SUNDRAY

User Guide

用户手册

SW-5024 v2.0

REV2.0.0

1910020821

CONTENTS

Package Contents

The following items should be found in your box:

- One 24-Port Gigabit Managed PoE Switch with 4 SFP Slots
- One Power Cord
- One Console Cable
- One USB Cable
- One Ground Cable
- Two mounting brackets and other fittings
- Installation Guide
- Resource CD for SW-5024, including:
  - This User Guide
  - CLI Reference Guide
  - 802.1X Client Software
  - USB Console Driver
  - Other Helpful Information

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1 About this Guide

This User Guide contains information for setup and management of SW-5024 24-Port Gigabit Managed PoE Switch with 4 SFP Slots. Please read this guide carefully before operation.

1.1 Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

1.2 Conventions

When using this guide, please notice that features of the switch may vary slightly depending on the model and software version you have, and on your location, language, and Internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

In this Guide the following conventions are used:

- The switch or the device mentioned in this Guide stands for SW-5024 24-Port Gigabit Managed PoE Switch with 4 SFP Slots without any explanation.
- **Menu Name→Submenu Name→Tab page** indicates the menu structure. **System→System Info→System Summary** means the System Summary page under the System Info menu option that is located under the System menu.
- **Bold font** indicates a button, a toolbar icon, menu or menu item.

Symbols in this Guide:

Symbol	Description
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	This format indicates important information that helps you make better use of your device.

More Info:

- The Installation Guide (IG) can be found where you find this guide or inside the package of the switch.

1.3 Overview of This Guide

Chapter	Introduction
Chapter 1 About This Guide	Introduces the guide structure and conventions.
Chapter 2 Introduction	Introduces the features, application and appearance of SW-5024 switch.
Chapter 3 Login to the Switch	Introduces how to log on to the Web management page.
Chapter 4 System	This module is used to configure system properties of the switch. Here mainly introduces: ● System Info: Configure the description, system time and network parameters of the switch. ● User Management: Configure the user name and password for users to log on to the Web management page with a certain access level. ● System Tools: Manage the configuration file of the switch. ● Access Security: Provide different security measures for the login to enhance the configuration management security. ● SDM Template: Manage the hardware TCAM resources.
Chapter 5 Switching	This module is used to configure basic functions of the switch. Here mainly introduces: ● Port: Configure the basic features for the port. ● LAG: Configure Link Aggregation Group. LAG is to combine a number of ports together to make a single high-bandwidth data path. ● Traffic Monitor: Monitor the traffic of each port. ● MAC Address: Configure the address table of the switch. ● L2TP: Configure the Layer 2 Tunneling Protocol feature.

Chapter	Introduction
Chapter 6 VLAN	This module is used to configure VLANs to control broadcast in LANs. Here mainly introduces: ● 802.1Q VLAN: Configure port-based VLAN. ● MAC VLAN: Configure MAC-based VLAN without changing the 802.1Q VLAN configuration. ● Protocol VLAN: Create VLANs in application layer to make some special data transmitted in the specified VLAN. ● VLAN VPN: VLAN VPN allows the packets with VLAN tags of private networks to be encapsulated with VLAN tags of public networks at the network access terminal of the Internet Service Provider. ● GVRP: GVRP allows the switch to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other switches, without having to individually configure each VLAN. ● Private VLAN: Designed to save VLAN resources of uplink devices and decrease broadcast. Private VLAN mainly used in campus or enterprise networks to achieve user layer-2-separation and to save VLAN resources of uplink devices.
Chapter 7 Spanning Tree	This module is used to configure spanning tree function of the switch. Here mainly introduces: ● STP Config: Configure and view the global settings of spanning tree function. ● Port Config: Configure CIST parameters of ports. ● MSTP Instance: Configure MSTP instances. ● STP Security: Configure protection function to prevent devices from any malicious attack against STP features.
Chapter 8 Ethernet OAM	This module is used to configure Ethernet OAM function of the switch. Here mainly introduces: ● Basic Config: Enable the Ethernet OAM function, configure its OAM mode, and check out the connection status. ● Link Monitoring: Configure the parameters about OAM link events and choose whether to notify the link event. ● RFI: Choose whether to notify the link faults like dying gasp and critical event. ● Remote Loopback: Start or stop the remote loopback; choose to ignore or to process the received remote loopback request. ● Statistics: View the statistics about the detailed Ethernet OAM traffic information and event log information. ● DLDP: Configure the DLDP function to allow the switch to monitor the physical configuration of the cables and detect whether a unidirectional link exists.

Chapter	Introduction
Chapter 9 Multicast	This module is used to configure multicast function of the switch. Here mainly introduces: ● IGMP Snooping: Configure global parameters of IGMP Snooping function, port properties, VLAN and multicast VLAN. ● MLD Snooping: Configure global parameters of MLD Snooping function, port properties, VLAN and multicast VLAN. ● Multicast Table: View the information of IPv4 and IPv6 multicast groups already on the switch.
Chapter 10 Routing	The module is used to configure several IPv4 unicast routing protocols. Here mainly introduces: ● Interface: Configure and view different types of interfaces: VLAN, loopback, routed port and port-channel interface. ● Routing table: Displays the routing information summary. ● Static Routing: Configure and view static routes. ● DHCP Server: Configure DHCP server. ● DHCP Relay: Configure DHCP relay. ● ARP: Displays the ARP information.
Chapter 11 QoS	This module is used to configure QoS function to provide different quality of service for various network applications and requirements. Here mainly introduces: ● DiffServ: Configure priorities, port priority, 802.1P priority and DSCP priority. ● Bandwidth Control: Configure rate limit feature to control the traffic rate on each port; configure storm control feature to filter broadcast, multicast and UL frame in the network. ● Voice VLAN: Configure voice VLAN to transmit voice data stream within the specified VLAN so as to ensure the transmission priority of voice data stream and voice quality.
Chapter 12 PoE	This module is used to configure the PoE function for the switch to supply power for PD devices. Here mainly introduces: ● PoE Config: Configure PoE function globally. ● PoE Time-Range: Configure the effective time for PoE port to supply power.

Chapter	Introduction
Chapter 13 ACL	This module is used to configure match rules and process policies of packets to filter packets in order to control the access of the illegal users to the network. Here mainly introduces: ● Time-Range: Configure the effective time for ACL rules. ● ACL Config: ACL rules. ● Policy Config: Configure operation policies. ● ACL Binding: Bind the ACL to a port/VLAN to take its effect on a specific port/VLAN. ● Policy Binding: Bind the policy to a port/VLAN to take its effect on a specific port/VLAN.
Chapter 14 Network Security	This module is used to configure the protection measures for the network security. Here mainly introduces: ● IP-MAC Binding: Bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together. ● IPv6-MAC Binding: Bind the IPv6 address, MAC address, VLAN ID and the connected Port number of the Host together. ● DHCP Snooping: DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding. ● DHCPv6 Snooping: DHCPv6 Snooping functions to monitor the process of the Host obtaining the IPv6 address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding. ● ARP Inspection: Configure ARP inspection feature to prevent the network from ARP attacks. ● ND Detection: Configure ND detection feature to prevent the network from ND attacks. ● IP Source Guard: Configure IP source guard feature to filter IP packets in the LAN. ● DoS Defend: Configure DoS defend feature to prevent DoS attack. ● 802.1X: Configure common access control mechanism for LAN ports to solve mainly authentication and security problems. ● PPPoE: Configure the PPPoE ID insertion feature. ● AAA: Configure the authentication, authorization and accounting features.

Chapter	Introduction
Chapter 15 SNMP	This module is used to configure SNMP function to provide a management frame to monitor and maintain the network devices. Here mainly introduces: ● SNMP Config: Configure global settings of SNMP function. ● Notification: Configure notification function for the management station to monitor and process the events. ● RMON: Configure RMON function to monitor network more efficiently.
Chapter 16 LLDP	This module is used to configure LLDP function to provide information for SNMP applications to simplify troubleshooting. Here mainly introduces: ● Basic Config: Configure the LLDP parameters of the device. ● Device Info: View the LLDP information of the local device and its neighbors. ● Device Statistics: View the LLDP statistics of the local device. ● LLDP-MED: Configure the LLDP-MED features.
Chapter 17 Maintenance	This module is used to assemble the commonly used system tools to manage the switch. Here mainly introduces: ● System Monitor: Monitor the memory and CPU of the switch. ● Log: View configuration parameters on the switch. ● Device Diagnostics: Test the connection status of the cable connected to the switch, test if the port of the switch and the connected device are available. ● Network Diagnostics: Test if the destination is reachable and the account of router hops from the switch to the destination.
Appendix A Password Recovery	Introduces the procedure to reset passwords on switches.
Appendix B Specifications	Lists the hardware specifications of the switch.
Appendix C 802.1X Clinet Software	Introduces how to use 802.1X Client Software provided for authentication.

Return to CONTENTS

Chapter 2 Introduction

Thanks for choosing the SW-5024 24-Port Gigabit Managed PoE Switch with 4 SFP Slots!

2.1 Overview of the Switch

Designed for workgroups and departments, SW-5024 provides wire-speed performance and full set of L2 and L2+ management features. It provides a variety of service features and multiple powerful functions with high security.

The EIA-standardized framework and smart configuration capacity can provide flexible solutions for a variable scale of networks. Static routing allows devices in different VLANs/subnets to communicate with each other in an IPv4/IPv6 network. OAM, L2TP and sFlow can meet the requirement of large ISP customers. ACL, 802.1x and Dynamic ARP Inspection provide robust security strategies. QoS and IGMP snooping/filtering optimize voice and video application. Link aggregation (LACP) increases aggregated bandwidth, optimizing the transport of business critical data. SNMP, RMON, WEB and CLI Log-in bring abundant management policies. L2 Managed Switch integrates multiple functions with excellent performance, and is friendly to manage, which can fully meet the need of the users demanding higher networking performance.

2.2 Appearance Description

2.2.1 Front Panel

The front panel of SW-5024 is shown as Figure 2-1.

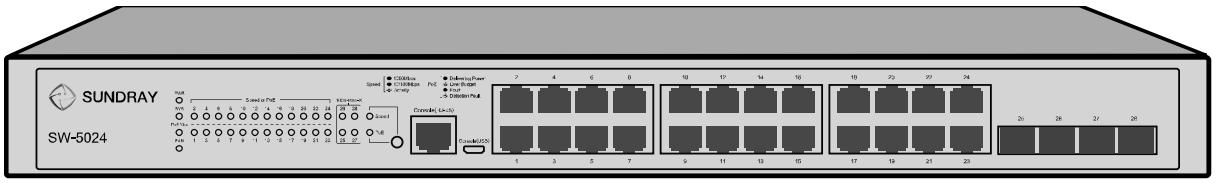


Figure 2-1 Front Panel of SW-5024

SW-5024 has an LED mode switch button which is for switching the LED status indication. When the Speed LED is on, the port LED is indicating the data transmission rate. When the PoE LED is on, the port LED is indicating the power supply status. By default the Speed LED is on. Pressing the mode switch button, the Speed LED will turn off and the PoE LED will light up. Then the PoE LED will turn off after being on for 60 seconds and the Speed LED will light up again.

When the Speed LED is on, the port LED is indicating the data transmission status.

- **LEDs**

Name	Status	Indication
PWR	On	The switch is powered on.
	Off	The switch is powered off or power supply is abnormal.

Name	Status		Indication
	Flashing		Power supply is abnormal.
SYS	Flashing		The switch works properly.
	On/Off		The switch works improperly.
FAN	Green		All the fans work properly.
	Yellow		Not all the fans work properly.
	Off		The switch works improperly.
Speed or PoE (Port 1-24）	Green	On	A 1000Mbps device is connected to the corresponding port but no activity.
		Flashing	A 1000Mbps device is connected to the corresponding port and data is being transmitted or received.
	Yellow	On	A 10/100Mbps device is connected to the corresponding port but no activity.
		Flashing	A 10/100Mbps device is connected to the corresponding port and data is being transmitted or received.
	Off		No device is connected to the corresponding port.
1000Base-X (Port 25-28)	On		There is a device linked to the corresponding SFP port but no activity.
	Flashing		The corresponding SFP port is transmitting or receiving data.
	Off		There is no device linked to the corresponding SFP port.

When the PoE LED is on, the port LED is indicating the power supply status.

- **LEDs**

Name	Status	Indication
PWR	On	The switch is powered on.
	Off	The switch is powered off or power supply is abnormal.
	Flashing	Power supply is abnormal.
SYS	Flashing	The switch works properly.
	On/Off	The switch works improperly.
PoE Max	On	The remaining PoE power≤7W.
	Flashing	The remaining PoE power keeps≤7W after this LED is on for 2 minutes.
	Off	The remaining PoE power＞7W.

Name	Status		Indication
FAN	Green		All the fans work properly.
	Yellow		Not all the fans work properly.
	Off		The switch works improperly.
Speed or PoE (Port 1-24）	Green	On	The port is supplying power normally.
		Flashing	The supply power exceeds the correponding port's maximum power.
	Yellow	On	Overload or short circuit is detected.
		Flashing	Power-on self-test has failed.
	Off		Not providing PoE power on the port.
1000Base-X (Port 25-28)	On		There is a device linked to the corresponding SFP port but no activity.
	Flashing		The corresponding SFP port is transmitting or receiving data.
	Off		There is no device linked to the corresponding SFP port.

- **Console (RJ-45) Port**

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

- **Console (USB) Port**

Designed to connect with the USB port of a computer for monitoring and configuring the switch. The switch has an RJ-45 console port and a micro-USB console port available. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector. If you are using the switch's Micro-USB console port with the USB port of a Windows PC, a driver for the USB port must be installed manually. The USB driver, named as 'USB Console Driver.exe', is provided on the resource CD.

- **10/100/1000Mbps RJ45 Port**

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each 10/100/1000Mbps RJ45 port has a corresponding 10/100/1000Mbps LED.

- **SFP Port**

Designed to install the SFP module. **SW-5024** features 4 individual SFP ports and supports 1000M SFP module connection only.

- **Port Feature**

Model	10/100/1000Mbps RJ45 Port	SFP Port	Console Port
SW-5024	24	4	2

2.2.2 Rear Panel

The rear panel of SW-5024 features a Kensington security slot, a Grounding Terminal (marked with⏚) and a power socket.

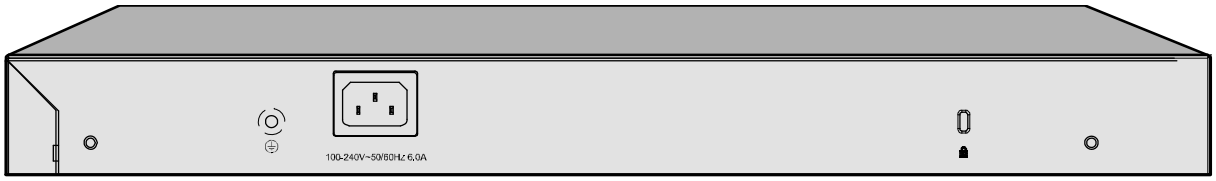


Figure 2-2 Rear Panel

- **Kensington Security Slot:** Secure the lock (not provided) into the security slot to prevent the device from being stolen.
- **Grounding Terminal:** The switch already comes with lightning protection mechanism. You can also ground the switch through the PE (Protecting Earth) cable of AC cord or with Ground Cable.
- **AC Power Socket:** Connect the female connector of the power cord here, and the male connector to the AC power outlet.

Return to CONTENTS

Chapter 3 Login to the Switch

3.1 Login

1) To access the configuration utility, open a web-browser and type in the default address http://192.168.0.1 in the address field of the browser, then press the **Enter** key.

Figure 3-1 Web-browser

Tips:

To log in to the switch, the IP address of your PC should be set in the same subnet addresses of the switch. The IP address is 192.168.0.x ("x" is any number from 2 to 254), Subnet Mask is 255.255.255.0.

2) After a moment, a login window will appear, as shown in Figure 3-2. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Login** button or press the **Enter** key.

Figure 3-2 Login

3.2 Configuration

After a successful login, the main page will appear as Figure 3-3, and you can configure the function by clicking the setup menu on the left side of the screen.

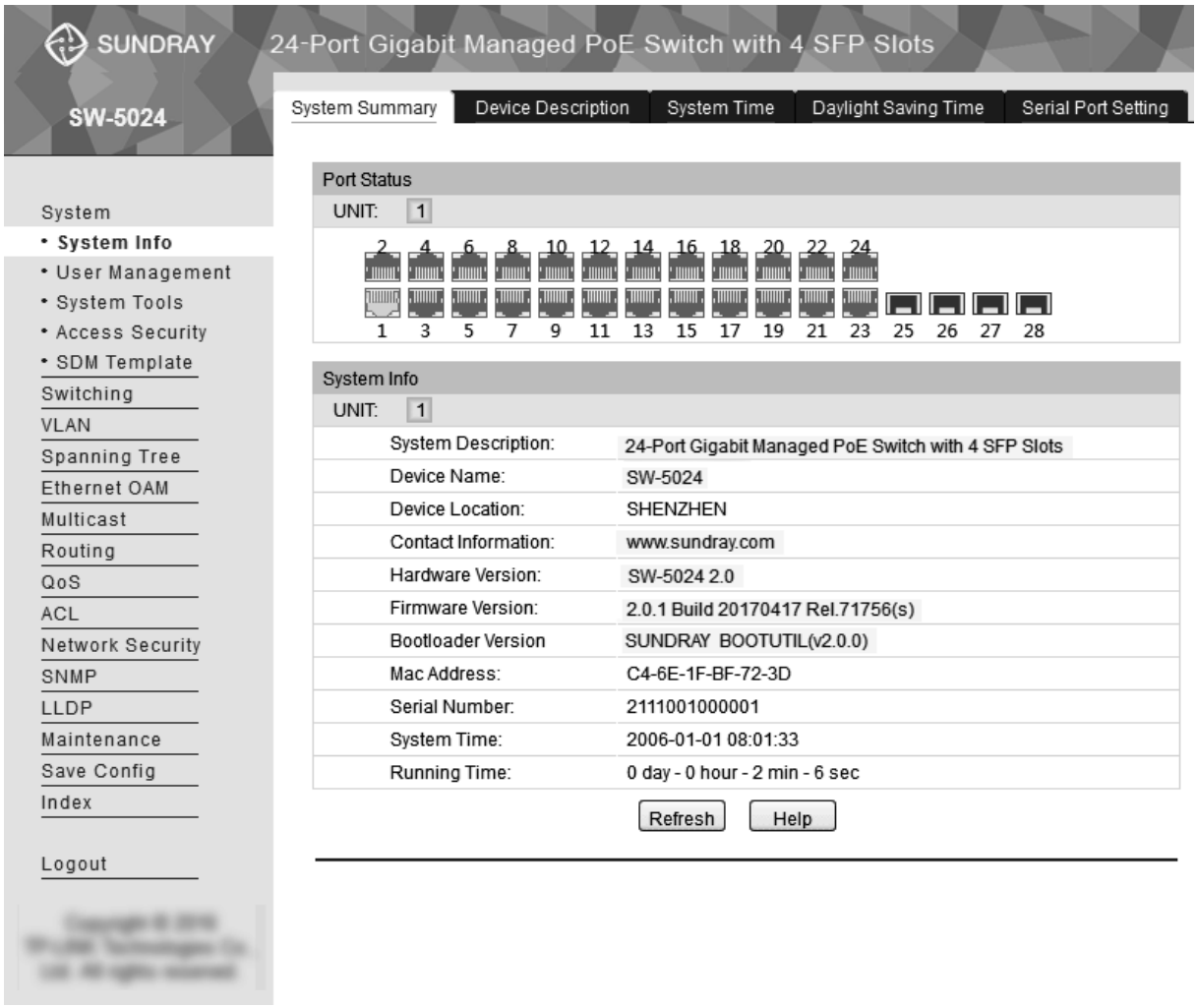


Figure 3-3 Main Setup-Menu

Note:

Clicking **Apply** can only make the new configurations effective before the switch is rebooted. If you want to keep the configurations effective even the switch is rebooted, please click **Save Config**. You are suggested to click **Save Config** before cutting off the power or rebooting the switch to avoid losing the new configurations.

Return to CONTENTS

Chapter 4 System

The System module is mainly for system configuration of the switch, including four submenus: **System Info**, **User Management**, **System Tools**, **Access Security** and **SDM Template**.

4.1 System Info

The System Info, mainly for basic properties configuration, can be implemented on **System Summary**, **Device Description**, **System Time**, **Daylight Saving Time** and **Serial Port Setting** pages.

4.1.1 System Summary

On this page you can view the port connection status and the system information.

The port status diagram shows the working status of 24 10/100/1000Mbps RJ45 ports and 4 SFP ports of the switch.

Choose the menu **System→System Info→System Summary** to load the following page.

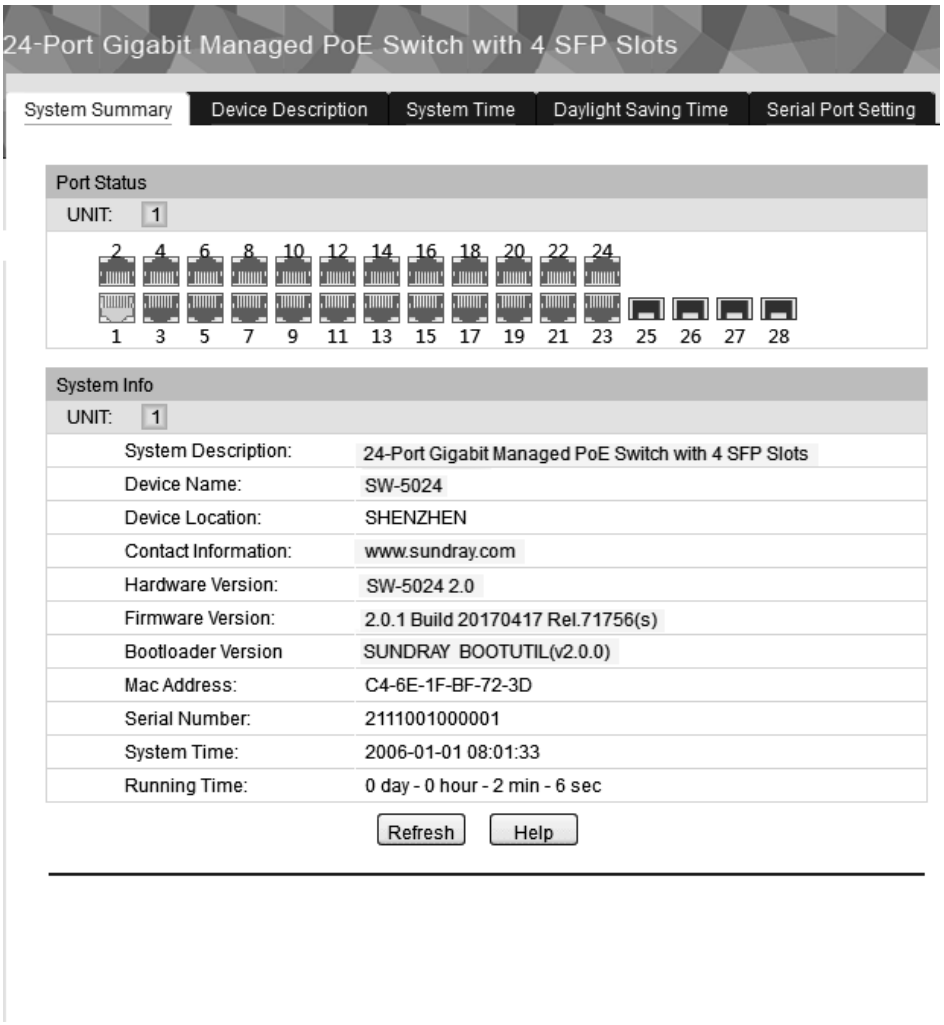


Figure 4-1 System Summary

- **Port Status**

 Indicates the 1000Mbps port is not connected to a device.

 Indicates the 1000Mbps port is at the speed of 1000Mbps.

 Indicates the 1000Mbps port is at the speed of 10Mbps or 100Mbps.

 Indicates the SFP port is not connected to a device.

 Indicates the SFP port is at the speed of 1000Mbps.

When the cursor moves on the port, the detailed information of the port will be displayed.

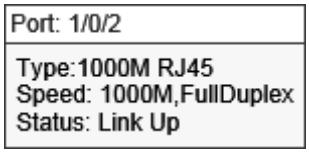


Figure 4-2 Port Information

- **Port Info**

Port: Displays the port number of the switch.

Type: Displays the type of the port.

Rate: Displays the maximum transmission rate of the port.

Status: Displays the connection status of the port.

Click a port to display the bandwidth utilization on this port. The actual rate divided by theoretical maximum rate is the bandwidth utilization. The following figure displays the bandwidth utilization monitored every four seconds. Monitoring the bandwidth utilization on each port facilitates you to monitor the network traffic and analyze the network abnormities.

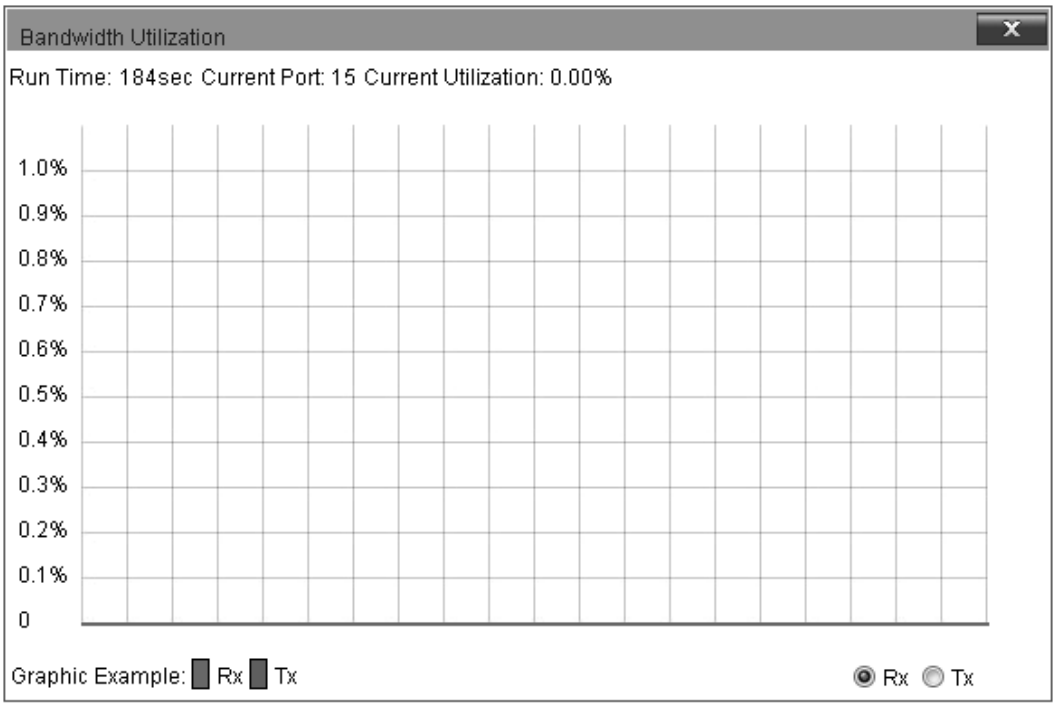


Figure 4-3 Bandwidth Utilization

- **Bandwidth Utilization**

Rx: Select Rx to display the bandwidth utilization of receiving packets on this port.

Tx: Select Tx to display the bandwidth utilization of sending packets on this port.

4.1.2 Device Description

On this page you can configure the description of the switch, including device name, device location and system contact.

Choose the menu **System→System Info→Device Description** to load the following page.

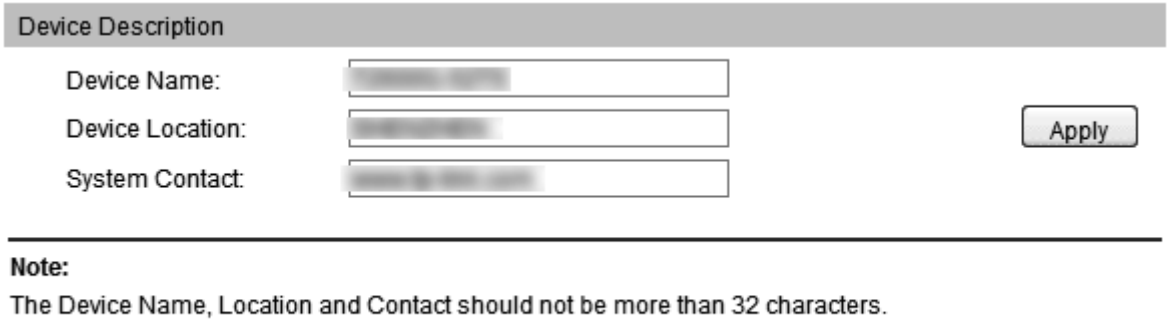


Figure 4-4 Device Description

The following entries are displayed on this screen:

- **Device Description**

Device Name: Enter the name of the switch.

Device Location: Enter the location of the switch.

System Contact: Enter your contact information.

4.1.3 System Time

System Time is the time displayed while the switch is running. On this page you can configure the system time and the settings here will be used for other time-based functions.

You can manually set the system time, get time from an NTP server or synchronize with PC's clock as the system time.

Choose the menu **System→System Info→System Time** to load the following page.

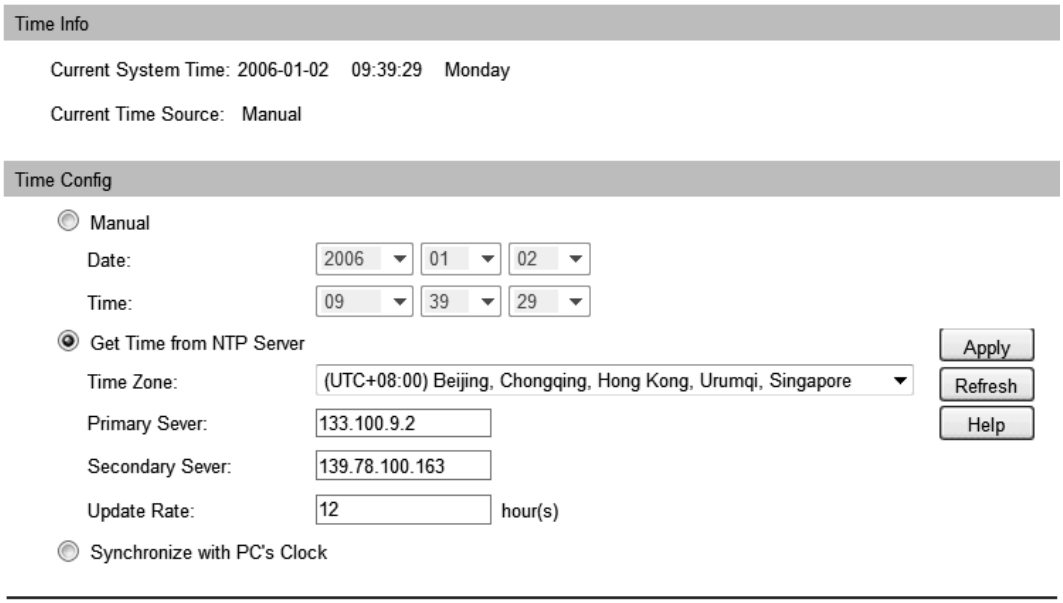


Figure 4-5 System Time

The following entries are displayed on this screen:

- **Time Info**

  Current System Time: Displays the current date and time of the switch.

  Current Time Source: Displays the current time source of the switch.

- **Time Config**

  Manual: When this option is selected, you can set the date and time manually.

Get Time from NTP Server:	When this option is selected, you can configure the time zone and the IP Address for the NTP Server. The switch will get UTC automatically if it has connected to an NTP Server. ● **Time Zone:** Select your local time. ● **Primary/Secondary Server:** Enter the IP Address for the NTP Server. ● **Update Rate:** Specify the rate fetching time from NTP server.
Synchronize with PC'S Clock:	When this option is selected, the administrator PC's clock is utilized.

Note:

1. The system time will be restored to the default when the switch is restarted and you need to reconfigure the system time of the switch.
2. When Get Time from NTP Server is selected and no time server is configured, the switch will get time from the time server of the Internet if it has connected to the Internet.

4.1.4 Daylight Saving Time

Here you can configure the Daylight Saving Time of the switch.

Choose the menu **System→System Info→Daylight Saving Time** to load the following page.

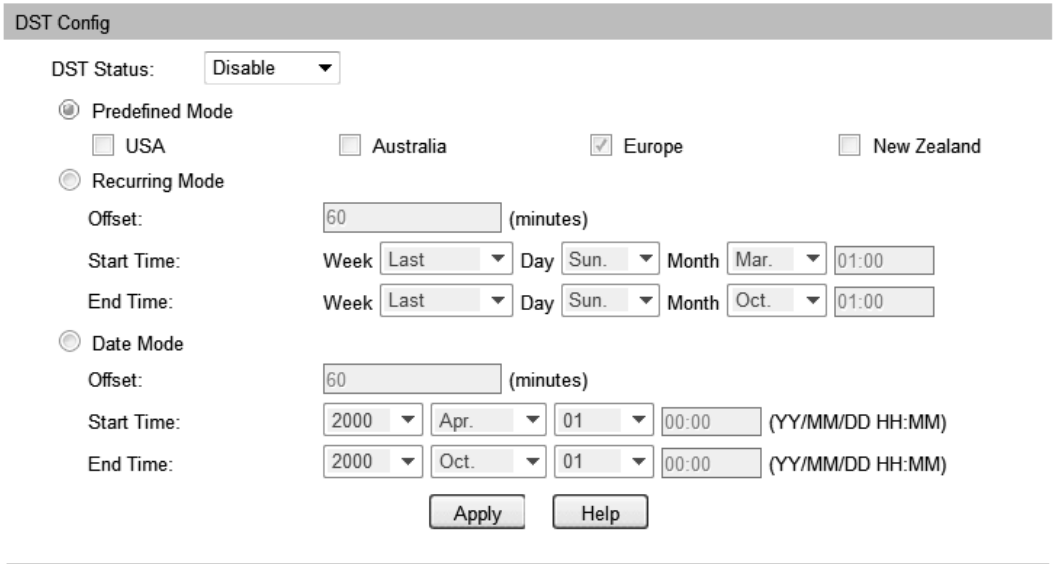


Figure 4-6 Daylight Saving Time

The following entries are displayed on this screen:

- **DST Config**

DST Status: Enable or disable the DST.

Predefined Mode: Select a predefined DST configuration.

- USA: Second Sunday in March, 02:00 ~ First Sunday in November, 02:00.
- Australia: First Sunday in October, 02:00 ~ First Sunday in April, 03:00.
- Europe: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00.
- New Zealand: Last Sunday in September, 02:00 ~ First Sunday in April, 03:00.

Recurring Mode: Specify the DST configuration in recurring mode. This configuration is recurring in use.

- Offset: Specify the time adding in minutes when Daylight Saving Time comes.
- Start/End Time: Select starting time and ending time of Daylight Saving Time.

Date Mode: Specify the DST configuration in Date mode. This configuration is recurring in use.

- Offset: Specify the time adding in minutes when Daylight Saving Time comes.
- Start/End Time: Select starting time and ending time of Daylight Saving Time.

Note:

1. When the DST is disabled, the predefined mode, recurring mode and date mode cannot be configured.
2. When the DST is enabled, the default daylight saving time is of European in predefined mode.

4.1.5 Serial Port Setting

On this page you can configure the Baud Rate of the console connection.

Choose the menu **System→System Info→Serial Port Setting** to load the following page.

Figure 4-7 User Table

The following entries are displayed on this screen:

- **Serial Port Settings**

  Baud Rate: Configure the baud rate of the console connection. It is 38400 bps by default.

  Data Bits: Displays the default data bits.

  Parity Bits: Displays the parity bits.

  Stop Bits: Displays the stop bits.

4.2 User Management

User Management functions to configure the user name and password for users to log on to the Web management page with a certain access level so as to protect the settings of the switch from being randomly changed.

The User Management function can be implemented on **User Table** and **User Config** pages.

4.2.1 User Table

On this page you can view the information about the current users of the switch.

Choose the menu **System→User Management→User Table** to load the following page.

Figure 4-8 User Table

4.2.2 User Config

On this page you can configure the access level of the user to log on to the Web management page. The switch provides four access levels: Admin, Operator, Power User and User. “Admin”

means that you can edit, modify and view all the settings of different functions. "Operator" means that you can edit, modify and view most of the settings of different functions. "Power User" means that you can edit, modify and view some of the settings of different functions. "User" means that you can only view some of the settings of different functions without the right to edit or modify. The Web management pages contained in this guide are subject to the admin's login without any explanation.

Choose the menu **System→User Management→User Config** to load the following page.

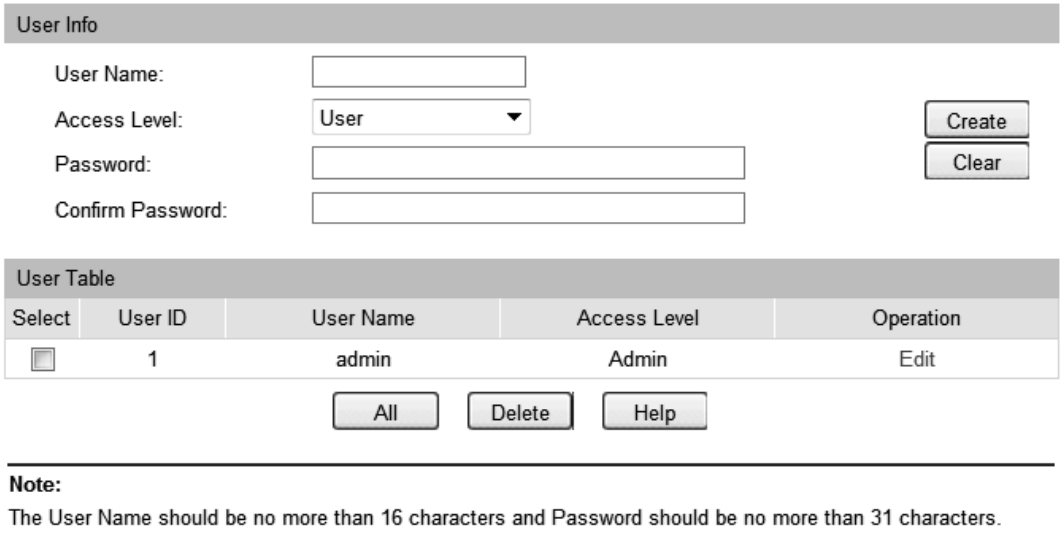


Figure 4-9 User Config

The following entries are displayed on this screen:

- **User Info**

User Name: Create a name for users' login.

Access Level: Select the access level to login.

- Admin: Admin can edit, modify and view all the settings of different functions.
- Operator: Operator can edit, modify and view most of the settings in different functions.
- Power User: Power User can edit, modify and view some of the settings in different functions.
- User: User only can view the settings without the right to edit and modify.

Password: Type a password for users' login.

Confirm Password: Retype the password.

- **User Table**

Select: Select the desired entry to delete the corresponding user information. It is multi-optional. The current user information can't be deleted.

User ID, User Name, Access Level: Displays the current user ID, user name, and access level.

Operation: Click the **Edit** button of the desired entry, and you can edit the corresponding user information. After modifying the settings, please click the **Apply** button to make the modification effective. Access level of the current user information cannot be modified.

4.3 System Tools

The System Tools function, allowing you to manage the configuration file of the switch, can be implemented on **Boot Config**, **Config Restore**, **Config Backup**, **Firmware Upgrade**, **System Reboot, Reboot Schedule** and **System Reset** pages.

4.3.1 Boot Config

On this page you can configure the boot file of the switch. When the switch is powered on, it will start up with the startup image. If it fails, it will try to start up with the backup image. If this fails too, you will enter into the bootutil menu of the switch.

Choose the menu **System** → **System Tools** → **Boot Config** to load the following page.

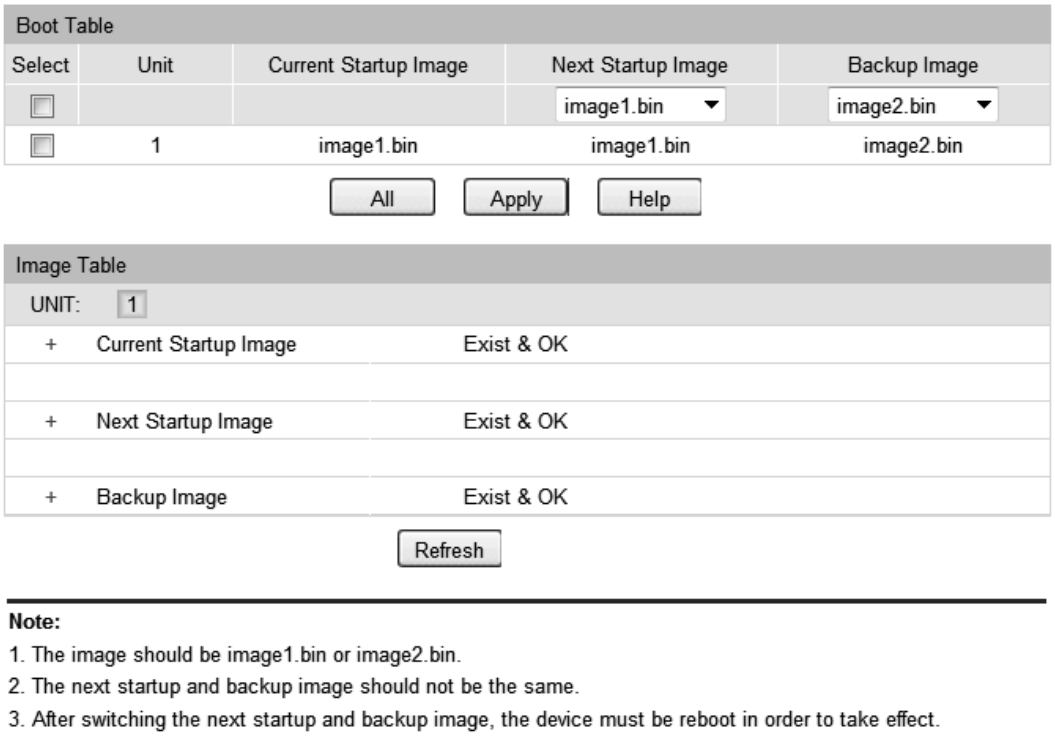


Figure 4-10 Boot Config

The following entries are displayed on this screen:

- **Boot Table**

Select: Select the unit(s).

Unit:	Displays the unit ID.
Current Startup Image:	Displays the current startup image.
Next Startup Image:	Select the next startup image.
Backup Image:	Select the backup boot image.

4.3.2 Config Restore

On this page you can upload a backup configuration file to restore your switch to this previous configuration.

Choose the menu **System→System Tools→Config Restore** to load the following page.

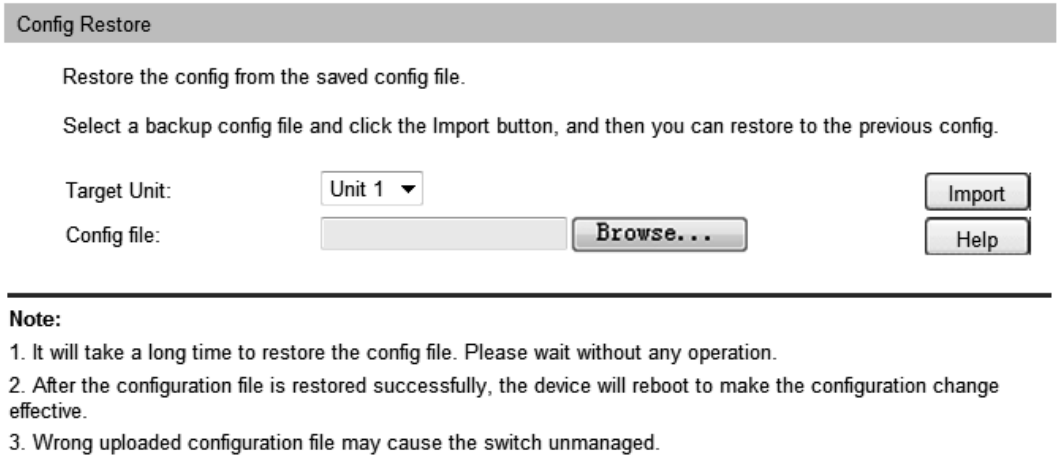


Figure 4-11 Config Restore

The following entries are displayed on this screen:

➢ **Config Restore**

Target Unit:	Select a member switch to import the configuration file.
Config File:	Click the **Browse** button to select a backup file and click the **Import** button to restore the startup configuration file.

Note:

1. It will take a few minutes to restore the configuration. Please wait without any operation.
2. After the configuration file is restored successfully, the device will reboot to make the configuration change effective.
3. Wrong uploaded configuration file may cause the switch unmanaged.

4.3.3 Config Backup

On this page you can download the current configuration and save it as a file to your computer for your future configuration restore.

Choose the menu **System→System Tools→Config Backup** to load the following page.

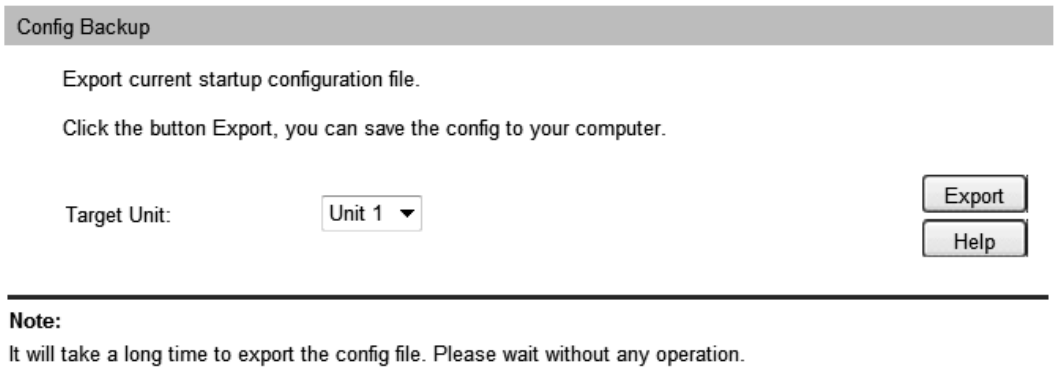


Figure 4-12 Config Backup

The following entries are displayed on this screen:

- **Config Backup**

  Target Unit: Select a member switch to export the configuration file.

Click the **Export** button to save the current startup configuration file to your computer. You are suggested to take this measure before upgrading.

Note:

It will take a few minutes to backup the configuration. Please wait without any operation.

4.3.4 Firmware Upgrade

The switch system can be upgraded via the Web management page. To upgrade the system is to get more functions and better performance.

Choose the menu **System→System Tools→Firmware Upgrade** to load the following page.

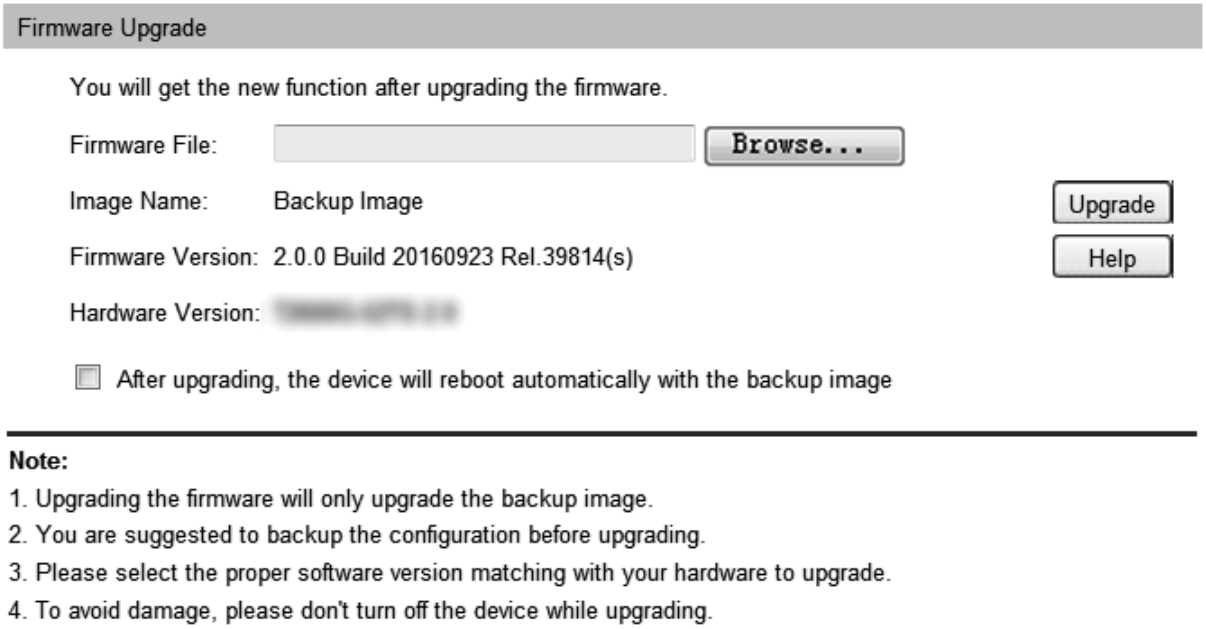


Figure 4-13 Firmware Upgrade

Please pay attention to the checkbox "**After upgrading, the device will reboot automatically with the backup image**". If the checkbox is checked, the switch will reboot with the uploaded firmware file, and the current Next Startup Image will switch to the Backup Image. If the checkbox is not checked, the uploaded firmware file will take place of the Backup Image. To start with the uploaded firmware, you should exchange the Next Startup Image and Backup Image in Boot Config and reboot the switch.

Note:

1. Upgrading the firmware will only upgrade the backup image.
2. You are suggested to backup the configuration before upgrading.
3. Please select the proper software version matching with your hardware to upgrade.
4. To avoid damage, please don't turn off the device while upgrading.

4.3.5 System Reboot

On this page you can reboot the switch and return to the login page. Please save the current configuration before rebooting to avoid losing the configuration unsaved.

Choose the menu **System→System Tools→System Reboot** to load the following page.

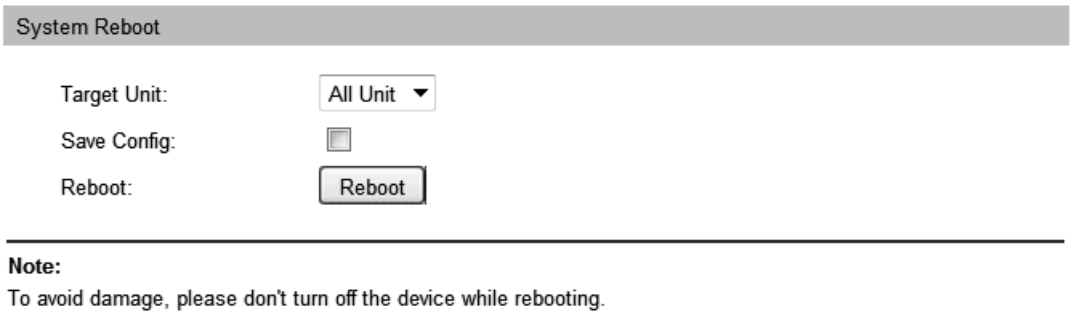


Figure 4-14 System Reboot

Note:

To avoid damage, please don't turn off the device while rebooting.

4.3.6 Reboot Schedule

On this page you can schedule a reboot plan for the switch. Users can configure the reboot schedule in two modes. The first one is to reboot the switch in a specific time interval. The second one is to reboot the switch at a specific time and date.

Users can choose whether to save the configurations before the reboot. If **Save Before Reboot** is not checked, the reboot schedule will be deleted after the next reboot.

Choose the menu **System→System Tools→Reboot Schedule** to load the following page.

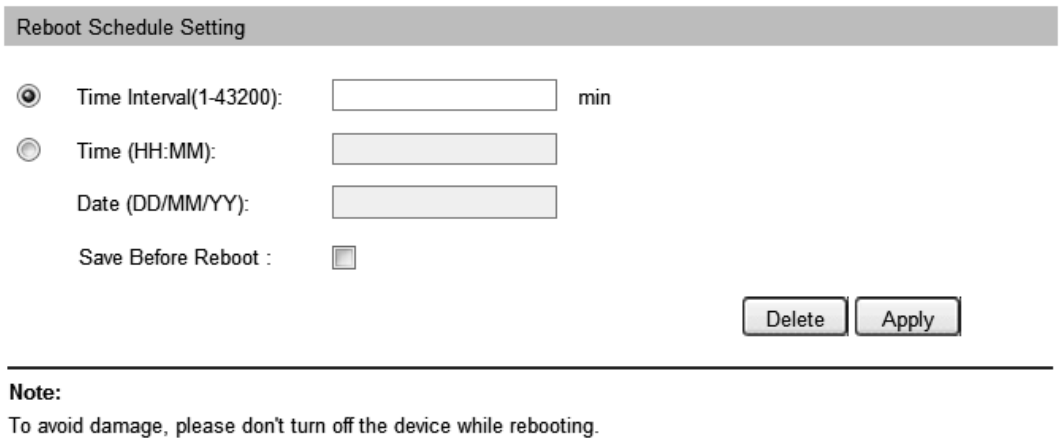


Figure 4-15 Reboot Schedule Setting

The following entries are displayed on this screen:

- **Reboot Schedule Setting**

Time Interval:	Specify a period of time. The switch will reboot after this period. It ranges from 1 to 43200 minutes. This reboot schedule recurs if users check the **Save Before Reboot**.
Time:	Specify the time for the switch to reboot, in the format of HH:MM.
Date:	Specify the date for the switch to reboot, in the format of DD/MM/YYYY. The date should be within 30 days. If no date is specified and the time you set here is later than the time that this above Time is set, the switch will reboot later that day; otherwise the switch will reboot at the time point the next day.
Save Before Reboot:	Select to save the switch's configurations before it reboots.

Note:

To avoid damage, please don't turn off the device while rebooting.

4.3.7 System Reset

On this page you can reset the switch to the default. All the settings will be cleared after the switch is reset.

Choose the menu **System→System Tools→System Reset** to load the following page.

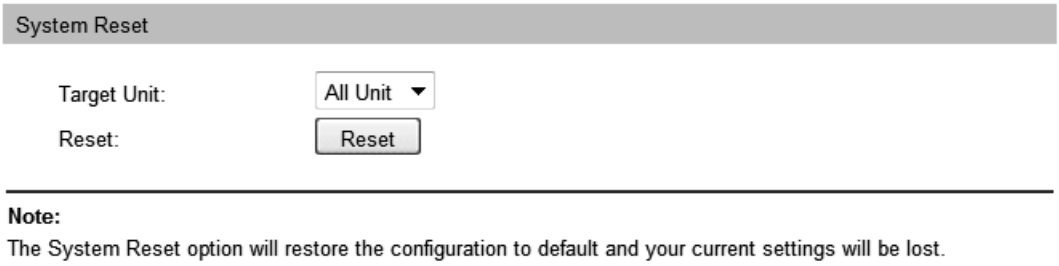


Figure 4-16 System Reset

Note:

After the system is reset, the switch will be reset to the default and all the settings will be cleared.

4.4 Access Security

Access Security provides different security measures for the remote login so as to enhance the configuration management security. It can be implemented on **Access Control**, **HTTP Config**, **HTTPS Config**, **SSH Config** and **Telnet Config** pages.

4.4.1 Access Control

On this page you can control the users logging on to the Web management page to enhance the configuration management security.

Choose the menu **System→Access Security→Access Control** to load the following page.

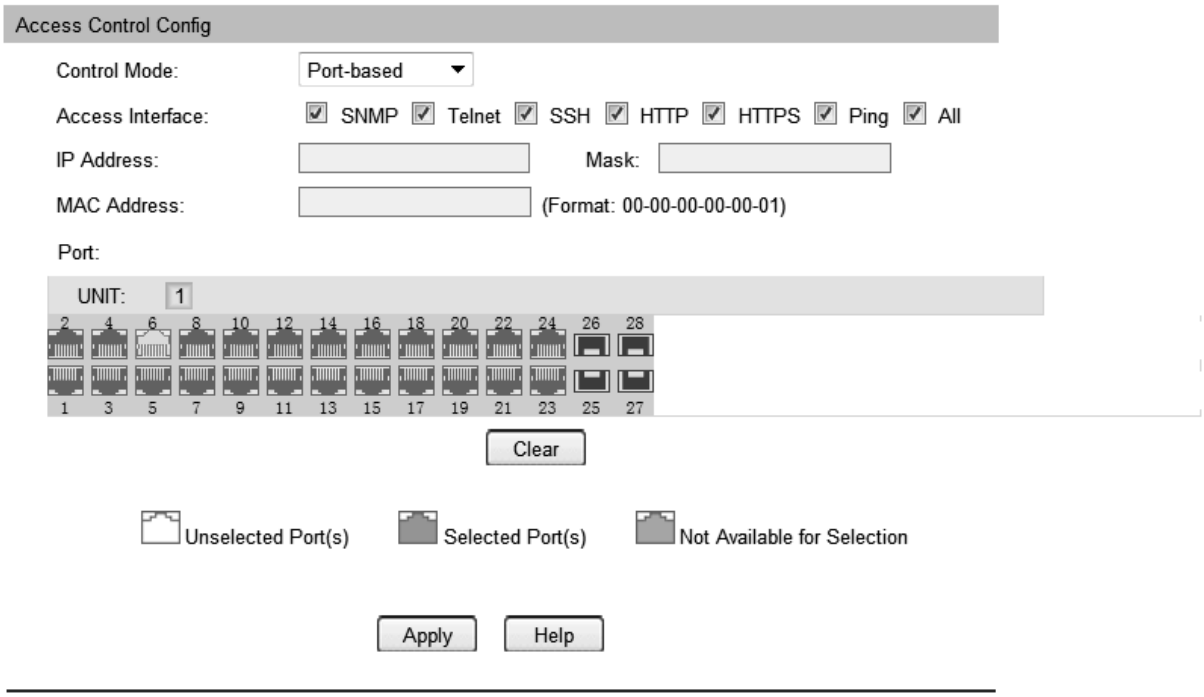


Figure 4-17 Access Control

The following entries are displayed on this screen:

- **Access Control Config**

Control Mode: Select the control mode for users to log on to the Web management page.

- Disable: Select to disable Access Control function.
- IP-based: Select this option to limit the IP-range of the users for login.
- MAC-based: Select this option to limit the MAC Address of the users for login.
- Port-based: Select this option to limit the ports for login.

Access Interface: Select the interface for access control to apply.

IP Address & Mask These fields is available to configure only when IP-based mode is selected. Only the users within the IP-range you set here are allowed for login.

MAC Address: The field is available to configure only when MAC-based mode is selected. Only the user with this MAC Address you set here are allowed for login.

Port: The field is available to configure only when Port-based mode is selected. Only the users connecting to the ports selected are allowed to manage the switch.

4.4.2 HTTP Config

With the help of HTTP (Hyper Text Transfer Protocol), you can manage the switch through a standard browser. The standards development of HTTP was coordinated by the Internet Engineering Task Force and the World Wide Web Consortium.

On this page you can configure the HTTP function.

Choose the menu **System→Access Security→HTTP Config** to load the following page.

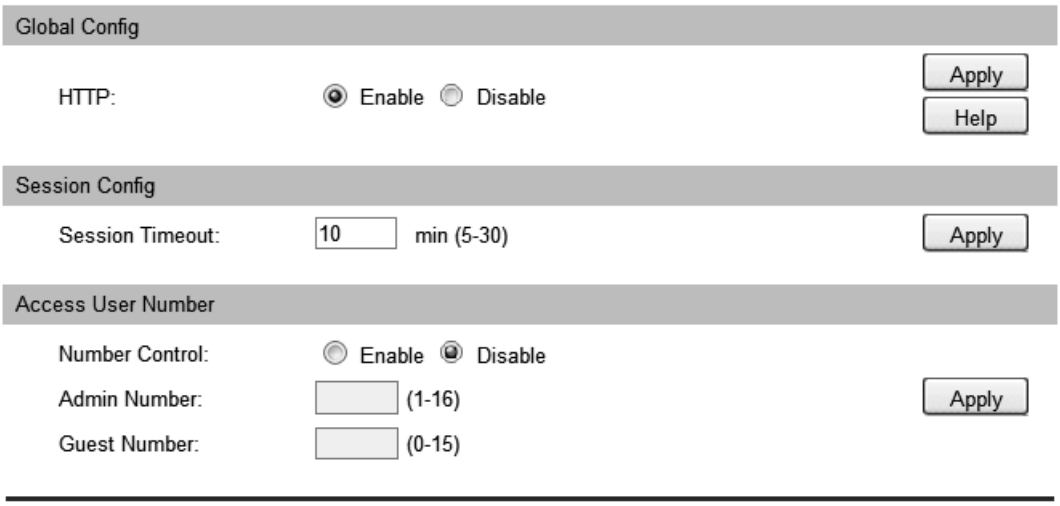


Figure 4-18 HTTP Config

The following entries are displayed on this screen:

- **Global Config**

  HTTP: Select Enable/Disable the HTTP function on the switch.

- **Session Config**

  Session Timeout: If you do nothing with the Web management page within the timeout time, the system will log out automatically. If you want to reconfigure, please login again.

- **Access User Number**

  Number Control: Select Enable/Disable the Number Control function.

  Admin Number: Enter the maximum number of the users logging on to the Web management page as Admin.

  Guest Number: Enter the maximum number of the users logging on to the Web management page as Guest.

4.4.3 HTTPS Config

SSL (Secure Sockets Layer), a security protocol, is to provide a secure connection for the application layer protocol (e.g. HTTP) communication based on TCP. SSL is widely used to

secure the data transmission between the Web browser and servers. It is mainly applied through ecommerce and online banking.

SSL mainly provides the following services:

1. Authenticate the users and the servers based on the certificates to ensure the data are transmitted to the correct users and servers;
2. Encrypt the data transmission to prevent the data being intercepted;
3. Maintain the integrality of the data to prevent the data being altered in the transmission.

Adopting asymmetrical encryption technology, SSL uses key pair to encrypt/decrypt information. A key pair refers to a public key (contained in the certificate) and its corresponding private key. By default the switch has a certificate (self-signed certificate) and a corresponding private key. The Certificate/Key Download function enables the user to replace the default key pair.

After SSL is effective, you can log on to the Web management page via https://192.168.0.1. For the first time you use HTTPS connection to log into the switch with the default certificate, you will be prompted that "The security certificate presented by this website was not issued by a trusted certificate authority" or "Certificate Errors". Please add this certificate to trusted certificates or continue to this website.

The switch also supports HTTPS connection for IPv6. After configuring an IPv6 address (for example, 3001::1) for the switch, you can log on to the switch's Web management page via https://[3001::1].

On this page you can configure the HTTPS function.

Choose the menu **System→Access Security→HTTPS Config** to load the following page.

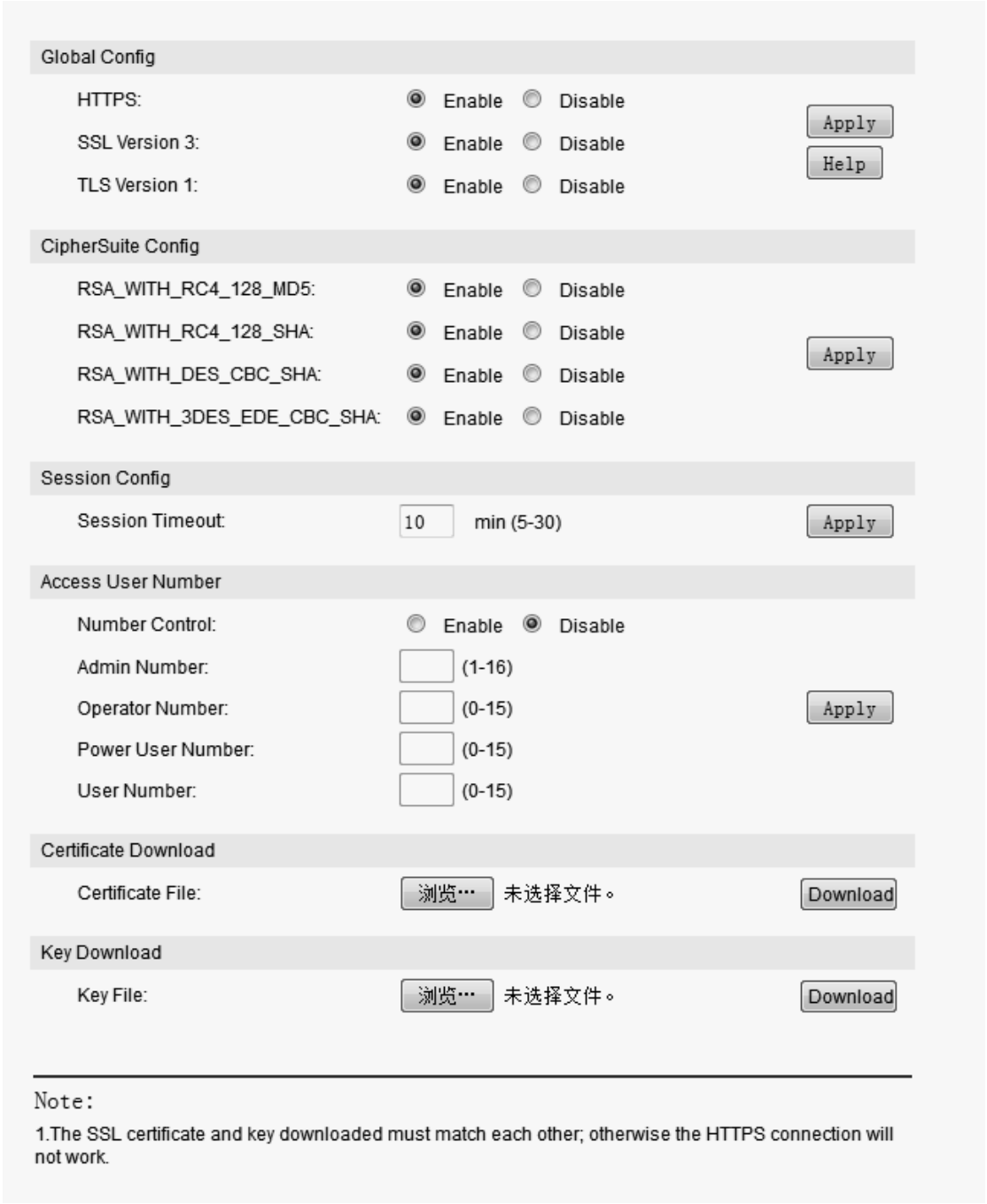


Figure 4-19 HTTPS Config

The following entries are displayed on this screen:

- **Global Config**

HTTPS: Select Enable/Disable the HTTPS function on the switch.

SSL Version 3: Enable or Disable Secure Sockets Layer Version 3.0. By default, it's enabled.

TLS Version 1: Enable or Disable Transport Layer Security Version 1.0. By default, it's enabled.

- **CipherSuite Config**

RSA_WITH_RC4_128_MD5: Key exchange with RC4 128-bit encryption and MD5 for message digest. By default, it's enabled.

RSA_WITH_RC4_128_SHA: Key exchange with RC4 128-bit encryption and SHA for message digest. By default, it's enabled.

RSA_WITH_DES_CBC_SHA: Key exchange with DES-CBC for message encryption and SHA for message digest. By default, it's enabled.

RSA_WITH_3DES_EDE_CBC_SHA: Key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest. By default, it's enabled.

- **Session Config**

Session Timeout: If you do nothing with the Web management page within the timeout time, the system will log out automatically. If you want to reconfigure, please login again.

- **Access User Number**

Number Control: Select Enable/Disable the Number Control function.

Admin Number: Enter the maximum number of the users logging on to the Web management page as Admin.

Operator Number: Enter the maximum number of the users logging on to the Web management page as Operator.

Power User Number: Enter the maximum number of the users logging on to the Web management page as Power User.

User Number: Enter the maximum number of the users logging on to the Web management page as User.

- **Certificate Download**

Certificate File: Select the desired certificate to download to the switch. The certificate must be BASE64 encoded.

- **Key Download**

Key File: Select the desired key to download to the switch. The key must be BASE64 encoded.

Note:

1. The SSL certificate and key downloaded must match each other; otherwise the HTTPS connection will not work.
2. To establish a secured connection using https, please enter https:// into the URL field of the browser.
3. It may take more time for https connection than that for http connection, because https connection involves authentication, encryption and decryption etc.

4.4.4 SSH Config

As stipulated by IETF (Internet Engineering Task Force), SSH (Secure Shell) is a security protocol established on application and transport layers. SSH-encrypted-connection is similar to a telnet connection, but essentially the old telnet remote management method is not safe, because the password and data transmitted with plain-text can be easily intercepted. SSH can provide information security and powerful authentication when you log on to the switch remotely through an insecure network environment. It can encrypt all the transmission data and prevent the information in a remote management being leaked.

Comprising server and client, SSH has two versions, V1 and V2 which are not compatible with each other. In the communication, SSH server and client can auto-negotiate the SSH version and the encryption algorithm. After getting a successful negotiation, the client sends authentication request to the server for login, and then the two can communicate with each other after successful authentication. This switch supports SSH server and you can log on to the switch via SSH connection using SSH client software.

SSH key can be downloaded into the switch. If the key is successfully downloaded, the certificate authentication will be preferred for SSH access to the switch.

Choose the menu **System→Access Security→SSH Config** to load the following page.

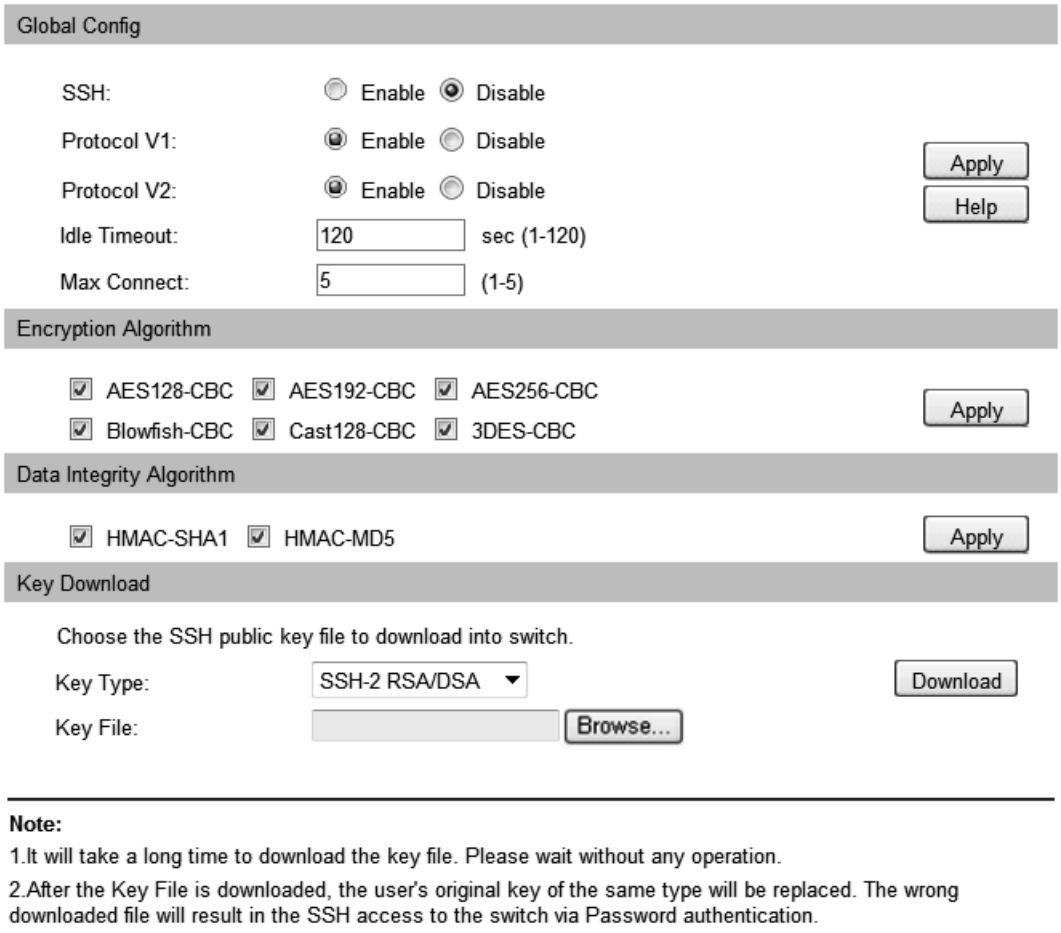


Figure 4-20 SSH Config

The following entries are displayed on this screen:

- **Global Config**

  SSH: Select Enable/Disable SSH function.

  Protocol V1: Select Enable/Disable SSH V1 to be the supported protocol.

  Protocol V2: Select Enable/Disable SSH V2 to be the supported protocol.

  Idle Timeout: Specify the idle timeout time. The system will automatically release the connection when the time is up. The default time is 120 seconds.

  Max Connect: Specify the maximum number of the connections to the SSH server. No new connection will be established when the number of the connections reaches the maximum number you set. The default value is 5.

- **Encryption Algorithm**

  Configure SSH encryption algorithms.

  AES128-CBC: Select the checkbox to enable the AES128-CBC algorithm of SSH.

  AES128-CBC: Select the checkbox to enable the AES128-CBC algorithm of SSH.

  AES192-CBC: Select the checkbox to enable the AES192-CBC algorithm of SSH.

  AES256-CBC: Select the checkbox to enable the AES256-CBC algorithm of SSH.

  Blowfish-CBC: Select the checkbox to enable the Blowfish-CBC algorithm of SSH.

  Cast128-CBC: Select the checkbox to enable the Cast128-CBC algorithm of SSH.

  3DES-CBC: Select the checkbox to enable the 3DES-CBC algorithm of SSH.

- **Data Integrity Algorithm**

  Configure SSH data integrity algorithms.

  HMAC-SHA1: Select the checkbox to enable the HMAC-SHA1 algorithm of SSH.

  HMAC-MD5: Select the checkbox to enable the HMAC-MD5 algorithm of SSH.

- **Key Download**

  Key Type: Select the type of SSH Key to download. The switch supports two types: SSH-2 RSA/DSA and SSH-1 RSA.

  Key File: Please ensure the key length of the downloaded file is in the range of 512 to 3072 bits.

  Download: Click the **Download** button to download the desired key file to the switch.

Note:

1. It will take a long time to download the key file. Please wait without any operation.
2. After the Key File is downloaded, the user's original key of the same type will be replaced. The wrong downloaded file will result in the SSH access to the switch via Password authentication.

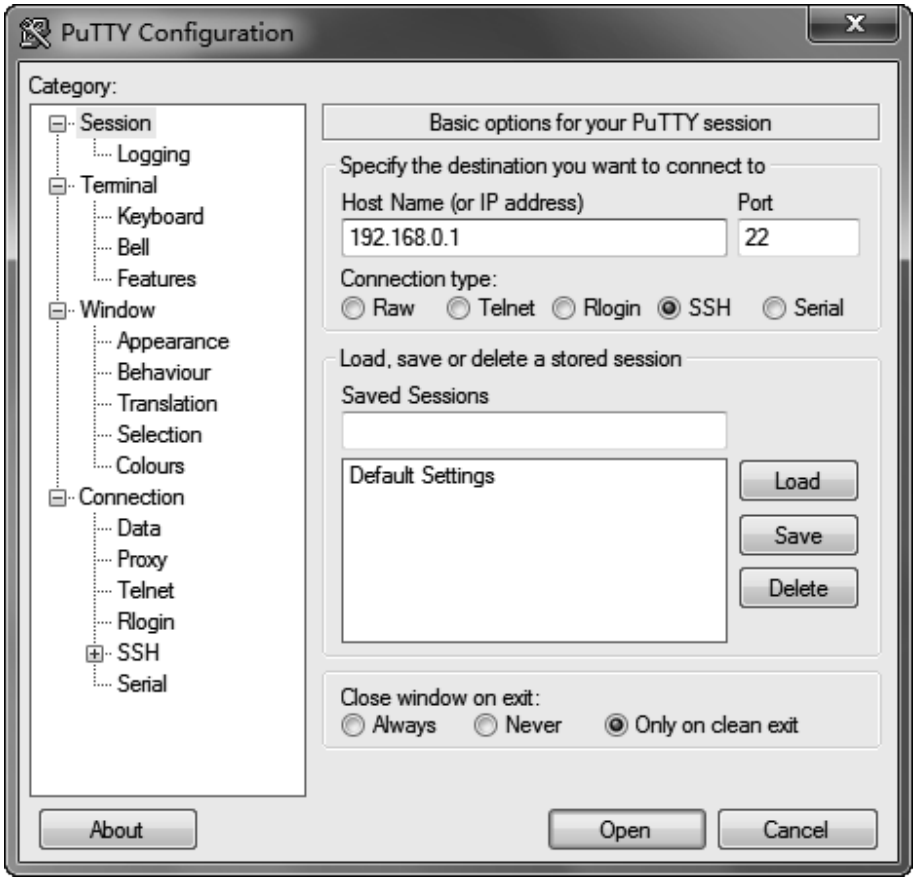
Application Example 1 for SSH:

➢ **Network Requirements**

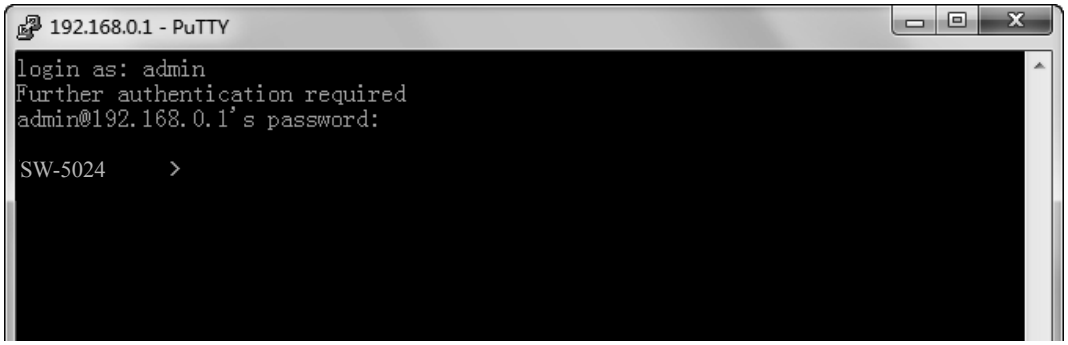
1. Log on to the switch via password authentication using SSH and the SSH function is enabled on the switch.
2. PuTTY client software is recommended.

➢ **Configuration Procedure**

1. Open the software to log on to the interface of PuTTY. Enter the IP address of the switch into **Host Name** field; keep the default value 22 in the **Port** field; select **SSH** as the Connection type.



2. Click the **Open** button in the above figure to log on to the switch. Enter the login user name and password, and then you can continue to configure the switch.



Application Example 2 for SSH:

➢ **Network Requirements**

1. Log on to the switch via key authentication using SSH and the SSH function is enabled on the switch.
2. PuTTY client software is recommended.

➢ **Configuration Procedure**

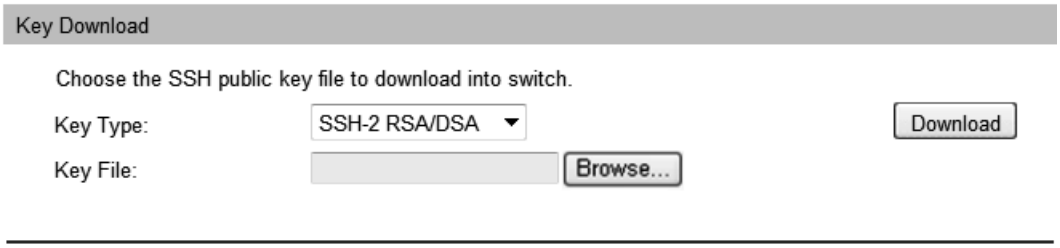
1. Select the key type and key length, and generate SSH key.

Note:

1. The key length is in the range of 512 to 3072 bits.
2. During the key generation, randomly moving the mouse quickly can accelerate the key generation.

2. After the key is successfully generated, please save the public key and private key to the computer.

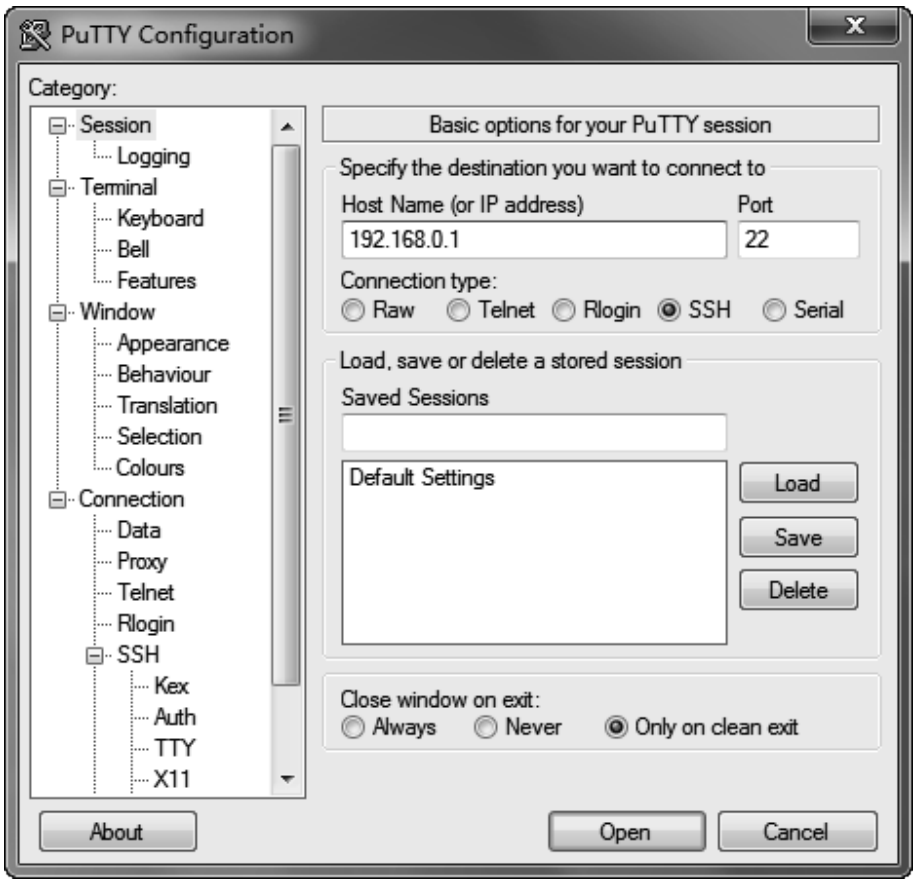
3. On the Web management page of the switch, download the public key file saved in the computer to the switch.



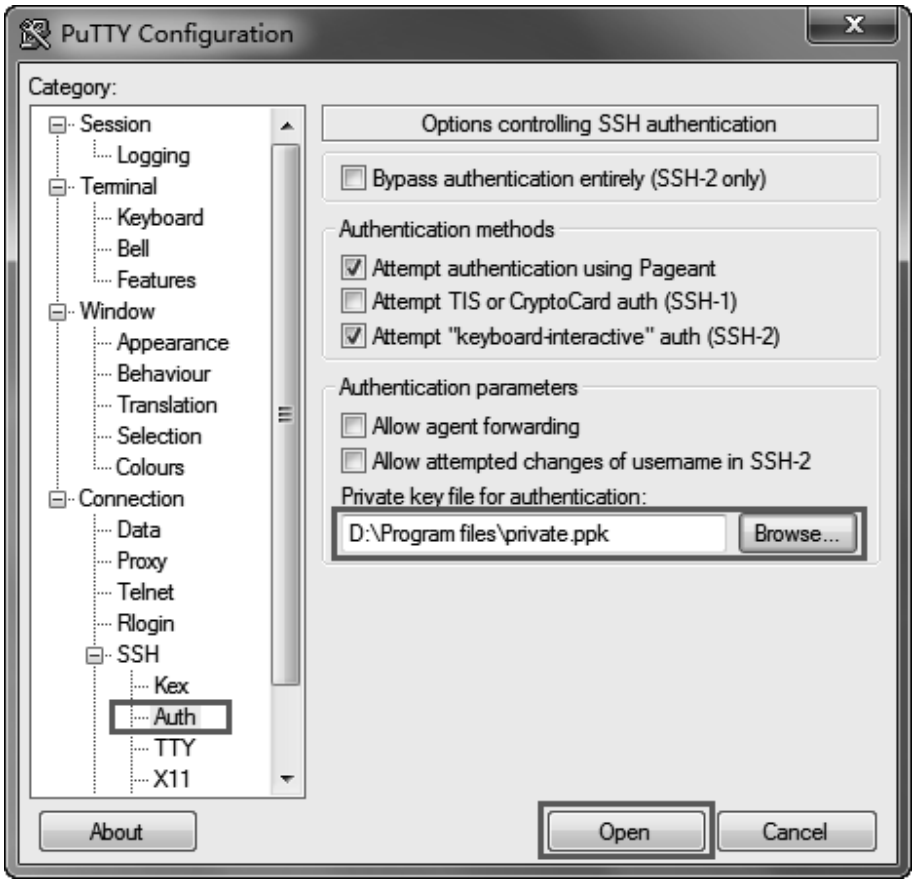
Note:

1. The key type should accord with the type of the key file.
2. The SSH key downloading cannot be interrupted.

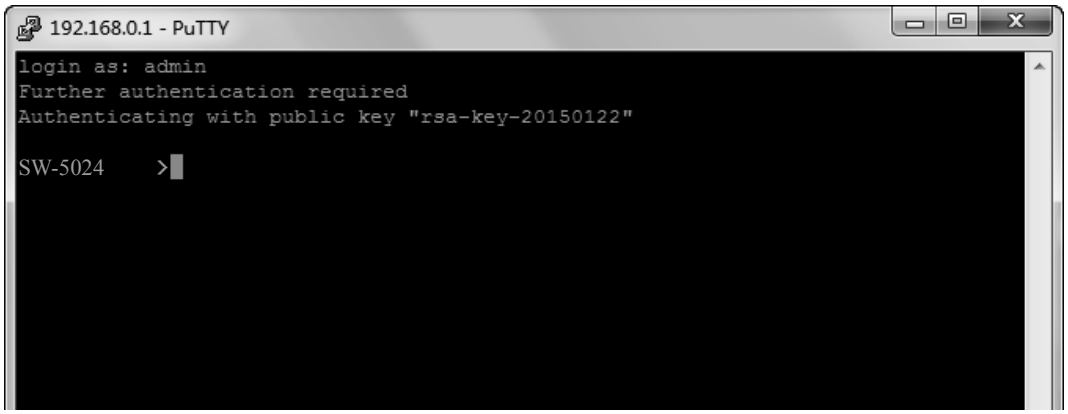
4. After the public key and private key are downloaded, please log on to the interface of PuTTY and enter the IP address for login.



5. Click **Browse** to download the private key file to SSH client software and click **Open**.



After successful authentication, please enter the login user name. If you log on to the switch without entering password, it indicates that the key has been successfully downloaded.



4.4.5 Telnet Config

On this page you can Enable/Disable Telnet function globally on the switch.

Choose the menu **System→Access Security→Telnet Config** to load the following page.

Figure 4-21 Access Control

The following entries are displayed on this screen:

- **Global Config**

Telnet: Select Enable/Disable Telnet function globally on the switch.

4.5 SDM Template

SDM (Switch Database Management) provides different templates for users to efficiently manage the hardware TCAM resources. Users can select the appropriate template according to the application environment.

4.5.1 SDM Template Config

On this page you can configure and view the SDM templates on the switch.

Choose the menu **System→SDM Template→SDM Template Config** to load the following page.

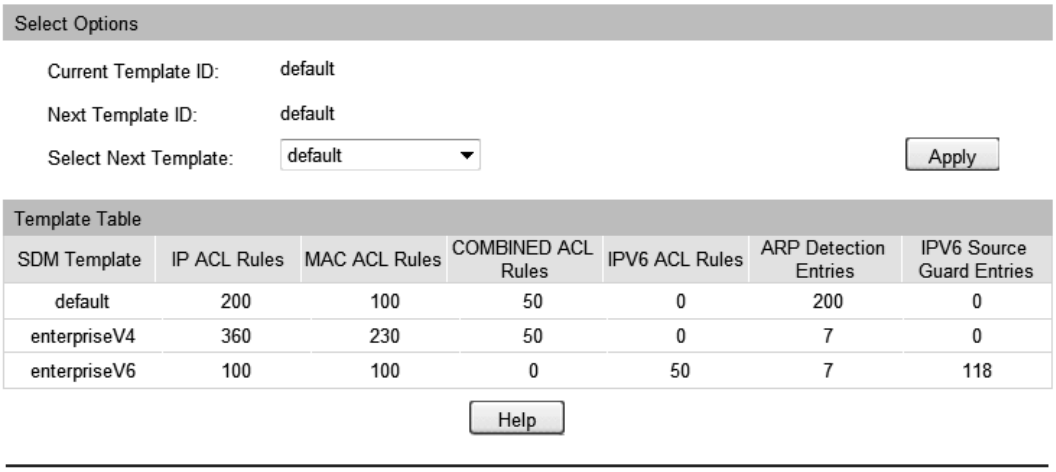


Figure 4-22 SDM Template Config

- **Select Options**

Current Template ID: Displays the SDM template currently in use.

Next Template ID: Displays the SDM template that will become active after a reboot.

Select Next Template: Configure the SDM template that will become active after the next reboot.

- **Template Table**

SDM Template:	Displays the template name.
IP ACL Rules:	Displays the number of TCAM entries for IP ACL Rules, which include Lay3 ACL Rules and Lay4 ACL Rules.
MAC ACL Rules:	Displays the number of TCAM entries for Lay2 ACL Rules.
Combined ACL Rules:	Displays the number of combined ACL rules.
IPv6 ACL Rules:	Displays the number of IPv6 ACL rules.
ARP Detection Entries:	Displays the number of TCAM entries for ARP defend.
IPv6 Source Guard Entries:	Displays the number of IPv6 source guard entries.

Return to CONTENTS

Chapter 5 Switching

Switching module is used to configure the basic functions of the switch, including four submenus: **Port**, **LAG**, **Traffic Monitor**, **MAC Address** and **L2TP**.

5.1 Port

The Port function, allowing you to configure the basic features for the port, is implemented on the **Port Config**, **Port Mirror**, **Port Security**, **Port Isolation** and **Loopback Detection** pages.

5.1.1 Port Config

On this page, you can configure the basic parameters for the ports. When the port is disabled, the packets on the port will be discarded. Disabling the port which is vacant for a long time can reduce the power consumption effectively. And you can enable the port when it is in need.

The parameters will affect the working mode of the port, please set the parameters appropriate to your needs.

Choose the menu **Switching→Port→Port Config** to load the following page.

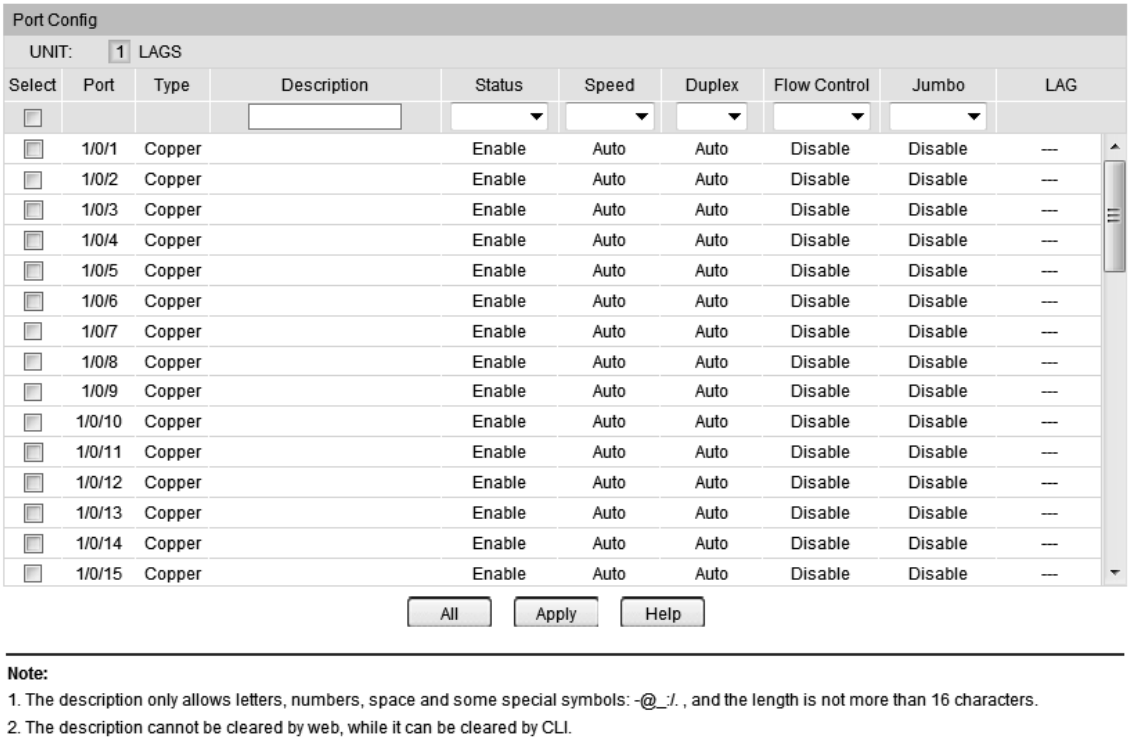


Figure 5-1 Port Config

The following entries are displayed on this screen:

- **Port Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select:	Select the desired port for configuration. It is multi-optional.
Port:	Displays the port number.
Type:	Displays the medium type of the port.
Description:	Give a description to the port for identification.
Status:	Allows you to Enable/Disable the port. When Enable is selected, the port/LAG can forward the packets normally.
Speed:	Select the Speed mode for the port. The device connected to the switch should be in the same Speed and Duplex mode with the switch. When 'Auto' is selected, the Speed mode will be determined by auto negotiation.
Duplex:	Select the Duplex mode for the port. When 'Auto' is selected, the Duplex mode will be determined by auto negotiation.
Flow Control:	Allows you to Enable/Disable the Flow Control feature. When Flow Control is enabled, the switch can synchronize the speed with its peer to avoid the packet loss caused by congestion.
Jumbo:	Allows you to Enable/Disable the Jumbo feature. The default maximum transmission unit (MTU) size is 1518 bytes. When Jumbo is enabled, the MTU size is 9216 bytes.
LAG:	Displays the LAG number which the port belongs to.

Note:

1. The switch cannot be managed through the disabled port. Please enable the port which is used to manage the switch.
2. The SFP ports support 1000M SFP module connection only.

5.1.2 Port Mirror

Port Mirror, the packets obtaining technology, functions to forward copies of packets from one/multiple ports (mirrored port) to a specific port (mirroring port). Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.

Choose the menu **Switching→Port→Port Mirror** to load the following page.

Figure 5-2 Mirror Group List

The following entries are displayed on this screen.

- **Mirror Session List**

Session: Displays the mirror session number.

Destination: Displays the mirroring port.

Mode: Displays the mirror mode. The value will be "Ingress Only", "Egress Only" or “Both”.

Source: Displays the mirrored ports.

Operation: You can configure the mirror session by clicking **Edit**, or clear the mirror session configuration by clicking the **Clear**.

Click **Edit** to display the following figure.

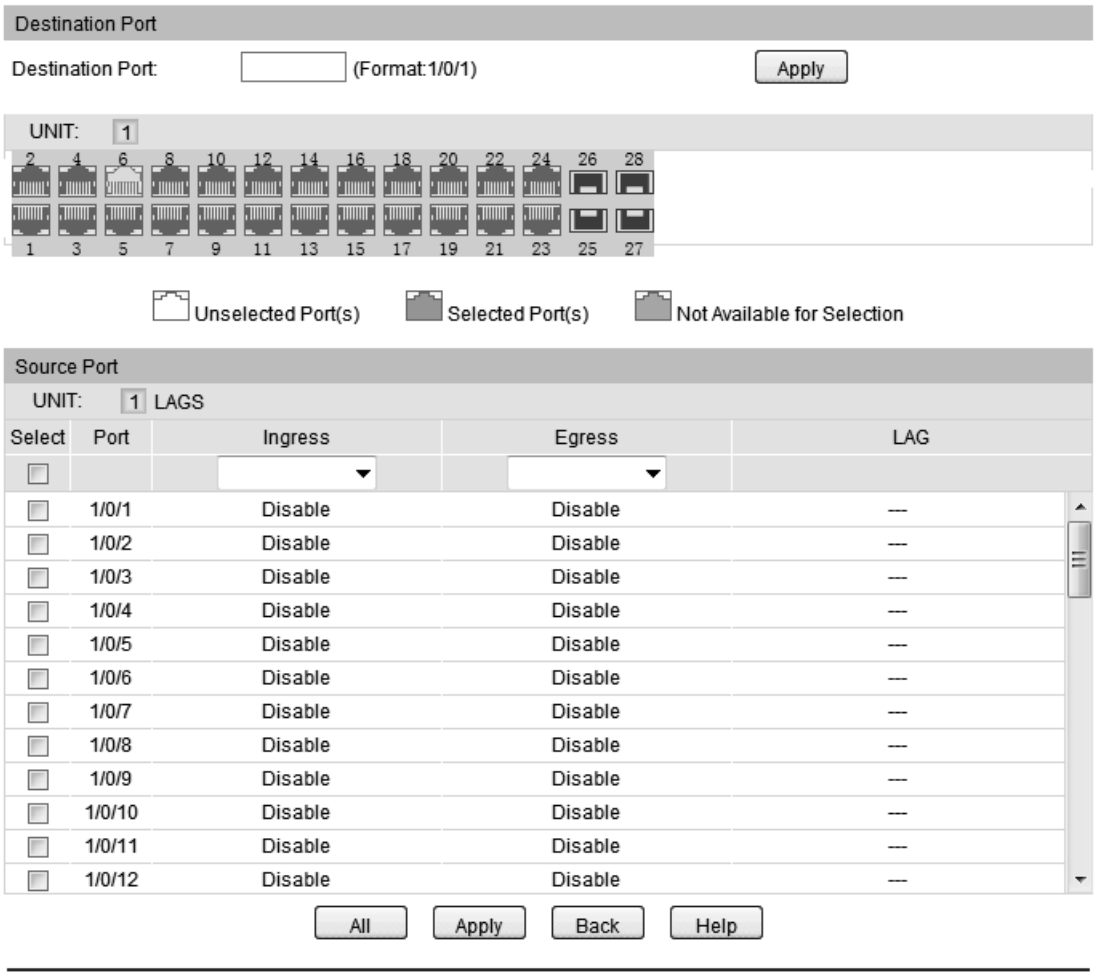


Figure 5-3 Port Mirror Config

The following entries are displayed on this screen:

- **Destination Port**

  Destination Port: Input or select a physical port from the port panel as the mirroring port.

- **Source Port**

  Select: Select the desired port as a mirrored port. It is multi-optional.

  Port: Displays the port number.

  Ingress: Select Enable/Disable the Ingress feature. When the Ingress is enabled, the incoming packets received by the mirrored port will be copied to the mirroring port.

  Egress: Select Enable/Disable the Egress feature. When the Egress is enabled, the outgoing packets sent by the mirrored port will be copied to the mirroring port.

  LAG: Displays the LAG number which the port belongs to. The LAG member cannot be selected as the mirrored port or mirroring port.

Note:

1. The LAG member cannot be selected as the mirrored port or mirroring port.
2. A port cannot be set as the mirrored port and the mirroring port simultaneously.
3. The Port Mirror function can span the multiple VLANs.

5.1.3 Port Security

MAC Address Table maintains the mapping relationship between the port and the MAC address of the connected device, which is the base of the packet forwarding. The capacity of MAC Address Table is fixed. MAC Address Attack is the attack method that the attacker takes to obtain the network information illegally. The attacker uses tools to generate the cheating MAC address and quickly occupy the MAC Address Table. When the MAC Address Table is full, the switch will broadcast the packets to all the ports. At this moment, the attacker can obtain the network information via various sniffers and attacks. When the MAC Address Table is full, the packets traffic will flood to all the ports, which results in overload, lower speed, packets drop and even breakdown of the system.

Port Security is to protect the switch from the malicious MAC Address Attack by limiting the maximum number of MAC addresses that can be learned on the port. The port with Port Security feature enabled will learn the MAC address dynamically. When the learned MAC address number reaches the maximum, the port will stop learning. Thereafter, the other devices with the MAC address unlearned cannot access to the network via this port.

Choose the menu **Switching→Port→Port Security** to load the following page.

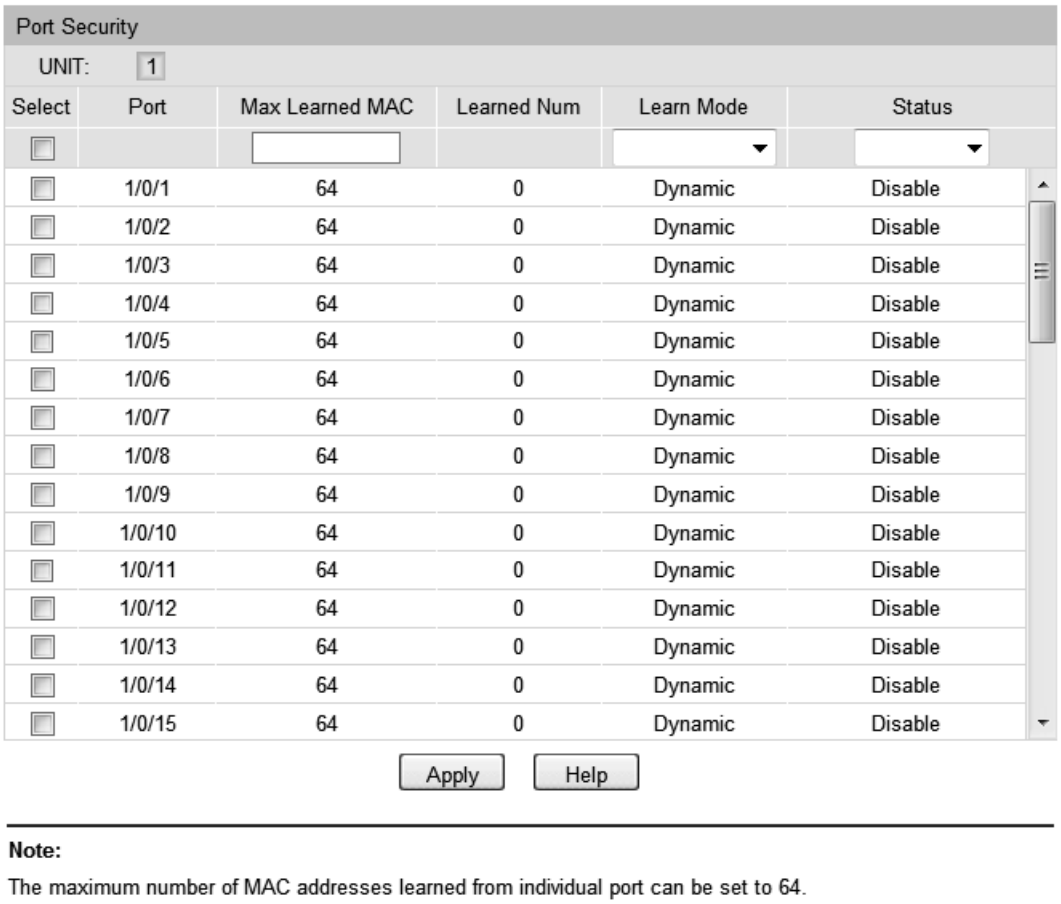


Figure 5-4 Port Security

The following entries are displayed on this screen:

➢ **Port Security**

Select: Select the desired port for Port Security configuration. It is multi-optional.

Port: Displays the port number.

Max Learned MAC: Specify the maximum number of MAC addresses that can be learned on the port.

Learned Num: Displays the number of MAC addresses that have been learned on the port.

Learn Mode: Select the Learn Mode for the port.

- **Dynamic:** When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time.
- **Static:** When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted.

- **Permanent:** When Permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.

Status: Select Enable/Disable the Port Security feature for the port.

Note:

The Port Security function is disabled for the LAG port member. Only the port is removed from the LAG, will the Port Security function be available for the port.

5.1.4 Port Isolation

Port Isolation provides a method of restricting traffic flow to improve the network security by forbidding the port to forward packets to the ports that are not on its forward portlist.

Choose the menu **Switching→Port→Port Isolation** to load the following page.

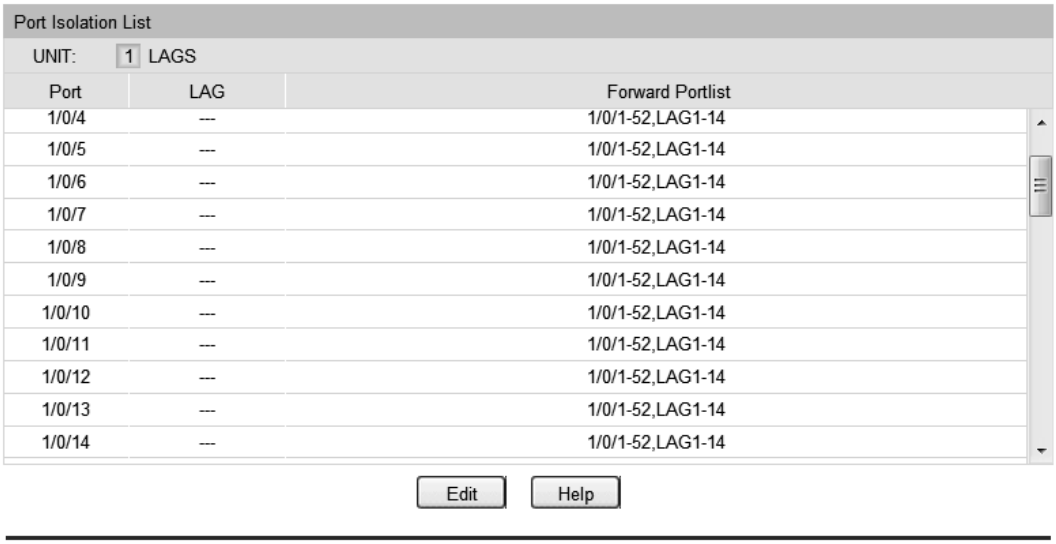


Figure 5-5 Port Isolation

The following entries are displayed on this screen:

➢ **Port Isolation List**

UNIT :1/LAGS : Click **1** to show the information of the physical ports. Click **LAGS** to show the information of the link aggregation groups.

Port: Displays the port number.

LAG : Displays the LAG number which the port belongs to.

Forward Portlist: Displays the forward portlist.

Click **Edit** to display the following figure.

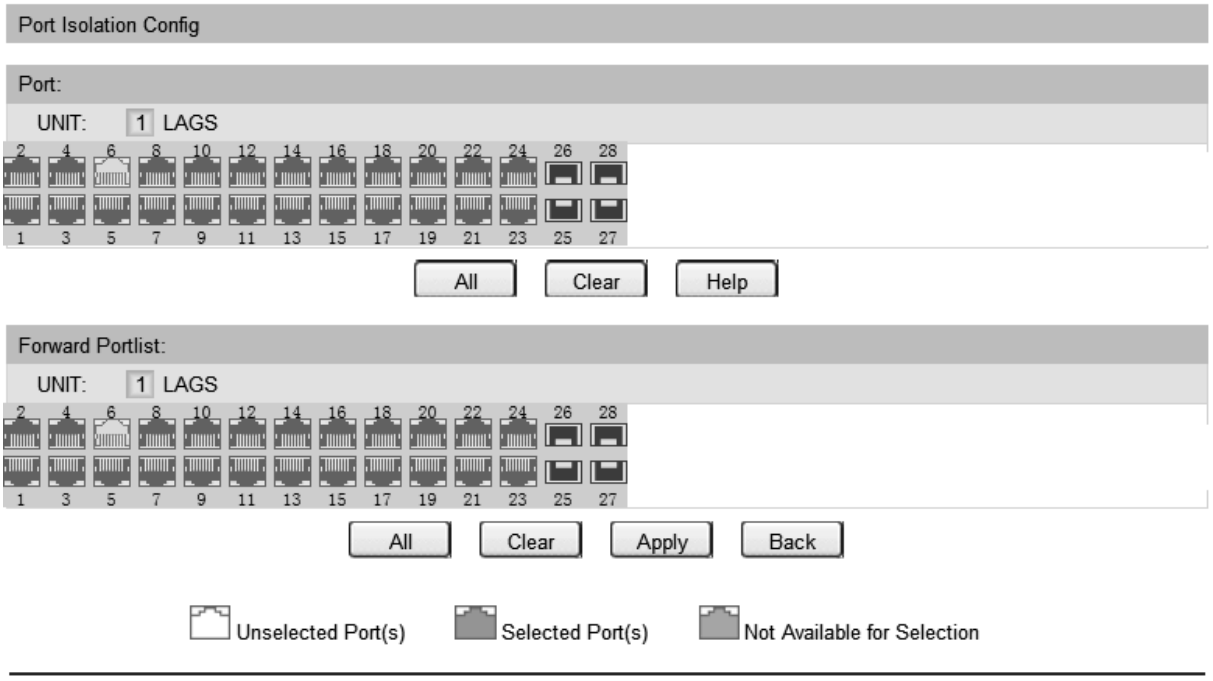


Figure 5-6 Port Isolation Config

5.1.5 Loopback Detection

With loopback detection feature enabled, the switch can detect loops using loopback detection packets. When a loop is detected, the switch will display an alert or further block the corresponding port according to the port configuration.

Choose the menu **Switching→Port→Loopback Detection** to load the following page.

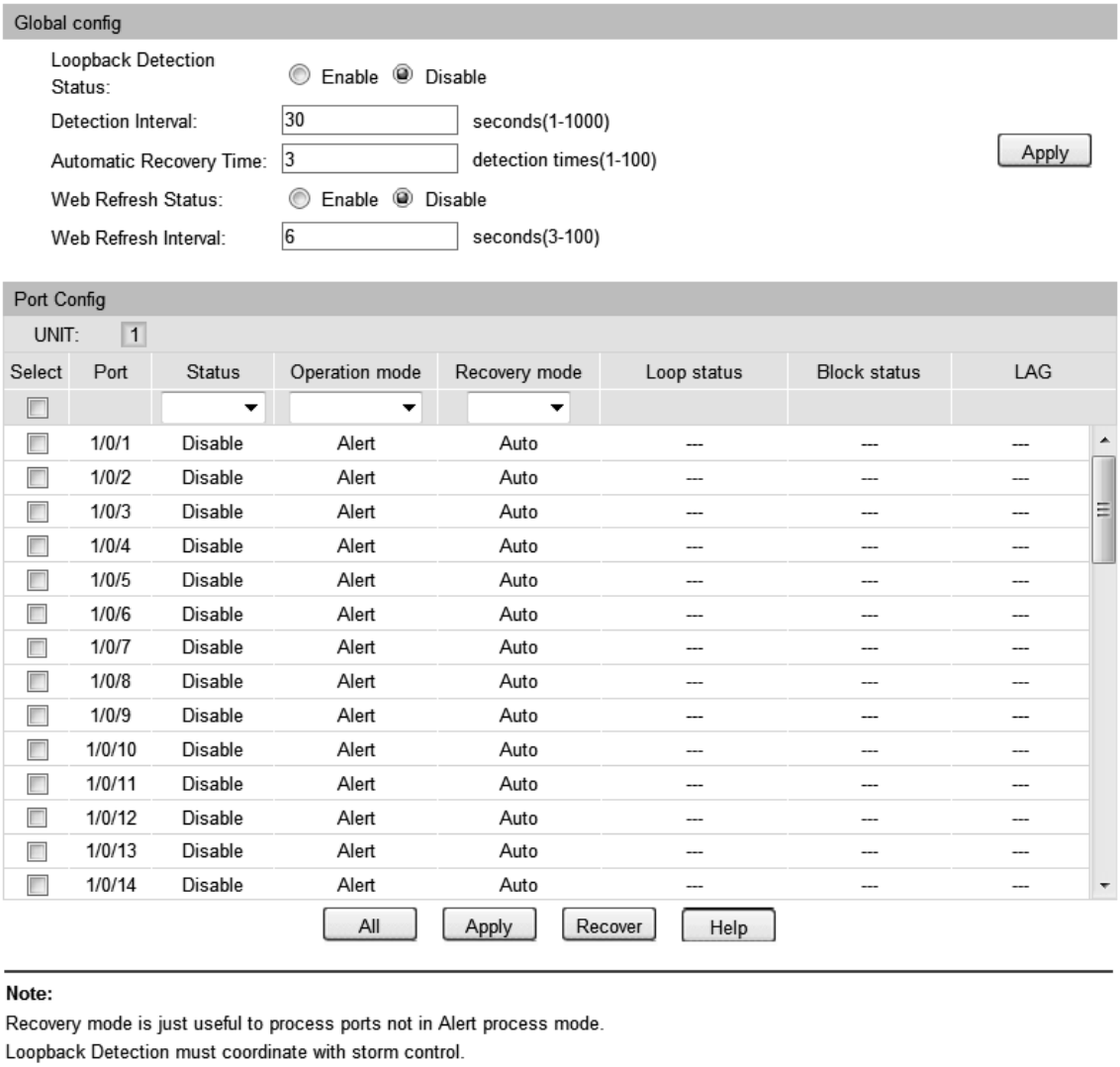


Figure 5-7 Loopback Detection Config

The following entries are displayed on this screen:

- **Global Config**

LoopbackDetection Status:	Here you can enable or disable Loopback Detection function globally.
Detection Interval:	Set a loopback detection interval between 1 and 1000 seconds. By default, it's 30 seconds.
Automatic Recovery Time:	Time after which the blocked port would automatically recover to normal status. It can be set as integral times of detection interval.
Web Refresh Status:	Here you can enable or disable web automatic refresh.
Web Refresh Interval:	Set a web refresh interval between 3 and 100 seconds. By default, it's 6 seconds.

➢ **Port Config**

Select:	Select the desired port for Loopback Detection configuration. It is multi-optional.
Port:	Displays the port number.
Status:	Enable or disable Loopback Detection function for the port.
Operation Mode:	Select the mode how the switch processes the detected loops. • Alert**:** When a loop is detected, display an alert. • Port based: When a loop is detected, display an alert and block the port.
Recovery Mode:	Select the mode how the blocked port recovers to normal status. • Auto: Block status can be automatically removed after recovery time. • Manual: Block status only can be removed manually.
Loop Status:	Displays the port status whether a loopback is detected.
Block Status:	Displays the port status about block or unblock.
LAG:	Displays the LAG number the port belongs to.
Recover:	Click the **Recover** button to manually remove the loop or block status of selected ports.

Note:

Loopback Detection must coordinate with storm control.

5.2 LAG

LAG (Link Aggregation Group) is to combine a number of ports together to make a single high-bandwidth data path, so as to implement the traffic load sharing among the member ports in the group and to enhance the connection reliability.

For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes **STP**, **QoS**, **VLAN**, **port attributes**, **MAC Address Learning mode** and other associated settings. More details are explained below:

- If the ports, which are enabled for the **802.1Q VLAN**, **STP**, **QoS** and **Port Configuration** (**Speed and Flow Control**), are in a LAG, their configurations would be the same as the LAG's.
- The ports, which are enabled for the **half-duplex**, **Port Security**, **Port Mirror** and **MAC Address Filtering**, cannot be added to the LAG.

If the LAG is needed, you are suggested to configure the LAG function here before configuring the other functions for the member ports.

Tips:

1. Calculate the bandwidth for a LAG: If a LAG consists of the four ports in the speed of 1000Mbps Full Duplex, the whole bandwidth of the LAG is up to 8000Mbps (2000Mbps * 4) because the bandwidth of each member port is 2000Mbps counting the up-linked speed of 1000Mbps and the down-linked speed of 1000Mbps.
2. The traffic load of the LAG will be balanced among the ports according to the Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.

The LAG function is implemented on the **LAG Table**, **Static LAG** and **LACP Config** configuration pages.

5.2.1 LAG Table

On this page, you can view the information of the current LAG of the switch.

Choose the menu **Switching→LAG→LAG Table** to load the following page.

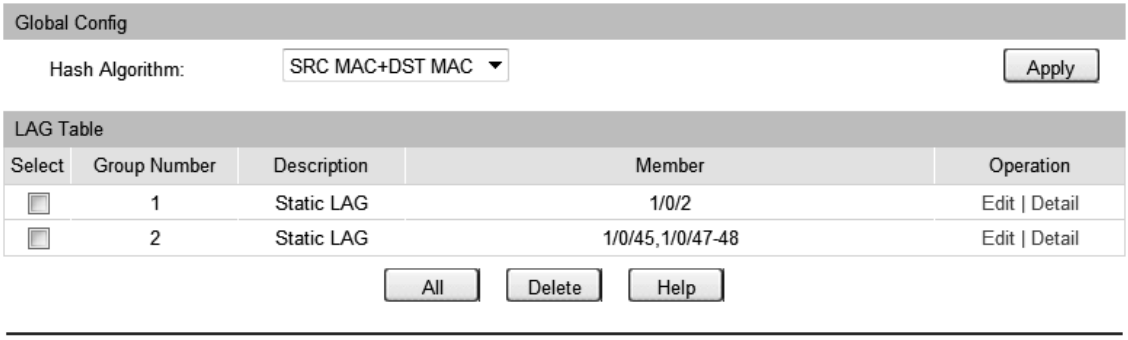


Figure 5-8 LAG Table

The following entries are displayed on this screen:

➢ **Global Config**

Hash Algorithm: Select the applied scope of Aggregate Arithmetic, which results in choosing a port to transfer the packets.

- **SRC MAC:** When this option is selected, the Aggregate Arithmetic will apply to the source MAC addresses of the packets.
- **DST MAC:** When this option is selected, the Aggregate Arithmetic will apply to the destination MAC addresses of the packets.
- **SRC MAC + DST MAC:** When this option is selected, the Aggregate Arithmetic will apply to the source and destination MAC addresses of the packets.
- **SRC IP:** When this option is selected, the Aggregate Arithmetic will apply to the source IP addresses of the packets.
- **DST IP:** When this option is selected, the Aggregate Arithmetic will apply to the destination IP addresses of

the packets.

- **SRC IP + DST IP:** When this option is selected, the Aggregate Arithmetic will apply to the source and destination IP addresses of the packets.

➢ **LAG Table**

Select: Select the desired LAG. It is multi-optional.

Group Number: Displays the LAG number here.

Description: Displays the description of LAG.

Member: Displays the LAG member.

Operation: Allows you to view or modify the information for each LAG.

- **Edit:** Click to modify the settings of the LAG.
- **Detail:** Click to get the information of the LAG.

Click the **Detail** button for the detailed information of your selected LAG.

Detail Info	
Group Number:	LAG1
LAG Type:	Static LAG
Port Status:	Enable
Speed:	Auto
Flow Control:	Disable
Ingress Bandwidth (bps):	--
Egress Bandwidth (bps):	--
Broadcast Control (bps):	--
Multicast Control (bps):	--
UL Control (bps):	--
QoS Priority:	CoS 0
Join VLAN:	1

Back

Figure 5-9 Detailed Information

5.2.2 Static LAG

On this page, you can manually configure the LAG.

Choose the menu **Switching→LAG→Static LAG** to load the following page.

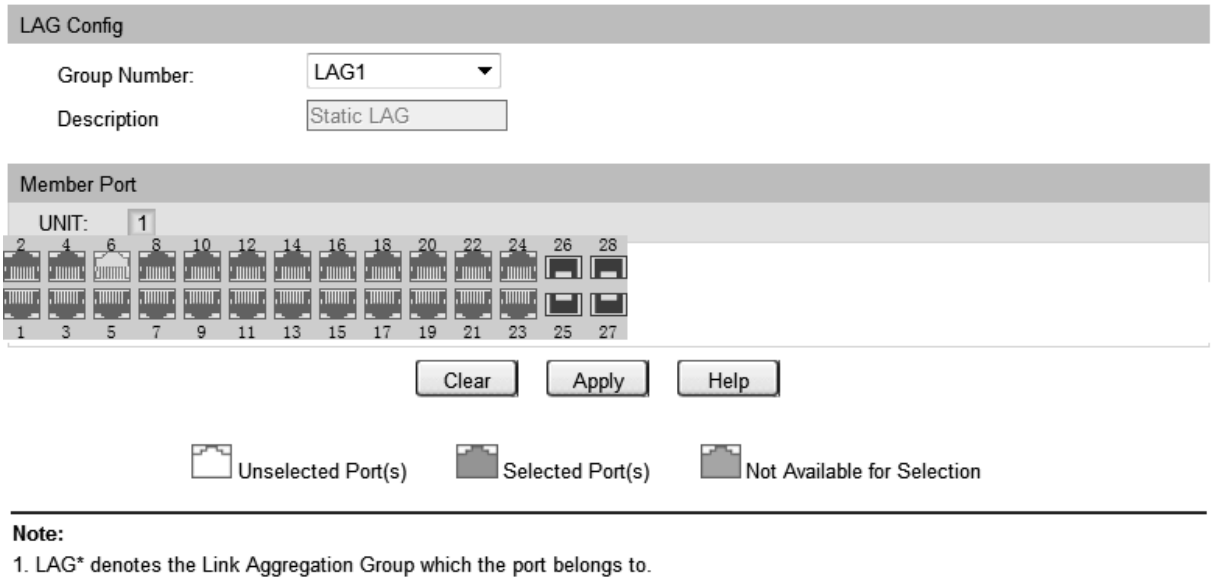


Figure 5-10 Manually Config

The following entries are displayed on this screen:

- **LAG Config**

  Group Number: Select a Group Number for the LAG.

  Description: Displays the description of the LAG.

- **Member Port**

  Member Port: Select the port as the LAG member. Clearing all the ports of the LAG will delete this LAG.

Tips:

1. The LAG can be deleted by clearing its all member ports.
2. A port can only be added to a LAG. If a port is the member of a LAG, the port number will be displayed in gray and cannot be selected.

5.2.3 LACP Config

LACP (Link Aggregation Control Protocol) is defined in IEEE802.3ad and enables the dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. The switch can dynamically group similarly configured ports into a single logical link, which will highly extend the bandwidth and flexibly balance the load.

With the LACP feature enabled, the port will notify its partner of the system priority, system MAC, port priority, port number and operation key (operation key is determined by the physical properties of the port, upper layer protocol and admin key). The device with higher priority will lead the aggregation and disaggregation. System priority and system MAC decide the priority of the device. The smaller the system priority, the higher the priority of the device is. With the same system priority, the device owning the smaller system MAC has the higher priority. The

device with the higher priority will choose the ports to be aggregated based on the port priority, port number and operation key. Only the ports with the same operation key can be selected into the same aggregation group. In an aggregation group, the port with smaller port priority will be considered as the preferred one. If the two port priorities are equal, the port with smaller port number is preferred. After an aggregation group is established, the selected ports can be aggregated together as one port to transmit packets.

On this page, you can configure the LACP feature of the switch.

Choose the menu **Switching→LAG→LACP Config** to load the following page.

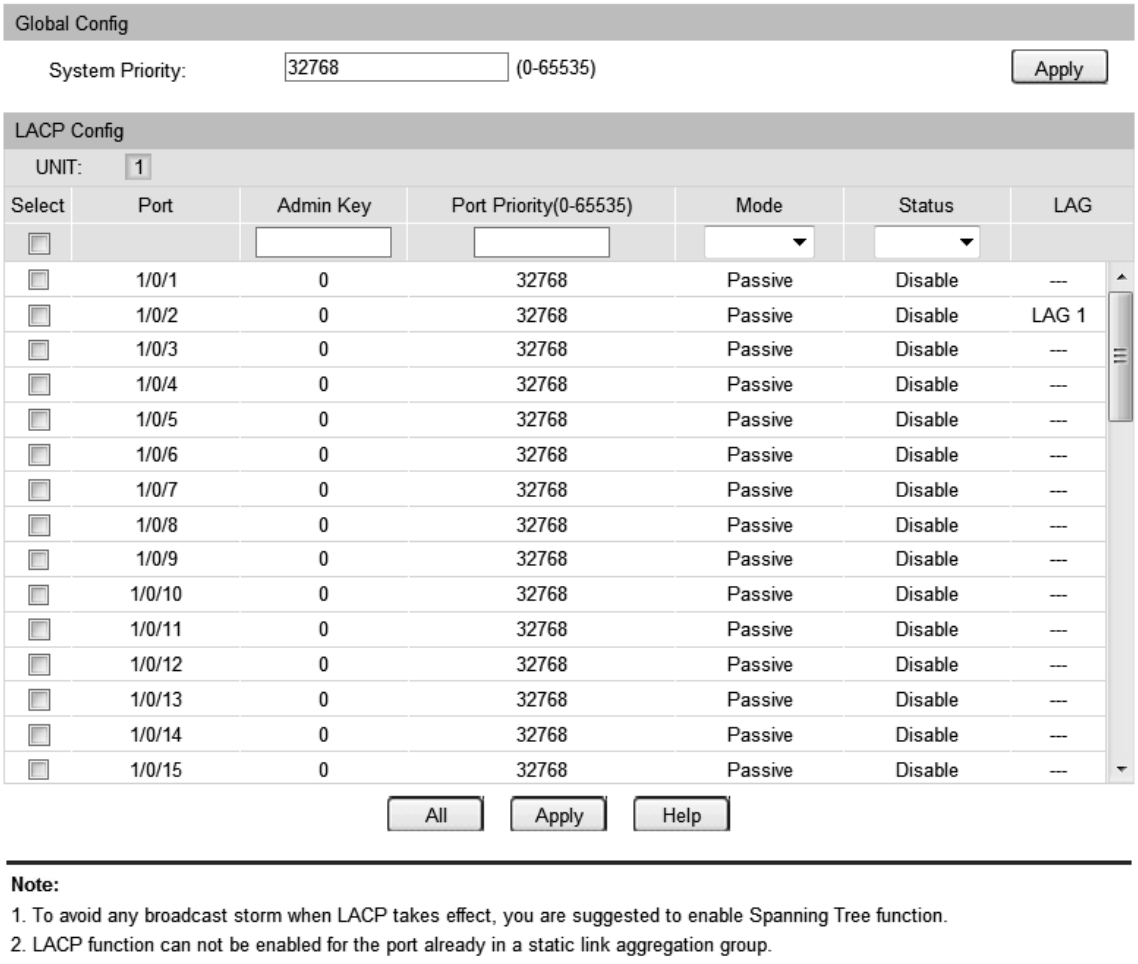


Figure 5-11 LACP Config

The following entries are displayed on this screen:

- **Global Config**

  System Priority: Specify the system priority for the switch. The system priority and MAC address constitute the system identification (ID). A lower system priority value indicates a higher system priority. When exchanging information between systems, the system with higher priority determines which link aggregation a link belongs to, and the system with lower priority adds the proper links to the link aggregation according to the selection of its partner.

- **LACP Config**

Select: Select the desired port for LACP configuration. It is multi-optional.

Port: Displays the port number.

Admin Key: Specify an Admin Key for the port. The member ports in a dynamic aggregation group must have the same Admin Key.

Port Priority: Specify a Port Priority for the port. This value determines the priority of the port to be selected as the dynamic aggregation group member. The port with smaller Port Priority will be considered as the preferred one. If the two port priorities are equal; the port with smaller port number is preferred.

Mode: Specify LACP mode for your selected port.

Status: Enable/Disable the LACP feature for your selected port.

LAG: Displays the LAG number which the port belongs to.

5.3 Traffic Monitor

The Traffic Monitor function, monitoring the traffic of each port, is implemented on the **Traffic Summary** and **Traffic Statistics** pages.

5.3.1 Traffic Summary

Traffic Summary screen displays the traffic information of each port, which facilitates you to monitor the traffic and analyze the network abnormity.

Choose the menu **Switching→Traffic Monitor→Traffic Summary** to load the following page.

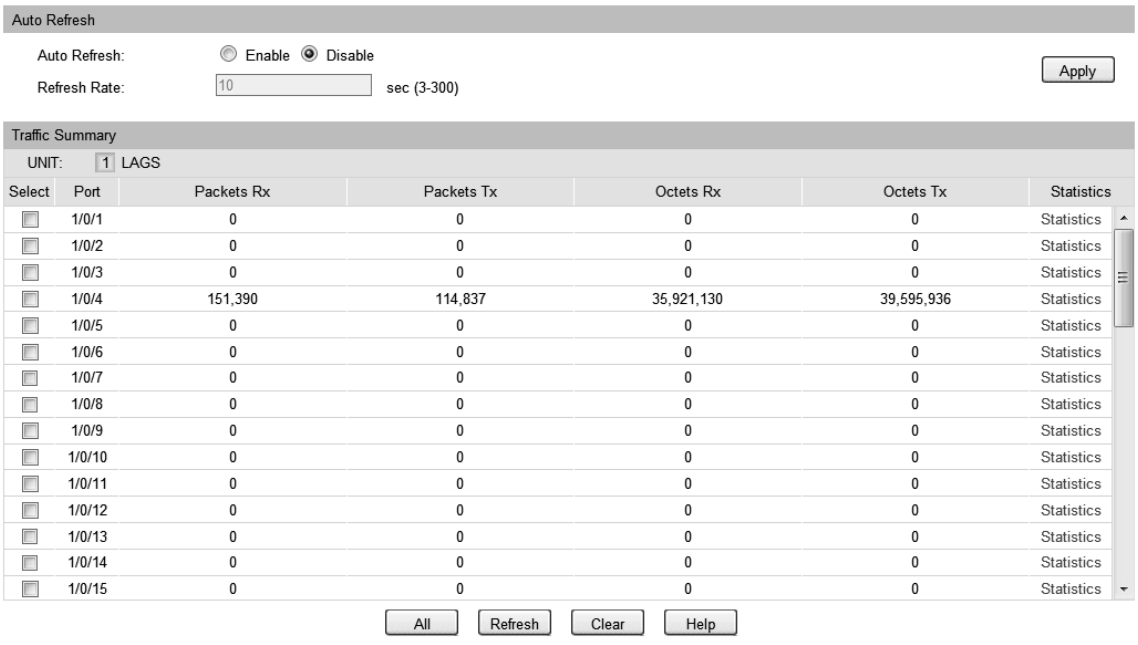


Figure 5-12 Traffic Summary

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Allows you to Enable/Disable refreshing the Traffic Summary automatically.

  Refresh Rate: Enter a value in seconds to specify the refresh interval.

- **Traffic Summary**

  UNIT:1/LAGS: Click **1** to show the information of the physical ports. Click **LAGS** to show the information of the link aggregation groups

  Select: Select the desired port for clearing. It is multi-optional.

  Port: Displays the port number.

  Packets Rx: Displays the number of packets received on the port. The error packets are not counted in.

  Packets Tx: Displays the number of packets transmitted on the port.

  Octets Rx: Displays the number of octets received on the port. The error octets are counted in.

  Octets Tx: Displays the number of octets transmitted on the port.

  Statistics: Click the **Statistics** button to view the detailed traffic statistics of the port.

5.3.2 Traffic Statistics

Traffic Statistics screen displays the detailed traffic information of each port, which facilitates you to monitor the traffic and locate faults promptly.

Choose the menu **Switching→Traffic Monitor→Traffic Statistics** to load the following page.

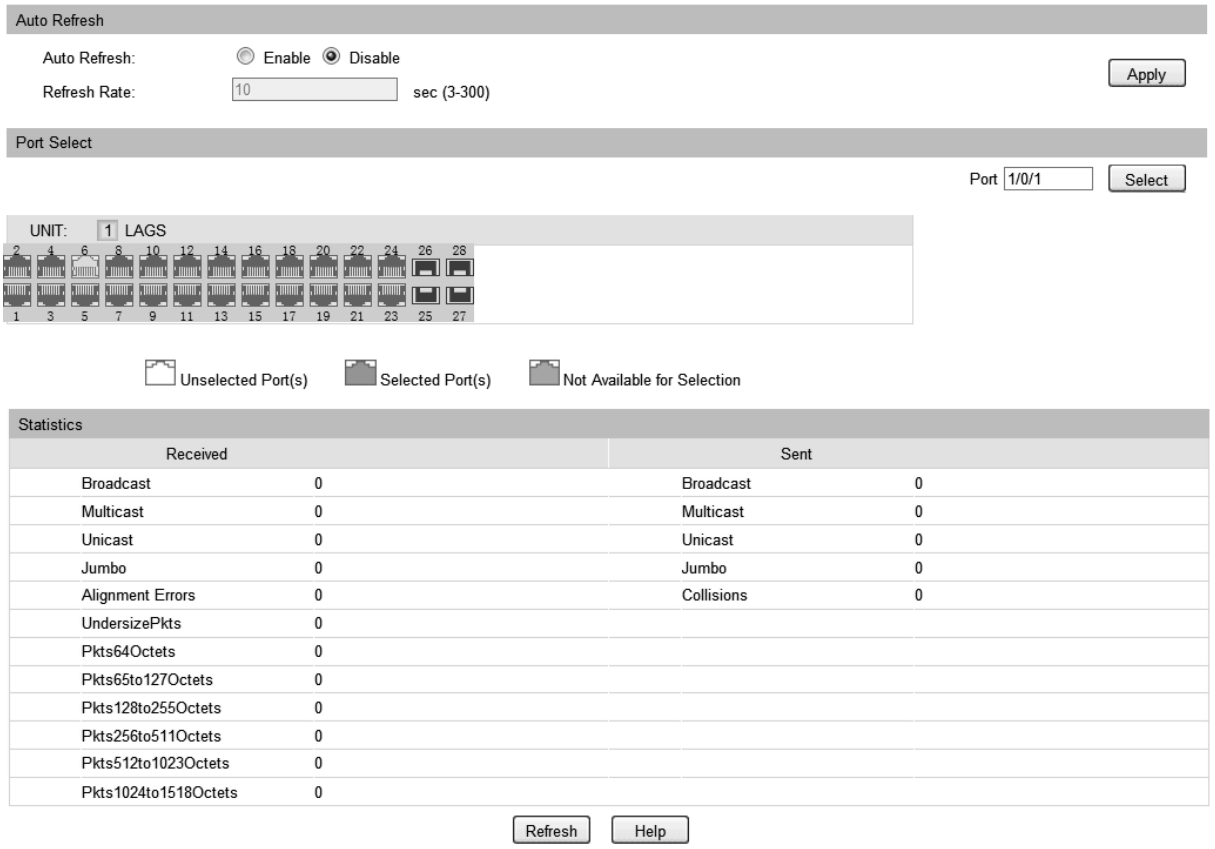


Figure 5-13 Traffic Statistics

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Allows you to Enable/Disable refreshing the Traffic Summary automatically.

  Refresh Rate: Enter a value in seconds to specify the refresh interval.

- **Port Select**

  UNIT:1/LAGS: Click **1** to show the information of the physical ports. Click **LAGS** to show the information of the link aggregation groups.

  Port: Select a desired port to view the traffic statistics from the port panel.

- **Statistics**

  Received: Displays the details of the packets received on the port.

  Sent: Displays the details of the packets transmitted on the port.

  Broadcast: Displays the number of good broadcast packets received or transmitted on the port. The error frames are not counted in.

  Multicast: Displays the number of good multicast packets received or transmitted on the port. The error frames are not counted in.

Unicast: Displays the number of good unicast packets received or transmitted on the port. The error frames are not counted in.

Jumbo: Displays the number of good jumbo packets received or transmitted on the port. The error frames are not counted in.

Alignment Errors: Displays the number of the received packets that have a bad Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The length of the packet is between 64 bytes and 1518 bytes.

UndersizePkts: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long.

Pkts64Octets: Displays the number of the received packets (including error packets) that are 64 bytes long.

Pkts65to127Octets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long.

Pkts128to255Octets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long.

Pkts256to511Octets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long.

Pkts512to1023Octets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long.

PktsOver1023Octets: Displays the number of the received packets (including error packets) that are over 1023 bytes.

Collisions: Displays the number of collisions experienced by a port during packet transmissions.

5.4 MAC Address

The main function of the switch is forwarding the packets to the correct ports based on the destination MAC address of the packets. Address Table contains the port-based MAC address information, which is the base for the switch to forward packets quickly. The entries in the Address Table can be updated by auto-learning or configured manually. Most entries are generated and updated by auto-learning. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and enhance the efficiency of packets forwarding remarkably. The address filtering feature allows the switch to filter the undesired packets and forbid its forwarding so as to improve the network security.

The types and the features of the MAC Address Table are listed as the following:

Type	**Configuration Way**	**Aging out**	**Being kept after reboot** (if the configuration is saved)	**Relationship between the bound MAC address and the port**
Static	Manually	No	Yes	The bound MAC address

Type	**Configuration Way**	**Aging out**	**Being kept after reboot** (if the configuration is saved)	**Relationship between the bound MAC address and the port**
Address Table	configuring			cannot be learned by the other ports in the same VLAN.
Dynamic Address Table	Automatically learning	Yes	No	The bound MAC address can be learned by the other ports in the same VLAN.
Filtering Address Table	Manually configuring	No	Yes	-

Table 5-1 Types and features of Address Table

This function includes four submenus: **Address Table**, **Static Address**, **Dynamic Address** and **Filtering Address**.

5.4.1 Address Table

On this page, you can view all the information of the Address Table.

Choose the menu **Switching→MAC Address→Address Table** to load the following page.

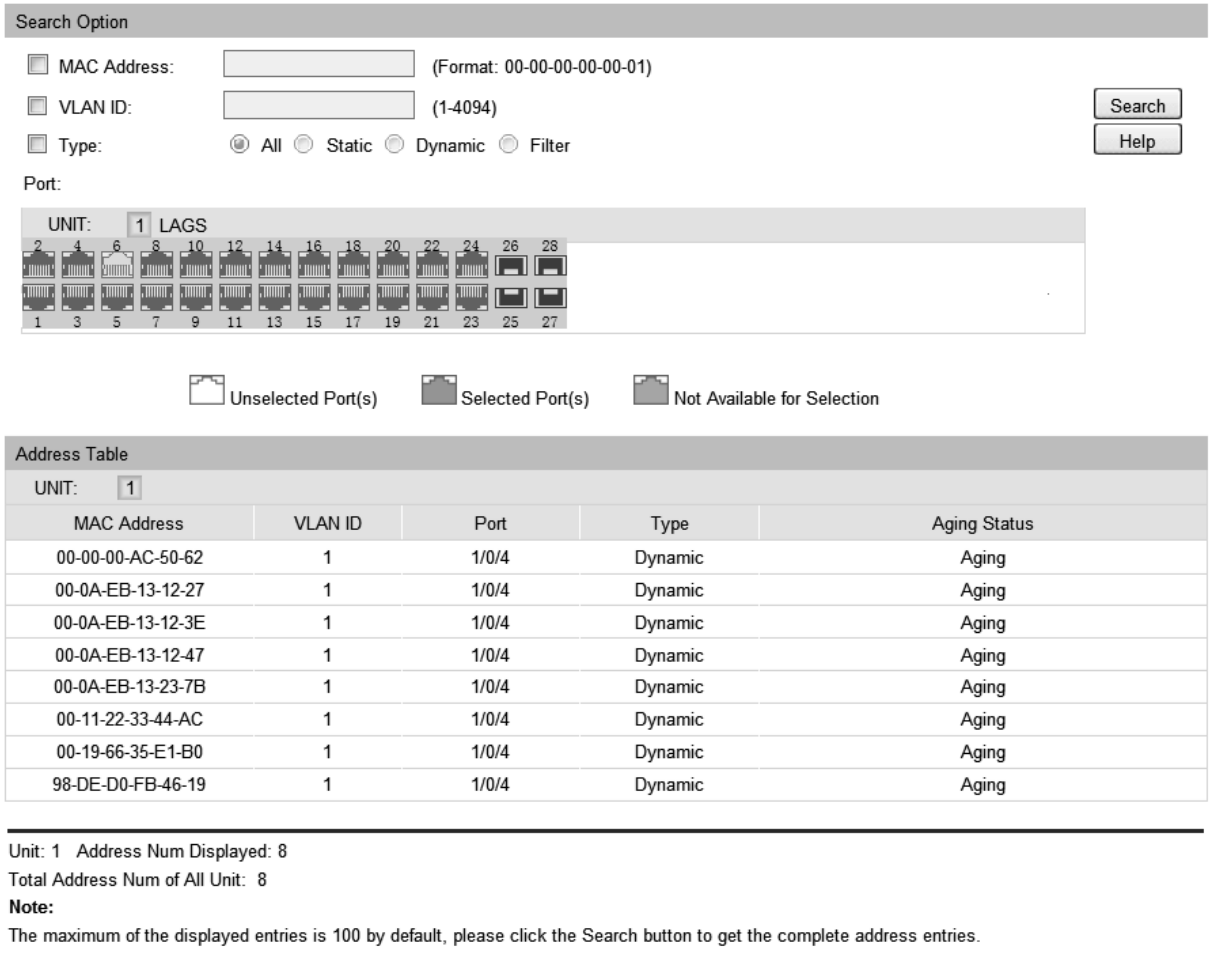


Figure 5-14 Address Table

The following entries are displayed on this screen:

- **Search Option**

  MAC Address: Enter the MAC address of your desired entry.

  VLAN ID: Enter the VLAN ID of your desired entry.

  Type: Select the type of your desired entry.

  - **All:** This option allows the address table to display all the address entries.
  - **Static:** This option allows the address table to display the static address entries only.
  - **Dynamic:** This option allows the address table to display the dynamic address entries only.
  - **Filter:** This option allows the address table to display the filtering address entries only.

  Port: Select the corresponding port number or LAG of your desired entry.

- **Address Table**

MAC Address: Displays the MAC address learned by the switch.

VLAN ID: Displays the corresponding VLAN ID of the MAC address.

Port: Displays the corresponding Port number of the MAC address.

Type: Displays the type of the MAC address.

Aging Status: Displays the aging status of the MAC address.

5.4.2 Static Address

The static address table maintains the static address entries which can be added or removed manually, independent of the aging time. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and remarkably enhance the efficiency of packets forwarding without learning the address. The static MAC address learned by the port with **Port Security** enabled in the static learning mode will be displayed in the Static Address Table.

Choose the menu **Switching→MAC Address→Static Address** to load the following page.

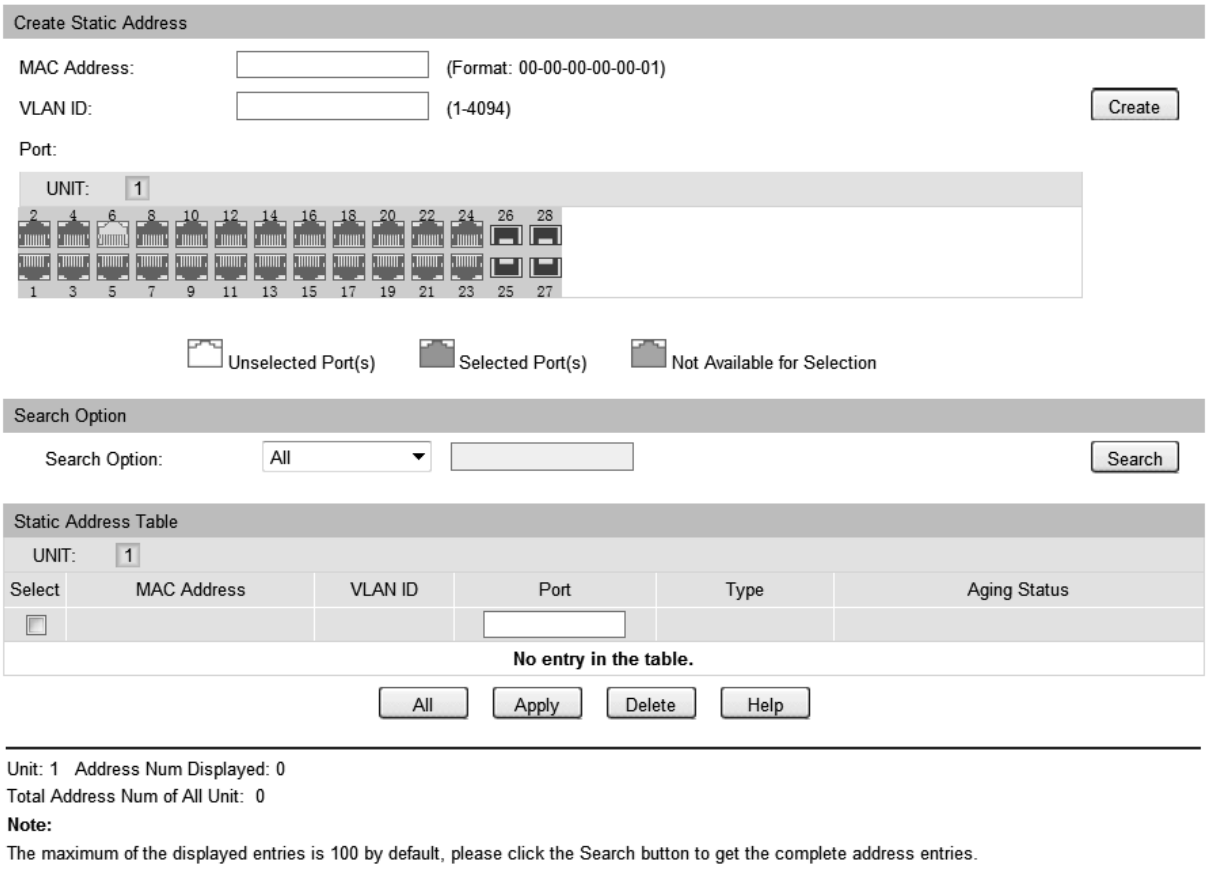


Figure 5-15 Static Address

The following entries are displayed on this screen:

➢ **Create Static Address**

MAC Address: Enter the static MAC Address to be bound.

VLAN ID: Enter the corresponding VLAN ID of the MAC address.

Port: Select the corresponding port of your desired entry.

➢ **Search Option**

Search Option: Select a Search Option from the pull-down list and click the **Search** button to find your desired entry in the Static Address Table.

- **MAC:** Enter the MAC address of your desired entry.
- **VLAN ID:** Enter the VLAN ID number of your desired entry.
- **Port:** Enter the Port number of your desired entry.

➢ **Static Address Table**

Select: Select the entry to delete or modify the corresponding port number. It is multi-optional.

MAC Address: Displays the static MAC Address.

VLAN ID: Displays the corresponding VLAN ID of the MAC address.

Port: Displays the corresponding port number of the MAC address. Here you can modify the port number to which the MAC address is bound. The new port should be in the same VLAN.

Type: Displays the type of the MAC address.

Aging Status: Displays the aging status of the MAC address.

Note:

1. If the corresponding port number of the MAC address is not correct, or the connected port (or the device) has been changed, the switch cannot forward the packets correctly. Please reset the static address entry appropriately.
2. If the MAC address of a device has been added to the Static Address Table, connecting the device to another port will cause its address not to be recognized dynamically by the switch. Therefore, please ensure the entries in the Static Address Table are correct and valid.
3. The MAC address in the Static Address Table cannot be added to the Filtering Address Table or bound to a port dynamically.

5.4.3 Dynamic Address

The dynamic address can be generated by the auto-learning mechanism of the switch. The Dynamic Address Table can update automatically by auto-learning or the MAC address aging out mechanism.

To fully utilize the MAC address table, which has a limited capacity, the switch adopts an aging mechanism for updating the table. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time.

On this page, you can configure the dynamic MAC address entry.

Choose the menu **Switching→MAC Address→Dynamic Address** to load the following page.

Figure 5-16 Dynamic Address

The following entries are displayed on this screen:

➢ **Aging Config**

Auto Aging: Allows you to Enable/Disable the Auto Aging feature.

Aging Time: Enter the Aging Time for the dynamic address.

➢ **Search Option**

Search Option: Select a Search Option from the pull-down list and click the **Search** button to find your desired entry in the Dynamic Address Table.

- **MAC:** Enter the MAC address of your desired entry.
- **VLAN ID:** Enter the VLAN ID number of your desired entry.
- **Port:** Enter the Port number of your desired entry.

➢ **Dynamic Address Table**

Select: Select the entry to delete the dynamic address or to bind the MAC address to the corresponding port statically. It is multi-optional.

MAC Address: Displays the dynamic MAC Address.

VLAN ID: Displays the corresponding VLAN ID of the MAC address.

Port: Displays the corresponding port number of the MAC address.

Type: Displays the type of the MAC address.

Aging Status: Displays the aging status of the MAC address.

Bind: Click the **Bind** button to bind the MAC address of your selected entry to the corresponding port statically.

Tips:

Setting aging time properly helps implement effective MAC address aging. The aging time that is too long or too short results in a decrease of the switch performance. If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from updating with network changes in time. If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch. It is recommended to keep the default value.

5.4.4 Filtering Address

The filtering address is to forbid the undesired packets to be forwarded. The filtering address can be added or removed manually, independent of the aging time. The filtering MAC address allows the switch to filter the packets which includes this MAC address as the source address or destination address, so as to guarantee the network security. The filtering MAC address entries act on all the ports in the corresponding VLAN.

Choose the menu **Switching→MAC Address→Filtering Address** to load the following page.

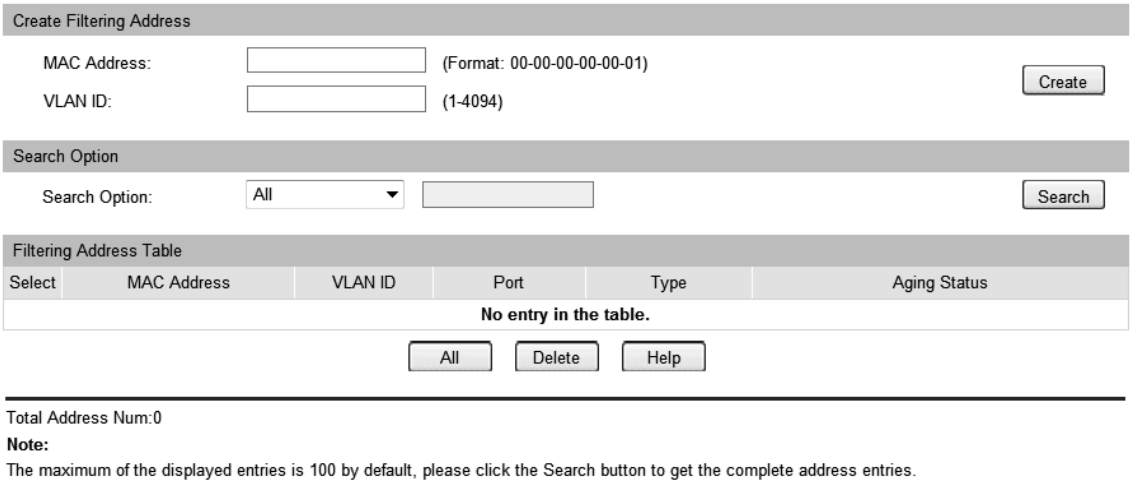


Figure 5-17 Filtering Address

The following entries are displayed on this screen:

- **Create Filtering Address**

  MAC Address: Enter the MAC Address to be filtered.

  VLAN ID: Enter the corresponding VLAN ID of the MAC address.

- **Search Option**

  Search Option: Select a Search Option from the pull-down list and click the **Search** button to find your desired entry in the Filtering Address Table.

  - **MAC Address:** Enter the MAC address of your desired entry.

- **VLAN ID:** Enter the VLAN ID number of your desired entry.

➢ **Filtering Address Table**

Select:	Select the entry to delete the corresponding filtering address. It is multi-optional.
MAC Address:	Displays the filtering MAC Address.
VLAN ID:	Displays the corresponding VLAN ID.
Port:	Here the symbol "--" indicates no specified port.
Type:	Displays the type of the MAC address.
Aging Status:	Displays the aging status of the MAC address.

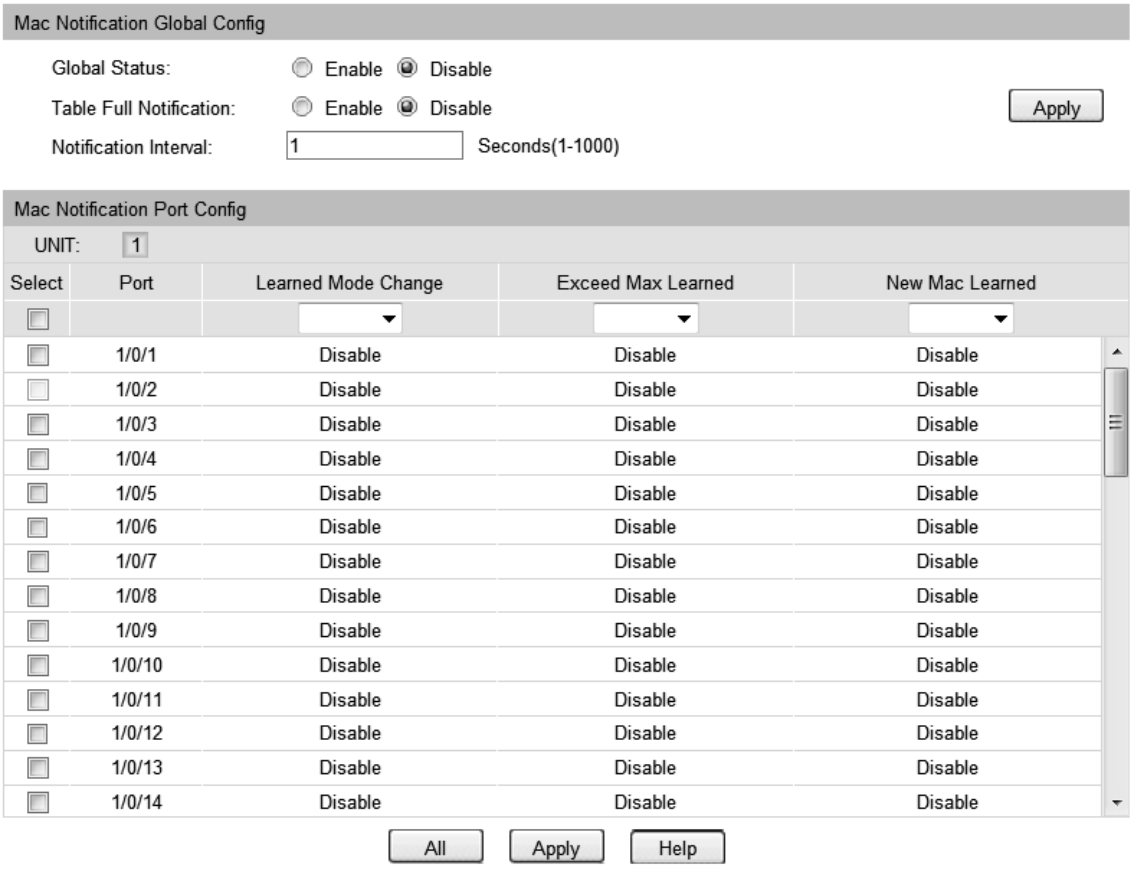
Note:

The MAC address in the Filtering Address Table cannot be added to the Static Address Table or bound to a port dynamically.

5.4.5 MAC Notification

The MAC notification function is used to monitor the status of the MAC address table, and the MAC address learned on each port.

Choose the menu **Switching→MAC Address→MAC Notification** to load the following page.



The following entries are displayed on this screen:

- **MAC Notification Global Config**

Global Status:	Enable/Disable the MAC notification globally.
Table Full Notification:	Enable/Disable the sending of a MAC Full Notification when the MAC address table is full.
Notification Interval:	Specify the interval time between notifications. It ranges from 1 to 1000 seconds and the default interval is 1 second.

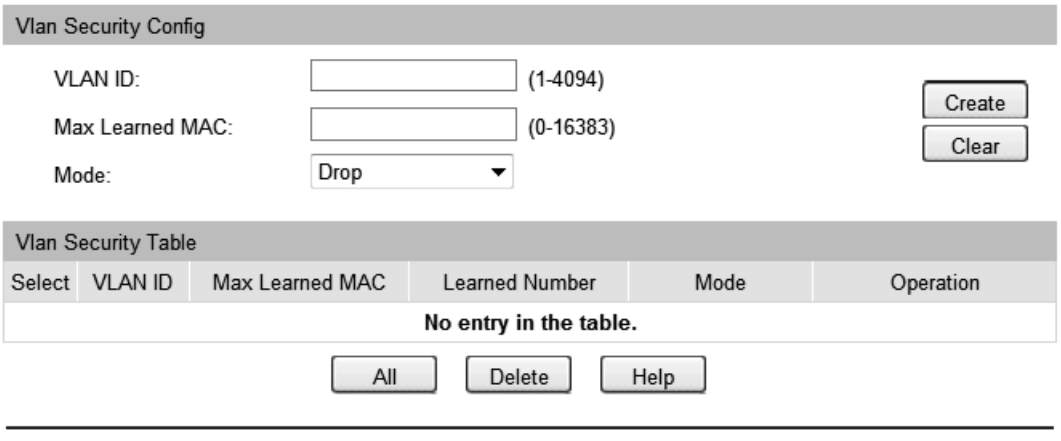
- **MAC Notification Port Config**

Select:	Select the specified port(s) for configuration. It is multi-optional.
Port:	Displays the port number.
Learned Mode Change:	Enable/Disable the Learned Mode Change notification on the port. The port's learned mode includes: Dynamic, Static and Permanent.
Exceed Max Learned:	Enable/Disable the Exceed Max Learned notification on the port. The number of the max learned MAC addresses on each port is 64 by default.
New MAC Learned:	Enable/Disable the New MAC Learned notification on the port.

5.4.6 MAC VLAN Security

The MAC VLAN Security function is used to configure the MAC address security in the specified VLAN.

Choose the menu **Switching→MAC Address→MAC VLAN Security** to load the following page.



The following entries are displayed on this screen:

- **MAC Notification Global Config**

VLAN ID:	Enter the VLAN ID to configure its MAC address security.

Max Learned MAC:	Specify the max MAC addresses that can be learned in this VLAN.
Mode:	Choose the mode to process the new arrival packets (whose source MAC address is not in the current VLAN's address table) when learned MAC number exceeds the max learned MAC number of VLAN security entry. • Drop: The packets will be dropped when learned mac number exceeds the max learned number of VLAN security entry. • Forward: The packets will be forward but not be learned when learned mac number exceeds the max learned number of VLAN security entry. • Disable: The vlan security entry exists, but is not valid.

➢ **VLAN Security Table**

Select:	Select the desired entry to delete the corresponding VLAN security entry. It's multi-optional.
VLAN ID:	Displays the VLAN ID of the VLAN security entry.
Max Learned MAC:	Displays the max learned MAC number of VLAN security entry.
Learned Number:	Displays the learned MAC number of VLAN security entry.
Mode:	Displays the mode of the vlan security entry.
Operation:	Click to edit the max learned MAC and the mode.

5.5 L2TP

L2TP (Layer 2 Tunneling Protocol) is a feature for service providers to transmit packets from different customers across their ISP networks and maintain Layer 2 protocol configurations of each customer. The supported Layer 2 protocols are STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) and PVST+(Per VLAN Spanning Tree Plus).

When L2TP is enabled and the switch receives the specified Layer 2 protocol packets from the UNI port, the switch encapsulates these packets with a special MAC address and sends them across the service-provider network through the NNI port. The devices in the ISP network do not process these packets but forward them as normal packets. The switch on the outbound side of the ISP network receives these packets on its NNI port and restore their MAC address to their original Layer 2 protocol destination MAC address.

The L2TP protocol is usually used with VLAN VPN feature. Thus the NNI ports that connecting to the ISP network are configured as VPN Up-link ports.

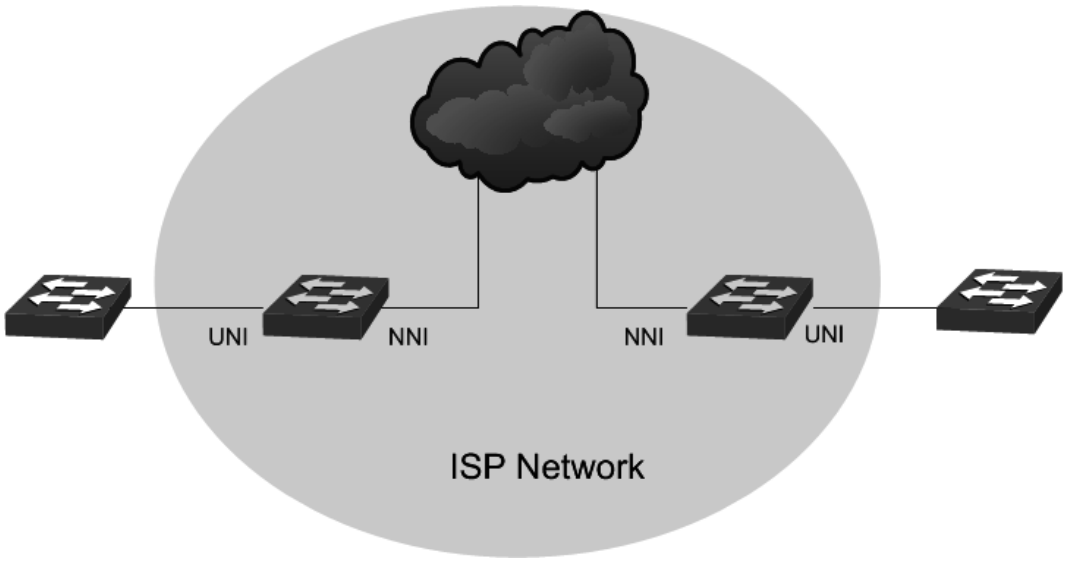


Figure 5-1 A Typical L2TP Topology

5.5.1 L2TP Config

Choose the menu **Switching→L2TP→L2TP Config** to load the following page.

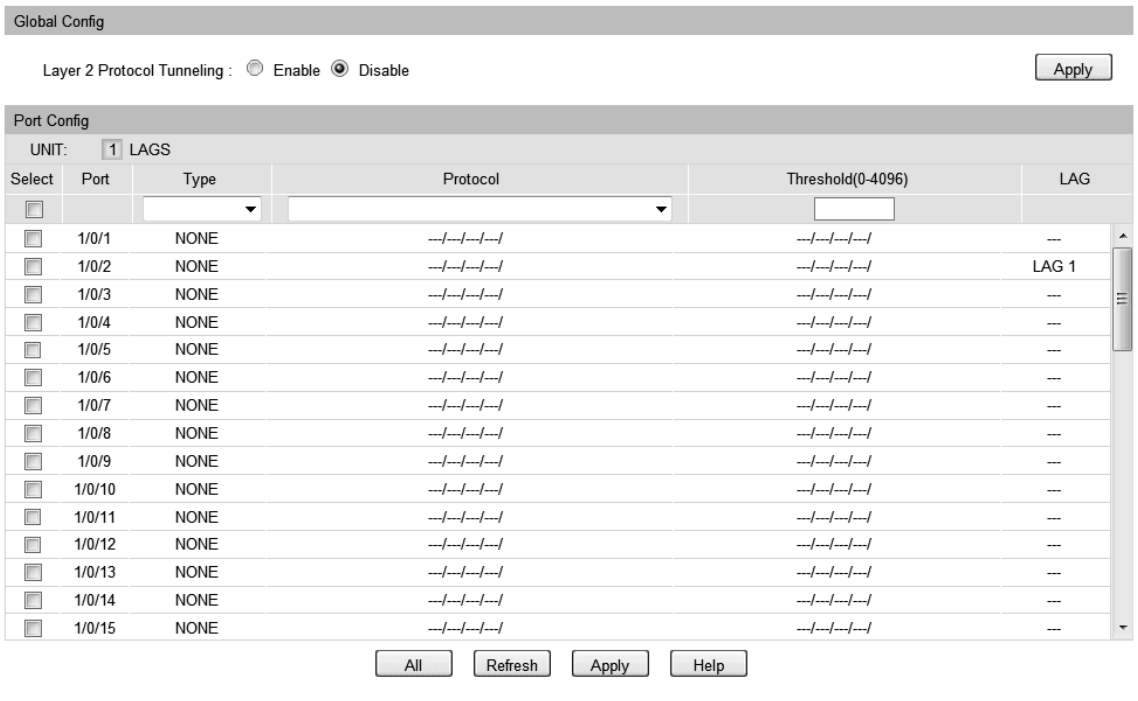


Figure 5-2 L2TP Config

Configuration Procedure:

1) Enable the Layer 2 Tunneling Protocol globally under **Global Config**.
2) Configure the tunneling and protocol type on the speicified port under **Port Config**.
3) Click **Apply** to save your configurations.

Entry Explannation:

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Specify the port(s) to configure its L2TP feature. It is multi-optional.

Type: Choose the port type according to its connecting device in the network.

- None: Disable the L2TP on this port.
- UNI: Specify the port's type as UNI if it is connecting to the user's local network.
- NNI: Specify the port's type as NNI if it is connecting to the ISP network.

Protocol: Select the supported Layer 2 protocol type. Packets of the specified protocol will be encapsulated with their destination MAC address before they are sent to the ISP network. Packets will be decapsulated to restore their Layer 2 protocol and MAC address information before they are sent to the customer network.

- STP: Enable protocol tunneling for the STP packets.
- GVRP: Enable protocol tunneling for the GVRP packets.
- 01000CCCCCCC: Enable protocol tunneling for the packets with their destination MAC address as 01000CCCCCCC, which includes CDP, VTP, PAgP and UDLD.
- 01000CCCCCCD: Enable protocol tunneling for the PVST+ packets.
- ALL: All the above Layer 2 protocols are supported for tunneling.

Threshold Configure the threshold for packets-per-second accepted for encapsulation. Packets beyond the threshold will be dropped. If no protocol is specified, the threshold applies to each Layer 2 protocol types.

LAG: Displays the port's aggregation group.

Return to CONTENTS

Chapter 6 VLAN

The traditional Ethernet is a data network communication technology based on CSMA/CD (Carrier Sense Multiple Access/Collision Detect) via shared communication medium. Through the traditional Ethernet, the overfull hosts in LAN will result in serious collision, flooding broadcasts, poor performance or even breakdown of the Internet. Though connecting the LANs through switches can avoid the serious collision, the flooding broadcasts cannot be prevented, which will occupy plenty of bandwidth resources, causing potential serious security problems.

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. The VLAN technology is developed for switches to control broadcast in LANs. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with one another as if they are in a LAN. However, hosts in different VLANs cannot communicate with one another directly. Therefore, broadcast packets are limited in a VLAN. Hosts in the same VLAN communicate with one another via Ethernet whereas hosts in different VLANs communicate with one another through the Internet devices such as router, the Layer 3 switch, etc. The following figure illustrates a VLAN implementation.

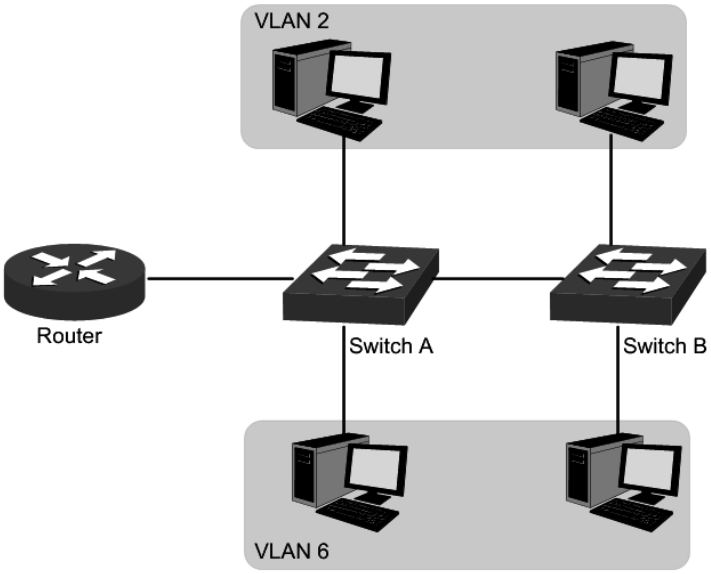


Figure 6-1 VLAN implementation

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

(1) Broadcasts are confined to VLANs. This decreases bandwidth utilization and improves network performance.

(2) Network security is improved. VLANs cannot communicate with one another directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 switches are used.

(3) Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you do not need to change its network configuration.

A VLAN can span across multiple switches, or even routers. This enables hosts in a VLAN to be dispersed in a looser way. That is, hosts in a VLAN can belong to different physical network segments. This switch supports 802.1Q VLAN to classify VLANs. VLAN tags in the packets are necessary for the switch to identify packets of different VLANs.

6.1 802.1Q VLAN

VLAN tags in the packets are necessary for the switch to identify packets of different VLANs. The switch works at the data link layer in OSI model and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into the data link layer encapsulation for identification.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

As shown in the following figure, a VLAN tag contains four fields, including TPID (Tag Protocol Identifier), Priority, CFI (Canonical Format Indicator), and VLAN ID.

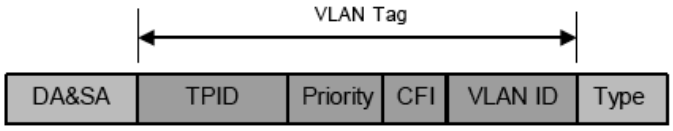


Figure 6-2 Format of VLAN Tag

(1) TPID: TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in this switch.

(2) Priority: Priority is a 3-bit field, referring to 802.1p priority. Refer to section "QoS & QoS profile" for details.

(3) CFI: CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.

(4) VLAN ID: VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When the switch receives a un-VLAN-tagged packet, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission.

In this User Guide, the tagged packet refers to the packet with VLAN tag whereas the untagged packet refers to the packet without VLAN tag, and the priority-tagged packet refers to the packet with VLAN tag whose VLAN ID is 0.

➢ **Link Types of ports**

When creating the 802.1Q VLAN, you should set the link type for the port according to its connected device. The link types of port including the following two types: **Untagged** and **Tagged**.

(1) **Untagged:** The untagged port can be added in multiple VLANs. If a VLAN-tagged packet arrives at a port and the VLAN ID in its VLAN tag does not match any of the VLAN the ingress port belongs to, this packet will be dropped. The packets forwarded by the untagged port are untagged.

(2) **Tagged:** The tagged port can be added in multiple VLANs. If a VLAN-tagged packet arrives at a port and the VLAN ID in its VLAN tag does not match any of the VLAN the ingress port belongs to, this packet will be dropped. When the VLAN-tagged packets are forwarded by the Tagged port, its VLAN tag will not be changed.

➢ **PVID**

PVID (Port VLAN ID) is the default VID of the port. When the switch receives an un-VLAN-tagged packet, it will add a VLAN tag to the packet according to the PVID of its received port and forward the packets.

When creating VLANs, the PVID of each port, indicating the default VLAN to which the port belongs, is an important parameter with the following two purposes:

(1) When the switch receives an un-VLAN-tagged packet, it will add a VLAN tag to the packet according to the PVID of its received port

(2) PVID determines the default broadcast domain of the port, i.e. when the port receives UL packets or broadcast packets, the port will broadcast the packets in its default VLAN.

Different packets, tagged or untagged, will be processed in different ways, after being received by ports of different link types, which is illustrated in the following table.

<table>
<tr><th rowspan="2">Port Type</th><th colspan="2">Receiving Packets</th><th colspan="2">Forwarding Packets</th></tr>
<tr><th>Untagged Packets</th><th>Tagged Packets</th><th>Untagged Packets</th><th>Tagged Packets</th></tr>
<tr><td>Untagged</td><td rowspan="2">When untagged packets are received, the port will add the default VLAN tag, i.e. the PVID of the ingress port, to the packets.</td><td rowspan="2">If the VID of packet is allowed by the port, the packet will be received.
If the VID of packet is forbidden by the port, the packet will be dropped.</td><td>The packet will be forwarded unchanged.</td><td>The packet will be forwarded after removing its VLAN tag</td></tr>
<tr><td>Tagged</td><td>The packet will be forwarded with the PVID of egress port as its VLAN tag.</td><td>The packet will be forwarded with its current VLAN tag.</td></tr>
</table>

Table 6-1 Relationship between Port Types and VLAN Packets Processing

IEEE 802.1Q VLAN function is implemented on the **VLAN Config** and **Port Config** pages.

6.1.1 VLAN Config

On this page, you can configure the 802.1Q VLAN and its ports.

Choose the menu **VLAN→802.1Q VLAN→VLAN Config** to load the following page.

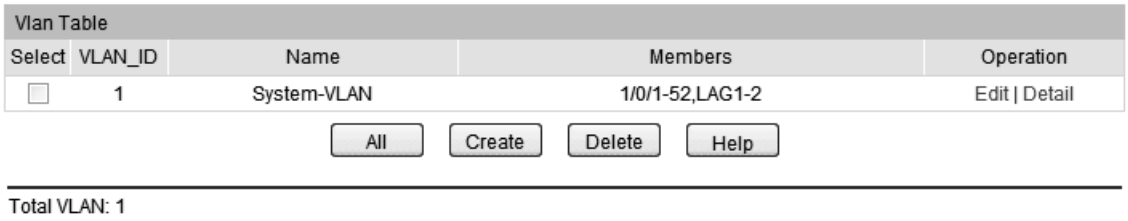


Figure 6-3 VLAN Table

To ensure the normal communication of the factory switch, the default VLAN of all ports is set to VLAN1.

The following entries are displayed on this screen:

- **VLAN Table**

Select:	Select the desired entry to delete the corresponding VLAN. It is multi-optional.
VLAN ID:	Displays the VLAN ID.
Name:	Displays the name of the specific VLAN.
Members:	Displays the port members in the VLAN.
Operation:	Allows you to view or modify the information for each entry. • **Edit:** Click to modify the settings of VLAN. • **Detail**: Click to get the information of VLAN.

Click **Edit** and the following content will be shown.

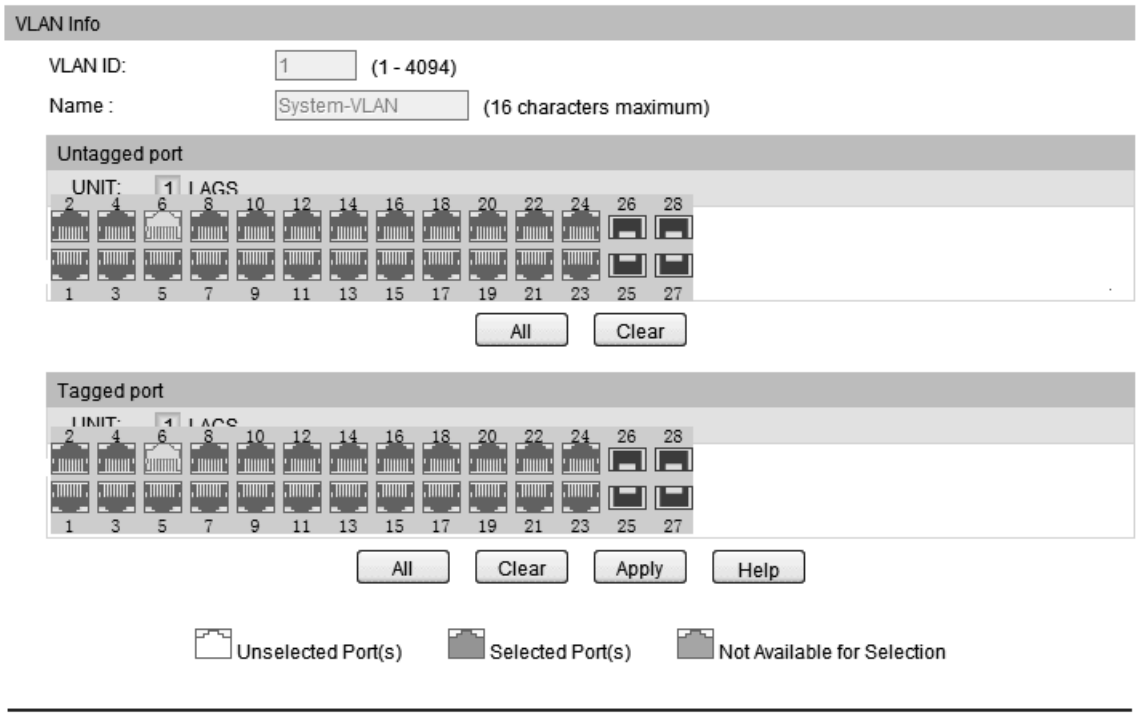


Figure 6-4 VLAN Info

- **VLAN Info**

VLAN ID:	Displays the ID number of VLAN.
Name:	Displays the name of the specific VLAN.
Untagged Port:	Displays the untagged ports of the specific VLAN.
Tagged Port:	Displays the tagged ports of the specific VLAN.

6.1.2 Port Config

Before creating the 802.1Q VLAN, please acquaint yourself with all the devices connected to the switch in order to configure the ports properly.

Choose the menu **VLAN→802.1Q VLAN→Port Config** to load the following page.

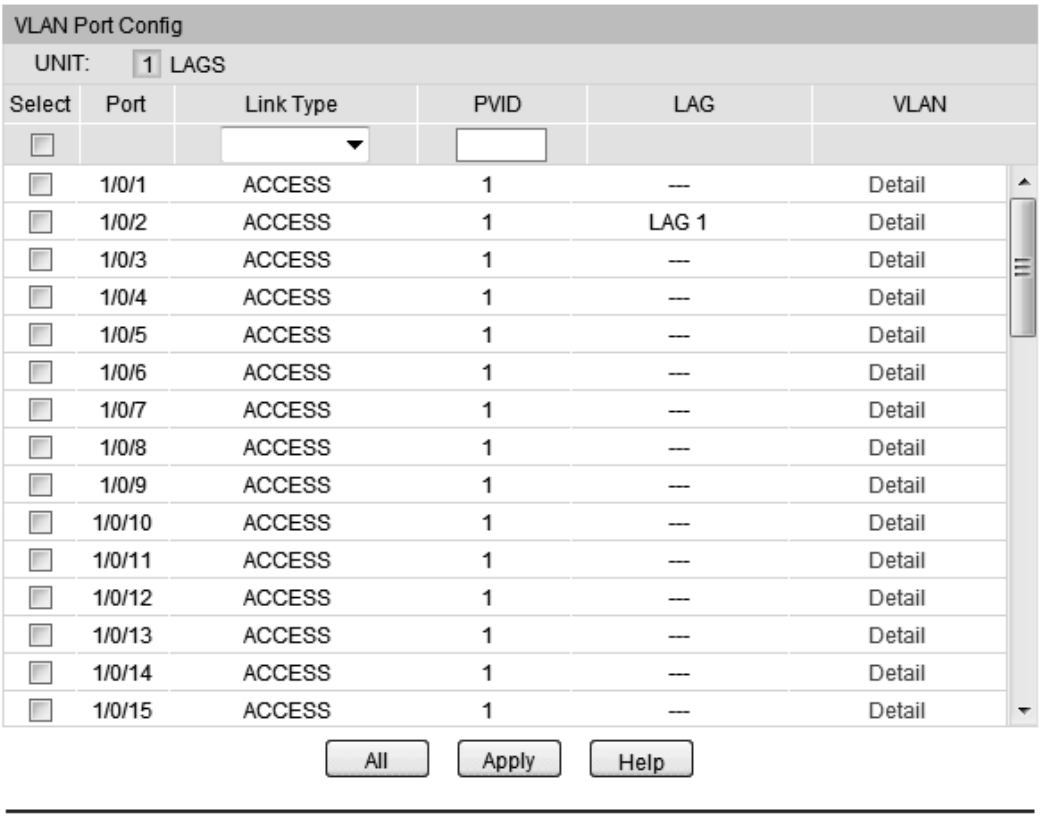


Figure 6-5 Port Config

The following entries are displayed on this screen:

- **VLAN Port Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired port for configuration. It is multi-optional.

Port: Displays the port number.

Link Type: Select the Link Type from the pull-down list for the port.

- **ACCESS:** The ACCESS port can be added in a single VLAN, and the egress rule of the port is UNTAG. The PVID is same as the current VLAN ID. If the current VLAN is deleted, the PVID will be set to 1 by default.
- **TRUNK:** The TRUNK port can be added in multiple VLANs. The egress rule of the port is UNTAG if the arriving packet's VLAN tag is the same as the port's PVID, otherwise the egress rule is TAG. The PVID can be set as the VID number of any valid VLAN.
- **GENERAL:** The GENERAL port can be added in multiple VLANs and set various egress rules according to the different VLANs. The default egress rule is UNTAG. The PVID can be set as the VID number of any valid VLAN.

PVID: Enter the PVID number of the port.

LAG: Displays the LAG to which the port belongs.

VLAN: Click the **Detail** button to view the information of the VLAN to which the port belongs.

Click the **Detail** button to view the information of the corresponding VLAN.

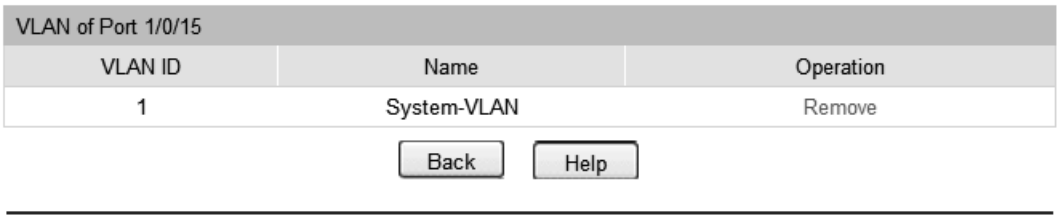


Figure 6-6 View the Current VLAN of Port

The following entries are displayed on this screen:

➢ **VLAN of Port**

VLAN ID: Displays the ID number of VLAN.

Name: Displays the user-defined description of VLAN.

Operation: Allows you to remove the port from the current VLAN.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected device.
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its

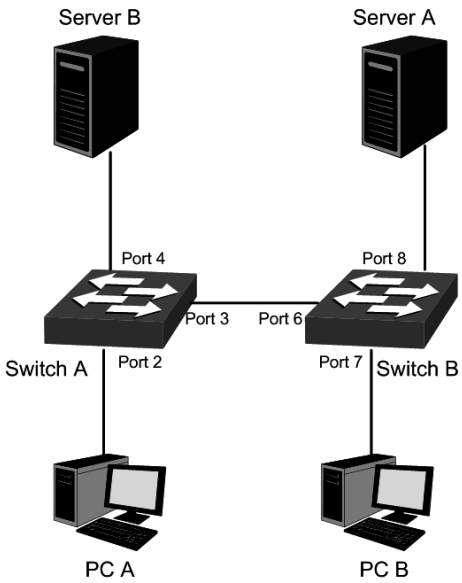
Step	Operation	Description
		member ports.
3	Modify/View VLAN.	Optional. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Edit/Detail** button to modify/view the information of the corresponding VLAN.
4	Delete VLAN	Optional. On the **VLAN→802.1Q VLAN→VLAN Config** page, select the desired entry to delete the corresponding VLAN by clicking the **Delete** button.

6.2 Application Example for 802.1Q VLAN

➢ **Network Requirements**

- Switch A is connecting to PC A and Server B;
- Switch B is connecting to PC B and Server A;
- PC A and Server A is in the same VLAN;
- PC B and Server B is in the same VLAN;
- PCs in the two VLANs cannot communicate with each other.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 2, Port 3 and Port 4 as ACCESS, TRUNK and ACCESS respectively

2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 2 and Port 3.
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 3 and Port 4.

- Configure switch B

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 7, Port 6 and Port 8 as ACCESS, TRUNK and ACCESS respectively.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 6 and Port 8.
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 6 and Port 7.

6.3 MAC VLAN

MAC VLAN technology is the way to classify VLANs according to the MAC addresses of Hosts. A MAC address corresponds to a single VLAN ID. For the device in a MAC VLAN, if its MAC address is bound to VLAN, the device can be connected to another member port in this VLAN and still takes its member role effect without changing the configuration of VLAN members.

The packet in MAC VLAN is processed in the following way:

- When receiving an untagged packet, the switch matches the packet with the current MAC VLAN. If the packet is matched, the switch will add a corresponding MAC VLAN tag to it. If no MAC VLAN is matched, the switch will add a tag to the packet according to the PVID of the received port. Thus, the packet is assigned automatically to the corresponding VLAN for transmission.
- When receiving tagged packet, the switch will process it basing on the 802.1Q VLAN. If the received port is the member of the VLAN to which the tagged packet belongs, the packet will be forwarded normally. Otherwise, the packet will be discarded.
- If the MAC address of a Host is classified into 802.1Q VLAN, please set its connected port of switch to be a member of this 802.1Q VLAN so as to ensure the packets forwarded normally.

6.3.1 MAC VLAN

On this page, you can create MAC VLAN and view the current MAC VLANs in the table.

Choose the menu **VLAN→MAC VLAN** to load the following page.

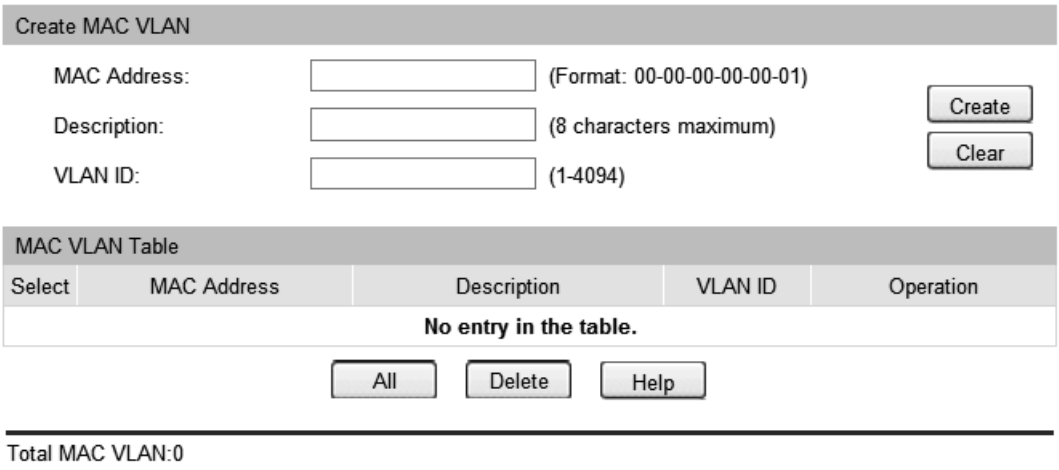


Figure 6-7 Create and View MAC VLAN

The following entries are displayed on this screen:

- **Create MAC VLAN**

MAC Address: Enter the MAC address.

Description: Give a description to the MAC address for identification.

VLAN ID: Enter the ID number of the MAC VLAN. This VLAN should be one of the 802.1Q VLANs the ingress port belongs to.

- **MAC VLAN Table**

Select: Select the desired entry. It is multi-optional.

MAC Address: Displays the MAC address.

Description: Displays the user-defined description of the MAC address.

VLAN ID: Displays the corresponding VLAN ID of the MAC address.

Operation: Click the **Edit** button to modify the settings of the entry. And click the **Modify** button to apply your settings.

6.3.2 Port Enable

On this page, you can enable the port for the MAC VLAN feature. Only the port is enabled, can the configured MAC VLAN take effect.

Choose the menu **VLAN→MAC VLAN→Port Enable** to load the following page.

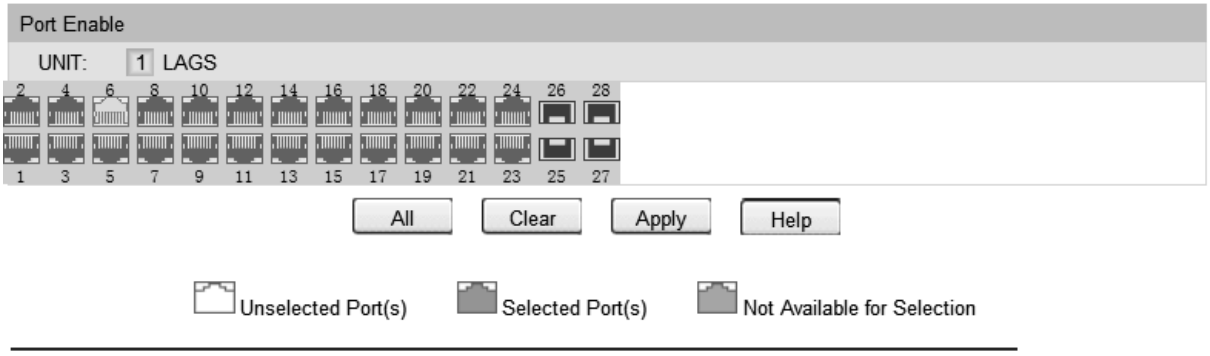


Figure 6-8 Enable Port for MAC VLAN

UNIT: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select your desired port for MAC VLAN function. All the ports are disabled for MAC VLAN function by default.

➢ **Configuration Procedure:**

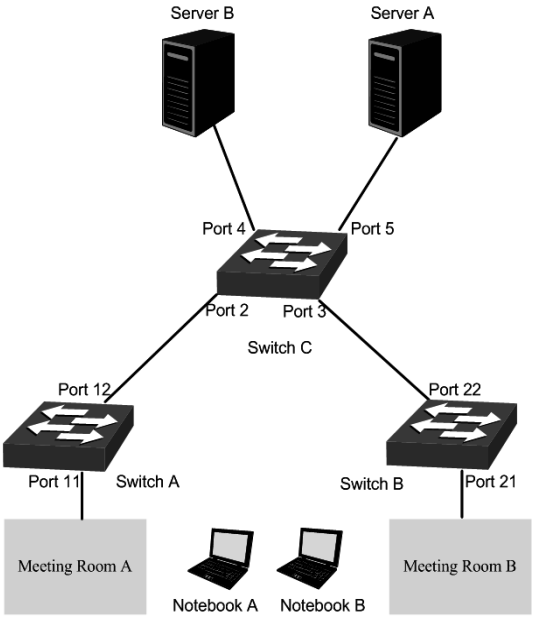
Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected device.
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its member ports.
3	Create MAC VLAN.	Required. On the **VLAN→MAC VLAN** page, create the MAC VLAN. For the device in a MAC VLAN, it's required to set its connected port of switch to be a member of this VLAN so as to ensure the normal communication.
4	Select your desired ports for MAC VLAN feature.	Required. On the **VLAN→MAC VLAN→Port Enable** page, select and enable the desired ports for MAC VLAN feature.

6.4 Application Example for MAC VLAN

➢ **Network Requirements**

- Switch A and switch B are connected to meeting room A and meeting room B respectively, and the two rooms are for all departments;
- Notebook A and Notebook B, special for meeting room, are of two different departments;
- The two departments are in VLAN10 and VLAN20 respectively. The two notebooks can just access the server of their own departments, that is, Server A and Server B, in the two meeting rooms;
- The MAC address of Notebook A is 00-19-56-8A-4C-71, Notebook B's MAC address is 00-19-56-82-3B-70.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 11 and Port 12 as GENERAL and TRUNK respectively.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 11 and Port 12, and configure the egress rule of Port 11 as Untag.
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 11 and Port 12, and configure the egress rule of Port 11 as Untag.
4	Configure MAC VLAN 10	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN10 with the MAC address as 00-19-56-8A-4C-71.
5	Configure MAC VLAN 20	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN20 with the MAC address as 00-19-56-82-3B-70.
6	Port Enable	Required. On the **VLAN→MAC VLAN→Port Enable** page, select and enable Port 11 and Port 12 for MAC VLAN feature.

- Configure switch B

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 21 and Port 22 as GENERAL and TRUNK respectively.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 21 and Port 22, and configure the egress rule of Port 21 as Untag.
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 21 and Port 22, and configure the egress rule of Port 21 as Untag.
4	Configure MAC VLAN 10	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN10 with the MAC address as 00-19-56-8A-4C-71.
5	Configure MAC VLAN 20	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN20 with the MAC address as 00-19-56-82-3B-70.
6	Port Enable	Required. On the **VLAN→MAC VLAN→Port Enable** page, select and enable Port 21 and Port 22 for MAC VLAN feature.

- Configure switch C

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 2 and Port 3 as GENERAL, and configure the link type of Port 4 and Port 5 as ACCESS.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 2, Port 3 and Port 5,
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 2, Port 3 and Port 4,

6.5 Protocol VLAN

Protocol VLAN is another way to classify VLANs basing on network protocol. Protocol VLANs can be sorted by IP, IPX, DECnet, AppleTalk, Banyan and so on. Through the Protocol VLANs, the broadcast domain can span over multiple switches and the Host can change its physical position in the network with its VLAN member role always effective. By creating Protocol VLANs, the network administrator can manage the network clients basing on their actual applications and services effectively.

This switch can classify VLANs basing on the common protocol types listed in the following table. Please create the Protocol VLAN to your actual need.

Protocol Type	Type value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

Table 6-1 Protocol types in common use

The packet in Protocol VLAN is processed in the following way:

1. When receiving an untagged packet, the switch matches the packet with the current Protocol VLAN. If the packet is matched, the switch will add a corresponding Protocol VLAN tag to it. If no Protocol VLAN is matched, the switch will add a tag to the packet according to the PVID of the received port. Thus, the packet is assigned automatically to the corresponding VLAN for transmission.
2. When receiving tagged packet, the switch will process it basing on the 802.1Q VLAN. If the received port is the member of the VLAN to which the tagged packet belongs, the packet will be forwarded normally. Otherwise, the packet will be discarded.
3. If the Protocol VLAN is created, please set its enabled port to be the member of corresponding 802.1Q VLAN so as to ensure the packets forwarded normally.

6.5.1 Protocol Group Table

On this page, you can create Protocol VLAN and view the information of the current defined Protocol VLANs.

Choose the menu **VLAN→Protocol VLAN→Protocol Group Table** to load the following page.

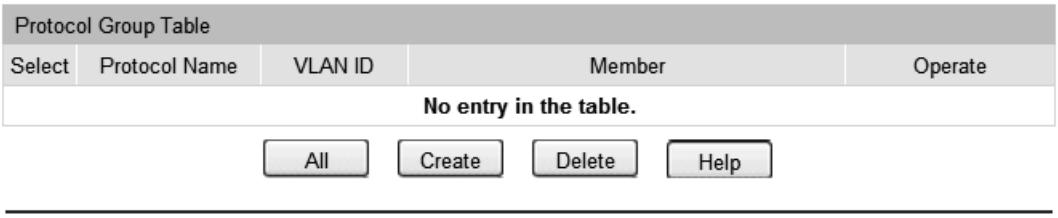


Figure 6-9 Create Protocol VLAN

The following entries are displayed on this screen:

- **Protocol Group Table**

  Select: Select the desired entry. It is multi-optional.

  Protocol Name: Displays the protocol of the protocol group.

VLAN ID: Displays the corresponding VLAN ID of the protocol.

Member: Displays the member of the protocol group.

Operate: Click the **Edit** button to modify the settings of the entry. And click the **Apply** button to apply your settings.

6.5.2 Protocol Group

On this page, you can configure the Protocol Group.

Choose the menu **VLAN→Protocol VLAN→Protocol Group** to load the following page.

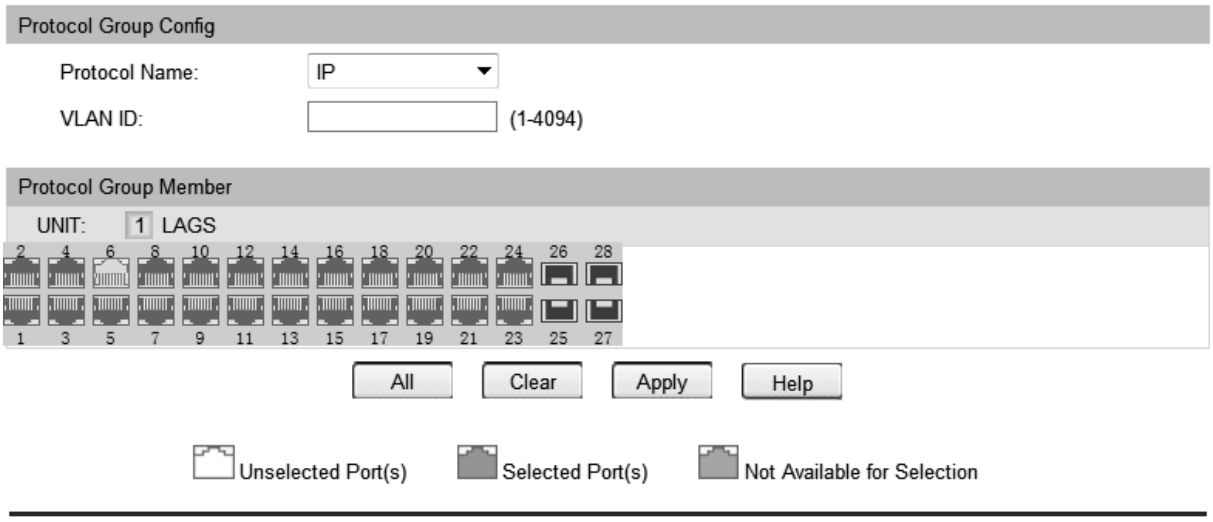


Figure 6-10 Enable Protocol VLAN for Port

- **Protocol Group Config**

Protocol Name: Select the defined protocol template.

VLAN ID: Enter the ID number of the Protocol VLAN. This VLAN should be one of the 802.1Q VLANs the ingress port belongs to.

- **Protocol Group Member**

UNIT: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

6.5.3 Protocol Template

The Protocol Template should be created before configuring the Protocol VLAN. By default, the switch has defined the IP Template, ARP Template, RARP Template, etc. You can add more Protocol Template on this page.

Choose the menu **VLAN→Protocol VLAN→Protocol Template** to load the following page.

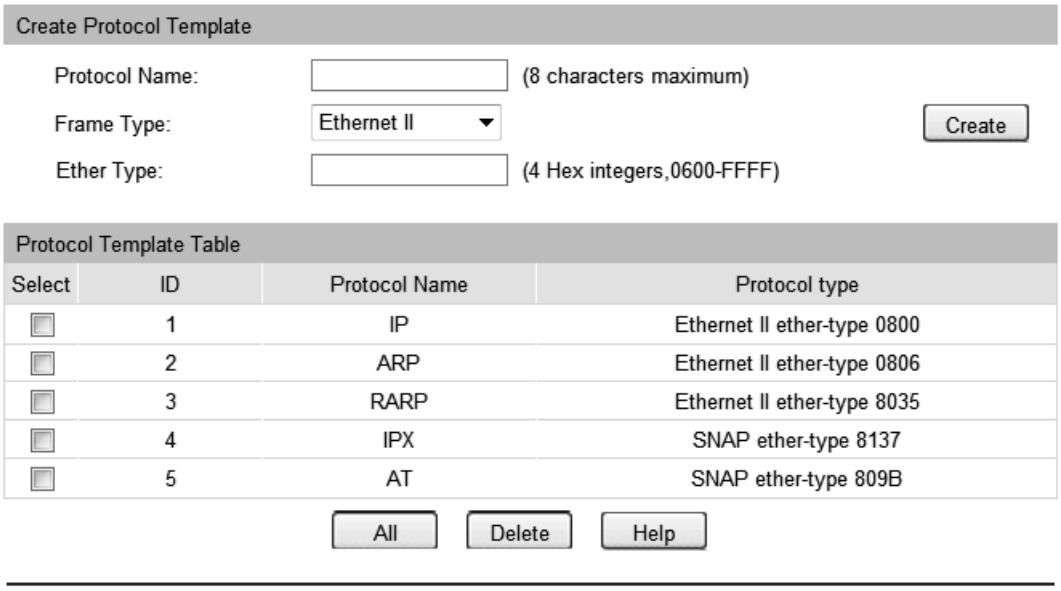


Figure 6-11 Create and View Protocol Template

The following entries are displayed on this screen:

➢ **Create Protocol Template**

Protocol Name: Give a name for the Protocol Template.

Frame Type: Select a Frame Type for the Protocol Template.

Ether Type: Enter the Ethernet protocol type field in the protocol template.

DSAP: Enter the DSAP field when selected LLC.

SSAP: Enter the SSAP field when selected LLC.

➢ **Protocol Template Table**

Select: Select the desired entry. It is multi-optional.

ID Displays the Protocol Template ID.

Protocol Name: Displays the Protocol Name.

Protocol Type: Displays the Protocol type.

Note:

The Protocol Template bound to VLAN cannot be deleted.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected

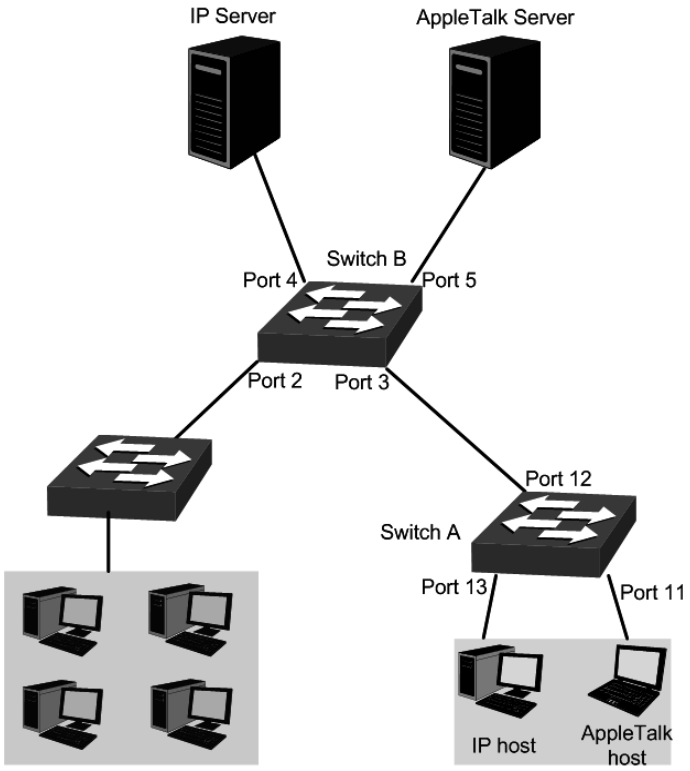
Step	Operation	Description
		device.
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its member ports.
3	Create Protocol Template.	Required. On the **VLAN→Protocol VLAN→Protocol Template** page, create the Protocol Template before configuring Protocol VLAN.
4	Create Protocol VLAN.	Required. On the **VLAN→Protocol VLAN→Protocol Group** page, select the protocol name and enter the VLAN ID to create a Protocol VLAN. Meanwhile, enable protocol VLAN for ports.
5	Modify/View VLAN.	Optional. On the **VLAN→Protocol VLAN→Protocol Group Table** page, click the **Edit** button to modify/view the information of the corresponding VLAN.
6	Delete VLAN.	Optional. On the **VLAN→Protocol VLAN→Protocol Group Table** page, select the desired entry to delete the corresponding VLAN by clicking the **Delete** button.

6.6 Application Example for Protocol VLAN

➢ **Network Requirements**

- Department A is connected to the company LAN via Port12 of switch A;
- Department A has IP host and AppleTalk host;
- IP host, in VLAN10, is served by IP server while AppleTalk host is served by AppleTalk server;
- Switch B is connected to IP server and AppleTalk server.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 11 and Port 13 as ACCESS, and configure the link type of Port 12 as GENERAL.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 12 and Port 13, and configure the egress rule of Port 12 as Untag.
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 11 and Port 12, and configure the egress rule of Port 12 as Untag.

- Configure switch B

Step	Operation	Description
1	Configure the Link Type of the ports	Required. On **VLAN→802.1Q VLAN→Port Config** page, configure the link type of Port 4 and Port 5 as ACCESS, and configure the link type of Port 3 as GENERAL.
2	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Port 3 and Port 4, and configure the egress rule of Port 3 as Untag.

Step	Operation	Description
3	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Port 3 and Port 5, and configure the egress rule of Port 3 as Untag.
4	Create Protocol Template	Required. On **VLAN→Protocol VLAN→Protocol Template** page, configure the protocol template practically. E.g. the Ether Type of IP network packets is 0800 and that of AppleTalk network packets is 809B.
5	Create Protocol VLAN 10	On **VLAN→Protocol VLAN→Protocol Group** page, create protocol VLAN 10 with Protocol as IP. Select and enable Port 3, Port 4 and Port 5 for Protocol VLAN feature.
6	Create Protocol VLAN 20	On **VLAN→Protocol VLAN→Protocol Group** page, create protocol VLAN 20 with Protocol as AppleTalk. Select and enable Port 3, Port 4 and Port 5 for Protocol VLAN feature.

6.7 VLAN VPN

With the increasing application of the Internet, the VPN (Virtual Private Network) technology is developed and used to establish the private network through the operators' backbone networks. VLAN-VPN (Virtual Private Network) function, the implement of a simple and flexible Layer 2 VPN technology, allows the packets with VLAN tags of private networks to be encapsulated with VLAN tags of public networks at the network access terminal of the Internet Service Provider. And these packets will be transmitted with double-tag across the public networks.

The VLAN-VPN function provides you with the following benefits:

(1) Provides simple Layer 2 VPN solutions for small-sized LANs or intranets.

(2) Saves public network VLAN ID resource.

(3) You can have VLAN IDs of your own, which is independent of public network VLAN IDs.

(4) When the network of the Internet Service Provider is upgraded, the user's network with a relative independence can still work normally without changing the current configurations.

In addition, the switch supports the feature to adjust the TPID Values of VLAN VPN Packets. TPID (Tag Protocol Identifier) is a field of the VLAN tag. IEEE 802.1Q specifies the value of TPID to be 0x8100. This switch adopts the default value of TPID (0x8100) defined by the protocol. Other manufacturers use other TPID values (such as 0x9100 or 0x9200) in the outer tags of VLAN-VPN packets. To be compatible with devices coming from other manufacturers, this switch can adjust the TPID values of VLAN-VPN packets globally. You can configure TPID values by yourself. When a port receives a packet, this port will replace the TPID value in the outer VLAN tag of this packet with the user-defined value and then send the packet again. Thus,

the VLAN-VPN packets sent to the public network can be recognized by devices of other manufacturers.

The position of the TPID field in an Ethernet packet is the same as the position of the protocol type field in the packet without VLAN Tag. Thus, to avoid confusion happening when the switch forwards or receives a packet, you must not configure the following protocol type values listed in the following table as the TPID value.

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

Table 6-2 Values of Ethernet frame protocol type in common use

This VLAN VPN function is implemented on the **VPN Config**, **VLAN Mapping** and **Port Enable** pages.

6.7.1 VPN Config

This page allows you to enable the VPN function, adjust the global TPID for VLAN-VPN packets and enable the VPN up-link port. When VPN mode is enabled, the switch will add a tag to the received tagged packet basing on the VLAN mapping entries.

Choose the menu **VLAN→VLAN VPN→VPN Config** to load the following page.

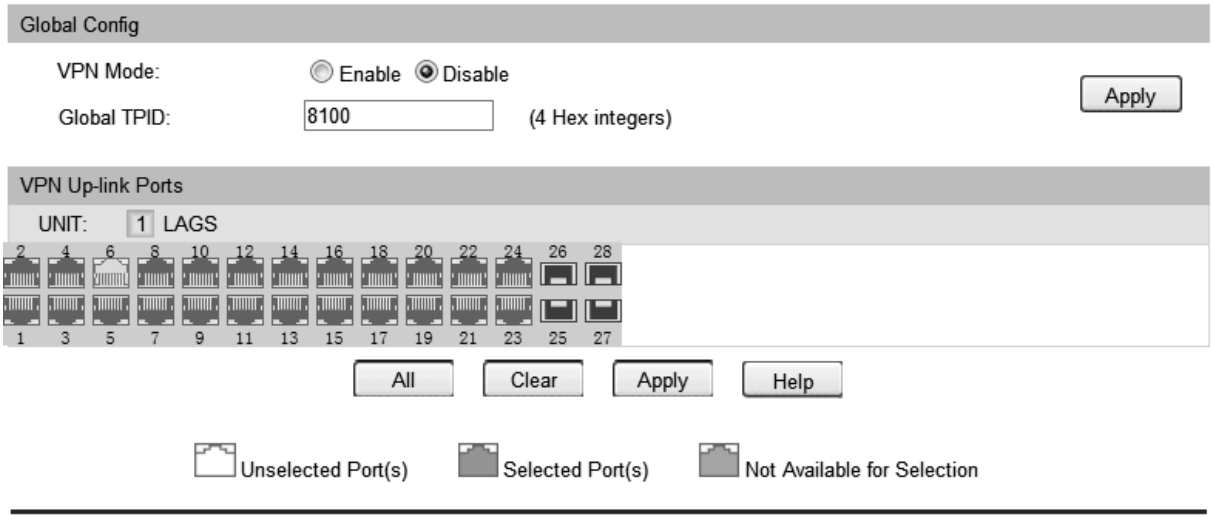


Figure 6-12 VPN Global Config

The following entries are displayed on this screen:

- **Global Config**

VPN Mode: Allows you to Enable/Disable the VLAN-VPN function.

Global TPID: Enter the global TPID (Tag protocol identifier).

- **VPN Up-link Ports**

Unit: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

VPN Up-link ports: Select the desired port as the VPN Up-link port.

Note:

If VPN mode is enabled, please create VLAN Mapping entries on the VLAN Mapping function page.

6.7.2 Port Enable

On this page, you can enable the port for the VLAN Mapping function. Only the port is enabled, can the configured VLAN Mapping function take effect.

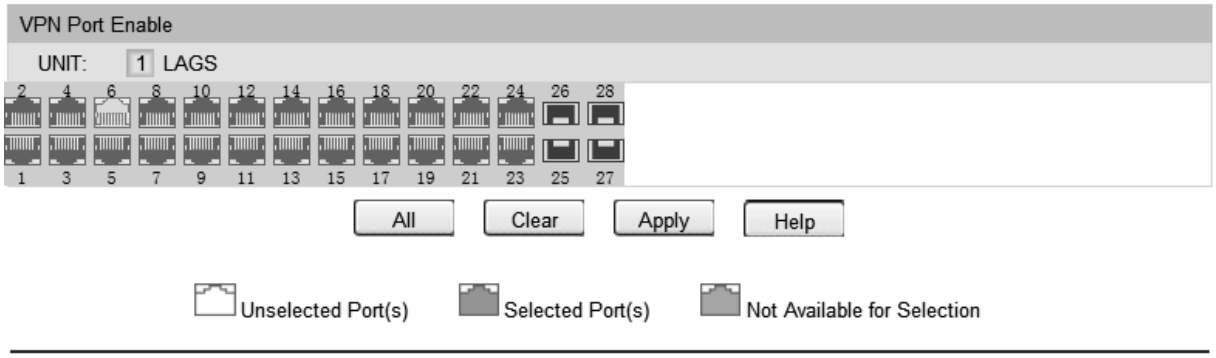


Figure 6-13 Enable Port for VLAN Mapping

- **VPN Port Enable**

UNIT: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select your desired port for VLAN Mapping function. All the ports are disabled for VLAN Mapping function by default.

6.7.3 VLAN Mapping

VLAN Mapping function defines a new VLAN TAG to be inserted before the VLAN TAG of the packets according to the VLAN Mapping entries. And these packets can be forwarded in the new VLAN. If VLAN VPN function is enabled, a received packet already carrying a VLAN tag will be tagged basing on the VLAN Mapping entries and becomes a double-tagged packet to be forwarded in the new VLAN.

Choose the menu **VLAN→VLAN VPN→VLAN Mapping** to load the following page.

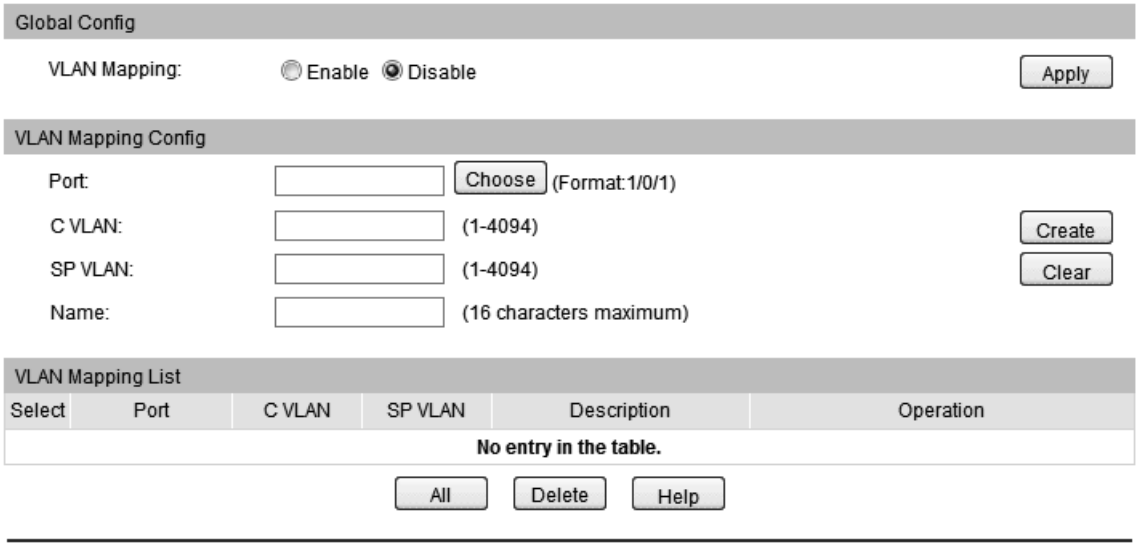


Figure 6-14 Create VLAN Mapping Entry

The following entries are displayed on this screen:

- **Global Config**

  VLAN Mapping: Enable/Disable the VLAN mapping function. Enable/Disable the VLAN mapping function. If VLAN mapping is disabled and VLAN VPN is enabled, the packet will be encapsulated with an outer tag according to the PVID of its arriving port.

- **VLAN Mapping Config**

  Port: Select/Input the port number.

  C VLAN: Enter the ID number of the Customer VLAN. C VLAN refers to the VLAN to which the packet received by switch belongs.

  SP VLAN: Enter the ID number of the Service Provider VLAN.

  Name: Give a name to the VLAN Mapping entry or leave it blank.

- **VLAN Mapping List**

  Select: Select the desired entry to delete the corresponding VLAN Mapping entry. It is multi-optional.

  Operation: Click the **Edit** button to modify the settings of the entry.

Click **Edit** to display the following figure:

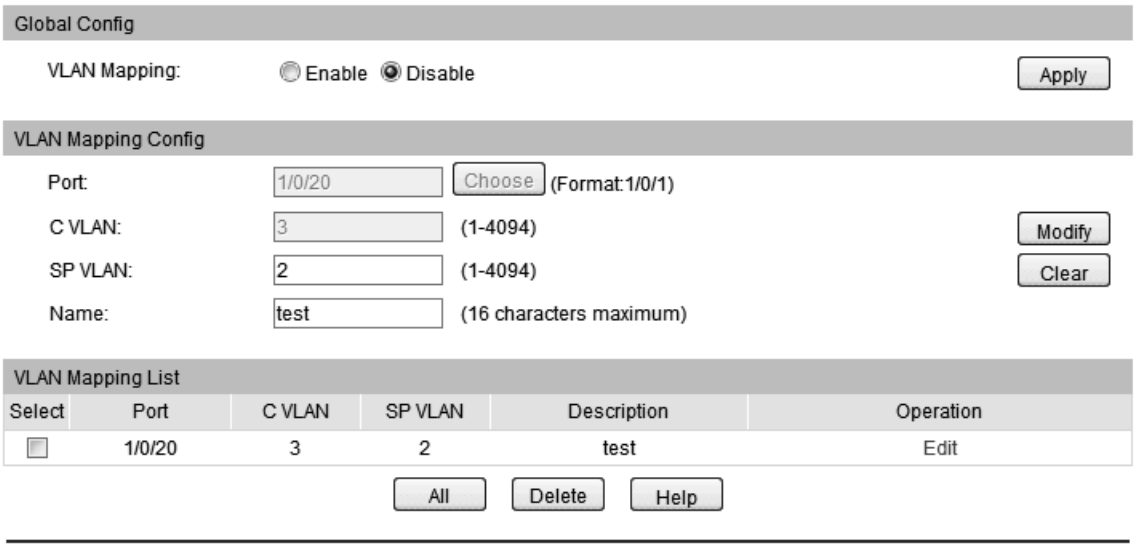


Figure 6-15 VLAN Mapping Entry Config

Modify the SP VLAN and name of the selected entry and click **Edit** to apply.

Note:

When VPN mode is globally enabled, VPN function takes effect on all ports. If VPN mode is disabled, VLAN Mapping function can be enabled by selecting your desired port on this Port Enable page.

Configuration Procedure of VLAN VPN Function:

Step	Operation	Description
1	Enable VPN mode.	Required. On the **VLAN→VLAN VPN→VPN Config** page, enable the VPN mode.
2	Configure the global TPID.	Optional. On the **VLAN→VLAN VPN→VPN Config** page, configure the global TPID basing on the devices connected to the up-link port.
3	Set the VPN up-link port.	Required. On the **VLAN→VLAN VPN→VPN Config** page, specify the desired port to be the VPN up-link port. It's required to set the port connected to the backbone networks to be up-link port.
4	Create VLAN Mapping entries.	Required. On the **VLAN→VLAN VPN→VLAN Mapping** page, configure the VLAN Mapping entries basing on the actual application.
5	Create SP (Service Provider) VLAN.	Optional. On the **VLAN→802.1Q VLAN** page, create the SP VLAN. For the steps of creating VLAN, please refer to 802.1Q VLAN.

Configuration Procedure of VLAN Mapping Function:

Step	Operation	Description
1	Create VLAN Mapping entries.	Required. On the **VLAN→VLAN VPN→VLAN Mapping** page, configure the VLAN Mapping entries basing on the actual application.
2	Enable VLAN Mapping function for port.	Required. On the **VLAN→VLAN VPN→Port Enable** page, enable VLAN Mapping function for the ports.
3	Create SP (Service Provider) VLAN	Optional. On the **VLAN→802.1Q VLAN** page, create the SP VLAN. For the steps of creating VLAN, please refer to 802.1Q VLAN.

6.8 GVRP

GVRP (GARP VLAN Registration Protocol) is an implementation of GARP (generic attribute registration protocol). GVRP allows the switch to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other switches, without having to individually configure each VLAN.

➢ **GARP**

GARP provides the mechanism to assist the switch members in LAN to deliver, propagate and register the information among the members. GARP itself does not work as the entity among the devices. The application complied with GARP is called GARP implementation, and GVRP is the implementation of GARP. When GARP is implemented on a port of device, the port is called GARP entity.

The information exchange between GARP entities is completed by messages. GARP defines the messages into three types: Join, Leave and LeaveAll.

- **Join Message:** When a GARP entity expects other switches to register certain attribute information of its own, it sends out a Join message. And when receiving the Join message from the other entity or configuring some attributes statically, the device also sends out a Join message in order to be registered by the other GARP entities.
- **Leave Message:** When a GARP entity expects other switches to deregister certain attribute information of its own, it sends out a Leave message. And when receiving the Leave message from the other entity or deregistering some attributes statically, the device also sends out a Leave message.
- **LeaveAll Message:** Once a GARP entity starts up, it starts the LeaveAll timer. After the timer times out, the GARP entity sends out a LeaveAll message. LeaveAll message is to deregister all the attribute information so as to enable the other GARP entities to re-register attribute information of their own.

Through message exchange, all the attribute information to be registered can be propagated to all the switches in the same switched network.

The interval of GARP messages is controlled by timers. GARP defines the following timers:

- **Hold Timer:** When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer, puts all registration information it receives before the timer times out into one Join message and sends out the message after the timer times out.
- **Join Timer:** To transmit the Join messages reliably to other entities, a GARP entity sends each Join message two times. The Join timer is used to define the interval between the two sending operations of each Join message.
- **Leave Timer:** When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and deregisters the attribute information if it does not receives a Join message again before the timer times out.
- **LeaveAll Timer:** Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveAll message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

➢ **GVRP**

GVRP, as an implementation of GARP, maintains dynamic VLAN registration information and propagates the information to other switches by adopting the same mechanism of GARP.

After the GVRP feature is enabled on a switch, the switch receives the VLAN registration information from other switches to dynamically update the local VLAN registration information, including VLAN members, ports through which the VLAN members can be reached, and so on. The switch also propagates the local VLAN registration information to other switches so that all the switching devices in the same switched network can have the same VLAN information. The VLAN registration information includes not only the static registration information configured locally, but also the dynamic registration information, which is received from other switches.

In this switch, only the port with TRUNK link type can be set as the GVRP application entity to maintain the VLAN registration information. GVRP has the following three port registration modes: Normal, Fixed, and Forbidden.

- **Normal:** In this mode, a port can dynamically register/deregister a VLAN and propagate the dynamic/static VLAN information.
- **Fixed:** In this mode, a port cannot register/deregister a VLAN dynamically. It only propagates static VLAN information. That is, the port in Fixed mode only permits the packets of its static VLAN to pass.
- **Forbidden:** In this mode, a port cannot register/deregister VLANs. It only propagates VLAN 1 information. That is, the port in Forbidden mode only permits the packets of the default VLAN (namely VLAN 1) to pass.

Choose the menu **VLAN→GVRP→GVRP Config** to load the following page.

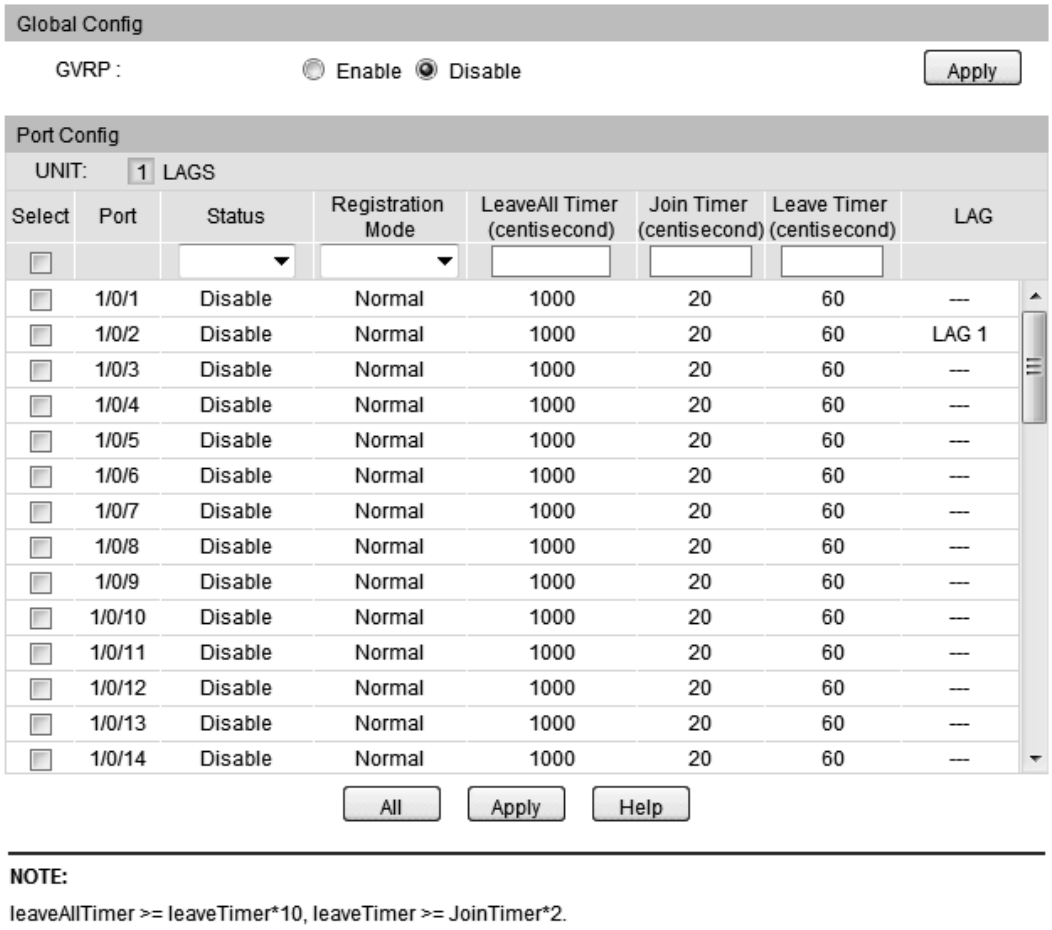


Figure 6-16 GVRP Config

Note:

If the GVRP feature is enabled for a member port of LAG, please ensure all the member ports of this LAG are set to be in the same status and registration mode.

The following entries are displayed on this screen:

- **Global Config**

  GVRP: Allows you to Enable/Disable the GVRP function.

- **Port Config**

  Unit: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

  Select: Select the desired port for configuration. It is multi-optional.

  Port: Displays the port number.

  Status: Enable/Disable the GVRP feature for the port. The port type should be set to TRUNK before enabling the GVRP feature.

  Registration Select the Registration Mode for the port.

Mode:

- **Normal:** In this mode, a port can dynamically register/ deregister a VLAN and propagate the dynamic/static VLAN information.
- **Fixed:** In this mode, a port cannot register/deregister a VLAN dynamically. It only propagates static VLAN information.
- **Forbidden:** In this mode, a port cannot register/deregister VLANs. It only propagates VLAN 1 information.

LeaveAll Timer: Once the LeaveAll Timer is set, the port with GVRP enabled can send a LeaveAll message after the timer times out, so that other GARP ports can re-register all the attribute information. After that, the LeaveAll timer will start to begin a new cycle. The LeaveAll Timer ranges from 1000 to 30000 centiseconds.

Join Timer: To guarantee the transmission of the Join messages, a GARP port sends each Join message two times. The Join Timer is used to define the interval between the two sending operations of each Join message. The Join Timer ranges from 20 to 1000 centiseconds.

Leave Timer: Once the Leave Timer is set, the GARP port receiving a Leave message will start its Leave timer, and deregister the attribute information if it does not receive a Join message again before the timer times out. The Leave Timer ranges from 60 to 3000 centiseconds.

LAG: Displays the LAG to which the port belongs.

Note:

LeaveAll Timer >= 10* Leave Timer, Leave Timer >= 2*Join Timer.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type of the port to be TRUNK.
2	Enable GVRP function.	Required. On the **VLAN→GVRP** page, enable GVRP function.
3	Configure the registration mode and the timers for the port.	Required. On the **VLAN→GVRP** page, configure the parameters of ports basing on actual applications.

6.9 Private VLAN

Private VLANs, designed to save VLAN resources of uplink devices and decrease broadcast, are sets of VLAN pairs that share a common primary identifier. To guarantee user information

security, the ease with which to manage and account traffic for service providers, in campus network, service providers usually require that each individual user is Layer-2 separated. VLAN feature can solve this problem. However, as stipulated by IEEE 802.1Q protocol, a device can only support up to 4094 VLANs. If a service provider assigns one VLAN per user, the VLANs will be far from enough; as a result, the number of users this service provider can support is limited.

Private VLAN adopts Layer 2 VLAN structure. A Private VLAN consists of a Primary VLAN and a Secondary VLAN, providing a mechanism for achieving layer-2-separation between ports. For uplink devices, all the packets received from the downstream are without VLAN tags. Uplink devices need to identify Primary VLANs but not Secondary VLANs. Therefore, they can save VLAN resources without considering the VLAN configuration in the lower layer. Meanwhile, the service provider can assign each user an individual Secondary VLAN, so that users are separated at the Layer 2 level.

Private VLAN technology is mainly used in campus or enterprise networks to achieve user Layer-2-separation and to save VLAN resources of uplink devices.

➢ **The Elements of a Private VLAN**

Promiscuous port: A promiscuous port connects to and communicates with the uplink device. The PVID of the promiscuous port is the same with the Primary VLAN ID. One promiscuous port can only join to one Primary VLAN.

Host port: A host port connects to and communicates with terminal device. The PVID of the host port is the same as the Secondary VLAN ID. One host port can only belong to one Private VLAN.

Primary VLAN: A Private VLAN has one Primary VLAN and one Secondary VLAN. Primary VLAN is the user VLAN uplink device can identify but it is not the actual VLAN the end user is in. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the host ports and to other promiscuous ports.

Secondary VLAN: .Secondary VLAN is the actual VLAN the end user is in. Secondary VLANs are associated with a primary VLAN, and are used to carry traffic from hosts to uplink devices. There are two types of secondary VLANS:

- Isolated VLAN—The VLAN that an isolated port is associated with is called isolated VLAN. Each isolated VLAN must bind to a primary VLAN.
- Community VLAN—The VLAN that a community port is associated with is called community VLAN. Each community VLAN must bind to a primary VLAN.

➢ **Features of Private VLAN**

1. A Private VLAN contains one Primary VLAN and one Secondary VLAN.
2. A VLAN cannot be set as the Primary VLAN and Secondary VLAN simultaneously.
3. A Secondary VLAN can only join one private VLAN.

4. A Primary VLAN can be associated with multi-Secondary VLANs to create multi-Private VLANs.

➢ **Private VLAN Implementation**

To hide Secondary VLANs from uplink devices and save VLAN resources, Private VLAN containing one Primary VLAN and one Secondary VLAN requires the following characteristics:

- Packets from different Secondary VLANs can be forwarded to the uplink device via promiscuous port and carry no corresponding Secondary VLAN information.
- Packets from Primary VLANs can be sent to end users via host port and carry no Primary VLAN information.

Private VLAN functions are implemented on the **PVLAN Config** and **Port Config** pages.

6.9.1 PVLAN Config

On this page, you can create Private VLAN and view the information of the current defined Private VLANs.

Choose the menu **VLAN→Private VLAN→PVLAN Config** to load the following page.

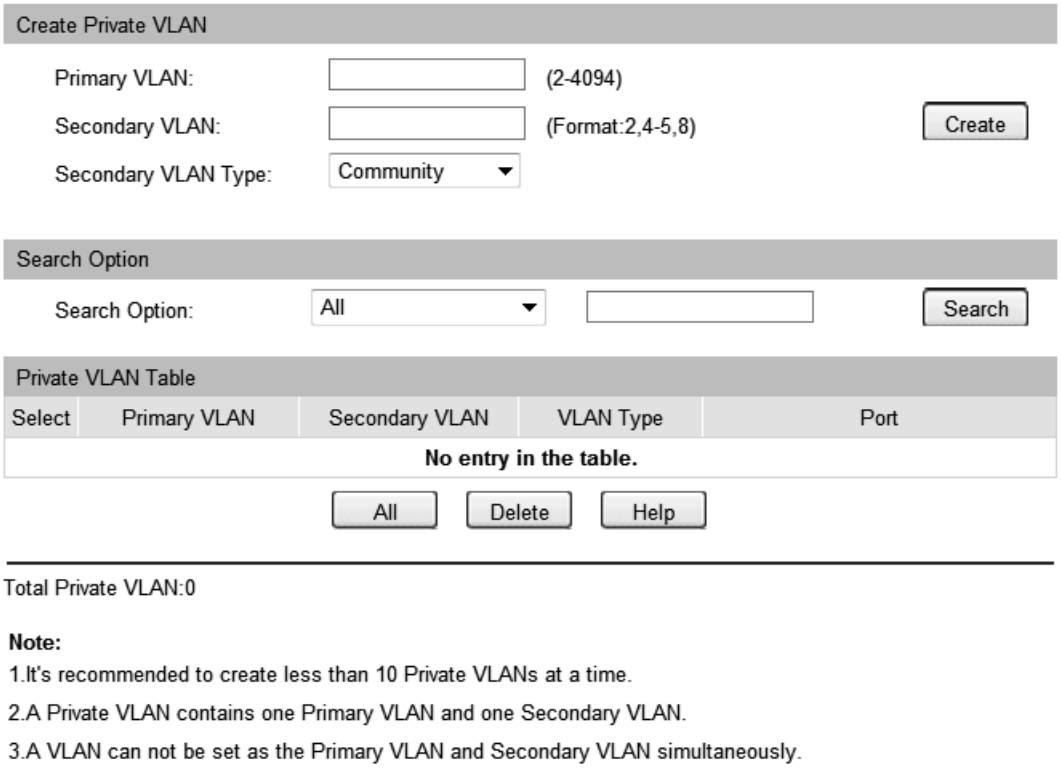


Figure 6-17 Create Private VLAN

The following entries are displayed on this screen:

➢ **Create Private VLAN**

Primary VLAN: Enter the ID number of the Primary VLAN.

Secondary VLAN: Enter the ID number of the Secondary VLAN.

- **Search Option**

Search Option: Select a Search Option from the pull-down list and click the **Search** button to find your desired entry in Private VLAN.

- **All**: Enter either the Primary VLAN ID or Secondary VLAN ID of the desired Private VLAN.
- **Primary VLAN ID:** Enter the Primary VLAN ID number of the desired Private VLAN.
- **Secondary VLAN ID:** Enter the Secondary VLAN ID number of the desired Private VLAN.

- **Private VLAN Table**

Select: Select the entry to delete. It is multi-optional.

Primary VLAN: Displays the Primary VLAN ID number of the Private VLAN.

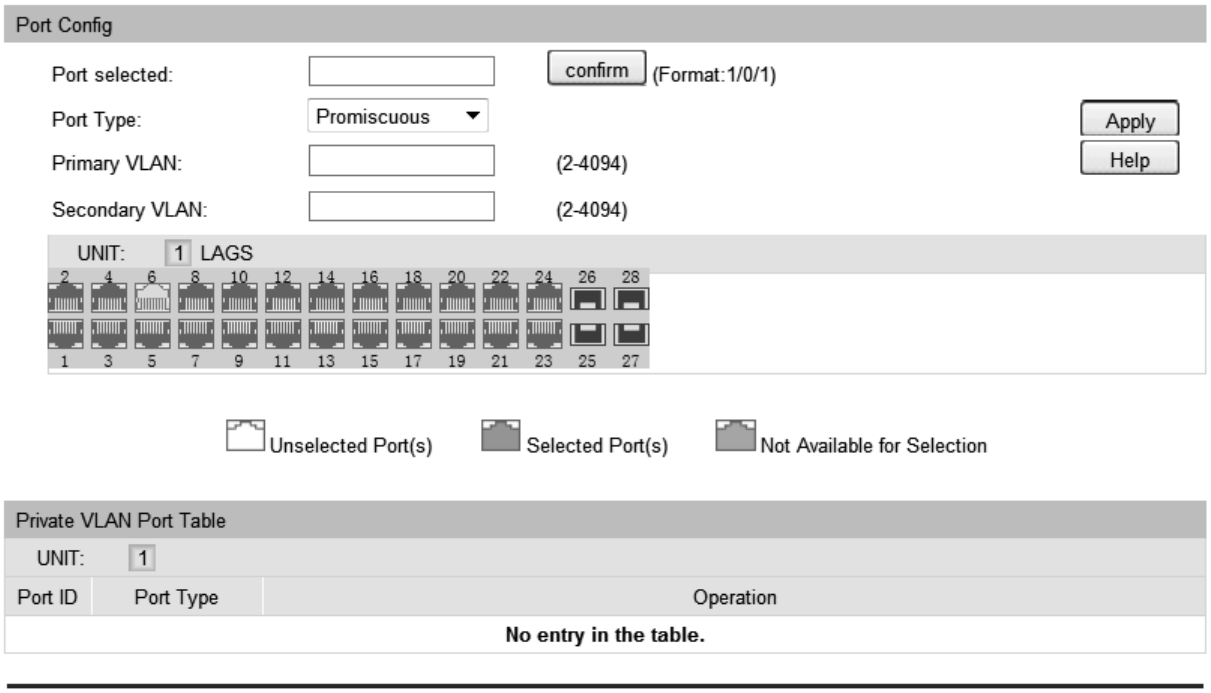
Secondary VLAN: Displays the Secondary VLAN ID number of the Private VLAN.

Port: Displays the port list of the Private VLAN.

6.9.2 Port Config

The Private VLAN provides two Port Types for the ports, Promiscuous and Host. Usually, the Promiscuous port is used to connect to uplink devices while the Host port is used to connect to the he terminal hosts, such as PC and Server.

Choose the menu **VLAN→Private VLAN→Port Config** to load the following page.



NOTE:
If you want to add a Promiscuous port to different Private VLANs with the same Primary VLAN, you just need add the Promiscuous port to any one of these Private VLANs.

Figure 6-18 Create and View Protocol Template

The following entries are displayed on this screen:

- **Port Config**

  Port selected: Select the desired port for configuration. You can input one or select from the port panel.

  Port Type: Select the Port Type from the pull-down list for the port.

  Primary VLAN: Specify the Primary VLAN the port belongs to.

  Secondary VLAN: Specify the Secondary VLAN the port belongs to.

  UNIT: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

- **Private VLAN Port Table**

  Port ID: Displays the port number.

  Port Type: Displays the corresponding Port Type.

Note:

1. A Host Port can only join to one Private VLAN.
2. A Promiscuous Port can only join to one Primary VLAN.
3. If you want to add a Promiscuous port to different Private VLANs with the same Primary VLAN, you need to add the Promiscuous port to any one of these Private VLANs.

➢ **Configuration Procedure:**

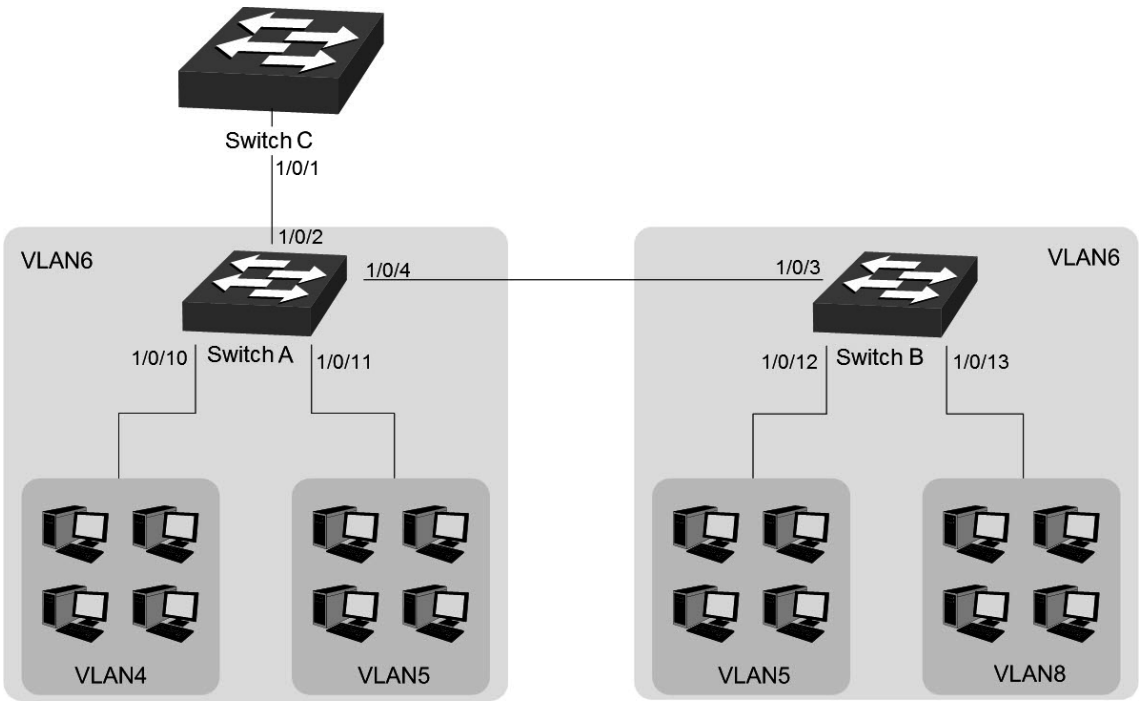
Step	Operation	Description
1	Create Private VLAN.	Required. On the **VLAN→Private VLAN→PVLAN Config** page, Enter the Primary VLAN and Secondary VLAN, select one type of secondary VLAN and then click the **Create** button.
2	Add ports to Private VLAN	Required. On the **VLAN→Private VLAN→Port Config** page, select the desired ports and configure the port types and click the **Apply** button.
3	Delete VLAN.	Optional. On the **VLAN→Private VLAN→PVLAN Config** page, select the desired entry to delete the corresponding VLAN by clicking the **Delete** button.

6.10 Application Example for Private VLAN

➢ **Network Requirements**

- Switch C is connecting to switch A, switch A is connecting to switch B;
- Switch A is connecting to VLAN4 and VLAN5;
- Switch B is connecting to VLAN5 and VLAN8;
- For switch C, packets from switch A and switch B have no VLAN tags. Switch C needs not to consider the VLANs of switch A and switch B;

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch C

Step	Operation	Description
1	Create VLAN6	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 6, owning Port 1/0/1.

- Configure switch A

Step	Operation	Description
1	Create Private VLANs.	Required. On the **VLAN→Private VLAN→PVLAN Config** page, Enter the Primary VLAN 6 and Secondary VLAN 4-5, select one type of secondary VLAN and then click the **Create** button.
2	Add Promiscuous port to Private VLANs	Required. On the **VLAN→Private VLAN→Port Config** page, configure the port type of Port 1/0/2 and Port 1/0/4 as **Promiscuous**, enter Primary VLAN 6 and Secondary VLAN 4, and click the **Apply** button.
3	Add Host port to Private VLANs	Required. On the **VLAN→Private VLAN→Port Config** page, configure the port type of Port 1/0/10 as **Host**, enter Primary VLAN 6 and Secondary VLAN 4, and click the **Apply** button. Configure the port type of Port 1/0/11 as **Host**, enter Primary VLAN 6 and Secondary VLAN 5, and click the **Apply** button

- Configure switch B

Step	Operation	Description
1	Create Private VLANs.	Required. On the **VLAN→Private VLAN→PVLAN Config** page, enter the Primary VLAN 6 and Secondary VLAN 5 and 8, select one type of secondary VLAN and then click the **Create** button.
2	Add Promiscuous port to Private VLANs	Required. On the **VLAN→Private VLAN→Port Config** page, configure the port type of Port 1/0/3 as **Promiscuous**, enter Primary VLAN 6 and Secondary VLAN 5, and click the **Apply** button.
3	Add Host port to Private VLANs	Required. On the **VLAN→Private VLAN→Port Config** page, configure the port type of 1/0/12 as **Host**, enter Primary VLAN 6 and Secondary VLAN 5, and click the **Apply** button. Configure the port type of Port 1/0/13 as **Host**, enter Primary VLAN 6 and Secondary VLAN 8, and click the **Apply** button

Return to CONTENTS

Chapter 7 Spanning Tree

STP (Spanning Tree Protocol), subject to IEEE 802.1D standard, is to disbranch a ring network in the Data Link layer in a local network. Devices running STP discover loops in the network and block ports by exchanging information, in that way, a ring network can be disbranched to form a tree-topological ring-free network to prevent packets from being duplicated and forwarded endlessly in the network.

BPDU (Bridge Protocol Data Unit) is the protocol data that STP and RSTP use. Enough information is carried in BPDU to ensure the spanning tree generation. STP is to determine the topology of the network via transferring BPDUs between devices.

To implement spanning tree function, the switches in the network transfer BPDUs between each other to exchange information and all the switches supporting STP receive and process the received BPDUs. BPDUs carry the information that is needed for switches to figure out the spanning tree.

- **STP Elements**

Bridge ID (Bridge Identifier): Indicates the value of the priority and MAC address of the bridge. Bridge ID can be configured and the switch with the lower bridge ID has the higher priority.

Root Bridge: Indicates the switch has the lowest bridge ID. Configure the best PC in the ring network as the root bridge to ensure best network performance and reliability.

Designated Bridge: Indicates the switch has the lowest path cost from the switch to the root bridge in each network segment. BPDUs are forwarded to the network segment through the designated bridge. The switch with the lowest bridge ID will be chosen as the designated bridge.

Root Path Cost: Indicates the sum of the path cost of the root port and the path cost of all the switches that packets pass through. The root path cost of the root bridge is 0.

Bridge Priority: The bridge priority can be set to a value in the range of 0~32768. The lower value priority has the higher priority. The switch with the higher priority has more chance to be chosen as the root bridge.

Root Port: Indicates the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root.

Designated Port: Indicates the port that forwards packets to a downstream network segment or switch.

Port Priority: The port priority can be set to a value in the range of 0~255. The lower value priority has the higher priority. The port with the higher priority has more chance to be chosen as the root port.

Path Cost: Indicates the parameter for choosing the link path by STP. By calculating the path cost, STP chooses the better links and blocks the redundant links so as to disbranch the ring-network to form a tree-topological ring-free network.

The following network diagram shows the sketch map of spanning tree. Switch A, B and C are connected together in order. After STP generation, switch A is chosen as root bridge, the path from port 2 to port 6 is blocked.

- Bridge: Switch A is the root bridge in the whole network; switch B is the designated bridge of switch C.
- Port: Port 3 is the root port of switch B and port 5 is the root port of switch C; port 1 is the designated port of switch A and port 4 is the designated port of switch B; port 6 is the blocked port of switch C.

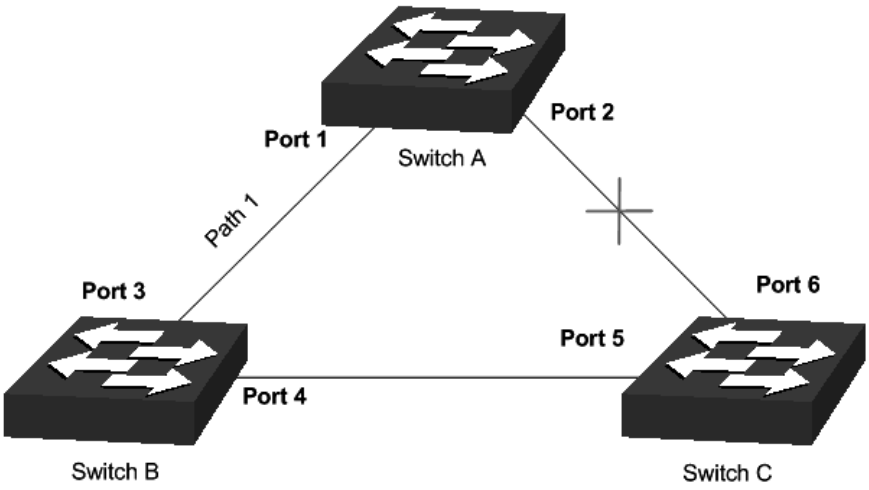


Figure 7-1 Basic STP diagram

➢ **STP Timers**

Hello Time:

Hello Time ranges from 1 to 10 seconds. It specifies the interval to send BPDU packets. It is used to test the links.

Max. Age:

Max. Age ranges from 6 to 40 seconds. It specifies the maximum time the switch can wait without receiving a BPDU before attempting to reconfigure.

Forward Delay:

Forward Delay ranges from 4 to 30 seconds. It specifies the time for the port to transit its state after the network topology is changed.

When the STP regeneration caused by network malfunction occurs, the STP structure will get some corresponding change. However, as the new configuration BPDUs cannot be spread in the whole network at once, the temporal loop will occur if the port transits its state immediately. Therefore, STP adopts a state transit mechanism, that is, the new root port and the designated port begins to forward data after twice forward delay, which ensures the new configuration BPDUs are spread in the whole network.

➢ **BPDU Comparing Principle in STP mode**

Assuming two BPDUs: BPDU X and BPDU Y

If the root bridge ID of X is smaller than that of Y, X is superior to Y.

If the root bridge ID of X equals that of Y, but the root path cost of X is smaller than that of Y, X is superior to Y.

If the root bridge ID and the root path cost of X equal those of Y, but the bridge ID of X is smaller than that of Y, X is superior to Y.

If the root bridge ID, the root path cost and bridge ID of X equal those of Y, but the port ID of X is smaller than that of Y, X is superior to Y.

➢ **STP Generation**

- In the beginning

In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

- Comparing BPDUs

Each switch sends out configuration BPDUs and receives a configuration BPDU on one of its ports from another switch. The following table shows the comparing operations.

Step	Operation
1	If the priority of the BPDU received on the port is lower than that of the BPDU if of the port itself, the switch discards the BPDU and does not change the BPDU of the port.
2	If the priority of the BPDU is higher than that of the BPDU of the port itself, the switch replaces the BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

Table 7-1 Comparing BPDUs

- Selecting the root bridge

The root bridge is selected by BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.

- Selecting the root port and designate port

The operation is taken in the following way:

Step	Operation
1	For each switch (except the one chosen as the root bridge) in a network, the port that receives the BPDU with the highest priority is chosen as the root port of the switch.
2	Using the root port BPDU and the root path cost, the switch generates a designated port BPDU for each of its ports. • Root ID is replaced with that of the root port; • Root path is replaced with the sum of the root path cost of the root port and the path cost between this port and the root port; • The ID of the designated bridge is replaced with that of the switch; • The ID of the designated port is replaced with that of the port.

3	The switch compares the resulting BPDU with the BPDU of the desired port whose role you want to determine. • If the resulting BPDU takes the precedence over the BPDU of the port, the port is chosen as the designated port and the BPDU of this port is replaced with the resulting BPDU. The port regularly sends out the resulting BPDU; • If the BPDU of this port takes the precedence over the resulting BPDU, the BPDU of this port is not replaced and the port is blocked. The port only can receive BPDUs.

Table 7-2 Selecting root port and designated port

Tips:

In a STP with stable topology, only the root port and designated port can forward data, and the other ports are blocked. The blocked ports only can receive BPDUs.

RSTP (Rapid Spanning Tree Protocol), evolved from the 802.1D STP standard, enable Ethernet ports to transit their states rapidly. The premises for the port in the RSTP to transit its state rapidly are as follows.

- The condition for the root port to transit its port state rapidly: The old root port of the switch stops forwarding data and the designated port of the upstream switch begins to forward data.
- The condition for the designated port to transit its port state rapidly: The designated port is an edge port or connecting to a point-to-point link. If the designated port is an edge port, it can directly transit to forwarding state; if the designated port is connecting to a point-to-point link, it can transit to forwarding state after getting response from the downstream switch through handshake.

➢ **RSTP Elements**

Edge Port: Indicates the port connected directly to terminals.

P2P Link: Indicates the link between two switches directly connected.

MSTP (Multiple Spanning Tree Protocol), compatible with both STP and RSTP and subject to IEEE 802.1s standard, not only enables spanning trees to converge rapidly, but also enables packets of different VLANs to be forwarded along their respective paths so as to provide redundant links with a better load-balancing mechanism.

Features of MSTP:

- MSTP combines VLANs and spanning tree together via VLAN-to-instance mapping table. It binds several VLANs to an instance to save communication cost and network resources.
- MSTP divides a spanning tree network into several regions. Each region has several internal spanning trees, which are independent of each other.
- MSTP provides a load-balancing mechanism for the packets transmission in the VLAN.

- MSTP is compatible with both STP and RSTP.

➢ **MSTP Elements**

MST Region (Multiple Spanning Tree Region): An MST Region comprises switches with the same region configuration and VLAN-to-Instances mapping relationship.

IST (Internal Spanning Tree)**:** An IST is a spanning tree in an MST.

CST (Common Spanning Tree): A CST is the spanning tree in a switched network that connects all MST regions in the network.

CIST (Common and Internal Spanning Tree): A CIST, comprising IST and CST, is the spanning tree in a switched network that connects all switches in the network.

The following figure shows the network diagram in MSTP.

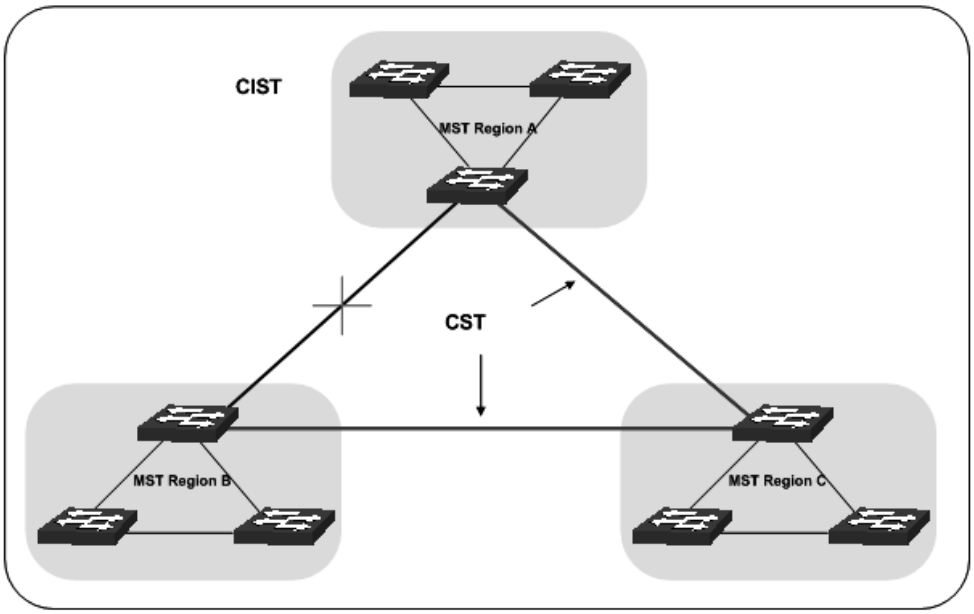


Figure 7-2 Basic MSTP diagram

➢ **MSTP**

MSTP divides a network into several MST regions. The CST is generated between these MST regions, and multiple spanning trees can be generated in each MST region. Each spanning tree is called an instance. As well as STP, MSTP uses BPDUs to generate spanning tree. The only difference is that the BPDU for MSTP carries the MSTP configuration information on the switches.

➢ **Port States**

In an MSTP, ports can be in the following four states:

- Forwarding: In this status the port can receive/forward data, receive/send BPDU packets as well as learn MAC address.
- Learning: In this status the port can receive/send BPDU packets and learn MAC address.
- Blocking: In this status the port can only receive BPDU packets.
- Disconnected: In this status the port is not participating in the STP.

➢ **Port Roles**

In an MSTP, the following roles exist:

- Root Port: Indicates the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root.
- Designated Port: Indicates the port that forwards packets to a downstream network segment or switch.
- Master Port: Indicates the port that connects a MST region to the common root. The path from the master port to the common root is the shortest path between this MST region and the common root.
- Alternate Port: Indicates the port that can be a backup port of a root or master port.
- Backup Port: Indicates the port that is the backup port of a designated port.
- Disabled: Indicates the port that is not participating in the STP.

The following diagram shows the different port roles.

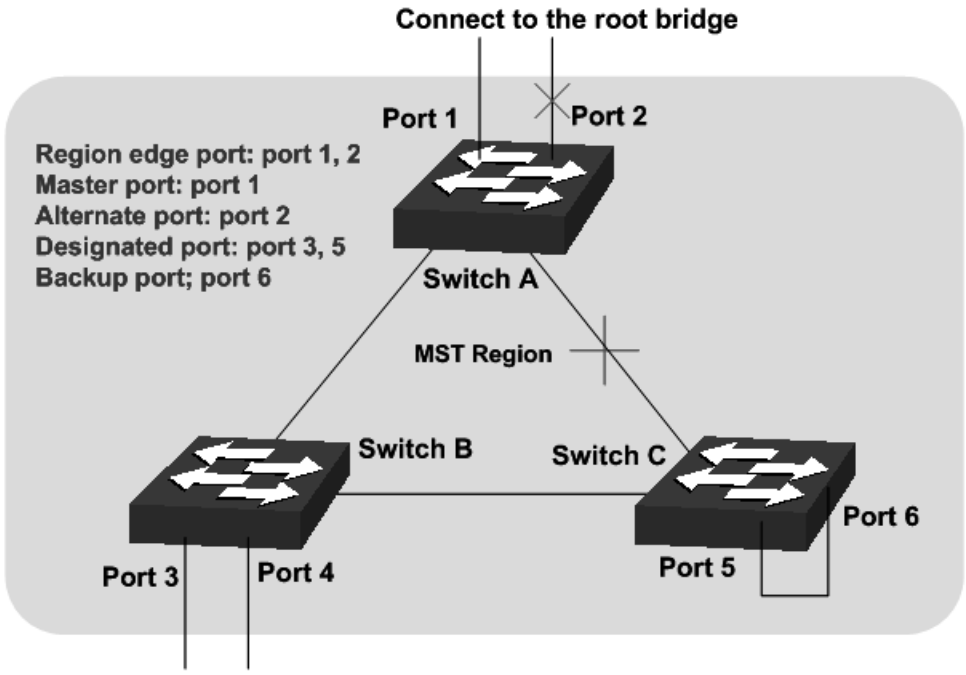


Figure 7-3 Port roles

The Spanning Tree module is mainly for spanning tree configuration of the switch, including four submenus: **STP Config**, **Port Config**, **MSTP Instance** and **STP Security**.

7.1 STP Config

The STP Config function, for global configuration of spanning trees on the switch, can be implemented on **STP Config** and **STP Summary** pages.

7.1.1 STP Config

Before configuring spanning trees, you should make clear the roles each switch plays in each spanning tree instance. Only one switch can be the root bridge in each spanning tree instance. On this page you can globally configure the spanning tree function and related parameters.

Choose the menu **Spanning Tree→STP Config→STP Config** to load the following page.

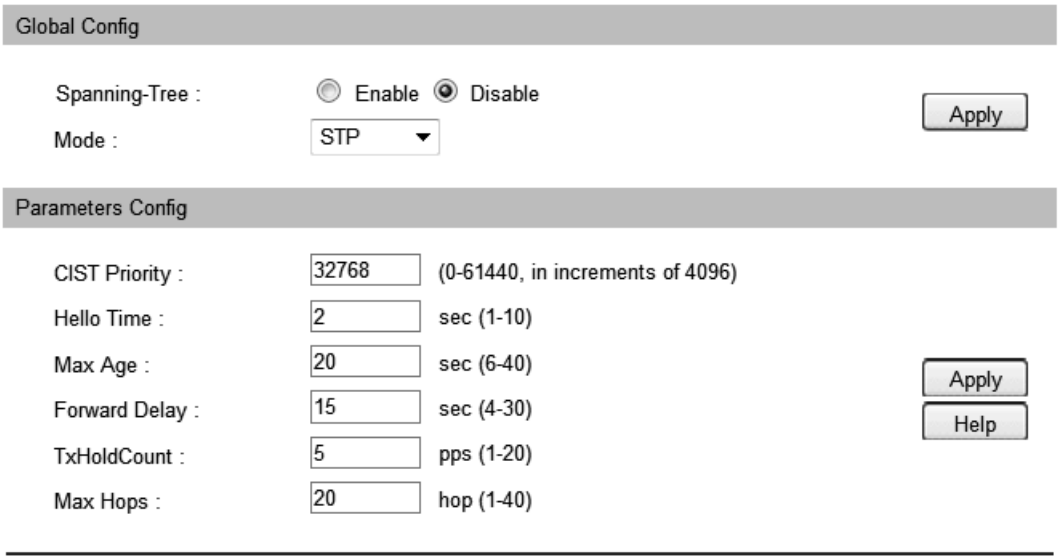


Figure 7-4 STP Config

The following entries are displayed on this screen:

- **Global Config**

Spanning-Tree: Select Enable/Disable STP function globally on the switch.

Mode: Select the desired STP mode on the switch.

- **STP**: Spanning Tree Protocol.
- **RSTP**: Rapid Spanning Tree Protocol.
- **MSTP**: Multiple Spanning Tree Protocol.

- **Parameters Config**

CIST Priority: Enter a value from 0 to 61440 to specify the priority of the switch for comparison in the CIST. CIST priority is an important criterion on determining the root bridge. In the same condition, the switch with the highest priority will be chosen as the root bridge. The lower value has the higher priority. The default value is 32768 and should be exact divisor of 4096.

Hello Time Enter a value from 1 to 10 in seconds to specify the interval to send BPDU packets. It is used to test the links. 2*(Hello Time + 1) ≤ Max Age. The default value is 2 seconds.

Max Age: Enter a value from 6 to 40 in seconds to specify the maximum time the switch can wait without receiving a BPDU before attempting to reconfigure. The default value is 20 seconds.

Forward Delay: Enter a value from 4 to 30 in seconds to specify the time for the port to transit its state after the network topology is changed. 2*(Forward Delay-1) ≥ Max Age. The default value is 15 seconds.

TxHold Count: Enter a value from 1 to 20 to set the maximum number of BPDU packets transmitted per Hello Time interval. The default value is 5pps.

Max Hops: Enter a value from 1 to 40 to set the maximum number of hops that occur in a specific region before the BPDU is discarded.

The default value is 20 hops.

Note:

1. The forward delay parameter and the network diameter are correlated. A too small forward delay parameter may result in temporary loops. A too large forward delay may cause a network unable to resume the normal state in time. The default value is recommended.
2. An adequate hello time parameter can enable the switch to discover the link failures occurred in the network without occupying too much network resources. A too large hello time parameter may result in normal links being regarded as invalid when packets drop occurred in the links, which in turn result in spanning tree being regenerated. A too small hello time parameter may result in duplicated configuration being sent frequently, which increases the network load of the switches and wastes network resources. The default value is recommended.
3. A too small max age parameter may result in the switches regenerating spanning trees frequently and cause network congestions to be falsely regarded as link problems. A too large max age parameter result in the switches unable to find the link problems in time, which in turn handicaps spanning trees being regenerated in time and makes the network less adaptive. The default value is recommended.
4. If the TxHold Count parameter is too large, the number of MSTP packets being sent in each hello time may be increased with occupying too much network resources. The default value is recommended.

7.1.2 STP Summary

On this page you can view the related parameters for Spanning Tree function.

Choose the menu **Spanning Tree→STP Config→STP Summary** to load the following page.

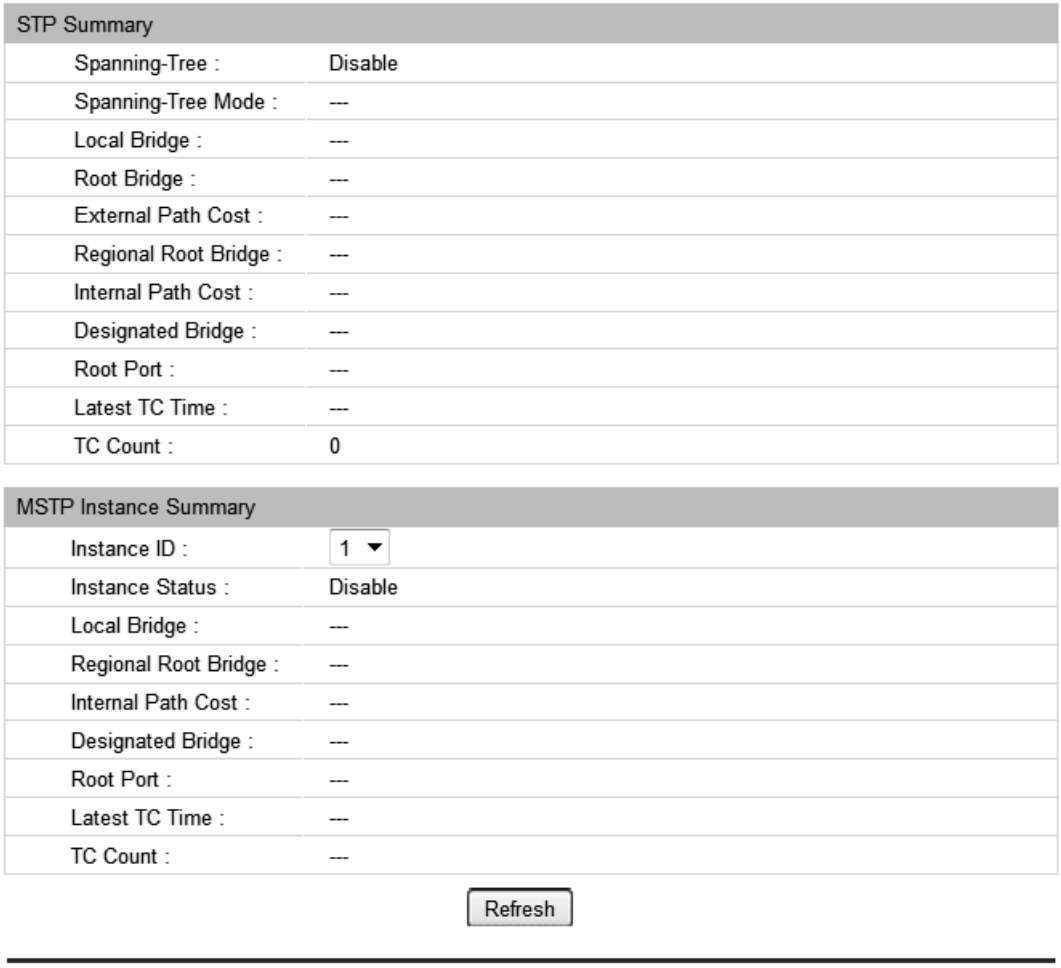


Figure 7-5 STP Summary

7.2 Port Config

On this page you can configure the parameters of the ports for CIST.

Choose the menu **Spanning Tree→Port Config** to load the following page.

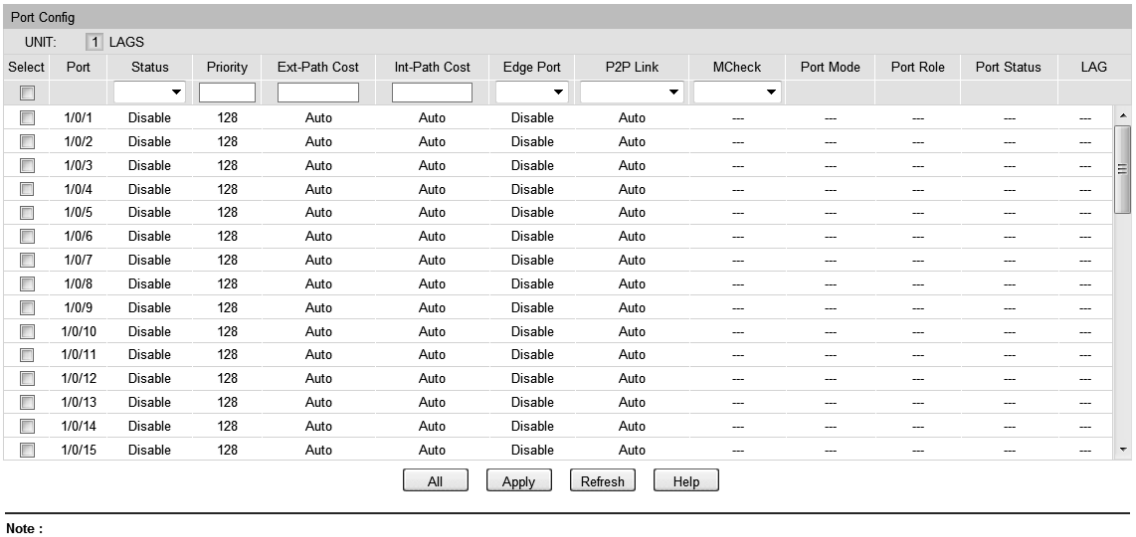


Figure 7-6 Port Config

The following entries are displayed on this screen:

- **Port Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired port for STP configuration. It is multi-optional.

Port: Displays the port number of the switch.

Status: Select Enable /Disable STP function for the desired port.

Priority: Enter a value from 0 to 240 divisible by 16. Port priority is an important criterion on determining if the port connected to this port will be chosen as the root port. The lower value has the higher priority.

ExtPath Cost: ExtPath Cost is used to choose the path and calculate the path costs of ports in different MST regions. It is an important criterion on determining the root port. The lower value has the higher priority.

IntPath Cost: IntPath Cost is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority.

Edge Port: Select Enable/Disable Edge Port. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

P2P Link: Select the P2P link status. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

MCheck: Select Enable to perform MCheck operation on the port. Unchange means no MCheck operation.

Port Mode: Display the spanning tree mode of the port.

Port Role: Displays the role of the port played in the STP Instance.

- **Root Port**: Indicates the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root.
- **Designated Port**: Indicates the port that forwards packets to a downstream network segment or switch.
- **Master Port**: Indicates the port that connects a MST region to the common root. The path from the master port to the common root is the shortest path between this MST region and the common root.
- **Alternate Port**: Indicates the port that can be a backup port of a root or master port.
- **Backup Port**: Indicates the port that is the backup port of a designated port.

- **Disabled**: Indicates the port that is not participating in the STP.

Port Status: Displays the working status of the port.

- **Forwarding**: In this status the port can receive/forward data, receive/send BPDU packets as well as learn MAC address.
- **Learning**: In this status the port can receive/send BPDU packets and learn MAC address.
- **Blocking**: In this status the port can only receive BPDU packets.
- **Disconnected**: In this status the port is not participating in the STP.

LAG: Displays the LAG number which the port belongs to.

Note:

1. Configure the ports connected directly to terminals as edge ports and enable the BPDU protection function as well. This not only enables these ports to transit to forwarding state rapidly but also secures your network.
2. All the links of ports in a LAG can be configured as point-to-point links.
3. When the link of a port is configured as a point-to-point link, the spanning tree instances owning this port are configured as point-to-point links. If the physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, temporary loops may be incurred.

7.3 MSTP Instance

MSTP combines VLANs and spanning tree together via VLAN-to-instance mapping table (VLAN-to-spanning-tree mapping). By adding MSTP instances, it binds several VLANs to an instance to realize the load balance based on instances.

Only when the switches have the same MST region name, MST region revision and VLAN-to-Instance mapping table, the switches can be regarded as in the same MST region.

The MSTP Instance function can be implemented on **Region Config**, **Instance Config** and **Instance Port Config** pages.

7.3.1 Region Config

On this page you can configure the name and revision of the MST region.

Choose the menu **Spanning Tree→MSTP Instance→Region Config** to load the following page.

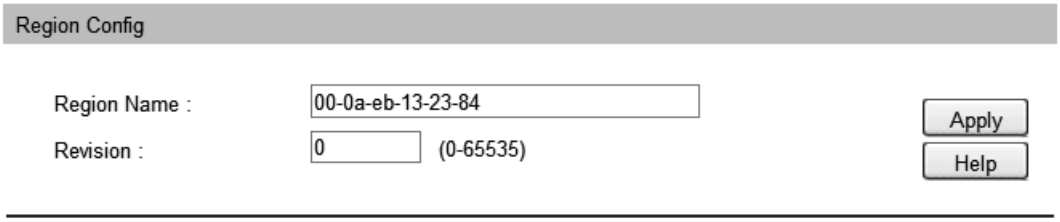


Figure 7-7 Region Config

The following entries are displayed on this screen:

- **Region Config**

Region Name: Create a name for MST region identification using up to 32 characters.

Revision: Enter the revision from 0 to 65535 for MST region identification.

7.3.2 Instance Config

Instance Configuration, a property of MST region, is used to describe the VLAN to Instance mapping configuration. You can assign VLAN to different instances appropriate to your needs. Every instance is a VLAN group independent of other instances and CIST.

Choose the menu **Spanning Tree→MSTP Instance→Instance Config** to load the following page.

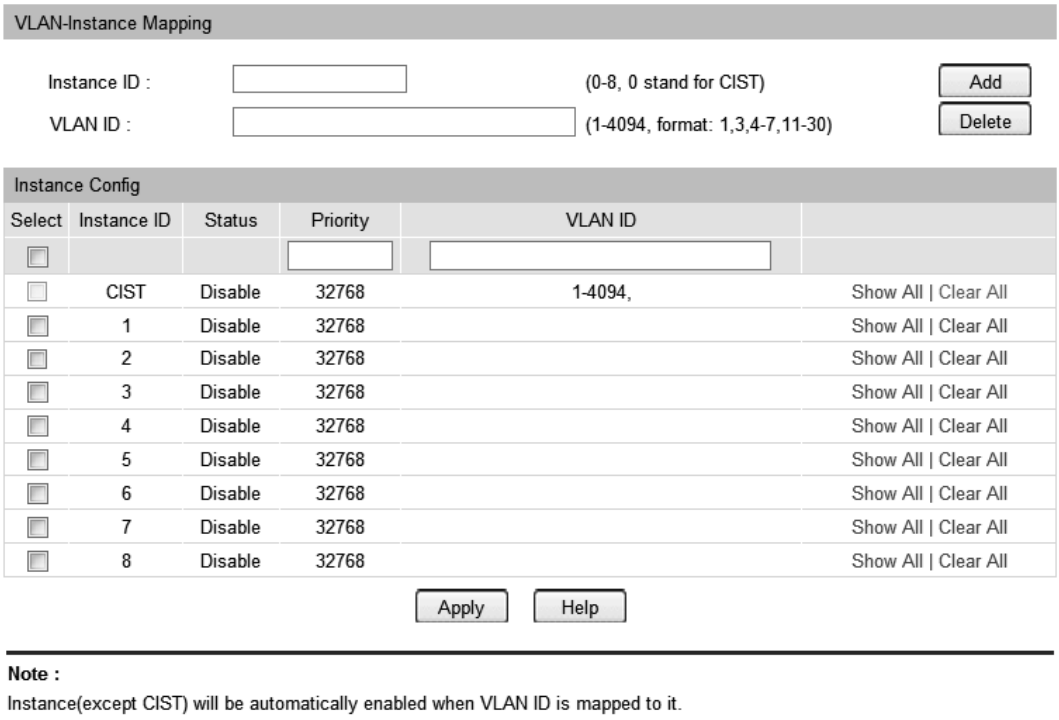


Figure 7-8 Instance Config

The following entries are displayed on this screen:

- **VLAN-Instance Mapping**

Instance ID: Enter the corresponding instance ID.

VLAN ID: Enter the desired VLAN ID. After modification here, the new VLAN ID will be added to the corresponding instance ID and the previous VLAN ID won't be replaced.

- **Instance Table**

Select: Select the desired Instance ID for configuration. It is multi-optional.

Instance ID:	Displays Instance ID of the switch.
Status:	Displays status of the instance.
Priority:	Enter the priority of the switch in the instance. It is an important criterion on determining if the switch will be chosen as the root bridge in the specific instance.
VLAN ID:	Enter the VLAN ID which belongs to the corresponding instance ID. After modification here, the previous VLAN ID will be cleared and mapped to the CIST.
Clear All:	Click **Clear All** to clear up all VLAN IDs from the instance ID. The cleared VLAN ID will be automatically mapped to the CIST.

7.3.3 Instance Port Config

A port can play different roles in different spanning tree instance. On this page you can configure the parameters of the ports in different instance IDs as well as view status of the ports in the specified instance.

Choose the menu **Spanning Tree→MSTP Instance→Instance Port Config** to load the following page.

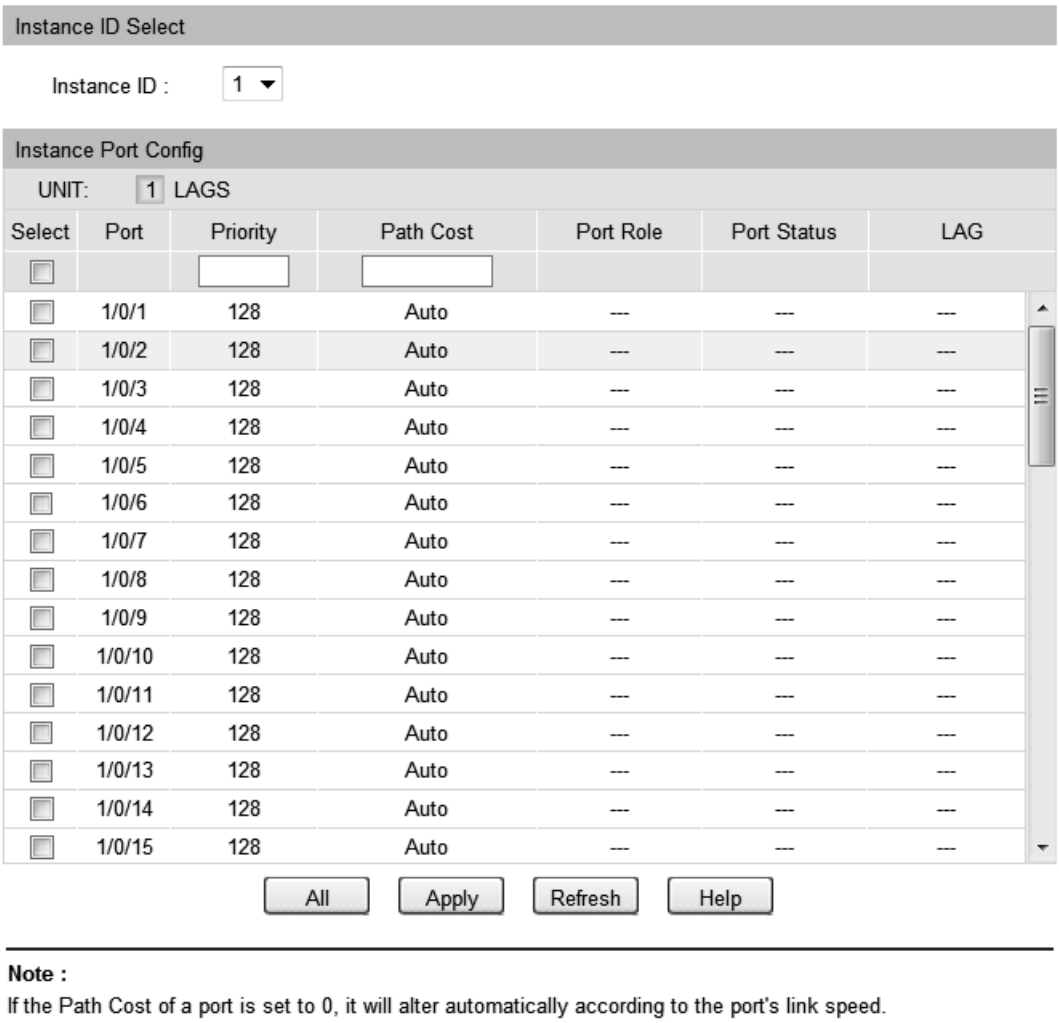


Figure 7-9 Instance Port Config

The following entries are displayed on this screen:

- **Instance ID Select**

  Instance ID: Select the desired instance ID for its port configuration.

- **Instance Port Config**

  UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

  Select: Select the desired port to specify its priority and path cost. It is multi-optional.

  Port: Displays the port number of the switch.

  Priority: Enter the priority of the port in the instance. It is an important criterion on determining if the port connected to this port will be chosen as the root port.

  Path Cost: Path Cost is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on

	determining the root port. The lower value has the higher priority.
Port Role:	Displays the role of the port played in the MSTP Instance.
Port Status:	Displays the working status of the port.
LAG:	Displays the LAG number which the port belongs to.

Note:

The port status of one port in different spanning tree instances can be different.

Global configuration Procedure for Spanning Tree function:

Step	Operation	Description
1	Make clear roles the switches play in spanning tree instances: root bridge or designated bridge	Preparation.
2	Globally configure MSTP parameters	Required. Enable Spanning Tree function on the switch and configure MSTP parameters on **Spanning Tree→STP Config→STP Config** page.
3	Configure MSTP parameters for ports	Required. Configure MSTP parameters for ports on **Spanning Tree→Port Config→Port Config** page.
4	Configure the MST region	Required. Create MST region and configure the role the switch plays in the MST region on **Spanning Tree→MSTP Instance→Region Config** and **Instance Config** page.
5	Configure MSTP parameters for instance ports	Optional. Configure different instances in the MST region and configure MSTP parameters for instance ports on **Spanning Tree→MSTP Instance→Instance Port Config** page.

7.4 STP Security

Configuring protection function for devices can prevent devices from any malicious attack against STP features. The STP Security function can be implemented on **Port Protect** and **TC Protect** pages.

Port Protect function is to prevent the devices from any malicious attack against STP features.

7.4.1 Port Protect

On this page you can configure loop protect feature, root protect feature, TC protect feature, BPDU protect feature and BPDU filter feature for ports. You are suggested to enable corresponding protection feature for the qualified ports.

- **Loop Protect**

In a stable network, a switch maintains the states of ports by receiving and processing BPDU packets from the upstream switch. However, when link congestions or link failures occurred to the network, a down stream switch does not receive BPDU packets for certain period, which results in spanning trees being regenerated and roles of ports being reselected, and causes the blocked ports to transit to forwarding state. Therefore, loops may be incurred in the network.

The loop protect function can suppresses loops. With this function enabled, a port, regardless of the role it plays in instances, is always set to blocking state, when the port does not receive BPDU packets from the upstream switch and spanning trees are regenerated, and thereby loops can be prevented.

- **Root Protect**

A CIST and its secondary root bridges are usually located in the high-bandwidth core region. Wrong configuration or malicious attacks may result in configuration BPDU packets with higher priorities being received by the legal root bridge, which causes the current legal root bridge to lose its position and network topology jitter to occur. In this case, flows that should travel along high-speed links may lead to low-speed links, and network congestion may occur.

To avoid this, MSTP provides root protect function. Ports with this function enabled can only be set as designated ports in all spanning tree instances. When a port of this type receives BDPU packets with higher priority, it transits its state to blocking state and stops forwarding packets (as if it is disconnected from the link). The port resumes the normal state if it does not receive any configuration BPDU packets with higher priorities for a period of two times of forward delay.

- **TC Protect**

A switch removes MAC address entries upon receiving TC-BPDU packets. If a user maliciously sends a large amount of TC-BPDU packets to a switch in a short period, the switch will be busy with removing MAC address entries, which may decrease the performance and stability of the network.

To prevent the switch from frequently removing MAC address entries, you can enable the TC protect function on the switch. With TC protect function enabled, if the account number of the received TC-BPDUs exceeds the maximum number you set in the TC threshold field, the switch will not performs the removing operation in the TC protect cycle. Such a mechanism prevents the switch from frequently removing MAC address entries.

- **BPDU Protect**

Ports of the switch directly connected to PCs or servers are configured as edge ports to rapidly transit their states. When these ports receive BPDUs, the system automatically configures these ports as non-edge ports and regenerates spanning trees, which may cause network topology jitter. Normally these ports do not receive BPDUs, but if a user maliciously attacks the switch by sending BPDUs, network topology jitter occurs.

To prevent this attack, MSTP provides BPDU protect function. With this function enabled on the switch, the switch shuts down the edge ports that receive BPDUs and reports these cases to the administrator. If a port is shut down, only the administrator can restore it.

➢ **BPDU Filter**

BPDU filter function is to prevent BPDUs flood in the STP network. If a switch receives malicious BPDUs, it forwards these BPDUs to the other switched in the network, which may result in spanning trees being continuously regenerated. In this case, the switch occupying too much CPU or the protocol status of BPDUs is wrong.

With BPDU filter function enabled, a port does not receive or forward BPDUs, but it sends out its own BPDUs. Such a mechanism prevents the switch from being attacked by BPDUs so as to guarantee generation the spanning trees correct.

Choose the menu **Spanning Tree→STP Security→Port Protect** to load the following page.

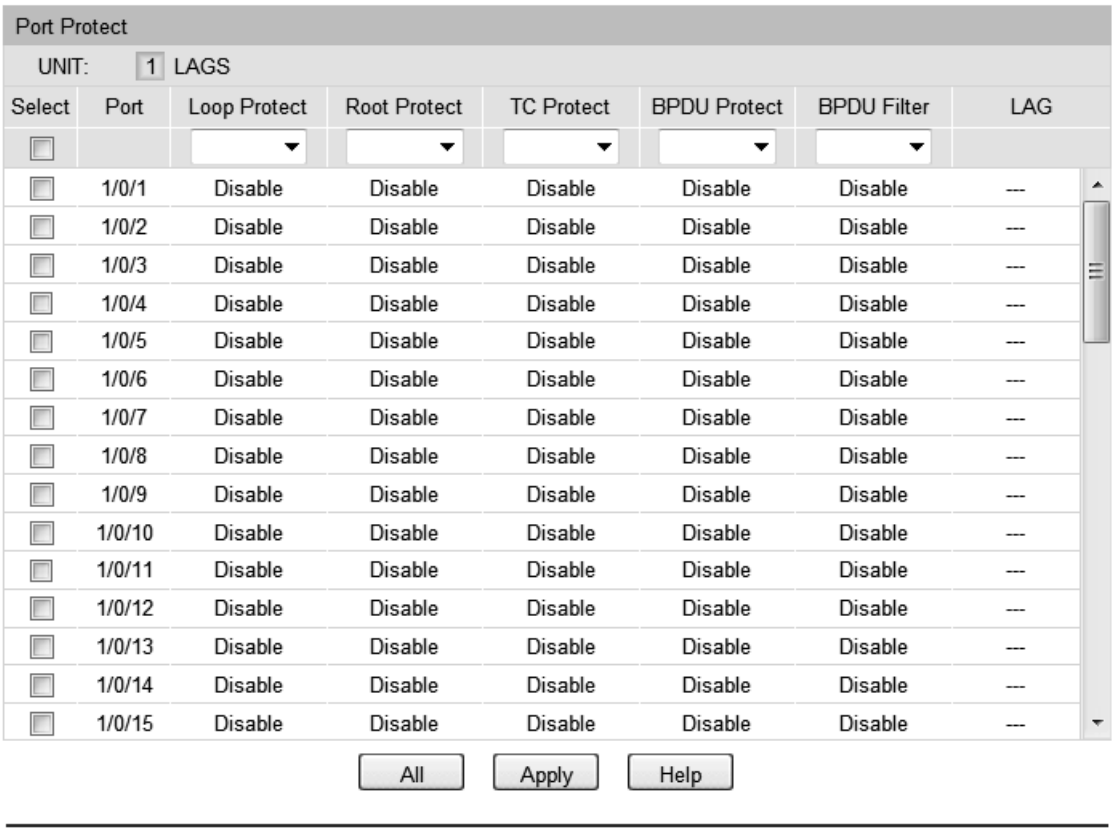


Figure 7-10 Port Protect

The following entries are displayed on this screen:

➢ **Port Protect**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired port for port protect configuration. It is multi-optional.

Port: Displays the port number of the switch.

Loop Protect: Loop Protect is to prevent the loops in the network brought by recalculating STP because of link failures and network congestions.

Root Protect: Root Protect is to prevent wrong network topology change caused by the role change of the current legal root bridge.

TC Protect: TC Protect is to prevent the decrease of the performance and stability of the switch brought by continuously removing MAC address entries upon receiving TC-BPDUs in the STP network.

BPDU Protect: BPDU Protect is to prevent the edge port from being attacked by maliciously created BPDUs

BPDU Filter: BPDU Filter is to prevent BPDUs flood in the STP network.

LAG: Displays the LAG number which the port belongs to.

7.4.2 TC Protect

When TC Protect is enabled for the port on **Port Protect** page, the TC threshold and TC protect cycle need to be configured on this page.

Choose the menu **Spanning Tree→STP Security→TC Protect** to load the following page.

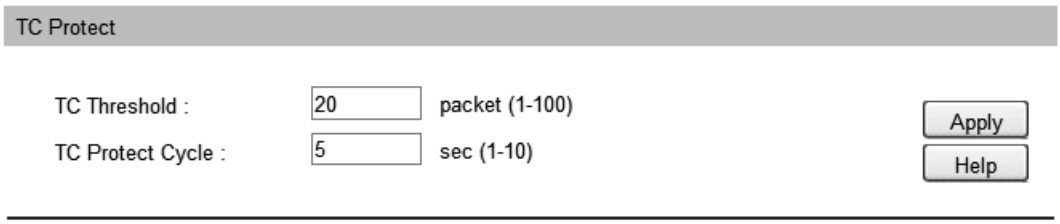


Figure 7-11 TC Protect

The following entries are displayed on this screen:

➢ **TC Protect**

TC Threshold: Enter a number from 1 to 100. It is the maximum number of the TC-BPDUs received by the switch in a TC Protect Cycle. The default value is 20.

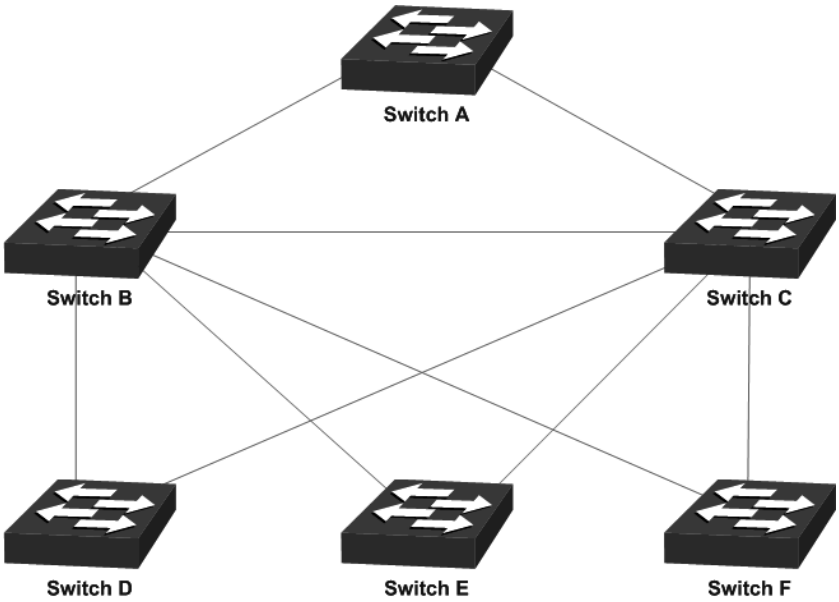
TC Protect Cycle: Enter a value from 1 to 10 to specify the TC Protect Cycle. The default value is 5.

7.5 Application Example for STP Function

➢ **Network Requirements**

- Switch A, B, C, D and E all support MSTP function.
- A is the central switch.
- B and C are switches in the convergence layer. D, E and F are switches in the access layer.
- There are 6 VLANs labeled as VLAN101-VLAN106 in the network.
- All switches run MSTP and belong to the same MST region.
- The data in VLAN101, 103 and 105 are transmitted in the STP with B as the root bridge. The data in VLAN102, 104 and 106 are transmitted in the STP with C as the root bridge.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch A:

Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN→VLAN Config** page, configure the link type of the related ports as Tagged, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable STP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→STP Config→Port Config** page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On **Spanning Tree→MSTP Instance→Region Config** page, configure the region and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-to-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.

- Configure Switch B:

Step	Operation	Description

Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN→VLAN Config** page, configure the link type of the related ports as Tagged, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable STP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→STP Config→Port Config** page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On **Spanning Tree→MSTP Instance→Region Config** page, configure the region and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-to-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.
5	Configure switch B as the root bridge of Instance 1	On **Spanning Tree→MSTP Instance→Instance Config** page, configure the priority of Instance 1 to be 0.
6	Configure switch B as the designated bridge of Instance 2	On **Spanning Tree→MSTP Instance→Instance Config** page, configure the priority of Instance 2 to be 4096.

- Configure Switch C:

Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN→VLAN Config** page, configure the link type of the related ports as Tagged, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable STP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→STP Config→Port Config** page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On **Spanning Tree→MSTP Instance→Region Config** page, configure the region and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-to-Instance mapping

	region	table. Map VLAN101, 103 and 105 to Instance 1; map VLAN102, 104 and 106 to Instance 2.
5	Configure switch C as the root bridge of Instance 1	On **Spanning Tree→MSTP Instance→Instance Config** page, configure the priority of Instance 1 to be 4096.
6	Configure switch C as the root bridge of Instance 2	On **Spanning Tree→MSTP Instance→Instance Config** page, configure the priority of Instance 2 to be 0.

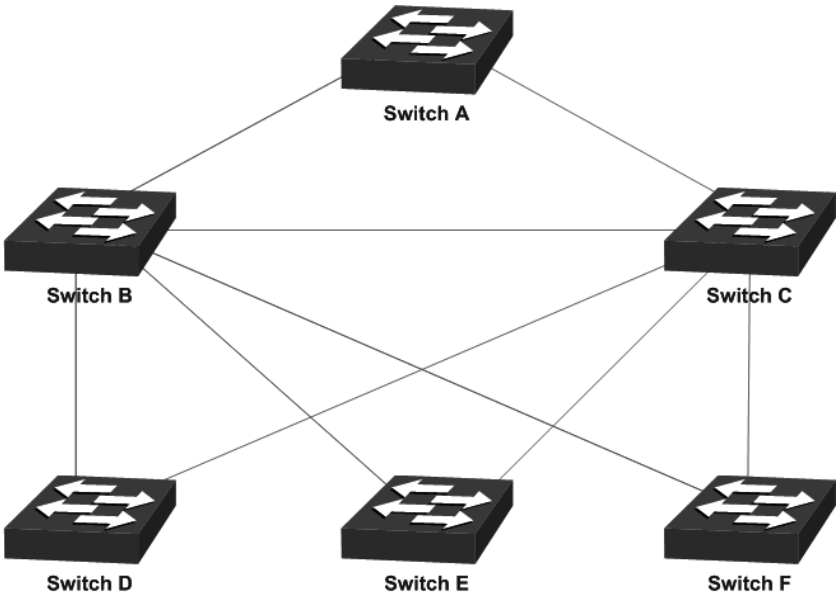
- Configure Switch D:

Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN→VLAN Config** page, configure the link type of the related ports as Tagged, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable STP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→STP Config→Port Config** page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On **Spanning Tree→MSTP Instance→Region Config** page, configure the region and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-to-Instance mapping table. Map VLAN101, 103 and 105 to Instance 1; map VLAN102, 104 and 106 to Instance 2.

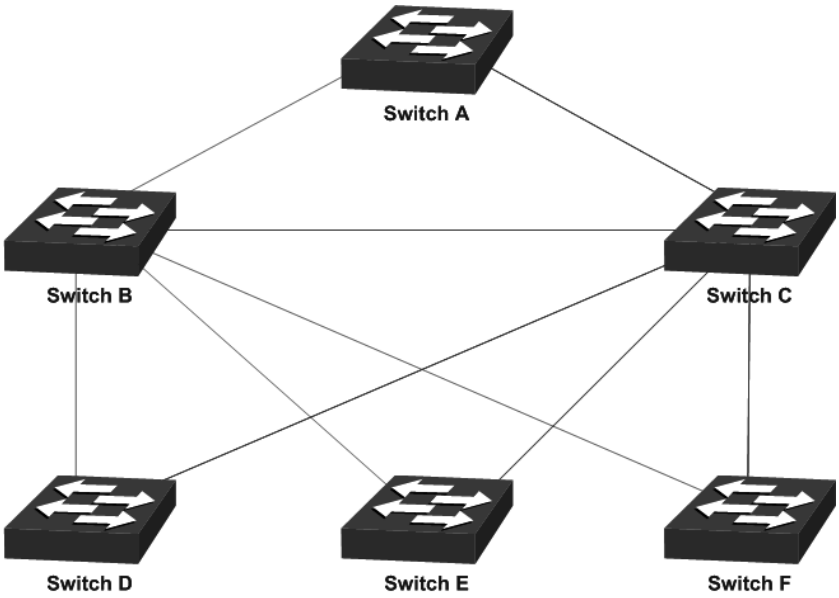
- The configuration procedure for switch E and F is the same with that for switch D.

➢ **The topology diagram of the two instances after the topology is stable**

- For Instance 1 (VLAN101, 103 and 105), the red paths in the following figure are connected links; the gray paths are the blocked links.



- For Instance 2 (VLAN102, 104 and 106), the blue paths in the following figure are connected links; the gray paths are the blocked links.



➢ **Suggestion for Configuration**

- Enable TC Protect function for all the ports of switches.
- Enable Root Protect function for all the ports of root bridges.
- Enable Loop Protect function for the non-edge ports.

Enable BPDU Protect function or BPDU Filter function for the edge ports which are connected to the PC and server.

Return to CONTENTS

Chapter 8 Ethernet OAM

➢ OAM Overview

Ethernet OAM (Operation, Administration, and Maintenance) is a Layer 2 protocol for monitoring and troubleshooting Ethernet networks. It can report the network status to network administrators through the OAMPDUs exchanged between two OAM entities, facilitating network management.

Ethernet OAM is a slow protocol with very limited bandwidth requirement. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on data traffic is negligible.

On a point-to-point link between two OAM-enabled devices, OAM helps to monitor the link status from the following three points.

1. Link performance monitoring, for detecting link errors.
2. Fault detection and alarm, for reporting link errors to the administrators.
3. Loopback testing, for detecting link errors through non-OAMPDUs.

Currently, Ethernet OAM is mainly used to monitor the data link in the "last mile".

➢ OAMPDUs

There are six types of OAMPDUs. The following figure shows the details of the most commonly used OAMPDUs, namely, Information OAMPDU, Event Notification OAMPDU and Loopback Control OAMPDU.

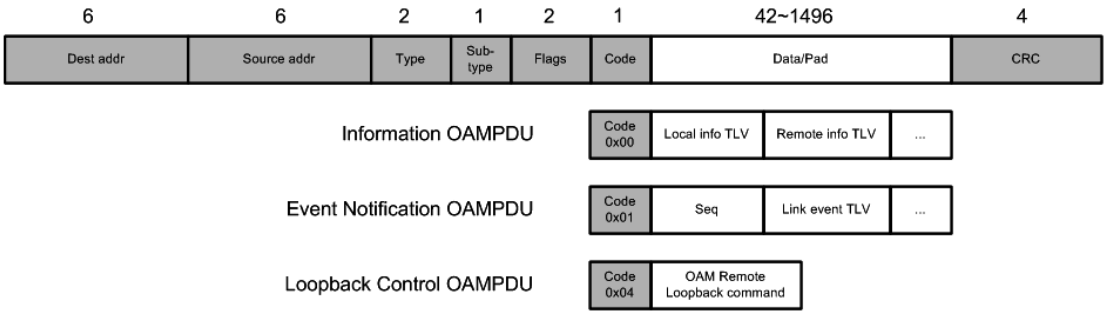


Figure 8-1 OAMPDUs

As Figure 8-1 shows, OAMPDUs are standard length Ethernet frames. They must be untagged and range from 64 to 1518 bytes.

(1) Dest addr: The Dest addr (Destination MAC address) of an OAMPDU is the Slow_Protocols_Multicast address (01:80:c2:00:00:02).
(2) Source addr: The Source addr is the MAC address associated with the port through which the OAMPDU is transmitted.
(3) Type: The type field is fixed to 0x8809.
(4) Sub-type: The Sub-type field is fixed to 0x03.
(5) Flags: The flags field contains status bits of an OAM entity.

(6) Code: The code field identifies the specific type of OAMPDU. As mentioned above, Information OAMPDU, Event Notification OAMPDU and Loopback control OAMPDU are commonly used, and their codes are 0x00, 0x01, and 0x04. The three OAMPDUs are described as follows.

Information OAMPDU: Information OAMPDU is used for discovery. It transmits the state information of an OAM entity (including local, remote, and organization-specific information) to another OAM entity, and maintains OAM connection.

Event Notification OAMPDU: Event Notification OAMPDU is used for link monitoring. It is sent as an alarm when a failure occurs to the link connecting the local OAM entity and a remote OAM entity.

Loopback Control OAMPDU: Loopback Control OAMPDU is used to control the remote client's OAM remote loopback state. Its Data field consists of a remote loopback command to enable or disable the OAM remote loopback, so that the local client can enable/disable loopback on the remote OAM entity.

- **OAM Functions**

As defined by IEEE 802.3 Clause 57, *Ethernet in the First Mile,* OAM functions include Discovery, Link Monitoring, Remote Failure Indication, and Remote Loopback.

Discovery

Discovery is the first phase of Ethernet OAM. During this phase, an OAM entity discovers other OAM entities and establishes connections using Information OAMPDUs.

As for OAM connection, an OAM entity can operate in two modes: active and passive. Only the active OAM entity can initiate an OAM connection process. The passive OAM entity waits and responds to OAM connection establishment requests. Interconnected OAM entities notify the peer of their OAM configuration information and the OAM capabilities of the local nodes to support OAM by exchanging Information OAMPDUs, and then determine if OAM connections can be established. Only when the settings concerning Loopback, link detecting, and link event of the both side match can an OAM connection be established.

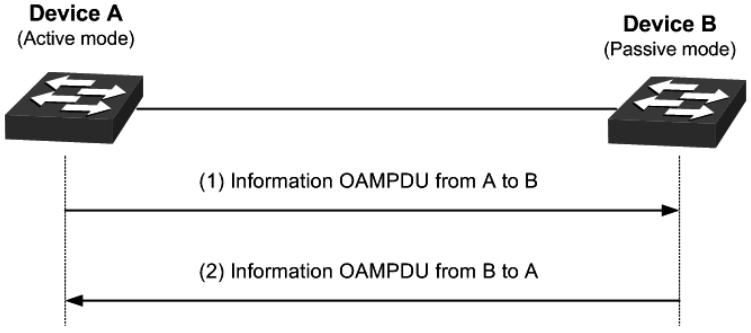


Figure 8-2 OAM Discovery

The difference between active OAM mode and passive OAM mode is shown as follows.

Item	Active OAM mode	Passive OAM mode
Initiating OAM Discovery	Available	Unavailable

Item	Active OAM mode	Passive OAM mode
Responding to OAM Discovery	Available	Available
Transmitting Information OAMPDUs	Available	Available
Transmitting Event Notification OAMPDUs	Available	Available
Transmitting Information OAMPDUs with the Data/Pad field being empty	Available	Available
Transmitting Loopback Control OAMPDUs	Available	Unavailable
Responding to Loopback Control OAMPDUs	Available (if both sides operate in active OAM mode)	Available
Transmitting organization-specific OAMPDUs	Available	Available

Table 8-1 Differences between active OAM mode and passive OAM mode

After an OAM connection is established, the OAM entities on both sides exchange Information OAMPDUs periodically to keep the OAM connection valid. The OAM entity considers the OAM connection invalid if it does not receive the Information OAMPDU from the peer entity for 5 seconds.

Link Monitoring

Link Monitoring is for detecting and locating link faults under a variety of circumstances. When there are problems detected on the link, the device will send its remote peer the Event Notification OAMPDUs to report link events. The link events are described as follows:

OAM Link Events	Description
Symbol Period Error	A Symbol Period Error event occurs if the number of symbol errors exceeds the threshold during a specific period of time.
Frame Error	A Frame Error event occurs if the number of frame errors exceeds the threshold during a specific period of time.
Frame Period Error	A Frame Period Error event occurs if the number of frame errors in specific number of received frames exceeds the threshold.
Frame Seconds Error	A Frame Seconds Error event occurs if the number of error frame seconds exceeds the threshold

	during a specific period of time. A second is called an error frame second if error frames occur in the second.

Table 8-2 OAM Link Events

Remote Failure Indication

Faults in Ethernet are difficult to detect, especially when the physical connection in the network is not interrupted but network performance degrades gradually. A flag in the OAMPDU allows an OAM entity to convey failure conditions to its peer. The failure conditions are as follows:

Link Fault: Peer link signal is lost. This is sent once per second in the Information OAMPDU.
Dying Gasp: An unrecoverable fault, such as power failure, occurs. This is sent immediately and continuously.
Critical Event: Unspecified critical event occurs. This is sent immediately and continuously.
As Information OAMPDUs are sent between the OAM entities periodically, an OAM entity can inform one of its OAM peers of link faults through Information OAMPDUs. So the network administrator can get informed of the link faults and take action in time.

Remote Loopback

Remote loopback helps to ensure the quality of links during installation or when troubleshooting. After the OAM connection is established, the active OAM entity can put its OAM peer into loopback mode using a loopback control OAMPDU.

With remote loopback enabled, the active OAM entity sends remote loopback requests and the peer responds. If the peer is in the loopback mode, it returns all frames except OAMPDUs and pause frames to the senders along the original paths. Through these return frames, administrators can test the link performance like delay, jitter, and frame loss rate.

The following figure shows how remote loopback testing works.

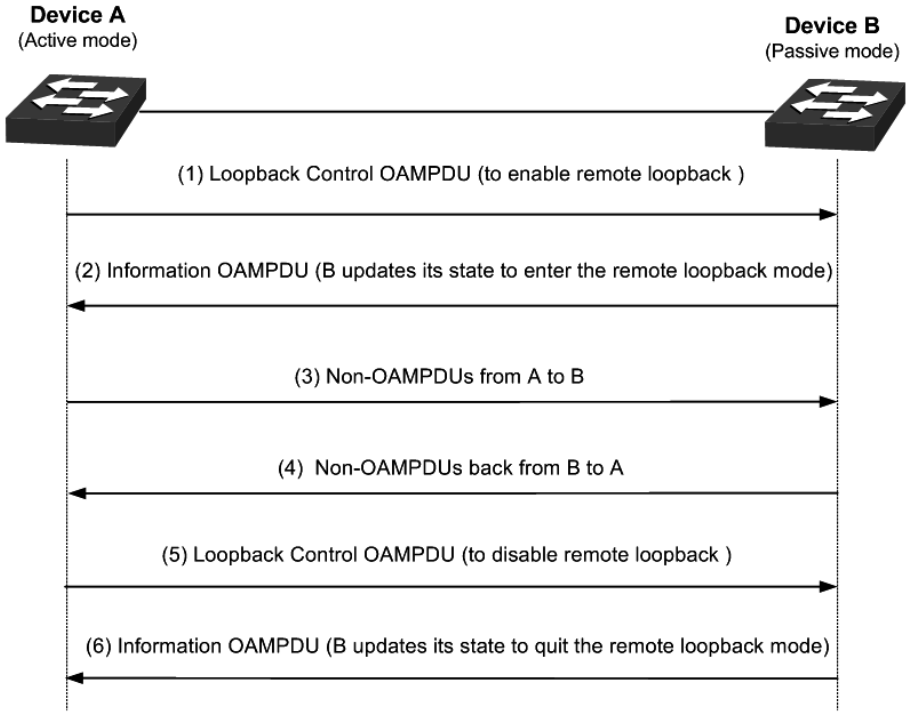


Figure 8-3 Remote Loopback

8.1 Basic Config

On the **Basic Config** page, you can enable the Ethernet OAM function on a specified port, and configure its OAM mode as active or passive. Also, you can check out the connection status on the **Discovery Info** page.

8.1.1 Basic Config

Choose the menu **Ethernet OAM**→ **Basic Config**→ **Basic Config** to load the following page.

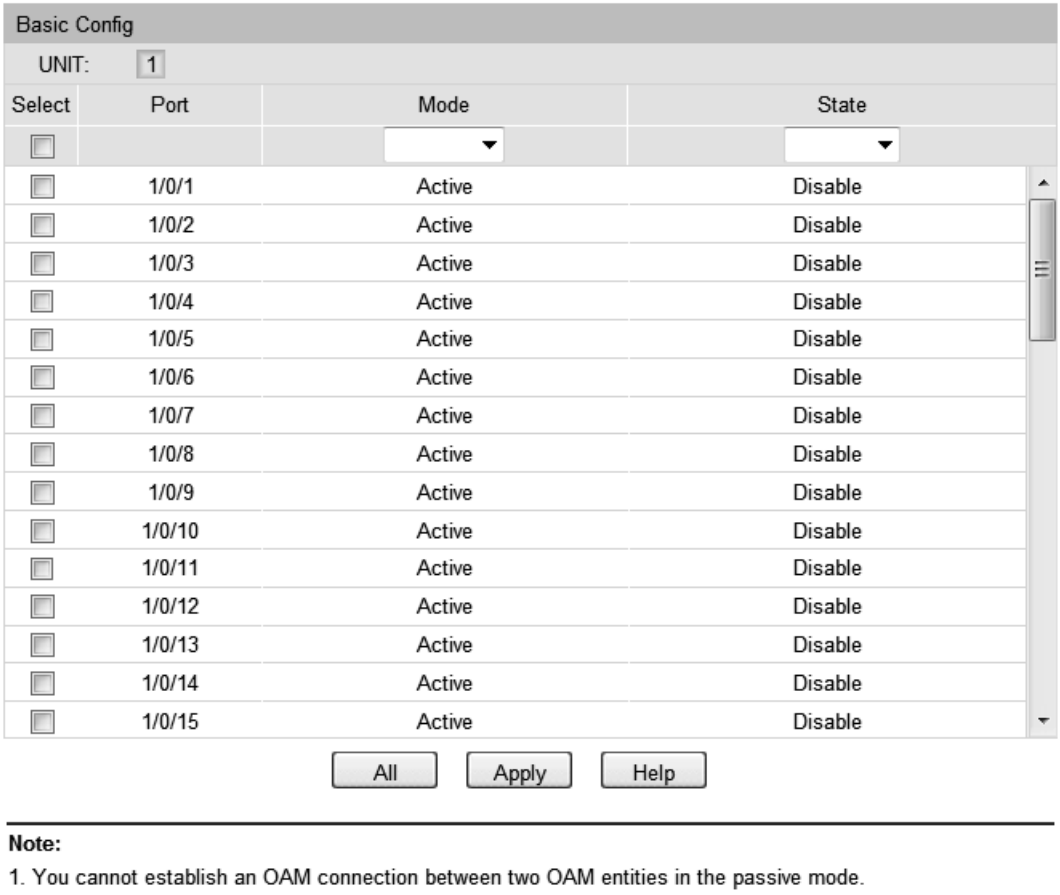


Figure 8-4 Basic Config

The following entries are displayed on this screen:

- **Basic Config**

Select: Select the desired port for configuration. It is multi-optional.

Mode: Select the OAM mode for the desired port.

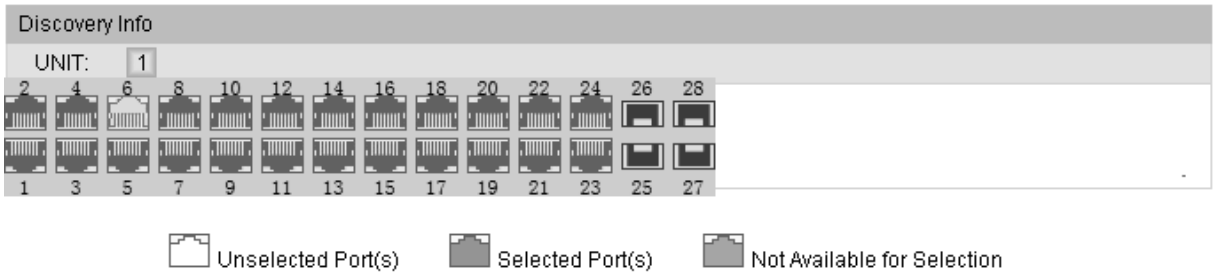
State: Select Enable/Disable the Ethernet OAM function for the desired port.

Note:

You cannot establish an OAM connection between two OAM entities that work in the passive mode.

8.1.2 Discovery Info

Choose the menu **Ethernet OAM→ Basic Config→ Discovery Info** to load the following page.



Local Client	
OAM:	Enable
Mode:	Active
Max OAMPDU:	1518 Bytes
Remote Loopback:	Supported
Unidirection:	Not Supported
Link Monitoring:	Supported
Variable Request:	Not Supported
PDU Revision:	0
Operation Status:	Operational
Loopback Status:	No Loopback

Remote Client	
Mode:	Active
Mac Address:	00-00-00-00-AA-BB
Vendor(OUI):	00055d
Max OAMPDU:	1518 Bytes
Remote Loopback:	Supported
Unidirection:	Not Supported
Link Monitoring:	Supported
Variable Request:	Not Supported
PDU Revision:	0
Vendor Information:	00000000

Figure 8-5 Discovery Info

The following entries are displayed on this screen:

- **Local Client**

The local client part shows the information of the local OAM entity.

OAM: Displays whether the OAM function is enabled or disabled on the selected port.

Mode: Displays the OAM mode of the selected port.

Max OAMPDU: Displays the maximum size of the OAMPDU.

Remote Loopback: Displays whether the local client supports remote loopback function.

Unidirection: Displays whether the local client supports unidirectional OAM operation.

Some devices support unidirectional OAM operation. These devices provide an OAMPDU-based mechanism to notify the remote OAM entity when one direction of a link is non-operational and therefore data transmission is disabled.

Link Monitoring: Displays whether the local client supports link monitoring function.

Variable Request: Displays whether the local client supports variable request. If supports, the local client can send some variable requests to the remote client to learn about the link status from the response of the remote client.

PDU Revision: Displays the Information TLV revision of Information OAMPDU.

Operation Status: Displays the operating status of the OAM connection.

- Disable: OAM is disabled on this port.
- LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.
- PassiveWait: The port is in passive mode and is waiting to see if the peer device is OAM capable.
- ActiveSendLocal: The port is in active mode and is sending local information.
- SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.
- SendLocalAndRemoteOK: The local device agrees the OAM peer entity.
- PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.
- PeeringRemotelyRejected: The remote OAM entity rejects the local device.
- NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex ports. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.

Loopback Status: Displays the loopback status.

- No Loopback: Neither the local client nor the remote client is in the loopback mode.
- Local Loopback: The local client is in the loopback mode.
- Remote Loopback: The remote client is in the loopback mode.

➢ **Remote Client**

The local client part shows the information of the remote OAM entity.

Mode:	Displays the OAM mode of the remote client.
Mac Address:	Displays the MAC address of the remote client.
Vendor(OUI):	Displays the vender's OUI of the remote client. An OUI address is a unique identifier assigned by IEEE to a device vendor.
Max OAMPDU:	Displays the maximum size of the OAMPDU.
Remote Loopback:	Displays whether the remote client supports remote loopback function.
Unidirection:	Displays whether the remote client supports unidirectional OAM operation.
Link Monitoring:	Displays whether the remote client supports link monitoring function.
Variable Request:	Displays whether the remote client supports variable request.
PDU Revision:	Displays the TLV revision of the OAMPDU.
Vendor Information:	Displays the vender information of the remote client.

8.2 Link Monitoring

On this page, you can configure the parameters about OAM link events, including the threshold and the detection period. Also, you can choose whether to notify the link event.

Choose the menu **Ethernet OAM→Link Monitoring→Link Monitoring** to load the following page.

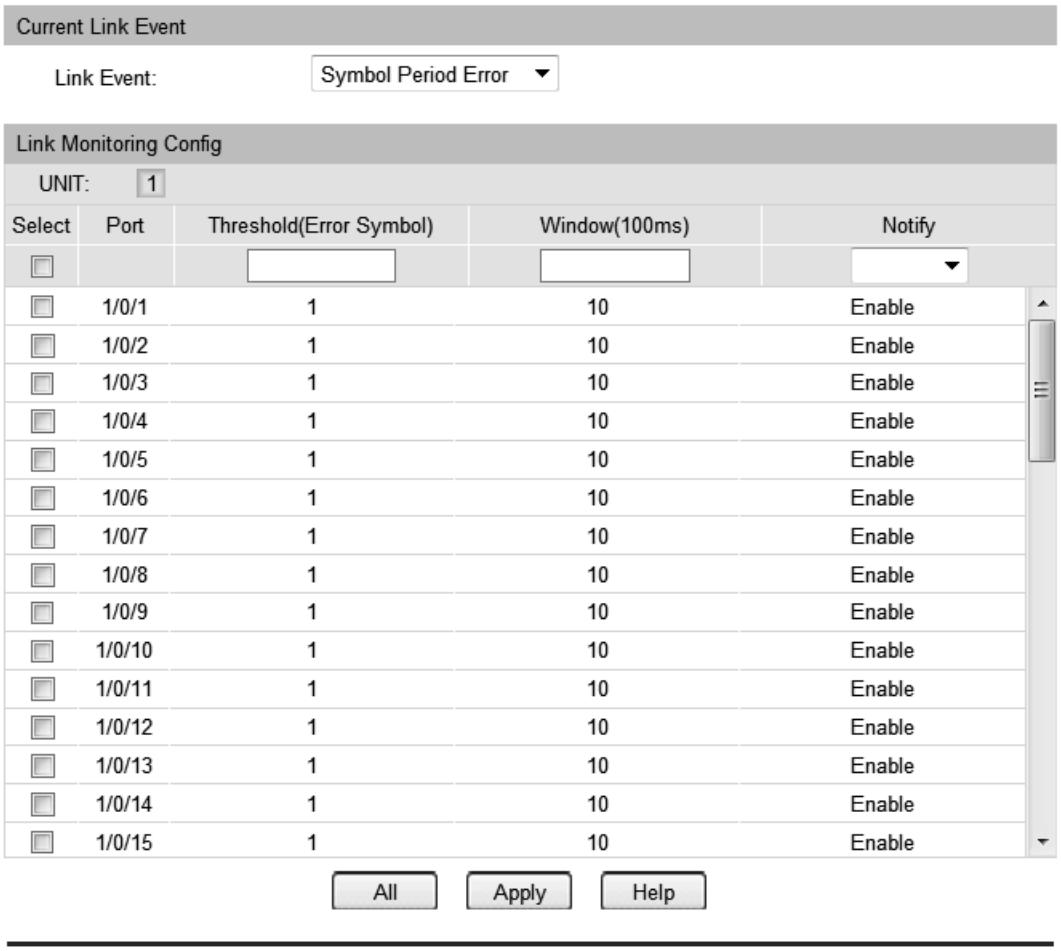


Figure 8-6 Link Monitoring

The following entries are displayed on this screen:

- **Link Monitoring Config**

Link Event: Select one type of the link events to configure. Link events include Symbol Period Error, Frame Error, Frame Period Error, and Frame Seconds Error. For more details about link events, please refer to **OAM Link Events**.

Select: Select the desired port for configuration. It is multi-optional.

Threshold: Specify the threshold for the selected link event.

- For Symbol Period Error, it is the number of error symbols in the period that is required to be exceeded.
- For Frame Error, it is the number of error frames in the period (measured by 100ms) that is required to be exceeded.
- For Frame Period Error, it is the number of error frames in the period (measured by frames) that is required to be exceeded.
- For Frame Seconds Error, it is the number of error frame seconds in the period that is required to be exceeded.

Window: Specify the detection period.

- For Frame Period Error, the period is specified by a number of received frames.
- For other link events, the period is specified by a time interval.

Notify: Choose whether to notify the selected link event or not.

8.3 RFI

On this page, you can choose whether to notify the link faults like dying gasp and critical event.

Choose the menu **Ethernet OAM→RFI→Remote Failure Indication** to load the following page.

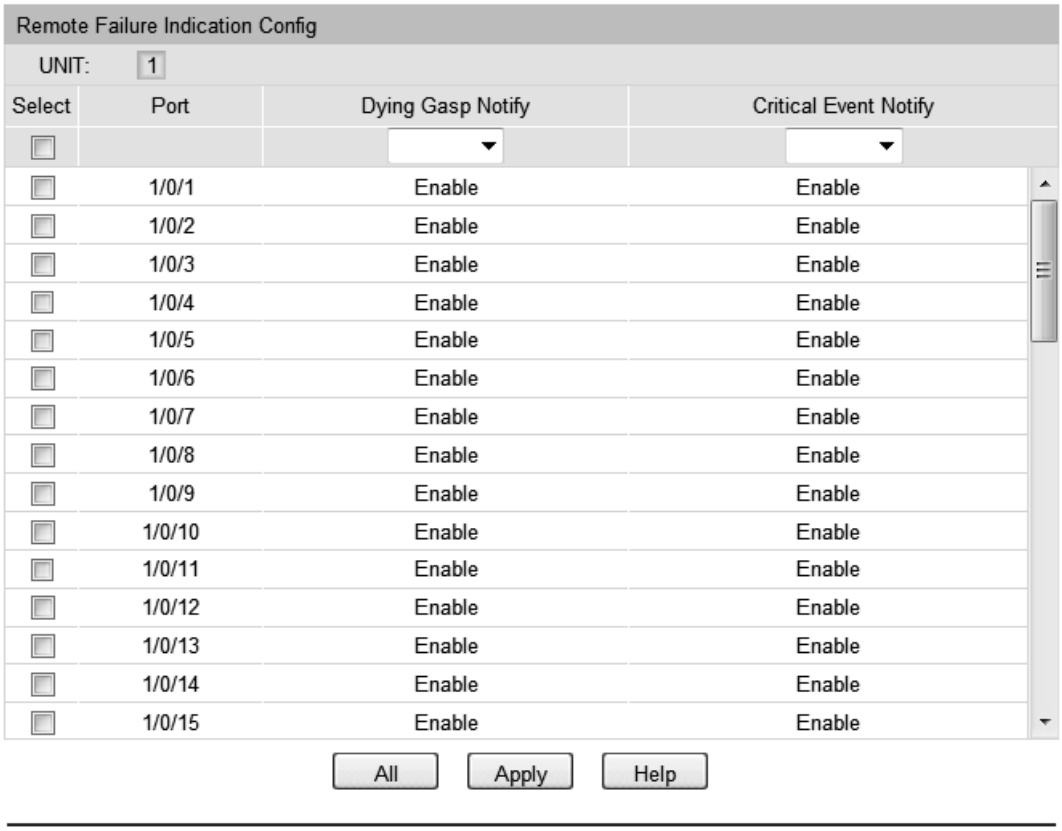


Figure 8-7 Remote Failure Indication

The following entries are displayed on this screen:

➢ **Remote Failure Indication Config**

Select: Select the desired port for configuration. It is multi-optional.

Dying Gasp Notify: Choose whether to notify the dying gasp or not.

Critical Event Notify: Choose whether to notify the critical event or not.

8.4 Remote Loopback

On this page, you can initiate remote loopback if the OAM connection is established and the local client works in active mode. You can also choose to ignore or to process the received remote loopback request.

Choose the menu **Ethernet OAM→Remote Loopback→Remote Loopback** to load the following page.

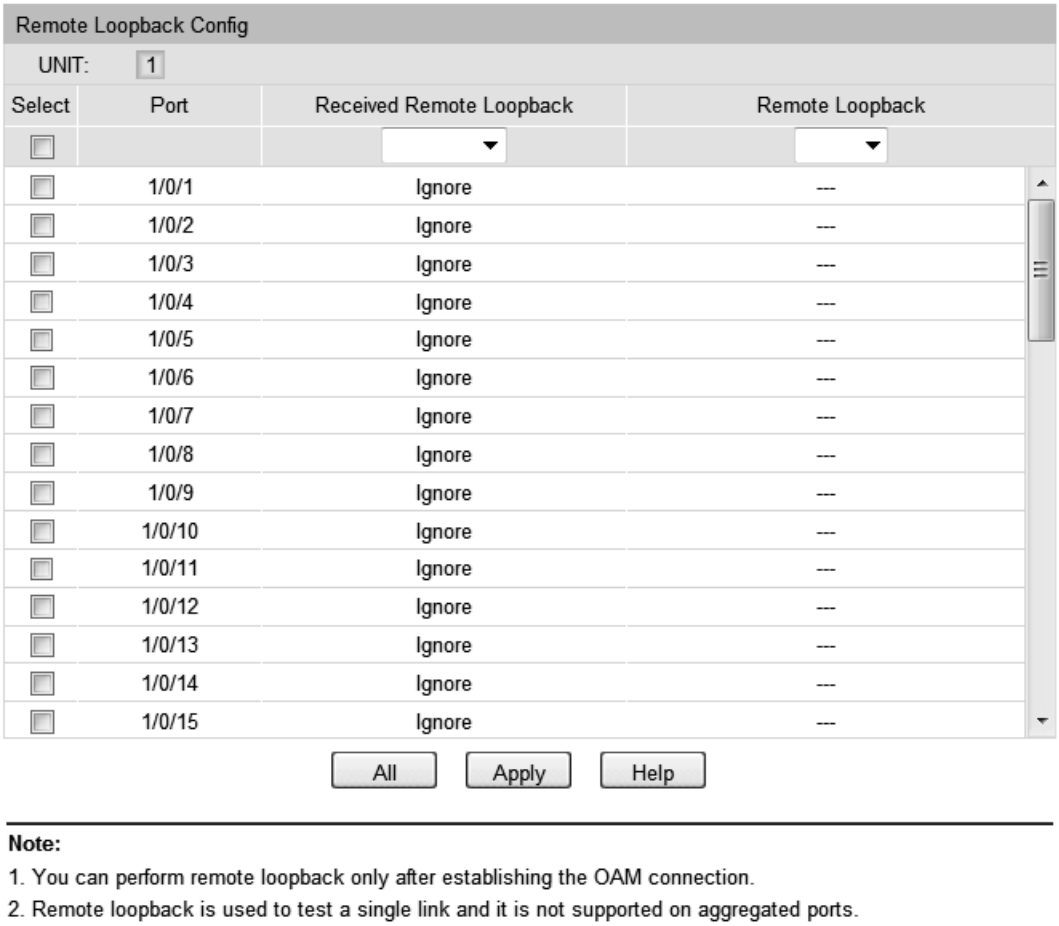


Figure 8-8 Remote Loopback

The following entries are displayed on this screen:

- **Remote Loopback Config**

  Select: Select the desired port for configuration. It is multi-optional.

  Received Remote Loopback: Choose to ignore or to process the received remote loopback request.

  Remote Loopback: To start or stop the remote loopback.

8.5 Statistics

You can view the statistics about the detailed Ethernet OAM traffic information and event log information of a specific port here.

8.5.1 Statistics

On this page, you can view the detailed Ethernet OAM traffic information of a specific port. The device will recount the numbers every time you click the **clear** button or the device is rebooted.

Choose the menu **Ethernet OAM→Statistics→Statistics** to load the following page.

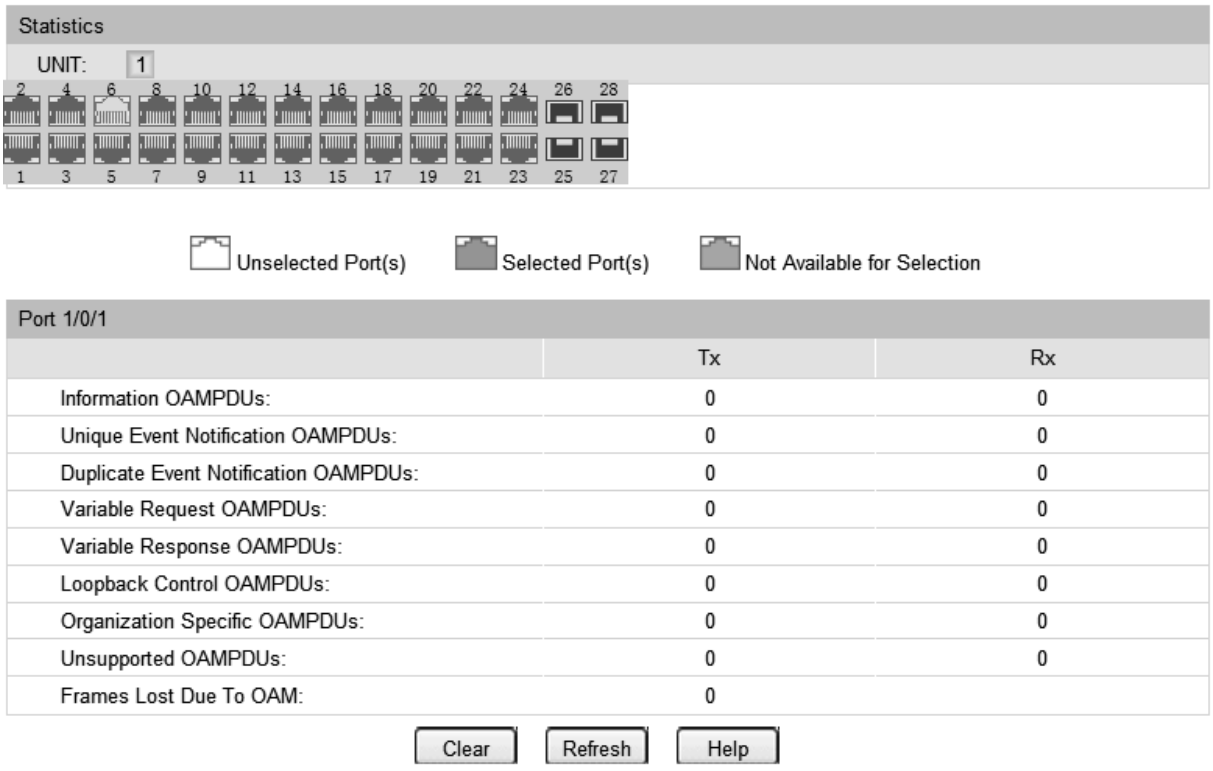


Figure 8-9 Statistics

The following entries are displayed on this screen:

- **Statistics**

Port Select:	Select a desired port from the port panel.
Tx:	Displays the number of OAMPDUs that have been transmitted on the port.
Rx:	Displays the number of OAMPDUs that have been received on the port.
Information OAMPDUs:	Displays the number of information OAMPDUs that have been transmitted or received on the port.

Unique Event Notification OAMPDUs:	Displays the number of unique event notification OAMPDUs that have been transmitted or received on the port.
Duplicate Event Notification OAMPDUs:	Displays the number of duplicate event notification OAMPDUs that have been transmitted or received on the port.
Variable Request OAMPDUs:	Displays the number of variable request OAMPDUs that have been transmitted or received on the port.
Variable Response OAMPDUs:	Displays the number of variable response OAMPDUs that have been transmitted or received on the port.
Loopback Control OAMPDUs:	Displays the number of loopback control OAMPDUs that have been transmitted or received on the port.
Organization Specific OAMPDUs:	Displays the number of organization specific OAMPDUs that have been transmitted or received on the port.
Unsupported OAMPDUs:	Displays the number of unsupported OAMPDUs that have been transmitted or received on the port.
Frames Lost Due To OAM:	Displays the number of frames that would otherwise be transmitted by the OAM sublayer, but did not due to an internal OAM sublayer transmit error.

8.5.2 Event Log

On this page, you can view the detailed Ethernet OAM event log information of a specific port. The device will recount the numbers every time you click the **clear** button or the device is rebooted.

Choose the menu **Ethernet OAM→Statistics→Event Log** to load the following page.

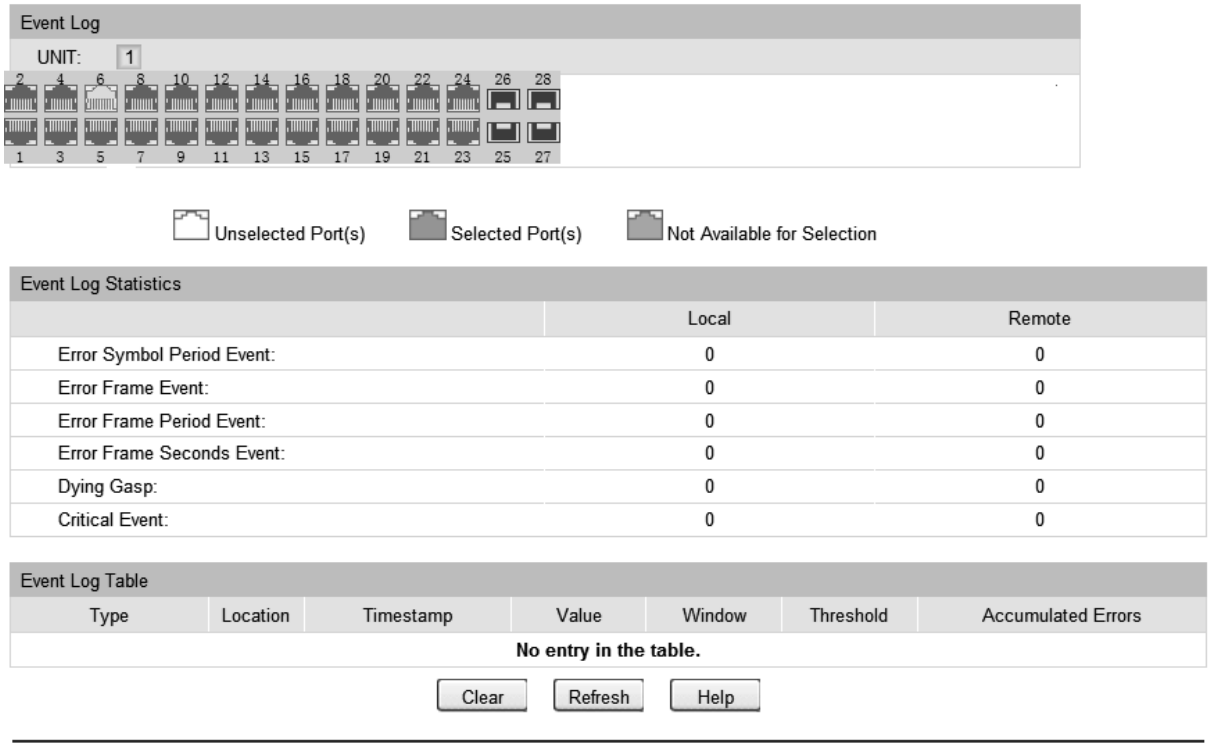


Figure 8-10 Event Log

The following entries are displayed on this screen:

- **Event Log Statistics**

Port Select: Select a desired port from the port panel.

Local: Displays the number of link events that have occurred on the local link.

Remote: Displays the number of link events that have occurred on the remote link.

Error Symbol Event: Displays the number of error symbol period link events that have occurred on the local link or remote link.

Error Frame Event: Displays the number of error frame link events that have occurred on the local link or remote link.

Error Frame Period Event: Displays the number of error frame period link events that have occurred on the local link or remote link.

Error Frame Seconds Event: Displays the number of error frame seconds link events that have occurred on the local link or remote link.

Dying Gasp: Displays the number of Dying Gasp link events that have occurred on the local link or remote link.

Critical Event: Displays the number of Critical Event link events that have occurred on the local link or remote link.

➢ **Event Log Table**

Type:	Displays the type of the link event.
Location:	Displays the location where the link event occurred.
Timestamp:	Displays the time reference when the link event occurred.
Value:	Displays the number of errors in the period.
Window:	Displays the period of the link event.
Threshold:	Displays the number of errors that is required to be exceeded in order for the event to be generated.
Accumulated Errors:	Displays the number of errors that have been detected since the OAM sublayer was reset.

8.6 DLDP

➢ **DLDP Overview**

DLDP (Device Link Detection Protocol) is a Layer 2 protocol that enables devices connected through fiber or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect whether a unidirectional link exists. When a unidirectional link appears, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional links can cause a variety of problems, such as spanning-tree topology loops. Once detecting a unidirectional link, DLDP can shut down the related port automatically or inform users.

➢ **DLDP Operation Mechanism**

1. DLDP Link States

DLDP defines 6 link states for a device：Initial, Inactive, Active, Advertisement, Probe and Disable.

State	Description
Initial	DLDP is disabled.
Inactive	DLDP is enabled but the link is down.
Active	This state is temporary and it indicates that: 1. DLDP is enabled and the link is up. 2. The neighbor entries in this device are empty.
Advertisement	This state indicates that no unidirectional link is detected, which includes two kinds of situations: 1. This device establishes bidirectional links with all its neighbors. 2. DLDP remains in Active state for more than 5 seconds.
Probe	A device enters this state from the Active state if it receives a packet from

State	Description
	an unknown neighbor. In this state, the device will send out Probe packets to detect whether the link is unidirectional.
Disable	This state indicates that a unidirectional link is detected.

Table 8-3 DLDP Link State

2. DLDP Work Process

The general DLDP work process chart is shown below:

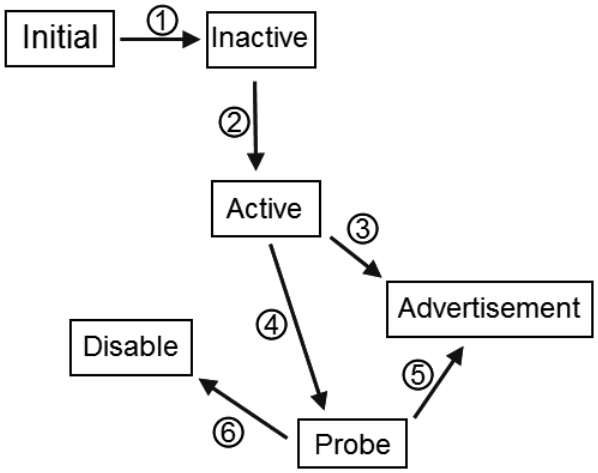


Figure 8-11 DLDP Process

The process is illustrated below:

①: When DLDP is enabled on the link in down state, the DLDP link state will transit to Inactive.

②: When the DLDP-enabled link is up, the DLDP link state will transit to Active. The device will send out Advertisement packets to the peer device with resynchronization tag in this state.

③: If the device doesn't receive any DLDP packets within 5 seconds, the DLDP link state will transit to Advertisement.

④: After receiving a packet from an unknown neighbor, the device's link state will transit from Active to Probe, and then send out several probe packets to detect the link state.

⑤: If the device receives echo packets from its peer device, the link state between them will be tagged as bidirectionally linked and the DLDP state will transit from Probe to Advertisement. A device in the Advertisement state will send advertisement packets.

⑥: If the device receives no echo packets after a specified period of time, the link will be tagged as unidirectional and the DLDP state will transit from Probe to Disable. This port will be shut down automatically or manually (depending on the Shut Mode configured).

The typical bidirectional link detection process is ②→④→⑤, and the typical unidirectional link detection process is ②→④→⑥.

On the **DLDP** page, you can enable the DLDP state globally and configure the interval of the advertisement packets and the port shutdown mode. You can also configure the refresh frequency of the port states and reset the certain port's DLDP state manually.

Choose the menu **Ethernet OAM→ DLDP→ DLDP Config** to load the following page.

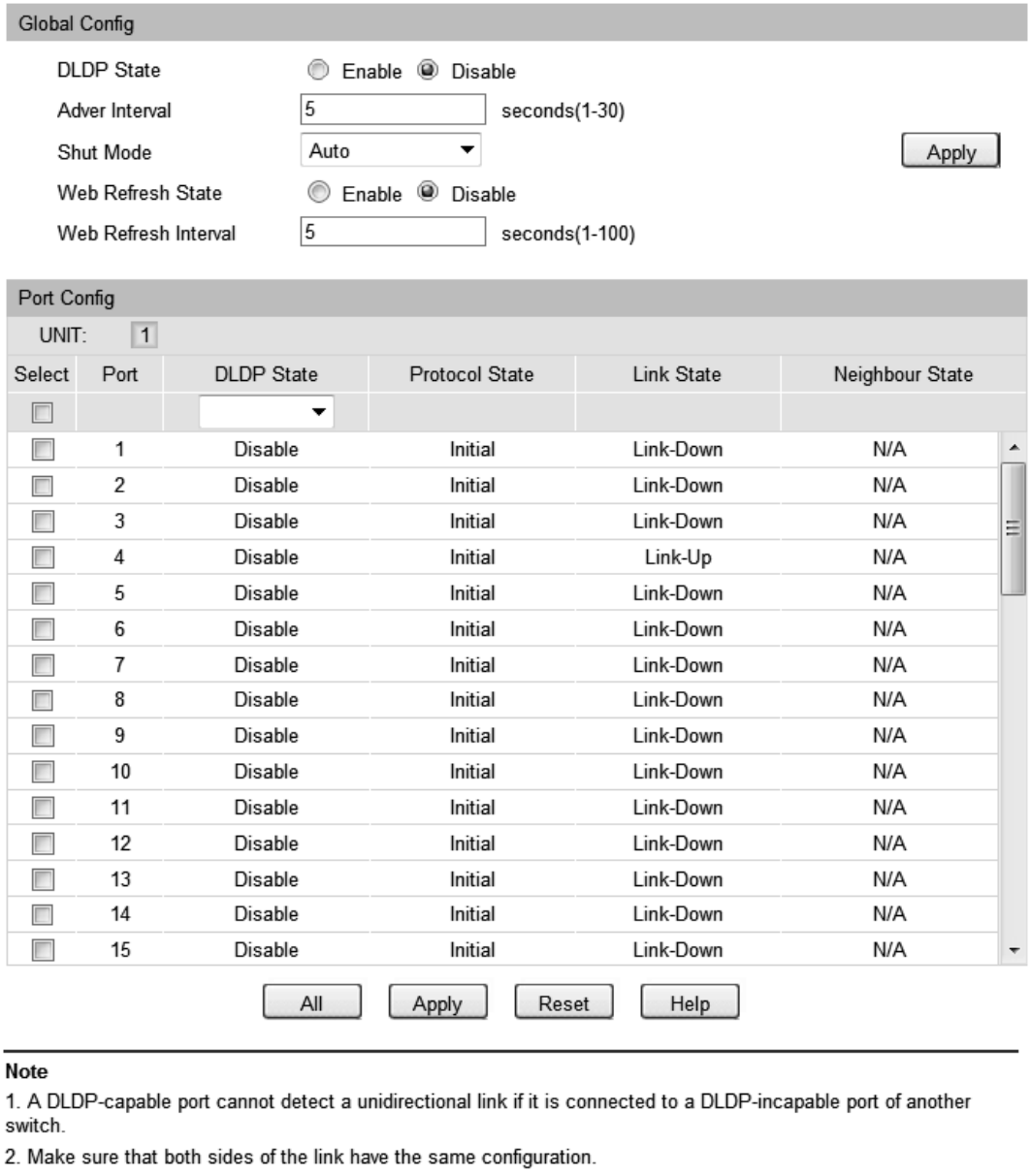


Figure 8-12 DLDP Config

The following entries are displayed on this screen:

- **Global Config**

  DLDP State: Enable/Disable the DLDP function globally.

  Adver Interval: Config the interval to send advertisement packets, ranging from 1 to 30 seconds. The default value is 5 seconds.

Shut Mode: Once detecting a unidirectional link, the port can be shut down in one of the following two modes:

- **Auto**: In this mode, DLDP generates logs and traps and shuts down the corresponding port on detecting unidirectional links, and the DLDP link state transits to Disable.
- **Manual**: In this mode, DLDP only generates logs and traps if it detects unidirectional links, and the operation to shut down the unidirectional link ports is accomplished by the administrator.

Web Refresh State: Enable/Disable the web automatic refresh function.

Web Refresh Interval: Configure the interval to refresh the web page, ranging from 1 to 100 seconds, and the default value is 5 seconds.

➢ **Port Config**

Select: Select the desired port for configuration. It is multi-optional.

Port: Port list of the switch.

DLDP State: Enable/Disable DLDP on the selected port.

Protocol State: Displays the DLDP protocol state.

Link State: Displays the state of the links.

Neighbor State: Displays the state of the selected port's neighbor.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Enable DLDP globally.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, configure DLDP State as Enable under the Global Config tab.
2	Enable DLDP on the specified port.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, configure DLDP State as Enable on specified port in the Port Config table.
3	Configure Shut Mode.	Optional. On the **Ethernet OAM→DLDP→DLDP Config** page, configure the Shut Mode as Auto or Manual under the Global Config tab.
4	Reset DLDP state.	Optional. On the **Ethernet OAM→DLDP→DLDP Config** page, select the specified ports or select all the ports in the Port Config table and click the **Reset** button to restore their state.

8.7 Application Example for DLDP

➢ **Network requirements**

1. Device A and Device B are connected through two fiber pairs, which are cross-connected, as shown in Figure 8-13.
2. The unidirectional link should be disconnected once being detected, and the ports shut down by DLDP can be restored after the fiber pairs are correctly connected.

➢ **Network Diagram**

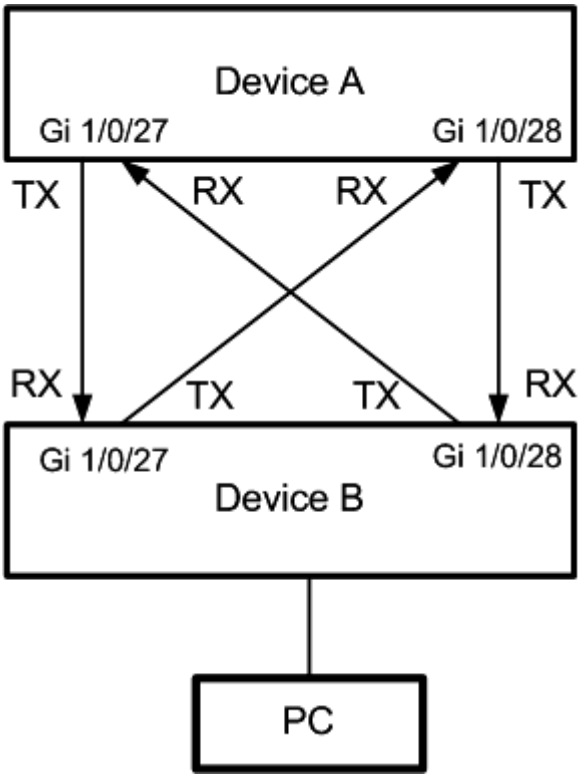


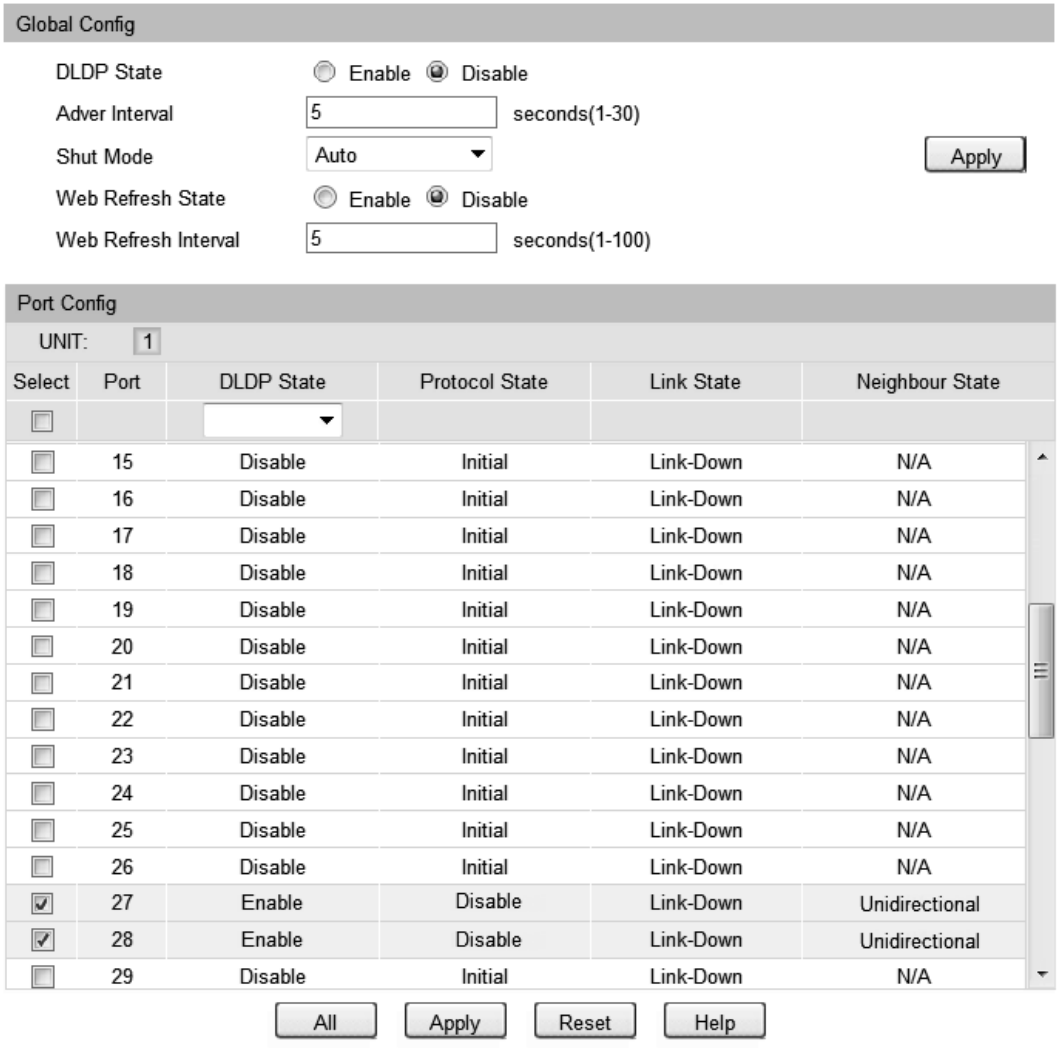
Figure 8-13 DLDP Application Example

➢ **Configuration Procedure**

Step	Operation	Description
1	Enable DLDP globally.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, configure DLDP State as enable under the Global Config tab in device A and B.
2	Enable DLDP on the specified ports.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, configure DLDP State as enable on Gigabit Ethernet ports 1/0/27 and 1/0/28 in the Port Config table in device A and device B.
3	Configure Shut Mode.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, configure the Shut Mode as auto under the Global Config tab in device A and B.

4	Check the ports' state.	Required. On the **Ethernet OAM→DLDP→DLDP Config** page, select ports 1/0/27 and 1/0/28 in the Port Config table and click the **Reset** button to bring them up.

The DLDP information of Gigabit Ethernet ports 1/0/27 and 1/0/28 is shown below:



Note

1. A DLDP-capable port cannot detect a unidirectional link if it is connected to a DLDP-incapable port of another switch.
2. Make sure that both sides of the link have the same configuration.

After these four ports are correctly connected, select ports 1/0/27 and 1/0/28 in the Port Config table and click the **Reset** button to restore their state from Disable.

Chapter 9 Multicast

➢ Multicast Overview

In the network, packets are sent in three modes: unicast, broadcast and multicast. In unicast, the source server sends separate copy information to each receiver. When a large number of users require this information, the server must send many pieces of information with the same content to the users. Therefore, large bandwidth will be occupied. In broadcast, the system transmits information to all users in a network. Any user in the network can receive the information, no matter the information is needed or not.

Point-to-multipoint multimedia business, such as video conferences and VoD (video-on-demand), plays an important part in the information transmission field. Suppose a point to multi-point service is required, unicast is suitable for networks with sparsely users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring this information is not certain, unicast and broadcast deliver a low efficiency. Multicast solves this problem. It can deliver a high efficiency to send data in the point to multi-point service, which can save large bandwidth and reduce the network load. In multicast, the packets are transmitted in the following way as shown in Figure 9-1.

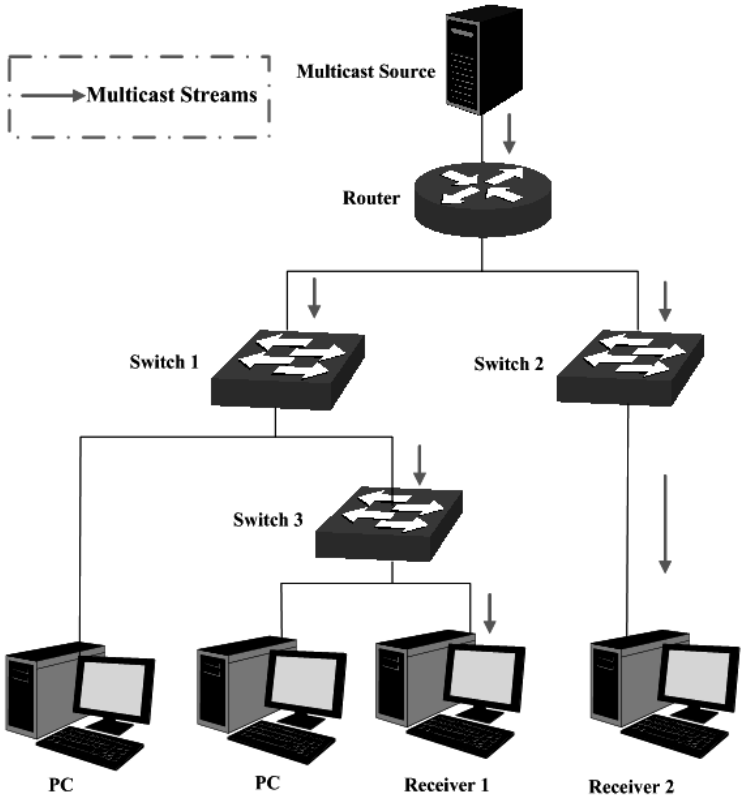


Figure 9-1 Information transmission in the multicast mode

Features of multicast:

1. The number of receivers is not certain. Usually point-to-multipoint transmission is needed;

2. Multiple users receiving the same information form a multicast group. The multicast information sender just need to send the information to the network device once;
3. Each user can join and leave the multicast group at any time;
4. Real time is highly demanded and certain packets drop is allowed.

➢ **IPv4 Multicast Address**

1. IPv4 Multicast IP Address:

As specified by IANA (Internet Assigned Numbers Authority), Class D IP addresses are used as destination addresses of multicast packets. The multicast IP addresses range from 224.0.0.0~239.255.255.255. The following table displays the range and description of several special multicast IP addresses.

Multicast IP address range	Description
224.0.0.0～224.0.0.255	Reserved multicast addresses for routing protocols and other network protocols
224.0.1.0～224.0.1.255	Addresses for video conferencing
239.0.0.0 ～ 239.255.255.255	Local management multicast addresses, which are used in the local network only

Table 9-1 Range of the special multicast IP

2. IPv4 Multicast MAC Address:

When a unicast packet is transmitted in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transmitted in an Ethernet network, the destination is not a receiver but a group with uncertain number of members, so a multicast MAC address, a logical MAC address, is needed to be used as the destination address.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address begins with 01-00-5E while the low-order 23 bits of a multicast MAC address are the low-order 23 bits of the multicast IP address. The mapping relationship is described as Figure 9-2.

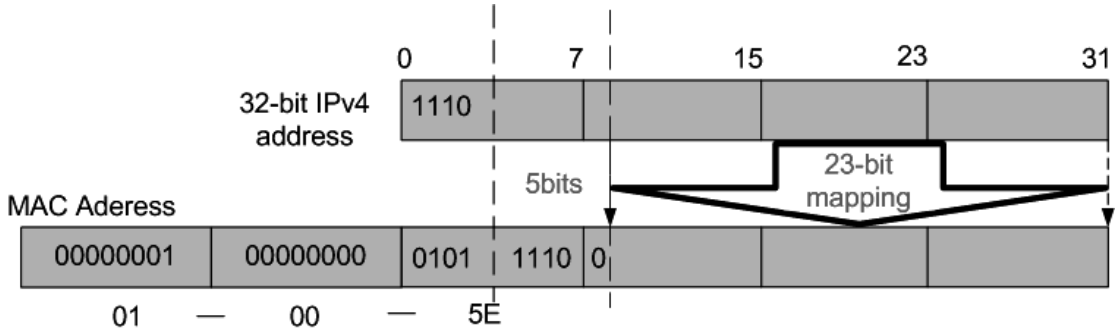


Figure 9-2 Mapping relationship between multicast IPv4 address and multicast MAC address

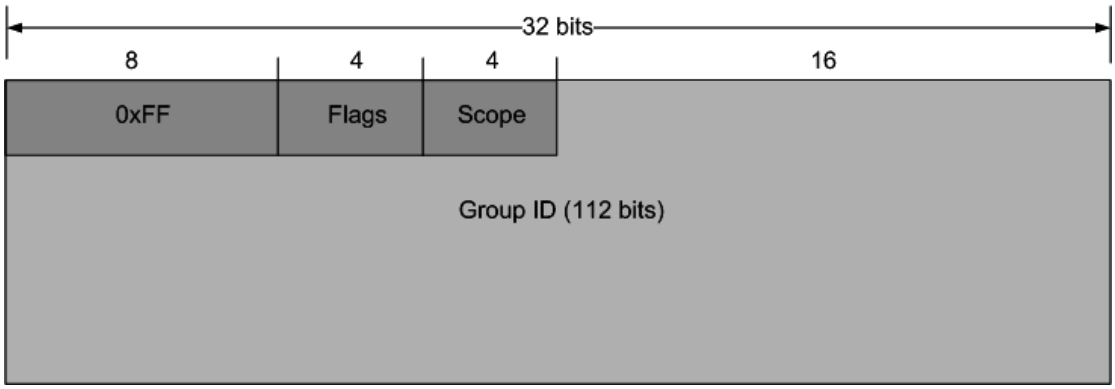
The high-order 4 bits of the IP multicast address are 1110, identifying the multicast group. Only 23 bits of the remaining low-order 28 bits are mapped to a multicast MAC address. In that way,

5 bits of the IP multicast address is not utilized. As a result, 32 IP multicast addresses are mapped to the same MAC addresses.

➢ **IPv6 Multicast Address**

1. IPv6 Multicast Address

An IPv6 multicast address is an identifier for a group of interfaces, and has the following format:



- 0XFF at the start of the address identifies the address as being a multicast address.
- Flags have 4 bits:

(1) The high-order flag is reserved, and must be initialized to 0.

(2) R: Set to 0 to indicate this IPv6 multicast address does not contain an embedded RP address; set to 1 to indicate this IPv6 multicast address contains an embedded RP address. When this bit is set to 1, the P and T bits must also be set to 1.

(3) P: Set to 0 to indicate this IPv6 multicast address is not based on a unicast prefix; set to 1 to indicate this IPv6 multicast address is based on a unicast prefix. When this bit is set to 1, the T bit must also be set to 1.

(4) T: Set to 0 to indicate that this address is an IPv6 multicast address permanently assigned by the Internet Assigned Numbers Authority (IANA); set to 1 to indicate that this address is a transient, or dynamically assigned IPv6 multicast address.

- Scope is a 4-bit value used to limit the scope of the multicast group. The values are as follows:

Value	Indication
0、3、F	reserved
1	Interface-Local scope
2	Link-Local scope
4	Admin-Local scope
5	Site-Local scope

6、7、9～D	unassigned
8	Organization-local scope
E	Global scope

Table 9-2 Indications of the Scope

- Group ID: 112 bits, IPv6 multicast group identifier that uniquely identifies an IPv6 multicast group in the scope defined by the Scope field.

Reserved Multicast Addresses:

Address	Indication
FF01::1	All interface-local IPv6 nodes
FF02::1	All link-local IPv6 nodes
FF01::2	All interface-local IPv6 routers
FF02::2	All link-local IPv6 routers
FF05::2	All site-local IPv6 routers
FF0X::	X ranges from 0 to F. These multicast addresses are reserved and shall never be assigned to any multicast group.

Table 9-3 Reserved IPv6 Multicast Addresses

The solicited-node multicast address is a multicast group that corresponds to an IPv6 unicast or anycast address. It is usually used for obtaining the Layer 2 link-layer addresses of neighboring nodes within the local-link or applied in IPv6 Duplicate Address Detection. A node is required to join the associated Solicited-Node multicast addresses for all unicast and anycast addresses that have been configured for the node's interfaces.

IPv6 Solicited-Node Multicast Address Format:

FF02:0:0:0:0:1:FFXX:XXXX

The IPv6 solicited-node multicast address has the prefix FF02:0:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address.

2. IPv6 Multicast MAC Address

The high-order 16 bits of an IPv6 multicast MAC address begins with 0x3333 while the low-order 32 bits of an IPv6 multicast MAC address are the low-order 32 bits of the IPv6 multicast IP address. The mapping relationship is described as the following figure:

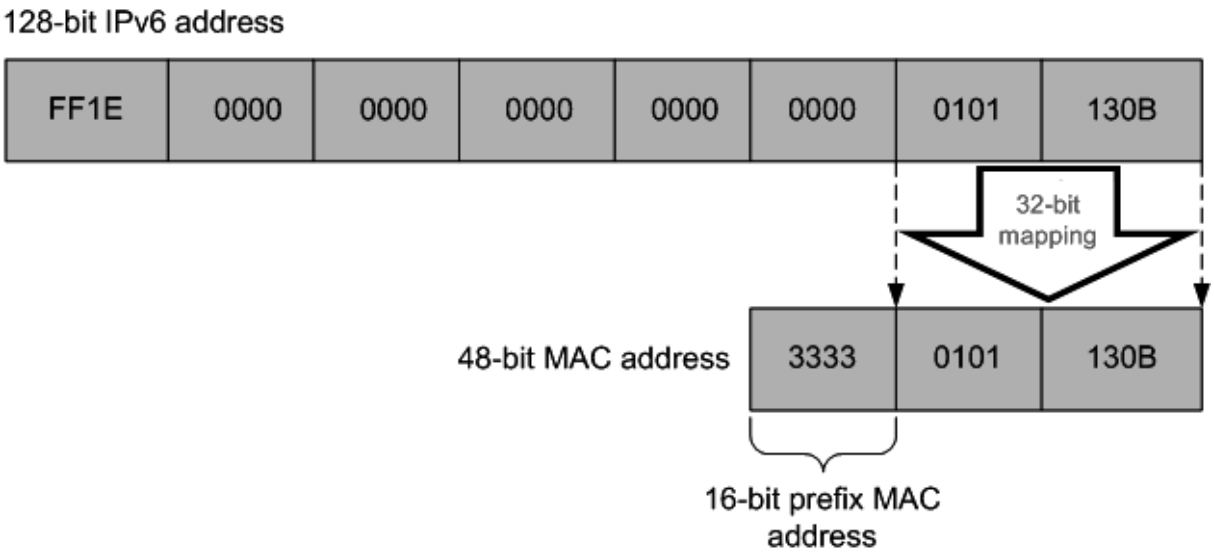


Figure 9-3 Mapping relationship between multicast IPv6 address and multicast IPv6 MAC address

The high-order 16 bits of the IP multicast address are 0x3333, identifying the IPv6 multicast group. The low-order 32 bits of the IPv6 multicast IP address are mapped to the multicast MAC address.

- **Multicast Address Table**

The switch is forwarding multicast packets based on the multicast address table. As the transmission of multicast packets cannot span the VLAN, the first part of the multicast address table is VLAN ID, based on which the received multicast packets are forwarded in the VLAN owning the receiving port. The multicast address table is not mapped to an egress port but a group port list. When forwarding a multicast packet, the switch looks up the multicast address table based on the destination multicast address of the multicast packet. If the corresponding entry cannot be found in the table, the switch will broadcast the packet in the VLAN owning the receiving port. If the corresponding entry can be found in the table, it indicates that the destination address should be a group port list, so the switch will deliver this multicast data to each port. The general format of the multicast address table is described as Figure 9-4 below.

VLAN ID	Multicast IP	Port

Figure 9-4 Multicast Address Table

- **IGMP Snooping**

In the network, the hosts apply to the near router for joining (leaving) a multicast group by sending IGMP (Internet Group Management Protocol) messages. When the up-stream device forwards down the multicast data, the switch is responsible for sending them to the hosts. IGMP Snooping is a multicast control mechanism, which can be used on the switch for dynamic registration of the multicast group. The switch, running IGMP Snooping, manages and controls the multicast group via listening to and processing the IGMP messages transmitted between the hosts and the multicast router, thereby effectively prevents multicast groups being broadcasted in the network.

- **MLD Snooping**

Multicast Listener Discovery(MLD)snooping is applied for efficient distribution of IPv6 multicast data to clients and routers in a Layer 2 network. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. The list is constructed and maintained by snooping IPv6 multicast control packets. MLD snooping performs a similar function in IPv6 as IGMP snooping in IPv4.

The Multicast module is mainly for multicast management configuration of the switch, including three submenus: **IGMP Snooping**, **MLD Snooping** and **Multicast Table.**

9.1 IGMP Snooping

- **IGMP Snooping Process**

The switch, running IGMP Snooping, listens to the IGMP messages transmitted between the host and the router, and tracks the IGMP messages and the registered port. When receiving IGMP report message, the switch adds the port to the multicast address table; when the switch listens to IGMP leave message from the host, the router sends the Group-Specific Query message of the port to check if other hosts need this multicast, if yes, the router will receive IGMP report message; if no, the router will receive no response from the hosts and the switch will remove the port from the multicast address table. The router regularly sends IGMP query messages. After receiving the IGMP query messages, the switch will remove the port from the multicast address table if the switch receives no IGMP report message from the host within a period of time.

- **IGMP Messages**

The switch, running IGMP Snooping, processes the IGMP messages of different types as follows.

1. IGMP Query Message

IGMP query message, sent by the router, falls into two types, IGMP general query message and IGMP group-specific-query message. The router regularly sends IGMP general message to query if the multicast groups contain any member. When receiving IGMP leave message, the receiving port of the router will send IGMP group-specific-query message to the multicast group and the switch will forward IGMP group-specific-query message to check if other members in the multicast group of the port need this multicast.

When receiving IGMP general query message, the switch will forward them to all other ports in the VLAN owning the receiving port. The receiving port will be processed: if the receiving port is not a router port yet, it will be added to the router port list with its router port time specified; if the receiving port is already a router port, its router port time will be directly reset.

When receiving IGMP group-specific-query message, the switch will send the group-specific query message to the members of the multicast group being queried.

2. IGMP Report Message

IGMP report message is sent by the host when it applies for joining a multicast group or responses to the IGMP query message from the router.

When receiving IGMP report message, the switch will send the report message via the router port in the VLAN as well as analyze the message to get the address of the multicast group the

host applies for joining. The receiving port will be processed: if the receiving port is a new member port, it will be added to the multicast address table with its member port time specified; if the receiving port is already a member port, its member port time will be directly reset.

3. Member Leave Message

The host will send IGMP leave message when leaving a multicast group to inform the router of its leaving.

When Immediate Leave is not enabled in a VLAN and a leave message is received on a port of this VLAN, the switch will generate Multicast-Address-Specific Queries (MASQs) on this port to check if there are other members in this multicast group. The user can control when a port membership is removed for an existing address in terms of the number and interval of MASQs. If there is no Report message received from this port during the switch maximum response time, the port on which the MASQ was sent is deleted from the multicast group. If the deleted port is the last member of the multicast group, the multicast group is also deleted. The switch will send leave message to the router ports of the VLAN.

In IPv4，Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that IPv4 multicast data is selectively forwarded to a list of ports that want to receive the data. This list is constructed by snooping IPv4 multicast control packets.

- **IGMP Snooping Fundamentals**

1. Ports

Router Port: Indicates the switch port directly connected to the multicast router.

Member Port: Indicates a switch port connected to a multicast group member.

2. Timers

Router Port Time: Within the time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. The default value is 300 seconds.

Member Port Time: Within the time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. The default value is 260 seconds.

Last Listener Query Interval: The interval between the switch sends out MASQs.

Last Listener Query Count: The number of MASQs that the switch sends before aging out a multicast address when there is no IGMP report response.

The IGMP Snooping function can be implemented on the following pages: **Snooping Config**, **Port Config**, **VLAN Config**, **Multicast VLAN**, **Querier Config**, **Profile Config**, **Profile Binding**, **Packet Statistics** and **IGMP Authentication**.

9.1.1 Snooping Config

To configure the IGMP Snooping on the switch, please firstly configure IGMP global configuration and related parameters on this page.

If the multicast address of the received multicast data is not in the multicast address table, the switch will broadcast the data in the VLAN. When Unknown Multicast Discard feature is enabled, the switch drops the received unknown multicast so as to save the bandwidth and enhance the process efficiency of the system. Please configure this feature appropriate to your needs.

Choose the menu **Multicast →IGMP Snooping →Snooping Config** to load the following page.

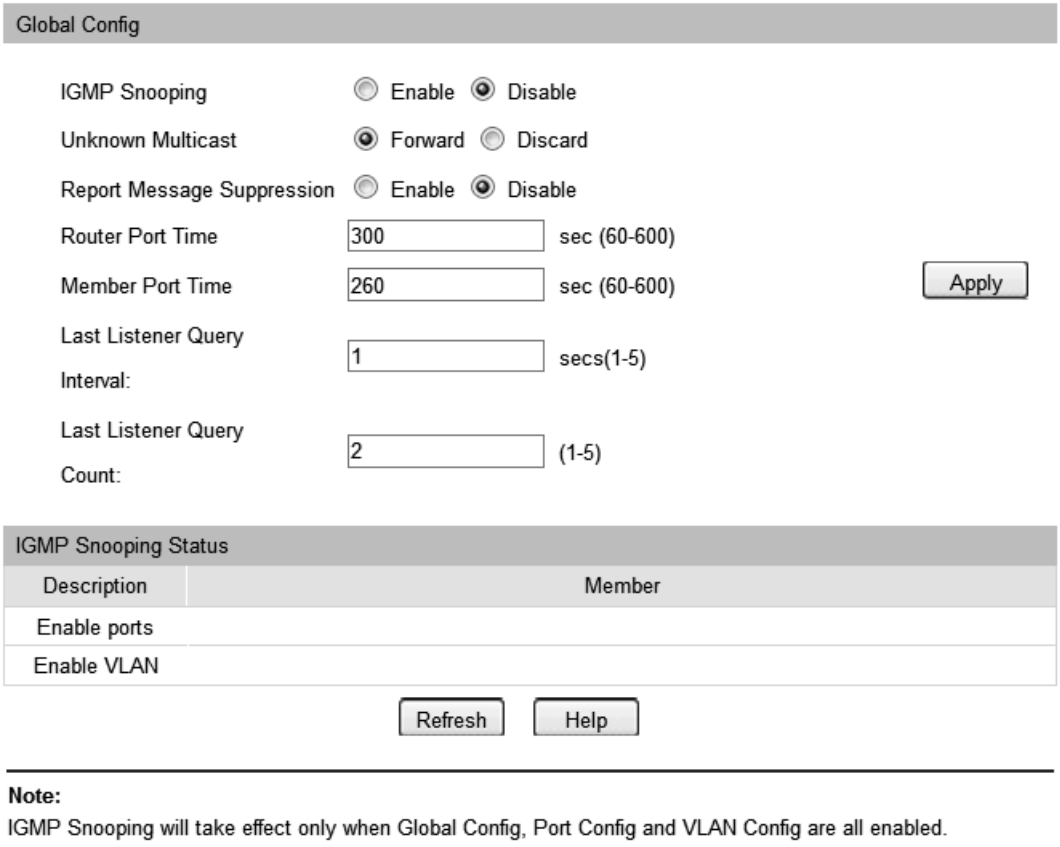


Figure 9-5 Basic Config

The following entries are displayed on this screen:

- **Global Config**

IGMP Snooping: Select Enable/Disable IGMP Snooping function globally on the switch.

Unknown Multicast: Select the operation for the switch to process unknown multicast, Forward or Discard.

Report Message Suppression: Enable or disable Report Message Suppression function globally. If this function is enabled, the first Report Message from the listener will be forwarded to the router ports while the subsequent Report Message will be suppressed to reduce the IGMP packets.

Router Port Time: Specify the aging time of the router port. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more.

Member Port Time: Specify the aging time of the member port. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more.

Last Listener Query Interval: Enter the interval between the switch sends out MASQs.

Last Listener Query Count: Enter the number of MASQs that the switch sends before aging out a multicast address when there is no IGMP report response.

- **IGMP Snooping Status**

Description: Displays IGMP Snooping status.

Member: Displays the member of the corresponding status.

9.1.2 Port Config

On this page you can enable or disable the IGMP Snooping and Fast Leave feature for ports of the switch.

Choose the menu **Multicast** →**IGMP Snooping** →**Port Config** to load the following page.

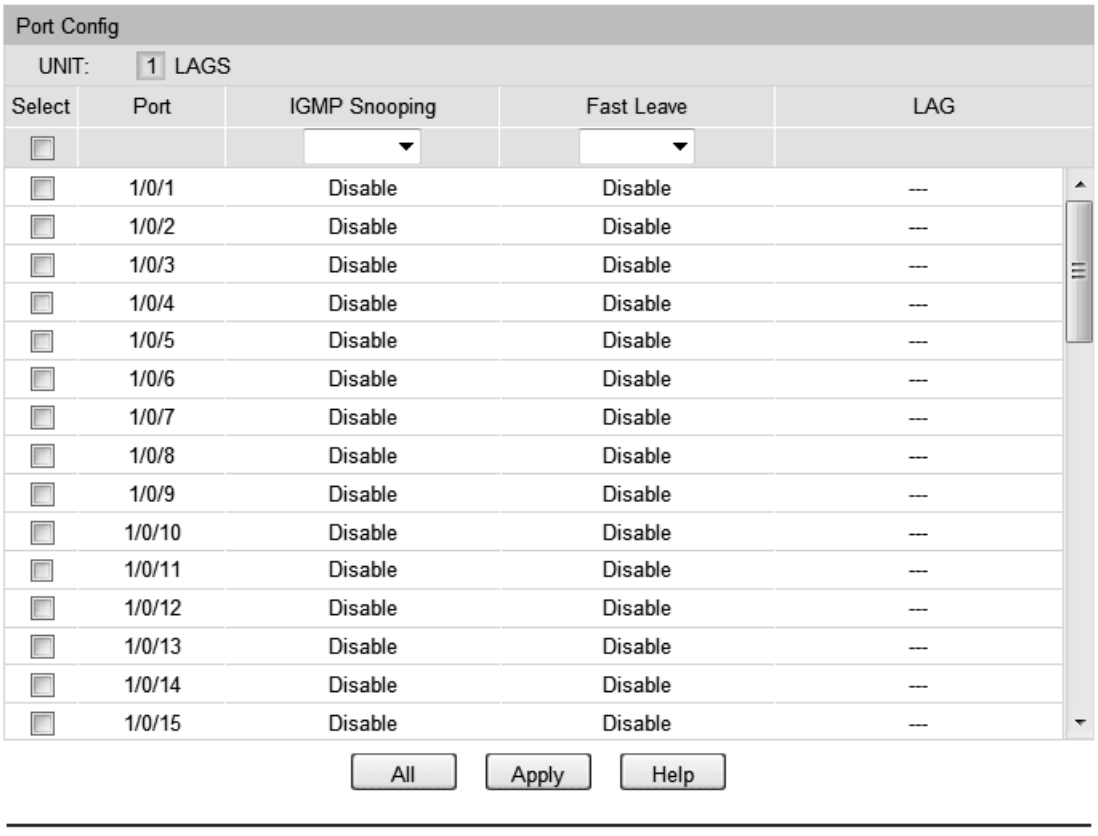


Figure 9-6 Port Config

The following entries are displayed on this screen:

- **Port Config**

UNIT:1/LAGS:	Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.
Select:	Select the desired port for IGMP Snooping feature configuration. It is multi-optional.
Port:	Displays the port of the switch.
IGMP Snooping:	Select Enable/Disable IGMP Snooping for the desired port.
Fast Leave:	Select Enable/Disable Fast Leave feature for the desired port. If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving IGMP leave messages.
LAG:	Displays the LAG number which the port belongs to.

Note:

1. Fast Leave on the port is effective only when the host supports IGMPv2 or IGMPv3.
2. When both Fast Leave feature and Unknown Multicast Discard feature are enabled, the leaving of a user connected to a port owning multi-user will result in the other users intermitting the multicast business.

9.1.3 VLAN Config

Multicast groups established by IGMP Snooping are based on VLANs. On this page you can configure different IGMP parameters for different VLANs.

Choose the menu **Multicast→IGMP Snooping→VLAN Config** to load the following page.

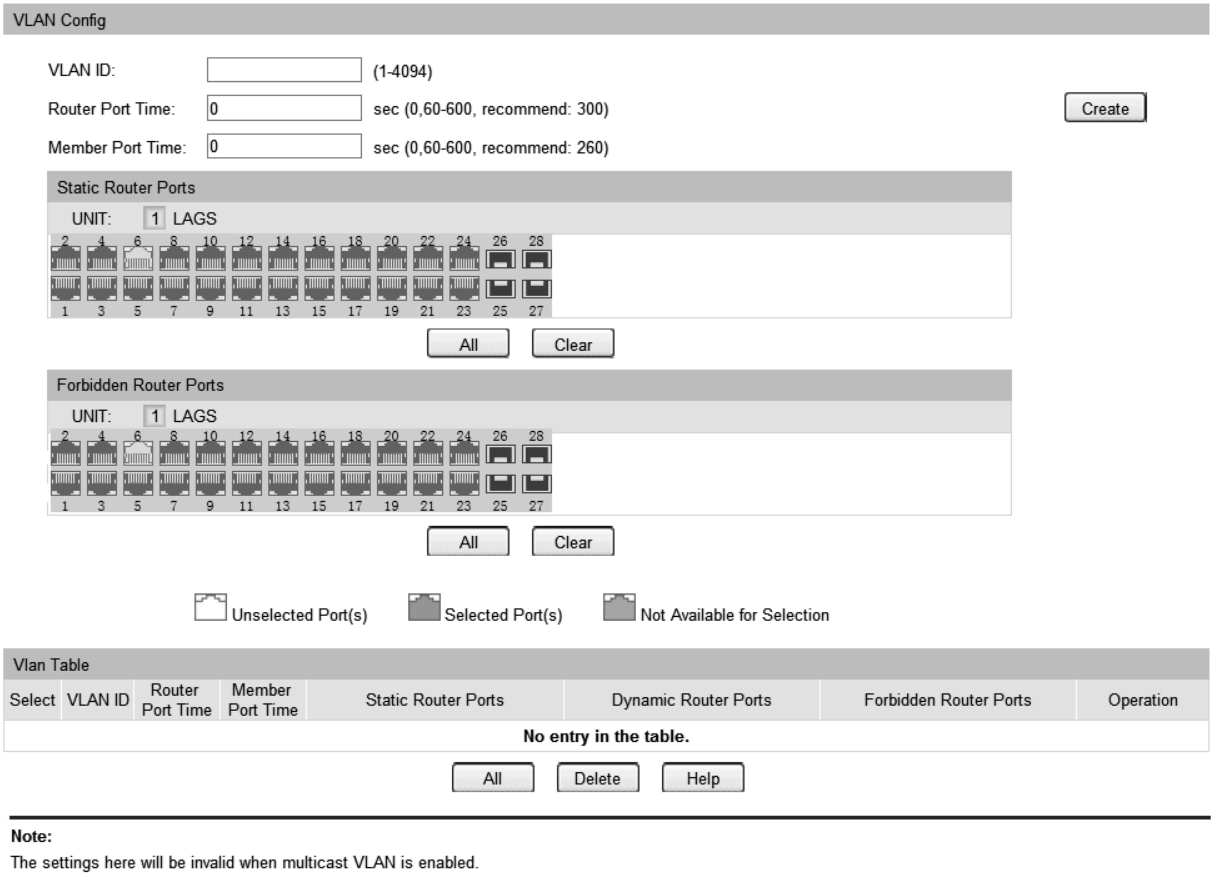


Figure 9-7 VLAN Config

The following entries are displayed on this screen:

- **VLAN Config**

VLAN ID: Enter the VLAN ID to enable IGMP Snooping for the desired VLAN.

Router Port Time: Specify the aging time of the router port. Within this time, if the switch doesn't receive IGMP query message from the router port, it will consider this port is not a router port any more. By default, it is 0 and the global router-time will be used.

Member Port Time: Specify the aging time of the member port. Within this time, if the switch doesn't receive IGMP report message from the member port, it will consider this port is not a member port any more. By default, it is 0 and the global member-time will be used.

Router Ports: Specify the static router port which is mainly used in the network with stable topology.

- **VLAN Table**

Select:	Select the desired VLAN ID for configuration. It is multi-optional.
VLAN ID:	Displays the VLAN ID.
Router Port Time:	Displays the router port time of the VLAN.
Member Port Time:	Displays the member port time of the VLAN.
Static Router Ports:	Displays the static router ports of the VLAN.
Dynamic Router Ports:	Displays the dynamic router ports of the VLAN.
Forbidden Router Ports:	Displays the forbidden router ports of the VLAN.

Note:

The settings here will be invalid when multicast VLAN is enabled.

- **Configuration procedure:**

Step	Operation	Description
1	Enable IGMP Snooping function	Required. Enable IGMP Snooping globally on the switch and for the port on **Multicast→IGMP Snooping→Snooping Config** and **Port Config** page.
2	Configure the multicast parameters for VLANs	Optional. Configure the multicast parameters for VLANs on **Multicast→IGMP Snooping→VLAN Config** page. If a VLAN has no multicast parameters configuration, it indicates the IGMP Snooping is not enabled in the VLAN, thus the multicast data in the VLAN will be broadcasted.

9.1.4 Multicast VLAN

In old multicast transmission mode, when users in different VLANs apply for join the same multicast group, the multicast router will duplicate this multicast information and deliver each VLAN owning a receiver one copy. This mode wastes a lot of bandwidth.

The problem above can be solved by configuring a multicast VLAN. By adding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves the bandwidth since multicast streams are transmitted only within the multicast VLAN and also guarantees security because the multicast VLAN is isolated from user VLANS.

Before configuring a multicast VLAN, you should firstly configure a VLAN as multicast VLAN and add the corresponding ports to the VLAN on the **802.1Q VLAN** page. If the multicast VLAN is enabled, the multicast configuration for other VLANs on the **VLAN Config** page will be invalid, that is, the multicast streams will be transmitted only within the multicast VLAN.

Choose the menu **Multicast→IGMP Snooping→Multicast VLAN** to load the following page.

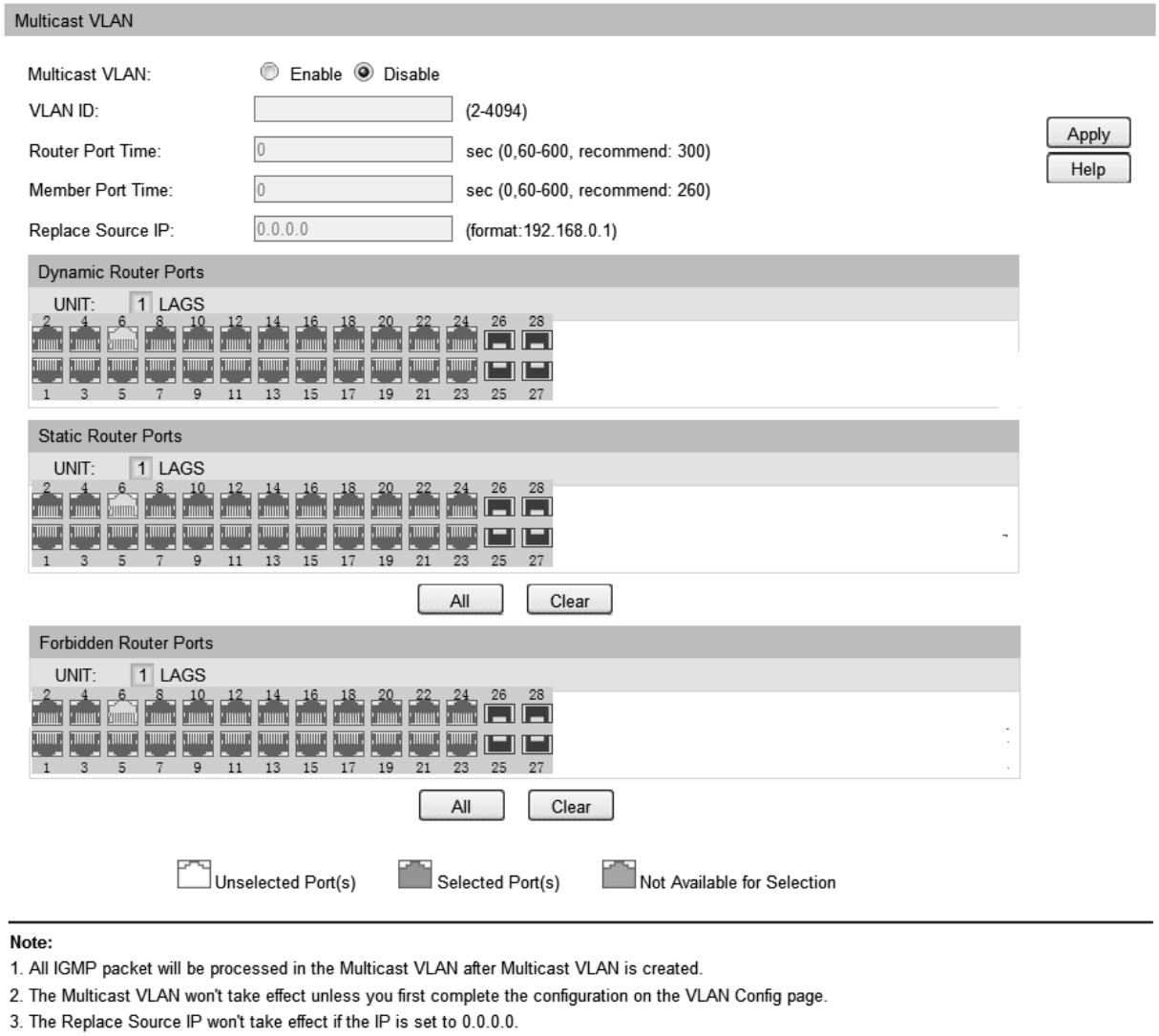


Figure 9-8 Multicast VLAN

The following entries are displayed on this screen:

- **Multicast VLAN**

  Multicast VLAN: Select Enable/Disable Multicast VLAN feature.

  VLAN ID: Enter the VLAN ID of the multicast VLAN.

  Router Port Time: Specify the aging time of the router port. Within this time, if the switch doesn't receive IGMP query message from the router port, it will consider this port is not a router port any more.

  Member Port Time: Specify the aging time of the member port. Within this time, if the switch doesn't receive IGMP report message from the member port, it will consider this port is not a member port any more.

Replace Source IP:	Specify the IP address with which the switch will replace the source of IGMP packets.
Dynamic Router Ports:	Displays the dynamic router ports of the multicast VLAN.
Static Router Ports:	Specify the static router port which is mainly used in the network with stable topology.
Forbidden Router Ports:	Specify the forbidden router ports which is mainly used to forbid ports becoming router ports.

Note:

1. The router port should be in the multicast VLAN, otherwise the member ports cannot receive multicast streams.
2. The Multicast VLAN won't take effect unless you first complete the configuration for the corresponding VLAN owning the port on the **802.1Q VLAN** page.
3. Configure the link type of the router port in the multicast VLAN as Tagged otherwise all the member ports in the multicast VLAN cannot receive multicast streams.
4. After a multicast VLAN is created, all the IGMP packets will be processed only within the multicast VLAN.

➢ **Configuration procedure:**

Step	Operation	Description
1	Enable IGMP Snooping function	Required. Enable IGMP Snooping globally on the switch and for the port on **Multicast→IGMP Snooping→Snooping Config** and **Port Config** page.
2	Create a multicast VLAN	Required. Create a multicast VLAN and add all the member ports and router ports to the VLAN on the **VLAN→802.1Q VLAN→VLAN Config** page. ● Configure the link type of the router ports as Tagged.
3	Configure parameters for multicast VLAN	Optional. Enable and configure a multicast VLAN on the **Multicast→IGMP Snooping→Multicast VLAN** page. It is recommended to keep the default time parameters.
4	Look over the configuration	If it is successfully configured, the VLAN ID of the multicast VLAN will be displayed in the IGMP Snooping Status table on the **Multicast→IGMP Snooping→Snooping Config** page.

Application Example for Multicast VLAN:

➢ **Network Requirements**

Multicast source sends multicast streams via the router, and the streams are transmitted to user A and user B through the switch.

Router: Its WAN port is connected to the multicast source; its LAN port is connected to the switch. The multicast packets are transmitted in VLAN3.

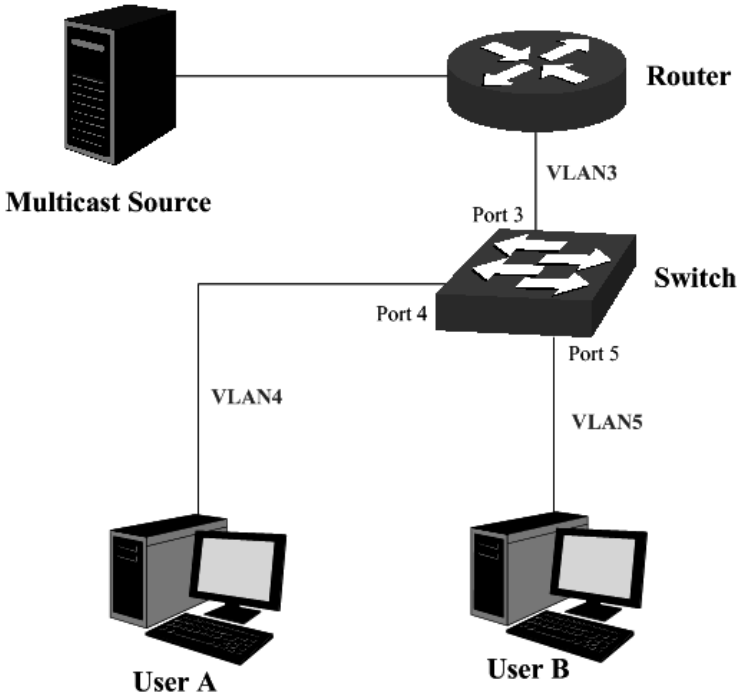
Switch: Port 3 is connected to the router and the packets are transmitted in VLAN3; port 4 is connected to user A and the packets are transmitted in VLAN4; port 5 is connected to user B and the packets are transmitted in VLAN5.

User A: Connected to Port 4 of the switch.

User B: Connected to port 5 of the switch.

Configure a multicast VLAN, and user A and B receive multicast streams through the multicast VLAN.

- **Network Diagram**



- **Configuration Procedure**

Step	Operation	Description
1	Create VLANs	Create three VLANs with the VLAN ID 3, 4 and 5 respectively, and specify the description of VLAN3 as Multicast VLAN on **VLAN→802.1Q VLAN** page.

2	Configure ports	On **VLAN→802.1Q VLAN** function pages. For port 3, configure its link type as Tagged, and add it to VLAN3, VLAN4 and VLAN5. For port 4, configure its link type as Untagged, and add it to VLAN3 and VLAN4. For port 5, configure its link type as Untagged, and add it to VLAN3 and VLAN5.
3	Enable IGMP Snooping function	Enable IGMP Snooping function globally on **Multicast→IGMP Snooping→Snooping Config** page. Enable IGMP Snooping function for port 3, port4 and port 5 on **Multicast→IGMP Snooping→Port Config** page.
4	Enable Multicast VLAN	Enable Multicast VLAN, configure the VLAN ID of a multicast VLAN as 3 and keep the other parameters as default on **Multicast→IGMP Snooping→Multicast VLAN** page.
5	Check Multicast VLAN	Port 3-5 and Multicast VLAN 3 will be displayed in the IGMP Snooping Status table on the **Multicast→IGMP Snooping→Snooping Config** page.

9.1.5 Querier Config

In an IP multicast network that runs IGMP, a Layer 3 multicast device works as an IGMP querier to send IGMP queries and manage the multicast table. But IGMP is not supported by the devices in Layer 2 network. IGMP Snooping Querier can act as an IGMP Router in Layer 2 network. It can help to create and maintain multicast forwarding table on the switch with the Query messages it generates.

Choose the menu **Multicast→IGMP Snooping→Querier Config** to load the following page.

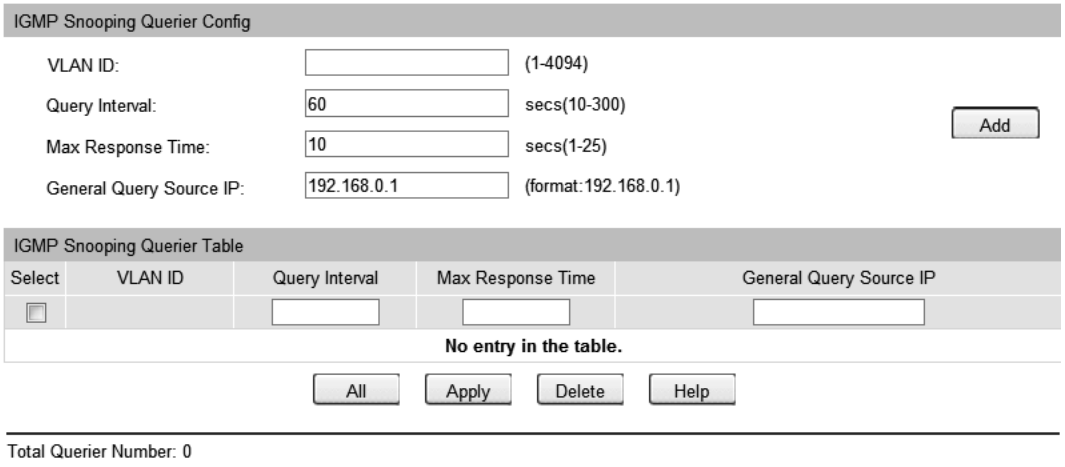


Figure 9-9 Querier Config

The following entries are displayed on this screen:

- **IGMP Snooping Querier Config**

VLAN ID:	Enter the ID of the VLAN that enables IGMP Snooping Querier.
Query Interval:	Enter the time interval of sending a general query frame by IGMP Snooping Querier.
Max Response Time:	Enter the maximal time for the host to respond to a general query frame sent by IGMP Snooping Querier.
General Query Source IP:	Enter the source IP of the general query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP.

➢ **IGMP Snooping Querier Table**

Select:	Select the desired entry. It is multi-optional.
VLAN ID:	Displays the ID of the VLAN that enables IGMP Snooping Querier.
Query Interval:	Displays the Query Interval of the IGMP Snooping Querier.
Max Response Time:	Displays the maximal time for the host to respond to a general query frame sent by IGMP Snooping Querier.
General Query Source IP:	Displays the source IP of the general query frame sent by IGMP Snooping Querier.

9.1.6 Profile Config

On this page you can configure an IGMP profile.

Choose the menu **Multicast→IGMP Snooping→Profile Config** to load the following page.

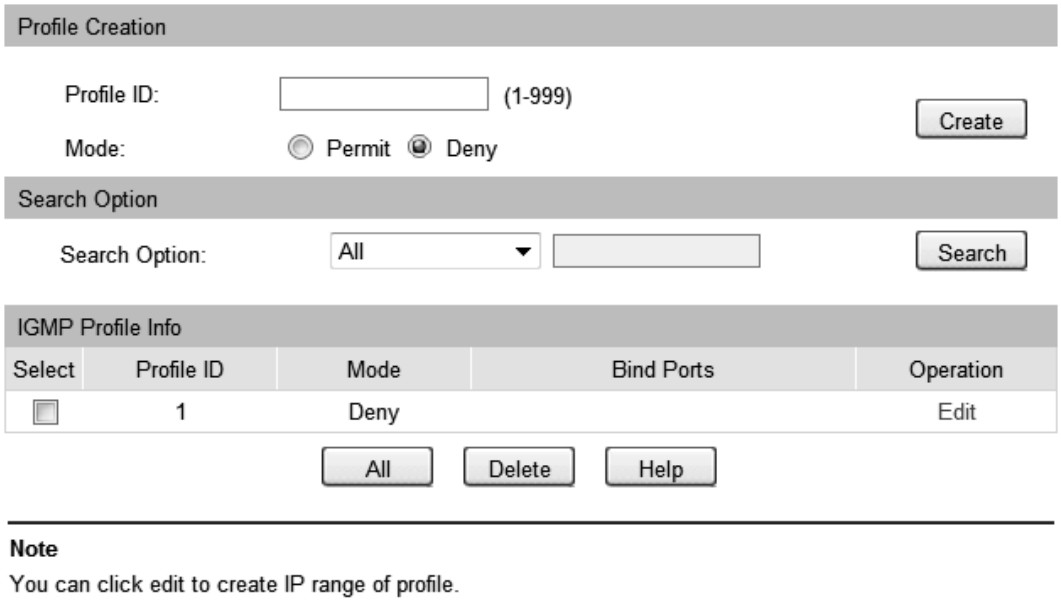


Figure 9-10 Profile Config

The following entries are displayed on this screen:

- **Profile Creation**

  Profile ID: Specify the Profile ID you want to create, and it should be a number between 1 and 999.

  Mode: The attributes of the profile.
  - **Permit**: Only permit the IP address within the IP range and deny others.
  - **Deny**: Only deny the IP address within the IP range and permit others.

- **Search Option**

  Search Option: Select the rules for displaying profile entries.
  - **All**: Display all profile entries.
  - **Profile ID**: Display profile entry of the ID.

- **IGMP Profile Info**

  Select: Select the desired entry for configuration.

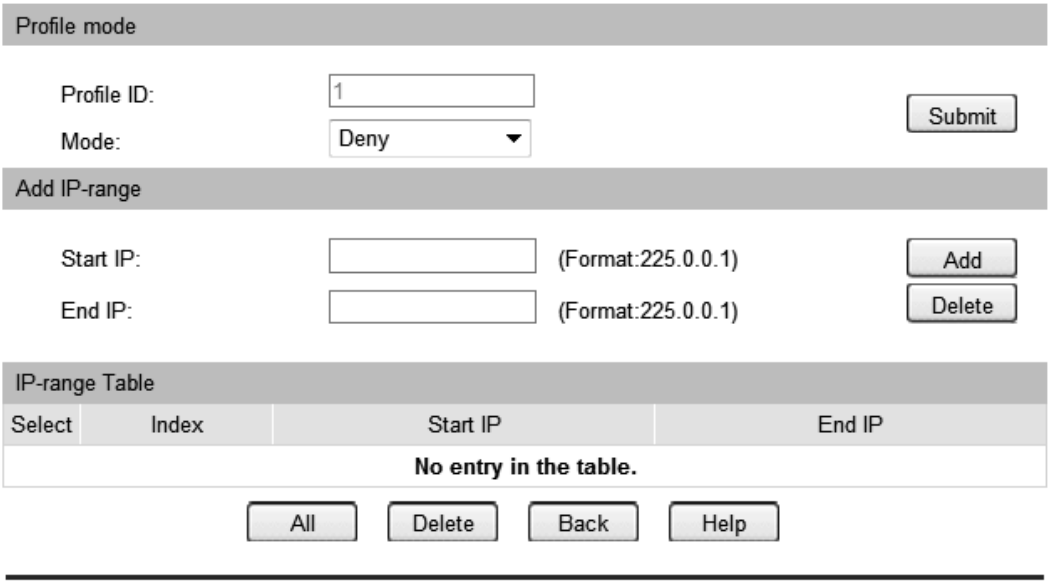
  Profile ID: Displays the profile ID.

  Mode: Displays the attribute of the profile.
  - **Permit**: Only permit the IP address within the IP range and deny others.
  - **Deny**: Only deny the IP address within the IP range and permit others.

  Bind Ports: Displays the ports that the Profile bound to.

  Operation: Click the **Edit** button to configure the mode or IP-range of the Profile.

After you have created a profile ID, click **Edit** to display the following figure.



The following entries are displayed on this screen:

- **Profile Mode**

  Profile ID: Displays the Profile ID you have created.

  Mode: The attributes of the profile.
  - **Permit**: Only permit the IP address within the IP range and deny others.
  - **Deny**: Only deny the IP address within the IP range and permit others.

- **Add IP-range**

  Start IP: Enter start IP address of the IP-range.

  End IP: Enter end IP address of the IP-range.

- **IP-range Table**

  Select: Select the desired entry for configuration.

  Index: Displays index of the IP-range which is not configurable.

  Start IP: Displays the start IP address of the IP-range.

  End IP: Displays the end IP address of the IP-range.

9.1.7 Profile Binding

When the switch receives IGMP report message, it examines the profile ID bound to the access port to determine if the port can join the multicast group. If the multicast IP is not filtered, the switch will add the port to the forward port list of the multicast group. Otherwise, the switch will drop the IGMP report message. In that way, you can control the multicast groups that users can access.

Choose the menu **Multicast→IGMP Snooping→Profile Binding** to load the following page.

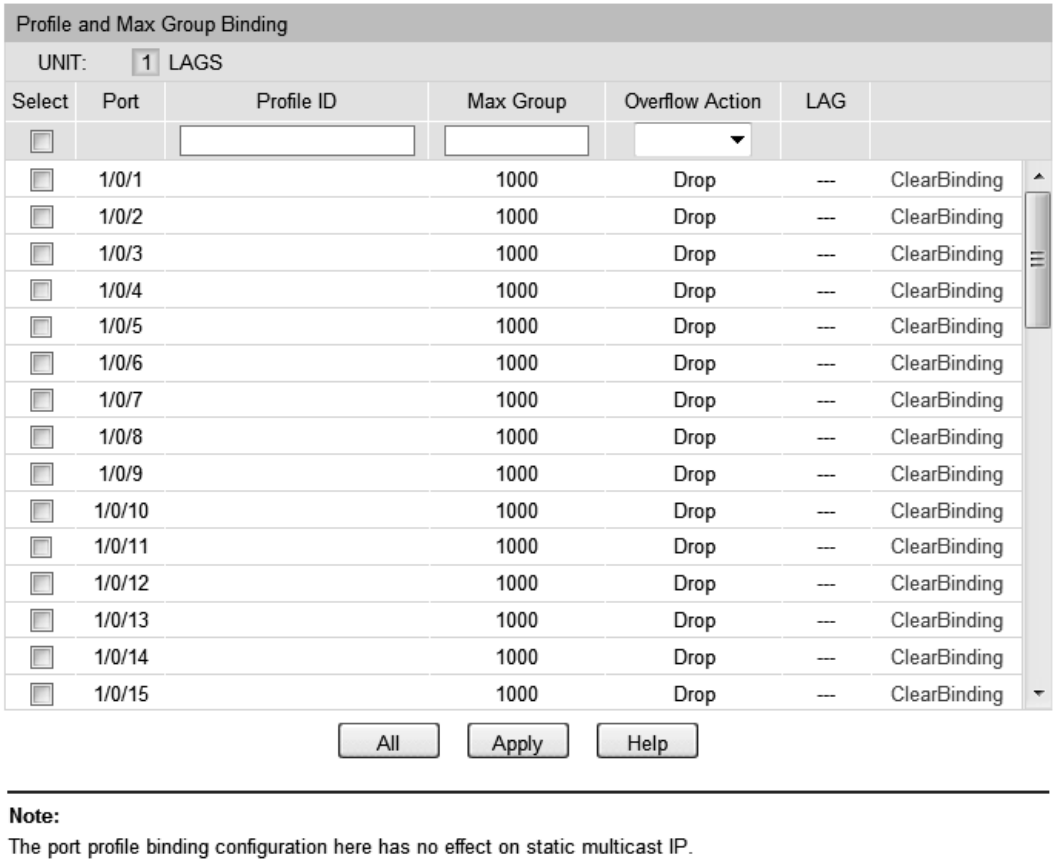


Figure 9-11 Profile Binding

The following entries are displayed on this screen:

- **Profile and Max Group Binding**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired entry for configuration.

Port: It is multi-optional. Displays the port number.

Profile ID: The existing Profile ID bound to the selected port.

Max Group: The maximum multicast group a port can join.

Overflow Action: The policy should be taken when the number of multicast group a port has joined reach the maximum.

- **Drop**: Drop the successive report packet, and this port can not join any other multicast group.
- **Replace**: When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

LAG: Displays the LAG number which the port belongs to.

Clear Binding: Click the **ClearBinding** button to clear all profiles bound to the port.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Create Profile	Required. Configure the Profile ID and mode on **Multicast→IGMP Snooping→Profile Config** page.
2	Configure IP-Range	Required. Click **Edit** of the specified entry in the IGMP Profile Info table on **Multicast→IGMP Snooping→Profile Config** page to configure the mode or IP-range of the Profile.
3	Configure Profile Binding for ports	Optional. Configure Profile Binding for ports on **Multicast→IGPM Snooping→Porfile Binding** page.

9.1.8 Packet Statistics

On this page you can view the multicast data traffic on each port of the switch, which facilitates you to monitor the IGMP messages in the network.

Choose the menu **Multicast→IGMP Snooping→Packet Statistics** to load the following page.

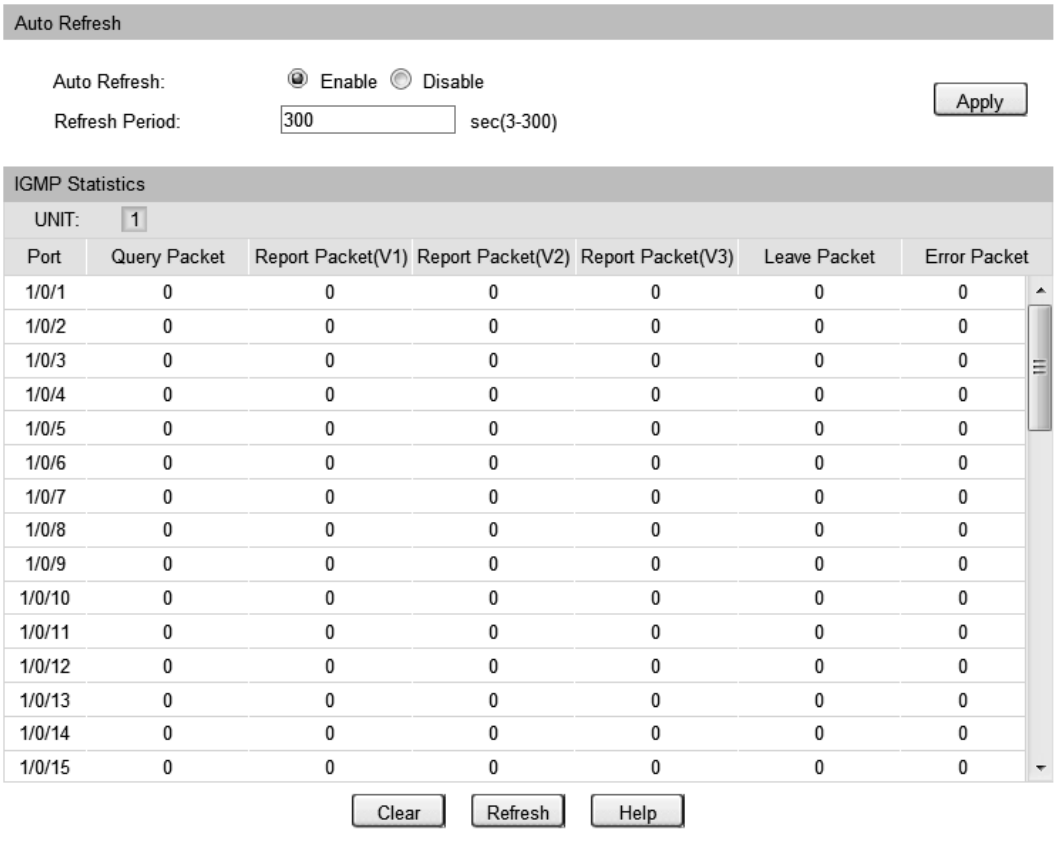


Figure 9-12 Packet Statistics

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Select Enable/Disable auto refresh feature.

  Refresh Period: Enter the time from 3 to 300 in seconds to specify the auto refresh period.

- **IGMP Statistics**

  Port: Displays the port number of the switch.

  Query Packet: Displays the number of query packets the port received.

  Report Packet (V1): Displays the number of IGMPv1 report packets the port received.

  Report Packet (V2): Displays the number of IGMPv2 report packets the port received.

  Report Packet (V3): Displays the number of IGMPv3 report packets the port received.

  Leave Packet: Displays the number of leave packets the port received.

  Error Packet: Displays the number of error packets the port received.

9.1.9 IGMP Authentication

IGMP Authentication (Internet Group membership Authentication Protocol) is a multicast authentication protocol used to authenticate who wants to join the limited multicast source. On this page you can configure IGMP Authentication feature for port.

Choose the menu **Multicast→IGMP Snooping→IGMP Authentication** to load the following page.

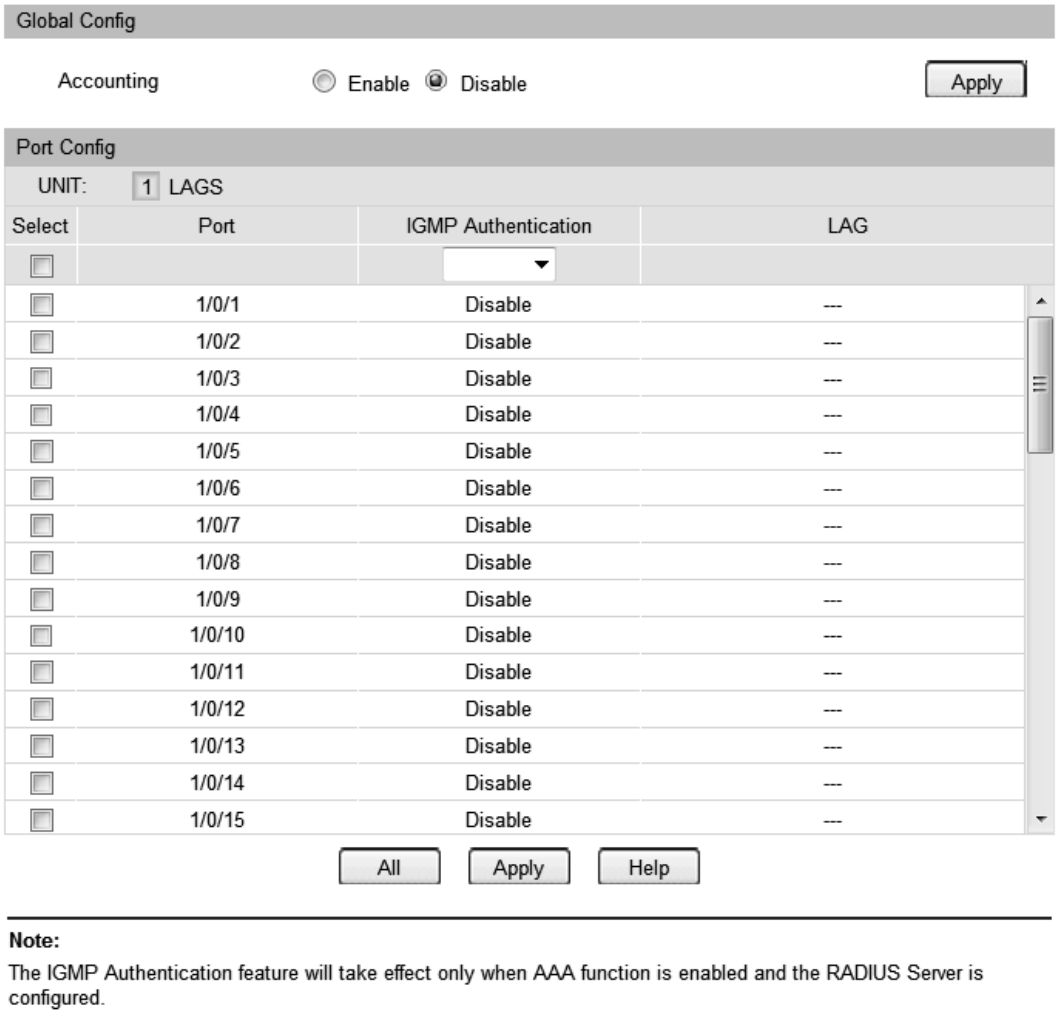


Figure 9-13 IGMP Authentication

The following entries are displayed on this screen:

- **Global Config**

  Accounting: Enable/Disable the IGMP Authentication Account feature.

- **Port Config**

  Select: Select the desired port for IGMP Authentication feature configuration. It is multi-optional.

  Port: Displays the port number of the switch.

  General Query Source IP: Enter the source IP of the general query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP.

  IGMP Authentication: Select Enable/Disable IGMP Authentication for the desired port.

  LAG: Displays the LAG number which the port belongs to.

Note:

The IGMP Authentication feature will take effect only when AAA function is enabled and the RADIUS server is configured. For how to enable AAA function and configure RADIUS server, please refer to 13.11 AAA.

9.2 MLD Snooping

➢ **MLD Snooping**

Multicast Listener Discovery (MLD) snooping is applied for efficient distribution of IPv6 multicast data to clients and routers in a Layer 2 network. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. The list is constructed and maintained by snooping IPv6 multicast control packets. MLD snooping performs a similar function in IPv6 as IGMP snooping in IPv4.

The switch, running MLD Snooping, listens to the MLD messages transmitted between the host and the router, and tracks the MLD messages and the registered port. When receiving MLD report message, the switch adds the port to the multicast address table; when the switch listens to MLD Done message from the host, the router sends the Multicast-Address-Specific Query message of the port to check if other hosts need this multicast, if yes, the switch will receive MLD report message; if no, the switch will receive no response from the hosts and the switch will remove the port from the multicast address table. The router regularly sends MLD query messages. After receiving the MLD query messages, the switch will remove the port from the multicast address table if the switch receives no MLD report message from the host within a period of time.

➢ **MLD Snooping Fundamentals**

1. MLD Messages

MLD Queries： MLD Queries include General Queries and Multicast-Address-Specific Queries (MASQs) and are sent out from the MLD router.

MLD Reports： When a host wants to join a multicast group or responds to the MLD queries, it will send out an MLD report.

MLD Done Messages： When a host wants to leave a multicast group, it will send out an MLD Done message to inform the IPv6 multicast routers of its leave.

2. Relevant Ports of the Switch

Router Port: Indicates the switch port that links toward the MLD router.

Member Port: Indicates the switch port that links toward the multicast members.

3. Timers

Router Port Aging Time: Within this time, if the switch does not receive MLD queries from the router port, it will delete this port from the router port list. The default value is 300 seconds.

Member Port Aging Time: Within this time, if the switch does not receive MLD reports from the member port, it will delete this port from the MLD multicast group. The default value is 260 seconds.

General Query Interval: The interval between the multicast router sends out general queries.

Last Listener Query Interval: The interval between the switch sends out MASQs.

Last Listener Query Count: The number of MASQs that the switch sends before aging out a multicast address when there is no MLD report response.

- **MLD Snooping Process**

1. General Query

The MLD router regularly sends MLD general queries to query if the multicast groups contain any members. When receiving MLD general queries, the switch will forward them to all other ports in the VLAN. The receiving port will be processed: if the receiving port is not a router port yet, it will be added to the router port list with its router port aging time specified; if the receiving port is already a router port, its router port aging time will be directly reset.

2. Membership Report

The host will send MLD report messages when it applies for joining a multicast group or responds to the MLD query message from the router.

When receiving MLD report message, the switch will forward the report message via the router port in the VLAN, and analyze the message to get the address of the multicast group the host applies for joining. If the multicast group does not exist, it will create the group entry. The receiving port will be processed: if the receiving port is a new member port, it will be added to the forward list of the multicast group with its member port aging time specified; if the receiving port is already a member port, its member port aging time will be directly reset.

3. Member Leave

The host will send MLD Done message when leaving a multicast group to inform the router of its leaving.

When Immediate Leave is not enabled in a VLAN and a Done message is received on a port of this VLAN, the switch will generate MASQs on this port to check if there are other members in this multicast group. The user can control when a port membership is removed for an exiting address in terms of the number and interval of MASQs. If there is no Report message received from this port during the switch maximum response time, the port on which the MASQ was sent is deleted from the multicast group. If the deleted port is the last member of the multicast group, the multicast group is also deleted. The switch will send Done message to the router ports of the VLAN.

In IPv6，Layer 2 switches can use Multicast Listener Discovery (MLD) Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data. This list is constructed by snooping IPv6 multicast control packets.

The MLD Snooping function can be implemented on **Snooping Config**, **Port Config**, **VLAN Config**, **Multicast VLAN**, **Querier Config**, **Profile Config**, **Profile Binding** and **Packet Statistics** pages.

9.2.1 Snooping Config

To configure the MLD Snooping on the switch, please firstly configure MLD global configuration and related parameters on this page.

Chose the menu **Multicast→MLD Snooping→Snooping Config** to load the following page.

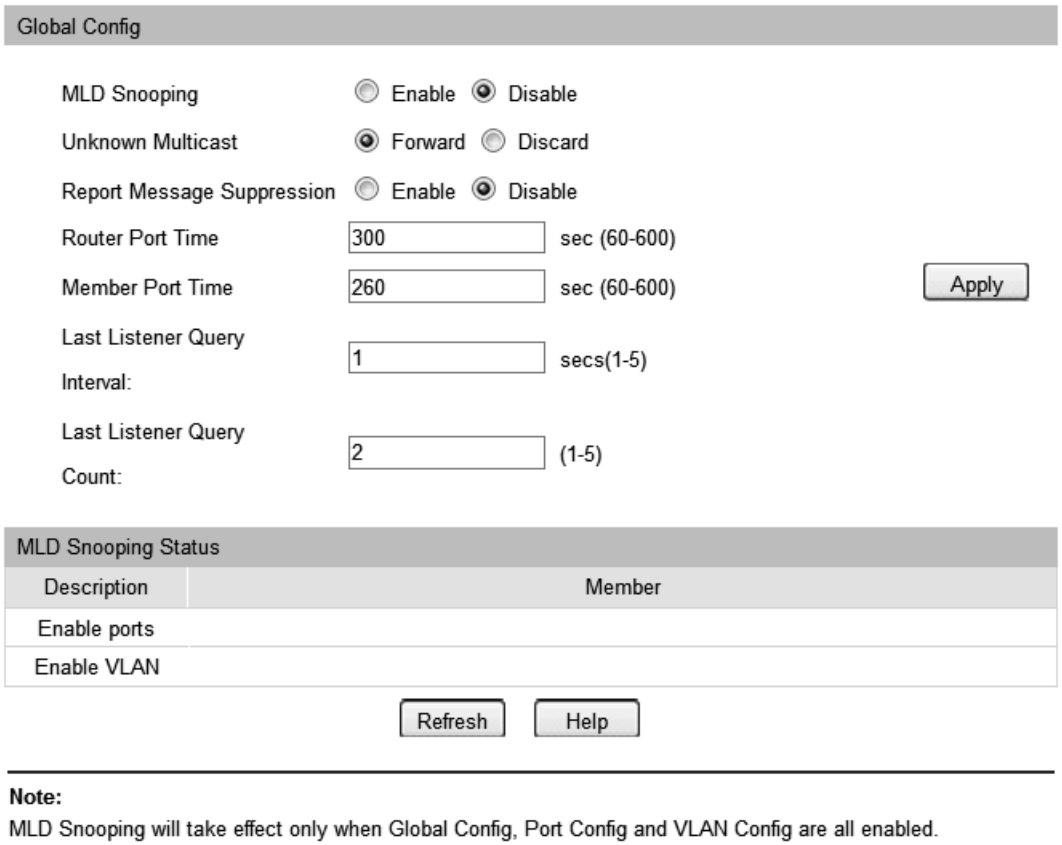


Figure 9-14 Snooping Config

The following entries are displayed on this screen:

- **Global Config**

  MLD Snooping: Enable or disable MLD Snooping function globally.

  Unknown Multicast: Choose to forward or drop unknown multicast data.

  Unknown IPv6 multicast packets refer to those packets without corresponding forwarding entries in the IPv6 multicast table:

  When unknown multicast filter is enabled, the switch will discard all received unknown IPv6 multicast packets;

  When unknown multicast filer is disabled, all unknown IPv6 multicast packets are flooded in the ingress VLAN.

Report Message Suppression: Enable or disable Report Message Suppression function globally. If this function is enabled, the first Report Message from the listener will forward to the router ports while the subsequent Report Message from the group will be suppressed to reduce the MLD traffic in the network.

Router Port Time: Enter the global router port aging time. If the router port does not receive Query Message in the aging time, it will be aged.

Member Port Time: Enter the global member port aging time. If the member port does not receive Report Message in the aging time, it will be aged.

Last Listener Query Interval: Enter the interval between the switch sends out MASQs.

Last Listener Query Count: Enter the number of MASQs that the switch sends before aging out a multicast address when there is no MLD report response.

- **MLD Snooping Status**

Description: Displays MLD Snooping status.

Member: Displays the member of the corresponding status.

Note:

1. Configurations of the Router Port Time and Member Port Time in **8.2.3 VLAN Config** override their global configurations here.
3. Before creating a Multicast VLAN, you should enable the MLD snooping function in this VLAN in **8.2.3 VLAN Config**.

Configuration Procedure of Multicast VLAN:

Step	Operation	Description
1	Create VLAN.	Required. On the **VLAN →802.1Q VLAN →VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its member ports.
2	Enable MLD Snooping globally.	Required. On the **Multicast →MLD Snooping →Global Config** page, enable the MLD Snooping function globally.
3	Enable MLD Snooping in the VLAN.	Required. On the **Multicast →MLD Snooping →VLAN Config** page, specify the VLAN ID as the VLAN created in step 1.
4	Enable the Multicast VLAN.	Required. On the **Multicast →MLD Snooping →Multicast** page, enable the **Multicast VLAN** function and specify the **Multicast VLAN ID** as the VLAN specified in Step 1.

9.2.2 Port Config

On this page you can configure MLD Snooping function with each single port.

Choose the menu **Multicast→MLD Snooping→Port Config** to load the following page.

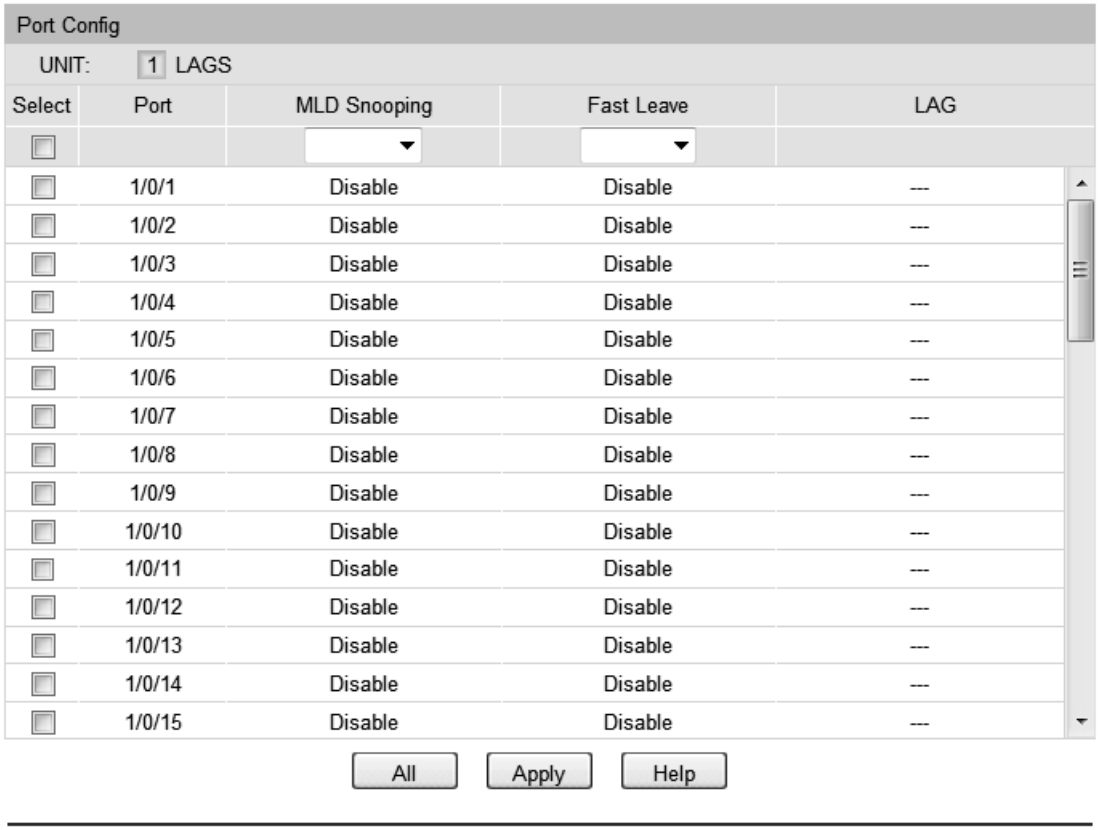


Figure 9-15 Port Config

The following entries are displayed on this screen:

- **Port Config**

UNIT:1/LAGS	Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.
Select:	Select the port you want to configure.
Port:	Displays the port number.
MLD Snooping:	Select Enable/Disable MLD Snooping for the desired port.
Fast Leave:	Select Enable/Disable Fast Leave feature for the desired port. If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD done messages.
LAG:	Displays the LAG number.

9.2.3 VLAN Config

On this page you can configure MLD Snooping function with each single VLAN. You need to create VLAN if you want to enable MLD Snooping function in this VLAN.

Choose the menu **Multicast→MLD Snooping→VLAN Config** to load the following page.

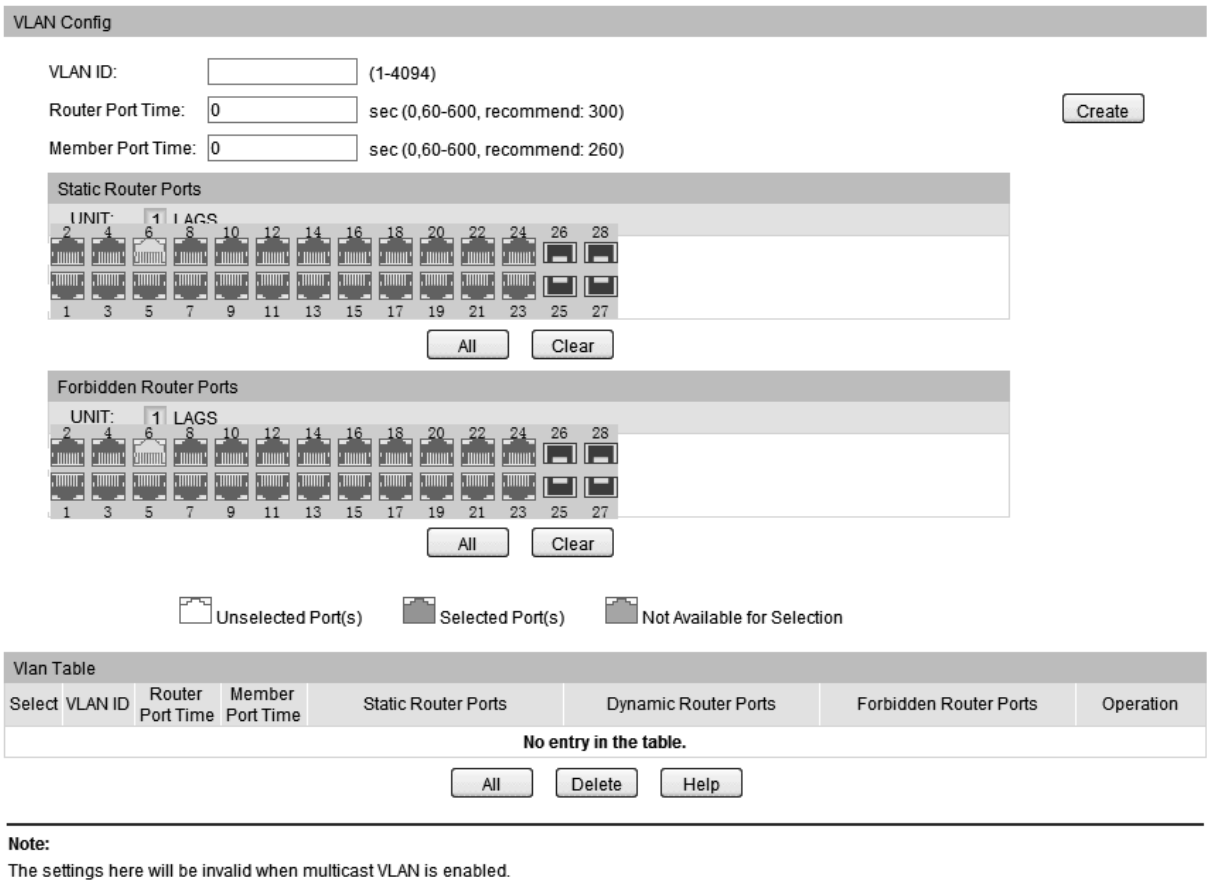


Figure 9-16 VLAN Config

The following entries are displayed on this screen:

- **VLAN Config**

VLAN ID: Enter the VLAN ID you want to configure.

Router Port Time: Specify the aging time of the router port. Within this time, if the switch don't receive MLD query message from the router port, it will consider this port is not a router port any more. By default, it is 0 and the global router-time will be used.

Member Port Time: Specify the aging time of the member port. Within this time, if the switch don't receive MLD report message from the member port, it will consider this port is not a member port any more. By default, it is 0 and the global member-time will be used.

Static Router Ports: Specify the static router port which is mainly used in the network with stable topology.

Forbidden Router Ports:	Specify the forbidden router ports which is mainly used to forbid ports becoming router ports.

- **VLAN Table**

Select:	Select the VLAN ID you want to change.
VLAN ID:	Displays the VLAN ID.
Router Port Time:	Displays the router port time of this VLAN.
Member Port Time:	Displays the member port time of this VLAN.
Static Router Ports:	Displays the static router ports of this VLAN.
Dynamic Router Ports:	Displays the dynamic router ports of this VLAN.
Forbidden Router Ports:	Displays the forbidden router ports of the VLAN.

Note:

1. The MLD snooping function in a VLAN will take effect when global MLD Snooping function is enabled in 9.2.1 Snooping Config and the VLAN is created in Chapter 6 VLAN.
2. When the router port time or member port time is set for a VLAN, this value overrides the value configured globally in 9.2.1 Snooping Config.

9.2.4 Multicast VLAN

In old multicast transmission mode, when users in different VLANs apply for join the same multicast group, the multicast router will duplicate this multicast information and deliver each VLAN owning a receiver one copy. This mode wastes a lot of bandwidth.

The problem above can be solved by configuring a multicast VLAN. By adding switch ports to the multicast VLAN and enabling MLD Snooping, you can make users in different VLANs share the same multicast VLAN. This saves the bandwidth since multicast streams are transmitted only within the multicast VLAN and also guarantees security because the multicast VLAN is isolated from user VLANS.

Before configuring a multicast VLAN, you should firstly configure a VLAN as multicast VLAN and add the corresponding ports to the VLAN on the **802.1Q VLAN** page. If the multicast VLAN is enabled, the multicast configuration for other VLANs on the **VLAN Config** page will be invalid, that is, the multicast streams will be transmitted only within the multicast VLAN.

Choose the menu **Multicast→MLD Snooping→Multicast VLAN** to load the following page.

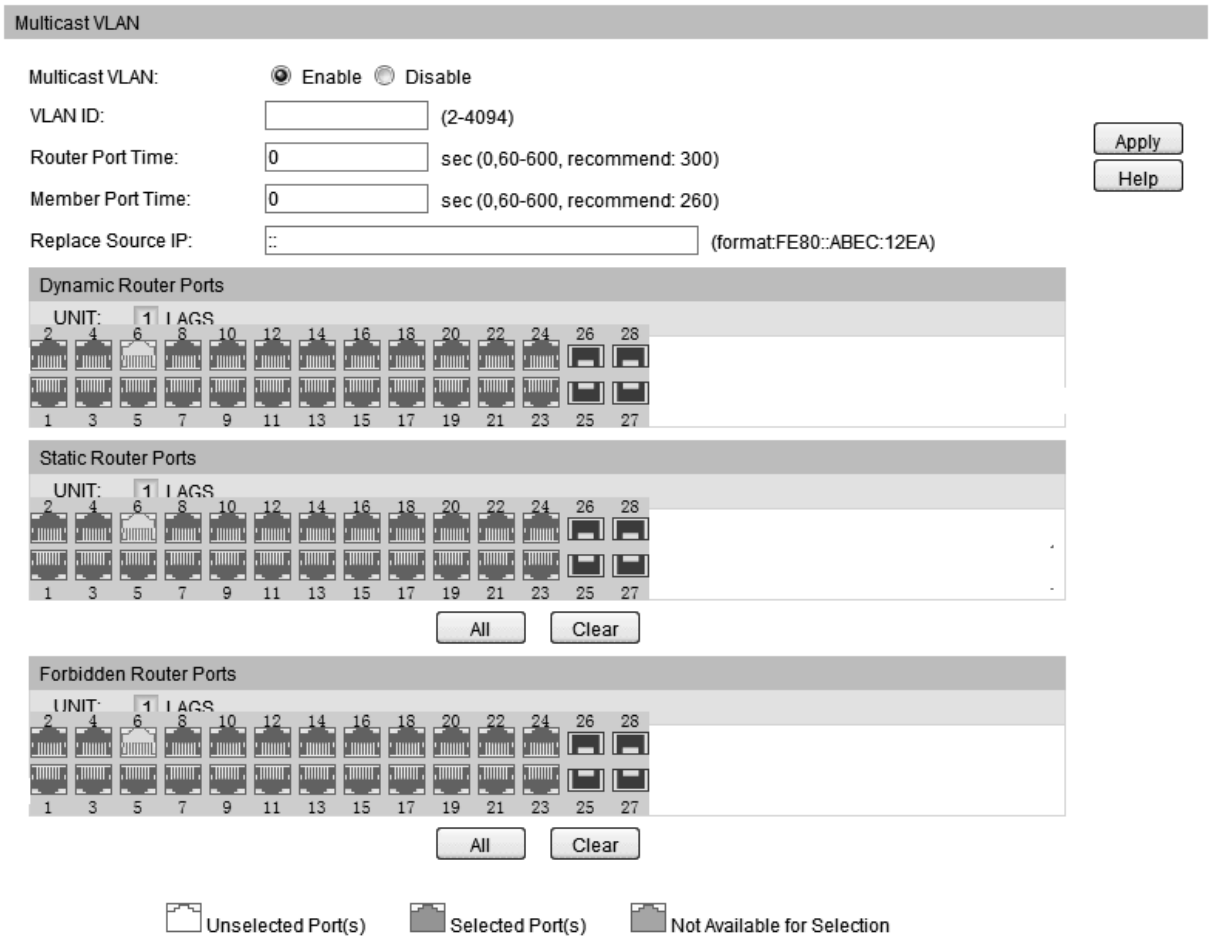


Figure 9-17 Multicast VLAN Config

The following entries are displayed on this screen:

- **Multicast VLAN**

Multicast VLAN: Select Enable/Disable Multicast VLAN feature.

VLAN ID: Enter the VLAN ID of the multicast VLAN.

Router Port Time: Specify the aging time of the router port. Within this time, if the switch doesn't receive IGMP query message from the router port, it will consider this port is not a router port any more.

Member Port Time: Specify the aging time of the member port. Within this time, if the switch doesn't receive IGMP report message from the member port, it will consider this port is not a member port any more.

Replace Source IP: Specify the IP address with which the switch will replace the source of MLD packets.

Dynamic Router Ports:	Displays the dynamic router ports of the multicast VLAN.
Static Router Ports:	Specify the static router port which is mainly used in the network with stable topology.
Forbidden Router Ports:	Specify the forbidden router ports which is mainly used to forbid ports becoming router ports.

Note:

1. The router port should be in the multicast VLAN, otherwise the member ports cannot receive multicast streams.
2. The Multicast VLAN won't take effect unless you first complete the configuration for the corresponding VLAN owning the port on the **802.1Q VLAN** page.
3. Configure the link type of the router port in the multicast VLAN as Tagged otherwise all the member ports in the multicast VLAN cannot receive multicast streams.
4. After a multicast VLAN is created, all the MLD packets will be processed only within the multicast VLAN.

9.2.5 Querier Config

In an IPv6 multicast network that runs MLD, a Layer 3 multicast device works as an MLD querier to send out MLD queries and manage the multicast table. But MLD is not supported by the devices in Layer 2 network. MLD Snooping Querier can act as an MLD Router in Layer 2 network. It can help to create and maintain multicast forwarding table on the switch with the Query messages it generates.

Choose the menu **Multicast→MLD Snooping→Querier Config** to load the following page.

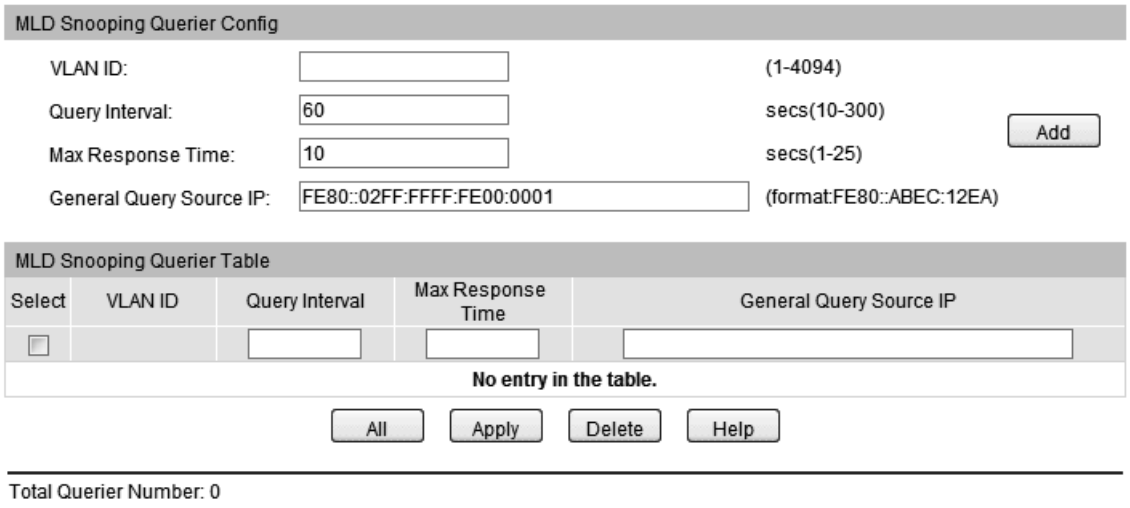


Figure 9-18 Querier Config

The following entries are displayed on this screen:

- **MLD Snooping Querier Config**

VLAN ID:	Enter the VLAN ID which you want to start Querier.
Query Interval:	Enter the Query message interval time. The Querier will send General Query Message within this interval.
Max Response Time:	Enter the value of Maximum Response Time of the Query message.
General Query Source IP:	Enter the Query Message source IP address. It is FE80::02FF:FFFF:FE00:0001 by default.

- **MLD Snooping Querier List**

Select:	Select the Querier you want to change.
VLAN ID:	Displays the VLAN ID.
Query Interval:	Displays the Query message interval time.
Max Response Time:	Displays the value of Maximum Response Time of the Query message.
General Query Source IP:	Displays the Query message source IP address.

Note:

The MLD Snooping Querier doesn't participate in the MLD Querier Election, but an MLD Snooping Querier will affect the MLD Querier Election in the IPv6 network running MLD because of its relatively smaller IP address.

9.2.6 Profile Config

On this page you can configure an MLD profile.

Choose the menu **Multicast→MLD Snooping→Profile Config** to load the following page.

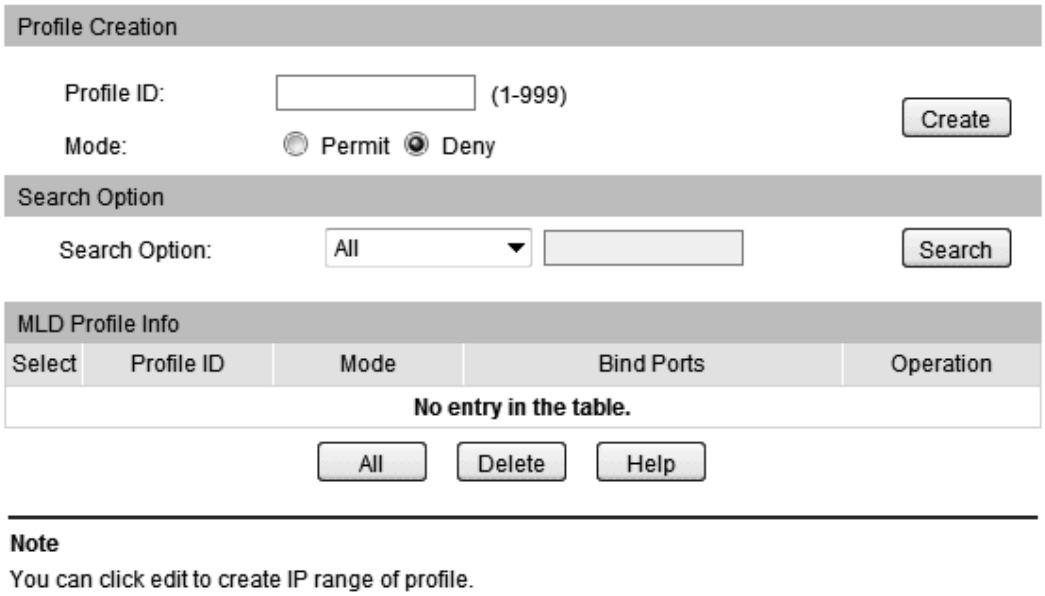


Figure 9-19 Profile Config

The following entries are displayed on this screen:

- **Profile Creation**

  Profile ID: Specify the Profile ID you want to create, and it should range from 1 to 999.

  Mode: The attributes of the profile.
  - **Permit**: Only permit the IP address within the IP range and deny others.
  - **Deny**: Only deny the IP address within the IP range and permit others.

- **Search Option**

  Search Option: Select the rules for displaying profile entries.
  - **All**: Display all profile entries.
  - **Profile ID**: Display profile entry of the ID.

- **MLD Profile Info**

  Select: Select the profile entries you want to config.

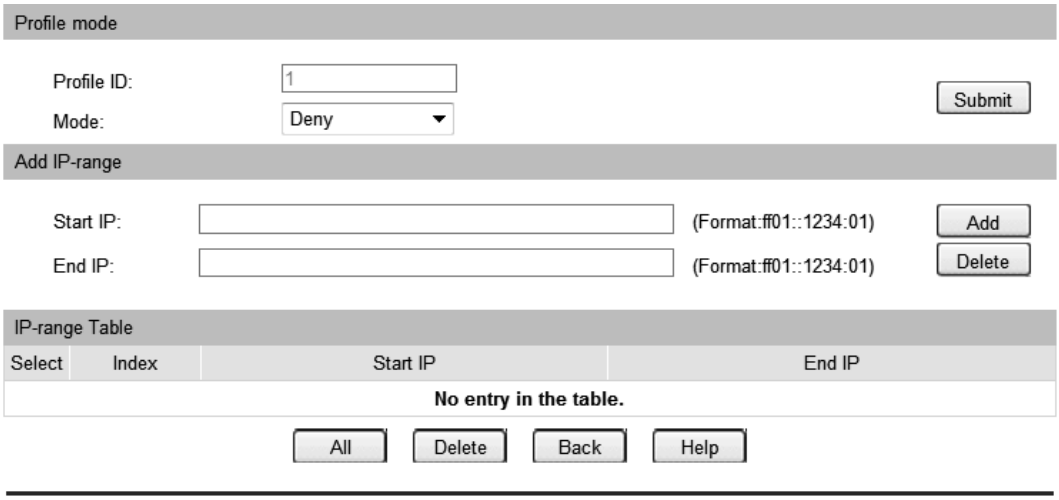
  Profile ID: Displays the profile ID.

  Mode: Displays the attribute of the profile.
  - **Permit**: Only permit the IP address within the IP range and deny others.
  - **Deny**: Only deny the IP address within the IP range and permit others.

Bind Ports: Displays the ports that the profile bound to.

Operation: Click the **Edit** button to configure the mode or IP-range of the Profile.

After you have created a profile ID, click **Edit** to display the following figure.



The following entries are displayed on this screen:

- **Profile Mode**

Profile ID: Displays the Profile ID you have created.

Mode: Displays the attribute of the profile.

- **Permit**: Only permit the IP address within the IP range and deny others.
- **Deny**: Only deny the IP address within the IP range and permit others.

- **Add IP-range**

Start IP: Enter start IP address of the IP-range.

End IP: Enter end IP address of the IP-range.

- **IP-range Table**

Select: Select the desired entry for configuration.

Index: Displays index of the IP-range which is not configurable.

Start IP: Displays the start IP address of the IP-range.

End IP: Displays the end IP address of the IP-range.

9.2.7 Profile Binding

When the switch receives MLD report message, it examines the profile ID bound to the access port to determine if the port can join the multicast group. If the multicast IP is not filtered, the switch will add the port to the forward port list of the multicast group. Otherwise, the switch will drop the MLD report message. In that way, you can control the multicast groups that users can access.

Choose the menu **Multicast→MLD Snooping→Profile Binding** to load the following page.

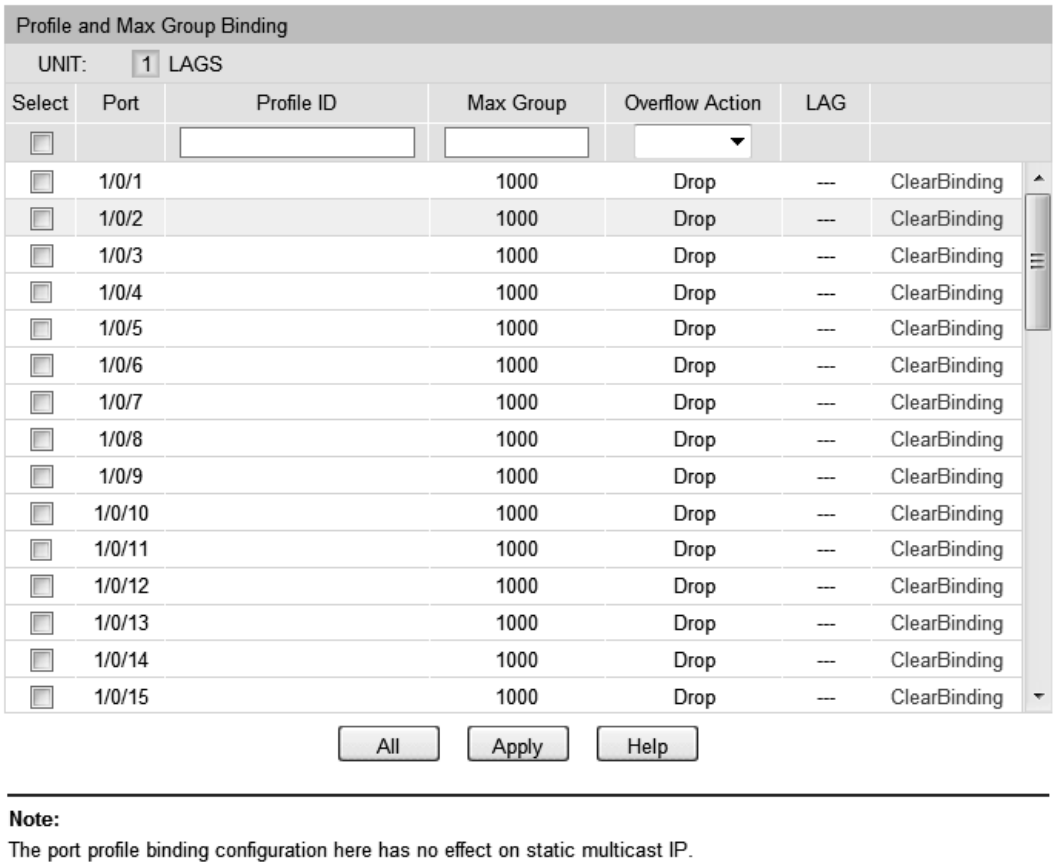


Figure 9-20 Profile Config

The following entries are displayed on this screen:

- **Profile and Max Group Binding**

UNIT:1/LAGS:	Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.
Select:	Select the desired port for multicast filtering. It is multi-optional.
Port:	The port to be bound.
Profile ID:	The existing Profile ID bound to the selected port.
Max Group:	The maximum multicast group a port can join, range from 0 to 1000.
Overflow Action:	The policy should be taken when the number of

multicast group a port has joined reach the maximum.

- **Drop:** Drop the successive report packet, and this port cannot join any other multicast group.
- **Replace:** When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

LAG: The LAG number which the port belongs to.

Clear Binding: Click the **Clear Binding** button to clear all profiles bound to the port.

➢ **Configuration Procedure:**

Step	Operation	Description
1	Create Profile	Required. Configure the Profile ID and mode on **Multicast→MLD Snooping→Profile Config** page.
2	Configure IP-Range	Required. Click **Edit** of the specified entry in the IGMP Profile Info table on **Multicast→MLD Snooping→Profile Config** page to configure the mode or IP-range of the Profile.
3	Configure Profile Binding for ports	Optional. Configure Profile Binding for ports on **Multicast→MLD Snooping→Porfile Binding** page.

9.2.8 Packet Statistics

On this page you can view the MLD packets the switch received. It helps you to monitor the MLD Snooping function.

Choose the menu **Multicast→MLD Snooping→Packet Statistics** to load the following page.

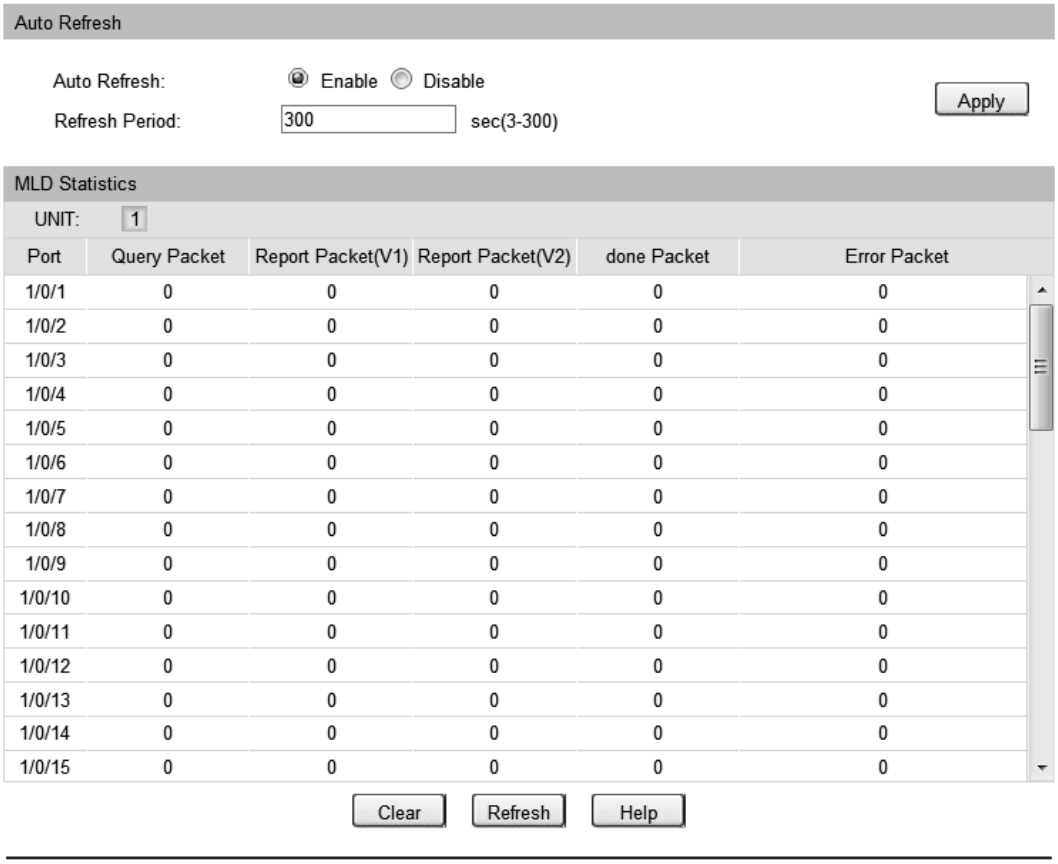


Figure 9-21 Packet Statistics

The following entries are displayed on this screen:

- **Auto Fresh**

Auto Fresh:	Select Enable/Disable auto fresh feature.
Fresh Period:	Enter the time from 3 to 300 seconds to specify the auto fresh period.

- **MLD Statistics**

Port:	Displays the port number of the switch.
Query Packet:	Displays the number of query packets the port received.
Report Packet (V1):	Displays the number of query packets the port received.
Report Packet (V2):	Displays the number of MLDv2 report packets the port received.
Done Packet:	Displays the number of leave packets the port received.

Error Packet: Displays the number of error packets the port received.

9.3 Multicast Table

In a network, receivers can join different multicast groups appropriate to their needs. The switch forwards multicast streams based on IPv4/IPv6 multicast address table.

The **Multicast Table** function is implemented on the **IPv4 Multicast Table**, **Static IPv4 Multicast Table, IPv6 Multicast Table** and **Static IPv6 Multicast Table** pages.

9.3.1 IPv4 Multicast Table

On this page you can view the information of the multicast groups already on the switch. Multicast IP addresses range from 224.0.0.0 to 239.255.255.255. The range for receivers to join is from 224.0.1.0 to 239.255.255.255.

Choose the menu **Multicast→Multicast Table→IPv4 Multicast Table** to load the following page.

Figure 9-22 IPv4 Multicast Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rule for displaying multicast IP table.

- **All**: Displays all multicast IP entries.
- **Multicast IP**: Enter the multicast IP address the desired entry must carry.
- **VLAN ID**: Enter the VLAN ID the desired entry must carry.
- **Forward Port**: Enter the port number the desired entry must carry.

➢ **Multicast IP Table**

Multicast IP: Displays multicast IP address.

VLAN ID: Displays the VLAN ID of the multicast group.

Forward Port: Displays the forward port of the multicast group.

Type: Displays the type of the multicast IP.

9.3.2 Static IPv4 Multicast Table

On this page you can configure the static IPv4 multicast table.

Choose the menu **Multicast→Multicast Table→Static IPv4 Multicast Table** to load the following page.

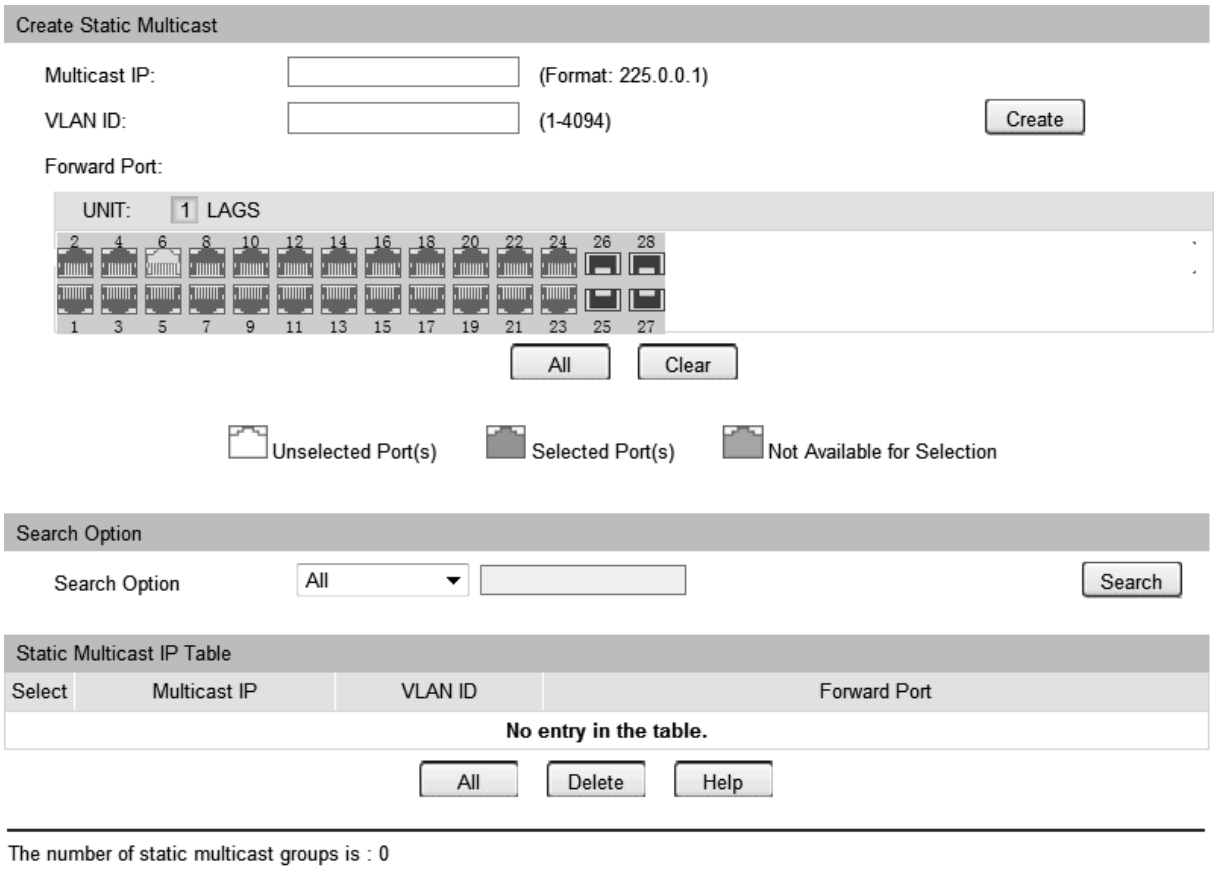


Figure 9-23 Static IPv4 Multicast Table

The following entries are displayed on this screen:

- **Create Static Multicast**

Multicast IP:	Enter the multicast IP address the desired entry must carry.
VLAN ID:	Enter the VLAN ID the desired entry must carry.
Forward Port:	Enter the forward ports.

➢ **Search Option**

Search Option: Select the rule for displaying multicast IP table.

- **All**: Displays all static multicast IP entries.
- **Multicast IP**: Enter the multicast IP address the desired entry must carry.
- **VLAN ID**: Enter the VLAN ID the desired entry must carry.
- **Forward Port**: Enter the port number the desired entry must carry.

➢ **Static Multicast Table**

Select: Select the static multicast group entries you want to configure.

Multicast IP: Displays multicast IP address.

VLAN ID: Displays the VLAN ID of the multicast group.

Forward Port: Displays the forward port of the multicast group.

9.3.3 IPv6 Multicast Table

This page displays the IPv6 multicast groups which are already on the switch.

Choose the menu **Multicast→Multicast Table→IPv6 Multicast Table** to load the following page.

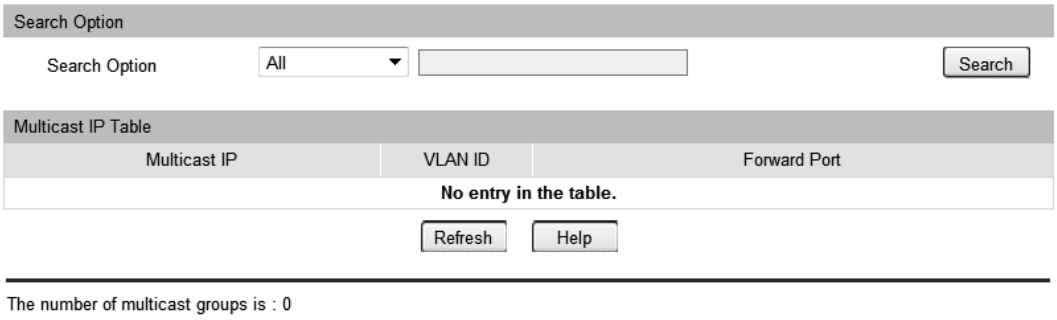


Figure 9-24 IPv6 Multicast Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying multicast IP table.

- **All**: Displays all multicast IP entries.
- **Multicast IP**: Enter the multicast IP address the desired entry must carry.
- **VLAN ID**: Enter the VLAN ID the desired entry must carry.
- **Forward Port**: Enter the port number the desired entry must carry.

➢ **Multicast IP Table**

Multicast IP:	Displays the multicast IP.
VLAN ID:	Displays the VLAN ID.
Forward Ports:	Displays the forward ports of the group.

9.3.4 Static IPv6 Multicast Table

On this page you can configure the static IPv6 multicast table.

Choose the menu **Multicast→Multicast Table→Static IPv6 Multicast Table** to load the following page.

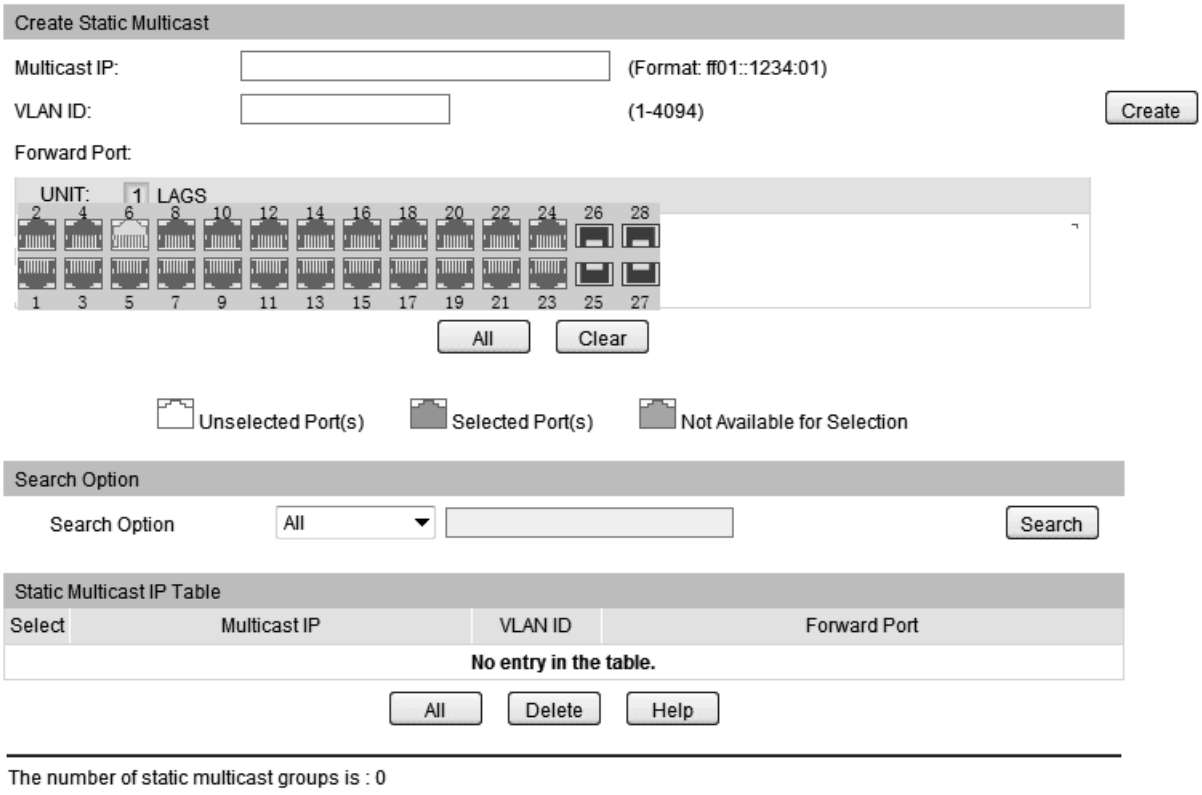


Figure 9-25 IPv6 Multicast Table

The following entries are displayed on this screen:

➢ **Create Static Multicast**

Multicast IP:	Enter the multicast IP address the desired entry must carry.
VLAN ID:	Enter the VLAN ID the desired entry must carry.
Forward Port:	Enter the forward ports.

➢ **Search Option**

Search Option:	Select the rule for displaying multicast IP table. • **All:** Displays all static multicast IP entries. • **Multicast IP:** Enter the multicast IP address the

desired entry must carry.

- **VLAN ID:** Enter the VLAN ID the desired entry must carry.
- **Forward Port:** Enter the port number the desired entry must carry.

➢ **Static Multicast Table**

Select:	Select the static multicast group entries you want to configure.
Multicast IP:	Displays multicast IP address.
VLAN ID:	Displays the VLAN ID of the multicast group.
Forward Port:	Displays the forward port of the multicast group.

Note:

The max number of multicast entries is 1000. The IPv4 multicast table and IPv6 multicast table share the total entry number of 1000.

Return to CONTENTS

Chapter 10 Routing

Routing is the method by which the host or gateway decides where to send the datagram. Routing is the task of finding a path from a sender to a desired destination. It may be able to send the datagram directly to the destination, if that destination is on one of the networks that are directly connected to the host or gateway. However, what if the destination is not directly reachable? The host or gateway will attempt to send the datagram to a gateway that is nearer to the destination. The goal of a routing protocol is very simple: It is to supply the information that is needed to do routing.

The Routing module is mainly for routing management configuration of the switch, including the following submenus: **Interface**, **Routing Table**, **Static Routing**, **DHCP Server**, **DHCP Relay** and **ARP**.

10.1 Interface

Interface is a virtual interface in Layer 3 mode and mainly used for realizing the Layer 3 connectivity between VLANs or routed ports. Each VLAN interface is corresponding to one VLAN. Each routed port is corresponding to one port. Each Layer 3 port-channel is corresponding to one port channel. Loopback Interface is purely software implemented. Interface has its own IP address and subnet mask to identify the subnet it belongs to, and it works as the gateway of the subnet to forward Layer 3 IP packets.

Introduction of IPv6 Address

IPv6 (Internet Protocol version 6), also called IPng (IP next generation), was developed by the IETF (Internet Engineering Task Force) as the successor to IPv4 (Internet Protocol version 4). Compared with IPv4, IPv6 increases the IP address size from 32 bits to 128 bits; this solves the IPv4 address exhaustion problem.

- **IPv6 features**

IPv6 has the following features:

1. **Adequate address space:** The source and destination IPv6 addresses are both 128 bits (16 bytes) long. IPv6 can provide 3.4 x 10^{38} addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.
2. **Header format simplification:** IPv6 cuts down some IPv4 header fields or move them to IPv6 extension headers to reduce the load of basic IPv6 headers, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of basic IPv6 headers is 40 bytes and is only twice that of IPv4 headers (excluding the Options field).
3. **Flexible extension headers:** IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the handling efficiency. The Options field in IPv4 packets

contains 40 bytes at most, while the size of IPv6 extension headers is restricted by that of IPv6 packets.

4. **Built-in security:** IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and improves the interoperability between different IPv6 applications.
5. **Automatic address configuration:** To simplify the host configuration, IPv6 supports stateful and stateless address configuration.
   - Stateful address configuration means that a host acquires an IPv6 address and related information from a server (for example, DHCP server).
   - Stateless address configuration means that a host automatically configures an IPv6 address and related information on basis of its own link-layer address and the prefix information advertised by a router.

   In addition, a host can generate a link-local address on basis of its own link-layer address and the default prefix (FE80::/64) to communicate with other hosts on the link.
6. **Enhanced neighbor discovery mechanism:** The IPv6 neighbor discovery protocol is a group of Internet control message protocol version 6 (ICMPv6) messages that manages the information exchange between neighbor nodes on the same link. The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP) message, Internet Control Message Protocol version 4 (ICMPv4) router discovery message, and ICMPv4 redirection message to provide a series of other functions.

➢ **Introduction to IPv6 address**

1. IPv6 address format

   An IPv6 address is represented as a series of 16-bit hexadecimals, separated by colons (:). An IPv6 address is divided into eight groups, and the 16 bits of each group are represented by four hexadecimal numbers which are separated by colons, for example, 2001:0d02:0000:0000:0014: 0000:0000:0095. The hexadecimal letters in IPv6 addresses are not case-sensitive.

   To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

   - Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in shorter format as 2001:d02:0:0:14:0:0:95.
   - Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address. For example, the above-mentioned address can be represented in the shortest format as 2001:d02::14:0:0:95.

Note:

Two colons (::) can be used only once in an IPv6 address, usually to represent the longest successive hexadecimal fields of zeros. If two colons are used more than once, the device is unable to determine how many zeros double-colons represent when converting them to zeros to restore a 128-bit IPv6 address.

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is represented in "IPv6 address/prefix length" format, where "IPv6 address" is an IPv6 address in any of the above-mentioned formats and "prefix length" is a decimal number indicating how many leftmost bits from the preceding IPv6 address are used as the address prefix.

2. IPv6 address classification

IPv6 addresses fall into three types: unicast address, multicast address, and anycast address.

- Unicast address: An identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.
- Multicast address: An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address. There are no broadcast addresses in IPv6. Their function is superseded by multicast addresses.
- Anycast address: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols' measure of distance).

The type of an IPv6 address is designated by the first several bits called format prefix. The following table lists the mappings between address types and format prefixes.

Type		Format Prefix (binary)	IPv6 Prefix ID
Unicast address	Unassigned address	00…0 (128 bits)	::/128
	Loopback address	00…1 (128 bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site-local address	1111111011	FEC0::/10

Type		Format Prefix (binary)	IPv6 Prefix ID
	Global unicast address (currently assigned)	001	2xxx::/4 or 3xxx::/4
	Reserved type (to be assigned in future)	Other formats	
Multicast address		11111111	FF00::/8
Anycast address		Anycast addresses are taken from unicast address space and are not syntactically distinguishable from unicast addresses.	

Table 10-1 Mappings between address types and format prefixes

3. IPv6 Unicast Address：

IPv6 unicast address is an identifier for a single interface. It consists of a subnet prefix and an interface ID.

- Subnet Prefix: This section is allocated by the IANA (The Internet Assigned Numbers Authority), the ISP (Internet Service Provider) or the organizations.
- Interface ID: An interface ID is used to identify interfaces on a link. The interface ID must be unique to the link.

There are several ways to form interface IDs. The IPv6 addresses with format prefixes 001 through 111, except for multicast addresses (1111 1111), are all required to have 64-bit interface IDs in EUI-64 format.

For all IEEE 802 interface types (for example, Ethernet and FDDI interfaces), Interface IDs in the modified EUI-64 format are constructed in the following way:

The first three octets (24 bits) are taken from the Organizationally Unique Identifier (OUI) of the 48-bit link-layer address (the MAC address) of the interface, the fourth and fifth octets (16 bits) are a fixed hexadecimal value of FFFE, and the last three octets (24 bits) are taken from the last three octets of the MAC address. The construction of the interface ID is completed by setting the universal/local (U/L) bit--the seventh bit of the first octet--to a value of 0 or 1. A value of 0 indicates a locally administered identifier; a value of 1 indicates a globally unique IPv6 interface identifier.

Take MAC address 0012:0B0A:2D51 as an example. Insert **FFFE** to the middle of the address to get 0012:0B**FF:FE**0A:2D51. Then set the U/L bit to 1 to obtain an interface ID in EUI-64 format as 0**2**12:0BFF:FE0A:2D51.

IPv6 unicast address can be classified into several types, as shown in Table 10-1. The two most common types are introduced below:

Global unicast address

A Global unicast address is an IPv6 unicast address that is globally unique and is routable on the global Internet.

Global unicast addresses are defined by a global routing prefix, a subnet ID, and an interface ID. The IPv6 global unicast address starts with binary value 001 (2000::/3). The global routing prefix is a value assigned to a site (a cluster of subnets/links) by IANA. The subnet ID is an identifier of a subnet within the site.

The figure below shows the structure of a global unicast address.

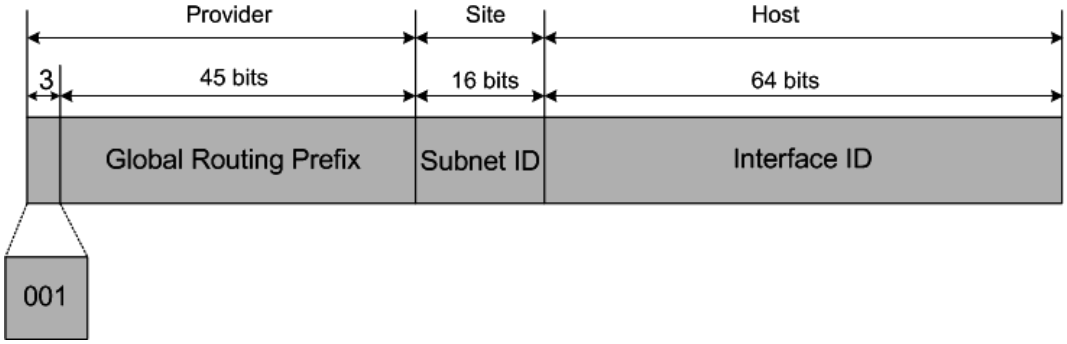


Figure 10-1 Global Unicast Address Format

Link-local address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate. The figure below shows the structure of a link-local address.

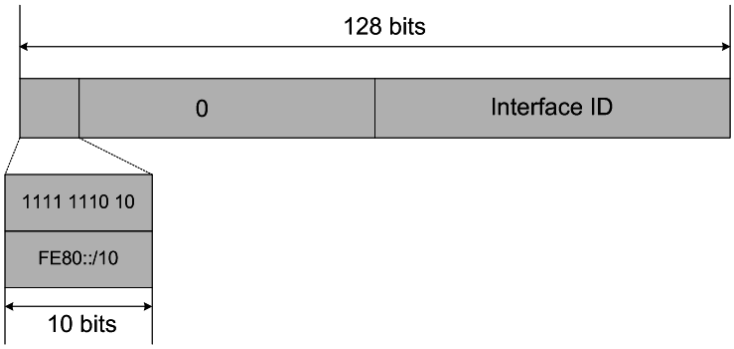


Figure 10-2 Link-local Address Format

IPv6 devices must not forward packets that have link-local source or destination addresses to other links.

Note:

You can configure multiple IPv6 addresses per interface, but only one link-local address.

- **IPv6 Neighbor Discovery**

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

1. IPv6 Neighbor Solicitation Message and Neighbor Advertisement Message

   A value of 135 in the Type field of the ICMP packet header identifies a neighbor solicitation (NS) message. Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link.

   After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement (NA) message, which has a value of 136 in the Type field of the ICMP packet header, on the local link. After the source node receives the neighbor advertisement, the source node and destination node can communicate.

   Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link.

   Address Resolution

   The address resolution procedure is as follows:

   - Node A multicasts an NS message. The source address of the NS message is the IPv6 address of an interface of node A and the destination address is the solicited-node multicast address of node B. The NS message contains the link-layer address of node A.
   - After receiving the NS message, node B judges whether the destination address of the packet corresponds to the solicited-node multicast address. If yes, node B can learn the link-layer address of node A, and unicasts an NA message containing its link-layer address.
   - Node A acquires the link-layer address of node B from the NA message.

   Neighbor Reachability Detection

   After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

   - Node A sends an NS message whose destination address is the IPv6 address of node B.
   - If node A receives an NA message from node B, node A considers that node B is reachable. Otherwise, node B is unreachable.

   Duplicate Address Detection

   Neighbor solicitation messages are used in the stateless autoconfiguration process to verify the uniqueness of unicast IPv6 addresses before the addresses are assigned to an interface. After node A acquires an IPv6 address, it will perform duplicate address detection (DAD) to determine whether the address is being used by other nodes (similar to the

gratuitous ARP function of IPv4). DAD is accomplished through NS and NA messages. The DAD procedure is as follows:

- Node A sends an NS message whose source address is the unassigned address :: and destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message contains the IPv6 address.
- If node B uses this IPv6 address, node B returns an NA message. The NA message contains the IPv6 address of node B.
- Node A learns that the IPv6 address is being used by node B after receiving the NA message from node B. Otherwise, node B is not using the IPv6 address and node A can use it.

2. IPv6 Router Advertisement Message

   Router advertisement (RA) messages, which have a value of 134 in the Type field of the ICMP packet header, are periodically sent out each configured interface of an IPv6 router.

   RA messages typically include the following information:

   - One or more onlink IPv6 prefixes that nodes on the local link can use to automatically configure their IPv6 addresses.
   - Lifetime information for each prefix included in the advertisement.
   - Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed.
   - Default router information (whether the device sending the advertisement should be used as a default router and, if so, the amount of time, in seconds, the device should be used as a default router).
   - Additional information for hosts, such as the hop limit and maximum transmission unit (MTU) a host should use in packets that it originates.

   RAs are also sent in response to device solicitation messages. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup or anytime needed so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

   Hosts discover and select default devices by listening to Router Advertisements (RAs).

   Stateless address autoconfiguration means that the node automatically configures an IPv6 address and other information for its interface according to the address prefix and other configuration parameters in the received RA messages.

3. IPv6 Neighbor Redirect Message

A value of 137 in the type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Devices send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination.

A device will send an IPv6 ICMP redirect message when the following conditions are satisfied:

- The receiving interface is the forwarding interface.
- The selected route itself is not created or modified by an IPv6 ICMP redirect message.
- The selected route is not the default route.
- The forwarded IPv6 packet does not contain any routing header.

You can configure the system's Layer 3 interfaces on this page.

Choose the menu **Routing→Interface→Interface Config** to load the following page.

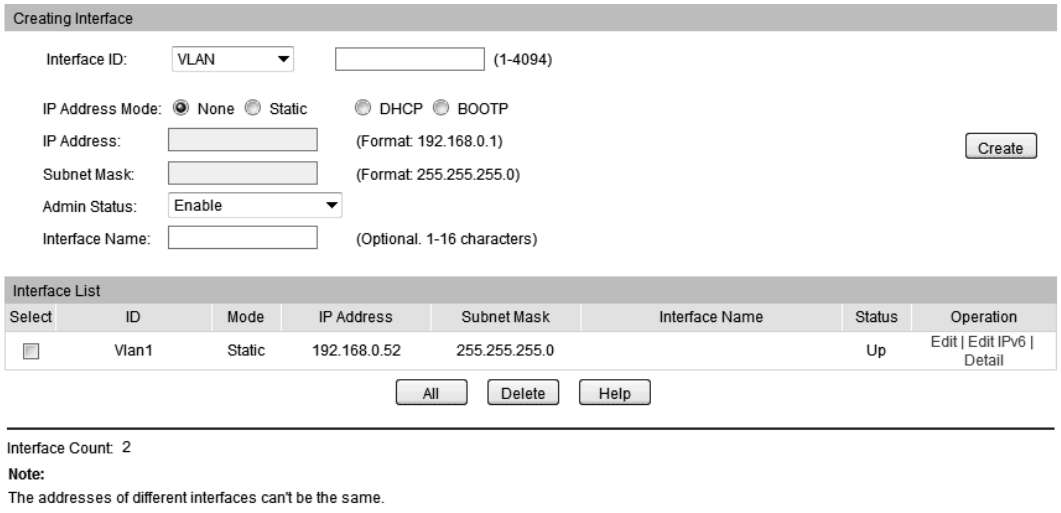


Figure 10-3 Interface Config

The following entries are displayed on this screen:

➢ **Create Interface**

Interface ID: Enter the ID of the interface corresponding to VLAN interface, loopback interface, routed port or port channel.

IP Address Mode: Specify IP Address allocation mode.

- **None**: without ip.
- **Static**: setup manually.
- **DHCP:** allocated through DHCP.
- **BOOTP**: allocated through BOOTP.

IP Address: Specify the IP address of the interface.

Subnet Mask: Specify the subnet mask of the interface's IP address.

Admin Status: Specify interface administrator status. Choose **Disable** to disable the interface's Layer 3 capabilities.

Interface Name: Specify the name of the network interface.

- **Interface List**

Select : Select the interfaces to modify or delete.

ID: Displays the ID of the interface.

Mode: Display IP address allocation mode.

- **None:** without ip.
- **Static:** setup manually.
- **DHCP:** allocated through DHCP.
- **BOOTP:** allocated through BOOTP.

IP Address: Displays the IP address of the interface.

Subnet Mask: Displays the subnet mask of the interface.

Interface Name: Displays the name of the interface.

Status: Displays interface current working status. Working status is up when admin status is enabled, line protocol is up and IP Address is set.

Operation: You can configure the interface by clicking the **Edit**, or check Detail information by clicking **Detail**.

- **For IPv4 interface**

Click **Edit** to display the following figure:

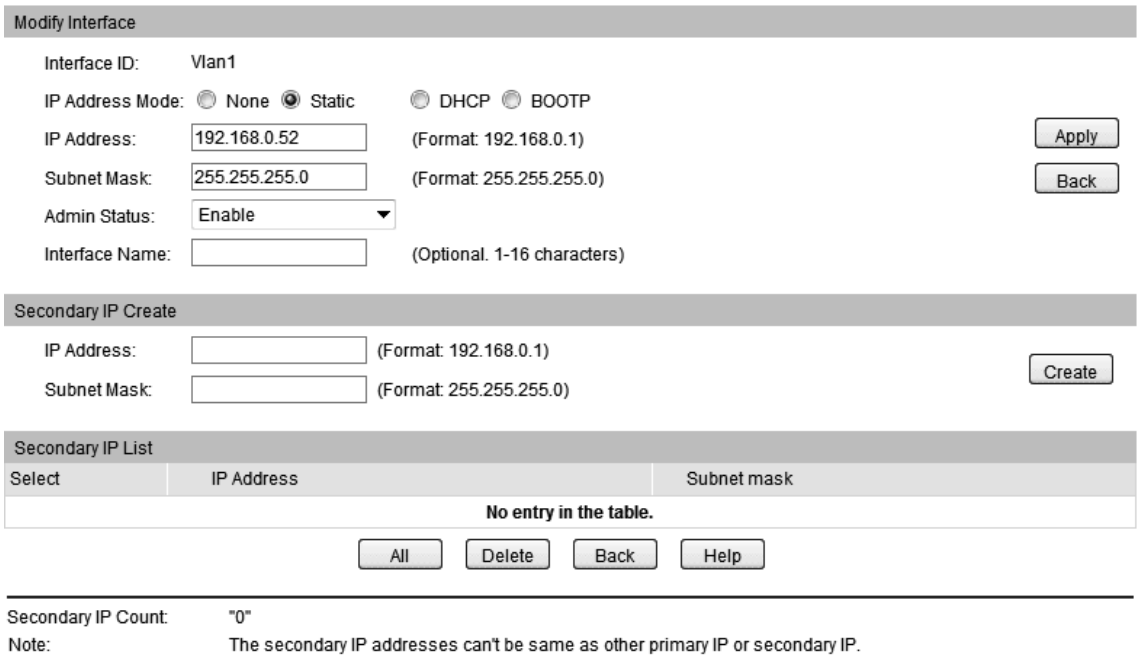


Figure 10-4 IPv4 Interface Config

➢ **Modify Interface**

Interface ID: Display the ID of the interface corresponding to the VLAN interface, loopback interface, routed port or port channel.

IP Address Mode: View and modify the IP address allocation mode.

- **None**: without ip.
- **Static**: setup manually.
- **DHCP**: allocated through DHCP.
- **BOOTP**: allocated through BOOTP.

IP Address: View and modify the IP address of the interface.

Subnet Mask: View and modify the subnet mask of the interface.

Admin Status: View and modify the Admin status. Choose **Disable** to disable the interface's Layer 3 capabilities.

Interface Name: View and modify the interface name.

➢ **Secondary IP Create**

IP Address: Specify the secondary IP address of the interface.

Subnet Mask: Specify the subnet mask of the interface's secondary IP address.

➢ **Secondary IP List**

Select: Select the secondary IP.

IP Address: Displays the secondary IP address of the current interface.

Subnet Mask: Displays the subnet mask of the secondary IP address.

- **For IPv6 interface**

Click **Edit** to display the following figure:

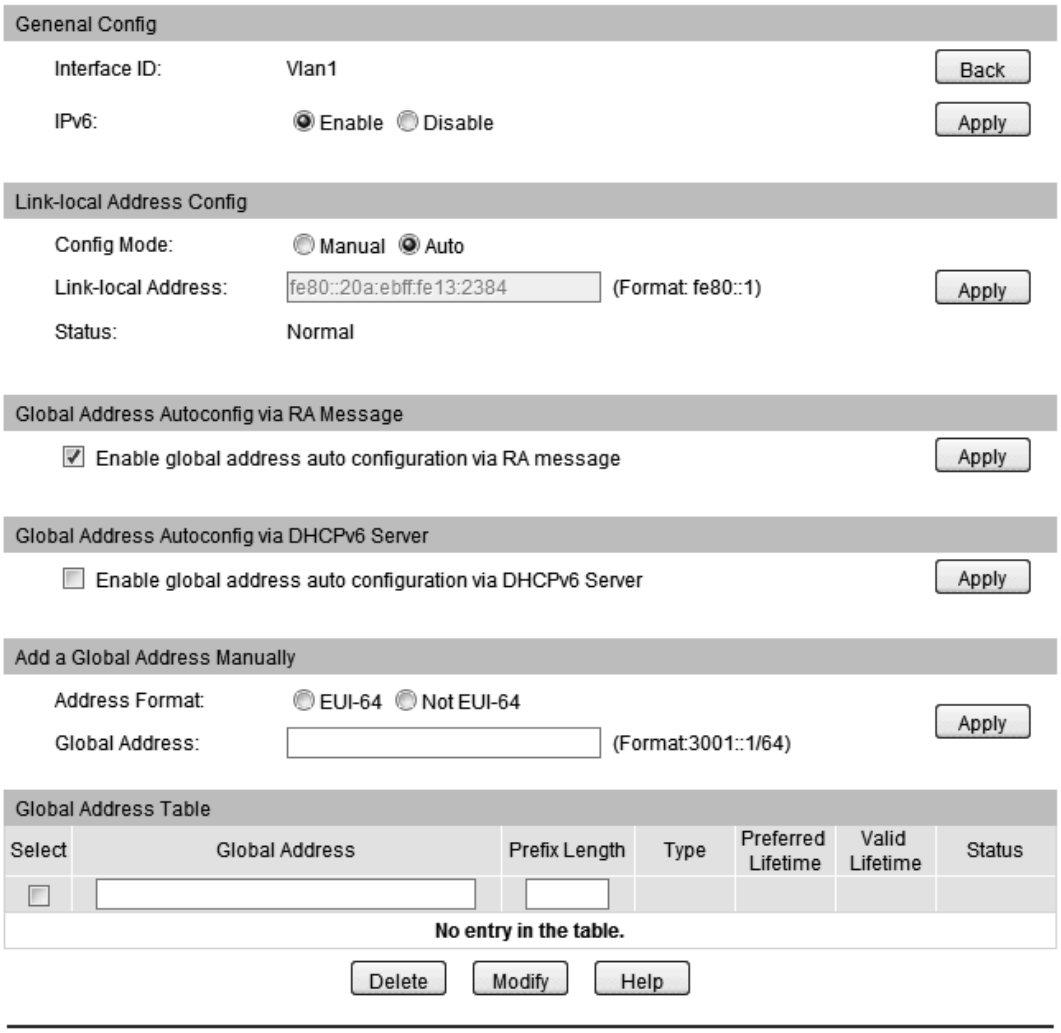


Figure 10-5 System IPv6

The following entries are displayed on this screen:

➢ **Global Config**

IPv6: Enable/Disable IPv6 function globally on the switch.

Interface ID: Choose the interface type and input the interface ID. Interface types include VLAN, routed port and port channel.

- **Link-local Address Config**

Config Mode: Select the link-local address configuration mode.

- **Manual:** When this option is selected, you should assign a link-local address manually.
- **Auto:** When this option is selected, the switch will generate a link-local address automatically.

Link-local Address: Enter a link-local address.

Status: Displays the status of the link-local address.

- **Normal:** Indicates that the link-local address is normal.
- **Try:** Indicates that the link-local address may be newly configured.
- **Repeat:** Indicates that the link-local address is duplicate. It is illegal to access the switch using the IPv6 address (including link-local and global address).

- **Global Address Autoconfig via RA Message**

Enable global address auto configuration via RA message: When this option is enabled, the switch automatically configures a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.

- **Global Address Autoconfig via DHCPv6 Server**

Enable Global Address Autoconfig via DHCPv6 Server: When this option is enabled, the system will try to obtain the global address from the DHCPv6 Server.

- **Add a global address manually**

Address Format: You can select the global address format according to your requirements.

- **EUI-64:** Indicates that you only need to specify an address prefix, and then the system will create a global address automatically.
- **Not EUI-64:** Indicates that you have to specify an intact global address.

Global Address: When selecting the mode of EUI-64, please input the address prefix here, otherwise, please input an intact IPv6 address here.

- **Global address Table**

Select: Select the desired entry to delete or modify the corresponding global address.

Global Address: Modify the global address.

Prefix Length:	Modify the prefix length of the global address.
Type:	Displays the configuration mode of the global address. ● **Manual:** Indicates that the corresponding address is configured manually. ● **Auto:** Indicates that the corresponding address is created automatically using the RA message or obtained from the DHCPv6 Server.
Preferred Lifetime/Valid Lifetime:	Displays the preferred time and valid time of the global address.
Status:	Displays the status of the global address. ● **Normal:** Indicates that the global address is normal. ● **Try:** Indicates that the global address may be newly configured. ● **Repeat:** Indicates that the corresponding address is duplicate. It is illegal to access the switch using this address.

Tips:

After adding a global IPv6 address to your switch manually here, you can configure your PC's global IPv6 address in the same subnet with the switch and login to the switch via its global IPv6 address.

Click **Detail** to display the following figure:

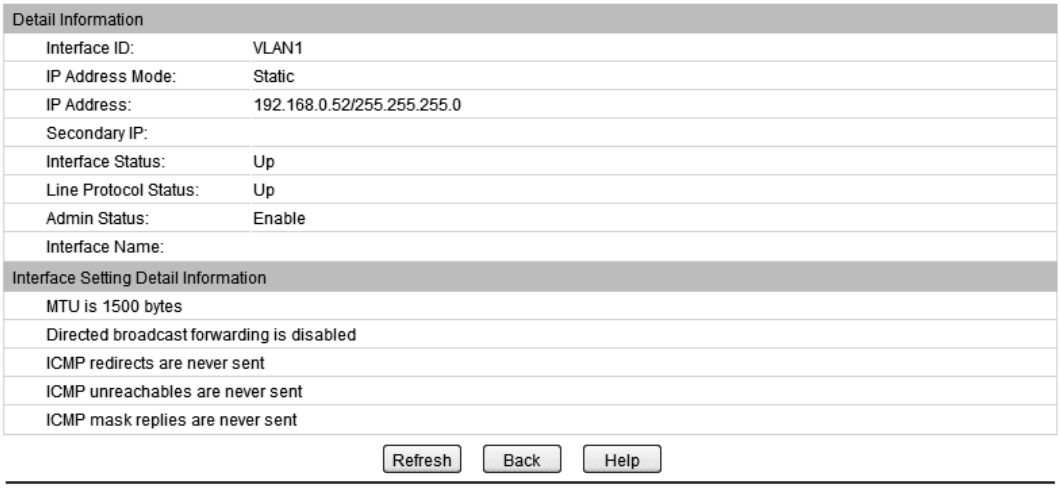


Figure 10-6 The Interface's Detail Information

➢ **Detail Information**

Interface ID: Displays the ID of the interface, including VLAN interface, loopback interface, routed port and port channel.

IP Address Mode: Displays the IP address allocation mode.

- **None**: without ip.
- **Static**: setup manually.
- **DHCP**: allocated through DHCP.
- **BOOTP**: allocated through BOOTP.

IP Address: Displays the IP address and subnet mask of the interface.

Secondary IP: Displays Secondary IP Address and subnet mask.

Interface Status: Displays the interface current working status, which is up when Admin Status is enable, line protocol is up and IP address is set.

Line Protocol Status: Displays the line protocol status, which is up if any up-link port is connected to the interface.

Admin Status: Displays the Admin status. Choose **Disable** to disable the interface's Layer 3 capabilities.

Interface Name: Displays the name of the interface.

➢ **Interface Setting Detail Information**

Displays the detailed setting information of the interface.

10.2 Routing Table

This page displays the routing information summary generated by different routing protocols.

10.2.1 IPv4 Routing Table

Choose the menu **Routing→Routing Table→IPv4 Routing Table** to load the following page.

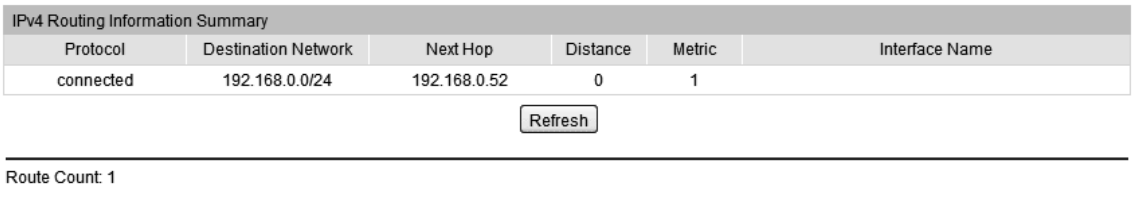


Figure 10-7 Routing Table

The following entries are displayed on this screen:

➢ **Routing Information Summary**

Protocol Displays the protocol of the route.

Destination/Mask: Displays the destination and subnet of the route.

Next Hop: Displays the IP address to which the packet should be sent next.

Distance: Displays the management distance of the route. The smaller the distance, the higher the priority.

Metric: Displays the metric of the route.

Interface name: Displays the description of the egress interface.

10.2.2 IPv6 Routing Table

Choose the menu **Routing→Routing Table→IPv6 Routing Table** to load the following page.

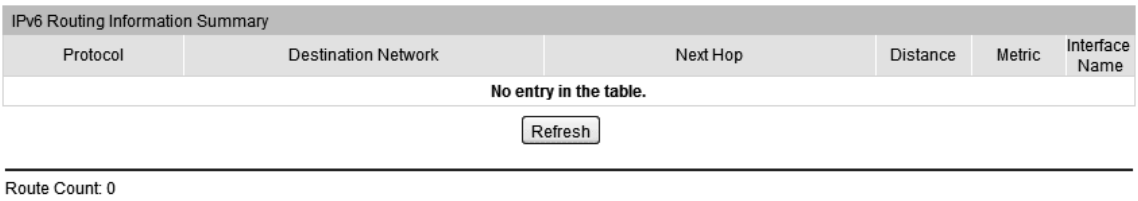


Figure 10-8 IPv6 Routing Table

The following entries are displayed on this screen:

- **IPv6 Routing Information Summary**

Protocol Displays the protocol of the route.

Destination/Mask: Displays the destination and subnet of the route.

Next Hop: Displays the IPv6 address to which the packet should be sent next.

Distance: Displays the management distance of the route. The smaller the distance, the higher the priority.

Metric: Displays the metric of the route.

Interface name: Displays the description of the egress interface.

10.3 Static Routing

Static routes are special routes manually configured by the administrator and cannot change automatically with the network topology accordingly. Hence, static routes are commonly used in a relative simple and stable network. Proper configuration of static routes can greatly improve network performance.

10.3.1 IPv4 Static Routing Config

Choose the menu **Routing→Static Routing→Static Routing Config** to load the following page.

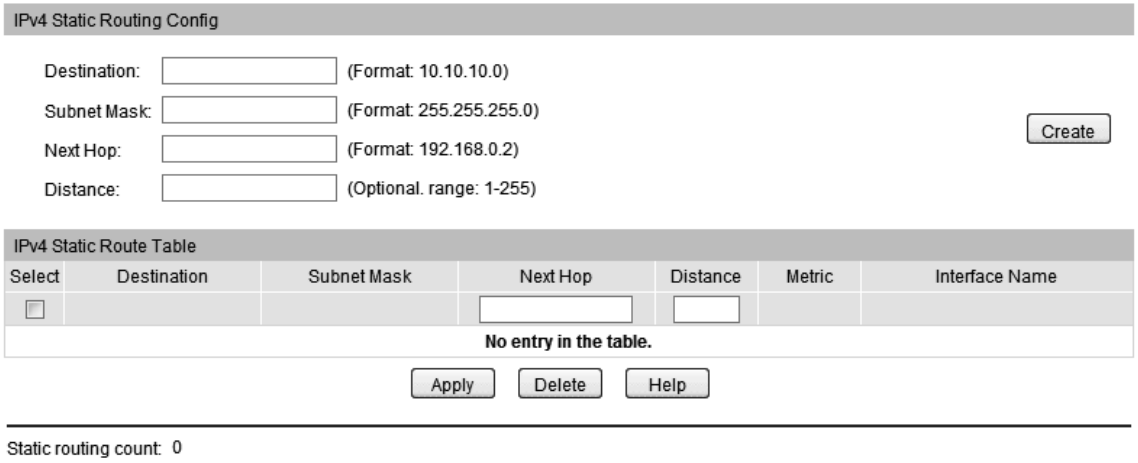


Figure 10-9 Static Routing Config

The following entries are displayed on this screen:

- **Static Routing Config**

Destination:	Specify the destination IP address of the packets.
Subnet Mask:	Specify the subnet mask of the destination IP address.
Next Hop:	Enter the IP address to which the packet should be sent next.
Distance:	Enter the distance metric of route. The smaller the distance, the higher the priority.

- **Static Route Table**

Select:	Specify the static route entries to modify.
Destination Address:	Displays the destination IP address of the packets.
Subnet Mask:	Displays the subnet mask of the destination IP address.
Next Hop:	Displays the IP address to which the packet should be sent next.
Distance:	Displays the distance metric of route. The smaller the distance, the higher the priority.
Metric:	Displays the metric of the route.
Interface Name:	Displays the name of the VLAN interface.

10.3.2 IPv6 Static Routing Config

Choose the menu **Routing→Static Routing→Static Routing Config** to load the following page.

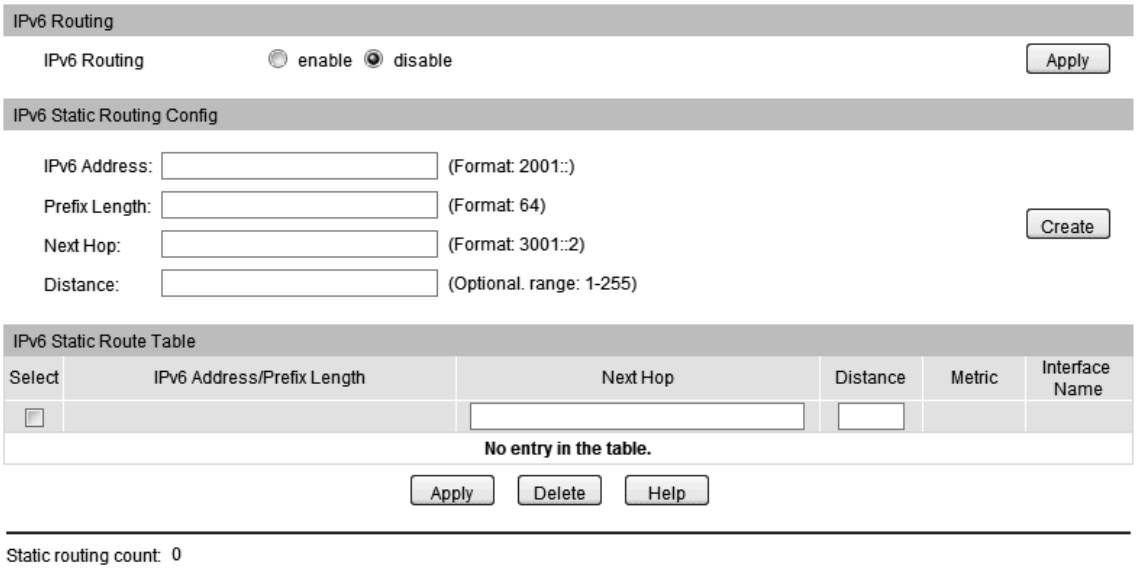


Figure 10-10 Static Routing Config

The following entries are displayed on this screen:

- **Static Routing Config**

IPv6 Address: Specify the destination IPv6 address of the packets.

Prefix Length: Specify the prefix length of the IPv6 address.

Next Hop: Enter the IPv6 address to which the packet should be sent next.

Distance: Enter the distance metric of route. The smaller the distance, the higher the priority.

- **Static Route Table**

Select: Select the IPv6 static route entries to modify.

IPv6 Address: Displays the destination IPv6 address of the packets.

Prefix Length: Displays the prefix length of the destination IPv6 address.

Next Hop: Displays the IPv6 address to which the packet should be sent next.

Distance: Displays the distance metric of route. The smaller the distance, the higher the priority.

Metric: Displays the metric of the route.

Interface Name: Displays the name of the VLAN interface.

10.4 DHCP Server

DHCP module is used to configure the DHCP functions of the switch, including two submenus, **DHCP Server** and **DHCP Relay**.

➢ **Overview**

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP is adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of DHCP participants so the administrator can manage the parameters of the host in the network.

As workstations and personal computers proliferate on the Internet, the administrative complexity of maintaining a network is increased by an order of magnitude. The assignment of local network resources to each client represents one such difficulty. In most environments, delegating such responsibility to the user is not plausible and, indeed, the solution is to define the resources in uniform terms, and to automate their assignment.

The DHCP dealt with the issue of assigning an internet address to a client, as well as some other resources.

➢ **DHCP Elements**

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to DHCP clients. Generally a DHCP server can allocate configuration parameters to more than one client. Figure 10-11 DHCP model shows you the model.

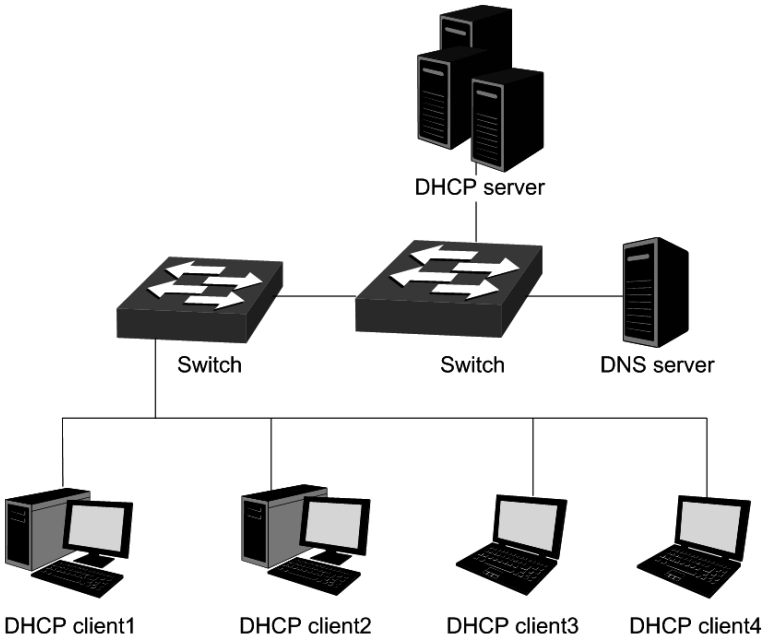


Figure 10-11 DHCP model

To meet the different requirements of DHCP clients, DHCP server is always designed to supply hosts with the configuration parameters in three policies.

1) Manual Assignment: For the specific DHCP clients (e.g., web server), the configuration parameters are manually specified by the administrator and are assigned to these clients via a DHCP server.

2) Automatic Assignment: The DHCP server must supplies the configuration parameters to DHCP client with the lease time continued for ever.

3) Dynamic Assignment: A network administrator assigns a range of IP addresses to DHCP server, and each client computer on the LAN is configured to request an IP address from the DHCP server with a fixed period of time (e.g., 2 hours), allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.

➢ **The Process of DHCP**

DHCP uses UDP as its transport protocol. DHCP messages from a client to a server are sent to the 'DHCP server' port (67), and DHCP messages from a server to a client are sent to the 'DHCP client' port (68). DHCP clients and servers both construct DHCP messages by filling in fields in the fixed format section of the message and appending tagged data items in the variable length option area. The process is shown as follows.

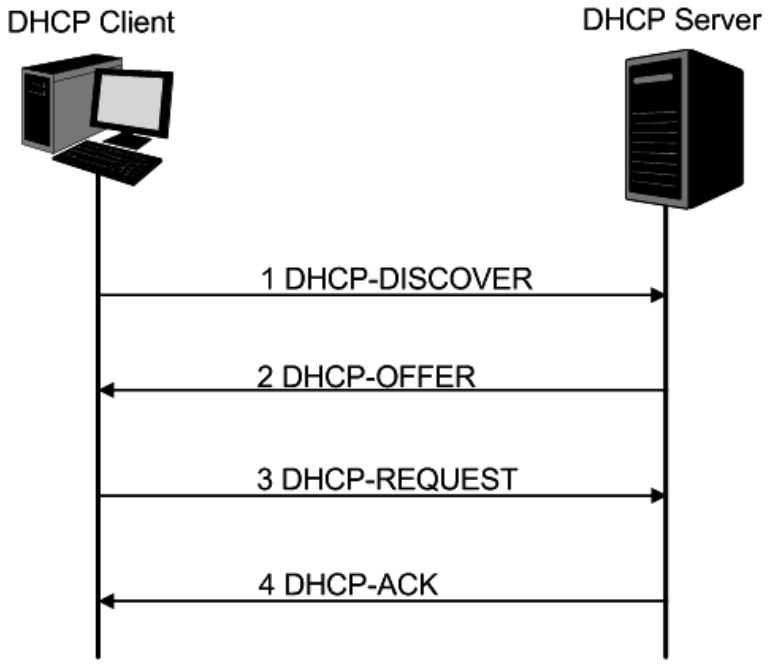


Figure 10-12 The Process of DHCP

1) DHCP discover: the client broadcasts messages on the physical subnet to discover available DHCP servers in the LAN. Network administrators can configure a local router (e.g. a relay agent) to forward DHCP-DISCOVER messages to a DHCP server in a different subnet.

2) DHCP offer: Each server who received the DHCP-DISCOVER message may respond a DHCP-OFFER message that includes configuration parameters (in the example below, IP address) to the client. The server unicast the DHCP-OFFER message to the client (using the DHCP/BOOTP relay agent if necessary) if possible, or may broadcast the message to a broadcast address on the client's subnet.

3) DHCP request: A client can receive DHCP offers from multiple servers, but it will accept only one DHCP-OFFER and broadcast a DHCP-REQUEST message which includes the server's identifier and the IP address offered by the server. Based on the server's identifier, servers are informed whose offer the client has accepted.

4) DHCP acknowledgement: The server selected in the DHCP-REQUEST message commits the binding for the client to persistent storage and responds with a DHCP-ACK message containing the configuration parameters for the requesting client. If the selected server is unable to satisfy the DHCP-REQUEST message (e.g., the requested IP address has been allocated), the server should respond with a DHCP-NAK message.

5) In Dynamic assignment policy, the DHCP client is assigned an IP address with a lease time (e.g. 2 hours) from the DHCP server. This IP address will be reclaimed by the DHCP server when its lease time expires. If the client wants to use the IP address continually, it should unicast a DHCP-REQUEST message to the server to extend its lease.

After obtaining parameters via DHCP, a host should be able to exchange packets with any other host in the networks.

- **The Format of DHCP Message**

Figure 10-12 The Process of DHCPgives the process of DHCP and Figure 10-13 describes each field in the DHCP message. The numbers in parentheses indicate the size of each field in octets. The names for the fields given in the figure will be used throughout this document to refer to the fields in DHCP messages.

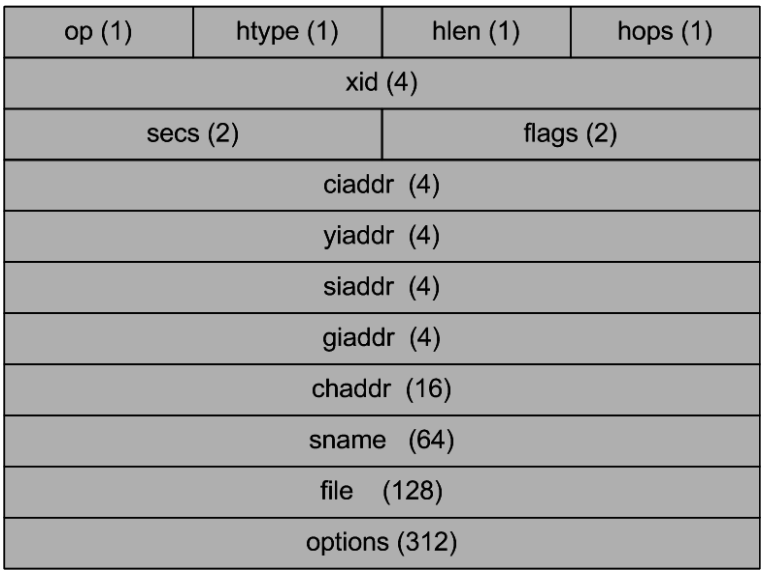


Figure 10-13 The Format of DHCP Message

1) op：Message type, '1' = BOOT-REQUEST, '2' = BOOT-REPLY.

2) htype：Hardware address type, '1' for ethernet.

3) hlen：Hardware address length, '6' for ethernet.

4) hops：Clients set this field to zero and broadcast the DHCP-REQUEST message , optionally used by relay-agents when booting via a relay-agent.

5) xid：Transaction ID, a random number chosen by the client, used by the client and server to associate messages.

6) secs：Filled in by client, seconds elapsed since client started trying to boot.

7) flags：A client that cannot receive unicast IP datagrams until its protocol software has been configured with an IP address should set the first bit in the 'flags' field to 1 in any DHCP-DISCOVER or DHCP-REQUEST message that client sends. A client that can receive unicast IP datagrams before its protocol software has been configured should clear the first bit to 0. A server or relay agent sending or relaying a DHCP message directly to a DHCP client should examine the first bit in the 'flags' field. If this bit is set to 1, the DHCP message should be sent as an IP broadcast and if the bit is cleared to 0, the message should be sent as an IP unicast. The remaining bits of the flags field are reserved for future use and must be set to zero by clients and ignored by servers and relay agents.

8) ciaddr：Client IP address, filled in by client in DHCPREQUEST when verifying previously allocated configuration parameters.

9) yiaddr：'your' (client) IP address, configuration parameters allocated to the client by DHCP server.

10) siaddr：IP address of next server to use in bootstrap, returned in DHCPOFFER, DHCPACK and DHCPNAK by server.

11) giaddr：Relay agent IP address, used in booting via a relay-agent.

12) chaddr：Client hardware address.

13) sname：Optional server host name, null terminated string.

14) file：Boot file name, null terminated string, "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER.

15) options：Optional parameters field. See the options documents (RFC 2132) for a list of defined options. We will introduce some familiar options in the next section.

➢ **DHCP Option**

This section defines a generalized use of the 'options' field for giving information useful to a wide class of machines, operating systems and configurations. Sites with a single DHCP server that is shared among heterogeneous clients may choose to define other, site-specific formats for the use of the 'options' field. Figure 10-14 gives the format of options field.

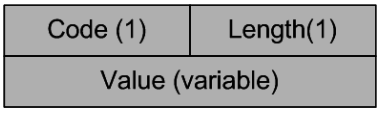


Figure 10-14 DHCP Option

All options begin with a Code octet, which uniquely identifies the option followed by the length octet. The value of the length octet does not include the Code and Length octets. The common options are illustrated as below.

1) option 1：Subnet Mask option. The subnet mask option is option1 which identifies the assigned IP address with network, and its length is 4 octets.

2) option 3：Router option. The router option is option 3 which specifies an IP address for routers on the client's subnet.

3) option 6：DNS option. The DNS option is option 6, and it assigns the IP address of domain name server to the client which allows the client can use the web service in the internet.

4) option 12：Host Name option. The option12 is used to specify the name of the client, which may be requested by the DHCP server for authentication.

5) option 50：Requested IP Address option. The option 50 is used in a DHCP-REQUEST message to allow the client to request the particular IP address.

6) option 51：Lease Time option. In DHCP-OFFER and DHCP-ACK message, the DHCP server uses this option to specify the lease time in which the clients can use the IP address legally.

7) option 53：Message Type option. This option is used to convey the type of the DHCP message. Legal values for this option show in Table 10-2:

Value	Message Type
1	DHCP-DISCOVER
2	DHCP-OFFER
3	DHCP-REQUEST
4	DHCP-DECLINE
5	DHCP-ACK
6	DHCP-NAK
7	DHCP-RELEASE
8	DHCP-INFORM

Table 10-2 Option 53

8) option 54：Server Identifier option. DHCP servers include option 54 in the DHCP-OFFER message in order to allow the client to distinguish between lease offers. DHCP clients use the option in a DHCP-REQUEST message to indicate which lease offers is being accepted.

9) option 55：Parameter Request List option. This option is used by a DHCP client to request values for specified configuration parameters.

10) option 61：Client hardware address.

11) option 66：TFTP server name option. This option is used to identify a TFTP server.

12) option 67：Boot-file name option. This option is used to identify a boot-file.

13) option 150：TFTP server address option. This option is used to specify the address of the TFTP server which assigns the boot-file to the client.

For particulars of DHCP option, please refer to RFC 2132. In the next section, DHCP Server and DHCP Relay function on this switch will be introduced in detail.

➢ **Application Environment of DHCP Server**

DHCP Server assigns IP address to the client efficiently in the following environment.

1) More and more device proliferates in the network, and it is a hard work to configure the IP parameter for every device manually.
2) There are not enough network resources to assign to every device exclusively.
3) Only a little device need static IP address to connect the network.

➢ **Details of DHCP Server**

A typical application of the switch working at DHCP Server function is shown below. It can be altered to meet the network requirement.

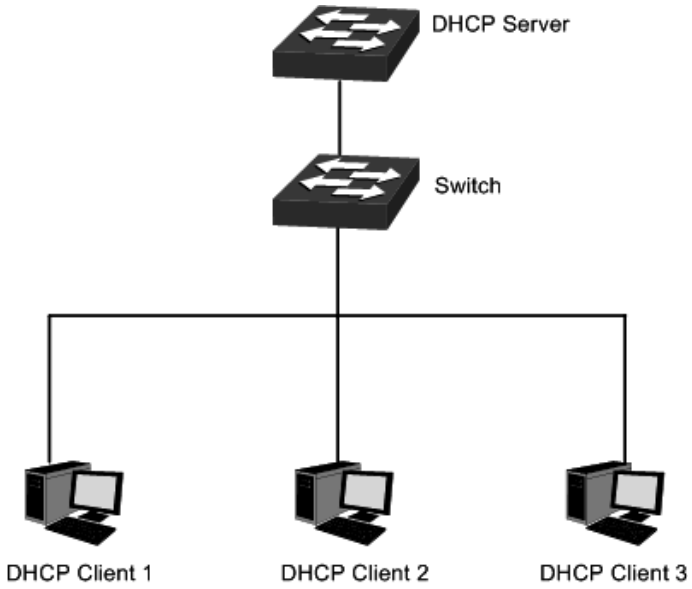


Figure 10-15 DHCP Server Application

To guarantee the process of assigning IP address fluency and in safety, and to keep the network run steadily, the DHCP Server function on the switch performs the following tasks.

- Create different IP pool for every VLAN. The device in different VLAN can get the IP address in different subnet.
- When receiving a DHCP-DISCOVER packet from the client, the switch judges the VLAN which the ingress port belong to, and chooses the IP in the same subnet with the VLAN interface to assign to the client.
- With a DHCP Relay running between the client and the server, when receiving a DHCP-DISCOVER packet transmitting from the Relay, the switch will choose the IP from the IP pool in the same subnet with the Relay's IP to assign to the client. If the IP pool is not configured on the switch or the configured IP pool doesn't match the Relay's network segment, the client may not get network parameters successfully.
- The switch can detect the IP address automatically before assigning it to avoid conflict.

➢ **IP Detection**

To avoid IP conflict, the switch will detect the IP address to be assigned in LAN through Ping test.

The DHCP server will send the Ping test packet with the destination IP being the IP address to be assigned. If the server receives the Reply packet from the destination host in the ping time,

it means that the IP address has been used, and the server will choose another IP as destination IP to test again. The server will assign the IP address if the server not receives the Reply packet in the Ping time.

- **Policy of IP Assignment**

The switch chooses the IP assigned to clients based on the rules shown as follows.

1) First, the server will choose the IP which has been bound to the client manually.
2) Then, the server will assign the IP which has been assigned to the client once.
3) For the next, the server will assign the IP which is specified in the DHCP-DISCOVER packet from the client.
4) At last, the server will choose the first IP from the IP pool which has not been assigned.

- **Tips for Configure DHCP Server Function**

1) Configure the Excluded IP address which cannot be assigned by the switch, e.g. web server's IP, broadcast IP of subnet and gateway's IP.
2) Specify IP address for specific clients, and then the switch will supply these IP address to them only forever.
3) Configure the IP pool in which the IP address can be assigned to the clients.

The DHCP Server, allowing the clients in all VLANs to get the IP address from the server automatically, is implemented on the **DHCP Server**, **Pool Setting**, **Manual Binding**, **Binding Table** and **Packet Statistics** pages.

10.4.1 DHCP Server

This page allows you to enable the DHCP Server function, configure the Excluded IP Address which cannot be assigned by the switch in every network.

Choose the menu **Routing→DHCP Server→DHCP Server** to load the following page.

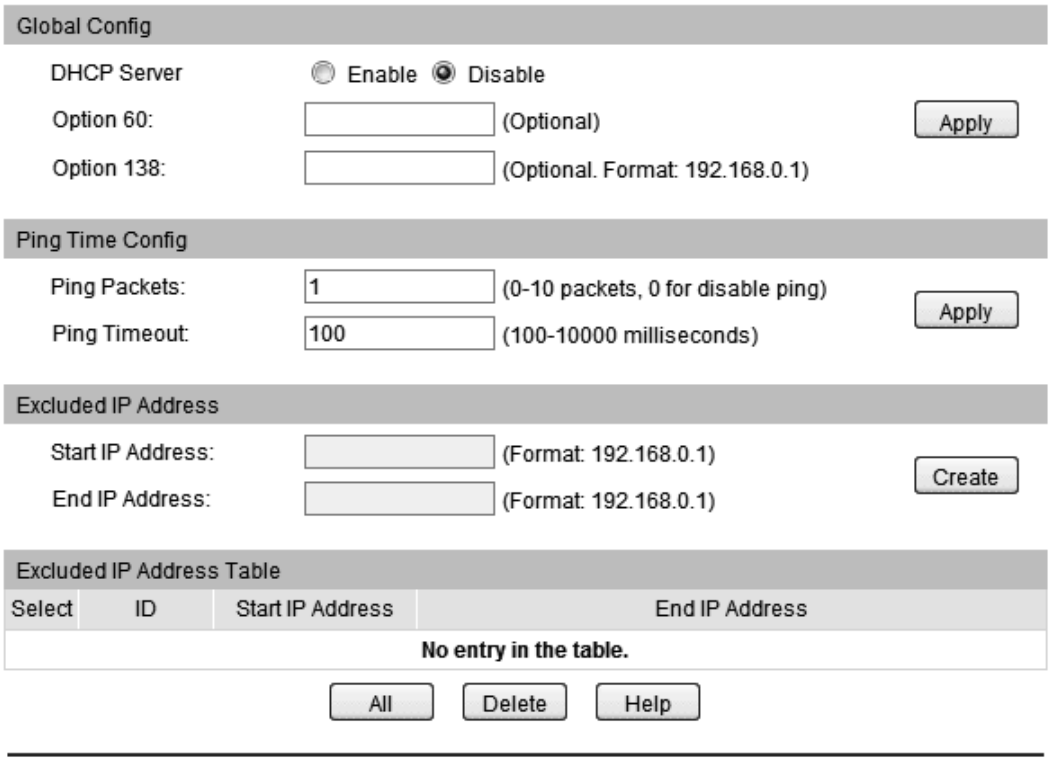


Figure10-16 DHCP Server

The following entries are displayed on this screen:

- **Global Config**

  DHCP Server: Enable/Disable the switch as a DHCP server.

  Option 60: Configure DHCP option 60. If this option is configured, DHCP server will response packets containing this option if the client running CAPWAP protocol requests this option.

  Option 138: Configure DHCP option 138. If this option is configured, DHCP server will response packets containing this option if the client running CAPWAP protocol request this option.

- **Ping Time Config**

  Ping Packets: The number of packets to be sent.

  Ping Timeout: The time it takes to determine the specific IP not exist.

- **Excluded IP Address**

Configure the Excluded IP Address which cannot be assigned by the switch.

Start IP Address: The first one of the IP addresses that should not be assigned.

End IP Address: The last one of the IP addresses that should not be assigned.

➢ **Excluded IP Address Table**

Select: Select the entry to delete the Excluded IP Address pool.

ID: Displays the corresponding ID of the Excluded IP Address pool.

Start IP Address: Displays the start IP Address of the Excluded IP Address pool.

End IP Address: Displays the last IP Address of the Excluded IP Address pool.

10.4.2 Pool Setting

This page shows you how to configure the IP pool in which the IP address can be assigned to the clients in the network.

Choose the menu **Routing→DHCP Server→Pool Setting** to load the following page.

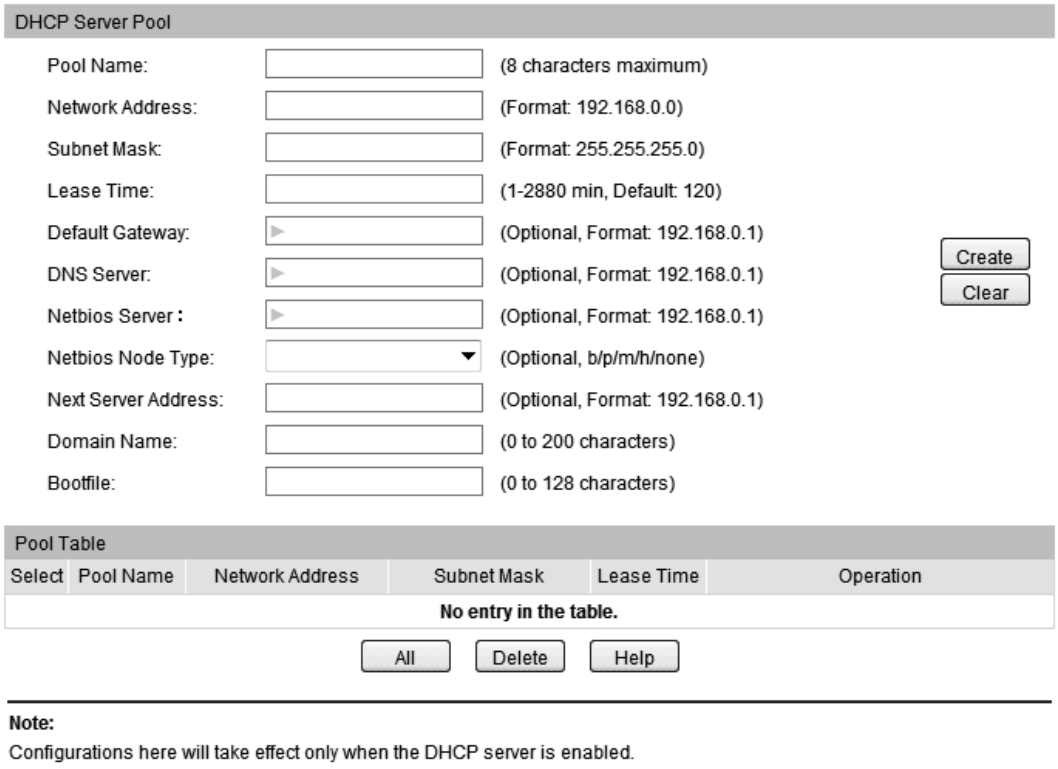


Figure 10-17 Pool Setting

The following entries are displayed on this screen:

➢ **DHCP Server Pool**

Pool Name: Enter the name of the pool.

Network Address: Specify the network number of the IP addresses in the pool.

Subnet Mask: Specify the corresponding subnet mask of the IP address in the pool.

Lease Time: Specify the lease time of IP addresses in the pool.

Default Gateway: Specify the IP address of the default gateway for a client.

DNS Server: Specify the IP address of the DNS server for a client.

Netbios Server: Specify the IP address of the Netbios server.

Netbios Node Type: Specify the node type of the Netbios server.

Next Server Address: Specify the next DHCP server's ip address during the DHCP boot process.

Domain Name: Specify the domain name of the DHCP client.

Bootfile: Specify the boot file name of the DHCP client.

- **Pool Table**

Select: Select the entry to delete the IP pool.

Pool Name: Displays the name of the IP Pool.

Network Address: Displays the network address of the IP Pool.

Subnet Mask: Displays the subnet mask of the IP Pool.

Lease Time: Displays the lease time of the IP Pool.

Operation: Allows you to view or modify the information of the corresponding IP Pool.

- Edit: Click to modify the settings of the Pool.
- Detail: Click to get the information of the Pool.

10.4.3 Manual Binding

In this page, you can specify the IP address for specific clients, and then the switch will supply these specified parameters to them only forever.

Choose the menu **Routing→DHCP Server→Manual Binding** to load the following page.

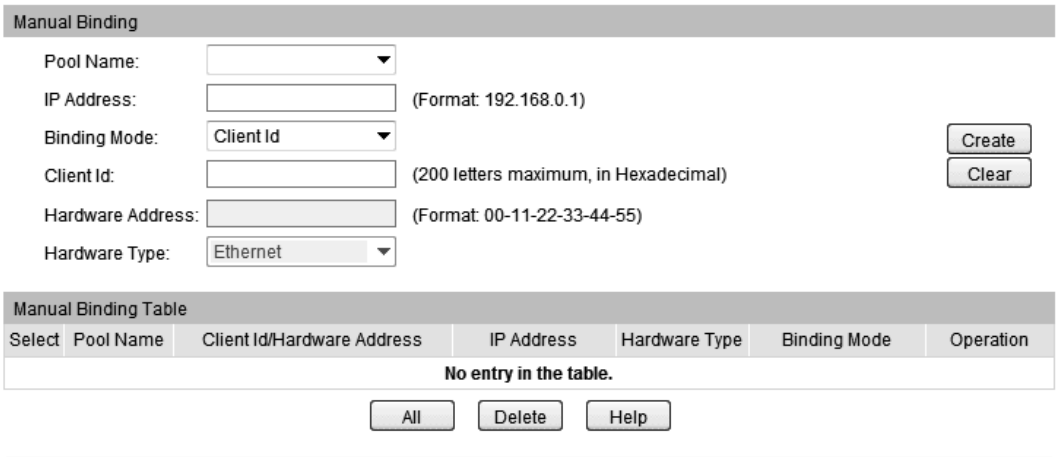


Figure 10-18 Manual Binding

The following entries are displayed on this screen:

- **Manual Binding**

Pool Name:	Select the IP Pool containing the IP address to be bound.
IP Address:	Specify the IP address to be bound.
Binding Mode:	Select the binding mode of the manual binding.
Client ID:	Specify the identifier of the client.
Hardware Address:	Specify the hardware address to be bound.
Hardware Type:	Select the hardware protocol of the client.

- **Manual Binding Table**

Displays the list of the configured binding entries of IP addresses and hardware addresses.

10.4.4 Binding Table

In this page, you can view the information about the clients attached to the Server.

Choose the menu **Routing→DHCP Server→Binding Table** to load the following page.

Figure 10-19 DHCP Server Binding Table

- **DHCP Server Binding Table**

ID:	Displays the ID of the client.
IP Address:	Displays the IP address that the Switch has allocated to the client.
Client ID / Hardware Address:	Displays the MAC address of the client.
Type:	Displays the type of this binding entry.
Lease Time Left(s):	Displays the lease time of the client left.

Click **Delete** to delete the selected entry.

10.4.5 Packet Statistics

In this page, you can view the DHCP packets the switch received or sent.

Choose the menu **Routing→DHCP Server→Packet Statistics** to load the following page.

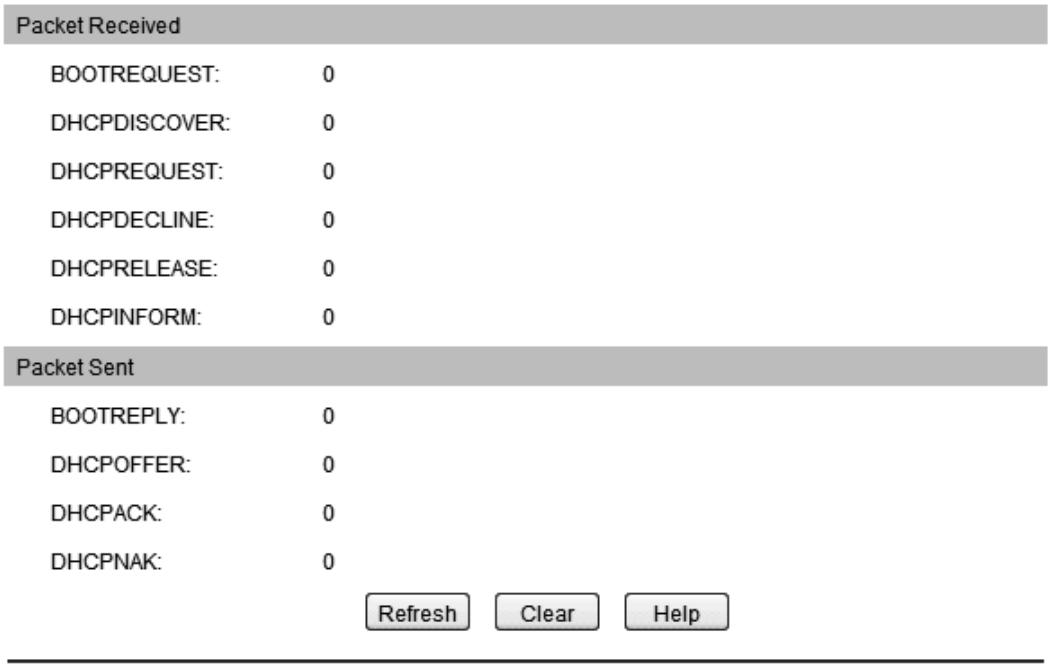


Figure10-20 Statistics

The following entries are displayed on this screen:

- **Packets Received**

  BOOTREQUEST: Displays the Bootp Request packet received.

  DHCPDISCOVER: Displays the Discover packet received.

  DHCPREQUEST: Displays the Request packet received.

  DHCPDECLINE: Displays the Decline packet received.

  DHCPRELEASE: Displays the Release packet received.

  DHCPINFORM: Displays the Inform packet received.

- **Packets Sent**

  BOOTREPLY: Displays the Bootp Reply packet sent.

  DHCPOFFER: Displays the Offer packet sent.

  DHCPACK: Displays the Ack packet sent.

  DHCPNAK: Displays the Nak packet sent.

- **Configuration Procedure:**

Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected device.

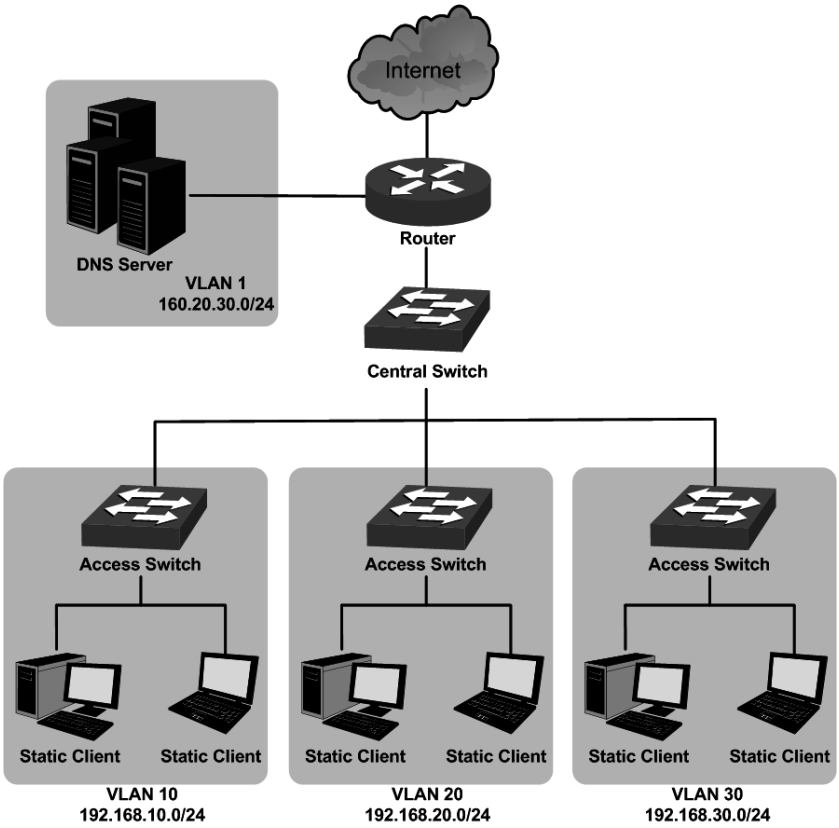
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its member ports.
3	Create VLAN interface.	Required. On the **Routing→Static Routing→Static Routing Config** page, create the interface IP address of the VLAN.
4	Enable DHCP Server.	Required. On the **Routing→DHCP Server→DHCP Server** page, enable the DHCP Server function.
5	Configure Excluded IP Address.	Optional. On the **Routing→DHCP Server→DHCP Server** page, configure the Excluded IP Address which cannot be assigned by the switch.
6	Configure IP Pool.	Required. On the **Routing→DHCP Server→Pool Setting** page, configure the parameters of IP Pool, including Mask, lease time, gateway and DNS address.
7	Bind IP Manually	Optional. On the **Routing→DHCP Server→Manual Binding** page, you can specify the IP address for specific clients.

10.4.6 Application Example for DHCP Server and Relay

➢ **Network Requirements**

- Every building in the campus belongs to separate VLANs with different network segments.
- The access points in each building are divided into two parts. One part is the fixed computers with static IP addresses in the teachers' offices; the other is the classroom, in which most clients are laptops with dynamic IP addresses obtained from the DHCP server.
- DNS Server is in VLAN 1and its IP address is 160.20.30.2.

➢ **Network Diagram**



Use the central switch and enable its DHCP server function to allocate IP addresses to clients in the network. Enable the DHCP relay function on each access switch in VLAN 10, 20 and 30. For details about DHCP relay, please refer to 10.5 DHCP Relay.

➢ **Configuration Procedure**

- Configure Central Switch

Step	Operation	Note
1	Create VLAN	Required. On page **VLAN→802.1Q VLAN→VLAN Config**, create VLAN10, VLAN20 and VLAN30, and configure their ports.
2	Create VLAN interface	Required. On page **Routing→Interface→Interface Config**, configure VLAN interface 192.168.10.1/24 for VLAN10, 192.168.20.1/24 for VLAN20, and 192.168.30.1 for VLAN30.
3	Enable DHCP Server	Required. On page **Routing→DHCP Server→DHCP Server**, enable DHCP Server function under the Global Config.
4	Configure the IP address pool	Required. On page **Routing→DHCP Server→Pool Setting**, configure IP address pool parameters for each VLAN interface. Take VLAN10 as an example, configure its Network Address as 192.168.10.0, Subnet Mask as 255.255.255.0, Default gateway as 192.168.10.1 (the IP address of the VLAN interface), DNS Server as 160.20.30.2, and customize the Pool Name and Lease Time.

Step	Operation	Note
5	Configure the reserved addresses	Required. On page **Routing→DHCP Server→DHCP Server**, under the Excluded IP Address, configure reserved IP addresses for the fixed computers in each VLAN.
6	Manually binding IP addresses	Optional. On page **Routing→ DHCP Server→Manual Binding**, bind specified ip addresses to the specific clients.

- Configure Access Switch

Step	Operation	Note
•	Enable DHCP Relay.	Required. On the **Routing→DHCP Server→Global Config** page, **enable** the DHCP Server function, and the DHCP Relay function will be enabled at the same time.
•	Configure Option 82 support.	Optional. On the **Routing→DHCP Relay→Global Config** page, configure the Option 82 parameters.
•	Configure DHCP Server.	Required. On the **Routing→DHCP Relay→DHCP Server** page, specify the DHCP Server with the IP address of the central switch.

10.5 DHCP Relay

➢ **Application Environment of DHCP Relay**

In DHCP model, DHCP clients broadcast its DHCP request, so the DHCP sever and clients must be on the same subnet, which require the DHCP server is available in every subnet. It is costly to build so much DHCP Server. DHCP relay agent solves the problem. Via a relay agent, DHCP clients request an IP address from the DHCP server in another subnet, and DHCP clients in different subnets can share the same DHCP server in the internet.

➢ **Details of DHCP Relay**

A typical application of the switch working at DHCP Relay function is shown below. It can be altered to meet the network requirement.

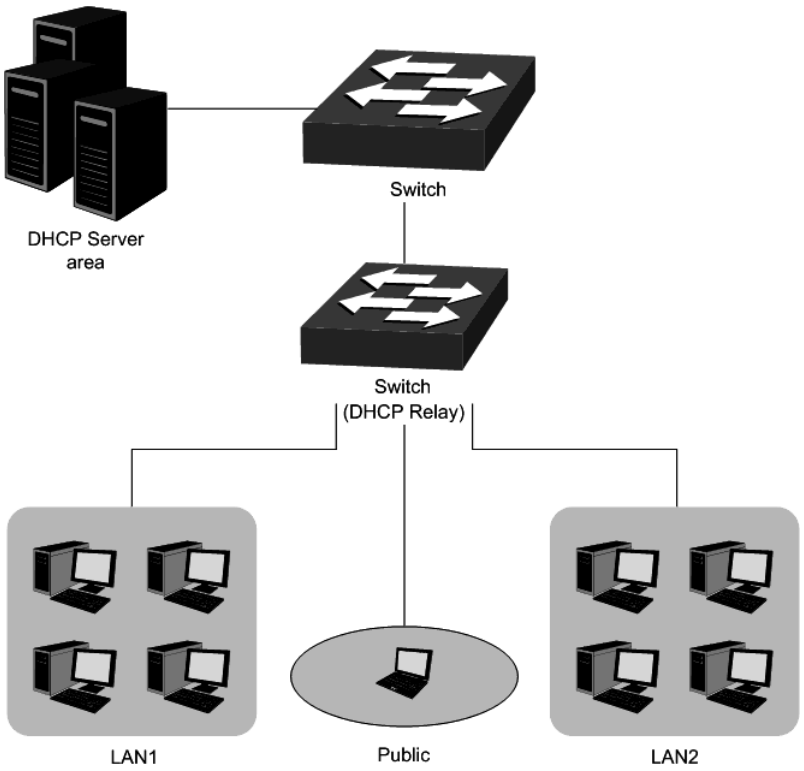


Figure 10-21 DHCP Relay Application

To allow all clients in different VLAN request IP address from one server successfully, the DHCP Relay function can transmit the DHCP packet between clients and server in different VLANs, and all clients in different VLANs can share one DHCP Server.

- When receiving DHCP-DISCOVER and DHCP-REQUEST packets, the switch will fill the giaddr field with the interface IP of the receiving port, optionally insert the option 82 information, and then forward the packet to the server.
- When receiving DHCP-OFFER and DHCP-ACP packets from the server, the switch will delete the option 82 information and forward the packet to the interface which receives the request.

The process will be shown as follows.

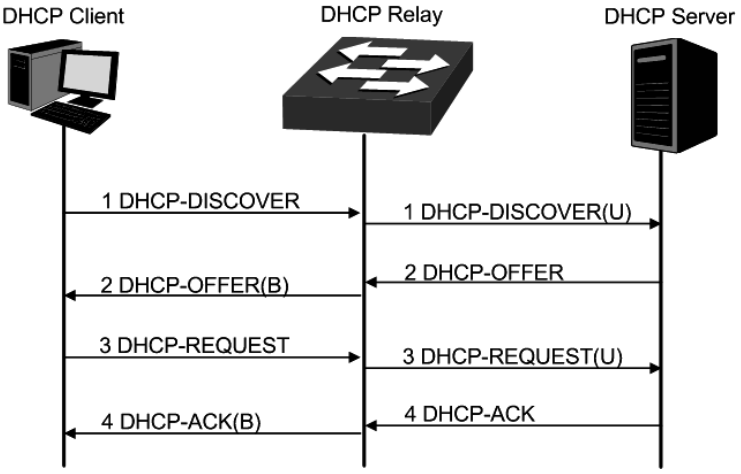


Figure 10-22 DHCP Relay Process

➢ **DHCP Relay Configuration**

1) Configure the Option 82 parameters to record the information of the clients. You are suggested to configure the option82 on the nearest Relay of the client.
2) Specify the DHCP Server which assigns IP addresses actually.

➢ **Option 82**

On this switch, Option 82 is used to record the location of the DHCP Client, the ethernet port and the VLAN, etc. Upon receiving the DHCP-REQUEST packet, the switch adds the Option 82 field to the packet and then transmits the packet to DHCP Server. The Server can be acquainted with the location of the DHCP Client via Option 82, so as to locate the DHCP Client, and assign the distribution policy of IP addresses and the other parameters for fulfilling the security control and account management of the client.

Option 82 can contain 255 sub-options at most. If Option 82 is defined, at least one sub-option should be defined. This Switch supports two sub-options, Circuit ID and Remote ID. Since there is no universal standard about the content of Option 82, different manufacturers define the sub-options of Option 82 to their need. For this Switch, the sub-options are defined as follows:

The Circuit ID is defined to be the number and VLAN of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of DHCP Relay device which receives the DHCP Request packets from DHCP Clients. Furthermore these two parameters also can be manually configured.

The format of Option 82 defined on the switch by default is given in the following figure. The numbers in parentheses indicate the size of each field in octets. By default, sub-option1 is Circuit ID option recording the VLAN and ethernet port information, while sub-option2 is Remote ID option recording the MAC address information of the client. You can define the sub-options manually.

Figure10-23 Option 82

Note:

The option 82 parameters configured on the switch should base on and meet the requirement of the network.

The DHCP Relay, allowing the clients to get the IP address from the server in another subnet, is implemented on the **DHCP Relay** page.

10.5.1 Global Config

This page allows you to enable the DHCP Relay function.

Choose the menu **Routing→DHCP Relay→Global Config** to load the following page.

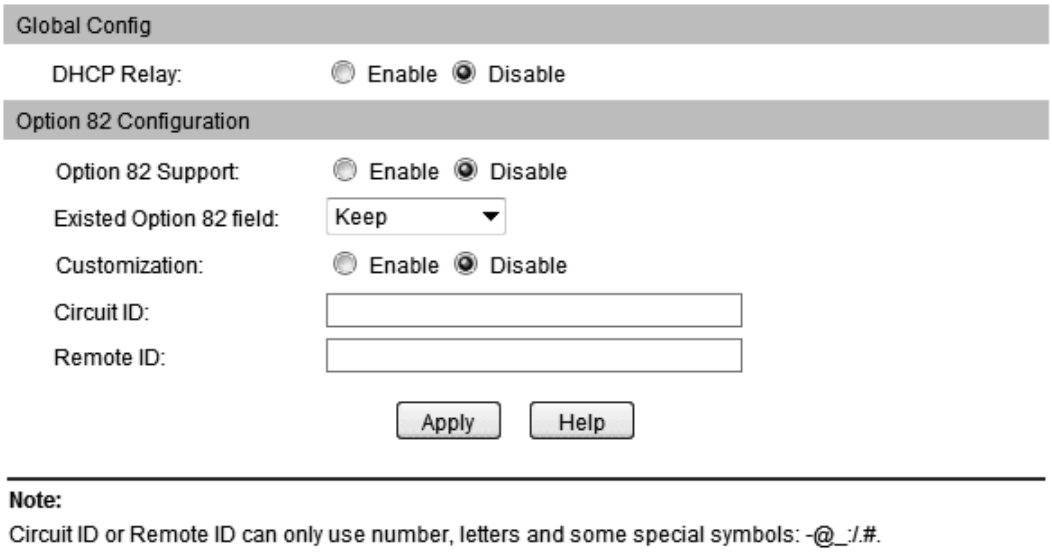


Figure 10-24 Global Config

The following entries are displayed on this screen:

- **Global Config**

DHCP Relay: Enable the DHCP relay feature.

- **Option 82 configuration**

Configure the Option 82 which cannot be assigned by the switch.

Option 82 Support: Enable or disable the Option 82 feature.

Existed Option 82 Field: Select the operation for the existed Option 82 field of the DHCP request packets from the Host.

- Keep: Indicates to keep the Option 82 field of the packets.
- Replace: Indicates to replace the Option 82 field of the packets with the switch defined one.
- Drop: Indicates to discard the packets including the Option 82 field.

Customization: Enable or disable the switch to define the Option 82 field.

Circuit ID: Enter the sub-option Circuit ID for the customized Option 82 field.

Remote ID: Enter the sub-option Remote ID for the customized Option 82 field.

10.5.2 DHCP Server

This page enables you to configure DHCP Servers on the specified interface.

Choose the menu **Routing→DHCP Relay→DHCP Server** to load the following page.

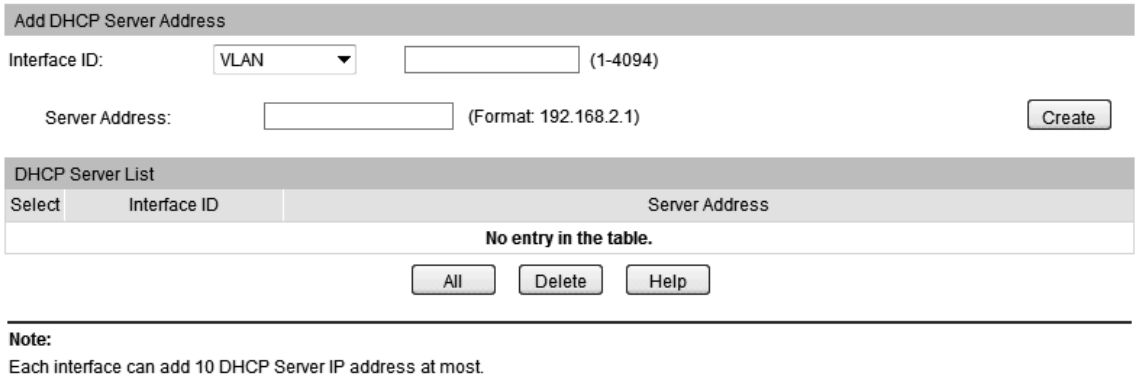


Figure 10-25 DHCP Server

The following entries are displayed on this screen:

- **Add DHCP Server Address**

  Interface ID: Select the interface type and enter the interface ID.

  Server Address: Enter the DHCP server IP address.

- **DHCP Server List**

  Select: Select the desire DHCP server item.

  Interface ID: Displays the interface ID.

  Server Address: Displays the DHCP server address.

Configuration Procedure:

Step	Operation	Description
1	Enable DHCP Relay.	Required. On the **Routing→DHCP Relay→Global Config** page, **enable** the DHCP Relay function.
2	Configure Option 82 support.	Optional. On the **Routing→DHCP Relay→Global Config** page, configure the Option 82 parameters.
3	Configure DHCP Server.	Required. On the **Routing→DHCP Relay→DHCP Server** page, specify the DHCP Server with IP address.

10.6 ARP

Address Resolution Protocol (ARP) records the mapping relationship between IP addresses and MAC addresses in the ARP table. You can also define a static ARP cache entry on the page Static ARP.

10.6.1 ARP Table

Choose the menu **Routing→ARP→ARP Table** to load the following page.

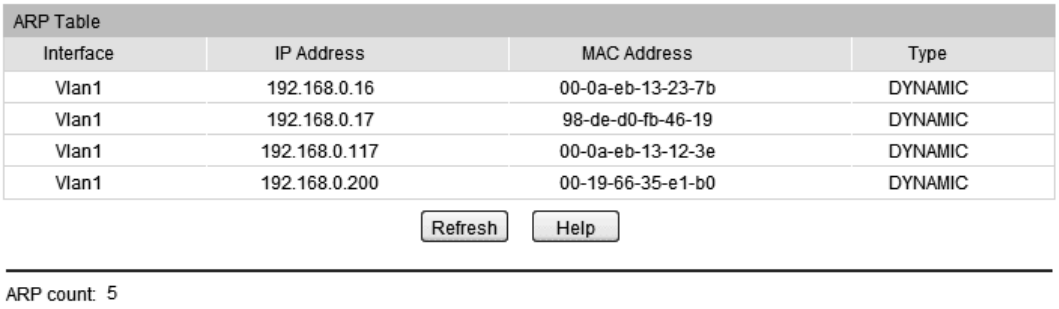


Figure 10-26 ARP Table

The following entries are displayed on this screen:

- **ARP Table**

Interface: Displays the network interface of ARP entry.

IP Address: Enter the IP address of the ARP entry.

MAC Address: Displays the MAC address of ARP entry.

Type: Displays the type of ARP entry, e.g. Static, Dynamic.

10.6.2 Static ARP

You can configure the static ARP entry on this page.

Choose the menu **Routing→ARP→Static ARP** to load the following page.

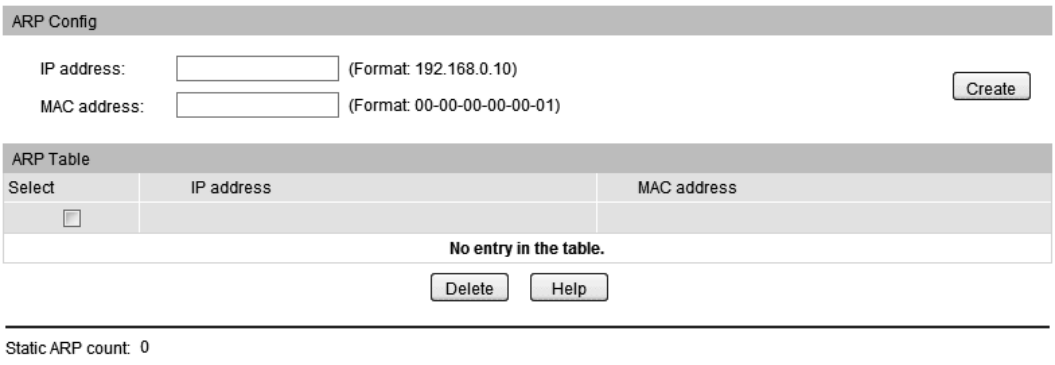


Figure 10-27 Static ARP

- **ARP Config**

IP Address: Configure the IP address of the ARP entry.

MAC address: Configure the MAC address of the ARP entry.

- **ARP Table**

Here you can view or delete the current static ARP entries.

Return to CONTENTS

Chapter 11 QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

➢ **QoS**

This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function.

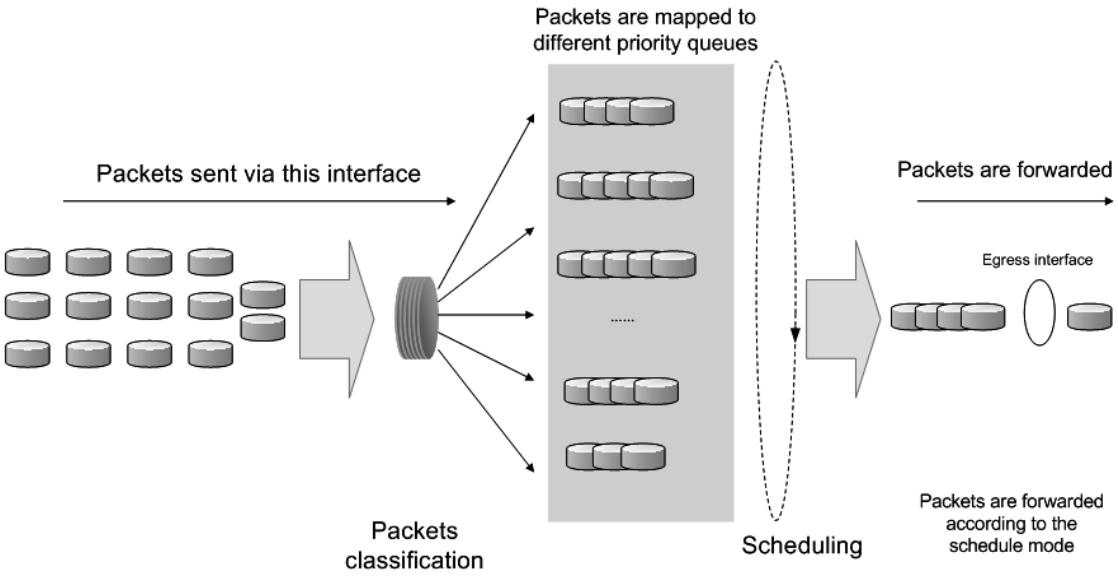


Figure 11-1 QoS function

- Traffic classification: Identifies packets conforming to certain characters according to certain rules.
- Map: The user can map the ingress packets to different priority queues based on the priority modes. This switch implements three priority modes based on port, on 802.1P and on DSCP.
- Queue scheduling algorithm: When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch supports four schedule modes: SP, WRR, SP+WRR and Equ.

➢ **Priority Mode**

This switch implements three priority modes based on port, on 802.1P and on DSCP. By default, the priority mode based on port is enabled and the other two modes are optional.

1. Port Priority

Port priority is just a property of the port. After port priority is configured, the data stream will be mapped to the egress queues according to the CoS of the port and the mapping relationship between CoS and queues.

2. 802.1P Priority

Figure 11-2 802.1Q frame

As shown in the figure above, each 802.1Q Tag has a Pri field, comprising 3 bits. The 3-bit priority field is 802.1p priority in the range of 0 to 7. 802.1P priority determines the priority of the packets based on the Pri value. On the Web management page of the switch, you can configure different priority tags mapping to the corresponding priority levels, and then the switch determine which packet is sent preferentially when forwarding packets. The switch processes untagged packets based on the default priority mode.

3. DSCP Priority

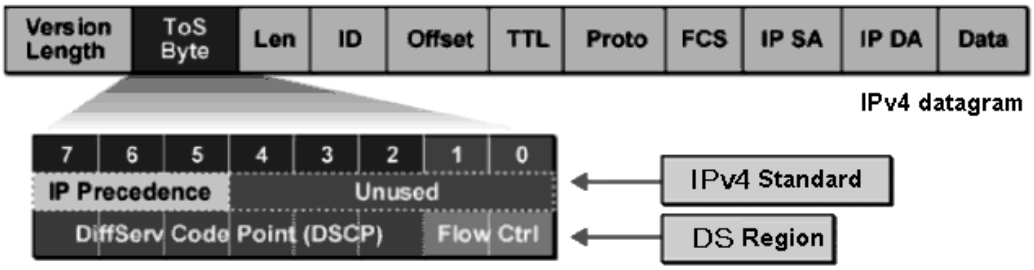


Figure 11-3 IP datagram

As shown in the figure above, the ToS (Type of Service) in an IP header contains 8 bits. The first three bits indicate IP precedence in the range of 0 to 7. RFC2474 re-defines the ToS field in the IP packet header, which is called the DS field. The first six bits (bit 0-bit 5) of the DS field indicate DSCP precedence in the range of 0 to 63. The last 2 bits (bit 6 and bit 7) are reserved. On the Web management page, you can configure different DS field mapping to the corresponding priority levels. Non-IP datagram with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode; the untagged non-IP datagram are mapped based on port priority mode.

- **Schedule Mode**

When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch implements eight scheduling queues, TC0, TC1, TC2, TC3, TC4, TC5, TC6 and TC7. TC0 has the lowest priority while TC7 has the highest priority. The switch provides four schedule modes: SP, WRR, SP+WRR and Equ.

1. SP-Mode: Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue

with higher priority is empty. The switch has eight egress queues labeled as TC0, TC1, TC2, TC3, TC4, TC5, TC6 and TC7. In SP mode, their priorities increase in order. TC7 has the highest priority. The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be "starved to death" because they are not served.

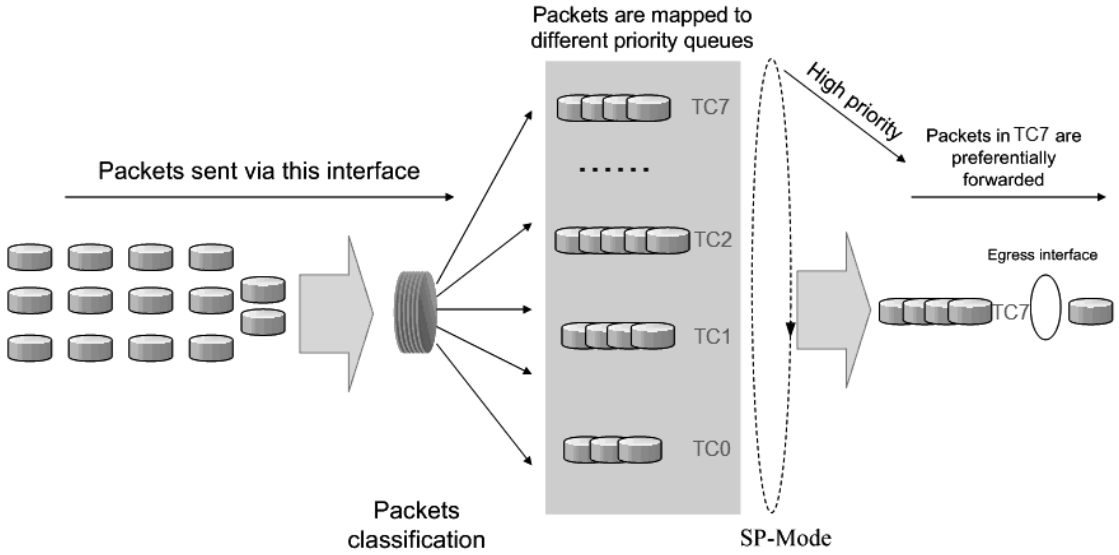


Figure 11-4 SP-Mode

2. WRR-Mode: Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. The weight value indicates the occupied proportion of the resource. WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time. In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of. The default weight value ratio of TC0, TC1, TC2, TC3, TC4, TC5, TC6 and TC7 is 1:2:4:8:16:32:64:127.

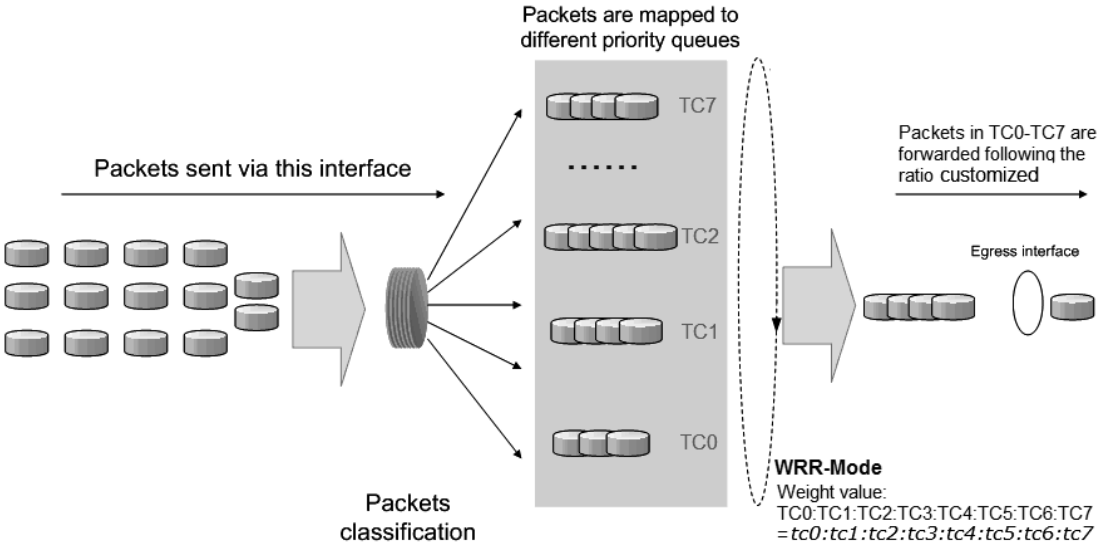


Figure 11-5 WRR-Mode

3. SP+WRR Mode: Strict-Priority + Weight Round Robin Mode. In this mode, the switch provides two scheduling groups, SP group and WRR group. Queues in SP group and WRR group are scheduled strictly based on Strict-Priority mode while the queues inside WRR group follow the WRR mode. In SP + WRR mode, TC7 and the queue with its weight value set as 0 are in the SP group; other queues, with none-zero weight value, belong to the WRR group and the weight value can be customized, ranging from 0 to 127. In this way, when scheduling queues, the switch allows TC7 and zero-weight-value queue to occupy the whole bandwidth following the SP mode and the queues in the WRR group will take up the bandwidth according to their ratio.
4. Equ-Mode: Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1:1:1:1:1.

Note:

In SP + WRR mode, TC7 and the queue with its weight value set as 0 are in the SP group.

The QoS module is mainly for traffic control and priority configuration, including three submenus: **DiffServ**, **Bandwidth Control** and **Voice VLAN**.

11.1 DiffServ

This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function.

This switch implements three priority modes based on port, on 802.1P and on DSCP, and supports four queue scheduling algorithms. The port priorities are labeled as CoS0, CoS1... CoS7.

The DiffServ function can be implemented on **Port Priority**, **Schedule Mode, 802.1P Priority** and **DSCP Priority** pages.

11.1.1 Port Priority

On this page you can configure the port priority.

Choose the menu **QoS→DiffServ→Port Priority** to load the following page.

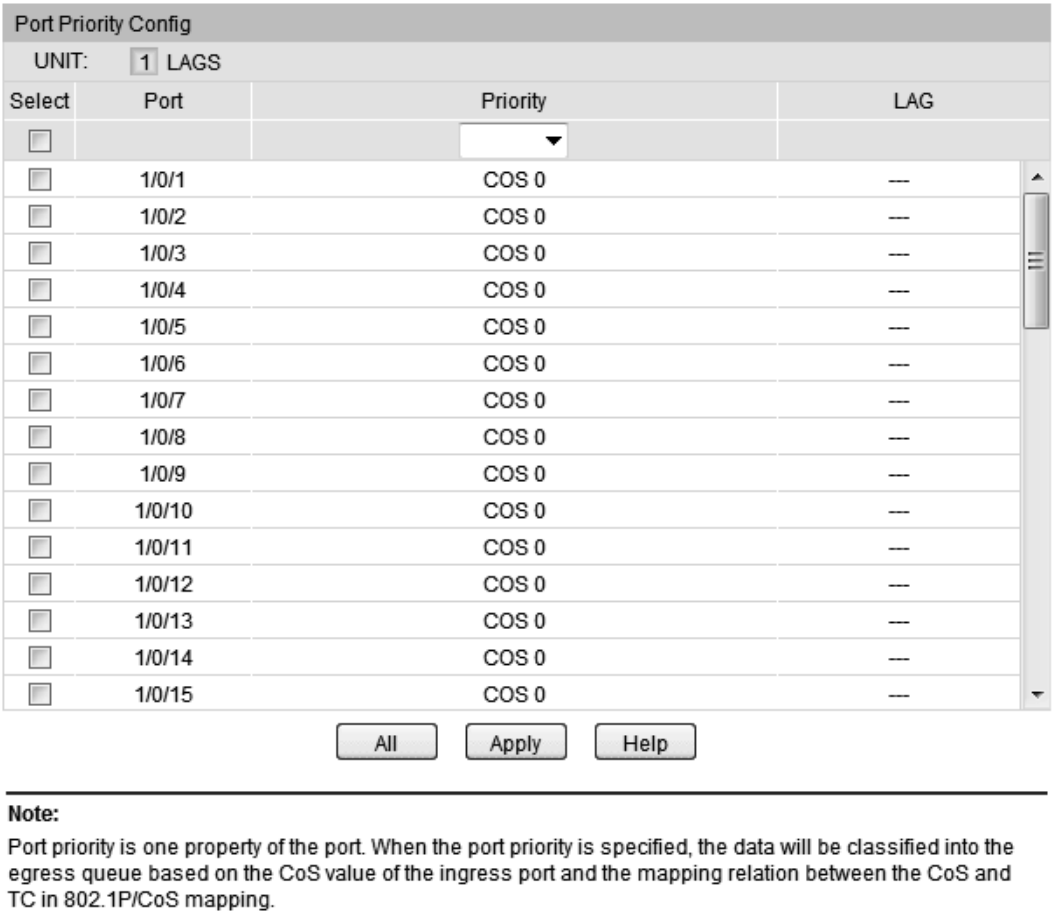


Figure 11-6 Port Priority Config

The following entries are displayed on this screen:

- **Port Priority Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired port to configure its priority. It is multi-optional.

Port: Displays the physical port number of the switch.

Priority: Specify the priority for the port.

LAG: Displays the LAG number which the port belongs to.

Configuration Procedure:

Step	Operation	Description
1	Select the port priority	Required. On **QoS→DiffServ→Port Priority** page, configure the port priority.
2	Configure the mapping relation between the 802.1P priority and TC	Required. On **QoS→DiffServ→802.1P Priority** page, configure the mapping relation between the 802.1P priority and TC.
3	Select a schedule mode	Required. On **QoS→DiffServ→Schedule Mode** page,

		select a schedule mode.

11.1.2 Schedule Mode

On this page you can select a schedule mode for the switch. When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1… TC7.

Choose the menu **QoS→DiffServ→Schedule Mode** to load the following page.

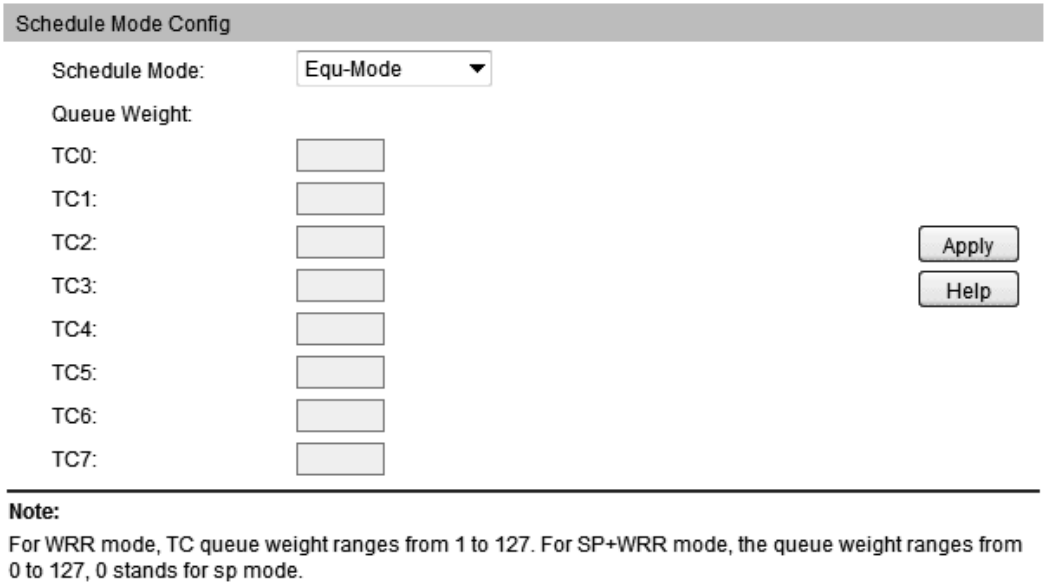


Figure 11-7 Schedule Mode

The following entries are displayed on this screen:

- **Schedule Mode Config**

Schedule Mode: Select a schedule mode.

- **SP-Mode**：Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.
- **WRR-Mode:** Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. The weight values of TC0-TC7 can be customized and their default values are 1:2:4:8:16:32:64:127 respectively.
- **SP+WRR-Mode:** Strict-Priority + Weight Round Robin Mode. In this mode, the switch provides two scheduling groups, SP group and WRR group. SP group is processed prior to WRR group. Queues in SP group are scheduled strictly based on Strict-Priority mode while the queues inside WRR group follow the WRR mode. In SP+WRR mode, TC7 and the queue with its weight value set as 0 are in the SP group; other queues, with none-zero weight value, belong to the WRR group and the weight value can be customized. The default weight values of TC0-TC6 are 1:2:4:8:16:32:64 respectively, while the value of TC7 is 0 and non-configurable.
- **Equ-Mode:** Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1:1:1:1:1.

Queue Weight: Input the queue weight of the 8 TC queues. Configuration is not available when Equ-Mode or SP-Mode is selected as the schedule mode.

11.1.3 802.1P Priority

On this page you can configure the mapping relation between the 802.1P priority tag-id/CoS-id and the TC-id.

802.1P gives the Pri field in 802.1Q tag a recommended definition. This field, ranging from 0-7, is used to divide packets into 8 priorities. 802.1P Priority is enabled by default, so the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode but the untagged packets are mapped based on port priority mode. With the same value, the 802.1P priority tag and the CoS will be mapped to the same TC.

Choose the menu **QoS→DiffServ→802.1P Priority** to load the following page.

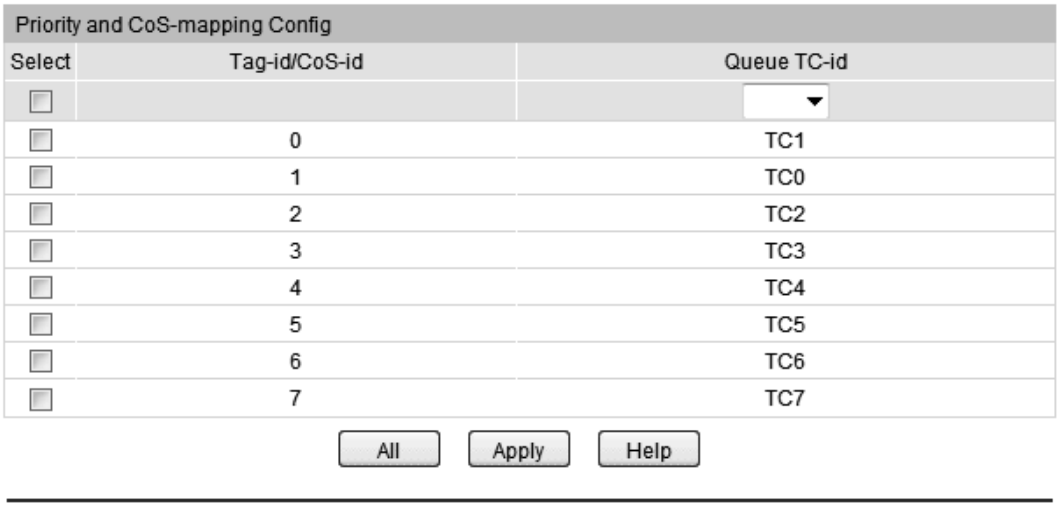


Figure 11-8 802.1P Priority

The following entries are displayed on this screen:

- **Priority and CoS-mapping Config**

Select: Select the desired 802.1P tag-id/cos-id for 802.1P priority configuration. It is multi-optional.

Tag-id/CoS-id: Indicates the precedence level defined by IEEE 802.1P and the CoS ID.

Queue TC-id: Indicates the priority level of egress queue the packets with tag and CoS-id are mapped to. The priority levels of egress queue are labeled as TC0, TC1, TC2 ...TC7.

Note:

To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

Configuration Procedure:

Step	Operation	Description
1	Configure the mapping relation between the 802.1P priority Tag/CoS and the TC	Required. On **QoS→DiffServ→802.1P Priority** page, configure the mapping relation between the 802.1P priority Tag/CoS and the TC.
2	Select a schedule mode	Required. On **QoS→DiffServ→Schedule Mode** page, select a schedule mode.

11.1.4 DSCP Priority

On this page you can configure DSCP priority. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP

Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority mode; non-IP datagram with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode if 802.1P Priority mode is enabled; the untagged non-IP datagram are mapped based on port priority mode.

Choose the menu **QoS→DiffServ→DSCP Priority** to load the following page.

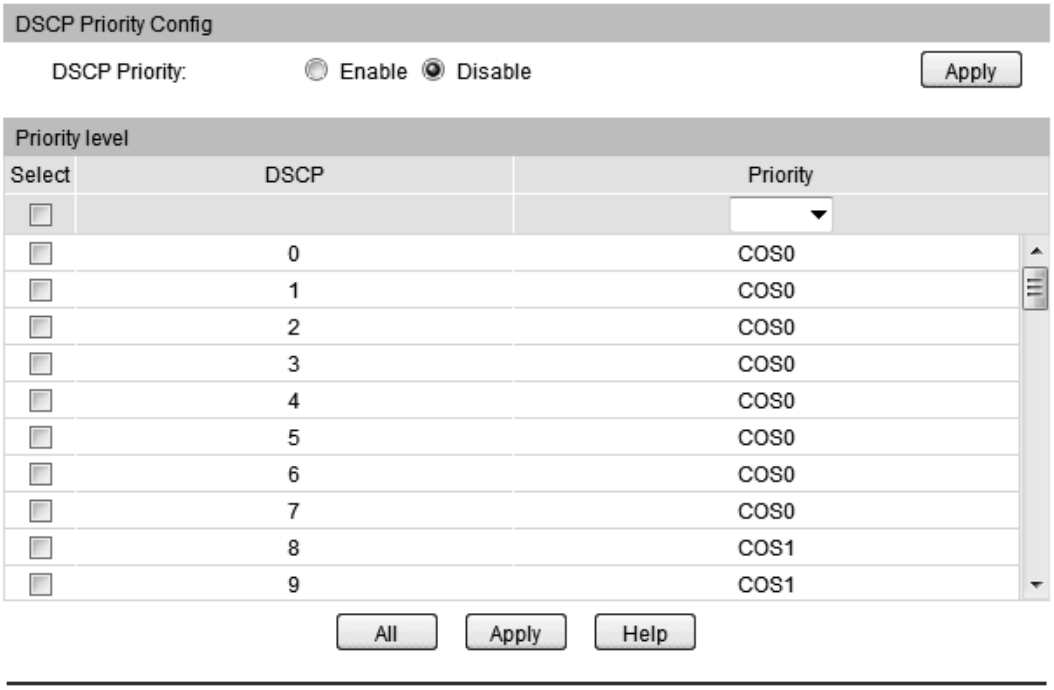


Figure 11-9 DSCP Priority

The following entries are displayed on this screen:

- **DSCP Priority Config**

  DSCP Priority: Select Enable or Disable DSCP Priority.

- **Priority Level**

  Select: Select the desired DSCP value for DSCP priority configuration. It is multi-optional.

  DSCP: Indicates the priority determined by the DS region of IP datagram. It ranges from 0 to 63.

  Priority Level: Indicates the 802.1P priority the packets with tag are mapped to. The priorities are labeled as CoS0 ~ CoS7.

Configuration Procedure:

Step	Operation	Description
1	Configure the mapping relation between the DSCP priority and 802.1P priority	Required. On **QoS→DiffServ→DSCP Priority** page, enable DSCP Priority and configure the mapping relation between the DSCP priority and CoS.

Step	Operation	Description
2	Configure the mapping relation between the CoS and the TC	Required. On **QoS→DiffServ→802.1P Priority** page, configure the mapping relation between the CoS and the TC.
3	Select a schedule mode	Required. On **QoS→DiffServ→Schedule Mode** page, select a schedule mode.

11.2 Bandwidth Control

Bandwidth function, allowing you to control the traffic rate and broadcast flow on each port to ensure network in working order, can be implemented on **Rate Limit** and **Storm Control** pages.

11.2.1 Rate Limit

Rate limit functions to control the ingress/egress traffic rate on each port via configuring the available bandwidth of each port. In this way, the network bandwidth can be reasonably distributed and utilized.

Choose the menu **QoS→Bandwidth Control→Rate Limit** to load the following page.

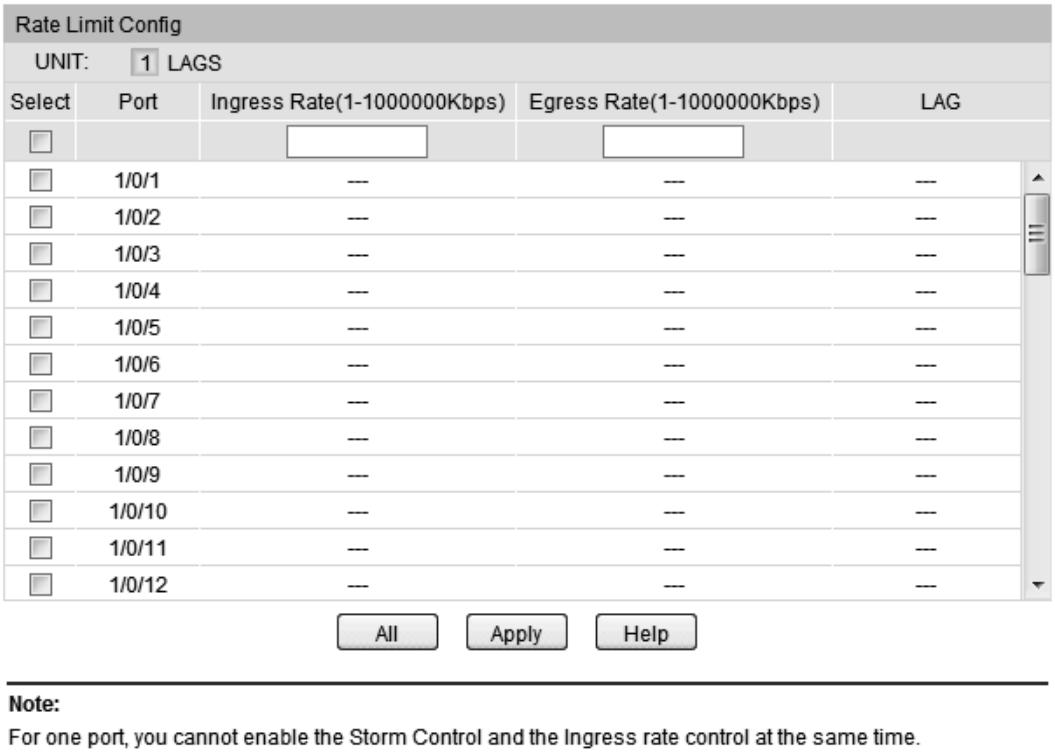


Figure 11-10 Rate Limit

The following entries are displayed on this screen:

- **Rate Limit Config**

  UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select:	Select the desired port for Rate configuration. It is multi-optional.
Port:	Displays the port number of the switch.
Ingress Rate (1-1000000Kbps):	Configure the bandwidth for receiving packets on the port. You can select a rate from the dropdown list or manually set Ingress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Ingress rate.
Egress Rate(1-1000000Kbps):	Configure the bandwidth for sending packets on the port. You can select a rate from the dropdown list or manually set Egress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Egress rate.
LAG:	Displays the LAG number which the port belongs to.

Note:

1. If you enable ingress rate limit feature for the storm control-enabled port, storm control feature will be disabled for this port.
2. When manually set Ingress/Egress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Ingress/Egress rate. For example, if you enter 1000Kbps for egress rate, the system will automatically select 1024Kbps as the real Egress rate.
3. When egress rate limit feature is enabled for one or more ports, you are suggested to disable the flow control on each port to ensure the switch works normally.

11.2.2 Storm Control

Storm Control function allows the switch to filter broadcast, multicast and UL frame in the network. If the transmission rate of the three kind packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

Choose the menu **QoS→Bandwidth Control→Storm Control** to load the following page.

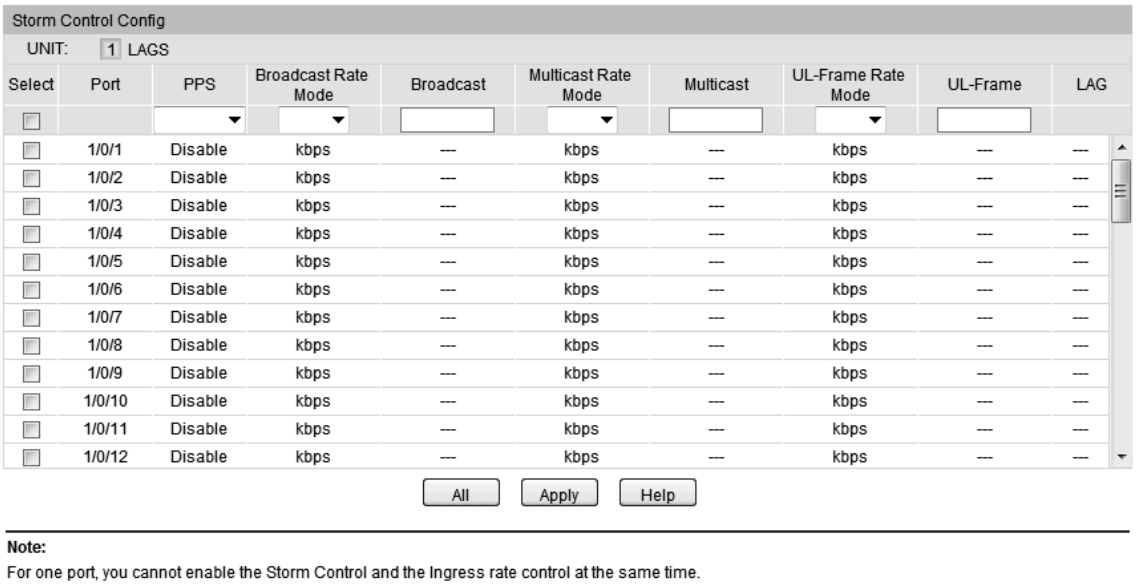


Figure 11-11 Storm Control

The following entries are displayed on this screen:

- **Storm Control Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select the desired port for Storm Control configuration. It is multi-optional.

Port: Displays the port number of the switch.

PPS: Enable or disable the PPS mode.

Broadcast Rate Mode: Select the broadcast rate mode, pps mode is invalid if the PPS is disabled.

- **kbps**: Specify the threshold in kbits per second.
- **ratio**: Specify the threshold as a percentage of the bandwidth.
- **pps**: Specify the threshold in packets per second.

Broadcast: Enable/Disable broadcast control feature for the port.

Mulitcast Rate Mode: Select the multicast rate mode, pps mode is invalid if PPS is disabled.

Multicast: Enable/Disable multicast control feature for the port.

UL-Frame Rate Mode:	Select the UL-Frame rate mode, pps mode is invalid if PPS is disabled.
UL-Frame:	Enable/Disable UL-Frame control feature for the port.
LAG:	Displays the LAG number which the port belongs to.

Note:

1. If you enable storm control feature for the ingress rate limit-enabled port, ingress rate limit feature will be disabled for this port.
2. If the PPS function is enabled, the storm control type can ONLY be pps. If the PPS function is disabled, the storm control type can be set as kbps or ratio.

11.3 Voice VLAN

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

- OUI Address (Organizationally unique identifier address)

The switch can determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC address of a packet complies with the OUI addresses configured by the system, the packet is determined as voice packet and transmitted in voice VLAN.

An OUI address is a unique identifier assigned by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It comprises the first 24 bits of a MAC address. You can recognize which vendor a device belongs to according to the OUI address. The following table shows the OUI addresses of several manufacturers. The following OUI addresses are preset of the switch by default.

Number	OUI Address	Vendor
1	00-01-e3-00-00-00	Siemens phone
2	00-03-6b-00-00-00	Cisco phone
3	00-04-0d-00-00-00	Avaya phone
4	00-60-b9-00-00-00	Philips/NEC phone
5	00-d0-1e-00-00-00	Pingtel phone
6	00-e0-75-00-00-00	Polycom phone
7	00-e0-bb-00-00-00	3com phone

Table 11-1 OUI addresses on the switch

- **Port Voice VLAN Mode**

A voice VLAN can operate in two modes: automatic mode and manual mode.

Automatic Mode: In this mode, the switch automatically adds a port which receives voice packets to voice VLAN and determines the priority of the packets through learning the source MAC of the UNTAG packets sent from IP phone when it is powered on. The aging time of voice VLAN can be configured on the switch. If the switch does not receive any voice packet on the ingress port within the aging time, the switch will remove this port from voice VLAN. Voice ports are automatically added into or removed from voice VLAN.

Manual Mode: You need to manually add the port of IP phone to voice VLAN, and then the switch will assign ACL rules and configure the priority of the packets through learning the source MAC address of packets and matching OUI address.

In practice, the port voice VLAN mode is configured according to the type of packets sent out from voice device and the link type of the port. The following table shows the detailed information.

Port Voice VLAN Mode	Voice Stream Type	Link type of the port and processing mode
Automatic Mode	TAG voice stream	Untagged: Not supported.
		Tagged: Supported. The default VLAN of the port cannot be voice VLAN.
	UNTAG voice stream	Untagged: Supported.
		Tagged: Not supported.
Manual Mode	TAG voice stream	Untagged: Not supported.
		Tagged：Supported. The default VLAN of the port should not be voice VLAN.
	UNTAG voice stream	Untagged: Supported.
		Tagged: Not supported.

Table 11-2 Port voice VLAN mode and voice stream processing mode

- **Security Mode of Voice VLAN**

When voice VLAN is enabled for a port, you can configure its security mode to filter data stream. If security mode is enabled, the port just forwards voice packets, and discards other packets whose source MAC addresses do not match OUI addresses. If security mode is not enabled, the port forwards all the packets.

Security Mode	Packet Type	Processing Mode
Enable	UNTAG packet	When the source MAC address of the packet is the OUI address that can be identified, the packet can be transmitted in the voice VLAN. Otherwise, the packet will be discarded.
	Packet with voice VLAN TAG	
	Packet with other VLAN TAG	The processing mode for the device to deal with the packet is determined by whether the port permits the VLAN or not, independent of voice VLAN security mode.
Disable	UNTAG packet	Do not check the source MAC address of the packet and all the packets can be transmitted in the voice VLAN.
	Packet with voice VLAN TAG	
	Packet with other VLAN TAG	The processing mode for the device to deal with the packet is determined by whether the port permits the VLAN or not, independent of voice VLAN security mode.

Table 11-3 Security mode and packets processing mode

Note:
Don't transmit voice stream together with other business packets in the voice VLAN except for some special requirements.

The Voice VLAN function can be implemented on **Global Config, Port Config** and **OUI Config** pages.

11.3.1 Global Config

On this page, you can configure the global parameters of the voice VLAN, including VLAN ID and aging time.

Choose the menu **QoS→Voice VLAN→Global Config** to load the following page.

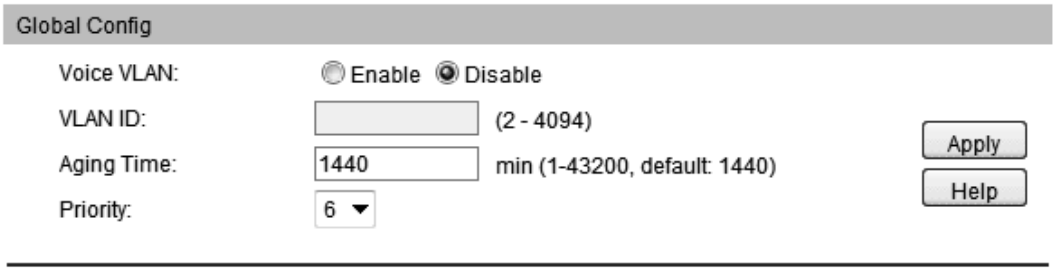


Figure 11-12 Global Configuration

The following entries are displayed on this screen:

- **Global Config**

  Voice VLAN: Select Enable/Disable Voice VLAN function.

  VLAN ID: Enter the VLAN ID of the voice VLAN.

Aging Time: Specifies the living time of the member port in auto mode after the OUI address is aging out.

Priority: Select the priority of the port when sending voice data.

11.3.2 Port Config

Before the voice VLAN function is enabled, the parameters of the ports in the voice VLAN should be configured on this page.

Choose the menu **QoS→Voice VLAN→Port Config** to load the following page.

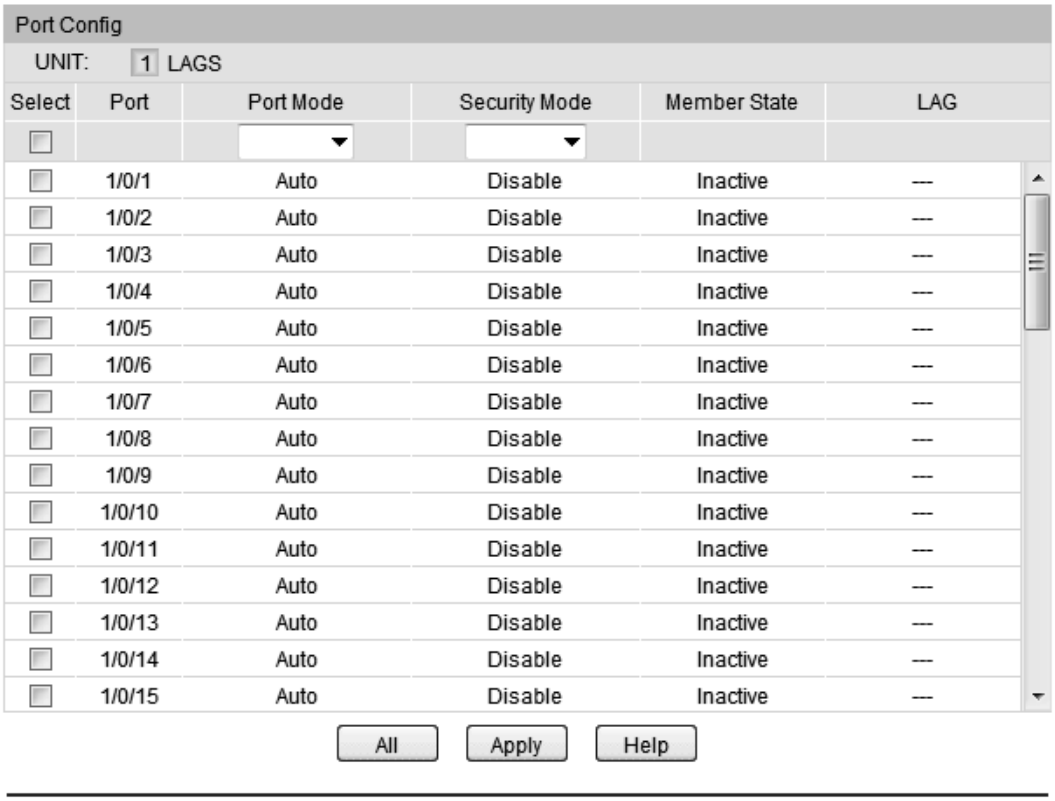


Figure 11-13 Port Config

Note:

To enable voice VLAN function for the LAG member port, please ensure its member state accords with its port mode.

If a port is a member port of voice VLAN, changing its port mode to be "Auto" will make the port leave the voice VLAN and will not join the voice VLAN automatically until it receives voice streams.

The following entries are displayed on this screen:

- **Port Config**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select:	Select the desired port for voice VLAN configuration. It is multi-optional.
Port:	Displays the port number of the switch.
Port Mode:	Select the mode for the port to join the voice VLAN. • **Auto:** In this mode, the switch automatically adds a port to the voice VLAN or removes a port from the voice VLAN by checking whether the port receives voice data or not. • **Manual:** In this mode, you can manually add a port to the voice VLAN or remove a port from the voice VLAN.
Security Mode:	Configure the security mode for forwarding packets. • **Disable:** All packets are forwarded. • **Enable:** Only voice data are forwarded.
Member State:	Displays the state of the port in the current voice VLAN.
LAG:	Displays the LAG number which the port belongs to.

11.3.3 OUI Config

The switch supports OUI creation and adds the MAC address of the special voice device to the OUI table of the switch. The switch determines whether a received packet is a voice packet by checking its OUI address. The switch analyzes the received packets. If the packets recognized as voice packets, the access port will be automatically added to the Voice VLAN.

Choose the menu **QoS→Voice VLAN→OUI Config** to load the following page.

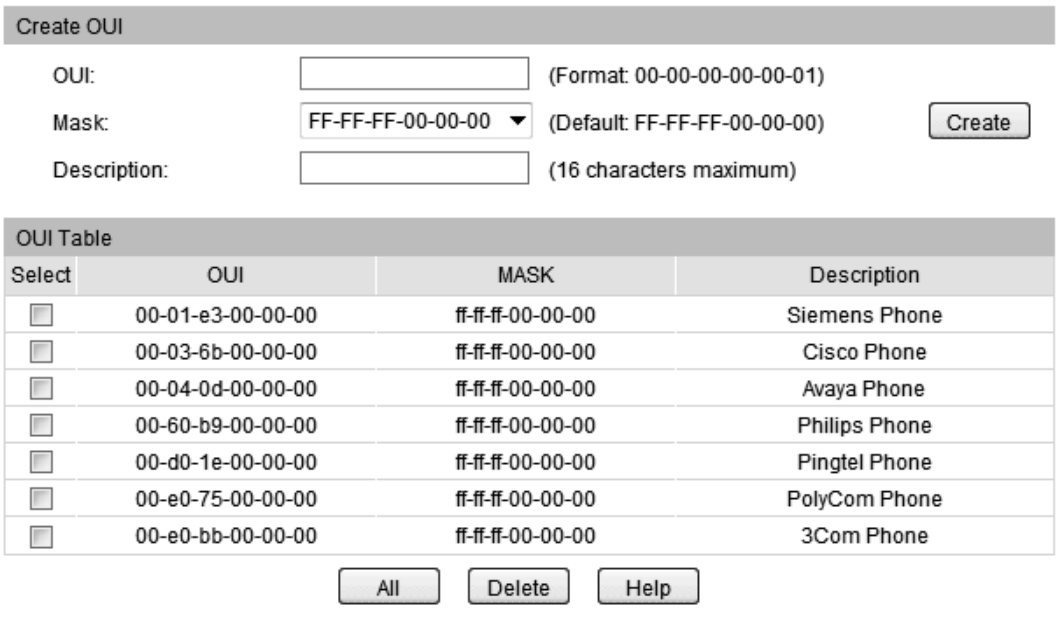


Figure 11-14 OUI Configuration

The following entries are displayed on this screen:

➢ **Create OUI**

OUI: Enter the OUI address of the voice device.

Mask: Enter the OUI address mask of the voice device.

Description: Give a description to the OUI for identification.

- **OUI Table**

Select: Select the desired entry to view the detailed information.

OUI: Displays the OUI address of the voice device.

Mask: Displays the OUI address mask of the voice device.

Description: Displays the description of the OUI.

Configuration Procedure of Voice VLAN:

Step	Operation	Description
1	Create VLAN	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN.
2	Add OUI address	Optional. On **QoS→Voice VLAN→OUI Config** page, you can check whether the switch is supporting the OUI template or not. If not, please add the OUI address.
3	Configure the parameters of the ports in voice VLAN.	Required. On **QoS→Voice VLAN→Port Config** page, configure the parameters of the ports in voice VLAN.
4	Enable Voice VLAN	Required. On **QoS→Voice VLAN→Global Config** page, configure the global parameters of voice VLAN.

Return to CONTENTS

Chapter 12 PoE

PoE (Power over Ethernet) technology describes a system to transmit electrical power along with data to remote devices over standard twisted-pair cable in an Ethernet network. It is especially useful for supplying power to IP telephones, wireless LAN access points, cameras and so on.

- **Composition**

A PoE system usually consists of PSE and PD.

PSE: Power sourcing equipment (PSE) is a device such as a switch that provides power on the Ethernet cable to the linked device.

PD: A powered device (PD) is a device accepting power from the PSE and thus consumes energy. PDs fall into two types, standard PDs and nonstandard PDs. Standard PDs refer to the powered devices that comply with IEEE 802.3af and IEEE 802.3at. Examples include wireless LAN access points, IP Phones, IP cameras, network hubs, embedded computers etc.

- **Advantage**

  - Cheap cabling: The remote device such as cameras can be powered by PSE in no need of prolonging its power cord additionally and Ethernet cable is much cheaper than AC wire or power cord.
  - Easy to connect: PoE uses only one Ethernet cable with no need of external power supply.
  - Reliable: A powered device can be either powered by PSE using Ethernet cable or powered through the provided power adapter. It is very convenient to provide a backup power supply for the PDs.
  - Flexibility: In compliance with IEEE 802.3af and IEEE 802.3at, global organizations can deploy PoE everywhere without concern for any local variance in AC power standards, outlets, plugs, or reliability.
  - Wide use: It can be applied to wireless LAN access points, IP Phones, IP cameras, network hubs, embedded computers etc.

SW-5024 is a Power Sourcing Equipment (PSE). All the Auto-Negotiation RJ45 ports on the switch support Power over Ethernet (PoE) function, which can automatically detect and supply power for those powered devices (PDs) complying with IEEE 802.3af and IEEE 802.3at. The maximum power **SW-5024** can supply is 384W and the maximum power each PoE port can supply is 30W.

PoE function can be configured in the two sections, **PoE Config** and **PoE Time-Range**.

12.1 PoE Config

All the RJ45 ports on the switch can be configured to supply power for the powered devices that comply with IEEE 802.3af and IEEE 802.3at. As the power every port or the system can provide is limited, some attributes should be set to make full use of the power and guarantee the adequate power to the linked PDs. When the power exceeds the maximum power limit or

the power is inadequate to power the device, the switch may disconnect the power supply to the PD linked to the port with lower priority. When detecting a PD is unplugged, the switch will stop supplying the power to the PD.

PoE Config, mainly for PoE attributes configuration, is implemented on **PoE Config** and **PoE Profile** pages.

12.1.1 PoE Config

On this page, you can configure the parameters to implement PoE function.

Choose the menu **PoE→PoE Config→PoE Config** to load the following page.

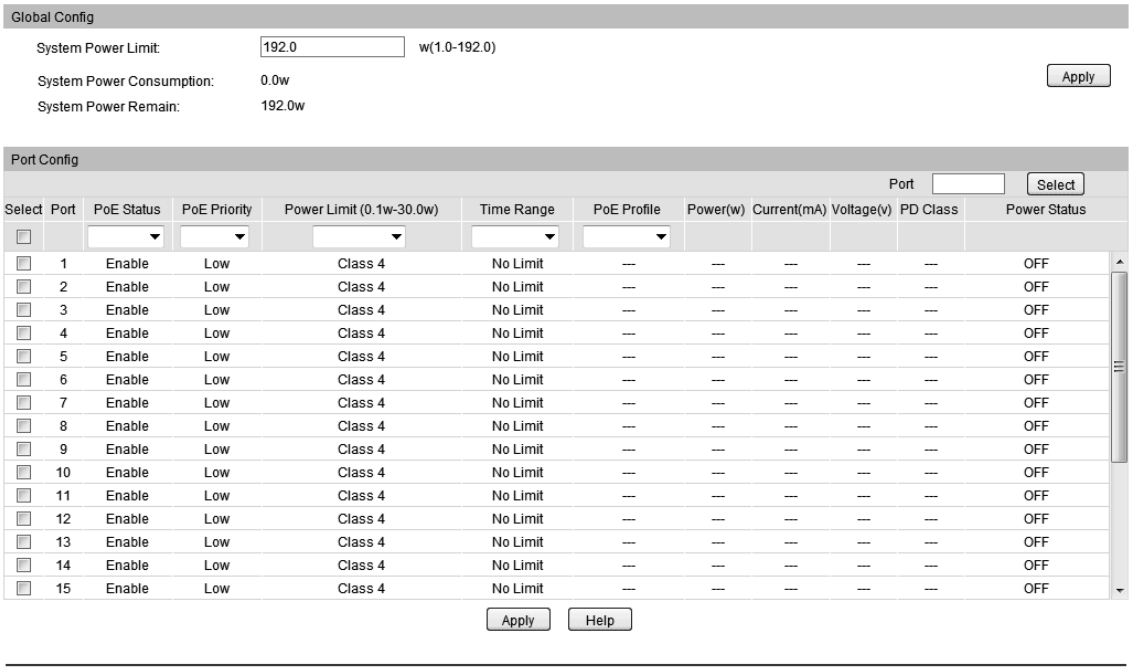


Figure 12-1 PoE Config

The following items are displayed on this screen:

- **Global Config**

  System Power Limit: Defines the max power the PoE switch can supply. It ranges from 1W to 384W.

  System Power Consumption: Displays the PoE switch's real time system power consumption.

  System Power Remain: Displays the PoE switch's real time remaining system power.

- **Port Config**

  Select: Select the desired port to configure its parameters.

  Port: Displays the port number.

PoE Status:	Select to disable/enable the PoE feature for the corresponding port. If set enable, the corresponding port can supply power to the linked PD (Powered Device).
PoE Priority:	The priority levels include High, Middle and Low in descending order. When the supply power exceeds the system power limit, the port with lower priority will stop supplying power; If these ports have the same priority levels, the port with smaller port number will stop supplying power first.
Power Limit (0.1w-30w):	Defines the max power the corresponding port can supply. Class1 represents 4W, Class2 represents 7W, Class3 represents 15.4W and Class4 represents 30W.
Time Range:	Select the time range for the PoE port to supply power. If **No limit** is selected, the PoE port will supply power all the time.
PoE Profile:	Select the profile you want to apply to the selected port. If a PoE Profile is selected, the three attributes including PoE Status, PoE Priority and Power Limit are not available.
Power (W):	Displays the port's real time power supply.
Current (mA):	Displays the port's real time current.
Voltage (V):	Displays the port's real time voltage.
PD Class:	Displays the class the linked PD (Powered Device) belongs to.
Power Status:	Displays the port's real time power status.

Note:

When Time Range is selected, the corresponding port's other PoE configurations would not work.

12.1.2 PoE Profile

PoE (Power over Ethernet) Profile is a short cut for the configuration of the PoE port. You can create some profiles to be applied to the ports. In a profile, the PoE status, PoE priority and Power limit are configured.

Choose the menu **PoE→PoE Config→Profile Profile** to load the following page.

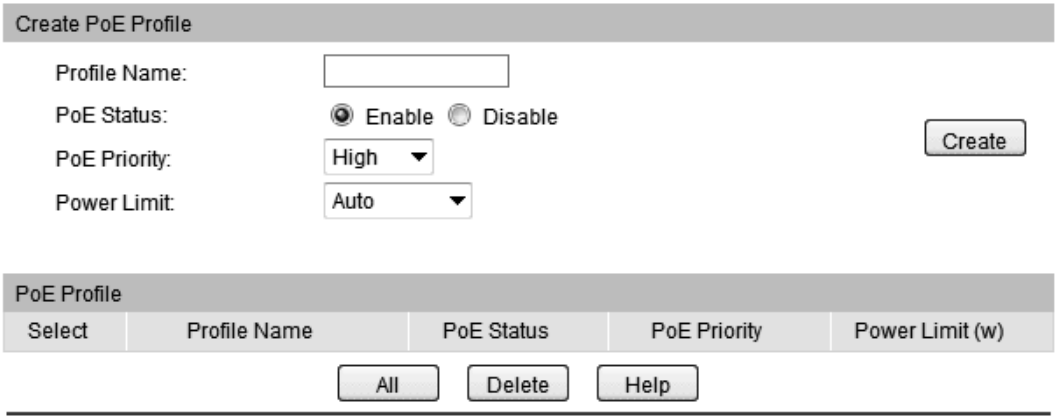


Figure 12-2 Profile Config

The following items are displayed on this screen:

- **Create PoE Profile**

  Profile Name: Enter the name of the profile.

  PoE Status: Select to the enable/disable PoE feature for the corresponding port. If set enable, the port may supply power to the linked PD (Power Device).

  PoE Priority: The priority levels include High, Middle and Low in descending order. When the supply power exceeds the system power limit, the PD linked to the port with lower priority will be disconnected.

  Power Limit: Defines the max power the corresponding port can supply. Class1 represents 4W, Class2 represents 7W, Class3 represents 15.4W, and Class4 represents 30W.

- **PoE Profile**

  Select: Select the desired profile to delete.

  Profile Name: Displays the name of the profile.

  PoE Status: Displays the PoE status of the port in the profile.

  PoE Priority: Displays the PoE priority of the port in the profile.

  Power Limit: Displays the max power the port in the profile can supply.

12.2 Time-Range

A time-range based PoE enables you to implement PoE power supply by differentiating the time-ranges. A time-range can be specified for each port. The port will not supply power when the specified time-range is configured and the system time is not within the time-range.

On this switch time-range consists of **Holiday**, **Absolute** and **Periodic**. A specific Time-range is the intersection of Absolute Time and Periodic Time, combined with the Holiday you defined.

Absolute Time-range defines one or several time ranges with specific starting time and ending time in the Gregorian calendar. Seven time ranges can be created at most, and their union is the Absolute Time-range. Absolute Time-range does not recur. If no absolute time range is configured, the Absolute Time-range takes effect from January 1, 2000 00:00 to December 31, 2099 24:00.

For example, under Absolute type, create time range 1 from January 1, 2015 00:00 to January 31, 2015 24:00, and time range 2 from March 1, 2015 00:00 to March 31, 2015 24:00, which makes Absolute Time-range effective in both January and March.

Periodic Time-range defines one or several time ranges with specific starting time and ending time in a week. Periodic Time-range recurs periodically on the day/days you configured in the week. Seven time ranges can be created at most, and their union is the Periodic Time-range. If no periodic time range is configured, the Periodic Time-range takes effect all the time from Monday to Sunday.

If the Holiday mode is configured as Include, the Time-range will be the intersection of the Absolute Time and the Periodic Time.

If the Holiday mode is configure as Exclude, the Time range will be the intersection of the Absolute Time and the Periodic Time, with Holiday excluded.

The Time-Range configuration can be implemented on **Time-Range Summary**, **Time-Range Create** and **Holiday Config** pages.

12.2.1 Time-Range Summary

On this page you can view or delete the current Time-ranges.

Choose the menu **PoE→Time-Range→Time-Range Summary** to load the following page.

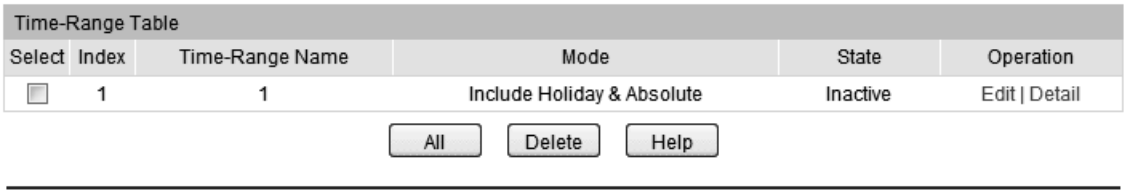


Figure 12-3 Time-Range Table

The following items are displayed on this screen:

- **Time-Range Table**

  Select: Select the desired entry to delete the corresponding time-range.

  Index: Displays the index of the time-range.

  Time-Range Name: Displays the name of the time-range.

Mode:	Displays the mode of the time-range. The mode can be one or a combination of the following modes: **Include/Exclude Holiday**, **Absolute** and **Periodic**. Refer to Time-Range Create and Holiday Config for more details.
State	Displays active state of the time-range.
Operation:	Click **Edit** to modify this time-range and click **Detail** to display the complete information of this time–range.

12.2.2 Time-Range Create

On this page you can create time-ranges.

Choose the menu **PoE→Time-Range→Time-Range Create** to load the following page.

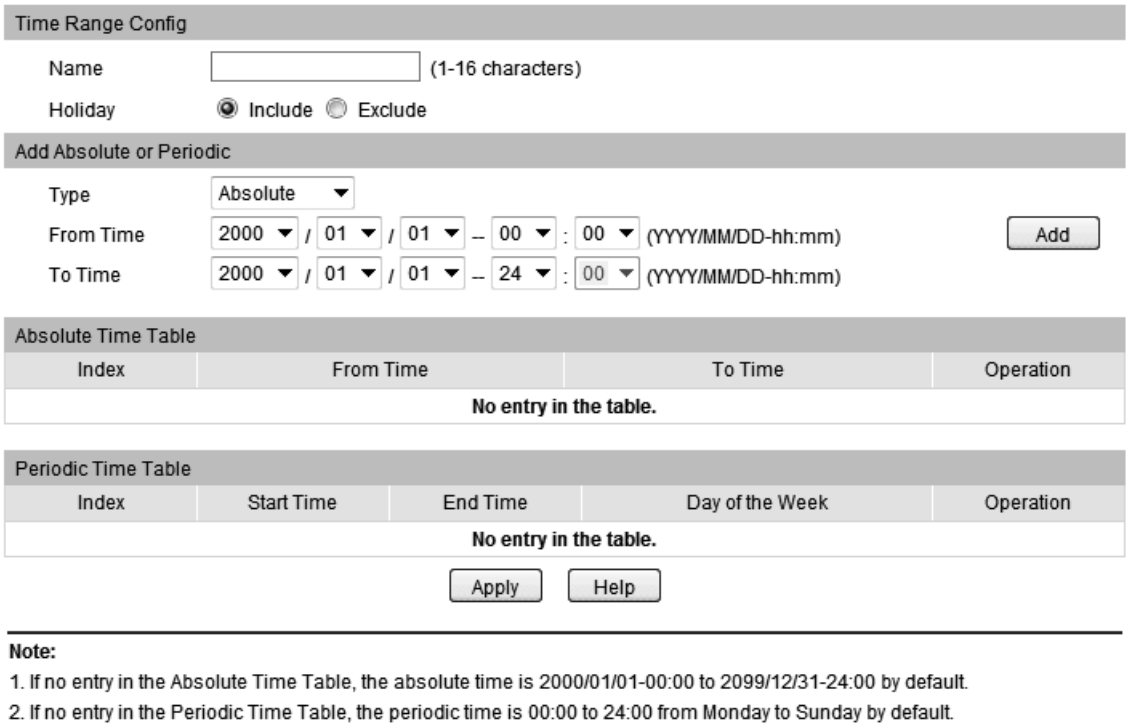


Figure 12-4 Time-Range Create

Note:

1. Up to 7 absolute time-ranges and 7 periodic time-ranges can be created in one Time-range.
2. If there is no entry in the Absolute Time table, the Absolute Time-range is from 2000/01/01-00:00 to 2099/12/31-24:00 by default.
3. If there is no entry in the Periodic Time table, the Periodic Time-range takes effect all the time from Monday to Sunday by default.

The following items are displayed on this screen:

- **Time Range Config**

Name:	Enter the name of the time-range for time identification.

Holiday: Select Holiday mode. By default, the mode is Include.

Include: The Holiday has no effect on the Time-range, which means the final Time-range will be the intersection of the Absolute Time and Periodic Time.

Exclude: The final Time range will be the intersection of the Absolute Time and the Periodic Time, with Holiday excluded.

- **Add Absolute or Periodic**

Type: Select the time range type, Absolute or Periodic.

Absolute Time-range defines up to 7 time ranges with specific starting time and ending time in the Gregorian calendar. It does not recur.

Periodic Time-range defines up to 7 time ranges with specific starting time and ending time in a week. Periodic Time-range recurs periodically on the day/days you configured in the week.

From Time: Set the start time of the absolute time range.

To Time: Set the end time of the absolute time range.

- **Absolute Time Table**

Index: Displays the index of the absolute time range.

From Time: Displays start time of the absolute time range.

To Time: Displays end time of the absolute time range.

Operation: Click the **Delete** button to delete the corresponding time range.

- **Periodic Time Table**

Index: Displays the index of the periodic time range.

Start Time: Displays the start time of the periodic time range.

End Time: Displays the end time of the periodic time range.

Day of the Week: Displays the recurring days in the periodic time range.

Operation: Click the **Delete** button to delete the corresponding time range.

12.2.3 Holiday Config

You can define holidays in this page. The holiday will be excluded from the Time-range you created if the Holiday mode is Exclude.

Choose the menu **PoE→Time-Range→Holiday Config** to load the following page.

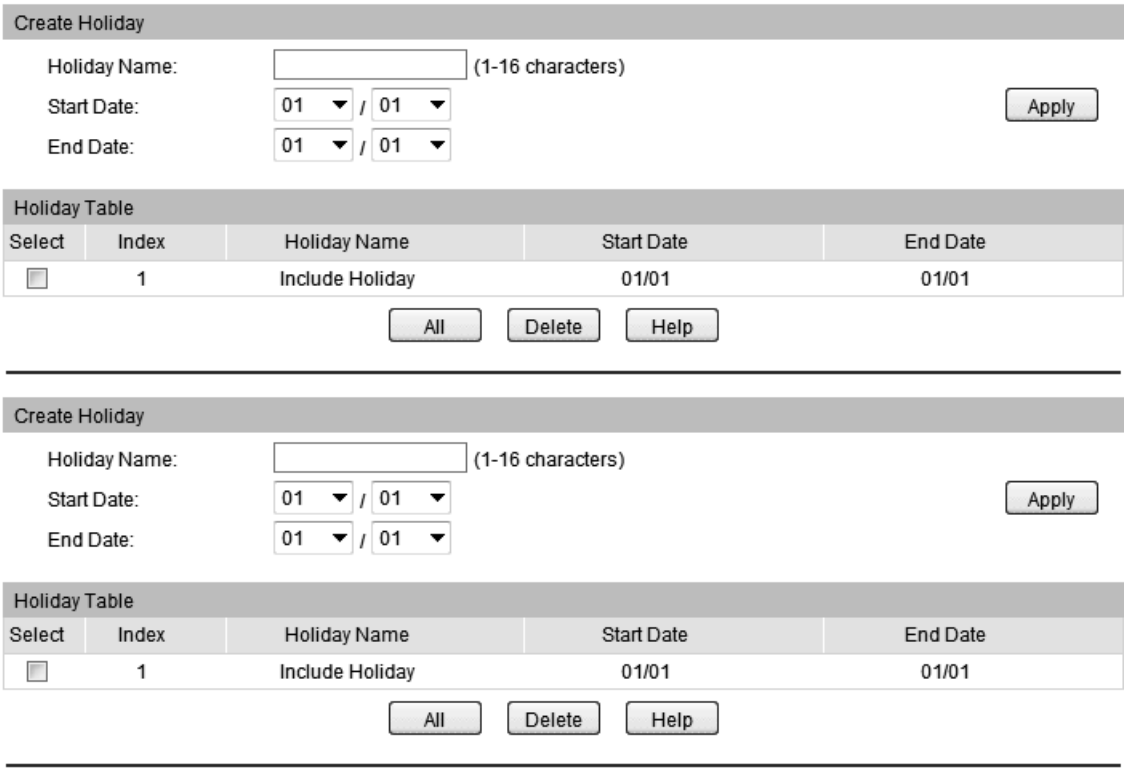


Figure 12-5 Holiday Configuration

The following entries are displayed on this screen:

- **Create Holiday**

  Holiday Name: Enter the name of the holiday.

  Start Date: Specify the start date of the holiday.

  End Date: Specify the end date of the holiday.

- **Holiday Table**

  Select: Select the desired entry to delete the corresponding holiday.

  Index: Displays the index of the holiday.

  Holiday Name: Displays the name of the holiday.

  Start Date: Displays the start date of the holiday.

  End Date: Displays the end date of the holiday.

Return to CONTENTS

Chapter 13 ACL

ACL (Access Control List) is used to filter packets by configuring match rules and process policies of packets in order to control the access of the illegal users to the network. Besides, ACL functions to control traffic flows and save network resources. It provides a flexible and secured access control policy and facilitates you to control the network security.

On this switch, ACLs classify packets based on a series of match conditions, which can be L2-L4 protocol key fields carried in the packets. A time-range based ACL enables you to implement ACL control over packets by differentiating the time-ranges.

The ACL module is mainly for ACL configuration of the switch, including four submenus: **Time-Range**, **ACL Config**, **Policy Config**, **ACL Binding** and **Policy Binding**.

13.1 Time-Range

If a configured ACL is needed to be effective in a specified time-range, a time-range should be firstly specified in the ACL. As the time-range based ACL takes effect only within the specified time-range, data packets can be filtered by differentiating the time-ranges.

On this switch absolute time, week time and holiday can be configured. Configure an absolute time section in the form of "the start date to the end date" to make ACLs effective; configure a week time section to make ACLs effective on the fixed days of the week; configure a holiday section to make ACLs effective on some special days. In each time-range, four time-slices can be configured.

The Time-Range configuration can be implemented on **Time-Range Summary**, **Time-Range Create** and **Holiday Config** pages.

13.1.1 Time-Range Summary

On this page you can view the current time-ranges.

Choose the menu **ACL→Time-Range→Time-Range Summary** to load the following page.

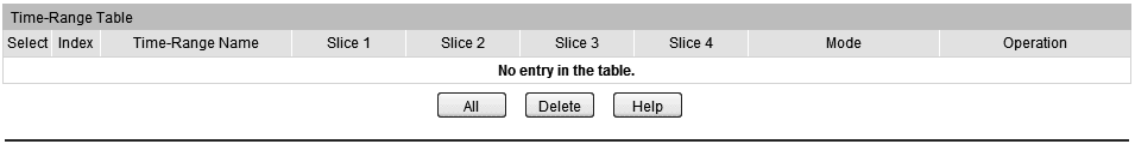


Figure 13-1 Time-Range Table

The following entries are displayed on this screen:

- **Time-Range Table**

  Select: Select the desired entry to delete the corresponding time-range.

  Index: Displays the index of the time-range.

  Time-Range Name: Displays the name of the time-range.

  Slice: Displays the time-slice of the time-range.

Mode: Displays the mode the time-range adopts.

Operation: Click the **Edit** button to modify the time-range. Click the **Detail** button to display the complete information of this time–range.

13.1.2 Time-Range Create

On this page you can create time-ranges.

Choose the menu **ACL→Time-Range→Time-Range Create** to load the following page.

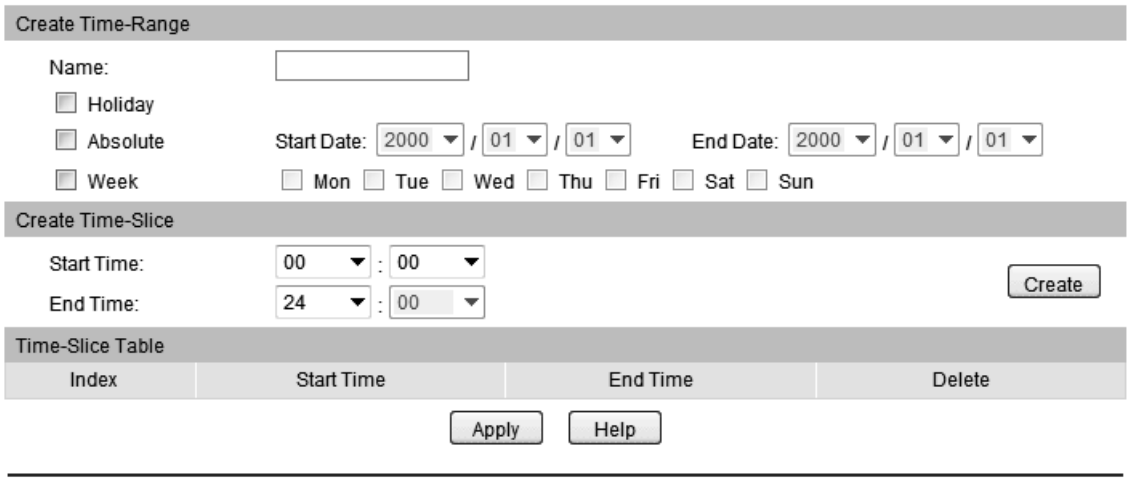


Figure 13-2 Time-Range Create

Note:

To successfully configure time-ranges, please firstly specify time-slices and then time-ranges.

The following entries are displayed on this screen:

- **Create Time-Range**

Name: Enter the name of the time-range for time identification.

Holiday: Select Holiday you set as a time-range. The ACL rule based on this time-range takes effect only when the system time is within the holiday.

Absolute: Select Absolute to configure absolute time-range. The ACL rule based on this time-range takes effect only when the system time is within the absolute time-range.

Week: Select Week to configure week time-range. The ACL rule based on this time-range takes effect only when the system time is within the week time-range.

- **Create Time-Slice**

Start Time: Set the start time of the time-slice.

End Time: Set the end time of the time-slice.

- **Time-Slice Table**

Index: Displays the index of the time-slice.

Start Time: Displays the start time of the time-slice.

End Time: Displays the end time of the time-slice.

Delete: Click the **Delete** button to delete the corresponding time-slice.

13.1.3 Holiday Config

Holiday mode is applied as a different secured access control policy from the week mode. On this page you can define holidays according to your work arrangement.

Choose the menu **ACL→Time-Range→Holiday Config** to load the following page.

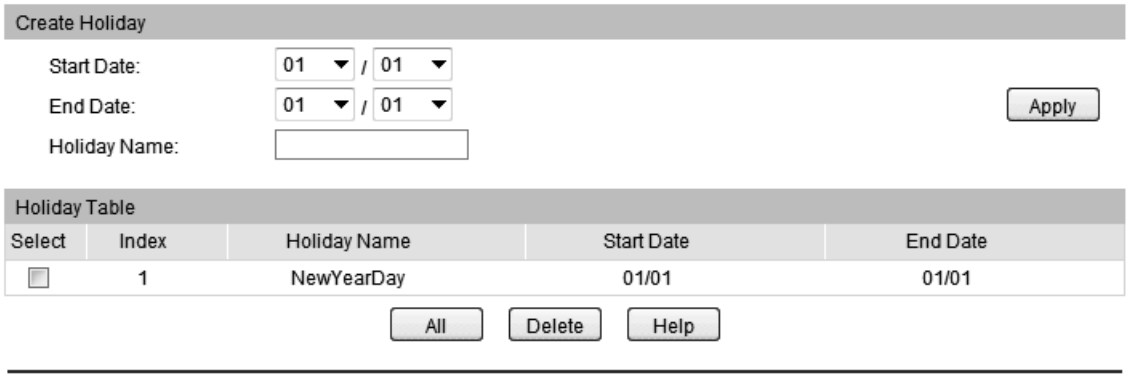


Figure 13-3 Holiday Configuration

The following entries are displayed on this screen:

- **Create Holiday**

Start Date: Specify the start date of the holiday.

End Date: Specify the end date of the holiday.

Holiday Name: Enter the name of the holiday.

- **Holiday Table**

Select: Select the desired entry to delete the corresponding holiday.

Index: Displays the index of the holiday.

Holiday Name: Displays the name of the holiday.

Start Date: Displays the start date of the holiday.

End Date: Displays the end date of the holiday.

13.2 ACL Config

An ACL may contain a number of rules, and each rule specifies a different package range. Packets are matched in match order. Once a rule is matched, the switch processes the matched packets taking the operation specified in the rule without considering the other rules, which can enhance the performance of the switch.

The ACL Config function can be implemented on **ACL Summary**, **ACL Create**, **MAC ACL**, **Standard-IP ACL**, **Extend-IP ACL**, **Combined ACL** and **IPv6 ACL** pages.

13.2.1 ACL Summary

On this page, you can view the current ACLs configured in the switch.

Choose the menu **ACL→ACL Config→ACL Summary** to load the following page.

Figure 13-4 ACL Summary

The following entries are displayed on this screen:

- **Search Option**

Select ACL: Select the ACL you have created

ACL Type: Displays the type of the ACL you select.

Rule Order: Displays the rule order of the ACL you select.

13.2.2 ACL Create

On this page you can create ACLs.

Choose the menu **ACL→ACL Config→ACL Create** to load the following page.

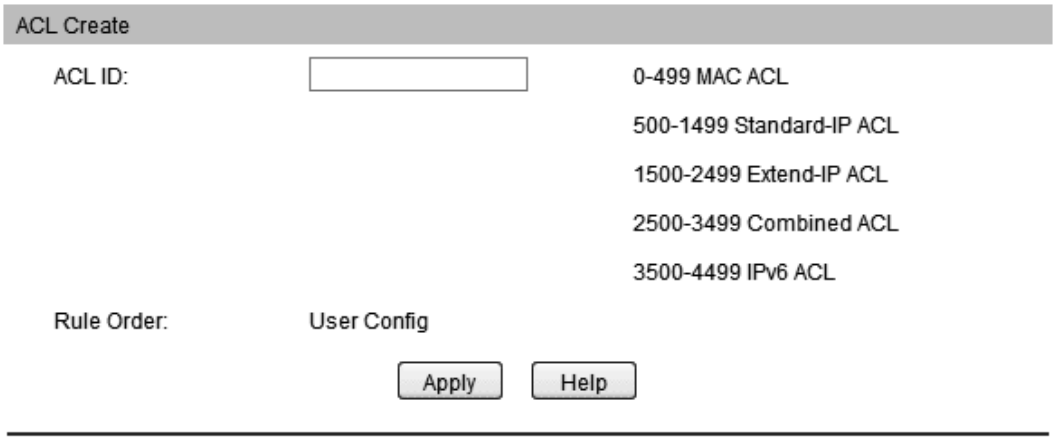


Figure 13-5 ACL Create

The following entries are displayed on this screen:

- **ACL Create**

ACL ID: Enter ACL ID of the ACL you want to create.

Rule Order: User Config order is set to be match order in this ACL.

13.2.3 MAC ACL

MAC ACLs analyze and process packets based on a series of match conditions, which can be the source MAC addresses and destination MAC addresses carried in the packets.

Choose the menu **ACL→ACL Config→MAC ACL** to load the following page.

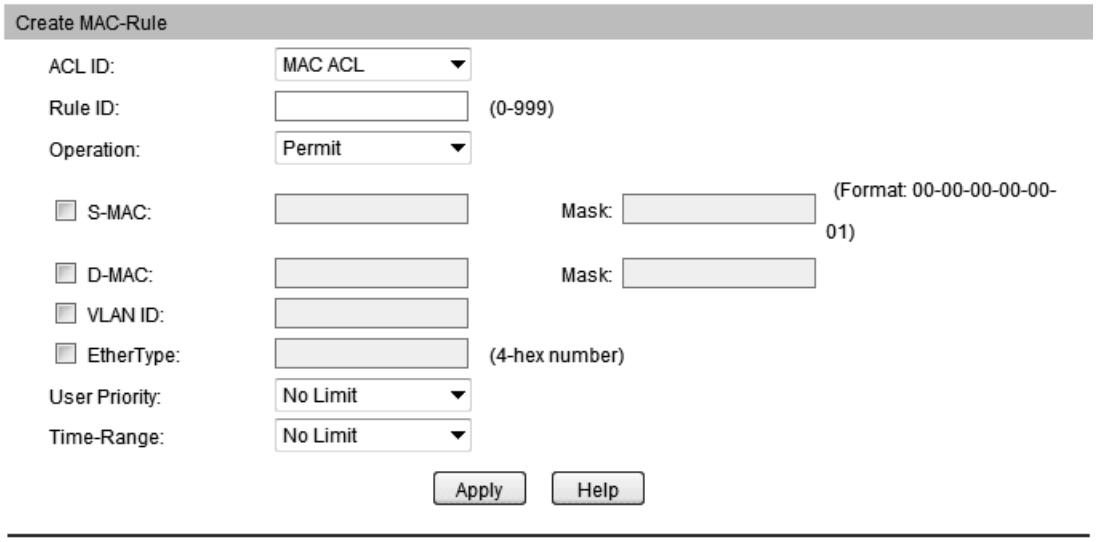


Figure 13-6 Create MAC Rule

The following entries are displayed on this screen:

- **Create MAC-Rule**

ACL ID: Select the desired MAC ACL for configuration.

Rule ID: Enter the rule ID.

Operation: Select the operation for the switch to process packets which match the rules.

- **Permit**: Forward packets.
- **Deny**: Discard Packets.

S-MAC: Enter the source MAC address contained in the rule.

D-MAC: Enter the destination MAC address contained in the rule.

MASK: Enter MAC address mask. If it is set to 1, it must strictly match the address.

VLAN ID: Enter the VLAN ID contained in the rule.

EtherType: Enter EtherType contained in the rule.

User Priority: Select the user priority contained in the rule for the tagged packets to match.

Time-Range: Select the time-range for the rule to take effect.

13.2.4 Standard-IP ACL

Standard-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Choose the menu **ACL→ACL Config→Standard-IP ACL** to load the following page.

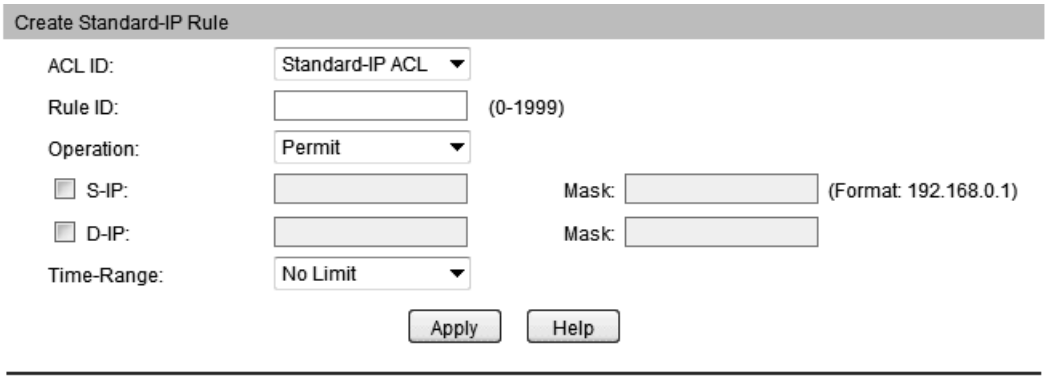


Figure 13-7 Create Standard-IP Rule

The following entries are displayed on this screen:

➢ **Create Standard-IP ACL**

ACL ID: Select the desired Standard-IP ACL for configuration.

Rule ID: Enter the rule ID.

Operation: Select the operation for the switch to process packets which match the rules.

- **Permit**: Forward packets.
- **Deny**: Discard Packets.

S-IP: Enter the source IP address contained in the rule.

D-IP: Enter the destination IP address contained in the rule.

Mask: Enter IP address mask. If it is set to 1, it must strictly match the address.

Time-Range: Select the time-range for the rule to take effect.

13.2.5 Extend-IP ACL

Extend-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses, destination IP addresses, IP protocol and other information of this sort carried in the packets.

Choose the menu **ACL→ACL Config→Extend-IP ACL** to load the following page.

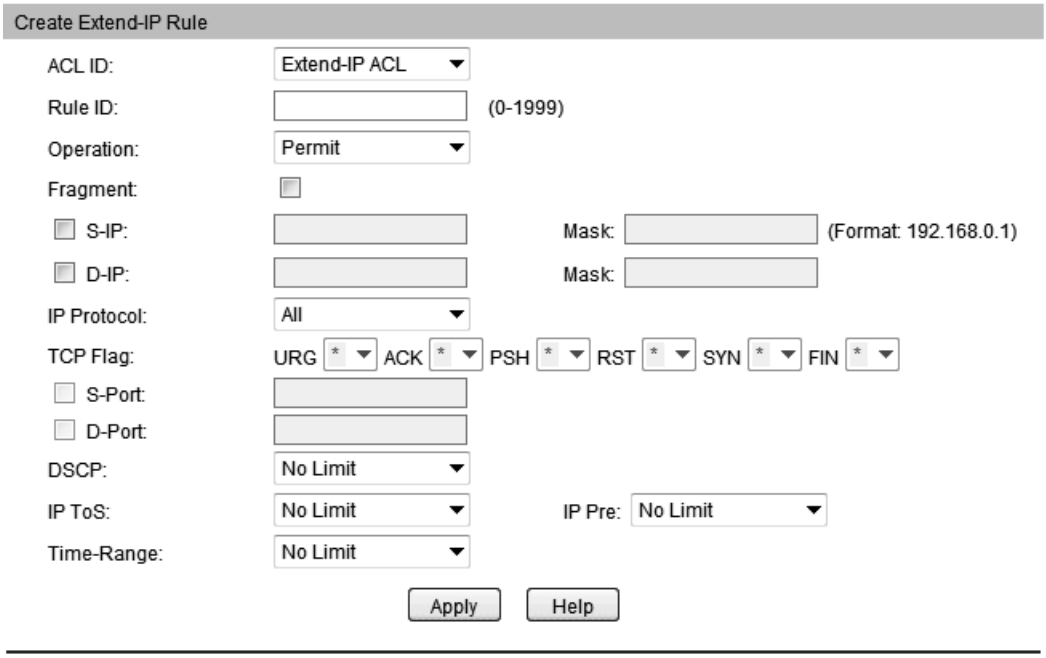


Figure 13-8 Create Extend-IP Rule

The following entries are displayed on this screen:

➢ **Create Extend-IP ACL**

ACL ID: Select the desired Extend-IP ACL for configuration.

Rule ID: Enter the rule ID.

Operation: Select the operation for the switch to process packets which match the rules.

- **Permit**: Forward packets.
- **Deny**: Discard Packets.

Fragment: Select if the rule will take effect on the fragment packets. When the fragment is selected, this rule will process all the fragments and the last piece of fragment will be always forwarded.

S-IP: Enter the source IP address contained in the rule.

D-IP: Enter the destination IP address contained in the rule.

Mask: Enter IP address mask. If it is set to 1, it must strictly match the address.

IP Protocol: Select IP protocol contained in the rule.

TCP Flag: Configure TCP flag when TCP is selected from the pull-down list of IP Protocol.

S-Port: Configure TCP/IP source port contained in the rule when TCP/UDP is selected from the pull-down list of IP Protocol.

D-Port: Configure TCP/IP destination port contained in the rule when TCP/UDP is selected from the pull-down list of IP Protocol.

DSCP: Enter the DSCP information contained in the rule.

IP ToS: Enter the IP ToS contained in the rule.

IP Pre: Enter the IP Precedence contained in the rule.

Time-Range: Select the time-range for the rule to take effect.

13.2.6 Combined ACL

Combined ACLs analyze and process data packets based on a series of match conditions, which can be the source MAC addresses, destination MAC addresses source IP addresses, destination IP addresses and other information of this sort carried in the packets.

Choose the menu **ACL→ACL Config→Combined ACL** to load the following page.

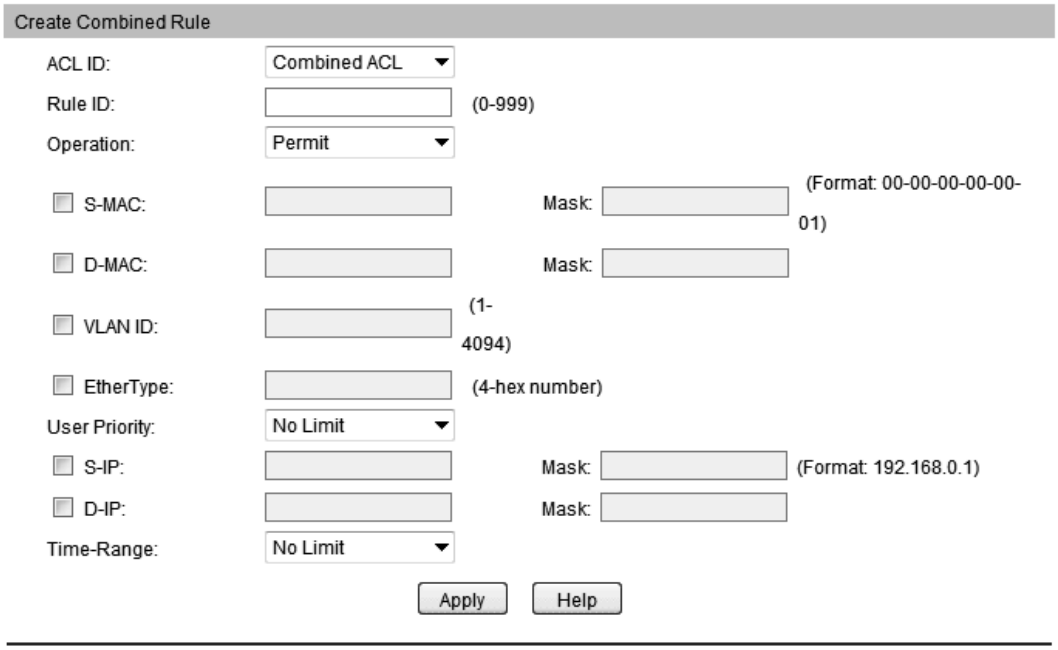


Figure 13-9 Combined ACL

The following entries are displayed on this screen:

➢ **Create combined Rule**

ACL ID: Select the desired Combined ACL for configuration.

Rule ID:	Enter the rule ID.
Operation:	Select the operation for the switch to process packets which match the rules. ● **Permit:** Forward packets. ● **Deny:** Discard Packets.
S-MAC:	Enter the source MAC address contained in the rule.
D-MAC:	Enter the destination MAC address contained in the rule.
Mask:	Enter IP address mask. If it is set to 1, it must strictly match the address.
VLAN ID	Enter the VLAN ID contained in the rule.
EtherType	Enter EtherType contained in the rule.
User Priority	Select the user priority contained in the rule for the tagged packets to match.
Fragment:	Select if the rule will take effect on the fragment packets. When the fragment is selected, this rule will process all the fragments and the last piece of fragment will be always forwarded.
S-IP:	Enter the source IP address contained in the rule.
D-IP:	Enter the destination IP address contained in the rule.
Mask:	Enter IP address mask. If it is set to 1, it must strictly match the address.
Time-Range:	Select the time-range for the rule to take effect.

Note:

Before binding a Combined ACL to an interface or VLAN, you should configure the SDM template as "default" or "enterpriseV4" and save your configurations. See **SDM Template** for more information about SDM template configuration.

13.2.7 IPv6 ACL

IPv6 ACLs analyze and process data packets based on a series of match conditions, such as the source IPv6 addresses, destination IPv6 addresses and port number carried in the packets.

Choose the menu **ACL→ACL Config→IPv6 ACL** to load the following page.

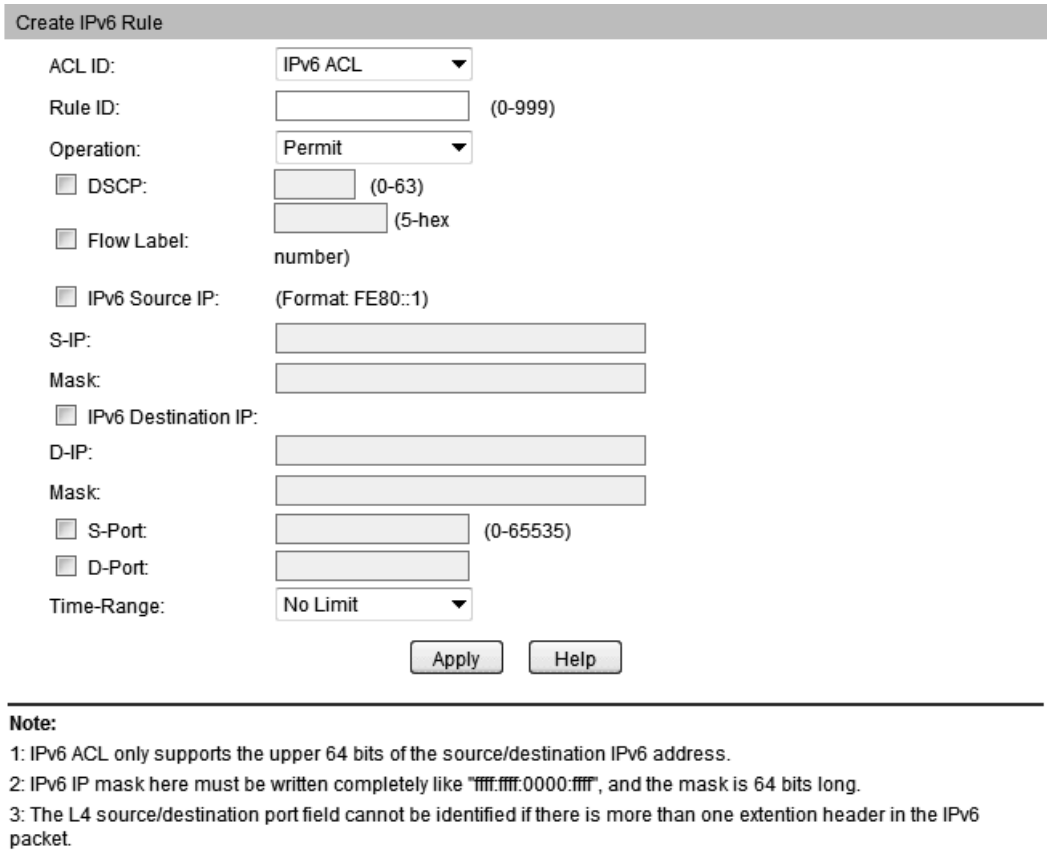


Figure 13-10 IPv6 ACL Config

The following entries are displayed on this screen:

- **Create Extend-IP ACL**

ACL ID: Select the desired IPv6 ACL for configuration.

Rule ID: Enter the rule ID.

Operation: Select the operation for the switch to process packets which match the rules.

- **Permit**: Forward packets.
- **Deny**: Discard Packets.

DSCP: Enter the DSCP information contained in the rule.

Flow Label: Enter the Flow Label information contained in the rule.

IPv6 Source IP: Click to enable the IPv6 source IP verification.

S-IP: Enter the source IPv6 address contained in the rule, you can input all the 128 bits, but only upper 64 bits are verified.

Mask: Enter IP address mask. If it is set to 1, the upper 64 bits in the source address of the packet must strictly match the S-IP you configured. This field is 64-bit long.

IPv6 Destination IP: Click to enable the IPv6 destination IP verification.

D-IP: Enter the destination IPv6 address contained in the rule, you can input all the 128 bits, but only upper 64 bits are verified.

Mask: Enter IP address mask. If it is set to 1, the upper 64 bits in the destination address of the packet must strictly match the D-IP you configured. This field is 64-bit long.

S-Port: Configure L4 source port contained in the rule when TCP/UDP is defined.

D-Port: Configure L4 destination port contained in the rule when TCP/UDP is defined.

Time-Range: Select the time-range for the rule to take effect.

Note:

Before binding an IPv6 ACL to an interface or VLAN, you should configure the SDM template as "enterpriseV6" and save your configurations. See **SDM Template** for more information about SDM template configuration.

13.3 Policy Config

A Policy is used to control the data packets those match the corresponding ACL rules by configuring ACLs and actions together for effect.

The Policy Config can be implemented on **Policy Summary**, **Police Create** and **Action Create** pages.

13.3.1 Policy Summary

On this page, you can view the ACL and the corresponding operations in the policy.

Choose the menu **ACL→Policy Config→Policy Summary** to load the following page.

Figure 13-11 Policy Summary

The following entries are displayed on this screen:

- **Search Option**

Select Policy: Select name of the desired policy for view. If you want to delete the desired policy, please click the **Delete** button.

- **Action Table**

Select: Select the desired entry to delete the corresponding policy.

Index: Displays the index of the policy.

ACL ID: Displays the ID of the ACL contained in the policy.

S-Mirror: Displays the source mirror port of the policy.

S-Condition: Displays the source condition added to the policy.

Redirect: Displays the redirect added to the policy.

QoS Remark: Displays the QoS remark added to the policy.

Operation: Edit the information of this action.

13.3.2 Policy Create

On this page you can create the policy.

Choose the menu **ACL→Policy Config→Policy Create** to load the following page.

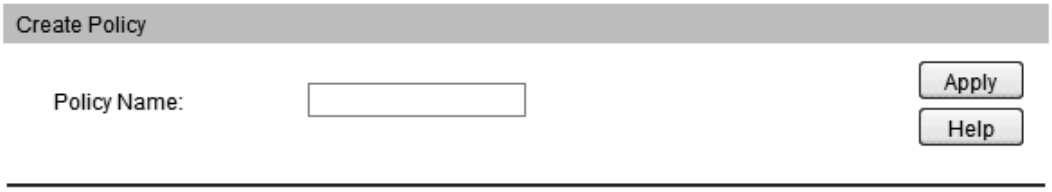


Figure 13-12 Create Policy

The following entries are displayed on this screen:

- **Create Policy**

Policy Name: Enter the name of the policy.

13.3.3 Action Create

On this page you can add ACLs for the policy.

Choose the menu **ACL→Policy Config→Action Create** to load the following page.

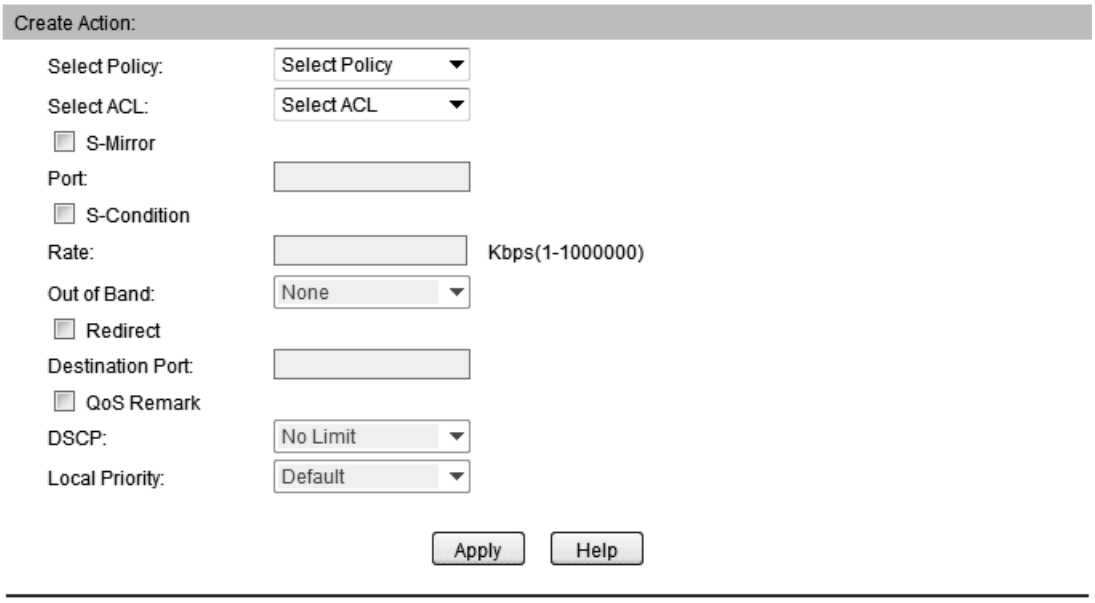


Figure 13-13 Action Create

The following entries are displayed on this screen:

- **Create Action**

Select Policy: Select the name of the policy.

Select ACL: Select the ACL for configuration in the policy.

S-Mirror: Select S-Mirror to mirror the data packets in the policy to the specific port.

S-Condition: Select S-Condition to limit the transmission rate of the data packets in the policy.

- **Rate:** Specify the forwarding rate of the data packets those match the corresponding ACL.
- **Out of Band:** Specify the disposal way of the data packets those are transmitted beyond the rate.

Redirect: Select Redirect to change the forwarding direction of the data packets in the policy.

- **Destination Port:** Forward the data packets those match the corresponding ACL to the specific port.

QoS Remark: Select QoS Remark to forward the data packets based on the QoS settings.

- **DSCP:** Specify the DSCP region for the data packets those match the corresponding ACL.
- **Local Priority:** Specify the local priority for the data packets those match the corresponding ACL.

13.4 ACL Binding

ACL Binding function can have the ACL take its effect on a specific port/VLAN. The ACL will take effect only when it is bound to a port/VLAN. In the same way, the port/VLAN will receive the data packets and process them based on the ACL only when the ACL is bound to the port/VLAN.

The ACL Binding can be implemented on **Binding Table**, **Port Binding** and **VLAN Binding** pages.

13.4.1 Binding Table

On this page view the ACL bound to port/VLAN.

Choose the menu **ACL→ACL Binding→Binding Table** to load the following page.

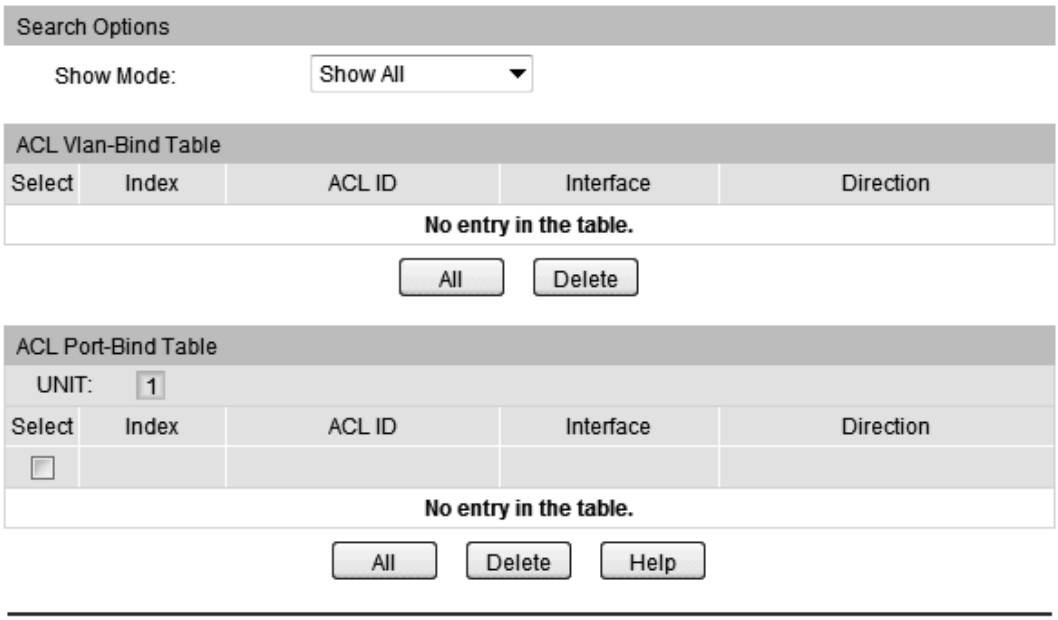


Figure 13-14 Binding Table

The following entries are displayed on this screen:

- **Search Option**

  Show Mode: Select a show mode appropriate to your needs.

- **ACL VLAN-Bind Table**

  Select: Select the desired entry to delete the corresponding binding ACL.

  Index: Displays the index of the binding ACL.

  ACL ID: Displays the ID of the binding ACL.

  Interface: Displays the port number or VLAN ID bound to the ACL.

  Direction: Displays the binding direction.

- **ACL Port-Bind Table**

  Select: Select the desired entry to delete the corresponding binding ACL.

  Index: Displays the index of the binding ACL.

  ACL ID: Displays the ID of the binding ACL.

  Interface: Displays the port number or VLAN ID bound to the ACL.

  Direction: Displays the binding direction.

13.4.2 Port Binding

On this page you can bind an ACL to a port.

Choose the menu **ACL→ACL Binding→Port Binding** to load the following page.

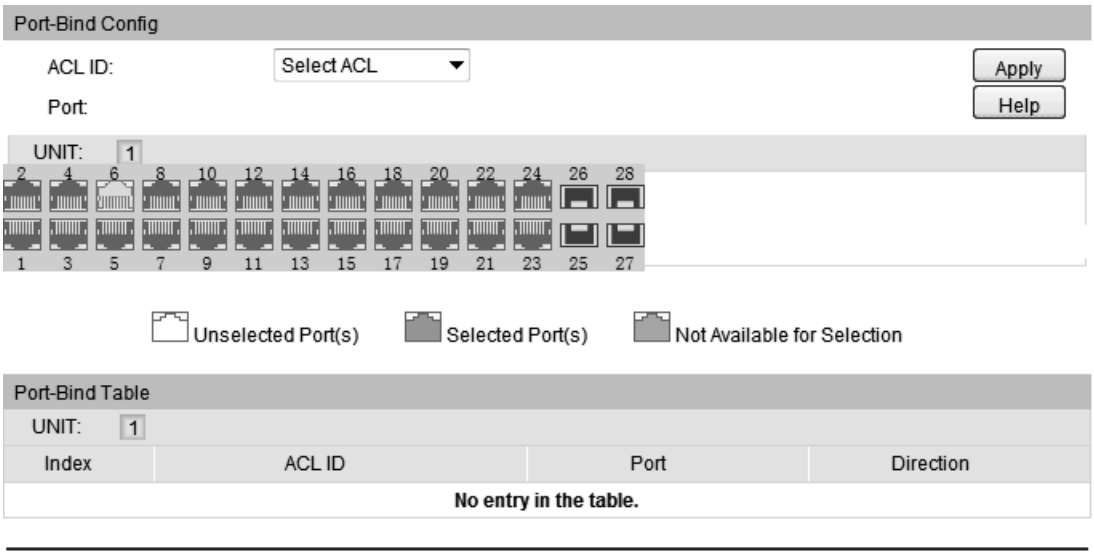


Figure 13-15 Bind the policy to the port

The following entries are displayed on this screen:

- **Port-Bind Config**

  ACL ID: Select the ID of the ACL you want to bind.

  Port: Select the number of the port you want to bind.

- **Port-Bind Table**

  Index: Displays the index of the binding ACL.

  ACL ID: Displays the ID of the binding ACL.

  Port: Displays the number of the port bound to the corresponding ACL.

Direction: Displays the binding direction.

13.4.3 VLAN Binding

On this page you can bind an ACL to a VLAN.

Choose the menu **ACL→ACL Binding→VLAN Binding** to load the following page.

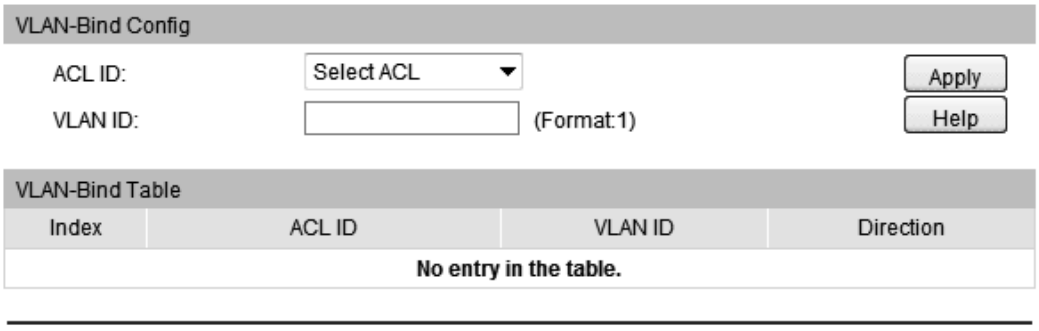


Figure 13-16 Bind the policy to the VLAN

The following entries are displayed on this screen:

- **VLAN-Bind Config**

  ACL ID: Select the ID of the ACL you want to bind.

  VLAN ID: Enter the ID of the VLAN you want to bind.

- **VLAN-Bind Table**

  Index: Displays the index of the binding ACL.

  ACL ID: Displays the ID of the binding ACL.

  VLAN ID: Displays the ID of the VLAN bound to the corresponding ACL.

  Direction: Displays the binding direction.

Configuration Procedure:

Step	Operation	Description
1	Configure ACL rules	Required. On **ACL→ACL Config** configuration pages, configure ACL rules to match packets.
2	Bind the ACL to the port/VLAN	Required. On **ACL→ACL Binding** configuration pages, bind the ACL to the port/VLAN to make the ACL effective on the corresponding port/VLAN.

13.5 Policy Binding

Policy Binding function can have the policy take its effect on a specific port/VLAN. The policy will take effect only when it is bound to a port/VLAN. In the same way, the port/VLAN will

receive the data packets and process them based on the policy only when the policy is bound to the port/VLAN.

The Policy Binding can be implemented on **Binding Table**, **Port Binding** and **VLAN Binding** pages.

13.5.1 Binding Table

On this page view the policy bound to port/VLAN.

Choose the menu **ACL→Policy Binding→Binding Table** to load the following page.

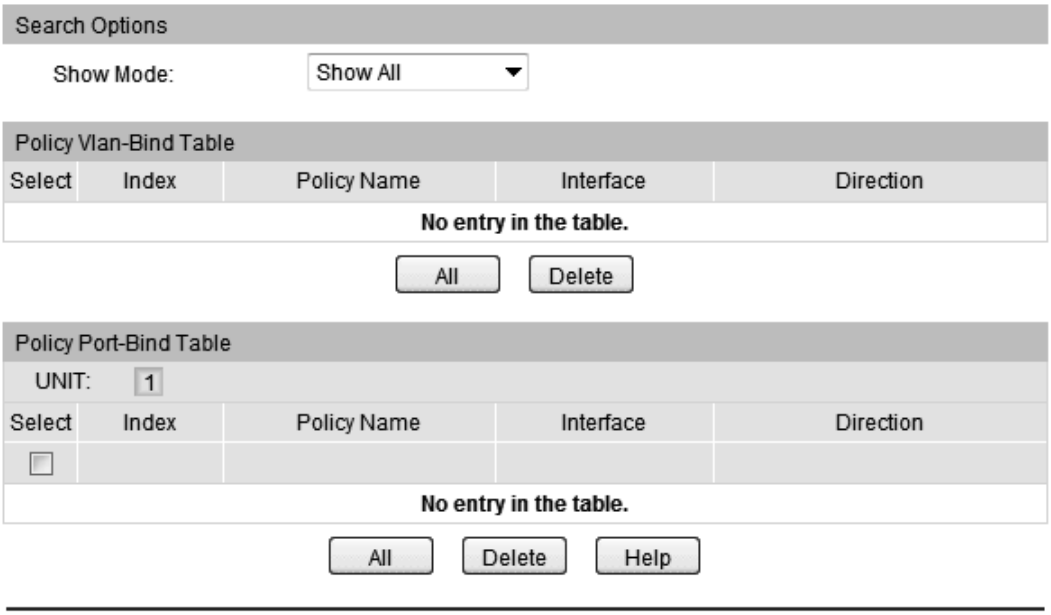


Figure 13-17 Binding Table

The following entries are displayed on this screen:

- **Search Option**

  Show Mode: Select a show mode appropriate to your needs.

- **Policy VLAN-Bind Table**

  Select: Select the desired entry to delete the corresponding binding policy.

  Index: Displays the index of the binding policy.

  Policy Name: Displays the name of the binding policy.

  Interface: Displays the port number or VLAN ID bound to the policy.

  Direction: Displays the binding direction.

- **Policy Port-Bind Table**

Select: Select the desired entry to delete the corresponding binding policy.

Index: Displays the index of the binding policy.

Policy Name: Displays the name of the binding policy.

Interface: Displays the port number or VLAN ID bound to the policy.

Direction: Displays the binding direction.

13.5.2 Port Binding

On this page you can bind a policy to a port.

Choose the menu **ACL→ACL Binding→Port Binding** to load the following page.

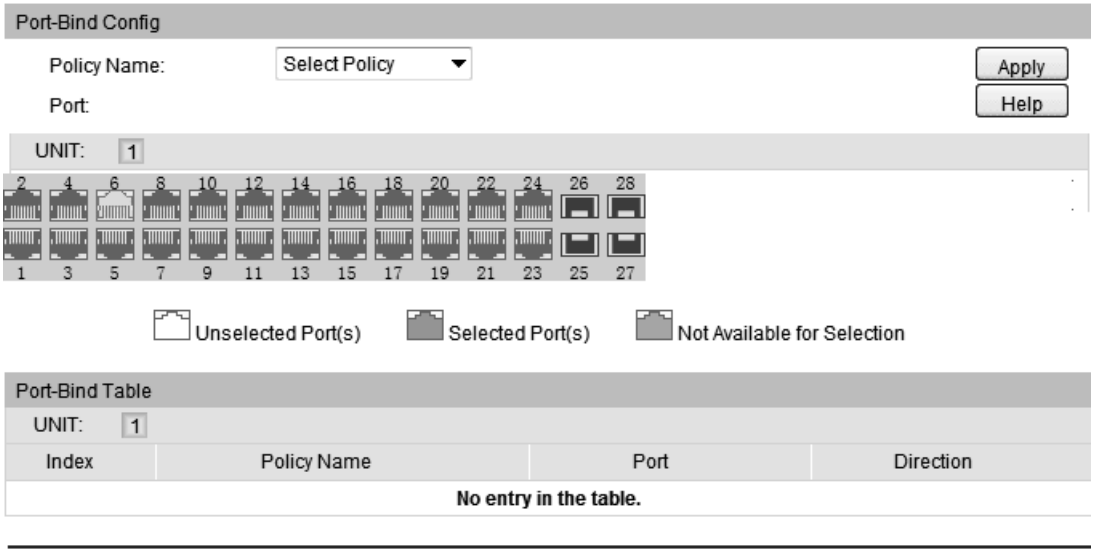


Figure 13-18 Bind the policy to the port

The following entries are displayed on this screen:

- **Port-Bind Config**

Policy Name: Select the name of the policy you want to bind.

Port: Select the number of the port you want to bind.

- **Port-Bind Table**

Index: Displays the index of the binding policy.

Policy Name: Displays the name of the binding policy.

Port: Displays the number of the port bound to the corresponding policy.

Direction: Displays the binding direction.

13.5.3 VLAN Binding

On this page you can bind a policy to a VLAN.

Choose the menu **ACL→Policy Binding→VLAN Binding** to load the following page.

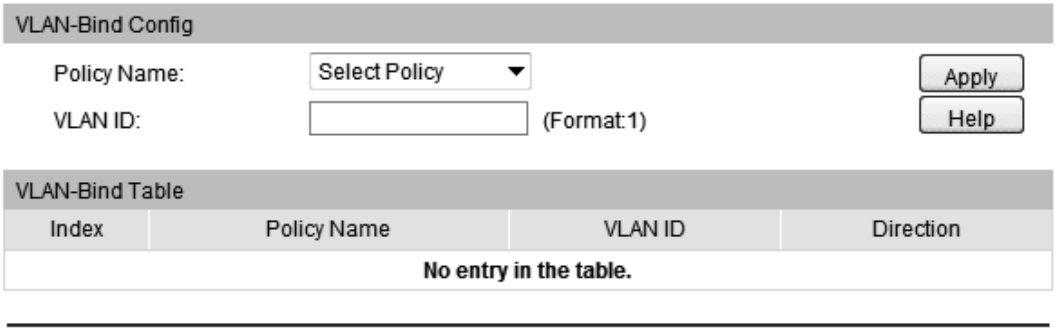


Figure 13-19 Bind the policy to the VLAN

The following entries are displayed on this screen:

- **VLAN-Bind Config**

  Policy Name: Select the name of the policy you want to bind.

  VLAN ID: Enter the ID of the VLAN you want to bind.

- **VLAN-Bind Table**

  Index: Displays the index of the binding policy.

  Policy Name: Displays the name of the binding policy.

  VLAN ID: Displays the ID of the VLAN bound to the corresponding policy.

  Direction: Displays the binding direction.

Configuration Procedure:

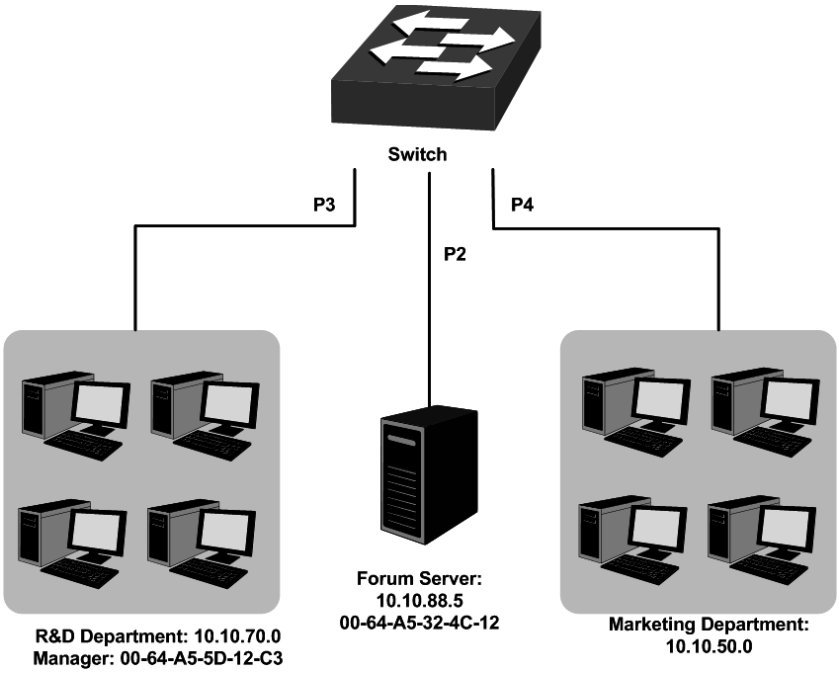
Step	Operation	Description
1	Configure ACL rules	Required. On **ACL→ACL Config** configuration pages, configure ACL rules to match packets.
2	Configure Policy	Required. On **ACL→Policy Config** configuration pages, configure the policy to control the data packets those match the corresponding ACL rules.
3	Bind the policy to the port/VLAN	Required. On **ACL→Policy Binding** configuration pages, bind the policy to the port/VLAN to make the policy effective on the corresponding port/VLAN.

13.6 Application Example for ACL

➢ **Network Requirements**

1. The manager of the R&D department can access to the forum of the company and the Internet without any forbiddance. The MAC address of the manager is 00-64-A5-5D-12-C3.
2. The staff of the R&D department cannot access to the Internet but can visit the forum.
3. The staff of the marketing department can access to the Internet but cannot visit the forum.
4. The R&D department and marketing department cannot communicate with each other.

➢ **Network Diagram**



Configuration Procedure

Step	Operation	Description
1	Configure for requirement 1	On **ACL→ACL Config→ACL Create** page, create ACL 11. On **ACL→ACL Config→MAC ACL** page, select ACL 11, create Rule 1, configure the operation as Permit, configure the S-MAC as 00-64-A5-5D-12-C3 and mask as FF-FF-FF-FF-FF-FF. On **ACL→Policy Config→Policy Create** page, create a policy named manager. On **ACL→Policy Config→Action Create** page, add ACL 11 to Policy manager. On **ACL→Policy Binding→Port Binding** page, select Policy manager to bind to port 3.

Step	Operation	Description
2	Configure for requirement 2 and 4	On **ACL→ACL Config→ACL Create** page, create ACL 500. On **ACL→ACL Config→Standard-IP ACL** page, select ACL 500, create Rule 1, configure operation as Deny, configure S-IP as 10.10.70.0 and mask as 255.255.255.0, configure D-IP as 10.10.50.0 and mask as 255.255.255.0. On **ACL→ACL Config→Standard-IP ACL** page, select ACL 500, create Rule 2, configure operation as Deny, configure S-IP as 10.10.70.0 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255. On **ACL→ACL Config→Standard-IP ACL** page, select ACL 500, create Rule 3, configure operation as Permit, configure S-IP as 10.10.70.0 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255. On **ACL→Policy Config→Policy Create** page, create a policy named limit1. On **ACL→Policy Config→Action Create** page, add ACL 500 to Policy limit1. On **ACL→Policy Binding→Port Binding** page, select Policy limit1 to bind to port 3.
3	Configure for requirement 3 and 4	On **ACL→ACL Config→ACL Create** page, create ACL 501. On **ACL→ACL Config→Standard-IP ACL** page, select ACL 501, create Rule 4, configure operation as Deny, configure S-IP as 10.10.50.0 and mask as 255.255.255.0, configure D-IP as 10.10.70.0 and mask as 255.255.255.0. On **ACL→ACL Config→Standard-IP ACL** page, select ACL 501, create Rule 5, configure operation as Deny, configure S-IP as 10.10.50.0 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255. On **ACL→Policy Config→Policy Create** page, create a policy named limit2. On **ACL→Policy Config→Action Create** page, add ACL 501 to Policy limit2. On **ACL→Policy Binding→Port Binding** page, select Policy limit2 to bind to port 4.

Return to CONTENTS

Chapter 14 Network Security

Network Security module is to provide the multiple protection measures for the network security, including five submenus: **IP-MAC Binding**, **IPv6-MAC Binding**, **DHCP Snooping**, **DHCPv6 Snooping**, **ARP Inspection**, **ND Detection**, **IP Source Guard, DoS Defend**, **802.1X**, **PPPoE** and **AAA**. Please configure the functions appropriate to your need.

14.1 IP-MAC Binding

The IP-MAC Binding function allows you to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together. Basing on the IP-MAC binding table, ARP Inspection and IP Source Guard functions can control the network access and only allow the Hosts matching the bound entries to access the network.

The following three IP-MAC Binding methods are supported by the switch.

(1) Manually: You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

(2) Scanning: You can quickly get the information of the IP address, MAC address, VLAN ID and the connected port number of the Hosts in the LAN via the ARP Scanning function, and bind them conveniently. You are only requested to enter the IP address on the ARP Scanning page for the scanning.

(3) DHCP Snooping: You can use DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

These three methods are also considered as the sources of the IP-MAC Binding entries. The entries from various sources should be different from one another to avoid collision. Among the entries in collision, only the entry from the source with the highest priority will take effect. These three sources (Manual, Scanning and Snooping) are in descending order of priority.

The **IP-MAC Binding** function is implemented on the **Binding Table**, **Manual Binding** and **ARP Scanning** pages.

14.1.1 Binding Table

On this page, you can view the information of the bound entries.

Choose the menu **Network Security→IP-MAC Binding→Binding Table** to load the following page.

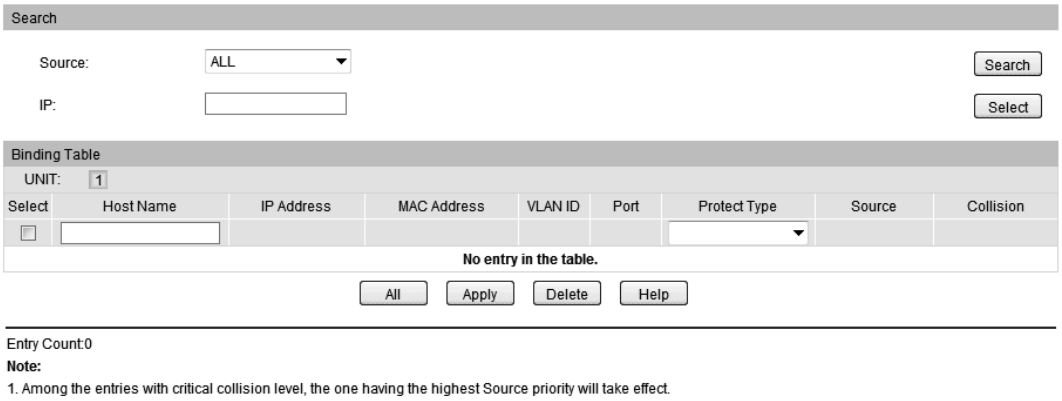


Figure 14-1 Binding Table

The following entries are displayed on this screen:

➢ **Search**

Source: Displays the Source of the entry.

- **All:** All the bound entries will be displayed.
- **Manual:** Only the manually added entries will be displayed.
- **Scanning:** Only the entries formed via ARP Scanning will be displayed.
- **Snooping:** Only the entries formed via DHCP Snooping will be displayed.

IP Select Click the Select button to quick-select the corresponding entry based on the IP address you entered.

➢ **Binding Table**

Select: Select the desired entry to modify the Host Name and Protect Type. It is multi-optional.

Host Name Displays the Host Name here.

IP Address Displays the IP Address of the Host.

MAC Address Displays the MAC Address of the Host.

VLAN ID: Displays the VLAN ID here.

Port: Displays the number of port connected to the Host.

Protect Type: Allows you to view and modify the Protect Type of the entry.

Source: Displays the Source of the entry.

Collision: Displays the Collision status of the entry.

- **Warning:** Indicates that the collision may be caused by

the MSTP function.

- **Critical:** Indicates that the entry has a collision with the other entries.

Note:

Among the entries with Critical collision level, the one with the highest Source priority will take effect.

14.1.2 Manual Binding

You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

Choose the menu **Network Security→IP-MAC Binding→Manual Binding** to load the following page.

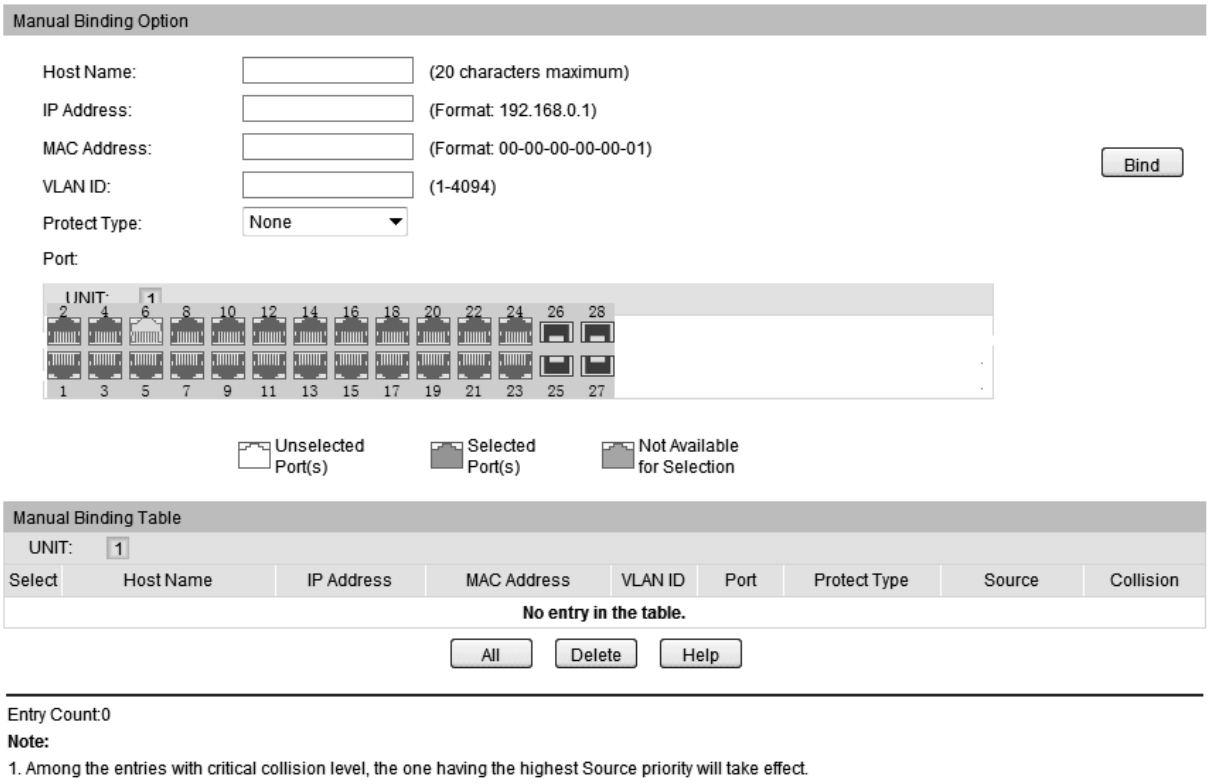


Figure 14-2 Manual Binding

The following entries are displayed on this screen:

➢ **Manual Binding Option**

Host Name: Enter the Host Name.

IP Address: Enter the IP Address of the Host.

MAC Address: Enter the MAC Address of the Host.

VLAN ID: Enter the VLAN ID.

Protect Type: Select the Protect Type for the entry.

Port: Select the number of port connected to the Host.

- **Manual Binding Table**

Select: Select the desired entry to be deleted. It is multi-optional.

Host Name: Displays the Host Name here.

IP Address: Displays the IP Address of the Host.

MAC Address: Displays the MAC Address of the Host.

VLAN ID: Displays the VLAN ID here.

Port: Displays the number of port connected to the Host.

Protect Type: Displays the Protect Type of the entry.

Source: Displays the source of the entry.

Collision: Displays the Collision status of the entry.

- **Warning:** Indicates that the collision may be caused by the MSTP function.
- **Critical:** Indicates that the entry has a collision with the other entries.

14.1.3 ARP Scanning

ARP (Address Resolution Protocol) is used to analyze and map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations correctly. IP address is the address of the Host on Network layer. MAC address, the address of the Host on Data link layer, is necessary for the packet to reach the very device. So the destination IP address carried in a packet need to be translated into the corresponding MAC address.

ARP functions to translate the IP address into the corresponding MAC address and maintain an ARP Table, where the latest used IP address-to-MAC address mapping entries are stored. When the Host communicates with a strange Host, ARP works as the following figure shown.

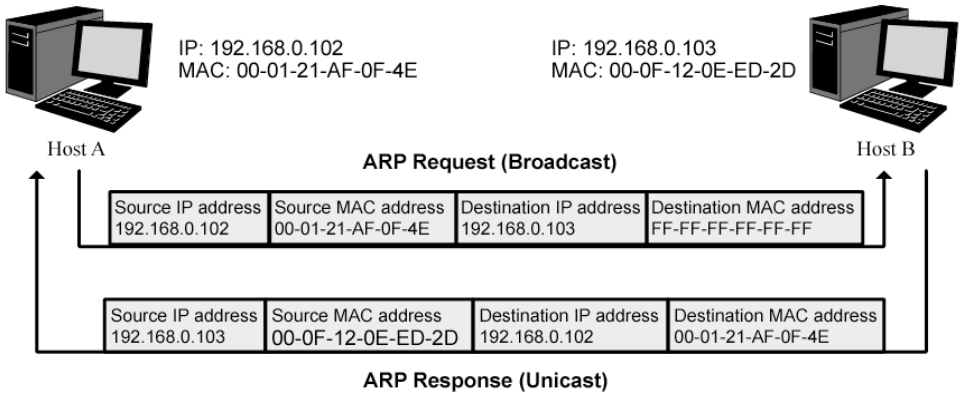


Figure 14-3 ARP Implementation Procedure

(1) Suppose there are two hosts in the LAN: Host A and Host B. To send a packet to Host B, Host A checks its own ARP Table first to see if the ARP entry related to the IP address of Host B exists. If yes, Host A will directly send the packets to Host B. If the corresponding MAC address is not found in the ARP Table, Host A will broadcast ARP request packet, which contains the IP address of Host B, the IP address of Host A, and the MAC address of Host A, in the LAN.

(2) Since the ARP request packet is broadcasted, all hosts in the LAN can receive it. However, only the Host B recognizes and responds to the request. Host B sends back an ARP reply packet to Host A, with its MAC address carried in the packet.

(3) Upon receiving the ARP reply packet, Host A adds the IP address and the corresponding MAC address of Host B to its ARP Table for the further packets forwarding.

ARP Scanning function enables the switch to send the ARP request packets of the specified IP field to the Hosts in the LAN or VLAN. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN and the connected port number of the Host by analyzing the packet and bind them conveniently.

Choose the menu **Network Security→IP-MAC Binding→ARP Scanning** to load the following page.

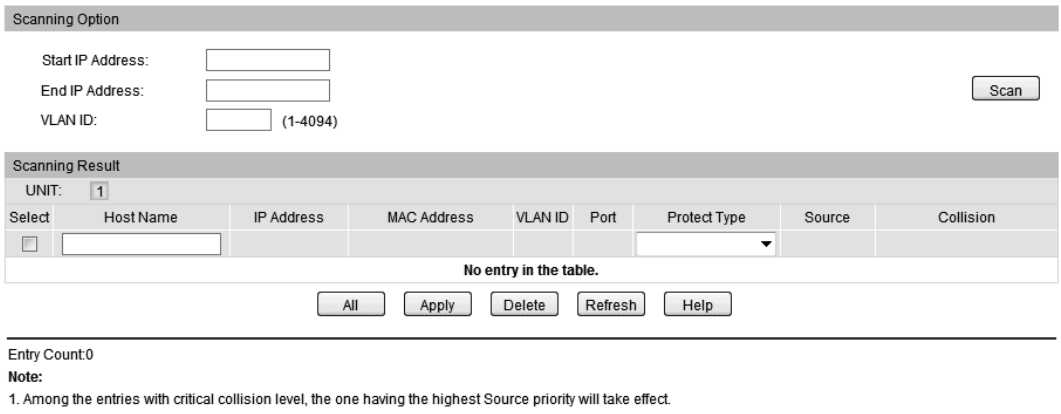


Figure 14-4 ARP Scanning

The following entries are displayed on this screen:

➢ **Scanning Option**

Start IP Address: Specify the Start IP Address.

End IP Address: Specify the End IP Address.

VLAN ID: Enter the VLAN ID.

Scan: Click the **Scan** button to scan the Hosts in the LAN.

➢ **Scanning Result**

Select: Select the desired entry to be deleted or bound. It is multi-optional.

Host Name:	Displays the Host Name here.
IP Address:	Displays the IP Address of the Host.
MAC Address:	Displays the MAC Address of the Host.
VLAN ID:	Displays the VLAN ID here.
Port:	Displays the number of port connected to the Host.
Protect Type:	Displays the Protect Type of the entry.
Source:	Displays the source of the entry.
Collision:	Displays the Collision status of the entry. • **Warning:** Indicates that the collision may be caused by the MSTP function. • **Critical:** Indicates that the entry has a collision with the other entries.

14.2 IPv6-MAC Binding

The IPv6-MAC Binding function allows you to bind the IPv6 address, MAC address, VLAN ID and the connected Port number of the Host together. Basing on the IPv6-MAC binding table, ND detection and IPv6 Source Guard functions can control the network access and only allow the Hosts matching the bound entries to access the network.

The following three IPv6-MAC Binding methods are supported by the switch.

(1) Manually: You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

(2) ND Snooping: You can use ND Snooping functions to monitor the process of the duplication address detection, And record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

(3) DHCP Snooping: You can use DHCPv6 Snooping functions to monitor the process of the Host obtaining the IPv6 address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

These three methods are also considered as the sources of the IPv6-MAC Binding entries. The entries from various sources should be different from one another to avoid collision. Among the entries in collision, only the entry from the source with the highest priority will take effect. These three sources (Manual, DHCP Snooping, ND Snooping) are in descending order of priority.

The IPv6-MAC Binding function is implemented on the **Binding Table**, **Manual Binding** and **ND Snooping** pages.

14.2.1 Binding Table

On this page, you can view the information of the IPv6-related bound entries.

Choose the menu **Network Security→IPv6-MAC Binding→Binding Table** to load the following page.

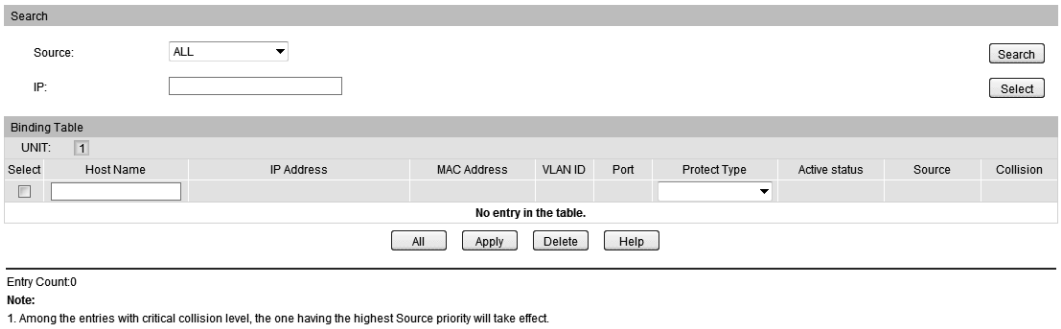


Figure 14-5 Binding Table

The following entries are displayed on this screen:

➢ **Search**

Source: Displays the Source of the entry.

- **All:** All the bound entries will be displayed.
- **Manual:** Only the manually added entries will be displayed.
- **ND Snooping:** Only the entries generated via ND snooping will be displayed.
- **DHCP Snooping:** Only the entries generated via DHCP Snooping will be displayed.

IP Select Click the Select button to quick-select the corresponding entry based on the IPv6 address you entered.

➢ **Binding Table**

Select: Select the desired entry to modify the Host Name and Protect Type. It is multi-optional.

Host Name Displays the Host Name here.

IP Address Displays the IPv6 Address of the Host.

MAC Address Displays the MAC Address of the Host.

VLAN ID: Displays the VLAN ID here.

Port: Displays the number of port connected to the Host.

Protect Type: Allows you to view and modify the Protect Type of the entry.

Active Status: Displays the active status of the entry.

Source: Displays the Source of the entry.

Collision: Displays the Collision status of the entry.

- **Warning:** Indicates that the collision may be caused by the MSTP function.
- **Critical:** Indicates that the entry has a collision with the other entries.

Note:

Among the entries with Critical collision level, the one with the highest Source priority will take effect.

14.2.2 Manual Binding

You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

Choose the menu **Network Security→IPv6-MAC Binding→Manual Binding** to load the following page.

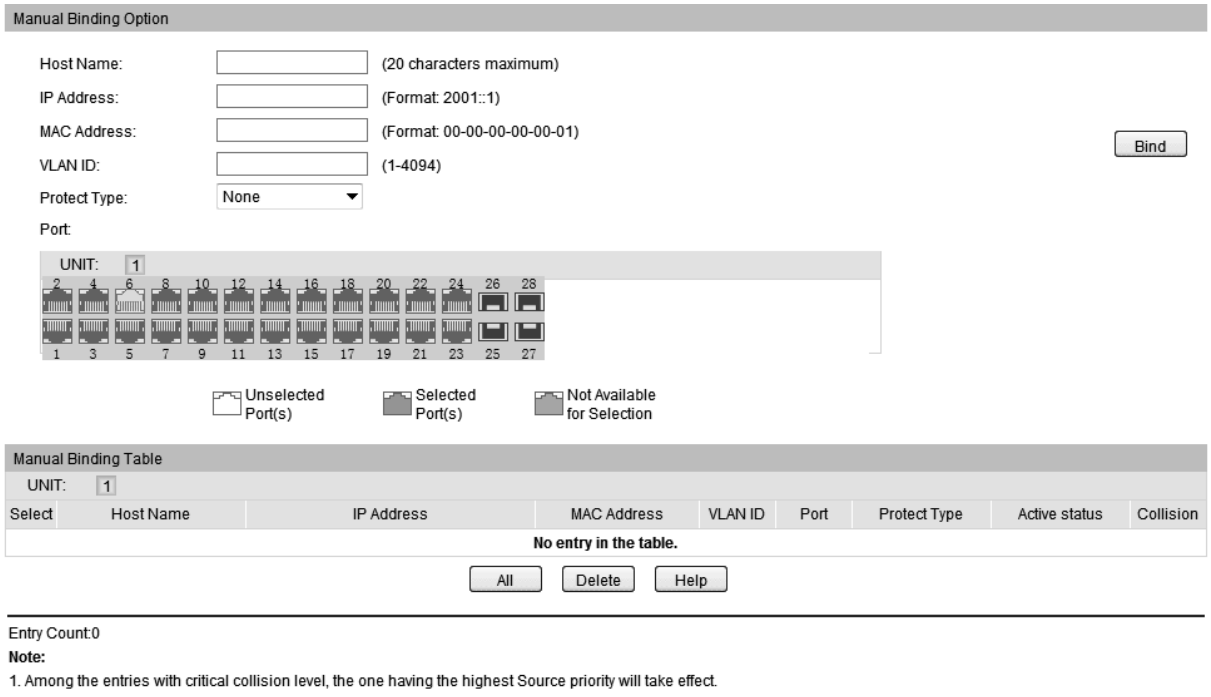


Figure 14-6 Manual Binding

The following entries are displayed on this screen:

➢ **Manual Binding Option**

Host Name: Enter the Host Name.

IP Address: Enter the IPv6 Address of the Host.

MAC Address: Enter the MAC Address of the Host.

VLAN ID: Enter the VLAN ID.

Protect Type: Select the Protect Type for the entry.

Port: Select the number of port connected to the Host.

➢ **Manual Binding Table**

Select: Select the desired entry to be deleted. It is multi-optional.

Host Name: Displays the Host Name here.

IP Address: Displays the IP Address of the Host.

MAC Address: Displays the MAC Address of the Host.

VLAN ID: Displays the VLAN ID here.

Port: Displays the number of port connected to the Host.

Protect Type: Displays the Protect Type of the entry.

Active Status: Displays the active status of the entry.

Collision: Displays the Collision status of the entry.

- **Warning:** Indicates that the collision may be caused by the MSTP function.
- **Critical:** Indicates that the entry has a collision with the other entries.

14.2.3 ND Snooping

ND snooping maintains an ND snooping table using the DAD NS messages in IPv6. ND snooping entries in this table is used to:

- Cooperate with the IPv6-MAC binding.
- Cooperate with the ND detection feature.
- Cooperate with the IPv6 Source Guard feature.

1. Creating an ND snooping entry

The switch only uses received DAD NS messages to create ND snooping entries.

2. Updating an ND snooping entry

Upon receiving an ND packet, the switch searches the ND snooping table for an entry containing the source IPv6 address of the packet. The switch matches the ND packet's MAC address and the receiving port against that in the entry.

- If both of them match those in the entry, the switch updates the aging time in this ND snooping entry.
- If neither of them matches the entry, the switch initiates a verification process.

1)The switch checks the validity of the existing ND snooping entry.

The switch sends out an NS message according to the ND snooping entry. If a corresponding NA message (whose source IPv6 address, source MAC address, receiving port, and source VLAN are consistent with those of the existing entry) is received, the device updates the aging time of the existing entry. If no corresponding NA message is received within one second after the NS message is sent, the device starts to check the validity of the received ND packet.

2)The switch checks the validity of the received ND packet.

The switch sends out an NS message to verify the reachability of the ND packet (marked as packet A). The NS message's destination IPv6 address is specified as the source IPv6 address of packet A. If a corresponding NA message (whose source IPv6 address, source MAC address, receiving port, and source VLAN are consistent with those of packet A) is received, the switch updates the existing entry. If no corresponding NA message is received within one second after the NS message is sent, the switch deletes the entry.

3. Aging out an ND snooping entry

An ND snooping entry is aged out after 120 minutes. If an ND snooping entry is not updated within 60 minutes, the switch initiates a verification. The switch sends out an NS message including the IPv6 address of the ND snooping entry.

- If a corresponding NA message is received (the source IPv6 address, source MAC address, receiving port, and source VLAN are consistent with those of the existing entry), the switch updates the aging time of the existing entry.
- If no corresponding NA message is received within one second after the NS message is sent out, the switch removes the entry when the timer expires.

Choose the menu **Network Security→IPv6-MAC Binding→ND Snooping** to load the following page.

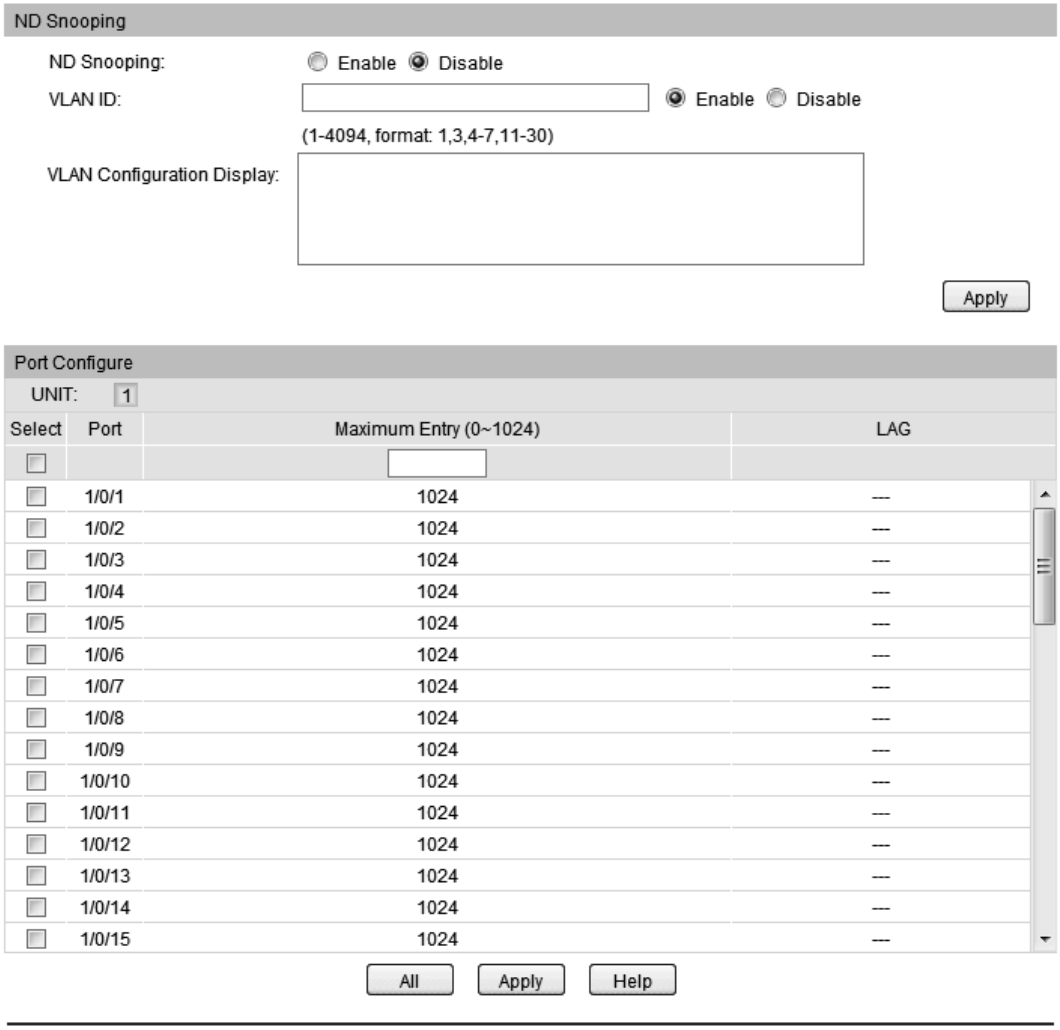


Figure 14-7 ARP Scanning

The following entries are displayed on this screen:

- **ND Snooping**

  ND Snooping: Enable/Disable the ND Snooping function globally.

  VLAN ID: Enable/Disable the ND Snooping function in the specified VLAN.

  VLAN Configuration Display: Displays the VLANs with ND Snooping function enabled.

- **Port Configure**

  UNIT:1: Click **1** to configure the physical ports.

  Select: Select your desired port for configuration. It is multi-optional.

  Port: Displays the number of port.

Maximum Entry:	Configure the max ND binding entries a port can learn via ND snooping.
LAG:	Displays the LAG which the port belongs to.

14.3 DHCP Snooping

Nowadays, the network is getting larger and more complicated. The amount of the PCs always exceeds that of the assigned IP addresses. The wireless network and the laptops are widely used and the locations of the PCs are always changed. Therefore, the corresponding IP address of the PC should be updated with a few configurations. DHCP (Dynamic Host Configuration Protocol), the network configuration protocol optimized and developed basing on the BOOTP, functions to solve the above mentioned problems.

➢ **DHCP Working Principle**

DHCP works via the "Client/Server" communication mode. The Client applies to the Server for configuration. The Server assigns the configuration information, such as the IP address, to the Client, so as to reach a dynamic employ of the network source. A Server can assign the IP address for several Clients, which is illustrated in the following figure.

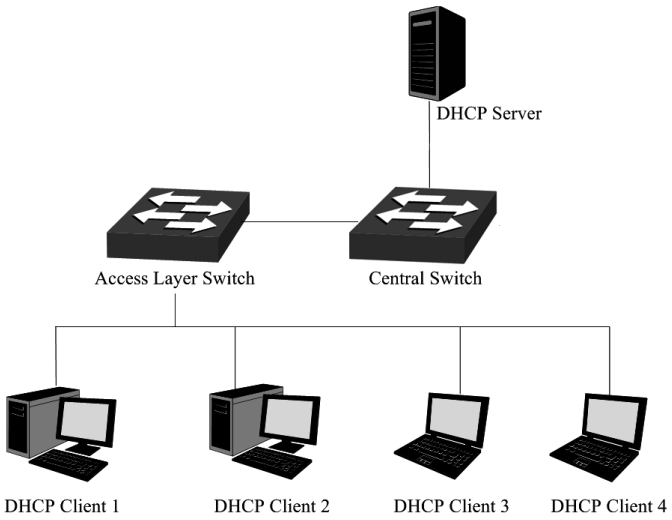


Figure 14-8 Network diagram for DHCP-snooping implementation

For different DHCP Clients, DHCP Server provides three IP address assigning methods:

(1) Manually assign the IP address: Allows the administrator to bind the static IP address to the specific Client (e.g.: WWW Server) via the DHCP Server.

(2) Automatically assign the IP address: DHCP Server assigns the IP address without an expiration time limitation to the Clients.

(3) Dynamically assign the IP address: DHCP Server assigns the IP address with an expiration time. When the time for the IP address expired, the Client should apply for a new one.

The most Clients obtain the IP addresses dynamically, which is illustrated in the following figure.

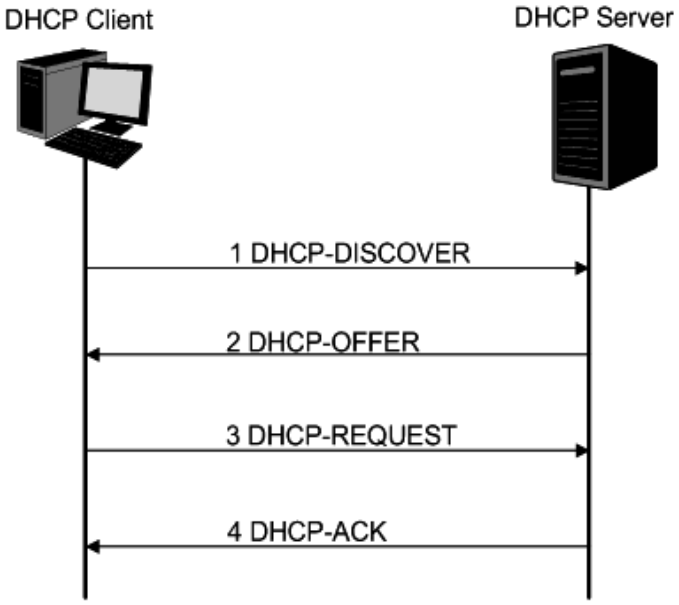


Figure 14-9 Interaction between a DHCP client and a DHCP server

(1) **DHCP-DISCOVER Stage:** The Client broadcasts the DHCP-DISCOVER packet to find the DHCP Server.

(2) **DHCP-OFFER Stage:** Upon receiving the DHCP-DISCOVER packet, the DHCP Server selects an IP address from the IP pool according to the assigning priority of the IP addresses and replies to the Client with DHCP-OFFER packet carrying the IP address and other information.

(3) **DHCP-REQUEST Stage:** In the situation that there are several DHCP Servers sending the DHCP-OFFER packets, the Client will only respond to the first received DHCP-OFFER packet and broadcast the DHCP-REQUEST packet which includes the assigned IP address of the DHCP-OFFER packet.

(4) **DHCP-ACK Stage:** Since the DHCP-REQUEST packet is broadcasted, all DHCP Servers on the network segment can receive it. However, only the requested Server processes the request. If the DHCP Server acknowledges assigning this IP address to the Client, it will send the DHCP-ACK packet back to the Client. Otherwise, the Server will send the DHCP-NAK packet to refuse assigning this IP address to the Client.

➢ **Option 82**

The DHCP packets are classified into 8 types with the same format basing on the format of BOOTP packet. The difference between DHCP packet and BOOTP packet is the Option field. The Option field of the DHCP packet is used to expand the function, for example, the DHCP can transmit the control information and network parameters via the Option field, so as to assign the IP address to the Client dynamically. For the details of the DHCP Option, please refer to RFC 2132.

Option 82 records the location of the DHCP Client. Upon receiving the DHCP-REQUEST packet, the switch adds the Option 82 to the packet and then transmits the packet to DHCP Server. Administrator can be acquainted with the location of the DHCP Client via Option 82 so as to locate the DHCP Client for fulfilling the security control and account management of Client. The Server supported Option 82 also can set the distribution policy of IP addresses and the other parameters according to the Option 82, providing more flexible address distribution way.

Option 82 can contain 255 sub-options at most. If Option 82 is defined, at least a sub-option should be defined. This switch supports two sub-options: Circuit ID and Remote ID. Since there is no universal standard about the content of Option 82, different manufacturers define the sub-options of Option 82 to their need. For this switch, the sub-options are defined as the following: The Circuit ID is defined to be the number of the port which receives the DHCP Request packets and its VLAN number. The Remote ID is defined to be the MAC address of DHCP Snooping device which receives the DHCP Request packets from DHCP Clients.

- **DHCP Cheating Attack**

During the working process of DHCP, generally there is no authentication mechanism between Server and Client. If there are several DHCP servers in the network, network confusion and security problem will happen. The common cases incurring the illegal DHCP servers are the following two:

(1) It's common that the illegal DHCP server is manually configured by the user by mistake.

(2) Hacker exhausted the IP addresses of the normal DHCP server and then pretended to be a legal DHCP server to assign the IP addresses and the other parameters to Clients. For example, hacker used the pretended DHCP server to assign a modified DNS server address to users so as to induce the users to the evil financial website or electronic trading website and cheat the users of their accounts and passwords. The following figure illustrates the DHCP Cheating Attack implementation procedure.

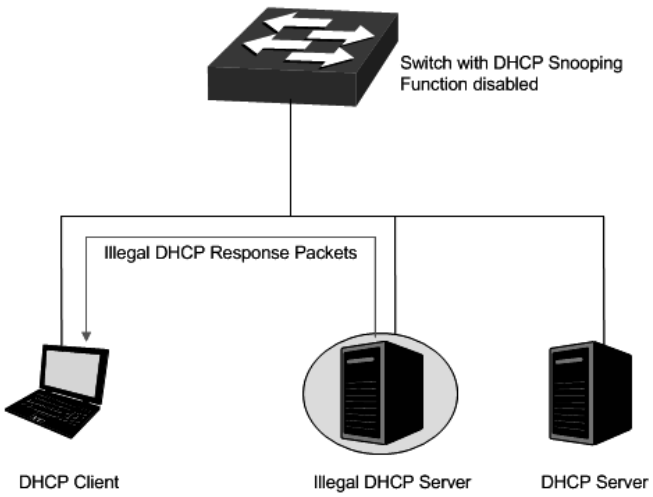


Figure 14-10 DHCP Cheating Attack Implementation Procedure

DHCP Snooping feature only allows the port connected to the DHCP Server as the trusted port to forward all types of DHCP packets and thereby ensures that users get proper IP addresses. DHCP Snooping is to monitor the process of the Host obtaining the IP address from DHCP

server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding. The bound entry can cooperate with the ARP Inspection, IP Source Guard and the other security protection features. DHCP Snooping feature prevents the network from the DHCP Server Cheating Attack by discarding the DHCP response packets on the distrusted port, so as to enhance the network security.

14.3.1 Global Config

Choose the menu **Network Security→DHCP Snooping→Global Config** to load the following page.

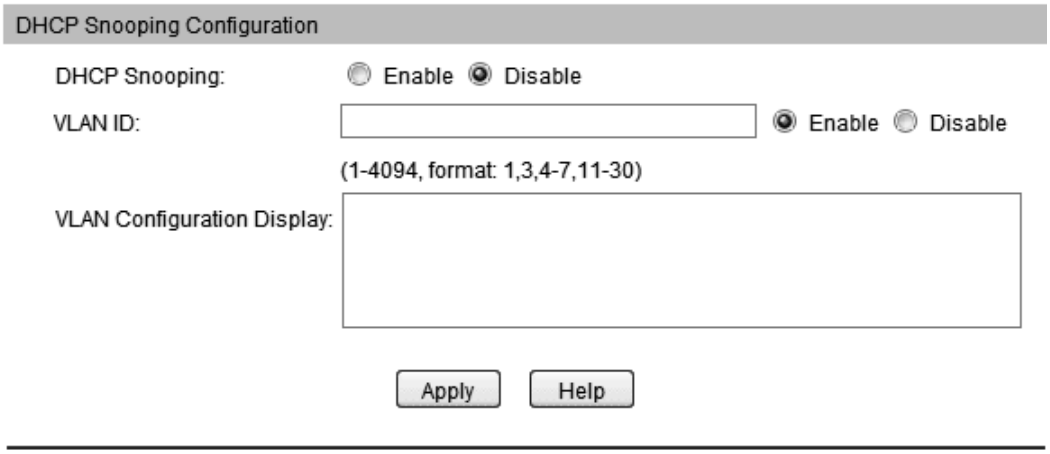


Figure 14-11 DHCP Snooping

The following entries are displayed on this screen:

- **DHCP Snooping Configuration**

DHCP Snooping:	Enable/Disable the DHCP Snooping function globally.
VLAN ID:	Enable/Disable the DHCP Snooping function in the specified VLAN.
VLAN Configuration Display:	Display the VLANs which enable DHCP Snooping function.

14.3.2 Port Config

Choose the menu **Network Security→DHCP Snooping→Port Config** to load the following page.

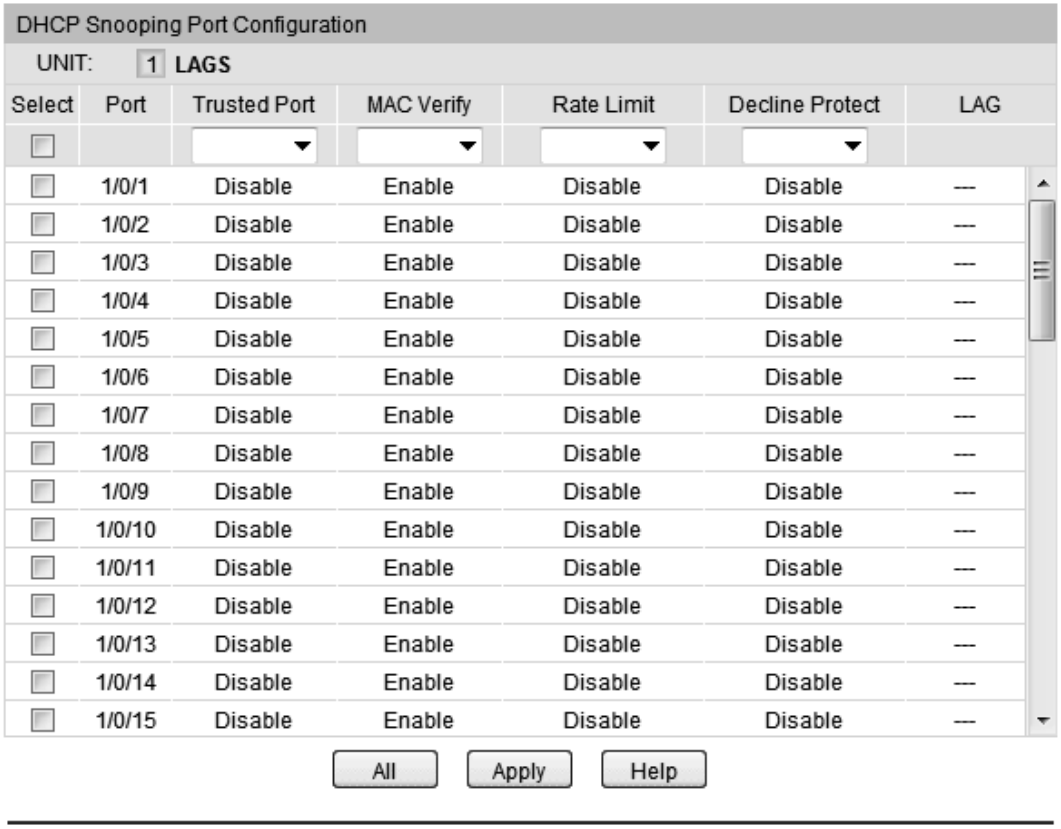


Figure 14-12 DHCP Snooping

➢ **DHCP Snooping Port Configuration**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select your desired port for configuration. It is multi-optional.

Port: Displays the port number.

Trusted Port: Select Enable/Disable the port to be a Trusted Port. Only the Trusted Port can receive the DHCP packets from DHCP servers.

MAC Verify: Select Enable/Disable the MAC Verify feature. There are two fields of the DHCP packet containing the MAC address of the Host. The MAC Verify feature is to compare the two fields and discard the packet if the two fields are different.

Rate Limit: Select the value to specify the maximum amount of DHCP messages that can be forwarded by the switch of this port per second. The excessive DHCP packets will be discarded.

Decline Protect: Select the value to specify the maximum amount of DHCP decline packets that can be forwarded by the switch of this port per second. The excessive DHCP decline packets will be discarded.

LAG: Displays the LAG to which the port belongs.

14.3.3 Option 82 Config

The switch can propagate the control information and the network parameters via the Option 82 field to provide more information for the Host. When the DHCP option 82 feature is enabled on the switch, a host is identified by the switch port through which it connects to the network (in addition to its MAC address). The DHCP option 82 feature is supported only when DHCP snooping is globally enabled.

Choose the menu **Network Security→DHCP Snooping→Option 82 Config** to load the following page.

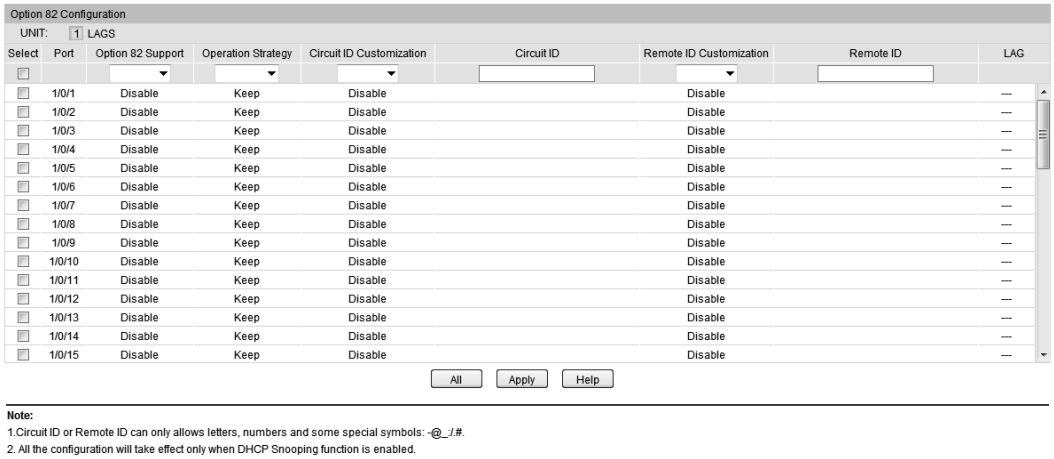


Figure 14-13 Option 82 Config

➢ **Option 82 Configuration**

UNIT:1/LAGS: Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.

Select: Select your desired port for configuration. It is multi-optional.

Port: Displays the port number.

Option 82 Support: Enable/Disable the Option 82 feature.

Operation Strategy: Select the operation for the existed Option 82 field of the DHCP request packets from the Host. The option 82 field in DHCP reply packets will be remove when the option 82

feature is enable，no matter which operation is configured for the existed option 82 filed.

- **Keep:** Indicates to keep the Option 82 field of the packets.
- **Replace:** Indicates to replace the Option 82 field of the packets with the switch defined one.
- **Drop:** Indicates to discard the packets including the Option 82 field.

Circuit ID Customization: Enable or disable the switch to define the Option 82 sub-option Circuit ID field. With Disable selected, configure VLAN ID and port number from which the packet is received as the circuit ID default value.

Circuit ID: Enter the sub-option Circuit ID for the customized Option 82 field.

Remote ID Customization: Enable or disable the switch to define the Option 82 sub-option Remote ID field. With Disable selected, configure the switch system MAC address as the remote ID default value.

Remote ID: Enter the sub-option Remote ID for the customized Option 82.

LAG: Displays the LAG to which the port belongs.

14.4 DHCPv6 Snooping

DHCPv6 Snooping functions to monitor the process of the host obtaining the IPv6 address from the DHCPv6 server. DHCPv6 Snooping records the IPv6 address, MAC address, VLAN and the connected port number of the host for automatic binding.

Choose the menu **Network Security→DHCPv6 Snooping→DHCPv6 Snooping** to load the following page.

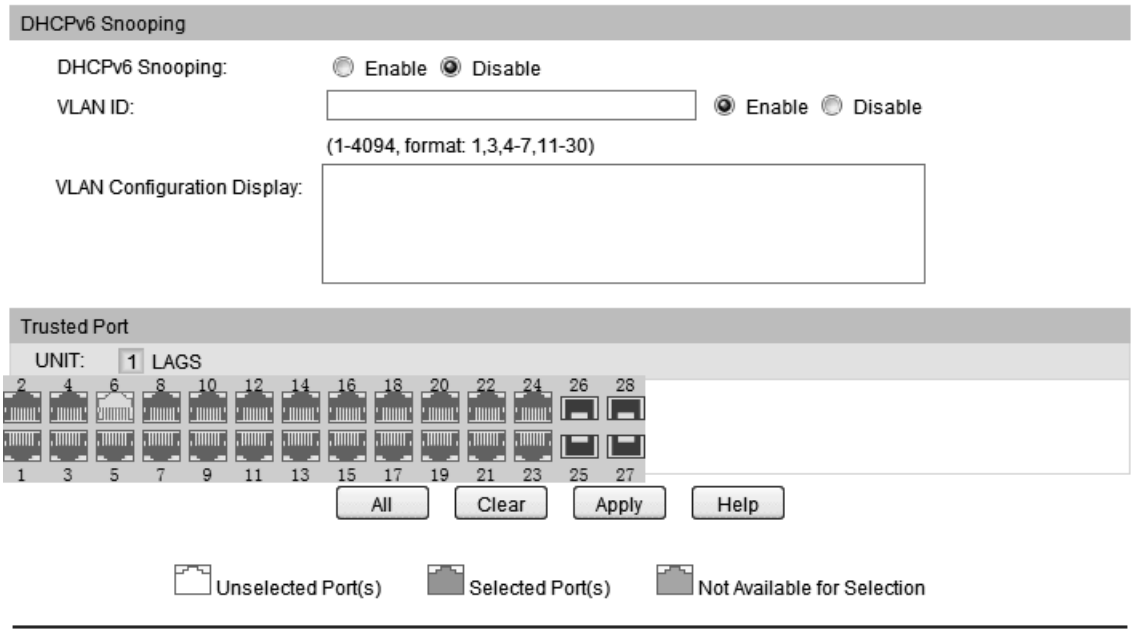


Figure 14-14 DHCPv6 Snooping

- **DHCPV6 Snooping**

DHCPv6 Snooping: Enable/Disable the DHCPv6 Snooping function globally.

VLAN ID: Enable/Disable the DHCPv6 Snooping function in the specified VLAN.

VLAN Configuration Display: Displays the VLANs with DHCPv6 Snooping function enabled.

- **Trusted Port**

UNIT:1/LAGS: Select the desired unit or LAGS for configuration.

Trusted Port: Select the port to be a Trusted Port. Only the Trusted Port can forward the DHCPv6 packets from DHCPv6 servers.

14.5 ARP Inspection

According to the ARP Implementation Procedure stated in 14.1.3 ARP Scanning, it can be found that ARP protocol can facilitate the Hosts in the same network segment to communicate with one another or access to external network via Gateway. However, since ARP protocol is implemented with the premise that all the Hosts and Gateways are trusted, there are high security risks during ARP Implementation Procedure in the actual complex network. Thus, the cheating attacks against ARP, such as imitating Gateway, cheating Gateway, cheating terminal Hosts and ARP Flooding Attack, frequently occur to the network, especially to the large network such as campus network. The following part will simply introduce these ARP attacks.

➢ **Imitating Gateway**

The attacker sends the MAC address of a forged Gateway to Host, and then the Host will automatically update the ARP table after receiving the ARP response packets, which causes that the Host cannot access the network normally. The ARP Attack implemented by imitating Gateway is illustrated in the following figure.

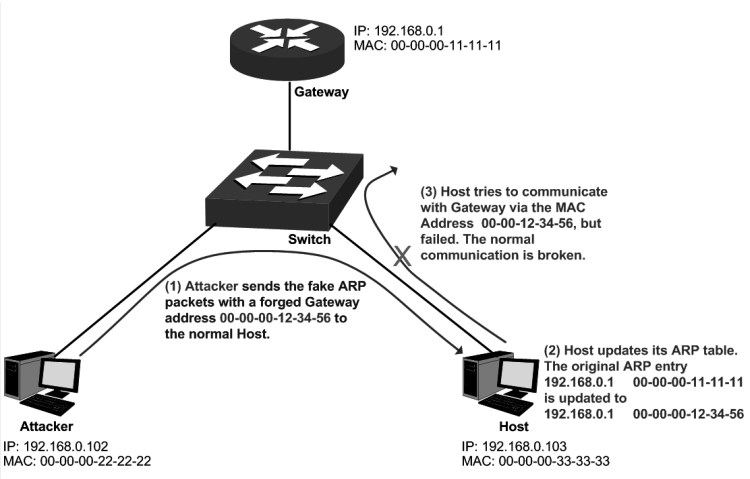


Figure 14-15 ARP Attack - Imitating Gateway

As the above figure shown, the attacker sends the fake ARP packets with a forged Gateway address to the normal Host, and then the Host will automatically update the ARP table after receiving the ARP packets. When the Host tries to communicate with Gateway, the Host will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

➢ **Cheating Gateway**

The attacker sends the wrong IP address-to-MAC address mapping entries of Hosts to the Gateway, which causes that the Gateway cannot communicate with the legal terminal Hosts normally. The ARP Attack implemented by cheating Gateway is illustrated in the following figure.

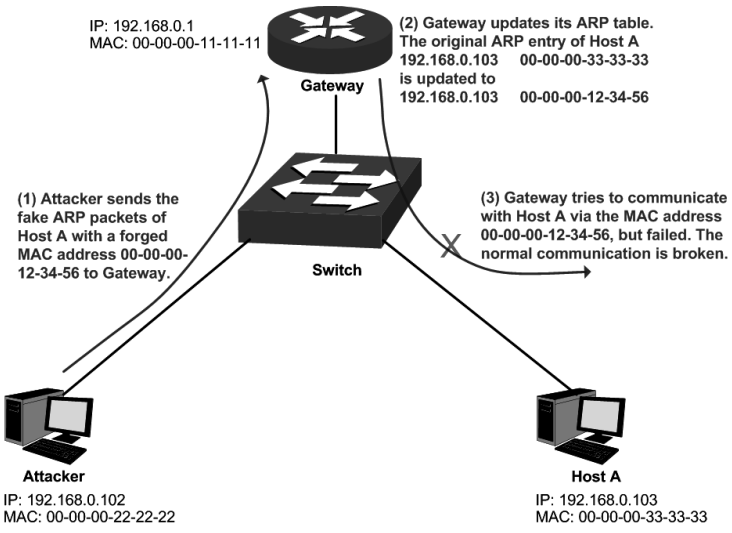


Figure 14-16 ARP Attack – Cheating Gateway

As the above figure shown, the attacker sends the fake ARP packets of Host A to the Gateway, and then the Gateway will automatically update its ARP table after receiving the ARP packets. When the Gateway tries to communicate with Host A in LAN, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

- **Cheating Terminal Hosts**

The attacker sends the false IP address-to-MAC address mapping entries of terminal Host/Server to another terminal Host, which causes that the two terminal Hosts in the same network segment cannot communicate with each other normally. The ARP Attack implemented by cheating terminal Hosts is illustrated in the following figure.

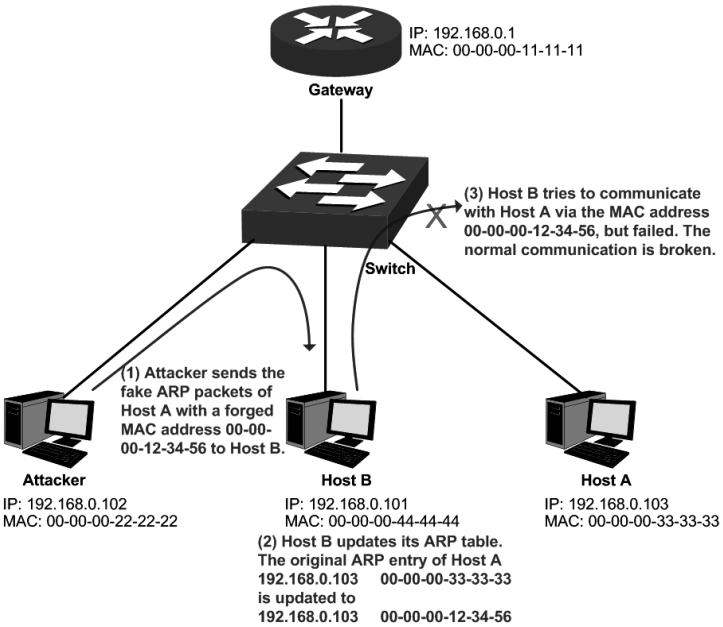


Figure 14-17 ARP Attack – Cheating Terminal Hosts

As the above figure shown, the attacker sends the fake ARP packets of Host A to Host B, and then Host B will automatically update its ARP table after receiving the ARP packets. When Host B tries to communicate with Host A, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

- **Man-In-The-Middle Attack**

The attacker continuously sends the false ARP packets to the Hosts in LAN so as to make the Hosts maintain the wrong ARP table. When the Hosts in LAN communicate with one another, they will send the packets to the attacker according to the wrong ARP table. Thus, the attacker can get and process the packets before forwarding them. During the procedure, the communication packets information between the two Hosts are stolen in the case that the Hosts were unaware of the attack. That is called Man-In-The-Middle Attack. The Man-In-The-Middle Attack is illustrated in the following figure.

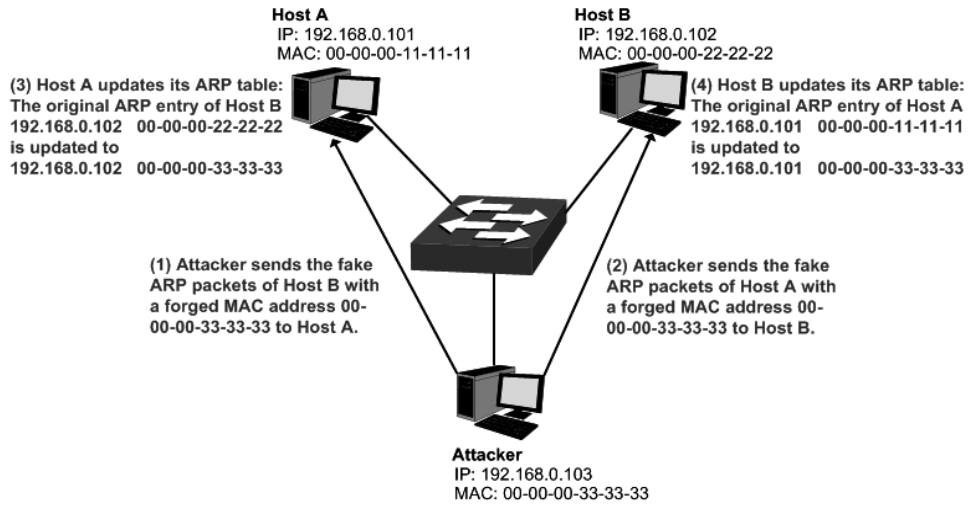


Figure 14-18 Man-In-The-Middle Attack

Suppose there are three Hosts in LAN connected with one another through a switch.

Host A: IP address is 192.168.0.101; MAC address is 00-00-00-11-11-11.

Host B: IP address is 192.168.0.102; MAC address is 00-00-00-22-22-22.

Attacker: IP address is 192.168.0.103; MAC address is 00-00-00-33-33-33.

1. First, the attacker sends the false ARP response packets.
2. Upon receiving the ARP response packets, Host A and Host B updates the ARP table of their own.
3. When Host A communicates with Host B, it will send the packets to the false destination MAC address, i.e. to the attacker, according to the updated ARP table.
4. After receiving the communication packets between Host A and Host B, the attacker processes and forwards the packets to the correct destination MAC address, which makes Host A and Host B keep a normal-appearing communication.
5. The attacker continuously sends the false ARP packets to the Host A and Host B so as to make the Hosts always maintain the wrong ARP table.

In the view of Host A and Host B, their packets are directly sent to each other. But in fact, there is a Man-In-The-Middle stolen the packets information during the communication procedure. This kind of ARP attack is called Man-In-The-Middle attack.

- **ARP Flooding Attack**

The attacker broadcasts a mass of various fake ARP packets in a network segment to occupy the network bandwidth viciously, which results in a dramatic slowdown of network speed. Meantime, the Gateway learns the false IP address-to-MAC address mapping entries from these ARP packets and updates its ARP table. As a result, the ARP table is fully occupied by the false entries and unable to learn the ARP entries of legal Hosts, which causes that the legal Hosts cannot access the external network.

The IP-MAC Binding function allows the switch to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together when the Host connects to the switch. Basing on the predefined IP-MAC Binding entries, the ARP Inspection functions to detect the ARP packets and filter the illegal ARP packet so as to prevent the network from ARP attacks.

The **ARP Inspection** function is implemented on the **ARP Detect**, **ARP Defend** and **ARP Statistics** pages.

14.5.1 ARP Detect

ARP Detect feature enables the switch to detect the ARP packets basing on the bound entries in the IP-MAC Binding Table and filter the illegal ARP packets, so as to prevent the network from ARP attacks, such as the Network Gateway Spoofing and Man-In-The-Middle Attack, etc.

Choose the menu **Network Security→ARP Inspection→ARP Detect** to load the following page.

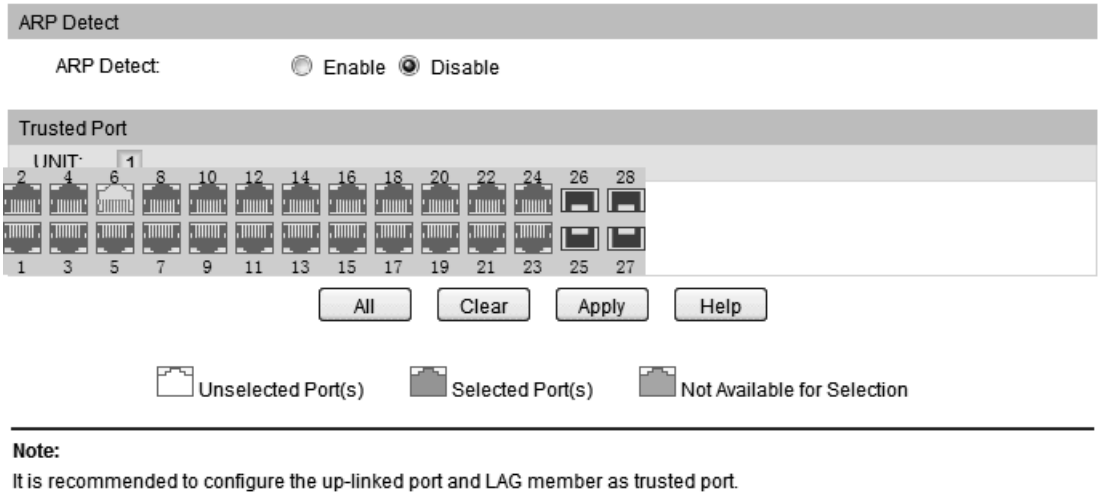


Figure 14-19 ARP Detect

The following entries are displayed on this screen:

- **ARP Detect**

  ARP Detect: Enable/Disable the ARP Detect function, and click the **Apply** button to apply.

- **Trusted Port**

  Trusted Port: Select the port for which the ARP Detect function is unnecessary as the Trusted Port. The specific ports, such as up-linked port, routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ARP Trusted Port before enabling the ARP Detect function.

Configuration Procedure:

Step	Operation	Description
1	Bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together.	Required. On the **IP-MAC Binding** page, bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together via Manual Binding, ARP Scanning or DHCP Snooping.
2	Enable the protection for the bound entry.	Required. On the **Network Security→IP-MAC Binding→Binding Table** page, specify a protect type for the corresponding bound entry.
3	Specify the trusted port.	Required. On the **Network Security→ARP Inspection→ARP Detect** page, specify the trusted port. The specific ports, such as up-linked port, routing port and LAG port, should be set as Trusted Port.
4	Enable ARP Detect feature.	Required. On the **Network Security→ARP Inspection→ARP Detect** page, enable the ARP Detect feature.

14.5.2 ARP Defend

With the ARP Defend enabled, the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP Attack flood.

Choose the menu **Network Security→ARP Inspection→ARP Defend** to load the following page.

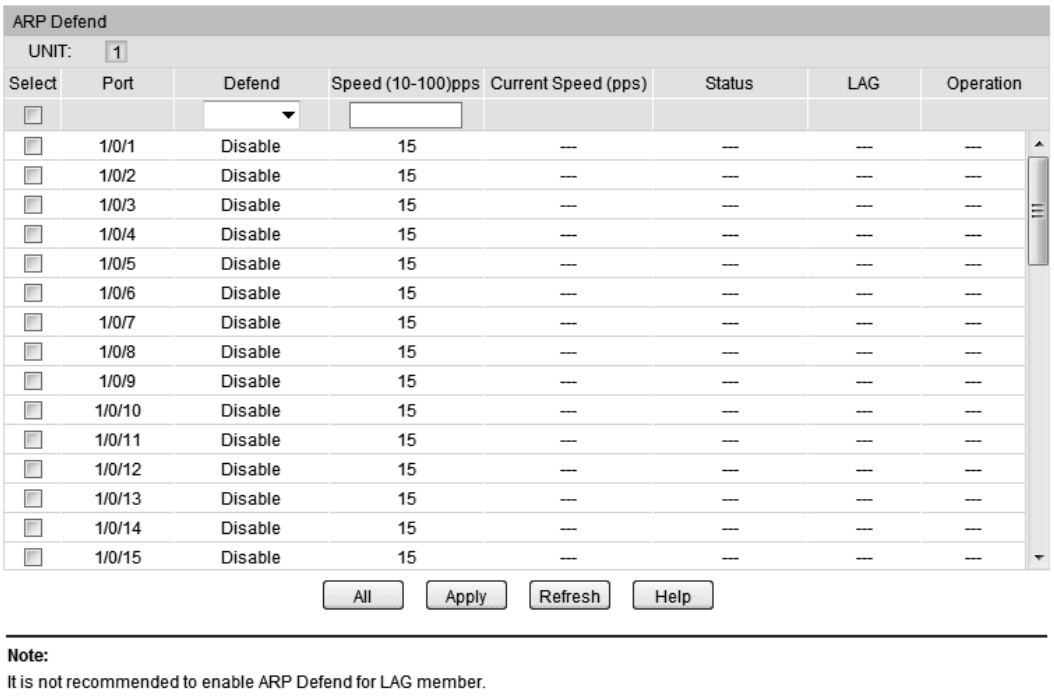


Figure 14-20 ARP Defend

The following entries are displayed on this screen:

- **ARP Defend**

Select:	Select your desired port for configuration. It is multi-optional.
Port:	Displays the port number.
Defend:	Select Enable/Disable the ARP Defend feature for the port.
Speed(10-100)pps:	Enter a value to specify the maximum amount of the received ARP packets per second.
Current Speed(pps):	Displays the current speed of the received ARP packets.
Status	Displays the status of the ARP attack.
LAG:	Displays the LAG to which the port belongs to.
Operation:	Click the **Recover** button to restore the port to the normal status. The ARP Defend for this port will be re-enabled.

Note:

It's not recommended to enable the ARP Defend feature for the LAG member port.

14.5.3 ARP Statistics

ARP Statistics feature displays the number of the illegal ARP packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **Network Security→ARP Inspection→ARP Statistics** to load the following page.

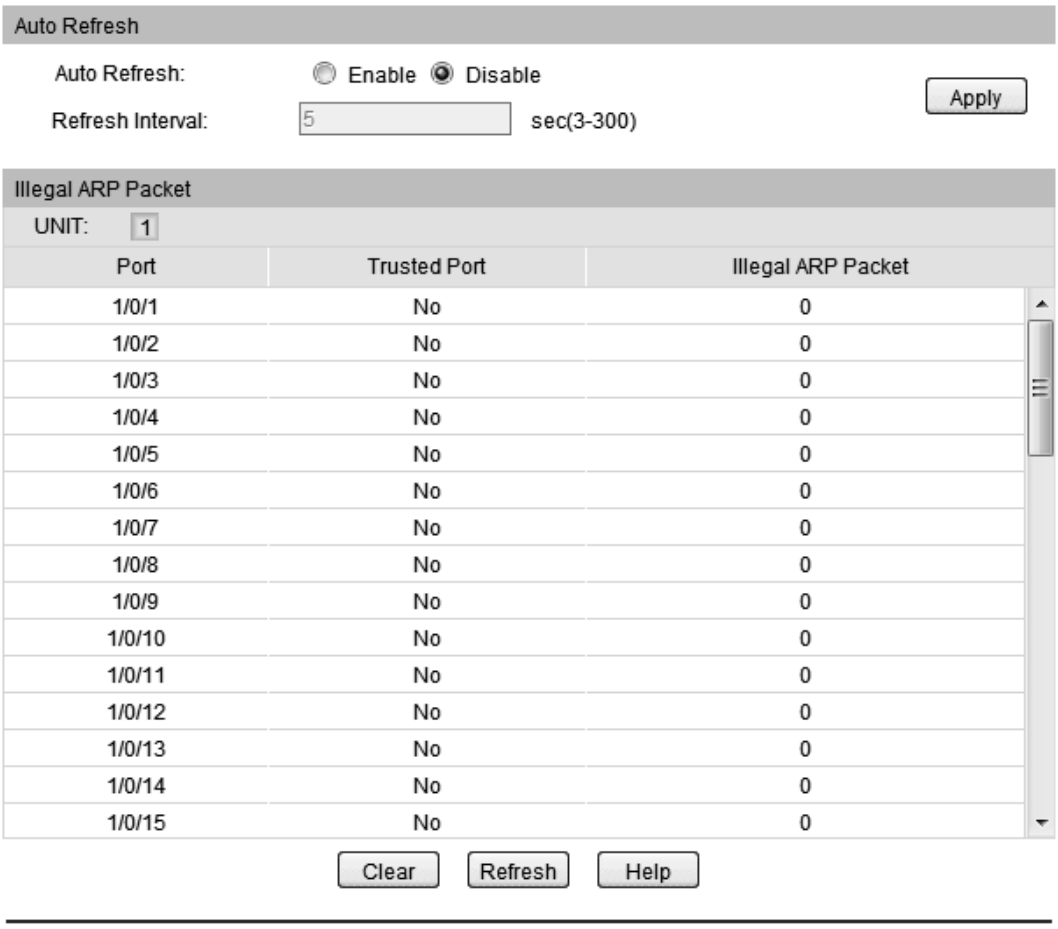


Figure 14-21 ARP Statistics

The following entries are displayed on this screen:

- **Auto Refresh**

Auto Refresh: Enable/Disable the Auto Refresh feature.

Refresh Interval: Specify the refresh interval to display the ARP Statistics.

- **Illegal ARP Packet**

Port: Displays the port number.

Trusted Port: Indicates the port is an ARP Trusted Port or not.

Illegal ARP Packet: Displays the number of the received illegal ARP packets.

14.6 ND Detection

- ND Brief Introduction

IPv6 Neighbor Discovery (ND) protocol uses five types of ICMPv6 messages to implement the following functions:

- Address resolution
- Neighbor reachability detection
- Duplicate address detection (DAD)
- Router/prefix discovery and address autoconfiguration
- Redirection

Five types of the ICMPv6 messages are listed below:

ICMPv6 Message	Function
Neighbor Solicitation (NS)	• Acquires the neighbor's link-layer address. • Verifies whether a neighbor is reachable. • Detects duplicate address.
Neighbor Advertisement (NA)	• Responses to an NS message. • Notifies the neighbor nodes of link layer changes
Router Solicitation (RS)	• Requests for an address prefix and other configuration parameters for autoconfiguration.
Router Advertisement (RA)	• Responses to an RS message. • Advertises information such as the prefix information options and flag bits.
Redirect (RR)	• Informs the source host of another next hop to a particular destination when certain conditions are met.

➢ ND Attack

Because of the absence of security mechanism, ND protocol is easy to be exploited by attackers. Attackers can exploit the ND protocols as follows:

- The attackers send forged NS/NA/RS packets with the IPv6 address of a victim host. The gateway or the other hosts who have received these NS/NA/RS packets will update their ND entry with the wrong address information. AS a result, all packets intended for the victim will be sent to the attacking host rather than the victim host.
- The attackers send forged RA packets with the IPv6 address of a victim gateway. All the hosts attached to the victim gateway may receive incorrect IPv6 configuration parameters and maintain false ND entries.

A forged ND packet has the following two features:

- The source MAC address in the Ethernet frame header is inconsistent with that carried in the source link layer address option of the ND packet.
- The mapping between the source IPv6 address and the source MAC address in the Ethernet

frame header is invalid.

➢ ND Detection Process

Generally, the ND detection feature uses the entries in the IPv6-MAC binding table to verify the packets received on the untrusted ports, thus filtering the forged ND packets and keeping out the attacks.

1. ND packets received on the ND-trusted port will not be checked.
2. RS/NS packets with their source IPv6 address unspecified will not be checked.
3. RA/RR packets received on the ND-untrusted port will be discarded directly; the other ND packets received on the ND-untrusted port will be checked.
   a) Source MAC consistence check. If the RS/NS packet's source MAC address in the Ethernet frame header is different from that carried in the source layer address option, the RS/NS packet will be discarded.
   b) IPv6-MAC binding check. Look up the IPv6-MAC binding table to compare the IPv6 address, MAC address, VLAN ID and receiving port between the entry and the ND packet. If a match is found, the ND packet is considered legal and forwarded; if no match is found, the ND packet is considered illegal and discarded directly.

Choose the menu **Network Security→ND Detection→ND Detection** to load the following page.

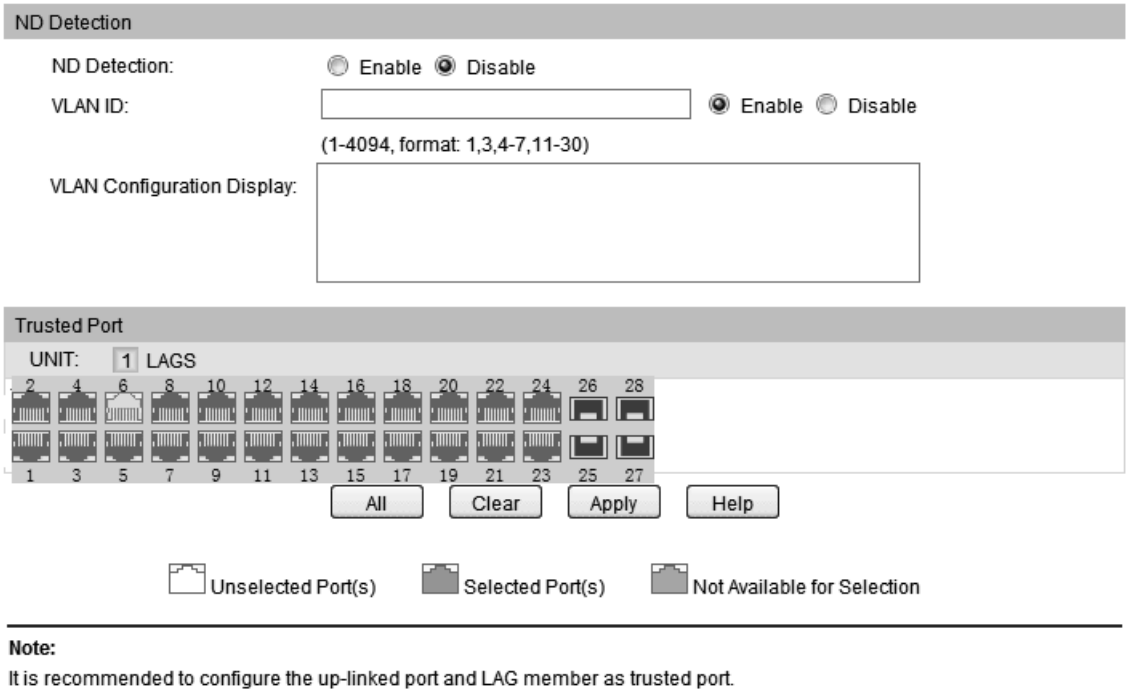


Figure 14-22 ND Detection

➢ **ND Detection**

ND Detection: Enable/Disable the ND Detection function.

VLAN ID: Enter the VLAN ID in which you want to enable/disable the ND

Detection function.

VLAN Configuration Display: Display the VLANs with ND detection function enabled.

- **Trusted Port**

UNIT:1/LAGS Select the desired unit or LAG for configuration.

Trusted Port: Select Enable/Disable the port to be a Trusted Port. Only the Trusted Port can forward the Router Advertisement Message and Router Redirect Message from Routers.

14.7 IP Source Guard

IP Source Guard is to filter the IP packets based on the IP-MAC Binding entries. Only the packets matched to the IP-MAC Binding rules can be processed, which can enhance the bandwidth utility.

Choose the menu **Network Security→IP Source Guard** to load the following page.

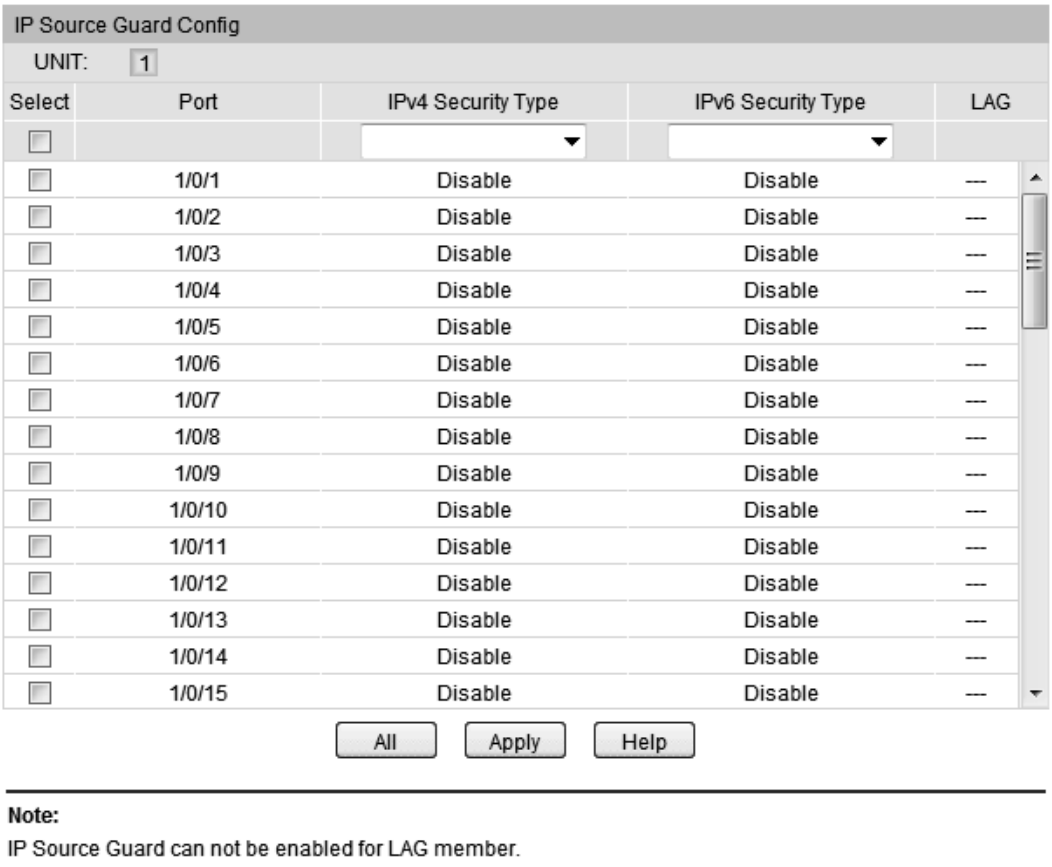


Figure 14-23 IP Source Guard

The following entries are displayed on this screen:

- **IP Source Guard Config**

Select: Select your desired port for configuration. It is multi-optional.

Port: Displays the port number.

IPv4 Security Type: Select Security Type for the port.

- **Disable:** Select this option to disable the IP Source Guard feature for the port.
- **SIP+MAC:** Only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed.

IPv6 Security Type: Select Security Type for the port.

- **Disable:** Select this option to disable the IPv6 Source Guard feature for the port.
- **SIPv6+MAC:** Only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed.

LAG: Displays the LAG to which the port belongs.

Note:

Before configuring IPv6 Security feature, you should configure the SDM template as "enterpriseV6" and save your configurations. See **SDM Template** for more information about SDM template configuration.

14.8 DoS Defend

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network.

With DoS Defend function enabled, the switch can analyze the specific fields of the IP packets and distinguish the malicious DoS attack packets. Upon detecting the packets, the switch will discard the illegal packets directly and limit the transmission rate of the legal packets if the over legal packets may incur a breakdown of the network. The switch can defend several types of DoS attack listed in the following table.

DoS Attack Type	Description
Land Attack	The attacker sends a specific fake SYN packet to the destination Host. Since both the source IP address and the destination IP address of the SYN packet are set to be the IP address of the Host, the Host will be trapped in an endless circle for building the initial connection. The performance of the network will be reduced extremely.
Scan SYNFIN	The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal. The switch can defend this type of illegal packet.
Xmascan	The attacker sends the illegal packet with its TCP index, FIN, URG

DoS Attack Type	Description
	and PSH field set to 1.
NULL Scan Attack	The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all the control fields set to 0 are considered as the illegal packets.
SYN packet with its source port less than 1024	The attacker sends the illegal packet with its TCP SYN field set to 1 and source port less than 1024.
Blat Attack	The attacker sends the illegal packet with its source port and destination port on Layer 4 the same and its URG field set to 1. Similar to the Land Attack, the system performance of the attacked Host is reduced since the Host circularly attempts to build a connection with the attacker.
Ping Flooding	The attacker floods the destination system with Ping broadcast storm packets to forbid the system to respond to the legal communication.
SYN/SYN-ACK Flooding	The attacker uses a fake IP address to send TCP request packets to the Server. Upon receiving the request packets, the Server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The Server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.

Table 14-1 Defendable DoS Attack Types

14.8.1 DoS Defend

On this page, you can enable the DoS Defend type appropriate to your need.

Choose the menu **Network Security→DoS Defend→DoS Defend** to load the following page.

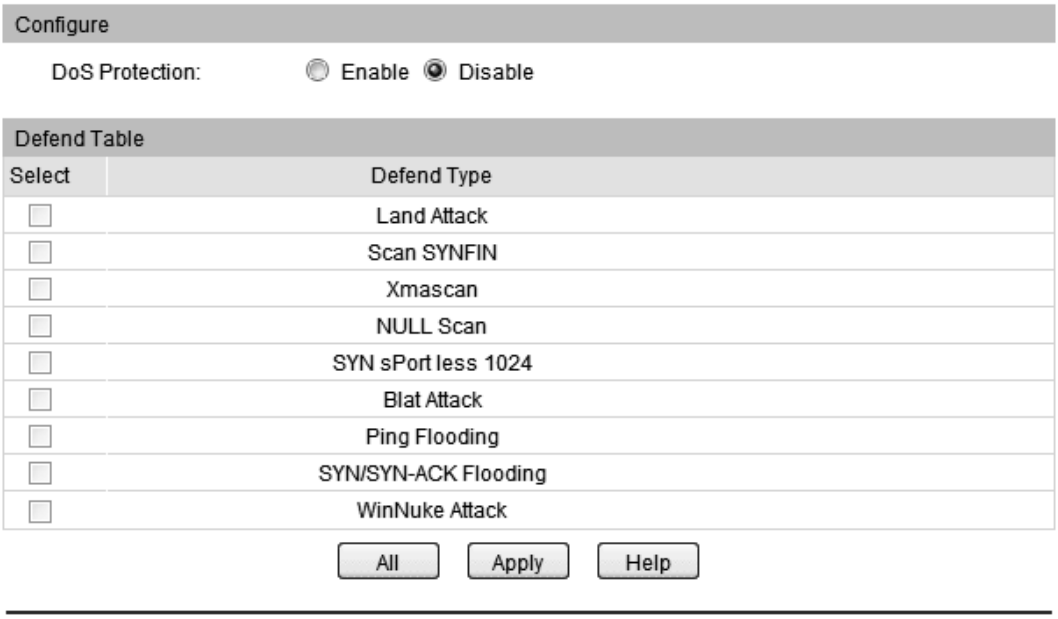


Figure 14-24 DoS Defend

The following entries are displayed on this screen:

- **Defend Config**

DoS Defend: Allows you to Enable/Disable DoS Defend function.

- **Defend Table**

Select: Select the entry to enable the corresponding Defend Type.

Defend Type: Displays the Defend Type name.

14.9 802.1X

The 802.1X protocol was developed by IEEE802 LAN/WAN committee to deal with the security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to solve mainly authentication and security problems.

802.1X is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access control devices. With the 802.1X protocol enabled, a supplicant can access the LAN only when it passes the authentication, whereas those failing to pass the authentication are denied when accessing the LAN.

- **Architecture of 802.1X Authentication**

802.1X adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system, as shown in the following figure.

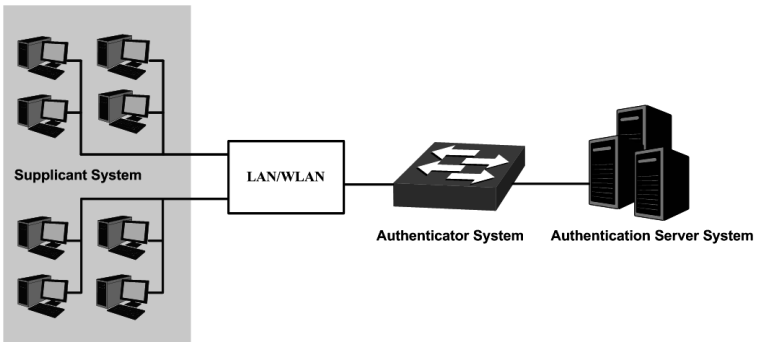


Figure 14-25 Architecture of 802.1X authentication

1. **Supplicant System:** The supplicant system is an entity in LAN and is authenticated by the authenticator system. The supplicant system is usually a common user terminal computer. An 802.1X authentication is initiated when a user launches client program on the supplicant system. Note that the client program must support the 802.1X authentication protocol.
2. **Authenticator System:** The authenticator system is usually an 802.1X-supported network device, such as this switch. It provides the physical or logical port for the supplicant system to access the LAN and authenticates the supplicant system.
3. **Authentication Server System:** The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server. Authentication Server can store user information and serve to perform authentication and authorization. To ensure a stable authentication system, an alternate authentication server can be specified. If the main authentication server is in trouble, the alternate authentication server can substitute it to provide normal authentication service.

➢ **The Mechanism of an 802.1X Authentication System**

IEEE 802.1X authentication system uses EAP (Extensible Authentication Protocol) to exchange information between the supplicant system and the authentication server.

1. EAP protocol packets transmitted between the supplicant system and the authenticator system are encapsulated as EAPOL packets.
2. EAP protocol packets transmitted between the authenticator system and the RADIUS server can either be encapsulated as EAPOR (EAP over RADIUS) packets or be terminated at authenticator system and the authenticator system then communicate with RADIUS servers through PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) protocol packets.
3. When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

➢ **802.1X Authentication Procedure**

An 802.1X authentication can be initiated by supplicant system or authenticator system. When the authenticator system detects an unauthenticated supplicant in LAN, it will initiate the 802.1X authentication by sending EAP-Request/Identity packets to the supplicant. The supplicant system can also launch an 802.1X client program to initiate an 802.1X authentication through the sending of an EAPOL-Start packet to the switch,

This switch can authenticate supplicant systems in EAP relay mode or EAP terminating mode. The following illustration of these two modes will take the 802.1X authentication procedure initiated by the supplicant system for example.

1. EAP Relay Mode

This mode is defined in 802.1X. In this mode, EAP-packets are encapsulated in higher level protocol (such as EAPOR) packets to allow them successfully reach the authentication server. This mode normally requires the RADIUS server to support the two fields of EAP: the EAP-message field and the Message-authenticator field. This switch supports EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP authentication way for the EAP relay mode. The following figure describes the basic EAP-MD5 authentication procedure.

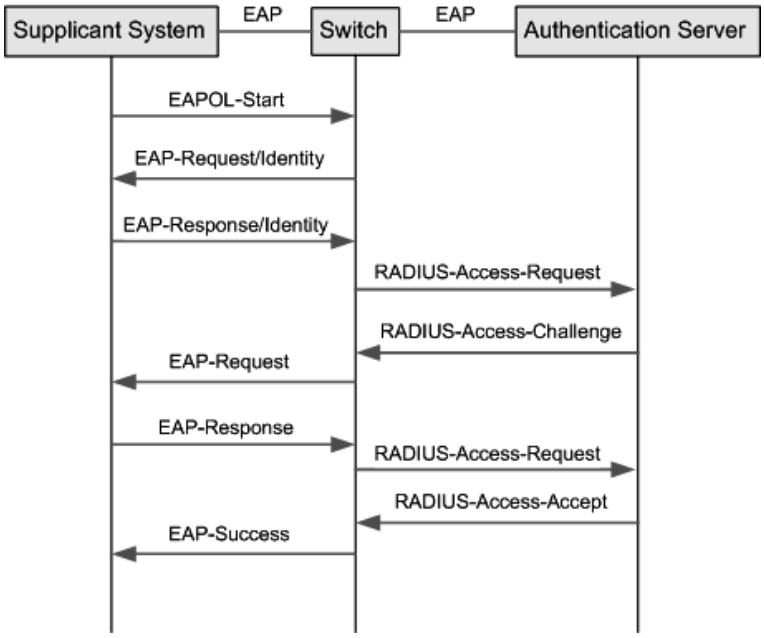


Figure 14-26 EAP-MD5 Authentication Procedure

(1) A supplicant system launches an 802.1X client program via its registered user name and password to initiate an access request through the sending of an EAPOL-Start packet to the switch. The 802.1X client program then forwards the packet to the switch to start the authentication process.

(2) Upon receiving the authentication request packet, the switch sends an EAP-Request/Identity packet to ask the 802.1X client program for the user name.

(3) The 802.1X client program responds by sending an EAP-Response/Identity packet to the switch with the user name included. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.

(4) Upon receiving the user name from the switch, the RADIUS server retrieves the user name, finds the corresponding password by matching the user name in its database, encrypts the

password using a randomly-generated key, and sends the key to the switch through an RADIUS Access-Challenge packet. The switch then sends the key to the 802.1X client program.

(5) Upon receiving the key (encapsulated in an EAP-Request/MD5 Challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-Response/MD5 Challenge packet) to the RADIUS server through the switch. (The encryption is irreversible.)

(6) The RADIUS server compares the received encrypted password (contained in a RADIUS Access-Request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS Access-Accept packet and an EAP-Success packet) to the switch to indicate that the supplicant system is authorized.

(7) The switch changes the state of the corresponding port to accepted state to allow the supplicant system access the network. And then the switch will monitor the status of supplicant by sending hand-shake packets periodically. By default, the switch will force the supplicant to log off if it cannot get the response from the supplicant for two times.

(8) The supplicant system can also terminate the authenticated state by sending EAPOL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

2. EAP Terminating Mode

In this mode, packet transmission is terminated at authenticator systems and the EAP packets are mapped into RADIUS packets. Authentication and accounting are accomplished through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. This switch supports the PAP terminating mode. The authentication procedure of PAP is illustrated in the following figure.

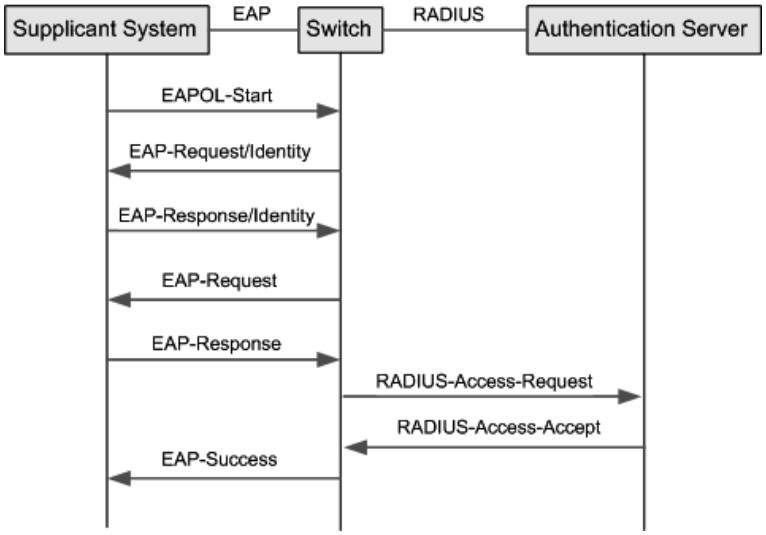


Figure 14-27 PAP Authentication Procedure

In PAP mode, the switch encrypts the password and sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication. Whereas the randomly-generated key in EAP-MD5 relay

mode is generated by the authentication server, and the switch is responsible to encapsulate the authentication packet and forward it to the RADIUS server.

- **802.1X Timer**

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way:

1. **Supplicant system timer (Supplicant Timeout):** This timer is triggered by the switch after the switch sends a request packet to a supplicant system. The switch will resend the request packet to the supplicant system if the supplicant system fails to respond in the specified timeout period.
2. **RADIUS server timer** (**Server Timeout**): This timer is triggered by the switch after the switch sends an authentication request packet to RADIUS server. The switch will resend the authentication request packet if the RADIUS server fails to respond in the specified timeout period.
3. **Quiet-period timer (Quiet Period):** This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the specified period before it processes another authentication request re-initiated by the supplicant system.

- **Guest VLAN**

Guest VLAN function enables the supplicants that do not pass the authentication to access the specific network resource.

By default, all the ports connected to the supplicants belong to a VLAN, i.e. Guest VLAN. Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated before accessing external resources. After passing the authentication, the ports will be removed from the Guest VLAN and be allowed to access the other resources.

With the Guest VLAN function enabled, users can access the Guest VLAN to install 802.1X client program or upgrade their 802.1x clients without being authenticated. If there is no supplicant past the authentication on the port in a certain time, the switch will add the port to the Guest VLAN.

With 802.1X function enabled and Guest VLAN configured, after the maximum number retries have been made to send the EAP-Request/Identity packets and there are still ports that have not sent any response back, the switch will then add these ports into the Guest VLAN according to their link types. Only when the corresponding user passes the 802.1X authentication, the port will be removed from the Guest VLAN and added to the specified VLAN. In addition, the port will back to the Guest VLAN when its connected user logs off.

The **802.1X** function is implemented on the **Global Config** and **Port Config** pages.

14.9.1 Global Config

On this page, you can enable the 802.1X authentication function globally and control the authentication process by specifying the Authentication Method, Guest VLAN and various Timers. Please disable Handshake feature if you are using other client softwares.

Choose the menu **Network Security→802.1X→Global Config** to load the following page.

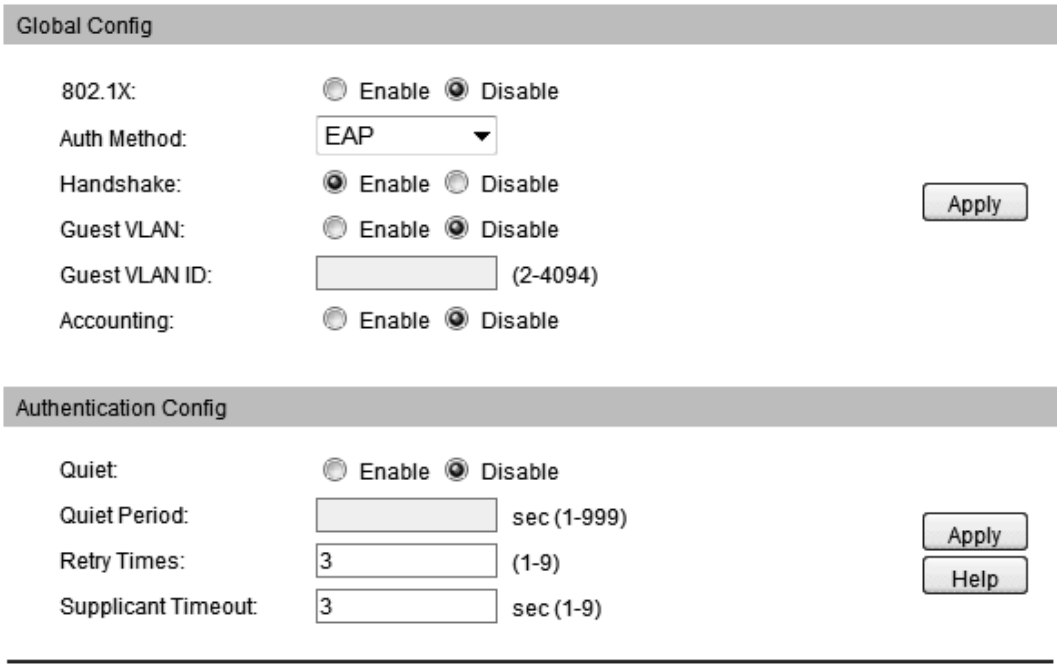


Figure 14-28 Global Config

The following entries are displayed on this screen:

➢ **Global Config**

802.1X: Enable/Disable the 802.1X function.

Auth Method: Select the Authentication Method from the pull-down list.

- **EAP:** EAP relay mode. IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP protocol packets with authentication data can be encapsulated in the advanced protocol (such as RADIUS) packets to be transmitted to the authentication server.
- **PAP:** EAP termination mode. IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The transmission of EAP packets is terminated at the switch and the EAP packets are converted to the other protocol (such as RADIUS) packets for transmission.

Handshake: Enable/Disable the Handshake feature. The Handshake feature is used to detect the connection status between the 802.1X Client and the switch. Please disable Handshake feature if you are using other client softwares instead of 802.1X Client.

Guest VLAN: Enable/Disable the Guest VLAN feature.

Guest VLAN ID: Enter your desired VLAN ID to enable the Guest VLAN feature. The supplicants in the Guest VLAN can access the specified network source.

➢ **Authentication Config**

Quiet: Enable/Disable the Quiet timer.

Quiet Period: Specify a value for Quiet Period. Once the supplicant failed to the 802.1X Authentication, then the switch will not respond to the authentication request from the same supplicant during the Quiet Period.

Retry Times: Specify the maximum transfer times of the repeated authentication request.

Supplicant Timeout: Specify the maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant.

14.9.2 Port Config

On this page, you can configure the 802.1X features for the ports basing on the actual network.

Choose the menu **Network Security→802.1X→Port Config** to load the following page.

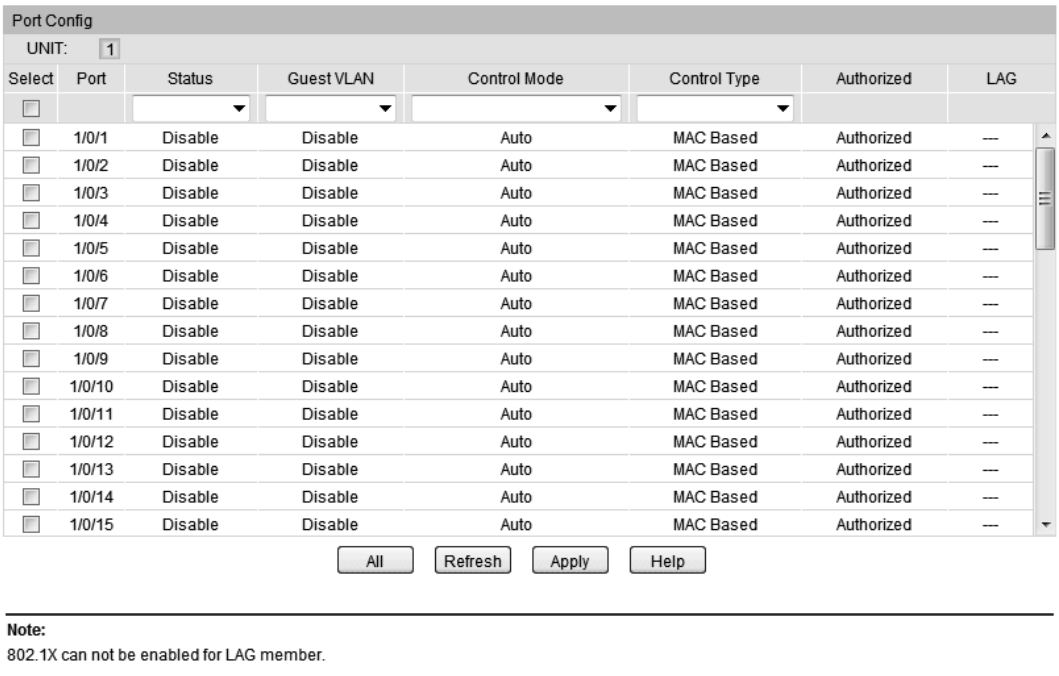


Figure 14-29 Port Config

The following entries are displayed on this screen:

➢ **Port Config**

Select: Select your desired port for configuration. It is multi-optional.

Port: Displays the port number.

Status: Select Enable/Disable the 802.1X authentication feature for the port.

Guest VLAN: Select Enable/Disable the Guest VLAN feature for the port.

Control Mode: Specify the Control Mode for the port.

- **Auto:** In this mode, the port will normally work only after passing the 802.1X Authentication.
- **Force-Authorized:** In this mode, the port can work normally without passing the 802.1X Authentication.
- **Force-Unauthorized:** In this mode, the port is forbidden working for its fixed unauthorized status.

Control Type: Specify the Control Type for the port.

- **MAC Based:** Any client connected to the port should pass the 802.1X Authentication for access.
- **Port Based:** All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1X Authentication.

Authorized: Displays the authentication status of the port.

LAG: Displays the LAG to which the port belongs to.

Configuration Procedure:

Step	Operation	Description
1	Install the 802.1X client software.	Required. For the client computers, you are required to install the 802.1X Client provided on the CD. Please refer to the software guide in the same directory with the software for more information.
2	Configure the 802.1X globally.	Required. By default, the global 802.1X function is disabled. On the **Network Security→802.1X→Global Config** page, configure the 802.1X function globally.
3	Configure the 802.1X for the port.	Required. On the **Network Security→802.1X→Port Config** page, configure the 802.1X feature for the port of the switch basing on the actual network.
4	Connect an authentication server to the switch and do some configuration.	Required. Record the information of the client in the LAN to the authentication server and configure the corresponding authentication username and password for the client.
5	Enable the AAA function globally.	Required. On the **Network Security→AAA→Global Conifg** page, enable the AAA function globally.

6	Configure the parameters of the authentication server.	Required. On the **Network Security→AAA→RADIUS Server Conifg** page, configure the parameters of the RADIUS server.

Note:

1. The 802.1X function takes effect only when it is enabled globally on the switch and for the port.
2. The 802.1X function cannot be enabled for LAG member ports. That is, the port with 802.1X function enabled cannot be added to the LAG.
3. The 802.1X function should not be enabled for the port connected to the authentication server.

14.10 PPPoE

- **PPPoE ID-Insertion Overview**
- The PPPoE ID-Insertion feature provides a way to extract a Vendor-specific tag as an identifier for the authentication, authorization, and accounting (AAA) access requests on an Ethernet interface. When enabled, the switch attaches a tag to the PPPoE discovery packets, which is called the PPPoE Vendor-Specific tag and it contains a unique line identifier. There are two formats of Vendor-specific tags: Circuit-ID format and Remote-ID format. The BRAS receives the tagged packet, decodes the tag, and uses the Circuit-ID/Remote-ID field of that tag as a NAS-Port-ID attribute in the RADIUS server for PPP authentication and AAA (authentication, authorization, and accounting) access requests. The switch will remove the Circuit-ID/Remote-ID tag from the received PPPoE Active Discovery Offer and Session-confirmation packets from the BRAS.

In this Chapter the switch will work as a DSLAM.

- **PPPoE ID-Insertion Operation Process**

The PPPoE ID insertion includes Circuit-ID tag and Remote-ID tag. The following process takes Circuit-ID insertion as an example:

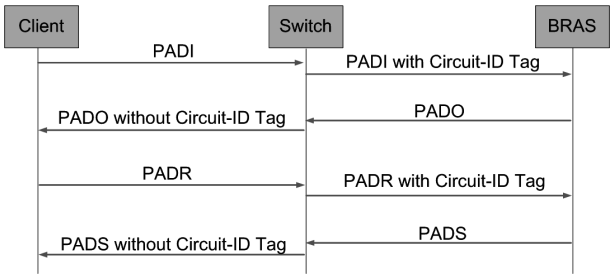


Figure 14-1 PPPoE Discovery Process

The PPPoE discovery process is illustrated below:

1. The client sends PADI (PPPoE Active Discovery Initiation) packets to the switch.
2. The switch intercepts PADI packets and inserts a unique Circuit-ID tag to them.
3. The switch forwards the PADI packets with Circuit-ID tag to the BRAS.

4. The BRAS responses with the PADO (PPPoE Active Discovery Offer) packets after receiving the PADI packets.
5. Upon receiving the PADO packets with the Circuit-ID tag, the switch will remove the tag and send the packets to the client. The switch will forward the PADO packets without the Circuit-ID tag directly.
6. The client sends PADR (PPPoE Active Discovery Request) packets according to the process.
7. The switch intercepts PADR packets and inserts a unique Circuit-ID tag to them.
8. The switch forwards the PADR packets with Circuit-ID tag to the BRAS.
9. The BRAS processes the received Circuit-ID tag in the PADR packets and extracts the Circuit-ID field to the RADIUS for accounting. And the BRAS allocates a PPP process session ID for this PPP session.
10. The BRAS responses with the PADS (PPPoE Active Discovery Session-confirmation) packets after receiving the PADR packets.
11. Upon receiving the PADS packets with the Circuit-ID tag, the switch will remove the tag and send the packets to the client. The switch will forward the PADS packets without the Circuit-ID tag directly.

On the **PPPoE ID Insertion** page, you can enable the PPPoE ID insertion function globally. Each port's PPPoE ID Insertion feature and type can be configured separately.

Choose the menu **Network Security→PPPoE→PPPoE ID Insertion** to load the following page.

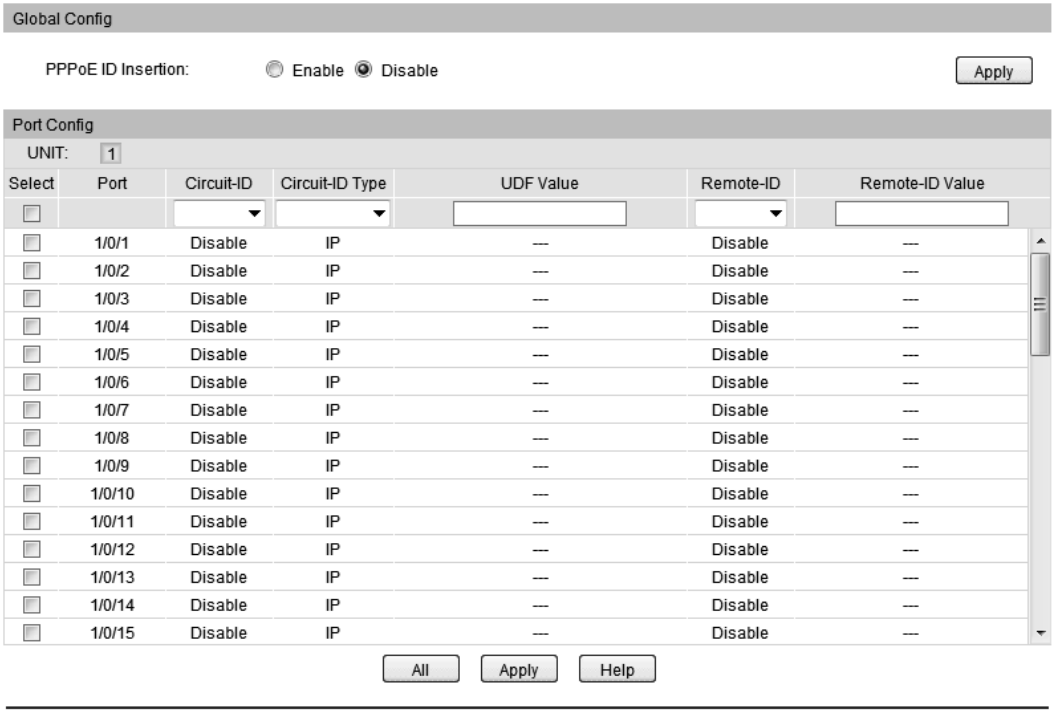


Figure 14-30 PPPoE Circuit-ID Config

The following entries are displayed on this screen:

➢ **Global Config**

PPPoE ID Insertion: Enable/Disable the PPPoE Circuit-ID Insertion function globally.

➢ **Port Config**

Select: Select the desired port for configuration. It is multi-optional.

Port: Displays the port number.

Circuit-ID: Enable/Disable the PPPoE Circuit-ID Insertion feature for the port.

Circuit-ID Type: Specify the Circuit-ID type for the port:

- **IP**: The IP address of the switch will be used to encode the Circuit-ID option. This is the default value.
- **MAC**: The MAC address of the switch will be used to encode the Circuit-ID option.
- **UDF**: The user specified string with the maximum length of 40 characters will be used to encode the Circuit-ID option.
- **UDF ONLY**: Only the user specified string with the maximum length of 40 will be used to encode the Circuit-ID option.

UDF Value: If the UDF is selected, specify a string with the maximum length of 40 characters to encode the Circuit-id option.

Remote-ID: Enable or Disable the PPPoE Remote-ID Insertion feature for the port.

Remote-ID Value: A user specified string with the maximum length of 40 characters to encode the Remote-id option

14.11 AAA

➢ **Overview**

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

Username and password pairs are used for login and privilege authentication. The authentication can be processed locally in the switch or centrally in the RADIUS/TACACS+ server(s). The local authentication username and password pairs can be configured in 4.2 User Management.

➢ **Applicable Access Application**

The authentication can be applied on the following access applications: Console, Telnet, SSH and HTTP.

➢ **Authentication Method List**

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

The administrator can set the authentication methods in a preferable order in the list. The switch uses the first listed method to authenticate users, if that method fails to respond, the switch selects the next authentication method in the method list. This process continues until there is a successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this circle, which means the secure server or the local switch denies the user's access, the authentication process stops and no other authentication methods are attempted.

➢ **802.1X Authentication**

802.1X protocol uses the RADIUS to provide detailed accounting information and flexible administrative control over authentication process. The Dot1x List feature defines the RADIUS server groups in the 802.1X authentication.

➢ **RADIUS/TACACS+ Server**

Users can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

➢ **Server Group**

Users can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

The switch has two built-in authentication server group, one for RADIUS and the other for TACACS+. These two server groups cannot be deleted, and the user-defined RADIUS/TACACS+ server will join these two server groups automatically.

14.11.1 Global Config

This page is used to enable/disable the AAA function globally.

Choose the menu **Network Security→AAA→Global Conifg** to load the following page.

Figure 14-31 AAA Global Config

➢ **Configuration Procedure**

Click Enable to enable the AAA function globally.

14.11.2 Privilege Elevation

This page is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

Choose the menu **Network Security→AAA→Global Conifg** to load the following page.

Figure 14-32 Privilege Elevate

➢ **Configuration Procedure**

Enter the Enable Password and click Enable button to elevate the current logged-in user from guest to admin. Only admin users can configure the following AAA settings.

Tips:

If the Enable password is verified locally, the Enable password should be previously set by the admin users using the command lines. For more details please refer to the command **enable password** in the Command Line Interface Guide on the resource CD.

14.11.3 RADIUS Server Config

This page is used to configure the authentication servers running the RADIUS security protocols.

Choose the menu **Network Security→AAA→RADIUS Conifg** to load the following page.

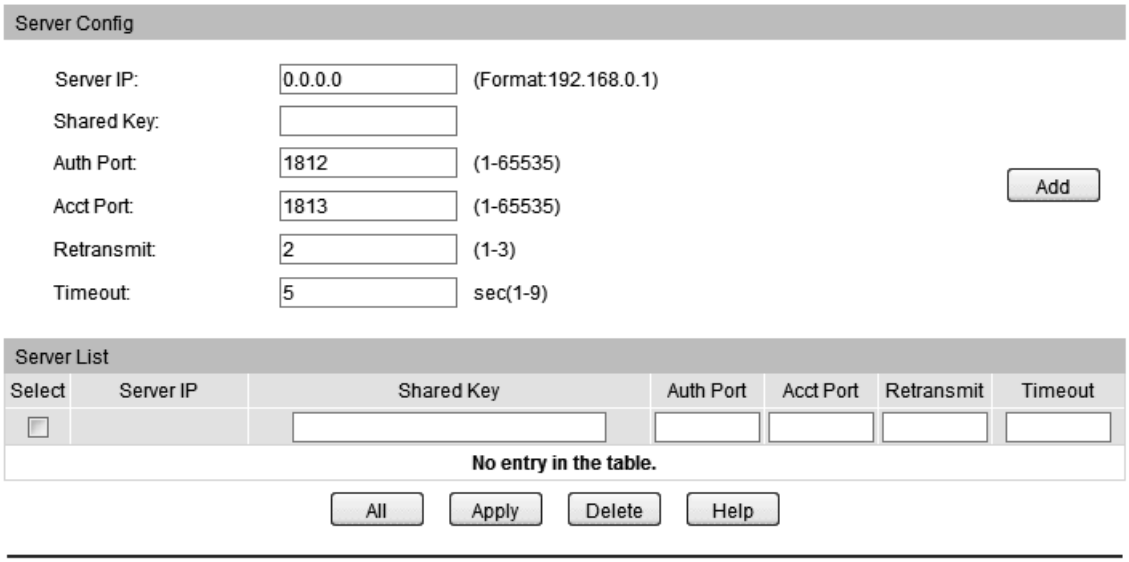


Figure 14-33 RADIUS Server Config

➢ **Configuration Procedure**

Configure the RADIUS server's IP and other relevant parameters under the Server Config.

View, edit and delete the configured RADIUS servers in the Server list.

➢ **Entry Description**

Server IP:	Enter the IP of the server running the RADIUS secure protocol.
Shared Key:	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Auth Port:	Specify the UDP destination port on the RADIUS server for authentication requests.
Acct Port:	Specify the UDP destination port on the RADIUS server for accounting requests.
Retransmit:	Specify the number of times a request is resent to a server if the server does not respond.
Timeout:	Specify the time interval that the switch waits for the server to reply before resending.

14.11.4 TACACS+ Server Config

This page is used to configure the authentication servers running the TACACS+ security protocols.

Choose the menu **Network Security→AAA→TACACS+ Conifg** to load the following page.

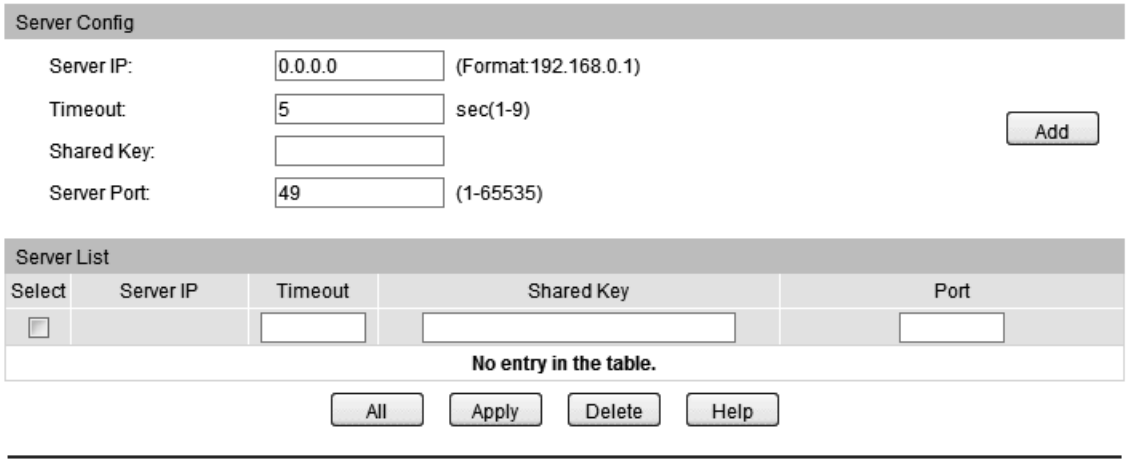


Figure 14-34 TACACS+ Server Config

➢ **Configuration Procedure**

Configure the TACACS+ server's IP and other relevant parameters under the Server Config.

View, edit and delete the configured TACACS+ servers in the Server list.

➢ **Entry Description**

Server IP:	Enter the IP of the server running the TACACS+ secure protocol.

Shared Key: Enter the shared key between the TACACS+ server and the switch. The TACACS+ server and the switch use the key string to encrypt passwords and exchange responses.

Timeout: Specify the time interval that the switch waits for the server to reply before resending.

Port: Specify the TCP port used on the TACACS+ server for AAA.

14.11.5 Authentication Server Group Config

On this page users can group authentication servers running the same secure protocol for authentication. The switch has two built-in authentication server group, one for RADIUS and the other for TACACS+. These two server groups cannot be edited or deleted. The server entries in one group are tried in the order they are added.

The server entries in one group are tried in the order they are added.

Choose the menu **Network Security→AAA→Server Group** to load the following page.

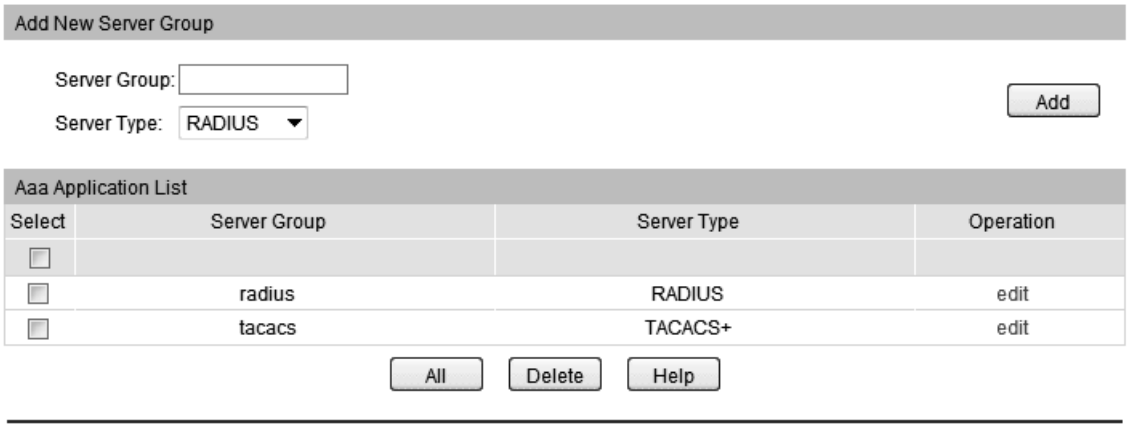


Figure 14-35 Create New Server Group

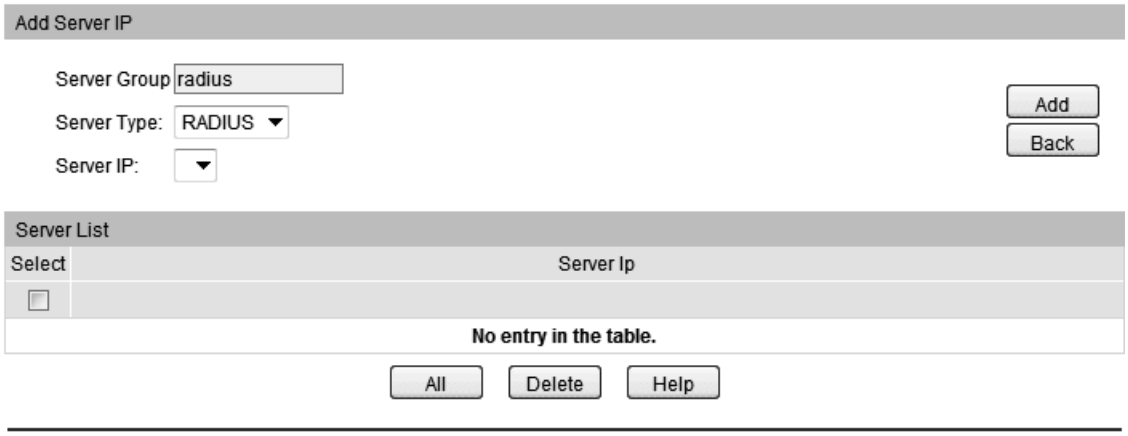


Figure 14-36 Add Server to Server Group

➢ **Configuration Procedure**

1) Configure the Server Group name and Server Type to create a server group.

2) Click edit in the Server Group List to configure the corresponding server group.

3) Select Server IP you have previously created and click add to add the server to the server group. (Figure 14-36)

View and delete the configured server groups in the Server Group list.

View and delete the configured servers in the server IP list.

➢ **Entry Description**

Server Group:	Define a server group with a group name.
Server Type:	Specify the server type as RADIUS or TACACS+.
Server IP	Select the IP of the server you have previously configured.

Note:

1. The two built-in server groups radius and tacacs+ cannot be deleted or edited.
2. Up to 16 servers can be added to one server group.

14.11.6 Authentication Method List Config

Before you configure AAA authentication on a certain application, you should define an authentication method list first. An authentication method list describes the sequence and authentication method to be queried to authenticate a user.

The switch uses the first method listed to authenticate users, if that method fails to respond, the switch selects the next authentication method in the method list. This process continues until there is a successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this circle, which means the secure server or the local switch denies the user's access, the authentication process stops and no other authentication methods are attempted.

For example, if a user defines an authentication login method list as tacacs-radius-local, the switch will send an authentication request to the fist TACACS+ server in the tacacs server group. If there is no response, the switch will send an authentication request to the second TACACS+ server in the tacacs server group and so on, until the tacacs server group list is exhausted. Then the RADIUS server group will be queried. If no authentication is accomplished in the RADIUS server list, the switch will authenticate the user locally. This forms a backup system for authentication.

Choose the menu **Network Security→AAA→Method List** to load the following page.

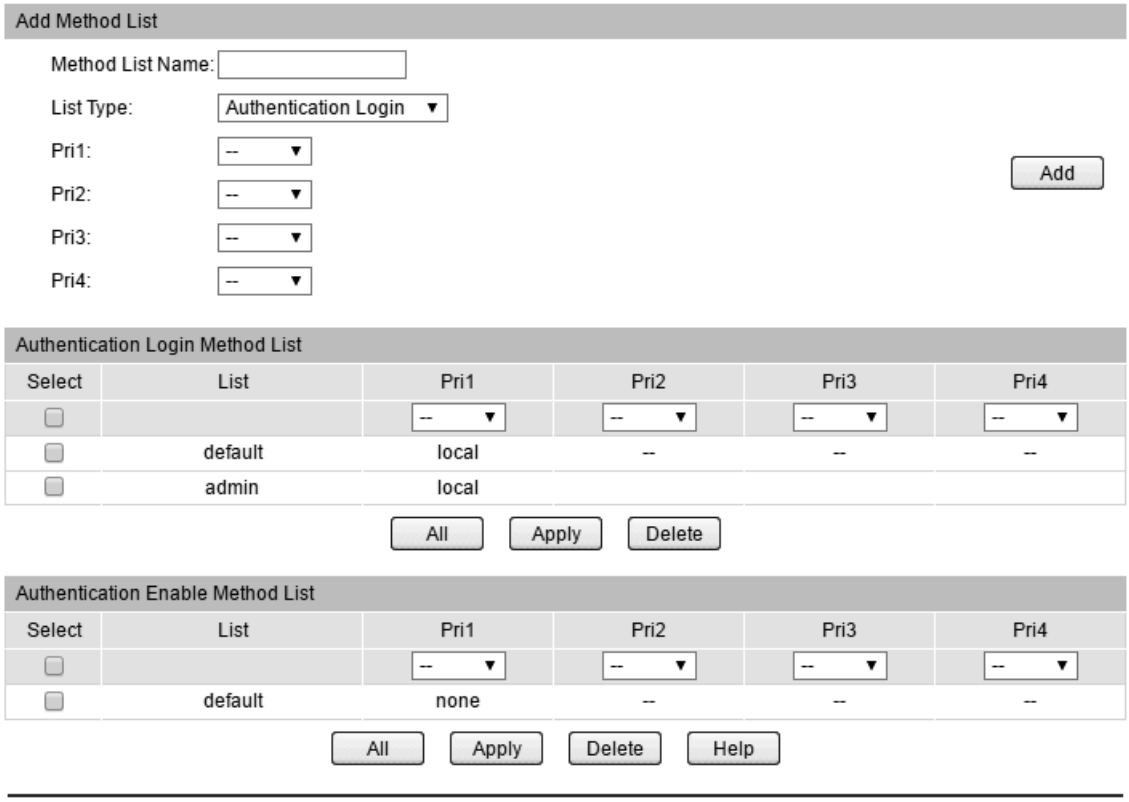


Figure 14-37 Authentication Method List Config

➢ **Configuration Procedure**

1) Enter the method list name.
2) Specify the authentication type as Login or Enable.
3) Configure the authencation method with priorities. The options are radius, tacacs, local or user-defined server groups.

View and delete the configured method priority list in the Authentication Login Method List and Authentication Enable Method List. .

➢ **Entry Description**

Method List Name:	Define a method list name.
List Type:	Specify the authentication type as Login or Enable. Login stands for the Authentication Login Method List, and Enable stands for the Authentication Enable Method list.
Pri1, Pri2, Pri3, Pri4:	Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails. local: Use the local database in the switch for authentication. none: No authentication is used. radius: Use the remote RADIUS server/server groups for

authentication.

tacacs: Use the remote TACACS+ server/server groups for authentication.

user-defined server group: Use the user-defined server groups for authentication.

Tips:

If the Enable password is verified on the remote RADIUS server, the switch will send the Enable authentication with the default username as $enable$.

14.11.7 Application Authentication List Config

Users can configure authentication method lists on the following access applications: console, telnet, ssh and http.

Choose the menu **Network Security→AAA→Global Config** to load the following page.

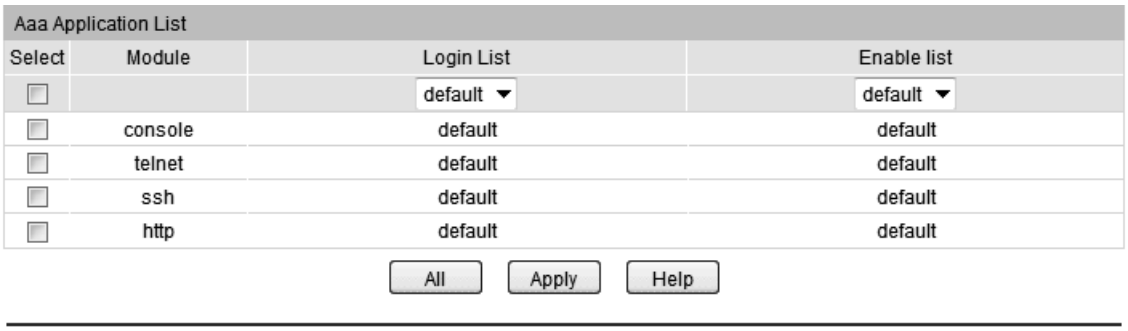


Figure 14-38 Application Authentication Settings

➢ **Configuration Procedure**

1) Select the application module.
2) Configure the authentication method list from the Login List drop-down menu. This option defines the authentication method for users accessing the switch.
3) Configure the authentication method list from the Enable List drop-down menu. Thisoption defines the authentication method for users requiring the administrator privilege.

➢ **Entry Description:**

Module: Lists of the configurable applications on the switch.

Login List: Configure an application for the login utilizing a previously configured method list.

Enable List: Configure an application to promote the user level to admin-level users utilizing a previously configured method list.

14.11.8 802.1X Authentication Server Config

This page is used to configure the RADIUS server group used in 802.1X Authentication, Accounting and IGMP Authentication.

Choose the menu **Network Security→AAA→Dot1x List** to load the following page.

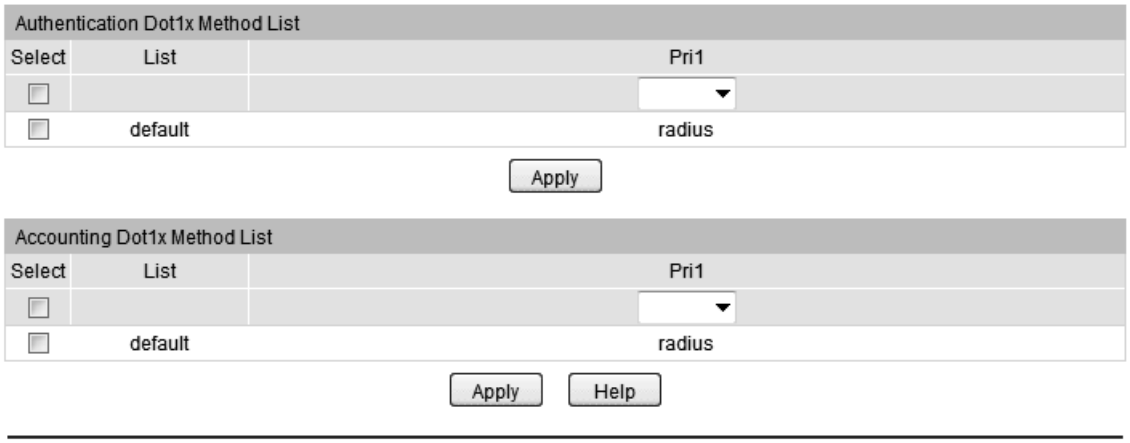


Figure 14-39 802.1X Config

➢ **Configuration Procedure**

1) Configure the 802.1X function globally and on the supplicant-connected port. Please refer to 802.1X for more details.
2) Configure the 802.1X Aunthentication RADIUS server group in the Authentication Dot1x Method List Table.
3) Configure the 802.1X Accounting RADIUS server group in the Authentication Dot1x Method List Table.

14.11.9 Default Settings

The AAA function is disabled by default.

No enable password is configure by default.

The RADIUS server's Auth Port is 1812, Acct Port is 1813, Retransmit is 2 times and Timeout is 5 seconds.

The TACACS+ server's communication Port is 49 and Timeout is 5 seconds.

All RADIUS servers are added in the server group radius.

All TACACS+ servers are added in the Server group tacacs.

The Authentication Login Method List contains local by default, and the default login username and passwords are both admin.

The Authentication Enable Method List is empty by default, which means users can prompt to administrator privilege without password.

The application console/telnet/ssh/http use the default Login List and default Enable list by default.

The 802.1X authentication uses the radius server group by default. The 802.1X accounting uses the radius server group by default.

Return to CONTENTS

Chapter 15 SNMP

- **SNMP Overview**

SNMP (Simple Network Management Protocol) has gained the most extensive application on the UDP/IP networks. SNMP provides a management frame to monitor and maintain the network devices. It is used for automatically managing the various network devices no matter the physical differences of the devices. Currently, the most network management systems are based on SNMP.

SNMP is simply designed and convenient for use with no need of complex fulfillment procedures and too much network resources. With SNMP function enabled, network administrators can easily monitor the network performance, detect the malfunctions and configure the network devices. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

- **SNMP Management Frame**

SNMP management frame includes three network elements: SNMP Management Station, SNMP Agent and MIB (Management Information Base).

SNMP Management Station: SNMP Management Station is the workstation for running the SNMP client program, providing a friendly management interface for the administrator to manage the most network devices conveniently.

SNMP Agent: Agent is the server software operated on network devices with the responsibility of receiving and processing the request packets from SNMP Management Station. In the meanwhile, Agent will inform the SNMP Management Station of the events whenever the device status changes or the device encounters any abnormalities such as device reboot.

MIB: MIB is the set of the managed objects. MIB defines a few attributes of the managed objects, including the names, the access rights, and the data types. Every SNMP Agent has its own MIB. The SNMP Management station can read/write the MIB objects based on its management right.

SNMP Management Station is the manager of SNMP network while SNMP Agent is the managed object. The information between SNMP Management Station and SNMP Agent are exchanged through SNMP (Simple Network Management Protocol). The relationship among SNMP Management Station, SNMP Agent and MIB is illustrated in the following figure.

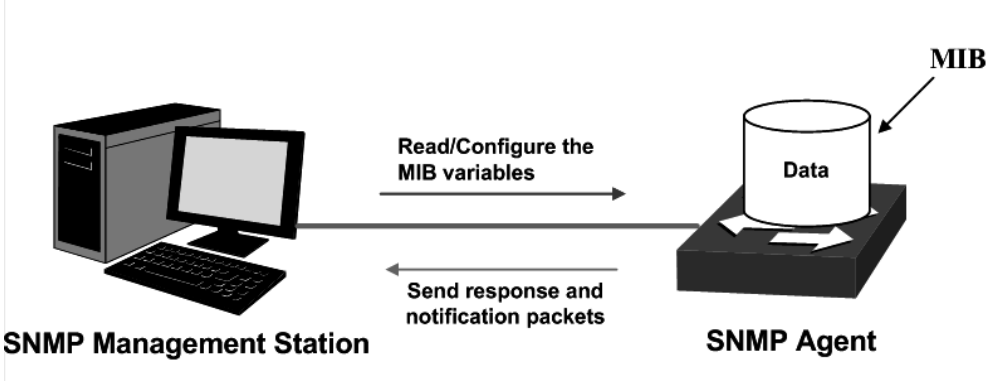


Figure 15-1 Relationship among SNMP Network Elements

➢ **SNMP Versions**

This switch supports SNMP v3, and is compatible with SNMP v1 and SNMP v2c. The SNMP versions adopted by SNMP Management Station and SNMP Agent should be the same. Otherwise, SNMP Management Station and SNMP Agent cannot communicate with each other normally. You can select the management mode with proper security level according to your actual application requirement.

SNMP v1: SNMP v1 adopts Community Name authentication. The community name is used to define the relation between SNMP Management Station and SNMP Agent. The SNMP packets failing to pass community name authentication are discarded. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password.

SNMP v2c: SNMP v2c also adopts community name authentication. It is compatible with SNMP v1 while enlarges the function of SNMP v1.

SNMP v3: Based on SNMP v1 and SNMP v2c, SNMP v3 extremely enhances the security and manageability. It adopts VACM (View-based Access Control Model) and USM (User-Based Security Model) authentication. The user can configure the authentication and the encryption functions. The authentication function is to limit the access of the illegal user by authenticating the senders of packets. Meanwhile, the encryption function is used to encrypt the packets transmitted between SNMP Management Station and SNMP Agent so as to prevent any information being stolen. The multiple combinations of authentication function and encryption function can guarantee a more reliable communication between SNMP Management station and SNMP Agent.

➢ **MIB Introduction**

To uniquely identify the management objects of the device in SNMP messages, SNMP adopts the hierarchical architecture to identify the managed objects. It is like a tree, and each tree node represents a managed object, as shown in the following figure. Thus the object can be identified with the unique path starting from the root and indicated by a string of numbers. The number string is the Object Identifier of the managed object. In the following figure, the OID of the managed object B is {1.2.1.1}. While the OID of the managed object A is {1.2.1.1.5}.

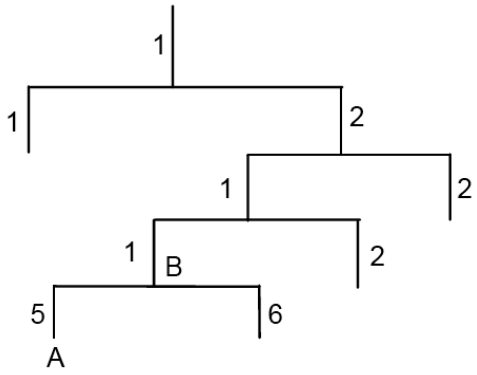


Figure 15-2 Architecture of the MIB tree

➢ **SNMP Configuration Outline**

1. Create View

The SNMP View is created for the SNMP Management Station to manage MIB objects. The managed object, uniquely identified by OID, can be set to under or out of the management of SNMP Management Station by configuring its view type (included/excluded). The OID of managed object can be found on the SNMP client program running on the SNMP Management Station.

2. Create SNMP Group

After creating the SNMP View, it's required to create a SNMP Group. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group. The Groups with these three items the same are considered to be the same. You can configure SNMP Group to control the network access by providing the users in various groups with different management rights via the Read View, Write View and Notify View.

3. Create SNMP User

The User configured in a SNMP Group can manage the switch via the client program on management station. The specified User Name and the Auth/Privacy Password are used for SNMP Management Station to access the SNMP Agent, functioning as the password.

SNMP module is used to configure the SNMP function of the switch, including three submenus: **SNMP Config**, **Notification** and **RMON**.

15.1 SNMP Config

The **SNMP Config** can be implemented on the **Global Config**, **SNMP View**, **SNMP Group**, **SNMP User** and **SNMP Community** pages.

15.1.1 Global Config

To enable SNMP function, please configure the SNMP function globally on this page.

Choose the menu **SNMP→SNMP Config→Global Config** to load the following page.

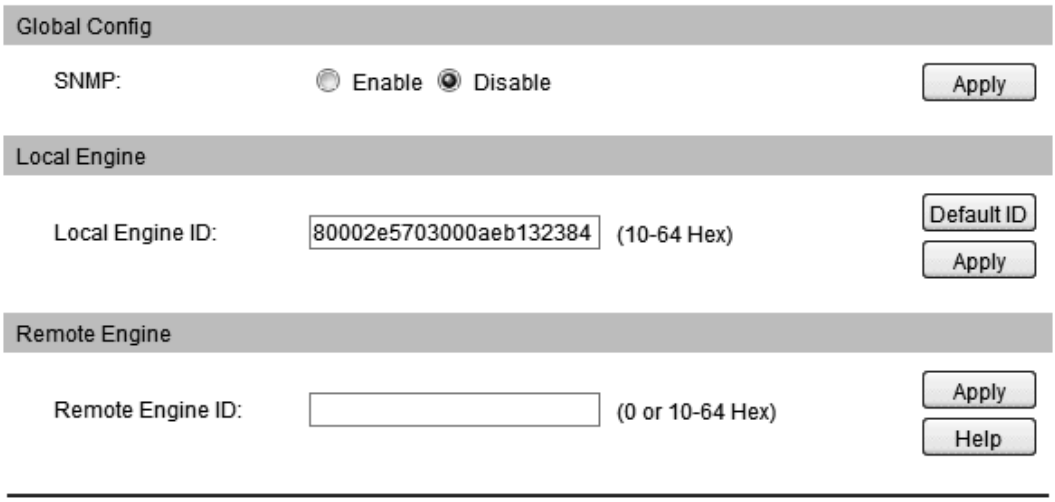


Figure 15-3 Global Config

The following entries are displayed on this screen:

- **Global Config**

  SNMP: Enable/Disable the SNMP function.

- **Local Engine**

  Local Engine ID: Specify the switch's Engine ID for the remote clients. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the switch.

- **Remote Engine**

  Remote Engine ID: Specify the Remote Engine ID for switch. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the remote device which receives traps and informs from switch.

Note:

The amount of Engine ID characters must be even.

15.1.2 SNMP View

The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Choose the menu **SNMP→SNMP Config→SNMP View** to load the following page.

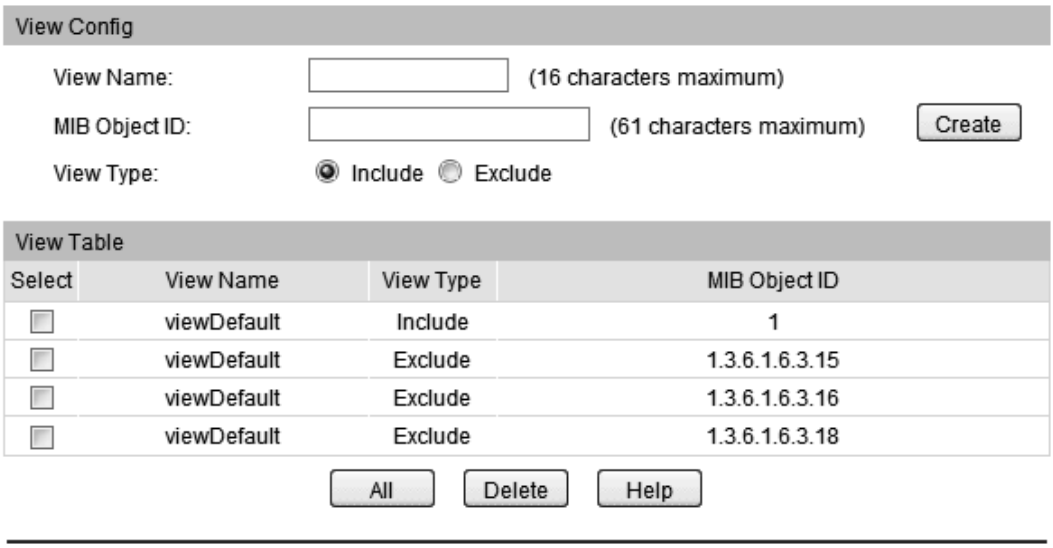


Figure 15-4 SNMP View

The following entries are displayed on this screen:

- **View Config**

View Name: Give a name to the View for identification. Each View can include several entries with the same name.

MIB Object ID: Enter the Object Identifier (OID) for the entry of View.

View Type: Select the type for the view entry.

- **Include**: The view entry can be managed by the SNMP management station.
- **Exclude**: The view entry cannot be managed by the SNMP management station.

- **View Table**

Select: Select the desired entry to delete the corresponding view. All the entries of a View will be deleted together.

View Name: Displays the name of the View entry.

View Type: Displays the type of the View entry.

MIB Object ID: Displays the OID of the View entry.

15.1.3 SNMP Group

On this page, you can configure SNMP Group to control the network access by providing the users in various groups with different management rights via the Read View, Write View and Notify View.

Choose the menu **SNMP→SNMP Config→SNMP Group** to load the following page.

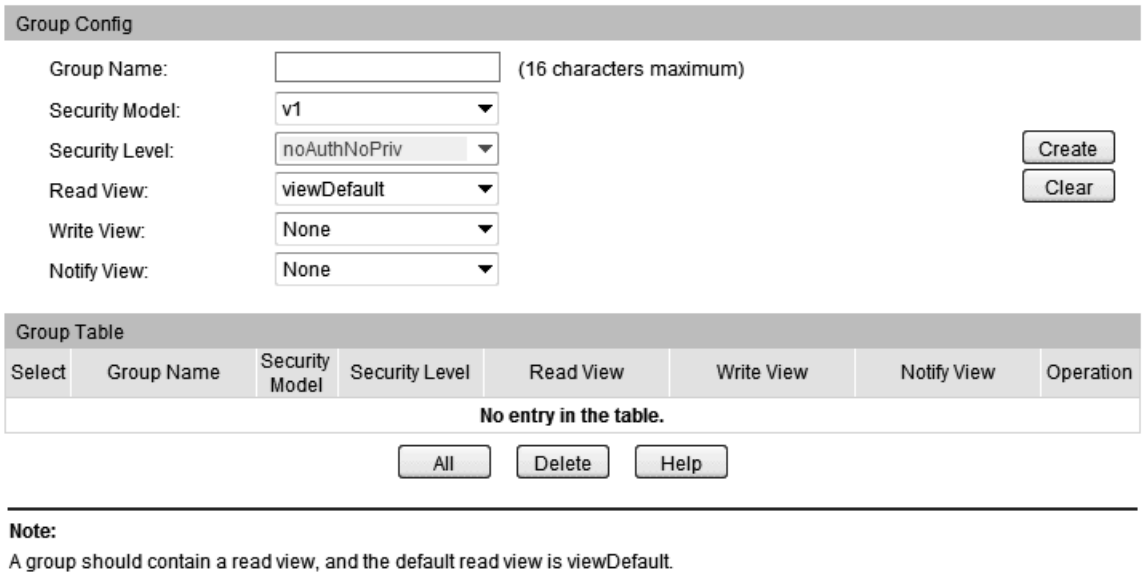


Figure 15-5 SNMP Group

The following entries are displayed on this screen:

➢ **Group Config**

Group Name: Enter the SNMP Group name. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group. The Groups with these three items the same are considered to be the same.

Security Model: Select the Security Model for the SNMP Group.

- **v1**: SNMPv1 is defined for the group. In this model, the Community Name is used for authentication. SNMP v1 can be configured on the SNMP Community page directly.
- **v2c**: SNMPv2c is defined for the group. In this model, the Community Name is used for authentication. SNMP v2c can be configured on the SNMP Community page directly.
- **v3**: SNMPv3 is defined for the group. In this model, the USM mechanism is used for authentication. If SNMPv3 is enabled, the Security Level field is enabled for configuration.

Security Level: Select the Security Level for the SNMP v3 Group.

- **noAuthNoPriv**: No authentication and no privacy security level is used.
- **authNoPriv**: Only the authentication security level is used.
- **authPriv**: Both the authentication and the privacy security levels are used.

Read View: Select the View to be the Read View. The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View.

Write View: Select the View to be the Write View. The management access is writing only and changes can be made to the assigned SNMP View. The View defined both as the Read View and the Write View can be read and modified.

Notify View: Select the View to be the Notify View. The management station can receive trap messages of the assigned SNMP view generated by the switch's SNMP agent.

- **Group Table**

Select: Select the desired entry to delete the corresponding group. It is multi-optional.

Group Name: Displays the Group Name here.

Security Model: Displays the Security Model of the group.

Security Level: Displays the Security Level of the group.

Read View: Displays the Read View name in the entry.

Write View: Displays the Write View name in the entry.

Notify View: Displays the Notify View name in the entry.

Operation: Click the **Edit** button to modify the Views in the entry and click the **Modify** button to apply.

Note:

Every Group should contain a Read View. The default Read View is viewDefault.

15.1.4 SNMP User

The User in a SNMP Group can manage the switch via the management station software. The User and its Group have the same security level and access right. You can configure the SNMP User on this page.

Choose the menu **SNMP→SNMP Config→SNMP User** to load the following page.

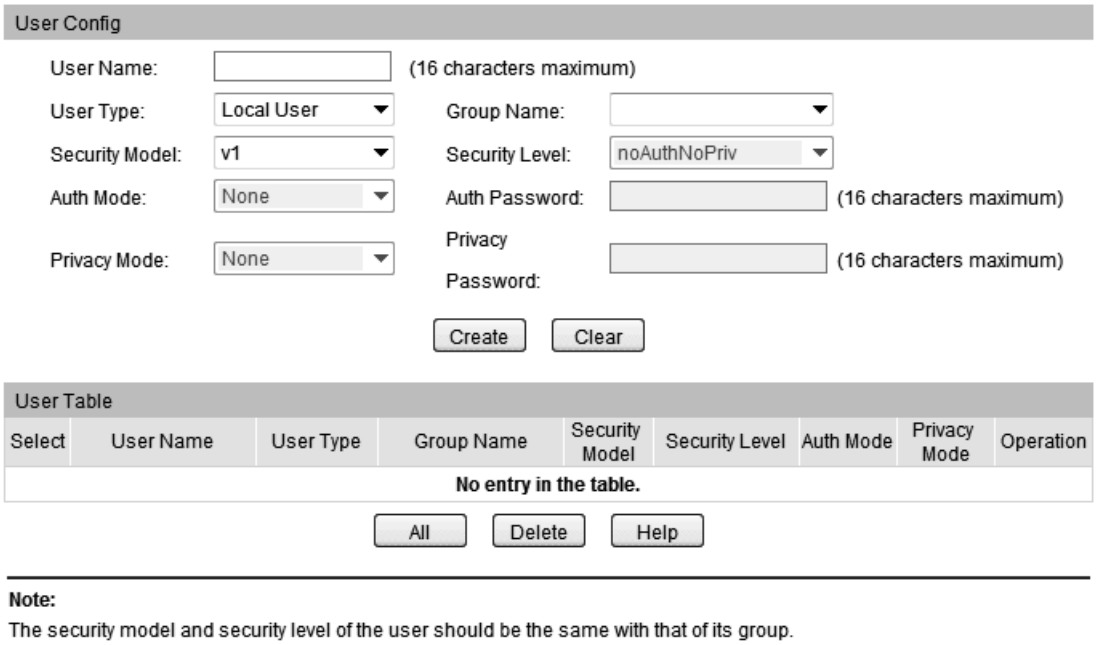


Figure 15-6 SNMP User

The following entries are displayed on this screen:

➢ **User Config**

User Name: Enter the User Name here.

User Type: Select the type for the User.

- **Local User**: Indicates that the user is connected to a local SNMP engine.
- **Remote User**: Indicates that the user is connected to a remote SNMP engine.

Group Name: Select the Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

Security Model: Select the Security Model for the User.

Security Level: Select the Security Level for the SNMP v3 User.

Auth Mode: Select the Authentication Mode for the SNMP v3 User.

- **None**: No authentication method is used.
- **MD5**: The port authentication is performed via HMAC-MD5 algorithm.
- **SHA**: The port authentication is performed via SHA (Secure Hash Algorithm). This authentication mode has a higher security than MD5 mode.

Auth Password: Enter the password for authentication.

Privacy Mode: Select the Privacy Mode for the SNMP v3 User.

- **None**: No privacy method is used.

- **DES**: DES encryption method is used.

Privacy Password: Enter the Privacy Password.

➢ **User Table**

Select: Select the desired entry to delete the corresponding User. It is multi-optional.

User Name: Displays the name of the User.

User Type: Displays the User Type.

Group Name: Displays the Group Name of the User.

Security Model: Displays the Security Model of the User.

Security Level: Displays the Security Level of the User.

Auth Mode: Displays the Authentication Mode of the User.

Privacy Mode: Displays the Privacy Mode of the User.

Operation: Click the **Edit** button to modify the Group of the User and click the **Modify** button to apply.

Note:

The SNMP User and its Group should have the same Security Model and Security Level.

15.1.5 SNMP Community

SNMP v1 and SNMP v2c adopt community name authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password. If SNMP v1 or SNMP v2c is employed, you can directly configure the SNMP Community on this page without configuring SNMP Group and User.

Choose the menu **SNMP→SNMP Config→SNMP Community** to load the following page.

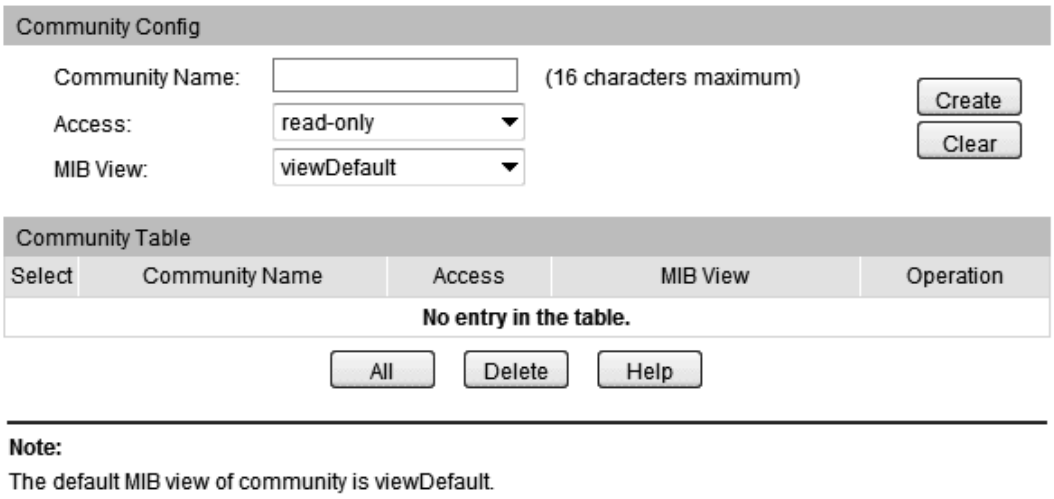


Figure 15-7 SNMP Community

The following entries are displayed on this screen:

➢ **Community Config**

Community Name: Enter the Community Name here.

Access: Defines the access rights of the community.

- **read-only:** Management right of the Community is restricted to read-only, and changes cannot be made to the corresponding View.
- **read-write:** Management right of the Community is read-write and changes can be made to the corresponding View.

MIB View: Select the MIB View for the community to access.

➢ **Community Table**

Select: Select the desired entry to delete the corresponding Community. It is multi-optional.

Community Name: Displays the Community Name here.

Access: Displays the right of the Community to access the View.

MIB View: Displays the Views which the Community can access.

Operation: Click the **Edit** button to modify the MIB View and the Access right of the Community, and then click the **Modify** button to apply.

Note:

The default MIB View of SNMP Community is viewDefault.

Configuration Procedure:

- If SNMPv3 is employed, please take the following steps:

Step	Operation	Description
1	Enable **SNMP** function globally.	Required. On the **SNMP→SNMP Config→Global Config** page, enable **SNMP** function globally.
2	Create SNMP View.	Required. On the **SNMP→SNMP Config→SNMP View** page, create SNMP View of the management agent. The default View Name is viewDefault and the default OID is 1.
3	Create SNMP Group.	Required. On the **SNMP→SNMP Config→SNMP Group** page, create SNMP Group for SNMPv3 and specify SNMP Views with various access levels for SNMP Group.
4	Create SNMP User.	Required. On the **SNMP→SNMP Config→SNMP**

		User page, create SNMP User in the Group and configure the auth/privacy mode and auth/privacy password for the User.

- If SNMPv1 or SNMPv2c is employed, please take the following steps:

Step	Operation		Description
1	Enable SNMP function globally.		Required. On the **SNMP→SNMP Config→Global Config** page, enable **SNMP** function globally.
2	Create SNMP View.		Required. On the **SNMP→SNMP Config→SNMP View** page, create SNMP View of the management agent. The default View Name is viewDefault and the default OID is 1.
3	Configure access level for the User.	Create SNMP Community directly.	Required alternatively. • Create SNMP Community directly. On the **SNMP→SNMP Config→SNMP Community** page, create SNMP Community based on SNMP v1 and SNMP v2c. • Create SNMP Group and SNMP User. Similar to the configuration way based on SNMPv3, you can create SNMP Group and SNMP User of SNMP v1/v2c. The User name can limit access to the SNMP agent from SNMP network management station, functioning as a community name. The users can manage the device via the Read View, Write View and Notify View defined in the SNMP Group.
		Create SNMP Group and SNMP User.	

15.2 Notification

With the Notification function enabled, the switch can initiatively report to the management station about the important events that occur on the Views (e.g., the managed device is rebooted), which allows the management station to monitor and process the events in time.

The notification information includes the following two types:

Trap：Trap is the information that the managed device initiatively sends to the Network management station without request.

Inform：Inform packet is sent to inform the management station and ask for the reply. The switch will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times. The Inform type, employed on SNMPv2c and SNMPv3, has a higher security than the Trap type.

On this page, you can configure the notification function of SNMP.

Choose the menu **SNMP→Notification→Notification Config** to load the following page.

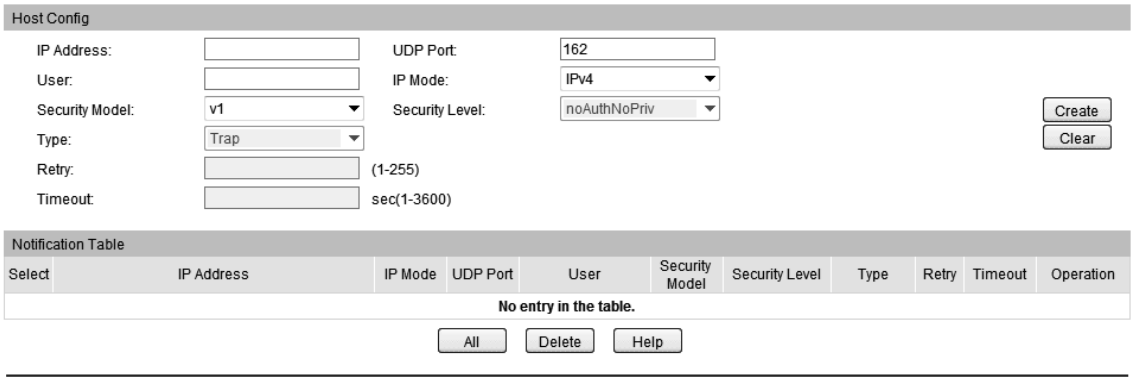


Figure 15-8 Notification Config

The following entries are displayed on this screen:

➢ **Host Config**

IP Address: Enter the IP Address of the management Host.

User: Enter the User name of the management station.

Security Model: Select the Security Model of the management station.

Type: Select the type for the notifications.

- **Trap:** Indicates traps are sent.
- **Inform:** Indicates informs are sent. The Inform type has a higher security than the Trap type.

Retry: Specify the amount of times the switch resends an inform request. The switch will resend the inform request if it doesn't get the response from the management station during the **Timeout** interval, and it will terminate resending the inform request if the resending times reach the specified **Retry** times.

Timeout: Specify the maximum time for the switch to wait for the response from the management station before resending a request.

UDP Port: Enter the number of the UDP port used to send notifications. The UDP port functions with the IP address for the notification sending. The default is 162.

IP Mode: Select the IP mode of the IP address.

Security Level: Select the Security Model of the management station.

➢ **Notification Table**

Select: Select the desired entry to delete the corresponding management station.

IP Address:	Displays the IP Address of the management host.
IP Mode:	Displays the IP mode of the IP address.
UDP Port:	Displays the UDP port used to send notifications.
User:	Displays the User name of the management station.
Security Model:	Displays the Security Model of the management station.
Security Level:	Displays the Security Level for the SNMP v3 User.
Type:	Displays the type of the notifications.
Retry:	Displays the amount of times the switch resends an inform request.
Timeout:	Displays the maximum time for the switch to wait for the response from the management station before resending a request.
Operation:	Click the **Edit** button to modify the corresponding entry and click the **Modify** button to apply.

15.3 RMON

RMON (Remote Monitoring) based on SNMP (Simple Network Management Protocol) architecture, functions to monitor the network. RMON is currently a commonly used network management standard defined by Internet Engineering Task Force (IETF), which is mainly used to monitor the data traffic across a network segment or even the entire network so as to enable the network administrator to take the protection measures in time to avoid any network malfunction. In addition, RMON MIB records network statistics information of network performance and malfunction periodically, based on which the management station can monitor network at any time effectively. RMON is helpful for network administrator to manage the large-scale network since it reduces the communication traffic between management station and managed agent.

- **RMON Group**

This switch supports the following four RMON Groups defined on the RMON standard (RFC1757): History Group, Event Group, Statistic Group and Alarm Group.

RMON Group	Function
History Group	After a history group is configured, the switch collects and records network statistics information periodically, based on which the management station can monitor network effectively.
Event Group	Event Group is used to define RMON events. Alarms occur when an event is detected.

RMON Group	Function
Statistic Group	Statistic Group is set to monitor the statistic of alarm variables on the specific ports.
Alarm Group	Alarm Group is configured to monitor the specific alarm variables. When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the switch to act in the set way.

The **RMON** Groups can be configured on the **Statistics**, **History, Event** and **Alarm** pages.

15.3.1 Statistics

On this page you can configure and view the statistics entry.

Choose the menu **SNMP→RMON→Statistics** to load the following page.

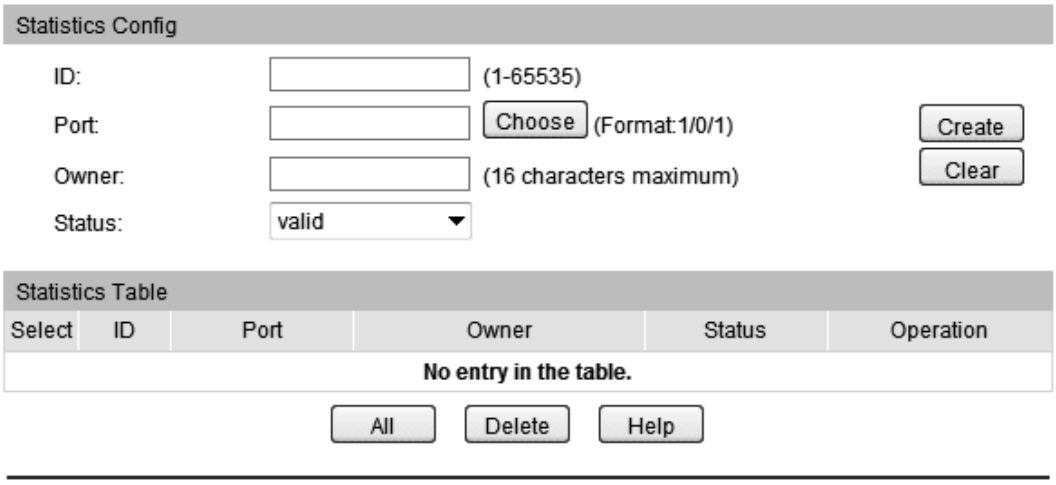


Figure 15-9 Statistics

The following entries are displayed on this screen:

- **Statistics Config**

  ID: Enter the ID number of statistics entry, ranging from 1 to 65535.

  Port: Enter or choose the Ethernet interface from which to collect the statistics.

  Owner: Enter the owner name.

  Status: Choose the status of statistics entry.
  - **valid**: The entry exists and is valid.
  - **underCreation**: The entry exists, but is not valid.

- **Statistics Table**

  Select: Select the desired entry to delete the corresponding statistics entry. It's multi-optional.

ID: Displays the ID number of the statistics entry.

Port: Displays the Ethernet interface from which to collect the statistics.

Owner: Displays the owner name.

Status: Displays the status of the statistics entry.

15.3.2 History

On this page, you can configure the History Group for RMON.

Choose the menu **SNMP→RMON→History** to load the following page.

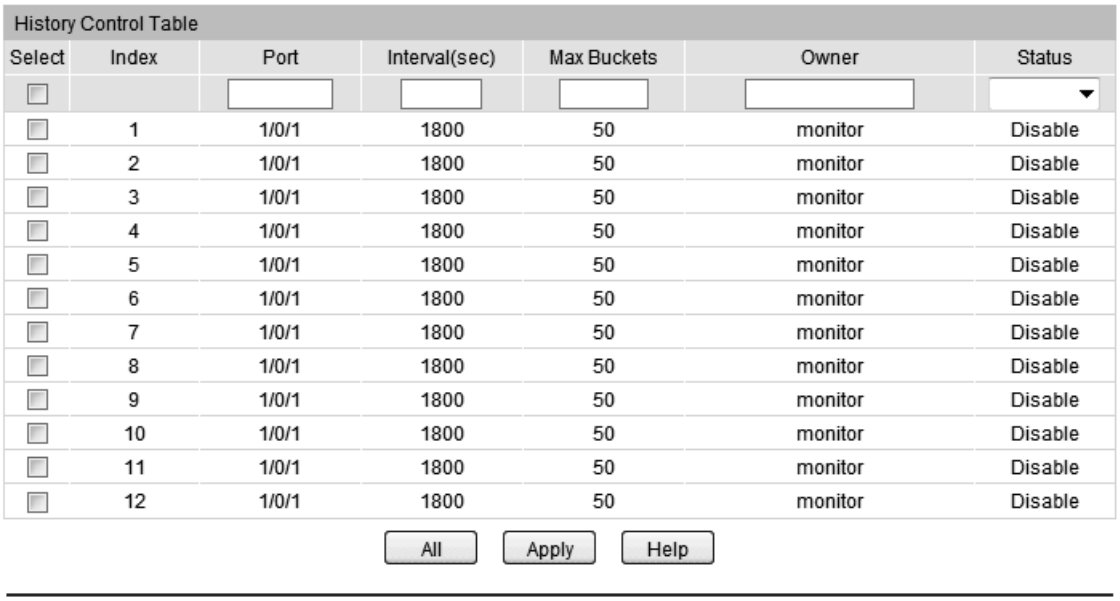


Figure 15-10 History Control

The following entries are displayed on this screen:

➢ **History Control Table**

Select: Select the desired entry for configuration.

Index: Displays the index number of the entry.

Port: Specify the port from which the history samples were taken.

Interval: Specify the interval to take samplings from the port.

Max Buckets: Displays the maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets. 130 buckets supported at most so far.

Owner: Enter the name of the device or user that defined the entry.

Status: Select Enable/Disable the corresponding sampling entry.

15.3.3 Event

On this page, you can configure the RMON events.

Choose the menu **SNMP→RMON→Event** to load the following page.

Event Table

Select	Index	User	Description	Type	Owner	Status
	1	public		None	monitor	Disable
	2	public		None	monitor	Disable
	3	public		None	monitor	Disable
	4	public		None	monitor	Disable
	5	public		None	monitor	Disable
	6	public		None	monitor	Disable
	7	public		None	monitor	Disable
	8	public		None	monitor	Disable
	9	public		None	monitor	Disable
	10	public		None	monitor	Disable
	11	public		None	monitor	Disable
	12	public		None	monitor	Disable

All Apply Help

Figure 15-11 Event Config

The following entries are displayed on this screen:

➢ **Event Table**

Select: Select the desired entry for configuration.

Index: Displays the index number of the entry.

User: Enter the name of the User or the community to which the event belongs.

Description: Give a description to the event for identification.

Type: Select the event type, which determines the act way of the network device in response to an event.

- **None**: No processing.
- **Log**: Logging the event.
- **Notify**: Sending trap messages to the management station.
- **Log&Notify**: Logging the event and sending trap messages to the management station.

Owner: Enter the name of the device or user that defined the entry.

Status: Select Enable/Disable the corresponding event entry.

15.3.4 Alarm Config

On this page, you can configure Statistic Group and Alarm Group for RMON.

Choose the menu **SNMP→RMON→Alarm** to load the following page.

Figure 15-12 Alarm Config

The following entries are displayed on this screen:

- **Alarm Config**

Select: Select the desired entry for configuration.

Index: Displays the index number of the entry.

Variable: Select the alarm variables from the pull-down list.

Statistics: Select the RMON statistics entry from which we get the value of the selected alarm variable.

Sample Type: Specify the sampling method for the selected variable and comparing the value against the thresholds.

- **Absolute:** Compares the values directly with the thresholds at the end of the sampling interval.
- **Delta:** Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Rising Threshold: Enter the rising counter value that triggers the Rising Threshold alarm.

Rising Event: Select the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold.

Falling Threshold: Enter the falling counter value that triggers the Falling Threshold alarm.

Falling Event: Select the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold.

Alarm Type:	Specify the type of the alarm. • **All:** The alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold. • **Rising:** When the sampled value exceeds the Rising Threshold, an alarm event is triggered. • **Falling:** When the sampled value is under the Falling Threshold, an alarm event is triggered.
Interval:	Enter the alarm interval time in seconds.
Owner:	Enter the name of the device or user that defined the entry.
Status:	Select Enable/Disable the corresponding alarm entry.

Note:

When alarm variables exceed the Threshold on the same direction continuously for several times, an alarm event will only be generated on the first time, that is, the Rising Alarm and Falling Alarm are triggered alternately for that the alarm following to Rising Alarm is certainly a Falling Alarm and vice versa.

Return to CONTENTS

Chapter 16 LLDP

LLDP (Link Layer Discovery Protocol) is a Layer 2 protocol that is used for network devices to advertise their own device information periodically to neighbors on the same IEEE 802 local area network. The advertised information, including details such as device identification, capabilities and configuration settings, is represented in TLV (Type/Length/Value) format according to the IEEE 802.1ab standard, and these TLVs are encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit). The LLDPDU distributed via LLDP is stored by its recipients in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

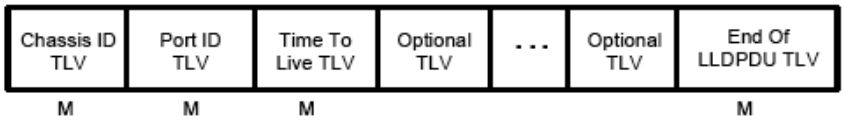
An IETF Standard MIB, as well as a number of vendor specific MIBs, have been created to describe a network's physical topology and associated systems within that topology. However, there is no standard protocol for populating these MIBs or communicating this information among stations on the IEEE 802 LAN. LLDP protocol specifies a set. The device running LLDP can automatically discover and learn about the neighbors, allowing for interoperability between the network devices of different vendors. This protocol allows two systems running different network layer protocols to learn about each other.

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power via MDI, inventory management, and device location details.

The LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

➢ LLDPDU Format

Each LLDPDU includes an ordered sequence of three mandatory TLVs followed by one or more optional TLVs plus an End of LLDPDU TLV, as shown in the figure below. Chassis ID TLV, Port ID TLV, TTL TLV and End TLV are the four mandatory TLVs for a LLDPDU. Optional TLVs provide various details about the LLDP agent advertising them and they are selected by network management.



M - mandatory TLV - required for all LLDPDUs

The maximum length of the LLDPDU shall be the maximum information field length allowed by the particular transmission rate and protocol. In IEEE 802.3 MACs, for example, the maximum LLDPDU length is the maximum data field length for the basic, untagged MAC frame (1500 octets).

➢ LLDP Working Mechanism

1) LLDP Admin Status

The transmission and the reception of LLDPDUs can be separately enabled for every port, making it possible to configure an implementation to restrict the port either to transmit only or receive only, or to allow the port to both transmit and receive LLDPDUs. Four LLDP admin statuses are supported by each port.

- Tx&Rx: the port can both transmit and receive LLDPDUs.
- Rx_Only: the port can receive LLDPDUs only.
- Tx_Only: the port can transmit LLDPDUs only.
- Disable: the port cannot transmit or receive LLDPDUs.

2) LLDPDU transmission mechanism

- If the ports are working in TxRx or Tx mode, they will advertise local information by sending LLDPDUs periodically.
- If there is a change in the local device, the change notification will be advertised. To prevent a series of successive LLDPDUs transmissions during a short period due to frequent changes in local device, a transmission delay timer is set by network management to ensure that there is a defined minimum time between successive LLDP frame transmissions.
- If the LLDP admin status of the port is changed from Disable/Rx to TxRx/Tx, the Fast Start Mechanism will be active, the transmit interval turns to be 1 second, several LLDPDUs will be sent out, and then the transmit interval comes back to the regular interval.

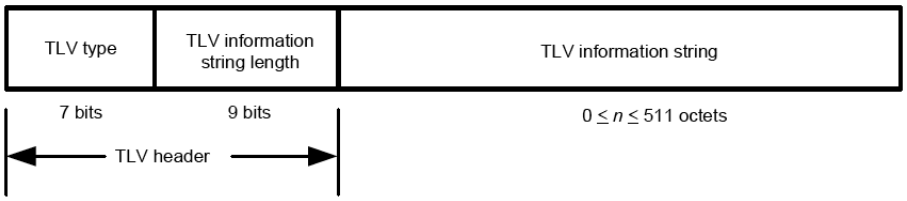
3) LLDPDU receipt mechanism

When a port is working in TxRx or Rx mode, the device will check the validity of the received LLDPDUs and the attached TLVs, save this neighbor information to the local device and then set the aging time of this information according to the TTL value of TTL (Time To Live) TLV. Once the TTL is 0, this neighbor information will be aged out immediately.

The aging time of the local information in the neighbor device is determined by TTL. Hold Multiplier is a multiplier on the Transmit Interval that determines the actual TTL value used in an LLDPDU. TTL = Hold Multiplier * Transmit Interval.

➢ TLV

TLV refers to Type/Length/Value and is contained in a LLDPDU. Type identifies what kind of information is being sent, Length indicates the length of information string in octets and Value is the actual information to be sent. The basic TLV Format is shown as follows:



Each TLV is identified by a unique TLV type value that indicates the particular kind of information contained in the TLV.

The following table shows the details about the currently defined TLVs.

TLV type	TLV Name	Description	Usage in LLDPDU
0	End of LLDPDU	Mark the end of the TLV sequence in LLDPDUs. Any information following an End Of LLDPDU TLV shall be ignored.	Mandatory
1	Chassis ID	Identifies the Chassis address of the connected device.	Mandatory
2	Port ID	Identifies the specific port that transmitted the LLDP frame. When the device does not advertise MED TLV, this field displays the port name of the port; when the device advertises MED TLV, this field displays the MAC address of the port.	Mandatory
3	Time To Live	Indicates the number of seconds that the neighbor device is to regard the local information to be valid.	Mandatory
4	Port Description	Identifies the description string of the port.	Optional
5	System Name	Identifies the system name.	Optional
6	System Description	Identifies the system description.	Optional
7	System Capabilities	Identifies the main functions of the system and the functions enabled.	Optional
8	Management Address	Identifies the management IP address, the corresponding interface number and OID (Object Identifier). The management IP address is specified by the user.	Optional
127	Organizationally Specific	Allows different organizations, such as IEEE 802.1, IEEE 802.3, IETF, as well as individual software and equipment vendors, to define TLVs that advertise information to remote device.	Optional

Optional TLVs are grouped into two categories including basic management TLV and Organizationally-specific TLV.

1) Basic Management TLV

A set of TLVs considered to be basic to the management of the network stations are required for all LLDP implementations.

2) Organizationally Specific TLV

Different organizations have defined various TLVs. For instance, Port VLAN ID TLV, Port and Protocol VLAN ID TLV, VLAN Name TLV And Protocol Identity TLV are defined by IEEE 802.1, while MAC/PHY Configuration/Status TLV, Power Via MDI TLV, Link Aggregation TLV and Maximum Frame TLV are defined by IEEE 802.3. Some specific TLVs are for LLDP-MED protocol, such as LLDP-MED Capabilities TLV, Network Policy TLV, Extended Power-via-MDI TLV, Hardware Revision TLV and so on.

Note:

For detailed introduction of TLV, please refer to IEEE 802.1AB standard and ANSI/TIA-1057.

In switch, the following LLDP optional TLVs are supported.

TLV Type	Description
Port Description TLV	The Port Description TLV allows network management to advertise the IEEE 802 LAN station's port description.
System Capabilities TLV	The System Capabilities TLV identifies the primary functions of the system and whether or not these primary functions are enabled.
System Description TLV	The System Description TLV allows network management to advertise the system's description, which should include the full name and version identification of the system's hardware type, software operating system, and networking software.
System Name TLV	The System Name TLV allows network management to advertise the system's assigned name, which should be the system's fully qualified domain name.
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher entities to assist discovery by network management.
Port VLAN ID TLV	The Port VLAN ID TLV allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
Port And Protocol VLAN ID TLV	The Port And Protocol VLAN ID TLV allows a bridge port to advertise a port and protocol VLAN ID.
VLAN Name TLV	The VLAN Name TLV allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation.
MAC/PHY Configuration/Status TLV	The MAC/PHY Configuration/Status TLV identifies: a)The duplex and bit-rate capability of the sending IEEE 802.3 LAN node that is connected to the physical medium; b)The current duplex and bit-rate settings of the sending IEEE 802.3 LAN node; c)Whether these settings are the result of auto-negotiation during link initiation or of manual set override

	action.
Max Frame Size TLV	The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

The LLDP module is mainly for LLDP function configuration of the switch, including three submenus: **Basic Config**, **Device Info**, **Device Statistics** and **LLDP-MED**.

16.1 Basic Config

LLDP is configured on the **Global Config** and **Port Config** pages.

16.1.1 Global Config

On this page you can configure the LLDP parameters of the device globally.

Choose the menu **LLDP→Basic Config→Global Config** to load the following page.

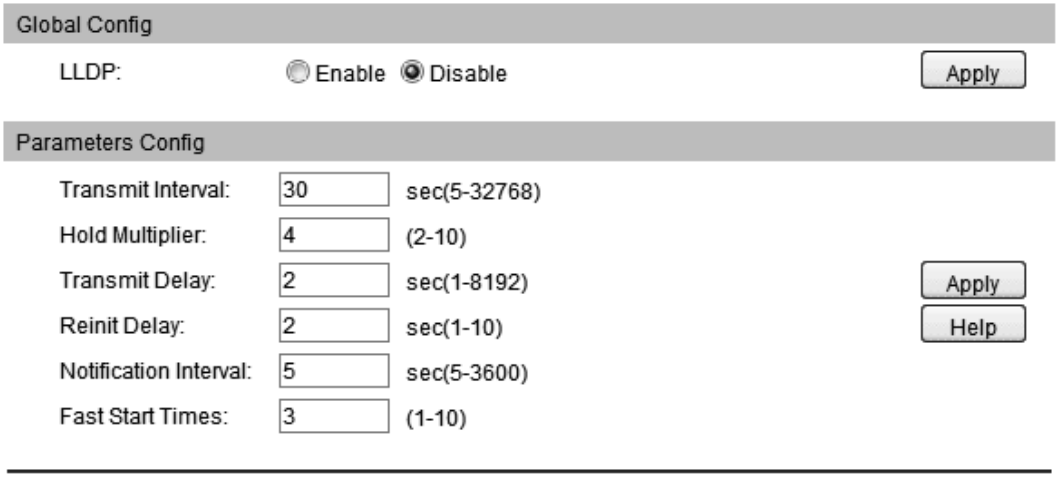


Figure 16-1 LLDP Global Configuration

The following entries are displayed on this screen:

- **Global Config**

  LLDP: Enable/disable LLDP function globally.

- **Parameters Config**

  Transmit Interval: Enter the interval for the local device to transmit LLDPDU to its neighbors. The default value is 30 seconds.

  Hold Multiplier: Enter a multiplier on the Transmit Interval. It determines the actual TTL (Time To Live) value used in an LLDPDU. TTL = Hold Multiplier * Transmit Interval. The default value is 4.

Transmit Delay: Enter a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. The default value is 2 seconds.

Reinit Delay: This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The default value is 2 seconds.

Notification Interval: Specify the interval of Trap message which will be sent from local device to network management system. The default value is 5 seconds.

Fast Start Times: When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The default value is 3.

16.1.2 Port Config

On this page you can configure all ports' LLDP parameters.

Choose the menu **LLDP→Basic Config→Port Config** to load the following page.

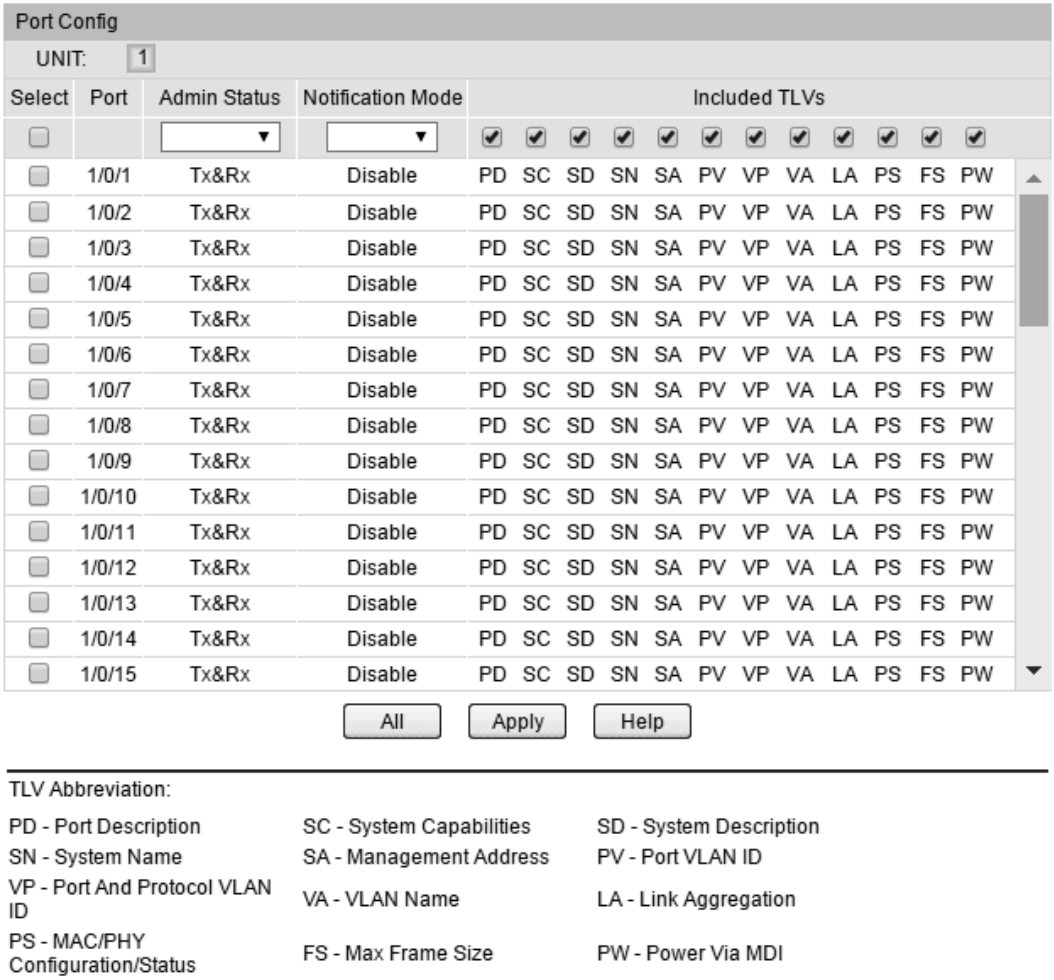


Figure 16-2 LLDP Port Config

The following entries are displayed on this screen:

- **LLDP Port Config**

Port Select:	Select the desired port(s) to configure.
Admin Status:	Select the port's LLDP operating mode: Tx&Rx: send and receive LLDP frames. Rx_Only: Only receive LLDP frames. Tx_Only: Only send LLDP frames. Disable: neither send nor receive LLDP frames.
Notification Mode:	Allows you to enable or disable the ports' SNMP notification. If enabled, the local device will notify the trap event to SNMP server.
Included TLVs:	Select TLVs to be included in outgoing LLDPDU.

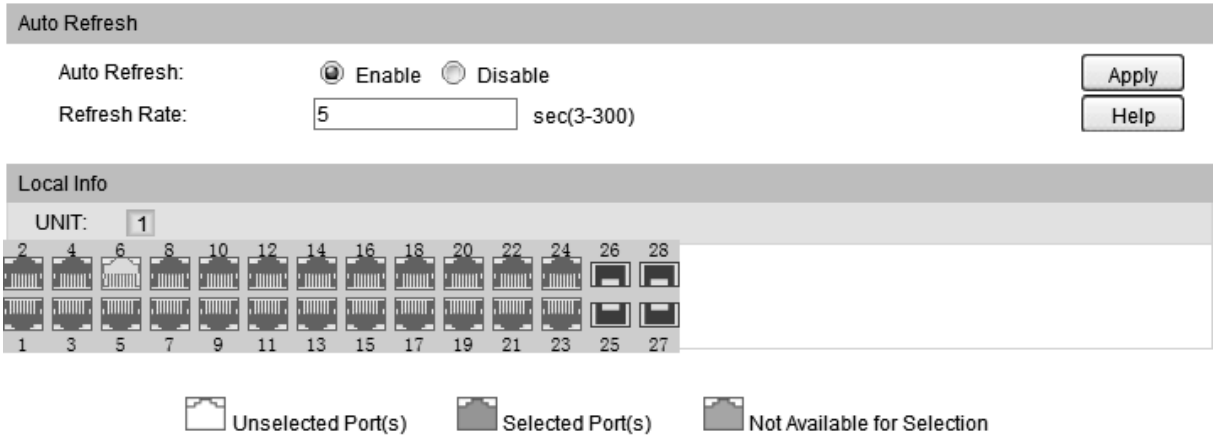
16.2 Device Info

You can view the LLDP information of the local device and its neighbors on the **Local Info** and **Neighbor Info** pages respectively.

16.2.1 Local Info

On this page you can see all ports' configuration and system information.

Choose the menu **LLDP→Device Info→Local Info** to load the following page.



Port 1/0/2

Local Interface:	1/0/2
Chassis ID Subtype:	MAC address
Chassis ID:	00-0A-EB-13-23-7B
Port ID Subtype:	Interface name
Port ID:	GigabitEthernet1/0/2
TTL:	120
Port Description:	GigabitEthernet1/0/2 Interface
System Name:	[redacted]
System Description:	[redacted]
System Capabilities Supported:	Bridge Router
System Capabilities Enabled:	Bridge Router
Management Address:	192.168.0.1

Figure 16-3 LLDP Local Information

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Enable/Disable the auto refresh function.

  Refresh Rate: Specify the auto refresh rate.

- **Local Info**

  Select the desired port number to display the information of the corresponding port.

  Local Interface: Display local port number.

  Chassis ID Subtype: Indicate the basis for the chassis ID, and the default subtype is MAC address.

  Chassis ID: Indicate the specific identifier for the particular chassis in local device.

  Port ID Subtype: Indicate the basis for the port ID, and the default subtype is interface name.

Port ID:	Indicate the specific identifier for the port in local device.
TTL:	Indicate the number of seconds that the recipient LLDP agent is to regard the information associated with this chassis ID and port ID identifier to be valid.
Port Description:	Display local port's description.
System Name:	Indicate local device's administratively assigned name.
System Description:	Display local device's system description.
System Capabilities Supported:	Display the supported function of the local device.
System Capabilities Enabled:	Display the primary function of the local device.
Management Address:	Display the supported function of the local device.

16.2.2 Neighbor Info

On this page you can get the information of the neighbors.

Choose the menu **LLDP→Device Info→Neighbor Info** to load the following page.

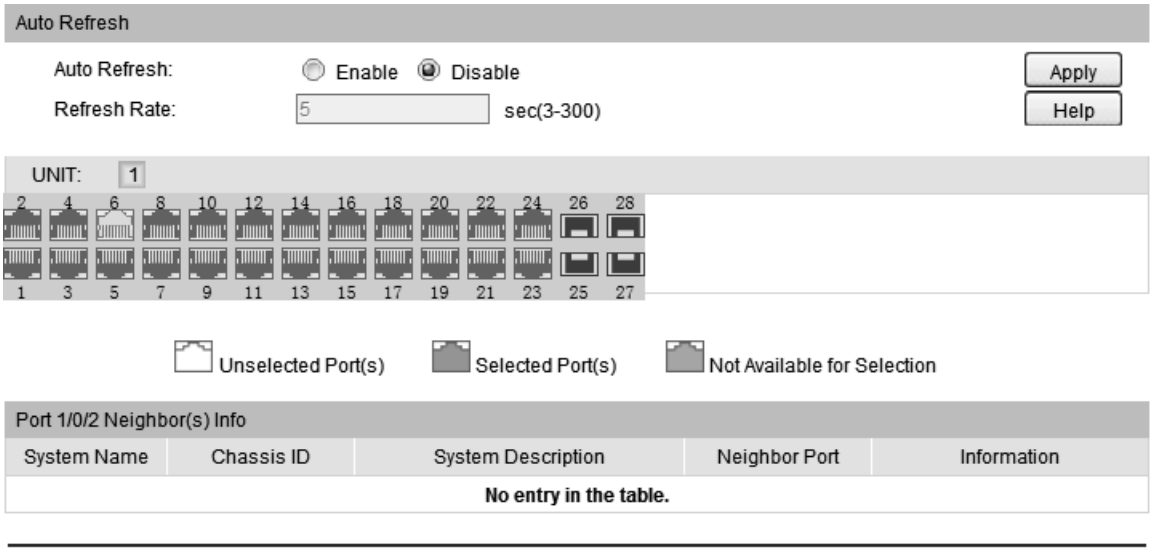


Figure 16-4 LLDP Neighbor Information

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Enable/Disable the auto refresh function.

  Refresh Rate: Specify the auto refresh rate.

- **Neighbor Info**

System Name: Displays the system name of the neighbor device.

Chassis ID: Displays the Chassis ID of the neighbor device.

System Description: Displays the system description of the neighbor device.

Neighbor Port: Displays the port number of the neighbor linking to local port.

Information: Click Information to display the detailed information of the neighbor device.

16.3 Device Statistics

You can view the LLDP statistics of the local device through this feature.

Choose the menu **LLDP→Device Statistics→Statistic Info** to load the following page.

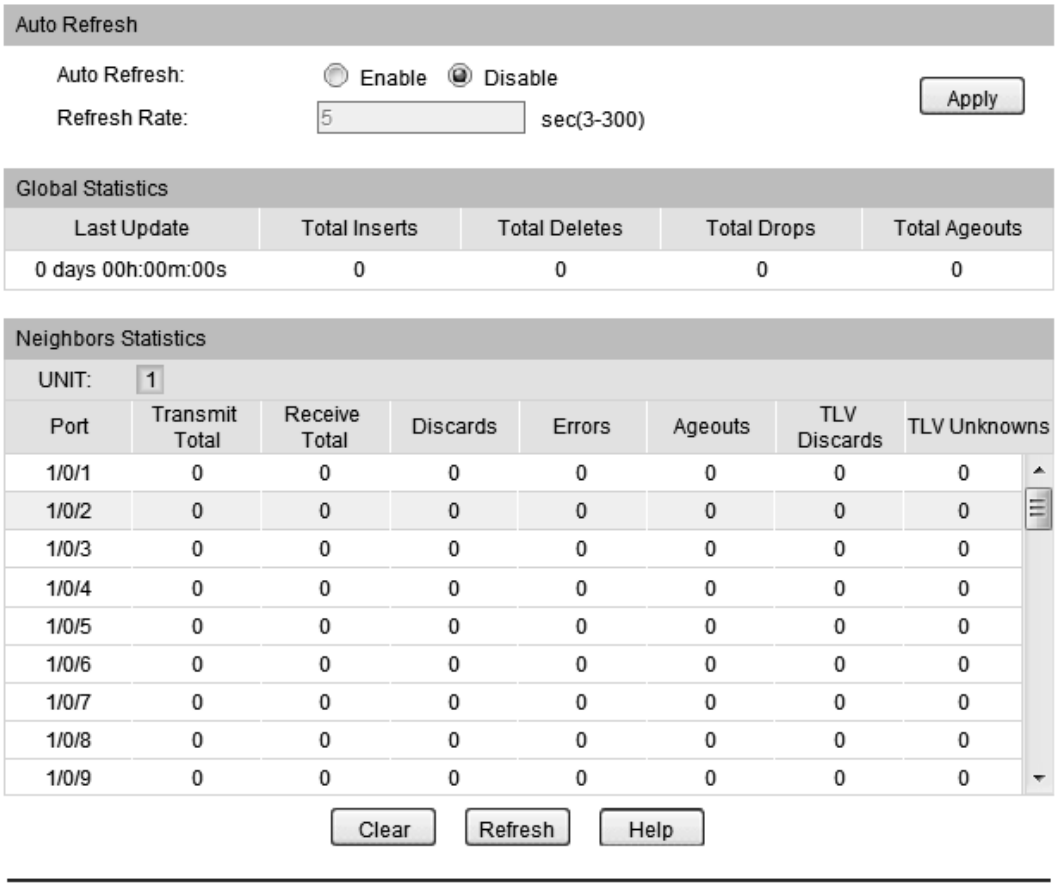


Figure 16-5 LLDP Statistic Information

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Enable/Disable the auto refresh function.

  Refresh Rate: Specify the auto refresh rate.

- **Global Statistics**

Last Update:	Displays latest update time of the statistics.
Total Inserts:	Displays the number of neighbors inserted till last update time.
Total Deletes:	Displays the number of neighbors deleted by local device.
Total Drops:	Displays the number of neighbors dropped by local device.
Total Ageouts:	Displays the number of overtime neighbors in local device.

- **Neighbor Statistics**

Port:	Displays local device's port number.
Transmit Total:	Displays the number of LLDPDUs sent by this port.
Receive Total:	Displays the number of LLDPDUs received by this port.
Discards:	Displays the number of LLDPDUs discarded by this port.
Errors:	Displays the number of error LLDPDUs received by this port.
Ageouts:	Displays the number of overtime neighbors linking to this port.
TLV Discards:	Displays the number of TLVs dropped by this port.
TLV Unknowns:	Displays the number of unknown TLVs received by this port.

16.4 LLDP-MED

LLDP-MED is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power via MDI, inventory management, and device location details.

- **Elements**

LLDP-MED Device: Refers to any device which implements this Standard.

LLDP-MED Device Type: LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices.

Network Connectivity Device: Refers to an LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. Bridge is a Network Connectivity Device.

Endpoint Device: Refers to an LLDP-MED Device at the network edge, providing some aspects of IP communications service, based on IEEE 802 LAN technology. Endpoint Devices may be a member of any of the Endpoint Device Classes. Endpoint Devices are composed of three defined Classes: Class I, Class II and Class III.

Generic Endpoint Device (Class I): The most basic class of Endpoint Device.

Media Endpoint Device (Class II): The class of Endpoint Device that supports media stream capabilities.

Communication Device Endpoint (Class III): The class of Endpoint Device that directly supports end users of the IP communication system.

TLV	Description

Network Policy TLV	The Network Policy TLV allows both Network Connectivity Devices and Endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes that apply for a set of specific applications on that port.
Location Identification TLV	The Location Identification TLV provides for advertisement of location identifier information to Communication Endpoint Devices, based on configuration of the Network Connectivity Device it's connected to. You can set the Location Identification content in Location Identification Parameters. If Location Identification TLV is included and Location Identification Parameters isn't set, a default value is used in Location Identification TLV.
Extended Power-Via-MDI TLV	The Extended Power-Via-MDI TLV is intended to enable advanced power management between LLDP-MED Endpoint and Network Connectivity Devices, and it allows advertisement of fine grained power requirement details, Endpoint power priority, as well as both Endpoint and Network Connectivity Device power status.
Inventory TLV	The Inventory TLV set contains seven basic Inventory management TLVs, that is, Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV and Asset ID TLV. If support for any of the TLVs in the Inventory Management set is implemented, then support for all Inventory Management TLVs shall be implemented.

LLDP-MED is configured on the **Global Config**, **Port Config**, **Local Info** and **Neighbor Info** pages.

16.4.1 Global Config

On this page you can configure the LLDP-MED parameters of the device globally.

Choose the menu **LLDP→LLDP-MED→Global Config** to load the following page.

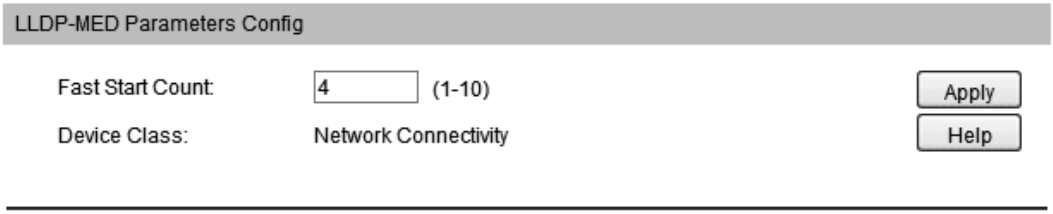


Figure 16-6 LLDP-MED Global Configuration

The following entries are displayed on this screen:

- **LLDP-MED Parameters Config**

Fast Start Count: When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted based on this parameter.

Device Class: LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices. In turn, Endpoint Devices are composed of three defined Classes: Class I, Class II and Class III. Bridge is a Network Connectivity Device.

16.4.2 Port Config

On this page you can configure all ports' LLDP-MED parameters.

Choose the menu **LLDP→LLDP-MED→Port Config** to load the following page.

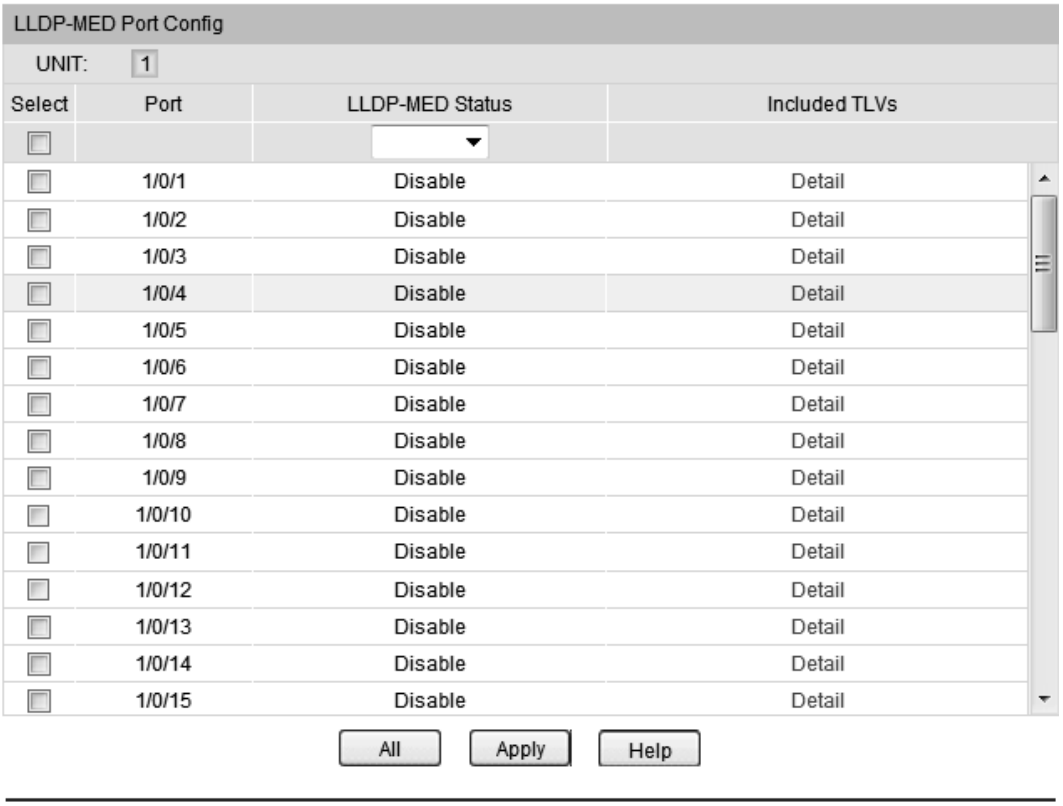


Figure 16-7 LLDP-MED Port Configuration

The following entries are displayed on this screen:

- **LLDP-MED Port Config**

Port: Displays local device's port number.

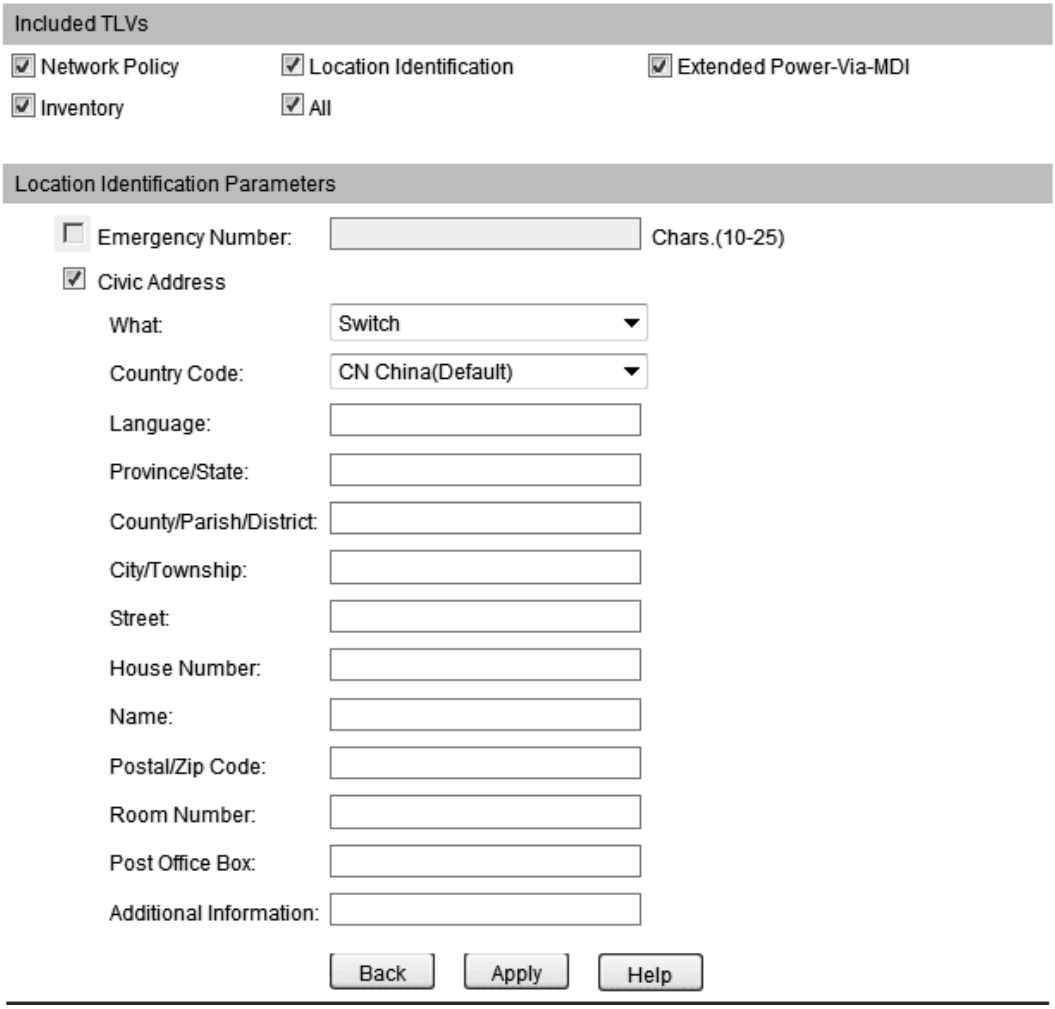
LLDP-MED Status: Configure the port's LLDP-MED status:

Enable: Enable the port's LLDP-MED status, and the port's Admin Status will be changed to Tx&Rx.

Disable: Disable the port's LLDP-MED status.

Included TLVs: Select TLVs to be included in outgoing LLDPDU.

Detail: Click the **Detail** button to display the included TLVs and select the desired TLVs.



- **Included TLVs**

  Select TLVs to be included in outgoing LLDPDU.

- **Location Identification Parameters**

  Configure the Location Identification TLV's content in outgoing LLDPDU of the port.

  Emergency Number: Emergency number is Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP.

  Civic Address: The Civic address is defined to reuse the relevant sub-fields of the DHCP option for Civic Address based Location Configuration Information as specified by IETF.

16.4.3 Local Info

On this page you can see all ports' LLDP-MED configuration.

Choose the menu **LLDP→LLDP-MED→Local Info** to load the following page.

Figure 16-8 LLDP-MED Local Information

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Enable/Disable the auto refresh function.

  Refresh Rate: Specify the auto refresh rate.

- **LLDP-MED Local Info**

  Select the local port number to display its LLDP information.

Note:

For the switches with PoE function, the local information displayed on the page also include Power Type, Power Source, Power Priority and Available Power Value.

16.4.4 Neighbor Info

On this page you can get the LLDP-MED information of the neighbors.

Choose the menu **LLDP→LLDP-MED→Neighbor Info** to load the following page.

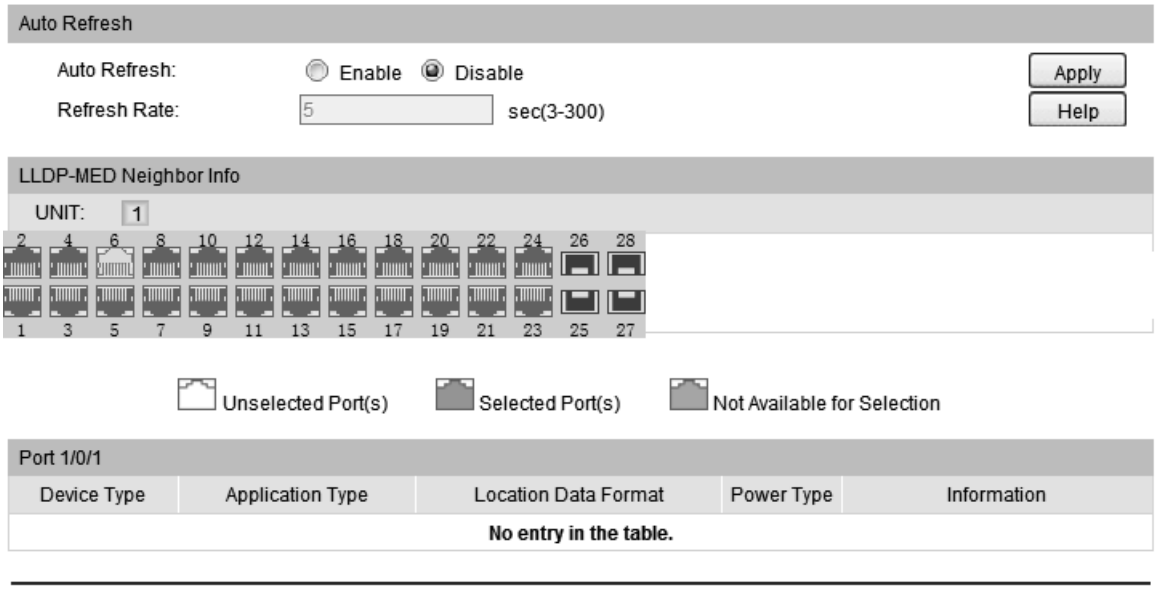


Figure 16-9 LLDP-MED Neighbor Information

The following entries are displayed on this screen:

- **Auto Refresh**

  Auto Refresh: Enable/Disable the auto refresh function.

  Refresh Rate: Specify the auto refresh rate.

- **Neighbor Info**

  Device Type: Displays the device type of the neighbor.

  Application Type: Displays the application type of the neighbor. Application Type indicates the primary function of the applications defined for the network policy.

  Local Data Format: Displays the location identification of the neighbor.

  Power Type: Displays the power type of the neighbor device, Power Sourcing Entity (PSE) or Powered Device (PD).

  Information: Click the **Information** button to display the detailed information of the corresponding neighbor.

Return to CONTENTS

Chapter 17 Maintenance

Maintenance module, assembling the commonly used system tools to manage the switch, provides the convenient method to locate and solve the network problem.

（1） System Monitor: Monitor the utilization status of the memory and the CPU of switch.

（2） sFlow: A technology for accurately monitoring network traffic at high speeds.

（3） Log: View the configuration parameters of the switch and find out the errors via the Logs.

（4） Device Diagnostics: Cable Test tests the connection status of the cable to locate and diagnoses the trouble spot of the network.

（5） Network Diagnostics: Test whether the destination device is reachable and detect the route hops from the switch to the destination device.

17.1 System Monitor

System Monitor functions to display the utilization status of the memory and the CPU of switch via the data graph. The CPU utilization rate and the memory utilization rate should fluctuate stably around a specific value. If the CPU utilization rate or the memory utilization rate increases markedly, please detect whether the network is being attacked.

The **System Monitor** function is implemented on the **CPU Monitor** and **Memory Monitor** pages.

17.1.1 CPU Monitor

Choose the menu **Maintenance→System Monitor→CPU Monitor** to load the following page.

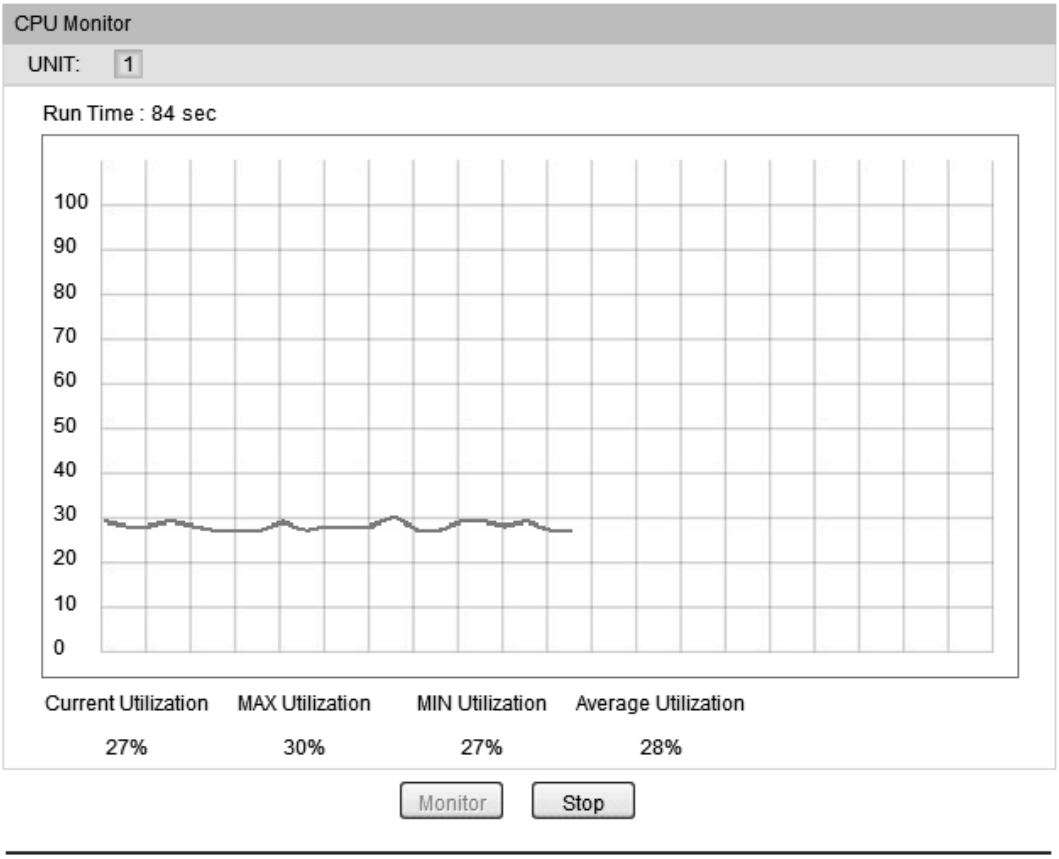


Figure 17-1 CPU Monitor

Click the **Monitor** button to enable the switch to monitor and display its CPU utilization rate every four seconds.

17.1.2 Memory Monitor

Choose the menu **Maintenance→System Monitor→Memory Monitor** to load the following page.

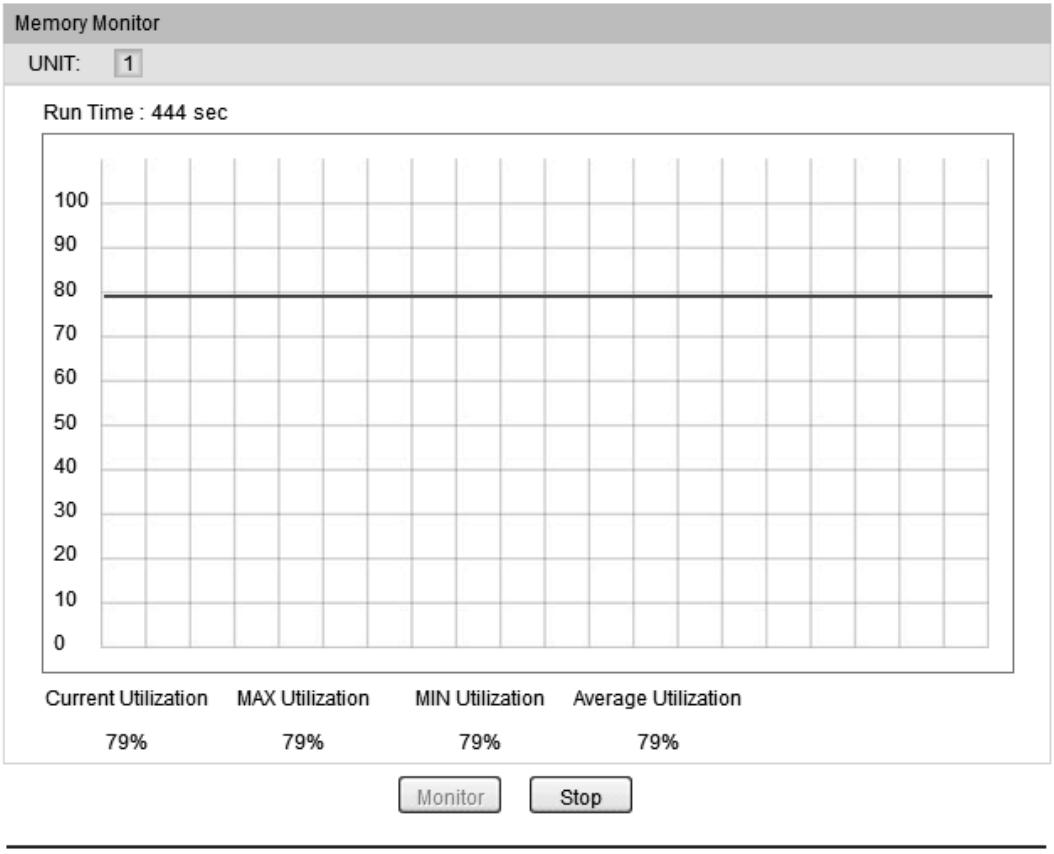


Figure 17-2 Memory Monitor

Click the **Monitor** button to enable the switch to monitor and display its Memory utilization rate every four seconds.

17.2 sFlow

sFlow (Sampled Flow) is a technology for accurately monitoring network traffic at high speeds. The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent is a virtual entity using sampling technology to capture traffic statistics from the device it is monitoring. The sFlow collector can be a host receiving sFlow datagrams from the sFlow agent.

The sFlow function is implemented as follows: the sFlow sampler takes samples of traffic statistics and sends sFlow datagrams to the sFlow agent for processing. The sFlow agent will forward sFlow datagrams to the sFlow collector for analysis. The analytic results can be displayed on the sFlow collector.

The **sFlow** function is implemented on the **sFlow Collector** and **sFlow Sampler** pages.

17.2.1 sFlow Collector

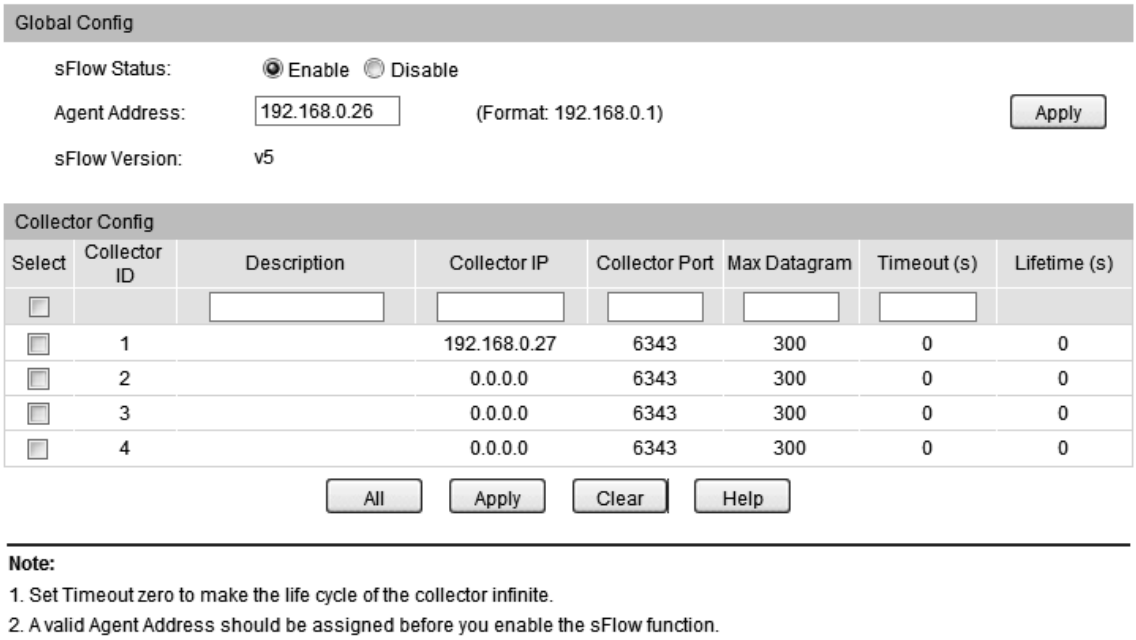


Figure 17-3 sFlow Collector

Configuration Procedure:

1) Click Enable to enable the sFlow function globally and configure the sFlow agent's IP under the Global Config. For example, you can set the switch's management IP as the sFlow agent's IP.
2) Select your desired collector and configure relevant parameters under the Collector Config.

Entry Description:

- **Global Config**

  sFlow Status: Choose to enable or disable the sFlow function globally on the switch.

  Agent Address: The IPv4 address of the sFlow agent.

  sFlow Version: Displays the sFlow version here.

- **Collector Config**

  Select: Select the desired collector. It is multi-optional.

  Collector ID: Displays the Collector ID here. The number of collectors you can configure is 4 at most.

  Description: Give a description to the collector for identification.

  Collector IP: Assign an IP address to the sFlow collector. The sFlow collector can be a host.

  Collector Port: Specify the udp port number for the sFlow collector.

Timeout (s): Specify the aging time of the sFlow collector. The collector will become invalid after this time. When the timeout is set to 0, it means the life cycle of the collector is infinite.

Lifetime (s): Specify the remaining time of the collector. Lifetime will count down from Timeout.

17.2.2 sFlow Sampler

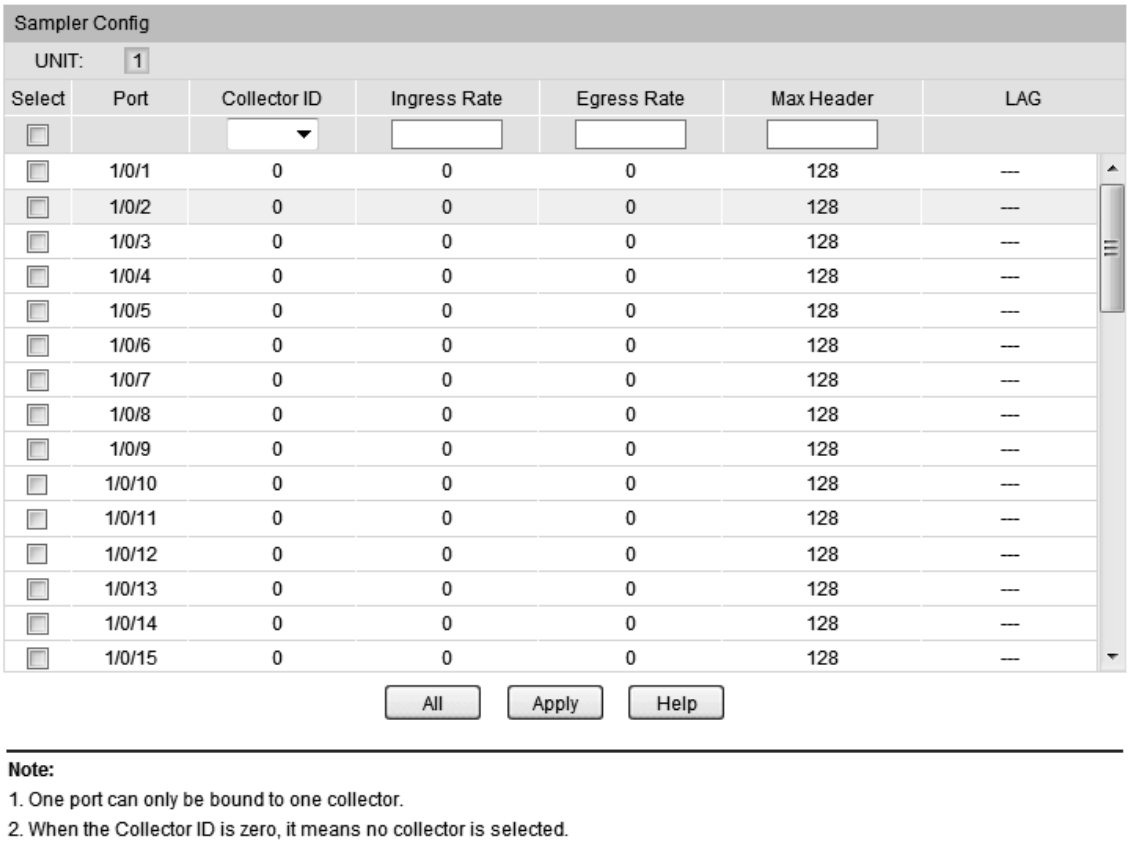


Figure 17-4 sFlow Sampler

Configuration Procedure:

Configure one or more ports to be a sampler and configure relevant parameters under the Sampler Config. One port can only be bound to one collector.

Entry Description:

Select Configure the desired port to be the sFlow sampler.

Port: Displays the port of the switch here.

Collector ID: Select the sFlow collector for the sFlow sampler. The sampler will send sFlow datagrams to corresponding collector via the sFlow agent. When the Collector ID is 0, it means no collector is selected.

Ingress Rate: Specify the ingress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before the next sample is taken.

Egress Rate: Specify the egress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before the next sample is taken.

Max Header: Specify the maximum number of bytes that should be copied from a sampled packet.

LAG: Displays the LAG number which the port belongs to.

17.2.3 Default Settings

Feature	Default Settings
Global sFlow function	Disabled.
sFlow Agent	The Agent Address is not defined.
sFlow Collector	● Collector Port is 6343. ● Max Datagram is 300 bytes. ● The other parameters are not defined.
sFlow Sampler	● Collector ID is 0.It means no collector is selected. ● Ingress Rate is 0. It means no packets will be sampled. ● Egress Rate is 0. It means no packets will be sampled. ● Max Header is 128 bytes.

17.3 Log

The Log system of switch can record, classify and manage the system information effectively, providing powerful support for network administrator to monitor network operation and diagnose malfunction.

The Logs of switch are classified into the following eight levels.

Severity	Level	Description
emergencies	0	The system is unusable.
alerts	1	Action must be taken immediately.
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warnings conditions

Severity	Level	Description
notifications	5	Normal but significant conditions
informational	6	Informational messages
debugging	7	Debug-level messages

Table 17-1 Log Level

The **Log** function is implemented on the **Log Table**, **Local Log**, **Remote Log** and **Backup Log** pages.

17.3.1 Log Table

The switch supports logs output to two directions, namely, log buffer and log file. The information in log buffer will be lost after the switch is rebooted or powered off whereas the information in log file will be kept effective even the switch is rebooted or powered off. Log Table displays the system log information in log buffer.

Choose the menu **Maintenance→Log→Log Table** to load the following page.

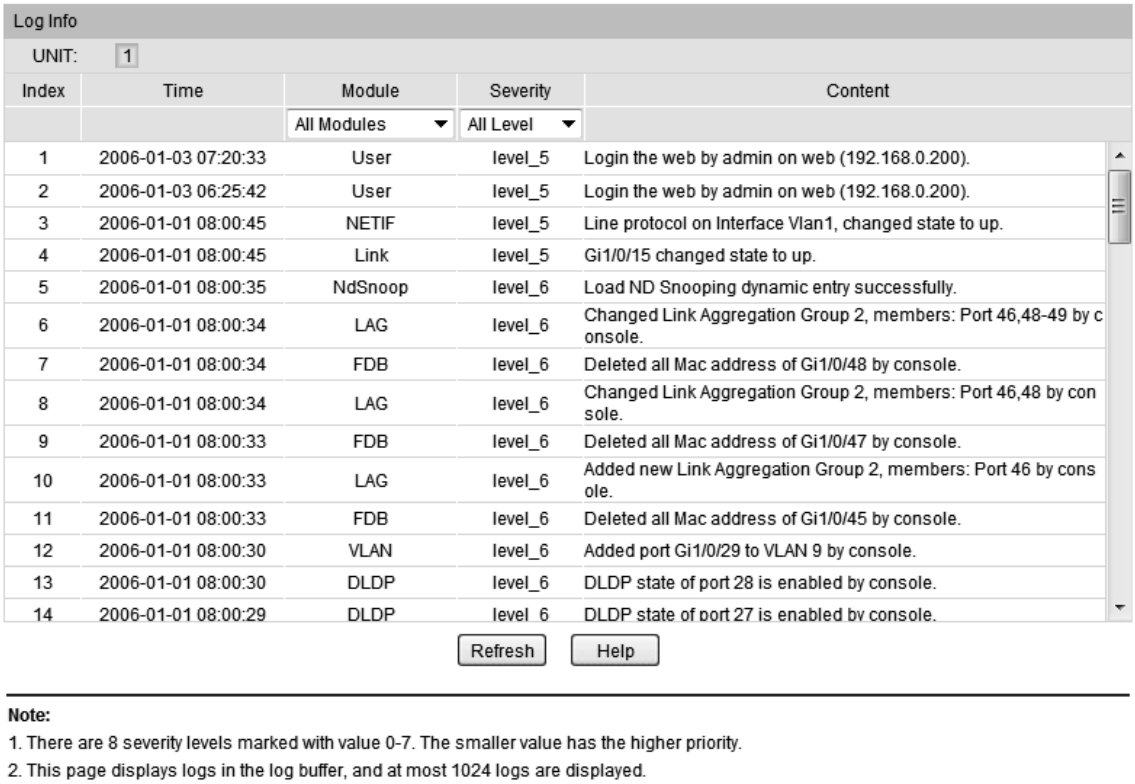


Figure 17-1 Log Table

The following entries are displayed on this screen:

- **Log Info**

Index: Displays the index of the log information.

Time: Displays the time when the log event occurs. The log can get the correct time after you configure on the System ->System Info->System Time Web management page.

Severity: Displays the severity level of the log information. You can select a severity level to display the log information whose severity level value is the same or smaller.

Content: Displays the content of the log information.

Note:

1. The logs are classified into eight levels based on severity. The higher the information severity is, the lower the corresponding level is.
2. This page displays logs in the log buffer, and at most 512 logs are displayed.

17.3.2 Local Log

Local Log is the log information saved in switch. By default, the logs with severities from level_0 to level_6 are saved in log buffer and the logs with severities from level_0 to level_3 are saved in log file meanwhile. On this page, you can set the output channel for logs.

Choose the menu **Maintenance→Log→Local Log** to load the following page.

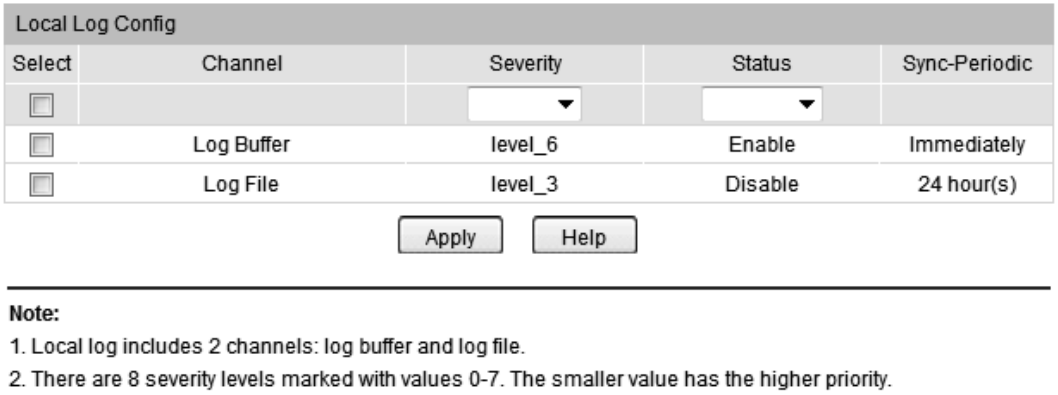


Figure 17-2 Local Log

The following entries are displayed on this screen:

➢ **Local Log Config**

Select: Select the desired entry to configure the corresponding local log.

Channel:

- **Log buffer:** Indicates the RAM for saving system log. The inforamtion in the log buffer is displayed on the Log Table page. It will be lost when the switch is restarted.
- **Log File:** Indicates the flash sector for saving system log. The information in the log file will not be lost after the switch is restarted and can be exported on the Backup Log page.

Severity: Specify the severity level of the log information output to each channel. Only the log with the same or smaller severity level value will be output.

Status: Enable/Disable the channel.

Sync-Periodic: Specify how frequent the log information would be synchronized to the log file.

17.3.3 Remote Log

Remote log feature enables the switch to send system logs to the Log Server. Log Server is to centralize the system logs from various devices for the administrator to monitor and manage the whole network.

Choose the menu **Maintenance→Log→Remote Log** to load the following page.

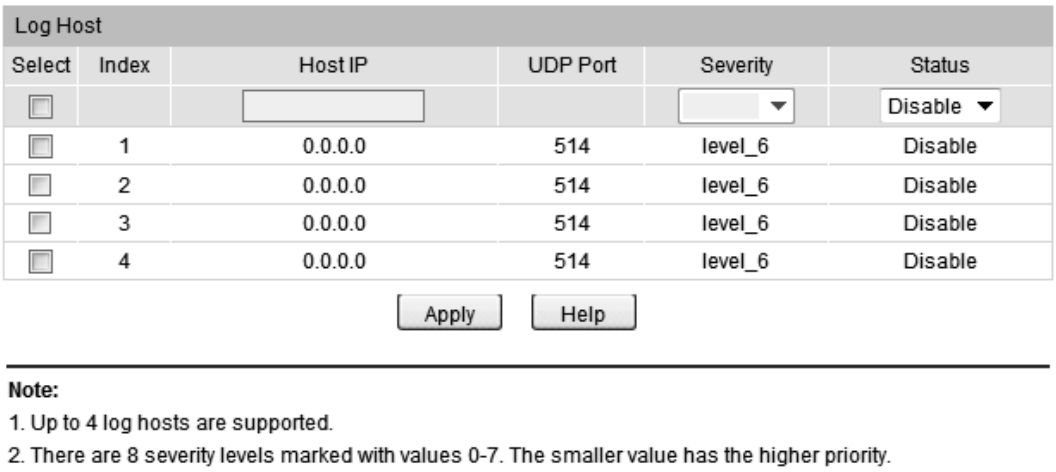


Figure 17-3 Log Host

The following entries are displayed on this screen:

- **Log Host**

Index: Displays the index of the log host. The switch supports 4 log hosts.

Host IP: Configure the IP for the log host.

UDP Port: Displays the UDP port used for receiving/sending log information. Here we use the standard port 514.

Severity: Specify the severity level of the log information sent to each log host. Only the log with the same or smaller severity level value will be sent to the corresponding log host.

Status: Enable/Disable the log host.

Note:

The Log Server software is not provided. If necessary, please download it on the Internet.

17.3.4 Backup Log

Backup Log feature enables the system logs saved in the switch to be output as a file for device diagnosis and statistics analysis. When a critical error results in the breakdown of the

system, you can export the logs to get some related important information about the error for device diagnosis after the switch is restarted.

Choose the menu **Maintenance→Log→Backup Log** to load the following page.

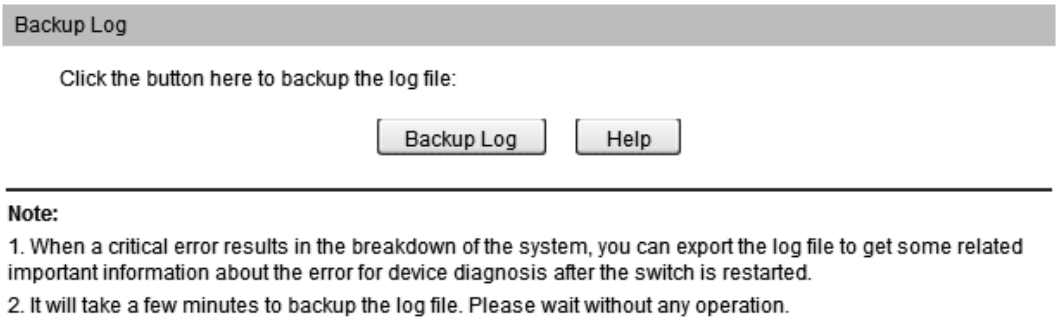


Figure 17-4 Backup Log

The following entry is displayed on this screen:

- **Backup Log**

  Backup Log: Click the **Backup Log** button to save the log as a file to your computer.

Note:

1. When a critical error results in the breakdown of the system, you can export the log file to get some related important information about the error for device diagnosis after the switch is restarted.
2. It will take a few minutes to backup the log file. Please wait without any operation.

17.4 Device Diagnostics

This switch provides Cable Test for device diagnose.

17.4.1 Cable Test

Cable Test functions to test the connection status of the cable connected to the switch, which facilitates you to locate and diagnose the trouble spot of the network.

Choose the menu **Maintenance→Device Diagnostics→Cable Test** to load the following page.

Figure 17-5 Cable Test

The following entries are displayed on this screen:

- **Cable Test**

Port:	Select the port for cable testing.
Pair:	Displays the Pair number.
Status:	Displays the connection status of the cable connected to the port. The test results of the cable include normal, close, open or impedance.
Length:	If the connection status is normal, here displays the length range of the cable.
Error:	If the connection status is close, open or impedance, here displays the error length of the cable.

Note:

1. The interval between two cable tests for one port must be more than 3 seconds.
2. The result is more reasonable when the cable pair is in the open status.
3. The result is just for your information.

17.5 Network Diagnostics

This switch provides Ping test and Tracert test functions for network Diagnostics.

17.5.1 Ping

Ping test function, testing the connectivity between the switch and one node of the network, facilitates you to test the network connectivity and reachability of the host so as to locate the network malfunctions.

Choose the menu **Maintenance→Network Diagnostics→Ping** to load the following page.

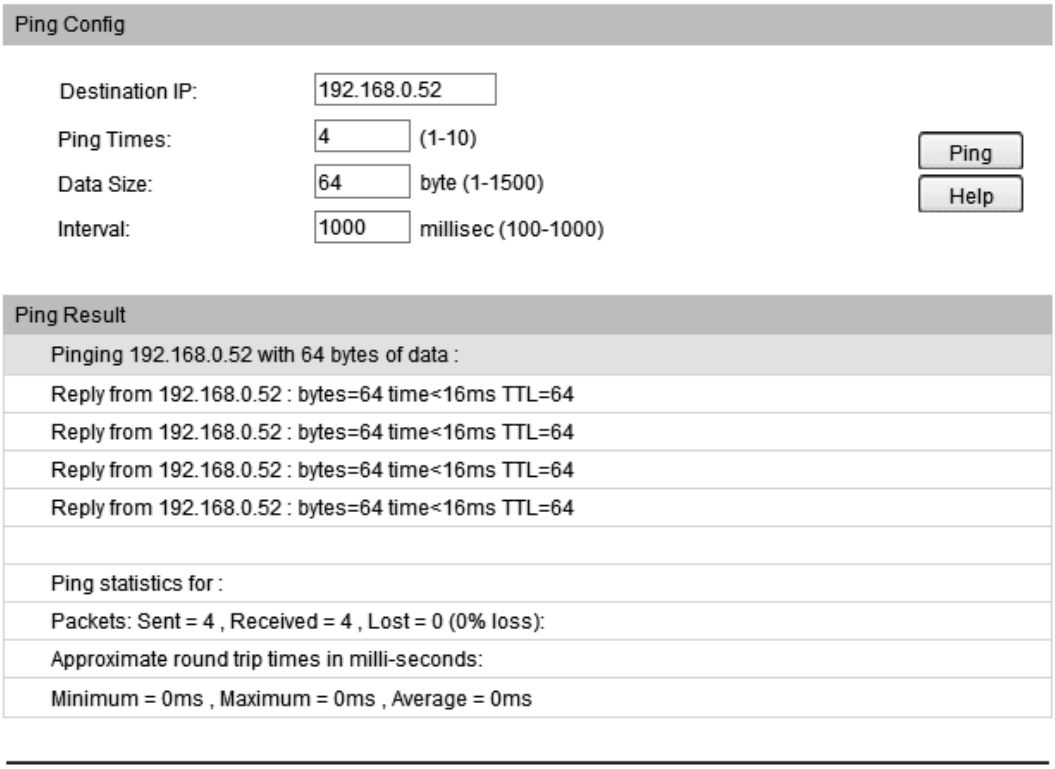


Figure 17-6 Ping

The following entries are displayed on this screen:

- **Ping Config**

Destination IP: Enter the IP address of the destination node for Ping test. Both IPv4 and IPv6 are supported.

Ping Times: Enter the amount of times to send test data during Ping testing. The default value is recommended.

Data Size: Enter the size of the sending data during Ping testing. The default value is recommended.

Interval: Specify the interval to send ICMP request packets. The default value is recommended.

17.5.2 Tracert

Tracert test function is used to test the connectivity of the gateways during its journey from the source to destination of the test data. When malfunctions occur to the network, you can locate trouble spot of the network with this tracert test.

Choose the menu **Maintenance→Network Diagnostics→Tracert** to load the following page.

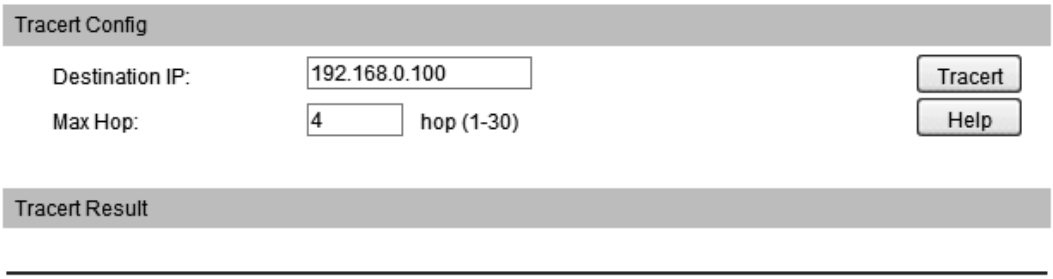


Figure 17-7 Tracert

The following entries are displayed on this screen:

- **Tracert Config**

  Destination IP: Enter the IP address of the destination device. Both IPv4 and IPv6 are supported.

  Max Hop: Specify the maximum number of the route hops the test data can pass through.

Return to CONTENTS

Appendix A. Password Recovery

This chapter introduces the procedure to reset passwords on switches.

Steps to reset the password:

1. For Security reasons, the Password Recovery feature requires the user to physically access the switch. Please attach a terminal or PC with terminal emulation program to the RJ-45/Micro-USB console port of the switch.
2. Configure the terminal or the terminal emulation program to use the following settings:
   - Baud rate: 38400 bps
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none
3. Power on the switch. After the message 'Hit any key to stop autoboot' is shown on the interface of the terminal emulation program, the switch will allows 3 seconds for the user to press any key to enter the BOOTUTIL Interface.
4. Enter 6 to select the 'Password recovery' option and enter Y to delete all the users and passwords. The default login username and password are both admin. The other configurations in the switch will not be changed.

```
Hit any key to stop autoboot:  0
                ************************************************
                *         SWITCH  BOOTUTIL(v2.0.0)         *
                ************************************************
                Copyright (c) 2017
                Create Date: Apr 26 2017 - 17:41:23

   Boot Menu
0  - Print this boot menu
1  - Reboot
2  - Reset
3  - Start
4  - Activate Backup Image
5  - Display image(s) info
6  - Password recovery

Enter your choice(0-6)

switch> 6
This will delete all the previously created accounts. Continue?[Y/N]:Y
Operation OK!
switch>
```

Appendix B. Specifications

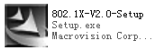
Standards	IEEE802.3i 10Base-T Ethernet
	IEEE802.3u 100Base-TX/ Fast Ethernet
	IEEE802.3ab 1000Base-T Gigabit Ethernet
	IEEE802.3z 1000Base-X Gigabit Ethernet
	IEEE802.3x Flow Control
	IEEE802.1p QoS
	IEEE802.1q VLAN
Transmission Rate	Ethernet: 10Mbps HD，20Mbps FD
	Fast Ethernet: 100Mbps HD，200Mbps FD
	Gigabit Ethernet: 2000Mbps FD
Transmission Medium	10Base-T: UTP/STP of Cat. 3 or above
	100Base-TX: UTP/STP of Cat. 5 or above
	1000Base-T: 4-pair UTP (≤100m) of Cat. 5e, Cat.6 or above
	1000Base-X: MMF or SMF SFP Module (Optional)
LED	PWR, SYS, PoE Max, FAN, Speed or PoE (Port 1-24), 1000Base-X (Port 25-28)
Transmission Method	Store and Forward
Packets Forwarding Rate	10BASE-T：14881pps/port 100BASE-TX：148810pps/port 1000Base-T：1488095pps/port 1000Base-X：1488095pps/port
Operating Environment	Operating Temperature: 0℃~ 40℃
	Storage Temperature: -40℃~ 70℃
	Operating Humidity: 10% ~ 90% RH Non-condensing
	Storage Humidity: 5% ~ 90% RH Non-condensing

Return to CONTENTS

Appendix C: 802.1X Client Software

In 802.1X mechanism, the supplicant Client should be equipped with the corresponding client software complied with 802.1X protocol standard for 802.1X authentication. When the switch works as the authenticator system, please take the following instructions to install the Supplicant for the supplicant Client.

1. Installation Guide

1) Double click the icon 

to load the following figure. Choose the proper language and click **Next** to continue.

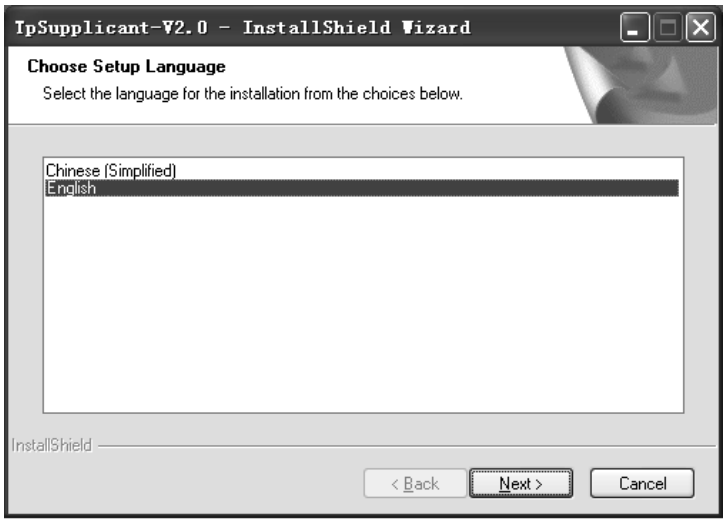


Figure C-1 Choose Setup Language

2) Please wait for the InstallShield Wizard preparing the setup shown as the following screen.

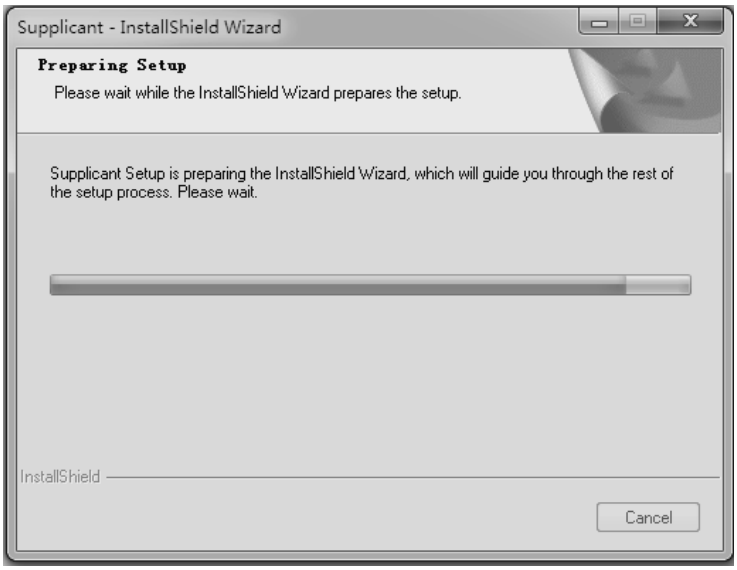


Figure C-2 Preparing Setup

3) Then the following screen will appear. Click **Next** to continue. If you want to stop the installation, click **Cancel**.

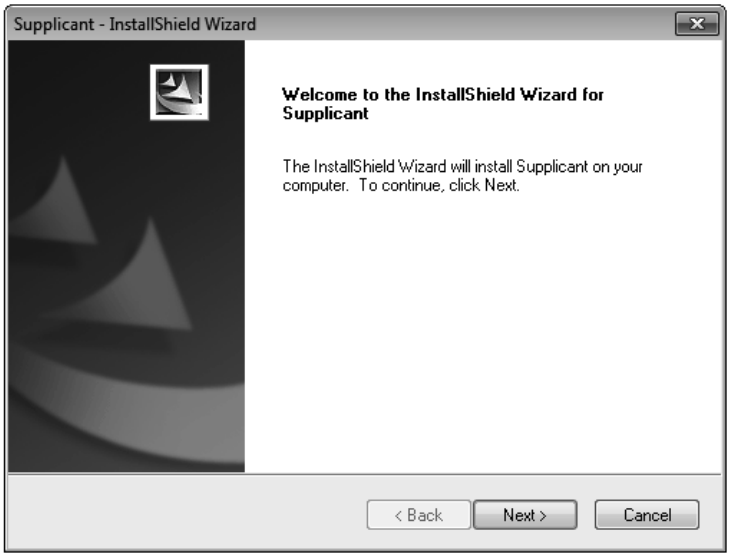


Figure C-3 Welcome to the InstallShield Wizard

4) To continue, choose the destination location for the installation files and click **Next** on the following screen.

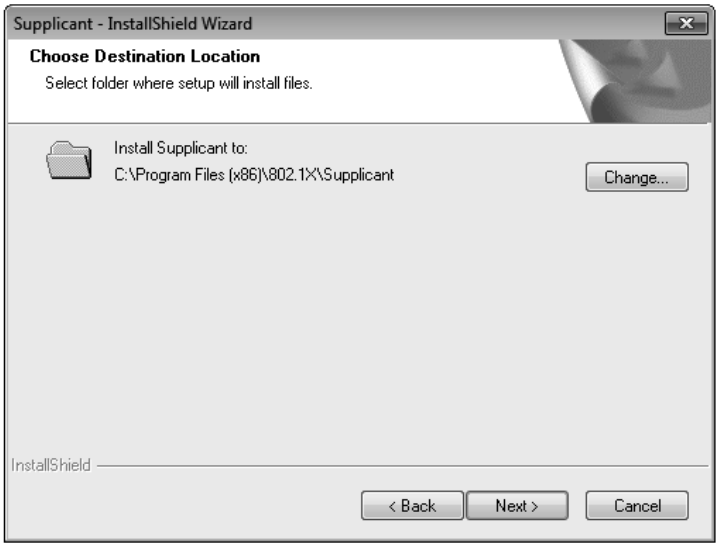


Figure C-4 Choose Destination Location

By default, the installation files are saved on the Program Files folder of system disk. Click the **Change** button to modify the destination location proper to your need.

5) Till now, The Wizard is ready to begin the installation. Click **Install** to start the installation on the following screen.

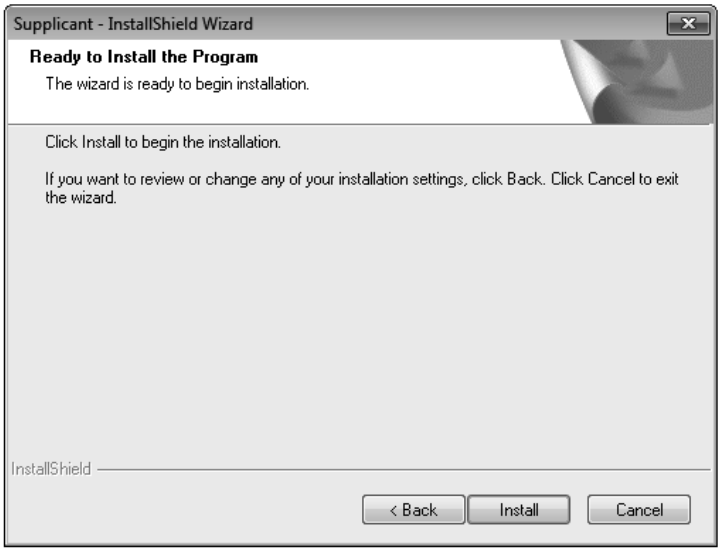


Figure C-5 Install the Program

6) The InstallShield Wizard is installing Supplicant shown as the following screen. Please wait.

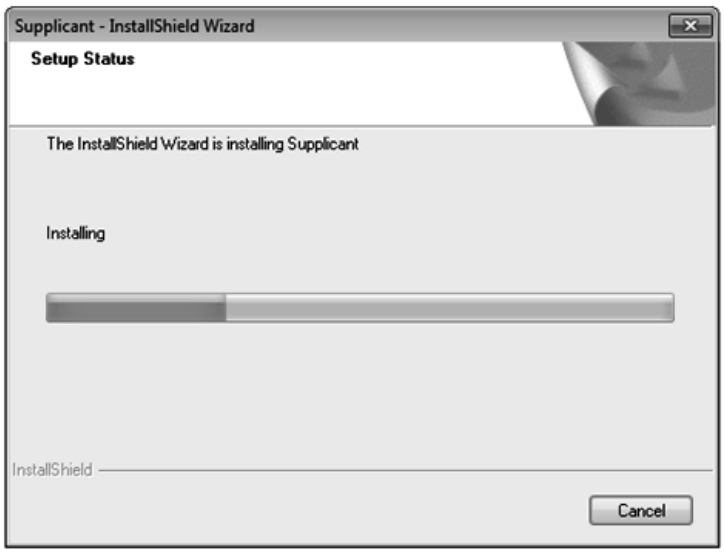


Figure C-6 Setup Status

7) On the following screen, click **Finish** to complete the installation.

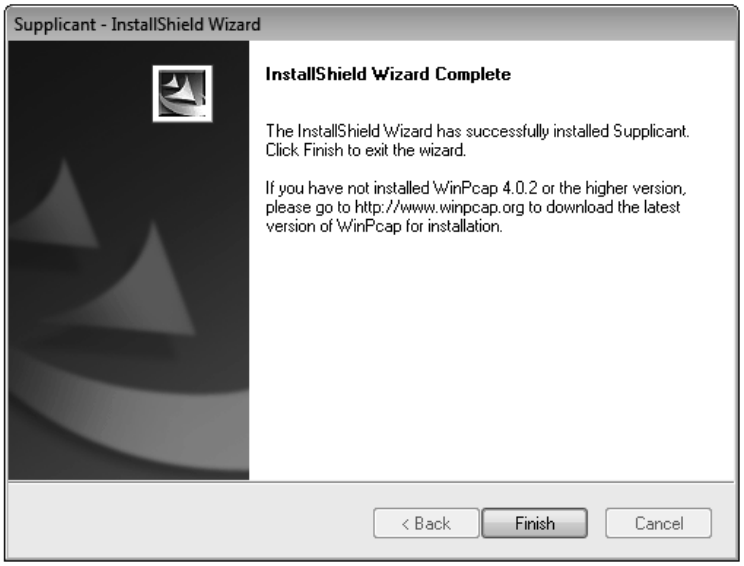


Figure C-7 InstallShield Wizard Complete

Note:

Please pay attention to the tips on the above screen. If you have not installed WinPcap 4.0.2 or the higher version on your computer, the 802.1X Client Software Supplicant can not work. It's recommended to go to http://www.winpcap.org to download the latest version of WinPcap for installation.

2. Uninstall Software

If you want to remove the 802.1X, please take the following steps:

1) On the Windows taskbar, click the **Start** button, point to **All Programs→Client →802.1X**, and then click **Uninstall 802.1X**, shown as the following figure.

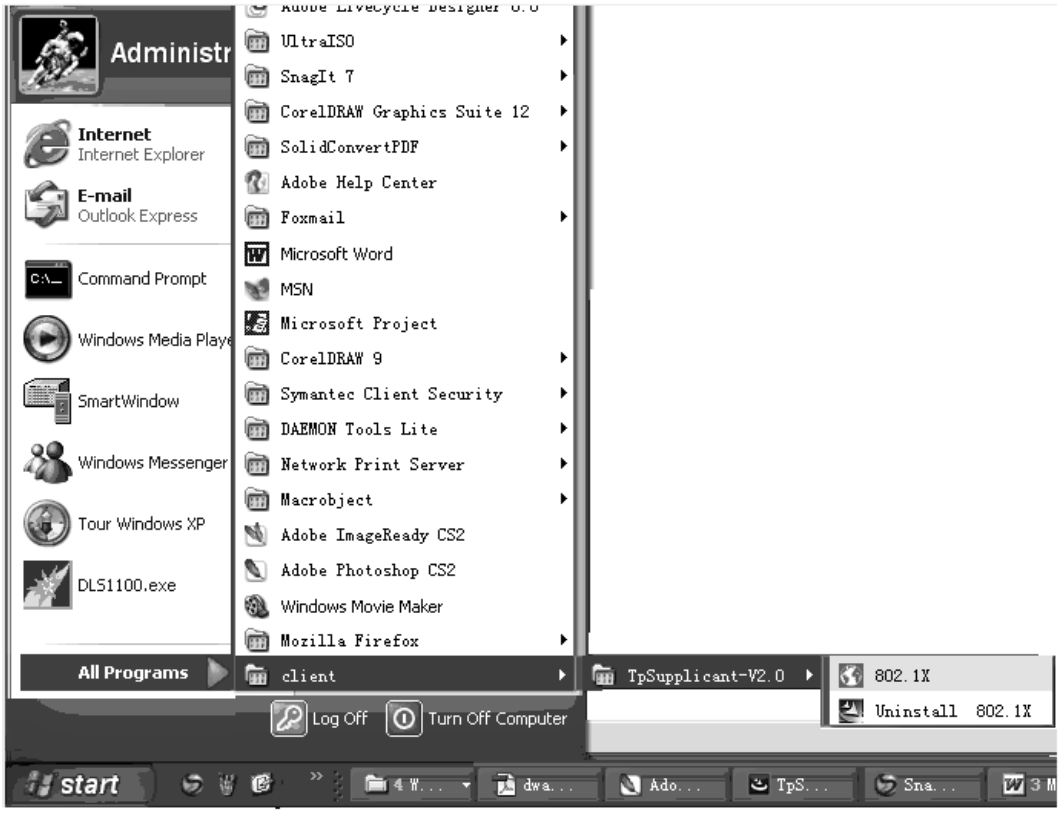


Figure C-8 Uninstall 802.1X

2) Then the following screen will appear. If you want to stop the remove process, click **Cancel**.

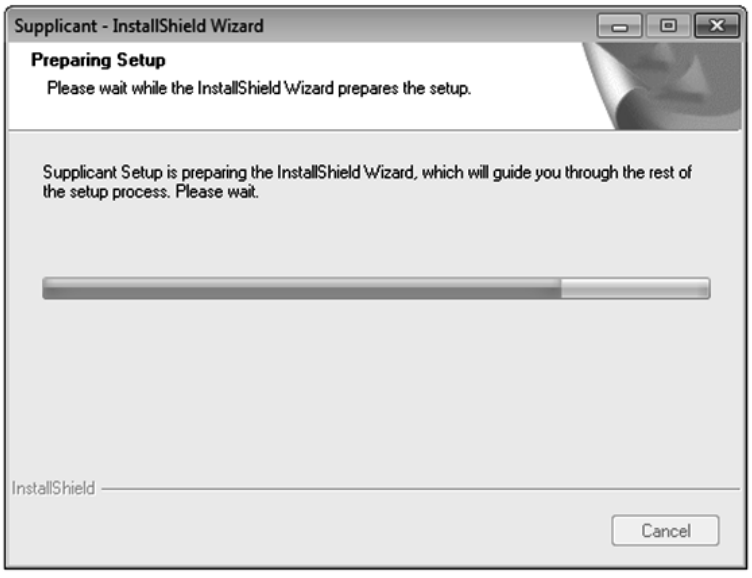


Figure C-9 Preparing Setup

3) On the continued screen, click **Yes** to remove the application from your PC.

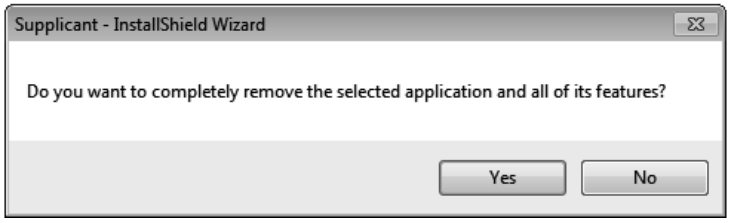


Figure C-10 Uninstall the Application

4) Click **Finish** to complete.

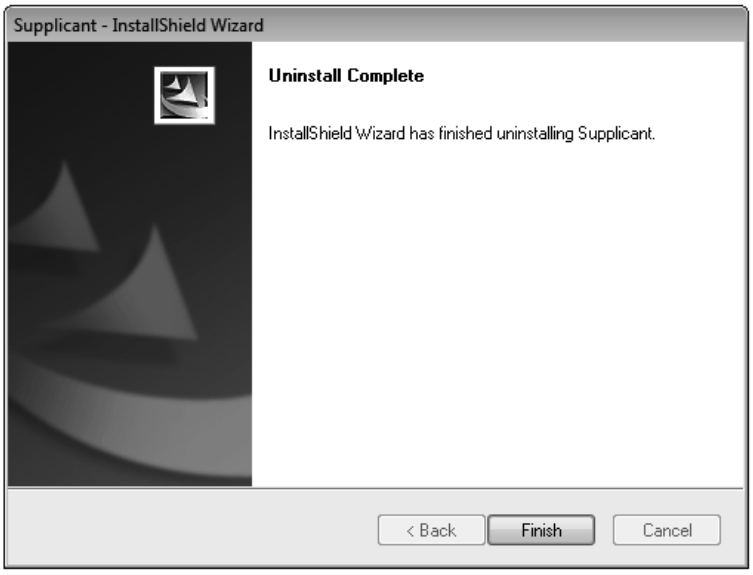
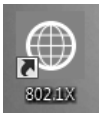


Figure C-11 Uninstall Complete

3. Configuration

1) After completing installation, double click the icon 

to run the 802.1X Client Software. The following screen will appear.

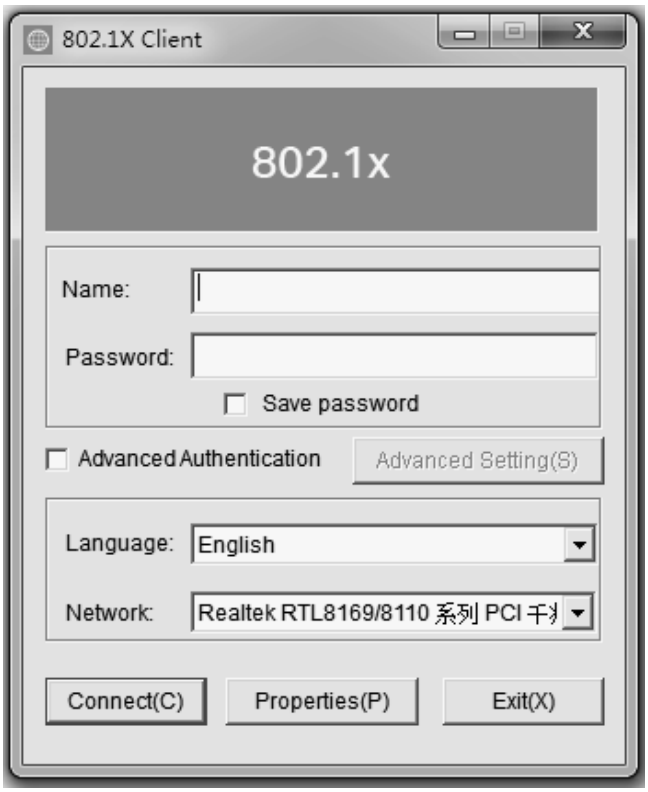


Figure C-12 802.1X Client

Enter the **Name** and the **Password** specified in the Authentication Server. The length of **Name** and **Password** should be less than 16 characters.

2) Click the **Properties** button on Figure C-12 to load the following screen for configuring the connection properties.

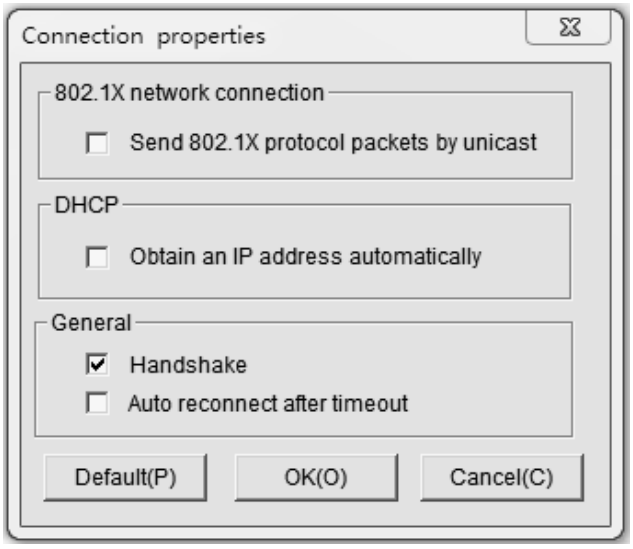


Figure C-13 Connection Properties

Send 802.1X protocol packets by Unicast: When this option is selected, the Client will send the EAPOL Start packets to the switch via multicast and send the 802.1X authentication packets via unicast.

Obtain an IP address automatically: Select this option if the Client automatically obtains the IP address from DHCP server. After passing the authentication, the Client can be assigned the IP address by DHCP server. The Client can access the network after getting the new IP address.

Auto reconnect after timeout: Select this option to allow the Client to automatically start the connection again when it does not receive the handshake reply packets from the switch within a period.

3) To continue, click **Connect** button after entering the **Name** and **Password** on Figure C-12. Then the following screen will appear to prompt that the Radius server is being searched.

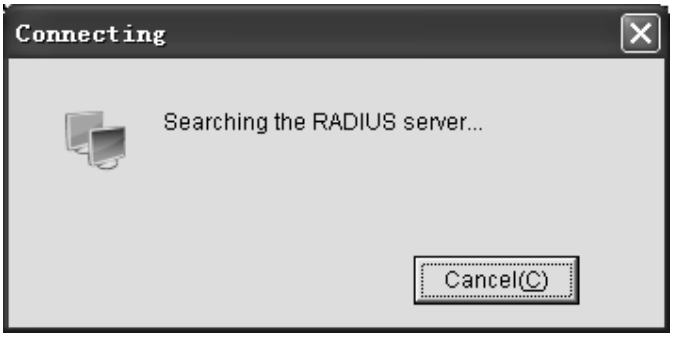


Figure C-14 Authentication Dialog

4) When passing the authentication, the following screen will appear.

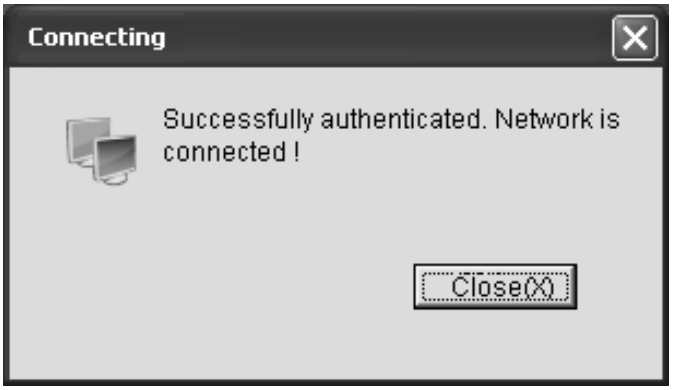


Figure C-15 Successfully Authenticated

5) Double click the icon on the right corner of desktop, and then the following connection status screen will pop up.

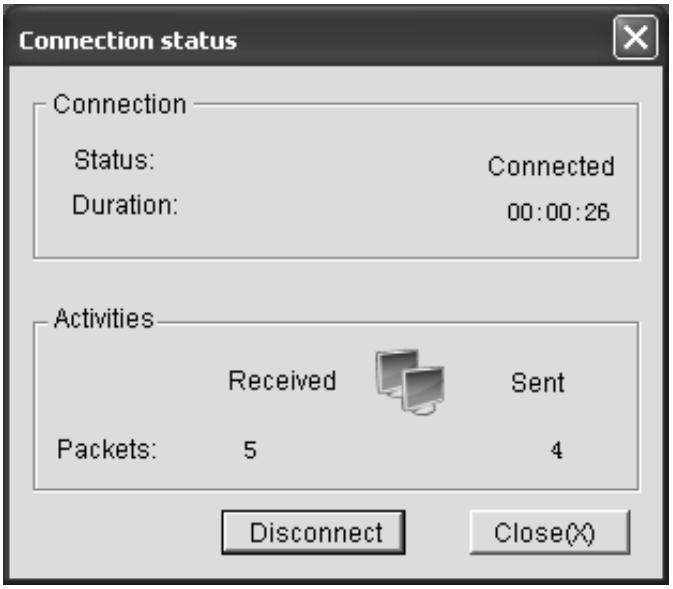
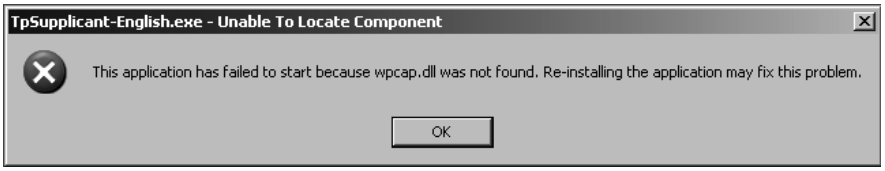


Figure C-16 Connection Status

4. FAQ:

Q1: Why does this error dialog box pop up when starting up the 802.1X Client Software?



A1: It's because the supported DLL file is missing. You are suggested to go to http://www.winpcap.org to download WinPcap 4.0.2 or the higher version for installation, and run the client software again.

Q2: Is this 802.1X Client Software compliable with the switches of the other manufacturers?

A2: No. This 802.1X Client Software is customized for SUNDRAY switches.

Q3: Is it safe to set the password being automatically saved?

A3: Yes. The password saved in the configuration files is encrypted.

Return to CONTENTS

目录

第1章 用户手册简介

本手册旨在帮助您正确使用这款交换机。手册中包括对交换机性能特征的描述以及配置交换机的详细说明。请在操作交换机前，详细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指 SW-5024 24-Port Gigabit Managed PoE Switch with 4 SFP Slots，下面简称为 SW-5024。
- 用 **>>** 符号表示配置页面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**。
- 正文中出现的<>尖括号标记的文字，表示 Web 页面的按钮名称，如<确定>。
- 正文中出现的**加粗**标记的文字，表示交换机的各个功能的名称，如**端口配置**页面。
- 正文中出现的“”双引号标记的文字，表示配置页面上出现的名词，如“IP 地址”。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.3 章节安排

章节	章节说明
第 1 章 用户手册简介	快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。
第 2 章 产品介绍	介绍本产品的特性、应用以及外观。
第 3 章 配置指南	介绍如何登录交换机的 Web 页面，并简要介绍页面特点。

章节	章节说明
第 4 章 系统管理	本模块主要用于配置交换机的系统属性，主要介绍了： ● 系统配置：配置交换机的描述、时间和网络参数。 ● 用户管理：配置登录交换机 Web 页面的用户的访问权限和身份。 ● 系统工具：集中对交换机的配置文件进行管理。 ● 安全管理：安全管理：针对不同的登录方式，增强用户管理交换机的安全性。包括安全配置、SSL 配置和 SSH 配置。
第 5 章 二层交换	本模块主要用于配置交换机的基本功能，主要介绍了： ● 端口管理：配置交换机端口的基本属性包括端口配置、端口监控、端口安全和端口隔离。 ● 汇聚管理：配置端口汇聚组。汇聚是将交换机的多个物理端口聚合在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。 ● 流量统计：统计流经各个端口的数据信息。 ● 地址表管理：配置交换机的地址表。地址表是交换机实现报文快速转发的基础。
第 6 章 VLAN	VLAN 主要用于隔离广播域，通过划分虚拟工作中来简化网络管理，主要介绍了： ● 802.1Q VLAN：划分基于端口的 VLAN，也是 MAC VLAN 和协议 VLAN 的基础。 ● MAC VLAN：在不改变原 802.1Q VLAN 配置的情况下划分 MAC VLAN。 ● 协议 VLAN：从应用层划分 VLAN，使某些特殊网络数据只能在指定 VLAN 中传输。 ● GVRP：通过在端口动态注册和注销 VLAN 信息来达到配置 VLAN 的目的，并传播 VLAN 信息到其它交换机中，简化配置 VLAN 时的操作。
第 7 章 生成树	生成树主要用于在局域网中消除环路。本模块主要用于配置交换机的生成树功能，主要介绍了： ● 基本配置：配置和查看交换机生成树功能的全局属性。 ● 端口配置：配置端口的 CIST 参数。 ● MSTP 实例：配置 MSTP 实例。 ● 安全配置：配置保护功能，以防止生成树网络中的设备遭受恶意攻击。
第 8 章 以太网 OAM	以太网 OAM(操作、管理和维护)是一个二层协议，用于以太网的监控和故障诊断。通过两个 OAM 实体之间交换 OAMPDUs，它可以将网络状态报告给网络管理员，以促进网络管理。
第 9 章 组播管理	本模块主要用于配置交换机的组播管理功能，主要介绍了： ● IGMP 侦听：配置 IGMP 侦听的全局参数、端口属性、VLAN 参数和组播 VLAN。IGMP 侦听可以有效抑制组播数据在网络中扩散。 ● 组播地址表：配置组播地址表。交换机在转发组播数据时是根据组播地址表来进行的。 ● 组播过滤：配置组播过滤功能，可以限制用户对组播节目的点播。 报文统计：查看各端口的组播报文流量，监控网络中 IGMP 报文。

章节	章节说明
第 10 章 路由	路由是主机或网关决定发送数据的方法。路由是查找从发送者到想要的目的地的路径的任务。如果该目的地位于直接连接到主机或网关的网络上，则可以直接将数据发送到目的地。
第 11 章 服务质量	本模块主要为网络中某些特殊应用程序提供保障，主要介绍了： ● QoS 配置：给网络中的数据流划分优先级，保障重要数据的传输，可分为端口优先级、802.1P 优先级和 DSCP 优先级。 ● 流量管理：可通过带宽控制来限制端口的数据流量；风暴抑制可限制局域网中各类广播包的传输带宽，节约网络资源。 ● 语音 VLAN：在指定 VLAN 中传输语音数据，提高语音数据的传输优先级，保证通话质量。
第 12 章 PoE	本模块主要用于配置交换机的 PoE 功能，通过交换机给 PD 设备供电，主要介绍了： ● PoE 配置：配置 PoE 功能的全局属性。 ● PoE 时间段：通过时间段控制 PoE 端口的供电时间。
第 13 章 访问控制	本模块通过配置对报文的匹配规则和处理操作来实现对数据包的过滤功能，有效防止非法用户对网络的访问，节约网络资源，主要介绍了： ● 时间段配置：通过时间段控制 ACL 条目的生效时间。 ● ACL 配置：配置 ACL 条目。 ● Policy 配置：配置 ACL 规则的处理方式。 ● 绑定配置：将 Policy 下发到端口和 VLAN，使之正式生效。
第 14 章 网络安全	本模块针对局域网中常见的网络攻击进行防护，主要介绍了： ● 四元绑定：是将计算机的 MAC 地址和 IP 地址，所属 VLAN 以及连接交换机的端口号四者绑定。 ● ARP 防护：对局域网中的 ARP 攻击进行防护。 ● DoS 防护：对常见的 DoS 攻击进行防护。 ● 802.1X 认证：配置交换机对局域网接入用户进行接入认证。
第 15 章 SNMP	SNMP 提供了一个管理框架来监控和维护互联网设备。本模块主要用于配置交换机的 SNMP 功能，主要介绍了： ● SNMP 配置：配置 SNMP 的基本属性。 ● 通知管理：配置 SNMP 通知管理，便于管理软件对交换机某些事件进行及时监控和处理。 ● RMON：配置 RMON 功能，便于网管更有效的监控网络。

章节	章节说明
第 16 章 LLDP	LLDP 功能主要用于不同的网络设备间相互学习对方的设备信息。SNMP 应用可以利用 LLDP 获取的信息，进行网络故障排除。本模块主要用于配置交换机的 LLDP 功能，主要介绍了： ● 基本配置：配置交换机 LLDP 功能的全局属性和端口属性。 ● 设备信息：查看本地信息和邻居设备信息。 ● 设备统计：查看 LLDP 全局统计信息和端口报文统计信息。 ● LLDP-MED：配置 LLDP-MED 全局参数和端口参数，查看 LLDP-MED 本地信息和邻居信息。
第 17 章 系统维护	系统维护模块将管理交换机的常用系统工具组合在一起，主要介绍了： ● 运行状态：对交换机内存和 CPU 进行监控。 ● 系统日志：查看在交换机上配置的参数。 ● 系统诊断：检测与交换机连接的线缆及对端设备的可用性。 ● 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。
第 18 章 软件系统维护	主要介绍了：当交换机出现软件故障时，如何进入交换机的 boot 菜单重新加载软件。
附录 A 802.1X 客户端软件使用说明	主要介绍了如何使用我司提供的 802.1X 客户端软件，并利用该软件进行认证。
附录 B 技术参数规格	技术参数规格表。

回目录

第2章 产品介绍

2.1 产品简介

SW-5024 交换机是为构建高安全、高性能网络需求而专门设计的新一代智能以太网交换机，具有完备的安全策略、完善的 QoS 策略、丰富的 VLAN 特性、易管理维护等特点。系统采用全新的软硬件平台，在安全接入策略、多业务支持、易管理和维护等方面为用户提供了全新的技术特性和解决方案，是理想的办公网、校园网的汇聚、接入层交换机以及中小企业、分支机构的核心交换机。

2.2 产品特性

完备的网络接入安全策略

- 一键快速绑定

支持 PORT/MAC/IP/VLAN ID 四元绑定，提供手动添加、自动扫描、DHCP 侦听三种绑定方式，支持跨 VLAN 扫描，根据不同网络环境，轻松实现快速绑定。

- ARP 攻击防护

内置特有的 ARP 入侵检测功能，对不匹配四元绑定表的非法 ARP 欺骗报文直接丢弃，有效杜绝内网 ARP 攻击；支持对非法 ARP 报文统计，帮助用户迅速定位 ARP 攻击源；同时还支持防合法 ARP 报文的泛滥攻击。

- DoS 攻击防护

内置深层次攻击检测功能，通过解析 IP 数据包，查看数据包中的特定字段是否符合 DoS 攻击数据包的特征，并采取相应的防护措施，直接丢弃非法数据包或者对合法的数据包进行限速，并且还能主动探测追踪 DoS 攻击的源头。

- 防 MAC 地址攻击

支持端口安全特性，可以有效防御 MAC 地址攻击。可以实现基于 MAC 地址允许或限制流量，每个端口允许设定最大 MAC 地址数量，支持静态配置或交换机动态学习，全面保障网络安全。

多层次，多元化的访问控制策略

- 访问控制（ACL）

强大硬件 ACL 能力，深度识别报文，支持 L2~L4 数据流分类，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、IP 协议类型、TCP/UDP 端口等定义 ACL。

- 策略控制（Policy）

支持基于端口、VLAN 下发 ACL，对符合相应 ACL 规则的数据包实现流分类，可进行流镜像、流监控、QoS 重标记和端口重定向四种行为控制，轻松实现网络监控，数据流量控制，优先级重标记和数据转发控制。

- 时间段控制

新增基于时间段的 ACL 控制，提供节假日、绝对时间、周期以及时间片段设置功能，多种时间段的灵活组合可轻松实现对时间精确控制的访问需求。

- 802.1X 认证

支持基于端口和基于 MAC 的 802.1X 认证，在用户接入网络时完成必要的身份认证，保证接入用户的合法性，支持 Guest VLAN，轻松设置来宾用户接入访问权限。

丰富的 VLAN 特性

- IEEE 802.1Q VLAN

IEEE 802.1Q VLAN 符合国际标准，完美融合了 Port VLAN，与主流设备完全兼容，加上人性化的操作方式，使组网更加便捷、准确、高效。

- MAC VLAN

通过 MAC 地址划分 VLAN，使用户可以灵活更改接入位置而不必重新划分 VLAN，在极大提高组网的灵活性的同时，简化了网络拓扑结构和配置管理。

- 协议 VLAN

通过协议来划分 VLAN，对特殊应用可设置自定义协议，实现安全通信。

- GVRP

基于 GARP 的工作机制，用来维护设备中的 VLAN 动态注册信息，使得局域网内的 VLAN 配置更快捷、方便。

完善多业务融合能力

- QoS

支持基于端口、IEEE802.1p 以及 DSCP 三种优先级模式，支持 Equ、SP（Strict Priority）、WRR（Weighted Round Robin）、SP+WRR 四种队列调度算法，每个端口 8 个输出队列，可以将不同优先级的报文映射到不同输出队列，保障关键业务数据优先处理，满足不同业务对基础网络的需求。

- 流量控制

带宽控制支持端口双向限速，限速的控制粒度为 64Kbps；风暴抑制支持对广播包、组播包、UL 包限速，避免网络资源被恶意浪费，提高网络效率。

- 语音 VLAN

内置语音设备 OUI 地址识别功能，通过 Voice VLAN 技术，对语音流进行有针对性的 QoS 配置，能够很好的解决语音设备数据流优先级的调整问题，保证通话质量。

- 组播管理

支持 IGMP V1/V2/V3，通过 IGMP Snooping 技术，能很好的支持组播应用，如 IPTV、视频会议等等；支持组播 VLAN，有效避免带宽浪费，减轻上游设备的组播负担；静态组播地址表减少学习时间，提高组播转发效率；未知组播报文丢弃功能，节省带宽，提高系统处理效率。

高可靠性设计

- 生成树

支持传统的 STP/RSTP/MSTP 二层链路保护技术，极大提高链路的容错、冗余备份能力，保证网络的稳定运行。支持 TC（Topology Change）报文保护，避免当设备受到恶意的 TC 报文攻击时，频繁的删除操作给设备带来很大负担。同时还支持环路保护、根桥保护、BPDU 保护、BPDU 过滤等功能。

- 链路汇聚

提供手工汇聚、动态 LACP 两种汇聚模式，能有效增加链路带宽，提高链路的可靠性，同时可以实现负载均衡、链路备份。

灵活、安全的网络管理

- 系统管理

支持 CLI 命令行（Console，Telnet，SSHV1/V2 ），Web 网管（HTTP、SSL V2/V3/TLSV1），SNMP（V1/V2c/V3）等多种管理方式。

- 安全管理

通过身份过滤检测技术，能够很好的解决设备安全管理难题，支持两级用户管理，提供管理人员数限制功能，增强配置安全性。

- 网络监控

支持端口双向数据监控，结合网络分析软件可以实时监控网络运行状态，RMON 功能可以实现统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

- 系统维护

支持 CPU、内存实时监控，支持 VCT 电缆检查以及端口环回测试，方便定位网络故障点，同时支持 Ping、Tracert 命令操作，轻松分析出现故障的网络节点。

- 系统日志

提供免费的日志服务器软件，为用户提供对设备系统日志的数据库统计分析功能，有效监控设备运行和网络状况。

- 集群管理

支持 NDP（邻居发现）、NTDP（邻居拓扑发现）和 Web 集群管理（仅支持被管理），轻松打造“零费用、免软件”的统一管理方式，支持信息产业部相关标准，兼容其它主流厂商的集群管理。

2.3 产品外观

2.3.1 前面板

交换机的前面板由 24 个 10/100/1000Mbps RJ45 端口、4 个 SFP 口、2 个 Console 口和指示灯组成。如下图所示。

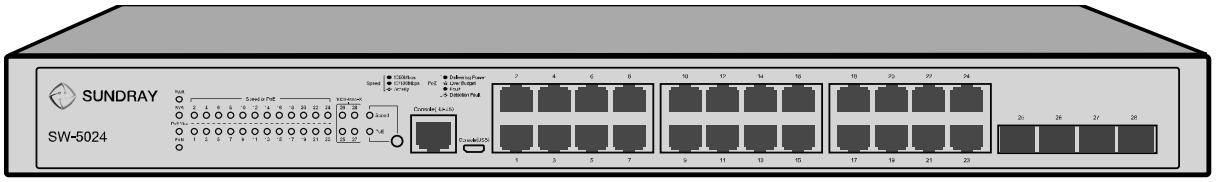


图 2-1 前面板

- **24 个 1000Mbps 自适应 RJ45 端口**

SW-5024 有 24 个 10/100/1000Mbps RJ45 端口，分别对应一个 10/100/1000Mbps 指示灯。

- **4 个 SFP 端口**

SFP 模块卡扩展槽位于千兆 RJ45 端口的右边，标识为 25-28 口。

- **2 个 Console 端口**

交换机控制端口，用于连接计算机或其他终端的串口以监控和配置交换机。其中，当您使用 Windows 电脑通过 USB 线来管理交换机时，USB 驱动需要手动安装。在配件 CD 中有 USB Console Driver.exe 的驱动文件。

- **指示灯**

交换机有 PWR、SYS、PoE Max、FAN、Speed or PoE(1-24 口)、1000Base-X（25-28 口）指示灯，可以通过指示灯监控交换机的工作状态。

SW-5024 有一个指示灯模式转换开关，可以改变指示灯的指示状态。当 Speed 指示灯点亮时，端口指示灯指示的是数据传输速率。当 PoE 指示灯点亮时，端口指示灯指示的是端口的供电状态。缺省情况下 Speed 指示灯亮。按下指示灯模式转换开关，可以切换指示灯的指示状态。

当 Speed 指示灯点亮时，端口指示灯指示的是数据传输速率，如下表所示。

指示灯	工作状态		工作说明
PWR	常亮		系统供电正常
	熄灭		系统未通电或供电异常
	闪烁		系统供电异常
SYS	闪烁		系统正常工作
	常亮/熄灭		系统异常
FAN	绿色		所有风扇正常运作
	黄色		不是所有风扇都正常运作
	熄灭		交换机异常
Speed or PoE (端口 1–24)	绿色	常亮	一个 1000Mbps 的设备被连接到对应的端口，但处于闲置状态
		闪烁	一个 1000Mbps 的设备被连接到对应的端口，并且有数据正在被传递或接收
	黄色	常亮	一个 10/100Mbps 的设备被连接到对应的端口，但处于闲置状态
		闪烁	一个 10/100Mbps 的设备被连接到对应的端口，并且有数据正在被传递或接收
	熄灭		没有连接设备
1000Base-X	常亮		对应端口连接了设备

指示灯	工作状态	工作说明
(端口 25–28)	闪烁	对应的 SFP 口正在传输或接收数据
	熄灭	对应的 SFP 口没有连接设备

当 PoE 指示灯点亮时，端口指示灯指示的是端口的供电状态，如下表所示。

指示灯	工作状态		工作说明
PWR	常亮		系统供电正常
	熄灭		系统未通电或供电异常
	闪烁		系统供电异常
SYS	闪烁		系统正常工作
	常亮/熄灭		系统异常
PoE Max	常亮		剩余功率小于等于7W
	闪烁		剩余功率持续小于7W超过两分钟
	熄灭		剩余功率大于等于7W
FAN	绿色		所有风扇正常运作
	黄色		不是所有风扇都正常运作
	熄灭		交换机异常
Speed or PoE (端口 1–24)	绿色	常亮	端口正在供电
		闪烁	供电功率超过相应端口的功率上限
	黄色	常亮	过载或短路状态
		闪烁	上电自检失败
	熄灭		未进行PoE供电
1000Base-X	常亮		对应端口连接了设备

指示灯	工作状态	工作说明
(端口 25–28)	闪烁	对应的 SFP 口正在传输或接收数据
	熄灭	对应的 SFP 口没有连接设备

2.3.2 后面板

交换机后面板由电源接口、防盗锁孔和防雷接地柱组成，如下图所示：

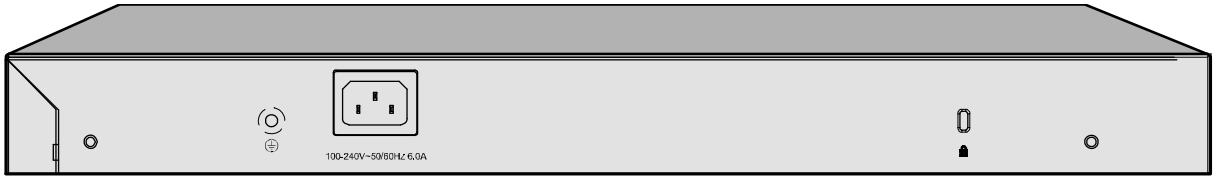


图 2-2 后面板

- **电源接口**

位于后面板左侧。SW-5024 接入电源需为 100-240V~ 50/60Hz 6.0A 的交流电源。

- **防雷接地柱**

位于电源接口左侧，请使用导线接地，以防雷击。

- **防盗锁孔**

将锁（未提供）插入锁孔内防止交换机被盗。

注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

回目录

第3章 配置指南

3.1 登录 Web 页面

第一次登录时，请确认以下几点：

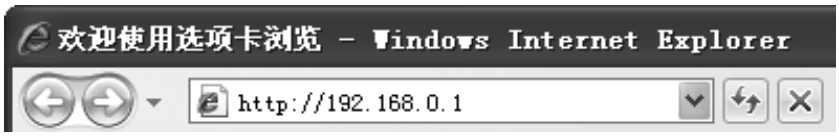
1) 交换机已正常加电启动，任一端口已与管理主机相连。

2) 管理主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装 IE 6.0 或以上版本的浏览器。

3) 管理主机 IP 地址已设为与交换机端口同一网段，即 192.168.0.X（X 为 2 至 254 之间的任意整数），子网掩码为 255.255.255.0。

4) 为保证更好地体验 Web 页面显示效果，请将显示器的分辨率调整到 1024×768 或以上像素。

打开浏览器，在地址栏输入 http://192.168.0.1 登录交换机的 Web 页面。



交换机登录页面如图 3-1 所示。

图 3-1 登录页面

在此页面输入交换机管理帐号的用户名和密码，出厂默认值均为 admin。成功登录后可以看到当前端口连接状态和交换机的系统信息，如图 3-2 所示。

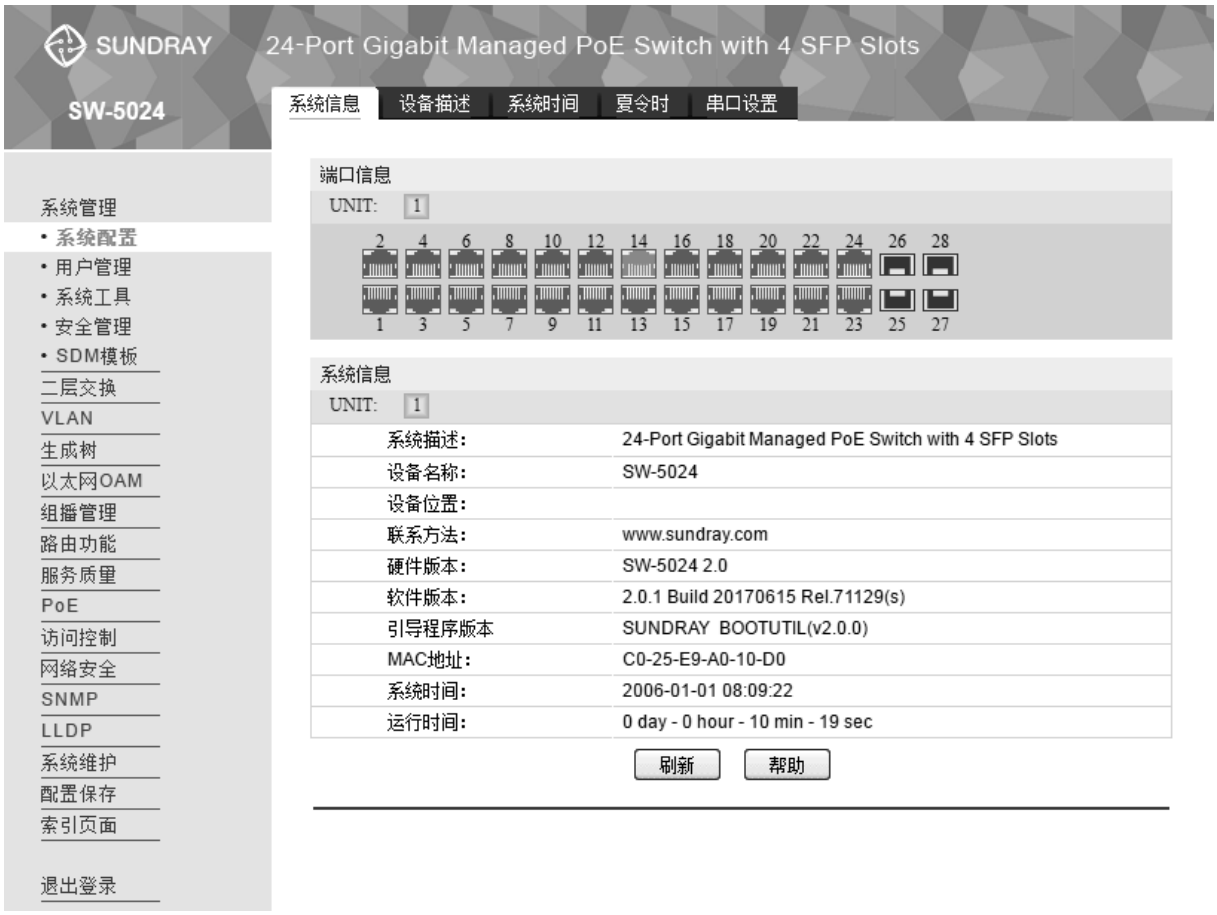


图 3-2 系统信息

3.2 Web 页面简介

3.2.1 页面总览

交换机典型的 Web 页面如图 3-3 所示。

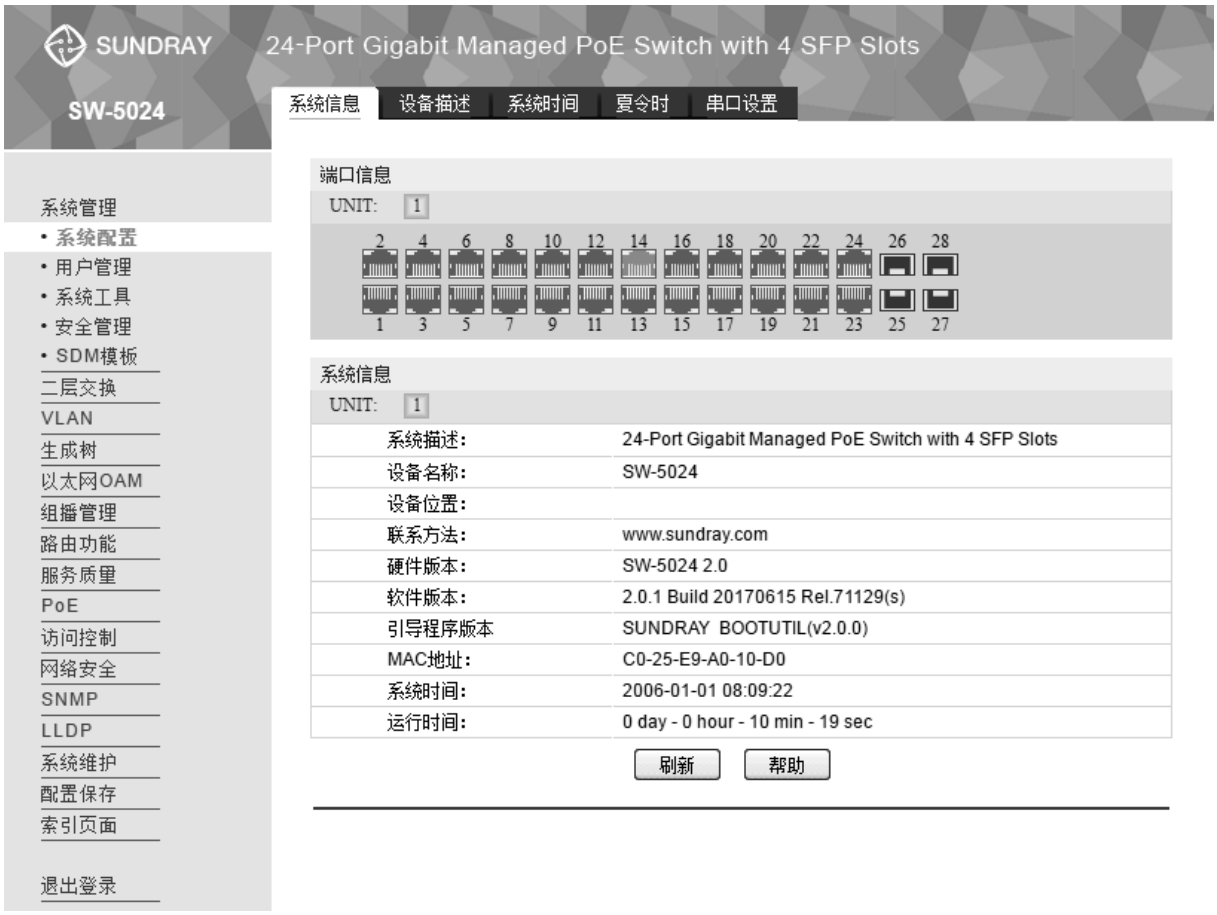


图 3-3 典型 Web 页面

左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域可分为三部分，条目配置区、列表管理区以及提示和注意区。

3.2.2 页面常见按键及操作

- **主菜单区按键**

按键	含义
配置保存	保存最终的配置。
退出登录	退出 Web 页面。

注意：

- 更改每一个配置后，点击<提交>按键只能使当前配置在交换机未重启前暂时生效；若需要当前配置在交换机重启后依旧生效，则需要点击<配置保存>。建议在交换机断电或重启前点击<配置保存>，以免丢失最新的配置。

- **条目配置区常见按键**

按键	含义
提交	提交当前的配置。
添加	添加当前配置条目。

按键	含义
修改	修改并保存编辑后的配置信息。
清空	快速清空当前配置项中已输入的所有信息。
帮助	打开当前功能的帮助页面。

说明：

- <修改>按键只有在编辑列表中的条目时才会出现，取代原本的<新增>按键。

➢ **列表管理区常见按键**

按键	含义
全选	选中当前列表中所有条目。
删除	删除选中的条目，可批量操作。
刷新	刷新列表。
选择	根据所输序号，快速选择至列表中的对应条目。

回目录

第4章 系统管理

系统管理模块主要用于配置交换机的系统属性，包括**系统配置**、**用户管理**、**系统工具**、**安全管理**以及 **SDM 模板**。

4.1 系统配置

系统配置用于配置交换机的基本属性，本功能包括**系统信息**、**设备描述**、**系统时间**、**夏令时管理**和**串口设置**五个配置页面。

4.1.1 系统信息

本页面用来查看本交换机的端口连接状态和系统信息。

端口状态指示了本交换机的 24 个 10/100/1000Mbps RJ45 端口以及 4 个 SFP 扩展模块槽的工作状态，其中标识为 1-24 的端口是 10/100/1000Mbps RJ45 端口，标识为 25~28 的端口是光纤模块端口。

进入页面的方法：**系统管理>>系统配置>>系统信息**

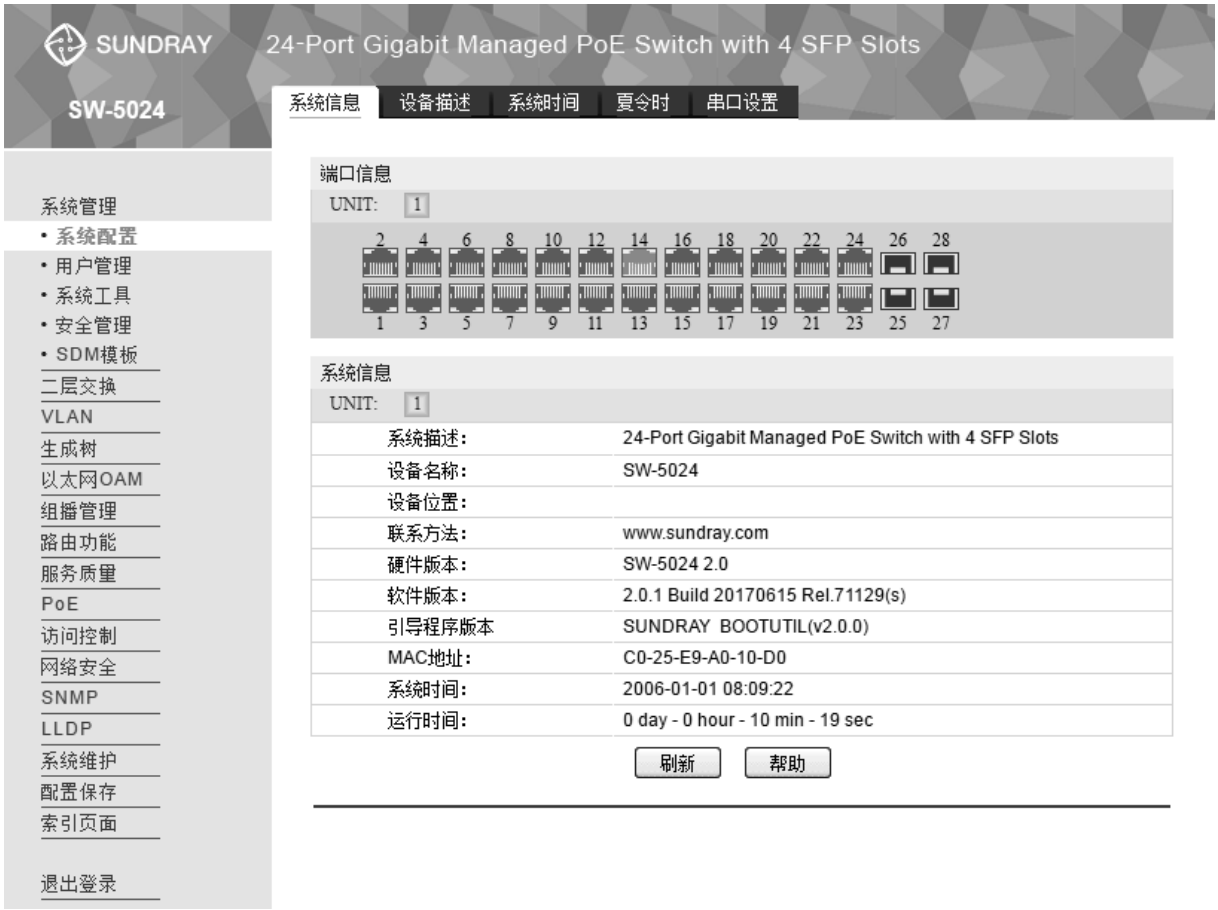


图 4-1 系统信息

条目介绍：

- **端口状态**

 1000M 端口未接入设备。

 1000M 端口工作速率为 1000Mbps。

 1000M 端口工作速率为 100Mbps /10Mbps。

 SFP 端口未接入设备。

 SFP 端口工作速率为 1000Mbps。

 SFP 端口工作速率为 100Mbps。

当鼠标移到某端口上时，会显示该端口的详细信息，如下图所示。

图 4-2 端口信息

条目介绍：

- **端口信息**

端口： 显示交换机的端口号。

类型： 显示端口的端口类型。

速率: 显示端口的最大传输速率。

状态： 现在端口的状态。

点击某端口，会显示此端口的带宽利用率，即实际传输速率与其最大传输速率的百分比，图中每隔 4 秒反馈一次监控值。查看各个端口的带宽利用率，可以了解各端口的流量概况，便于监控网络流量和分析网络异常。如下图所示。

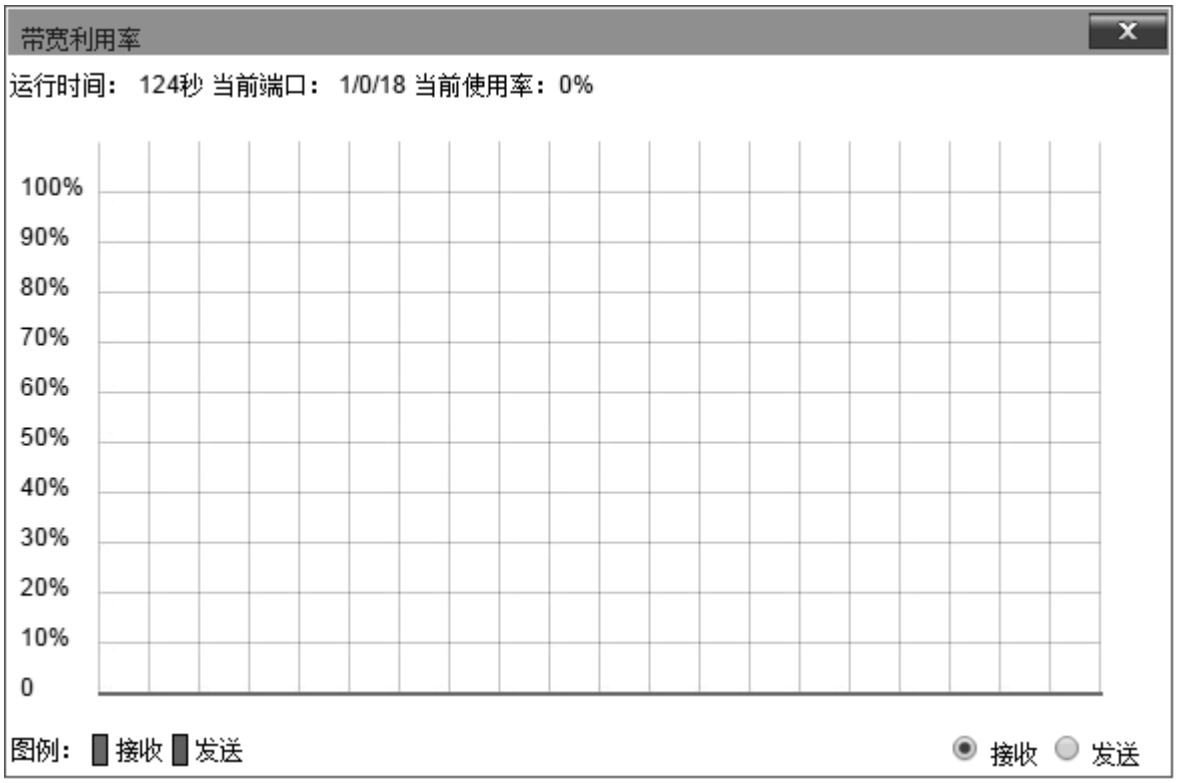


图 4-3 带宽利用率

条目介绍：

- **带宽利用率**

接收	点击后，显示此端口接收数据的带宽利用率。
发送	点击后，显示此端口发送数据的带宽利用率。

4.1.2 设备描述

本页面用来配置交换机的描述信息，包括设备名称、设备位置、联系方法。

进入页面的方法：**系统管理>>系统配置>>设备描述**

图 4-4 设备描述

条目介绍：

- **设备描述**

设备名称：	填写交换机的名称。

设备位置： 填写交换机的位置信息。

联系方法： 填写联系方法。

4.1.3 系统时间

本页面用来配置交换机的系统时间。系统时间是交换机工作时使用的时间，其它功能（如访问控制）中的时间信息以此处为准。可以选择手动设置时间或者连接到一个 NTP（网络时间协议）服务器获取 UTC 时间，也可以获取当前管理 PC 的时间作为交换机的系统时间。

进入页面的方法：**系统管理>>系统配置>>系统时间**

图 4-5 系统时间

条目介绍：

- **时间信息**

当前系统时间： 显示交换机当前的日期、时间。

当前时间来源： 显示交换机当前的时间来源。

- **时间配置**

手动配置时间： 勾选后，手动配置日期、时间。

从 NTP 服务器获取时间： 勾选后，配置时区和 NTP 服务器的 IP 地址，交换机将自动获取 UTC 时间。此时交换机必须连接至 NTP 服务器。

- 时区：选择所在的时区。
- 首选/备选 NTP 服务器：填写 NTP 服务器的 IP 地址。
- 时间获取周期：设定从 NTP 服务器获取时间的周期。

从管理主机获取时间： 勾选后，将管理主机的时间配置为交换机的系统时间。

注意：

- 如果向指定的时间服务器请求时间不成功，交换机会选择向上一次成功获取时间的服务器地址和网络上默认的公用时间服务器地址来获取时间。

4.1.4 夏令时配置

本页面用于配置交换机的夏令时功能。

进入页面的方法：**系统管理>>系统配置>>夏令时**

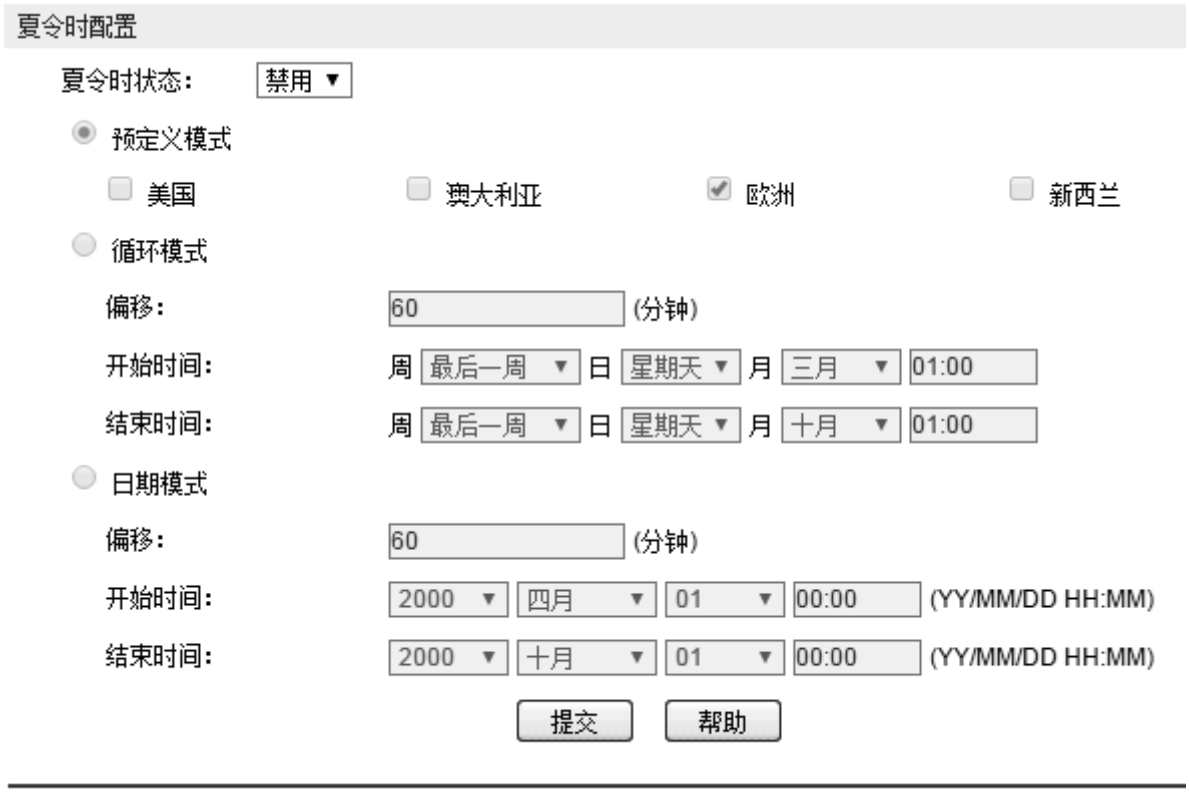


图 4-6 夏令时配置

条目介绍：

- **夏令时配置**

夏令时状态： 选择启用或禁用夏令时功能。

预定义模式： 选择一个预定义的夏令时配置。

- 美国：三月的第二个星期天 02:00 ~ 十一月的第一个星期天 02:00。
- 澳大利亚: 十月的第一个星期天 02:00 ~ 四月的第一个星期天 03:00。
- 欧洲: 三月的最后一个星期天 01:00 ~ 十月的最后一个星期天 01:00。
- 新西兰: 九月的最后一个星期天 02:00 ~ 四月第一个星期天 03:00。

循环模式： 配置夏令时功能。在这一模式下做的配置可以循环使用。

- 偏移: 指定当夏令时来临时，需要调整的时间额度。单位为分钟。
- 开始/结束时间: 分别选择夏令时开始和结束的时间。其中“周”表示一个月中的第几周；“日”表示星期几；“月”表示月份。

日期模式： 配置夏令时功能。在这一模式下做的配置只能在生效一次（开始时间的年份为当前年份）。

- 偏移: 指定当夏令时来临时，需要调整的时间额度。单位为分钟。
- 开始/结束时间: 分别选择夏令时开始和结束的时间。

注意：

- 当夏令时状态为禁用时，预定义模式、循环模式和日期模式都不可配置。
- 启用夏令时功能后，缺省配置为预定义模式下的欧洲配置模式。

4.1.5 串口设置

在这个页面上，您可以配置串口的波特率。

选择**系统→系统信息→串口设置**，配置下面的页面。

图 4-7 串口设置

以下的条目会显示在这个屏幕上：

- **串口设置**

波特率: 配置串口的波特率。它在默认情况下是 38400 bps。

数据位: 显示默认的数据位。

奇偶校验位: 显示奇偶校验位。

停止位: 显示停止位。

4.2 用户管理

用户管理用来限制登录交换机 Web 页面的用户的访问权限和身份，以保护交换机的有效配置。

本功能包括**用户列表**和**用户配置**两个配置页面。

4.2.1 用户列表

可以在本页查看到当前交换机存在的全部用户。

进入页面的方法：**系统管理>>用户管理>>用户列表**

图 4-8 用户列表

4.2.2 用户配置

本页用来配置登录交换机 Web 页面的用户的身份类型。本交换机提供四种类型的用户：管理员，操作员，高级用户和普通用户。管理员，可以编辑、修改和查看交换机各个功能的配置；操作员，操作员可以编辑，修改和查看大部分不同功能的设置；高级用户: 高级用户可以编辑，修改和查看不同功能的设置；普通用户：仅可以查看交换机各个功能的配置情况。本说明书内如无特殊说明，均以“管理员”身份登录时的 Web 页面为准。

进入页面的方法：**系统管理>>用户管理>>用户配置**

图 4-9 用户配置

条目介绍：

- **用户信息**

用户名： 填写登录 Web 页面的用户名。

访问等级： 选择该用户名的访问等级。

密码：	填写该用户名的登录密码。
确认密码：	再次输入该用户名的登录密码，两次输入的密码需保持一致。

- **用户列表**

选择：	勾选条目进行删除，可多选。但是不可以对当前登录用户自身进行删除。
序号、用户名、类型、状态：	显示当前用户的序号、用户名、用户类型和用户状态。
操作：	点击对应条目的<编辑>按键，可以修改该条目的用户信息。修改完毕后点击<修改>按键，修改内容生效。但是不允许修改当前登录用户自身的用户类型和状态。

4.3 系统工具

系统工具功能集中对交换机的配置文件进行管理。

4.3.1 Boot 配置

在这个页面上，您可以配置交换机的 boot 文件。当交换机启动时，将从当前镜像启动。如果失败了，交换机将尝试从备份镜像启动。如果这也失败了，你将进入 bootutil 菜单。

进入页面的方法：系统管理→系统工具→启动参数

图 4-10 Boot 配置

以下的条目会显示在这个屏幕上：

- **启动参数**

  选择: 选择单元(s)。

  成员: 显示成员。

  当前镜像: 显示当前的启动镜像。

  下次启动镜像: 选择下一个启动镜像。

  备份镜像: 选择备份的 boot 镜像。

4.3.2 配置导入

进入页面的方法：**系统管理>>系统工具>>配置导入**.

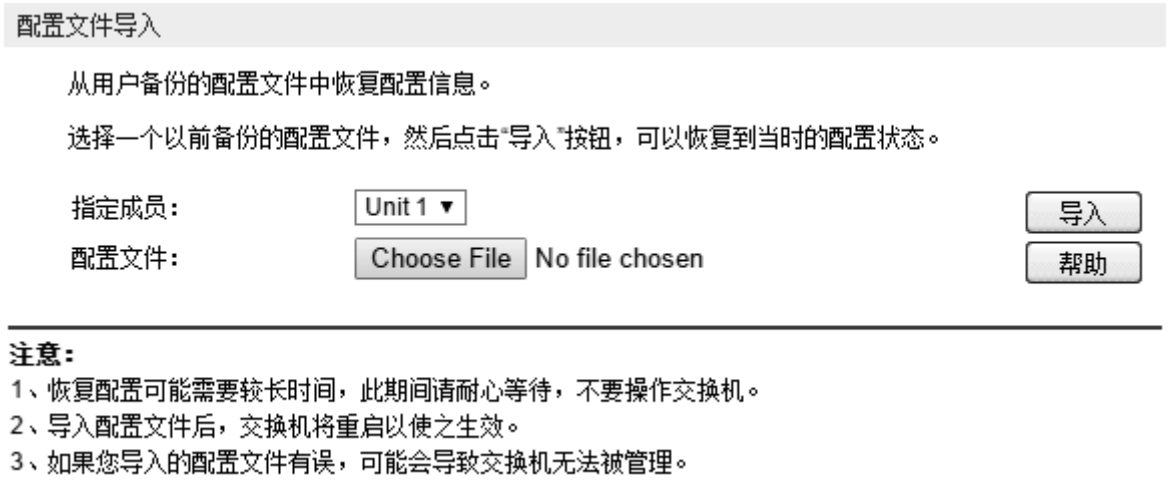


图 4-11 配置导入

条目介绍：

- **配置文件导入**

  配置文件导入： 从用户备份的配置文件中恢复配置。

注意：

- 备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

4.3.3 配置导出

在这个页面上，您可以下载当前的配置，并将它作为文件保存到您的计算机中，以备将来的配置恢复。

进入页面的方法：系统→系统工具→配置导出

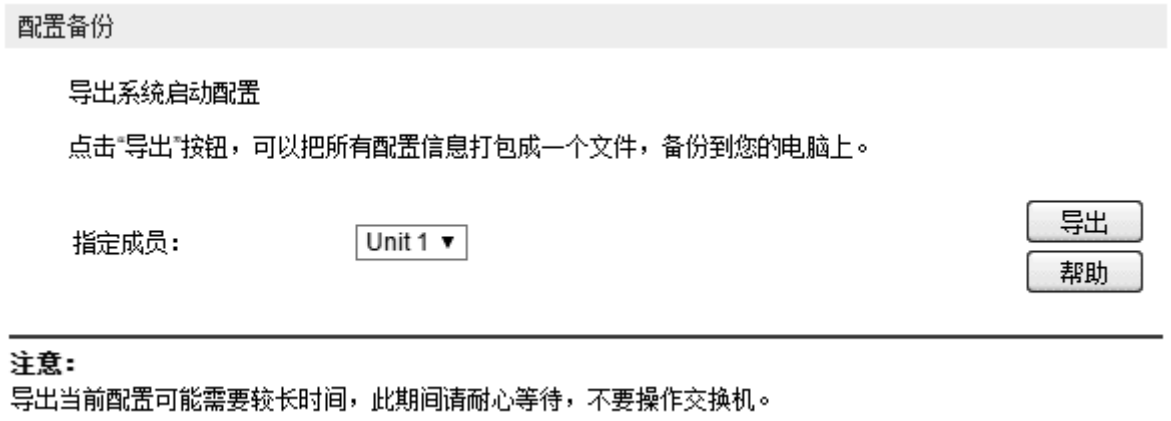


图 4-12 配置备份

以下的条目会显示在这个屏幕上：

- **配置备份**

指定成员: 选择一个交换机来导出配置文件。

单击**导出**按钮将当前启动配置文件保存到您的计算机中。建议您在升级之前采取这一措施。

注意:

备份配置需要几分钟时间。请在没有任何操作的情况下等待。

4.3.4 软件升级

本交换机可以通过 Web 方式升级系统文件，系统升级后将获得更完善的功能。

进入页面的方法：**系统管理>>系统工具>>软件升级**

图 4-12 软件升级

注意：

- 升级过程中不能被中断。
- 升级时请选择与当前硬件版本一致的软件。
- 升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。
- 当升级结束后，设备将会自动重新启动。
- 建议升级前备份配置信息。

4.3.5 系统重启

在此处可以重新启动交换机，交换机重启后自动返回到登录页面。重启前请先保存当前配置，否则重启后，未保存的配置信息将丢失。

进入页面的方法：**系统管理>>系统工具>>系统重启**

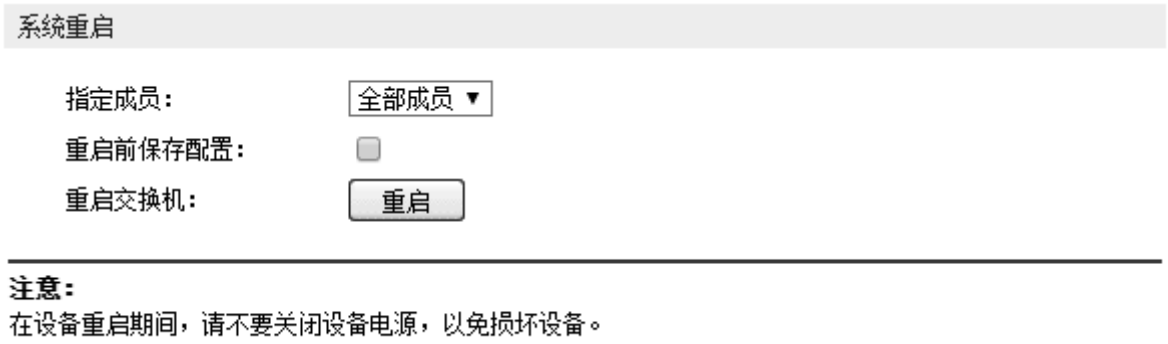


图 4-14 系统重启

注意：

- 在设备重启期间，请不要关闭设备电源，以免损坏设备。

4.3.6 计划重启

在这个页面上，您可以为交换机设置一个重新启动计划。用户可以用两种模式来配置重新启动的时间表。第一个是在特定的时间间隔内重新启动交换机。第二种是在特定的时间和日期重新启动交换机。

用户可以选择是否在重新启动之前保存配置。如果没有选择**重新启动之前保存**，那么重新启动的时间表将在下一次重新启动之后被删除。

进入页面的方法：系统→系统工具→计划重启

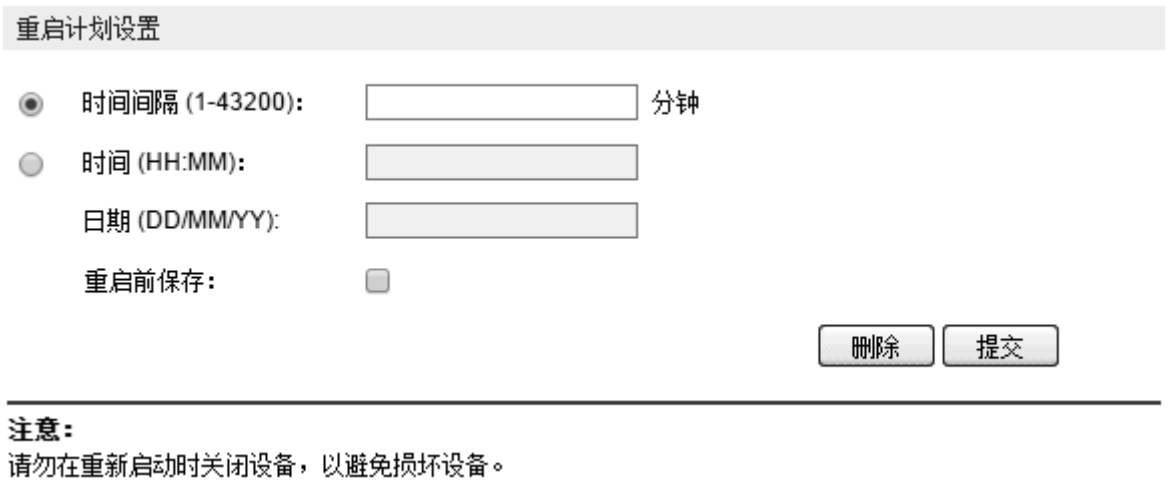


图 4-15 重启计划设置

以下的条目会显示在这个屏幕上：

- **重新启动计划设置**

时间间隔: 指定一段时间。交换机将在这段时间后重新启动。它的范围从 1 到 43200 分钟。如果用户选择了**在重新启动之前保存**，这个重新启动计划设置的配置仍会保留。

时间: 用 HH:MM 的格式指定交换机重启的时间。

日期: 日期应该在 30 天内。如果没有指定日期和时间设置比上面的时间晚，则交换机会晚启动；否则交换机将第二天重新启动。

重启前保存: 选择在重新启动之前保存交换机的配置。

注意:

为了避免损坏，请在重新启动时不要关闭设备。

4.3.7 软件复位

通过软件复位，可以将交换机恢复为出厂设置状态，所有配置数据将被清除。

进入页面的方法：**系统管理>>系统工具>>软件复位**

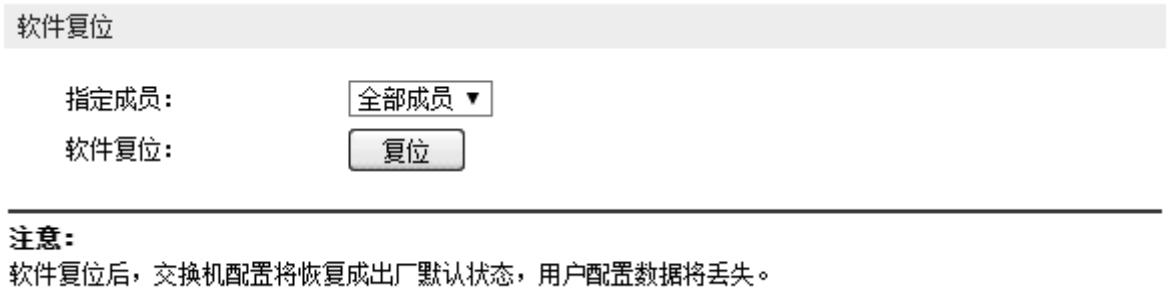


图 4-16 软件复位

注意：

- 软件复位后，交换机配置将恢复成出厂默认状态，配置的数据将丢失。

4.4 安全管理

安全管理功能是针对不同的远程登录方式，采取相应的安全措施，以增强用户管理交换机的安全性。

4.4.1 安全配置

本页用来限制登录交换机 Web 页面的用户的身份及人数，从而增强了交换机配置管理的安全性。其中，管理员及受限用户的定义请参考 **4.2 用户管理**。

进入页面的方法：**系统管理>>安全管理>>安全配置**

图 4-17 身份限制

条目介绍：

- **身份限制**

限制类型： 选择限制用户身份的类型。

- 基于 IP：用来限制访问交换机 Web 页面的用户的 IP 网段。
- 基于 MAC：用来限制访问交换机 Web 页面的用户的主机 MAC 地址。
- 基于端口：用来限制访问交换机 Web 页面的交换机端口号。

接入端口： 选择不同的接入端口，如 SNMP, Telnet, SSH 等。

IP 地址、掩码： 选择“基于 IP”时才能进行配置。只允许指定 IP 网段的用户才可以通过 Web 页面访问交换机。

MAC 地址： 选择“基于 MAC”时才能进行配置。只允许指定 MAC 地址的用户才可以通过 Web 页面访问交换机。

4.4.2 HTTP 配置

在 HTTP(超级文本传输协议)的帮助下，您可以通过标准的浏览器来管理交换机。HTTP 的标准开发是由 Internet 工程任务小组和万维网联盟协调的。

在这个页面下，您可以配置 HTTP 功能。

进入页面的方法：系统→安全管理→HTTP 配置

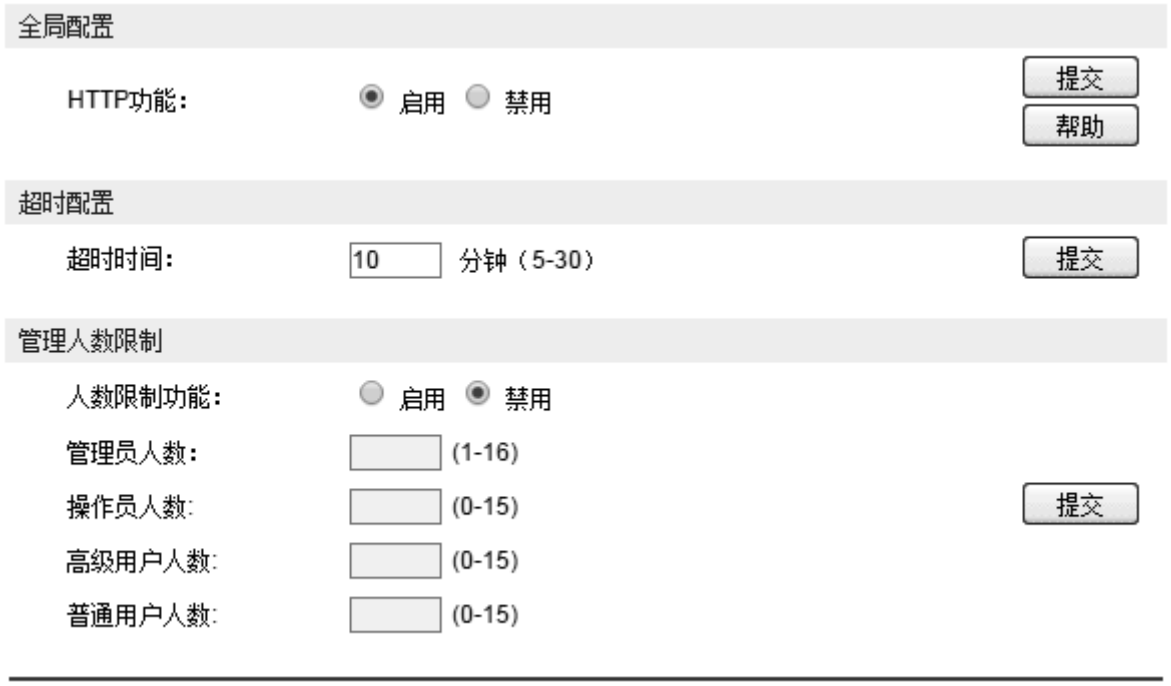


图 4-18 HTTP 配置

以下的条目会显示在这个屏幕上：

- **全局配置**

  HTTP: 选择启用/禁用交换机上的 HTTP 功能。

- **超时配置**

  超时时间: 如果在超时时间内对 Web 管理页面不做任何处理，系统将自动退出。如果您想要重新配置，请再次登录。

- **管理人数限制**

  人数限制功能： 选择启用/禁用数量控制功能。

  管理员人数: 输入作为管理员登录网页管理的最大用户数量。
  操作员人数： 输入作为操作员登录网页管理的最大用户数量。
  高级用户人数： 输入作为高级用户登录网页管理的最大用户数量。
  普通用户人数： 输入作为普通用户登录网页管理的最大用户数量。

4.4.3 HTTPS 配置

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于 TCP 的应用层协议提供安全连接，如为普通的 HTTP 连接提供更安全的 HTTPS 连接。SSL 协议广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输，多使用在电子商务、网上银行等领域，为网络上数据通讯提供安全性保证。

SSL 协议提供的服务主要有：

1. 对用户和服务器进行基于证书的身份认证，确保数据发送到正确的用户和服务器；

2. 对传输数据进行加密，以防止数据中途被窃取；

3. 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 采用非对称加密技术，使用“密钥对”进行数据的加密/解密，“密钥对”由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名）和对应私钥，也可以通过证书/密钥导入功能替换默认的密钥对，但 SSL 证书/密钥必须配对导入，否则 HTTPS 不能正常连接。

本功能生效后，即可通过 https://192.168.0.1 登录交换机的 Web 页面。初次使用交换机默认的证书通过 HTTPS 登陆交换机时，浏览器可能会提示“该证书是自签名的而不被信任”或“证书错误”，此时请将此证书添加为信任证书，或者继续浏览此网站即可。

该交换机还支持对 IPv6 的 HTTPS 连接。配置 IPv6 地址(例如，3001:1)后，您可以通过 https://[3001:1] 登录到交换机的网页管理页面。

在这个页面上，您可以配置 HTTPS 功能。

进入页面的方法：系统管理→安全管理→HTTPS 配置

图 4-19 HTTPS 配置

以下的条目会显示在这个屏幕上：

- **全局配置**

SSL 功能： 选择启用/禁用交换机上的 SSL 功能。

SSL3: 启用或禁用 SSL3.0 版本。默认情况下，它是启用的。

TLS 1: 启用或禁用 TLS1.0。默认情况下，它是启用的。

- **加密套件配置**

RSA_WITH_RC4_128_MD5: 与 RC4 128 位加密密钥交换密钥和 MD5 交换消息摘要。默认情况下，它是启用的。

RSA_WITH_RC4_128_SHA: 与 RC4 128 位加密密钥交换密钥和 SHA 交换消息摘要。默认情况下，它是启用的。

RSA_WITH_DES_CBC_SHA: 与 DES-CBC 消息加密交换密钥和 SHA 交换消息摘要。默认情况下，它是启用的。

RSA_WITH_3DES_EDE_CBC_SHA: 与 3DES 和 DES-EDE3-CBC 消息加密交换密钥和 SHA 交换消息摘要。默认情况下，它是启用的。

- **超时配置**

超时时间: 如果在超时时间内对 Web 管理页面不做任何处理，系统将自动退出。如果您想要重新配置，请再次登录。

- **管理人数限制**

人数限制功能: 选择启用/禁用人数限制功能。

管理员人数: 输入作为管理员登录网页管理的最大用户数量。

高级用户人数: 输入作为高级用户人数登录网页管理的最大用户数量。

高级用户人数: 输入作为普通用户人数登录网页管理的最大用户数量。

访客数量: 输入作为访客登录网页管理的最大用户数量。

- **证书导入**

SSL 证书: 选择要导入到交换机的 SSL 证书。

- **密钥导入**

SSL 密钥: 选择导入到交换机的 SSL 密钥。

注意:

1. SSL 证书和密钥下载必须彼此匹配;否则 HTTPS 连接将无法工作。
2. 建立一个安全连接使用 https，请输入 https://到浏览器的地址栏。
3. 与 http 连接相比，https 连接可能需要更多的时间，因为 https 连接涉及到身份验证、加密和解密等。

4.4.4 SSH 配置

SSH（Secure Shell，安全外壳）是由 IETF（Internet Engineering Task Force，因特网工程任务组）所制定，建立在应用层和传输层基础上的安全协议。SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上是使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境

远程登录到设备时，SSH 功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

SSH 是由服务器端和客户端组成的，并且有 V1 和 V2 两个不兼容的版本。在通讯过程中，SSH 服务器与客户端会自动互相协商 SSH 版本号和加密算法，协商一致后，由客户端向服务器端发起请求登录的认证请求，认证通过后双方即可进行信息的交互。本交换机支持 SSH 服务器功能，可以使用 SSH 客户端软件通过 SSH 连接方式登录交换机。

SSH 密钥导入是将 SSH 的公钥文件导入至交换机中。如果密钥导入成功，交换机会优先选用密钥认证的方式接受 SSH 登入。

进入页面的方法：系统管理>>安全管理>>SSH 配置

图 4-17 SSH 配置

条目介绍：

- **全局配置**

SSH 功能： 选择是否启用 SSH 功能。

协议版本 1： 选择是否启用对协议版本 1 的支持。

协议版本 2： 选择是否启用对协议版本 2 的支持。

静默时长： 填写静默时长。该时间内客户端无任何操作时，连接会自动断开。默认为 120 秒。

最大连接数： 填写 SSH 同时可允许的最大连接数，连接数若满，将无法再建立新的连接。默认为 5。

加密算法： 选择所需的加密算法。

密钥完整性算法： 选择所需的密钥完整性算法。

- **密钥导入**

密钥类型： 选择所要导入的密钥类型。本机支持 SSH-1 RSA，SSH-2 RSA 和 SSH-2 DSA 三种类型的密钥。

密钥文件： 选择要导入的密钥文件。

导入密钥： 点击此按键，将所选的 SSH 密钥导入交换机。

注意：

- 请确保导入的文件是密钥长度为 512 至 3072 比特的 SSH 公钥。
- 导入密钥文件后，交换机中此用户原有的同类型密钥将会被覆盖。如果导入的密钥文件有误，SSH 会转用密码认证的方式登陆。

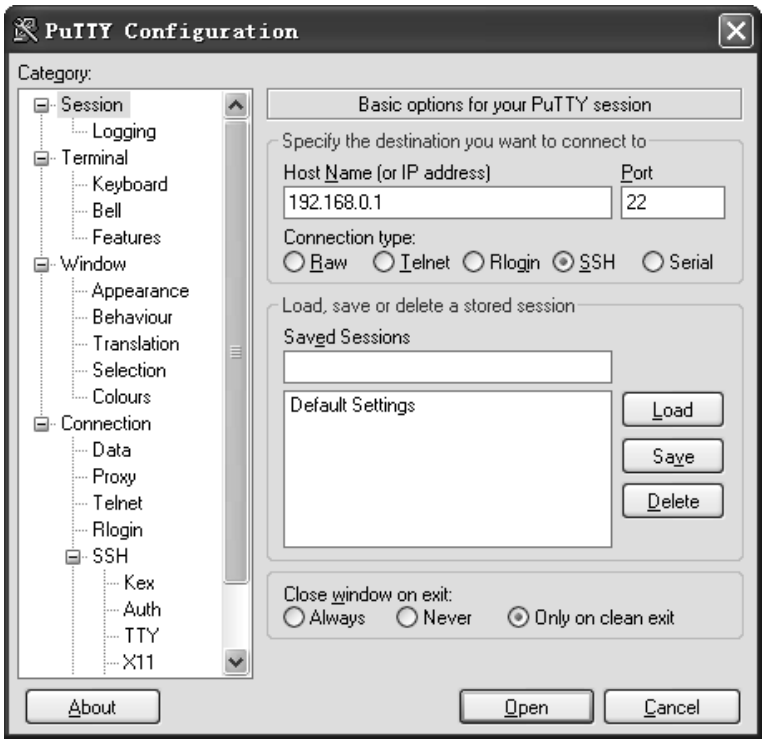
组网应用 1：

- **组网需求**

1. 使用 SSH 功能的“密码认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

- **配置步骤**

1. 打开软件，登录 PuTTY 的主界面。在“Host Name”处填写交换机的 IP 地址；“Port”保持默认的 22；“Connection type”处选择 SSH 的接入方式。如下图所示。



2. 点击<Open>按键，即可登录到交换机。操作方法与 telnet 相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。

注意：

完成上述配置步骤后，Putty 客户端显示“SW-5024>”表明您已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在超级终端上设置该密码。详细步骤请参考《命令行手册》中的 **1.1.2 配置特权模式密码**。

组网应用 2：

- **组网需求**

1. 使用 SSH 功能的“密钥认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

- **配置步骤**

1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。

注意：

- 密钥长度的范围为 256 至 3072 比特。
- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

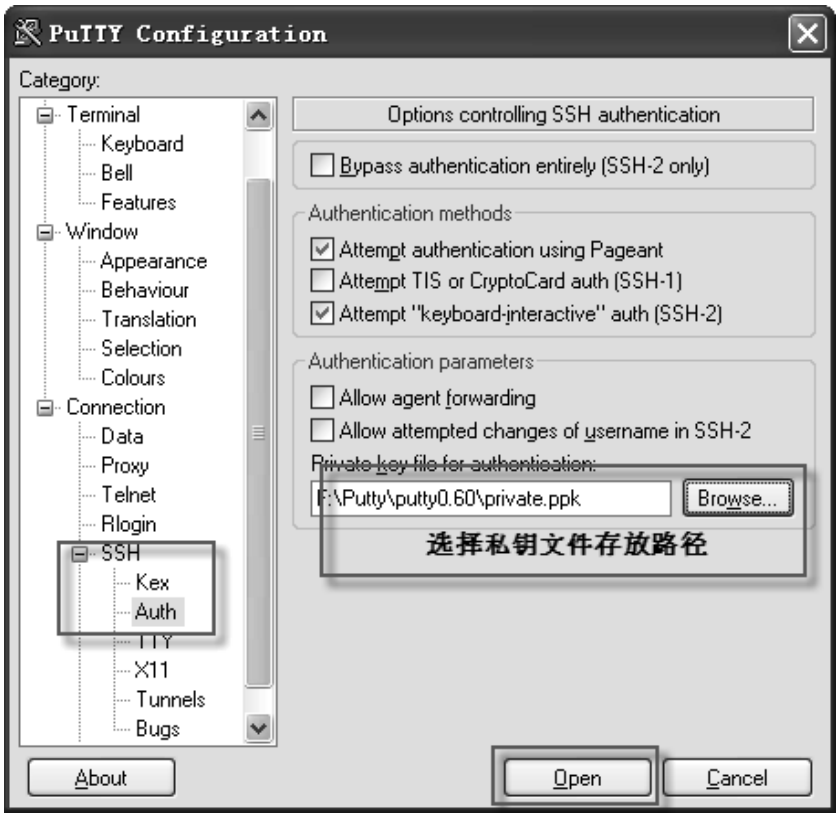
2. 密钥生成后，将公钥和私钥文件保存在主机上。如下图所示。

3. 在交换机配置页面上，将保存至主机上的公钥文件导入交换机中。

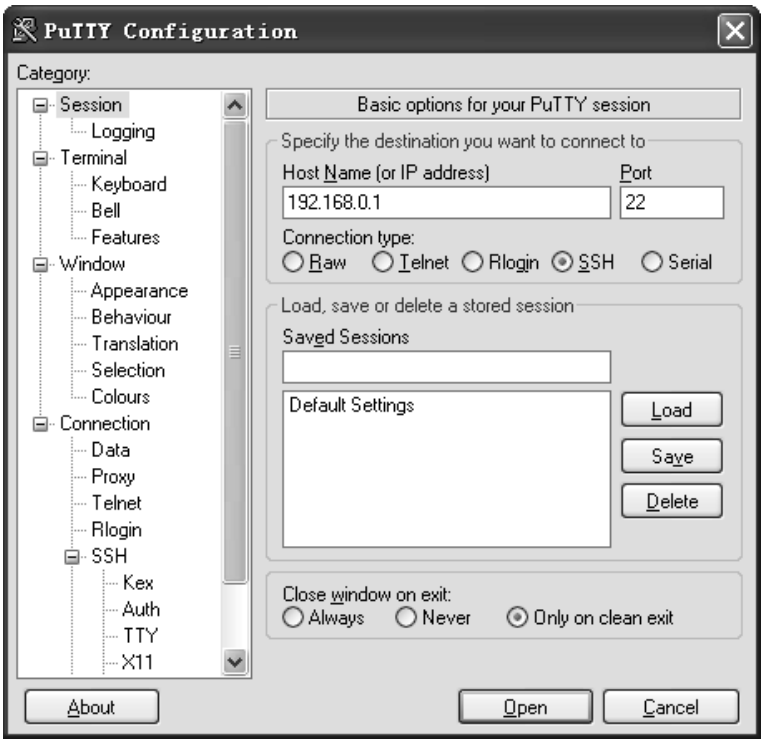
注意：

- 密钥类型要与密钥文件的类型保持一致。
- 载入 SSH 密钥的过程不能被中断。

4. 将私钥文件导入至 SSH 客户端软件中。如下图所示。



5. 经过上面步骤后，公钥和私钥文件都已导入，接着即可进入版本、密钥与算法协商配置操作。打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH 后，点击<open>按钮与服务器建立连接并进行协商。



6. 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。

注意：

完成上述配置步骤后，Putty 客户端显示“SW-5024>”表明您已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在超级终端上设置该密码。详细步骤请参考《命令行手册》中的 **1.1.2 配置特权模式密码**。

4.4.5 Telnet 配置

在这个页面上，您可以在交换机上启用/禁用 Telnet 功能。

进入页面的方法：系统管理→安全管理→Telnet 配置

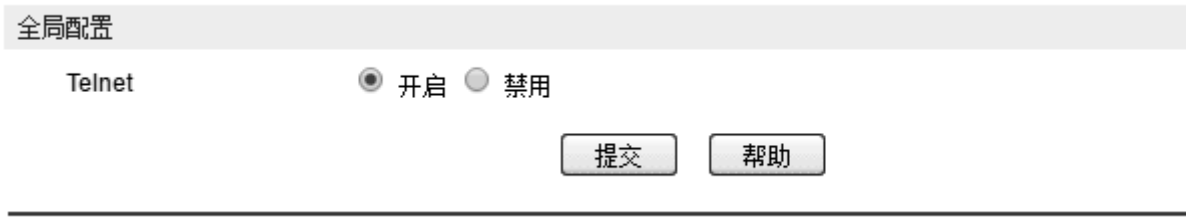


图 4-21 接入控制

以下的条目会显示在这个屏幕上：

- **全局配置**

  Telnet: 在交换机上选择全局启用/禁用 Telnet 功能。

4.5 SDM 模板

SDM(交换机数据库管理)为用户提供了不同的模板来有效地管理硬件 TCAM 资源。用户可以根据应用程序环境选择适当的模板。

4.5.1 SDM 模板配置

此页面可以配置和查看 SDM 模板视图。

进入页面的方法：菜单模板→系统→SDM 模板配置

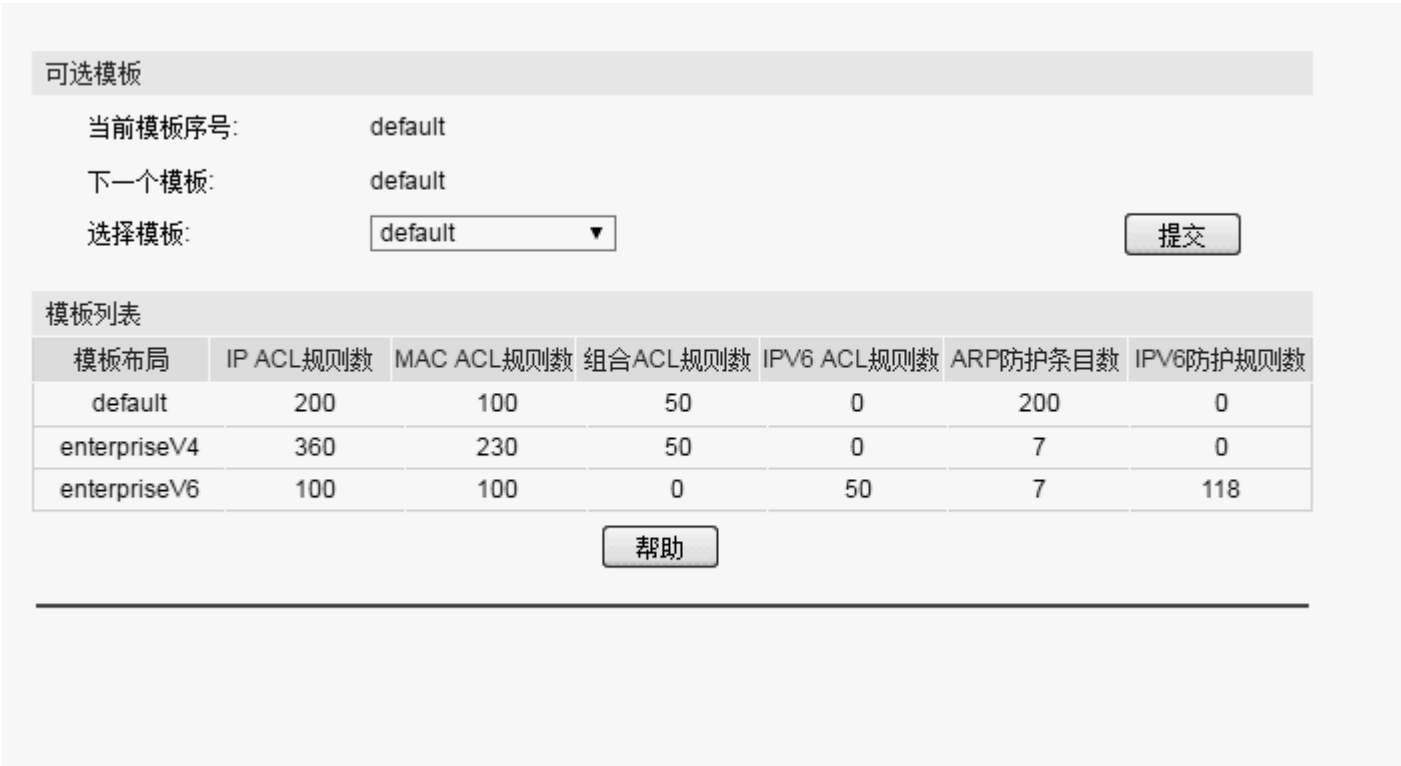


Figure 4-22 SDM Template Config

- **可选模板**

  当前模板序号: 显示当前使用的 SDM 模板。

  下一个模板: 显示下次重启后将被使用的 SDM 模板。

  选择模板: 选择下次重启后将被使用的 SDM 模板。

- **模板列表**

  模板布局: 显示模板名称。

  IP ACL 规则数: 显示 IP ACL 规则数，包括 Lay3 ACL 和 Lay4 ACL。

  MAC ACL 规则数: 显示二层 ACL 规则数。

  组合 ACL 规则数: 显示组合 ACL 规则数。

  IPv6 ACL 规则数: 显示 IPv6 ACL 规则数。

  ARP 防护条目数: 显示用于 ARP 防护的条目数。

  IPv6 防护规则数: 显示 IPv6 源防护规则数。

第5章 二层交换

二层交换模块主要用于配置交换机的基本功能，包括**端口管理**、**汇聚管理**、**流量统计**、**地址表管理**以及 **L2TP** 五个部分。

5.1 端口管理

端口管理用于配置交换机端口的基本属性，包括**端口配置**、**端口监控**、**端口安全**、**端口隔离**和**环路监测**五个配置页面。

5.1.1 端口配置

端口配置用来配置交换机端口的各项基本参数。端口状态选择“禁用”时，交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

端口基本参数将会直接影响端口的工作方式，请结合实际情况进行配置。

进入页面的方法：二层交换>>端口管理>>端口配置

图 5-1 端口配置

条目介绍：

- **端口配置**

  选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

类型： 显示交换机端口类型。

描述： 填写端口的描述信息，以区分各个端口的用途。

状态： 选择端口状态。只有状态为启用时，端口才能正常转发数据包。

速率、双工： 选择端口的传输速率及传输模式。与交换机相连的设备必须与交换机的传输速率及双工状态保持一致。当选择“Auto”选项时，该端口的速率双工由自动协商决定。默认为 Auto。对于 SFP 端口，本系列交换机暂不提供自动协商。

流控： 选择端口的流控状态。启用流控能够同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口状态配置为禁用则不能通过该端口管理交换机，请将要进行管理的端口配置为启用状态。
- 从属于同一个汇聚组的所有成员端口的相应参数配置应该保持一致。

5.1.2 端口监控

端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

进入页面的方法：二层交换>>端口管理>>端口监控

图 5-2 端口监控

条目介绍：

➢ **监控组列表**

监控组： 显示监控组的组号。

监控端口： 显示每个监控组的唯一的一个监控端口号。

监控方式： 显示每个监控组的监控方式。分为入口监控和出口监控。

被监控端口： 显示每个监控组的所有被监控端口。

操作： 点击<编辑>按键，对每个监控组的配置进行修改。

点击<编辑>按键，显示界面如下图所示：

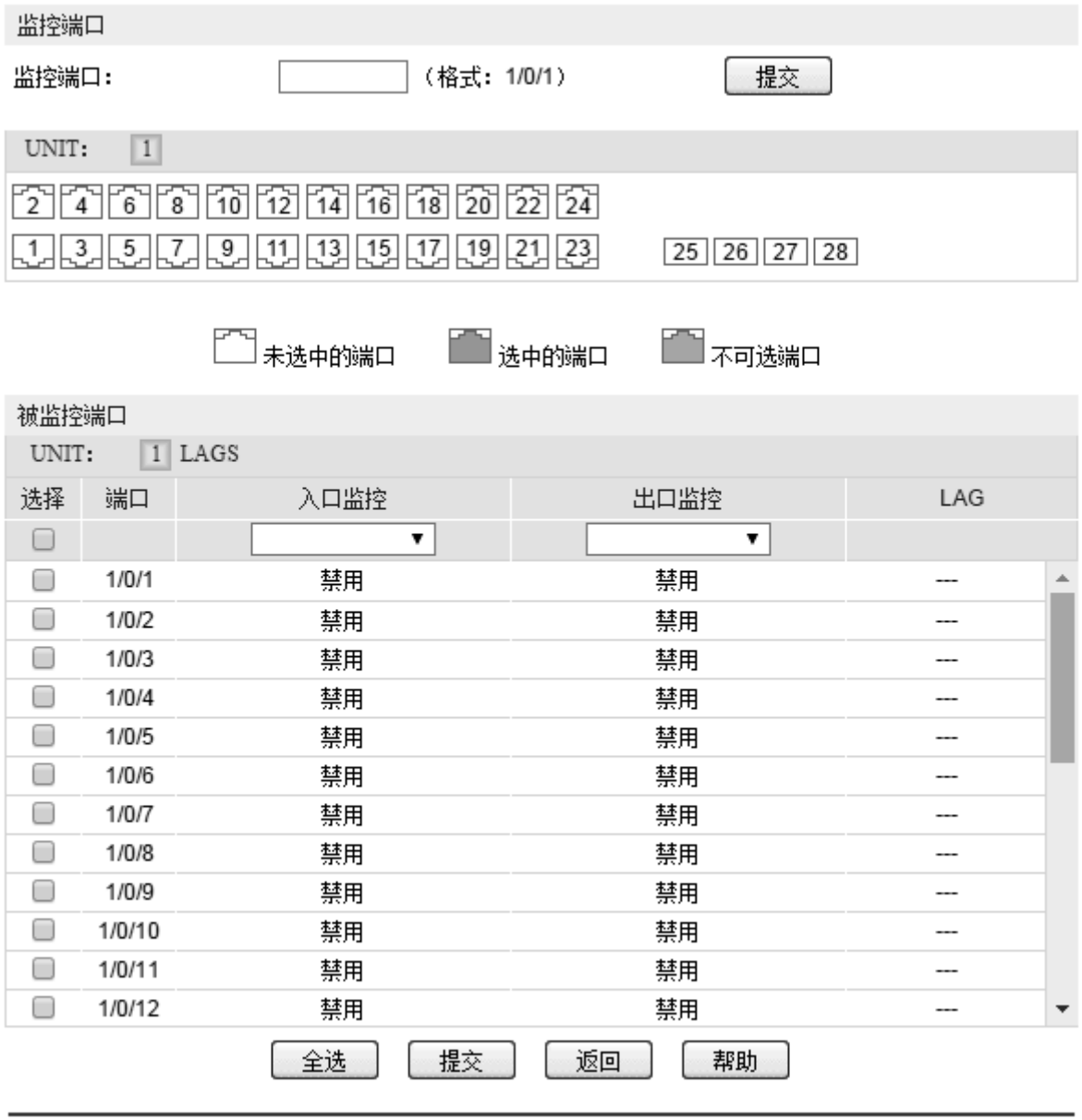


图 5-3 编辑监控组

条目介绍：

- **监控组选择**

  选择组号： 选择需要进行配置的监控组组号。

- **监控端口配置**

  监控端口： 在此处选择该监控组的监控端口。

- **被监控端口**

选择：	勾选端口配置为被监控端口，可多选。
端口：	显示交换机的端口号。
入口监控：	对被监控端口收到的数据进行监控，复制到监控端口。
出口监控：	对被监控端口发出的数据进行监控，复制到监控端口。
LAG：	显示端口当前所属的汇聚组。汇聚组成员端口不能选为监控端口和被监控端口。

注意：

- 汇聚组的成员端口既不能作为监控端口，也不能作为被监控端口。
- 一个端口不可以既作为监控端口又作为被监控端口。
- 端口监控功能可以跨越 VLAN 进行监控。

5.1.3 端口安全

交换机地址表维护着端口和接入端的 MAC 地址的对应关系，并以此建立交换路径，地址表的大小是固定的。地址表攻击是指利用工具产生欺骗 MAC，快速填满地址表，交换机地址表被填满后，交换机将以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探，攻击获取网络信息。地址表满了后，数据流以泛洪的方式发送到所有端口，会造成交换机负载过大，网络缓慢和丢包甚至瘫痪。

端口安全通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击并控制端口的网络流量。如果端口启用端口安全功能，将动态学习接入的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，以保证安全性。

进入页面的方法：二层交换>>端口管理>>端口安全

图 5-4 端口安全

条目介绍：

- **端口安全**

选择： 勾选端口配置端口安全，可多选。

端口： 显示交换机的端口号。

最大学习地址数： 填写对应端口最多可以学习的 MAC 地址数目。默认为 64。

已学习地址数： 显示对应端口已经学习的 MAC 地址数目。

学习模式： 选择 MAC 地址学习的模式。

- 动态：MAC 地址学习受老化时间的限制，老化时间过后，所学的 MAC 地址将被删除。
- 静态：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目清空。
- 永久：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目保持不变。

状态： 选择是否启用端口安全功能。

注意：

- 当端口为汇聚组成员，该端口的端口安全功能被禁用。只有将端口从汇聚组中去掉，才可以使用端口的端口安全功能。

5.1.4 端口隔离

通过端口隔离功能，可以为交换机的任意物理端口指定转发端口。设置了端口隔离功能后，每个物理端口只能向自己的转发端口转发数据包。

进入页面的方法：二层交换>>端口管理>>端口隔离

端口	LAG	转发端口
1/0/1	---	1/0/1-28,LAG1-14
1/0/2	---	1/0/1-28,LAG1-14
1/0/3	---	1/0/1-28,LAG1-14
1/0/4	---	1/0/1-28,LAG1-14
1/0/5	---	1/0/1-28,LAG1-14
1/0/6	---	1/0/1-28,LAG1-14
1/0/7	---	1/0/1-28,LAG1-14
1/0/8	---	1/0/1-28,LAG1-14
1/0/9	---	1/0/1-28,LAG1-14
1/0/10	---	1/0/1-28,LAG1-14
1/0/11	---	1/0/1-28,LAG1-14

图 5-5 端口隔离

条目介绍：

- **端口隔离列表**

端口： 显示交换机的端口号。

转发端口： 显示可转发的端口列表。

5.1.5 环路监测

环路监测（Loopback Detection）通过环路监测数据包检测交换机连接的网络中是否存在环路，当检测出环路时根据用户设定处理相应的端口。

进入页面的方法：二层交换>>端口管理>>环路监测

图 5-6 环路监测

条目介绍：

- **全局配置**

环路监测功能： 选择是否启用交换机的环路监测功能。

环路监测间隔： 设置环路监测的时间间隔，默认值为 30。

自动恢复时间： 设置被阻塞环路端口的自动恢复时间，设置值为环路监测间隔的整数倍，默认为 3。

页面自动刷新： 选择是否启用页面的自动刷新功能。

自动刷新间隔： 设置页面自动刷新的时间间隔，默认值为 6。

- **端口配置**

端口选择： 点击<选择>按钮，可根据所输端口号快速选择相应端口。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用此功能。

处理模式： 选择端口发现环路时的处理模式：
- Alert：端口上发现环路时只发出报警信息。
- Port based：端口上发现环路时发出报警信息，同时阻塞端口。

恢复模式： 选择端口被阻塞后的恢复模式：
- Auto：端口被阻塞后，经过自动恢复时间后将自动解除阻塞。
- Manual：端口被阻塞后只能手动接触阻塞状态。

环路状态： 显示该端口是否监测到外部环路。

阻塞状态： 显示该端口是否因为监测到环路而处于阻塞状态。

LAG： 显示该端口当前所属的汇聚组。

手动恢复： 重置选定端口状态，解除阻塞。

注意：
- 环路监测务必与风暴抑制配合使用。

5.2 汇聚管理

LAG（Link Aggregation Group，端口汇聚组）是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现流量在汇聚组中各个成员端口之间进行分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、GVRP、VLAN、端口属性、MAC 地址学习等。具体说明如下：

- 开启 **GVRP**、**802.1Q VLAN**、**语音 VLAN**、**生成树**、**QoS 配置**、**DHCP 侦听**及**端口配置**（速率双工、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启**端口安全**、**端口监控**、**MAC 地址过滤**、**静态 MAC 地址绑定**、**802.1X 认证**功能的端口，不能加入汇聚组。
- 开启 **ARP 防护**、**DoS 防护**功能的端口，建议不要将其加入汇聚组。

如果需要配置汇聚组，建议在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。

说明：
- LAG 带宽的计算：当使用四个全双工 1000Mbps 端口构成 LAG 时，由于每一个端口上行和下行各是 1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 LAG 技术汇聚在一起形成的总带宽为 8000Mbps。
- LAG 的流量会根据选路算法均衡分配到各个成员端口中去。当 LAG 中的一个或几个端口连接断开的时候，这些端口的流量会转移到 LAG 中其它链接正常的端口中去，即具备链路冗余备份功能。

按照汇聚方式的不同，端口汇聚可以分为两类：手动配置和 LACP 配置。本功能包括**汇聚列表**、**手动配置**和 **LACP 配置**三个配置页面。

5.2.1 汇聚列表

在本页可以查看到交换机当前的全部汇聚组。

进入页面的方法：二层交换>>汇聚管理>>汇聚列表

图 5-7 汇聚列表

条目介绍：

- **全局配置**

  选路算法： 根据选路算法规则，选择转发数据的端口。
  - 源目的 MAC 地址：仅使用数据包中的源目的 MAC 地址信息。
  - 源目的 IP 地址：仅使用数据包中的源目的 IP 地址信息。

- **汇聚列表**

  选择： 勾选汇聚组进行删除，可多选。

  组号： 显示汇聚组的序号。

  描述： 显示汇聚组的描述信息。

  成员： 显示属于汇聚组的物理端口。

  操作： 对单个汇聚组进行相应配置。
  - 编辑：修改汇聚组的描述和成员端口。
  - 查看：查看汇聚组的端口状态信息。

点击<查看>按键，可以看到所选汇聚组的详细信息。

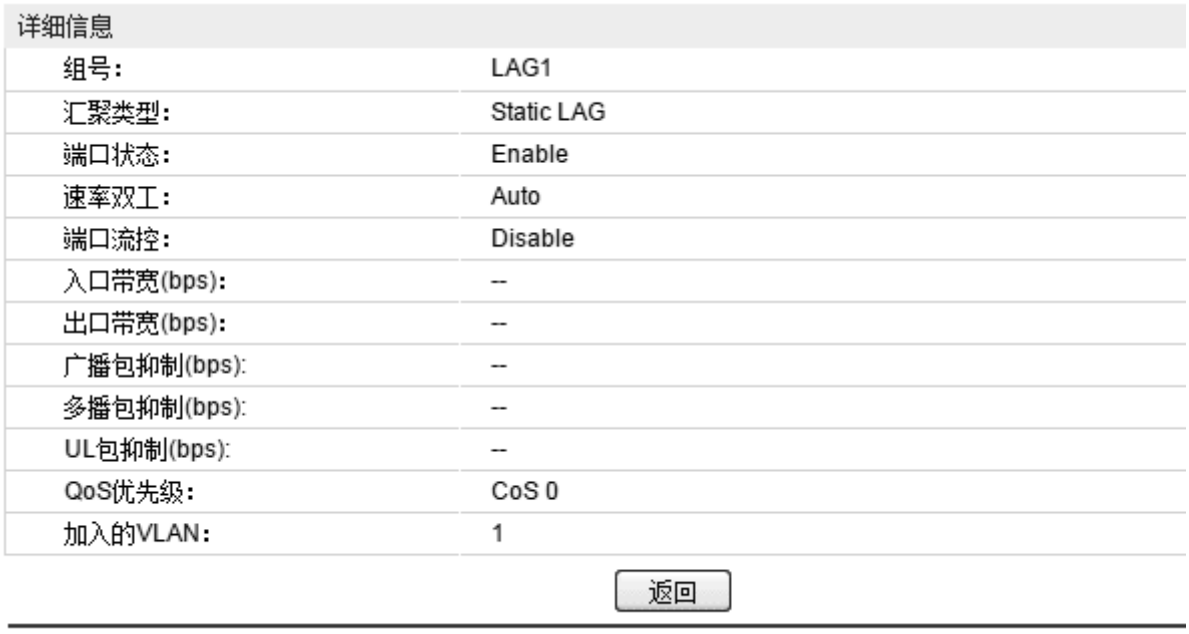


图 5-8 汇聚组状态

5.2.2 手动配置

在本页可以对汇聚组进行手动配置，手动配置的汇聚端口的 LACP 状态为禁用。

进入页面的方法：二层交换>>汇聚管理>>手动配置

图 5-9 手动配置

条目介绍：

- **汇聚组配置**

  汇聚组号： 选择汇聚组的序号，组号格式为 LAG*。

该组描述： 显示汇聚组的描述信息。

- **成员端口**

成员端口： 勾选属于汇聚组的物理端口，清空表示删除该汇聚组。

说明：

- 要删除一个已配置的 LAG，将该 LAG 的成员清空并提交即可。
- 一个端口仅可以处于一个汇聚组中。即若端口已成为其它 LAG 的成员端口，或者已汇聚成为 LACP 中的成员时，该端口处于灰化状态，不能勾选。

5.2.3 LACP 配置

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是基于 IEEE802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。汇聚的双方通过协议交互汇聚信息，将匹配的链路汇聚在一起收发数据，汇聚组内端口的添加和删除是协议自动完成的，具有很高的灵活性并提供了负载均衡的能力。

启用端口的 LACP 功能后，该端口向对端通告本端的系统优先级、系统 MAC、端口优先级、端口号和操作 Key（由端口的物理属性、上层协议信息和管理 Key 决定）。设备优先级高的一端将主导汇聚及解汇聚，设备优先级由系统优先级和系统 MAC 决定，系统优先级值小的设备优先级高，系统优先级值相同时系统 MAC 较小的设备优先级高。设备优先级高的一端将根据端口优先级、端口号以及操作 Key 选择汇聚端口，操作 Key 相同的端口才能被选入同一个汇聚组，同一个汇聚组内端口优先级值小的端口会被优先选择，当端口优先级相同的时候，端口号小的会被优先选择。双方交互汇聚信息后被选择的端口将汇聚在一起收发数据。

在本页可以配置交换机的 LACP 功能。

进入页面的方法：二层交换>>汇聚管理>>LACP 配置

图 5-10 LACP 配置

条目介绍：

- **全局配置**

系统优先级： 与系统的 MAC 地址一起决定设备优先级，设备优先级高的一端将主导汇聚及解汇聚。默认为 32768。

- **LACP 配置**

选择： 勾选端口配置端口 LACP 功能，可多选。

端口： 显示交换机的端口号。

管理 Key： 处于同一汇聚组的成员，需配置相同的管理 Key。

端口优先级： 决定了成为汇聚组成员的端口的优先级。端口优先级值小的端口会被优先选择。若端口优先级相同，则端口号小的会被优先选择。默认为 32768。

模式： 显示交换机模式

状态： 选择相应端口是否启用 LACP 功能。

LAG： 显示端口当前所属的汇聚组。

5.3 流量统计

流量统计用于统计流经各个端口的数据信息，本功能包括**流量概览**和**详细统计**两个配置页面。

5.3.1 流量概览

流量概览用来显示交换机各端口的流量信息，便于监控网络流量和分析网络异常。

进入页面的方法：二层交换>>流量统计>>流量概览

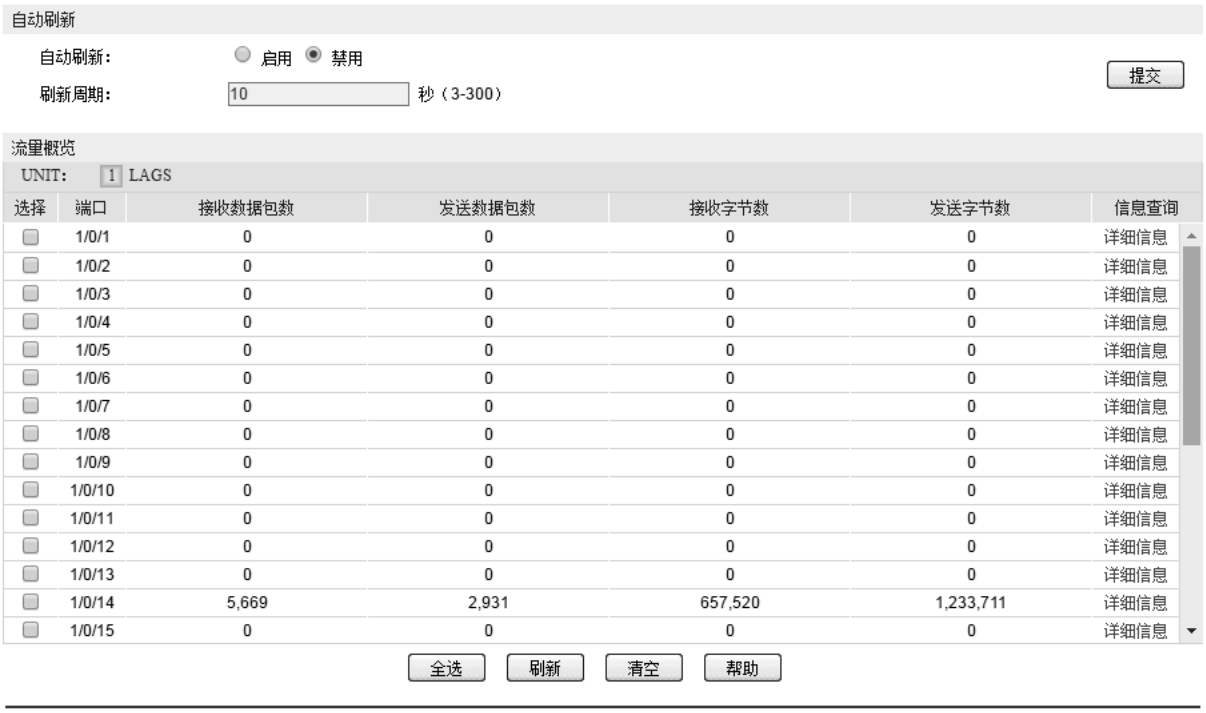


图 5-11 流量概览

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为 10 秒。

- **流量概览**

端口选择： 点击<选择>按键，可根据所输端口号，快速查找端口条目。

端口： 显示交换机的端口号。

接收数据包数： 统计交换机各端口接收的数据包数，不包括错误的数据包。

发送数据包数： 统计交换机各端口发送的数据包数。

接收字节数： 统计交换机各端口接收的字节数，包括错误的数据包的字节数。

发送字节数： 统计交换机各端口发送的字节数。

信息查询： 点击查询相应端口的详细统计信息。

5.3.2 详细统计

详细统计用来统计各端口传输数据包的详细信息，便于定位网络问题。

进入页面的方法：二层交换>>流量统计>>详细统计

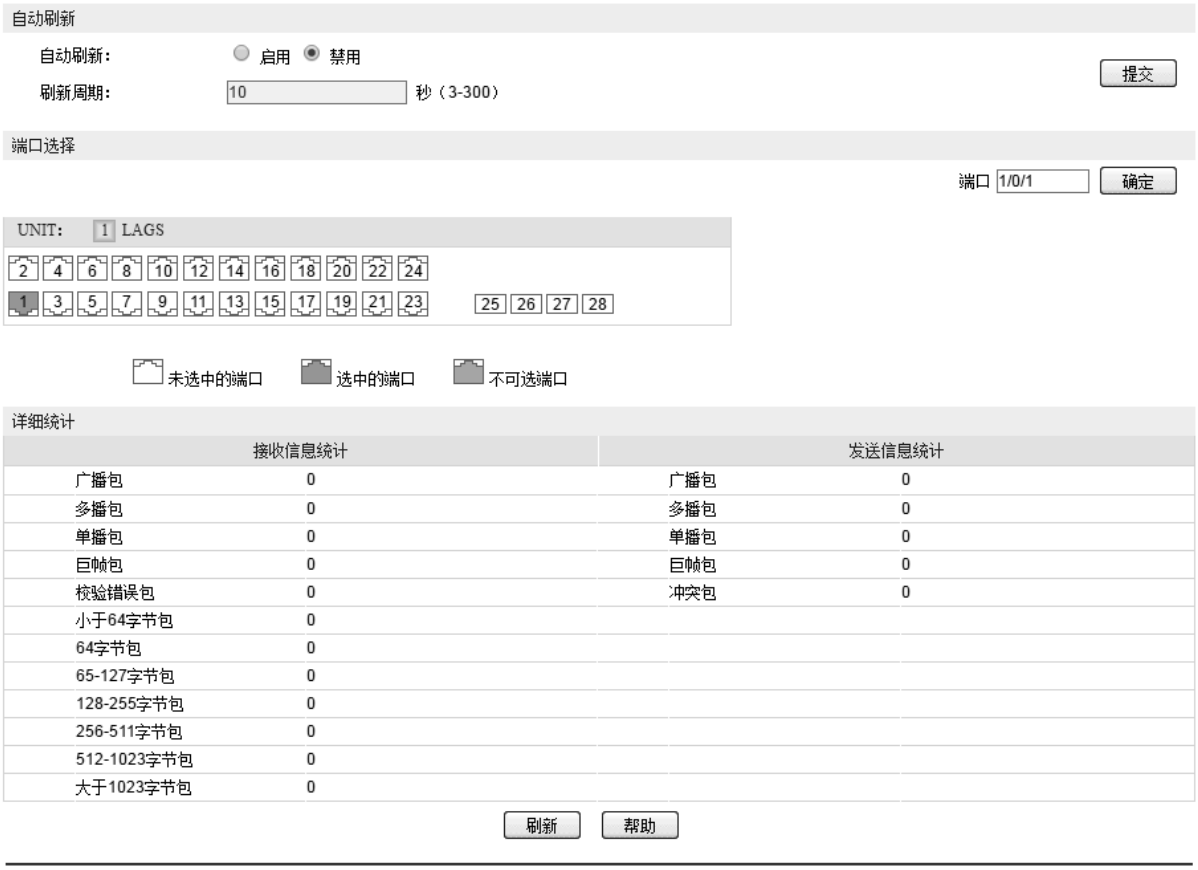


图 5-12 详细统计

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

- **详细统计**

端口： 输入要查看流量信息的交换机端口号。

接收信息统计： 统计该端口接收数据包的详细信息。

发送信息统计： 统计该端口发送数据包的详细信息。

广播包： 端口接收/发送的含有效广播地址的数据包数目（不含错误帧）。

组播包： 端口接收/发送的含有效组播地址的数据包数目（不含错误帧）。

单播包： 端口接收/发送的含有效单播地址的数据包数目（不含错误帧）。

Alignment 错误包： 端口接收的长度为 64-1518 字节的校验和错误且字节数不对齐的数据帧数目。

小于 64 字节包： 端口接收的长度小于 64 字节的数据帧数目（不含错误帧）。

64 字节包： 端口接收的长度为 64 字节的数据帧数目（包含错误帧）。

65-127 字节包： 端口接收的长度为 65-127 字节的数据帧数目（包含错误帧）。

128-255 字节包： 端口接收的长度为 128-255 字节的数据帧数目（包含错误帧）。

256-511 字节包： 端口接收的长度为 256-511 字节的数据帧数目（包含错误帧）。

512-1023 字节包： 端口接收的长度为 512-1023 字节的数据帧数目（包含错误帧）。

大于 1023 字节包： 端口接收的长度大于 1023 字节小于 jumbo 帧长的数据帧数目（包含错误帧）。

冲突包： 端口工作在半双工模式下发送数据包时产生的冲突包数目。

5.4 地址表管理

交换机的主要功能是对报文进行转发，也就是根据报文的目的 MAC 地址将报文输出到相应的端口。地址表包含了端口间报文转发的地址信息，是交换机实现报文快速转发的基础。地址表中的表项可以通过自动学习和手动绑定两种方式进行更新和维护，多数地址表条目都是通过自动学习功能来创建和维护的，而对于某些相对固定的连接来说，手动绑定可以提高交换机的效率，通过 MAC 地址过滤功能可以使交换机对不期望转发的数据帧进行过滤，从而提升了网络安全性。

地址表的分类及特点如下表所示：

地址表类别	配置方式	有无老化时间	重启后是否被保留（配置保存后）	已绑定的 MAC 地址与端口的关系
静态地址表	手动配置	无	是	在同一 VLAN 中，已绑定的 MAC 地址不能被其它端口学习
动态地址表	自动学习	有	否	已绑定的 MAC 地址可以重新被其它端口学习
过滤地址表	手动配置	无	是	-

本功能包括**地址表显示**、**静态地址表**、**动态地址表**和**过滤地址表**四个配置页面。

5.4.1 地址表显示

在本页可以查看到交换机地址表的全部信息。

进入页面的方法：二层交换>>地址表管理>>地址表显示

图 5-13 地址表显示

条目介绍：

- **查询选项**

MAC 地址： 填写欲查找条目需包含的 MAC 地址信息。

VLAN ID： 填写欲查找条目需包含的 VLAN ID 信息。

端口： 选择欲查找条目需包含的交换机端口。

地址类型： 选择欲查找条目需包含的地址类型信息。

- 全部：显示全部地址表条目。
- 静态：显示静态地址表条目。
- 动态：显示动态地址表条目。
- 过滤：显示过滤地址表条目。

- **地址表**

MAC 地址： 显示交换机学习到的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

5.4.2 静态地址表

静态地址表记录了端口的静态地址。静态地址是不会老化的 MAC 地址，它区别于一般的由端口学习得到的动态地址。静态地址只能手动添加和删除，不受最大老化时间的限制。这对于某些相对固定的连接来说，可减少地址学习步骤，从而提高交换机的转发效率。静态地址表也可以显示在**端口安全**功能中自动学习到的静态 MAC 地址。

进入页面的方法：二层交换>>地址表管理>>静态地址表

图 5-14 静态地址表

条目介绍：

- **新建条目**

  MAC 地址： 填写静态绑定的 MAC 地址。

  VLAN ID： 填写 MAC 地址条目对应的 VLAN ID。

  端口： 选择静态绑定的交换机端口号。

- **查找条目**

查找选项： 选择静态地址表的显示规则，可以快速查找到所需的条目。

- MAC：填写欲查找条目需包含的 MAC 地址信息。
- VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。
- 端口号：配置欲查找条目需包含的交换机端口号。

➢ **静态地址表**

选择： 勾选条目进行删除或修改该条目对应的交换机端口号，可多选。

MAC 地址： 显示静态绑定的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。可以在此修改与静态 MAC 地址绑定的端口，但是修改后的端口必须是 VLAN 的成员端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

注意：

- 如果地址的端口指定错误，或使用过程中端口（或设备）被人为改变，必须重新设置该静态地址表项，否则交换机将无法正确转发数据。
- 静态地址一旦被设置，如果把有此地址的网络设备连接到交换机的其它端口，交换机将不能动态识别。因此必须保证静态地址表中的表项都是正确有效的。
- 凡是加入到静态地址表的地址，不能同时加入到过滤地址表，也不能被端口动态绑定。
- 若 802.1X 模块开启，此功能禁用。

5.4.3 动态地址表

动态地址是交换机通过自动学习获取的 MAC 地址，交换机通过自动学习新的地址和自动老化掉不再使用的地址来不断更新其动态地址表。

交换机的地址表的容量是有限的，为了最大限度利用地址表的资源，交换机使用老化机制来更新地址表，即：系统在动态学习地址的同时，开启老化定时器，如果在老化时间内没有再次收到相同地址的报文，交换机就会把该 MAC 地址从表项删除。

在本页可以配置交换机的动态地址表功能。

进入页面的方法：二层交换>>地址表管理>>动态地址表

图 5-15 动态地址表

条目介绍：

- **老化配置**

自动老化： 选择是否启用自动老化。

老化时间： 填写地址老化时间。默认为 300 秒。

- **查找条目**

查找选项： 选择动态地址表的显示规则，可以快速查找到所需的条目。

- MAC：填写欲查找条目需包含的 MAC 地址信息。
- VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。
- 端口号：选择欲查找条目需包含的交换机端口号。
- LAG ID：选择欲查找条目需包含的 LAG ID。

- **动态地址表**

选择： 勾选动态地址条目进行删除或将该条目绑定为静态地址，可多选。

MAC 地址： 显示动态绑定的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

绑定： 将动态绑定的地址条目转化为静态绑定。

说明：

- 老化时间过长会导致交换机的地址表中保存过多过时的地址表项，从而耗尽地址表的资源，导致交换机无法根据网络的变化更新地址表。老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。建议使用默认值。

5.4.4 过滤地址表

通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤，过滤地址不会被老化，只能手工进行添加和删除。在过滤地址表中添加受限的 MAC 地址后，交换机将自动过滤掉源/目的地址为这个地址的帧，以达到安全的目的。过滤地址表中的地址对所有的交换机端口都生效。

进入页面的方法：二层交换>>地址表管理>>过滤地址表

图 5-16 过滤地址表

条目介绍：

- **新建条目**

  MAC 地址： 填写过滤的 MAC 地址。

  VLAN ID： 填写 MAC 地址条目对应的 VLAN ID。

- **查找条目**

  查找选项： 选择过滤地址表的显示规则，可以快速查找到所需的条目。
  - MAC：填写欲查找条目需包含的 MAC 地址信息。
  - VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。

- **过滤地址表**

  选择： 勾选过滤地址条目进行删除，可多选。

  MAC 地址： 显示过滤的 MAC 地址。

  VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

  端口： 此处为"--"，表示无指定端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

注意：

- 已加入到过滤地址表中的地址不能被加入到静态地址表中，也不能被端口动态绑定。
- 若 802.1X 模块开启，此功能禁用。

5.4.5 MAC 通知配置

MAC 通知功能用于监视 MAC 地址表的状态，以及在每个端口上学习的 MAC 地址。

进入页面的方法：二层交换→地址表管理→MAC 通知配置

以下的条目会显示在这个屏幕上：

- **全局配置**

全局配置: 全局启用/禁用 MAC 通知。

满表通知: 当 MAC 地址表满时，启用/禁用 MAC 地址表满的通知。

通知间隔: 指定通知之间的间隔时间。它的范围从 1 到 1000 秒，默认时间间隔为 1 秒。

- **端口配置**

选择: 选择指定的端口(s)配置。它是多选的。

端口: 显示端口号。

学习模式更改: 启用/禁用在端口上的学习模式更改通知。该端口的学习模式包括:动态、静态和永久。

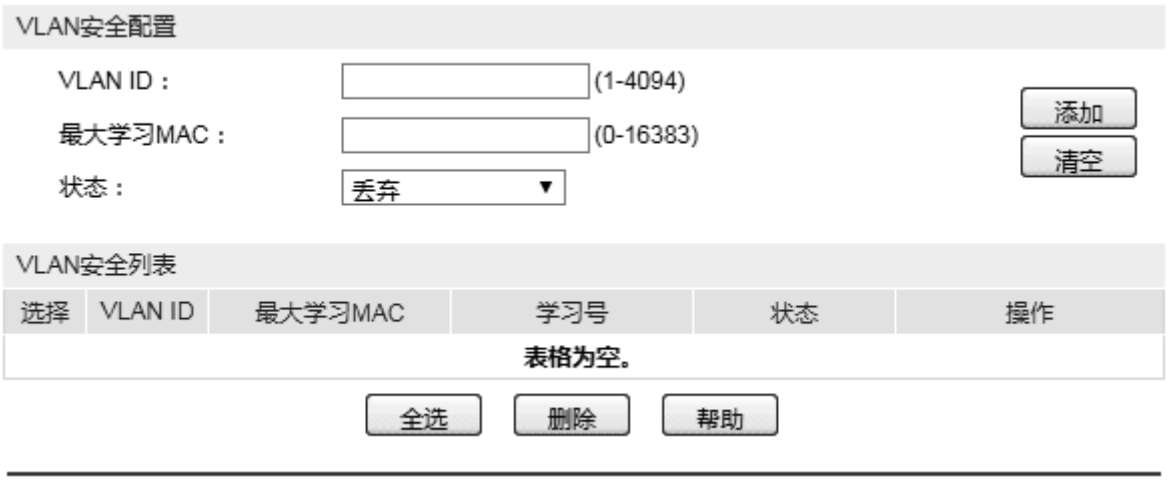
超过学习的最大数量: 启用/禁用在端口上的超过最大数的学习通知。默认情况下，每个端口上最多的 MAC 地址是 64。

新学习的 MAC: 启用/禁用在端口上的新学习的 MAC 通知。

5.4.6 MAC VLAN 安全

MAC VLAN 安全功能用于在指定的 VLAN 中配置 MAC 地址安全。

进入页面的方法：二层交换→地址表管理→MAC VLAN 安全



以下的条目会显示在这个屏幕上：

- **VLAN 安全配置**

VLAN ID: 输入 VLAN ID 来配置它的 MAC 地址安全。

最大学习 MAC 数: 指定在这个 VLAN 中可以学习的最大 MAC 地址数。

状态: 选择对新数据包的处理方法（其源 MAC 地址不在当前 VLAN 地址表中）。当学习 MAC 数量超过 VLAN 安全项的最大学习 MAC 数量。

• 丢弃：当学习的 MAC 数量超过 VLAN 安全项的最大学习数量时，数据包将被丢弃。

• 转发：当学习的 MAC 数量超过 VLAN 安全项的最大学习数量时，数据包被转发，但不会被学习。

• 禁用：VLAN 安全条目存在，但不会生效。

- **VLAN 安全列表**

选择: 选择一个或多个条目进行删除。

VLAN ID:	显示 VLAN 安全条目的 VLAN ID。
最多学习的 MAC 数量:	显示 VLAN 安全条目下的最大 MAC 数。
学习号:	:显示 VLAN 安全条目下的学习 MAC 数量。
状态:	显示 VLAN 安全条目的模式。
操作:	点击可编辑最大学习的 MAC 数和模式。

5.5 L2TP

L2TP(第二层隧道协议)是一个对服务提供者的功能，可以跨不同的 ISP 网络传输数据包并维护每个客户的第二层协议配置。支持的二层协议有 STP(生成树协议)，GVRP(GARP VLAN 注册协议)，CDP(思科发现协议)，VTP(VLAN 中继协议)，PAgP(端口聚合协议)，UDLD(单向链接检测)和 PVST+（每个 VLAN 生成树+)。

当启用 L2TP 并且交换机接收到从 UNI 端口来的特定的第 2 层协议数据包时，交换机会用特殊的 MAC 地址封装这些包并通过 NNI 端口跨不同的服务提供者来发送他们。ISP 网络中的设备不处理这些数据包，而是将它们转发为正常的数据包。ISP 网络的外端交换机接收到 NNI 端口上的这些数据包，并将其 MAC 地址恢复到原来的第二层协议目的地 MAC 地址。

L2TP 协议通常是使用 VLAN VPN 功能。因此，连接到 ISP 网络的 NNI 端口被配置为 VPN 连接端口。

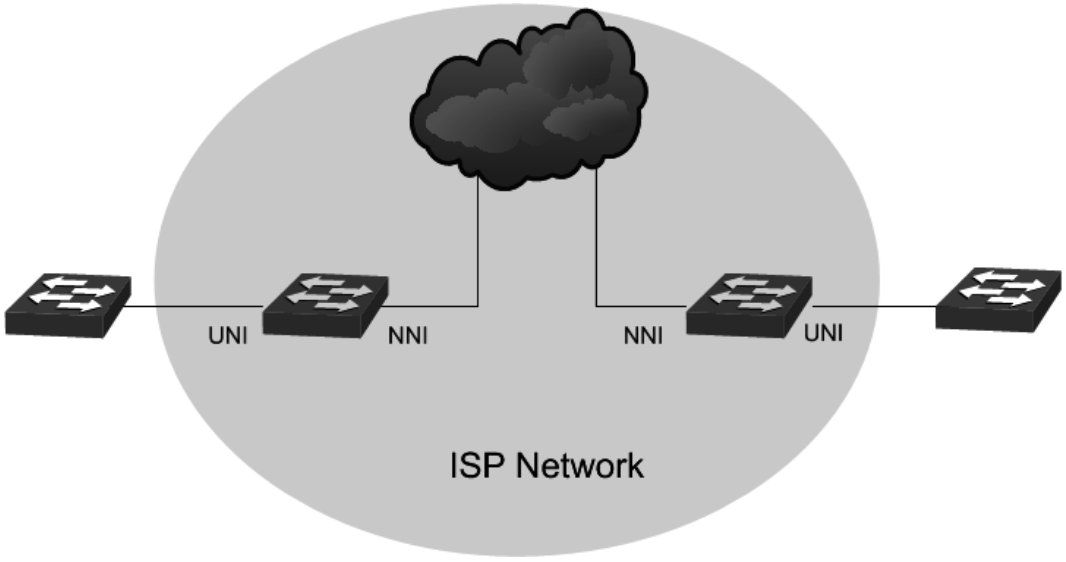


图 5-1 A 典型 L2TP 拓扑

5.5.1 L2TP Config

进入页面的方法：二层交换→L2TP→L2TP 配置

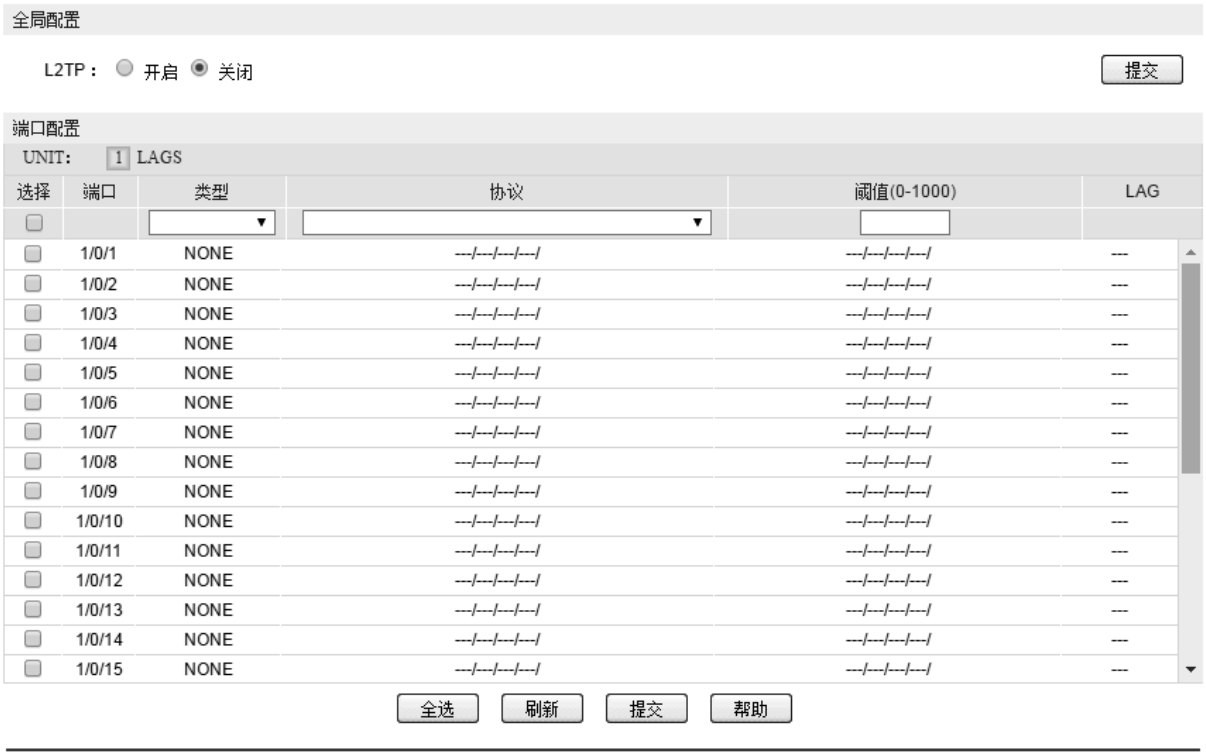


图 5-2 L2TP 配置

配置步骤:

1) 在**全局配置**下使能全局第二层隧道协议。
2) 在**端口配置**下配置隧道和协议类型。
3) 单击**应用**保存您的配置。

条目解释:

UNIT:1/LAGS: 单击 **1** 配置物理端口。单击 **LAGS** 配置链接聚合组。

选择: 指定端口来配置其 L2TP 特性。它是多选的。

类型: 根据网络中的连接设备选择端口类型。

- 没有:在这个端口禁用 L2TP。
- UNI:指定端口的类型作为 UNI，如果是连接到用户的本地网络。
- NNI:指定端口的类型作为 NNI，如果是连接到 ISP 网络。

协议: 选择支持 2 层协议的类型。在发送到 ISP 网络之前，指定协议的包将被封装在目标 MAC 地址中。在发送到客户网络之前，数据包将被解封装，以恢复他们的 2 层协议和 MAC 地址。

- STP:使能协议隧道 STP 的数据包。
- GVRP:使能 GVRP 包的协议隧道。

- 01000CCCCCCC:对于目的地 MAC 地址为 01000CCCCCCC，包括 CDP，VTP PAgP，UDLD，使能协议数据包的隧道
- 01000CCCCCCD:对于 PVST +包，使能协议隧道。
- 所有: 支持所有上述第二层隧道协议。

阈值: 配置可以接受封装的每秒发包数。超过阈值的数据包将被丢弃。如果没有指定协议，则阈值将应用于每一种 2 层协议类型。

LAG: 显示端口的聚合组。

第6章 VLAN

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现 LAN 互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network）技术，这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文被限制在一个 VLAN 内。同一个 VLAN 内的主机通过传统的以太网通信方式进行报文的交互，而不同 VLAN 内的主机之间则需要通过路由器或三层交换机等网络层设备进行通信。如图 6-1 所示。

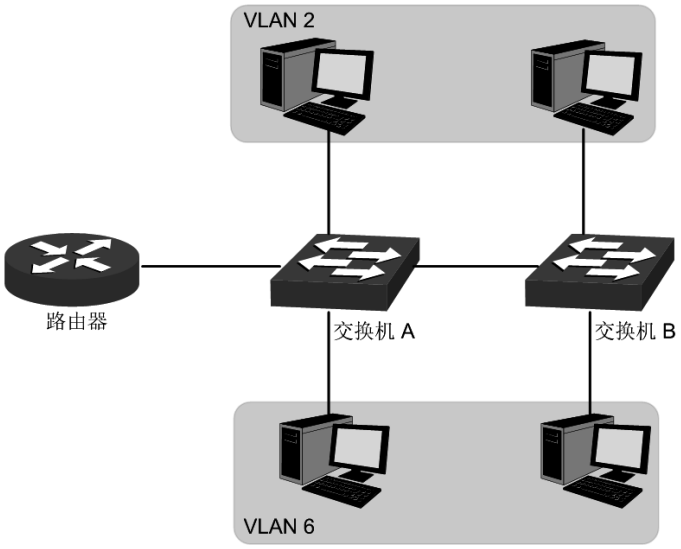


图 6-1 VLAN 示意图

VLAN 的优点如下：

1) 提高网络性能。将广播包限制在 VLAN 内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。

2) 增强网络安全。不同 VLAN 的设备不能互相访问，不同 VLAN 的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

3) 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

VLAN 的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机。本交换机支持的 VLAN 划分方式包括 802.1Q VLAN、MAC VLAN 和协议 VLAN 三种。MAC VLAN 和协议 VLAN 仅对 untag 数据包和优先级 tag 数据包生效，当一个数据包同时满足 802.1Q VLAN、MAC VLAN 和协议 VLAN 时，交换机将按照 MAC VLAN、协议 VLAN、PVID 的顺序来处理数据包，在相应 VLAN 中转发数据包。

6.1 802.1Q VLAN

由于普通交换机工作在 OSI 模型的数据链路层，若要交换机能够识别不同 VLAN 的数据包，只能对数据包的数据链路层封装进行 VLAN 识别。因此，VLAN 识别字段被添加到数据链路层封装中。

IEEE 802.1Q 协议为了标准化 VLAN 实现方案，对带有 VLAN 标识的数据包结构进行了统一规定。协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息，如图 6-2 所示。VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

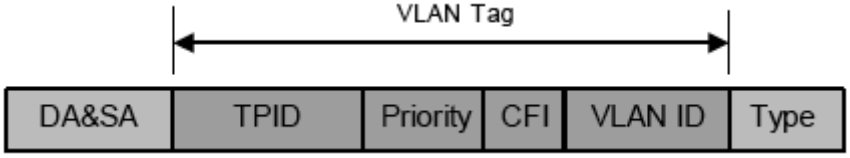


图 6-2 VLAN Tag 组成字段

1) TPID：用来表示本数据帧是带有 VLAN Tag 的数据。该字段长度为 16bit。协议规定的缺省取值为 0x8100。

2) Priority：用来表示数据包的传输优先级。

3) CFI：以太网交换机中，CFI 总被设置为 0。由于兼容特性，CFI 常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧 CFI 设置为 1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。

4) VLAN ID：用来标识该报文所属 VLAN 的编号。该字段长度为 12bit，取值范围为 0~4095。由于 0 和 4095 通常不使用，所以 VLAN ID 的取值范围一般为 1~4094。VLAN ID 简称 VID。

交换机利用 VLAN ID 来识别报文所属的 VLAN，当接收到的数据包不携带 VLAN Tag 时，交换机会为该数据包封装带有接收端口缺省 VLAN ID 的 VLAN Tag，将数据包在接收端口的缺省 VLAN 中进行传输。

本手册中，对包含 VLAN Tag 字段的数据包我们简称为 tag 帧，untag 帧指数据包中没有 VLAN Tag 字段的数据包，优先级 tag 帧指数据包中有 VLAN Tag 字段，但 VLAN ID 为 0 的数据包。

- **端口的三种链路类型**

在创建 802.1Q VLAN 时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

1) ACCESS：端口只能属于 1 个 VLAN，出口规则为 UNTAG，多为连接用户终端设备的端口。当 ACCESS 类型端口加入了其它 VLAN 时，则自动退出原有 VLAN。

2) TRUNK：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，常用于网络设备之间级连。在网络中 VLAN 经常跨接在不同交换机上，TRUNK 类型端口的出口规则为 TAG，能够保证转发各种 VLAN 的数据包时不改变其携带的 VLAN 信息。

3) GENERAL：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于网络设备之间连接，也可以用于连接用户设备。GENERAL 类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

- **PVID 与 VLAN 数据包处理关系**

PVID（Port VLAN ID），就是端口的缺省 VID。当交换机的端口接收到的报文不带 VLAN Tag 时，交换机会根据接收端口的 PVID 值为该报文插入 VLAN Tag，并进行转发。

当在局域网中划分 VLAN 时，PVID 是每个端口的一个重要参数，表示端口默认所属的 VLAN。它有两个用途：

1) 当端口收到 untag 报文时，将根据 PVID 为数据包插入 VLAN Tag。

2) PVID 指定了端口的默认广播域，即当端口接收到 UL 包或广播包的时候，交换机将这些数据包在该端口的缺省 VLAN 内广播。

端口的链路类型本质上是交换机对出入端口的 VLAN Tag 的处理方式，详细规则如表 6-1 所示。

<table>
<tr><td rowspan="2">端口类型</td><td colspan="2">对接收报文的处理</td><td rowspan="2">发送报文时的处理</td></tr>
<tr><td>报文不带 Tag</td><td>报文带 Tag</td></tr>
<tr><td>Access</td><td rowspan="3">接收报文，并为报文添加缺省的 VLAN Tag 即输入端口的 PVID。</td><td>当 VID＝端口 PVID，接收报文。
当 VID≠端口 PVID，丢弃报文。</td><td>去掉 Tag 后，发送报文。</td></tr>
<tr><td>Trunk</td><td rowspan="2">当 VID 属于端口允许通过的 VLAN ID 时，接收报文。
当 VID 不属于该端口允许通过的 VLAN ID 时，丢弃报文。</td><td>保持原有 Tag 发送报文。</td></tr>
<tr><td>General</td><td>当出口规则配置为 TAG 时，保持原有 tag 发送报文。
当出口规则配置为 UNTAG 时，去 tag 后发送报文。</td></tr>
</table>

表 6-1 端口类型与 VLAN 数据处理关系

IEEE 802.1Q VLAN 功能包括 **VLAN 配置**、**端口配置**两个配置页面。

6.1.1 VLAN 配置

在 VLAN 配置页面中可以查看当前已经创建的 802.1Q VLAN。

进入页面的方法：**VLAN>>802.1Q VLAN>>VLAN 配置**

图 6-3 查看 VLAN 列表

在缺省情况下，为了保证交换机在出厂情况下能正常通信，所有端口的缺省 VLAN 均为 VLAN1，只有属于 VLAN1 的端口才能访问交换机 Web 页面。VLAN1 无法编辑和删除。

条目介绍：

- **VLAN 配置列表**

选择： 勾选条目进行删除，可多选。

VLAN ID： 显示 VLAN ID。

名称： 显示 VLAN 的描述信息。

成员： 显示 VLAN 的端口成员。

操作： 对单个 VLAN 条目进行相应操作。

- 编辑：修改 VLAN 配置。
- 查看：查看 VLAN 配置信息。

点击<编辑>按键，可以对相应的 VLAN 进行编辑。点击<新建>按键，可以创建新的 VLAN。

图 6-4 创建或编辑 802.1Q VLAN

条目介绍：

- **VLAN 配置**

VLAN ID： 填写 VLAN ID。

VLAN 名称： 填写 VLAN 的描述信息，以便区分各个 VLAN 的用途。

6.1.2 端口配置

在创建 802.1Q VLAN 时，需要对端口连接的设备进行了解，以便设置各端口的参数。

进入页面的方法：**VLAN>>802.1Q VLAN>>端口配置**

图 6-5 802.1Q VLAN—端口配置

条目介绍：

- **VLAN 端口配置**

选择： 勾选端口配置端口类型和 PVID 值，可多选。

端口： 显示交换机的端口号。

端口类型： 选择交换机的端口类型。默认为 ACCESS。

- ACCESS：该端口只能加入一个 VLAN，出口规则为 UNTAG。PVID 值与当前 VLAN ID 的值保持相同。如果 VLAN 删除，相应端口的 PVID 会自动置为默认值 1。
- TRUNK：该端口可加入多个 VLAN，出口规则为 TAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。
- GENERAL：该端口可加入多个 VLAN，且允许根据不同 VLAN 选择不同的出口规则，默认出口规则为 UNTAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。

PVID： 填写交换机物理端口的 PVID 值。默认为 1。

LAG： 显示端口当前所属的汇聚组。

所属 VLAN： 查询本端口所加入的 VLAN 信息。

点击<查询>按键，可以查询相应端口所属。

图 6-6 查看端口所属 VLAN

条目介绍：

- **端口加入的 VLAN**

VLAN ID： 显示 VLAN ID。

名称： 显示 VLAN 的名称信息。

从该 VLAN 移除： 点击<移除>按键，将本端口从相应 VLAN 中移除。

802.1Q VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	编辑/查看 VLAN	可选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面点击<编辑>或<查看>按键，可以对相应的 VLAN 进行编辑和查看。
4	删除 VLAN	可选操作。在**VLAN>>802.1Q VLAN>>VLAN 配置**页面勾选相应的VLAN条目，点击<删除>按键进行删除。

6.2 MAC VLAN

MAC VLAN是VLAN的另一种划分方法，根据每个主机的MAC地址来划分VLAN，即对每个主机的MAC地址均划分到VLAN中。MAC VLAN的优点在于，将MAC地址与VLAN绑定后，该MAC地址对应的设备可以随意切换端口，只要连接到相应VLAN的成员端口即可，而不必改变VLAN成员的配置。

MAC VLAN 中数据包处理有如下特点：

1. 当端口收到 UNTAG 数据包时，首先查看是否创建配置相应的 MAC VLAN，若已创建 MAC VLAN，则给数据包插入 MAC VLAN 的 TAG；若没有相应的 MAC VLAN，则根据接收端口的 PVID 值给数据包插入 TAG，并将数据包在相应的 VLAN 中转发。
2. 当端口收到 TAG 数据包时，交换机按照 802.1Q VLAN 的方式处理该帧。如果接收端口允许该 VLAN 的数据包通过，则正常转发；如果不允许，则丢弃该数据包。

3. 将某个主机的 MAC 划分到 802.1Q VLAN 中后，为了保证该主机能够在此 VLAN 内正常通信，请将其接入端口设置成相应的 802.1Q VLAN 成员。详情请查看表 6-1 端口类型与 VLAN 数据处理关系。

6.2.1 MAC VLAN

在 MAC VLAN 页面中，可以创建 MAC VLAN 并查看当前已创建的 MAC VLAN。

进入页面的方法：**VLAN>>MAC VLAN>>MAC VLAN**

图 6-7 创建并查看 MAC VLAN

条目介绍：

- **MAC VLAN 配置**

  MAC 地址： 输入 MAC 地址。

  MAC 描述： 输入对 MAC 地址的描述，以便区分各个 MAC 的用途。

  VLAN ID： 输入该 MAC VLAN 对应的 VLAN ID，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

- **MAC VLAN 列表**

  选择： 勾选条目进行删除，可多选。

  MAC 地址： 显示 MAC 地址。

  MAC 描述： 显示此 MAC 的描述信息，以便区分各个 MAC 的设备。

  VLAN ID： 显示该 MAC 对应的 VLAN ID。

  操作： 点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

MAC VLAN 配置步骤：

步骤	操作	说明

1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面结合实际网络结构设置端口链路类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	创建 MAC VLAN	必选操作。在 **VLAN>>MAC VLAN>>MAC VLAN** 页面创建 MAC VLAN。创建了 MAC VLAN 后，对应 MAC 地址的设备在交换机上的连接端口也必须是 VLAN 成员，才能保证正常通信。

6.2.2 端口启用

在端口启用页面中，您可以启用端口的 MAC VLAN 功能，只有启用了端口的 MAC VLAN 功能，MAC VLAN 功能才能生效。

进入页面的方法：**VLAN→MAC VLAN→端口使能**。

图 6-1 开启 MAC VLAN 端口

➢ **配置过程**

UNIT:单击 1 以配置物理端口。单击 LAGS 配置链路聚合组。

选择您想要设为 MAC VLAN 的端口。默认情况下，所有端口都禁用了 MAC VLAN 的功能。

步骤	操作	描述
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面结合实际网络结构设置端口链路类型。
2	创建 VLAN.	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN** 配置页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	创建 MAC VLAN.	必选操作。在 **VLAN>>MAC VLAN>>MAC VLAN** 页面创建 MAC VLAN。创建了 MAC VLAN 后，对应 MAC 地址的设备在交换机上的连接端口也必须是 VLAN 成员，才能保证正常通信。
4	选择您要启用 MAC	必选操作。在 **VLAN>>MAC VLAN>>端口使能**页面中，选择和启用

步骤	操作	描述
	VLAN 的端口	端口的 MAC VLAN 功能。

6.3 协议 VLAN

协议VLAN是按照网络层协议来划分VLAN，可将网络中应用的服务类型与协议VLAN进行绑定，并实现特定目标。通过配置协议VLAN，交换机可以对端口上收到的未携带VLAN Tag 的报文进行分析，根据不同的封装格式及特殊字段的数值将报文与用户设定的协议模板相匹配，为匹配成功的报文添加相应的VLAN Tag，实现将属于指定协议的数据自动分发到特定的VLAN 中传输的功能。对于希望针对具体应用和服务来管理用户的网络管理员，可通过划分协议VLAN来进行管理。

➢ **以太网数据封装格式**

为清楚地了解交换机对报文协议的识别过程，先简略介绍以太网常用的数据封装格式。目前以太网的报文封装主要有两种，分别为Ethernet II封装和802.2/802.3封装，两种报文的封装格式如下：

- Ethernet II封装

- 802.2/802.3封装

DA、SA 分别表示报文的目的 MAC 地址和源 MAC 地址，数字表示此字段的长度，单位为字节，如源目的 MAC 地址字段共占用了 12 字节。

由于以太网报文的最大长度为 1500 字节，转换成 16 进制数字为 0x05DC，所以 802.2/802.3 封装的 Length 字段取值范围为 0x0000～0x05DC。而 Ethernet II 型封装中的 Type 字段取值范围为 0x0600～0xFFFF。Type 或 Length 字段取值为 0x05DD～0x05FF 的报文将被认为是非法报文，交换机将直接丢弃。交换机根据这两个字段的取值范围的不同来区分 Ethernet II 型和 802.2/802.3 型报文。

802.2/802.3 封装有 3 种扩展封装格式：

- 802.3 raw封装

在源地址和目的地址之后只封装 Length 字段，之后即是 DATA，没有其他字段。目前只有 IPX 协议支持 802.3 raw 封装。802.3 raw 封装在 Length 字段后两个字节的取值固定为 0xFFFF。

- 802.2 LLC（Logic Link Control，逻辑链路控制）封装

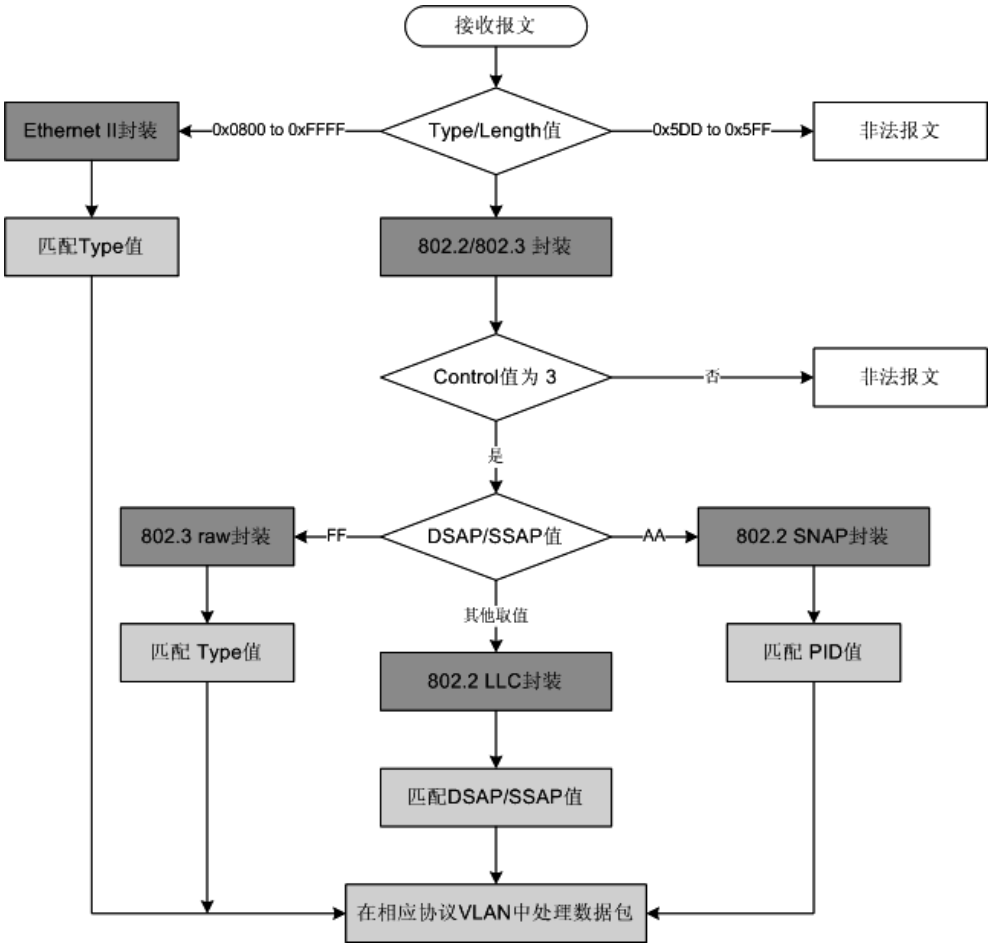
在源、目的地址后封装 Length、DSAP（Destination Service Access Point，目的服务访问点）、SSAP（Source Service Access Point，源服务访问点）和 Control 字段，其中 Control 字段的取值固定为 3。802.2 LLC 封装中的 DSAP 和 SSAP 是用来标识上层协议类型的字段。例如，当两个字段同时取值为 0xE0 时，表示上层协议为 IPX。

- 802.2 SNAP（Sub-Network Access Protocol，子网接入协议）封装按802.3标准型报文进行封装。在802.2 SNAP封装中，DSAP和SSAP字段的取值均固定为0xAA，Control字段取值为3。交换机根据DSAP和SSAP字段的取值区分802.2 LLC和802.2 SNAP封装。

以太网报文到底采用哪种封装格式，取决于发送该报文的设备，同一个设备可能可以同时发送两种格式的报文。目前最常使用的封装格式是 Ethernet II 封装格式。

IP 协议、ARP 协议、和 RARP 协议均支持 802.3 和 Ethernet II 两种报文封装格式，但是并非所有协议都支持上述所有封装格式。交换机通过匹配两种封装类型的特征值来区分报文所属的协议。

➢ **交换机对报文协议的匹配规则**



➢ **交换机协议VLAN的实现方式**

本交换机可以通过协议模板来匹配报文，根据协议在指定的VLAN中传输报文。协议模板是用来匹配报文所属协议类型的标准，包括“封装格式”和“协议类型”两部分。在创建协议VLAN前需要设定相应的协议模板。表 6-2是常见网络层协议支持的封装格式，设置协议模板可以参考。同时交换机也预设的部分协议模板，可以直接根据相应的协议模板创建协议VLAN。

封装 / 协议	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP
IP（0x0800）	支持	不支持	不支持	支持

IPX（0x8137）	支持	支持	支持	支持
AppleTalk（0x809B）	支持	不支持	不支持	支持

表 6-2 常见协议支持的封装格式

- **本交换机对各种VLAN数据包处理特点**

1. 当端口收到UNTAG数据包时，首先查看是否创建配置相应的协议VLAN，若已创建协议VLAN，则给数据包插入协议VLAN的TAG；若没有相应的协议VLAN，则根据接收端口的PVID值给数据包插入TAG，并将数据包在相应的VLAN中转发。
2. 当端口收到TAG数据包时，交换机按照802.1Q VLAN的方式处理该帧。如果接收端口属于携带该VLAN TAG的数据包通过，则正常转发；如果不属于，则丢弃该数据包。
3. 创建了协议VLAN后，为了保证数据的正常传输，请将协议VLAN的使能端口设置为相应802.1Q VLAN成员。详情请查看表 6-1 端口类型与VLAN数据处理关系。

6.3.1 协议组列表

在协议组列表页面中，可以查看、创建或编辑协议VLAN。

进入页面的方法：**VLAN>>协议 VLAN>>协议组列表**

图 6-8 协议组列表

条目介绍：

- **协议 VLAN 列表**

选择： 勾选条目进行删除，可多选。

协议类型： 显示协议 VLAN 的协议类型。

VLAN ID： 显示协议 VLAN ID。

成员： 显示协议 VLAN 成员端口。

操作： 点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

点击<新建>按钮，可以创建新的协议 VLAN。

6.3.2 协议组配置

在此页面中，可以修改相应的协议VLAN。

进入页面的方法：VLAN>>协议 VLAN>>协议组配置

图 6-9 协议组配置

条目介绍：

- **协议组配置**

  协议类型： 选择需要修改的协议 VLAN 类型。

  VLAN ID： 配置协议 VLAN ID。

- **协议组成员**

  端口选择： 勾选协议 VLAN 成员端口，将成员端口与协议 VLAN 进行关联。设置了协议 VLAN 成员端口后，当这些端口收到 Untag 数据包时，将优先判断是否存在相应的协议 VLAN。若存在，则将数据包在相应的协议 VLAN 中转发数据包；若不存在，则将数据包按照 802.1Q VLAN 规则进行转发。

注意：

- 协议 VLAN 成员端口需要匹配报文的协议来为各种报文封装不同的 VLAN Tag，则需要属于多个 VLAN。而且，在协议 VLAN 的情况下，由于该端口连接客户端，所以该端口出口规则要设置为 Untag。综上所述，设置协议 VLAN 成员端口前，请将端口配置为 GENERAL 端口，并配置该端口在转发来自协议 VLAN 的报文时出口规则为 Untag。

6.3.3 协议模板

配置协议VLAN前应先配置协议模板，本交换机在出厂默认情况下已经定义了IP、ARP和RARP等协议模板，若需要更多的协议模板时，请在此页面中添加。

进入页面的方法：**VLAN>>协议 VLAN>>协议模板**

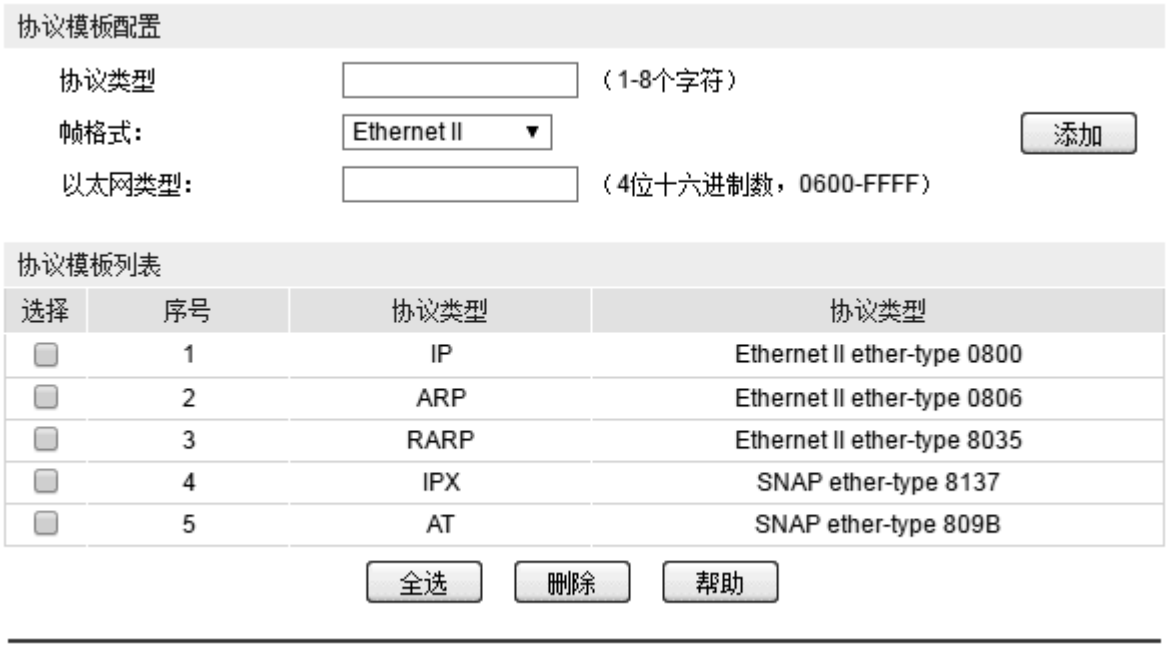


图 6-10 协议模板

条目介绍：

- **协议模板配置**

  协议类型： 配置新定义的协议模板的名称。

  以太网类型： 配置该协议模板中协议类型值。

  帧格式： 配置该协议使用的封装格式。

- **协议模板列表**

  选择： 勾选条目进行删除，可多选。

  序号： 显示协议序号。

  协议类型： 显示协议模板的名称。

  协议类型： 显示该协议模板中协议类型值。

注意：

- 当协议模板与 VLAN 绑定后，将无法删除协议模板。

协议 VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 VLAN>>802.1Q VLAN>>端口配置页面结合实际网络结构设置端口链路类型。协议 VLAN 成员端口的在协议 VLAN 中出口规则需要设置为 Untag。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，

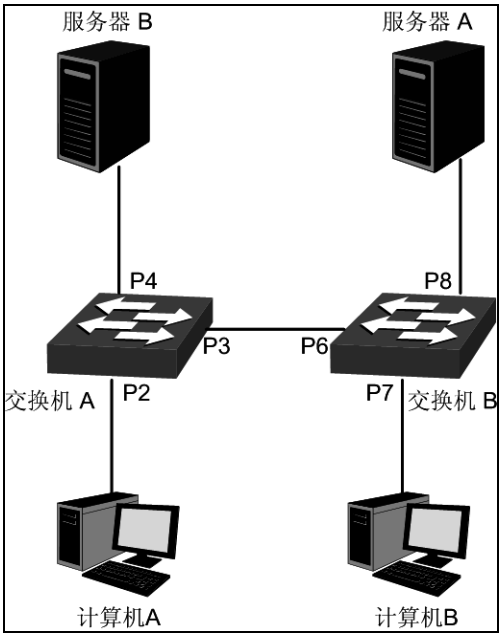
步骤	操作	说明
		在此页面中请同时勾选 VLAN 包含的端口。
3	创建协议模板	必选操作。配置协议 VLAN 前应先在 VLAN>>协议 VLAN>>协议模板页面配置协议模板。
4	创建协议 VLAN	必选操作。在 VLAN>>协议 VLAN>>**协议组列表**页面中点击<新建>按键来创建协议 VLAN。
5	编辑/查看 VLAN	可选操作。在 VLAN>>协议 VLAN>>**协议组列表**页面点击<编辑>按键对相应的 VLAN 进行编辑。
6	删除 VLAN	可选操作。在 VLAN>>协议 VLAN>>**协议组列表**页面勾选相应的 VLAN 条目，点击<删除>按键进行删除。

6.4 802.1Q VLAN 功能的组网应用

- **组网需求**

- 交换机 A 连接了计算机 A 和服务器 B；
- 交换机 B 连接了计算机 B 和服务器 A；
- 计算机 A 和服务器 A 同属于一个部门；
- 计算机 B 和服务器 B 同属于一个部门；
- 两个部门以 VLAN 划分，相互之间不能通信。

- **组网图**



图中的“P 数字”表示交换机的端口号。

➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 2 的类型为 ACCESS；设置端口 3 的类型为 TRUNK；端口 4 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 2 和端口 3。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 3 和端口 4。

- 配置交换机 B：

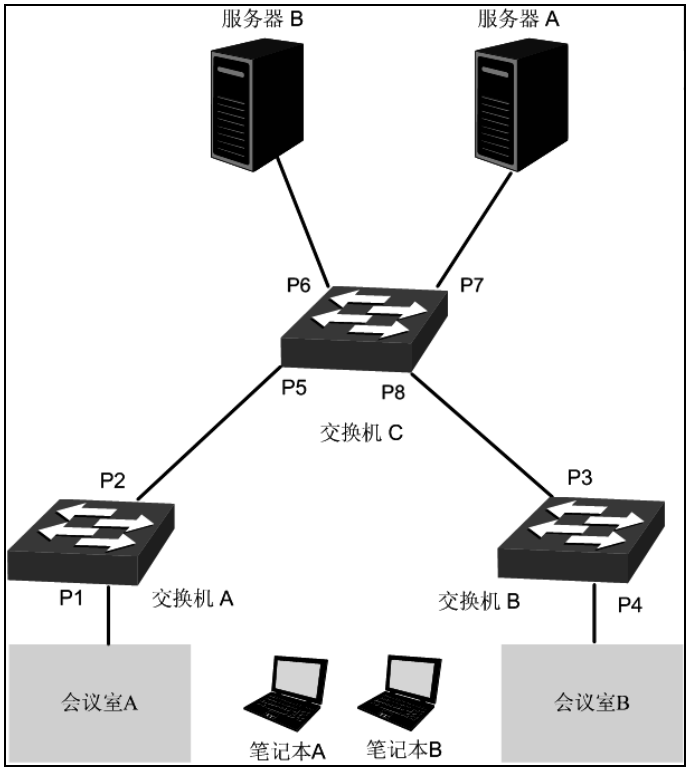
步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 7 的类型为 ACCESS；设置端口 6 的类型为 TRUNK；端口 8 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 6 和端口 8。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 6 和端口 7。

6.5 MAC VLAN 功能的组网应用

➢ **组网需求**

- 交换机 A 和交换机 B 分别连接到两个会议室，会议室为各部门共用；
- 笔记本 A 和笔记本 B 为会议室专用电脑，分别属于不同部门；
- 两个部门分别属于 VLAN10 和 VLAN20。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即服务器 A 和服务器 B；
- 笔记本 A 和笔记本 B 的 MAC 地址分别为 00-19-56-8A-4C-71、00-19-56-82-3B-70。

➢ **组网图**



图中的“P 数字”表示交换机的端口号。

➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 1 的端口类型为 GENERAL，端口 2 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 1 和端口 2，端口 1 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 1 和端口 2，端口 1 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 VLAN>>MAC VLAN 页面创建 MAC VLAN10，关联的 MAC 地址为 00-19-56-8A-4C-71。
5	设置 MAC VLAN 20	在 VLAN>>MAC VLAN 页面创建 MAC VLAN20，关联的 MAC 地址为 00-19-56-82-3B-70。

- 配置交换机 B：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 4 的端口类型为 GENERAL，端口 3 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 3 和端口 4，端口 4 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 3 和端口 4，端口 4 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 VLAN>>MAC VLAN 页面创建 MAC VLAN10，关联的 MAC 地址为 00-19-56-8A-4C-71。
5	设置 MAC VLAN 20	在 VLAN>>MAC VLAN 页面创建 MAC VLAN20，关联的 MAC 地址为 00-19-56-82-3B-70。

- 配置交换机 C：

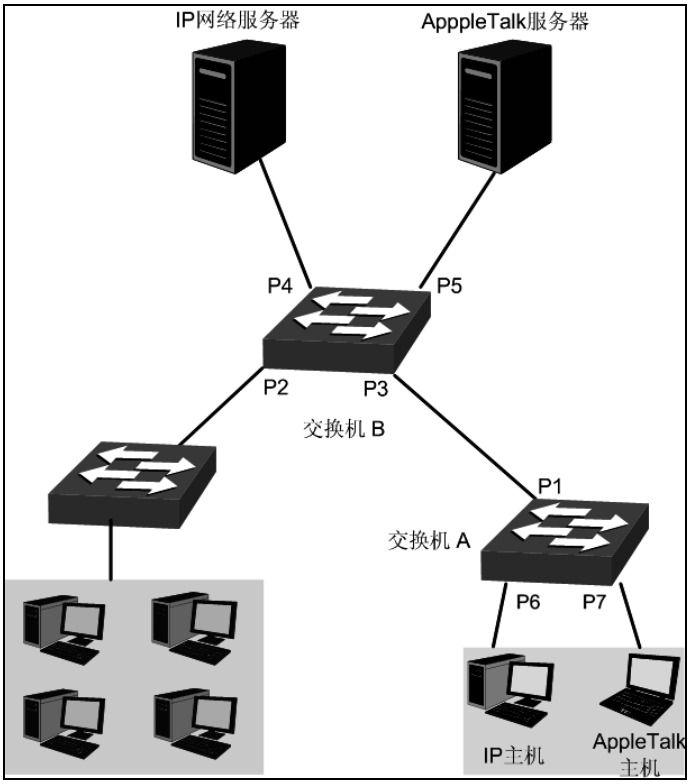
步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 5 和端口 8 的端口类型为 GENERAL，端口 6 和端口 7 的端口类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 5、端口 7 和端口 8。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 4、端口 7 和端口 8。

6.6 协议 VLAN 功能的组网应用

➢ **组网需求**

- 平面部门通过内部交换机 A 的端口 1 连入公司局域网；
- 平面部门中分别有 IP 主机和 AppleTalk 主机；
- IP 主机需要 IP 网络服务器提供服务，属于 VLAN10；AppleTalk 主机需要 AppleTalk 服务器提供服务，属于 VLAN20；
- 交换机 A 分别连接了 IP 网络服务器和 AppleTalk 网络服务器；

➢ **组网图**



图中的“P 数字”表示交换机的端口号。

➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 6 和端口 7 的端口类型为 ACCESS，端口 1 的端口类型为 GENERAL。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 1 和端口 6，端口 1 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 1 和端口 7，端口 7 的出口规则设置为 Untag。

- 配置交换机 B：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 4 和端口 5 的端口类型为 ACCESS，端口 3 的端口类型为 GENERAL。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 3 和端口 4，端口 3 的出口规则设置为 Tag。

步骤	操作	说明
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 3 和端口 5，端口 3 的出口规则设置为 Tag。
4	创建协议模板	必选操作。此处请根据实际情况在 VLAN>>协议 VLAN>>协议模板页面配置协议模板。例如 IP 网络数据包以 Ethernet II 类型封装，Ether Type 字段为0800；AppleTalk 网络数据包以 SNAP 类型封装，PID 字段为809B。
5	设置协议 VLAN 10	在 VLAN>>协议 VLAN>>**协议组列表**页面中点击<新建>按键来创建协议 VLAN10，关联 IP 协议，并勾选成员端口 3。
6	设置协议 VLAN 20	在 VLAN>>协议 VLAN>>**协议组列表**页面中点击<新建>按键来创建协议 VLAN20，关联 AppleTalk 协议，并勾选成员端口 3。

6.7 VLAN VPN

VLAN VPN（虚拟私有网络）是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。VLAN-VPN 通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag， 穿越运营商的骨干网络。

VLAN-VPN 功能为您提供了以下好处:

1) 为小型局域网或企业内部网提供了简单的二层 VPN 解决方案。

2) 节约公用网络 VLAN ID 资源。

3) 用户可以规划自己的私网 VLAN ID，不会导致和公网 VLAN ID 冲突。

4) 当 ISP 进行网络升级时，用户网络可以在不改变当前配置的情况下正常工作。

此外，该交换机支持调整 VLAN VPN 数据包的 TPID 值。TPID(标签协议标识符)是 VLAN Tag 中的一个字段。IEEE 802.1 Q 定义 TPID 的默认值是 0x8100。该交换机采用协议定义的 TPID 默认值（0x8100）。其他制造商可以在 VLAN-VPN 数据包的外部 tag 中使用其他 TPID 值(如 0x9100 或 0x9200)。为兼容其他厂商的设备，该交换机可以调整 VLAN-VPN 数据包的 TPID 值，您可以自己配置。当一个端口接收到一个数据包时，这个端口会将数据包的外部 VALN tag 替换成用户自己定义的 TPID 值，再重新发送数据包。因此，发送到公共网络的 VLAN-VPN 数据包可以被其他制造商的设备所识别。

以太网数据包中 TPID 字段的位置与不带 VLAN tag 数据包中的协议类型字段的位置相同。因此，为了避免在交换机转发或接收数据包时发生冲突，您不能将以下表中所列的协议类型值配置为 TPID 值。

协议类型	数值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137

协议类型	数值
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表 6-1 常用的以太网帧协议类型值

本功能包括 **VPN 配置**、**端口使能**和 **VLAN 映射**三个配置页面。

6.7.1 VPN 配置

在这个页面，你可以启用/禁用 VPN 功能，调整 VLAN-VPN 数据包的全局 TPID，使能 VPN 上联端口。当 VPN 模式启用时，交换机将根据 VLAN 映射条目对接收到的有标记的数据包添加一个标记。

进入页面的方法：**VLAN→VLAN VPN→VPN配置**

图 6-2 VPN 全局配置

以下的条目显示在这个屏幕上:

- **全局配置**

  VPN 模式 选择启用/禁用 VLAN-VPN 功能。

  全局 TPID 填写全局 TPID。

- **VPN 上联端口**

  单元 单击 1 以配置物理端口。单击 LAGS 配置链路聚合组。

  VPN 上联端口 勾选端口作为 VPN 上联端口。

注意:

如果启用了 VPN 模式，请在 VLAN 映射功能页面上创建 VLAN 映射条目。

6.7.2 端口使能

在这个页面上，可以启用端口的VLAN VPN功能。只有启用了端口，VLAN映射功能的配置才能生效。

图 6-3 开启 VLAN 映射端口

- **VPN端口使能**

  UNIT 单击 1 以配置物理端口。单击 LAGS 配置链路聚合组。

勾选端口启用 VLAN VPN 功能，默认情况下所有端口都不启用 VLAN VPN 功能。

6.7.3 VLAN 映射

VLAN 映射功能将根据 VLAN 映射关系，在数据包的 VLAN tag 之前插入一个新的 VLAN tag。数据包可以在新的 VLAN 中转发。如果启用了 VLAN VPN 功能，接收到的已经携带 VLAN tag 的数据包将会基于 VLAN 映射条目再封装上一个 tag，变成双重标记的数据包，在新的 VLAN 中继续转发。

进入页面的方法：**VLAN→VLAN VPN→VLAN 映射**

图 6-4 新建 VLAN 映射端口

以下的条目显示在这个屏幕上:

- **全局配置**

VLAN 映射：	启用/禁用 VLAN 映射功能

- **VLAN 映射配置**

端口	选择或者输入端口号。
C VLAN	Customer VLAN ID（用户 VLAN ID）。
SP VLAN	Service Provider VLAN ID（服务商 VLAN ID）。
名称	配置 VLAN 映射条目名称。

- **VLAN 映射列表**

选择	勾选条目进行删除，可多选。
端口：	显示 VLAN 端口。
C_VLAN：	显示 C_VLAN 信息。
SP_VLAN：	显示 SP_VLAN 信息。
名称：	显示 VLAN 名称信息。
操作:	点击对应条目【编辑】按键，可以修改该条目的参数。修改完毕后，点击【修改】按键，修改内容生效。

单击<编辑>可以进行 VLAN 映射列表相关配置

图 6-5 VLAN 映射入口配置

注意:

当 VPN 模式全局启用时，所有端口的 VPN 功能生效。如果 VPN 模式被禁用，可以通过端口使能页面选择您想要的端口来启用 VLAN 映射功能。

VLAN VPN 功能的配置过程:

步骤	操作	描述
	启用 VPN 模式。	必选操作。在 VLAN→VLAN VPN→VPN 配置页面使能 VPN 模式。
	配置全局 TPID。	可选操作。在 VLAN→VLAN VPN→VPN 配置页面基于上联端口连接的设备，配置全局 TPID。
	设置 VPN 上联端口。	必选操作。在 VLAN→VLAN VPN→VPN 配置页面设置端口为VPN上联端口。连接到主干网络的端口需设置为上联端口。
	创建 VLAN 映射条目。	必选操作。在 VLAN→VLAN VPN→VLAN 映射页面根据实际的应用需求配置 VLAN 映射条目。
	创建 SP(服务提供者)VLAN。	可选操作。在 VLAN→802.1Q VLAN 页面创建 SP VLAN。创建 VLAN 的步骤，请参考 802.1Q VLAN 章节。

VLAN 映射功能的配置过程:

步骤	操作	描述
	创建 VLAN 映射条目。	必选操作。在 VLAN→VLAN VPN→VLAN 映射页面根据实际的应用需求配置 VLAN 映射条目。
	启用端口的 VLAN 映射功能。	必选操作。VLAN→VLAN VPN→端口使能页面使能端口的 VLAN 映射功能。
	创建 SP(服务提供者)VLAN。	可选操作。在 VLAN→802.1Q VLAN 页面创建 SP VLAN。创建 VLAN 的步骤，请参考 802.1Q VLAN 章节。

6.8 GVRP

GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。

- **GARP 简介**

GARP提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息。GARP本身不作为一个实体存在于设备中，遵循GARP协议的应用实体称为GARP应用，GVRP就是GARP的一种应用。当GARP应用实体存在于设备的某个端口上时，该端口称为GARP应用实体。

网络中的GARP应用实体之间通过传递GARP消息来完成相关的信息交换，GARP协议定义有三类消息，分别为Join消息、Leave消息和LeaveAll消息，三种消息完成相关属性信息的注册或注销。

Join消息：当一个GARP应用实体希望其它设备注册自己的属性信息时，它将对外发送Join消息；当收到其它实体的Join消息或本设备静态配置了某些属性，需要其它GARP应用实体进行注册时，它也会向外发送Join消息。

Leave消息：当一个GARP应用实体希望其它设备注销自己的属性信息时，它将对外发送Leave消息；当收到其它实体的Leave消息注销某些属性或静态注销了某些属性后，它也会向外发送Leave消息。

LeaveAll消息：每个GARP应用实体启动后，将同时启动LeaveAll定时器。当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，LeaveAll消息用来注销所有的属性，以使其它GARP应用实体重新注册本实体上所有的属性信息。

通过消息交互，所有待注册的属性信息可以传播到同一局域网中的所有GARP应用实体。

GARP消息发送的时间间隔通过定时器来控制。GARP协议定义了四种定时器，用于控制GARP消息的发送周期：

Hold定时器：当GARP应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条Join消息对外发送，而是启动Hold定时器，当该定时器超时后，GARP应用实体将此时段内收到的所有注册信息放在同一个Join消息中向外发送，从而节省带宽资源。

Join定时器：GARP应用实体可以通过将每个Join消息向外发送两次来保证消息的可靠传输，在第一次发送的Join消息没有得到回复的时候，GARP应用实体会第二次发送Join消息。两次Join消息发送之间的时间间隔用Join定时器来控制。

Leave定时器：当一个GARP应用实体希望注销某属性信息时，将对外发送Leave消息，接收到该消息的GARP应用实体启动Leave定时器，如果在该定时器超时之前没有收到Join消息，则注销该属性信息。

LeaveAll定时器：每个GARP应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，以使其它GARP应用实体重新注册本实体上所有的属性信息。随后再启动LeaveAll定时器，开始新的一轮循环。

- **GVRP 简介**

GVRP是GARP的一种应用。它基于GARP的工作机制，维护设备中的VLAN动态注册信息，并传播VLAN信息到其它设备中。

设备启动GVRP特性后，能够接收来自其它设备的VLAN注册信息，并动态更新本地的VLAN注册信息，包括当前的VLAN成员、这些VLAN成员可以通过哪个端口到达等；同时设备能够将本地的VLAN注册信息向其它设备传播，以便使同一局域网内所有设备的VLAN信息一致。GVRP传播的VLAN注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

在本交换机中，只有TRUNK类型端口才能作为GVRP应用实体，维护交换机的VLAN注册信息。GVRP的端口注册模式有三种：Normal、Fixed和Forbidden，各模式描述如下：

Normal模式：允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。

Fixed模式：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。Fixed模式的端口只允许本端口所属的静态VLAN信息通过。

Forbidden模式：禁止该端口动态注册、注销VLAN，不传播除VLAN1以外的任何的VLAN信息。Forbidden模式的端口，只允许系统默认VLAN（VLAN1）通过。

进入页面的方法：**VLAN>>GVRP>>GVRP配置**

图 6-11 配置 GVRP

注意：

- 若启用了 LAG 组成员端口的 GVRP 功能，请保持所有成员端口的状态和注册模式一致。

条目介绍：

- **全局配置**

  GVRP 功能： 选择是否启用交换机的 GVRP 功能。

- **端口配置**

端口选择： 点击<选择>按键，可根据所输端口号快速查找相应条目。

选择： 勾选端口，配置端口 GVRP 功能参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用此功能。端口启用 GVRP 功能之前需要将端口类型设置为 Trunk。

注册模式： 选择端口的注册模式。

- Normal 模式：允许该端口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed：禁止该端口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。
- Forbidden：禁止该端口动态注册、注销 VLAN，只允许缺省 VLAN 通过。

LeaveAll 定时器： 每个端口启动 GARP 后，同时启动 LeaveAll 定时器，端口将对外循环发送 LeaveAll 消息，以使其它端口重新注册其所有的属性信息。LeaveAll 定时器的取值范围为 1000-30000 厘秒。

Join 定时器： GARP 端口可以将每个 Join 数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用 Join 定时器来控制。Join 定时器的取值范围为 20-1000 厘秒。

Leave 定时器： 接收到 Leave 数据包的 GARP 端口启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 数据包，则注销相应属性信息。Leave 定时器的取值范围为 60-3000 厘秒。

LAG： 显示端口当前所属的汇聚组。

注意：

- LeaveAll 定时器值要大于等于 10 倍 Leave 定时器，Leave 定时器值要大于等于 2 倍 Join 定时器。

GVRP 配置步骤：

步骤	操作	说明
	设置端口类型	必选操作。在 VLAN>>802.1Q VLAN>>端口配置页面将端口类型设置为 TRUNK。
	启用 GVRP 功能	必选操作。在 VLAN>>GVRP 页面启用 GVRP 功能。
	配置端口的注册模式以及各定时器时长。	必选操作。在 VLAN>>GVRP 页面中根据实际应用情况设置端口的参数并启用端口。

6.9 私有 VLAN

私有 VLAN 旨在节省 VLAN 资源、防止广播风暴。为保证用户信息安全，易于服务提供商管理，在校园网络中，服务提供者通常要求每个用户是 2 层分离的，VLAN 可以解决这个问题。然而，IEEE

802.1Q 协议规定一个设备最多只能支持 4094 个 VLAN。如果一个服务提供者为每个用户分配一个 VLAN，VLAN 将远远不够，这将导致服务提供者能够支持的用户数量比较有限。

私有 VLAN 采用 2 层 VLAN 结构。私有 VLAN 包含一个主 VLAN 和一个辅助 VLAN，提供一种机制来实现不同端口的 2 层分离。对于上行设备，从下游接收到的所有数据包没有 VLAN 标记，上行设备需要识别主 VLAN 而不是辅助 VLAN。因此，它们可以在不考虑底层 VLAN 配置的情况下节省 VLAN 资源。与此同时，服务提供者可以为每个用户分配一个单独的辅助 VLAN，实现用户 2 层隔离。

私有 VLAN 技术主要用于校园或企业网络实现用户的 2 层分离和节省 VLAN 资源。

- **私有VLAN的组成**

Promiscuous端口: Promiscuous端口与上行设备连接和通信。Promiscuous端口的PVID与主VLAN ID相同，一个Promiscuous端口只能加入到一个主VLAN。

Host端口: Host端口与终端设备连接并通信。Host端口的PVID与辅助VLAN ID相同，一个Host端口只能属于一个私有VLAN。

主VLAN:一个私有VLAN包括一个主VLAN和一个辅助VLAN。主VLAN是上行设备可以识别的用户VLAN但不是终端用户所在的实际VLAN。私有VLAN中的每个端口都是主VLAN的成员。主VLAN的Promiscuous端口可以和Host端口通信，也可以和其他Promiscuous端口通信。

辅助VLAN:辅助VLAN是终端用户所在的实际VLAN。辅助VLAN与主VLAN相关联，用于从主机到上行设备的通信。辅助VLAN有两种类型:

- 隔离VLAN-与隔离端口相关联的VLAN是隔离VLAN。每个隔离VLAN必须绑定一个主VLAN。
- 团体VLAN-与团体端口相关联的VLAN是团体VLAN。每个团体VLAN必须绑定一个主VLAN。

- **私有VLAN特性**

1. 一个私有VLAN包含一个主VLAN和一个辅助VLAN。
2. 一个VLAN不能同时被设置为主VLAN和辅助VLAN。
3. 一个辅助VLAN只能加入一个私有VLAN。
4. 一个主VLAN可以与多个辅助VLAN关联，从而创建多个私有VLAN。

- **私有VLAN的实现**

为了确保从上行设备中无法看到辅助VLAN信息，并且节省VLAN资源，私有VLAN（包含一个主VLAN和一个辅助VLAN）需要以下特点:

- 从不同辅助VLAN转发的数据包可以通过Promiscuous端口发送到上行设备，并且没有辅助VLAN信息。
- 从主VLAN转发的数据包可以通过Host端口发送到终端用户，并且没有主VLAN信息。

在 PVLAN 配置和端口配置页面上实现了私有 VLAN 的功能。

6.9.1 PVLAN 配置

在这个页面上，您可以创建私有VLAN并查看当前定义的私有VLAN信息。

进入页面的方法：**VLAN→私有VLAN→PVLAN**

图 6-6 新建私有 VLAN

以下的条目会显示在屏幕上:

- **创建私有 VLAN**

  主 VLAN 填写主 VLAN ID。

  辅助 VLAN 填写辅助 VLAN ID。

  辅助 VLAN 类型 显示私有 VLAN 的辅助 VLAN 类型。

- **查找条目**

  查找选项 选择私有 VLAN 的显示规则，可以帮助您快速查找到所需的条目。

  全部 填写欲查找条目需包含的主 VLAN ID 或辅助 VALN ID。

  主 VLAN ID 填写欲查找条目需包含的主 VLAN ID。

  辅助 VLAN ID 填写欲查找条目需包含的辅助 VLAN ID。

- **私有 VLAN 表**

  选择 勾选条目进行删除或修改交换机私有 VLAN 配置信息，可多选。

  主 VLAN 显示私有 VLAN 的主 VLAN ID。

辅助 VLAN	显示私有 VLAN 的辅助 VLAN ID。
端口	显示私有 VLAN 的端口号。

6.9.2 端口配置

私有 VLAN 支持的接口类型有两种:Promiscuous 和 Host。一般来说，Promiscuous 端口和上行设备相连，Host 端口和用户端的电脑或者服务器相连。

进入页面的方法：**VLAN→私有 VLAN→端口配置**

图 6-7 端口配置

以下的条目显示在屏幕上:

- **端口配置**

选择的端口	在此处选择需配置的端口号。你可以手动输入一个或者从下面的端口列表中选择一个。
端口类型	从下拉列表中选择端口类型。
主 VLAN	指定端口所属的主 VLAN。
辅助 VLAN	指定端口所属的辅助 VLAN。

➢ **私有 VLAN 端口列表**

端口号 显示私有 VLAN 的端口号。

端口类型 显示对应的端口类型。

注意:

- 一个 Host 端口只能加入到一个私有 VLAN。
- 一个 Promiscuous 端口只能加入到一个主 VLAN。
- 如果要将一个 Promiscuous 端口添加到具有相同主 VLAN 的不同私有 VLAN 上，只需要将 Promiscuous 端口添加到这些私有 VLAN 中的任何一个。

➢ **配置过程:**

步骤	操作	描述
1	创建私有 VLAN	必选操作。在 VLAN→私有 VLAN→PVLAN 配置页面输入主 VLAN 和辅助 VLAN，选择一种辅助 VLAN，然后单击创建按钮。
2	添加端口到私有 VLAN	必选操作。在 VLAN→私有 VLAN→端口配置页面中选择所需的端口和配置端口类型并单击应用按钮。
3	删除 VLAN	可选操作。在 VLAN→私有 VLAN→PVLAN 配置页面中，选择所需删除 VLAN 的条目，单击删除按钮。

第7章 生成树

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息，BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。STP 即是通过在设备之间传递 BPDU 来确定网络的拓扑结构。

- **BPDU 格式及字段说明**

要实现生成树的功能，交换机之间传递 BPDU 报文实现信息交互，所有支持 STP 协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。

标准生成树的 BPDU 帧格式及字段说明：

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Protocol identifier： 协议标识

Version： 协议版本

Message type： BPDU 类型

Flag： 标志位

Root ID： 根桥 ID，由 2 字节的优先级和 6 字节 MAC 地址构成

Root path cost： 根路径开销

Bridge ID： 桥 ID，表示发送 BPDU 的桥的 ID，由 2 字节优先级和 6 字节 MAC 地址构成

Port ID： 端口 ID，标识发出 BPDU 的端口

Message age： BPDU 生存时间

Maximum age： 当前 BPDU 的老化时间，即端口保存 BPDU 的最长时间

Hello time： 根桥发送 BPDU 的周期

Forward delay： 表示在拓扑改变后，交换机在发送数据包前维持在监听和学习状态的时间

- **STP 的基本概念**

桥 ID（Bridge Identifier）：桥 ID 是桥的优先级和其 MAC 地址的综合数值，其中桥优先级是一个可以设定的参数。桥 ID 越低，则桥的优先级越高，这样可以增加其成为根桥的可能性。

根桥（Root Bridge）：具有最小桥 ID 的交换机是根桥。请将环路中所有交换机当中最好的一台设置为根桥交换机，以保证能够提供最好的网络性能和可靠性。

指定桥（Designated Bridge）：在每个网段中，到根桥的路径开销最低的桥将成为指定桥，数据包将通过它转发到该网段。当所有的交换机具有相同的根路径开销时，具有最低的桥 ID 的交换机会被选为指定桥。

根路径开销（Root Path Cost）：一台交换机的根路径开销是根端口的路径开销与数据包经过的所有交换机的根路径开销之和。根桥的根路径开销是零。

桥优先级（Bridge Priority）：是一个用户可以设定的参数，数值范围从 0 到 61440。设定的值越小，优先级越高。交换机的桥优先级越高，才越有可能成为根桥。

根端口（Root Port）：非根桥的交换机上离根桥最近的端口，负责与根桥进行通信，这个端口到根桥的路径开销最低。当多个端口具有相同的到根桥的路径开销时，具有最高端口优先级的端口会成为根端口。

指定端口（Designated Port）：指定桥上向本交换机转发数据的端口。

端口优先级（Port Priority）：数值范围从 0 到 255，值越小，端口的优先级就越高。端口的优先级越高，才越有可能成为根端口。

路径开销（Path Cost）：STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

生成树基本概念的组网示意图如图 7-1 所示。交换机 A、B、C 三者顺次相连，经 STP 计算过后，交换机 A 被选为根桥，端口 2 和端口 6 之间的线路被阻塞。

- 桥：交换机 A 为整个网络的根桥；交换机 B 是交换机 C 的指定桥。
- 端口：端口 3 和端口 5 分别为交换机 B 和交换机 C 的根端口；端口 1 和端口 4 分别为交换机 A 和交换机 B 的指定端口；端口 6 为交换机 C 的阻塞端口。

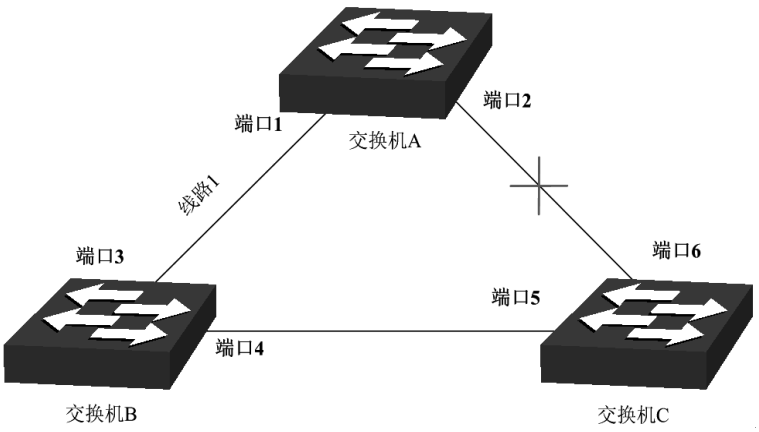


图 7-1 生成树基本概念组网图

➢ **STP 定时器**

联络时间（Hello Time）：

数值范围从 1 秒到 10 秒。是指根桥向其它所有交换机发出 BPDU 数据包的时间间隔，用于交换机检测链路是否存在故障。

老化时间（Max. Age）：

数值范围从 6 秒到 40 秒。如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。

传输时延（Forward Delay）：

数值范围从 4 秒到 30 秒。是指交换机的端口状态迁移所用的时间。

当网络故障引发生成树重新计算时，生成树的结构将发生相应的变化。但是重新计算得到的新配置消息无法立刻传遍整个网络，如果端口状态立刻迁移的话，可能会产生暂时性的环路。为此，生成树协议采用了一种状态迁移的机制，新的根端口和指定端口开始数据转发之前要经过 2 倍的传输时延，这个延时保证了新的配置消息已经传遍整个网络。

- **STP 模式的 BPDU 的优先级比较原则**

假定有两条 BPDU X 和 Y，则：

如果 X 的根桥 ID 小于 Y 的根桥 ID，则 X 优于 Y

如果 X 和 Y 的根桥 ID 相同，但 X 的根路径开销小于 Y，则 X 优于 Y

如果 X 和 Y 的根桥 ID 和根路径开销相同，但 X 的桥 ID 小于 Y，则 X 优于 Y

如果 X 和 Y 的根桥 ID、根路径开销和桥 ID 相同，但 X 的端口 ID 小于 Y，则 X 优于 Y

- **STP 的计算过程**

- 初始状态

每台交换机在初始时会生成以自己为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

- 最优 BPDU 的选择

每台交换机都向外发送自己的 BPDU，同时也会收到其它交换机发送的 BPDU。比较过程如下表所述：

步骤	内容
1	当端口收到的BPDU比本端口BPDU的优先级低时，交换机将丢弃接收到的BPDU，保留该端口的 BPDU；否则，交换机将接收到的 BPDU 替换成为该端口的 BPDU。
2	交换机将所有端口的 BPDU 进行比较，选出最优的 BPDU 作为本交换机的 BPDU。

表 7-1 最优 BPDU 的选择

- 根桥的选择

通过交换配置消息，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

- 根端口、指定端口的选择

根端口、指定端口的选择过程如下表所述：

步骤	内容
1	非根桥交换机将接收到最优 BPDU 的那个端口指定为根端口。

步骤	内容
2	交换机根据根端口的 BPDU 和根端口的路径开销，为其它端口计算一个端口 BPDU： • 根桥 ID 替换为根端口的根桥 ID； • 根路径开销替换为根端口的根路径开销加上本端口到根端口的路径开销； • 指定桥 ID 替换为自身设备的 ID； • 指定端口 ID 替换为自身端口 ID。
3	交换机使用计算出来的 BPDU 和需要确定端口角色的端口上的 BPDU 进行比较，并根据比较结果进行不同的处理： • 如果计算出来的 BPDU 优，则设备就将该端口定为指定端口，端口上的 BPDU 被计算出来的 BPDU 替换，并周期性向外发送。 • 如果端口上的 BPDU 优，则设备不更新该端口 BPDU 并将此端口阻塞，该端口将不再转发数据，只接收但不发送配置消息；

表 7-2 根端口、指定端口的选择

说明：

- 在拓扑稳定状态，只有根端口和指定端口转发数据，其它的端口都处于阻塞状态，它们只接收 BPDU 报文而不转发数据。

➢ **RSTP**

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的 STP，他大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。RSTP 的端口状态实现快速迁移的前提如下：

- 根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。
- 指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

➢ **RSTP 的基本概念**

边缘端口（Edge Port）：直接与终端相连而不是与其它交换机相连的端口。

点对点链路：是两台交换机之间直接连接的链路。

➢ **MSTP**

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 802.1S 标准建立的，他既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

MSTP 的特点如下：

- MSTP 通过 VLAN-实例映射表，把 VLAN 和生成树联系起来，将多个 VLAN 捆绑到一个实例中，并以实例为基础实现负载均衡。
- MSTP 把一个生成树网络划分成多个域，每个域内形成多棵内部生成树，各个生成树之间彼此独立。

- MSTP 在数据转发过程中实现 VLAN 数据的负载分担。
- MSTP 兼容 STP 和 RSTP。

➢ **MSTP 的基本概念**

MST 域（Multiple Spanning Tree Region，多生成树域）：由具有相同域配置和相同 VLAN-实例映射关系的交换机所构成。

IST（Internal Spanning Tree，内部生成树）：MST 域内的一棵生成树。

CST（Common Spanning Tree，公共生成树）：连接网络内所有 MST 域的单生成树。

CIST（Common and Internal Spanning Tree，公共和内部生成树）：连接网络内所有设备的单生成树，由 IST 和 CST 共同构成。

MSTP 基本概念的组网图如图 7-2 所示。

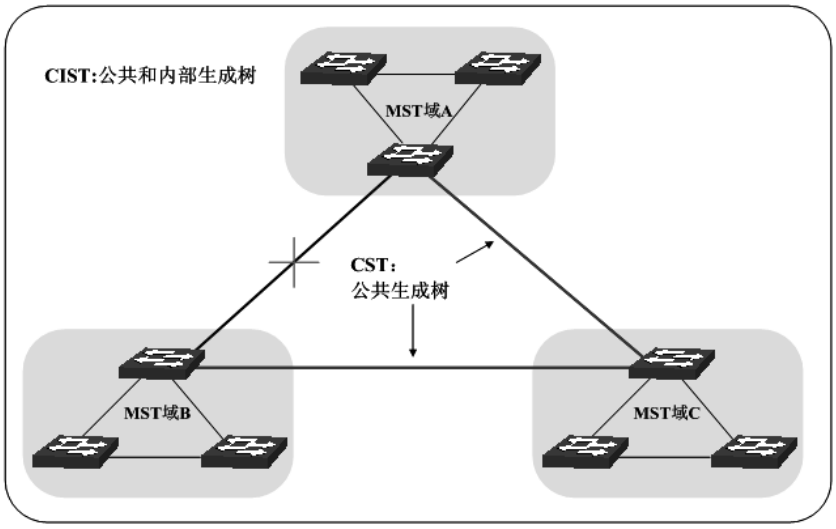


图 7-2 MSTP 基本概念组网图

➢ **MSTP 的基本原理**

MSTP 将整个网络划分为多个 MST 域，各个域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。MSTP 同 STP 一样，使用 BPDU 进行生成树的计算，只是 BPDU 中携带的是 MSTP 的配置信息。

➢ **MSTP 模式的 BPDU 优先级比较原则**

假定有两条 MSTP 的 BPDU X 和 Y，则：

如果 X 的总根 ID 小于 Y 的总根 ID，则 X 优于 Y；

如果 X 和 Y 的总根 ID 相同，但 X 的外部路径开销小于 Y，则 X 优于 Y；

如果 X 和 Y 的总根 ID 和外部路径开销相同，但 X 的域根 ID 小于 Y 的域根 ID，则 X 优于 Y；

如果 X 和 Y 的总根 ID、外部路径开销和域根 ID 相同，但 X 的内部路径开销小于 Y，则 X 优于 Y；

如果 X 和 Y 的总根 ID、外部路径开销、域根 ID 和内部路径开销相同，但 X 的桥 ID 小于 Y，则 X 优于 Y；

如果 X 和 Y 的总根 ID、外部路径开销、域根 ID、内部路径开销和桥 ID 均相同，但 X 的端口 ID 小于 Y，则 X 优于 Y。

➢ **端口状态**

MSTP 中，根据端口是否转发数据和如何处理 BPDU 报文，可将端口状态划分为以下四种：

- 转发：接收并转发数据，接收并发送 BPDU 报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送 BPDU 报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送 BPDU 报文，不进行地址学习。
- 断开：物理链路断开。

➢ **端口角色**

MSTP 的端口角色分为以下几种：

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master 端口：连接 MST 域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和 Master 端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口角色的示意图如图 7-3 所示。

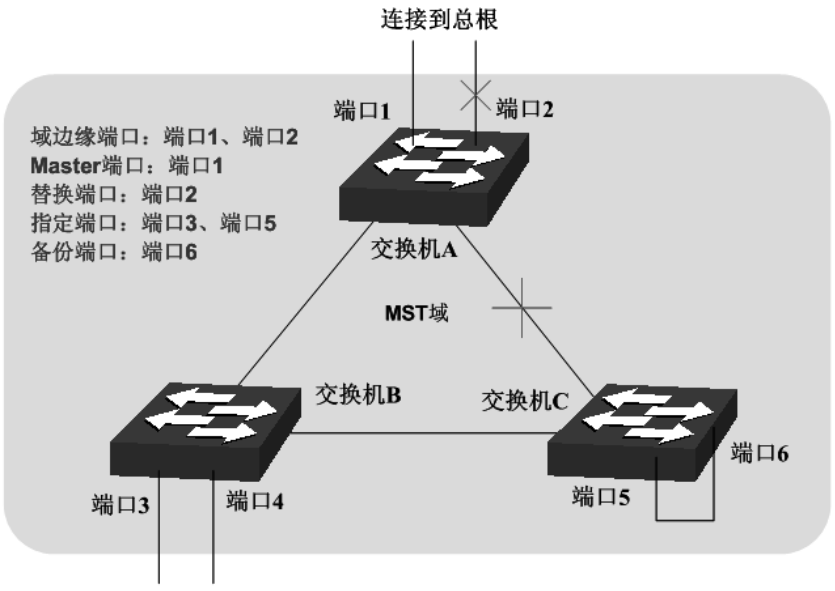


图 7-3 端口角色示意图

生成树模块主要用于配置交换机的生成树功能，包括**基本配置**、**端口配置**、**MSTP 实例**以及**安全配置**四个部分。

7.1 基本配置

基本配置用于配置和查看交换机生成树功能的全局属性，本功能包括**基本配置**和**生成树信息**两个配置页面。

7.1.1 基本配置

配置生成树前请明确各交换机在每个生成树实例中的地位，每个生成树实例中只有一台交换机处于根桥地位。配置交换机的生成树功能，首先需要在本页配置交换机生成树的全局功能和相关参数。

进入页面的方法：生成树>>基本配置>>基本配置

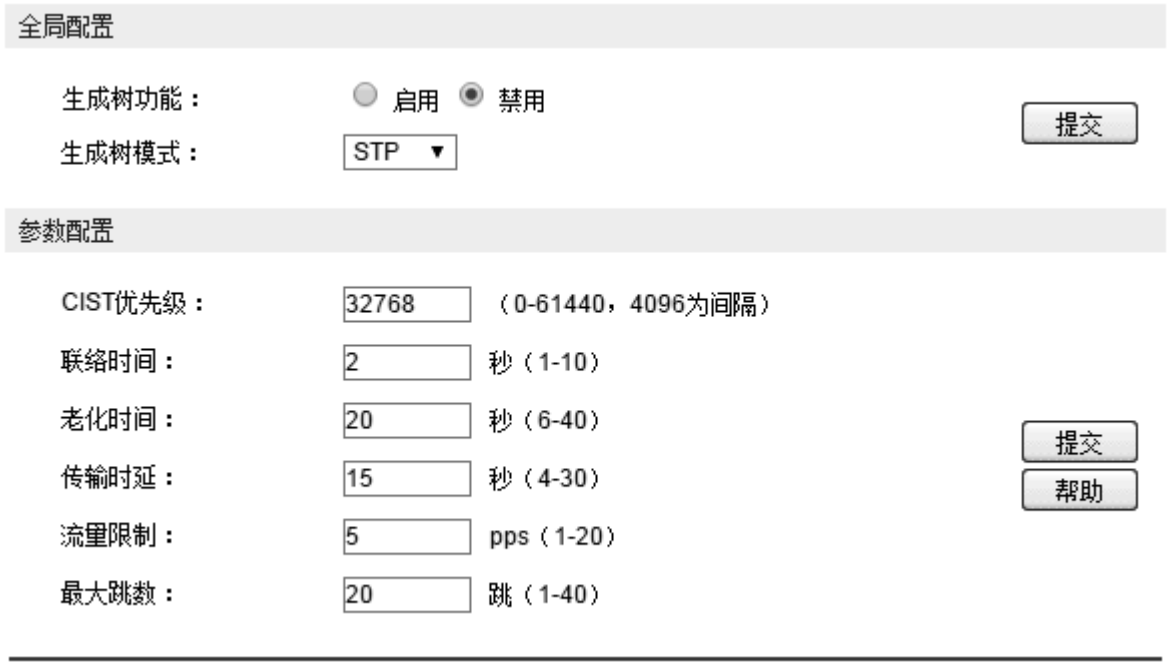


图 7-4 基本配置

条目介绍：

- **全局配置**

生成树功能： 选择是否启用交换机的生成树功能。

生成树模式： 选择交换机的生成树模式。

- STP：生成树兼容模式。
- RSTP：快速生成树兼容模式。
- MSTP：多重生成树模式。

- **参数配置**

CIST 优先级： 填写交换机的 CIST 优先级。CIST 优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。值越小，表示优先级越高。默认为 32768，且必须是 4096 的倍数。

联络时间： 填写交换机发送协议报文的周期，用于检测链路是否存在故障。并且，2×（联络时间+1）≤老化时间。默认为 2 秒。

老化时间： 填写协议报文在交换机中能够保存的最大生存期。默认为 20 秒。

传输时延： 在网络拓扑改变后，交换机的端口状态迁移的延时时间。并且，2×（传输延时－1）≥老化时间。默认为 15 秒。

流量限制： 填写在每个联络时间内，端口最多能够发送的协议报文的速度。默

认为 5pps。

最大跳数： 填写协议报文被转发的最大跳数，它限制了生成树的规模。默认为 20 跳。

注意：

- 设备的传输时延参数的长短与 STP 的规模有关。如果传输时延过小，可能会引入临时的环路；如果传输时延过大，网络可能会较长时间不能恢复连通。建议采用默认值。
- 合适的联络时间可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果联络时间过长，在链路发生丢包时，交换机会误以为链路出现了故障，从而引发网络中生成树的重新计算；如果联络时间过短，交换机将频繁发送重复的配置消息，增加了交换机的负担，浪费了网络资源。建议采用默认值。
- 如果老化时间过小，交换机会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果老化时间过大，交换机不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力。建议采用默认值。
- 如果流量限制过大，每个联络时间内发送的 MSTP 报文数会很多，从而占用过多的网络资源。建议采用默认值。

7.1.2 生成树信息

本页用来查看交换机生成树功能的相关参数。

进入页面的方法：生成树>>基本配置>>生成树信息

图 7-5 基本信息

7.2 端口配置

本页用来配置交换机端口的 CIST 参数。

进入页面的方法：生成树>>端口配置>>端口配置

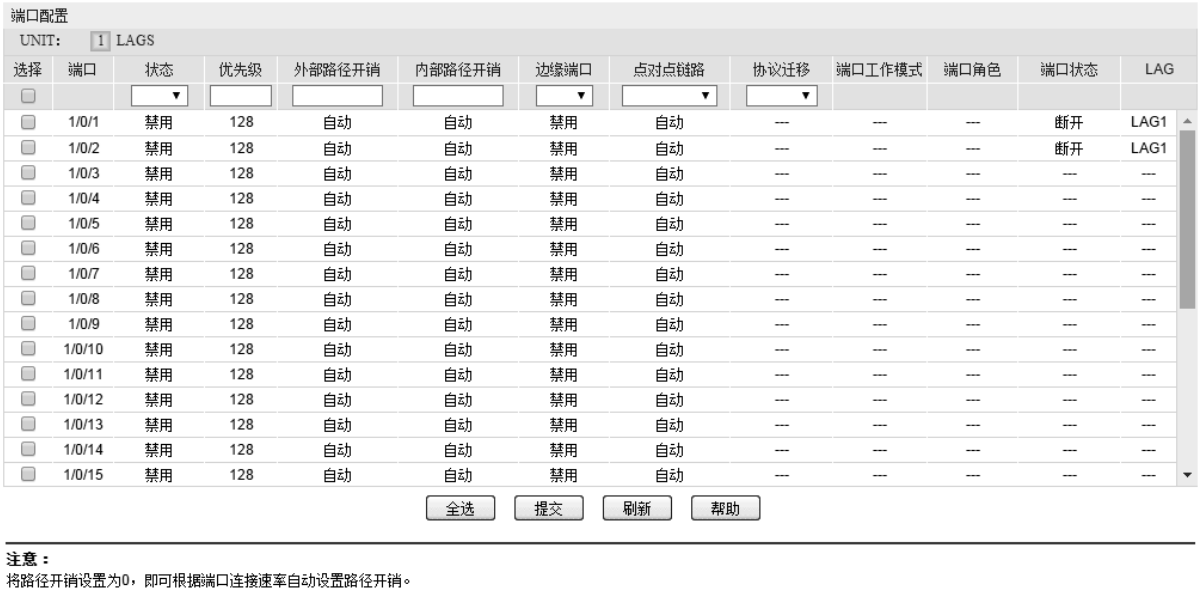


图 7-6 端口配置

条目介绍：

- **端口配置**

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口 STP 功能，可多选。

端口： 显示交换机的端口号。

状态： 选择该端口是否启用 STP 功能。

优先级： 确定与该端口连接的端口是否会被选为根端口的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。默认为 128，范围 0-240，且为 16 的倍数。

外部路径开销： 在不同 MST 域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

内部路径开销： 在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

边缘端口： 选择是否启用边缘端口。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

点对点链路： 选择端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

协议迁移： 启用端口开始一次协议迁移检查。

工作模式： 显示端口所处的生成树模式。

端口角色： 显示端口在生成树实例中担任的角色。

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master 端口：连接多生成树域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和 Master 端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口状态： 显示端口所处的工作状态。

- 转发：接收并转发数据，接收并发送协议报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送协议报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送协议报文，不进行地址学习。
- 断开：物理链路断开。

LAG： 显示端口当前所属的汇聚组。

注意：

- 对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。
- 对于属于汇聚组的端口，所有端口都可以被配置成与点对点链路相连。
- 当端口被设置为与点对点链路相连，则该端口所在的所有生成树实例均被设置为与点对点链路相连。如果端口实际物理链路不是点对点链路，却配置为强制点对点链路，则有可能会引入临时环路。

7.3 MSTP 实例

MSTP 设置了 VLAN-实例映射表（即 VLAN 和生成树的对应关系表），把 VLAN 和生成树联系起来。通过增加 MSTP 实例（将多个 VLAN 整合到一个集合中），将多个 VLAN 捆绑到一个实例中，并以实例为基础实现负载均衡。

只有当多台交换机的 MST 域名、MST 域的修订级别、VLAN-实例映射表完全相同时，它们才能属于同一个 MST 域。本功能包括**域配置**、**实例配置**和**实例端口**三个配置页面。

7.3.1 域配置

本页用来配置 MST 域的域名和修订级别。

进入页面的方法：生成树>>MSTP 实例>>域配置

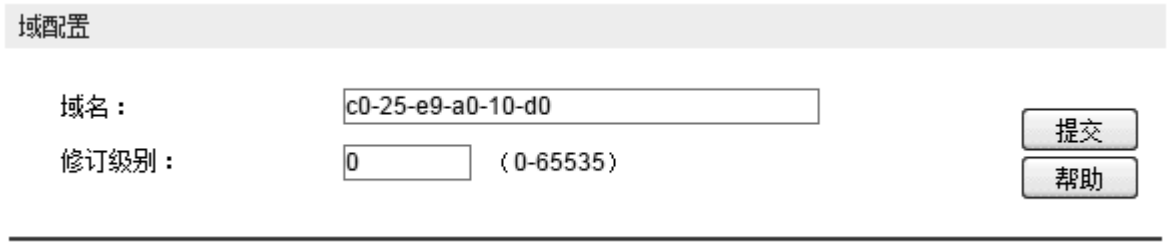


图 7-7 域配置

条目介绍：

- **域配置**

域名： 填写域名来标识 MST 域，最长可用 32 个字符。

修订级别： 填写修订级别来标识 MST 域。

7.3.2 实例配置

实例配置是 MST 域的一个属性，用来描述 VLAN 和生成树实例的映射关系。请按需要将 VLAN 分配至不同的实例，每个实例就是一个“VLAN 组”，不受其它实例和公共生成树的影响。

进入页面的方法：生成树>>MSTP 实例>>实例配置

图 7-8 实例配置

条目介绍：

- **实例配置**

实例 ID 选择：	点击<选择>按键，可根据所输 ID 号，快速选择相应实例。
选择：	勾选条目配置实例状态及优先级，可多选。
实例 ID：	显示交换机的实例 ID 号。
状态：	选择是否启用相应实例。
优先级：	在对应实例 ID 中，确定该交换机是否会被选为根桥的重要依据。默认为 32768，且必须是 4096 的倍数。
VLAN ID：	填写该实例 ID 所包含的 VLAN ID。若之前已存在 VLAN ID，在此修改后，之前的 VLAN ID 将被清空，并映射至 CIST 中。

- **VLAN-实例映射**

VLAN ID：	填写需要添加的 VLAN ID。若对应实例 ID 中已有 VLAN ID，在此修改后，新的 VLAN ID 将被添加，而不会将之前的覆盖。
实例 ID：	填写实例 ID。

注意：

- 当 GVRP 和 MSTP 同时启用时，GVRP 报文将沿着生成树实例 CIST 进行传播。因此如果希望通过 GVRP 在网络中发布某个 VLAN，则需在配置 MSTP 的“VLAN-实例映射”时保证把这个 VLAN 映射到 CIST 上。关于 GVRP 的相关介绍请参见 6.7 GVRP。

7.3.3 实例端口

端口在不同的生成树实例中可以担任不同的角色，本页用来配置不同实例 ID 中的端口的参数，同时在此可以查看端口在特定实例中的状态信息。

进入页面的方法：生成树>>MSTP 实例>>实例端口

图 7-9 实例端口

条目介绍：

- **实例端口配置**

实例 ID： 选择需要配置端口属性的实例 ID。

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口的优先级和路径开销，可多选。

端口： 显示交换机的端口号。

优先级： 在对应实例 ID 中，确定与该端口连接的端口是否会被选为根端口的重要依据。默认为 128，范围 0-240，且为 16 的倍数。

路径开销： 在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

端口角色： 显示端口在生成树实例中担任的角色。

端口状态： 显示端口所处的工作状态。

LAG： 显示端口当前所属的汇聚组。

注意：

- 同一端口在不同的生成树实例中的端口状态可以不同。

安全树功能全局配置步骤：

步骤	操作	说明
1	明确交换机在生成树实例中的角色：根桥或指定桥	准备工作。
2	配置 MSTP 的全局参数	必选操作。在**生成树>>基本配置>>基本配置**页面，开启交换机的生成树功能，并配置 MSTP 的参数。
3	配置端口的 MSTP 参数	必选操作。**生成树>>端口配置>>端口配置**页面进行配置。
4	配置 MST 域	必选操作。**生成树>>MSTP 实例>>域配置**、**实例配置**页面，创建 MST 域，及交换机在 MST 域中的角色。
5	配置实例端口的 MSTP 参数	可选操作。**生成树>>MSTP 实例>>实例端口**页面，为 MST 域内不同的实例，配置实例端口的 MSTP 属性。

7.4 安全配置

通过配置设备的保护功能，来防止生成树网络中的设备遭受各种形式的恶意攻击。本功能包括**端口保护**和 **TC 保护**两个配置页面。

7.4.1 端口保护

- **环路保护：**

在网络拓扑稳定时，交换机通过不断接收上游交换机发送的 BPDU 报文，来保持本机各个端口的端口状态。但是当发生链路拥塞或者单向链路故障时，位于下游的交换机无法收到 BPDU 报文，将会重新计算生成树，重新选择端口角色，这时阻塞端口会迁移到转发状态，从而导致网络中产生环路。

环路保护功能会抑制这种环路的产生。对于启用了环路保护的端口，当没有接收到上游交换机发送的 BPDU 报文，引起 STP 重新计算时，不论其端口角色如何，该端口将一直被设置为阻塞状态。

- **根桥保护：**

在设计网络拓扑时，CIST 的根桥和备份根桥大多处于一个高带宽的核心域内。但是，当维护人员错误配置或遭受到网络中的恶意攻击时，网络中的合法根桥有可能会收到优先级更高的 BPDU 报文，致使当前合法根桥失去了根桥的地位，从而导致网络拓扑结构的错误变动。这种错误的变动，使得原来应该通过高速链路的流量被牵引到低速链路上，引起网络拥塞。

为了防止这种情况发生，MSTP 提供根桥保护功能：对于启用了根桥保护功能的端口，他在所有实例上的端口角色只能为“指定端口”。当该端口收到优先级更高的 BPDU 时，立刻将该端口的端口状态转化为“阻塞”状态，不再转发报文（相当于将此端口相连的链路断开）。当在 2 倍的传输时延时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

- **TC 保护**

交换机收到 TC-BPDU 报文（网络拓扑发生变化的通知报文）后，会将本机的地址表项删除。当有人伪造 TC-BPDU 报文恶意攻击交换机时，交换机短时间内收到大量 TC-BPDU 报文，频繁的删除操作给交换机带来很大负担，给网络的稳定带来很大隐患。通过在交换机上启用 TC 保护功能，可以避免交换机频繁地删除地址表项。

启用 TC 保护功能后，交换机在“TC 保护周期”内，收到 TC-BPDU 的最大数目为“TC 保护阈值”处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

- **BPDU 保护**

交换机上直接与 PC 或服务器相连的端口会被设置为“边缘端口”，以实现这些端口的快速迁移。当这些端口接收到 BPDU 报文时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。而这些端口一般情况下不会收到 BPDU 报文。如果有人用伪造的 BPDU 报文恶意攻击交换机，就会引起网络拓扑的震荡。

MSTP 提供 BPDU 保护功能来防止这种攻击：启用了 BPDU 保护功能后，如果边缘端口收到了 BPDU 报文，MSTP 就将这些端口关闭，同时通知网管这些端口被 MSTP 关闭，被关闭的端口只能由网络管理人员来恢复。

- **BPDU 过滤**

BPDU 过滤用来防止恶意的 BPDU 洪泛攻击。交换机收到恶意的 BPDU 报文以后，会向网络中的其它交换机转发，致使网络内的交换机不停的进行 STP 计算，从而导致交换机的 CPU 占用率过高或者 BPDU 报文的协议状态错误等。

启用了 BPDU 报文过滤功能的端口，将不再接收和转发任何 BPDU 报文，但是会向外发送自身的 BPDU 报文，从而防止交换机受到 BPDU 报文的攻击，保证 STP 计算的正确性。

在本页可以对交换机的各个端口配置上述几种保护功能，建议对符合条件的端口启用保护功能。

进入页面的方法：生成树>>安全配置>>端口保护

图 7-10 端口保护

条目介绍：

- **端口保护**

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口保护功能，可多选。

端口： 显示交换机的端口号。

环路保护： 防止由于链路拥塞或者单向链路故障，导致下游设备重新计算生成树，由此产生的网络环路现象。

根桥保护： 防止当前合法根桥会失去根桥的地位，引起网络拓扑结构的错误变动。

TC 保护： 防止恶意伪造的 TC 报文在 STP 协议网络中传播，导致桥设备的地址表不断清空，而引起的网络吞吐量下降。

BPDU 保护： 防止边缘端口受到恶意伪造的协议报文的攻击。

BPDU 过滤： 防止 STP 协议网络中协议报文泛洪。

LAG： 显示端口当前所属的汇聚组。

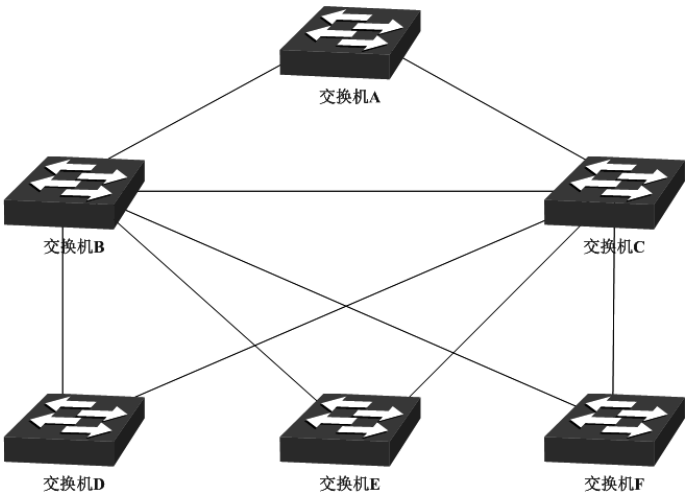
7.5 STP 功能的组网应用

- **组网需求**

- 交换机 A、B、C、D、E 均支持 MSTP 功能；

- A 为中心交换机；
- B、C 为汇聚层交换机，D、E、F 为接入层交换机；
- 整个网络中共有 6 个 VLAN，为 VLAN101-VLAN106；
- 所有设备运行 MSTP，并且所有设备均属于同一个 MST 域；
- VLAN101、103 和 105 的数据流量以 B 为根桥，VLAN102、104 和 106 的数据流量以 C 为根桥。阻断网络中的环路，并能达到数据转发过程中 VLAN 数据的冗余备份以及负载分担效果。

➢ **组网图**



➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“SWITCH”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。

- 配置交换机 B：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。
5	将交换机 B 配置为实例 1 的根桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 1 的优先级设置为 0。
6	将交换机 B 配置为实例 2 的指定桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 2 优先级设置为 4096。

- 配置交换机 C

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。
5	将交换机 C 配置为实例 1 的指定桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 1 的优先级设置为 4096。
6	将交换机 C 配置为实例 2 的根桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 2 优先级设置为 0。

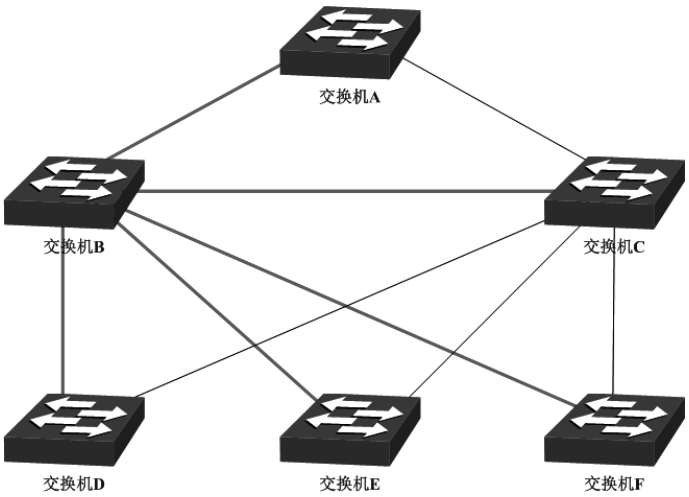
- 配置交换机 D

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“SWITCH”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。

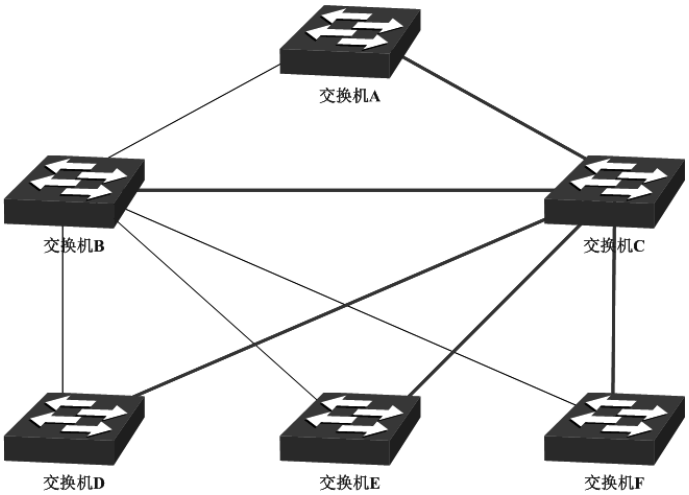
- 交换机 E 和交换机 F 的配置方法同交换机 D

➢ **拓扑稳定以后两个实例所生成的动态拓扑结构**

- 对于实例 1（VLAN 101 103 105）而言，连通的链路为下图中红色的路径，灰色的路径断开。



- 对于实例 2（VLAN 102 104 106）而言，连通的链路为下图中蓝色的路径，灰色的路径断开。



➢ **配置建议**

- 所有交换机的端口均建议启用“TC 保护”功能。
- 根桥交换机的所有端口建议启用“根桥保护”功能。
- 非边缘端口建议启用“环路保护”功能。
- 连接 PC 与服务器的边缘端口，建议启用“BPDU 保护”或“BPDU 过滤”功能。

回目录

第8章 以太网 OAM

➢ OAM 概略

以太网 OAM(操作、管理和维护)是一个二层协议，用于以太网的监控和故障诊断。通过两个 OAM 实体之间交换 OAMPDUs，它可以将网络状态报告给网络管理员，以促进网络管理。

以太网 OAM 是一个慢协议，它对带宽要求非常有限。帧传输速率限制在每秒 10 帧，因此，OAM 对数据流量的影响是可以忽略不计的。

用户通过在两个点到点连接的设备上启用以太网 OAM 功能，可以监控这两台设备之间的链路状态，OAM 可以从以下三点来监视链路状态。

1) 链路性能监测：对链路的各种性能进行监测。

2) 故障侦测和告警：通过发送检测报文来探测链路的连通性，当链路出现故障时及时通知网络管理员。

3) 环路测试：通过非以太网 OAM 协议报文的环回来检测链路故障。

以太网 OAM 是一种监控网络故障的工具，目前主要用于解决以太网接入“最后一公里”中常见的链路问题。

➢ OAMPDUs

有六个类型的 OAMPDUs。下面的图显示了最常用的 OAMPDUs，即信息 OAMPDU、事件通知 OAMPDU 和环回控制 OAMPDU。

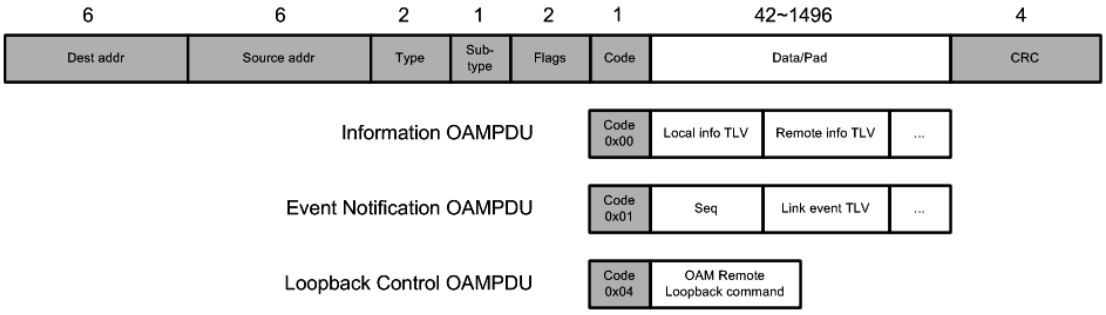


图 8-1 OAMPDUs

如图 8-1 所示，OAMPDUs 是标准长度的以太网帧。它们必须是无标记的，范围从 64 到 1518 字节。

1) Dest addr：OAMPDU 的 Dest addr (目的地 MAC 地址) 是慢协议组播地址 (01:80:c2:00:00:02).

2) Source add：Source addr 是 OAMPDU 传播端口相关的 MAC 地址。

3) Type：type 字段是固定的 0x8809。

4) Sub-type：sub-type 字段是固定的 0x03。

5) Flags：flag 字段包含 OAM 实体的状态位。

6) Code：code 字段标识 OAMPDU 的特定类型。如上所述，信息 OAMPDU，事件通知 OAMPDU 和环回控制 OAMPDU 是常用的，及其代码分别为 0x00，0x01，0x04。三种 OAMPDUs 描述

如下。

信

息 OAMPDU：用于将 OAM 实体的状态信息（包括本地信息、远端信息和自定义信息）发给远端 OAM 实体，以保持以太网 OAM 连接。

事件通知 OAMPDU：一般用于链路监控，对连接本端和远端 OAM 实体的链路上所发生的故障进行告警。

环回控制 OAMPDU：主要用于远端环回控制，用来控制远端设备的 OAM 环回状态，该报文中带有使能或去使能环回功能的信息，根据该信息开启或关闭远端环回功能。

- **OAM 功能**

如 IEEE 802.3 中 57 条所定义的，第一英里的以太网，OAM 功能包括 OAM 发现、链路监控、远端故障指示和远端环回。

发现

发现是以太网 OAM 的第一阶段。在这个阶段，一个 OAM 实体发现其他 OAM 实体，使用信息 OAMPDUs 来建立连接。

至于 OAM 连接，OAM 实体可以选择两种模式:主动和被动。只有激活的 OAM 实体可以启动 OAM 连接过程。被动的 OAM 实体等待和响应 OAM 连接建立请求。相互关联的 OAM 实体告知对端 OAM 配置信息，以确定 OAM 链接能否建立。通过交换信息，然后确定 OAM 可以建立连接。只有当环回、链接检测和链接事件的设置在两边都匹配的情况下，才能建立一个 OAM 连接。

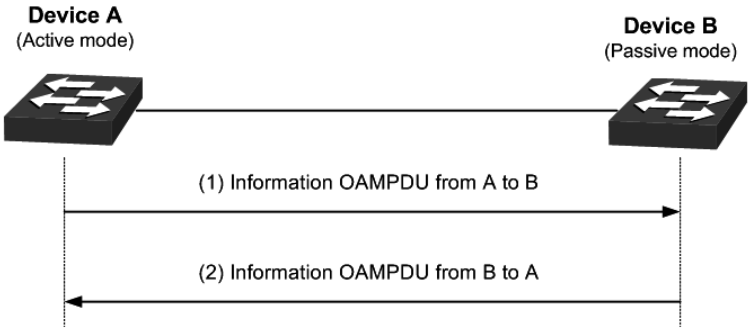


图 8-2 OAM 发现

主动 OAM 模式和被动 OAM 模式如下所示

项目	主动 OAM 模式	被动 OAM 模式
启动 OAM 发现	提供	不提供
回应 OAM 发现	提供	提供
传输信息 OAMPDUs	提供	提供
传输事件通知 OAMPDUs	提供	提供
传输信息 OAMPDUs 且 Data/Pad 字段为空	提供	提供

项目	主动 OAM 模式	被动 OAM 模式
传输环回控制 OAMPDUs	提供	不提供
回应环回控制 OAMPDUs	提供（如果两边都是主动 OAM 模式）	提供
传输特定组织 OAMPDUs	提供	提供

表 8-1 主动 OAM 模式与被动 OAM 模式之间的差异

OAM 建立连接后，OAM 实体双方交换信息 OAMPDUs，定期保持 OAM 连接有效。如果 5 秒不接收信息 OAMPDU， OAM 实体认为 OAM 连接无效。

链路监控

链路监控能在多种情况下检测和定位链路故障。当链路上发现有问题时，设备将发送事件通知 OAMPDUs 报告链路事件。链路事件被描述如下:

OAM 链路事件	描述
错误信号周期	如果符号错误的数量在某一特定时间内超过阈值，就会发生错误信号周期事件。
错误帧	如果错误帧的数量超过了某一特定时间段内的阈值，就会发生错误帧事件。
错误帧周期	如果在特定数量的接收帧中的错误帧的数量超过阈值，就会发生错误帧周期事件。
错误帧秒数	如果错误帧秒数超过阈值，就会发生错误帧秒数事件。

表 8-2 OAM 连接事件

远端故障指示

以太网的故障检测非常困难，特别是在网络物理通信没有中断而网络性能缓慢下降的情况下。OAMPDU 中的 flag 允许 OAM 实体转达失败条件。失败条件如下:

链路错误:对端链路信号丢失。它在信息 OAMPDU 中每秒发送一次。

致命故障:一个不可恢复的错误，比如电源故障发生。这是立即和连续发送的。

紧急事件:未指定的紧急事件发生。这是立即和连续发送的。

定期在 OAM 实体之间发送信息 OAMPDUs，OAM 实体可以通知对端 OAM 链路错误。因此，网络管理员可以及时了解链路故障并及时采取行动。

远端环回

远端环回帮助确保在安装期间或在故障排除期间的链路质量。OAM 建立连接后，主动的 OAM 实体可以使用环回控制 OAMPDU 使其对端进入环回模式。

启用了远端环回，主动的 OAM 实体发送远端环回请求和对端回应。如果对端在环回模式下，它沿着原来的路径返回除了 OAMPDUs 和暂停帧外的所有帧。通过这些返回帧，管理员可以测试链路性能，比如延迟、抖动和帧损耗率。

下面的图显示了远端环回是如何工作的。

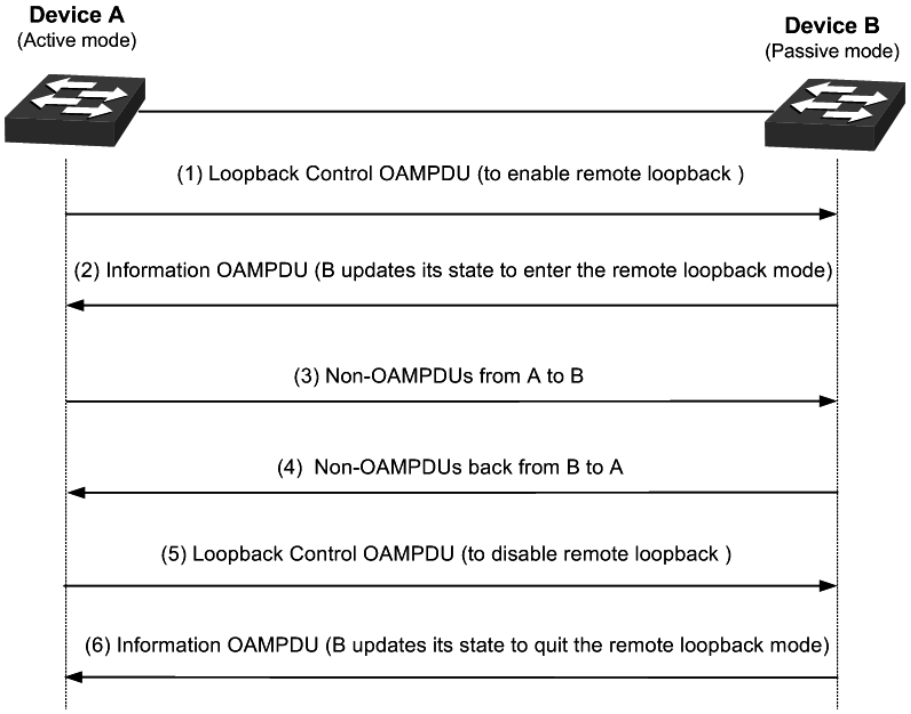


图 8-3 远程环回

8.1 基本配置

在基本配置页面上，您可以在指定的端口上启用以太网 OAM 功能，并将其 OAM 模式配置为主动或被动。此外，您还可以查看发现信息页面上的连接状态。

8.1.1 基本配置

进入页面的方法：以太网 OAM→基本配置→基本配置

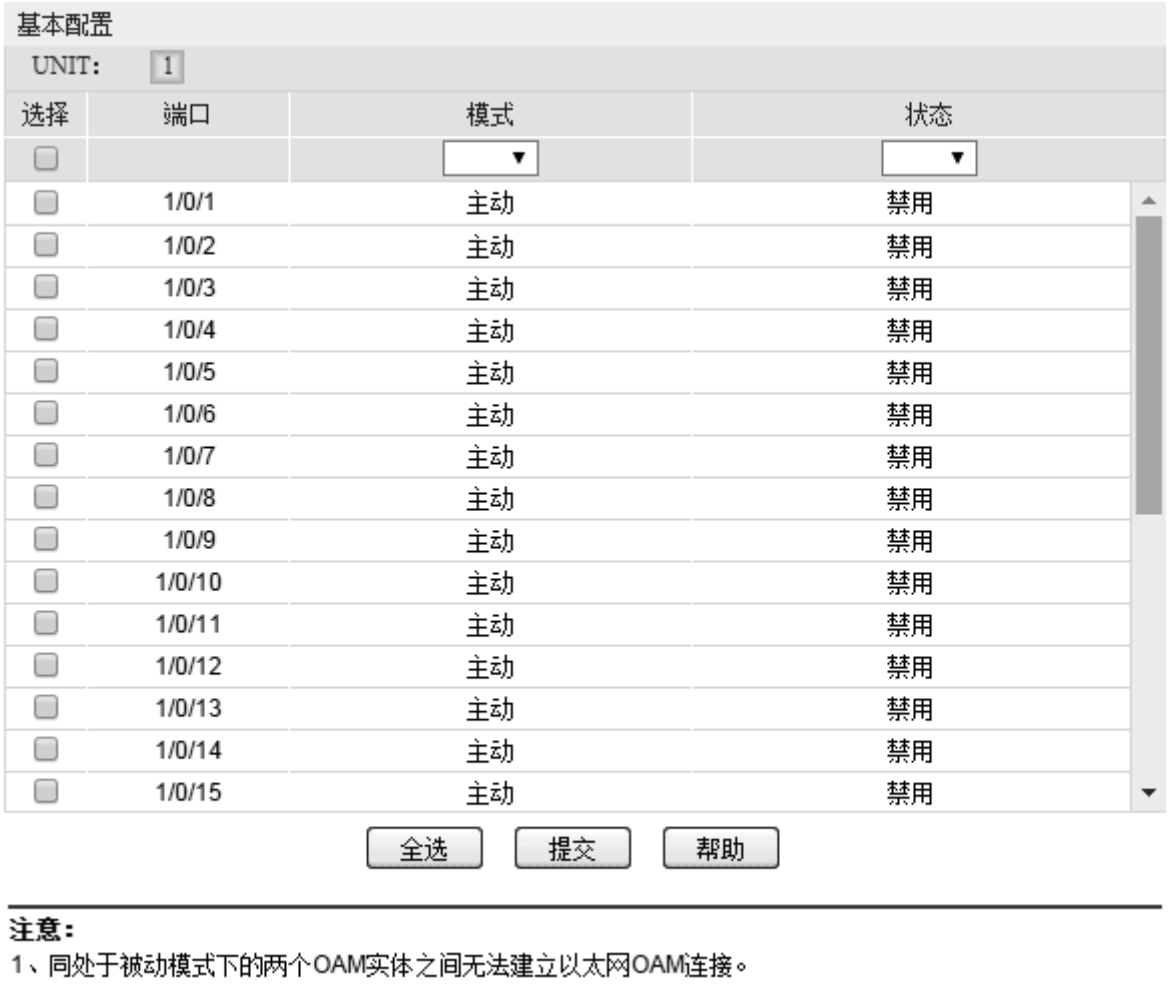


图 8-4 基本配置

以下的条目显示在屏幕上:

- **基本配置**

选择: 勾选条目配置端口，可多选。

模式: 选择以太网 OAM 工作模式。

状态: 选择是否启用以太网 OAM 功能。

注意:

在被动模式下工作的两个 OAM 实体之间不能建立 OAM 连接。

8.1.2 发现信息

进入页面的方法：以太网 OAM→基本配置→发现信息

图 8-5 发现信息

以下的条目显示在屏幕上:

- 本端

本地客户端部分显示了本地 OAM 实体的信息。

OAM:	显示选定的端口上 OAM 功能是否启用或禁用。
模式:	显示所选端口的 OAM 模式。
以太网 OAM 报文最大长度:	显示以太网 OAM 报文的最大长度。
远端环回:	显示本地客户端是否支持远程环回功能。
单向链路:	显示本地客户端是否支持单向 OAM 操作。
链路监控:	显示本地客户端是否支持链路监控功能。
MIB 变量获取:	显示本地客户端是否支持变量请求。如果支持，本地客户端可以向远程客户端发送一些变量请求，以了解远程客户端响应的链接状态。

报文版本: 显示信息 OAMPDU 报文的 information TLV 的版本。

运行状态: 显示 OAM 连接的操作状态。

- Disable: 在该端口上 OAM 是禁用的。
- LinkFault: 当检测到有链路故障，则传输带有链路故障指示的 OAMPDUs 报文。
- PassiveWait: 端口是在被动模式下，则等待查看对端设备是否开启 OAM 功能。
- ActiveSendLocal: 端口是在主动模式下，则发送本地信息。
- SendLocalAndRemote: 本地端口发现了对端但尚未接受或拒绝对端的配置。
- SendLocalAndRemoteOK: 本地设备同意 OAM 对端实体。
- PeeringLocallyRejected: 本地 OAM 实体拒绝远程对端 OAM 实体。
- PeeringRemotelyRejected: 远程 OAM 实体拒绝本地设备。
- NonOperHalfDuplex: 由于以太网 OAM 功能没有完全设计工作在半双工端口。这个值表示启用了以太网 OAM，但是端口处于半双工操作中。

环回状态: 显示回路状态。

- No Loopback:本地客户端和远程客户端不在环回模式。
- Local Loopback: 本地客户端在环回模式。
- Remote Loopback: 远程客户端在环回模式。

8.2 链路监控

通过链路监控，您可以检测和发现各种环境下的数据链路层故障。以太网 OAM 通过交互事件通知 OAMPDU 来监控链路。当一端 OAM 实体监控到一般链路事件时，将向其对端发送事件通知 OAMPDU 以进行通报。

进入页面的方法：以太网 OAM→链接监控→链路监控

图 8-6 链路监控

以下的条目显示在屏幕上:

- **链接监控配置**

链路事件: 选择要进行监控的链路事件。

选择: 为配置选择所需的端口。它是多选的。

检测阈值: 输入触发链路事件的检测阈值。

检测窗口: 输入链路事件的检测窗口。

通知: 选择是否启用事件通知。

8.3 远端故障指示

以太网故障通常比较难诊断，特别是当物理通信仍然正常而网络性能却在慢慢下降。OAMPDU 定义了一个标志（即 Flag 域）允许以太网 OAM 实体将故障信息通知给对端，该标志定义了 OAM 支持的链路事件。

进入页面的方法：以太网 OAM→远端故障指示→远程故障指示

图 8-7 远程失败提示

以下的条目显示在屏幕上:

- **远程故障指示配置**

选择: 勾选条目配置端口，可多选。

端口: 显示交换机的端口号。

致命故障通知: 选择是否启用致命故障通知。

紧急事件通知: 选择是否启用紧急事件通知。

8.4 远端环回

本端 OAM 实体可以发送环回控制 OAMPDU 给对端 OAM 实体请求进入远端环回模式。该功能为链路问题的解决提供了必要的帮助。在远端环回模式下，当收到除 OAMPDU 以外的报文时，会将其按原路返回。

进入页面的方法：以太网 OAM→远端环回→远端环回

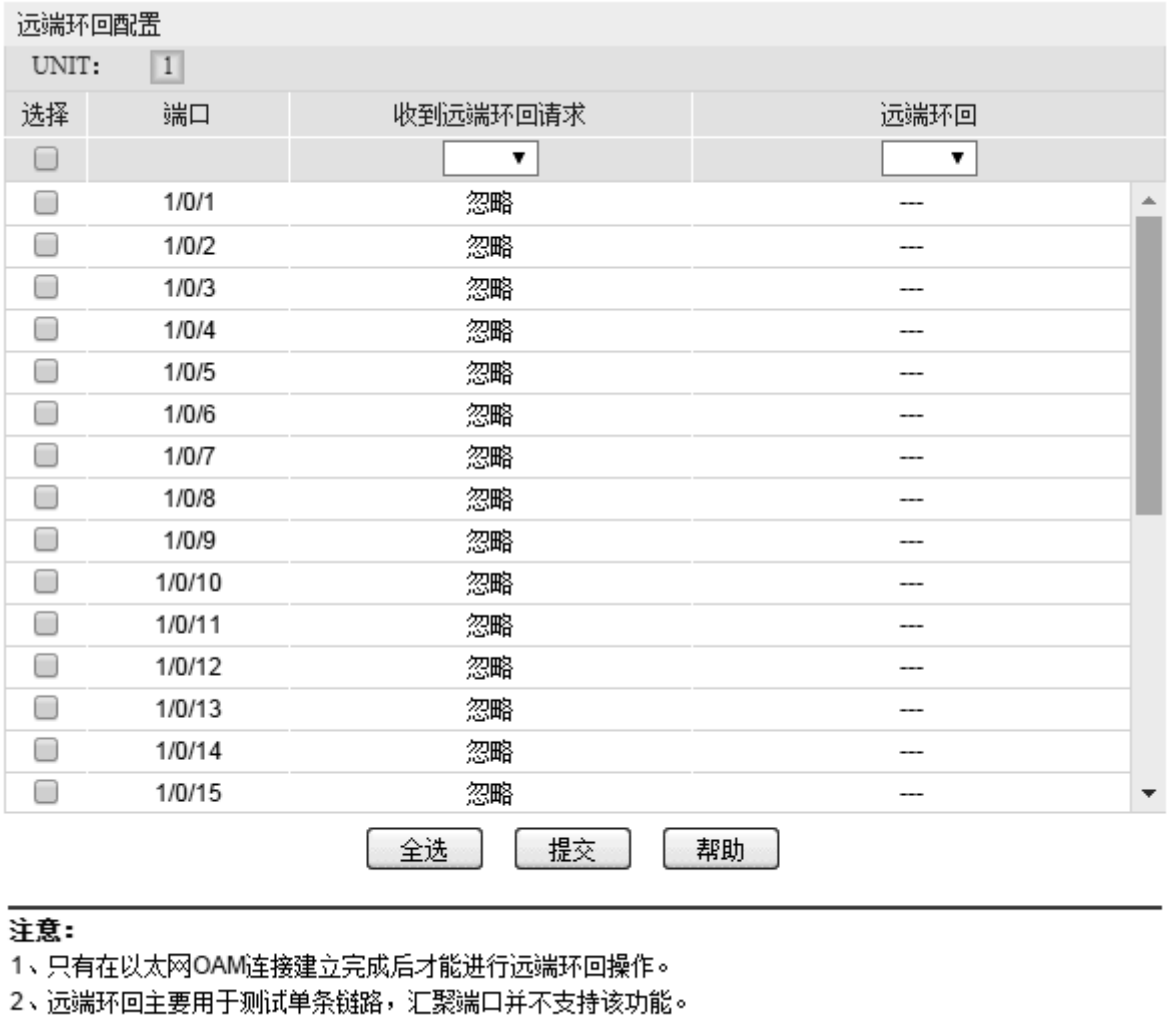


图 8-8 远程环回

以下的条目显示在屏幕上:

- **远程回路配置**

选择: 勾选条目配置端口，可多选。

端口: 显示交换机的端口号。

收到远端环回请求: 选择忽略或者处理收到的远端环回请求。

远端环回: 选择开始或者停止远端环回功能。

8.5 统计信息

您可以查看关于特定端口的详细以太网 OAM 流量信息和事件日志信息的统计信息。

8.5.1 统计信息

在这个页面上，您可以查看特定端口的详细的以太网 OAM 流量信息。当你点击清除按钮或设备重新启动时，该设备将重新计算这些数字。

进入页面的方法：以太网 OAM→统计信息→统计信息

图 8-9 统计信息

以下的条目显示在屏幕上:

- **统计**

信息 OAMPDUs: 显示接收、发送信息 OAMPDU 的数目。

Unique 事件通知 OAMPDUs: 显示接收、发送 Unique 事件通知 OAMPDU 的数目。

Duplicate 事件通知 OAMPDUs: 显示接收、发送 Duplicate 事件通知 OAMPDU 的数目。

MIB 变量请求 OAMPDUs: 显示接收、发送 MIB 变量请求 OAMPDU 的数目。

MIB 变量回应 OAMPDUs: 显示接收、发送 MIB 变量回应 OAMPDU 的数目。

环回控制 OAMPDUs: 显示接收、发送环回控制 OAMPDU 的数目。

组织自定义 OAMPDUs: 显示接收、发送组织自定义 OAMPDU 的数目。

未支持 OAMPDUs: 显示接收、发送未支持 OAMPDU 的数目。

OAM 导致的帧丢失: 显示由于 OAM 子层内部发送错误导致帧丢失的数目。

8.5.2 事件日志

在这个页面上，您可以查看特定端口的详细的以太网 OAM 事件日志信息。当你点击清除按钮或设备重新启动时，该设备将重新计算这些数字。

进入页面的方法：以太网 OAM→统计→事件日志

图 8-10 事件记录

以下的条目显示在屏幕上::

- **事件日志统计**

本端: 显示发生在本端的链路事件数目。

远端: 显示发生在远端的链路事件数目。

错误信号周期事件: 显示发生在本端、远端的错误信号周期事件数目。

错误帧事件: 显示发生在本端、远端的错误帧事件数目。

错误帧周期事件: 显示发生在本端、远端的错误帧周期事件数目。

错误帧秒数事件: 显示发生在本端、远端的错误帧秒数事件数目。

致命故障: 显示发生在本端、远端的致命故障数目。

紧急事件: 显示发生在本端、远端的紧急事件数目。

- **事件日志表**

类型: 显示链路事件的类型。

位置: 显示链路事件发生的位置。

时间: 显示链路事件发生的时间。

检测值: 显示在检测窗口期间检测到的错误数目。

检测窗口: 显示链路事件的检测窗口。

检测阈值: 显示链路事件的检测阈值。

累计错误: 显示自从 OAM 子层重置之后累计检测到的错误数目。

8.6 DLDP

- **DLDP 概略**

DLDP(设备连接检测协议)是一个 2 层协议，可以监控光纤或铜质双绞线的链路状态，来检测是否存在单向链路。当出现单向链路时，本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。单向链路会引起一系列问题，比如生成树拓扑环路等。一旦检测到单向链路，DLDP 就可以自动关闭相关端口，或者通知用户。

- **DLDP 运行机制**

1. DLDP 链接状态

DLDP 定义了一个设备的 6 个链接状态:初始化、未连通、活动、通告、探测和单通。

状态	描述
初始化	DLDP 是禁用的。
未连通	DLDP 是启用的，但是链路是关闭的。
活动	这个状态是暂时的，它表明: 1. DLDP 是启用的，链路正在建立。 2. 这个设备中的邻居条目是空的。
通告	这个状态表示没有检测到任何单向链路，包括两种情况: 1. 该设备与所有的邻居建立双向链路。 2. DLDP 仍处于活动状态超过 5 秒。
探测	如果一个设备从一个未知的邻居那里接收到一个数据包，就会从活动状态进入这个状态。在这种状态下，设备将发送探测数据包，以检测链路是否为单向的。
单通	这个状态表示检测到一个单向链路。

表 8-3 DLDP 连接状态

2. DLDP 工作过程

通常的 DLDP 工作过程如下:

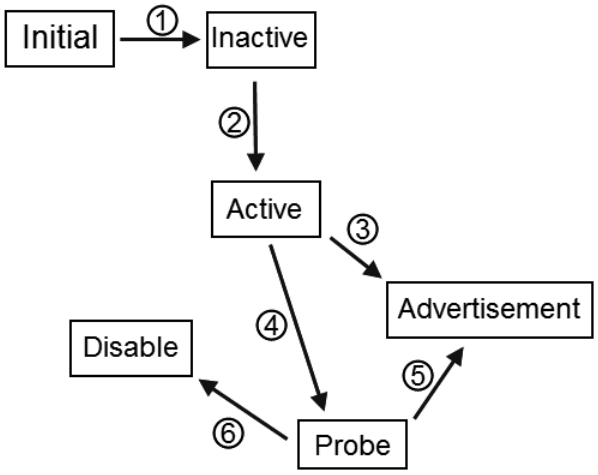


图 8-11 DLDP 进程

①: 当启用 DLDP，DLDP 链接状态将变为未连通。

②: 当 DLDP 使能链路建立起来，DLDP 链接状态将变为活动。该设备将在这个状态下发送带有 resynchronization 标记的通告包发给对端设备。

③: 如果在 5 秒内设备没有收到任何 DLDP 数据包，DLDP 链路状态将变到通告。

④: 从一个未知的邻居处收到一个数据包，设备的链接状态将从活动变到探测，然后发送几个探测数据包检测连接状态。

⑤: 如果设备接收到 echo 数据包，它们之间的链接状态将被标记为双向链接和 DLDP 状态将从探测变到通告。通告状态的设备会发送通告数据包。

⑥: 如果指定的一段时间后设备没有收到 echo 数据包，该链接将被标记为单向，并且 DLDP 状态将从探测变到单通。该端口将自动或手动关闭(取决于所配置的关闭模式)。

典型的双向链路检测过程是 ②→④→⑤， 典型的单向链路检测过程是一个 ②→④→⑥.

在 DLDP 页面上，您可以启用全局 DLDP 状态，并配置通告包和端口关闭模式的时间间隔。您还可以配置端口状态的刷新频率，并手动重置特定端口的 DLDP 状态。

进入页面的方法：以太网 OAM→DLDP→DLDP 配置.

图 8-12 DLDP 配置

以下的条目显示在屏幕上:

- **全局配置**

DLDP 状态: 在这里您可以启用或禁用 DLDP。

广告间隔时间: 设置广告间隔在 1 到 30 秒之间。默认值为 5 秒。

关闭模式: 使 DLDP 处于自动模式或手动模式以关闭检测到的单向链路。 默认为自动模式。

Web 页面刷新状态: 在这里您可以启用或禁用自动刷新。

Web 页面刷新间隔: 将 Web 刷新间隔设置为 1 到 100 秒。默认值为 5 秒。

- **端口配置**

选择: 选择 DLDP 配置所需的端口，可多选。

端口: 交换机端口列表。

DLDP 状态: 开启或禁用 DLDP 功能。

协议状态: 显示端口的 DLDP 协议状态。

链接状态: 显示端口的链路状态。

邻居状态: 显示端口的邻居状态。

- **配置过程:**

步骤	操作	描述
1	全局使能 DLDP	必选操作。在**以太网 OAM→DLDP→DLDP 配置**，配置全局 DLDP 状态。
2	在特定端口上使能 DLDP	必选操作。在**以太网 OAM→DLDP→DLDP 配置**， 配置端口 DLDP 状态。
3	配置关闭模式	可选操作。在**以太网 OAM→DLDP→DLDP 配置**，关闭模式配置为自动或手动。
4	重置 DLDP 状态	可选操作。在**以太网 OAM→DLDP→DLDP 配置**，选择指定的端口或端口配置表中选择所有端口并单击**重置**按钮来恢复他们的状态。

8.7 DLDP 的应用例子

- **网络需求**

1. 设备 A 和设备 B 通过两对光纤连接，这两对光纤交叉连接，如图 8-13 所示。
2. 在检测到单向链路的时候应该断开连接，并且通过 DLDP 来关闭的端口可以在光纤对连接正确后恢复。

- **网络框图**

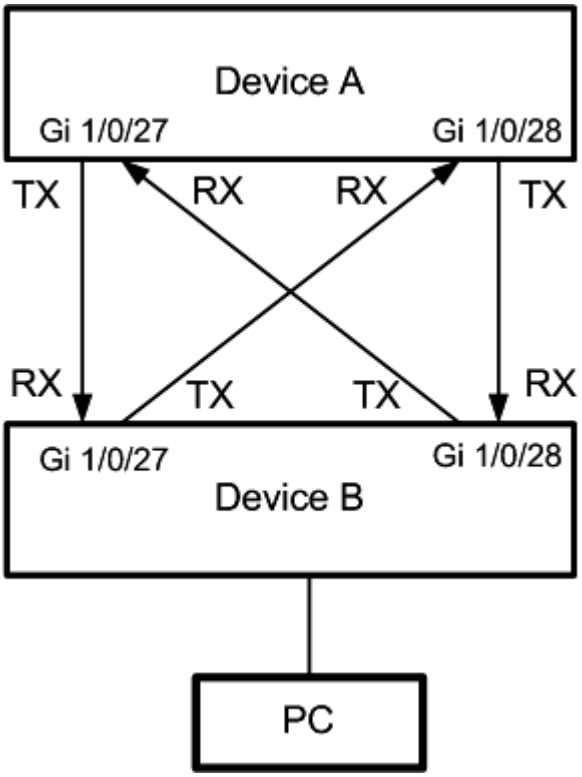


图 8-13 DLDP 应用例子

- **配置过程**

步骤	操作	描述
1	全局使能 DLDP	必选操作。在**以太网 OAM→DLDP→DLDP 配置**，配置设备 A 和 B 的 DLDP 状态。
2	在特定端口上使能 DLDP	必选操作。在**以太网 OAM→DLDP→DLDP 配置**，启用以太网端口 1/0/27 和 1/0/28 的 DLDP。
3	配置关闭模式	必选操作。在**以太网 OAM→DLDP→DLDP 配置**，配置关闭模式。
4	检查端口状态	必选操作。在**以太网 OAM→DLDP→DLDP 配置**，选择端口 1/0/27 和 1/0/28，点击**重置**按钮。

千兆以太网端口 1/0/27 和 1/0/28 中的 DLDP 信息如下所示:

这四个端口连接正确后，选择端口 1/0/27 和 1/0/28，然后单击**重置**按钮来恢复。

第9章 组播管理

➢ 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。数据采用单播（Unicast）方式传输时，服务器会为每一个接收者单独传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，这样将会大量占用网络资源。数据采用广播（Broadcast）方式传输时，系统会把信息一次性的传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如图 8-1 所示。

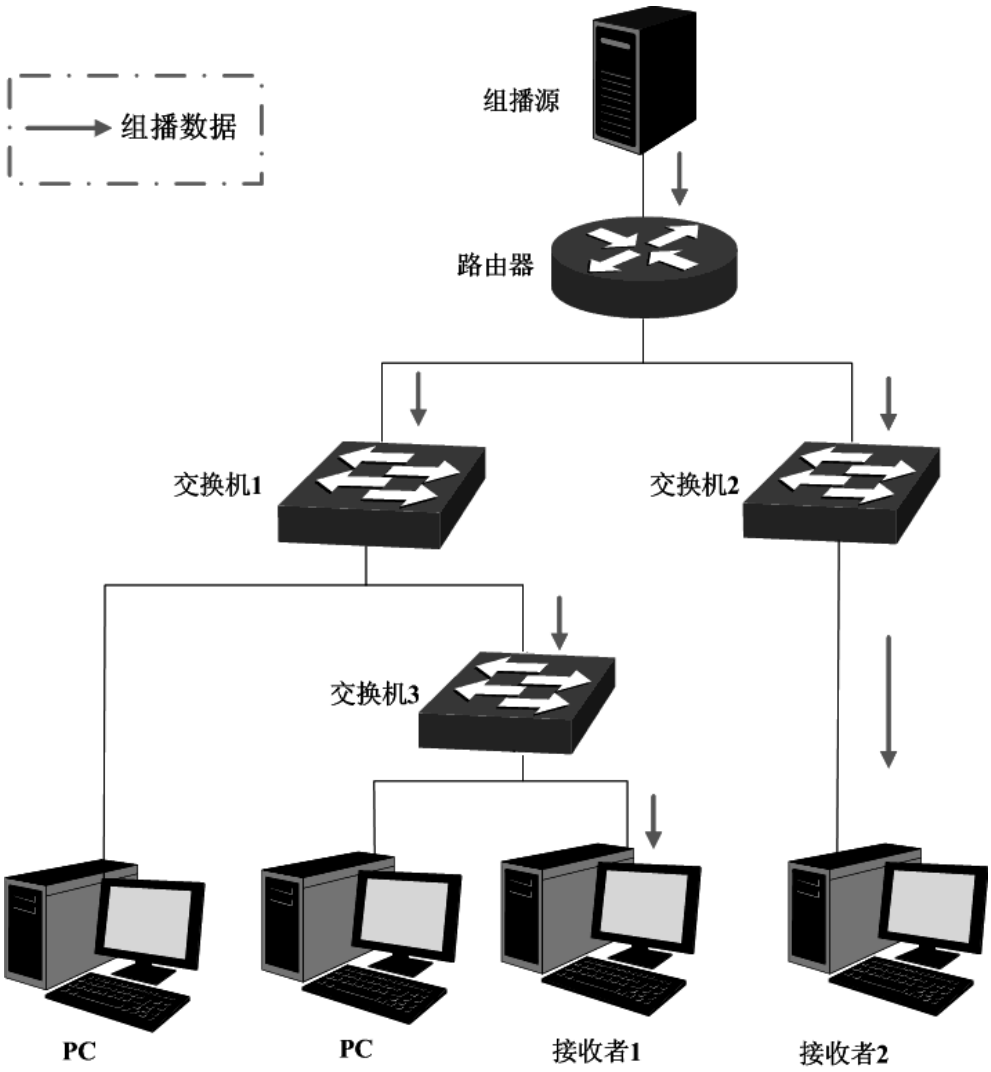


图 8-1 组播传输信息的方式

组播的特点是：

- 服务对象不固定，通常是一对多的关系；
- 把服务对象看成一个组，发送端只需要发送一次数据到相关网络设备即可；

- 每个用户可以随时加入或退出组播组；
- 实时性要求较高，允许一定的丢帧现象发生。

➢ **IPv4 组播地址**

IPv4 组播 IP 地址：

根据 IANA（Internet Assigned Numbers Authority，因特网编号授权委员会）规定，组播报文的 IP 地址使用 D 类 IP 地址，组播 IP 地址范围是 224.0.0.0～239.255.255.255。其中，几个特殊组播 IP 地址段的范围及说明如下：

组播地址范围	说明
224.0.0.0～224.0.0.255	路由协议及其它底层拓扑发现和维护协议的保留地址
224.0.1.0～224.0.1.255	会议及电视会议
239.0.0.0～239.255.255.255	局域网内部使用地址，不能用于 internet

表 8-1 特殊的组播 IP 地址段

IPv4 组播 MAC 地址：

以太网传输单播 IP 报文的时候，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播报文时，传输目标不再是一个具体的接收者，而是一个成员不确定的组，所以需要使用组播 MAC 地址作为目的地址，组播 MAC 地址是一个逻辑的 MAC 地址。

IANA 规定，组播 MAC 地址的高 24bit 位是以 01-00-5E 开头，低 23bit 为组播 IP 地址的低 23bit，映射关系如图 8-2 所示：

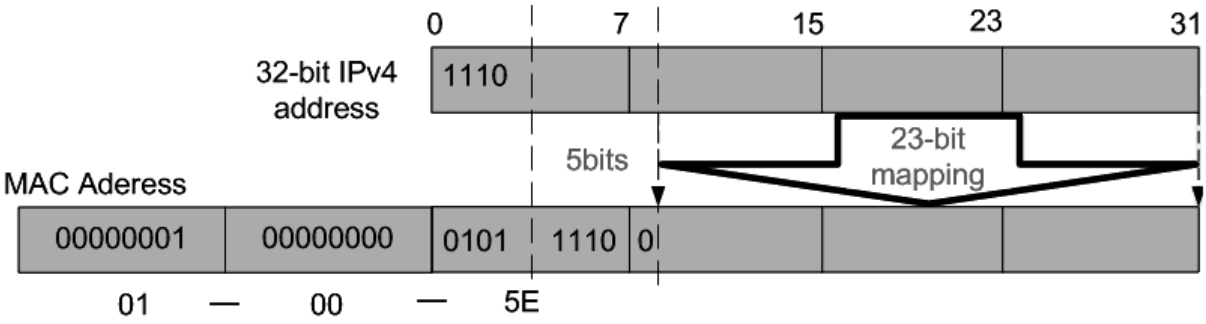


图 8-2 组播 MAC 地址和组播 IP 地址的对应关系

由于 IP 组播地址的高 4bit 是 1110，标识了组播组，而低 28bit 中只有 23bit 被映射到组播 MAC 地址上，这样 IP 组播地址中就会有 5bit 没有使用，从而出现了 32 个 IP 组播地址映射到同一 MAC 地址上的结果。

➢ **组播地址表**

交换机在转发组播数据时是根据组播地址表来进行的。由于组播数据不能跨越 VLAN 传输，因此组播地址表的第一部分是 VLAN ID，当交换机收到组播数据包时，数据包只能在接收端口所在的 VLAN 内转发。组播地址表对应的出口端口不是一个，而是一组端口列表。转发数据时，交换机根据组播数据的目的组播地址查找组播地址表，如果在组播地址表中查不到相应的条目，则把该组播数据广播，即向接收端口所在 VLAN 内的所有端口上转发；如果能查找到对应的条目，则目的地址应该是一组端口列表，于是交换机把这个组播数据复制成多份，每份转发到一个端口，从而完成组播数据的交换。组播地址表一般格式如图 8-3 所示。

VLAN ID	组播 IP	端口

图 8-3 组播地址表

➢ **IGMP 侦听**

网络中的主机通过发送 IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP 侦听（IGMP Snooping）是组播约束机制，交换机用他来完成组播组的动态注册，运行 IGMP 侦听的交换机通过侦听和分析主机与组播路由器之间交互的 IGMP 报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

组播管理模块主要用于配置交换机的组播管理功能，包括 **IGMP 侦听**、**MLD 侦听**、**组播地址表**三个部分。

9.1 IGMP 侦听

➢ **IGMP 侦听的工作过程**

交换机侦听用户主机与路由器之间的交互 IGMP 报文，跟踪组播信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（IGMP Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（IGMP Leave）时，路由器会发送该端口的特定组查询报文（Group-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（IGMP Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

➢ **IGMP 报文**

运行了 IGMP 侦听的交换机对不同类型的 IGMP 报文的处理方法如下。

1. 查询报文（IGMP Query）

由路由器发出，又可分为通用查询报文和特定组查询报文。路由器定时发出通用查询报文，以查询该网段有哪些组播组的成员。当路由器收到 IGMP 离开报文后，会通过接收端口向该组播组发送 IGMP 特定组查询报文，交换机会将此报文转发，以确定该端口中是否还有组播组的其它组成员。

对于通用查询报文，交换机会将此报文通过 VLAN 内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

对于特定组查询报文，交换机要向被查询的组播组的成员转发 IGMP 特定组查询报文。

2. 报告报文（IGMP Report）

由主机发出，当主机想主动加入某一组播组或对路由器查询报文给予响应时产生此种报文。

在收到 IGMP 报告报文时，交换机将此报文通过 VLAN 内的路由器端口转发出去，同时从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

3. 离开报文（IGMP Leave）

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开报文，因此交换机无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送 IGMP 报告报文，因此当其对应的成员端口时间超时后，交换机就会将该端口从相应的组播地址表中删除。运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到 IGMP 离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组查询报文，然后重置成员端口时间为离开滞后时间，离开滞后时间超时后，交换机将此端口从相应的组播地址表中删除。如果删除离开端口后组播组中没有其它组成员存在，则将整个组播组删除。

- **IGMP 侦听的基本概念**

1. 相关端口

路由器端口（Router Port）：交换机上连接路由组播设备的端口。

成员端口（Member Port）：交换机上连接组播组成员的端口。

2. 相关定时器

路由器端口时间：这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是 300 秒。

成员端口时间：这段时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口不再有主机属于组播组。默认是 260 秒。

离开滞后时间：从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。默认是 1 秒。

本功能包括**基本配置**、**端口参数**、**VLAN 参数**、**组播 VLAN**、**查询器配置**、**配置文件配置**、**配置文件绑定**、**报文统计**、**IMGP 认证**九个配置页面。

9.1.1 基本配置

配置本交换机的 IGMP 侦听功能，首先要在本页配置 IGMP 侦听的全局功能和相关参数。

如果交换机收到的组播数据没有在组播地址表内，该组播数据会在 VLAN 内广播；当交换机启用“未知组播报文丢弃”功能后，交换机收到不在组播地址表中的组播数据报文时，会将此报文丢弃，从而节省带宽，并提高系统的处理效率，请根据实际情况配置该功能。

进入页面的方法：组播管理>>IGMP 侦听>>基本配置

图 8-4 基本配置

条目介绍：

- **全局配置**

  IGMP 侦听： 选择是否启用交换机的 IGMP 侦听功能。

  未知组播报文： 选择交换机对未知组播报文的处理方法。

  Report 报文抑制： 选择是否开启 Report 报文抑制功能，如果开启该功能，则特定组播组的第一个 Report 报文将发往路由器端口，接下来的 Report 报文将被抑制，不发往路由器端口。Report 报文抑制功能有助于减少网络中 IGMP 数据包的流量。

- **IGMP 侦听信息**

  描述： 显示 IGMP 侦听的配置项。

  成员： 显示对应配置项的成员。

9.1.2 端口参数

本页用来配置交换机端口的 IGMP 侦听属性。

进入页面的方法：组播管理>>IGMP 侦听>>端口参数

图 8-5 端口参数

条目介绍：

- **端口配置**

选择： 勾选条目配置端口的 IGMP 侦听功能，可多选。

端口号： 显示交换机的端口号。

IGMP 侦听： 选择该端口是否启用 IGMP 侦听功能。

快速离开功能： 当端口启动快速离开功能后，交换机收到 IGMP 离开报文时，直接将该端口从组播组中删除。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口的快速离开功能只能在主机支持 IGMPv2 或 v3 时生效。
- 当快速离开功能与“未知组播报文丢弃”功能同时开启的情况下，如果某个端口下有多个用户，一个用户的快速离开，可能会造成同一组播组中其它用户的组播业务中断。

9.1.3 VLAN 参数

IGMP 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 IGMP 参数。本页用于配置每个 VLAN 的 IGMP 侦听参数。

进入页面的方法：组播管理>>IGMP 侦听>>VLAN 参数

图 8-6 VLAN 参数

条目介绍：

- **VLAN 参数**

VLAN ID： 填写启用 IGMP 侦听功能的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。

成员端口时间： 在所设时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口失效。

静态路由器端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

禁用路由器端口： 选择禁用被配置成路由器端口的端口。

- **VLAN 列表**

选择： 勾选条目配置 VLAN 参数，可多选。

VLAN ID： 显示 VLAN ID。

路由器端口时间： 显示 VLAN 的路由器端口时间。

成员端口时间： 显示 VLAN 的成员端口时间。

静态路由器端口： 显示 VLAN 的静态路由器端口。

动态路由器端口： 显示 VLAN 的动态路由器端口。

禁用路由器端口： 显示 VLAN 内禁止被配置成路由器端口的端口。

注意：

- 当“组播 VLAN”功能启用时，本页的配置将失效。

配置步骤：

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在**组播管理>>IGMP 侦听>>基本配置**、**端口配置**页面，启用交换机的 IGMP 侦听功能和端口的 IGMP 侦听功能。
2	配置 VLAN 的组播参数	可选操作。在**组播管理>>IGMP 侦听>>VLAN 参数**页面，为交换机的各个 VLAN 配置组播参数。 没有配置组播参数的 VLAN，表示没有在该 VLAN 内开启 IGMP 侦听功能，那么该 VLAN 中的组播数据会广播。

9.1.4 组播 VLAN

对于传统的组播数据转发方式，当处于不同 VLAN 的用户加入同一个组播组时，组播路由器会为每个包含接收者的 VLAN 复制并转发一份组播数据。这样的组播点播方式，浪费了大量的带宽。

通过配置组播 VLAN，可以有效的解决上述问题。将交换机的端口加入到组播 VLAN 中并启用 IGMP 侦听功能，使不同 VLAN 内的用户共用一个组播 VLAN 接收组播数据，组播数据只在组播 VLAN 内进行传输，从而节省了带宽。同时由于组播 VLAN 与普通的 VLAN 完全隔离，安全和带宽都得以保证。

配置组播 VLAN 之前，需要在 **802.1Q VLAN** 功能处预先配置一个 VLAN 作为组播 VLAN，并将相应的端口加入此 VLAN 中。组播 VLAN 启用后，在 **VLAN 参数**页面中为其它 VLAN 配置的组播参数将失效，即组播数据不再通过除组播 VLAN 以外的其它 VLAN 转发。

进入页面的方法：组播管理>>IGMP 侦听>>组播 VLAN

图 8-7 组播 VLAN

条目介绍：

- **组播 VLAN**

组播 VLAN： 选择是否启用组播 VLAN。

VLAN ID： 填写组播 VLAN 的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。

成员端口时间： 在所设时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口失效。

替换源 IP 指定 IGMP 数据包源 IP 地址被替换后的 IP 地址。

动态路由器端口： 显示组播 VLAN 的动态路由器端口。

静态路由器端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

禁用路由器端口： 选择禁用被配置成路由器端口的端口。

注意：

- 路由器端口必须均在组播 VLAN 中，否则成员端口无法收到组播数据。
- 必须在 802.1Q VLAN 功能处完成端口的相关 VLAN 属性配置，组播 VLAN 才能正常运行。
- 组播 VLAN 中的成员端口的端口类型推荐为 GENERAL。
- 组播 VLAN 中的路由器端口的端口类型必须配置为 TRUNK 或者是出口规则为“带 tag”的 GENERAL 端口，否则组播 VLAN 内的所有的组播成员端口都无法接收到组播数据。
- 当建立了组播 VLAN 后，所有的 IGMP 报文均只在组播 VLAN 内处理。

配置步骤：

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在**组播管理>>IGMP 侦听>>基本配置**、**端口配置**页面，启用交换机的 IGMP 侦听功能和端口的 IGMP 侦听功能。
2	创建组播 VLAN	必选操作。在 **VLAN>>802.1Q VLAN** 页面，创建组播 VLAN，并将所有成员端口和路由器端口加入该 VLAN 中。 ● 配置成员端口的端口类型为 GENERAL。 ● 配置路由端口的端口类型为 TRUNK 或出口规则为“带 tag”的 GENERAL。
3	配置组播 VLAN 的参数	可选操作。进入**组播管理>>IGMP 侦听>>组播 VLAN** 页面，启用组播 VLAN 并配置组播 VLAN 的组播参数。 时间参数建议使用默认值。
4	查看配置情况	若配置成功，则在**组播管理>>IGMP 侦听>>基本配置**页面中的“已启用的 VLAN”条目处，显示组播 VLAN 的 VLAN ID。

组网应用：

➢ **组网需求**

组播源通过路由器转发组播数据，组播数据流通过交换机被转发到接收端用户 A 和用户 B。

路由器：WAN 口与组播源相连；LAN 口与交换机相连，且通过 VLAN3 转发数据。

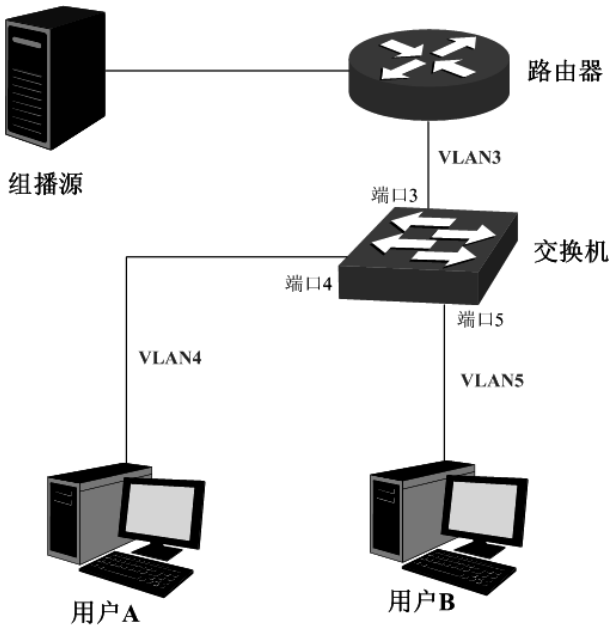
交换机：端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4 转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

用户 A：与交换机的端口 4 相连。

用户 B：与交换机的端口 5 相连。

配置组播 VLAN，使用户 A 和用户 B 通过组播 VLAN 接收组播数据。

➢ **组网图**



➢ **配置步骤**

配置交换机：

步骤	操作	说明
1	创建 VLAN	在 **VLAN>>802.1Q VLAN** 功能处，创建 VLAN3、4、5，并将 VLAN3 的描述填写为“组播 VLAN”。
2	配置端口属性	在 **VLAN>>802.1Q VLAN** 功能处。 配置端口 3 的端口类型为 GENERAL，出口规则 TAG，并加入 VLAN3、4、5 中。 配置端口 4 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、4 中。 配置端口 5 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、5 中。
3	启用 IGMG 侦听	在**组播管理>>IGMP 侦听>>基本配置**页面，启用 IGMP 侦听功能。 在**组播管理>>IGMP 侦听>>端口配置**页面，启用端口 3、4、5 的 IGMP 侦听功能。
4	启用组播 VLAN	在**组播管理>>IGMP 侦听>>组播 VLAN** 页面，启用组播 VLAN，并配置组播 VLAN 的 VLAN ID 为 3，其它参数建议使用默认值。
5	检查组播 VLAN	在**组播管理>>IGMP 侦听>>基本配置**页面，“IGMP 侦听信息”处，“已启用的端口”显示为 3、4、5，“已启用的 VLAN”显示为 3。

9.1.5 查询器配置

在运行了 IGMP 的组播网络中，会有一台三层组播设备充当 IGMP 查询器，负责发送 IGMP 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。而网络中的二层设备可以通过侦听三层组播设备与主机之间交互的 IGMP 报文来建立二层组播转发表项，实现二层组播转发。但是，在一个没有三层组播设备的网络中，由于没有设备负责 IGMP 查询

器的功能，这样网络中不会周期性存在 IGMP 协议交互的报文，二层设备也无法通过侦听 IGMP 报文来建立二层的组播转发表项。为了解决这个问题，可以在二层设备上使用 IGMP 侦听查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。本页面主要用于配置 IGMP 侦听查询器的相关参数。

进入页面的方法：组播管理→IGMP 侦听→查询器配置

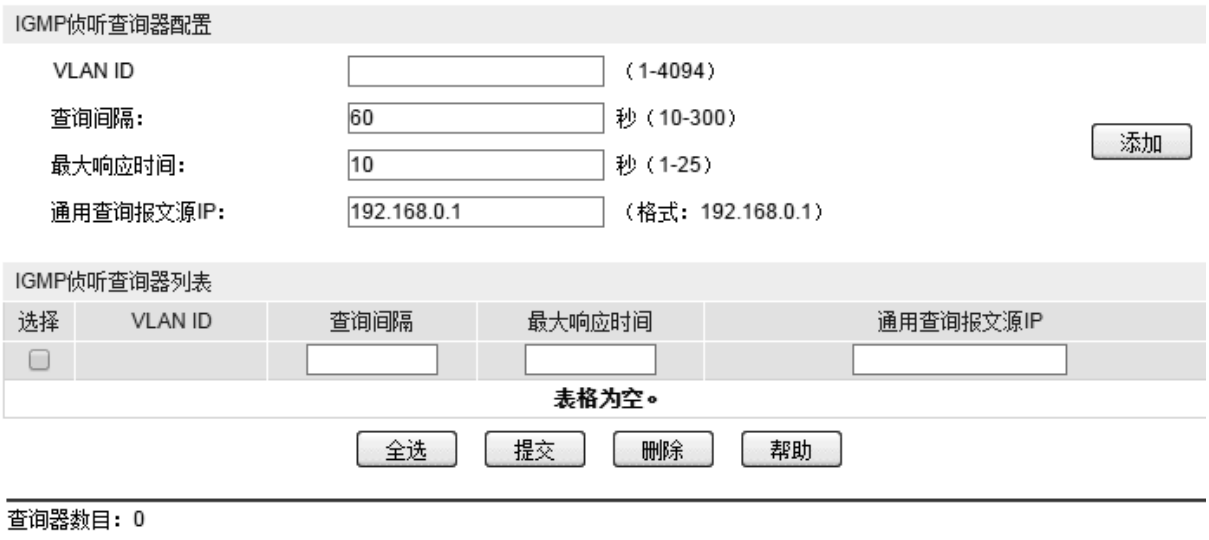


图 9-1 查询配置

条目介绍:

- **IGMP 侦听查询器配置**

  VLAN ID： 输入需要启动查询器的 VLAN ID。

  查询时间间隔： 输入查询间隔时间。查询器会按照间隔时间发送通用查询报文。

  最大响应时间： 输入主机响应查询器发送的通用查询报文的最大响应时间。

  通用查询报文源 IP： 输入通用查询报文的源 IP 地址。不可以是组播 IP 或者广播 IP。

- **IGMP 侦听查询器表**

  选择： 选择需要配置的 VLAN 条目。

  VLAN ID： 显示 VLAN ID。

  查询间隔： 显示查询间隔。

  最大响应时间： 显示最大响应时间。

  通用查询报文源 IP： 显示通用查询报文的源 IP 地址。

9.1.6 配置文件配置

在启用了 IGMP 侦听功能后，您可以通过配置组播过滤，来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。

进入页面的方法：组播管理→IGMP 侦听→配置文件配置

图 9-2 配置文件

条目介绍:

- **创建配置文件**

  配置文件 ID: 输入您想创建的配置文件 ID，区间为 1-999。

  模式: 配置文件的过滤模式。
  允许：只允许加入配置文件中 IP 地址范围内的组播组。
  拒绝：拒绝加入配置文件中 IP 地址范围内的组播组。

- **显示设置**

  显示设置: 选择显示配置文件条目的规则。
  全部：显示所有配置条目。
  配置文件 ID：显示所选 ID 对应的配置条目。

- **IGMP 配置文件信息**

  选择: 选择需要进行配置的条目。

  配置文件 ID: 显示配置文件 ID。

  模式: 显示配置文件的过滤模式。
  允许：只允许加入配置文件中 IP 地址范围内的组播组。
  拒绝：拒绝加入配置文件中 IP 地址范围内的组播组。

  绑定端口: 显示配置文件所绑定的端口。

  操作: 点击编辑按钮可以配置该配置文件的模式和过滤 IP 地址区间。

9.1.7 配置文件绑定

当交换机接收到IGMP报文时，检查绑定到接入端口的配置文件ID以确定端口是否可以加入组播组。如果没有过滤组播IP，交换机则将该端口加入到组播组的转发端口列表中，否则交换机将丢弃IGMP报文信息。您可以通过设置组播组来让不同用户访问。

进入页面的方法：组播管理→IGMP 侦听→配置文件绑定

图 9-3 配置文件绑定

条目介绍:

- **配置文件与最大加入组数目绑定**

选择： 选择所需的端口进行配置。可多选。

端口： 显示端口号。可多选。

配置文件 ID： 与端口绑定的配置文件 ID。

最大加入组数目： 端口允许加入的最大组播组数目。

溢出操作： 当端口所加入组播组数等于或超过最大组播组数时采取的动作。
丢弃：不再加入新的组播组，接收到的报文信息将被丢弃。
替换：允许加入新的组播组，已有的最小组播组将被替换。

LAG 显示端口所属的汇聚组。

- **配置过程:**

步骤	操作	描述
1	创建配置文件	必选操作。在组播管理→IGMP 侦听→配置文件配置页面上配置 IGMP 配置文件 ID 和模式。
2	配置 IP 范围	必选操作。点击组播管理→IGMP 侦听→配置文件配置页面上的 IGMP 配置文件信息的编辑按钮，配置 IGMP 配置文件的模式和 IP 范围。
3	配置文件绑定	可选操作。在组播管理→IGMP 侦听→配置文件绑定页面上进行绑定文件绑定。

9.1.8 报文统计

您可以在本页查看交换机各端口的组播报文流量信息，便于您监控网络中 IGMP 报文。

进入页面的方法：组播管理→IGMP 侦听→报文统计

图 9-4 报文统计

以下的条目显示在屏幕上:

- **自动刷新**

自动刷新： 选择启用/禁用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

- **IGMP 统计**

端口： 显示交换机的端口号。

查询报文： 显示端口接收到的查询报文的数目。

报告报文（V1）： 显示端口接收到的 IGMPv1 报告报文的数目。

报告报文（V2）： 显示端口接收到的 IGMPv2 报告报文的数目。

报告报文（V3）： 显示端口接收到的 IGMPv3 报告报文的数目。

离开报文： 显示端口接收到的离开报文的数目。

错误报文： 显示端口接收到的错误报文的数目。

9.1.9 IGMP 认证

IGAP（Internet Group membership Authentication Protocol，IGMP 认证协议）是一个组播认证协议，用来对想要加入受限组播源的用户进行认证。

进入页面的方法：组播管理→IGMP 侦听→IGMP 认证

图 9-5 IGMP 认证

以下的条目显示在屏幕上:

- **计费配置**

  认证计费： 启用或禁用 IGMP 认证计费功能。

- **端口配置**

  选择： 选择所需的端口进行配置。可多选。

  端口号： 显示交换机的端口号。

IGMP 认证： 选择启用或禁用端口的 IGMP 认证功能。

LAG： 显示端口所属的汇聚组。

注意:

IGMP 身份验证功能只有在启用 AAA 功能并配置 RADIUS 服务器时才会生效。如何启用 AAA 功能和配置 RADIUS 服务器，请参阅 13.11 AAA。

9.2 MLD 侦听

- **MLD** 侦听

MLD Snooping（Multicast Listener Discovery Snooping，MLD 侦听）是运行在交换机上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。启用 MLD 侦听功能可以有效地避免组播数据在网络中广播。启用 MLD 侦听，IPv6 组播数据可以选择性地转发到希望接收数据的端口列表，避免产生泛洪。IPv6 中的 MLD 侦听类似于 IPv4 中的 IGMP 侦听功能。

运行 MLD 侦听功能的交换机会侦听用户主机与路由器之间的交互 MLD 报文，跟踪 MLD 信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（MLD Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（MLD Done Leave）时，路由器会发送该端口的特定组播地址查询报文（Multicast-Address-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（MLD Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

- **MLD 侦听的基本概念**

1. MLD 消息

MLD 查询报文：由 MLD 路由器发出，查询报文包括通用查询报文和特定组播地址查询报文。

MLD 报告报文：当主机想主动加入某一组播组或对路由器查询报文给予响应时，它将产生此种报文。

MLD 离开报文：当主机想离开一个组播组，它将发送一个 MLD 离开报文来通知 IPv6 组播路由器。

2. 相关端口

路由器端口：交换机上连接 MLD 路由器的端口

成员端口：交换机上连接组播组成员的端口。

3. 相关定时器

路由器端口老化时间：这段时间内，如果交换机没从路由器端口接收到 MLD 查询报文，就认为该路由器端口失效。默认是 300 秒。

成员端口老化时间：这段时间内，如果交换机没有从成员端口接收到 MLD 报告报文，就认为该成员端口不再有主机属于多播组。默认是 260 秒。

通用查询间隔：路由器发送通用查询报文的时间间隔。

最后监听成员查询间隔：交换机发出特定组播地址查询报文的时间间隔。

最后监听成员查询次数：如果 MLD 报告报文没有得到回应，交换机在组播地址老化之前发送的特定组播地址查询报文的数量。

➢ **MLD 侦听过程**

- 通用查询

MLD 路由器会定期发送 MLD 通用查询报文来查询组播组是否有包含成员。在接收 MLD 通用查询报文后，交换机会将此报文通过 VLAN 内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

- 成员报告

当主机想主动加入某一组播组或对路由器 MLD 查询报文给予响应时，主机会发出 MLD 报告报文。

在收到 MLD 报告报文时，交换机将此报文通过 VLAN 内的路由器端口转发出去，同时从该报文中解析出主机要加入的组播组地址。如果组播组不存在，将会创建新的组播组条目。交换机同时会对该报文的接收端口做相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

- 成员离开

主机离开组播组时，会通过发送 MLD 离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到 MLD 离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组播地址查询报文。用户可以根据特定组播地址查询报文的数量和时间间隔来控制一个端口的成员是否被移除。如果在交换机最大响应时间内没有收到来自该端口的报告信息，该端口将从组播组中删除。如果被删除的端口是组播组的最后一个成员，那么组播组也会被删除。交换机将把 MLD 离开报文发送给 VLAN 路由器端口。

在 IPv6 中，2 层交换机可以使用 MLD 侦听来限制组播流量的泛洪，IPv6 组播数据有选择地转发到要接收数据的端口列表。

本功能包括**基本配置**、**端口参数**、**VLAN 参数**、**组播 VLAN**、**查询器配置**、**配置文件配置**、**配置文件绑定**、**报文统计**八个配置页面。

9.2.1 基本配置

配置本交换机的 MLD 侦听功能，首先要在本页配置 MLD 侦听的全局功能和相关参数。

进入页面的方法：组播管理→MLD 侦听→基本配置

图 9-6 侦听配置

以下的条目显示在屏幕上:

- **全局配置**

MLD 侦听： 选择是否启用交换机的 MLD 侦听功能。

未知组播报文： 选择交换机对未知组播报文的处理方法。

Report 报文抑制： 选择是否开启 Report 报文抑制功能，如果开启该功能，则特定组播组的第一个 Report 报文将发往路由器端口，接下来的 Report 报文将被抑制，不发往路由器端口。Report 报文抑制功能有助于减少网络中 IGMP 数据包的流量。

路由器端口时间： 在所设时间内，如果交换机没从路由器端口接收到 MLD 查询报文，就认为该路由器端口失效。

成员端口时间： 在所设时间内，如果交换机没有从成员端口接收到 MLD 报告报文，就认为该成员端口失效。

最后监听成员查询次数： 输入最后监听成员查询次数。当组播组没有其他组播成员端口，将会发送该次数的特定组查询报文检查是否还有其他组播成员。

- **MLD 侦听信息**

描述： 显示 MLD 侦听的配置项。

成员文： 显示对应配置项的成员。

注意:

1. 在 8.2.3 VLAN 配置中，路由器端口时间和成员端口时间的配置会覆盖本章节的全局配置。
2. 在创建一个组播 VLAN 之前，您需要在 8.2.3 VLAN 配置中启用 MLD 侦听功能。

组播 VLAN 的配置过程

步骤	操作	描述
1	创建 VLAN。	必选操作。在 **VLAN>>802.1Q VLAN** 功能处，点击创建按钮创建一个 VLAN，输入 VLAN ID 和 VLAN 的描述，并指定它的成员端口。
2	全局启用 MLD 侦听。	必选操作。在**组播管理>>MLD 侦听>>基本配置**页面，全局启用交换机的 MLD 侦听功能。
3	启用 VLAN 中的 MLD 侦听。	必选操作。在**组播管理→MLD 侦听→VLAN 参数配置**页面，指定 VLAN ID。
4	启用组播 VLAN。	必选操作。在**组播管理→MLD 侦听→组播 VLAN** 页面，使能组播 VLAN 功能并指定组播 VLAN ID。

9.2.2 端口参数

本页用来配置交换机端口的 MLD 侦听属性。

进入页面的方法：组播管理>>MLD 侦听>>端口参数

图 9-7 端口配置

以下的条目显示在屏幕上:

- **端口配置**

选择： 勾选条目配置端口的 MLD 侦听功能，可多选。

端口号： 显示交换机的端口号。

MLG 侦听： 选择该端口是否启用 MLD 侦听功能。

快速离开功能： 端口启动快速离开功能后，交换机收到 MLD 离开报文时，直接将该端口从组播组中删除。

LAG： 显示端口所属的汇聚组。

9.2.3 VLAN 参数

MLD 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 MLD 参数。本页用于配置每个 VLAN 的 MLD 侦听参数。

进入页面的方法：组播管理>>MLD 侦听>>VLAN 参数

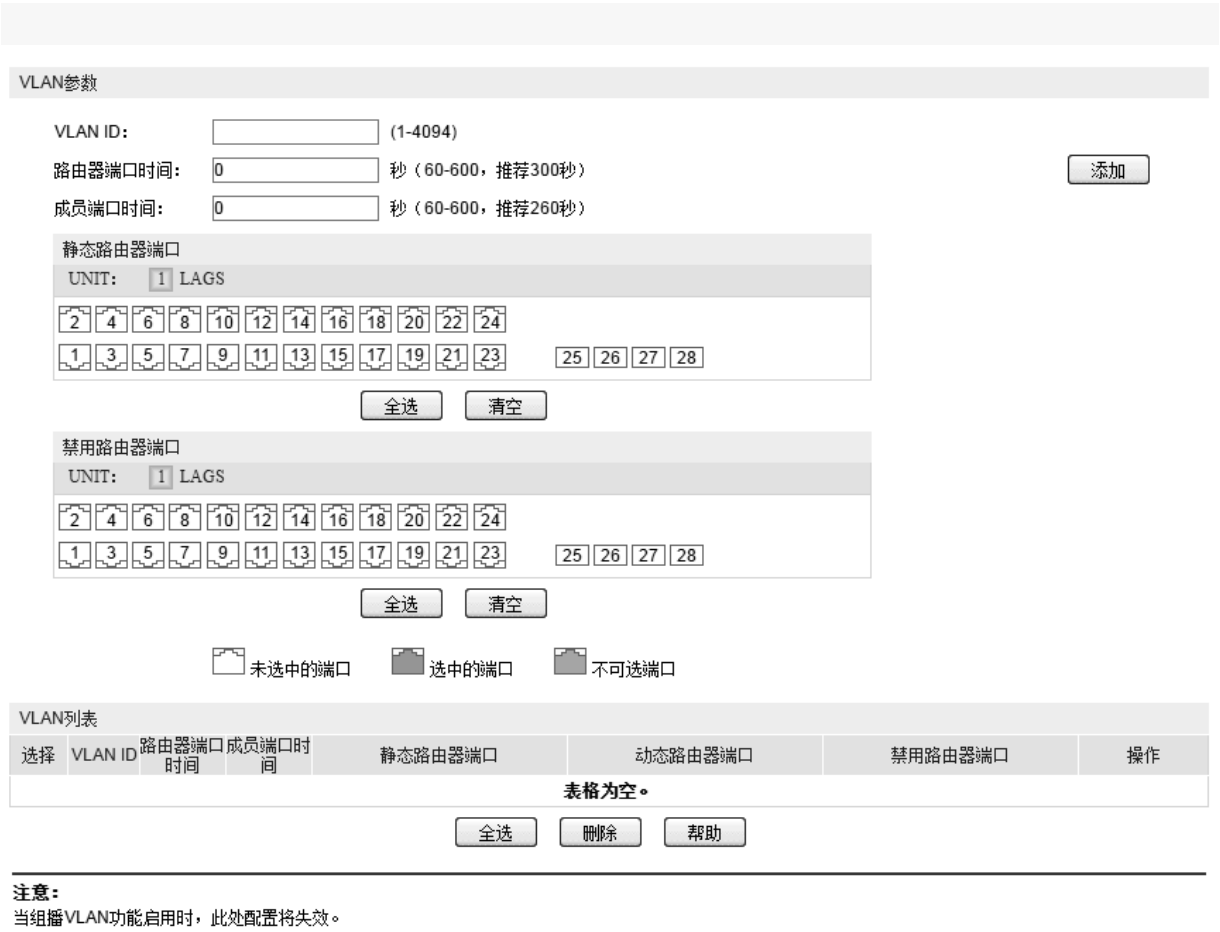


图 9-8 VLAN 配置

条目介绍：

- **VLAN 配置**

VLAN ID： 填写启用 MLD 侦听功能的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。

成员端口时间： 在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。

静态路由器端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

禁用路由器端口： 选择禁用配置成路由器端口的端口。

- **VLAN 列表**

选择： 勾选条目配置 VLAN 参数，可多选。

VLAN ID： 显示 VLAN ID。

路由器端口时间： 显示 VLAN 的路由器端口时间。

成员端口时间： 显示 VLAN 的成员端口时间。

静态路由器端口： 显示 VLAN 的静态路由器端口。

动态路由器端口： 显示 VLAN 的动态路由器端口。

禁用路由器端口： 显示 VLAN 内禁止被配置成路由器端口的端口。

注意:

1. 在 9.2.1 基本配置中全局启用 MLD 侦听功能和在第六章中创建 VLAN 后，VLAN 中的 MLD 侦听会生效。
2. 当为 VLAN 设置路由器端口时间或成员端口时间时，该值将全局覆盖 9.2.1 基本配置中的配置。

9.2.4 组播 VLAN

对于传统的组播数据转发方式，当处于不同 VLAN 的用户加入同一个组播组时，组播路由器会为每个包含接收者的 VLAN 复制并转发一份组播数据。这样的组播点播方式，浪费了大量的带宽。

通过配置组播 VLAN，可以有效的解决上述问题。将交换机的端口加入到组播 VLAN 中并启用 MLD 侦听功能，使不同 VLAN 内的用户共用一个组播 VLAN 接收组播数据，组播数据只在组播 VLAN 内进行传输，从而节省了带宽。同时由于组播 VLAN 与普通的 VLAN 完全隔离，安全和带宽都得以保证。

配置组播 VLAN 之前，需要在 **802.1Q VLAN** 功能处预先配置一个 VLAN 作为组播 VLAN，并将相应的端口加入此 VLAN 中。组播 VLAN 启用后，在 **VLAN 参数**页面中为其它 VLAN 配置的组播参数将失效，即组播数据不再通过除组播 VLAN 以外的其它 VLAN 转发。

进入页面的方法：组播管理>>MLD 侦听>>组播 VLAN

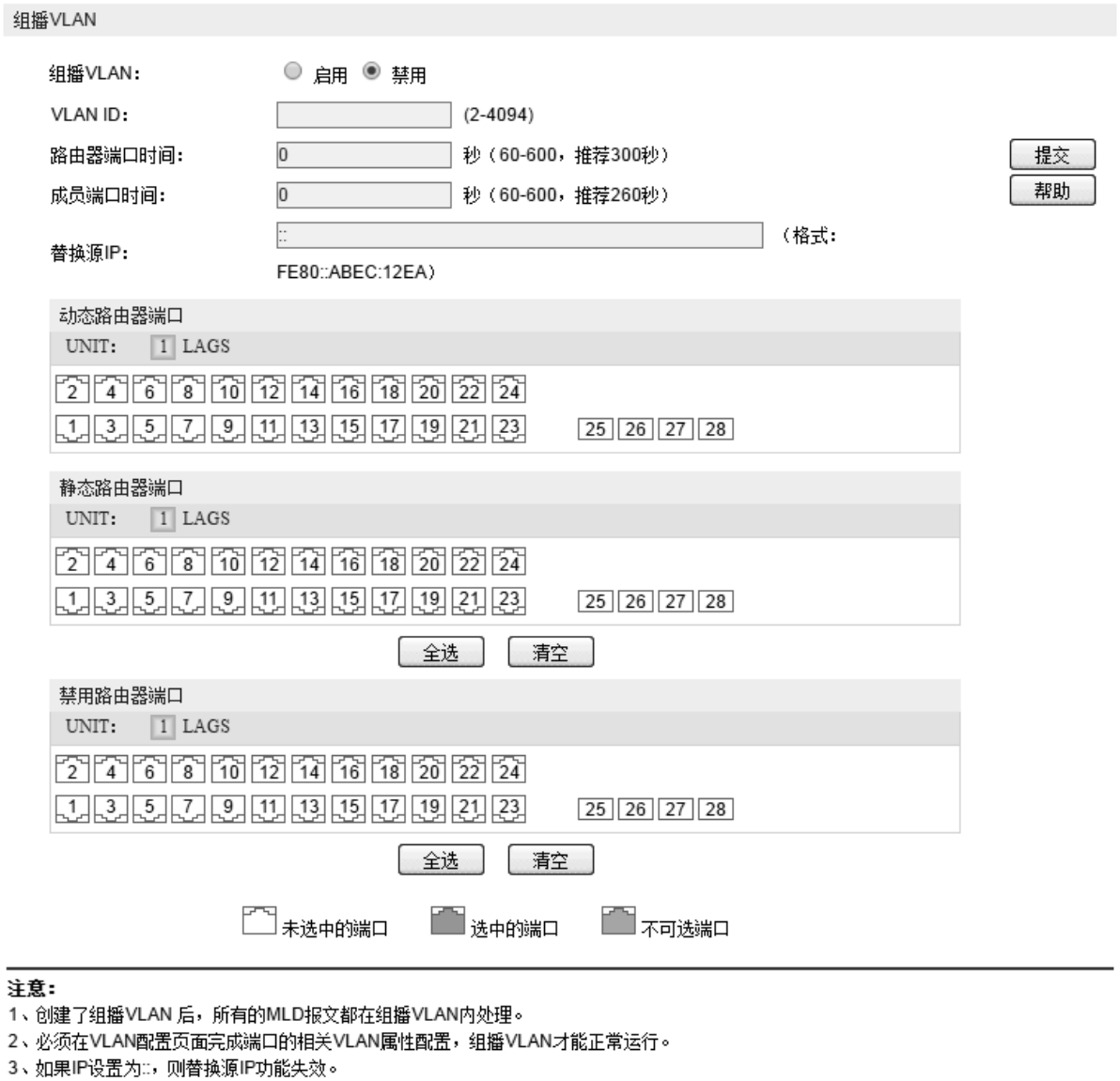


图 9-9 组播 VLAN 配置

条目介绍：

- **组播 VLAN**

组播 VLAN： 选择是否启用组播 VLAN。

VLAN ID： 填写组播 VLAN 的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。

成员端口时间： 在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。

替换源 IP： 指定 IGMP 数据包源 IP 地址被替换后的 IP 地址。

静态路由器端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

动态路由器端口： 显示组播 VLAN 的动态路由器端口。

禁用路由器端口： 选择禁用被配置成路由器端口的端口。

注意:

1. 路由器端口必须均在组播 VLAN 中，否则成员端口无法收到组播数据。
2. 必须在 802.1Q VLAN 功能处完成端口的相关 VLAN 属性配置，组播 VLAN 才能正常运行。
3. 组播 VLAN 中的成员端口的端口类型推荐为 GENERAL。
4. 组播 VLAN 中的路由器端口的端口类型必须配置为 TRUNK 或者是出口规则为“带 tag”的 GENERAL 端口，否则组播 VLAN 内的所有的组播成员端口都无法接收到组播数据。
5. 当建立了组播 VLAN 后，所有的 MLD 报文均只在组播 VLAN 内处理。

9.2.5 查询器配置

在运行了 MLD 的组播网络中，会有一台三层组播设备充当 MLD 查询器，负责发送 MLD 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。而网络中的二层设备可以通过侦听三层组播设备与主机之间交互的 MLD 报文来建立二层组播转发表项，实现二层组播转发。但是，在一个没有三层组播设备的网络中，由于没有设备负责 MLD 查询器的功能，这样网络中不会周期性存在 MLD 协议交互的报文，二层设备也无法通过侦听 MLD 报文来建立二层的组播转发表项。为了解决这个问题，可以在二层设备上使用 MLD 侦听查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。本页面主要用于配置 MLD 侦听查询器的相关参数。

进入页面的方法：组播管理→MLD 侦听→查询器配置

图 9-10 侦听配置

以下的条目显示在屏幕上:

- **MLD 侦听查询器配置**

VLAN ID： 输入需要启动查询器的 VLAN ID。

查询间隔： 输入查询间隔时间。查询器会按照间隔时间发送通用查询报文。

最大响应时间： 输入主机响应查询器发送的通用查询报文的最大响应时间。

通用查询报文源 IP： 输入通用查询报文的源 IP 地址。不可以是组播 IP 或者广播 IP。

- **MLD 侦听查询器列表**

VLAN ID： 显示 VLAN ID。

查询间隔： 显示查询间隔。

最大响应时间： 显示最大响应时间。

通用查询报文源 IP： 显示通用查询报文源 IP 地址。

注意:

MLD 侦听查询器不参与 MLD 查询器选择，但由于相对较小的 IP 地址，MLD 侦听查询器会影响 IPv6 网络中 MLD 查询器选择。

9.2.6 配置文件配置

在启用了 MLD 侦听功能后，您可以通过配置组播过滤，来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。

进入页面的方法：组播管理→MLD 侦听→配置文件配置

图 9-11 配置文件

条目介绍：

- **创建 MLD 配置文件**

配置文件 ID： 输入您想创建的配置文件 ID，区间为 1-999。

模式： 配置文件的过滤模式。
允许：只允许加入配置文件中 IP 地址范围内的组播组。
拒绝：拒绝加入配置文件中 IP 地址范围内的组播组。

- **显示设置**

显示设置： 选择显示配置文件条目的规则。
全部：显示所有配置条目。
配置文件 ID：显示所选 ID 对应的配置条目。

- **MLD 配置文件信息**

选择： 选择需要进行配置的条目。

配置文件 ID： 显示配置文件 ID。

模式： 显示配置文件的过滤模式。
允许：只允许加入配置文件中 IP 地址范围内的组播组。
拒绝：拒绝加入配置文件中 IP 地址范围内的组播组。

绑定端口： 显示配置文件所绑定的端口。

操作： 点击编辑按钮可以配置该配置文件的模式和过滤 IP 地址区间。

9.2.7 配置文件绑定

当交换机接收到 MLD 报文时，检查绑定到接入端口的配置文件 ID 以确定端口是否可以加入组播组。如果没有过滤组播 IP，交换机则将该端口加入到组播组的转发端口列表中，否则交换机将丢弃 MLD 报文信息。您可以通过设置组播组来让不同用户访问。

进入页面的方法：组播管理→MLD 侦听→配置文件绑定

图 9-12 配置文件

条目介绍:

- **配置文件和最大加入组数目绑定**

选择: 选择所需的端口进行配置。可多选。

端口: 显示端口号。可多选。

配置文件 ID: 与端口绑定的配置文件 ID。

最大加入组数目: 端口允许加入的最大组播组数目。

溢出操作: 当端口所加入组播组数等于或超过最大组播组数时采取的动作。
丢弃：不再加入新的组播组，接收到的报文信息将被丢弃。
替换：允许加入新的组播组，已有的最小组播组将被替换。

LAG 显示端口所属的汇聚组。

- **配置过程:**

步骤	操作	描述
1	创建配置文件	必选操作。在组播管理→MLD 侦听→配置文件配置页面上配置 IGMP 配置文件 ID 和模式。

2	配置 IP 范围	必选操作。点击组播管理→IGMP 侦听→配置文件配置页面上的 IGMP 配置文件信息的编辑按钮，配置 IGMP 配置文件的模式和 IP 范围。
3	配置文件绑定	可选操作。在组播管理→MLD 侦听→配置文件绑定页面上进行绑定文件绑定。

9.2.8 报文统计

您可以在本页查看交换机各端口的组播报文流量信息，便于您监控网络中 MLD 报文。

进入页面的方法：组播管理→MLD 侦听→报文统计

图 9-13 报文统计

以下的条目显示在屏幕上:

- **自动更新**

自动更新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

- **MLD 统计**

端口： 显示交换机的端口号。

查询报文： 显示端口接收到的查询报文的数目。

报告报文（V1）： 显示端口接收到的 MLDv1 报告报文的数目。

报告报文（V2）： 显示端口接收到的 MLDv2 报告报文的数目。

离开报文： 显示端口接收到的离开报文的数目。

错误报文： 显示端口接收到的错误报文的数目。

9.3 组播地址表

在网络中，信息接收者可以加入各自所需的组播组，交换机在转发组播数据时是根据组播地址表来进行的。

本功能包括 **IPv4 组播地址表**、**IPv4 静态组播地址表**、**IPv6 组播地址表**和 **IPv6 静态组播地址表**四个配置页面。

9.3.1 IPV4 组播地址表

在本页可以查看到交换机中已存在的所有 IPv4 组播地址表信息。组播地址范围是 224.0.0.0～239.255.255.255，可以加入的有效组播地址范围是 224.0.1.0～239.255.255.255。

进入页面的方法：组播管理>>组播地址表>>IPV4 组播地址表

图 8-8 地址表显示

条目介绍：

- **显示设置**

显示设置： 选择组播地址表的显示规则，可以帮助您快速查找到所需的条目。

- 全部: 显示全部组播 IP 条目。
- 组播 IP：设置欲查找条目需包含的组播 IP 地址信息。
- VLAN ID：设置欲查找条目需包含的 VLAN ID 信息。
- 端口：设置欲查找条目需包含的端口。

- **组播 IP 表**

组播 IP： 显示组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

9.3.2 IPv4 静态组播地址表

IPv4 静态组播地址表不是通过 IGMP 侦听学习到的，不受动态组播组及组播过滤的影响，对于某些固定的组播组，可以提高数据传输质量并增加安全性。

进入页面的方法：组播管理>>组播地址表>>IPv4 静态组播地址表

图 8-9 静态地址表

条目介绍：

- **新建条目**

组播 IP： 填写静态绑定的组播 IP 地址。

VLAN ID： 填写组播 IP 对应的 VLAN ID。

转发端口： 填写组播 IP 的转发端口。

- **显示设置**

显示设置： 选择静态组播IP表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：显示全部静态组播 IP 表条目。
- 组播 IP：设置欲查找条目需包含的组播 IP 地址信息。
- VLAN ID：设置欲查找条目需包含的 VLAN ID 信息。
- 端口：设置欲查找条目需包含的端口。

➢ **静态组播 IP 地址表**

选择： 勾选条目进行删除，可多选。

组播 IP： 显示绑定的组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

9.3.3 IPv6 组播地址表

在本页可以查看到交换机中已存在的所有 IPv6 组播地址表信息。

进入页面的方法：组播管理>>组播地址表>>IPV6 组播地址表

图 9-14 IPv6 组播列表

以下的条目显示在屏幕上:

➢ **显示设置**

显示设置： 选择组播地址表的显示规则，可以帮助您快速查找到所需的条目。

- 全部: 显示全部组播 IP 条目。
- 组播 IP：设置欲查找条目需包含的组播 IP 地址信息。
- VLAN ID：设置欲查找条目需包含的 VLAN ID 信息。
- 端口：设置欲查找条目需包含的端口。

➢ **组播 IP 表**

组播 IP： 显示组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

9.3.4 IPv6 静态组播地址表

IPv6 静态组播地址表不是通过 MLD 侦听学习到的，不受动态组播组及组播过滤的影响，对于某些固定的组播组，可以提高数据传输质量并增加安全性。

进入页面的方法：组播管理>>组播地址表>>IPv6 静态组播地址表

图 9-15 IPv6 组播列表

以下的条目显示在屏幕上:

- **新建条目**

  组播 IP： 填写静态绑定的组播 IP 地址。

  VLAN ID： 填写组播 IP 对应的 VLAN ID。

  转发端口： 填写组播 IP 的转发端口。

- **显示设置**

  显示设置： 选择静态组播 IP 表的显示规则，可以帮助您快速查找到所需的条目。
  - 全部：显示全部静态组播 IP 表条目。
  - 组播 IP：设置欲查找条目需包含的组播 IP 地址信息。
  - VLAN ID：设置欲查找条目需包含的 VLAN ID 信息。
  - 端口：设置欲查找条目需包含的端口。

- **静态组播表**

选择： 勾选条目进行删除，可多选。

组播 IP： 显示绑定的组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

注意:

组播条目的最大数量是 1000。IPv4 组播表和 IPv6 组播表共享 1000 的总条目数。

第10章 路由

在网络中通常由传统路由器或者运行了路由协议的以太网交换机实现不同网络间的数据转发。路由是指路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径上的最后一个路由节点则将数据转发给目标主机。

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。常用的路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。路由表中的每一个路由条目基本都包含如下基本属性：

- 目的网络地址：用于标识该条路由条目所指向的目标网络。
- 子网掩码：用于标识目标网络的子网掩码。
- 下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。
- 下一跳接口：用于标识数据从本地发出的出接口。

路由条目的来源有三种，分别为直连路由、静态路由和动态路由。

1) 直连路由：通过数据链路层协议发现的，通常为与路由器直接连接的网络的路由。

2) 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

3) 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。

10.1 接口

网络接口是一种三层模式下的虚拟接口，主要用于实现 VLAN、路由端口之间的三层互通。每个 VLAN 接口对应一个 VLAN，路由端口对应一个物理端口，环回接口是纯软件接口的。网络接口通过地址与子网掩码参数确定了一个 IP 网段（或称为 IP 子网），并作为该网段的网关对需要跨网段的报文进行基于 IP 地址的三层转发。

您可以在这个页面上配置系统的三层接口。

进入页面的方法：路由功能→接口→接口设置

图 10-1 接口配置

以下的条目显示在屏幕上:

- **创建接口**

接口 ID: 输入网络接口对应的 ID，VLAN ID、环回 ID 或用户端口。

IP 地址模式: 设置 IP 地址申请模式。 无：无 IP， 静态：手动设置， DHCP：通过 DHCP 申请， BOOTP：通过 BOOTP 申请。

IP 地址: 设置网络接口的 IP 地址。

子网掩码: 设置网络接口 IP 地址的子网掩码。

管理状态: 设置网络接口的管理状态。选择'关闭'来关闭此接口的三层功能。

接口名称: 设置网络接口的接口名称。

- **接口列表**

选择: 选择接口条目进行修改或删除。

ID: 显示该网络接口对应的 ID。

模式: 显示 IP 地址申请模式。

IP 地址 显示网络接口的 IP 地址。

子网掩码: 显示该网络接口的子网掩码。

接口名称: 显示该网络接口的接口名称。

状态: 显示网络接口的当前运行状态。只有当管理状态为开启、line protocol 为 UP 并且设置了 IP 地址的情况下，运行状态为 UP。

操作: 单击'编译'修改网络接口设置， 或单击'详细'查看详细信息。

- **IPv4 接口**

点击编辑显示如下图片：

图 10-2 IPv4 接口配置

➢ **修改接口**

接口 ID: 此接口对应 ID，VLAN ID， 环回 ID 或端口号。

IP 地址模式: 设置 IP 地址申请模式。 无：无 IP， 静态：手动设置， DHCP：通过 DHCP 申请， BOOTP：通过 BOOTP 申请。

IP 地址: 设置接口 IP。

子网掩码: 设置接口子网掩码。

管理状态: 设置接口管理状态。选择'关闭'可以关闭接口的三层功能。

接口名: 设置接口名称。

- **创建第二 IP**

  IP 地址: 指定接口的第二 IP 地址。

  子网掩码: 指定接口的第二 IP 地址的子网掩码。

- **第二 IP 列表**

  选择: 选择要删除的第二 IP。

  IP 地址: 显示当前接口的第二 IP 地址。

  子网掩码: 显示第二 IP 地址的子网掩码。

- **IPv6 接口**

点击编辑来显示如下图片:

图 10-3 系统 IPv6

以下的条目显示在屏幕上:

- **IPv6 全局配置**

IPv6 功能: 选择启用/禁用按钮全局配置交换机的 IPv6 功能。

接口 ID: 选择开启 IPv6 功能的接口 ID，接口类型包括 VLAN、路由端口、汇聚接口。

- **IPv6 链路本地地址配置**

链路本地地址配置方式: 您可以根据需要，让系统自动生成一个链路本地地址，或者使用纯手工的方式配置链路本地地址。

- 手动: 选择此选项时，您需要手工配置链路本地地址。
- 自动: 选择此选项时，交换机会自动生成一个链路本地地址。

IPv6 链路本地地址: 当使用手动方式配置链路本地地址时，在此输入交换机的链路本地地址。

链路本地地址状态: 显示交换机链路本地地址的状态。

- 正常: 表明链路本地地址状态是正常的。
- 试探: 表明链路本地地址可能是新配置的。
- 重复: 表明交换机的链路本地地址与链路上其它节点重复，此时不能用 IPv6 地址（包括链路本地地址和全球地址）访问交换机。

- **通过 RA 消息配置 IPv6 全球地址**

允许使用 RA 消息进行全球地址自动配置: 当该选项被启用时，系统将接受来自路由器的 RA 消息进行全球地址的自动配置。

- **通过 DHCPv6 获取全球地址**

启用通过 DHCPv6 获取全球地址 当该选项被启用时，系统将尝试使用 DHCPv6 获取全球地址。

- **手动添加 IPv6 全球地址**

配置方式:

- EUI-64: 当使用 EUI-64 方式时，您仅需指定一个地址前缀，系统将自动为你生成一个全球地址。
- 非 EUI-64: 当使用非 EUI-64 方式时，您需要指定一个完整的 IPv6 全球地址。

IPv6 全球地址: 当使用 EUI-64 方式配置全球地址时，在此输入地址前缀。当使用非 EUI-64 方式配置全球地址时，在此输入完整的 IPv6 地址。

- **系统当前 IPv6 全球地址列表**

选择: 您可以在此选择要修改或删除的 IPv6 全球地址。

IPv6 全球地址: 当修改 IPv6 全球地址的时候，在此输入新的 IPv6 全球地址。

前缀长度: 当修改 IPv6 全球地址的时候，在此输入新的 IPv6 全球地址前缀长度。

地址类型: 显示全球地址的配置模式。

- 手动: 表示对应地址是用户手动配置的。
- 自动: 表示对应地址是系统通过接收 RA 消息自动生成，或者通过 DHCPv6 获取。

首选时间: 显示全球地址的首选时间。

有效时间: 显示全球地址的有效时间。

状态: 显示全球地址的状态。

- 正常: 表明全球地址状态是正常的。
- 试探: 表明全球地址可能是新配置的。
- 重复: 表明全球地址与链路上其它节点重复，此时不能用该 IPv6 全球地址访问交换机。

建议:

将全球 IPv6 地址手动添加到您的交换机后，您可以配置您的电脑的全球 IPv6 地址和交换机的地址在同一子网中，然后您可以通过交换机的全球 IPv6 地址来登录。

单击细节显示下面的图::

图 10-4 接口详细信息

➢ **详细信息**

接口 ID: 显示网络接口 ID，VLAN ID、环回 ID 或用户端口。

IP 地址模式: 显示 IP 地址申请模式。 None：无 IP， Static：手动设置， DHCP：通过 DHCP 申请， BOOTP：通过 BOOTP 申请。

IP 地址 显示 IP 地址和子网掩码。

第二 IP: 显示第二 IP 地址和子网掩码。

接口状态: 显示网络接口当前状态。只有设置了 IP，管理状态为'开启'，并且连接状态为'连接'时，接口状态才为'连接'。

连接状态: 显示是否有上联端口接入到当前网络接口。

管理状态: 显示网络接口管理状态。如果设置为'关闭'， 那么接口的三层功能将被关闭。

接口名称： 显示网络接口名称。

- **接口设置信息**

显示接口的详细设置信息。

10.2 路由表

该页面显示由不同路由协议生成的路由信息摘要。

10.2.1 IPv4 路由表

进入页面的方法：路由功能→路由表→IPv4 路由表

图 10-5 路由表

以下的条目显示在屏幕上:

- **路由信息汇总**

路由协议： 显示路由协议

目的网络: 显示路线的目的地。

下一跳地址: 显示下一个数据包应该发送到哪个 IP 地址。

管理距离： 显示路线的管理距离。距离越小，优先级越高。

度量值： 显示路由的度量。

接口名称： 显示出路接口的描述。

10.2.2 IPv6 路由表

进入页面的方法：路由功能→路由表→IPv6 路由表

图 10-6 IPv6 路由表

以下的条目显示在屏幕上:

- **路由信息汇总**

路由协议： 显示路由协议

目的网络: 显示路线的目的地。

下一跳地址: 显示下一个数据包应该发送到哪个 IP 地址。

管理距离： 显示路线的管理距离。距离越小，优先级越高。

度量值： 显示路由的度量。

接口名称： 显示出路接口的描述。

10.3 静态路由

静态路由是由管理员手动配置的特殊路由，因此不能随网络拓扑结构自动改变。因此，静态路由通常在相对简单和稳定的网络中使用。静态路由的适当配置可以极大地提高网络性能。

10.3.1 IPv4 静态路由条目

静态路由是一种特殊的路由，它是由管理员手工配置，不随网络拓扑的改变而自动变化，故多用于网络规模较小，拓扑结构固定的网络中，具有简单、高效、可靠等优点。

进入页面的方法：路由功能→静态路由→IPV4 静态路由条目

图 10-7 静态路由配置

以下的条目显示在屏幕上:

- **静态路由配置**

目的地址： 设定数据报文需要到达的目的 IP 地址。

子网掩码: 设定目的 IP 地址的子网掩码。

下一跳地址: 指定一个 IP 地址，交换机下一步会将符合条件的数据包转发到该地址上。

管理距离： 指定路由条目的管理距离。管理距离越小，优先级越高。

- **静态路由条目**

选择： 选择静态路由条目进行修改。

目的地址： 显示数据报包需要到达的目的 IP 地址。

子网掩码: 显示目的 IP 地址的子网掩码。

下一跳地址： 显示下一跳地址。

管理距离： 显示路由条目的管理距离。管理距离越小，优先级越高。

度量值 显示路由的度量。

接口名称： 显示网络接口的接口名称。

10.3.2 IPv6 静态路由条目

进入页面的方法：路由功能→静态路由→IPV6 静态路由条目

图 10-8 静态路由配置

以下的条目显示在屏幕上:

- **IPv6 路由**

  IPv6 路由： 开启/关闭 IPv6 路由

- **静态路由配置**

  目的地址： 设定数据报文需要到达的目的 IP 地址。

  子网掩码: 设定目的 IP 地址的子网掩码。

  下一跳地址: 指定一个 IP 地址，交换机下一步会将符合条件的数据包转发到该地址上。

  管理距离： 指定路由条目的管理距离。管理距离越小，优先级越高。

- **静态路由条目**

选择：	选择静态路由条目进行修改。
目的地址：	显示数据报包需要到达的目的 IP 地址。
下一跳地址：	显示下一跳地址。
管理距离：	显示路由条目的管理距离。管理距离越小，优先级越高。
度量值	显示路由的度量。
接口名称	显示网络接口的接口名称。

10.4 DHCP 服务器

DHCP 模块用于配置交换机的 DHCP 功能，包括两个子菜单、DHCP 服务器和 DHCP 中继。

DHCP(动态主机配置协议)是 TCP / IP 网络上给主机网络配置的协议,它提供了一个框架,用于给主机分配配置信息。DHCP 增加了可重复利用的网络地址和其他的配置选项自动分配的能力。DHCP 捕捉 DHCP 参与者的行为，这样管理员可以管理网络中主机的参数。

工作站和个人电脑在互联网上激增,因此维护网络的复杂性增加了一个数量级。给每个客户端分配本地网络资源就代表了这样一种困难。在大多数环境中,将这种任务委托给用户是不合理的。事实上,解决方案是将资源定义为统一格式并自动分配。

DHCP 负责将互联网地址和一些其他资源分配给客户。

10.4.1 DHCP 服务器

用于开启或关闭 DHCP 服务器。当 DHCP 服务器开启时 DHCP 中继会同时开启。

进入页面的方法：路由功能→DHCP 服务器→DHCP 服务器

图 10-9 DHCP 服务器

以下的条目显示在屏幕上:

- **全局配置**

  DHCP 服务器： 开启或关闭 DHCP 服务器。

  Option 60： 配置 DHCP Option 60 选项字段，如果该选项字段不为空且运行 CAPWAP 协议的客户端通过 DHCP 向服务器请求获取 option 60 选项时，服务器发出的报文将会带上该选项。

  Option 138： 配置 DHCP Option 138 选项字段，如果该选项字段不为空且运行 CAPWAP 协议的客户端通过 DHCP 向服务器请求获取 option 138 选项时，服务器发出的报文将会带上该选项。

- **Ping 配置**

  Ping 报文数： 每次确定 IP 存在的时候发出的报文数。

  Ping 超时： Ping 超过该时间则认为指定 IP 不存在。

- **不分配 IP 设置**

  起始 IP 地址： 不分配的起始 IP 地址。

  结束 IP 地址： 不分配的结束 IP 地址。

- **不分配 IP 列表**

选择： 选择删除不分配的 IP 地址池的条目。

序号： 显示序号信息。

起始 IP 地址： 显示不分配的 IP 地址池的起始 IP 地址。

结束 IP 地址： 显示不分配的 IP 地址池的结束 IP 地址。

10.4.2 地址池设置

DHCP 服务器从地址池中为客户端选择并分配 IP 地址及其他相关参数。

进入页面的方法：路由功能→DHCP 服务器→地址池设置

图 10-10 地址池设置

以下的条目显示在屏幕上:

- **DHCP 服务器地址池**

地址池名称： 地址池的名称，最大支持 8 个字符。

网络地址： 地址池网络地址。

掩码： 地址池掩码。

租期： 客户端能使用从该地址池所分配的 IP 地址的时间。

默认网关： 配给客户端的网关，最大可设置 8 个，为可选配置。

DNS 服务器： 分配给客户端的 DNS 服务器，最大可设置 8 个，为可选配置。

Netbios 服务器： 配给客户端的 WINS 服务器，最大可设置 8 个，为可选配置。

Netbios 节点类型： 客户端 Netbios 节点类型，可设置为空，为可选配置。

下一个服务器地址: 引导过程的下一个服务器地址，为可选配置。

客户端域名： 给客户端设置的域名，为可选配置。

启动文件名： 引导过程中用到的镜像文件名，为可选配置。

- **地址池列表**

选择： 选择删除 IP 地址池的条目。

名称： 显示 IP 池的名称。

网络号： 显示 IP 池的网络地址。

租期： 显示租期。

掩码： 显示 IP 池的子网掩码。

操作 允许您查看或修改相应的 IP 池的信息。

10.4.3 静态绑定

可将 MAC 地址与 IP 地址进行绑定，服务器收到已绑定 MAC 的 DHCP 请求时，会将所绑定的 IP 地址发送给客户端。

进入页面的方法：路由功能→DHCP 服务器→DHCP 服务器静态绑定设置

图 10-11 手动绑定

以下的条目显示在屏幕上:

- **DHCP 服务器静态绑定设置**

  地址池名称： 地址池的名称，从已配置地址池中选取。

  绑定 IP： 与 MAC 地址绑定的 IP 地址。

  绑定方式： 设定 IP 与客户端 ID 绑定或者 IP 与硬件地址绑定。

  客户端 ID： 绑定的客户端 ID。

  硬件地址： 所绑定的 MAC 地址。

  硬件类型： 选择为 Ethernet 或者 IEEE802 类型。

- **静态绑定列表**

显示 IP 地址和硬件地址绑定条目的列表。

10.4.4 绑定表

在这个页面中，您可以查看连接到服务器的客户的信息。

进入页面的方法：路由功能→DHCP 服务器→绑定表

图 10-12 已分配 IP 列表

- **已分配 IP 列表**

  选择： 选择对应条目

  ID： 显示客户端的 ID。

  IP 地址： 显示交换机分配给客户端的 IP 地址。

  客户端 ID/MAC 地址： 显示客户端的 MAC 地址。

  类型： 显示这个绑定条目的类型。

  剩余租期（秒） 显示剩余租期时间

10.4.5 报文统计

在这个页面中，您可以查看交换机接收或发送的 DHCP 报文数目。

进入页面的方法：路由功能→DHCP 服务器→报文统计


接收报文
BOOTREQUEST: 0
DHCPDISCOVER: 0
DHCPREQUEST: 0
DHCPDECLINE: 0
DHCPRELEASE: 0
DHCPINFORM: 0
发送报文
BOOTREPLY: 0
DHCPOFFER: 0
DHCPACK: 0
DHCPNAK: 0
刷新
清空
帮助

图 10-13 报文统计

以下的条目显示在屏幕上:

- **接收报文**

BOOTREQUEST： 显示接收到的 Bootp Request 报文数目。

DHCPDISCOVER： 显示接收到的 Discover 报文数目。

DHCPREQUEST 显示接收到的 Request 报文数目。

DHCPDECLINE: 显示接收到的 Decline 报文数目。

DHCPRELEASE: 显示接收到的 Release 报文数目。

DHCPINFORM: 显示接收到的 Inform 报文数目。

- **发送报文**

BOOTREPLY: 显示发送的 Bootp Reply 报文数目。

DHCPOFFER： 显示发送的 Offer 报文数目。

DHCPACK 显示发送的 Ack 报文数目。

DHCPNAK: 显示发送的 Nak 报文数目。

- **配置过程:**

步骤	操作	描述
1	设置端口链接类型	必选操作。**VLAN→802.1 q VLAN→端口配置**页面，设置端口的链接类型。
2	创建 VLAN	必选操作。在 **VLAN→802.1 q VLAN→VLAN 配置**页面，点击创建按钮创建一个 VLAN。输入 VLAN ID 和 VLAN 的描述。同时，指定它的成员端口。
3	创建 VLAN 接口	必选操作。在**路由功能→静态路由→静态路由配置**页面，创建 VLAN 的接口 IP 地址。
4	使能 DHCP 服务器	必选操作。在**路由功能→DHCP 服务器→DHCP 服务器**页面，启用 DHCP 服务器的功能。
5	配置不分配 IP 地址	可选操作。在**路由功能→DHCP 服务器→DHCP 服务器**页面，配置不分配 IP 地址。
6	配置 IP 地址池	必选操作。在**路由功能→DHCP 服务器→地址池设置**页面，配置 IP 地址池的参数，包括掩码、租赁时间、网关和 DNS 地址。
7	手动绑定 IP	可选操作。在**路由功能→DHCP 服务器→手动绑定**页面中，您可以为特定客户指定 IP 地址。

10.5 DHCP 中继

10.5.1 全局配置

通过 DHCP 中继功能，交换机能在不同的接口或子网中获取 IP 地址。在特定的接口中指定 DHCP 服务器，开启 DHCP 中继功能并指定服务器的地址，在其他接口的设备就能获取 IP 地址。DHCP 中继功能可以减少网络中 DHCP 服务器的数量。

进入页面的方法：路由功能→DHCP 中继→全局配置

图 10-14 全局设置

以下的条目显示在屏幕上:

- **全局配置**

  DHCP 中继: 开启或关闭 DHCP 中继。

- **Option 82 的配置**

  Option 82 支持： 选择是否启用 Option 82 字段。

  已存在 option 82 处理 保留: 保留数据包中的 Option 字段信息。
  替换: 替换数据包中的 Option 字段信息，替换为交换机自定义的选项内容。
  丢弃: 丢弃包含 Option 82 字段的数据包。

  Option 82 自定义： 选择交换机是否自定义 Option 82 选项内容。

  电路 ID 子选项： 输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。

  远程 ID 子选项 输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

10.5.2 接口中继配置

该页面允许您在指定的接口上配置 DHCP 服务器。

进入页面的方法：路由功能→DHCP 中继→接口中继配置

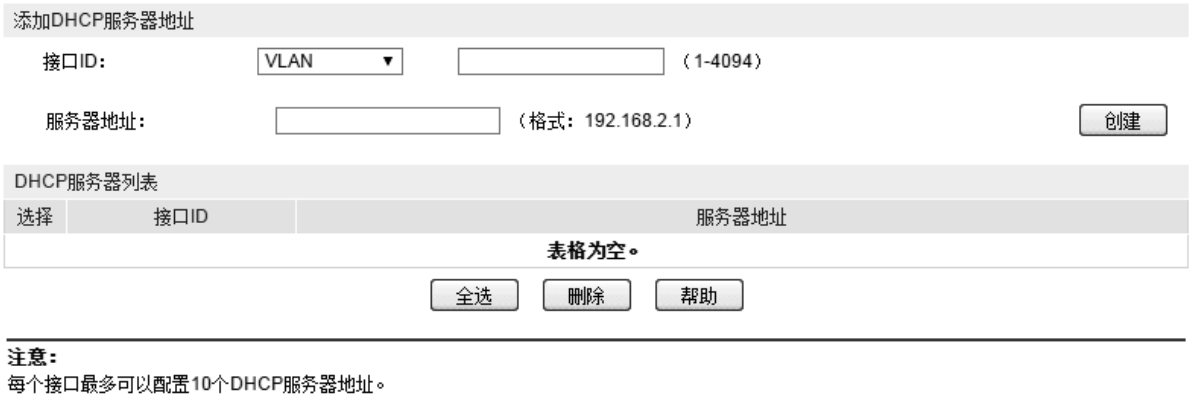


图 10-15 DHCP 服务器

以下的条目显示在屏幕上:

- **添加 DHCP 服务器地址**

  接口 ID： 选择接口类型，输入接口 ID。

  服务器地址： 输入 DHCP 服务器的 IP 地址。

- **DHCP 服务器列表**

  选择： 选择需要管理的 DHCP 服务器条目。

  接口 ID： 显示接口 ID。

  服务器地址: DHCP 服务器地址。

配置过程:

步骤	操作	描述
1	使能 DHCP 中继。	必选操作。在**路由功能→DHCP 中继→全局配置**页面，启用 DHCP 中继功能。
2	.配置选项 82 支持。	可选操作。在**路由功能→DHCP 中继→全局配置**页面，配置 Option 82 参数。
3	配置 DHCP 服务器。	必选操作。在**路由功能→DHCP 中继→DHCP 服务器**页面，指定的 DHCP 服务器的 IP 地址。

10.6 ARP

地址解析协议(ARP)记录 ARP 映射表中 IP 地址和 MAC 地址之间的映射关系。您还可以在页面静态 ARP 中定义一个静态 ARP 缓存条目。

10.6.1 ARP 表

进入页面的方法：路由功能→ARP→ARP 表

图 10-16 ARP 列表

以下的条目显示在屏幕上:

- **ARP 列表**

接口： ARP 条目对应的网络接口。

IP 地址： ARP 条目中的 IP 地址。

MAC 地址： ARP 条目中 IP 对应的 MAC 地址。

类型： ARP 条目类型，例如：‘静态‘或者‘动态‘。

10.6.2 静态 ARP

您可以在这个页面上配置静态 ARP 条目。

进入页面的方法：路由功能→ARP→静态 ARP

图 10-17 静态 ARP

- **ARP 配置**

  IP 地址： 设定 ARP 条目中的 IP 地址。

  MAC 地址： 设定 ARP 条目中 IP 对应的 MAC 地址。

- **ARP 条目**

  选择： 选择静态 ARP 条目进行修改。

  IP 地址： ARP 条目中的 IP 地址。

  MAC 地址： ARP 条目中 IP 对应的 MAC 地址。

回目录

第11章 服务质量

服务质量模块主要用于流量控制管理和优先级配置，针对各种网络应用的不同需求，为其提供不同的服务质量，对带宽资源进行最优配置，从而提供更高质量的网络服务体验，包括 **QoS 配置**、**流量管理**以及**语音 VLAN** 三个部分。

11.1 QoS 配置

QoS（Quality of Service 即服务质量）功能用以提高网络传输的可靠性，提供高质量的网络服务体验。在传统的 IP 网络中，所有的报文都被无区别的等同对待，网络尽最大的努力（Best-Effort）发送报文，但对时延、可靠性等性能不能提供任何保证。伴随着网络技术、多媒体技术的飞速发展，IP 网在现有的 www， FTP， E-mail 等服务的基础上，越来越多承载交互式多媒体通信业务如电视会议、远程教学、视频点播、可视电话等，而每种业务要求的传输时延、可变迟延、吞吐量和丢包率都不同。因此，为用户各种业务提供不同的服务质量（QoS）成为 Internet 发展的重要挑战。

通常所说的 QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

- **QoS 工作原理**

本交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来决定不同优先级队列的数据包被转发的方式，从而实现了 QoS 功能。

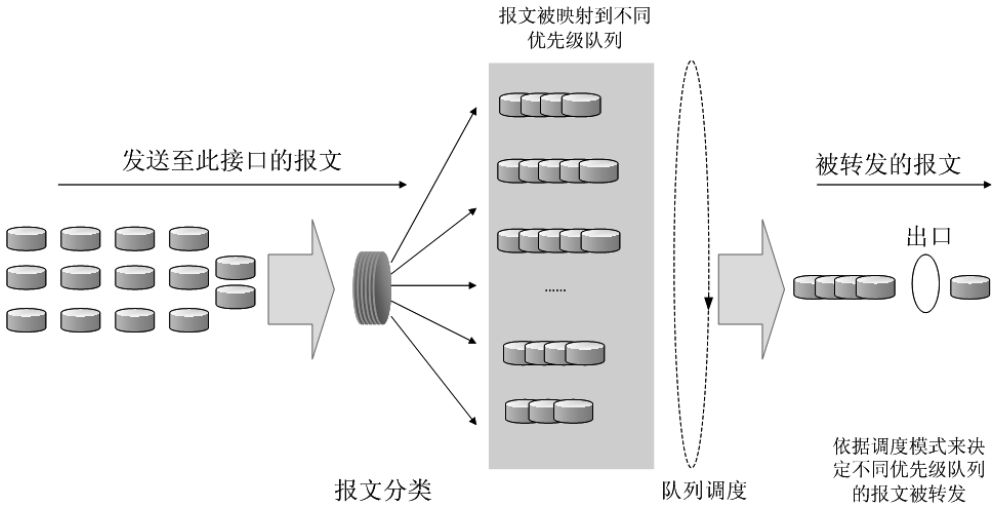


图 9-1 QoS 工作原理

- 报文分类：依据一定的匹配规则识别出对象。
- 映射：用户可以根据优先级模式，将进入交换机的报文映射到不同的优先级队列中。本交换机提供三种优先级模式：基于端口的优先级、802.1P 优先级和 DSCP 优先级。
- 队列调度：当网络拥塞时，必须解决多种数据流同时竞争使用资源的问题，通常采用队列调度加以解决。本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR 模式和无优先级模式（Equ）。

- **优先级模式**

本交换机共有基于端口的优先级、IEEE 802.1P 优先级和 DSCP 优先级三种模式。其中基于端口的优先级是默认被启用的，其它两种优先级模式可供选择。

1. 基于端口的优先级

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据入端口的 CoS 值以及 802.1P 中 CoS 到队列之间的映射关系来确定数据流的出口队列。

2. 802.1P 优先级

图 9-2 802.1Q 的帧格式

如图所示，每一个 802.1Q Tag 中都有一个 Pri 域，该域由三个 bit 为组成，取值范围是 0~7。802.1P 优先级就是根据 Pri 的域值来决定数据帧的优先级。通过交换机的配置页面可配置不同的 Pri 域对应不同的优先级，交换机发送数据帧时，会根据数据帧的 Tag 决定发送的优先级。对于 Untagged 帧，交换机则按照该入口端口的默认优先级对数据帧进行 QoS 处理。

3. DSCP 优先级

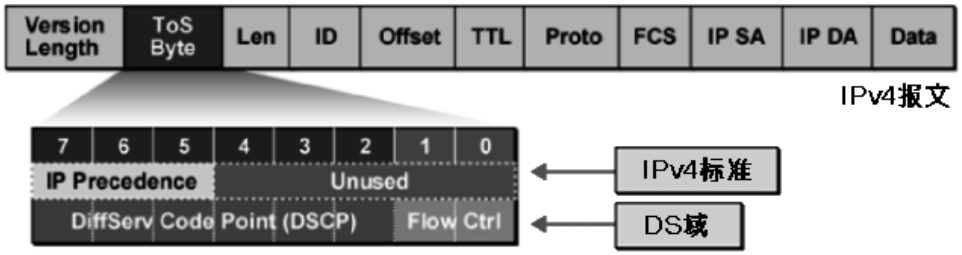


图 9-3 IP 报文

如图所示，IP 报文头部的 ToS（Type of Service，服务类型）字段共有 8bit，前 3 个 bit 表示的是 IP 的优先级，取值范围是 0~7。RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域。其中 DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的 DS 字段对应不同的优先级，交换机发送 IP 包时，会根据 IP 包的 DS 域决定发送的优先级。对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

注意：

- 当没有启用 DSCP 优先级时，交换机根据数据包是否带有 802.1Q Tag 确定使用哪种优先级模式。对于带有 Tag 的数据包，应用 802.1P 优先级；否则应用端口优先级。当启用 DSCP 优先级时，如果接收的数据包是 IP 包，则应用 DSCP 优先级；对于非 IP 包，如果数据帧带有 Tag 则应用 802.1P 优先级，否则应用端口优先级。

➢ **调度模式**

在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。本交换机共实现了8 个调度队列—TC0 到 TC7，其中 TC0 对应最低优先级的队列，TC7 对应到最高优先级的队列。同时，本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR 模式和无优先级模式（Equ）。

1. SP-Mode：严格优先级模式。SP 模式的调度算法是交换机优先转发当前优先级最高的数据帧，等最高优先级数据帧全部转发完后，再转发次高级优先级的数据帧。本交换机有 8 个出口队列，依次为 TC0-TC7，在 SP 队列模式下他们的优先级依次升高，TC7 有最高优先级。SP 队列的缺点是，在拥塞发生时，如果较高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

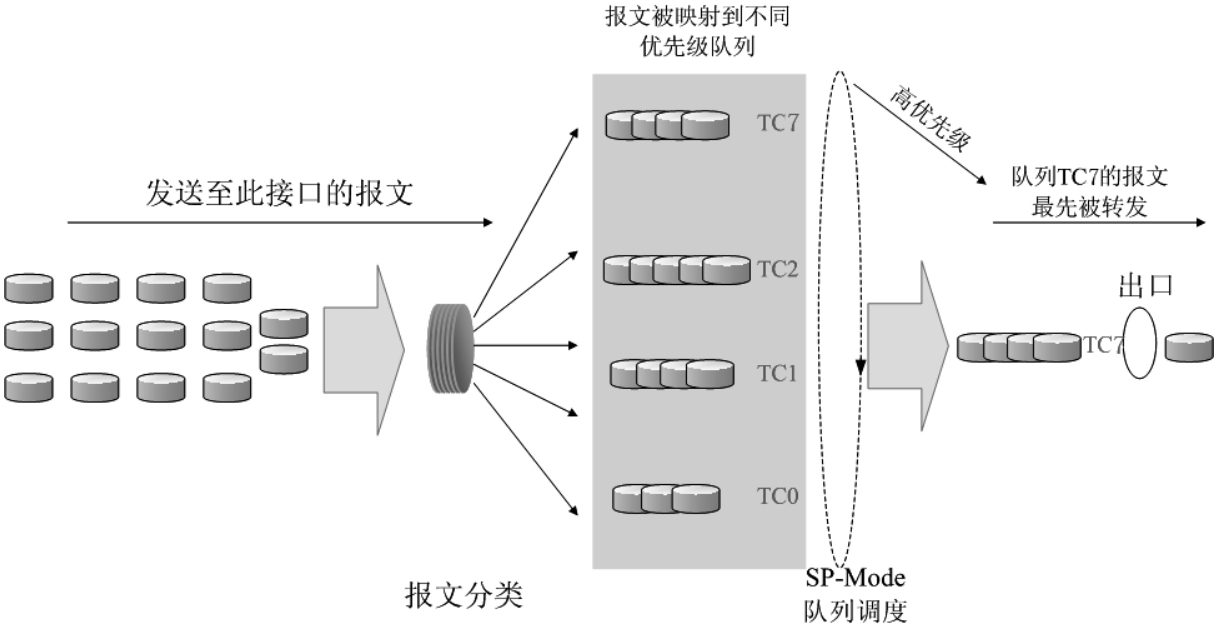


图 9-4 严格优先级模式

2. WRR-Mode：WRR 优先级模式。WRR 模式的调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间。加权值表示获取资源的比重。WRR 队列避免了采用 SP 调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。TC0-TC7 的默认权重比是 1:2:4:8:16:32:64:127。

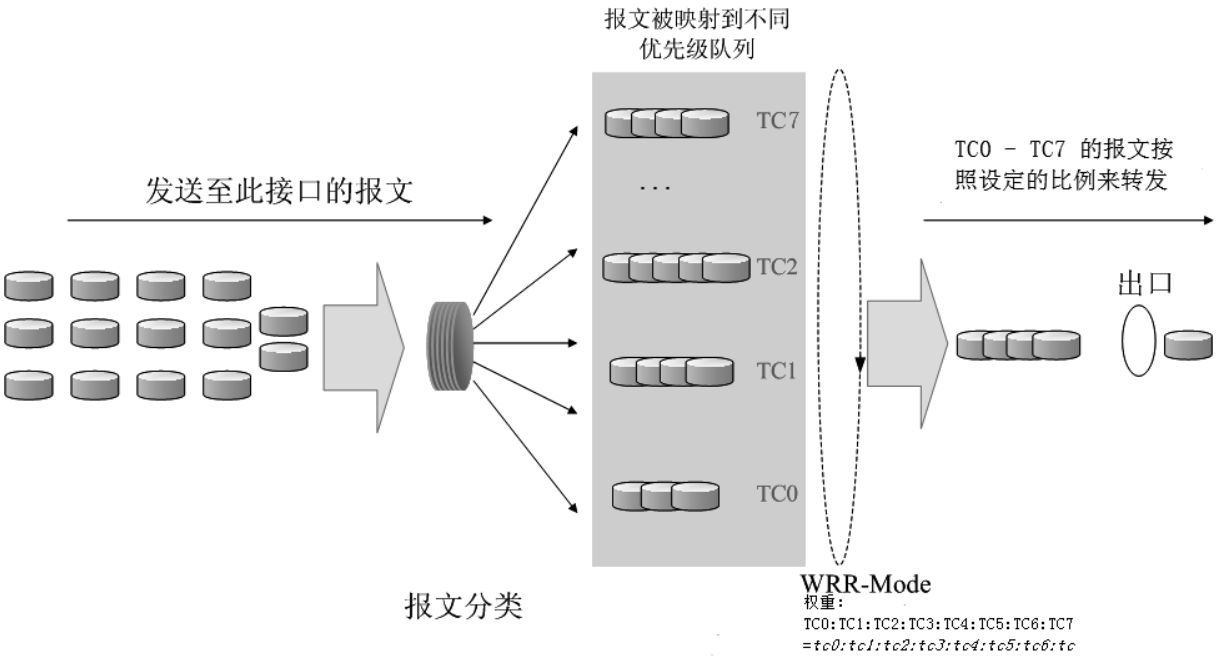


图 9-5 WRR 优先级模式

3. SP+WRR-Mode：SP+WRR 优先级模式，这种模式是前两种模式的混合。在这种模式下，交换机提供了两个调度组，分别是 SP 组和 WRR 组。其中 SP 组和 WRR 组之间遵循的是严格优先级调度规则，而 WRR 组内部队列遵循的是 WRR 调度模式。在 SP + WRR 模式中，TC7 和权重设为 0 的队列属于 SP 组；其他权重非 0 的队列属于 WRR 组，并且它们的权重可以设为 0 到 127。这种情况下，安排队列的时候，交换机允许 TC7 和权重为 0 的队列占据 SP 模式下的整个带宽，WRR 组中的队列会根据它们的比率来占据带宽。

4. Equ-Mode：无优先级模式。这种模式下所有队列公平的占用带宽，实际上这是 WRR 模式的一种特殊情况，所有的队列权重比是 1:1:1:1:1:1:1:1。

本交换机实现了基于端口、基于 802.1P 和基于 DSCP 的三种优先级模式以及四个队列调度模式。端口优先级以 CoS 0，CoS1…CoS 7 表示。QoS 配置功能包括**端口配置**、**DSCP 映射**、**802.1P/CoS 映射**和**队列调度模式**四个配置页面。

11.1.1 端口配置

在基本配置页面中，可以进行基于端口优先级的配置。

进入页面的方法：服务质量>>QoS 配置>>端口配置

图 9-6 基本配置

条目介绍：

- **端口优先级配置**

选择： 勾选端口配置端口优先级，可多选。

端口： 显示交换机的物理端口。

优先级： 配置端口的所属优先级等级。

LAG： 显示当前端口所属的汇聚组。

配置步骤：

步骤	操作	说明
1	选择端口的优先级	必选操作。在**服务质量>>QoS 配置>>端口配置**页面设置各端口的优先级。
2	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS 配置>>802.1P/CoS 映射**页面的**优先级等级**表格中设置优先级与队列的映射关系。

3	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>队列调度模式**页面设置调度模式。

11.1.2 调度模式

在这个页面上，您可以选择交换机的调度模式。当网络拥挤时，许多包争夺资源的问题必须解决，通常是以队列调度的方式解决的。交换机根据优先级队列和调度算法设置控制数据包的转发顺序。优先级被标记为 TC0，TC1…TC7。

进入页面的方法：服务质量→QoS 配置→调度模式

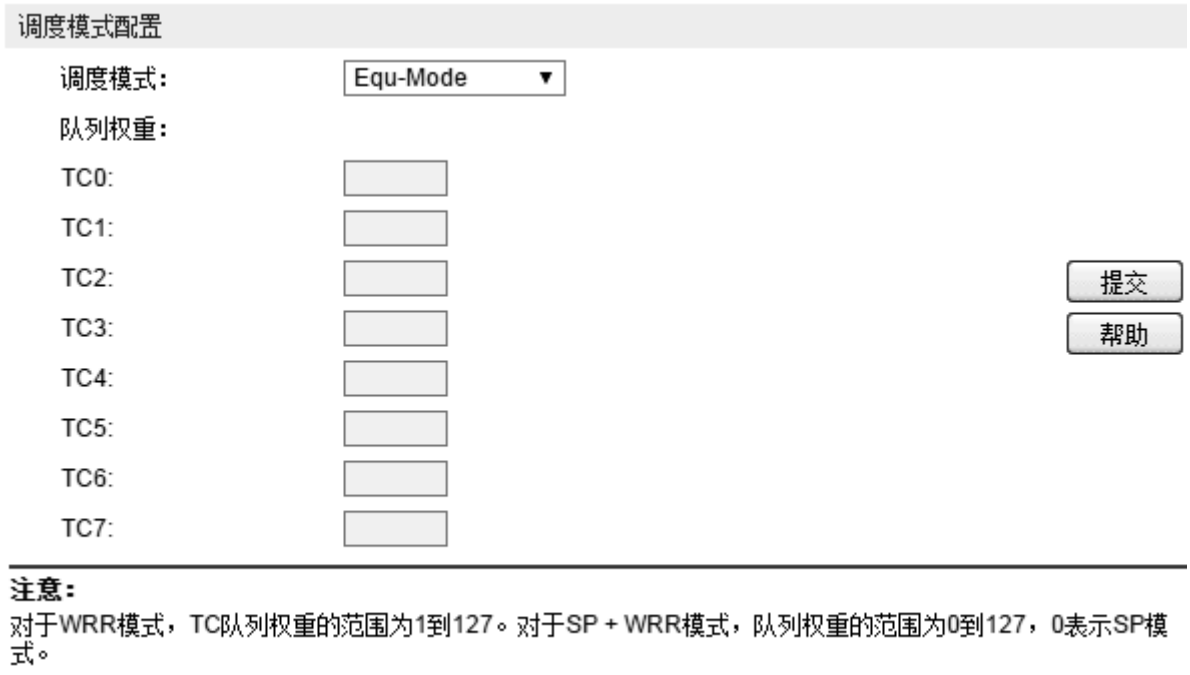


图 11-1 调度模式

以下的条目显示在屏幕上:

- **调度模式配置**

调度模式: 选择一个调度模式。

- **SP-Mode**：严格的优先级模式。在这种模式下，具有更高优先级的队列将占据整个带宽。只有在具有较高优先级的队列为空时，才会发送具有较低优先级的包。
- **WRR-Mode:**权重循环模式。在这种模式下，根据每个队列的权重值，所有队列中的信息包都按顺序发送。的重量值 TC0-TC7 可以分别定制他们的值 1:2:4:8:16:32:64:127。
- **SP+WRR-Mode:**严格的优先级+权重循环模式。在这种模式下，交换机提供两个调度组，SP 组和 WRR 组。SP 组在 WRR 组之前被处理。
- **Equ-Mode:** 在这种模式下，所有队列都占用带宽。权重为 1:1:1:1:1:1:1:1。

队列权重: 输入 8 个 TC 队列的队列权重。选择配置 Equ-Mode 时不可用或 SP-Mode 调度模式。

11.1.3 802.1P

在802.1P配置页面中，可以配置802.1P优先级。802.1P对802.1Q tag中的Pri字段进行了的定义，利用该字段可以将数据包划分为8个优先级。开启802.1P优先级后，交换机根据数据包是否带有802.1Q tag来确定所使用的优先级模式。对于带有tag的数据包，应用802.1P优先级；否则应用端口优先级。

进入页面的方法：服务质量>>QoS 配置>>802.1P

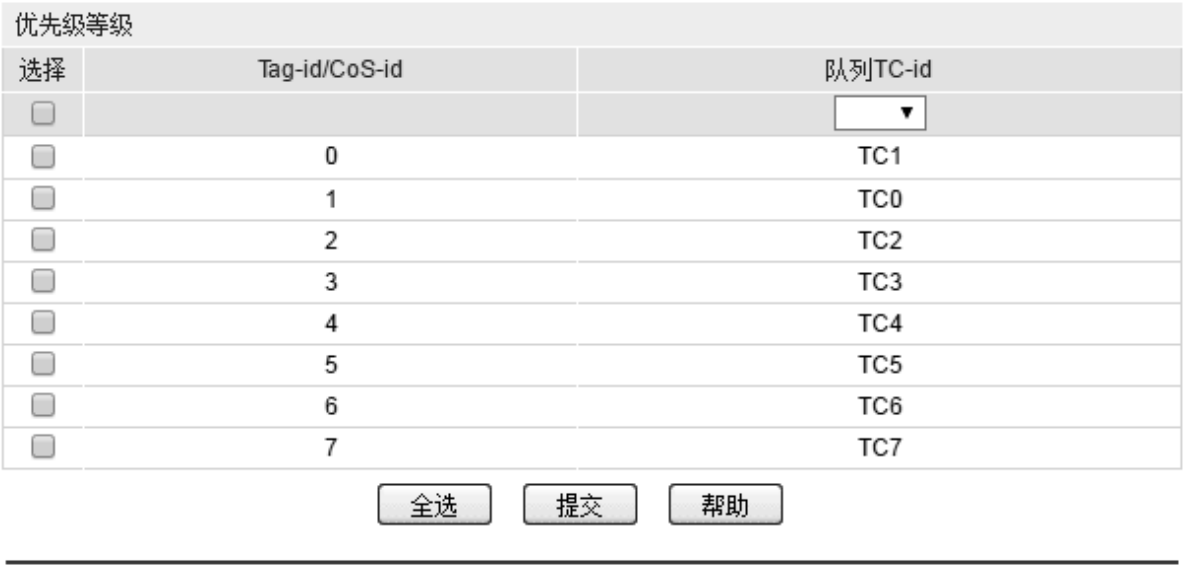


图 9-8 802.1P 优先级

条目介绍：

- **Tag 与 CoS 到出口队列映射配置**

Tag-id/CoS-id： IEEE802.1P 协议里规定的 8 个优先级等级。

队列 TC-id： 对应不同等级的优先级队列。以 TC0，TC1…TC7 表示。

配置步骤：

步骤	操作	说明
1	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS 配置>>802.1P/CoS 映射**页面中的**优先级等级**表格中设置优先级与队列的映射关系。
2	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>队列调度模式**页面设置调度模式。

11.1.4 DSCP

在 DSCP 映射配置页面中，可以进行 DSCP 优先级的配置。DSCP（DiffServ Code Point，区分服务编码点）是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。开启 DSCP 优先级后，如果转发的数据包是 IP 报文，则交换机应用 DSCP 优先级；对于非 IP 报文，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 tag 来决定采用哪种优先级模式。

图 9-7 DSCP 优先级

条目介绍：

- **优先级配置**

  DSCP 优先级： 选择是否启用 DSCP 优先级。

- **优先级**

  DSCP： 数据包的 DSCP 优先级，优先级级别为 0~63。

  优先级： 将数据包根据 DSCP 优先级映射到 802.1P 优先级 CoS0~CoS7。

配置步骤：

步骤	操作	说明
1	设置 DSCP 优先级与 CoS 优先级的映射关系	必选操作。在**服务质量>>QoS 配置>>DSCP 映射**页面启用 DSCP 优先级，设置 DSCP 优先级与 802.1P 优先级的映射关系。
2	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS 配置>>802.1P/CoS 映射**

		页面的**优先级等级**表格中设置优先级与队列的映射关系。
3	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>队列调度模式**页面设置调度模式。

11.2 流量管理

流量管理用于限制交换机端口的带宽和广播流量，保证网络正常有效的运行，包括**带宽控制**和**风暴抑制**两个配置页面。

11.2.1 带宽控制

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

进入页面的方法：服务质量>>流量管理>>带宽控制

图 9-10 带宽控制

条目介绍：

- **带宽控制**

端口选择： 点击<选择>按键，可根据所输端口号，快速选中相应端口。

选择： 勾选端口以配置端口带宽，可多选也可不选。

入口带宽（bps）： 配置端口接收数据时的带宽，可从下拉菜单中选择或者手动输入。若选择“手动输入”，则系统会自动选择与 64Kbps 整数倍最近的值作为入口带宽。若选择“禁用”选项，则该端口的入口带宽控制会被取消，该端口的入口带宽将恢复为最大带宽。

出口带宽（bps）： 配置端口转发数据时的带宽，可从下拉菜单中选择或者手动输入。若选择“手动输入”，则系统会自动选择与 64Kbps 整数倍最近的值作为出口带宽。若选择“禁用”选项，则该端口的出口带宽控制会被取消，该端口的出口带宽将恢复为最大带宽。

LAG： 显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用广播风暴抑制，再启用入口带宽限制将使其失效。
- 若在设置入口带宽或出口带宽时选择了手动输入，则系统会自动选择与 64Kbps 整数倍最近的值作为出口带宽。例如：输入 1023Kbps 作为出口带宽，则系统会自动选择 1024Kbps 作为真正的出口带宽。
- 在端口上启用出口带宽限制时，建议将各端口的流量控制禁用，以保证交换机的正常工作。

11.2.2 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本交换机可以对三种常见的广播帧（广播包、组播包、UL 包）进行限制。

进入页面的方法：服务质量>>流量管理>>风暴抑制

图 9-11 风暴抑制

条目介绍：

- **风暴抑制**

选择： 勾选端口以配置风暴抑制参数，可多选也可不选。

广播包抑制（bps）： 对由普通广播引起的风暴进行抑制。配置广播包的最大接收速度，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的广播包抑制。

组播包抑制（bps）： 对由组播引起的风暴进行抑制。配置组播包的最大接收速度，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的组播包抑制。

UL 包抑制（bps）： 交换机对未学习到地址的单播包（UL 包）进行广播，对由此引起的风暴进行控制。配置 UL 包的最大接收速度，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的 UL 包抑制。

LAG： 显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用入口带宽限制，再启用广播风暴抑制将使其失效。

11.3 语音 VLAN

语音VLAN是为语音数据流而专门划分的VLAN。通过划分语音VLAN可以使语音数据自动被划分到语音VLAN中进行传输，便于对语音流进行有针对性的QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

- **语音数据流识别方法**

本交换机可以根据数据包中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到语音VLAN中传输。

OUI（Organizationally Unique Identifier）是MAC地址的前24位（二进制），是IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符，从OUI地址可以判断出该设备是哪一个厂商的产品。下表是常见语音设备商家产品的OUI地址，已在本交换机中设置为缺省OUI地址，设定不同的掩码可以调节交换机对MAC地址匹配的深度。

序号	OUI 地址	设备商家
1	00-01-E3-00-00-00	Siemens phone
2	00-03-6B-00-00-00	Cisco phone
3	00-04-0D-00-00-00	Avaya phone
4	00-60-B9-00-00-00	Philips/NEC phone

5	00-D0-1E-00-00-00	Pingtel phone
6	00-E0-75-00-00-00	Polycom phone
7	00-E0-BB-00-00-00	3com phone

表 9-1 本交换机中缺省 OUI 地址

- **端口的语音 VLAN 模式**

端口的语音VLAN模式包括自动模式和手动模式，是指端口加入语音VLAN的方式。

自动模式：系统利用IP电话上电时发出的协议报文（UNTAG报文），通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将自动把语音报文的输入端口加入语音VLAN，配置报文的优先级。在设备上可以设置语音VLAN的老化时间。如果在老化时间内，系统没有从输入端口收到任何语音报文，系统将把该端口从语音VLAN中删除。端口的添加/删除过程由系统自动实现。

手动模式：需要手动把IP电话接入端口加入语音VLAN中，再通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将下发ACL规则、配置报文的优先级。

在实际应用中，端口模式的设置需要结合语音设备发出的报文形式和端口的链路类型来进行设置，具体请参考下表。

端口语音 VLAN 模式	语音流类型	端口链路类型及处理方式
自动模式	TAG 语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。
		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。
手动模式	TAG 语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。
		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 必须是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。

表 9-2 端口模式与语音数据流的处理关系

- **语音 VLAN 安全模式**

当端口使能了语音VLAN功能后，通过配置端口的安全模式还可以过滤数据流。若启用安全模式，则端口只转发语音数据包，对于其它源MAC地址不匹配OUI地址的数据包，端口将直接丢弃。若禁用安全模式，则端口转发所有数据包。

安全模式	报文类型	处理方式
启用	UNTAG 报文	当该报文源 MAC 地址是可识别的 OUI 地址时，允许该报文在语音 VLAN 内传输，否则将该报文丢弃。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。
禁用	UNTAG 报文	不对报文的源 MAC 地址进行检查，所有报文均可在语音 VLAN 内传输。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。

表 9-3 安全模式与各种数据的处理关系

注意：

- 除非有特殊需求，请不要在语音 VLAN 中同时传输语音和其它业务数据。

11.3.1 全局配置

在全局配置页面中，可以设置语音VLAN的全局参数，包括VLAN ID、老化时间、以及语音数据包的传输优先级等等。

进入页面的方法：服务质量>>语音 VLAN>>全局配置

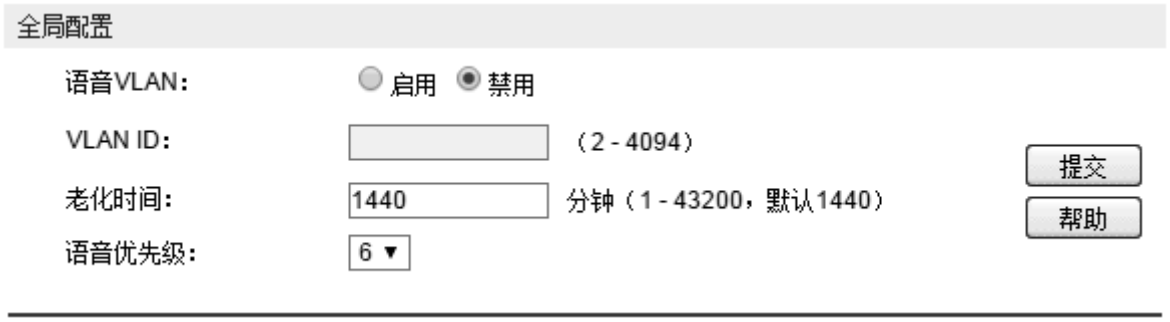


图 9-12 语音 VLAN 全局配置

条目介绍：

- **全局配置**

语音 VLAN： 选择是否启用语音 VLAN 功能。

VLAN ID： 输入该语音 VLAN 的 VLAN ID。

老化时间： 设置自动模式下的端口成员在 OUI 地址老化后的存活时间。

语音优先级： 选择端口发送语音数据包时的数据传输优先级。

11.3.2 端口配置

在启用语音 VLAN 功能之前，需要在端口配置页面中配置各端口的功能参数。

进入页面的方法：服务质量>>语音 VLAN>>端口配置

图 9-13 语音 VLAN 端口配置

注意：

- 若 LAG 组成员端口要启用语音 VLAN 功能，请保持端口的成员模式和端口模式一致。
- 当端口为语音 VLAN 的成员端口时，修改该端口的成员模式为“自动”，此端口首先会退出语音 VLAN，直到收到语音数据时再自动加入语音 VLAN。

条目介绍：

- **端口配置**

选择： 勾选端口配置端口的语音 VLAN 参数，可多选。

端口： 显示交换机的端口号。

成员模式： 设置端口加入语音 VLAN 的方式，有手动和自动两种方式。

- 自动：交换机根据端口是否收到语音数据自动维护端口加入或退出语音 VLAN。
- 手动：请根据需要手动设置端口加入或退出语音 VLAN。

安全模式： 设置端口转发数据包的模式。

- 禁用：端口转发所有数据。
- 启用：端口只转发语音数据。

成员状态： 显示端口当前在语音 VLAN 中的状态。

LAG： 显示端口当前所属的汇聚组。

11.3.3 OUI 配置

本交换机支持新建 OUI 条目，将特殊语音设备的 MAC 地址添加到交换机支持的 OUI 信息中，并以此 OUI 地址判断数据是否是语音数据。当交换机接收到数据包时，将分析数据包并判断是否是语音数据，如果是语音数据则将该端口自动加入语音 VLAN。

进入页面的方法：服务质量>>语音 VLAN>>OUI 配置

图 9-14 语音 VLAN OUI 配置

条目介绍：

- **新建条目**

OUI 地址： 输入语音设备的 OUI 地址。

OUI 掩码： 输入 OUI 地址掩码，常见为 FF-FF-FF-00-00-00。

OUI 描述： 对此 OUI 进行描述，以便区分不同 VoIP 设备。

- **OUI 列表**

OUI 地址： 显示语音设备的 OUI 地址。

OUI 掩码： 显示语音设备的 OUI 地址掩码。

OUI 描述： 显示此 OUI 的描述信息。

语音 VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型，并根据表 9-2 设置语音设备连接端口的端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	添加 OUI 地址	可选操作。在**服务质量>>语音 VLAN>>OUI 配置**页面中的查看交换机是否支持相应的 OUI 模板，若不支持请在此页面中添加。
4	使能端口语音 VLAN 特性	必选操作。在**服务质量>>语音 VLAN>>端口配置**页面设置语音 VLAN 中各端口的功能参数。
5	使能语音 VLAN	必选操作。在**服务质量>>语音 VLAN>>全局配置**页面中使能语音 VLAN 功能，并设置全局参数。

回目录

第12章 PoE

PoE（Power over Ethernet，以太网供电，又称远程供电）是指设备通过以太网线对外接 PD（Powered Device，受电设备）设备（如 IP 电话、无线 AP、网络摄像头等）进行远程供电。

- PoE 系统组成

  PoE 系统通常包括 PSE 和 PD。

  - PSE

    PSE（Power Sourcing Equipment，供电设备）是指可以通过以太网线对连接在其上的 PD 设备进行供电的设备。PSE 会自动寻找、检测 PD，对 PD 分类，并向其供电。当检测到 PD 拔出后，PSE 停止供电。

  - PD

    PD（Powered Device，受电设备）是接受 PSE 供电的设备。分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE802.3af 标准的 PD 设备。PD 设备在接受 PoE 电源供电的同时，允许连接其他电源供电，进行电源冗余备份。

- PoE 的优点

  - 连接简捷：网络终端不需外接电源，只需要一根网线；
  - 可靠：PD 设备可接受 PoE 电源供电或连接其他电源，即具备电源冗余备份功能；
  - 标准：符合 IEEE 802.3af 标准和 IEEE 802.3at 标准，使用全球统一的电源接口；
  - 应用前景广泛：可以用于 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头、数据采集等。

SW-5024 的每个 RJ45 口都支持 PoE 功能，能自动检测 PD 设备，并为符合 IEEE 802.3af 和 IEEE 802.3at 标准的 PD 设备供电。整个交换机能提供的最大功率是 384W，每个 PoE 端口能提供的最大功率是 30W。

PoE 功能配置包括 **PoE 配置**和 **PoE 时间段**两个部分。

12.1 PoE 配置

SW-5024 上的所有 RJ45 口都可以用于为标准 PD 设备供电，由于系统以及每个端口所能提供的功率是有限的，为了保证给每个 PD 提供合适的功率以及充分利用系统功率，必须要对交换机进行一些设置。当功率超过了系统功率上限，或不能给 PD 提供合适的功率时，交换机会根据这些设置断开对某些设备的供电。当检测到 PD 拔出后，交换机会停止对其供电。

PoE 配置包括 **PoE 配置**和 **PoE Profile** 两个配置页面。

12.1.1 PoE 配置

在 PoE 配置页面，可以对 PoE 功能的相关参数进行配置。

进入页面的方法：PoE>>PoE 配置>>PoE 配置

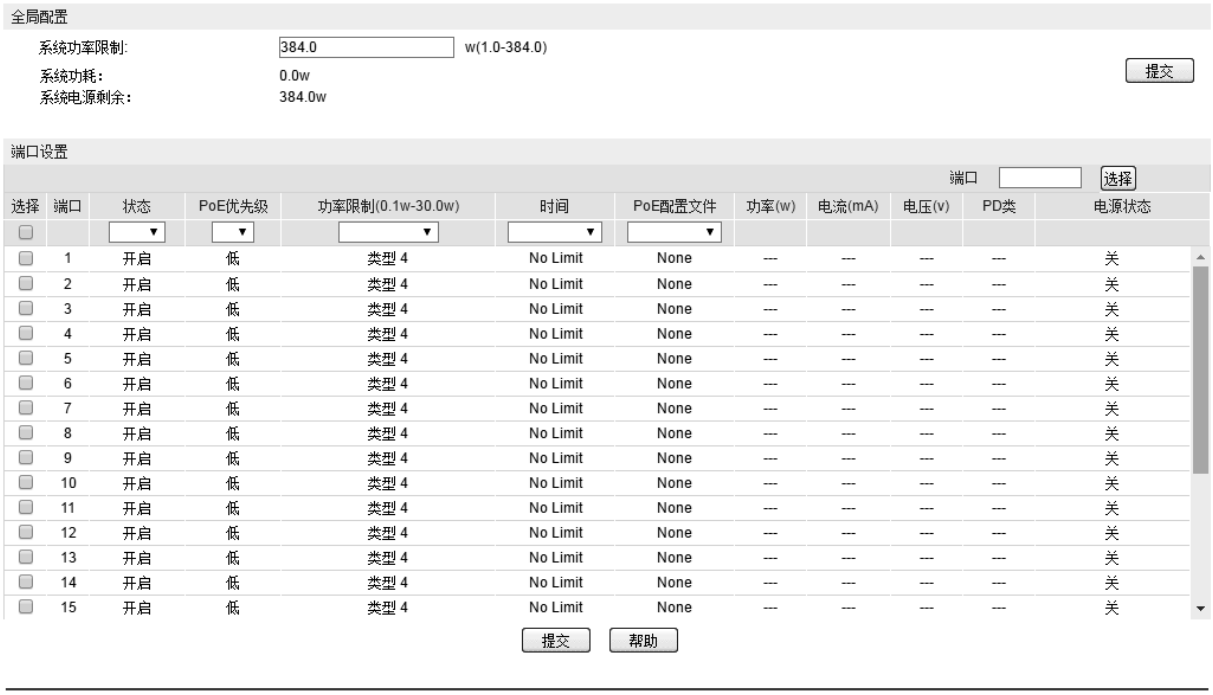


图 10-1 PoE 配置

条目介绍：

- **全局配置**

系统功率限制： 配置交换机能提供的最大功率。

系统功率： 显示当前使用的系统功率。

剩余电量： 显示当前剩余的系统功率。

- **端口配置**

端口选择： 点击<选择>按键，可根据所输端口号快速选择相应条目。

选择： 勾选端口配置端口的 PoE 参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用端口的 PoE 功能。

优先级： 当剩余功率不够时，与供电管理方式一起决定对新接入的 PD 的供电方式，优先级等级包括高、中、低三种。

最大功率(0.1w-30w)： 设定相应端口能提供的最大功率。Class 1 代表 4w，Class 2 代表 7w，Class 3 代表 15.4w，Class 4 代表 30w。也可以选择自动或者手动输入，手动输入范围值为 0.1w-30w。

时间段： 为端口选择供电的时间段。如果选择**无限制**，该端口将一直供电。

PoE Profile： 选择 Profile 文件应用到已选端口。应用了 Profile 文件的端口的以下三个 PoE 属性不可编辑：状态、优先级、最大功率。

功率(w)： 显示端口当前的功率。

电流(mA)： 显示端口当前的电流。

电压(v)： 显示端口当前的电压。

PD Class： 显示连接的 PD 设备所属的类别。

供电状态： 显示端口当前的供电状态。

12.1.2 PoE 配置文件

PoE Profile 文件用于对具有相同属性的 PoE 接口进行批量配置，以简化用户的操作。在 PoE Profile 文件中，配置了端口的三个 PoE 属性：状态、优先级、最大功率。创建一个 PoE Profile 文件，然后将其应用于相应的端口，可简化配置过程。

在 PoE Profile 页面，可以创建新的 PoE Profile 文件或查看 PoE Profile 列表。

进入页面的方法：PoE>>PoE 配置>>PoE 配置文件

图 10-2 PoE Profile

条目介绍：

- **创建 PoE Profile**

文件名称： 输入 Profile 文件的名称。

PoE 状态： 选择启用或禁用相应端口的 PoE 功能。

PoE 优先级： 当剩余功率不够时，与供电管理方式一起决定对新接入的 PD 的供电方式，优先级等级包括高、中、低三种。

功率限制： 设定相应端口能提供的最大功率。Class 1 代表 4w，Class 2 代表 7w，Class 3 代表 15.4w，Class 4 代表 30w。也可以选择自动或者手动输入，手动输入范围值为 0.1w-30w。

- **PoE 配置文件**

选择： 选择 Profile 条目进行删除。

文件名称： 显示 Profile 文件的名称。

PoE 状态： 显示 Profile 文件中设置的端口 PoE 状态。

PoE 优先级： 显示 Profile 文件中设置的端口 PoE 优先级。

最大功率： 显示 Profile 文件中设置的端口 PoE 最大功率。

12.2 时间段

当用户需要某些端口在特定时间段供电时，可以先配置时间段，然后将其应用于这些端口即可。这些端口将只在指定的时间段内供电。

本交换机可设置的时间段包括绝对时间、周期时间和节假日。绝对时间可以设置在自然日内的生效日期，周期时间则可以设置在每周的固定工作日生效，同时可以根据需要设置节假日来应对某些特殊意义的日期。在每个时间段内，还可以设置四个小的时间片段使生效时间更灵活。

本功能包括 **PoE 时间段列表**、**新建 PoE 时间段**和 **PoE 节假日定义**三个配置页面。

12.2.1 PoE 时间段列表

在 PoE 时间段列表页面，可以查看当前已添加的时间段信息。

进入页面的方法：PoE>>时间段>>时间段信息

图 10-3 查看 PoE 时间段列表

条目介绍：

- **时间段列表**

选择： 选择时间段条目进行删除。

序号： 显示时间段条目的序号。

时间片段名称： 显示时间段的名称。

应用模式： 显示时间段的应用模式。

状态： 显示时间段的状态。

操作： 点击相应按键可以查看或编辑相应时间段的详细配置信息。

12.2.2 新建 PoE 时间段

在新建 PoE 时间段页面，可以添加时间段信息。

进入页面的方法：PoE>>时间段>>新建时间段

图 10-4 新建 PoE 时间段

注意：

- 在此页面中，请先配置时间片段，再定义时间段，否则无法配置成功。

条目介绍：

- **时间段定义**

  名称： 填写时间段的名称，便于区分各个时间段的信息。

  假期： 选择不包含节假日后，当系统日期在节假日内时，使用该时间段的端口将停止供电。

- **时间片段**

  绝对时间： 配置时间段的绝对时间模式。只有当系统日期在绝对时间内时，使用该时间段的端口才会供电。

  周期： 配置时间段的周期模式。只有当系统日期在周期时间内时，使用该时间段的端口才会供电。

  起始时间： 配置时间段中时间片段的起始时间。

  结束时间： 配置时间段中时间片段的结束时间。

- **时间片段列表**

  序号： 显示时间片段的序号。

起始时间： 显示时间段中时间片段的起始时间。

结束时间： 显示时间段中时间片段的结束时间。

操作： 点击删除即可删除相应的时间片段。

12.2.3 假期定义

PoE 节假日定义可以提供与工作日不同的供电方式。在本页面，可以根据工作安排自行定义节假日。

进入页面的方法：PoE>>时间段>> PoE 节假日定义

图 10-5 PoE 节假日定义

条目介绍：

- **节假日定义**

起始日期： 配置节假日起始日期。

结束日期： 配置节假日结束日期。

节假日名称： 填写节假日名称，请输入英文字符。

- **节假日列表**

选择： 选择节假日条目进行删除。

序号： 显示节假日条目的序号。

节假日名称： 显示节假日名称。

起始日期： 显示节假日起始日期。

结束日期： 显示节假日结束日期。

回目录

第13章 访问控制

随着网络规模的扩大以及流量的增加，如何有效地控制网络安全和分配带宽已成为网络管理的重要内容。ACL（Access Control List，访问控制列表）功能，通过配置报文的匹配规则和处理方式来实现对数据包的过滤功能，从而有效防止非法用户对网络的访问。另外 ACL 功能也可以控制流量，节约网络资源。ACL 功能对网络安全的控制提供了很大的方便。

在本交换机中，ACL 功能可以对数据包的 L2-L4 层的协议字段进行匹配。通过定义时间段可以设置 ACL 规则的生效时间，配置 policy 可以对匹配了 ACL 规则的数据包进行处理。

13.1 时间段配置

当用户配置的 ACL 规则需要在特定时间段生效时，可以先配置时间段，然后设置 ACL 规则直接引用该时间段即可。ACL 规则只在指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

本交换机可设置的时间段包括绝对时间、周期时间和节假日。绝对时间可以设置在自然日内的生效日期，周期时间则可以设置在每周的固定工作日生效，同时可以根据需要设置节假日来应对某些特殊意义的日期。在每个时间段内，还可以设置四个小的时间片段使生效时间更灵活。

本功能包括**时间段列表**、**新建时间段**和**节假日定义**三个配置页面。

13.1.1 时间段列表

在时间段列表页面，可以查看当前已添加的时间段信息。

进入页面的方法：访问控制>>时间段配置>>时间段列表

图 11-1 查看时间段列表

条目介绍：

- **时间段列表**

选择： 选择时间段条目进行删除。

序号： 显示时间段条目的序号。

时间段名字： 显示时间段的名称。

时间片段： 显示时间段中的时间片段。

应用模式： 显示时间段的应用模式。

操作： 点击相应按键可以查看或编辑相应时间段的详细配置信息。

13.1.2 新建时间段

在新建时间段页面，可以添加时间段信息。

进入页面的方法：访问控制>>时间段配置>>新建时间段

图 11-2 创建时间段

注意：

- 在此页面中，请先配置时间片段，再定义时间段，否则无法配置成功。

条目介绍：

- **时间段定义**

  时间段名称： 填写时间段的名称，便于区分各个时间段的信息。

  节假日： 配置时间段的节假日模式。只有当系统日期在节假日内时，基于该时间段的 ACL 规则才能生效。

  绝对时间： 配置时间段的绝对时间模式。只有当系统日期在绝对时间内，基于该时间段的 ACL 规则才能生效。

  周期： 配置时间段的周期模式。只有当系统日期在周期时间内，基于该时间段的 ACL 规则才能生效。

- **时间片段**

  起始时间： 配置时间段中时间片段的起始时间。

  结束时间： 配置时间段中时间片段的结束时间。

- **时间片段列表**

  序号： 显示时间片段的序号。

  起始时间： 显示时间段中时间片段的起始时间。

  结束时间： 显示时间段中时间片段的结束时间。

  操作： 点击删除即可删除相应的时间片段。

13.1.3 假期定义

节假日定义可以提供与工作日不同的安全访问控制策略。在本页面，可以根据工作安排自行定义节假日。

进入页面的方法：访问控制>>时间段配置>>节假日定义

图 11-3 节假日定义

条目介绍：

- **节假日定义**

起始日期： 配置节假日起始日期。

终止日期： 配置节假日终止日期。

假日名称： 填写假日名称，请输入英文字符。

- **节假日列表**

选择： 选择节假日条目进行删除。

序号： 显示节假日条目的序号。

假日名称： 显示假日名称。

起始日期： 显示节假日起始日期。

终止日期： 显示节假日终止日期。

13.2 ACL 配置

在 ACL 功能中，一个 ACL 可以包括多个规则，而每个规则可以针对数据包中特定字段内容进行匹配。在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，交换机将对该报文执行第一次匹配的规则指定的动作，以此来提高交换机的效率。

ACL 配置功能包括 ACL 列表、新建 ACL、MAC ACL、标准 IP ACL 和扩展 IP ACL 五个配置页面。

13.2.1 ACL 列表

在 ACL 列表页面，可以查看交换机中当前已配置的 ACL 详细信息。

进入页面的方法：访问控制>>ACL 配置>>ACL 列表

图 11-4 查看 ACL 列表

条目介绍：

- **ACL 显示**

  选择 ACL： 选择已创建的 ACL。

  ACL 类型： 显示该 ACL 的类型。

  规则排序： 显示该 ACL 内部的规则如何排序。

- **规则列表**

此处可以查看或编辑 ACL 内部的详细规则信息，点击条目的操作按键可以对规则条目进行排序。

13.2.2 新建 ACL

在新建 ACL 页面，可以创建 ACL。

进入页面的方法：访问控制>>ACL 配置>>新建 ACL

图 11-5 创建 ACL

条目介绍：

- **创建 ACL**

  ACL ID： 配置 ACL ID。

  规则排序： 配置该 ACL 内部的规则如何排序。默认为用户配置。
  用户配置：按照用户配置规则的先后顺序进行规则匹配。

13.2.3 MAC ACL

MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>>MAC ACL

图 11-6 为 MAC ACL 添加规则

条目介绍：

- **MAC ACL**

访问控制列表 ID： 选择需要配置的 ACL ID。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。

- 允许：转发数据包。
- 丢弃：丢弃数据包。

源 MAC： 填写规则包含的源 MAC 地址信息。

目的 MAC： 填写规则包含的目的 MAC 地址信息。

地址掩码： 填写 MAC 地址掩码，掩码置 1 表示严格匹配。

VLAN ID： 配置规则包含的 VLAN 信息。

以太网类型： 配置规则包含的以太网类型信息。

用户优先级： 选择该规则对数据包的 tag 优先级字段的匹配要求。默认为无限制。

时间段： 选择规则生效的时间段名称。默认为无限制。

13.2.4 标准 IP ACL

标准 IP ACL 可以根据数据包的 IP 地址信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>>标准 IP ACL

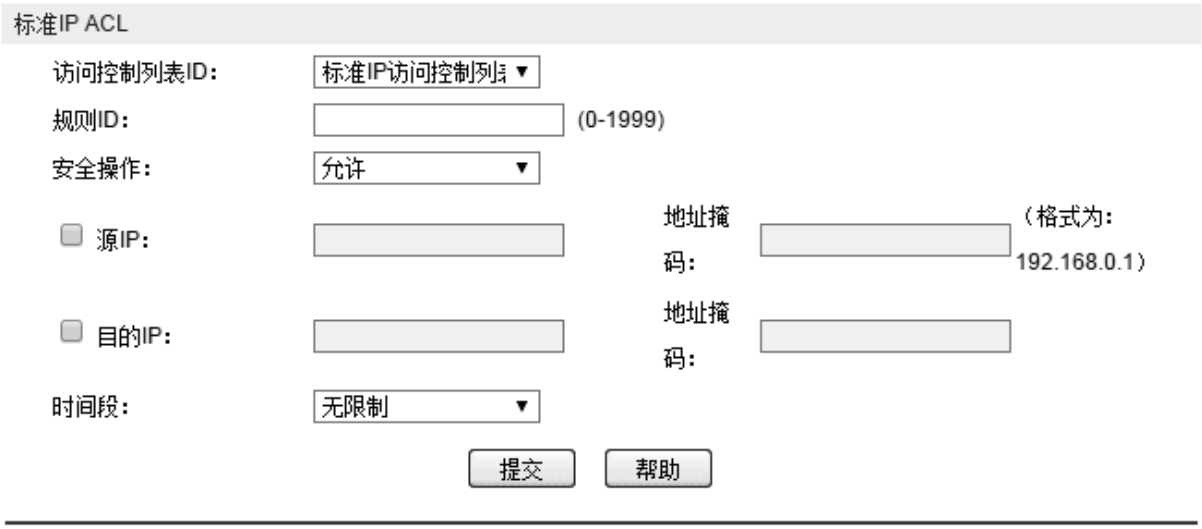


图 11-7 为标准 IP ACL 添加规则

条目介绍：

- **标准 IP ACL**

访问控制列表 ID：	选择需要配置的 ACL ID。
规则 ID：	填写规则 ID。
安全操作：	选择交换机对满足匹配规则的数据包的处理方式。默认为允许。 ● 允许：转发数据包。 ● 丢弃：丢弃数据包。
源 IP：	填写规则包含的源 IP 地址信息。
目的 IP：	填写规则包含的目的 IP 地址信息。
地址掩码：	填写 IP 地址掩码，掩码置 1 表示严格匹配。
时间段：	选择规则生效的时间段名称。

13.2.5 扩展 IP ACL

扩展 IP ACL 可以根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>扩展 IP ACL

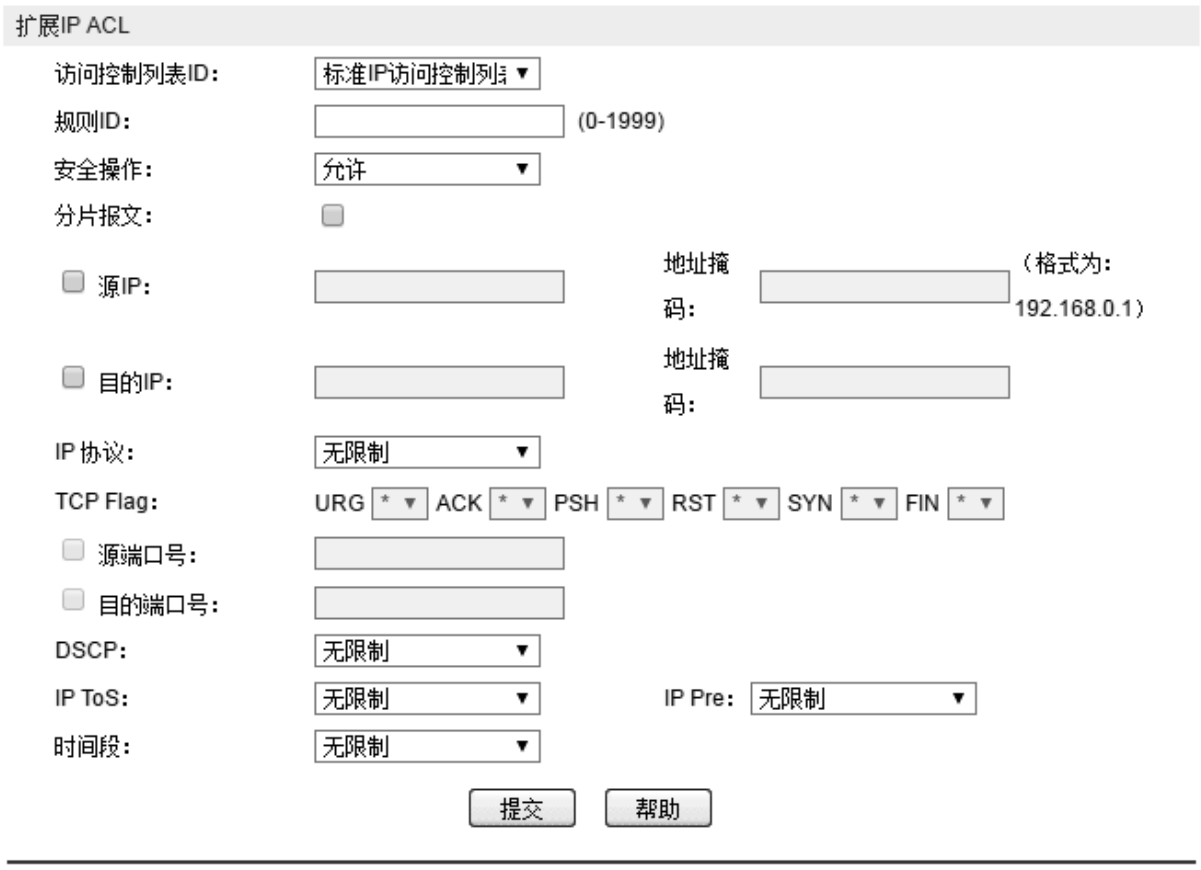


图 11-8 为扩展 IP ACL 添加规则

条目介绍：

- **扩展 IP ACL**

访问控制列表 ID： 选择需要配置的 ACL ID。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。

- 允许：转发数据包。
- 丢弃：丢弃数据包。

源 IP： 填写规则包含的源 IP 地址信息。

目的 IP： 填写规则包含的目的 IP 地址信息。

地址掩码： 填写 IP 地址掩码，掩码置 1 表示严格匹配。

IP 协议： 选择规则包含的 IP 协议信息。

TCP Flag： 当 IP 协议选择 TCP 时，此处配置 Flag 匹配条件。

源端口号： 当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 源端口号。

目的端口号： 当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 目的端口号。

DSCP： 填写规则包含的 DSCP 域信息。

IP ToS： 填写规则包含的 IP ToS 字段信息。

IP Pre： 填写规则包含的 IP Precedence 字段信息。

时间段： 选择规则生效的时间段名称。

13.2.6 组合 ACL

组合 ACL 可以根据报文的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置→组合 ACL

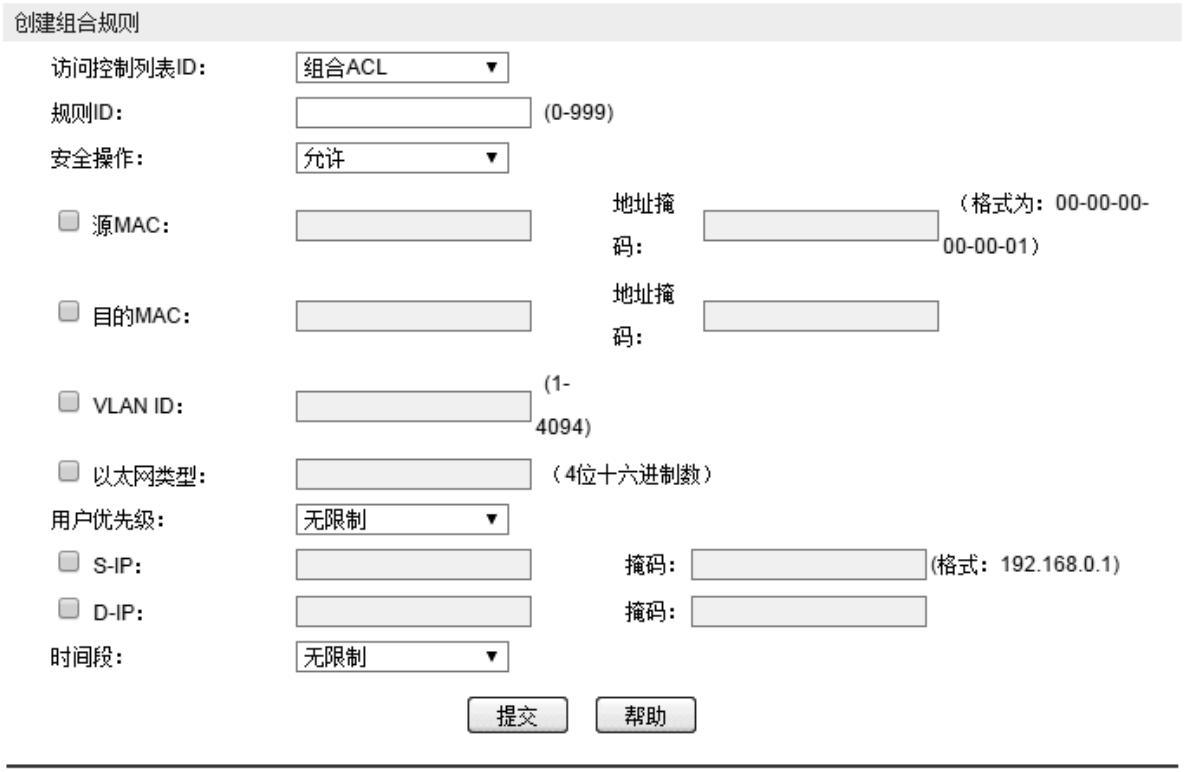


图 13-1 组合 ACL

以下的条目显示在屏幕上:

- **创建组合规则**

访问控制列表 ID： 选择需要配置的 ACL。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。

- 允许：转发数据包。
- 丢弃：丢弃数据包

源 MAC： 填写规则包含的源 MAC 地址信息。

目的 MAC： 填写规则包含的目的 MAC 地址信息。

地址掩码： 填写 MAC 地址掩码，掩码置 1 表示严格匹配。

VLAN ID： 输入规则中包含的 VLAN ID。

以太网类型： 配置规则包含的以太网类型信息。

用户优先级： 选择该规则对数据包的 tag 优先级字段的匹配要求。默认为无限制。

S-IP： 输入规则中包含的源 IP 地址。

D-IP： 输入规则中包含的目的 IP 地址。

掩码： 输入 IP 地址的子网掩码。如果设置为 1，它必须严格匹配地址。

时间段： 选择规则生效的时间段名称。

注意:

组合 ACL 绑定到一个接口或 VLAN 之前，您应该配置 SDM 模板为“默认”或“enterpriseV4”并保存您的配置。有关 SDM 模板配置的更多信息，请参见 SDM 模板。

13.2.7 IPv6 ACL

IPv6 ACL 可以根据报文的源 IPv6 地址、目的 IPv6 地址、端口号等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置→IPv6 ACL

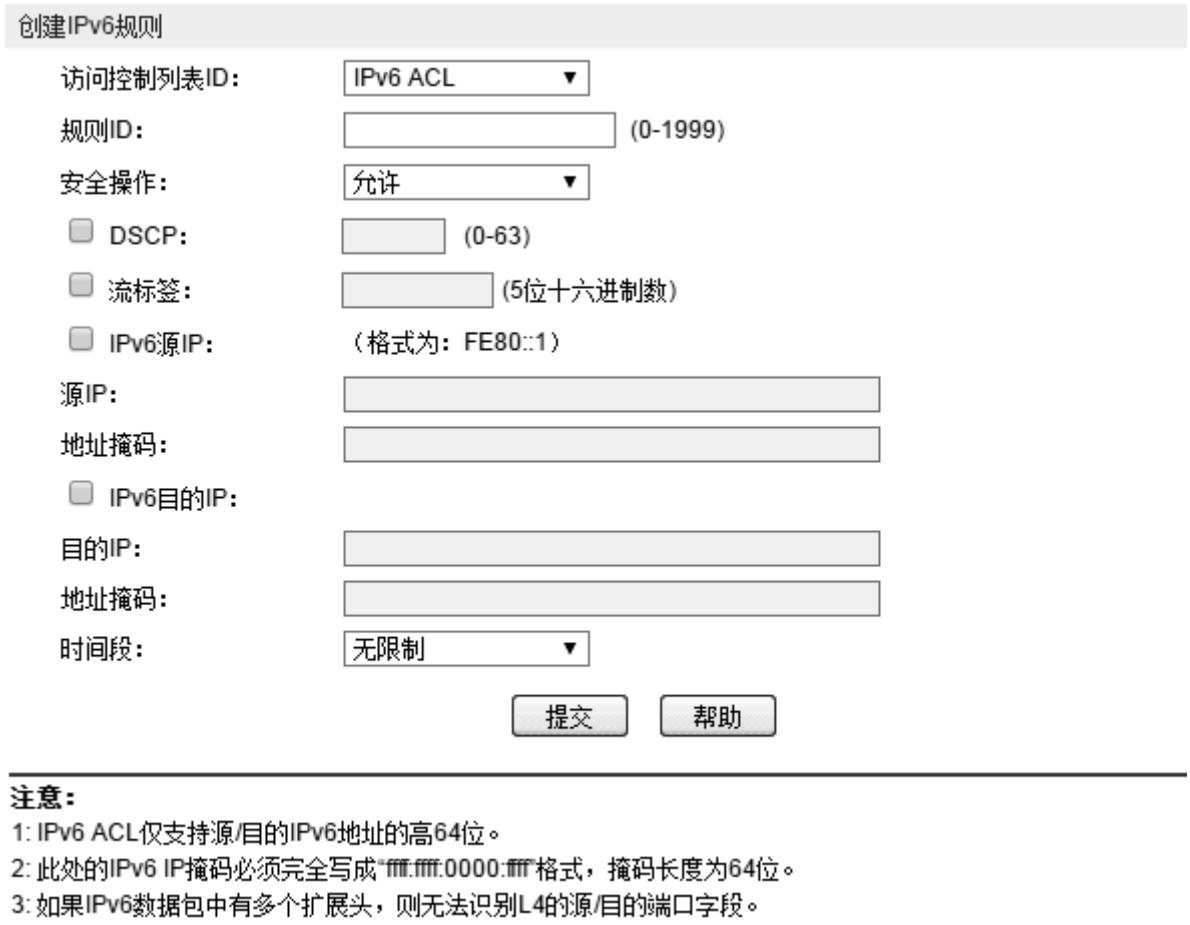


图 13-2 IPv6 ACL 配置

以下的条目显示在屏幕上:

- **创建 IPv6 规则**

访问控制列表 ID： 选择需要配置的 ACL。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式；
允许：转发数据包。
拒绝：丢弃数据包。

DSCP： 填写规则包含的 DSCP 域信息。

流标签： 输入规则中的流标签。

IPv6 源 IP： 输入规则中的源 IPv6 地址，可以输入 128 位，但只支持高 64 位。

地址掩码： 填写 IP 地址掩码，掩码置 1 表示严格匹配。

IPv6 目的 IP： 输入规则中的目的 IPv6 地址，可以输入 128 位，但只支持高 64 位。

地址掩码： 填写 IP 地址掩码，掩码置 1 表示严格匹配。

时间段： 选择规则生效的时间段名称。

注意:

IPv6 ACL 绑定到一个接口或 VLAN 之前，您应该配置 SDM 模板为 “enterpriseV6”并保存您的配置。有关 SDM 模板配置的更多信息，请参见 SDM 模板。

13.3 Policy 配置

Policy 功能是将 ACL 规则和处理方式组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，处理方式包括流镜像、流监控、QoS 重标记和端口重定向。

Policy 配置功能包括 **Policy 列表**、**新建 Policy**、**配置 Policy** 三个配置页面。

13.3.1 Policy 列表

在 Policy 页面可以查看数据包处理方式，对匹配了 ACL 规则的数据包的执行相对应的处理方式。

进入页面的方法：访问控制>>Policy 配置> Policy 列表

图 11-9 查看 Policy 列表

条目介绍：

- **Policy 显示**

选择 Policy： 选择需要查看的 policy 名称。当需要删除相应的 policy 时，选择后点击删除按键即可。

- **Action 列表**

选择： 选择动作条目进行删除。

序号： 显示动作条目的序号。

ACL ID： 显示此 Policy 中包含的 ACL。

流镜像： 显示此 Policy 中的流镜像端口。

流监管： 显示该 Policy 中添加的流监管动作信息。

端口重定向： 显示该 Policy 中添加的端口重定向动作信息。

QoS 重标记： 显示该 Policy 中添加的 QoS 重标记动作信息。

操作： 点击<编辑>按键，可以对编辑相应的 policy 条目。

13.3.2 新建 Policy

在此页面中可以创建 Policy。

进入页面的方法：访问控制>>Policy 配置>新建 Policy

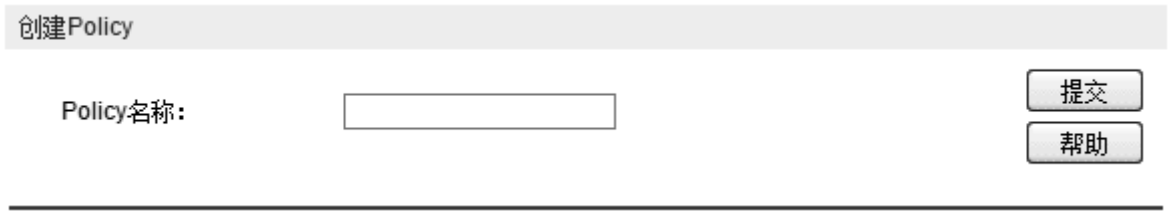


图 11-10 创建 Policy

条目介绍：

- **创建 Policy**

  Policy 名称： 填写 Policy 的名称。

13.3.3 配置 Policy

在此页面中，可以配置 Policy 对应的 ACL 规则以及包含的动作，此动作是对匹配了相应 ACL 规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy 配置>配置 Policy

图 11-11 为 Policy 添加 ACL 并设置动作

条目介绍：

- **Policy 设置**

  选择 Policy： 选择 Policy 的名称。

选择 ACL： 选择 ACL 作为 Policy 作用的对象。

流镜像： 配置该 Policy 的数据包执行流镜像动作，镜像到选定的端口。

流监管： 配置该 Policy 的数据包执行流限速动作。

- 额定速率：为匹配了相应 ACL 的数据包配置额定转发速率。
- 超速处理：为超过额定速率的数据包选择处理方式。

端口重定向： 配置该 Policy 的数据包执行端口重定向动作，改变转发端口。

- 指定出口端口：将匹配了相应 ACL 的数据包指定到固定端口转发。

QoS 重标记： 配置该 Policy 的数据包执行 QoS 动作，根据 QoS 功能具体配置情况转发。

- DSCP：为匹配了相应 ACL 的数据包指定 DSCP 域。
- 本地优先级：为匹配了相应 ACL 的数据包指定优先级。

13.4 ACL 绑定

只有将 ACL 和端口/VLAN 绑定，ACL 才能生效；同样只有绑定了 ACL 的端口和 VLAN 才会对接收到的数据包根据 ACL 进行匹配处理。

绑定配置功能包括**绑定列表、端口绑定、VLAN 绑定**三个配置页面。

13.4.1 绑定列表

在此页面中可以查看已进行端口/VLAN 绑定的 ACL 条目。

进入页面的方法：访问控制>>ACL 绑定>绑定列表

图 11-12 绑定列表

条目介绍：

- **选择显示模式**

  选择显示模式： 请根据需要选择显示模式。

- **ACL 绑定列表**

  选择： 选择绑定条目进行删除。

  序号： 显示绑定条目的序号。

  ACL ID： 显示绑定的 ACL ID。

  绑定接口： 显示与相应 ACL 绑定的端口号或 VLAN ID。

  方向： 显示绑定的方向。

13.4.2 端口绑定

在此页面中可以将 ACL 与端口进行绑定。

进入页面的方法：访问控制>> ACL 绑定>端口绑定

图 11-13 将 ACL 与端口进行绑定

条目介绍：

- **端口绑定配置**

  ACL ID： 选择需要绑定的 ACL 的 ID。

  端口： 配置需要绑定的端口号。

- **端口绑定列表**

序号： 显示绑定条目的序号。

ACL ID： 显示绑定的 ACL 的 ID。

端口： 显示与相应 ACL 绑定的端口号。

方向： 显示绑定的方向。

13.4.3 VLAN 绑定

在此页面中可以将 ACL 与 VLAN 进行绑定。

进入页面的方法：访问控制>> ACL 绑定>VLAN 绑定

图 11-14 将 ACL 与 VLAN 进行绑定

条目介绍：

- **VLAN 绑定配置**

ACL ID： 选择需要绑定的 ACL 的 ID。

VLAN ID： 填写需要绑定的已建立的 VLAN ID。

- **VLAN 绑定列表**

序号： 显示绑定条目的序号。

ACL ID： 显示绑定的 ACL 的 ID。

VLAN ID： 显示与相应 ACL 绑定的 VLAN ID。

方向： 显示绑定的方向。

配置步骤：

步骤	操作	说明
1	配置 ACL 规则	必选操作。在**访问控制>>ACL 配置**标签页中配置 ACL 规则对数据包进行匹配。
2	将 ACL 与端口/VLAN 绑定	必选操作。在**访问控制>>ACL 绑定**标签页中将 ACL 与端口/VLAN 进行绑定，将 ACL 应用到相应的端口/VLAN 上。

13.5 绑定配置

只有将 Policy 和端口/VLAN 绑定，Policy 才能生效；将 Policy 与端口/VLAN 进行绑定后，端口和 VLAN 会对接收到的数据包根据 Policy 进行匹配处理。绑定配置功能将 Policy 应用到某个端口或者 VLAN 上。

绑定配置功能包括**绑定列表、端口绑定、VLAN 绑定**三个配置页面。。

13.5.1 绑定表

在此页面中可以查看已进行端口/VLAN 绑定的 Policy 条目。

进入页面的方法：访问控制>>绑定配置>绑定列表

图 13-3 绑定列表

以下的条目显示在屏幕上:

- **选择显示模式**

  选择显示模式： 请根据需要选择显示模式。

- **Policy 绑定 VLAN 列表**

  选择： 选择绑定条目进行删除。

  序号： 显示绑定条目的序号。

  Policy 名称： 显示绑定的 Policy 名称。

  绑定接口： 显示与相应 Policy 绑定的 VID。

  方向： 显示绑定的方向。

- **Policy 绑定端口列表**

  选择： 选择绑定条目进行删除。

  序号： 显示绑定条目的序号。

  Policy 名称： 显示绑定的 Policy 名称。

  绑定接口： 显示与相应 Policy 绑定的端口号。

  方向： 显示绑定的方向。

13.5.2 端口绑定

在此页面中可以将 Policy 与端口进行绑定。

进入页面的方法：访问控制>>绑定配置>端口绑定

图 13-4 端口绑定配置

以下的条目显示在屏幕上:

- **端口绑定配置**

  Policy 名称： 选择要绑定的 policy 的名称。

  端口： 选择要绑定的端口号。

- **端口绑定列表**

  序号： 显示绑定条目的序号。

  Policy 名称： 显示绑定的 Policy 名称。

  端口： 显示与相应 Policy 绑定的端口号。

方向： 显示绑定的方向。

13.5.3 VLAN 绑定

在此页面中可以将 Policy 与 VLAN 进行绑定。

进入页面的方法：访问控制>>绑定配置>VLAN 绑定

图 13-5 VLAN 绑定配置

以下的条目显示在屏幕上:

- **VLAN-绑定配置**

Policy 名称： 选择要绑定的 policy 的名称。

VLAN ID： 填写需要绑定的已建立的 VLAN ID。

- **VLAN-绑定列表**

序号： 显示绑定条目的序号。

Policy 名称： 显示绑定的 Policy 名称。

VLAN ID： 显示与相应 Policy 绑定的 VLAN ID。

方向： 显示绑定的方向。

配置过程:

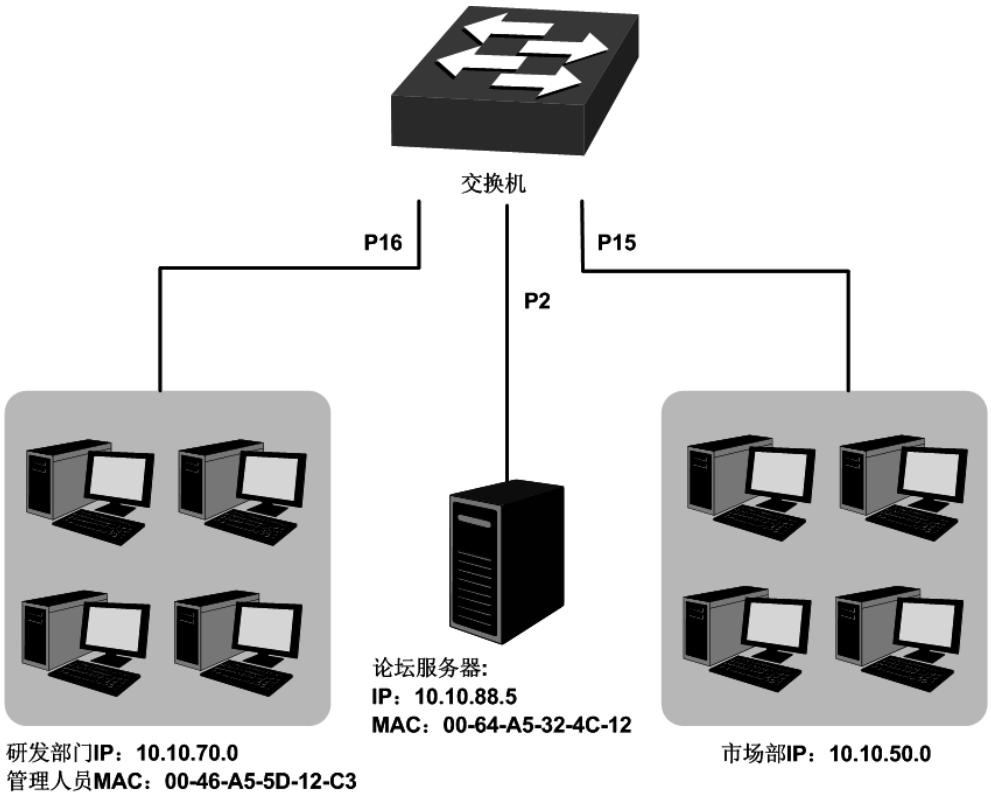
步骤	操作	描述
1	配置 ACL 规则	必选操作。在**访问控制→ACL 配置**页面配置 ACL 规则对数据包进行匹配。
2	配置 policy	必选操作。在**访问控制>>Policy 配置**页面配置 Policy，对匹配了相应 ACL 规则的数据包，通过 Policy 设置进行处理。
3	绑定 policy 到端口/VLAN	必选操作。在**访问控制>>绑定配置**三个标签页中将 Policy 与端口/VLAN 进行绑定，将 Policy 应用到相应的端口/VLAN 上。

13.6 访问控制功能组网应用

- **组网需求**

1. 研发部门的管理人员自由访问公司论坛，管理人员 MAC 地址为 00-46-A5-5D-12-C3。
2. 研发部门工作人员在工作时间可以访问公司论坛。
3. 市场部人员在工作时间不能访问公司论坛。
4. 市场部和研发部门之间互相不能访问。

- **组网图**



- **配置步骤**

步骤	操作	说明
1	需求 1 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 11。 在**访问控制>>ACL 配置>>MAC ACL** 页面，选择 ACL 11，创建规则 1，安全操作设置为允许；勾选源 MAC 设置为 00-46-A5-5D-12-C3，掩码为 FF-FF-FF-FF-FF-FF；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 manager。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 11 应用到 Policy manager。 在**访问控制>>绑定配置>>端口绑定**页面，选择 Policy manager 与端口 16 绑定。

步骤	操作	说明
2	需求 2、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 100。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 1，安全操作设置为丢弃；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.50.0，掩码为 255.255.255.0；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 2，安全操作设置为允许；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择 work_time。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 3，安全操作设置为丢弃；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit1。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 100 应用到 Policy limit1。 在**访问控制>>绑定配置>>端口绑定**页面，选择 Policy limit1 与端口 16 绑定。
3	需求 3、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 101。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 101，创建规则 4，安全操作设置为丢弃；设置源 IP 为 10.10.50.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.70.0，掩码为 255.255.255.0；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 101，创建规则 5，安全操作设置为丢弃；设置源 IP 为 10.10.50.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择 work_time。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit2。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 101 应用到 Policy limit2。 在**访问控制>>绑定配置>>端口绑定**页面，选择 Policy limit2 与端口 15 绑定。

回目录

第14章 网络安全

网络安全模块为保护局域网安全提供了多项安全措施，包括**四元绑定**、**IPv6-MAC 绑定**、**DHCP 侦听**、**DHCPv6 侦听**、**ARP 防护**、**ND 检测**、**IP 源防护**、**DoS 防护**、**802.1X 认证**、**PPPoE** 以及 **AAA**，请根据实际需要进行配置。

14.1 四元绑定

四元绑定，是将计算机的 MAC 地址、IP 地址、所属 VLAN 以及与之相连的交换机的端口号四者绑定，以下这四个参数信息简称四元信息。该功能可以启用 ARP 防护和 IP 源防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种四元绑定方式：

1) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

2) 扫描绑定：通过 ARP 扫描获取局域网用户的四元信息，并根据实际需要选择扫描结果进行绑定。此绑定方式只需在相应的功能页面输入 IP 地址段进行扫描。

3) DHCP 侦听：通过 DHCP 侦听功能侦听 DHCP 广播包，记录数据包中的 IP、MAC 和 VLAN ID 等信息。当局域网中搭建了 DHCP 服务器给局域网用户分配 IP 地址时，DHCP 侦听功能可以很方便地记录局域网用户的四元信息。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是扫描绑定，DHCP 侦听优先级最低。

本功能包括**绑定列表**、**手动绑定**和**扫描绑定**。

14.1.1 绑定列表

在绑定列表页面中，可以查看当前交换机已进行四元绑定的局域网计算机条目信息。

进入页面的方法：网络安全>>四元绑定>>绑定列表

图 12-1 查看四元绑定信息

条目介绍：

- **搜索条目**

来源： 选择查看不同来源的四元绑定条目。

- 全部来源：查看全部四元绑定条目。
- 手动添加：只查看手动添加的四元绑定条目。
- ARP 扫描：只查看通过 ARP 扫描获得的四元绑定条目。
- DHCP 侦听：只查看通过 DHCP 侦听获得的四元绑定条目。

IP： 单击选择按钮，根据您输入的 IP 地址快速选择相应的条目。

- **四元绑定表**

选择： 勾选条目可修改主机名及防护范围，可多选。

主机名： 显示主机描述名称。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示并编辑此条目支持的防护范围。

来源： 显示此条目的来源。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

注意：

- 冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。

14.1.2 手动绑定

当已经获取了局域网用户的四元信息时，可以将四元信息静态绑定。

进入页面的方法：网络安全>>四元绑定>>手动绑定

图 12-2 手动绑定四元信息

条目介绍：

- **手动绑定**

  主机名： 输入主机描述名称。

  IP 地址： 输入主机 IP 地址。

  MAC 地址： 输入主机 MAC 地址。

  VLAN ID： 输入 VLAN ID。

  端口： 输入主机连接的交换机端口。

  防护范围： 选择此条目支持的防护范围。

  绑定： 点击此按键将上述输入信息进行绑定。

- **手动绑定条目**

  选择： 勾选条目进行删除。

  主机名： 显示主机描述名称。

  IP 地址： 显示主机 IP 地址。

  MAC 地址： 显示主机 MAC 地址。

  VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

14.1.3 扫描绑定

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的 IP 地址解析为数据链路层地址。IP 地址只是主机在网络层中的地址，如果要将网络层中数据包传送给目的主机，必须知道目的主机的数据链路层地址（比如以太网络 MAC 地址）。因此必须将 IP 地址解析为数据链路层地址。

ARP 协议用于将 IP 地址解析为 MAC 地址，并在主机内部维护一张 ARP 表，记录最近与本主机通信的其它主机的 MAC 地址与 IP 地址的对应关系。当主机需要与陌生主机通信时，首先进行 ARP 地址解析，ARP 地址解析过程如图 12-3 所示：

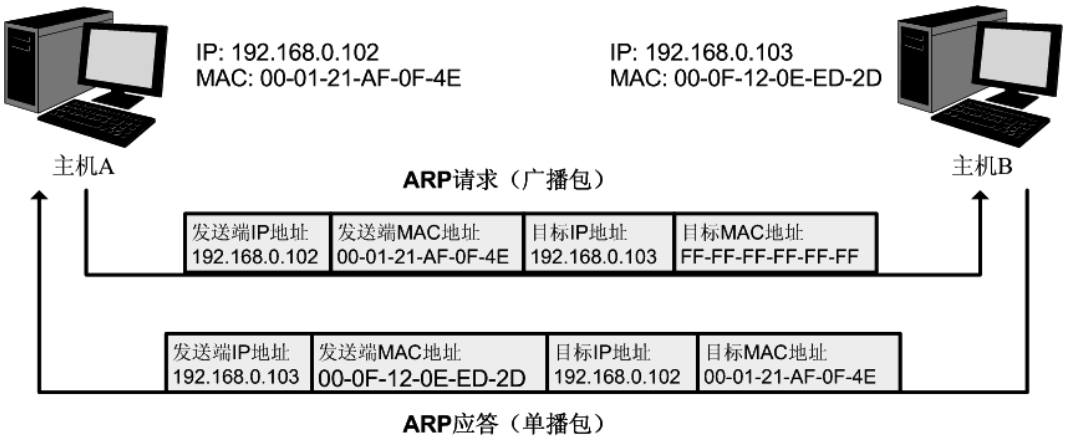


图 12-3 ARP 地址解析图

1) A 在自己的 ARP 表中查询是否存在主机 B 的 IP 地址和 MAC 地址的对应条目。若存在，直接向主机 B 发送数据。若不存在，则 A 向整个局域网中广播一份称为“ARP 请求”的数据链路帧，这个请求包含发送端（即主机 A）的 IP 地址和 MAC 地址以及接收端（即主机 B）的 IP 地址。

2) 局域网的每个主机接收到主机 A 广播的 ARP 请求后，目的主机 B 识别出这是发送端在询问它的 IP 地址，于是给主机 A 发出一个 ARP 应答。这个应答包含了主机 B 的 MAC 地址。

3) 主机 A 接收到主机 B 发出的 ARP 应答后，就将主机 B 的 IP 地址与 MAC 地址的对应条目添加自己的 ARP 表中，以便后续报文的转发。

扫描绑定功能即通过交换机向局域网或 VLAN 发送指定 IP 段的 ARP 请求报文，当收到相应的 ARP 应答报文时，将分析 ARP 应答报文来获得四元信息。由此可见，通过扫描绑定功能可以很方便的将局域网用户的四元信息进行绑定。

进入页面的方法：网络安全>>四元绑定>>扫描绑定

图 12-4 扫描绑定四元信息

条目介绍：

- **ARP 扫描**

  起始 IP 地址： 输入起始 IP 地址。

  结束 IP 地址： 输入结束 IP 地址。

  VLAN ID: 输入 VLAN ID，在相应的 VLAN 中进行扫描。若留空，则发送 untag 数据包进行扫描。

  扫描： 点击<扫描>按键将对局域网计算机进行扫描。

- **扫描结果**

  选择： 勾选条目进行删除。

  主机名： 显示主机描述名称或对主机进行描述以便区分。

  IP 地址： 显示主机 IP 地址。

  MAC 地址： 显示主机 MAC 地址。

  VLAN ID： 显示 VLAN ID。

  端口： 显示主机连接的交换机端口。

  防护范围： 显示此条目支持的防护范围或者对此条目开启防护功能。

  冲突： 显示此绑定条目与其它条目的冲突状态。
  - 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
  - 严重：已确定的冲突条目。

14.2 IPv6-MAC 绑定

IPv6-MAC 绑定，是将计算机的 MAC 地址、IPv6 地址、所属 VLAN 以及与之相连的交换机的端口号四者绑定。该功能可以启用 ND 侦听和 IPv6 防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种绑定方式：

4) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

5) ND 侦听：通过 ND 侦听功能侦听重复地址检测过程，并记录主机的 IP 地址、MAC 地址、VLAN 和主机的连接端口号，可通过此方式进行绑定。

6) DHCP 侦听：通过 DHCPv6 侦听功能侦听 DHCPv6 广播包，记录 DHCPv6 服务器给局域网用户分配 IPv6 地址的过程，并记录主机的 IP、MAC 地址、VLAN 和主机的连接端口号，可通过此方式进行绑定。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是 DHCPv6 侦听，ND 侦听优先级最低。

本功能包括**绑定列表**、**手动绑定**和 **ND 侦听**。

14.2.1 绑定列表

在这个页面中，您可以查看 IPv6 相关的绑定条目的信息。

进入页面的方法：网络安全→IPv6-MAC 地址绑定→绑定列表

图 14-1 绑定列表

条目介绍：

- **搜索条目**

来源： 查看不同来源的四元绑定条目。

- 全部来源：查看全部四元绑定条目。
- 手动添加：只查看手动添加的四元绑定条目。
- ND 侦听：只查看通过 ND 侦听获得的条目。
- DHCP 侦听：只查看通过 DHCPv6 侦听获得的四元绑定条目。

IP： 单击选择按钮，根据您输入的 IPv6 地址快速选择相应的条目。

- **绑定列表**

选择： 勾选条目可修改主机名及防护范围，可多选。

主机名： 显示主机描述名称。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示并编辑此条目支持的防护范围。

活动状态： 显示条目的活动状态。

来源： 显示此条目的来源。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

注意:

- 冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。

14.2.2 手动绑定

当已经获取了局域网用户的四元信息时，可以将四元信息静态绑定。

进入页面的方法：网络安全→IPv6-MAC 地址绑定→手动绑定

图 14-2 手动绑定

条目介绍：

- **手动绑定**

主机名： 输入主机描述名称。

IP 地址： 输入主机 IP 地址。

MAC 地址： 输入主机 MAC 地址。

VLAN ID： 输入 VLAN ID。

防护范围： 选择此条目支持的防护范围。

端口： 输入主机连接的交换机端口。

绑定： 点击此按键将上述输入信息进行绑定。

- **手动绑定条目**

选择： 勾选条目进行删除。

主机名： 显示主机描述名称。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围。

活动状态： 显示该条目的活动状态。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

14.2.3 ND 侦听

ND 侦听功能用于侦听重复地址检测过程，并记录主机的 IP 地址、MAC 地址、VLAN 和主机的连接端口号，进行自动绑定。

进入页面的方法：网络安全→IPv6-MAC 地址绑定→ND 侦听

图 14-3 ARP 侦听

条目介绍：

- **ND 侦听**

ND 侦听： 全局启用/禁用 ND 侦听功能。

VLAN ID： 在指定 VLAN 中启用/禁用 ND 侦听功能。

VLAN 配置显示： 显示已启用 ND 侦听功能的 VLAN ID。

- **端口配置**

选择： 选择所需的端口进行配置，可多选。

端口： 显示端口号。

最大条目： 设置端口通过 ND 侦听功能可以学习到的最大绑定条目。

LAG： 显示端口属于的汇聚组。

14.3 DHCP 侦听

随着网络规模的不断扩大和网络复杂度的提高，经常出现计算机的数量超过可供分配的 IP 地址的情况。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在 BOOTP 协议基础上进行了优化和扩展而产生的一种网络配置协议，并有效解决了上面这些问题。

- **DHCP 工作原理**

DHCP 采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现网络资源的动态配置。通常一台服务器可以为多台客户端分配 IP，如图 12-5 所示：

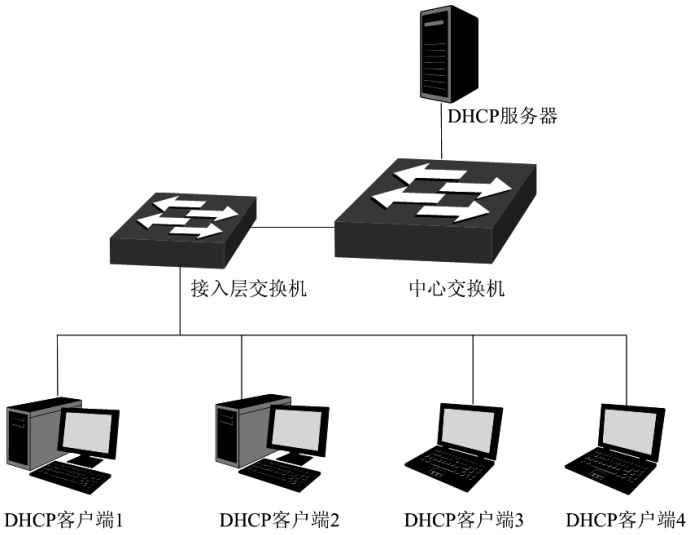


图 12-5 DHCP 网络典型应用

针对 DHCP 客户端的需求不同，DHCP 服务器提供三种 IP 地址分配策略：

1) 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定 IP 地址。通过 DHCP 将固定 IP 地址分配给客户端。

2) 自动分配地址：DHCP 服务器为客户端分配租期为无限长的 IP 地址。

3) 动态分配地址：DHCP 服务器为客户端分配具有一定有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。

绝大多数客户端均通过动态分配地址的方式获取 IP 地址，其获取 IP 地址的过程如下图所示：

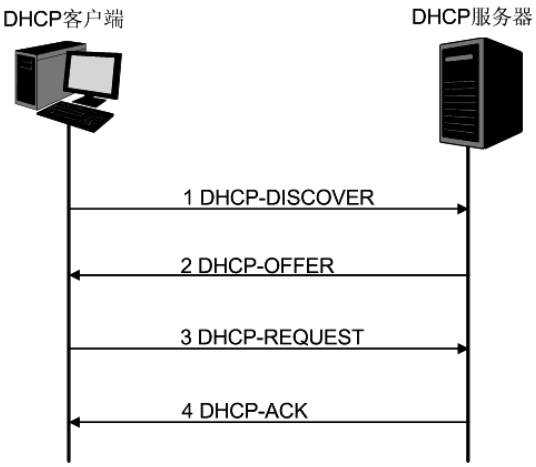


图 12-6 动态获取 IP 地址的过程

1) 发现阶段，客户端以广播方式发送 DHCP-DISCOVER 报文寻找 DHCP 服务器。

2) 提供阶段，DHCP 服务器接收到客户端发送的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序从地址池中选出一个 IP 地址，与其它参数一起通过 DHCP-OFFER 报文发送给客户端（发送方式根据客户端发送的 DHCP-DISCOVER 报文中的 flag 字段决定，具体请见 DHCP 报文格式的介绍）。

3) 选择阶段，如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，客户端只接受第一个收到的 DHCP-OFFER 报文，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。

4) 确认阶段，DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回 DHCP-ACK 报文；否则将返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

- **Option 82**

DHCP 报文格式基于 BOOTP 的报文格式，共有 8 种类型的报文，每种报文的格式相同。DHCP 和 BOOTP 消息的不同主要体现在选项(Option)字段,并利用 Option 字段来实现功能扩展。例如 DHCP 可以利用 Option 字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。更多 DHCP Option 选项的介绍，请参见 RFC 2132。

Option 82 选项记录了 DHCP 客户端的位置信息，交换机接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制订 IP 地址和其它参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

- **DHCP 服务欺骗攻击**

在 DHCP 工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的 DHCP 服务器，通常分为两种情况：

1) 用户不小心配置的 DHCP 服务器，由此引起的网络混乱非常常见。

2) 黑客将正常的 DHCP 服务器中的 IP 地址耗尽，然后冒充合法的 DHCP 服务器，为客户端分配 IP 地址等配置参数。例如黑客利用冒充的 DHCP 服务器，为用户分配一个经过修改的 DNS 服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如图 12-7 所示。

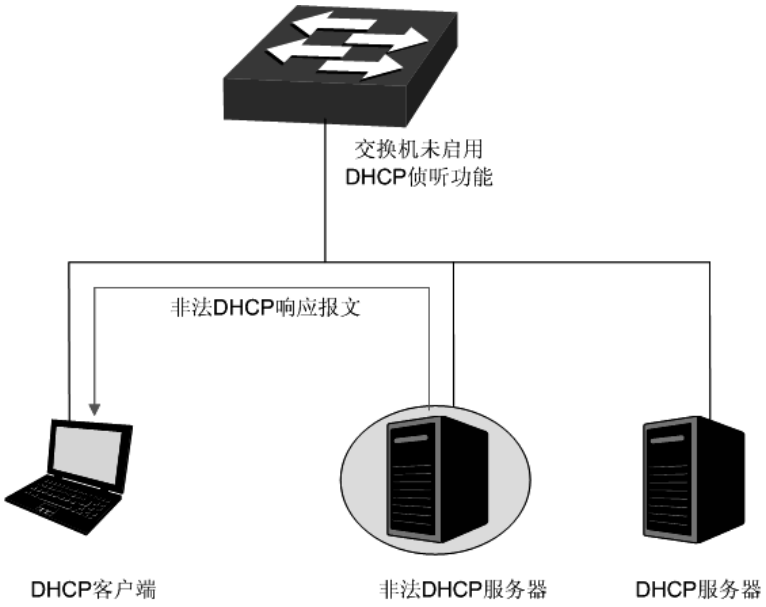


图 12-7 DHCP 服务欺骗攻击

DHCP 侦听是运行在交换机上的一种 DHCP 安全特性。通过设置 DHCP 服务器的连接端口为授信端口，只处理授信端口发来的 DHCP 响应报文；通过监听 DHCP 报文，记录用户从 DHCP 服务器获取局域网用户的四元信息，进行绑定后与 ARP 攻击防护配合使用；同时也可以过滤不可信任的 DHCP 信息，防止局域网中发生 DHCP 服务欺骗攻击，提高网络的安全性。

14.3.1 全局配置

进入页面的方法：网络安全→DHCP 侦听→全局配置

图 14-4 DHCP 侦听

条目介绍：

- **DHCP 侦听配置**

DHCP 侦听： 选择启用/禁用 DHCP 侦听功能。

VLAN ID： 在指定 VLAN 中启用/禁用 DHCP 侦听功能。

VLAN 配置显示： 显示已启用 DHCP 侦听功能的 VLAN ID。

14.3.2 端口配置

进入页面的方法：网络安全→DHCP 侦听→端口配置

图 14-5 DHCP 侦听

- **DHCP 侦听端口配置**

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

授信端口： 选择是否配置端口为授信端口，只有授信端口才正常转发来自正常 DHCP 服务器端的消息，请将连接有 DHCP 服务器的端口设为授信端口。

MAC 验证： 选择是否启用 MAC 验证功能。DHCP 消息中有两个字段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

流量控制： 选择是否对 DHCP 数据包启用流量控制功能，超出流量部分的 DHCP 数据包将被丢弃。

Decline 侦听： 选择是否启用端口的 Decline 侦听功能。

LAG： 显示端口当前所属的汇聚组。

14.3.3 Option82 配置

交换机可以利用 Option 82 字段传递控制信息和网络配置参数，为客户端提供更加丰富的网络配置信息。Option 82 功能的配置只有在 DHCP 侦听功能开启之后才会生效。

进入页面的方法：网络安全→DHCP 侦听→Option 82 配置

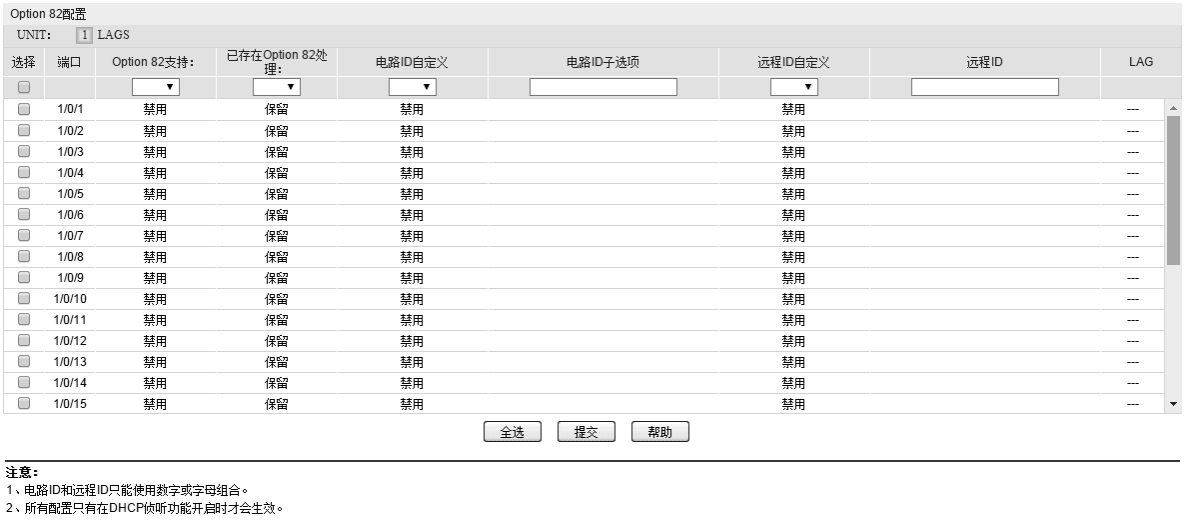


图 14-6 Option 82 配置

- **Option 82 配置**

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

Option 82 支持： 选择是否启用 Option 82 功能。

已存在 Option 82 处理： 当客户端的 DHCP 请求数据包已经有 Option 82 字段时，选择对此字段的操作。如果已经启用 Option 82 功能，DHCP 服务器回复报文中的 option 82 字段将会被移除，与所配置的对此字段的操作无关。

保留：保留数据包中的 Option 字段信息。

替换：替换数据包中的 Option 字段信息，替换为交换机自定义的选项内容。

丢弃：丢弃包含 Option 82 字段的数据包。

电路 ID 自定义： 开启或禁用自定义 Option 82 选项电路 ID 子选项。当选择禁用时，电路 ID 子选项默认的内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号。

电路 ID 子选项： 输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。

远程 ID 自定义 开启或禁用自定义 Option 82 选项中远程 ID 子选项。当选择禁用时，远程 ID 子选项默认的内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

远程 ID： 输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

14.4 DHCPv6 侦听

DHCPv6 侦听功能可以侦听主机从 DHCPv6 服务器获取 IPv6 地址的过程，记录用户从 DHCPv6 服务器获取局域网用户的四元信息。

进入页面的方法：网络安全→DHCPv6 侦听→DHCPv6 侦听

图 14-7 DHCPv6 侦听

- **DHCPv6 侦听**

DHCPv6 侦听： 选择启用/禁用 DHCP 侦听功能。。

VLAN ID： 在指定 VLAN 中启用/禁用 DHCP 侦听功能。

VLAN 配置显示： 显示已启用 DHCP 侦听功能的 VLAN ID。

- **信任端口**

信任端口： 将端口配置为信任端口，只有信任端口才能转发来自 DHCPv6 服务器端的报文。

14.5 ARP 防护

根据 11.1.3 扫描绑定所述的 ARP 地址解析过程可知，利用 ARP 协议，可以实现相同网段内的主机之间正常通信或者通过网关与外网进行通信。但由于 ARP 协议是基于网络中的所有主机或者网关都

为可信任的前提制定的，因此在实际复杂的网络中，此过程存在大量的安全隐患，从而导致针对 ARP 协议的欺骗攻击非常常见。网关仿冒、欺骗网关、欺骗终端用户和 ARP 泛洪攻击均是在学校等大型网络中常见的 ARP 攻击，以下简单介绍这几种常见攻击：

- **网关仿冒**

攻击者发送错误的网关 MAC 给受害者，而网络中的受害者收到这些 ARP 响应报文时，自动更新 ARP 表，导致不能正常访问网络。如图 12-9 所示。

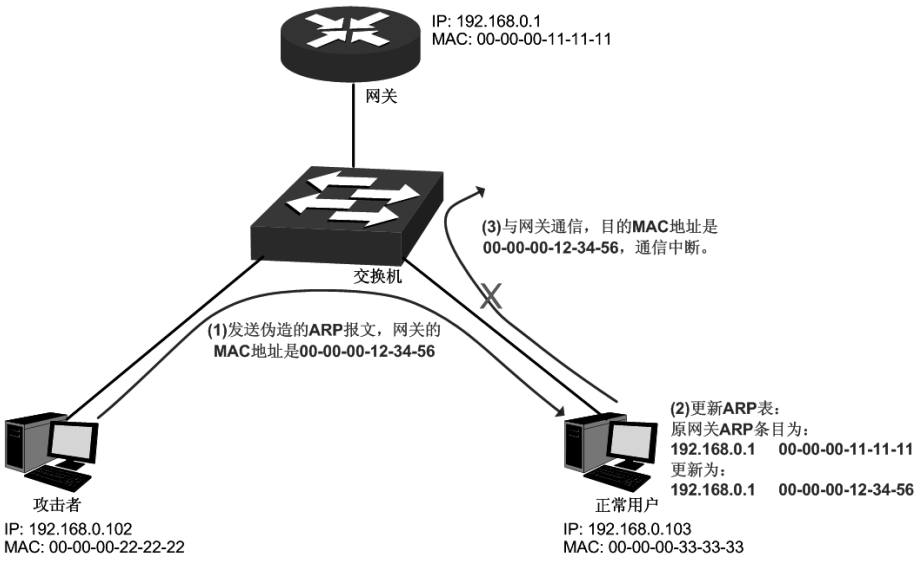


图 12-9 ARP 攻击-网关仿冒示意图

如图，攻击者发送伪造的网关 ARP 报文给局域网中的正常用户，相应的局域网用户收到此报文后更新自己的 ARP 表项。当局域网中正常用户要与网关进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗网关**

攻击者发送错误的终端用户的 IP/MAC 的对应关系给网关，导致网关无法和合法终端用户正常通信。如图 12-10 所示。

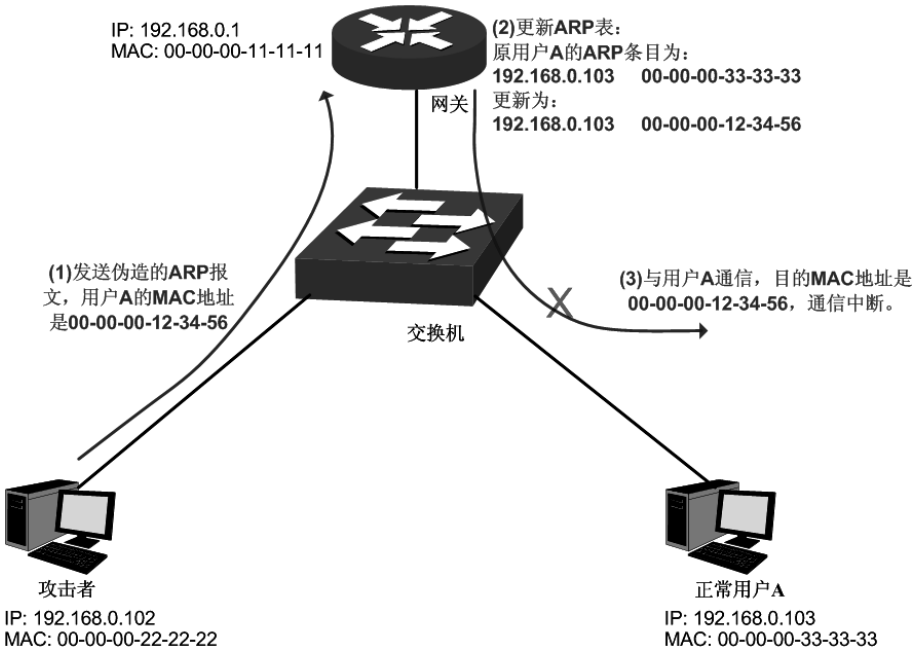


图 12-10 ARP 攻击-欺骗网关示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给网关，网关收到此报文后更新自己的 ARP 表项，当网关与局域网中用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗终端用户**

攻击者发送错误的终端用户/服务器的 IP/MAC 的对应关系给受害的终端用户，导致同网段内两个终端用户之间无法正常通信。如图 12-11 所示。

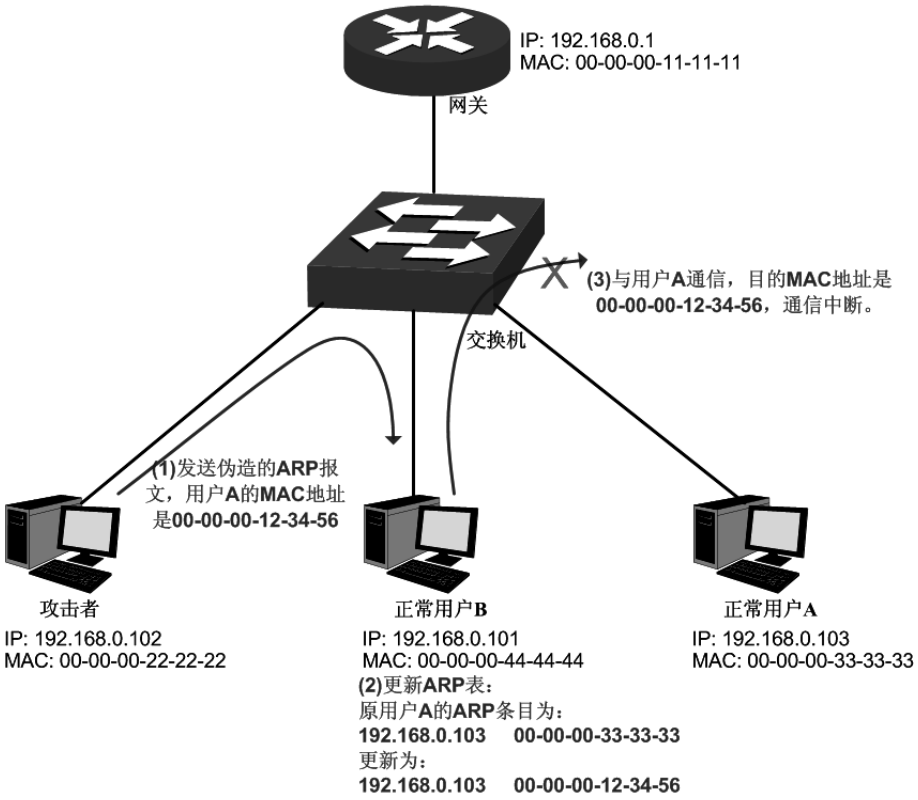


图 12-11 ARP 攻击-欺骗普通用户示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给用户 B，用户 B 收到此报文后更新自己的 ARP 表项，当用户 B 与用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **中间人攻击**

攻击者不断向局域网中计算机发送错误的 ARP 报文，使受害主机一直维护错误的 ARP 表项。当局域网主机互相通信时，将数据包发给攻击者，再由攻击者将数据包进行处理后转发。在这个过程中，攻击者窃听了通信双方的数据，而通信双方对此并不知情。这就是中间人攻击。如图 12-12 所示。

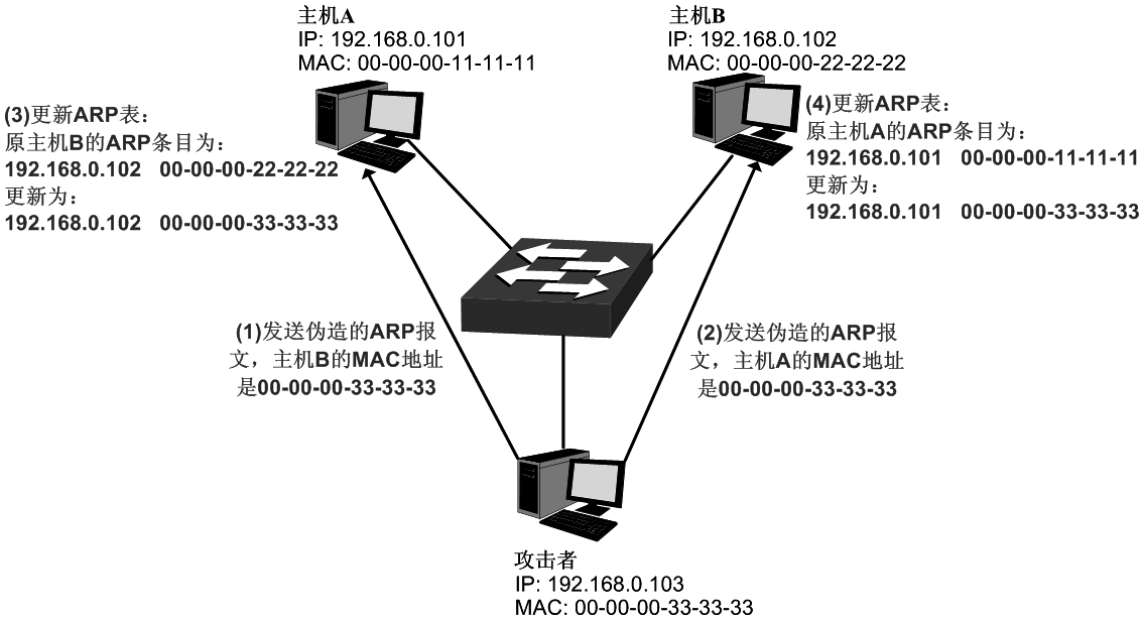


图 12-12 中间人攻击

假设同一个局域网内，有 3 台主机通过交换机相连：

A 主机：IP 地址为 192.168.0.101，MAC 地址为 00-00-00-11-11-11；

B 主机：IP 地址为 192.168.0.102，MAC 地址为 00-00-00-22-22-22；

攻击者：IP 地址为 192.168.0.103，MAC 地址为 00-00-00-33-33-33。

1. 首先，攻击者向主机 A 和主机 B 发送伪造的 ARP 应答报文。
2. A 主机和 B 主机收到此 ARP 应答后，更新各自的 ARP 表。
3. A 主机和 B 主机通信时，将数据包发送给错误的 MAC 地址，即攻击者。
4. 攻击者窃听了通信数据后，将数据包处理后再转发到正确的 MAC 地址，使 A 主机和 B 主机保持正常的通信。
5. 攻击者连续不断地向 A 主机和 B 主机发送伪造的 ARP 响应报文，使二者的始终维护错误的 ARP 表。

在 A 主机和 B 主机看来，彼此发送的数据包都是直接到达对方的，但在攻击者看来，其担当的就是“第三者”的角色。这种嗅探方法，也被称作“中间人”的方法。

- **ARP 泛洪攻击**

攻击者伪造大量不同 ARP 报文在同网段内进行广播，消耗网络带宽资源，造成网络速度急剧降低；同时，网关学习此类 ARP 报文，并更新 ARP 表，导致 ARP 表项被占满，无法学习合法用户的 ARP 表，导致合法用户无法访问外网。

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在 ARP 防护功能中则利用在交换机中绑定的四元信息对 ARP 报文进行检查，过滤非法 ARP 报文。通过上述两步可以很好的对局域网中 ARP 攻击进行防御。

本功能包括**防 ARP 欺骗**、**防 ARP 攻击**和**报文统计**三个功能配置页面。

14.5.1 防 ARP 欺骗

防 ARP 欺骗功能，通过四元绑定表对交换机收到的 ARP 报文进行检查，过滤非法的 ARP 报文，以此防御局域网中的 ARP 攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 欺骗

图 12-13 防 ARP 欺骗

条目介绍：

- **防 ARP 欺骗**

  防 ARP 欺骗： 选择启用并单击<提交>按键即可启用防 ARP 欺骗功能。

- **信任端口**

  信任端口： 勾选无须启用防 ARP 欺骗功能的信任端口。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

配置步骤：

步骤	操作	说明
1	绑定四元信息条目	必选操作。在**四元绑定**功能中将接入用户的四元信息进行绑定，手动绑定、扫描绑定和 DHCP 侦听方式均可进行绑定
2	对四元信息条目启用防护	必选操作。在**网络安全>>四元绑定>>绑定列表**页面中对相应

步骤	操作	说明
		的四元条目启用防护。
3	设置信任端口	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中设置信任端口，上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。
4	启用防 ARP 欺骗	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中启用防 ARP 欺骗功能。

14.5.2 防 ARP 攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阀值，在单位时间内不可超过设定值。超过设定值时，交换机将停止处理 ARP 数据包 300 秒，能够有效的避免 ARP 泛洪攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 攻击

图 12-14 防 ARP 攻击

条目介绍：

- **防 ARP 攻击配置**

选择： 勾选端口配置端口防 ARP 攻击功能参数，可多选。

端口： 显示交换机的端口号。

防护功能： 选择是否启用防 ARP 攻击功能。

速率： 填写端口每秒允许接收的 ARP 数据包个数。

当前速率： 显示端口当前收到的 ARP 数据包速率。

状态： 显示端口当前防 ARP 攻击状态。

LAG： 显示端口当前所属的汇聚组。

操作： 点击<恢复>按键使端口恢复正常状态，并重新启用防 ARP 攻击功能。

注意：

- 建议 LAG 端口不要开启防 ARP 攻击功能。

14.5.3 报文统计

通过报文统计功能，可以直观地查看各个端口收到的非法 ARP 数据包个数，并以此定位网络问题，并采取相应的防护措施。

进入页面的方法：网络安全>>ARP 防护>>报文统计

图 12-15 报文统计

条目介绍：

- **自动刷新**

自动刷新： 设置是否自动刷新端口统计情况。

刷新周期： 设置自动刷新周期。

- **ARP 非法数据包统计**

端口： 显示交换机的端口号。

信任端口： 显示端口是否是 ARP 信任端口。

非法 ARP 报文： 显示端口收到的非法 ARP 数据包数量。

14.6 ND 探测

ND (Neighbor Discovery Protocol)探测功能可以保护交换机免受 IPv6 路由欺骗，IPv6 重复地址检测欺骗和 IPv6 地址解析欺骗等恶意 NDP 攻击。

进入页面的方法：网络安全→ND 探测→ND 探测

图 14-8 ND 检测

- **ND 检测**

ND 检测： 选择启用/禁用 ND 探测功能。

VLAN ID： 在指定 VLAN 上启用/禁用 ND 探测功能。

VLAN 配置显示： 显示已启用 ND 检测的 VLAN ID。

- **信任端口**

信任端口： 选择启用/禁用端口作为信任端口。只有信任端口才能转发路由器广告信息和重定向消息。

14.7 IP 源防护

IP 源保护根据四元绑定列表过滤 IP 数据包。数据包只有匹配绑定规则才可以被处理，以此提高带宽利用率。

进入页面的方法：网络安全→IP 源防护

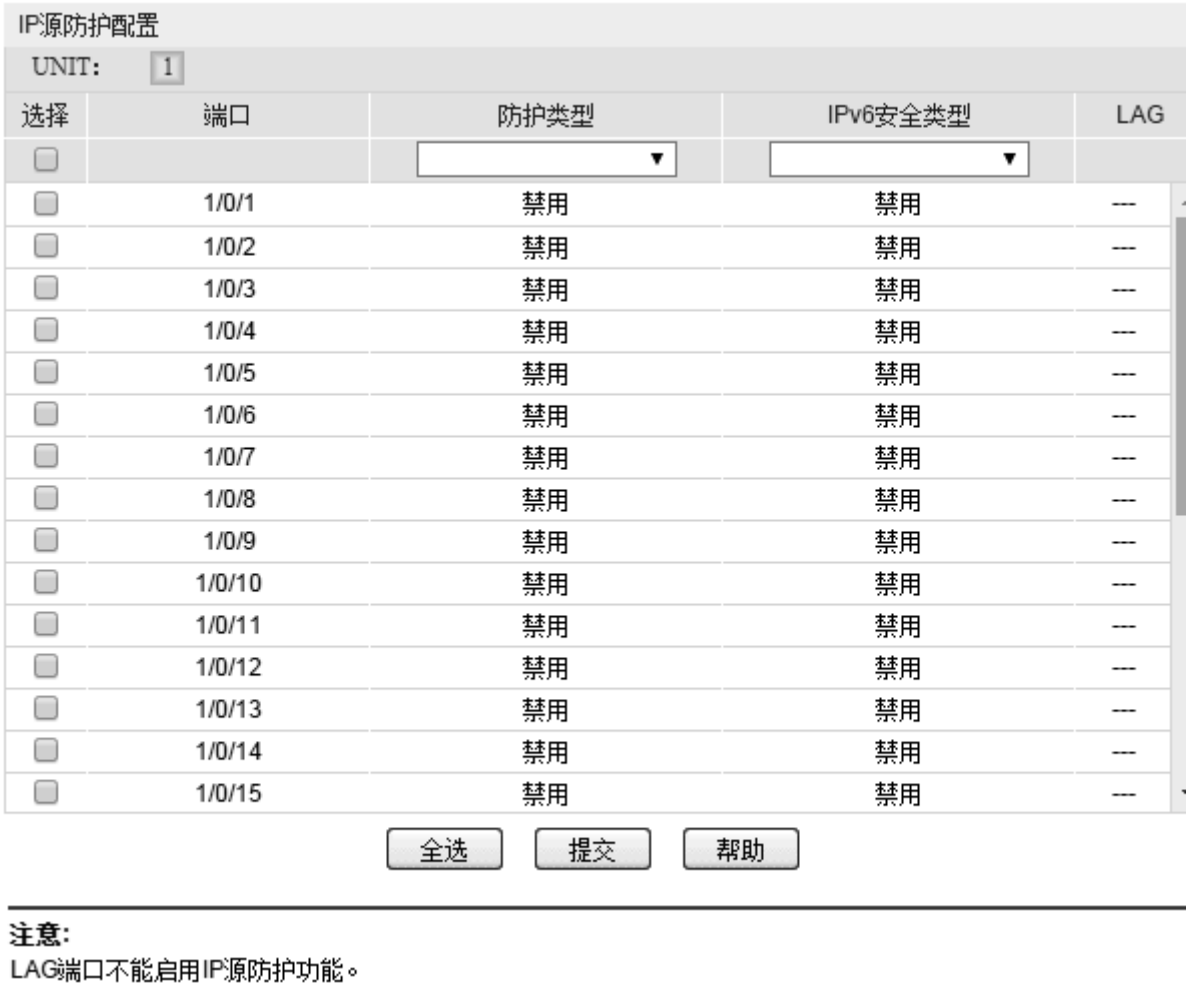


图 14-9 IP 源防护

以下的条目显示在屏幕上:

- **ip 源保护配置**

选择： 勾选端口配置 IP 源防护功能，可多选。

端口： 显示交换机的端口号。

防护类型： 选择端口的安全类型。

禁用：禁用端口的 IP 源防护功能。

SIP+MAC：数据包的 IP、源 MAC 地址、端口号只有匹配四元绑定列表才可以被处理。

IPv6 安全类型： 选择端口的安全类型。

禁用：禁用端口的 IPv6 源防护功能。

SIPv6+MAC：数据包的 IPv6、源 MAC 地址、端口号只有匹配四元绑定列表才可以被处理。

LAG： 显示端口当前所属的汇聚组。

注意:

配置 IPv6 安全特性之前，您需要配置 SDM 模板为“enterpriseV6”并保存您的配置。有关 SDM 模板配置的更多信息，请参见 SDM 模板。

14.8 DoS 防护

DoS（Denial of Service，拒绝服务）攻击是指攻击者利用网络协议实现的缺陷，耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问甚至崩溃。

DoS 攻击的具体的影响如下：

1) 耗尽服务器的资源，包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。使服务器疲于响应此类报文，导致网络瘫痪。

2) 由于交换机接收到此类报文需经过 CPU 处理，因此若请求报文数量过多，会导致交换机 CPU 利用率持续上升，无法正常工作。

本交换机通过解析 IP 数据包，分析数据包中的特定字段，并判断是否符合 DoS 攻击数据包的特征。对于非法的数据包，交换机将直接丢弃；而对于某些正常的数据包，由于流量过大可能导致受害主机瘫痪时，交换机可以对此类数据包进行限速。本交换机能够防护的 DoS 攻击种类如表 12-1 所示。

DoS 攻击类型	攻击特征
Land Attack	向目标主机发送一个特别伪造的 SYN 包，其 IP 源地址和目的地址都被设置为目标主机的 IP 地址，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度上降低了系统性能。
Scan SYNFIN	TCP 标志位 SYN、FIN 位被置 1 的数据包。由于 SYN 标志用来初始化连接的，FIN 标志用来表示发端已完成发送任务请求关闭连接，所以 SYN/FIN 肯定是非法的数据包，本交换机能够识别此类攻击。
Xmascan	TCP 序号置为 0，FIN、URG、PSH 位置为 1 的数据包。
NULL Scan	TCP 序号置为 0，所有控制位置为 0 的数据包。在正常的 TCP 连接以及数据传输过程中，不会出现所有控制位置 0 的情况，此类数据包为非法的数据包。
SYN sPort less 1024	TCP SYN 标志位置 1，源端口小于 1024 的数据包。
Blat Attack	数据包的 L4 源端口等于目的端口且 URG 置位。此攻击方式类似于 Land Attack，被攻击主机因尝试和自己建立连接使系统性能下降。
Ping Flooding	利用 Ping 广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。

SYN/SYN-ACK Flooding	每当我们进行一次标准的 TCP 连接，都会有一个三次握手的过程，而 TCP-SYN Flood 只进行前两个步骤，服务方在一定时间内等待请求方 ASK 消息。由于一台服务器可用的 TCP 连接是有限的，如果攻击方发送大量此类连接请求，则服务方 TCP 连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常的网络服务，从而造成拒绝服务。

表 12-1 本交换机支持的 DoS 防护种类

在此页面中可以根据实际需要启用合适的 DoS 防护策略。

进入页面的方法：网络安全>>DoS 防护>>DoS 防护

图 12-16 DoS 防护

条目介绍：

- **全局配置**

  DoS 攻击防护： 选择是否启用交换机的 DoS 防护功能。

- **攻击防护列表**

  选择： 勾选启用相应 DoS 防护。

  防护类型： 显示防护类型。

14.9 802.1X 认证

802.1X 协议是 IEEE802 LAN/WAN 委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

本交换机可以作为一个认证系统来对网络中的计算机进行认证。连接在端口上的用户设备如果能通过交换机认证，就可以访问局域网中的资源；如果不能通过交换机认证，则无法访问局域网中的资源。

- **802.1X 体系结构**

802.1X 的系统是采用典型的 Client/Server 体系结构，包括三个实体，如图 12-17 所示。

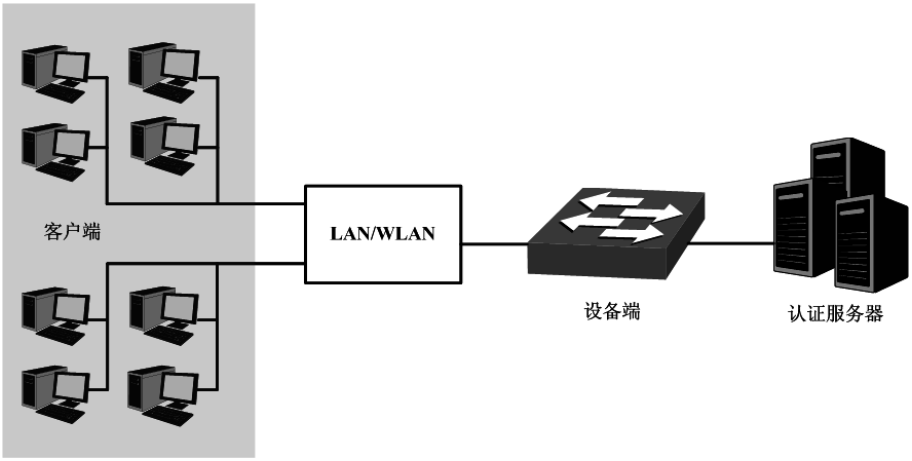


图 12-17 802.1X 认证的体系结构

1) 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起 802.1X 认证，并由设备端对其进行认证。客户端软件必须为支持 802.1X 认证的用户终端设备。

2) 设备端：通常为支持 802.1X 协议的网络设备，如本交换机，为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。

3) 认证服务器：为设备端提供认证服务的实体，例如可以使用 RADIUS 服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

- **802.1X 认证工作机制**

IEEE 802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。

1) 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

2) 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是设备端终结 EAP 协议报文，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证。

3) 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

- **802.1X 认证过程**

认证过程可以由客户端主动发起，也可以由设备端发起。一方面当设备端探测到有未经过认证的用户使用网络时，就会主动向客户端发送 EAP-Request/Identity 报文，发起认证；另一方面客户端可以通过客户端软件向设备端发送 EAPOL-Start 报文，发起认证。

802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP 中继方式

EAP 中继方式是 IEEE 802.1X 标准规定的，将 EAP（扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。本交换机支持的 EAP 中继方式是 EAP-MD5，EAP-MD5 认证过程如图 12-18 所示。

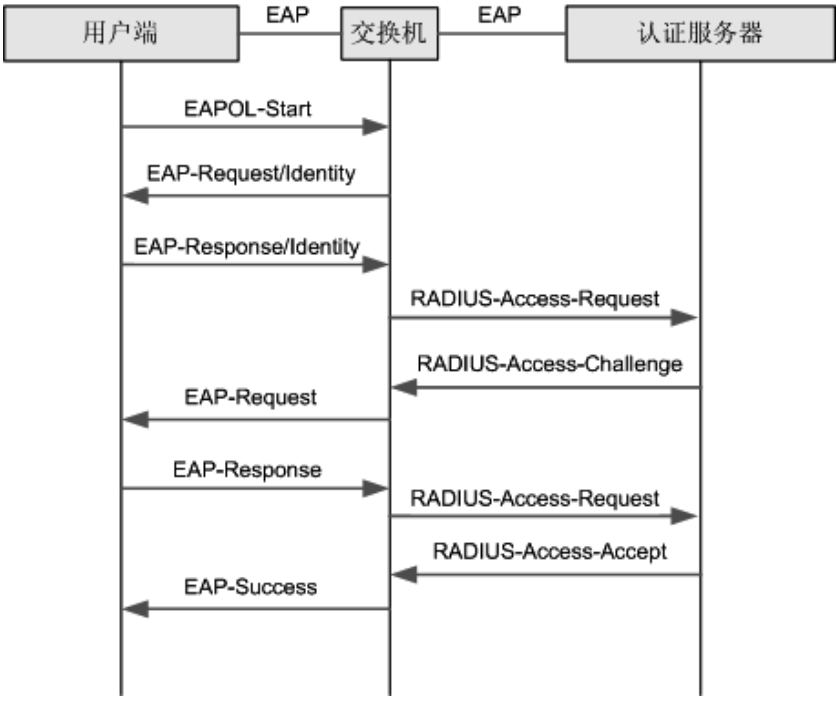


图 12-18 EAP-MD5 认证过程

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。

3) 客户端程序响应设备端发出的请求， 将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。

5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理(此种加密算法通常是不可逆的,生成 EAP-Response/MD5 Challenge 报文)，并通过设备端传给认证服务器。

6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线，设备端把端口状态从授权状态改变成未授权状态。

2. EAP 终结方式

EAP 终结方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。设备端与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。本交换机支持的 EAP 终结方式是 PAP，PAP 认证过程如图 12-19 所示。

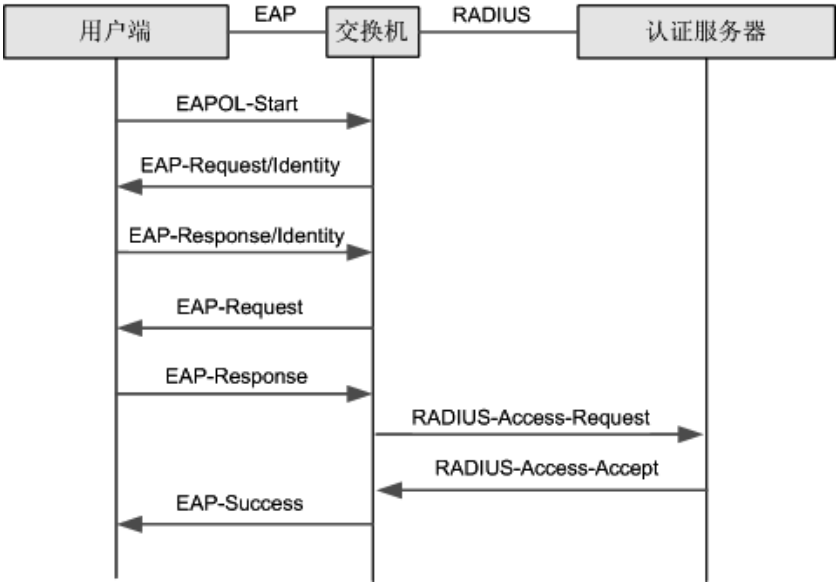


图 12-19 PAP 认证过程

在 PAP 模式中，交换机对用户口令信息进行加密，然后把用户名、随机加密字和客户端加密后的口令信息一起转发给认证服务器进行相关的认证处理；而在 EAP-MD5 模式中，随机加密字由认证服务器产生，交换机只负责把认证信息报文封装后转发。

- **802.1X 定时器**

802.1X 认证过程中会启动多个定时器以控制接入用户、设备以及 RADIUS 服务器之间进行合理、有序的交互。本交换机中的 802.1X 定时器主要有以下三种：

1) **客户端认证超时定时器**：当交换机向客户端发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到客户端的响应，交换机将重发该报文。

2) **认证服务器超时定时器**：当交换机向认证服务器发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到认证服务器的响应，交换机将重发认证请求报文。

3) **静默定时器**：对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设置），在静默期间，交换机不再处理该用户的认证请求。

- **Guest VLAN**

Guest VLAN 功能用来允许未通过认证的用户访问某些特定资源。

用户认证端口在通过 802.1X 认证之前属于一个缺省 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，但此时不能够访问其它网络资源；认证成功后，端口离开 Guest VLAN，用户可以访问其它的网络资源。

用户可以在 Guest VLAN 中获取 802.1X 客户端软件、升级客户端或执行其它一些用户升级程序。如果因为没有专用的认证客户端或者客户端版本过低等原因，导致一定的时间内端口上无客户端认证成功，本交换机会把该端口加入到 Guest VLAN。

开启 802.1X 特性并正确配置 Guest VLAN 后，当交换机向客户端发送 EAP-Request/Identity 报文而没有收到客户端的回应时，该端口将按照各自的链路类型被加入到 Guest VLAN 内。此时如果 Guest VLAN 中有用户发起认证且认证失败，相应连接端口仍会留在 Guest VLAN 内；如果认证成功，端口离开 Guest VLAN，加入配置的 VLAN 中。用户下线后，端口将返回 Guest VLAN 中。

本交换机 802.1X 认证功能包括**全局配置**和**端口配置**两个配置页面。

14.9.1 全局配置

在全局配置功能页面，可以开启全局 802.1X 认证功能，选择本交换机提供的认证方法，并设置 Guest VLAN 以及各种定时器来协调整个系统的 802.1X 认证过程。

进入页面的方法：网络安全>>802.1X 认证>>全局配置

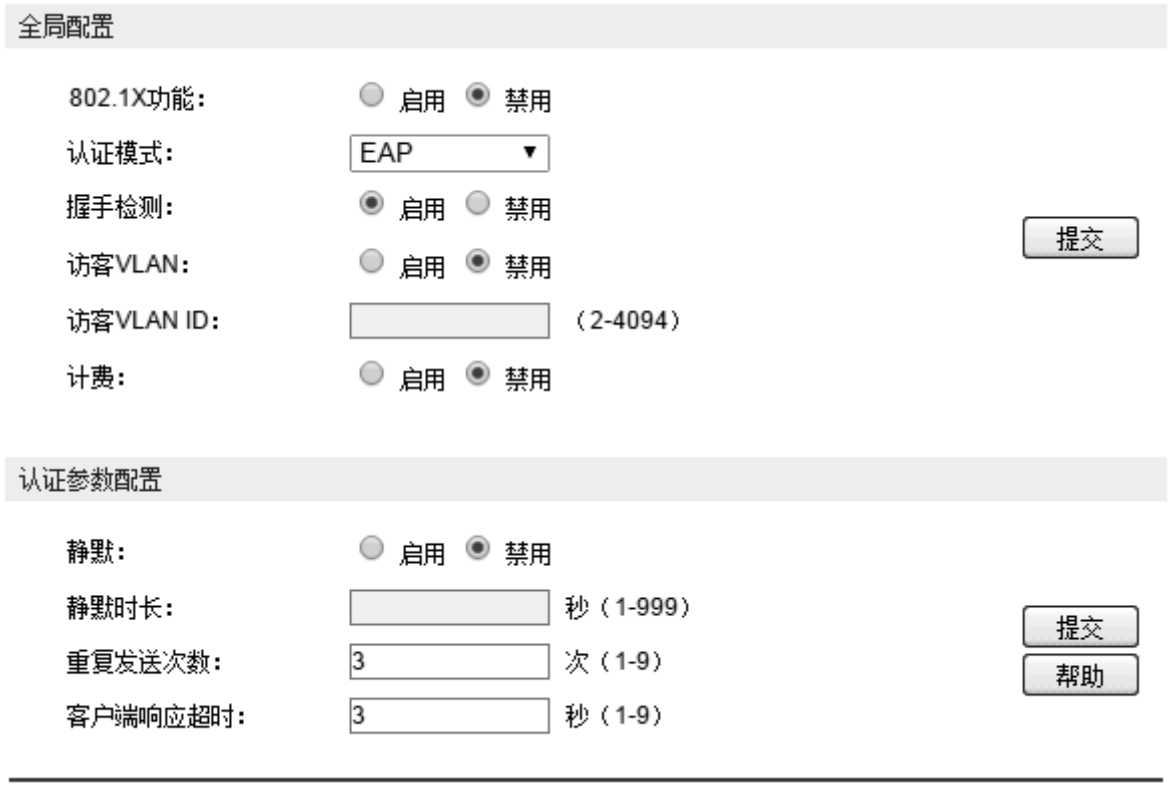


图 12-20 全局配置

条目介绍：

- **全局配置**

802.1X 功能： 选择是否启用 802.1X 认证功能。

认证模式： 选择 802.1X 认证模式。

- EAP-MD5：交换机与认证服务器之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其它高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器。
- PAP：用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。

握手检测： 设置是否启用握手检测。

访客 VLAN： 选择是否启用 Guest VLAN 功能。

访客 VLAN ID： 填写启用 Guest VLAN 的 VLAN ID。Guest VLAN 中的用户可以访问指定的网络资源。

计费： 设置是否计费。

- **认证参数配置**

静默： 选择是否启用静默计时器。

静默时长： 填写静默时长。用户认证失败后，在静默时间内不再处理同一用户的 802.1X 认证请求。

重复发送次数： 填写认证报文的最大重传次数。

客户端响应超时： 填写交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。

14.9.2 端口配置

在端口配置功能页面，可以根据实际的网络情况设置端口的 802.1X 功能特性。

进入页面的方法：网络安全>>802.1X 认证>>端口配置

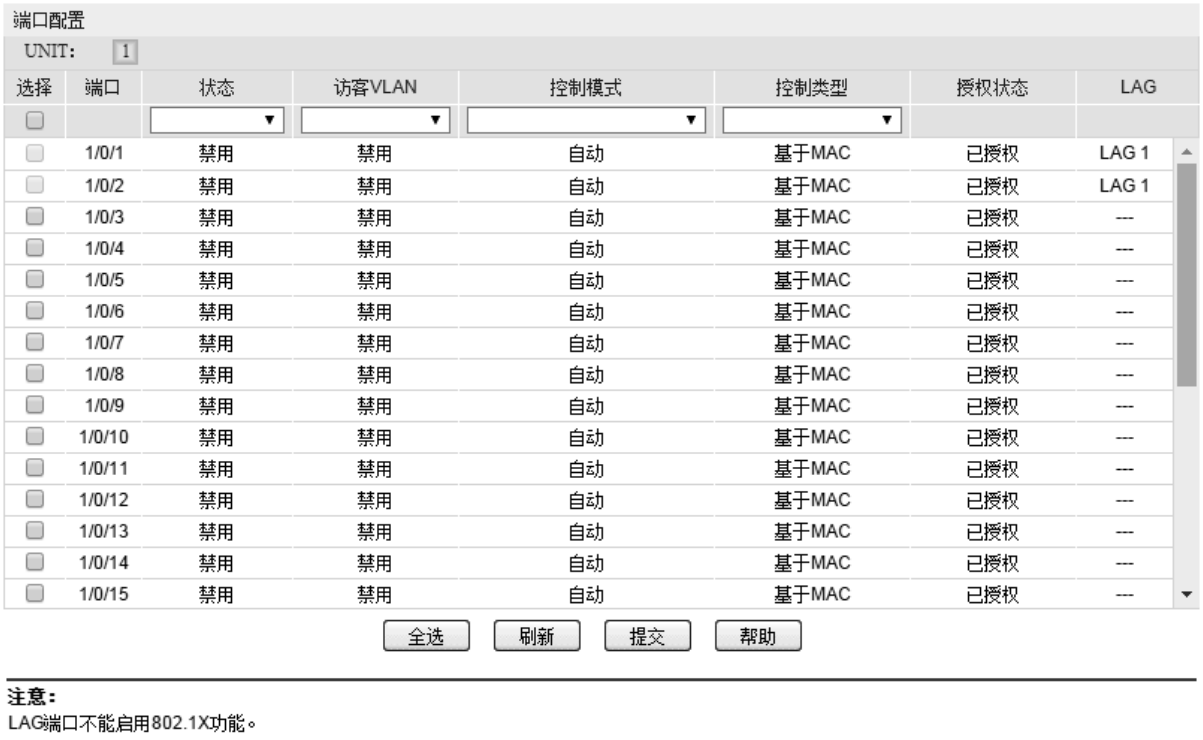


图 12-21 端口配置

条目介绍：

- **端口配置**

选择： 勾选端口，配置端口的 802.1X 认证状态，可多选。

端口： 显示交换机端口号。

状态： 选择该端口是否启用 802.1X 认证。

访客 VLAN： 选择该端口是否启用 Guest VLAN。

控制模式： 选择该端口的控制模式。

- 自动：端口需要进行认证。
- 强制已认证：端口不需要认证即可访问网络。
- 强制不认证：端口永远无法通过认证。

控制类型： 选择该端口的控制类型。

- 基于 MAC：该端口连接的所有计算机都需要认证。
- 基于 Port：该端口连接的某个用户通过认证后，其它用户均无须认证即可访问网络。

授权状态： 显示此端口的授权状态。

LAG： 显示端口当前所属的汇聚组。

14.10 PPPoE

在 **PPPoE ID 插入**页面上，您可以在全局启用 PPPoE ID 插入功能。每个端口的 PPPoE ID 插入特性和类型都可以单独配置。

进入页面的方法：网络安全→PPPoE 配置→ PPPoE ID 插入

图 14-10 PPPoE ID 插入配置

以下的条目显示在屏幕上:

- **全局配置**

PPPoE ID 插入： 全局启用/禁用 PPPoE 电路 ID 插入功能。

- **端口配置**

选择： 勾选需要配置的端口，可多选。

端口： 显示交换机的端口号。

电路 ID：	启用/禁用 PPPoE 电路 ID 插入特性。
电路 ID 类型：	指定端口的电路 ID 类型。
UDF 值：	如果电路 ID 类型选择 UDF，用户可以指定最大长度为 40 个字符的字符串，用于编码电路 ID 选项。
远程 ID：	启用或禁用 PPPoE 远程 ID 插入特性。
远程 ID 值：	用户可以指定最大长度为 40 个字符的字符串，用于编码远程 ID 选项。

14.11 AAA

- **AAA 简介**

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，提供了认证、授权、计费三种安全功能。这三种安全功能的具体作用如下：

认证：验证用户是否可以获得网络访问权。

授权：授权用户可以使用哪些服务。

计费：记录用户使用网络资源的情况

用户可以只使用 AAA 提供的一种或两种安全服务。

用户名和密码成对使用，用于登录和权限验证。认证可以在交换机本地处理，也可以在 RADIUS/TACACS+服务器处理。本地用户名和密码身份验证可以在 4.2 章节中的用户管理中配置。

- **访问应用程序**

本交换机支持通过 Console、Telnet、SSH 和 HTTP 进行身份认证。

- **RADIUS/TACACS+服务器**

用户可以通过 RADIUS/TACACS+服务器对交换机和服务器之间的连接进行配置。

- **服务器组**

用户可以自定义服务器组，服务器组可以包含多个运行同样安全协议的服务器，比如 RADIUS 和 TACACS+。在服务器列表中，用户可以定义服务器的响应顺序。当用户尝试接入交换机时，交换机将会请求服务器组中的第一个服务器进行认证，如果在一定时间内没有收到响应，第二个服务器将进行响应，以此类推。

本交换机有两个内置的认证服务器组，一个是 RADIUS，另一个是 TACACS+。这两个服务器组不能删除，用户自定义的 RADIUS/TACACS+服务器也将自动加入这两个服务器组。

14.11.1 全局配置

在全局配置页面上，您可以全局启用/禁用 AAA 功能。

进入页面的方法：网络安全→AAA→全局配置

图 14-11 全局配置

➢ **配置过程**

AAA： 全局启用/禁用 AAA 功能。

14.11.2 提升特权

在提升特权配置页面上，您可以将当前登录用户从访客升级到管理员，并获得管理员级别的权限。认证密码可以通过 RADIUS/TACACS+服务器、用户自定义服务器组或本地交换机认证。

进入页面的方法：网络安全→AAA→全局配置

图 14-12 提升特权

➢ **配置过程**

启用 Admin： 输入使能密码并单击提交按钮，当前登录的用户从访客升级到管理员。只有管理员用户才能配置以下 AAA 设置。

建议:

如果使能密码本地验证，使能密码需要在命令行手册中预先通过管理员身份设置。更多详细信息请参考 CD 中命令行手册的使能密码章节。

14.11.3 RADIUS 服务器配置

该页面用于配置运行 RADIUS 安全协议的认证服务器。

进入页面的方法：网络安全→AAA→ RADIUS 配置

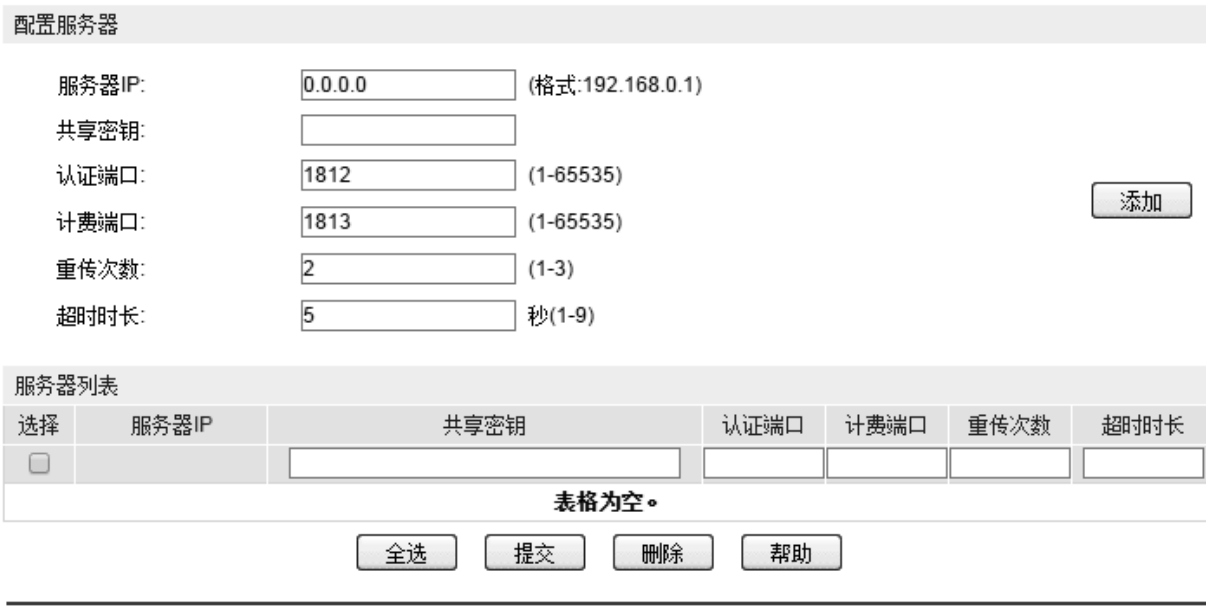


图 14-13 RADIUS 配置

- **配置过程**

在配置服务器页面中配置 RADIUS 服务器的 IP 地址和其他相关参数。

在服务器列表页面中查看、编辑和删除 RADIUS 服务器。

- **配置服务器**

服务器 IP： 输入运行 RADIUS 安全协议的服务器的 IP。

共享密钥： 输入 RADIUS 服务器和交换机之间的共享密钥。RADIUS 服务器和交换机通过密钥字符串来加密密码和交换响应信息。

认证端口： 指定 RADIUS 服务器上用于身份验证请求的 UDP 目的端口。

计费端口： 指定 RADIUS 服务器上用于计数请求的 UDP 目的端口。

重传次数： 指定如果服务器不响应，对服务器的请求次数。

超时时长： 指定在重新发送之前，交换机等待服务器应答的时间间隔。

- **服务器列表**

选择： 选择服务器 IP。支持多选。

服务器 IP： 显示运行 RADIUS 安全协议的服务器的 IP。

共享密钥： 输入 RADIUS 服务器和交换机之间的共享密钥。RADIUS 服务器和交换机通过密钥字符串来加密密码和交换响应信息。

认证端口： 指定 RADIUS 服务器上用于身份验证请求的 UDP 目的端口。

计费端口： 指定 RADIUS 服务器上用于计数请求的 UDP 目的端口。

重传次数： 指定如果服务器不响应，对服务器的请求次数。

超时时长： 指定在重新发送之前，交换机等待服务器应答的时间间隔。

14.11.4 TACACS+服务器配置

该页面用于配置运行 TACACS+安全协议的认证服务器。

进入页面的方法：网络安全→AAA→TACACS + 配置

图 14-14 TACACS+ 服务器配置

- **配置过程**

在配置服务器页面中配置 TACACS+服务器的 IP 地址和其他相关参数。

在服务器列表页面中查看、编辑和删除 TACACS+服务器。

- **配置服务器**

服务器 IP： 输入运行 TACACS +安全协议的服务器 IP。

超时时长： 指定在重新发送之前，交换机等待服务器应答的时间间隔。

共享密钥： 输入 TACACS +服务器和交换机之间的共享密钥。TACACS+服务器和交换机通过密钥字符串来加密密码和交换响应信息。

端口： 指定 TACACS +服务器的 TCP 端口。

- **服务器列表**

选择： 选择服务器 IP。支持多选。

服务器 IP： 输入运行 TACACS +安全协议的服务器 IP。

超时时长： 指定在重新发送之前，交换机等待服务器应答的时间间隔。

共享密钥： 输入 TACACS +服务器和交换机之间的共享密钥。TACACS+服务器和交换机通过密钥字符串来加密密码和交换响应信息。

端口： 指定 TACACS +服务器的 TCP 端口。

14.11.5 认证服务器组配置

在认证服务器组页面上，用户可以对运行相同安全协议的认证服务器进行分组。交换机有两个内置的认证服务器组，一个是 RADIUS，另一个是 TACACS+。这两个服务器组不能编辑或删除。一个组中的服务器按顺序进行响应。

进入页面的方法：网络安全→AAA→服务器组

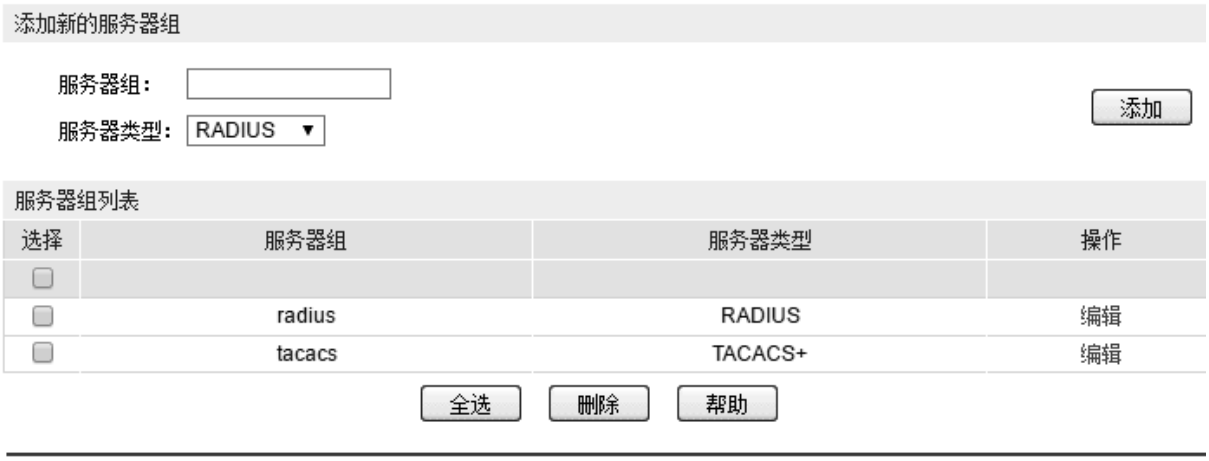


图 14-15 新建服务器组

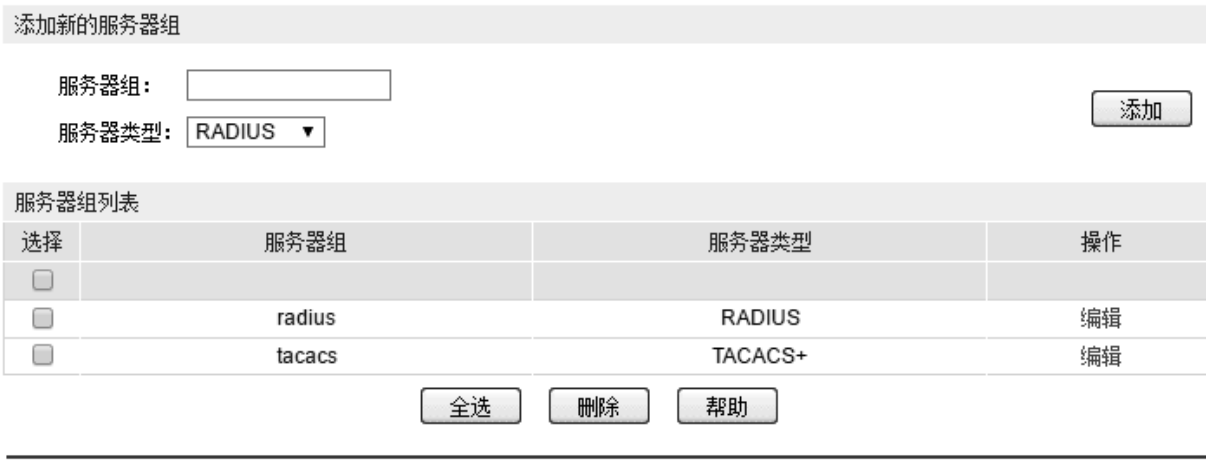


图 14-16 添加服务器到服务器组

- **配置过程**

1) 配置服务器组名称和服务器类型，创建一个服务器组。

2) 点击服务器组列表中的编辑，配置相应的服务器组。

3) 选择您以前创建的服务器 IP 并单击添加，添加服务器到服务器组。(图 14-36)

在服务器组列表中查看和删除服务器组。

在服务器 IP 列表中查看和删除服务器。

- **条目描述**

服务器组： 定义服务器组名称。

服务器类型： 指定服务器类型为 RADIUS 或 TACACS +。

服务器 IP： 选择您先前配置的服务器 IP。

注意:

1. 两个内置服务器组 RADIUS 和 TACACS +不能删除或编辑。
2. 一个服务器组中最多可以添加 16 个服务器。

14.11.6 认证方法列表配置

在进行 AAA 认证之前，您需要先定义一个认证方法列表。认证方法列表描述了用户认证的顺序和认证方法。

交换机使用认证方法列表中的第一个方法来认证用户，如果第一个方法没有得到响应，交换机会选择认证下一个认证方法。此过程会一直持续，直到认证成功或者所有认证方法都全部尝试过。如果认证方法全部尝试过后仍然认证失败，意味着安全服务器或者本地交换机拒绝这个用户接入，认证过程将会中止，不会再尝试其他认证方法。

进入页面的方法：网络安全→AAA→方法列表

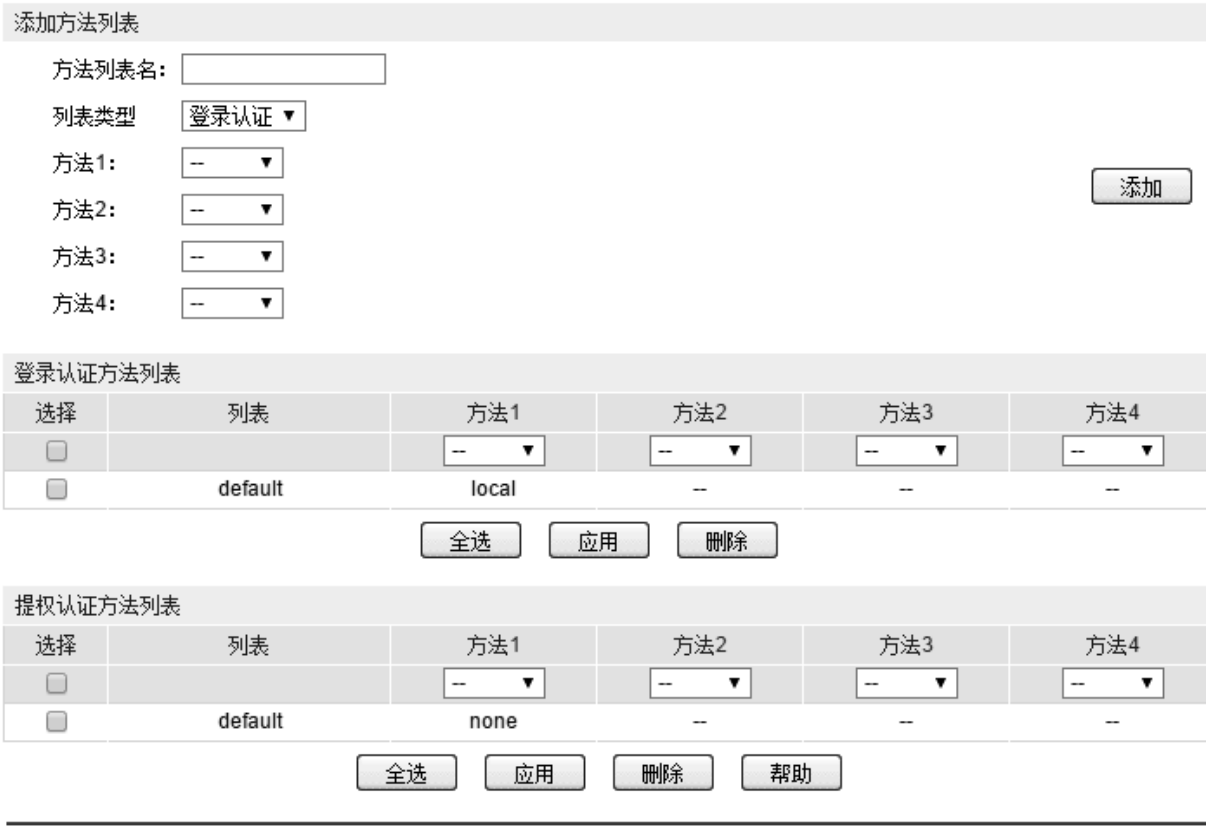


图 14-17 认证方法列表

➢ **配置过程**

1) 输入认证方法列表名称。

2) 指定身份认证类型为登录或启用。

3) 配置认证方法的优先级。这些选项包括 radius、tacacs、本地和用户自定义服务器组。

在身份认证登录方法列表和身份认证启用方法列表中查看和删除配置方法优先级列表。

- **条目描述**

方法列表名：	定义认证方法列表名称。
方法类型：	指定身份认证类型为登录或启用。
方法：	指定身份认证方法。只有当前面的方法没有响应时，才会尝试下一个认证方法。如果失败了，则不会。
Local：	在交换机中使用本地数据库进行身份验证。
None：	不使用身份认证。
Radius：	使用远程 radius 服务器/服务器组进行身份认证。
Tacacs：	使用远程 tacacs +服务器/服务器组进行身份认证。
用户自定义服务器组：	使用用户自定义服务器组进行身份认证。

建议:

如果在远程 RADIUS 服务器上验证了启用密码，则该交换机将以$Enable$为默认用户名发送启用身份验证。

14.11.7 应用身份认证列表配置

用户可以使用以下访问应用程序配置身份认证方法列表: console、telnet、ssh 和 http。

进入页面的方法：网络安全→AAA→全局配置

AAA配置列表

选择	模块	登录列表	提权列表
☐		default ▼	default ▼
☐	console	default	default
☐	telnet	default	default
☐	ssh	default	default
☐	http	default	default

全选 提交 帮助

图 14-18 应用认证配置

- **配置过程**

1) 选择应用程序模块。

2) 从登录列表下拉菜单中配置认证方法列表。该选项为访问交换机的普通用户定义了身份认证方法。

3) 从授权列表下拉菜单中配置认证方法列表。这个选项为需要管理员权限的用户定义了身份认证方法。

➢ **条目描述**

选择： 勾选需要配置的端口，可多选。

模块： 访问应用程序列表。

登陆列表： 使用之前配置的方法列表配置登录应用程序。

提权列表： 使用之前配置的方法列表配置将访客级别提升到管理员级别的应用程序。

14.11.8 802.1X 认证服务器配置

这个页面是用来配置使用 802.1X 身份认证、计费和 IGMP 认证的 RADIUS 服务器组。

进入页面的方法：网络安全→AAA→Dot1x 列表

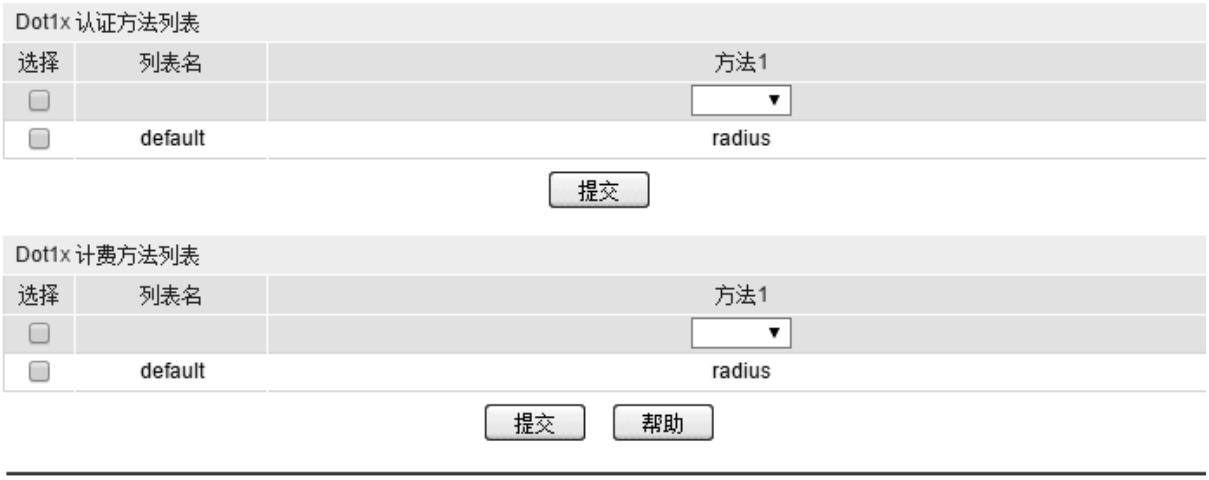


图 14-19 802.1X 配置

➢ **配置过程**

1) 在全局配置和端口配置中配置 802.1X 功能。请参阅 802.1X 获取更多详细信息。

2) 在 Dot1x 认证方法列表中配置 802.1X 身份认证 RADIUS 服务器组。

3) 在 Dot1x 计费方法列表中配置 802.1X 计费 RADIUS 服务器组。

14.11.9 默认设置

缺省情况下禁用 AAA 功能

缺省情况下不配置使能密码。

RADIUS 服务器的认证端口是 1812，计费端口是 1813，重传次数 2 次，超时时长 5 秒。

TACACS+服务器的通信端口是 49，超时时长 5 秒。

所有 RADIUS 服务器都在 RADIUS 服务器组中添加。

所有 TACACS +服务器都在 TACACS+服务器组中添加。

缺省情况下认证登录方法列表包括 local，默认的登录用户名和密码都是 admin。

缺省情况下认证启用方法列表是空的，这意味着用户可以在没有密码的情况下使用管理员特权。

缺省情况下 console / telnet / ssh / http 访问应用程序使用默认登录列表和默认启用列表。

缺省情况下 802.1 X 认证和 802.1X 计费都使用 radius 服务器组。

回目录

第15章 SNMP

- **SNMP 概述**

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前 UDP/IP 网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。SNMP 结构简单，使用方便，并且能够屏蔽不同设备的物理差异，实现对不同设备的自动化管理，所以得到了广泛的支持和应用，目前大多数网络管理系统和平台都是基于 SNMP 的。

SNMP 的最大优势就是设计简单，他既不需要复杂的实现过程，也不会占用太多的网络资源，便于使用。SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP 可实现统计、配置和测试等功能；当网络出故障时，可实现各种错误检测和恢复功能。

- **SNMP 的管理框架**

SNMP 包括三个网络元素：SNMP 管理者（SNMP Manager），SNMP 代理（SNMP Agent），MIB 库（Management Information Base，管理信息库）。

SNMP 管理者：运行在 SNMP 客户端程序的工作站，提供了非常友好的人机交互页面，方便网络管理员完成绝大多数的网络设备管理工作。

SNMP 代理：驻留在被管理设备上的一个进程，负责接受、处理来自 SNMP 管理者的请求报文。在一些紧急情况下，SNMP 代理也会通知 SNMP 管理者事件的变化。

MIB 库：被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 SNMP 代理都有自己的 MIB。SNMP 管理者根据权限可以对 MIB 中的对象进行读/写操作。

SNMP 管理者是 SNMP 网络的管理者，SNMP 代理是 SNMP 网络的被管理者，他们之间通过 SNMP 协议来交互管理信息。SNMP 管理者、SNMP 代理、MIB 库三者的关系如图 13-1 所示。

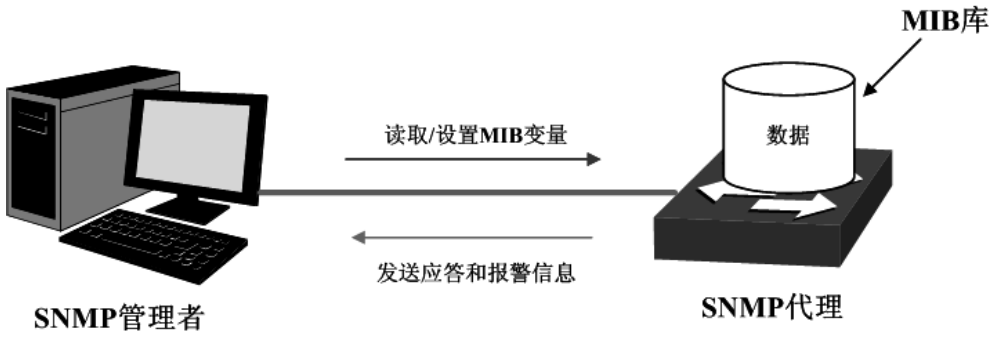


图 13-1 SNMP 网元关系图

- **SNMP 的协议版本**

本交换机提供了 SNMPv3 的管理功能，同时兼容 SNMPv1 和 SNMPv2c，SNMP 管理者和 SNMP 代理的 SNMP 版本需要一致，它们之间才能相互通信，可以根据自己的应用需求，选择不同安全级别的管理模式。

SNMPv1：采用团体名（Community Name）认证。团体名用来定义 SNMP 管理者和 SNMP 代理的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP 管理者对 SNMP 代理的访问。

SNMPv2c：也采用团体名认证。它在兼容 SNMPv1 的同时又扩充了 SNMPv1 的功能。

SNMPv3：SNMPv3 在前两个版本 v1、v2c 的基础上大大加强了安全性和用户可控制性，他采用了 VACM（View-based Access Control Model，基于视图的访问控制模型）及 USM（User-Based Security Model，基于用户的安全模型）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 SNMP 管理者和 SNMP 代理之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP 管理者和 SNMP 代理之间的通信提供更高的安全性。

➢ **MIB 库简介**

MIB 是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，被管理对象可以用一串数字唯一确定，这串数字是被管理对象的 OID（Object Identifier，对象标识符）。MIB 的结构如图 13-2 所示。图中，B 的 OID 为{1.2.1.1}，A 的 OID 为{1.2.1.1.5}。

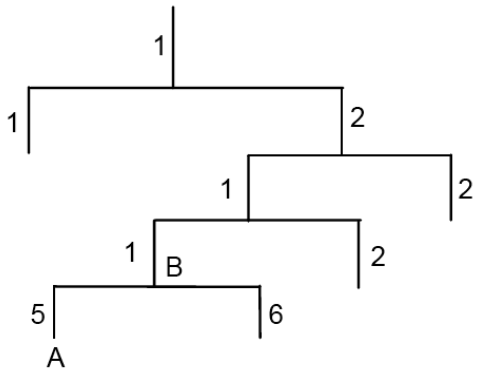


图 13-2 MIB 树结构

➢ **SNMP 配置概要**

- 创建视图

MIB 视图是全部 MIB 管理对象的一个子集。管理对象以 OID（Object Identifier，对象标识符）来表示，通过配置管理对象的视图类型（包括/排除），来达到控制该管理对象能否被管理的目的。各管理对象的 OID 可以在 SNMP 管理软件上找到。

- 创建 SNMP 组

创建完视图之后，需要创建 SNMP 组，只有“组名”、“安全模式”、“安全级别”三项均相同的组，才被认为是同一个组。同时可以为各个 SNMP 组添加只读/只写/通知视图，从而满足了处于不同组内的用户对交换机功能的访问权限不同的需求。

- 创建用户

用户创建于 SNMP 组中，SNMP 管理端使用此处创建的用户及其认证/加密密码来登录 SNMP 代理端。

SNMP 模块主要用于配置交换机的 SNMP 功能，包括 **SNMP 配置**和**通知管理**两个部分。

15.1 SNMP 配置

在本功能处可以配置 SNMP 的各项基本功能，包括**全局配置**、**视图管理**、**组管理**、**用户管理**和**团体管理**五个配置页面。

15.1.1 全局配置

配置交换机的 SNMP 功能，首先需要在本页配置交换机 SNMP 的全局功能。

进入页面的方法：SNMP>>SNMP 配置>>全局配置

图 13-3 全局配置

条目介绍：

- **全局配置**

  SNMP 功能： 选择是否启用交换机的 SNMP 功能。

- **本地引擎配置**

  本地引擎 ID： 填写本地 SNMP 实体的引擎 ID。本地用户建立在本地引擎之下。

- **远程引擎配置**

  远程引擎 ID： 填写 SNMP 管理端的引擎 ID。远程用户建立在远程引擎之下。

注意：

- 引擎 ID 的字符个数必须为偶数。

15.1.2 视图管理

在 SNMP 报文中使用管理变量（OID）来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。本页用来配置 SNMP 的视图。

进入页面的方法：SNMP>>SNMP 配置>>视图管理

图 13-4 视图管理

条目介绍：

- **新建视图**

视图名称： 填写视图条目的名称。一个视图可以有多个同名的视图条目。

MIB 子树 OID： 填写该视图条目的管理变量（OID）。

视图类型： 选择 OID 的类型。

- 包括：该 OID 可以被管理软件管理。
- 排除：该 OID 不能被管理软件管理。

- **视图列表**

选择： 勾选条目进行删除。同一视图下的所有视图条目会被同时选择。

视图名称： 显示视图名称。

视图类型： 显示对应 OID 的类型。

MIB 子树 OID： 显示对应视图下的管理变量（OID）。

15.1.3 组管理

本页用来配置 SNMP 的组，组内的用户通过只读、只写、通知视图来达到访问控制的目的。

进入页面的方法：SNMP>>SNMP 配置>>组管理

图 13-5 组管理

条目介绍：

- **组配置**

组名： 填写组名。与“安全模式”和“安全级别”三项共同组成该组的标识，三项均相同才被认为是同一组。

安全模式： 选择组的安全模式。

- v1：SNMP v1，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v2c：SNMP v2c，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v3：SNMP v3，采用 USM 认证。

安全级别： 选择 SNMP v3 的组的安全级别。

只读视图： 选择只读视图，对所选的视图只能被查看不能被编辑。

只写视图： 选择只写视图，对所选的视图只能被编辑不能被查看。若要进行读写操作，则需要同时在“只读视图”中添加。

通知视图： 选择通知视图，管理软件可以接收到所选视图发送的异常警报信息。

- **组列表**

选择： 勾选条目进行删除，可多选。

组名： 显示 SNMP 组的组名。

安全模式： 显示组的安全模式。

安全级别： 显示组的安全级别。

只读视图： 显示组中具有只读权限的视图名称。

只写视图： 显示组中具有只写权限的视图名称。

通知视图： 显示组中具有通知权限的视图名称。

操作： 点击对应条目的<编辑>按键，可以修改该条目的视图。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 一个组必须具备一个只读视图，默认只读视图为 viewDefault。

15.1.4 用户管理

SNMP 管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。本页用来配置 SNMP 的用户。

进入页面的方法：SNMP>>SNMP 配置>>用户管理

图 13-6 用户管理

条目介绍：

- **用户配置**

用户名： 填写用户名。

用户类型： 选择用户类型。

- 本地用户：建立在本地引擎下的用户。
- 远程用户：建立在远程引擎下的用户。

组名： 选择组名。通过“组名”、“安全模式”、“安全级别”来确定用户所属的组。

安全模式： 选择安全模式。

安全级别： 选择安全级别。

认证模式： 选择 SNMP v3 用户的认证模式。

- 无：不认证。
- MD5：信息摘要算法。
- SHA：安全散列算法，比 MD5 的安全性更高。

认证密码： 输入认证密码。

加密模式： 选择 SNMP v3 用户的加密模式。

- 无：不加密。
- DES：数据加密标准。

加密密码： 输入加密密码。

➢ **用户列表**

选择： 勾选条目进行删除，可多选。

用户名： 显示用户名。

用户类型： 显示用户类型。

组名： 显示组名。

安全模式： 显示安全模式。

安全级别： 显示安全级别。

认证模式： 显示认证模式。

加密模式： 显示加密模式。

操作： 点击对应条目的<编辑>按键，可以修改该用户所属的组。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

15.1.5 团体管理

SNMP v1 和 SNMP v2c 采用团体名（Community Name）认证，团体名起到了类似于密码的作用。若使用的是 SNMP v1 和 SNMP v2c，配置完视图之后，可以直接在本页配置 SNMP 的团体。

进入页面的方法：SNMP>>SNMP 配置>>团体管理

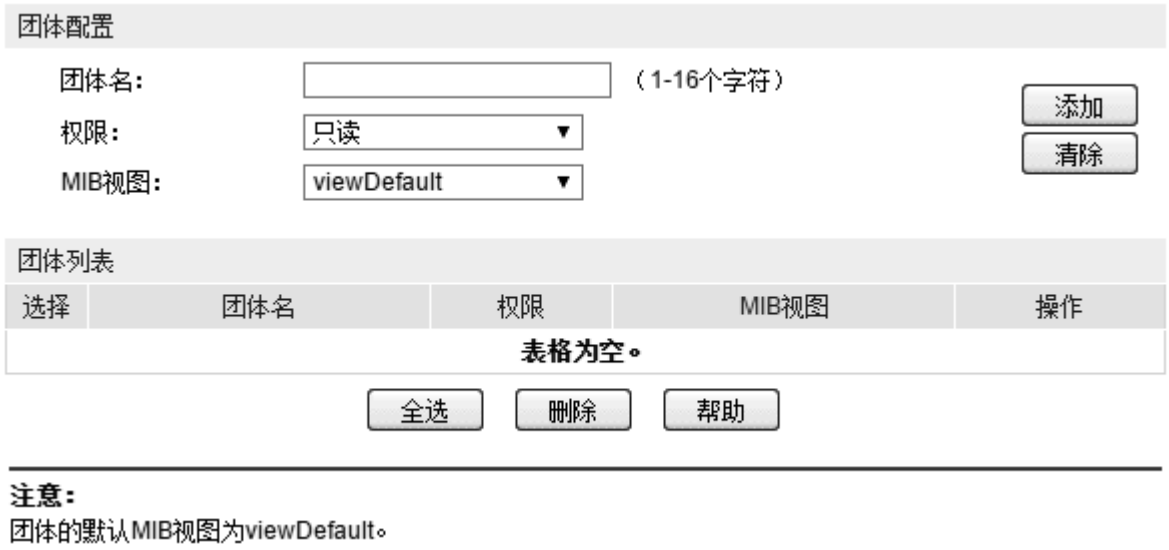


图 13-7 团体管理

条目介绍：

- **团体配置**

团体名： 填写团体名。

权限： 选择该团体对视图的访问权限。

- 只读：团体对相应视图具有只读权限。
- 读写：团体对相应视图具有读写权限。

MIB 视图： 选择团体可访问的视图。

- **团体列表**

选择： 勾选条目进行删除，可多选。

团体名： 显示团体名。

权限： 显示团体对视图的访问权限。

MIB 视图： 显示团体可访问的视图。

操作： 点击对应条目的<编辑>按键，可以修改该团体的访问视图及访问权限。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 团体的默认 MIB 视图为 viewDefault。

SNMP 功能配置步骤：

- 若使用 SNMPv3 版本

步骤	操作	说明

步骤	操作	说明
1	启用 SNMP 全局功能	必选操作。在 **SNMP>>SNMP 配置>>全局配置**页面，启用交换机的 SNMP 功能。
2	创建视图	可选操作。在 **SNMP>>SNMP 配置>>视图管理**页面，创建管理对象的视图。默认视图名为 viewDefault，OID 为 1。
3	创建 SNMP 组	必选操作。在 **SNMP>>SNMP 配置>>组管理**页面，创建 SNMPv3 类型的组，并为组添加不同访问权限的视图。
4	创建 SNMP 组内的用户	必选操作。在 **SNMP>>SNMP 配置>>用户管理**页面，创建 SNMPv3 组内的用户，并配置用户的认证/加密模式及密码。

- 若使用 SNMPv1 版本或 SNMPv2c 版本

<table>
<tr><th>步骤</th><th colspan="3">操作</th><th>说明</th></tr>
<tr><td>1</td><td colspan="3">启用 SNMP 全局功能。</td><td>必选操作。在 SNMP>>SNMP 配置>>全局配置页面，启用交换机的 SNMP 功能。</td></tr>
<tr><td>2</td><td colspan="3">创建视图</td><td>可选操作。在 SNMP>>SNMP 配置>>视图管理页面，创建管理对象的视图。默认视图名为 viewDefault，OID 为 1。</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">配置访问权限</td><td>直接设置</td><td>创建团体</td><td rowspan="3">二者必选其一。
• 直接设置是在 SNMP>>SNMP 配置>>团体管理页面，以 SNMPv1 和 v2c 版本的团体名进行设置。
• 间接设置采用与 SNMPv3 版本一致的命令形式，添加用户到 v1/v2c 类型的组，即相当于 SNMPv1 和 SNMPv2c 版本的团体名。在 SNMP 管理软件上用来登录交换机的团体名需要跟这里配置的用户名一致，该组下创建的 v1/v2c 用户（团体）的读、写视图与该组的读写视图对应。</td></tr>
<tr><td rowspan="2">间接设置</td><td>创建 SNMP 组</td></tr>
<tr><td>创建 SNMP 组内的用户</td></tr>
</table>

15.2 通知管理

通知管理功能是交换机主动向管理软件报告某些视图的重要事件（如设备重启等），便于管理员通过管理软件对交换机一些特定事件进行及时监控和处理。

通知报文分为以下两种：

Trap：发送 Trap 报文通知 SNMP 管理者。

Inform：发送 Inform 报文通知 SNMP 管理者，并且要求 SNMP 管理者返回信息。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重复发送该 Inform 报文。Inform 具有更高的可靠性，仅在 SNMP v2c 和 SNMP v3 可以使用。

本页用来配置 SNMP 的通知管理功能。

进入页面的方法：SNMP>>通知管理>>通知管理

图 13-8 通知管理

条目介绍：

- **新建条目**

目的 IP 地址： 填写管理主机的 IP 地址。

UDP 端口： 填写管理主机上启用供通知过程使用的 UDP 端口，与 IP 地址共同作用。默认为 162。

团体名/用户名： 配置管理软件的团体名/用户名。

安全模式： 选择用户的安全模式。

安全级别： 配置 SNMP v3 的用户的安全级别。

通知类型： 选择使用的通知报文的类型。

- Trap：以 Trap 方式发送通知。
- Inform：以 Inform 方式发送通知，Inform 具有更高的可靠性。

重传： 填写 Inform 报文的重传次数。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重复发送 Inform 报文。默认为 3。

超时： 填写交换机等待 Inform 回应报文的时间。超过该时间后，将重新发送 Inform 报文。默认为 100 秒。

- **目的主机列表**

选择： 勾选条目进行删除，可多选。

目的 IP 地址： 显示管理主机的 IP 地址。

UDP 端口： 显示管理主机上启用供通知过程使用的 UDP 端口。

团体名/用户名： 显示管理软件的团体名/用户名。

安全模式： 显示用户的安全模式。

安全级别： 显示 SNMP v3 的用户的安全级别。

通知类型： 显示使用的通知报文的类型。

超时： 显示 Inform 报文的重传次数。

重传： 显示收到 Inform 报文回应报文的超时时间。

操作： 点击对应条目的<编辑>按键，可以修改该通知条目的参数。修改完毕后点击<修改>按键，修改内容生效。

15.3 RMON

RMON（Remote Monitoring，远程网络监视）完全基于 SNMP 体系结构，是 IETF（Internet Engineering Task Force，因特网工程任务组）提出的标准监控规范，他使 SNMP 更为有效、更为积极主动地监控远程设备。利用 RMON 功能，网管可以快速跟踪网络、网段或设备出现的故障，积极采取防范措施，防止网络资源的失效。同时 RMON MIB 也可以记录网络性能和故障的数据，可以在任何时候访问历史数据从而进行有效的故障诊断。RMON 减少了 SNMP 管理者同代理间的通信流量，使得网管可以简单而有效地管理大型网络。

- **RMON 的工作原理**

RMON 代理在 RMON MIB 中存储网络信息，交换机置入 RMON 代理后，具有了 RMON 探测的功能。管理者使用 SNMP 的基本命令与 RMON 代理交互数据信息，收集网络管理信息。但是由于设备资源的限制，管理者无法获取 RMON MIB 的全部数据，一般只可以收集到四个组的信息，这四个组是：历史组、事件组、统计组和警报组。

- **RMON 组**

本交换机支持 RMON 规范（RFC1757）中定义的历史组、事件组、统计组和警报组。

RMON 组	功能	元素
历史组	周期性地收集网络统计信息，存储起来以便日后提取，从而有效的监测网络。	采样端口、采用间隔、创建者。
事件组	定义事件序号及事件的处理方式。此处定义的事件主要用在警报组中警报触发产生的事件。	事件描述、事件类型、创建者、用户名。
统计组	监测报警变量在指定端口的统计值。	丢弃数据包、丢弃字节、数据包发送、广播数据包、组播数据包、CRC 错误帧、过小（或超大）的数据报文、冲突帧以及以下长度的数据包：64、65~127、128~255、256~511、512~1023 和 1024~10240 字节。
警报组	定期对指定的警报变量进行监测，一旦计数器超过阈值则触发警报。	警报变量、样例类型、时间间隔、阈值上限、阈值下限、警报触发方式。

在本功能处可以配置 RMON 的各个组，包括**历史采样**、**事件配置**和**警报管理**三个配置页面。

15.3.1 统计

在这个页面上，您可以配置和查看统计条目。

进入页面的方法：SNMP→RMON→统计组

图 15-9 报文统计

以下的条目显示在屏幕上:

- **统计信息配置**

ID 号： 输入统计条目的 ID 号，从 1 到 65535。

端口： 输入或选择用于收集统计信息的以太网接口。

所有者： 输入所有者名称。

状态： 选择统计条目的状态。
•有效：条目存在且是有效的。
•存在：条目存在，但不是有效的。

- **统计表**

选择： 选择想要删除的相应统计条目。它是多选的。

ID 号： 显示统计条目的 ID 号。

端口： 显示用于收集统计信息的以太网接口。

创建者： 显示所有者名称。

状态： 显示统计条目的状态。

15.3.2 历史组

本页用来配置 RMON 的历史组。

进入页面的方法：SNMP>>RMON>>历史采样


历史采样控制

选择	序号	采样端口	采样间隔（秒）	最大采样数目	创建者	状态
	1	1/0/1	1800	50	monitor	禁用
	2	1/0/1	1800	50	monitor	禁用
	3	1/0/1	1800	50	monitor	禁用
	4	1/0/1	1800	50	monitor	禁用
	5	1/0/1	1800	50	monitor	禁用
	6	1/0/1	1800	50	monitor	禁用
	7	1/0/1	1800	50	monitor	禁用
	8	1/0/1	1800	50	monitor	禁用
	9	1/0/1	1800	50	monitor	禁用
	10	1/0/1	1800	50	monitor	禁用
	11	1/0/1	1800	50	monitor	禁用
	12	1/0/1	1800	50	monitor	禁用

全选 提交 帮助

图 13-9 历史采样

条目介绍：

- **历史采样控制**

选择： 勾选条目配置采样属性。

序号： 显示采样条目的序号。

采样端口： 选择进行采样的端口。

采样间隔（秒）： 填写端口采样的时间间隔。默认为 1800 秒。

创建者： 填写创建该采样条目的实体。

状态： 选择是否启用所选采样条目。

15.3.3 事件配置

本页用来配置 RMON 的事件组。

进入页面的方法：SNMP>>RMON>>事件组


事件配置

选择	序号	用户名	描述	类型	创建者	状态
	1	public		无	monitor	禁用
	2	public		无	monitor	禁用
	3	public		无	monitor	禁用
	4	public		无	monitor	禁用
	5	public		无	monitor	禁用
	6	public		无	monitor	禁用
	7	public		无	monitor	禁用
	8	public		无	monitor	禁用
	9	public		无	monitor	禁用
	10	public		无	monitor	禁用
	11	public		无	monitor	禁用
	12	public		无	monitor	禁用

全选 提交 帮助

图 13-10 事件配置

条目介绍：

- **事件配置**

选择： 勾选条目配置事件属性。

序号： 显示事件条目的序号。

用户名： 填写事件所属的用户。当对应事件需要发送通知时，将会根据此用户名进行发送。

描述： 填写该事件的描述信息。

类型： 选择事件的类型。

- 无：不做任何操作。
- 日志：将事件记录在交换机中，通过 SNMP 管理软件读取。
- 通知：向管理主机发送报警消息。
- 日志&通知：将事件记录在交换机中并向管理主机发送报警消息。

创建者： 填写创建该事件条目的实体。

状态： 选择是否启用所选事件条目。

15.3.4 警报组

本页用来配置 RMON 的统计组和警报组。

进入页面的方法：SNMP>>RMON>>警报管理

警报配置

选择	序号	计数器	统计条目	样例类型	上升阈值	上升事件	下降阈值	下降事件	启动警报	时间间隔（秒）	创建者	状态
	1	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	2	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	3	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	4	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	5	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	6	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	7	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	8	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	9	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	10	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	11	RecBytes		绝对值	100		100		全部	1800	monitor	禁用
	12	RecBytes		绝对值	100		100		全部	1800	monitor	禁用

全选 提交 帮助

图 13-11 警报配置

条目介绍：

- **事件配置**

选择： 勾选条目配置警报属性。

序号： 显示警报条目的序号。

计数器： 选择警报变量。

端口： 选择进行警报监视的端口号。

样例类型： 为警报变量选择取样的方法，再将取样的值与阈值进行比较。

- 绝对值:在一个取样周期结束时将取样结果直接与阈值进行比较。
- 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。

上升阈值： 填写触发警报的上升阈值。默认为 100。

上升事件： 选择触发上升阈值警报的事件的序号。

下降阈值： 填写触发警报的下降阈值。默认为 100。

下降事件： 选择触发下降阈值警报的事件的序号。

启动警报： 选择警报触发的方式。

- 上升：只在触发上升阈值后触发警报。
- 下降：只在触发下降阈值后触发警报。
- 全部：触发上升和下降阈值均触发警报。

时间间隔（秒）： 填写警报的时间间隔。默认为 1800 秒。

创建者： 填写创建该警报条目的实体。

状态： 选择是否启用所选警报条目。

注意：

- 当警报变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生警报事件。即上升警报和下降警报是交替产生的，出现了一次上升警报，则下一次必为下降警报。

回目录

第16章 LLDP

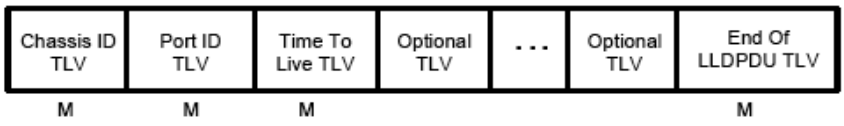
链路层发现协议 LLDP（Link Layer Discovery Protocol）是一个二层协议，在符合 IEEE802 标准的局域网络中，允许网络设备周期性地向邻居设备通告自己的设备信息。LLDP 根据 IEEE802.1AB 标准把设备的标识、性能和配置等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给邻居设备，邻居设备收到这些信息后将其以标准的 MIB（Management Information Base，管理信息库)形式保存起来。网络管理系统可以通过管理协议 SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息，以查询及判断链路的通信状况。

为了描述网络的物理拓扑和拓扑中的相关系统，IETF（Internet Engineering Task Force， 互联网工程任务组）组织提出了标准 MIB，一些公司也提出了私有 MIB。但是，IEEE 802 局域网站点并没有统一的标准来传输 MIB 信息。LLDP 解决了这一问题。LLDP 协议允许不同厂商的网络设备协同工作，运行 LLDP 协议的设备能够自动检测并学习邻居设备的信息。LLDP 还可以使运行不同网络层协议的系统互相学习对方的设备信息。

SNMP 应用可以利用 LLDP 获取的信息，进行网络故障排除，从而提高网络的稳定性，维持正确的网络拓扑。

➢ LLDPDU

每一个 LLDPDU 携带四个必须的 TLV 以及一个或者多个可选的 TLV。如下图所示，Chassis ID TLV，Port ID TLV， TTL TLV 和 End TLV 是每个 LLDPDU 所必须携带的四个 TLV。可选的 TLV 是由网络管理系统决定的，它们提供了关于本地 LLDP 设备的详细信息。



LLDPDU 的最大长度由特定的传输速率和协议所允许的最大报文长度决定。就 IEEE 802.3 MAC 协议来说，LLDPDU 的最大长度是不带 TAG 的基本 MAC 帧的最大长度，即 1500 字节。

➢ LLDP 工作机制

1) LLDP 的工作模式

每个端口都可以分别配置 LLDPDU 的接收和发送功能，这样端口可以配置四种工作模式：

- 发送接收：既发送也接收 LLDPDU。
- 只接收：只对接收到的 LLDPDU 进行处理，而不向外发送 LLDPDU。
- 只发送：只向外发送 LLDPDU，而不对接收到的 LLDPDU 进行处理。
- 禁用：既不向外发送 LLDPDU，也不对接收到的 LLDPDU 进行处理。

2) LLDPDU 的传输机制

- 当端口工作在发送接收模式或者只发送模式时，设备会周期性地向邻居设备发送 LLDPDU 以通告自己的信息。
- 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避

免设备连续地发送 LLDPDU 而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保 LLDPDU 的发送有一个固定的最小时间差。

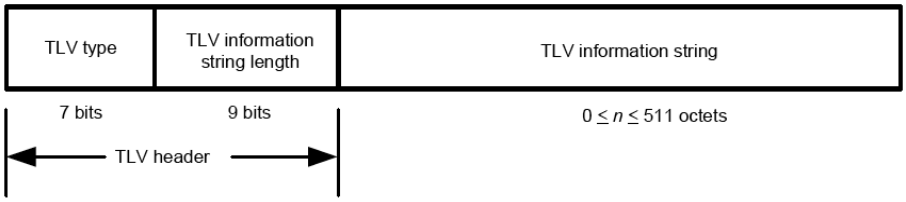
- 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为 1s，快速发出一些 LLDPDU 之后，设备恢复正常的发送周期。

3) LLDPDU 的接收机制

当端口工作在发送接收模式或只接收模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 TTL（Time To Live，生存时间）TLV 中 TTL 的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

➢ TLV

TLV 是 LLDPDU 的基本组成单位，是 Type/Length/Value 的简称，即类型/长度/值。基本 TLV 的格式如下图所示：



每个 TLV 的类型都是不一样的，根据 TLV 的类型可以判断 TLV 中的信息类型。

下表是目前定义的各种 TLV 的详细信息。

TLV 类型	TLV 名称	说明	是否必须携带
0	End of LLDPDU	标识 LLDPDU 结束。任何在 End Of LLDPDU TLV 之后的信息将被丢弃。	是
1	Chassis ID	标识连接设备的 Chassis ID	是
2	端口 ID	标识发送端口的 ID 信息	是
3	Time To Live	本地设备信息在邻居设备上的老化时间	是
4	端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述	否
5	系统名称	用以向邻居发布本地设备的系统名称	否
6	系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述	否
7	系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息	否
8	管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理	否

TLV 类型	TLV 名称	说明	是否必须携带
127	组织定义	允许不同的组织、软件和设备生产商定义向邻居设备发送信息的 TLV	否

TLV 一般分为两类，基本 TLV 和组织定义的 TLV。

1) 基本 TLV

基本 TLV 是实现 LLDP 协议必不可少的，它们包含网络管理的基本信息。

2) 组织定义的 TLV

不同的组织定义了许多不同的 TLV。端口 VLAN ID、协议 VLAN ID、VLAN 名称以及协议标识 TLV 都是 IEEE 802.1 定义的，MAC/PHY 配置/状态、供电能力、链路聚合以及最大帧长度 TLV 则是由 IEEE 802.3 定义的。

注意:

要获取更多关于 TLV 的详细信息，请参考 IEEE 802.1AB 标准。

本交换机中所支持的可携带 TLV 如下表所示：

端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述。
系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息。
系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。
系统名称	用以向邻居发布本地设备的系统名称。
管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。
端口 VLAN ID	用以向邻居发布本端口所处 802.1Q VLAN 的 ID。
协议 VLAN ID	用以向邻居发布本端口所处协议 VLAN 的 ID。
VLAN 名称	用以向邻居发布本端口所处 VLAN 被指派的名称。
链路聚合	用以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口 ID。
MAC/PHY 配置/状态	用以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。
最大帧长度	用以向邻居发布本端口的 MAC 和 PHY 支持的最大帧长度。
供电能力	用以向邻居发布本端口的基本供电信息。

表 14-1 本交换机中所支持的可携带 TLV

LLDP 模块主要用来配置交换机的 LLDP 功能，包括**基本配置**、**设备信息**、**设备统计**和 **LLDP-MED**

四个部分。

16.1 基本配置

本功能包括**基本配置**和**端口配置**两个功能配置页面。

16.1.1 基本配置

配置交换机的 LLDP 功能，首先需要在本页配置交换机 LLDP 的全局功能和相关参数。

进入页面的方法：LLDP>>基本配置>>基本配置

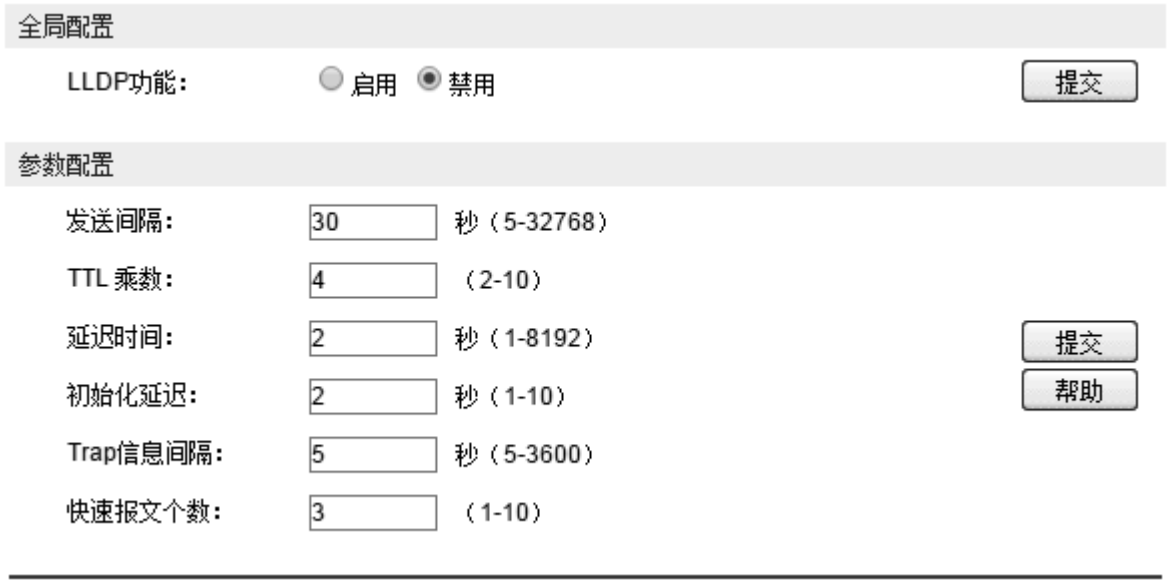


图 14-1 基本配置

条目介绍：

- **全局配置**

  LLDP 功能: 选择是否启用 LLDP。

- **参数配置**

  发送间隔: 配置本地设备向邻居设备发送 LLDPDU 的时间间隔。默认为 30 秒。

  TTL 乘数: TTL 乘数用以控制本地设备发送的 LLDPDU 中 TTL 字段的值，TTL 即为本地信息在邻居设备上的存活时间。TTL=TTL 乘数*发送间隔。默认值为 4。

  延迟时间: 配置本地设备向邻居设备发送 LLDPDU 的延迟时间。当本地配置发生变化时，将延迟指定时间再发送 LLDPDU 通知邻居设备，从而可以避免由于本地配置频繁变化而导致 LLDPDU 的频繁发送。默认值为 2 秒。

  初始化延迟: 当端口 LLDP 工作模式改变时，将延迟一段时间再进行初始化，以避免端口 LLDP 工作模式频繁改变导致端口不断执行初始化。默认值为 3 秒。

Trap 信息间隔: 配置本地设备向网管系统发送 Trap 信息的发送时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。默认值为 5 秒。

快速报文个数: 当端口 LLDP 工作模式从禁用（或只接收）切换为发送接收（或只发送）时，为了让其它设备尽快发现本设备，将启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDPDU 后再恢复为正常的发送周期。默认值为 3 个。

16.1.2 端口配置

在本页可以配置所有端口的 LLDP 参数。

进入页面的方法：**LLDP>>基本配置>>端口配置**

图 14-2 端口配置

条目介绍：

- **全局配置**

选择: 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

端口状态: 选择端口的 LLDP 工作状态：

- 发送接收： 既发送也接收 LLDPDU。
- 只接收：只对接收到的 LLDPDU 进行处理，而不向外发送 LLDPDU。
- 只发送： 只向外发送 LLDPDU，而不对接收到的 LLDPDU 进行处理。
- 禁用： 既不向外发送 LLDPDU，也不对接收到的 LLDPDU 进行处理。

SNMP 通知: 配置本端口是否启用 SNMP 通知。启用此功能时，如果发生 trap 事件，本地设备将会通知 SNMP 服务器。

TLV 字段: 配置发送的 LLDPDU 中包含的 TLV 类型。

16.2 设备信息

本功能包括**本地信息**和**邻居信息**两个配置页面。

16.2.1 本地信息

在本页可以查看各端口的配置参数及系统参数。

进入页面的方法：**LLDP>>设备信息>>本地信息**

图 14-3 本地信息

条目介绍：

- **自动刷新**

  自动刷新: 选择是否启用自动刷新功能。

  刷新周期: 填写自动刷新的时间周期。默认为 30 秒。

- **本地信息**

  端口选择: 点击快速选择相应端口。

16.2.2 邻居信息

在本页可查看邻居设备的信息。

进入页面的方法：**LLDP>>设备信息>>邻居信息**

图 14-4 邻居信息

条目介绍：

- **自动刷新**

  自动刷新: 选择是否启用自动刷新功能。

  刷新速度: 填写自动刷新的时间周期。默认为 5 秒。

- **邻居设备信息**

  端口选择: 点击快速选择相应端口。

16.3 设备统计

在本页可以查看本地设备 LLDP 相关统计信息。

进入页面的方法：**LLDP>>设备统计>>统计信息**

图 14-5 统计信息

条目介绍：

- **自动刷新**

  自动刷新： 选择是否启用自动刷新功能。

  刷新周期： 填写自动刷新的时间周期。默认为 5 秒。

- **全局统计**

  更新时间： 显示此统计数据的更新时间。

  邻居总数： 显示最新更新时本地设备已经创建的邻居数量。

  删除总数： 显示最新更新时本地设备已经删除的邻居数量。

  丢弃总数： 显示最新更新时本地设备已经丢弃的邻居数量。

超时总数： 显示最新更新时本地设备上已经老化的邻居数量。

- **详细统计**

端口： 显示本地端口号。

发送报文： 显示本端口已经发送的 LLDPDU 数量。

接收报文： 显示本端口已经接收到的 LLDPDU 数量。

丢弃报文： 显示本端口丢弃的 LLDPDU 数量。

错误报文： 显示本端口接收的错误 LLDPDU 数量。

超时邻居： 显示本端口连接的邻居设备中老化邻居的数量。

丢弃 TLV： 显示本端口接收 LLDPDU 时，丢弃的 TLV 数量。

未知 TLV： 显示本端口接收的 LLDPDU 中包含的未知 TLV 的数量。

16.4 LLDP-MED

LLDP-MED （Link Layer Discovery Protocol-Media Endpoint Discovery，用于媒体终端发现的链路层发现协议）是 LLDP 协议的一个扩展，它仅适用于 LLDP-MED 规定的网络连接设备和终端设备之间的交互。

LLDP-MED 包括**全局配置**、**端口配置**、**本地信息**和**邻居信息**四个页面。

16.4.1 全局配置

在本页可以配置本地设备的 LLDP-MED 参数。

进入页面的方法：**LLDP>> LLDP-MED >>全局配置**

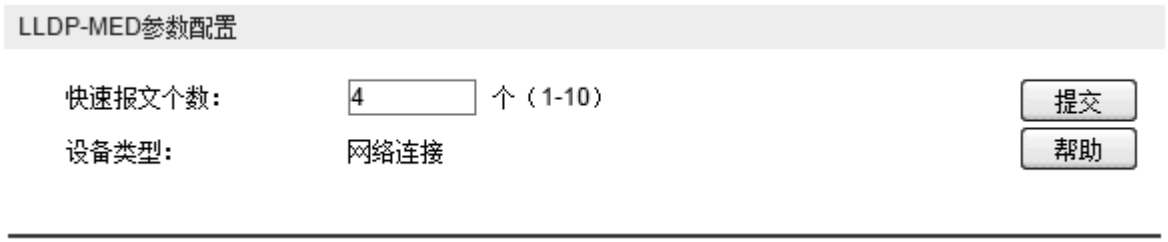


图 14-6 全局配置

条目介绍：

- **LLDP-MED 参数配置**

快速报文个数： 当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU，其默认值为 4。

设备类型： LLDP-MED 规定了两种设备类型，分别是网络连接设备（Network Connectivity Device）和终端设备（Endpoint Device），其中终端设备又可以分为 I、II 和 III 型共三种。交换机是一种网络连接设备。

16.4.2 端口配置

在本页可以配置所有端口的 LLDP-MED 状态和 TLV。

进入页面的方法：**LLDP>> LLDP-MED >>端口配置**

图 14-7 端口配置

条目介绍：

- **LLDP-MED 端口配置**

  选择： 勾选端口配置端口参数，可多选。

  端口： 显示交换机的端口号。

  LLDP-MED 状态： 启用/禁用端口的 LLDP-MED 功能。

  - 启用：启用端口的 LLDP-MED 功能，同时端口的 LLDP 状态会被设置为发送接收。
  - 禁用：禁用端口的 LLDP-MED 功能。

  TLV 字段： 选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 信息。

点击<详细>按键即可进入如下页面，在本页可以配置端口发送的 LLDPDU 中包含的可选 LLDP-MED 的 TLV。

图 14-8 TLV 字段

条目介绍：

- **TLV 字段**

网络策略： 网络策略 TLV 允许网络连接设备和终端设备发布本端口的 VLAN 配置与二层和三层属性。

设备地址： 设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。您可以在**设备地址参数**中配置设备端口的详细地址。如果没有配置**设备地址参数**而又包含了设备地址 TLV，那么将会使用一个默认的地址信息。

扩展供电能力： 扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交互详细的供电信息，例如供电优先级、供电状态等

资产信息： 资产信息中包含七种基本的资产信息 TLV，分别为硬件版本 TLV、固件版本 TLV、软件版本 TLV、序列号 TLV、制造厂商名称 TLV、模块名称 TLV 和资产跟踪 ID TLV。

- **设备地址参数**

紧急号码： 紧急号码是紧急呼叫服务使用的号码,用以呼叫 CAMA 或者 PSAP，字符长度介于 10 到 25 之间。

普通地址： 普通地址使用 IETF 规定的地址信息格式。

- 类型：描述本地设备充当的设备角色，当前有三种选择：DHCP 服务器，switch 和 LLDP-MED 终端。
- 国家代码：ISO 3166 规定的代表国家的两个字符的代码，例如 CN、US 等。
- 语言、省/州等：普通地址的详细信息。

16.4.3 本地信息

在本页可以查看所有端口的 LLDP-MED 配置信息。

进入页面的方法：**LLDP>> LLDP-MED >>本地信息**

图 14-9 本地信息

条目介绍：

- **自动刷新**

  自动刷新： 选择是否启用自动刷新功能。

  刷新周期： 填写自动刷新的时间周期。默认为 30 秒。

- **本地信息**

  端口选择： 点击快速选择相应端口。

  本地端口： 显示本地端口号。

  设备类型： 显示 LLDP-MED 规定的本地设备类型。

  应用类型： 显示本地设备支持的各种应用。

媒体策略未知标记：	显示网络策略 TLV 中包含的未知标记位设置。
已标记 VLAN：	显示应用所需 VLAN Tag 类型：tagged 或者 untagged。
VLAN ID：	显示端口所处 802.1Q VLAN 的 ID 值。
二层优先级：	显示特定应用使用的二层优先级。
QOS DSCP 值：	显示特定应用使用的 DSCP 值。
供电类型：	显示 LLDP-MED 设备的供电类型： 供电设备（PSE：Power Sourcing Entity ）或者受电设备（PD：Powered Device）。
供电来源：	显示供电设备或者受电设备的供电来源。
端口供电优先级：	显示本端口供电信息在所有端口中的位置，当供电能力不足时，供电优先级低的端口将停止供电，以满足高优先级的端口供电。
端口 PoE 能提供的电量值：	显示本端口通过 PoE 能给 PD 设备提供的最大电量值。

16.4.4 邻居信息

在本页可以查看所有端口邻居的 LLDP-MED 信息。

进入页面的方法：**LLDP>> LLDP-MED >>邻居信息**

图 14-10 邻居信息

条目介绍：

- **自动刷新**

  自动刷新： 选择是否启用自动刷新功能。

  刷新周期： 填写自动刷新的时间周期。默认为 5 秒。

- **LLDP-MED 邻居信息**

  端口选择： 点击快速选择相应端口。

回目录

第17章 系统维护

系统维护模块将管理交换机的常用系统工具组合在一起，为定位并排除交换机和网络故障提供便捷的方法。

1) 运行状态：对交换机内存和 CPU 进行监控。

2) 系统日志：通过系统日志查看在交换机上的配置参数并找出错误的配置。

3) 系统诊断：检测与交换机连接的线缆是否有故障及对端设备的可用性。

4) 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。

17.1 运行状态

在本功能中可以通过曲线数据监控交换机 CPU 和内存的使用情况，CPU 和内存使用率应该在一定数值上下波动。当 CPU 和内存使用率波动较大且明显增大时，请检查网络是否受到攻击。

本功能包括 **CPU 监控**和**内存监控**两个配置页面。

17.1.1 CPU 监控

进入页面的方法：系统维护>>运行状态>>CPU 监控

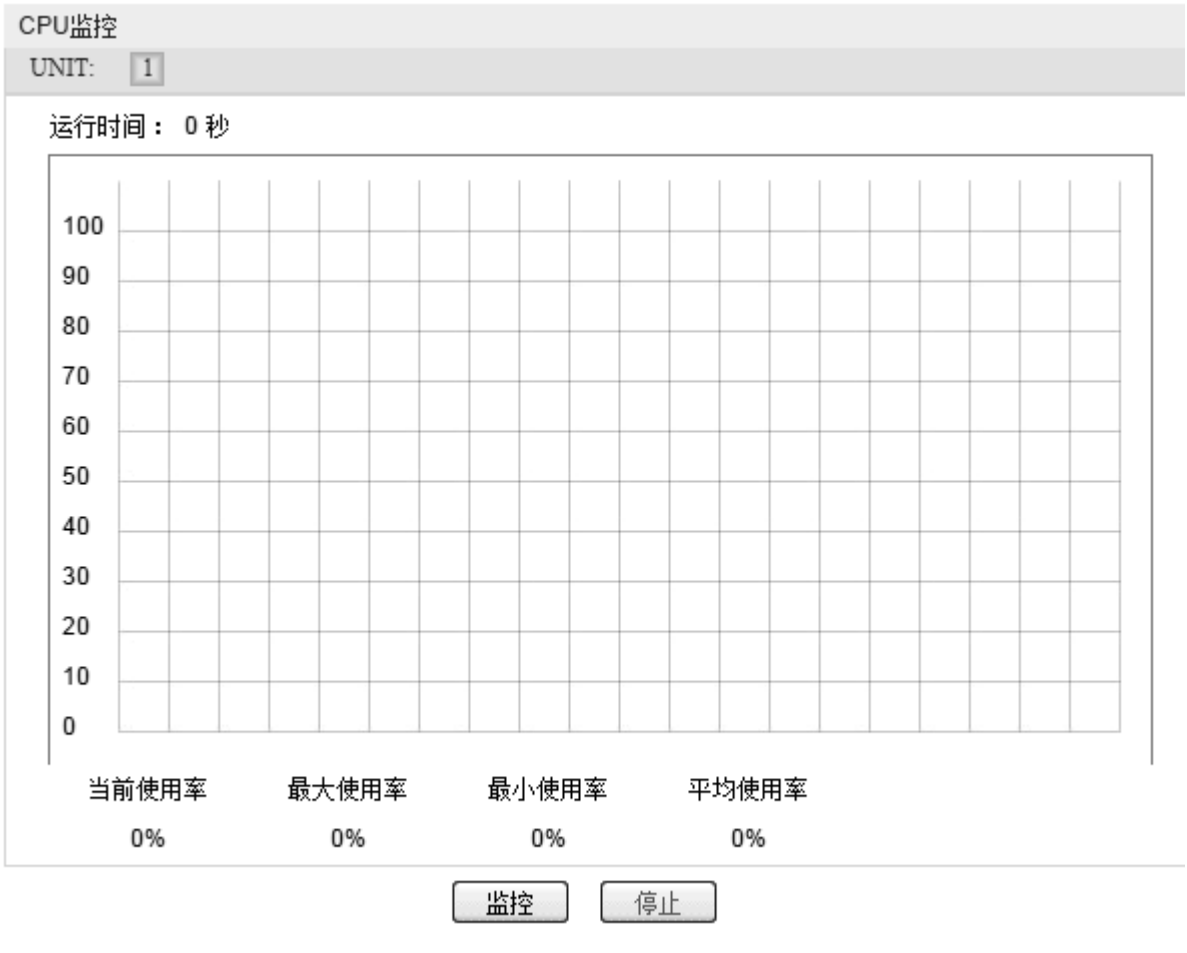


图 16-1 CPU 监控

点击<监控>按键，图中会每隔 4 秒反馈一次监控数值，显示交换机 CPU 使用率。

17.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

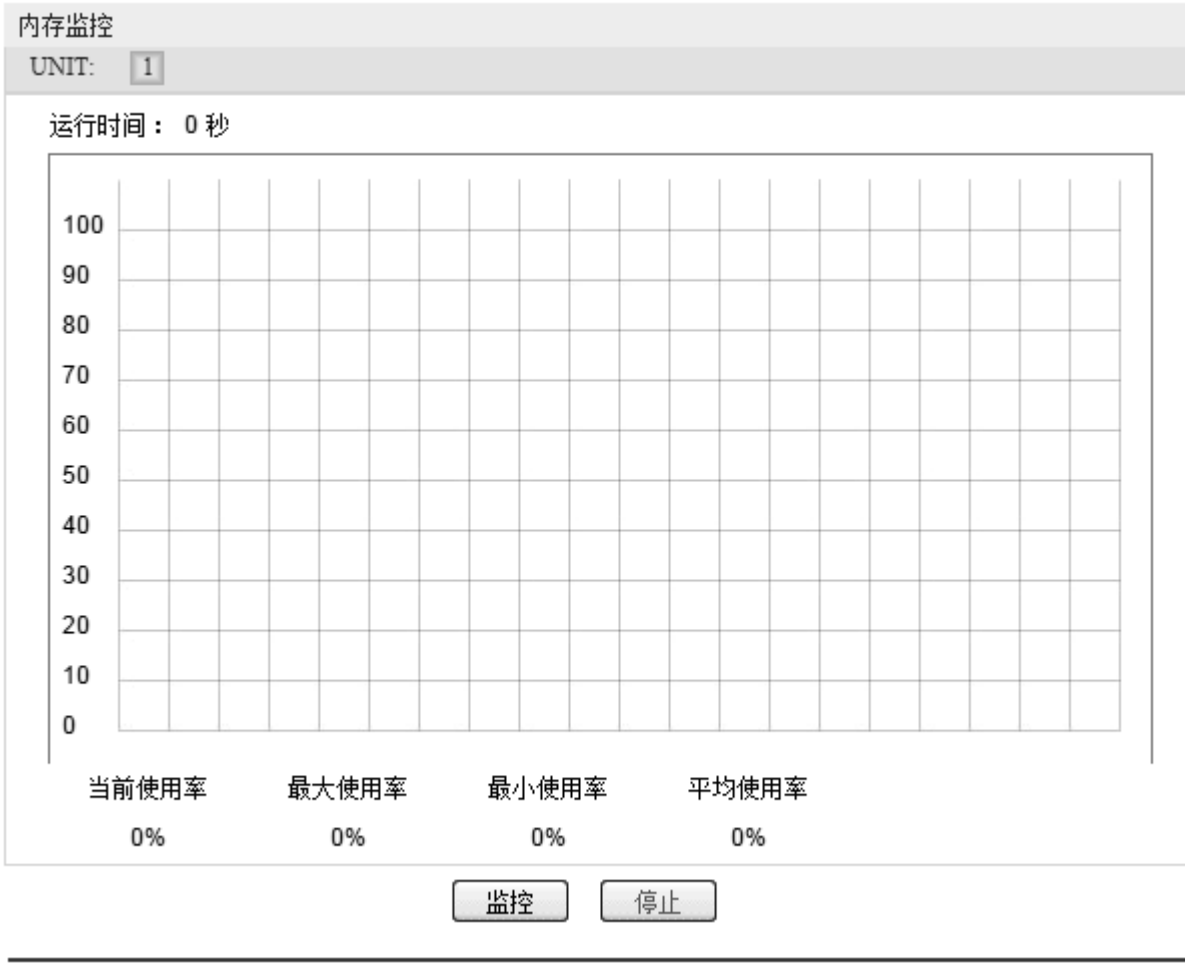


图 16-2 内存监控

点击<监控>按键，图中会每隔 4 秒反馈一次监控数值，显示交换机内存使用率。

17.2 sFlow 监控

sFlow 是一种可以精确监控高速网络流量的技术。sFlow 监控系统由 sFlow 代理（嵌入在交换机或路由器或独立探测器中）和中央 sFlow 收集器组成。sFlow 代理运用采样技术对监控的网络设备进行流量统计采样。sFlow 收集器对来自 sFlow 代理的数据进行处理。

本功能包括 **sFlow 收集和 sFlow 采样**两个功能页面。

17.2.1 sFlow 收集

进入页面的方法：**系统维护>>sFlow 监控>>sFlow 收集**

图 17-1 sFlow 收集

配置过程:

1) 点击开启全局使能 sFlow 功能，并配置 sFlow 代理的 IP 地址。例如，您可以将交换机的管理 IP 设置为 sFlow 代理的 IP。

2) 选择你想要使用的收集器，并进行相关参数配置。

条目描述:

- **全局配置**

sFlow 状态	全局启用/禁用 sFlow 功能。
代理地址	sFlow 代理的 IPv4 地址。
sFlow 版本	显示 sFlow 版本。

- **收集器配置**

选择	选择要配置的收集器。可多选。
收集器 ID	在此处显示收集器 ID。最多可配置 4 个收集器。
描述	填写收集器的描述信息。
收集器 IP	指定收集器的 IP 地址。
收集器端口	指定收集器的端口号。
最大数据报	指定单个数据报中可以发送的最大字节数。
超时(s)	指定收集器的老化时间。收集器将在超时时间过后失效。如果超时时间设置为 0，收集器的生命周期无限长。
生命周期(s)	指定收集器的生命周期。生命周期将从超时开始倒计时。

17.2.2 sFlow 采样

进入页面的方法：**系统维护>>sFlow 监控>>sFlow 采样**

采样设置

UNIT: 1

选择	端口	收集器ID	进口速率	出口速率	最大包头	LAG
	1/0/1	0	0	0	128	---
	1/0/2	0	0	0	128	---
	1/0/3	0	0	0	128	---
	1/0/4	0	0	0	128	---
	1/0/5	0	0	0	128	---
	1/0/6	0	0	0	128	---
	1/0/7	0	0	0	128	---
	1/0/8	0	0	0	128	---
	1/0/9	0	0	0	128	---
	1/0/10	0	0	0	128	---
	1/0/11	0	0	0	128	---
	1/0/12	0	0	0	128	---
	1/0/13	0	0	0	128	---
	1/0/14	0	0	0	128	---
	1/0/15	0	0	0	128	---

全选 提交 帮助

注意：：
1. 一个端口只能绑定到一个收集器。
2. 当收集器ID为零时，表示未选择收集器。

图 17-2 sFlow 采样

配置过程:

配置一个或多个端口作为采样器，并进行相关参数配置。一个端口只能绑定到一个收集器。

条目描述:

选择	选择要配置成采样器的端口。
端口	显示交换机的端口号。
收集器 ID	为 sFlow 采样器选择 sFlow 收集器。采样器将通过 sFlow 代理将数据报发送给收集器。当收集器 ID 为 0，表示未选择收集器。
进口速率	指定采样器的进口采样频率。
出口速率	指定采样器的出口采样频率。
最大包头	指定从采样数据报复制的最大字节数。
LAG	显示端口所属的汇聚组。

17.2.3 默认设置

功能	默认设置
全局 sFlow	禁用
sFlow 代理	代理地址未定义。
sFlow 收集器	• 收集器端口是 6343。 • 最大数据报是 300 个字节。 • 其他参数未定义。
sFlow 采样器	• 收集器 ID 为 0，表示未选择收集器。 • 进口速率为 0，表示不取样。 • 出口速率是 0，表示不取样。 • 最大包头是 128 个字节。

17.3 系统日志

本交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。

本交换机的系统日志分为八个等级，如表 16-1 所示。

级别名称	等级	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debugging	7	调试过程产生的信息

表 16-1 日志等级

本功能包括**日志列表**、**本地日志**、**远程日志**和**日志导出**四个功能页面。

17.3.1 日志列表

系统日志可以保存到两个不同的地方：日志缓冲区和日志文件。日志缓冲区的日志信息在交换机重启后将会丢失，日志文件里的日志信息在交换机重启后仍然有效。日志列表显示了日志缓冲区中的系统日志信息。

进入页面的方法：系统维护>>系统日志>>日志列表

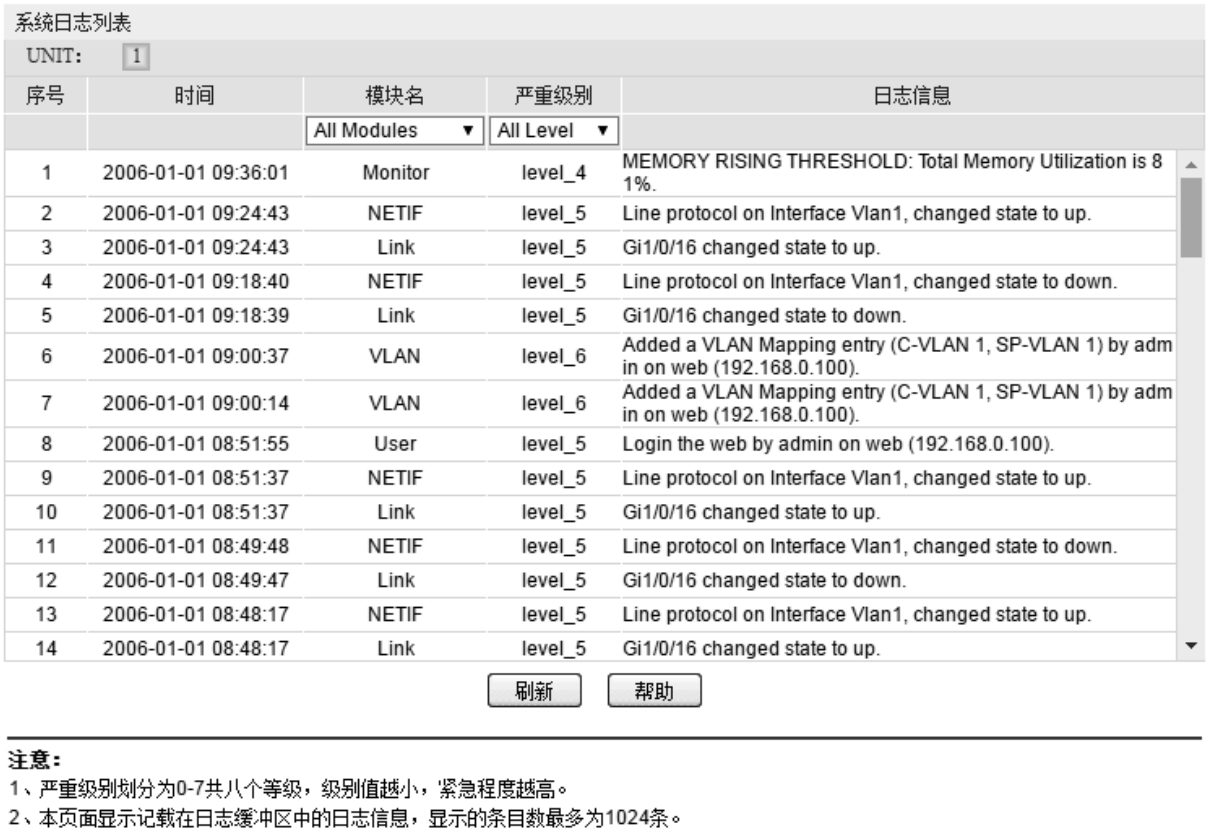


图 16-3 日志列表

条目介绍：

- **系统日志列表**

序号： 显示该日志信息的序号。

时间： 显示该日志信息的发生时间。需先在**系统管理>>系统配置>>系统时间页面**进行配置后，系统日志才能获取到正确的时间。

模块名： 显示该日志信息所属功能模块，从下拉列表可选择显示某一模块的日志信息。

严重级别： 显示该日志信息的严重级别，从下拉列表选择某一级别，可显示小于或等于该级别值的日志信息。

日志信息： 显示该日志信息的内容。

注意：

- 严重级别划分为 0-7 共八个等级，级别值越小，紧急程度越高。
- 本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为 512 条。

17.3.2 本地日志

本地日志是指保存在本交换机上的所有系统日志信息。在缺省情况下，所有的系统日志将保存到日志缓冲区，而等级为 level_0 到 level_3 的系统日志将同时保存到日志文件中。在此页面中可以对日志的存储区进行配置。

进入页面的方法：系统维护>>系统日志>>本地日志

图 16-4 本地日志

条目介绍：

- **系统日志列表**

选择：	勾选相应的日志输出方向进行配置。
日志缓冲区：	**日志列表**页面上显示的即为缓冲区中的信息，在断电重启后这些信息将会丢失。
日志文件：	日志文件中的日志信息在断电重启后不会丢失，可通过导出日志文件来查看。
严重级别：	限定各个输出方向上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会进行输出。
状态：	启用/禁用该输出方向。

17.3.3 远程日志

远程日志功能可以将本交换机的系统日志发送到日志服务器上。日志服务器相当于一个可维护的共用消息区，它可以对网络中各设备产生的日志信息进行集中的监控和管理。

进入页面的方法：系统维护>>系统日志>>远程日志

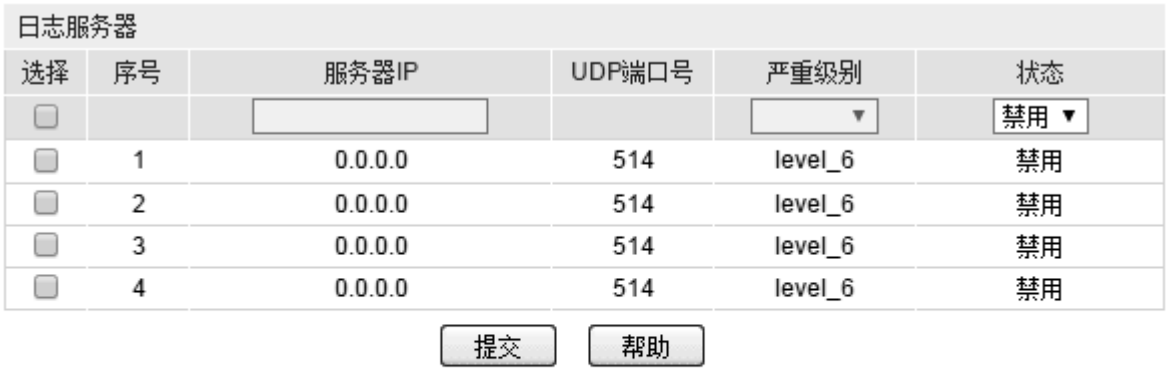


图 16-5 日志服务器

条目介绍：

- **日志服务器**

选择： 勾选相应的日志服务器进行配置。

序号： 日志服务器序号。本交换机共支持 4 个日志服务器。

服务器 IP： 配置日志服务器的 IP 地址。

UDP 端口号： 发送/接收系统日志时所用到的 UDP 端口号，这里使用标准的 514 端口。

严重级别： 限定发往各个服务器上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会发送到相应的服务器。

状态： 启用/禁用该服务器。

17.3.4 日志导出

日志导出功能可以将保存在交换机里的日志信息以文件的形式导出，作为设备诊断和统计分析之用。尤其在发生严重错误导致系统崩溃时，可在重启后导出日志信息，以获取跟错误相关的一些重要信息，为诊断设备提供支持。

进入页面的方法：系统维护>>系统日志>>日志导出

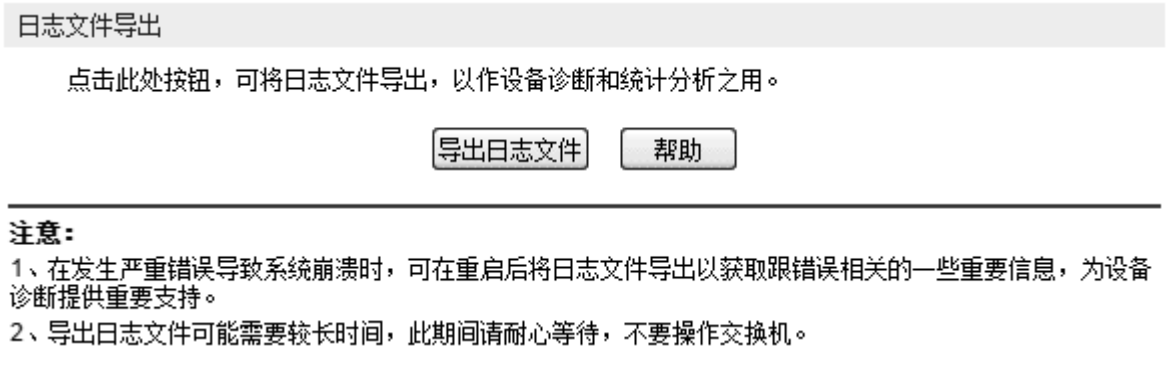


图 16-6 日志导出

条目介绍：

- **日志文件导出**

  导出日志文件： 点击此按键导出日志文件中的日志信息。

17.4 系统诊断

本交换机提供了线缆检测和环回检测功能。

17.4.1 线缆检测

线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

进入页面的方法：系统维护>>系统诊断>>线缆检测

图 16-7 线缆检测

条目介绍：

- **线缆检测**

  检测端口： 选择要进行线缆检测的端口。

线对：	显示线对序号。
线路状态：	检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。 ● 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。 ● 短路：线路金属内芯互相接触，导致短路。 ● 阻抗失配：网线质量问题。
线路长度：	若线路为正常状态，显示该线缆的长度范围。
出错长度（米）：	若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

注意：

- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

17.5 网络诊断

本交换机提供了 Ping 检测和 Tracert 检测功能。

17.5.1 Ping 检测

Ping 检测功能可以检测交换机与某网络设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping 检测过程如下：

1) 交换机向目标设备发送 ICMP 请求报文；
2) 如果网络工作正常，则目标设备在接收到该报文后，向交换机返回 ICMP 应答报文；显示相关统计信息；
3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息。

进入页面的方法：系统维护>>网络诊断>>Ping 检测

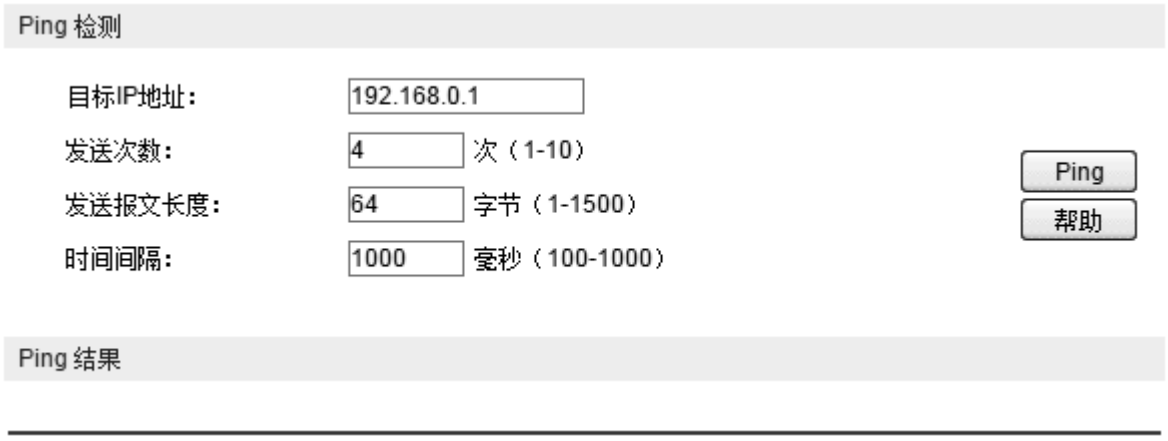


图 16-9 Ping 检测

条目介绍：

- **Ping 检测**

目标 IP 地址： 填写需要测试的目标节点的 IP 地址。

发送次数： 填写 Ping 检测时发送的检测包次数。建议使用缺省值。

发送报文长度： 填写 Ping 检测时发送的检测包长度。建议使用缺省值。

时间间隔： 发送 ICMP 请求报文的时间间隔。

17.5.2 Tracert 检测

Tracert 检测可以查看交换机到目标节点所经过的路由器。当网络出现故障时，使用该命令可以分析出现故障的网络节点。

在 IP 数据包首部中包含一个 TTL 字段，当数据包在网络中转发时，每经过一个路由 TTL 字段的值减 1。当接收的 IP 数据包的 TTL 字段为 0 或 1 时，路由器将此数据包丢弃，并给发送源回复一个 ICMP 超时报文。这样能有效防止数据包在网络发生故障时，无休止地在网络中流动。

Tracert 检测过程如下：

1) 交换机发送一个 TTL 为 1 的报文给目的设备；
2) 第一跳（即该报文所到达的第一个路由器）回应一个 TTL 超时的 ICMP 报文（该报文中含有第一跳的 IP 地址），这样交换机就得到了第一个路由器的地址；
3) 交换机重新发送一个 TTL 为 2 的报文给目的设备；
4) 第二跳回应一个 TTL 超时的 ICMP 报文，这样交换机就得到了第二个路由器的地址；
5) 重复以上过程直到最终到达目的设备，交换机就得到了从它到目的设备所经过的所有路由器的地址。

进入页面的方法：系统维护>>网络诊断>>Tracert 检测

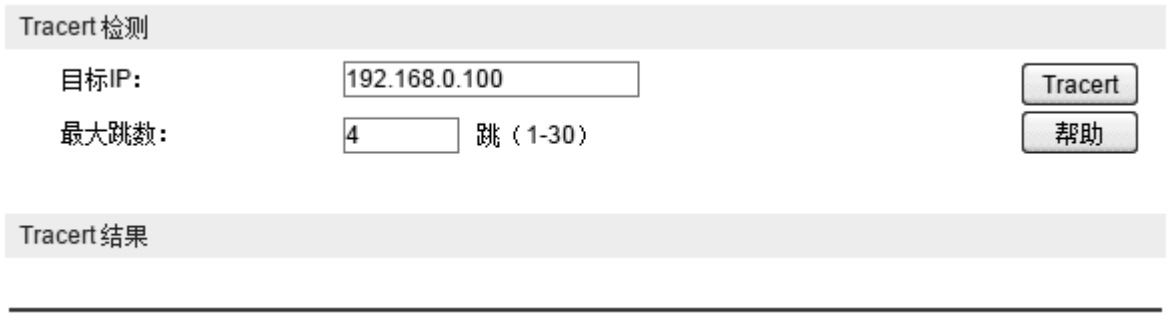


图 16-10 Tracert 检测

条目介绍：

- **Tracert 检测**

目标 IP： 填写目的设备的 IP 地址。

最大跳数： 填写测试报文发送的最大跳数。

回目录

第18章 软件系统维护

在本交换机中，可以通过FTP功能加载软件。FTP（File Transfer Protocol，文件传输协议）在TCP/IP协议族中属于应用层协议，主要用于在远端服务器和本地主机之间传输文件，是IP网络上传输文件的通用协议。当交换机软件出故障导致无法正常启动时，也可以采用FTP功能重新加载软件。

18.1 硬件连接图

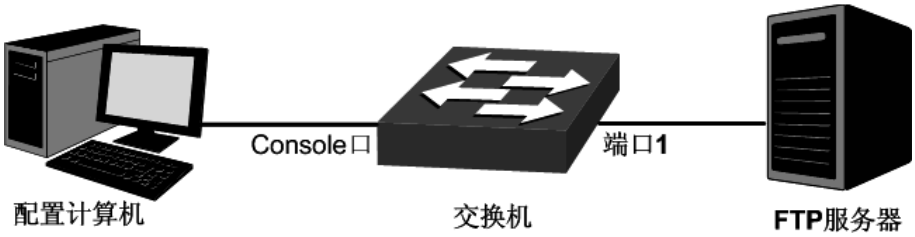


图 17-1 利用 FTP 加载软件连接图

1. FTP 服务器通过端口 1 连接到交换机。
2. 配置计算机通过 Console 口与交换机连接。配置计算机和 FTP 服务器可以是同一台主机。
3. 将交换机软件存储在 FTP 服务器的共享目录下，并记录相应用户名、密码以及交换机软件名称，以便后续使用。

18.2 配置超级终端

完成硬件连接后，请按照下面步骤配置管理计算机的超级终端，以便管理交换机。

1. 选择**开始>>所有程序>>附件>>通讯>>超级终端**，打开超级终端。

图 17-2 打开超级终端

2. 弹出如图 17-3 所示的连接描述窗口，在名称处键入一个名称，点击**确定**。

图 17-3 连接描述

3. 在图 17-4 中选择连接串口，点击**确定**。

图 17-4 连接端口选择

4. 在图 17-5 中对端口进行参数设置：每秒位数“38400”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，然后点击**确定**即可。

图 17-5 端口属性设置

18.3 密码重置

请按照下面提示步骤进行操作：

1. 将配置计算机的串口连接到交换机的Console口，并打开配置成功的超级终端。

2. 将交换机断电重启，当在超级终端界面中看到提示信息“Hit any key to stop autoboot”，用户需要在3秒内按下任意按键进入bootUtil菜单。如下图所示：

```
Hit any key to stop autoboot:  0
                 ************************************************
                 *          SWITCH  BOOTUTIL(v2.0.0)            *
                 ************************************************
                 Copyright (c) 2017
                 Create Date: Apr 26 2017 - 17:41:23

   Boot Menu
0  - Print this boot menu
1  - Reboot
2  - Reset
3  - Start
4  - Activate Backup Image
5  - Display image(s) info
6  - Password recovery

Enter your choice(0-6)

switch> 6
This will delete all the previously created accounts. Continue?[Y/N]:Y
Operation OK!
switch>
```

4. 按下“6”按键选择“Password recovery”选项，并按下“Y”按键删除所有用户名和密码。复位后恢复到出厂默认设置，登录交换机的用户名和密码均为admin。

回目录

附录 A 802.1X 客户端软件使用说明

在 802.1X 体系结构中，客户端作为接入设备需要安装相应的客户端软件，且软件遵循 802.1X 协议标准才能够顺利通过认证。当使用本交换机进行认证时，请使用我司提供的客户端软件进行认证。

1. 安装说明

1. 双击安装软件图标，弹出安装语言选择对话框，如下图 1 所示。

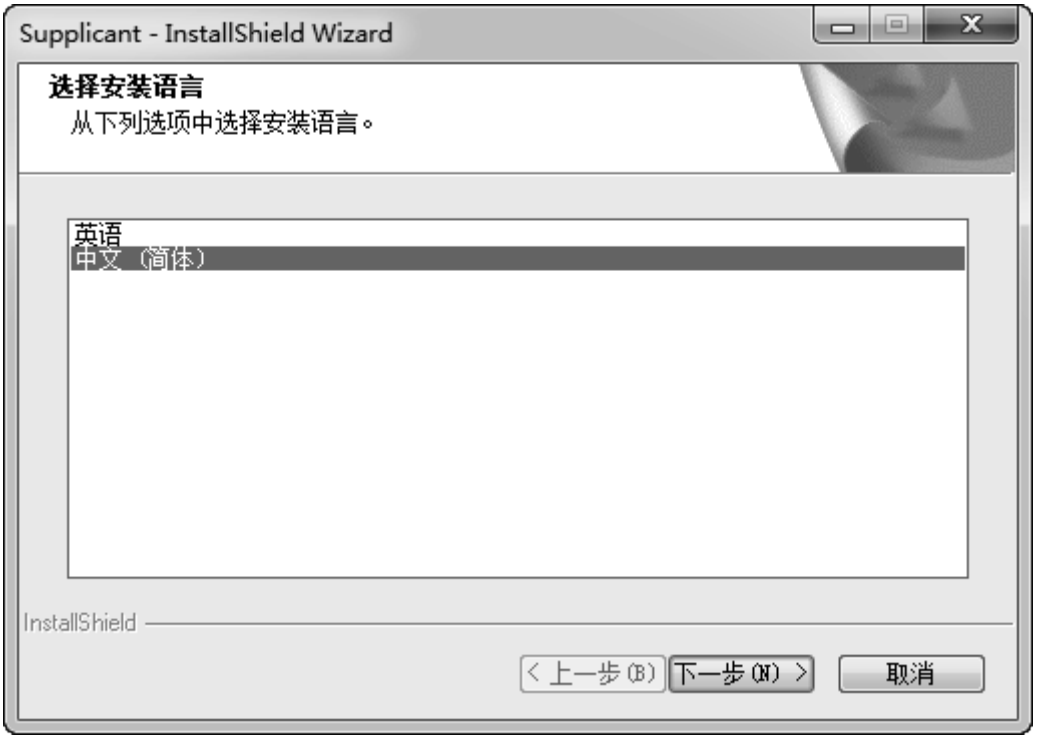


图 1 选择安装语言对话框

2. 单击下一步进入安装准备过程，如下图 2 所示：

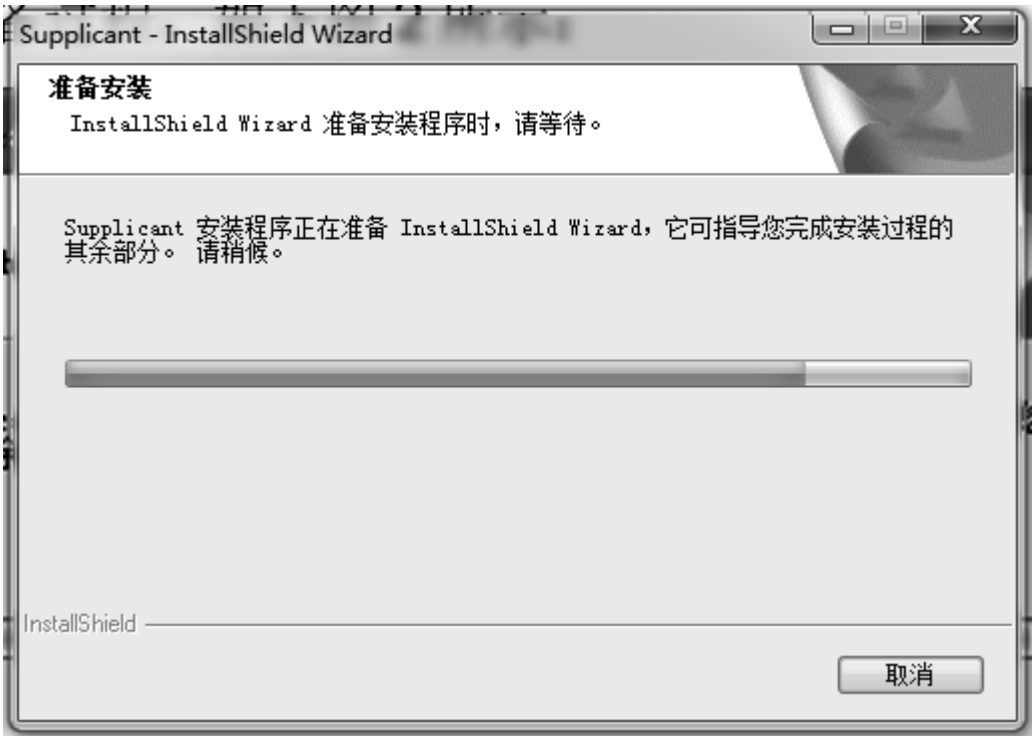


图 2 准备安装对话框

3. 等待片刻，系统准备工作完成后，将自动弹出欢迎对话框，如下图 3 所示，此时可点击<取消>终止安装过程：

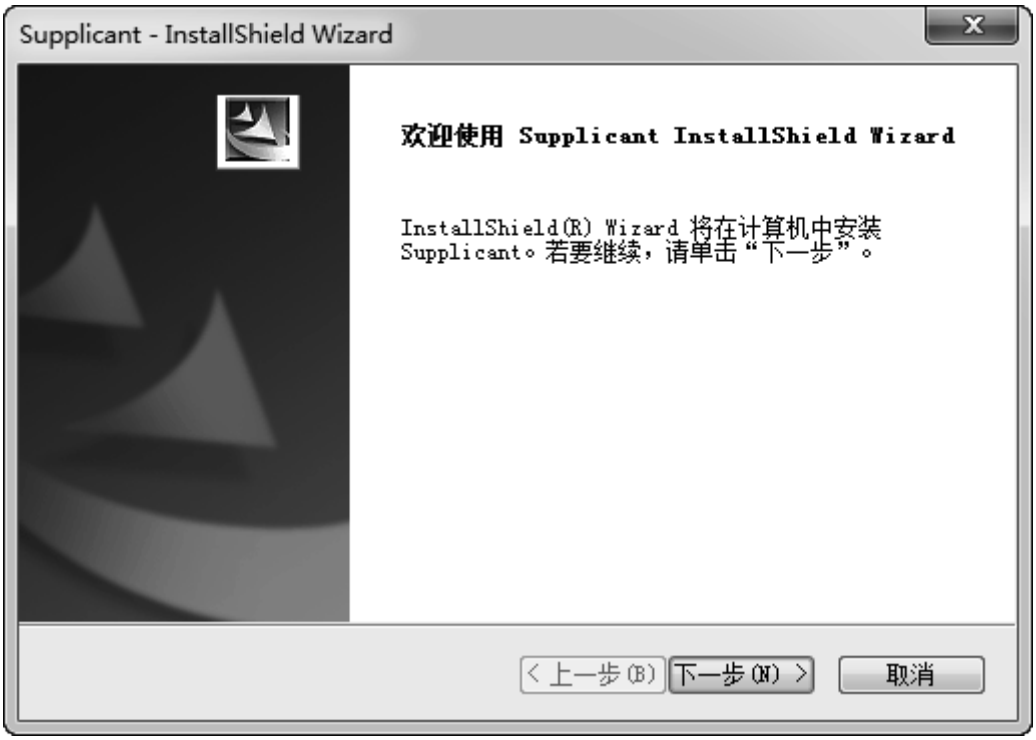


图 3 欢迎对话框

4. 点击<下一步>进行安装路径的选择，如下图 4 所示。点击<更改...>可以选择合适的安装路径。

图 4 安装路径对话框

5. 至此，安装所需参数已确定。点击<下一步>，弹出安装对话框。如下图 5 所示：

图 5 正在安装

6. 点击<安装>，开始安装 802.1X 客户端软件，如下图 6 所示：

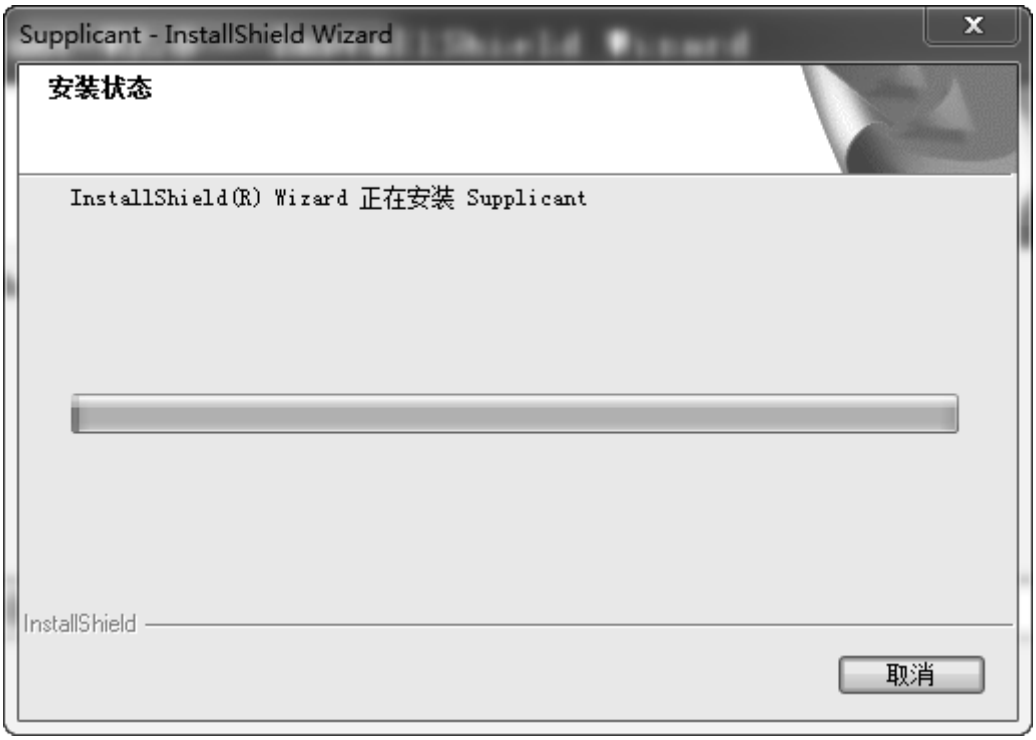


图 6 安装过程

7. 等待片刻，将弹出安装完成对话框。如下图 7 所示：

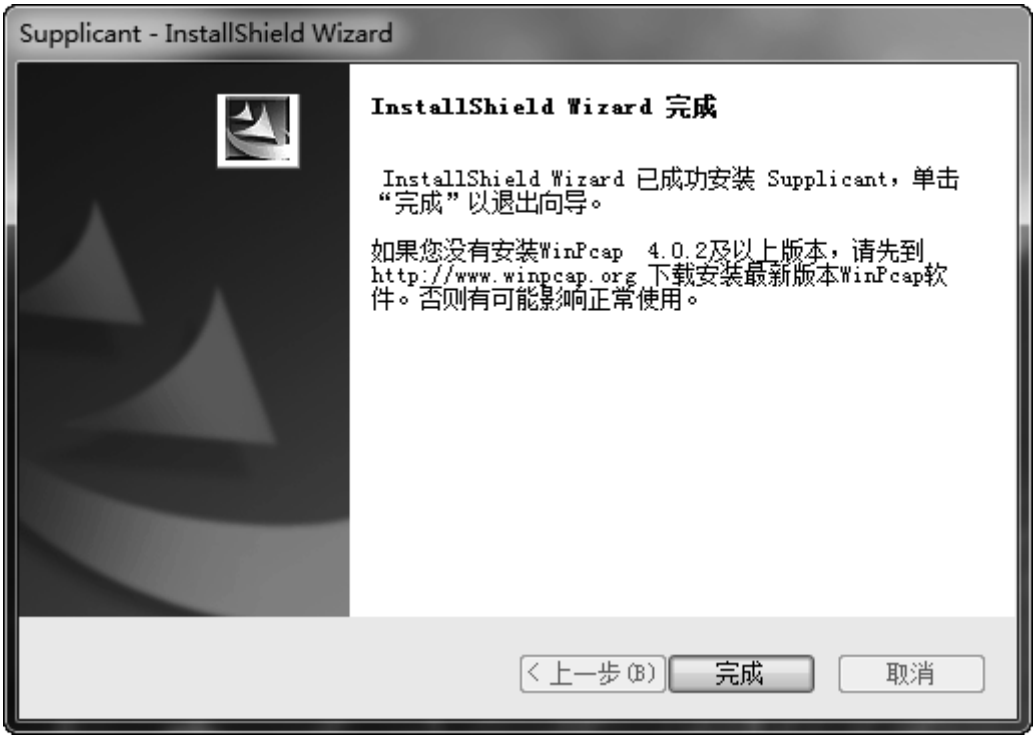


图 7 安装完成对话框

8. 根据页面提示，安装完成后，如果计算机上没有安装 WinPcap 4.0.2 版本以上的软件，将无法使用该 802.1X 客户端进行认证。请在网上下载 WinPcap 软件并安装。点击<完成>退出。

2. 卸载说明

当需要卸载 802.1X 时，可以按照下面步骤执行：

1. 选择：**开始 >> 所有程序 >> 802.1X >>卸载 802.1X 客户端**进行客户端软件卸载。软件卸载准备对话框如下图 8 所示：

图 8 软件卸载准备

2. 点击<是>，开始卸载软件，如下图 9 所示：

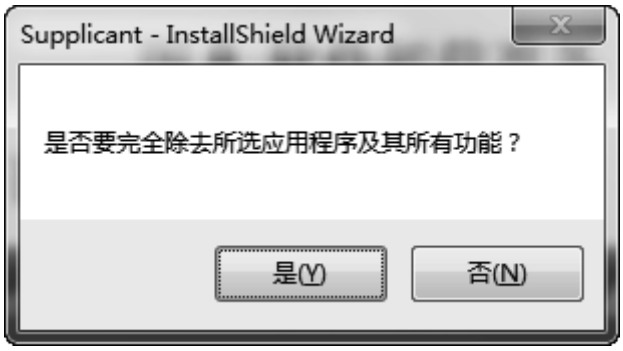


图 9 卸载软件

3. 卸载结束后，点击<完成>关闭窗口即可，如下图 10 所示：

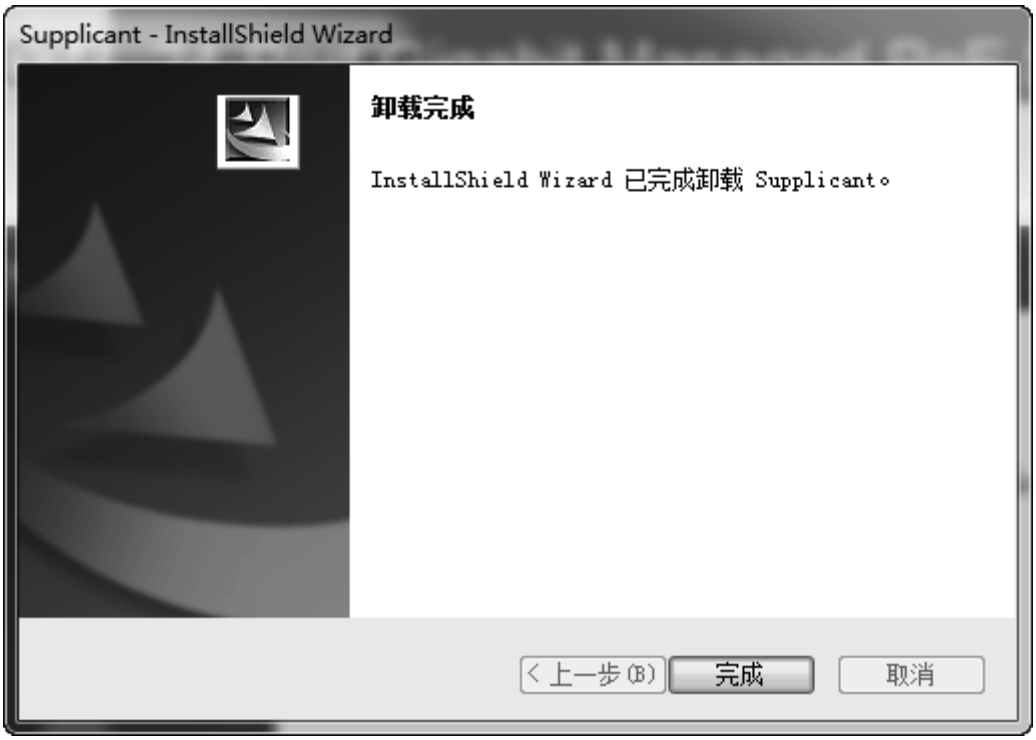


图 10 完成卸载

3. 使用说明

1. 安装完成后，双击桌面 802.1X 客户端软件图标 

运行应用程序，弹出程序主对话框如下图 11 所示：

图 11 主对话框

在用户名和密码中输入服务器端设定好的用户名和密码，注意用户名和密码均不得多于 16 个字符。

2. 点击<属性>按键，弹出属性对话框，可以对拨号属性进行适当的设置，如下图 12 所示：

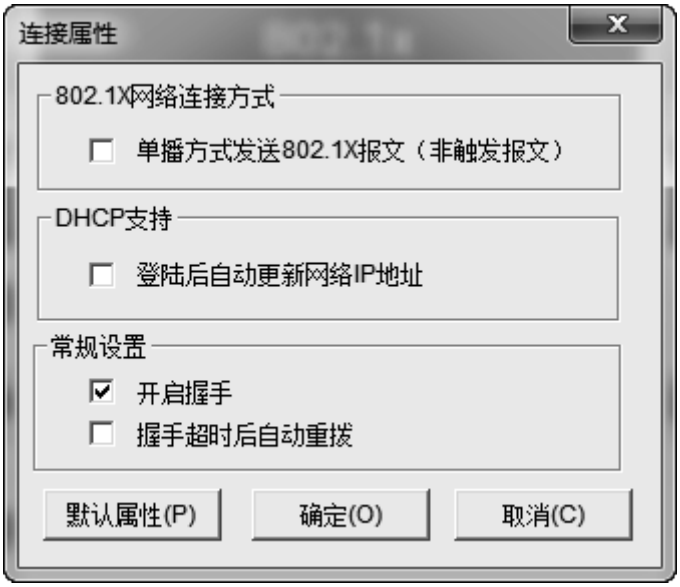


图 12 属性对话框

单播方式发送 802.1X 报文（非触发报文）：选择此项时，客户端将以组播的方式向交换机申请认证，然后以单播方式发送认证报文。

登陆后自动更新 IP 地址：如果接入网络中设置了 DHCP 服务器为客户端分配 IP，请选择此项功能。认证成功后 DHCP 服务器会自动给客户端分配 IP 地址，客户端获得新的 IP 地址后才能访问网络。

握手超时后自动重拨：选择此项时，如果客户端在一定的时间内没有收到交换机的握手应答报文，则说明客户端和交换机的连接可能出现问题，这时客户端软件将自动重新发起连接。

3. 在主窗口如图 11 界面下如果点击<连接>，将弹出认证状态对话框显示认证过程，如下图 13 所示：

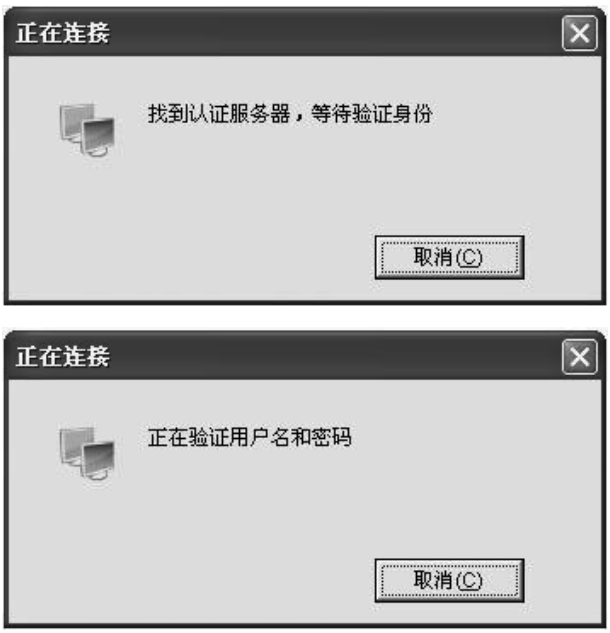


图 13 认证状态对话框

4. 当顺利的通过认证后，会显示一个认证通过对话框，如下图 14 所示：

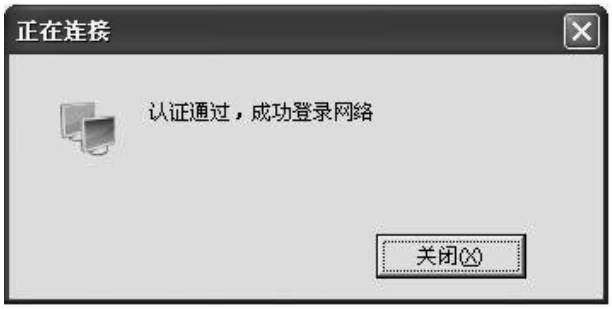


图 14 认证通过对话框

5. 双击系统托盘中的连接状态图标，将弹出连接状态对话框，如下图 15 所示：

图 15 连接状态对话框

4. 常见问题：

1. 当我运行该软件的时候为什么会出现如下图所示的错误对话框？

图 16 缺失 DLL 对话框

答：如果出现图 16 对话框，说明缺少了支持的 DLL 文件，如果没有安装 WinPcap 4.0.2 或以上版本，请先到 http://www.winpcap.org 下载安装最新版本 WinPcap 软件，然后重新运行该客户端。

2. 可以使用该软件拨号其它公司生产的交换机吗？

答：不可以，该软件是专门为我司交换机定制。

3. 如果我设置保存密码会不会不安全？

答：不会，保存到配置文件中的密码已经经过加密。

回目录

附录 B 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3 10Base-T 以太网 IEEE 802.3u 100Base-TX 快速以太网 IEEE 802.3ab 1000Base-T 千兆以太网 IEEE 802.3z 千兆以太网（光纤） ANSI/IEEE 802.3 N-Way 自动协商 IEEE 802.3x 流量控制 IEEE 802.1p 优先级 IEEE 802.1q VLAN IEEE 802.1X 基于端口的访问认证 CSMA/CD Ethernet IEEE 802.3af IEEE 802.3at
数据传输速率	以太网：10Mbps 半双工，20Mbps 全双工 快速以太网：100Mbps 半双工，200Mbps 全双工 千兆以太网：2000Mbps 全双工
网络介质	10Base-T：3 类或以上 UTP/STP（≤100m） 100Base-TX：5 类或以上 UTP/STP（≤100m） 1000Base-T：超 5 类或以上 UTP/STP（≤100m）
传输方式	存储转发
背板带宽	56Gbps
MAC 地址学习	自动更新，支持 16K 地址空间
包转发速率	10Base-T：14881pps/端口 100Base-TX：148810pps/端口 1000Base-T：1488095pps/端口
交流输入	100-240V~ 50/60Hz 6.0A
工作温度	0℃~40℃
存储温度	-40℃~70℃
工作湿度	10%~90%（RH 无凝结）
存储湿度	5%~90%（RH 无凝结）

回目录