MORRELL®
A TRUSTED GERMAN NAME

SW-MNG-24GE4/10GSFP

24-Port 10/100/1000Mbps + 4-Port 10Gbps SFP Managed Ethernet Switch

User Manual

Ver 1.0 |6/15/2016

Table of Contents

Chapter 1 Product Introduction

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

1.1 Product Overshow

This is a new generation designed for high security and high performance network the second layer switch. Provides twenty-four 10/100/1000Mbps self-adaption RJ45 port, plus four 10 Gigabit --1000/10000Mbps SFP+ optical port, it can be used to link bandwidth higher upstream equipment. Using store-and-forward technology, combined with dynamic memory allocation. Ensure bandwidth effective allocation to each port. Special design is a flow control.It can avoid packet loss effectively when nodes in the sending and receiving data. Built-in high reliability, design for wide voltage input application power supply, even if the voltage is not stable of power grid, also can guarantee the equipment can work normally.

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

1.2 Features

- Supports IEEE 802.3, IEEE 802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3az.
- Integrated High-Performance Cortex-A9 processor.
- Supports MAC address auto-learning and auto-aging.
- Twenty-four 10/100/1000Mbps self-adaption RJ45 port, plus four 10 gigabit port --- 10/100/1000/10000Mbps SFP+ optical port, it can be used to link bandwidth higher upstream equipment.
- Store and forward mode operates.
- LED indicators for monitoring power, link/activity.
- Support QoS, port mirroring, link aggregation protocol.
- 19 inches full metal iron shell and internal power adapter design, suitable for rack installation.

1.3 Package Contents

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

- One 24-Port 10/100/1000Mbps + 4-Port 10 Gigabit Web Smart Ethernet Switch
- One set of installation components
- One AC power cord
- One User Manual

Chapter 2 External Component Description

2.1 Front Panel

The front panel of the Switch consists of series of LED indicators, 24 x 10/100/1000Mbps RJ-45 ports, 4 x 1000/10000Mbps SFP+ ports, 1 Console port, A reset button, A series of LED lights:

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 Link LED.

SFP+ ports (25S, 26S, 27S, 28S):
Designed to install the SFP+ module and connect to the device with a bandwidth of 1000Mbps or 10000Mbps. Each has a corresponding Link/Act（1000M and 10G）LED.

Control port (Console):
It is used to connect a computer or terminal serial implementation of monitoring and configuring the switch.

Reset key (Reset):
Keep the device is turned on and press the button for about 4 seconds.The system restore 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.

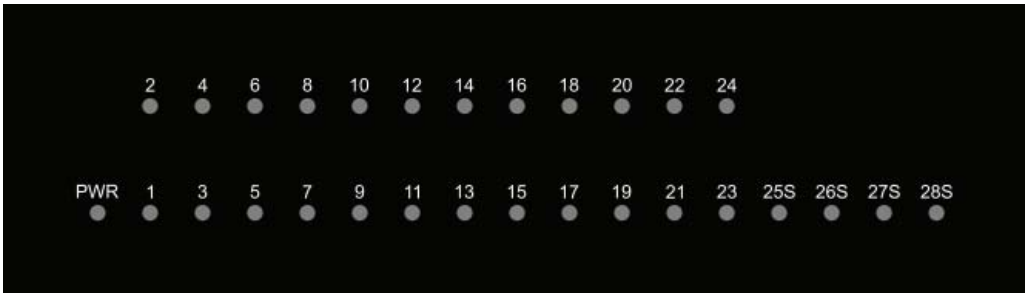


Figure 2 - LED Indicators

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

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off
1~28LED	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

2.2 Rear Panel

The rear panel of the Switch contains AC power connector 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:
Located on the left side of the power supply connector, use wire grounded to prevent electric shock.

Chapter 3 Installing and Connecting the Switch

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

3.1 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.

3.1.1 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.

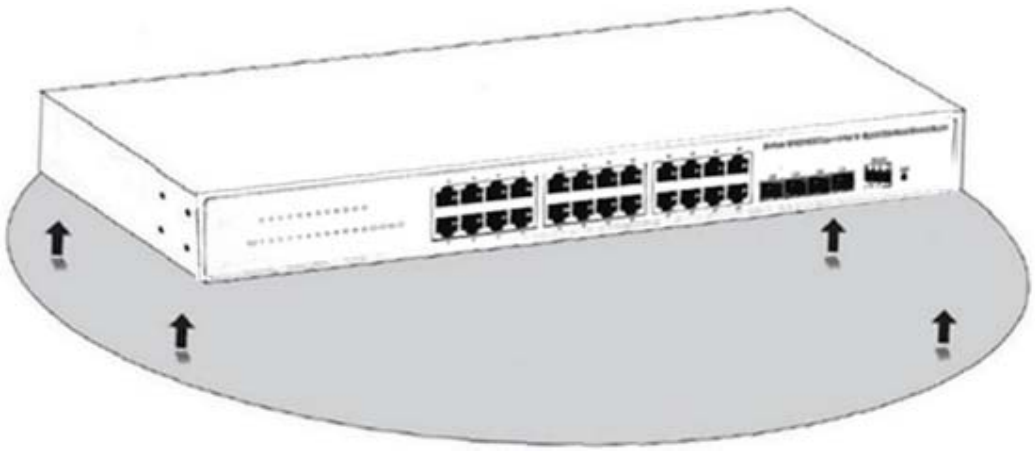


Figure 4 - Desktop installation

3.1.2 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.

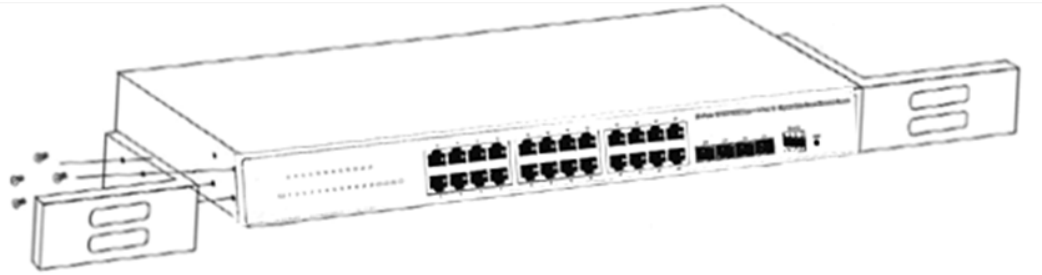


Figure 5 - Attaching Brackets

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

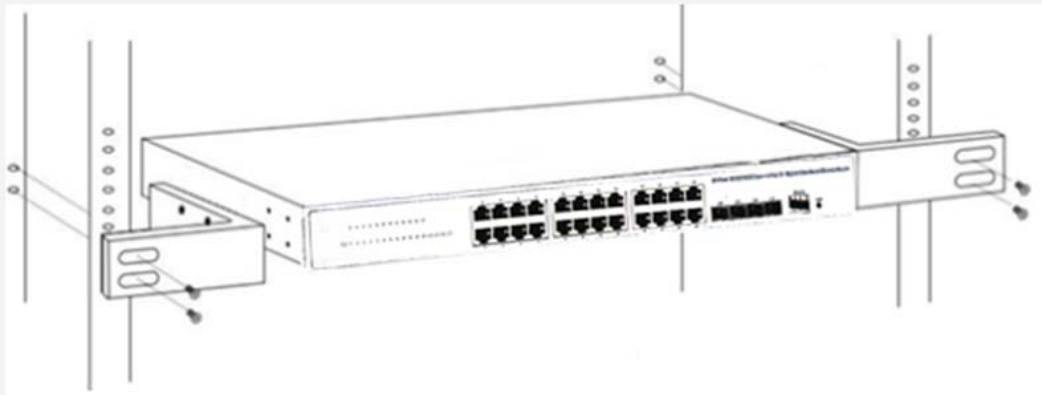


Figure 6 - Mounting Switch

3.1.3 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.

3.2 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 status indicator lights corresponding ports of the Switch.

Figure 7 - Connect Computer (NIC) to the Switch

3.3 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 user name	admin
Default password	admin

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

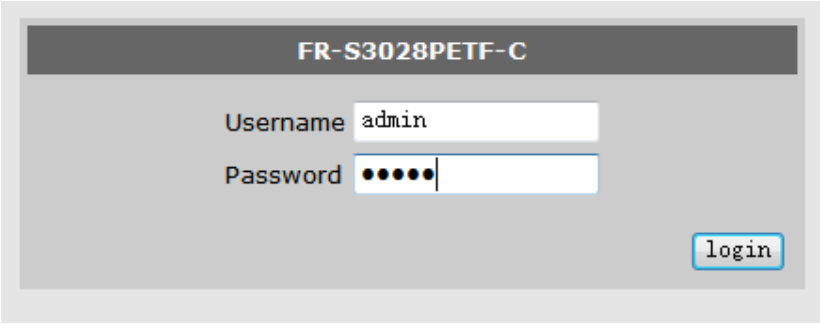
a. Connect the Switch with the computer NIC interface.

b. Power on the Switch.

c. 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.

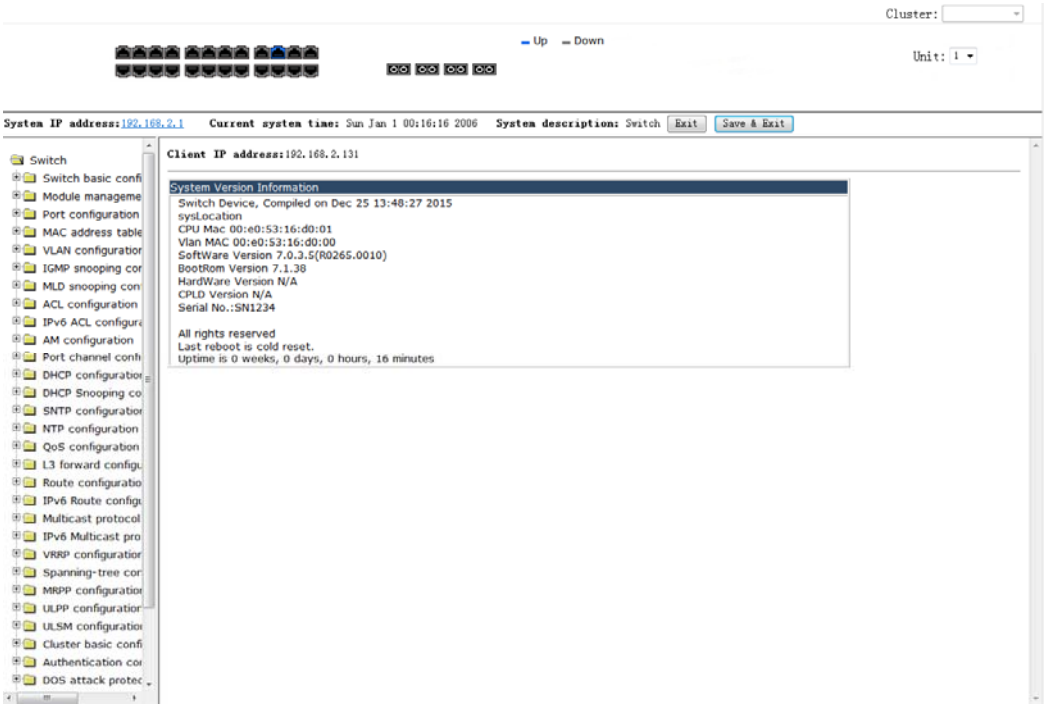
d. Open the browser, and enter ***http://192.168.2.1*** and then press "Enter". The Switch login window appears, as shown below.

e.



f. Enter the ID and Password (The default ID is **admin**.Password is **admin**), and then

click **"OK"** to log in to the Switch configuration window as below.



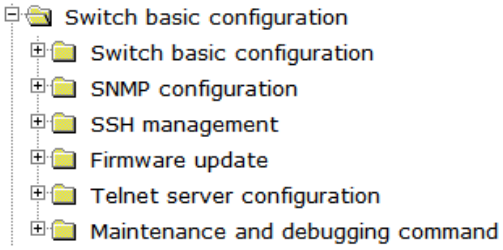
In the Web GUI, the left column shows the configuration menu and the rest of the screen area displays the configuration settings.

Chapter 4 Switch Configuration

Switch configuration interface consists of 3 main areas, areas for the status bar at the top, the area on the left menu bar, right the main configuration window. Blue in the status bar indicates the RJ45 port connected, black corresponds to the RJ45 port means port is not connected. Select the different functions in the function menu bar, you can modify all settings in the main configuration window.

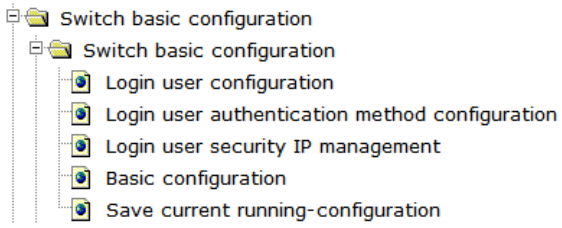
4.1 Switch basic configuration.

Choose **Switch basic configuration,** and the following page appears.
There are"Switch basic configuration", "SNMP configuration", "SSH management", "Firmware update", "Telnet server configuration", "Maintenance and debugging command", configuration web pages.



4.1.1 Switch basic configuration.

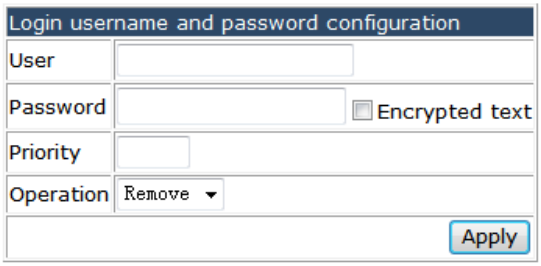
Choose **Switch basic configuration > Switch basic configuration,** and the following page appears.There are "Login user configuration", "Login user authentication method configuration", "Login user security IP management", "Basic configuration", "Save current running-configuration", configuration web pages.



4.1.1.1 Login user configuration.

Choose **Switch basic configuration > Switch basic configuration > Login user configuration,** and the following page appears.Enter the user name and password, and choose whether to encrypt the text, and sets the user priority, then you want to add or remove users.

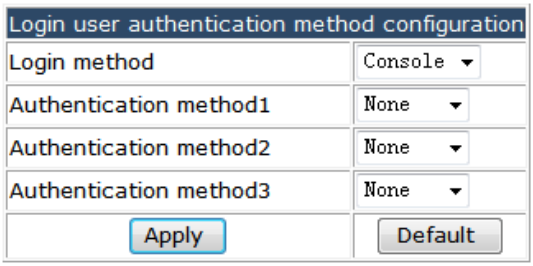
Notes: User names and passwords between 1-32 characters. Priority between 1-15, defaults to 1.



User			
User name	Password	State	Priority
admin	admin	Plain text	15

4.1.1.2 Login user authentication method configuration.

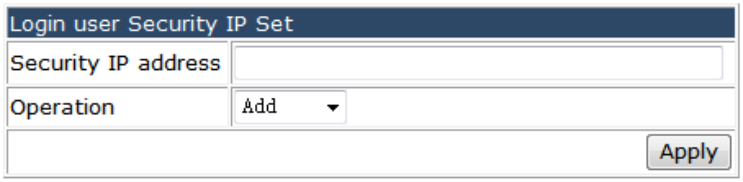
Choose **Switch basic configuration > Switch basic configuration > Login user authentication method configuration,** and the following page appears. Set the login and authentication methods, or to restore the default.
Login methods including Console, Vty, WEB, authentication methods. Authentication method including Local, RADIUS, Tacacs.

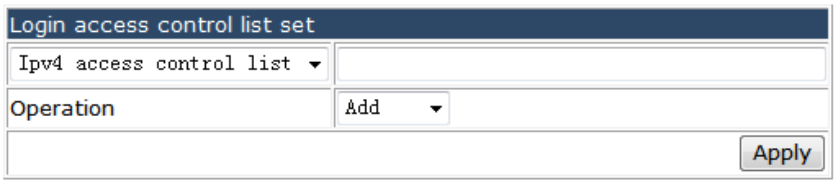


Login user authentication method				
Login method	Authentication method1	Authentication method2	Authentication method3	
console	None	None	None	None
vty	local	None	None	None
web	local	None	None	None

4.1.1.3 Login user security IP management.

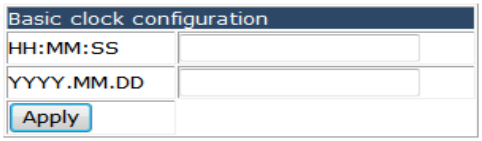
Choose **Switch basic configuration > Switch basic configuration > Login user security IP management,** and the following page appears. Here you can add or delete an user's login security IP. In the user access control list settings, add or remove the Ipv4/Ipv6 Security address.

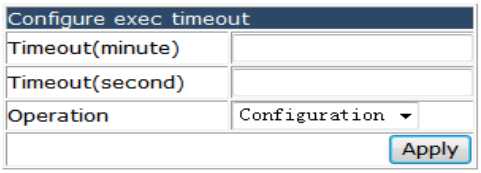


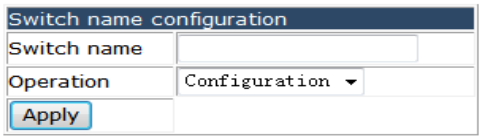


4.1.1.4 Basic configuration.

Choose **Switch basic configuration > Switch basic configuration > Basic configuration,** and the following page appears.You can change the time, the switch name, configure the exec timeout.

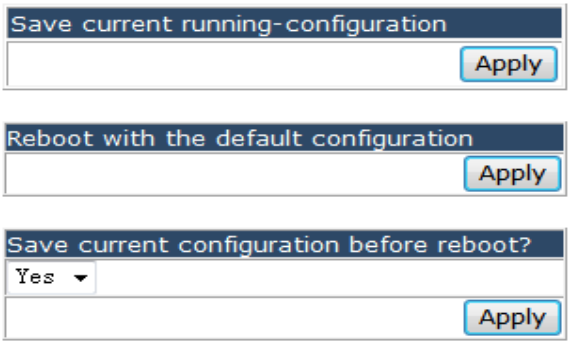






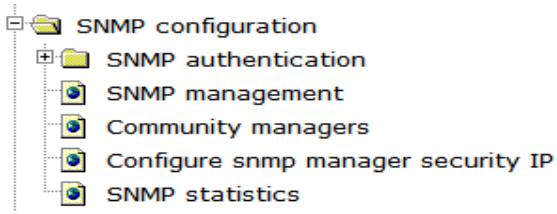
4.1.1.5 Save current running-configuration.

Choose **Switch basic configuration > Switch basic configuration > Save current running-configuration,** and the following page appears.These three function provide to save current running-configuration, reboot with restore configuration to default, and reboot with save current configuration or not.



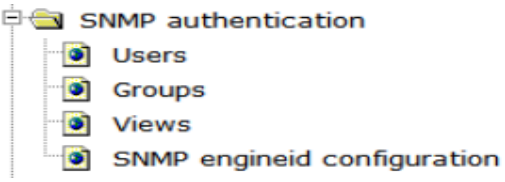
4.1.2 SNMP configuration.

Choose **Switch basic configuration > SNMP configuration,** and the following page appears.Changing SNMP authentication parameters must start SNMP function first, go to “SNMP Management” page to change item “SNMP Agent state ” to open.There are "SNMP authentication", "SNMP management", "Community managers", "Configure snmp manager security IP", "SNMP statistics", configuration web pages.



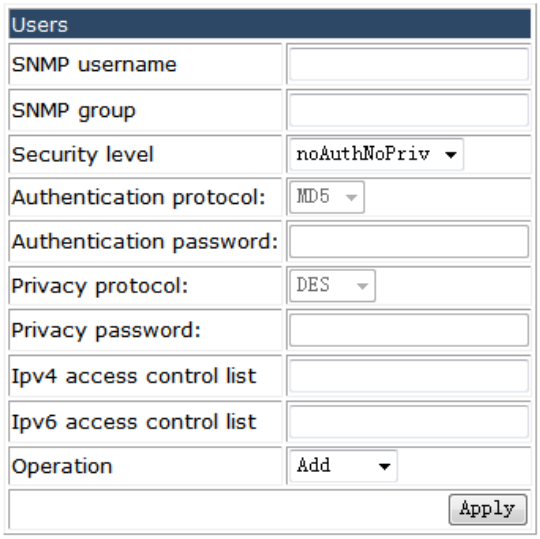
4.1.2.1 SNMP authentication.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication,** and the following page appears.There are "Users", "Groups", "show”,”SNMP engineid configuration", configuration web pages.



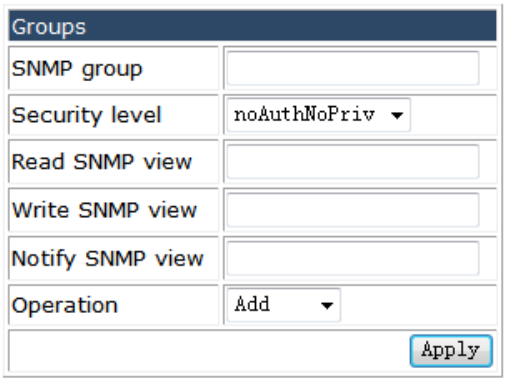
4.1.2.1.1 Users.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > Users,** and the following page appears.Here you can set the SNMP user name, SNMP group, and the security level, the IPv4 and IPv6 access control lists. Security level including ,no certification and no encryption, authentication without encryption, authentication with encryption.
Note: the Authentication password and Privacy password in 8-32 characters.
Note: the SNMP User name and SNMP Group in 1-32 characters.



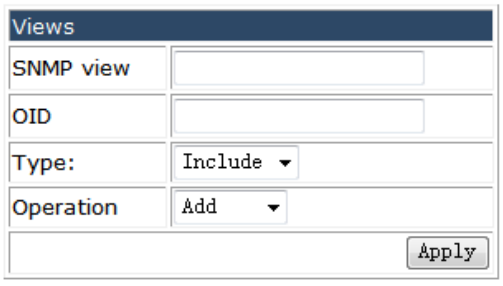
4.1.2.1.2 Groups.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > Groups,** and the following page appears.Set the security level, read SNMP shows, write SNMP shows, notifies the SNMP show operation.



4.1.2.1.3 shows.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > shows,** and the following page appears.His page allow to add or remove a SNMP policy. Fill the show item and OID to include or exclude the corresponding MIB.

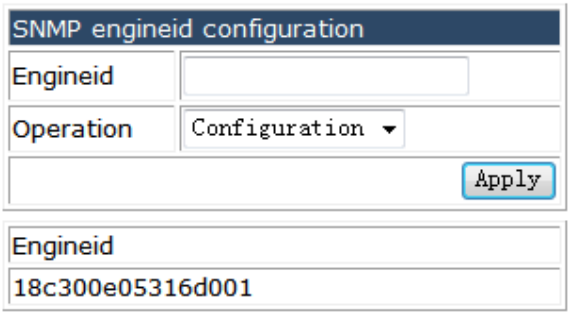


SNMP view	OID	Type
v1defaultviewname	1.0.	Include
v1defaultviewname	1.2.	Include
v1defaultviewname	1.3.	Include

4.1.2.1.4 SNMP engineid configuration.

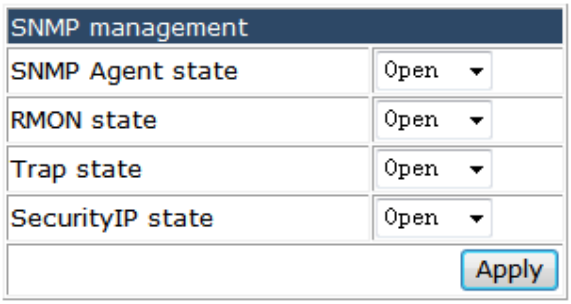
Choose **Switch basic configuration > SNMP configuration > SNMP authentication >**

SNMP engineid configuration, and the following page appears.If not necessary, don't change the default engineid value.



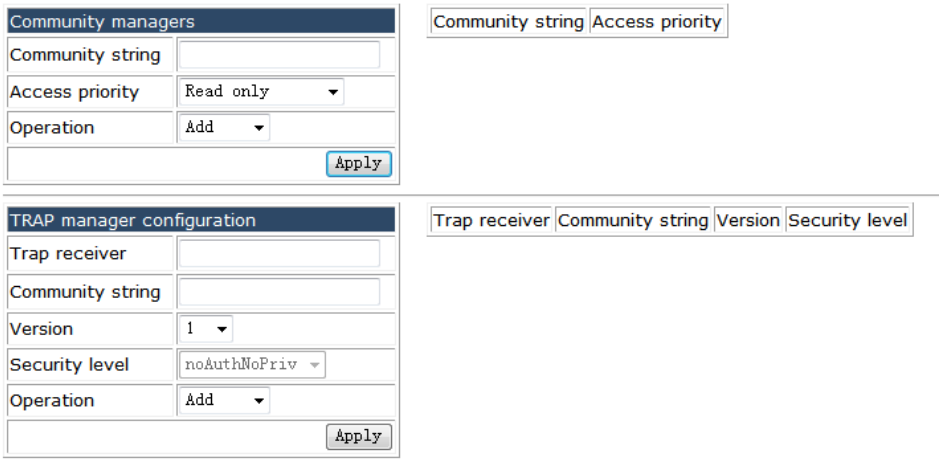
4.1.2.2 SNMP management.

Choose **Switch basic configuration > SNMP configuration > SNMP management,** and the following page appears.You can open or close SNMP, RMON, Trap, Security IP state function.



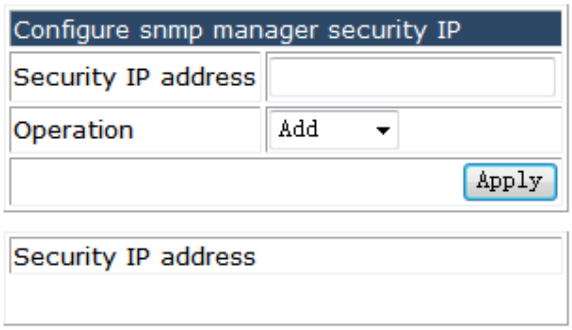
4.1.2.3 Community managers.

Choose **Switch basic configuration > SNMP configuration > Community managers,** and the following page appears. At this page, you can configure the community string for different priority, and set the Trap receiver address,community string,version,security level for trap message.



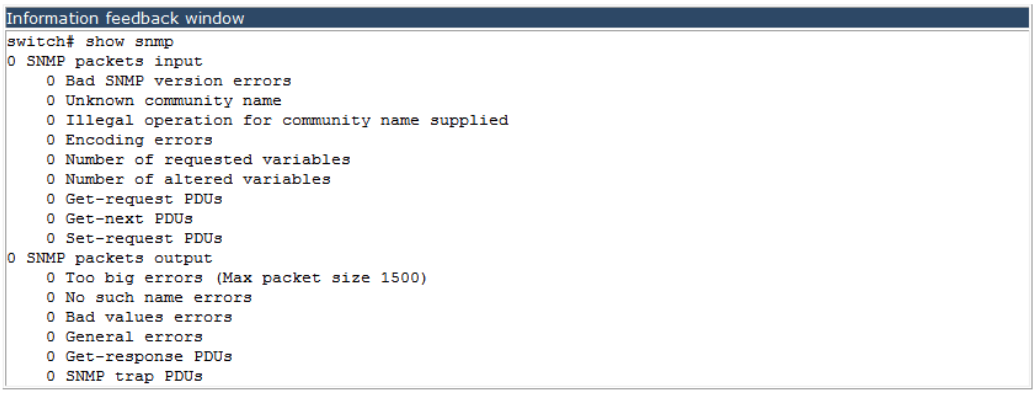
4.1.2.4 Configure snmp manager security IP.

Choose **Switch basic configuration > SNMP configuration > Configure snmp manager security IP,** and the following page appears. You can add or remove Security IP address for SNMP management.



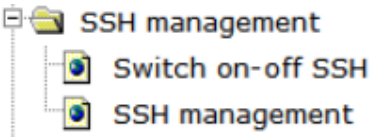
4.1.2.5 SNMP statistics.

Choose **Switch basic configuration > SNMP configuration > SNMP statistics,** and the following page appears. From this window ,you can read the detail statistics message for SNMP.



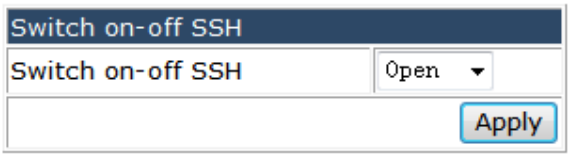
4.1.3 SSH management.

Choose **Switch basic configuration > SSH management,** and the following page appears. There are"Switch on-off SSH", "SSH management", configuration web pages.



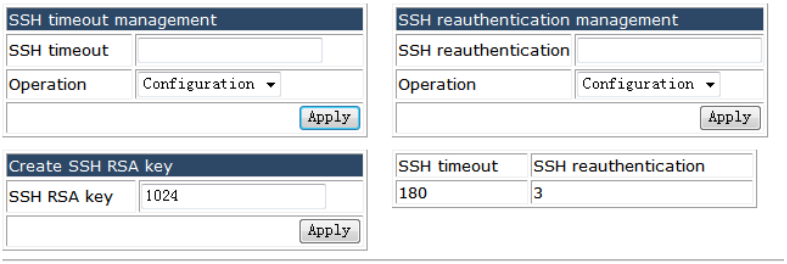
4.1.3.1 Switch on-off SSH.

Choose **Switch basic configuration > SSH management > Switch on-off SHH,** and the following page appears. Choose open or close to turn on-off SSH function.



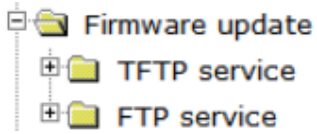
4.1.3.2 SSH management.

Choose **Switch basic configuration > SSH management > SSH management,** and the following page appears. You can set the SSH timeout, SSH re-certification number and create a SHH RSA keys.



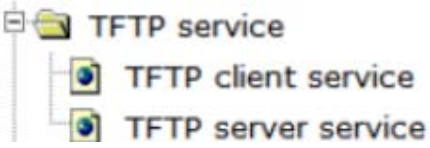
4.1.4 Firmware update.

Choose **Switch basic configuration > Firmware update,** and the following page appears.There are"TFTP service", "FTP service", configuration web pages.



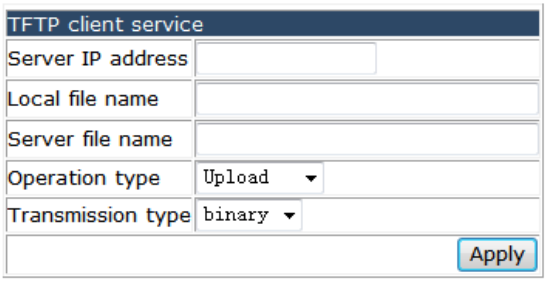
4.1.4.1 TFTP service.

Choose **Switch basic configuration > Firmware update > TFTP service,** and the following page appears.There are"TFTP client service", "TFTP server service", configuration web pages.



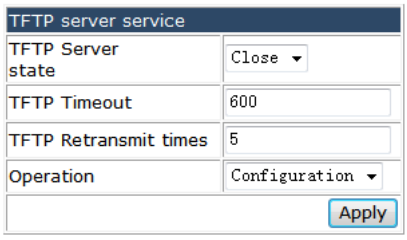
4.1.4.1.1 TFTP client service.

Choose **Switch basic configuration > Firmware update > TFTP service > TFTP client service,** and the following page appears.You can set the TFTP client service.



4.1.4.1.2 TFTP server service.

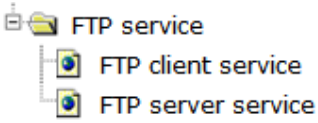
Choose **Switch basic configuration > Firmware update > TFTP service > TFTP server service,** and the following page appears.You can open or close the TFTP server function, set timeout and retransmit times value, or reset these parameters to factory default.



TFTP Server state	TFTP Timeout	TFTP Retransmit times
Close	600	5

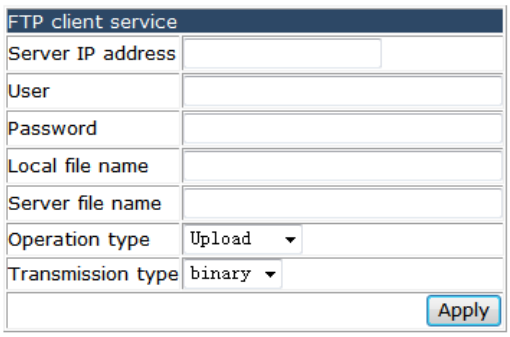
4.1.4.2 FTP service.

Choose **Switch basic configuration > Firmware update > FTP service,** and the following page appears.There are “FTP client service", "FTP server service", configuration web pages.



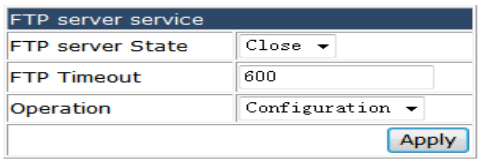
4.1.4.2.1 FTP client service.

Choose **Switch basic configuration > Firmware update > FTP service > FTP client service,** and the following page appears.Fill the IP address, User name, Password of the FTP server, setting the local file name and server file name, then you can upload or download the file to the FTP server. Also you can select the transmit type using binary or ASCII.

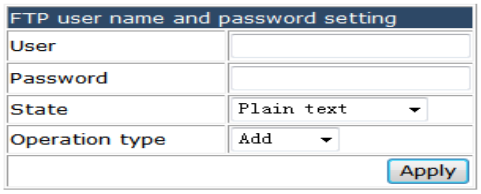


4.1.4.2.2 FTP server service.

Choose **Switch basic configuration > Firmware update > FTP service > FTP server service,** and the following page appears.You can choose open or close the FTP server function. Also you can set timeout value, user name,password, and plain text or encrypted text display the password for the FTP server.



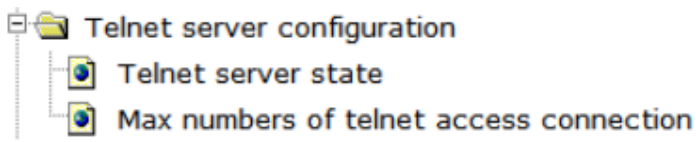
FTP server State	FTP Timeout
Close	600



User name	Password	State

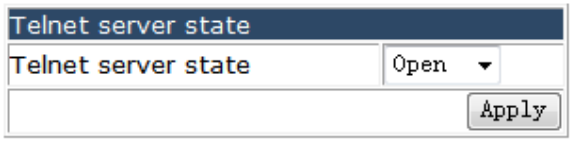
4.1.5 Telnet server configuration.

Choose **Switch basic configuration > Telnet server configuration,** and the following page appears.There are"Telnet server state", "Max numbers of telnet access connection", configuration web pages.



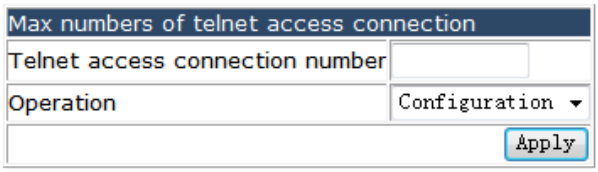
4.1.5.1 Telnet server state.

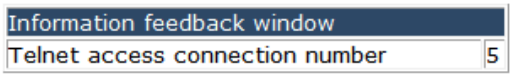
Choose **Switch basic configuration > Telnet server configuration > Telnet server state,** and the following page appears.You can open or close the Telnet Server.



4.1.5.2 Max number of telnet access connection.

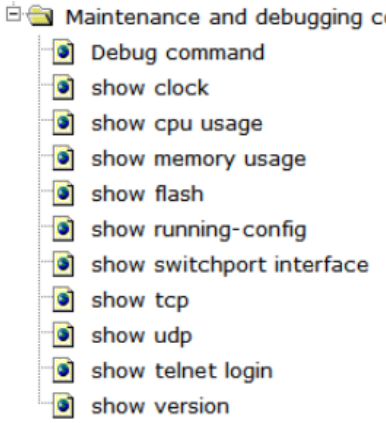
Choose **Switch basic configuration > Telnet server configuration > Max number of telnet access connection,** and the following page appears.Set Max number of Telnet access.The default number is 5.





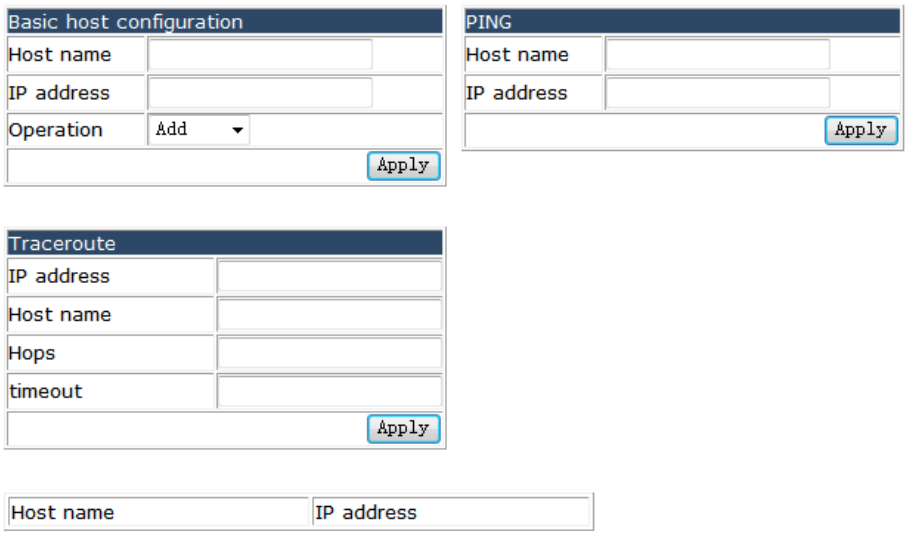
4.1.6 Maintenance and debugging command.

Choose **Switch basic configuration > Maintenance and debugging command,** and the following page appears.There are"Debug command", "show clock", "show cpu usage", "show memory usage", "show flash", "show running-config", "show switchport interface", "show tcp", "show udp", "show telnet login", "show version", configuration web pages.



4.1.6.1 Debug command.

Choose **Switch basic configuration > Maintenance and debugging command > Debug command,** and the following page appears.You can add or remove the Host name and IP address to the list. And you can test the connectivity between switch and the destination host via ping or traceroute method..



4.1.6.2 Show clock.

Choose **Switch basic configuration > Maintenance and debugging command > show clock,** and the following page appears.You can see the current time information of the device.

4.1.6.3 Show cpu usage.

Choose **Switch basic configuration > Maintenance and debugging command > show cpu usage,** and the following page appears.You can see the CPU usage information of the device.

4.1.6.4 Show cpu show memory usage.

Choose **Switch basic configuration > Maintenance and debugging command > show Memory usage,** and the following page appears.You can see the memory usage information of the device.

```
Information feedback window
switch# show memory usage
The memory total 512 MB , free 437805056 bytes , usage is 18.45%
```

4.1.6.5 Show flash.

Choose **Switch basic configuration > Maintenance and debugging command > show flash,** and the following page appears.You can see the all the files store in the flash, and the flash usage of the device.

```
Information feedback window
switch# show flash
-rw-        1.7K            backupstartup.cfg
-rw-        4               board_web_language
-rw-        13.1M           nos.img
-rw-        1.0K            startup.cfg
Drive : flash:
Size:14.0M  Used:13.9M  Avaliable:64.0K  Use:100%
```

4.1.6.6 Show running-config.

Choose **Switch basic configuration > Maintenance and debugging command > show running-config,** and the following page appears.You can see the running-configure information of the device.

```
Information feedback window
switch# show run
!
no service password-encryption
!
hostname switch
sysLocation FullRiver Industrial Area Economic Development Zone LiLing City HuNan Province China
sysContact 0731-2325 0117
!
authentication logging enable
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
```

4.1.6.7 Show switchport interface.

Choose **Switch basic configuration > Maintenance and debugging command > show switchport interface,** and the following page appears.You can see all the ports and their type and mode information of device.

Information feedback window

```
switch# show switchport interface
Ethernet1/0/1
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/2
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/3
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/4
```

4.1.6.8 Show tcp.

Choose **Switch basic configuration > Maintenance and debugging command > show tcp,** and the following page appears.You can see the current TCP connection information of the device.

Information feedback window

```
switch# show tcp
LocalAddress     LocalPort  ForeignAddress   ForeignPort     State       IF  VRF
192.168.2.1      80         192.168.2.22     49342           ESTABLISHED0   0
127.0.0.1        2650       127.0.0.1        32862           ESTABLISHED0   0
127.0.0.1        32862      127.0.0.1        2650            ESTABLISHED0   0
0.0.0.0          6633       0.0.0.0          0               LISTEN      0   0
0.0.0.0          80         0.0.0.0          0               LISTEN      0   0
0.0.0.0          22         0.0.0.0          0               LISTEN      0   0
0.0.0.0          23         0.0.0.0          0               LISTEN      0   0
127.0.0.1        2650       0.0.0.0          0               LISTEN      0   0
```

4.1.6.9 Show udp.

Choose **Switch basic configuration > Maintenance and debugging command > show udp,** and the following page appears.You can see the current UDP transmission information of the device.

Information feedback window

```
switch# show udp
LocalAddress     LocalPort  ForeignAddress   ForeignPort     State
0.0.0.0          161        0.0.0.0          0               CLOSE
0.0.0.0          3071       0.0.0.0          0               CLOSE
```

4.1.6.10 Show telnet login.

Choose **Switch basic configuration > Maintenance and debugging command > show telnet login,** and the following page appears.You can see the current client host logined via telnet.

Information feedback window

```
switch# show telnet login
Authenticate login by local.
Login user:
```

4.1.6.11 Show version.

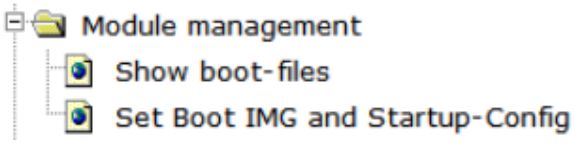
Choose **Switch basic configuration > Maintenance and debugging command > show version,** and the following page appears.You can see the detail version information of the device.

System Version Information

```
FR-S3028TF-C Device, Compiled on Feb 01 16:58:10 2016
sysLocation FullRiver Industrial Area Economic Development Zone LiLing City HuNan Province China
CPU Mac 00:e0:53:16:d0:01
Vlan MAC 00:e0:53:16:d0:00
SoftWare Version 7.0.3.5(R0265.0012)
BootRom Version 7.1.38
HardWare Version N/A
CPLD Version N/A
Serial No.:SN1234
Copyright (C) 2008-2016 by Liling FullRiver Electronic & Technology Limited
All rights reserved
Last reboot is warm reset.
Uptime is 0 weeks, 0 days, 6 hours, 26 minutes
```

4.2 Module management.

Choose **Module management**, and the following page appears.There are"Show boot-files", "Set Boot IMG and Startup-Config", configuration web pages.



4.2.1 Show boot-files.

Choose **Module management > Show boot-files,** and the following page appears.You can see the current boot file and configure file, also the next boot time files.

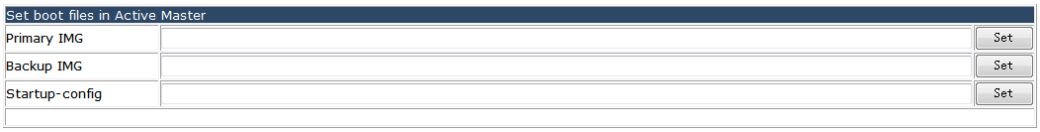
Information feedback window

```
Booted files on switch
The primary img file at the next boot time:       flash:/nos.img
The backup img file at the next boot time:        flash:/nos.img
Current booted img file:                          flash:/nos.img

The startup-config file at the next boot time:    NULL
Current booted startup-config file:               NULL
```

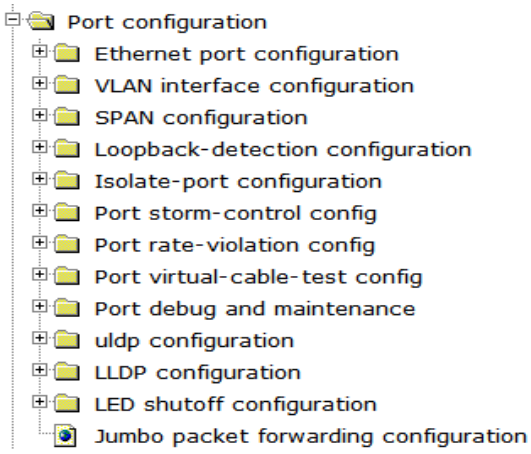
4.2.2 Set Boot IMG and Startup-Config.

Choose **Module management > Set Boot IMG and Startup-Config,** and the following page appears.You can specify the boot files and startup-config file for next boot time.



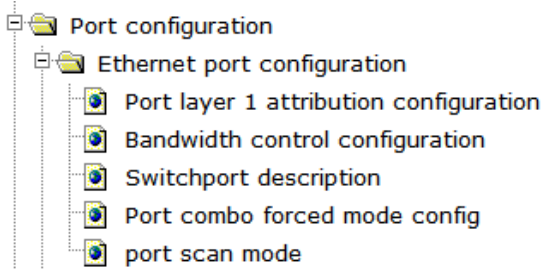
4.3 Port configuration.

Choose **Port configuration,** and the following page appears.There are"Ethernet port configuration", "VLAN interface configuration", "SPAN configuration", "Loopback-detection configuration", "Isolate-port configuration", "Port storm-control config", "Port rate-violation config", "Port virtual-cable-test config", "Port debug and maintenance", "uldp configuration", "LLDP configuration", "LED shutoff configuration", "Jumbo packet forwarding configuration", configuration web pages.



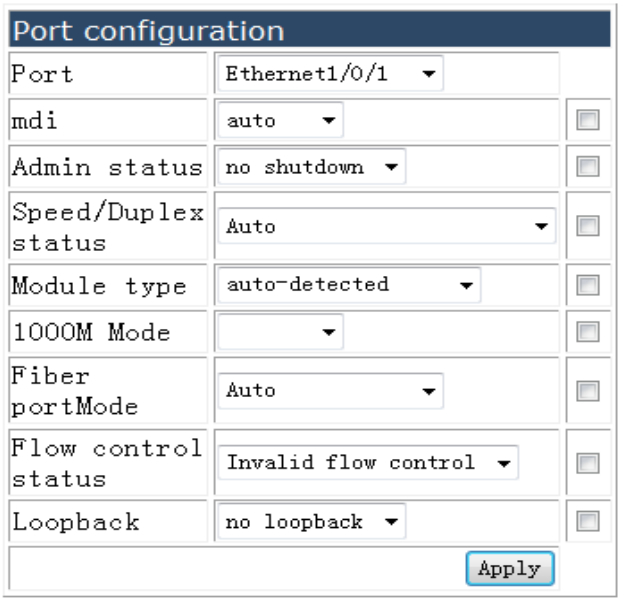
4.3.1 Ethernet port configuration.

Choose **Port configuration > Ethernet port configuration,** and the following page appears.There are "Port layer 1 attribution configuration", "Bandwidth control configuration", "Switchport description", "Port combo forced mode config", "Port scan mode", configuration web pages.



4.3.1.1 Port layer 1 attribution configuration.

Choose **Port configuration > Ethernet port configuration > Port layer 1 attribution configuration,** and the following page appears.You can set the parameters for every port, and the Port List table display the configuration information for each port.



Port-Specify the port to be configured.
mdi-Set the interface type for the port, auto means support automatic flip, across means support cross wire, normal means support straight-through line.
Admin status-Shutdown or no shutdown the port.
Speed/Duplex status-Set the speed and duplex mode including 10M/Half、 10M/Full、 100M/Half、 100M/Full、 1000M/Half、 1000M/Full and so on.
Module type-Set the 100M light module type supported by the switch including auto-detected, no-phy-integrated, phy-integrated,this parameter just for SFP+ optical port.
Fiber port Mode-Include auto and non negotiation mode.
Flow control status-Set valid or invalid flow control.
Loopback-Whether to configure loop detection function.

Port list

Port	mdi	managementStatus	Speed	Mode	1000M Mode	Fiber portMode	Flow control	loopback
Ethernet1/0/1	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/2	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/3	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/4	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/5	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/6	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/7	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/8	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/9	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/10	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback

4.3.1.2 Bandwidth control configuration.

Choose **Port configuration > Ethernet port configuration > Bandwidth control configuration,** and the following page appears.You can limit the bandwidth rang 1-10000000Kb for each port divided for transmit and receive direction.

Bandwidth control configuration

Port	Bandwidth control level	Control type	Operation
Ethernet1/0/1		Transmit	Configuration

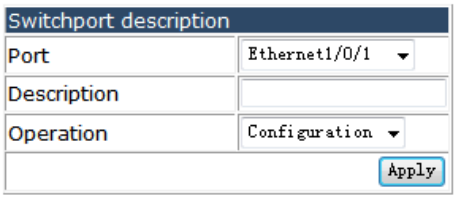
Apply

Port list

Port	Ingress bandwidth threshold(Kb)	Engress bandwidth threshold(Kb)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000

4.3.1.3 Switchport description.

Choose **Port configuration > Ethernet port configuration > Switchport description,** and the following page appears.You can set the description of the switch port.

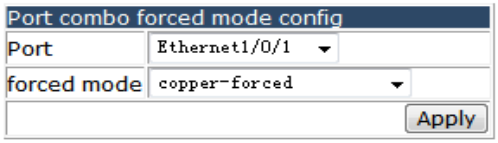


Port list

Port	Description
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	
Ethernet1/0/10	
Ethernet1/0/11	
Ethernet1/0/12	
Ethernet1/0/13	

4.3.1.4 Port combo forced mode config.

Choose **Port configuration > Ethernet port configuration > Port combo forced mode config,** and the following page appears.You can set the combination models to copper-forced, copper-prefered-auto,SFP-forced or SFP-preferred-auto for each port.



Information feedback window

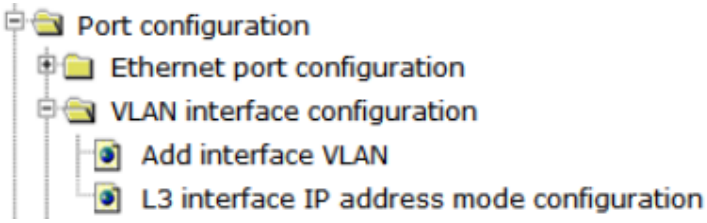
Port	forced mode
Ethernet1/0/1	no support
Ethernet1/0/2	no support
Ethernet1/0/3	no support
Ethernet1/0/4	no support
Ethernet1/0/5	no support
Ethernet1/0/6	no support
Ethernet1/0/7	no support
Ethernet1/0/8	no support
Ethernet1/0/9	no support
Ethernet1/0/10	no support
Ethernet1/0/11	no support

4.3.1.5 Port scan mode.

Choose **Port configuration > Ethernet port configuration > Port scan mode,** and the following page appears.You can change the port scan mode to Mode-interrupt or Mode-poll mode.

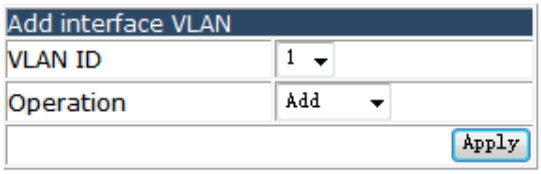
4.3.2 VLAN interface configuration.

Choose **Port configuration > VLAN interface configuration**, and the following page appears.There are "Add interface VALN", "L3 interface IP address mode configuration", configuration web pages.



4.3.2.1 Add interface configuration.

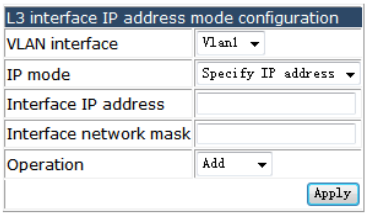
Choose **Port configuration > VLAN interface configuration > Add interface configuration,** and the following page appears.You can add or remove a VLAN interface.



Vlan ID	State
Vlan1	Layer 3 interface

4.3.2.2 L3 interface IP address mode configuration.

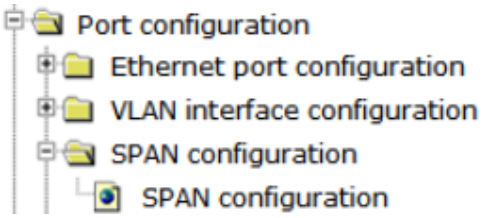
Choose **Port configuration > VLAN interface configuration > L3 interface IP address mode configuration,** and the following page appears.Here you can add or remove the L3 interface mode, set IP mode, the interface IP address, interface network mask.



VLAN interface	IP mode	Interface IP address	Interface network mask
Vlan1	Specify IP address	192.168.2.1	255.255.255.0

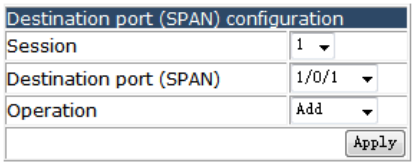
4.3.3 SPAN configuration.

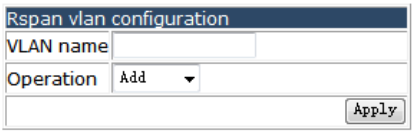
Choose **Port configuration > SPAN configuration,** and the following page appears.

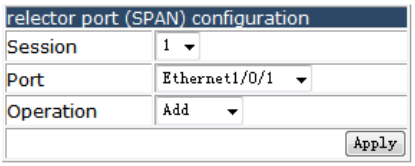


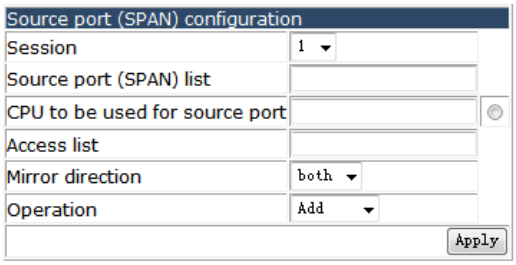
4.3.3.1 SPAN configuration.

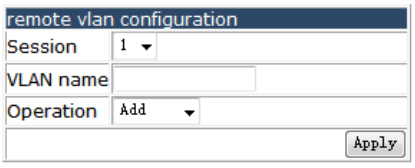
Choose **Port configuration > SPAN configuration > SPAN configuration,** and the following page appears.You can set the destination and source port parameters, also can set the Romote-SPAN configuration.

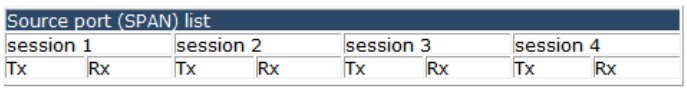






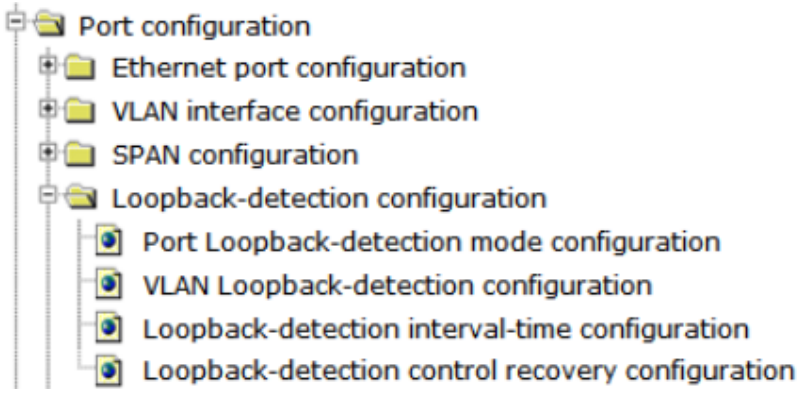






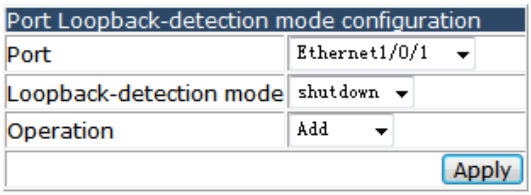
4.3.4 Loopback-detection configuration.

Choose **Port configuration > Loopback-detection configuration**, and the following page appears.There are "Port Loopback-detection mode configuration", "VLAN Loopback-detection configuration", "Loopback-detection interval-time configuration", "Loopback-detection control recovery configuration", configuration web pages.



4.3.4.1 Port Loopback-detection mode configuration.

Choose **Port configuration > Loopback-detection configuration > Port Loopback-detection mode configuration**, and the following page appears.You can change the Loopback-detection mode to shutdown or block for each port.

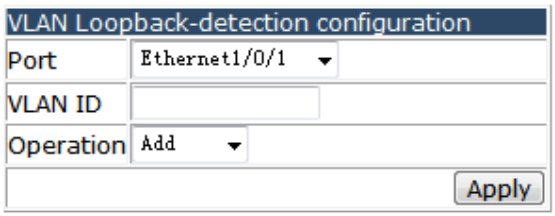


Information feedback window

Port	Loopback-detection mode
Ethernet1/0/1	no control mode
Ethernet1/0/2	no control mode
Ethernet1/0/3	no control mode
Ethernet1/0/4	no control mode
Ethernet1/0/5	no control mode
Ethernet1/0/6	no control mode
Ethernet1/0/7	no control mode
Ethernet1/0/8	no control mode
Ethernet1/0/9	no control mode
Ethernet1/0/10	no control mode
Ethernet1/0/11	no control mode
Ethernet1/0/12	no control mode
Ethernet1/0/13	no control mode
Ethernet1/0/14	no control mode

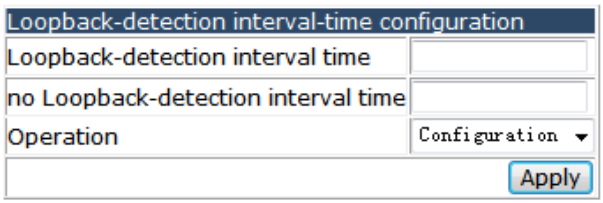
4.3.4.2 VLAN Loopback-detection configuration.

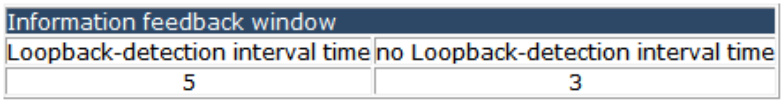
Choose **Port configuration > Loopback-detection configuration > VLAN Loopback-detection configuration,** and the following page appears.You can specify the VLAN that loop detection on or off.



4.3.4.3 Loopback-detection interval-time configuration.

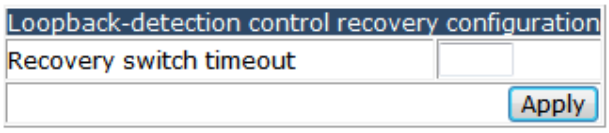
Choose **Port configuration > Loopback-detection configuration > Loopback-detection interval-time configuration,** and the following page appears.You can set no Loopback-detection interval time and Loopback-detection interval time.





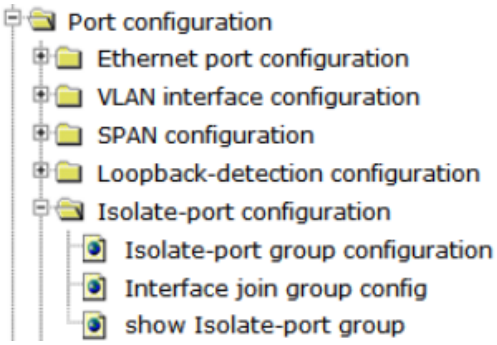
4.3.4.4 Loopback-detection control recovery configuration.

Choose **Port configuration > Loopback-detection configuration > Loopback-detection control recovery configuration,** and the following page appears.You can set the recovery detection interval to allow switch recovery the connection automatically after remove the loop cable.



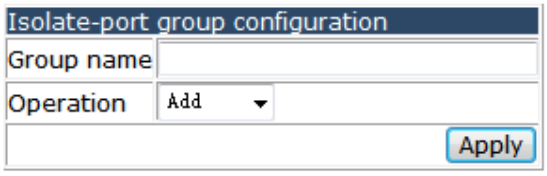
4.3.5 Isolate-port configuration.

Choose **Port configuration > Isolate-port configuration,** and the following page appears.
There are "Isolate-port configuration", "Interface join group config", "show Isolate-port group", configuration web pages.



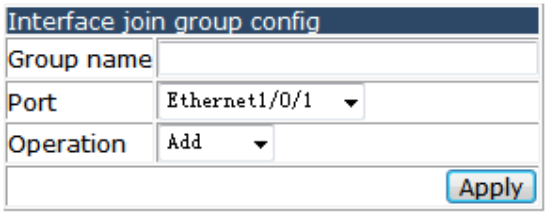
4.3.5.1 Isolate-port configuration.

Choose **Port configuration > Isolate-port configuration > Isolate-port configuration,** and the following page appears.You can add or remove an Isolate-port group.



4.3.5.2 Interface join group config.

Choose **Port configuration > Isolate-port configuration > Interface join group config,** and the following page appears.You can add or remove a port to an isolation group.

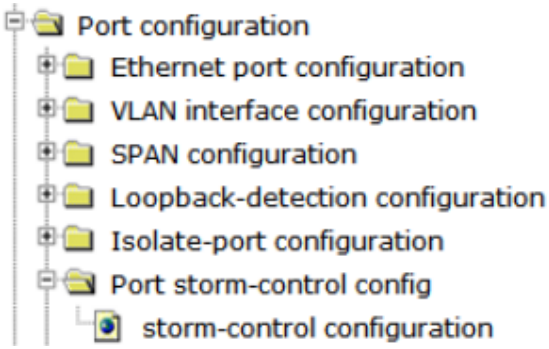


4.3.5.3 Show Isolate-port group.

Choose **Port configuration > Isolate-port configuration > show Isolate-port group,** and the following page appears.You can show the group number for each group.Space means show all groups.

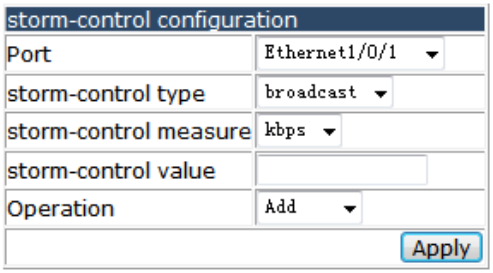
4.3.6 Port storm-control config

Choose **Port configuration > Port storm-control config,** and the following page appears.



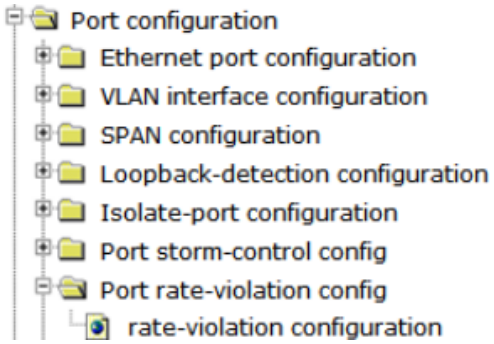
4.3.6.1 Storm-control config

Choose **Port configuration > Port storm-control config > Storm-control configuration,** and the following page appears.You can choose the port for the configure storm-control rule. The storm-control detect type include broadcast, multicast and unicast frame, and the measure unit could be kbps or pps, the threshold value rang is 1-1000000.



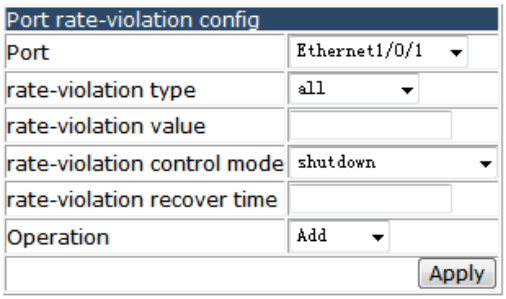
4.3.7 Port rate-violation config

Choose **Port configuration > Port rate-violation config,** and the following page appears.



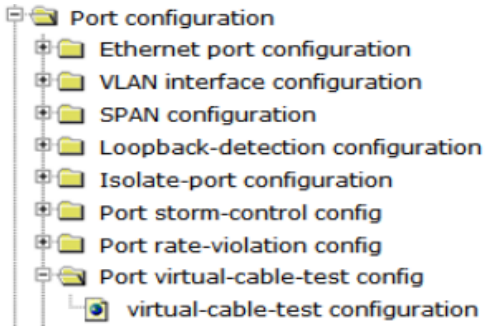
4.3.7.1 Port rate-violation config

Choose **Port configuration > Port rate-violation config > Rate-violation configuration,** and the following page appears.You can choose the port for the rate-violation rule, the detecting data type include all, broadcast, control, multicast and unicast, the rate-violation value rang is 200-2000000, the control mode include shutdown, shutdown recovery and block, and the recover time rang is 0-86400.



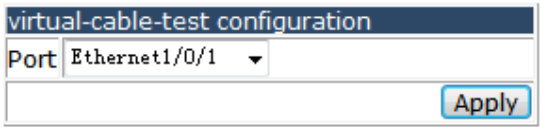
4.3.8 Port virtual-cable-test config.

Choose **Port configuration > Port virtual-cable-test config,** and the following page appears.



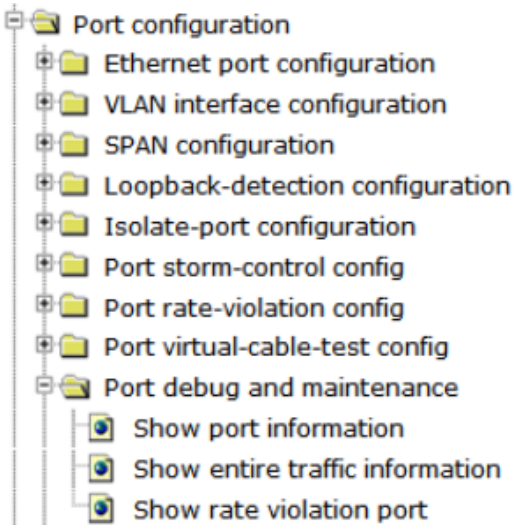
4.3.8.1 Virtual-cable-test configuration.

Choose **Port configuration > Port virtual-cable-test config > Virtual-cable-test configuration,** and the following page appears.You can check the connected status for each port.



4.3.9 Port debug and maintenance.

Choose **Port configuration > Port debug and maintenance,** and the following page appears.There are "Show port information", "Show entire traffic information", "Show rate violation port", configuration web pages.



4.3.9.1 Show port information.

Choose **Port configuration > Port debug and maintenance > Show port information,** and the following page appears.You can show the current detail information for each port.

Please select port: Ethernet1/0/1

Information feedback window

```
Interface brief:
  Ethernet1/0/1 is down, line protocol is down
  Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1
  Hardware is Gigabit-TX,  address is 00-e0-53-16-d0-01
  PVID is 1
  MTU 1500 bytes, BW 10000 Kbit
  Time since last status change: 0w- 0d- 3h- 26m- 58s   (12418 seconds)
  Encapsulation ARPA, Loopback  not set
  Auto-duplex ,  Auto-speed
  FlowControl is off,  MDI type is auto
Transceiver info:
Statistics:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
  Input packets statistics:
    0 input packets, 0 bytes, 0 no buffer
    0 unicast packets, 0 multicast packets, 0 broadcast packets
    0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
    0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments , 0 pause frame
  Output packets statistics:
    0 output packets, 0 bytes, 0 underruns
    0 unicast packets, 0 multicast packets, 0 broadcast packets
    0 output errors, 0 collisions, 0 late collisions , 0 pause frame
  Input and output packets by length:
(64)         bytes:          0, (65~127)    bytes:          0,
(128~255)    bytes:          0,  (256~511)   bytes:          0,
(512~1023)   bytes:          0, (1024~1518) bytes:          0
```

4.3.9.2 Show entire traffic information.

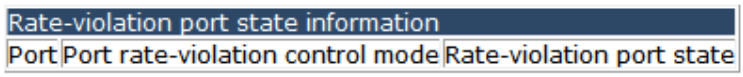
Choose **Port configuration > Port debug and maintenance > Show entire traffic information,** and the following page appears.You can show the statistics data for the receiving and transmission packets for all ports.

Show entire traffic information

Port	Receiving statistics						
	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)	Total packets	Error packets
Ethernet1/0/1	0	0	0	0	0	0	0
Ethernet1/0/2	0	0	0	0	0	0	0
Ethernet1/0/3	0	0	0	0	0	0	0
Ethernet1/0/4	0	0	0	0	0	0	0
Ethernet1/0/5	0	0	0	0	0	0	0
Ethernet1/0/6	0	0	0	0	0	0	0
Ethernet1/0/7	45438	0	0	3	0	57371	0
Ethernet1/0/8	0	0	0	0	0	0	0
Ethernet1/0/9	0	0	0	0	0	0	0
Ethernet1/0/10	0	0	0	0	0	0	0
Ethernet1/0/11	0	0	0	0	0	0	0
Ethernet1/0/12	0	0	0	0	0	0	0
Ethernet1/0/13	0	0	0	0	0	0	0
Ethernet1/0/14	0	0	0	0	0	0	0
Ethernet1/0/15	0	0	0	0	0	0	0
Ethernet1/0/16	0	0	0	0	0	0	0
Ethernet1/0/17	0	0	0	0	0	0	0
Ethernet1/0/18	0	0	0	0	0	0	0
Ethernet1/0/19	0	0	0	0	0	0	0
Ethernet1/0/20	0	0	0	0	0	0	0
Ethernet1/0/21	0	0	0	0	0	0	0

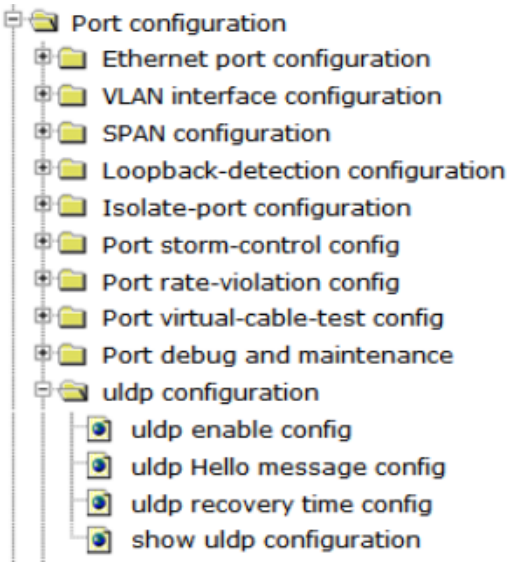
4.3.9.3 Show rate violation port.

Choose **Port configuration > Port debug and maintenance > Show rate violation port,** and the following page appears.Here you can show the port rate violation state information.



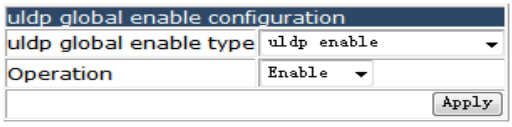
4.3.10 ULDP configuration.

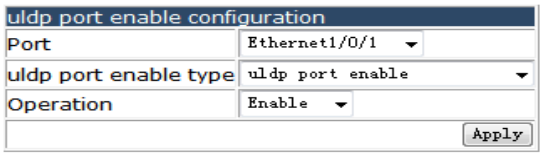
Choose **Port configuration > ULDP configuration,** and the following page appears.There are "ULDP enable config", "ULDP Hello message", "ULDP recovery time config", "Show ULDP configuration", configuration web pages.



4.3.10.1 ULDP enable config.

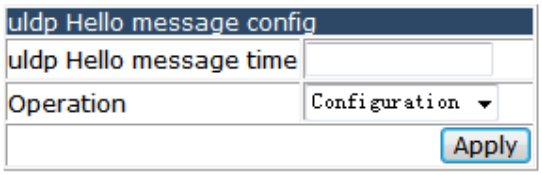
Choose **Port configuration > ULDP configuration > ULDP enable config,** and the following page appears.You can set the ULDP configuration for the global device or for every independent port. For global the type include ULDP enable, ULDP aggressive-mode, ULDP manual shutdown and ULDP reset all port. And for one port the type include ULDP port enable, ULDP port aggressive-mode, ULDP reset port.





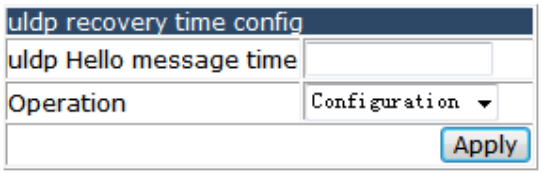
4.3.10.2 ULDP Hello message config.

Choose **Port configuration > ULDP configuration > ULDP Hello message config,** and the following page appears.You can set the Hello message interval.



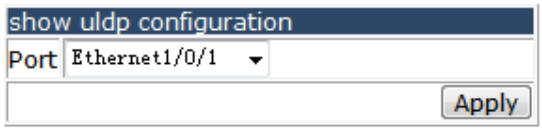
4.3.10.3 ULDP recovery time config.

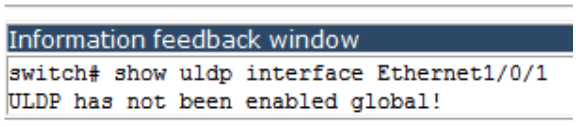
Choose **Port configuration > ULDP configuration > ULDP recovery time config,** and the following page appears.Here you can set the recovery interval.



4.3.10.3 Show ULDP configuration.

Choose **Port configuration > ULDP configuration > Show ULDP configuration,** and the following page appears.Here you can show each port configured ULDP.

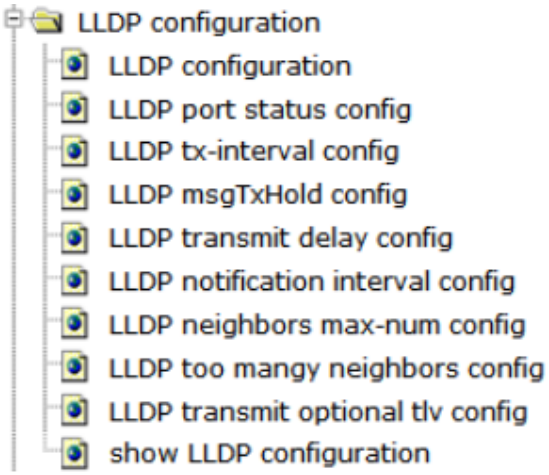




4.3.11 LLDP configuration.

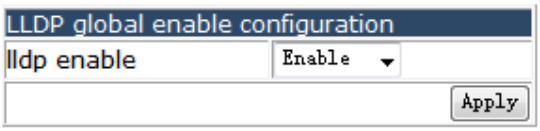
Choose **Port configuration > LLDP configuration,** and the following page appears.There are "LLDP configuration", "LLDP port status config", "LLDP tx-interval config", "LLDP msgTxHold config", "LLDP transmit delay config", "LLDP notification

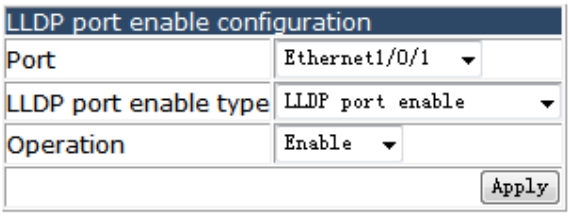
interval config", "LLDP neighbors max-num config", "LLDP too mangy neighbors config", "LLDP transmit optional tlv config", "show LLDP configuration", configuration web pages.



4.3.11.1 LLDP configuration.

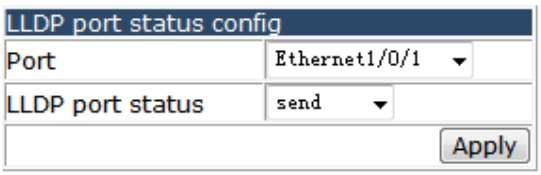
Choose **Port configuration > LLDP configuration > LLDP configuration,** and the following page appears.You can enable the LLDP configuration for the global device or for every independent port. For one port the enable type include LLDP port enable and LLDP port trap enable.





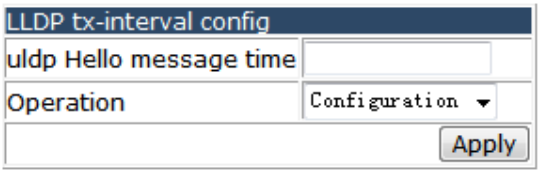
4.3.11.2 LLDP port status config.

Choose **Port configuration > LLDP configuration > LLDP port status configuration,** and the following page appears.You can set the LLDP status for each port, and the options include send, receive, both and disable.



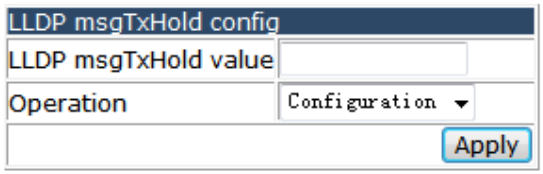
4.3.11.3 LLDP tx-interval config.

Choose **Port configuration > LLDP configuration > LLDP tx-interval config,** and the following page appears.You can set the interval time that device sending LLDP Hello message.



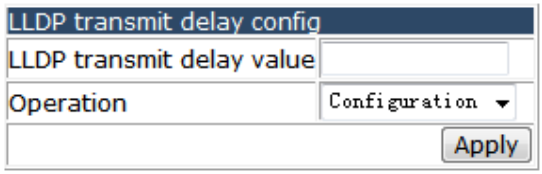
4.3.11.4 LLDP msgTxHold config.

Choose **Port configuration > LLDP configuration > LLDP msgTxHold config,** and the following page appears.You can set the LLDP aging time algorithm.



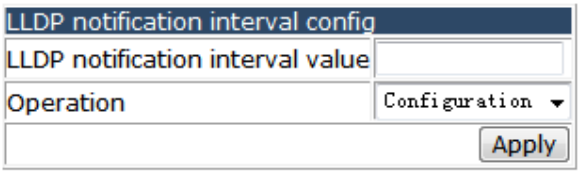
4.3.11.5 LLDP transmit delay config.

Choose **Port configuration > LLDP configuration > LLDP transmit delay config,** and the following page appears.You can modify the LLDP packets propagation delay values.



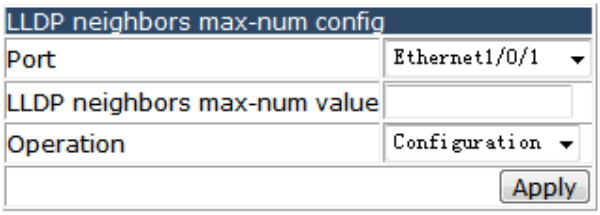
4.3.11.6 LLDP notification interval config.

Choose **Port configuration > LLDP configuration > LLDP notification interval config,** and the following page appears.You can set the LLDP notification interval configurations.



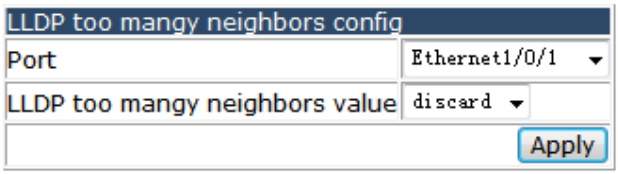
4.3.11.7 LLDP neighbors max-num config.

Choose **Port configuration > LLDP configuration > LLDP neighbors max-num config,** and the following page appears.You can set the amount of message number in the Remote MIB Table.



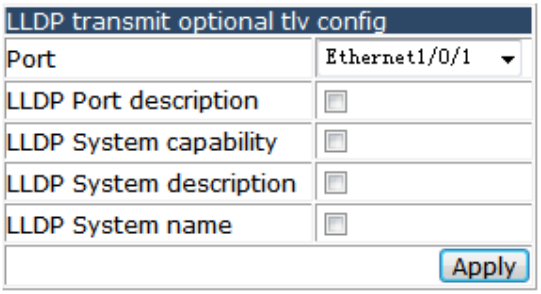
4.3.11.8 LLDP too mangy neighbors config.

Choose **Port configuration > LLDP configuration > LLDP too mangy neighbors config,** and the following page appears.You can choose to discard or delete message after fill full of the Remote table.



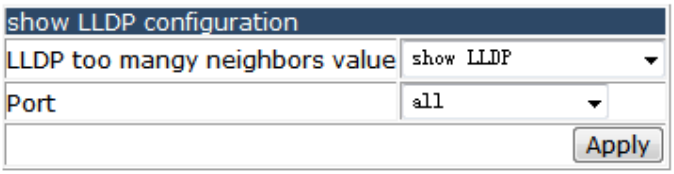
4.3.11.9 LLDP transmit optional tlv config.

Choose **Port configuration > LLDP configuration > LLDP transmit optional tlv config,** and the following page appears.You can choose the optional tlv for the transmitting LLDP message.



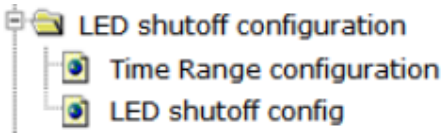
4.3.11.10 show LLDP configuration.

Choose **Port configuration > LLDP configuration > show LLDP configuration,** and the following page appears.You can show the status and statistics data for LLDP function.



4.3.12 LED shutoff configuration.

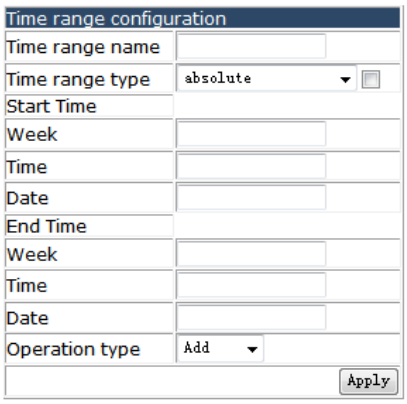
Choose **Port configuration > LED shutoff configuration,** and the following page appears.
There are "Time Range configuration", "LED shutoff config", configuration web pages.



4.3.12.1 Time Range configuration.

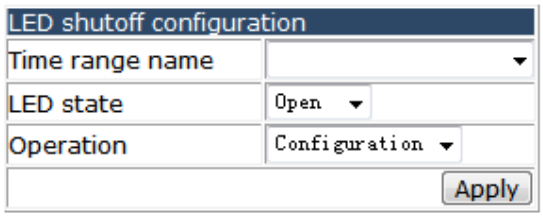
Choose **Port configuration > LED shutoff configuration > Time Range configuration,** and the following page appears.You can set the time range for the LED shutoff rule.

In the absolute mode you must input the start-time , end-time is not necesary. You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic. You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values,separate them with ",", such as:1-7:monday-sunday;127:daily;31:weekdays;96:weekend. Input date format: YYYY.MM.DD. Input week format: number (1:Monday etc.),if input multi-week values,separate them with ",",such as:1,2 identify monday&tuesday.. Input time format: HH:MM:SS.



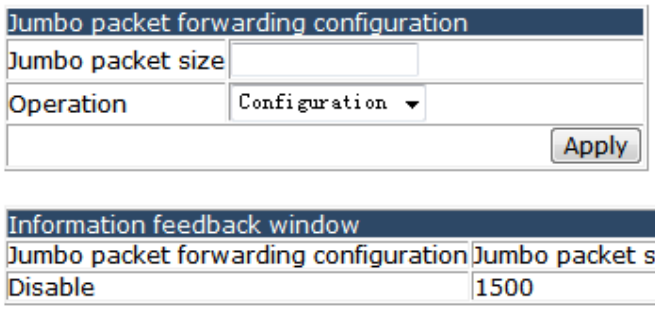
4.3.12.2 LED shutoff config.

Choose **Port configuration > LED shutoff configuration > LED shutoff config,** and the following page appears.You can design the LED to open or close at the time you configured.



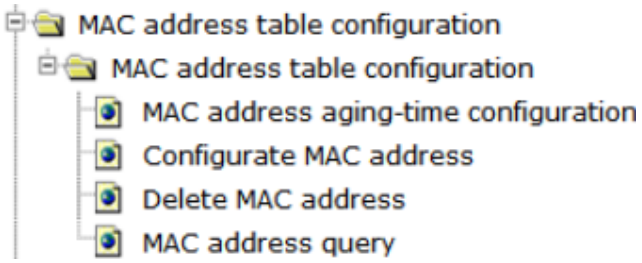
4.3.13 Jumbo packet forwarding configuration.

Choose **Port configuration > Jumbo packet forwarding configuration,** and the following page appears.You can set the size of the Jumbo packet ranging 1500-16000.



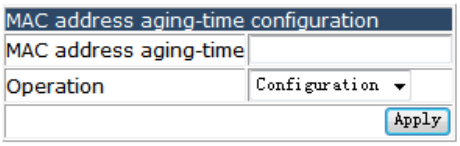
4.4 MAC address table configuration.

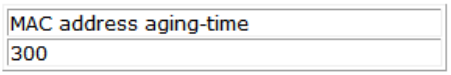
Choose **MAC address table configuration > MAC address table configuration**, and the following page appears.There are "MAC address aging-time configuration", "Configurate MAC address", "Delete MAC address", "MAC address query", configuration web pages.



4.4.1 MAC address table configuration.

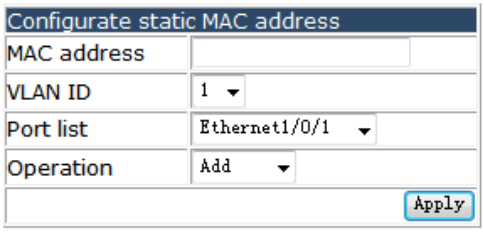
Choose **MAC address table configuration > MAC address table configuration > MAC address aging-time configuration,** and the following page appears.You can set the MAC address aging time.

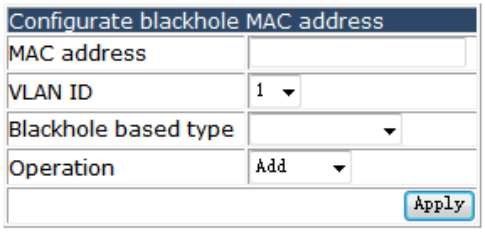




4.4.2Configuration MAC address.

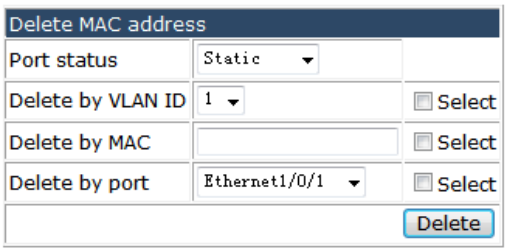
Choose **MAC address table configuration > MAC address table configuration > Configuration MAC address,** and the following page appears.You can set a static MAC address corresponding to a physic port. Also you can block the data with a static MAC address as its source or destination address.





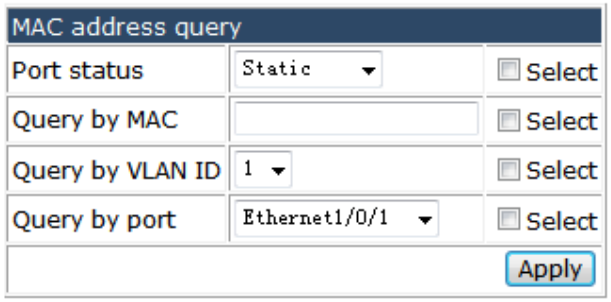
4.4.3 Delete MAC address.

Choose **MAC address table configuration > MAC address table configuration > Delete MAC address,** and the following page appears.You can delete MAC address from the static MAC address table, dynamic MAC address table or blackhole table by VLAN ID, MAC or port.



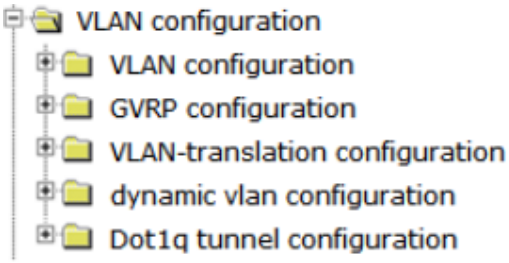
4.4.4 MAC address query.

Choose **MAC address table configuration > MAC address table configuration > MAC address query,** and the following page appears.You can show the static MAC address table, dynamic MAC address table or blackhole table by VLAN ID, MAC or port.



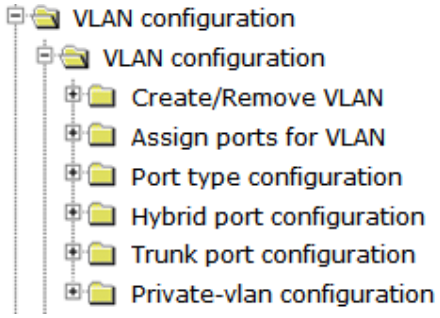
4.5 VLAN configuration.

Choose **VLAN configuration**, and the following page appears.There are "VLAN configuration", "GVRP configuration", "VLAN-translation configuration", "Dynamic VLAN configuration", "Dot1q tunnel configuration", configuration web pages.



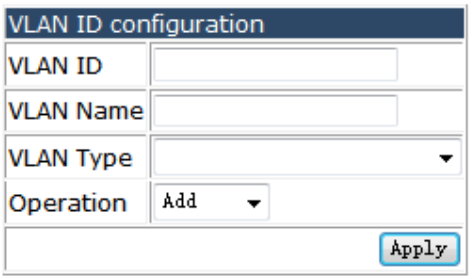
4.5.1 VLAN configuration.

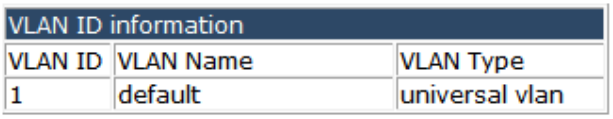
Choose **VLAN configuration > VLAN configuration**, and the following page appears.There are "Create/Remove", "Assign ports for VLAN", "Port type configuration", "Hybrid port configuration", "Trunk port configuration", "Private-vlan configuration", configuration web pages.



4.5.1.1 VLAN ID configuration.

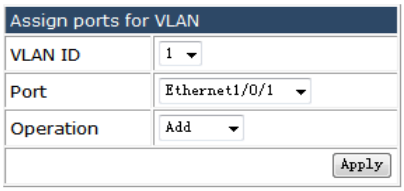
Choose **VLAN configuration > VLAN configuration > Crate/Remove VLAN > VLAN ID configuration**, and the following page appears.Here you are allowed to create or delete VLAN.VLAN type is divided into Private VLAN (isolated), Private VLAN (community), Private VLAN (primary) and universal VLAN.

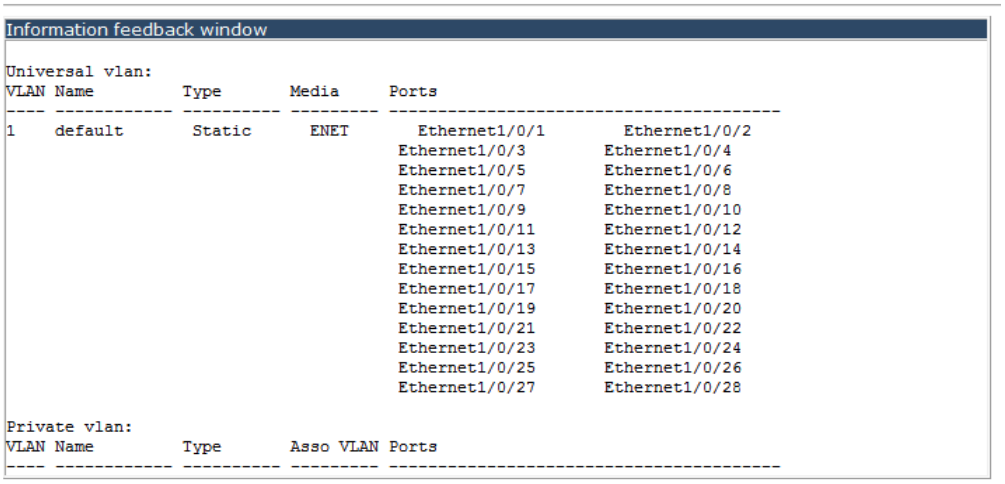




4.5.1.2 Assign ports for VLAN.

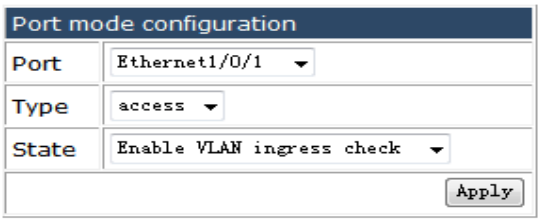
Choose **VLAN configuration > VLAN configuration > Assign ports for VLAN > Assign ports for VLAN,** and the following page appears.You can appoint a port to a configured VLAN.





4.5.1.3 Set port mode(access/hybrid/trunk).

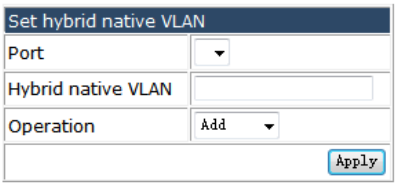
Choose **VLAN configuration > VLAN configuration > Port type configuration > Set port mode(access/hybrid/trunk),** and the following page appears.You can change any port to access, trunk or hybrid mode. Also you can choose enable VLAN ingress check or disable VLAN ingress check mode.

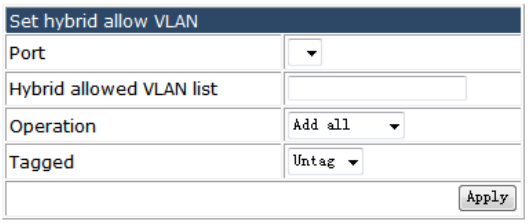


Port mode configuration		
Port	Type	State
Ethernet1/0/1	access	Open
Ethernet1/0/2	access	Open
Ethernet1/0/3	access	Open
Ethernet1/0/4	access	Open
Ethernet1/0/5	access	Open
Ethernet1/0/6	access	Open
Ethernet1/0/7	access	Open
Ethernet1/0/8	access	Open
Ethernet1/0/9	access	Open
Ethernet1/0/10	access	Open

4.5.1.4 VLAN setting for hybrid port.

Choose **VLAN configuration > VLAN configuration > Hybrid port configuration > VLAN setting for hybrid port,** and the following page appears.You can set Hybrid native VLAN ID for the hybrid port as its PVID. Also You can design which VLAN can be allowed to access to the hybrid port and whether tag or Untag the data, and the operation method including Add all, Add,Except add, Cover add and remove.

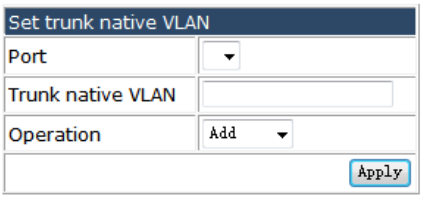


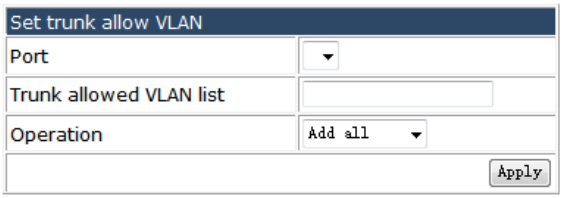


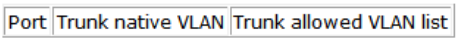
Port	Hybrid native VLAN	Hybrid Tagged allowed VLAN list	Hybrid UnTagged allowed VLAN list

4.5.1.5 VLAN setting for trunk port.

Choose **VLAN configuration > Trunk port configuration > VLAN setting for trunk port,** and the following page appears.You can set Trunk native VLAN ID for the truck port as its PVID. Also You can design which VLAN can be allowed to access to the trunk port, the operation method including Add all, Add，Except add, Cover add and remove.

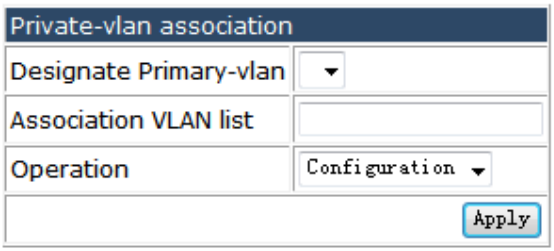


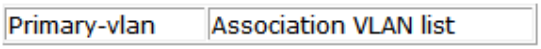




4.5.1.6 Private-vlan association.

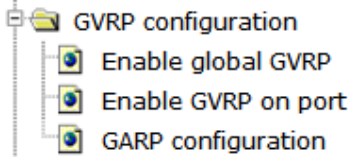
Choose **VLAN configuration > Private-vlan configuration > Private-vlan association,** and the following page appears.You can set the association VLAN to bind with the primary-vlan, then the members in association VLANs can communicate with primary-vlan.





4.5.2 GVRP configuration.

Choose **VLAN configuration > GVRP configuration**, and the following page appears.There are "Enable global GVRP", "Enable GVRP on port", "GARP configuration", configuration web pages.

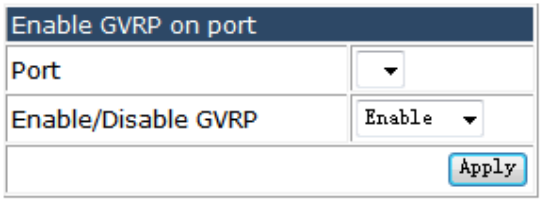


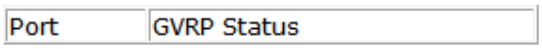
4.5.2.1 Enable global GVRP.

Choose **VLAN configuration > GVRP configuration > Enable global GVRP**, and the following page appears.You can enable or disable the global GVRP. To configure port GVRP must enable the global GVRP first.

4.5.2.2 Enable GVRP on port.

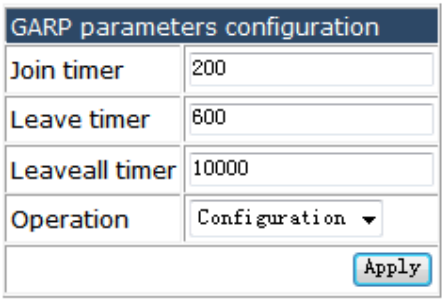
Choose **VLAN configuration > GVRP configuration > Enable GVRP on port**, and the following page appears.You can enable or disable GVRP function for each port.





4.5.2.3 GARP configuration.

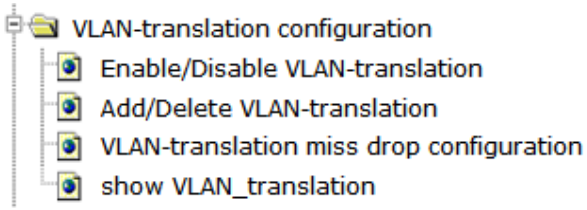
Choose **VLAN configuration > GVRP configuration > GARP configuration**, and the following page appears.You can set the GVRP timer parameters.



4.5.3 VLAN-translation configuration.

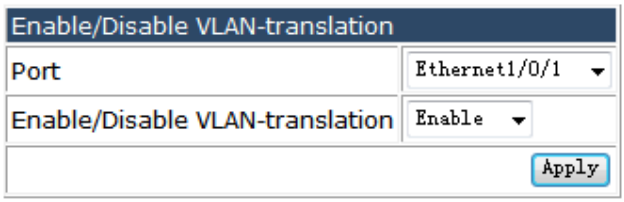
Choose **VLAN configuration > VLAN-translation configuration**, and the following page appears.

There are "Enable/Disable VLAN-translation", "Add/Delete VLAN-translation", "VLAN-translation miss drop configuration", "show VLAN-translation", configuration web pages.



4.5.3.1 Enable/Disable VLAN-translation.

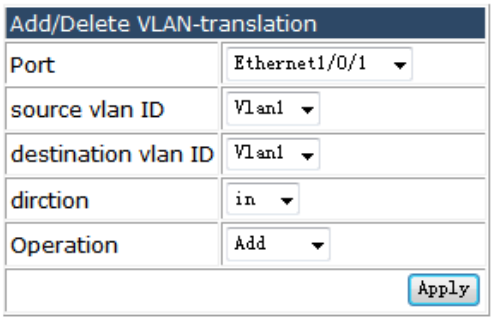
Choose **VLAN configuration > VLAN-translation configuration > Enable/Disable VLAN-translation,** and the following page appears.You can enable or disable the port VLAN translation mode.



Port	VLAN-translation Status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable
Ethernet1/0/12	Disable
Ethernet1/0/13	Disable

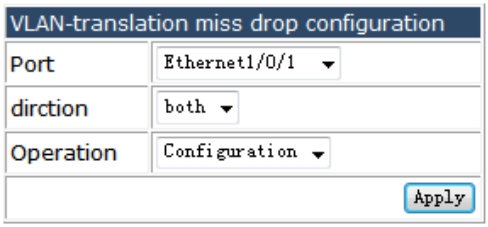
4.5.3.2 Add/Delete VLAN-translation.

Choose **VLAN configuration > VLAN-translation configuration > Add/Delete VLAN-translation,** and the following page appears.You can set the translation policy for each port, data transmit in or out the port the source VLAN ID will be translated to the destination VLAN ID.



4.5.3.3 VLAN-translation miss drop configuration.

Choose **VLAN configuration > VLAN-translation configuration > VLAN-translation miss drop configuration,** and the following page appears.You can decide to whether discard data failed to execute VLAN-translation and the transmission direction for the operation.

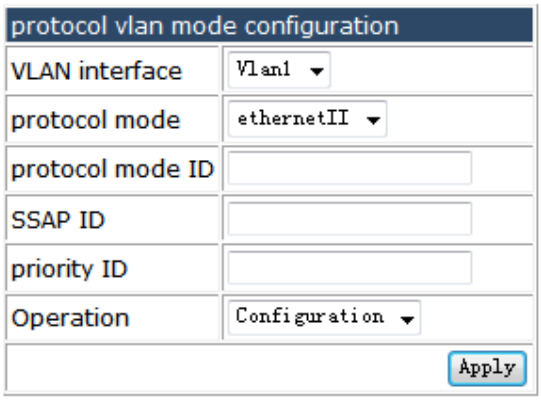


4.5.3.4 Show VLAN-translation.

Choose **VLAN configuration > VLAN-translation configuration > Show VLAN-translation,** and the following page appears.You can show the VLAN-translation information for all ports enabled this function.

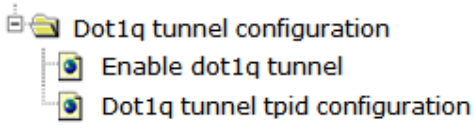
4.5.4 Dynamic VLAN configuration.

Choose **VLAN configuration > Dynamic VLAN configuration > Protocol VLAN configuration > Protocol VLAN mode configuration,** and the following page appears.You can set protocol-vlan rules, the protocol mode include Ethernet Ⅱ, snap, LLC and all, the protocol mode ID rang for ethernet Ⅱ or snap rang is 1-65536, for llc is 0-255, the SSAP ID just for llc rang is 0-255, the priority ID rang is 0-7.



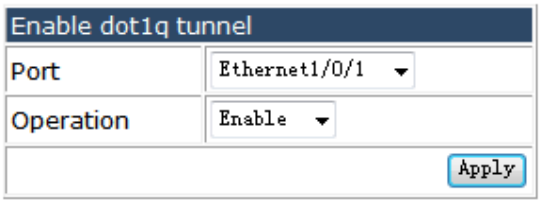
4.5.5 Dot1q tunnel configuration.

Choose **VLAN configuration > Dot1q tunnel configuration,** and the following page appears.There are "Enable dot1q tunnel", "Dot1q tunnel tpid configuration", configuration web pages.



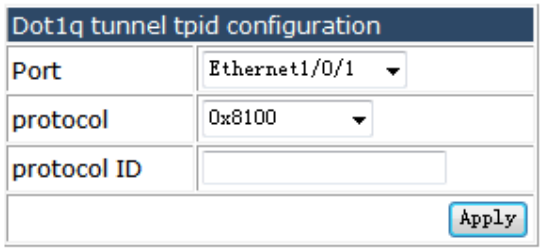
4.5.5.1 Enable dot1q tunnel.

Choose **VLAN configuration > Dot1q tunnel configuration > Enable dot1q tunnel,** and the following page appears.You can enable or disable dot1q tunnel function for every Trunk port.



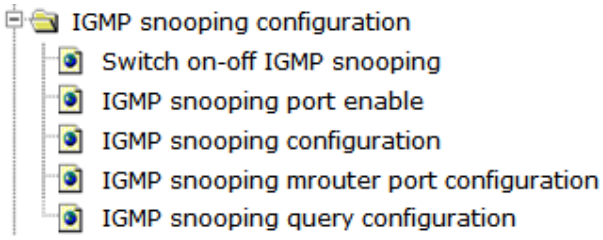
4.5.5.2 Dot1q tunnel tpid configuration.

Choose **VLAN configuration > Dot1q tunnel configuration >** Dot1q tunnel tpid configuration, and the following page appears.You can configure the Dot1q protocol for trunk, please keep this value the same with the connected device.



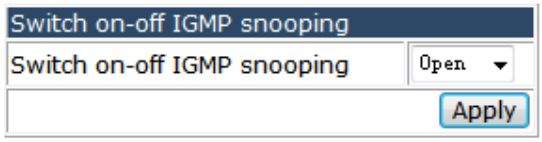
4.6 IGMP snooping configuration.

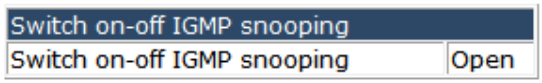
Choose **IGMP snooping configuration,** and the following page appears.There are "Switch on-off IGMP snooping", "IGMP snooping port enable", "IGMP snooping configuration", "IGMP snooping mrouter port configuration", "IGMP snooping query configuration", configuration web pages.



4.6.1 Switch on-off IGMP snooping.

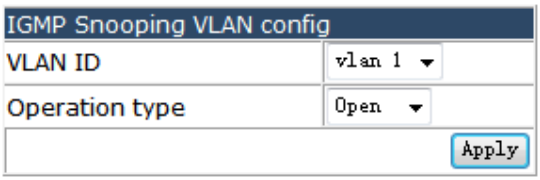
Choose **IGMP snooping configuration > Switch on-off IGMP snooping,** and the following page appears.You can open or close the IGMP snooping function.





4.6.2 IGMP snooping port enable.

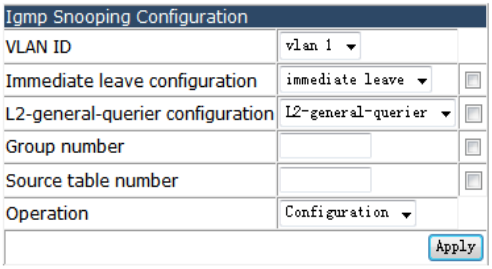
Choose **IGMP snooping configuration > IGMP snooping port enable,** and the following page appears.You can open or close the IGMP Snooping function for different VLAN.



IGMP Snooping VLAN config	
VLAN ID	Operation type
1	CLOSE

4.6.3 IGMP snooping configuration.

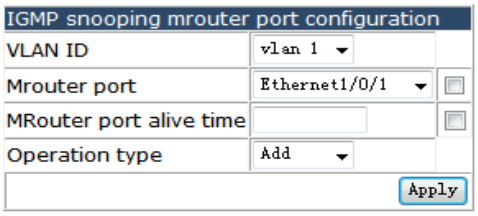
Choose **IGMP snooping configuration > IGMP snooping configuration,** and the following page appears.You can set the IGMP Snooping parameters for each VLAN, choose enable Immediate leave configuration and L2-general-querier configuration or not. The default value for Group number is 50 and for Source table number is 40, it is recommended not to change them.



VLAN ID	Immediate leave configuration	L2-general-querier configuration	Group number	Source table number
1	Disable	Disable		

4.6.4 IGMP snooping mrouter port configuration.

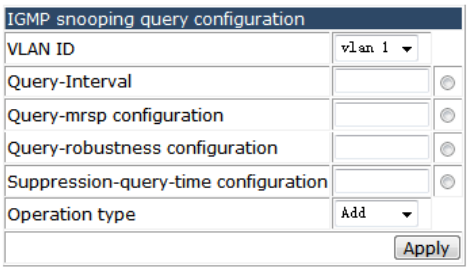
Choose **IGMP snooping configuration > IGMP snooping mrouter port configuration,** and the following page appears.You can choose the Mrouter port which connecting with the router for VLAN, and the Mrouter port alive time for dynamic Mrouter port.



VLAN ID	Mrouter port	MRouter port alive time
1		

4.6.5 IGMP snooping query configuration.

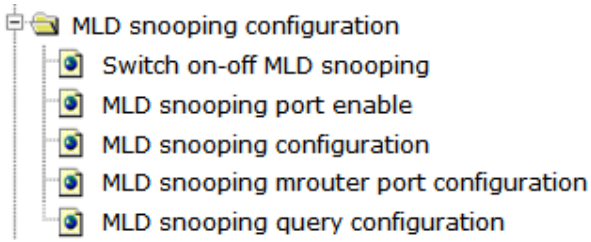
Choose **IGMP snooping configuration > IGMP snooping query configuration,** and the following page appears.You can set the query parameters for VLAN, the default value for those four options are 125, 10, 2, 255, they are recommended to keep default.



VLAN ID	Query-Interval	Query-mrsp configuration	Query-robustness configuration	Suppression-query-time configuration
1				

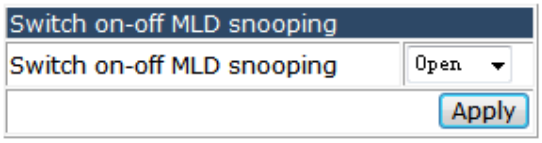
4.7 MLD snooping configuration.

Choose **MLD snooping configuration,** and the following page appears.There are "Switch on-off MLD snooping", "MLD snooping port enable", "MLD snooping configuration", "MLD snooping mrouter port configuration", "MLD snooping query configuration", configuration web pages.



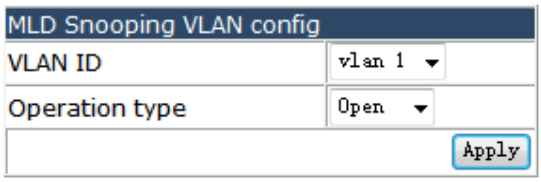
4.7.1 Switch on-off MLD snooping.

Choose **MLD snooping configuration > Switch on-off MLD snooping,** and the following page appears.You can open or close the MLD snooping function.



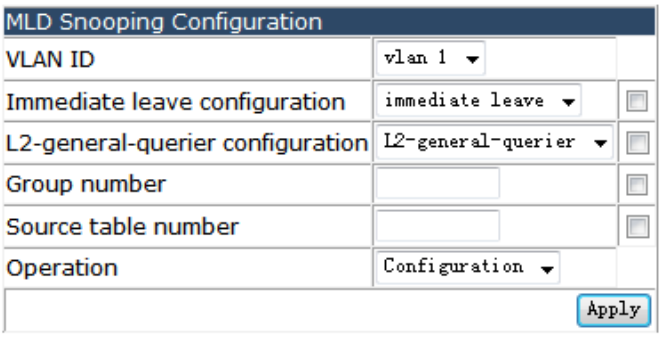
4.7.2 MLD snooping port enable.

Choose **MLD snooping configuration > MLD snooping port enable,** and the following page appears.You can open or close the MLD snooping function for each VLAN.



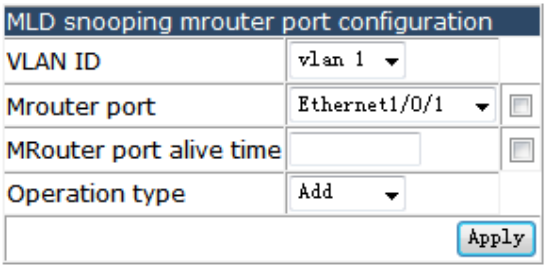
4.7.3 MLD snooping configuration.

Choose **MLD snooping configuration > MLD snooping configuration,** and the following page appears.You can set the MLD Snooping parameters for each VLAN, choose enable Immediate leave configuration and L2-general-querier configuration or not. The default value for Group number is 50 and for Source table number is 40, it is recommended not to change them.



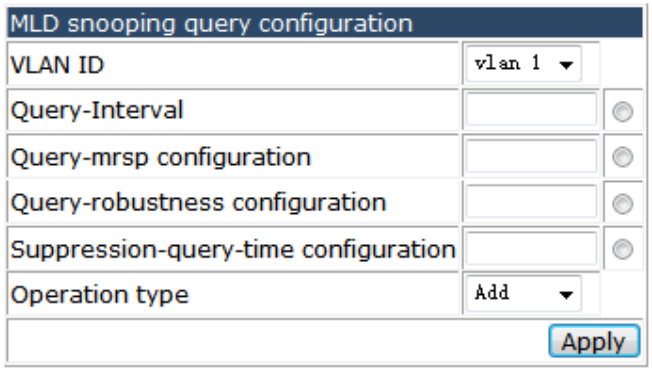
4.7.4 MLD snooping mrouter port configuration.

Choose **MLD snooping configuration > MLD snooping mrouter port configuration,** and the following page appears.You can choose the Mrouter port which connecting with the router for VLAN, and the Mrouter port alive time for dynamic Mrouter port.



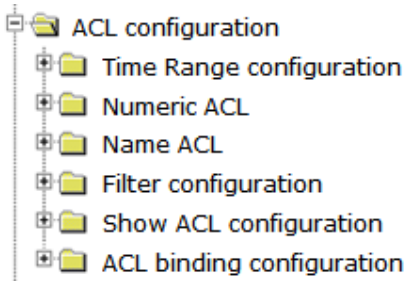
4.7.5 MLD snooping query configuration.

Choose **MLD snooping configuration > MLD snooping query configuration,** and the following page appears.You can set the query parameters for VLAN, the default value for those four options are 125, 10, 2, 255, they are recommended to keep default.



4.8 ACL configuration.

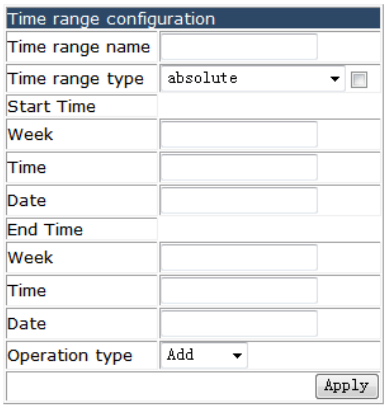
Choose **ACL configuration,** and the following page appears.There are "Time Range configuration", "Numeric ACL", "Name ACL", "Filter configuration", "Show ACL configuration", "ACL binding configuration", configuration web pages.



4.8.1 Time Range configuration.

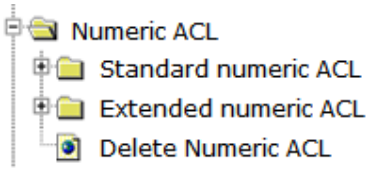
Choose **ACL configuration > Time Range configuration > Time Range configuration,** and the following page appears.You can set the time policies for ACL rules.

In the absolute mode you must input the start-time , end-time is not necesary. You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic. You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values,separate them with ",", such as:1-7:monday-sunday;127:daily;31:weekdays;96:weekend. Input date format: YYYY.MM.DD. Input week format: number (1:Monday etc.),if input multi-week values,separate them with ",",such as:1,2 identify monday&tuesday.. Input time format: HH:MM:SS.



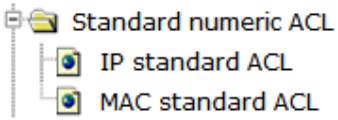
4.8.2 Numeric ACL.

Choose **Numeric ACL,** and the following page appears.There are "Standard numeric ACL", "Extended numeric ACL", "Delete Numeric ACL", configuration web pages.



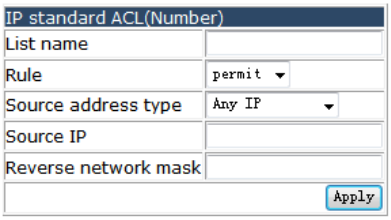
4.8.2.1 Standard numeric ACL.

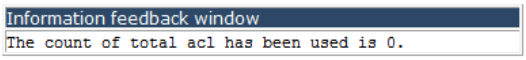
Choose **ACL configuration > Numeric ACL > Standard numeric ACL,** and the following page appears.There are "IP standard ACL", "MAC standard ACL", configuration web pages.



4.8.2.1.1 IP standard ACL.

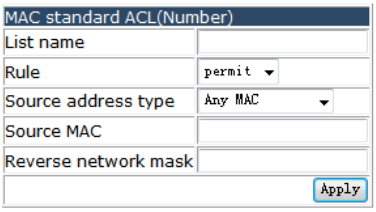
Choose **ACL configuration > Numeric ACL > Standard numeric ACL > IP standard ACL,** and the following page appears.You can add a ACL rule to permit or deny data from different source address. If the type is Any IP don't need set IP address and mask, if the type is Host IP don't need to set Reverse network mask, if the type is Specified IP the IP address and Reverse network mask decided which IP will be controlled.

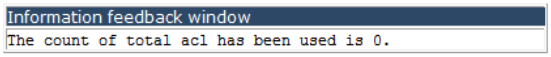




4.8.2.1.2 MAC standard ACL.

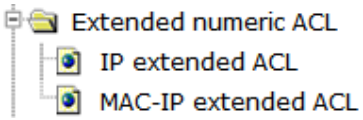
Choose **ACL configuration > Numeric ACL > Standard numeric ACL > MAC standard ACL,** and the following page appears.You can add a MAC ACL rule to permit or deny data from different source MAC address. If the type is Any MAC don't need set MAC address and mask, if the type is Host MAC don't need to set Reverse network mask, if the type is Specified MAC the MAC address and Reverse network mask decided which MAC will be controlled.





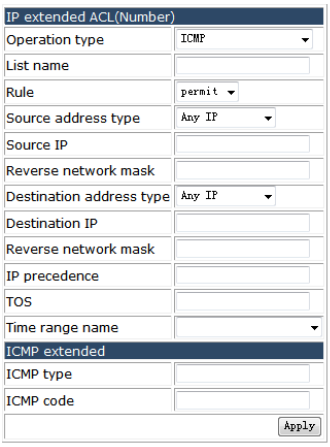
4.8.2.2 Extended numeric ACL.

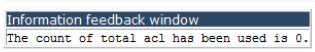
Choose **ACL configuration > Numeric ACL > Extended numeric ACL,** and the following page appears.There are "IP extended ACL", "MAC-IP extended ACL", configuration web pages.



4.8.2.2.1 IP extended ACL.

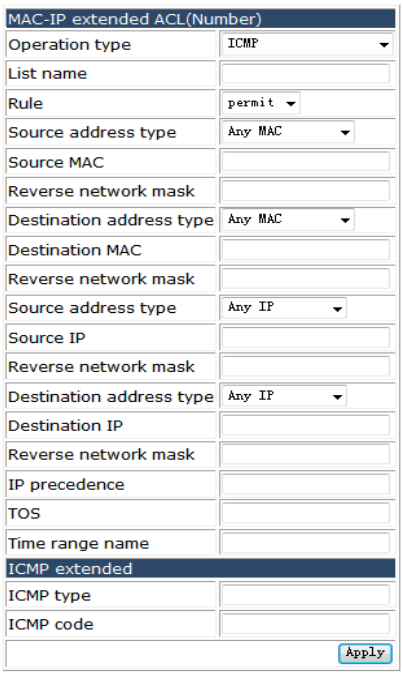
Choose **ACL configuration > Numeric ACL > Extended numeric ACL > IP extended ACL,** and the following page appears.You can configure the extended ACL with advanced function include Operation type, Source address, Destination address, IP precedence, TOS, Time range and the protocol features. The Operation type include ICMP, IGMP, TCP, UDP, EIGRP, GRE, IGRP, IPINIP, OSPF, IP, Specified_protocol.

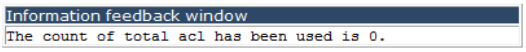




4.8.2.2.2 MAC-IP extended ACL.

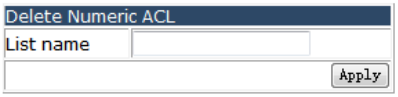
Choose **ACL configuration > Numeric ACL > Extended numeric ACL > MAC-IP extended ACL,** and the following page appears.You can configure the extended MAC-IP ACL with advanced function, and the qualification can be both MAC and IP address.





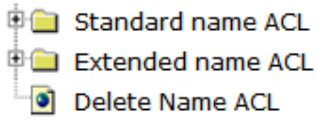
4.8.2.3Delete Numeric ACL.

Choose **ACL configuration > Numeric ACL > Extended numeric ACL > Delete Numeric ACL,** and the following page appears.You can delete Numeric ACL rules bast on their List names.



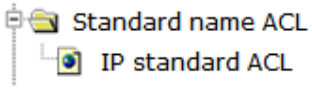
4.8.3 Name ACL.

Choose **ACL configuration > Name ACL,** and the following page appears.There are "Standard name ACL", "Extended name ACL", "Delete name ACL", configuration web pages.



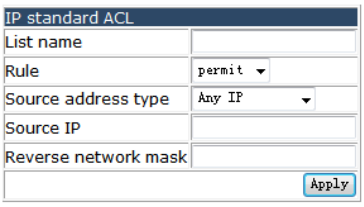
4.8.3.1 Standard name ACL.

Choose **ACL configuration > Name ACL > Standard name ACL,** and the following page appears.



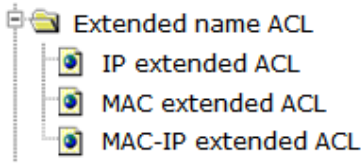
4.8.3.1.1 IP standard ACL.

Choose **ACL configuration > Name ACL > Standard name ACL > IP standard ACL,** and the following page appears.You can add a ACL rule to permit or deny data from different source address. The List name must start with letter. If the type is Any IP don't need set IP address and mask, if the type is Host IP don't need to set Reverse network mask, if the type is Specified IP the IP address and Reverse network mask decided which IP will be controlled.



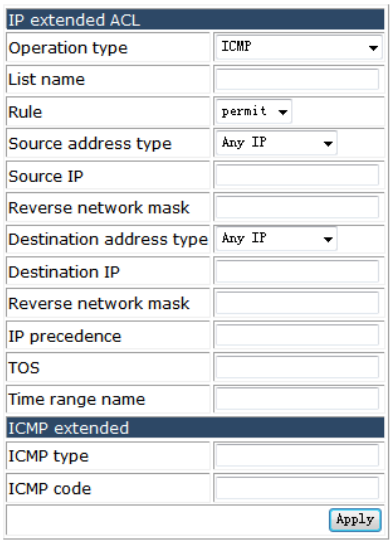
4.8.3.2 Extended name ACL.

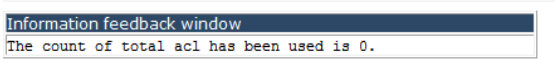
Choose **ACL configuration > Name ACL > Extended name ACL,** and the following page appears.There are "IP extended ACL", "MAC extended ACL", "MAC-IP extended ACL", configuration web pages.



4.8.3.2.1 IP extended ACL.

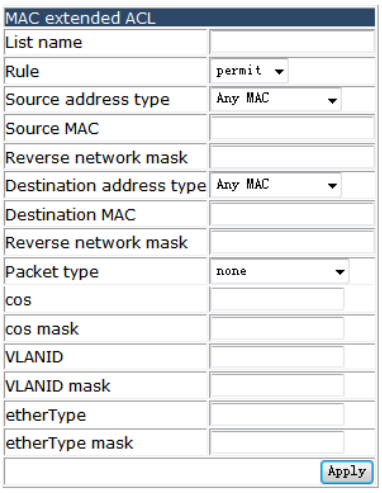
Choose **ACL configuration > Name ACL > Extended name ACL > IP extended ACL,** and the following page appears.You can configure the extended ACL with advanced function include Operation type, Source address, Destination address, IP precedence, TOS, Time range and the protocol features. The List name must start with letter. The Operation type include ICMP, IGMP, TCP, UDP, EIGRP, GRE, IGRP, IPINIP, OSPF, IP, Specified_protocol.





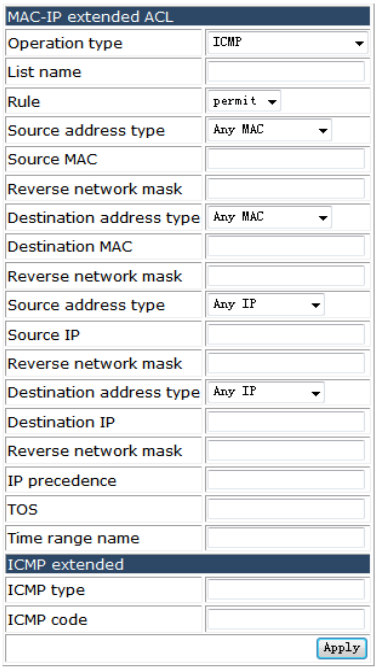
4.8.3.2.2 MAC extended ACL.

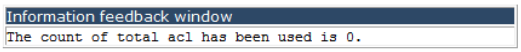
Choose **ACL configuration > Name ACL > Extended name ACL > MAC extended ACL,** and the following page appears.You can configure the extended MAC ACL with advanced function include Source address, Destination address, Packet type, COS, COS mask, VLAN ID, VLAN ID mask, ether Type and ether Type mask. The List name must start with letter. The Packet type include Tagged-802.3,Tagged-eth2,Untagged-802.3,Untagged-eth2.



4.8.3.2.3 MAC-IP extended ACL.

Choose **ACL configuration > Name ACL > Extended name ACL > MAC-IP extended ACL,** and the following page appears.You can configure the extended MAC-IP ACL with advanced function, and the qualification can be both MAC and IP address. The List name must start with letter.



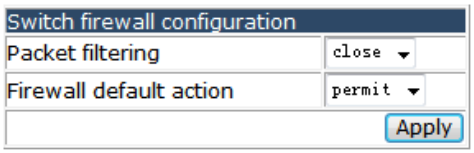


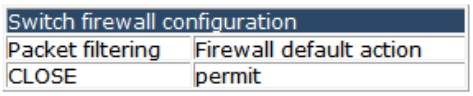
4.8.3.3 Delete Name ACL.

Choose **ACL configuration > Name ACL > Delete name ACL,** and the following page appears.You can delete Name ACL rules bast on their List names.

4.8.4 Firewall configuration.

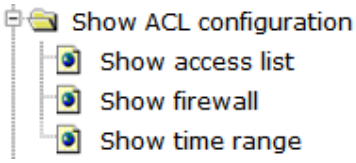
Choose **ACL configuration > Filter configuration > Firewall configuration,** and the following page appears.You must open the Packet filtering function to make the ACL list take effect. The Firewall default action is permit means data mismatching the ACL rule is permitted.





4.8.5 Show ACL configuration.

Choose **ACL configuration > Show ACL configuration,** and the following page appears.There are "Show access list", "Show firewall", "Show time range", configuration web pages.



4.8.5.1 Show access list.

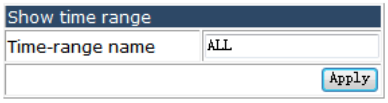
Choose **ACL configuration > Show ACL configuration > Show access list,** and the following page appears.You can show the access-list by name or show all table.

4.8.5.2 Show firewall.

Choose **ACL configuration > Show ACL configuration > Show firewall,** and the following page appears.You can show the status of firewall.

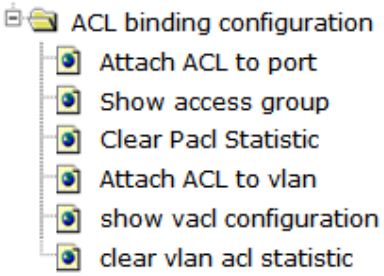
4.8.5.3 Show time range.

Choose **ACL configuration > Show ACL configuration > Show time range,** and the following page appears.You can show time range list by name or show all table.



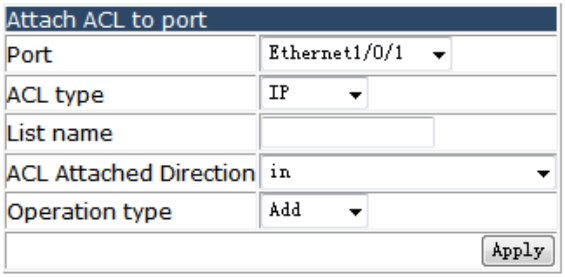
4.8.6 ACL binding configuration.

Choose **ACL configuration > ACL binding configuration,** and the following page appears.There are "Attach ACL to port", "Show access group", "Clear PACL Statistic", "Attach ACL to vlan", "Show VACL configuration", "Clear vlan ACL statistic", configuration web pages.



4.8.6.1 Attach ACL to port.

Choose **ACL configuration > ACL binding configuration > Attach ACL to port,** and the following page appears.You can attach an IP, MAC or MAC-IP ACL rule to a port, and decide whether to enable traffic-statistic.

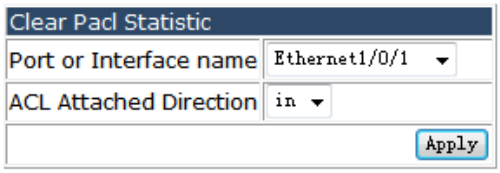


4.8.6.2 Show access group.

Choose **ACL configuration > ACL binding configuration > Show access group,** and the following page appears.You can show which ACL rules are attached to one port, or all the ACL and port binding status.

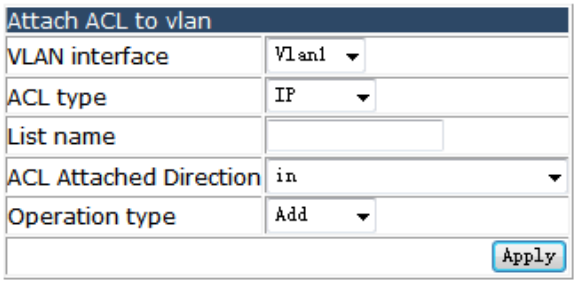
4.8.6.3 Clear PACL Statistic.

Choose **ACL configuration > ACL binding configuration > Clear PACL Statistic,** and the following page appears.You can clear packet filter statistics at the specified port.



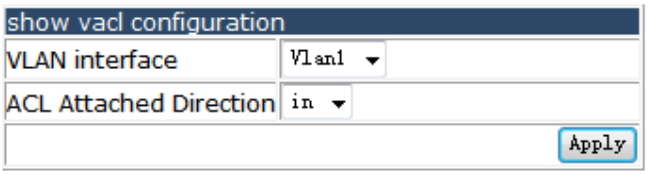
4.8.6.4 Attach ACL to vlan.

Choose **ACL configuration > ACL binding configuration > Attach ACL to vlan,** and the following page appears.You can attach an IP, MAC or MAC-IP ACL rule to a VLAN and decide whether to enable traffic-statistic.



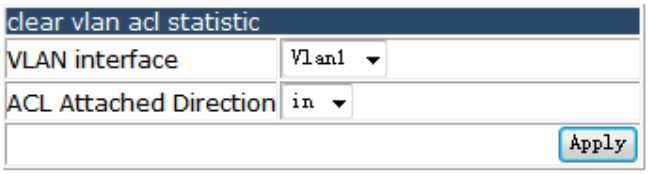
4.8.6.5 Show VACL configuration.

Choose **ACL configuration > ACL binding configuration > Show VACL configuration,** and the following page appears.You can show which ACL rules are attached to a VLAN, or all the ACL and VLAN binding status.



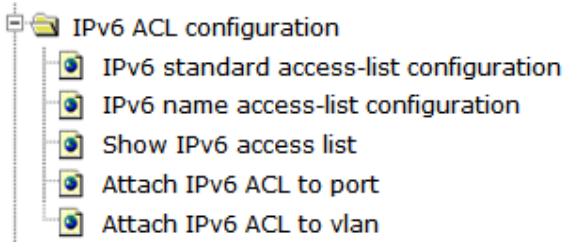
4.8.6.6 Clear vlan ACL statistic.

Choose **ACL configuration > ACL binding configuration > Clear vlan ACL statistic,** and the following page appears.You can clear packet filter statistics at the specified VLAN.



4.9 IPv6 ACL configuration.

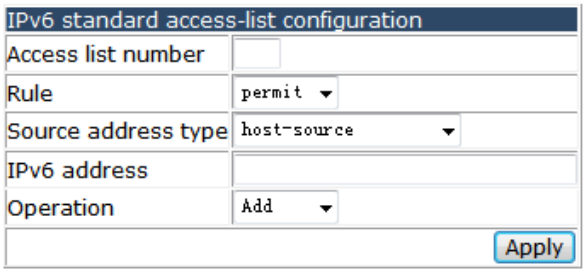
Choose **IPv6 ACL configuration,** and the following page appears.There are "IPv6 standard access-list configuration", "IPv6 name access-list configuration", "Show IPv6 access list", "Attach IPv6 ACL to port", "Attach IPv6 ACL to vlan", configuration web pages.



4.9.1 IPv6 standard access-list configuration.

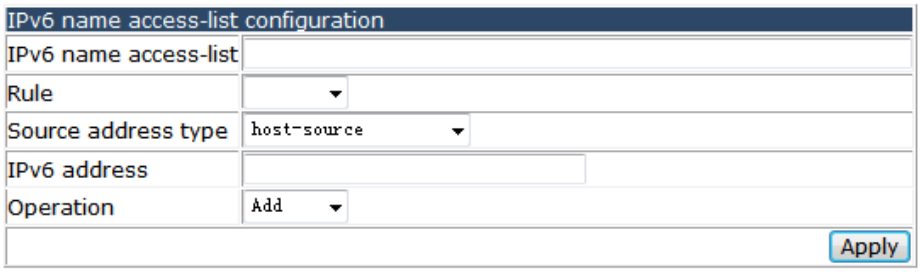
Choose **IPv6 ACL configuration > IPv6 standard access-list configuration,** and the following page appears.You can add an IPv6 ACL rule to permit or deny data from

different source address. If the type is any -source don't need set IPv6 address, if the type is host-source fill a full IPv6 address, if the type is IPv6 source prefix the IPv6 address show fill a prefix.



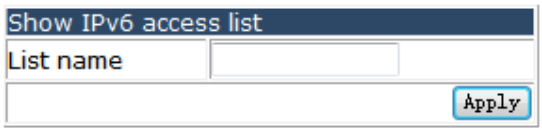
4.9.2 IPv6 name access-list configuration.

Choose **IPv6 ACL configuration > IPv6 name access-list configuration,** and the following page appears.You can add an IPv6 ACL rule to permit or deny data from different source address. If the type is any -source don't need set IPv6 address, if the type is host-source fill a full IPv6 address, if the type is IPv6 source prefix the IPv6 address show fill a prefix.The List name must start with letter.



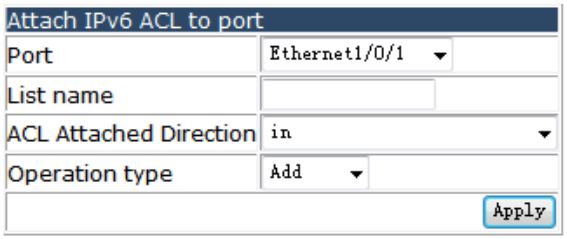
4.9.3 Show IPv6 access list.

Choose **IPv6 ACL configuration > Show IPv6 access list,** and the following page appears.You can show the IPv6 ACL rule by List name or all the IPv6 ACL table by fill "all".



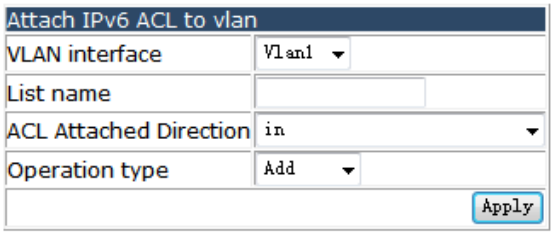
4.9.4 Attach IPv6 ACL to port.

Choose **IPv6 ACL configuration > Attach IPv6 ACL to port,** and the following page appears.You can attach an IPv6 ACL rule to a port, and decide whether to enable traffic-statistic.



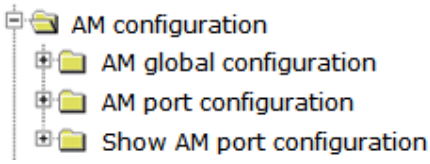
4.9.5 Attach IPv6 ACL to vlan.

Choose **IPv6 ACL configuration > Attach IPv6 ACL to vlan,** and the following page appears.You can attach an IPv6 ACL rule to a VLAN, and decide whether to enable traffic-statistic.



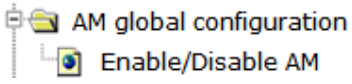
4.10 AM configuration.

Choose **AM configuration,** and the following page appears.There are "AM global configuration", "AM port configuration", "Show AM port configuration", configuration web pages.



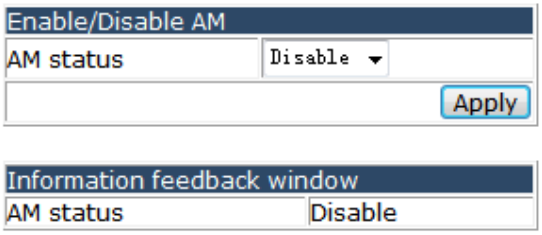
4.10.1 AM global configuration.

Choose **AM configuration > AM global configuration,** and the following page appears.



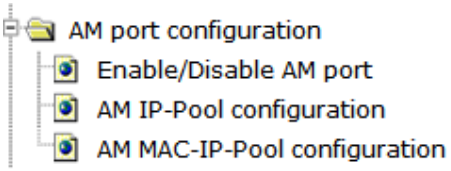
4.10.1.1 Enable/Disable AM.

Choose **AM configuration > AM global configuration > Enable/Disable AM,** and the following page appears.You can enable or disable the AM function.



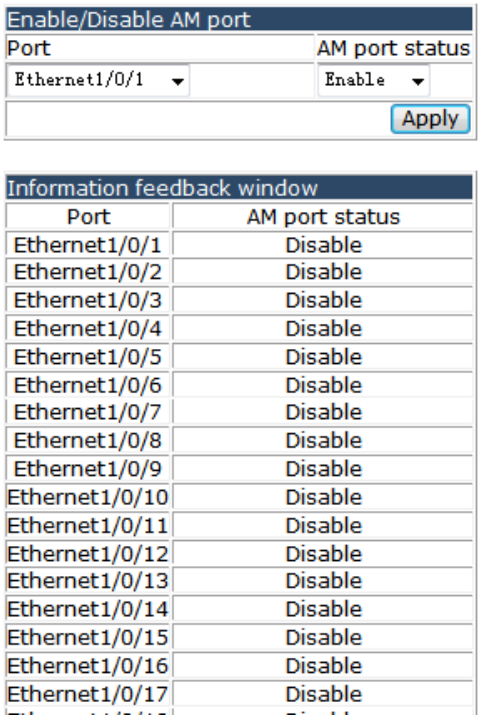
4.10.2 AM port configuration.

Choose **AM configuration > AM port configuration,** and the following page appears.There are "Enable/Disable AM port", "AM IP-Pool configuration", "AM MAC-IP-Poll configuration", configuration web pages.



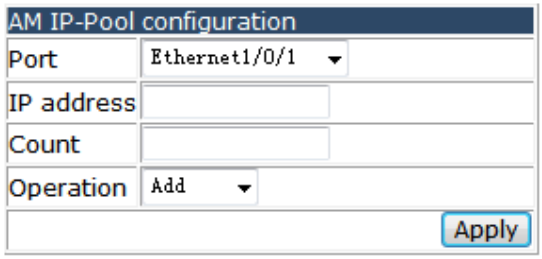
4.10.2.1 Enable/Disable AM port.

Choose **AM configuration > AM port configuration > Enable/Disable AM port,** and the following page appears.You can enable or disable AM function for each port.



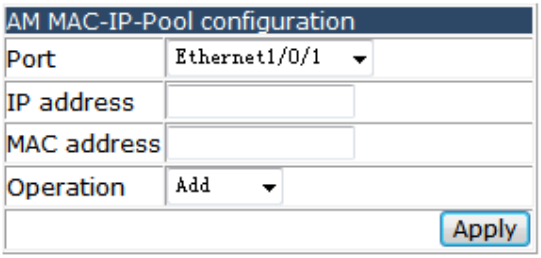
4.10.2.2 AM IP-Pool configuration.

Choose **AM configuration > AM port configuration > AM IP-Pool configuration,** and the following page appears.You can set the IP pool start from the IP address and the count decide the number of continuous IP.



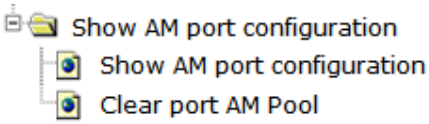
4.10.2.3 AM MAC-IP-Poll configuration.

Choose **AM configuration > AM port configuration > AM MAC-IP-Poll configuration , and the following page appears.You can set the MAC-IP address for each port, only data matched both MAC and IP address are permit.**



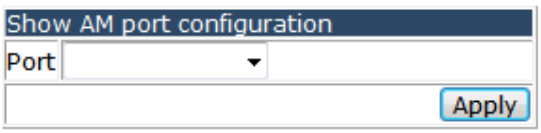
4.10.3 Show AM port configuration.

Choose **AM configuration > Show AM port configuration,** and the following page appears.There are "Show AM port configuration", "Clear port", configuration web pages.



4.10.3.1 Show AM port configuration.

Choose **AM configuration > Show AM port configuration > Show AM port configuration,** and the following page appears.You can show the AM rule for each port.

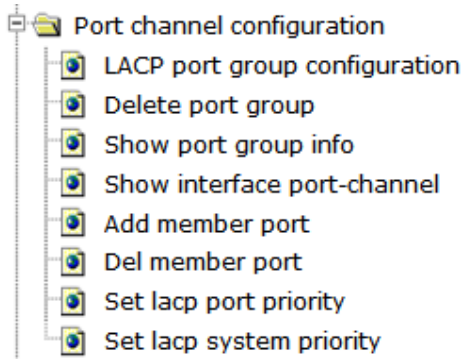


4.10.3.2 Clear port configuration.

Choose **AM configuration > Show AM port configuration > Clear port configuration,** and the following page appears.You can clear the all the AM pool, ip pool or MAC-IP pool.

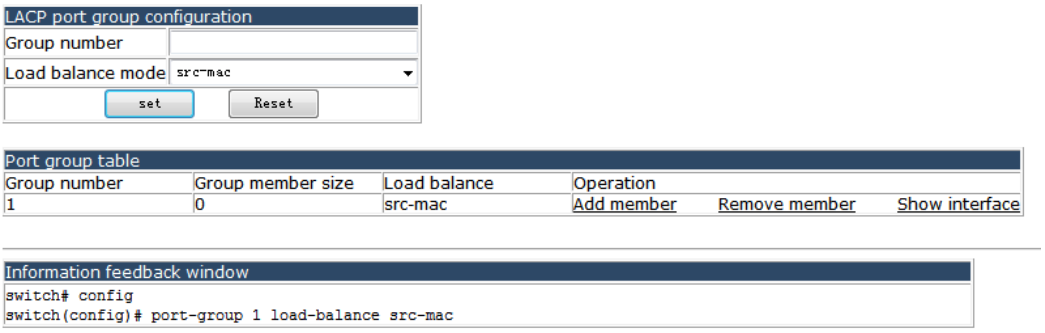
4.11 Port channel configuration.

Choose **Port channel configuration,** and the following page appears.There are "LACP port group configuration", "Delete port group", "Show port group info", "Show interface port-channel", "Add member port", "Del member port", "Ste LACP port priority", "Set LACP system priority", configuration web pages.



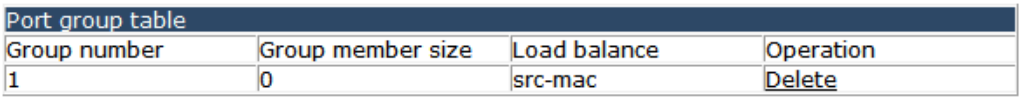
4.11.1 LACP port group configuration.

Choose **Port channel configuration > LACP port group configuration,** and the following page appears.You can set the LACP port group with the Load balance mode src-mac, dst-mac, dst-src-mac, src-IP, dst-ip, or dst-src-ip.



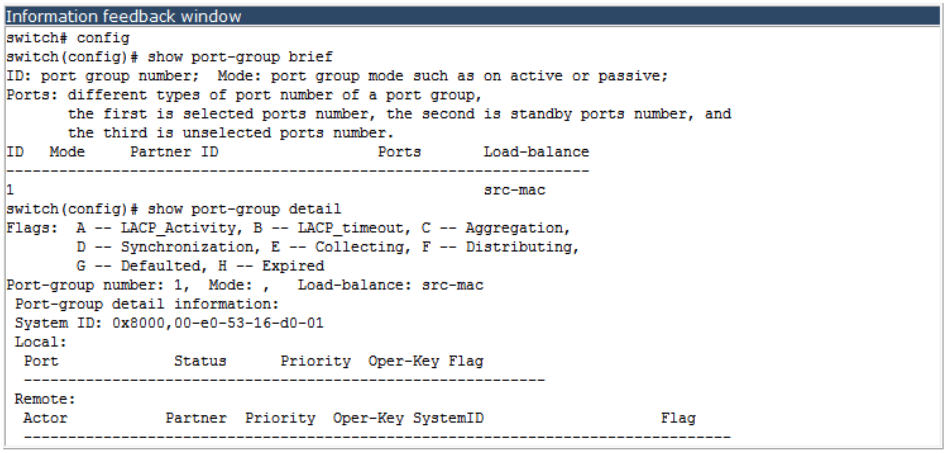
4.11.2 Delete port group.

Choose **Port channel configuration > Delete port group,** and the following page appears.You can delete any rule in the Port group table.



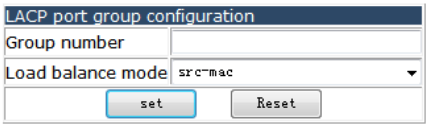
4.11.3 Show port group info.

Choose **Port channel configuration > Show port group info,** and the following page appears.You can show the brief information and detail information of the port group function.



4.11.4 Show interface port-channel.

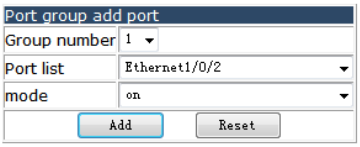
Choose **Port channel configuration > Show interface port-channel,** and the following page appears.You can show the brief and statistic information for every group number by click the “show interface” option.



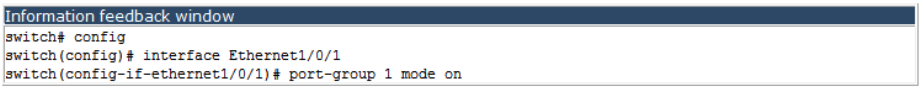
Port group table					
Group number	Group member size	Load balance	Operation		
1	1	src-mac	Add member	Remove member	Show interface

4.11.5 Add member port.

Choose **Port channel configuration > Add member port,** and the following page appears.You can add a physical port to a port group via on, active or passive mode.

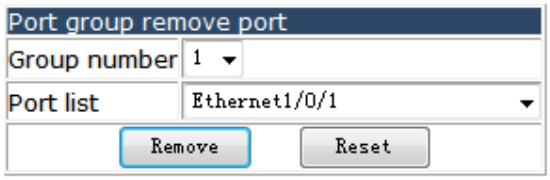


Port group port list	
Index	Port Name
1	Ethernet1/0/1



4.11.6 Del member port.

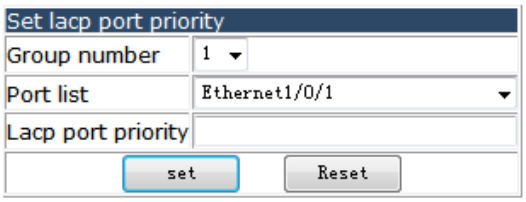
Choose **Port channel configuration > Del member port,** and the following page appears.You can remove a physical port from a port group.



Port group port list	
Index	Port Name
1	Ethernet1/0/1

4.11.7 Set LACP port priority.

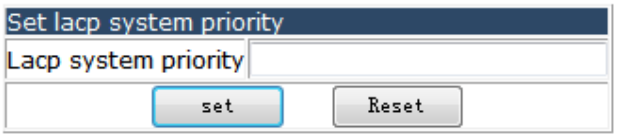
Choose **Port channel configuration > Set LACP port priority,** and the following page appears.You can set the LACP priority for the appointed port in a port group.



Port group port list	
Group number	Port Name
1	Ethernet1/0/1

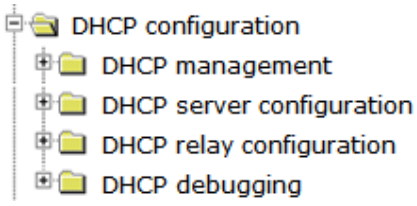
4.11.8 Set LACP system priority.

Choose **Port channel configuration > Set LACP system priority,** and the following page appears.You can set the LACP system priority.



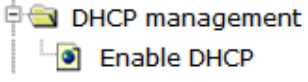
4.12 DHCP configuration.

Choose **DHCP configuration,** and the following page appears.There are "DHCP management", "DHCP server configuration", "DHCP relay configuration", "DHCP debugging", configuration web pages.



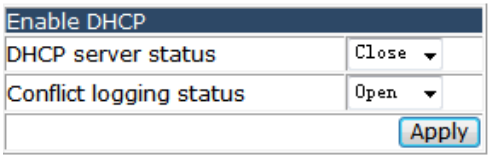
4.12.1 DHCP management.

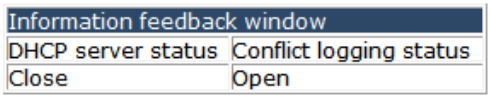
Choose **DHCP configuration > DHCP management,** and the following page appears.



4.12.1.1 Enable DHCP.

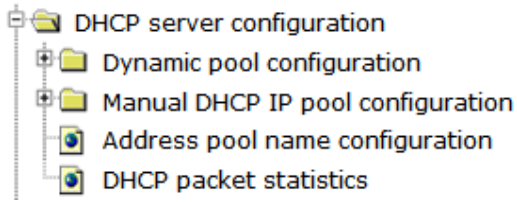
Choose **DHCP configuration > DHCP management > Enable DHCP,** and the following page appears.You can open or close the DHCP server and conflict logging function.





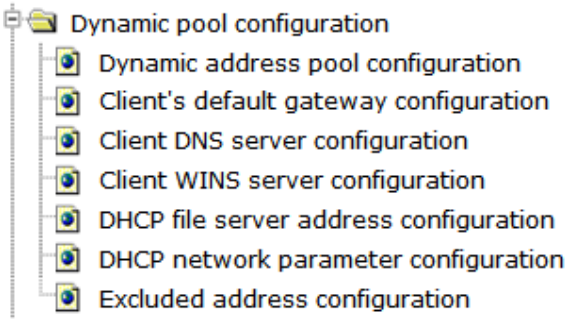
4.12.2 DHCP server configuration.

Choose **DHCP configuration > DHCP server configuration,** and the following page appears.There are "Dynamic pool configuration", "Manual DHCP IP pool configuration", "Address pool name configuration", "DHCP packet statistics", configuration web pages.



4.12.2.1 Dynamic pool configuration.

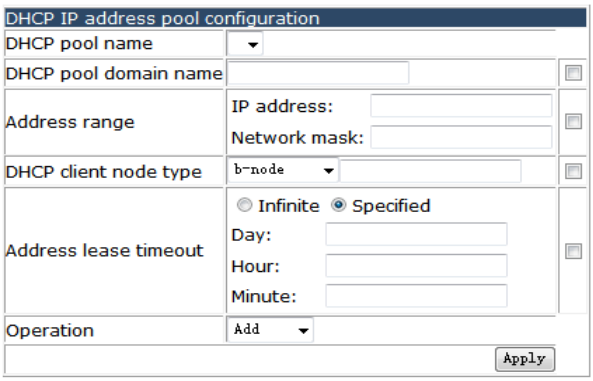
Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration,** and the following page appears.There are "Dynamic address pool configuration", "Client's default gateway configuration", "Client DNS server configuration", "Client WINS server configuration", "DHCP file server address configuration", "DHCP network parameter configuration", "Excluded address configuration", configuration web pages.



4.12.2.1.1 Dynamic address pool configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Dynamic address pool configuration,** and the following page appears.You can set a DHCP pool, the IP address and Network mask decide the address

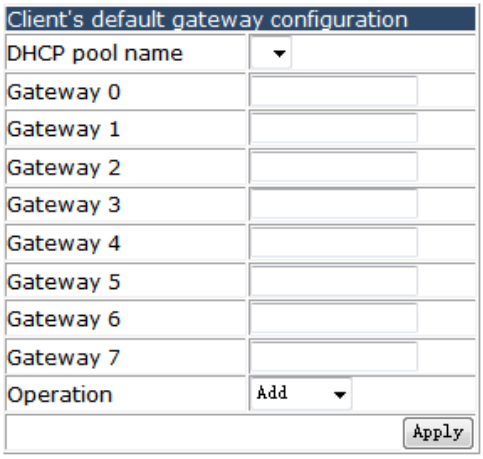
range, the node type include b-node, p-node, m-node and h-node, and you can set the lease time.



4.12.2.1.2 Client's default gateway configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Client's default gateway configuration,** and the following page appears.

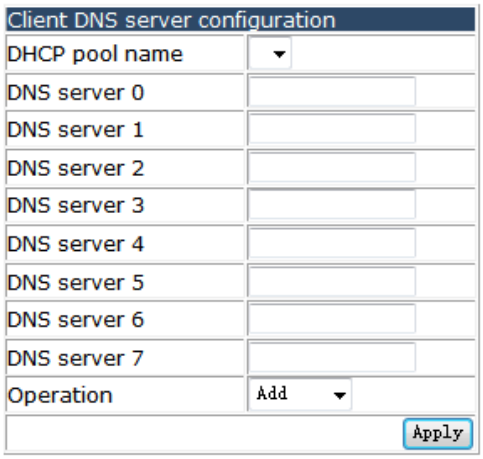
You can set the default gateway for DHCP clients.



4.12.2.1.3 Client DNS server configuration.

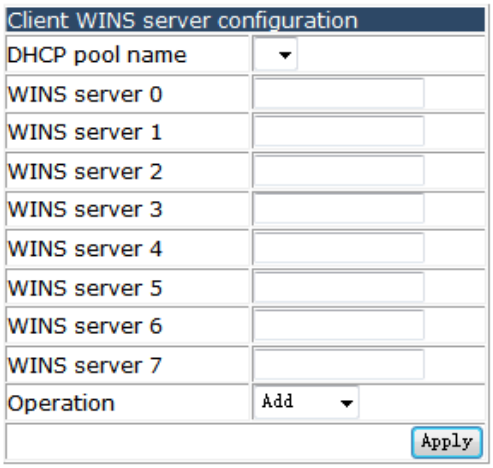
Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Client DNS server configuration,** and the following page appears.

You can set the DNS server address for DHCP client.



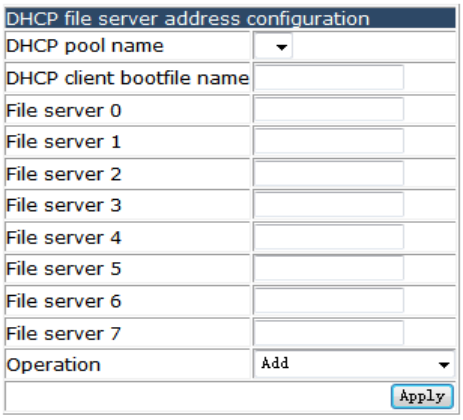
4.12.2.1.4 Client WINS server configuration.

Choose **DHCP configuration> DHCP server configuration > Dynamic pool configuration > Client WINS server configuration,** and the following page appears. You can set the WINS server for DHCP clients.



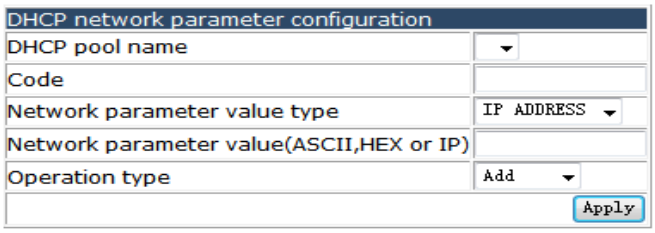
4.12.2.1.5 DHCP file server address configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > DHCP file server address configuration,** and the following page appears.You can set the bootfile name and the supplied server IP address.



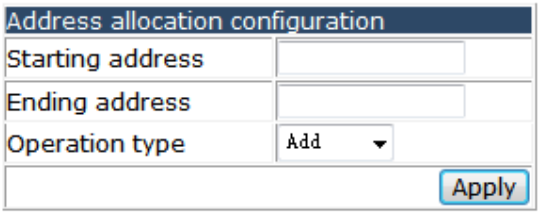
4.12.2.1.6 DHCP network parameter configuration.

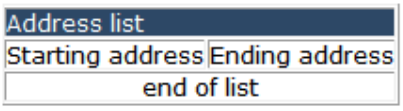
Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > DHCP network parameter configuration,** and the following page appears.You can add option parameters for DHCP pool to complete the advanced function for DHCP, if not necessary don't configure.



4.12.2.1.7 Excluded address configuration.

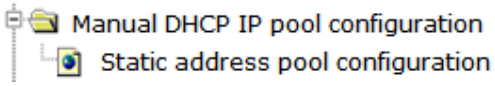
Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Excluded address configuration,** and the following page appears.You can set the excluded address for the DHCP pool address range.





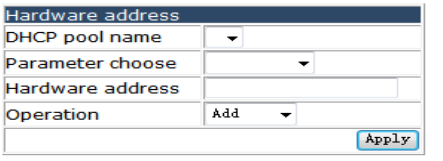
4.12.2.2 Manual DHCP IP pool configuration.

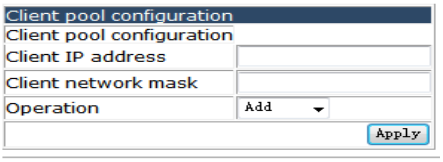
Choose **DHCP configuration > DHCP server configuration > Manual DHCP IP pool configuration,** and the following page appears.

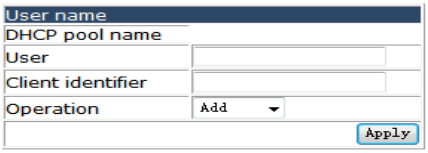


4.12.2.2.1 Static address pool configuration.

Choose **DHCP configuration > DHCP server configuration > Manual DHCP IP pool configuration > Static address pool configuration,** and the following page appears. You can set a hardware address with format rfc, ethernet or ieee802, and set a client IP address also, then the IP address will static to assign to the hardware address. And if you set a client IP address and client identifier, then the address will static to assign to the client with the identifier information.

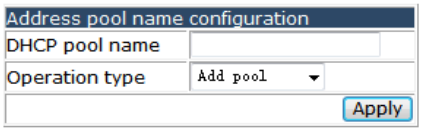


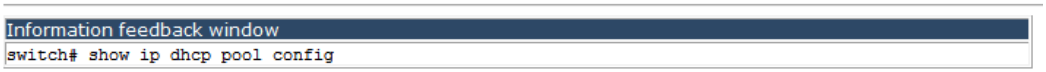




4.12.2.3 Address pool name configuration.

Choose **DHCP configuration > DHCP server configuration > Address pool name configuration,** and the following page appears.You can add a DHCP pool or remove a pool.





4.12.2.4 DHCP packet statistics.

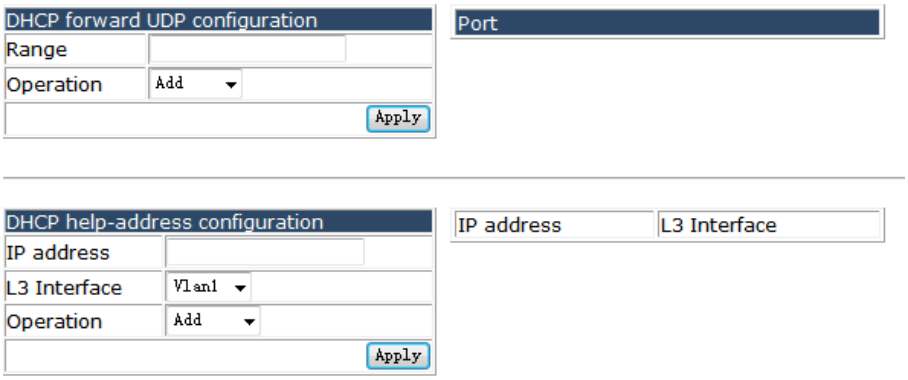
Choose **DHCP configuration > DHCP server configuration > DHCP packet statistics,** and the following page appears.You can show the statistics information for DHCP.

DHCP packet statistics	
Address pool number	0
Proxy database	0
Dynamical assignment address	0
Manual binded address	0
Address conflict	0
Binding exceeding lease time	0
Errors	0
Received DHCP packet statistics	
Received	0
DHCP DISCOVER	0
DHCP REQUEST	0
DHCP DECLINE	0
DHCP RELEASE	0
DHCP INFORM	0
Transmitted DHCP packet statistics	
Transmitted	0
DHCP OFFER	0
DHCP ACK	0
DHCP NAK	0
DHCP RELAY	0
DHCP FORWARD	0

Clear Show

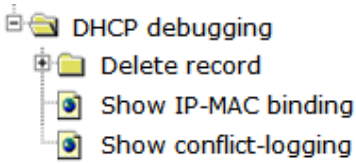
4.12.3 DHCP relay configuration.

Choose **DHCP configuration > DHCP relay configuration > DHCP relay configuration,** and the following page appears.You can set the DHCP forward range to 67 and set the DHCP server IP as the help-address.



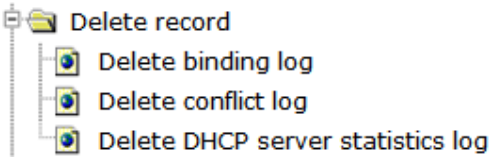
4.12.4 DHCP debugging.

Choose **DHCP configuration > DHCP debugging,** and the following page appears.There are "Delete record", "Show IP-MAC binding", "Show conflict-logging", configuration web pages.



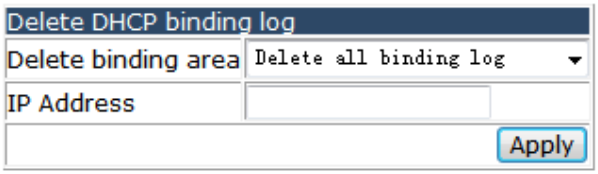
4.12.4.1 Delete record.

Choose **DHCP configuration > DHCP debugging > Delete record,** and the following page appears.There are "Delete binding log", "Delete conflict log", "Delete DHCP server statistics log", configuration web pages.



4.12.4.1.1 Delete binding log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete binding log,** and the following page appears.You can delete the record of one IP address binding with hardware address, or delete all binding table.

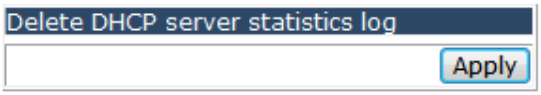


4.12.4.1.2 Delete conflict log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete conflict log,** and the following page appears.You can delete the conflict log of one IP address or delete all conflict log.

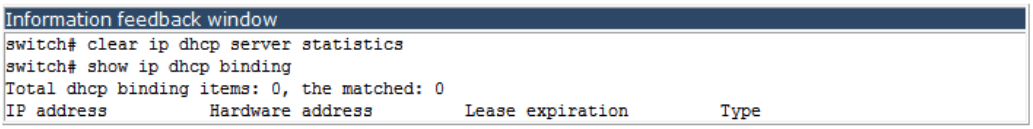
4.12.4.1.3 Delete DHCP server statistics log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete DHCP server statistics log,** and the following page appears.You can remove the DHCP server statistics logging.



4.12.4.2 Show IP-MAC binding.

Choose **DHCP configuration > DHCP debugging > Show IP-MAC binding,** and the following page appears.You can show the IP and hardware address binding information.

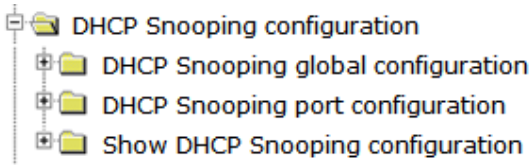


4.12.4.3 Show conflict-logging.

Choose **DHCP configuration > DHCP debugging > Show conflict-logging,** and the following page appears.You can show the DHCP conflict information.

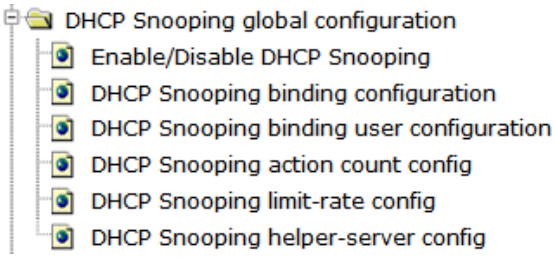
4.13 DHCP Snooping configuration.

Choose **DHCP Snooping configuration,** and the following page appears.There are "DHCP Snooping global configuration", "DHCP Snooping port configuration", "Show DHCP Snooping configuration", configuration web pages.



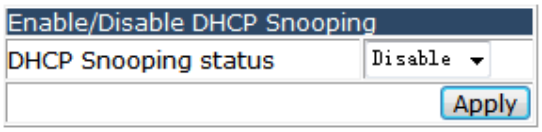
4.13.1 DHCP Snooping global configuration.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration,** and the following page appears.There are "Enable/Disable DHCP Snooping", "DHCP Snooping binding configuration", "DHCP Snooping binding user configuration", "DHCP Snooping action count config", "DHCP Snooping limit-rate config", "DHCP Snooping helper-server config", configuration web pages.



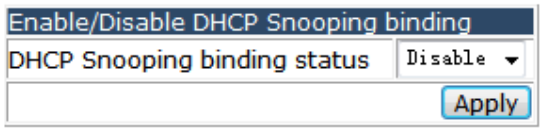
4.13.1.1 Enable/Disable DHCP Snooping.

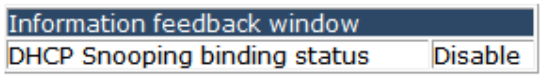
Choose **DHCP Snooping configuration > DHCP Snooping global configuration > Enable/Disable DHCP Snooping,** and the following page appears.You can enable or disable the DHCP Snooping function.



4.13.1.2 DHCP Snooping binding configuration.

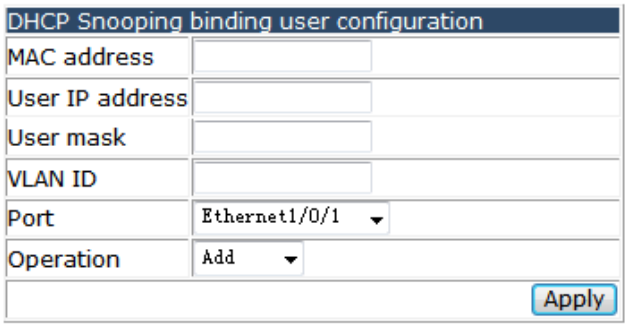
Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping binding configuration,** and the following page appears.You can enable or disable the DHCP Snooping binding function.





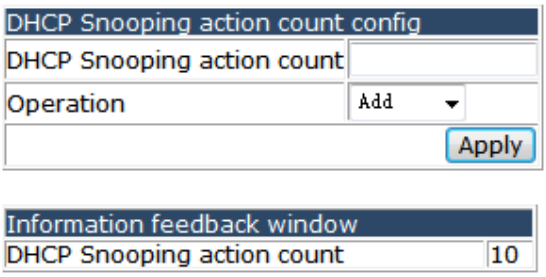
4.13.1.3 DHCP Snooping binding user configuration.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping binding user configuration,** and the following page appears.You can bind the MAC address, IP address, VLAN ID and port for a client.



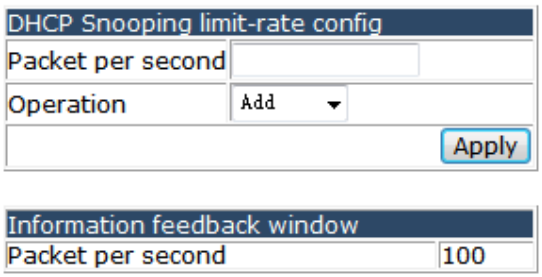
4.13.1.4 DHCP Snooping action count config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping action count config,** and the following page appears.You can set the count of the DHCP Snooping action.



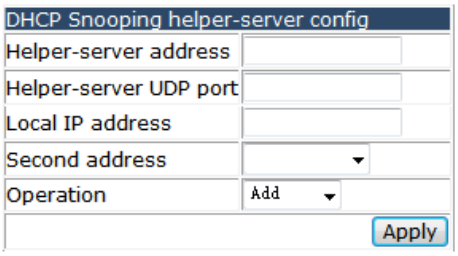
4.13.1.5 DHCP Snooping limit-rate config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping limit-rate config,** and the following page appears.You can set the count of the request and reply packets transmitting per second.



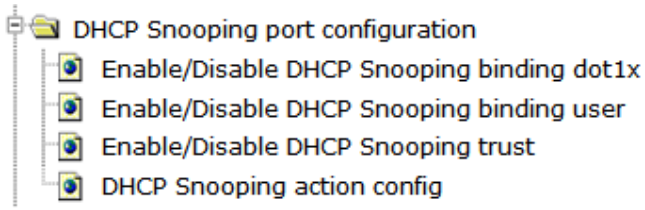
4.13.1.6 DHCP Snooping helper-server config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping helper-server config,** and the following page appears.You can set the helper-server address to save binding information detected by switch. The UDP port default is 9119, and local IP address should be the management IP of switch, you can choose the server as the primary or secondary server.



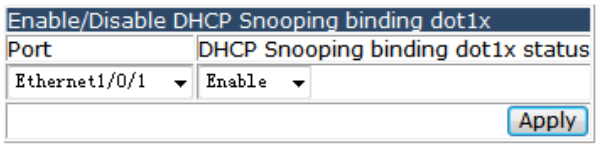
4.13.2 DHCP Snooping port configuration.

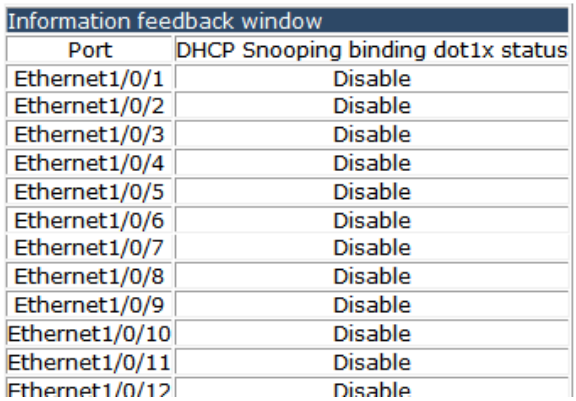
Choose **DHCP Snooping configuration,** and the following page appears.There are "Enable/Disable DHCP Snooping binding dot1x", "Enable/Disable DHCP Snooping binding user", "Enable/Disable DHCP Snooping trust", "DHCP Snooping action config", configuration web pages.



4.13.2.1 Enable/Disable DHCP Snooping binding dot1x.

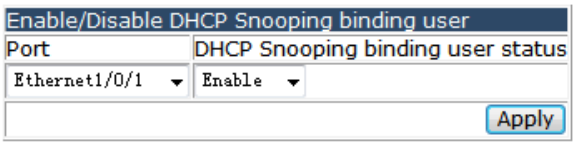
Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping binding dot1x,** and the following page appears.You can enable or disable DHCP Snooping binding dot1x function for each port.

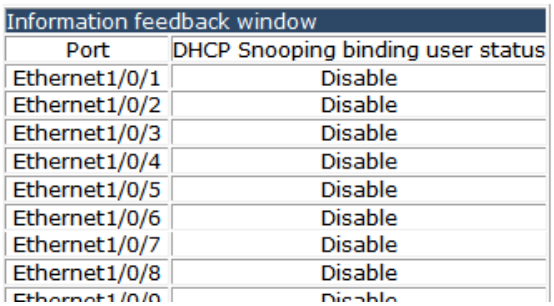




4.13.2.2 Enable/Disable DHCP Snooping binding user.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping binding user,** and the following page appears.You can enable or disable the DHCP Snooping binding user function for each port.



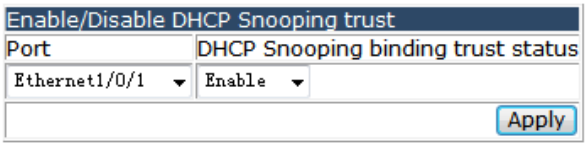


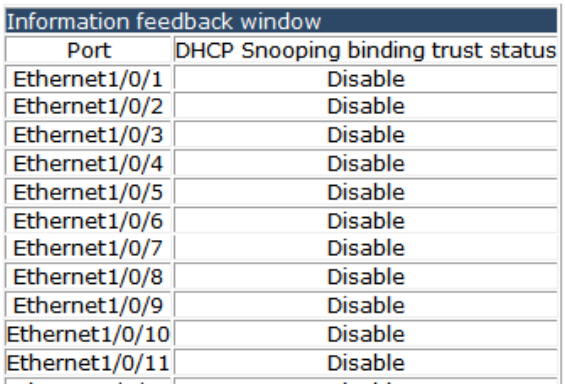
Information feedback window

Port	DHCP Snooping binding user status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

4.13.2.3 Enable/Disable DHCP Snooping trust.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping trust,** and the following page appears.You can enable or disable DHCP Snooping binding trust function for each port.



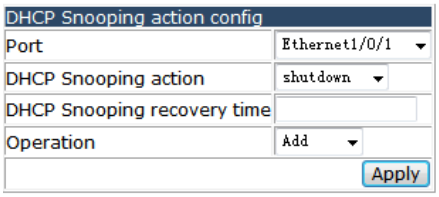


Information feedback window

Port	DHCP Snooping binding trust status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable

4.13.2.4 DHCP Snooping action config.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > DHCP Snooping action config,** and the following page appears.You can choose shutdown or blackhole the port while invalid DHCP packet detected, and the recover time.

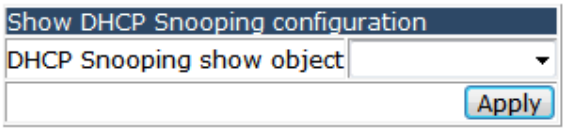


Information feedback window

Port	DHCP Snooping action	DHCP Snooping recovery time
Ethernet1/0/1	none	0
Ethernet1/0/2	none	0
Ethernet1/0/3	none	0
Ethernet1/0/4	none	0
Ethernet1/0/5	none	0
Ethernet1/0/6	none	0
Ethernet1/0/7	none	0
Ethernet1/0/8	none	0
Ethernet1/0/9	none	0
Ethernet1/0/10	none	0
Ethernet1/0/11	none	0

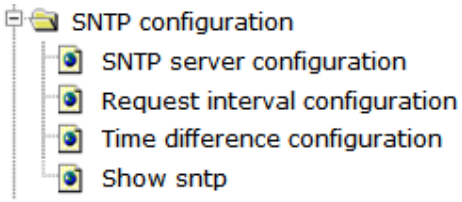
4.13.3 Show DHCP Snooping configuration.

Choose **DHCP Snooping configuration > Show DHCP Snooping configuration > Show DHCP Snooping configuration,** and the following page appears.You can show the DHCP Snooping information for one port or all ports.



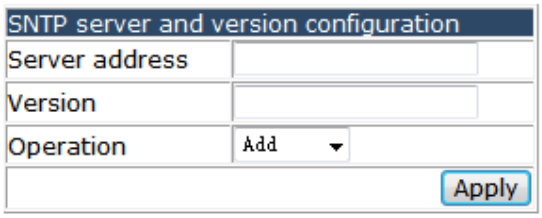
4.14 SNTP configuration.

Choose **SNTP configuration,** and the following page appears.There are "SNTP server configuration", "Request interval configuration", "Time difference configuration", "Show SNTP", configuration web pages.



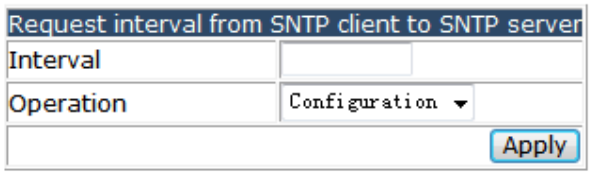
4.14.1 SNTP server configuration.

Choose **SNTP configuration > SNTP server configuration,** and the following page appears.You can set the SNTP server address and client version.



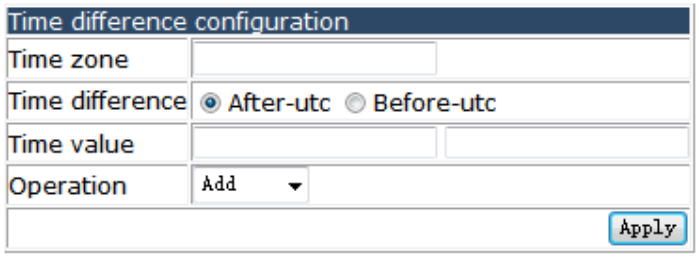
4.14.2 Request interval configuration.

Choose **SNTP configuration > Request interval configuration,** and the following page appears.You can set the time interval that the client send request.



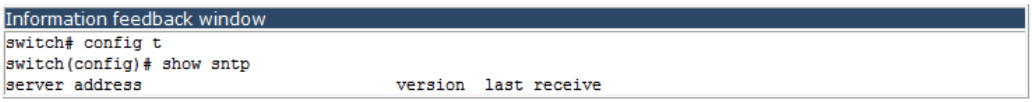
4.14.3 Time difference configuration.

Choose **SNTP configuration > Time difference configuration,** and the following page appears.You can set the Time zone, and add or subtract a value from the time obtain from server.



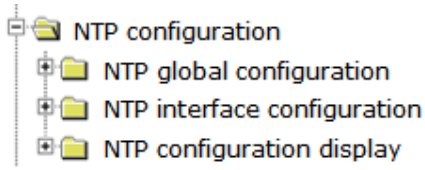
4.14.4 Show SNTP.

Choose **SNTP configuration > Show SNTP,** and the following page appears.You can show the detail information for SNIP.



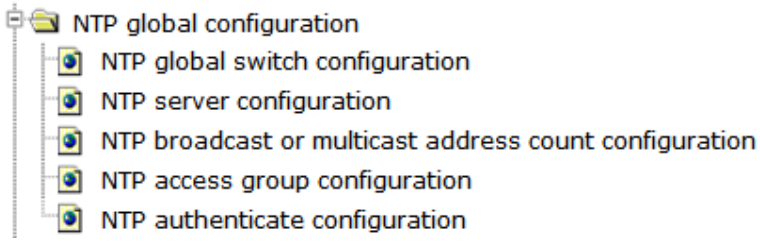
4.15 NTP configuration.

Choose **NTP configuration,** and the following page appears.There are "NTP global configuration", "NTP interface configuration", "NTP configuration", configuration web pages.



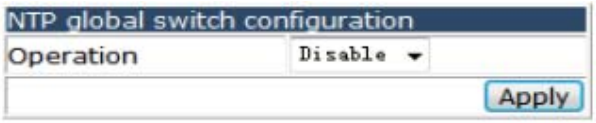
4.15.1 NTP global configuration.

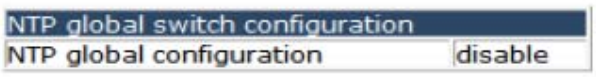
Choose **NTP configuration > NTP global configuration,** and the following page appears.There are "NTP global switch configuration", "NTP server configuration", "NTP broadcast or multicast address count configuration", "NTP access group configuration", "NTP authenticate configuration", configuration web pages.



4.15.1.1 NTP global switch configuration.

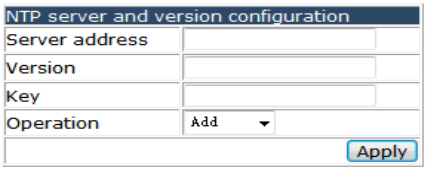
Choose **NTP configuration > NTP global configuration > NTP global switch configuration,** and the following page appears.You can enable or disable the NTP global switch function.





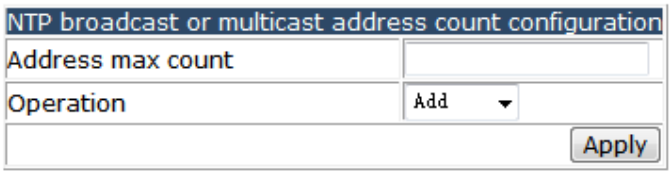
4.15.1.2 NTP server configuration.

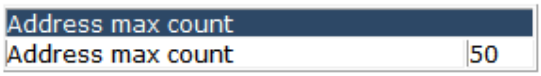
Choose **NTP configuration > NTP global configuration > NTP server configuration,** and the following page appears.You can set the NTP server address, version and key parameters.



4.15.1.3 NTP broadcast or multicast address count configuration.

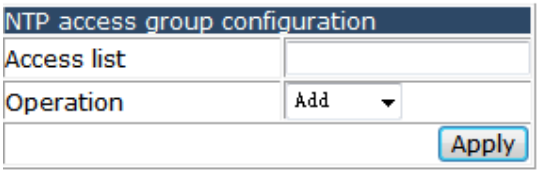
Choose **NTP configuration > NTP global configuration > NTP broadcast or multicast address count configuration,** and the following page appears, You can set the max count of the NTP broadcast or multicast address.





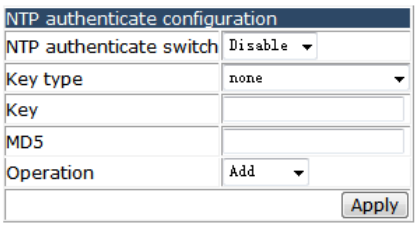
4.15.1.4 NTP access group configuration.

Choose **NTP configuration > NTP global configuration > NTP access group configuration,** and the following page appears.You can set a access list for NTP.



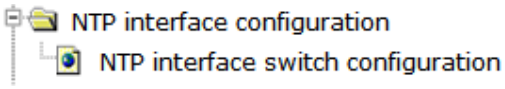
4.15.1.5 NTP authenticate configuration.

Choose **NTP configuration > NTP global configuration > NTP authenticate configuration,** and the following page appears.You can set authentication-key, trust-key or without key for NTP authenticate.



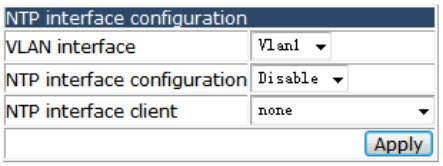
4.15.2 NTP interface configuration.

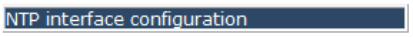
Choose **NTP configuration,** and the following page appears.There are "NTP interface switch configuration", configuration web pages.



4.15.2.1 NTP interface switch configuration.

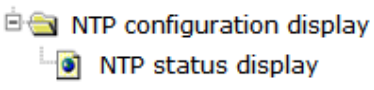
Choose **NTP configuration > NTP interface switch configuration,** and the following page appears.You can set the NTP FOR VLAN, the NTP interface client include none, broadcast, no broadcast, multicast, no multicast, IPv6 multicast, no NTP interface IPv6 multicast.





4.15.3 NTP configuration display.

Choose **NTP configuration,** and the following page appears.There are "NTP status display", configuration web pages.

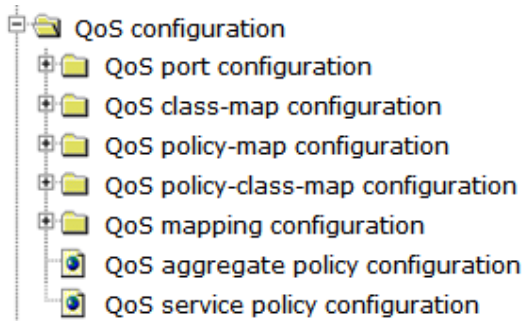


4.15.3.1 NTP status display.

Choose **NTP configuration > NTP status display,** and the following page appears.You can show the NTP status.

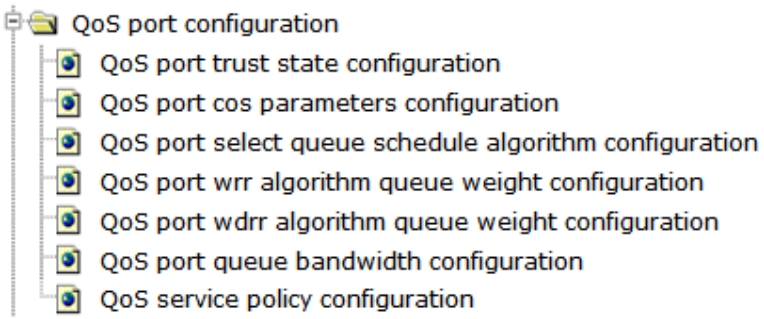
4.16 QoS configuration.

Choose **QoS configuration,** and the following page appears.There are "QoS port configuration", "QoS class-map configuration", "QoS policy-map configuration", "QoS policy-class-map configuration", "QoS mapping configuration", "QoS aggregate policy", "QoS service policy configuration", configuration web pages.



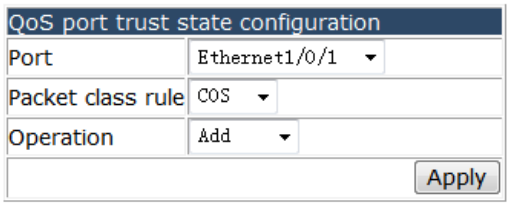
4.16.1 QoS port configuration.

Choose **QoS configuration > QoS port configuration,** and the following page appears.There are "QoS port trust state configuration", "QoS port cos parameters configuration", "QoS port select queue schedule algorithm configuration", "QoS port WRR algorithm queue weight configuration", "QoS port WDRR algorithm queue weight configuration", "QoS port queue bandwidth configuration", "QoS service policy configuration", configuration web pages.



4.16.1.1 QoS port trust state configuration.

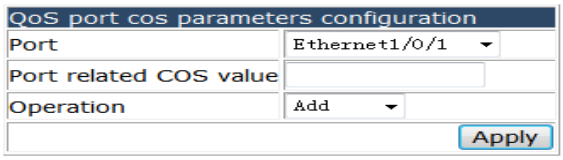
Choose **QoS configuration > QoS port configuration > QoS port trust state configuration,** and the following page appears.You can set the QOS trust packet class to cos or dscp for each port.



Information feedback window	
Port	Trust class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS
Ethernet1/0/5	COS
Ethernet1/0/6	COS
Ethernet1/0/7	COS
Ethernet1/0/8	COS
Ethernet1/0/9	COS
Ethernet1/0/10	COS
Ethernet1/0/11	COS
Ethernet1/0/12	COS

4.16.1.2 QoS port cos parameters configuration.

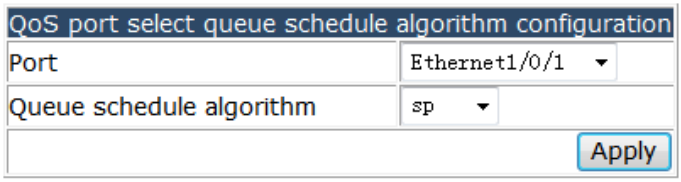
Choose **QoS configuration > QoS port configuration > QoS port COS parameters configuration,** and the following page appears.You can set the default COS value for each port.



Information feedback window	
Port	Port related COS value
Ethernet1/0/1	0
Ethernet1/0/2	0
Ethernet1/0/3	0
Ethernet1/0/4	0
Ethernet1/0/5	0
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0
Ethernet1/0/9	0
Ethernet1/0/10	0
Ethernet1/0/11	0
Ethernet1/0/12	0

4.16.1.3 QoS port select queue schedule algorithm configuration.

Choose **QoS configuration > QoS port configuration > QoS port select queue schedule algorithm configuration,** and the following page appears.You can set the QoS queue schedule algorithm to sp, wrr or wdrr mode.



Information feedback window	
Port	Trust class
Ethernet1/0/1	wrr
Ethernet1/0/2	wrr
Ethernet1/0/3	wrr
Ethernet1/0/4	wrr
Ethernet1/0/5	wrr
Ethernet1/0/6	wrr
Ethernet1/0/7	wrr
Ethernet1/0/8	wrr
Ethernet1/0/9	wrr
Ethernet1/0/10	wrr
Ethernet1/0/11	wrr
Ethernet1/0/12	wrr
Ethernet1/0/13	wrr
Ethernet1/0/14	wrr
Ethernet1/0/15	wrr

4.16.1.4 QoS port WRR algorithm queue weight configuration.

Choose **QoS configuration > QoS port configuration > QoS port WRR algorithm queue weight configuration,** and the following page appears.You can set the WRR queue Weight value for each port.

QoS port wrr algorithm queue weight configuration	
Port	Ethernet1/0/1
Weight1	
Weight2	
Weight3	
Weight4	
Weight5	
Weight6	
Weight7	
Weight8	
Operation	Add
	Apply

Information feedback window	
Port	Queue weight
Ethernet1/0/1	1 2 3 4 5 6 7 8
Ethernet1/0/2	1 2 3 4 5 6 7 8
Ethernet1/0/3	1 2 3 4 5 6 7 8
Ethernet1/0/4	1 2 3 4 5 6 7 8
Ethernet1/0/5	1 2 3 4 5 6 7 8
Ethernet1/0/6	1 2 3 4 5 6 7 8
Ethernet1/0/7	1 2 3 4 5 6 7 8

4.16.1.5 QoS port WDRR algorithm queue weight configuration.

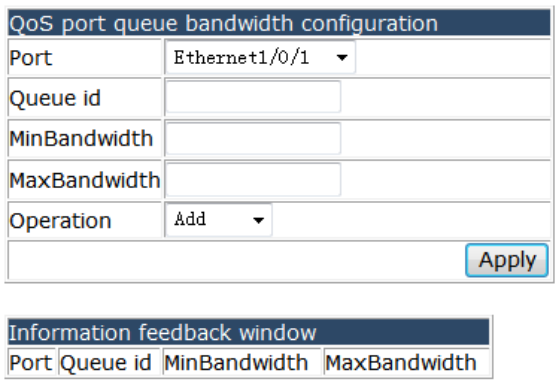
Choose **QoS configuration > QoS port configuration > QoS port WDRR algorithm queue weight configuration,** and the following page appears.You can set the WDRR queue Weight value for each port.

QoS port wdrr algorithm queue weight configuration	
Port	Ethernet1/0/1
Weight1	
Weight2	
Weight3	
Weight4	
Weight5	
Weight6	
Weight7	
Weight8	
Operation	Add
	Apply

Information feedback window	
Port	Queue weight
Ethernet1/0/1	16 32 64 128 256 512 1024 1024
Ethernet1/0/2	16 32 64 128 256 512 1024 1024
Ethernet1/0/3	16 32 64 128 256 512 1024 1024
Ethernet1/0/4	16 32 64 128 256 512 1024 1024
Ethernet1/0/5	16 32 64 128 256 512 1024 1024
Ethernet1/0/6	16 32 64 128 256 512 1024 1024
Ethernet1/0/7	16 32 64 128 256 512 1024 1024
Ethernet1/0/8	16 32 64 128 256 512 1024 1024
Ethernet1/0/9	16 32 64 128 256 512 1024 1024
Ethernet1/0/10	16 32 64 128 256 512 1024 1024

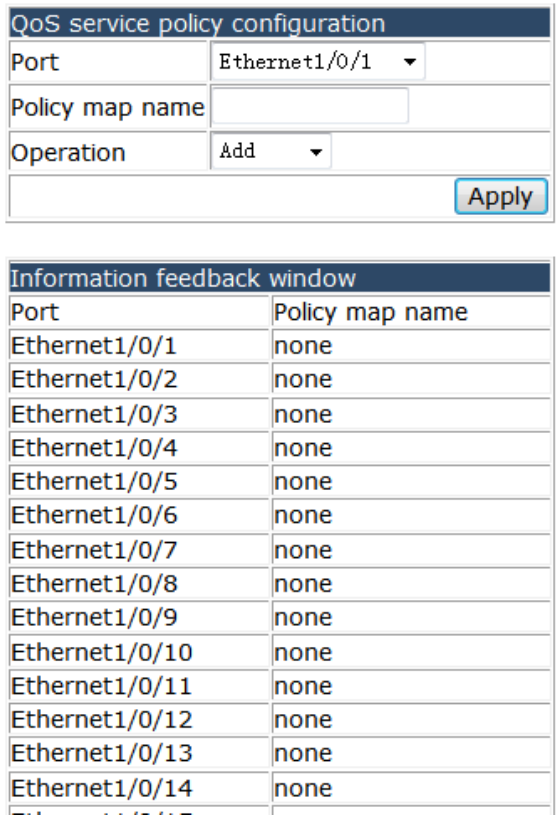
4.16.1.6 QoS port queue bandwidth configuration.

Choose **QoS configuration > QoS port configuration > QoS port queue bandwidth configuration,** and the following page appears.You can set the MinBandwidth and MaxBandwidth value for different Queue of each port.



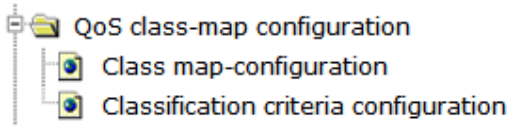
4.16.1.7 QoS service policy configuration.

Choose **QoS configuration > QoS port configuration > QoS service policy configuration,** and the following page appears.You can mapping a policy-map to a physical port, the policy map setting refer to QoS policy-map configuration.



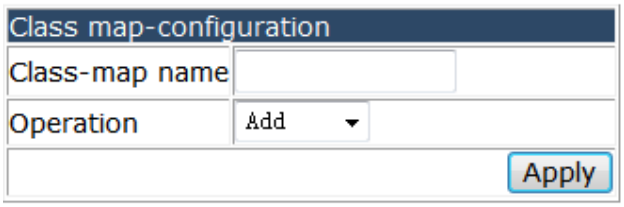
4.16.2 QoS class-map configuration.

Choose **QoS configuration > QoS class-map configuration,** and the following page appears.There are "Class map-configuration", "Classification criteria configuration", configuration web pages.



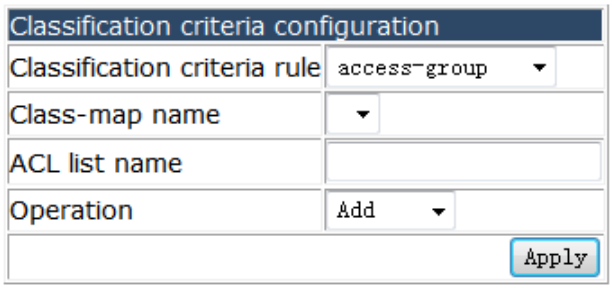
4.16.2.1 Class map-configuration.

Choose **QoS configuration > QoS class-map configuration > Class map-configuration,** and the following page appears.You can add a Class-map rule.



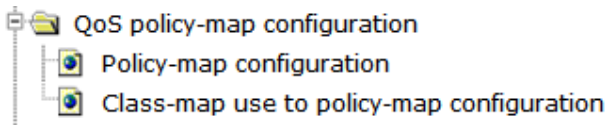
4.16.2.2 Classification criteria configuration.

Choose **QoS configuration > QoS class-map configuration > Classification criteria configuration,** and the following page appears.You can set the matching criteria for the class-map table.The classification criteria rule include access-group, IP-dscp, IP Precedence, Vlan, COS, C-Vlan, IPv6-dscp, IPv6-flowlable.



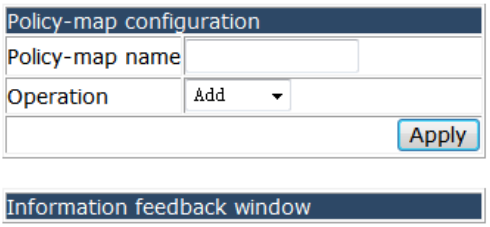
4.16.3 QoS policy-map configuration.

Choose **QoS configuration > QoS policy-map configuration,** and the following page appears.There are "Policy map-configuration", "Class-map use to policy-map configuration", configuration web pages.



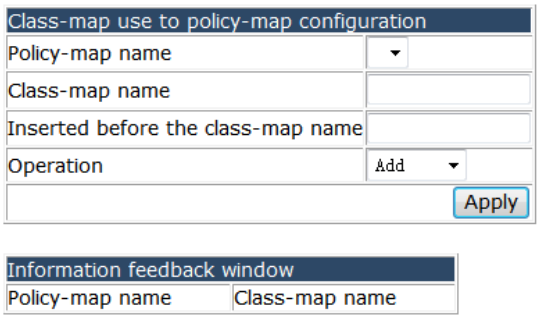
4.16.3.1 Policy-map configuration.

Choose **QoS configuration > QoS policy-map configuration > Policy-map configuration,** and the following page appears.You can add a Policy-map rule.



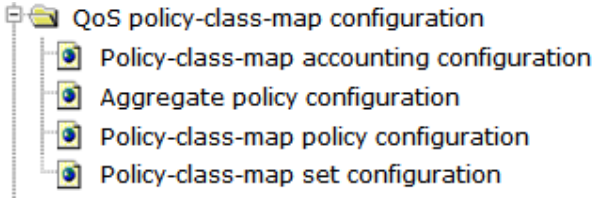
4.16.3.2 Class-map use to policy-map configuration.

Choose **QoS configuration > QoS policy-map configuration > Class-map use to policy-map configuration,** and the following page appears.You can configure the class-map use to policy-map.



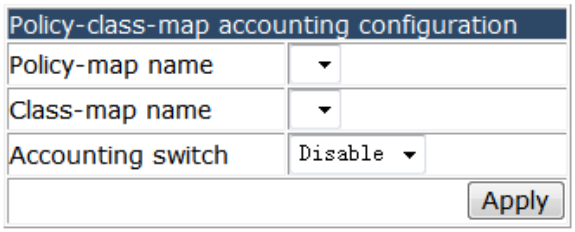
4.16.4 QoS policy-class-map configuration.

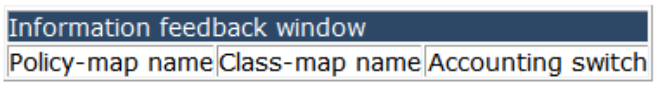
Choose **QoS configuration > QoS policy-class-map configuration,** and the following page appears.There are "Policy-class-map accounting configuration", "Aggregate policy configuration", "Policy-class-map policy configuration", "Policy-class-map set configuration", configuration web pages.



4.16.4.1 Policy-class-map accounting configuration.

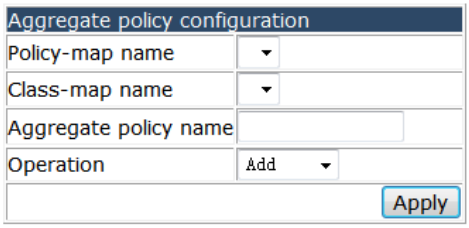
Choose **QoS configuration > QoS policy-class-map configuration > Policy-class-map accounting configuration,** and the following page appears.You can enable or disable the policy-class-map.

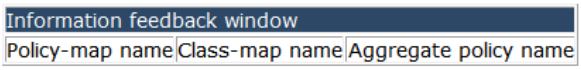




4.16.4.2 Aggregate policy configuration.

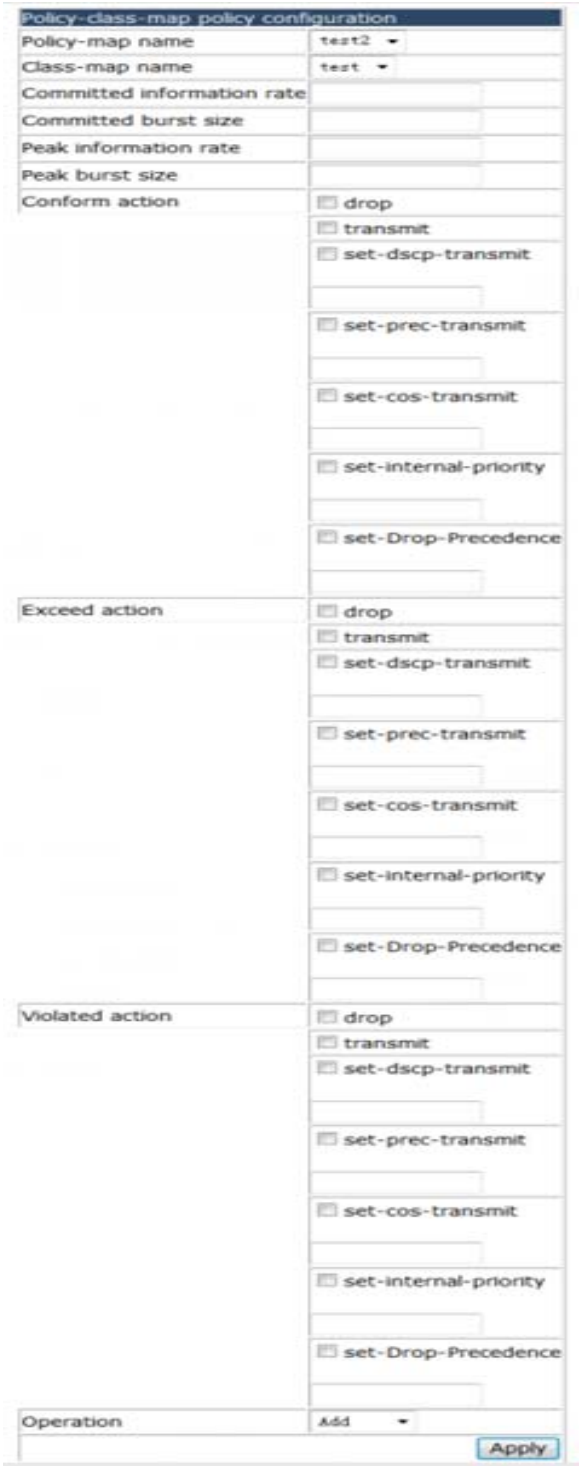
Choose **QoS configuration > QoS policy-class-map configuration > Aggregate policy configuration,** and the following page appears.You can set the Aggregate policy.





4.16.4.3 Policy-class-map policy configuration.

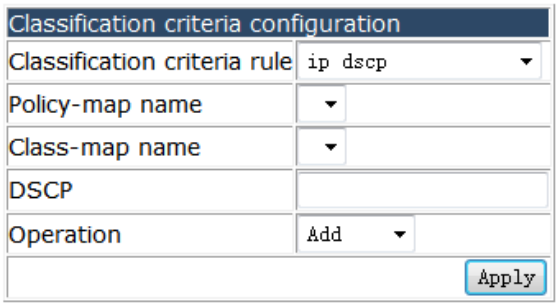
Choose **QoS configuration > QoS policy-class-map configuration > Policy-class-map policy configuration,** and the following page appears.You can set the policy-class-map policy.



4.16.4.4 Policy-class-map set configuration.

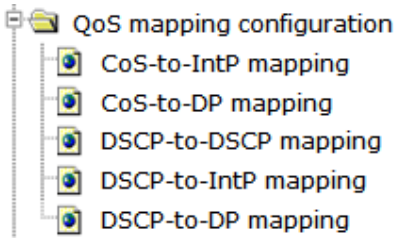
Choose **QoS configuration > QoS policy-class-map configuration >**

Policy-class-map set configuration, and the following page appears.You can set new classification criteria rule for classified traffic. The rule include IP DSCP, IP precedence, DROP precedence, Internal Priority, COS, C-vid, S-vid.



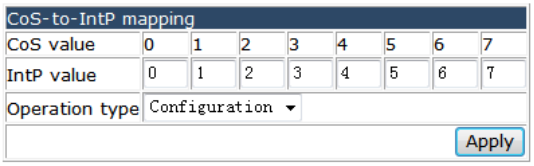
4.16.5 QoS mapping configuration.

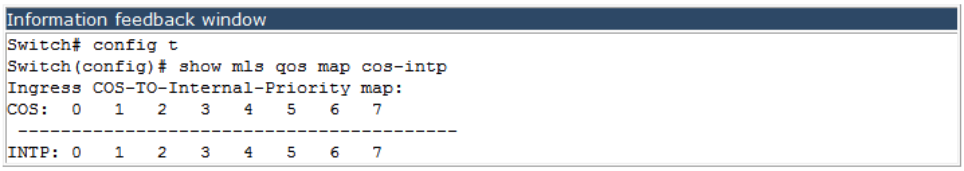
Choose **QoS configuration > QoS mapping configuration,** and the following page appears.There are "COS-to-IntP mapping", "COS-to-DP mapping", "DSCP-to-DSCP mapping", "DSCP-to-IntP mapping", "DSCP-to-DP mapping", configuration web pages.



4.16.5.1 COS-to-IntP mapping.

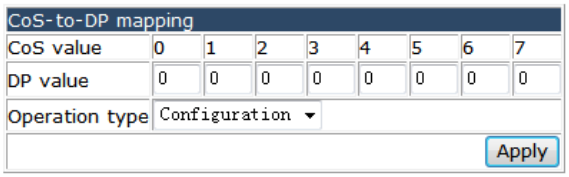
Choose **QoS configuration > QoS mapping configuration > COS-to-IntP mapping,** and the following page appears.You can set the mapping COS-to-IntP.





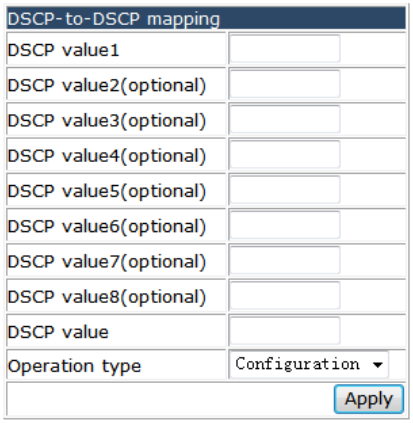
4.16.5.2 COS-to-IntP mapping.

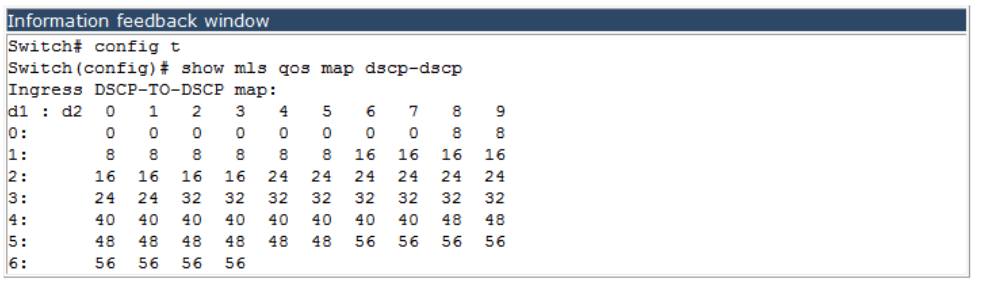
Choose **QoS configuration > QoS mapping configuration > COS-to-DP mapping,** and the following page appears.You can set the mapping COS-to-DP.



4.16.5.3 DSCP-to-DSCP mapping.

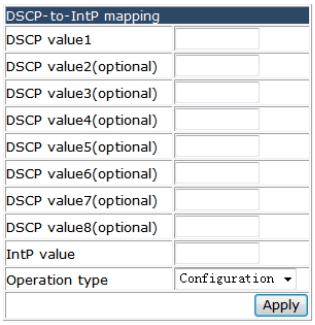
Choose **QoS configuration > QoS mapping configuration > DSCP-to-DSCP mapping,** and the following page appears.You can set the mapping DSCP-to-DSCP.

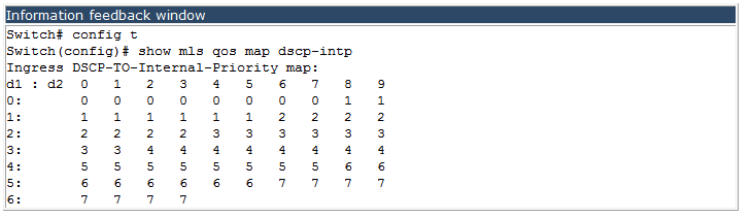




4.16.5.4 DSCP-to-IntP mapping.

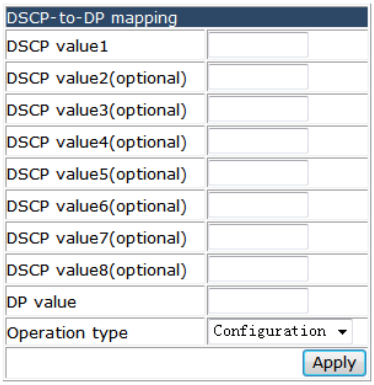
Choose **QoS configuration > QoS mapping configuration > DSCP-to-IntP mapping,** and the following page appears.You can set the mapping DSCP-to-IntP.

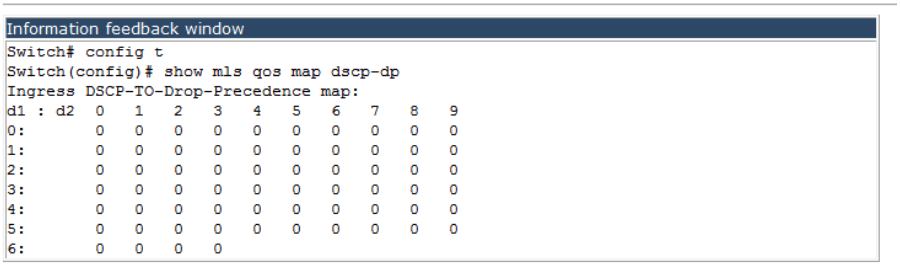




4.16.5.5 DSCP-to-DP mapping.

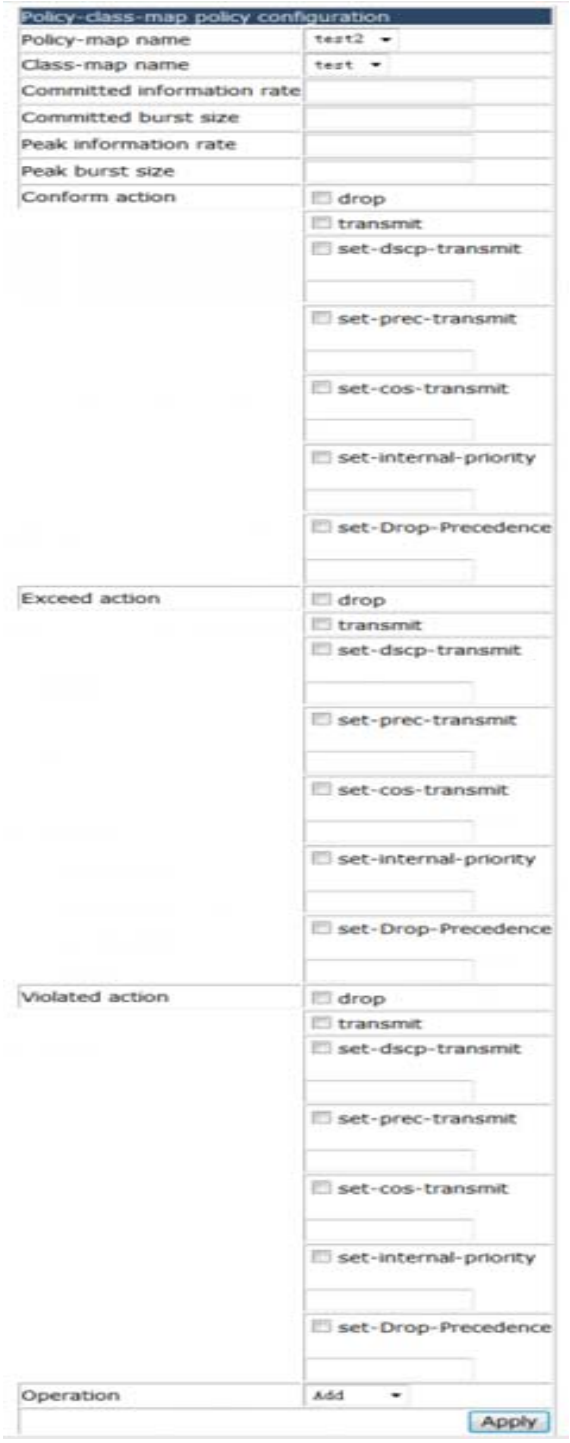
Choose **QoS configuration > QoS mapping configuration > DSCP-to-DP mapping,** and the following page appears.You can set the mapping DSCP-to-DP.





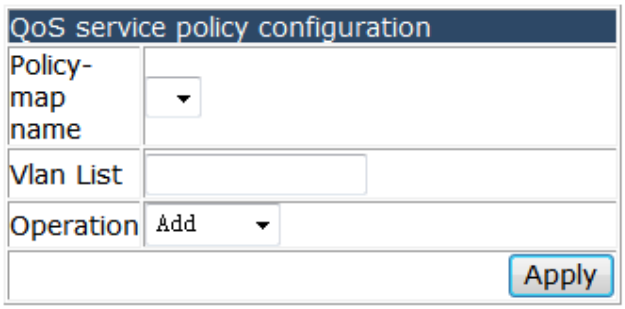
4.16.6 QoS aggregate policy configuration.

Choose **QoS configuration > QoS aggregate policy,** and the following page appears. You can set QoS-aggregate-policy strategy.You can set the QoS aggregate policy.



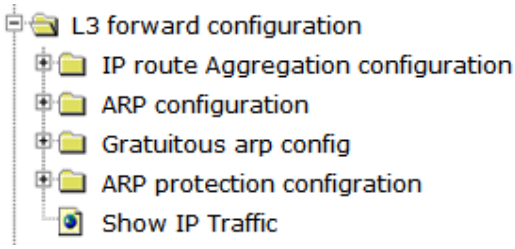
4.16.7 QoS service policy configuration.

Choose **QoS configuration > QoS service policy configuration,** and the following page appears.You can apply the policy-map to a VLAN.



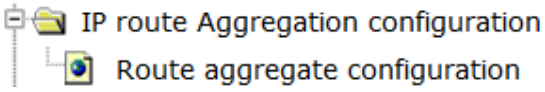
4.17 L3 forward configuration.

Choose **L3 forward configuration,** and the following page appears.There are "IP route Aggregation configuration", "ARP configuration", "Gratuitous ARP config", "ARP protection configuration", "Show IP Traffic", configuration web pages.



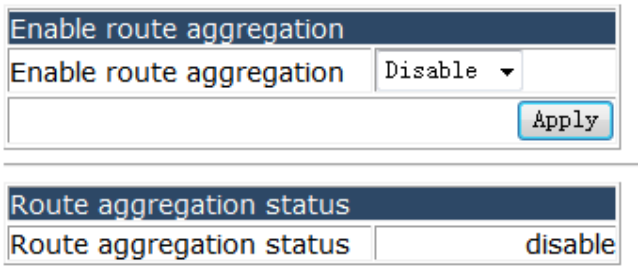
4.17.1 IP route Aggregation configuration.

Choose **L3 forward configuration > IP route Aggregation configuration,** and the following page appears.There are "Route aggregate configuration", configuration web pages.



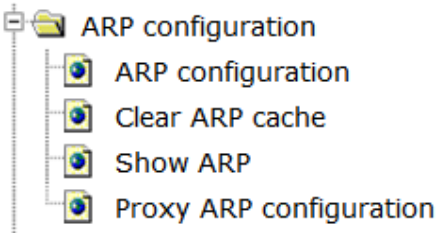
4.17.1.1 Route aggregate configuration.

Choose **L3 forward configuration > IP route Aggregation configuration > Route aggregate configuration,** and the following page appears.You can enable or disable the route aggregation function.



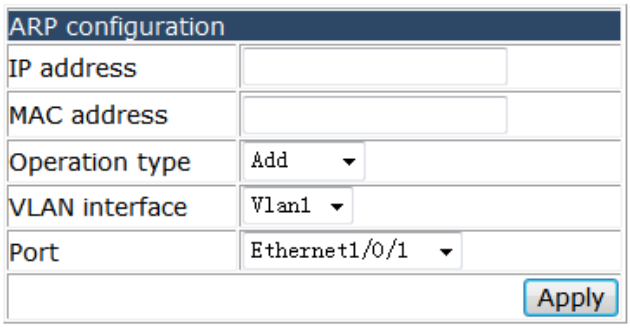
4.17.2 ARP configuration.

Choose **L3 forward configuration > ARP configuration,** and the following page appears.There are "ARP configuration", "Clear ARP cache", "Show ARP", "Proxy ARP configuration", configuration web pages.



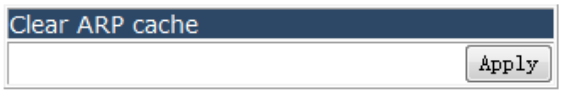
4.17.2.1 ARP configuration.

Choose **L3 forward configuration > ARP configuration > ARP configuration,** and the following page appears.You can add IP, MAC, VLAN and port binding rules.



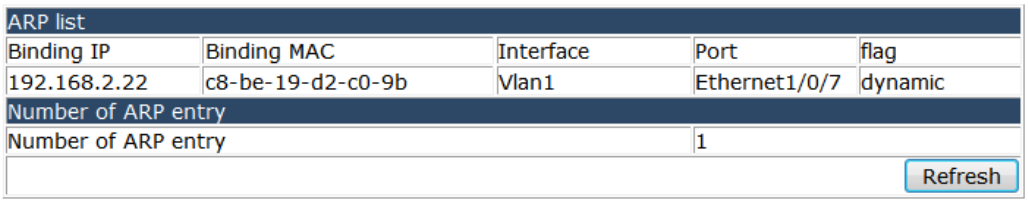
4.17.2.2 Clear ARP cache.

Choose **L3 forward configuration > ARP configuration > Clear ARP cache,** and the following page appears.You can clear the ARP cache table.



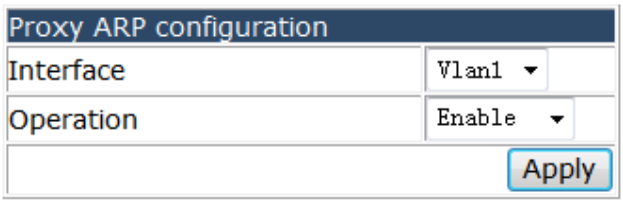
4.17.2.3 Show ARP.

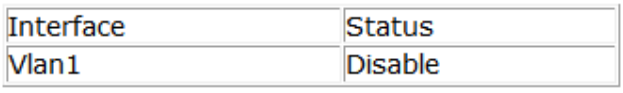
Choose **L3 forward configuration > ARP configuration > Show ARP,** and the following page appears.You can show the ARP list.



4.17.2.4 Proxy ARP configuration.

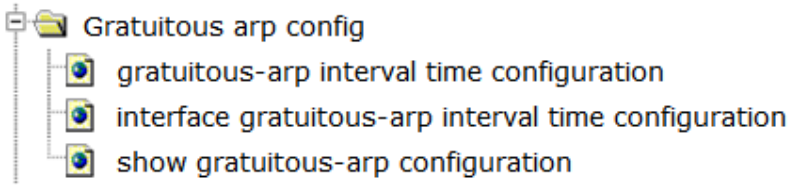
Choose **L3 forward configuration > ARP configuration > Proxy ARP configuration,** and the following page appears.You can enable or disable the ARP proxy function for each VLAN.





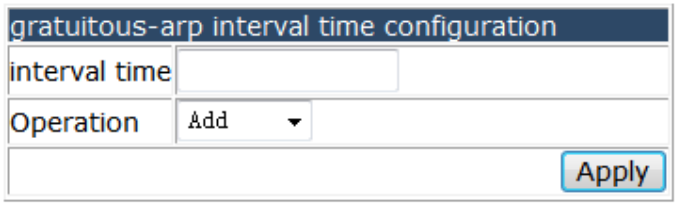
4.17.3 Gratuitous ARP config.

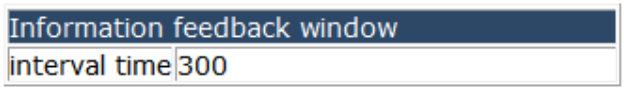
Choose **L3 forward configuration > Gratuitous ARP config,** and the following page appears.There are "Gratuitous-ARP interval time configuration", "Interface Gratuitous-ARP interval time configuration", "Show Gratuitous-ARP configuration", configuration web pages.



4.17.3.1 Gratuitous-ARP interval time configuration.

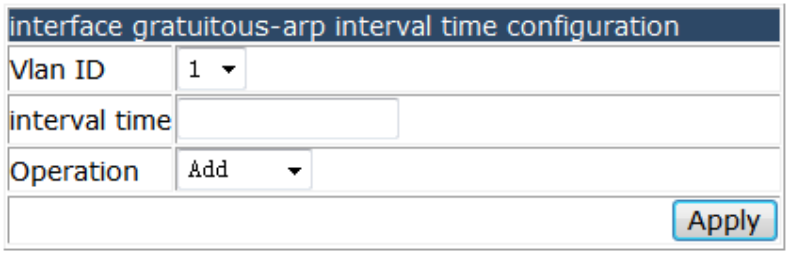
Choose **L3 forward configuration > Gratuitous ARP config > Gratuitous-ARP interval time configuration,** and the following page appears.You can set up the Gratuitous-ARP interval time.





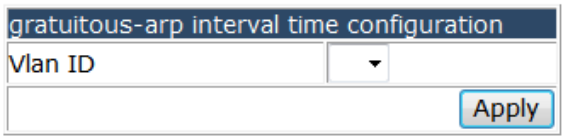
4.17.3.2 Interface Gratuitous-ARP interval time configuration.

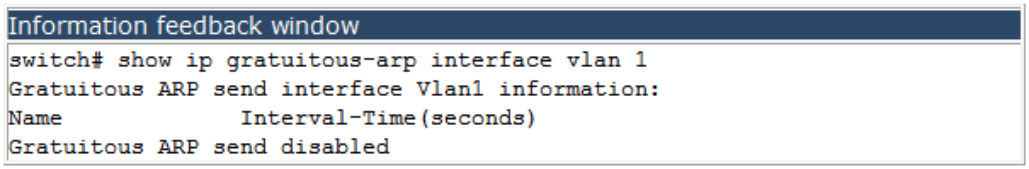
Choose **L3 forward configuration > Gratuitous ARP config > Interface Gratuitous-ARP interval time configuration,** and the following page appears.You can set the gratuitous-arp interval time for each VLAN.



4.17.3.3 Show Gratuitous-ARP configuration.

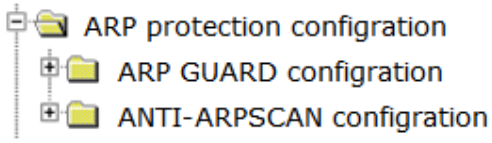
Choose **L3 forward configuration > Gratuitous ARP config > Show Gratuitous-ARP configuration,** and the following page appears.You can show the gratuitous-arp information for each VLAN.





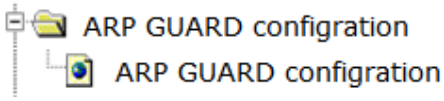
4.17.4 ARP protection configuration.

Choose **L3 forward configuration > ARP protection configuration,** and the following page appears.There are "ARP GUARD configuration", "ANTI-ARPSCAN configuration", configuration web pages.



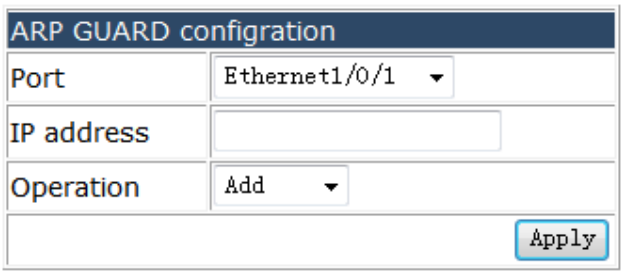
4.17.4.1 ARP protection configuration.

Choose **L3 forward configuration > ARP protection configuration > ARP protection configuration,** and the following page appears.There are "ARP GUARD configuration", configuration web pages.



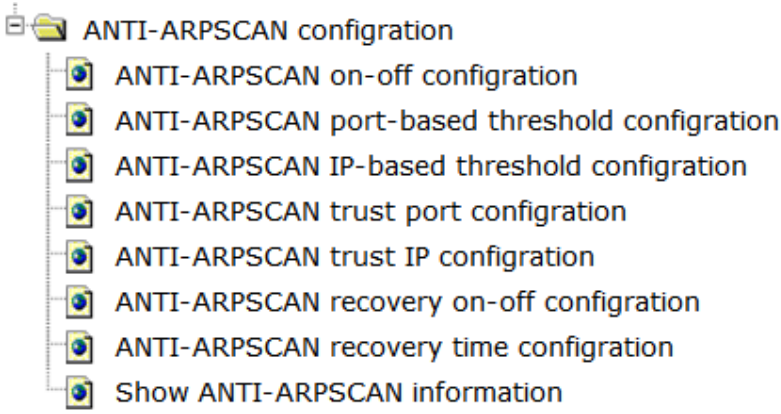
4.17.4.1.1 ARP GUARD configuration.

Choose **L3 forward configuration > ARP protection configuration > ARP protection configuration > ARP protection configuration,** and the following page appears.You can configure the arp guard IP address for each port.



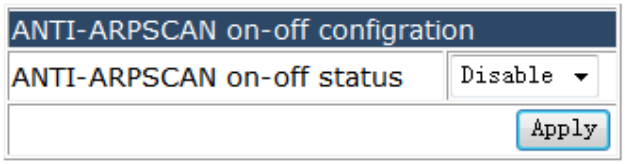
4.17.4.2 ANTI-ARPSCAN configuration.

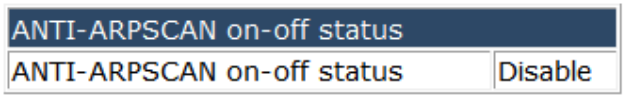
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration,** and the following page appears.There are "ANTI-ARPSCAN on-off configuration", "ANTI-ARPSCAN port-based threshold configuration", "ANTI-ARPSCAN IP-based threshold", "ANTI-ARPSCAN trust port configuration", "ANTI-ARPSCAN trust IP configuration", "ANTI-ARPSCAN recovery on-off configuration", "ANTI-ARPSCAN recovery time configuration", "Show ANTI-ARPSCAN information", configuration web pages.



4.17.4.2.1 ANTI-ARPSCAN on-off configuration.

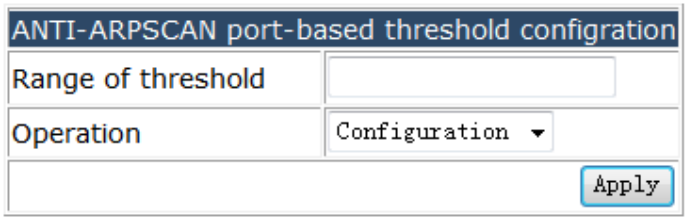
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN on-off configuration,** and the following page appears. You can enable or disable ANTI-ARPSCAN.

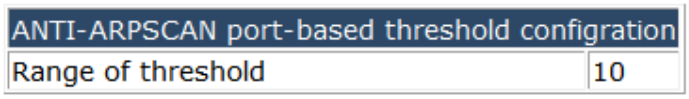




4.17.4.2.2 ANTI-ARPSCAN port-based threshold configuration.

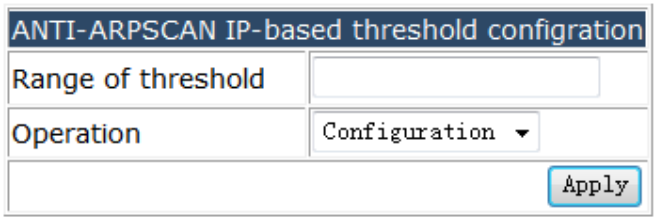
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN port-based threshold configuration,** and the following page appears.You can set the threshold value of receiving ARP message for the port-base anti-arpscan function.

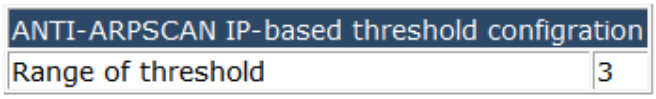




4.17.4.2.3 ANTI-ARPSCAN IP-based threshold.

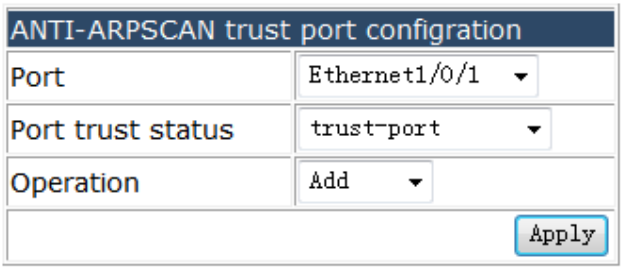
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN IP-based threshold,** and the following page appears. You can set the threshold value of receiving ARP message for the IP-base anti-arpscan function.





4.17.4.2.4 ANTI-ARPSCAN trust port configuration.

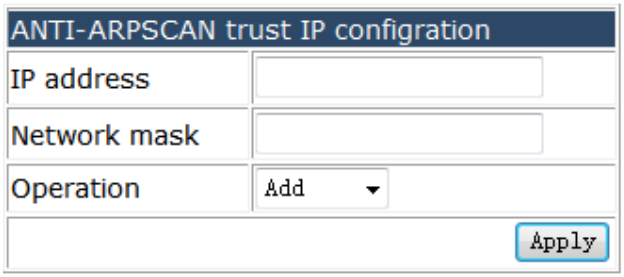
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN trust port configuration,** and the following page appears.You can set the trust-port or supertrust-port for anti-arpscan function.



4.17.4.2.5 ANTI-ARPSCAN trust IP configuration.

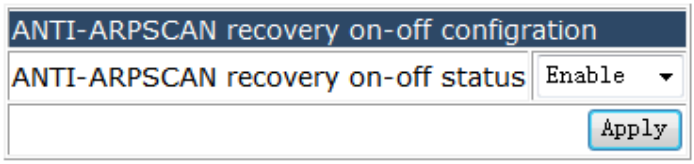
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN**

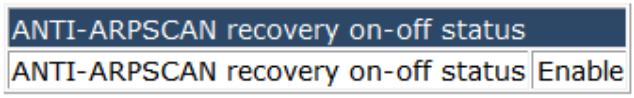
configuration > ANTI-ARPSCAN trust IP configuration, and the following page appears.You can set the trust IP for anti-arpscan function.



4.17.4.2.6 ANTI-ARPSCAN recovery on-off configuration.

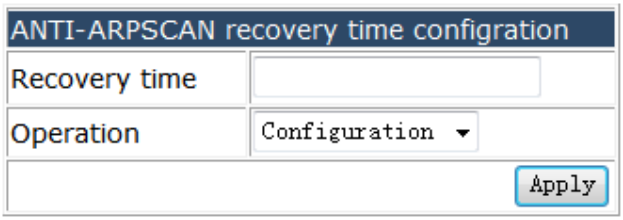
Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN recovery on-off configuration,** and the following page appears.You can enable or disable the recovery function for anti-arpscan.





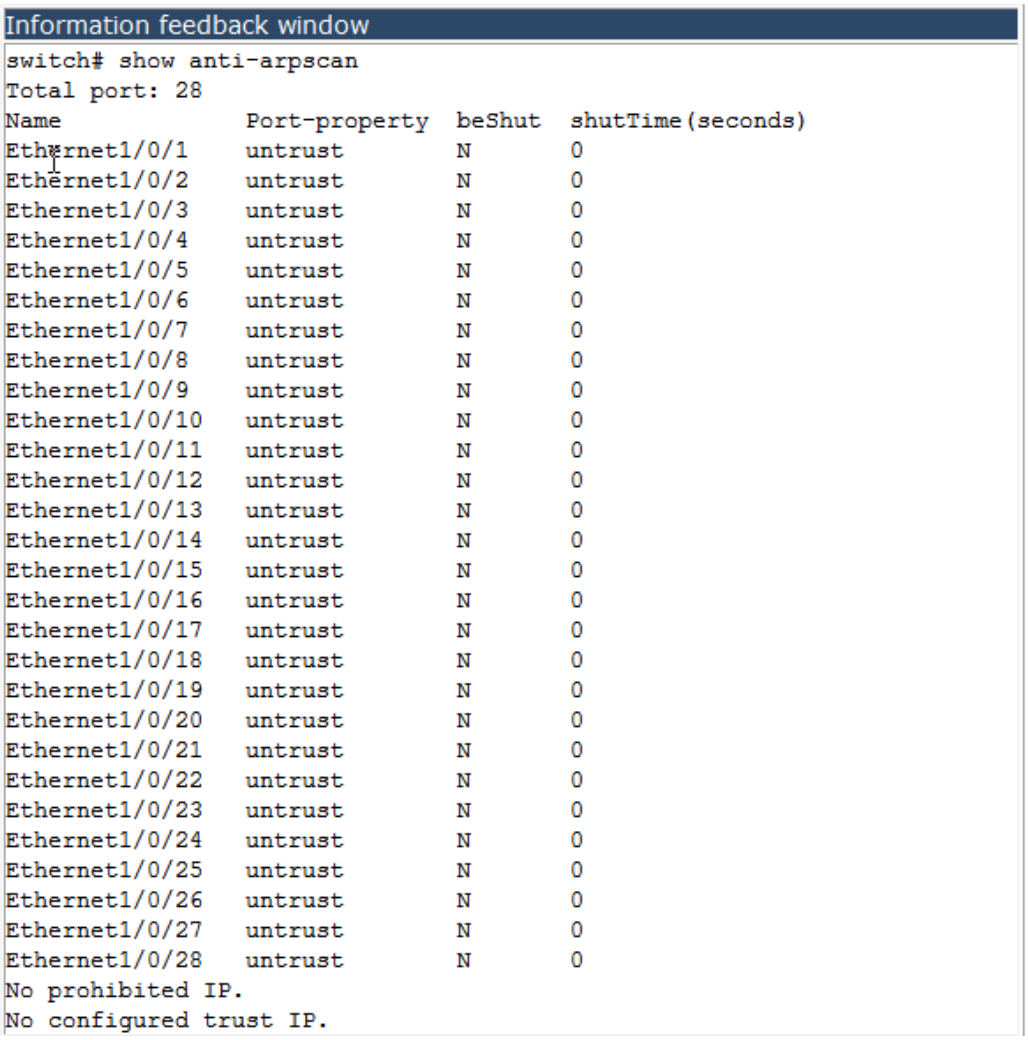
4.17.4.2.7 ANTI-ARPSCAN recovery time configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN recovery time configuration,** and the following page appears.You can set ANTI-ARPSCAN recovery time.



4.17.4.2.8 Show ANTI-ARPSCAN information.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > Show ANTI-ARPSCAN information,** and the following page appears. You can show the detail information of the anti-arpscan function.



4.17.5 Show IP Traffic.

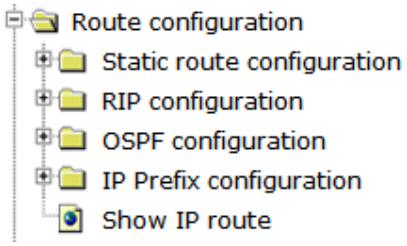
Choose **L3 forward configuration,** and the following page appears.You can show the statistics for different traffic protocol.

Information feedback window

```
switch# show ip traffic
IP statistics:
  Rcvd:  98575 total, 99466 local destination
         0 header errors, 0 address errors
         0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:  128480 generated, 0 forwarded
         2 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
  Sent:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens          83, TcpAttemptFails           0
  TcpCurrEstab             3, TcpEstabResets          131
  TcpInErrs                0, TcpInSegs             99463
  TcpMaxConn             768, TcpOutRsts               0
  TcpOutSegs          129366, TcpPassiveOpens       13809
  TcpRetransSegs           0, TcpRtoAlgorithm          1
  TcpRtoMax           120000, TcpRtoMin              200
UDP statistics:
  UdpInDatagrams           0, UdpInErrors              0
  UdpNoPorts               0, UdpOutDatagrams          3
```

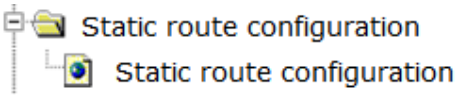
4.18 Route configuration.

Choose **Route configuration,** and the following page appears.There are "Static route configuration", "RIP configuration", "OSPF configuration", "IP Prefix configuration", "Show IP route", configuration web pages.



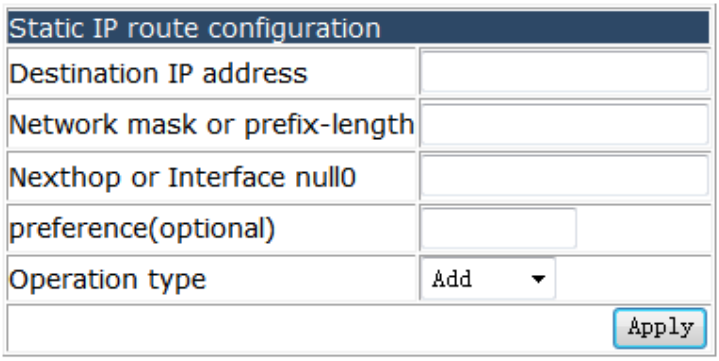
4.18.1 Static route configuration.

Choose **Route configuration > Static route configuration,** and the following page appears.



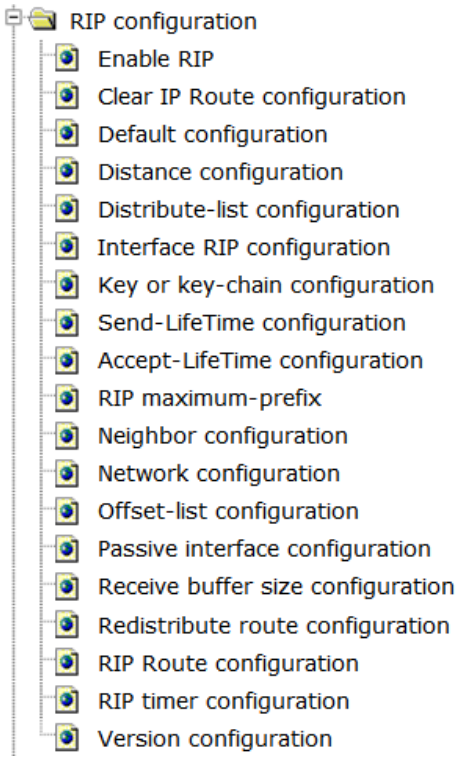
4.18.1.1 Static route configuration.

Choose **Route configuration > Static route configuration,** and the following page appears.You can configure static IP route rules to indicate the route arrive to the destination IP.



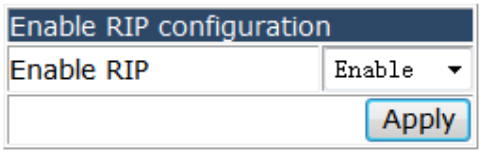
4.18.2 RIP configuration.

Choose **Route configuration > RIP configuration,** and the following page appears.There are "Enable RIP", "Clear IP Route configuration", "Default configuration", "Distance configuration", "Distribute-list configuration", "Interface RIP configuration", "Key or key-chain configuration", "Send-LifeTime configuration", "Accept-LiftTime configuration", "RIP maximum-prefix", "Neighbor configuration", "Network configuration", "Offset-list configuration", "Passive interface configuration", "Receive buffer size configuration", "Receive route configuration", "RIP route configuration", "RIP timer configuration", "Version configuration", configuration web pages.



4.18.2.1 Enable RIP.

Choose **Route configuration > RIP configuration > Enable RIP,** and the following page appears.You can enable or disable the RIP function.

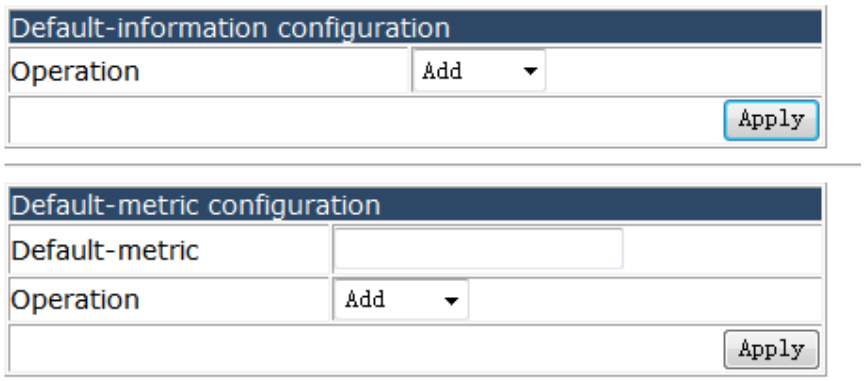


4.18.2.2 Clear IP Route configuration.

Choose **Route configuration > RIP configuration > Clear IP Route configuration,** and the following page appears.You can clear the IP route by different classes, the route class include IP-address, kernel, static, connected, rip, OSPF, ISIS, BGP, ALL.

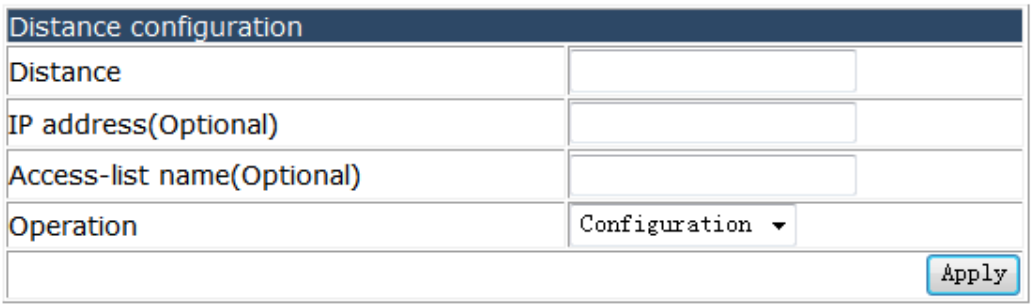
4.18.2.3 Default configuration.

Choose **Route configuration > RIP configuration > Default configuration,** and the following page appears.You can originate the default-information to RIP. And set the defualt-metric value.



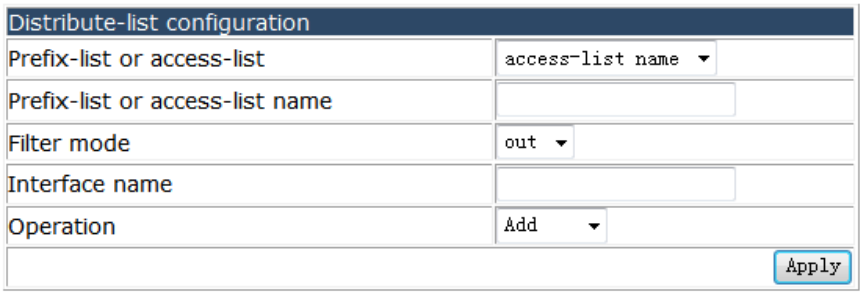
4.18.2.4 Distance configuration.

Choose **Route configuration > RIP configuration > Distance configuration,** and the following page appears.You can set the distance for IP segment, and set the access-list.



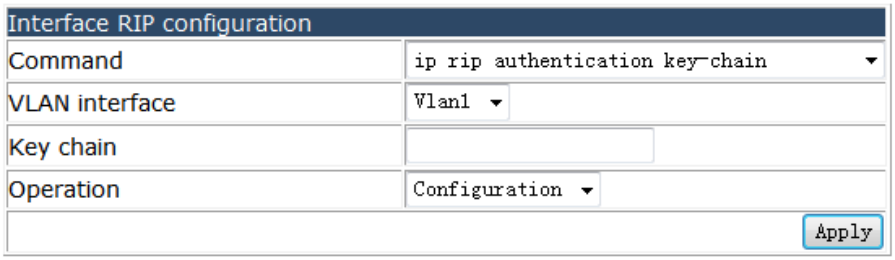
4.18.2.5 Distribute-list configuration.

Choose **Route configuration > RIP configuration > Distribute-list configuration,** and the following page appears.You can set the distribute-list, the filter method can by prefix-list or access-list, the filter mode can be out or in.



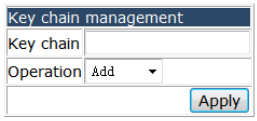
4.18.2.6 Interface RIP configuration.

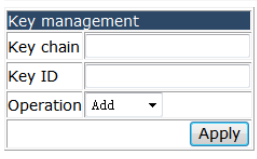
Choose **Route configuration > RIP configuration > Interface RIP configuration,** and the following page appears.You can configure the RIP interface via different command include ip rip authentication key-chain, ip rip authentication mode, ip rip authentication string, ip rip authentication cisco-compatible, no ip rip receive-packet, ip rip receive version, no ip rip send-packet, ip rip send version, ip rip split-horizon.

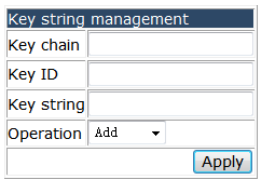


4.18.2.7 Key or key-chain configuration.

Choose **Route configuration > RIP configuration > Key or key-chain configuration,** and the following page appears.You can set Key chain, key and key string parameters.

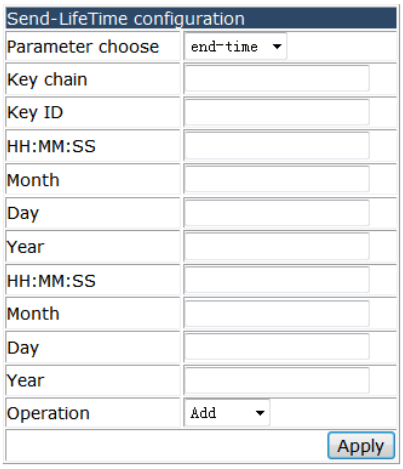






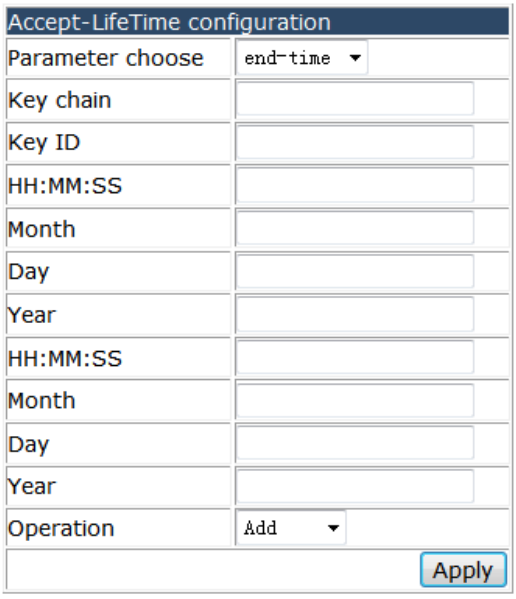
4.18.2.8 Send-LifeTime configuration.

Choose **Route configuration > RIP configuration > Send-LifeTime configuration,** and the following page appears.You can set Send-Lift time parameters include end-time, duration, infinite.



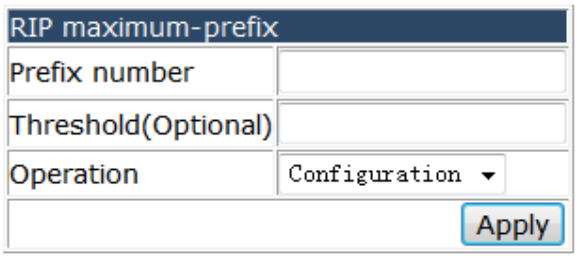
4.18.2.9 Accept-LiftTime configuration.

Choose **Route configuration > RIP configuration > Accept-LiftTime configuration,** and the following page appears.You can set Accept-Lift time parameters include end-time, duration, infinite.



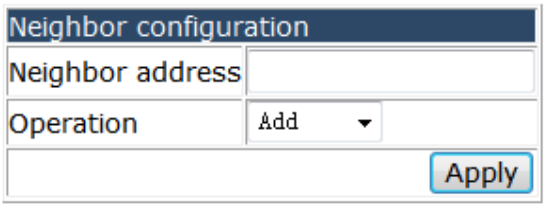
4.18.2.10 RIP maximum-prefix.

Choose **Route configuration > RIP configuration > RIP maximum-prefix,** and the following page appears.You can configure the RIP maximum-prefix.



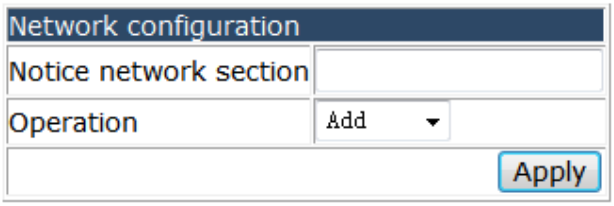
4.18.2.11 Neighbor configuration.

Choose **Route configuration > RIP configuration > Neighbor configuration,** and the following page appears.You can set the IP address of the neighbor.



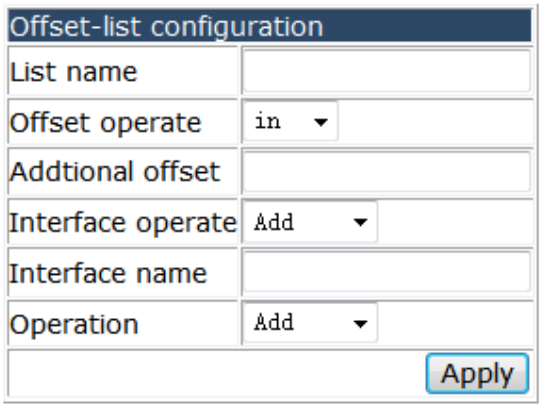
4.18.2.12 Network configuration.

Choose **Route configuration > RIP configuration > Network configuration,** and the following page appears.You can set the network section that allow to notice RIP.



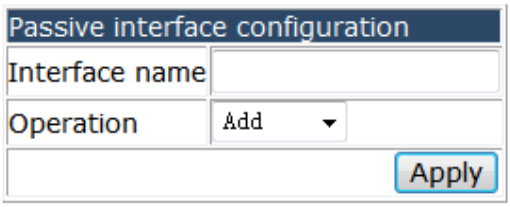
4.18.2.13 Offset-list configuration.

Choose **Route configuration > RIP configuration > Offset-list configuration,** and the following page appears.You can set the offset-list to add the metric for route.



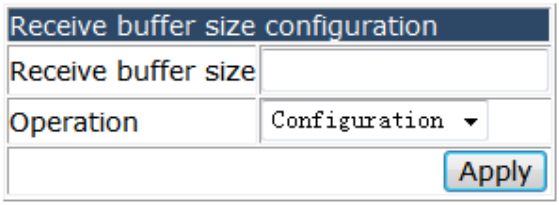
4.18.2.14 Passive interface configuration.

Choose **Route configuration > RIP configuration > Passive interface configuration,** and the following page appears.You can set the passive interface.



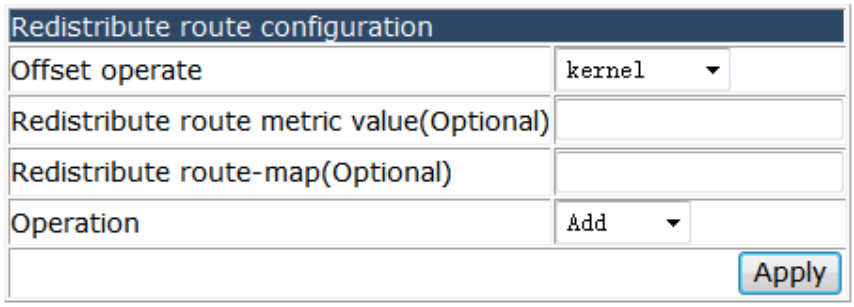
4.18.2.15 Receive buffer size configuration.

Choose **Route configuration > RIP configuration > Receive buffer size configuration,** and the following page appears.You can configure the receive buffer size.



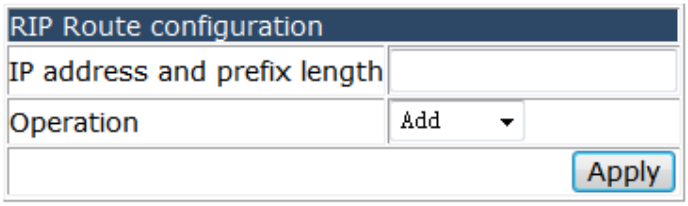
4.18.2.16 Receive route configuration.

Choose **Route configuration > RIP configuration > Receive route configuration,** and the following page appears.You can set the redistribute route rule, the offset operate include kernel, connected, static, ospf, isis, bgp.



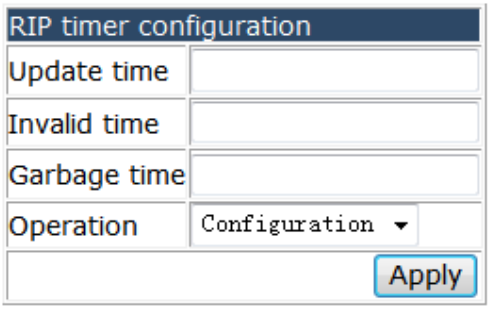
4.18.2.17 RIP route configuration.

Choose **Route configuration > RIP configuration > RIP route configuration,** and the following page appears.You can add or remove RIP Route.



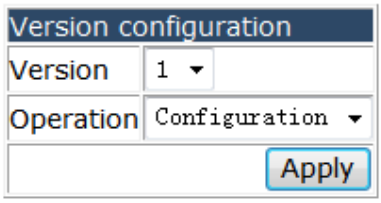
4.18.2.18 RIP timer configuration.

Choose **Route configuration > RIP configuration > RIP timer configuration,** and the following page appears.You can set the timers for RIP.



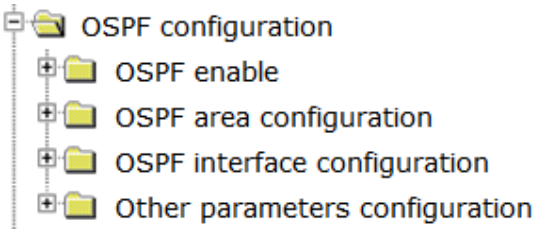
4.18.2.19 Version configuration.

Choose **Route configuration > RIP configuration > Version configuration,** and the following page appears.You can configure the version to RIP1 or RIP2.



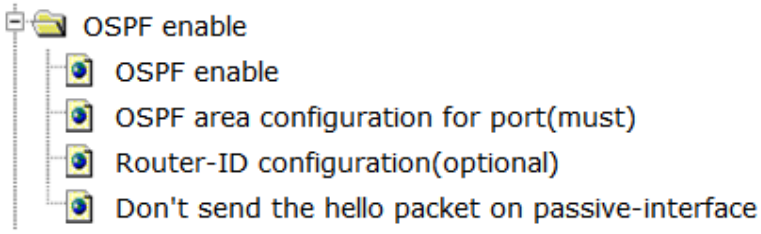
4.18.3 OSPF configuration.

Choose **Route configuration > OSPF configuration,** and the following page appears. There are "OSPF enable", "OSPF area configuration", "OSPF interface configuration", "Other parameters configuration", configuration web pages.



4.18.3.1 OSPF enable.

Choose **Route configuration > OSPF configuration > OSPF enable,** and the following page appears.There are "OSPF enable", "OSPF area configuration for port(must)", "Router-ID configuration(optional)", "Don't send the hello packet on passive-interface", configuration web pages.



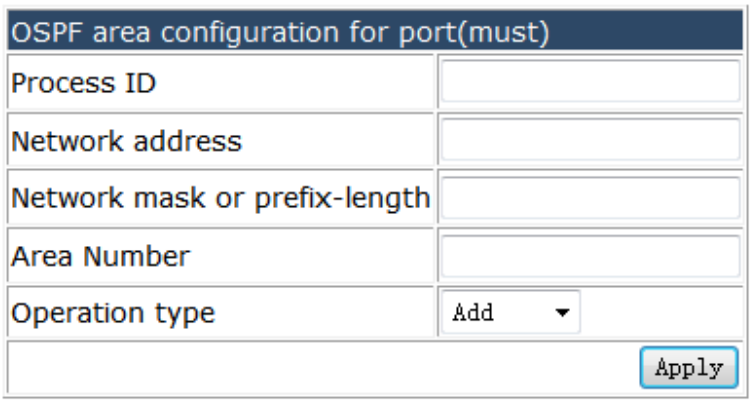
4.18.3.1.1 OSPF enable.

Choose **Route configuration > OSPF configuration > OSPF enable > OSPF enable,** and the following page appears.You can enable or disable OSPF function.

4.18.3.1.2 OSPF area configuration for port(must).

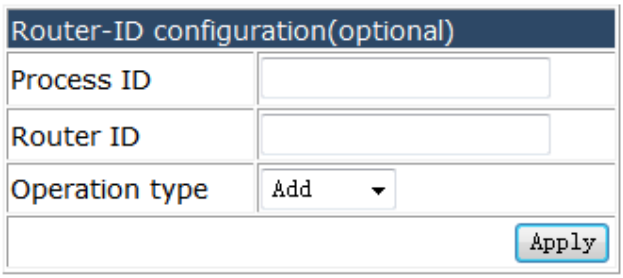
Choose **Route configuration > OSPF configuration > OSPF enable > OSPF area configuration for port(must),** and the following page appears.You can configure OSPF

areas.



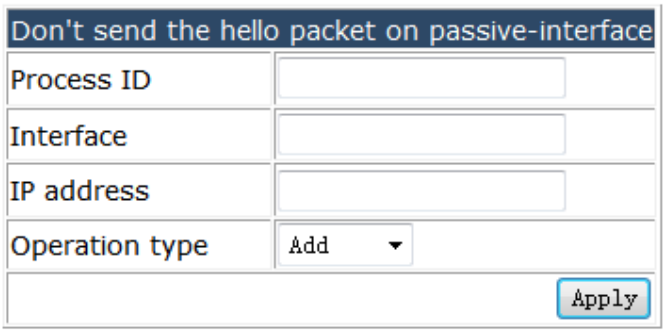
4.18.3.1.3 Router-ID configuration(optional).

Choose **Route configuration > OSPF configuration > OSPF enable > Router-ID configuration(optional),** and the following page appears.You can configure the router-ID for the OSPF process.



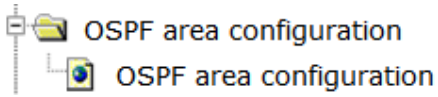
4.18.3.1.4 Don’t send the hello packet on passive-interface.

Choose **Route configuration > OSPF configuration > OSPF enable > Don’t send the hello packet on passive-interface,** and the following page appears.You can set the passive-interfaces don’t send hello packet anymore.



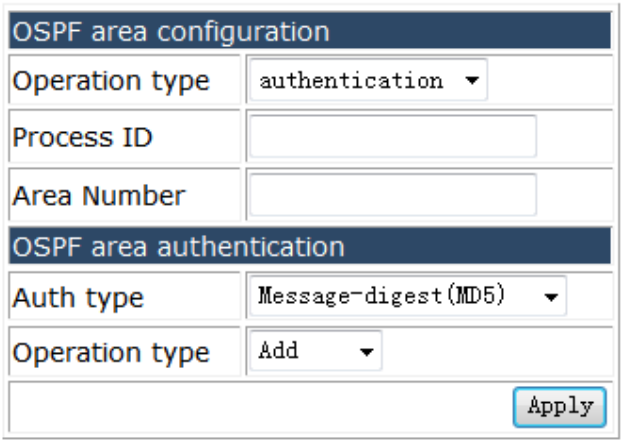
4.18.3.2 OSPF area configuration.

Choose **Route configuration > OSPF configuration > OSPF area configuration,** and the following page appears.There are "OSPF area configuration", configuration web pages.



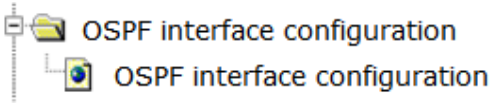
4.18.3.2.1 OSPF area configuration.

Choose **Route configuration > OSPF configuration > OSPF area configuration > OSPF area configuration,** and the following page appears.You can set different parameters for OSPF area, the operation type include authentication, default-cost, filter-list, nssa, range, stub, virtual-link.



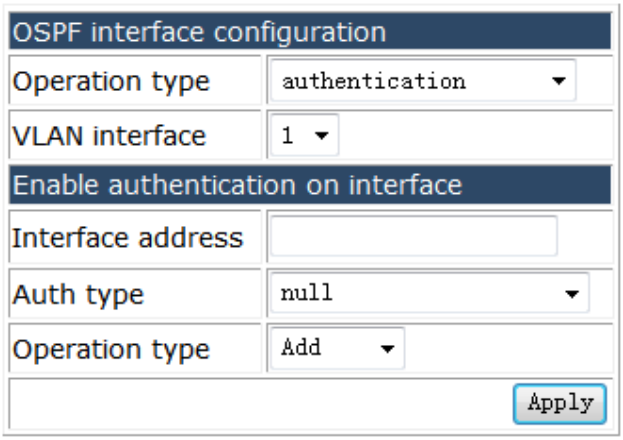
4.18.3.3 OSPF interface configuration.

Choose **Route configuration > OSPF configuration > OSPF interface configuration,** and the following page appears.There are "OSPF interface configuration", configuration web pages.



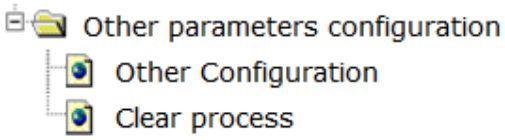
4.18.3.3.1 OSPF interface configuration.

Choose **Route configuration > OSPF configuration > OSPF interface configuration > OSPF interface configuration,** and the following page appears.You can set different parameters for OSPF interface, the operation type include authentication, authentication-key, cost, database-filter, dead-interval, disable, hello-interval, message-digest-key, mtu, mtu-ignore, network, priority, retransmit-interval, transmit-delay.



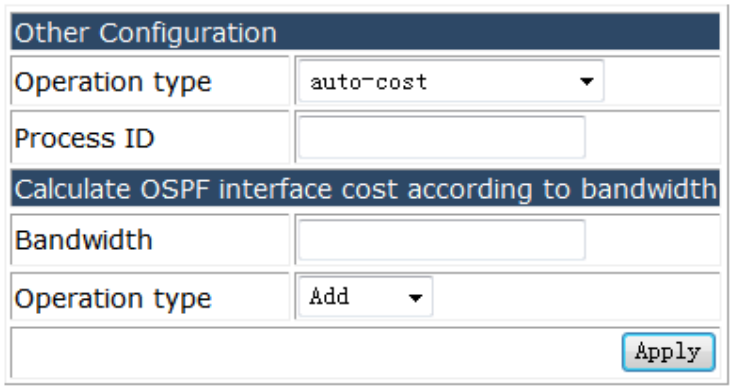
4.18.3.4 Other parameters configuration.

Choose **Route configuration > OSPF configuration > Other parameters configuration,** and the following page appears.There are "Other Configuration", "Clear process", configuration web pages.



4.18.3.4.1 Other Configuration.

Choose **Route configuration > OSPF configuration > Other parameters configuration > Other Configuration,** and the following page appears.You can set other parameters for OSPF, the operation type include auto-cost, compatible, default-information, default-metric, distance, distribute-list, host, max-concurrent-dd, neighbor, abr-type, database, database-external, passive-interface, redistribute, summary-address, timers-spf.

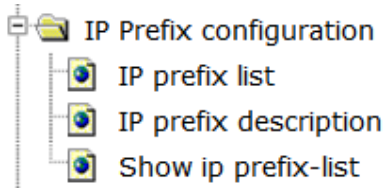


4.18.3.4.2 Clear process.

Choose **Route configuration > OSPF configuration > Other parameters configuration > Clear process,** and the following page appears.You can clear OSFP process.

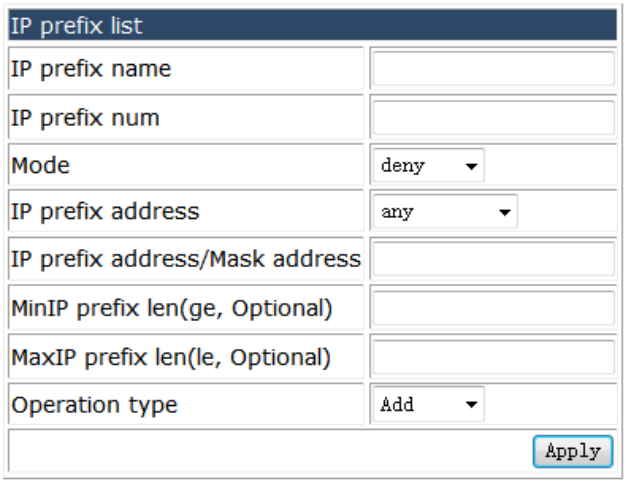
4.18.4 IP Prefix configuration.

Choose **Route configuration > IP Prefix configuration,** and the following page appears. There are "IP prefix list", "IP prefix description", "Show IP prefix-list", configuration web pages.



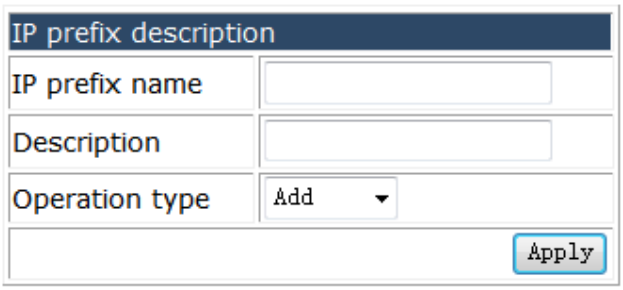
4.18.4.1 IP prefix list.

Choose **Route configuration > IP Prefix configuration > IP prefix list,** and the following page appears.You can set IP prefix list to deny or permit designated IP section accessing.



4.18.4.2 IP prefix description.

Choose **Route configuration > IP Prefix configuration > IP prefix description,** and the following page appears.You can set description for IP prefix name.

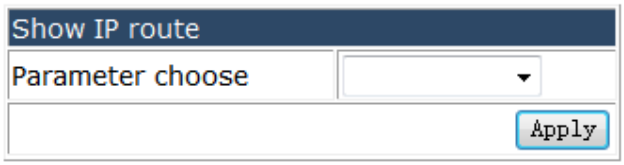


4.18.4.3 Show IP prefix-list.

Choose **Route configuration > IP Prefix configuration > Show IP prefix-list,** and the following page appears.You can show the IP prefix-list.

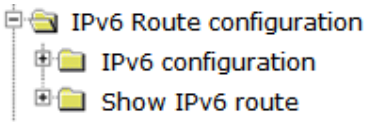
4.18.5 Show IP route.

Choose **Route configuration > Show IP route,** and the following page appears.
You can show IP route with different parameter include destination, prefix, database, connected, static, rip, ospf, bgp, isis, kernel, statistics.



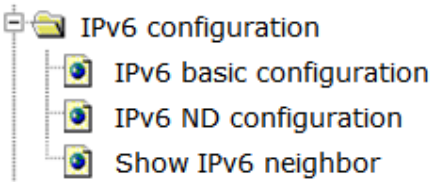
4.19 IPv6 Route configuration.

Choose **IPv6 Route configuration,** and the following page appears.There are "IPv6 configuration", "Show IPv6 route", configuration web pages.



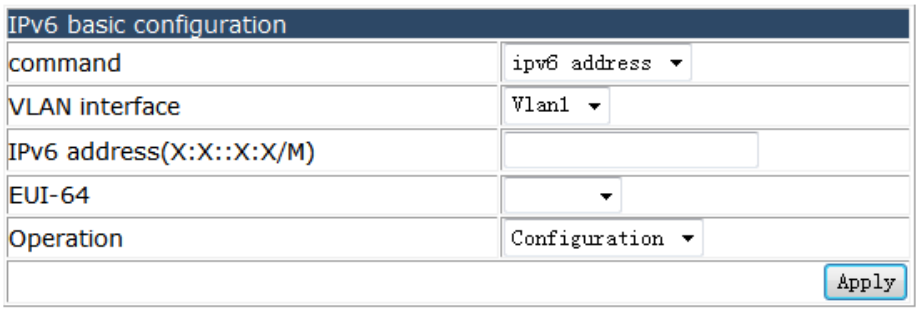
4.19.1 IPv6 configuration.

Choose **IPv6 Route configuration > IPv6 configuration,** and the following page appears.There are "IPv6 basic configuration", "IPv6 ND configuration", "Show IPv6 neighbor", configuration web pages.



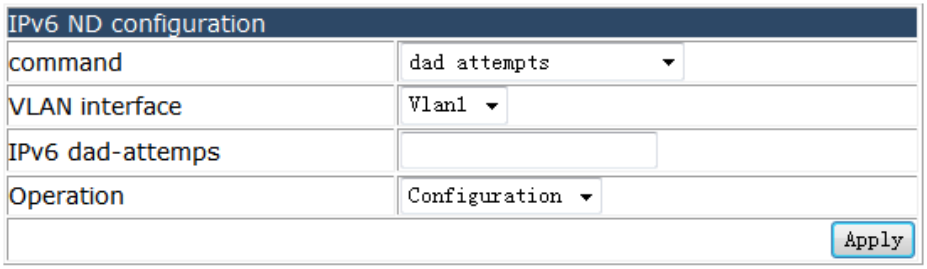
4.19.1.1 IPv6 basic configuration.

Choose **IPv6 Route configuration > IPv6 configuration > IPv6 basic configuration,** and the following page appears.You can set the IPv6 address or IPv6 route for VLAN.



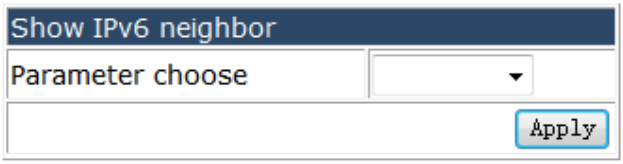
4.19.1.2 IPv6 ND configuration.

Choose **IPv6 Route configuration > IPv6 configuration > IPv6 ND configuration,** and the following page appears.You set IPv6 ND parameters via different command include dad attempts, ns-interval, supress-ra, ra-lifetime, min-ra-interval, max-ra-interval, prefix, neighbor, clear ipv6 neighbor.



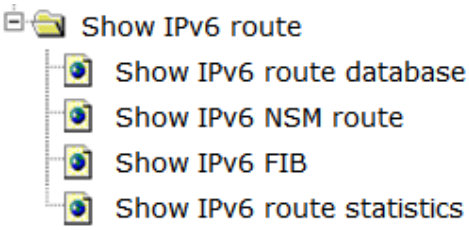
4.19.1.3 Show IPv6 neighbor.

Choose **IPv6 Route configuration > IPv6 configuration > Show IPv6 neighbor,** and the following page appears.You can show IPv6 neighbor by Address, Count, VLAN, Ethernet.



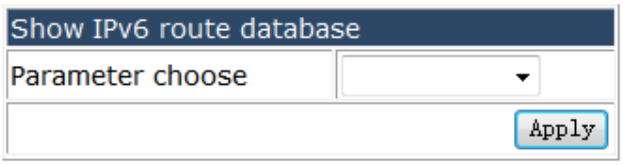
4.19.2 Show IPv6 route.

Choose **IPv6 Route configuration > Show IPv6 route,** and the following page appears.There are "Show IPv6 route database", "Show IPv6 NSM route", "Show IPv6 FIB", "Show IPv6 route statistics", configuration web pages.



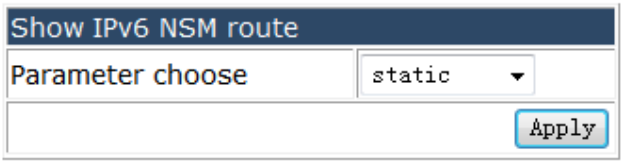
4.19.2.1 Show IPv6 route database.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 route database,** and the following page appears.You can show IPv6 route database by destination, prefix, database.



4.19.2.2 Show IPv6 NSM route.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 NSM route,** and the following page appears.You can show IPv6 NSM route by parameter include static, bgp, isis, rip, ospf, connected, kernel, database.



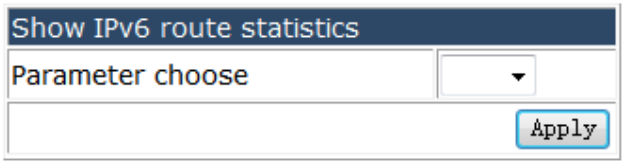
4.19.2.3 Show IPv6 FIB.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 FIB,** and the

following page appears.You can show IPv6 FIB by local, vrf, statistics.

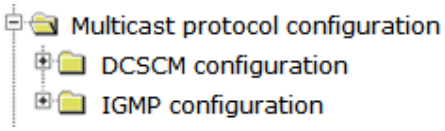
4.19.2.4 Show IPv6 route statistics.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 route statistics,** and the following page appears.You can show IPv6 statistics by vrf.



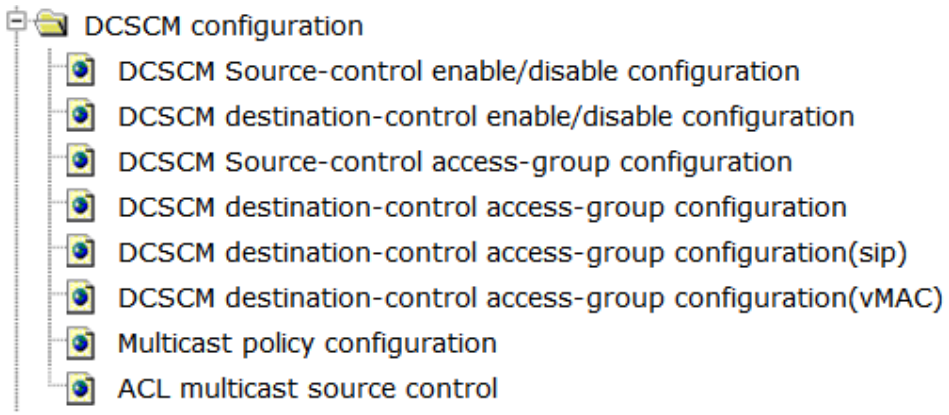
4.20 Multicast protocol configuration.

Choose **Multicast protocol configuration,** and the following page appears.There are "DCSCM configuration", "IGMP configuration", configuration web pages.



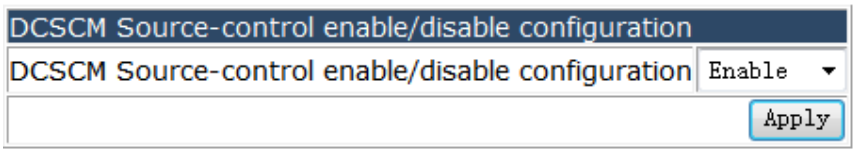
4.20.1 DCSCM configuration.

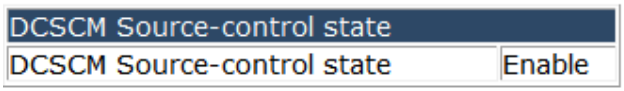
Choose **Multicast protocol configuration > DCSCM configuration,** and the following page appears.There are "DCSCM Source-control enable/disable configuration", "DCSCM destination-control enable/disable configuration", "DCSCM Source-control access-group configuration", "DCSCM destination-control access-group configuration", "DCSCM destination-control access-group configuration(SIP)", "DCSCM destination-control access-group configuration(vMAC)", "Multicast policy configuration", "ACL multicast source control", configuration web pages.



4.20.1.1 DCSCM Source-control enable/disable configuration.

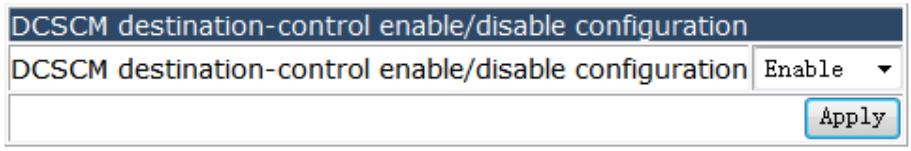
Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM Source-control enable/disable configuration, and the following page appears.You can Enable or Disable DCSCM Source-control.

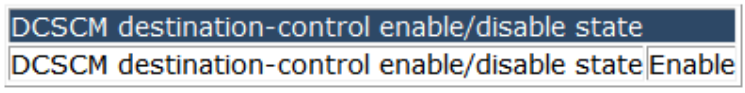




4.20.1.2 DCSCM destination-control enable/disable configuration.

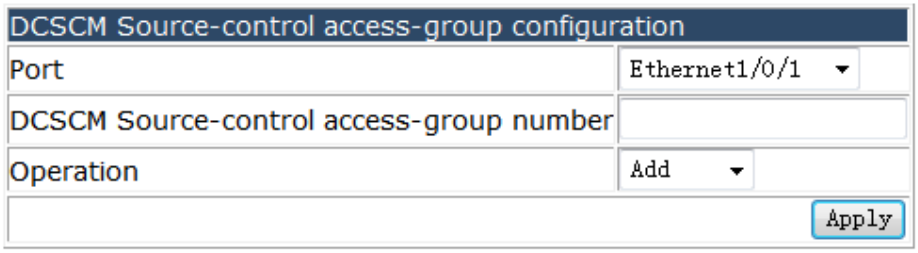
Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM destination-control enable/disable configuration, and the following page appears.You can Enable or Disable DCSCM destination-control.

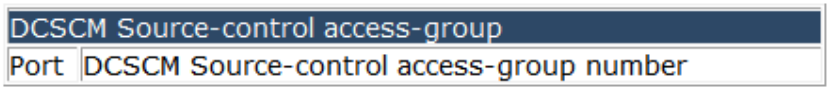




4.20.1.3 DCSCM Source-control access-group configuration.

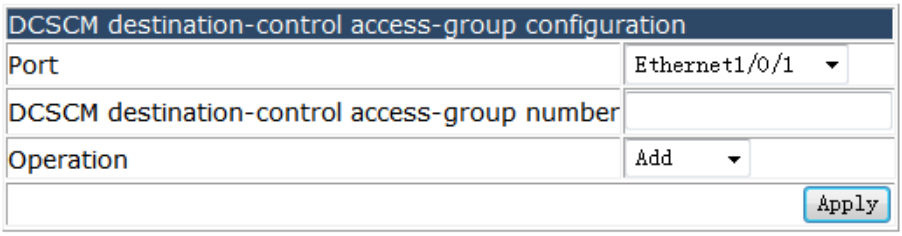
Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM Source-control access-group configuration**,** and the following page appears.You can add or remove DCSCM Source-control access-group.

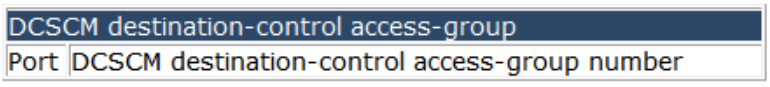




4.20.1.4 DCSCM destination-control access-group configuration.

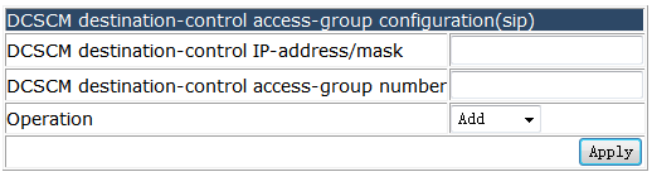
Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM Source-control access-group configuration**,** and the following page appears.
You can add or remove DCSCM destination-control access-group.





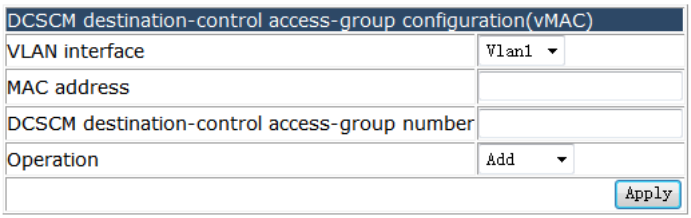
4.20.1.5 DCSCM destination-control access-group configuration(SIP).

Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM Source-control access-group configuration(SIP)**,** and the following page appears.
You can add or remove DCSCM destination-control access-group(SIP).



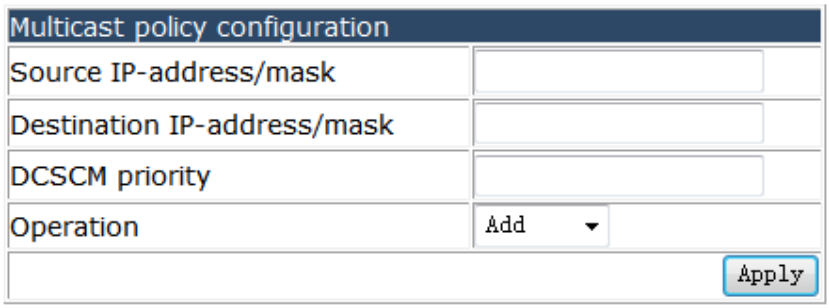
4.20.1.6 DCSCM destination-control access-group configuration(vMAC).

Choose **Multicast protocol configuration > DCSCM configuration >** DCSCM Source-control access-group configuration(vMAC), and the following page appears. You can add or remove DCSCM Source-control access-group(vMAC).



4.20.1.7 Multicast policy configuration.

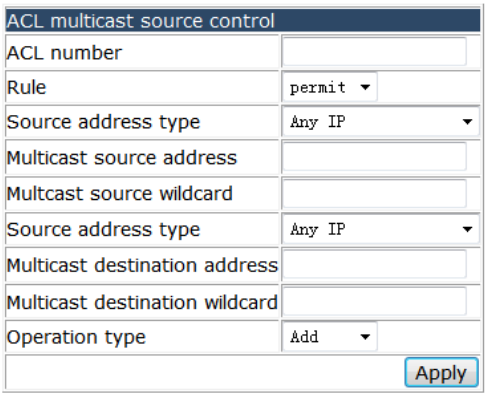
Choose **Multicast protocol configuration > DCSCM configuration >** Multicast policy configuration, and the following page appears.You can set the DCSCM multicast policy.

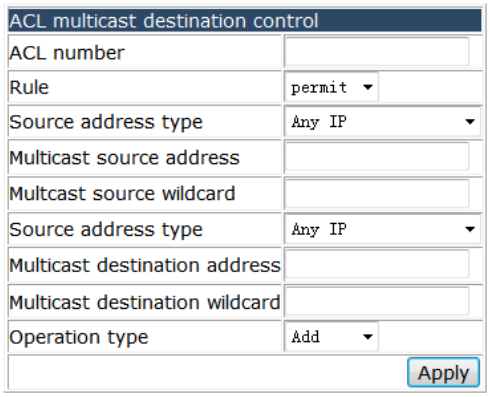


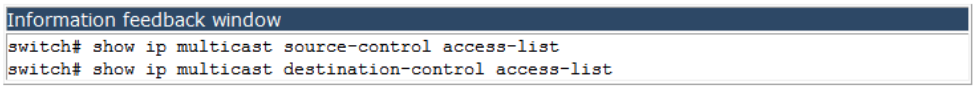
4.20.1.8 ACL multicast source control.

Choose **Multicast protocol configuration > DCSCM configuration >** ACL multicast source control, and the following page appears.You can set the ACL multicast source and

destination control to permit or deny the designated IP address.

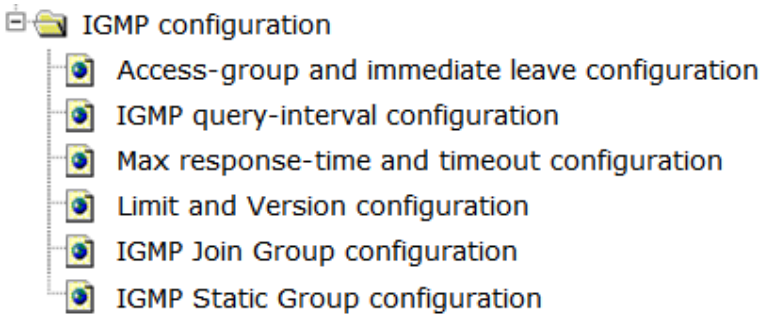






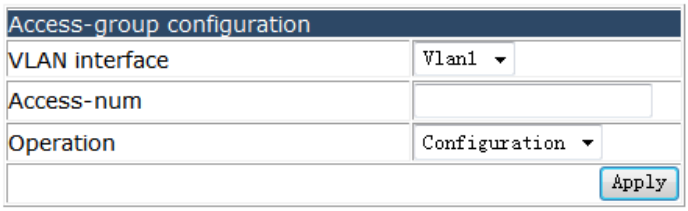
4.20.2 IGMP configuration.

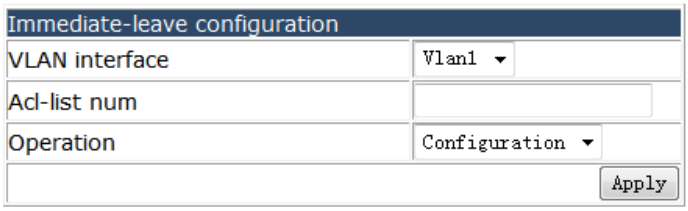
Choose **Multicast protocol configuration > IGMP configuration,** and the following page appears.There are "Access-group and immediate leave configuration", "IGMP query-interval configuration", "Max response-time and timeout configuration", "Limit and Version configuration", "IGMP Join Group configuration", "IGMP Static Group configuration", configuration web pages.



4.20.2.1 Access-group and immediate leave configuration.

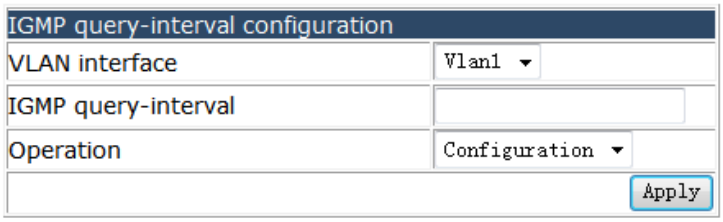
Choose **Multicast protocol configuration > IGMP configuration > Access-group and immediate leave configuration,** and the following page appears.You can set the IGMP access-group and immediate-leave group for VLAN.

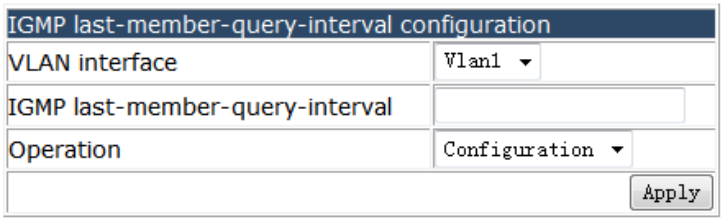




4.20.2.2 IGMP query-interval configuration.

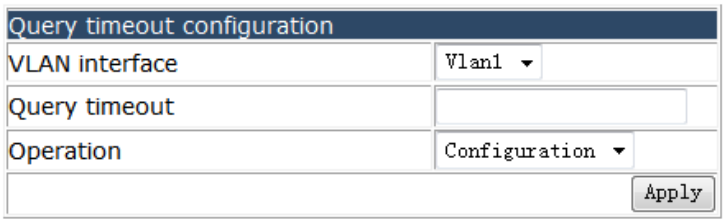
Choose **Multicast protocol configuration > IGMP configuration > IGMP query-interval configuration,** and the following page appears.You can set the IGMP query-interval and last-member-query-interval for VLAN.

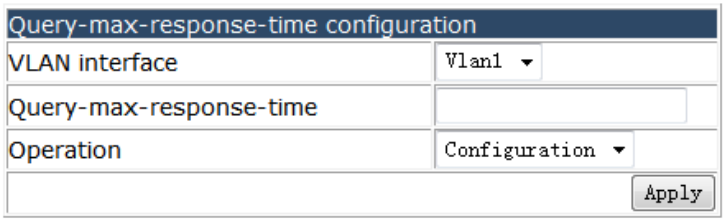




4.20.2.3 Max response-time and timeout configuration.

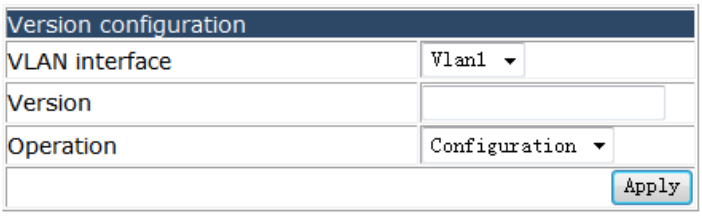
Choose **Multicast protocol configuration > IGMP configuration > Max response-time and timeout configuration,** and the following page appears.You can set the query timeout value and query-max-response-time for VLAN.

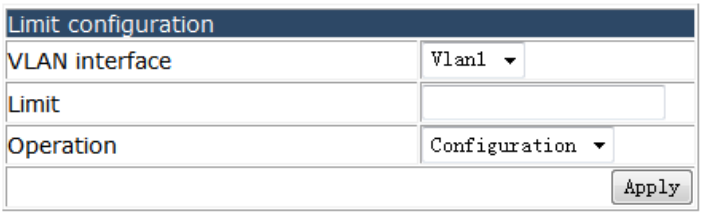




4.20.2.4 Limit and Version configuration.

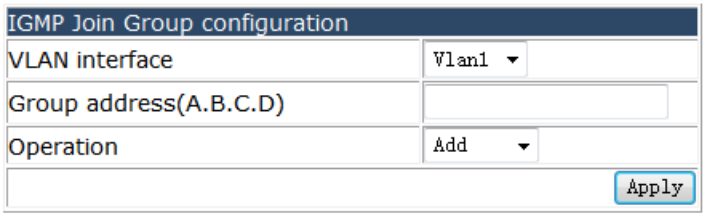
Choose **Multicast protocol configuration > IGMP configuration > Limit and Version configuration,** and the following page appears.You can set the IGMP version and limit parameter.





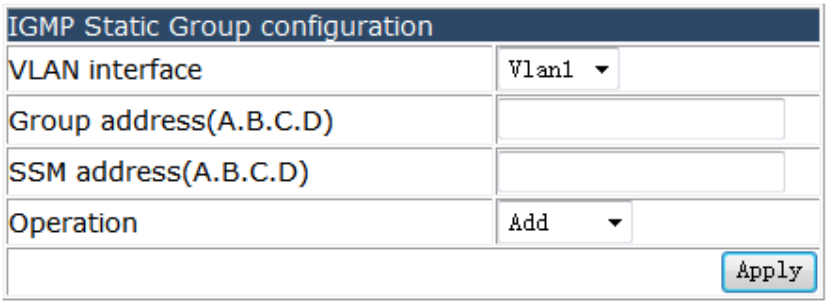
4.20.2.5 IGMP Join Group configuration.

Choose **Multicast protocol configuration > IGMP configuration > IGMP Join Group configuration,** and the following page appears.You can add or remove VLAN to a IGMP group.



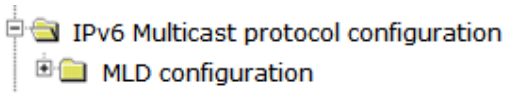
4.20.2.6 IGMP Static Group configuration.

Choose **Multicast protocol configuration > IGMP configuration > IGMP Static Group configuration,** and the following page appears.You can add or remove VLAN to a static IGMP group with designated source.



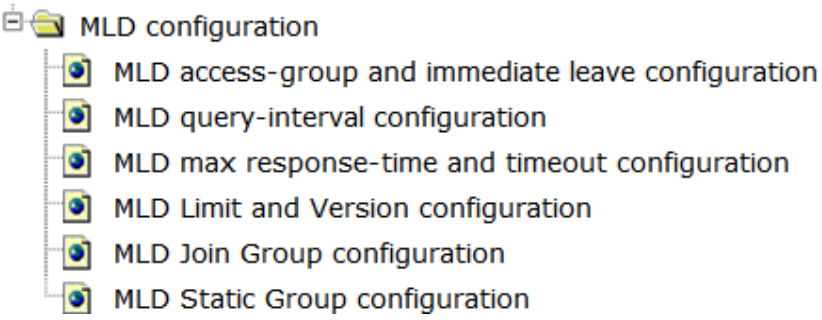
4.21 IPv6 Multicast protocol configuration.

Choose **IPv6 Multicast protocol configuration,** and the following page appears.



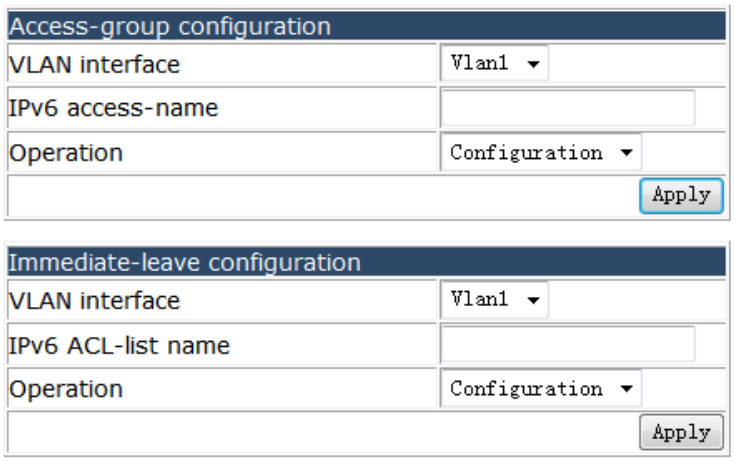
4.21.1 MLD configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration,** and the following page appears.There are "MLD access-group and immediate leave configuration", "MLD query-interval configuration", "MLD max response-time and timeout configuration", "MLD Limit and Version configuration", "MLD Join Group configuration", "MLD Static Group configuration", configuration web pages.



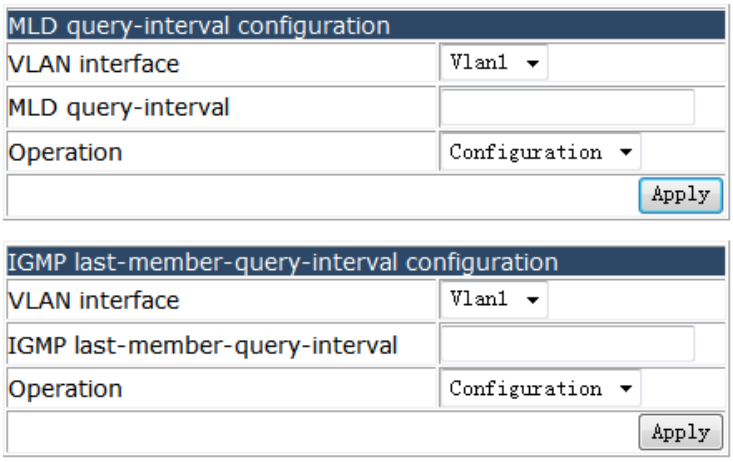
4.21.1.1 MLD access-group and immediate leave configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD access-group and immediate leave configuration,** and the following page appears. You can set the IPv6 access-group and IPv6 immediate-leave group for VLAN.



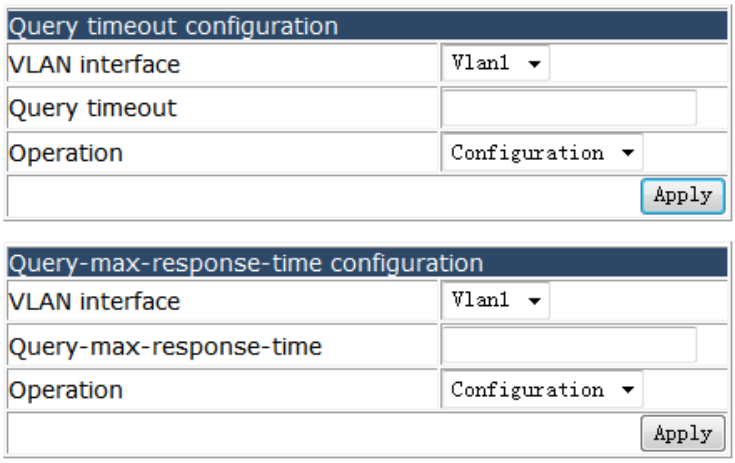
4.21.1.2 MLD query-interval configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD query-interval configuration,** and the following page appears.You can set the MLD query-interval and IGMP last-member-query-interval for VLAN.



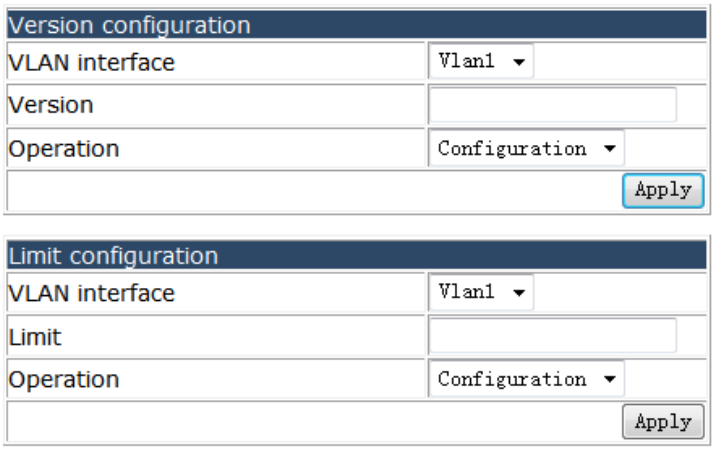
4.21.1.3 MLD max response-time and timeout configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD max response-time and timeout configuration,** and the following page appears.You can set the query timeout value and query-max-response-time for VLAN.



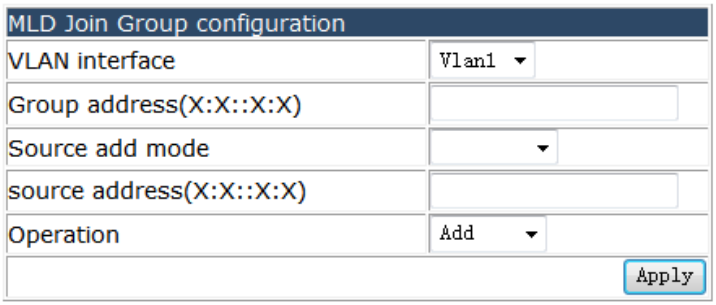
4.21.1.4 MLD Limit and Version configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Limit and Version configuration,** and the following page appears.You can set the MLD version and limit parameter.



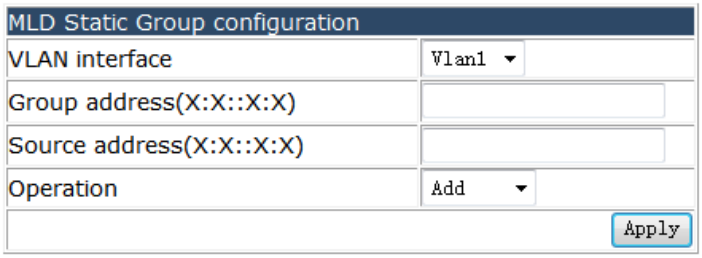
4.21.1.5 MLD Join Group configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Join Group configuration,** and the following page appears.You can add or remove VLAN to a MLD group and choose to include or exclude designated source.



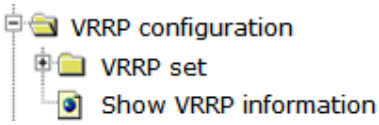
4.21.1.6 MLD Static Group configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Static Group configuration,** and the following page appears.You can add or remove VLAN to a static MLD group with designated source.



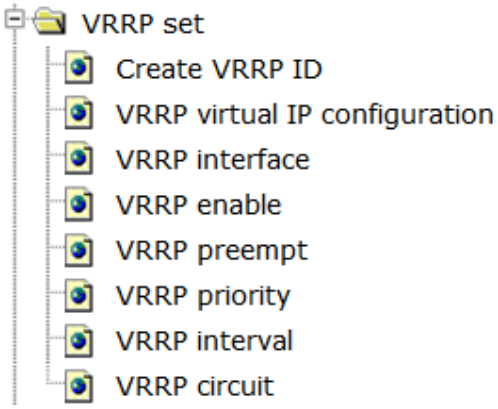
4.22 VRRP configuration.

Choose **VRRP configuration,** and the following page appears.There are "VRRP set", "Show VRRP information", configuration web pages.



4.22.1 VRRP set.

Choose **VRRP configuration > VRRP set,** and the following page appears.There are "Create VRRP ID", "VRRP virtual IP configuration", "VRRP interface", "VRRP enable", "VRRP preempt", "VRRP priority", "VRRP interval", "VRRP circuit", configuration web pages.

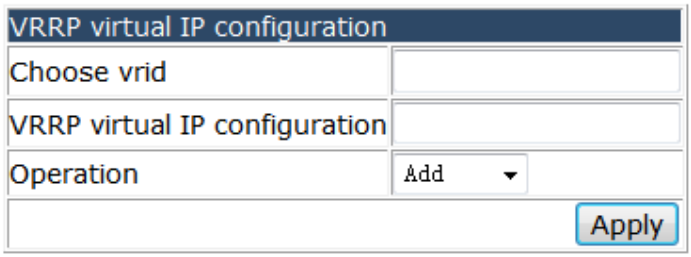


4.22.1.1 Create VRRP ID.

Choose **VRRP configuration > VRRP set > Create VRRP ID,** and the following page appears.You can create a VRRP ID.

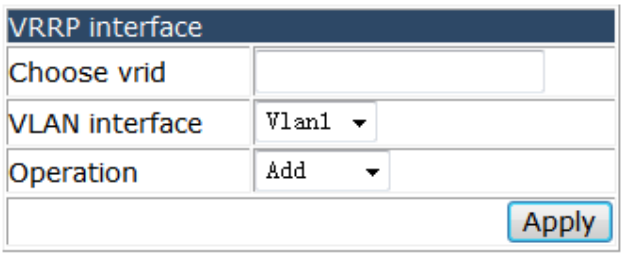
4.22.1.2 VRRP virtual IP configuration.

Choose **VRRP configuration > VRRP set > VRRP virtual IP configuration,** and the following page appears.You can set the VRRP virtual IP for the VRRP ID.



4.22.1.3 VRRP interface.

Choose **VRRP configuration > VRRP set > VRRP interface,** and the following page appears.You can set the VLAN interface for the VRRP ID.



4.22.1.4 VRRP enable.

Choose **VRRP configuration > VRRP set > VRRP enable,** and the following page appears.You can enable or disable the VRRP function for the VRRP ID.

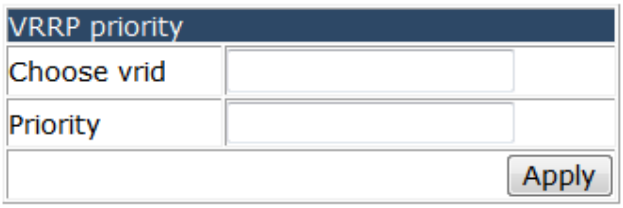
Notice:Before enable VRRP,please finish the setting of Virtual IP and Interface

4.22.1.5 VRRP preempt.

Choose **VRRP configuration > VRRP set > VRRP preempt,** and the following page appears.You can set the VRRP preempt to ture or false for VRRP ID.

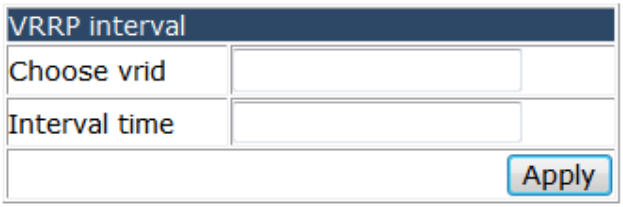
4.22.1.6 VRRP priority.

Choose **VRRP configuration > VRRP set > VRRP priority,** and the following page appears.
You can set VRRP Priority.



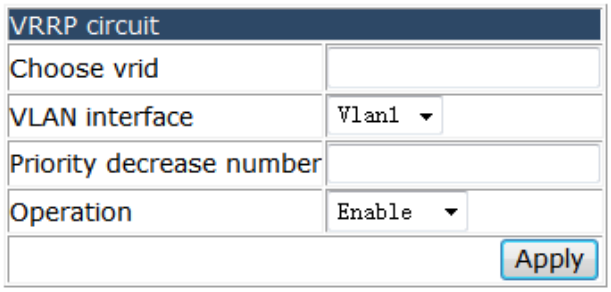
4.22.1.7 VRRP interval.

Choose **VRRP configuration > VRRP set > VRRP interval,** and the following page appears.You can set VRRP interval.



4.22.1.8 VRRP circuit.

Choose **VRRP configuration > VRRP set > VRRP circuit,** and the following page appears.You can set the priority decrease number for the VRRP ID.

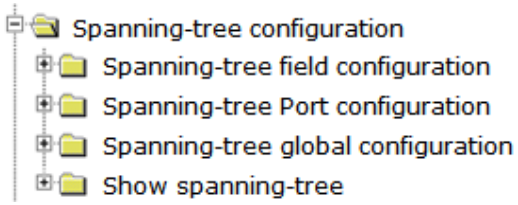


4.22.2 Show VRRP information.

Choose **VRRP configuration > Show VRRP information,** and the following page appears.You can show the VRRP information.

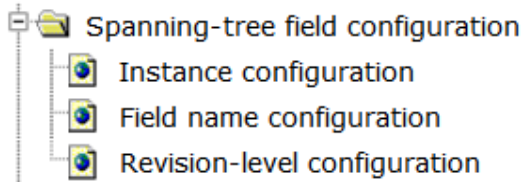
4.23 Spanning- tree configuration.

Choose **Spanning- tree configuration,** and the following page appears.There are "Spanning-tree field configuration", "Spanning-tree Port configuration", "Spanning-tree global configuration", "Show Spanning-tree", configuration web pages.



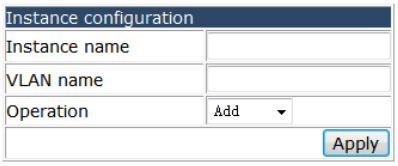
4.23.1 Spanning-tree field configuration.

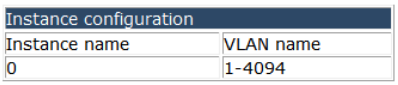
Choose **Spanning- tree configuration > Spanning-tree field configuration,** and the following page appears.There are "Instance configuration", "Field name configuration", "Revision-level configuration", configuration web pages.

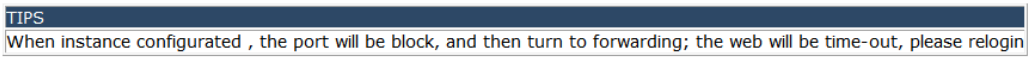


4.23.1.1 Instance configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration > Instance configuration,** and the following page appears.You can configure instance and associate with VLAN.



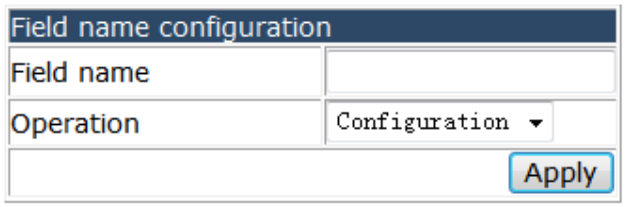




4.23.1.2 Field name configuration.

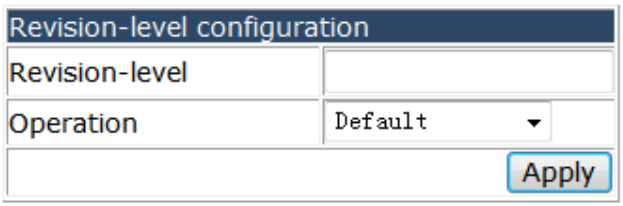
Choose **Spanning- tree configuration > Spanning-tree field configuration > Field**

name configuration, and the following page appears.You can configure the MSTP field name.



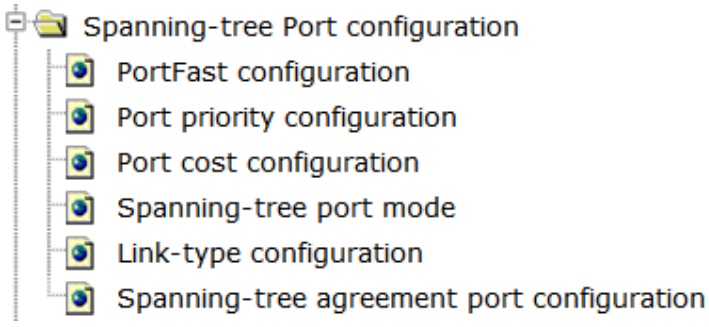
4.23.1.3 Revision-level configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration > Revision-level configuration,** and the following page appears.You can configure MSTP revision-level.



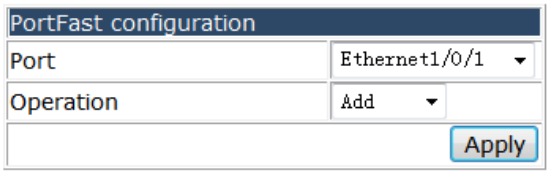
4.23.2 Spanning-tree Port configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration,** and the following page appears.There are "PortFast configuration", "Port priority configuration", "Port cost configuration", "Spanning-tree port mode", "Link-type configuration", "Spanning-tree agreement port configuration", configuration web pages.



4.23.2.1 PortFast configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > PortFast configuration,** and the following page appears.You can set the any port to be PortFast.

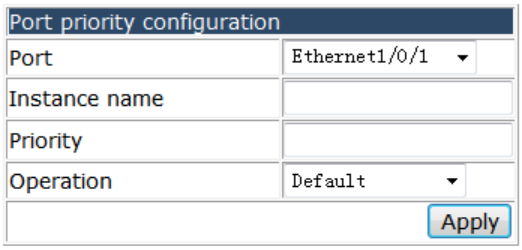


PortFast configuration	
Port	Ethernet1/0/1
Operation	Add
	Apply

PortFast configuration	
Port	PortType(1/0)
Ethernet1/0/1	1
Ethernet1/0/2	1
Ethernet1/0/3	1
Ethernet1/0/4	1
Ethernet1/0/5	1
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0
Ethernet1/0/9	0
Ethernet1/0/10	0
Ethernet1/0/11	0
Ethernet1/0/12	0
Ethernet1/0/13	0
Ethernet1/0/14	0
Ethernet1/0/15	0
Ethernet1/0/16	0
Ethernet1/0/17	0
Ethernet1/0/18	0

4.23.2.2 Port priority configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Port priority configuration,** and the following page appears.You can set the priority and associate Instance to each port.

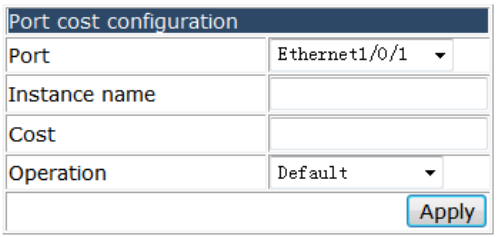


Port priority configuration	
Port	Ethernet1/0/1
Instance name	
Priority	
Operation	Default
	Apply

Port priority configuration	
Ethernet1/0/1 of Instance 2	Operation port path cost 0, Port priority 48, Port Identifier 048.001
Ethernet1/0/2 of Instance 1	Operation port path cost 0, Port priority 16, Port Identifier 016.002

4.23.2.3 Port cost configuration.

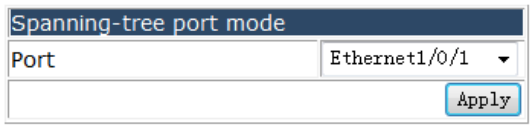
Choose **Spanning- tree configuration > Spanning-tree Port configuration > Port cost configuration,** and the following page appears.You can set the port cost and associate Instance to each port.

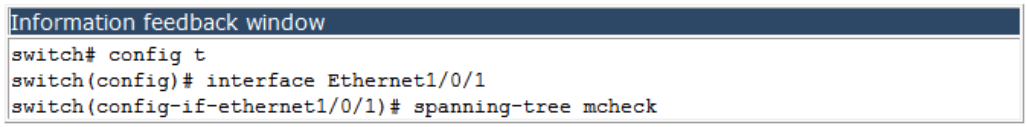


Port cost configuration	
Ethernet1/0/1 of Instance 2	Operation port path cost 2222, Port priority 48, Port Identifier 048.001
Ethernet1/0/2 of Instance 1	Operation port path cost 33333, Port priority 16, Port Identifier 016.002

4.23.2.4 Spanning-tree port mode.

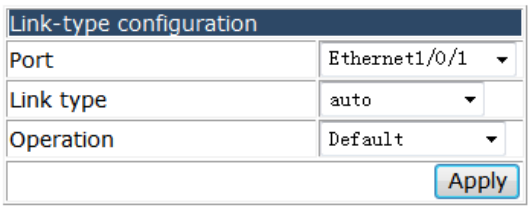
Choose **Spanning- tree configuration > Spanning-tree Port configuration > Spanning-tree port mode,** and the following page appears.You can force the port to work on SMTP mode.





4.23.2.5 Link-type configuration.

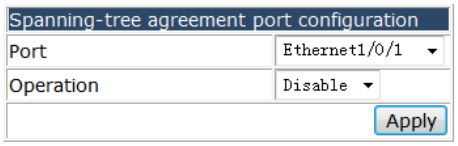
Choose **Spanning- tree configuration > Spanning-tree Port configuration > Link-type configuration,** and the following page appears.You can set the link type to auto, force-false or force-true for each port.



Link-type configuration	
Port	Link type
Ethernet1/0/1	auto
Ethernet1/0/2	Force True
Ethernet1/0/3	Force False
Ethernet1/0/4	auto
Ethernet1/0/5	auto
Ethernet1/0/6	auto
Ethernet1/0/7	auto
Ethernet1/0/8	auto
Ethernet1/0/9	auto
Ethernet1/0/10	auto
Ethernet1/0/11	auto
Ethernet1/0/12	auto
Ethernet1/0/13	auto
Ethernet1/0/14	auto
Ethernet1/0/15	auto

4.23.2.6 Spanning-tree agreement port configuration.

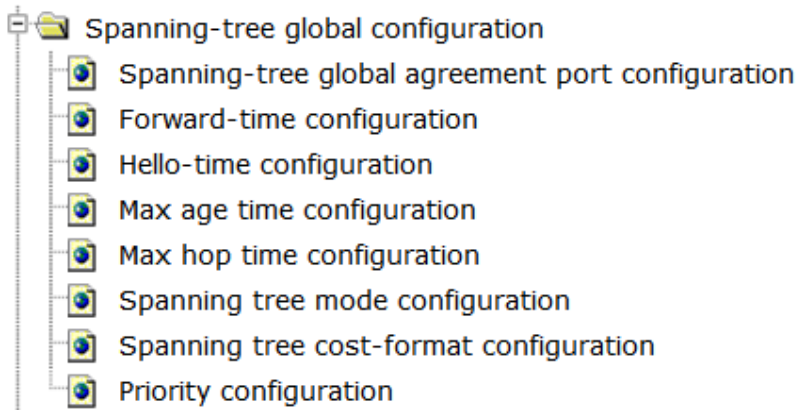
Choose **Spanning- tree configuration > Spanning-tree Port configuration > Spanning-tree agreement port configuration,** and the following page appears.You can enable or disable the spanning-tree function for each port.



Spanning-tree agreement port configuration	
Port	Spanning-tree agreement port configuration
Ethernet1/0/1	enable
Ethernet1/0/2	enable
Ethernet1/0/3	enable
Ethernet1/0/4	enable
Ethernet1/0/5	enable
Ethernet1/0/6	disable
Ethernet1/0/7	disable
Ethernet1/0/8	disable
Ethernet1/0/9	enable
Ethernet1/0/10	enable
Ethernet1/0/11	enable
Ethernet1/0/12	enable
Ethernet1/0/13	enable
Ethernet1/0/14	enable

4.23.3 Spanning-tree global configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration,** and the following page appears.There are "Spanning-tree global agreement port configuration", "Forward-time configuration", "Hello-time configuration", "Max age time configuration", "Max hop time configuration", "Spanning tree mode configuration", "Spanning tree cost-format configuration", "Priority configuration", configuration web pages.

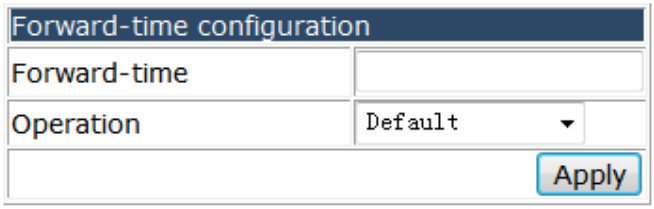


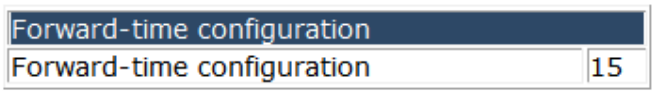
4.23.3.1 Spanning-tree global agreement port configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning-tree global agreement port configuration,** and the following page appears.You can enable or disable Spanning-tree global agreement.

4.23.3.2 Forward-time configuration.

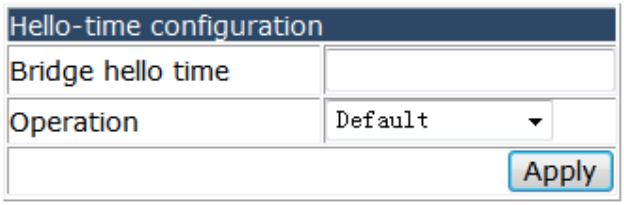
Choose **Spanning- tree configuration > Spanning-tree global configuration > Forward-time configuration,** You can set the forward-time, and notice that: 2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age, Bridge_Max_Age >= 2×(Bridge_Hello_Time + 1.0 seconds).





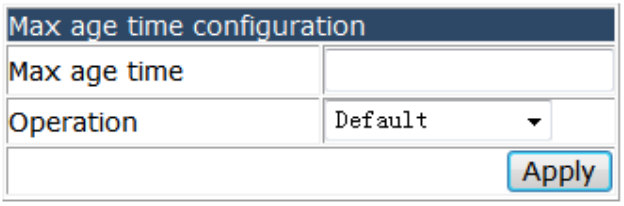
4.23.3.3 Hello-time configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Hello-time configuration,** and the following page appears.You can set Hello-time interval.



4.23.3.4 Max age time configuration.

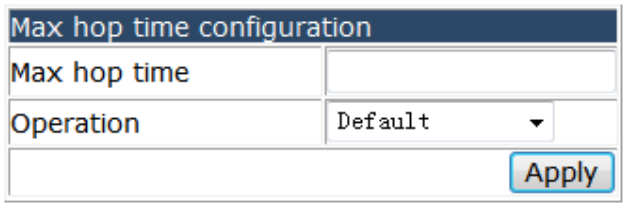
Choose **Spanning- tree configuration > Spanning-tree global configuration > Max age time configuration,** and the following page appears.You can set Max age time.



4.23.3.5 Max hop time configuration.

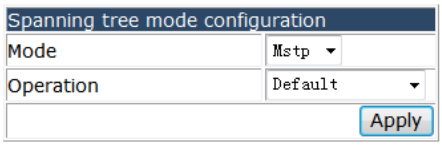
Choose **Spanning- tree configuration > Spanning-tree global configuration > Max hop time configuration,** and the following page appears.You can set the Max hop

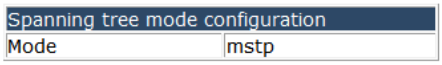
for BPDU.



4.23.3.6 Spanning tree mode configuration.

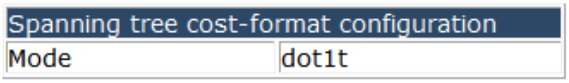
Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning tree mode configuration,** and the following page appears.You can set the Spanning tree work mode to MSTP, STP or RSTP.





4.23.3.7 Spanning tree cost-format configuration.

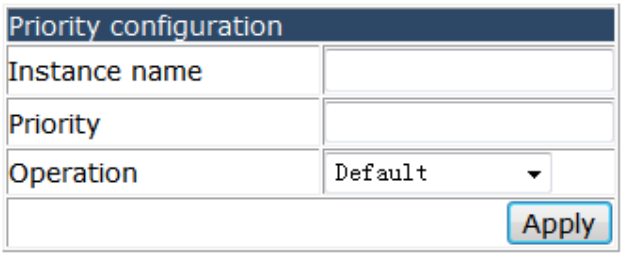
Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning tree cost-format configuration,** and the following page appears.You can set the Spanning tree cost-format to dot1t or dot1d.

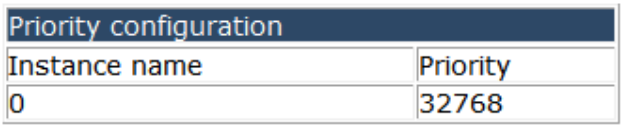


4.23.3.8 Priority configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Priority configuration,** and the following page appears.You can set the priority for different

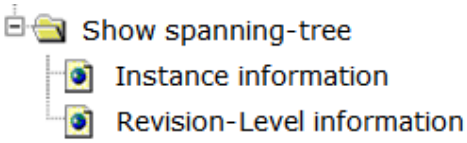
Instance.





4.23.4 Show Spanning-tree.

Choose **Spanning- tree configuration > Show Spanning-tree,** and the following page appears.There are "Instance information", "Revision-Level information", configuration web pages.



4.23.4.1 Instance information.

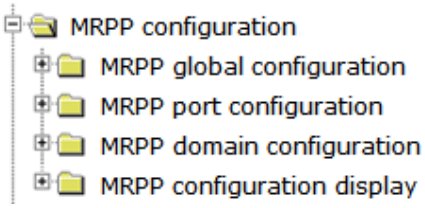
Choose **Spanning- tree configuration > Show Spanning-tree > Instance information,** and the following page appears.You can show the detail information for Spanning-tree Instance.

4.23.4.2 Revision-Level information.

Choose **Spanning- tree configuration > Show Spanning-tree > Revision-Level information,** and the following page appears.You can show the Spanning-tree mst configuration information.

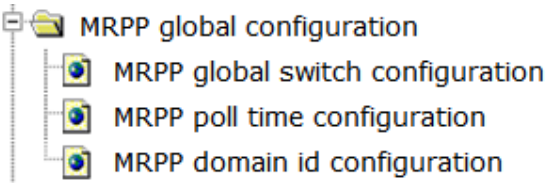
4.24 MRPP configuration.

Choose **MRPP configuration,** and the following page appears.There are "MRPP global configuration", "MRPP port configuration", "MRPP domain configuration", "MRPP configuration display", configuration web pages.



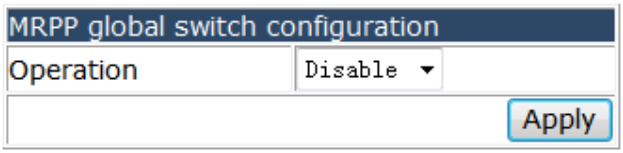
4.24.1 MRPP global configuration.

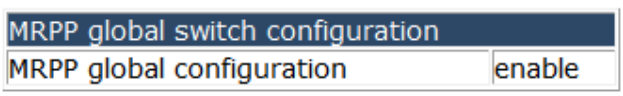
Choose **MRPP configuration > MRPP global configuration,** and the following page appears.There are "MRPP global switch configuration", "MRPP poll time configuration", "MRPP domain id configuration", configuration web pages.



4.24.1.1 MRPP global switch configuration.

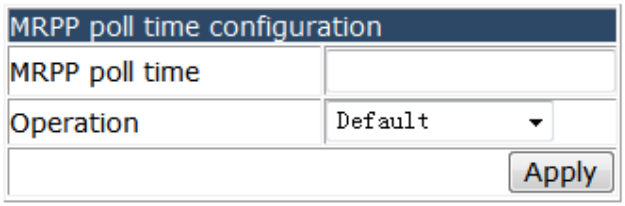
Choose **MRPP configuration > MRPP global configuration > MRPP global switch configuration,** and the following page appears.You can enable or disable the MRPP function.





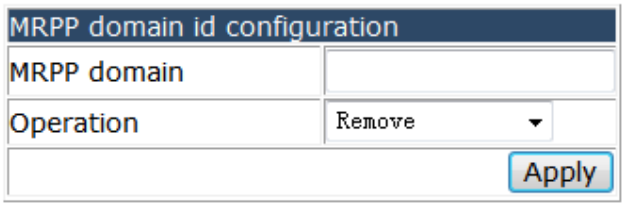
4.24.1.2 MRPP poll time configuration.

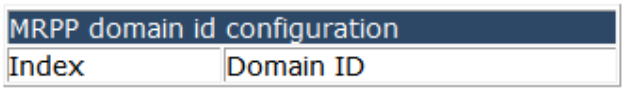
Choose **MRPP configuration > MRPP global configuration > MRPP poll time configuration,** and the following page appears.You can configure MRPP poll time.



4.24.1.3 MRPP domain id configuration.

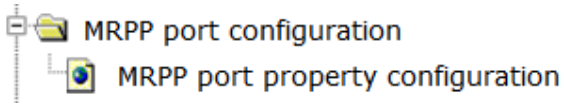
Choose **MRPP configuration > MRPP global configuration > MRPP domain id configuration,** and the following page appears.You can configure the domain ID for MRPP.





4.24.2 MRPP port configuration.

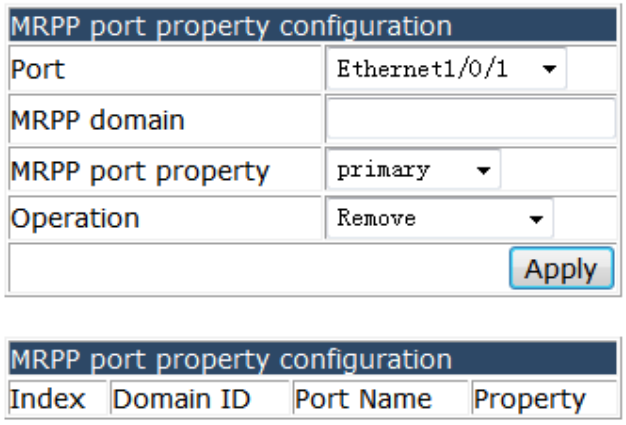
Choose **MRPP configuration > MRPP port configuration,** and the following page appears.



4.24.2.1 MRPP port property configuration.

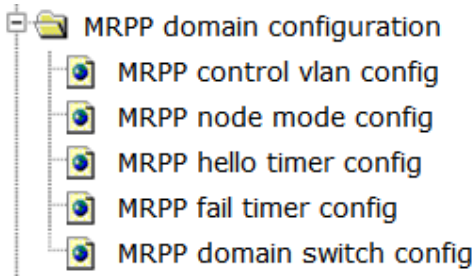
Choose **MRPP configuration > MRPP port configuration > MRPP port property configuration,** and the following page appears.You can add or remove any port to MRPP

domain, and set the port property to primary or secondary.



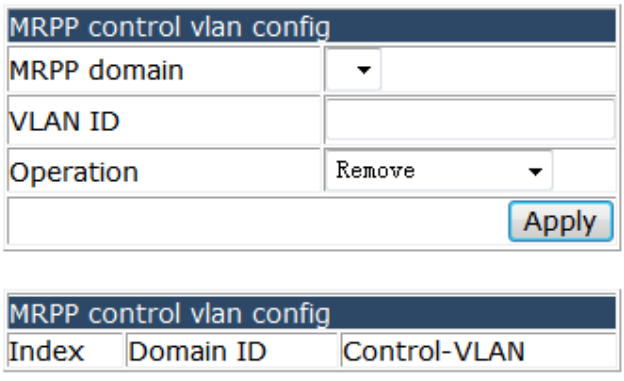
4.24.3 MRPP domain configuration.

Choose **MRPP configuration > MRPP domain configuration,** and the following page appears.There are "MRPP control vlan config", "MRPP node mode config", "MRPP hello timer config", "MRPP fail timer config", "MRPP domain switch config", configuration web pages.



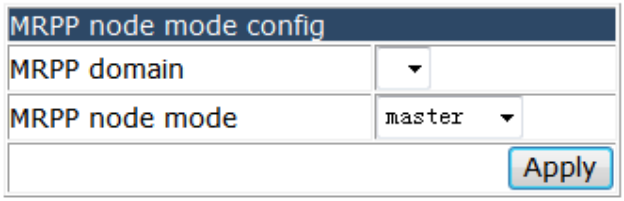
4.24.3.1 MRPP control vlan config.

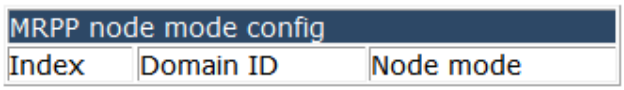
Choose **MRPP configuration > MRPP domain configuration > MRPP control vlan config,** and the following page appears.You can configure the MRPP control VLAN for MRPP domain.



4.24.3.2 MRPP node mode config.

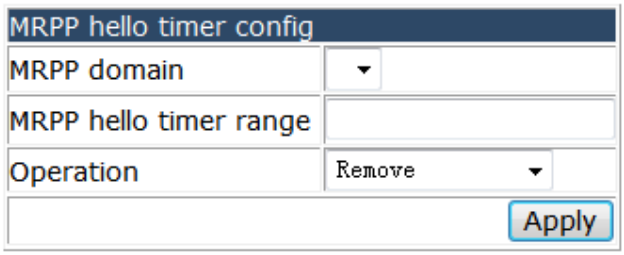
Choose **MRPP configuration > MRPP domain configuration > MRPP node mode config,** and the following page appears.You can configure the MRPP ring node mode to master or transit.

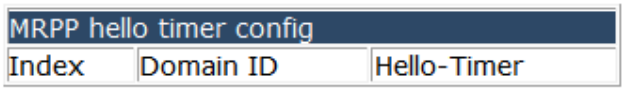




4.24.3.3 MRPP hello timer config.

Choose **MRPP configuration > MRPP domain configuration > MRPP hello timer config,** and the following page appears.You can set the MRPP hello timer range for the MRPP domain.



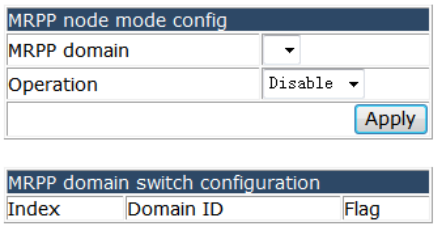


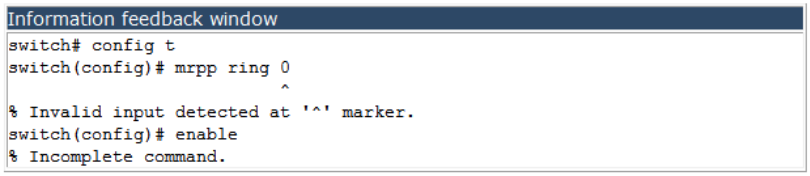
4.24.3.4 MRPP fail timer config.

Choose **MRPP configuration > MRPP domain configuration > MRPP fail timer config > MRPP fail timer config,** and the following page appears.You can configure the MRPP hello message fail timer range for MRPP domain.

4.24.3.5 MRPP domain switch config.

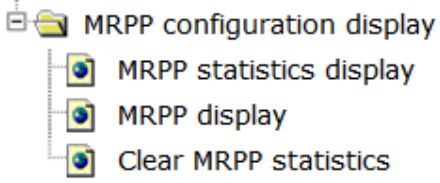
Choose **MRPP configuration > MRPP domain configuration > MRPP domain switch config,** and the following page appears.You can enable or disable the MRPP domain.





4.24.4 MRPP configuration display.

Choose **MRPP configuration > MRPP configuration display,** and the following page appears.There are "MRPP statistics display", "MRPP display", "Clear MRPP statistics", configuration web pages.



4.24.4.1 MRPP statistics display.

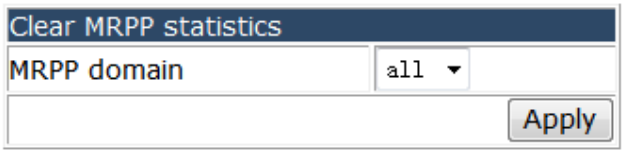
Choose **MRPP configuration > MRPP configuration display > MRPP statistics display,** and the following page appears.You can show the statistics information for each MRPP domain or for all domains.

4.24.4.2 MRPP display.

Choose **MRPP configuration > MRPP configuration display > MRPP display,** and the following page appears.You can show the configuration of the MRPP domain or all MRPP domains.

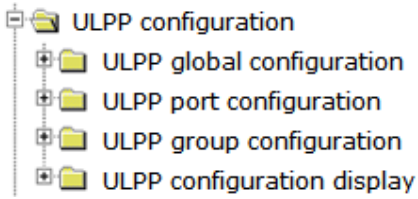
4.24.4.3 Clear MRPP statistics.

Choose **MRPP configuration > MRPP configuration display > Clear MRPP statistics,** and the following page appears.You can clear the statistics for each MRPP domain or all domains.



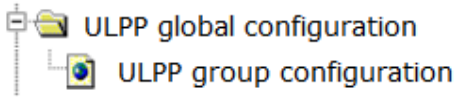
4.25 ULPP configuration.

Choose **ULPP configuration,** and the following page appears.There are "ULPP global configuration", "ULPP port configuration", "ULPP group configuration", "ULPP configuration display", configuration web pages.



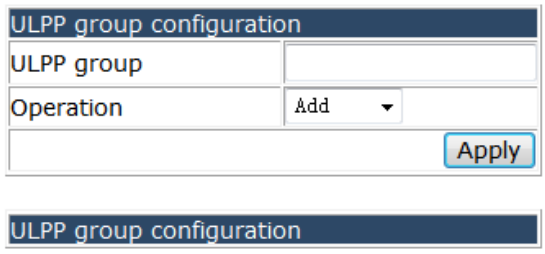
4.25.1 ULPP global configuration.

Choose **ULPP configuration > ULPP global configuration,** and the following page appears.



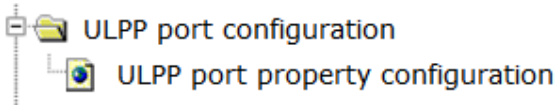
4.25.1.1 ULPP group configuration.

Choose **ULPP configuration > ULPP global configuration > ULPP group configuration,** and the following page appears.You can add or remove ULPP group.



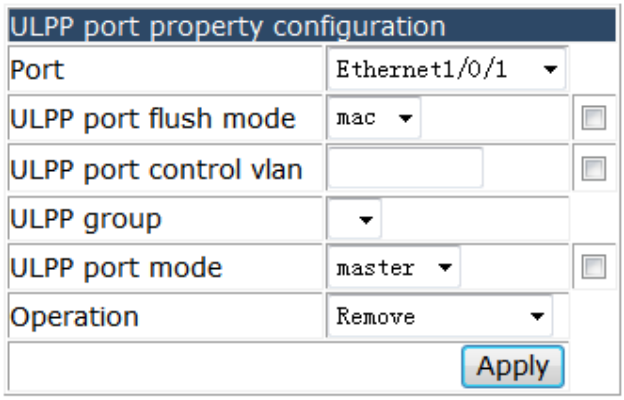
4.25.2 ULPP port configuration.

Choose **ULPP configuration > ULPP port configuration,** and the following page appears.



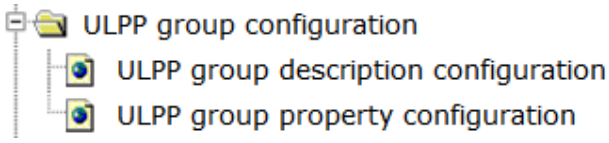
4.25.2.1 ULPP port property configuration.

Choose **ULPP configuration > ULPP port configuration > ULPP port property configuration,** and the following page appears.You can configure the property for ULPP port, the flush mode could be mac or arp, and you can set the port as the master port or slave port.



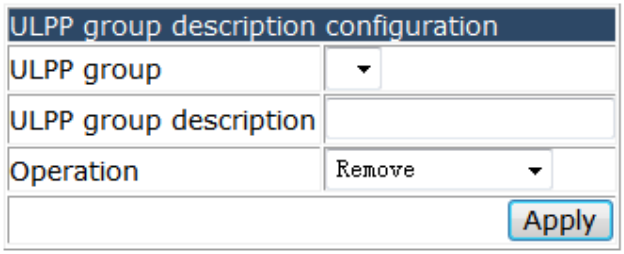
4.25.3 ULPP group configuration.

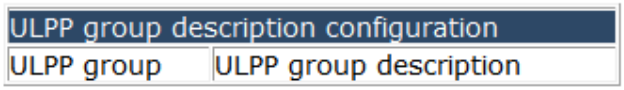
Choose **ULPP configuration > ULPP group configuration,** and the following page appears.There are "ULPP description configuration", "ULPP group property configuration", configuration web pages.



4.25.3.1 ULPP description configuration.

Choose **ULPP configuration > ULPP group configuration > ULPP description configuration,** and the following page appears.You can set description for ULPP group.

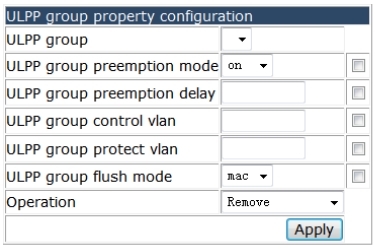


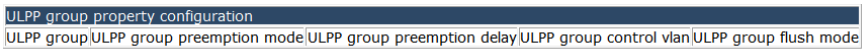


4.25.3.2 ULPP group property configuration.

Choose **ULPP configuration > ULPP group configuration > ULPP group property configuration,** and the following page appears.You can configure the property for ULPP group, the group preemption mode can be set to on or off, the flush mode could be mac or

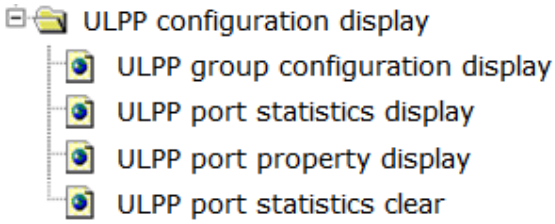
arp.





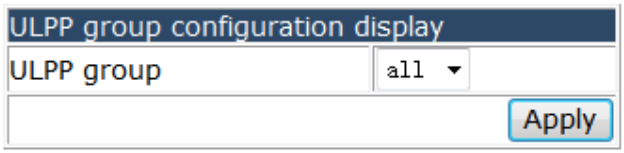
4.25.4 ULPP configuration display.

Choose **ULPP configuration > ULPP configuration display,** and the following page appears.There are "ULPP group configuration display", "ULPP port statistics display", "ULPP port property display", "ULPP port statistics clear", configuration web pages.



4.25.4.1 ULPP group configuration display.

Choose **ULPP configuration > ULPP configuration display > ULPP group configuration display,** and the following page appears.You can show the ULPP group configuration information.



4.25.4.2 ULPP port statistics display.

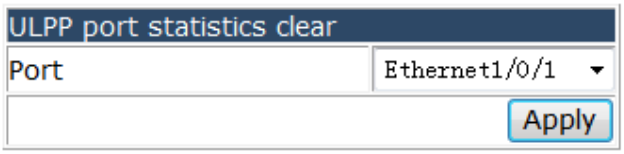
Choose **ULPP configuration > ULPP configuration display > ULPP port statistics display,** and the following page appears.You can show ULPP flush counter for each physical port or port-channel.

4.25.4.3 ULPP port property display.

Choose **ULPP configuration > ULPP configuration display > ULPP port property display,** and the following page appears.You can show ULPP flush-receive port list.

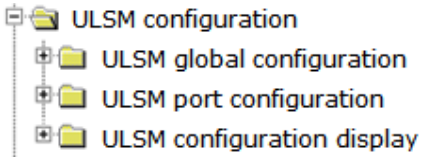
4.25.4.4 ULPP port statistics clear.

Choose **ULPP configuration > ULPP configuration display > ULPP port statistics clear,** and the following page appears.You can clear ULPP flush counter for each physical port or port-channel.



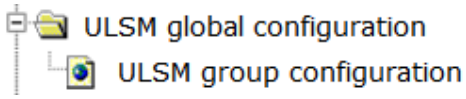
4.26 ULSM configuration.

Choose **ULSM configuration,** and the following page appears.There are "ULSM global configuration", "ULSM port configuration", "ULSM configuration display", configuration web pages.



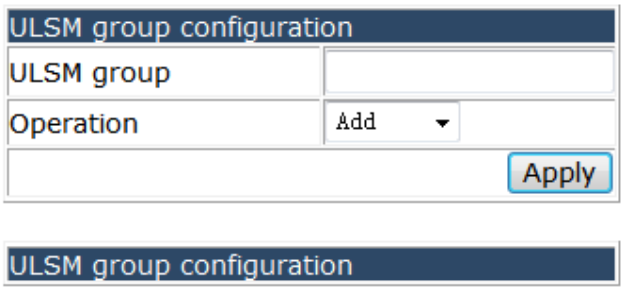
4.26.1 ULSM global configuration.

Choose **ULSM configuration > ULSM global configuration,** and the following page appears.



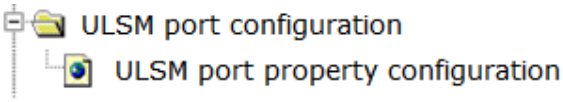
4.26.1.1 ULSM group configuration.

Choose **ULSM configuration > ULSM global configuration > ULSM group configuration,** and the following page appears.You can add or remove ULSM group.



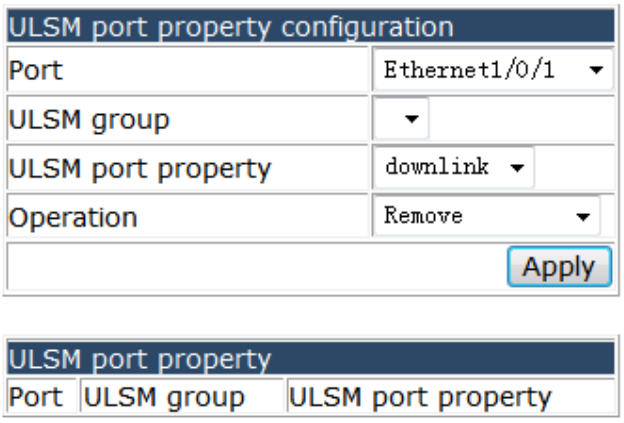
4.26.2 ULSM port configuration.

Choose **ULSM configuration > ULSM port configuration,** and the following page appears.



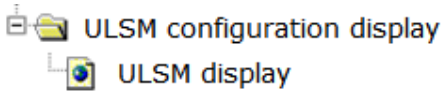
4.26.2.1 ULSM port property configuration.

Choose **ULSM configuration > ULSM port configuration > ULSM port property configuration,** and the following page appears.You can add or remove a physical port or port-channel to ULSM group and set the property as downlink or uplink.



4.26.3 ULSM configuration display.

Choose **ULSM configuration > ULSM configuration display,** and the following page appears.

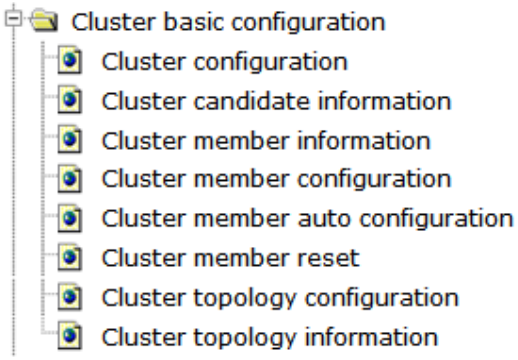


4.26.3.1 ULSM display.

Choose **ULSM configuration > ULSM configuration display > ULSM display,** and the following page appears.You can show the state of ULSM group.

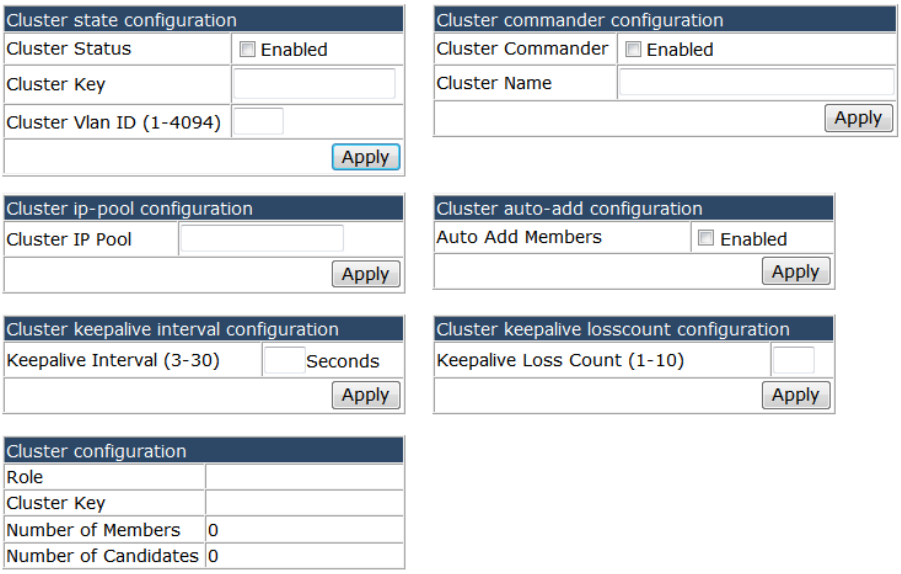
4.27 Cluster basic configuration.

Choose **Cluster basic configuration,** and the following page appears.There are "Cluster configuration", "Cluster candidate information", "Cluster member information", "Cluster member configuration", "Cluster member auto configuration", "Cluster member reset", "Cluster topology configuration", "Cluster topology information", configuration web pages.



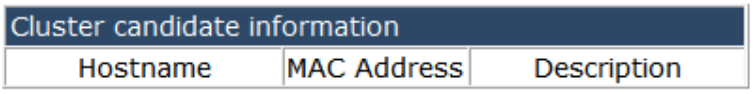
4.27.1 Cluster configuration.

Choose **Cluster basic configuration > Cluster configuration,** and the following page appears.You can enable cluster and configure key, VLAN ID, name, IP pool, auto add member, keepalive interval and loss count for the Cluster.



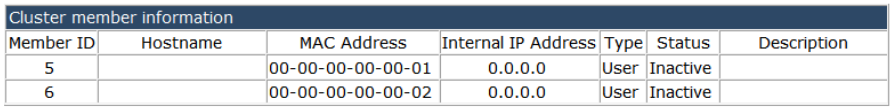
4.27.2 Cluster candidate information.

Choose **Cluster basic configuration > Cluster candidate information,** and the following page appears.You can see the Cluster candidate information.



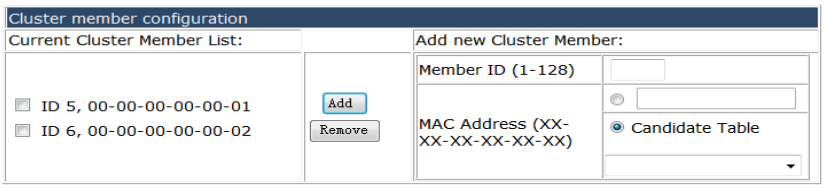
4.27.3 Cluster member information.

Choose **Cluster basic configuration > Cluster member information,** and the following page appears.You can see the Cluster member information.



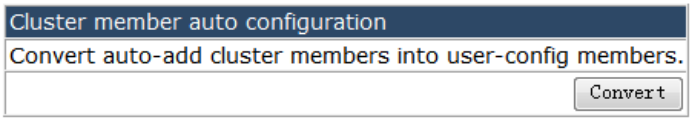
4.27.4 Cluster member configuration.

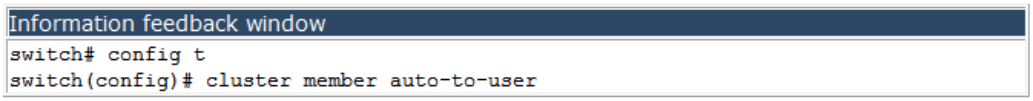
Choose **Cluster basic configuration > Cluster member configuration,** and the following page appears.You can add or remove member to the Cluster group.



4.27.5 Cluster member auto configuration.

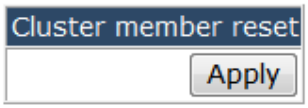
Choose **Cluster basic configuration > Cluster member auto configuration,** and the following page appears.You can Convert auto-add cluster members into user-config members vice versa.





4.27.6 Cluster member reset.

Choose **Cluster basic configuration > Cluster member reset,** and the following page appears.You can rest the member switch by using this command on command switch.



4.27.7 Cluster topology configuration.

Choose **Cluster basic configuration > Cluster topology configuration,** and the following page appears.You can configure the Cluster topology.

4.27.8 Cluster topology information.

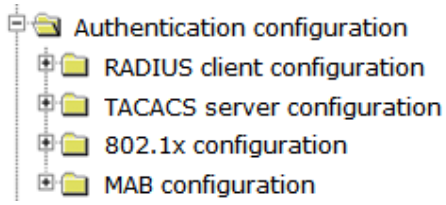
Choose **Cluster basic configuration > Cluster topology information,** and the following page appears.You can show the cluster topology information and clear the cluster table.

Cluster topology information							
Serial Number	Role	Hostname	MAC Address	Upstream Local Port	Upstream Remote Port	Leaf Node	Description
-	Commander	switch	00-e0-53-16-d0-01	-root-	-root-	-	FR-S3028PETF-C
1	Unknow		00-00-00-00-00-01			Yes	
2	Unknow		00-00-00-00-00-02			Yes	

Clear cluster table. Clear

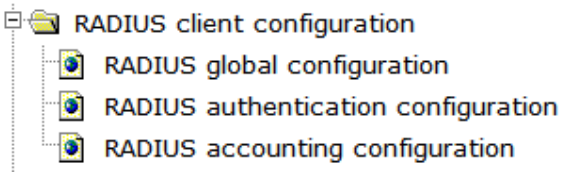
4.28 Authentication configuration.

Choose **Authentication configuration,** and the following page appears.There are "RADIUS client configuration", "TACACS server configuration", "802.1x configuration", "MAB configuration", configuration web pages.



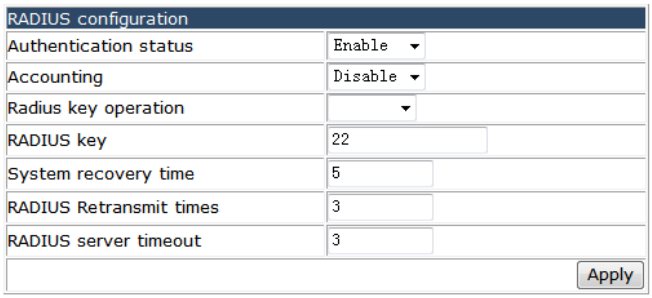
4.28.1 RADIUS client configuration.

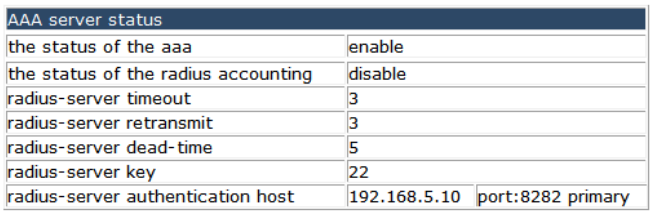
Choose **Authentication configuration > RADIUS client configuration,** and the following page appears.There are "RADIUS global configuration", "RADIUS authentication configuration", "RADIUS accounting configuration", configuration web pages.

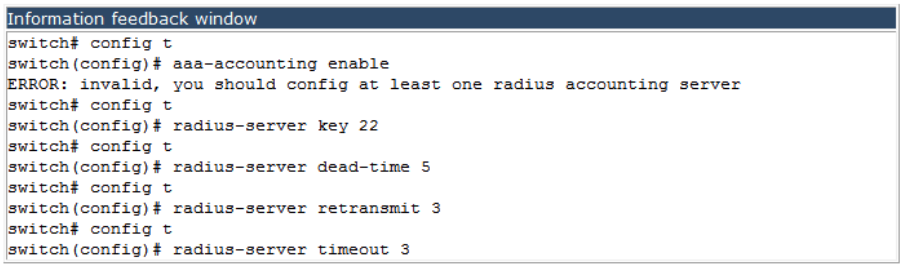


4.28.1.1 RADIUS global configuration.

Choose **Authentication configuration > RADIUS client configuration > RADIUS global configuration,** and the following page appears.You can set the radius global configuration.

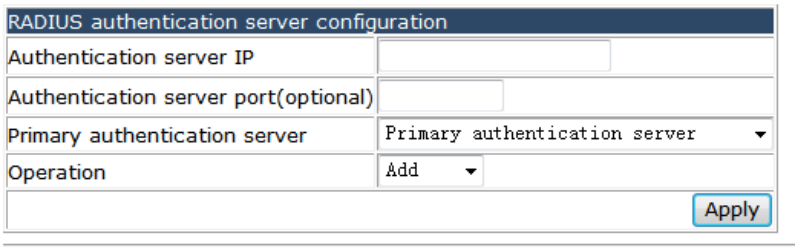






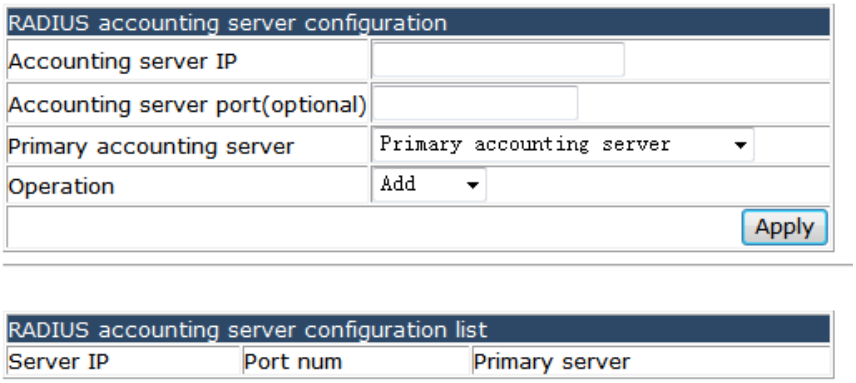
4.28.1.2 RADIUS authentication configuration.

Choose **Authentication configuration > RADIUS client configuration > RADIUS authentication configuration,** and the following page appears.You can set the information of the primary and non-primary Radius authentication server.



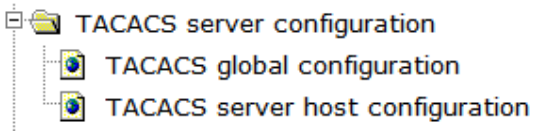
4.28.1.3 RADIUS accounting configuration.

Choose **Authentication configuration > RADIUS client configuration > RADIUS accounting configuration, a**nd the following page appears.You can set the information of the primary and non-primary Radius accounting server.



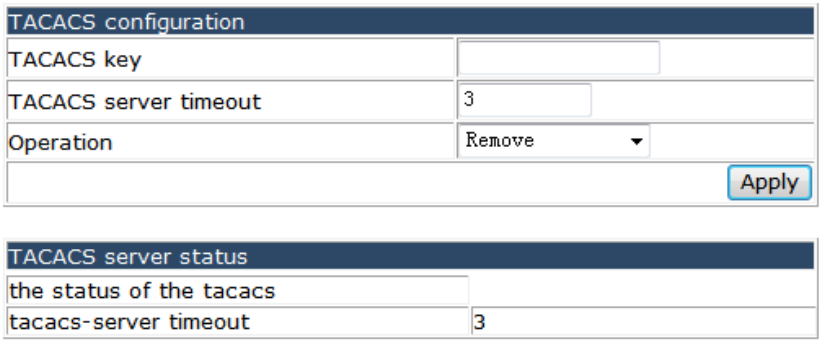
4.28.2 TACACS server configuration.

Choose **Authentication configuration > TACACS server configuration,** and the following page appears.There are "TACACS global configuration", "TACACS server host configuration", configuration web pages.



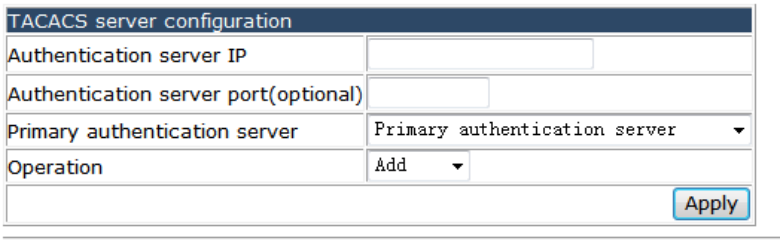
4.28.2.1 TACACS global configuration.

Choose **Authentication configuration > TACACS server configuration > TACACS global configuration,** and the following page appears.You can set the TACACS server configuration.



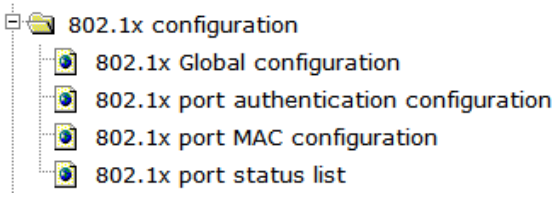
4.28.2.2 TACACS server host configuration.

Choose **Authentication configuration > TACACS server configuration > TACACS server host configuration,** and the following page appears.You can set the information of the primary and non-primary TACACS authentication server.



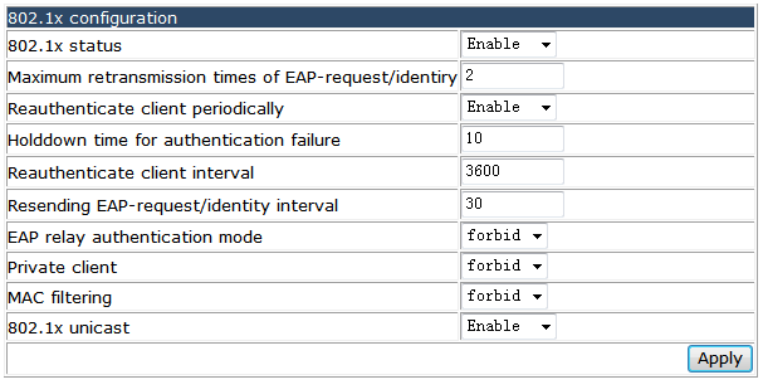
4.28.3 802.1x configuration.

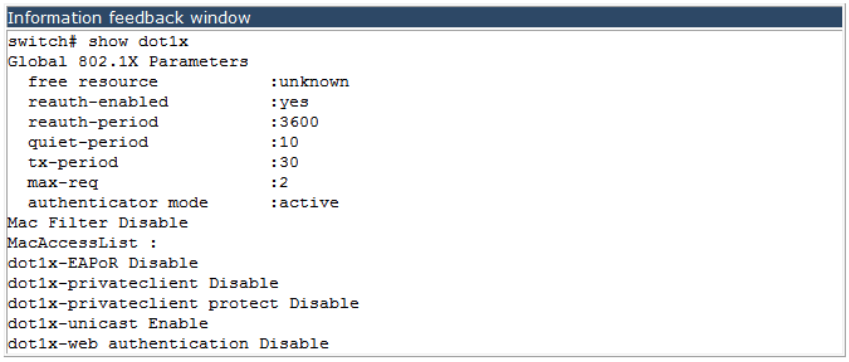
Choose **Authentication configuration > 802.1x configuration,** and the following page appears.There are "802.1x Global configuration", "802.1x port authentication configuration", "802.1x port MAC configuration", "802.1x port status list", configuration web pages.



4.28.3.1 802.1x Global configuration.

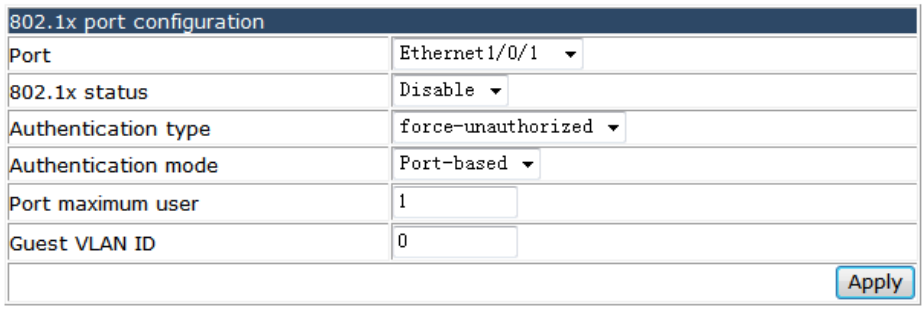
Choose **Authentication configuration > 802.1x configuration > 802.1x Global configuration,** and the following page appears.You can set the 802.1X global configuration, the EAP relay authentication mode, Private client and MAC filtering can be set to permit or forbid.

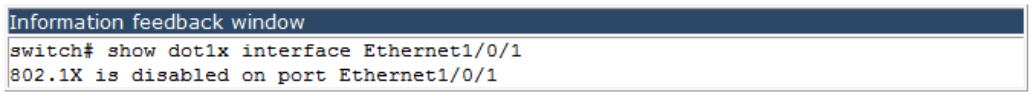




4.28.3.2 802.1x port authentication configuration.

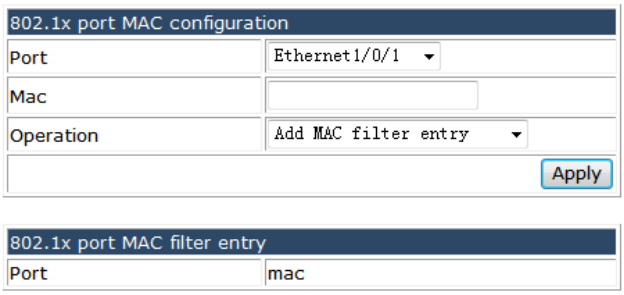
Choose **Authentication configuration > 802.1x configuration > 802.1x port authentication configuration,** and the following page appears.You can configure the 802.1x authentication for each port, the Authentication mode can be force-unauthorized, Auto(802.1X) or force-authorized, the Authentication mode can be Port-based or MAC-based.





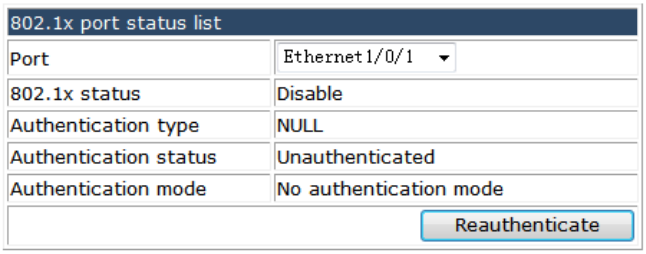
4.28.3.3 802.1x port MAC configuration list.

Choose **Authentication configuration > 802.1x configuration > 802.1x port MAC configuration,** and the following page appears.You can set a MAC address to add MAC filter entry or remove MAC filter entry for each port.



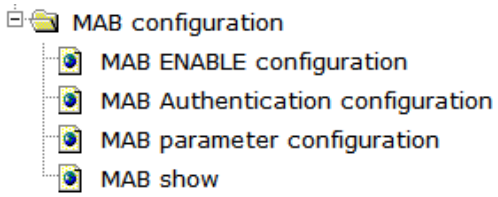
4.28.3.4 802.1x port status list.

Choose **Authentication configuration > 802.1x configuration > 802.1x port status list,** and the following page appears.You can show the 802.1X authentication status of each port or reauthenticate the port.



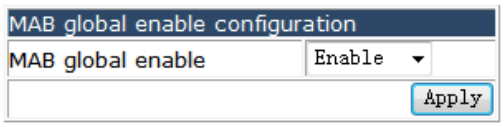
4.28.4 MAB configuration.

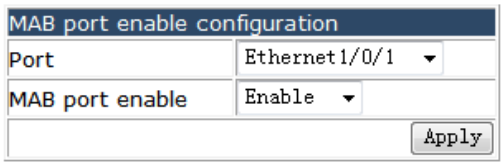
Choose **Authentication configuration > MAB configuration,** and the following page appears.There are "MAB ENABLE configuration", "MAB Authentication configuration", "MAB parameter configuration", "MAB show", configuration web pages.



4.28.4.1 MAB ENABLE configuration.

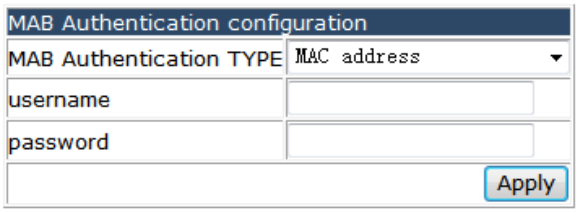
Choose **Authentication configuration > MAB configuration > MAB ENABLE configuration,** and the following page appears.You can enable or disable the mac-authentication-bypass function for global or each port.





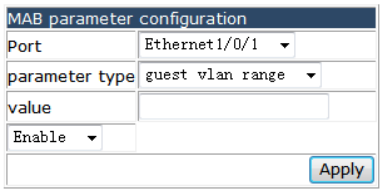
4.28.4.2 MAB Authentication configuration.

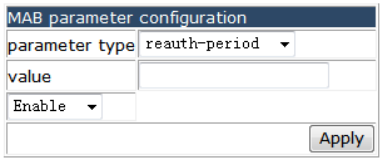
Choose **Authentication configuration > MAB configuration > MAB Authentication configuration,** and the following page appears.You can set the MAB authentication type to MAC address or username and password.

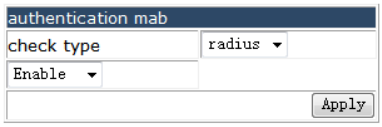


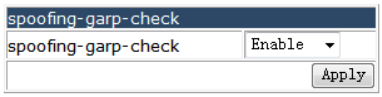
4.28.4.3 MAB parameter configuration.

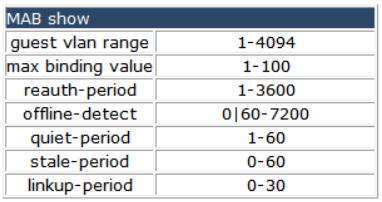
Choose **Authentication configuration > MAB configuration > MAB parameter configuration,** and the following page appears.You can set MAB parameter.









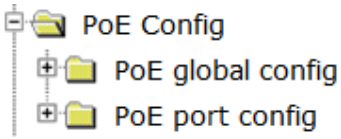


4.28.4.4 MAB show.

Choose **Authentication configuration > MAB configuration > MAB show,** and the following page appears.You can show the MAB information for each port or all ports.

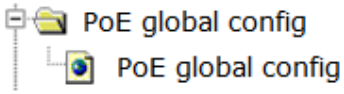
4.29 PoE Config.

Choose **PoE Config,** and the following page appears.There are "PoE global config ","PoE port config", configuration web pages.



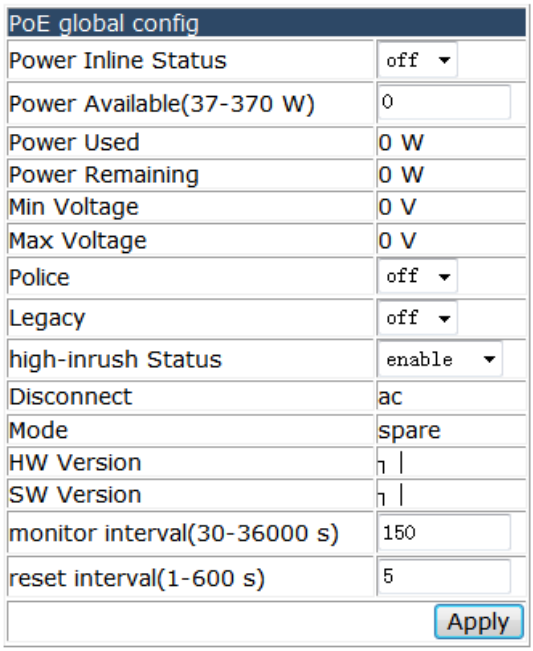
4.29.1 PoE global config.

Choose **PoE Config > PoE global config,** and the following page appears.There are "PoE global config", configuration web pages.



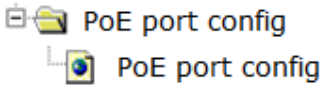
4.29.1.1 PoE global config

1.Choose **PoE Config > PoE global config> PoE global config,** and the following page appears.You can set the POE global configuration..



4.29.2 PoE port config.

Choose **PoE Config > PoE port config,** and the following page appears.There are "**PoE port config**", configuration web pages.



4.29.2.1 PoE port config

2.Choose **PoE Config > PoE port config > PoE port config,** and the following page appears.You can set the POE parameters for each port , the status could be auto, static and disable, the priority could be low, high or critical.

PoE port config

Interface	Status	Priority	monitor status
Ethernet1/0/1	auto	low	off

Apply

Max Power

Interface	Max Power(1-30000mW)
Ethernet1/0/1	30000 mW

Apply

Time range name

Interface	Time range name
Ethernet1/0/1	

Apply

Unset Time range name

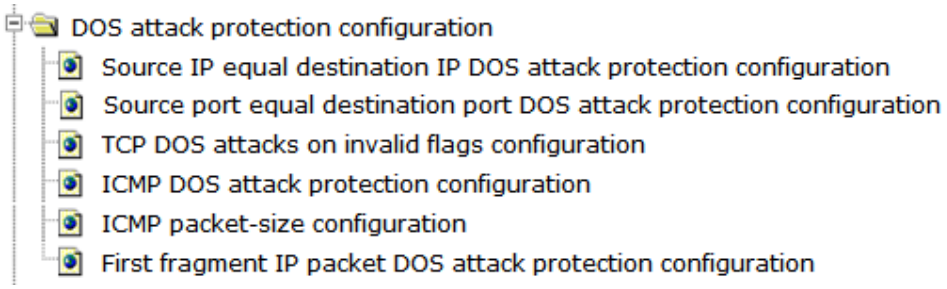
Interface: Ethernet1/0/1

Default

Interface	Status	Oper	Power(mW)	Max Power(1-30000mW)	Current(mA)	Volt(V)	Priority	Class	Time range name
Ethernet1/0/1	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/2	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/3	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/4	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/5	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/6	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/7	disable	faulty	-1	0	-1	-1	critical	-1	NULL

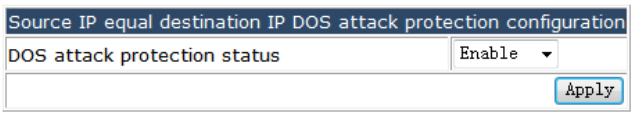
4.30 DOS attack protection configuration.

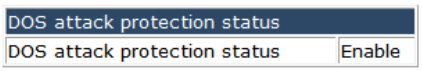
Choose **DOS attack protection configuration,** and the following page appears.There are "Source IP equal destination IP DOS attack protection configuration", "Source port equal destination port DOS attack protection configuration", "TCP DOS attacks in invalid flags configuration", "ICMP DOS attack protection configuration, "ICMP packet-size configuration", "First fragment IP packet DOS attack protection configuration", configuration web pages.

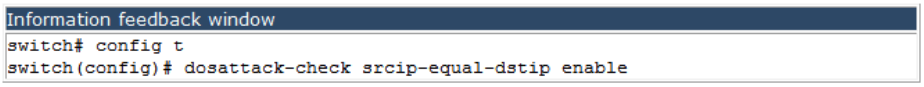


4.30.1 Source IP equal destination IP DOS attack protection configuration.

Choose **DOS attack protection configuration > Source IP equal destination IP DOS attack protection configuration,** and the following page appears.You can enable or disable the protection function for DOS attack with source IP equal destination IP.

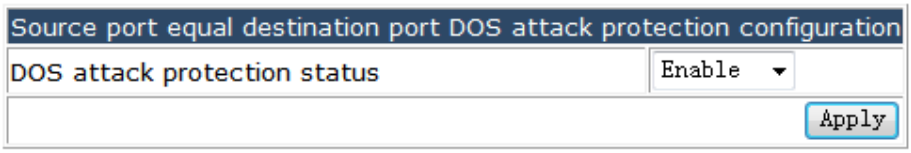


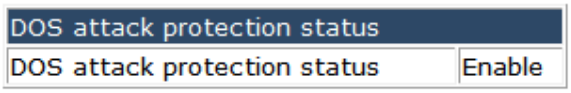




4.30.2 Source port equal destination port DOS attack protection configuration.

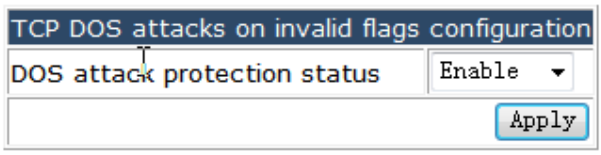
Choose **DOS attack protection configuration > Source port equal destination port DOS attack protection configuration,** and the following page appears.You can enable or disable the protection function for DOS attack with source port equal destination port.

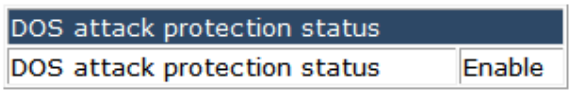




4.30.3 TCP DOS attacks on invalid flags configuration.

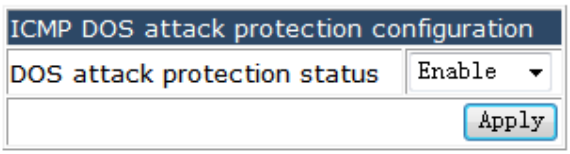
Choose **DOS attack protection configuration > TCP DOS attacks on invalid flags configuration,** and the following page appears.You can enable or disable the protection function for TCP DOS attacks on invalid flags.

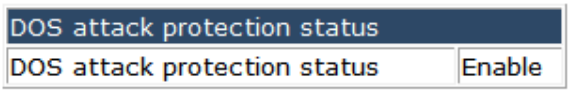




4.30.4 ICMP DOS attack protection configuration.

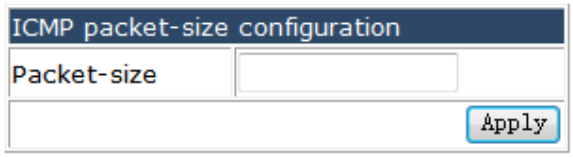
Choose **DOS attack protection configuration > ICMP DOS attack protection configuration,** and the following page appears.You can enable or disable the protection function for ICMP DOS attack.





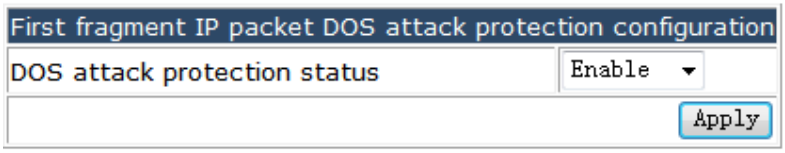
4.30.5 ICMP packet-size configuration.

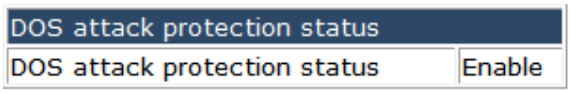
Choose **DOS attack protection configuration > ICMP packet-size configuration,** and the following page appears.You can set the ICMP packet-size for ICMP DOS attack protection.



4.30.6 First fragment IP packet DOS attack protection configuration.

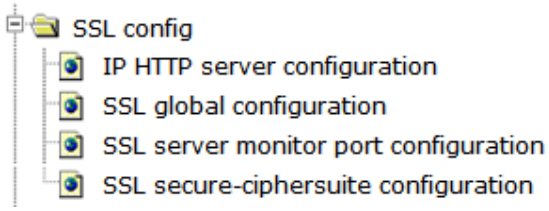
Choose **DOS attack protection configuration > First fragment IP packet DOS attack protection configuration,** and the following page appears.You can enable or disable the protection function for first fragment IP packet DOS attack.





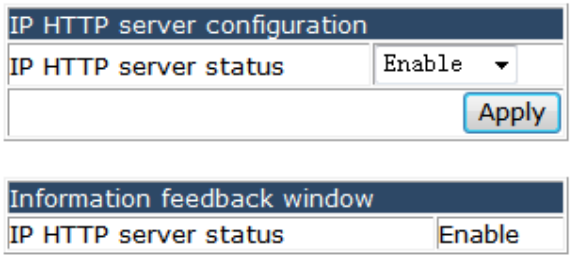
4.31 SSL config.

Choose **SSL config,** and the following page appears.There are "IP HTTP server configuration", "SSL global configuration", "SSL server monitor port configuration", "SSL secure-ciphersuite configuration", configuration web pages.



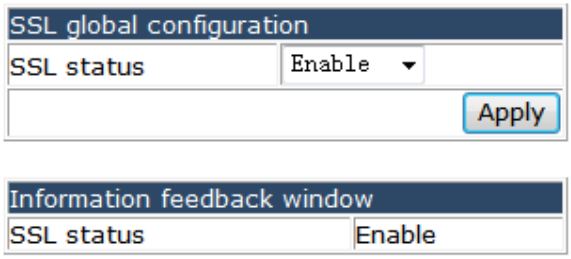
4.31.1 IP HTTP server configuration.

Choose **SSL config > IP HTTP server configuration,** and the following page appears.You can enable or disable the IP HTTP server.



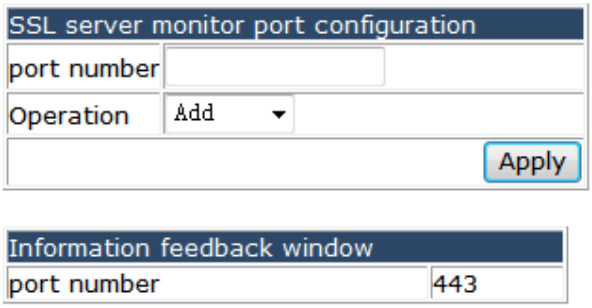
4.31.2 SSL global configuration.

Choose **SSL config > SSL global configuration,** and the following page appears.You can enable or disable the SSL function.



4.31.3 SSL server monitor port configuration.

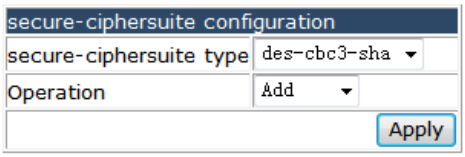
Choose **SSL config > SSL server monitor port configuration,** and the following page appears.You can set the SSL server monitor port.

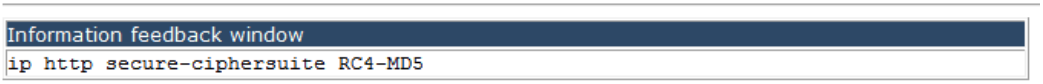


4.31.4 SSL secure-ciphersuite configuration.

Choose **SSL config > SSL secure-ciphersuite configuration,** and the following page

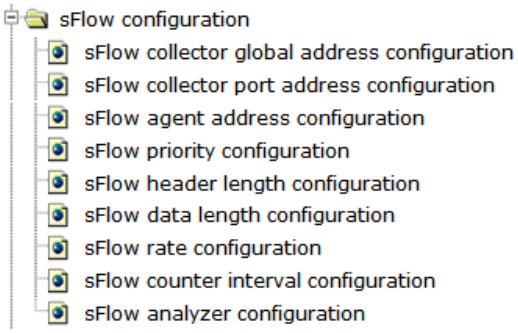
appears.You can configure the SSL secure-ciphersuite type to des-cbc3-sha, rc4-128-sha or des-cbc-sha.





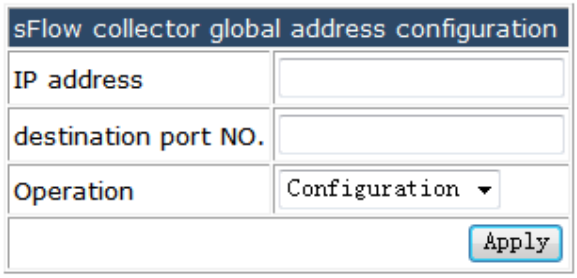
4.32 sFLOW configuration.

Choose **sFLOW configuration,** and the following page appears.There are "sFLOW collector global address configuration", "sFLOW collector port address configuration", "sFLOW agent address configuration", "sFLOW priority configuration", "sFLOW header length configuration", "sFLOW data length configuration", "sFLOW rate configuration", "sFLOW counter interval configuration", "sFLOW analyzer configuration", configuration web pages.



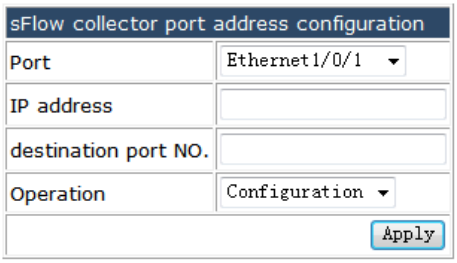
4.32.1 sFLOW collector global address configuration.

Choose **sFLOW configuration > sFLOW collector global address configuration,** and the following page appears.You can set the sFLOW collector global address and destination port.



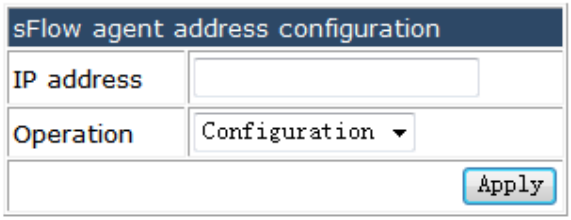
4.32.2 sFLOW collector port address configuration.

Choose **sFLOW configuration > sFLOW collector port address configuration,** and the following page appears.You can set the IP address and destination port for each physical port.



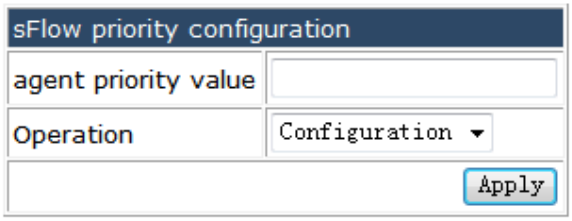
4.32.3 sFLOW agent address configuration.

Choose **sFLOW configuration > sFLOW agent address configuration,** and the following page appears.You can set the address of the sFLOW agent.



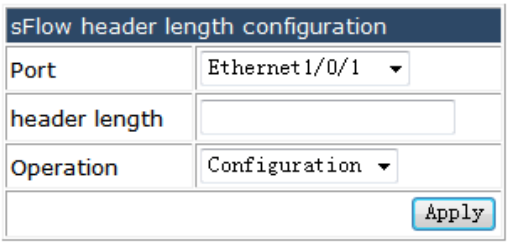
4.32.4 sFLOW priority configuration.

Choose **sFLOW configuration > sFLOW priority configuration,** and the following page appears.You can set the priority of the sFLOW agent.



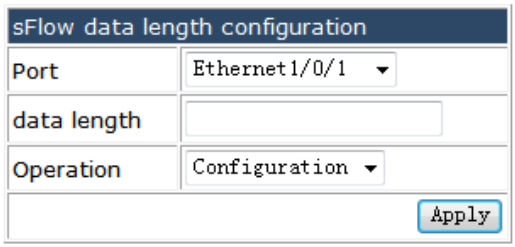
4.32.5 sFLOW header length configuration.

Choose **sFLOW configuration > sFLOW header length configuration,** and the following page appears.You can set the sFLOW header length.



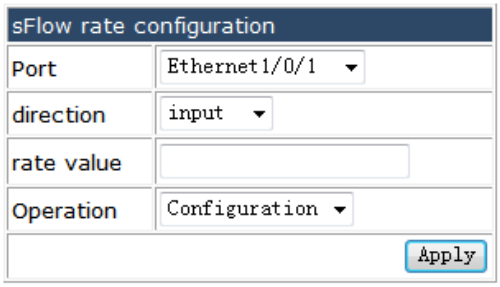
4.32.6 sFLOW data length configuration.

Choose **sFLOW configuration > sFLOW data length configuration,** and the following page appears.You can set the sFLOW data length.



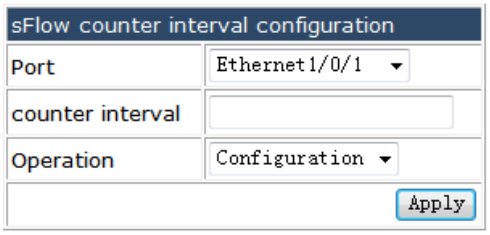
4.32.7 sFLOW rate configuration.

Choose **sFLOW configuration > sFLOW rate configuration,** and the following page appears.You can set sFLOW rate value for direction input and output.



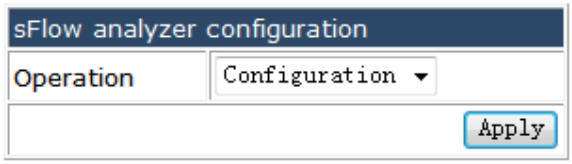
4.32.8 sFLOW counter interval configuration.

Choose **sFLOW configuration > sFLOW counter interval configuration,** and the following page appears.You can set sFLOW counter interval.



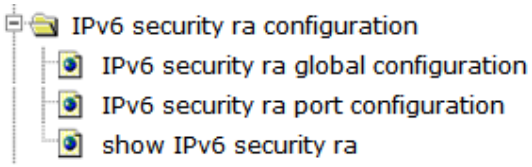
4.32.9 sFLOW analyzer configuration.

Choose **sFLOW configuration > sFLOW analyzer configuration,** and the following page appears.You can configure or remove the slfowtrend sFLOW analyzer.



4.33 IPv6 security ra configuration.

Choose **IPv6 security ra configuration,** and the following page appears.There are "IPv6 security ra global configuration", "IPv6 security ra port configuration", "Show IPv6 security ra", configuration web pages.



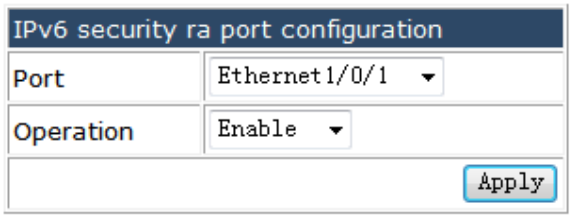
4.33.1 IPv6 security ra global configuration.

Choose **IPv6 security ra configuration > IPv6 security ra global configuration,** and the following page appears.You can enable or disable the IPv6 security ra function..

4.33.2 IPv6 security ra port configuration.

Choose **IPv6 security ra configuration > IPv6 security ra port configuration,** and the

following page appears.You can enable or disable the IPv6 security ra for each physical port.

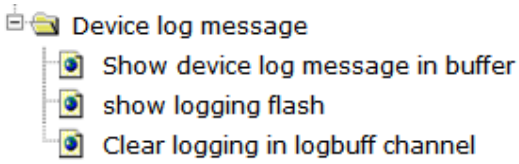


4.33.3 Show IPv6 security ra.

Choose **IPv6 security ra configuration > Show IPv6 security ra,** and the following page appears.You can show the IPv6 security state for each port or all ports.

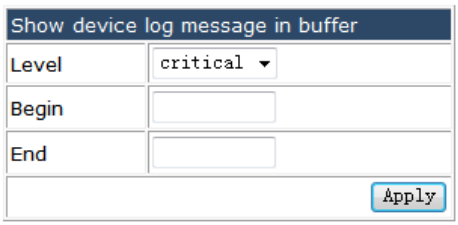
4.34 Device log message.

Choose **Device log message,** and the following page appears.There are "Show device log message in buffer", "Show logging flash", "Clear longing in logbuff channel", configuration web pages.



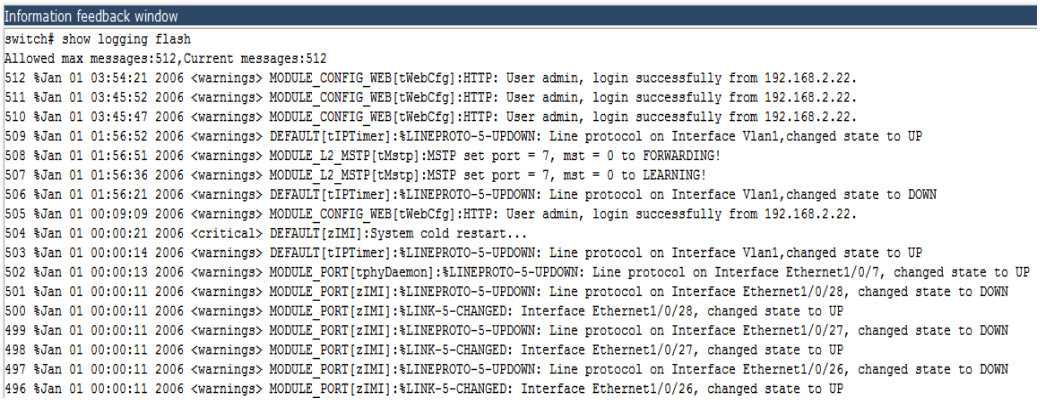
4.34.1 Show device log message in buffer.

Choose **Device log message > Show device log message in buffer,** and the following page appears.You can show the device log message with level critical or warning, and you can choose the ID range of the message.



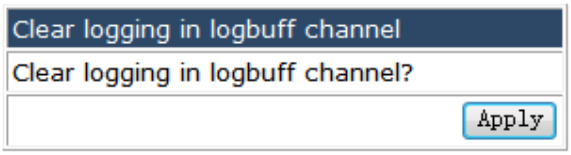
4.34.2 Show logging flash.

Choose **Device log message > Show logging flash,** and the following page appears.You can show the logging flash.



4.34.3 Clear logging in logbuff channel.

Choose **Device log message > Clear longing in logbuff channel,** and the following page appears.You can clear the logging in the logbuff channel..



Appendix: Technical Specifications

Specification		
Standards		IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3az, IEEE802.3ae.
Number of Ports		24 x 10/100/1000Mbps Auto-Negotiation ports 4 x 1000/10000Mbps SFP+ ports
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) 10GBase-LR 10GBase-SR
capability	Store-and-Forward	Supports
	Switching Capacity	128Gbps
	MAC Address Learning	Automatically learning, automatically Update 16K Table
Environment		Operating Temperature: 0□~40□ Storage Temperature: -40□~70□ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~95% non-condensing
LED indicators	Per-Port	Link/Act : 10/100/10000Mbps:Green
	Other	Power：Green
Dimensions (W × D × H)		440x330x44mm (19 metal case)
Power		AC 100V~240V 50/60HZ 1A (Internal Power supply)

MORRELL®
A TRUSTED GERMAN NAME

www.morrelltelecom.com
sales@morrelltelecom.com
morrelltelecom