PS5026G-2GS-24PoE
Managed Full Gigabit
Industrial Ethernet PoE Switch

User Manual

Version 1.0, 2017.8.29

Table of Contents

Chapter 1 Product Introduction

Congratulations on your purchasing of the Web Smart Ethernet Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1 Product Overview

This is a new generation designed for high security and high performance network the second layer Switch. Provides twenty-four 10/100/1000Mbps self-adaption RJ-45 port, and two 100/1000Mbps SFP optical ports, all ports support wire-speed forwarding, can provide you with larger network flexibility. Support VLAN ACL based on port, easily implement network monitoring, traffic regulation, priority tag and traffic control. Support traditional STP/RSTP/MSTP 2 link protection technology; greatly improve the ability of fault tolerance, redundancy backup to ensure the stable operation of the network. Support ACL control based on the time, easy control the access time accurately. Support 802.1x authentication based on the port and MAC, easily set user access. Perfect QOS strategy and plenty of VLAN function, easy to maintenance and management, meet the networking and access requirements of small and medium-sized enterprises, intelligent village, hotel, office network and campus network.
This Switch 24 ports support POE power supply function, support IEEE802.3at standard, 802.3af downward compatibility, power supply equipment for Ethernet, can automatically detect identification standard of electrical equipment, and through the cable for the power supply.

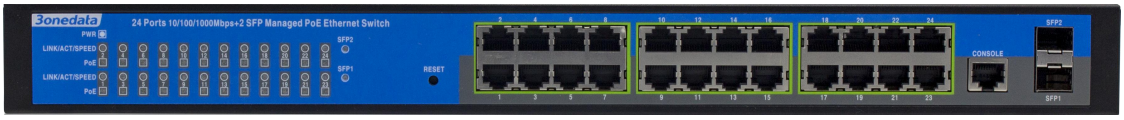
1.2 Features

- Comply with IEEE 802.3i, IEEE 802.3u, IEEE802.3x, IEEE802.3ab, IEEE802.1q, IEEE802.1p standards
- Supports IEEE802.3af, IEEE802.3at standards
- Supports PoE power up to 30W for each PoE port, all power up to 380W
- Supports manage the POE port, support POE port power on/off and port output power restriction
- Support Web interface management
- 24 x 10/100/1000Mbps Auto MDI/MDI-X Ethernet port,Support ports Auto MDI/MDIX
- 8K entry MAC address table of the Switch with auto-learning and auto-aging
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- supports QoS (quality of service), port mirror, Link aggregation protocol
- Support packet length 9216Bytes jumbo frame packet forwarding at wire speed
- LED indicators for monitoring PSE, Link / Activity/Speed

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of 24 x 10/100/1000Mbps RJ-45 ports, 2 x 1000Mbps SFP ports, 1 x CONSOLE port, 1 x RESET button and a series of LED indicators as shown as below.



10/100/1000Mbps RJ-45 ports (1~24):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

SFP ports (SFP1, SFP2):

Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

CONSOLE port (CONSOLE):

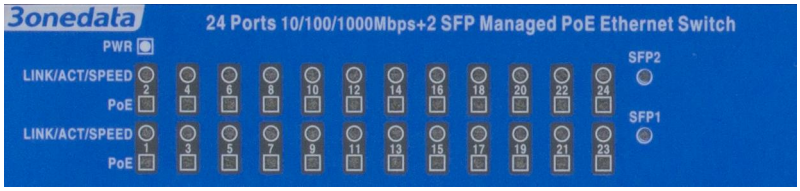
Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

RESET button (RESET):

Keep the device powered on and press down the button for about 5 seconds. The system restores the factory default settings.

LED indicators:

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.



The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Red	On	Power On
		Off	Power Off
LINK/ACT	Orange	On	A device is connected to the port

/SPEED (1~24)	(10/100Mbps)	Off	A device is disconnected to the port
	Green (1000Mbps)	Flashing	Sending or receiving data
LINK/ACT /SPEED (SFP1,2)	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data
PoE (1~24)	Yellow	On	A Powered Device is connected to the port, which supply power successfully.
		Off	No Powered Device connected to the port, or no power is supplied according to the power limits of the port.
		Flashing	The PoE power circuit may be in short or the power current may be overloaded.

1.3.2 Rear Panel

The rear panel of the Switch contains AC power connector and one marker shown as below.

AC Power Connector:
Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

Grounding Terminal:
The Switch already comes with Lightning Protection Mechanism. You can also ground the Switch through the PE (Protecting Earth) cable of AC cord or with Ground Cable.

1.4 Environment

- Operating Temperature: 0℃~45℃
- Storage Temperature: -40℃~70℃
- Operating Humidity: 10%~90% non-condensing
- Storage humidity: 5%~90% non-condensing

1.5 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One PoE Managed Ethernet Switch
- Four rubber feet, two mounting ears and eights screws
- One AC power cord
- One User Manual

Chapter 2 Installing and Connecting the Switch

This part describes how to install your Web Smart Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1 Desktop Installation

Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

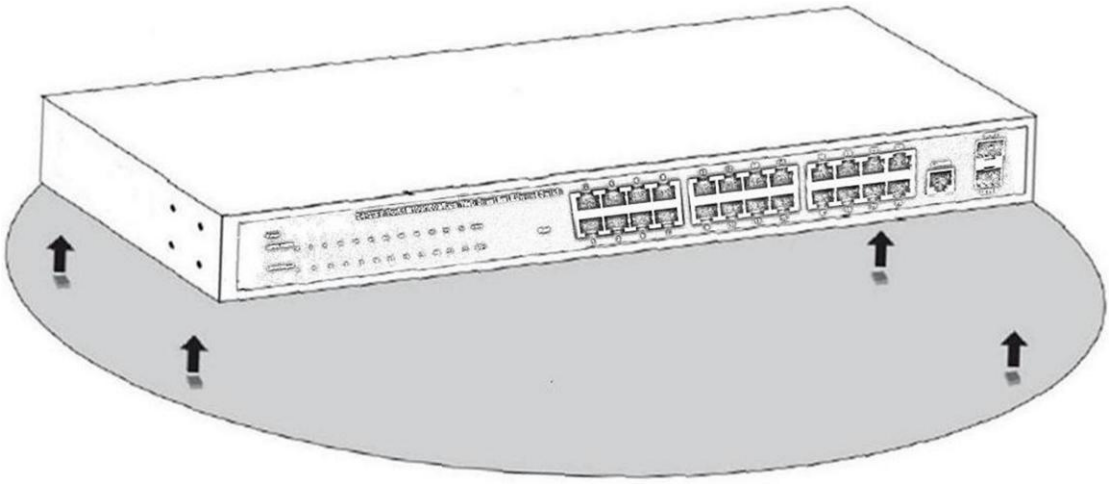


Figure 4 - Desktop Installation

2.1.2 Rack-mountable Installation in 19-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

a. attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

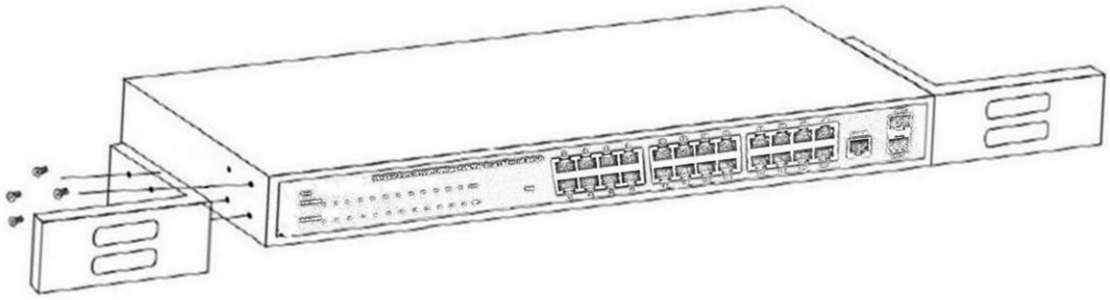


Figure 5 - Bracket Installation

b. use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

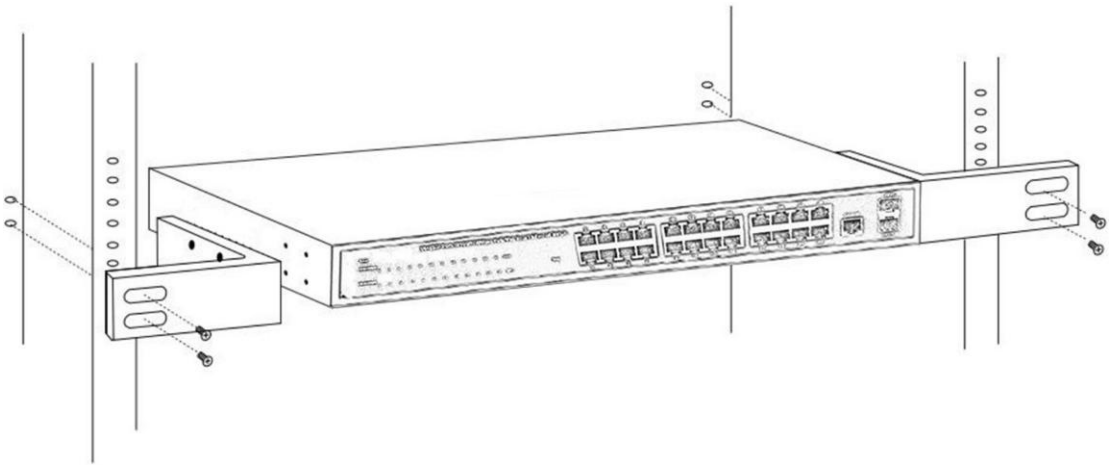


Figure 6 - Rack Installation

2.1.3 Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2 Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

Chapter 3 How to Login the Switch

3.1 How to Login the Switch

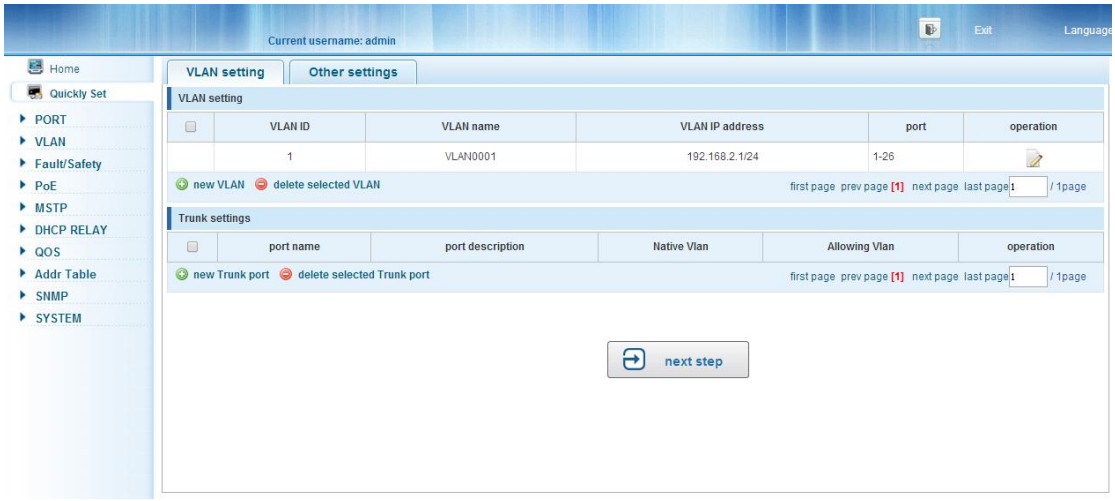
As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.2.1
Default Username	admin
Default Password	admin

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" ranges 2~254), for example, 192.168.2.100.
4. Open the browser, and enter http://192.168.2.1 and then press "Enter". The Switch login window appears, the following picture:

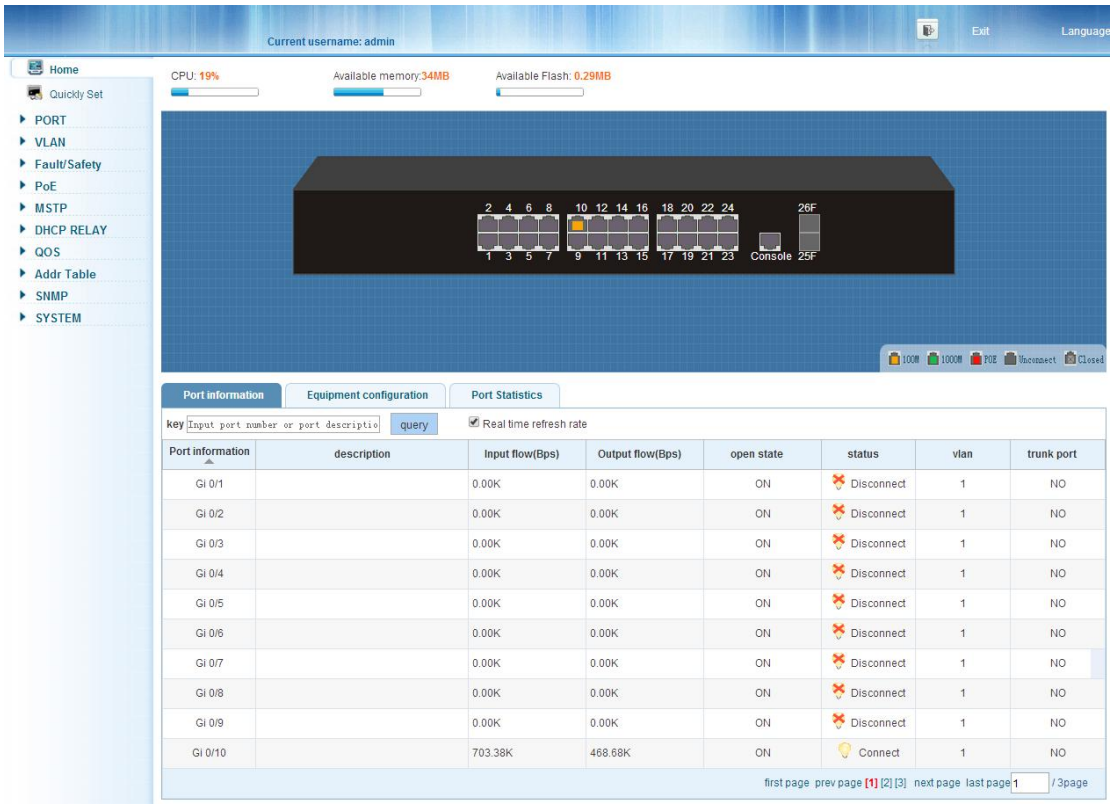
5. Enter the user name and password (factory default user name admin, password for admin) and can choose the English interface, and then click "login", you can log in to the following switch configuration window.


Current username: admin
Exit
Language
Home
Quickly Set
PORT
VLAN
Fault/Safety
PoE
MSTP
DHCP RELAY
QOS
Addr Table
SNMP
SYSTEM
VLAN setting
Other settings
VLAN setting
VLAN ID
VLAN name
VLAN IP address
port
operation
1
VLAN0001
192.168.2.1/24
1-26
new VLAN
delete selected VLAN
first page prev page [1] next page last page 1 / 1page
Trunk settings
port name
port description
Native Vlan
Allowing Vlan
operation
new Trunk port
delete selected Trunk port
first page prev page [1] next page last page 1 / 1page
next step

Chapter 4 Switch Configuration

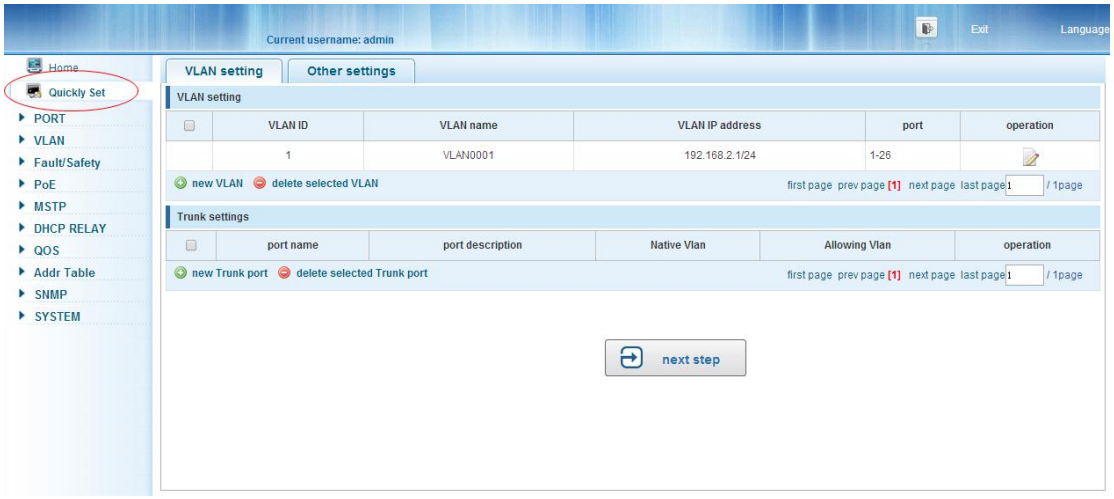
This Switch Managed switch software provides rich layer 2 functionality for switches in your networks. This chapter describes how to use Web-based management interface(Web UI) to this switch configure managed switch software features.

In the Web UI, the left column shows the configuration menu. Above you can see the information for switch system, such as memory. The middle shows the switch's current link status. Green squares indicate the port link is up, while gray squares indicate the port link is down. The rest of the screen area displays the configuration settings.



4.1 Quickly Set

In the navigation bar to select **"Quickly Set"**, can create a VLAN in this module, add the port in the VLAN, set the basic information and modify the switch login password as shown.



【Parameter Description】

Parameter	Description
VLAN ID	VLAN number, 26GE default VLAN 1
VLAN name	VLAN mark
Manage IP	Manage the IP address of the VLAN

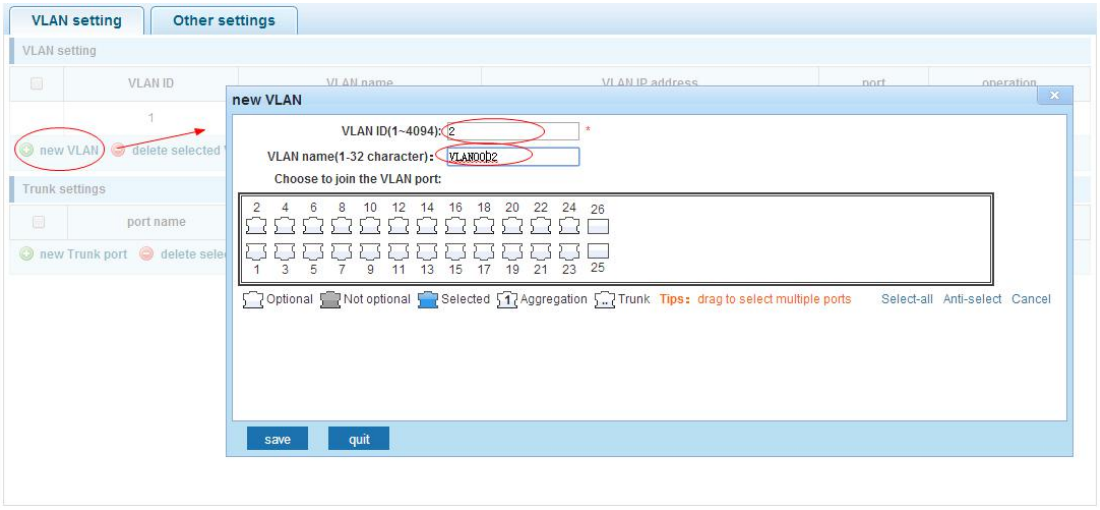
【Instructions】

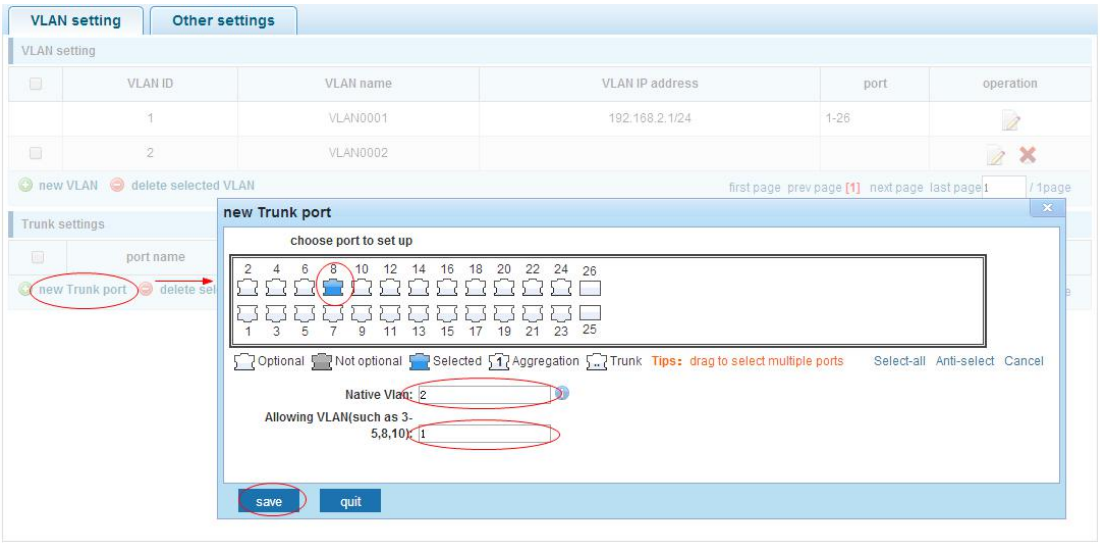
Native VLAN: As a Trunk, the port will belong to a Native VLAN. The so-called Native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

Allowed VLAN list: A Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the port of the list to limit the flow of some VLAN can't through the Trunk.

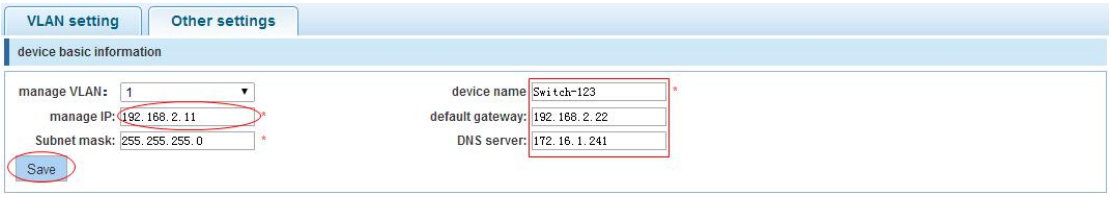
【Configuration Example】

VLAN setting: Such as create VLAN 2, Sets the port 8 to Trunk, Native VLAN 2.

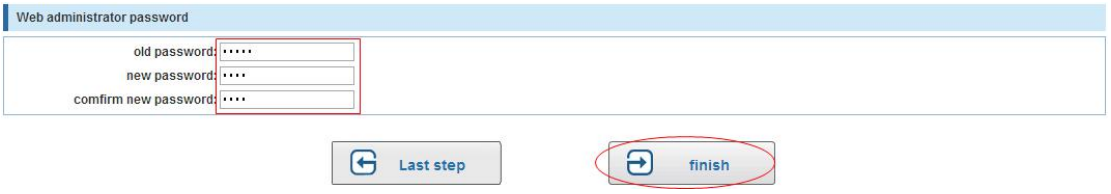




Click "next step" button, into other settings, such as: Manage IP address set as 192.168.2.11, device name set as Switch-123, Default gateway set as 192.168.2.22, DNS server set as 172.16.1.241.

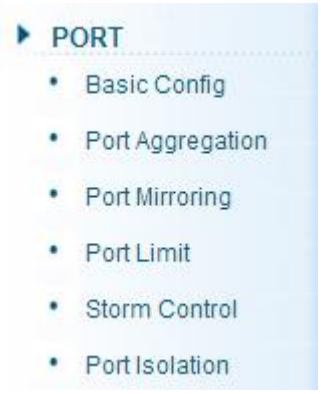


Use 192.168.2.11 to log in, set a new password for 1234.



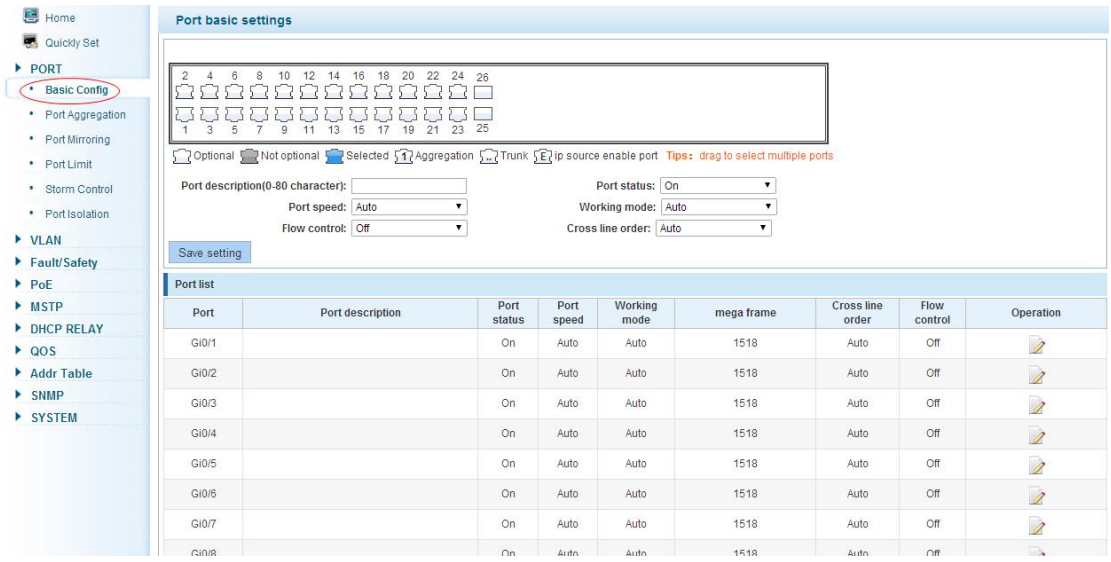
4.2 PORT

In the navigation bar to select **"PORT"**, You may conduct **Basic Config**, **Port Aggregation**, **Port Mirroring**, **Port Limit**, **Storm Control** and **Port Isolation**.



4.2.1 Basic Config

In the navigation bar to select **"Port>Basic Config"**, for panel port to port described, port speed, port status, working mode, flow control, cross line order configuration as shown.



【Parameter Descriptionion】

Parameter	Description
Port	Select the current configuration port number
Port status	Open or close ports
Flow control	Open or close the port flow control function

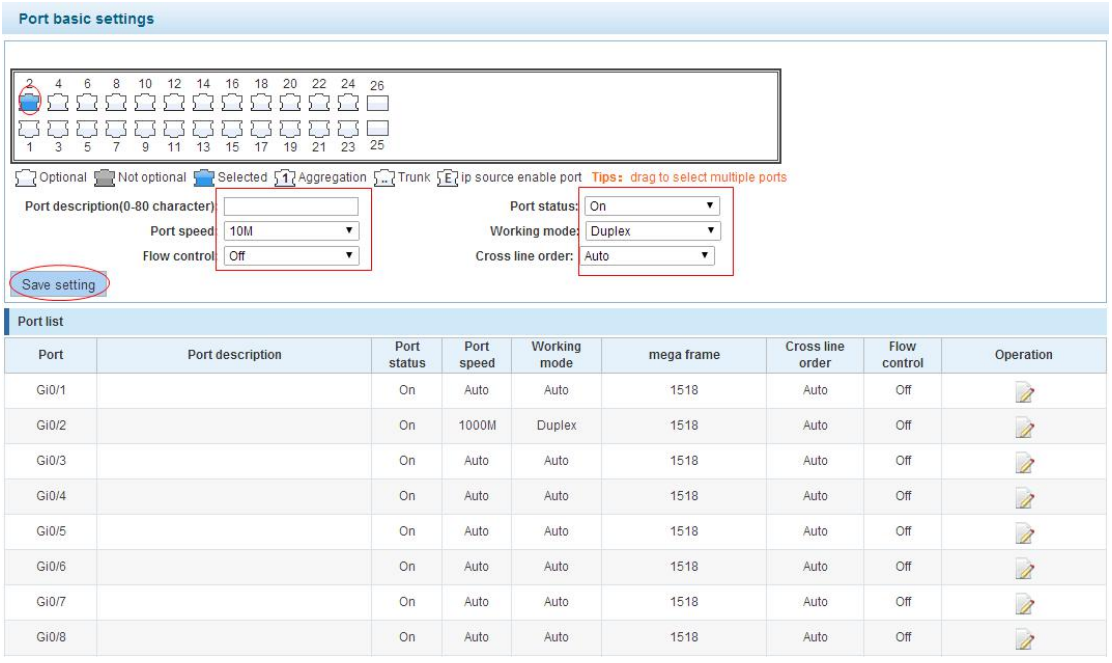
Port speed	Can choose the following kinds: Self negotiated 10M 100M 1000M
Working mode	Can choose the following kinds: Self negotiated Half duplex Duplex
Port described	The port is described
Cross line sequence	Whether open intersection line sequence

【Instructions】

Open flow control should be negotiated will close, negotiated close is to set port speed rate and working mode; Set the port rate more than actual rate of port, the port will be up.

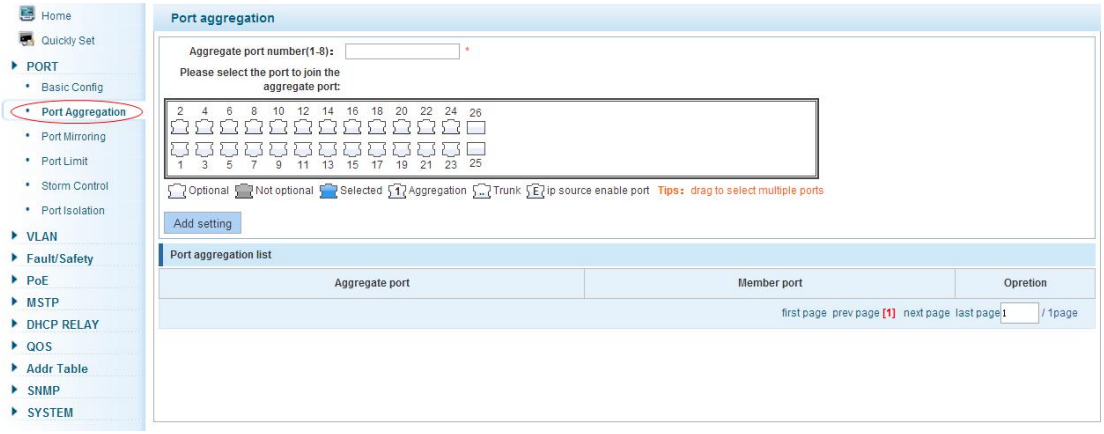
【Configuration Example】

Such as: The port is set to 10M, Duplex,cross line sequence set to Auto, open flow control and port state.



4.2.2 Port Aggregation

In the navigation bar to select **"Port>Port Aggregation",** in order to expand the port bandwidth or achieve the bandwidth of the redundancy backup as shown.

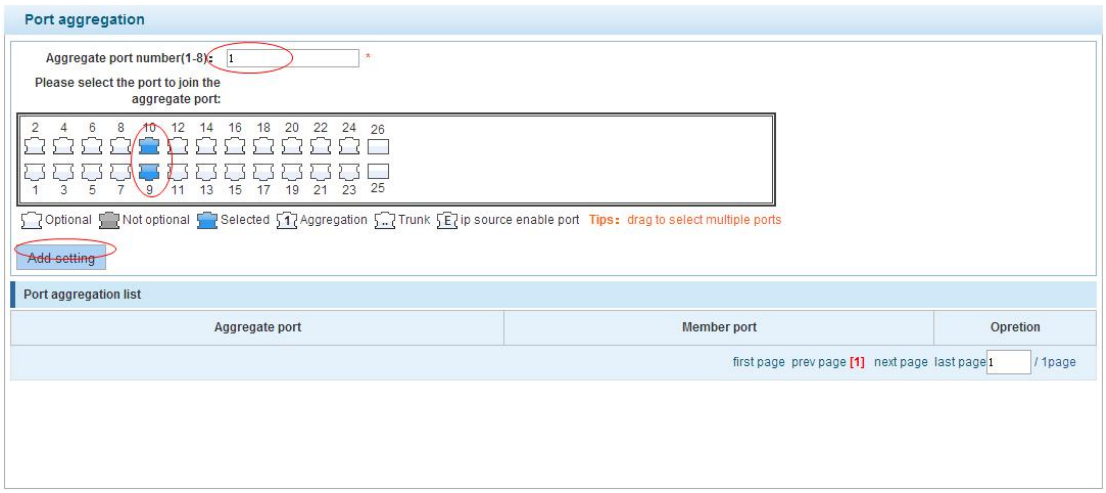


【Instructions】

The monitor port in the port image can not be added!

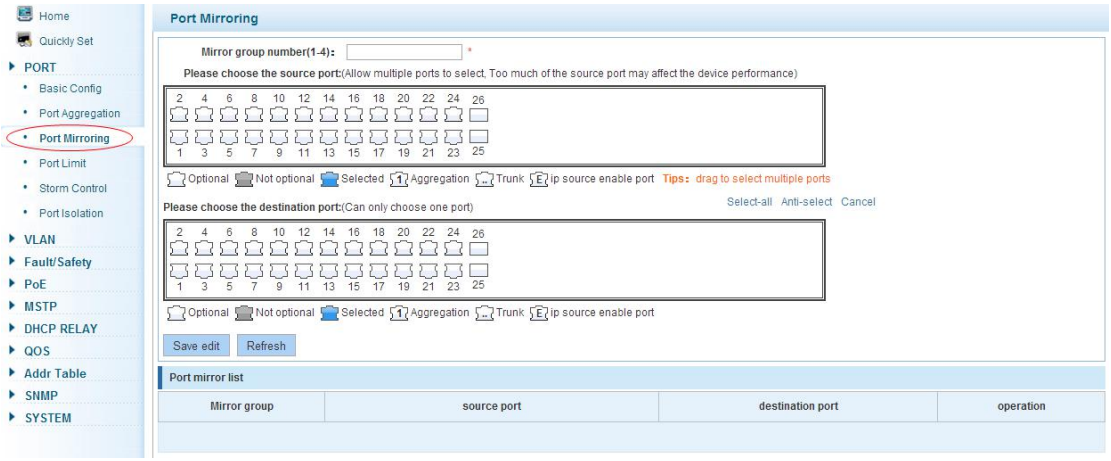
【Configuration Example】

Such as: Set the port 9, 10, for aggregation port 1, lets this aggregation port 1 connected to other switch aggregation port 1 to build switch links.



4.2.3 Port Mirroring

In the navigation bar to select **"Port>Port Mirroring"**, open port mirror feature, all packets on the source port are copied and forwarded to the destination port, destination port is usually connected to a packet analyzer to analyze the source port, multiple ports can be mirrored to a destination port as shown.



【Parameter Description】

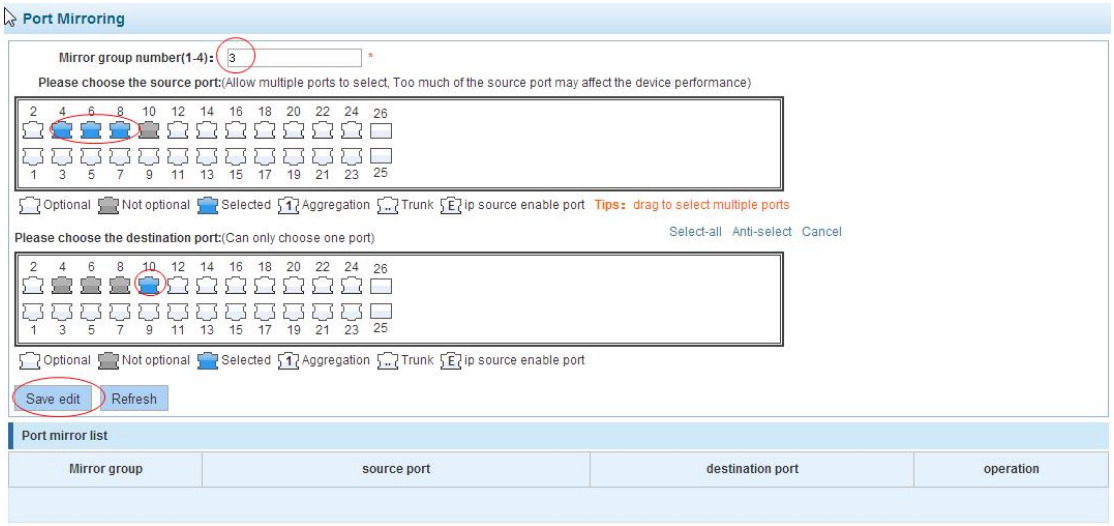
Parameter	Description
Mirror group	Range: 1-4
Source port	To monitor the port in and out of flow
Destination port	Set destination port, All packets on the source port are copied and forwarded to the destination port

【Instructions】

The port of the aggregate port can not be used as a destination port and the source port, destination port and source port can not be the same.

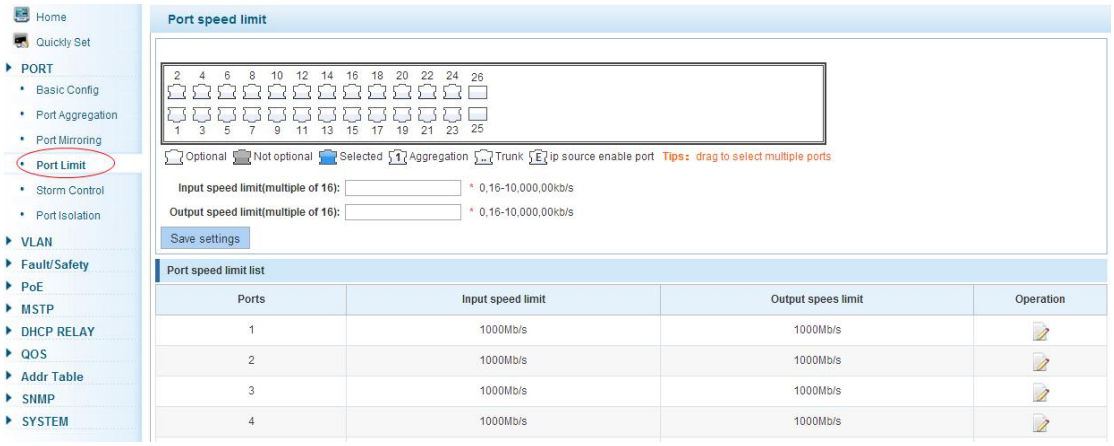
【Configuration Example】

Such as: Set a mirror group for port 10 regulatory port 4, 6, 8 on and out flow conditions.



4.2.4 Port Limit

In the navigation bar to select **"Port>Port Limit "**, to port output, input speed limit as shown.



【Parameter Description】

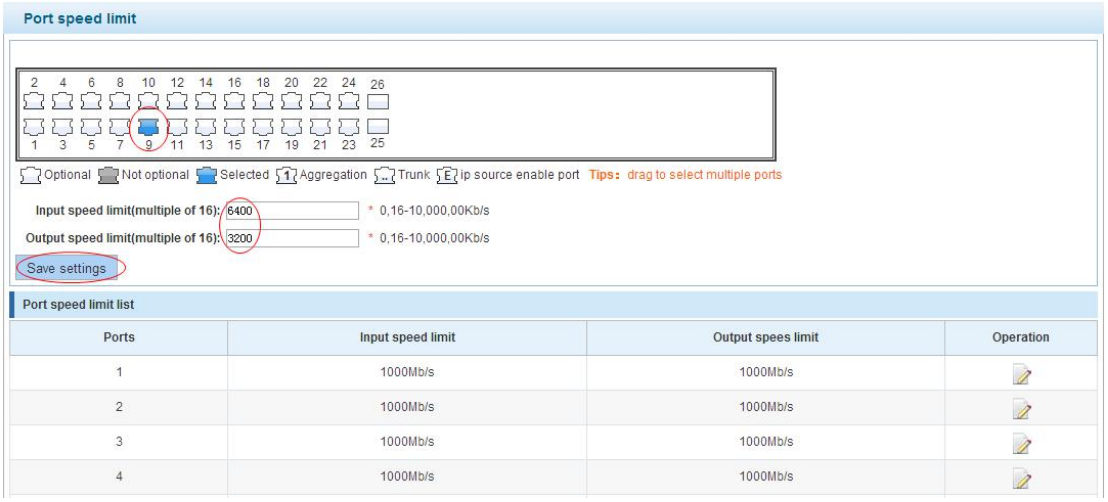
Parameter	Description
Input speed limit	Set port input speed
Output speed limit	Set port output speed

【Instructions】

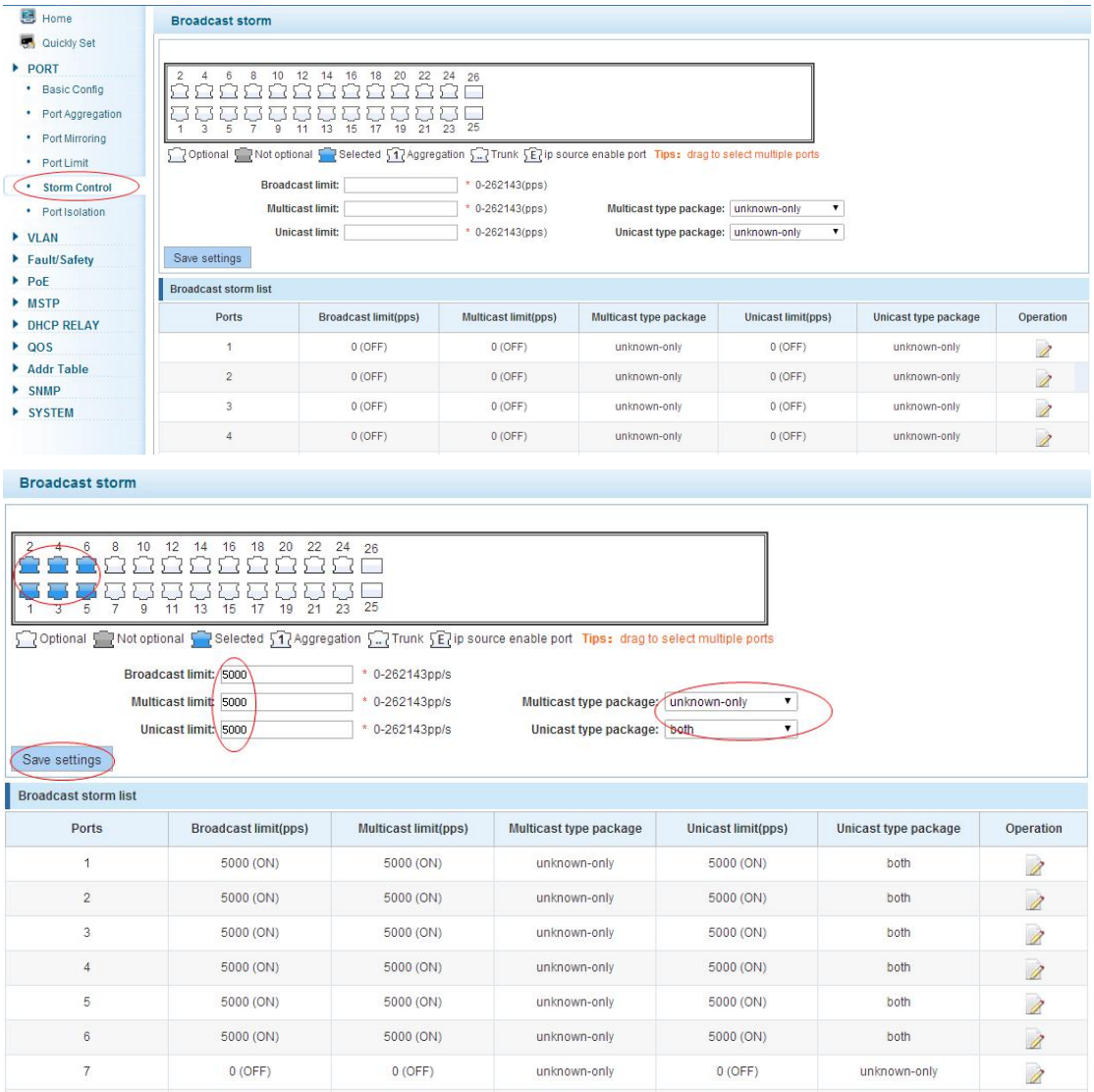
1Mbit/s=1000Kbit/s=1000/8KB/s=125KB/s. That is, the theoretical rate of 1M bandwidth is 125KB/s.

【Configuration Example】

Such as: The port 9 input rate is set to 6400KB/s, the output rate is set to 3200KB/s.



4.2.5 Storm Control

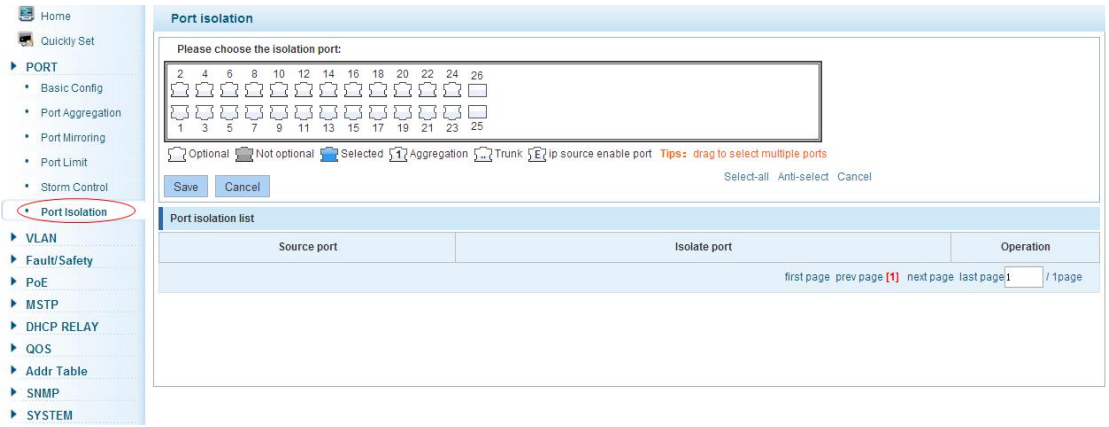


Broadcast storm list

Ports	Broadcast limit(pps)	Multicast limit(pps)	Multicast type package	Unicast limit(pps)	Unicast type package	Operation
1	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
2	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
3	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
4	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
5	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
6	5000 (ON)	5000 (ON)	unknown-only	5000 (ON)	both	
7	0 (OFF)	0 (OFF)	unknown-only	0 (OFF)	unknown-only	

4.2.6 Port Isolation

In the navigation bar to select **"Port>Port Isolation"**, one port can be isolated to one or multiple destination ports as shown.

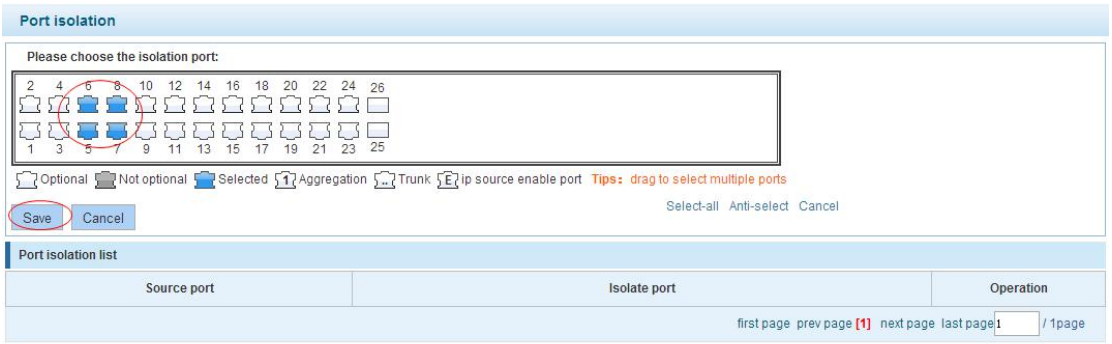


【Parameter Description】

Parameter	Description
Source port	Choose a port, to configure the isolated port
Isolated port	Port will be isolated

【Configuration Example】

Such as: Isolate port 5,6,7,8 port separately.



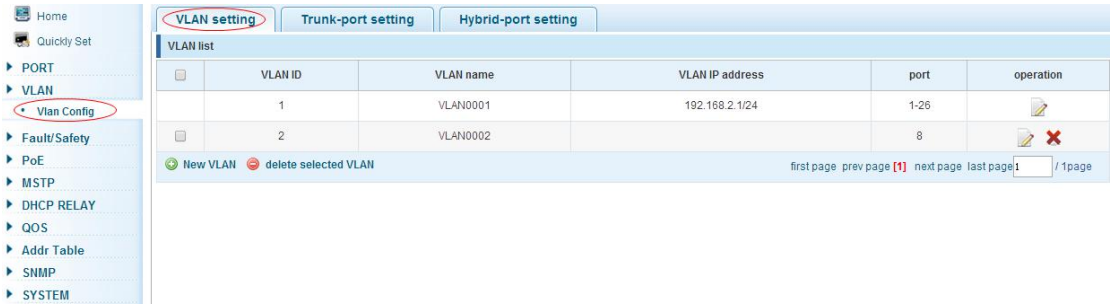
Configuration success after, Isolate port 5,6,7,8 port separately.

4.3 VLAN

In the navigation bar to select **"VLAN"**. You can manage the **VLAN setting, Trunk-port Setting** and **Hybrid-port Setting** as shown.

4.3.1 VLAN setting

In the navigation bar to select **"VLAN>VLAN Config>VLAN setting"**, VLANs can be created and set the port to the VLAN(port default state for the access mode) as shown.



【Parameter Description】

Parameter	Description
VLAN ID	VLAN number, 26GE default VLAN 1
VLAN name	VLAN mark
VLAN IP address	Manage switch ip address

【Instructions】

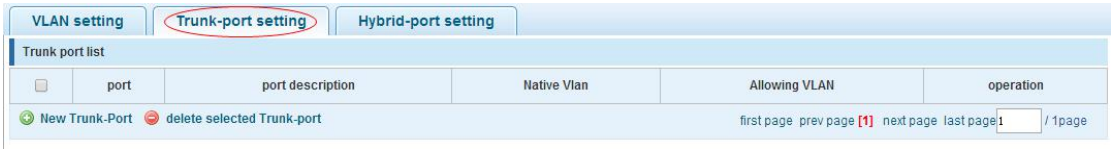
Management VLAN, the default VLAN cannot be deleted. Add ports to access port, port access mode can only be a member of the VLAN.

【Configuration Example】

Such as: Connect switches pc1, pc2 couldn't ping each other, will be one of the PC connection port belongs to a VLAN 2.

4.3.2 Trunk-port setting

In the navigation bar to select **"VLAN>VLAN Config>Trunk-port setting"**, can set port to Trunk port as shown.



【Parameter Description】

Parameter	Description
Native VLAN	Only set one
Allowing VLAN	Can set up multiple

【Instructions】

Native VLAN: As a Trunk, the port will belong to a Native VLAN. The so-called Native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

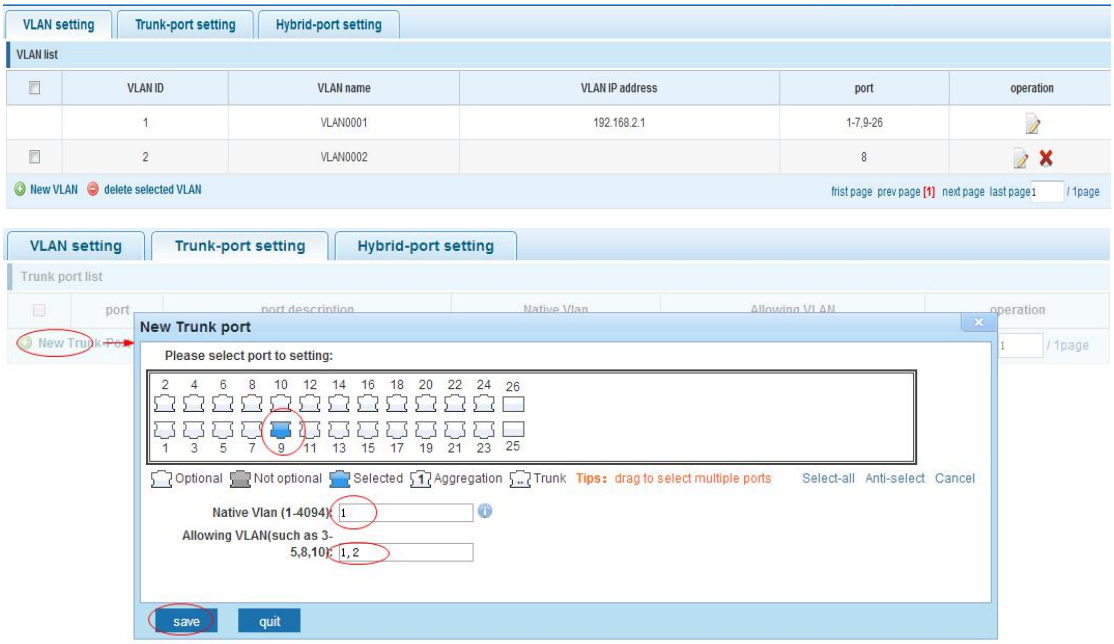
Allowed VLAN list: A Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the port of the list to limit the flow of some VLAN can't through the Trunk.

【Configuration Example】

Such as: PVID=VLAN2.

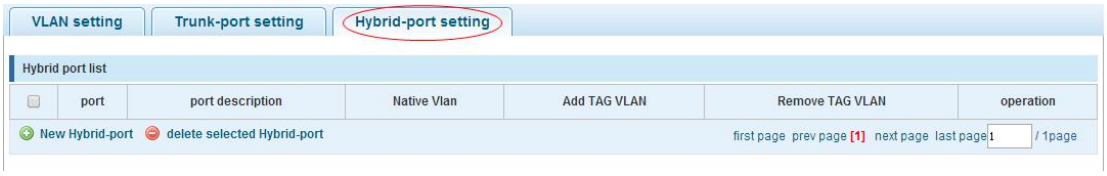
PC1: 192.168.2.122, port 8, access VLAN2.

PC2: 192.168.2.123, port 9, Trunk allowed VLAN 1-2.
PC3: 192.168.2.124, port 10, access VLAN1 (The default port belongs to VLAN1).
Can let the PC2 PING PC1, cannot PING PC3.



4.3.3 Hybrid-port setting

In the navigation bar to select **"VLAN>VLAN Config>Hybrid-port setting",** can set the port to take the tag and without the tag as shown.



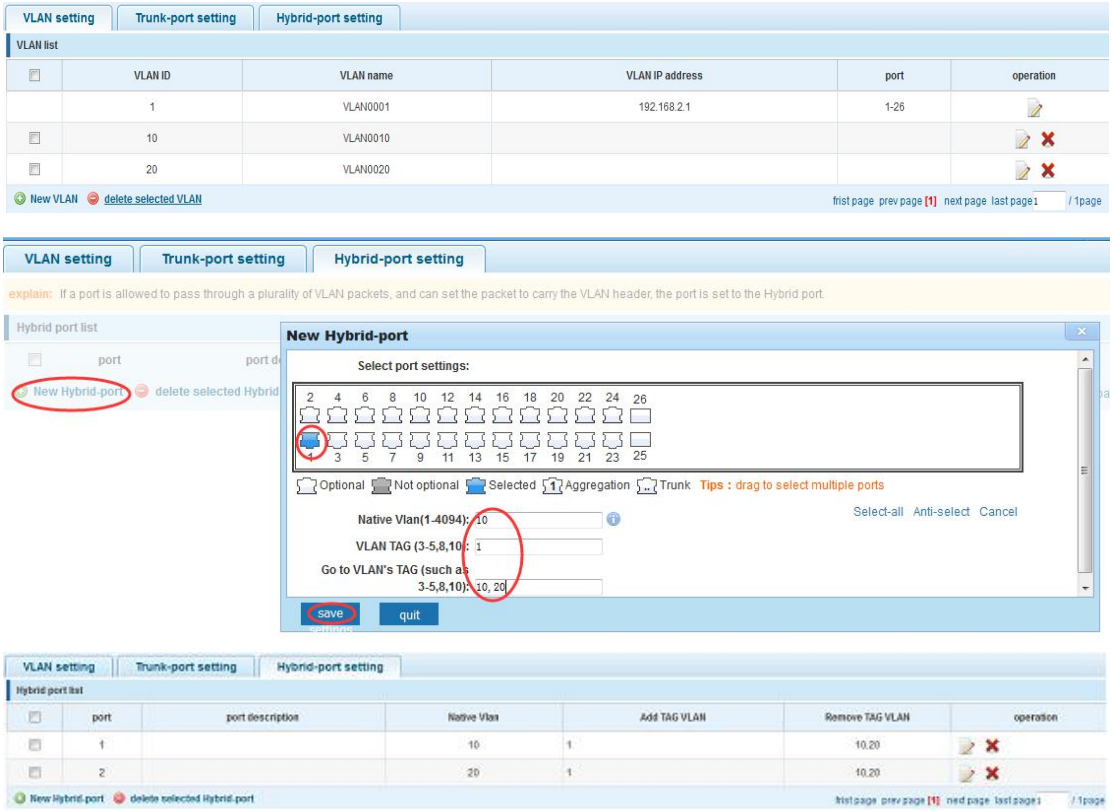
【Instructions】

Hybrid port to packet: Receives a packet, judge whether there is a VLAN information, if there is no play in port PVID, exchanged and forwarding, if have, whether the Hybrid port allows the VLAN data into, if can be forwarded, or discarded (untag on port configuration is not considered, untag configuration only work when to send it a message).
Hybrid port to send packet:
1. Determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag).
2. If it is untag stripping VLAN information, send again, if the tag is sent directly.

【Configuration Example】

Such as: Create VLANs 10, 20, VLAN sets the Native VLAN port 1 to 10, to tag VLAN for

10, 20, sets the Native VLAN port 2 to 20, to tag VLAN for 10, 20.



This system e0/1 and the receive system e0/2 PC can be exchanged, but when each data taken from a VLAN is different.

Data from the pc1, by inter0/1 pvid VLAN10 encapsulation VLAN10 labeled into switches, switch found system e0/2 allows 10 data through the VLAN, so the data is forwarded to the system e0/2, because the system e0/2 VLAN is untagged 10, then switches at this time to remove packet VLAN10 tag, in the form of ordinary package sent to pc2, pc1 -> p2 is VLAN10 walking at this time.

Again to analyze pc2 gave pc1 package process, data from the pc2, by inter0/2 pvid VLAN20 encapsulation VLAN20 labeled into switch, switch found system e0/1 allows VLAN by 20 data, so the data is forwarded to the system e0/1, because the system e0/1 on the VLAN is untagged 20, then switches remove packets on VLAN20 tag at this time, in the form of ordinary package sent to pc1, pc2 at this time -> pc1 is VLAN 20.

4.4 Fault/Safety

In the navigation bar to select **"Fault/Safety"**, you can set **Anti Attack, Channel Detection** and **ACL** configuration.

4.4.1 Anti Attack

4.4.1.1 DHCP

In the navigation bar to select **"fault/safety>Anti Attack>Anti DHCP Attack"**, open the DHCP anti-attack function, intercepting counterfeit DHCP server and address depletion attack packets ban kangaroo DHCP server as shown.

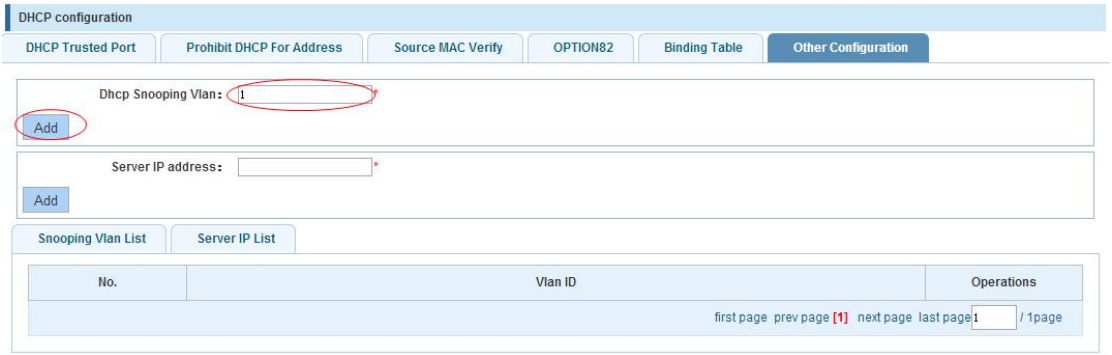
【Instructions】

DHCP trusted port configuration, select the port as a trusted port. Prohibit DHCP for address, select the port and save, you can disable this feature for the port.
Open DHCP attack prevention function, need to set the DHCP protective VLAN simultaneously, other functions to take effect.

【Configuration Example】

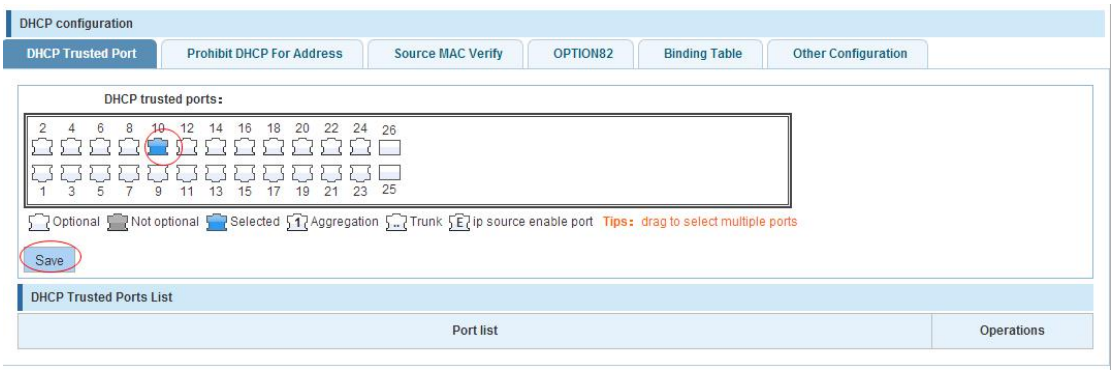
Such as: 1. DHCP snooping open.

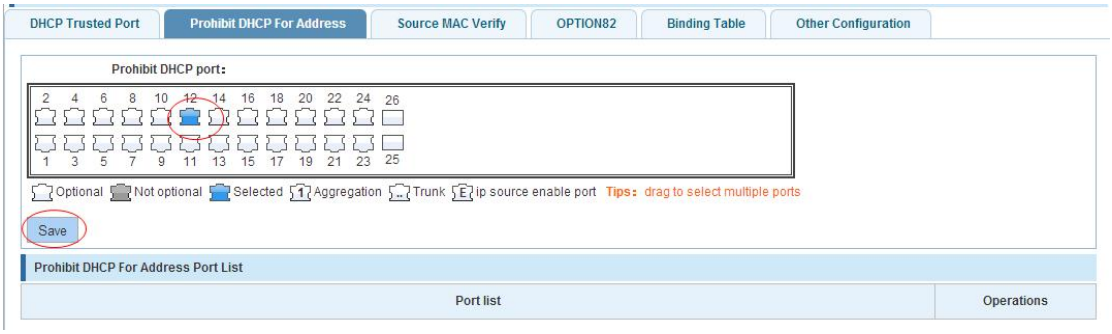
2. Setting DHCP snooping VLAN.



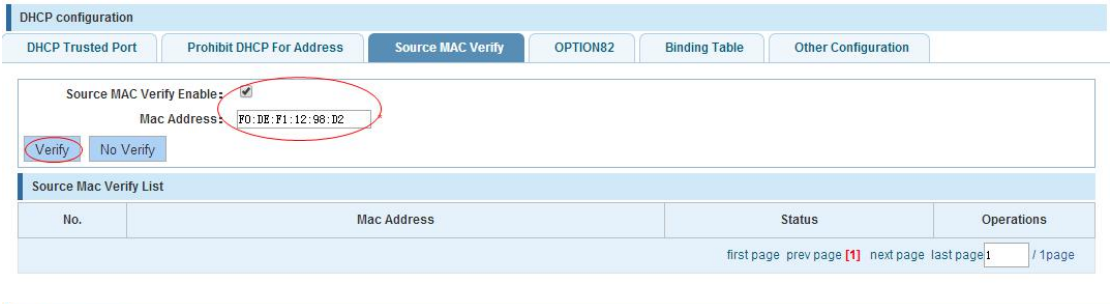
3.

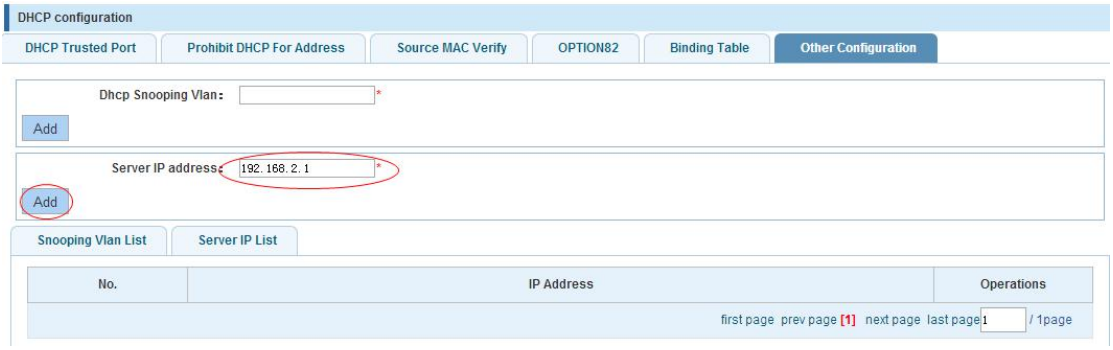
Set the connection router 10 ports for trust, then 6 port is set to the prohibit.



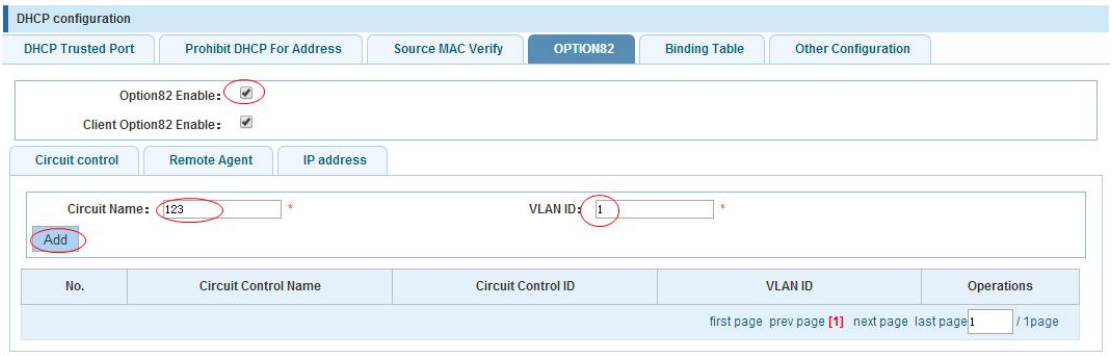


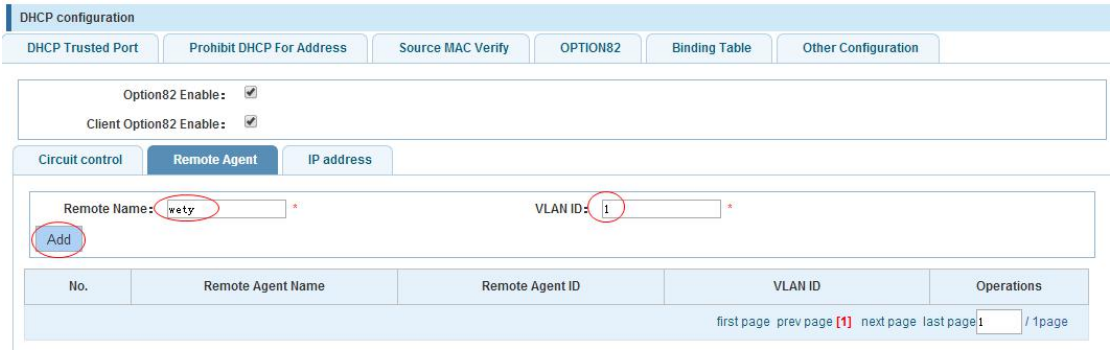
3. Verify source mac F0: DE: F1: 12: 98: D2, set server IP address to 192.168.2.1.

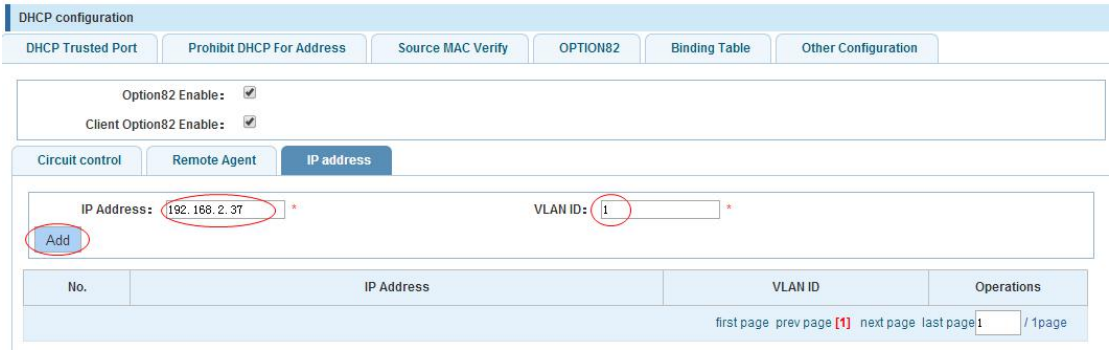




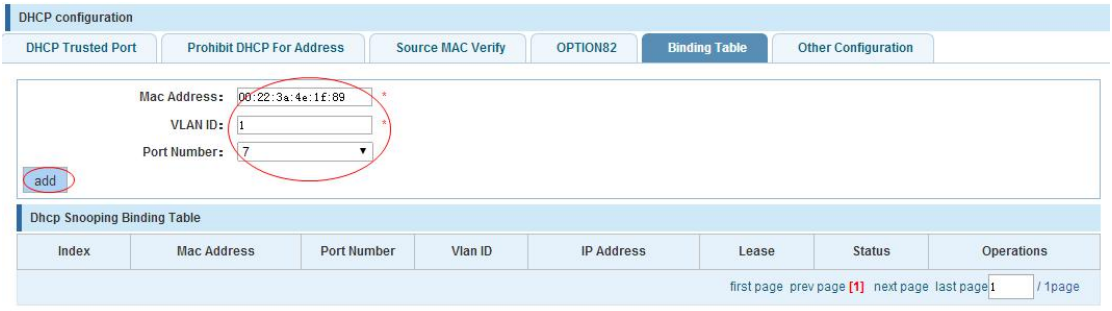
4. Set option82 information.





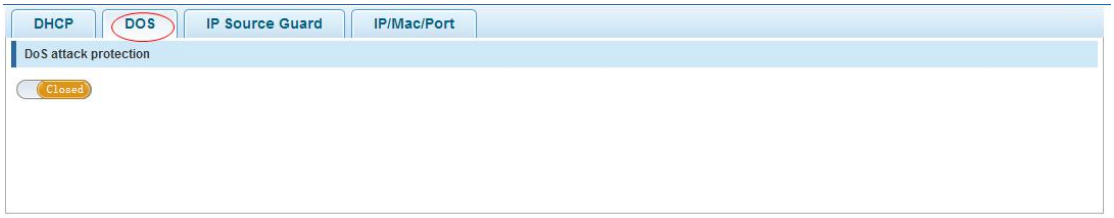


5. The port 7 for binding.



4.4.1.2 DOS

In the navigation bar to select **"Fault/Safety>Anti Attack>Anti DOS"**, open the anti DOS attack function, intercept land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users as shown.



【Instructions】

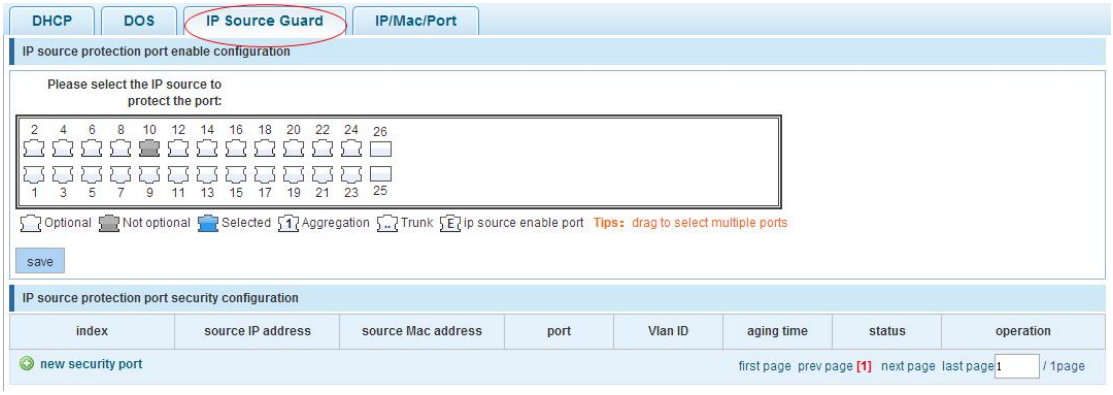
Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users.

【Configuration Example】

Such as: Open the anti DOS attack function.

4.4.1.3 IP Source Guard

In the navigation bar to select **"Fault/Safety>Anti Attack>IP Source Guard"**, through the source port security is enabled, on port forwarding the packet filter control, prevent illegal message through the port, thereby limiting the illegal use of network resources, improve the safety of the port as shown.

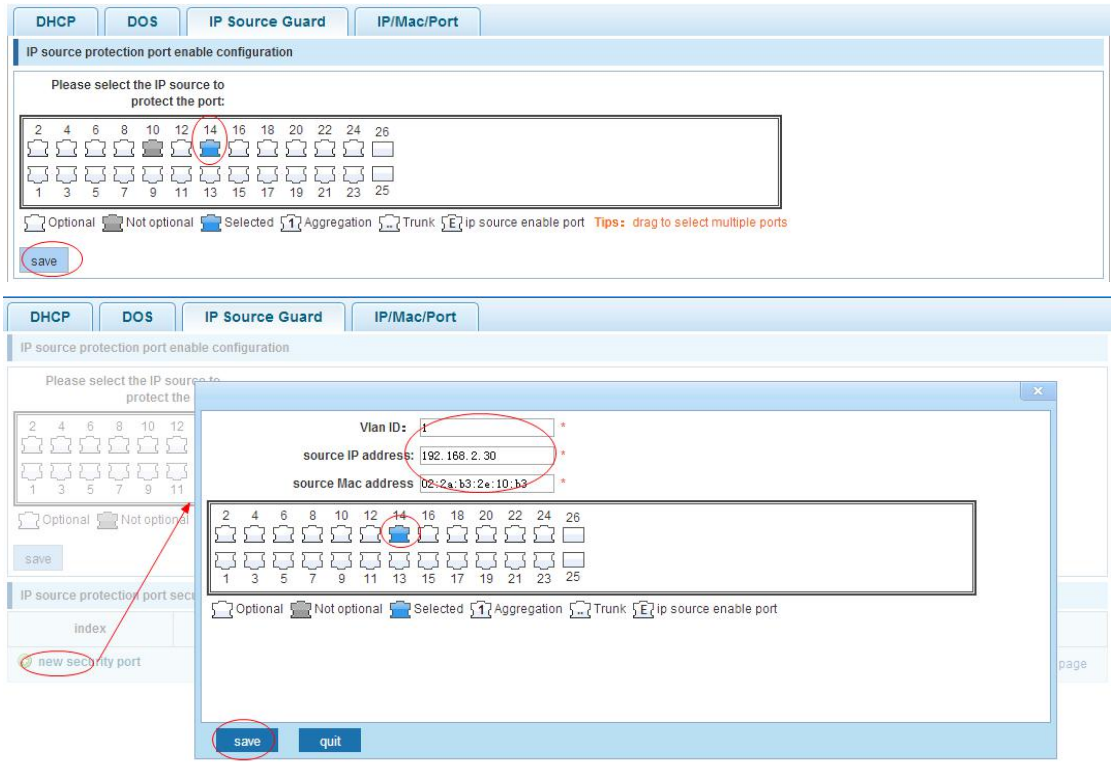


【Instructions】

Add the port that is currently being used as a IP source protection enable port, the port will not be able to use.

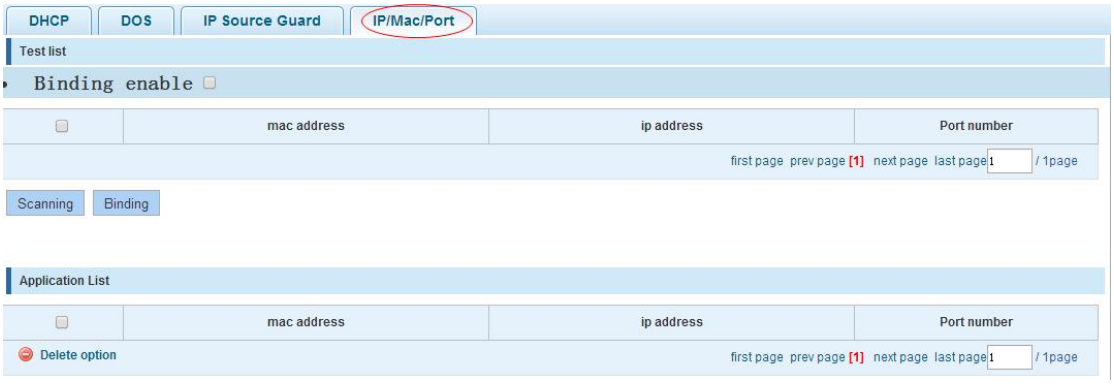
【Configuration Example】

Such as: To open source IP protection enabled port first, then to binding.



4.4.1.4 IP/Mac/Port

In the navigation bar to select **"Fault/Safety>Anti Attack>IP/Mac/Port"**, automatically detect the port based IP address, MAC address of the mapping relationship, and then realize the function of a key binding as shown.

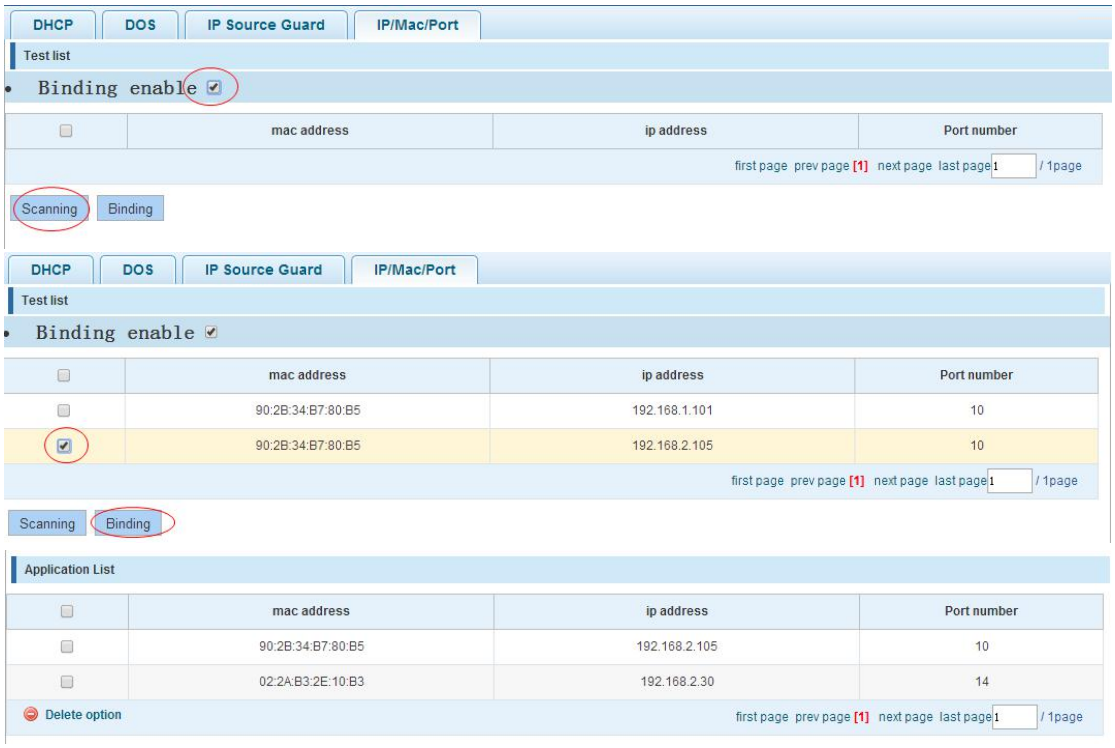


【Instructions】

A bond must be bound before the binding to enable the switch to open, and if you want to access shall be binding and switch the IP address of the same network segment.

【Configuration Example】

Such as: The binding to make first can open, must be a key bindings port 7.

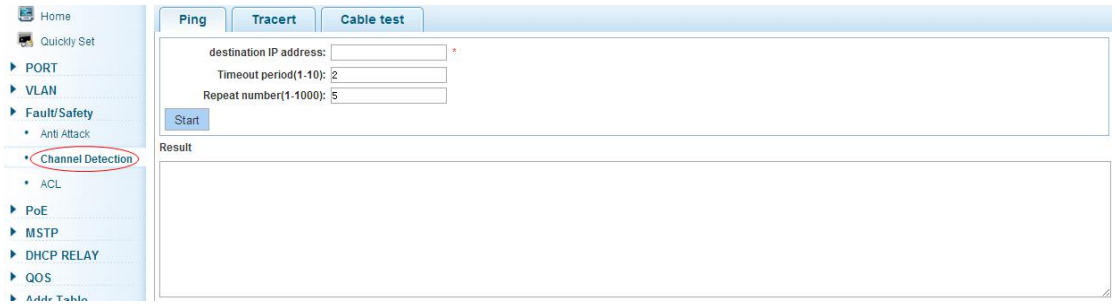


Can check the delete option.

4.4.2 Channel Detection

4.4.2.1 Ping

In the navigation bar to select **"Fault/Safety>Channel Detection>Ping testing"**, use ping function to test internet connect and host whether to arrive as shown.



【Parameter Description】

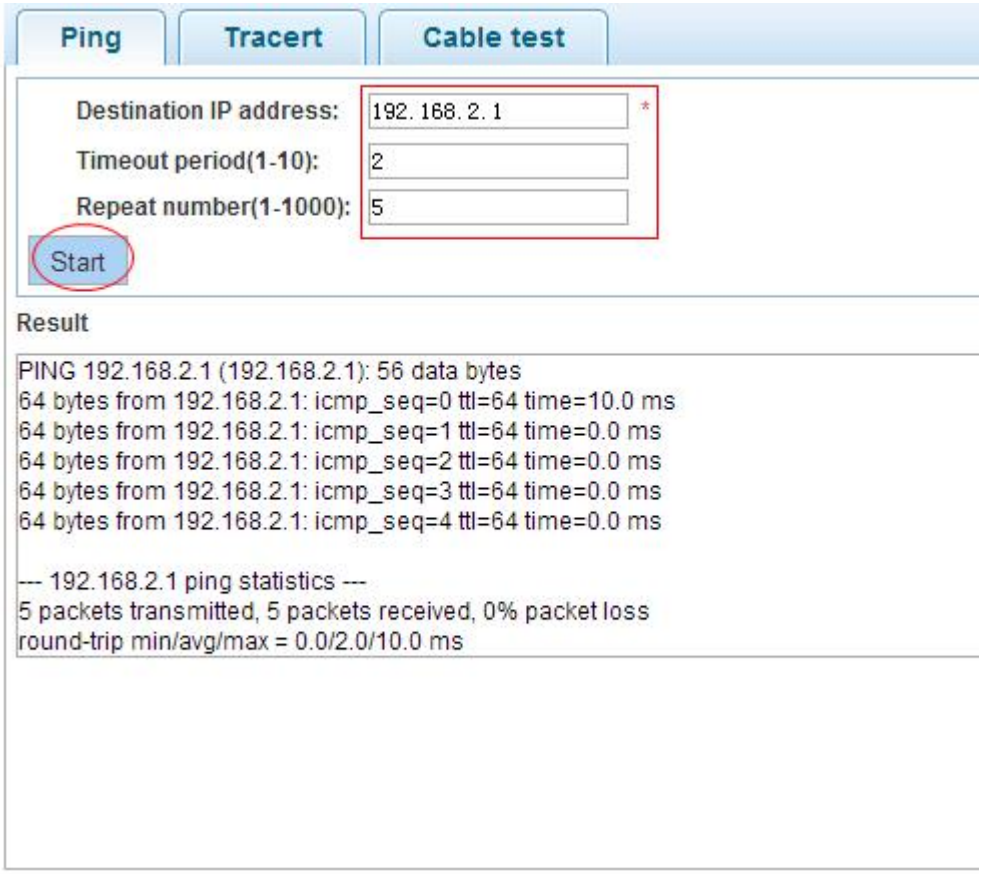
Parameter	Description
Destination IP address	Fill in the IP address of the need to detect
Timeout period	Range of 1 to 10
Repeat number	Testing number

【Instructions】

Use ping function to test internet connect and host whether to arrive.

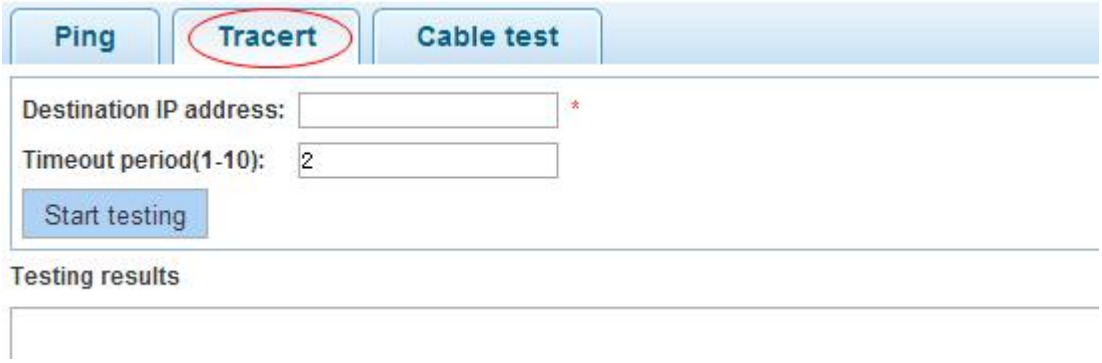
【Configuration Example】

Such as: Ping connect the IP address of the PC.



4.4.2.2 Tracert

In the navigation bar to select **"Fault/Safety>Channel Detection>Tracert testing"**, tracert detection can detect to the destination through as shown.



【Parameter Description】

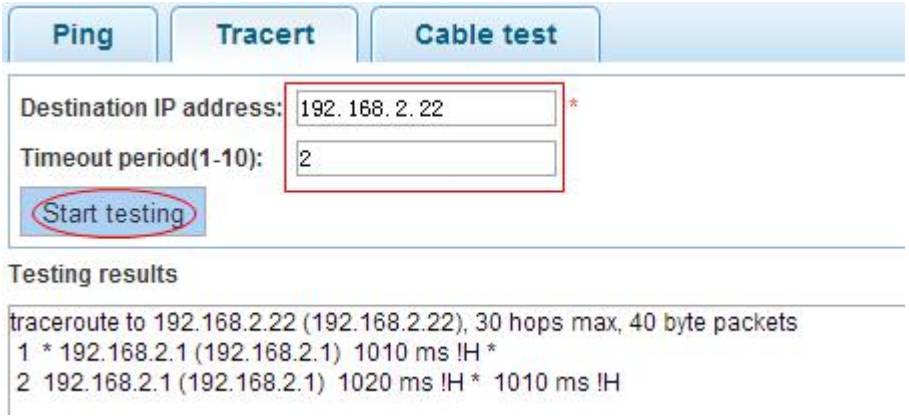
Parameter	Description
Destination IP address	Fill in the IP address of the need to detect
Timeout period	Range of 1 to 10

【Instruction】

The function is used to detect more is up to and reach the destination path. If a destination unreachable, diagnose problems.

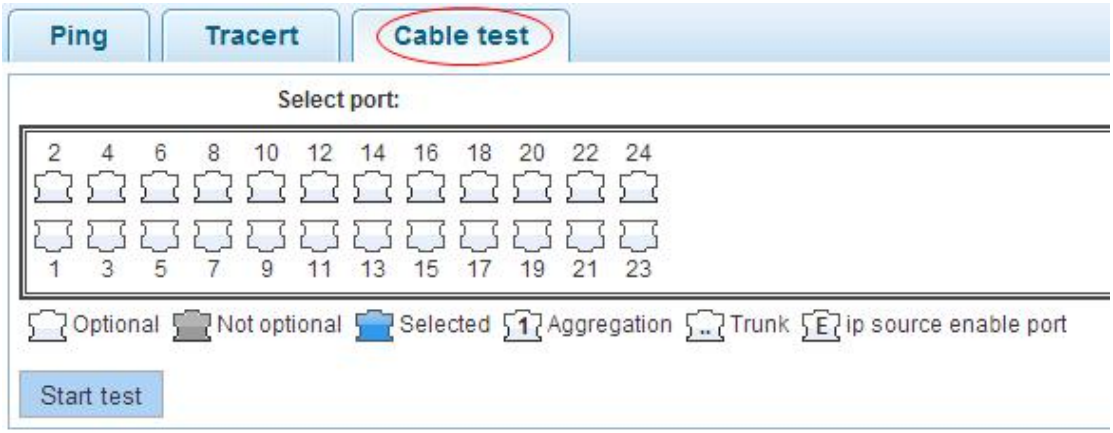
【Configuration Example】

Such as: Ping connect the IP address of the PC.

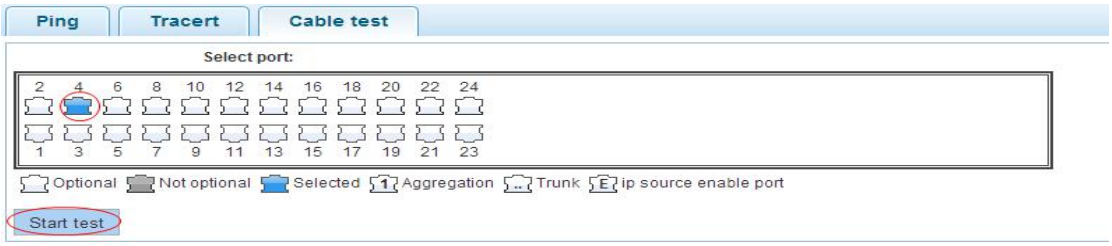


4.4.2.3 Cable test

In the navigation bar to select **"Fault/Safety>Channel Detection>Cable testing"**, can detect connection device status as shown.

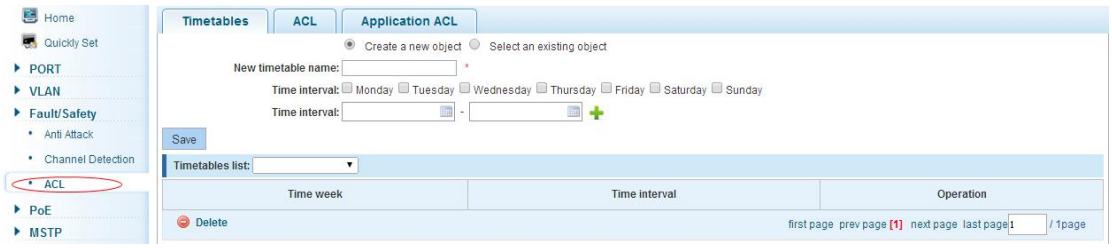


【Configuration Example】



4.4.3 ACL

In the navigation bar to select **"Fault/Safety>ACL",** can be applied to port ACL rules and settings to take effect in time.



【Instruction】

The ACL rules are sequenced, row in front of the match will be priority rule. Many, if the strategy items operating time is relatively longer.

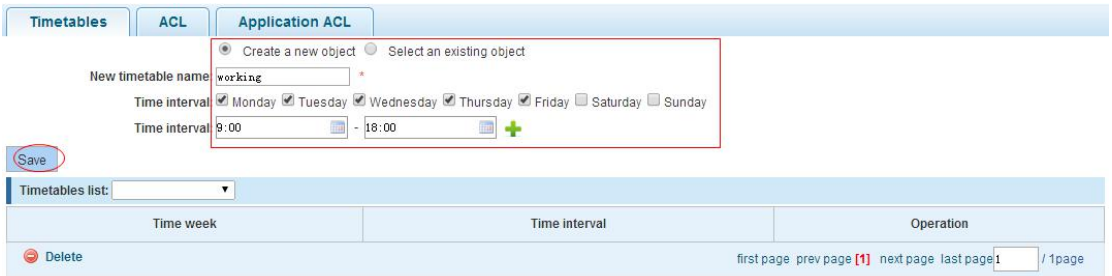
Basic principles:

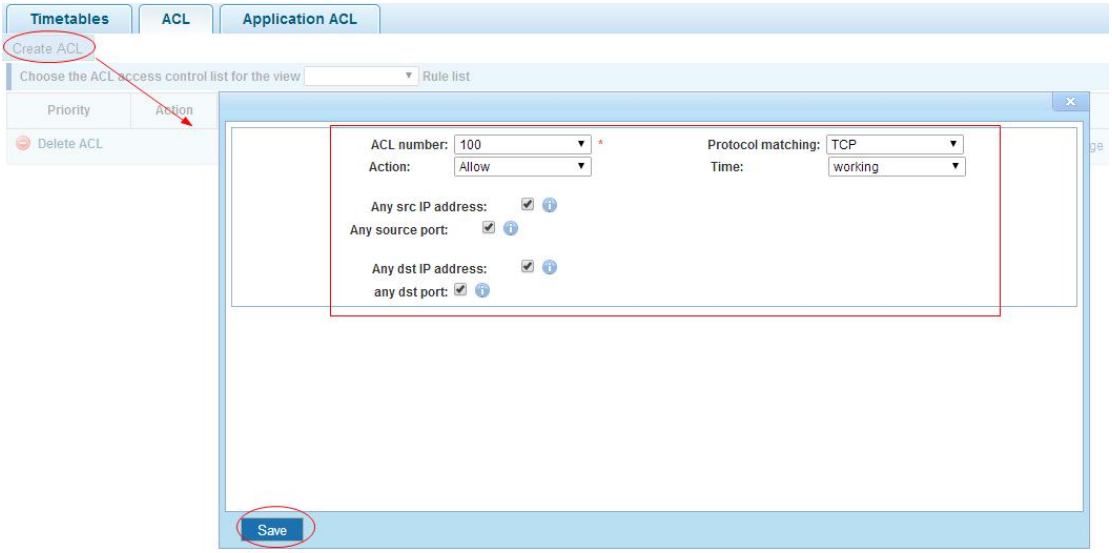
1. According to the order, as long as there is a meet, will not continue to find.
2. Implied refused, if don't match, so must match the final implied refused entry, cisco default.
3. Any only under the condition of the minimum permissions to the user can satisfy their demand.
4. Don't forget to apply the ACL to the port.

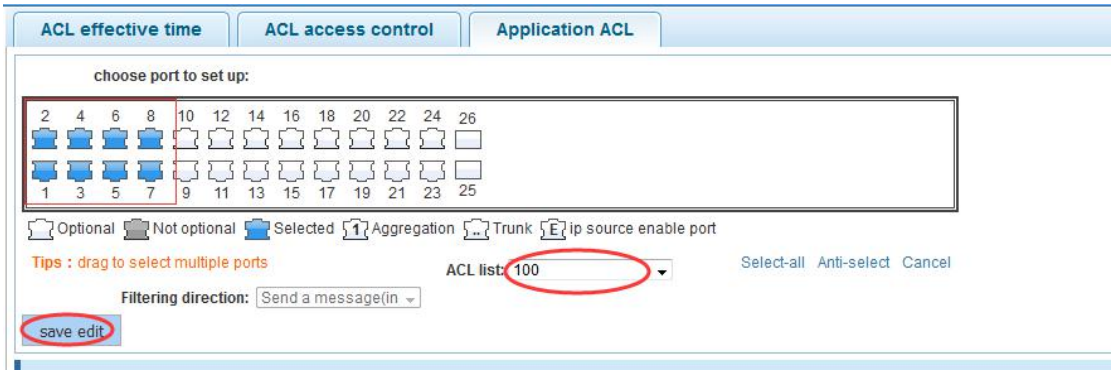
【Configuration Example】

Such as: Test time is every Monday to Friday 9 to 18 points, set port 1-8 cannot access the network.

Steps: Building ACL time - building ACL rules - is applied to the port.

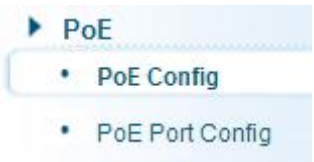






4.5 PoE

In the navigation bar to select"**PoE**", you can set **PoE Config** and **PoE port Config** configuration.

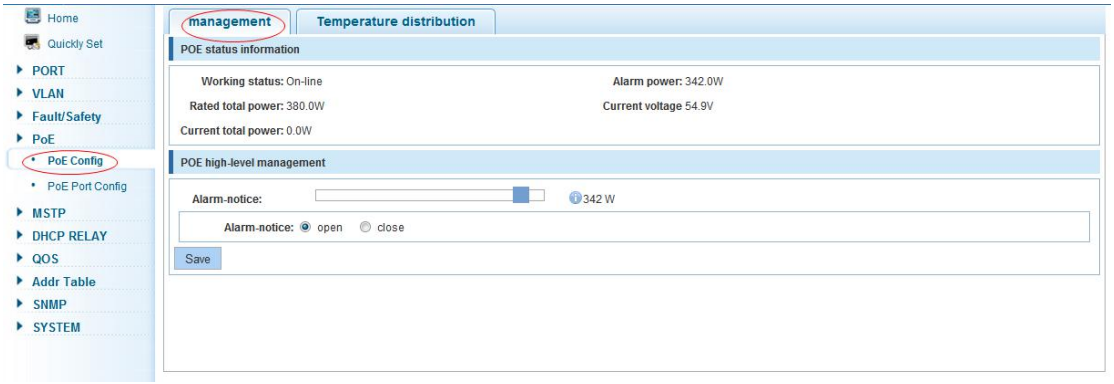


4.5.1 PoE config

In the navigation bar to select"**PoE config**", you can set **management** and **Temperature distribution**.

4.5.1.1 management

In the navigation bar to select **"PoE Config>management"**, To view the PoE state information and set up the configuration. The fllowing picture:



【Parameter description】

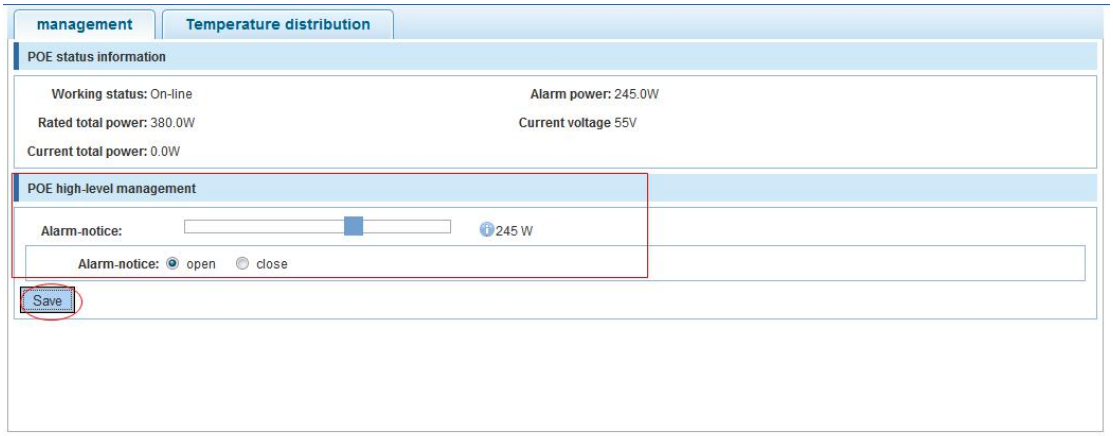
Parameter	Description
Supply mode	Select the mode of PSE power supply
Alarm-power	Configuration of the alarm threshold
Reserved power	Configuration to keep power
Alarm notice	State configuration warning announcement.

【Instruction】

In practical application, it is required to control the system to transmit trap notification when the power change and the port are up and down.
Receive the Trap notices the Snmp must be open, and set the Trap to the target host.

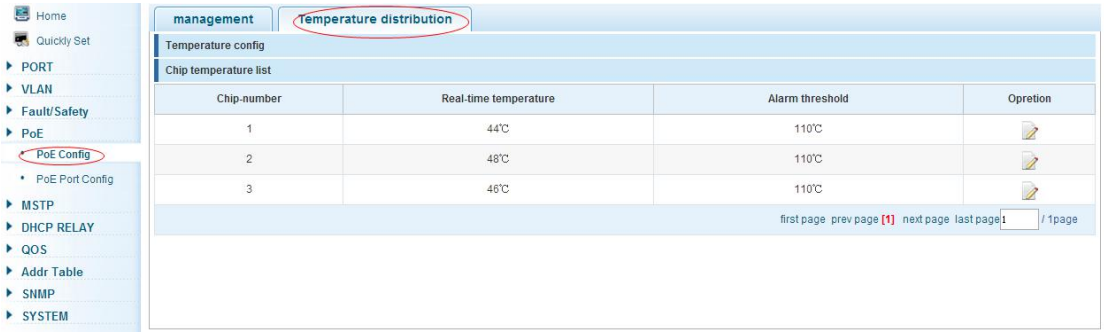
【Configuration example】

Such as:alarm power set to 245 W, reserved power to 15%, open the supply mode and the alarm power;



4.5.1.2 Temperature config

In the navigation bar to select **"PoE Config>Temperature config"**, The alarm threshold can be set up PoE chips. the fllowing picture:



【Parameter description】

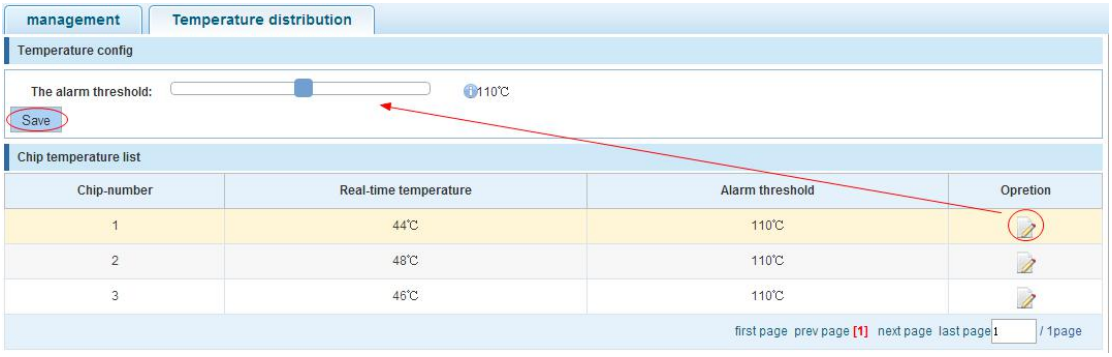
Parameter	Description
Alarm threshold	Configuration temperature alarm threshold, the range of 70-149

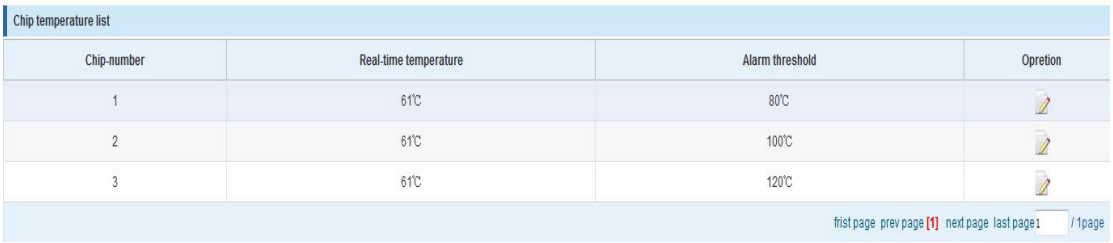
【Instruction】

Receive the Trap notices the Snmp must be open, and set the Trap to the target host.

【Configuration example】

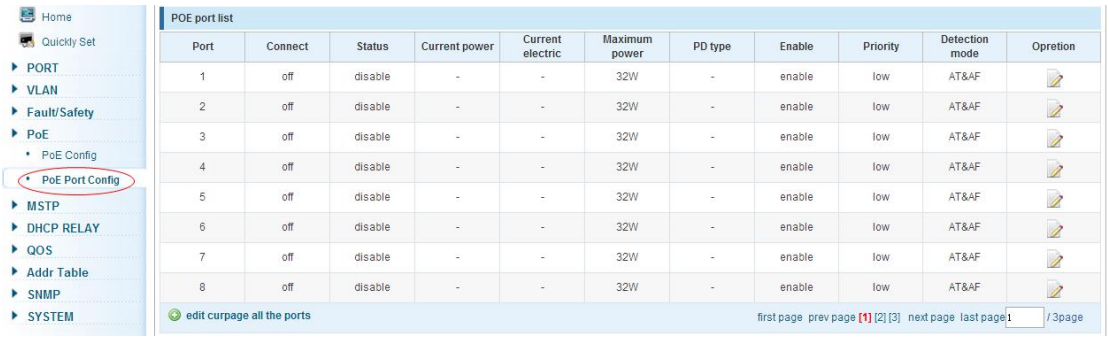
Such as: 1 warning threshold is set to 80 chip, chip 2 warning threshold is set to 100, chip 3 alarm threshold is set to 120





4.5.2 PoE port Config

In the navigation bar to select **"PoE>PoE port Config"**, Can be set to port PoE. The fllowing picture:



【Parameter description】

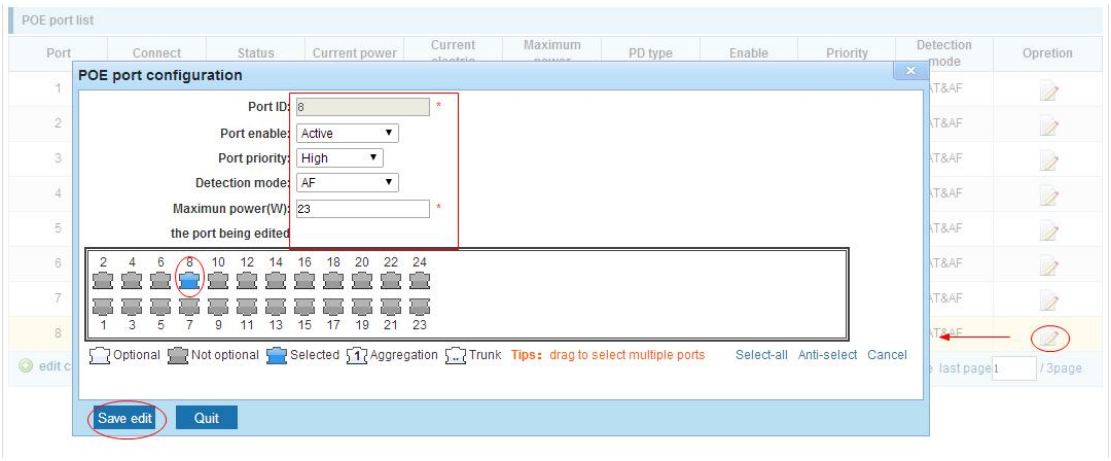
Parameter	Description
Maximum power	Select configure port maximum power
Enable	Select configuration can make state
Priority	Configure port priority, when the load exceeds the PoE power, low priority under the port of equipment will be dropped first
Detection mode	Configure port detection mode

【Instruction】

Receive the Trap notices the Snmp must be open, and set the Trap to the target host.

【Configuration example】

such as: port 8 enable set to active, will set the maximum power to 23 W, detection mode for AF, priority is high.

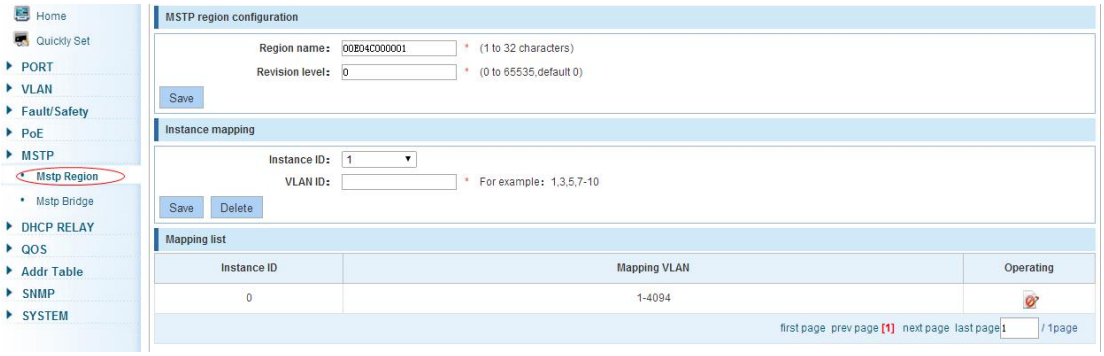


4.6 MSTP

In the navigation bar to select **"MSTP"**, you can set to the **MSTP Region** and **MSTP Bridge** configuration.

4.6.1 MSTP Region

In the navigation bar to select **"MSTP>MSTP Region"**, can modify the domain and domain name, add instance is mapped to a VLAN as shown.



【Parameter Description】

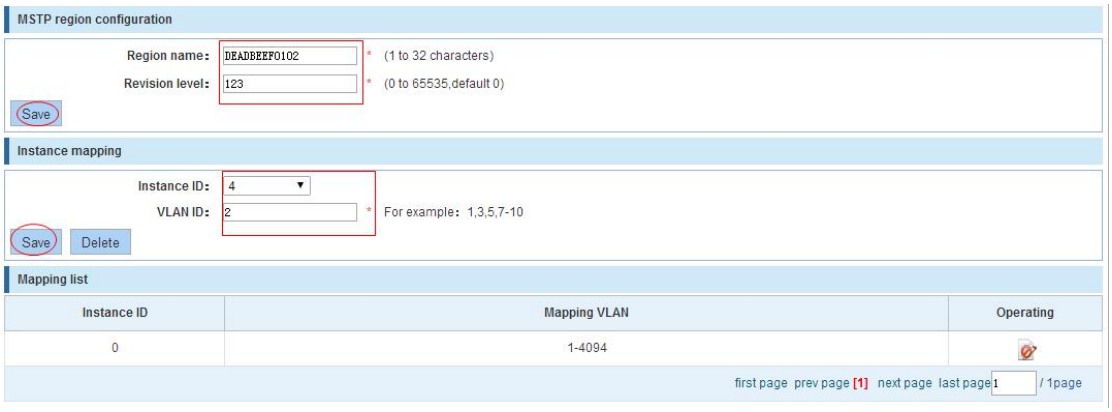
Parameter	Description
Region name	Configure the region name
Revision level	Parameter configuration revision level
Instance ID	Select configuration instance ID
VLAN ID	Mapping of the VLAN configuration instance

【Instruction】

An instance can only be mapped to a VLAN, instance and VLAN is a one-to-one relationship.

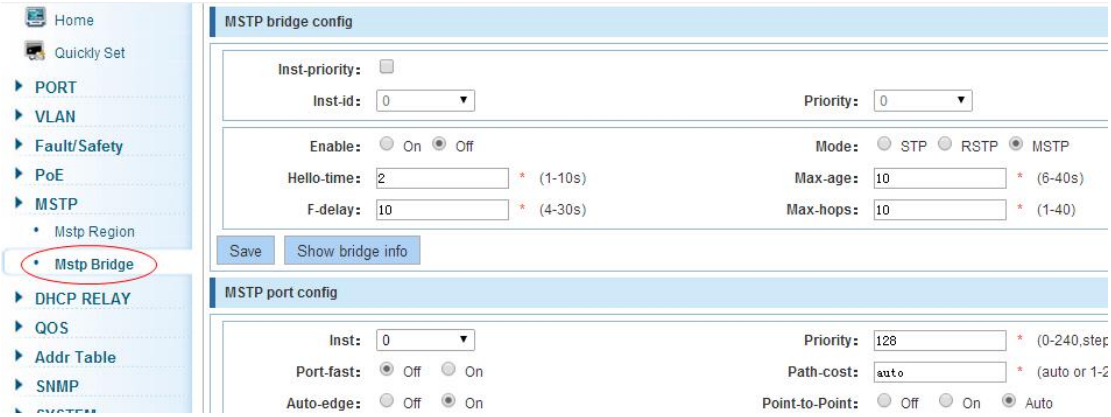
【Configuration Example】

Such as: Change the region to DEADBEEF0102, region name is 123, instance 4 is mapped to a VLAN 2, in the first need to create a VLAN 2.



4.6.2 MSTP Bridge

In the navigation bar to select **"MSTP>MSTP Bridge"**, can be related to bridge, port configuration as shown.



【Parameter Description】

Parameter	Description
Inst-priority	Whether open instance priority setting
Instance ID	Select the created instance id is configured
Enable	Whether to open the STP bridge function
Bridge priority	Priority setting bridge example, the default instance bridge priority for 32768

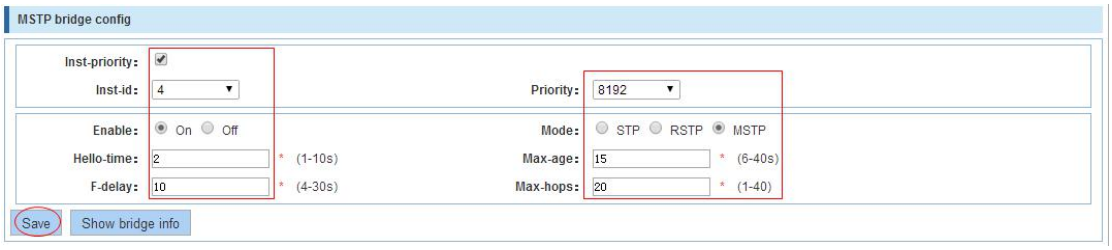
Mode	The model is divided into: the STP, RSTP, MSTP
Hello-time	Switches sends bpdus in packet interval
Max-age	Ports are not yet received a message in the time, will initiate topology changes
Forward-delay	The state of the port switch time
Port-priority	Set port instance priority, defaults to 128, you must enter multiple of 16, the range of 0-240
Path-cost	Configure port costs
Port-fast	Select configuration state
Auto-ege	Select configuration state
Point-to-point	Select configuration state
Bpdu guard	Select configuration state
Bpdu filter	Select configuration state
Compatible	Select configuration state
Root guard	Select configuration state
TC guard	Select configuration state
TC filter	Select configuration state

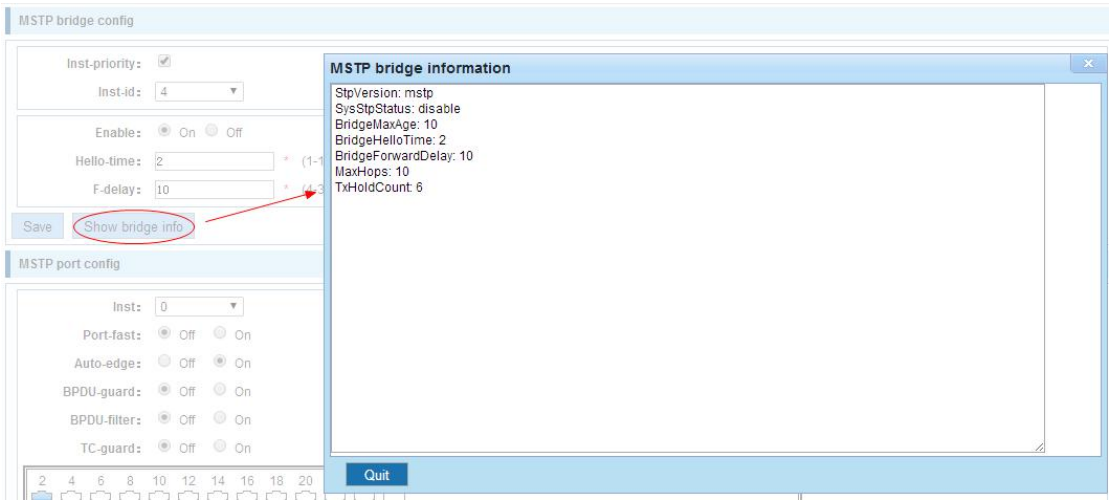
【Instruction】

(1) (hello_time+1)×2<=max_age<=(f_delay-1)×2, enable the switch to set instance priority.
(2) Enable STP or switch mode would spend 2 times of the forward delay time.

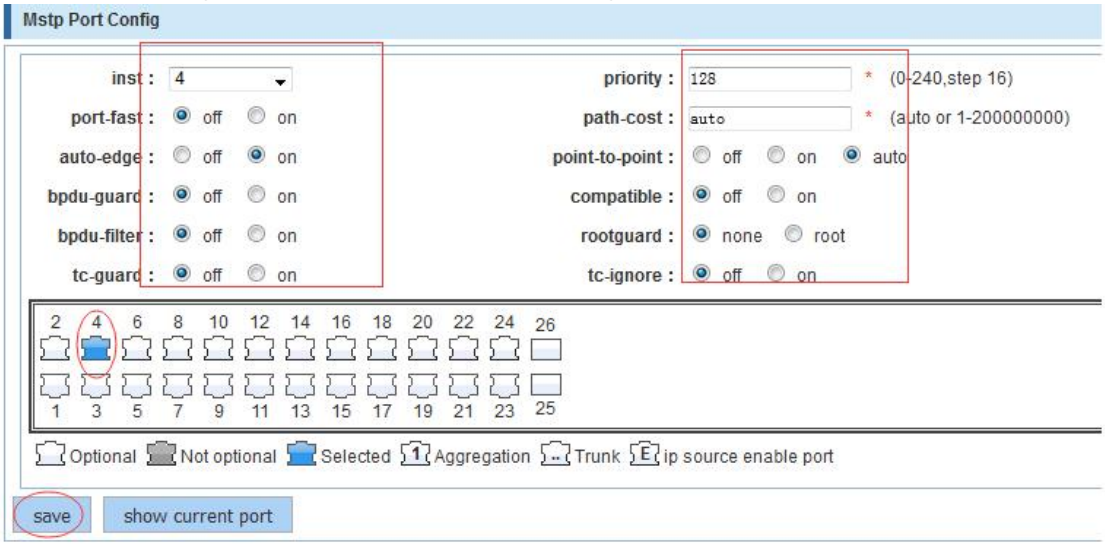
【Configuration Example】

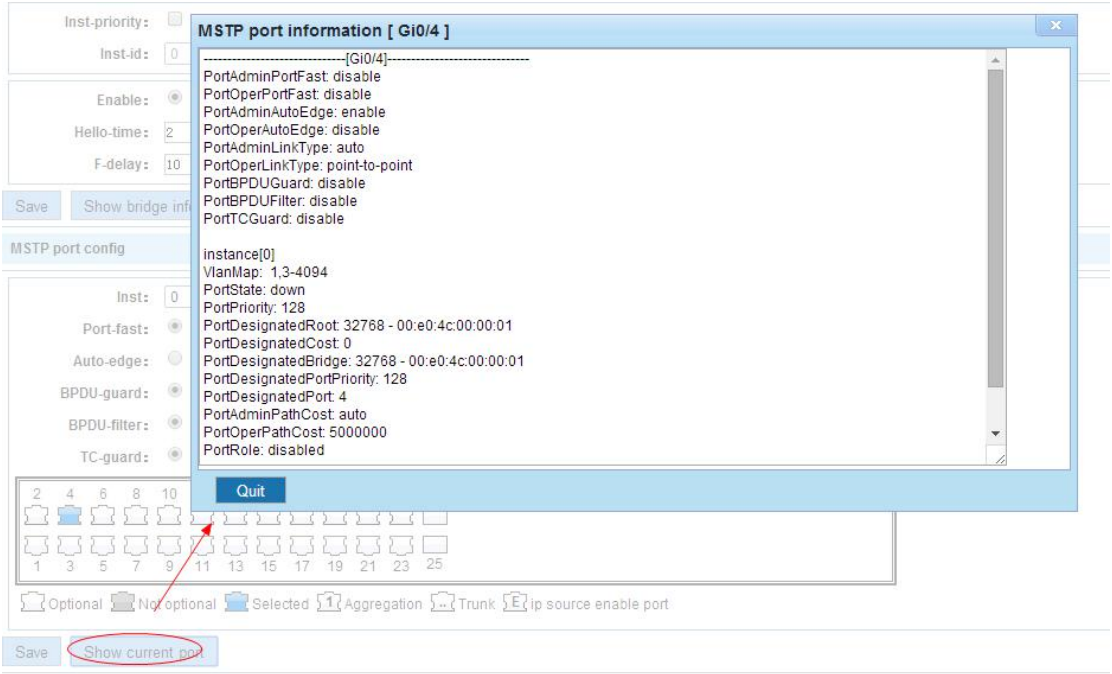
Such as: 1) Open the STP, configuration has to create an instance of the priority, configuration time Parameters, set the pattern to MSTP.





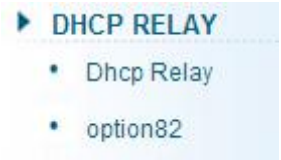
2) Set MSTP has launched port configuration, select the created instance, set priority (port configuration is not online, on-line configuration will only take effect, can click on the "view the current configuration" button to view the configured completed).





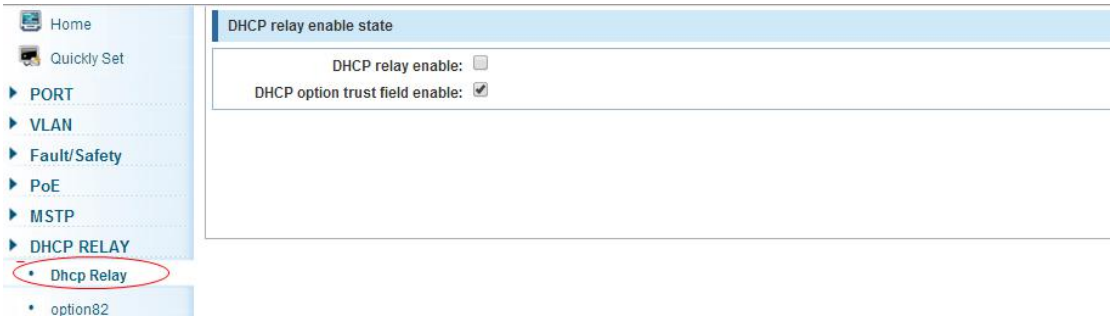
4.7 DHCP Relay

In the navigation bar to select **"DHCP Relay"**, you can set to the **DHCP Relay** and **option82**.



4.7.1 DHCP Relay

In the navigation bar to select **"DHCP Relay",** open the DHCP relay function, set up and view the relay server IP address and its status as shown.



【Parameter Description】

Parameter	Description

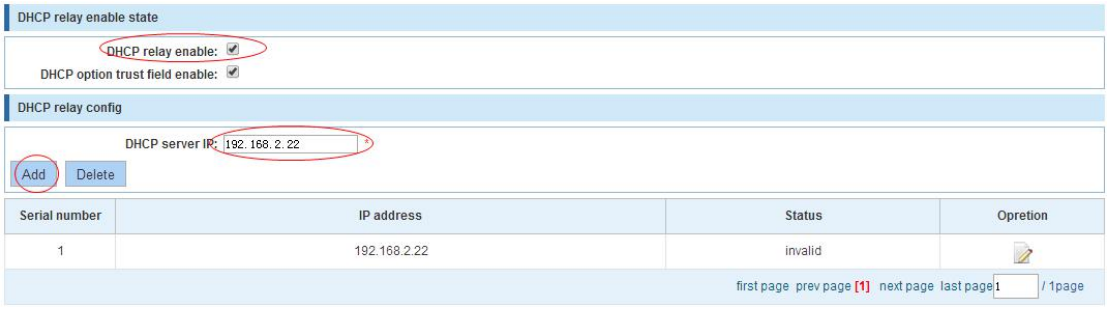
IP address	DHCP server address
Status	Invalid and vaild

【Instruction】

If open the function of relay agent, then receives the broadcast DHCP message, to be delivered in the form of unicast to configure on the server. The DHCP server to IP and switches in the same network segment will only take effect.

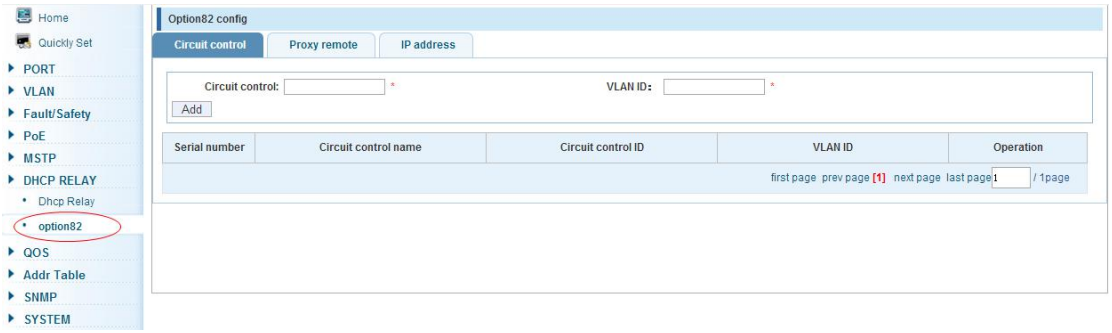
【Configuration Example】

Such as: Setting DHCP server IP for 192.168.2.22.



4.7.2 Option82

In the navigation bar to select **"DHCP Relay>option82"**, can set to option82 circuit control, proxy remote, IP address as shown.



【Parameter Description】

Parameter	Description
VLAN id	The DHCP request message in the VLAN, value range is 1 ~ 4094
Circuit control	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63
Proxy remote	Configuration ASCII remote id string value, the length of the range of 1 ~ 63

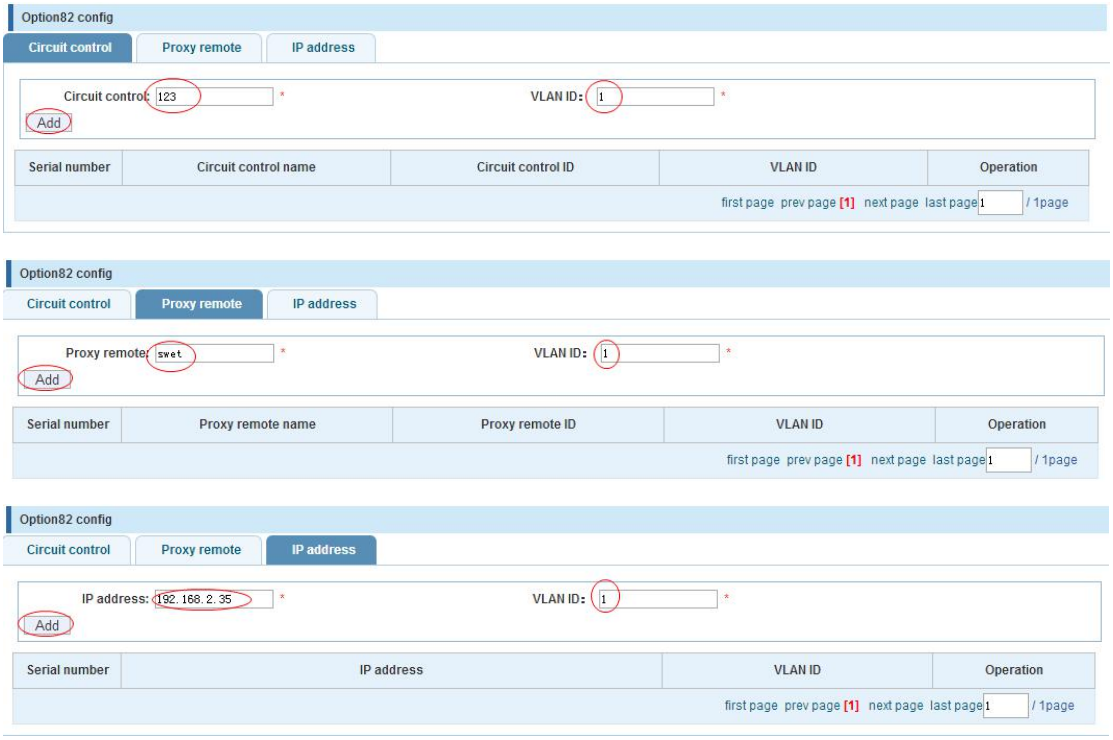
IP address	Decimal IP address

【Instruction】

Switches, relay information to the DHCP server will take option82, VLAN ID must be configured to DHCP message taken VLAN can bring option82 information.

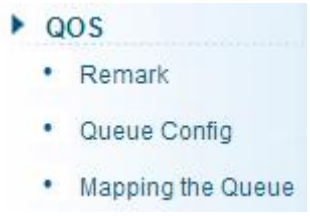
【Configuration Example】

Such as: Add circuit control, proxy remote, IP address information.



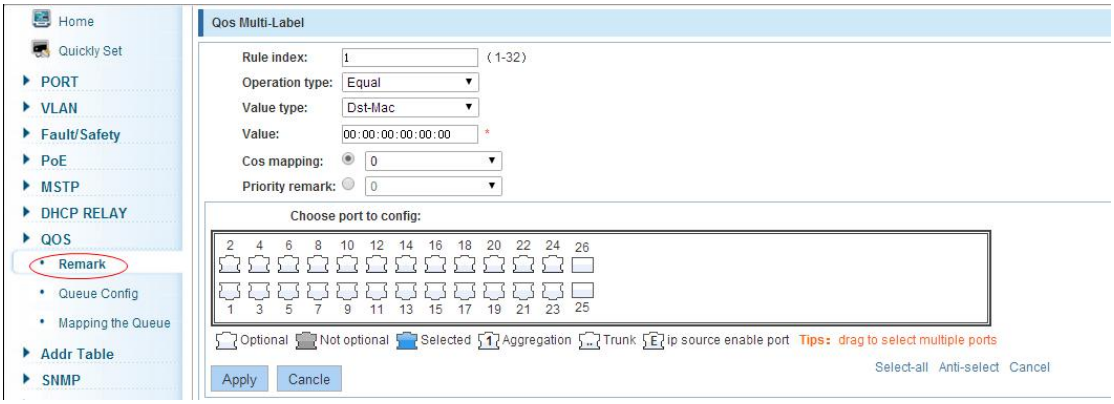
4.8 QOS

In the navigation bar to select **"QOS"**, you can set to the **Remark, Queue Config** and **Mapping the Queue**.



4.8.1 Remark

In the navigation bar to select **"QOS>Remark",** according to the rules for port traffic bag tag or queue map as shown.



【Parameter Description】

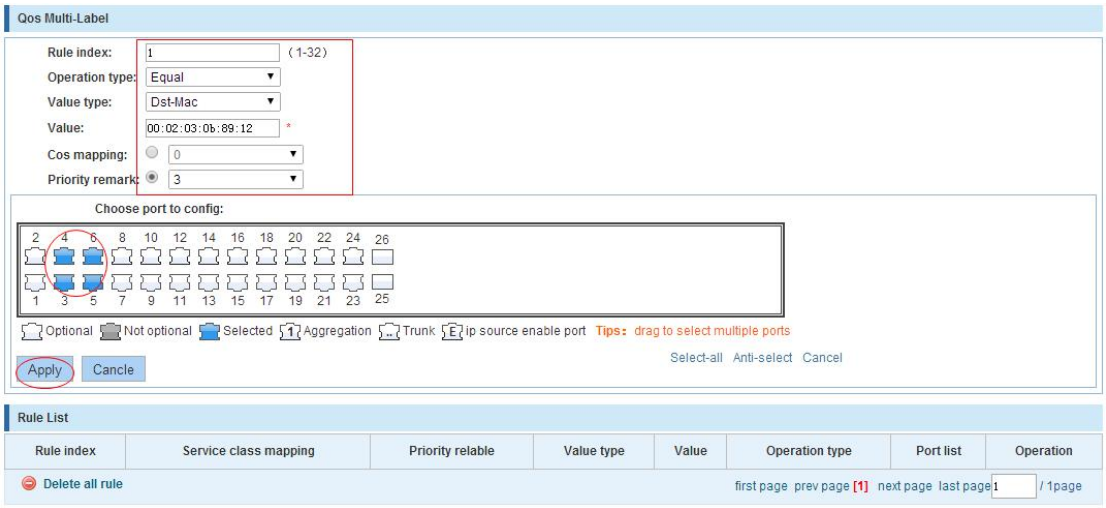
Parameter	Parameter
Rule index	By setting the rule of heavy tag index number, the current switch can be set up 32 rule
Operation type	Choose always said - match the match, all the data for tags Choose can be set to equal matching rules, comply with the rules of heavy tag data
Server class mapping	Adaptable to the rules of the heavy tag which data is mapped to a queue
Priority relable	Conform to the rules of heavy tag data to the marked priority values
Value tye	Set heavy tag matching rules, such as choice goal Mac, just check the data destination Mac address is in accordance with the rules
value	Set the value of matching, such as choice goal Mac for HH: HH:HH:HH:HH:HH
Choose port to config	The application of heavy tag on which interface
apply	Click on the application of heavy marking rules to take effect

【Instruction】

According to the different matching rules to map different packages to different cos, and then according to the mapping relationship cos and queue queue to map different packages to different queue, can also set the priority value of a tag heavy bag.

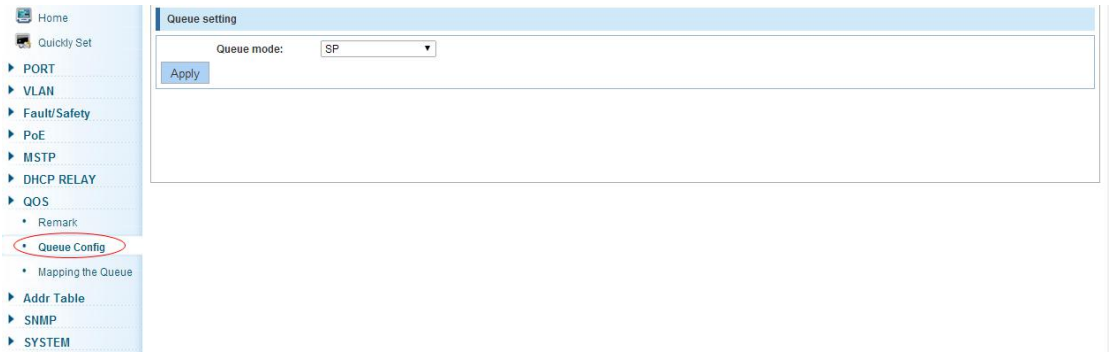
【Configuration Example】

Such as: Will the destination address for 00:02:03:0b:89:12 packets are forwarded to the port 3, 4, 5, 6, priority of remarked as 3.



4.8.2 Queue Config

In the navigation bar to select **"QOS>Queue Config"**, can be set up queue scheduling policy as shown.



【Parameter Description】

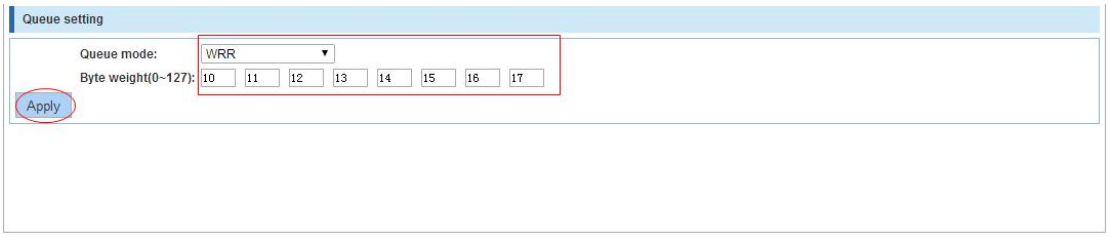
Parameter	Description
Scheduling strategy	Can choose four kinds of modes: RR round-robin scheduling SP absolute priority scheduling WRR weighted round-robin scheduling WFQ weighted fair scheduling
WRR-weights	Set the weights of each queue, they will be in proportion to occupy the bandwidth to send data

【Instruction】

Queue 7 can not for 0.

【Configuration Example】

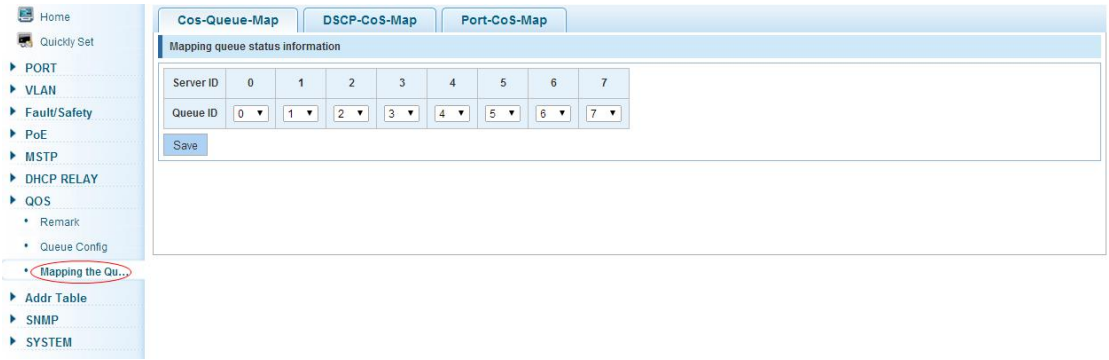
Such as: Set the scheduling strategy for WRR, weight value respectively, 10, 11, 12, 12, 14, 15, 16, 17.



4.8.3 Mapping the Queue

4.8.3.1 Service class queue mapping

In the navigation bar to select **"QOS>Mapping the Queue>Service class queue mapping"**, service category can be mapped to the corresponding queue as shown.

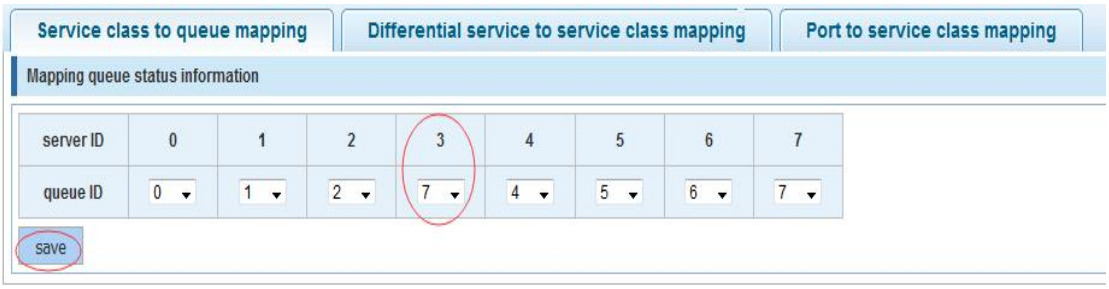


【Parameter Description】

Parameter	Description
Server ID	COS the VLAN priority fields (0 to 7)
Queue ID	Set each cosine value mapping queue number (0 to 7)

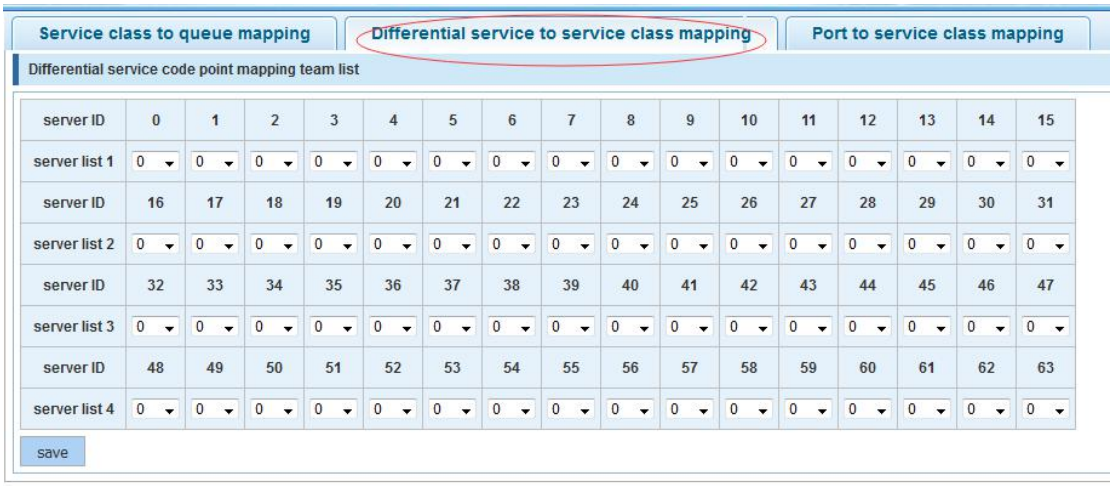
【Configuration Example】

Such as: Cos 3 mapping to the queue 7, set the queue weight 7 to 10.



4.8.3.2 Differential service class mapping

In the navigation bar to select **"QOS>Mapping the Queue>Differential service class mapping"**, differential service can be mapped to the corresponding service categories as shown.



【Parameter Description】

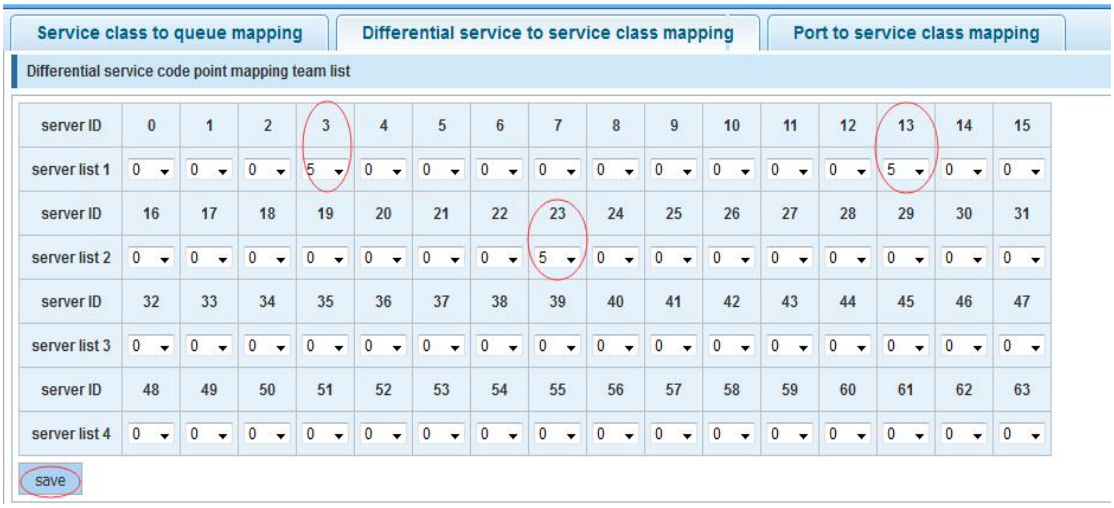
Parameter	Description
Server list	DSCP field has seven (0-63) is divided into four tables
Queue ID	Map the DSCP to COS fields (0 to 7), based on the cosine is mapped to a queue

【Instruction】

Cos priority is greater than the DSCP, DSCP priority is greater than the port.

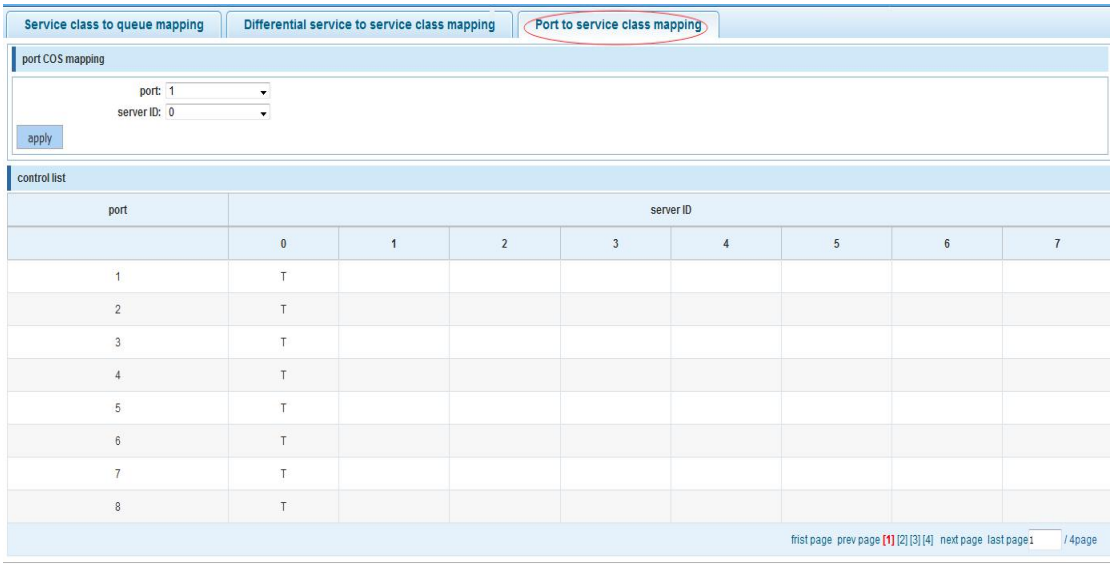
【Configuration Example】

Such as: The DSCP value of 3, 12, 23 mapping to cos 5.



4.8.3.3 Port to service class mapping

In the navigation bar to select **"QOS>Mapping the Queue>Port to service class mapping"**, port can be mapped to the corresponding service categories as shown.



【Parameter Description】

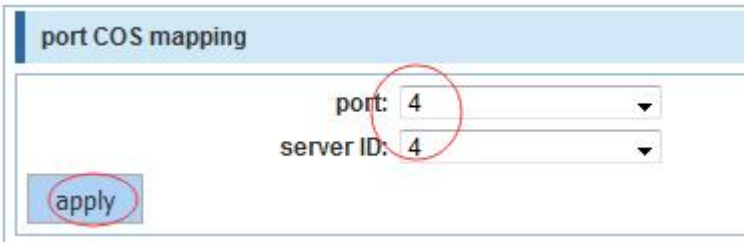
Parameter	Description
Port	Select the port number (1-26)
Service ID	Mapped to the service ID, and then according to the service ID into the queue

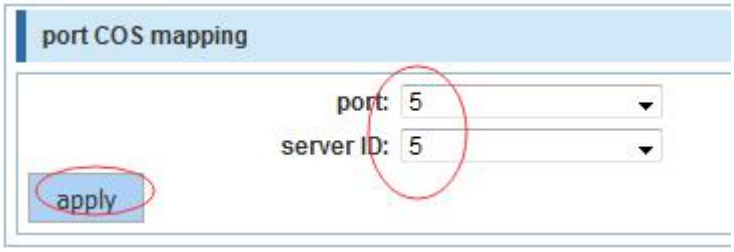
【Instruction】

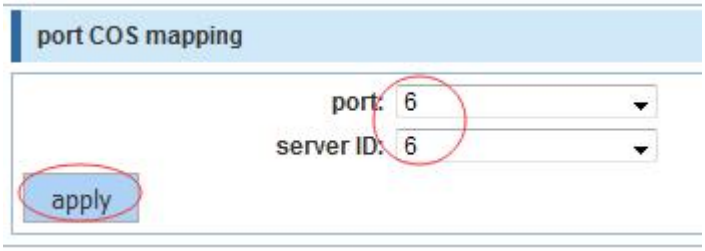
Cos priority is greater than the DSCP, DSCP priority is greater than the port.

【Configuration Example】

Such as: Port 4, 5, 6 respectively cos4, cos5, cos6.





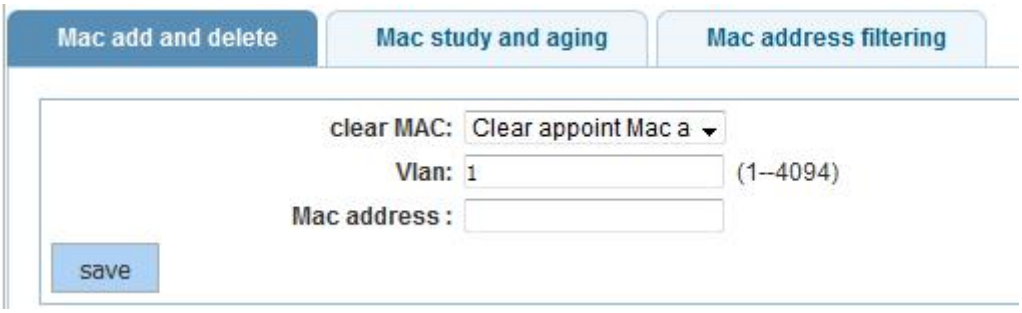


control list

port	server ID							
	0	1	2	3	4	5	6	
1	T							
2	T							
3	T							
4					T			
5						T		
6							T	
7	T							
8	T							

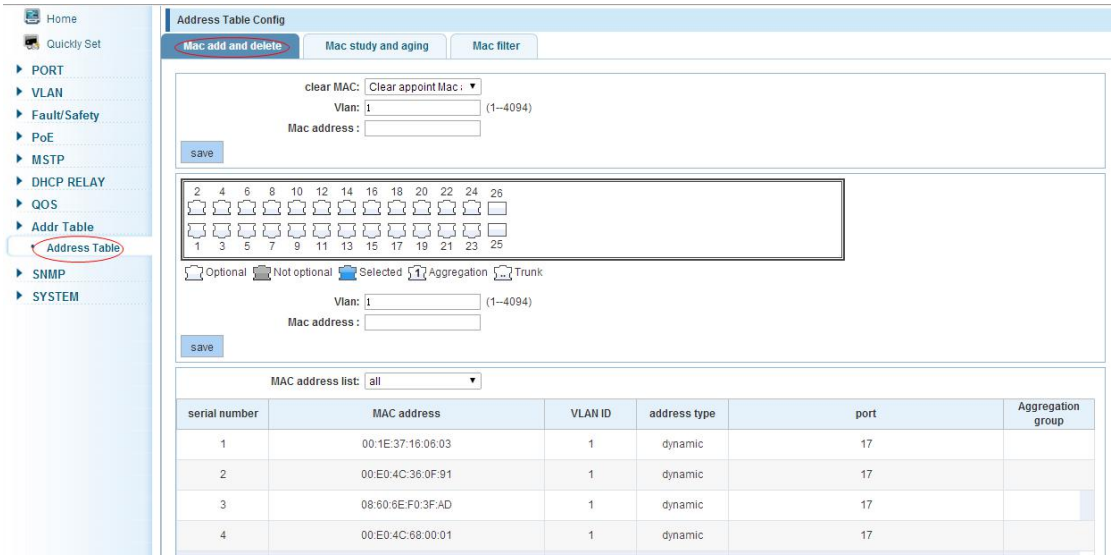
4.9 Address Table

In the navigation bar to select **"Address Table"**, you can set to **MAC add and delete, MAC study and Aging** and **MAC address filtering**.



4.9.1 Mac add and delete

In the navigation bar to select **"Address Table>Address Table>Mac add and delete"**, you can add static Mac and delete Mac and view to the current of the Mac address table as shown.



【Parameter Description】

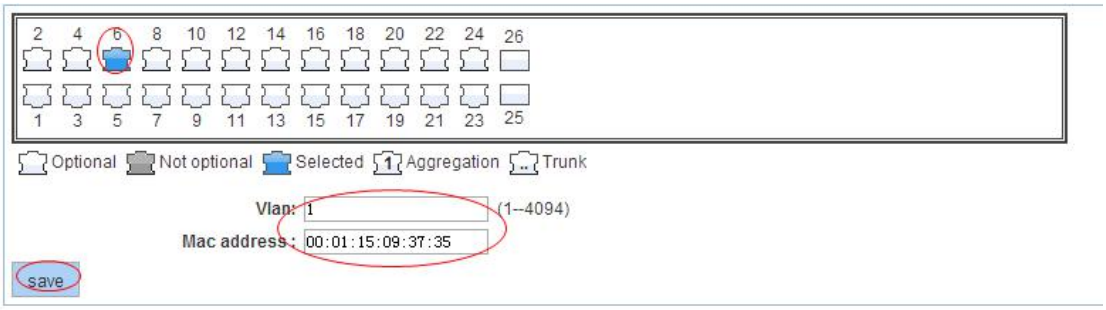
Parameter	Description
Clear Mac	Can choose to clear the multicast Mac address, clear dynamic unicast Mac address, clear static unicast Mac address, clear the specified Mac address, Mac address table
VLAN	Fill in the need to add or delete VLAN id, not create vlans to create can only take effect

【Instruction】

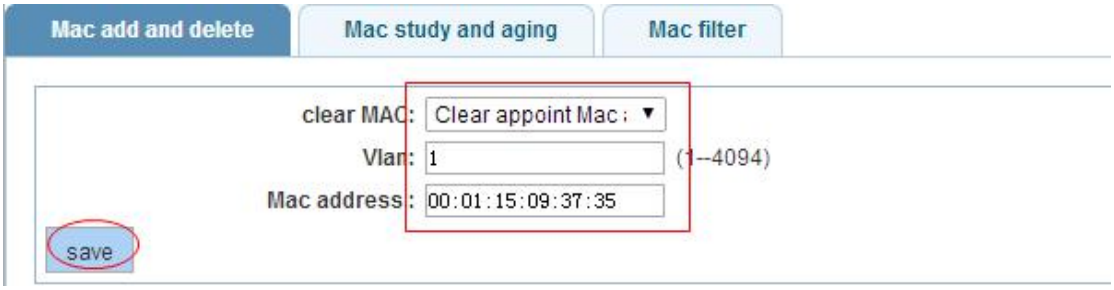
According to different conditions to clear Mac address, view/add/learn the Mac address, Mac address filtering.

【Configuration Example】

Such as: 1) The port 6 Mac set to static Mac.

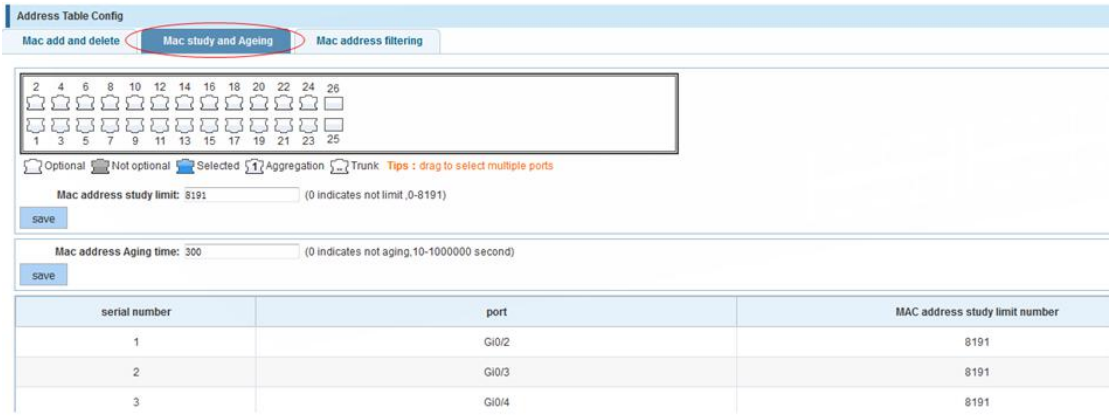


2) Clear port 6 static Mac addresses.



4.9.2 Mac study and Aging

In the navigation bar to select **"Address Table>Mac study and Aging",** can be set up port Mac address study limit and Mac address aging time as shown.

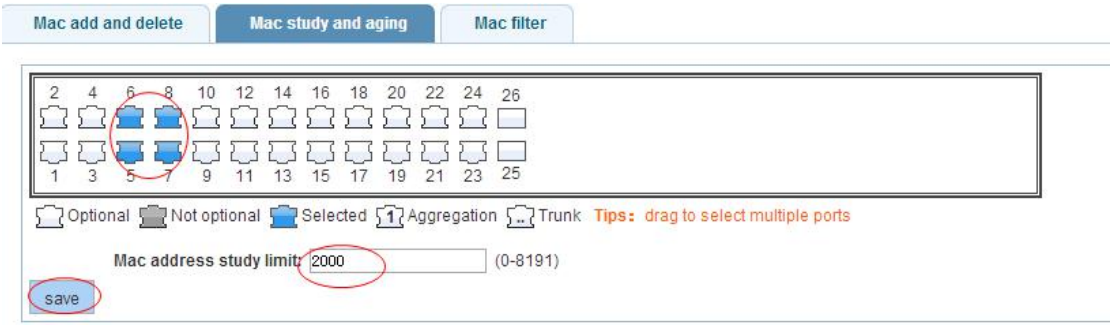


【Parameter Description】

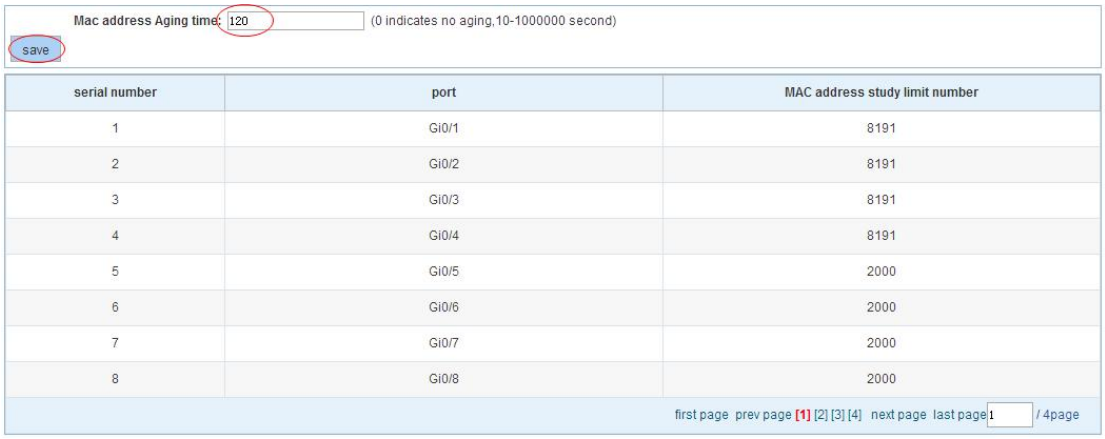
Parameter	Description
Mac address	Range 0-8191, default 8191
Mac address study limit	Default 300

【Configuration Example】

Such as: 1) Setting port 5,6,7,8 address study limit for 2000.

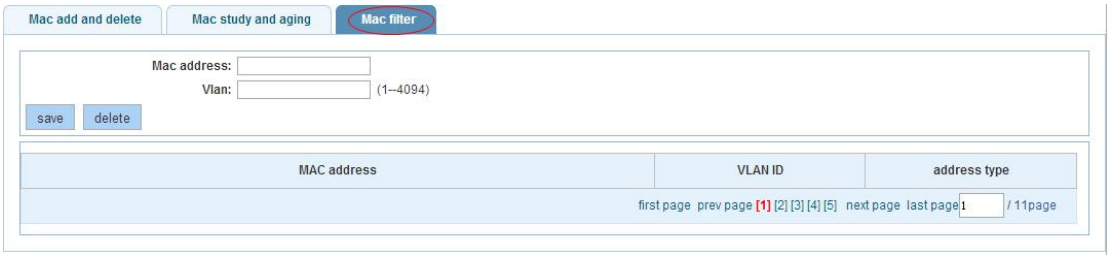


2) Will be dropped or learn the Mac address of the port equipment after 2 minutes disappear automatically from the Mac address table.



4.9.3 Mac address filtering

In the navigation bar to select **"Address Table>Mac address Filtering"**, can be filtered according to the condition does not need the Mac address as shown.



【Parameter Description】

Parameter	Description
Mac address	Can not add multicast Mac address
VLAN	VLAN number

【Configuration Example】

Such as: The Mac address for 00:20:15:09:12:12 added to the filter in the table.

4.10 SNMP

In the navigation bar to select **"SNMP"**, you can set to the **SNMP Config** and **RMON Config**.

4.10.1 SNMP Config

4.10.1.1 SNMP Config

In the navigation bar to select **"SNMP>SNMP Config"**, you can SNMP function enable as shown.

【Instruction】

The SNMP function must be turned on in the configuration RMON, otherwise it will be configured to fail.

【Configuration Example】

Such as: Open SNMP.

4.10.1.2 Community Config

In the navigation bar to select **"SNMP >SNMP Config>Community Config"**, can specify group access as shown.

【Parameter Description】

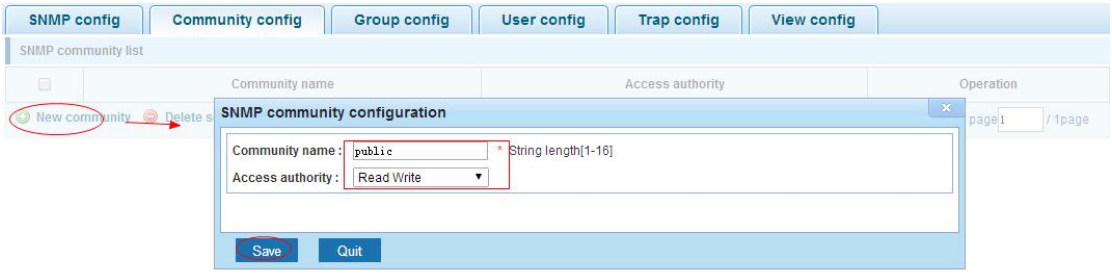
Parameter	Description
Group	Community string, is equal to the NMS and SNMP agent communication between the password
Access authority	Read-only: specify the NMS (SNMP host) of MIB variables can only be read, cannot be modified Read-only can write: specify the NMS (SNMP host) of MIB variables can only read, can also be modified

【Instruction】

The upper limit of the number of groups is 8.

【Configuration Example】

Such as: Add a read-write group called public.



4.10.1.3 Group Config

In the navigation bar to select **"SNMP>SNMP Config>Group Config"**, setting SNMP group as shown.

【Parameter Description】

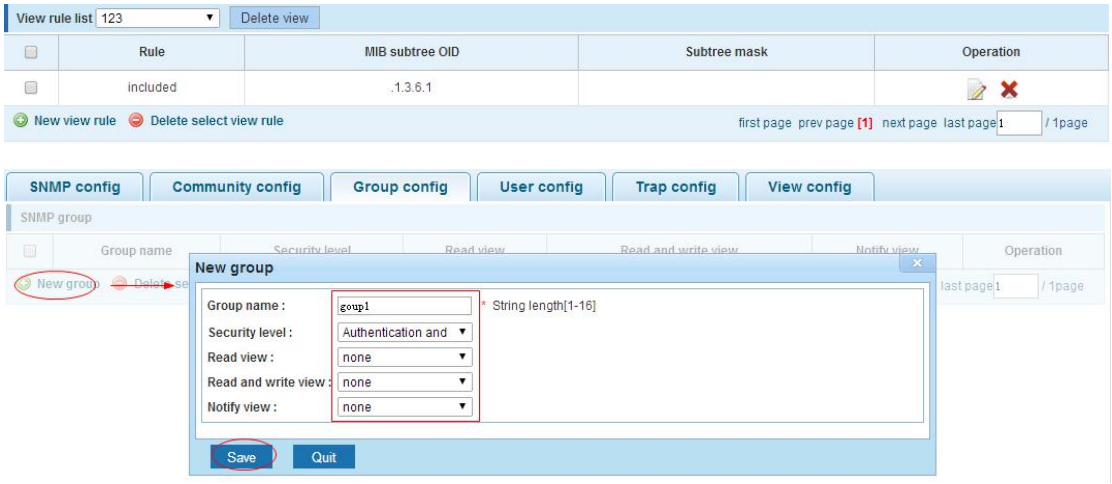
Parameter	Description
Group name	Group name
Security level	Attestation not only encryption: This group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: This group of users' messages don't need to verify data transmission also does not need to be kept secret Both authentication and encryption: This group of users need to verify the news of transmission and transmission of data need to be kept secret
Read view, read and write view, study view	The associated view name

【Instruction】

Before the cap on the number set of configuration of 8, the new group needs a new view to create a group.

【Configuration Example】

Such as: Firstly, new view 123, then new group of goup1.



4.10.1.4 User config

In the navigation bar to select **"SNMP>SNMP Config>User Config"**, setting SNMP user

as shown.

【Parameter Description】

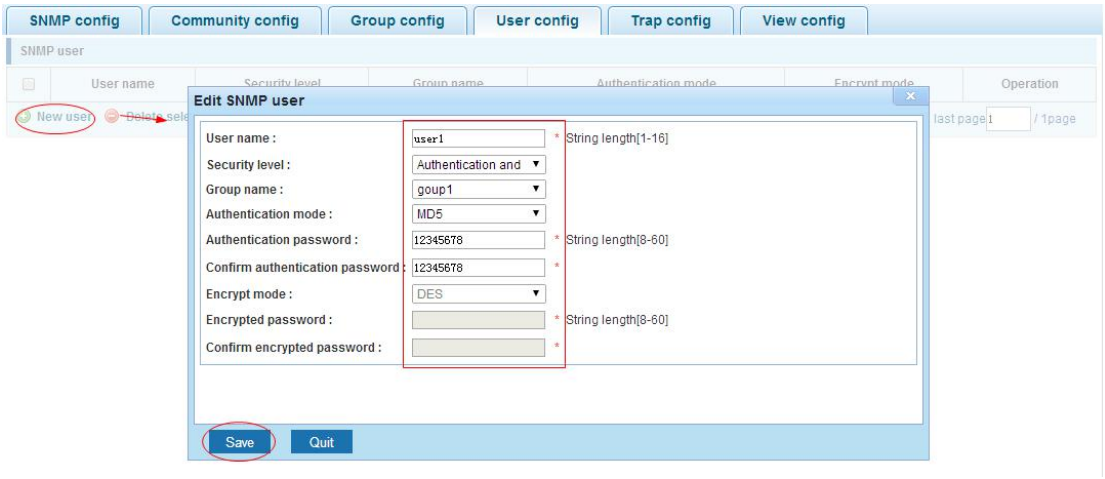
Parameter	Description
User name	User name, range 1-16
Security level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not need to be kept secret Both authentication and encryption: this group of users need to verify the news of transmission and transmission of data need to be kept secret
Authentication mode	Specified use MD5 authentication protocol or SHA authentication protocol
Authentication password	Range 8-10
Encrypt mode	Specified using AES encryption protocol or DES encryption protocol
Group name	A user group name
Encrypt password	Range 8-60

【Instruction】

Cap on the number configuration of 8, users need a new view and group to use, the user's security level must be consistent with the group level of security. Add a user authentication and encryption, and configure belong to groups of users, the user will be used for Snmpv3 connection.

【Configuration Example】

Such as: New view 123, the newly built group group1, new users user1.



4.10.1.5 Trap

In the navigation bar to select **"SNMP>SNMP Config>Trap Config"**, can specify sent the trap messages to SNMP host (NMS) as shown.

【Parameter Description】

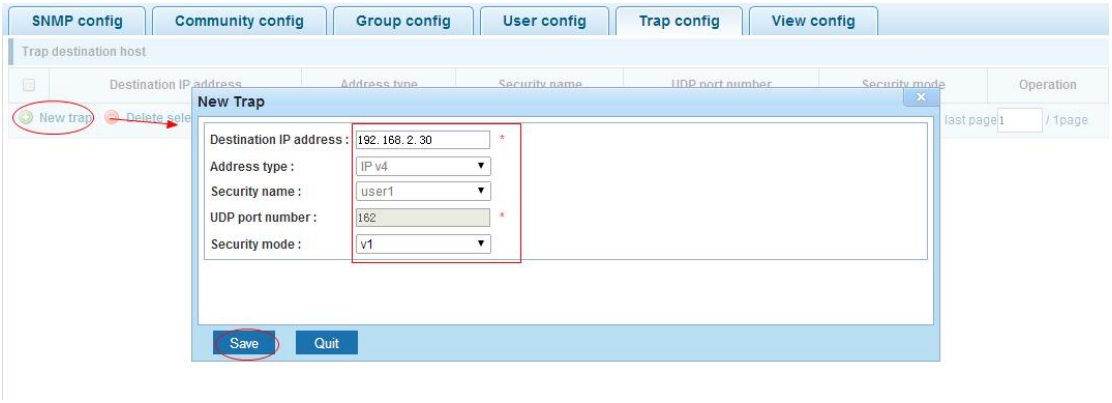
Parameter	Description
Destination ip address	SNMP host ipv4 address
Security name	SNMP user name
Version	V1, V2, V3
Security mode	Specified using AES encryption protocol or DES encryption protocol
Group name	User group name

【Instruction】

The Trap cap on the number configuration of 8, you can configure a number of different SNMP Trap host used to receive messages. Trigger the trap message time: Port Linkup/Linkdown, equipment of cold - start (restart when power supply drop)/warm - start (a warm restart), and RMON set port statistical fluctuation threshold.

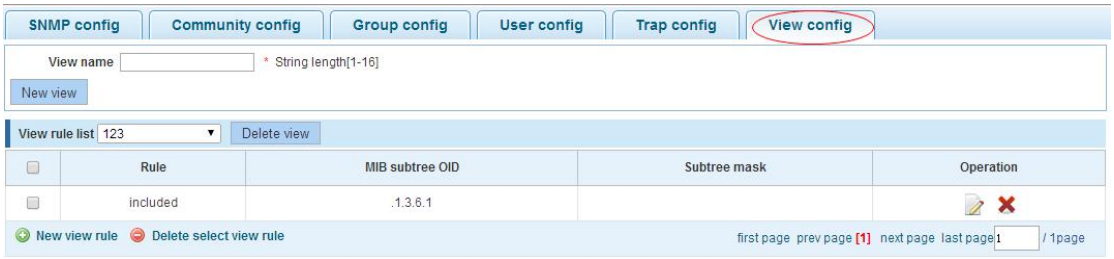
【Configuration Example】

Such as: Setting hoset 192.168.2.30 receive trap information.



4.10.1.6 View config

In the navigation bar to select **"SNMP>SNMP Config>View Config"**, set the view the rules to allow or disable access to some of the MIB object as shown.



【Parameter Description】

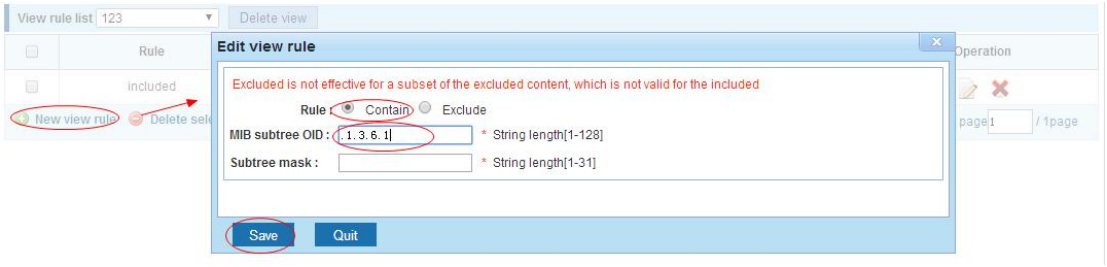
Parameter	Description
View name	View mane
Include	Indicate the MIB object number contained within the view
Exclude	Indicate the MIB object son number was left out of view
MIB subtree OID	View the associated MIB object, is a number of MIB
Subtree mask	MIB OID mask

【Instruction】

Each view is best to configure a view rule, otherwise it will affect the SNMP function.

【Configuration Example】

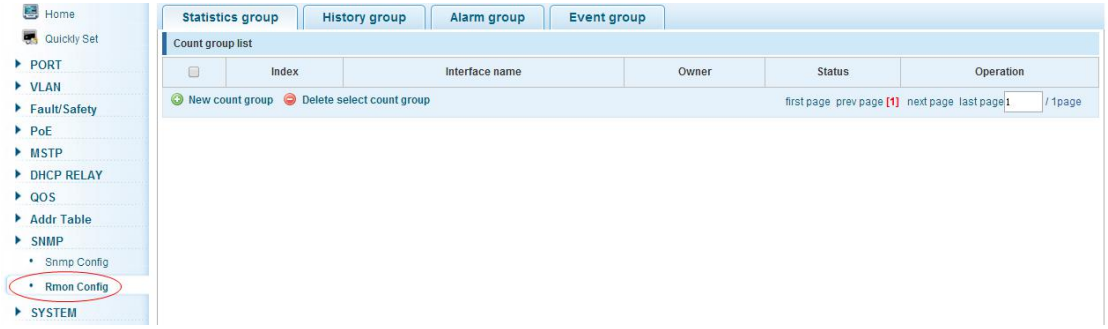
Such as: Establish a view 123, MIB subtree oid 1.3.6.1 contain among them.



4.10.2 Rmon Config

4.10.2.1 Statistics Group

In the navigation bar to select **"SNMP>RMON Config>Statistics Group"**, set an Ethernet interface statistics as shown.



【Parameter Description】

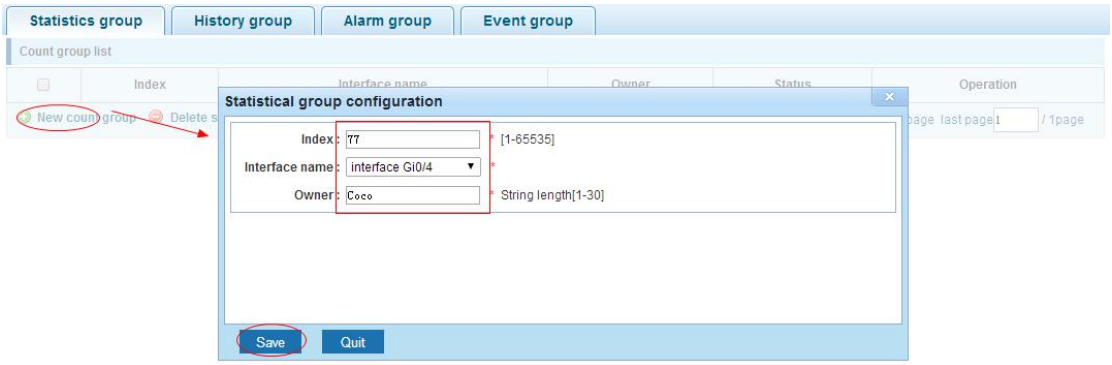
Parameter	Description
Index	The index number, the value range of statistical information table is 1 ~ 65535
Interface mane	To monitor the source port
Ower	Set the table creator, range: 1 ~ 30 characters of a string

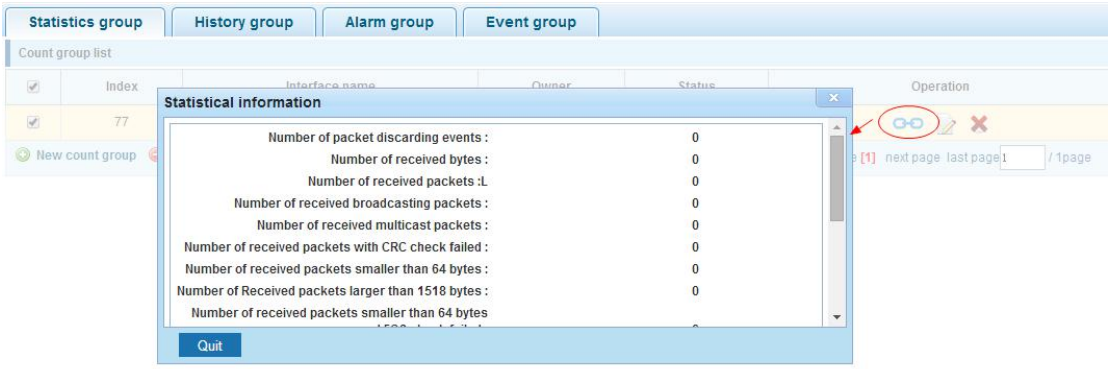
【Instruction】

At the time of configuration RMON SNMP functions must be open, otherwise the prompt dialog box will appear.

【Configuration Example】

Such as: Set up monitoring Ethernet port after 4 to check the data.





4.10.2.2 History Group

In the navigation bar to select **"SNMP>RMON Config>History Group"**, record the history of an Ethernet interface information as shown.

【Parameter Description】

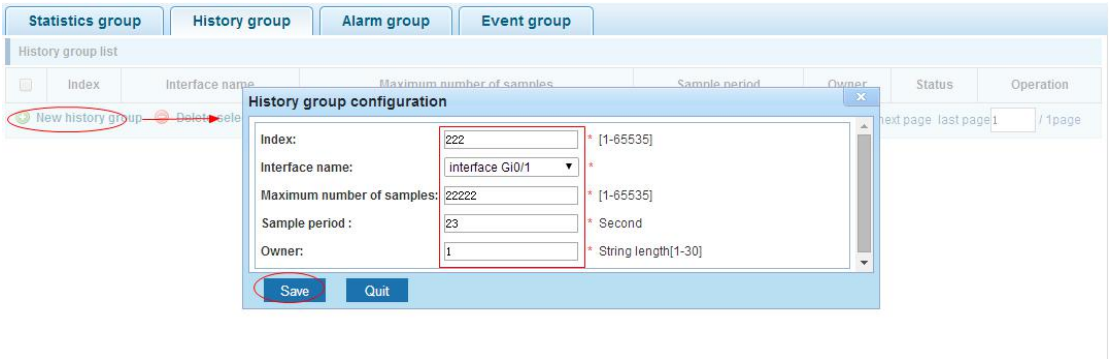
Parameter	Description
index	Historical control table item index number, value range is 1 ~ 65535
Interface name	To record the Ethernet interface
Maximum number of samples	Set the history control table item of the corresponding table capacity, namely the Max for number of records the history table, value range is 1 ~ 65535
Sample period	Set up the statistical period, scope for 5 ~ 3600, the unit is in seconds
owner	Set the table creator, range: 1 ~ 30 characters of a string

【Instruction】

At the time of configuration RMON SNMP functions must be open, otherwise the prompt dialog box will appear.

【Configuration Example】

Such as: Monitor Ethernet port 4 historical information.



4.10.2.3 Alarm Group

In the navigation bar to select **"SNMP>RMON Config>Alarm Group"**, define alarm group as shown.

【Parameter Description】

Parameter	Description
Index	The alarm list items index number, value range is 1 ~ 65535
Static table	Statistical type values :3:DropEvents; 4:Octets; 5:Pkts; 6:BroadcastPkts; 7:MulticastPkts; 8:CRCAlignErrors; 9:UndersizePkts; 10:OversizePkts; 11:Fragments; 12:Jabbers; 12:Collisions; 14:Pkts64Octets; 15:Pkts65to127Octets; 16:Pkts128to255Octets; 17:Pkts256to511Octets; 18:Pkts512to1023Octets; 19:Pkts1024to1518Octets
Statistical index	Set up the corresponding statistics statistical index number, decided to statistics to monitor the port number
Sampling interval	Sampling time interval, the scope for 5 ~ 65535, the unit for seconds
The sampling type	Sample types for the absolute value of sampling, the

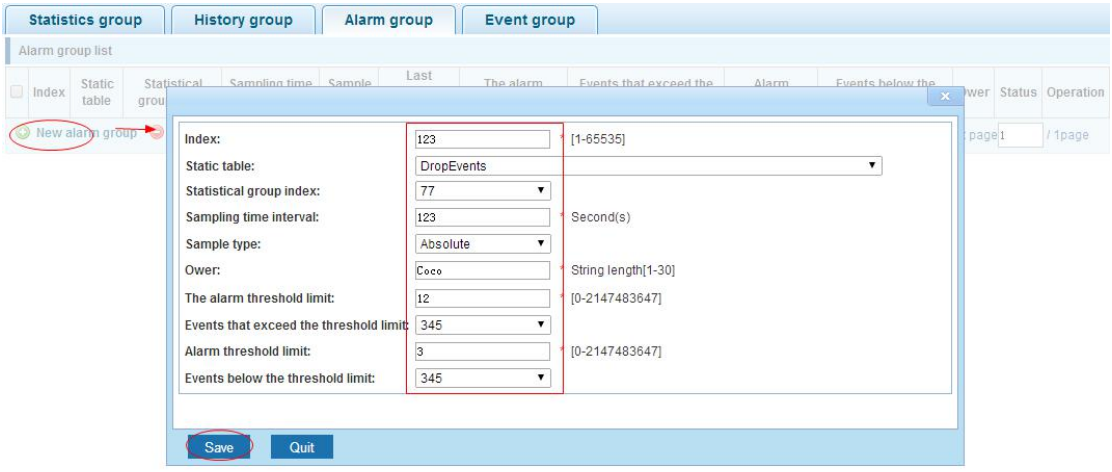
	sampling time arrived directly extracting the value of a variable
The latest sampling	Sampling type for change value sampling, extraction of the arrival of the sampling time is variable in the change of the sampling interval value
The alarm threshold upper limit	Set the upper limit the Parameter values
The alarm threshold lower limit	Set the lower limit Parameter values
Above/below the threshold limit of events	Upper/lower limit reached, for each event
Owner	Set the table creator, ownername for 1 ~ 30 characters of a string

【Instruction】

At the time of configuration RMON SNMP functions must be open, otherwise the prompt dialog box will appear. This configuration need to configure statistics groups and events.

【Configuration Example】

Such as: New statistics group of 77 and the event group 345, set up more than 12 and below the lower limit 3, beyond the scope of alarm.



4.10.2.4 Event Group

In the navigation bar to select **"SNMP>RMON Config>Event Group"**, the way in which define events trigger and record them as shown.

【Parameter Description】

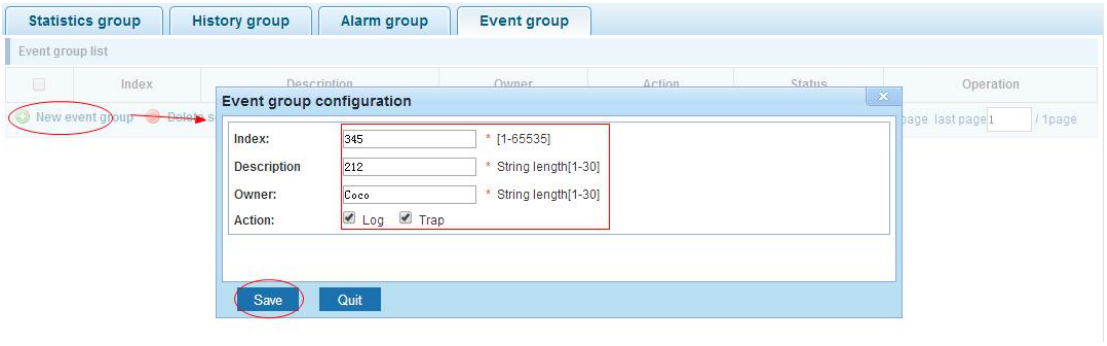
Parameter	Description
Index	The index number, the value range of the event table is 1 ~ 65535
Description	The Trap events, when the event is triggered, the system will send the Trap message Log events, when the event is triggered, the system will log
Owner	Set the table creator, ownername for 1 ~ 30 characters of a string

【Instruction】

At the time of configuration RMON SNMP functions must be open, otherwise the prompt dialog box will appear.

【Configuration Example】

Such as: Create an event to trigger 345, the system sends the trap message and log.



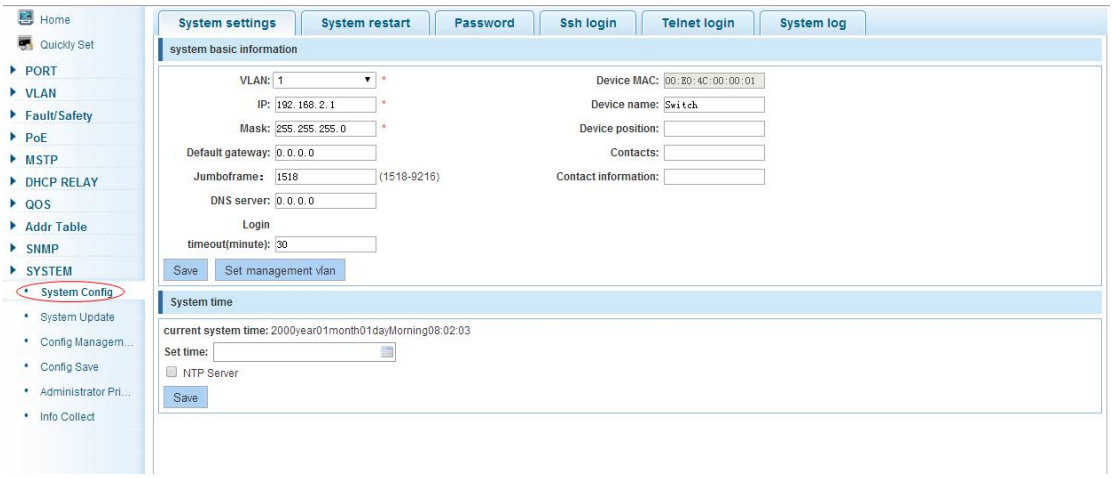
4.11 System

In the navigation bar to select **"System"**, you can set to the **System Config, System Update, Config Management, Config Save, Administor Privileges** and **Info Collect**.

4.11.1 System Config

4.11.1.1 System settings

In the navigation bar to select **"System>System Config>System settings"**, basic information set switch as shown.

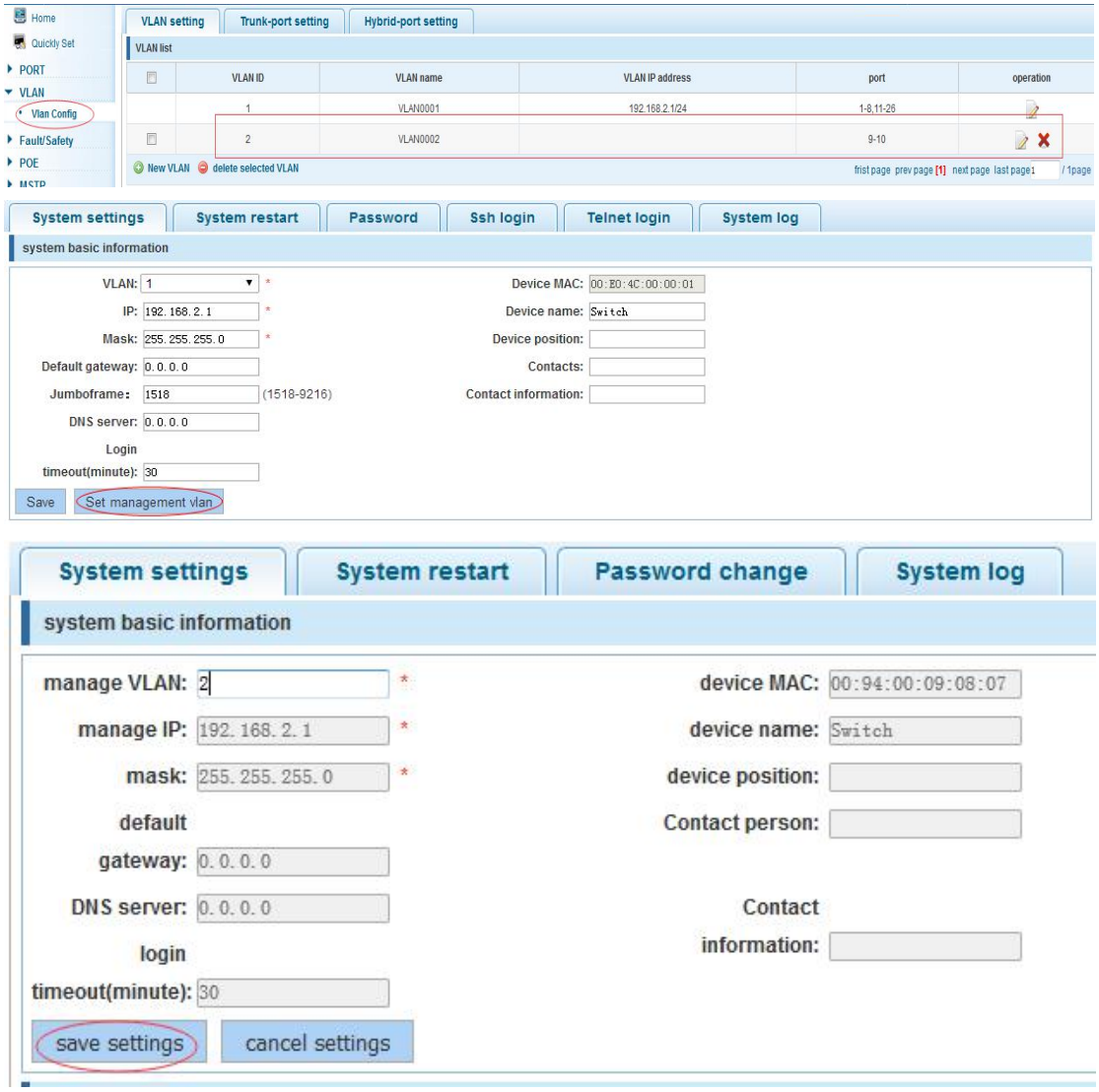


【Parameter Description】

Parameter	Description
Device name	Switch name
Manage VLAN	Switches use VLAN management
Manage ip	Switch IP address management
Timeout	Don't use more than login timeout after login to log in again

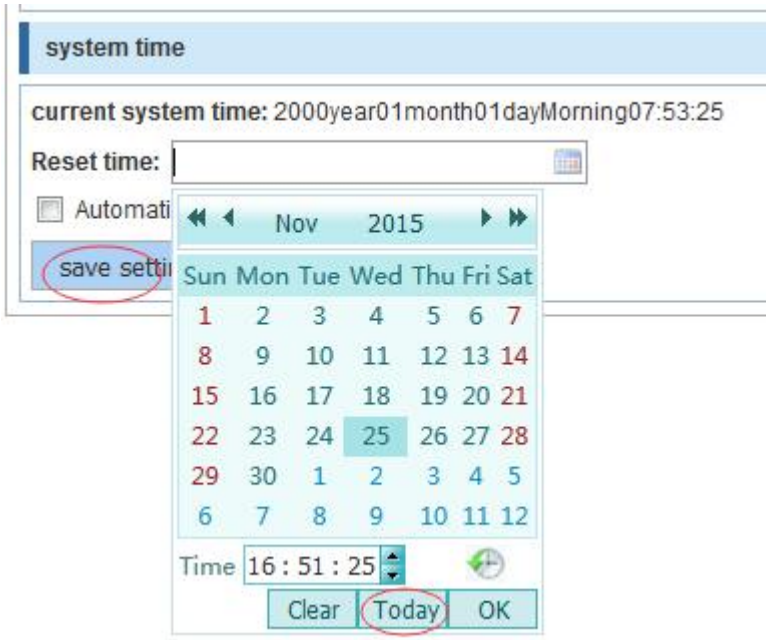
【Configuration Example】

Such as: 1) Set up the VLAN 2 is management VLAN, should first created VLAN 2 the VLAN Settings, and set a free port in the VLAN 2.



2) Insert the PC interface 9 or 10 ports, set up the management IP for 192.168.2.12, device name is yoyo, timeout for 20 minutes.

3) Use 192.168.1.12 logging in, sets the system time.



4.11.1.2 System restart

In the navigation bar to select **"System Config>System restart"**, equipment can be restarted as shown.

【Instruction】

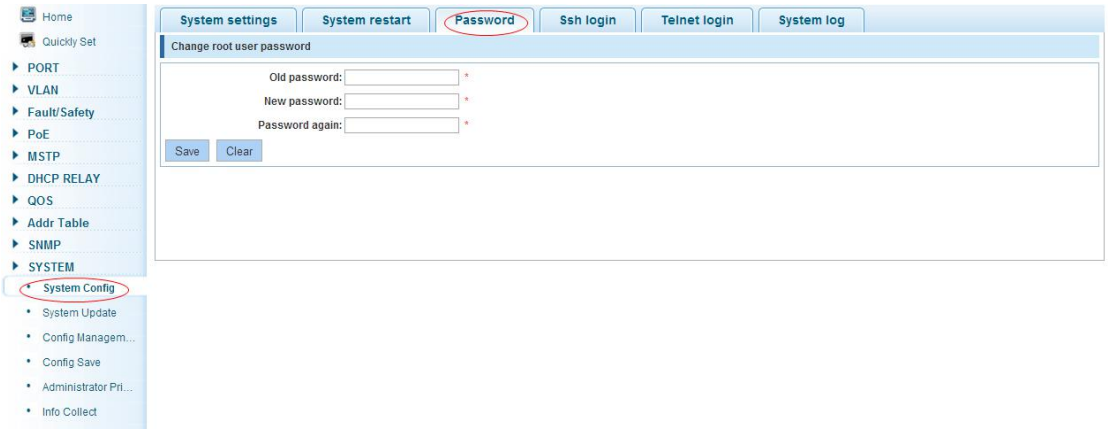
Click the button to restart the switch.The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after device restart.

【Configuration Example】

Such as: Click "restart" button.

4.11.1.3 Password

In the navigation bar to select **"System Config>Password",** the password change to equipment as shown.



【Instruction】

1. If you set a new Web login password, then log in again after seting the new password.
2. Password can not contain Chinese, full-width characters, question marks and spaces.
3. If forget the password reset, can be reset in the console.

switch(config) # password admin.
New Password:3456.
Confirm Password:3456.

【Configuration Example】

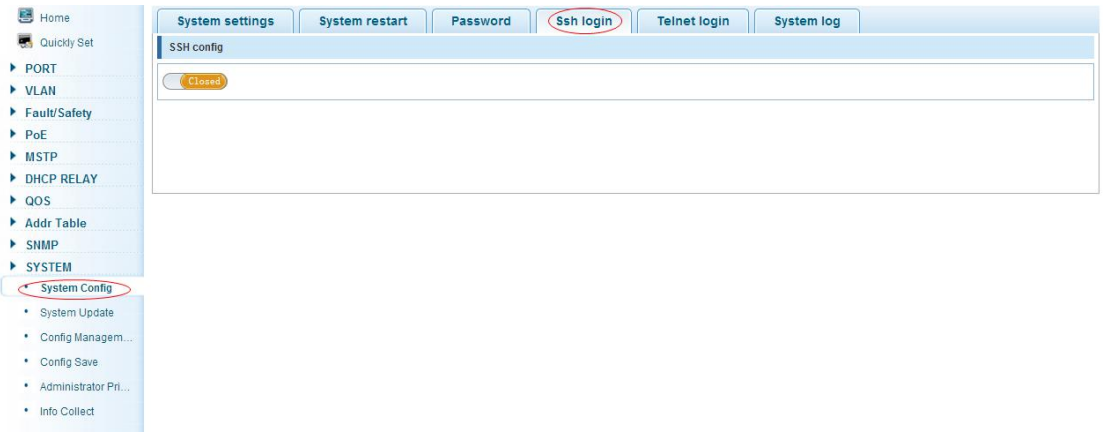
Such as: Amend the password to 1234.

4.11.1.4 SSH login

In the navigation bar to select **"System Config>SSH login"**, equipment can be restarted as shown.

【Instruction】

Configure the user through the SSH login device to be turned on to enable the switch.

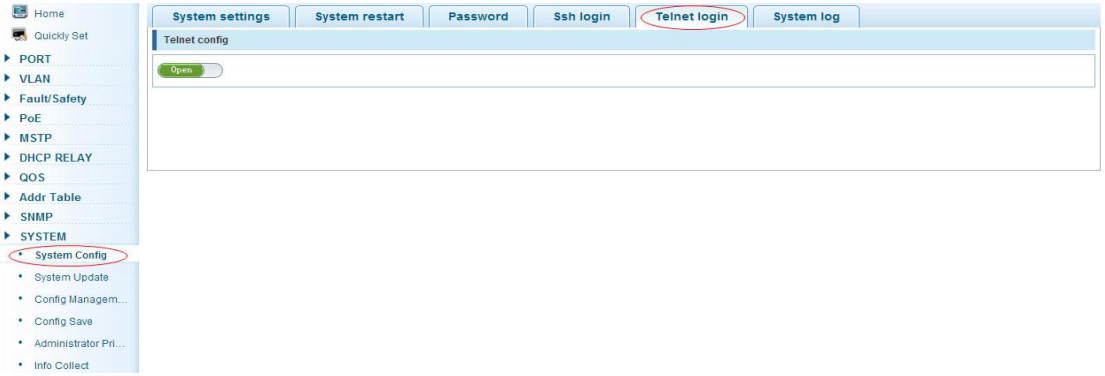


【Configuration Example】

Such as: the SSH open, CRT can be used to log on.

4.11.1.5 Telnet login

In the navigation bar to select **"System Config>Telnet login"**, equipment can be restarted as shown.



【Instruction】

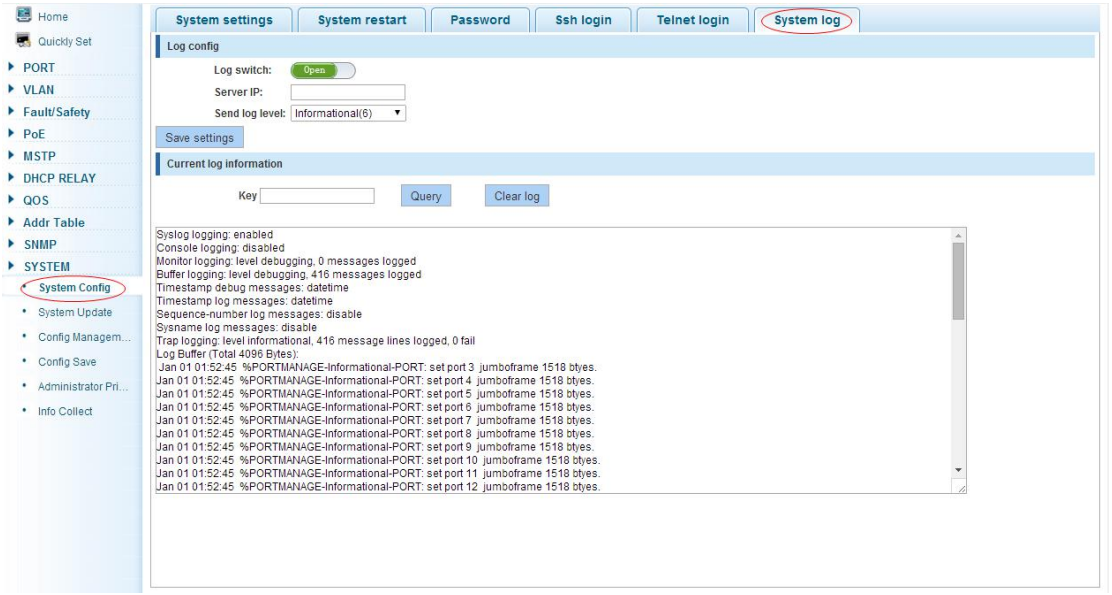
Configure the user through the Telnet login device to be turned on to enable the switch.

【Configuration Example】

Such as: Telnet will open, the computer Telnet function opens, can be logged on.

4.11.1.6 System log

In the navigation bar to select **"System Config>system log"**, to view the log and set up the log server as shown.



【Parameter Description】

Parameter	Description
Log switch	Open and close
Server IP	Appoint to server address
Send log level	0-7
key	Enter the required query of characters

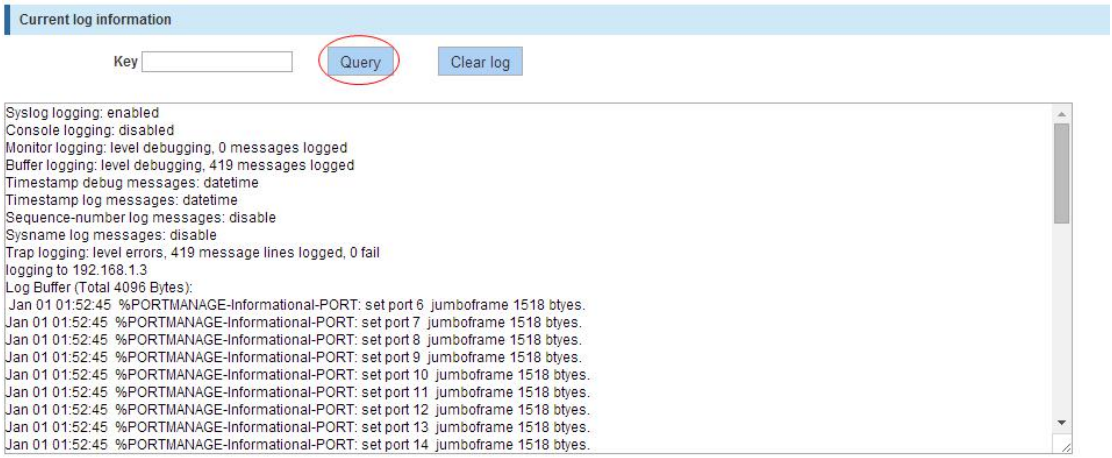
【Instruction】

Open log switch, set up the syslog server, system log will automatically be pushed to the server.

【Configuration Example】

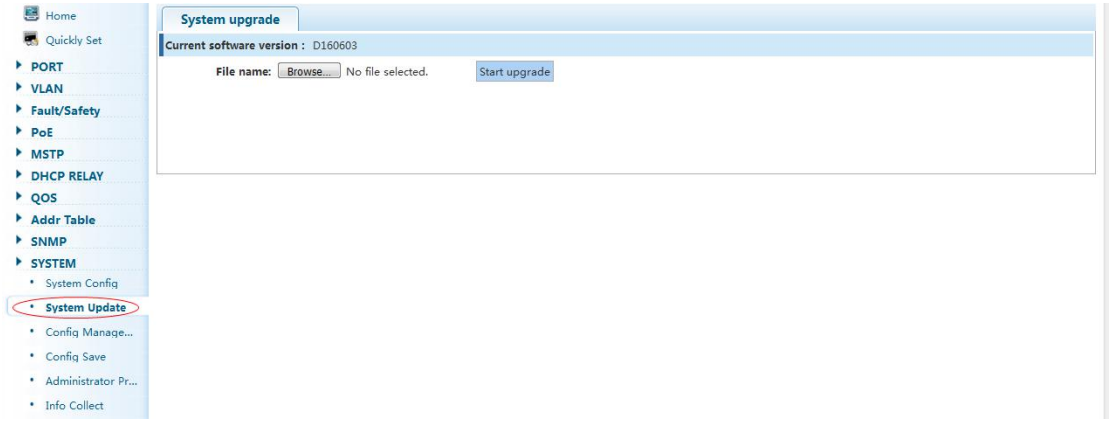
Such as: 1) The error log information in 192.168.1.3 pushed to the server.

2) Input the Mac keywords, click "query" button, click on the "clear log" button, can clear the log.

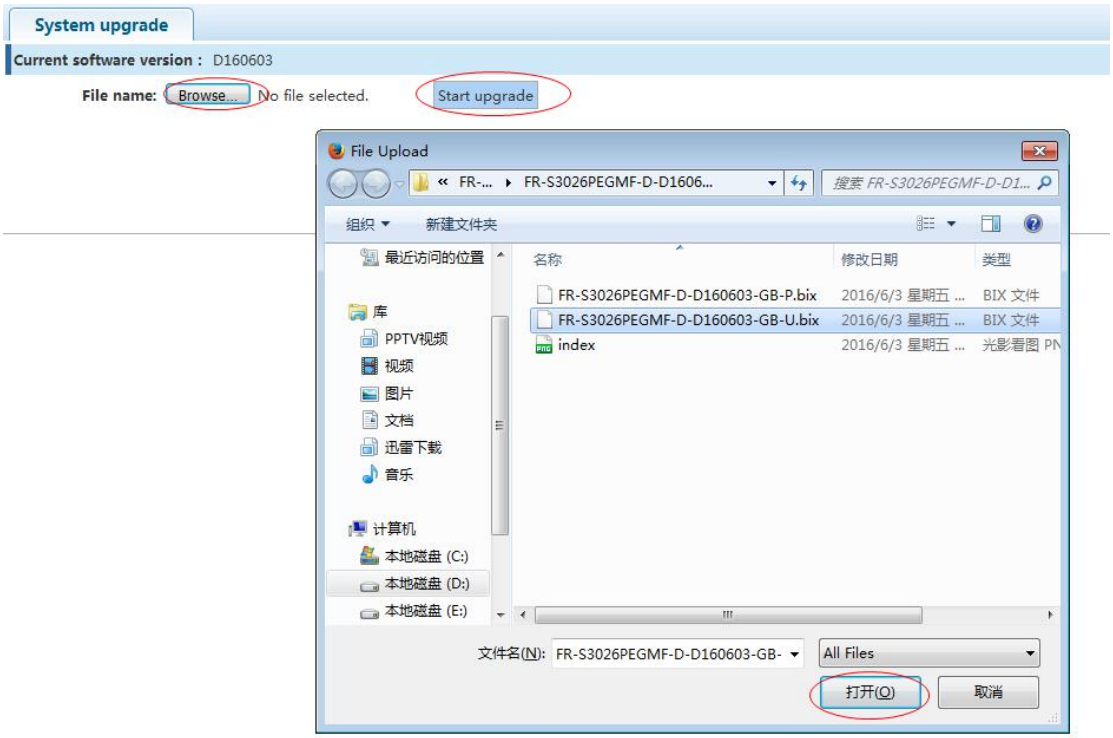


4.11.2 System Upgrade

In the navigation bar to select **"System>System Upgrade"**. Optional upgrade file to upgrade as shown.



Such as: select the file to upgrade.



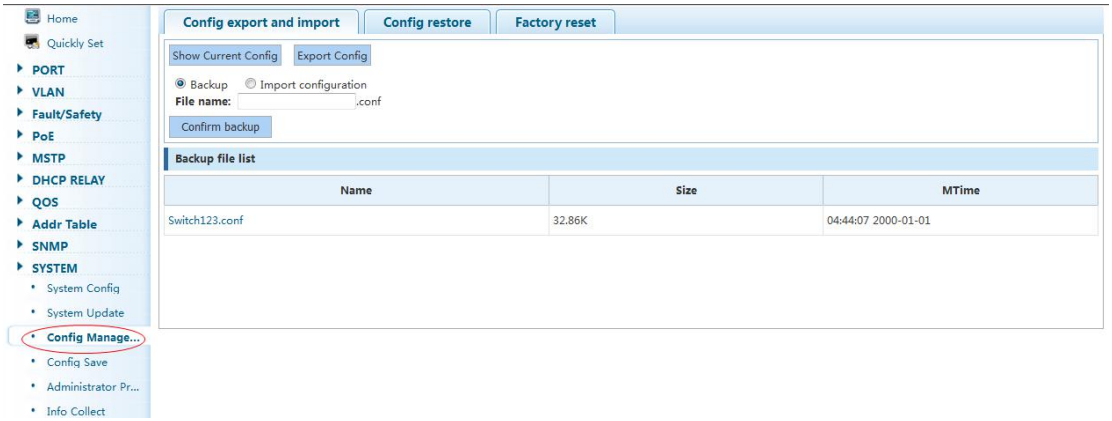
【Instruction】

1. Please confirm that the upgraded version of the same model and the same model.
2. In the upgrade process, you may encounter flash to make the page is temporarily unable to respond to the page, this time can not power off or restart the device, until prompted to upgrade successfully!

4.11.3 Config Management

4.11.3.1 Current configuration

In the navigation bar to select **"System>Config Management>Current configuration"**, can import and export configuration files, the backup file as shown.

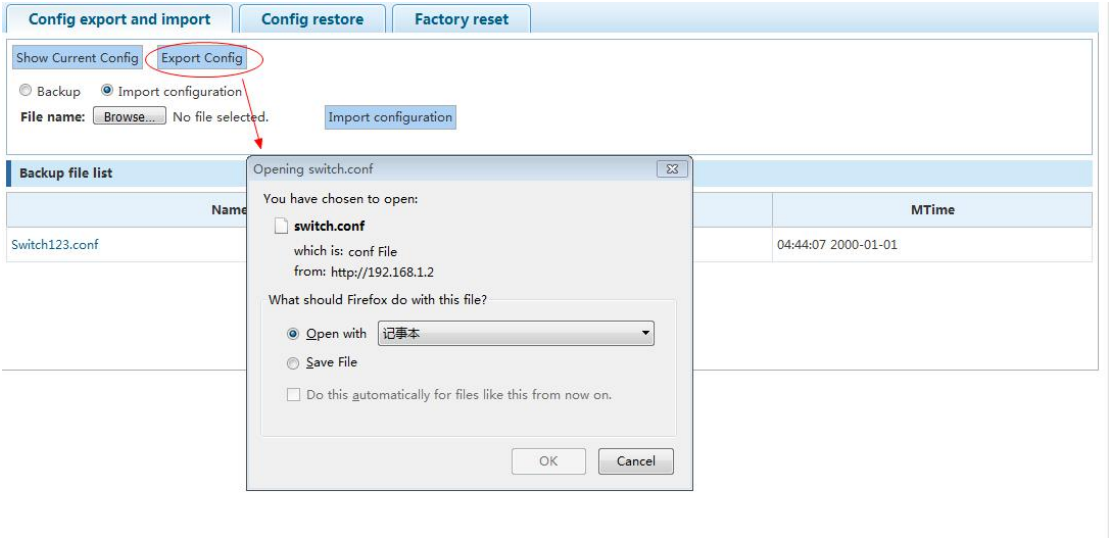


【Instruction】

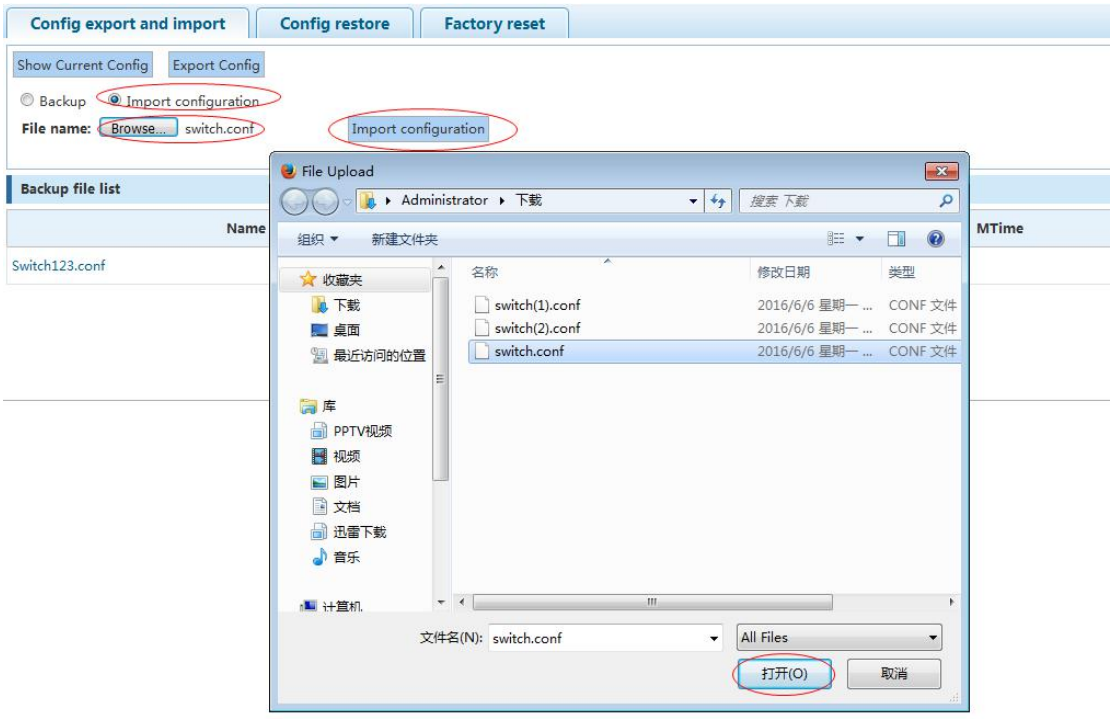
Import process can not be closed or refresh the page, or import will fail!
After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect.

【Configuration Example】

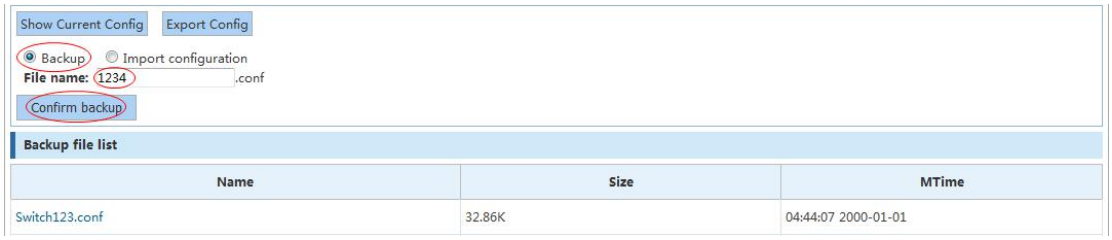
Such as: 1) In the configuration first save the page, click save configuration to save the current configuration, then export the configuration.



2) import configuration.

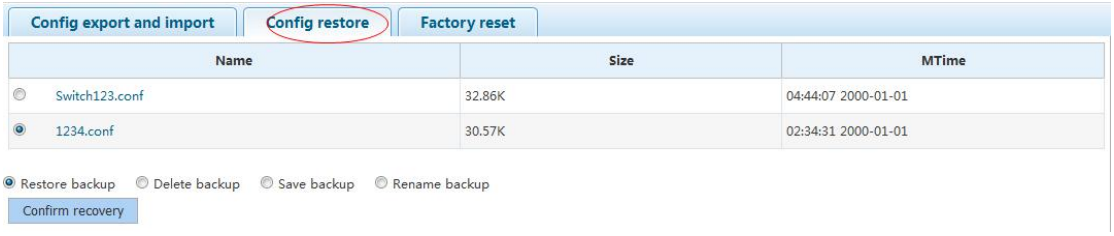


3) backup.



4.11.3.2 Configuration backup

In the navigation bar to select **"System>Config Management>Configuration backup"**, you can configure backup file as shown.

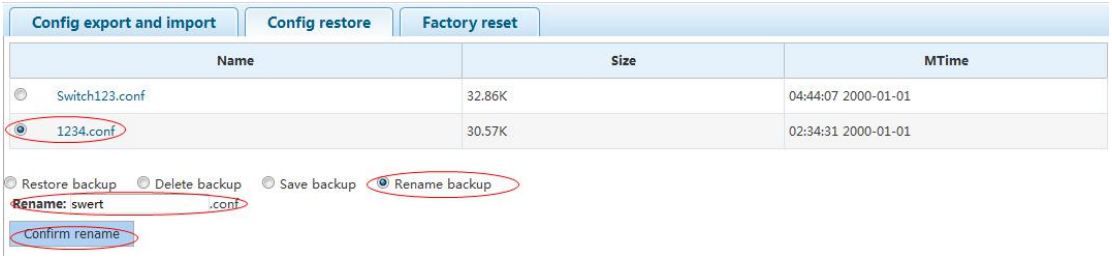


【Instruction】

Operating this page should be in the current configuration page first, the backup file.

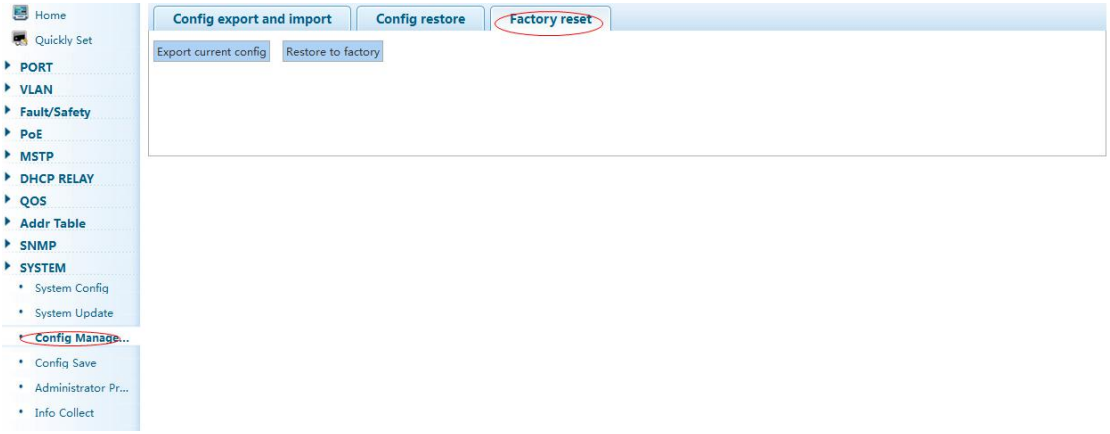
【Configuration Example】

Such as: Restore backup.



4.11.3.3 Restore factory configuration

In the navigation bar to select **"System>Config Management>Restore factory configuration",** can export the current configuration and restore factory configuration as shown.

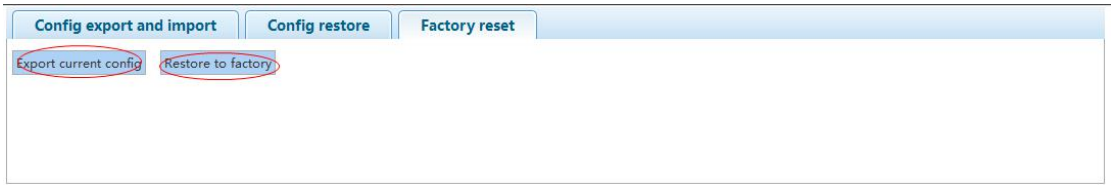


【Instruction】

Restore the factory configuration, will delete all the current configuration. If you have any useful configuration, the current system can lead the factory configuration again after the current configuration.

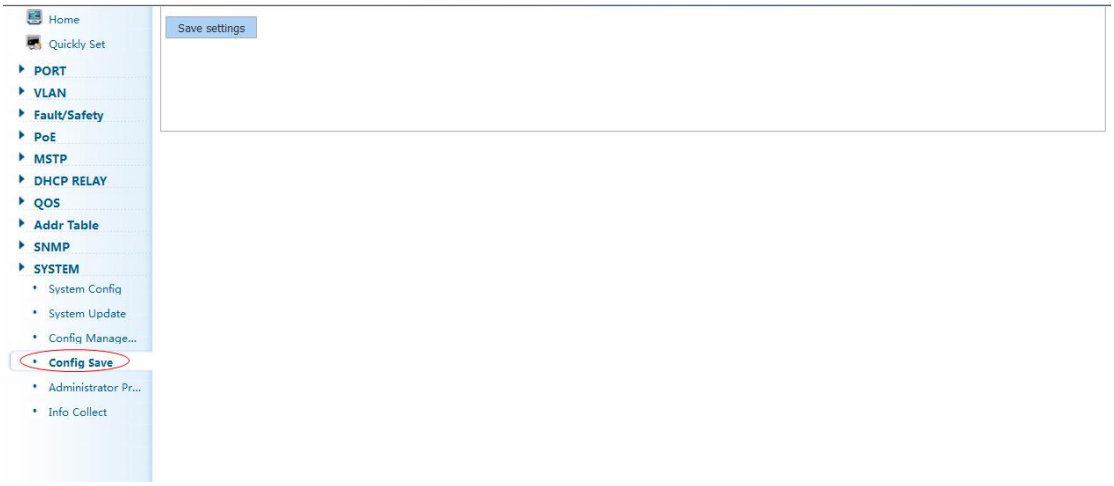
【Configuration Example】

Such as: Restore configuration can be the guide before they leave the current configuration.



4.11.4 Config Save

In the navigation bar to select **"System>Config Save"**, you can save current configuration as shown.

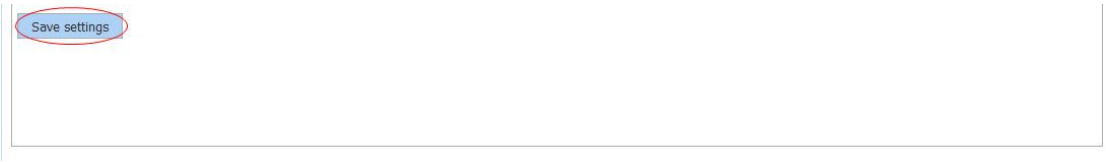


【Instruction】

Save settings will delete all default configurations. If there are useful configurations, click backup Configurations before save the settings.

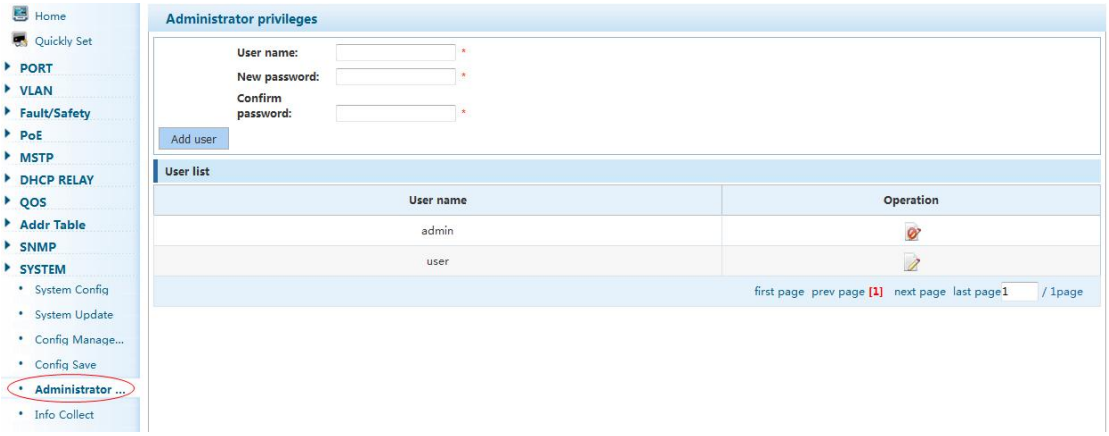
【Configuration Example】

Such as: Click "save settings" button.



4.11.5 Administrator Privileges

In the navigation bar to select **"System>Administrator Privileges"**, configurable ordinary users as shown.

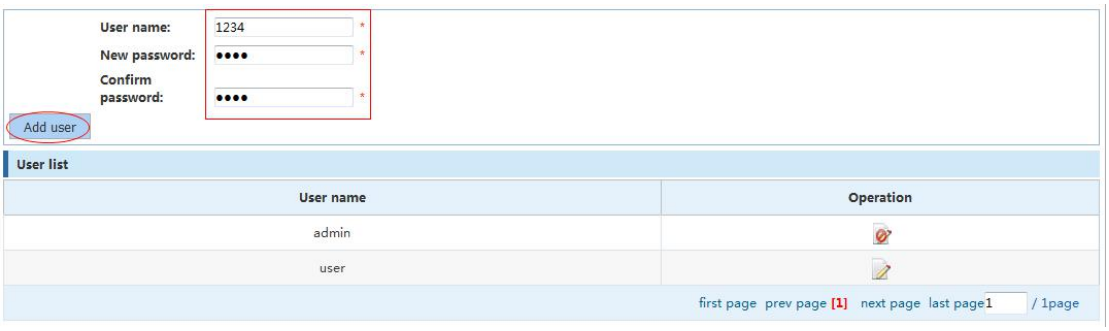


【Instruction】

Only the admin of the super administrator can access this page is used to manage users and visitors. The user can log in the Web management system of equipment for routine maintenance. In addition to the admin and user, can add up to five users. Ordinary users can only access information system home page.

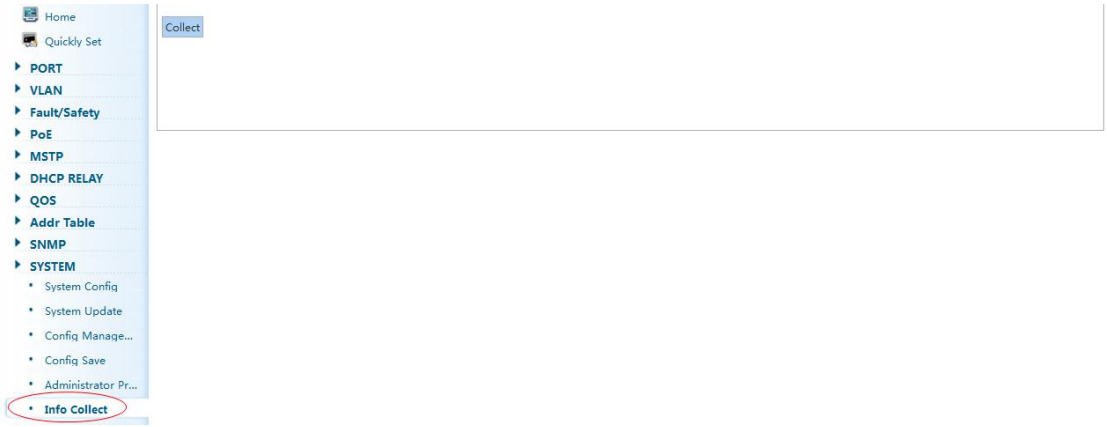
【Configuration Example】

Such as:



4.11.6 Info Collect

In the navigation bar to select **"System>Info Collect"**, you can collect to the system debug information as shown.

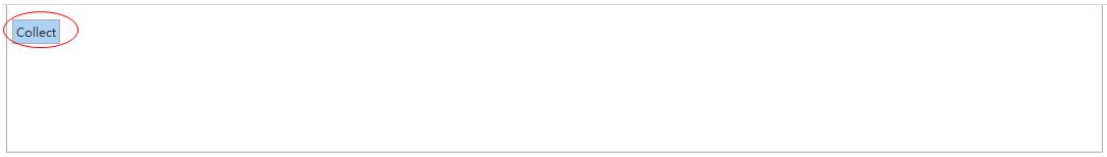


【Instruction】

Collect useful information, it may take a few moment.

【Configuration Example】

Such as: Click on "collect" button.



Appendix: Technical Specifications

Hardware Features		
Standards		IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3z, IEEE 802.3at, IEEE 802.3af, IEEE 802.1q, IEEE 802.1p
Network Media (Cable)		10Base-T: UTP category 3, 4, 5 cable (maximum 100m) 100Base-Tx: UTP category 5, 5e cable (maximum 100m) 1000Base-T: UTP category 5e, 6 cable (maximum 100m) 1000Base-SX:62.5 μm/50 μm MMF(2m~550m) 1000Base-LX:62.5 μm/50 μm MMF(2m~550m) or 10 μm SMF(2m~5000m)
Number of Ports		24 x 10/100/1000Mbps Auto-Negotiation ports 2 x 100/1000Mbps SFP ports 1x Console port
Transfer Method		Store-and-Forward
Switching Capacity		52G
MAC Address Learning		8K
Packet Forwarding Rate		38.69Mpps
Packet Buffer		4.1Mbit
Jumbo Frame		9216Bytes
PoE Ports(RJ45)		24* PoE ports compliant with 802.3at/af
PoE Budget		380W
Power Pin Assignment		1/2(+),3/6(-)
Indicators	Per Device	Power,System
	Per Port	Link/Activity/Speed, PoE
Frame Filtering and Forward Rate		10Mbps: 14880pps 100Mbps: 148800pps 1000Mbps: 1488000pps
Dimensions (L × W × H)		440*208*44 mm
Power Supply		100~240VAC,50/60HZ,400W internal power
Power consumption		Maximum(PoE on): 435W (220V/50Hz)
Environment		Operating Temperature: 0℃~50℃ Storage Temperature: -40℃~70℃ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~90% non-condensing

Software Specification	
Basic function	Ethernet Setup STP/RSTP/MSTP Storm-control Port Monitor Port rate-limit MAC filtering
Three layers of functional	The ARP deception, the network cheating Filtering the IP port Static binding IP and MAC Arp trust port Static routing capacity Ping and Traceroute
The security policy	ACE capacity ACL QoS DAI
VLAN	Port based VLAN 802.1Q VLAN
Safety features	Radius Tacacs+ Preventing DOS attacks dot1x The gateway ARP deception
Application protocol	DHCP Relay DHCP snooping DHCP Client FTP/TFTP
Management	HTTP WEB Telnet SSH Console
Other function	LLDP IGMP Snooping SNMPV1,V2c,V3 RMON(1,2,3,9)
POE Management	POE Status Power supply management mode(auto/energy/static) The port priority