ORIGO

# L3 Switch Series (PoE)

# User Manual

# Table of Contents

# Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device.
- Connecting to the network.
- Starting the web-based configuration utility.

## Power

### Connecting to Power

Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.

Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.


Figure 1. Rear View AC Power Socket.

## Connecting to the Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer.

2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.

3. Repeat Step 1 and Step 2 for each device to connect to the switch.

We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.

Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

## Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility. Be sure to disable any pop-up blocker.

Browser Restrictions:

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.

2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.

When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.2.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.

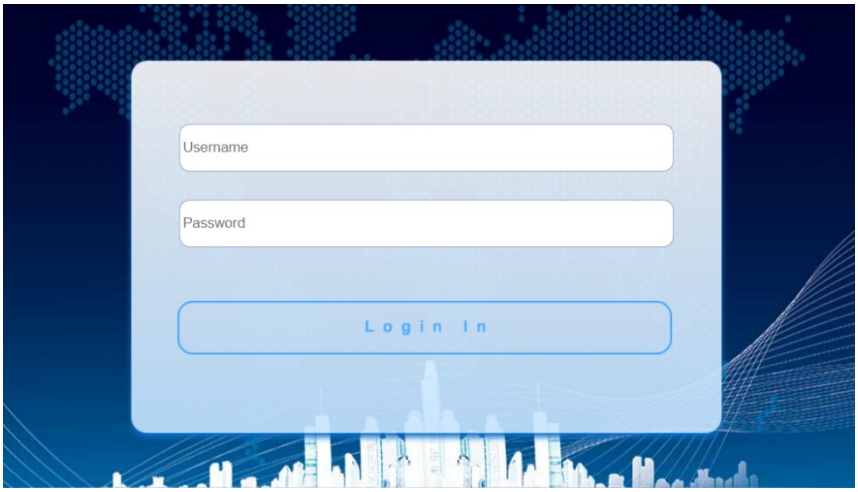



Figure 2. Login Window

## Logging In

The default username is admin and the default password is admin. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

1. Enter the default user ID (admin) and the default password (admin).
2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin) it is recommended that you change your password immediately.

When the login attempt is successful, the System Information window displays.

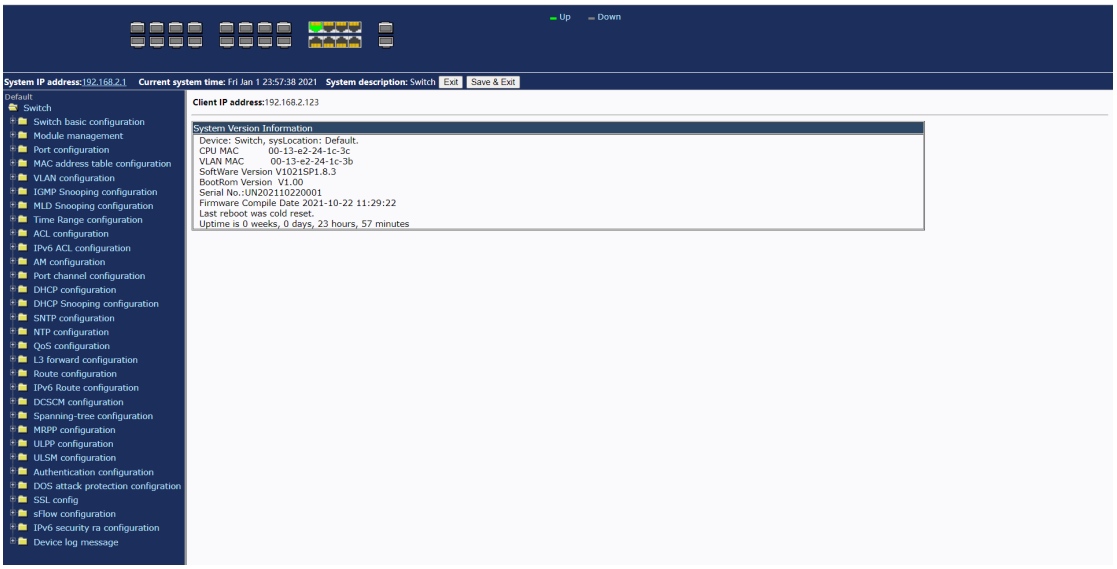



Figure 3. System Information.

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the Launching the Configuration Utility section in the Administration Guide for additional information.

## Logging Out

By default, the application logs out after ten minutes of inactivity.

To logout, click Logout in the top right corner of any page. The system logs out of the device.
When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

# Web-based Switch Configuration

The smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

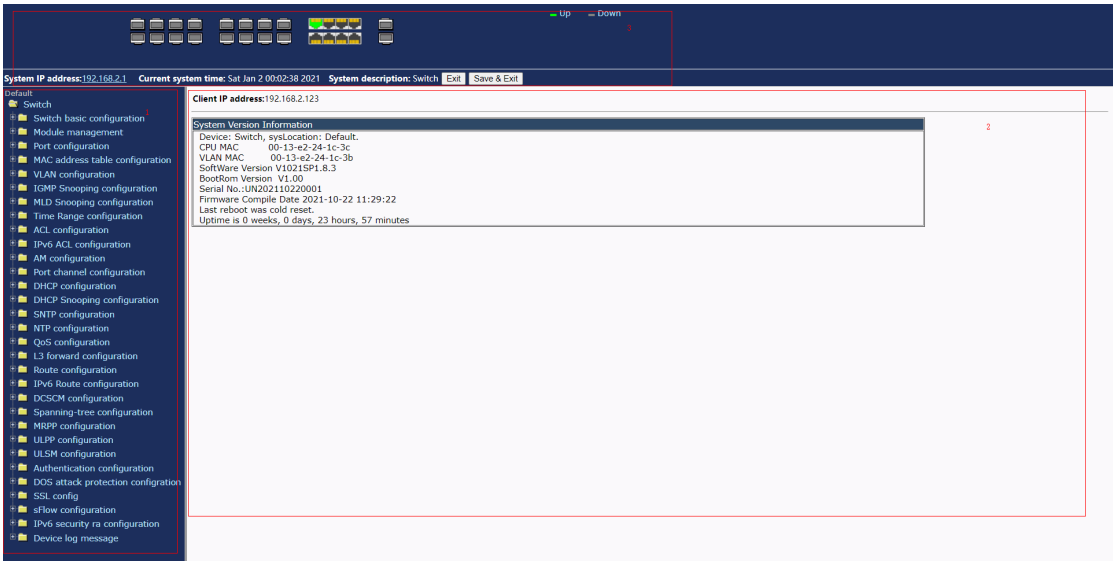



Figure 4. User Interface.

# Console Port Interface

The PoE smart switch has a monitor port (Console port). Rate 9600bps, standard RJ45 plug.

Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:

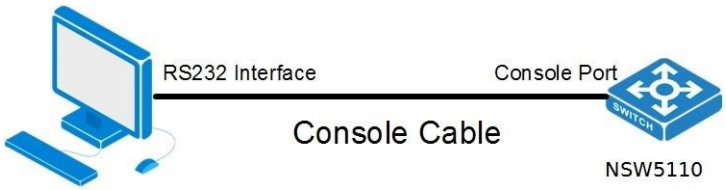



Figure 5.

The RJ45 connector used by the Console port is shown in the figure below, and the RJ45 plug corresponds to the RJ45 socket, from left to right numbered from 1 to 8.

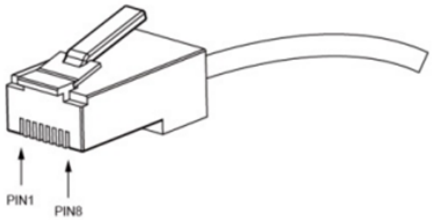



Figure 6.

This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug(DB25) and 9-hole plug(DB9), RJ45 head into the switch's console port socket, DB25 and DB9 can be used according to the requirements of the terminal serial port, the cable internal connection schematic as follows:

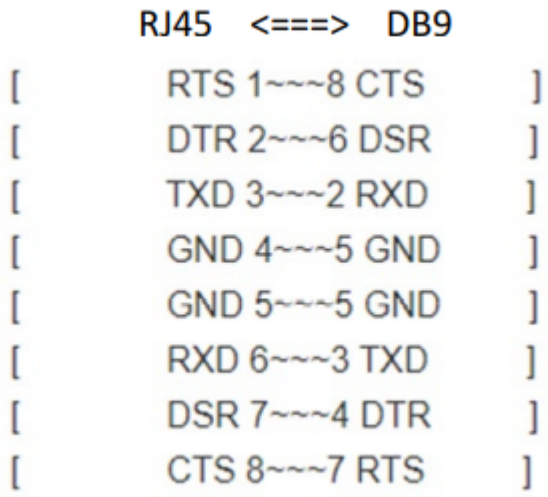



Figure 7.

# 1. Switch basic configuration

## 1.1 Switch basic configuration

### 1.1.1 Login user configuration

Login user management module, users in this module can add or delete user operations.

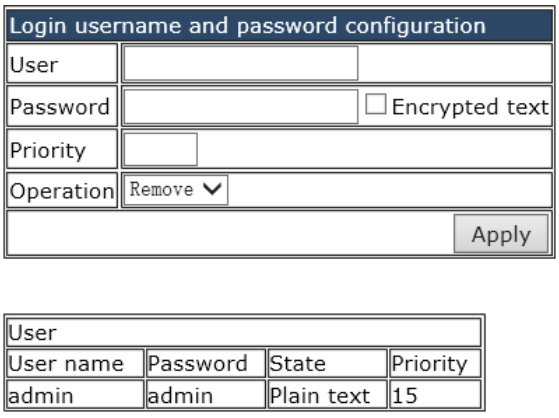



Figure 8.

| | | |
|---|---|---|
| **User** | User name to operate, 1-32 characters. | |
| **Password** | User password, choose the password encryption, otherwise no encryption of 1-32 characters. | |
| **Priority** | Used to specify permission level, default level 15. | |
| **Operation** | Add | Create new users. |

| | | |
|---|---|---|
| | Remove | Delete the specified user (password and priority can not be entered). |

### 1.1.2 Login user authentication method configuration

Login user authentication method configuration module, the user can configure console.vty.web authentication method used in login, authentication method can be any one or combination of Local.RADIUS and TACACS.preferences from left to right when the login method is combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as you pass an authentication method, the user can log in. AAA functions and RADIUS servers should be configured before using RADIUS authentication. If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.

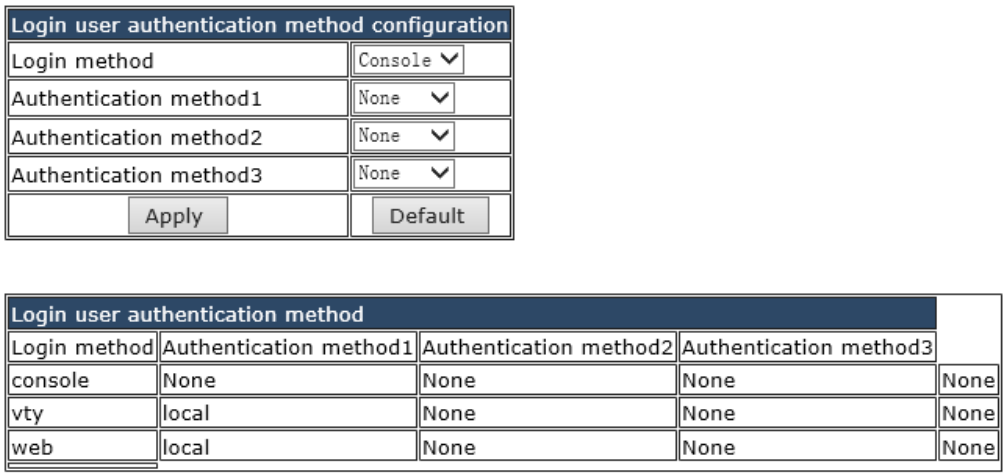



Figure 9.

| Login method | Authentication method | |
|---|---|---|
| **console** | **local** | Authentication using the local user account database. |
| **vty** | **radius** | Authentication using remote Radius server. |
| **web** | **tacacs** | Authentication using remote Tacacs server. |
| **Default** | Default console no authentication, vty and web local authentication. | |

### 1.1.3 Logging user Security IP management

Login user security IP configuration module, where users can configure the security IP. IPv6 address for login switch, or configure access control list.

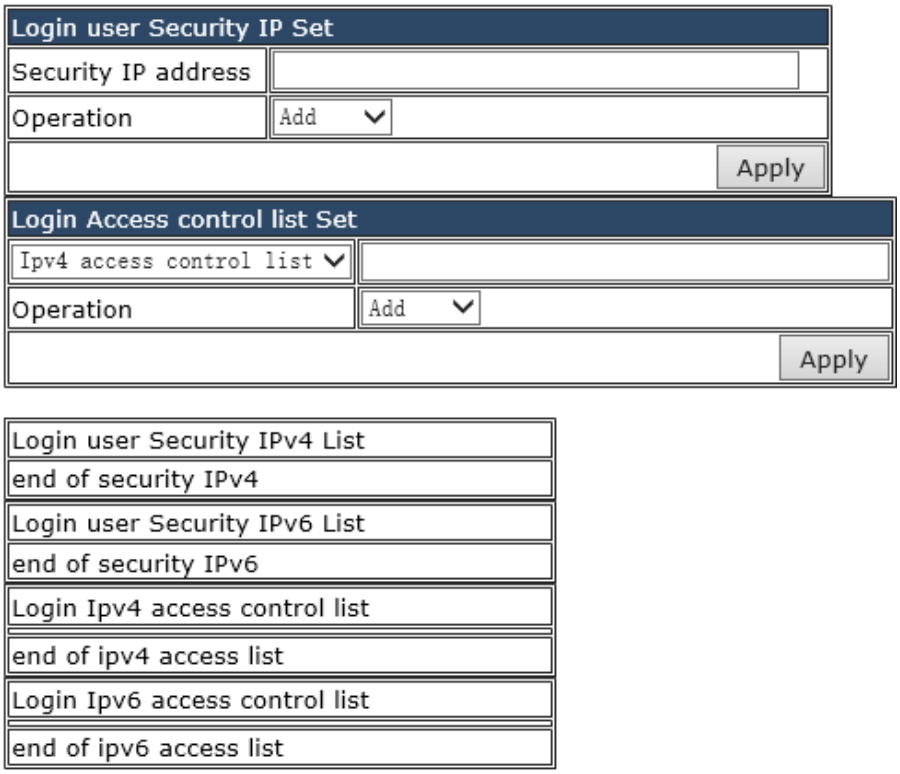



Figure 10.

| | | |
|---|---|---|
| **Security IP address** | Fill in the specified security IP or IPv6 address (the access control list is valid until the IPv6 address is filled in). | |
| **IPv4/IPv6 access control list** | Standard access control list number, scope 1-64. | |
| **Operation** | Add | Add address or list number. |
| | Remove | Delete address or list number. |

### 1.1.4 Basic configuration

Basic configuration module, in which users can configure switch current time, exit privilege mode timeout and switch name respectively.

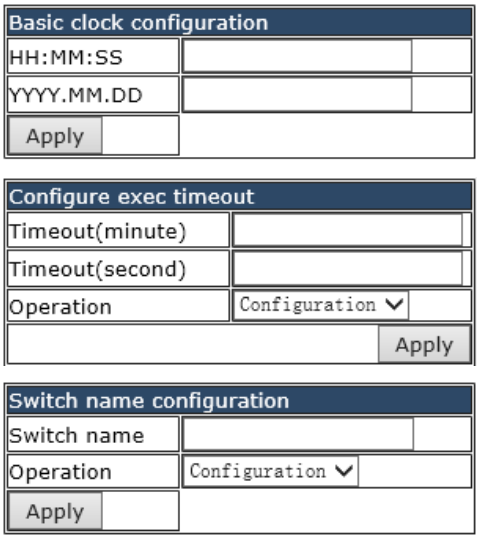



Figure 11.

| | |
|---|---|
| **HH:MM:SS** | Current time, format: hours:minutes:seconds. |
| **YYYY.MM.DD** | Current date, format: Year.Month.Day. |

| | | |
|---|---|---|
| **Timeout (minute)** | Exit privilege mode timeout score 0-35791. | |
| **Timeout (second)** | Seconds of exit privilege mode timeout (not set separately), 0-59 seconds. | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Restore default (default timeout: 10 minutes). |

| | | |
|---|---|---|
| **Switch name** | Fill in the new name of the switch to be changed, 1-64 characters. | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Do recovery default (default name: Switch). |

### 1.1.5 Save current running-configuration

Save the current configuration module, the user can save the current set configuration, can also leave the factory initial settings restart, but also choose whether to save the current set configuration before restart.

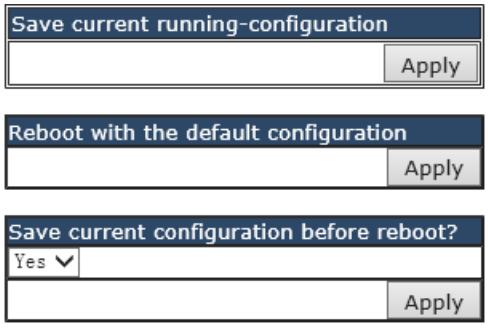



Figure 12.

# 1.2 SNMP authentication

## 1.2.1 SNMP authentication

### 1.2.1.1 User

SNMP user management module, users can add or delete SNMP user operations in this module.

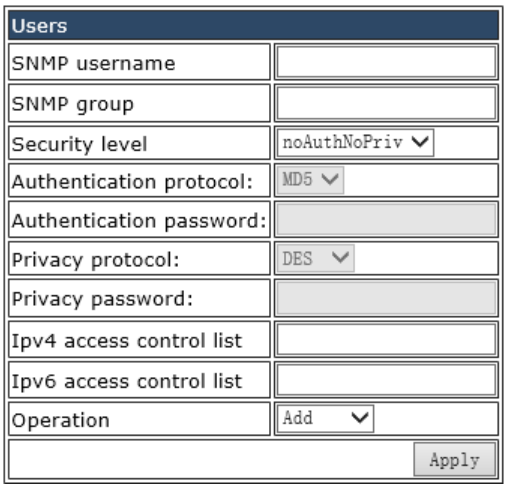



Figure 13.

| | | |
|---|---|---|
| **SNMP username** | User name to operate, 1-32 characters. | |
| **SNMP group** | User group to join, 1-32 characters. | |
| **Security level** | noAuthNoPriv | Uncertified non-encrypted level. |
| | authNoPriv | Authentication but not encryption level. |
| | authpriv | Authentication and encryption level. |
| **Authentication protocol:** | MD5 | HMAC MD5 algorithm for authentication. |
| | SHA | Authentication uses HMAC SHA algorithms. |
| **Authentication password:** | Password for authentication. | |
| **Privacy protocol:** | DES | Encryption DES algorithm. |
| | AES | Encryption AES algorithm. |
| | 3DES | Encryption with 3DES algorithm. |
| **Privacy password:** | Password for encryption. | |
| **Ipv4 access control list** | Standard IPv4 access control list number, range: 1-64 characters. | |
| **Ipv6 access control list** | Standard IPv6 access control list number, range: 1-64 characters. | |

| | | |
|---|---|---|
| **Operation** | Add | Add SNMP users. |
| | Remove | Delete SNMP users. |

### 1.2.1.2 Groups

SNMP group management module in which users can add or delete SNMP group operations.

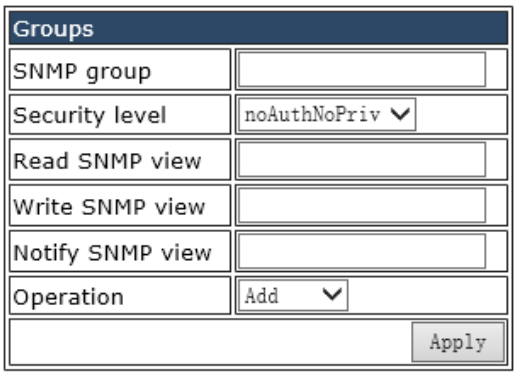



Figure 14.

| | | |
|---|---|---|
| **SNMP group** | User group name to operate, 1-32 characters. | |
| **Security level** | noAuthNoPriv | Uncertified non-encrypted level. |
| | authNoPriv | Authentication but not encryption level. |
| | authpriv | Authentication and encryption level. |
| **Read SNMP view** | Name of readable view, including 1-32 characters. | |
| **Write SNMP view** | Name of writable view, including 1-32 characters. | |
| **Notify SNMP view** | Notice the name of the view, including 1-32 characters. | |
| **Operation** | Add | Add SNMP groups. |
| | Remove | Delete SNMP groups. |

### 1.2.1.3 Views

SNMP view management module in which users can add or delete SNMP view operations.

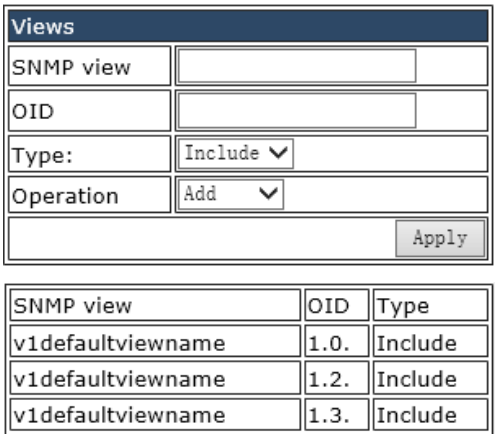


Figure 15.

| | | |
|---|---|---|
| **SNMP view** | User view name to operate, 1-32 characters. | |
| **OID** | OID number to operate, decimal. | |
| **Type:** | Include | Include this OID. |
| | Exclude | Exclude this OID. |
| **Operation** | Add | Add view. |
| | Remove | Delete view. |

#### 1.2.1.4 SNMP engineid configuration

SNMP Engineid configuration module, the user can configure SNMP Engineid operation in this module.

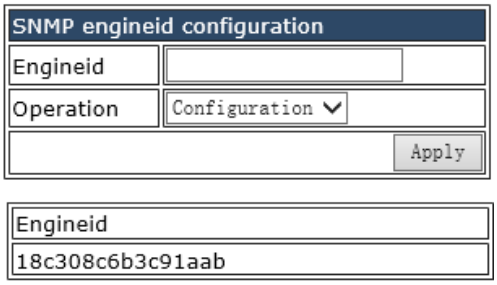



Figure 16.

| | | |
|---|---|---|
| **Engineid** | Engine id, Hex, 1-32 characters. | |
| **Operation** | configuration | Configuration operations. |
| | Default | Restore default (default is company ID plus local MAC address). |

### 1.2.2 SNMP management

SNMP network management function switch module, users can enable or disable SNMP functions.

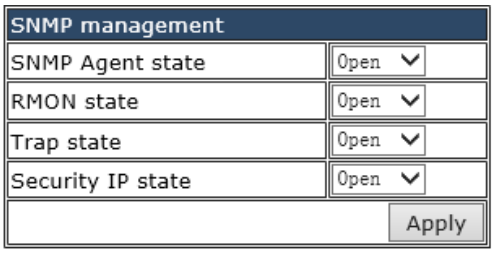



Figure 17.

### 1.2.3 Community managers

The group string management module where users can SNMP group string management and configure TRAP management settings.

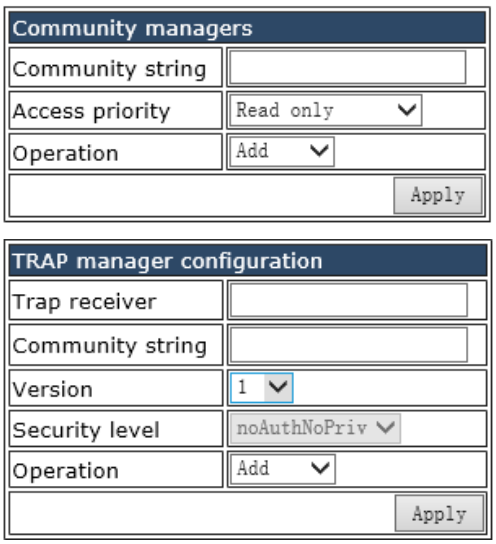



Figure 18.

| | | |
|---|---|---|
| **Community string** | Community string name, 1-255 characters. | |
| **Access priority** | Read only | Read-only permission level. |
| | Read and write | Read and write permission level. |
| **Operation** | Add | Do Community string add operations. |
| | Remove | Do Community string delete operations. |

| | | |
|---|---|---|
| **Trap receiver** | Recipient IPv4/IPv6 address of Trap information. | |
| **Community string** | Community string name, V1/V2 version: 1-255 characters, V3 version: 1-24 characters. | |
| **Version** | Three versions: V1/V2C/V3. | |
| **Security level (V3 version support only)** | noAuthNoPriv | Uncertified non-encrypted level. |
| | authNoPriv | Authentication but not encryption level. |
| | authpriv | Authentication and encryption level. |
| **Operation** | Add | For Trap information receiver add operation. |
| | Remove | For Trap information receiver remove operation. |

### 1.2.4 Configure snmp manager security IP

The administrator IP the address setting module, where the user can add or delete the SNMP manager's safe IP address.

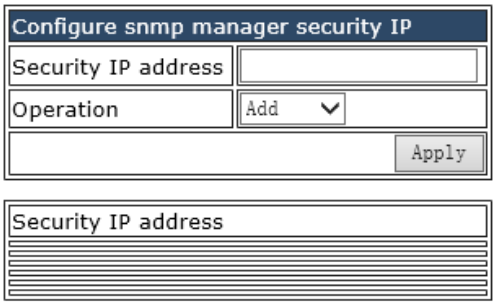



Figure 19.

| | | |
|---|---|---|
| **Security IP address** | SNMP Management Security IPv4/IPv6 Address. | |
| **Operation** | Add | Add a Security IP. |
| | Remove | Remove a Security IP. |

### 1.2.5 SNMP statistics

SNMP statistical information module, users in this module can view the SNMP function feedback information.

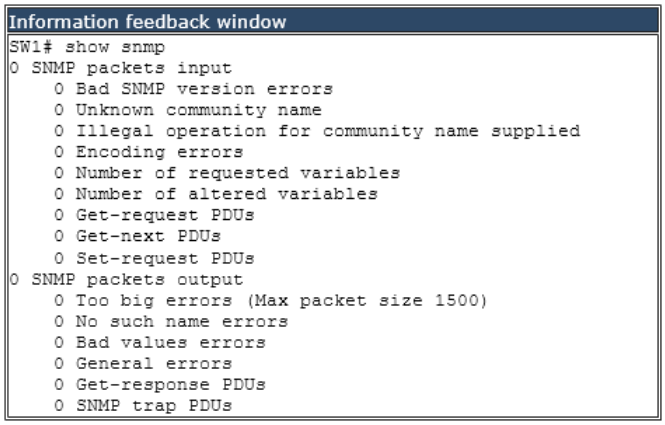



Figure 20.

## 1.3 SSH management

### 1.3.1 Switch on-off SSH

SSH function switch module in which the user can enable or disable switches by SSH.

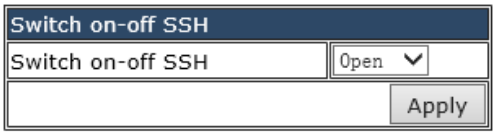



Figure 21.

### 1.3.2 SSH management

SSH management configuration module, the user can configure the SSH timeout, SSH authentication times and SSH RSA secret key modulus, and can also view the user login status of the SSH server.

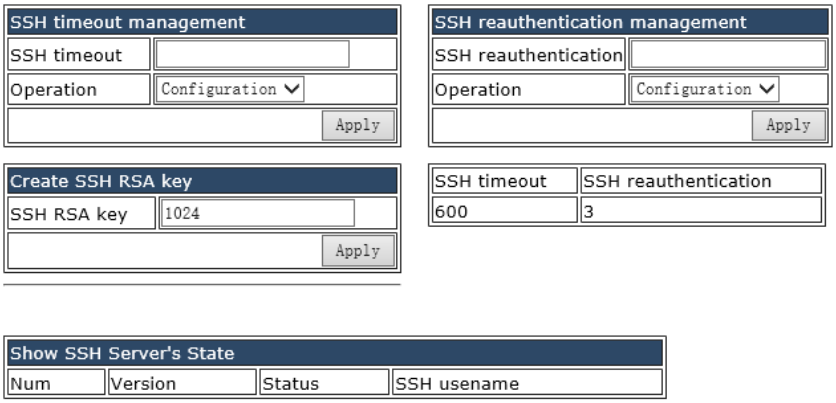



Figure 22.

| | | |
|---|---|---|
| **SSH timeout** | Timeout of exit SSH login status, 10-600 seconds. | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Recovery default (default 180 s). |

| | | |
|---|---|---|
| **SSH reauthentication** | SSH number of re-authentications when logged in, 1-10. | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Restore default (default re-authentication 3 times). |

| | |
|---|---|
| **SSH RSA key** | A module for calculating RSA keys, ranging from 768-2048, default 1024. |

## 1.4 Firmware update

### 1.4.1 TFTP service

#### 1.4.1.1 TFTP client service

TFTP client service module, the user can upload or download files by TFTP way, and can upgrade the firmware of the switch by this method.

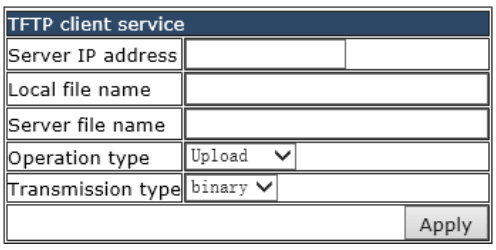


Figure 23.

| | | |
|---|---|---|
| **Server IP address** | TFTP address IP peer server, point decimal. | |
| **Local file name** | Name of destination file to upload or download, 1-100 characters. | |
| **Server file name** | Source name to upload or download, 1-100 characters. | |
| **Operation type** | Upload | To upload files. |
| | Download | To download files. |
| **Transmission type** | binary | Transfer files in binary format (default). |
| | ascii | Transfer files in ascii format. |

#### 1.4.1.2 TFTP server service

TFTP server-side service module, users can configure the TFTP server settings in this module.

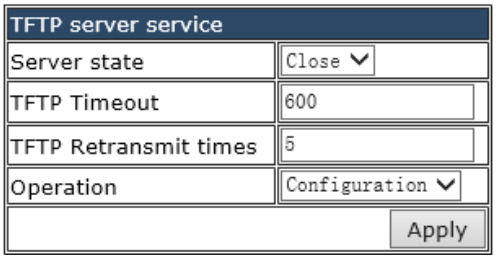



Figure 24.

| | | |
|---|---|---|
| **Server state** | Open | Enable TFTP server functionality. |
| | Close | Disable TFTP server functionality (default). |
| **TFTP Timeout** | TFTP service exit timeout, range 5-3600 s (default 600 s). | |
| **TFTP Retransmit times** | TFTP number of retransmissions after transmission failure, range 1-20 (default 5). | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Restore default. |

### 1.4.2 FTP service

#### 1.4.2.1 FTP client service

FTP client service module, the user can upload or download files by FTP way, and can upgrade the firmware of the switch by this method.

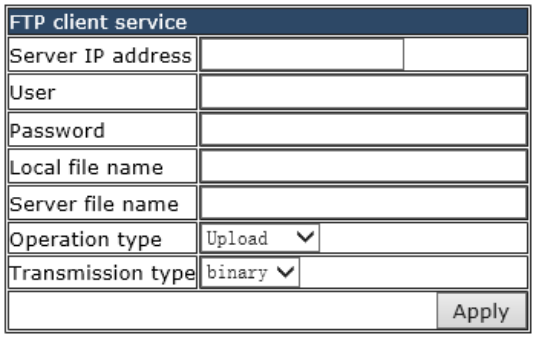



Figure 25.

| | | |
|---|---|---|
| **Server IP address** | FTP address IP peer server, point decimal. | |
| **User** | FTP server-to-server username, 1-100 characters. | |
| **Password** | FTP server-side user password, 1-100 characters. | |
| **Local file name** | Name of destination file to upload or download, 1-100 characters. | |
| **Server file name** | Source name to upload or download, 1-100 characters. | |
| **Operation type** | Upload | To upload files. |
| | Download | To download files. |
| **Transmission type** | binary | Transfer files in binary format (default). |
| | ascii | Transfer files in ascii format. |

### 1.4.2.2 FTP server service

FTP server service module, the user can configure various settings of FTP server.

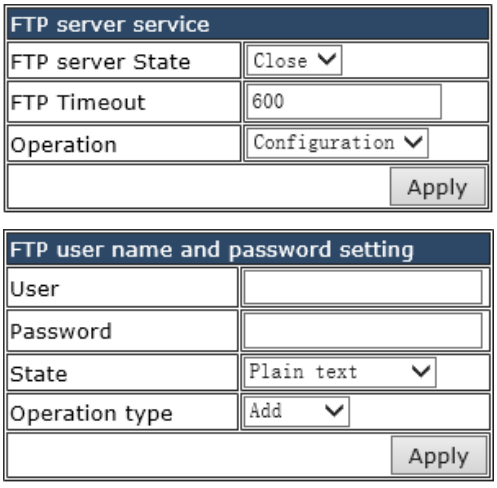



Figure 26.

| | | |
|---|---|---|
| **FTP server state** | Open | Enable FTP server functionality. |
| | Close | Disable FTP server functionality (default). |

| | | |
|---|---|---|
| **FTP Timeout** | FTP service exit timeout, range 5-3600 s (default 600 s). | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Restore default. |

| | | |
|---|---|---|
| **User** | FTP service username to operate, 1-32 characters. | |
| **Password** | FTP service user password to operate, 1-16 characters. | |
| **State** | Plain text | Do not encrypt FTP service password. |
| | Encrypted | Encryption of FTP service passwords. |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

# 1.5 Telnet server configuration

## 1.5.1 Telnet server state

Telnet server status module, where users can enable or disable login switches by Telnet.

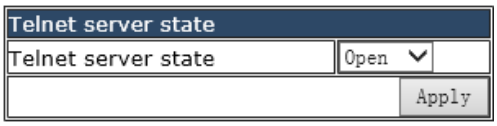



Figure 27.

## 1.5.2 Max numbers of telnet access connection

Telnet connect the maximum number module, the user can configure the maximum number of connections to the switch by Telnet.

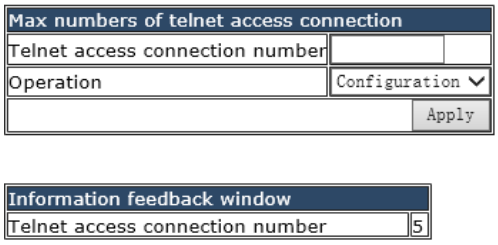



Figure 28.

| | | |
|---|---|---|
| **Telnet access connection number** | Maximum number of connections logged in by Telnet, range 1-16 (default 5). | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Restore default. |

# 1.6 Maintenance and debugging command

## 1.6.1 Debug command

Maintenance and debugging command module. the user can configure the mapping relationship between host and IP, also can run ping command and route tracking command.

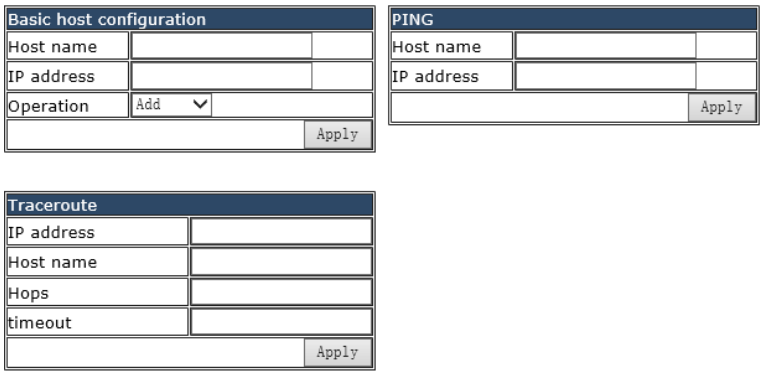



Figure 29.

| | | |
|---|---|---|
| **Host name** | Host name for mapping, 1-64 characters. | |
| **IP address** | IP address for mapping, point decimal. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

| | |
|---|---|
| **Host name** | To ping the host name, configure the mapping relationship between the host and the IP. |
| **IP address** | IP address to ping, decimal. |

| | |
|---|---|
| **IP address** | IP address for routing tracing, point decimal. |
| **Host name** | Host name for routing tracing, 1-64 characters. |
| **Hops** | Number of hops, route, range 1-255. |
| **timeout** | Tracking timeout, 100-10000. |

## 1.6.2 show clock

This module is used to display the current system time and date.

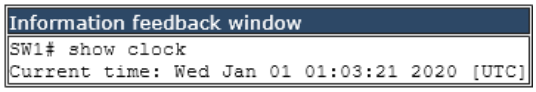



Figure 30.

### 1.6.3 show cpu usage

This module is used to display resource usage cpu current system.

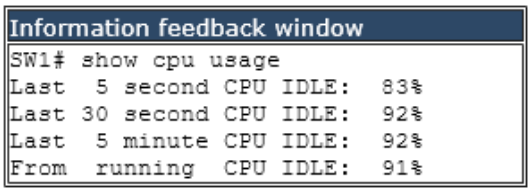



Figure 31.

### 1.6.4 show memory usage

This module is used to display the current system memory resource usage.

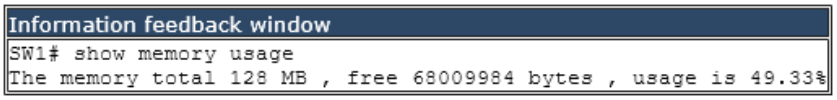



Figure 32.

### 1.6.5 show flash

This module is used to display the current system flash storage resource usage.

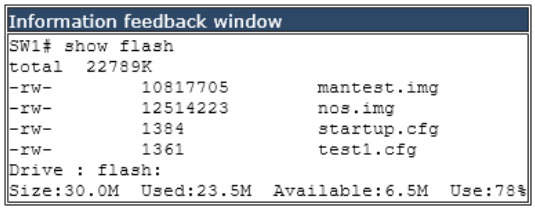



Figure 33.

### 1.6.6 show running-config

This module is used to display configuration information in the current system run.

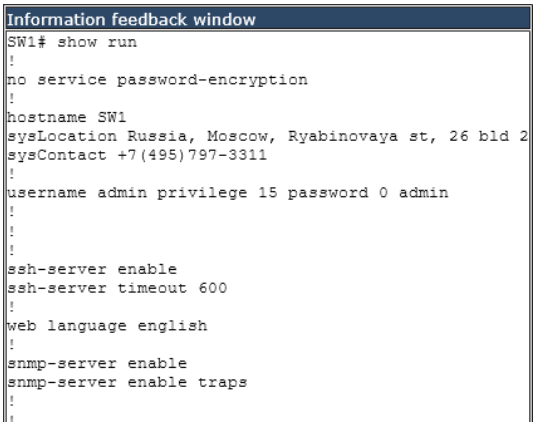



Figure 34.

### 1.6.7 show switchport interface

This module is used to display the port information of the current switch.

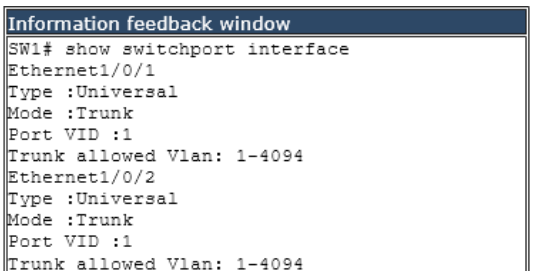



Figure 35.

### 1.6.8 show tcp

This module is used to display tcp connection information for the current switch.

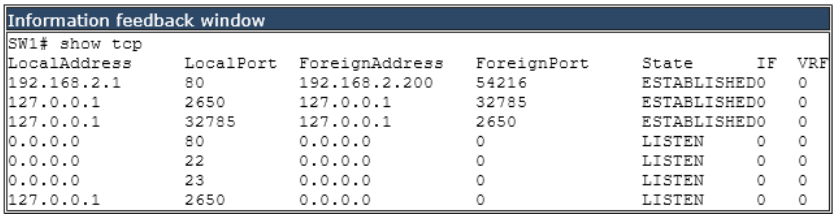



Figure 36.

### 1.6.9 show udp

This module is used to display udp connection information for the current switch.

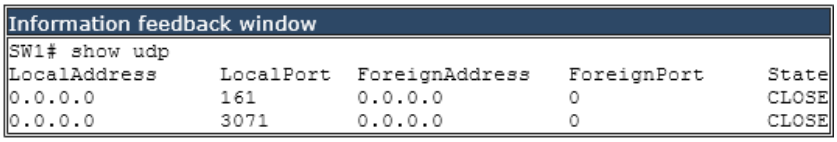



Figure 37.

### 1.6.10 show telnet login

This module is used to display the user information that is currently logged in to the switch by telnet.

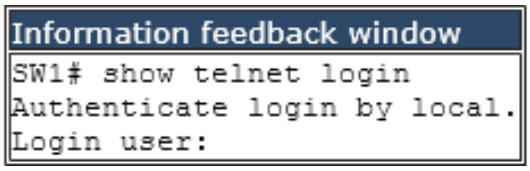



Figure 38.

### 1.6.11 show version

This module is used to display the user information that is currently logged in to the switch by telnet.

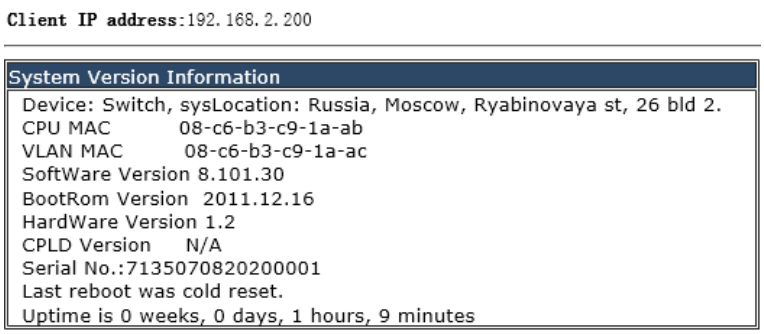



Figure 39.

# 2. Module management

## 2.1 Show boot-files

This module is used to display system firmware and configuration files for the next restart of the switch.

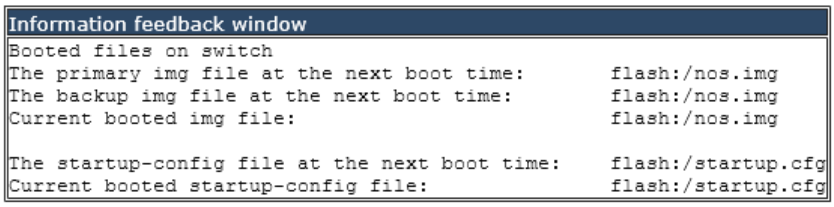



Figure 40.

## 2.2 Set Boot IMG and Startup-Config

This module is used to configure the system firmware and configuration files for the next restart of the switch.

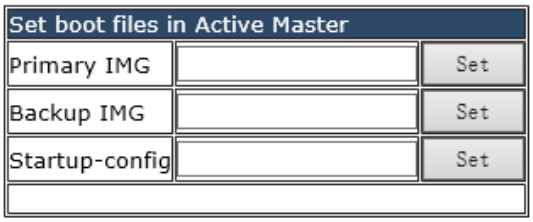



Figure 41.

| | |
|---|---|
| **Primary IMG** | System firmware first boot item when switch restarts. |
| **Backup IMG** | System firmware second boot item when switch restarts. |
| **Startup-config** | Start configuration file on switch restart. |

# 3. Port configuration

## 3.1 Ethernet port configuration

This chapter mainly configures the related port function of Ethernet port.

### 3.1.1 Port layer 1 attribution configuration

This page is mainly used to configure the basic properties of physical ports.

To display the "Port layer 1 attribution configuration" page, click Port configuration -> Ethernet port configuration -> Port layer 1 attribution configuration, click "Apply" to configure.

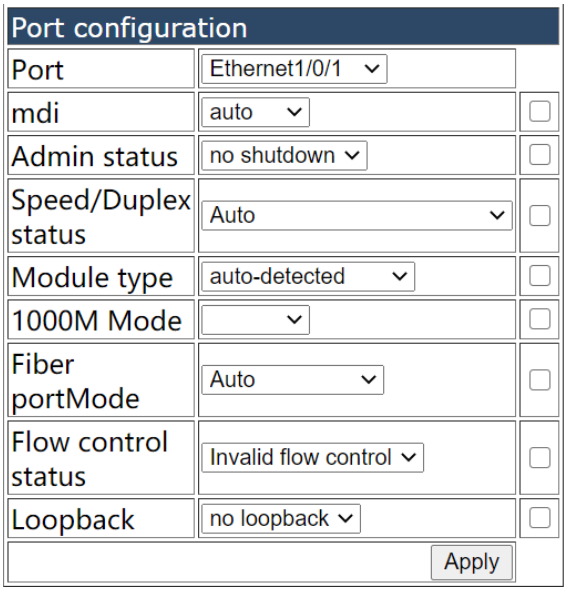



Figure 42.

| | |
|---|---|
| **entry** | describe |
| **Mdi** | Invalid settings. |
| **Admin status** | Port status:<br>Shutdown: enable<br>no shutdown: disable |
| **Speed/Duplex status** | Port rate and Working mode. |
| **Module type** | Port types such as Ethernet port, Gigabit optical port, etc. |
| **1000M Mode** | Mode configuration in Gigabit port configuration. |
| **Fiber portMode** | Invalid settings. |
| **Flow control status** | Port Flow Control. |
| **Loopback** | Port loop detection:<br>Loopback: enable<br>No Loopback: disable |
| **Port rate** | Port rate: 10:10M<br>100:100M<br>1000:1000M<br>Auto: Automatic negotiation rate |
| **Working mode** | Working mode: |

| | |
|---|---|
| | Auto: Automatic negotiation mode<br>Half: Half duplex mode<br>Full: Full duplex mode |

Port list

| Port | mdi | managementStatus | Speed | Mode | 1000M Mode | Fiber portMode | Flow control | loopback |
|---|---|---|---|---|---|---|---|---|
| Ethernet1/0/1 | auto | No Shutdown | 10M | full | 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 |

Figure 43.

| **entry** | describe |
|---|---|
| **Mdi** | Invalid settings. |
| **managementStatus** | Port enable status:<br>Shutdown: enable<br>no shutdown: disable |
| **Speed** | Port rate: 10:10M<br>100:100M<br>1000:1000M<br>Auto: Automatic negotiation rate |
| **Mode** | Working mode:<br>Auto: Automatic negotiation mode<br>Half: Half duplex mode<br>Full: Full duplex mode |
| **1000M Mode** | Mode configuration in Gigabit port configuration. |

| | |
|---|---|
| **Fiber portMode** | Invalid settings. |
| **Flow control** | Port Flow Control. |
| **Loopback** | Port loop detection:<br>Loopback: enable<br>No Loopback: disable |

### 3.1.2 Bandwidth control configuration

The page is configured for bandwidth control.

To display the "Bandwidth control configuration" page, click Port configuration -> Ethernet port configuration -> Bandwidth control configuration, click "Apply" to configure.

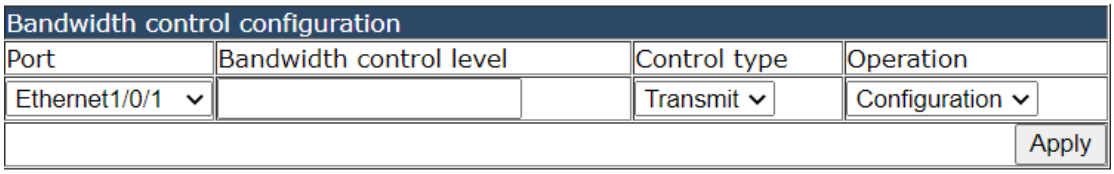



Figure 44.

| | |
|---|---|
| **entry** | describe |
| **Bandwidth control level** | Bandwidth control rate in the range of Kbps 1-1000000. |
| **Control type** | Control type:<br>Transmit:send<br>receive:receive<br>Both: send and receive |
| **Operation** | Configuration:<br>User-defined configuration<br>Default:<br>Restore default configuration |

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 |

Figure 45.

| | |
|---|---|
| **Port** | Ethernet port name. |

| | |
|---|---|
| **Ingress bandwidth threshold(Kb)** | Displays the current received data bandwidth limit in the range of Kbps 1-1000000. |
| **Engress bandwidth threshold(Kb)** | Displays the bandwidth limit of the current sending data, ranging from 1-1000000kbps. |

### 3.1.3 Switchport description

The page can be used to set the port name.

To display the "Switchport description" page, click Port configuration -> Ethernet port configuration -> Switchport description, click "Apply" to configure.

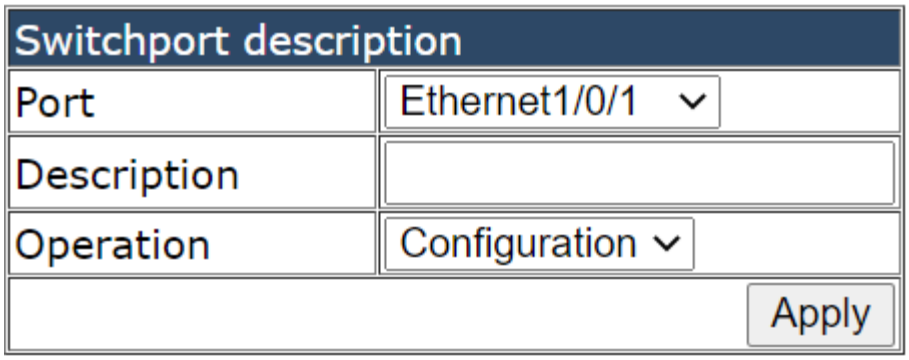



Figure 46.

| | |
|---|---|
| **Port** | Ethernet port name. |
| **Description** | Port description name, length 1-200 characters. |
| **Operation** | Configuration:<br>User-defined configuration<br>Default:<br>Restore default configuration |

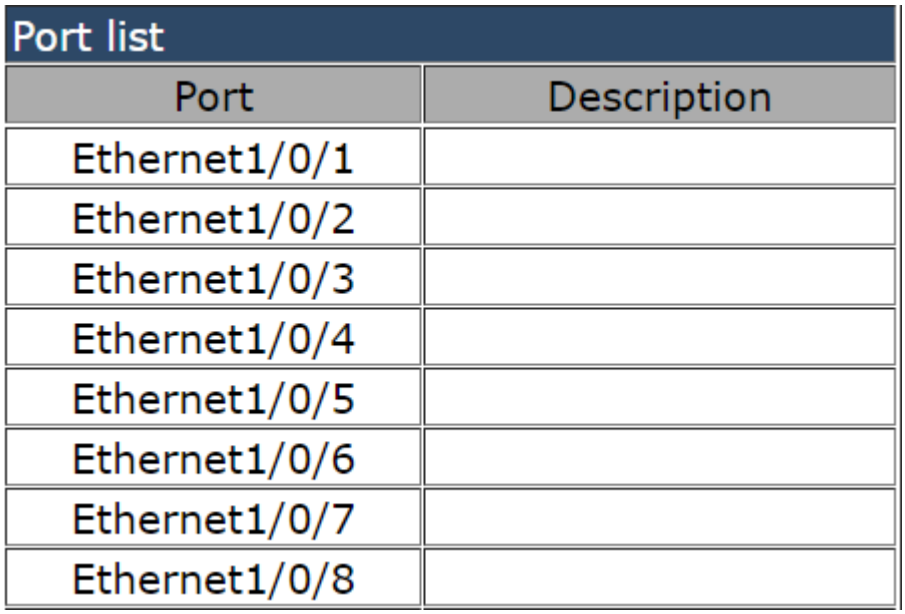


Figure 47.

| | |
|---|---|
| **Port** | Ethernet port name. |
| **Description** | Port description name, length 1-200 characters. |

### 3.1.4 Port combo forced mode config

This page can be used to configure the combo port interface type to switch.

To display the "Port combo forced mode config" page, click Port configuration -> Ethernet port configuration -> Port combo forced mode config, click "Apply" to configure.

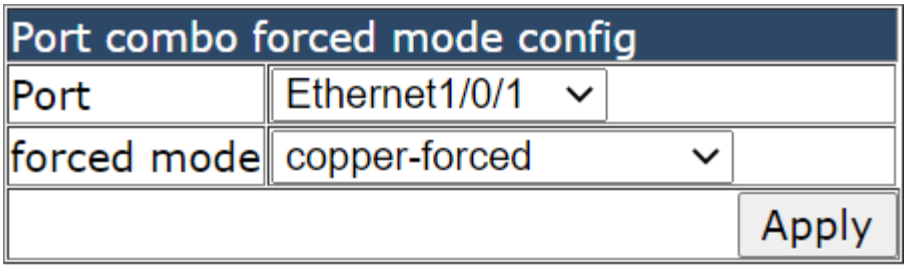



Figure 48.

| | |
|---|---|
| **Port** | Ethernet port name. |
| **forced mode** | Configure combo port current interface type:<br>Copper-forced: copper<br>Sfp-forced: fiber<br>sfp-preferred-auto: Automatic switching |

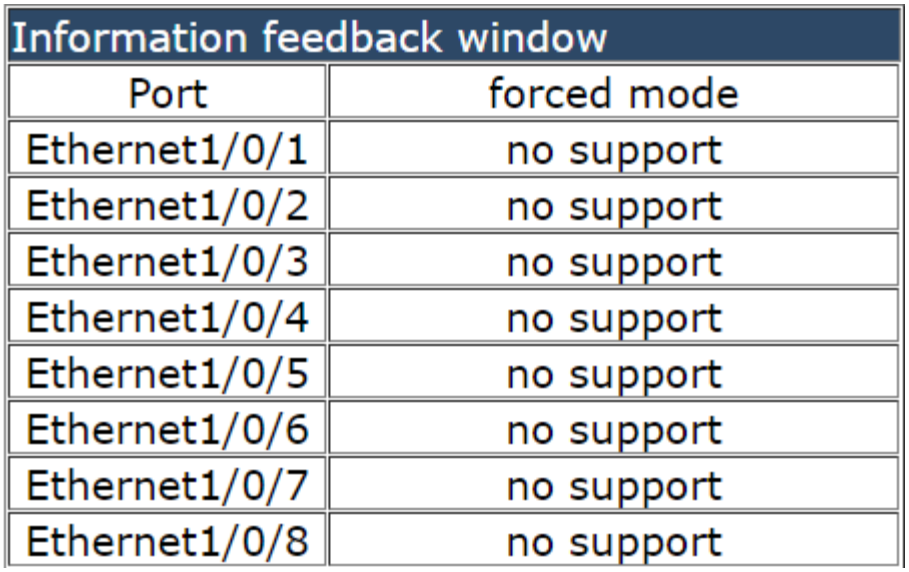



Figure 49.

| | |
|---|---|
| **Port** | Ethernet port name. |
| **forced mode** | Configure combo port current interface type: |

| | |
|---|---|
| | Copper-forced: copper<br>Sfp-forced: fiber<br>sfp-preferred-auto: Automatic switching |

### 3.1.5 port scan mode

This function switch is not supported for the time being.

## 3.2 VLAN interface configuration

This chapter mainly realizes the creation of VLAN interface and the configuration of interface address.

### 3.2.1 Add interface VLAN

This page is mainly used to create VLAN interfaces.

To display the "add interface VLAN" page, click Port configuration -> VLAN interface configuration -> add interface VLAN, click "Apply" to configure.

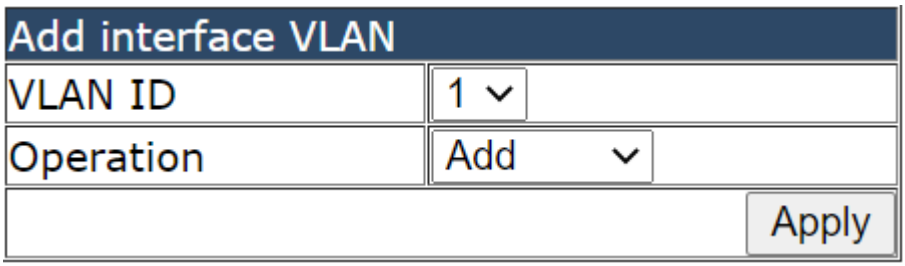



Figure 50.

| entry | describe |
|---|---|
| **VLAN ID** | VLAN ID created. |
| **Operation** | Action: Add/Remove |

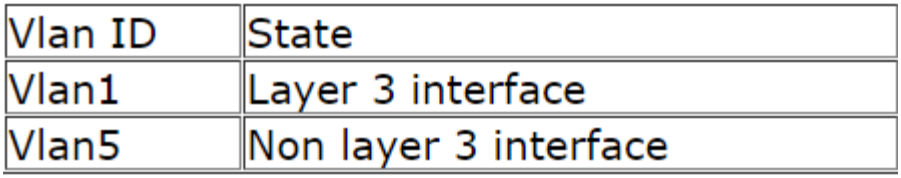



Figure 51.

| entry | describe |
|---|---|
| **VLAN ID** | VLAN ID added. |
| **State** | Is VLAN a layer 3 interface. |

### 3.2.2 L3 interface IP address mode configuration

The page can be used to configure IP address and subnet mask for the VLAN interface.

To display the "L3 interface IP address mode configuration" page, click Port configuration -> VLAN interface configuration -> L3 interface IP address mode configuration, click "Apply" to configure.

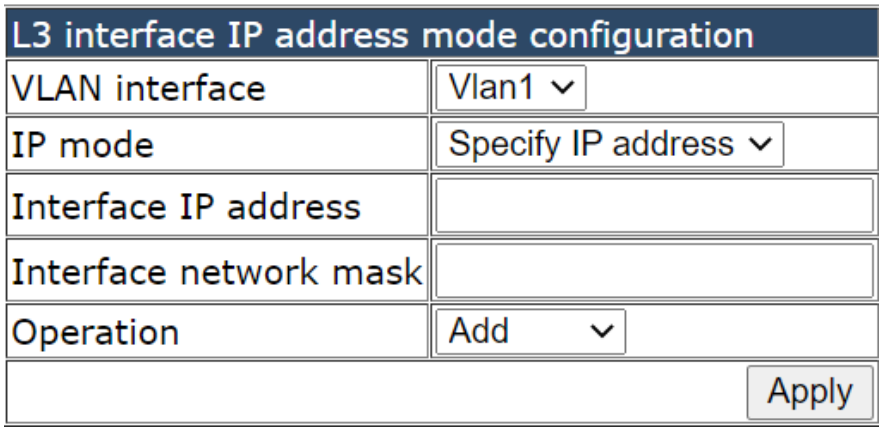



Figure 52.

| | |
|---|---|
| **entry** | describe |
| **VLAN interface** | VLAN ID of layer 3 interface created. |
| **IP mode** | Access to interface IP address:<br>bootp-client: bootp-client Automatic acquisition<br>dhcp-client: dhcp-client Automatic acquisition<br>Specify IP address: User self configuration |
| **Interface IP address** | IP address, e.g. A.B.C D. |
| **Interface network mask** | Network mask: for example: 255.255.255.0. |
| **Operation** | Action: Add/Remove |

## 3.3 SPAN configuration

This section can be used for port mirroring function configuration.

To display the "SPAN configuration" page, click Port configuration -> VLAN interface configuration -> SPAN configuration, click "Apply" to configure.

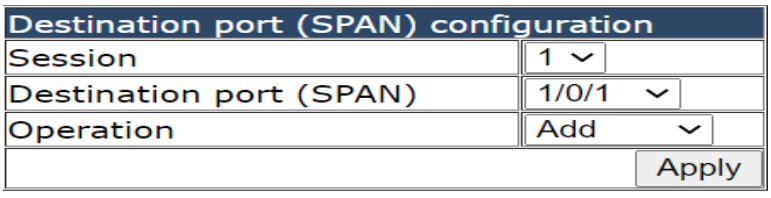



Figure 53.

| | |
|---|---|
| **entry** | describe |
| **Session** | Mirror Session. |
| **Destination port (SPAN)** | Mirror destination port. |

| | |
|---|---|
| **Operation** | Action: Add/Remove |

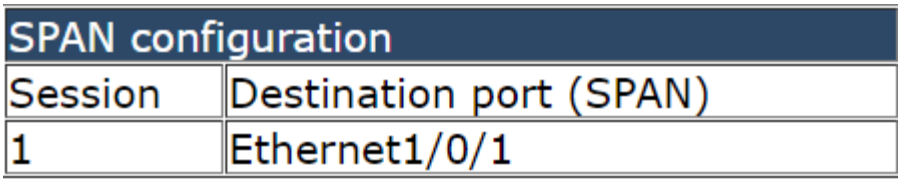



Figure 54.

| | |
|---|---|
| **entry** | describe |
| **Session** | Mirror Session. |
| **Destination port (SPAN)** | Mirror destination port. |

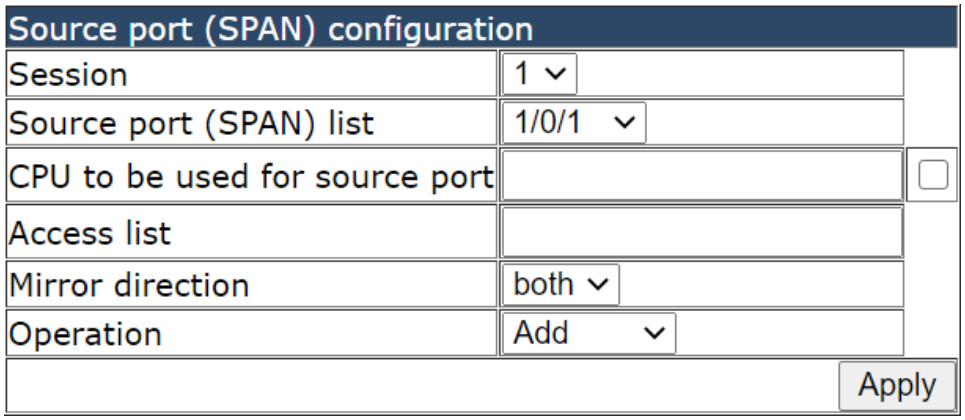



Figure 55.

| | |
|---|---|
| **entry** | describe |
| **Session** | Mirror Session. |
| **Source port (SPAN) list** | Mirror Source Port. |
| **CPU to be used for source port** | CPU used as the source of data. |
| **Access list** | The access control list set for the mirror source port. |
| **Mirror direction** | What kind of data is needed to filter to the destination port:<br>Both: Sending and receiving<br>Rx: receive<br>Tx: send |
| **Operation** | Add: Add configuration for the corresponding operation<br>Remove: Delete the corresponding configuration |

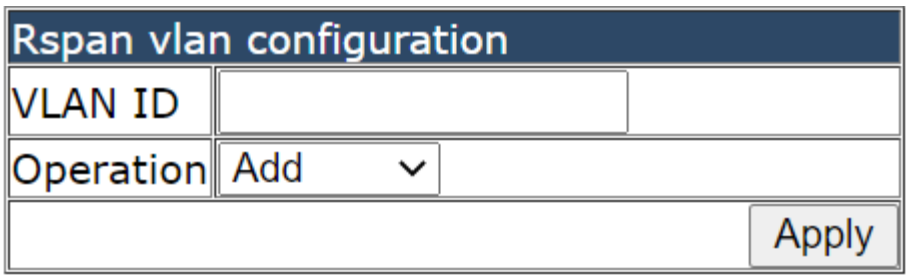



Figure 56.

| | |
|---|---|
| **entry** | describe |
| **VLAN ID** | VLAN ID. |
| **Operation** | Add: Add configuration for the corresponding operation<br>Remove: Delete the corresponding configuration |

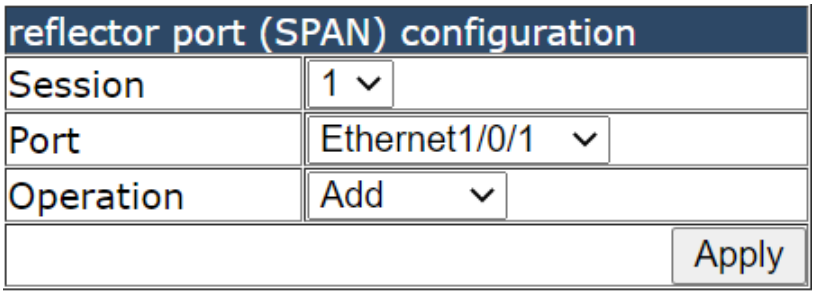



Figure 57.

| | |
|---|---|
| **entry** | describe |
| **Session** | Mirroring Session. |
| **Port** | Ethernet port number. |
| **Operation** | Add: Add configuration for the corresponding operation<br>Remove: Delete the corresponding configuration |

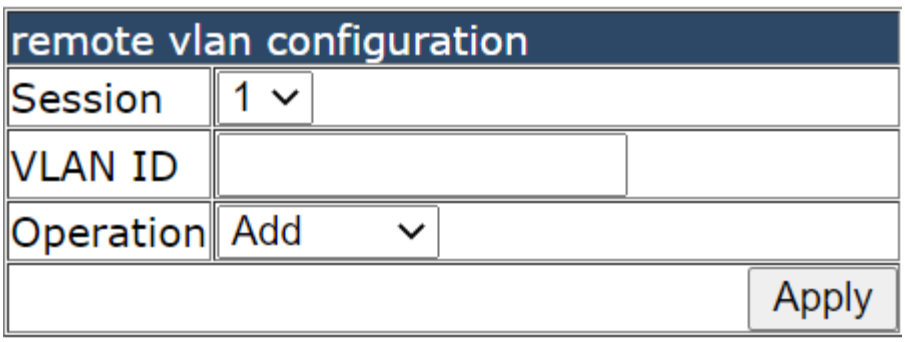



Figure 58.

| entry | describe |
|---|---|
| **Session** | Mirroring Session. |
| **VLAN ID** | VLAN ID. |
| **Operation** | Add: Add configuration for the corresponding operation<br>Remove: Delete the corresponding configuration |

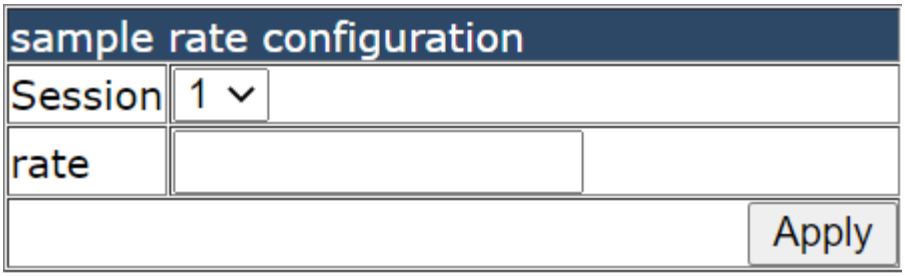



Figure 59.

| entry | describe |
|---|---|
| **Session** | Mirroring Session. |
| **rate** | It indicates how many packets are mirrored to the destination port. |

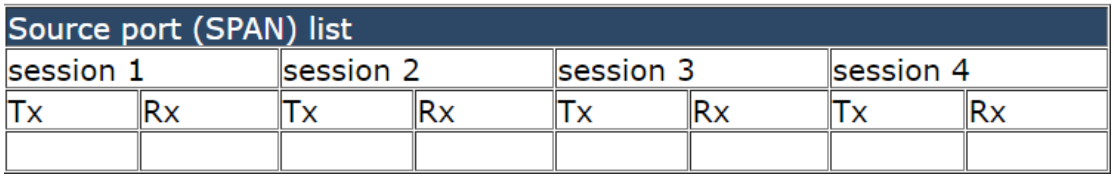



Figure 60.

| entry | describe |
|---|---|
| **Session** | Mirroring Session. |
| **Tx/Rx** | Direction of source port mirror data. |
| **Ethernet1/0/10** | Mirror Source Port for Session. |

## 3.4 Loopback-detection configuration

This chapter is mainly for port loop detection function configuration.

### 3.4.1 Port Loopback-detection mode configuration

The configuration of the page is used to set the loop detection control method.

To display the "Port Loopback-detection mode configuration" page, click Port configuration -> Port Loopback-detection configuration -> Port Loopback-detection mode configuration, click "Apply" to configure.

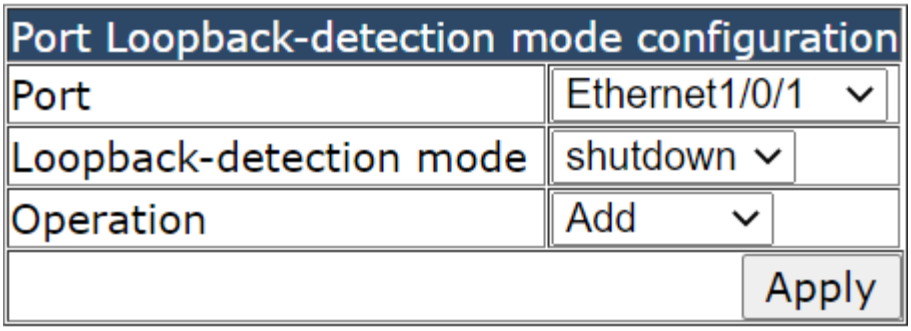



Figure 61.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **Loopback-detection mode** | Operation in case of loop:<br>Shutdown: Disable port<br>block: Block port |
| **Operation** | Operation of loop detection function:<br>Add:<br>Open loop detection and configure control mode<br>Remove:<br>Disable loop detection |

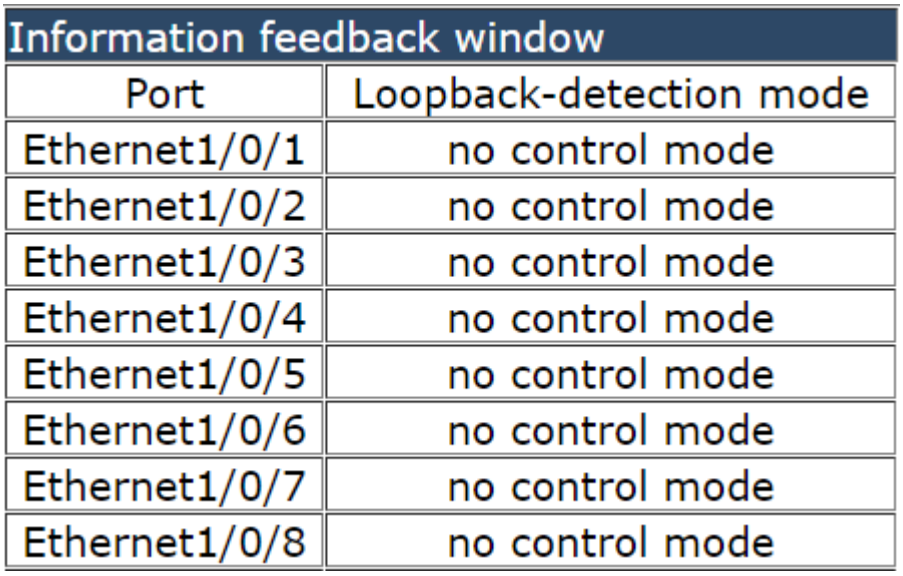



Figure 62.

| | |
|---|---|
| **entry** | describe |

| | |
|---|---|
| **Port** | Ethernet port name. |
| **Loopback-detection mode** | Shutdown: Disable port<br>block: Block port<br>no control mode: Disable port loop detection |

### 3.4.2 VLAN Loopback-detection configuration

This page can be used to configure VLAN loop detection function enabled or disabled.

To display the "VLAN Loopback-detection configuration" page, click Port configuration -> Port Loopback-detection configuration -> VLAN Loopback-detection configuration, click "Apply" to configure.

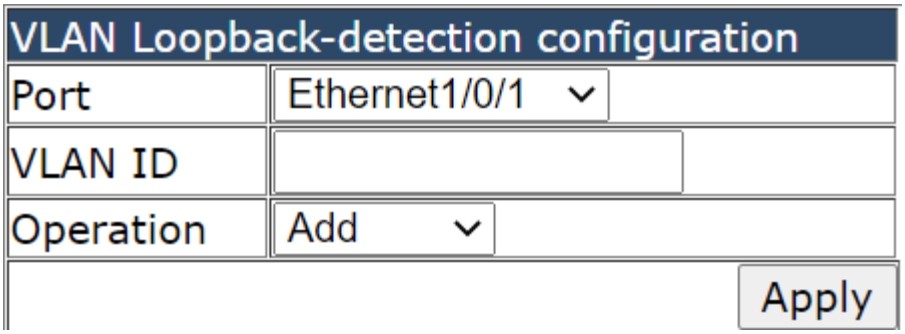



Figure 63.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **VLAN ID** | VLAN ID, range 1-4094. |
| **Operation** | Add: Enable VLAN loop detection<br>Remove: Disable VLAN loop detection |

### 3.4.3 Loopback-detection interval-time configuration

This page can be used to configure the loop detection interval.

To display the "Loopback-detection interval-time configuration" page, click Port configuration -> Port Loopback-detection configuration -> Loopback-detection interval-time configuration, click "Apply" to configure.

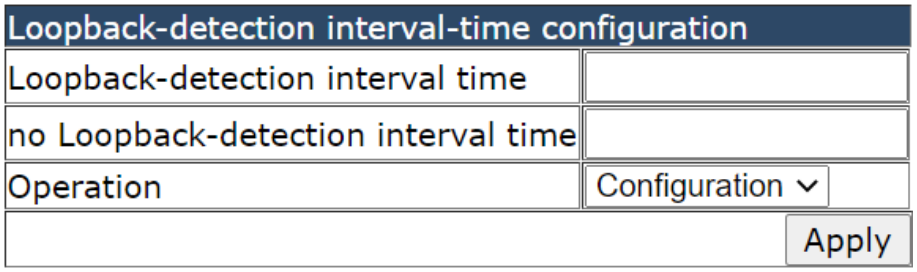



Figure 64.

| entry | describe |
|---|---|
| **Loopback-detection interval time** | Interval time between loops, size 5-300 seconds. |
| **no Loopback-detection interval time** | No loop interval, size 1-30 seconds. |
| **Operation** | Configuration: Set the test time by yourself.<br>Default: Restore the default configuration, there is a loop detection interval of 5 seconds, there is no loop detection interval of 3 seconds. |

### 3.4.4 Loopback-detection control recovery configuration

This page is used to configure loop detection to automatically return to an uncontrolled state.

To display the "Loopback-detection control recovery configuration" page, click Port configuration -> Port Loopback-detection configuration -> Loopback-detection control recovery configuration, click "Apply" to configure.

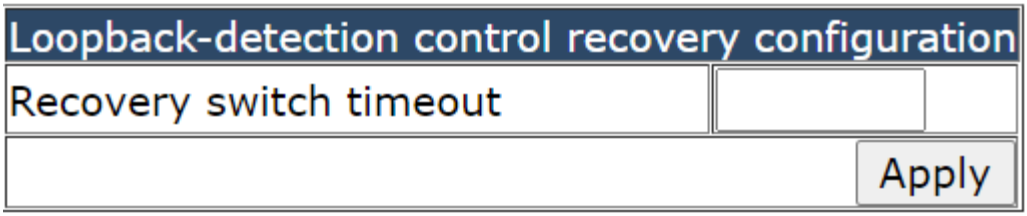



Figure 65.

| entry | describe |
|---|---|
| **Recovery switch timeout** | When a port is disabled or blocked due to a loop, it automatically recovers to an uncontrolled time, the size range is 0-3600 seconds. When it is configured as 0, the auto recovery function is disabled. |

## 3.5 Isolate-port configuration

This section can set up port isolation related functions.

### 3.5.1 Isolate-port group configuration

This page can be used to add or delete isolated groups.

To display the "Isolate-port group configuration" page, click Port configuration -> Isolate-port configuration -> Isolate-port group configuration, click "Apply" to configure.

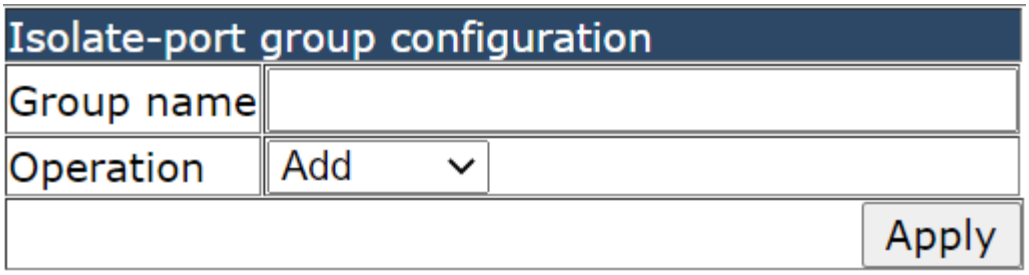



Figure 66.

| entry | describe |
|---|---|
| **Group name** | Isolation group name, example: aaaa. |
| **Operation** | Add: Create an isolation group<br>Remove: Delete an isolation group |

### 3.5.2 Interface join group config

This page can be used to add ports for isolation groups.

To display the "Interface join group config" page, click Port configuration -> Isolate-port configuration -> Interface join group config, click "Apply" to configure.

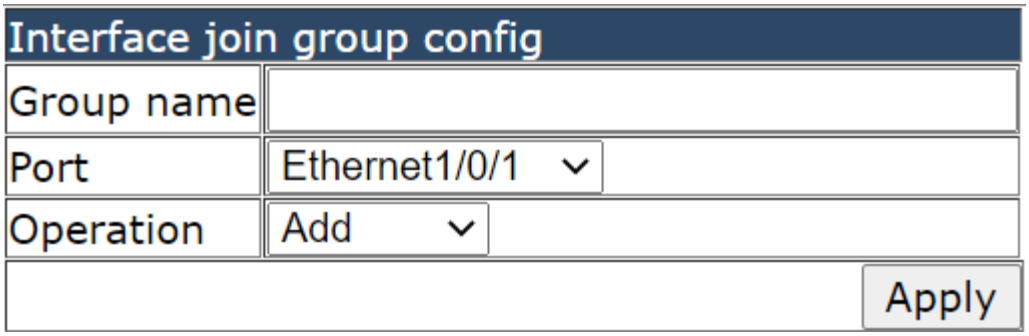



Figure 67.

| entry | describe |
|---|---|
| **Group name** | Created isolation group name, example: aaaa. |
| **Port** | Ethernet port name. |
| **Operation** | Add: Add ports to the isolation group<br>Remove: Delete ports in isolation groups |

### 3.5.3 show isolate-port group

This page is used to display isolation group information.

To display the "show Isolate-port group" page, click Port configuration -> Isolate-port configuration -> show Isolate-port group, click "Apply" to view.

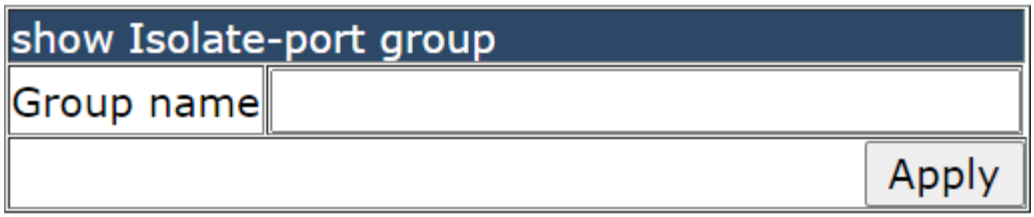



Figure 68.

| entry | describe |
|---|---|
| **Group name** | Created isolation group name, example: aaaa. |

## 3.6 Port storm-control config

This chapter can set up storm control related functions.

### 3.6.1 Port storm-control config

This page can be configured for the storm control function of the port.

To display the "Port storm-control config" page, click Port configuration -> Port storm-control config -> Port storm-control config, click "Apply" to configure.

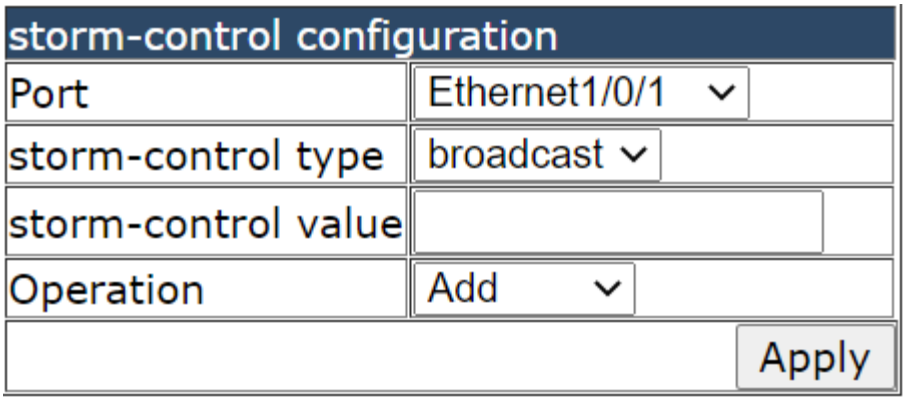



Figure 69.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **storm-control type** | Broadcast/Multicast/Unicast |
| **storm-control value** | Storm control rate, ranging from 1-1000000 kbps or 1-1488095 pps. |
| **Operation** | Add: Turn on the storm control function and configure the speed limit<br>Remove: Disable Storm Control |

| Information feedback window | |
|---|---|
| Port | storm-control type |
| Ethernet1/0/1 | None |
| Ethernet1/0/2 | None |
| Ethernet1/0/3 | None |
| Ethernet1/0/4 | None |
| Ethernet1/0/5 | None |
| Ethernet1/0/6 | None |
| Ethernet1/0/7 | None |
| Ethernet1/0/8 | None |

Figure 70.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **storm-control type** | Broadcast/Multicast/Unicast |

### 3.6.2 storm-control bypass configuration

This page can configure storm control unit, filter protocol, filter protocol status and other functions.

To display the "storm-control bypass configuration" page, click Port configuration -> Port storm-control config -> storm-control bypass configuration, click "Apply" to configure.

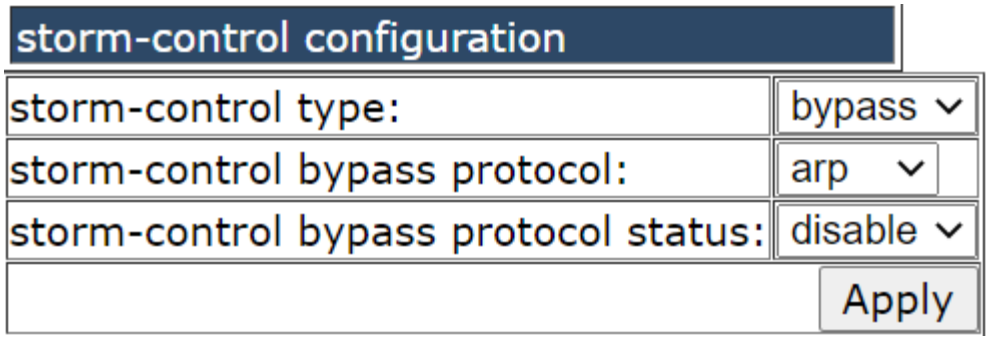



Figure 71.

| entry | describe |
|---|---|
| **storm-control type** | Bypass: Bypass Protocol<br>Kbps: Storm control rate units<br>pps: Storm control rate units |
| **storm-control bypass protocol** | Broadcast Storm Filter Agreement |
| **storm-control bypass protocol status** | Disable: Disable protocol filtering<br>Enable: Enable protocol filtering |

## 3.7 Port rate-violation config

This chapter is mainly used for the configuration of rate limiting functions.

### 3.7.1 rate-violation configuration

This page is mainly used to configure the rate limit function.

To display the "rate-violation configuration" page, click Port configuration -> Port rate-violation config -> rate-violation configuration, click "Apply" to configure.

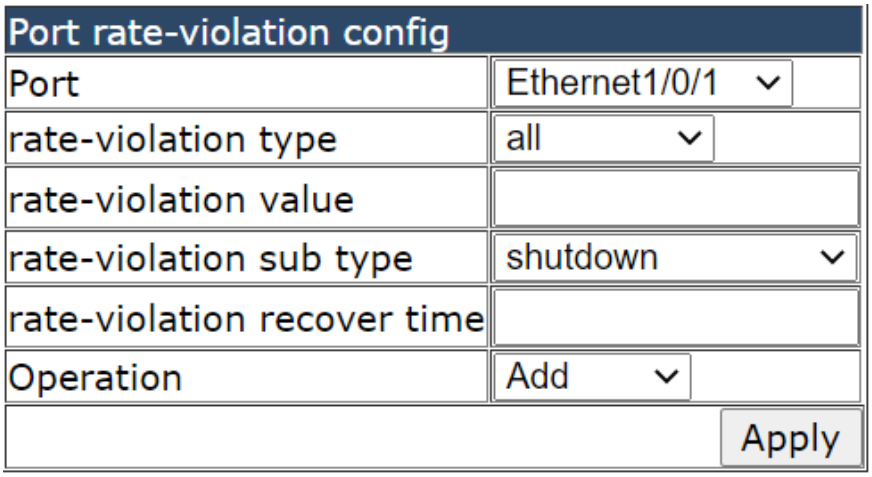



Figure 72.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **rate-violation type** | Type of breach:<br>All/Broadcast/Multicast/Unicast/<br>Control: Operation violation |
| **rate-violation value** | Limit rate, range 200-2000000. |
| **rate-violation sub type** | Overspeed operation:<br>Shutdown: Disable port<br>Block: Block port |
| **rate-violation recover time** | The time when the port overspeed is automatically resumed after it is disabled, if the size is 0-86400 seconds, configuring 0 seconds means no automatic recovery. |
| **Operation** | Add: Function Enable<br>Remove: Function disabled |

## 3.8 Port virtual-cable-test config

This chapter can be used to detect port link lines.

### 3.8.1 virtual-cable-test configuration

This chapter can be used to detect port link lines.

To display the "virtual-cable-test configuration" page, click Port configuration -> Port virtual-cable-test config -> virtual-cable-test configuration, click "Apply" to configure.

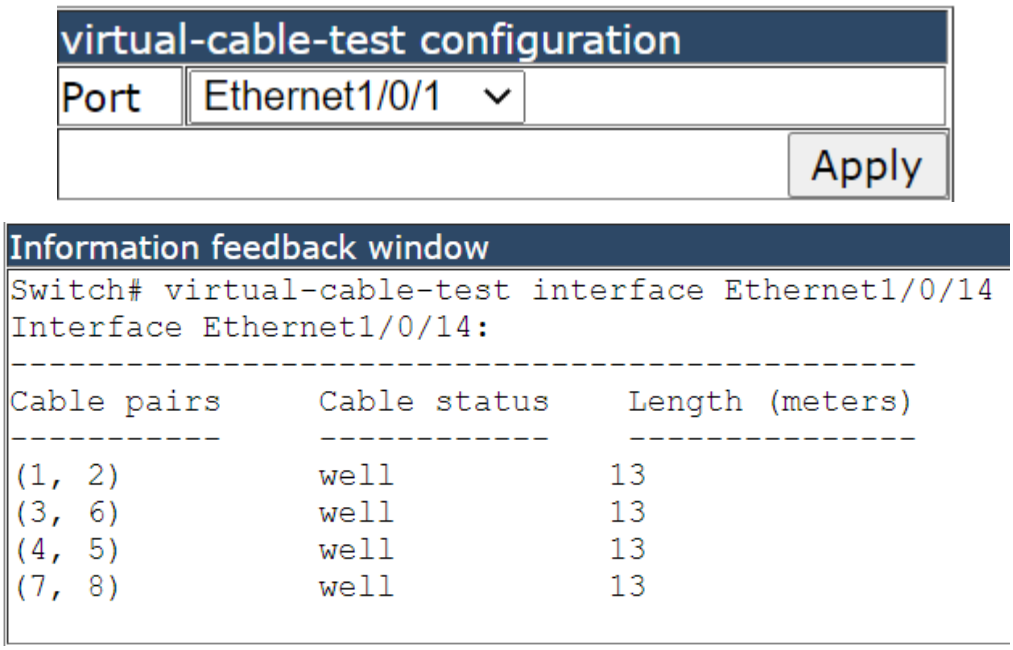



Figure 73.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |

## 3.9 Port debug and maintenance

This section is mainly used to view port, overall traffic statistics, port rate violation configuration and other information view.

### 3.9.1 Show port information

This page can be used to view port details.

To display the "Show port information" page, click Port configuration -> Port debug and maintenance -> Show port information, click "Apply" to view.

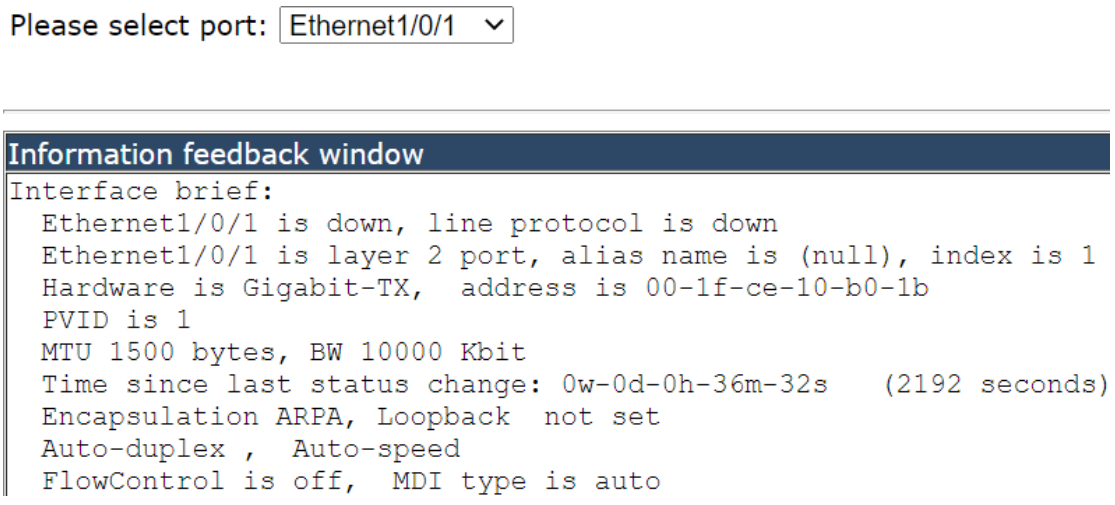


Figure 74.

### 3.9.2 Show entire traffic information

This page can be used to view statistics of overall traffic.

To display the "Show entire traffic information" page, click Port configuration -> Port debug and maintenance -> Show entire traffic information, click "Apply" to view.

Show entire traffic information

| Port | Receiving statistics | | | | | Transmitting statistics | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total packets | Error packets | Dropped packets | 5 minute rate(packets/sec) | Last 5 second rate(packets/sec) | Total packets | Error packets | Dropped packets | 5 minute rate(packets/sec) | Last 5 second rate(packets/sec) |
| Ethernet1/0/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Ethernet1/0/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 75.

### 3.9.3 Show rate violation port

This page can be used to view port rate violation function configuration information.

To display the "Show rate violation port" page, click Port configuration -> Port debug and maintenance -> Show rate violation port, click "Apply" to view.

Rate-violation port state information

| Port | Port rate-violation control mode | Rate-violation port state |
|---|---|---|
| Ethernet1/0/1 | shutdown | down |

Figure 76.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **Port rate-violation control mode** | Shutdown: Disable port<br>Block: Block port |
| **Rate-violation port state** | Status of current port:<br>Down: Not connected<br>Up: Connected<br>Forwarding: forward<br>Block: block |

## 3.10 uldp configuration

This chapter is mainly used for the configuration of single link detection function.

### 3.10.1 uldp enable config

This page can be used to enable or disable single link detection protocols.

To display the "uldp enable config" page, click Port configuration -> uldp configuration -> uldp enable config, click "Apply" to configure.

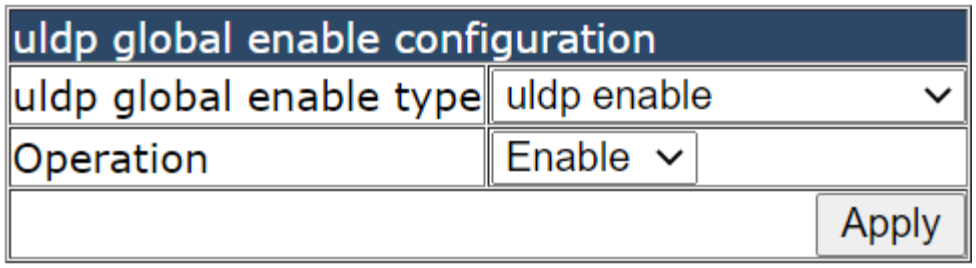



Figure 77.

| entry | describe |
|---|---|
| **uldp global enable type** | uldp enable: Turn on the ULDP function of all ports that support ULDP functions.<br><br>uldp aggressive-mode: Configure all ports ULDP working mode for positive mode.<br><br>uldp manual shutdown: global close auto disable port, switch to manual close port. |
| **Operation** | Enable: Function Enable<br>Disable: Function Disable |

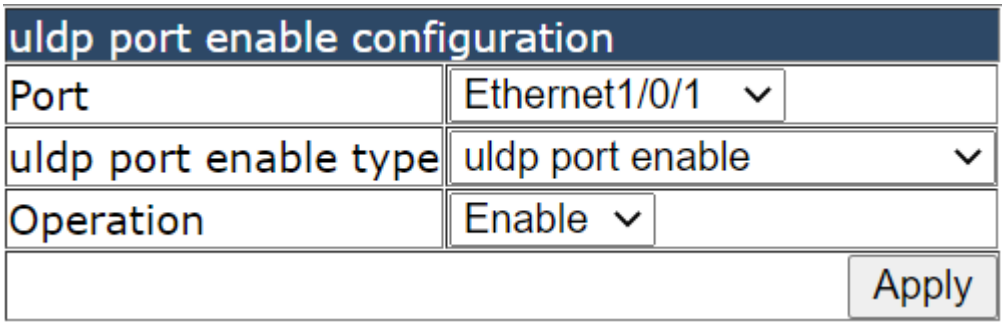



Figure 78.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **uldp global enable type** | Uldp port enable: Turn on the ULDP function of the specified port.<br><br>uldp port aggressive-mode: Configure the specified port ULDP working mode to positive mode. |
| **Operation** | Enable: Function Enable<br>Disable: Function Disable |

### 3.10.2 uldp Hello message config

This page is used to Hello the message sending interval.

To display the "uldp Hello message config" page, click Port configuration -> uldp configuration -> uldp Hello message config, click "Apply" to configure.

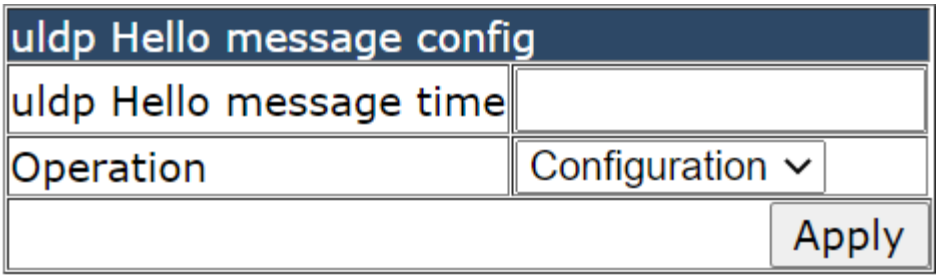



Figure 79.

| entry | describe |
|---|---|
| **uldp Hello message time** | Message sending interval, range 5-100 seconds. |
| **Operation** | Configuration: User self-configuration<br>Default: Restore the default configuration, the default configuration is 10 seconds. |

### 3.10.3 uldp recovery time config

This page can be used to configure ULDP auto recovery time.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration -> uldp recovery time config, click "Apply" to configure.

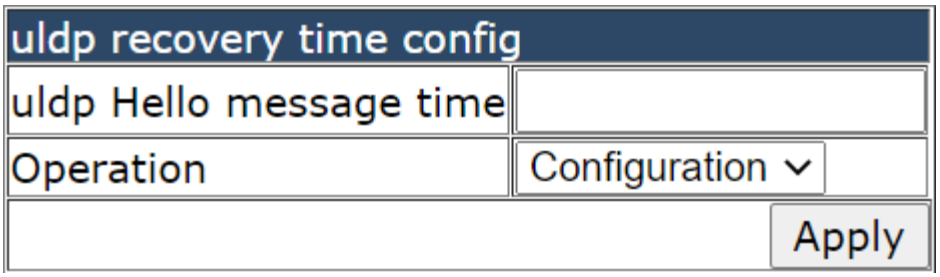



Figure 80.

| entry | describe |
|---|---|
| **uldp Hello message time** | Automatic recovery time after the port is disabled, ranging from 30-86400 seconds to 0 seconds without automatic recovery. |
| **Operation** | Configuration: User self-configuration<br>Default: Restore default configuration, default configuration is 0 seconds. |

### 3.10.4 show uldp configuration

This page can be used to view port ULDP configuration information.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration -> uldp recovery time config, click "Apply" to view.

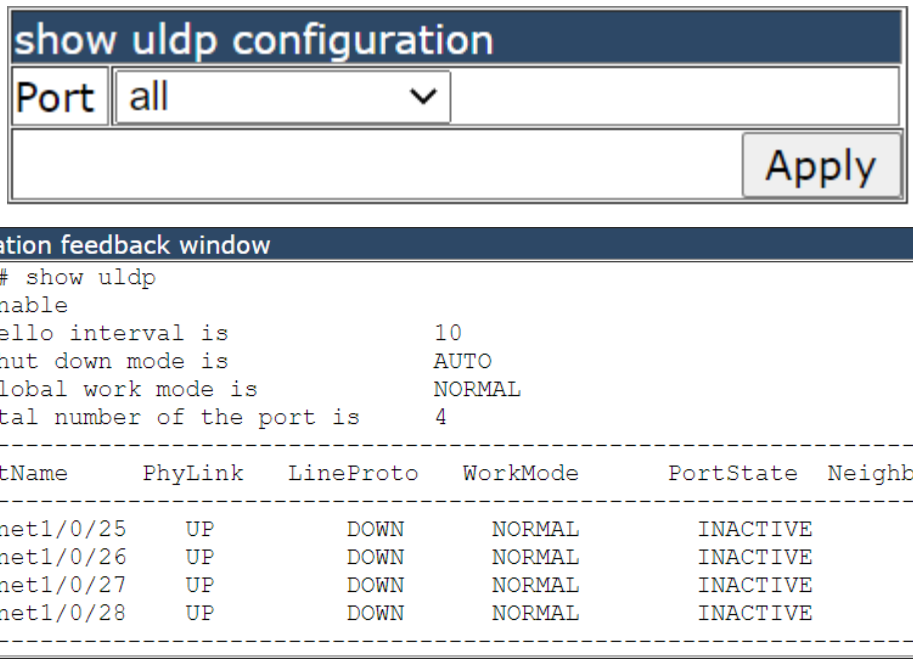



Figure 81.

## 3.11 LLDP configuration

This chapter can be used to configure LLDP related functions.

### 3.11.1 LLDP configuration

This page can be configured to enable or disable LLDP functionality.

To display the "LLDP configuration" page, click Port configuration -> LLDP configuration -> LLDP configuration, click "Apply" to configure.

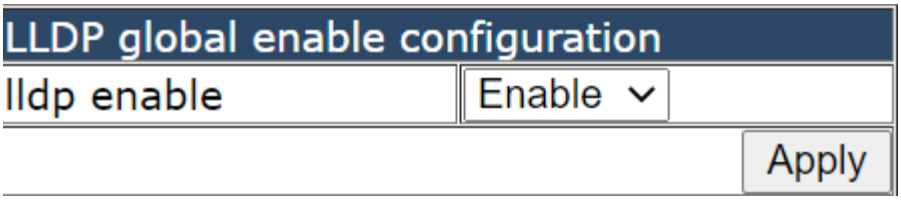



Figure 82.

| entry | describe |
|---|---|
| **lldp enable** | Enable: Global On LLDP Function<br>Disable: Global Off LLDP Function |

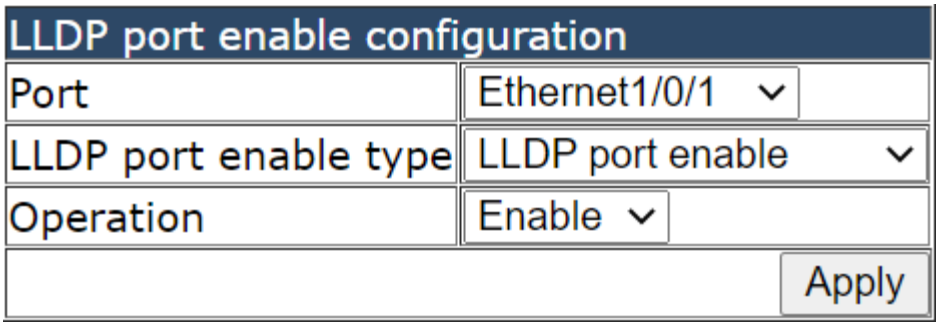



Figure 83.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **LLDP port enable type** | Enable or disable LLDP functions. |
| **Operation** | Turn on or off LLDP function. |

### 3.11.2 LLDP port status config

This page can configure port status.

To display the "LLDP port status config" page, click Port configuration -> LLDP configuration -> LLDP port status config, click "Apply" to configure.

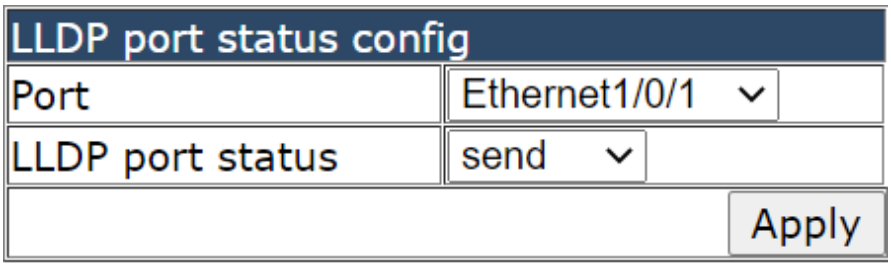



Figure 84.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **LLDP port status** | Send: Send only data<br>Receive: Receive only data<br>Both: Sending and receiving data simultaneously<br>Disable: Both sending and receiving are prohibited |

### 3.11.3 LLDP tx-interval config

This page can configure the interval between sending updates.

To display the "LLDP tx-interval config" page, click Port configuration -> LLDP configuration -> LLDP tx-interval config, click "Apply" to configure.

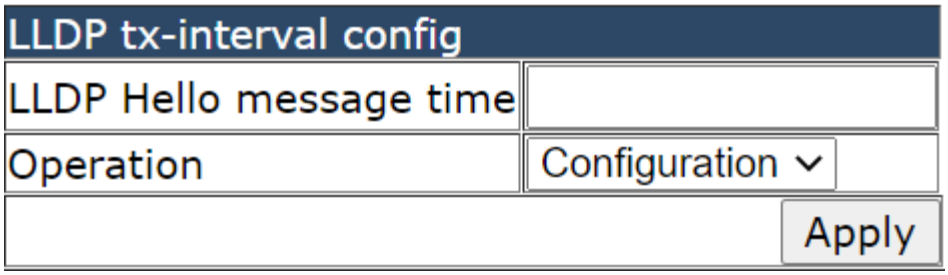



Figure 85.

| entry | describe |
|---|---|
| **LLDP Hello message time** | Update message sending interval between 5-32768 seconds. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Restore the default configuration, the default configuration is 30 seconds. |

### 3.11.4 LLDP msgTxHold config

This page can configure the value of the message aging time multiplier.

To display the "LLDP msgTxHold config" page, click Port configuration -> LLDP configuration -> LLDP msgTxHold config, click "Apply" to configure.

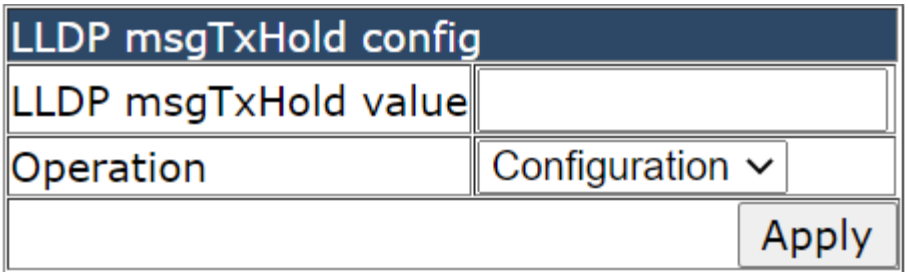



Figure 86.

| entry | describe |
|---|---|
| **LLDP msgTxHold value** | Numerical magnitude between 2-10. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Restore default configuration, default configuration is 4. |

### 3.11.5 LLDP transmit delay config

This page can configure the sending delay time of the update message.

To display the "LLDP transmit delay config" page, click Port configuration -> LLDP configuration -> LLDP transmit delay config, click "Apply" to configure.

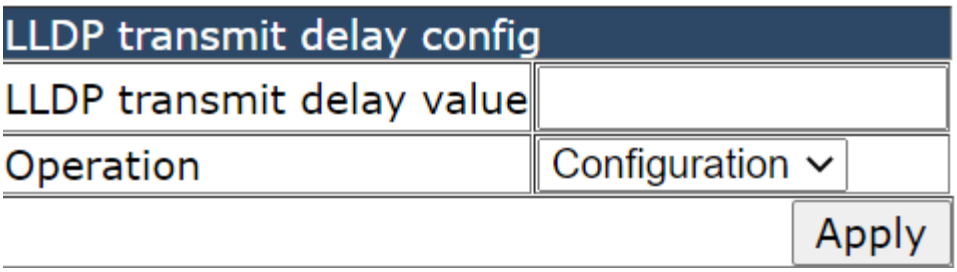



Figure 87.

| entry | describe |
|---|---|
| **LLDP transmit delay value** | Value between 1-8192 seconds. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Restore default configuration for 2 seconds |

### 3.11.6 LLDP notification interval config

This page can configure the interval between sending Trap messages.

To display the "LLDP notification interval config" page, click Port configuration -> LLDP configuration -> LLDP notification interval config, click "Apply" to configure.

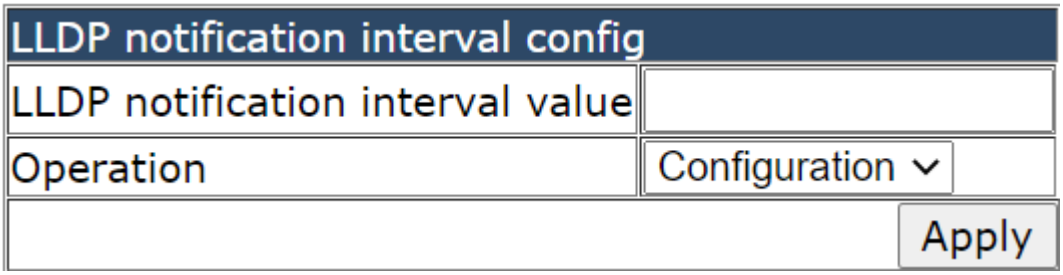



Figure 88.

| entry | describe |
|---|---|
| **LLDP notification interval value** | Value between 5 and 3600 seconds. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Restore default configuration for 5 seconds |

### 3.11.7 LLDP neighbors max-num config

This page can be used to Remote Table the settings for save entries.

To display the "LLDP neighbors max-num config" page, click Port configuration -> LLDP configuration -> LLDP neighbors max-num config, click "Apply" to configure.

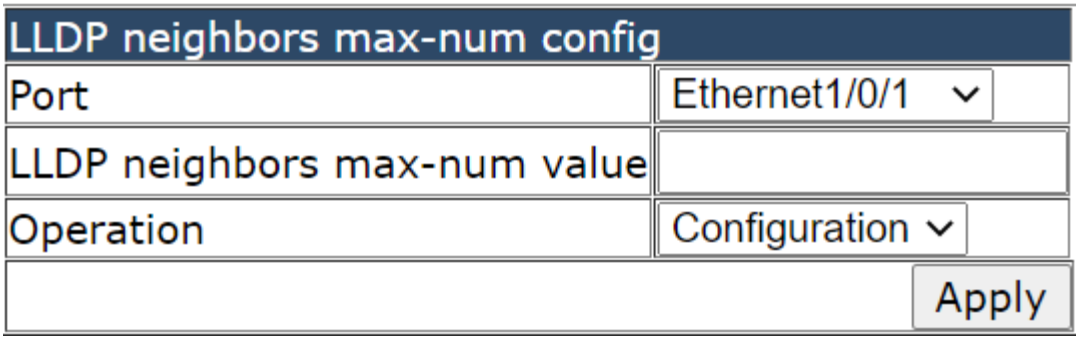



Figure 89.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **LLDP neighbors max-num value** | Remote table maximum save entry size 5-500. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Restore default configuration, default configuration is 100 |

### 3.11.8 LLDP too many neighbors config

This page can be used to set up operations after Remote Table is full.

To display the "LLDP too many neighbors config" page, click Port configuration -> LLDP configuration -> LLDP too many neighbors config, click "Apply" to configure.

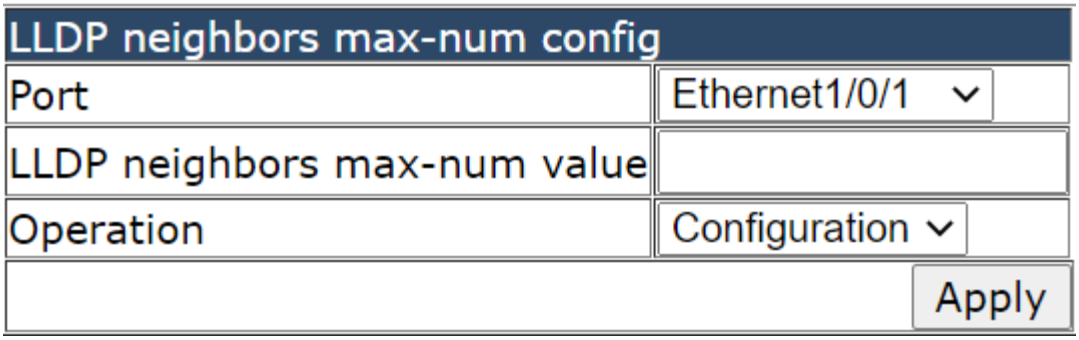



Figure 90.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **LLDP too many neighbors value** | Discard: Discard new neighbor information<br>Delete: Delete the neighbor information with the least aging time in the remore table, and then |

| | |
|---|---|
| | add new neighbor information |

### 3.11.9 LLDP transmit optional tlv config

This page can configure port TLV properties.

To display the "LLDP transmit optional tlv config" page, click Port configuration -> LLDP configuration -> LLDP transmit optional tlv config, click "Apply" to configure.

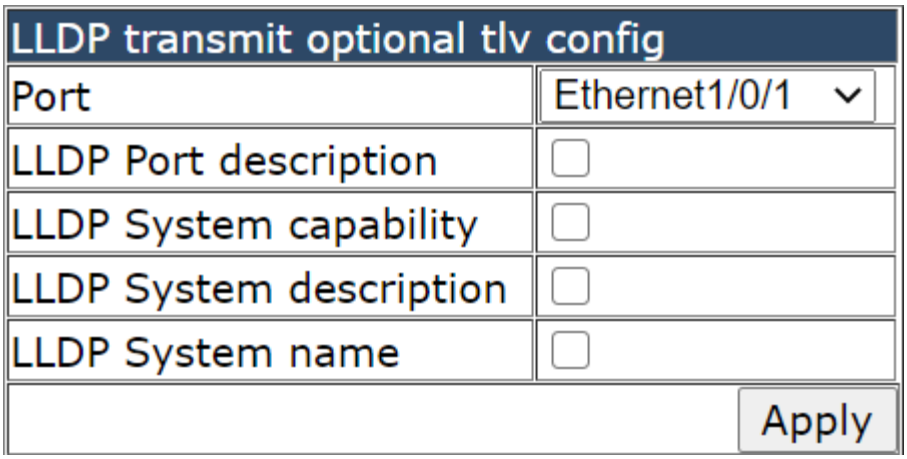


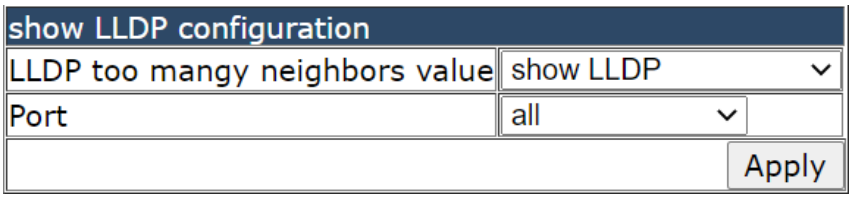

Figure 91.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **LLDP Port description** | Port description name information needs to be configured. |
| **LLDP System capability** | Information describing system capabilities. |
| **LLDP System description** | Message describing the system. |
| **LLDP System name** | System name information. |

### 3.11.10 show LLDP configuration

This page can be used to view LLDP configuration messages.

To display the "show LLDP configuration" page, click Port configuration -> LLDP configuration -> show LLDP configuration, click "Apply" to view.



**Information feedback window**

```
Switch# show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been disabled globally.
LLDP enabled port : NULL
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
-------------END-----------------
```

| show LLDP configuration | |
|---|---|
| LLDP too mangy neighbors value | show LLDP port |
| Port | Ethernet1/0/14 |
| | Apply |

**Information feedback window**

```
Switch# show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been disabled globally.
LLDP enabled port : NULL
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
-------------END-----------------
```

| show LLDP configuration | |
|---|---|
| LLDP too mangy neighbors value | show LLDP |
| Port | all |
| | Apply |

**Information feedback window**

```
Switch# show lldp traffic
   PortName          Ageouts     FramesDiscarded     FramesInErrors     FramesIn     FramesOut     TLVsDiscarded     TLVsUnrecognized
-------------------  -------     ---------------     --------------     --------     ---------     -------------     ----------------
  Ethernet1/0/14          0                   0                  0            0             0                 0                    0
```

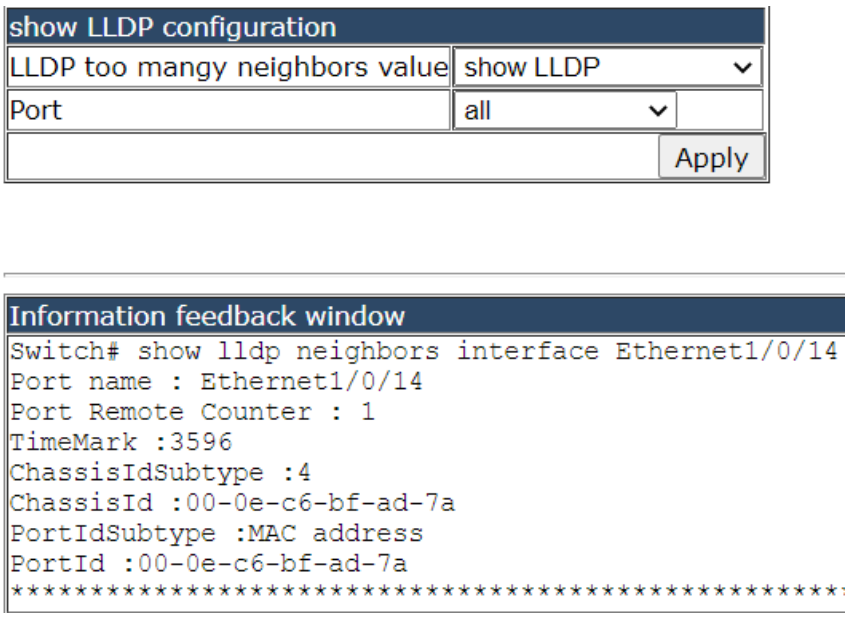



Figure 92.

## 3.12 LED shutoff configuration

This chapter can be used to set the timing of led lights out.

### 3.12.1 Time Range configuration

This page can be used to set the time range for led lights to go out.

To display the "Time Range configuration" page, click Port configuration -> LED shutoff configuration -> Time Range configuration, click "Apply" to configure.

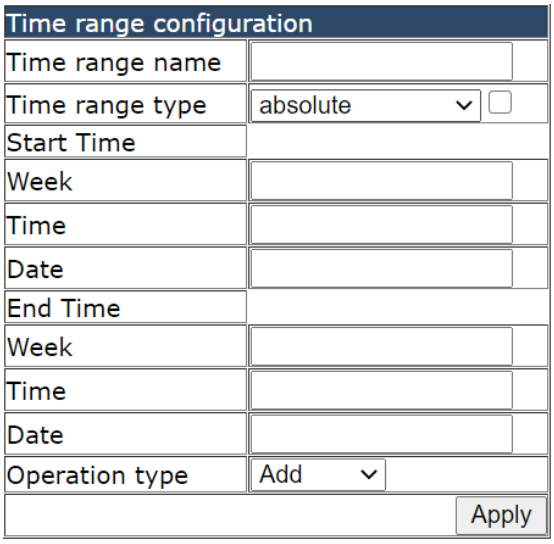



Figure 93.

| entry | describe |
|---|---|
| **Time range name** | Time range name, length 1-64 characters. |
| **Time range type** | Absolute:<br>Absolute time range, date required |

| | |
|---|---|
| | Absolute-periodic:<br>Absolute cycle time range<br>Periodic:<br>Period Time Range |
| **Week** | Range: 1-7 |
| **Time** | Time format: 14:00 |
| **Date** | Date Scope: 2001.1.1-2038.12.31 |

### 3.12.2 LED shutoff config

This page can be used for LED timing extinguishing configuration.

To display the "LED shutoff config" page, click Port configuration -> LED shutoff configuration -> LED shutoff config, click "Apply" to configure.

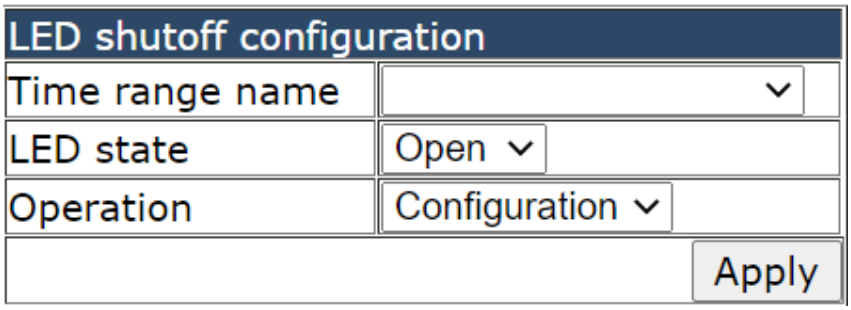



Figure 94.

| **entry** | describe |
|---|---|
| **Time range name** | With the configured time range name. |
| **LED state** | LED lamp status. |
| **Operation** | Configuration:<br>User self-configuration<br>Default:<br>Function disabled |

## 3.13 Jumbo packet forwarding configuration

This section can be used for the configuration of super packet forwarding.

This page can be used to set the time range for led lights to go out.

To display the "LED shutoff config" page, click Port configuration -> LED shutoff configuration -> LED shutoff config, click "Apply" to configure.

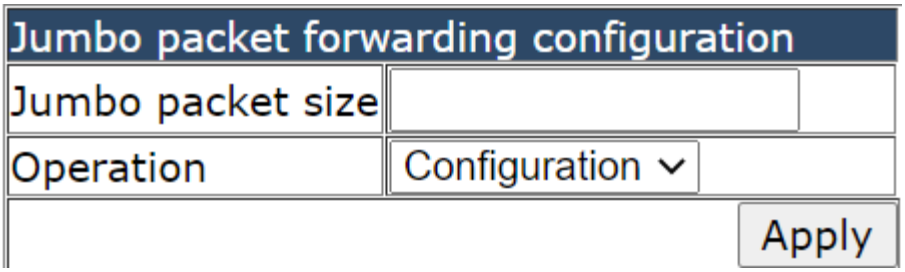



Figure 95.

| | |
|---|---|
| **entry** | describe |
| **Jumbo packet size** | Range: 1500-12270 |
| **Operation** | Configuration:<br>User self-configuration<br>Default: Function disabled |

# 4. MAC address table configuration

## 4.1 MAC address table configuration

### 4.1.1 MAC address aging-time configuration

Each time the switch learns a MAC address, it will store the address and set the aging time. When the time is over, the address will be removed from the switch.

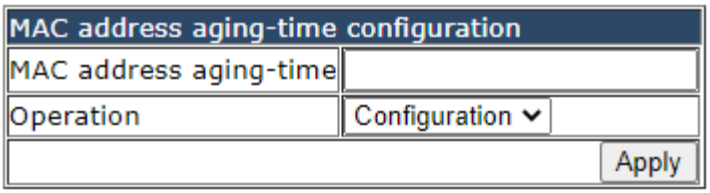



Figure 96.

| | | |
|---|---|---|
| **MAC address aging-time** | The aging time range is 10-1000000, 0 means no aging. | |
| **Operation** | Configuration | Set the aging time into the switch. |
| | Default | Restore the aging time of the switch to the default state. |

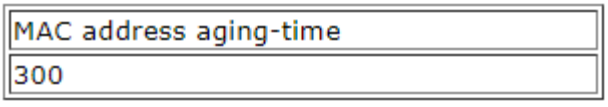



Figure 97. Display the current MAC address aging time.

### 4.1.2 Configurate MAC address

Configure static or Blackhole MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

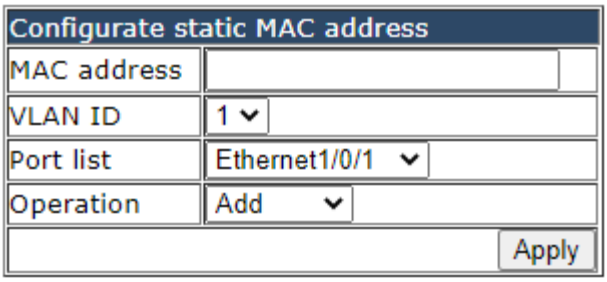



Figure 98.

| | | |
|---|---|---|
| **MAC address** | Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx. | |
| **VLAN ID** | Created VLAN ID. | |
| **Port list** | Mapped port. | |
| **Operation** | Add | The mapping relationship between MAC address and port and VLAN will be added. |
| | Remove | Delete the mapping relationship of the specified MAC address, VLAN, and port. |

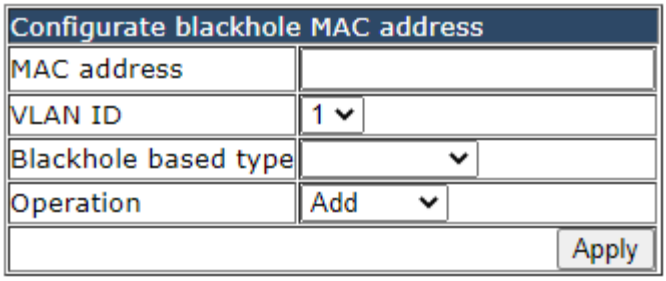



Figure 99.

| | | |
|---|---|---|
| **MAC address** | Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx, packets with this address will be discarded and will not be forwarded to the network by the switch. | |
| **VLAN ID** | Created VLAN ID. | |
| **Blackhole based type** | source | Source based on source address filter. |
| | destination | Target based on target address filter. |
| | both | Both are based on source address and destination address filters, the default value is both. |
| **Operation** | Add | The mapping relationship between MAC address and port and VLAN will be added. |
| | Remove | Delete the mapping relationship of the specified MAC address, VLAN, and port. |

| MAC address | VLAN ID | Port |
|---|---|---|
| 00-11-22-cc-bb-dd | 1 | Ethernet1/0/1 |
| 00-11-55-cc-bb-df | 1 | Blackhole |

Figure 100. Display current existing MAC address, port, VLAN mapping relationship.

### 4.1.3 Delete MAC address

Quickly delete the MAC address in the switch.

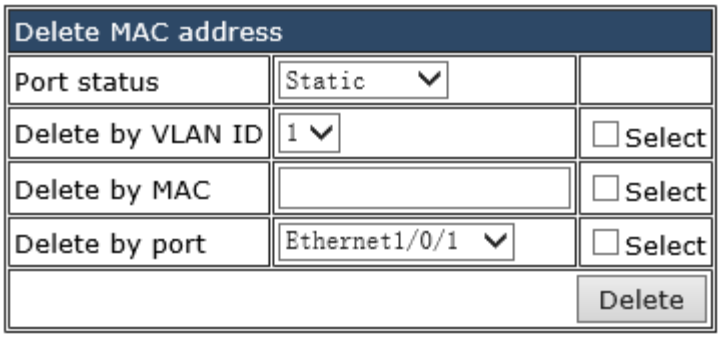



Figure 101.

| | | |
|---|---|---|
| **Port status** | Static | User-created and assigned MAC address. |
| | Dynamic | The MAC address automatically learned by the switch through the message. |
| | Blackhole | The user creates the assigned MAC address, but the packet of this address will not be forwarded by the switch. |
| **Delete by VLAN ID** | The created VLAN ID, delete the selected address type in the VLAN. | |
| **Delete by MAC** | Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx. | |
| **Delete by port** | Delete all MAC addresses under the port. | |

| MAC address | VLAN ID | Status |
|---|---|---|
| 00-1a-33-44-de-fd | 1 | Ethernet1/0/1 |
| 10-55-df-98-77-55 | 1 | Blackhole |

Figure 102. Display the current mapping relationship between MAC address, VLAN ID, and port.

### 4.1.4 MAC address query

Quickly query the MAC address in the switch.

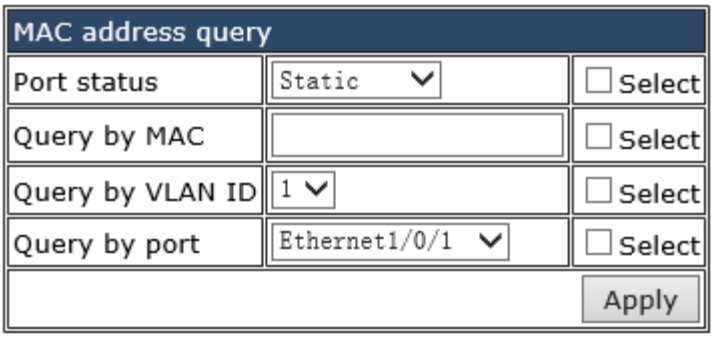



Figure 103.

| | | |
|---|---|---|
| **Port status** | Static | User-created and assigned MAC address. |
| | Dynamic | The MAC address automatically learned by the switch through the message. |
| | Blackhole | The user creates the assigned MAC address, but the packet of this address will not be forwarded by the switch. |
| **Query by VLAN ID** | Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx. | |
| **Query by MAC** | The created VLAN ID, showing the address in the VLAN. | |
| **Query by port** | Find the MAC address by port. | |

Note: Check the small box at the back to make the condition take effect. By default, there is no condition. When there is no condition, all MAC address information will be displayed.

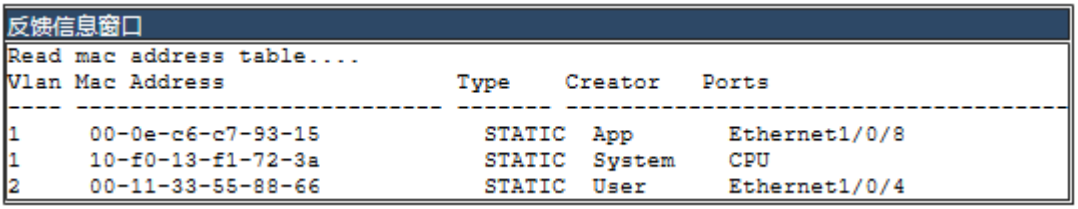



Figure 104. Display the results of the query.

# 5. VLAN configuration

## 5.1 VLAN configuration

### 5.1.1 Create/Remove VLAN

VLAN configuration function module, users add or delete VLANs in this module.

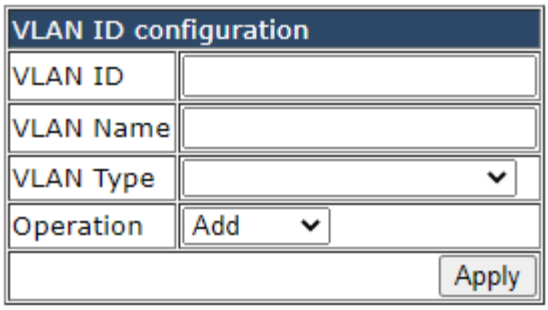



Figure 105.

| | | |
|---|---|---|
| **VLAN ID** | The serial number of the VLAN, range: 2-4094. | |
| **VLAN name** | By default, the default is VLAN plus four-digit serial number, range: 1-64 characters. | |
| **VLAN type** | Private vlan (isolated). Private vlan (community). Private vlan (primary). universal vlan; There are three dedicated VLANs in the Primary port: Primary VLAN, Isolated VLAN and Community VLAN can communicate with the ports of the Isolated VLAN and Community VLAN related to this Primary VLAN; the ports in the Isolated VLAN are isolated from each other and are only related to it. The ports in the Primary VLAN communicate with each other; the ports in the Community VLAN can communicate with each other or with the related Primary VLAN ports; there is no communication between the ports in the Community VLAN and the ports in the Isolated VLAN. There is no communication between the ports in the Community VLAN and the ports in the Isolated VLAN. | |
| **Operation** | Add | Add VLAN. |
| | Remove | Remove VLAN. |

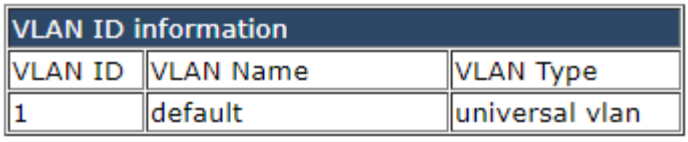



Figure 106.

### 5.1.2 Assign ports for VLAN

Assign ports to the VLAN, and users add and remove ports in the VLAN in this module.

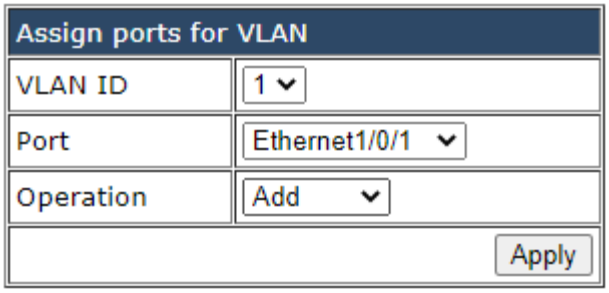


Figure 107.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN. | |
| **Port** | Port name. | |
| **Operation** | Add | Add port to VLAN. |
| | Remove | Remove the port from the VLAN port list. |

### 5.1.3 Port type configuration

Switch port type setting, the user can change the switch port type in this module.

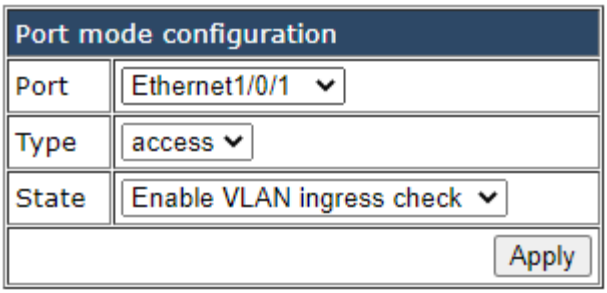
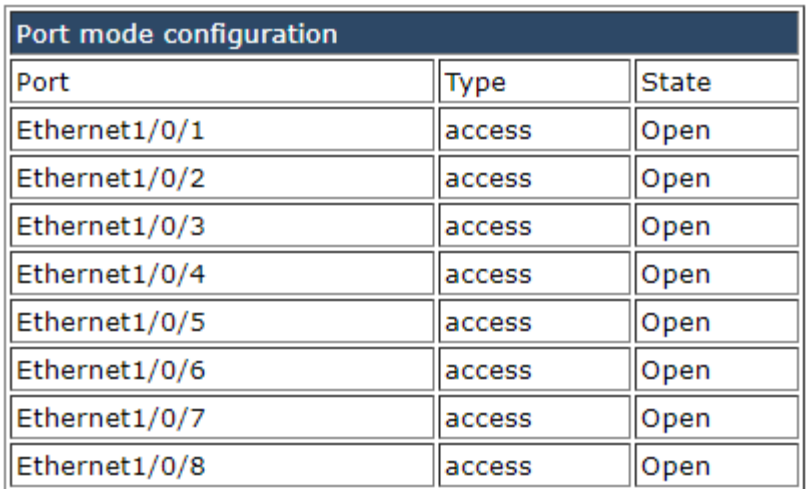



Figure 108.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Type** | access | |
| | trunk | |
| | hybrid | |
| **State** | Enable VLAN ingress check | When a data packet enters the switch, the VLAN ingress filter checks whether the ingress port of the data packet belongs to the given (forwarded) VLAN. |
| | Disable VLAN ingress check | When a data packet enters the switch, the VLAN ingress filter does not check whether the ingress port of the data packet belongs to the given (forwarded) VLAN. |



| 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 |

Figure 109.

### 5.1.4 Hybrid port configuration

Switch Hybrid port VLAN configuration, the user changes the attributes of the switch's Hybrid port type in this module.

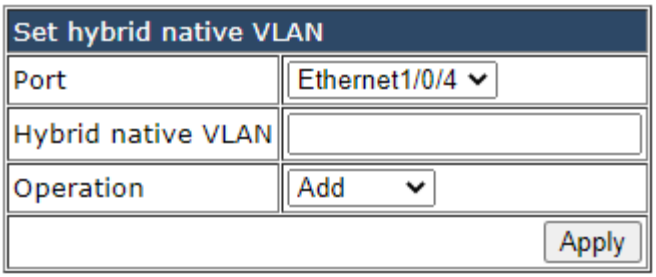



Figure 110.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Hybrid native VLAN** | PVID of the port, VLAN TAG tag when the port is sending and receiving data frames. | |
| **Operation** | Add | Add port to VLAN. |
| | Remove | Remove the port from the VLAN port list. |

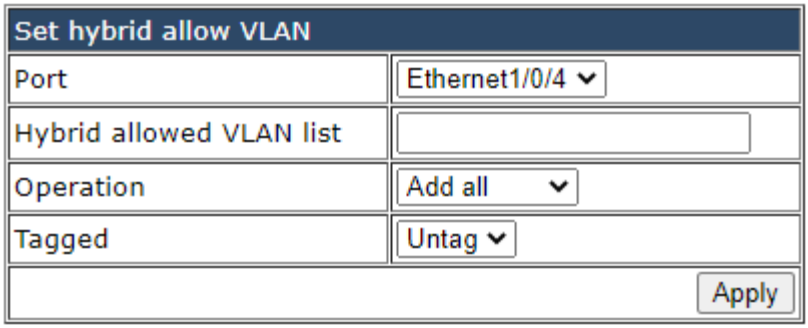



Figure 111.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Hybrid allowed VLAN list** | List of allowed VLANs, connected with "-" and ";". | |
| **Operation** | Add all | Add port to all VLANs, 1-4094. |
| | Add | Add a VLAN to the list of existing passed VLANs. |
| | Except add | Add the port to all VLANs outside the specified VLAN. |
| | Cover add | Clear the original passed VLAN list, and then add the specified VLAN list to the VLAN list. |
| | Remove | Remove the specified VLAN list from the existing passed VLAN list. |
| **Tagged** | Untag method to join. | |
| | Tag way to join. | |

| Port | Hybrid native VLAN | Hybrid Tagged allowed VLAN list | Hybrid UnTagged allowed VLAN list |
|---|---|---|---|
| Ethernet1/0/4 | 1 | | |

Figure 112. Display detailed information of Hybrid port.

### 5.1.5 Trunk port configuration

Switch trunk port VLAN configuration, the user can change the attributes of the trunk port type of the switch in this module.

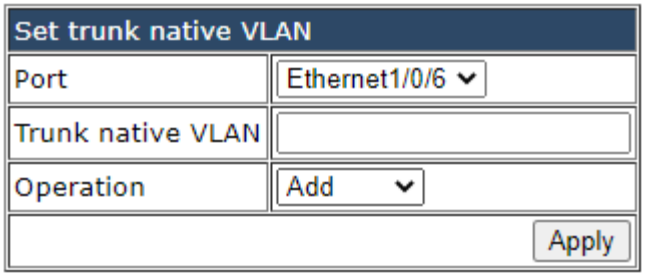



Figure 113.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Trunk native VLAN** | PVID of the port, VLAN TAG tag when the port is sending and receiving data frames. | |
| **Operation** | Add | Add port to VLAN. |
| | Remove | Remove the port from the VLAN port list. |

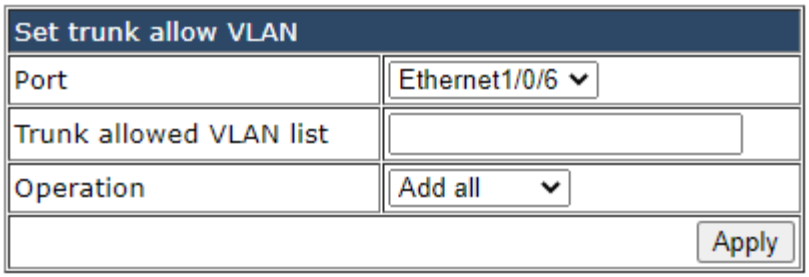



Figure 114.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Trunk allowed VLAN list** | List of allowed VLANs, connected with "-" and ";" | |
| **Operation** | Add | Add port to all VLANs, 1-4094. |
| | Remove | Add a VLAN to the list of existing passed VLANs. |
| | Except add | Add the port to all VLANs outside the specified VLAN. |
| | Cover add | Clear the original passed VLAN list, and then add the specified VLAN list to the VLAN list. |
| | Remove | Remove the specified VLAN list from the existing passed VLAN list. |

| Port | Trunk native VLAN | Trunk allowed VLAN list |
|---|---|---|
| Ethernet1/0/6 | 1 | 1-4094 |

Figure 115. Display the detailed information of the trunk port.

### 5.1.6 Private-vlan configuration

Switch Private-vlan binding operation, the user binds the private-vlan relationship in this module.

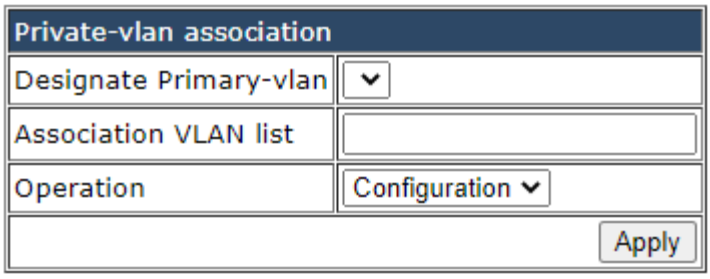



Figure 116.

| | |
|---|---|
| **Designate Primary-vlan** | Created Primary-vlan. |

| | | |
|---|---|---|
| **Association VLAN list** | The secondary VLAN associated with the Primary-vlan, the secondary VLAN includes private vlan (isolated), private vlan (community). | |
| **Operation** | Configuration | Associate the secondary VLAN with the primary VLAN. |
| | Default | Clear the primary-vlan association. |


Figure 117. Display the related information of Primary-vlan.

# 5.2 GVRP configuration

## 5.2.1 Enable global GVRP

The switch starts the global GVRP setting, and the user turns on or off the global GVRP.

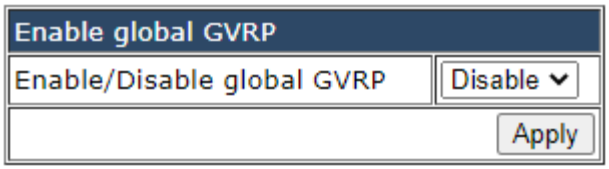



Figure 118.

| | | |
|---|---|---|
| **Enable/Disable global GVRP** | Enable | Start the global GVRP module function. |
| | Disable | Disable the global GVRP module function. |


Figure 119.

## 5.2.2 Enable GVRP on port

The switch port starts GVRP settings, and the user opens or closes the port GVRP.

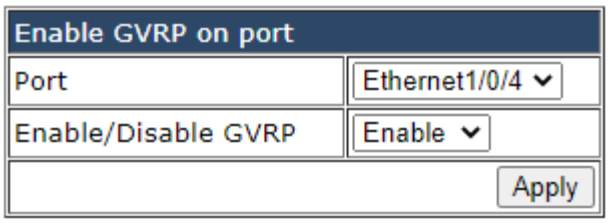



Figure 120.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Enable/Disable** | Enable | Start the port GVRP module function. |

| | | |
|---|---|---|
| **GVRP** | Disable | Disable the port GVRP module function. |

| Port | GVRP Status |
|---|---|
| Ethernet1/0/4 | Disable |
| Ethernet1/0/6 | Disable |

Figure 121. Display the GVRP status of each port.

### 5.2.3 GARP configuration

The switch configures GARP parameters, and the user sets the value of various timers to manage GARP.

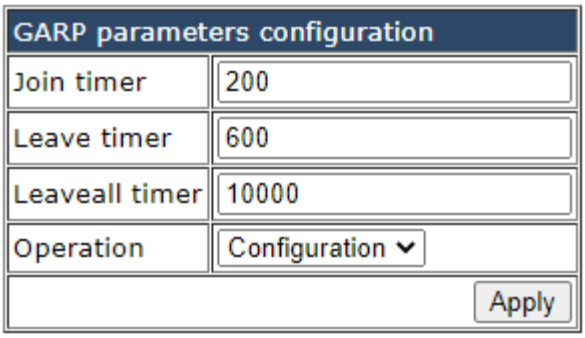



Figure 122.

| | | |
|---|---|---|
| **Join timer** | 200-500ms. | |
| **Leave timer** | 500-1200ms. | |
| **Leaveall timer** | 500-60000ms. | |
| **Operation** | configuration | Modify the value of the timer. |
| | default | Restore the timer value to the default configuration. |

## 5.3 VLAN-translation configuration

### 5.3.1 Enable/Disable VLAN-translation

The switch port starts the VLAN-translation setting, and the user opens or closes the port VLAN-translation.

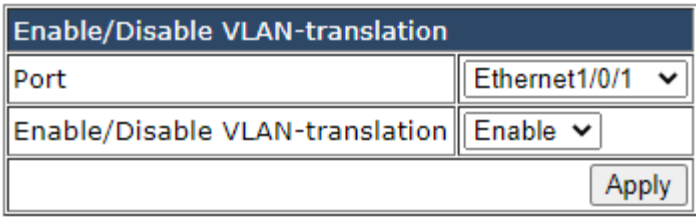
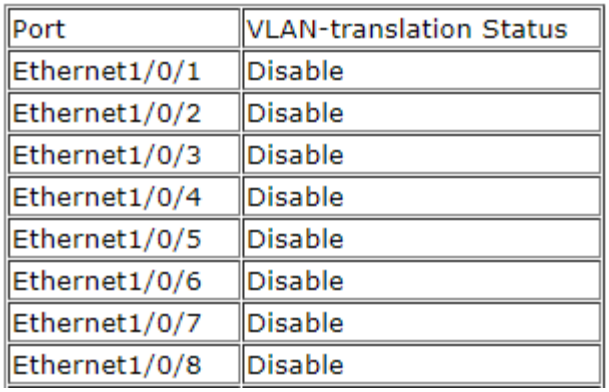



Figure 123.

| | | |
|---|---|---|
| **Port** | Port name | |
| **Enable/Disable VLAN-translation** | Enable | Enable the VLAN-translation function of the port. |
| | Disable | Disable the VLAN-translation function of the port. |



| 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 |

Figure 124. Display the VLAN-translation status of each port.

### 5.3.2 Add/Delete VLAN-translation

Switch VLAN-translation conversion settings, the user sets the VLAN-translation conversion relationship.

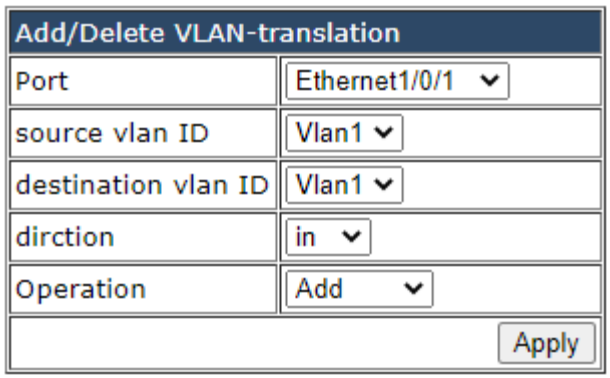



Figure 125.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Source vlan ID** | Configured VLAN. | |
| **Destination vlan ID** | Configured VLAN. | |
| **dirction** | in | Configure the conversion direction of VLAN-translation as the ingress conversion function. |
| | out | Configure the conversion direction of VLAN-translation as the egress conversion function. |
| **Operation** | Add | Add VLAN-translation conversion relationship. |
| | Remove | Remove VLAN-translation conversion relationship. |

### 5.3.3 VLAN-translation miss drop configuration

When the switch VLAN-translation fails to find the translation relationship, the packet loss settings are set. The user sets the direction of the packet loss configuration when the VLAN-translation finds the translation relationship.

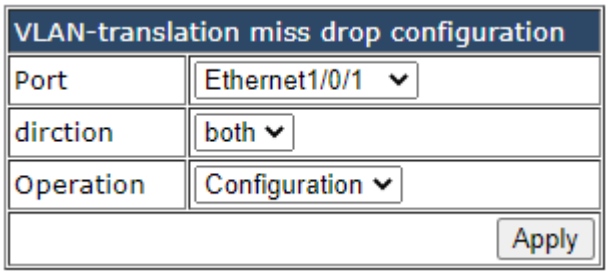



Figure 126.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **dirction** | both | The port performs VLAN-translation search and translation relationship configuration for packet loss at both the egress and the ingress. |
| | in | Packet loss configuration when the port performs VLAN-translation lookup translation relationship at the ingress. |
| | out | Packet loss configuration when the port performs VLAN-translation lookup translation relationship at the egress. |
| **Operation** | Configuration | Add VLAN-translation to find the packet loss configuration when searching for translation relations. |
| | Cancel | Delete the configuration of packet loss when searching for translation relationship in VLAN-translation. |

### 5.3.4 show VLAN-translation

The display of switch VLAN-translation related configuration, the user can check the switch VLAN-translation configuration.


Figure 127.

| | |
|---|---|
| **Apply** | Confirm that you want to view VLAN-translation related configuration information. |

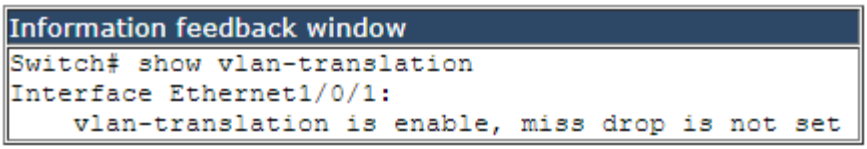



Figure 128. Display VLAN-translation related configuration information.

## 5.4 dynamic VLAN configuration

### 5.4.1 VLAN protocol configuration

Switch VLAN protocol table entry configuration, user configuration protocol VLAN parameters to generate VLAN.

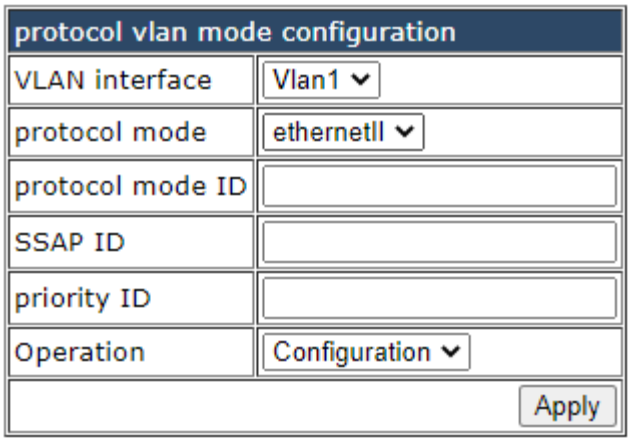



Figure 129.

| | | |
|---|---|---|
| **VLAN interface** | Created VLAN. | |
| **Protocol mode** | ethernetII | VLAN is divided according to data packets in ethernetII format. |
| | snap | VLAN is divided according to data packets in snap format. |
| | llc | VLAN is divided according to data packets in the LLC format. |
| | all | Used when cancel operation, restore all protocol VLAN to static VLAN. |
| **Protocol mode ID** | The ID range of ethernetII and snap is 1536-65535, and the ID range of llc is 0-255. | |
| **SSAP ID** | It is only set in the llc protocol, range: 0-255. | |
| **Priority ID** | Queue priority, range: 0-7. | |
| **Operation** | configuration | Modify VLAN parameters and configure to dynamic protocol VLAN. |
| | cancel | Restore VLAN from dynamic VLAN to static. |

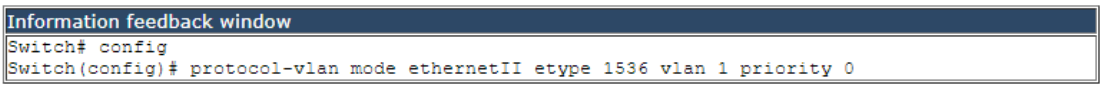



Figure 130. Display configuration info.

# 5.5 Dot1q tunnel configuration

## 5.5.1 Enable dot1q tunnel

Switch dot1q tunnel configuration, the user configures the port to enable the dot1q tunnel function.

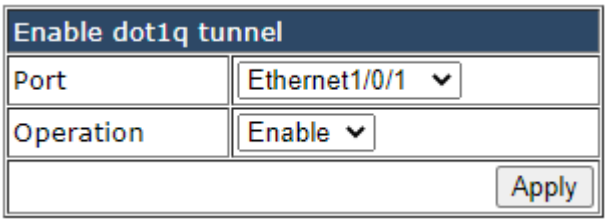



Figure 131.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Operation** | Enable | Enable dot1q tunnel. |
| | Disable | Disable dot1q tunnel. |

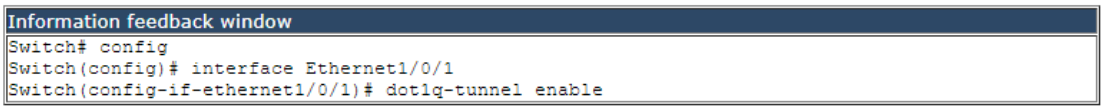



Figure 132. Display the execution process and results.

## 5.5.2 dot1q tunnel tpid configuration

Switch port dot1q tunnel tpid configuration, users configure port dot1q tunnel tpid parameters.

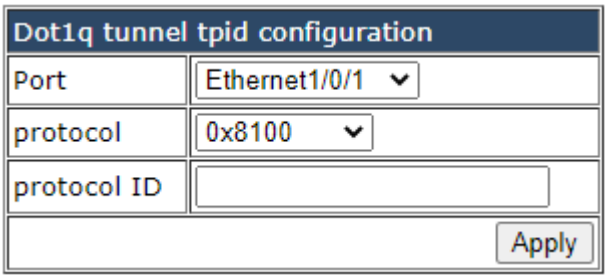



Figure 133.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **Protocol** | 0x8100 | Set the outer TPID to 0x8100. |
| | 0x9100 | Set the outer TPID to 0x9100. |

| | | |
|---|---|---|
| | 0x9200 | Set the outer TPID to 0x920 |
| | protocol ID | Set a custom TPID. |
| **Protocol ID** | The value of the custom TPID. | |

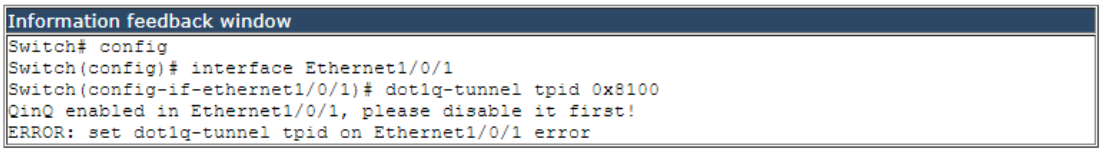



Figure 134. Display the execution process and results.

# 6. IGMP Snooping configuration

## 6.1 Switch on-off IGMP Snooping

Switch IGMP Snooping global switch, snooping IGMP messages.

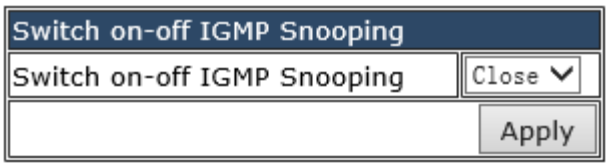



Figure 135.

| | | |
|---|---|---|
| **Switch on-off IGMP Snooping** | Open | Turn on the global switch of IGMP Snooping on the switch. |
| | Close | Turn off the global switch of IGMP Snooping on the switch. |

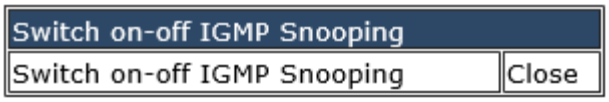



Figure 136. Display the current global status of IGMP Snooping.

## 6.2 IGMP Snooping port enable

Configure IGMP Snooping port switch.

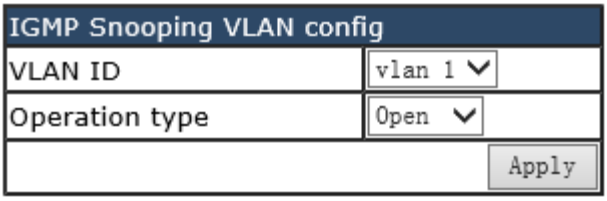



Figure 137.

| | |
|---|---|
| **VLAN ID** | Created VLAN ID. |

| | | |
|---|---|---|
| **Operation type** | Open | Open VLAN interface IGMP Snooping. |
| | Close | Close VLAN interface IGMP Snooping. |

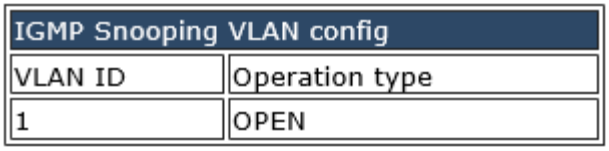



Figure 138. Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface.

## 6.3 IGMP Snooping configuration

Configure IGMP Snooping based on VLAN interface.

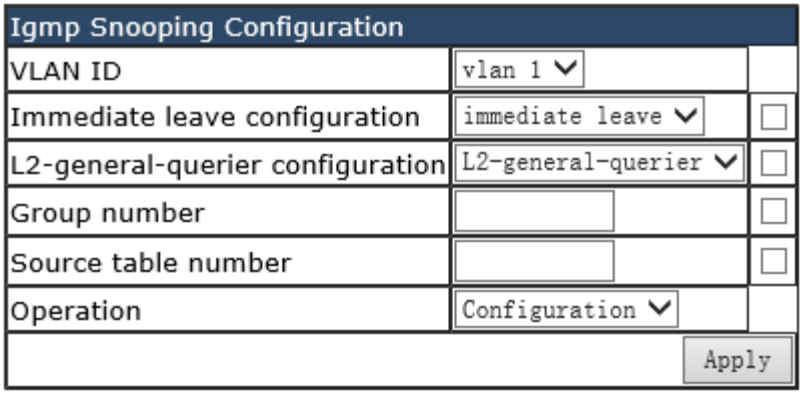



Figure 139.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Immediate leave configuration** | IGMP fast leave function in VLAN. | |
| **L2-general-querier configuration** | Used to send regular queries regularly to help switches in this network segment learn the mrouter port. | |
| **Group number** | The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535. | |
| **Source table number** | The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535. | |
| **Operation type** | Configuration | Configure the checked parameters into the selected VLAN. |
| | Default | Restore the checked parameters to the default state. |

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are

unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

| VLAN ID | Immediate leave configuration | L2-general-querier configuration | Group number | Source table number |
|---|---|---|---|---|
| 1 | Disable | Disable | 50 | 40 |

Figure 140. Display the configuration parameters of the existing VLAN.

## 6.4 IGMP Snooping mrouter configuration

IGMP Snooping mrouter port parameter configuration.

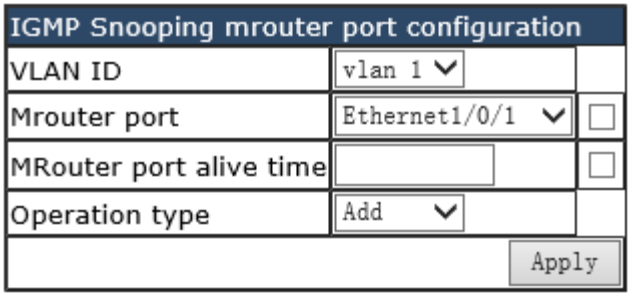



Figure 141.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Mrouter port** | Port name. | |
| **Mrouter port alive time** | Time to live of the port, range: 1-65535. | |
| **Operation type** | Add | Add the mrouter port parameter configuration checked under the selected VLAN. |
| | Remove | Delete the mrouter port parameter configuration checked under the selected VLAN. |

| VLAN ID | Mrouter port | MRouter port alive time |
|---|---|---|
| 1 | | 255 |

Figure 142. Display current configuration information.

## 6.5 IGMP Snooping query configuration

IGMP Snooping query parameter configuration.

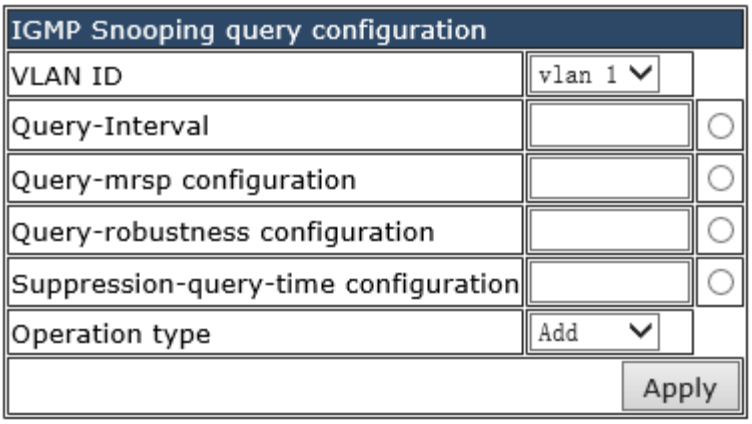



Figure 143.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Query-Interval** | IGMP Snooping query interval, range: 1-65535. | |
| **Query-mrsp configuration** | Maximum response time for group query. | |
| **Query-robustness configuration** | IGMP Snooping robustness, range: 2-10. | |
| **Suppression-query-time configuration** | Prohibited query time, range: 1-65535. | |
| **Operation type** | Add | Add the mrouter port parameter configuration checked under the selected VLAN. |
| | Remove | Delete the mrouter port parameter configuration checked under the selected VLAN. |

| VLAN ID | Query-Interval | Query-mrsp configuration | Query-robustness configuration | Suppression-query-time configuration |
|---|---|---|---|---|
| 1 | 125 | 10 | 2 | 255 |

Figure 144. Display current configuration information.

# 7. MLD Snooping configuration

## 7.1 Switch on-off MLD Snooping

Configure MLD Snooping global status switch.

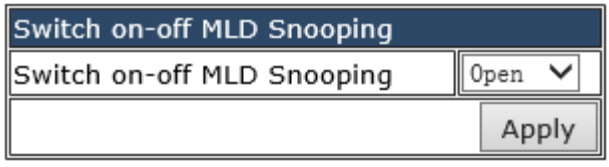



Figure 145.

| | | |
|---|---|---|
| **Switch on-off MLD Snooping** | Open | Turn on the global switch of MLD Snooping on the switch. |
| | Close | Turn off the global switch of MLD Snooping on the switch. |

## 7.2 MLD Snooping port enable

Configure MLD Snooping port switch.

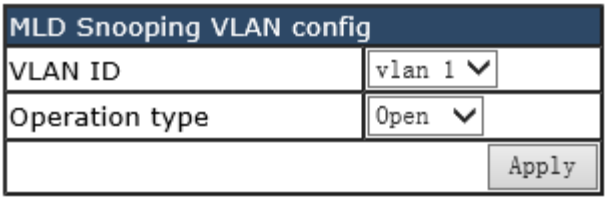



Figure 146.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Operation type** | Open | Open VLAN interface MLD Snooping. |
| | Close | Close VLAN interface MLD Snooping. |

## 7.3 MLD Snooping configuration

MLD Snooping configuration based on VLAN interface.

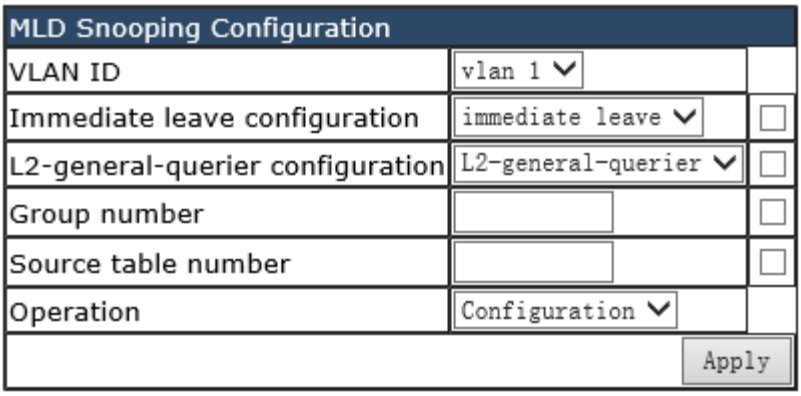



Figure 147.

| | |
|---|---|
| **VLAN ID** | Created VLAN ID. |
| **Immediate leave configuration** | MLD fast leave function in VLAN. |
| **L2-general-querier configuration** | Used to send regular queries regularly to help switches in this network segment learn the mrouter port. |
| **Group number** | The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535. |

| | | |
|---|---|---|
| **Source table number** | The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535. | |
| **Operation** | Configuration | Configure the checked parameters into the selected VLAN. |
| | Default | Restore the checked parameters to the default state. |

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

## 7.4 MLD Snooping mrouter port configuration

MLD Snooping MRouter port parameter configuration.

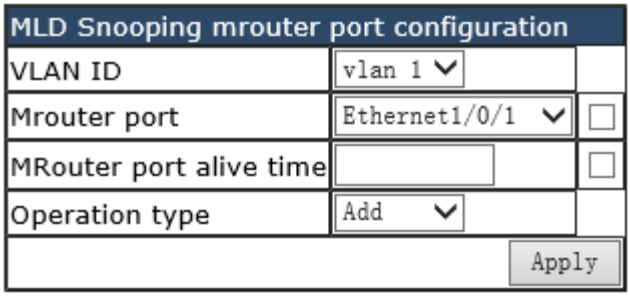



Figure 148.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Mrouter port** | Port name. | |
| **Mrouter port alive time** | Time to live of the port, range: 1-65535. | |
| **Operation type** | Add | Add the mrouter port parameter configuration checked under the selected VLAN. |
| | Remove | Delete the mrouter port parameter configuration checked under the selected VLAN. |

## 7.5 MLD Snooping query configuration

MLD Snooping query parameter configuration.

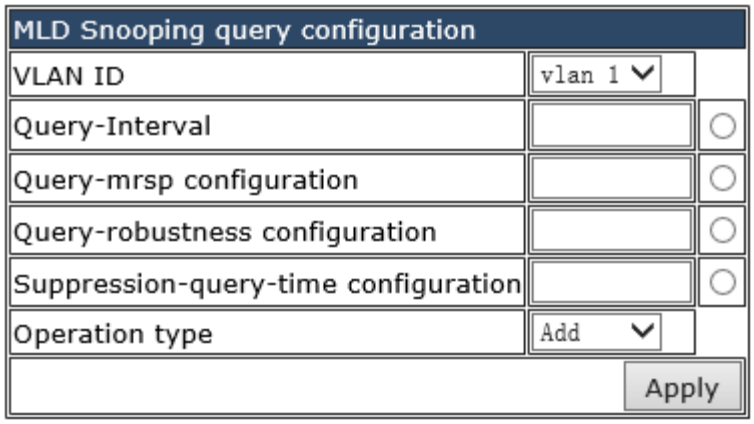



Figure 149.

| | | |
|---|---|---|
| **VLAN ID** | Created VLAN ID. | |
| **Query-Interval** | MLD Snooping query interval, range: 1-65535. | |
| **Query-mrsp configuration** | Maximum response time for group query. | |
| **Query-robustness configuration** | MLD Snooping robustness, range: 2-10. | |
| **Suppression-query-time configuration** | Prohibited query time, range: 1-65535. | |
| **Operation type** | Add | Add the mrouter port parameter configuration checked under the selected VLAN. |
| | Remove | Delete the mrouter port parameter configuration checked under the selected VLAN. |

# 8. Time Range configuration

## 8.1 Time Range configuration

Time Range configuration module, the user can add or delete the operation of in this module, which can be applied to various ACL.

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;31:daily;96:weekdays;127: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.

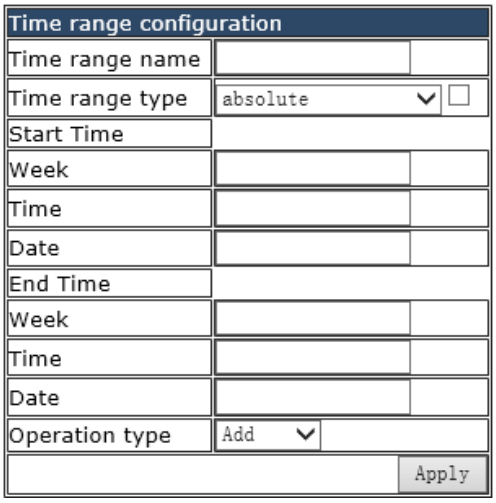



Figure 150.

| | | |
|---|---|---|
| **Time range name** | Time period names must begin with alphabetic or numeric characters, 1-64 characters. | |
| **Time range type** | absolute | Absolutely |
| | absolute-periodic | Absolute-periodic |
| | periodic | periodic |
| **Week** | Start or end weeks, "1-7":"monday-sunday"; "31":"daily"; "96":"weekdays"; "127":"weekend". | |
| **Time** | Start or end time, HH:MM:SS. | |
| **Date** | Start or end date, YYYY.MM.DD, range2001.1.1-2038.12.31. | |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

# 9. ACL configuration

## 9.1 Numeric ACL

### 9.1.1 Standard numeric ACL

#### 9.1.1.1 IP standard ACL

The digital standard IP access list configuration module, where users can create or modify parameters for the digital standard IP access list.

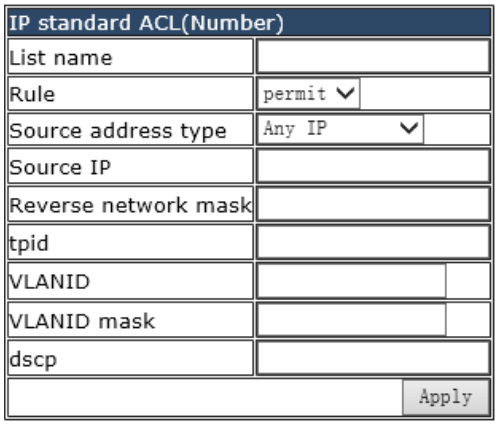



Figure 151.

| | | |
|---|---|---|
| **List name** | Digital Standard IP Access List Number 1-99. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **tpid** | Label Protocol Identification, 0-65535. | |
| **VLANID** | VLAN ID, 1-4094. | |
| **VLANID mask** | VLAN mask，0-4095 | |
| **dcsp** | IP message priority, 0-63. | |

### 9.1.1.2 MAC standard ACL

The digital standard MAC access list configuration module, where users can create or modify parameters for the digital standard MAC access list.

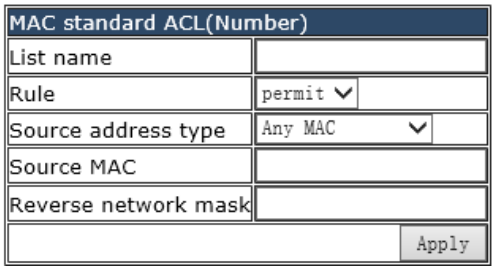



Figure 152.

| | | |
|---|---|---|
| **List name** | Digital Standard MAC Access List Number, 700-799. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any MAC | Match any MAC address. |
| | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Source IP** | Source MAC address. | |
| **Reverse network mask** | Source MAC address inverse mask. | |

## 9.1.2 Extended numeric ACL

### 9.1.2.1 IP extended ACL

The digital extension IP access list configuration module, where users can create or modify parameters for the digital extension IP access list.

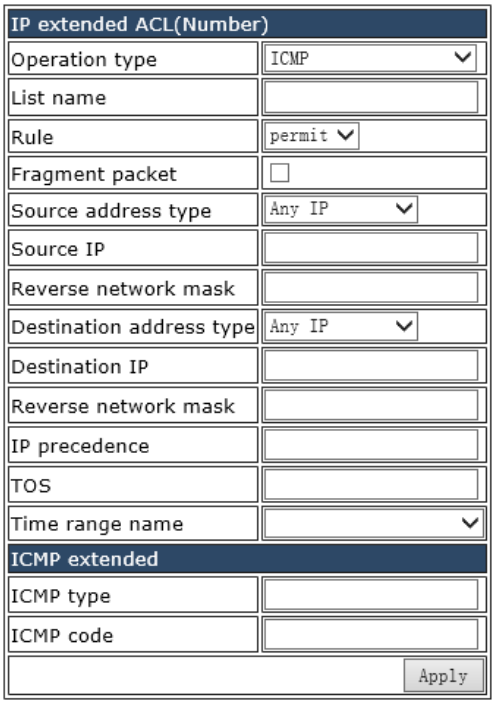



Figure 153.

| | | |
|---|---|---|
| **Operation type** | Extended operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol. | |
| **List name** | Digital extensions IP access list numbers, 100-199. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |

| | | |
|---|---|---|
| **Fragment packet** | Optional whether long messages are transmitted in pieces. | |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **Destination address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Destination IP** | Destination IP, decimal points. | |
| **Reverse network mask** | Destination IP address mask, decimal point. | |
| **IP precedence** | IP priority, 0-7. | |
| **TOS** | Service type, 0-15. | |
| **Time range name** | Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters. | |
| **ICMP type** | ICMP message type, 0-255. | |
| **ICMP code** | ICMP message code, 0-255. | |

#### 9.1.2.2 MAC-IP extended ACL

Digital extension MAC-IP access list configuration module, where users can create or modify parameters for the digital extension MAC-IP access list.

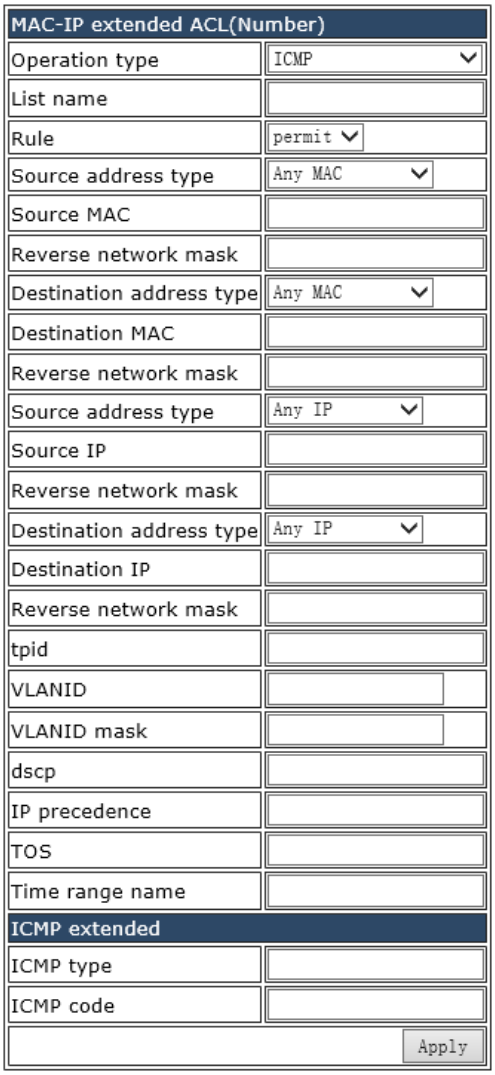



Figure 154.

| | | |
|---|---|---|
| **Operation type** | Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol. | |
| **List name** | Digital Extension MAC-IP Access List Number, 3100-3199. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any MAC | Match any MAC address. |
| | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Source MAC** | Source MAC address. | |
| **Reverse network mask** | Source MAC address inverse mask. | |
| **Destination address** | Any MAC | Match any MAC address. |

| | | |
|---|---|---|
| **type** | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Destination MAC** | Destination MAC. | |
| **Reverse network mask** | Destination MAC address inverse mask. | |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **Destination address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Destination IP** | Destination IP address, decimal point. | |
| **Reverse network mask** | Destination IP address mask, decimal point. | |
| **tpid** | Label Protocol Identification, 0-65535. | |
| **VLANID** | VLAN ID, 1-4094. | |
| **VLANID mask** | VLAN mask, 0-4095. | |
| **dcsp** | IP message priority, 0-63. | |
| **IP precedence** | IP priority, 0-7. | |
| **TOS** | Service type, 0-15. | |
| **Time range name** | Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters. | |
| **ICMP type** | ICMP message type, 0-255. | |
| **ICMP code** | ICMP message code, 0-255. | |

### 9.1.3 Delete Numeric ACL

Delete the digital access list module, where the user can delete the specified digital access list.

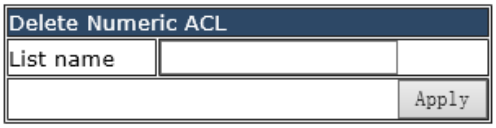


Figure 155.

| | |
|---|---|
| **List name** | Specify numeric access list numbers, 1-3199. |

# 9.2 Name ACL

## 9.2.1 Standard name ACL

### 9.2.1.1 IP standard ACL

Naming standard IP access list configuration module, where users can create or modify parameters for naming standard IP access list.

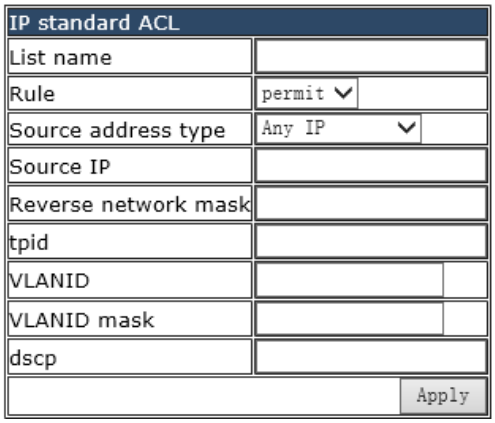



Figure 156.

| | | |
|---|---|---|
| **List name** | Nomenclature criteria IP access list names, strings must start with letters, 1-64 characters. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **tpid** | Label Protocol Identification, 0-65535. | |
| **VLANID** | VLAN ID, 1-4094. | |
| **VLANID mask** | VLAN mask, 0-4095 | |
| **dcsp** | IP message priority, 0-63. | |

## 9.2.2 Extended name ACL

### 9.2.2.1 IP extended ACL

Name extension IP access list configuration module, where users can create or modify parameters for named extension IP access list.

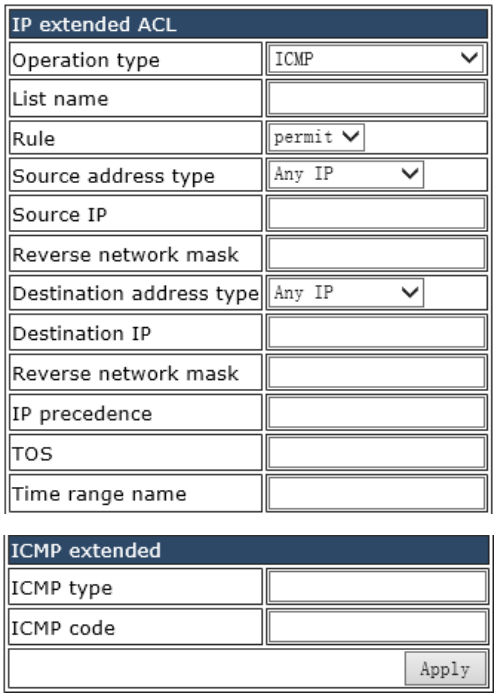



Figure 157.

| | | |
|---|---|---|
| **Operation type** | Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol. | |
| **List name** | Name extensions IP access list names, strings must start with letters, 1-64 characters. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Fragment packet** | Optional whether long messages are transmitted in pieces. | |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **Destination address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |

| | | |
|---|---|---|
| | Host IP | Match the specified host IP. |
| **Destination IP** | Destination IP, decimal points. | |
| **Reverse network mask** | Destination IP address mask, decimal point. | |
| **IP precedence** | IP priority, 0-7. | |
| **TOS** | Service type, 0-15. | |
| **Time range name** | Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters. | |
| **ICMP type** | ICMP message type, 0-255. | |

#### 9.2.2.2 MAC extended ACL

Name extension MAC access list configuration module, where users can create or modify parameters for named extension MAC access list.


Figure 158.

| | | |
|---|---|---|
| **List name** | Digital Extension MAC-IP Access List Number, 3100-3199. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any MAC | Match any MAC address. |
| | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Source MAC** | Source MAC address. | |

| | | |
|---|---|---|
| **Reverse network mask** | Source MAC address inverse mask. | |
| **Destination address type** | Any MAC | Match any MAC address. |
| | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Destination MAC** | Destination MAC address. | |
| **Reverse network mask** | Destination MAC address inverse mask. | |
| **Packet type** | none | none |
| | tagged-802-3 | Format of marked Ethernet 802-3 packets. |
| | tagged-eth2 | Format of marked Ethernet II packets. |
| | untagged-802-3 | Format of unmarked Ethernet 802-3 packets. |
| | untagged-eth2 | Format of unmarked Ethernet II packets. |
| **cos** | cos, 0-7. | |
| **cos mask** | cos mask, 0-7. | |
| **VLANID** | VLAN ID, 1-4094. | |
| **VLANID mask** | VLAN mask, 0-4095. | |
| **etherType** | Ethernet type field value, 1536-65535. | |
| **etherType mask** | Ethernet type field value mask, 0-65535. | |

#### 9.2.2.3 MAC-IP extended ACL

Name extension MAC-IP access list configuration module, where users can create or modify parameters for named extension MAC-IP access list.


Figure 159.

| | | |
|---|---|---|
| **Operation type** | Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol. | |
| **List name** | Digital Extension MAC-IP Access List Number, 3100-3199. | |
| **Rule** | permit | Rule permit. |
| | deny | Rule deny. |
| **Source address type** | Any MAC | Match any MAC address. |
| | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Source MAC** | Source MAC address. | |
| **Reverse network mask** | Source MAC address inverse mask. | |
| **Destination address** | Any MAC | Match any MAC address. |

| | | |
|---|---|---|
| **type** | Specified MAC | Match MAC specified address. |
| | Host MAC | Match the specified host MAC. |
| **Destination MAC** | Destination MAC address. | |
| **Reverse network mask** | Destination MAC address inverse mask. | |
| **Source address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Source IP** | Source IP address, decimal point. | |
| **Reverse network mask** | Source IP address mask, decimal point. | |
| **Destination address type** | Any IP | Match any IP address. |
| | Specified IP | Match IP specified address. |
| | Host IP | Match the specified host IP. |
| **Destination IP** | Destination IP, decimal points. | |
| **Reverse network mask** | Destination IP address mask, decimal point. | |
| **tpid** | Label Protocol Identification, 0-65535. | |
| **VLANID** | VLAN ID, 1-4094. | |
| **VLANID mask** | VLAN mask, 0-4095. | |
| **dcsp** | IP message priority, 0-63. | |
| **IP precedence** | IP priority, 0-7. | |
| **TOS** | Service type, 0-15. | |
| **Time range name** | Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters. | |
| **ICMP type** | ICMP message type, 0-255. | |
| **ICMP code** | ICMP message code, 0-255. | |

### 9.2.3 Delete name ACL

Delete the named access list module, where users can delete the specified named access list.

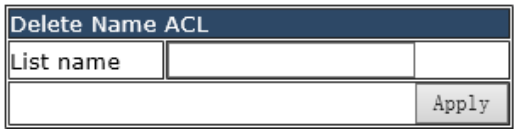


Figure 160.

| | |
|---|---|
| **List name** | String must start with a letter, 1-64 characters. |

# 9.3 Filter configuration

## 9.3.1 Firewall configuration

Firewall ACL configuration module in which users can operate switch firewall configuration.

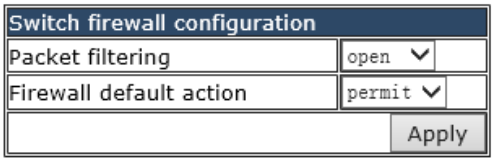



Figure 161.

| | | |
|---|---|---|
| **Packet filtering** | open | open |
| | close | close |
| **Firewall default action** | permit | Rule permit. |
| | deny | Rule deny. |

# 9.4 Show ACL configuration

## 9.4.1 Show access list

The access control list module is displayed in which the user can display ACL specified information or all ACL information.

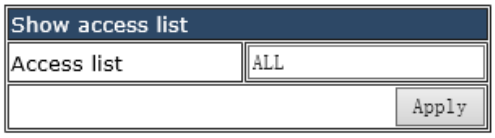



Figure 162.

| | |
|---|---|
| **Access list** | Specify the ACL name or number to display ALL display all ACL. |

## 9.4.2 Show firewall

Display packet filtering function configuration information module, user in this module can display firewall status information.


Figure 163.

### 9.4.3 Show time range

Display time range function configuration information module, where users can display configured custom time information.

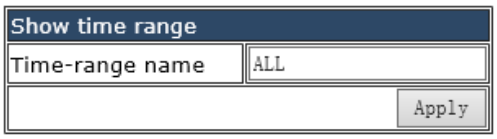



Figure 164.

| | |
|---|---|
| **Time-range name** | Specifies the time period name to display, ALL displays all time period information. |

## 9.5 ACL binding configuration

### 9.5.1 Attach ACL to port

ACL port binding module, the user can bind and delete the access list of the specified port.

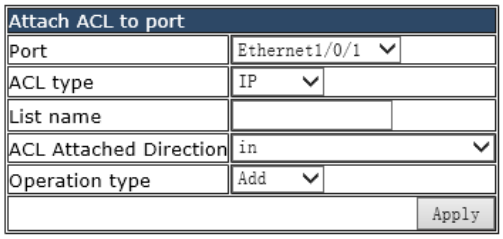



Figure 165.

| | | |
|---|---|---|
| **Port** | Designated port number. | |
| **ACL type** | IP | IP type. |
| | MAC | MAC type. |
| | MAC-IP | MAC-IP type. |
| **List name** | Specify access list name, 1-64 characters. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

### 9.5.2 Show access group

The configuration information module on ACL display port, where the user can display the ACL binding information of the specified port or all ports.

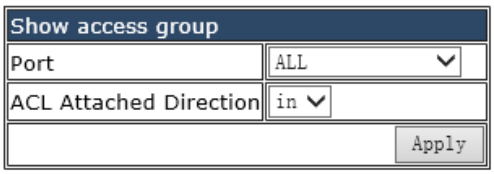



Figure 166.

| | | |
|---|---|---|
| **Port** | Specifies the port number to display the information ALL displays all port information. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |

### 9.5.3 Clear Pacl Statistic

The statistical information module ACL the port, where the user can clear the ACL statistics of the specified port.

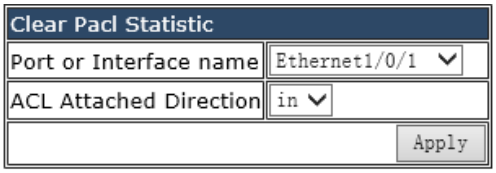



Figure 167.

| | | |
|---|---|---|
| **Port or Interface name** | Specifies the port number to clear statistics. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |

### 9.5.4 Attach ACL to vlan

ACL vlan binding module, where users can bind and delete access lists to specified VLAN.

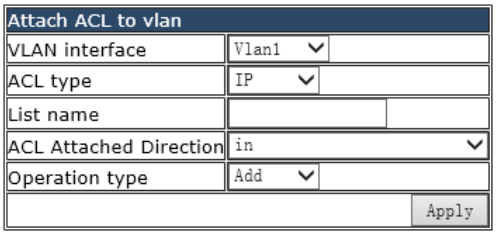



Figure 168.

| | |
|---|---|
| **VLAN interface** | Specifies the VLAN number to operate on. |
| **ACL type** | Specifies the type of ACL to bind: IP.MAC.MAC-IP. |
| **List name** | Specify access list name, 1-64 characters. |

| | | |
|---|---|---|
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

### 9.5.5 show vacl configuration

The vlan acl configuration information module is displayed in which the user can display ACL binding information for the specified VLAN or all VLAN.

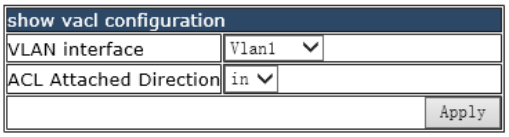



Figure 169.

### 9.5.6 clear vlan acl statistic

Clear the VLAN acl statistical information module, where the user can clear the ACL statistics of the specified VLAN.

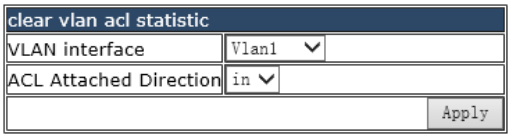



Figure 170.

| | | |
|---|---|---|
| **VLAN interface** | Specifies the VLAN number to clear statistics. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |

# 10. IPv6 ACL configuration

## 10.1 IPv6 standard access-list configuration

IPv6 standard access list configuration module, users can create, delete or modify parameters for digital standard IPv6 access lists.

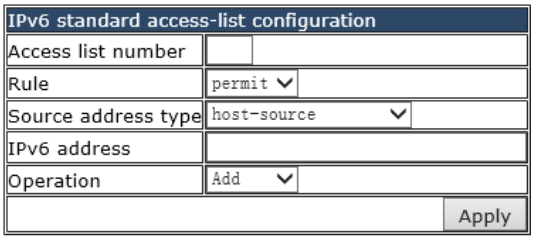



Figure 171.

| | | |
|---|---|---|
| **Access list number** | Digital Standard IPv6 Access List Number, 500-599. | |
| **Rule** | Permit | Rule permit. |
| | Deny | Rule deny. |
| **Source address type** | Specifies IPv6 source host | Matches IPv6 specified source host. |
| | All IPv6 source hosts | Match any IPv6 source host. |
| | IPv6 source address | Match IPv6 specified source address. |
| **IPv6 address** | IPv6 address to operate. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 10.2 IPv6 name access-list configuration

IPv6 named access table configuration module, the user can create, delete, or modify parameters on the named standard IPv6 access list.

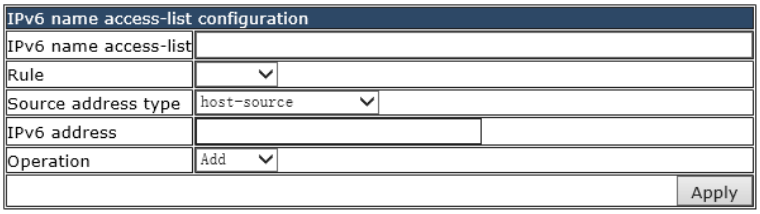



Figure 172.

| | | |
|---|---|---|
| **IPv6 name access-list** | Name of access list. | |
| **Rule** | Permit | Rule permit. |
| | Deny | Rule deny. |
| **Source address type** | Specifies IPv6 source host | Matches IPv6 specified source host. |
| | All IPv6 source hosts | Match any IPv6 source host. |
| | IPv6 source address | Match IPv6 specified source address. |
| **IPv6 address** | IPv6 address to operate. | |
| **Operation** | Add | Add operations. |

| | | |
|---|---|---|
| | Remove | Delete operations. |

## 10.3 Show IPv6 access list

Show IPv6 access control list module where users can display IPv6 access list to create, delete, or modify parameters.


Figure 173.

| | |
|---|---|
| **List name** | Specifies the ACL name or number to display, 0-64 characters. |

## 10.4 Attach IPv6 ACL to port

IPv6 ACL port binding module, the user can bind and delete the IPv6 access list on the specified port.

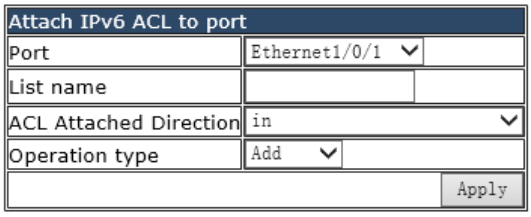



Figure 174.

| | | |
|---|---|---|
| **Port** | Designated port number. | |
| **List name** | Specify access list name, 1-64 characters. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

## 10.5 Attach IPv6 ACL to vlan

IPv6 ACL VLAN binding module, the user can bind and delete the IPv6 access list to the specified VLAN.

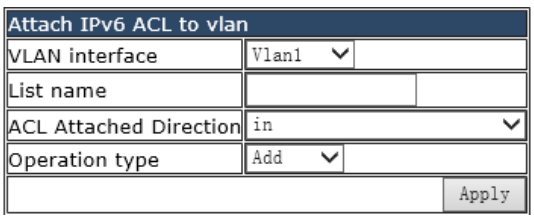


Figure 175.

| | | |
|---|---|---|
| **VLAN interface** | VLAN number specified. | |
| **List name** | Specify access list name, 1-64 characters. | |
| **ACL Attached Direction** | in | Application ACL only. |
| | in and traffic-statistics | Application ACL and flow monitoring. |
| **Operation type** | Add | Add operations. |
| | Remove | Delete operations. |

# 11. AM configuration

## 11.1 AM global configuration

### 11.1.1 Enable/Disable AM

AM switch configuration module, the user can start or close the global AM function in this module.

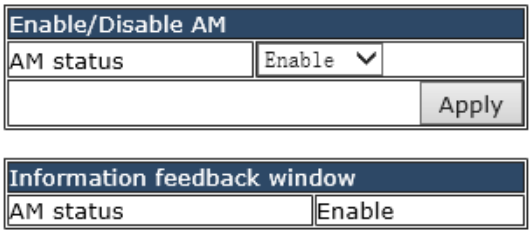



Figure 176.

## 11.2 AM port configuration

### 11.2.1 Enable/Disable AM port

AM port switch configuration module, where the user can start or close the AM function of the specified port.

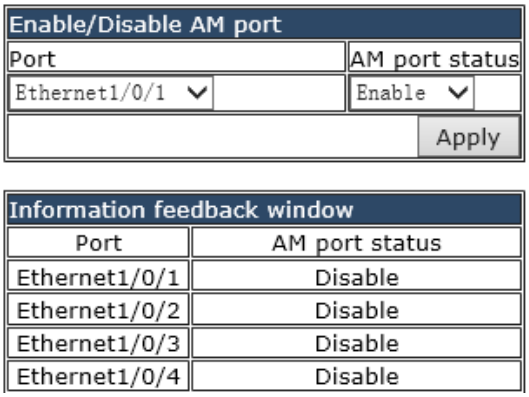



Figure 177.

| | |
|---|---|
| **Port** | Specifies the port number. |

| | |
|---|---|
| **AM port status** | Enable or disable. |

### 11.2.2 AM IP-Pool configuration

AM IP-Pool configuration module, the user can set up an AM IP segment on the specified port, allowing / rejecting messages within the segment to be forwarded through the port.

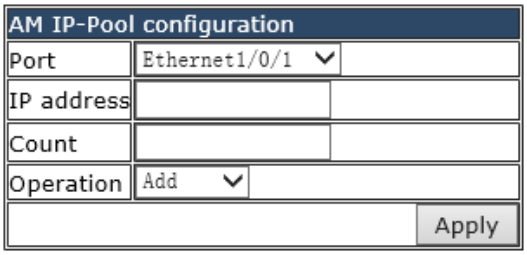



Figure 178.

| | | |
|---|---|---|
| **Port** | Designated port number. | |
| **IP address** | Beginning IP address, decimal point. | |
| **Count** | Number of consecutive addresses after starting IP address, 1-32. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

### 11.2.3 AM MAC-IP-Pool configuration

AM MAC-IP-Pool configuration module, the user can set up an AM MAC-IP segment on the specified port, allowing / rejecting messages from within the segment to be forwarded through the port.

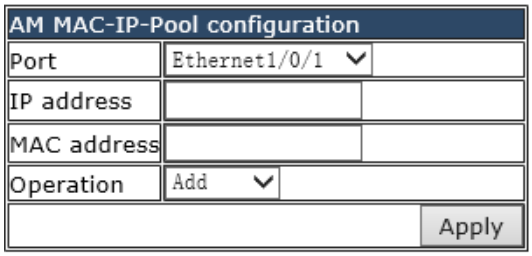



Figure 179.

| | | |
|---|---|---|
| **Port** | Designated port number. | |
| **IP address** | Beginning IP address, decimal point. | |
| **MAC address** | Source MAC address. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 11.3 Show AM port configuration

### 11.3.1 Show AM port configuration

The AM port configuration module is displayed in which the user can display the AM function configuration information of the specified port.

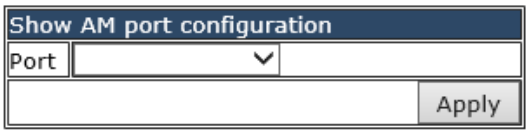



Figure 180.

| | |
|---|---|
| **Port** | Designated port number. |

### 11.3.2 Clear port AM Pool

AM Pool address pool cleanup module, where users can configure the specified AM Pool to clear.

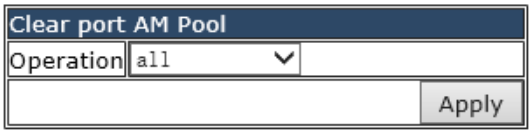



Figure 181.

| | | |
|---|---|---|
| **Operation** | all | Clear all AM Pool. |
| | ip-pool | Clear ip-pool only. |
| | mac-ip-pool | Clear mac-ip-pool only. |

# 12. Port channel configuration

Configure port related features settings using the Port Channel configuration page.

## 12.1 LACP port group configuration

This section can be used to create convergent groups.

To display the “LACP port group configuration” page, click Port channel configuration -> LACP port group configuration, click “Apply” to configure.

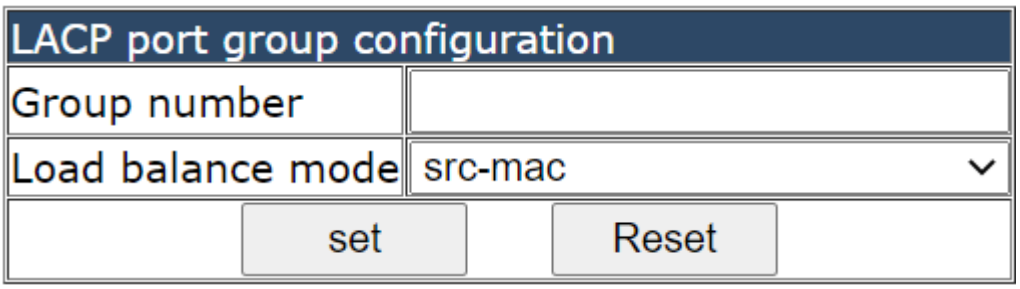



Figure 182.

| entry | describe |
|---|---|
| **Group number** | Range: 1-128. |
| **Load balance mode** | **src-mac**: Execute load balancing according to source MAC.<br>**dst-mac**: Execute load balancing according to target MAC.<br>**dst-src-mac**: Execute load balancing based on source and target MAC.<br>**src-ip**: Execute load balancing according to source IP.<br>**dst-ip**: Execute load balancing according to target IP.<br>**dst-src-ip**: Execute load balancing according to target IP source.<br>**dst-src-mac-ip**: Perform load balancing based on target and source Mac and source IP. |

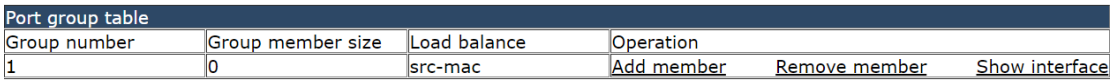



Figure 183.

| entry | describe |
|---|---|
| **Group number** | Convergence group created, size range: 1-128. |
| **Group member size** | Number of members in convergent groups. |
| **Load balance mode** | **src-mac**: Execute load balancing according to source MAC.<br>**dst-mac**: Execute load balancing according to target MAC.<br>**dst-src-mac**: Execute load balancing based on source and target MAC.<br>**src-ip**: Execute load balancing according to source IP.<br>**dst-ip**: Execute load balancing according to target IP.<br>**dst-src-ip**: Execute load balancing according to target IP source.<br>**dst-src-mac-ip**: Perform load balancing based on target and source Mac and source IP. |
| **Operation** | Click on the entry in the corresponding action bar and jump to the corresponding settings page. |

## 12.2 Delete port group

This page can be used to delete created convergent groups.

To display the “Delete port group” page, click Port channel configuration -> Delete port group, click “Apply” to configure.

| Port group table | | | |
|---|---|---|---|
| Group number | Group member size | Load balance | Operation |
| 1 | 0 | src-mac | Delete |

Figure 184.

| | |
|---|---|
| **entry** | describe |
| **Group number** | Range: 1-128. |
| **Group member size** | Number of members in convergent groups. |
| **Load balance** | **src-mac**: Execute load balancing according to source MAC.<br>**dst-mac**: Execute load balancing according to target MAC.<br>**dst-src-mac**: Execute load balancing based on source and target MAC.<br>**src-ip**: Execute load balancing according to source IP<br>**dst-ip**: Execute load balancing according to target IP.<br>**dst-src-ip**: Execute load balancing according to target IP source.<br>**dst-src-mac-ip**: Perform load balancing based on target and source Mac and source IP. |

## 12.3 Show port group info

This page can view the information of the convergent group configuration.

To display the “Show port group info” page, click Port channel configuration -> Show port group info, click “Apply” to view.

```
Information feedback window
Switch# config
Switch(config)# show port-group brief
ID: port group number;  Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
       the first is selected ports number, the second is standby ports number, and
       the third is unselected ports number.
ID   Mode     Partner ID                  Ports       Load-balance
-----------------------------------------------------------------
1                                                     src-mac
Switch(config)# show port-group detail
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Port-group number: 1,  Mode: ,   Load-balance: src-mac
 Port-group detail information:
 System ID: 0x8000,00-1f-ce-10-b0-1b
 Local:
  Port             Status      Priority  Oper-Key Flag
  ---------------------------------------------------------
 Remote:
  Actor           Partner  Priority  Oper-Key SystemID                    Flag
  ---------------------------------------------------------------------------
```

Figure 185.

## 12.4 Show interface port-channel

This page can view the information of the convergent group port.

To display the “Show interface port-channel” page, click Port channel configuration -> Show interface port-channel, click “Apply” to view.

```
Information feedback window
Switch# show interface port-channel 1
Interface brief:
  Port-Channel1 is down, line protocol is down
  Port-Channel1 is layer 2 port, alias name is (null), index is 53
  Port-Channel1 is LAG port, member is :
      Hardware is EtherChannel, address is 00-1f-ce-10-b0-1b
  PVID is 1
  MTU 1500 bytes, BW 10000 Kbit
  Time since last status change:0w-0d-3h-21m-9s  (12069 seconds)
  Encapsulation ARPA, Loopback not set
  Force half-duplex, Auto-speed
  FlowControl is off, MDI type is auto
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
```

Figure 186.

## 12.5 Add member port

This page can be used to add port members to a convergence group.

To display the “Add member port” page, click Port channel configuration -> Add member port, click “Apply” to configure.

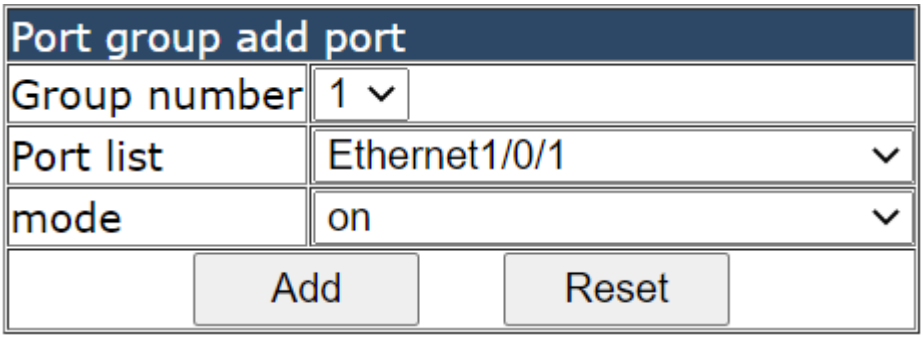



Figure 187.

| | |
|---|---|
| **entry** | describe |
| **Group number** | To create a convergent group number. |
| **Port list** | Ethernet port name. |
| **mode** | On: force port to join port channel without LACP enabled.<br>Active: Enable the LACP on the port and set it to Active mode.<br>Passive: Enable LACP on the port and set it to passive mode. |

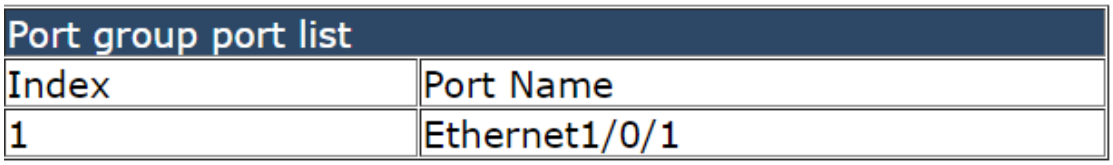



Figure 188.

| | |
|---|---|
| **entry** | describe |
| **Index** | To create a convergent group numb. |
| **Port Name** | Ethernet port name added to convergence group. |

## 12.6 Del member port

This page can be used to delete port members within the convergence group.

To display the “Del member port” page, click Port channel configuration -> Del member port, click “Apply” to configure.

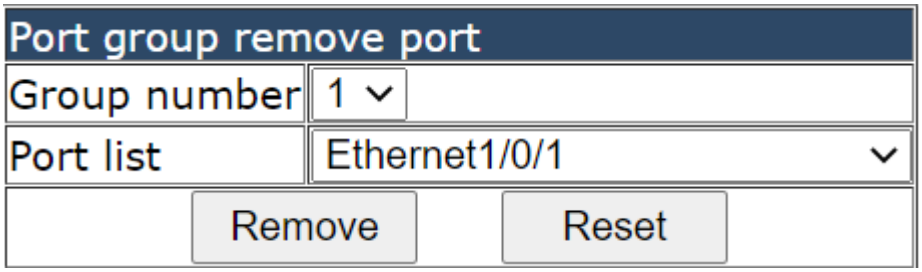



Figure 189.

| entry | describe |
|---|---|
| **Group number** | To create a convergent group number. |
| **Port list** | Ethernet port name. |

## 12.7 Set lacp port priority

This page is available with setting port priority.

To display the “Set lacp port priority” page, click Port channel configuration -> Set lacp port priority, click set to set, click Reset to restore default settings.

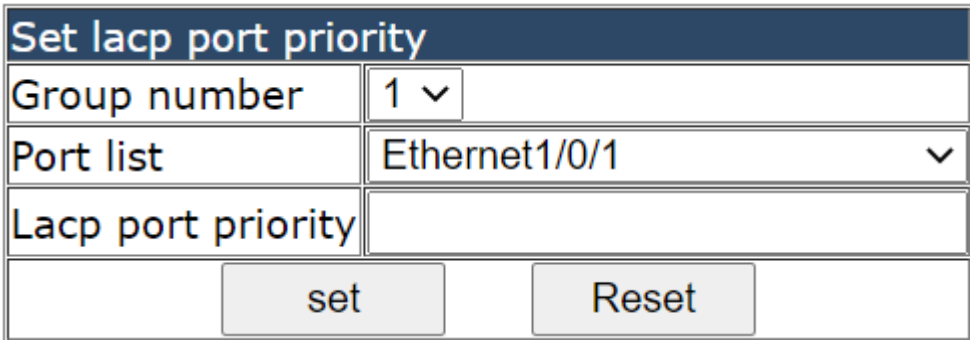



Figure 190.

| entry | describe |
|---|---|
| **Group number** | To create a convergent group number. |
| **Port list** | Ethernet port name added to convergence group. |
| **Lacp port priority** | Range: 0-65535. |

## 12.8 Set lacp system priority

This page is available with setting system priorities.

To display the “Set lacp system priority” page, click Port channel configuration -> Set lacp system priority, click set to set, click Reset to restore default settings.

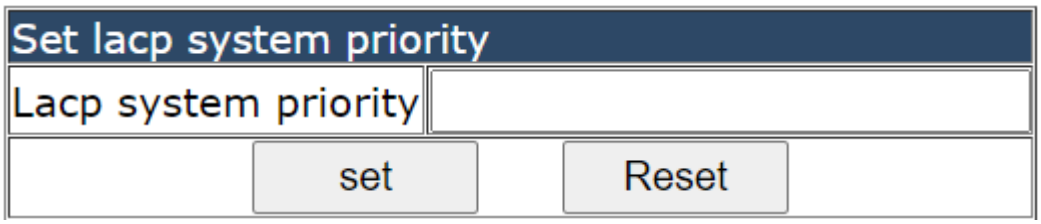



Figure 191.

| entry | describe |
|---|---|
| **Lacp system priority** | Range: 0-65535. |

# 13. DHCP configuration

## 13.1 DHCP management

### 13.1.1 Enable DHCP

DHCP status configuration and query, the user configures the DHCP server status and address conflict log status in this module, and checks the DHCP server status and address conflict log status.

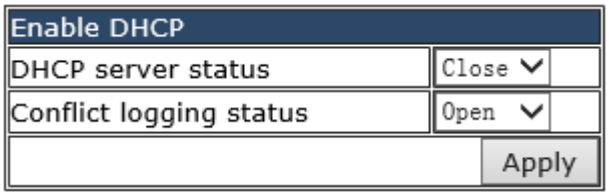



Figure 192.

| | | |
|---|---|---|
| **DHCP server status** | Close | Close DHCP server. |
| | Open | Open DHCP server. |
| **Conflict logging status** | Close | Close address conflict logging. |
| | Open | Open address conflict logging. |
| **Apply** | Apply the currently selected configuration to the switch to make the configuration effective. | |

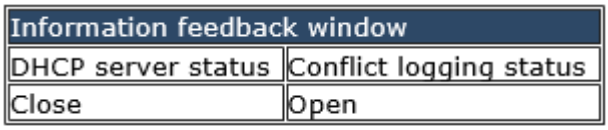



Figure 193.

| | | |
|---|---|---|
| **DHCP server status** | Close | The current DHCP server is off. |
| | Open | The current DHCP server is on. |

| | | |
|---|---|---|
| **Conflict logging status** | Close | The current address conflict log is off. |
| | Open | The current address conflict log is open. |

# 13.2 DHCP server configuration

## 13.2.1 Dynamic pool configuration

### 13.2.1.1 Dynamic address pool configuration

Switch DHCP address pool configuration, the user configures the DHCP address pool parameters.

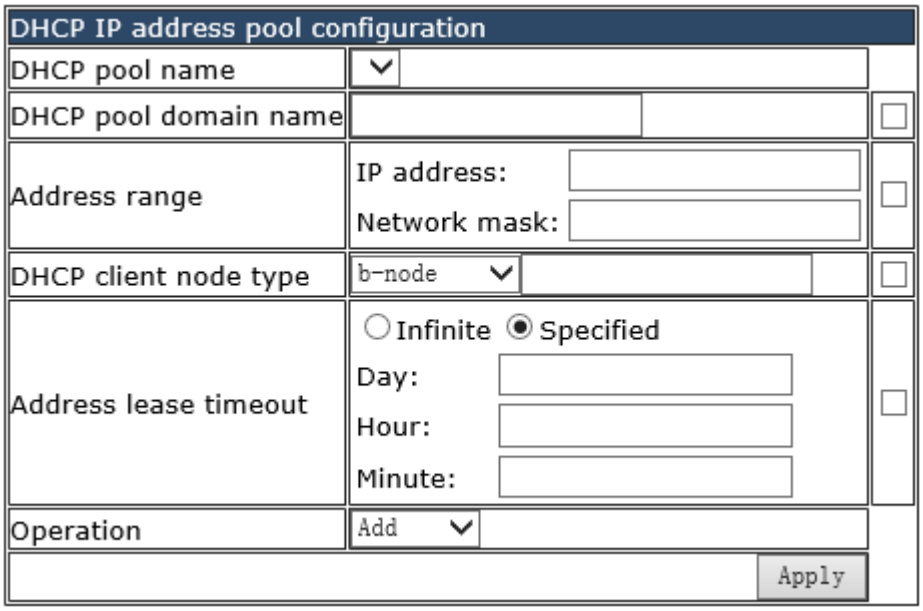



Figure 194.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **DHCP pool domain name** | The domain name of the currently selected address pool. After configuration, you need to tick the box at the back to apply the domain name to the switch during application. | |
| **Address range** | IP address | Network number of the address pool. |
| | Network mask | Netmask of the address pool. |
| **DHCP client node type** | b-node | Broadcast node. |
| | p-node | For point-to-point nodes. |
| | m-node | Used for hybrid nodes to perform point-to-point communication after broadcasting. |
| | h-node | Hybrid nodes that broadcast after peer-to-peer communication. |
| | Designate | Hexadecimal node type, from 0 to 255. |

| | | |
|---|---|---|
| **Address lease timeout** | Infinite | The lease period of the address is unlimited, and the number of days/hours/minutes below do not need to be filled in. |
| | Specified | There is a time limit for the lease of the address. You can rent it according to the lease time filled in below, and it will be automatically recovered if the time is exceeded. |
| **Operation** | Add | Add the above four parameters with check boxes to the switch, the parameters without check boxes will not be operated. |
| | Remove | Restore the four parameters with check boxes to the default configuration, and the parameters without check boxes will not be operated. |

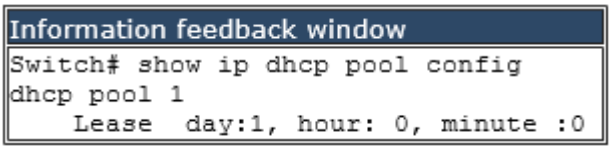



Figure 195. Information display of the currently configured address pool.

### 13.2.1.2 client's default gateway configuration

The switch DHCP client default gateway configuration, the user configures the gateway parameters of the DHCP address pool.

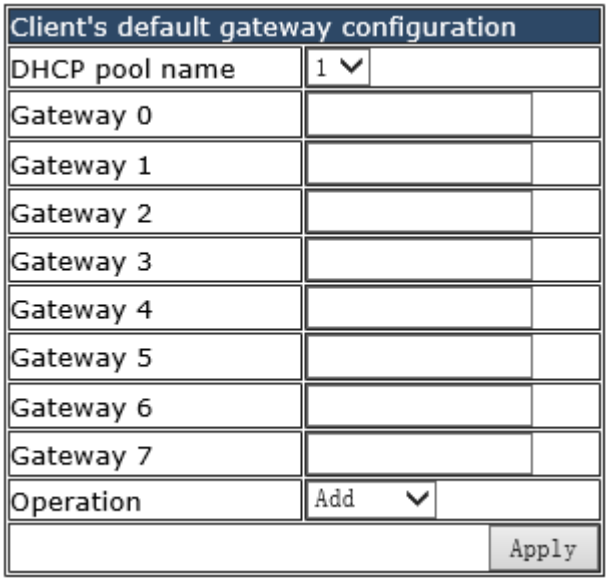



Figure 196.

| | |
|---|---|
| **DHCP pool name** | The name of the created address pool. |
| **Gateway0-7** | Gateway IP address in dotted decimal format. Gateway 0 has the highest |

| | | |
|---|---|---|
| | priority. The smaller the number, the higher the priority. The gateway can be set to zero or more, but the setting must start with 0 and no vacancies can appear in the middle, otherwise the gateway will be Ignore the following parameters, such as setting gateway 0-1 and gateway 7, only gateway 0-1 takes effect. | |
| **Operation** | Add | Add the gateway effectively set above to the currently selected DHCP address pool. |
| | Remove | Clear all gateways and restore to the default state. |

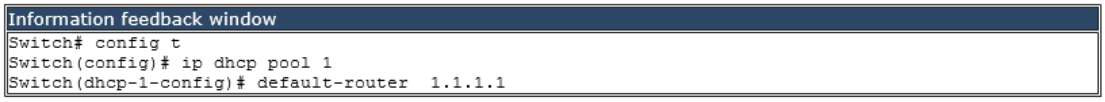



Figure 197. Information display after application.

### 13.2.1.3 Client DNS server configuration

The switch DHCP client DNS server configuration, the user configures the DNS server parameters of the DHCP address pool.

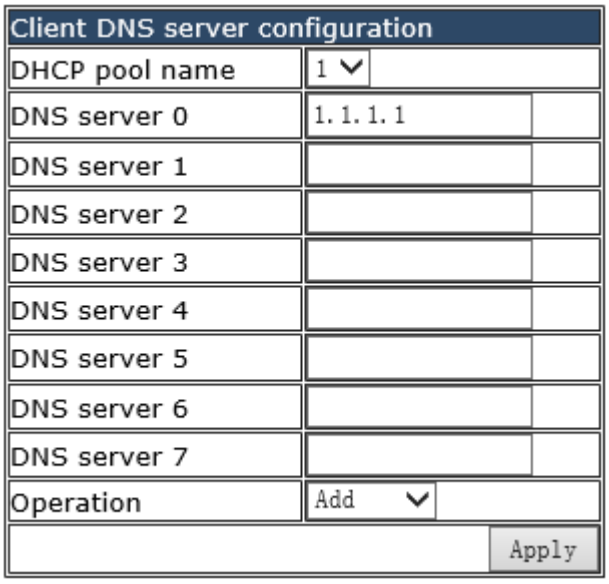



Figure 198.

| | |
|---|---|
| **DHCP pool name** | The name of the created address pool. |
| **DNS server 0-7** | For the IP address in dotted decimal format, DNS server 0 has the highest priority. The smaller the number, the higher the priority. The DNS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise the DNS server The following parameters will be ignored, such as setting DNS server 0-1 and DNS server 7, only DNS |

| | | |
|---|---|---|
| | server 0-1 takes effect. | |
| **Operation** | Add | Add the DNS server effectively set above to the currently selected DHCP address pool. |
| | Remove | Clear all DNS servers and restore to the default state. |


Figure 199. Information display after application.

### 13.2.1.4 Client WINS server configuration

The switch DHCP client WINS server configuration, the user configures the WINS server parameters of the DHCP address pool.

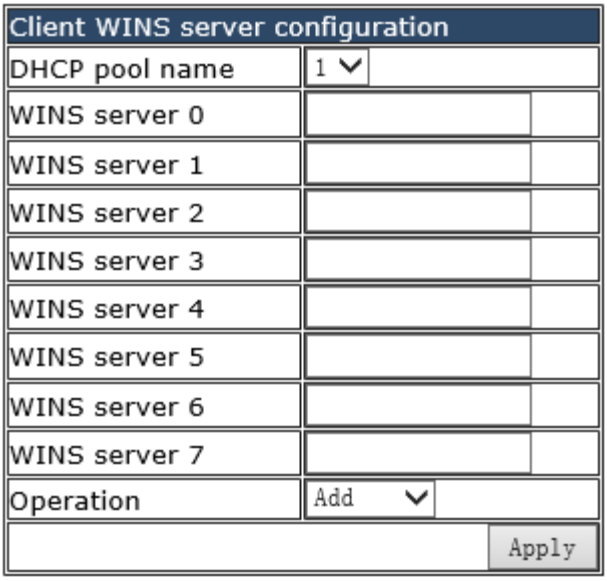



Figure 200.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **WINS server 0-7** | The WINS server IP address in dotted decimal format. WINS server 0 has the highest priority. The smaller the number, the higher the priority. The WINS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise WINS server will ignore the following parameters, such as setting WINS server 0-1 and WINS server 7, only WINS server 0-1 takes effect. | |
| **Operation** | Add | Add the WINS server effectively set above to the currently selected DHCP address pool. |
| | Remove | Clear all WINS servers and restore them to the default |

| | | |
|---|---|---|
| | | state. |


Figure 201. Information display after application.

### 13.2.1.5 DHCP file server address configuration

The switch client import file stores the address configuration, and the user configures the parameters of the DHCP address pool client import file.

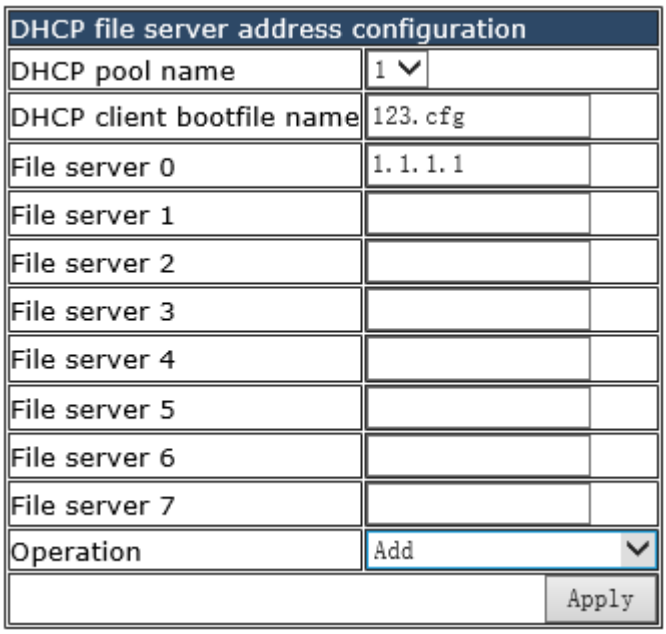



Figure 202.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **DHCP client bootfile name** | Specify the name of the file to be imported for the client. Usually used for diskless workstations, these workstations need to download configuration files from the server at startup. | |
| **File server 0-7** | The IP address in dotted decimal format has the highest priority for importing file server 0. The smaller the number, the higher the priority. The importing file server can be set to zero or more, but the setting must start from 0 and there should be no vacancies in the middle, otherwise Importing file server will ignore the following parameters, such as setting import file server 0-1 and import file server 7, only import file server 0-1 takes effect. | |
| **Operation** | Add | Add the imported file server effectively set above to the currently selected DHCP address pool. |

| | | |
|---|---|---|
| | Remove | Clear all imported file servers and restore to the default state. |

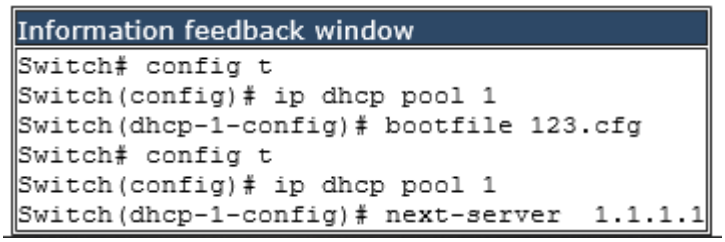



Figure 203. Information display after application.

### 13.2.1.6 DHCP network parameter configuration

Switch network parameter configuration, the user configures the network parameters of the DHCP address pool.

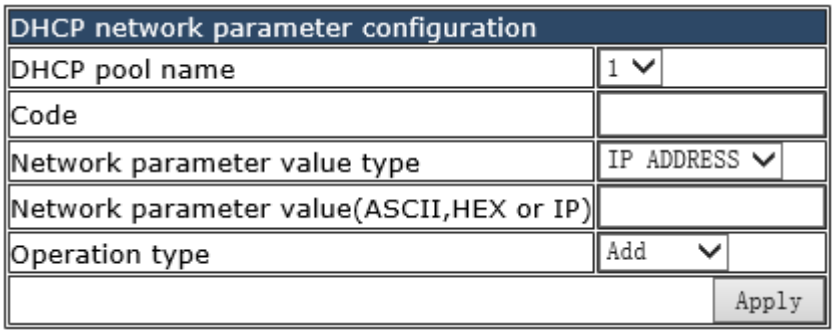



Figure 204.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **Code** | The code range of network parameters is 0-254, and each code corresponds to a different function in DHCP. The definition of option codes is described in detail in RFC2123. | |
| **Network parameter value type** | There are three types of network parameter values: ASCII, HEX, and IP ADDRESS. | |
| **Network parameter value (ASCII, HEX or IP)** | ASCII string, up to 255 characters;<br>Hexadecimal value, not greater than 510, and must be an even number;<br>IP address in decimal format, up to 63 IP addresses can be configured. | |
| **Operation** | Add | Add the network parameters of the selected address pool to the switch. |
| | Remove | Clear the network parameters filled in the selected address pool (delete according to the code of the network |

| | | |
|---|---|---|
| | | parameter). |

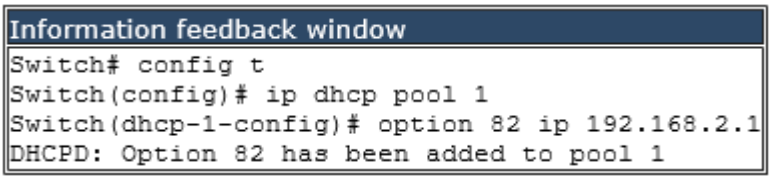



Figure 205. Information display after application.

#### 13.2.1.7 Excluded address configuration

Excluding the dynamic allocation address configuration, the user configures the addresses that are not used for dynamic allocation.

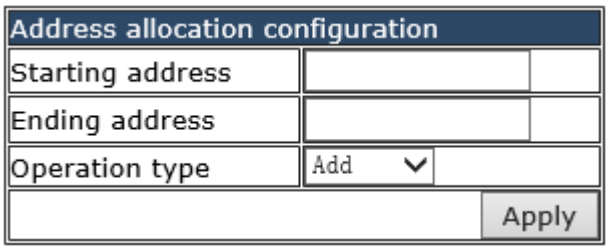



Figure 206.

| | | |
|---|---|---|
| **Starting address** | Start address not used for dynamic allocation. | |
| **Ending address** | End address not used for dynamic allocation. | |
| **Operation type** | Add | Add the address range that is not used and dynamically allocated to the switch. |
| | Remove | Delete the address range that is not used and dynamically allocated from the switch. |

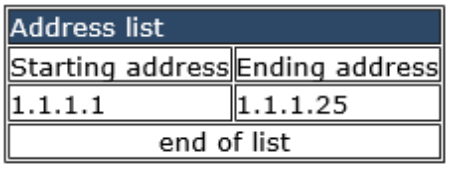



Figure 207. Display the address range currently not used for dynamic allocation.

### 13.2.2 Manual DHCP IP pool configuration

#### 13.2.2.1 Static address pool configuration

Switch static address pool configuration, and manually bind client parameters.

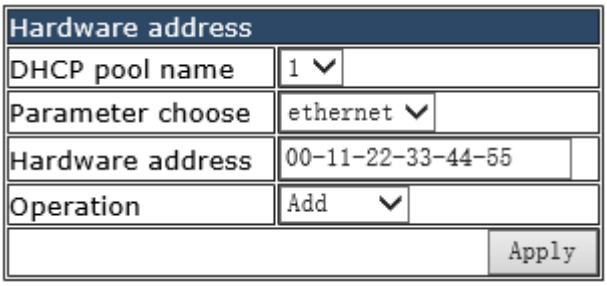



Figure 208.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **Parameter choose** | The protocol type used by the client is rfc\ethernet\ieee802.<br>RFC ID: RFC protocol number, valid range is 1-255. | |
| **Hardware address** | Hardware address. | |
| **Operation** | Add | Add manually bound hardware address and protocol type. |
| | Remove | Remove the manually bound hardware address and protocol type. |

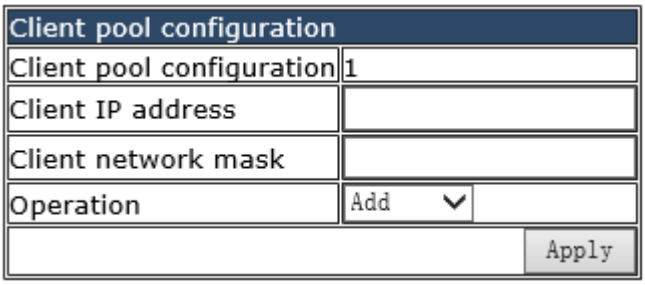



Figure 209.

| | | |
|---|---|---|
| **Client pool configuration** | The name of the created address pool (modify the selection through the address pool name of the user's hardware address). | |
| **Client IP address** | IP address assigned by the DHCP server to the client. | |
| **Client network mask** | The subnet mask assigned by the DHCP server to the client IP. | |
| **Operation** | Add | Add manually bound IP address and subnet mask. |
| | Remove | Delete the manually bound IP address and subnet mask. |

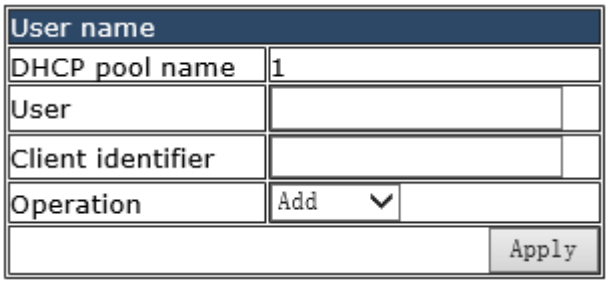



Figure 210.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool (modify the selection through the address pool name of the user's hardware address). | |
| **user** | Client user name. | |
| **Client identifier** | The identifier of the client, for example: 44-11-22-33-44-55 (MAC address). | |
| **Operation** | Add | Add manually bound client identifier and user name. |
| | Remove | Delete the manually bound client identifier and user name. |

### 13.2.3 Address pool name configuration

DHCP server address pool name configuration, user settings add and delete the address pool name.

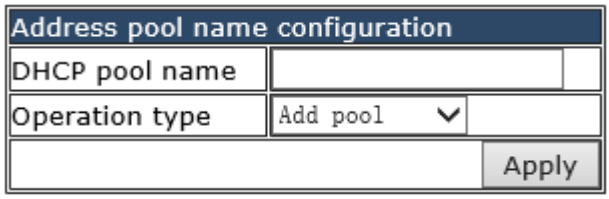



Figure 211.

| | | |
|---|---|---|
| **DHCP pool name** | The name of the created address pool. | |
| **Operation type** | Add pool | Add the address pool of the DHCP server. |
| | Remove pool | Delete the address pool of the DHCP server. |

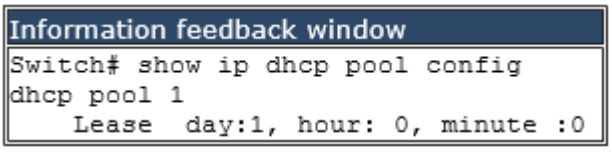



Figure 212. Display the address pool of the current DHCP server.

### 13.2.4 DHCP packet statistics

DHCP server data packet statistics, users can view DHCP data packets.

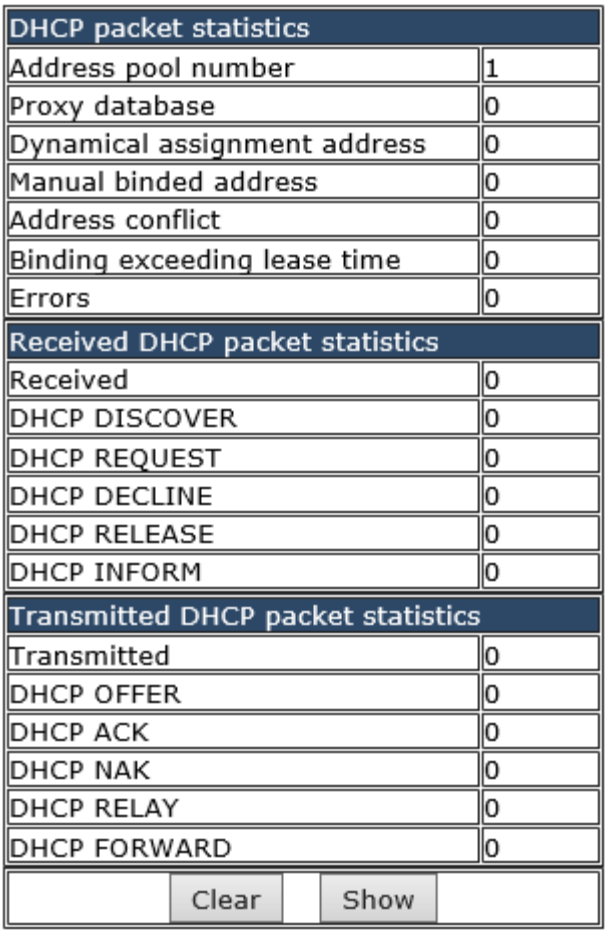



Figure 213. It can be viewed in real time by clicking “Clear and” “Show”.

## 13.3 DHCP relay configuration

### 13.3.1 DHCP relay configuration

The switch DHCP relay configuration, the user configures the port range, and the switch sends UDP broadcast messages to the port.

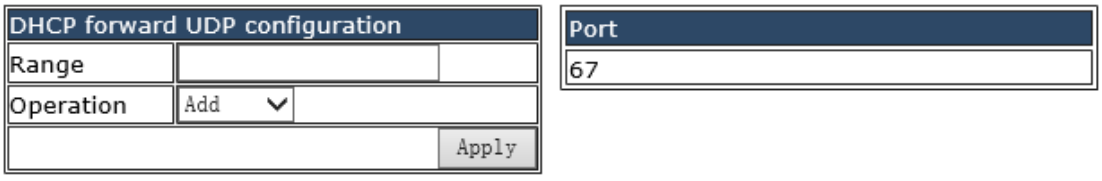



Figure 214.

| | | |
|---|---|---|
| **Range** | Port used by DHCP to forward UDP packets. | |
| **Operation** | Add | Add the port used by DHCP to forward UDP packets. |
| | Remove | Delete the port through which DHCP forwards UDP |

| | | |
|---|---|---|
| | | packets. |

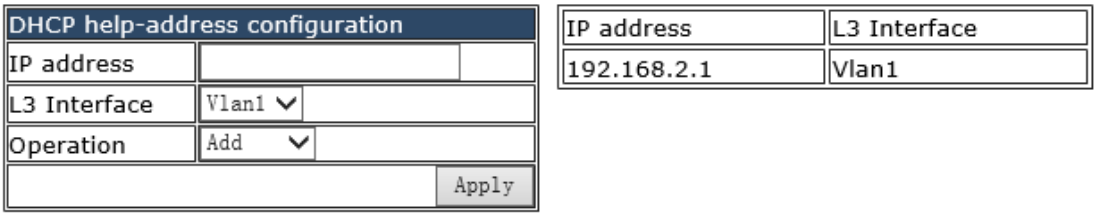



Figure 215.

| | | |
|---|---|---|
| **IP address** | IP address of the Layer 3 interface. | |
| **L3 Interface** | Established Layer 3 interface. | |
| **Operation** | Add | Add a Layer 3 interface for DHCP to forward UDP packets. |
| | Remove | Delete the Layer 3 interface through which DHCP forwards UDP packets. |

# 13.4 DHCP debugging

## 13.4.1 Delete record

### 13.4.1.1 Delete binding log

DHCP binding record deletion, users can delete all binding records or delete specified binding records, static binding records need to be deleted in the static address pool configuration.

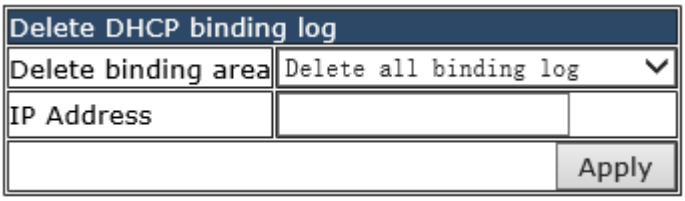



Figure 216.

| | | |
|---|---|---|
| **Delete binding area** | Delete all binding log. | Delete all binding records, no need to fill in the IP address below. |
| | Delete specify binding log. | Delete the specified binding record, fill in the deleted IP in the IP address below. |
| **IP Address** | IP address in dotted decimal notation. | |

### 13.4.1.2 Delete conflict log

The DHCP conflict record is deleted, and the user can delete all conflict records or delete the specified conflict record.

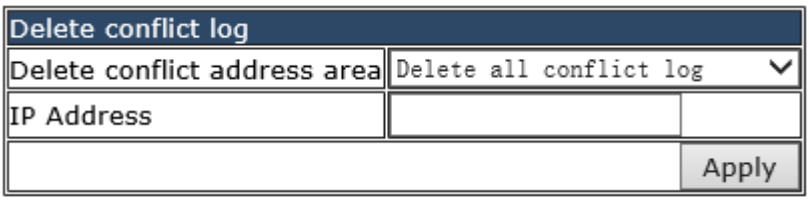



Figure 217.

| | | |
|---|---|---|
| **Delete conflict log** | Delete all conflict log | Delete all conflict records, no need to fill in the IP address below. |
| | Delete specify binding log | Delete the specified conflict record, fill in the deleted IP in the IP address below. |
| **IP Address** | IP address in dotted decimal notation. | |

#### 13.4.1.3 Delete DHCP server statistics log

Deleting the statistics records of the DHCP server, the user can delete all the statistics records of the DHCP server.


Figure 218. After deleting the statistical record of the DHCP server, the statistical information of the DHCP packet will be cleared.

### 13.4.2 show IP-MAC binding

The DHCP server's IP and MAC binding status, the user can view the binding entries and the relationship between the bound IP and MAC.

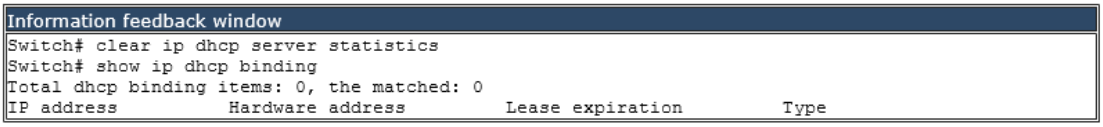



Figure 219.

| | | |
|---|---|---|
| **IP address** | Client's IP address. | |
| **Hardware address** | The hardware address or MAC address of the client. | |
| **Lease expiration** | Client IP expiration time. | |
| **Type** | Manual | Manual binding. |
| | Dynamic | Dynamic allocation. |

### 13.4.3 show conflict-logging

The conflict record of the DHCP server, the user can view the conflict situation.

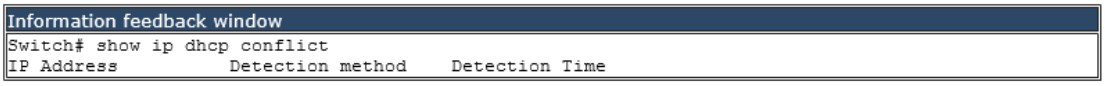



Figure 220.

| | |
|---|---|
| **Display info** | Description. |
| **IP Address** | Conflicting IP address. |
| **Detection method** | The conflicting method was detected. |
| **Detection Time** | The time when the conflict was detected. |

# 14. DHCP Snooping configuration

## 14.1 DHCP Snooping global configuration

### 14.1.1 Enable/Disable DHCP Snooping

With the enabling and disabling of the DHCP Snooping module, users can view and operate the status of DHCP Snooping.

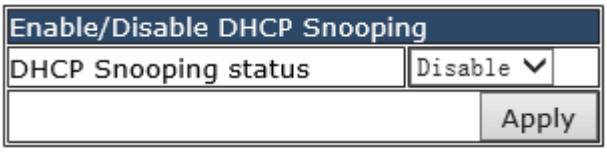



Figure 221.

| | | |
|---|---|---|
| **DHCP Snooping status** | Disable | Disable DHCP Snooping. |
| | Enable | Enable DHCP Snooping. |

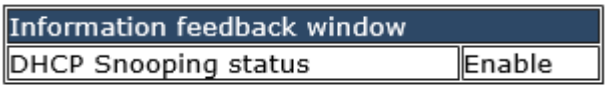



Figure 222. Display the current DHCP Snooping status.

### 14.1.2 DHCP Snooping binding configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

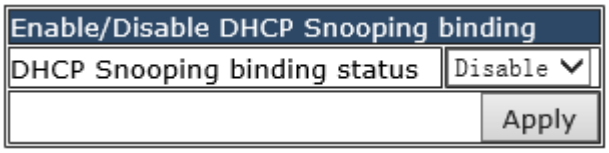


Figure 223.

| | | |
|---|---|---|
| **DHCP Snooping binding status** | Disable | Disable DHCP Snooping binding function. |
| | Enable | Enable DHCP Snooping binding function. |

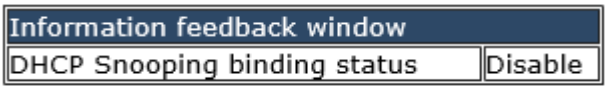



Figure 224. Shows whether the current DHCP Snooping binding status function is enabled.

### 14.1.3 DHCP Snooping binding user configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

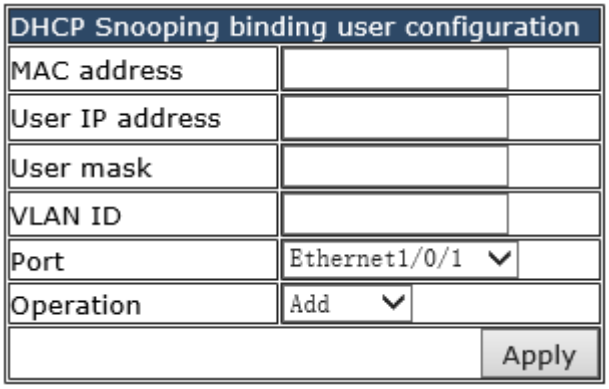



Figure 225.

| | | |
|---|---|---|
| **MAC address** | The MAC address of the statically bound user is the only index of the bound user. | |
| **User IP address** | Statically bind the user's IP address. | |
| **User mask** | Statically bind the user's subnet mask. | |
| **VLAN ID** | Statically bind the VLAN ID of the user. | |
| **Port** | Bind the user's access port statically, the port is associated with the VLAN ID, and the port is required to allow the VLAN to pass. | |
| **Operation** | Add | Add DHCP Snooping binding user relationship. |
| | Remove | Delete DHCP Snooping binding user relationship. |

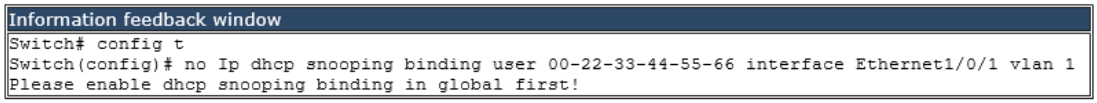


Figure 226. Display the process and error messages or results generated during application execution.

### 14.1.4 DHCP Snooping action count config

DHCP Snooping defense action number configuration, if the number of alarm messages is greater than the set number, it will force the restoration of the earliest defense measures to send new defense measures.

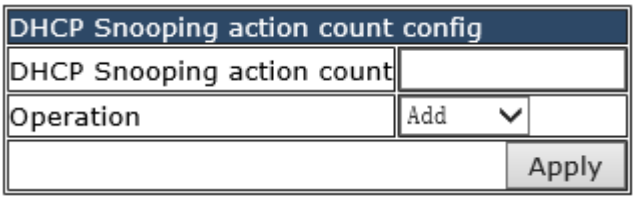



Figure 227.

| | | |
|---|---|---|
| **DHCP Snooping action count** | Set the maximum number of defense actions to avoid exhaustion of switch resources caused by attacks. | |
| **Operation** | Add | Configure the number of defense actions filled in above. |
| | Remove | Reduce the number of defense actions to 10. |


Figure 228. Display the current number of DHCP Snooping defense actions.

### 14.1.5 DHCP Snooping limit-rata config

DHCP Snooping packet receiving rate limit sets the number of DHCP messages sent per second.

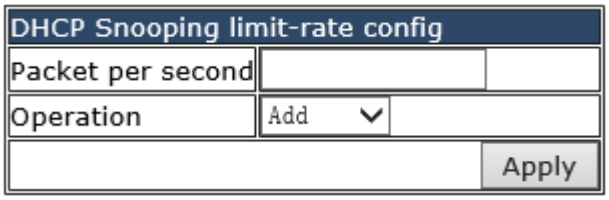



Figure 229.

| | | |
|---|---|---|
| **Packet per second** | Range: 0-100. | |
| **Operation** | Add | Configure the number of packets per second. |
| | Remove | Restore the default number of packets per second, the default is 100. |

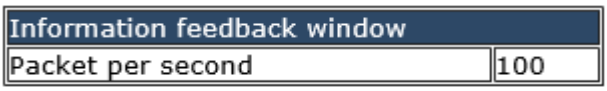



Figure 230. Display the number of packets per second configured for the current DHCP Snooping.

### 14.1.6 DHCP Snooping helper-server config

DHCP SNOOPING will send the monitored binding information to HELPER SERVER for storage. If the switch starts abnormally, you can recover the bound data from the HELPER SERVER.

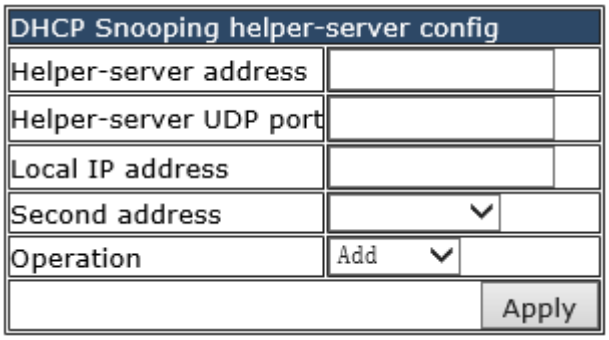



Figure 231.

| | | |
|---|---|---|
| **Helper-server address** | HELPER server address. | |
| **Helper-server UDP port** | DHCP SNOOPING and HELPER SERVER use UDP protocol for communication, the port range is 1-65535. | |
| **Local IP address** | The effective management IP address of the switch. | |
| **Second address** | Two HELPER server addresses are allowed, DHCP SNOOPING will first try to connect to the PRIMARY server. Only when the PRIMARY server cannot be accessed, the switch HELPER server will connect to the SECONDARY server. Set the PRIMARY server before setting up the SECONDARY server. | |
| **Operation** | Add | Add HELPER server address. |
| | Remove | Delete the HELPER server address, you can leave it blank when deleting. |


Figure 232.

Display the process and error messages or results generated during application execution.

## 14.2 DHCP Snooping port configuration

### 14.2.1 Enable/Disable DHCP Snooping binding dot1x

DHCP SNOOPING will notify the DOT1X module of the binding information captured by the user controlled by the DOT1X. DHCP Snooping port binding dot1x function needs to enable DHCP Snooping binding configuration first.

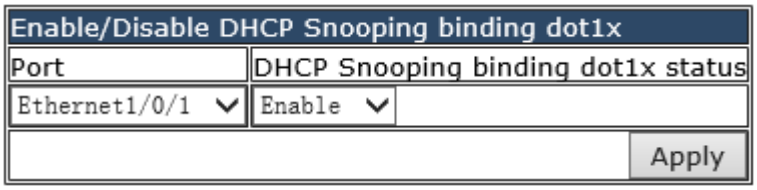



Figure 233.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **DHCP Snooping binding dot1x status** | Enable | Enable the dot1x status of DHCP Snooping port binding. |
| | Disable | Disable the dot1x binding status of the DHCP Snooping port. |

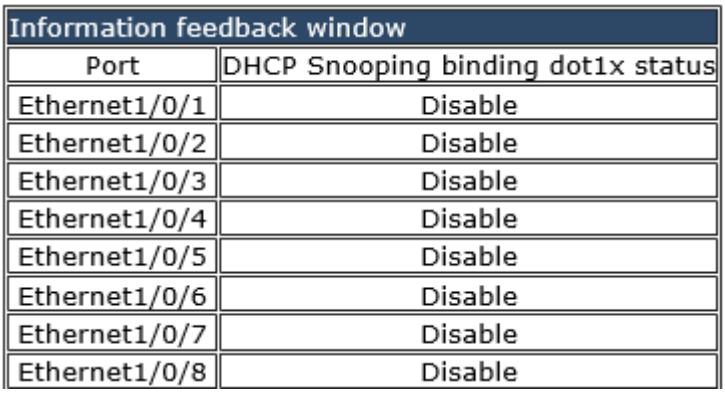



Figure 234. Display the dot1x binding status of each DHCP Snooping port of the switch.

### 14.2.2 Enable/Disable DHCP Snooping binding user

When this function is enabled on the port, DHCP SNOOPING will treat the captured binding information as a trusted user who is allowed to access all resources. The DHCP Snooping port binding user status function needs to enable the DHCP Snooping binding configuration first.

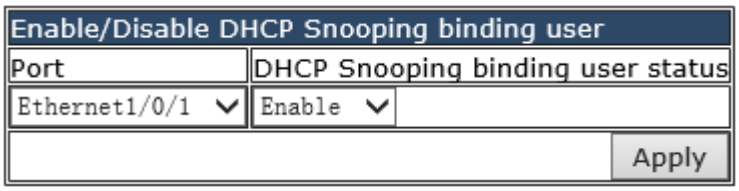



Figure 235.

| | |
|---|---|
| **Port** | Port name. |

| | | |
|---|---|---|
| **DHCP Snooping binding user status** | Enable | Enable DHCP Snooping port binding user status. |
| | Disable | Disable DHCP Snooping port binding user status. |

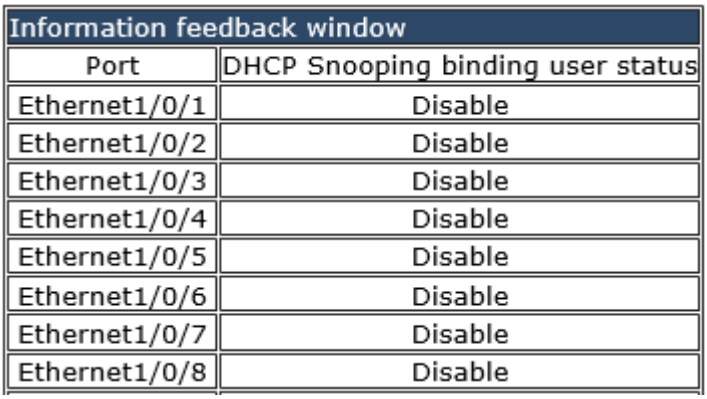



Figure 236. Display the status of users bound to each DHCP Snooping port of the switch.

### 14.2.3 Enable/Disable DHCP Snooping trust

When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted; all security history records will be cleared.

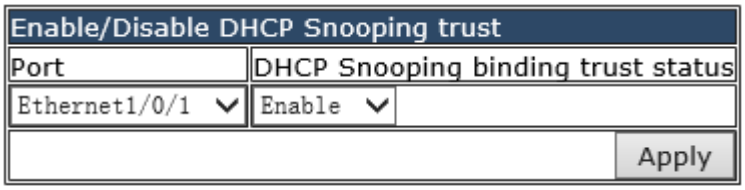



Figure 237.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **DHCP Snooping binding trust status** | Enable | Enable DHCP Snooping port trust attribute status. |
| | Disable | Disable the trust attribute status of the DHCP Snooping 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 |

Figure 238. Display the trust attribute status of each DHCP Snooping port of the switch.

### 14.2.4 DHCP Snooping action config

Automatic port defense action, the port will detect the fake DHCP server, and the trusted port will not detect the fake DHCP server, so the corresponding defense action will never be triggered. When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted.

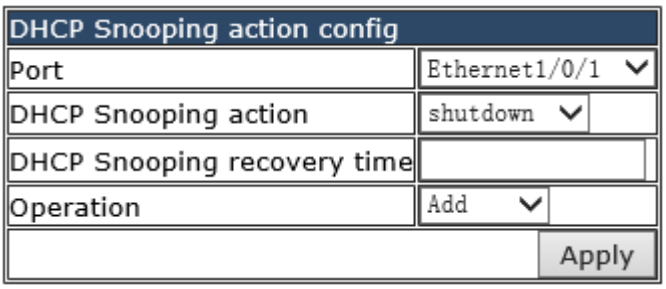



Figure 239.

| | | |
|---|---|---|
| **Port** | Port name. | |
| **DHCP Snooping action** | shutdown | Automatically close the port. |
| | blackhole | Block traffic from fake DHCP server based on MAC. |
| **DHCP Snooping recovery time** | The user can set the recovery after performing automatic defense operations. | |
| **Operation** | Add | Add DHCP Snooping port automatic defense configuration. |
| | Remove | Delete DHCP Snooping port automatic defense configuration. |

| 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 |

Figure 240. Display the automatic defense configuration of each DHCP Snooping port.

## 14.3 show DHCP Snooping configuration

### 14.3.1 show DHCP Snooping configuration

Display detailed configuration of DHCP Snooping.

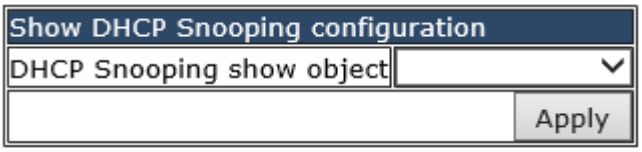



Figure 241.

| | | |
|---|---|---|
| **DHCP Snooping show object** | All | All ports are displayed. |
| | Ethernet1/0/1-28 | Only display information about one port. |

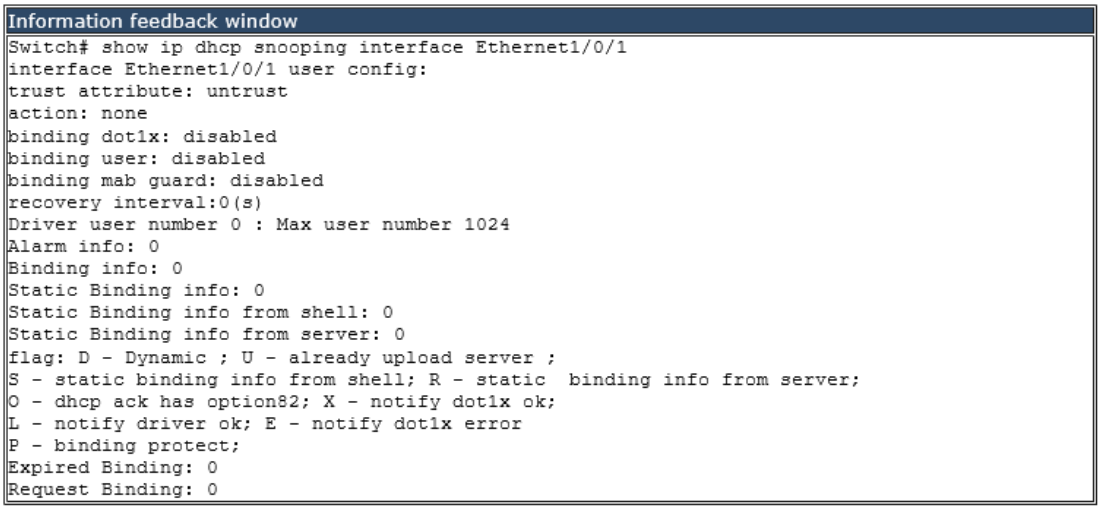



Figure 242. Select Ethernet1/0/1, only display the DHCP Snooping information of Ethernet1/0/1.

# 15. SNTP configuration

## 15.1 SNTP server configuration

SNTP the server settings module, the user can add or delete the specified time server as the clock source.

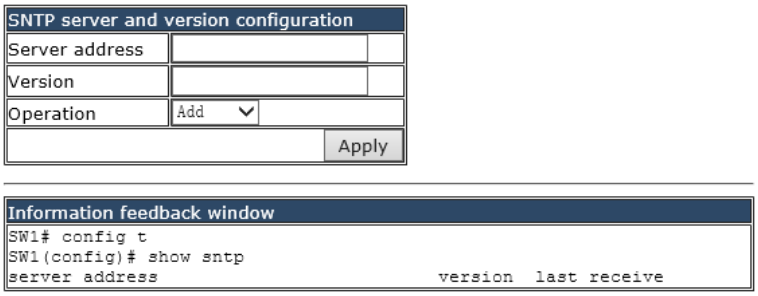



Figure 243.

| | | |
|---|---|---|
| **Server address** | The specified time server address decimal point. | |
| **Version** | Version number, range 1-4, default 4. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 15.2 Request interval configuration

Send request interval setting module, where the user can set the interval SNTP the client sends a request to the NTP/SNTP. By default, the interval is 64 seconds.

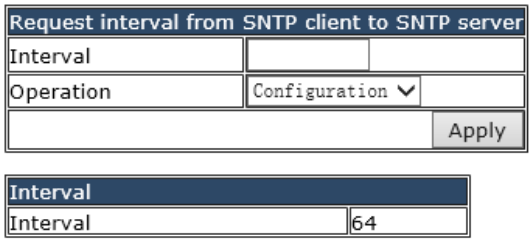



Figure 244.

| | | |
|---|---|---|
| **Interval** | Duration value, range 16-16284 s. | |
| **Operation** | Configuration | Configuration operations. |
| | Default | Do recovery default (default 64 s). |

## 15.3 Time difference configuration

SNTP the time zone and UTC time difference setting module where the client is located, the user can set the switch's current time zone and name it.

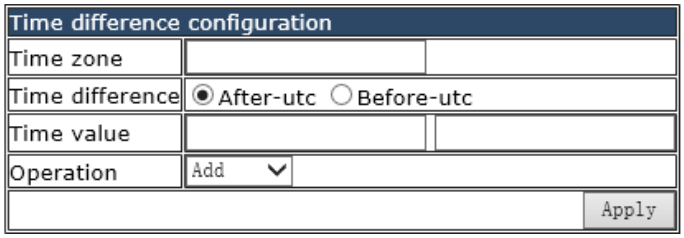



Figure 245.

| | | |
|---|---|---|
| **Time zone** | Time zone name, 1-16 characters. | |
| **Time difference** | Add | Increased time zone behavior. |
| | Reduce | Reduced time zone behavior. |
| **Time value** | Time zone specific change hours 0-23. | Time zone specific change minute value 0-59. |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 15.4 Show sntp

Display SNTP module, where users can view the current information status SNTP the switch.


Figure 246.

# 16. NTP configuration

## 16.1 NTP global configuration

### 16.1.1 NTP global switch configuration

NTP service global switch configuration module, user can NTP service global switch operation.

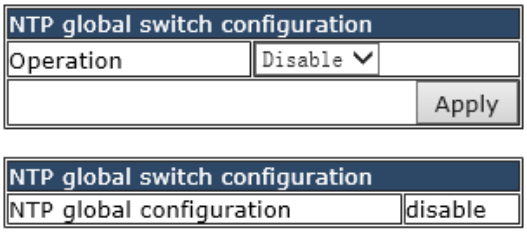



Figure 247.

| | | |
|---|---|---|
| **Operation** | Disable | Close operation. |
| | Enable | Start (default). |

### 16.1.2 NTP server configuration

NTP the server configuration module, the user can configure the specified time server of the switch time source in this module.

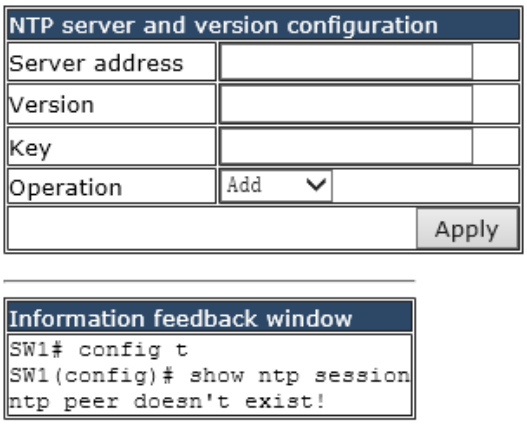



Figure 248.

| | | |
|---|---|---|
| **Server address** | The specified time server address decimal point. | |
| **Version** | Version number, range 1-4, default 4. | |
| **Key** | Secret key value, range 1-4294967295. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

### 16.1.3 NTP broadcast or multicast address count configuration

NTP service address number configuration module, the user can configure the maximum number of broadcast or multicast servers supported by the switch NTP client.

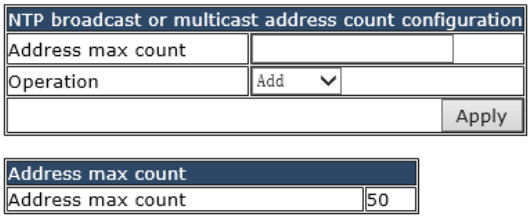



Figure 249.

| | | |
|---|---|---|
| **Address max count** | Maximum number of broadcast or multicast servers supported NTP clients, 1-100 (default 50). | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

### 16.1.4 NTP access group configuration

NTP access control list configuration module, where users can configure switch NTP access control list.

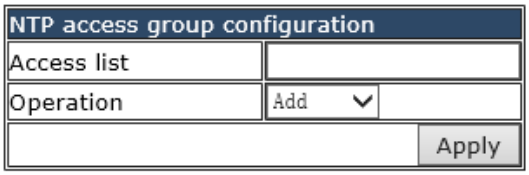



Figure 250.

| | | |
|---|---|---|
| **Access list** | IPv4: 1-99; IPv6: 50-599. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

### 16.1.5 NTP authenticate configuration

NTP verification configuration module, the user can configure the switch NTP authentication related items.

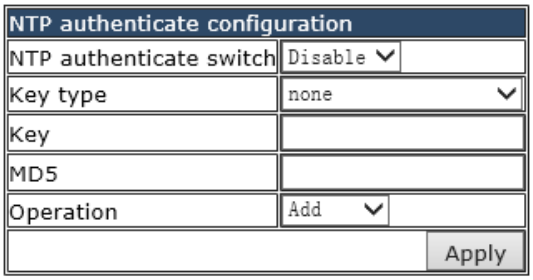



Figure 251.

| | | |
|---|---|---|
| **NTP authenticate switch** | Disable | Close NTP validation (default). |
| | Enable | Enable NTP validation. |
| **Key type** | none | none |
| | authentication-key | Authentication secret key. |
| | trusted-key | Trust key. |
| **Key** | Secret key value, range 1-4294967295. | |
| **Md5** | The MD5 value of the secret key, which ranges from 1-16 of ascii code. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 16.2 NTP interface configuration

### 16.2.1 NTP interface switch configuration

NTP service interface switch configuration module, the user can specify the NTP service interface switch operation.

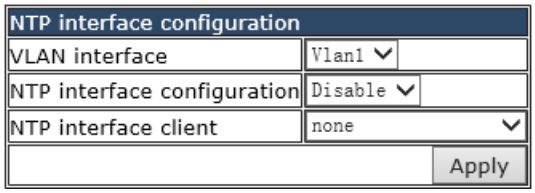



Figure 252.

| | | |
|---|---|---|
| **VLAN interface** | VLAN1 | VLAN interface for current switch configurable. |
| **NTP interface configuration** | Disable | Close operation. |
| | Enable | Start-up operation. |
| **NTP interface client** | none | Interface NTP client type. |
| | broadcast | |
| | no broadcast | |
| | multicast | |
| | no multicast | |
| | ipv6 multicast | |
| | no ipv6 multicast | |

## 16.3 NTP configuration display

### 16.3.1 NTP status display

NTP status display module, where users can view NTP service current status information.


Figure 253.

# 17. QOS port configuration

## 17.1 QOS port configuration

### 17.1.1 QOS port trust state configuration

Configure port trust rules.

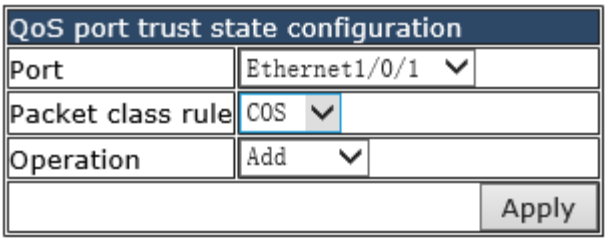



Figure 254.

| | | |
|---|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. | |
| **Packet class rule** | COS | Cos to int mapping based on intp field. |
| | DSCP | Intp field based on dscp to intp mapping. |
| **Operation** | Add | Add a trust rule for the port. |
| | Remove | Remove a trust rule for the port. |

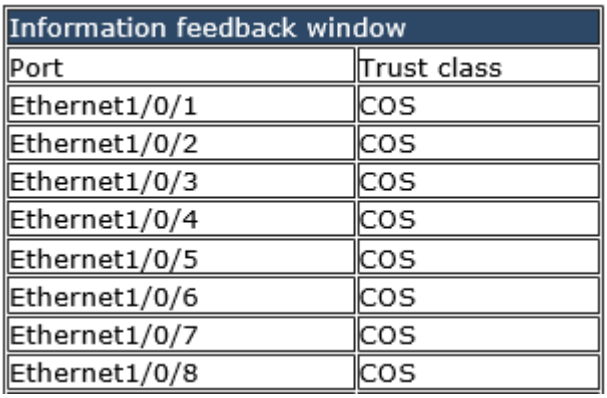



Figure 255.

### 17.1.2 QOS port COS parameters configuration

Configure the COS value of the port, regardless of whether the trust rule of the current port is trusted.

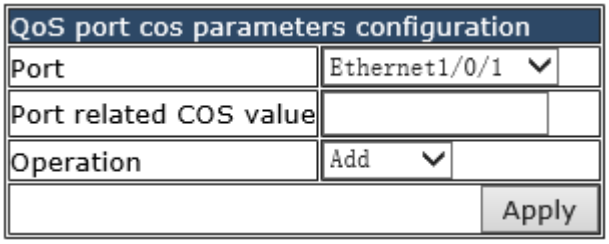



Figure 256.

| | |
|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. |
| **Port related** | The default COS value of the port, range: 0-7. |

| | | |
|---|---|---|
| **COS value** | | |
| **Operation** | Add | Add the COS value of the port. |
| | Remove | Delete the COS value of the port and restore it to 0. |

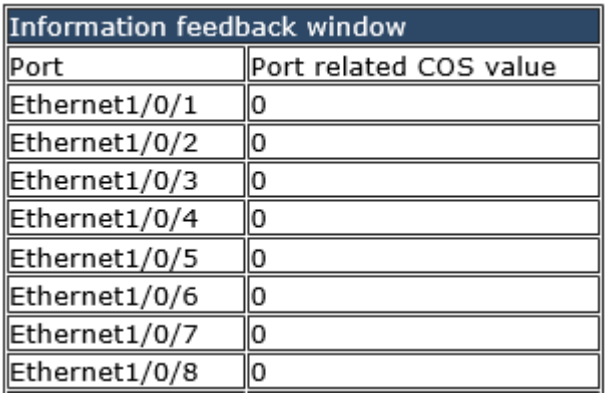



Figure 257.

### 17.1.3 QOS port select queue schedule algorithm configuration

Configure the port to process the priority of packets according to different queue scheduling algorithms.

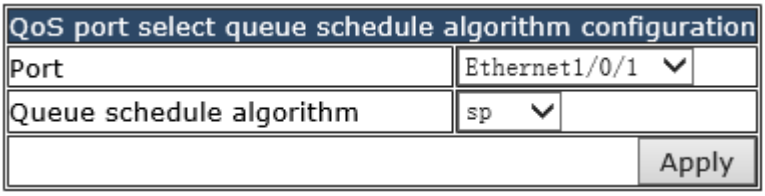



Figure 258.

| | | |
|---|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. | |
| **Queue schedule algorithm** | sp | Strict queuing priority, packet transmission in order of priority. |
| | wrr | Weighted round-robin scheduling. Rotate scheduling between queues to ensure that each queue gets a certain amount of service time. |
| | wdrr | Weighted difference round-robin scheduling, based on message length transmission, based on the combined effect of weight and K value to generate the length of transmission in the message queue. |

| Information feedback window | |
|---|---|
| Port | Trust class |
| Ethernet1/0/1 | sp |
| Ethernet1/0/2 | wdrr |
| Ethernet1/0/3 | wrr |
| Ethernet1/0/4 | wrr |
| Ethernet1/0/5 | wrr |
| Ethernet1/0/6 | wrr |
| Ethernet1/0/7 | wrr |
| Ethernet1/0/8 | wrr |

Figure 259. Display the queue scheduling algorithm trusted by the current port.

### 17.1.4 QOS port wrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, and allocate the number of packets according to the weight value.

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

Figure 260.

| | |
|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. |
| **Weight1** | The weight value of queue 1, the range is 0-127. |
| **Weight2** | The weight value of queue 2, the range is 0-127. |
| **Weight3** | The weight value of queue 3, the range is 0-127. |
| **Weight4** | The weight value of queue 4, the range is 0-127. |
| **Weight5** | The weight value of queue 5, the range is 0-127. |
| **Weight6** | The weight value of queue 6, the range is 0-127. |
| **Weight7** | The weight value of queue 7, the range is 0-127. |
| **Weight8** | The weight value of queue 8, the range is 0-127. |

| | | |
|---|---|---|
| | | |
| **Operation** | Add | Add the weight of each queue to the port, and fill in all the weights of each queue before adding. |
| | Remove | To restore the weight of each queue of the port to the default, you need to add the value of eight queues. |

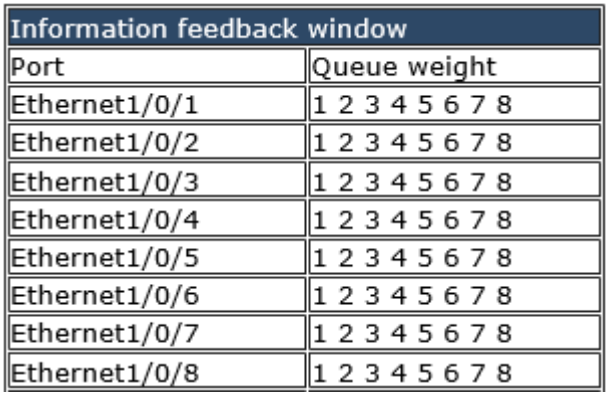



Figure 261. Information feedback window.

### 17.1.5 QOS port wdrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, transmit based on the length of the message, and generate the transmission length in the message queue based on the combined action of the weight and the K value.

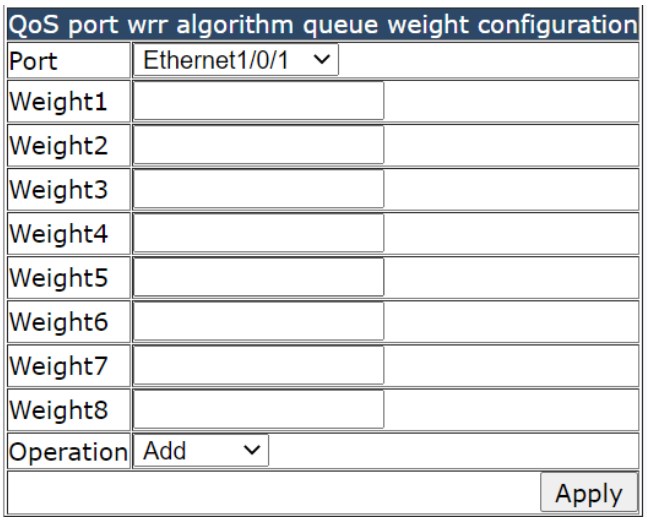



Figure 262.

| | |
|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. |
| **Weight1** | The weight value of queue 1, the range is 0-32767. |
| **Weight2** | The weight value of queue 2, the range is 0-32767. |

| | | |
|---|---|---|
| **Weight3** | The weight value of queue 3, the range is 0-32767. | |
| **Weight4** | The weight value of queue 4, the range is 0-32767. | |
| **Weight5** | The weight value of queue 5, the range is 0-32767. | |
| **Weight6** | The weight value of queue 6, the range is 0-32767. | |
| **Weight7** | The weight value of queue 7, the range is 0-32767. | |
| **Weight8** | The weight value of queue 8, the range is 0-32767. | |
| **Operation** | Add | Add the weight of each queue to the port, and fill in all the weights of each queue before adding. |
| | Remove | To restore the weight of each queue of the port to the default, you need to add the value of eight queues. |

### 17.1.6 QOS service policy configuration

Configure the port's policy table, and the port will process packets according to the rules of the classification table in the policy table.

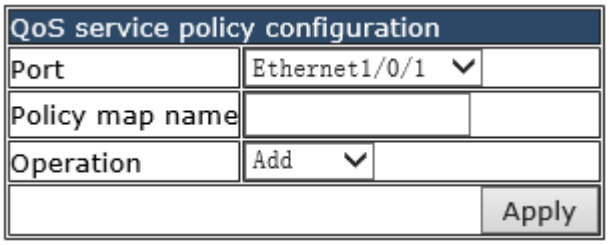



Figure 263.

| | | |
|---|---|---|
| **Port** | To configure the port name, click to expand the remaining ports. | |
| **Policy map name** | The name of the policy table, added by the policy table configuration. | |
| **Operation** | Add | Policy for adding ports. |
| | Remove | Delete port policy. |

## 17.2 QOS class-map configuration

### 17.2.1 Class map-configuration

Create and delete classification tables, view the currently configured classification tables.

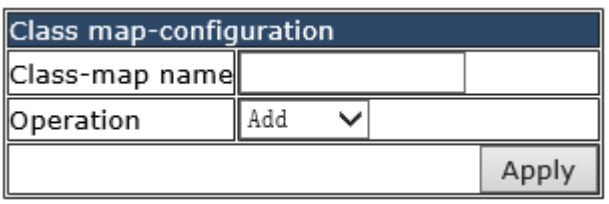


Figure 264.

| | | |
|---|---|---|
| **Class-map name** | Class-map name, range: 1-64 character. | |
| **Operation** | Add | Add Class-map. |
| | Remove | Remove Class-map. |

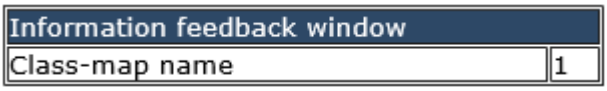



Figure 265. Display the currently created class-map name.

### 17.2.2 classification criteria configuration

Set the rules and corresponding parameters for classification matching.

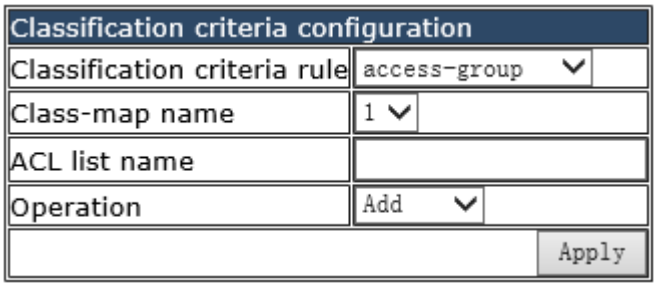



Figure 266.

| | | |
|---|---|---|
| **Classification criteria rule** | accesss-group | Match the specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **ACL list name** | Created ACL name, 1-64 characters. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

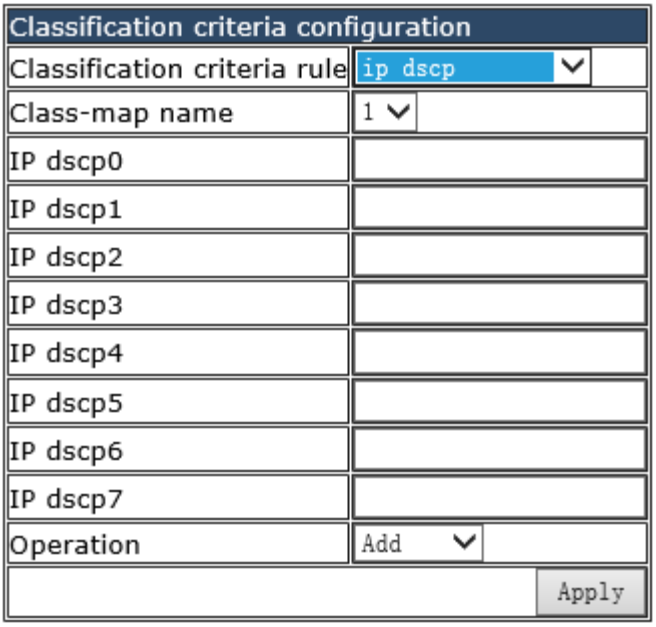



Figure 267.

| | | |
|---|---|---|
| **Classification criteria rule** | ip dscp | Match the specified DSCP value, this parameter is the DSCP list. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **IP dscp 0-7** | One or more DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

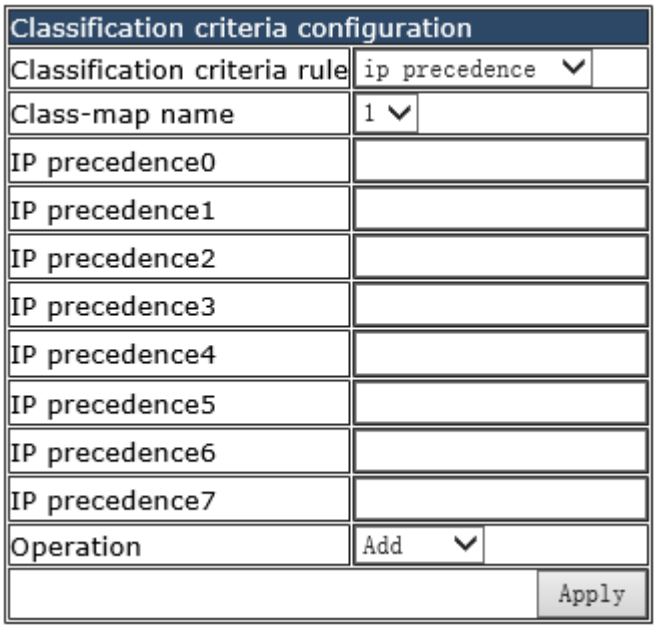


Figure 268.

| | | |
|---|---|---|
| **Classification criteria rule** | ip precedence | Match the specified ip priority, this parameter is the IP priority list. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **IP precedence 0-7** | One or more ip priority values can be set, the list contains up to 8 IP priority values, and the valid range is 0~7. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

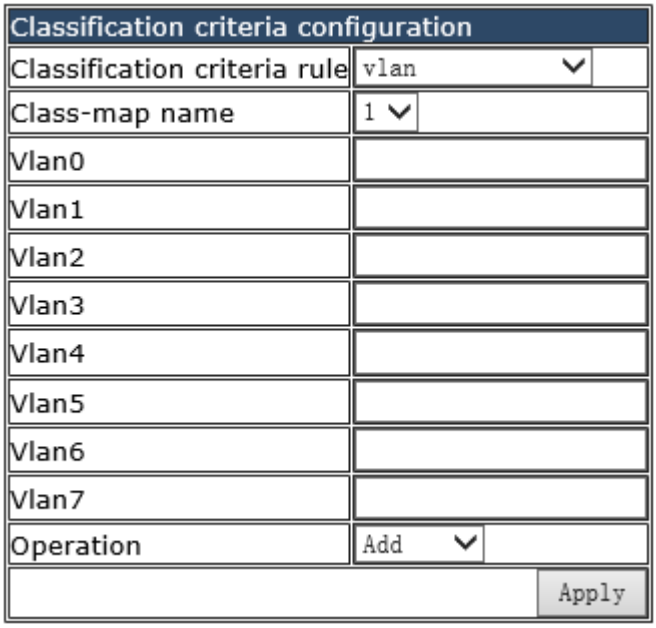



Figure 269.

| | | |
|---|---|---|
| **Classification criteria rule** | vlan | Match the specified vlan, this parameter is a list of vlan id. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **Vlan 0-7** | One or more VLAN IDs can be set, including 8 VLAN IDs at most, ranging from 1 to 4094. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

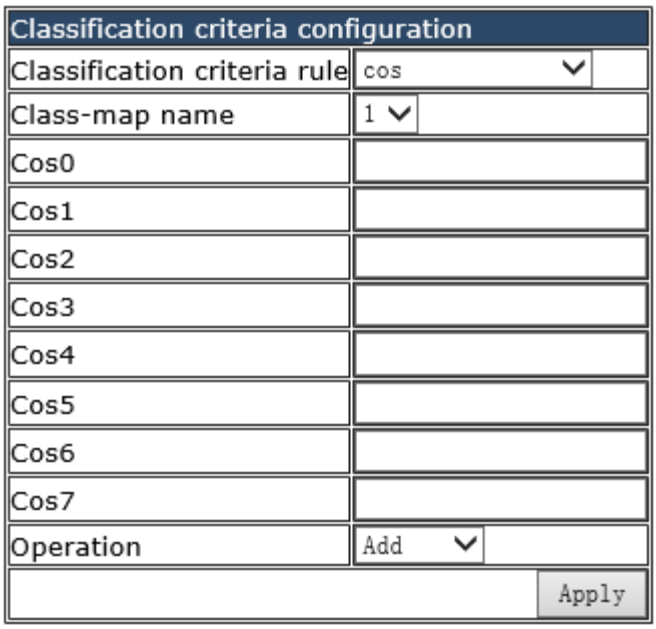



Figure 270.

| | | |
|---|---|---|
| **Classification criteria rule** | cos | Match the specified CoS value, this parameter is a list of vlan id. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **Cos 0-7** | One or more cos values can be set, the parameter is a CoS list composed of up to 8 CoS, the range is 0~7. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

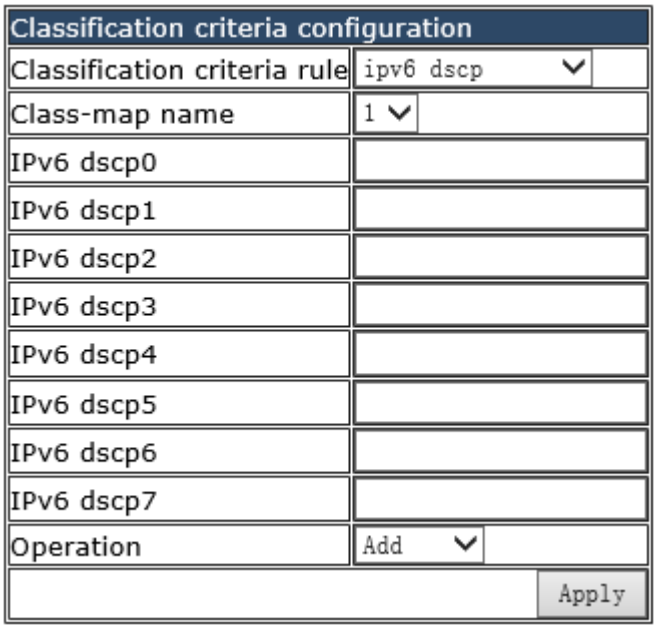


Figure 271.

| | | |
|---|---|---|
| **Classification criteria rule** | ipv6 dscp | Match the specified ipv6 DSCP value, this parameter is the ipv6 DSCP list. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **IPv6 dscp 0-7** | One or more ipv6 DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

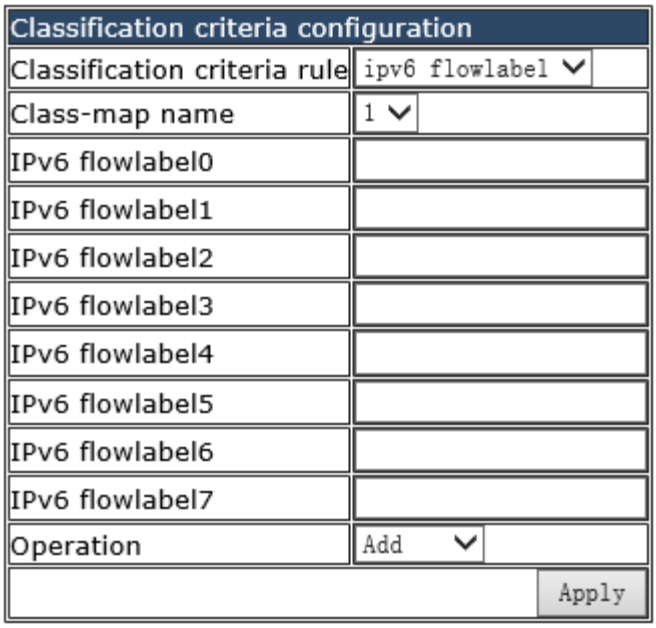



Figure 272.

| | | |
|---|---|---|
| **Classification criteria rule** | ipv6 flow label | Match the specified IPv6 flow label, this parameter is the value of the IPv6 flow label DSCP list. |
| **Class-map name** | The name of the created class-matching table, select by clicking the drop-down. | |
| **IPv6 flow label 0-7** | One or more IPv6 flow label values can be set, ranging from 0 to 1048575. | |
| **Operation** | Add | Add matching rules. |
| | Remove | Remove matching rules. |

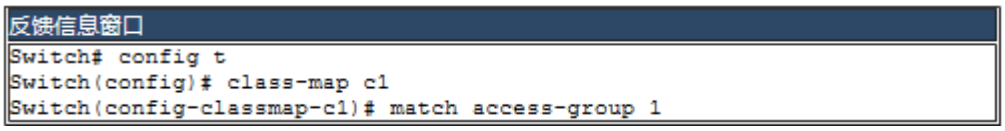



Figure 273. Display configuration application execution process and return result.

# 17.3 QoS policy configuration

## 17.3.1 QoS policy configuration

Configure the policy table burst-group, provide the policy class-map to use.

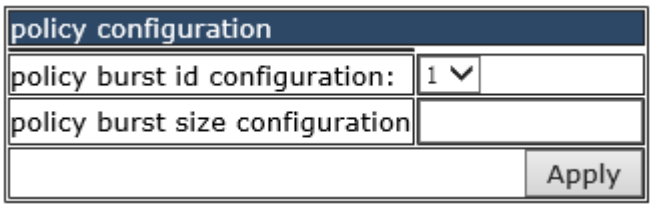



Figure 274.

| | |
|---|---|
| **Policy burst id configuration** | There are only two IDs, 1 and 2. |
| **Policy burst size configuration** | The default is 1024, the range that can be set: 1-8192. |

# 17.4 QOS policy-map configuration

## 17.4.1 policy-map configuration

Create and delete policy tables, and collaborate with classification tables to create packet in and out rules.

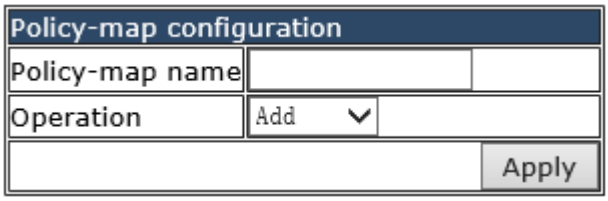



Figure 275.

| | | |
|---|---|---|
| **Policy-map name** | Policy-map name, range: 1-64 character. | |
| **Operation** | Add | Add policy-map. |
| | Remove | Remove policy-map. |


Figure 276. Display the currently created policy-map.

### 17.4.2 Class-map use to policy-map config

Apply the class-map to the policy-map.

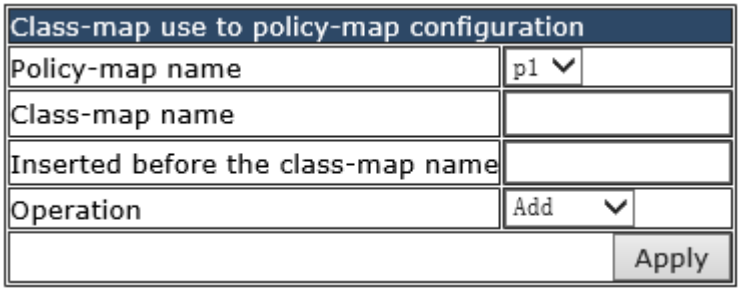



Figure 277.

| | | |
|---|---|---|
| **policy-map name** | The name of the created policy-map. | |
| **class-map name** | The name of the classification table created by the classification matching table, this table will be applied to the policy-map. | |
| **Inserted before the class-map name** | Prior to the insertion of the classification matching table, the name of the classification table that has been applied to the strategy table, and the priority of the newly applied classification matching table is increased. | |
| **Operation** | Add | Add an association between the strategy table and the classification table. |
| | Remove | Remove an association between the strategy table and the classification table. |

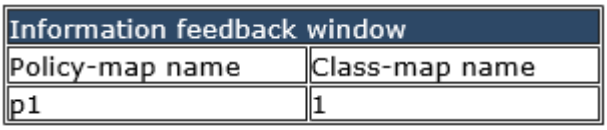



Figure 278. Display the association between the created policy table and the classification matching table.

## 17.5 QoS policy-class-map configuration

### 17.5.1 Policy-class-map accounting configuration

Configure the statistics switch of the strategy table and the classification matching table, and display the association between the strategy table and the classification matching table.

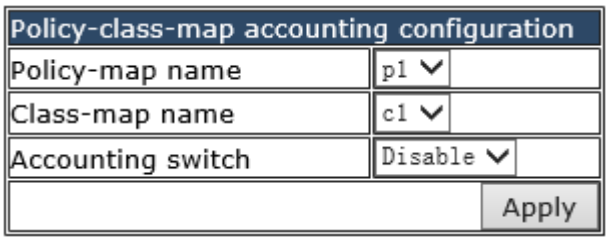



Figure 279.

| | | |
|---|---|---|
| **Policy-map name** | The name of the policy-map that has been created. | |
| **Class-map name** | The name of the classification matching table that has been created. | |
| **Accounting switch** | Disable | Disable the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association. |
| | Enabled | Start the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association. |

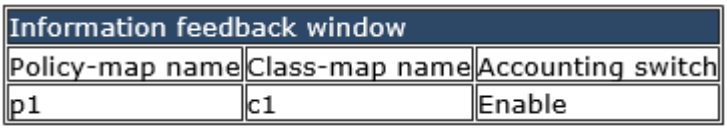



Figure 280. Display the traffic statistics switch information of the associated policy-map and class-map table.

## 17.5.2 Aggregate policy configuration

Configure the set strategy of the associated policy table and classification matching table. The policy mapping refers to the aggregation policy, and the aggregation policy is applied to the classified traffic. The same policy set can be referenced by different policy class mappings.

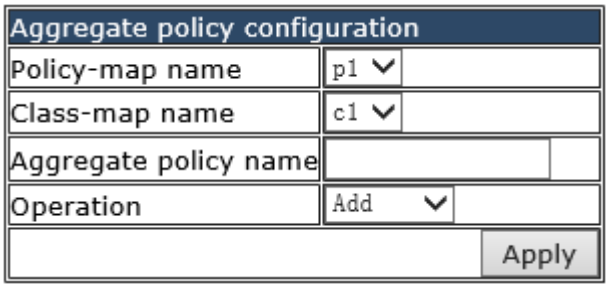



Figure 281.

| | |
|---|---|
| **Policy-map name** | Name of the created policy table. |

| | | |
|---|---|---|
| **Class-map name** | Classification match table created. | |
| **Aggregate policy name** | The name of the aggregation strategy, 1-64 characters in length. | |
| **Operation** | Add | Start the set strategy associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table. |
| | Remove | Close the set strategy associated with the strategy table and the classification matching table, and automatically establish the association between the strategy table and the classification matching table without association. |

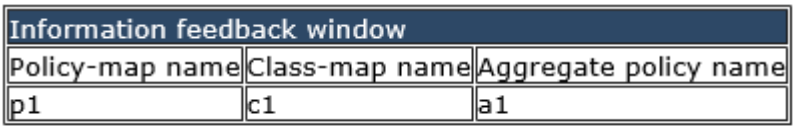



Figure 282. Display the set policy information of the associated policy table and the classification matching table.

### 17.5.3 Policy-class-map policy configuration

Configure the information rate in the policy mapping configuration mode.

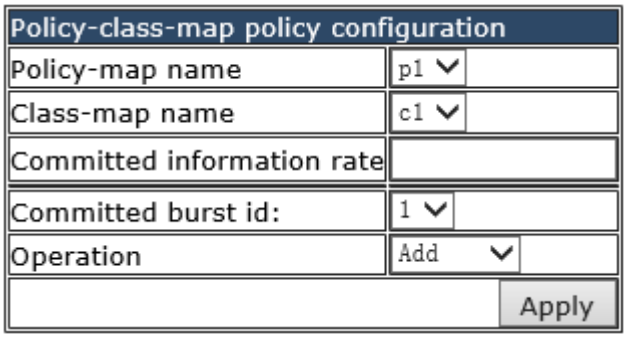



Figure 283.

| | |
|---|---|
| **Policy-map name** | Name of the created policy table. |
| **Class-map name** | Classification match table created. |
| **Committed information rate** | Committed Information Rate-CIR (Committed Information Rate), in Kbps, ranging from 1 to 10,000,000. |
| **Committed burst ID** | The burst ID range is 1 and 2, and the main commitment is the burst size. |

| | | |
|---|---|---|
| **Operation** | Add | Add the strategy information rate and burst size associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table. |
| | Remove | Delete the policy information rate and burst size associated with the policy table and the classification matching table, and automatically establish the association if there is no associated policy table and the classification matching table. |

### 17.5.4 Policy-class-map set configuration

Configure the priority of packets in the policy mapping configuration mode. Assign a new DSCP and IP priority to the classified traffic. Only the classified traffic that meets the matching criteria will be assigned a new value.

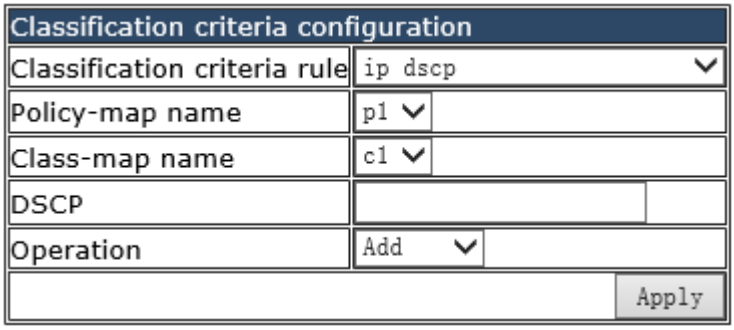



Figure 284.

| | | |
|---|---|---|
| **Classification criteria rule** | ip dscp | Set the DSCP value again according to the rules defined in the policy-map and class-map. |
| | ip precedence | Set the IP priority again according to the rules defined in the policy-map and class-map. |
| | drop-precedence | Set the discarding priority again according to the rules defined in the policy-map and class-map. |
| | internal-priority | Set the internal priority again according to the rules defined by the policy-map and class-map. |
| | cos | Set the COS value again according to the rules defined by the policy table and the classification matching table. |
| | ipv6 default next hop vrf | Set the default next hop address again according to the rules defined in the policy table and classification matching table. |
| **Policy-map name** | The name of the created policy table. | |
| **Class-map name** | Created classification match table. | |
| **DSCP** | DSCP value, range: 0-63. | |

| | | |
|---|---|---|
| **Precedence** | IP priority, range: 0-7. | |
| **Drop-precedence** | Drop priority, range: 0-2. | |
| **Internal-priority** | Internal priority, range: 0-7. | |
| **COS** | COS value, range: 0-7. | |
| **Vrf** | Vrf value, range: 0-252. | |
| **IPv6 Address (X:X::X:X)** | IPv6 default next hop address. | |
| **Operation** | Add | Add the priority and queue value associated with the strategy table and the classification matching table. |
| | Remove | Remove the priority and queue value associated with the strategy table and the classification matching table. |

# 17.6 QoS mapping configuration

## 17.6.1 COS-to-IntP mapping

Configure the value mapped from the COS value to the internal priority (queue).

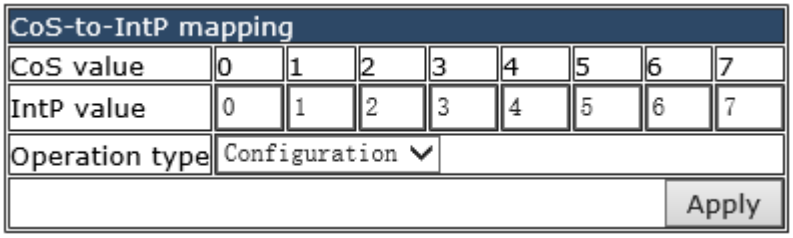



Figure 285.

| | | |
|---|---|---|
| **CoS value** | The COS value carried in the message or the default COS value assigned when entering. | |
| **IntP value** | The value of the internal priority (queue) to which the COS value will be mapped. | |
| **Operation type** | Configuration | Configure the value of COS to IntP. |
| | Default | Restore the mapping relationship to the default state. |

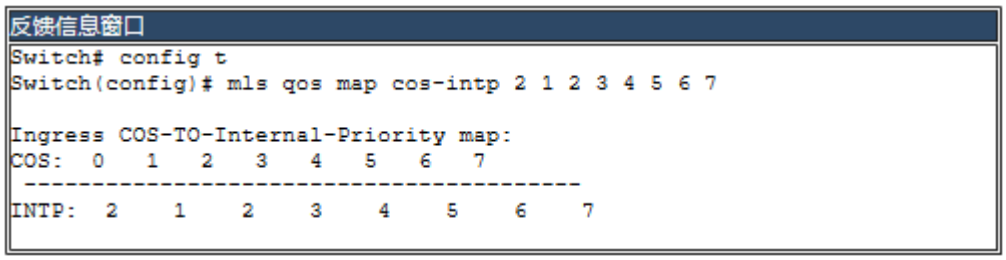


Figure 286. Display the execution process and the current mapping relationship.

### 17.6.2 COS-to-DP mapping

Configure the value mapped from the COS value to the drop priority (queue).

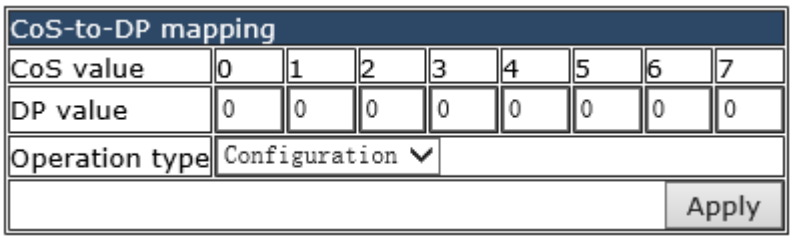



Figure 287.

| | | |
|---|---|---|
| **CoS value** | The COS value carried in the message or the default COS value assigned when entering. | |
| **IntP value** | The value of the drop priority (queue) to which the COS value will be mapped. | |
| **Operation type** | Configuration | Configure COS to drop priority value. |
| | Default | Restore the mapping relationship to the default state. |

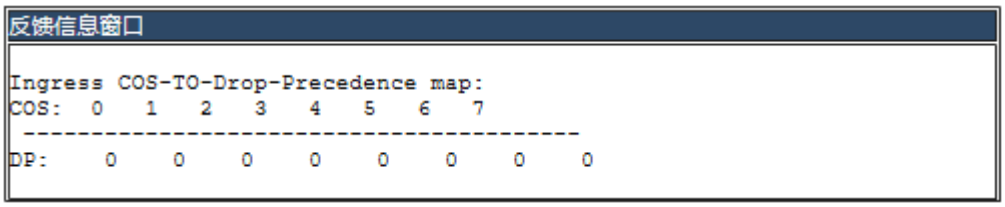



Figure 288. Display the execution process and the current mapping relationship.

### 17.6.3 DSCP-to-DSCP mapping

Configure the mapping from DSCP value to DSCP value.

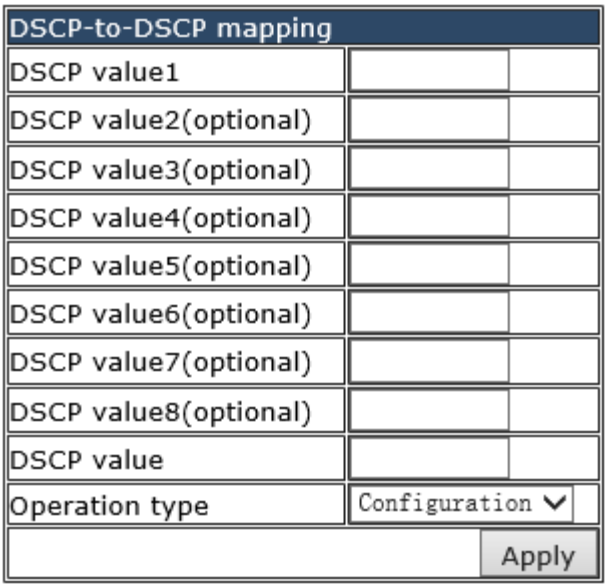


Figure 289.

| | | |
|---|---|---|
| **DSCP value1-DSCP value8 (optional)** | Up to eight DSCP values can be configured to the new DSCP value, among which DSCP value1 is required, DSCP value2-8 is optional, range: 0-63. | |
| **DSCP value** | New DSCP value, range: 0-63. | |
| **Operation type** | Configuration | Configure DSCP to DSCP value. |
| | Default | Restore the mapping relationship to the default state. |

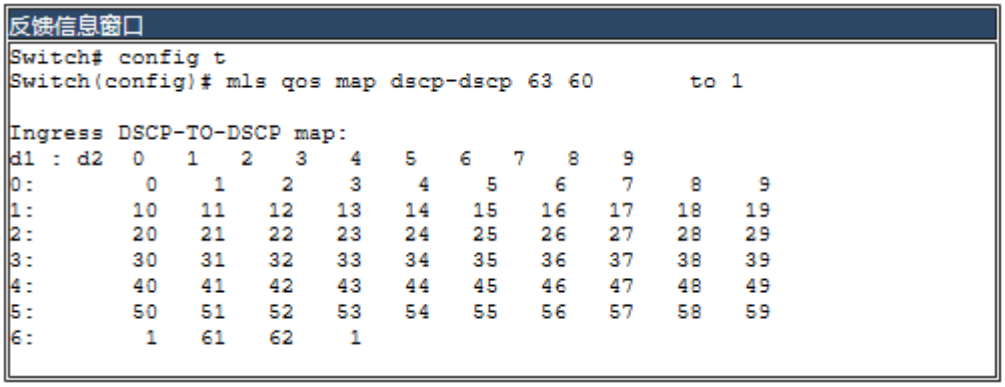



Figure 290. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.4 DSCP-to-IntP mapping

Configure the value mapped from the DSCP value to the IntP value.

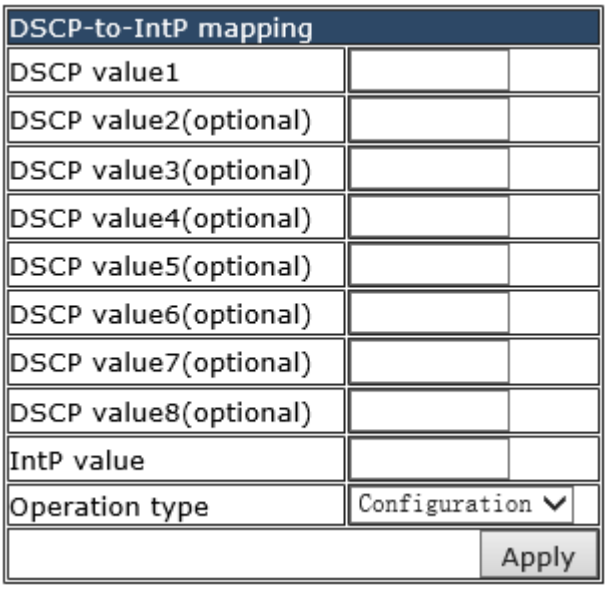



Figure 291.

| | |
|---|---|
| **DSCP value1-** | Up to eight DSCP values can be configured to the new IntP value, among which |

| | | |
|---|---|---|
| **DSCP value8 (optional)** | DSCP value1 is required, DSCP value2-8 is optional, range: 0-63. | |
| **IntP value** | New IntP value, range: 0-7. | |
| **Operation type** | Configuration | Configure DSCP to IntP value. |
| | Default | Restore the mapping relationship to the default state. |

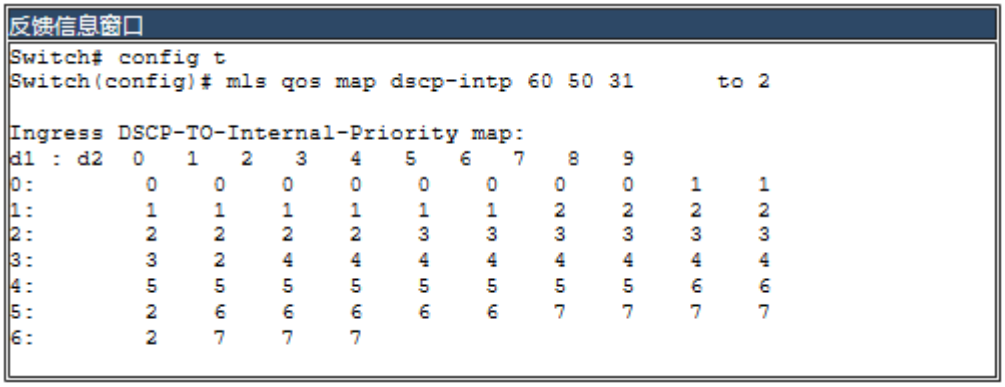



Figure 292. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.5 DSCP-to-DP mapping

Configure the value mapped from the DSCP value to the DP value.

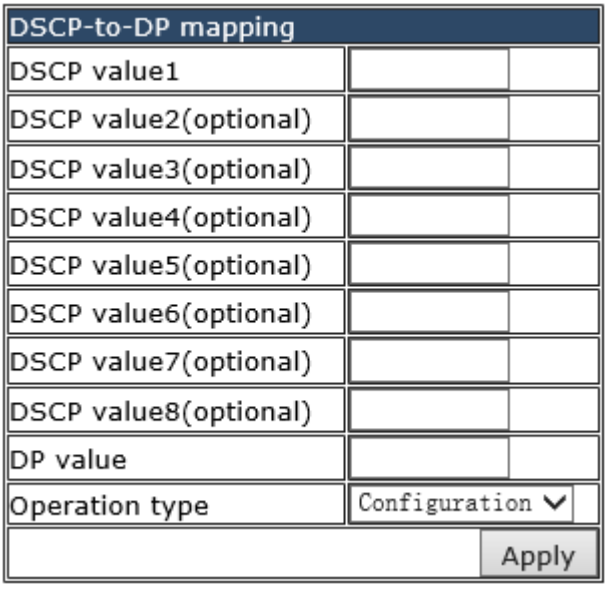



Figure 293.

| | |
|---|---|
| **DSCP value1-DSCP value8 (optional)** | Up to eight DSCP values can be configured to the new DP value, among which DSCP value1 is required, DSCP value2-8 is optional, range: 0-63. |

| | | |
|---|---|---|
| **DP value** | New DP value, range: 0-2. | |
| **Operation type** | Configuration | Configure DSCP to DP value. |
| | Default | Restore the mapping relationship to the default state. |

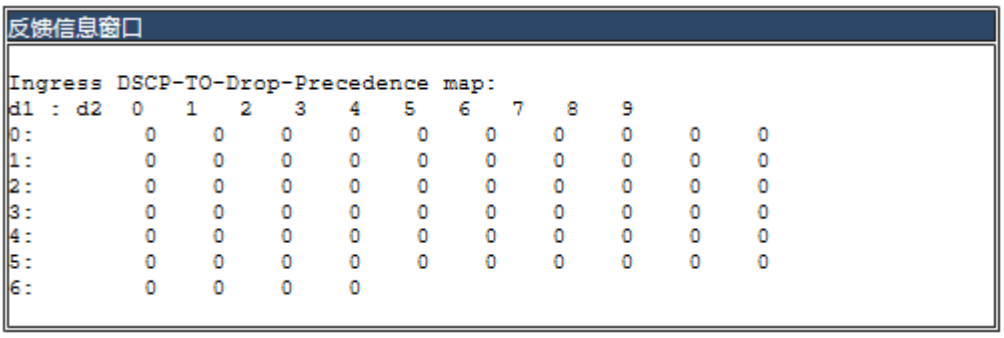



Figure 294. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.6 EXP-to-IntP mapping

Configure the value mapped from EXP value to IntP.

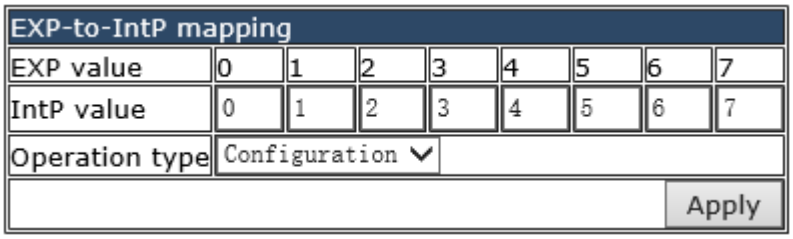



Figure 295.

| | | |
|---|---|---|
| **EXP value** | EXP value carried in the message, range: 0-7. | |
| **IntP value** | New IntP value, range: 0-7. | |
| **Operation type** | Configuration | Configure DSCP to IntP value. |
| | Default | Restore the mapping relationship to the default state. |

### 17.6.7 EXP-to-DP mapping

Configure the value mapped from EXP value to DP.

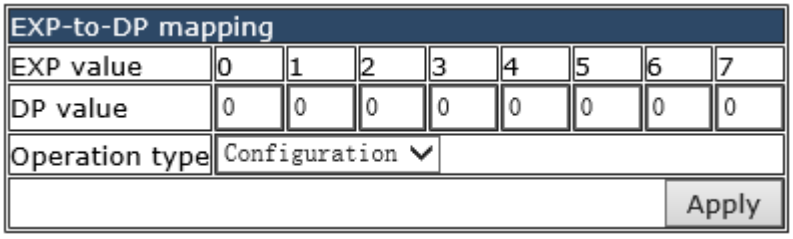


Figure 296.

| | | |
|---|---|---|
| **EXP value** | EXP value carried in the message, range: 0-7. | |
| **DP value** | New DP value, range: 0-2. | |
| **Operation type** | Configuration | Configure EXP to DP value. |
| | Default | Restore the mapping relationship to the default state. |

### 17.6.8 IntP-to-DSCP mapping

Configure the value mapped from IntP value to DSCP.

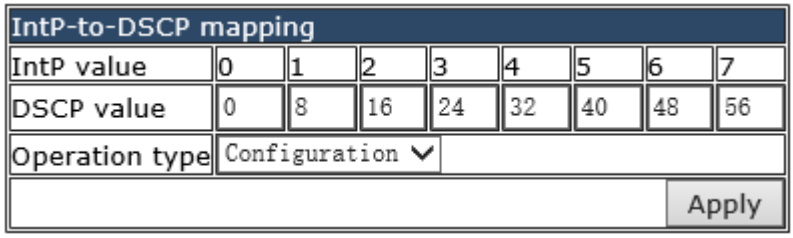



Figure 297.

| | | |
|---|---|---|
| **IntP value** | The value of the internal priority of the message, range: 0-7. | |
| **DSCP value** | New DSCP value, range: 0-63. | |
| **Operation type** | Configuration | Configure IntP to DSCP value. |
| | Default | Restore the mapping relationship to the default state. |

### 17.6.9 IntP-to-EXP mapping

Configure the value mapped from IntP value to EXP.

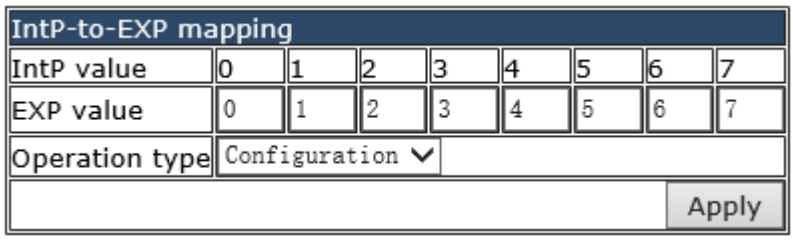



Figure 298.

| | | |
|---|---|---|
| **IntP value** | The value of the internal priority of the message, range: 0-7. | |
| **EXP value** | New EXP value, range: 0-7. | |
| **Operation type** | Configuration | Configure IntP to EXP value. |
| | Default | Restore the mapping relationship to the default state. |

## 17.7 QoS aggregate policy configuration

Configure the new aggregation strategy and the information rate and burst id of the aggregation strategy.

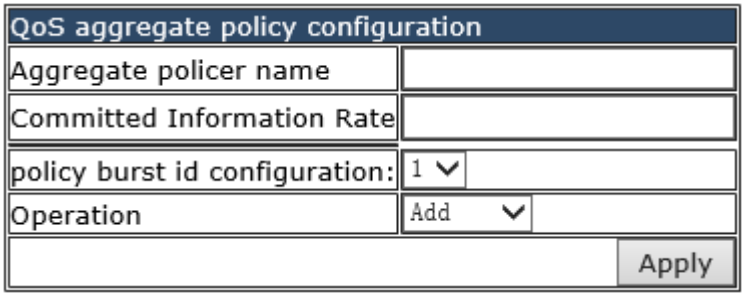



Figure 299.

| | | |
|---|---|---|
| **Aggregate policer name** | New aggregate policer name, range: 1-64 character. | |
| **Committed Information Rate** | Information Rate, range: 1-10000000 kbit/s. | |
| **Policy burst id configuration** | Burst id configuration, range: 1-2. | |
| **Operation** | Add | Add aggregate policer. |
| | Remove | Remove aggregate policer. |

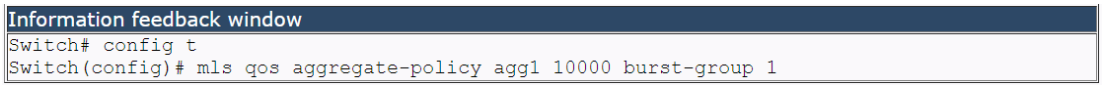



Figure 300. Display the configuration process and results, no error will be reported after normal configuration.

## 17.8 QoS service policy configuration

Configure VLAN Association Policy.

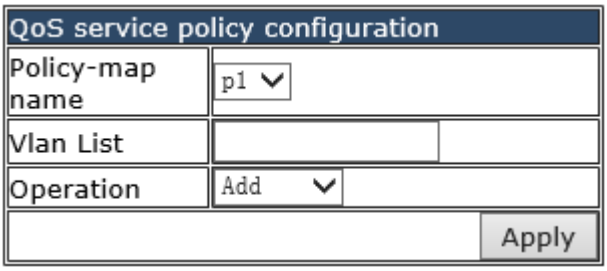



Figure 301.

| | | |
|---|---|---|
| **Policy-map name** | The name of the created strategy, select by clicking the drop-down. | |
| **VLAN List** | VLAN ID, range: 1-4094. | |
| **Operation** | Add | Add VLAN-based policy. |
| | Remove | Remove VLAN-based policy. |

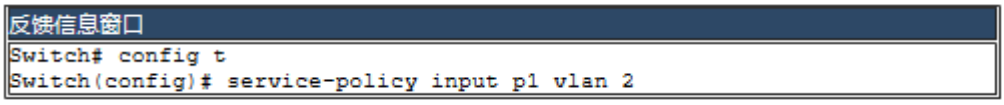



Figure 302. Display the configuration process and results, no error will be reported after normal configuration.

# 18. L3 forward configuration

## 18.1 IP route Aggregation configuration

### 18.1.1 Route aggregate configuration

This page is used for enabled or disabled configuration of routing aggregation.

To display the “Route aggregate configuration” page, click L3 forward configuration -> IP route Aggregation configuration -> Route aggregate configuration, click “Apply” to configure.

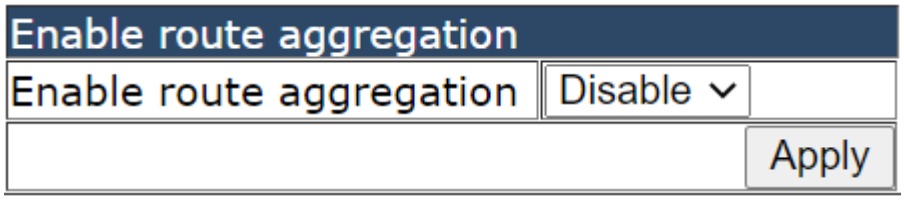



Figure 303.

| entry | describe |
|---|---|
| **Enable route aggregation** | Enable: Enable routing aggregation.<br>Disable: Disable routing aggregation. |


Figure 304.

| entry | describe |
|---|---|
| **Routing aggregation state** | Enable: Enable routing aggregation.<br>Disable: Disable routing aggregation. |

## 18.2 ARP configuration

### 18.2.1 ARP configuration

This page is used to configure ARP static entries.

To display the “ARP configuration” page, click L3 forward configuration -> ARP configuration -> ARP configuration, click “Apply” to configure.

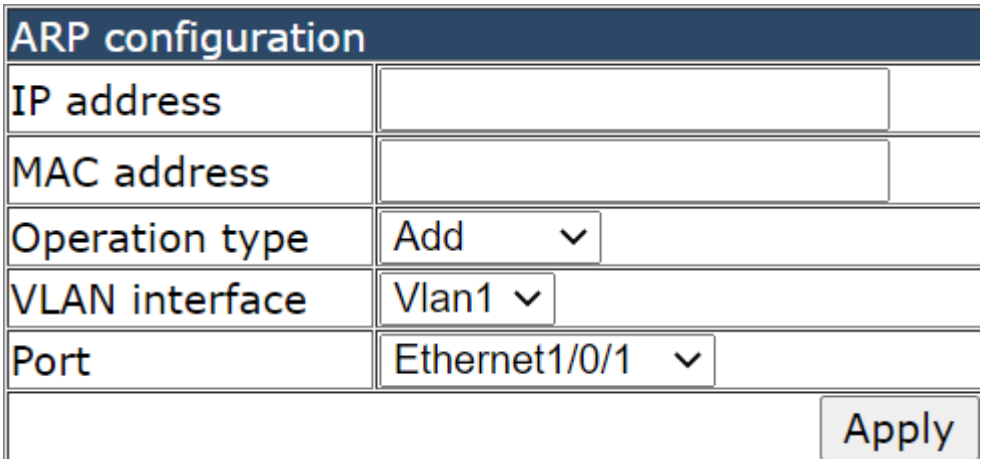



Figure 305.

| | |
|---|---|
| **entry** | describe |
| **IP address** | IP address, e.g .1.1.1.1. |
| **MAC address** | MAC address. |
| **Operation type** | Add: Apply the above settings.<br>Remove: Delete the above. |
| **VLAN interface** | VLAN id created. |
| **Port** | Ethernet port name. |

### 18.2.2 Clear ARP cache

This page is used to clear ARP statistics.

To display the “Clear ARP cache” page, click L3 forward configuration -> ARP configuration -> Clear ARP cache, click “Apply” to configure.


Figure 306.

### 18.2.3 Show ARP

This page is used to view the information of the ARP table.

To display the “Clear ARP cache” page, click L3 forward configuration -> ARP configuration -> Clear ARP cache.

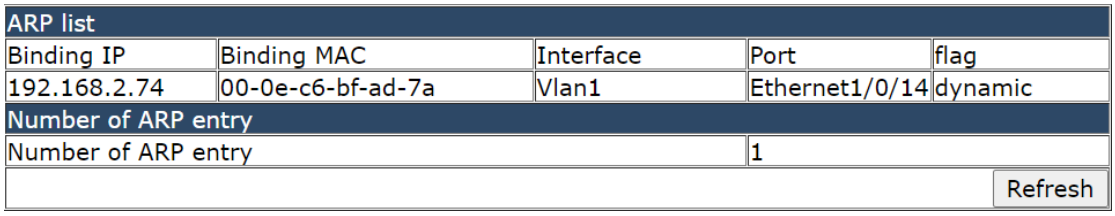



Figure 307.

## 18.3 Gratuitous arp config

### 18.3.1 gratuitous-arp interval time configuration

This page is used to configure the global free ARP send time interval.

To display the “gratuitous-arp interval time configuration” page, click L3 forward configuration -> Gratuitous arp config -> gratuitous-arp interval time configuration, click “Apply” to configure.

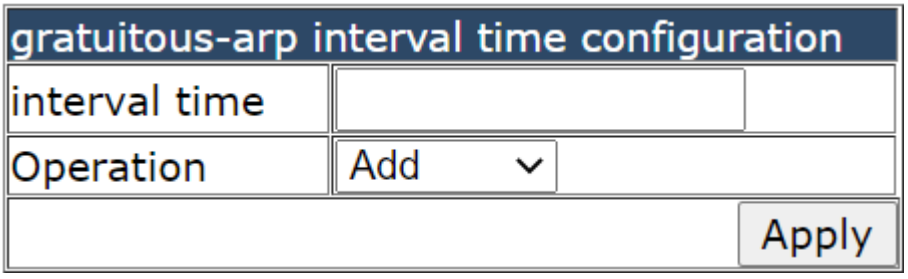



Figure 308.

| | |
|---|---|
| **entry** | describe |
| **interval time** | Range: 5-1200 seconds. |
| **Operation** | Add: Apply the above settings.<br>Remove: Recovery default interval 300 seconds. |

### 18.3.2 interface gratuitous-arp interval time configuration

This page is used to set vlan interface free ARP send interval configuration.

To display the “interface gratuitous-arp interval time configuration” page, click L3 forward configuration -> Gratuitous arp config -> interface gratuitous-arp interval time configuration, click “Apply” to configure.

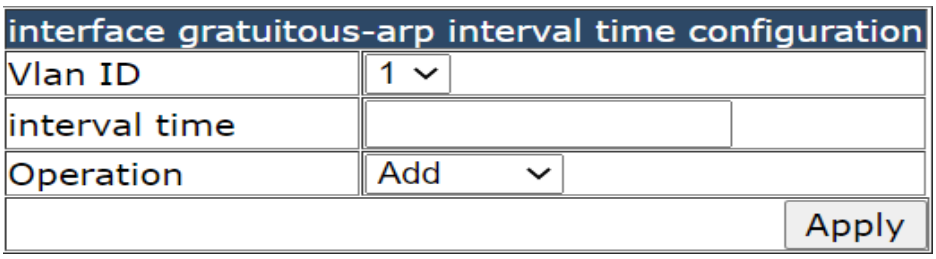



Figure 309.

| | |
|---|---|
| **entry** | describe |
| **VLAN ID** | Vlan ID created. |
| **interval time** | Range: 5-1200 seconds. |
| **Operation** | Add: Apply the above settings.<br>Remove: Recovery default interval 300 seconds. |

### 18.3.3 show gratuitous-arp configuration

This page is used to view ARP free configuration information.

To display the “show gratuitous-arp configuration” page, click L3 forward configuration -> Gratuitous arp config -> show gratuitous-arp configuration, click “Apply” to view.

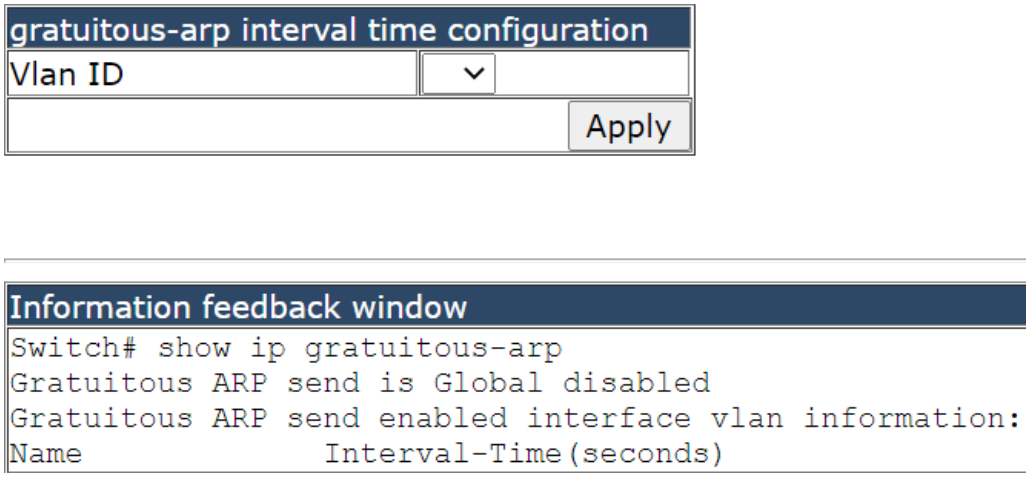



Figure 310.

## 18.4 ARP protection configuration

### 18.4.1 ARP GUARD configuration

#### 18.4.1.1 ARP GUARD configuration

This page is used for ARP GUARD configuration.

To display the “ARP GUARD configuration” page, click L3 forward configuration -> ARP protection configuration -> ARP GUARD configuration -> ARP GUARD configuration, click “Apply” to configure.

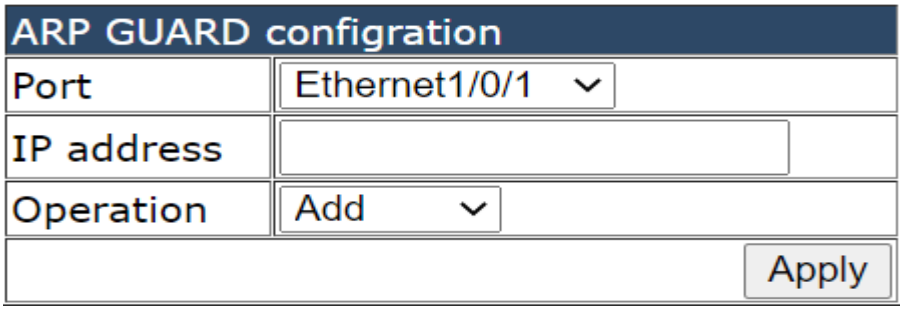



Figure 311.

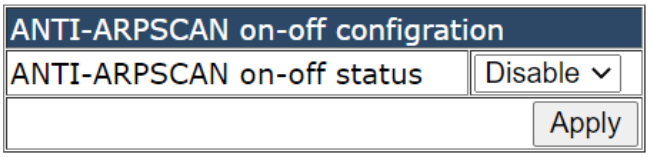
| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **IP address** | IP address, e.g .1.1.1.1. |
| **Operation** | Add: Apply the above settings.<br>Remove: Delete the above. |

## 18.4.2 ANTI-ARPSCAN configuration

### 18.4.2.1 ANTI-ARPSCAN on-off configuration

This page is used to configure the anti ARP scan function switch.

To display the “ARP GUARD configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN on-off configuration, click “Apply” to configure.



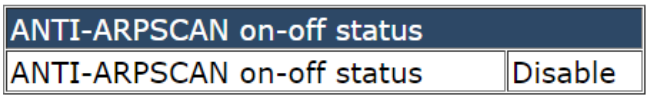




Figure 312.

| entry | describe |
|---|---|
| **ANTI-ARPSCAN on-off status** | Enable: Function Enable.<br>Disable: Function disabled. |

### 18.4.2.2 ANTI-ARPSCAN port-based threshold configuration

This page is available for port-based configuration of anti-scan ARP thresholds.

To display the “ANTI-ARPSCAN port-based threshold configuration” page, click L3 forward configuration ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN port-based threshold configuration, click “Apply” to configure.

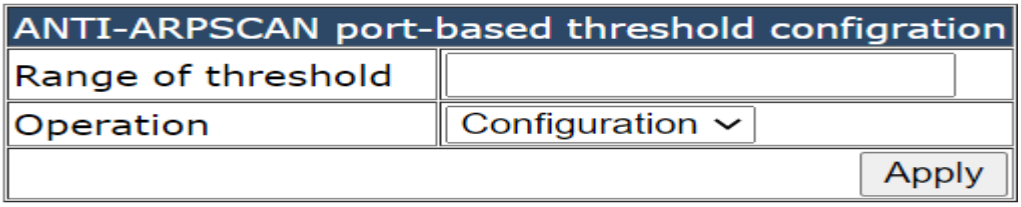



Figure 313.

| entry | describe |
|---|---|
| **Range of threshold** | Size range: 2-200, unit pack/s. |
| **Operation** | Configuration: Application settings.<br>Default: Restore default 10 packs/s. |

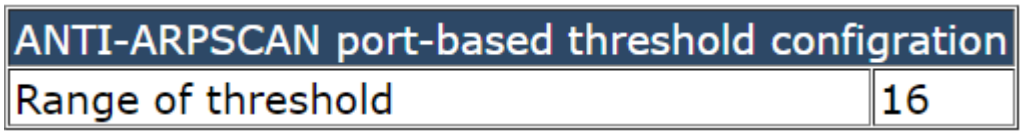



Figure 314.

| entry | describe |
|---|---|
| **Range of threshold** | Current configured threshold, size range:<br>2-200, unit pack/second. |

### 18.4.2.3 ANTI-ARPSCAN IP-based threshold configuration

This page is used to configure the IP-based anti ARP scan threshold.

To display the “ANTI-ARPSCAN IP-based threshold configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN IP-based threshold configuration, click “Apply” to configure.

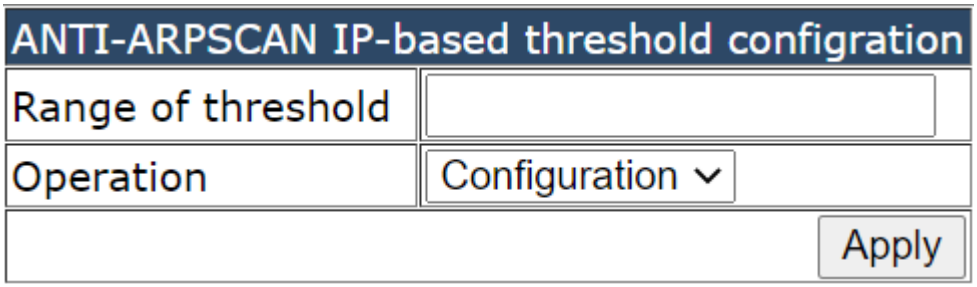



Figure 315.

| entry | describe |
|---|---|

| | |
|---|---|
| **Range of threshold** | Size range: 2-200, unit pack/s. |
| **Operation** | Configuration: Application settings.<br>Default: Restore default 6 packs/s. |

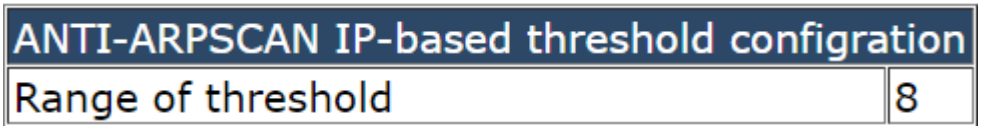



Figure 316.

| entry | describe |
|---|---|
| **Range of threshold** | Current configured threshold, size range:<br>2-200, unit pack/second. |

### 18.4.2.4 ANTI-ARPSCAN trust port configuration

This page is used to set the port to anti ARP scan trust port.

To display the “ANTI-ARPSCAN trust port configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN trust port configuration, click “Apply” to configure.

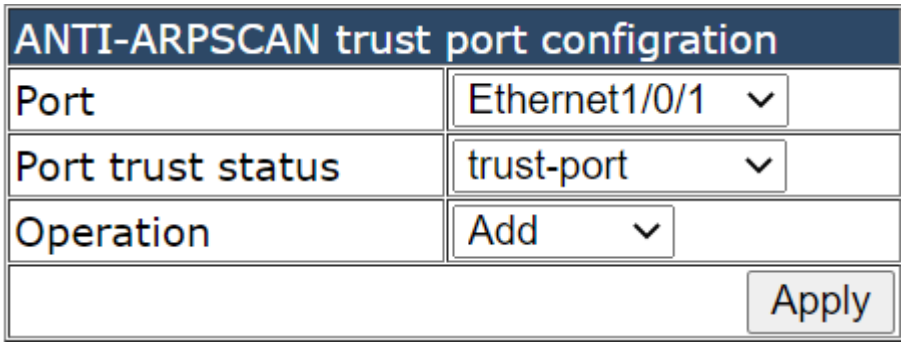



Figure 317.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **Port trust status** | trust-port: Trust port.<br>supertrust-port: Super trust port.<br>iptrust-port: IP trust port. |
| **Operation** | Add: Application settings.<br>Remove: Delete the corresponding settings. |

### 18.4.2.5 ANTI-ARPSCAN trust IP configuration

This page can be used to prevent ARP scanning trust IP configuration.

To display the “ANTI-ARPSCAN trust IP configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN trust ip configuration, click “Apply” to configure.

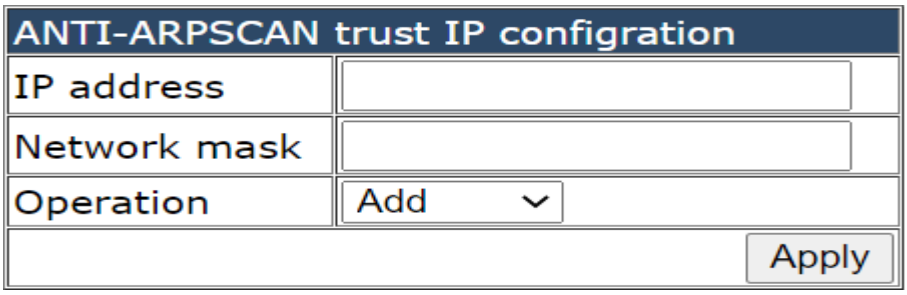



Figure 318.

| entry | describe |
|---|---|
| **IP address** | IP address, e.g .1.1.1.1. |
| **Network mask** | Corresponding IP address mask. |
| **Operation** | Add: Application settings.<br>Remove: Delete the corresponding settings. |

### 18.4.2.6 ANTI-ARPSCAN recovery on-off configuration

This page can be used to prevent ARP scanning automatic recovery switch configuration.

To display the “ANTI-ARPSCAN recovery on-off configuration” page, click L3 forward configuration ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN recovery on-off configuration, click “Apply” to configure.

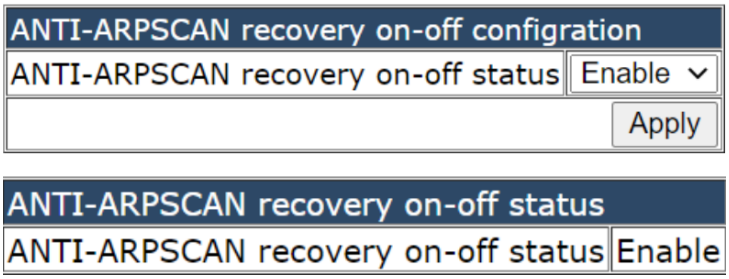



Figure 319.

| entry | describe |
|---|---|
| **ANTI-ARPSCAN recovery on-off status** | Enable: Enable automatic recovery function.<br>Disable: Disable automatic recovery function. |

### 18.4.2.7 ANTI-ARPSCAN recovery time configuration

This page can be used to configure the automatic recovery time against ARP scanning.

To display the “ANTI-ARPSCAN recovery time configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN recovery time configuration, click “Apply” to configure.

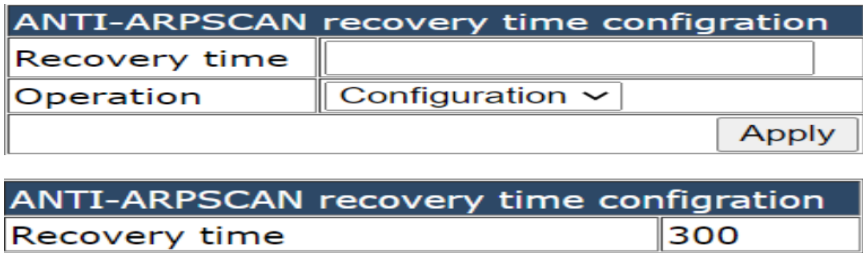



Figure 320.

| | |
|---|---|
| **entry** | describe |
| **Recovery time** | Size range: 5-86400 per second. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Recovery default auto recovery 300 seconds. |

#### 18.4.2.8 Show ANTI-ARPSCAN information

This page is used to view anti ARP scan run information.

To display the “Show ANTI-ARPSCAN information” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> Show ANTI-ARPSCAN information, click “Apply” to view.

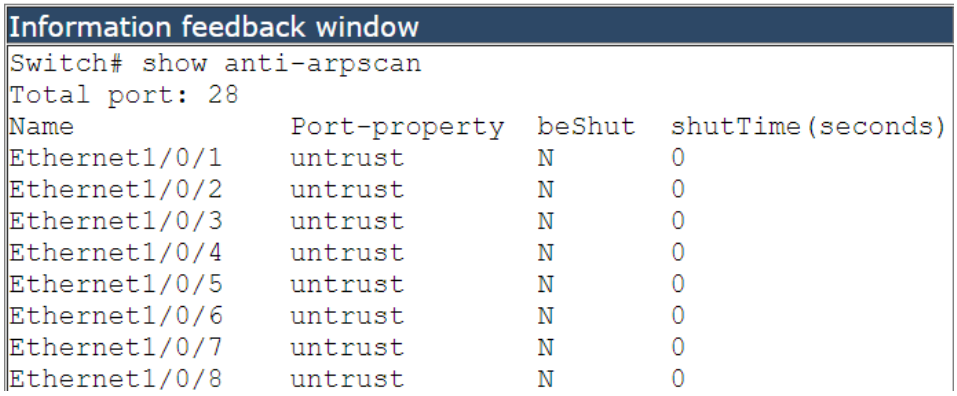



Figure 321.

## 18.5 Show IP Traffic

This page can be used to view statistics for IP packets.

To display the “Show IP Traffic” page, click L3 forward configuration -> ARP protection configuration -> Show IP Traffic, click “Apply” to view.

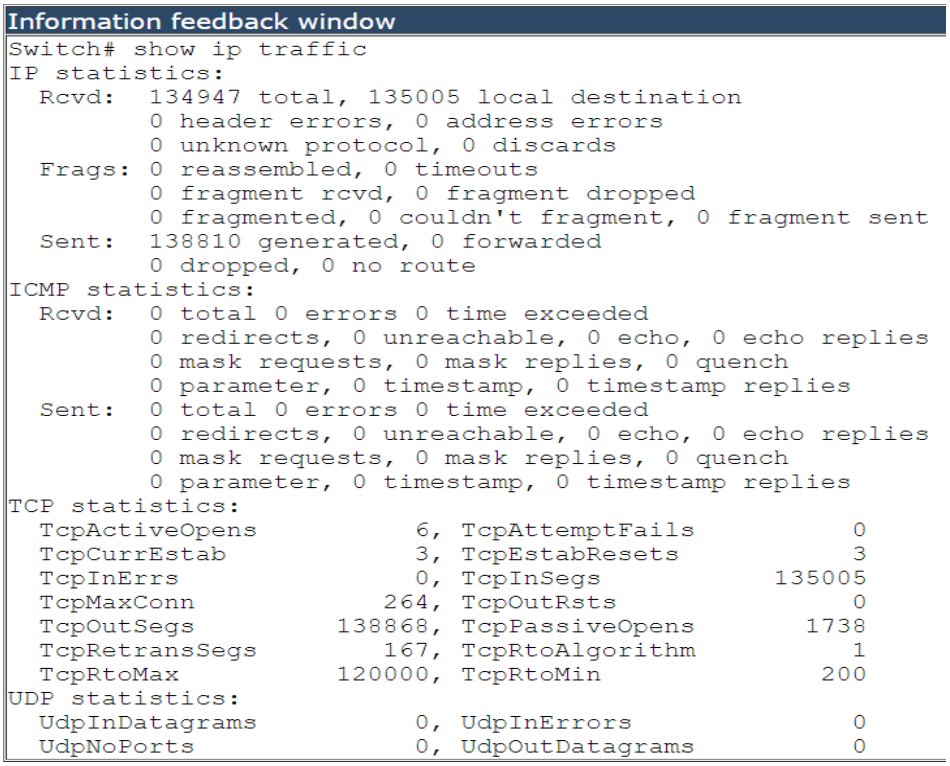



Figure 322.

# 19. Route configuration

## 19.1 Policy based routing

The directory function is to be developed.

## 19.2 Static route configuration

### 19.2.1 Static route configuration

This page can be used for the basic configuration of static routing.

To display the “Static route configuration” page, click Route configuration -> Static route configuration -> Static route configuration, click “Apply” to configure.

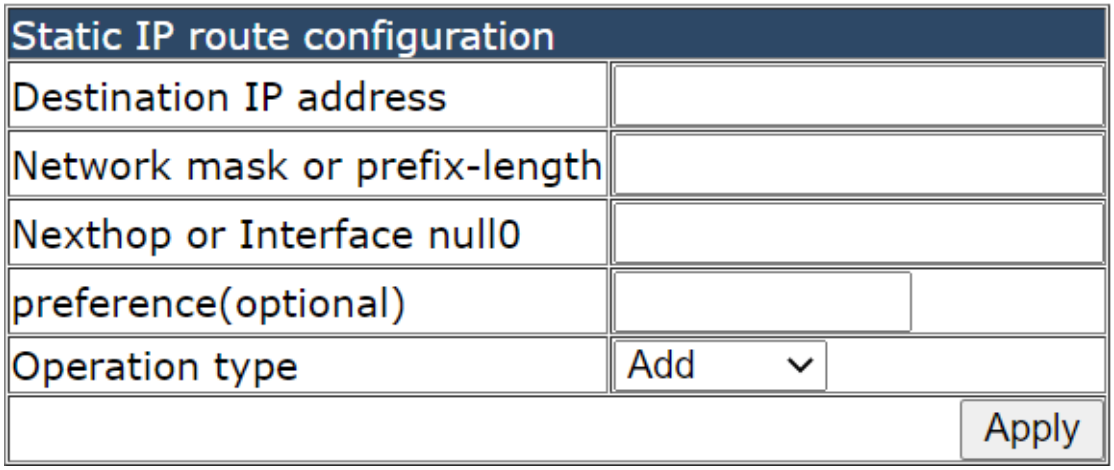



Figure 323.

| | |
|---|---|
| **entry** | describe |
| **Destination IP address** | IP address, format: 10.10.11.11. |
| **Network mask or prefix-length** | Subnet mask in the following format: 255.255.255.0; or mask length. |
| **Nexthop or Interface null0** | IP address, format: 10.10.11.11. or null0. |
| **Preference (optional)** | Range: 1-255. |
| **Operation type** | Add: Add the above settings.<br>Remove: Delete the above. |

# 20. IPv6 Route configuration

## 20.1 IPv6 configuration

### 20.1.1 IPv6 basic configuration

This page is used to vlan the ipv6 address of the interface and the configuration of ipv6 routing.

If you want to display the “IPv6 Basic Configuration” page, click IPv6 Route configuration -> IPv6 configuration -> IPv6 basic configuration, click “Apply” to configure.

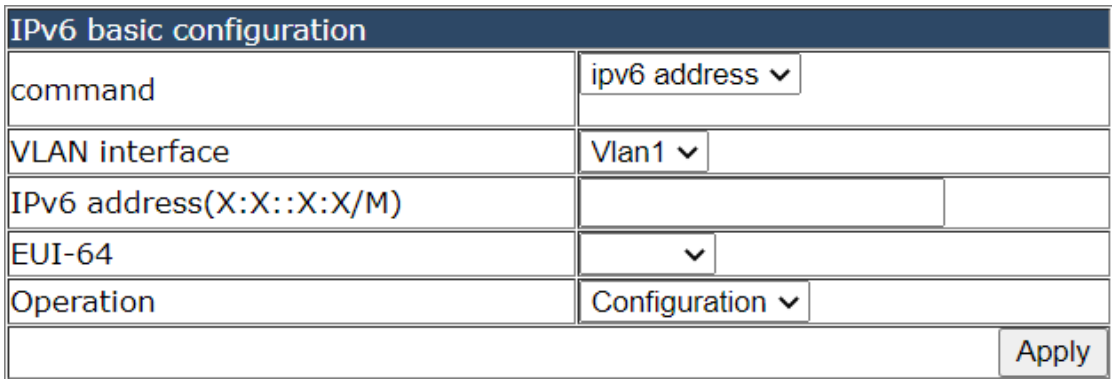



Figure 324.

| entry | describe |
|---|---|
| **IPv6 address** | Vlan interface ipv6 address configuration. |
| **VLAN interface** | Vlan created. |
| **IPv6 address** | Example: 2001:3f:ed8::99/64. |
| **EUI-64** | IPv6 address is automatically generated based on the eui64 interface identifier of the interface. |
| **Operation** | Configure: User self-configuration.<br>Default: Restore default configuration. |

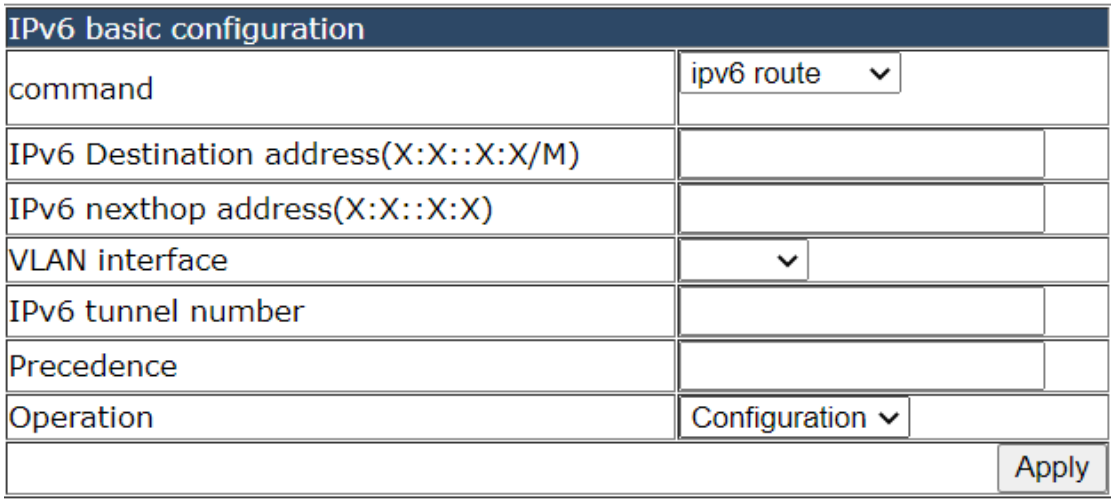



Figure 325.

Note: the switch does not support ipv6 routing configuration, the configuration of this page is not effective.

### 20.1.2 IPv6 ND configuration

This page is used for settings that can be used for neighbor discovery related functions.

If you display the “IPv6 ND Configuration” page, click IPv6 Route configuration -> IPv6 configuration -> IPv6 ND Configuration, click “Apply” to configure.

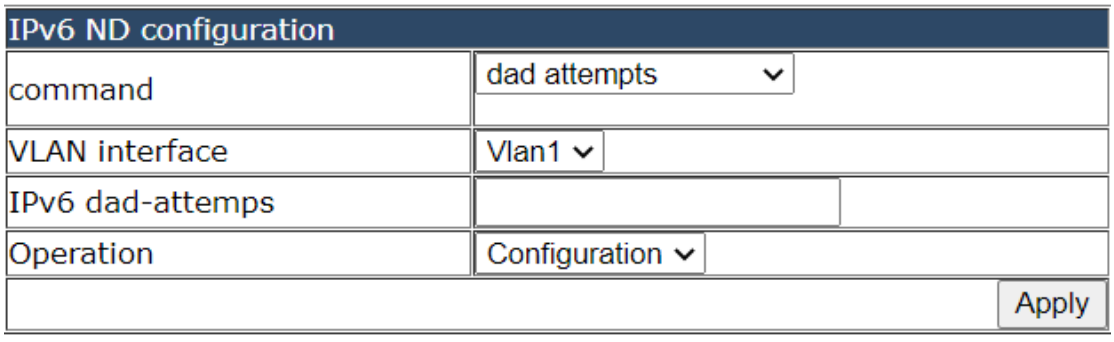



Figure 326.

| entry | describe |
|---|---|
| **Data attempts** | During duplicate address detection, the neighbor request message number continuously sent by the interface is set. |
| **VLAN interface** | Vlan created. |
| **IPv6 dad-attemps** | Range: 0-10. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Default request message number is 1. |

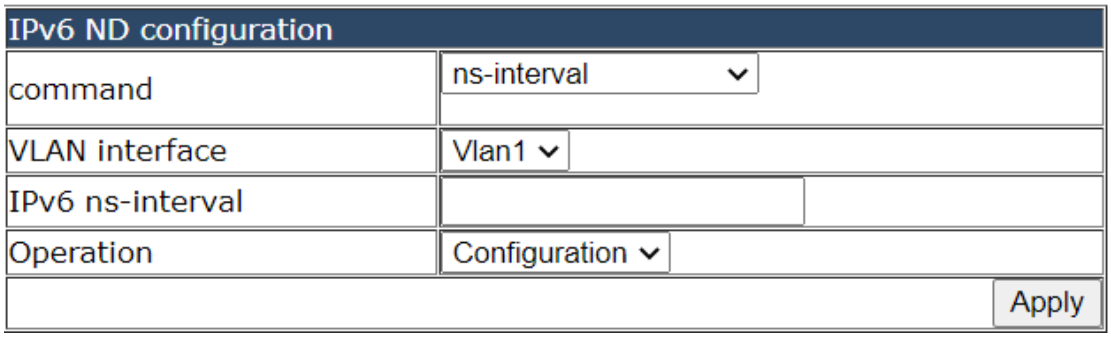



Figure 327.

| entry | describe |
|---|---|
| **ns-interval** | Time interval setting for neighbor request messages. |
| **VLAN interface** | Vlan created. |
| **IPv6 ns-interval** | Size range: 1-3600, per second. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Default request message number is 1 second. |

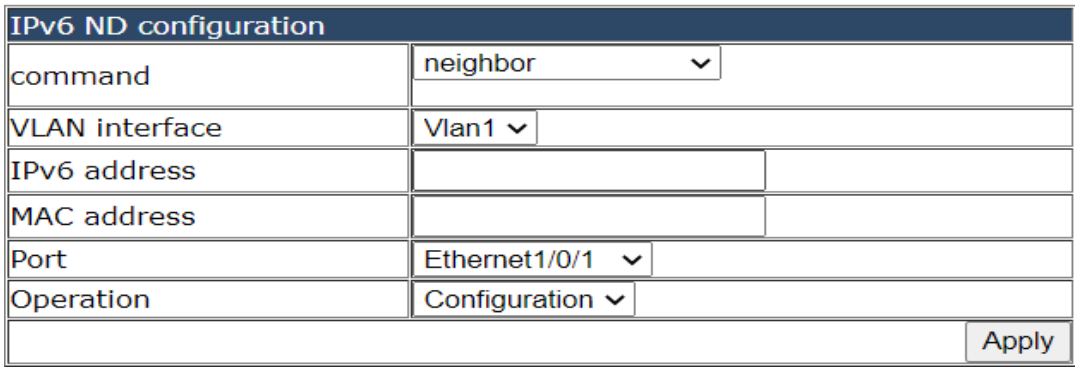



Figure 328.

| entry | describe |
|---|---|
| **Neighbor** | Set the Static Neighbor Table Item. |
| **VLAN interface** | Vlan created. |
| **IPv6 address** | Static Neighbor IPv6 Address. |
| **MAC address** | Static Neighbor MAC Address. |
| **Port** | Ethernet port name. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Delete the corresponding static neighbor table item. |

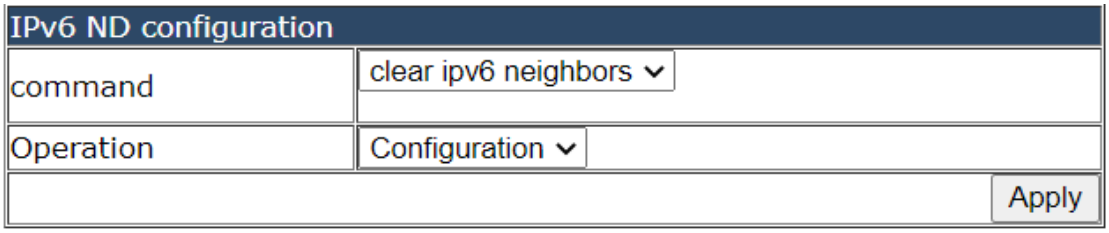



Figure 329.

| entry | describe |
|---|---|
| **Clear ipv6 neighbor** | Clear neighbor table items, but can not delete static neighbor table items. |
| **Operation** | Configuration: Delete neighbor table item.<br>Default: Delete Neighbor Table Item. |

### 20.1.3 Show IPv6 neighbor

This page is used to view ipv6 neighbor information.

To display the “Show IPv6 neighbor” page, click IPv6 Route configuration -> IPv6 configuration -> Show IPv6 neighbor, click “Apply” to view.

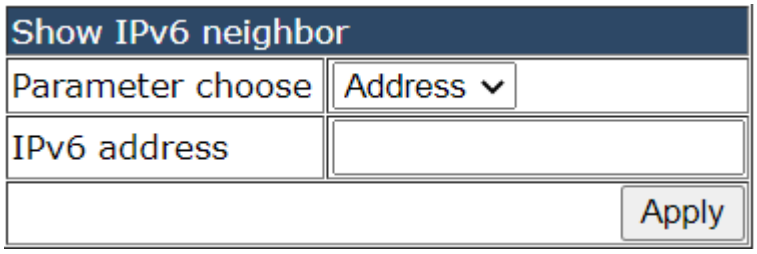



Figure 330.

| entry | describe |
|---|---|

| | |
|---|---|
| **Address** | Based on address. |
| **IPv6 address** | IPv6 address. |

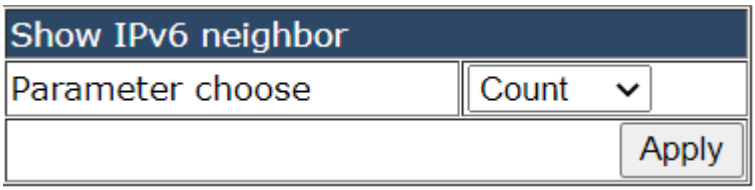



Figure 331.

| | |
|---|---|
| **entry** | describe |
| **Count** | Display counter information. |

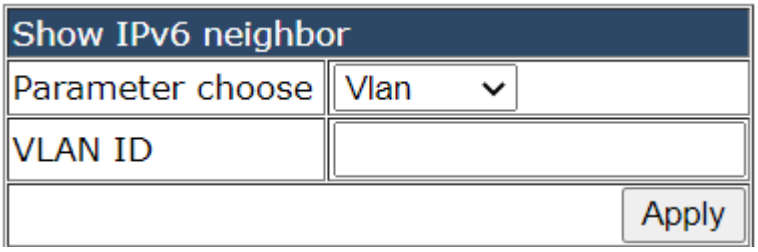



Figure 332.

| | |
|---|---|
| **entry** | describe |
| **Vlan** | Vlan Based Interface. |
| **Vlan id** | Vlan id created. |

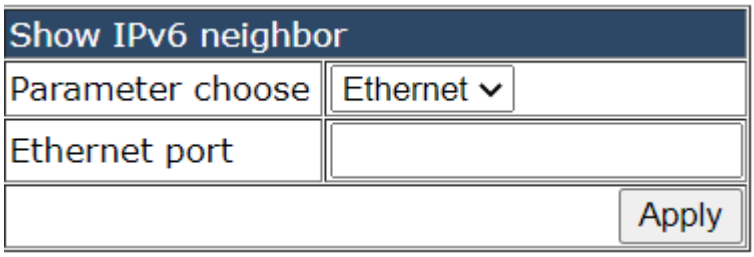



Figure 333.

| | |
|---|---|
| **entry** | describe |
| **ethernet** | Based on Ethernet port. |
| **Ethernet port** | Physical Port Name. |

## 20.2 Show IPv6 route

### 20.2.1 Show IPv6 route database

This page is used to view IPv6 routing table database information.

To display the “Show IPv6 route database” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 route database, click “Apply” to view.

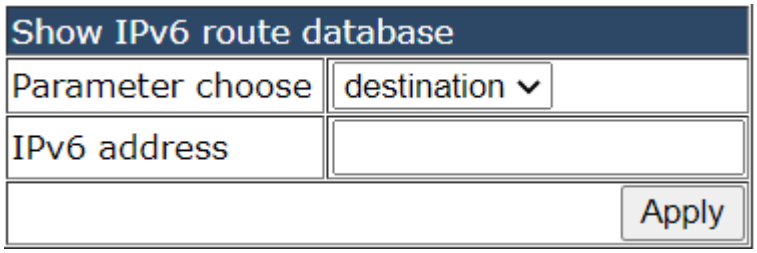



Figure 334.

| | |
|---|---|
| **entry** | describe |
| **Destination** | Based on ipv6 address. |
| **IPv6 address** | IPv6 address in the routing table. |

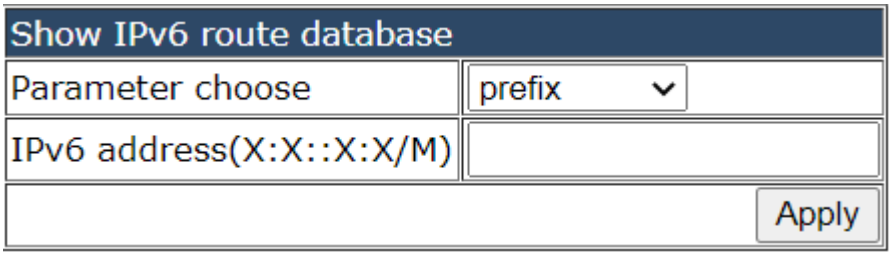



Figure 335.

| | |
|---|---|
| **entry** | describe |
| **Prefix** | Based on ipv6 address. |
| **IPv6 address** | IPv6 address in the routing table. |

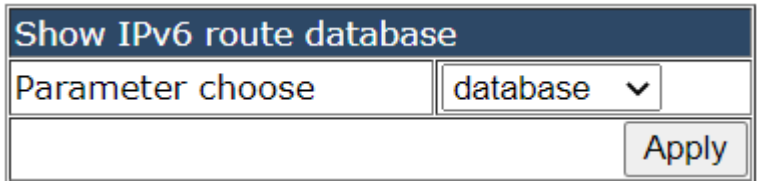



Figure 336.

| | |
|---|---|
| **entry** | describe |

| | |
|---|---|
| **database** | Routing table database information. |

### 20.2.2 Show IPv6 NSM route

This page is used to view IPv6 NSM routing table information.

To display the “Show IPv6 NSM route” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 NSM route, click “Apply” to view.

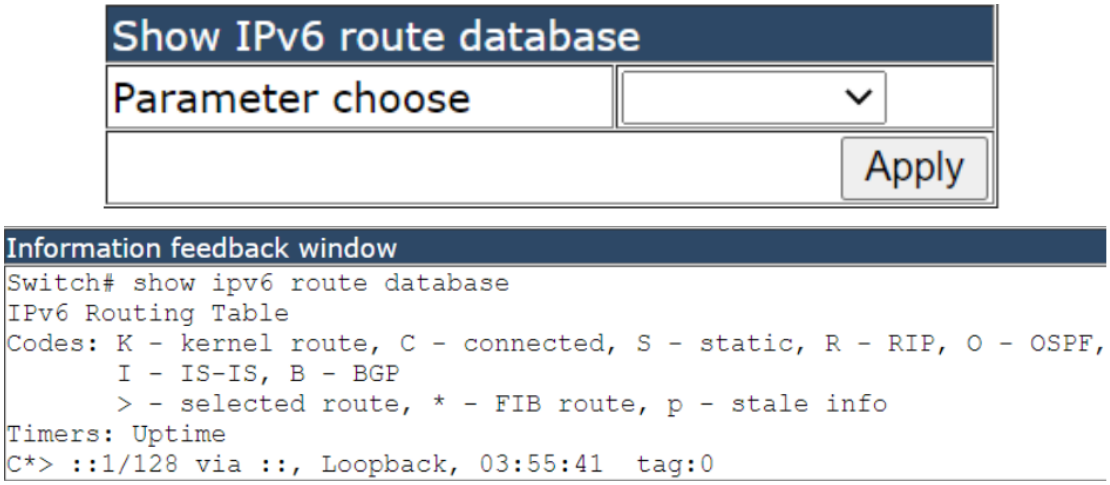



Figure 337.

| | |
|---|---|
| **entry** | describe |
| **connected** | IPv6 routing table information from NSM. |

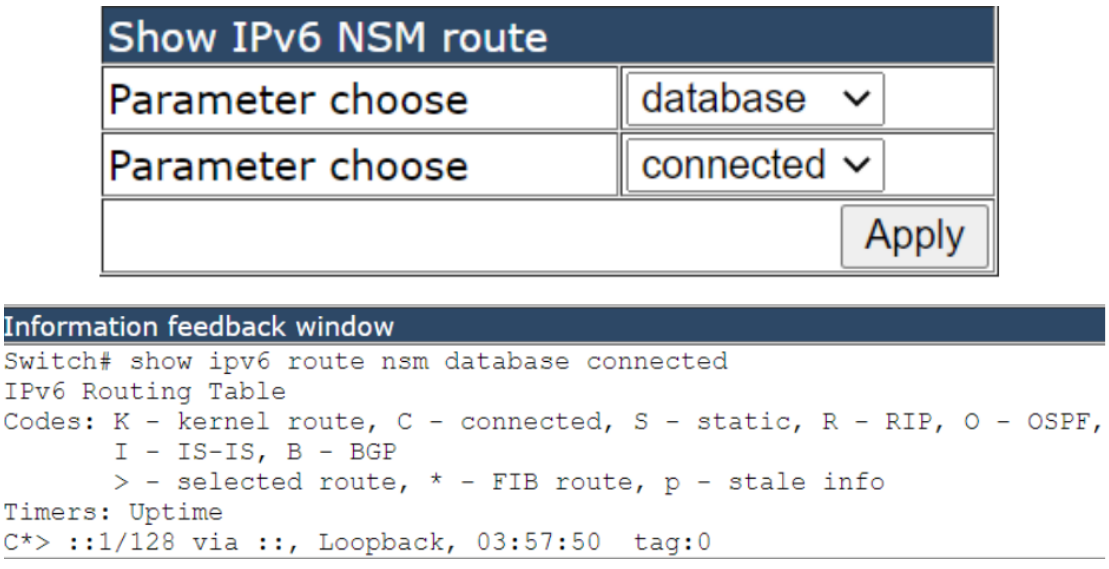



Figure 338.

| | |
|---|---|
| **entry** | describe |
| **database** | IPv6 Routing Table Database. |

| | |
|---|---|
| **connected** | Route table information. |

### 20.2.3 Show IPv6 FIB

This page is used to view IPv6 forward information.

To display the “Show IPv6 FIB” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 FIB, click “Apply” to view.

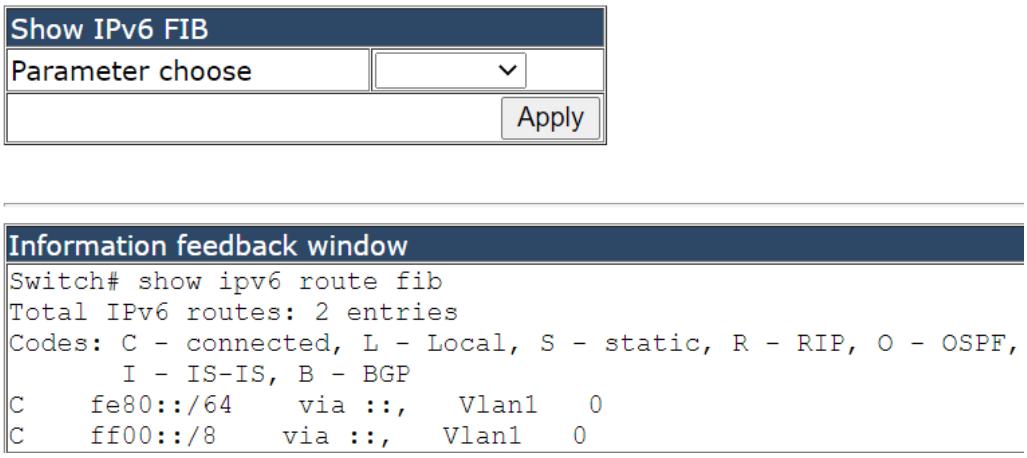



Figure 339.

| | |
|---|---|
| **entry** | describe |
| **Blank parameters** | Forwarding Information Database. |

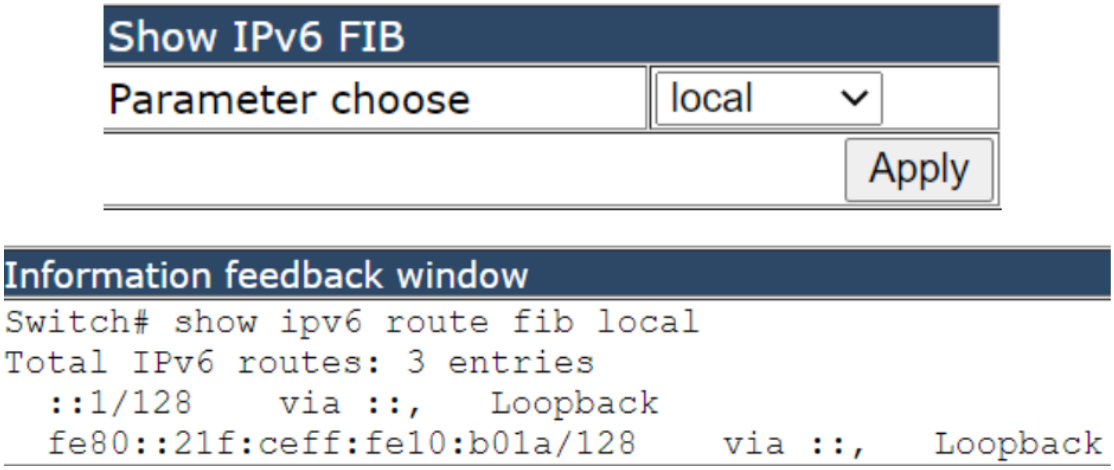



Figure 340.

| | |
|---|---|
| **entry** | describe |
| **Local** | Local table. |

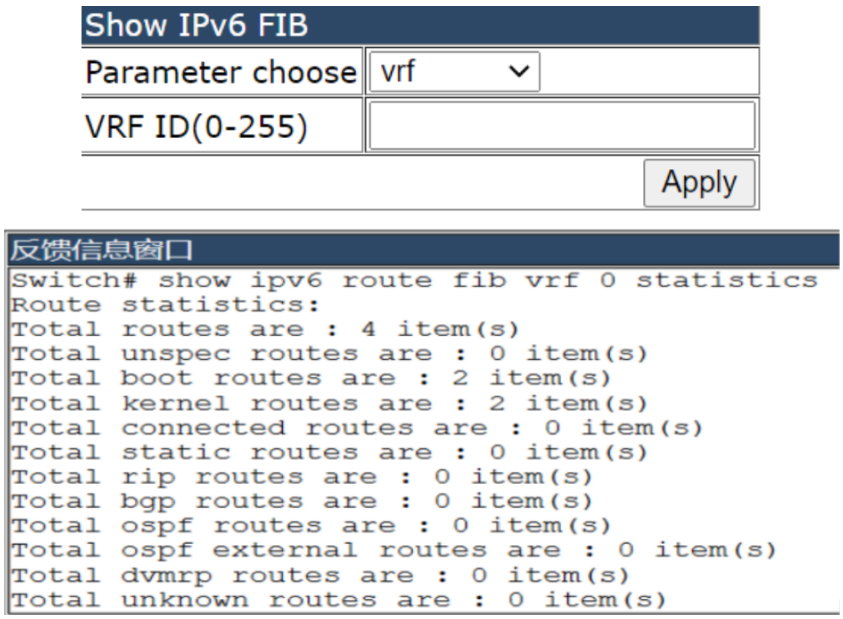



Figure 341.

| **entry** | describe |
|---|---|
| **Vrf** | Virtual routing transponder. |
| **VRF ID (0-255)** | Virtual Route Forwarder Number. |

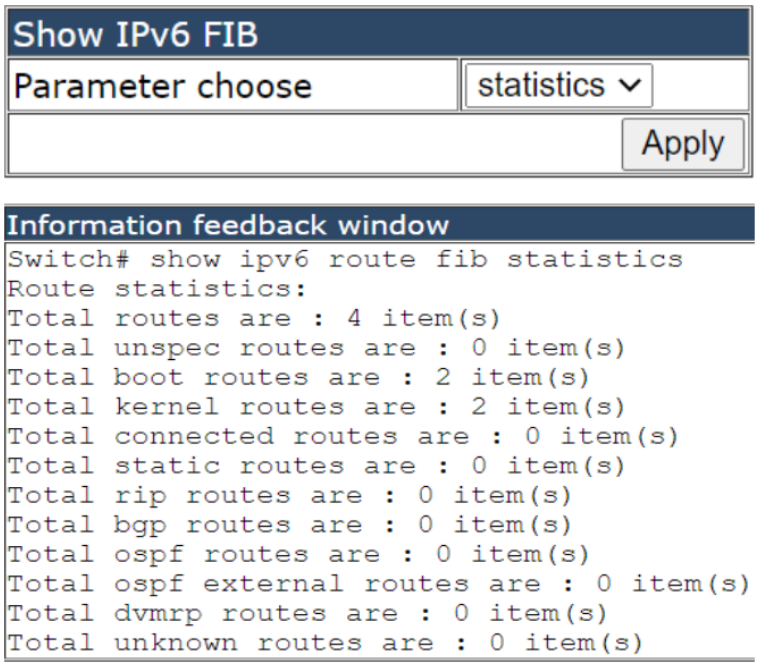



Figure 342.

| **entry** | describe |
|---|---|
| **statistics** | Routing table statistics. |

### 20.2.4 Show IPv6 route statistics

This page is used to view IPv6 routing statistics.

To display the “Show IPv6 route statistics” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 route statistics, click “Apply” to view.

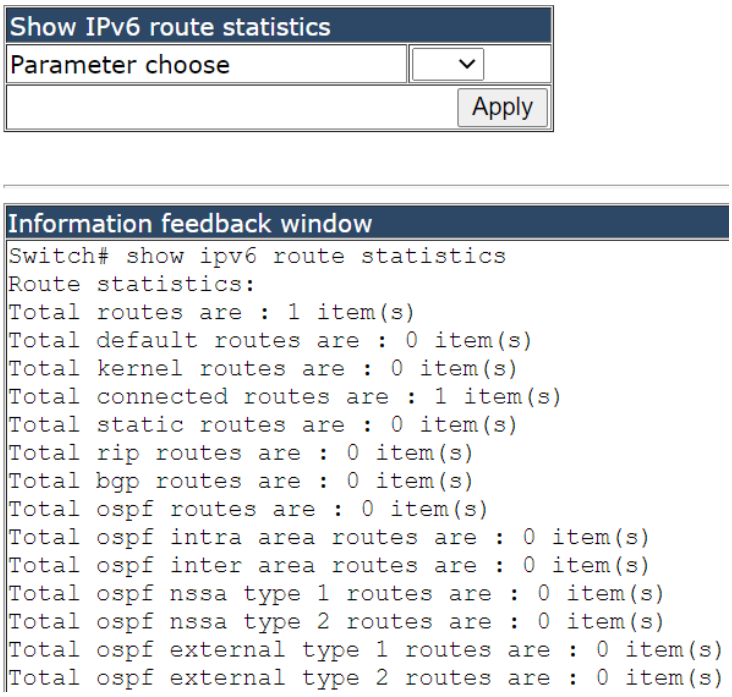



Figure 343.

Note: the corresponding function of parameter vrf has not been realized.

# 21. DCSCM configuration

## 21.1 DCSCM Source-control enable/disable configuration

Configure Dcscm multicast source control configuration and view the configuration status.

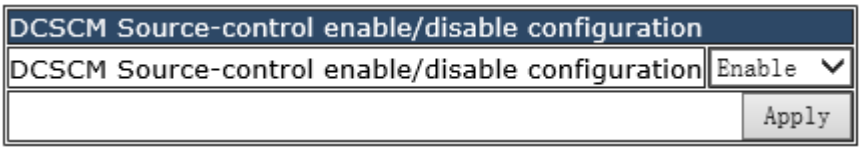



Figure 344.

| | | |
|---|---|---|
| **Dcscm Source-control enable/disable configuration** | Enable | Enable dcscm multicast source control configuration. |
| | Disable | Disable dcscm multicast source control configuration. |

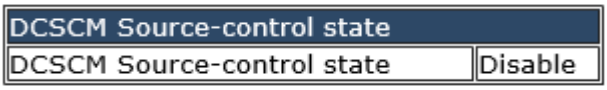



Figure 345. Display the current configuration status.

## 21.2 DCSCM destination-control enable/disable configuration

Configure Dcscm multicast destination control configuration and view configuration status.

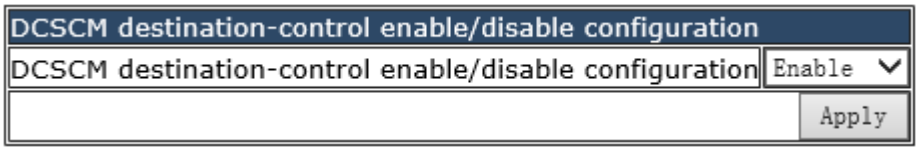



Figure 346.

| | | |
|---|---|---|
| **Dcscm destination-control enable/disable configuration** | Enable | Enable dcscm multicast destination control configuration. |
| | Disable | Disable dcscm multicast destination control configuration. |

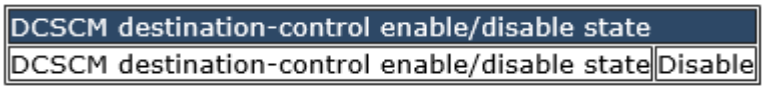



Figure 347. Display the current configuration status.

## 21.3 DCSCM Source-control access-group configuration

Configure Dcscm multicast source control list configuration and view the configuration status of the configuration list.

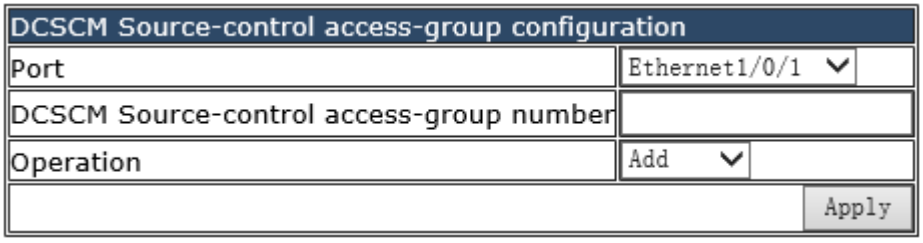



Figure 348.

| | | |
|---|---|---|
| **Port** | Port name | |
| **DCSCM destination-control access-group number** | Match the multicast data message imported from the interface according to the configured source control list number. The source control list number is derived from the ACL multicast source control configuration of ACL multicast control, range: 5000-5099. | |
| **Operation** | Add | Add source control list number under port. |
| | Remove | Delete the source control list from the port. |

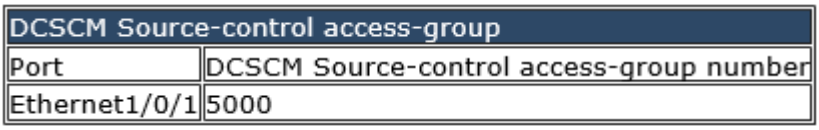



Figure 349. Display the currently configured port and the corresponding source control list number (there is no port configured by default).

## 21.4 DCSCM destination-control access-group configuration

Configure Dcscm multicast destination control list configuration and view configuration list configuration status.

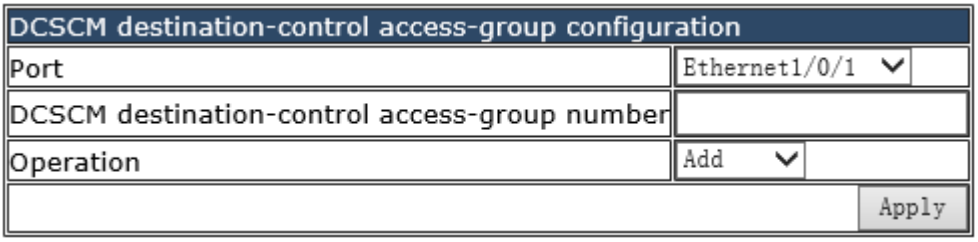



Figure 350.

| | | |
|---|---|---|
| **Port** | Port name | |
| **DCSCM destination-control access-group number** | Match the multicast data message imported from the interface according to the configured destination control list number. The destination control list number is derived from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999. | |
| **Operation** | Add | Add the destination control list number under the port. |
| | Remove | Delete the destination control list from the port. |

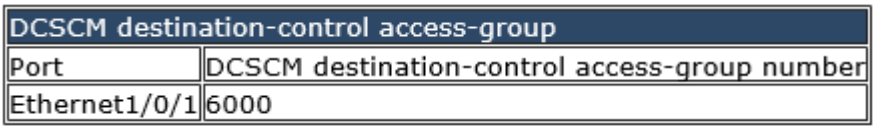



Figure 351. Display the currently configured port and the corresponding destination control list number (there is no port configured by default).

## 21.5 DCSCM destination-control access-group configuration (sip)

Configure the IP-based Dcscm port multicast destination control list configuration and view the configuration list configuration status.

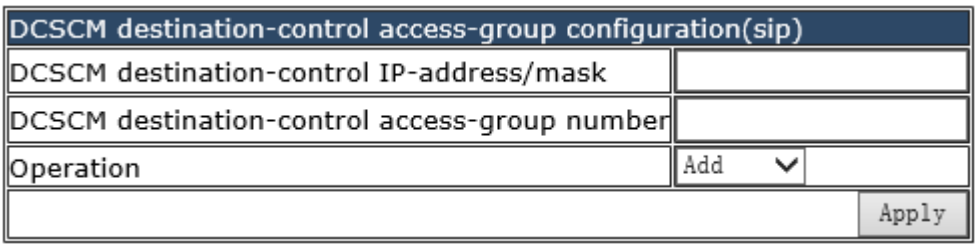



Figure 352.

| | | |
|---|---|---|
| **DCSCM destination-control IP-address/mask** | Determine the members of the multicast group according to the specified network end and mask. When the multicast group member matches the control list number, the interface can be added, otherwise the interface is not added. | |
| **DCSCM destination-control access-group number** | Match the multicast data message imported from the specified network according to the configured destination control list number. The destination control list number is configured from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999. | |
| **Operation** | Add | Add the destination control list number under the designated network terminal. |
| | Remove | Delete the destination control list from the specified network segment. |

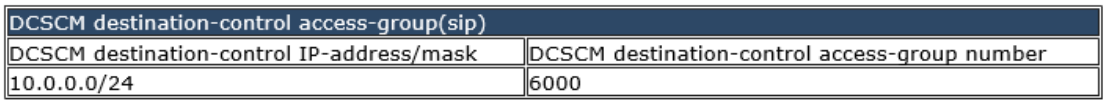



Figure 353.

Display the current configured destination IP address and the corresponding destination control list number (there is no configured port by default).

## 21.6 DCSCM destination-control access-group configuration (vMAC)

Configure VLAN-MAC based Dcscm multicast source control list configuration and view the configuration list configuration status.

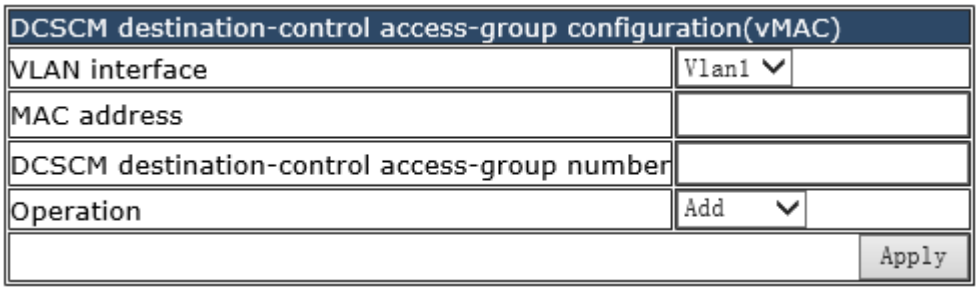



Figure 354.

| | | |
|---|---|---|
| **VLAN interface** | VLAN interface. | |
| **MAC address** | Transmit the source MAC address of IGMP-REPORT, the format is “xx-xx-xx-xx-xx-xx”. | |
| **DCSCM destination-control access-group number** | Match the multicast data message imported from the interface according to the configured destination control list number. The destination control list number is derived from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999. | |
| **Operation** | Add | Add the destination control list number to the host corresponding to the MAC address in the VLAN. |
| | Remove | Delete the destination control list from the corresponding MAC address host under the VLAN. |

DCSCM destination-control access-group(vMAC)

| VLAN interface | MAC address | DCSCM destination-control access-group number |
|---|---|---|
| 1 | 01-00-22-33-44-55 | 6000 |

Figure 355. Display the mac host and the corresponding destination control list number under the currently configured vlan (there is no configured port by default).

## 21.7 Multicast policy configuration

Configure multicast policy and view configuration status.

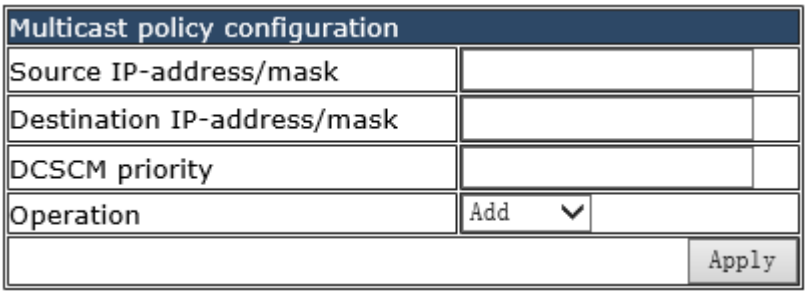



Figure 356.

| | | |
|---|---|---|
| **Source IP-address/mask** | The source IP address range of multicast data packets, format: 192.168.2.0/24. | |
| **Destination IP-address/mask** | The destination IP address range of multicast data packets, format: 224.0.0.0/8. | |
| **DCSCM priority** | Specify priority, range: 0-7. | |
| **Operation** | Add | Configure the switch matching priority of multicast data packets in a specified range to be modified to a specified value, and TOS is also specified to the same value. |
| | Remove | Delete the priority policy of multicast data in the specified |

| | | |
|---|---|---|
| | | range. |


Figure 357. Display the currently configured multicast policy.

## 21.8 ACL multicast source control

Configure ACL access rules and view the configuration status of the configuration list.

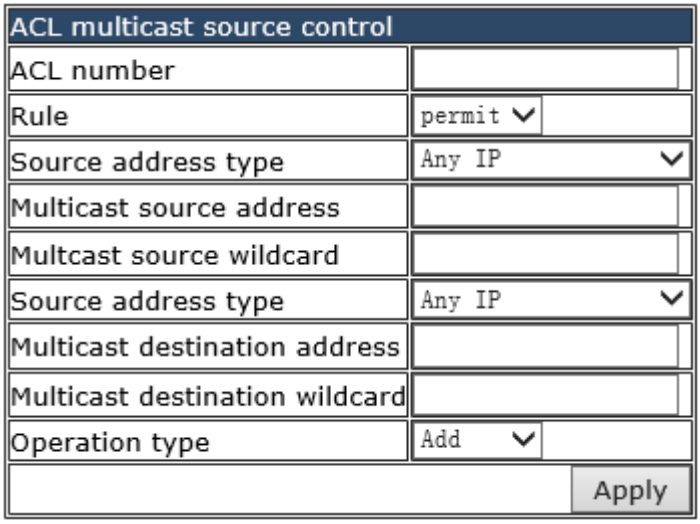



Figure 358.

| | | |
|---|---|---|
| **ACL number** | ACL number, range: 5000-5099. | |
| **Rule** | permit | Allow the following rules to pass. |
| | deny | Reject the following rules to pass. |
| **Source address type** | Specified address | An address range determined by IP addresses and address wildcards. |
| | Any IP | Any host address. |
| | Host Address | A specified address (set in the multicast source/destination IP address). |
| **Multicast source/destination address** | The address type is the host address and the IP address set when specifying the address, for example: 10.1.1.0 or 192.168.5.1. | |
| **Multcast source/destination wildcard** | The address type is the wildcard set when specifying the address, for example: 0.0.0.255. | |
| **Operation type** | Add | Add the set rules to the ACL number, and other functions use the source control list number to use these rules. |

| | | |
|---|---|---|
| | Remove | Delete the rule of ACL number. |

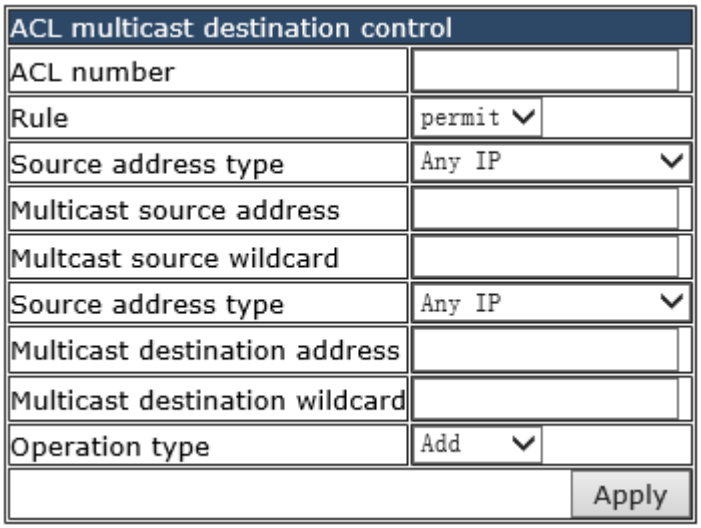



Figure 359.

| | | |
|---|---|---|
| **ACL number** | ACL number, range: 5000-5099. | |
| **Rule** | permit | Allow the following rules to pass. |
| | deny | Reject the following rules to pass. |
| **Source address type** | Specified address | An address range determined by IP addresses and address wildcards. |
| | Any IP | Any host address. |
| | Host Address | A specified address (set in the multicast source/destination IP address). |
| **Multicast source/destination address** | The address type is the host address and the IP address set when specifying the address, for example: 10.1.1.0 or 192.168.5.1. | |
| **Multcast source/destination wildcard** | The address type is the wildcard set when specifying the address, for example: 0.0.0.255. | |
| **Operation type** | Add | Add the set rules to the ACL number, and other functions use the source control list number to use these rules. |
| | Remove | Delete the rule of ACL number. |

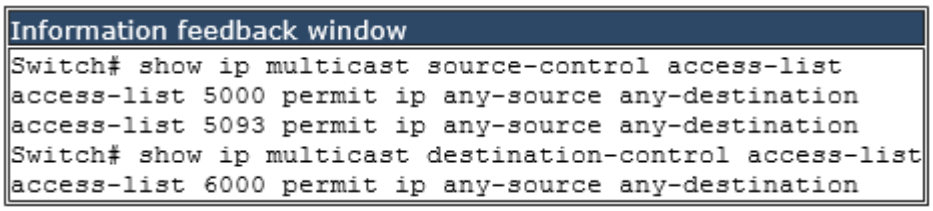


Figure 360. Display the currently configured multicast source control list number and multicast destination control list number rules.

# 22. Spanning-tree configuration

## 22.1 Spanning-tree field configuration

### 22.1.1 Instance configuration

This page can be used to configure the mapping relationship between the spanning tree instance and the VLAN.

To display the “Instance configuration” page, click Spanning-tree configuration -> Spanning-tree field configuration -> Instance configuration, click “Apply” to configure.

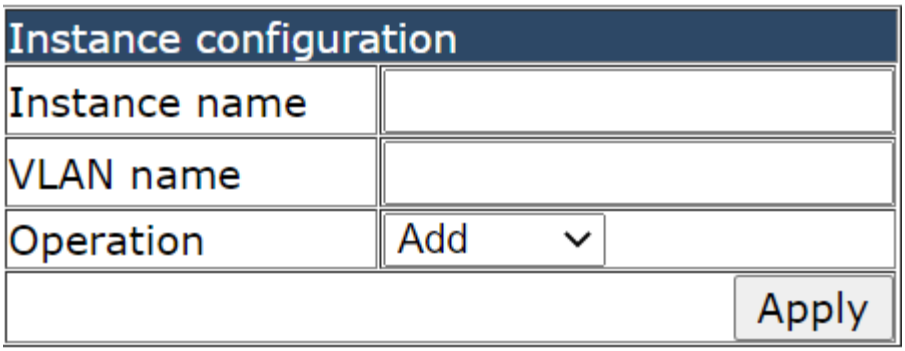



Figure 361.

| | |
|---|---|
| **entry** | describe |
| **Instance name** | Generating tree instance ID, range 0-64. |
| **VLAN name** | VLAN ID, range: 1-4094. |
| **Operation** | Add: Add the above configuration information.<br>Remove: Delete the above configuration information. |

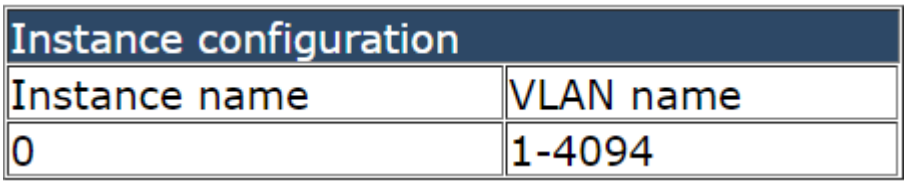



Figure 362.

| | |
|---|---|
| **entry** | describe |
| **Instance name** | Generating tree instance ID, size range 0-64. |
| **VLAN name** | VLAN ID, range: 1-4094. |

### 22.1.2 Field name configuration

This page can be used to configure MSTP domain name.

To display the “Instance configuration” page, click Spanning-tree configuration -> Spanning-tree field configuration -> Field name configuration, click “Apply” to configure.

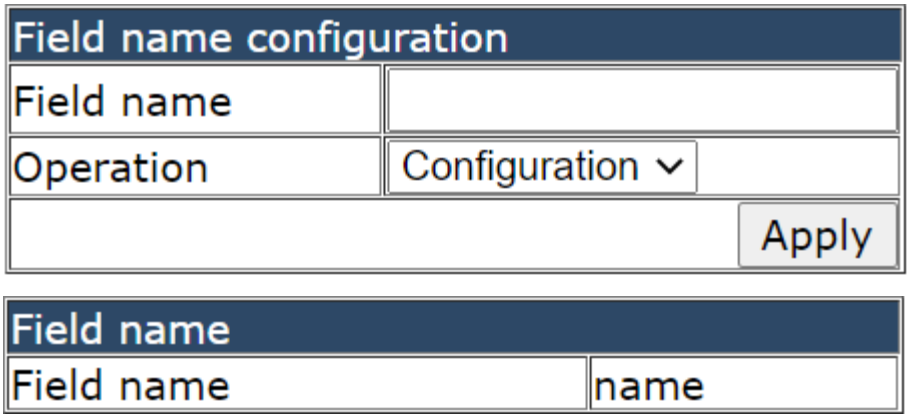



Figure 363.

| entry | describe |
|---|---|
| **Field name** | MSTP domain name, the length is 1-32 characters. |
| **Operation** | Configuration: Use the above configuration.<br>Default: Default does not match domain name. |

### 22.1.3 Revision-level configuration

This page can be used to configure MSTP revision level.

To display the “Instance configuration” page, click Spanning-tree configuration -> Spanning-tree field configuration -> Revision-level configuration, click “Apply” to configure.

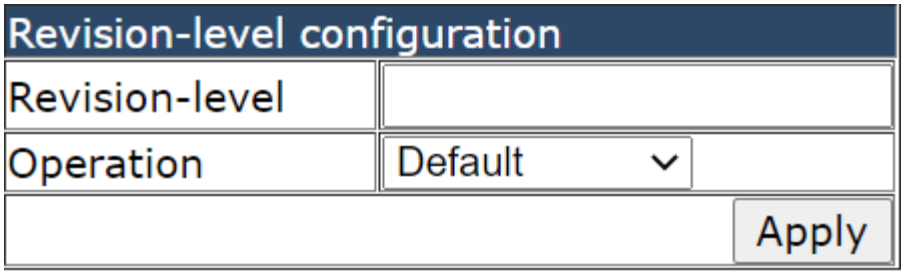



Figure 364.

| entry | describe |
|---|---|
| **Revision-level** | Range :0-65535. |
| **Operation** | Configuration: Use the above configuration.<br>Default: Restore default configuration 0. |


Figure 365.

| entry | describe |
|---|---|
| **Revision-level** | MSTP revision level with configuration, size range: 0-65535. |

## 22.2 Spanning-tree Port configuration

### 22.2.1 PortFast configuration

This page can be used for the configuration of edge ports.

To display the “PortFast configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> PortFast configuration, click “Apply” to configure.

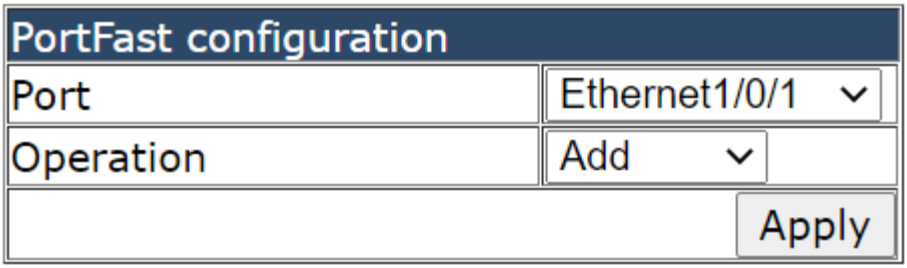
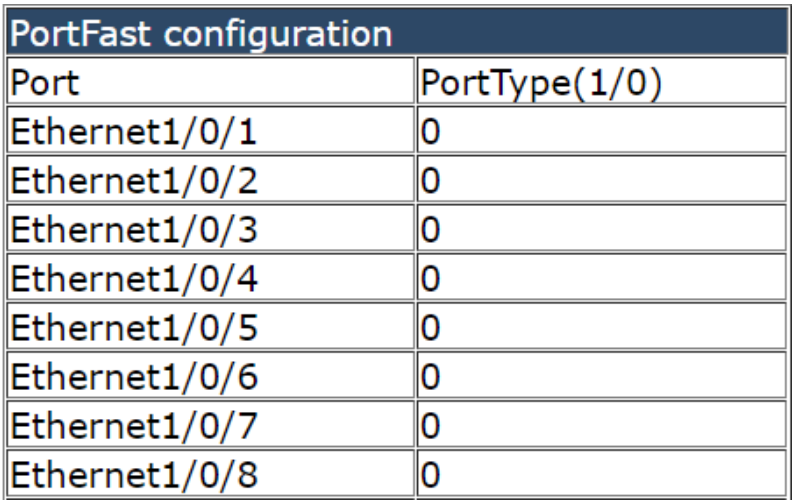



Figure 366.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **Operation** | Add: Configure the above port type to an edge port.<br>Remove: Configure the above port type to be a non-edge port. |



| PortFast configuration | |
|---|---|
| Port | PortType(1/0) |
| 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 |

Figure 367.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **PortType(1/0)** | 1: Represents an edge port.<br>0: Represents a non-edge port. |

### 22.2.2 Port priority configuration

This page can be used for configuration of instance port priority.

To display the “PortFast configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Port priority configuration, click “Apply” to configure.

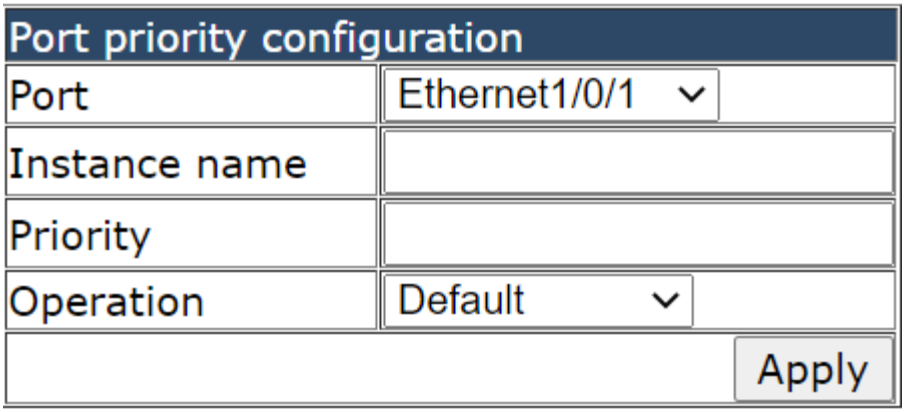



Figure 368.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **Instance name** | Generate tree instance name. |
| **Priority** | The size range is: 0-240, multiple of 16. |
| **Operation** | Configuration: Apply the above configuration. |

| | |
|---|---|
| | Default: Restore default priority 32768. |

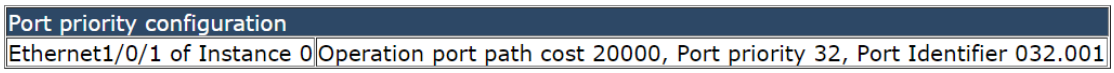



Figure 369.

### 22.2.3 Port cost configuration

This page can be used to configure port path costs.

To display the “Port cost configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Port cost configuration, click “Apply” to configure.

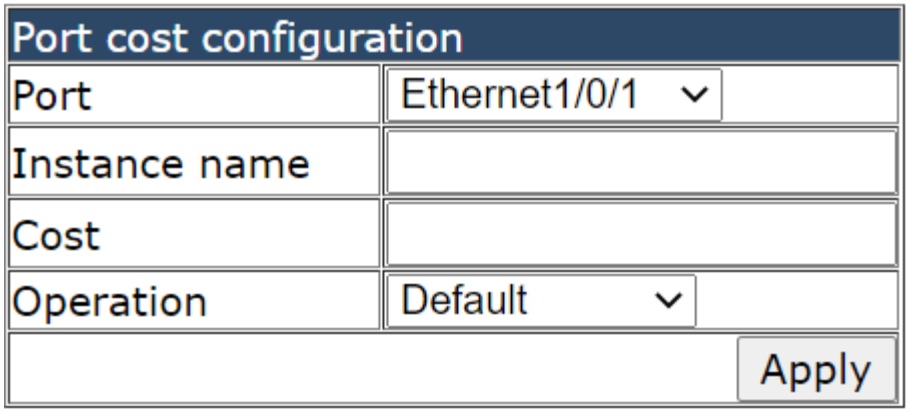



Figure 370.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **Instance name** | Generate tree instance name. |
| **Cost** | Size range: 0-200000000. |
| **Operation** | Configuration: Apply the above configuration.<br>Default: Recovery port default path cost. |

### 22.2.4 Spanning-tree port mode

This page can be used to configure the spanning tree running mode where the port is located.

To display the “Spanning-tree port mode” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Spanning-tree port mode, click “Apply” to configure.

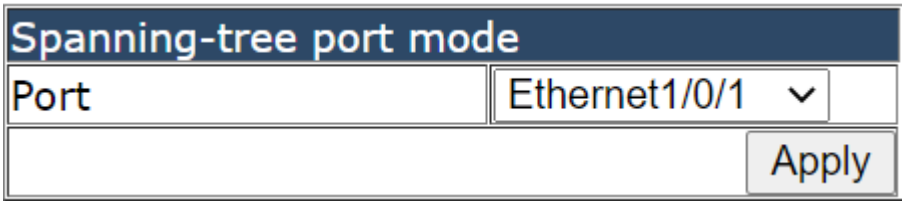



Figure 371.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |

### 22.2.5 Link-type configuration

This page can be used to configure port link types.

To display the “Link-type configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Link-type configuration, click “Apply” to configure.

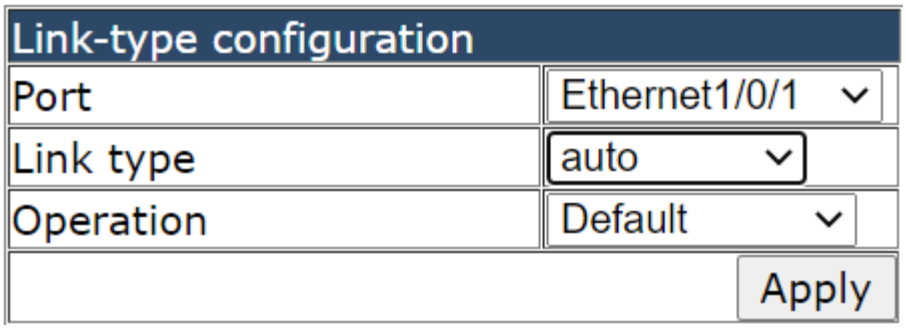



Figure 372.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **Link type** | Auto: Automatic consultations.<br>Force-true: Point-to-point type.<br>Force-false: Non-point-to-point type. |
| **Operation** | Configuration: Apply the above configuration.<br>Default: Auto is the default link type for the recovery port. |

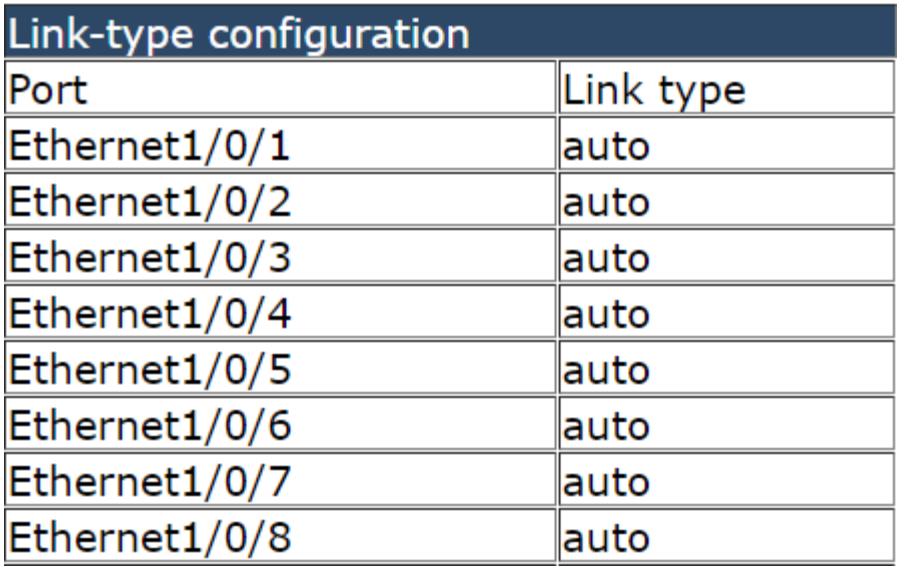



Figure 373.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **Link type** | Auto: Automatic consultations.<br>Force-true: Point-to-point type.<br>Force-false: Non-point-to-point type. |

### 22.2.6 Spanning-tree agreement port configuration

This page can be used to configure enable or disable the tree generation function under the port.

To display the “Spanning-tree agreement port configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Spanning-tree agreement port configuration, click “Apply” to configure.

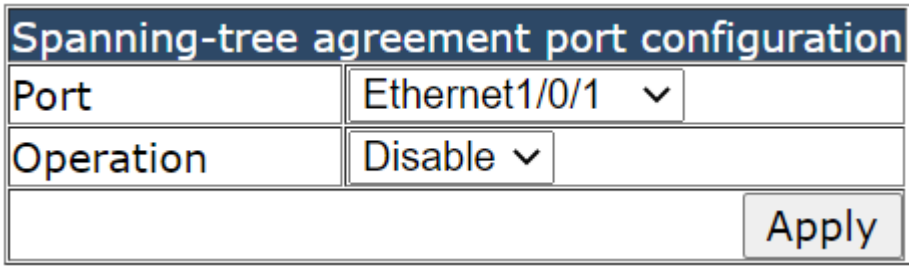



Figure 374.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **Operation** | Enable: Port enable spanning tree function.<br>Disable: Port disables spanning tree functionality. |

## 22.3 Spanning-tree global configuration

### 22.3.1 Spanning-tree global agreement port configuration

This page uses the build tree function with global enable.

To display the “Spanning-tree global agreement port configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning-tree global agreement port configuration, click “Apply” to configure.

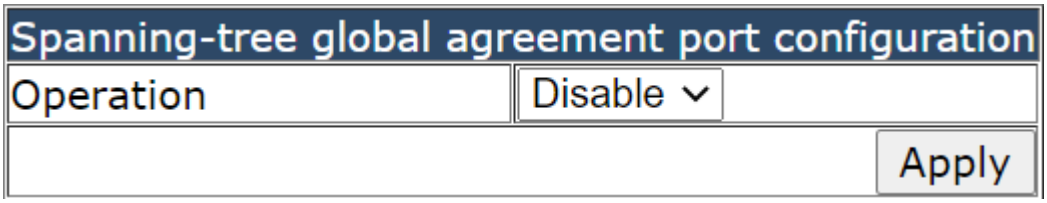



Figure 375.

| entry | describe |
|---|---|

| | |
|---|---|
| **Operation** | Enable: enable spanning tree function.<br>Disable: disable spanning tree functionality. |

### 22.3.2 Forward-time configuration

This page can be used to configure forwarding delay time.

To display the “Forward-time configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Forward-time configuration, click “Apply” to configure.

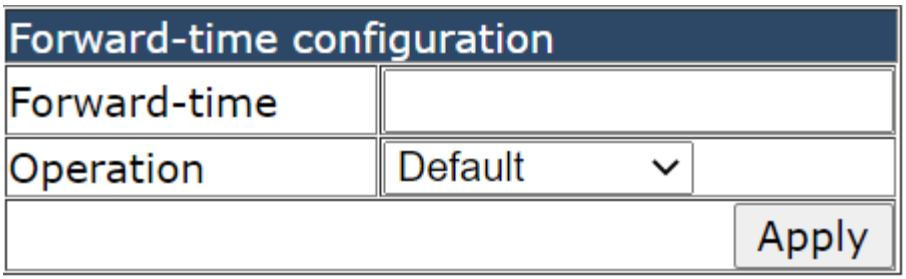



Figure 376.

| entry | describe |
|---|---|
| **Forward-time** | Size range: 4-30, in seconds, the following conditions shall be met:<br>2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age<br>Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds). |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default 15s. |

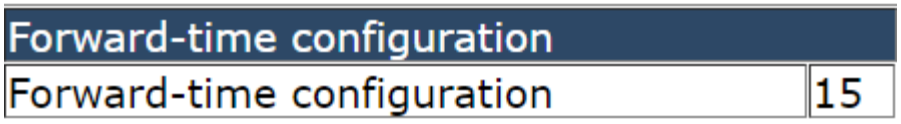



Figure 377.

| entry | describe |
|---|---|
| **Forward-time configuration** | Configuration of current forwarding delay time. |

### 22.3.3 Hello-time configuration

This page can be used to bpdu the configuration of the sending interval.

To display the “Hello-time configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Hello-time configuration, click "Apply" to configure.

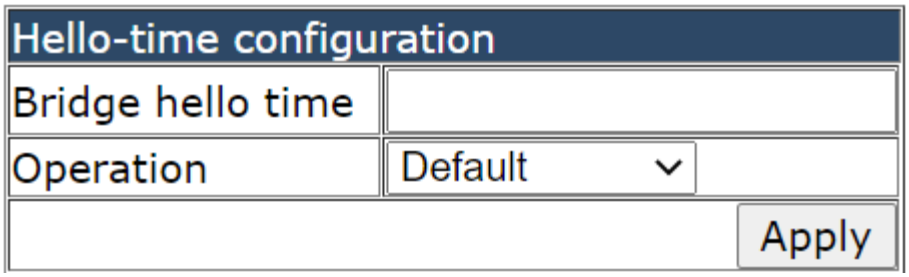



Figure 378.

| entry | describe |
|---|---|
| **Bridge hello time** | Size range: 1-10, in seconds, the following conditions shall be met:<br>2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age<br>Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds). |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default 2s. |


Figure 379.

| entry | describe |
|---|---|
| **Bridge hello time** | Current HELLO Maximum Survival Time Configuration. |

### 22.3.4 Max age time configuration

This page can be used to configure the maximum aging time of BPDU messages.

To display the “Max age time configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max age time configuration, click “Apply” to configure.

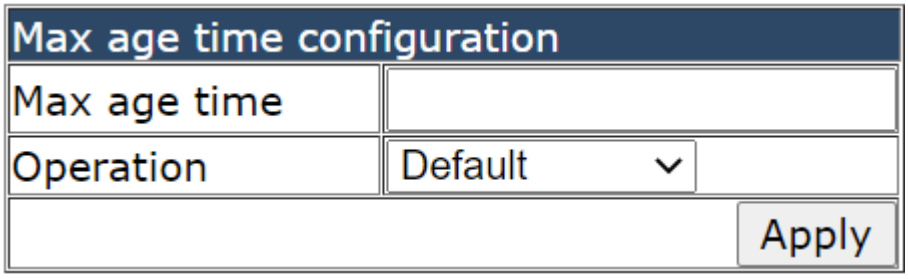



Figure 380.

| entry | describe |
|---|---|

| | |
|---|---|
| **Max age time** | Size range: :6-40, in seconds, the following conditions shall be met:<br>2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age<br>Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds). |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default 20s. |


Figure 381.

| **entry** | describe |
|---|---|
| **Max age time** | Configuration of current maximum aging time. |

### 22.3.5 Max hop time configuration

This page can be used to BPDU the maximum number of hops that packets are forwarded in the spanning tree domain.

To display the “Max hop time configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max hop time configuration, click “Apply” to configure.

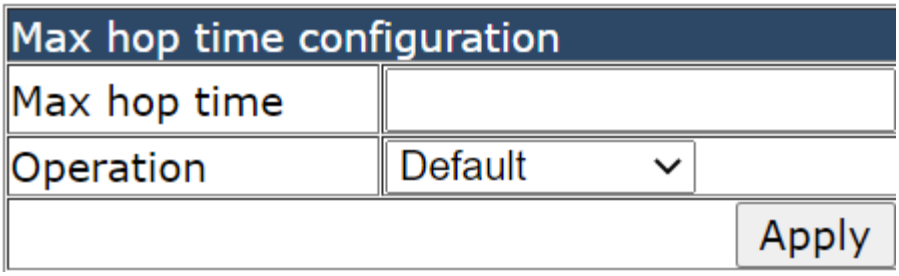



Figure 382.

| **entry** | describe |
|---|---|
| **Max hop time** | Numerical range: 1-40. |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default 20s. |


Figure 383.

| entry | describe |
|---|---|
| **Max hop time** | Maximum number of hops currently configured. |

### 22.3.6 Spanning tree mode configuration

This page is used to set the running mode of the switch spanning tree.

To display the “Spanning tree mode configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning tree mode configuration, click “Apply” to configure.

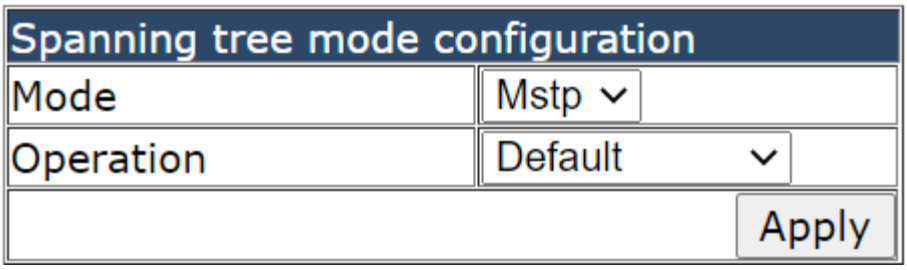



Figure 384.

| entry | describe |
|---|---|
| **Mode** | Generating tree protocol<br>type: Mstp.Stp.Rstp |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default configuration mode to mstp. |

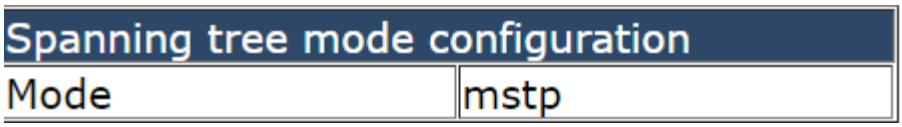



Figure 385.

| entry | describe |
|---|---|
| **Mode** | Current run spanning tree protocol type. |

### 22.3.7 Spanning tree cost-format configuration

This page is used to set the global configuration path cost format.

To display the “Spanning tree cost-format configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning tree cost-format configuration, click “Apply” to configure.

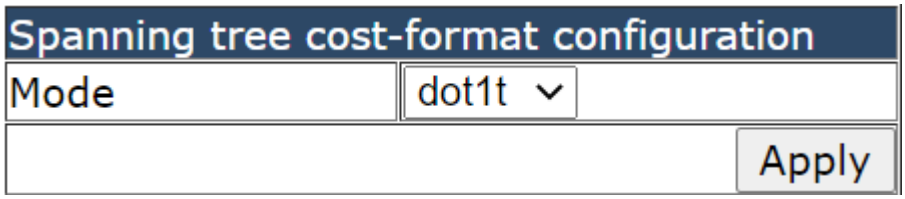


Figure 386.

| | |
|---|---|
| **entry** | describe |
| **Mode** | Path cost format: Dot1t.Dot1d. |

### 22.3.8 Priority configuration

This page is used to set the bridge priority of the spanning tree instance.

To display the “Priority configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Priority configuration, click “Apply” to configure.

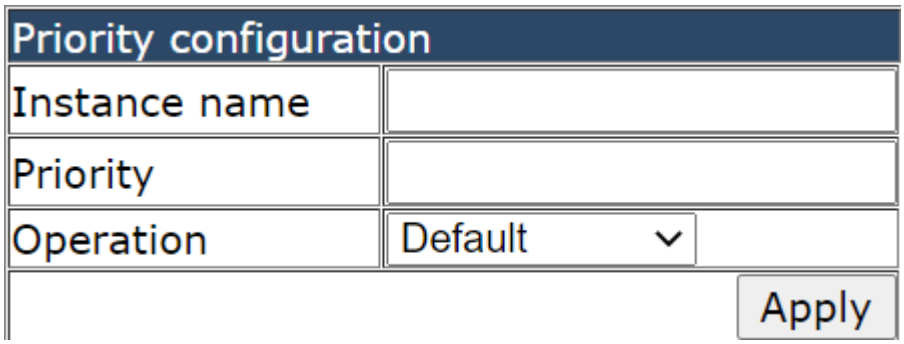



Figure 387.

| | |
|---|---|
| **entry** | describe |
| **Instance name** | Generate tree instance name. |
| **Priority** | Numerical range: 0-61440, and an integer multiple of 4096. |
| **Operation** | Configuration: Configure the above settings.<br>Default: Restore default configuration priority 32768. |

## 22.4 Show spanning-tree

### 22.4.1 Instance information

This page can be used to view information for the specified instance.

To display the “Instance information” page, click Spanning-tree configuration -> Show spanning-tree -> Instance information, click “Apply” to view.

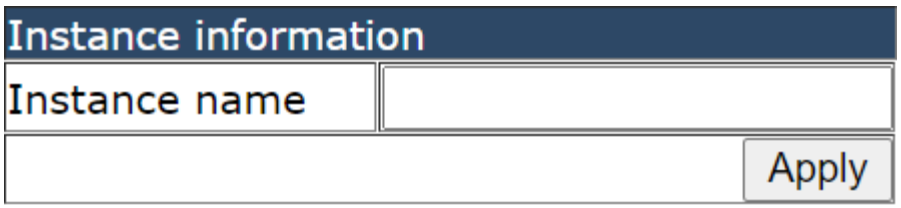



Figure 388.

| entry | describe |
| --- | --- |
| **Instance name** | Generate tree instance name. |

```
Information feedback window
Switch# show spanning-tree mst 0 detail
********************************** Process 0 ************************
############################ Instance 0 ############################
vlans mapped: 1-4094
Root Id     : this switch
Root Times  :  Max Age 20, Hello Time 2, Forward Delay 15, Max hops 20
Port 14 (Ethernet1/0/14) of Instance 0 is   DSGN forwarding
Port info:   port id  128.14   priority  128   cost  0
Designated root has priority 32768, address 001f.ce10.b01b
Designated bridge has priority 32768, address 001f.ce10.b01b
BPDU: sent     2348(TCN 0, CONFIG 0, MST 2348)
      received 0(TCN 0, CONFIG 0, MST 0)
```

Figure 389.

### 22.4.2 Revision-Level information

This page can be used to view configuration information for the spanning tree domain.

To display the “Revision-Level information” page, click Spanning-tree configuration -> Show spanning-tree -> Revision-Level information, click “Apply” to view.

```
Information feedback window
Switch# show spanning-tree mst config
Name          name
Revision      0
Instance      Vlans Mapped
---------------------------------
00            1-4094
---------------------------------
```

Figure 390.

# 23. MRPP configuration

## 23.1 MRPP global configuration

### 23.1.1 MRPP global switch configuration

This page is used to enable or disable MRPP protocols.

To display the “MRPP global switch configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP global switch configuration, click “Apply” to configure.

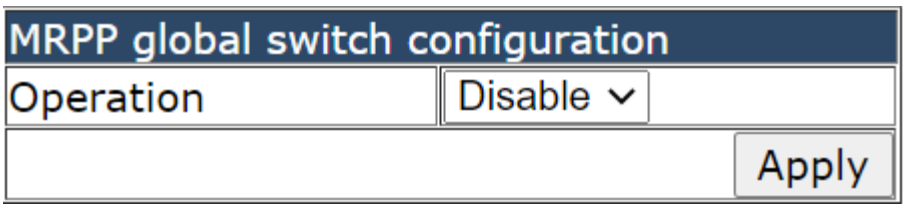



Figure 391.

| entry | describe |
|---|---|
| **Operation** | Enable: Enable MRPP protocol functionality.<br>Disable: Close MRPP Protocol Function. |

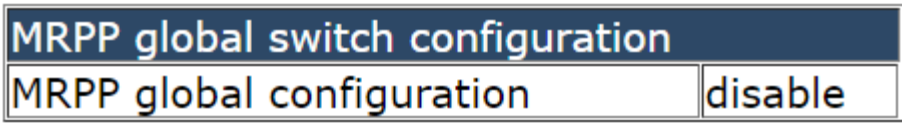



Figure 392.

| entry | describe |
|---|---|
| **MRPP global configuration** | Disable: Current mrpp protocol status is closed.<br>Enable: Current mrpp protocol status opens. |

### 23.1.2 MRPP poll time configuration

This page can be used to configure MRPP query time.

To display the “MRPP poll time configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP poll time configuration, click “Apply” to configure.

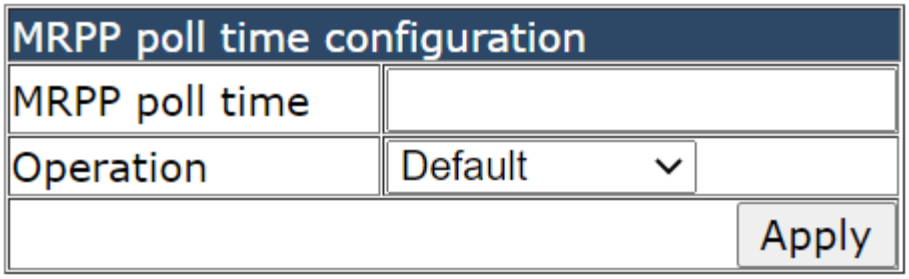



Figure 393.

| entry | describe |
|---|---|
| **MRPP poll time** | Range: 20-200, unit milliseconds. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Restore default ms 100. |

Figure 394.

| entry | describe |
|---|---|
| **MRPP poll time** | Current configured query time. |

### 23.1.3 MRPP domain id configuration

This page is used to set the ID number of the MRPP domain.

To display the “MRPP domain id configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP domain id configuration, click “Apply” to configure.

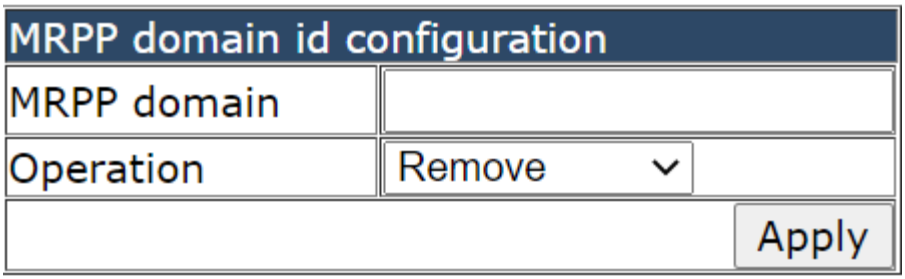



Figure 395.

| entry | describe |
|---|---|
| **MRPP domain** | ID range: 1-4096. |
| **Operation** | Configuration: Apply the above settings.<br>Default: Delete configured domain ID. |

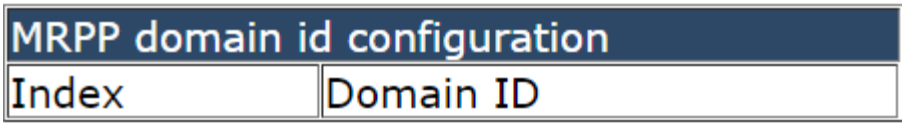



Figure 396.

| entry | describe |
|---|---|
| **Domain ID** | Domain ID range: 1-4096. |

## 23.2 MRPP port configuration

### 23.2.1 MRPP port property configuration

This page can be used to configure the primary and secondary ports of the MRPP ring.

To display the “MRPP port property configuration” page, click MRPP configuration -> MRPP port configuration -> MRPP port property configuration, click “Apply” to configure.

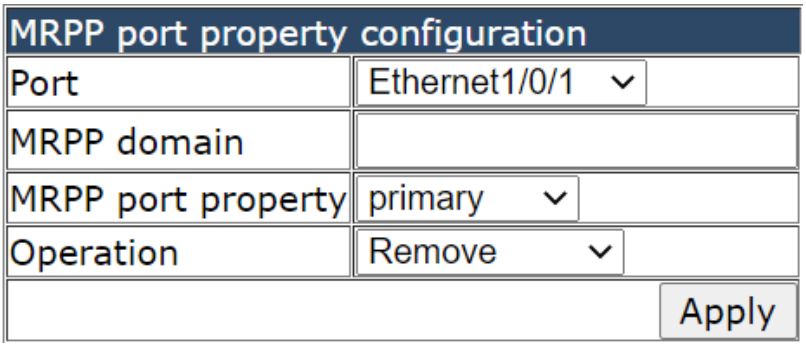



Figure 397.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **MRPP domain** | MRPP domain ID, range: 1-4096. |
| **MRPP port property** | Primary: Main port.<br>Secondary: Secondary port. |
| **Operation** | Add: Apply the above configuration.<br>Remove: Delete the above configuration. |

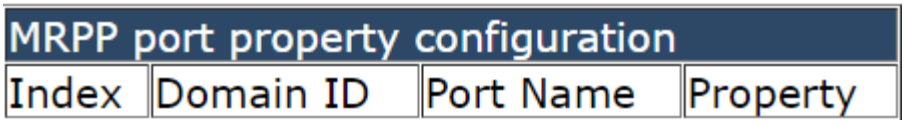



Figure 398.

| | |
|---|---|
| **entry** | describe |
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **Port Name** | Ethernet port. |
| **Property** | Primary: Main port.<br>Secondary: Secondary port. |

## 23.3 MRPP domain configuration

### 23.3.1 MRPP control vlan config

This page can be used to configure control VLAN for MRPP rings.

To display the “MRPP control vlan configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP control vlan configuration, click “Apply” to configure.

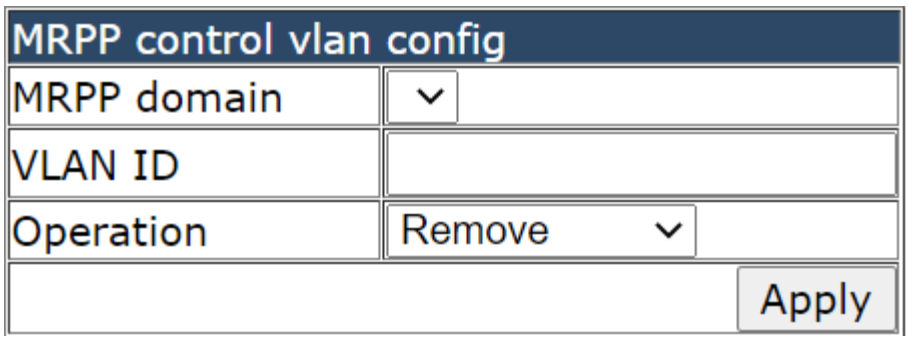



Figure 399.

| | |
|---|---|
| **entry** | describe |
| **MRPP domain** | MRPP domain ID, range created: 1-4096. |
| **VLAN ID** | VLAN ID, range: 1-4094. |
| **Operation** | Configuration: Apply the above configuration.<br>Remove: Delete the above configuration. |

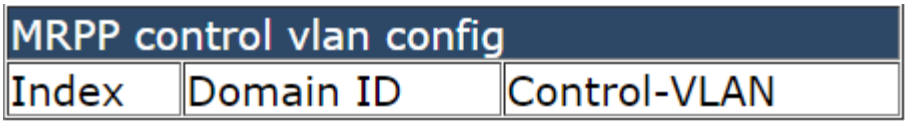



Figure 400.

| | |
|---|---|
| **entry** | describe |
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **Operation** | Scope of control VLAN, for current MRPP domain configuration: 1-4094. |

### 23.3.2 MRPP node mode config

This page can be used to configure MRPP nodes.

To display the “MRPP node mode configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP node mode configuration, click “Apply” to configure.

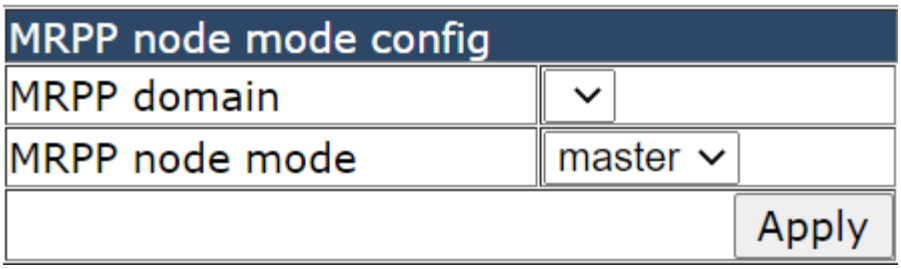



Figure 401.

| | |
|---|---|
| **entry** | describe |

| | |
|---|---|
| **MRPP domain** | MRPP domain ID, range: 1-4096. |
| **MRPP node mode** | Master: Master node.<br>Transit: Transmission node. |

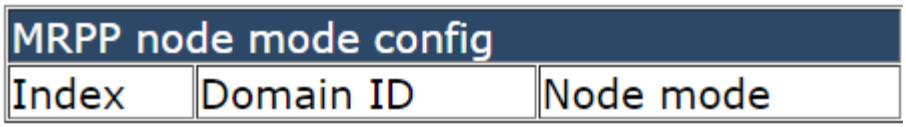



Figure 402.

| | |
|---|---|
| **entry** | describe |
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **Node mode** | Master: Master node.<br>Transit: Transmission node. |

### 23.3.3 MRPP hello timer config

This page can be used to MRPP Hello the configuration of message sending intervals.

To display the “MRPP hello timer configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP hello timer configuration, click “Apply” to configure.

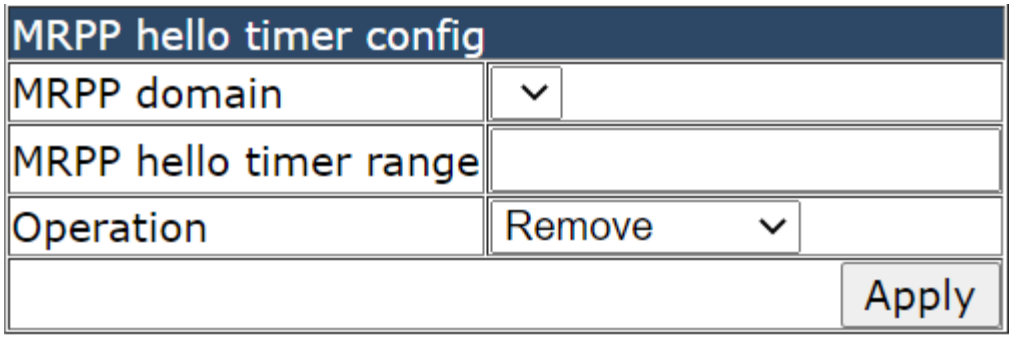



Figure 403.

| | |
|---|---|
| **entry** | describe |
| **MRPP domain** | MRPP domain ID, range: 1-4096. |
| **MRPP hello timer range** | Interval time range: 1-100 seconds. |
| **Operation** | Configuration: Apply the above configuration.<br>Remove: Delete the above configuration and restore the default configuration to 1 second. |

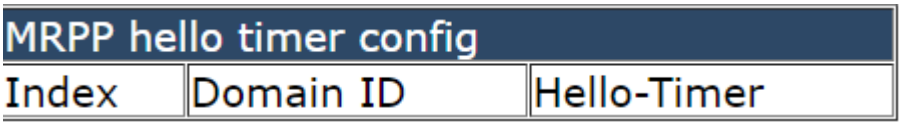


Figure 404.

| entry | describe |
|---|---|
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **Hello-Timer** | Hello message sending interval when the current configuration takes effect. |

### 23.3.4 MRPP fail timer config

This page is used MRPP configure the health message receive timeout.

To display the “MRPP fail timer configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP fail timer configuration, click “Apply” to configure.

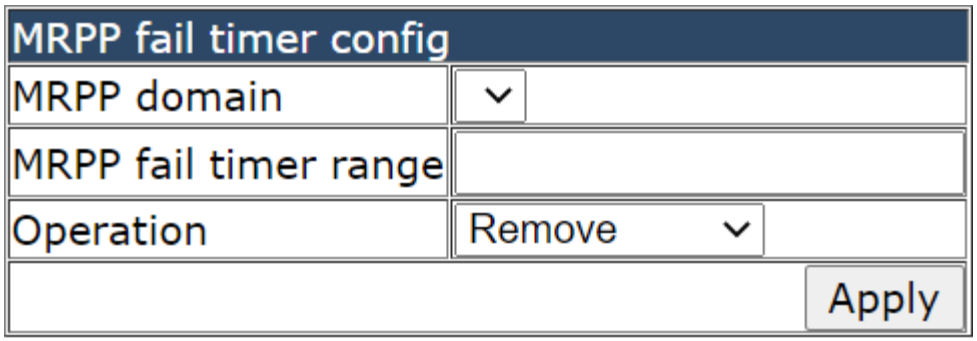



Figure 405.

| entry | describe |
|---|---|
| **MRPP domain** | MRPP domain ID, range: 1-4096. |
| **MRPP fail timer range** | Interval time range: 1-300 seconds. |
| **Operation** | Configuration: Apply the above configuration.<br>Remove: Delete the above configuration and restore the default configuration to 3 second. |

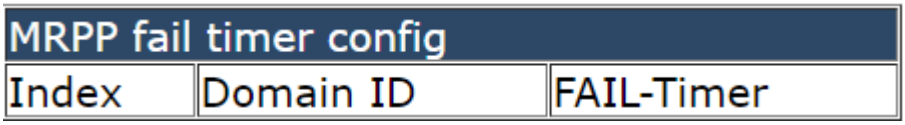



Figure 406.

| entry | describe |
|---|---|
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **FAIL-Timer** | Receive timeout when the current configuration takes effect. |

### 23.3.5 MRPP domain switch config

This page can be used to enable or disable MRPP rings.

To display the “MRPP domain switch config” page, click MRPP configuration -> MRPP domain configuration -> MRPP domain switch config, click “Apply” to configure.

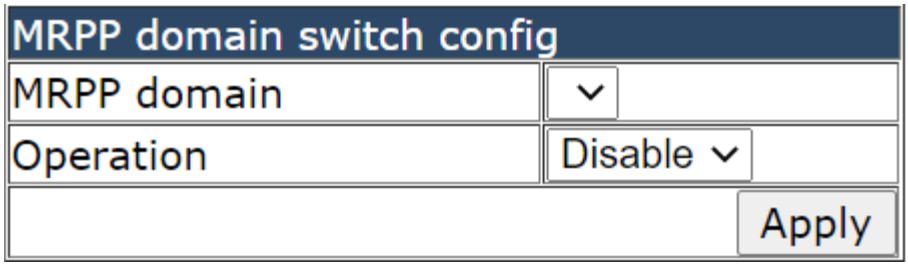



Figure 407.

| | |
|---|---|
| **entry** | describe |
| **MRPP domain** | MRPP domain ID, range: 1-4096. |
| **Operation** | Enable: Enable the corresponding MRPP ring.<br>Disable: Disable the corresponding MRPP ring. |

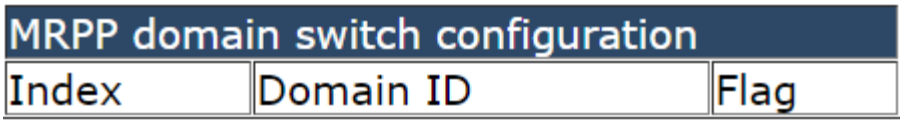



Figure 408.

| | |
|---|---|
| **entry** | describe |
| **Domain ID** | MRPP domain ID, range: 1-4096. |
| **Flag** | The enable state disable or enable of the currently configured active MRPP domain. |

## 23.4 MRPP configuration display

### 23.4.1 MRPP display

This page can be used to view configuration information for MRPP domains.

To display the “MRPP display” page, click MRPP configuration -> MRPP domain configuration -> MRPP display, click “Apply” to view.

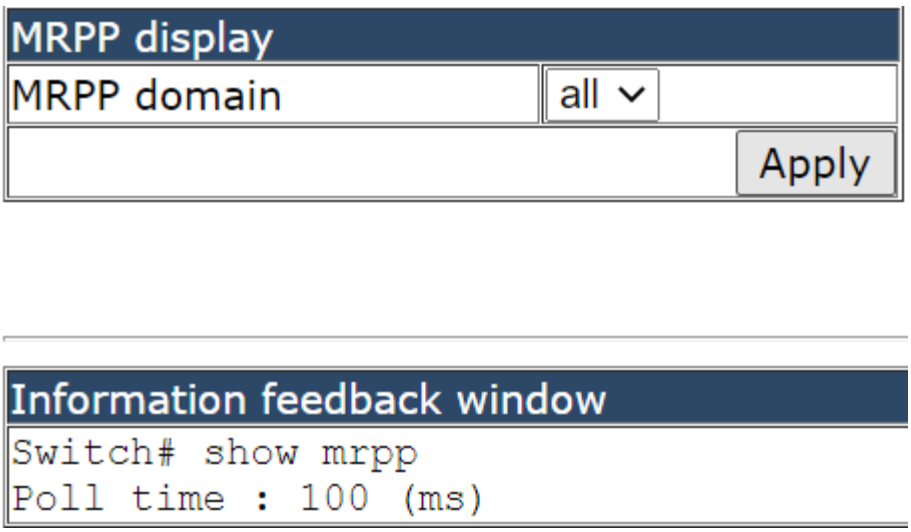



Figure 409.

| entry | describe |
|---|---|
| **Domain ID** | MRPP domain ID, range: 1-4096. |

### 23.4.2 MRPP statistics display

This page can be used to view statistics of MRPP domain data and status changes.

To display the “MRPP statistics display” page, click MRPP configuration -> MRPP domain configuration -> MRPP statistics display, click “Apply” to view.

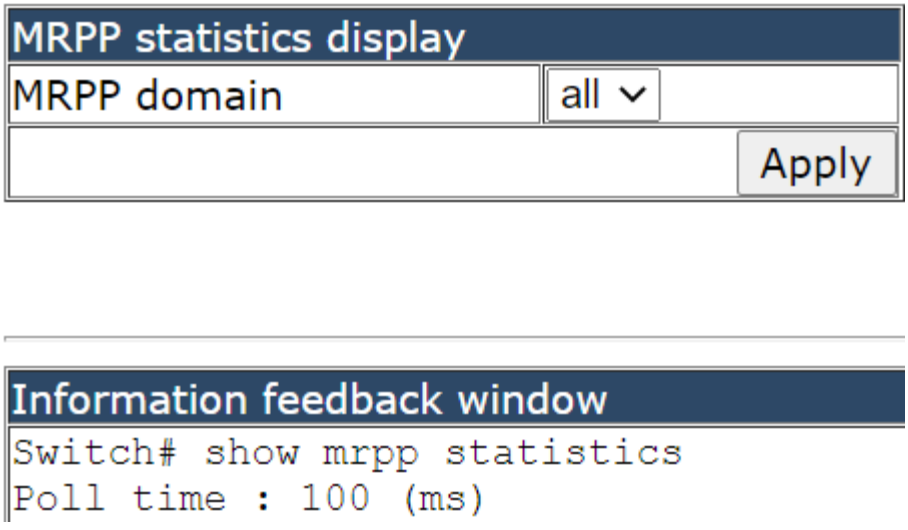



Figure 410.

| entry | describe |
|---|---|
| **Domain ID** | MRPP domain ID, range: 1-4096. |

### 23.4.3 Clear MRPP statistics

This page can be used to clear statistics for MRPP domains.

To display the “Clear MRPP statistics” page, click MRPP configuration -> MRPP domain configuration -> Clear MRPP statistics, click “Apply” to configure.

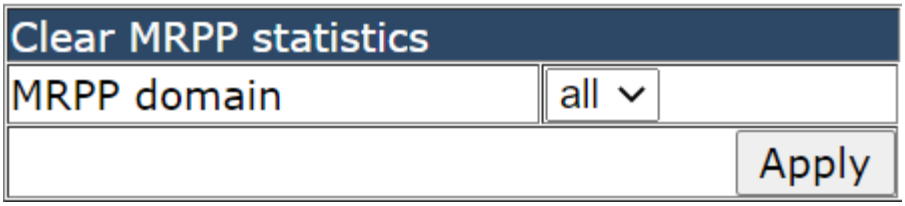



Figure 411.

# 24. ULPP configuration

## 24.1 ULPP global configuration

### 24.1.1 ULPP group configuration

This page can be used to add or delete ULPP groups.

To display the “ULPP group configuration” page, ULPP configuration -> ULPP global configuration -> ULPP group configuration, click “Apply” to configure.

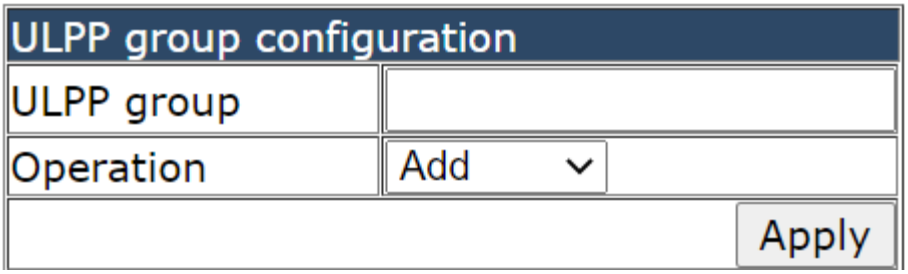



Figure 412.

| | |
|---|---|
| **entry** | describe |
| **ULPP group** | Group ID size range: 1-48. |
| **Operation** | Add: Add ULPP groups.<br>Remove: Delete ULPP groups. |


Figure 413.

| | |
|---|---|
| **entry** | describe |
| **ULPP group** | ULPP groups created. |

## 24.2 ULPP port configuration

### 24.2.1 ULPP port property configuration

This page can be used to set the port as the master-slave port of the ulpp group. It can also enable or disable receiving MAC address and ARP update packets, can also configure a control VLAN for the port.

To display the “ULPP port property configuration” page, ULPP configuration -> ULPP port configuration -> ULPP port property configuration, click “Apply” to configure.

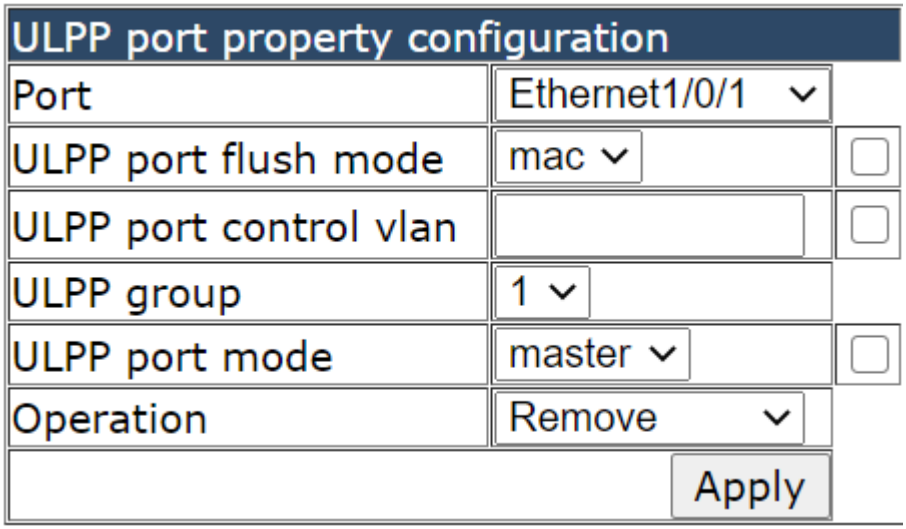



Figure 414.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **ULPP port flush mode** | Mac: Receive mac update packets.<br>Arp: Receive arp more packets. |
| **ULPP port control vlan** | Vlan created. |
| **ULPP group** | ULPP groups created. |
| **ULPP port mode** | Master: Main port.<br>Slave: Slave port. |
| **Operation** | Configuration: Apply the above configuration.<br>Remove: Delete the above configuration. |

## 24.3 ULPP group configuration

### 24.3.1 ULPP group description configuration

This page can be used to configure the description name for ULPP group.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP group configuration -> ULPP group description configuration, click “Apply” to configure.

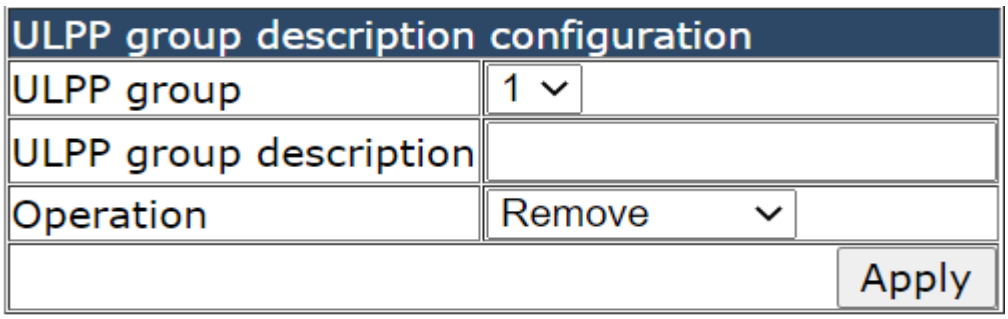



Figure 415.

| | |
|---|---|
| **entry** | describe |
| **ULPP group** | ULPP groups created. |
| **ULPP group description** | 1-128 characters in length. |
| **Operation** | Configuration:<br>Apply the above configuration.<br>Remove:<br>Delete the above configuration. |

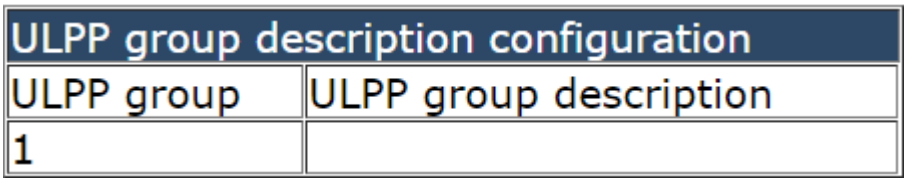



Figure 416.

| | |
|---|---|
| **entry** | describe |
| **ULPP group** | ULPP groups created. |
| **ULPP group description** | Description of ULPP groups currently set. |

### 24.3.2 ULPP group property configuration

This page can be used to configure the ulpp group properties of preemption mode, preemption delay, protection VLAN, control VLAN, flush mode, etc.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP group configuration -> ULPP group property configuration, click “Apply” to configure.

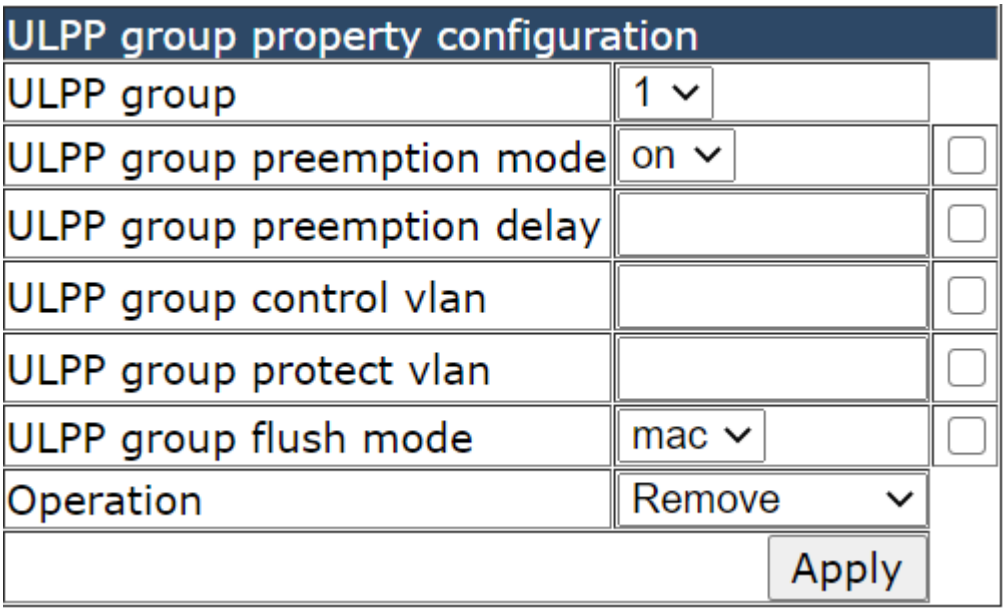
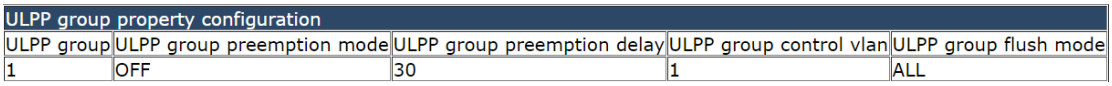



Figure 417.

| entry | describe |
|---|---|
| **ULPP group** | ULPP groups created. |
| **ULPP group preemption mode** | On: Preemptive mode enabled.<br>Off: Disable Preemptive Mode. |
| **ULPP group preemption delay** | Delay time range: 1-600, per second. |
| **ULPP group control vlan** | Created VLAN, VLAN ID between 1-4094. |
| **ULPP group protect vlan** | MSTP instance list, value range: 1-4094. |
| **ULPP group flush mode** | Mac: Send mac update packet.<br>Arp: Send arp update packet. |
| **Operation** | Configuration:<br>Apply the above configuration.<br>Remove:<br>Delete the above configuration. |



ULPP group property configuration

| ULPP group | ULPP group preemption mode | ULPP group preemption delay | ULPP group control vlan | ULPP group flush mode |
|---|---|---|---|---|
| 1 | OFF | 30 | 1 | ALL |

Figure 418.

| entry | describe |
|---|---|
| **ULPP group** | ULPP group created. |
| **ULPP group preemption mode** | On: Preemptive mode enabled.<br>Off: Disable Preemptive Mode. |

| | |
|---|---|
| **ULPP group preemption delay** | Delay time for current configuration. |
| **ULPP group control vlan** | ULPP group control VLAN currently set. |
| **ULPP group protect vlan** | MSTP instance list, value range: 1-4094. |
| **ULPP group flush mode** | Mac: Send mac update packet.<br>Arp: Send arp update packet.<br>ALL: Send mac and arp update packet. |

## 24.4 ULPP configuration display

### 24.4.1 ULPP group configuration display

This page can be used to view configuration information for ULPP groups.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP group configuration display, click “Apply” to view.

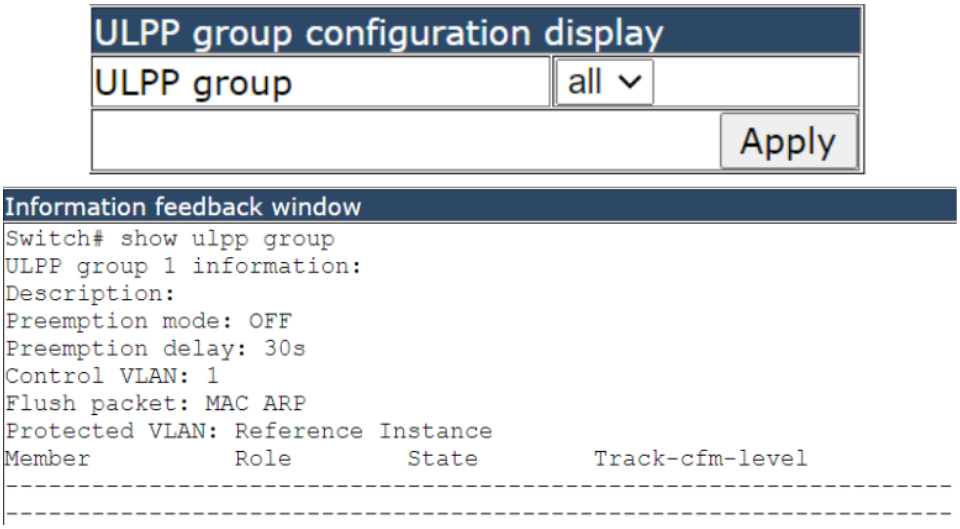



Figure 419.

### 24.4.2 ULPP port statistics display

This page can be used to view ULPP port statistics.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port statistics display, click “Apply” to view.

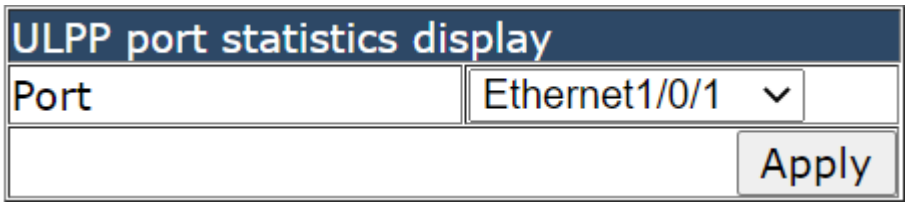



Figure 420.

### 24.4.3 ULPP port property display

This page can be used to view ULPP port configuration information.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port property display, click “Apply” to view.

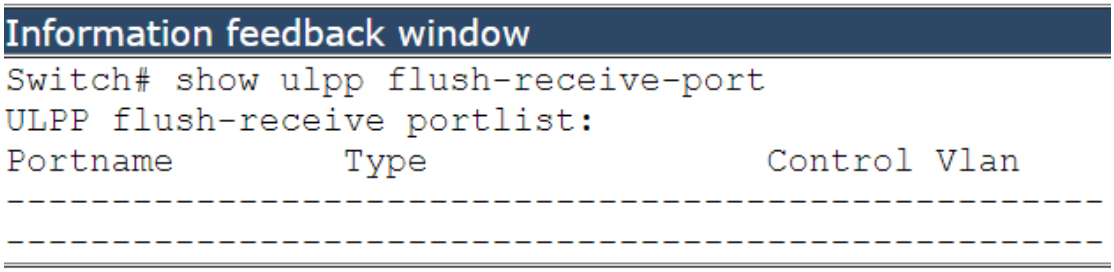



Figure 421.

### 24.4.4 ULPP port statistics clear

This page can be used to clear statistics of ULPP related data on the port.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port statistics clear, click “Apply” to view.

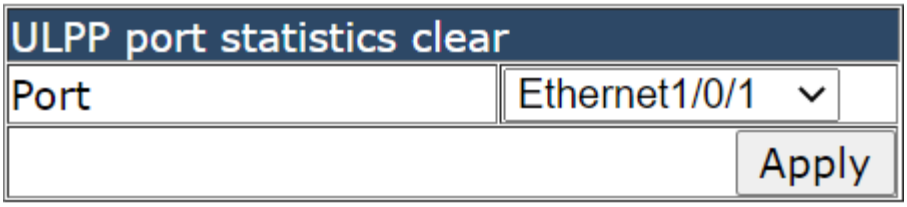



Figure 422.

# 25. ULSM configuration

## 25.1 ULSM global configuration

### 25.1.1 ULSM group configuration

This page can be used to create or delete ULSM groups.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM global configuration -> ULSM group configuration, click “Apply” to configure.

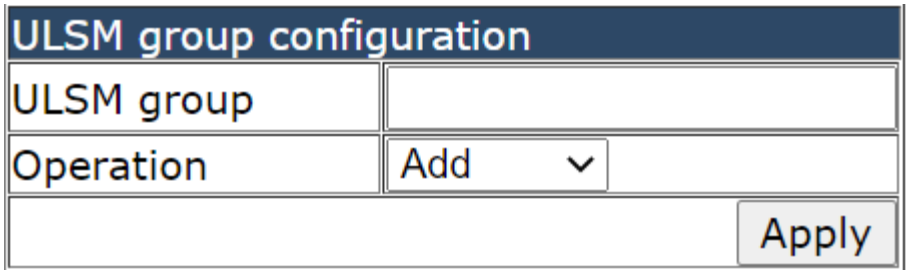



Figure 423.

| | |
|---|---|
| **entry** | describe |
| **ULSM group** | Group ID range: 1-32. |
| **Operation** | Add: Create a ULSM group. |

| | |
|---|---|
| | Remove: Removing ULSM groups of corresponding ID. |


Figure 424.

| entry | describe |
|---|---|
| **ULSM group** | ULSM groups created. |

## 25.2 ULSM port configuration

### 25.2.1 ULSM port property configuration

This page can be used to add uplink or downlink ports for ULSM groups that have been created.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM port configuration -> ULSM port property configuration, click “Apply” to configure.

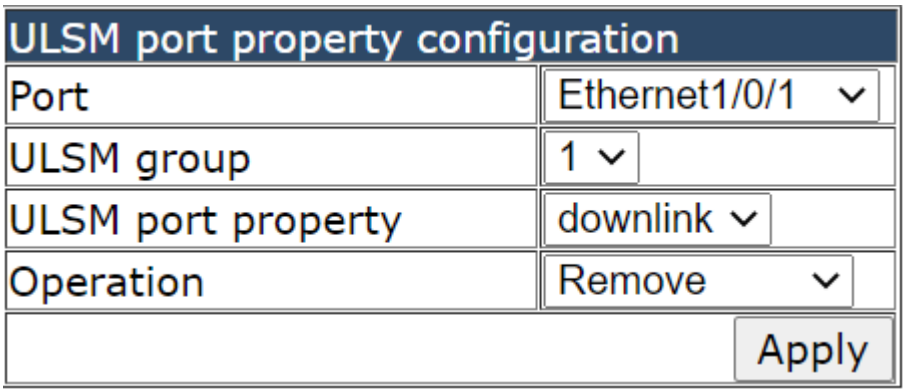



Figure 425.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **ULSM group** | ULSM groups created. |
| **ULSM port property** | Uplink: Uplink port.<br>Downlink: Downlink port. |
| **Operation** | Configuration: Apply the above settings.<br>Remove: Delete the above. |

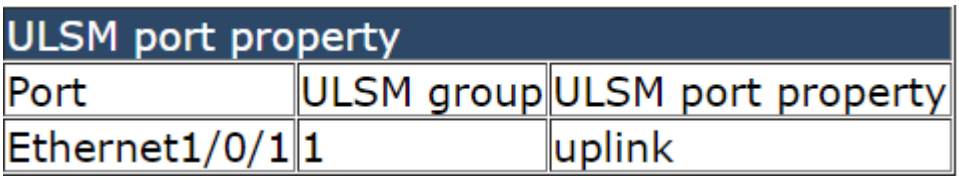


Figure 426.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **ULSM group** | ULSM groups created. |
| **ULSM port property** | Current ULSM groups correspond to configured upper and lower ports.<br>Uplink: Uplink port.<br>Downlink: Downlink port. |

## 25.3 ULSM configuration display

### 25.3.1 ULSM display

This page can be used to view the current status of the ULSM group and the status of the upper and lower ports within the group.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM port configuration -> ULSM port property configuration, click “Apply” to view.

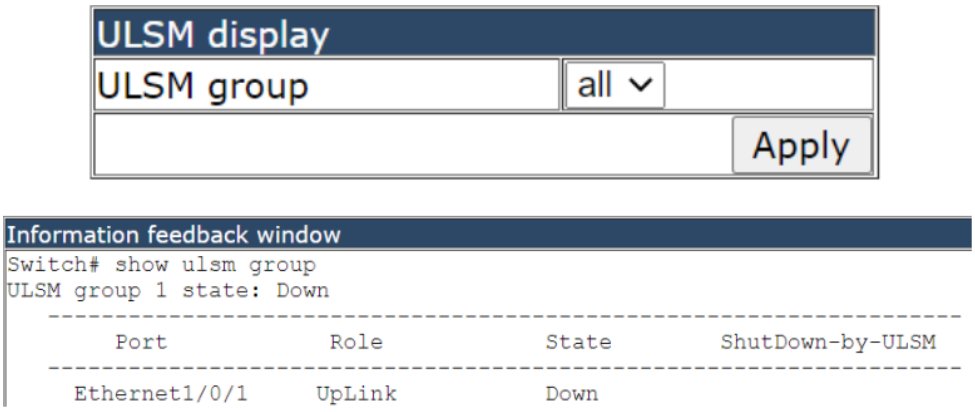



Figure 427.

# 26. Authentication configuration

## 26.1 RADIUS client configuration

### 26.1.1 RADIUS global configuration

RADIUS global configuration module, the users in this module can configure the global RADIUS function services.

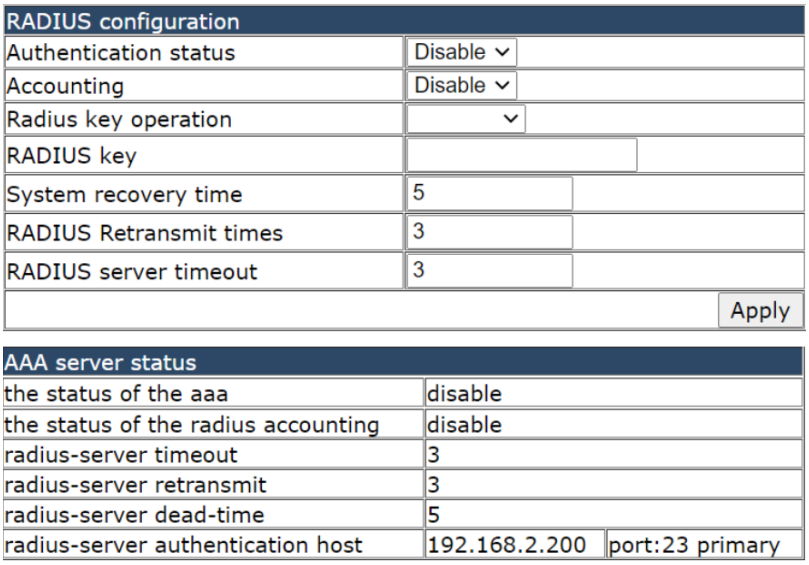



Figure 428.

| | | |
|---|---|---|
| **Authentication status** | Enable | Enable RADIUS certification services. |
| | Disable | Disabling RADIUS certification services. |
| **Accounting** | Enable | Enable RADIUS billing services. |
| | Disable | Disabling RADIUS billing services. |
| **Radius key operation** | Add | Add RADIUS key. |
| | Remove | Delete RADIUS key. |
| **RADIUS key** | Key string, 1-64 characters. | |
| **System recovery time** | Radius service recovery time from downtime to accessibility, 1-255 minutes. | |
| **RADIUS Retransmit times** | Radius authentication packet retransmission time, 1-100 seconds. | |
| **RADIUS server timeout** | The corresponding time of the radius server, 1-100 seconds. | |

### 26.1.2 RADIUS authentication configuration

RADIUS authentication configuration module, the users in this module can configure the RADIUS authentication server.

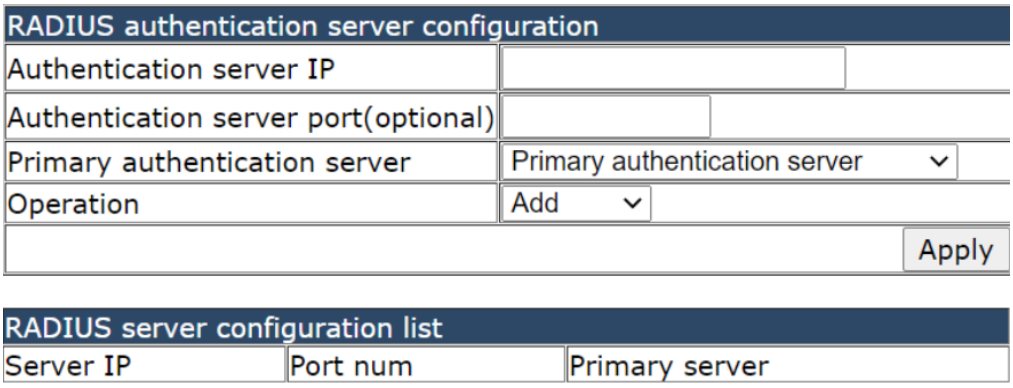



Figure 429.

| | | |
|---|---|---|
| **Authentication server IP** | The address of IPv4 or IPv6 of the radius authentication server. | |
| **Authentication server port** | Port number of radius authentication server(optional), 0-65535. | |
| **Primary authentication server** | Primary authentication server | Specify radius server as primary authentication server. |
| | Non-Primary authentication server | Specify radius server as non-primary authentication server. |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

### 26.1.3 RADIUS accounting configuration

Radius authentication and accounting module, the users in this module can configure the RADIUS billing server.

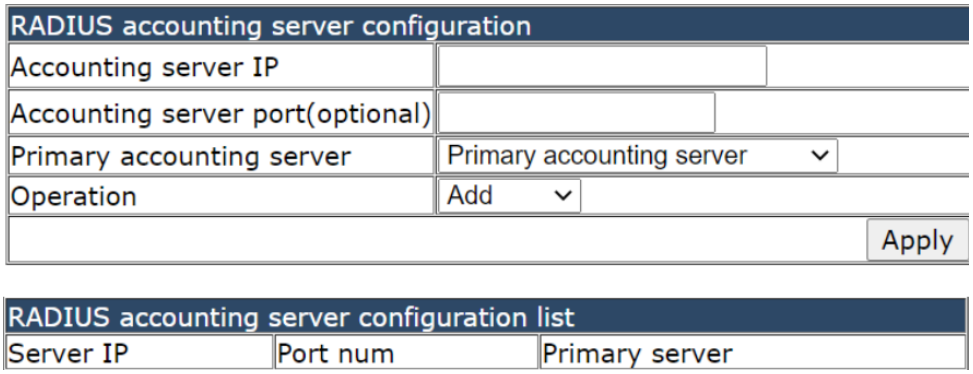



Figure 430.

| | |
|---|---|
| **Accounting server IP** | Radius authentication server IPv4 or IPv6 address. |
| **Accounting server port** | Radius authentication server port number (optional), 0-65535. |

| | | |
|---|---|---|
| **Primary accounting server** | Primary accounting server | Specify radius server as primary accounting server. |
| | Non-Primary accounting server | Specify radius server as non-primary accounting server. |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

# 26.2 TACACS server configuration

## 26.2.1 TACACS global configuration

TACACS global configuration module, the users in this module can configure the global TACACS function services.

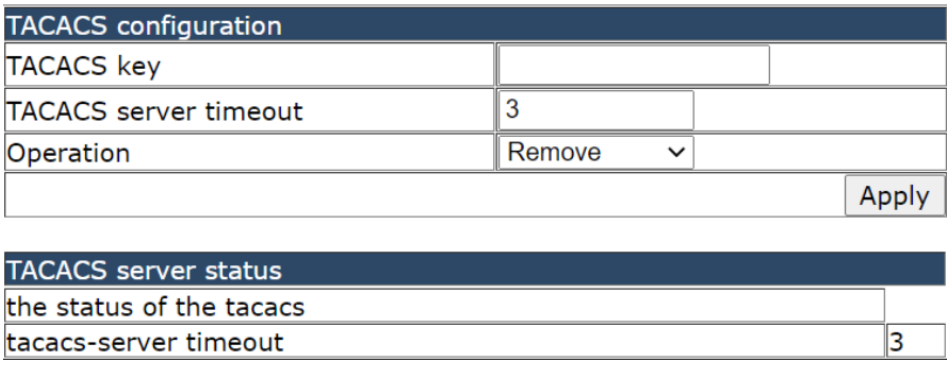



Figure 431.

| | | |
|---|---|---|
| **TACACS key** | TACACS authentication key, 1-16 characters. | |
| **TACACS server timeout** | TACACS authentication timeout, 1-60 seconds, default 3 seconds. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 26.2.2 TACACS server host configuration

TACACS server configuration module, the users in this module can configure the TACACS authentication server.

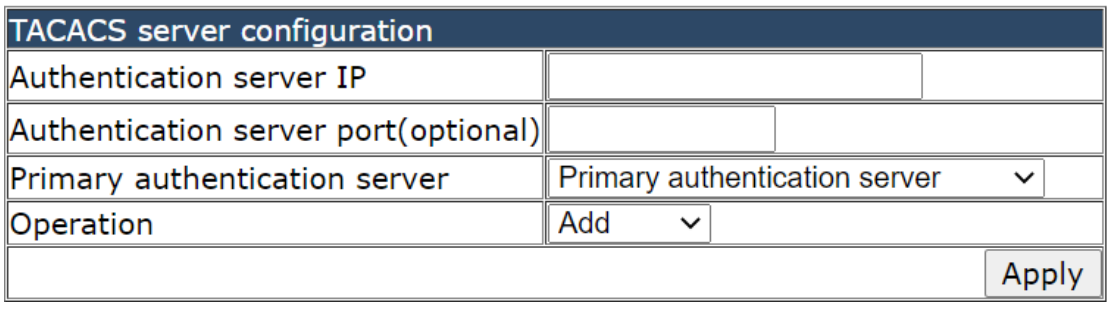



Figure 432.

| | | |
|---|---|---|
| **Authentication server IP** | TACACS authentication server IPv4 address, decimal point. | |
| **Authentication server port** | TACACS authentication server port number (optional), 0-65535. | |
| **Primary authentication server** | Primary accounting server | Specify TACACS server as primary accounting server. |
| | Non-Primary accounting server | Specify TACACS server as non-primary accounting server. |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

# 26.3 802.1x configuration

## 26.3.1 802.1x Global configuration

802.1x Global Configuration Module, the users in this module can configure the global 802.1x function services.

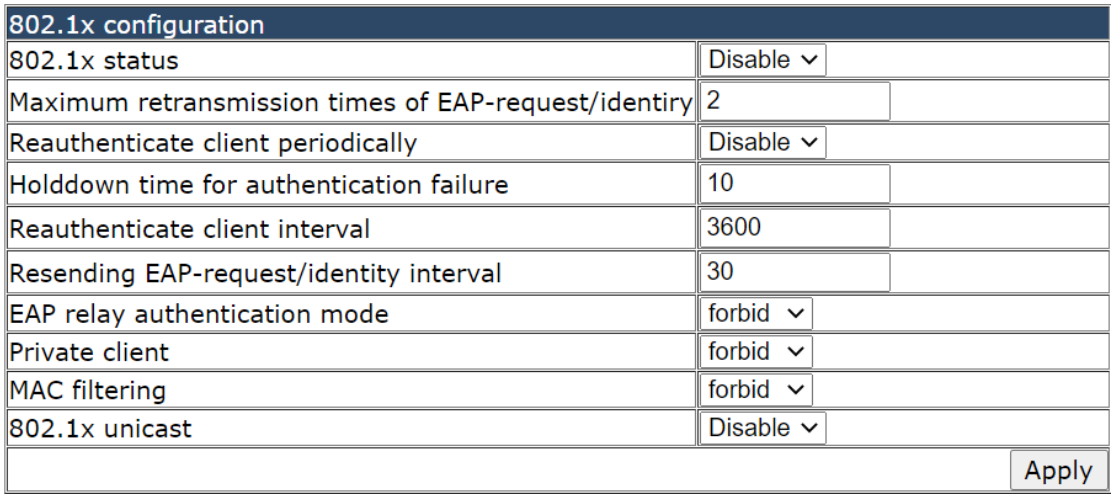



Figure 433.

| | |
|---|---|
| **802.1x status** | Boot or turn off 802.1x function. |
| **Maximum retransmission times of EAP-request/identiry** | Scope 1-10. |
| **Reauthenticate client periodically** | Start or close periodic recertification. |
| **Holddown time for authentication failure** | Range 1-65535 seconds, default 10 seconds. |
| **Reauthenticate client interval** | Range 1-65535 seconds, default 3600 seconds. |
| **Resending EAP-request/identity interval** | Range 1-65535 seconds, default 30 seconds. |

| | |
|---|---|
| **EAP relay authentication mode** | Ban or permit EAP relay authentication. |
| **Private client** | Prohibit or allow private clients. |
| **MAC filtering** | Ban or permit MAC address filtering. |
| **802.1x unicast** | Disable or enable 802.1x unicast teleport function. |

### 26.3.2 802.1x port authentication configuration

802.1x port authentication configuration module, in this module the users can configure the 802.1x function of the specified port.

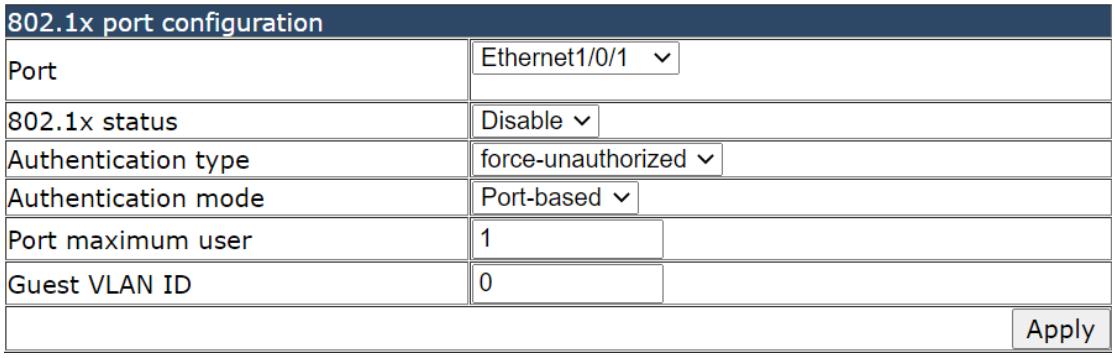



Figure 434.

| | | |
|---|---|---|
| **Port** | Designated port number. | |
| **802.1x status** | Boot or close 802.1x on this port. | |
| **Authentication type** | force-unauthorized | Mandatory unauthorized. |
| | force-authorized | Mandatory authorization. |
| | Auto (802.1x) | automatism (802.1x authorization). |
| **Authentication mode** | Port-based | Based on port. |
| | Mac-based | Based on MAC. |
| **Port maximum user** | Maximum number of users allowed to connect to the ports, 1-256, default 1. | |
| **Guest VLAN ID** | Guest VLAN, 0-4094, default 0. | |

### 26.3.3 802.1x port MAC configuration

802.1x port MAC configuration module, the users in this module can add or delete port 802.1x functions MAC specified ports.

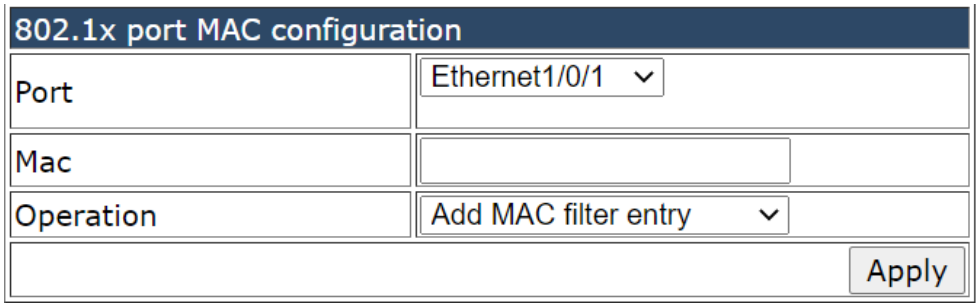



Figure 435.

| | |
|---|---|
| **Port** | Specifies the port number. |
| **MAC** | MAC address to operate. |
| **Operation** | Add or delete port MAC address filter table items. |

### 26.3.4 802.1x port status list

802.1x port MAC status list, the user can view 802.1 status information on x specified port and authenticate 802.1x in this module.

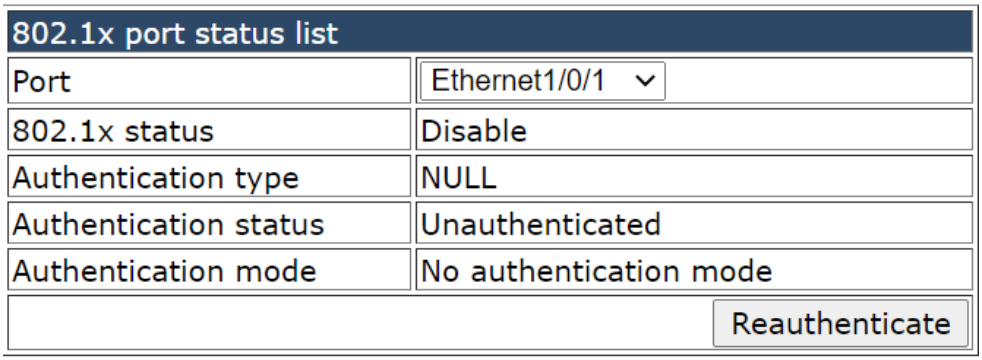



Figure 436.

## 26.4 MAB configuration

### 26.4.1 MAB ENABLE configuration

MAB enable configuration module, the users in this module can MAB the function of global enable and specified port enable operation.

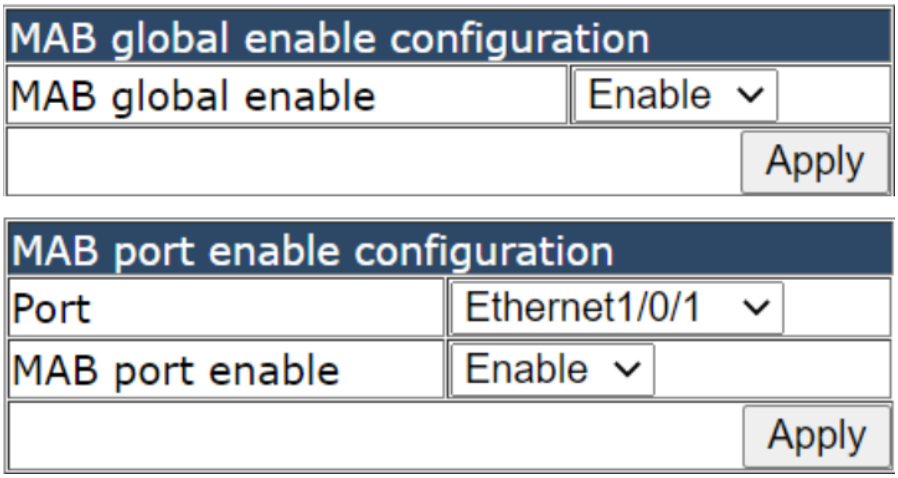



Figure 437.

| | |
|---|---|
| **MAB global enable** | Global enable or disable MAB function. |
| **Port** | Specifies the port number. |
| **MAB port enable** | Function on or off MAC specified port. |

### 26.4.2 MAB Authentication configuration

MAB user authentication configuration module, the users in this module can configure the MAB user authentication mode.

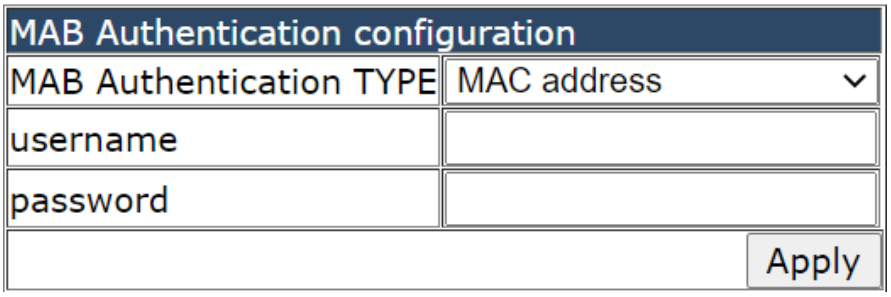



Figure 438.

| | | |
|---|---|---|
| **MAB Authentication TYPE** | Mac address | Authentication based on MAC address. |
| | Username and password | Authentication based on username and password (to be configured). |
| **username** | user name for authentication, 1-32 characters. | |
| **password** | password for authentication, 1-32 characters. | |

### 26.4.3 MAB parameter configuration

MAB parameter configuration module, the users in this module can configure the parameters of the MAB function.

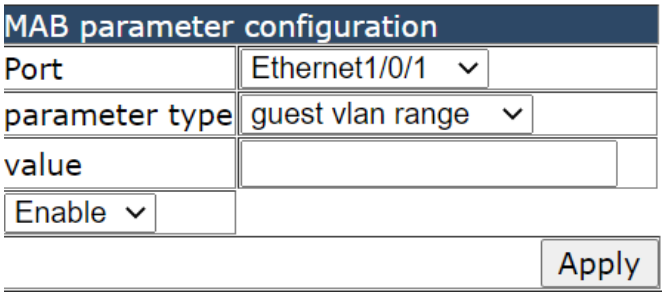



Figure 439.

| | | |
|---|---|---|
| **Port** | Specify port name. | |
| **parameter type** | Guest vlan range | VLAN operation for guest. |
| | Max binding value | Operation of maximum binding on ports. |
| **value** | After the parameter type is selected, the corresponding parameter value range can be set. | |
| **Enable\|Disable** | Boot or close port MAB parameter configuration. | |

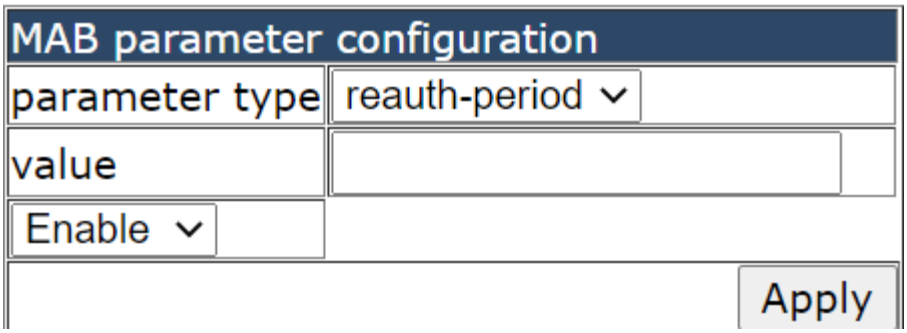



Figure 440.

| | | |
|---|---|---|
| **parameter type** | Reauth period | MAB time interval for re-authentication after failed authentication. |
| | Offline-detect | Detect the scan time of each port online status, 0 does not detect. |
| | Quiet-period | Configure the silence time after MAB authentication failure. |
| | Stale-period | Configure the time to delete bound users after the MAB port is closed. |
| | Linkup-period | Configure the restart time range after MAB port shutdown. |
| **value** | After the parameter type is selected, the corresponding parameter value can be set. | |
| **Enable\|Disable** | Boot or close global MAB parameter configuration. | |

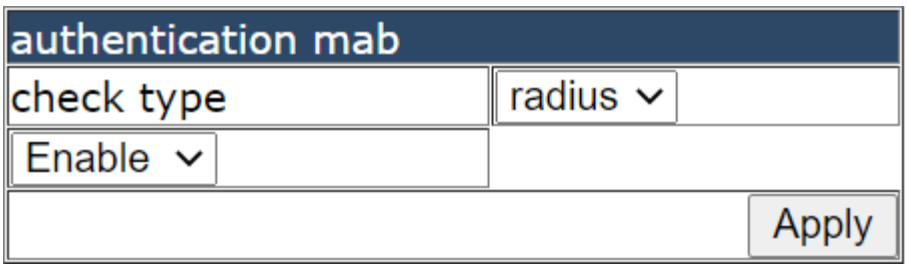



Figure 441.

| | |
|---|---|
| **Check type** | MAC address authentication uses radius or none to verify user login. |
| **Enable\|Disable** | Start or close validation mode configuration. |

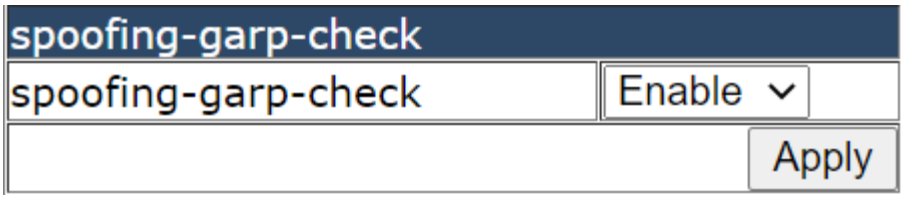



Figure 442.

| | |
|---|---|
| **spoofing-garp-check** | Activate or close check fake free ARP configuration. |

### 26.4.4 MAB show

MAB display module, the users can display mAb status of specified port or all ports in this module.

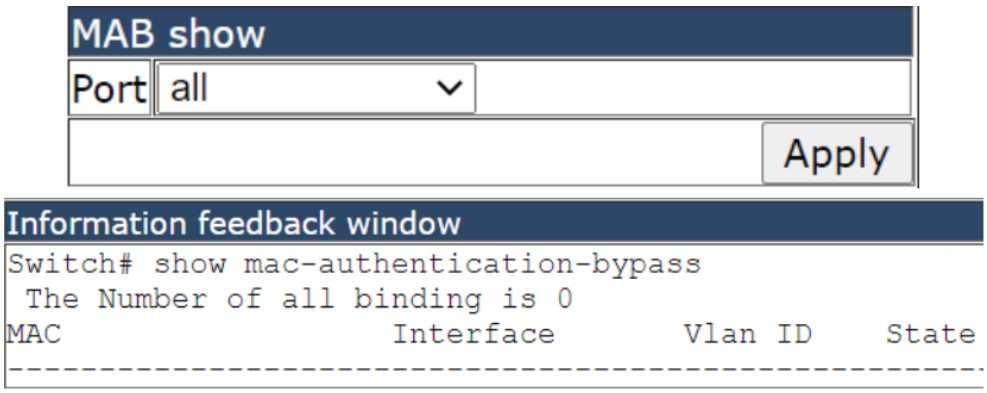



Figure 443.

| | |
|---|---|
| **Port** | Displays information MAB the specified port or all ports. |

# 27. PoE Config

# 27.1 PoE Global Config

## 27.1.1 PoE Global Config

This page can be used to globally configure PoE properties and view PoE global property information.

To display the “PoE Global Config” page, click PoE Config -> PoE Global Config -> PoE Global Config, click "Apply" to configure.

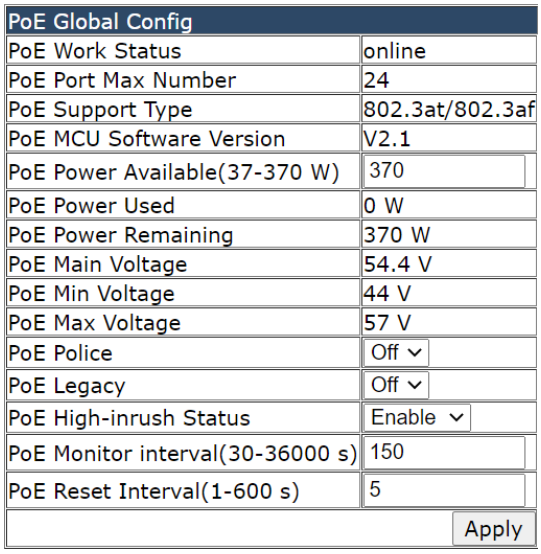



Figure 444.

| entry | describe |
|---|---|
| **PoE Power Available** | Maximum power supported by current switches. |
| **PoE Police** | Enable status of priority power supply policy:<br>Off: disable<br>On: enable |
| **PoE Legacy** | Current status of standard PD detection function:<br>Off: disable<br>On: enable |
| **PoE High-inrush Status** | Enable/Disable. |
| **PoE Monitor interval** | Check whether the PD connected to the current port is in the detection interval of normal communication, range: 30-36000 seconds. |
| **PoE Reset Interval** | Port reset time range: 1-600 per second. |

# 27.2 PoE Port Config

## 27.2.1 PoE Port Config

This page can be used to configure PoE properties under ports.

To display the “PoE Port Config” page, click PoE Config -> PoE Port Global Config -> PoE Port Config, click "Apply" to configure.

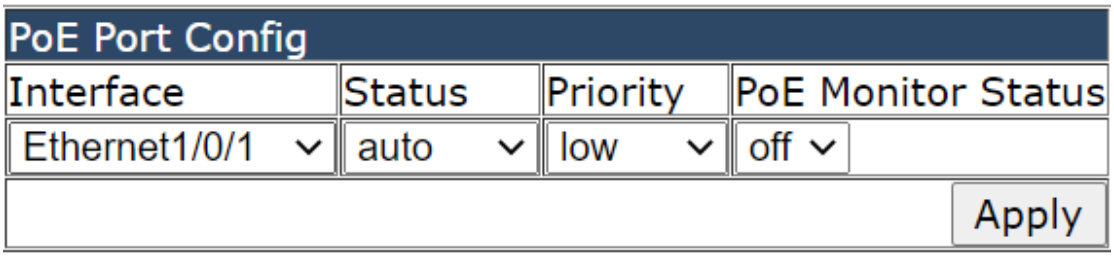



Figure 445.

| | |
|---|---|
| **entry** | describe |
| **Interface** | Current configured Ethernet ports. |
| **Status** | Auto: Normal power supply<br>Static: Forced power supply<br>Disable: No power supply |
| **Priority** | Low: low priority<br>High: high priority<br>Critical: highest priority |
| **PoE Monitor Status** | Off: Disable port monitoring<br>ON: Enable port monitoring |

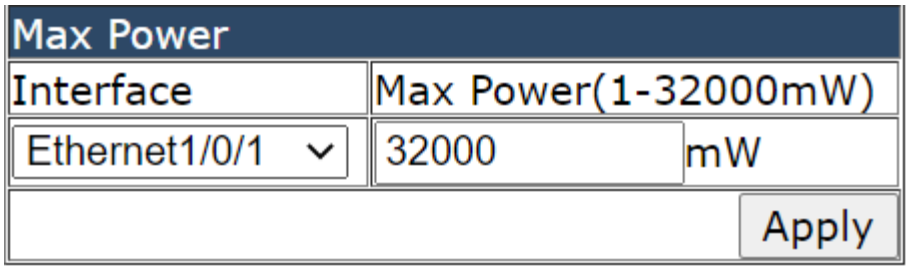
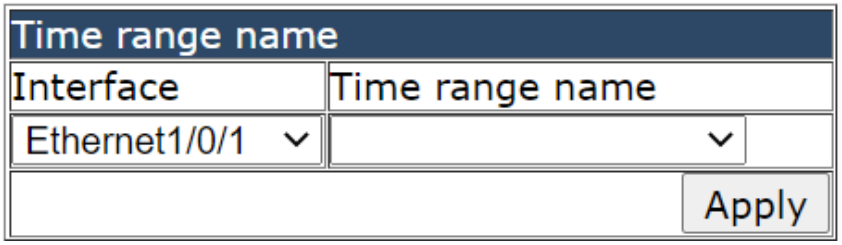



Figure 446.

| | |
|---|---|
| **entry** | describe |
| **Interface** | Current configured Ethernet ports. |
| **Max Power** | Sets the maximum output power supported by the current port, size range: 1-32000, unit mW; For example: 100, 200, 3000. |



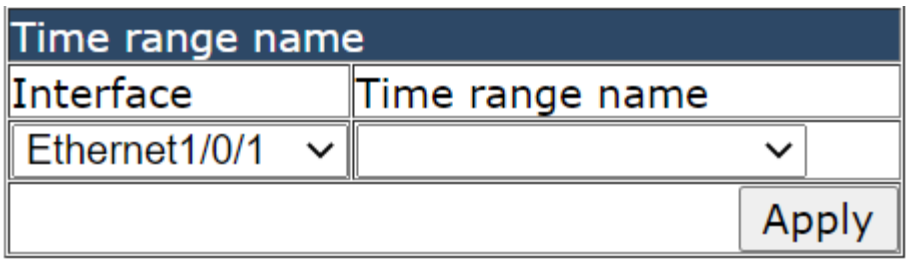



Figure 447.

| | |
|---|---|
| **entry** | describe |
| **Interface** | Current configured Ethernet ports. |
| **Time range name** | The time range name defined by the switch. |

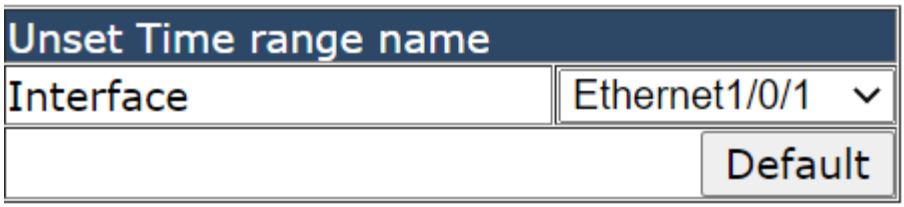



Figure 448.

| | |
|---|---|
| **entry** | describe |
| **Interface** | Current configured Ethernet ports. |
| **Default** | |

# 28. DOS attack protection configuration

## 28.1 Source IP equal destination IP DOS attack protection configuration

Source IP equal to destination IP anti DoS attack configuration module, the user can start or turn off the DOS attack function IP equal to the destination in this module.

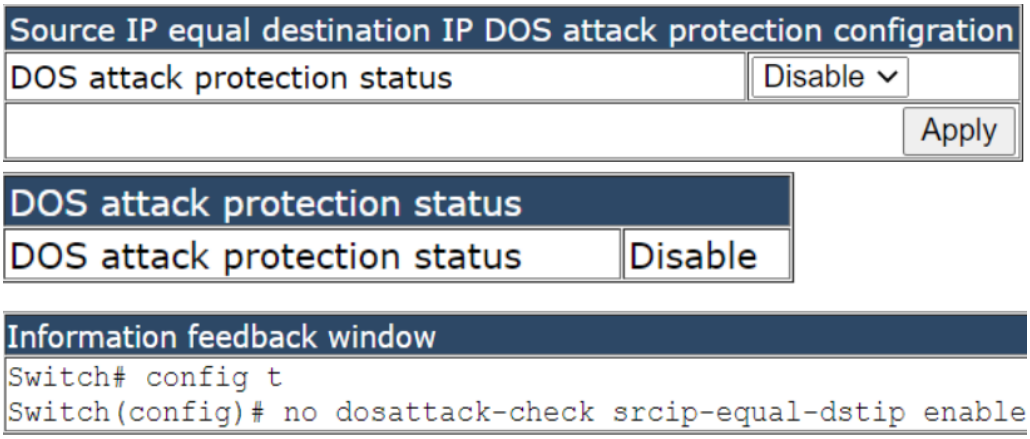


Figure 449.

## 28.2 Source port equal destination port DOS attack protection configuration

Source port equal to destination port anti DoS attack configuration module, the users in this module can start or close the source port equal to the destination port DOS attack function.

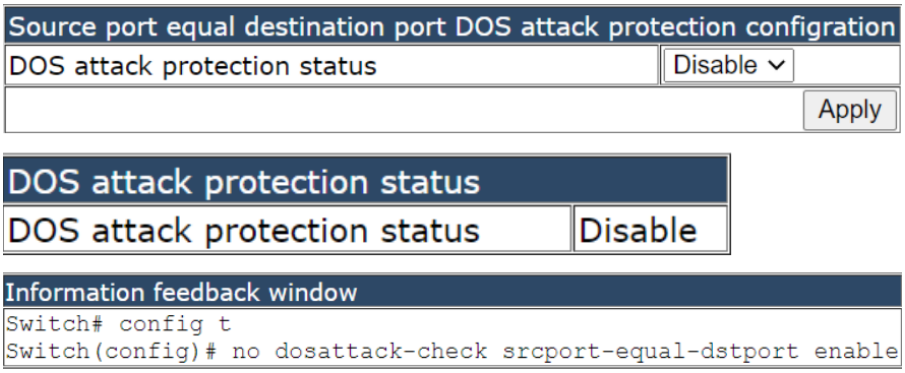



Figure 450.

## 28.3 TCP DOS attacks on invalid flags configuration

TCP DoS attack invalid flag bit configuration module, the users in this module can start or close the DOS attack function to check unauthorized TCP tags.

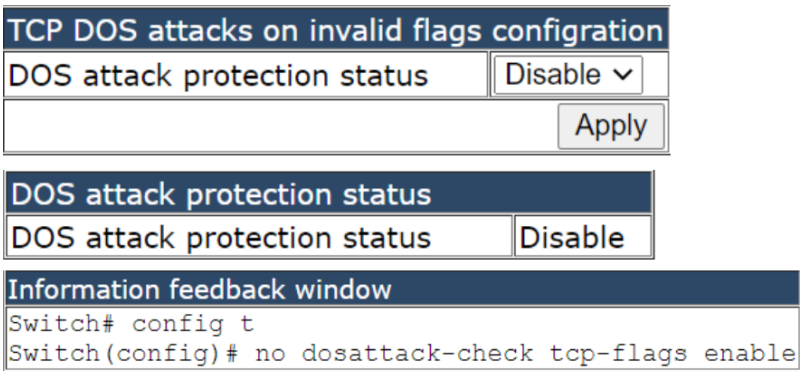



Figure 451.

## 28.4 ICMP DOS attack protection configuration

ICMP anti DoS attack configuration module, the user can start or turn off the DOS attack check function of the anti-ICMP fragment in this module.

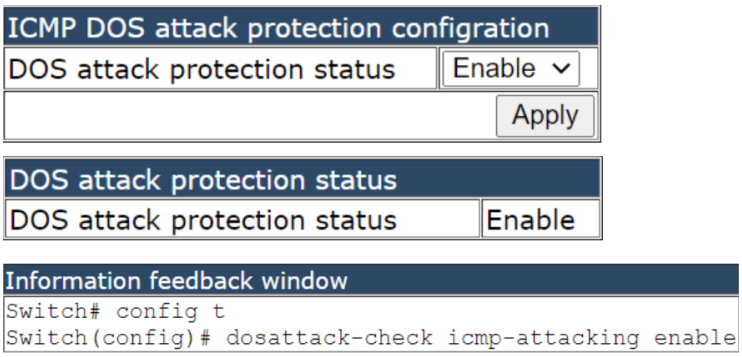


Figure 452.

## 28.5 ICMP packet-size configuration

The maximum ICMP message configuration module is allowed, the users can configure the maximum net length of icmpv4 packets in this module.

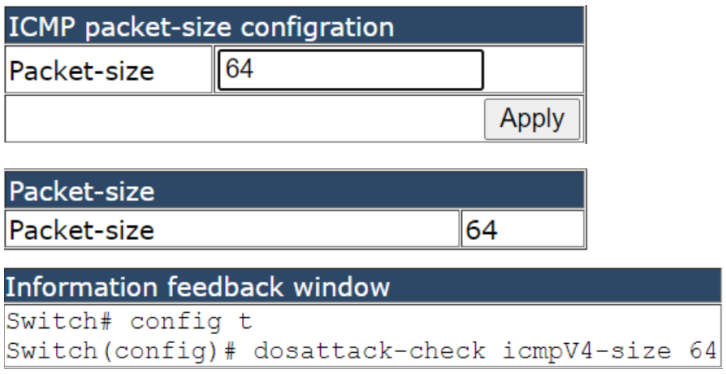



Figure 453.

| | |
|---|---|
| **Packet-size** | Maximum net length of allowed ICMPv4 packets, 64-1023, default 512. |

## 28.6 First fragment IP packet DOS attack protection configuration

The first IP packet fragment anti DoS attack configuration module, the user can start or turn off the DOS attack function against the first IP message fragment in this module.

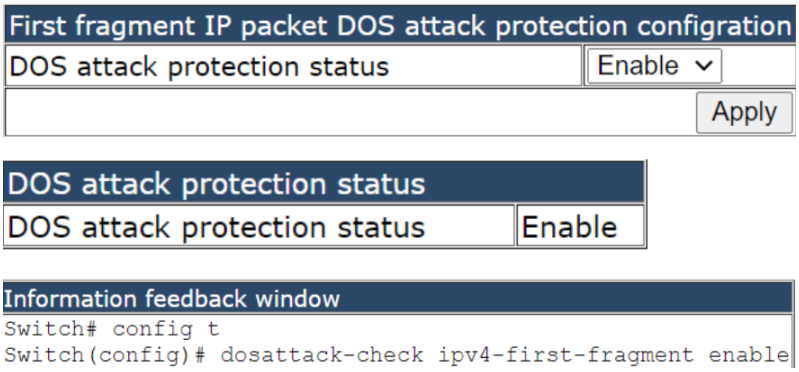



Figure 454.

# 29. SSL config

## 29.1 IP HTTP server configuration

HTTP server configuration module, the user can start or stop the HTTP service of the switch by using this module again.

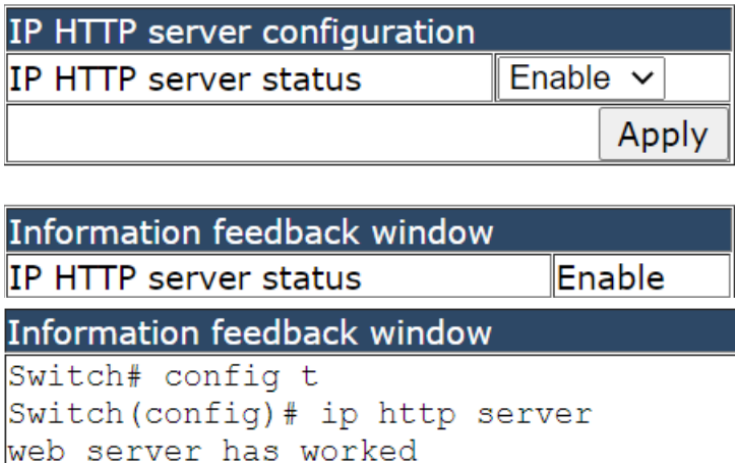



Figure 455.

## 29.2 SSL global configuration

SSL function switch configuration module, the users in this module can start or close the switch SSL service function.

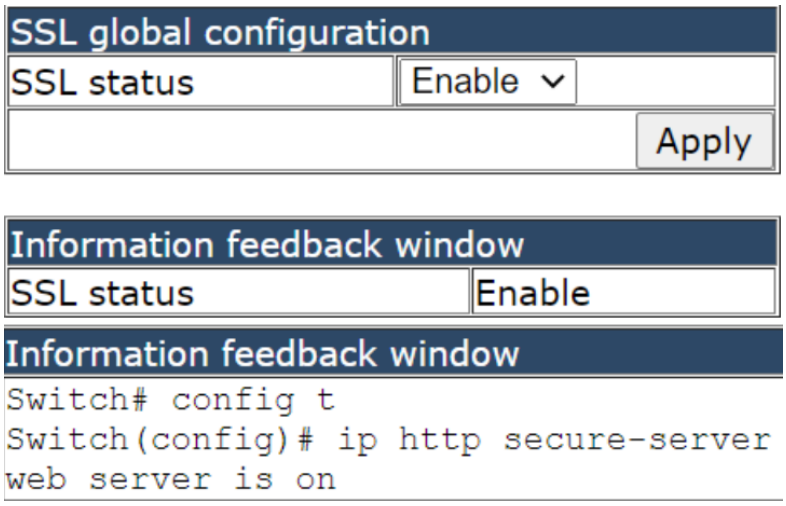



Figure 456.

## 29.3 SSL server monitor port configuration

SSL server monitor port number start configuration module, the users can configure SSL server listening port number in this module.

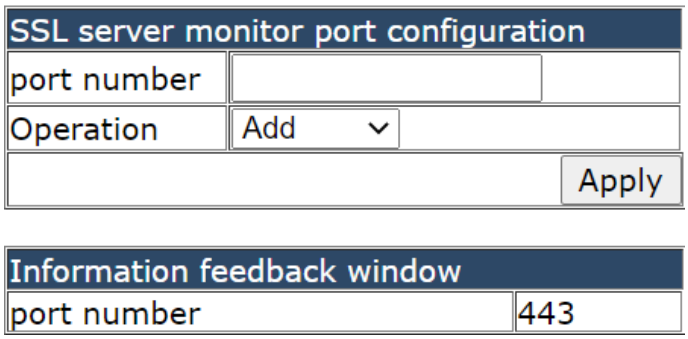



Figure 457.

| | | |
|---|---|---|
| **Port** | Specifies the port number. | |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

## 29.4 SSL secure-ciphersuite configuration

SSL encryption suite configuration module, the users can configure the encryption suite type of SSL service in this module.

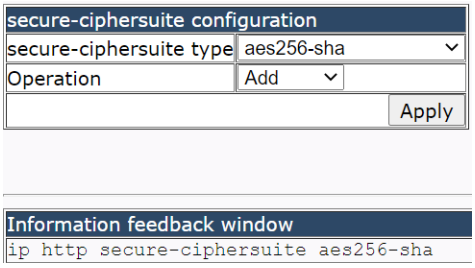



Figure 458.

| | | |
|---|---|---|
| **secure-ciphersuite type** | aes256-sha | aes256-sha encryption is used. |
| | ecdhe-rsa-aes256-sha | ecdhe-rsa-aes256-sha encryption is used. |
| **Operation** | Add | Add operations. |
| | Remove | Delete operations. |

# 30. sFlow configuration

## 30.1 sFlow collector global address configuration

This page can be used to configure the global sFlow analyzer address.

To display the “sFlow collector global address configuration” page, sFlow configuration -> sFlow collector global address configuration, click “Apply” to configure.

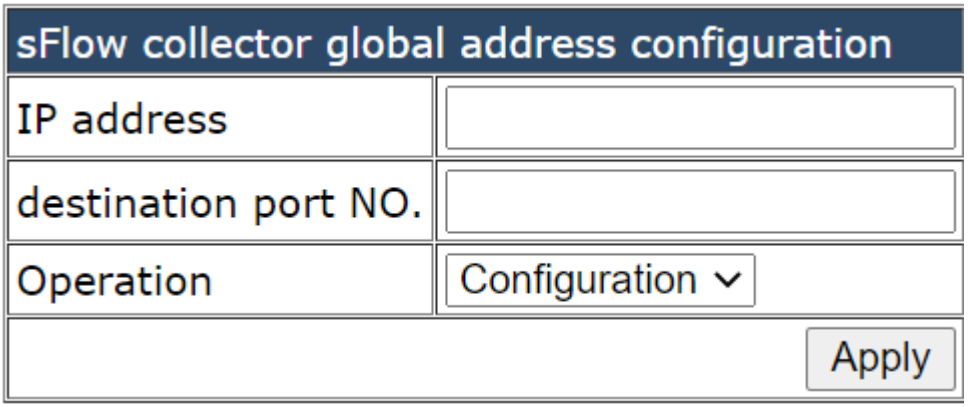



Figure 459.

| | |
|---|---|
| **entry** | describe |

| | |
|---|---|
| **IP address** | sFlow Analyzer Address. |
| **destination port NO.** | Range between 1025 and 65535. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.2 sFlow collector port address configuration

This page can be used to configure port sFlow analyzer address.

To display the “sFlow collector port address configuration” page, sFlow configuration -> sFlow collector port address configuration, click “Apply” to configure.

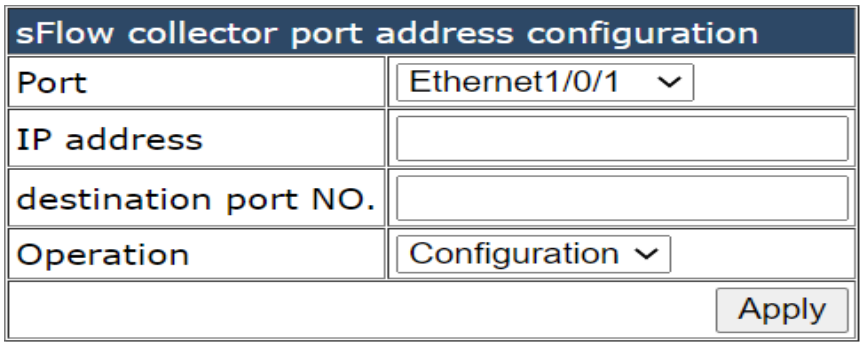



Figure 460.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port number. |
| **IP address** | sFlow Analyzer Address. |
| **destination port NO.** | Range between 1025 and 65535. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.3 sFlow agent address configuration

This page can be used for sFlow agent configuration.

To display the “sFlow agent address configuration” page, sFlow configuration -> sFlow agent address configuration, click “Apply” to configure.

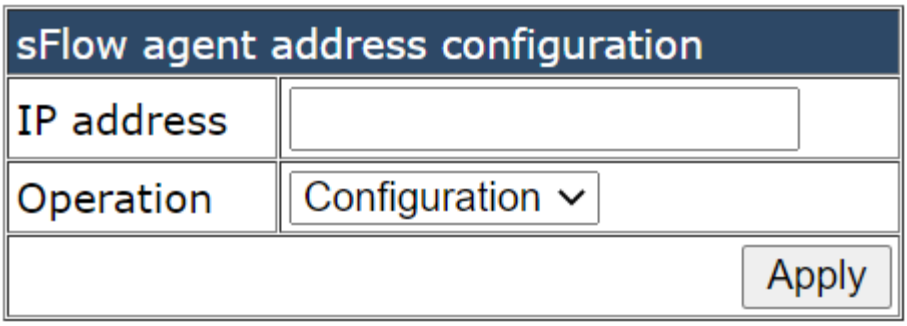



Figure 461.

| | |
|---|---|
| **entry** | describe |
| **IP address** | sFlow agent address. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.4 sFlow priority configuration

This command is used to set the priority of the sample message.

To display the “sFlow priority configuration” page, sFlow configuration -> sFlow priority configuration, click “Apply” to configure.

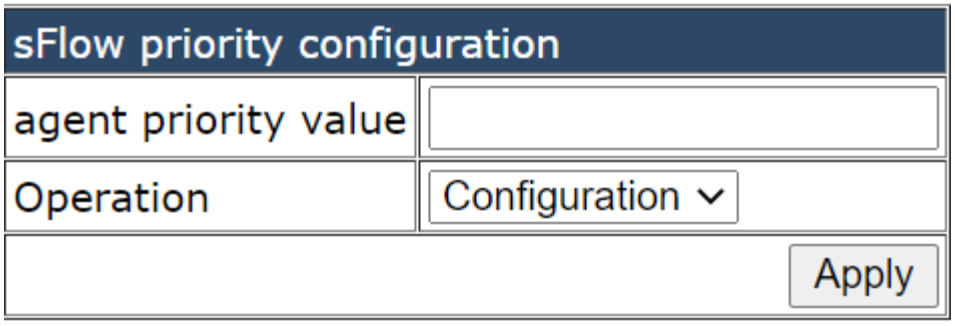



Figure 462.

| | |
|---|---|
| **entry** | describe |
| **agent priority value** | Range: 0-3. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.5 sFlow header length configuration

This page can be used to configure the length of header packets copied in sFlow data sampling.

To display the “sFlow header length configuration” page, sFlow configuration -> sFlow header length configuration, click “Apply” to configure.

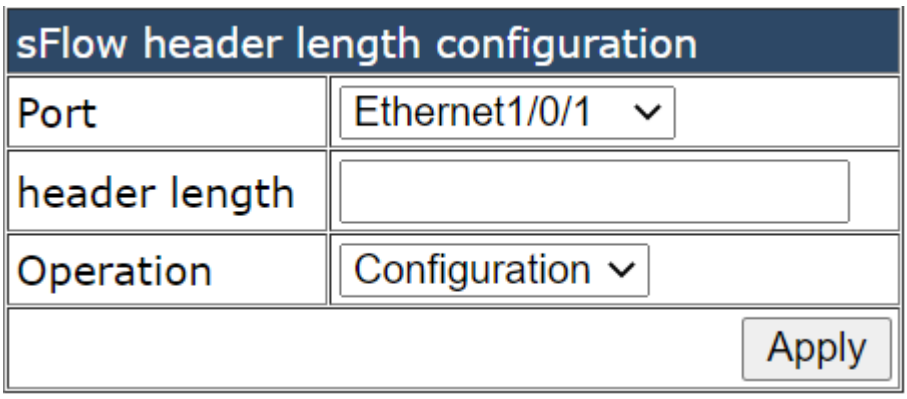



Figure 463.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **header length** | Length range: 32-256. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.6 sFlow data length configuration

This page is used to configure sflow packet length.

To display the “sFlow header length configuration” page, sFlow configuration -> sFlow data length configuration, click “Apply” to configure.

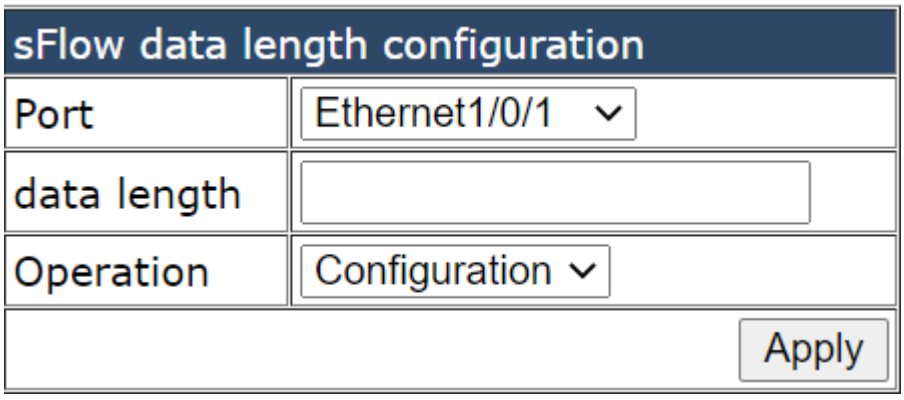



Figure 464.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **data length** | Length range: 500-1470. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default: |

| | |
|---|---|
| | Restore default configuration, default value is 1400. |

## 30.7 sFlow rate configuration

This page can be used to configure port hardware sampling rates.

To display the “sFlow rate configuration” page, sFlow configuration -> sFlow rate configuration, click “Apply” to configure.

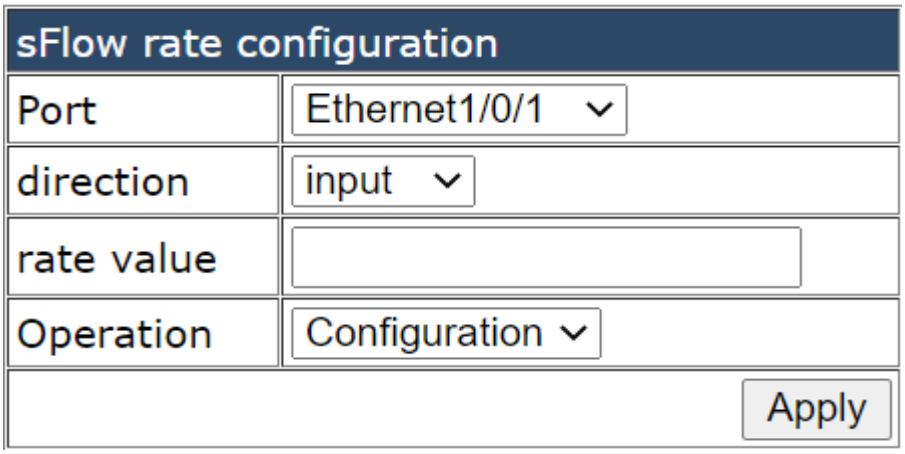



Figure 470.

| | |
|---|---|
| **entry** | describe |
| **Port** | Ethernet port name. |
| **direction** | Input: receive data.<br>Output: send data. |
| **rate value** | Rate range: 1000-16383500. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.8 sFlow counter interval configuration

This page can be used to configure sFlow statistical sampling intervals.

To display the “sFlow counter interval configuration” page, sFlow configuration -> sFlow counter interval configuration, click “Apply” to configure.

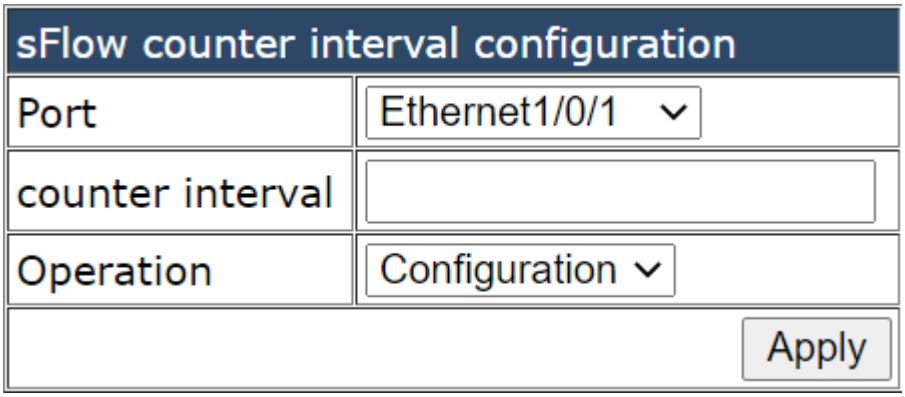



Figure 466.

| entry | describe |
|---|---|
| **Port** | Ethernet port name. |
| **counter interval** | Sampling interval range: 20-120. |
| **Operation** | Configuration:<br>User self-configuration.<br>Default:<br>Restore default configuration. |

## 30.9 sFlow analyzer configuration

This page can be used for globally enabled sFlow analyzers.

To display the “sFlow analyzer configuration” page, sFlow configuration -> sFlow analyzer configuration, click “Apply” to configure.

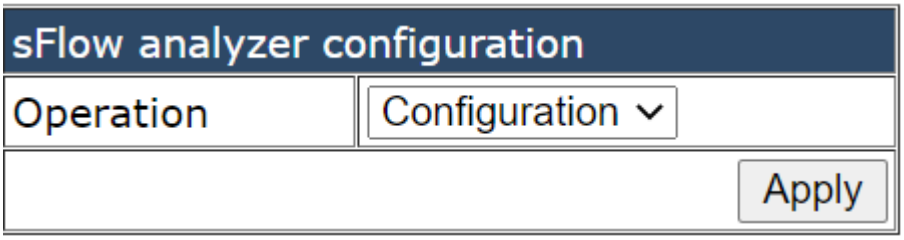



Figure 467.

| entry | describe |
|---|---|
| **Operation** | Configuration: Function Enable.<br>Remote: Function disabled. |

# 31. IPv6 security ra configuration

## 31.1 IPv6 security ra global configuration

Launch the global IPv6 security RA module, the user can start or close the global IPv6 security RA function in this module.

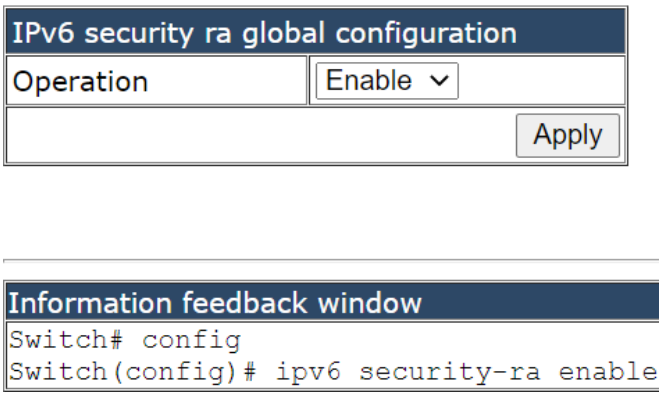



Figure 468.

## 31.2 IPv6 security ra port configuration

Start port IPv6 security RA module, the user can start or close the security RA function IPv6 the specified port in this module.

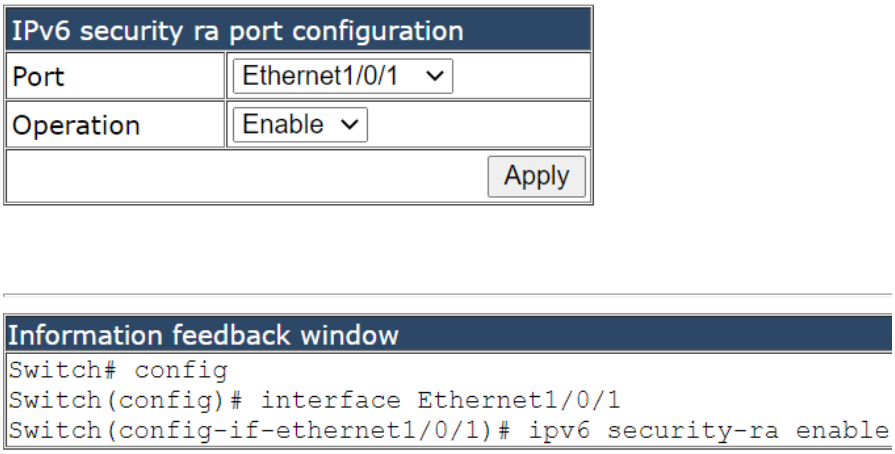



Figure 469.

| | | |
|---|---|---|
| **Port** | Specifies the port number. | |
| **Operation** | Enable | Start operation. |
| | Disable | Close operation. |

## 31.3 show IPv6 security ra

Show IPv6 security RA configuration module, the user can display the specified port or global IPv6 security RA function configuration information in this module.

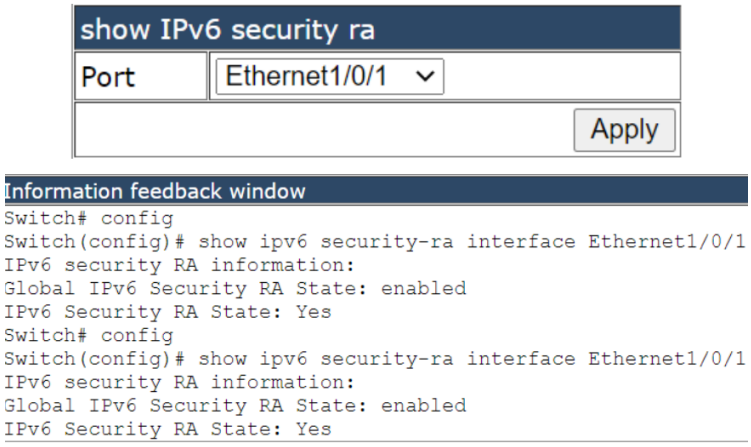



Figure 470.

| | |
|---|---|
| **Port** | Specifies the port number ALL represents all. |

# 32. Device log message

## 32.1 Show device log message

View device log information module, where the users can view system key logs and warning logs.

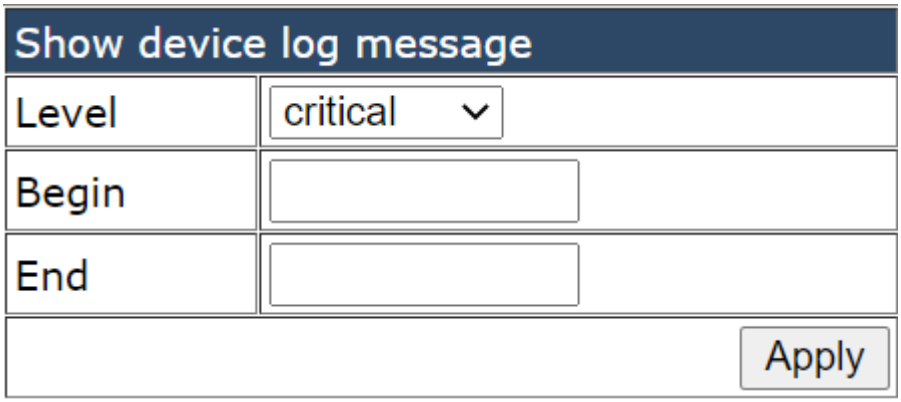



Figure 471.

| | | |
|---|---|---|
| **Level** | critical | Key-level log information. |
| | warnings | Warning Level Log Information. |
| **Begin** | To see where the log information starts. | |
| **End** | To see the end location of the log information. | |

## 32.2 Clear logging in logbuff channel

Clears all log message modules in the buffer, the users in this module can clear all log messages in the buffer.

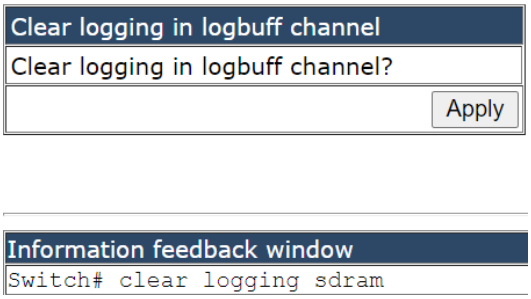

Clear logging in logbuff channel
Clear logging in logbuff channel?
Apply
Information feedback window
Switch# clear logging sdram

Figure 472.