MORRELL®

A TRUSTED GERMAN NAME

SW-MNG-24GE2GSFP

24-Port 10/100/1000Mbps + 2-Port Gigabit SFP Managed Ethernet Switch

User Manual

Version 1.1 | 10/22/2016

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

The Web Smart Ethernet Switch provides the seamless network connection. This device integrates 1000Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package. With 24-10/100/1000Mbps Auto-Negotiation RJ45 ports, all ports support Auto MDI/MDIX function. The Switch with a low-cost, easy-to-use, high per-formance upgrade your old network to a 1000Mbps Gigabit network. It is essential to helping solve network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources.

The switch is easy to install and use. It requires no configuration and installation. It is a great selection for office network.

1.2 Features

- Comply with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, EEE802.3ad standards
- Supports IEEE802.3x flow control for Full-duplex Mode and back pressure for Half-duplex Mode
- Supports MAC address auto-learning and auto-aging
- Store and forward mode operates
- Support SNMP/RMON/TELENT
- Supports IEEE802.1Q VLAN,4K VLAN Table
- Support IEEE802.1p Priority Queues
- Support ACL Function, 1.5K-entry ALC table
- Support Storm Control
- Support QoS、Port Mirroring、Link Aggregation Protocol
- LED indicators for monitoring power, link/activity
- Web-based Management Support
- Internal power adapter supply

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 SFP ports,1 x Console port, 1 x Reset button and a series of LED indicators as shown as below.

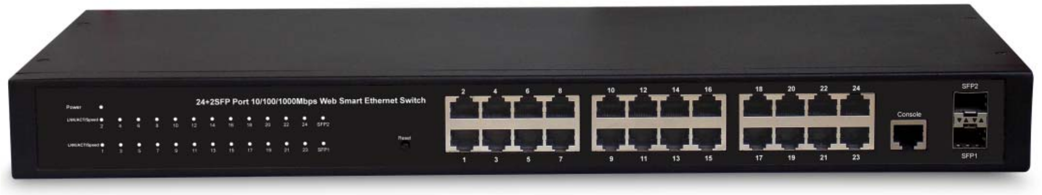


Figure 1 - Front Panel

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.

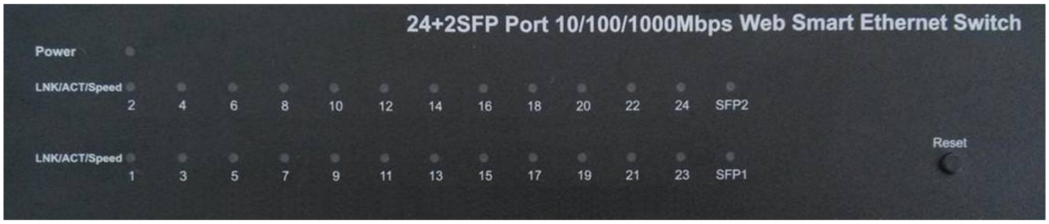

24+2SFP Port 10/100/1000Mbps Web Smart Ethernet Switch
Power
LNK/ACT/Speed
2 4 6 8 10 12 14 16 18 20 22 24 SFP2
LNK/ACT/Speed
1 3 5 7 9 11 13 15 17 19 21 23 SFP1
Reset

Figure 2 - LED Indicators

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

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Red	On	Power On
		Off	Power Off
LNK/ACT/ Speed (1~24)	10/100Mbps: Amber	On	A device is connected to the port
	1000Mbps: Green	Off	A device is disconnected to the port
		Flashing	Sending or receiving data
SFP1 SFP2	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

1.3.2 Rear Panel

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

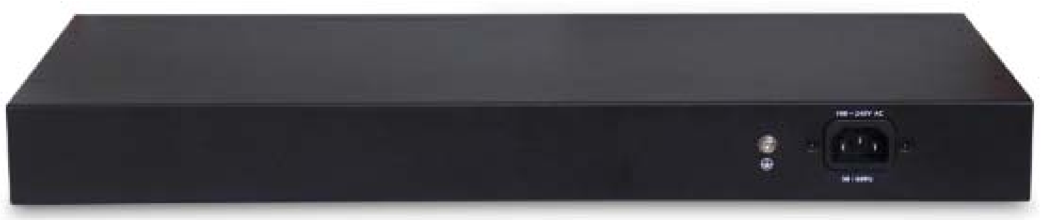


Figure 3 - Rear Panel

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 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 Web Smart 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.

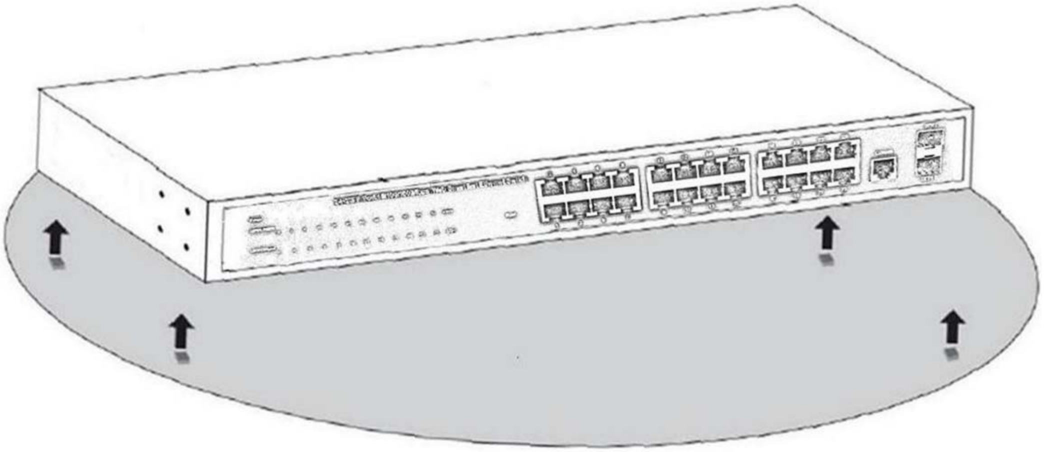


Figure 4 - Desktop Installation

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.

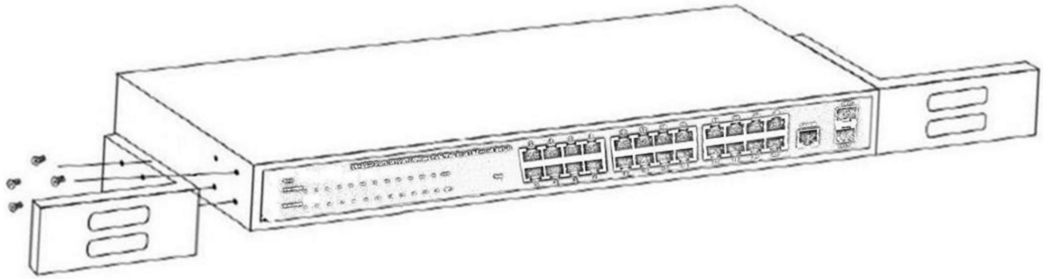


Figure 5 - Bracket Installation

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

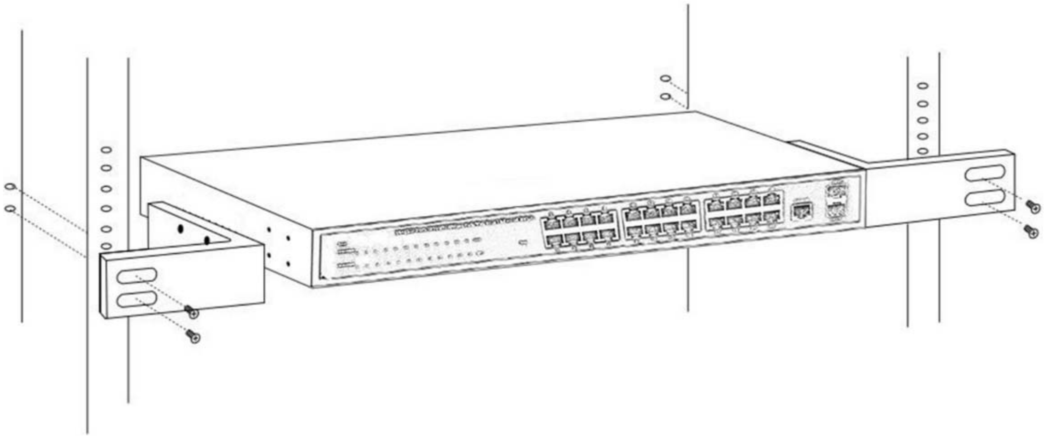


Figure 6 - Rack Installation

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.

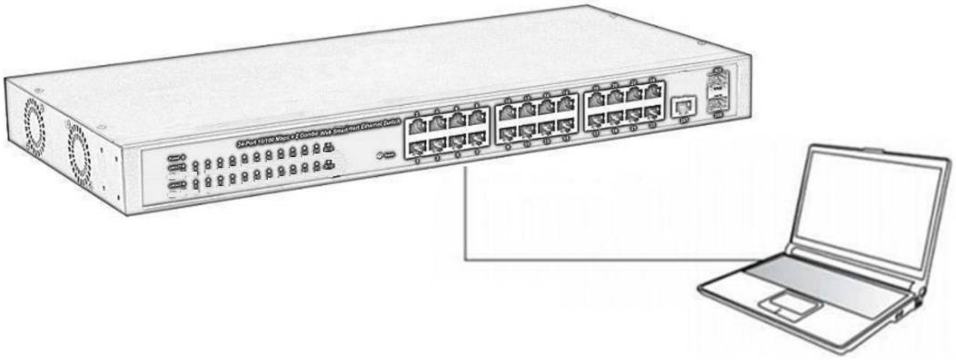
2.2 Connect Computer (NIC) to the Switch

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 Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. Switch ports will automatically adjust to the characteristics(MDI/MDI-X, speed, duplex) of the device to which is connected.



Please refer to the LED Indicator Specification. The LNK/ACT/Speed LEDs for each port lights on when the link is available.

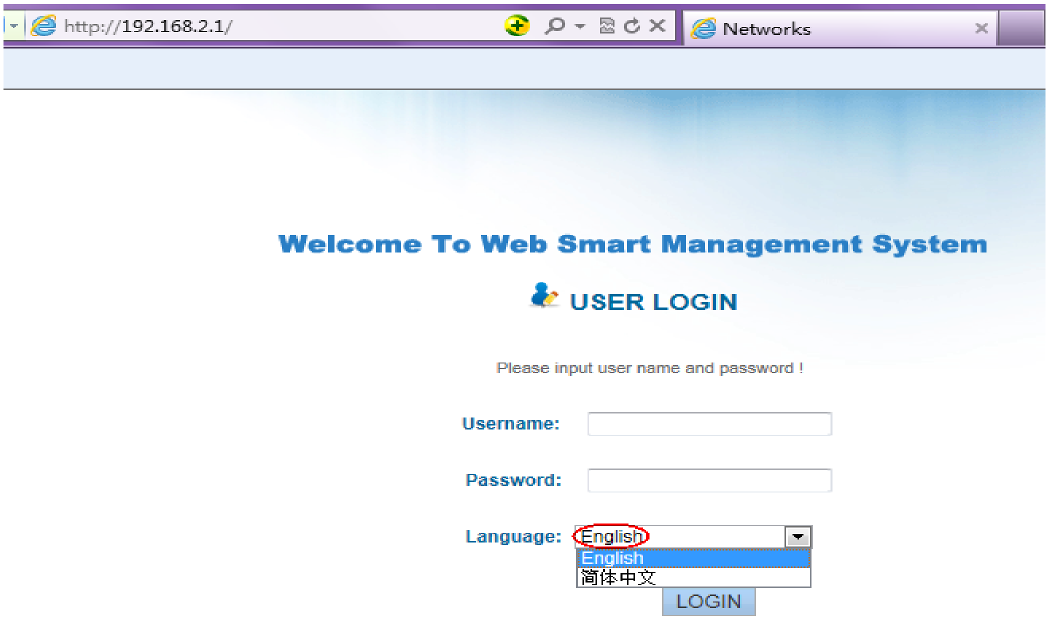
3.2 How to Login the Switch

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:



Welcome To Web Smart Management System

USER LOGIN

Please input user name and password !

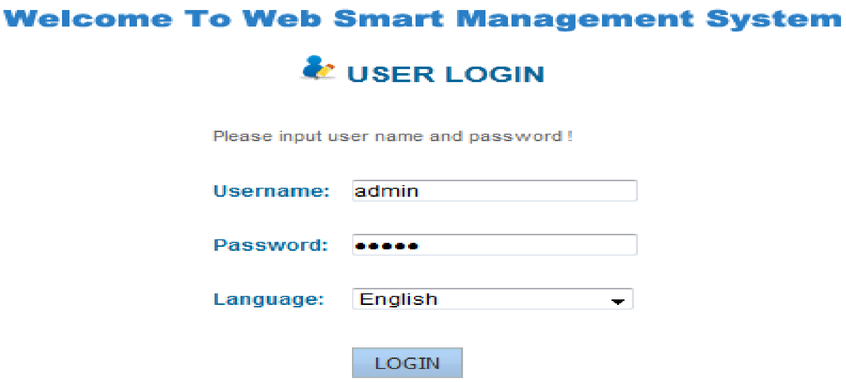
Username:

Password:

Language: English

Figure 7- Login Windows

5. Switching language to english .Enter the Username and Password (The factory default Username is **admin** and Password is **admin**), and then click “login” to log in to the Switch configuration window as below.



Welcome To Web Smart Management System

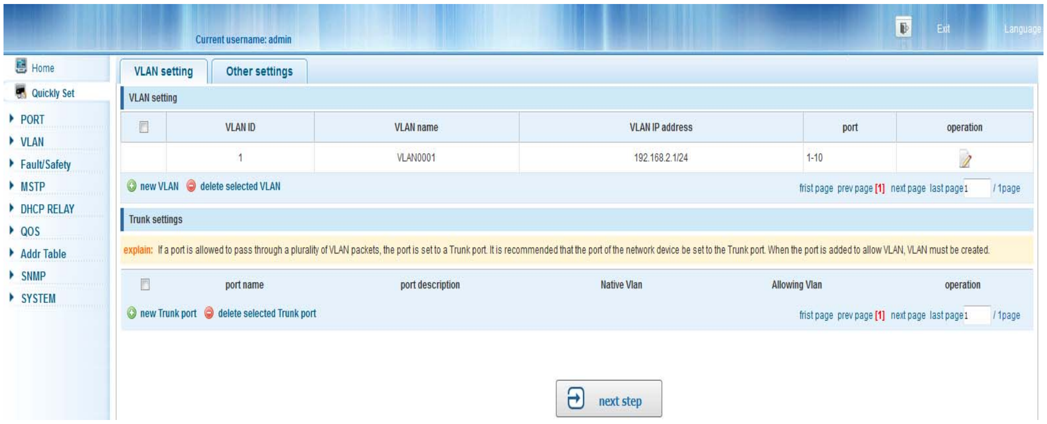
USER LOGIN

Please input user name and password !

Username: admin

Password: •••••

Language: English



Current username: admin

VLAN setting

□	VLAN ID	VLAN name	VLAN IP address	port	operation
	1	VLAN0001	192.168.2.1/24	1-10	

Trunk settings

explain: If a port is allowed to pass through a plurality of VLAN packets, the port is set to a Trunk port. It is recommended that the port of the network device be set to the Trunk port. When the port is added to allow VLAN, VLAN must be created.

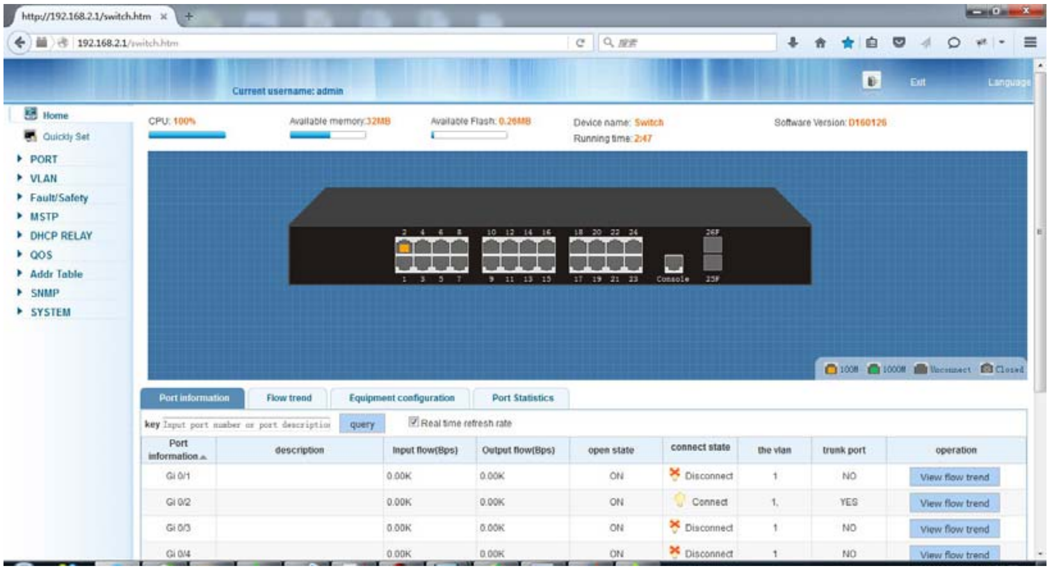
□	port name	port description	Native Vlan	Allowing Vlan	operation

new Trunk port
delete selected Trunk port
frist page prev page [1] next page last page 1 / 1page
next step

Chapter 4 Switch Configuration

The Web Smart Ethernet 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, software version.The middle shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.



Current username: admin

CPU: 100%

Available memory:32MB

Available Flash: 0.26MB

Device name: Switch

Running time: 2:47

Software Version: D160126

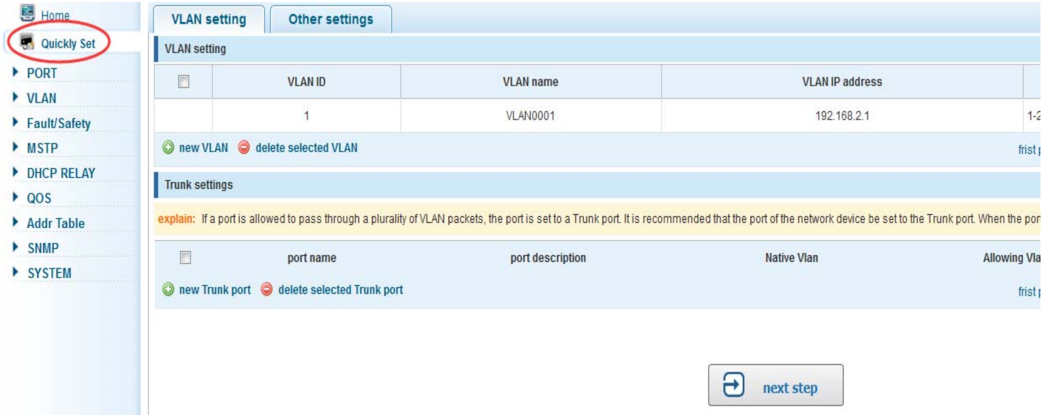
key Input port number or port description

☑ Real time refresh rate

Port information	description	Input flow(Bps)	Output flow(Bps)	open state	connect state	the vlan	trunk port	operation
Gi 0/1		0.00K	0.00K	ON	Disconnect	1	NO	View flow trend
Gi 0/2		0.00K	0.00K	ON	Connect	1,	YES	View flow trend
Gi 0/3		0.00K	0.00K	ON	Disconnect	1	NO	View flow trend
Gi 0/4		0.00K	0.00K	ON	Disconnect	1	NO	View flow trend

4.1 Quickly setting

In the navigation bar to select **"quickly setting"**, can create a VLAN in this module, add the port in the VLAN ,set the basic information and modify the switch login password. the following picture:



VLAN setting

☐	VLAN ID	VLAN name	VLAN IP address	
	1	VLAN0001	192.168.2.1	1-2

Trunk settings

explain: If a port is allowed to pass through a plurality of VLAN packets, the port is set to a Trunk port. It is recommended that the port of the network device be set to the Trunk port. When the por

☐	port name	port description	Native Vlan	Allowing Vla

【parameter description】

parameter	description
VLAN ID	VLAN number,24GE default VLAN 1
VLAN name	VLAN mark
Manage IP	Manage the IP address of the VLAN
device name	Switch name
Manage VLAN	Switches management in use of the VLAN

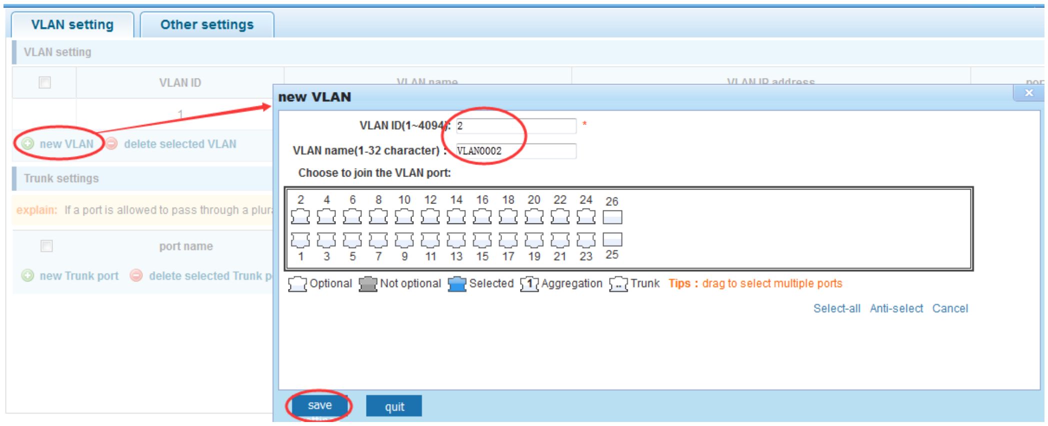
【instructions】

Native VLAN: as a Trunk, the mouth 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 mouth of the list to limit the flow of some VLAN can't through the Trunk.

【Configuration example】

1） VLAN setting：such as create VLAN 2 ,Sets the port 8 to Trunk ,Native VLAN 2

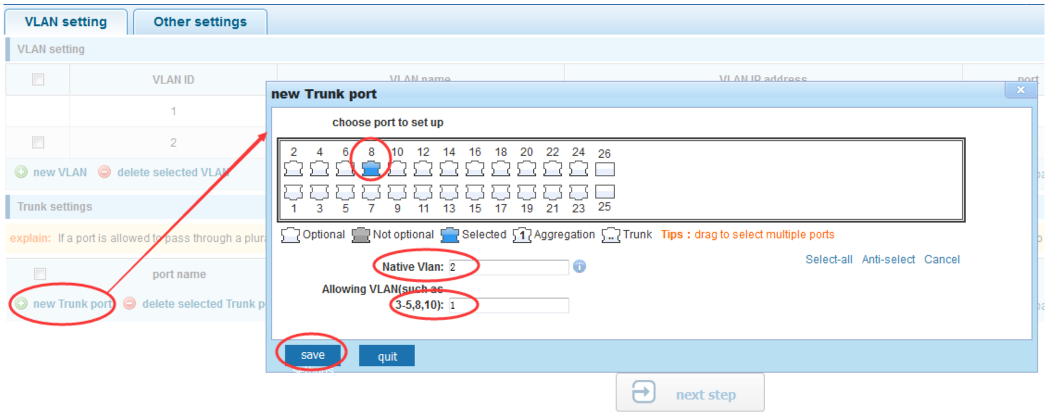


new VLAN

VLAN ID(1~4094): 2 *

VLAN name(1-32 character) : VLAN0002

Choose to join the VLAN port:



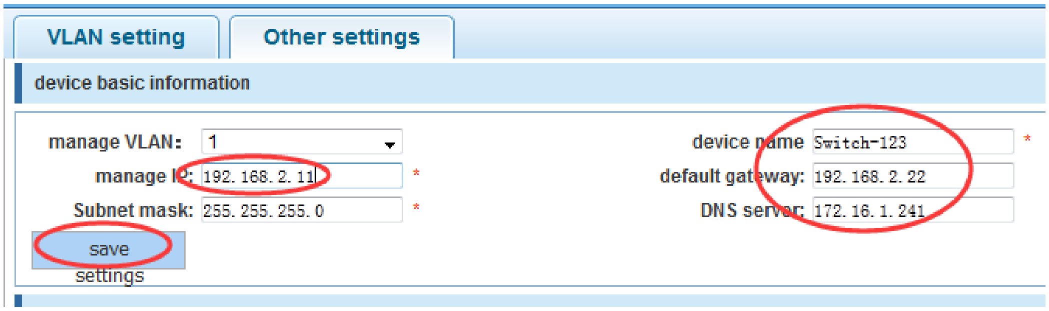
new Trunk port

choose port to set up

Native Vlan: 2

Allowing VLAN(such as 3-5,8,10): 1

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 with the dns server set as 172.16.1.241



device basic information

manage VLAN: 1

manage IP: 192. 168. 2. 11 *

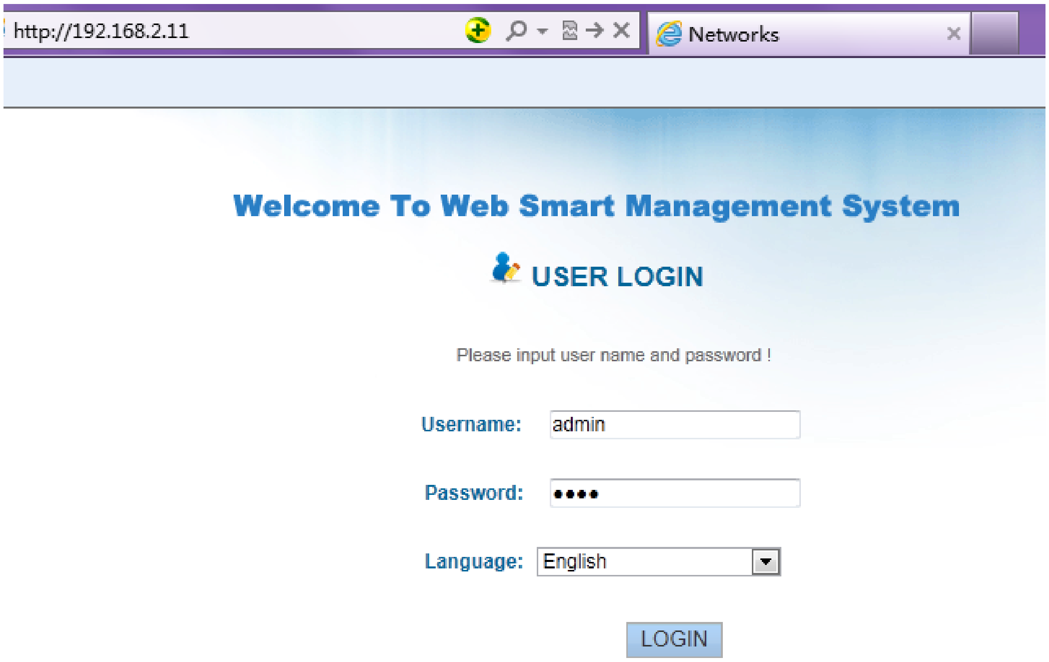
Subnet mask: 255. 255. 255. 0 *

device name Switch-123 *

default gateway: 192. 168. 2. 22

DNS server: 172. 16. 1. 241

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



http://192.168.2.11

Welcome To Web Smart Management System

USER LOGIN

Please input user name and password !

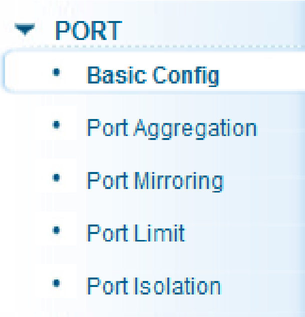
Username: admin

Password: ●●●●

Language: English

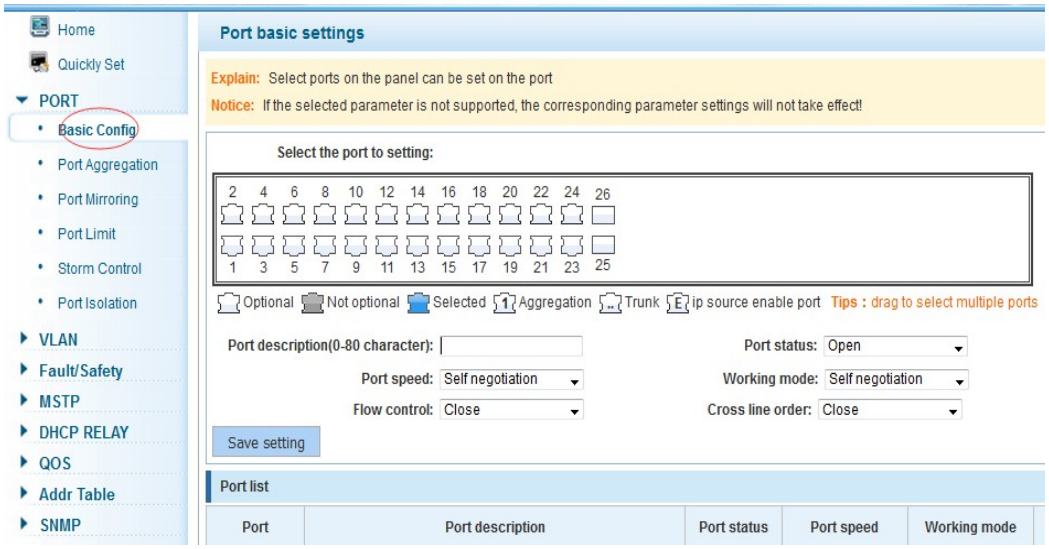
4.2 PORT

In the navigation bar to select **“PORT”**,You may conduct **basic config, port aggregation, port mirroring , port limit** 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, the following picture:



Explain: Select ports on the panel can be set on the port

Notice: If the selected parameter is not supported, the corresponding parameter settings will not take effect!

Select the port to setting:

Tips : drag to select multiple ports

Port description(0-80 character):

Port status: Open

Port speed: Self negotiation

Working mode: Self negotiation

Flow control: Close

Cross line order: Close

Port	Port description	Port status	Port speed	Working mode

【parameter description】

parameter	description
port	Select the current configuration port number
port status	Choose whether to close link port
flow control	Whether open flow control

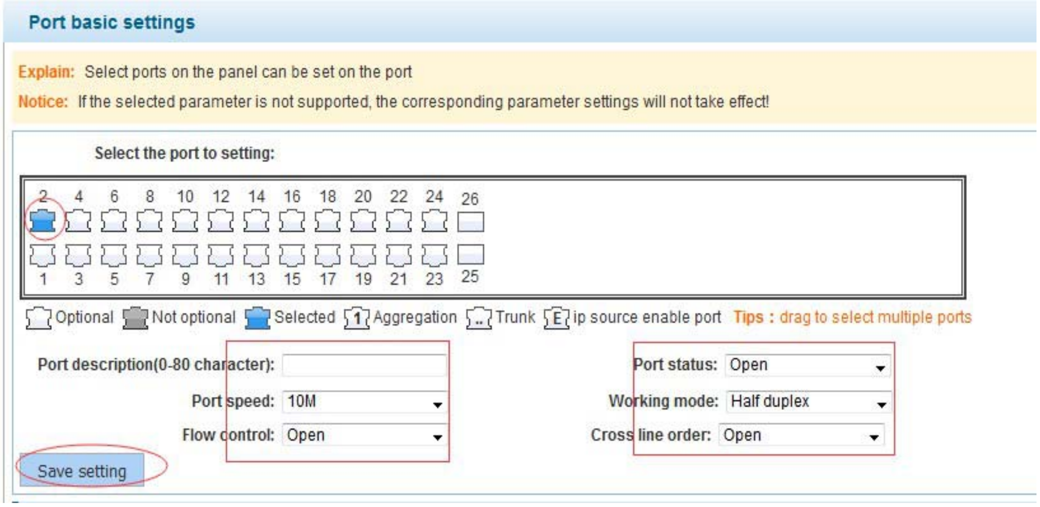
port speed	Can choose the following kinds: Aggregation 10 M 100 M 1000 M
working mode	Can choose the following kinds: Self negotiated 10 M 100 M 1000 M
port described	The port is described
Cross line sequence	Whether open intersection line sequence

【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 10 M, half duplex, open flow control and cross line sequence and port state



Port basic settings

Explain: Select ports on the panel can be set on the port

Notice: If the selected parameter is not supported, the corresponding parameter settings will not take effect!

Select the port to setting:

Port description(0-80 character):

Port speed: 10M

Flow control: Open

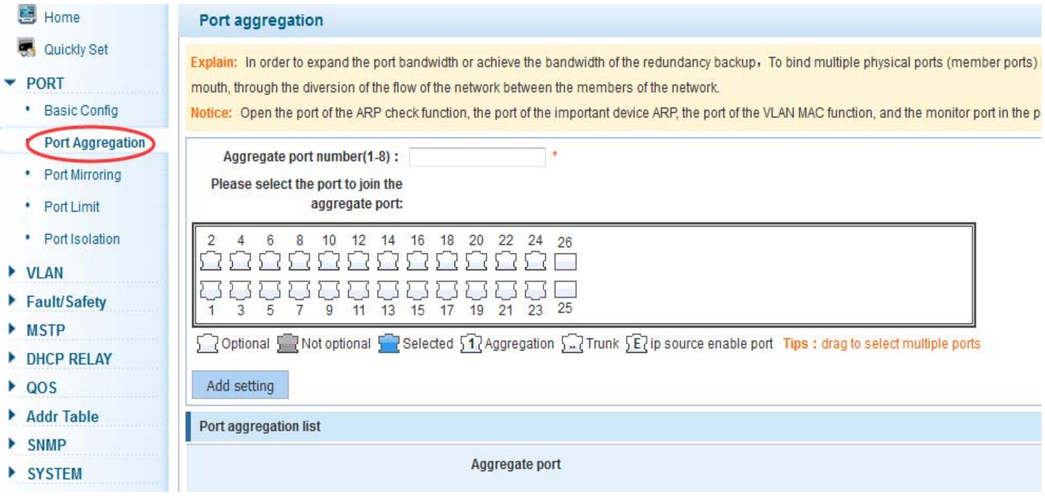
Port status: Open

Working mode: Half duplex

Cross line order: Open

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,the following picture:



Port aggregation

Explain: In order to expand the port bandwidth or achieve the bandwidth of the redundancy backup，To bind multiple physical ports (member ports) mouth, through the diversion of the flow of the network between the members of the network.

Notice: Open the port of the ARP check function, the port of the important device ARP, the port of the VLAN MAC function, and the monitor port in the p

Aggregate port number(1-8) : *

Please select the port to join the aggregate port:

Tips : drag to select multiple ports

Port aggregation list

【parameter description】

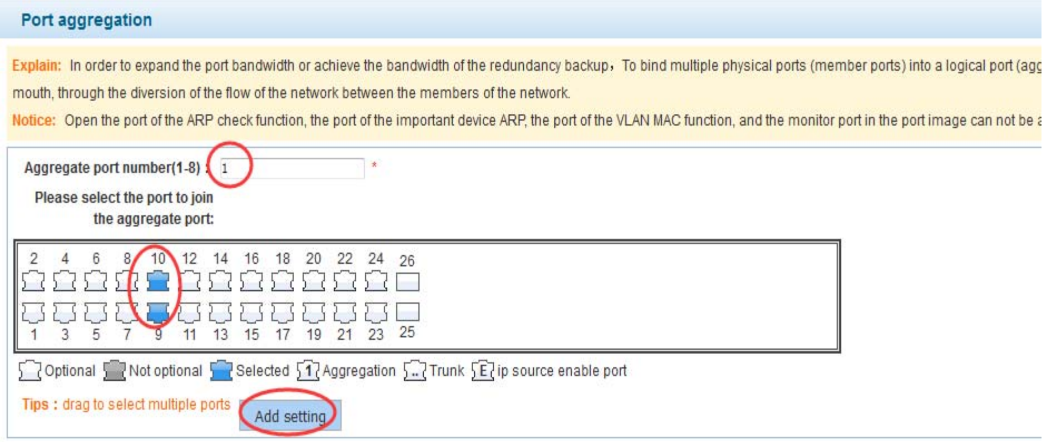
parameter	description
Aggregation port	26GE switch can be set up eight link trunk group, group_1 to group_8
Member port	For each of the members of the group and add your own port, and with members of other groups

【instructions】

Open the port of the ARP check function, the port of the important device ARP, the port of the VLAN MAC function, and 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 .



Port aggregation

Explain: In order to expand the port bandwidth or achieve the bandwidth of the redundancy backup，To bind multiple physical ports (member ports) into a logical port (agg mouth, through the diversion of the flow of the network between the members of the network.

Notice: Open the port of the ARP check function, the port of the important device ARP, the port of the VLAN MAC function, and the monitor port in the port image can not be a

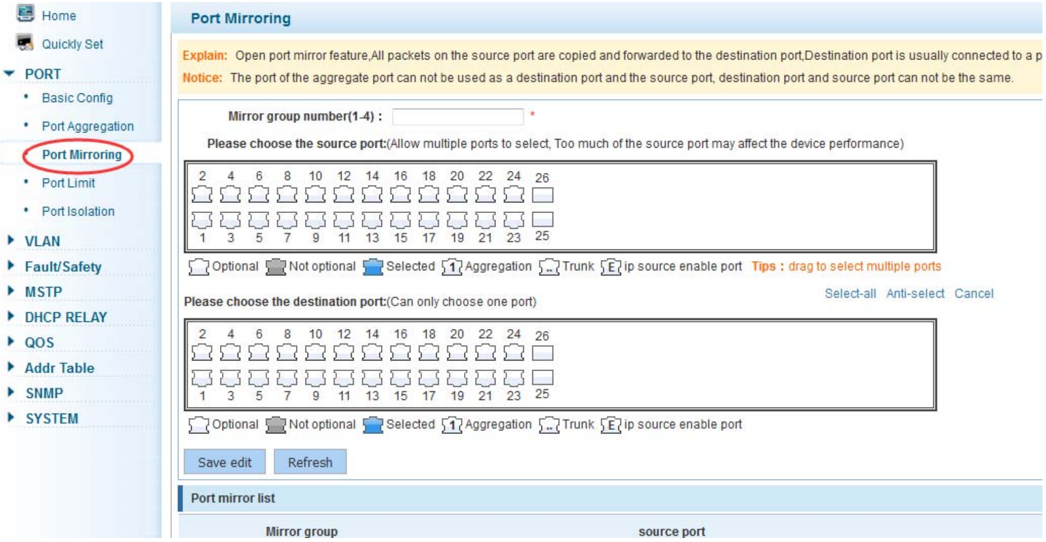
Aggregate port number(1-8) : 1 *

Please select the port to join the aggregate port:

Tips : drag to select multiple ports

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,the following picture:



Port Mirroring

Explain: 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 p

Notice: 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.

Mirror group number(1-4) : *

Please choose the source port:(Allow multiple ports to select, Too much of the source port may affect the device performance)

Please choose the destination port:(Can only choose one port)

Port mirror list

Mirror group	source port

【parameter description】

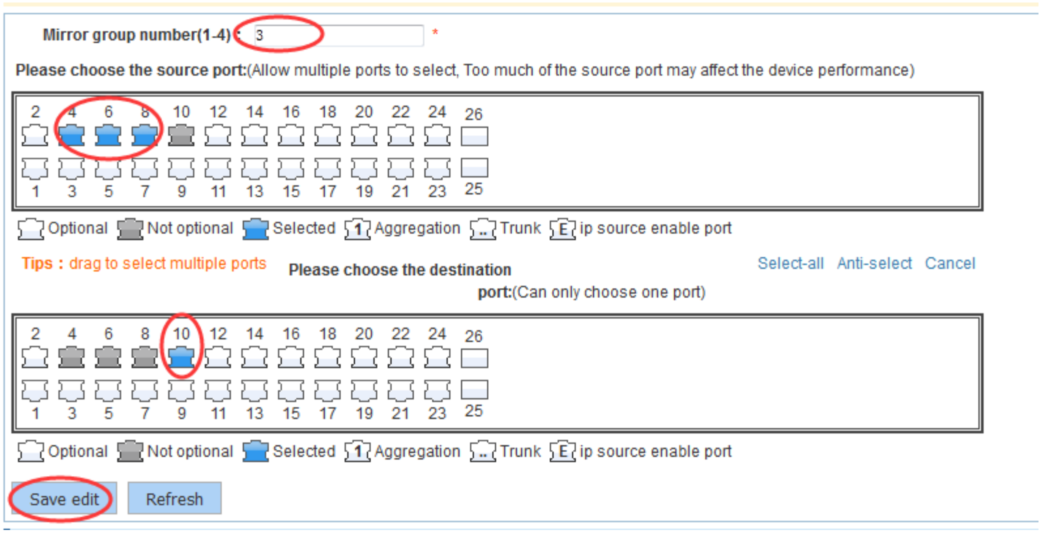
parameter	**description**
Source port	To monitor the port in and out of flow
Destination port	Set destination port,All packets on the source port are copied and forwarded to the destination port
Mirror group	Range :1-4

【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



Mirror group number(1-4): 3 *

Please choose the source port:(Allow multiple ports to select, Too much of the source port may affect the device performance)

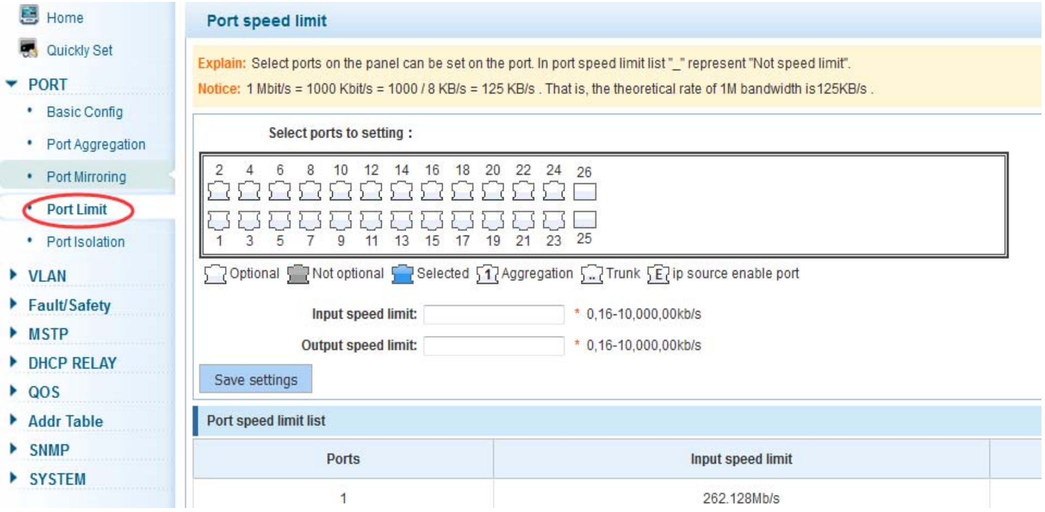
Tips：drag to select multiple ports

Please choose the destination port:(Can only choose one port)

4.2.4 Port rate-limit

In the navigation bar to select **“PORT>port rate-limit** ”,

To port output, input speed limit,the following picture:



Port speed limit

Explain: Select ports on the panel can be set on the port. In port speed limit list "_" represent "Not speed limit".

Notice: 1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is125KB/s .

Select ports to setting :

Input speed limit: * 0,16-10,000,00kb/s

Output speed limit: * 0,16-10,000,00kb/s

Port speed limit list

Ports	Input speed limit
1	262.128Mb/s

【parameter description】

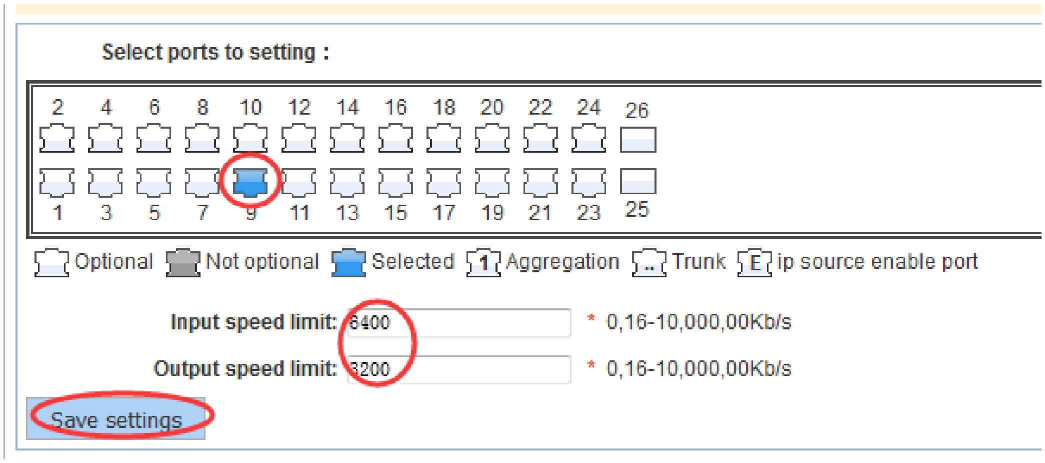
parameter	description
Input speed limit	Set port input speed
Output speed limit	Set port output speed

【instructions】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is125KB/s .

【Configuration example】

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



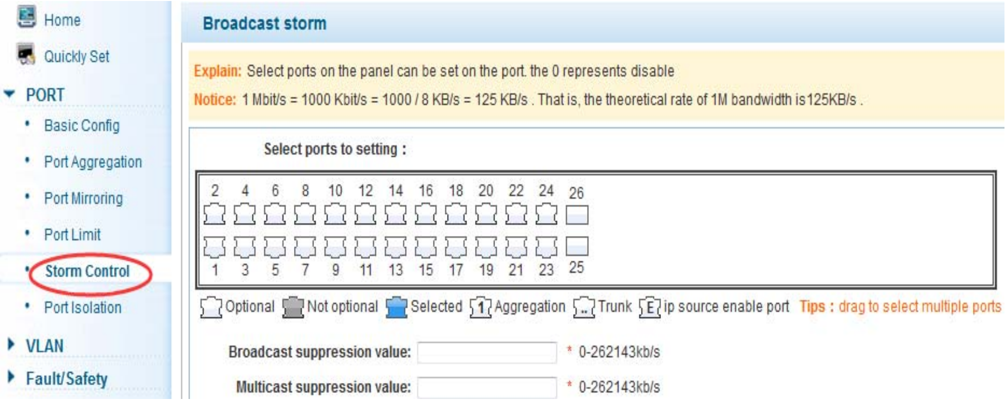
Input speed limit: 6400 * 0,16-10,000,00Kb/s

Output speed limit: 3200 * 0,16-10,000,00Kb/s

4.2.5 Storm control

In the navigation bar to select **“PORT>Storm control”**,

To port storm control config,the following ficture:



Explain: Select ports on the panel can be set on the port. the 0 represents disable

Notice: 1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is125KB/s .

Broadcast suppression value: * 0-262143kb/s

Multicast suppression value: * 0-262143kb/s

【parameter description】

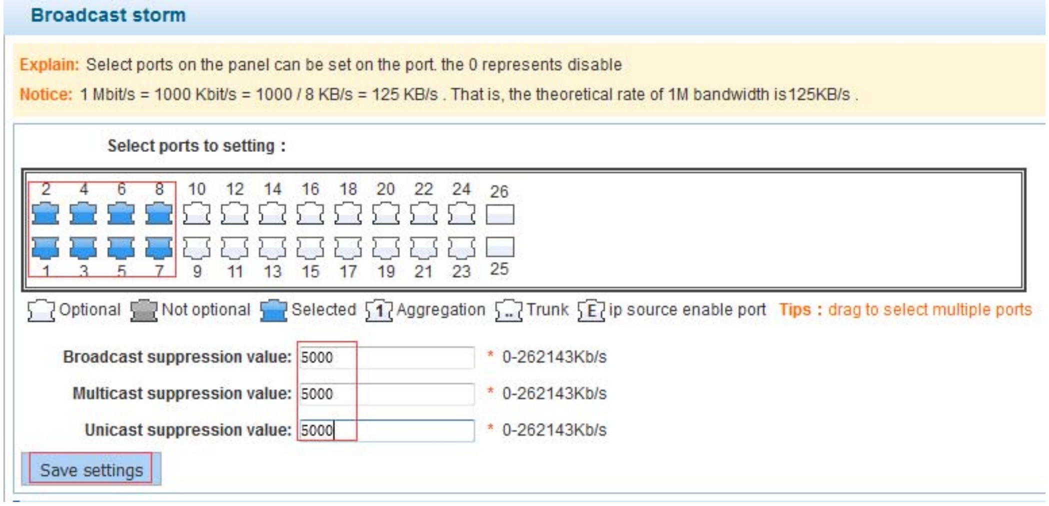
parameter	description
Broadcast suppression value	Storm suppression value of the broadcast packets
Multicast suppression value	Storm suppression value of the multicast packets
Unicast suppression value	Storm suppression value of the unicast packets

【instructions】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is125KB/s .

【Configuration example】

Such as: should be forwarded to the port 1-8 of all kinds of packet forwarding rate is 5000 KB/s



Broadcast storm

Explain: Select ports on the panel can be set on the port. the 0 represents disable

Notice: 1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s . That is, the theoretical rate of 1M bandwidth is125KB/s .

Select ports to setting :

Tips : drag to select multiple ports

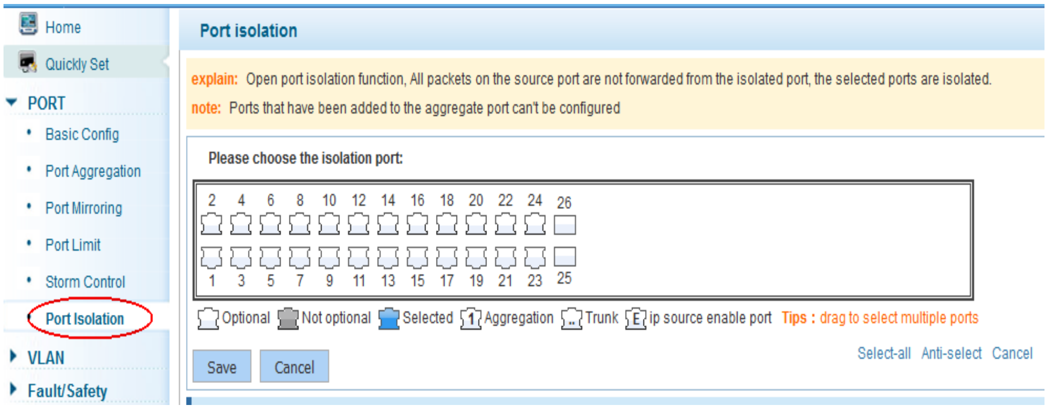
Broadcast suppression value: 5000 * 0-262143Kb/s

Multicast suppression value: 5000 * 0-262143Kb/s

Unicast suppression value: 5000 * 0-262143Kb/s

4.2.6 Port isolation

In the navigation bar to select **"PORT>port isolation "**,
ports are isolated.the following picture：



Port isolation

explain: Open port isolation function, All packets on the source port are not forwarded from the isolated port, the selected ports are isolated.

note: Ports that have been added to the aggregate port can't be configured

Please choose the isolation port:

Tips : drag to select multiple ports

【parameter description】

parameter	description
Source port	Choose a port, to configure the isolated port

Isolated port	Port will be isolated

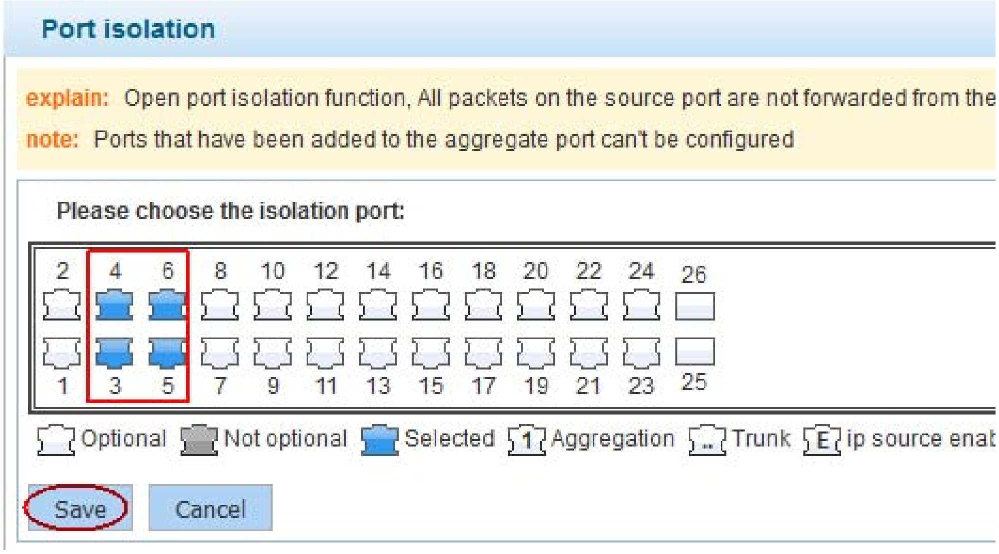
【instructions】

Open port isolation function, All packets on the source port are not forwarded from the isolated port, the selected ports are isolated.

Ports that have been added to the aggregate port aren't also capable of being a destination port and source port, destination port and source port cannot be the same

【Configuration example】

Such as: the port 3, 4, 5, and 6 ports are isolated

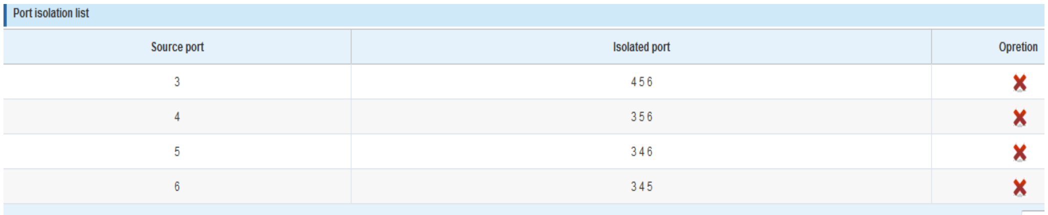


Port isolation

explain: Open port isolation function, All packets on the source port are not forwarded from the

note: Ports that have been added to the aggregate port can't be configured

Please choose the isolation port:

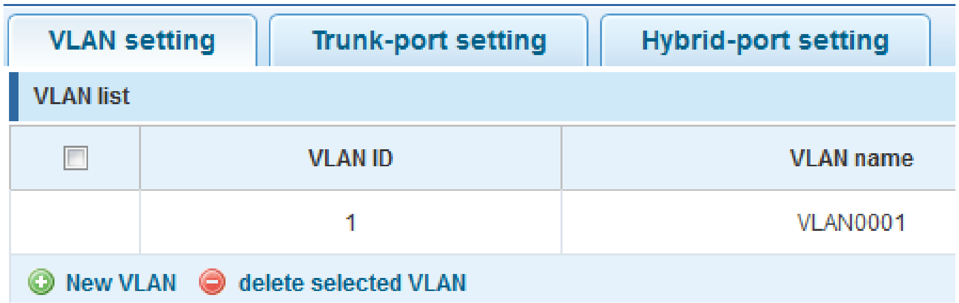


Port isolation list

Source port	Isolated port	Opretion
3	4 5 6	✘
4	3 5 6	✘
5	3 4 6	✘
6	3 4 5	✘

4.3 VLAN

In the navigation bar to select**"VLAN"**,You can manage the **VLAN config, Trunk Settings** and **Hybrid Settings** ,the following picture:

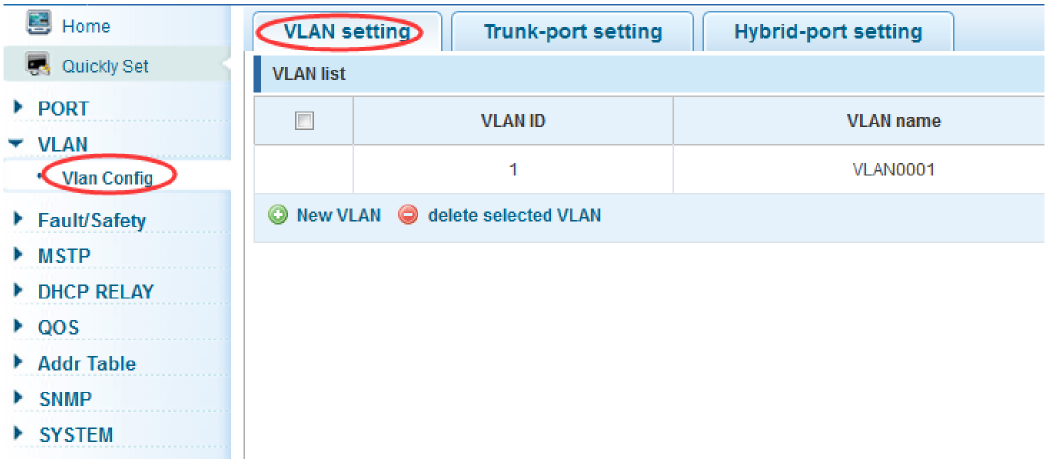


VLAN list

□	VLAN ID	VLAN name
	1	VLAN0001

4.3.1 VLAN config

In the navigation bar to select“**VLAN config**”,Vlans can be created and set the port to the VLAN (port default state for the access mode) ,the following picture：



VLAN list

□	VLAN ID	VLAN name
	1	VLAN0001

【parameter description】

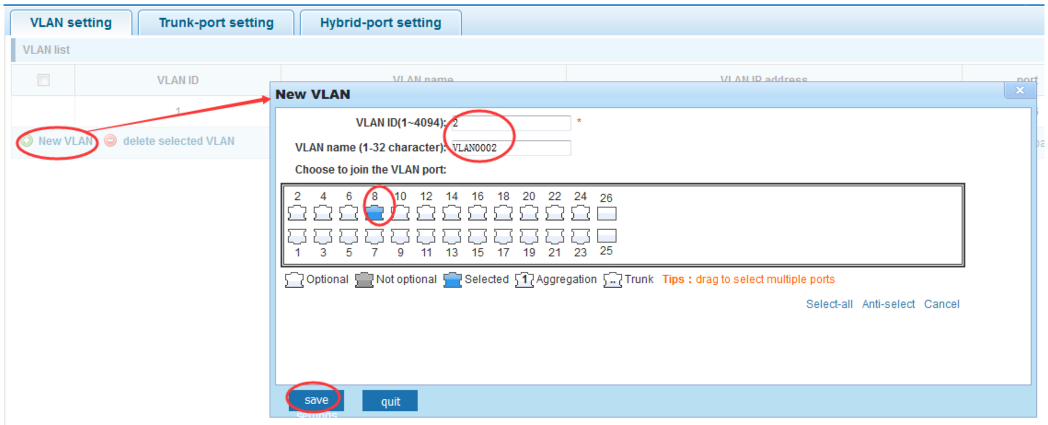
parameter	**description**
VLAN ID	VLAN number,24GE default VLAN 1
VLAN name	VLAN mark
VLAN IP address	Manage switch ip address

【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



VLAN ID(1~4094): 2 *

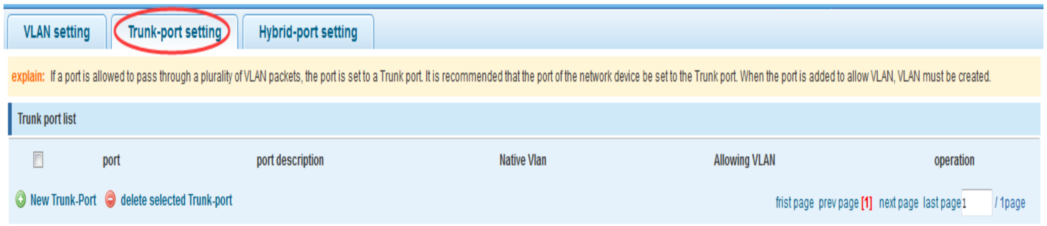
VLAN name (1-32 character): VLAN0002

Choose to join the VLAN port:

Tips：drag to select multiple ports

4.3.2 Trunk-port setting

In the navigation bar to select**“VLAN config>trunk-port setting”**,can set port to Trunk port,the following picture：


VLAN setting
Trunk-port setting
Hybrid-port setting
Trunk port list
New Trunk-Port
delete selected Trunk-port
frist page prev page [1] next page last page1 / 1page

explain: If a port is allowed to pass through a plurality of VLAN packets, the port is set to a Trunk port. It is recommended that the port of the network device be set to the Trunk port. When the port is added to allow VLAN, VLAN must be created.

□	port	port description	Native Vlan	Allowing VLAN	operation

【parameter description】

parameter	description
Native VLAN	Only set one
Allowing vlan	Can set up multiple

【instructions】

Native VLAN: as a Trunk, the mouth 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 mouth of the list to limit the flow of some VLAN can't through the Trunk.

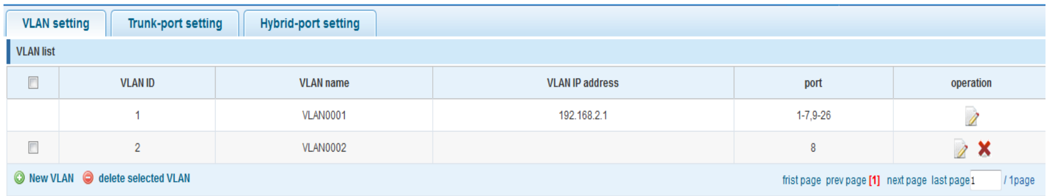
【Configuration example】

Such as：PVID=VLAN2

PC1：192.168.2.122,port 8, access VLAN2

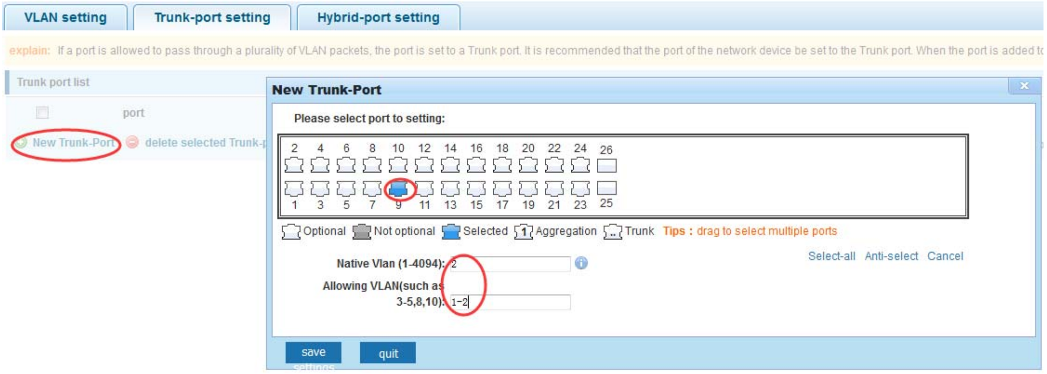
PC2：192.168.2.123,port 9, Trunk allowed VLAN 1-2

PC3：192.168.2.124,port 10, access VLAN1（The default port belongs to VLAN1）
Can let the PC2 PING PC1, cannot PING PC3



VLAN list

□	VLAN ID	VLAN name	VLAN IP address	port	operation
	1	VLAN0001	192.168.2.1	1-7,9-26	
□	2	VLAN0002		8	



explain: If a port is allowed to pass through a plurality of VLAN packets, the port is set to a Trunk port. It is recommended that the port of the network device be set to the Trunk port. When the port is added t

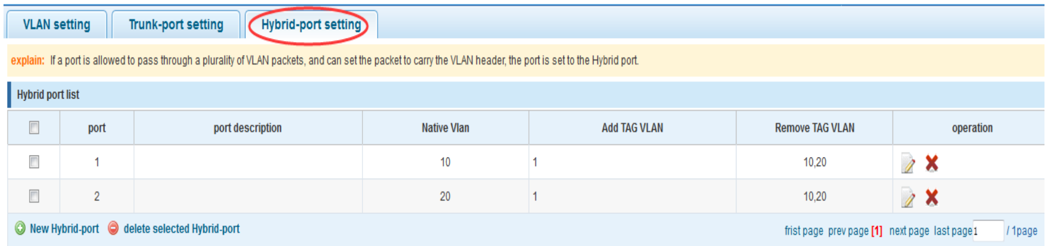
Trunk port list

Native Vlan (1-4094): 2

Allowing VLAN(such as 3-5,8,10): 1-2

4.3.3 Hybrid-port setting

In the navigation bar to select**“VLAN config>hybrid-port setting”**,Can set the port to take the tag and without the tag ,the following picture：


VLAN setting
Trunk-port setting
Hybrid-port setting

explain: If a port is allowed to pass through a plurality of VLAN packets, and can set the packet to carry the VLAN header, the port is set to the Hybrid port.

Hybrid port list

□	port	port description	Native Vlan	Add TAG VLAN	Remove TAG VLAN	operation
□	1		10	1	10,20	
□	2		20	1	10,20	

New Hybrid-port
delete selected Hybrid-port
frist page prev page [1] next page last page1 / 1page

【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)

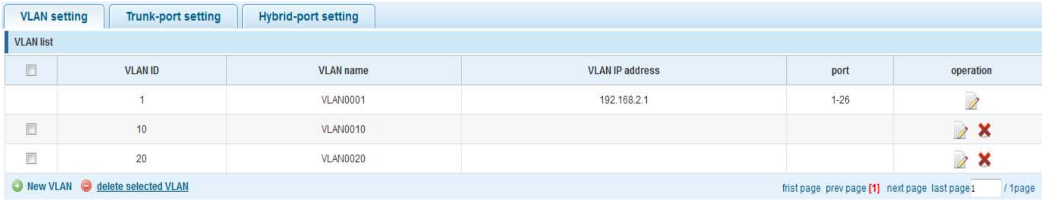
Hybrid port to send packet:

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

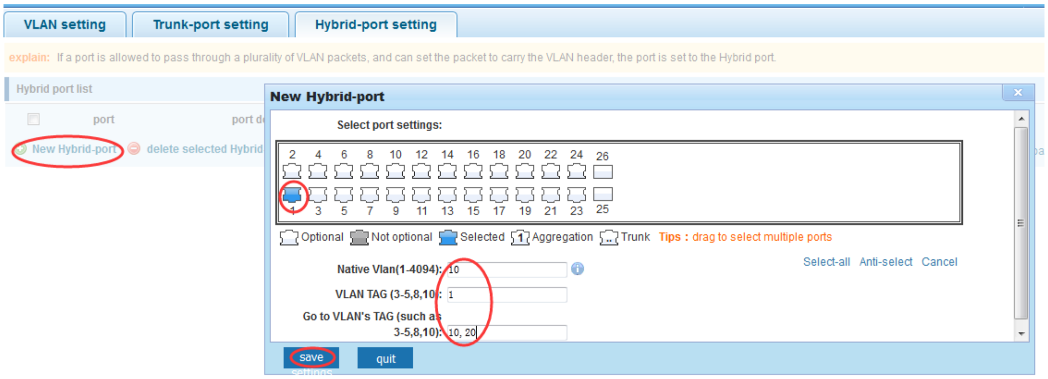
【Configuration example】

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



VLAN list

□	VLAN ID	VLAN name	VLAN IP address	port	operation
	1	VLAN0001	192.168.2.1	1-26	
□	10	VLAN0010			
□	20	VLAN0020			

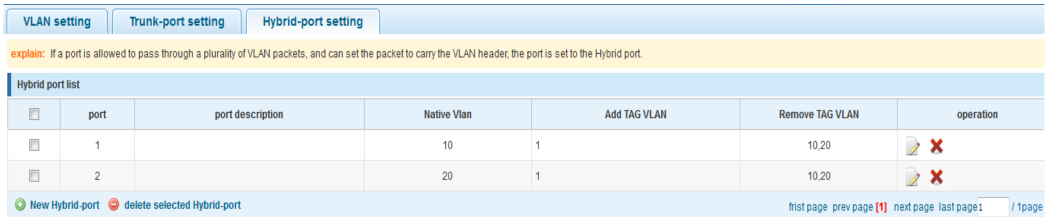


explain: If a port is allowed to pass through a plurality of VLAN packets, and can set the packet to carry the VLAN header, the port is set to the Hybrid port.

Native Vlan(1-4094): 10

VLAN TAG (3-5,8,10): 1

Go to VLAN's TAG (such as 3-5,8,10): 10, 20


VLAN setting
Trunk-port setting
Hybrid-port setting

explain: If a port is allowed to pass through a plurality of VLAN packets, and can set the packet to carry the VLAN header, the port is set to the Hybrid port.

Hybrid port list

□	port	port description	Native Vlan	Add TAG VLAN	Remove TAG VLAN	operation
□	1		10	1	10,20	
□	2		20	1	10,20	

New Hybrid-port
delete selected Hybrid-port
frist page prev page [1] next page last page 1 / 1page

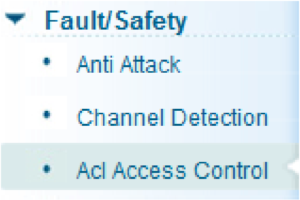
This system e0/1 and the receive system e0/2 PC can be exchanged, but when each data taken from a VLAN is different.

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

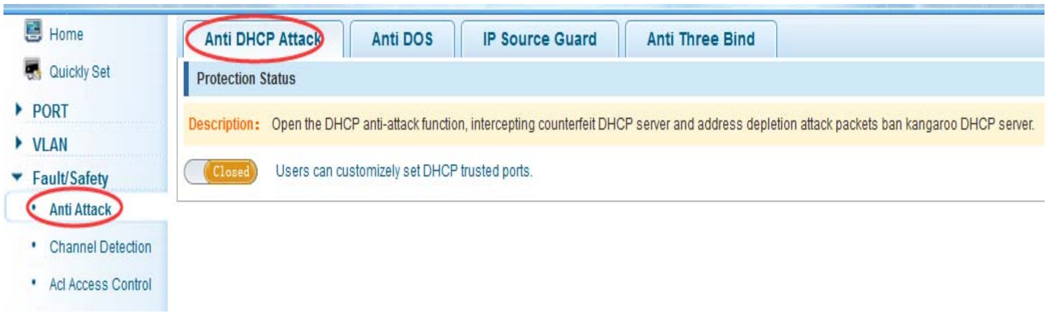
In the navigation bar to select**“fault/safety”**,you can set **anti attack**、**channle detection and ACLaccess control** configuration 。



4.4.1 Anti attack

4.4.1.1 Anti DHCP attack

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,the following picture：



Description： Open the DHCP anti-attack function, intercepting counterfeit DHCP server and address depletion attack packets ban kangaroo DHCP server.

Users can customizely set DHCP trusted ports.

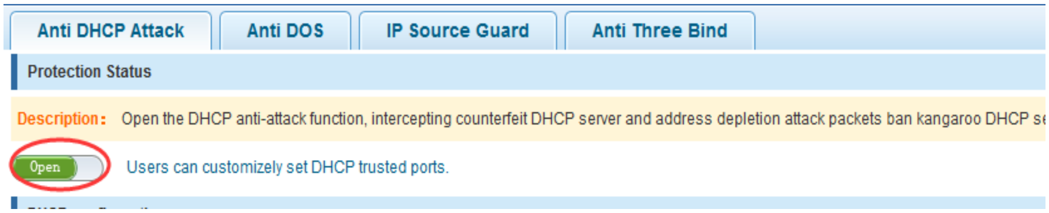
【instructions】

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】

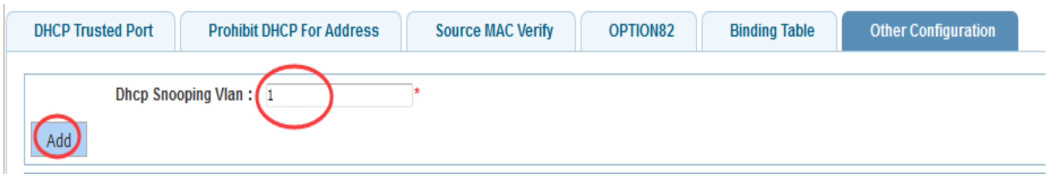
Such as：1.dhcp snooping open



Description： Open the DHCP anti-attack function, intercepting counterfeit DHCP server and address depletion attack packets ban kangaroo DHCP se

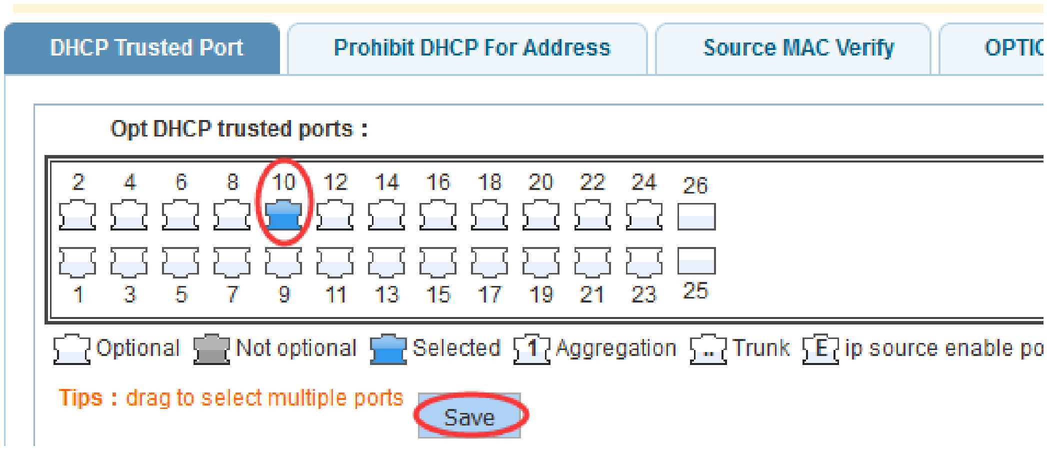
Users can customizely set DHCP trusted ports.

2.Setting dhcp snooping vlan



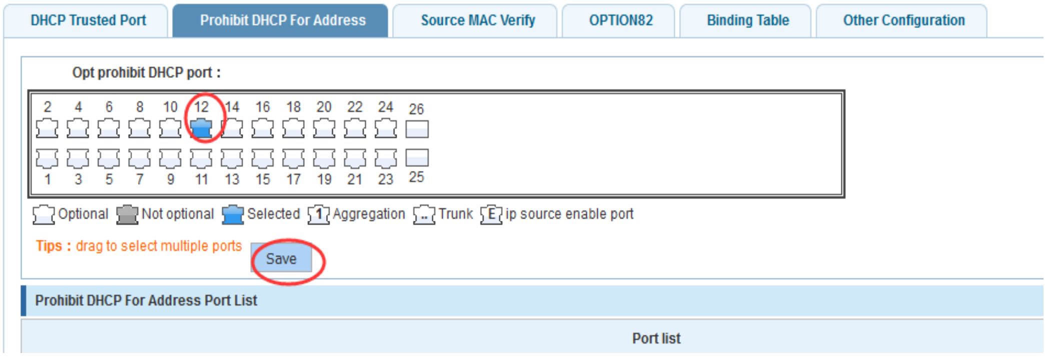
Dhcp Snooping Vlan : 1 *

Set the connection router 10 ports for trust, then 12 port is set to the prohibit



Opt DHCP trusted ports :

Tips : drag to select multiple ports



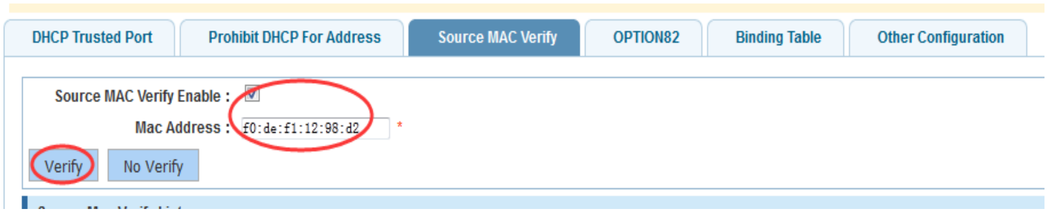
Opt prohibit DHCP port :

Tips : drag to select multiple ports

Prohibit DHCP For Address Port List

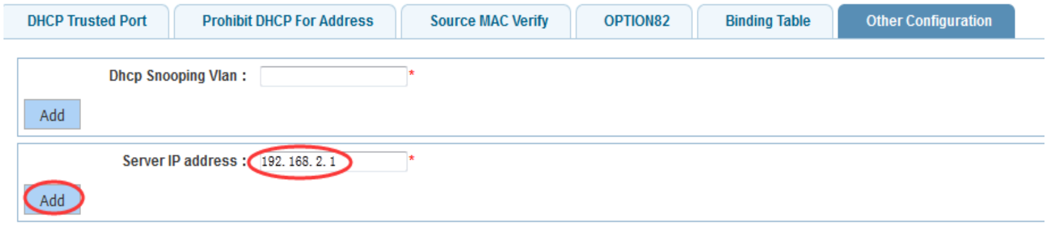
Port list

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



Source MAC Verify Enable : ☑

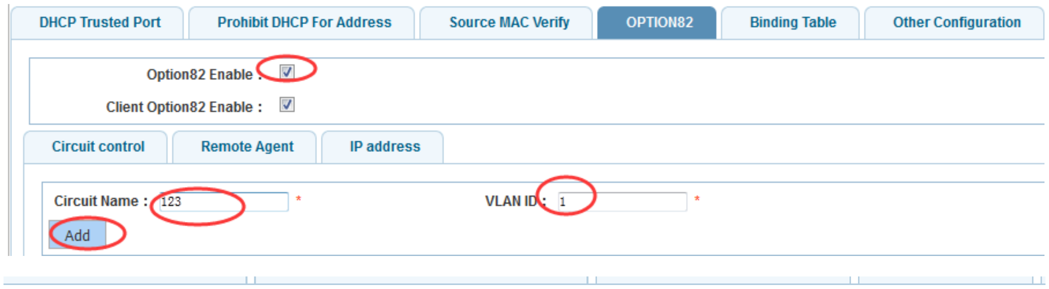
Mac Address : f0:de:f1:12:98:d2 *



Dhcp Snooping Vlan : *

Server IP address : 192. 168. 2. 1 *

4.Set option82 information

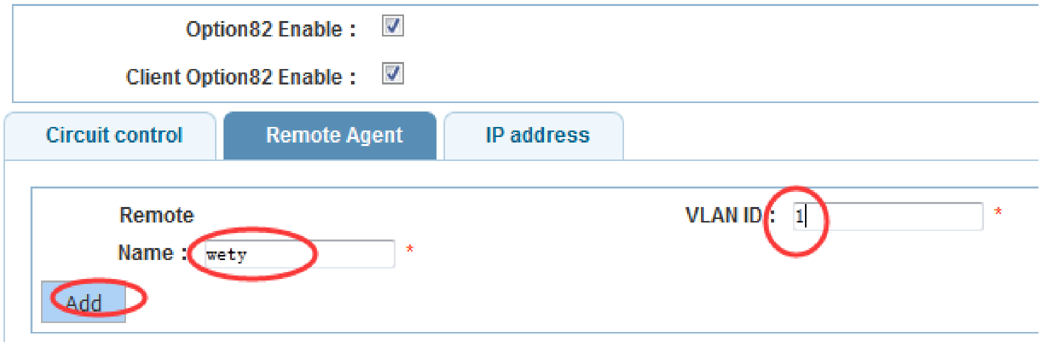


Option82 Enable : ☑

Client Option82 Enable : ☑

Circuit Name : 123 *

VLAN ID : 1 *

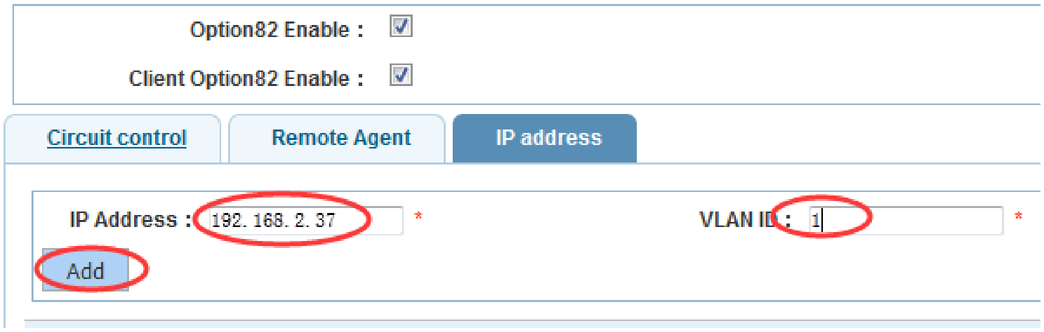


Option82 Enable : ☑

Client Option82 Enable : ☑

Remote Name : wety *

VLAN ID : 1 *



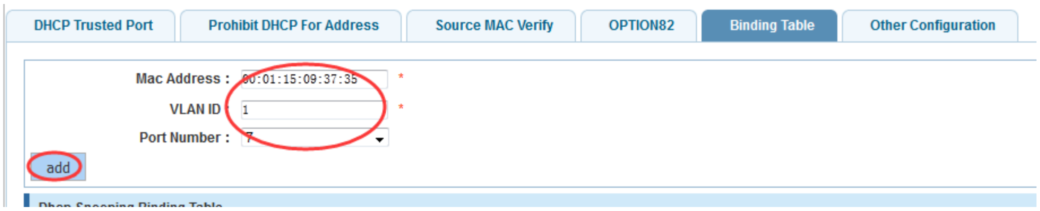
Option82 Enable : ☑

Client Option82 Enable : ☑

IP Address : 192. 168. 2. 37 *

VLAN ID : 1 *

5.The port 7 for binding



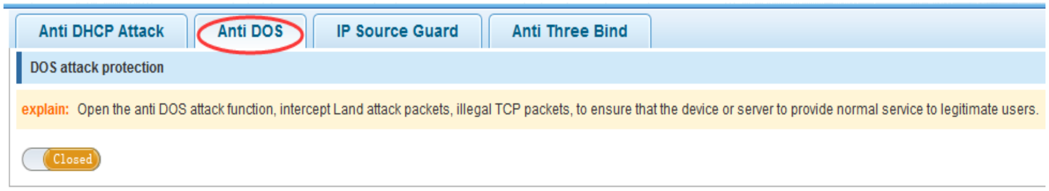
Mac Address : 00:01:15:09:37:35 *

VLAN ID : 1 *

Port Number : 7

4.4.1.2 Anti DOS

In the navigation bar to select**“fault/safety>anti attack>anti dhcp attack”**,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.,the following picture：



DOS attack protection

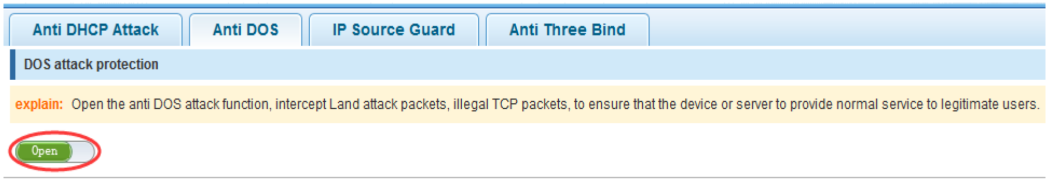
explain: Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users.

【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

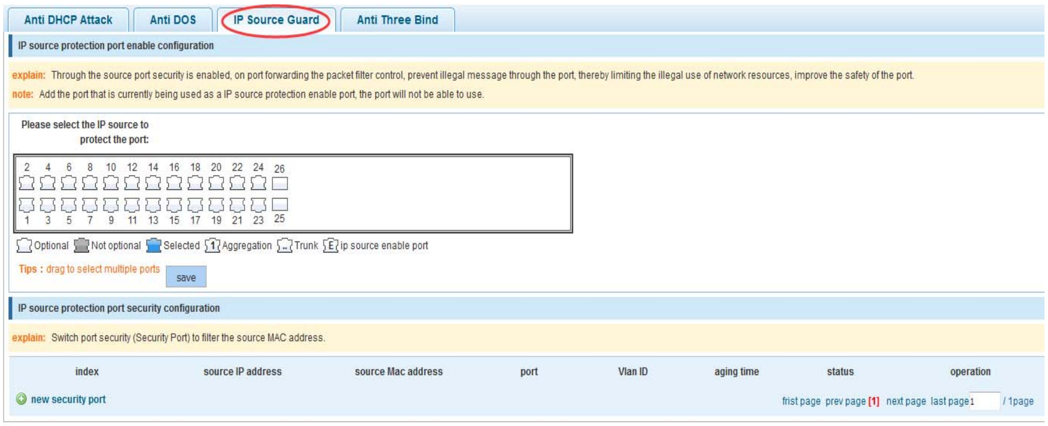


DOS attack protection

explain: 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.

4.4.1.3 IPsource 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,the following picture：



IP source protection port enable configuration

explain: 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.

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

Please select the IP source to protect the port:

Tips : drag to select multiple ports

IP source protection port security configuration

explain: Switch port security (Security Port) to filter the source MAC address.

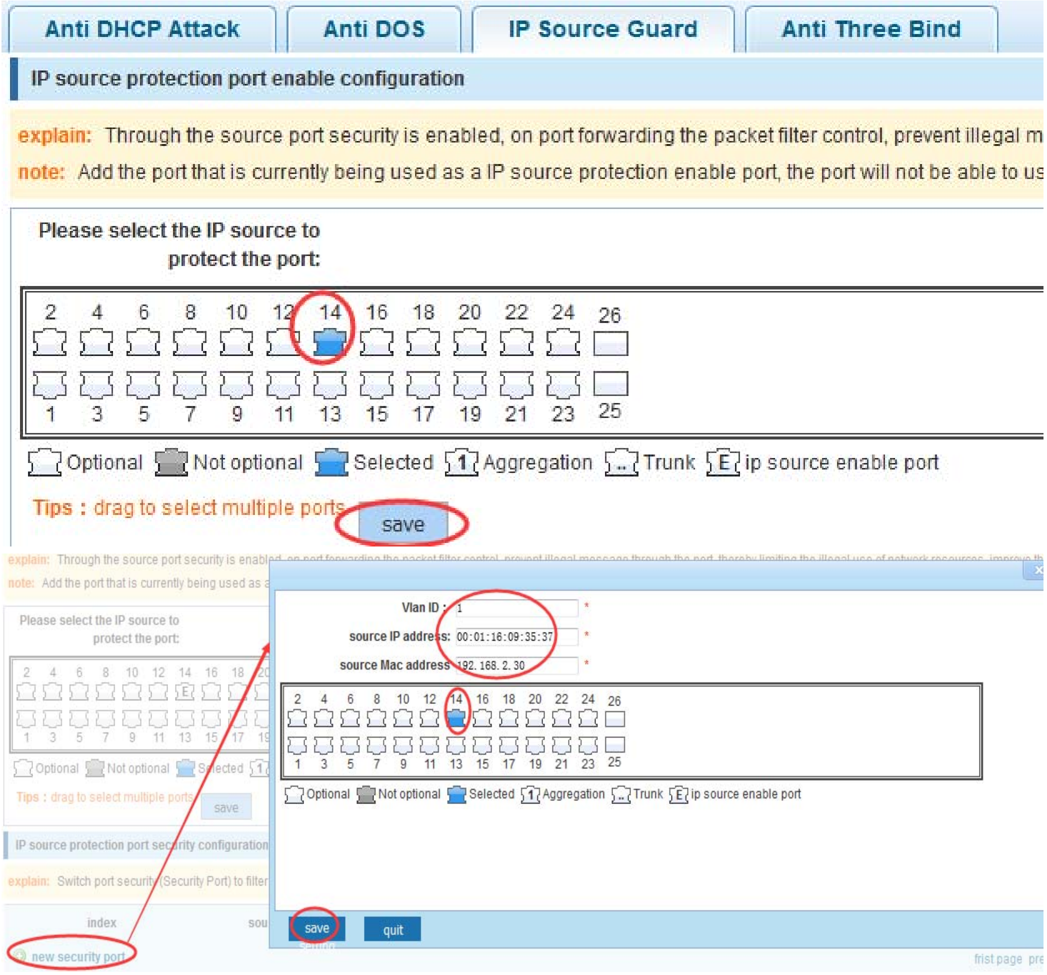
index	source IP address	source Mac address	port	Vlan ID	aging time	status	operation

【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



IP source protection port enable configuration

explain: Through the source port security is enabled, on port forwarding the packet filter control, prevent illegal m

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

Please select the IP source to protect the port:

Tips : drag to select multiple ports

IP source protection port security configuration

explain: Switch port security (Security Port) to filter

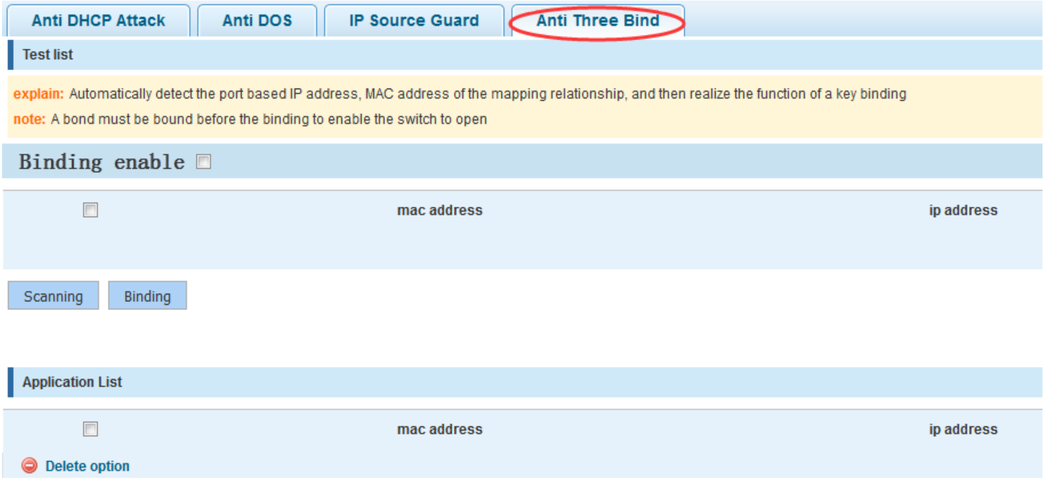
Vlan ID : 1 *

source IP address: 00:01:16:09:35:37 *

source Mac address 192. 168. 2. 30 *

4.4.1.4 Anti three bind

In the navigation bar to select**“fault/safety>anti attack>anti three bind”**,Automatically detect the port based IP address, MAC address of the mapping relationship, and then realize the function of a key binding,the following picture：



Test list

explain: Automatically detect the port based IP address, MAC address of the mapping relationship, and then realize the function of a key binding

note: A bond must be bound before the binding to enable the switch to open

Binding enable □

□	mac address	ip address

Application List

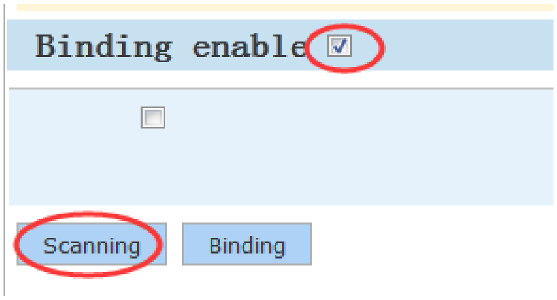
□	mac address	ip address

【instructions】

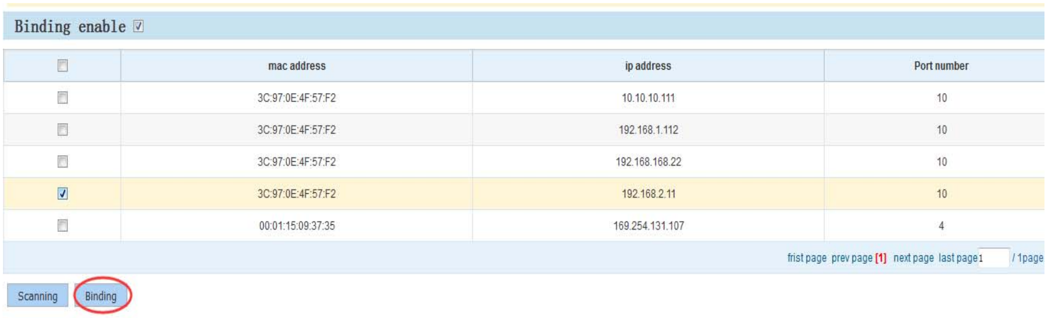
A bond must be bound before the binding to enable the switch to open,And if you want to access shall be binding and switch the IP address of the same network segment 。

【Configuration example】

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

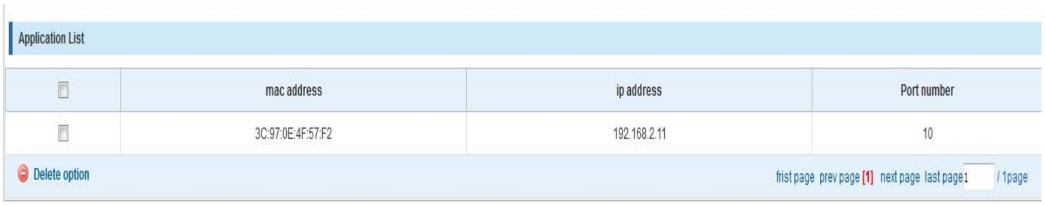


Binding enable ☑



Binding enable ☑

□	mac address	ip address	Port number
□	3C:97:0E:4F:57:F2	10.10.10.111	10
□	3C:97:0E:4F:57:F2	192.168.1.112	10
□	3C:97:0E:4F:57:F2	192.168.168.22	10
☑	3C:97:0E:4F:57:F2	192.168.2.11	10
□	00:01:15:09:37:35	169.254.131.107	4



Application List

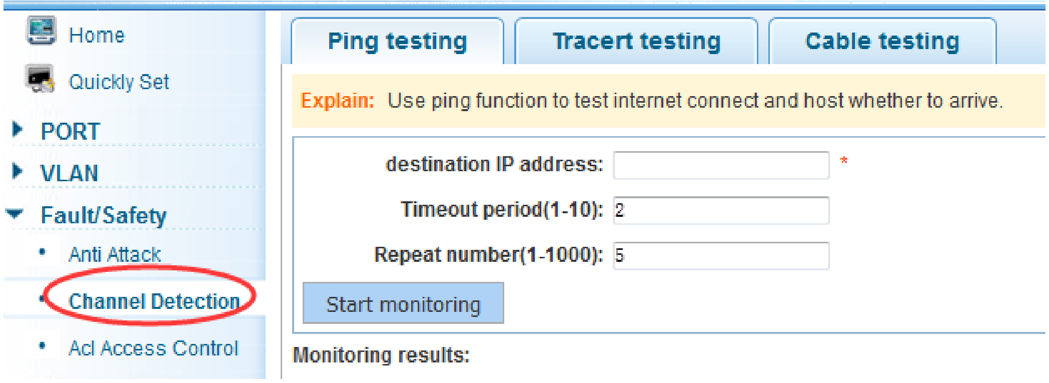
□	mac address	ip address	Port number
□	3C:97:0E:4F:57:F2	192.168.2.11	10

Can check the delete option.

4.4.2 Channel detection

4.4.2.1 Ping testing

In the navigation bar to select**“fault/safety> channel detection>ping testing”**,Use ping function to test internet connect and host whether to arrive. The following picture :



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

destination IP address: *

Timeout period(1-10): 2

Repeat number(1-1000): 5

Monitoring results:

【parameter description】

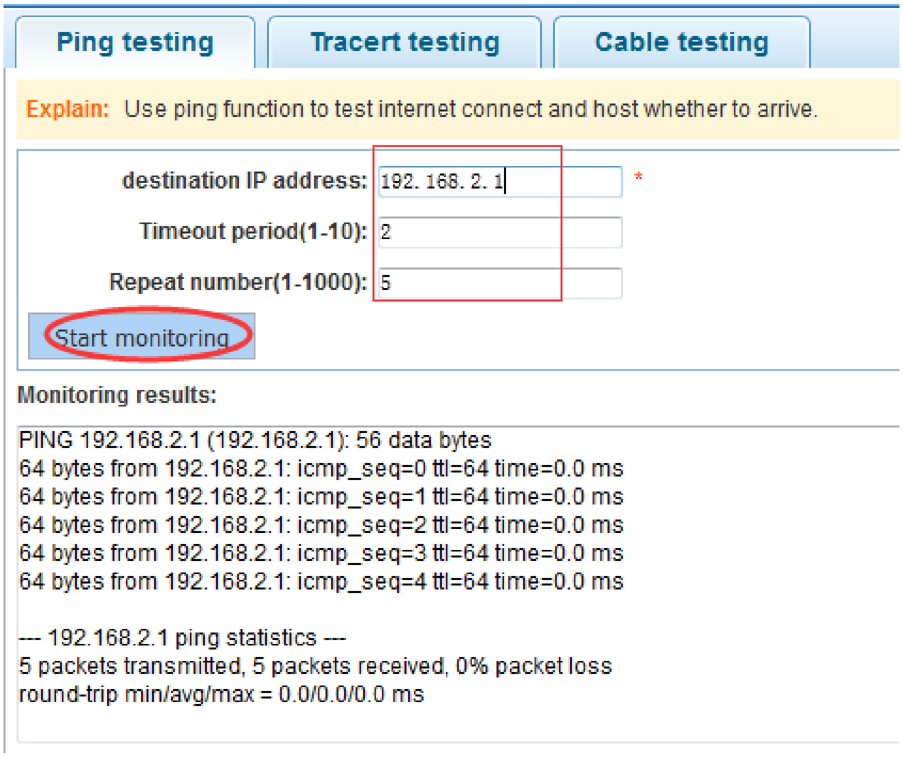
parameter	description
destination IP address	Fill in the IP address of the need to detect
Timeout period	Range of 1 to 10
Repeat number	Testing number

【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



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

destination IP address: 192. 168. 2. 1 *

Timeout period(1-10): 2

Repeat number(1-1000): 5

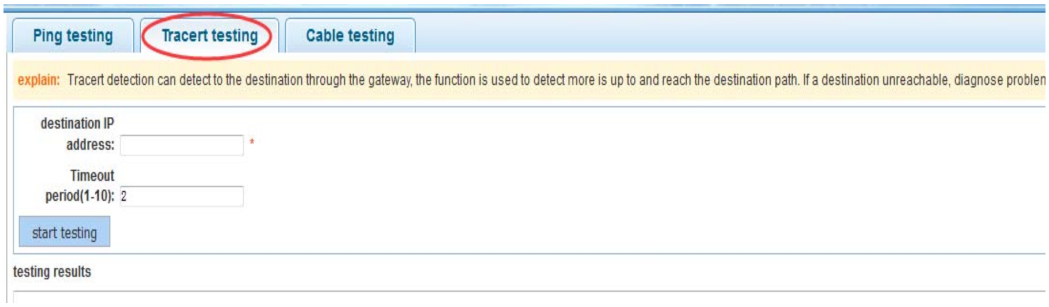
Monitoring results:

```
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.0 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

4.4.2.2 Tracert testing

In the navigation bar to select**"fault/safety> channel detection>tracert testing"**,Tracert detection can detect to the destination through the .following picture :



explain: Tracert detection can detect to the destination through the gateway, the function is used to detect more is up to and reach the destination path. If a destination unreachable, diagnose problen

destination IP address: *

Timeout period(1-10): 2

testing results

【parameter description】

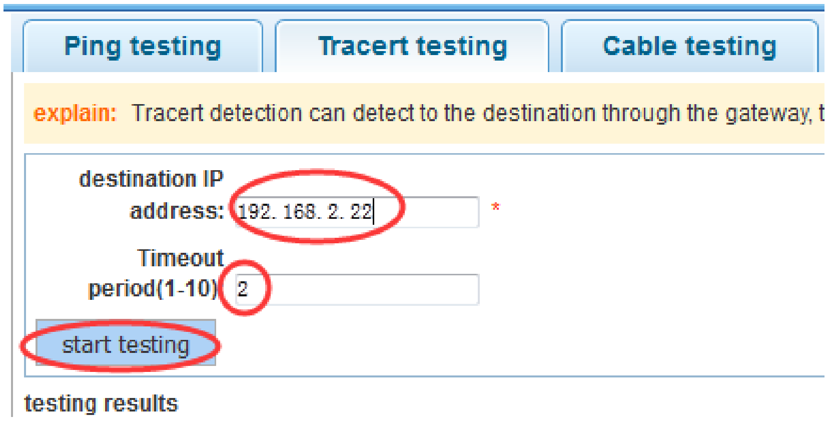
parameter	description
destination IP address	Fill in the IP address of the need to detect
Timeout period	Range of 1 to 10

【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



explain: Tracert detection can detect to the destination through the gateway, t

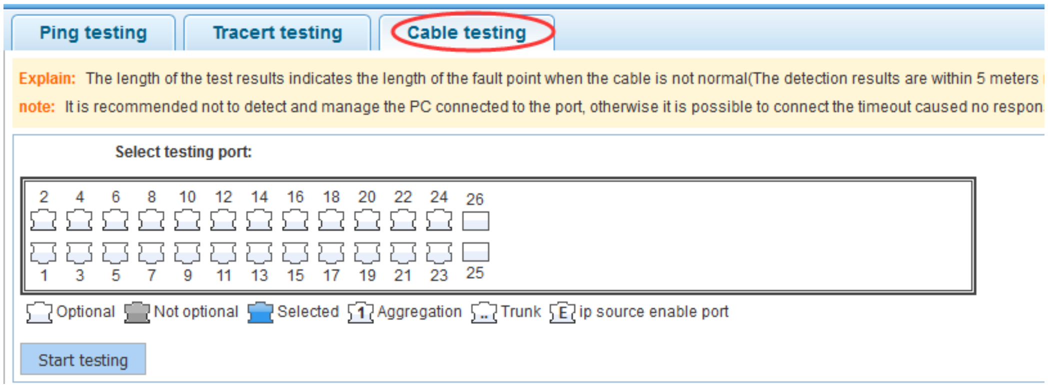
destination IP address: 192. 168. 2. 22 *

Timeout period(1-10): 2

testing results

4.4.2.3 Cable testing

In the navigation bar to select**“fault/safety> channel detection>cable tracert testing”**,Can detect connection device status ,the following picture：

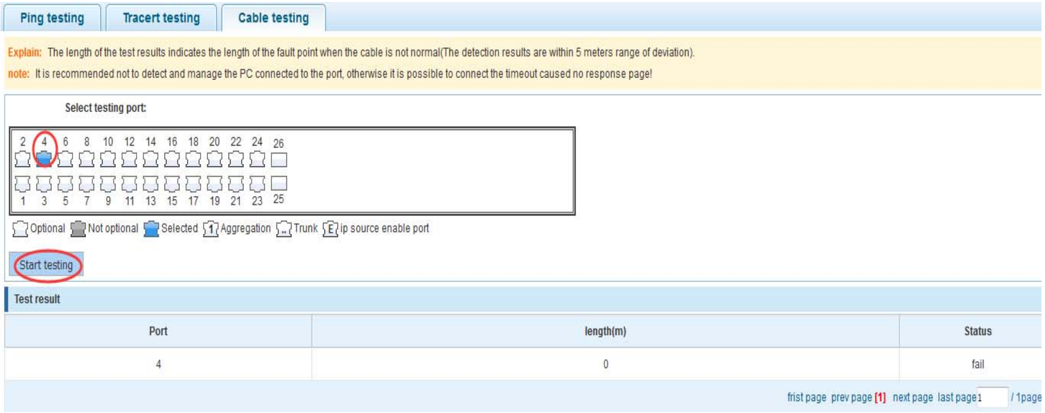


Explain: The length of the test results indicates the length of the fault point when the cable is not normal(The detection results are within 5 meters

note: It is recommended not to detect and manage the PC connected to the port, otherwise it is possible to connect the timeout caused no respon

Select testing port:

【Configuration example】



Explain: The length of the test results indicates the length of the fault point when the cable is not normal(The detection results are within 5 meters range of deviation).

note: It is recommended not to detect and manage the PC connected to the port, otherwise it is possible to connect the timeout caused no response page!

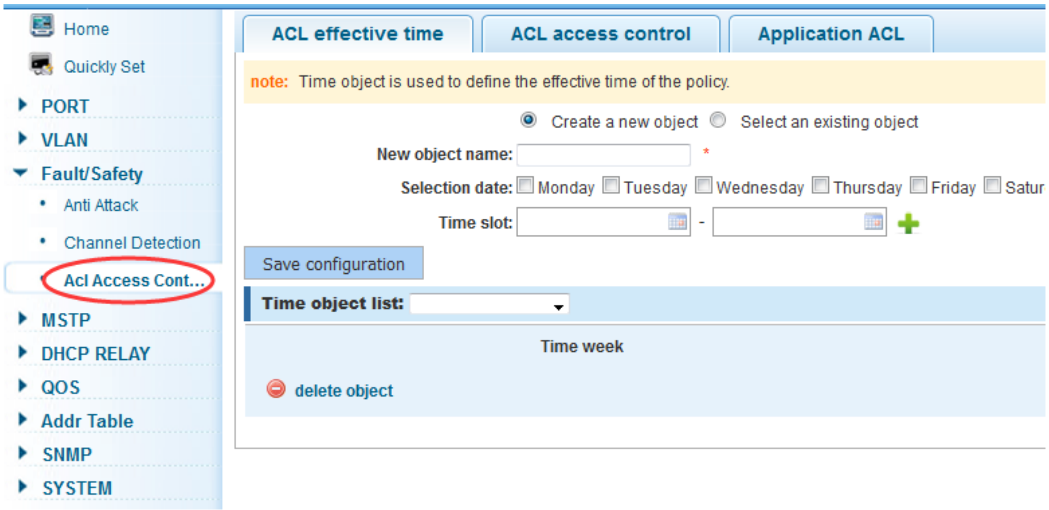
Select testing port:

Test result

Port	length(m)	Status
4	0	fail

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



note: Time object is used to define the effective time of the policy.

● Create a new object ○ Select an existing object

New object name: ______ *

Selection date: □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Satur

Time slot: ______ - ______

【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

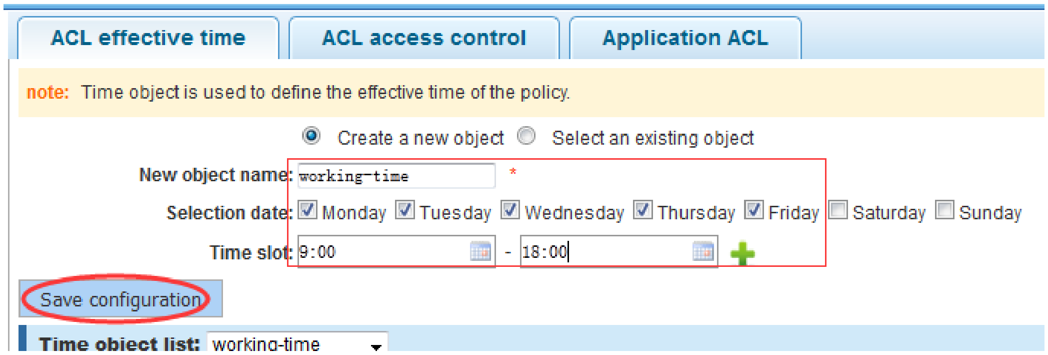
3, any only under the condition of the minimum permissions to the user can satisfy their demand

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



note: Time object is used to define the effective time of the policy.

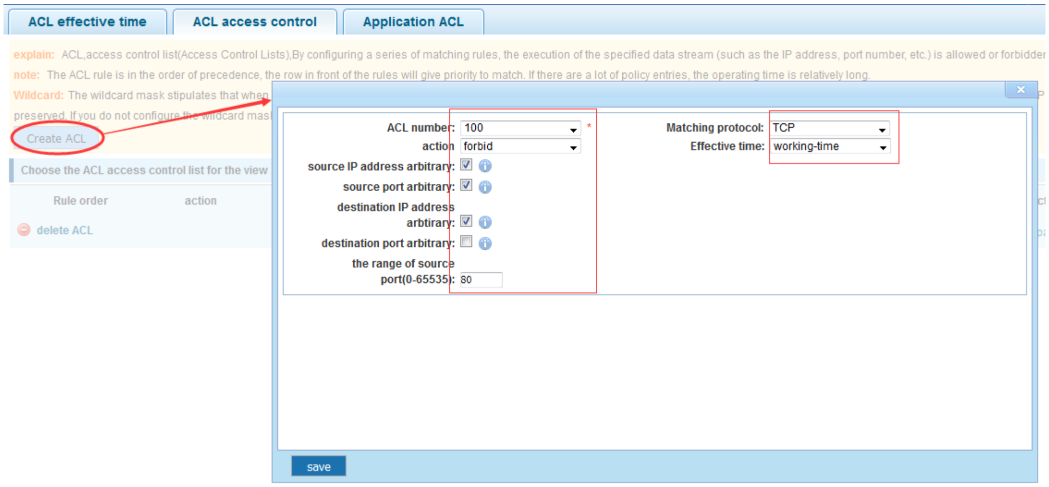
● Create a new object ○ Select an existing object

New object name: working-time *

Selection date: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Time slot: 9:00 - 18:00

Time object list: working-time



explain: ACL,access control list(Access Control Lists),By configuring a series of matching rules, the execution of the specified data stream (such as the IP address, port number, etc.) is allowed or forbidder

note: The ACL rule is in the order of precedence, the row in front of the rules will give priority to match. If there are a lot of policy entries, the operating time is relatively long.

Wildcard: The wildcard mask stipulates that when

preserved. If you do not configure the wildcard masl

Choose the ACL access control list for the view

Rule order action

ACL number: 100 *

action forbid

source IP address arbitrary: ☑

source port arbitrary: ☑

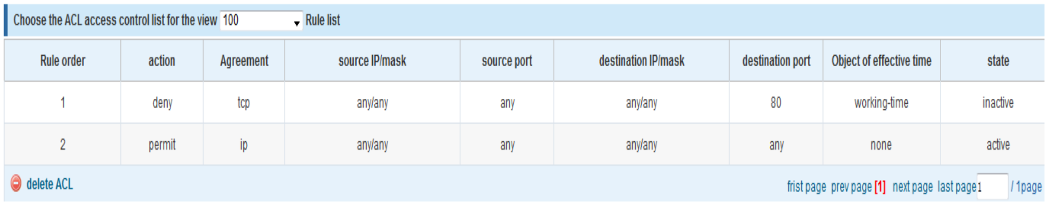
destination IP address arbtirary: ☑

destination port arbitrary: □

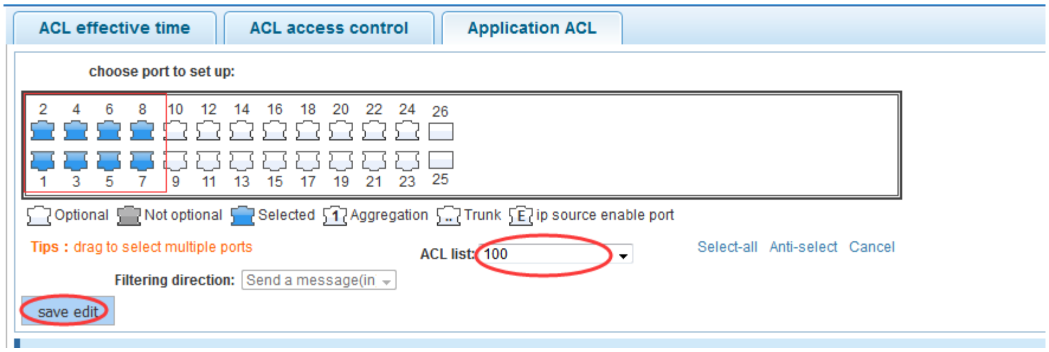
the range of source port(0-65535): 80

Matching protocol: TCP

Effective time: working-time


Choose the ACL access control list for the view 100 Rule list

Rule order	action	Agreement	source IP/mask	source port	destination IP/mask	destination port	Object of effective time	state
1	deny	tcp	any/any	any	any/any	80	working-time	inactive
2	permit	ip	any/any	any	any/any	any	none	active



choose port to set up:

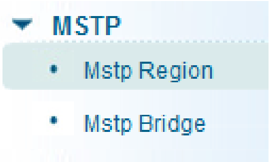
Tips : drag to select multiple ports

ACL list: 100

Filtering direction: Send a message(in

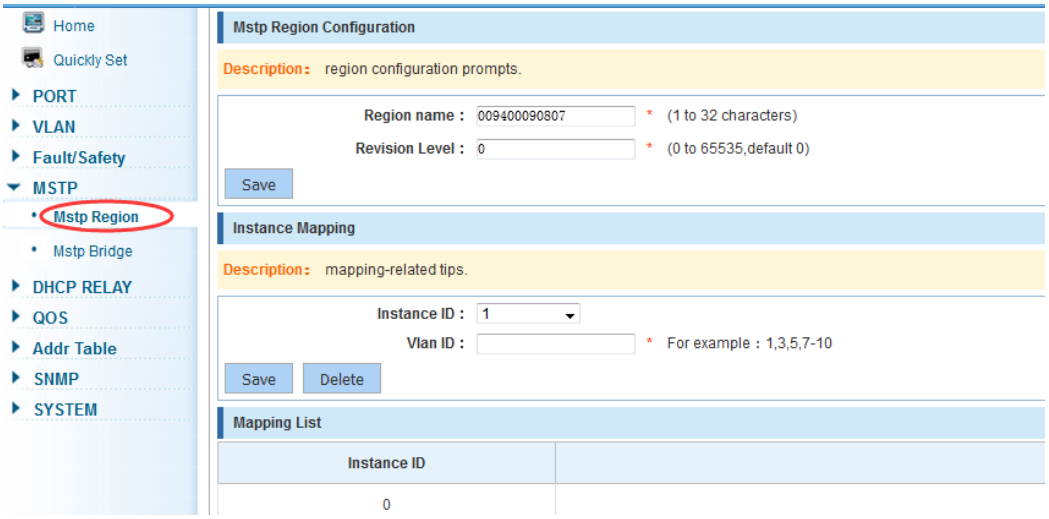
4.5 MSTP

In the navigation bar to select**"MSTP"**,you can set to the **MSTP region and MSTP bridge configuration**。



4.5.1 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.the following picture



Mstp Region Configuration

Description： region configuration prompts.

Region name： 009400090807 * (1 to 32 characters)

Revision Level： 0 * (0 to 65535,default 0)

Instance Mapping

Description： mapping-related tips.

Instance ID： 1

Vlan ID： * For example：1,3,5,7-10

Mapping List

Instance ID	
0	

【parameter description】

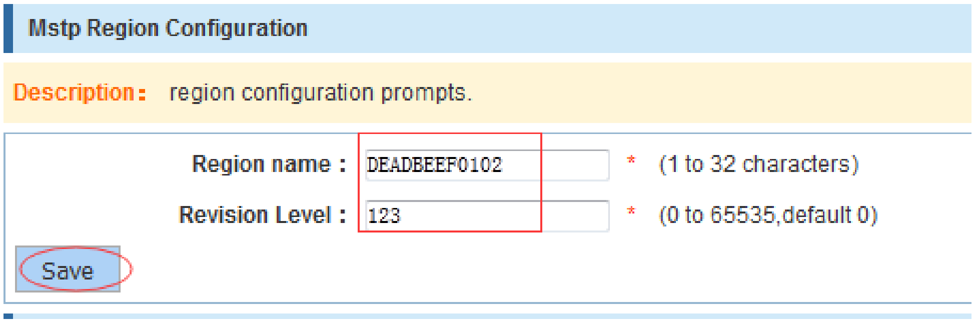
parameter	description
Region name	Configure the region name
Revision level	Parameter configuration revision level
Instance ID	Select configuration instance ID
VLAN ID	Mapping of the VLAN configuration instance

【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

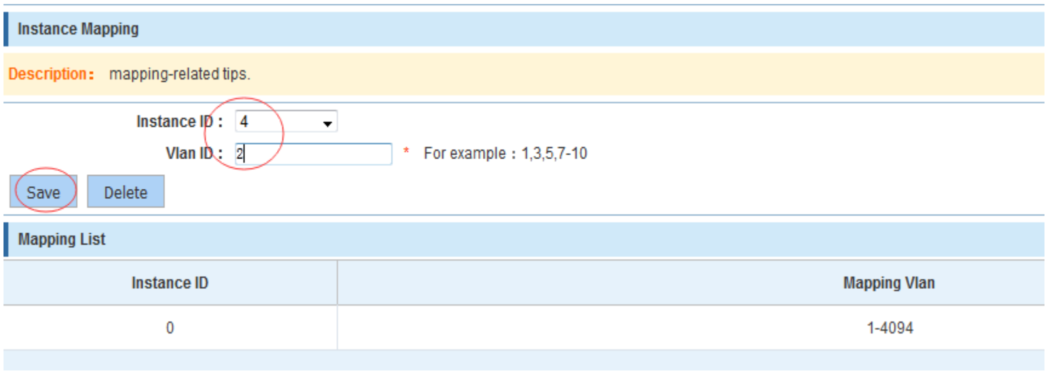


Mstp Region Configuration

Description: region configuration prompts.

Region name : DEADBEEF0102 * (1 to 32 characters)

Revision Level : 123 * (0 to 65535,default 0)



Instance Mapping

Description: mapping-related tips.

Instance ID : 4

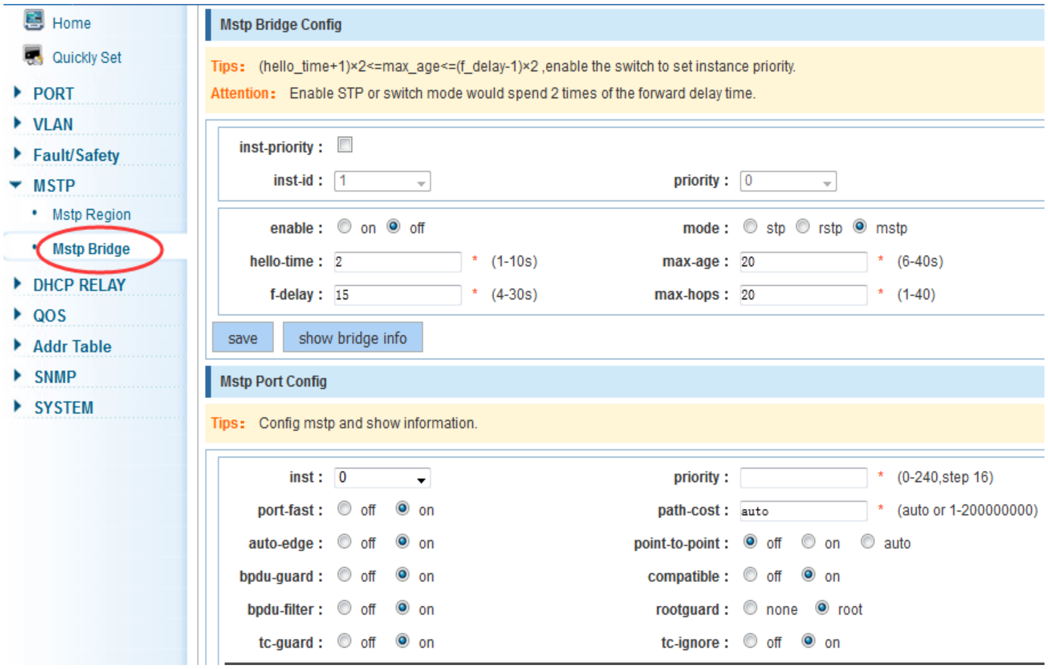
Vlan ID : 2 * For example : 1,3,5,7-10

Mapping List

Instance ID	Mapping Vlan
0	1-4094

4.5.2 MSTP bridge

In the navigation bar to select**“MSTP>MSTP bridge”**,Can be related to bridge, port configuration,the following picture:



Mstp Bridge Config

Tips: (hello_time+1)×2<=max_age<=(f_delay-1)×2 ,enable the switch to set instance priority.

Attention: Enable STP or switch mode would spend 2 times of the forward delay time.

inst-priority : □

inst-id : 1 priority : 0

enable : ○ on ● off mode : ○ stp ○ rstp ● mstp

hello-time : 2 * (1-10s) max-age : 20 * (6-40s)

f-delay : 15 * (4-30s) max-hops : 20 * (1-40)

Mstp Port Config

Tips: Config mstp and show information.

inst : 0 priority : * (0-240,step 16)

port-fast : ○ off ● on path-cost : auto * (auto or 1-200000000)

auto-edge : ○ off ● on point-to-point : ● off ○ on ○ auto

bpdu-guard : ○ off ● on compatible : ○ off ● on

bpdu-filter : ○ off ● on rootguard : ○ none ● root

tc-guard : ○ off ● on tc-ignore : ○ off ● on

【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

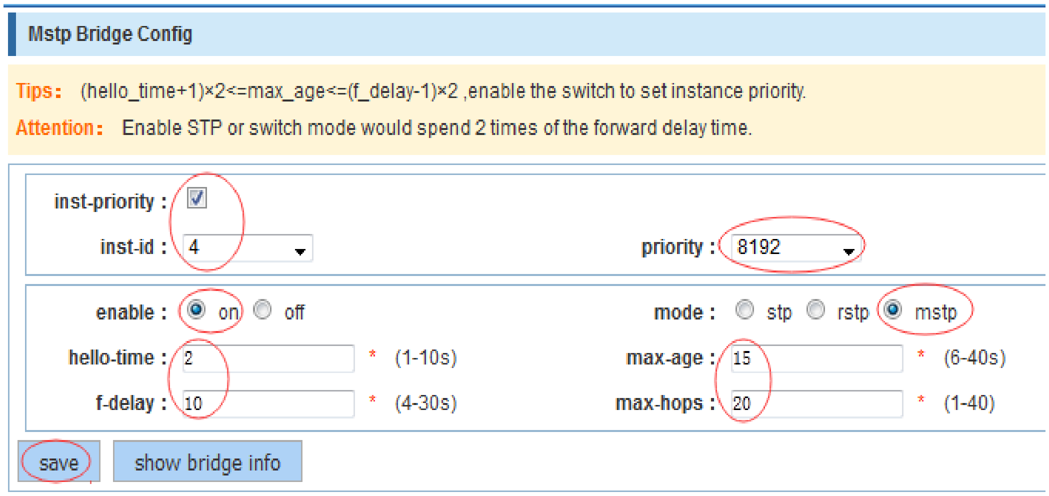
【instruction】

(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



Mstp Bridge Config

Tips： (hello_time+1)×2<=max_age<=(f_delay-1)×2 ,enable the switch to set instance priority.

Attention： Enable STP or switch mode would spend 2 times of the forward delay time.

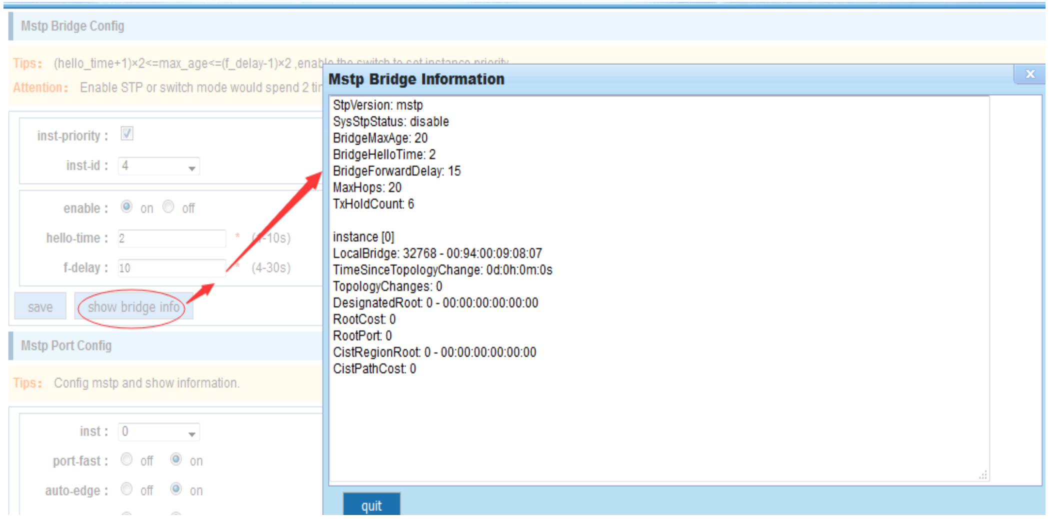
inst-priority : ☑

inst-id : 4 ▾ priority : 8192 ▾

enable : ● on ○ off mode : ○ stp ○ rstp ● mstp

hello-time : 2 * (1-10s) max-age : 15 * (6-40s)

f-delay : 10 * (4-30s) max-hops : 20 * (1-40)

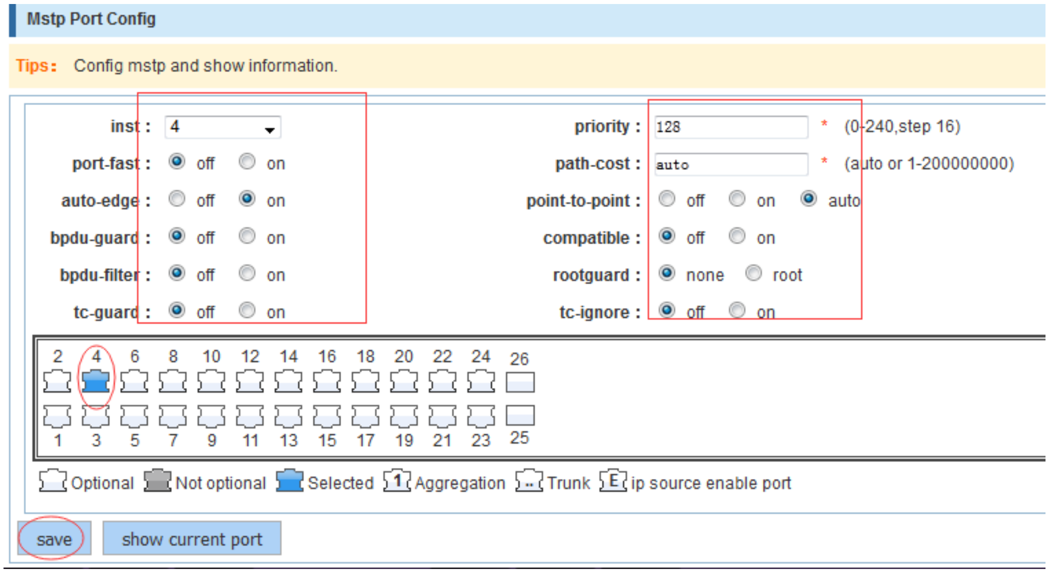


Mstp Bridge Information

```
StpVersion: mstp
SysStpStatus: disable
BridgeMaxAge: 20
BridgeHelloTime: 2
BridgeForwardDelay: 15
MaxHops: 20
TxHoldCount: 6

instance [0]
LocalBridge: 32768 - 00:94:00:09:08:07
TimeSinceTopologyChange: 0d:0h:0m:0s
TopologyChanges: 0
DesignatedRoot: 0 - 00:00:00:00:00:00
RootCost: 0
RootPort: 0
CistRegionRoot: 0 - 00:00:00:00:00:00
CistPathCost: 0
```

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)



Mstp Port Config

Tips： Config mstp and show information.

inst : 4 ▾ priority : 128 * (0-240,step 16)

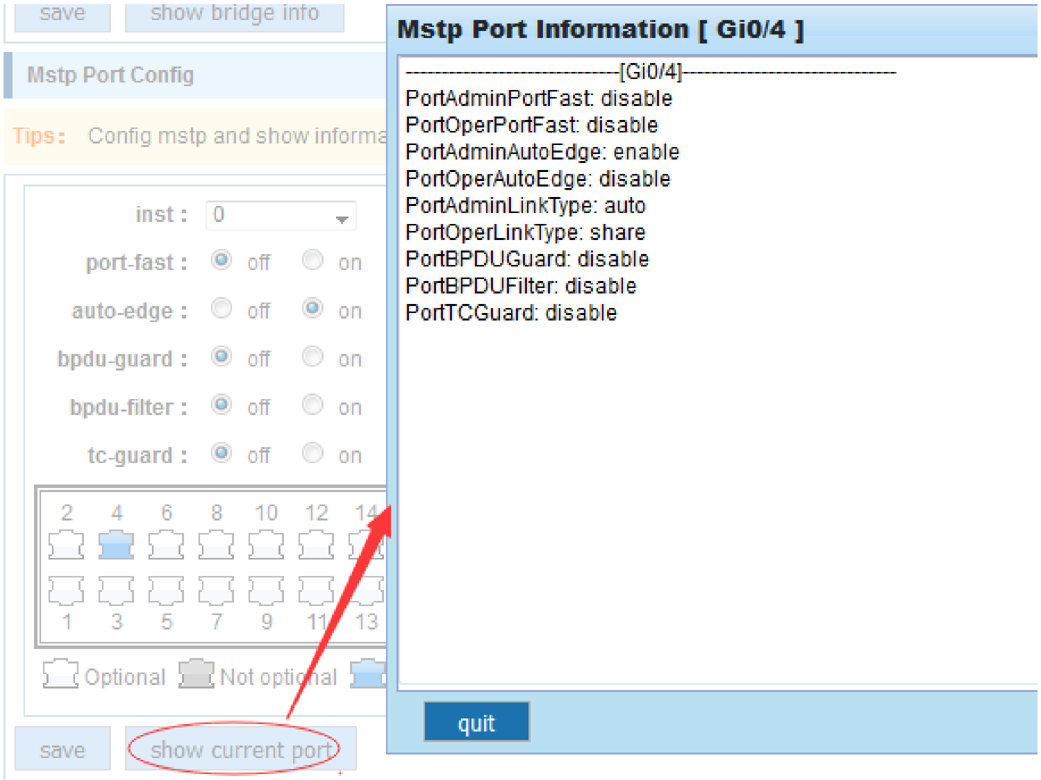
port-fast : ● off ○ on path-cost : auto * (auto or 1-200000000)

auto-edge : ○ off ● on point-to-point : ○ off ○ on ● auto

bpdu-guard : ● off ○ on compatible : ● off ○ on

bpdu-filter : ● off ○ on rootguard : ● none ○ root

tc-guard : ● off ○ on tc-ignore : ● off ○ on



inst : 0

port-fast : ● off ○ on

auto-edge : ○ off ● on

bpdu-guard : ● off ○ on

bpdu-filter : ● off ○ on

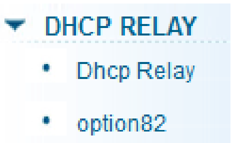
tc-guard : ● off ○ on

Mstp Port Information [Gi0/4]

```
------------------------------[Gi0/4]------------------------------
PortAdminPortFast: disable
PortOperPortFast: disable
PortAdminAutoEdge: enable
PortOperAutoEdge: disable
PortAdminLinkType: auto
PortOperLinkType: share
PortBPDUGuard: disable
PortBPDUFilter: disable
PortTCGuard: disable
```

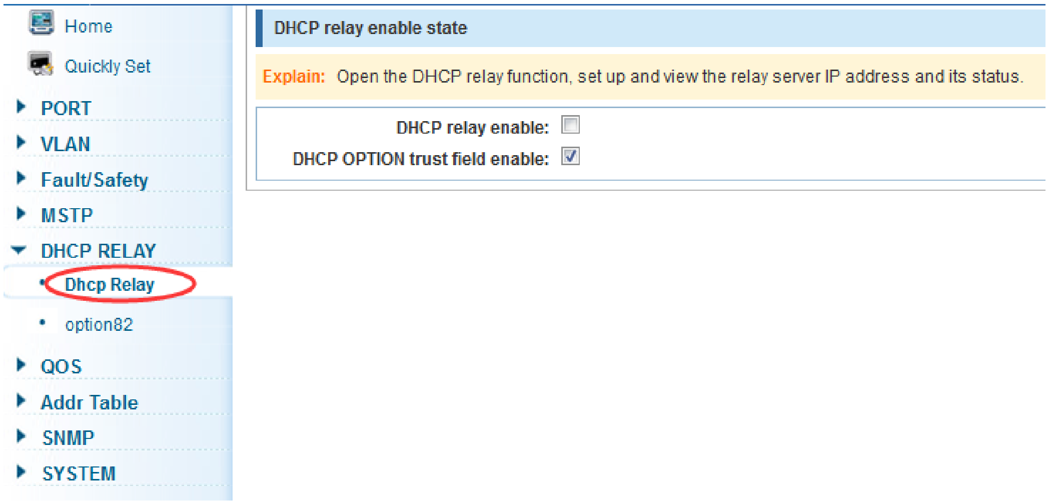
4.6 DHCP relay

In the navigation bar to select**"DHCP relay"**,you can set to the **DHCP relay and option82**。



4.6.1 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.the following picture



DHCP relay enable state

Explain: Open the DHCP relay function, set up and view the relay server IP address and its status.

DHCP relay enable: □
DHCP OPTION trust field enable: ☑

【parameter description】

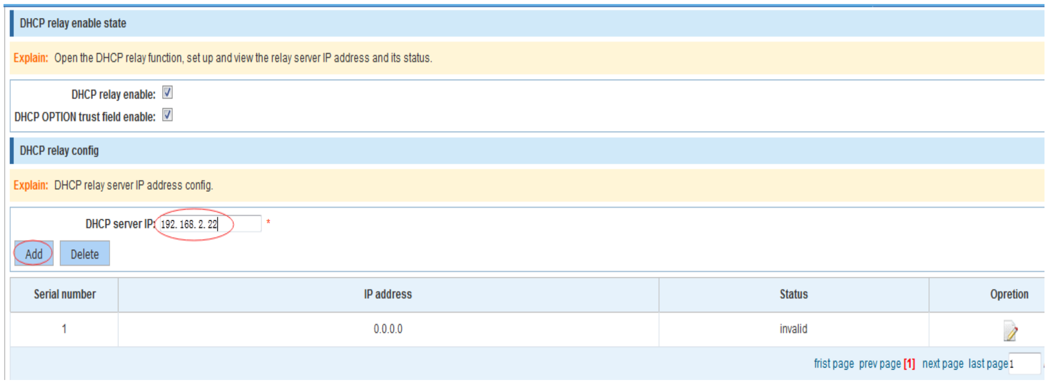
parameter	description
IP address	DHCP server address
status	Invalid and vaild

【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



DHCP relay enable state

Explain: Open the DHCP relay function, set up and view the relay server IP address and its status.

DHCP relay enable: ☑
DHCP OPTION trust field enable: ☑

DHCP relay config

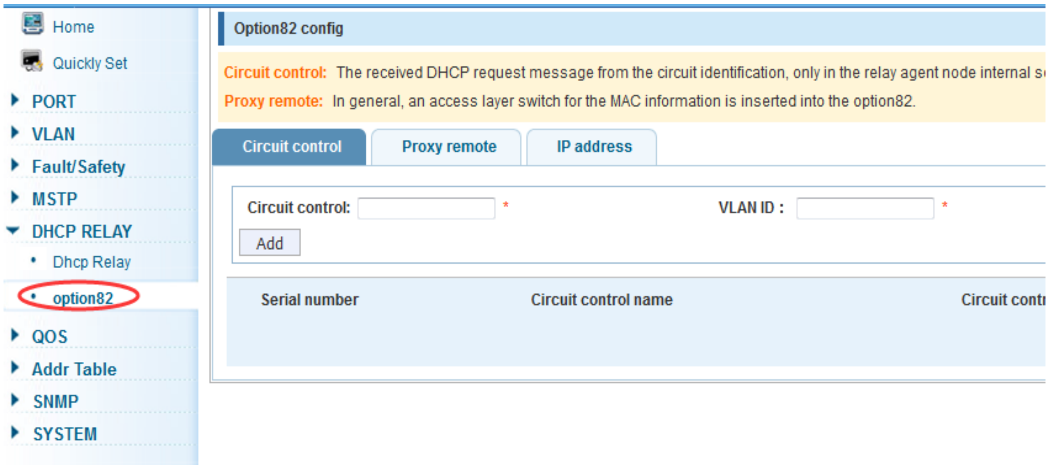
Explain: DHCP relay server IP address config.

DHCP server IP: 192. 168. 2. 22 *

Serial number	IP address	Status	Opretion
1	0.0.0.0	invalid	

4.6.2 0ption82

In the navigation bar to select**“DHCP relay>option82”**,can set to OPTION82circuit control、proxy remote 、ip address。the following picture:



Option82 config

Circuit control: The received DHCP request message from the circuit identification, only in the relay agent node internal s

Proxy remote: In general, an access layer switch for the MAC information is inserted into the option82.

Circuit control: * VLAN ID : *

Serial number	Circuit control name	Circuit contr

【parameter description】

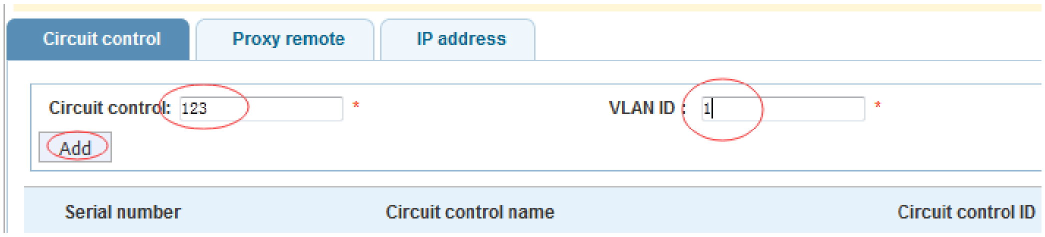
parameter	description
VLAN id	the DHCP request message in the VLAN, value range is 1 ~ 4094
Circuit control	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63
Proxy remote	Configuration ASCII remote id string value, the length of the range of 1 ~ 63
IP address	Decimal IP 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.

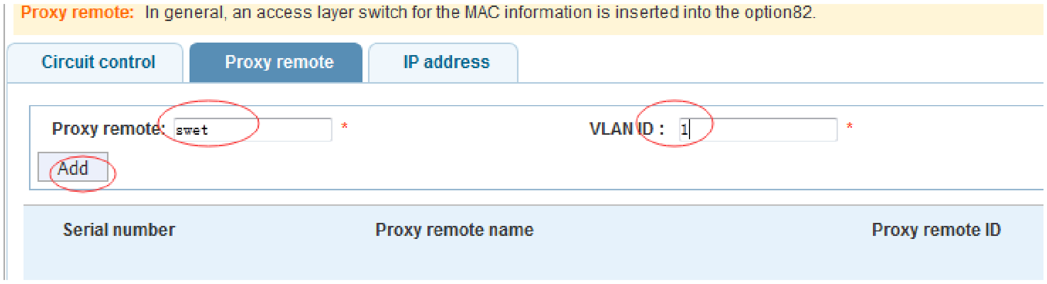
【Configuration example】

Sach as：add circuit control、proxy remote、ip address information



Circuit control: 123 * VLAN ID : 1 *

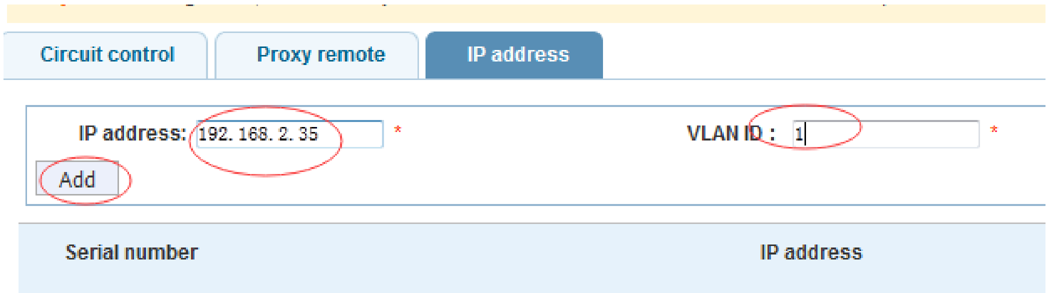
Serial number	Circuit control name	Circuit control ID



Proxy remote: In general, an access layer switch for the MAC information is inserted into the option82.

Proxy remote: swet * VLAN ID : 1 *

Serial number	Proxy remote name	Proxy remote ID



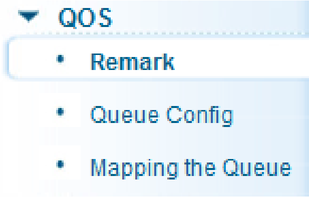
IP address: 192. 168. 2. 35 *

VLAN ID : 1 *

Serial number	IP address

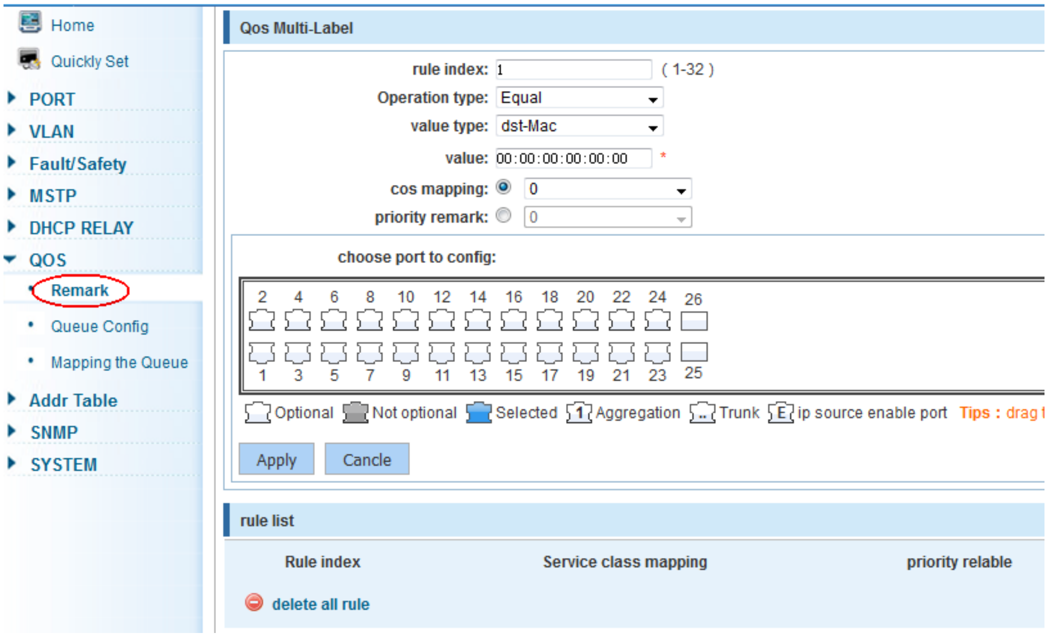
4.7 QoS

In the navigation bar to select**"QoS"**,you can set to the **Remark、queue config and mapping the queue**。



4.7.1 Remark

In the navigation bar to select**"QoS>Remark"**,According to the rules for port traffic bag tag or queue map。the following picture



rule index: 1 (1-32)

Operation type: Equal

value type: dst-Mac

value: 00:00:00:00:00:00 *

cos mapping: ● 0

priority remark: ○ 0

Rule index	Service class mapping	priority relable

【parameter description】

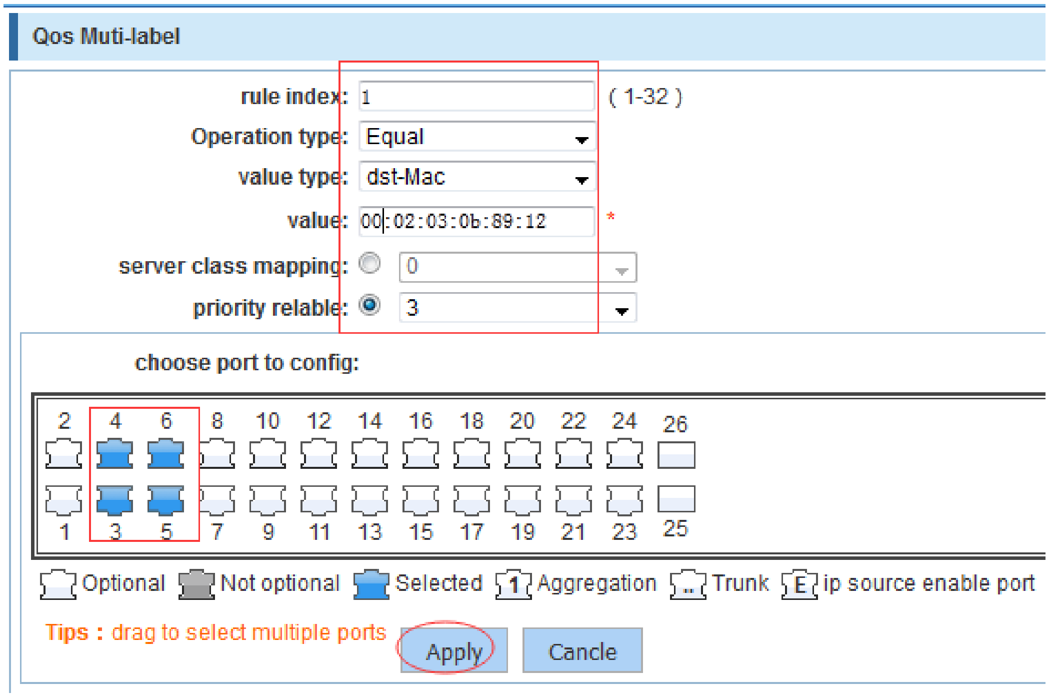
parameter	parameter
Rule index	By setting the rule of heavy tag index number, the current switch can be set up 32 rule
Operation type	Choose always said - match the match, all the data for tags Choose can be set to equal matching rules, comply with the rules of heavy tag data
Server class mapping	Adaptable 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



Qos Muti-label

rule index: 1 (1-32)

Operation type: Equal

value type: dst-Mac

value: 00:02:03:0b:89:12 *

server class mapping: ○ 0

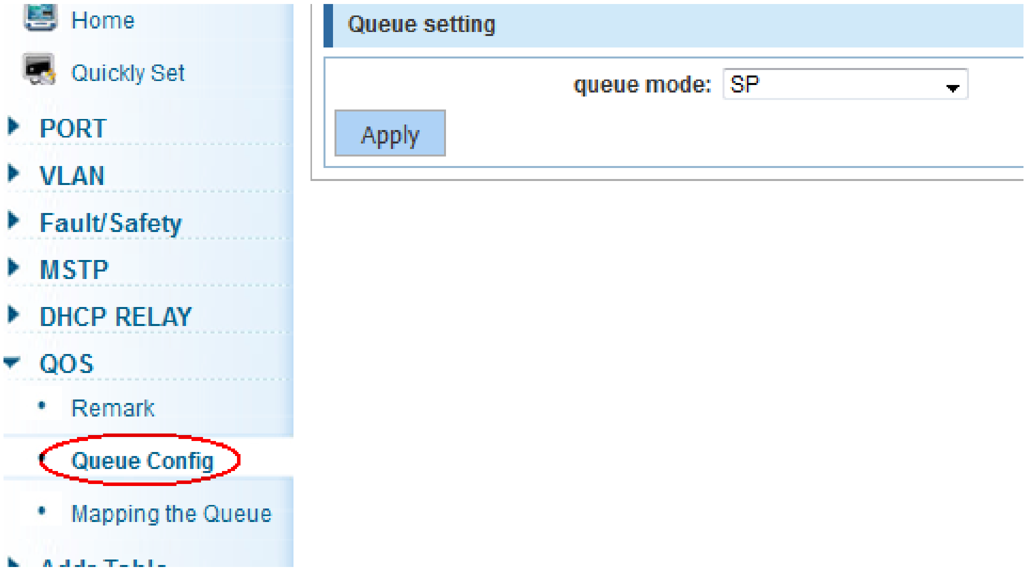
priority relable: ● 3

choose port to config:

Tips : drag to select multiple ports

4.7.2 Queue config

In the navigation bar to select“ **QoS>queue config”**,Can be set up queue scheduling policy 。 the following picture:



Queue setting

queue mode: SP

【parameter description】

parameter	description
Scheduling strategy	Can choose four kinds of modes: RR round-robin scheduling

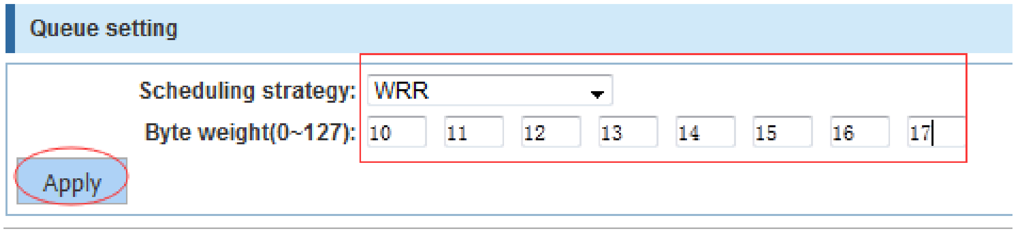
	SP absolute priority scheduling WRR weighted round-robin scheduling WFQ weighted fair scheduling
WRR-weights	Set the weights of each queue, they will be in proportion to occupy the bandwidth to send data

【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.



Queue setting

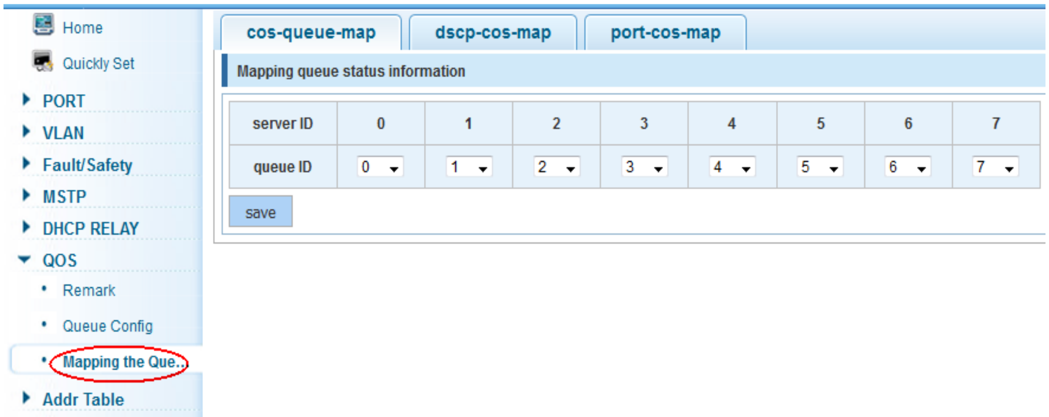
Scheduling strategy: WRR

Byte weight(0~127): 10 11 12 13 14 15 16 17

4.7.3 Mapping the queue

4.7.3.1 Service class queue mapping

In the navigation bar to select**“QoS>mapping the queue”**,Service category can be mapped to the corresponding queue.the following picture



Mapping queue status information

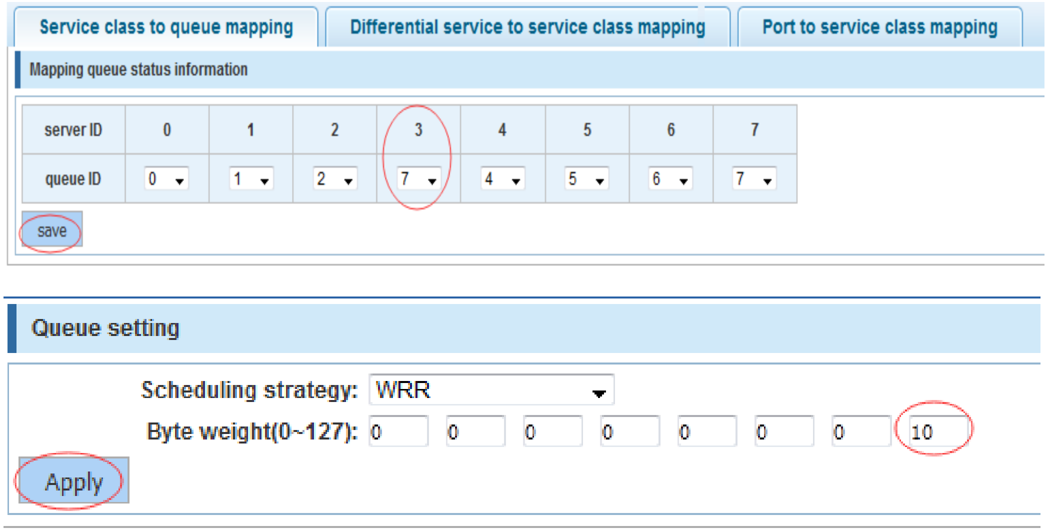
server ID	0	1	2	3	4	5	6	7
queue ID	0	1	2	3	4	5	6	7

【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


Service class to queue mapping
Differential service to service class mapping
Port to service class mapping

Mapping queue status information

server ID	0	1	2	3	4	5	6	7
queue ID	0	1	2	7	4	5	6	7

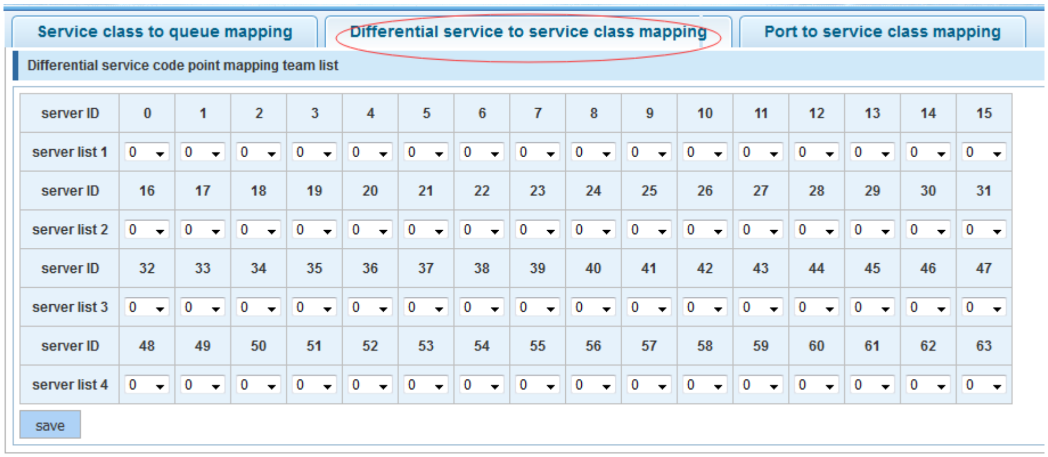
Queue setting

Scheduling strategy: WRR

Byte weight(0~127): 0 0 0 0 0 0 0 10

4.7.3.2 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.the following picture:


Service class to queue mapping
Differential service to service class mapping
Port to service class mapping

Differential service code point mapping team list

server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
server list 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
server list 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
server list 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
server list 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

【parameter description】

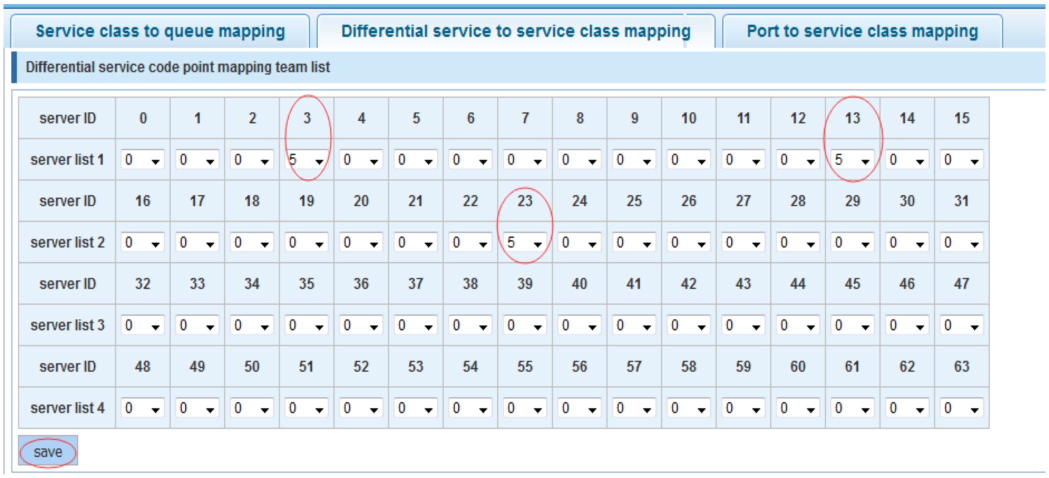
parameter	description
Server list	DSCP field has seven (0-63) is divided into four tables
Queue ID	Map the DSCP to COS fields (0 to 7), based on the cosine is mapped to a queue

【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

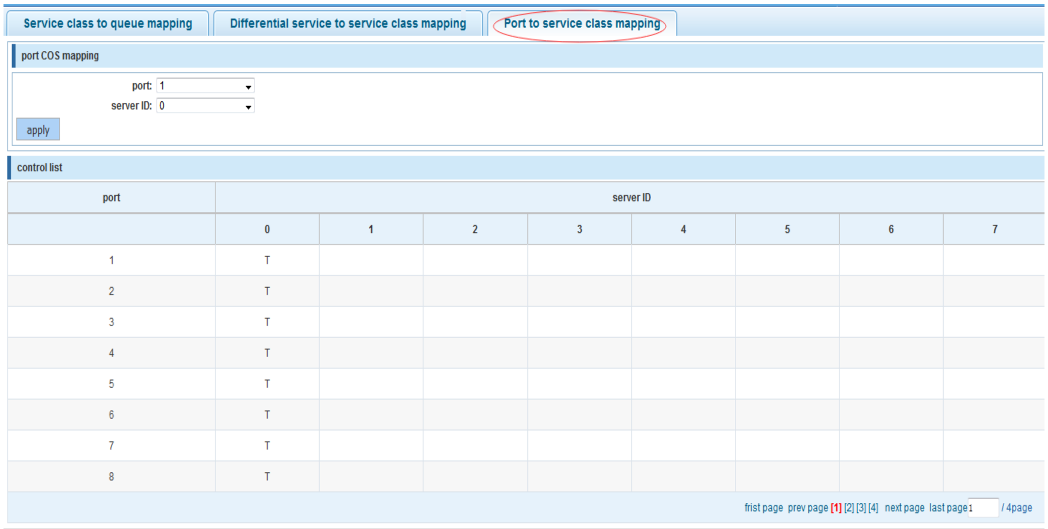

Service class to queue mapping
Differential service to service class mapping
Port to service class mapping
save

Differential service code point mapping team list

server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
server list 1	0	0	0	5	0	0	0	0	0	0	0	0	0	5	0	0
server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
server list 2	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0
server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
server list 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
server list 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

4.7.3.3 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。the following picture:


Service class to queue mapping
Differential service to service class mapping
Port to service class mapping
apply
frist page prev page [1] [2] [3] [4] next page last page 1 / 4page

port COS mapping

port: 1

server ID: 0

control list

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

【parameter description】

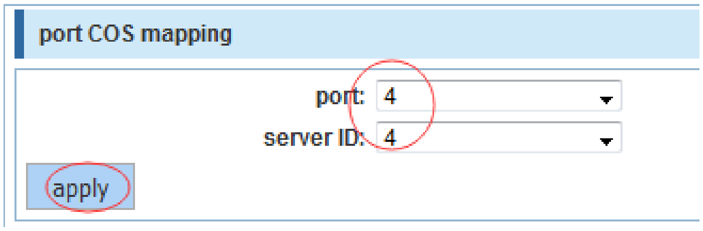
parameter	description
Port	Select the port number (0-24)
Service ID	Mapped to the service ID, and then according to the service ID into the queue

【instruction】

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

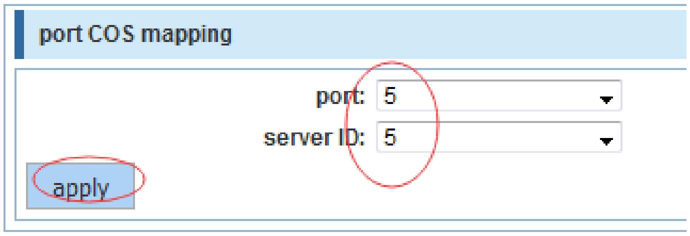
【Configuration example】

Such as：port 4、5、6 respectively cos4、cos5、cos6.


port COS mapping

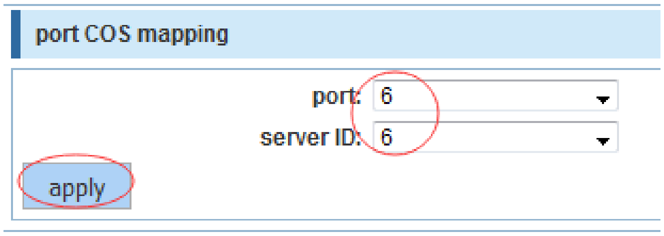
port: 4

server ID: 4


port COS mapping

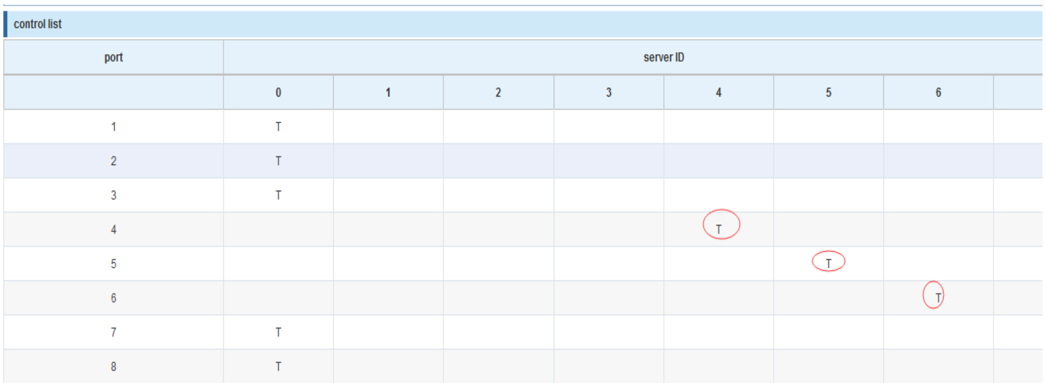
port: 5

server ID: 5


port COS mapping

port: 6

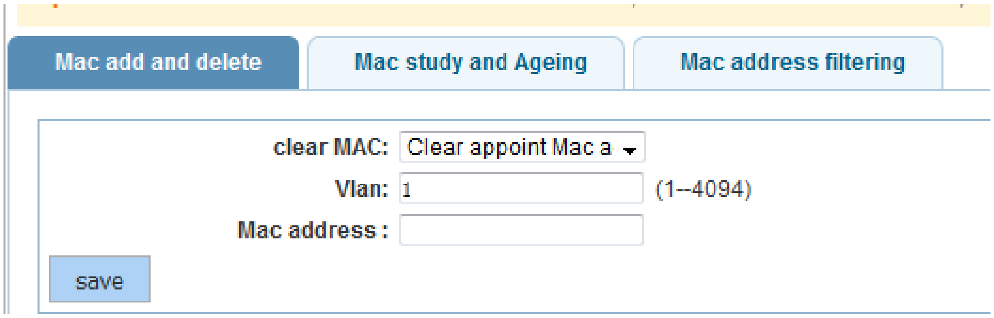
server ID: 6


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						

4.8 Address table

In the navigation bar to select**“Address table”**,you can set to **MAC add and delete**、**MACstudy and aging and MAC address filtering**。



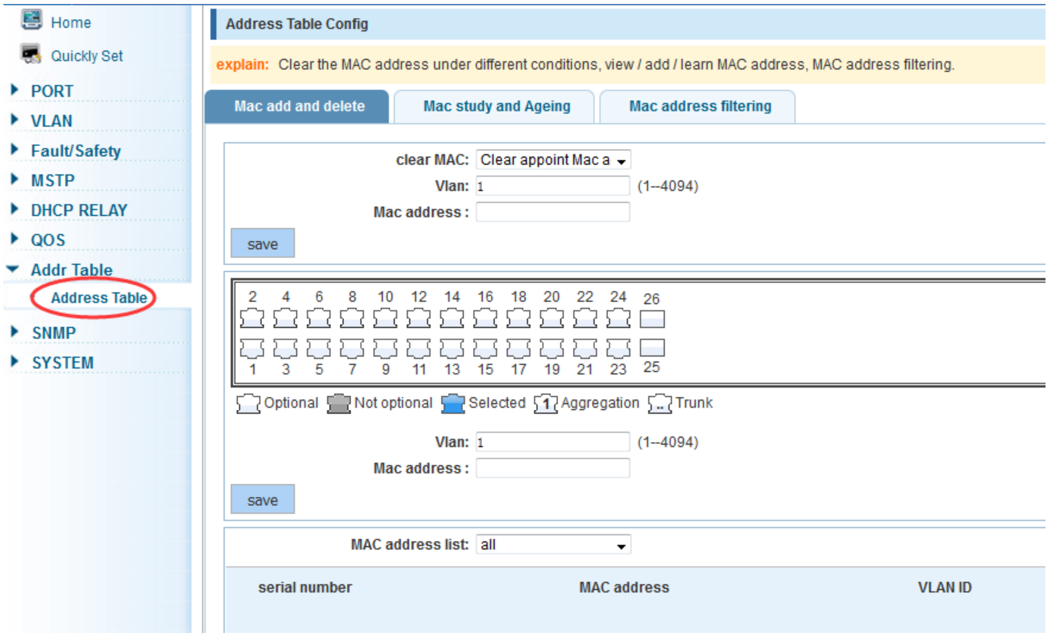
clear MAC: Clear appoint Mac a

Vlan: 1 (1--4094)

Mac address :

4.8.1 Mac add and delete

In the navigation bar to select**"Address table>Mac add and delete"**,You can add static Mac and delete Mac and view to the current of the Mac address table.the following picture:



Address Table Config

explain: Clear the MAC address under different conditions, view / add / learn MAC address, MAC address filtering.

clear MAC: Clear appoint Mac a

Vlan: 1 (1--4094)

Mac address :

Vlan: 1 (1--4094)

Mac address :

MAC address list: all

serial number	MAC address	VLAN ID

【parameter description】

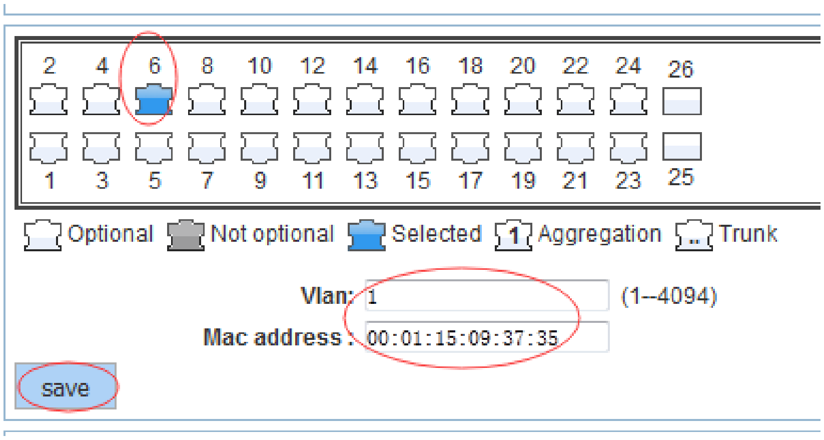
parameter	description
Clear Mac	Can choose to clear the multicast Mac address, clear dynamic unicast Mac address, clear static unicast Mac address, clear the specified Mac address, Mac address table
VLAN	Fill in the need to add or delete VLAN id, not create vlans to create can only take effect

【instruction】

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

【Configuration example】

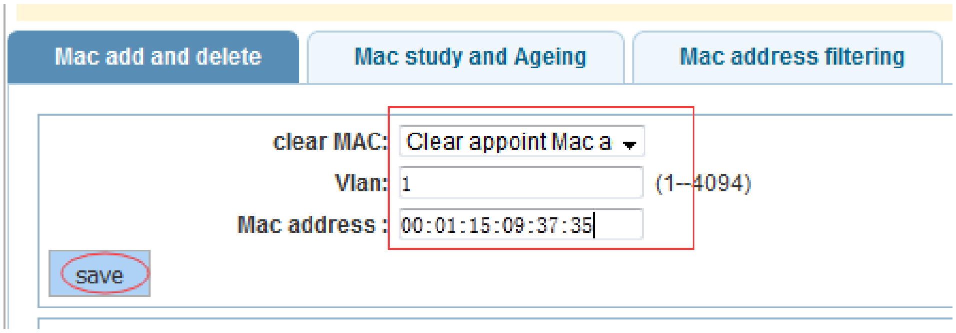
Such as: 1) the port 6 Mac set to static Mac



Vlan: 1 (1--4094)

Mac address : 00:01:15:09:37:35

2）clear port 6 static Mac addresses



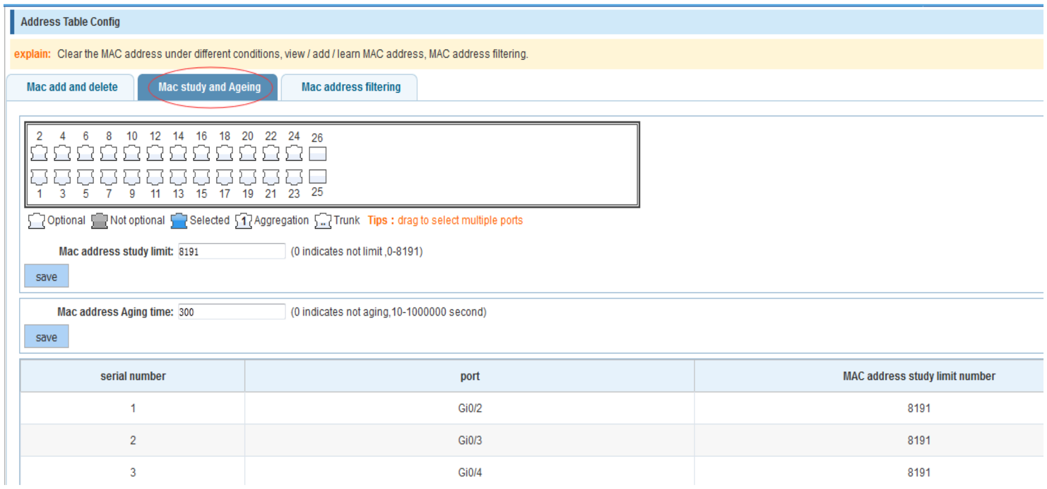
clear MAC: Clear appoint Mac a

Vlan: 1 (1--4094)

Mac address : 00:01:15:09:37:35

4.8.2 Mac study and laging

In the navigation bar to select“**address table>Mac study and laging**”,Can be set up port Mac address study limit and Mac address aging time . the following picture:



explain: Clear the MAC address under different conditions, view / add / learn MAC address, MAC address filtering.

Tips : drag to select multiple ports

Mac address study limit: 8191 (0 indicates not limit ,0-8191)

Mac address Aging time: 300 (0 indicates not aging,10-1000000 second)

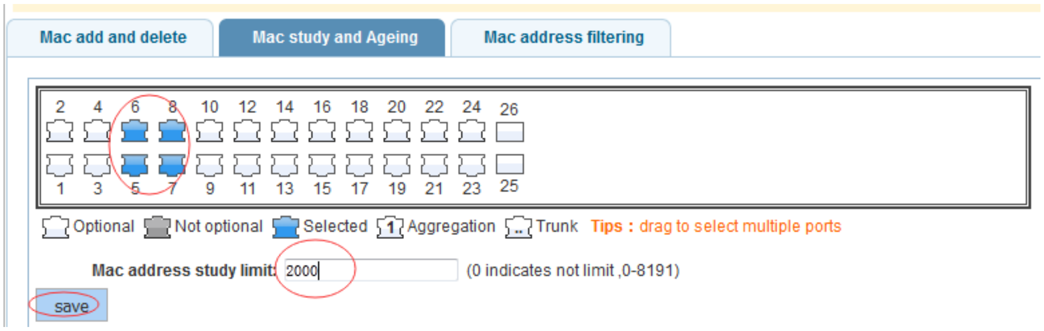
serial number	port	MAC address study limit number
1	Gi0/2	8191
2	Gi0/3	8191
3	Gi0/4	8191

【parameter description】

parameter	description
Mac address	Range 0-8191,default 8191
Mac address study limit	Default 300

【Configuration example】

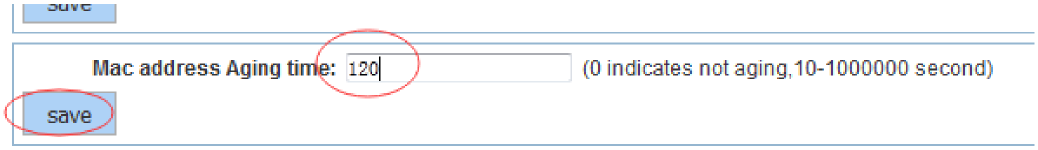
Such as: 1) setting port 5, 6, 7, 8 address study limit for 2000



Tips : drag to select multiple ports

Mac address study limit: 2000 (0 indicates not limit ,0-8191)

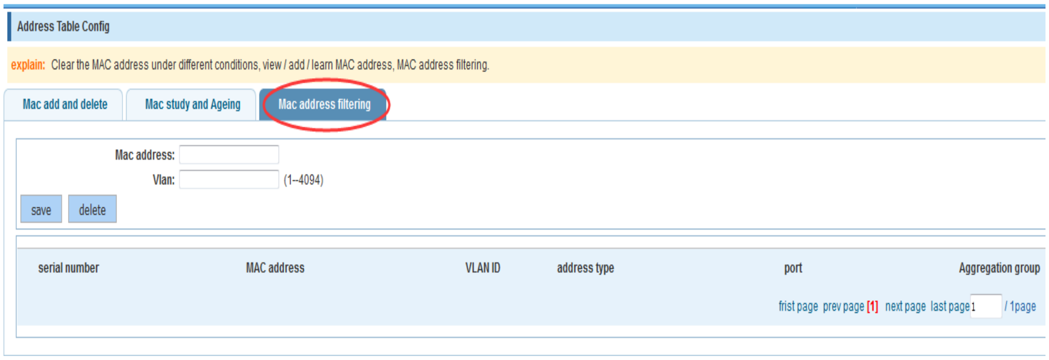
2) will be dropped or learn the Mac address of the port equipment after 2 minutes disappear automatically from the Mac address table



Mac address Aging time: 120 (0 indicates not aging,10-1000000 second)

4.8.3 Mac address filtering

In the navigation bar to select“**address table>Mac address table**”,Can be filtered according to the condition does not need the Mac address. the following picture:



explain: Clear the MAC address under different conditions, view / add / learn MAC address, MAC address filtering.

Mac address:

Vlan: (1--4094)

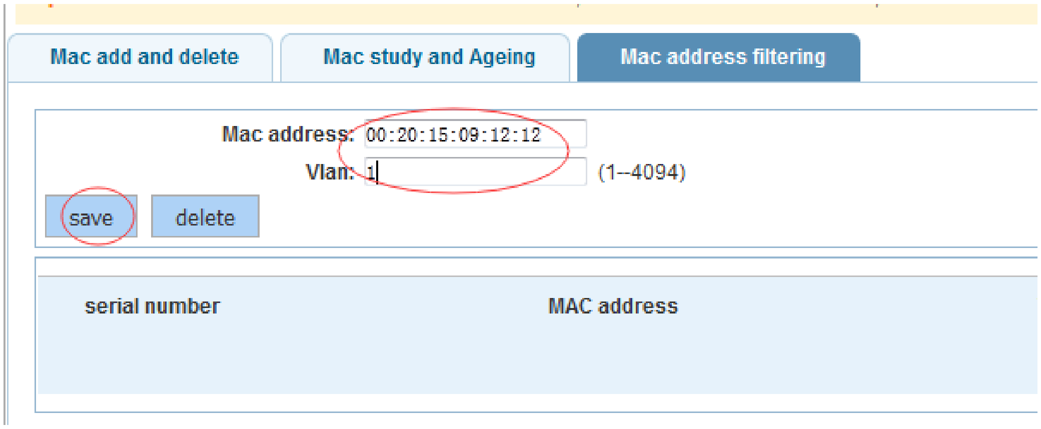
serial number	MAC address	VLAN ID	address type	port	Aggregation group

【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



Mac address: 00:20:15:09:12:12

Vlan: 1 (1--4094)

serial number	MAC address

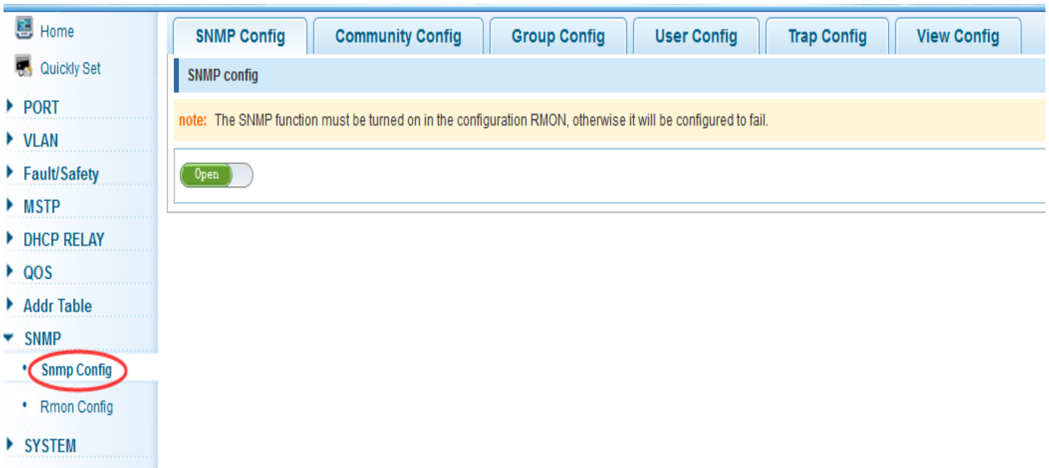
4.9 Snmp config

In the navigation bar to select**"Snmp"**,you can set to the **Snmp config and Rmon config**。

4.9.1 Snmp config

4.9.1.1 Snmp config

In the navigation bar to select**"Snmp >Snmp config"**,you can Snmp function enable。the following picture:



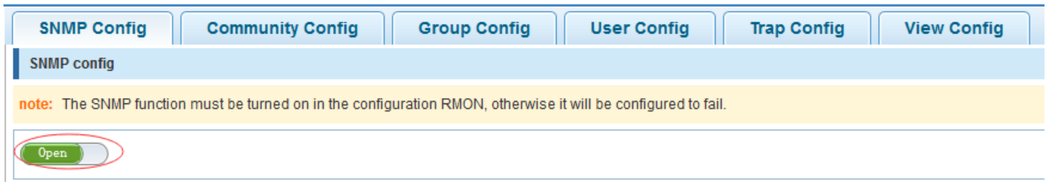
note: The SNMP function must be turned on in the configuration RMON, otherwise it will be configured to fail.

【instruction】

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

【Configuration example】

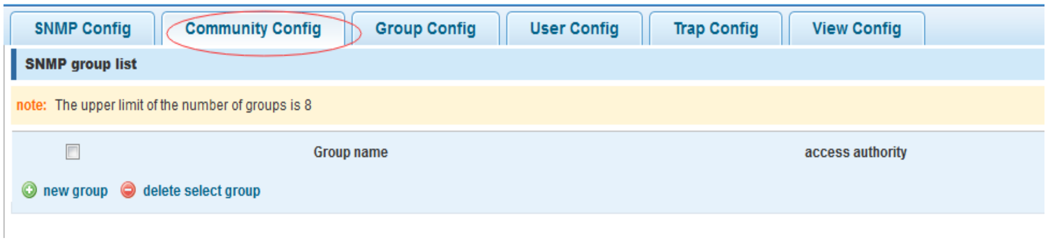
Such as： open Snmp



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

4.9.1.2 Community config

In the navigation bar to select“**Snmp >Snmp config>community config**”,Can specify group access. the following picture



note: The upper limit of the number of groups is 8

□	Group name	access authority

【parameter description】

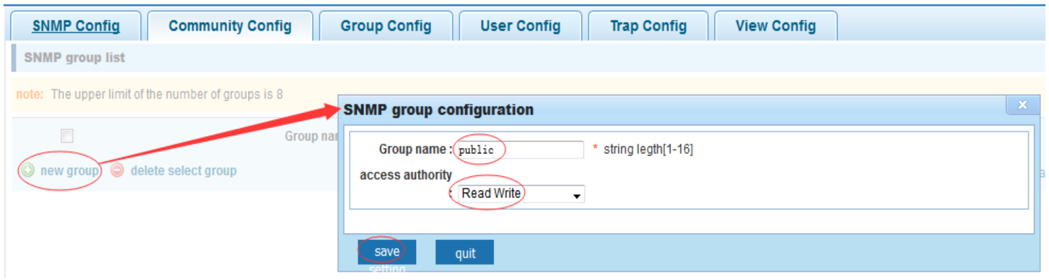
parameter	description
group	Community string, is equal to the NMS and Snmp agent communication between the password
Access authority	Read-only: specify the NMS (Snmp host) of MIB variables can only be read, cannot be modified Read-only can write: specify the NMS (Snmp host) of MIB variables can only 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



SNMP group list

note: The upper limit of the number of groups is 8

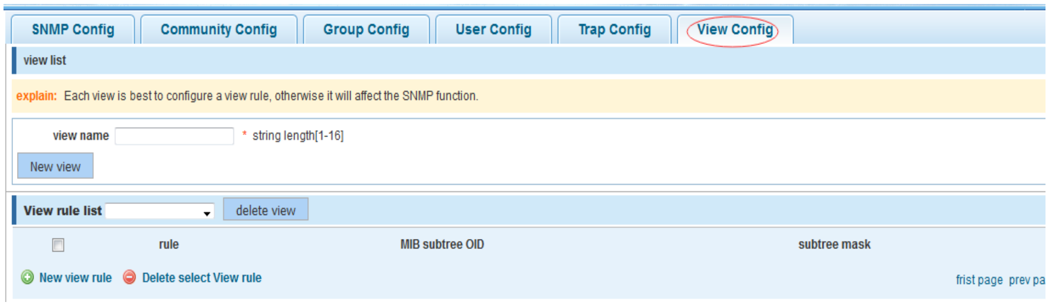
SNMP group configuration

Group name : public * string legth[1-16]

access authority Read Write

4.9.1.3 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. the following picture



view list

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

view name * string length[1-16]

View rule list

□	rule	MIB subtree OID	subtree mask

【parameter description】

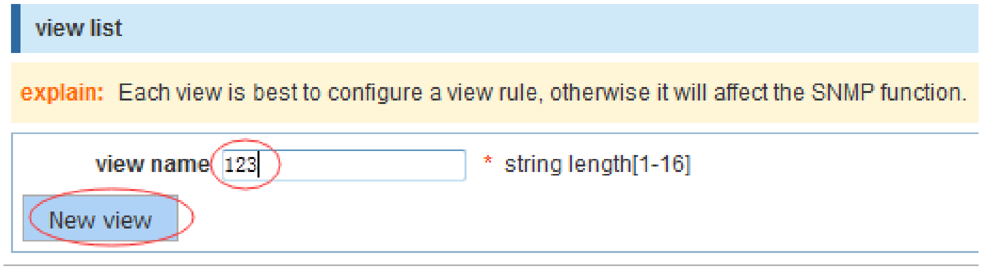
parameter	description
View name	Wiew mane
include	Indicate the MIB object number contained within the view
exclude	Indicate the MIB object son number was left out of view
MIB subtree OID	View the associated MIB object, is a number of MIB
subtree mask	MIB OID mask

【instruction】

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

【Configuration example】

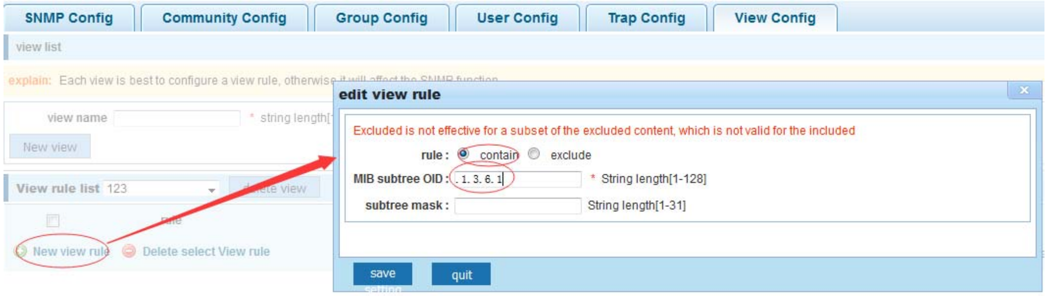
such as: establish a view 123 , MIB subtree oid .1.3.6.1 contain among them



view list

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

view name 123 * string length[1-16]



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

view name * string length[

edit view rule

Excluded is not effective for a subset of the excluded content, which is not valid for the included

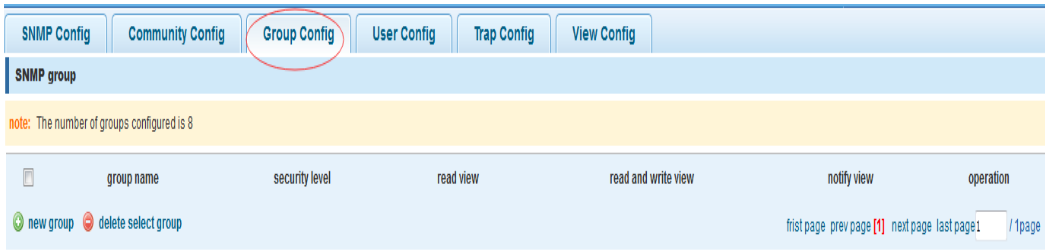
rule : ● contain ○ exclude

MIB subtree OID : .1.3.6.1 * String length[1-128]

subtree mask : String length[1-31]

4.9.1.4 Group config

In the navigation bar to select**"Snmp>Snmp config>group config"**,setting Snmp group。the following picture



note: The number of groups configured is 8

□	group name	security level	read view	read and write view	notify view	operation

frist page prev page [1] next page last page 1 / 1page

【parameter description】

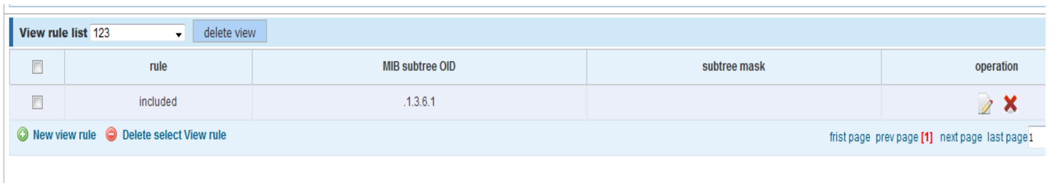
parameter	description
Group name	Group name
Security level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not 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.

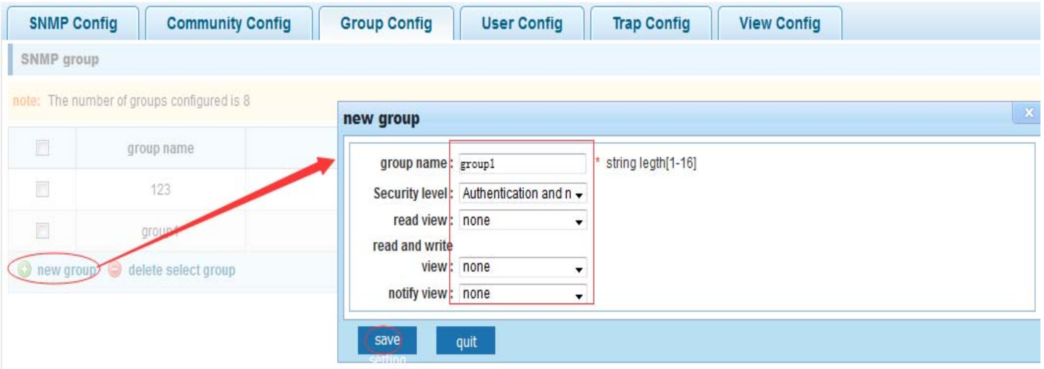
【Configuration example】

Such as: firstly, new view 123, then new group of goup1



View rule list 123

□	rule	MIB subtree OID	subtree mask	operation
□	included	.1.3.6.1		



note: The number of groups configured is 8

group name: group1 * string legth[1-16]

Security level: Authentication and n

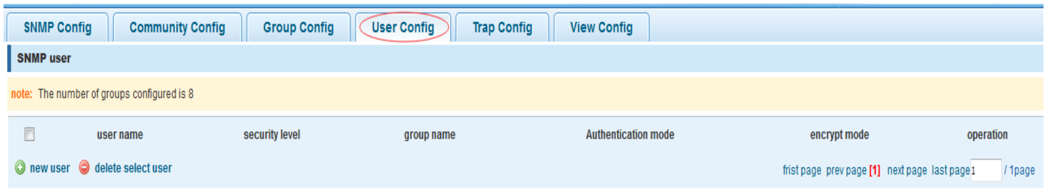
read view: none

read and write view: none

notify view: none

4.9.1.5 User config

In the navigation bar to select**“Snmp>Snmp config>user config”**,setting Snmp user。the following picture:



note: The number of groups configured is 8

□	user name	security level	group name	Authentication mode	encrypt mode	operation

【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

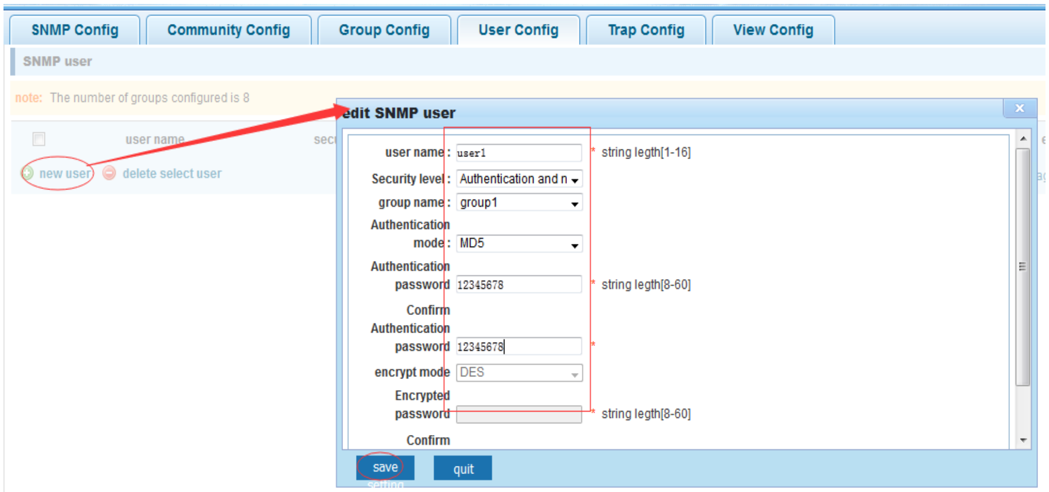
	protocol
Group name	A user group name
encrypt password	Range 8-60

【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



note: The number of groups configured is 8

user name : user1 * string legth[1-16]

Security level : Authentication and n

group name : group1

Authentication mode : MD5

Authentication password 12345678 * string legth[8-60]

Confirm Authentication password 12345678 *

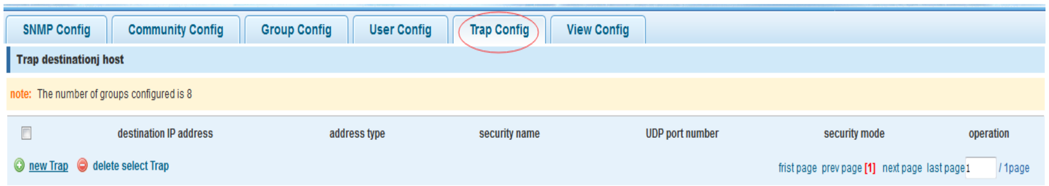
encrypt mode DES

Encrypted password * string legth[8-60]

Confirm

4.9.1.6 Trap

In the navigation bar to select**“Snmp>Snmp config>Trap”**,Can specify sent the trap messages to Snmp host (NMS). the following picture:



note: The number of groups configured is 8

□	destination IP address	address type	security name	UDP port number	security mode	operation

【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

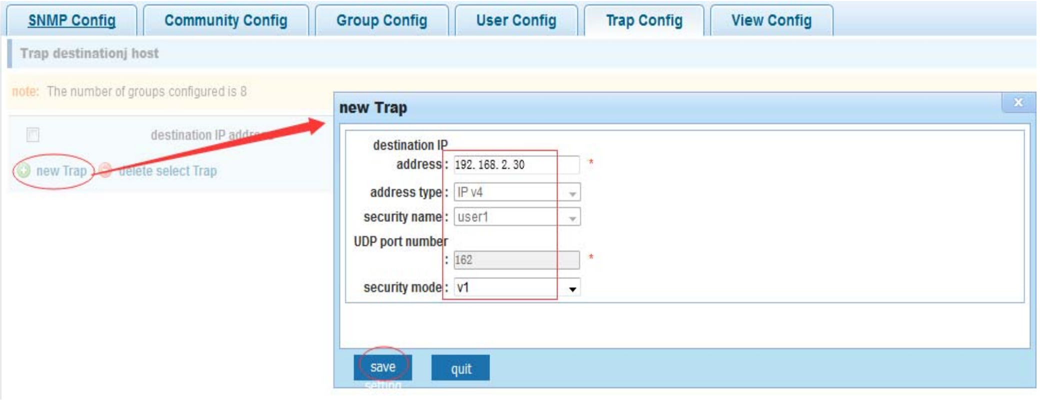
	protocol
Group name	User group name

【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 port statistical fluctuation threshold.

【Configuration example】

Such as：setting hoset 192.168.2.30 receive trap information

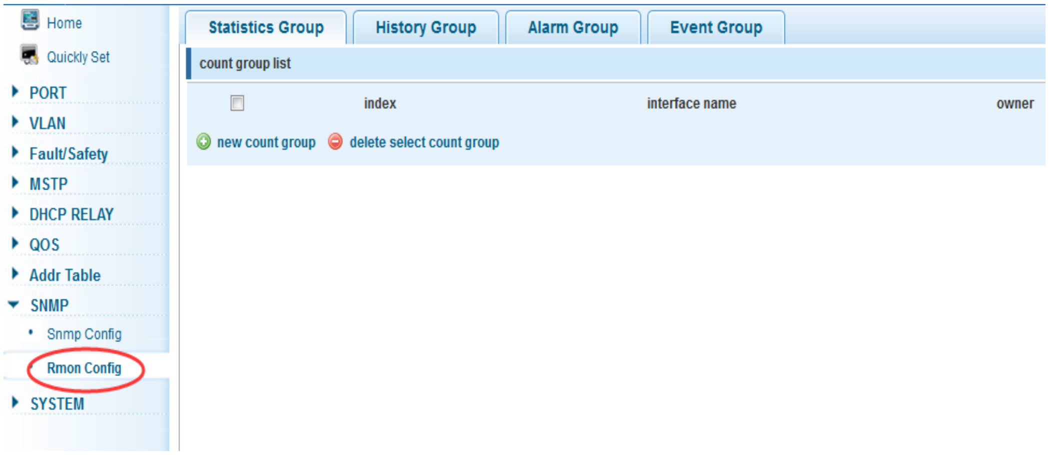


destination IP address: 192. 168. 2. 30 *
address type: IP v4
security name: user1
UDP port number: 162 *
security mode: v1

4.9.2 Rmon config

4.9.2.1 Statistics group

In the navigation bar to select**“Snmp>Rmon config>**statistics group**”**,Set an Ethernet interface statistics 。the following picture:



【parameter description】

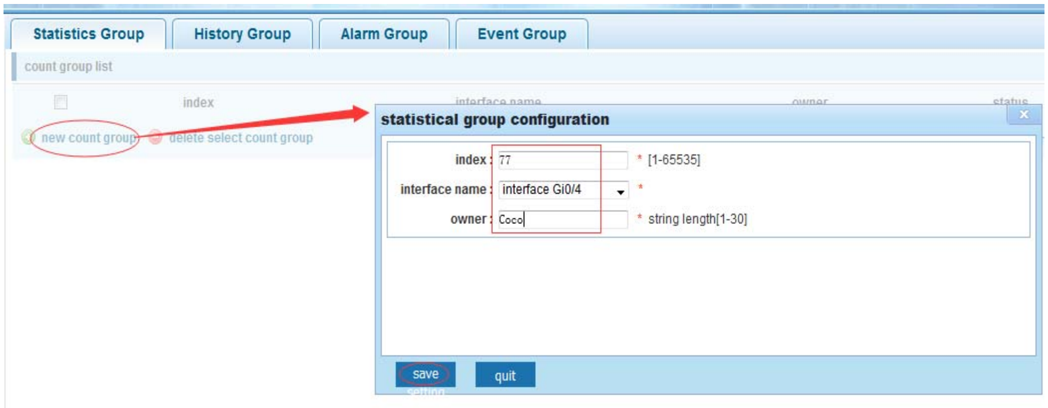
parameter	description
index	The index number, the value range of statistical information table is 1 ~ 65535
Interface mane	To monitor the source port
ower	Set the table creator, range: 1 ~ 30 characters of a string

【instruction】

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

【Configuration example】

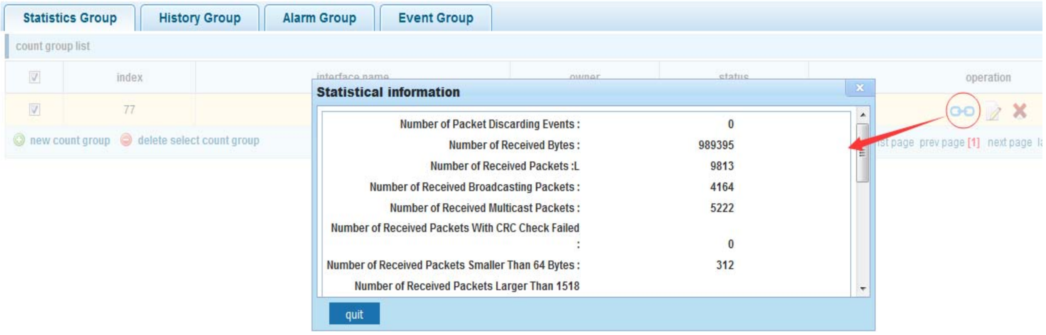
Such as: set up monitoring Ethernet port after 4 to check the data



index : 77 * [1-65535]

interface name : interface Gi0/4 *

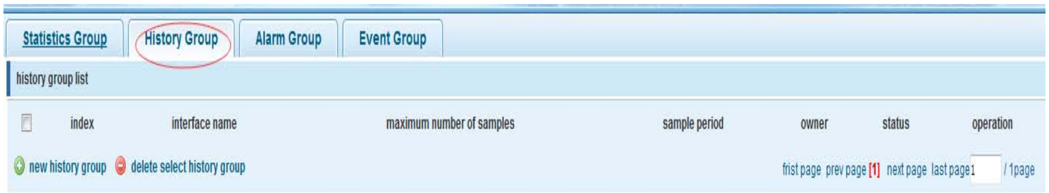
owner : Coco * string length[1-30]



Number of Packet Discarding Events :	0
Number of Received Bytes :	989395
Number of Received Packets :L	9813
Number of Received Broadcasting Packets :	4164
Number of Received Multicast Packets :	5222
Number of Received Packets With CRC Check Failed :	0
Number of Received Packets Smaller Than 64 Bytes :	312
Number of Received Packets Larger Than 1518	

4.9.2.2 History group

In the navigation bar to select**“Snmp>Rmon config>history group”,**Record the history of an Ethernet interface information. the following picture



【parameter description】

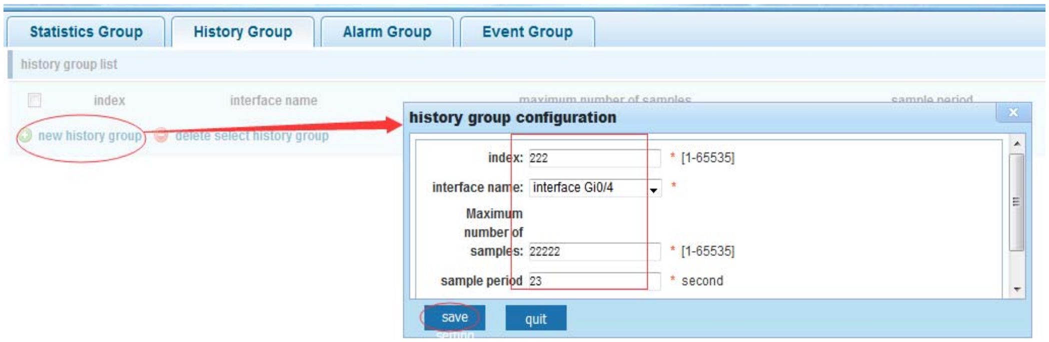
parameter	description
index	Historical control table item index number, value range is 1 ~ 65535
Interface name	To record the Ethernet interface
Maximum number of samples	Set the history control table item of the corresponding table capacity, namely the Max for number of records the history table, value 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



index: 222 * [1-65535]

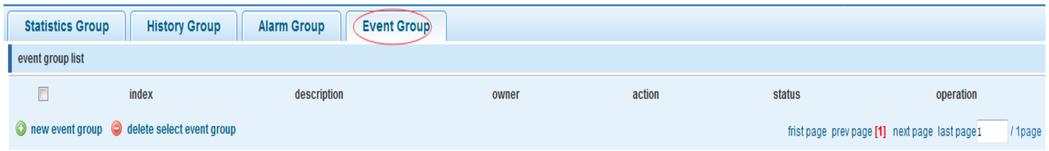
interface name: interface Gi0/4 *

Maximum number of samples: 22222 * [1-65535]

sample period 23 * second

4.9.2.3 Event group

In the navigation bar to select“**Snmp >Rmon config>event group”**,The way in which define events trigger and record them. the following picture



【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

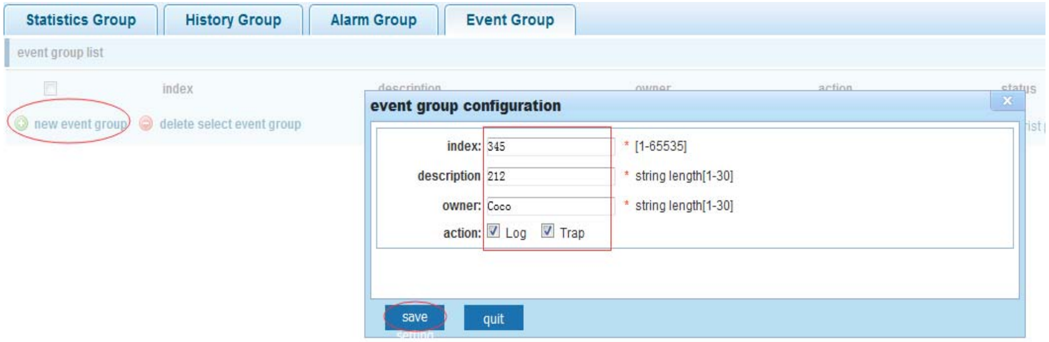
	send the Trap message Log events, when the event is triggered, the system will log
owner	Set the table creator, ownername for 1 ~ 30 characters of a string

【instruction】

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

【Configuration example】

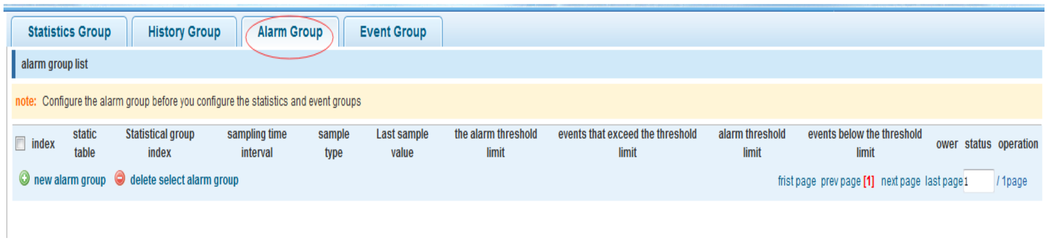
Such as: create an event to trigger 345, the system sends the trap message and log



index: 345 * [1-65535]
description 212 * string length[1-30]
owner: Coco * string length[1-30]
action: ☑ Log ☑ Trap

4.9.2.4 Alarm group

In the navigation bar to select“ **Snmp>Rmon config>alarm group”**,define alarm group。the following picture



note: Configure the alarm group before you configure the statistics and event groups

□ index	static table	Statistical group index	sampling time interval	sample type	Last sample value	the alarm threshold limit	events that exceed the threshold limit	alarm threshold limit	events below the threshold limit	ower	status	operation

【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

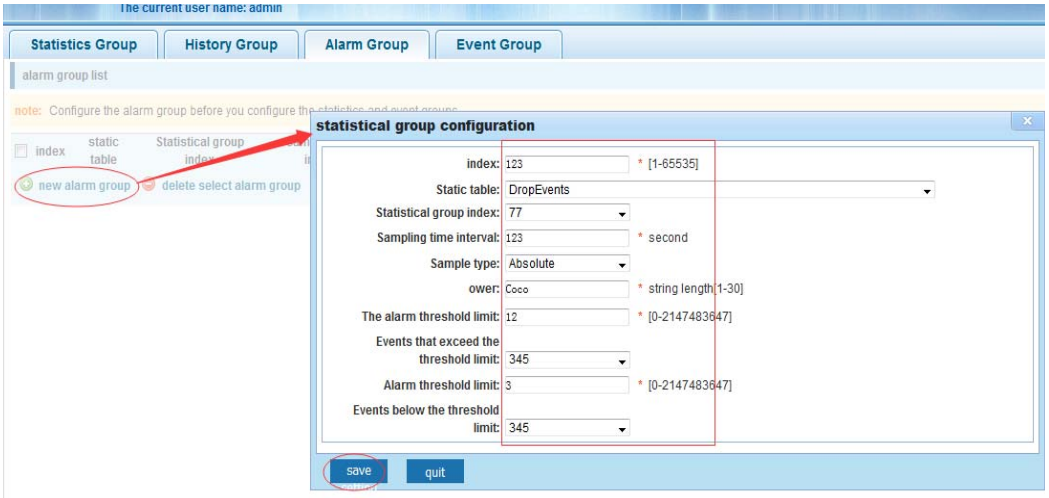
Sampling interval	Sampling time interval, the scope for 5 ~ 65535, the unit for seconds
The sampling type	Sample types for the absolute value of sampling, the sampling time arrived directly extracting the value of a variable
The latest sampling	Sampling type for change value sampling, extraction of the 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



note: Configure the alarm group before you configure the statistics and event groups

statistical group configuration

index: 123 * [1-65535]

Static table: DropEvents

Statistical group index: 77

Sampling time interval: 123 * second

Sample type: Absolute

ower: Coco * string length[1-30]

The alarm threshold limit: 12 * [0-2147483647]

Events that exceed the threshold limit: 345

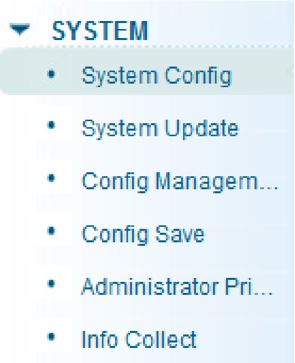
Alarm threshold limit: 3 * [0-2147483647]

Events below the threshold limit: 345

4.10 SYSTEM

In the navigation bar to select**"SYSTEM"**,you can set to the **system config**、**system**

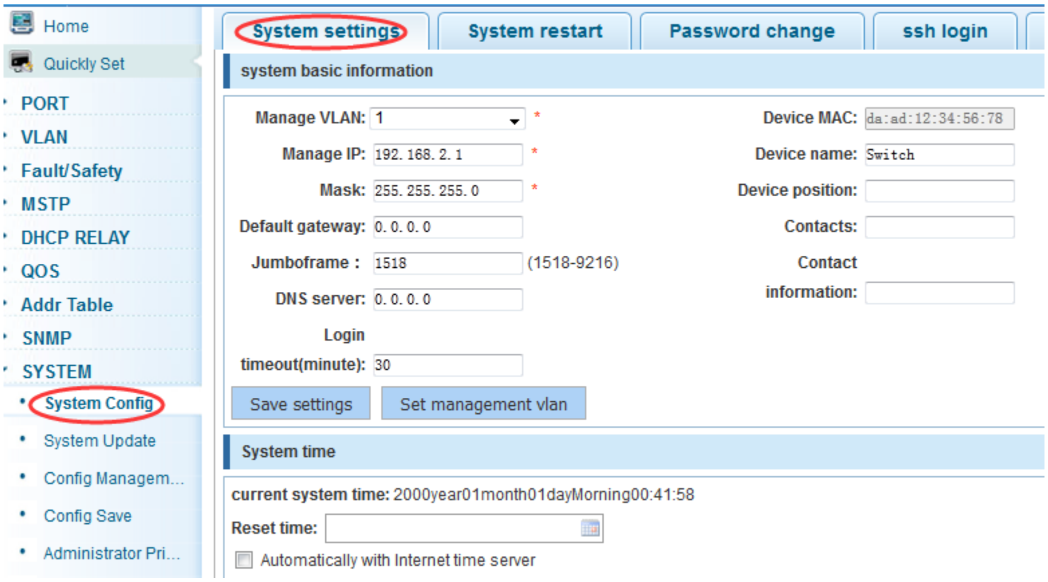
update、config management、config save、administor privileges and info collect。



4.10.1 System config

4.10.1.1 System settings

In the navigation bar to select**"SYSTEM>system config>System settings"**,Basic information set switch. the following picture:



system basic information

Manage VLAN: 1 *

Manage IP: 192. 168. 2. 1 *

Mask: 255. 255. 255. 0 *

Default gateway: 0. 0. 0. 0

Jumboframe : 1518 (1518-9216)

DNS server: 0. 0. 0. 0

Login timeout(minute): 30

Device MAC: da:ad:12:34:56:78

Device name: Switch

Device position:

Contacts:

Contact information:

System time

current system time: 2000year01month01dayMorning00:41:58

Reset time:

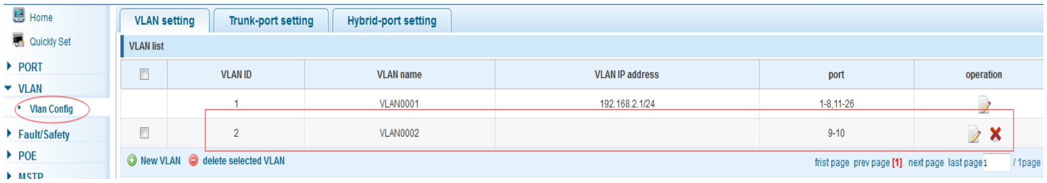
□ Automatically with Internet time server

【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

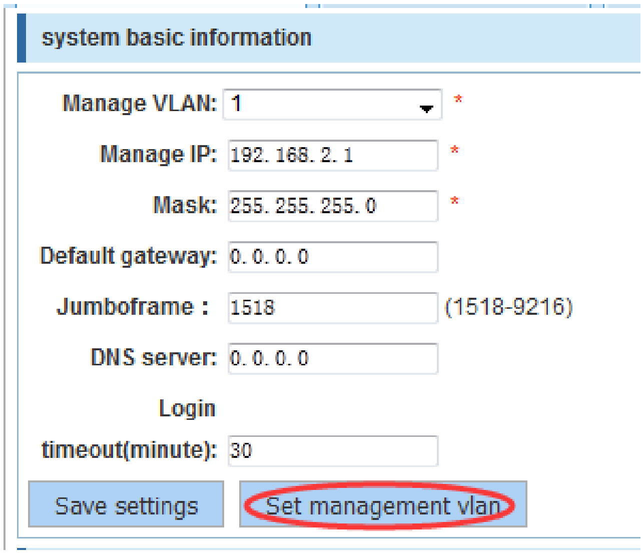
【Configuration example】

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



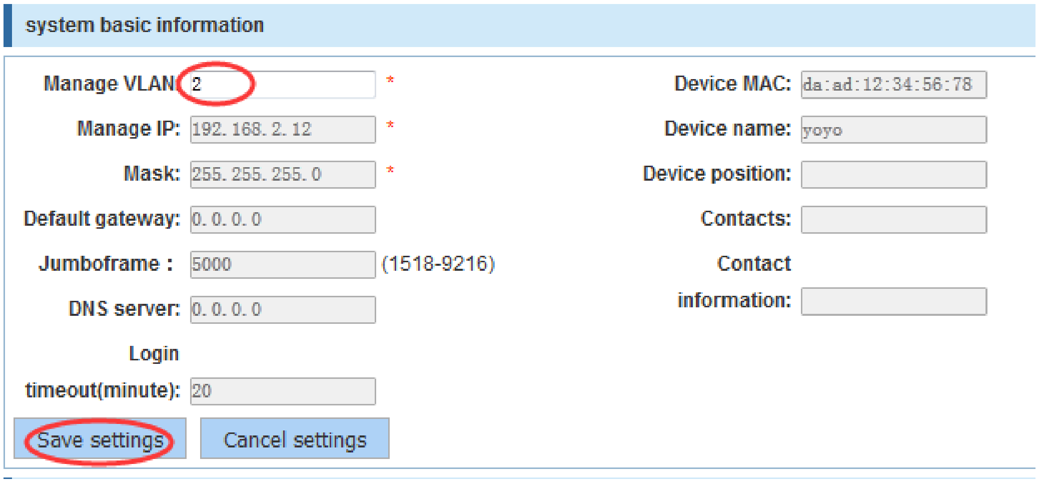
VLAN list

□	VLAN ID	VLAN name	VLAN IP address	port	operation
	1	VLAN0001	192.168.2.1/24	1-8,11-26	✎
□	2	VLAN0002		9-10	✎ ✗



system basic information

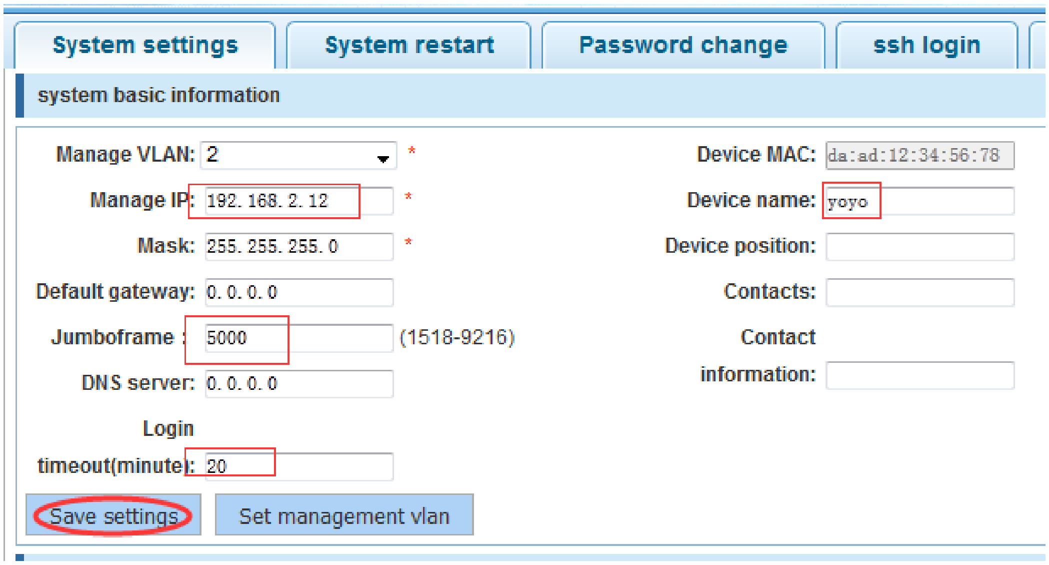
Manage VLAN:	1	*
Manage IP:	192. 168. 2. 1	*
Mask:	255. 255. 255. 0	*
Default gateway:	0. 0. 0. 0	
Jumboframe :	1518	(1518-9216)
DNS server:	0. 0. 0. 0	
Login timeout(minute):	30	



system basic information

Manage VLAN	2	*	Device MAC:	da:ad:12:34:56:78
Manage IP:	192. 168. 2. 12	*	Device name:	yoyo
Mask:	255. 255. 255. 0	*	Device position:	
Default gateway:	0. 0. 0. 0		Contacts:	
Jumboframe :	5000	(1518-9216)	Contact information:	
DNS server:	0. 0. 0. 0			
Login timeout(minute):	20			

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 ,Jumboframe for 5000.



System settings | System restart | Password change | ssh login

system basic information

Manage VLAN: 2 *

Manage IP: 192. 168. 2. 12 *

Mask: 255. 255. 255. 0 *

Default gateway: 0. 0. 0. 0

Jumboframe : 5000 (1518-9216)

DNS server: 0. 0. 0. 0

Login timeout(minute): 20

Device MAC: da:ad:12:34:56:78

Device name: yoyo

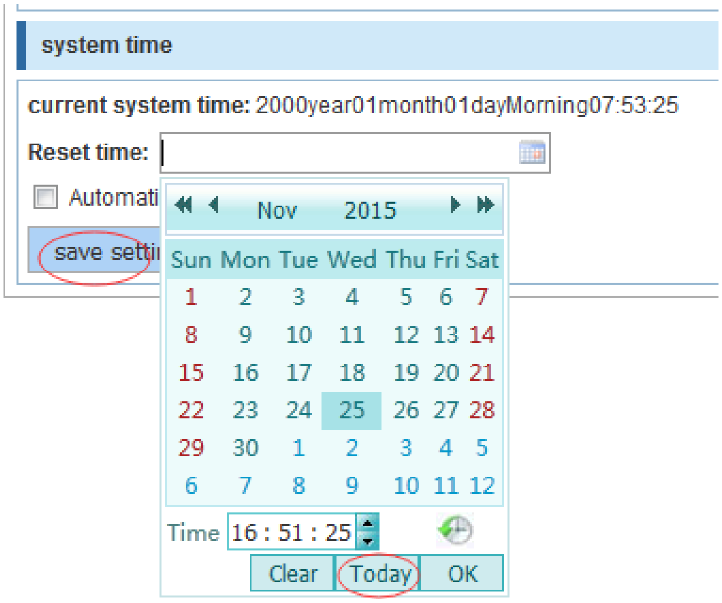
Device position:

Contacts:

Contact information:

Save settings | Set management vlan

3) use 192.168.1.12 logging in, sets the system time



system time

current system time: 2000year01month01dayMorning07:53:25

Reset time:

□ Automati

save setti

Nov 2015

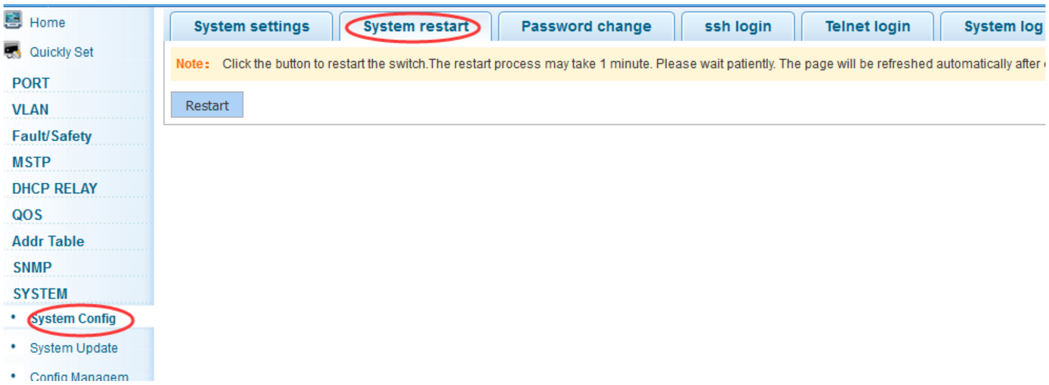
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Time 16 : 51 : 25

Clear | Today | OK

4.10.1.2 System restart

In the navigation bar to select“**SYSTEM>system config>system restart**”,equipment can be restarted. the following picture:



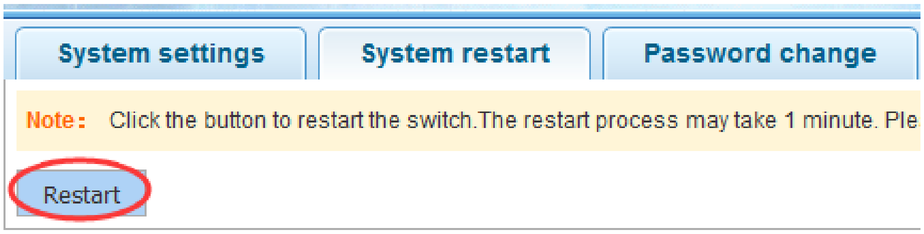
Note： Click the button to restart the switch.The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after

【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】

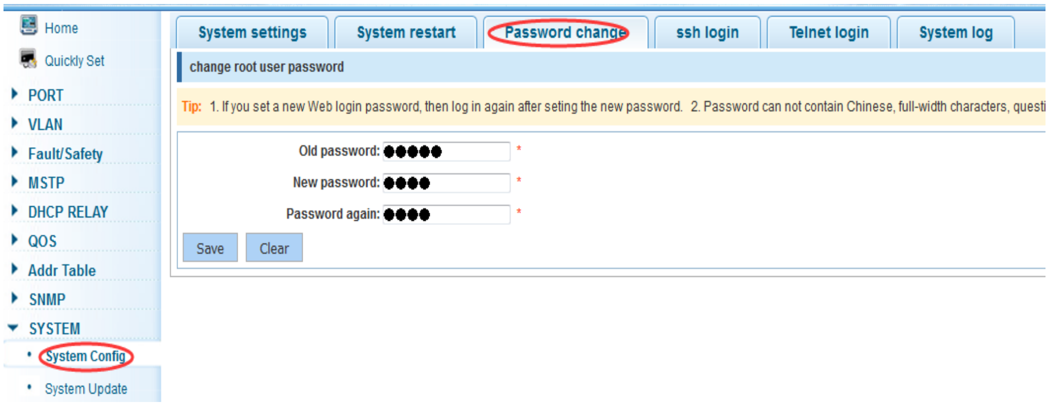
Such as：click“restart”button



Note： Click the button to restart the switch.The restart process may take 1 minute. Ple

4.10.1.3 Password change

In the navigation bar to select**“SYSTEM>system config>password change”**,The password change to equipment. the following picture：



change root user password

Tip: 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, questi

Old password: ●●●●● *

New password: ●●●● *

Password again: ●●●● *

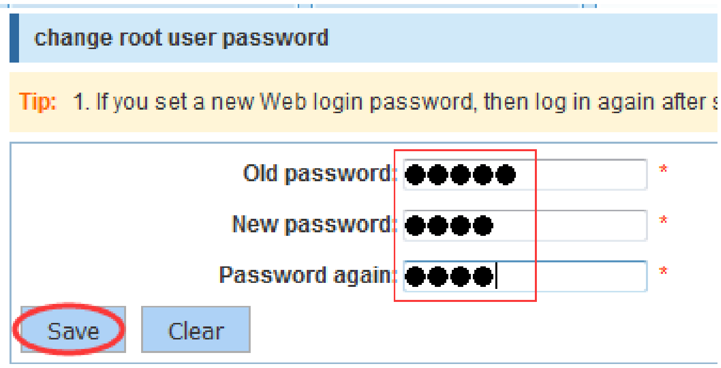
【instruction】

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.



change root user password

Tip: 1. If you set a new Web login password, then log in again after s

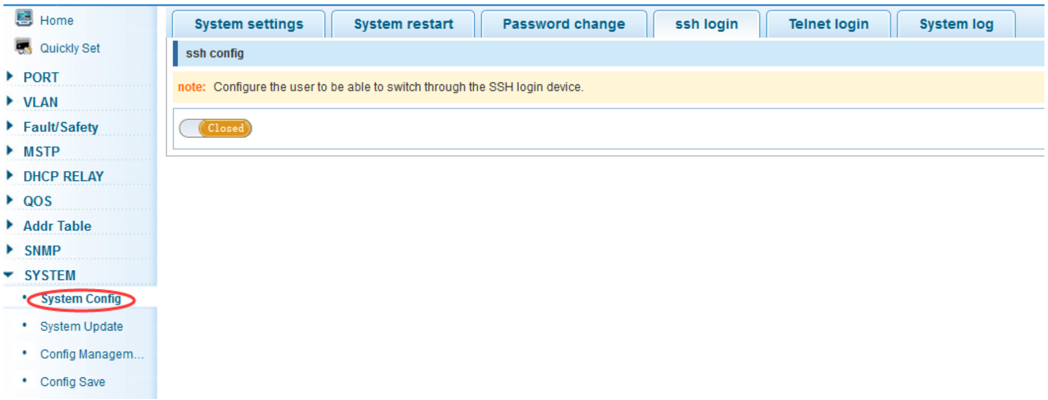
Old password: ●●●●● *

New password: ●●●● *

Password again: ●●●● *

4.10.1.4 SSH login

In the navigation bar to select“**SYSTEM>system config>ssh login**”,SSH open。the following picture：



ssh config

note: Configure the user to be able to switch through the SSH login device.

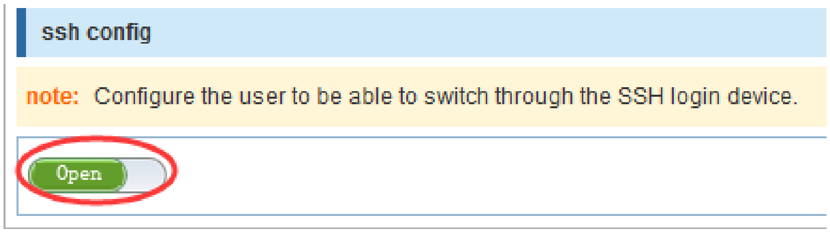
Closed

【instruction】

Configure the user to be able to switch through the SSH login device.

【Configuration example】

Such as：SSH open,you can CRT to log in

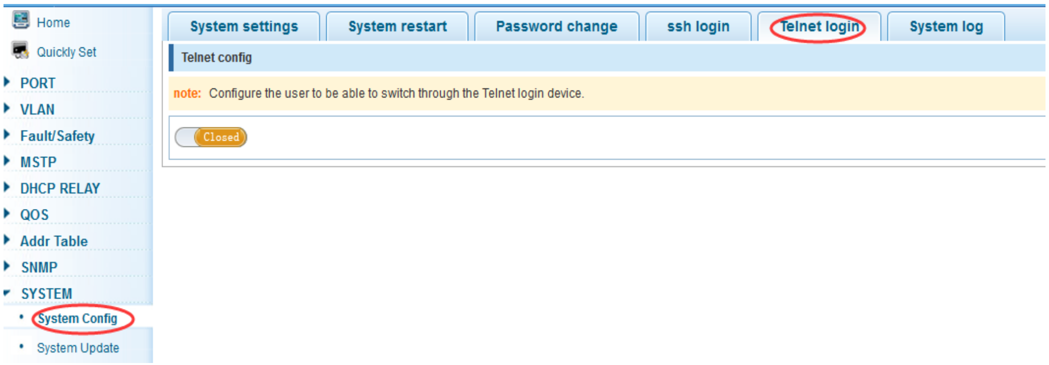


ssh config

note: Configure the user to be able to switch through the SSH login device.

4.10.1.5 Telnet login

In the navigation bar to select**“SYSTEM>system config>Telnet login”**,Telnet open。The following picture：



Telnet config

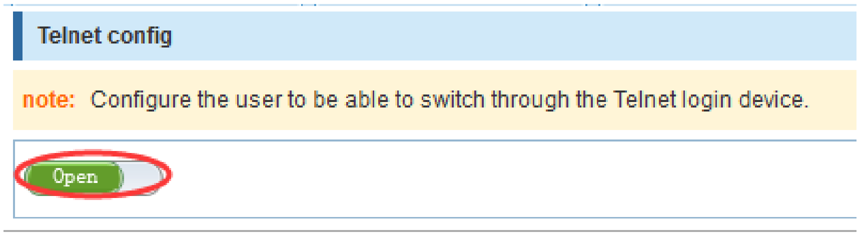
note: Configure the user to be able to switch through the Telnet login device.

【instruction】

Configure the user to be able to switch through the Telnet login device.

【Configuration example】

Such as：Telnet open,PC Telnet functiono open,you can log in

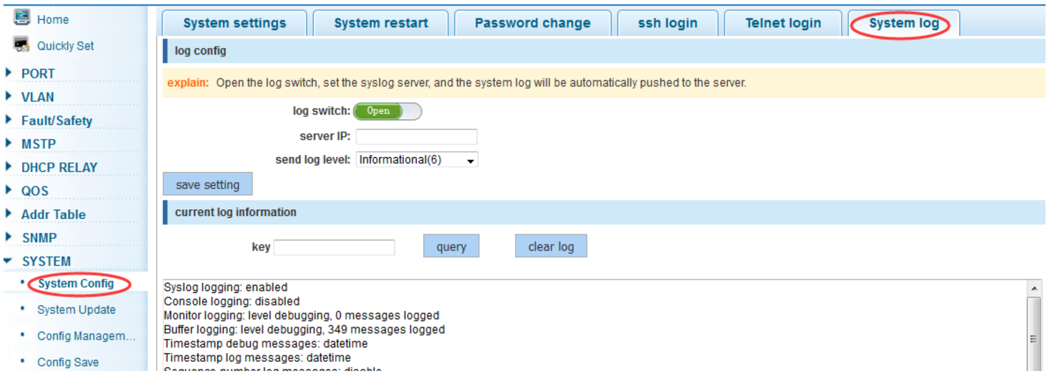


Telnet config

note: Configure the user to be able to switch through the Telnet login device.

4.10.1.6 System log

In the navigation bar to select**“SYSTEM>system config>system log”**,to view the log and set up the log server. the following picture:



log config

explain: Open the log switch, set the syslog server, and the system log will be automatically pushed to the server.

log switch: Open

server IP:

send log level: Informational(6)

current log information

key

```
Syslog logging: enabled
Console logging: disabled
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 349 messages logged
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence number log messages: disable
```

【parameter description】

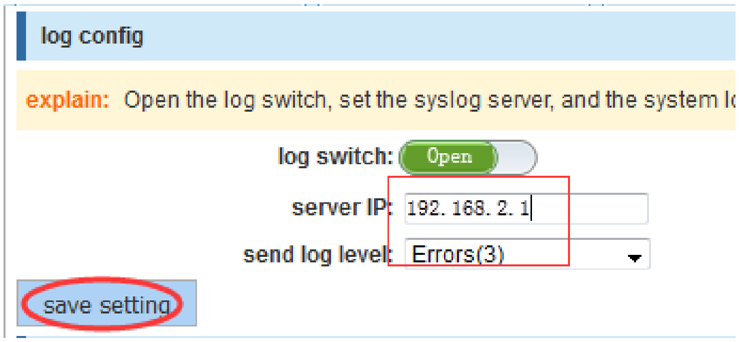
parameter	description
Log switch	Open and close
Server ip	Appoint to server address
Send log level	0-7
key	Enter the required query of characters

【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 192.168.2.1 pushed to the server



log config

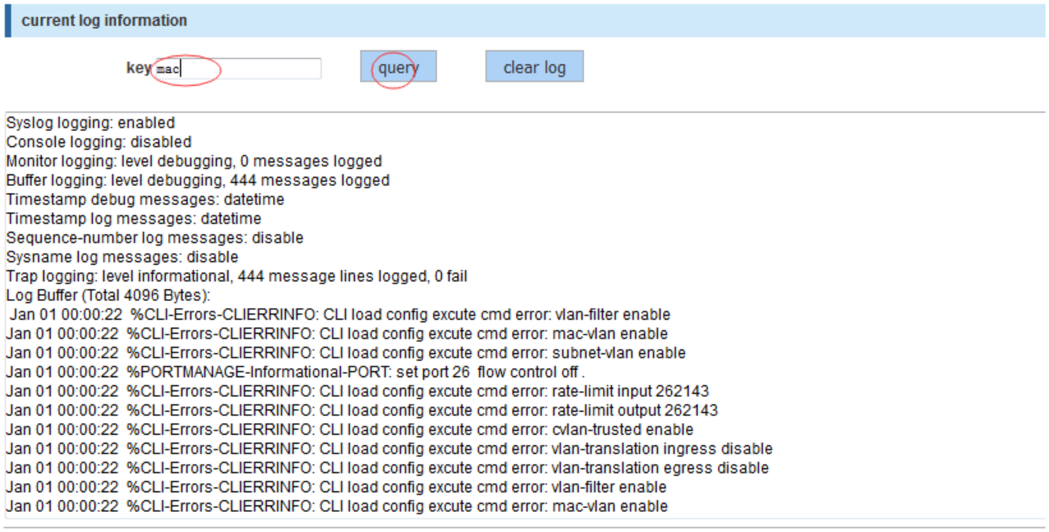
explain: Open the log switch, set the syslog server, and the system l

log switch: Open

server IP: 192. 168. 2. 1

send log level: Errors(3)

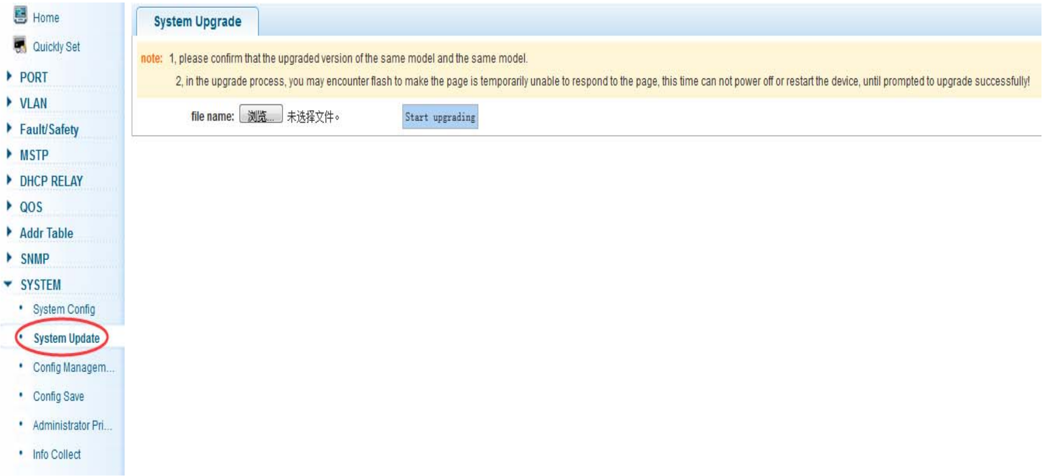
2) input the Mac keywords ,click “query”button, click on the "clear log" button, can clear the log



```
Syslog logging: enabled
Console logging: disabled
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 444 messages logged
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: disable
Sysname log messages: disable
Trap logging: level informational, 444 message lines logged, 0 fail
Log Buffer (Total 4096 Bytes):
 Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-filter enable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: mac-vlan enable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: subnet-vlan enable
Jan 01 00:00:22  %PORTMANAGE-Informational-PORT: set port 26  flow control off .
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: rate-limit input 262143
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: rate-limit output 262143
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: cvlan-trusted enable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-translation ingress disable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-translation egress disable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: vlan-filter enable
Jan 01 00:00:22  %CLI-Errors-CLIERRINFO: CLI load config excute cmd error: mac-vlan enable
```

4.10.2 System upgrade

In the navigation bar to select**“SYSTEM>system upgrade”**,Optional upgrade file to upgrade. the following picture



note: 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!

file name: 未选择文件。

【instruction】

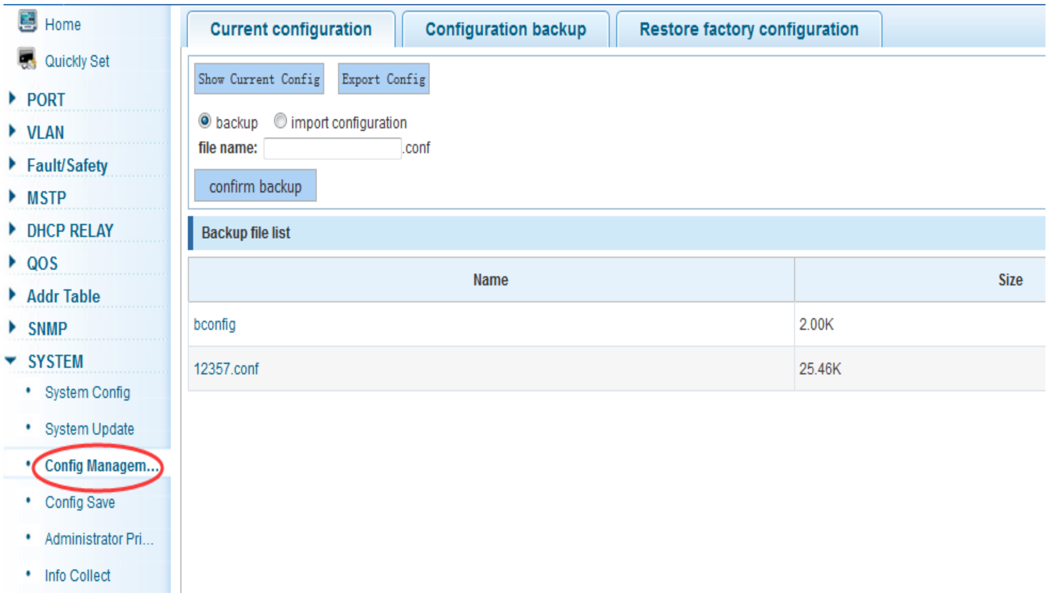
1　please confirm that the upgraded version of the same model and the same model.

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!

4.10.3 Config management

4.10.3.1 Current configuration

In the navigation bar to select**“SYSTEM>config management>current configuration”**,can import and export configuration files, the backup file. the following picture:



● backup ○ import configuration

file name: .conf

Backup file list

Name	Size
bconfig	2.00K
12357.conf	25.46K

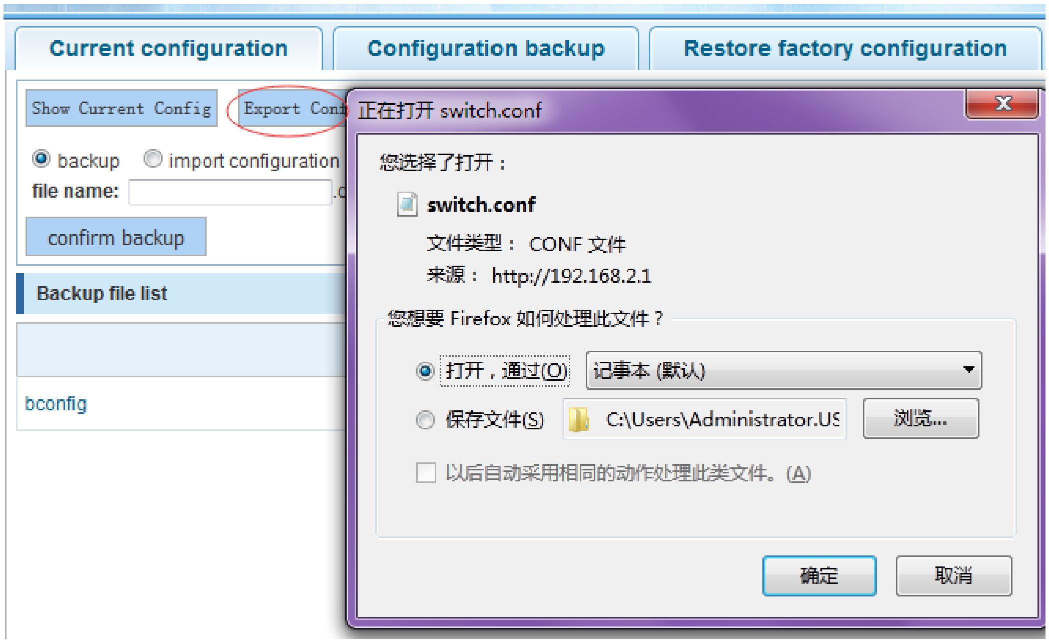
【instruction】

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



● backup ○ import configuration

file name:

正在打开 switch.conf

您选择了打开：

switch.conf

文件类型： CONF 文件

来源： http://192.168.2.1

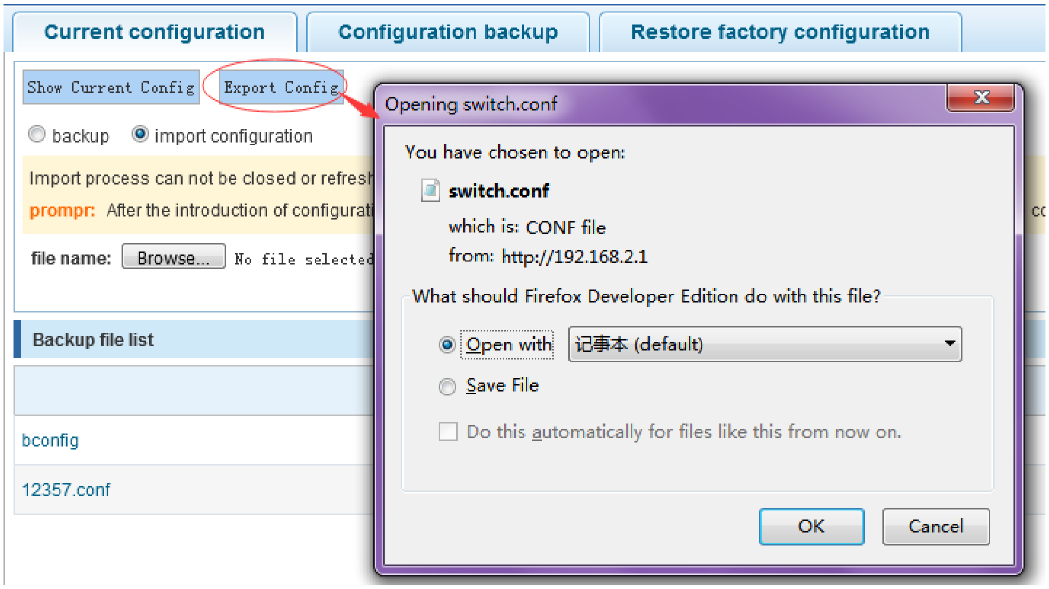
您想要 Firefox 如何处理此文件？

● 打开，通过(O) 记事本 (默认)

○ 保存文件(S) C:\Users\Administrator.US

□ 以后自动采用相同的动作处理此类文件。(A)

2) import configuration



○ backup ● import configuration

Import process can not be closed or refresh

prompr: After the introduction of configurati

file name: No file selected

Opening switch.conf

You have chosen to open:

switch.conf

which is: CONF file

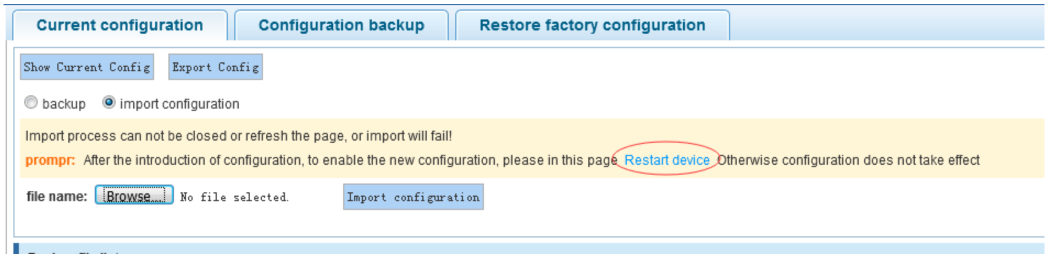
from: http://192.168.2.1

What should Firefox Developer Edition do with this file?

● Open with 记事本 (default)

○ Save File

□ Do this automatically for files like this from now on.



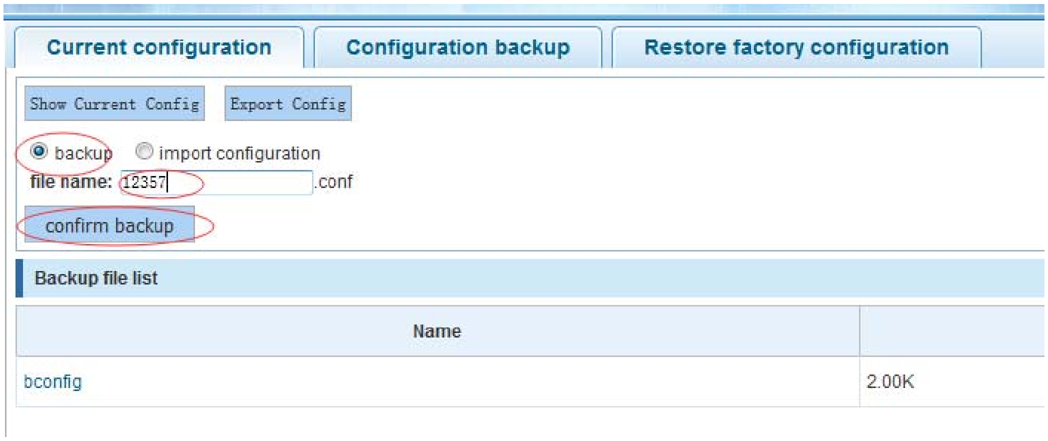
○ backup ● import configuration

Import process can not be closed or refresh the page, or import will fail!

prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect

file name: No file selected.

3）backup



● backup ○ import configuration

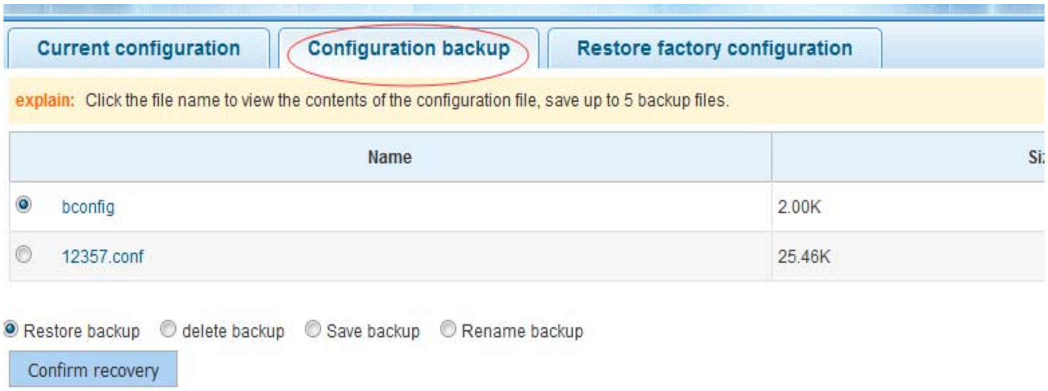
file name: 12357 .conf

Backup file list

Name	
bconfig	2.00K

4.10.3.2 Configuration backup

In the navigation bar to select**“SYSTEM>config management>configuration backup”**,you can configure backup file。the following picture:



explain: Click the file name to view the contents of the configuration file, save up to 5 backup files.

	Name	Si
●	bconfig	2.00K
○	12357.conf	25.46K

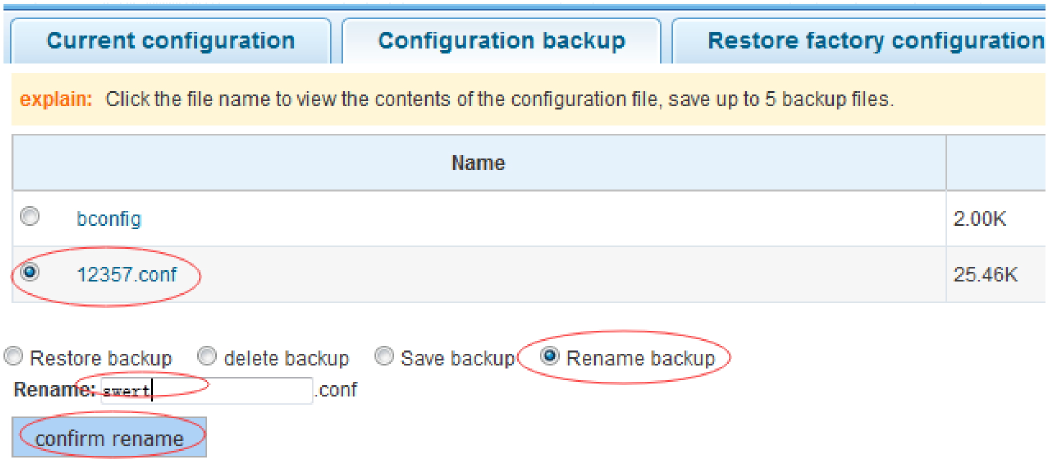
● Restore backup ○ delete backup ○ Save backup ○ Rename backup

【instruction】

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

【Configuration example】

Such as：restore backup



explain: Click the file name to view the contents of the configuration file, save up to 5 backup files.

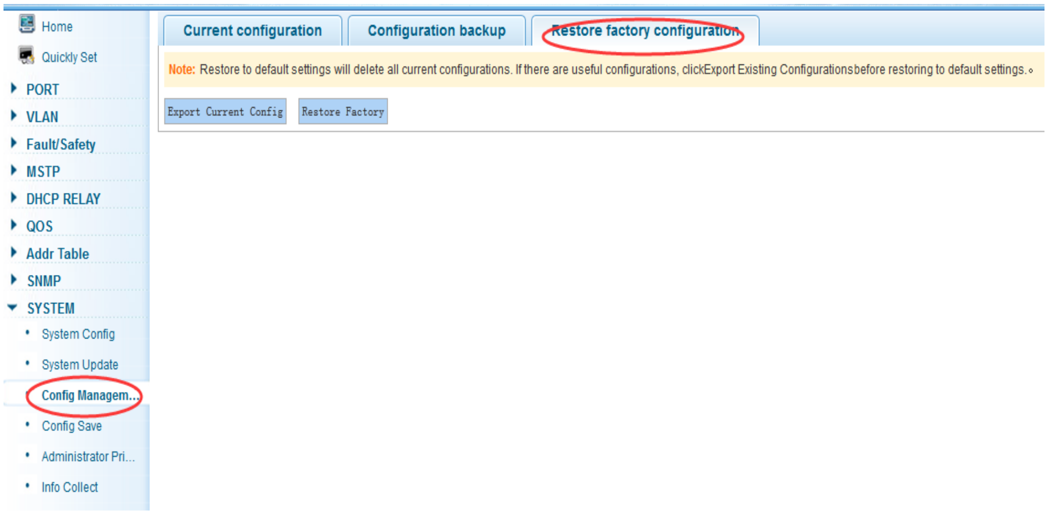
Name	
○ bconfig	2.00K
● 12357.conf	25.46K

○ Restore backup ○ delete backup ○ Save backup ● Rename backup

Rename: swert .conf

4.10.3.3 Restore factory configuration

In the navigation bar to select**“SYSTEM>config management>restore factory configuraton”**,Can export the current configuration and restore factory configuration .the following picture:



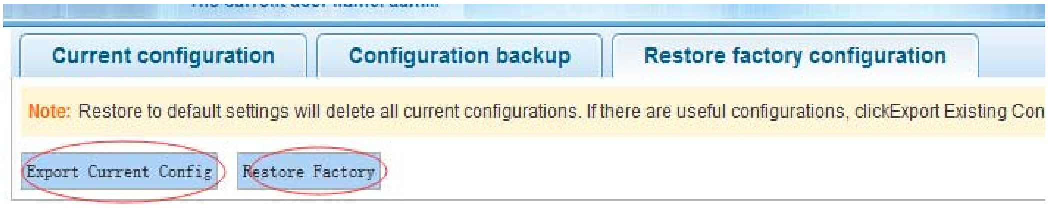
Note: Restore to default settings will delete all current configurations. If there are useful configurations, clickExport Existing Configurationsbefore restoring to default settings.。

【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】

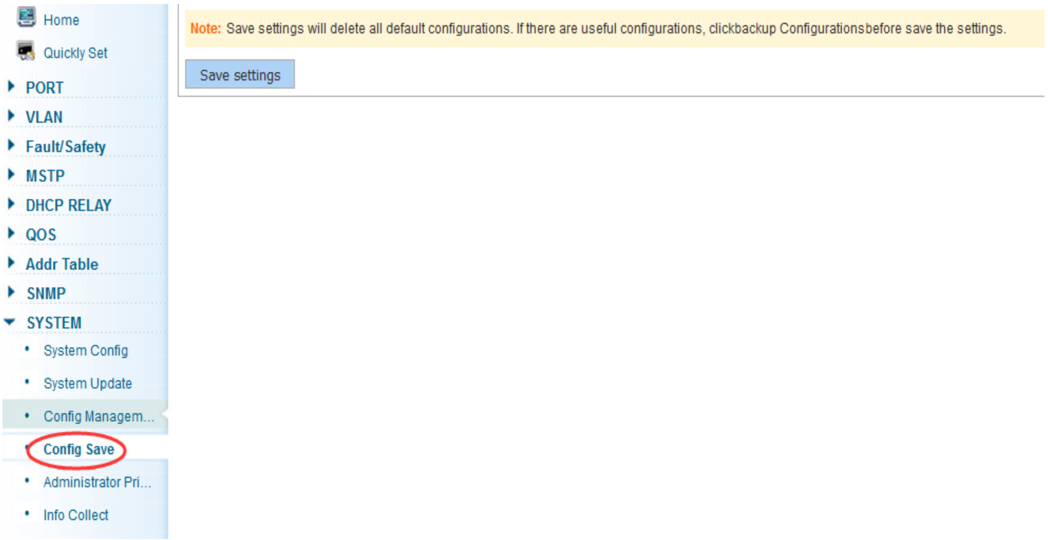
Such as: restore configuration can be the guide before they leave the current configuration



Note: Restore to default settings will delete all current configurations. If there are useful configurations, clickExport Existing Con

4.10.4 Config save

In the navigation bar to select“**SYSTEM >config save”**,you can save current configuration。the following picture



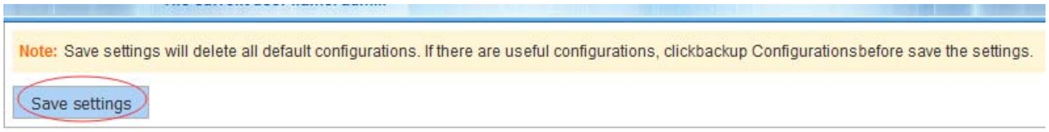
Note: Save settings will delete all default configurations. If there are useful configurations, clickbackup Configurationsbefore save the settings.

【instruction】

Save settings will delete all default configurations. If there are useful configurations, clickbackup Configurationsbefore save the settings.

【Configuration example】

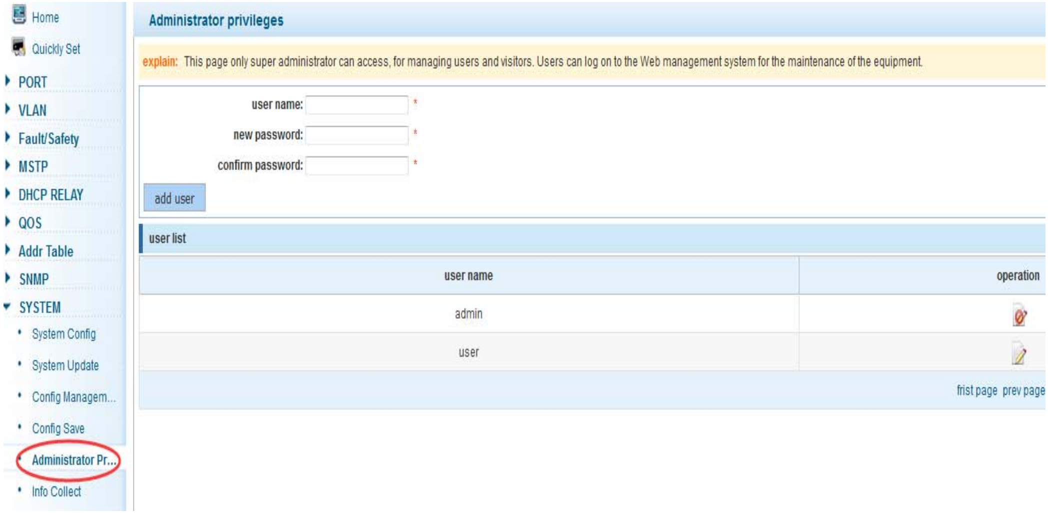
Such as：click“save settings”button



Note: Save settings will delete all default configurations. If there are useful configurations, clickbackup Configurationsbefore save the settings.

4.10.5 Administrator privileges

In the navigation bar to select**“SYSTEM>administrator privileges”**,Configurable ordinary users. the following picture



Administrator privileges

explain: This page only super administrator can access, for managing users and visitors. Users can log on to the Web management system for the maintenance of the equipment.

user name: *

new password: *

confirm password: *

user list

user name	operation
admin	
user	

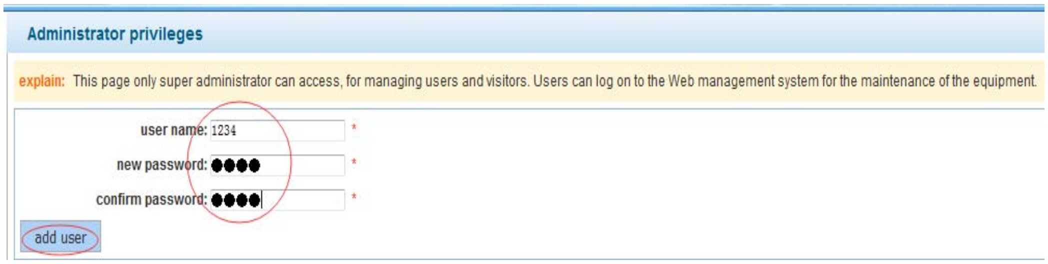
frist page prev page

【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:



Administrator privileges

explain: This page only super administrator can access, for managing users and visitors. Users can log on to the Web management system for the maintenance of the equipment.

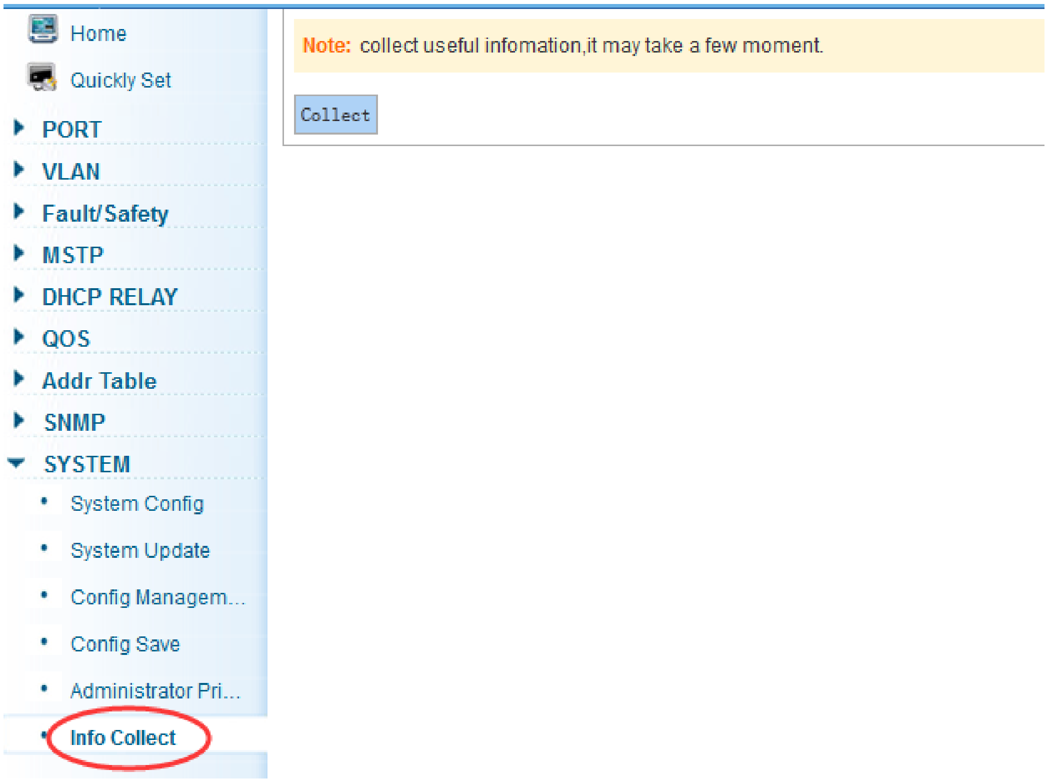
user name: 1234 *

new password: ●●●● *

confirm password: ●●●● *

4.10.6 Info collect

In the navigation bar to select**“SYSTEM>info collect”**,you can collect to the system debug information。the following picture



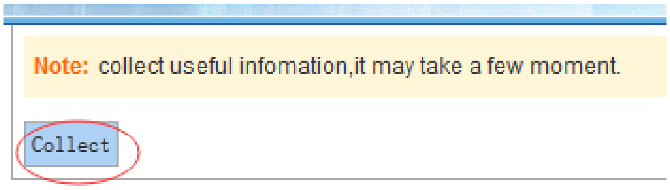
Note: collect useful infomation,it may take a few moment.

【instruction】

collect useful infomation,it may take a few moment.

【Configuration example】

Such as: click on "collect" button



Note: collect useful infomation,it may take a few moment.

Appendix: Technical Specifications

Hardware Features	
Standards	IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.3ad
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)
Number of Ports	24 x 10/100/1000Mbps Auto-Negotiation ports 2 x SFP ports 1 x Console port
Transfer Method	Store-and-Forward
Switching Capacity	52G
MAC Address Learning	Automatically learning, automatically update 8K Table
Frame Filtering and Forward Rate	10Mbps: 14880pps 100Mbps: 148800pps 1000Mbps: 1488000pps
Dimensions (L × W × H)	440*208*44 mm
Environment	Operating Temperature: 0□~40□ Storage Temperature: -10□~70□ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~90% non-condensing
Power Supply	AC 100V~240V 50/60Hz (Internal Power supply)

MORRELL®
A TRUSTED GERMAN NAME

www.morrelltelecom.com
sales@morrelltelecom.com
morrelltelecom