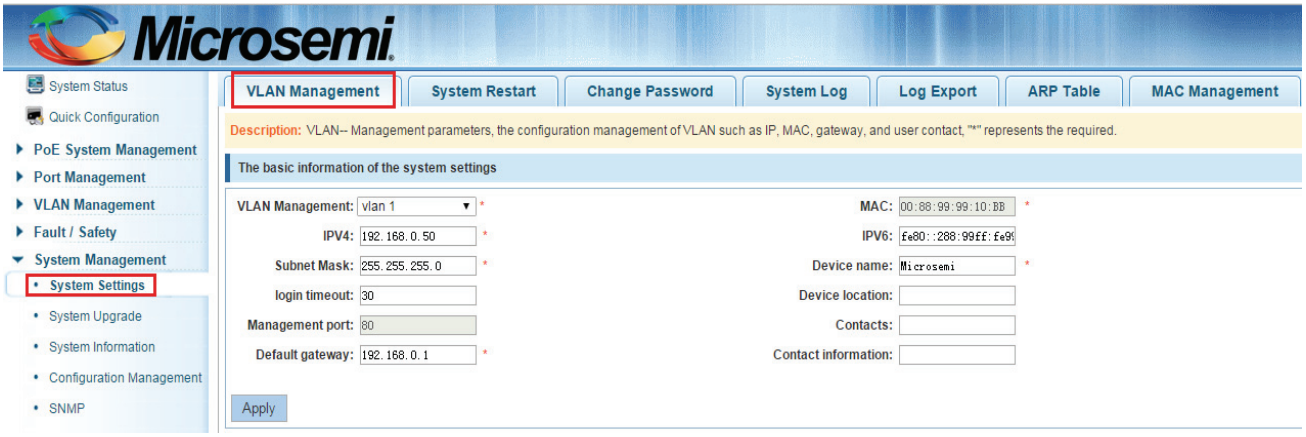


Figure 2-3: Switch management IP address

- Management VLAN: switch management VLAN ID, the default is 1;
- MAC Address: MAC address of the switch device;
- Management IP: switch management VLAN current IP address;
- Subnet Mask: The current switch management VLAN subnet mask information;
- Default Gateway: switch management VLAN current default gateway;
- Device Name: hostname of the switch;
- Device Location: switch placement;
- Timeout login: more than 5 minutes by default, Web Interface login screen return;
- Management Port: The default is 80;
- IPv6:switch management VLAN current IPv6 address;
- Contacts: the name of the Contact;
- Contact information: the contact information of the Contact;

The default management VLAN is VLAN1. it cannot be deleted.

2.4.2 CONFIGURATION MANAGEMENT IP ADDRESS

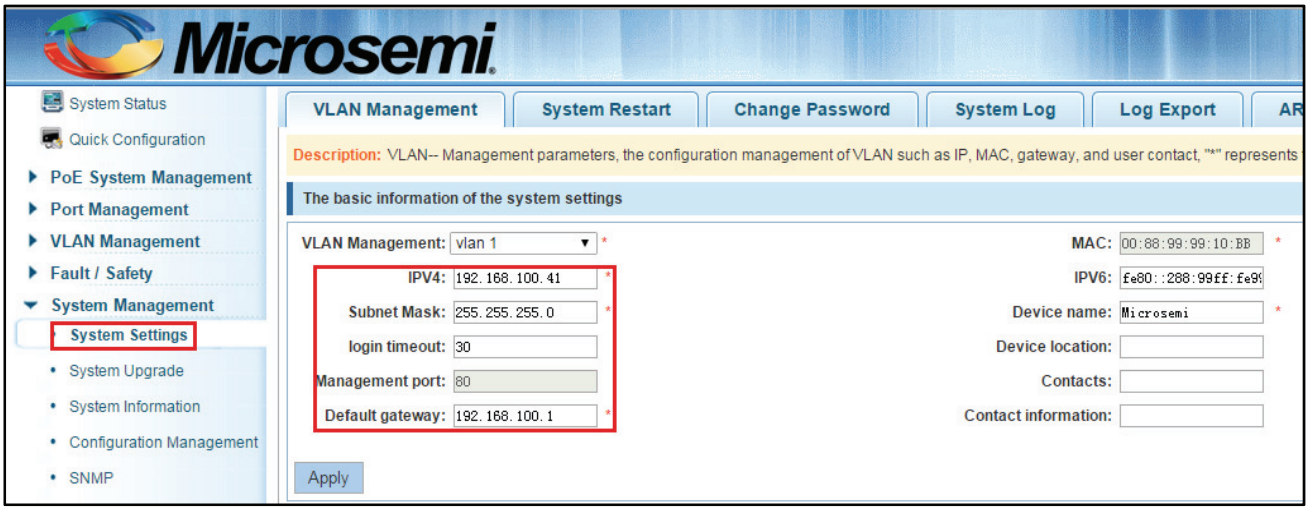


Figure 2-4: Changing the switch management address

To configure the switch management IP address is as follows:

1. In the IP address text box to enter the IP address, such as 192.168.100.41
2. In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.0
3. In the Gateway Address text box to enter the gateway address, such as 192.168.100.1
4. Click on "Save Settings" button to complete the configuration

3 INTRODUCTION WEB MANAGEMENT PAGE

3.1 WEB MANAGEMENT PAGE INTRODUCTION

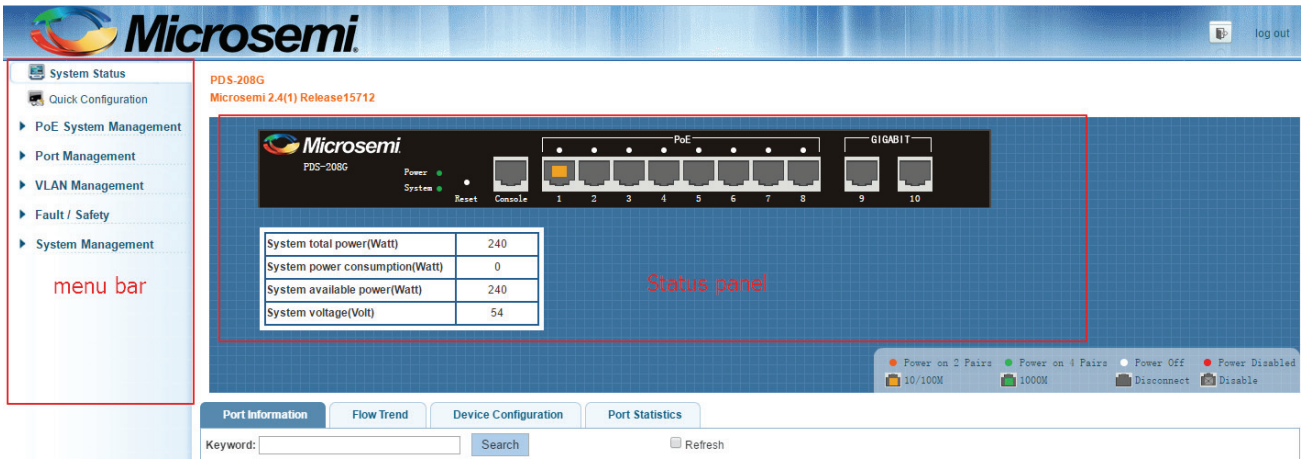


Figure 3-1: Switch WEB management page

3.1.1 THE MENU BAR

Figure 3-2: Menu Bar

WEB management page menu bar includes: Home system, quick configuration, port management, VLAN management, fault / security, system management, PoE system management seven menu.

Menu contains a secondary menu, the default switch management secondary display hidden menu, you can click a menu to hide or display a secondary menu.

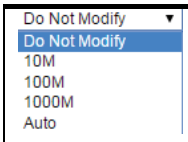
The following table lists each menu level and second-level menu contains this table, you can quickly find what they want to configure:

A menu	B menu	Page Functions
Home System	N/A	FIG panel display switch port, product version information
Quick Configuration		vlan set, trunk settings, SNMP settings, POE and other configuration settings
PoE system management	PoE PowerManagement	View, modify system configuration PRoE
	PoE port Settings	View, edit PoE port configuration
Port Management	basic settings	Port description, status, speed, work mode, Mtu Settings
	Storm Control	Setting broadcast, multicast, and unicast storm limit.
	flow control	Select the port flow control
	Port Aggregation	Check the switch port aggregation, and can add / delete / modify port aggregation
	Port Mirroring	Set up a mirror port and mirror port. Only one port mirroring, which can have multiple mirrored ports.
	Port speed	View / Modify port uplink and downlink rate limit
VLAN management	VLAN management	① add, delete VLAN, VLAN or the port to remove from a VLAN; ② add, delete TRUNK, the port is added to or deleted from TRUNK TRUNK in
Fault / Security	Attack prevention	① Check the ARP table status, activate / deactivate the port ARP anti-spoofing function; ② enable / disable port security, and set the IP and MAC binding legal relative ③ Activate/disable prevent illegal DHCP server functions, and can set the port to trust/untrusted state
	Channel detection	The Ping function is used to detect switches connected to other device connectivity
	Access control	Configure a series of ACL IP, expansion of IP, the expansion of MAC rules, comply with the rules of the data can flow through
	Multicast listening	Activate/disable IGMP Snooping, add/remove multicast routing configuration
	STP	Open or close the spanning tree function, prevent broadcast

		storm caused by the loop
System management	System Settings	(1) set up the management VLAN IP address and subnet mask (2) restart the system (3) to modify the user password and Telnet login password (4) the system log view and collection 5. Check the ARP table entry 6. The MAC address table query, static MAC address configuration (add or delete a static MAC address)
	System upgrade	Software upgrade switches
	System information	(1) memory information (2) the system task
	Configuration management	(1) the backup and restore backup configuration file (2) to restore factory default configuration
	SNMP	Open the SNMP and TRAP, community name, TRAP services such as host
	System diagnostics	Used to collect the memory usage, CPU usage, process status, the current configuration, version, link together group, the ARP deception, CPU speed limit, control information such as the storm.
	QOS	Open or close the function
	LLDP	1) open or close the function, configuration corresponding parameters (2) the neighbor information (3) port state
	The WEB console	Enter legal command line switches for operation

3.2 PAGE CONTROLS

Controls	Functional description
	Text box, for text input, such as the VLAN ID number, port description, etc
	Check box, is used to specify a list of selected items

	A drop-down box, is used to select the corresponding list items
Choose File	Click browse after selection of the local computer software version or configuration files
	Edit button, click later to enter edit mode
	Delete the current rules
Refresh	Refresh the current page configuration
Apply	Submit the current page configuration information
Cancel	Cancel the current page configuration information
OK	The current system to provide the information to perform confirm the operation
Cancel	The current system to provide the information to perform to cancel the operation

3.3 WEB PAGE TIMEOUT HANDLING

When the long time operation management of WEB page, the system will cancel the login, return to the WEB landing page, as shown in figure 2-1.

 WEB management page default timeout for5 minutes.

3.4 THE FOURTH CHAPTER QUICK CONFIGURATION

Click on "Quick Configuration", can quickly to Configuration of the device commonly used functions, such as a VLAN, SNMP, POE function, etc. According to the steps, the configurations of step by step, also can choose configuration.

3.5 VLAN SETTING

Click on "Quick Configuration" Settings" into the Quick Configuration of VLAN Configuration page. Can view the current equipment VLAN information, according to the demand of new VLAN, modify, VLAN, delete VLAN, etc., after the completion of the configuration, click "Next".

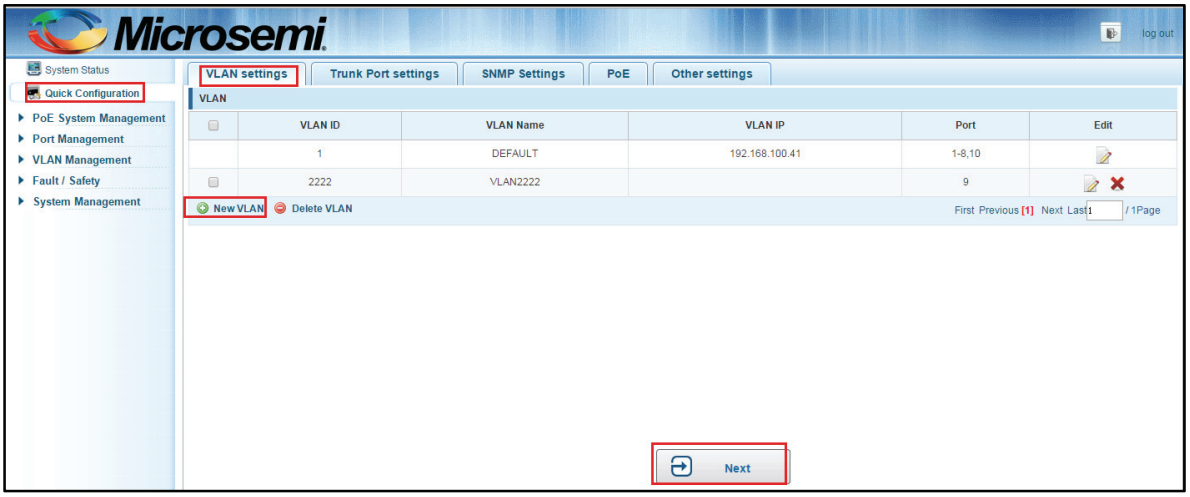


Figure 3-3: VLAN Setting

3.6 TRUNK SETTING

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

Figure 3-4: Trunk Setting

3.7 SNMP CONFIGURATION

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

Figure 3-5: SNMP Setting

3.8 POE SETTING

1.Click on "Quick Configuration""PoE" into the Quick Configuration Settings page. Can undertake configuration on the current equipment POE function, according to the corresponding port demand allocation information such as the power supply mode and power.

2.Configuration is complete, click "Next" to enter other Settings page. Or click on "Previous" back to the SNMP Settings page.

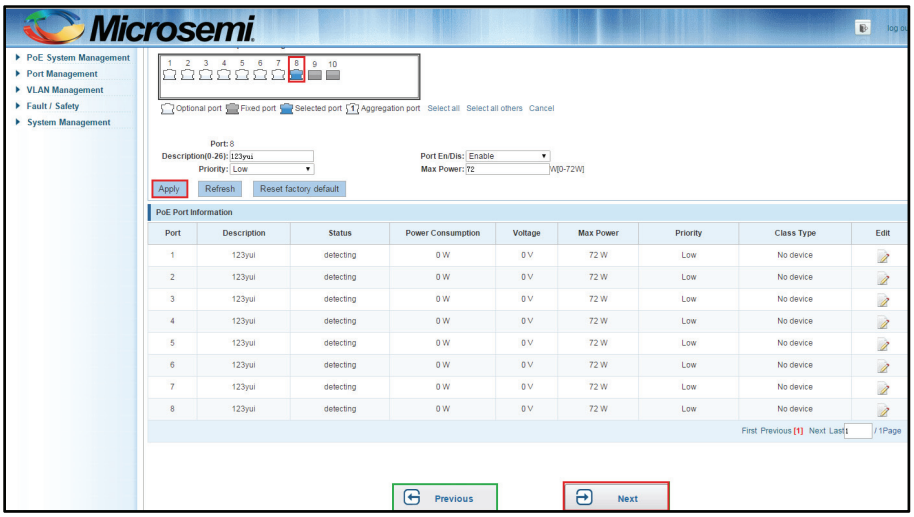


Figure 3-6: POE setting

3.9 THE OTHER SETTINGS

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

3.End of the configuration is Complete, click on "Complete" rapid configuration, or click the "Previous" back to the POE Settings page.

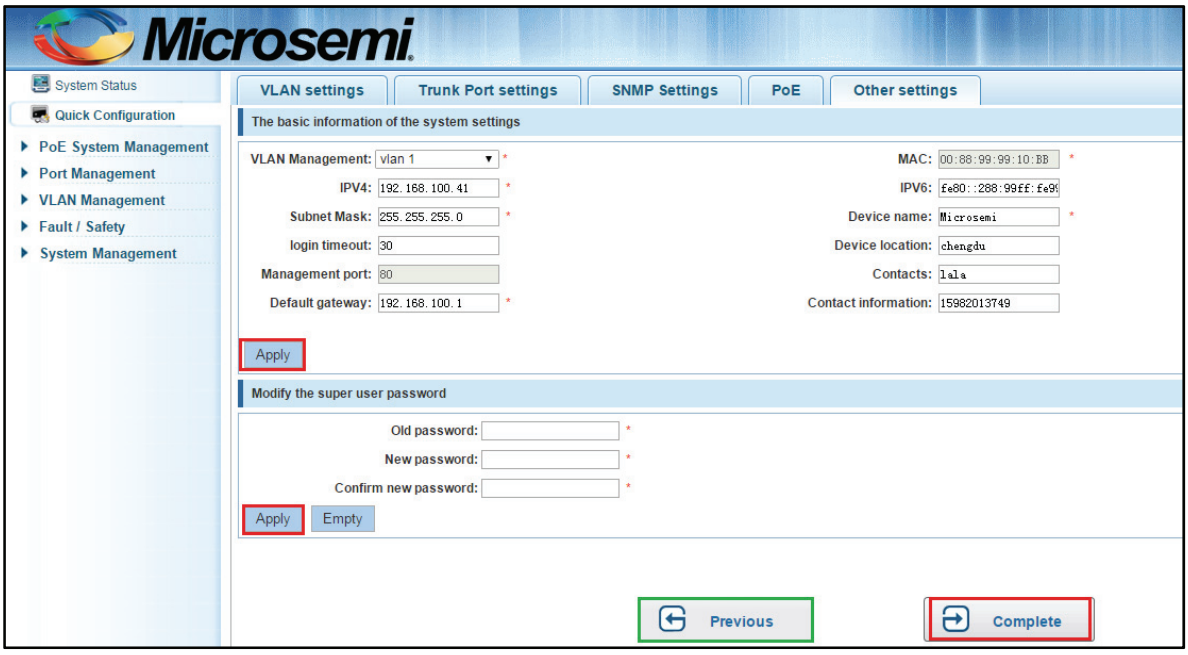


Figure 3-7: Other settings

4 POE SYSTEMS MANAGEMENT

4.1 POE THE SYSTEM CONFIGURATION

Click on "PoE System Management""Power Management", you can view the PoE System Management has configuration information:

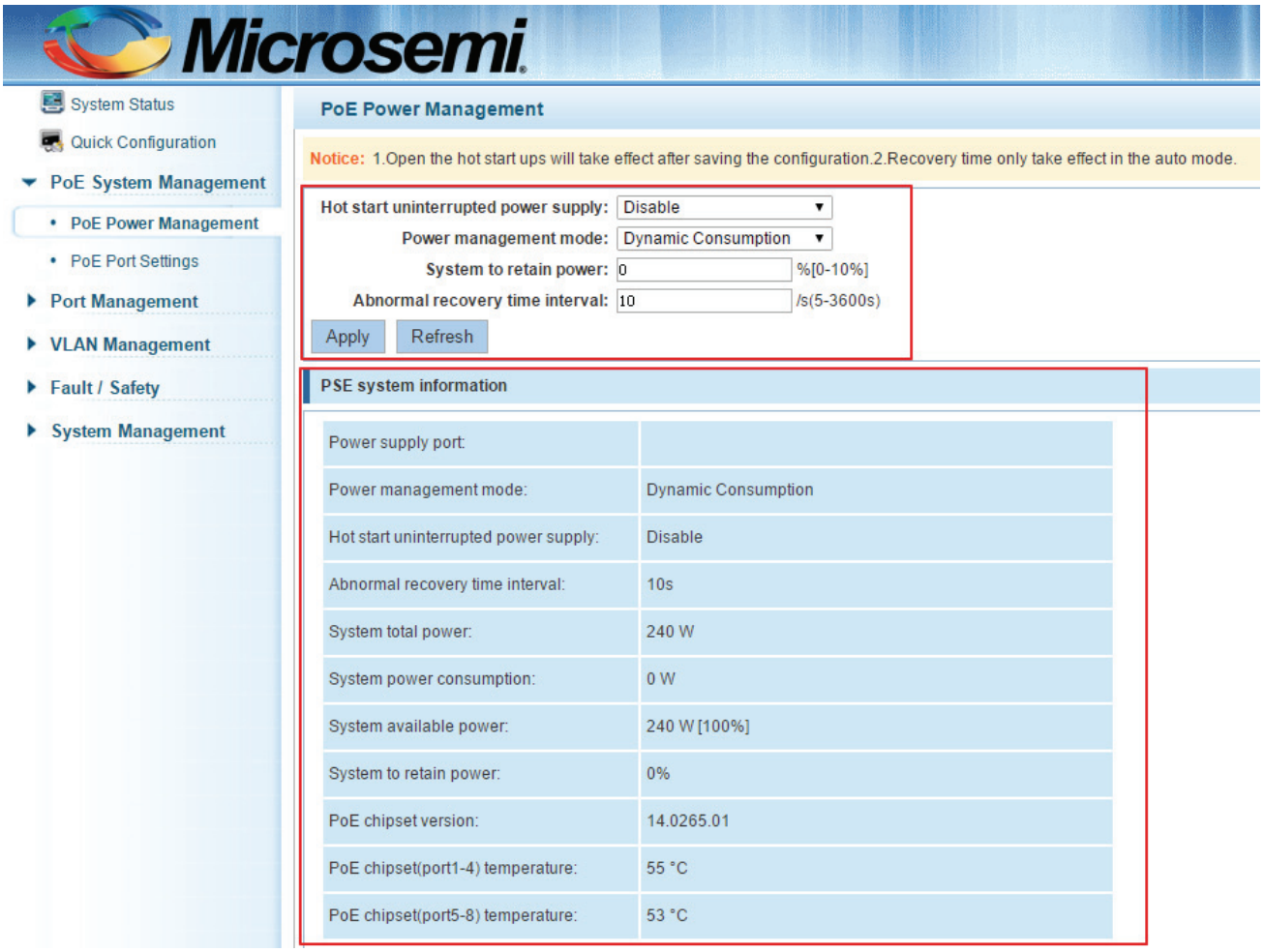


Figure 4-1: View the PoE system management configuration information

4.1.1 OPEN HOT START

Click on "PoE System Management""PoE Power Management", in the warm start uninterrupted Power supply drop-down list, select "Enable", click "Apply" button, complete the configuration:

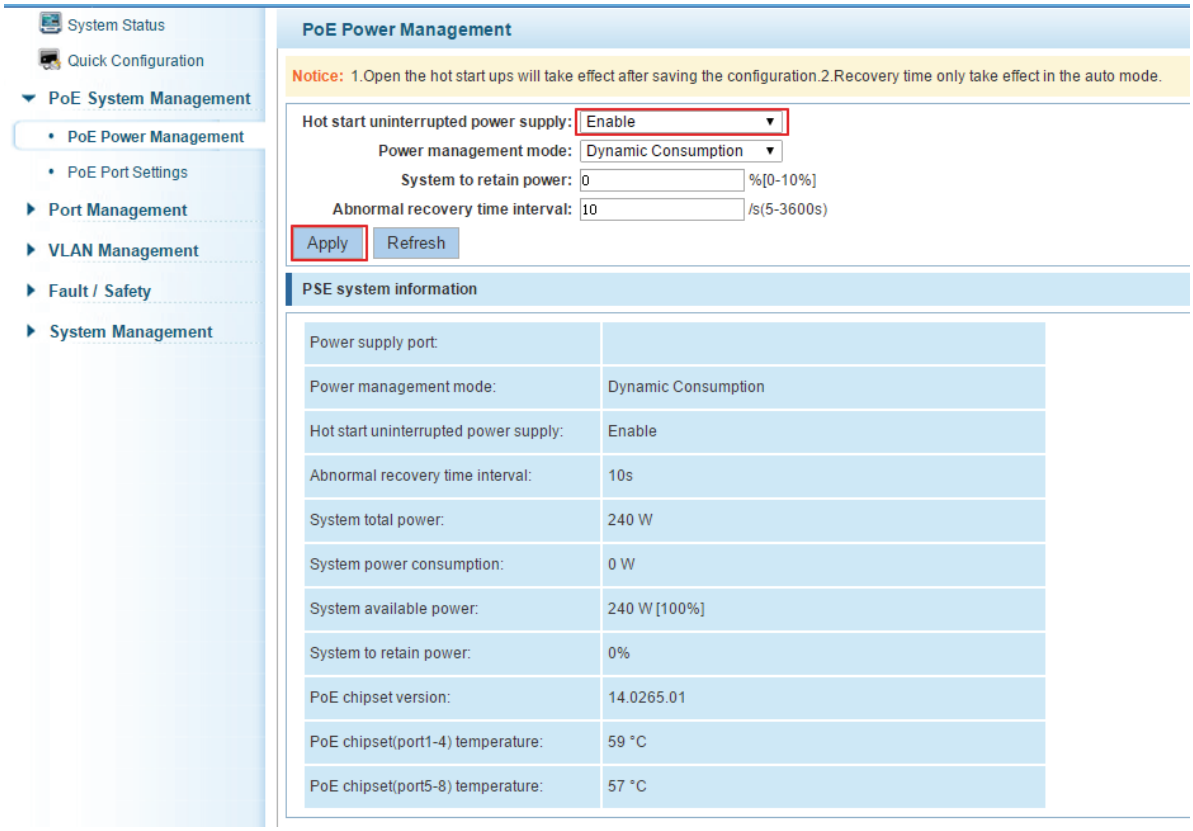


Figure 4-2: Open the hot start uninterrupted power supply

Power supply port:	
Power management mode:	Dynamic Consumption
Hot start uninterrupted power supply:	Enable
Abnormal recovery time interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W [100%]
System to retain power:	0%
PoE chipset version:	14.0265.01
PoE chipset(port1-4) temperature:	59 °C
PoE chipset(port5-8) temperature:	59 °C

Figure 4-3: Set up after a successful result

Open the warm start uninterrupted power supply configuration steps are as follows:

Configuration type	Steps	Operation description
Open the hot start uninterrupted power supply	**Step1**	In the warm start uninterrupted power supply drop-down list, select "Enable".
	Step2	Click "Apply" button, complete the configuration.

By default, turn off the hot start function.

4.1.2 CLOSE THE HOT START

Click on "PoE System Management""PoE Power Management", in the warm start uninterrupted Power supply drop-down list, select "Disable", click "Apply" button, complete the configuration:

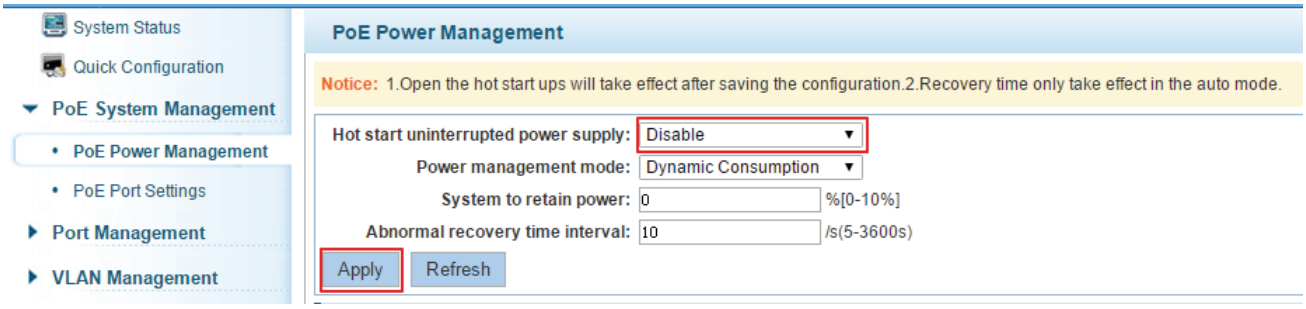


Figure 4-4: Close the warm start uninterrupted power supply

Power supply port:	
Power management mode:	Dynamic Consumption
Hot start uninterrupted power supply:	Disable
Abnormal recovery time interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W [100%]
System to retain power:	0%
PoE chipset version:	14.0265.01
PoE chipset(port1-4) temperature:	59 °C
PoE chipset(port5-8) temperature:	59 °C

Figure 4-5: Set up the success

Close the warm start uninterrupted power supply configuration steps are as follows:

Configuration type	Steps	Operation description
Close the warm start uninterrupted power supply	Step1	In hot start uninterrupted power supply drop-down list, select "Disable"
	Step2	Click "Apply" button, complete the configuration.

4.1.3 MODIFYING THE POWER SUPPLY MODE

Click on "PoE System Management""PoE Power Management", needs in the Power supply mode drop-down list, select Power supply mode, click "Apply" button, complete the configuration; The power supply mode choice: energy saving mode:

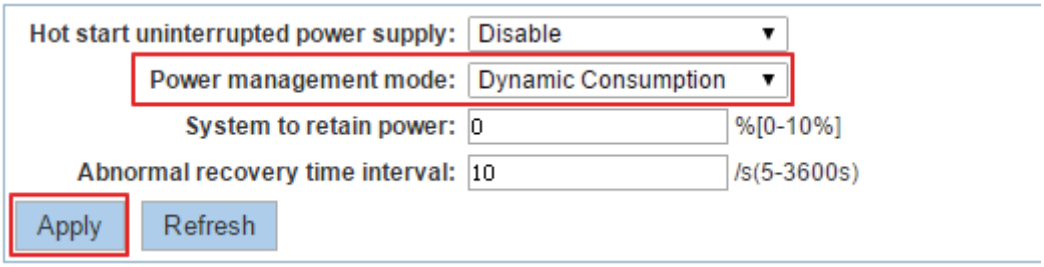


Figure 4-6: Modify the power supply mode

Power supply port:	
Power management mode:	Dynamic Consumption
Hot start uninterrupted power supply:	Disable
Abnormal recovery time interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W [100%]
System to retain power:	0%
PoE chipset version:	14.0265.01
PoE chipset(port1-4) temperature:	59 °C
PoE chipset(port5-8) temperature:	59 °C

Figure 4-7: Set up after a successful result

Modify the power supply mode configuration steps are as follows:

Configuration Type	step	Operation Description
Modify power mode	**Step1**	Select Power Mode drop-down list "Dynamic Consumption";
	Step2	Click the "Apply" button to complete the configuration.

By default, the power supply mode to automatic mode.

4.1.4 SETTING THE SYSTEM TO RETAIN POWER

Click "PoE System Management""PoE Power Management"，In the text box, the system keeps the input power required to retain power, click on the "Apply" button to complete the configuration; here the system to retain power 10%

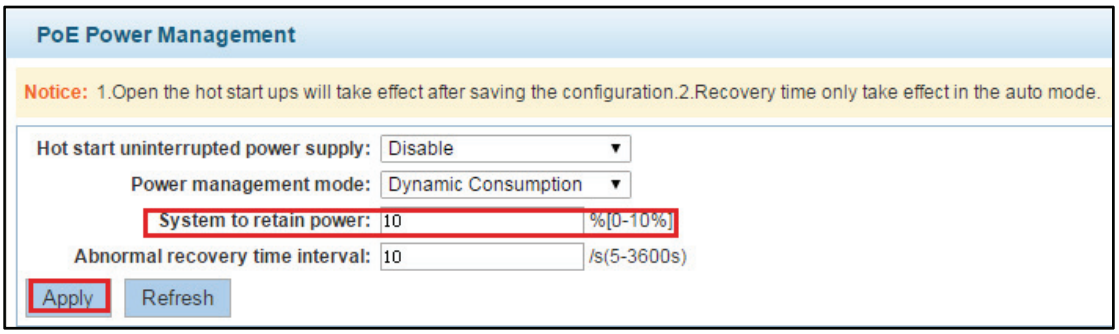


Figure 4-8: Set the system to retain power

Power supply port:	
Power management mode:	Dynamic Consumption
Hot start uninterrupted power supply:	Disable
Abnormal recovery time interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	216 W [90%]
System to retain power:	10%
PoE chipset version:	14.0265.01
PoE chipset(port1-4) temperature:	59 °C
PoE chipset(port5-8) temperature:	59 °C

Figure 4-9: Setting Success

Is disposed to retain power system configured as follows:

Configuration Type	Step	Operation Description
Modify power mode	**Step1**	Enter a value in the text box to retain power in the system;
	Step2	Click the "Apply" button to complete the configuration.

You can use the system to retain power in the power saving mode;

System retains the power range of 0-10%

4.1.5 SETTING THE RECOVERY INTERVAL

Click on "PoE System Management""PoE Power Management", abnormal recovery time in the text box to set the time interval, click on the "Apply" button to complete the configuration; this time interval: 10s

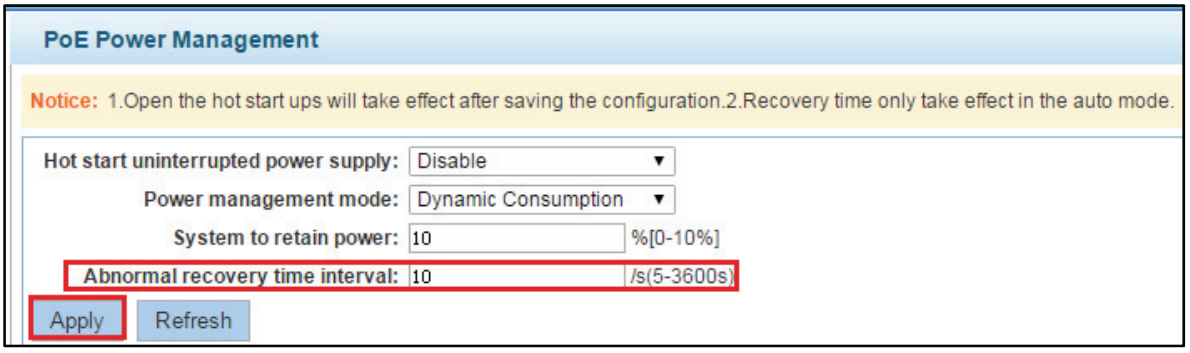


Figure 4-10: Setting the recovery interval

Power supply port:	
Power management mode:	Dynamic Consumption
Hot start uninterrupted power supply:	Disable
Abnormal recovery time interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	216 W [90%]
System to retain power:	10%
PoE chipset version:	14.0265.01
PoE chipset(port1-4) temperature:	61 °C
PoE chipset(port5-8) temperature:	59 °C

Figure 4-11:Setting after successful results

Set the recovery interval configuration steps are as follows:

Configuration Type	Step	Operation Description
Set the recovery interval	**Step1**	Input error recovery interval text box, enter "10";
	Step2	Click the "Apply" button to complete the configuration.

Gap time default is 10s;

System retains power range 5-3600s.

4.2 POE PORT CONFIGURATION

Clickon "PoE System Management""PoE Port Settings", you can view information POE port configuration:

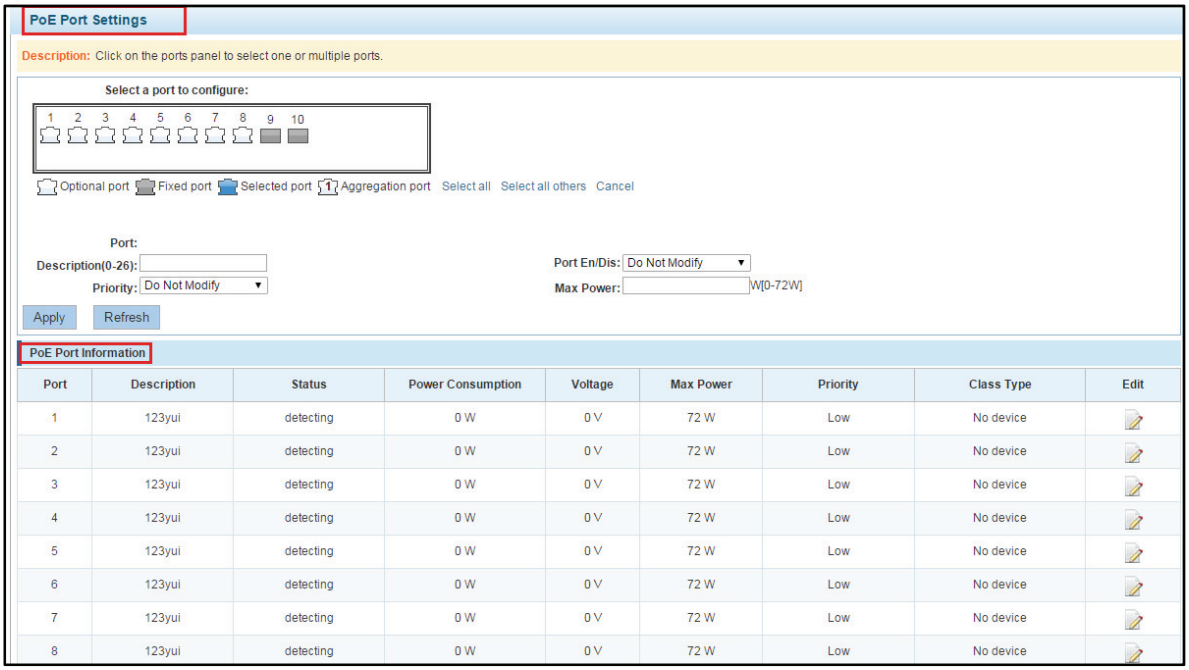


Figure 4-12: POE port configuration information

4.2.1 MODIFY ENABLE POWER

Click on "PoE System Management""PoE Power Management", in the port panel, select the port number to be configured, so that power can choose to: Disable, click on the "Apply" button to complete the

configuration:

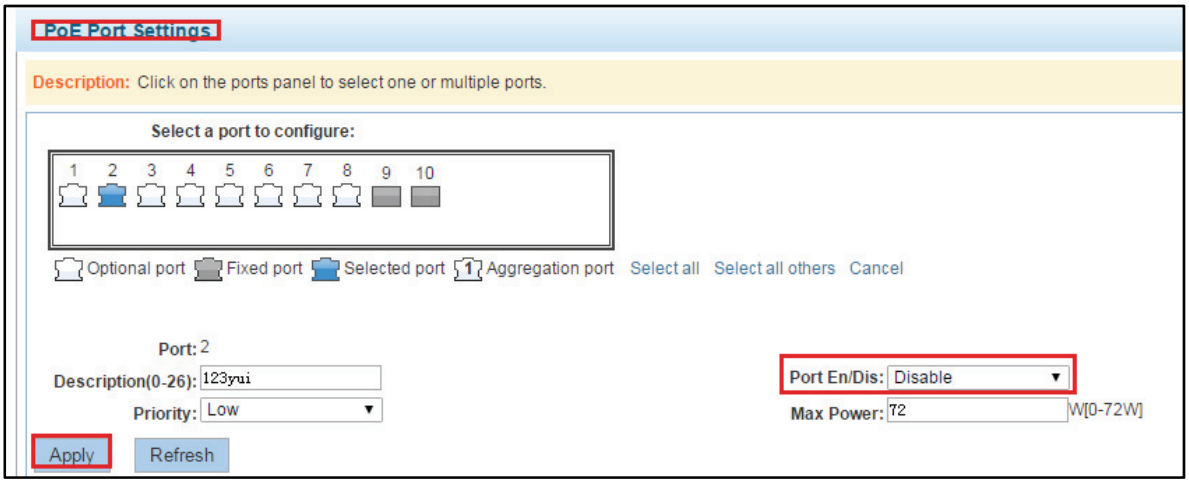
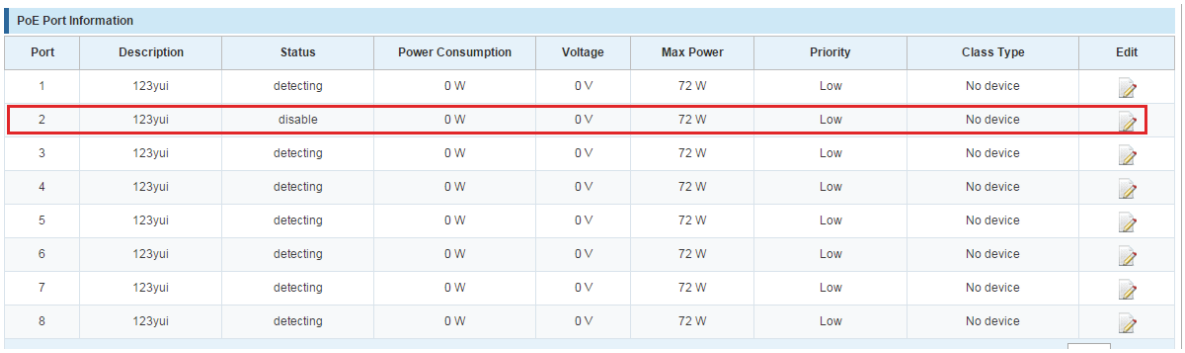


Figure 4-13: Modify power enabled



PoE Port Information

Port	Description	Status	Power Consumption	Voltage	Max Power	Priority	Class Type	Edit
1	123yui	detecting	0 W	0 V	72 W	Low	No device	
2	123yui	disable	0 W	0 V	72 W	Low	No device	
3	123yui	detecting	0 W	0 V	72 W	Low	No device	
4	123yui	detecting	0 W	0 V	72 W	Low	No device	
5	123yui	detecting	0 W	0 V	72 W	Low	No device	
6	123yui	detecting	0 W	0 V	72 W	Low	No device	
7	123yui	detecting	0 W	0 V	72 W	Low	No device	
8	123yui	detecting	0 W	0 V	72 W	Low	No device	

Figure 4-14: Setting Results of successfully

Modify power enable configuration steps are as follows:

Configuration Type	Step	Operation Description
Modify Enable Power	**Step1**	In the port panel, select the need to configure the port number 2;
	Step2	Do not power enables a pulldown menu, select "Disabled";
	Step3	Click the "Apply" button to complete the configuration.

The default power supply is turned on is enabled;

Can select multiple ports bulk edit.

4.2.2 MODIFY THE PORT DESCRIPTION

Click on "PoE System Management""PoE Port Settings", in the port panel, select the need to configure the port number in the port description text box, enter a description, click on the "Apply" button to complete the configuration：

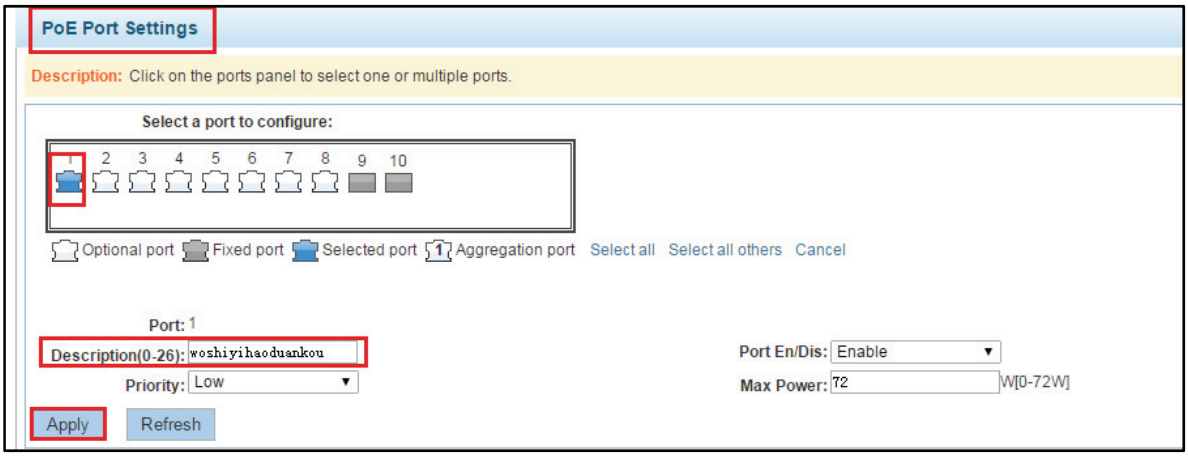
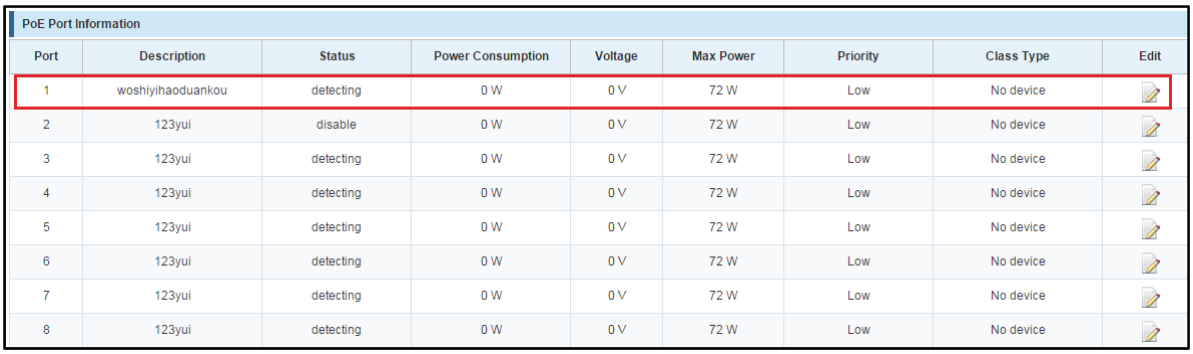


Figure 4-15: Modify the port description



PoE Port Information

Port	Description	Status	Power Consumption	Voltage	Max Power	Priority	Class Type	Edit
1	woshiyihaoduankou	detecting	0 W	0 V	72 W	Low	No device	
2	123yui	disable	0 W	0 V	72 W	Low	No device	
3	123yui	detecting	0 W	0 V	72 W	Low	No device	
4	123yui	detecting	0 W	0 V	72 W	Low	No device	
5	123yui	detecting	0 W	0 V	72 W	Low	No device	
6	123yui	detecting	0 W	0 V	72 W	Low	No device	
7	123yui	detecting	0 W	0 V	72 W	Low	No device	
8	123yui	detecting	0 W	0 V	72 W	Low	No device	

Figure 4-16: Setting Success

Modifying port configuration is described as follows:

Configuration Type	Step	Operation Description
Modify port description	**Step1**	In the port panel, select the need to configure the port number 1;
	Step2	Port Description text box, type in "I'm One Port" ；
	Step3	Click the "Apply" button to complete the configuration.

The default is no port description;

Can select multiple ports bulk edit.

4.2.3 MODIFY THE PRIORITY

Click on "PoE System Management""PoE Port Settings", in the port panel, select the port number to be configured, select the desired priority, click on the "Apply" button to complete the configuration in thePriority drop-down list:

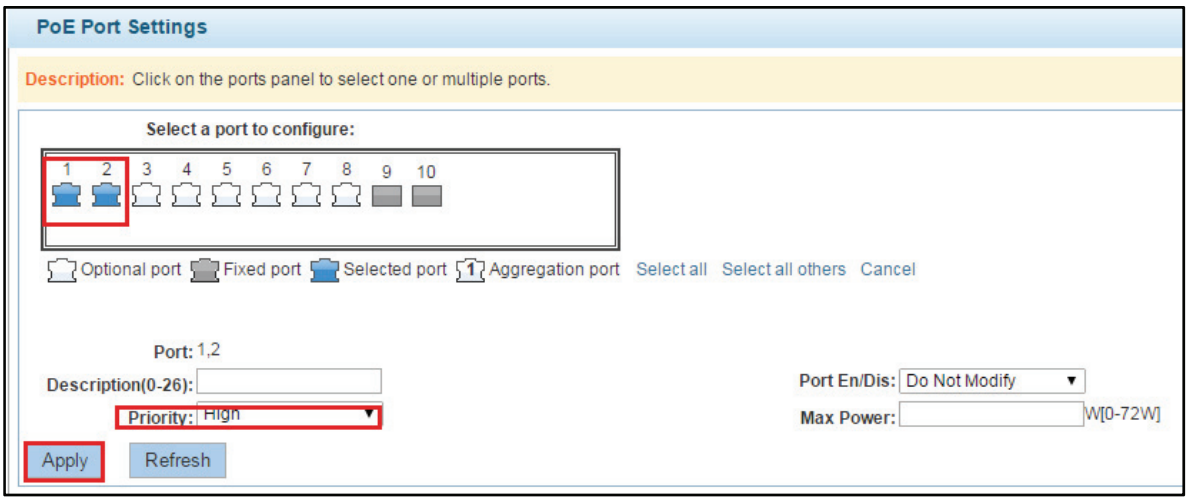


Figure 4-17: Modify priority

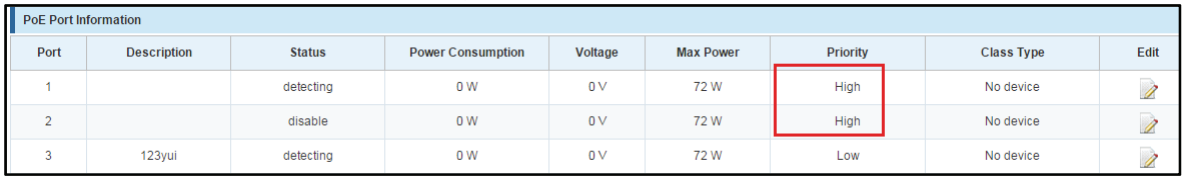


Figure 4-18: Setting Results of successfully

Modify priority configuration steps are as follows:

Configuration Type	Step	Operation Description
Modify priority	**Step1**	In the port panel, select the port number to be configured 1,2;
	Step2	Select Priority drop-down list in the "high";
	Step3	Click the "Apply" button to complete the configuration.

The default priority is low;

There are four priority levels can be selected: critical, high, medium, low;

Can select multiple ports bulk edit.

4.2.4 MODIFY THE MAXIMUM POWER

Click on "PoE System Management""PoE Port Settings", in the port panel, select the port number to be configured, the maximum value of the input power required in the text box, click on the "Apply" button to complete theconfiguration:

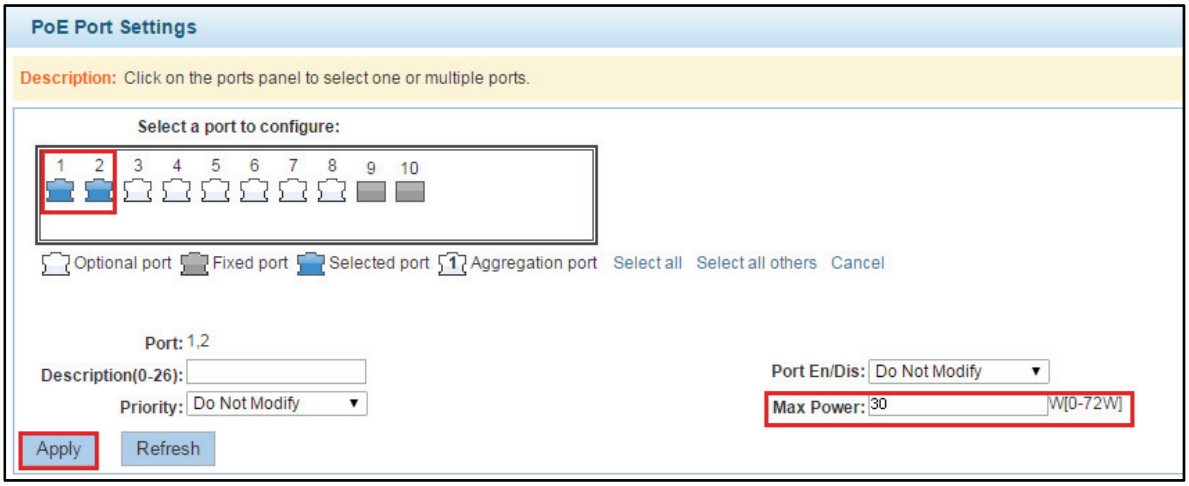


Figure 4-19: Modify the maximum power

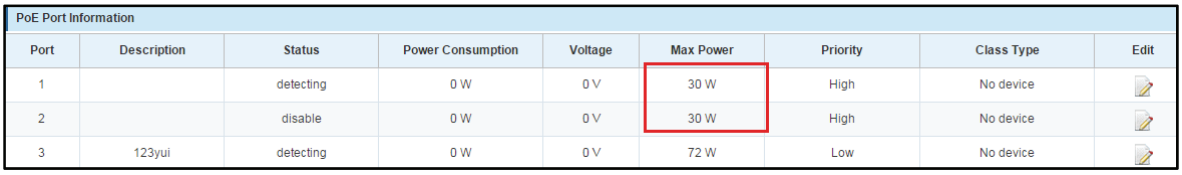


Figure 4-20: Setting Success

Modify the maximum power configuration steps are as follows:

Configuration Type:	Step	Operation Description
To modify the maximum power	**Step1**	In the port panel, select the port number to be configured 1,2;
	Step2	Maximum power input text box, enter "30";
	Step3	Click the "Apply" button to complete the configuration.

The default maximum power of 72w;

Maximum power range: 0-72w;

Can select multiple ports bulk edit.

4.2.5 MODIFY POWER DISTRIBUTION

Click on "PoE System Management""PoE Port Settings", in the port panel, select the port number to be configured, the value of the input power distribution needs in the text box, click on the "Apply" button to complete the configuration:

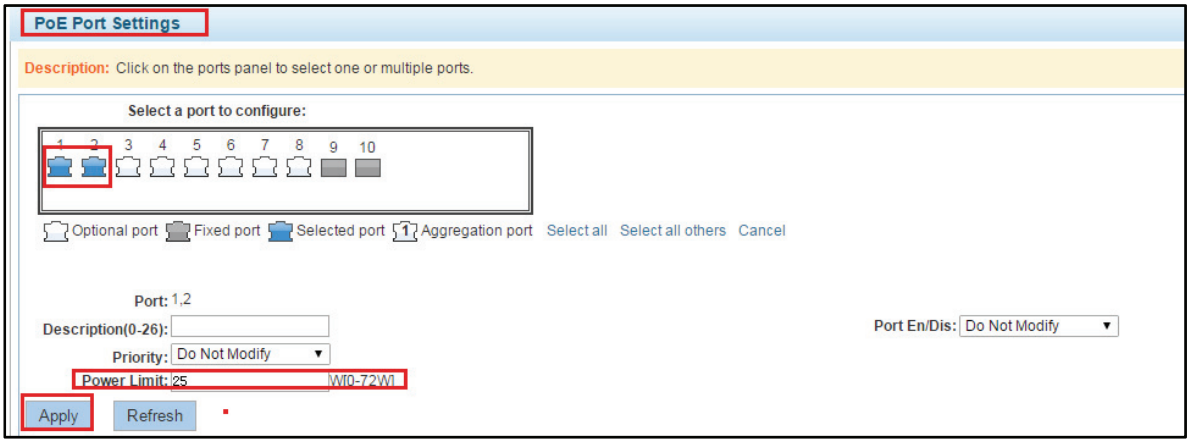
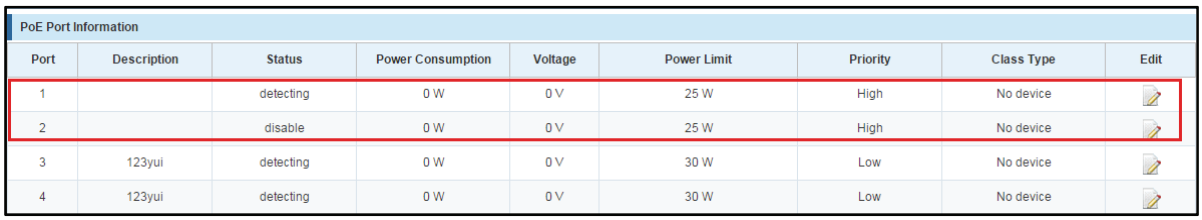


Figure 4-21: Modify power distribution



PoE Port Information

Port	Description	Status	Power Consumption	Voltage	Power Limit	Priority	Class Type	Edit
1		detecting	0 W	0 V	25 W	High	No device	
2		disable	0 W	0 V	25 W	High	No device	
3	123yui	detecting	0 W	0 V	30 W	Low	No device	
4	123yui	detecting	0 W	0 V	30 W	Low	No device	

Figure 4-22: Setting Results of successfully

Modify power distribution configuration steps are as follows:

Configuration Type	Step	Operation Description
Modify power distribution	**Step1**	In the port panel, select the port number to be configured 1,2;
	Step2	In the power distribution box, enter the text "25";
	Step3	Click the "Apply" button to complete the configuration.

1-8 default port assignment power 30w, maximum allocated power 72w;

Allocated in static power supply mode is enabled.

Maximum power range: 0-72w;

Can select multiple ports bulk edit.

5 CHAPTER VI PORT MANAGEMENT

5.1 BASIC SETTINGS

5.1.1 CHECK THE PORT CONFIGURATION

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

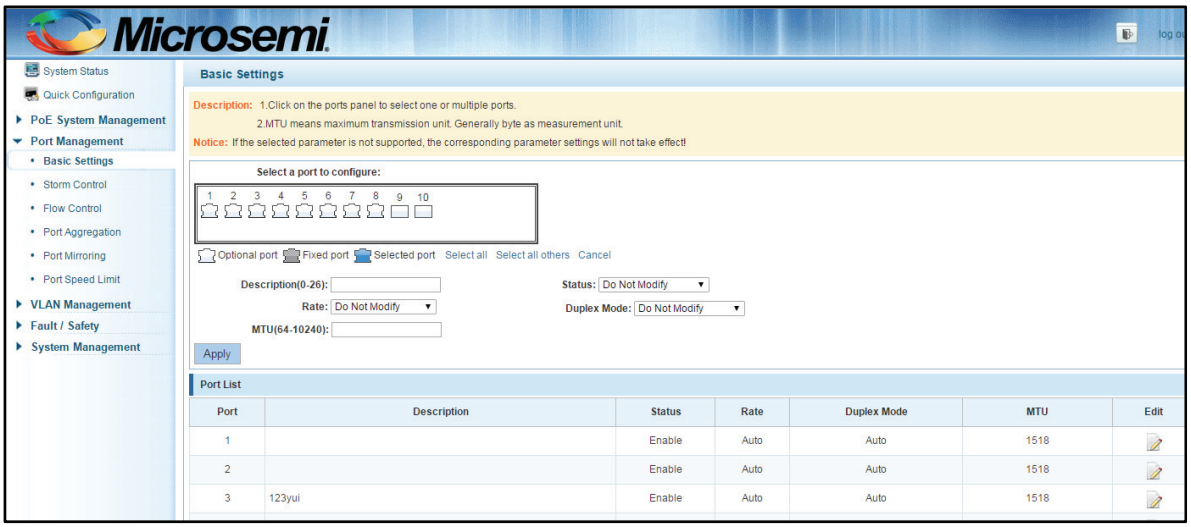


Figure 5-1: Port list information

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

- Port: The number of the port;
- Port Description: Displays the contents of the switch port description;
- Port Status: switch port status information, on / off;
- Port Rate: Displays the switch port speed configuration, auto-negotiation / 10/100/1000;
- Working Mode: Displays the switch port configuration duplex, auto-negotiation / full / half duplex;
- Mtu: Indicates the port is the maximum length of the packet;

Reminder

Optical multiplexing port rate can only auto-negotiation / 1000; mode only auto-negotiation / full duplex.

5.1.2 CONFIGURING PORT PROPERTIES

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

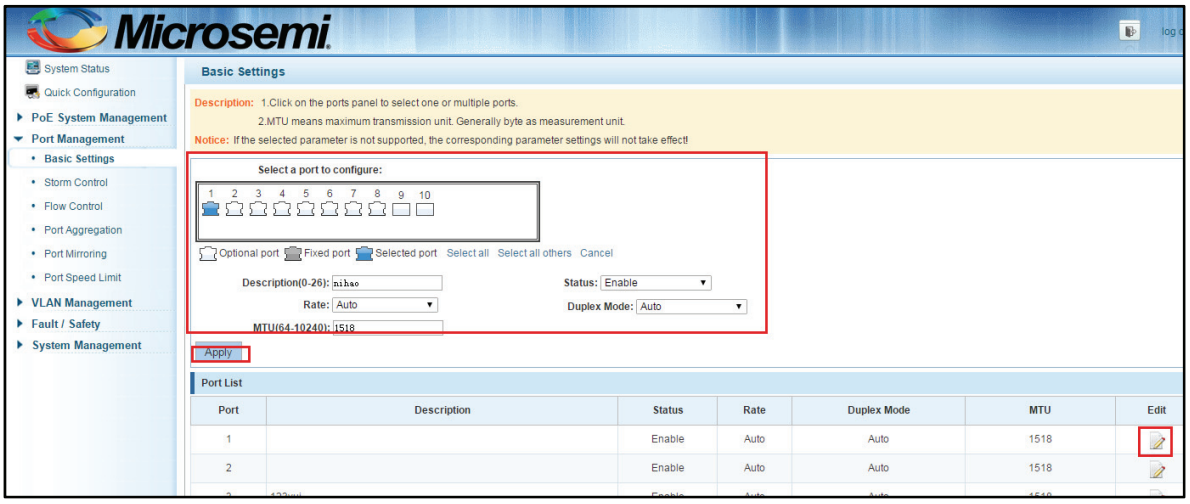


Figure 5-2: Port Properties configuration of FIG.

To configure port properties as follows:

Step	Operation Description
Step1	Click the "Edit" icon
Step2	In the Port Properties configuration page Fill / select the value to be configured
Step3	Click the "Apply" button to complete the configuration.

Reminder

Description column supports input Chinese characters。

5.2 STORM CONTROL

5.2.1 CHECK THE PORT SETTINGS STORM

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

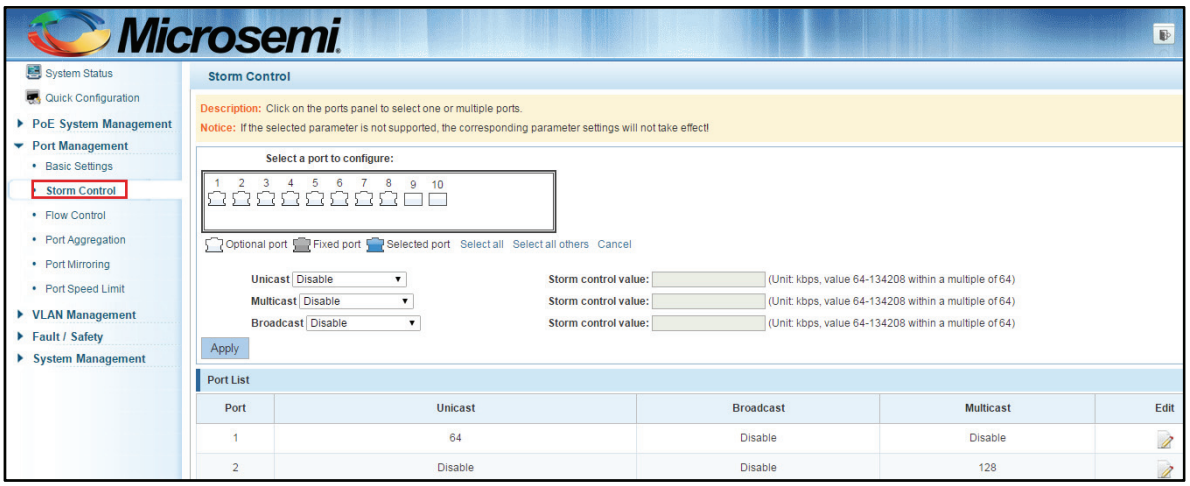


Figure 5-3: Storm Control List information

In the list of ports which shows the property values of the current storm control switch:

- Port: The number of the port
- Unicast: unknown unicast packets control
- Broadcast: Broadcast packet control
- Multicast: multicast packets control prompt
- When set the control value is not a multiple of 64, the system automatically matches similar multiples of 64.
- Control value unicast, broadcast, multicast, while only a single value for the control.

By clicking on the port panel "" corresponding port" , select the port to be controlled.

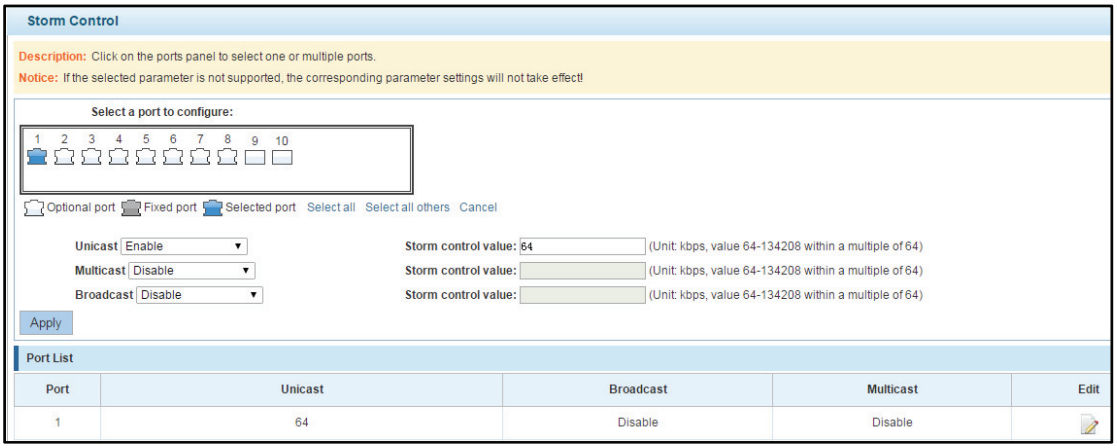


Figure 5-4: Configuring Storm Control information

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

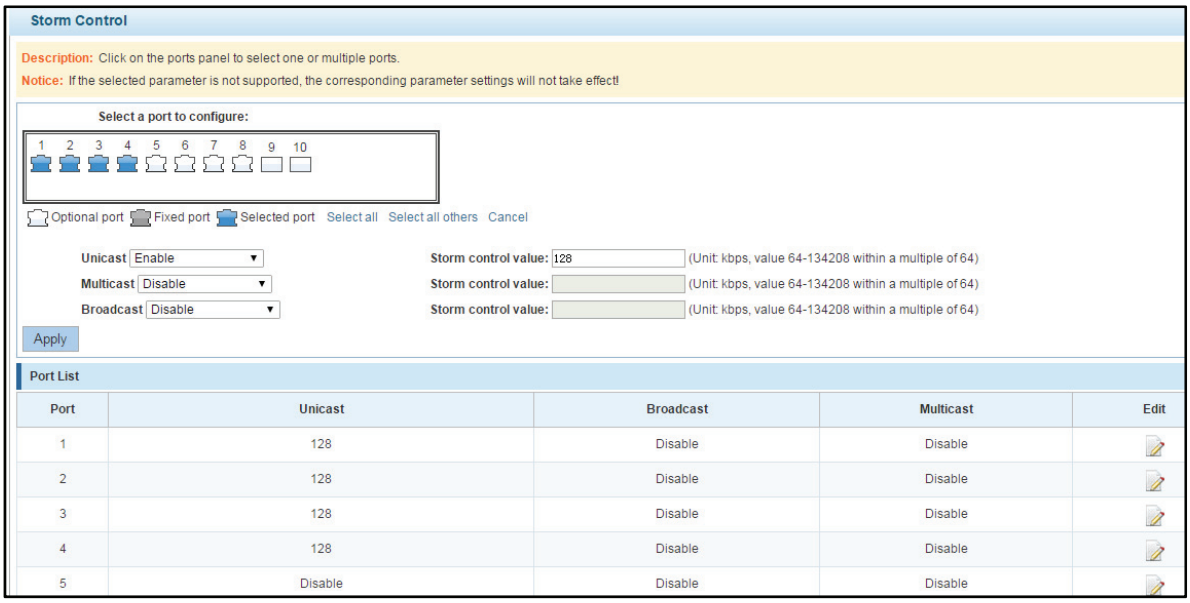


Figure 5-5: Bulk edit configuration information

After the selected ports in the Storm Control category, set the unicast, multicast, broadcast value, such as setting the port number 1 unicast storm control is 128. Click Save Settings.

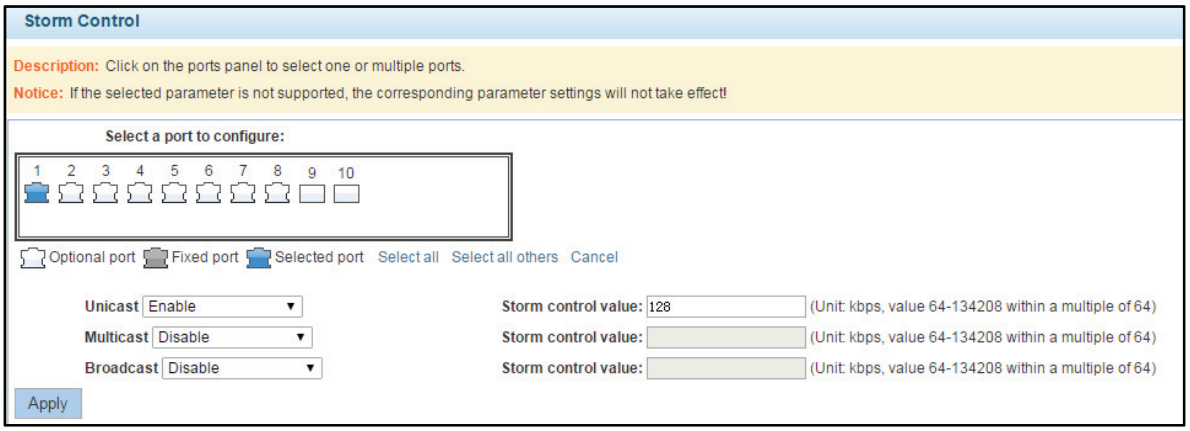


Figure 5-6: Configuring Storm Control information

After the configuration, as shown below:

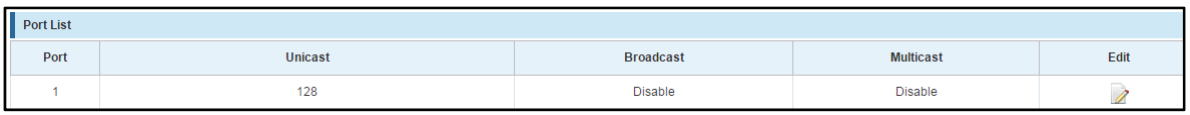


Figure 5-7: Configuration successfully Storm Control information flow control

5.2.2 VIEWING TRAFFIC CONTROL LIST

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

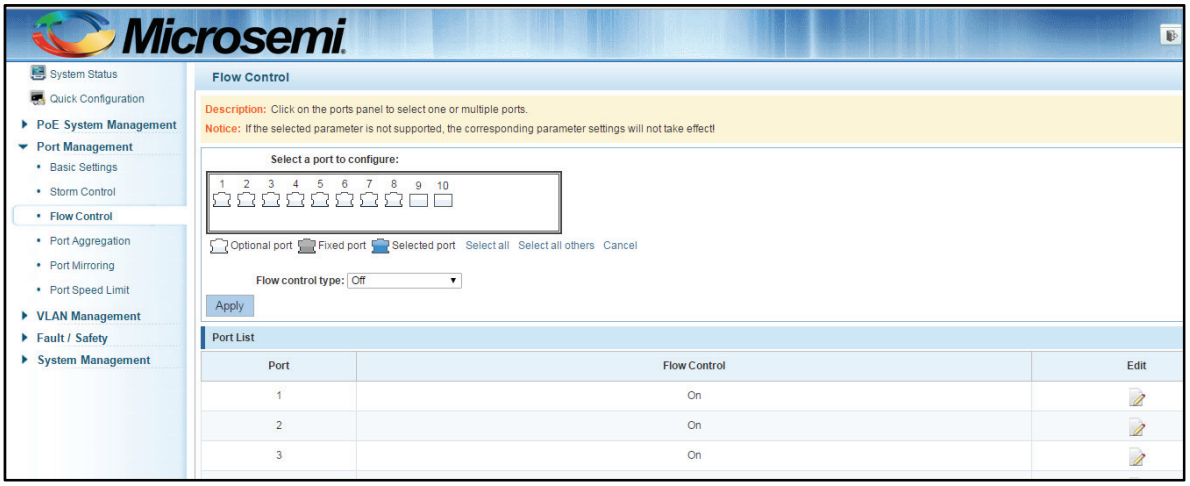


Figure 5-8: Flow Control Information

5.2.3 CONFIGURING FLOW CONTROL

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

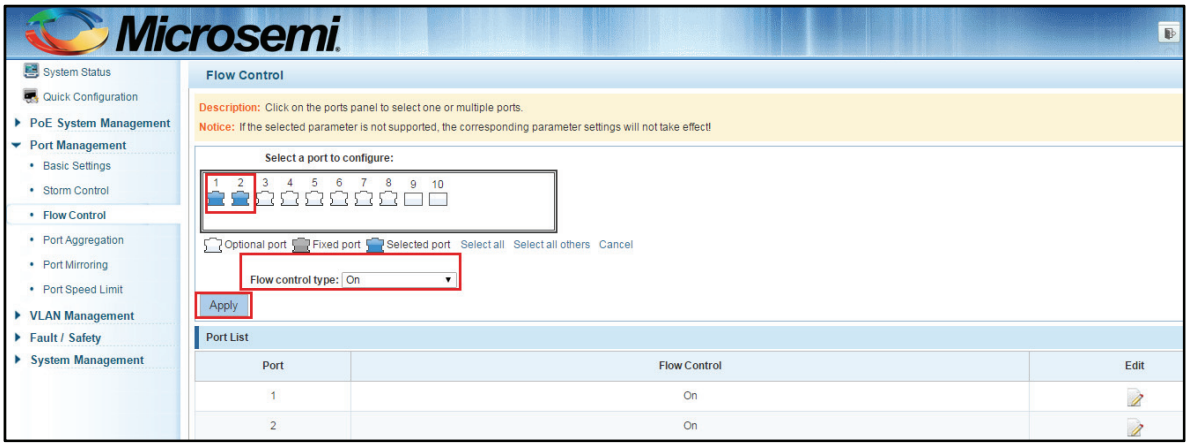


Figure 5-9: Open port flow control function

Open port traffic control, follow these steps:

Configuration Type	Step	Operation Description
Open port traffic control	**Step1**	Select Open port traffic control;
	Step2	Select Open in "Flow control type"on;
	Step3	Click "Apply"

View Configuration list to display configuration is successful:

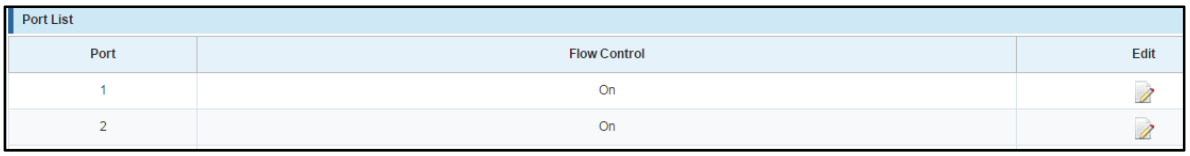


Figure 5-10: Port flow control status

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

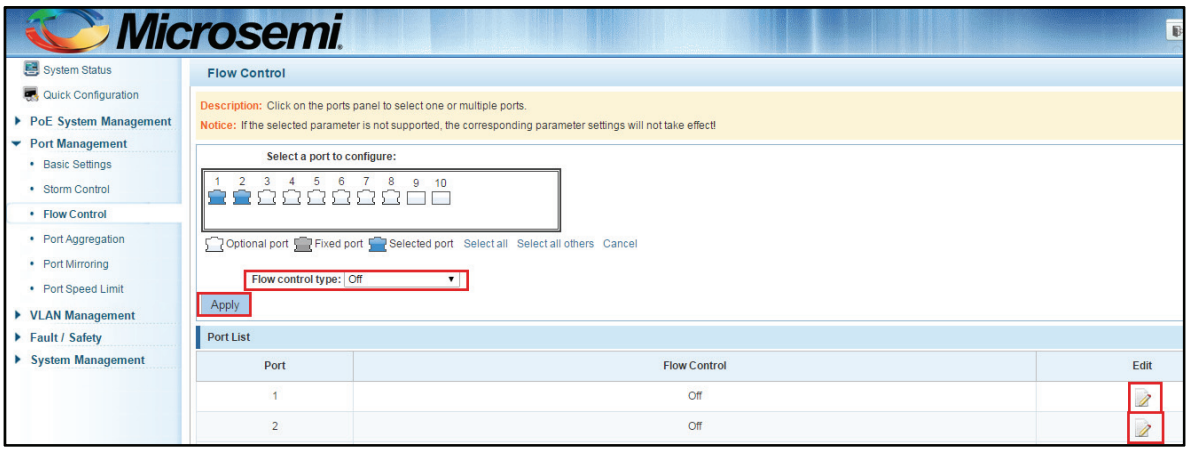


Figure 5-11: Close the port flow control

Close port traffic control, follow these steps:

Configuration Type	Step	Operation Description
Close port traffic control	**Step1**	Select the button to the right of the port or directly selected port;
	Step2	In the "Flow control type" select Off;
	Step3	Click "Apply";

5.3 PORT AGGREGATION

5.3.1 VIEWING PORT AGGREGATION CONFIGURATION

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

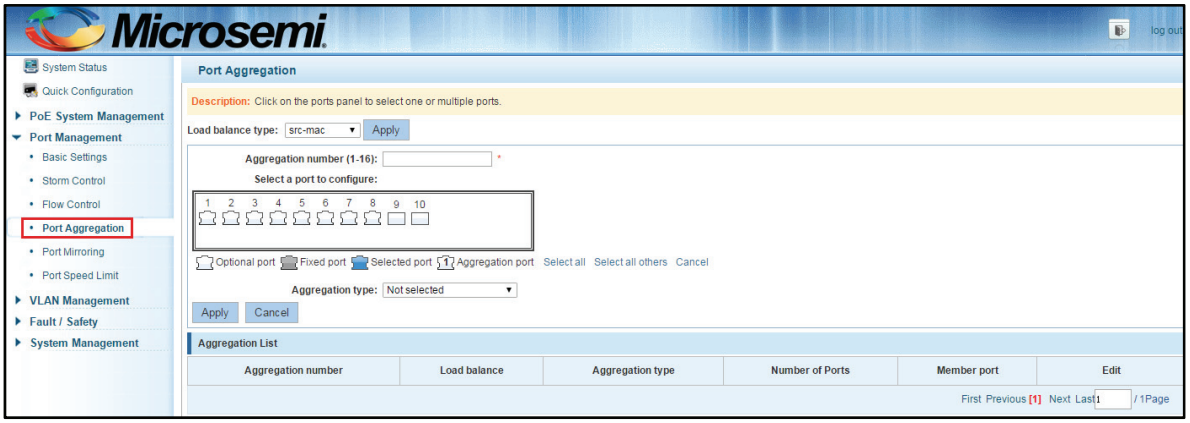


Figure 5-12: Aggregation port configuration information

In the port aggregation list which shows the current switch port configuration information for the polymerization properties:

- Aggregation number: display link aggregation group number value;
- Load Balancing: Displays the current link aggregation group load balancing judgment condition;
- Aggregate types: Displays whether to use a polymerization port LACP protocol;
- Member ports quantity: Displays the number of ports in the link aggregation group contains a total of member port: Displays the current port link aggregation group member prompt
- Each aggregate port can bind up to eight member ports, port to transfer data among members of the network traffic through the shunt rules.
- Port aggregation group must ensure that the port speed, duplex, port state agreement, or can not ATTACH after configuration.

5.3.2 ADD PORT AGGREGATION

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

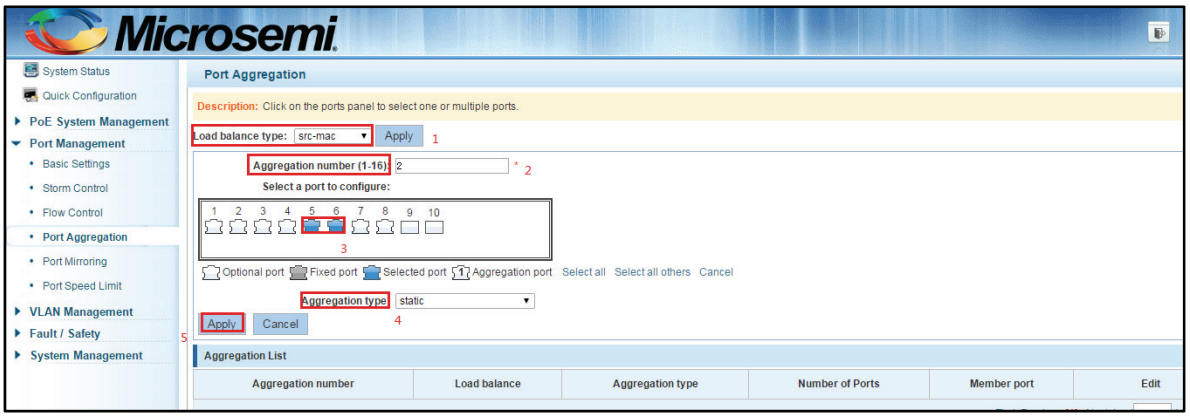


Figure 5-13: Port Aggregation Configuration area

Increase port aggregation, follow these steps:

Configuration Type	Step	Operation Description
Increase port aggregation	**Step1**	Select the option to load the shunt in the load balancing list.
	Step2	Enter the number in the "Aggregation number" in.
	Step3	Select the aggregated ports in the panel ◦
	Step4	Select the aggregation type.
	Step5	Click the "Apply" button to complete the configuration.

5.3.3 MODIFYING PORT AGGREGATION

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

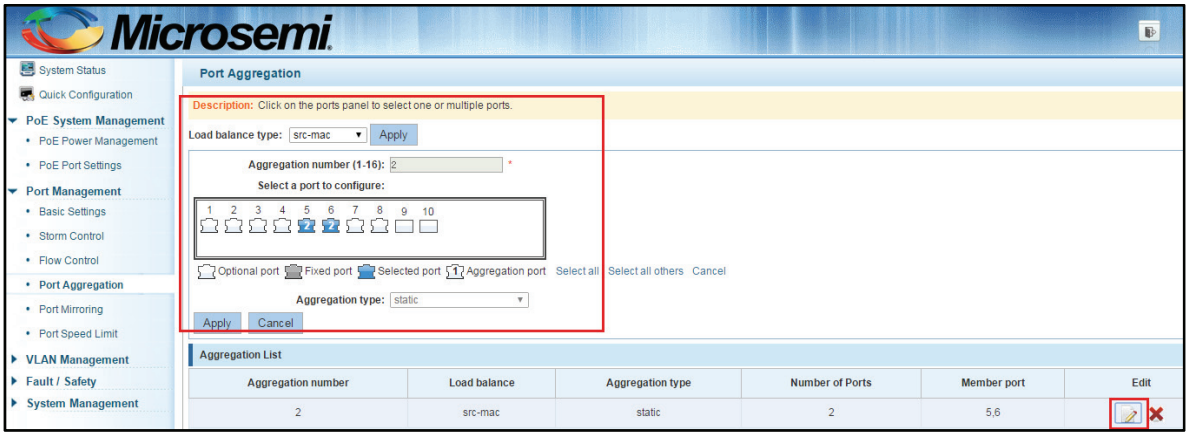


Figure 5-14: To modify the port aggregation

Modify Link Aggregation Procedure:

Configuration Type	Step	Operation Description
Modify port aggregation	**Step1**	In the "Aggregation List Click to modify the right of the port aggregation
	Step2	In the port aggregation configuration page to modify the load balancing type and click Next to "Apply".
	Step3	Select the port to be added to the aggregation port.
	Step4	Click the "Apply" button to complete the configuration.

5.3.4 DELETE PORT AGGREGATION

Select the port to be deleted aggregation, click the "X" button, you can delete the configured port aggregation:

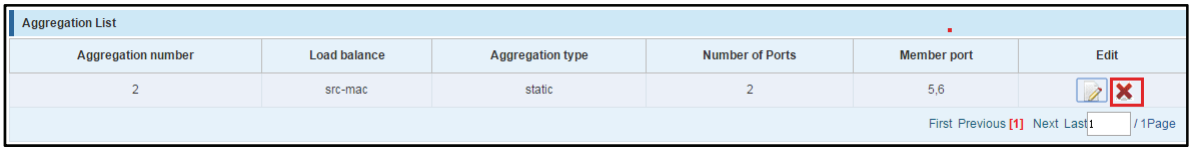


Figure 5-15: Delete port aggregation

To delete a port aggregation group, follow these steps:

Configuration Type	Step	Operation Description
Remove port aggregation	**Step1**	Click the link aggregation group on the right. ""
	Step2	Confirm Delete to finish deleting the configuration

5.4 PORT MIRRORING

5.4.1 PORT MIRRORING CONFIGURATION

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

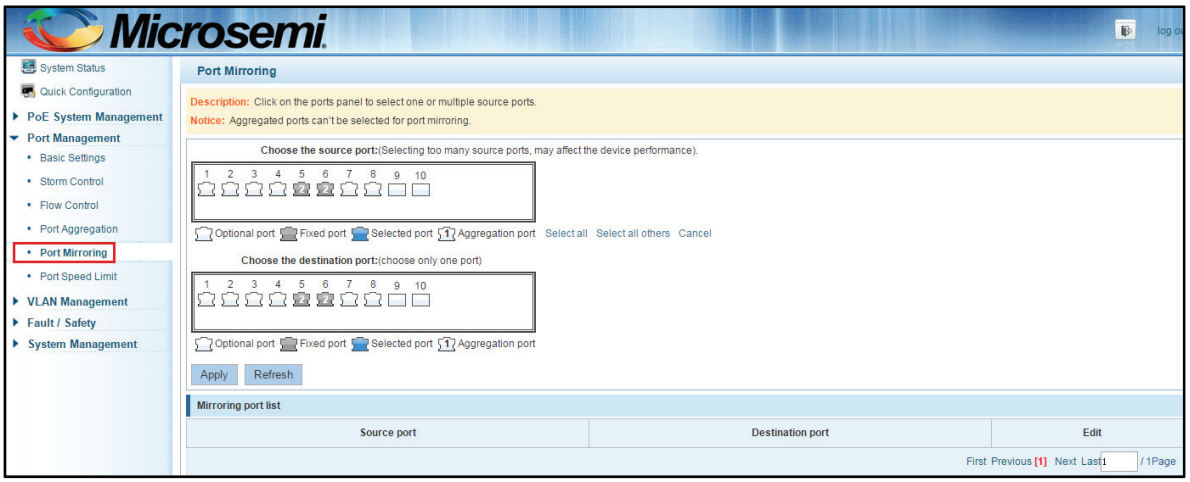


Figure 5-16: Port mirroring configuration information

In the Port Mirroring is a property list which shows the configuration of the current mirror switch:

Mirroring group: mirroring group ID, can be configured up to seven mirroring group;

Source Port: The port forwarding on the source data is mirrored to the destination port;

Destination port: mirror data sent to the destination port.

- Port aggregation port can not be used as the destination port and source port;
- Destination port and source port can not be the same;
- Same group mirroring group can have only one destination port.

5.4.2 ADD PORT MIRRORING GROUP

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

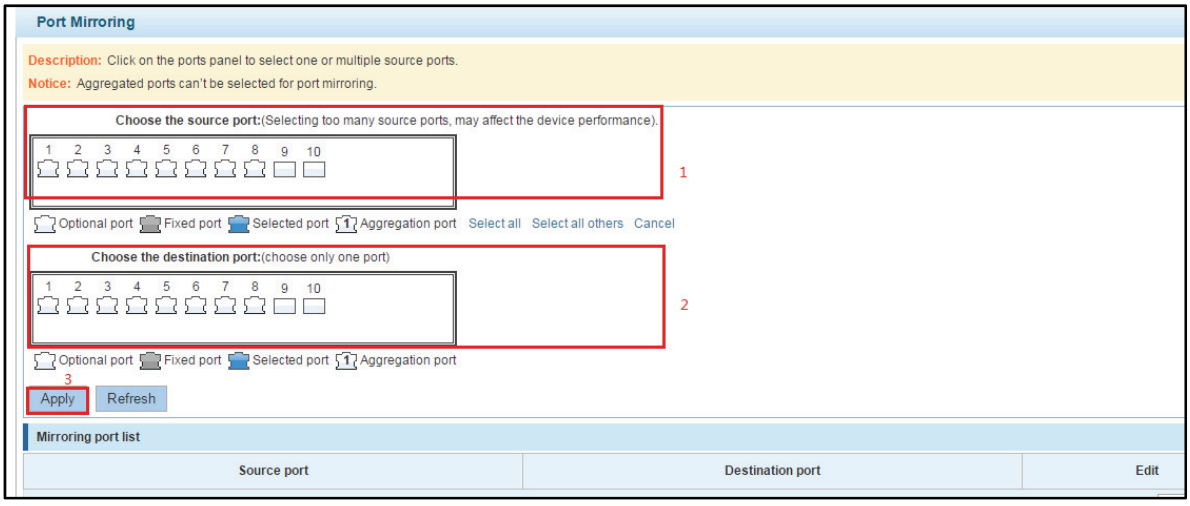


Figure 5-17: Add port mirroring group

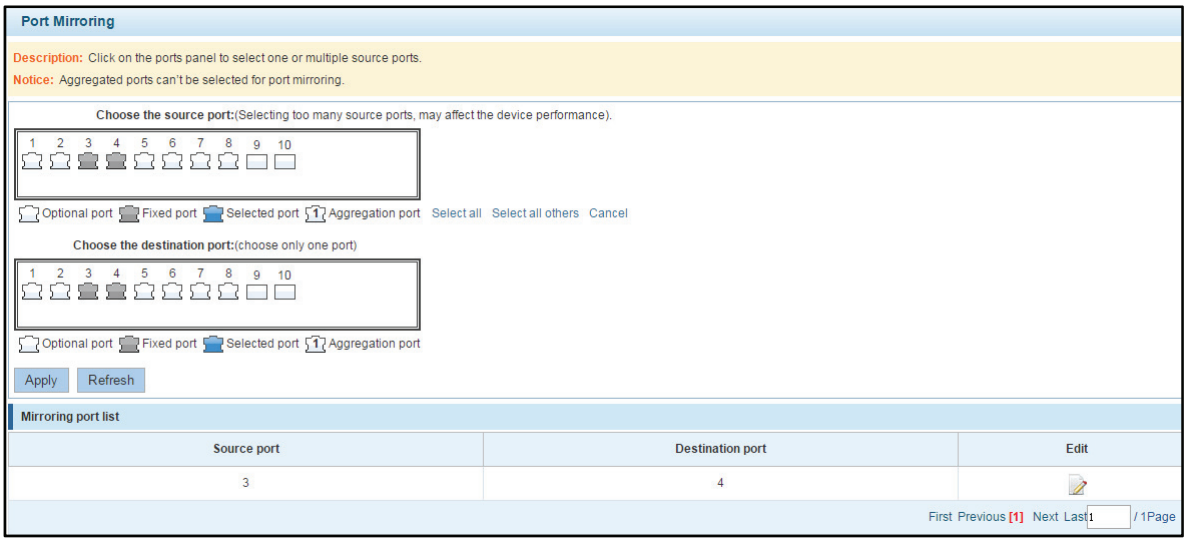


Figure 5-18: Add port mirroring group results

Port mirroring configuration steps are as follows:

Configuration Type	Step	Operation Description
Port Mirroring Configuration	**Step1**	Select "Source Port"
	Step2	Select "Destination Port"
	Step3	Click"Apply"

Configuration instructions:

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

5.4.3 TO MODIFY THE PORT MIRRORING GROUP

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

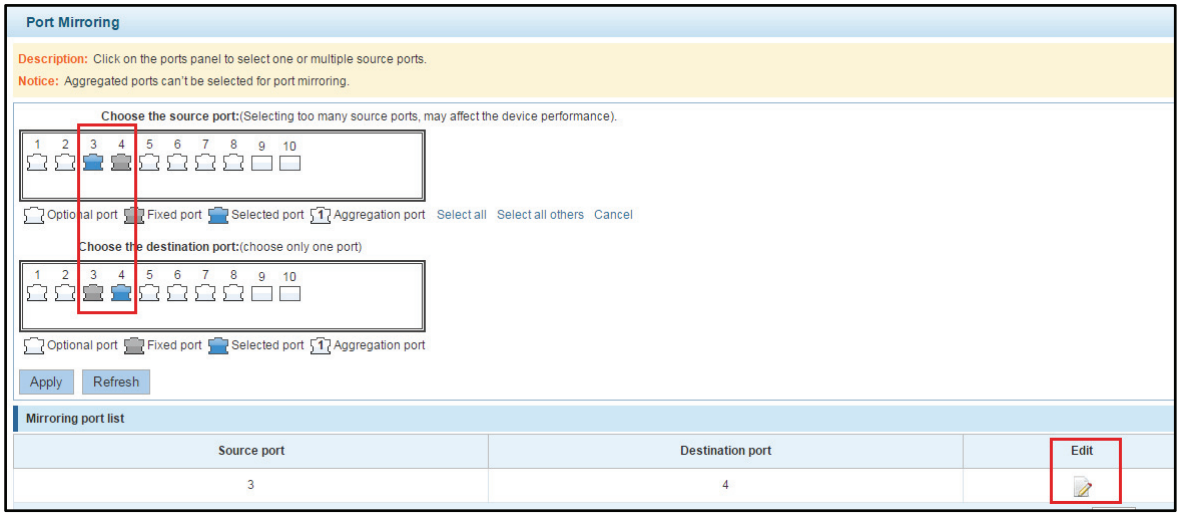


Figure 5-19: To modify the port mirroring group

Modify the port mirroring configuration steps are as follows:

Configuration Type	Step	Operation Description
Modify mirroring group	**Step1**	In the image you want to modify the operation of the group column, click on " " ;
	Step2	Add or remove the corresponding port in the panel;
	Step3	Click "Apply"

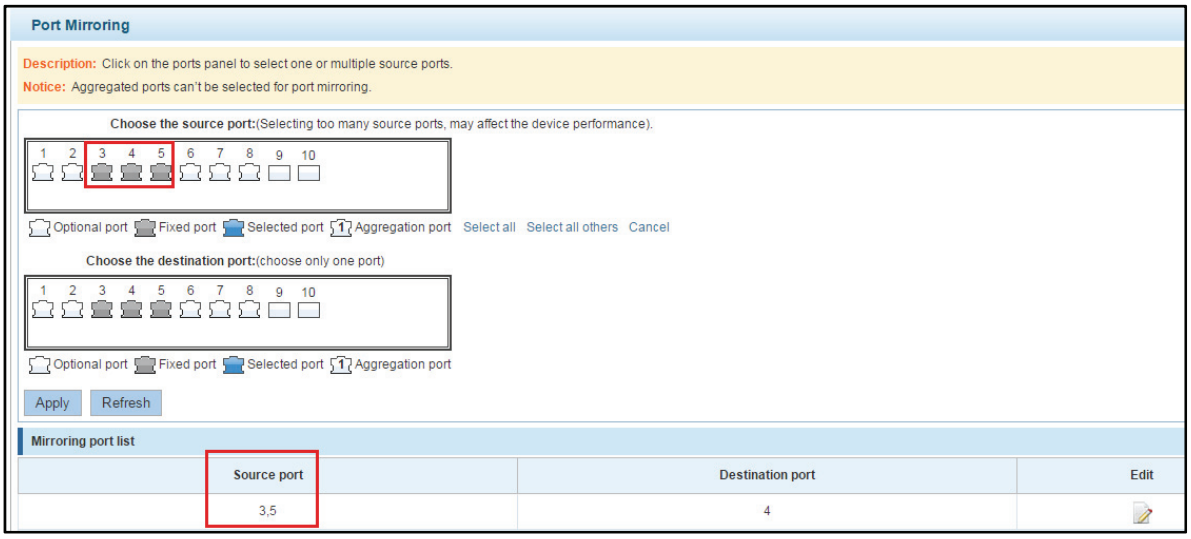


Figure 5-20: Modify successful port mirroring group

5.4.4 DELETE A PORT MIRRORING GROUP

Remove the current port mirroring, click the " " button in the action bar, click on the source port and destination port, respectively cancel the currently selected port, and click Apply. (Note: The current version supports only one port mirroring group)

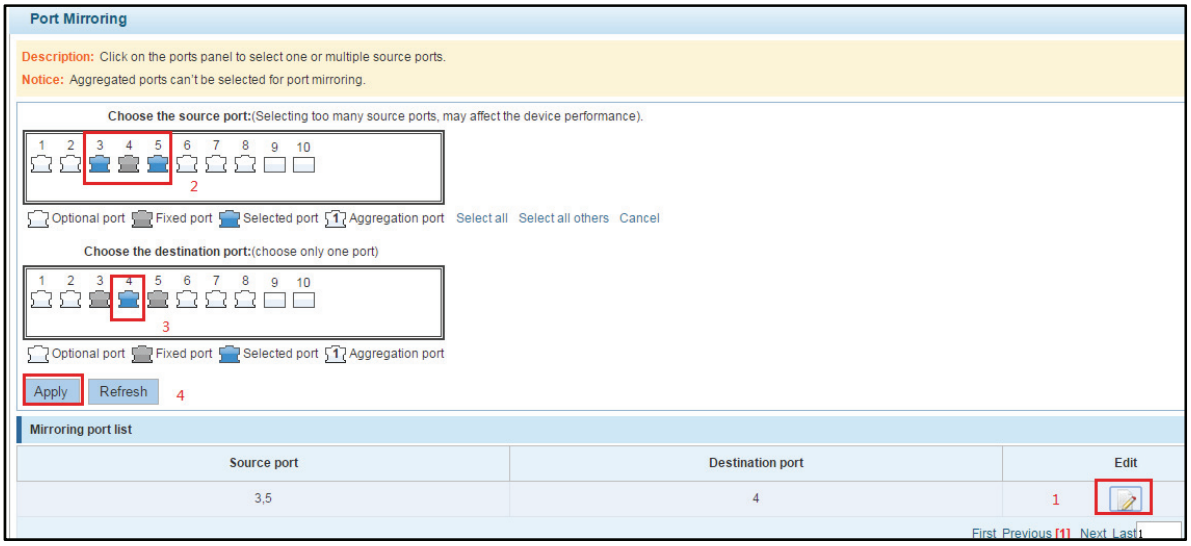


Figure 5-21: Delete port mirroring group

Remove port mirroring configuration steps are as follows:

Configuration Type	Step	Operation Description
Remove Mirroring Configuration	**Step1**	In the image you want to modify the operation of the group column, click " " ;
	Step2	In the panel, click Cancel the source port, destination port and then click Cancel;
	Step3	Click "Apply"

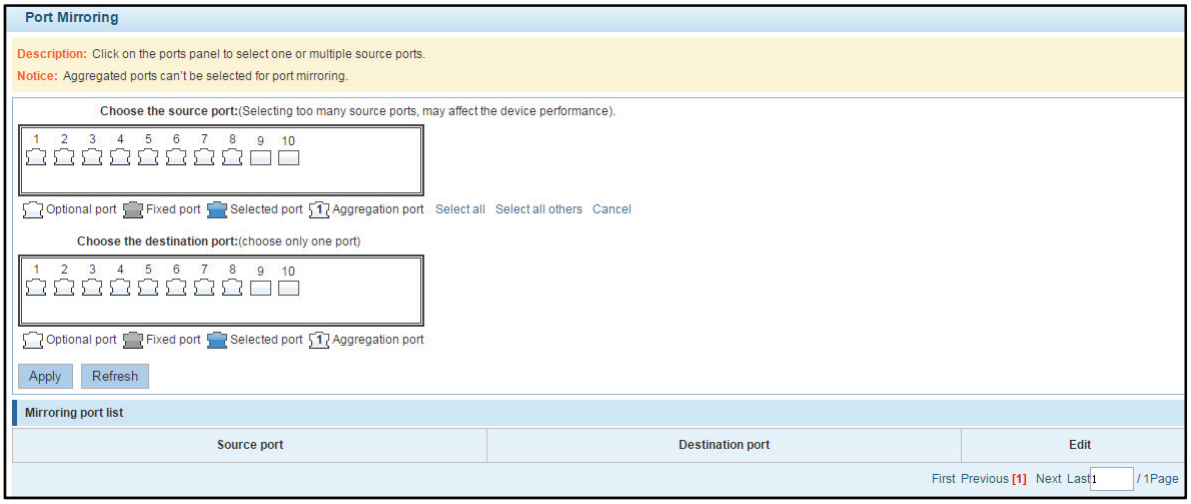


Figure 5-22: Deleted successfully port mirroring

5.5 PORT SPEED

5.5.1 VIEW PORT RATE LIMITING

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

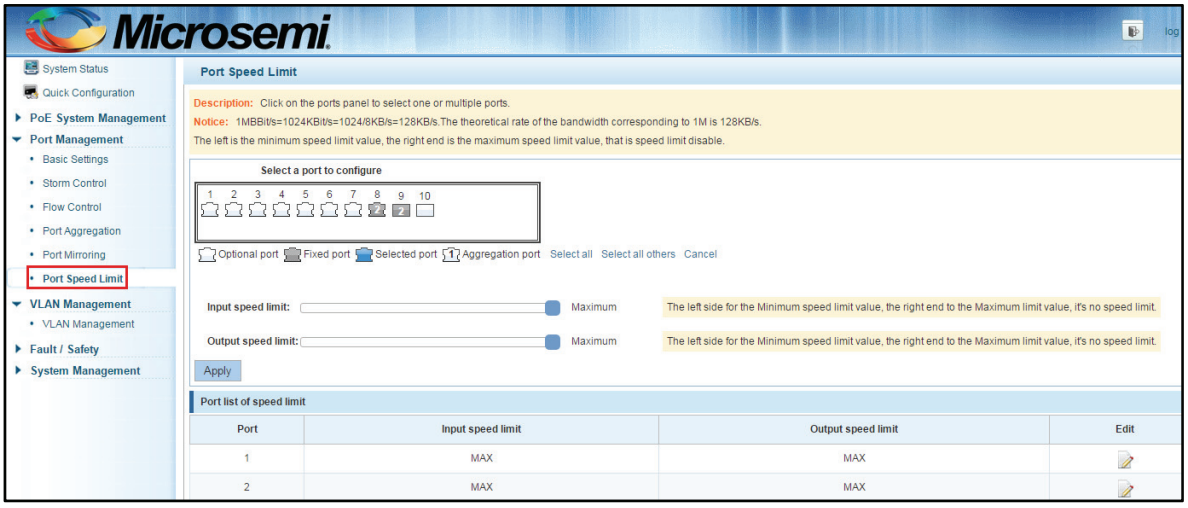


Figure 5-23: View Rate Configuration information

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

Port: The number of the port;

Input limit: uplink port speed;

Output speed: port downstream rate;

Reminder

To select multiple ports on the front panel, which can set the speed limit.

5.5.2 CONFIGURE PORT ACCESS RATE

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

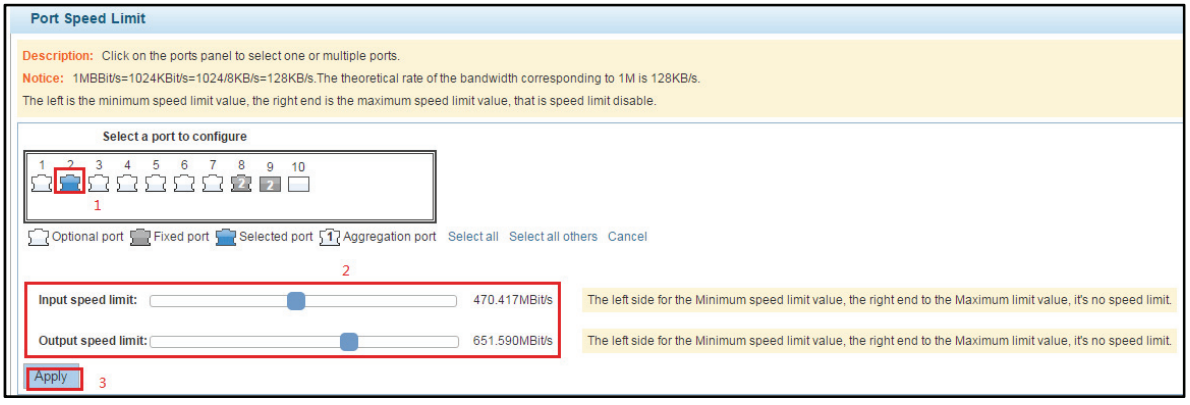


Figure 5-24: Configure port rate limiting entrance

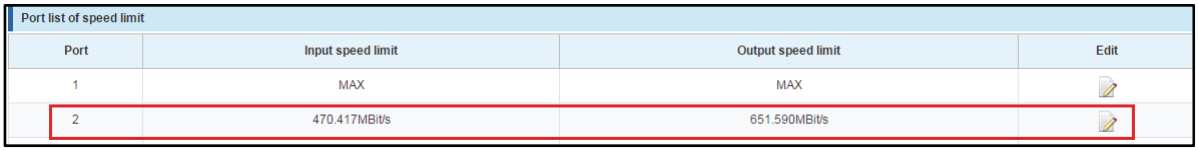


Figure 5-25: Port entrance speed limit results

Entrance port rate limiting configuration steps are as follows:

Configuration Type	Step	Operation Description
Uplink port rate limiting configuration	**Step1**	Click on the right side of the port "2" Icon or select multiple icons;
	Step2	Set rate limiting strip port value;
	Step3	Click the lower right corner "Apply" button to complete the configuration.

5.5.3 REMOVE THE PORT SPEED LIMIT

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

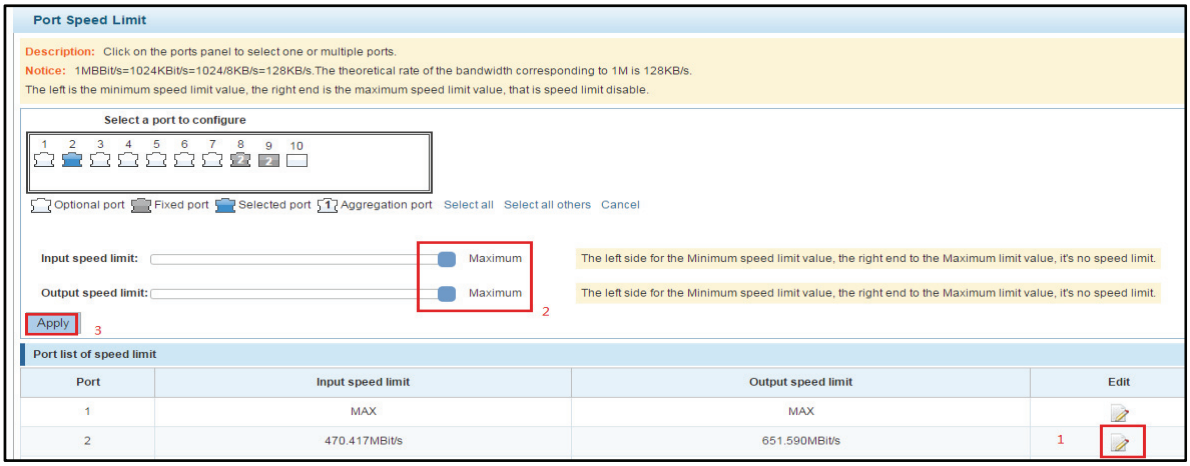


Figure 5-26: Remove the port speed limit

Remove uplink port rate limiting steps are as follows:

Configuration Type	Step	Operation Description
Remove port rate limiting	**Step1**	Click on the right side of the port icon ；
	Step2	In the area of the port rate configuration value rate strip pulled to the far right;
	Step3	Click the "Apply" button to complete the configuration.

6 VLAN MANAGEMENT

6.1 VLAN MANAGEMENT

6.1.1 CHECK VLAN CONFIGURATION INFORMATION

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

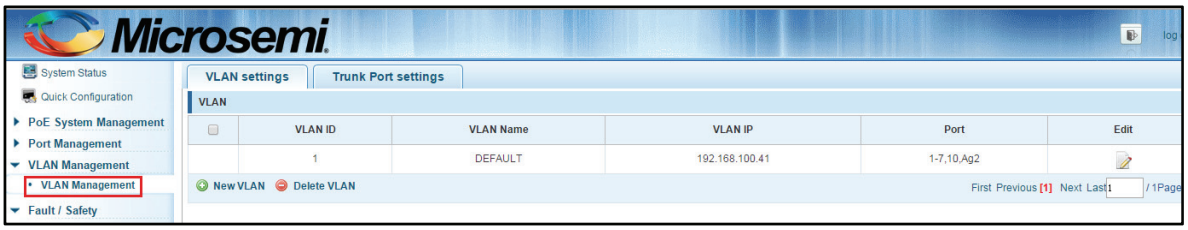


Figure 6-1: VLAN configuration information

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

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

6.1.2 ADDING A VLAN

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

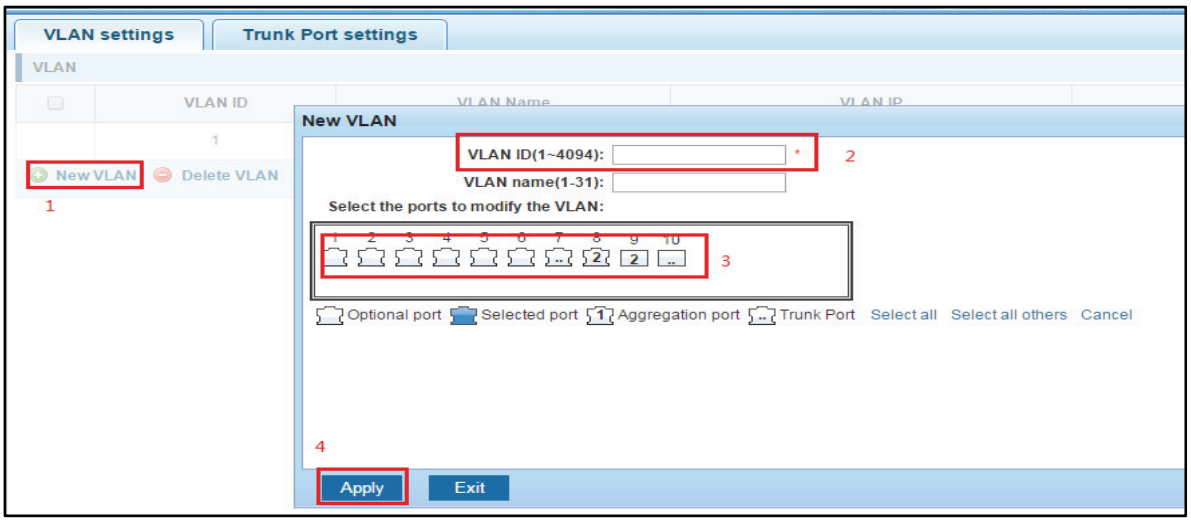


Figure 6-2: Adding a VLAN

Adding a VLAN, follow these steps:

Step	Operation Description
Step1	Click "NEW vlan" connection;
Step2	Value added VLAN VLAN ID of the page to fill in;
Step3	Click the lower right corner "Apply" button to complete the configuration.

VLAN ID is set in the range of 2-4094;

New VLAN operations simultaneously, you can enter VLAN name in the "VLAN name" text box (support Chinese);

NVLAN operations simultaneously, you can select ports in the port panel, added to a new VLAN.

6.1.3 REMOVE VLAN

1. Single vlan delete

To delete the selected VLAN, click the "X" button to delete the selected VLAN:

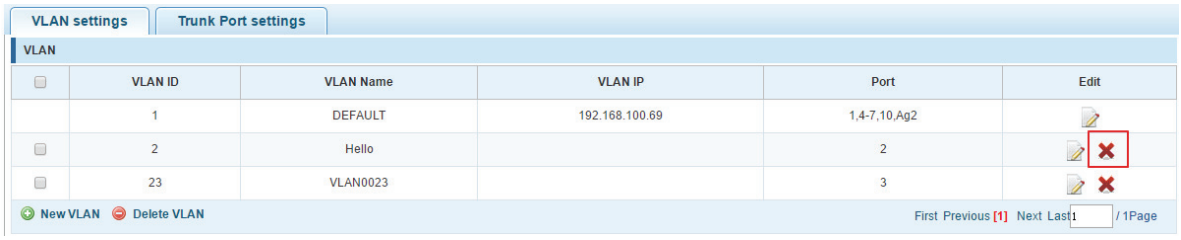


Figure 6-3: Delete a single VLAN

2. Delete multiple vlan

First select the VLAN you want to be deleted before the "" checkbox, then click "Delete VLAN" button to delete the selected VLAN:

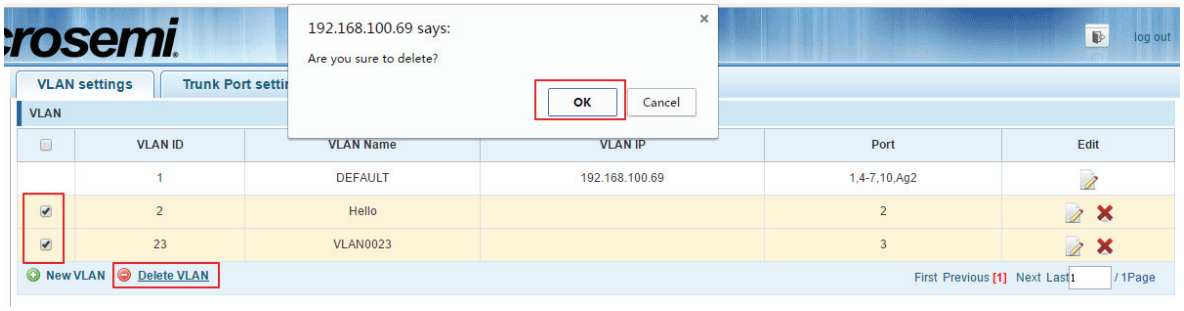


Figure 6-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps

Step	Operation Description
Step1	I want to delete VLAN check box;
Step2	Click on the bottom left "Delete VLAN" connection;
Step3	Confirm delete.

VLAN 1 is the management VLAN, it can not be deleted.

6.1.4 EDITING VLAN

1. Port to a VLAN

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

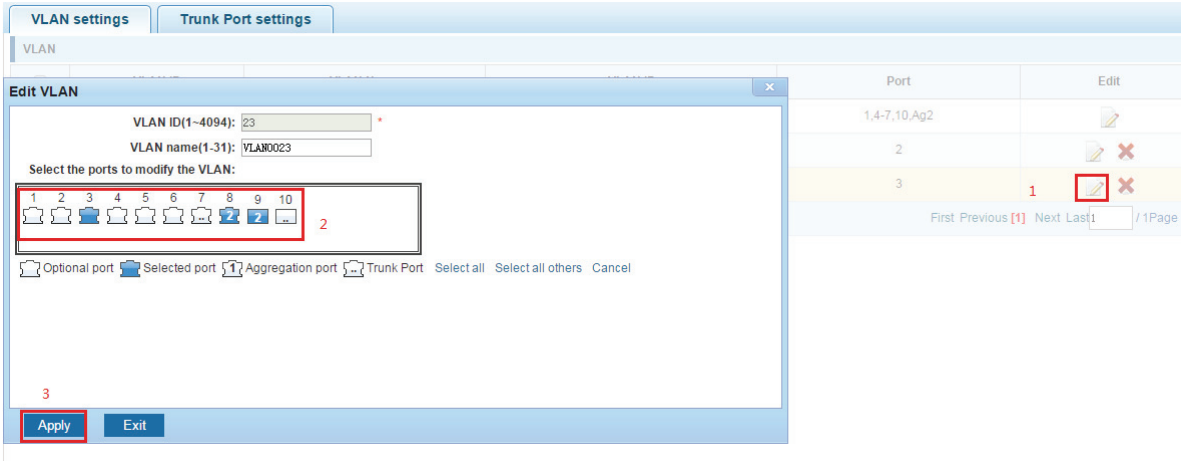


Figure 6-5: Add the port to the VLAN

Add the port to the VLAN, follow these steps:

Step	Operation Description
Step1	Click“ ”icon 。
Step2	Selected to join the ports in the port panel.
Step3	Click the lower right corner "Apply" button to complete the configuration.

2. To remove the port from a VLAN

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

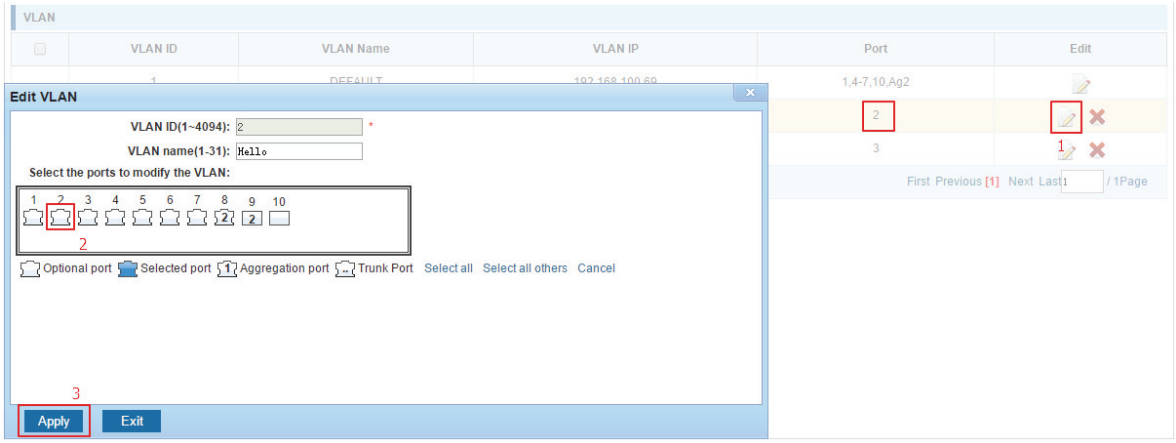


Figure 6-6: To remove the port from the VLAN.

Procedure to remove the port from VLAN as follows

Step	Operation Description
Step1	Click on the icon “ ” ；
Step2	Remove the port to be removed from the port panel ；
Step3	Click on the lower right corner of the "Apply" button to complete the configuration

Delete - TRUNK mode port from the original VLAN, the default is VLAN 1.

6.1.5 VIEW TRUNK PORT SETTINGS

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

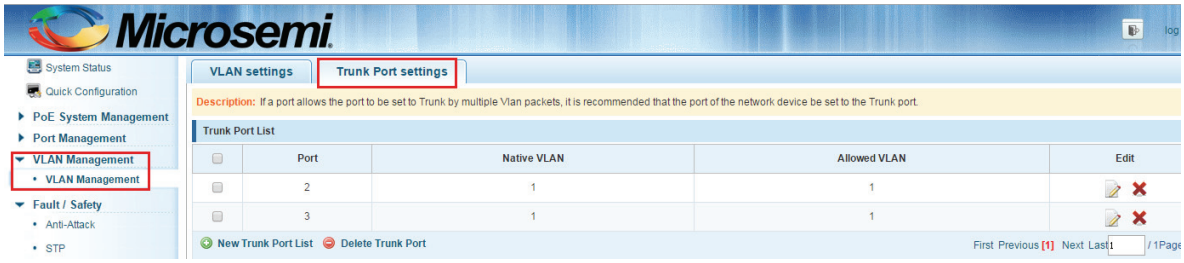


Figure 6-7: View trunk configuration information

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

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

6.1.6 INCREASED TRUNK

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

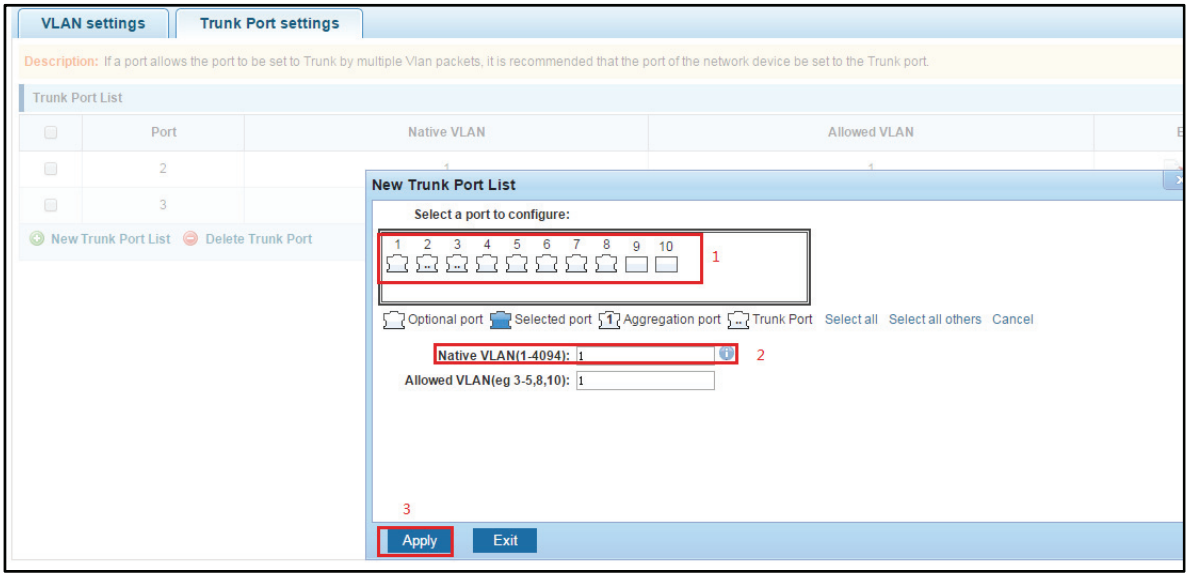


Figure 6-8: Trunk

The steps to increase trunk are as follows：

Step	Operating Description
Step1	Click on the "new trunk port list" button; ；
Step2	Select the port to be set on the port panel ；
Step3	Set local VLAN ；
Step4	Set by allowing the VLAN number ；
Step5	Click on the lower right corner of the "application" button to complete the configuration 。

Allows the VLAN to create in VLAN before setting.

6.1.7 DELETE TRUNK PORT

1. Delete a single trunk port

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

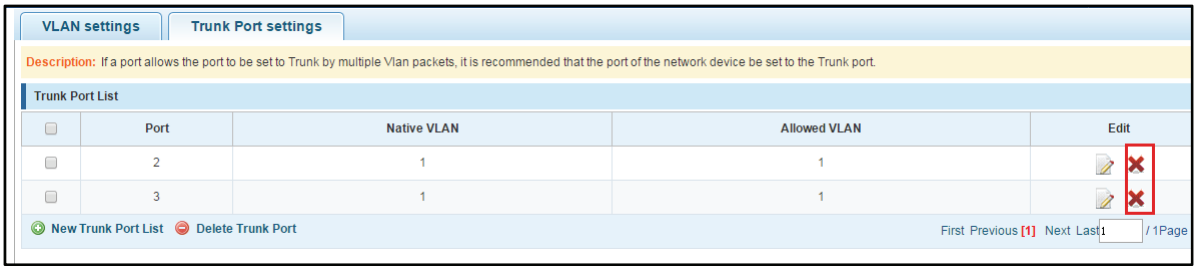


Figure 6-9: Delete a single trunk port

2. Multiple trunk ports simultaneously deleted

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

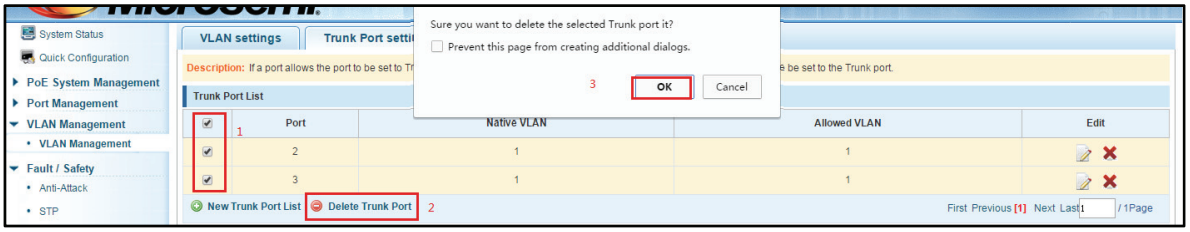


Figure 6-10: Delete multiple trunk ports

The procedure for removing multiple trunk ports is as follows

Step	Operation Description
Step1	Delect the check box to delete the trunk port;；
Step2	Click on the lower left corner of the "Trunk Port Delete" button；
Step3	Confirm complete delete。

7 FAILURE / SAFETY

7.1 ANTI ATTACK

7.1.1 ANTI ARP FRAUD

7.1.1.1 View ARP configuration

Click the "Fault/Safety""Anti-Attack""ARP Deception" to check the current switches has been configured for ARP information:

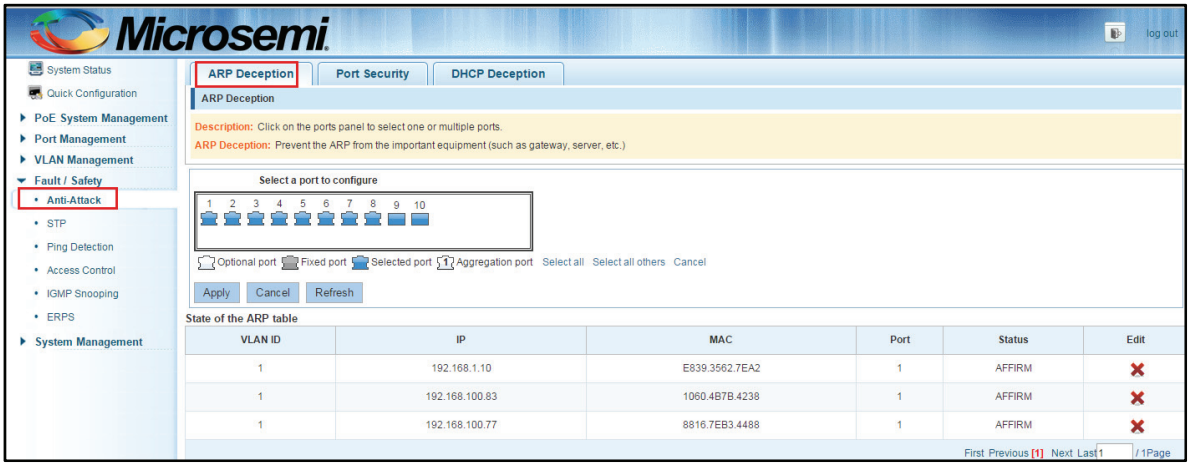


Figure 7-1: View port ARP configuration information

Displayed in the ARP state table is the property value of the current switch ARP configuration:

VLAN ID: display the number of VLAN values;

The IP address: IP address current configuration display switch;

The MAC address: display switch current MAC;

Click "Refresh" button, display refresh configuration information.

7.1.1.2 Activates ARP anti cheat function

In the ARP anti cheat configuration table, click the "Apply" button to complete the configuration of one or more ports that need to be activated to prevent ARP deception in the port panel.

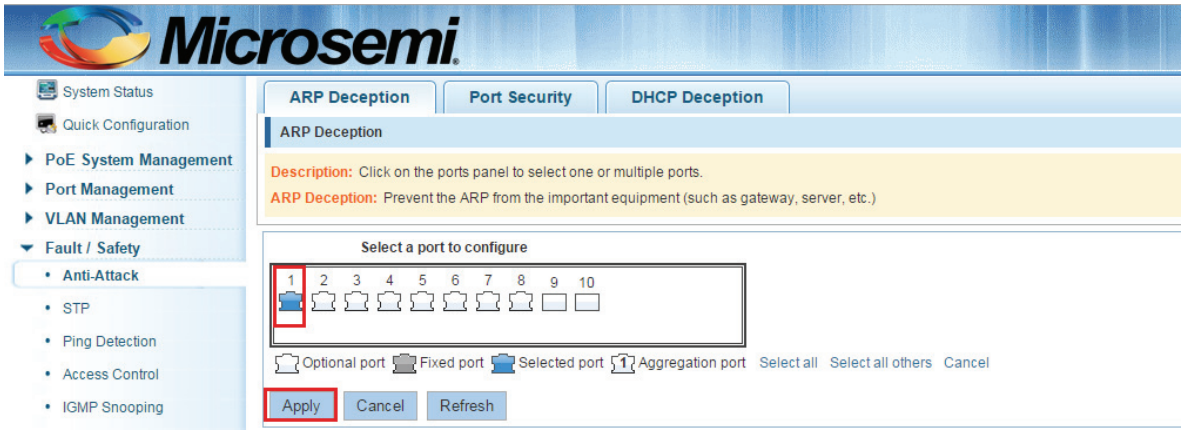


Figure 7-2: Anti fraud configuration

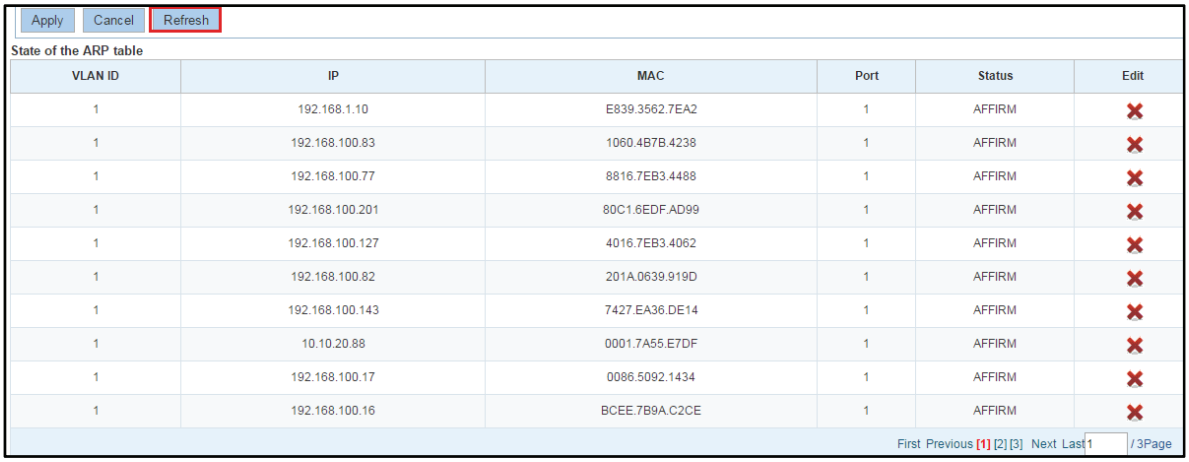


Figure 7-3: Refresh ARP status table

The configuration steps for the ARP anti cheat function of the active port are as follows:

Configuration type	Step	Operation Description
Enable ARP anti cheat	**Step1**	Activate ARP anti cheat Step1 click on the port panel to activate the port to activate the anti ARP cheat; ；
	Step2	Click on the lower left corner of the "Apply" button to complete the configuration ；
	Step3	Click the "Refresh" button in the lower left corner to see the ARP status table.

Each port up to learn 200 different ARP message, more than 200 after this port Enter the jam will, can not normally forward data.

7.1.1.3 Disable ARP anti cheat function

In the ARP anti deception configuration table, click on the port panel need to disable the anti ARP deception of one or more ports, so that it is not selected, and then click the "Apply" button to complete the configuration.

.

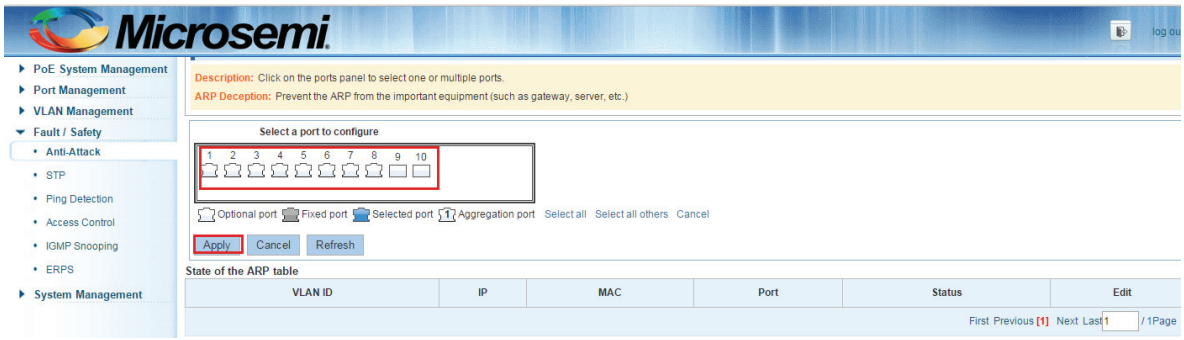


Figure 7-4: Disable ARP anti cheat function

The configuration steps to disable ARP anti fraud:

Configuration type	**Step**	Operation Description
Disable ARP anti cheat	**Step1**	Click on the port panel you need to disable one or more ports of anti ARP deception, so that it is in a state of.
	Step2	Click on the lower right corner of the "Apply" button to complete the configuration.

After an interface receives 200 ARP requests that the interface even PC virus, a chance to put this off exchange interface. So the switch of the cascade interface can not open the ARP anti cheat function.

Open anti ARP anti spoofing, proposed to open storm control.

7.1.1.4 Delete miscarriage of justice ARP

State of the ARP table

VLAN ID	IP	MAC	Port	Status	Edit
1	192.168.20.83	1060.4B7B.4238	1	AFFIRM	✖
1	192.168.50.83	1060.4B7B.4238	1	AFFIRM	✖
1	192.168.100.50	D43D.7E63.2760	1	AFFIRM	✖
1	192.168.100.160	7427.EA36.DD67	1	AFFIRM	✖
1	192.168.1.56	C860.00E0.2B7D	1	AFFIRM	✖
1	172.16.32.1	1060.4B7B.4238	1	AFFIRM	✖
1	192.168.100.39	4016.7EB1.EB6D	1	ATTACK	✖

Figure 7-5: Delete miscarriage of justice ARP

ARP anti deception is likely to be false in some ARP packets to attack the message and reject the ARP, or the attack message is mistaken for legitimate messages. If there is a miscarriage of justice, you can click the delete button in the action column to delete the wrong item. ：

Configuration type	Step	Operation Description
Delete the configuration steps for ARP:	**Step1**	Remove the false ARP configuration Step1 click on the action bar delete button, select the confirmation delete.

When an interface receives 200 ARP request, will think this interface with PC virus, the opportunity will be closed this interface exchange. So the switch of the cascade interface can not open the ARP anti cheat function.

Open anti ARP anti spoofing, proposed to open storm control.

7.1.2 PORT SECURITY

7.1.2.1 Configuration port security

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

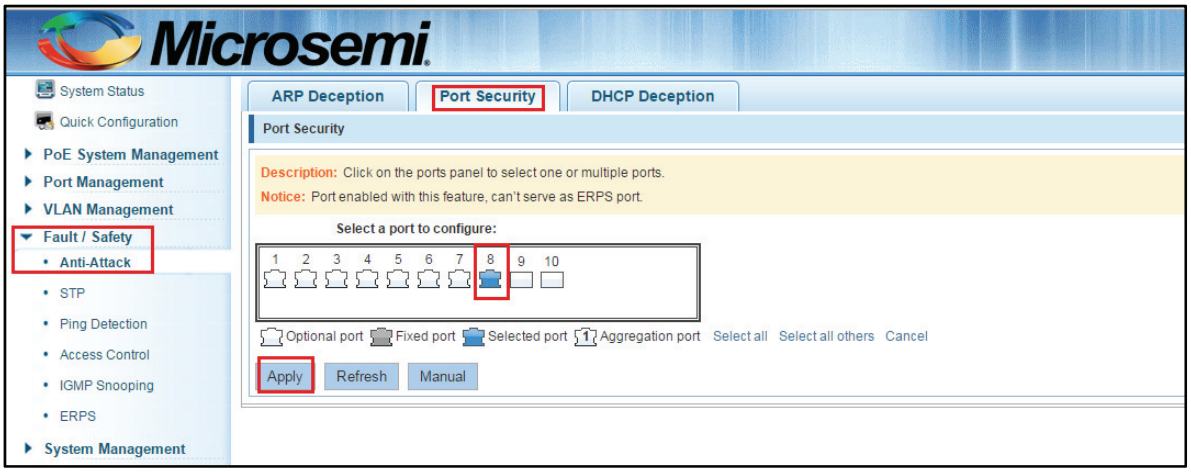


Figure 7-6: Port security configuration

- This function is based on the configuration of port;
- Need to choose the port security port;
- Save the configuration (i.e. open port security).
- Click "Refresh" button to refresh the display, switch the binding information.
- Click "Manual" button, you can manually configure the port binding information.

7.1.2.2 Manual configuration

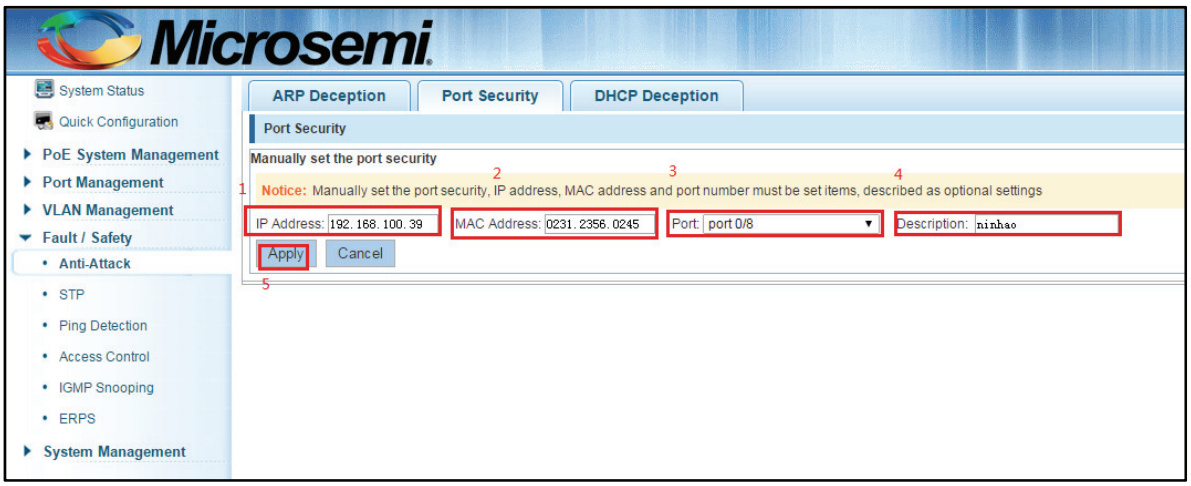


Figure 7-7: Port security manual configuration

Configuration instructions:

The manual mode need to configure the IP address, MAC address, port and description

Port security manual configuration steps are as follows:

Configuration type	**Step**	Operation Description
	Step1	Select IP address, MAC address, port number, description
	Step2	Click "Apply""

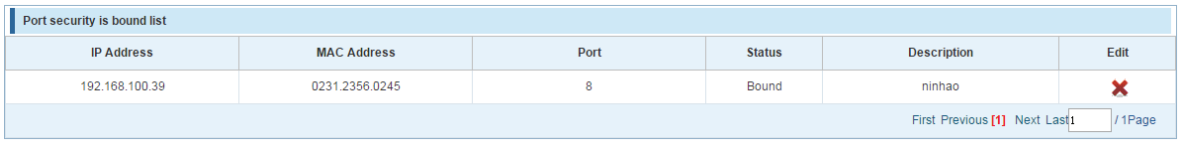


Figure 7-8: Port security bound configuration results

7.1.2.3 Cancel port security binding configuration

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

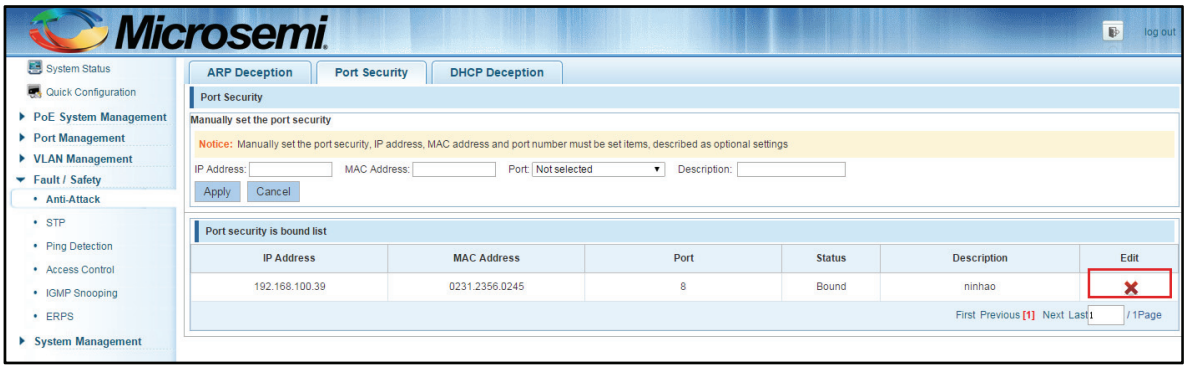


Figure 7-9: Cancel port security bound

7.1.3 ANTI DHCP ATTACK

7.1.3.1 view anti DHCP attack configuration

Click the "Fault/Safety""Anti-Attack""DHCP Deception", the configuration information show the anti DHCP attack:

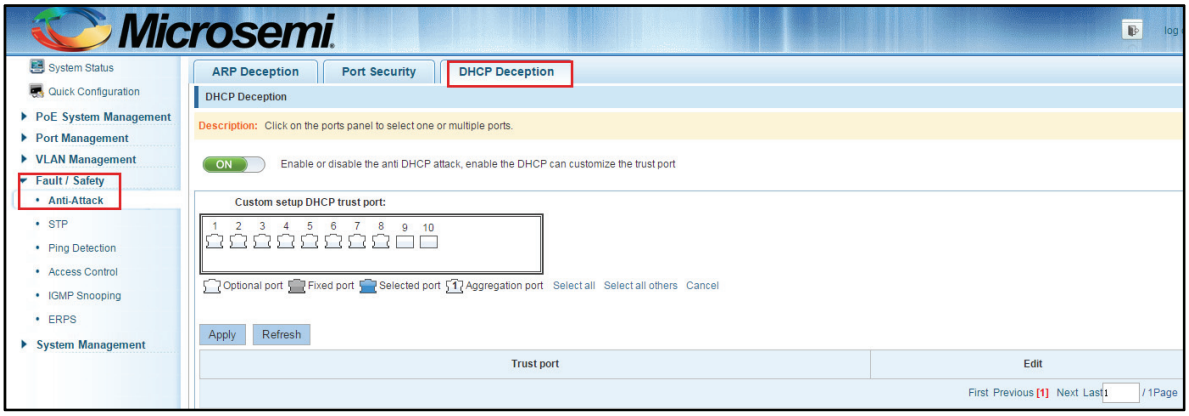


Figure 7-10: View anti DHCP attack configuration information

Click "Refresh" button, display refresh configuration information.

7.1.3.2 Open anti DHCP attack function

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

to open the anti DHCP attack:

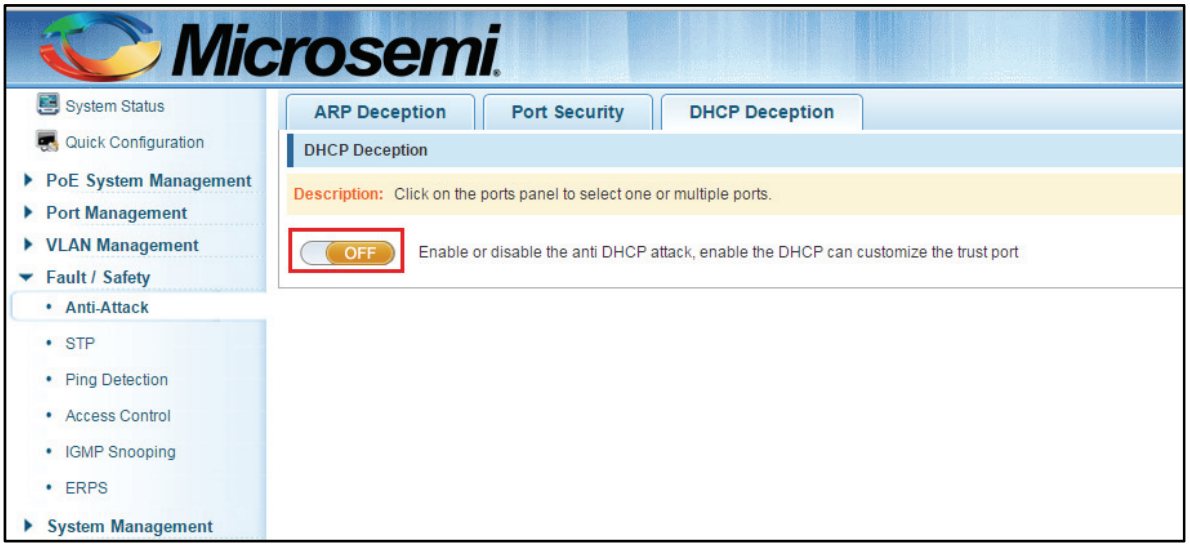


Figure 7-11: Activation of anti DHCP attack function

7.1.3.3 Open anti DHCP attack function

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

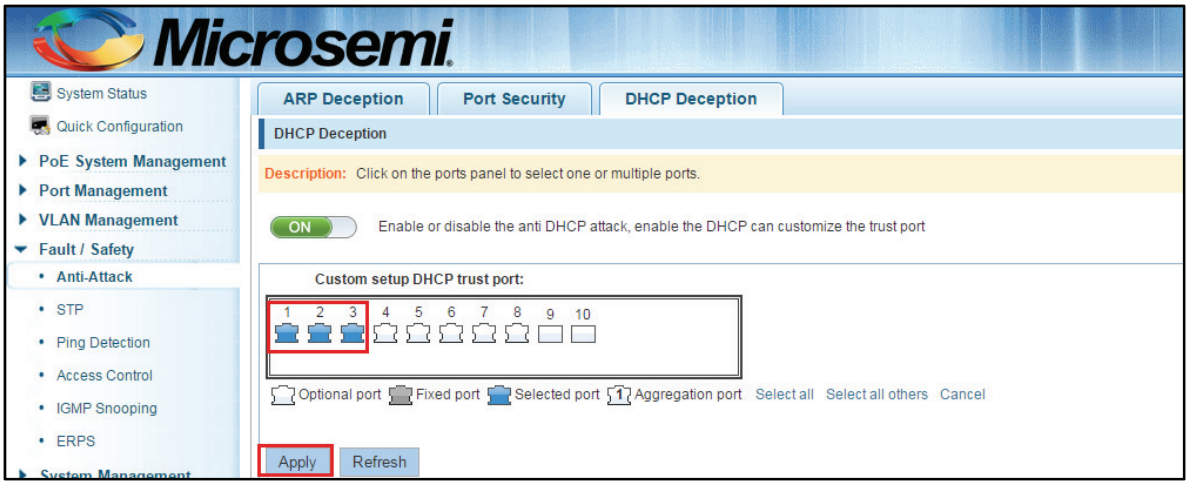


Figure 7-12: Activation of anti DHCP attack function

Figure 7-13: Activation of anti DHCP attack function

7.1.3.4 Sets the port to DHCP non trusted port

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

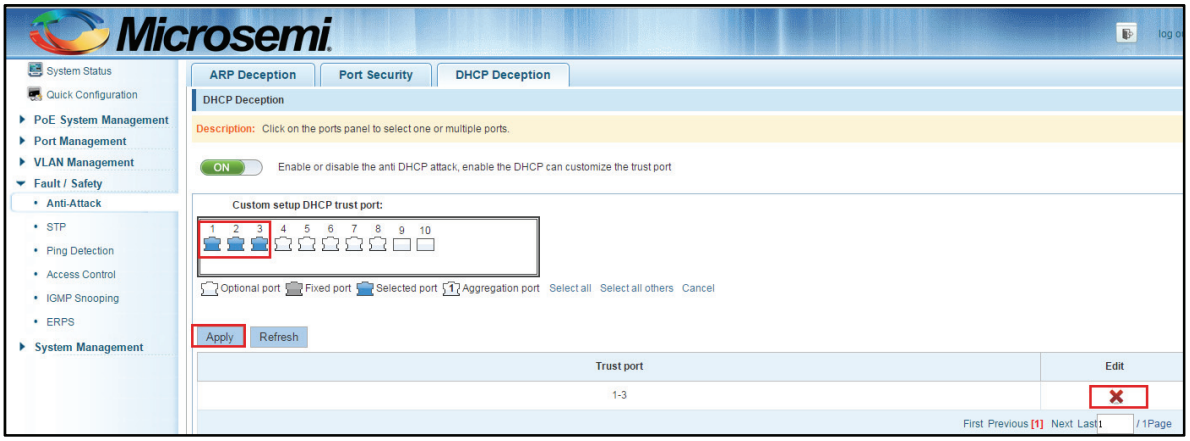


Figure 7-14: Disable anti illegal DHCP server functions

The activation of anti DHCP attack function, is the port setting for trust status;

Disable - preventing DHCP attack, is set to a non trusted state port.

7.1.3.5 Off anti DHCP attack function

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

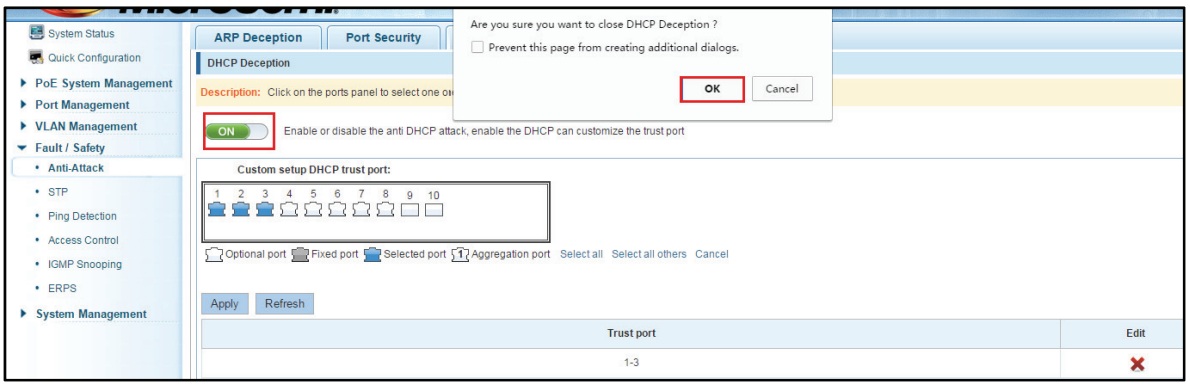


Figure 7-15: Off anti DHCP attack function

7.2 SPANNING TREE

7.2.1 VIEW SPANNING TREE CONFIGURATION

Click the "Fault/Safety""STP" can view the current spanning tree configuration:

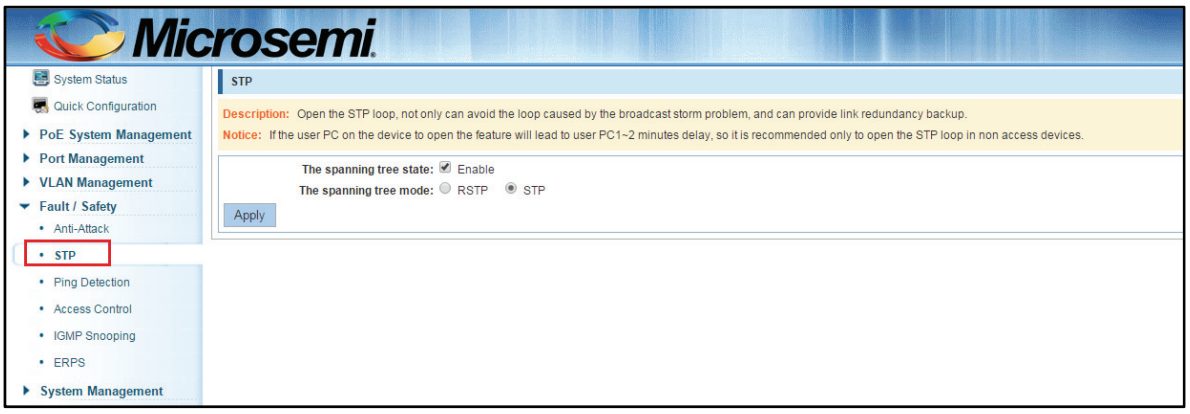


Figure 7-16: View spanning tree configuration information

Be careful: STP is enabled by default, the default mode for stp. Blocking the corresponding port by default for the loop.

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

7.2.2 TO CHANGE THE SPANNING TREE MODEL

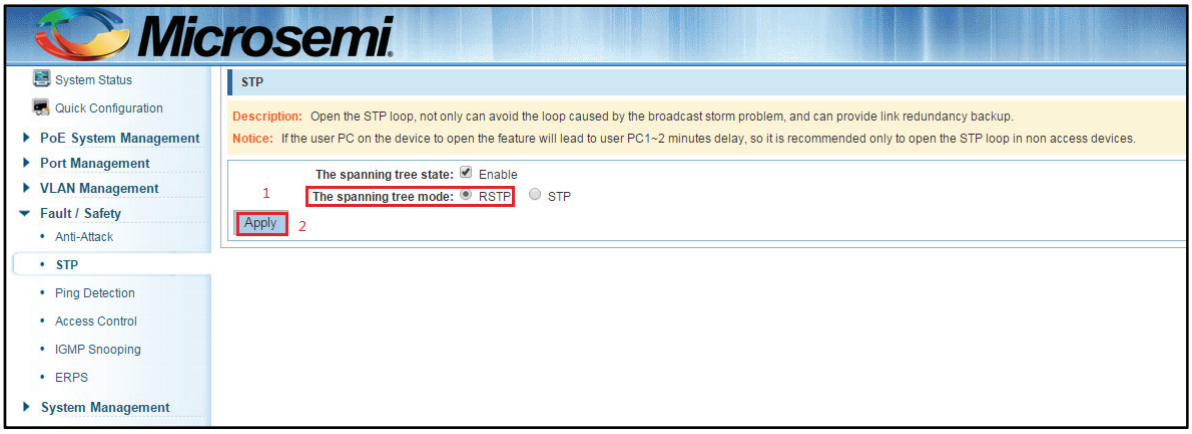


Figure 7-17: Changing the spanning tree pattern

Configuration type	Step	Operation Description
Spanning tree	**Step1**	Select STP mode;

configuration	**Step2**	Click on the button "Apply" to save the current configuration mode

7.2.3 CLOSE SPANNING TREE FUNCTION

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

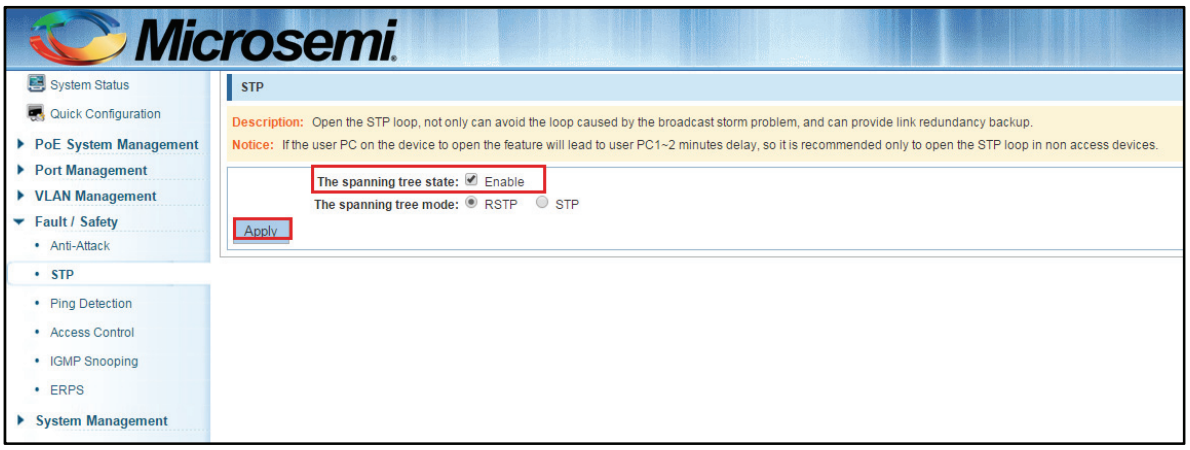


Figure 7-18: Close spanning tree

7.3 PING DETECTION

Click the "Fault/Safety""ping Detection"can view the Ping Detecion configuration:

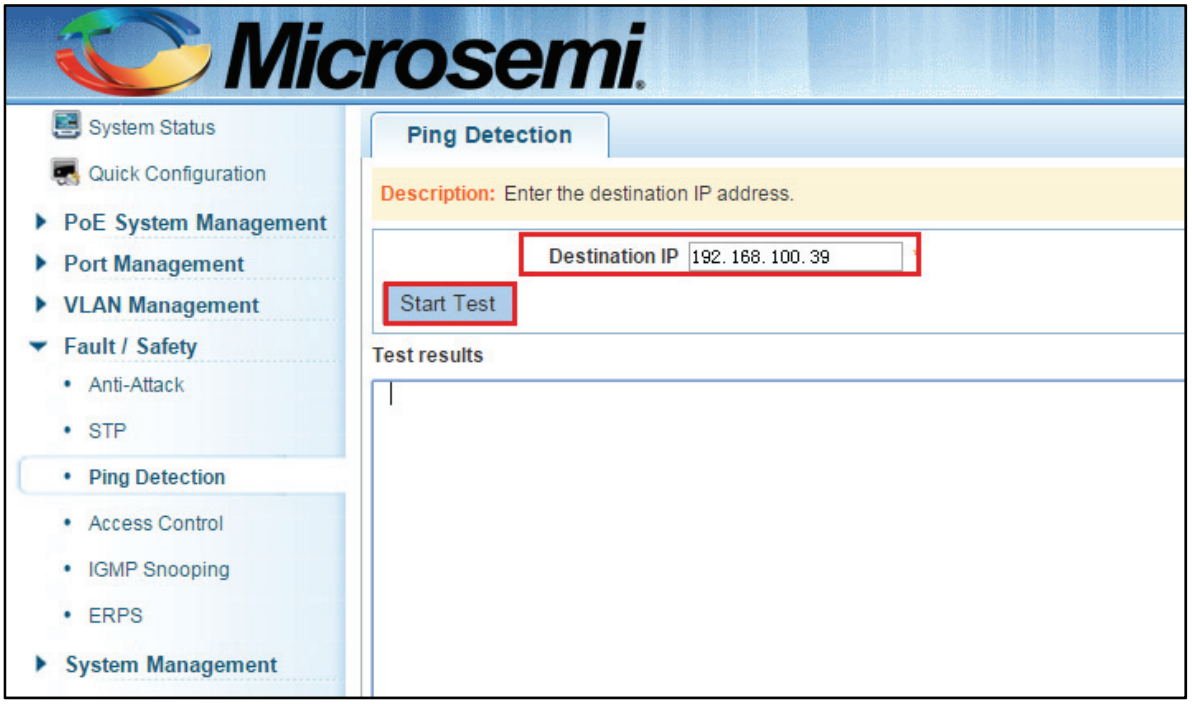


Figure 7-19: PING information

7.4 ACCESS CONTROL

7.4.1 ACL ACCESS CONTROL LIST

7.4.1.1 view access control list

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

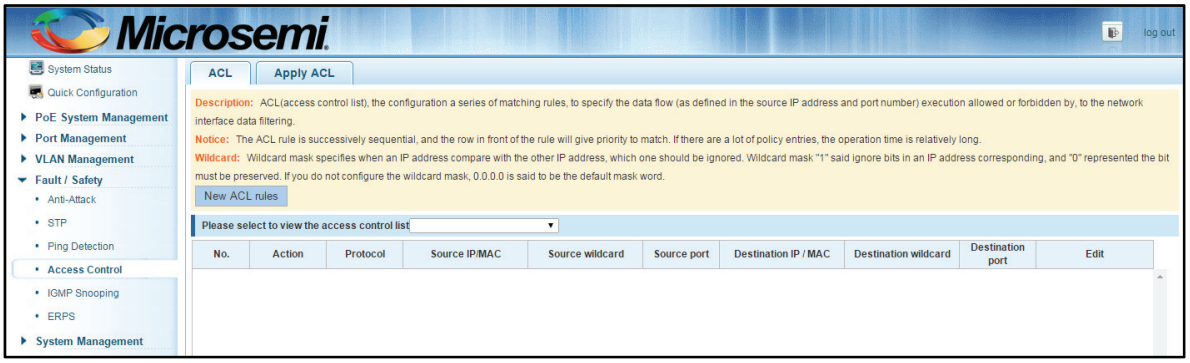


Figure 7-20: Access control list

7.4.1.2 Increased access rules

1. Increase the standard IP access rules

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

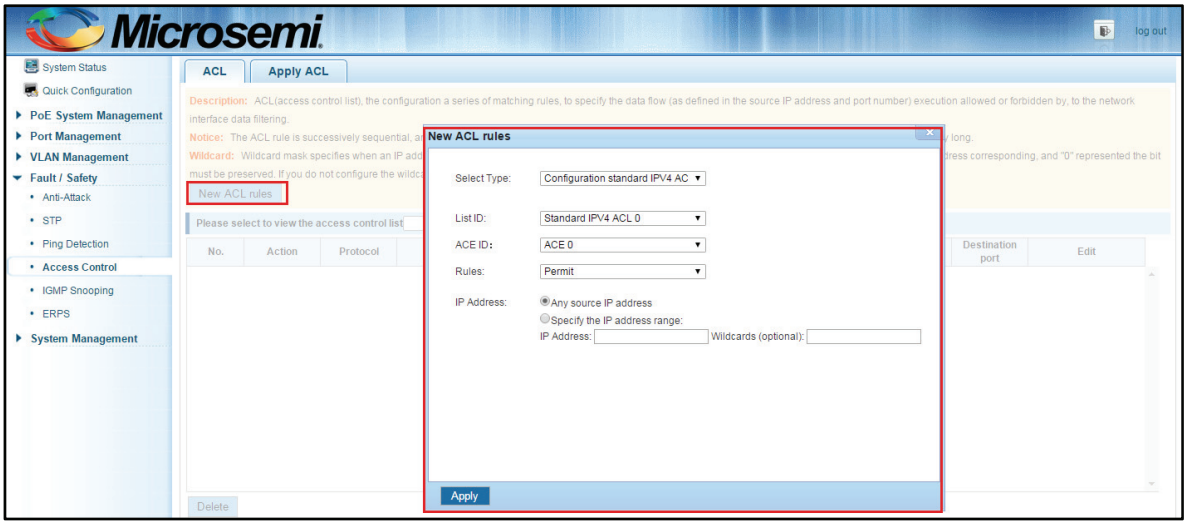


Figure 7-21: Configuration standard IP access control list

2. Increase the extended IP access rule

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

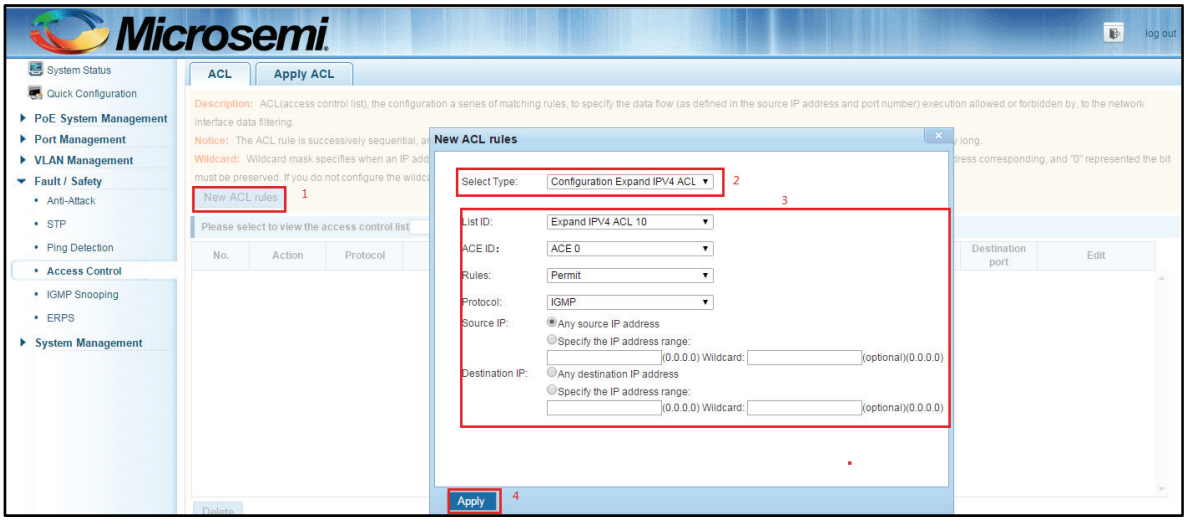


Figure 7-22: Configuration standard IP access control list

3. Increasing expand MAC access rules:

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

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

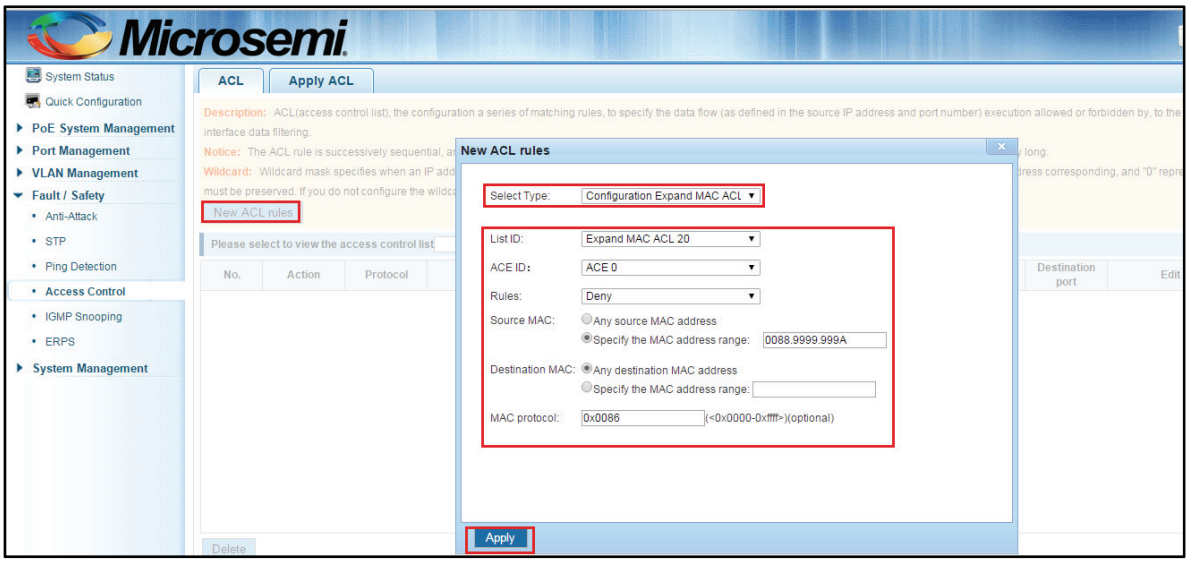


Figure 7-23: Configuration extended MAC access control list

Configuration instructions

ACE ID is an optional rule. Do not fill: the default is 0;

The extended IP protocol access control list, type: TCP, UDP, IP, IGMP.

7.4.1.3 Modify configuration

Rules for modifying port applications

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

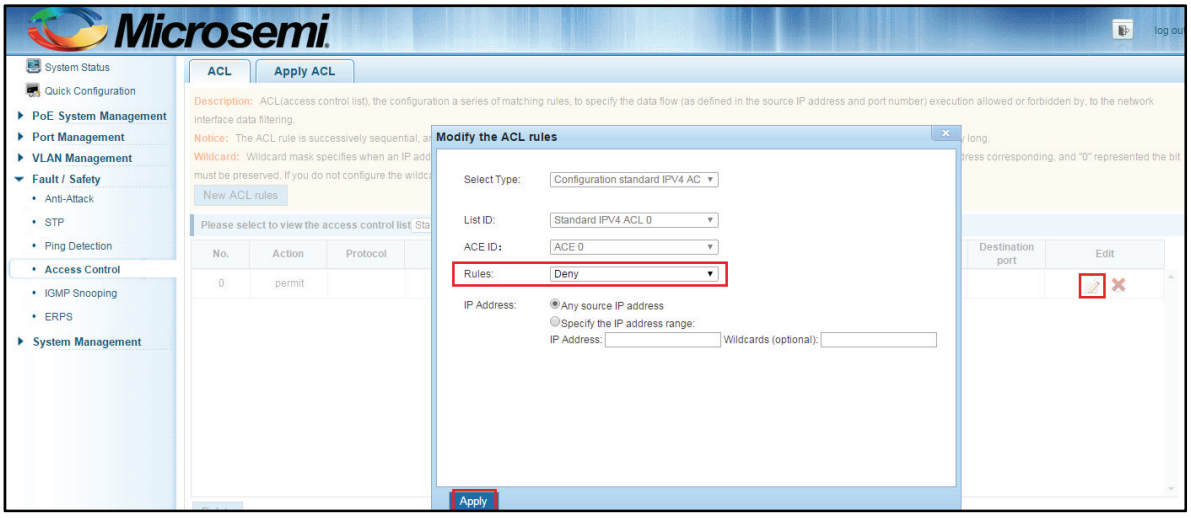


Figure 7-24: To modify the ACL rule

Configuration instructions

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

7.4.1.4 Delete rule

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

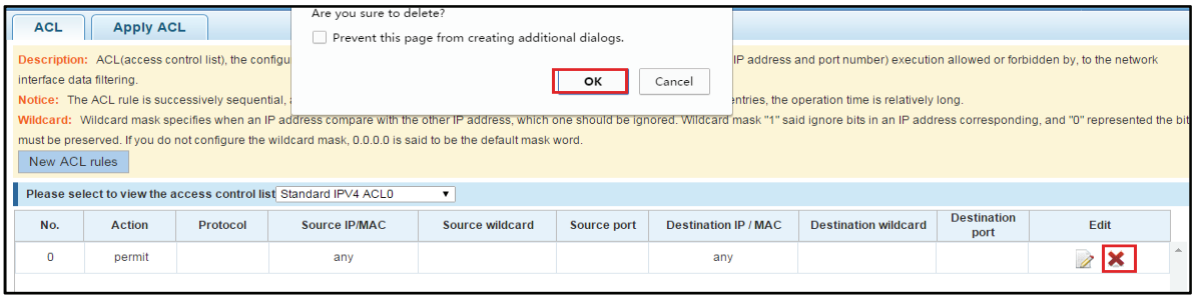


Figure 7-25: Delete rules

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

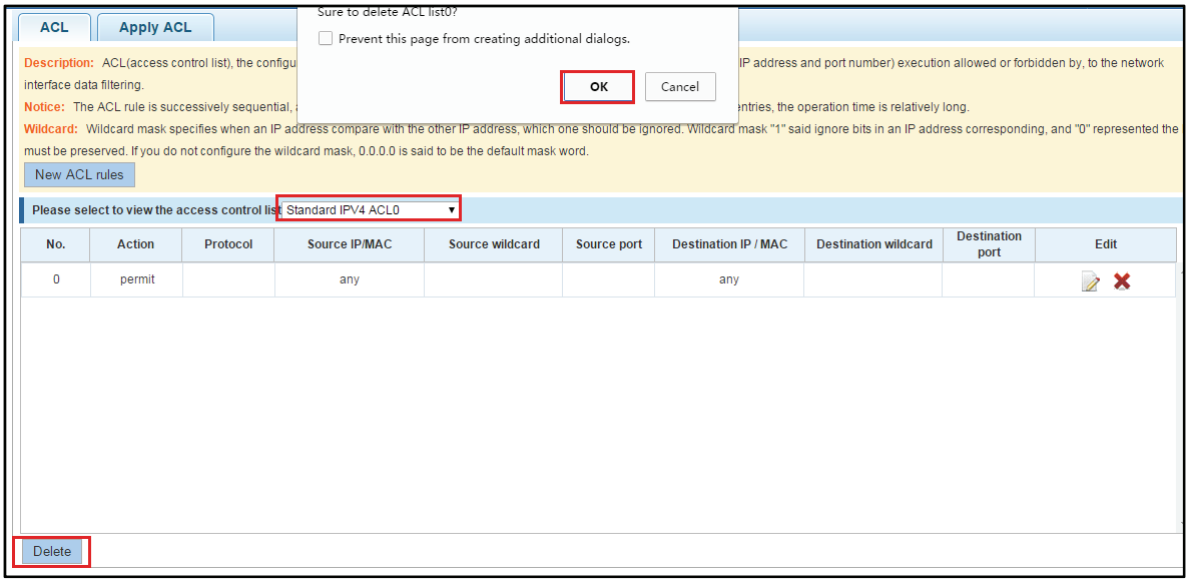


Figure 7-26: Delete ACL rules

Configuration instructions

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

7.4.2 APPLICATION ACL

7.4.2.1 View application ACL

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

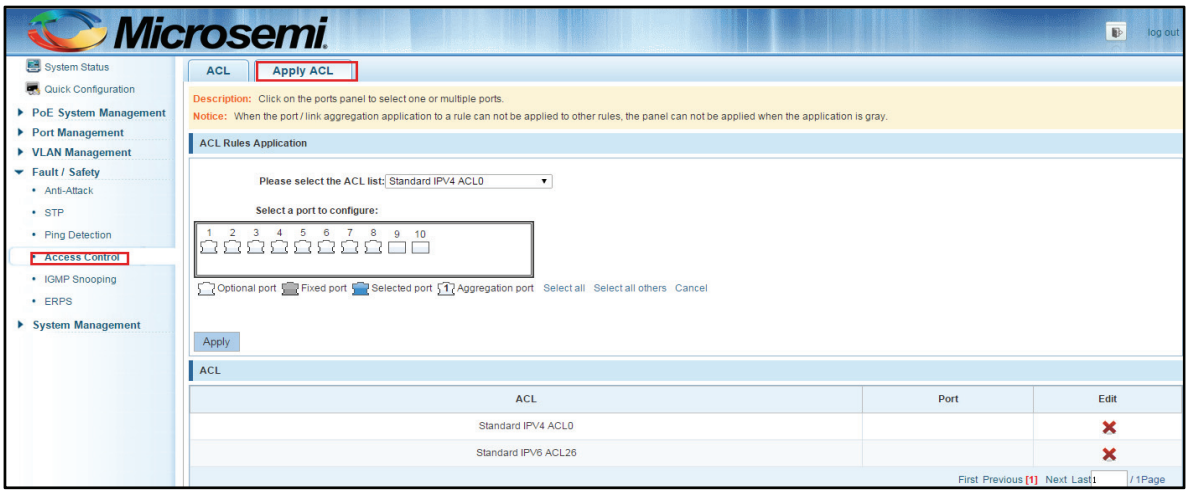


Figure 7-27: View application ACL rules

7.4.2.2 Increased application ACL

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

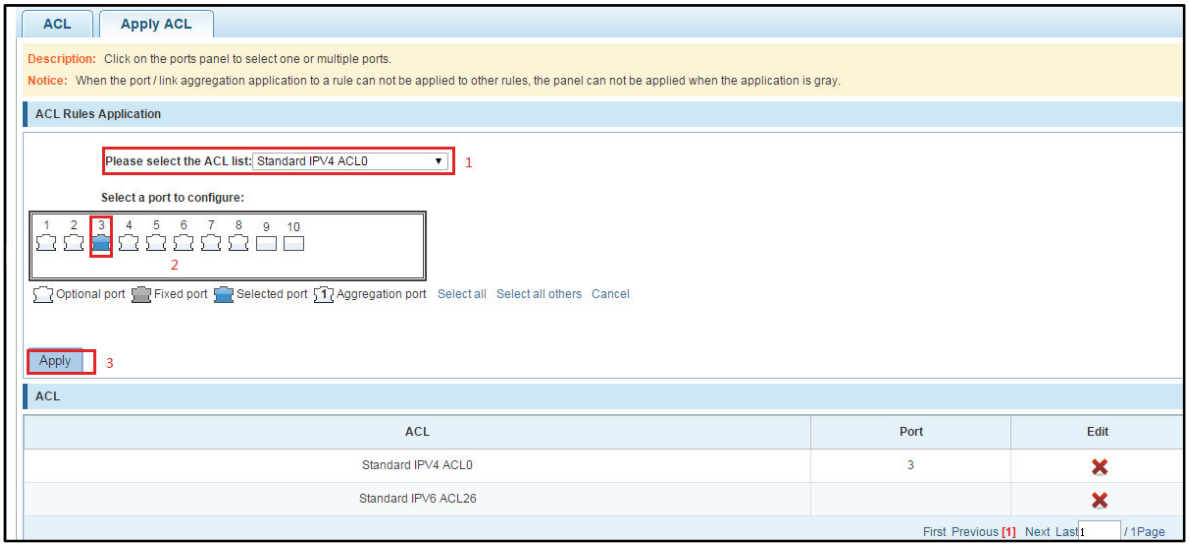


Figure 7-28: Add applications ACL

7.4.2.3 Delete application ACL

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

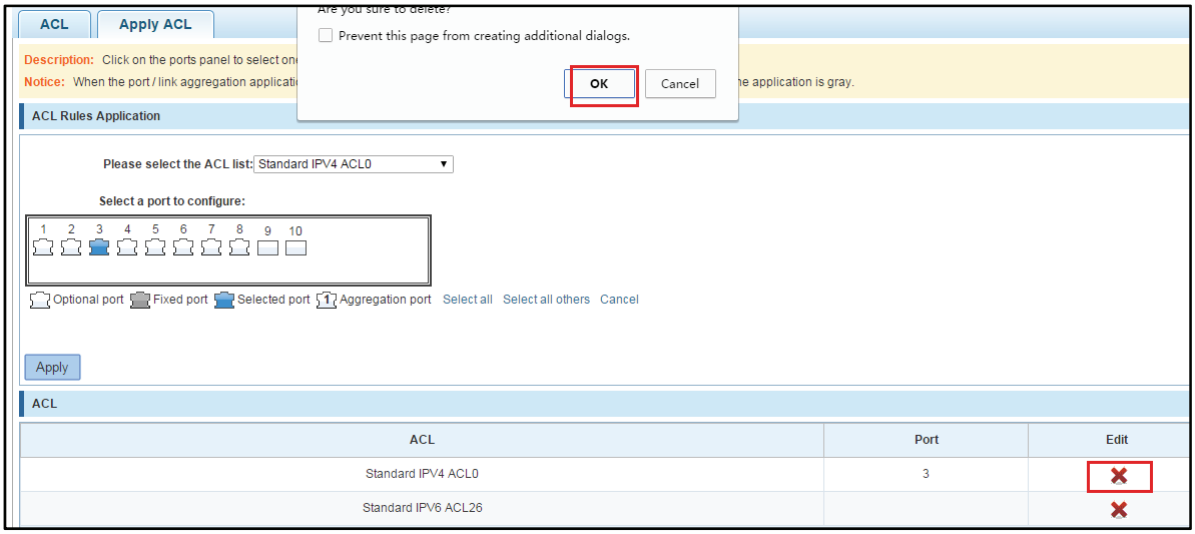


Figure 7-29: Delete application ACL

7.5 MULTICAST LISTENER

7.5.1 VIEW MULTICAST LISTENER (SNOOPING IGMP) CONFIGURATION

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

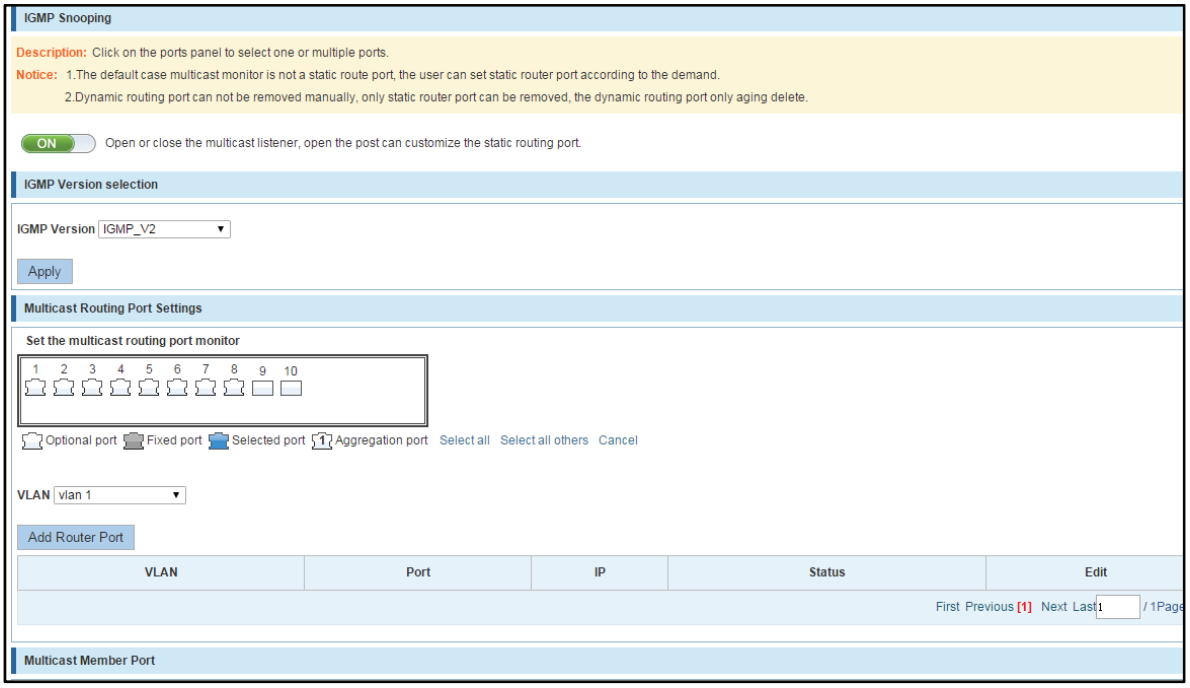


Figure 7-30: View Snooping IGMP configuration information

7.5.2 ACTIVE MULTICAST LISTENER FUNCTION

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

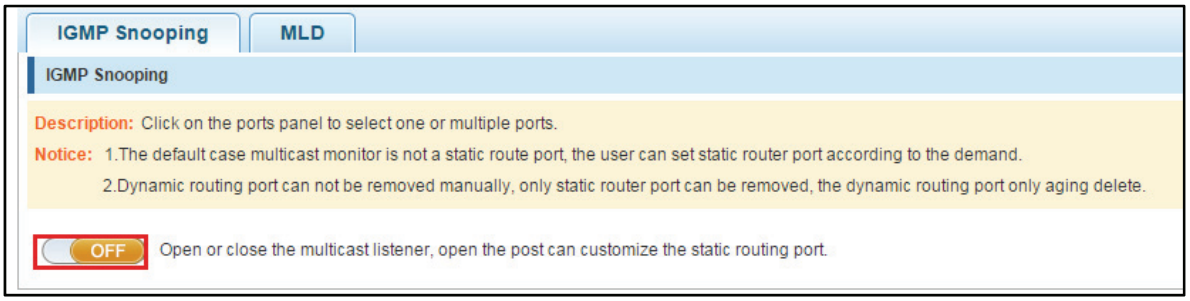


Figure 7-31: Open multicast listener configuration

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

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

The default version of V2 - IGMP.

7.5.3 DISABLE MULTICAST LISTENER FUNCTION

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

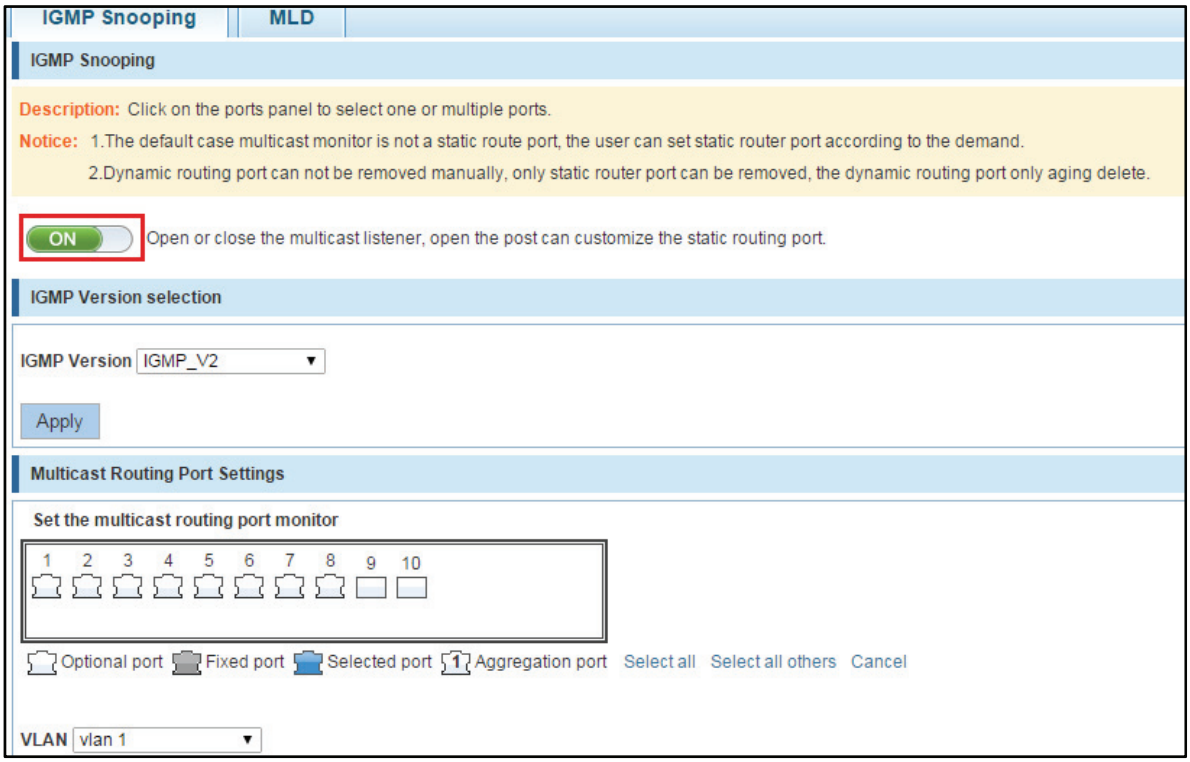


Figure 7-32: Closed multicast listener function operation

7.5.4 CONFIGURATION MULTICAST ROUTING

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

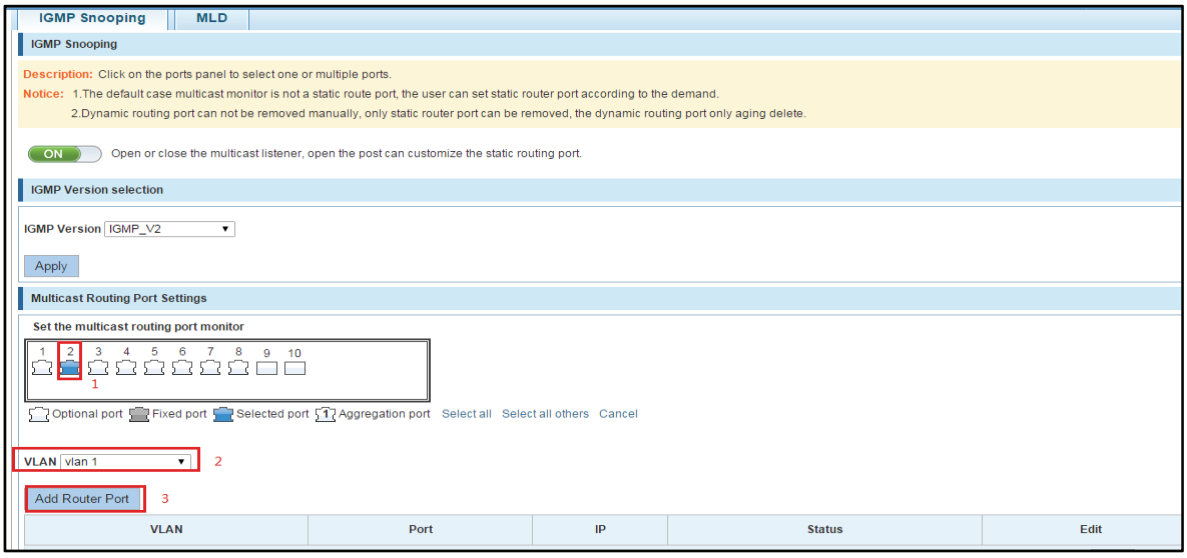


Figure 7-33: Configuration of multicast routing

Multicast routing configuration steps are as follows:

Configuration type	Step	Operation Description
Multicast routing configuration	**Step1**	In the port panel to select multicast listener routing port; ;
	Step2	Select vlan;
	Step3	Click on the "Add Router Port" button to complete the configuration.

7.5.5 IGMP VERSION

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

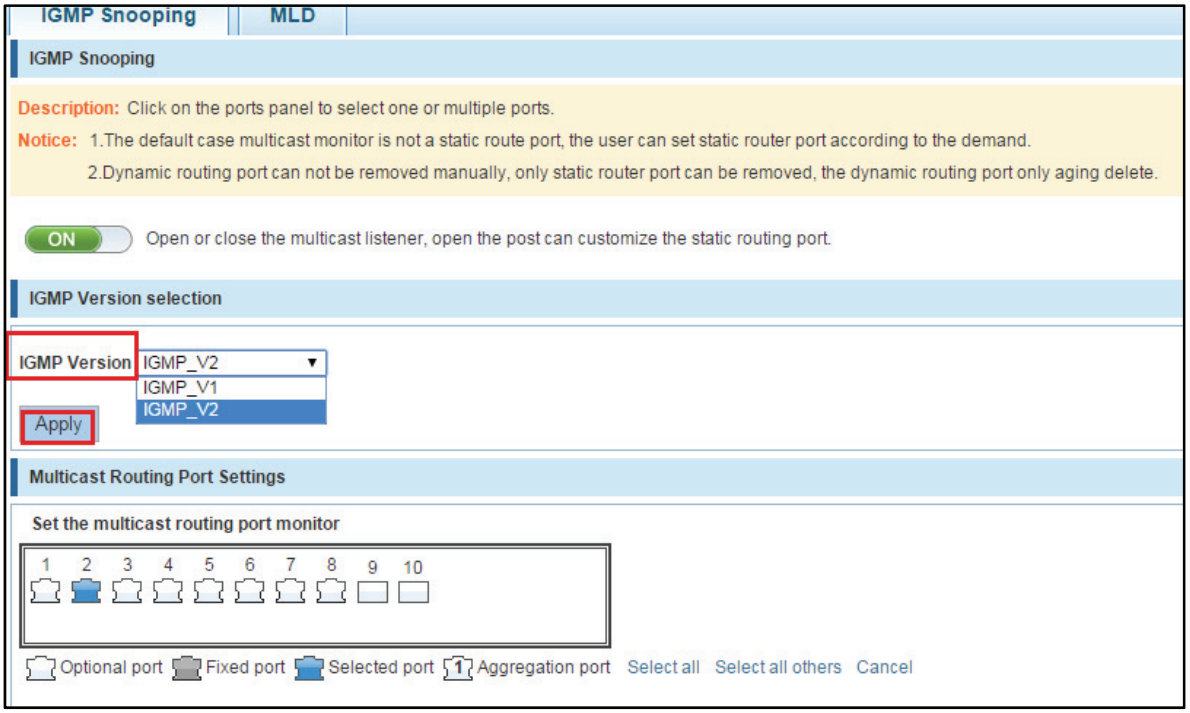


Figure 7-34: Configuration IGMP version

IGMP version configuration steps are as follows:

Configuration type	Step	Operation Description
Multicast routing configuration	**Step1**	Select the required version number;
	Step2	Click the "Apply" button to complete the configuration.

7.5.6 VIEW MLD CONFIGURATION

Click the "Fault/Safety""MLD" to view the current switches has been configured for MLD information:

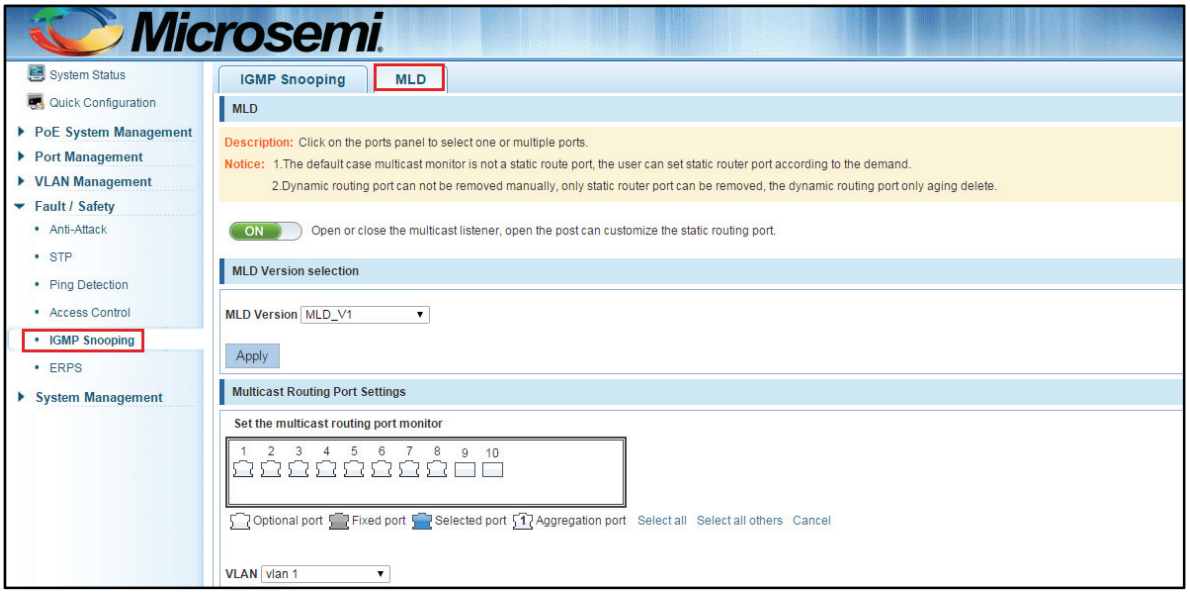


Figure 7-35: View MLD configuration information

7.5.7 ACTIVATION MLD FUNCTION

Click "Fault / Safety""MLD", click on the "Off" button to activate MLD functions:

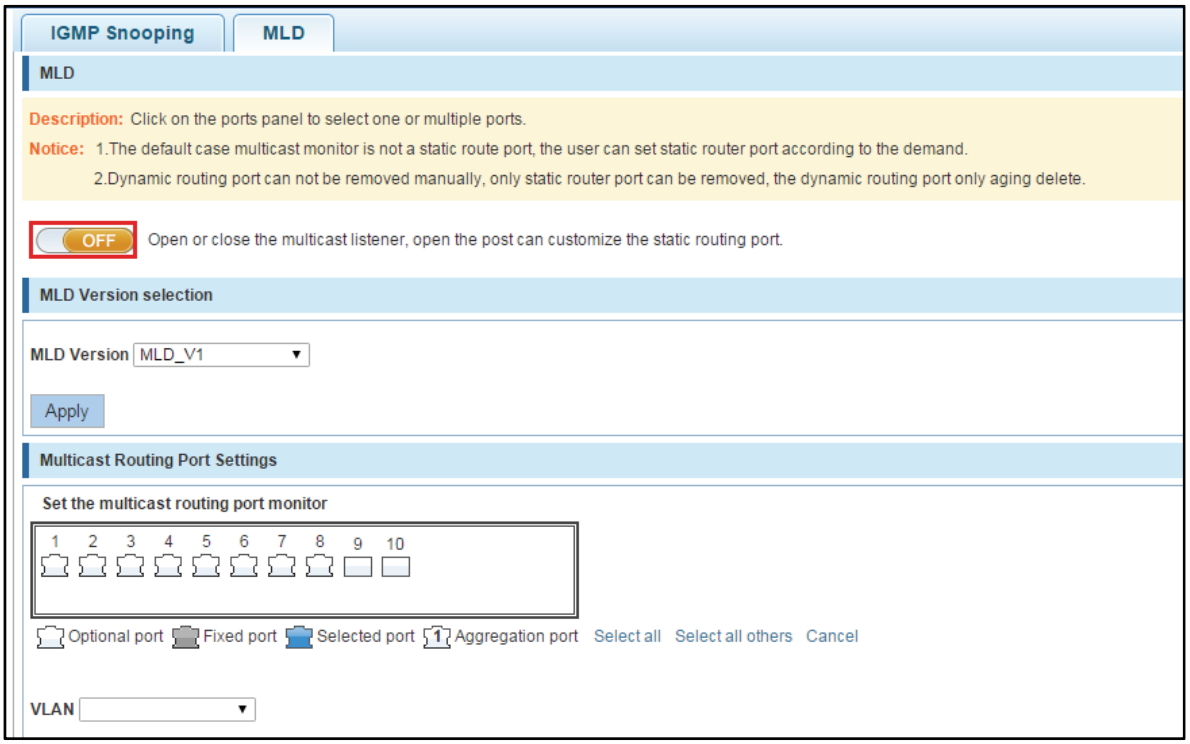


Figure 7-36: Open MLD functions configuration

By default, MLD is not turned on;

After opening MLD By default, all VLAN are open;

The default MLD version V1

7.5.8 DISABLING MLD FUNCTION

Click on "Fault / Safety""MLD", click "OK" button to disable MLD functions:

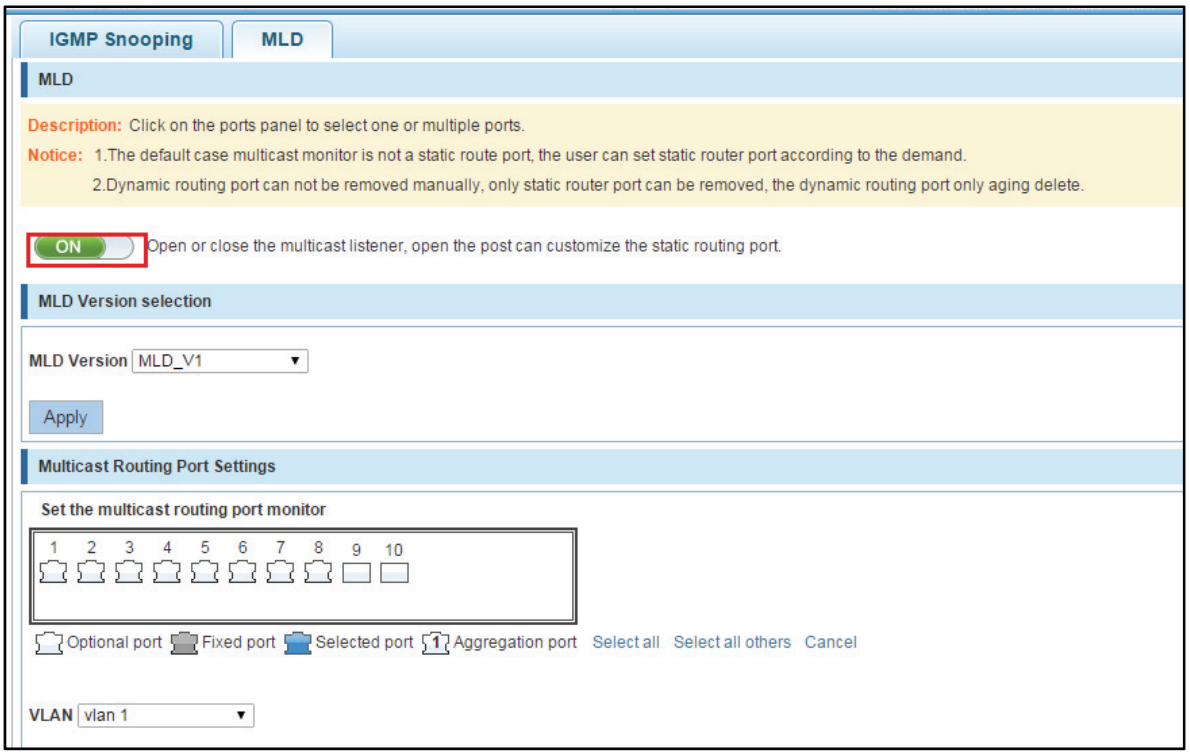


Figure 7-37: Close MLD function operation

7.5.9 CONFIGURING MULTICAST ROUTING

Listens on port panel, select routing port, select vlan, click on the "Add Router Port" button can be configured for multicast routing:

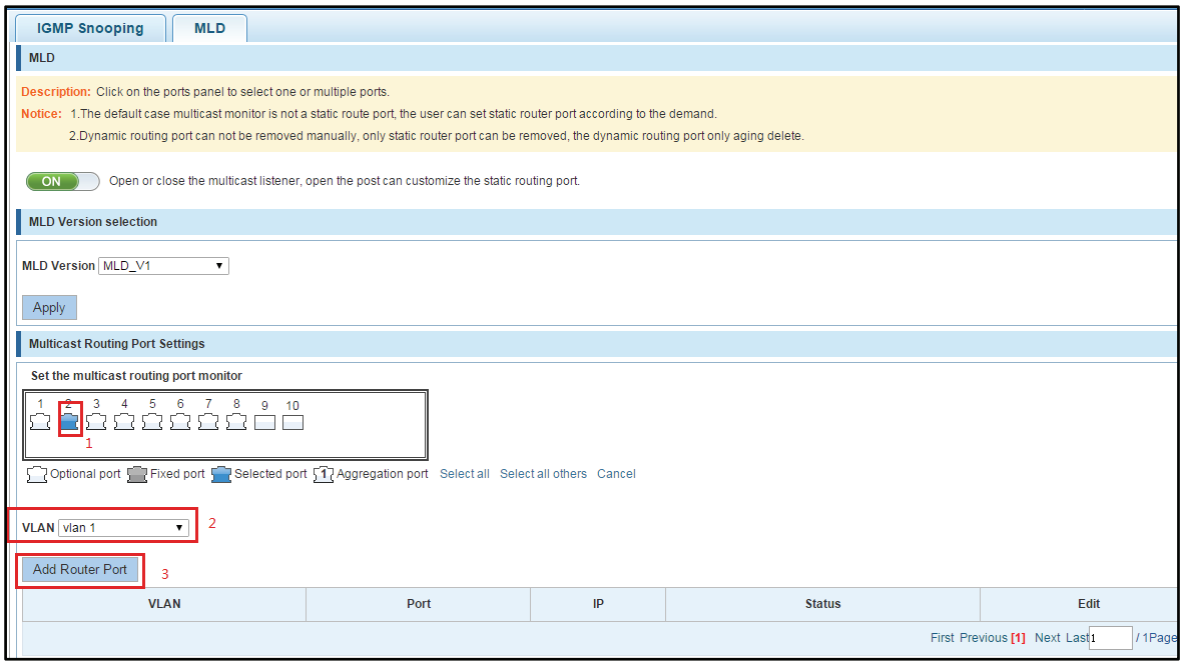


Figure 7-38: Configuring Multicast Routing

Multicast routing configuration steps are as follows:

Configuration Type	Step	Operation Description
Multicast Routing Configuration	**Step1**	On the panel, select Multicast Listener port router ports;
	Step2	Select vlan;
	Step3	Click on "Add Router Port" button to complete the configuration.

8 SYSTEM MANAGEMENT

8.1 SYSTEM SETTINGS

8.1.1 VLAN MANAGEMENT

8.1.1.1 VLAN Management View

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

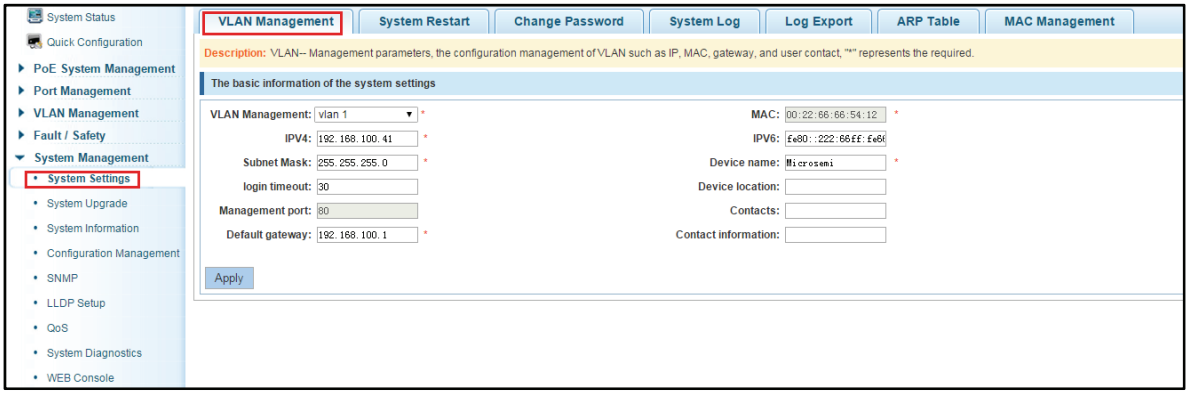


Figure 8-1: View VLAN management

- In the management VLAN page displays the property values of the current switch configuration management:
- Management VLAN: switch management VLAN ID, the default is 1;
- MAC Address: MAC address of the switch device;
- Management IP: switch management VLAN current IP address;
- Subnet Mask: The current switch management VLAN subnet mask information;
- Default Gateway: switch management VLAN current default gateway;
- Device Name: hostname of the switch;
- Device Location: switch placement;
- Timeout login: more than 5 minutes by default, Web Interface login screen return;
- Management Port: The default is 80.
- IPv6: switch management VLAN current IPv6 address;
- Contacts: the name of the Contact;
- Contact Information : the contact information of the Contact;

The default management VLAN is VLAN1, it can not be deleted.

8.1.1.2IP address configuration management

Modify the parameters of the corresponding dialog box, you can configure the management **I**P address:

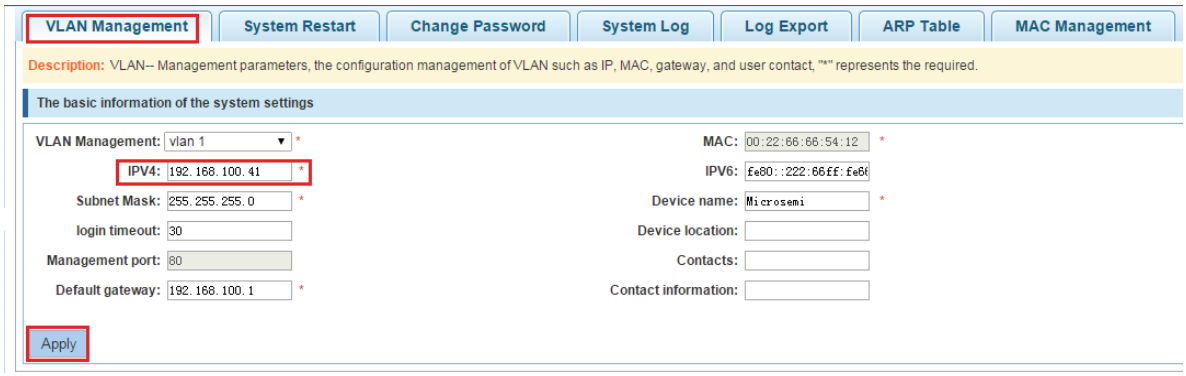


Figure 8-2: Changing the switch management address

To configure the switch management IP address is as follows:

Step	Operation Description
Step1	To modify the parameters, as follows: In the IP address text box to enter the IP address, such as 192.168.100.41 In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.0 In the Gateway Address text box to enter the gateway address, such as 192.168.100.1
Step2	Click the "Apply" button to complete the configuration.

8.1.2 SYSTEM RESTART

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

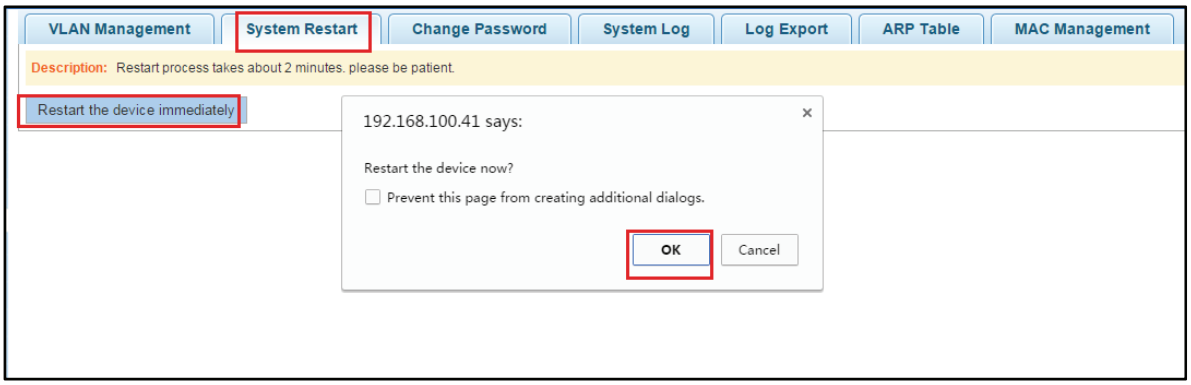


Figure 8-3: Reboot

Restart the device, follow these steps:

Configuration Type	Step	Operation Description
Reboot the device	**Step1**	Click on "Start the device immediately" button
	Step2	Click OK in the box that pops up "OK" button
	Step3	Prompted to save the current configuration, depending on your need to select "OK" or "Cancel"
	Step4	After the restart the progress bar moves to 100%, reboot the device

Equipment during the restart, WEB page can not be accessed;

When the device reboot is complete, we need to re-access the switch management WEB page.

8.1.3 PASSWORD CHANGE

8.1.3.1 Modify the superuser password

Click on the navigation bar "System Management""System Settings""Change Password", modify the value in the edit text box corresponding to the superuser password: Old password: password, the new password: admin, confirm the new password: admin, click "Apply"button:

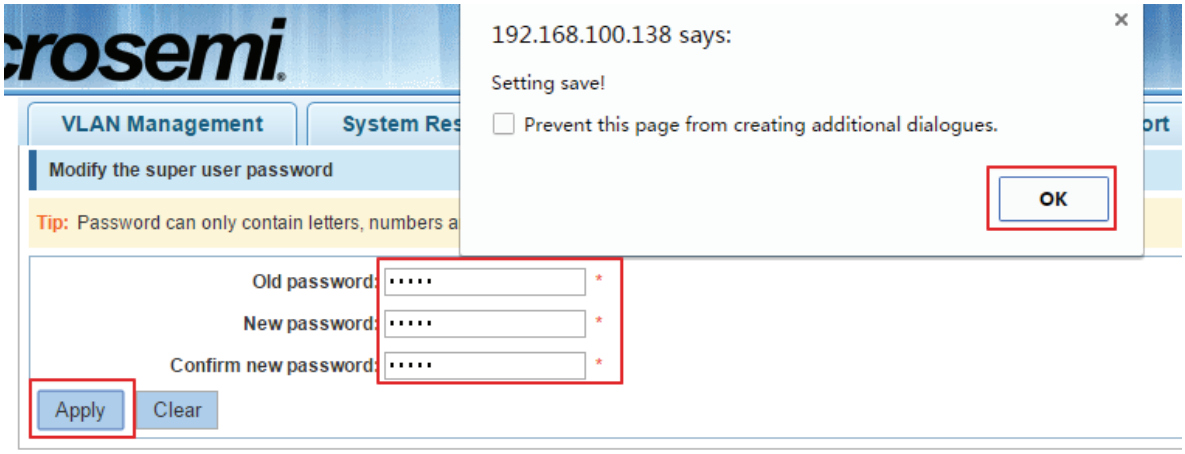


Figure 8-4: Super user password changes

Supervisor password, follow these steps:

Configuration Type	Step	Operation Description
Modify the super user password	**Step1**	Enter the old password: password;
	Step2	Enter the new password: admin;
	Step3	Confirm new password: admin
	Step4	Click the "Apply" button;
	Step5	Pop-up dialog box, click "OK" button.

Password can be set only alphanumeric characters and underscores.

8.1.4 SYSTEM LOG

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

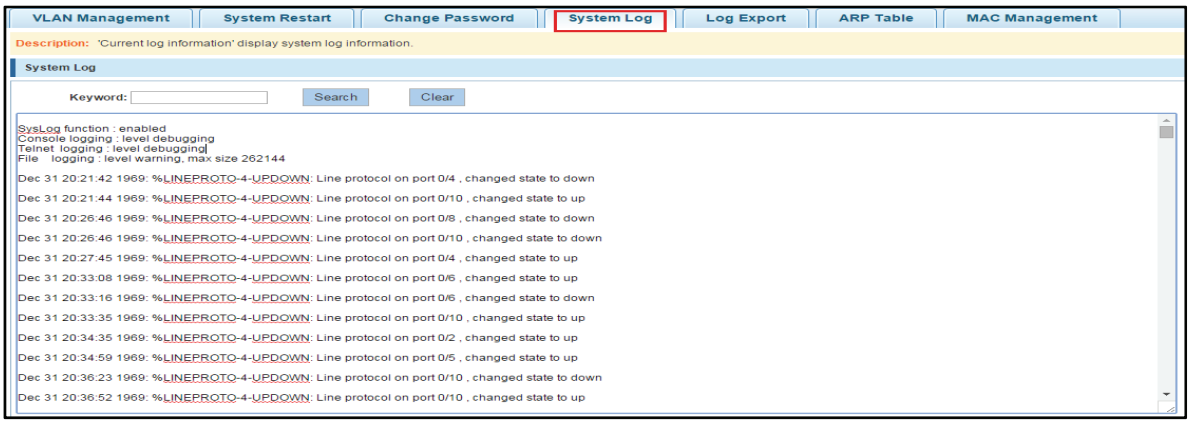


Figure 8-5: System Log Management

Log management system WEB page to view the contents of the command line is consistent with the results of the command show logging;

Click "Clear" button to clear the current log information switch ；

8.1.5 EXPORT LOG

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

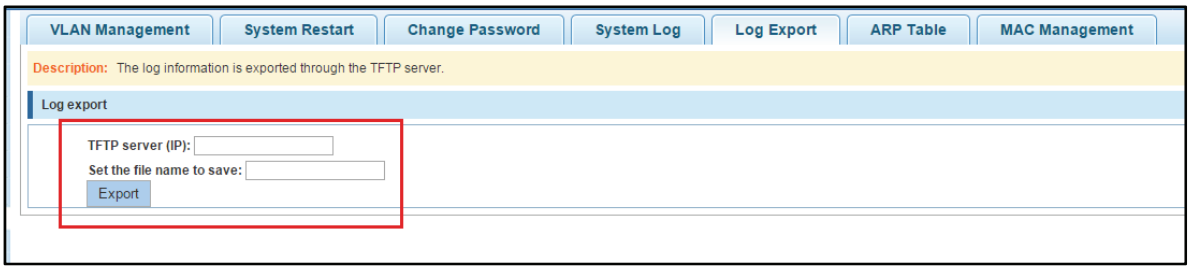


Figure 8-6: Log Export

8.1.6 ARP TABLE

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

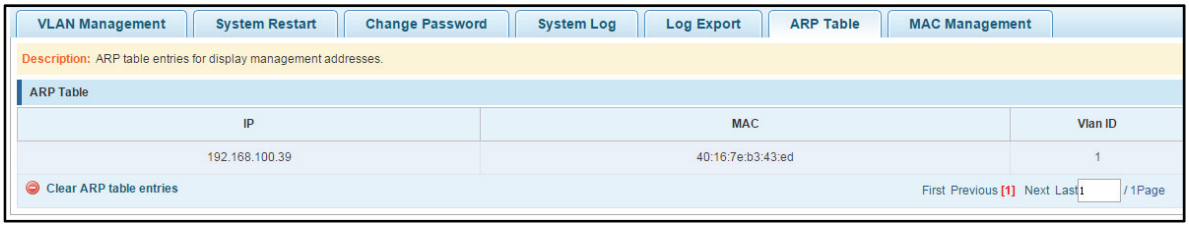


Figure 8-7: ARP message

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

8.1.7 MAC ADDRESS MANAGEMENT

8.1.7.1 MAC address lookup

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

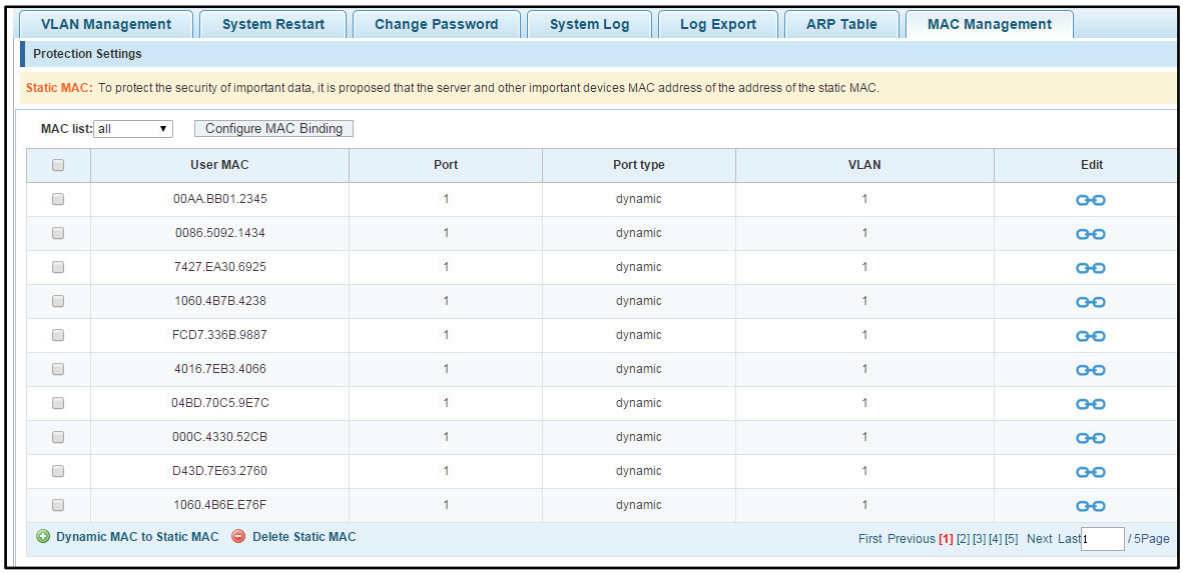


Figure 8-8: MAC address lookup display

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

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

You can query the MAC address type:

Query Type	Step	Operation Description
According to the type of query MAC address	**Step1**	Type in the MAC address MAC check list next to the drop-down box Select: All / static / dynamic;

8.1.7.2 Add a static MAC address type

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

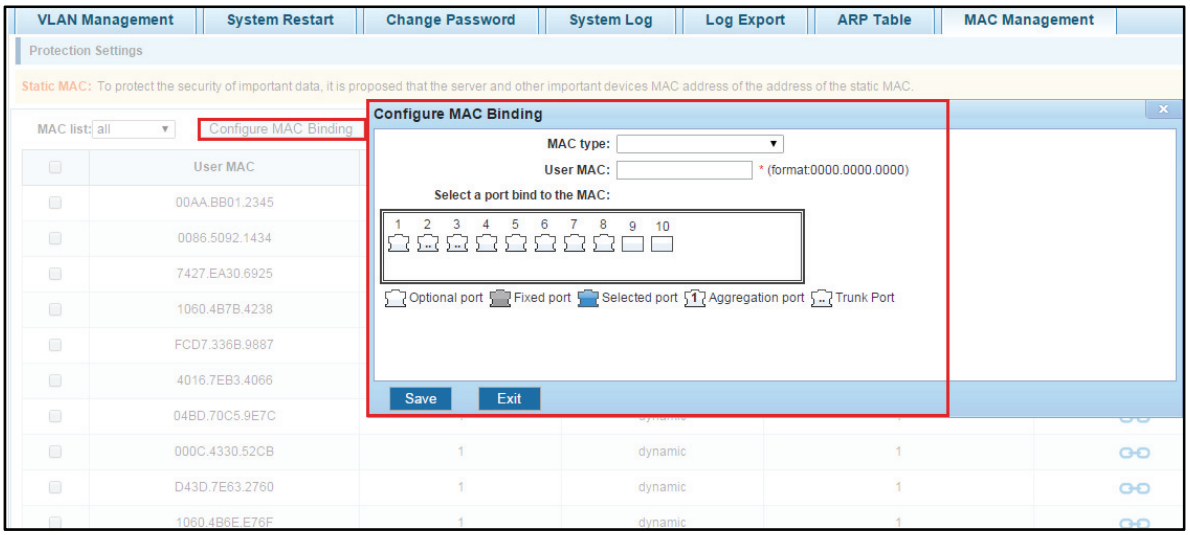


Figure 8-9: MAC addresses statically bound static configuration

Statically typed MAC address configuration steps are as follows:

Configuration Type	Step	Operation Description
Statically typed MAC address configuration	**Step1**	Click the "Configure MAC Binding" button;
	Step2	In the "User MAC" text box to enter the MAC address, such as 0001.7A4F.74D2;
	Step3	Select ports in the port panel;
	Step4	Click on "save", to complete the configuration.

Use“ ” Button binding static MAC address

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

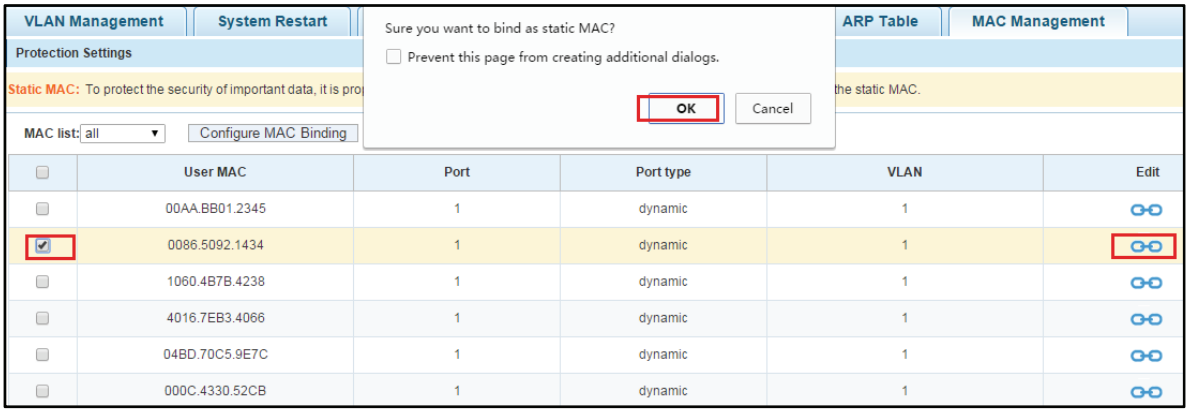


Figure 8-10: MAC address of the static binding configuration

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

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

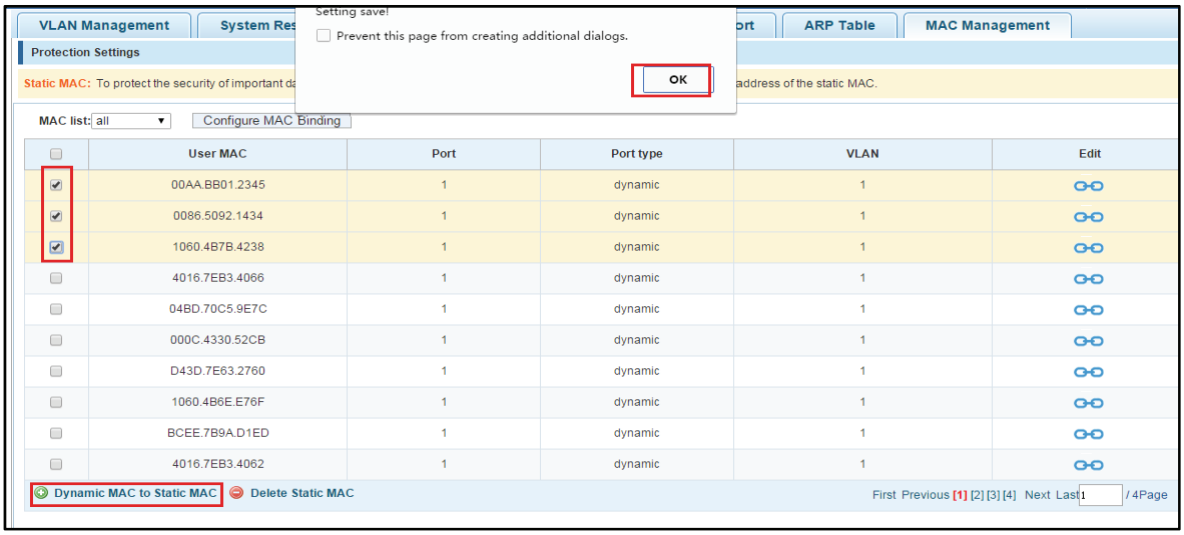


Figure 8-11: Batch-MAC binding configuration

8.1.7.3 Remove the static MAC address type

1. Single MAC records are deleted

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

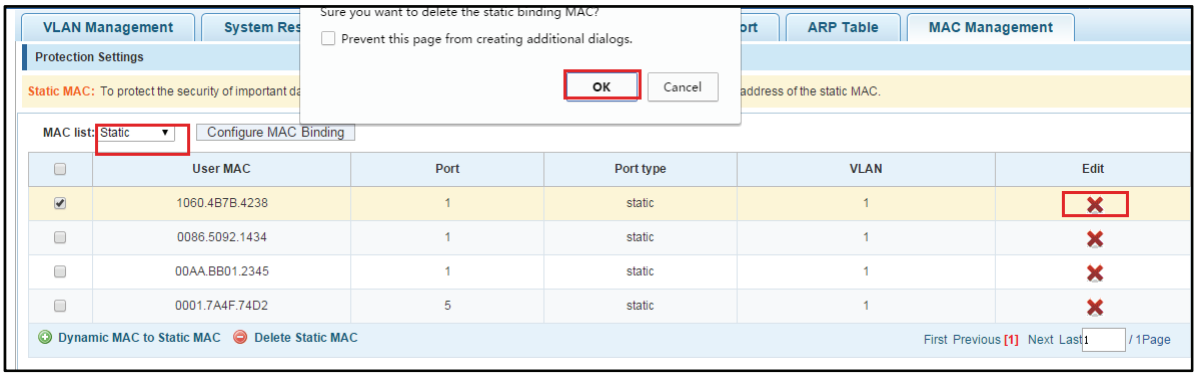


Figure 8-12: MAC address deletion

Remove MAC address configuration steps are as follows:

Configuration Type	Step	Operation Description
Remove MAC address configuration	**Step1**	To delete the selected MAC address.
	Step2	Click“ ✖ ” button to delete the configuration

2. Batch delete a static MAC address

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

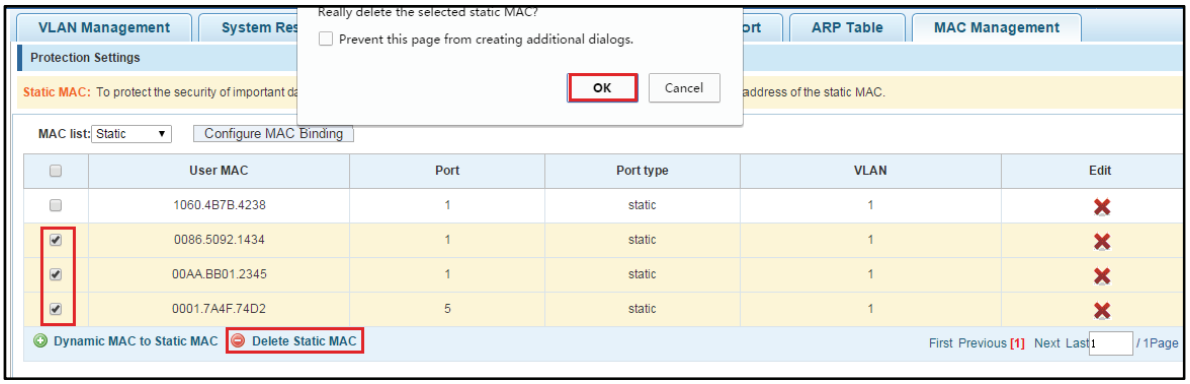


Figure 8-13: MAC address batch deletion deletion

8.2 SYSTEM UPGRADE

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

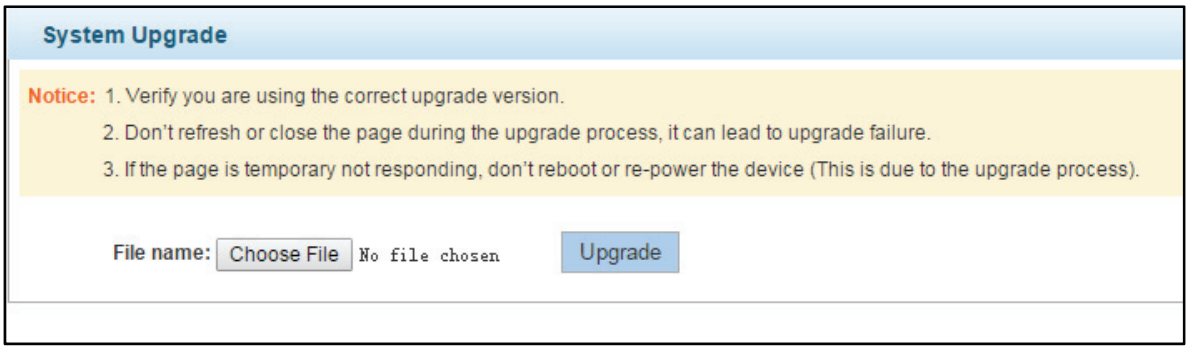


Figure 8-14: Switch System Upgrade

Do not upgrade process will switch off;

Ensure the correctness of the upgrade before the upgrade file;

Must be saved before the upgrade configuration to avoid configuration loss;

After the upgrade process is completed, the switch will automatically restart, the application of new software.

Switch system upgrade steps are as follows

Configuration Type	Step	Operation Description
Switch Software Upgrade	**Step1**	Click "Choose File" button to select the switch upgrade file;
	Step2	Click the "Upgrade" button switch to start the upgrade new software;
	Step3	When the upgrade progress bar is at 100%, the switch will automatically reboot, completion of the upgrade is completed.

The upgrade process Do not leave the switch software upgrades WEB page;

After the upgrade is complete, the switch will automatically reboot;

Equipment during the restart, WEB page can not be accessed;

When the device reboot is complete, we need to re-access the switch management WEB page.

8.3 SYSTEM INFORMATION

8.3.1 MEMORY INFORMATION

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

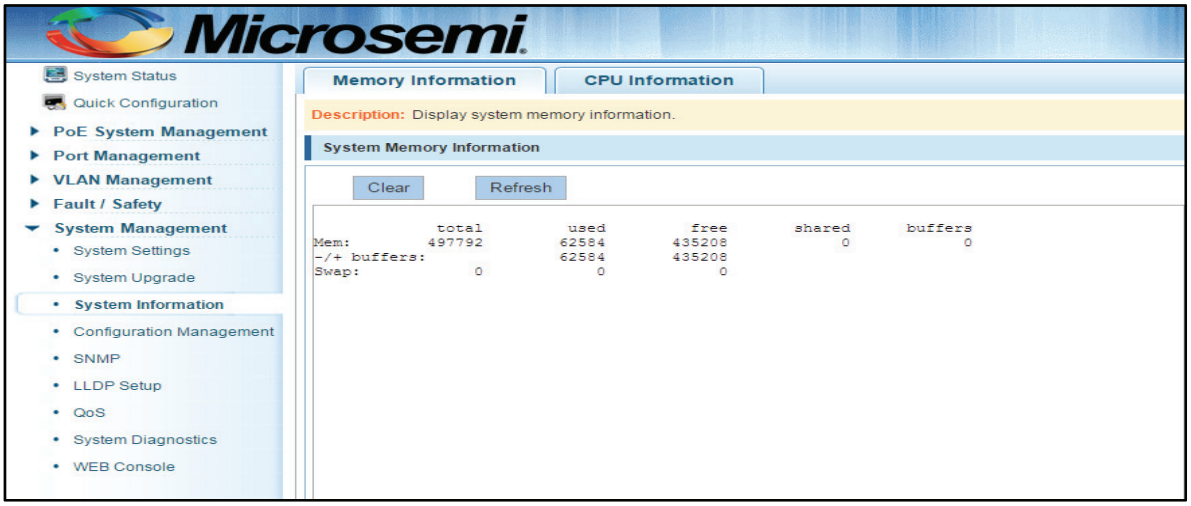


Figure 8-15: System memory information

See the WEB page of memory information content consistent with the results show the memory command command line;

Click on the "Clear" button to Clear the current switches in the memory information;

Click on the "Refresh" button to Refresh the current switches in the memory information.

8.3.2 THE SYSTEM TASK

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

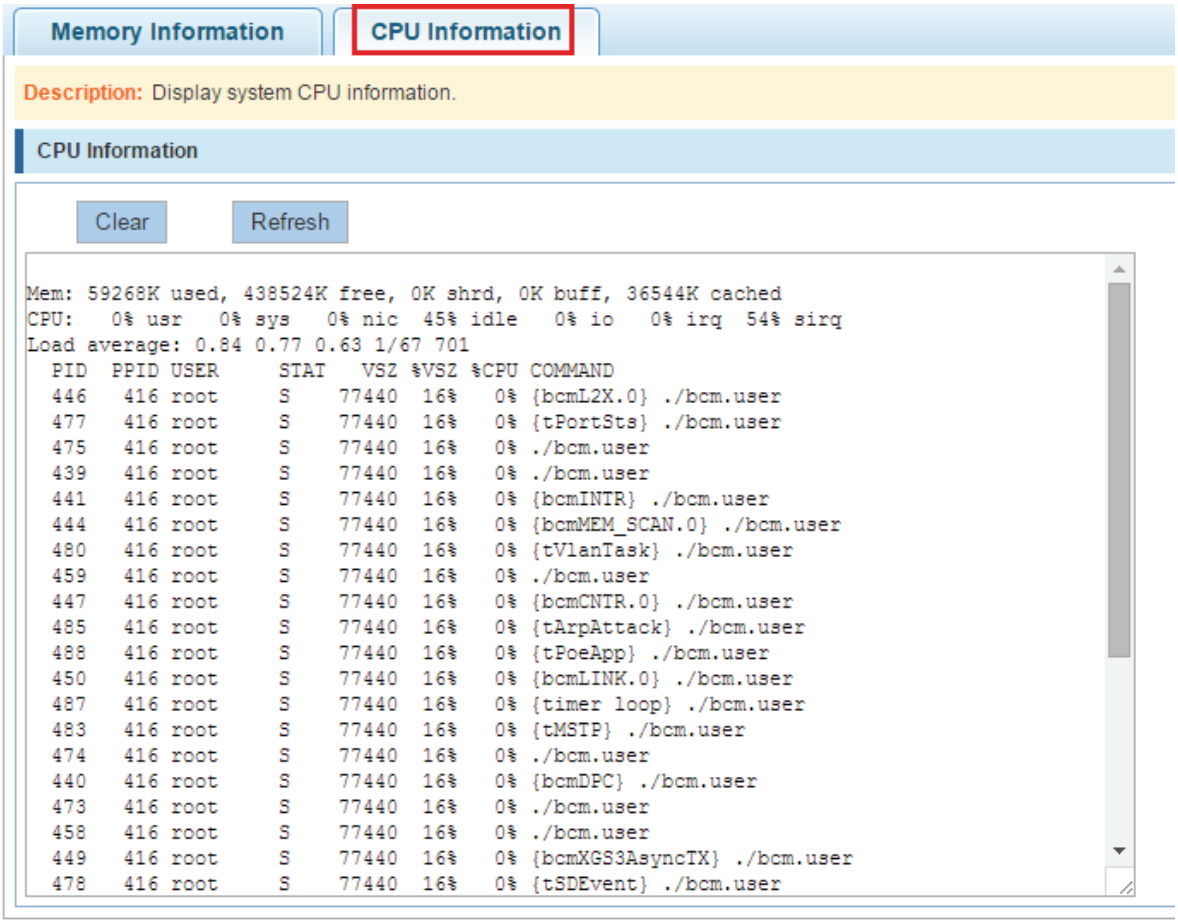


Figure 8-16: CPU information

WEB pages to the content of the system task view consistent with the results show the CPU commands command line;click on the "Clear" button to remove the current switches in the system;

Click on the "Refresh" button to Refresh the current switches in the system task.

8.4 CONFIGURATION MANAGEMENT

8.4.1 CONFIGURATION MANAGEMENT

1. To see the current configuration

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

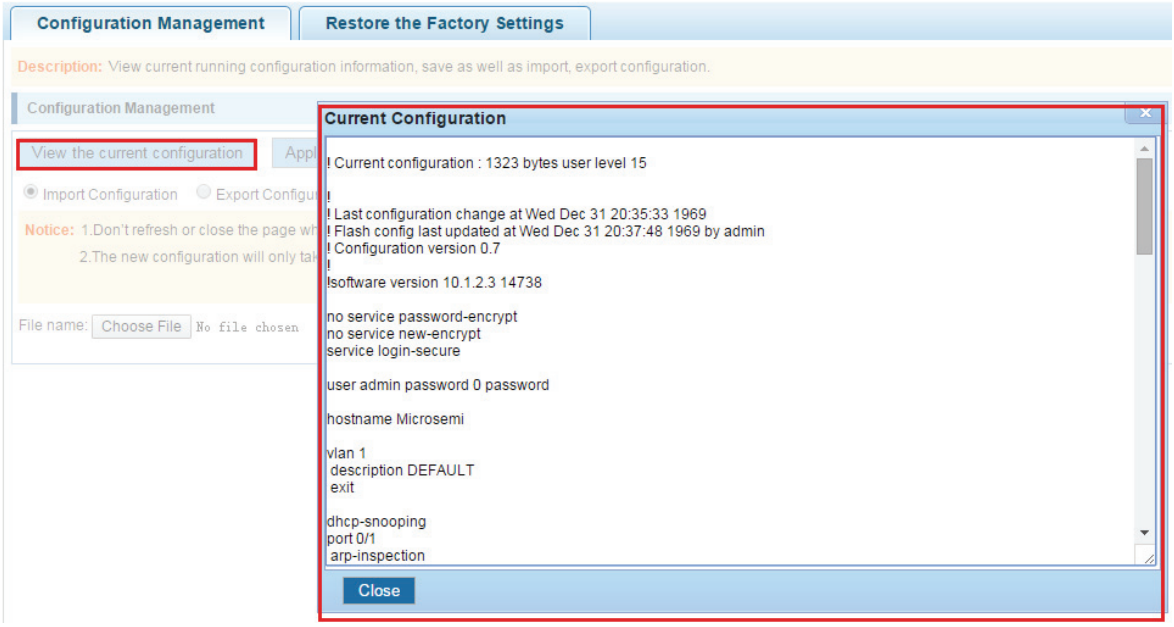


Figure 8-17: View the current configuration

2. Save the current configuration

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

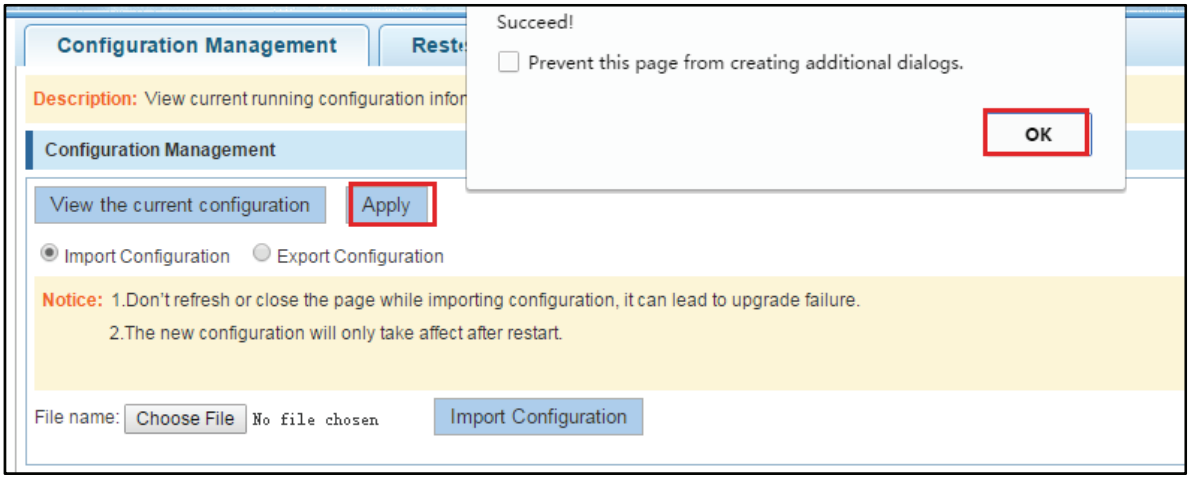


Figure 8-18: To save the current configuration

3. The configuration

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

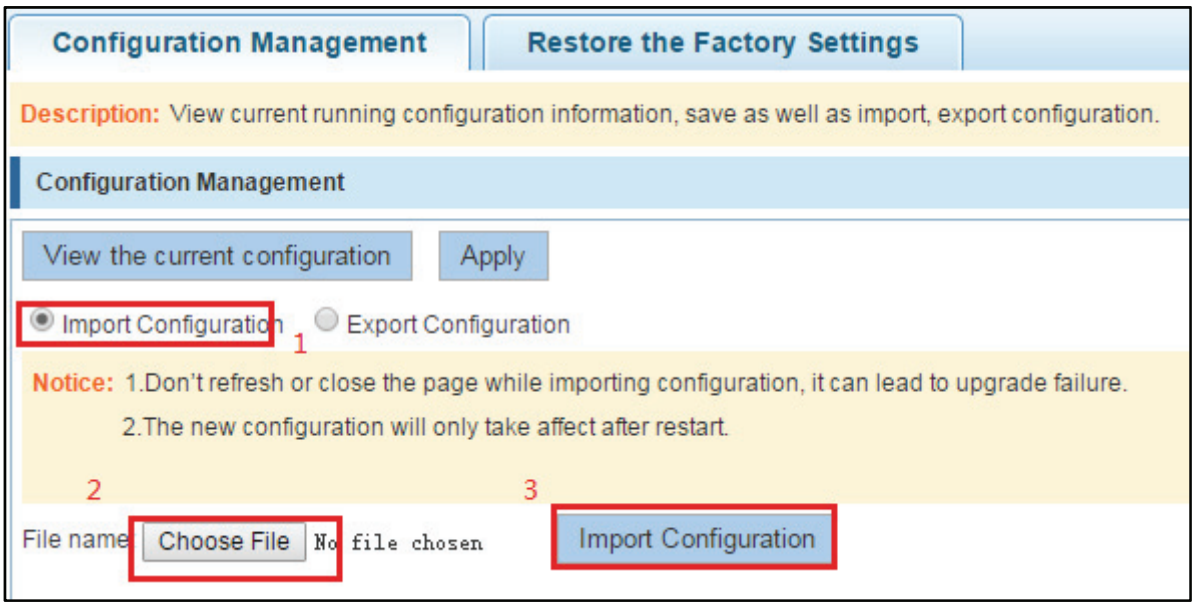


Figure 8-19: Imported configuration

Import the configuration steps are as follows:

Configuration type	Steps	Operation Description
Telnet login password	**Step1**	Select the "Import Configuration";
	Step2	Click "Choose File" button to find you want to import the configuration File;
	Step3	Click on "Import Configuration" button;
	Step4	Confirm the restart.

Table 8-8 import configuration steps

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

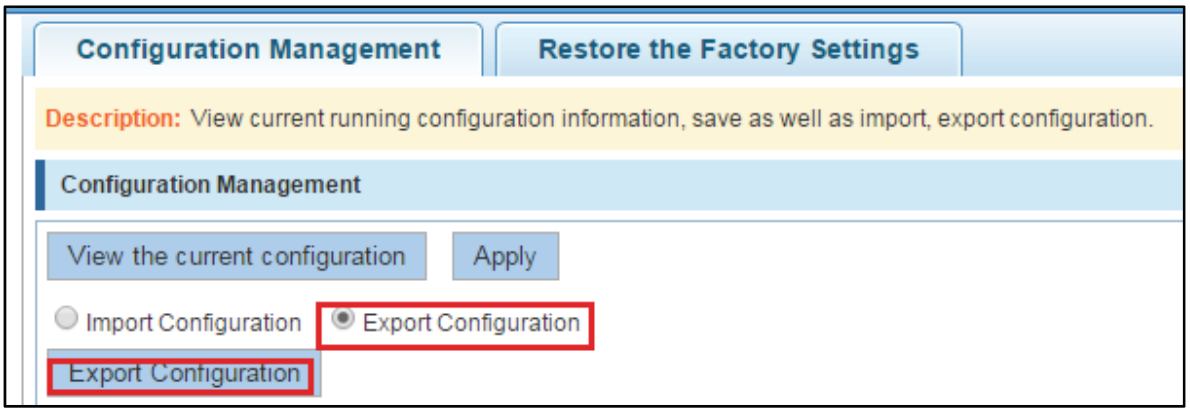


Figure 8-20: Export configuration

8.4.2 RESTORE FACTORY SETTINGS

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

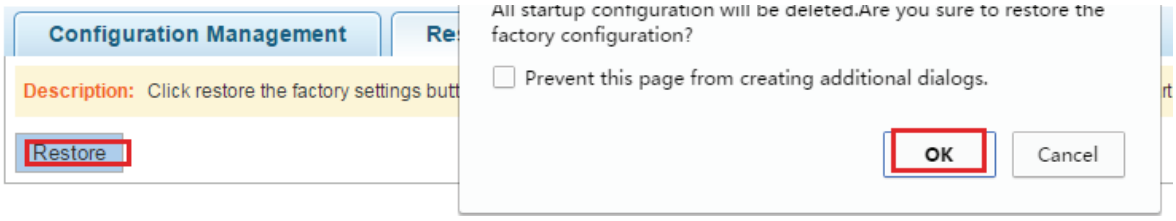


Figure 8-21: Restore factory Settings

Factory default operation steps are as follows:

Configuration type	Steps	Operation Description
Restore the factory Settings	**Step1**	Click the "Restore the Factory Settings" button
	Step2	In the pop-up confirmation box, click the "OK" button
	Step3	After the completion of the reset switch, wait for equipment to restart, switch back to factory default configuration

8.5 SNMP

8.5.1 CHECK THE SNMP

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

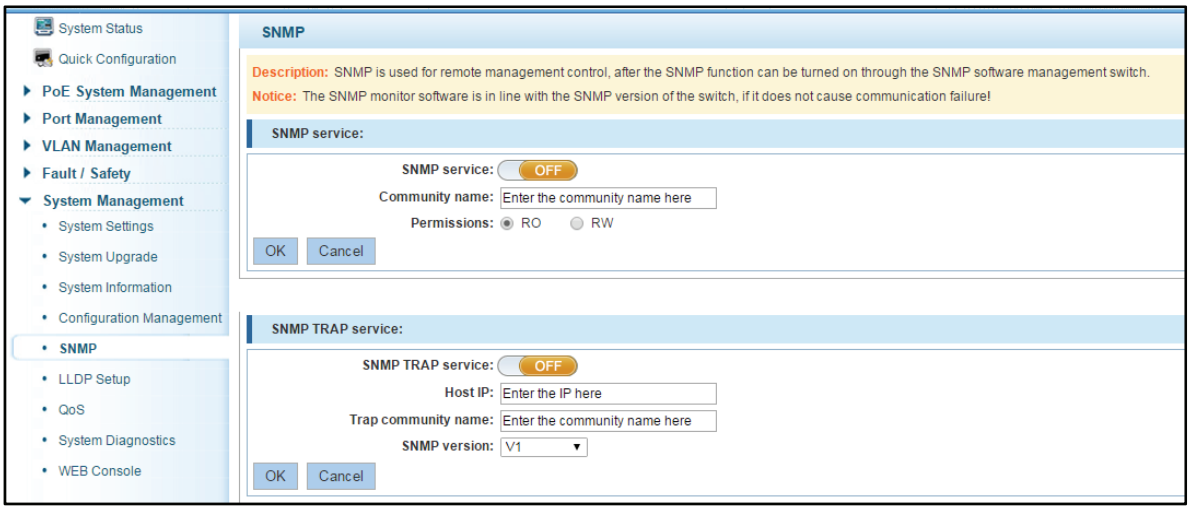


Figure 8-22: View the SNMP configuration information

By default SNMP is not open;

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

8.5.2 ACTIVATE THE SNMP

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

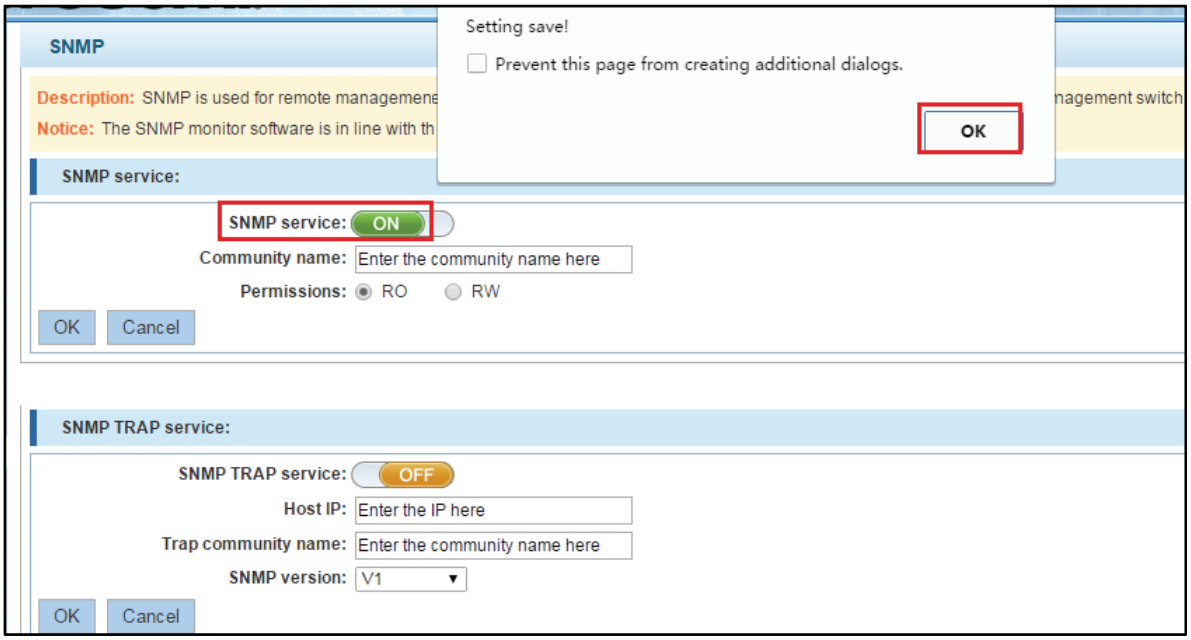


Figure 8-23: Activation SNMP function

Activation function SNMP configuration steps are as follows:

Configuration type	Steps	Operation Description
Activate the function of SNMP	**Step1**	Choose open SNMP options;
	Step2	Click "OK" button to complete the configuration.

Before configure other function, must first open the SNMP function;

SNMP V1 and V2C version support.

8.5.3 TO DISABLE THE SNMP

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

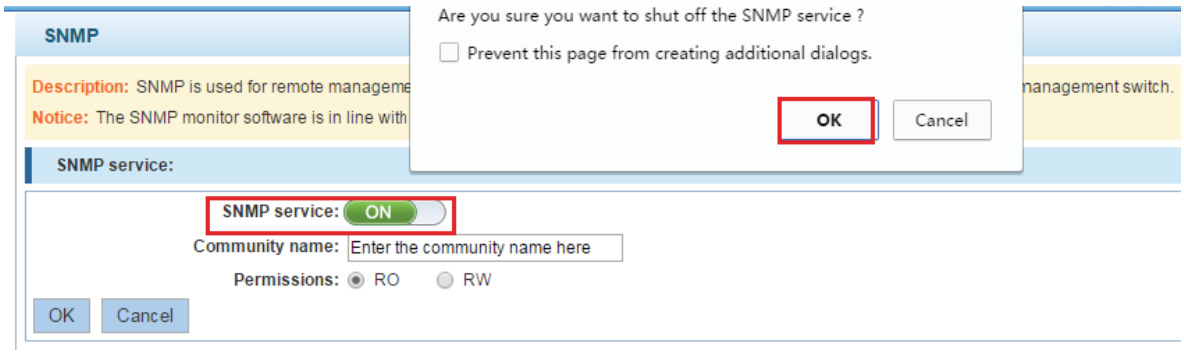


Figure 8-24: Disable the SNMP function

Disable the SNMP function configuration steps are as follows:

Configuration type	Steps	Operation Description
Disable the SNMP function	**Step1**	Choose close SNMP options;
	Step2	Click "OK" button to complete the configuration.

8.5.4 ACTIVATE THE TRAP

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

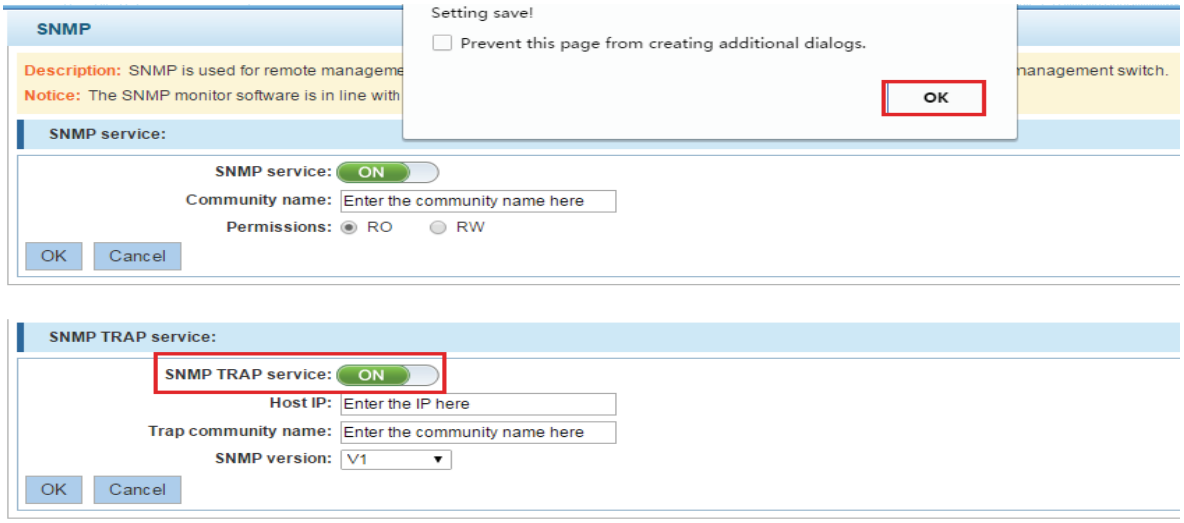


Figure 8-25: Activation function of the TRAP

Activate the TRAP function configuration steps are as follows:

Configuration type	Steps	Operation Description
Activate the TRAP function	**Step1**	Select "ON" option;
	Step2	Click "OK" button to complete the configuration.

With open the TRAP, service host can send real-time TRAP message.

8.5.5 DISABLE THE TRAP

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

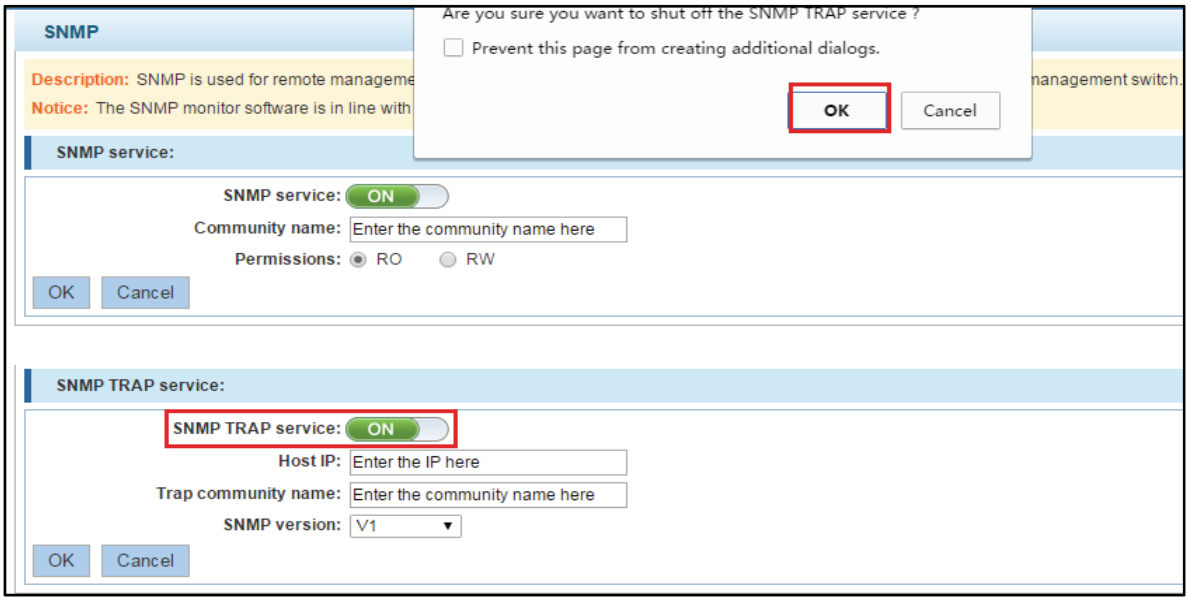


Figure 8-26: Disable TRAP function

Disable the TRAP function configuration steps are as follows:

Configuration type	Step	OperationDescription
Disable the TRAP function	**Step1**	Select "ON" to "OFF" option.
	Step2	Click "OK" button to complete the configuration.

8.5.6 INCREASE OF COMMUNITY

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

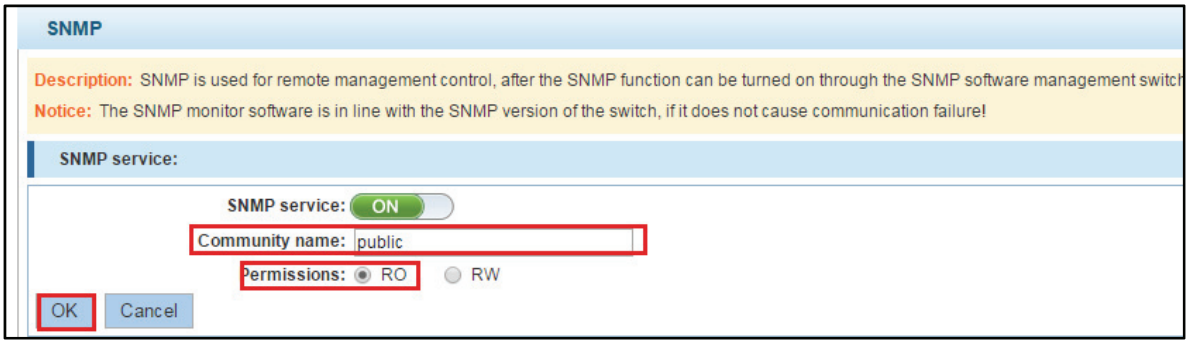


Figure 8-27: Increase community

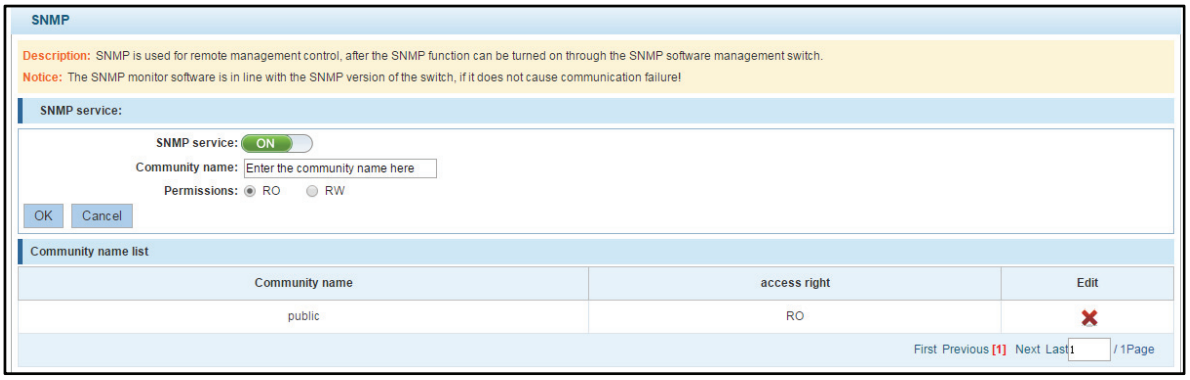


Figure 8-28: Community results

Increase community configuration steps are as follows:

Configuration type	Step	OperationDescription
Increase community name	**Step1**	In the community name dialog box input: the public;
	Step2	Select "RO" permissions;
	Step3	Click on "OK" button, complete the configuration.

Community has two kinds of read-only and read-write permi

When the SNMP closed, hidden community list, close the TRAP

8.5.7 DELETE THE COMMUNITY NAME

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

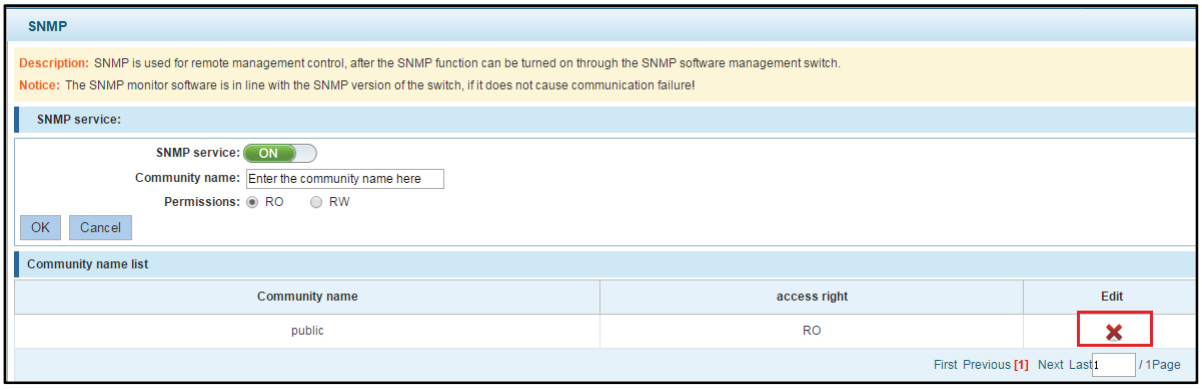


Figure 8-29: Delete community 30

8.5.8 ADDED THE SNMP TRAP SERVICE HOST

Click on the "System Management""SNMP", in the host IP text box input: 192.168.100.83, TRAP community name: public, SNMP version choice: V2C, click the "OK" button, complete the configuration:

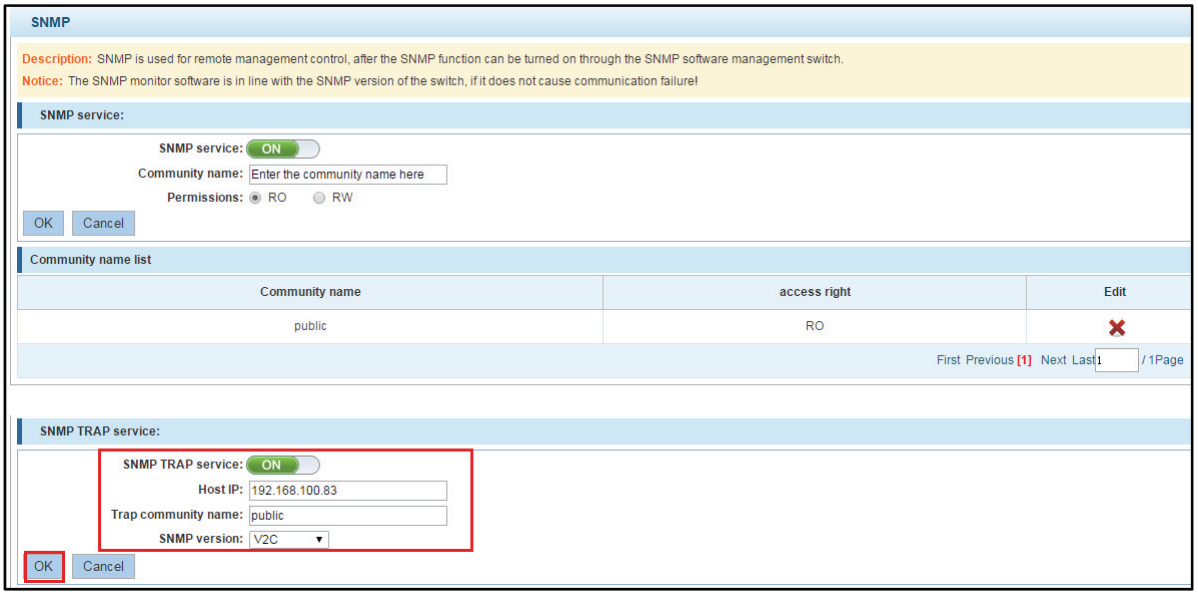


Figure 8-30: Increases the SNMP TRAP service host

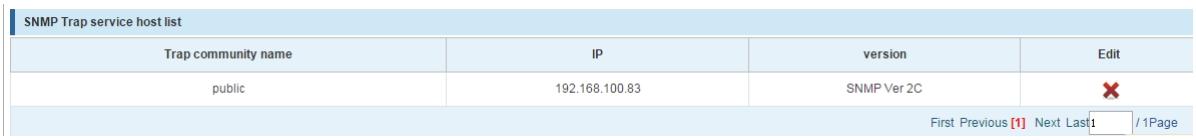


Figure 8-5: SNMP TRAP service host

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

Configuration type	Step	Description
Increase the SNMP TRAP service host	**Step1**	In the host IP dialog box input: 192.168.100.83;
	Step2	In TRAP community name dialog input: public;
	Step3	Select the SNMP version: V2C
	Step4	Click on "OK" button, complete the configuration.

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

8.5.9 DELETE THE SNMP TRAP SERVICE HOST

Click on the "System Management""SNMP", in the SNMP TRAP service host list need to delete the object, click  "finish" configuration:

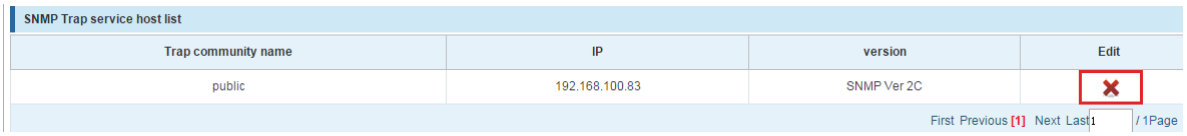


Figure 8-31: Delete community

8.6 LLDP FOUND

8.6.1 CHECK THE LLDP CONFIGURATION

Click on the "System Management""LLDP Setup", can collect the basic information of the current device:

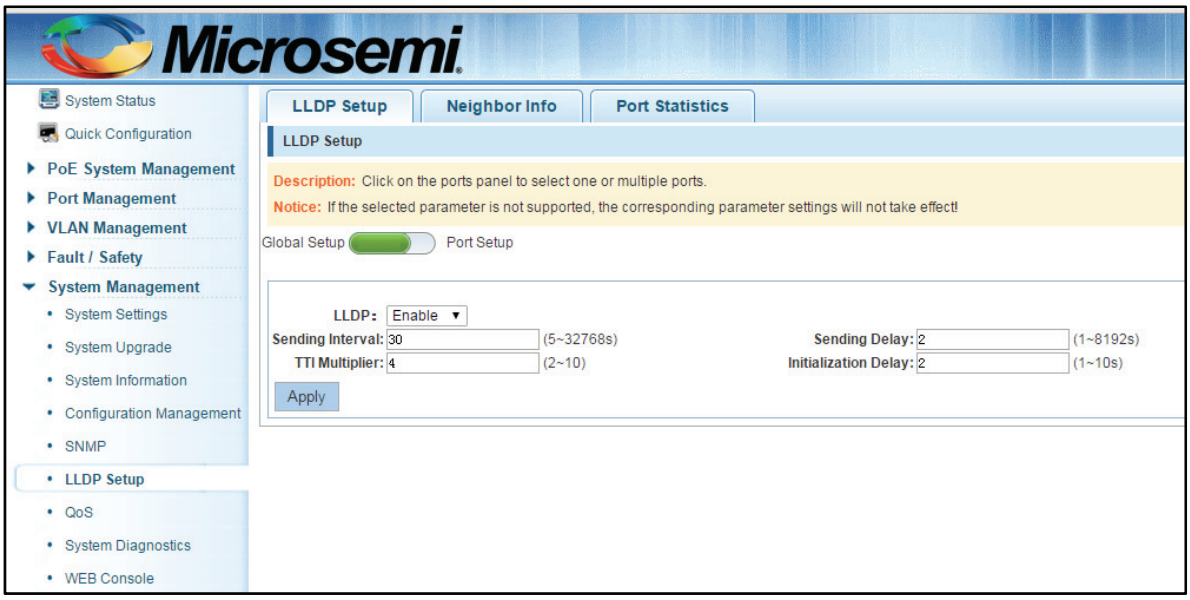


Figure 8-32: LLDP configuration view

8.6.2 CHANGE THE LLDP CONFIGURATION

Click on the "System Management""LLDP Setup", change the current configuration parameters, click "Apply" application, confirm the currentconfiguration

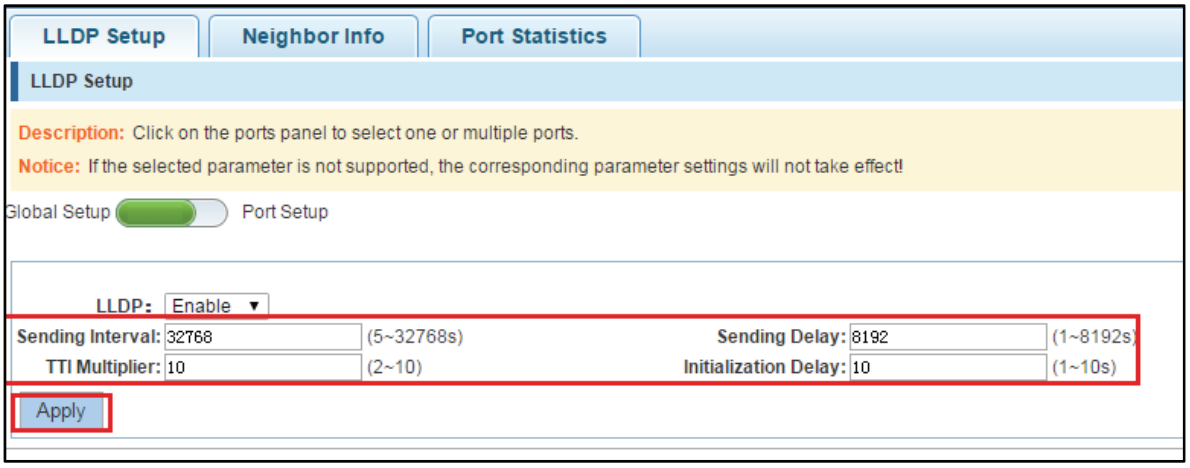


Figure 8-33: LLDP configuration parameters

8.6.3 CLOSE THE LLDP GLOBAL PARAMETERS CONFIGURATION

Click on the "System Management""LLDP Setup", click the LLDP enabled drop-down box, select disable, click "Apply" to confirm the current configuration, after close the LLDP global parameters configuration:

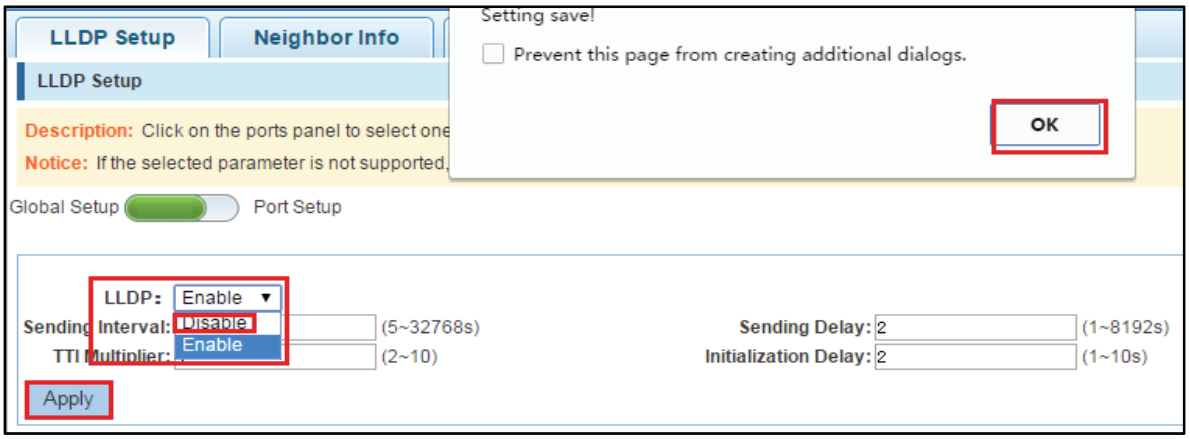


Figure 8-34: Closing the LLDP global parameters configuration

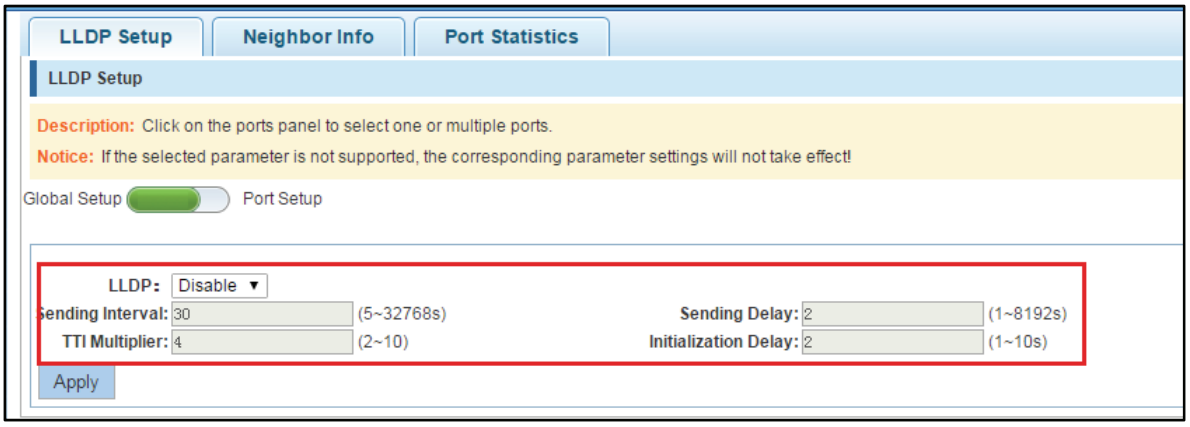


Figure 8-35: Successfully closed LLDP global parameters configuration

8.6.4 THE LLDP PORT CONFIGURATION

Click on "System Management""LLDP Setup", click on the slide button by the "Global Setup" to "Port Setup" to view the current configuration LLDP Port:

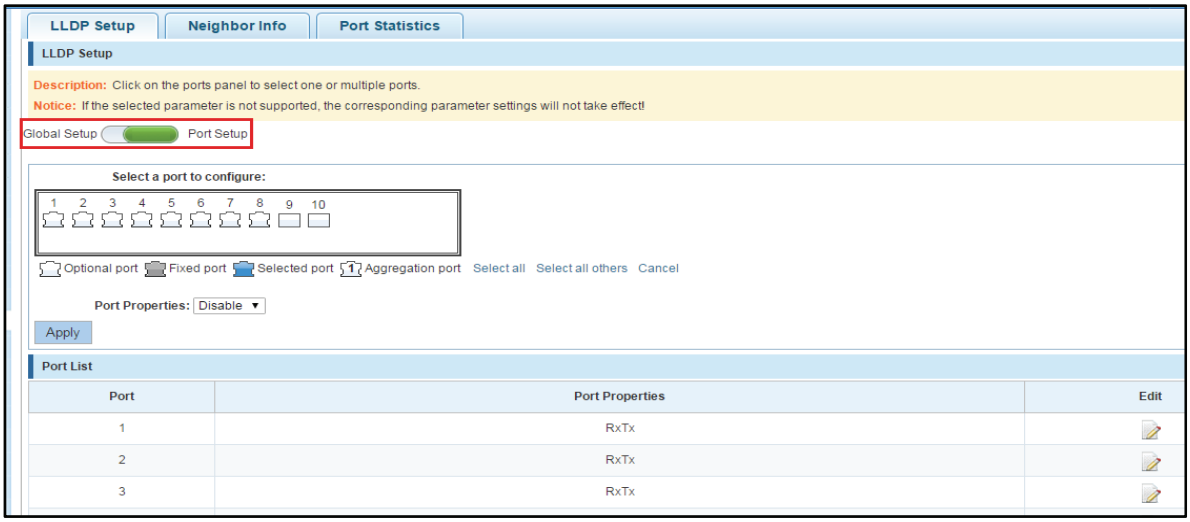


Figure 8-36: LLDP port configuration view

8.6.5 SET PORT LLDP PERFORMANCE

Click on the "System Management""LLDP Setup", choose to configure the Port after, choose the Port need to configure the attributes, click on the button "Port Properties", click "Apply" application of the currently selected configuration

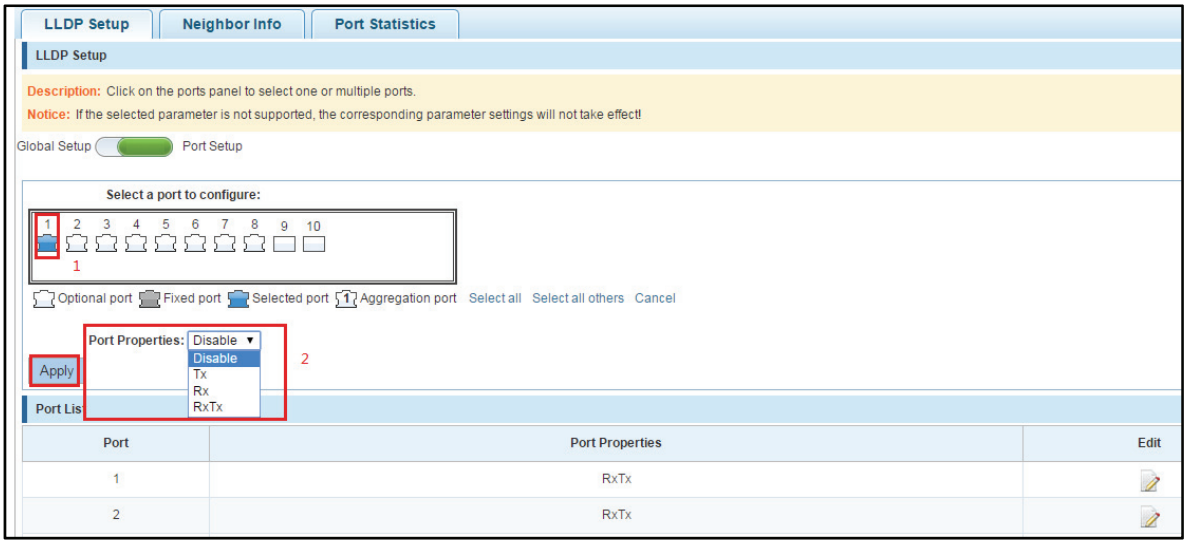


Figure 8-37: Setting LLDP port properties

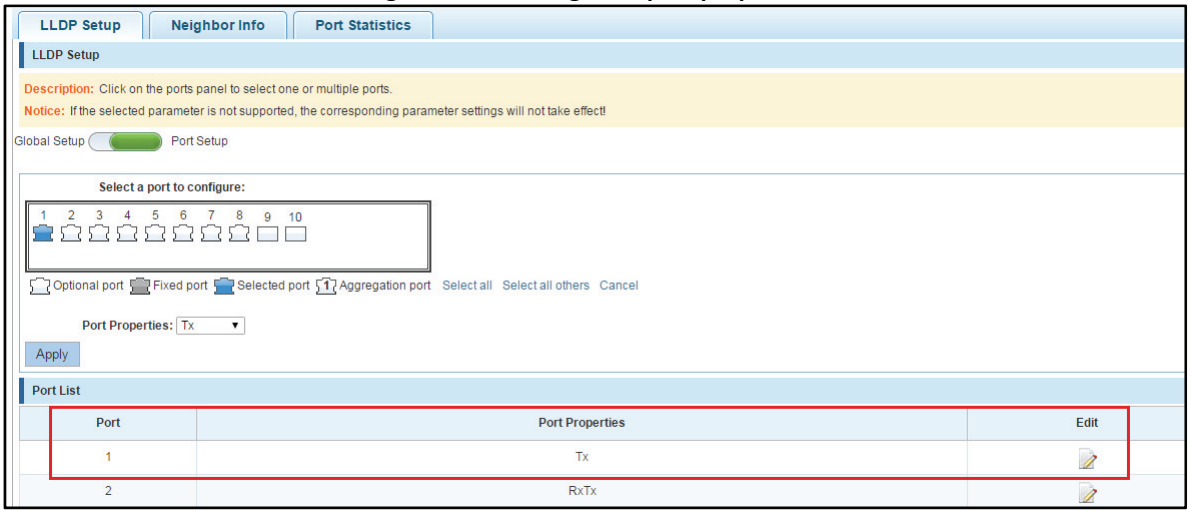


Figure 8-38: Port properties configuration is successful

8.6.6 VIEW THE LLDP NEIGHBOR INFORMATION

Click on the "System Management""Neighbor Info", you can view the current equipment Neighbor information:

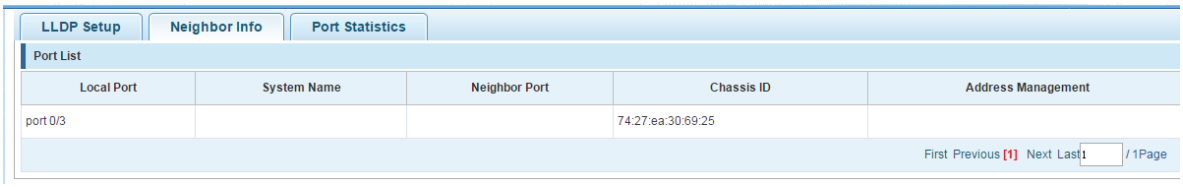


Figure 8-39: View LLDP neighbor information

8.6.7 CHECK THE LLDP PORT INFORMATION

Click on the "System Management""Port Statistics", you can view the current Port information:

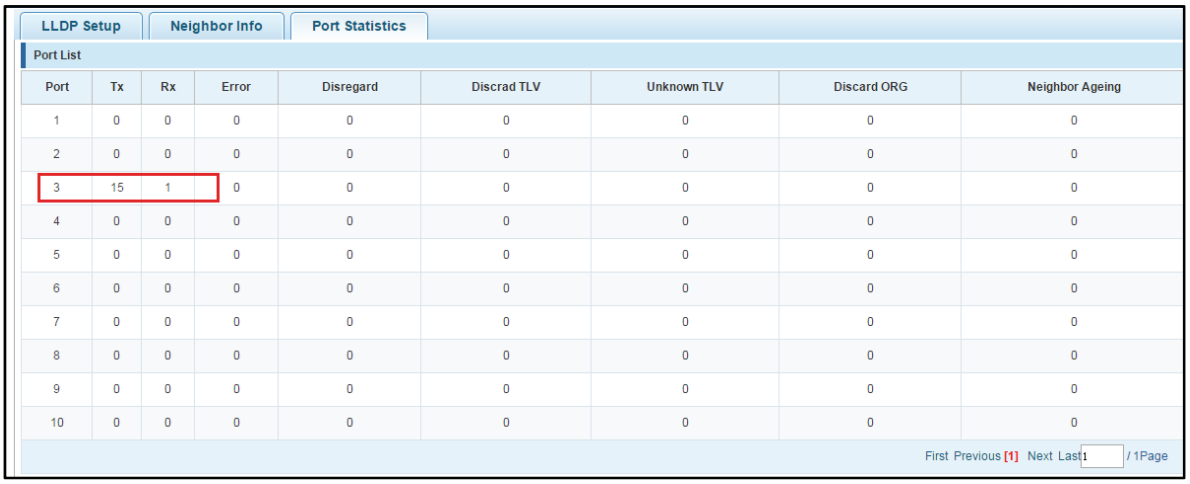


Figure 8-40: LLDP port information

8.7 QOS

8.7.1 VIEW THE QOS CONFIGURATION

Click on the "System Management""QOS", can view the device QOS basic information:

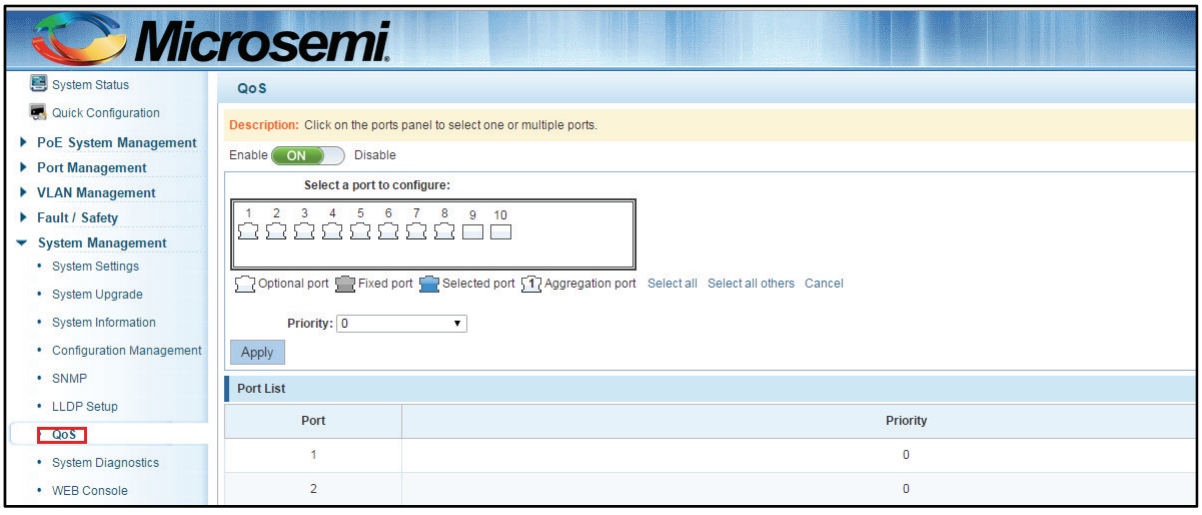


Figure 8-41: QoS configuration

By default, close the QoS function.

8.7.2 THE CONFIGURATION OF PORT PRIORITY

Click ON "System Management""QOS" slide button from "OFF" to "ON", after open the QOS, choose to configure port (can be set in bulk), set the port priority, click "Apply" to confirm and applied successfully.

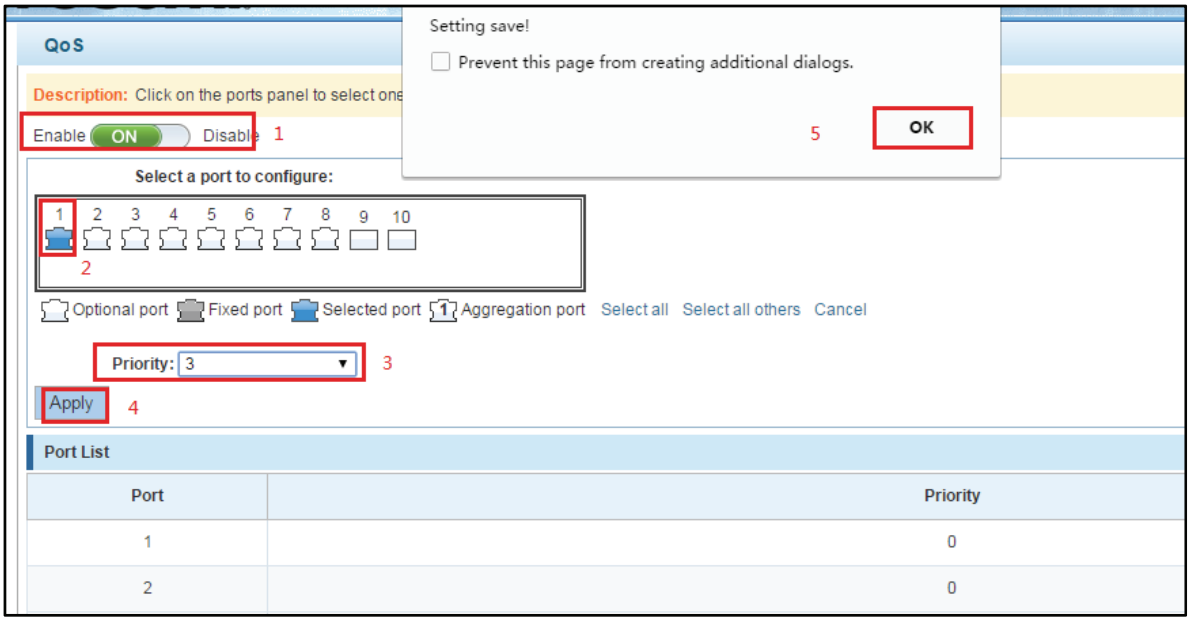


Figure 8-42: Setting port priority

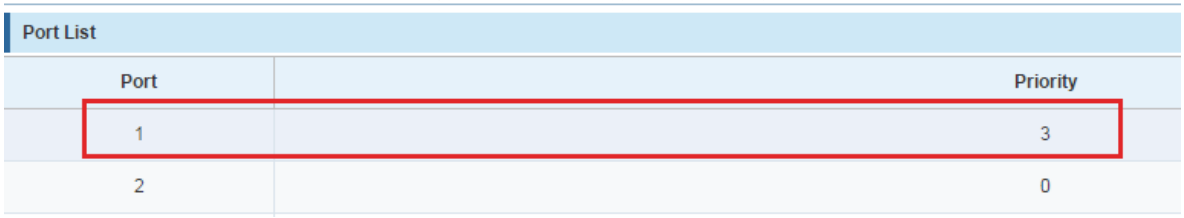


Figure 8-43: Successful port priority setup

8.7.3 TO DISABLE THE QOS

Click ON the "System Management""QoS", slide the button by the "ON" slide to "OFF", click "OK" to close the QoS function:

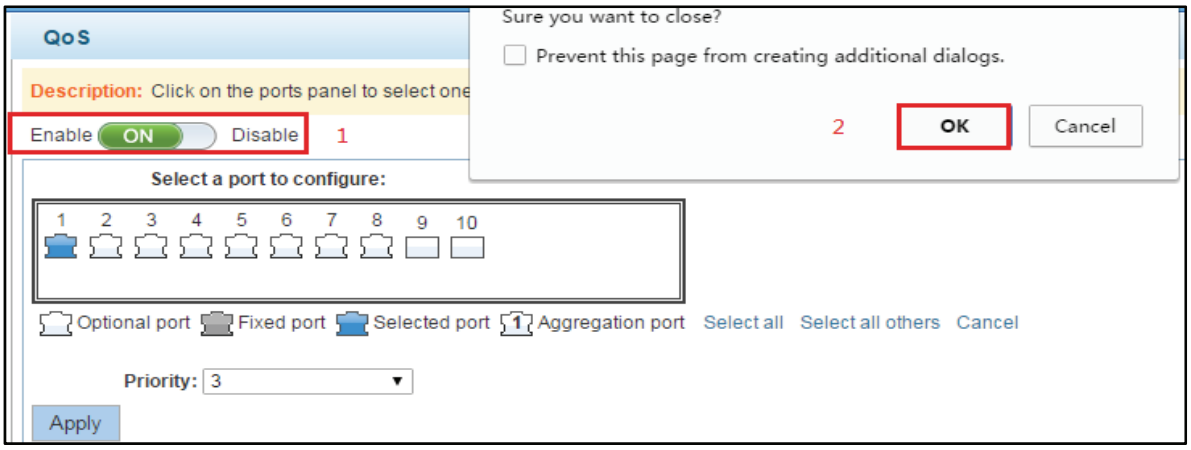


Figure 8-44: Closing the QoS function

8.7.4 A KEY FAULT COLLECTION

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

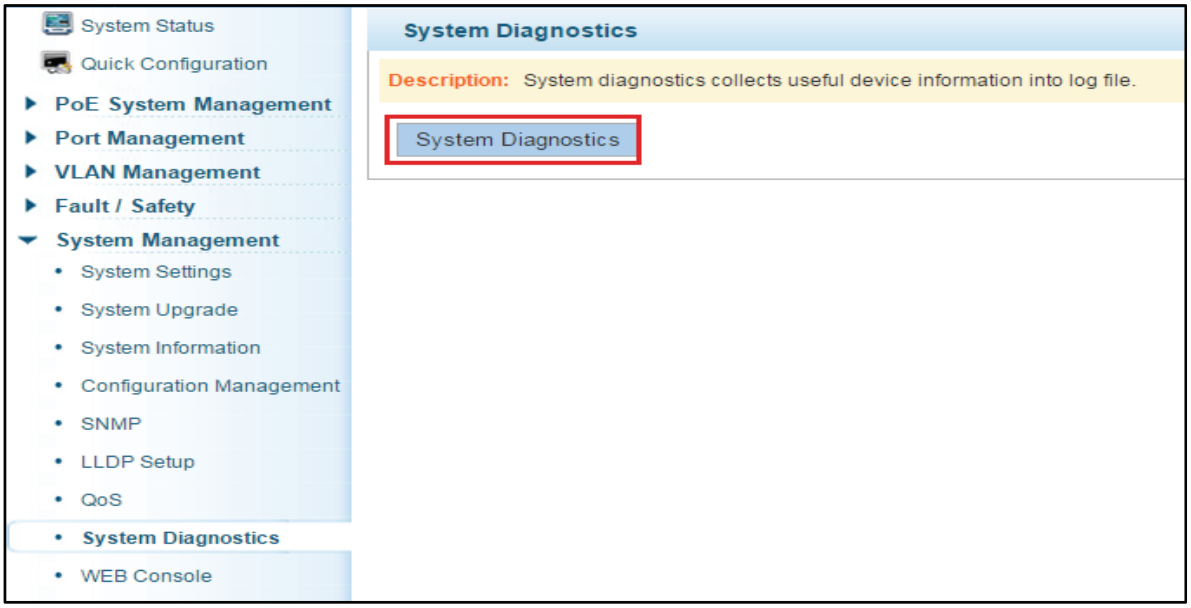


Figure 8-45: Key fault collection

8.8 THE WEB CONSOLE

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

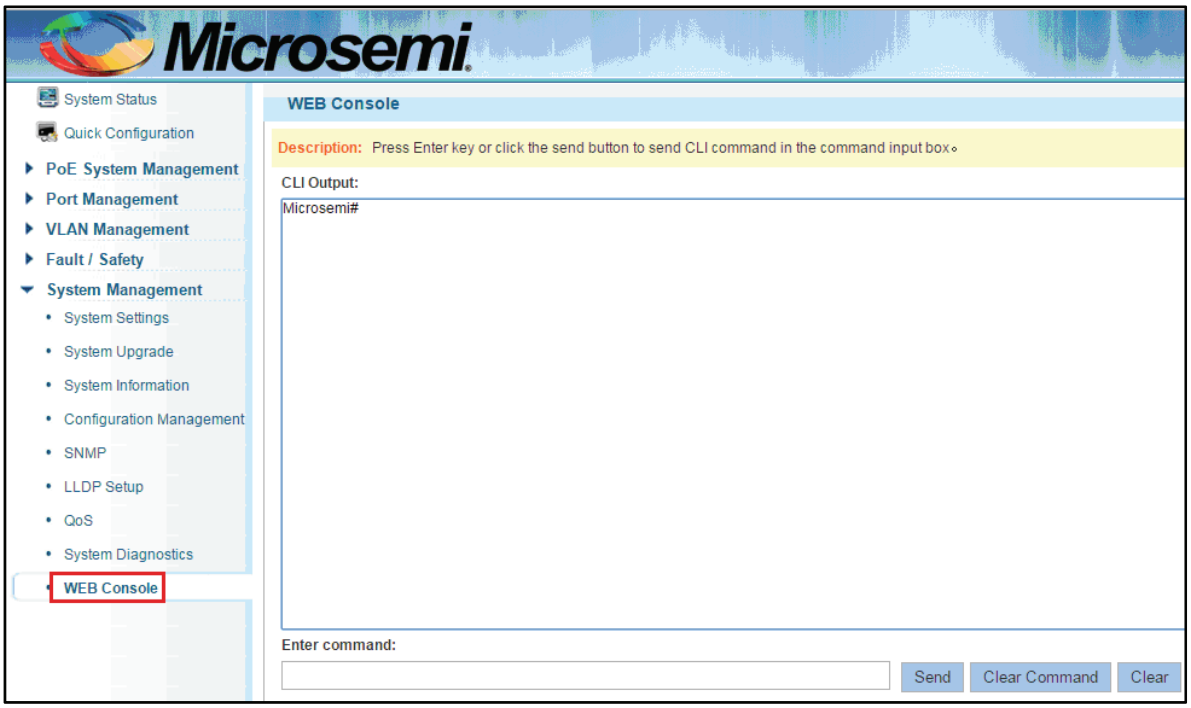


Figure 8-46: Web console

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

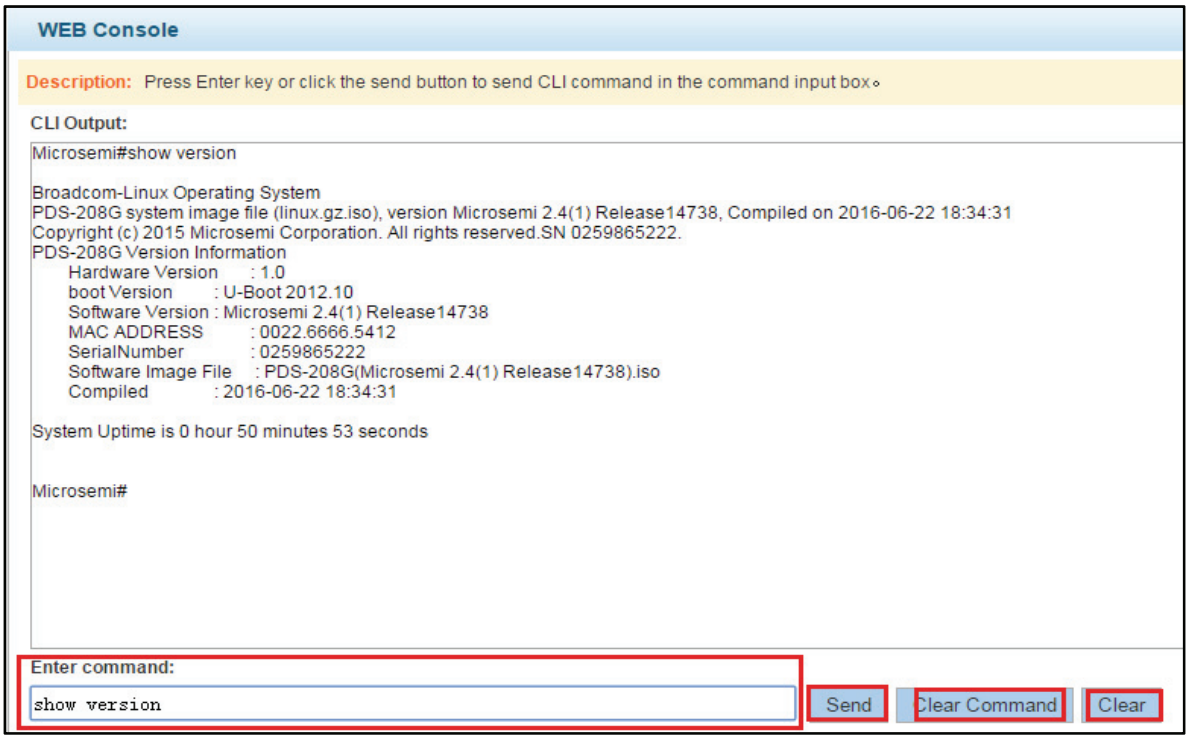


Figure 8-47: Web console operation

9 APPENDIX A: SWITCHES DEFAULT CONFIGURATION

Table 9-1 make a list of some important switch the default configuration information, for your reference.

Configuration items		The default configuration
System	The user name/password	admin/password
	IP address	IP address：192.168.0.50 Subnet mask：255.255.255.0
	A serial port baud rate	115200
	MAC address aging time	300secs
	Equipment host name	Microsemi
PORT	Port state	The activation
	Port rate	Automatic negotiation
	Port duplex mode	Automatic negotiation
	Link Aggregation	Not configured
	Port broadcast storm	Disable
	The port working mode	Access
	NATIVE VLAN	1
Shut down VLAN	The management VLAN	VLAN 1
	VLAN function mode	802.1Q
IGMP Snooping	Global IGMP Snooping function	Disable

10 APPENDIX B: SWITCH TERMS

Term	English	Statement
1000Base-T		1000Mbit/s Ethernet base band standard, with 4 pair five kind UTP for connection ,transmission speed up to 1000Mbit/s
100Base-T		100Mbit/s Ethernet base band standard, with 2 pair five kind UTP for connection ,The maximum transmission speed is 100Mbit/s
10Base-T		10Mbit/s Ethernet base band standard, with 2 pair UTP(3/4/5 kind) for connection ,The maximum transmission speed is 10Mbit/s
Auto	Auto-Negotiation	Make the switch device to negotiate work efficiency and full duplex mode in best performance automatic
ARP	Address Resolution Protocol	To the network layer IP address resolution for the physical address of the data link layer
BPDU	Bridge Protocol Data Unit	STP delivering bpdus between devices to determine the topology of the network.BPDU contains enough information to ensure that equipment to complete the calculation process of spanning tree
Broadcast		Refers to broadcast packets in the IP subnet, all within the subnet host will receive these messages
Full Duplex		Full duplex refers to receive and send data using two independent channels, but at the same time, each other
Half Duplex		Half duplex is refers to the sending and receiving Shared a channel, the same time can only be sent or received, so half duplex may lead to conflict
HTTP	Hypertext Transfer Protocol	Hypertext transfer protocol defines how information is formatted, how is transmitted, as well as in various orders taken by the browser and server responses.IP between the host and and multicast router in the immediate vicinity of establishing and maintaining
IGMP	Internet Group Management Protocol	TCP/IP protocol family, be responsible for the management of IP multicast member agreement used in IP between the host and and multicast router in the immediate vicinity of establishing and maintaining multicast group membership

Term	English	Statement
IGMP Querier	Internet Group Management Protocol Querier	In running the IGMP multicast networks, there will be a three layer multicast device ACTS as the IGMP query, responsible for sending IGMP query message, make three layer multicast equipment can turn to establish and maintain in the network layer multicast published items, in normal forwarding network layer multicast data
IGMP-Snooping	Internet Group Management Protocol Snooping	Running on the layer 2 Ethernet switches multicast constraint mechanism, to manage and control group was part of the TCP/IP protocol in the complete set.Its main tasks, there are two: one is addressing, the second is management segmentation data
IP	Internet Protocol	Internet protocol is the open systems interconnection model (OSI model), one of the main agreement is part of the TCP/IP protocol in full.Its main tasks, there are two: one is addressing, the second is management segmentation data
LACP	Link Aggregation Control Protocol	An implementation link dynamic convergence and convergence of agreement.LACP Protocol by LACPDU (Link Aggregation Control Protocol Data Unit, Link together Control Protocol Data Unit) and mutual information to end
LAN	Local Area Network	Local area network (LAN) is located in the relatively limited area (for example, a building) within a group of computers, printers and other equipment to connect the communication network.LAN can allow any connected device and other devices on the interaction
PVID	Port VLAN ID	The default VLAN ID
SNMP	Simple Network Management Protocol	To ensure management information transmitted between any two points in a network, is advantageous for the network administrator of any node in the network retrieval information, modify information, locate fault, fault diagnosis, capacity planning and generate reports
STP	Spanning Tree Protocol	Formulated according to the association of the IEEE 802.1 D standard, physical loop is used to eliminate the data link layer in the local area network (LAN) protocol.To run the equipment of the agreement by interaction with each other, found in the network

Term	English	Statement
		message loop and have a choice to blocking of certain port, will eventually clip to form a loop loop network structure of tree network structure, so as to prevent the proliferation of in loop network message and an infinite loop, avoid the host by repeated receiving the same Cause of the decline of the message processing capacity of message
VLAN	Virtual Local Area Network	Virtual local area network (LAN) is a kind of through the equipment within the local area network (LAN) logically, not physically divided into small segments so as to realize the technology of virtual team
VID	VLAN ID	VLAN id

11 SAFETY INFORMATION

IMPORTANT SAFETY INFORMATION

-  Installation and removal of the PoE Media converter must be carried out by qualified personnel only.
- AC Power cord set:
  The power cord must have regulatory agency approval for the specific country in which it is used (i.e., UL, CSA, VDE, etc.).
- The power cord must be a three-conductor type (two current carrying conductors; one ground conductor) terminated on one end by an IEC 60320 appliance coupler (for connection to the PoE Media Converter), and on the other end by a plug containing a ground (earth) contact.
- The power cord must be rated for a minimum of 250Vac RMS operation, with a minimum rated current capacity of 5 amps (or a minimum wire gauge of 18 AWG (0.75mm2).

 PoE Media converters installed in Australia require power cords with a minimum wire gauge of 16 AWG (1.0 mm2).

 The "Data-In" PoE injector and "PoE" ports are shielded RJ45 data sockets. They cannot be used as Plain Old Telephone Service (POTS) telephone sockets. Only RJ45 data connectors may be connected to these sockets.

The AC wall socket-outlet must be near the PoE Media converter and easily accessible. You can remove AC power from the PoE Media converter by disconnecting the AC power cord from either the wall socket-outlet or the PoE media converter appliance coupler.

The PoE Media Converter Data-In and Data & Power Out interfaces are qualified as SELV (Safety Extra-Low Voltage) circuits according to IEC 60950-1. These interfaces can only be connected to SELV interfaces on other equipment.

WARNINGS!

- Read the installation instructions before connecting the PoE Media Converter to its power source.
- Follow basic electricity safety measures whenever connecting the PoE Media Converter to its power source.

-  A voltage mismatch can cause equipment damage and may pose a fire hazard. If the voltage indicated on the label is different from the power outlet voltage, do not connect the PoE Media converter to this power outlet.

RECYCLING AND DISPOSAL

Disposal instructions for old products. The WEEE (Waste Electrical and Electronic Equipment) national environmental initiatives has been put in place to ensure that products are recycled using best available treatment, recovery and recycling techniques to ensure human health and high environmental protection. Your product is designed and manufactured with high quality materials and components, which can be recycled and reused. Do not dispose of your old product in your general household waste bin. Inform yourself about the local separate collection system for electrical and electronic products marked by this symbol:

Use one of the following disposal options:

1. Dispose of the complete product (including its cables, plugs and accessories) in the designated WEEE collection facilities.
2. If you purchase a replacement product, hand your complete old product back to the retailer. He should accept it as required by the national WEEE legislation.