User Guide

JetStream 8-Port Gigabit Smart Switch

T1500G-10MPS/T1500G-8T (TL-SG2008)

REV1.0.1

1910012042

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE Mark Warning

CE

This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Industry Canada Statement

CAN ICES-3 (A)/NMB-3(A)

Safety Information

- When product has power button, the power button is one of the way to shut off the product; When there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。
- 此為甲類資訊技術設備，于居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

Explanation of the symbols on the product label

Symbol	Explanation
	AC voltage
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.
	Indoor use only

CONTENTS

Package Contents

The following items should be found in your box:

- One Gigabit Smart Switch
- One power cord
- Four rubber cushions

  Two mounting brackets and other fittings
- Installation Guide
- Resource CD, including:
  - This User Guide
  - CLI Reference Guide
  - SNMP Mibs
  - 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 T1500G-10MPS/ T1500G-8T JetStream 8-Port Gigabit Smart Switch. 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

In this Guide the following conventions are used:

- The switch or device mentioned in this Guide stands for T1500G-10MPS/T1500G-8T JetStream 8-Port Gigabit Smart Switch without any explanation.

Tips:

The T1500G-10MPS/T1500G-8T switchs are sharing this User Guide. They just differ in the number of LED indicators and ports. For simplicity, we will take T1500G-10MPS for example throughout this Guide. However, differences with significance will be presented with figures or notes as to attract your attention.

- **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.

1.3 Overview of This Guide

Chapter	Introduction
Chapter 1 About This Guide	Introduces the guide structure and conventions.

Chapter	Introduction
Chapter 2 Introduction	Introduces the features, application and appearance of T1500G-10MPS/T1500G-8T.
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.
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. ● DHCP Filtering: Monitor the process of the host obtaining the IP address from DHCP server.
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.
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	Introduction
Chapter 8 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. ● Multicast IP: Configure multicast IP table. ● Multicast Filter: Configure multicast filter feature to restrict users ordering multicast programs. ● Packet Statistics: View the multicast data traffic on each port of the switch, which facilitates you to monitor the IGMP messages in the network.
Chapter 9 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 10 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 11 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: ● ACL Config: ACL rules. ● Policy Config: Configure operation policies. ● Policy Binding: Bind the policy to a port/VLAN to take its effect on a specific port/VLAN.

Chapter	Introduction
Chapter 12 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. ● 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. ● ARP Inspection: Configure ARP inspection feature to prevent the network from ARP attacks. ● 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. ● AAA: Configure the authentication, authorization and accounting features.
Chapter 13 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 13 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 LLDP-MED parameters of the device.

Chapter	Introduction
Chapter 14 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 Specifications	Lists the hardware specifications of the switch.
Appendix B Glossary	Lists the glossary used in this manual.

Return to CONTENTS

Chapter 2 Introduction

2.1 Overview of the Switch

Designed for workgroups and departments, T1500G-10MPS/T1500G-8T from TP-Link provides wire-speed performance and full set of layer 2 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. QoS and IGMP snooping/filtering optimize voice and video application. Link aggregation (LACP) increase aggregated bandwidth, optimizing the transport of business critical data. SNMP, RMON, WEB/CLI/Telnet Log-in bring abundant management policies.T1500G-10MPS/T1500G-8T 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

■ **T1500G-10MPS**

The front panel of T1500G-10MPS is shown as Figure 2-1.

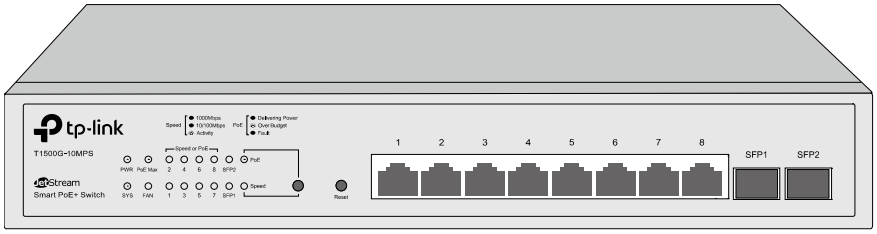


Figure 2-1 Front Panel of T1500G-10MPS

The following parts are located on the front panel of T1500G-10MPS:

➢ **LEDs**

T1500G-10MPS 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 status. 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.

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

Name	Status		Indication
SYS	Flashing		The switch is working normally.
	On/Off		The switch is working abnormally.
FAN	Green		All the fans work properly
	Yellow		Not all the fans work properly
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
Speed or PoE	Green	On	A 1000Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Yellow	On	A 10/100Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Off		No device is connected to the corresponding port.
SPF1, SFP2	Green	On	A 1000Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Yellow	On	A 10/100Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Off		No device is connected to the corresponding port.

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

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 is working normally.
	On/Off	The switch is working abnormally.
FAN	Green	All the fans work properly
	Yellow	Not all the fans work properly

Name	Status		Indication
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
Speed or PoE	Green	On	The port is supplying power normally
		Flashing	The supply power exceeds the corresponding port's maximum power
	Yellow	On	Overload or short circuit is detected
		Flashing	Power-on self-test has failed
	Off		No device is connected to the corresponding port.
SPF1, SFP2	Green	On	A 1000Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Yellow	On	A 10/100Mbps device is connected to the corresponding port, but no activity
		Flashing	Data is being transmitted or received
	Off		No device is connected to the corresponding port.

➢ **Reset**

Press this button for five seconds or above to reset the software setting back to factory default setting.

➢ **10/100/1000Mbps RJ45 Port and PoE Port**

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

➢ **SFP Port**

Designed to install the SFP module. T1500G-10MPS features 2 SFP transceiver ports.

■ **T1500G-8T**

The front panel of T1500G-8T is shown as Figure 2-2.

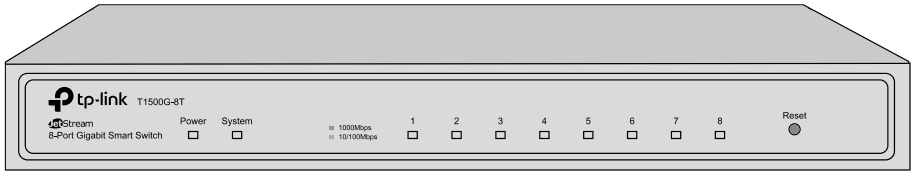


Figure 2-2 Front Panel of T1500G-8T

The following parts are located on the front panel of T1500G-8T:

- **LEDs**

Name	Status	Indication
Power	On	The switch is powered on
	Off	The switch is powered off or power supply is abnormal
	Flashing	Power supply is abnormal
System	Flashing	The switch is working normally.
	On/Off	The switch is working abnormally.
1-8	On (Green)	The corresponding port is connected to a 1000Mbps device
	On (Yellow)	The corresponding port is connected to a 10/100Mbps device
	Flashing	The corresponding port is transmitting/receiving data

- **Reset**

Press this button for five seconds or above to reset the software setting back to factory default settings.

2.2.2 Rear Panel

■ **T1500G-10MPS**

The rear panel of T1500G-10MPS features a Kensington Security Slot, a power socket and a Grounding Terminal (marked with⏚).

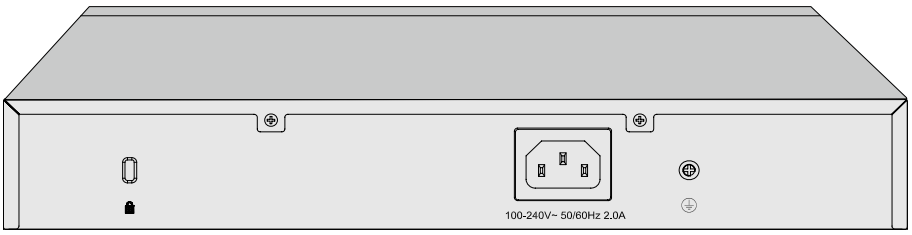


Figure 2-3 Rear Panel of the switch

- **Kensington Security Slot**

  Secure the lock (not provided) into the security slot to prevent the device from being stolen.

- **Power Socket**

  Connect the female connector of the power cord here, and the male connector to the AC (Alternating Current) power outlet. Please make sure the voltage of the power supply meets the requirement of the input voltage.

➢ **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.

■ **T1500G-8T**

The rear panel of T1500G-8T features a power socket, 8 10/100/1000Mbps Ethernet ports and a Kensington Security Slot.

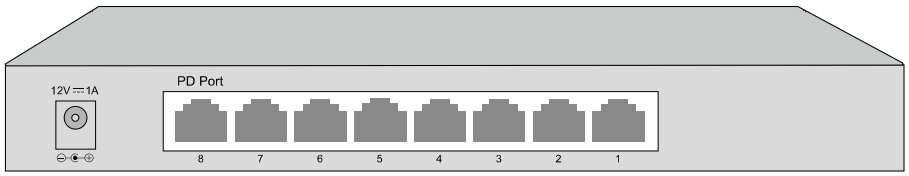


Figure 2-4 Rear Panel of T1500G-8T

➢ **Power Socket**

Connect the power socket and AC (Alternating Current) power outlet with the provided DC power adapter and AC power cord. Please make sure the voltage of the power supply meets the requirement of the input voltage.

➢ **Port 1-8**

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

Please note that port 8 is a PD (Powered Device) port that supports being powered by a PSE (Power Sourcing Equipment) complying with 802.3af standard. The DC power input takes precedence over the PD port. If the DC input fails, the PoE input on the PD port will supply power to the switch instead.

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. For the detailed instructions as to how to do this, please refer to Appendix B.

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.

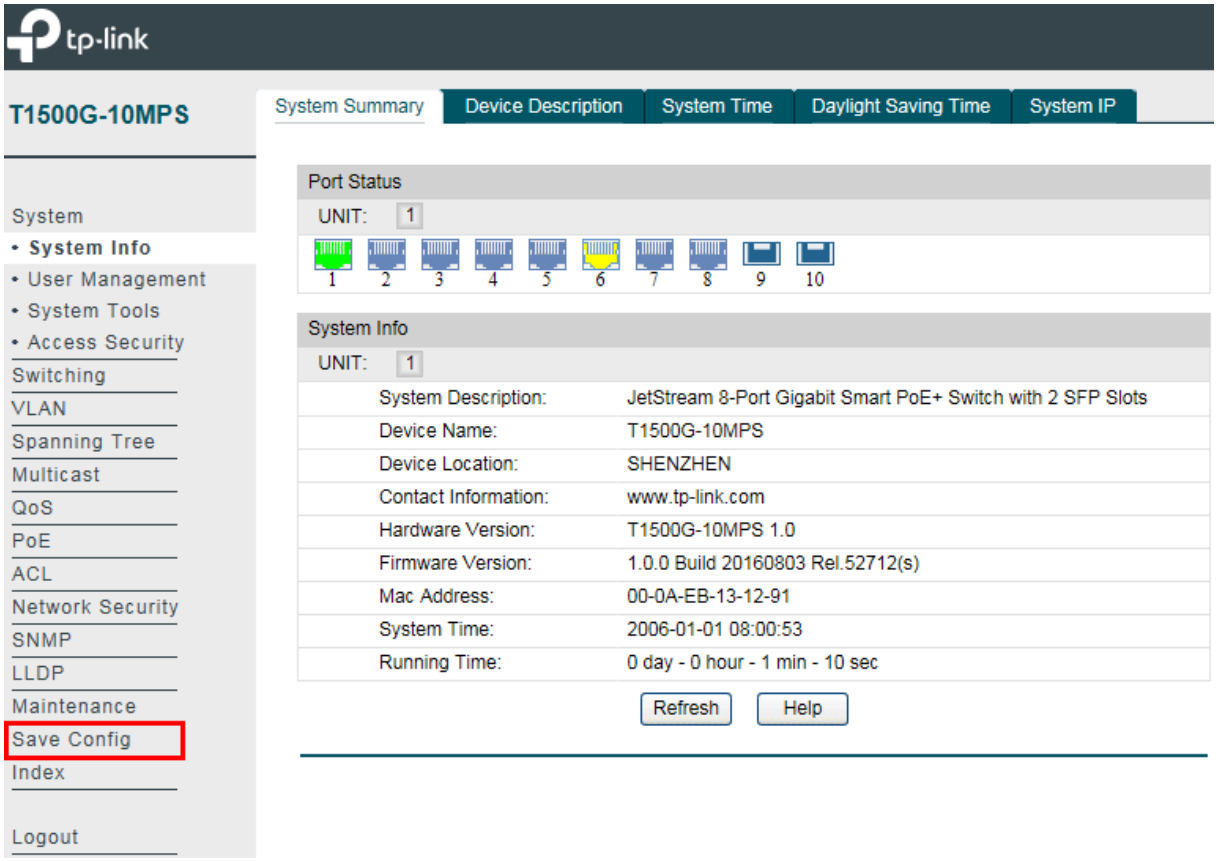


Figure 3-3 Main Setup-Menu

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** and **Access Security**.

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 **System IP** 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 8 10/100/1000Mbps RJ45 ports and 2 SFP ports of the switch.

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

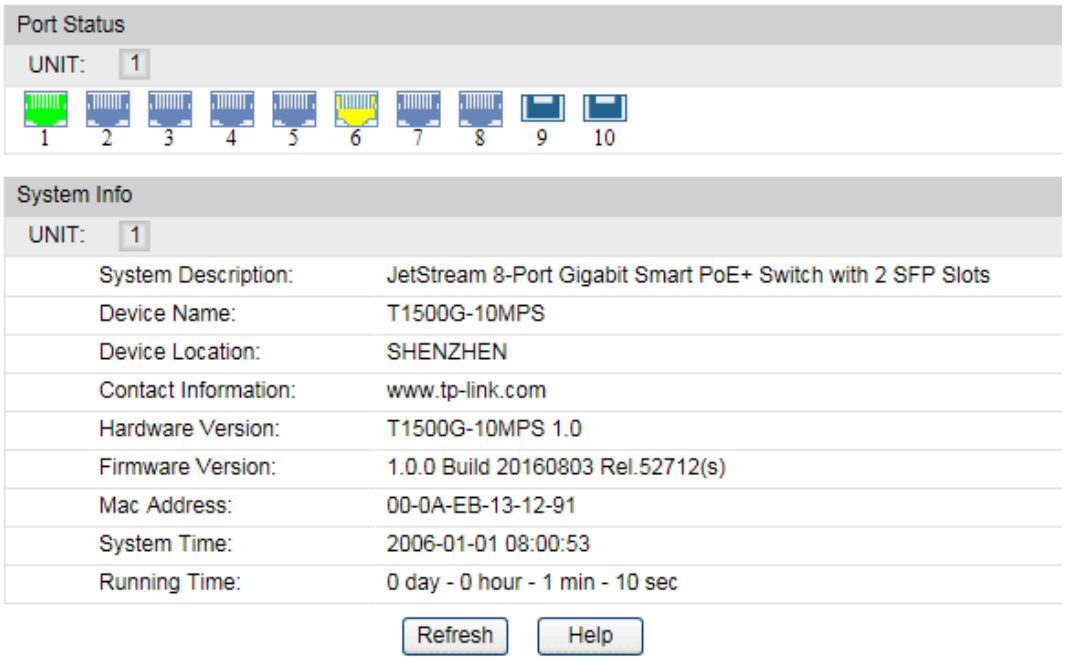


Figure 4-1 System Summary

➢ **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.

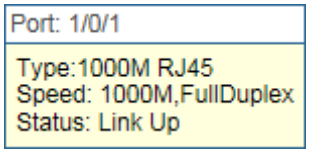


Figure 4-2 Port Information

- **Port Info**

Port:	Displays the port number of the switch.
Type:	Displays the type of the port.
Speed:	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.

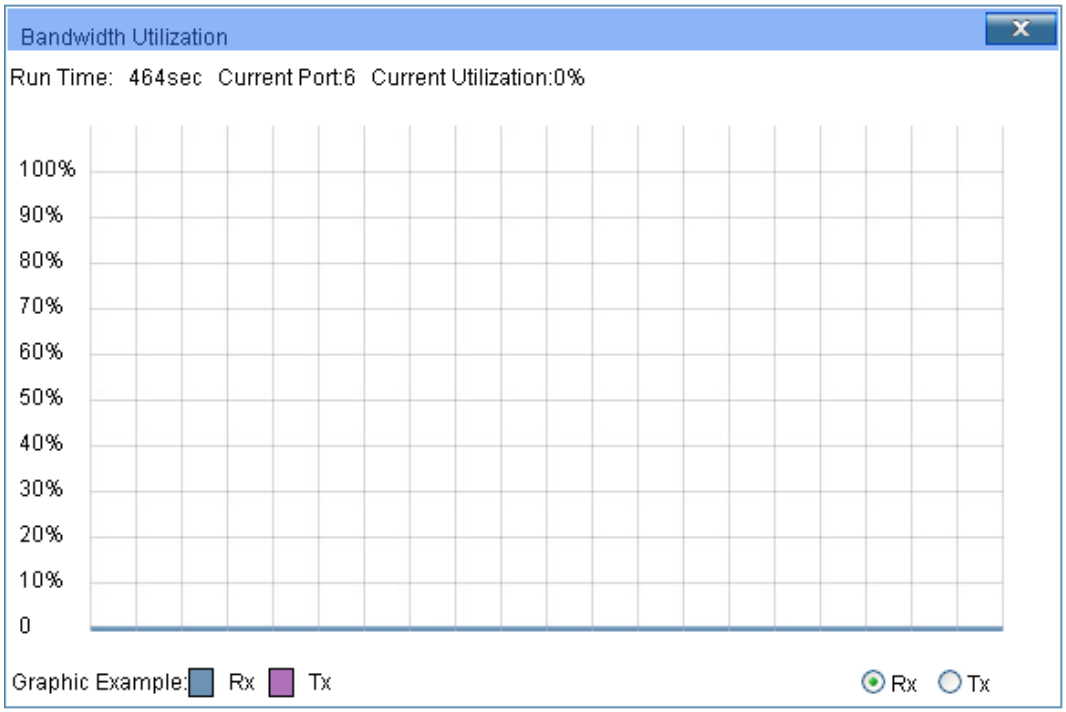


Figure 4-3 Bandwidth Utilization

- **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.

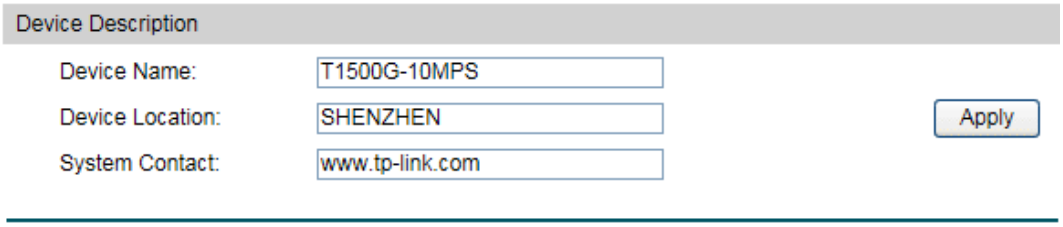


Figure 4-4 Device Description

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 or synchronize with PC's clock as the system time.

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

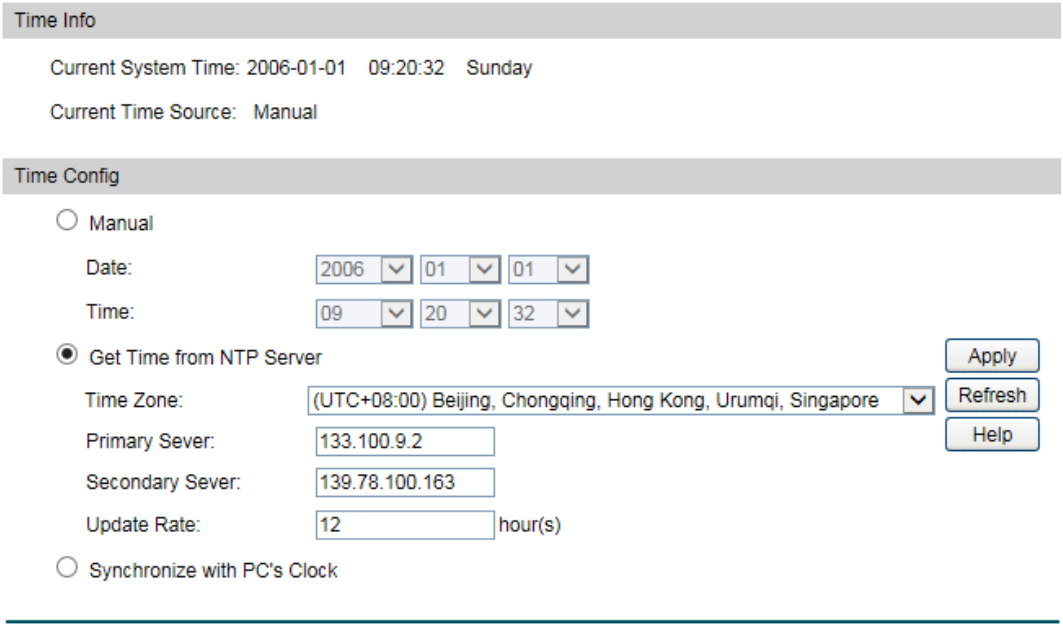


Figure 4-5 System Time

The following entries are displayed on this screen:

➢ **Time Info**

Current System Date: 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.

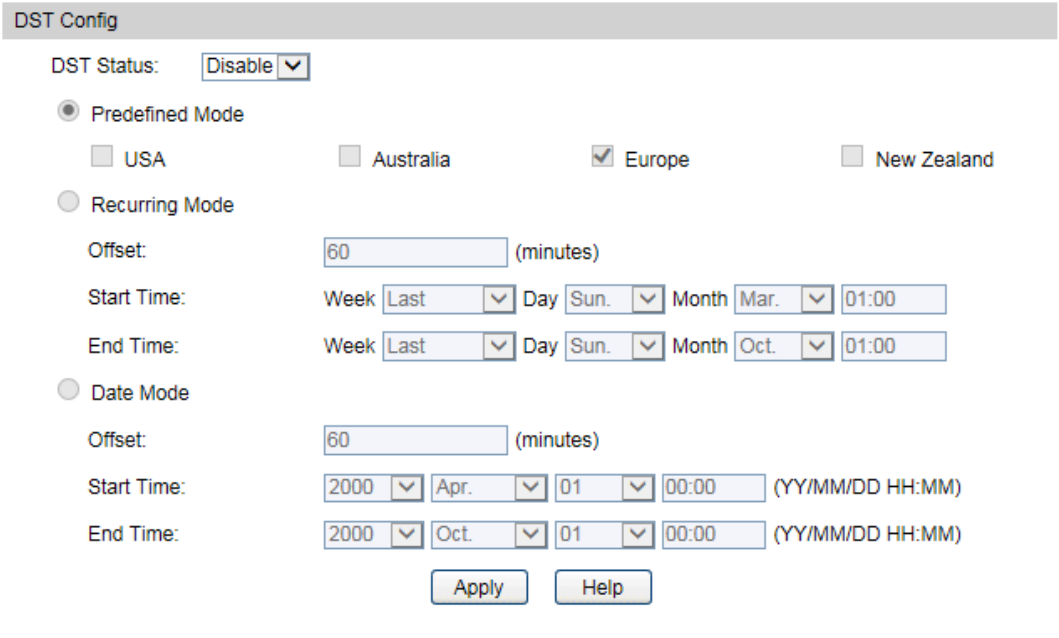


Figure 4-6 Daylight Saving Time

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 to First Sunday in November, 02:00.
- Australia: First Sunday in October, 02:00 to First Sunday in April, 03:00.
- Europe: Last Sunday in March, 01:00 to Last Sunday in October, 01:00.
- New Zealand: Last Sunday in September, 02:00 to 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 System IP

Each device in the network possesses a unique IP Address. You can log on to the Web management page to operate the switch using this IP Address. The switch supports three modes to obtain an IP address: Static IP, DHCP and BOOTP. The IP address obtained using a new mode will replace the original IP address. On this page you can configure the system IP of the switch.

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

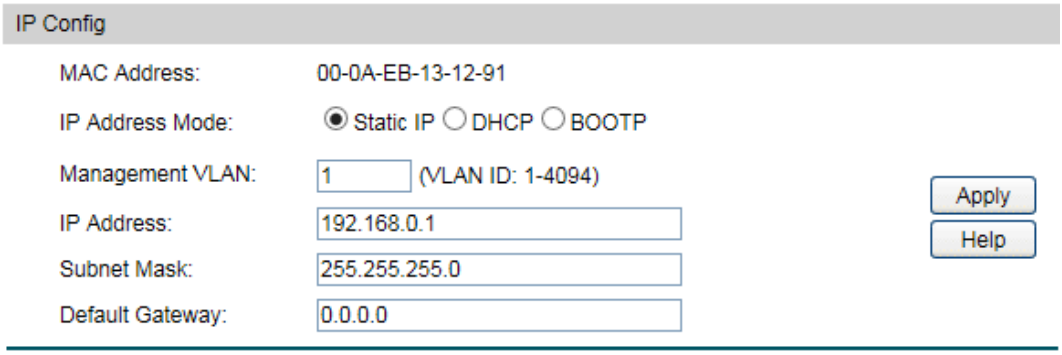


Figure 4-7 System IP

The following entries are displayed on this screen:

➢ **IP Config**

MAC Address: Displays MAC Address of the switch.

IP Address Mode: Select the mode to obtain IP Address for the switch.

- Static IP: When this option is selected, you should enter IP Address, Subnet Mask and Default Gateway manually.
- DHCP: When this option is selected, the switch will obtain network parameters from the DHCP Server.
- BOOTP: When this option is selected, the switch will obtain network parameters from the BOOTP Server.

Management VLAN: Enter the ID of management VLAN, the only VLAN through which you can get access to the switch. By default VLAN1 owning all the ports is the Management VLAN and you can access the switch via any port on the switch. However, if another VLAN is created and set to be the Management VLAN, you may have to reconnect the management station to a port that is a member of the Management VLAN.

IP Address: Enter the system IP of the switch. The default system IP is 192.168.0.1 and you can change it appropriate to your needs.

Subnet Mask: Enter the subnet mask of the switch.

Default Gateway: Enter the default gateway of the switch.

Note:

1. Changing the IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.
2. The switch only possesses one IP address. The IP address configured will replace the original IP address.
3. If the switch gets the IP address from DHCP server, you can see the configuration of the switch in the DHCP server; if DHCP option is selected but no DHCP server exists in the network, a few minutes later, the switch will restore the setting to the default.

4. If DHCP or BOOTP option is selected, the switch will get network parameters dynamically from the Internet, which means that IP address, subnet mask and default gateway cannot be configured.
5. By default, the IP address is 192.168.0.1.

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.

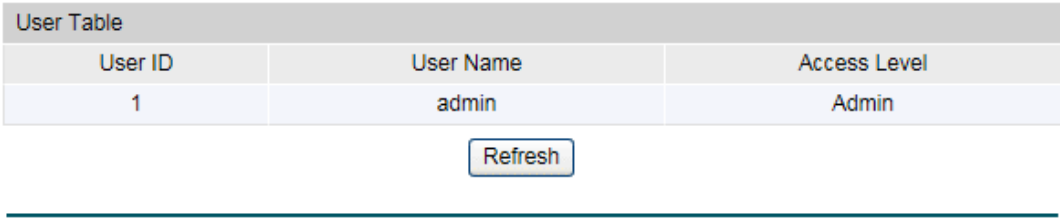


Figure 4-8 User Table

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.

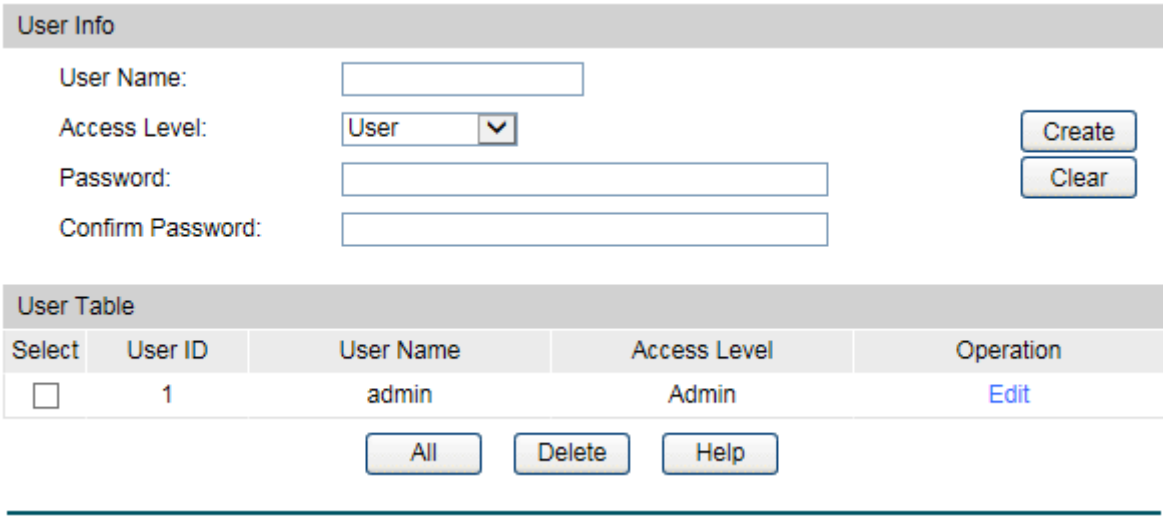


Figure 4-9 User Config

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, Name and 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 **Modify** button to make the modification effective. Access level and user status 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** 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.

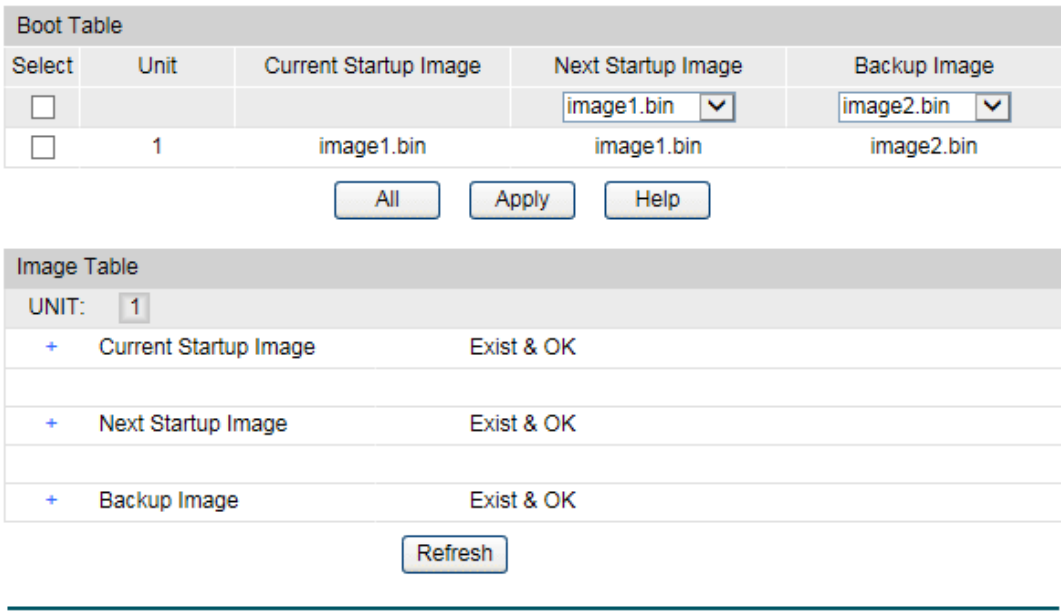


Figure 4-10 Boot Config

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.

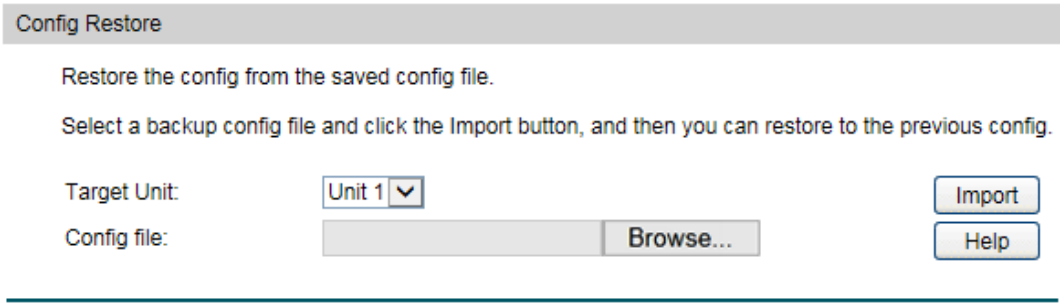


Figure 4-11 Config Restore

The following entries are displayed on this screen:

- **Config Restore**

Restore Config: 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. To avoid any damage, please don't power down the switch while being restored.
3. After being restored, the current settings of the switch will be lost. 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.

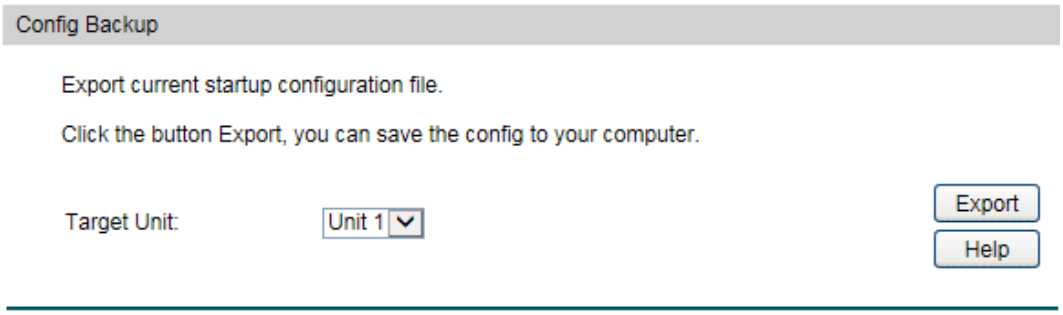


Figure 4-12 Config Backup

The following entries are displayed on this screen:

- **Config Backup**

Backup Config: Click the **Export** button to save the current configuration as a 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. Go to http://www.tp-link.com to download the updated firmware.

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

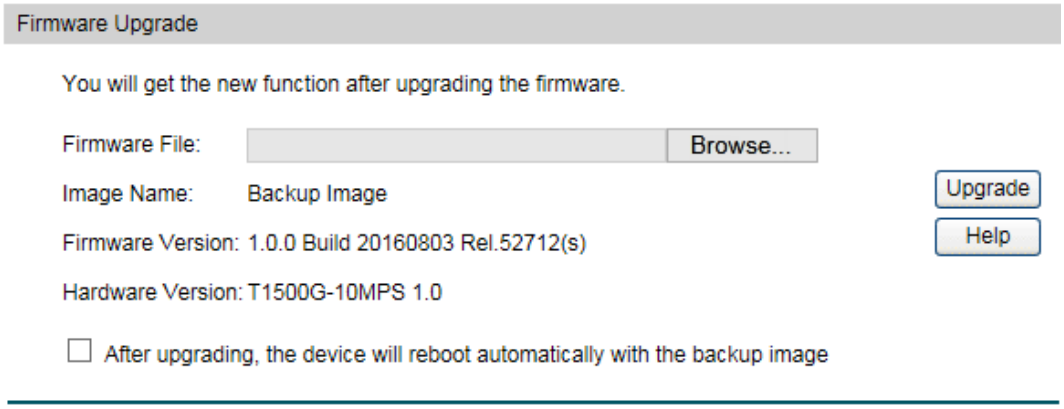


Figure 4-13 Firmware Upgrade

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. Don't interrupt the upgrade.
2. Please select the proper software version matching with your hardware to upgrade.
3. To avoid damage, please don't turn off the device while upgrading.
4. After upgrading, the device will reboot automatically.
5. You are suggested to backup the configuration before 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.

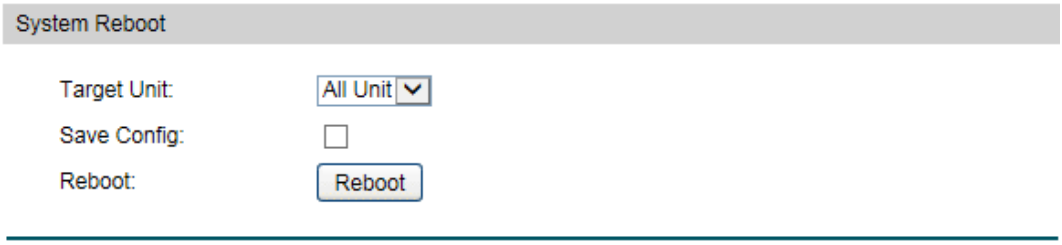


Figure 4-14 System Reboot

Note:

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

4.3.6 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 4-15 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.

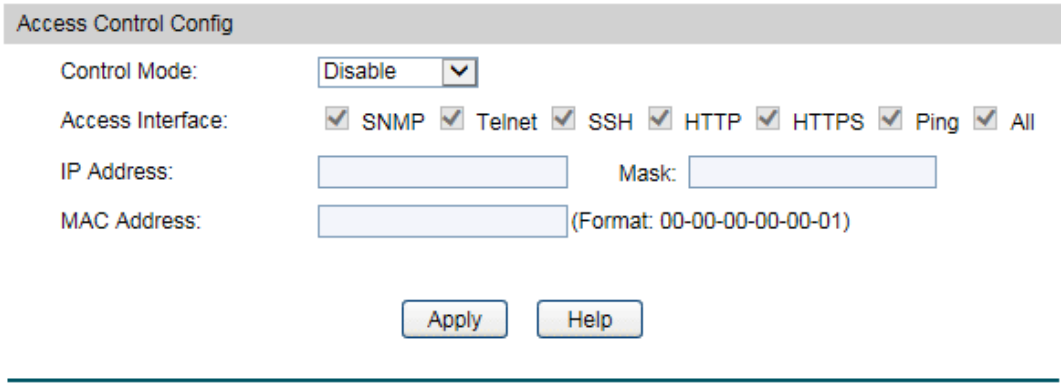


Figure 4-16 Access Control

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.

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.

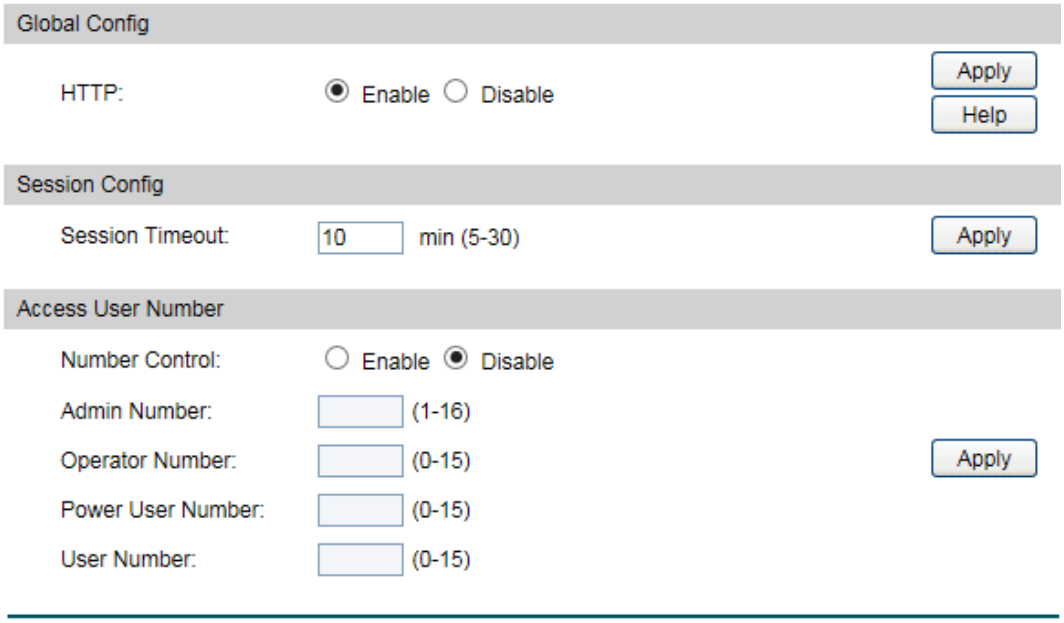


Figure 4-17 HTTP Config

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.

  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.

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.

On this page you can configure the HTTPS function.

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

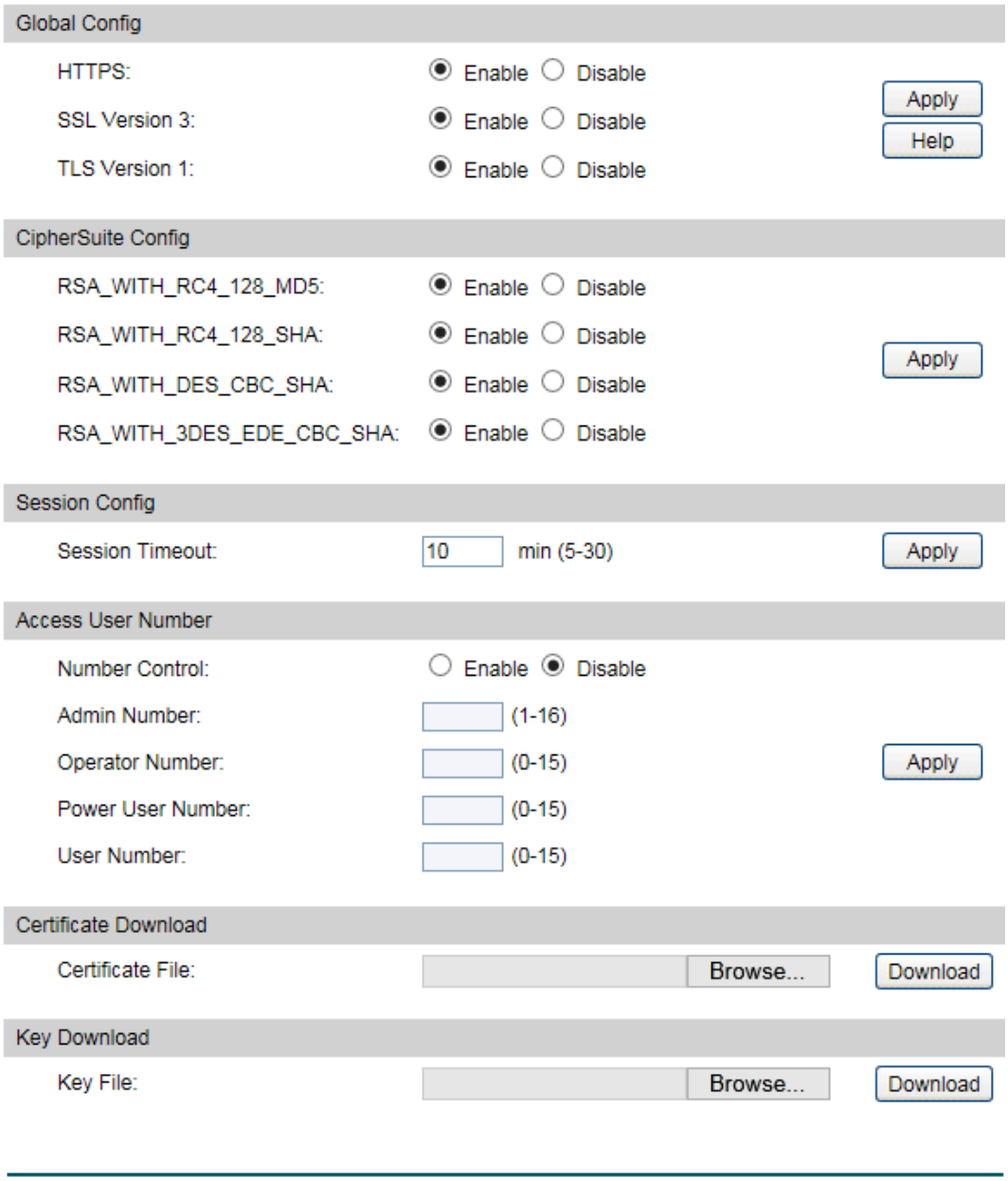


Figure 4-18 HTTPS Config

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.

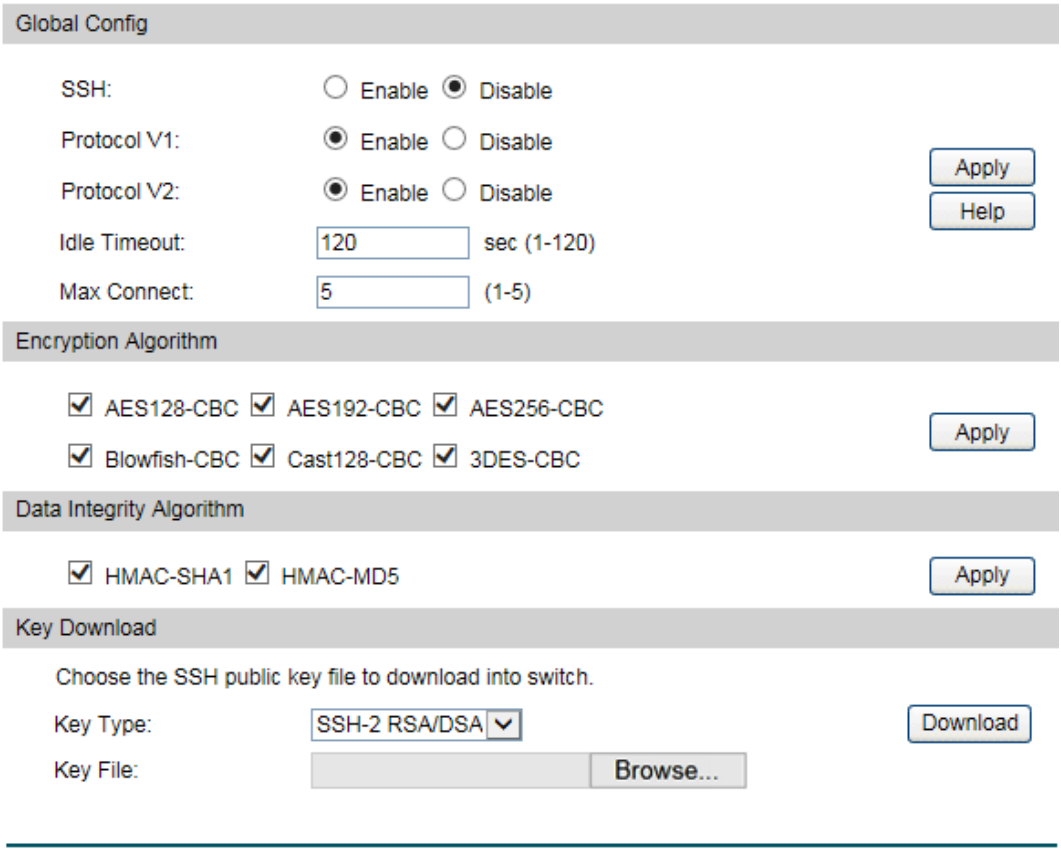


Figure 4-19 SSH Config

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.

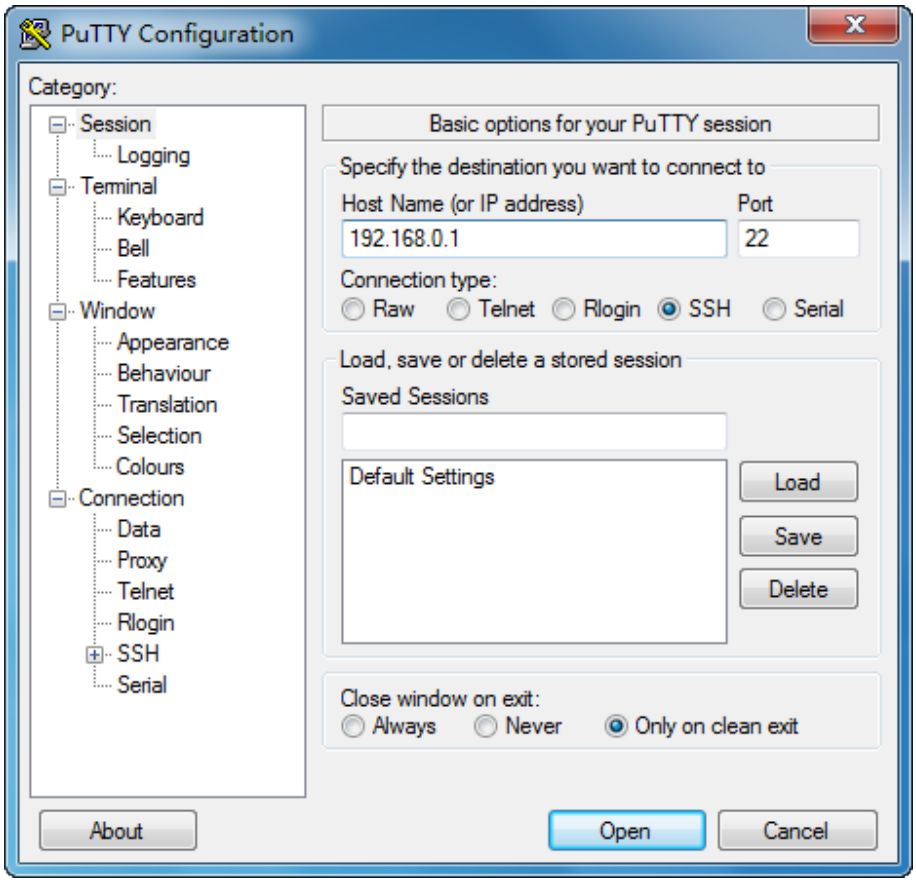
Application Example 1 for SSH:

➢ **Network Requirements**

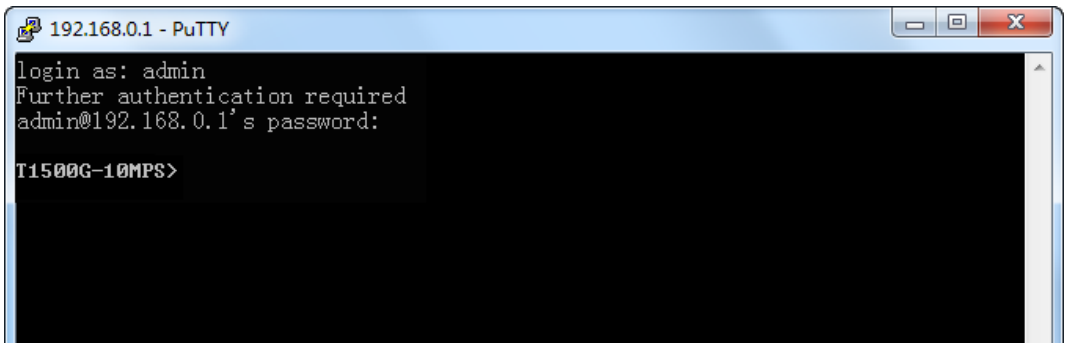
1. Log on to the switch via password authentication using SSH and the SSH function is enabled on the switch.
2. PuTTY client software is recommended.

➢ **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.



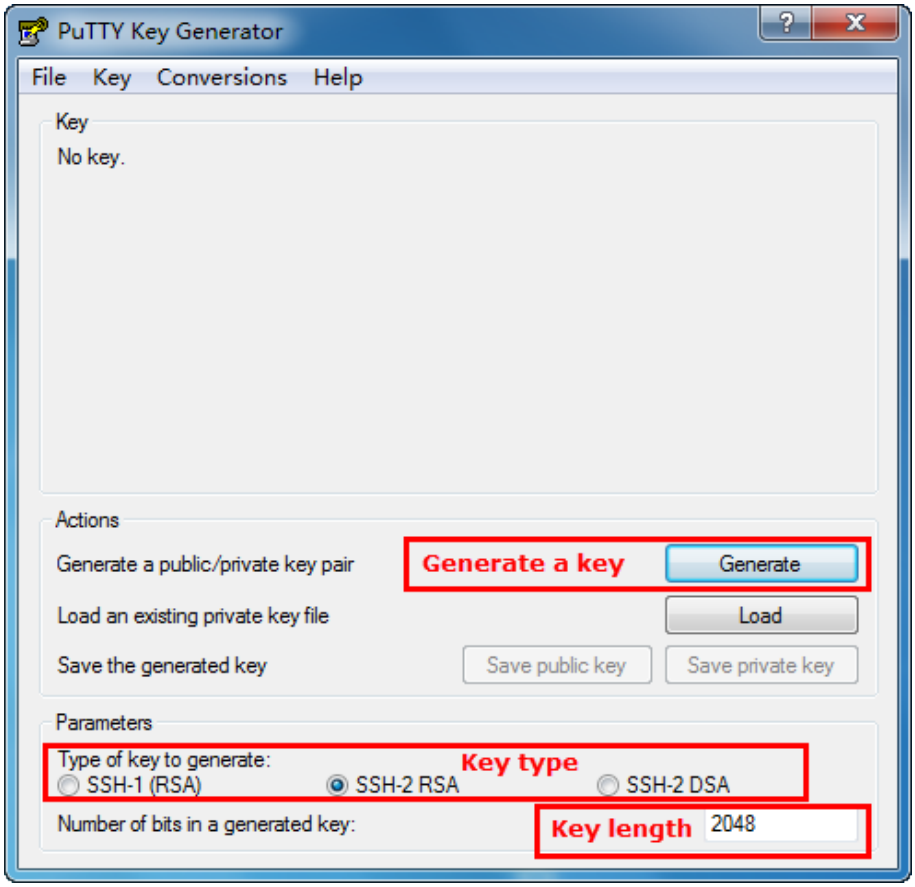
Application Example 2 for SSH:

➢ **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**

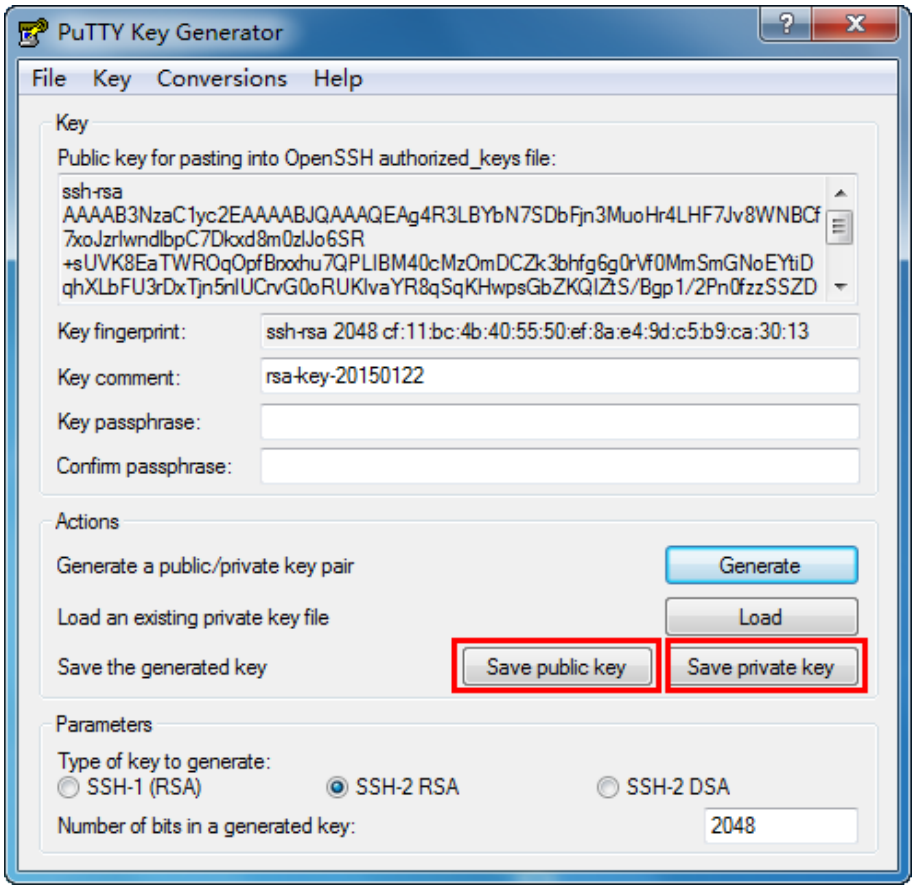
1. Select the key type and key length, and generate SSH key.



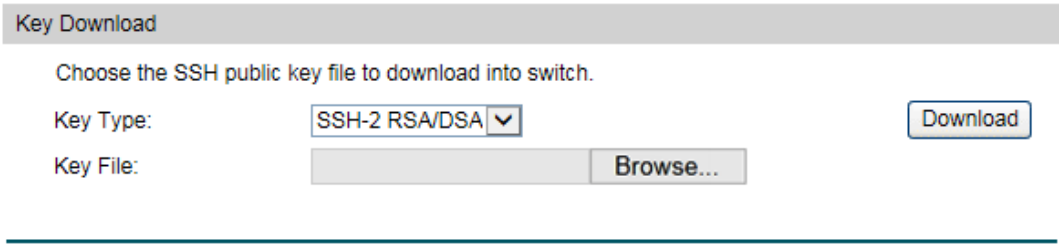
Note:

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.



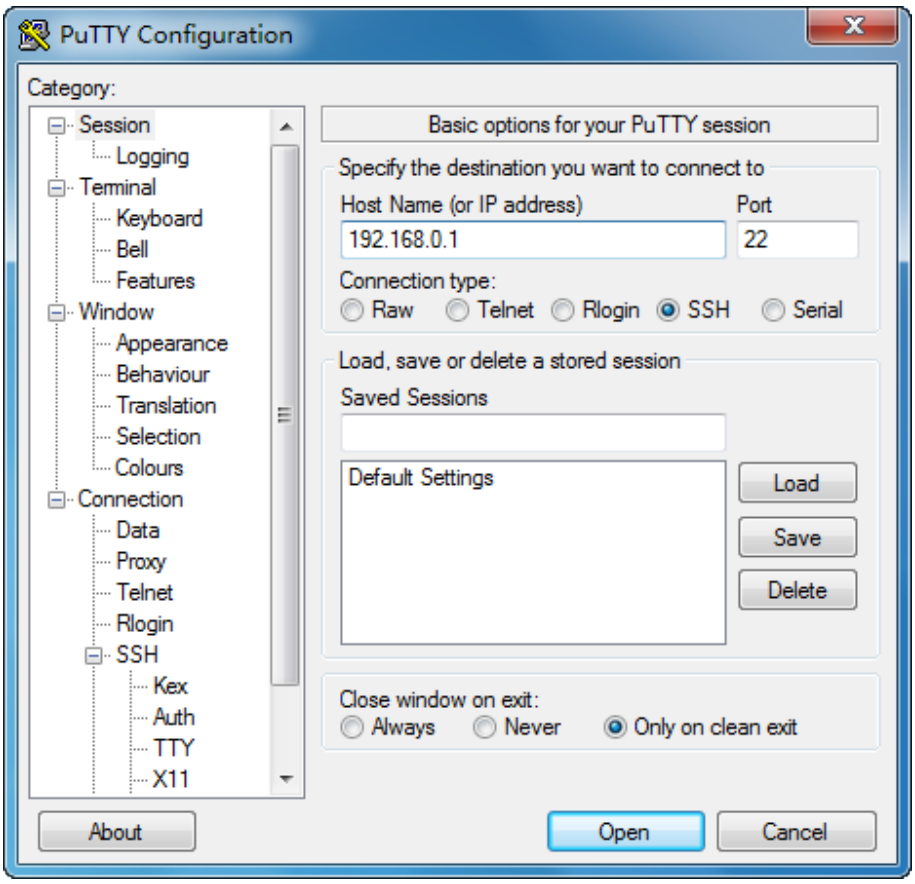
3. On the Web management page of the switch, download the public key file saved in the computer to the switch.



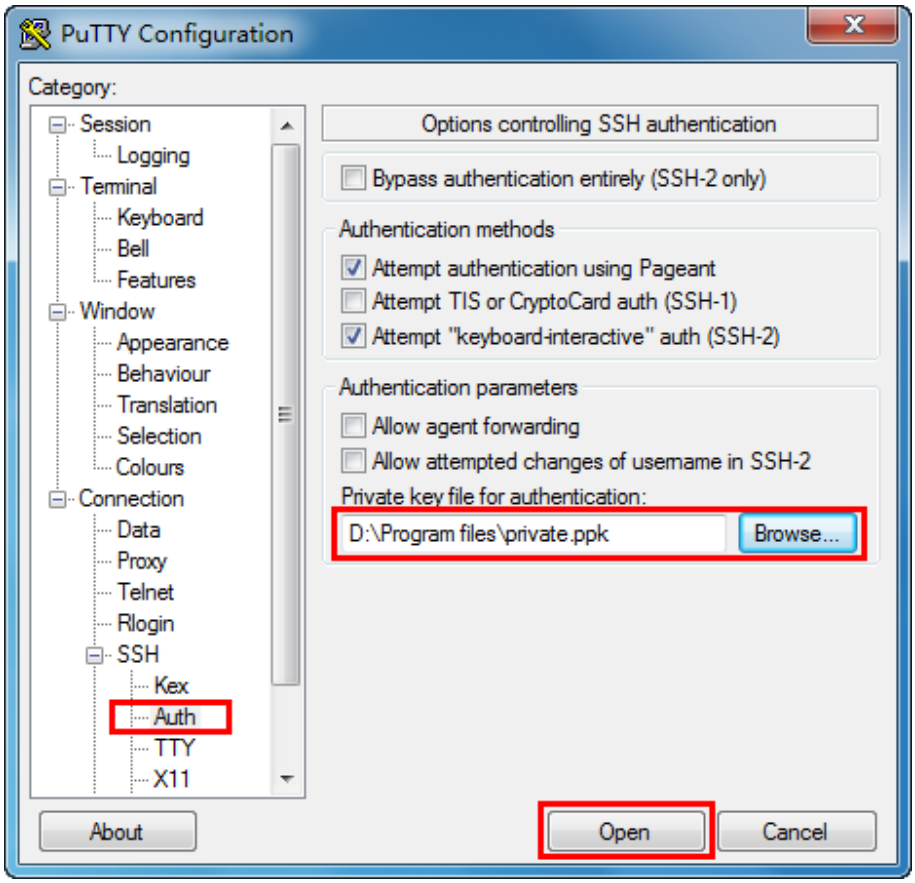
Note:

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

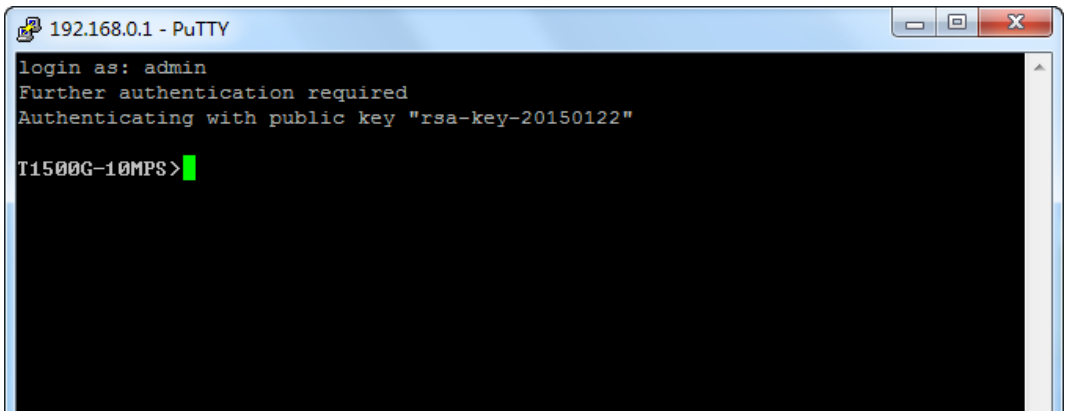
4. After the public key and private key are downloaded, please log on to the interface of PuTTY and enter the IP address for login.



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.

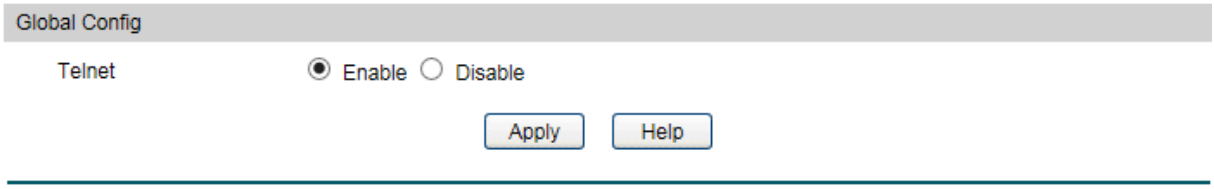


Figure 4-20 Telnet Config

The following entries are displayed on this screen:

- **Global Config**

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

Return to CONTENTS

Chapter 5 Switching

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

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.

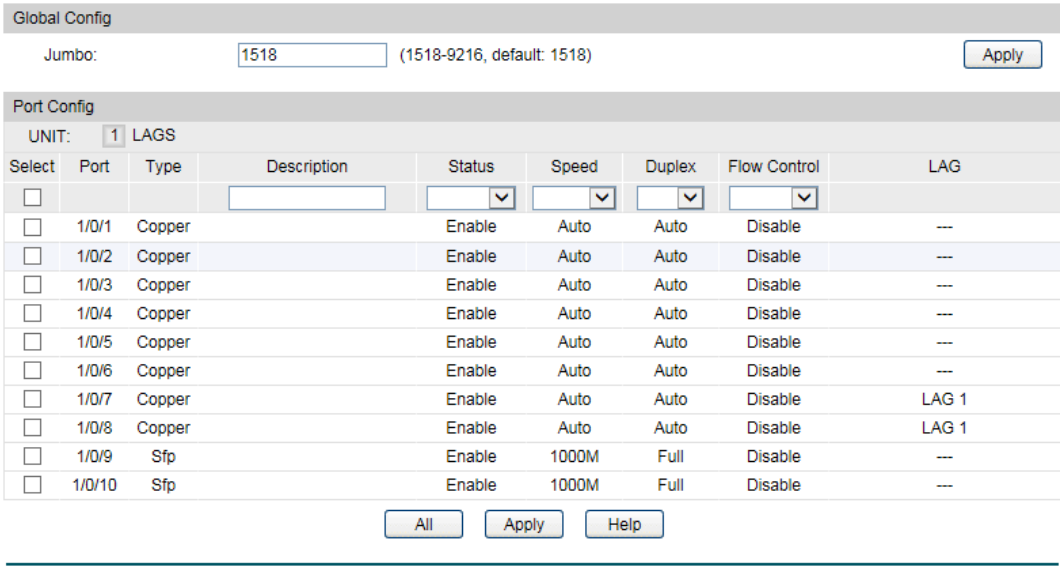


Figure 5-1 Port Config

The following entries are displayed on this screen:

- **Global Config**

  Jumbo: Specify the global jumbo size. The default maximum transmission unit (MTU) size is 1518 bytes.

- **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 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.
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 parameters of the port members in a LAG should be set as the same.
3. When using the SFP port with a 100M module or a gigabit module, you need to configure its corresponding **Speed and Duplex** mode. For 100M module, please select **100MFD** while select **1000MFD** for gigabit module. By default, the **Speed and Duplex** mode of SFP port is 1000MFD.

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.

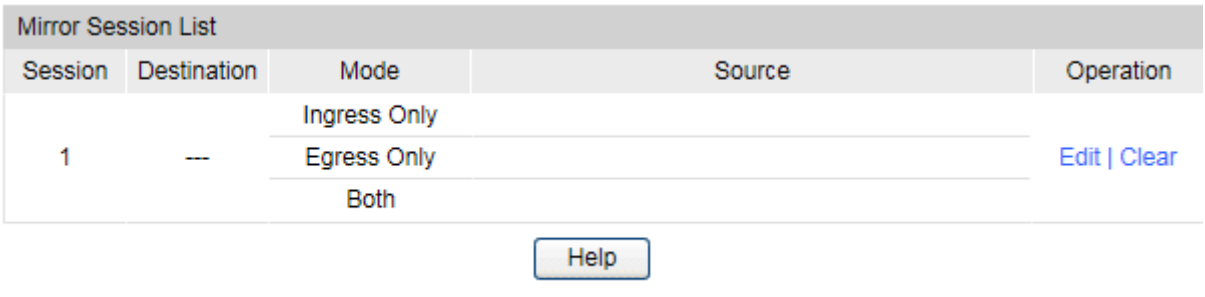


Figure 5-2 Mirror Group List

➢ **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.

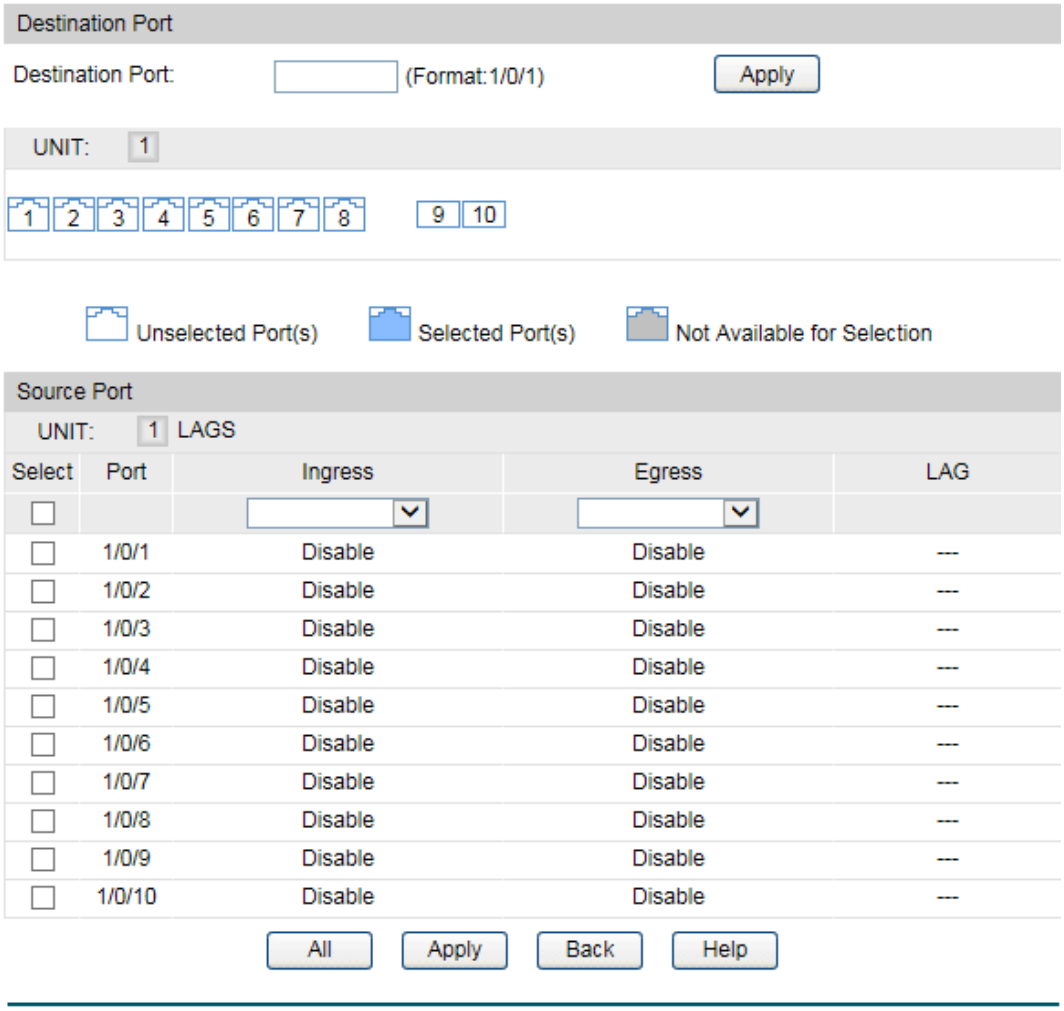


Figure 5-3 Port Mirror Config

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.

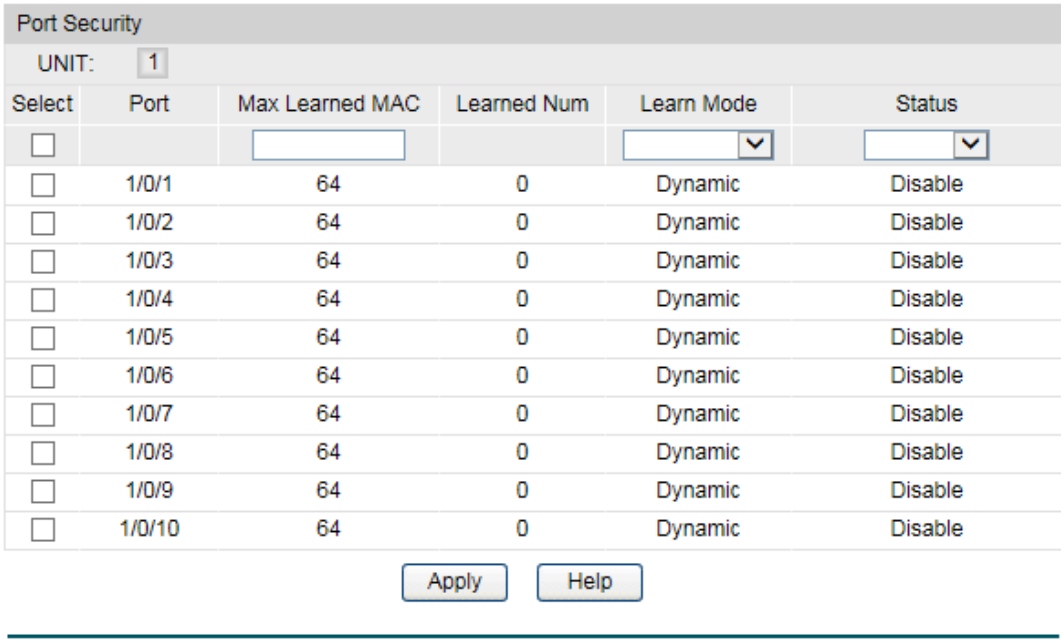


Figure 5-4 Port Security

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: Choose the mode that the switch adopts when the threshold limit on selected port is exceeded.

- **Drop:** Packets arrived on the port with new MAC addresses will be dropped when the threshold limit is

exceeded.

- **Forward:** Packets arrived on the port with new MAC addresses will be forwarded but the addresses will not be learned when the threshold limit is exceeded.
- **Disable**: The threshold is not valid.

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.

Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/1-10,LAG1-6
1/0/2	---	1/0/1-10,LAG1-6
1/0/3	---	1/0/1-10,LAG1-6
1/0/4	---	1/0/1-10,LAG1-6
1/0/5	---	1/0/1-10,LAG1-6
1/0/6	---	1/0/1-10,LAG1-6
1/0/7	---	1/0/1-10,LAG1-6
1/0/8	---	1/0/1-10,LAG1-6
1/0/9	---	1/0/1-10,LAG1-6
1/0/10	---	1/0/1-10,LAG1-6

Edit Help

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.

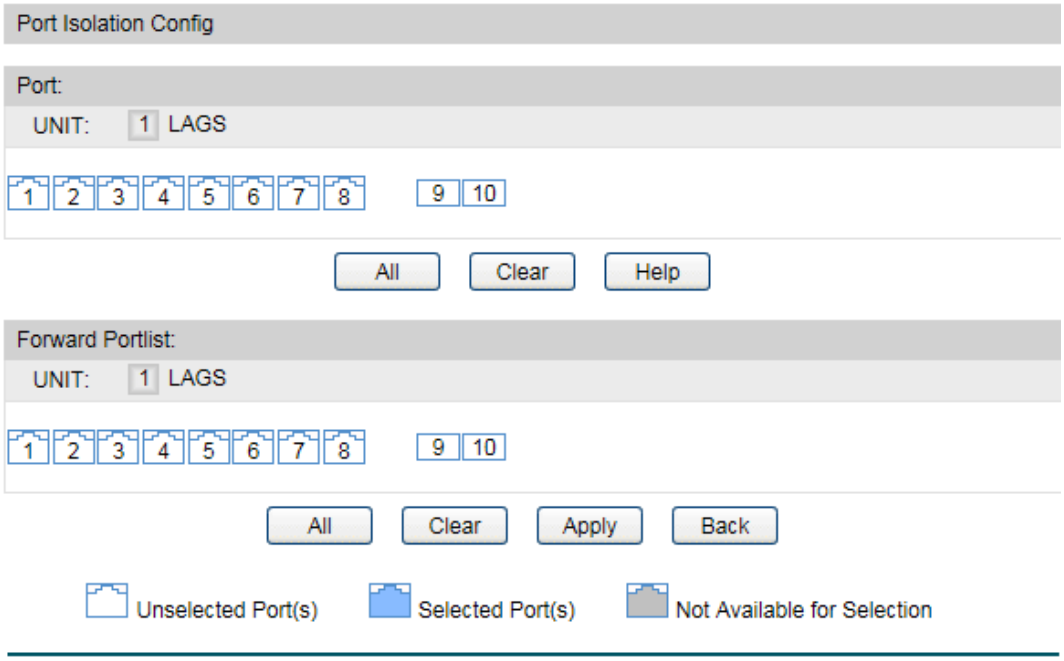


Figure 5-6 Port Isolation Config

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.

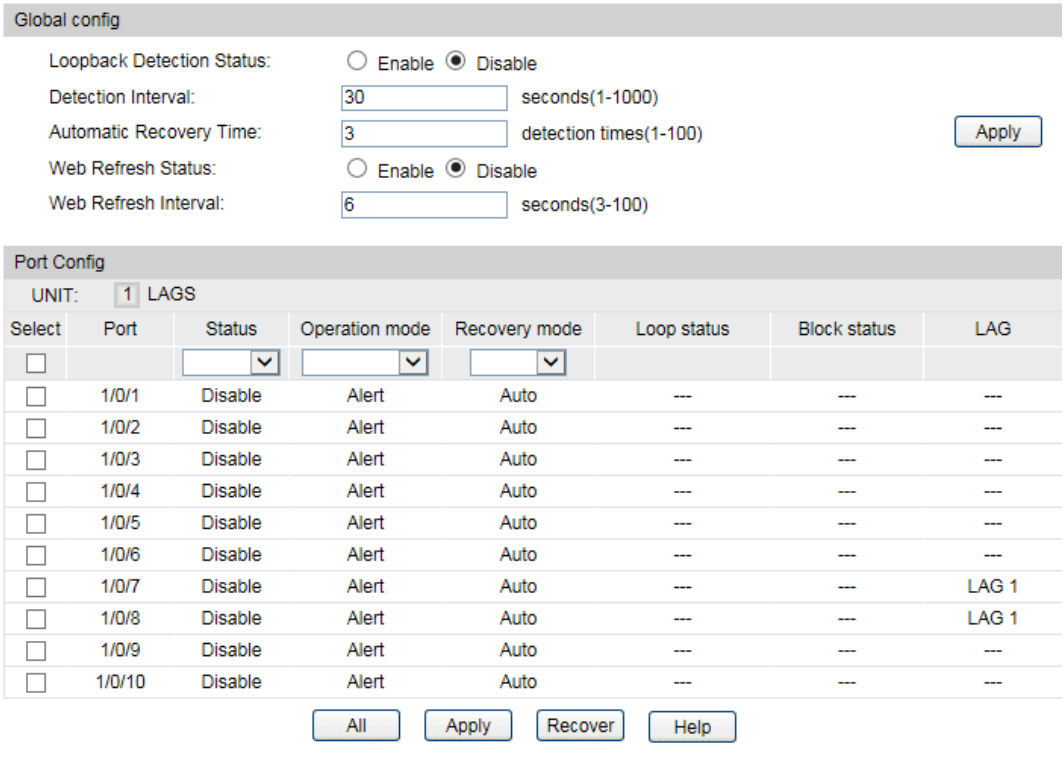


Figure 5-7 Loopback Detection Config

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**

UNIT:1/LAGS:	Click **1** to configure the physical ports. Click **LAGS** to configure the link aggregation groups.
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. The further explains are following:

- 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 should be the same.
- 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.

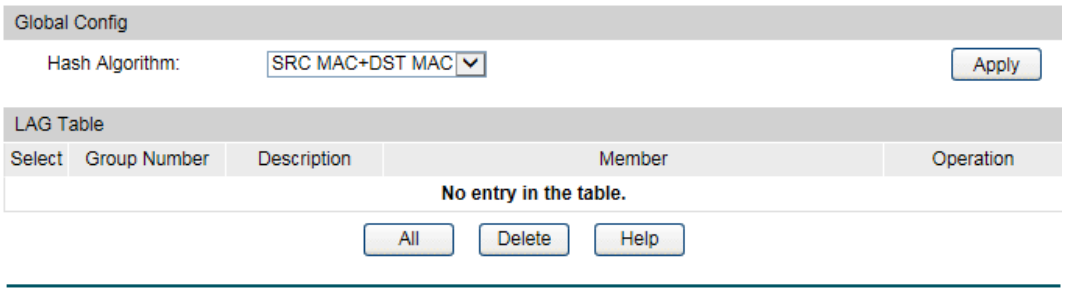


Figure 5-8 LAG Table

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.

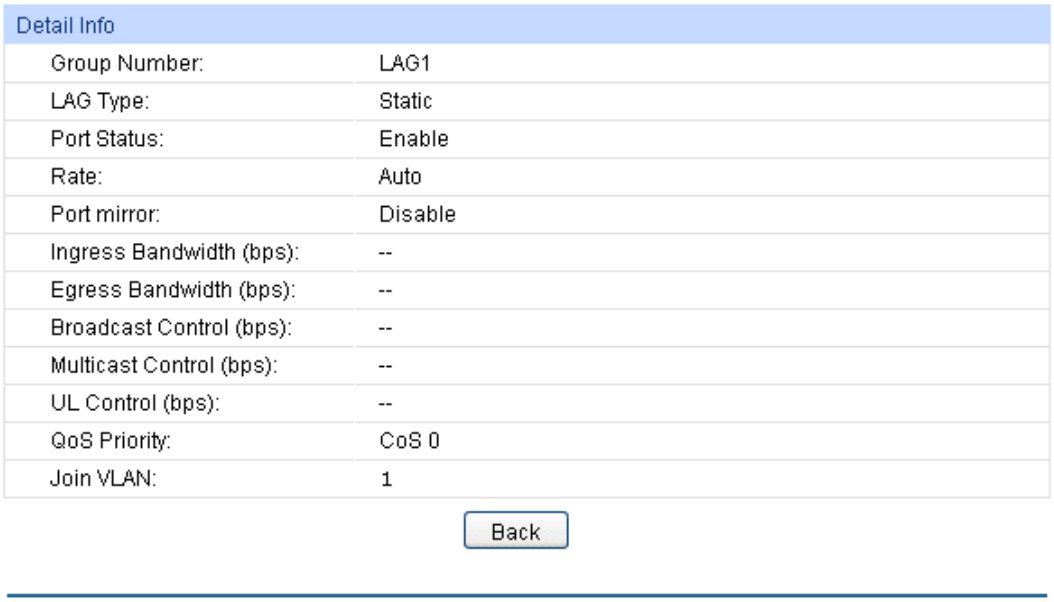


Figure 5-9 Detailed Information

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.

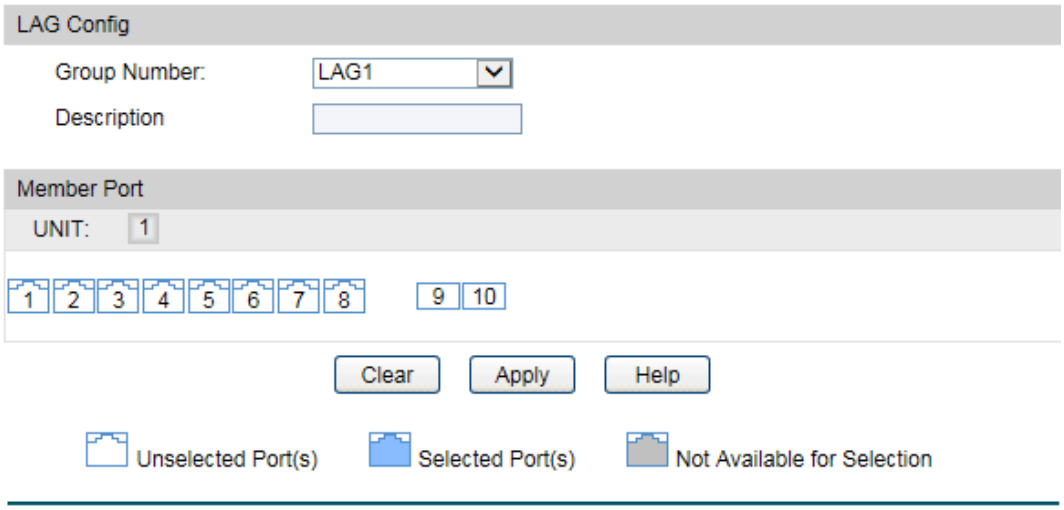


Figure 5-10 Manually Config

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.

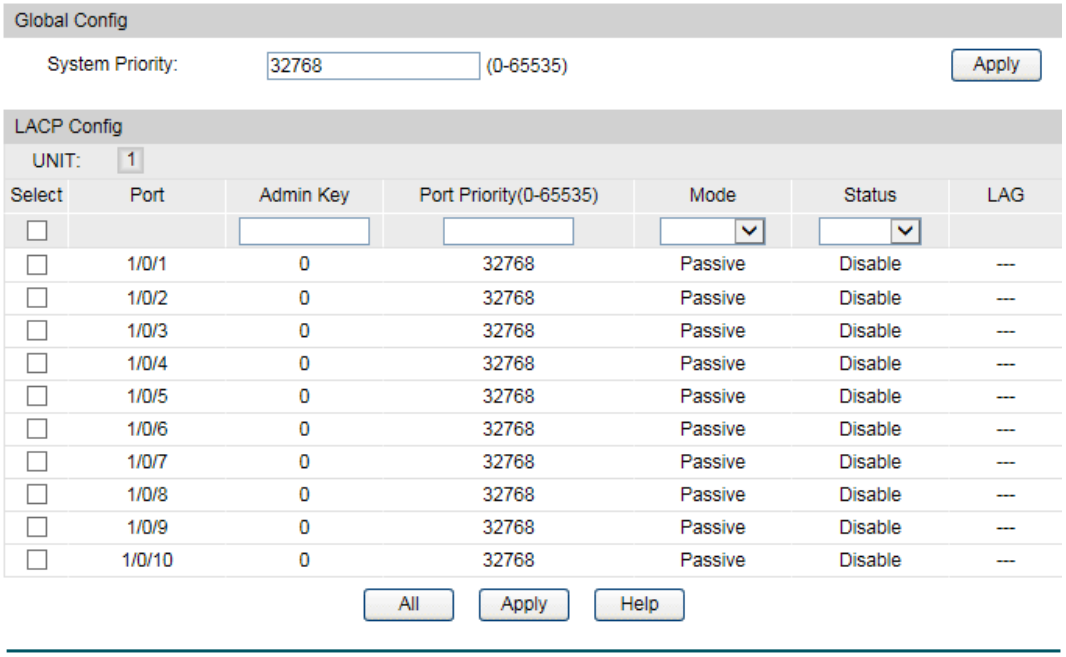


Figure 5-11 LACP Config

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.

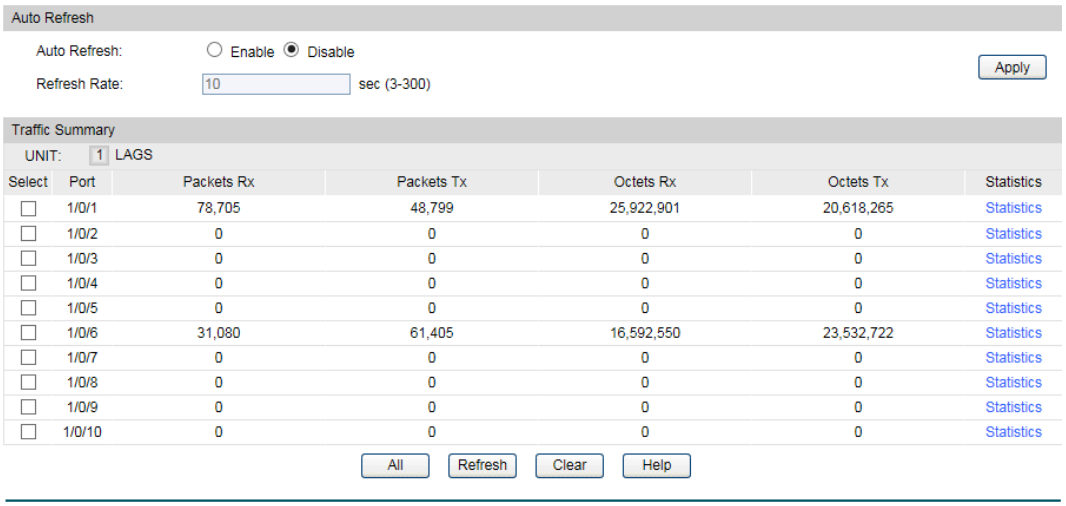


Figure 5-12 Traffic Summary

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.

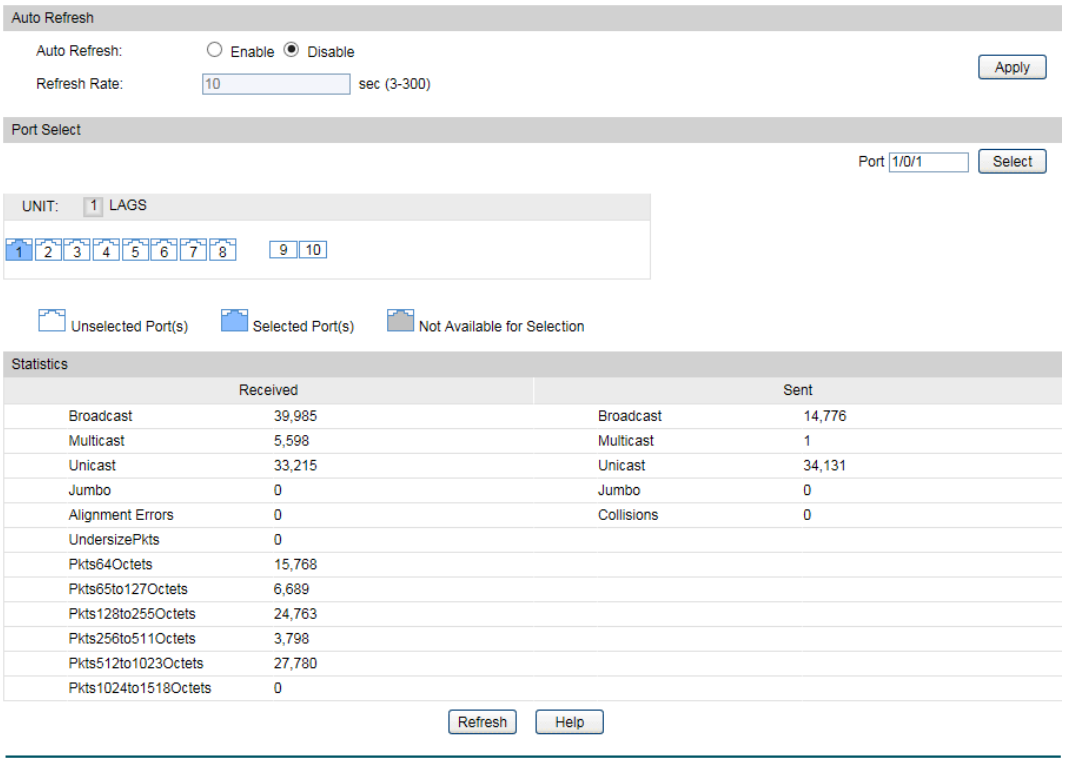


Figure 5-13 Traffic Statistics

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: Enter a port number and click the **Select** button or select the port to view the traffic statistics of the corresponding port.

- **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.

Alignment Errors:	For T1500G-10MPS//: Displays the number of the received packets that have a bad Frame Check Sequence (FCS) with a non-integral octet (Alignment Error) and have a bad FCS with an integral octet (CRC Error). The length of the packet is between 64 bytes and 1518 bytes. For : Displays the number of the received packets that have a bad Frame Check Sequence (FCS) . The length of the packet is from 64 bytes to maximal bytes of the jumbo frame(usually 10240 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 the 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 Address Table	Manually configuring	No	Yes	The bound MAC address 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.

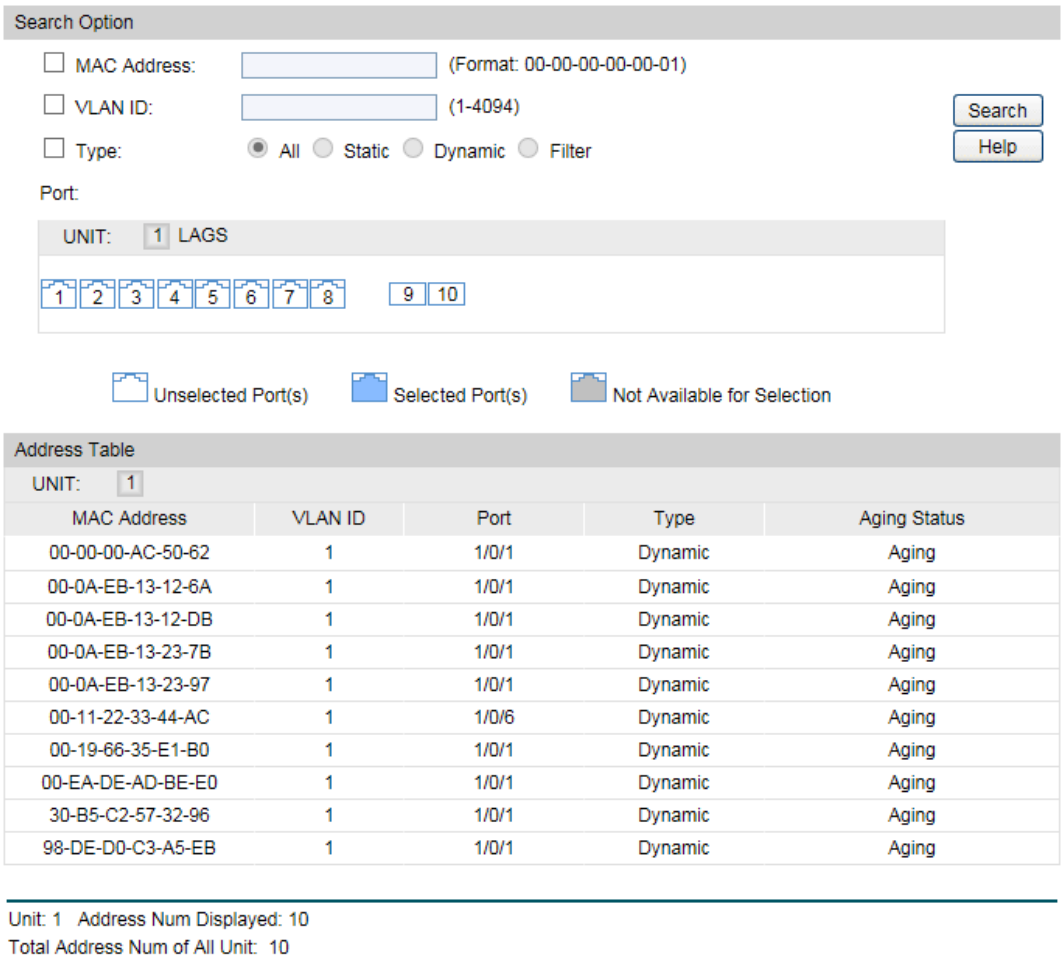


Figure 5-14 Address Table

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.

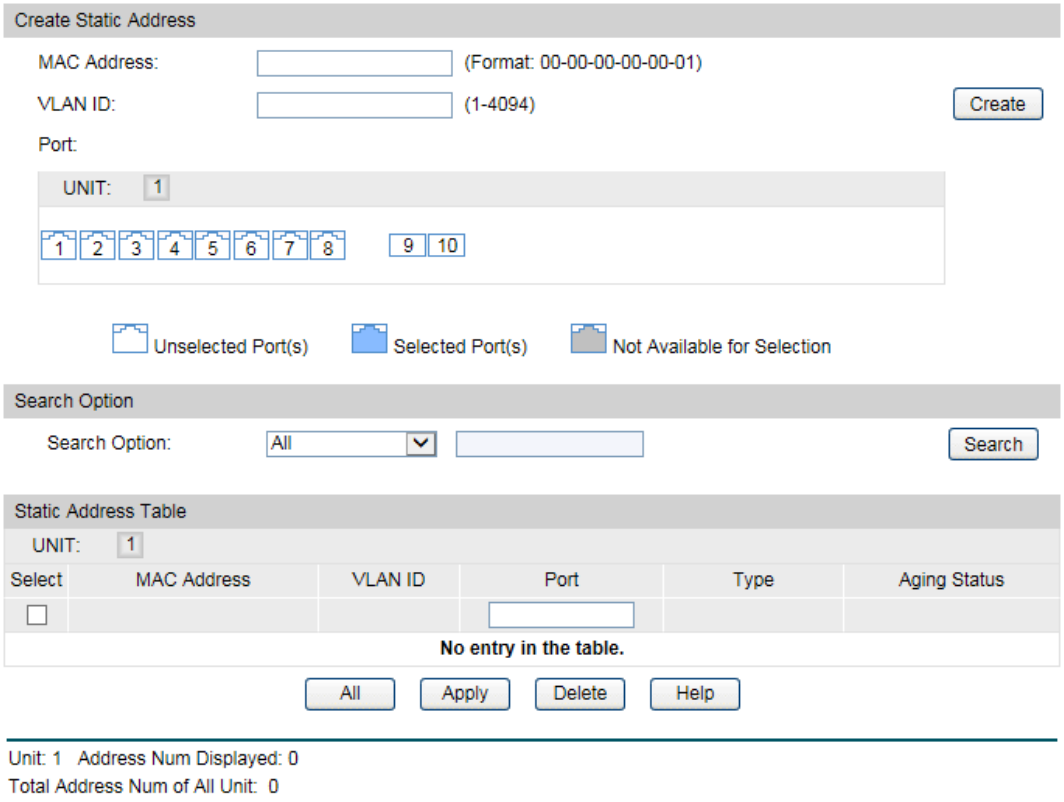


Figure 5-15 Static Address

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.

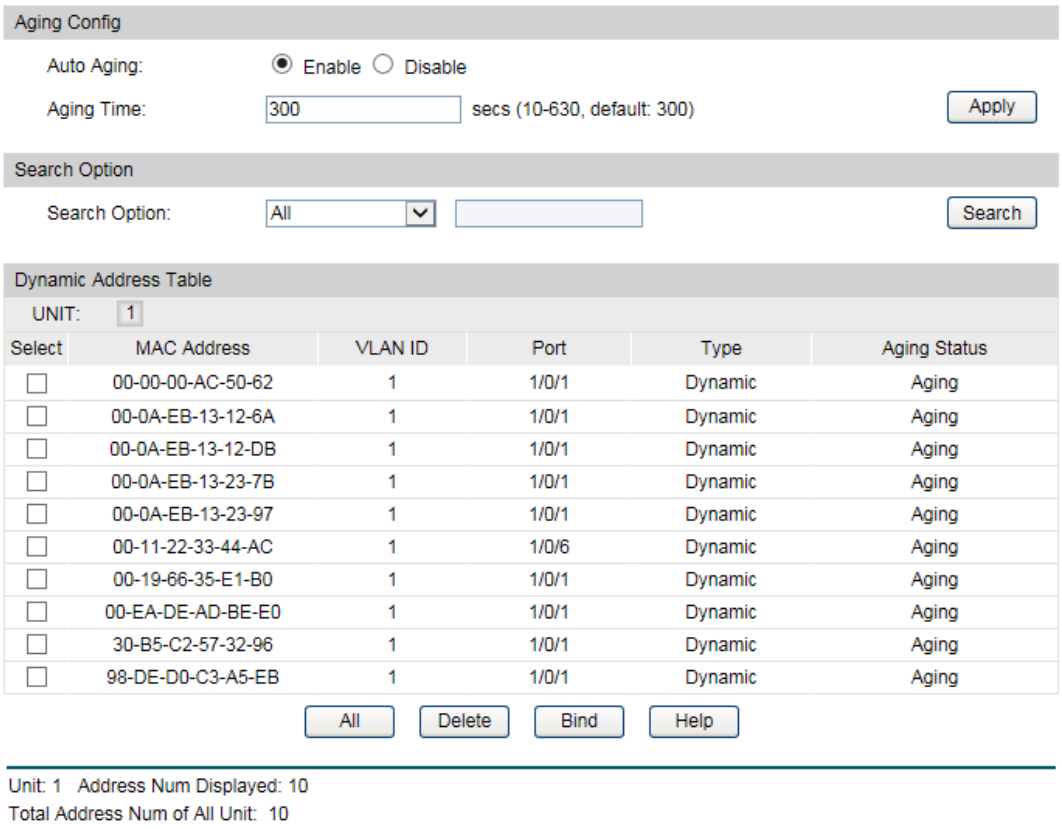


Figure 5-16 Dynamic Address

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.

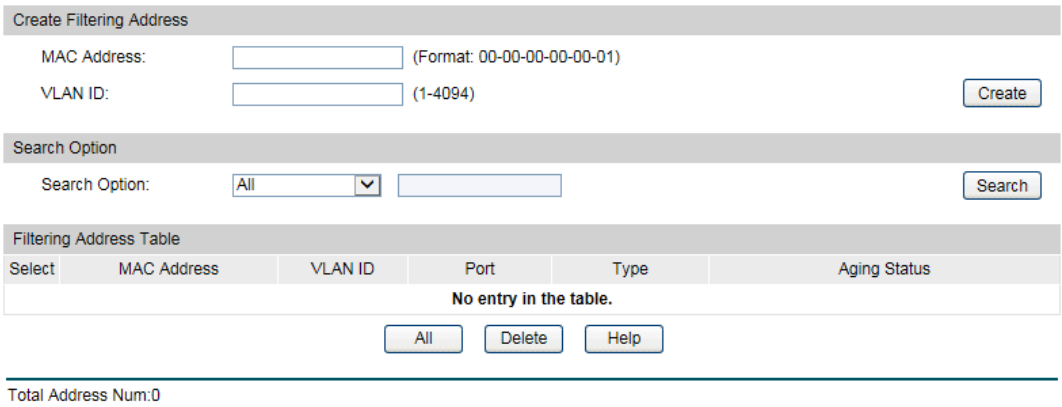


Figure 5-17 Filtering Address

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.

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.

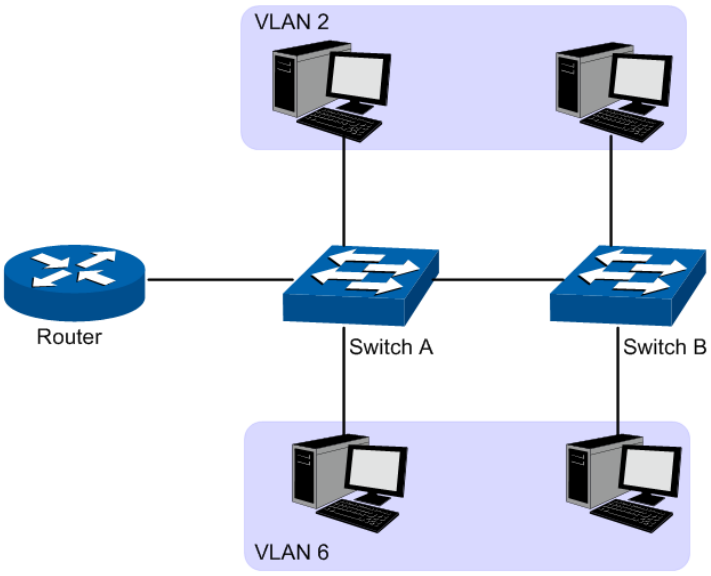


Figure 6-1 VLAN implementation

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.

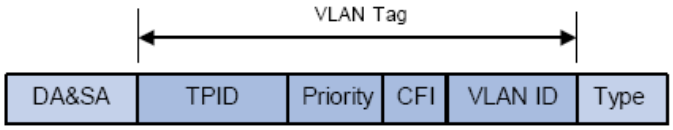


Figure 6-1 Format of VLAN Tag

(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.

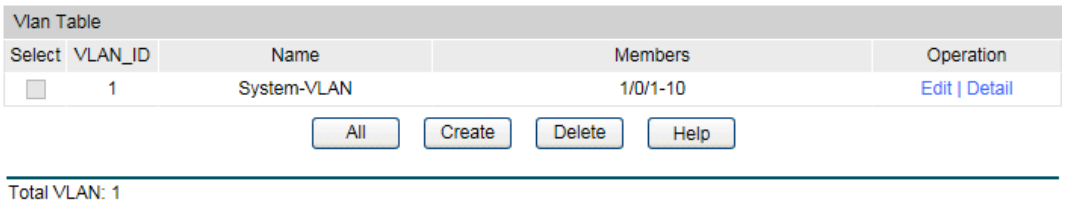


Figure 6-2 VLAN Table

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.

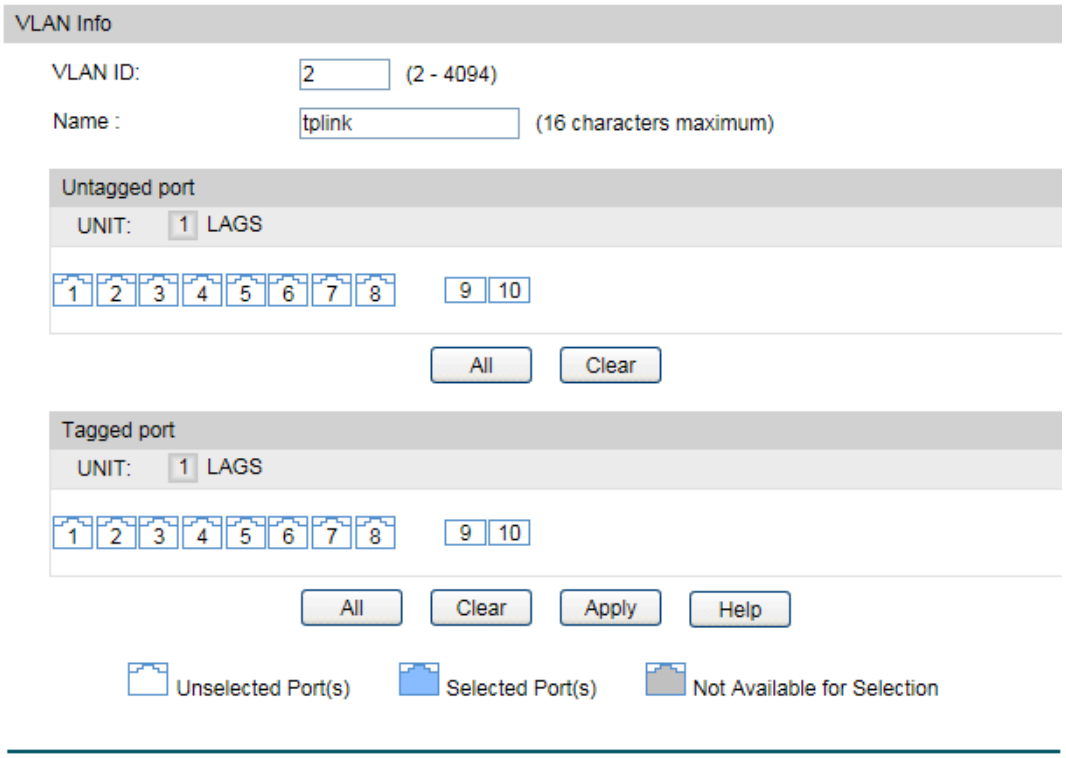


Figure 6-3 VLAN Info

➢ **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.

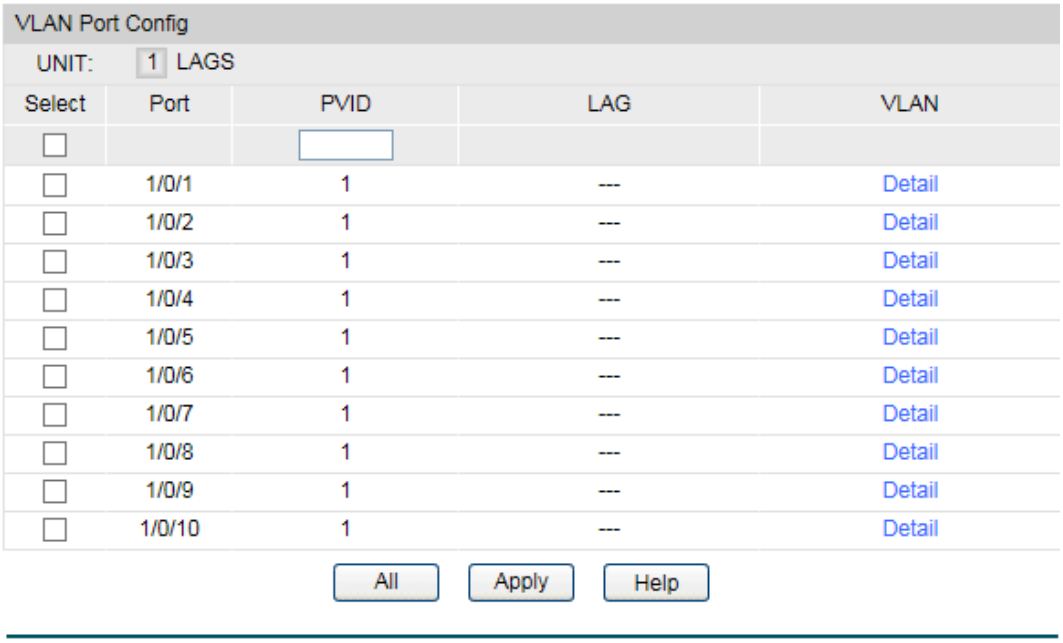


Figure 6-4 Port Config

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.

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.

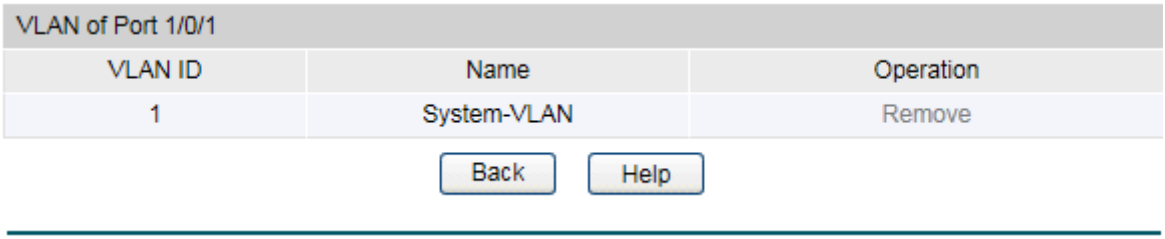


Figure 6-5 View the Current VLAN of Port

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:

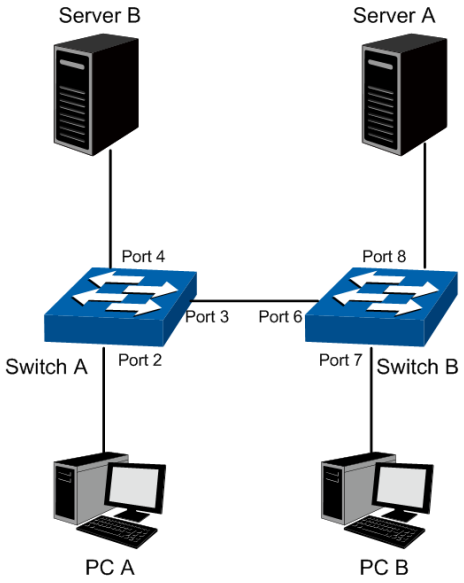
Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected device.
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its 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	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Untagged Port 2 and Tagged Port 3.
2	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Tagged Port 3 and Untagged Port 4.

- Configure switch B

Step	Operation	Description
1	Create VLAN10	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 10, owning Tagged Port 6 and Untagged Port 8.
2	Create VLAN20	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, create a VLAN with its VLAN ID as 20, owning Tagged Port 6 and Untagged Port 7.

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 to 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 to 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.

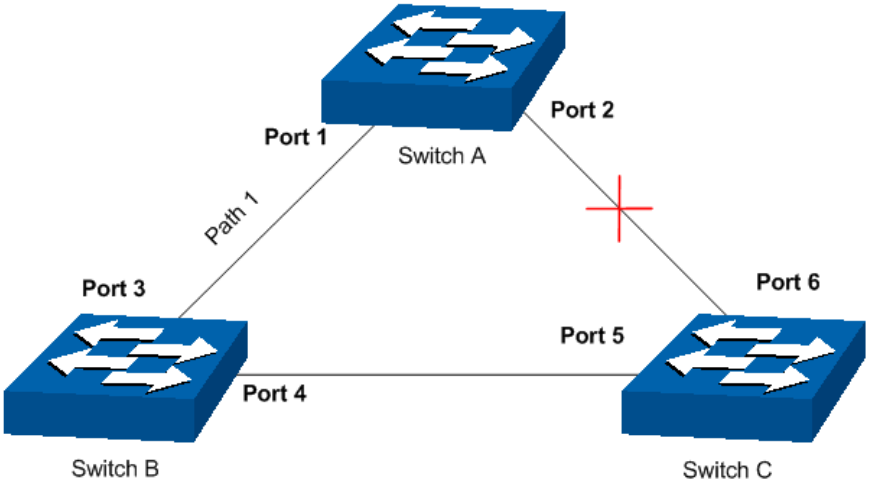


Figure 7-1 Basic STP diagram

➢ **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.

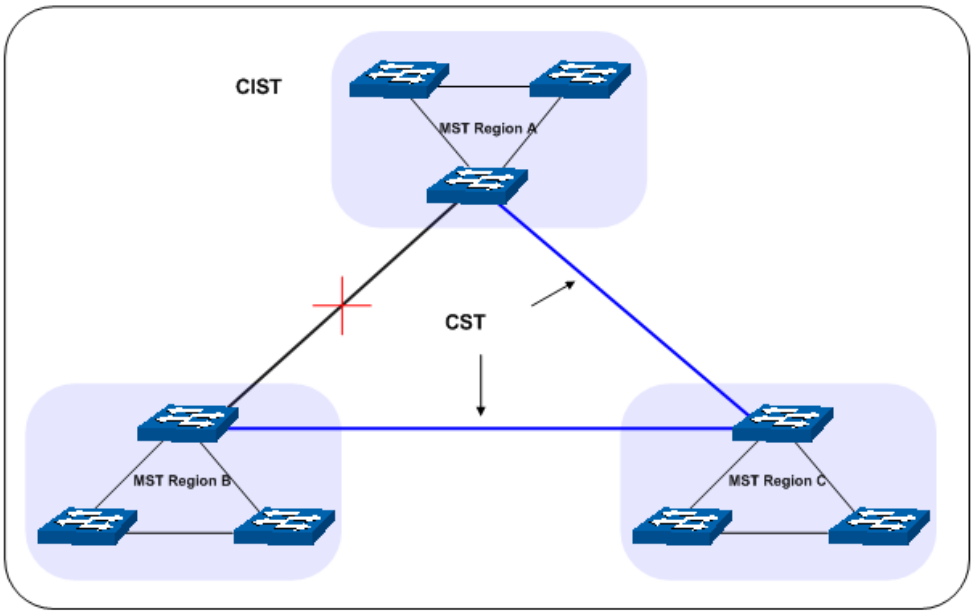


Figure 7-2 Basic MSTP diagram

➢ **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.

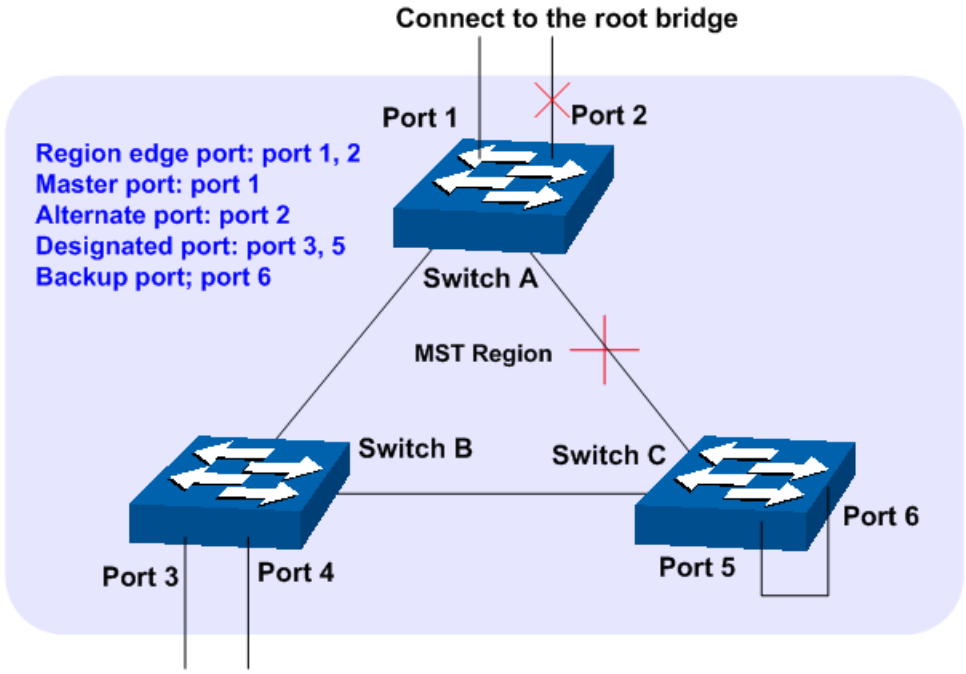


Figure 7-3 Port roles

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.

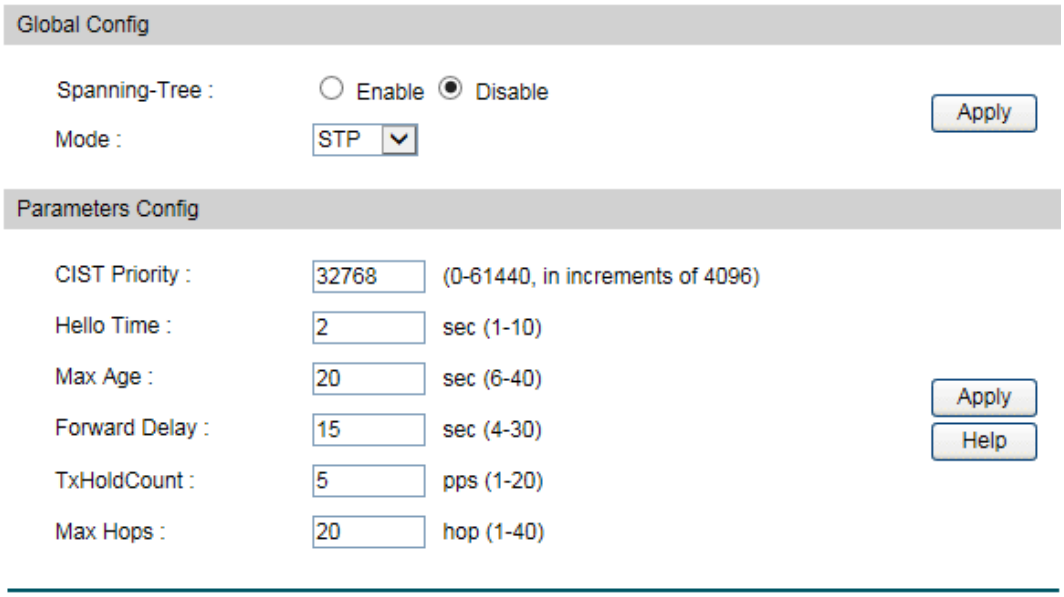


Figure 7-4 STP Config

The following entries are displayed on this screen:

- **Global Config**

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

Version: Select the desired STP version 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.

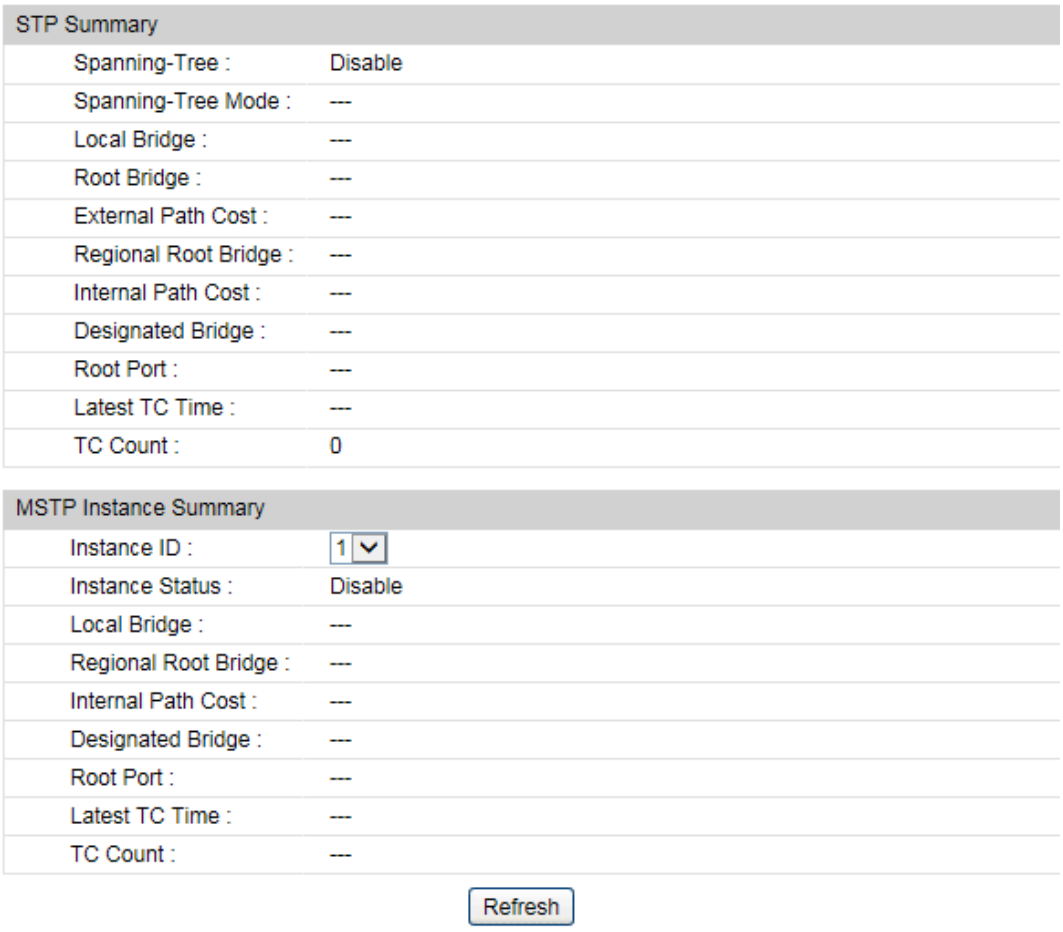


Figure 7-5 STP Summary

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.

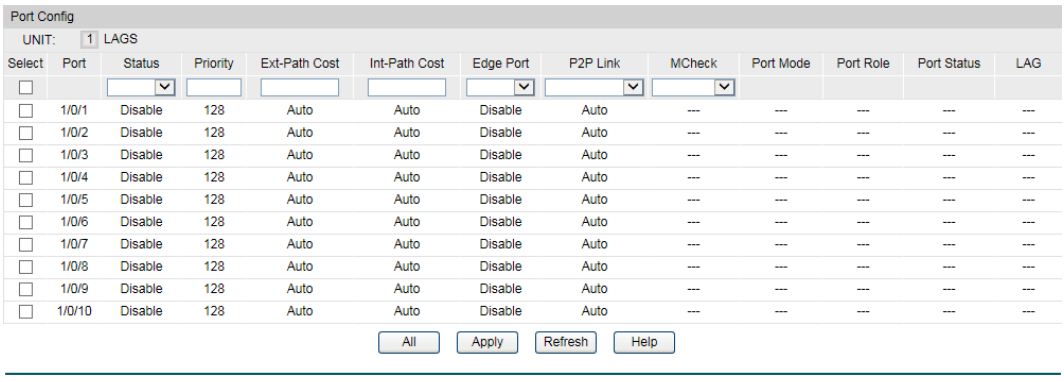


Figure 7-6 Port Config

The following entries are displayed on this screen:

➢ **Port Config**

Port Select: Click the **Select** button to quick-select the corresponding port based on the port number you entered.

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: 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: 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.

STP Version: Displays the STP version 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.

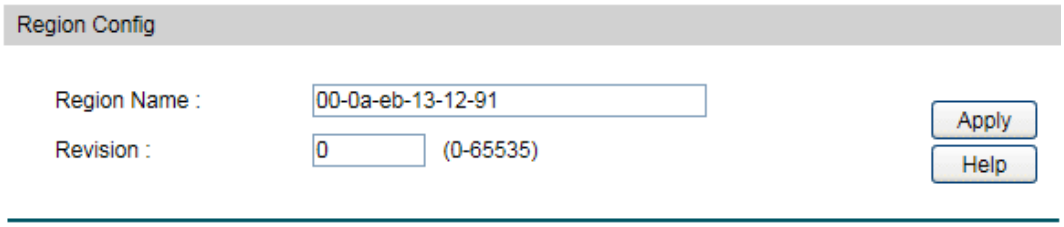


Figure 7-7 Region Config

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.

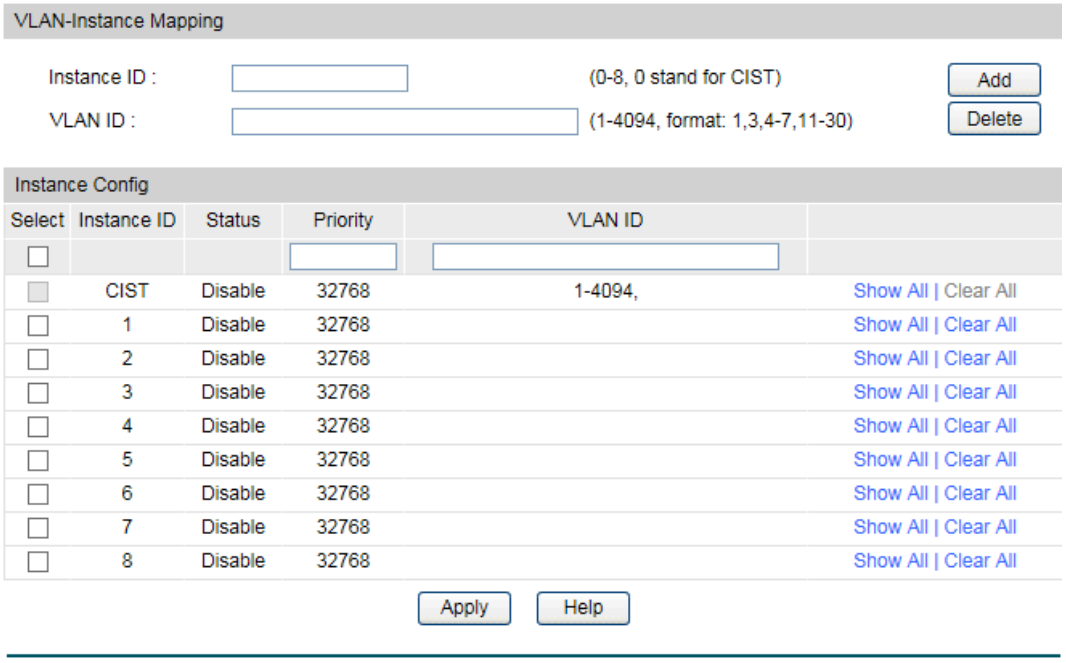


Figure 7-8 Instance Config

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.

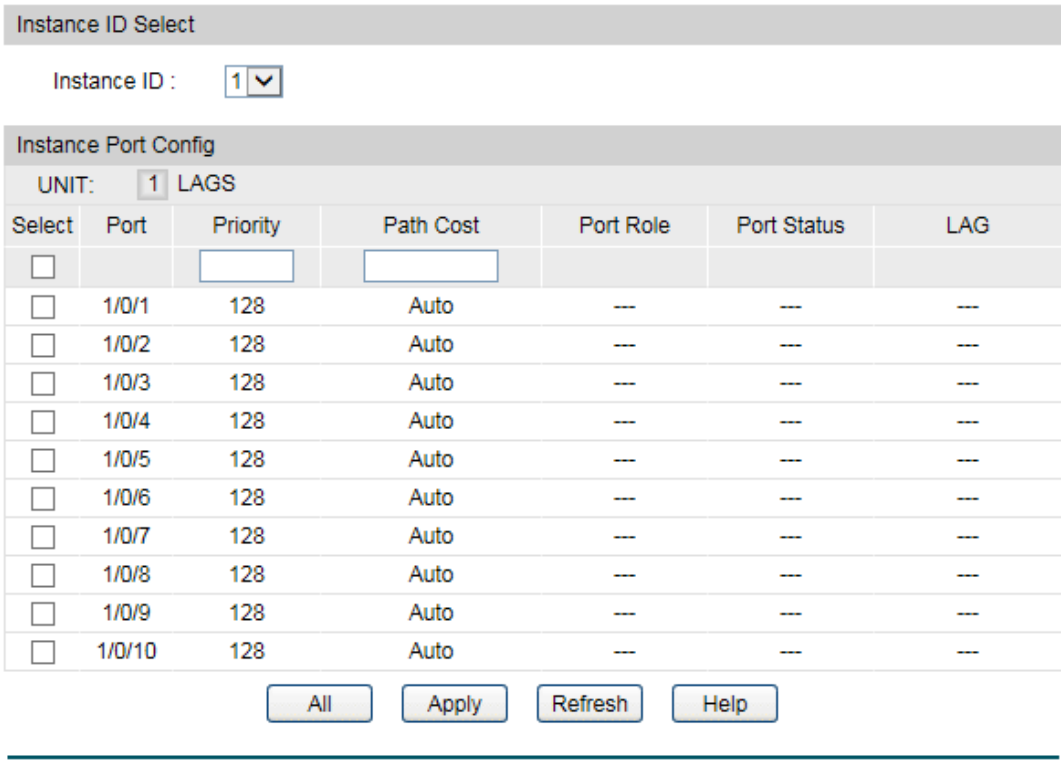


Figure 7-9 Instance Port Config

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** page.

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.

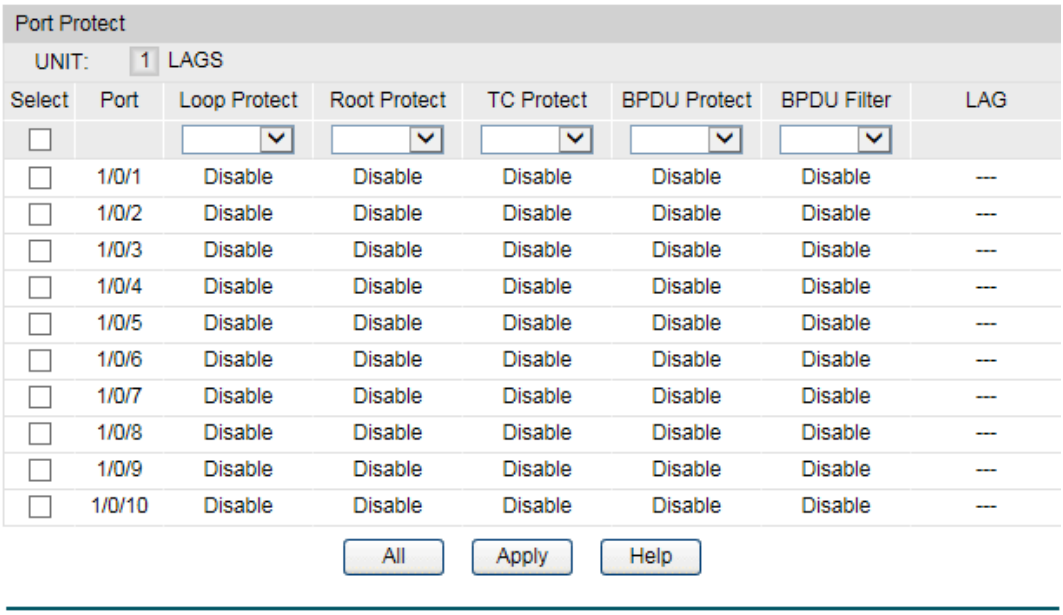


Figure 7-10 Port Protect

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.

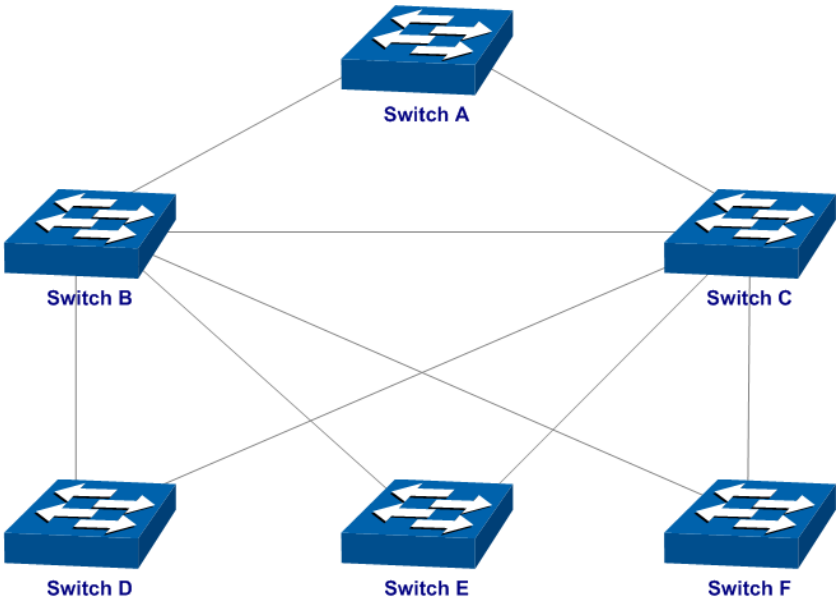
BPDU Protect:	BPDU Protect is to prevent the edge port from being attacked by maliciously created BPDUs
BPDU Filter:	BPDU Filter is to prevent BPDUs flood in the STP network.
LAG:	Displays the LAG number which the port belongs to.

7.5 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** 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.

Step	Operation	Description
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 as TP-Link 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
1	Configure ports	On **VLAN→802.1Q VLAN** 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 as TP-Link 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** 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 as TP-Link 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.
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:

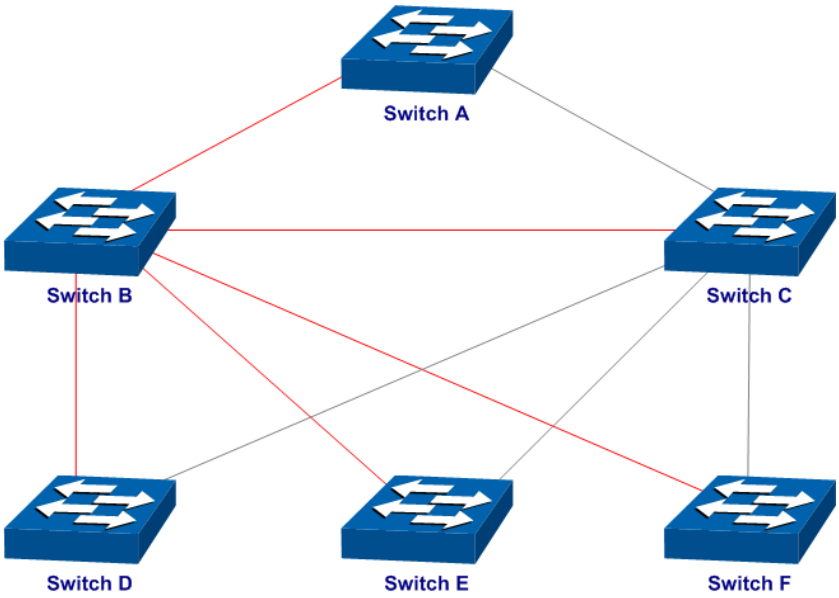
Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN** page, configure the link type of the related ports as Tagged, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable STP function	On **Spanning Tree→STP Config→STP Config** 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 as TP-Link and keep the default revision setting.

Step	Operation	Description
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.

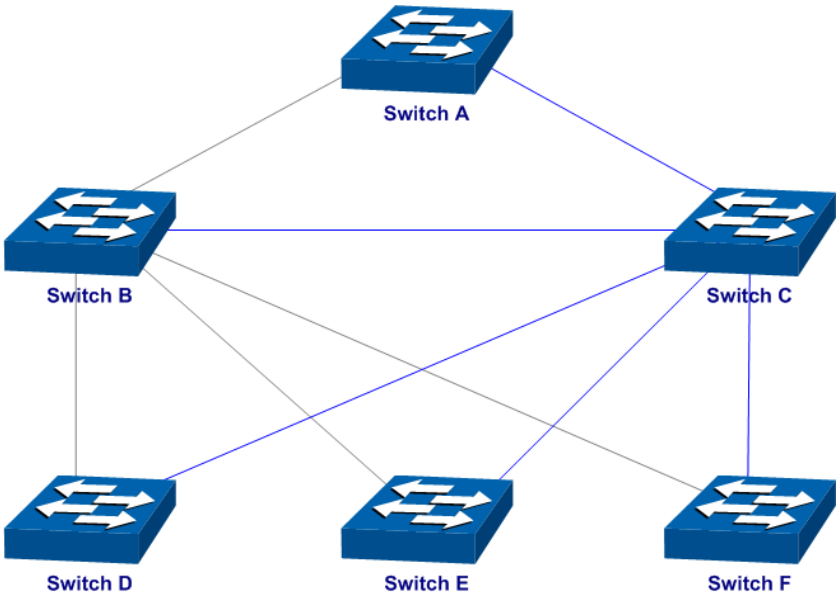
- The configuration procedure for switch E and F is the same with that for switch D.

➢ **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 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 8-1.

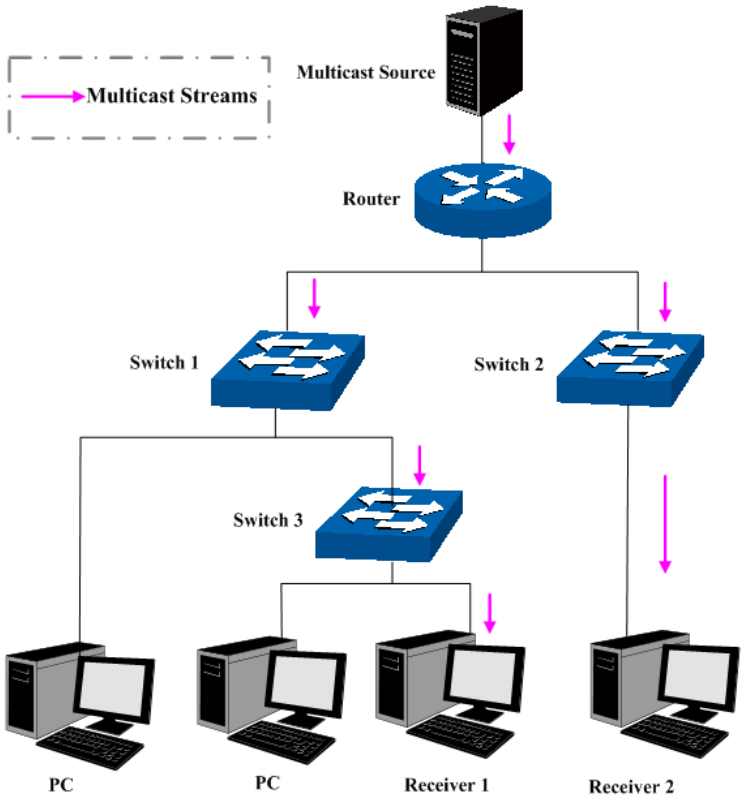


Figure 8-1 Information transmission in the multicast mode

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 8-1 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 8-2.

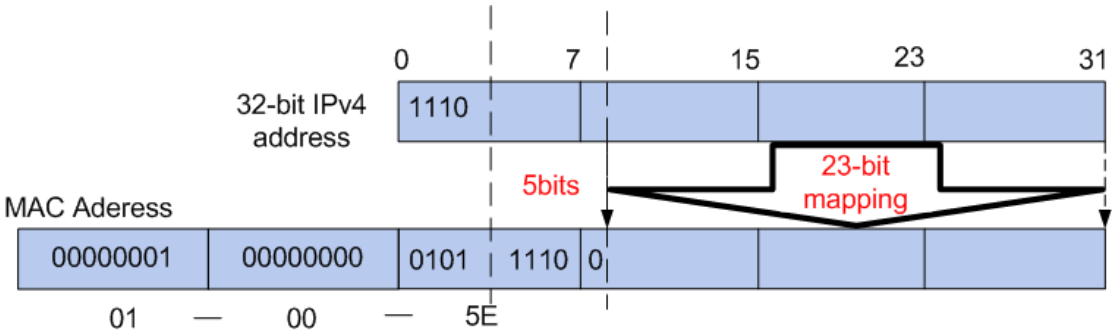


Figure 8-2 Mapping relationship between multicast IPv4 address and multicast MAC address

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.

➢ **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 8-3 below.

VLAN ID	Multicast IP	Port

Figure 8-3 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.

The Multicast module is mainly for multicast management configuration of the switch, including the following submenus: **IGMP Snooping** and **Multicast Table.**

8.1 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** and **Packet Statistics**.

8.1.1 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.

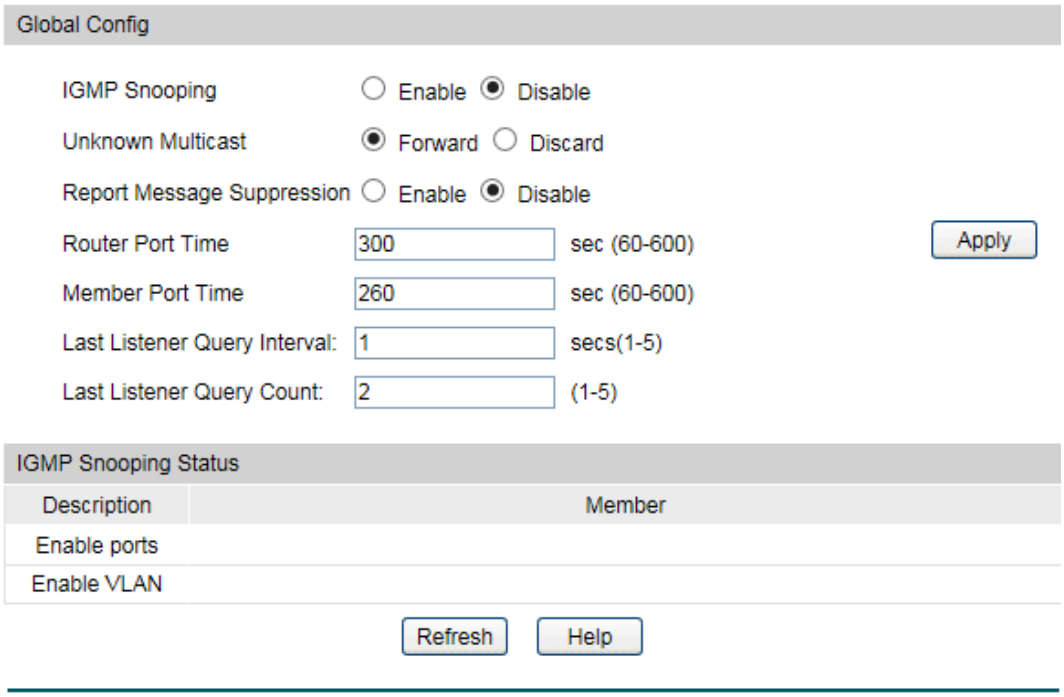


Figure 8-4 Basic Config

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.

8.1.2 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.

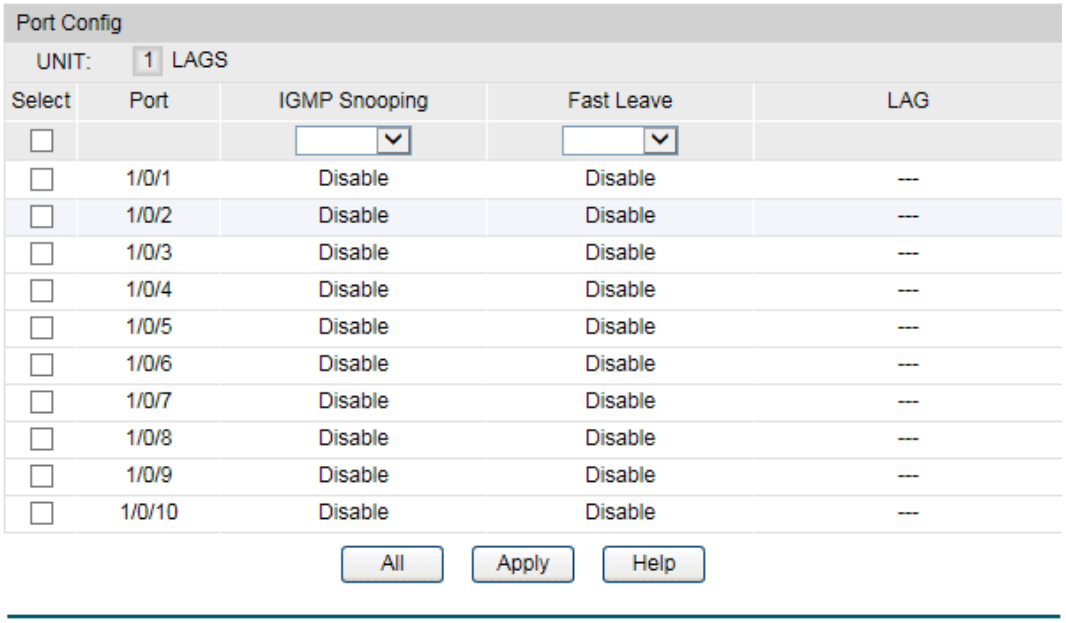


Figure 8-5 Port Config

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.

8.1.3 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.

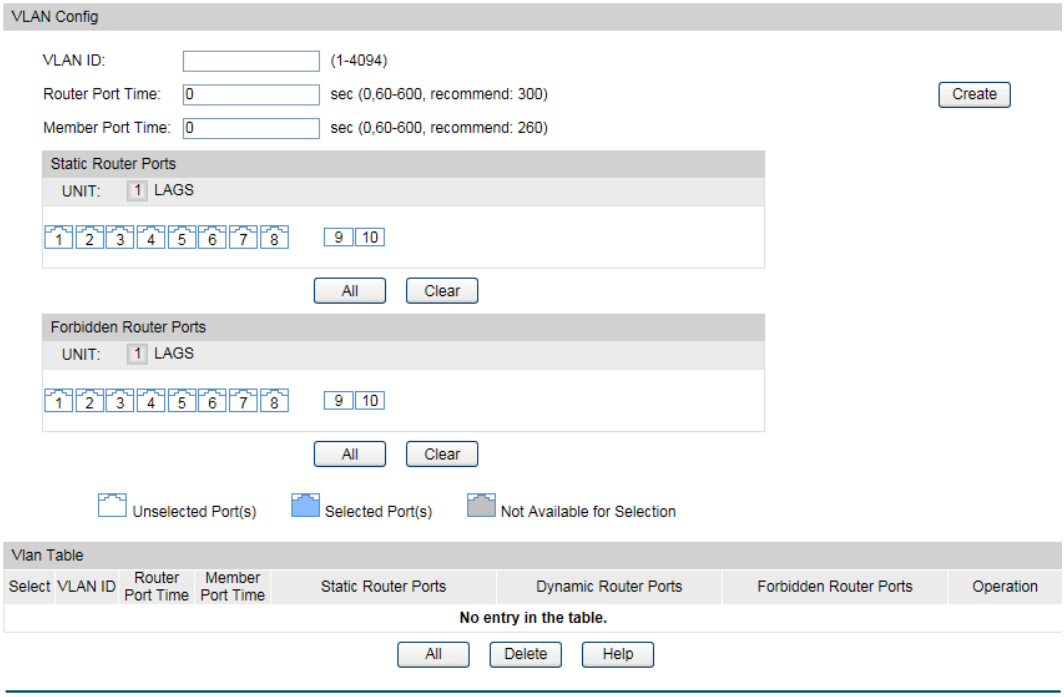


Figure 8-6 VLAN Config

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.

- **Static Router Ports**

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

Static Router Ports: Select one or more ports to be the static router ports in the VLAN. All multicast data in this VLAN will be forwarded through the static router ports.

- **Forbidden Router Ports**

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

Forbidden Router Ports: Select the ports to forbid them from being router ports in the VLAN.

- **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.

Operation Click **Edit** to modify the IGMP Snooping information in this 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	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.

8.1.4 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.

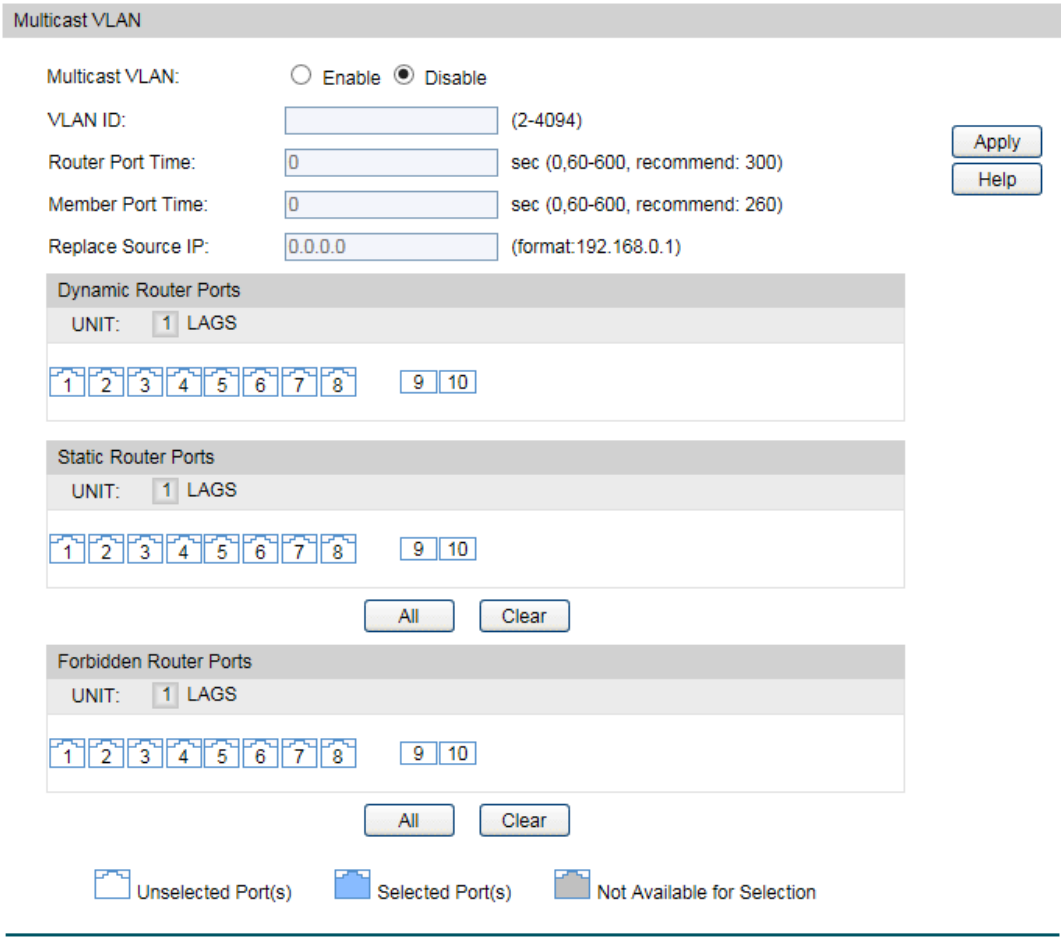


Figure 8-7 Multicast VLAN

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.

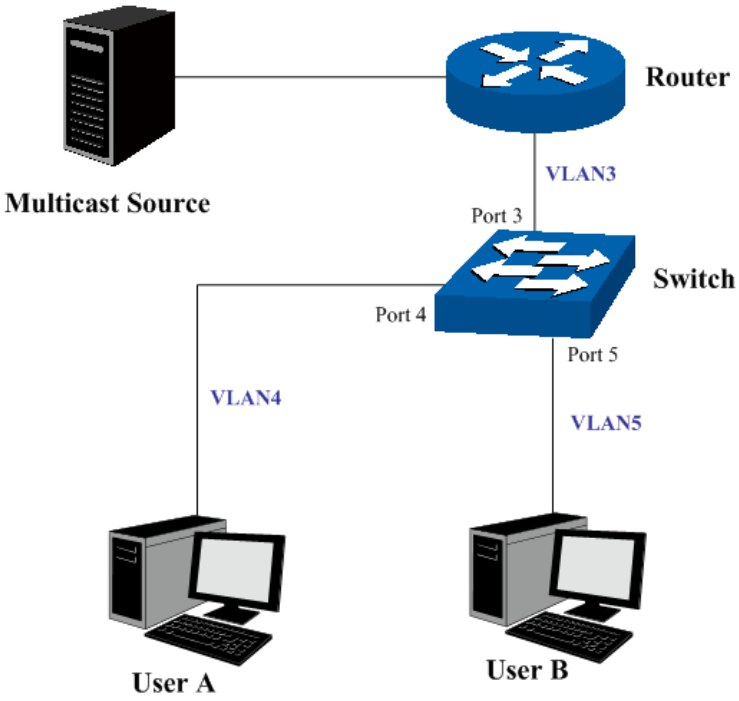
Switch: Port 3 is connected to the router and the packets are transmitted in VLAN3; port 4 is connected to user A and the packets are transmitted in VLAN4; port 5 is connected to user B and the packets are transmitted in VLAN5.

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.

8.1.5 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.

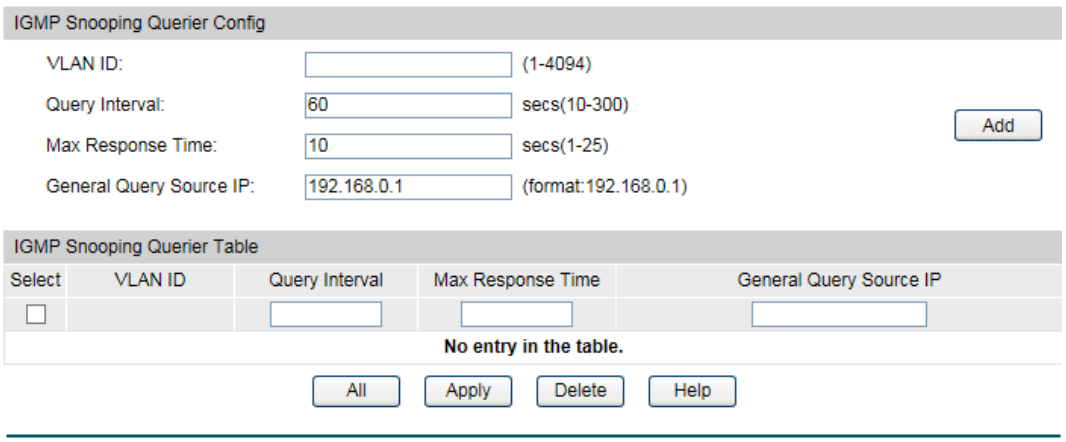


Figure 8-8 Querier Config

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.

8.1.6 Profile Config

On this page you can configure an IGMP profile.

Choose the menu **Multicast→IGMP Snooping→Profile Config** to load the following page.

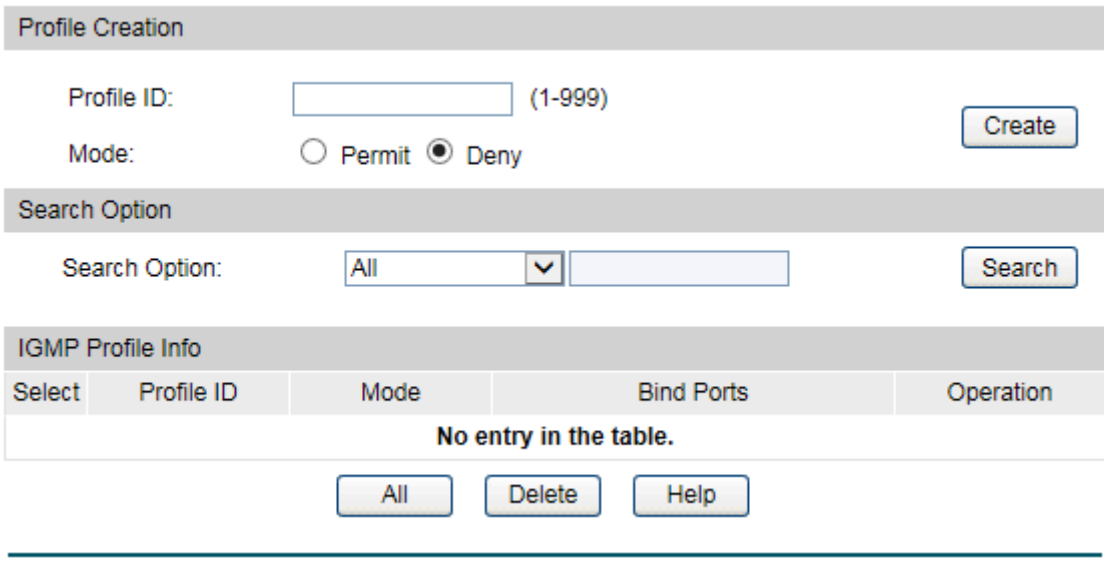


Figure 8-9 Profile Config

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.

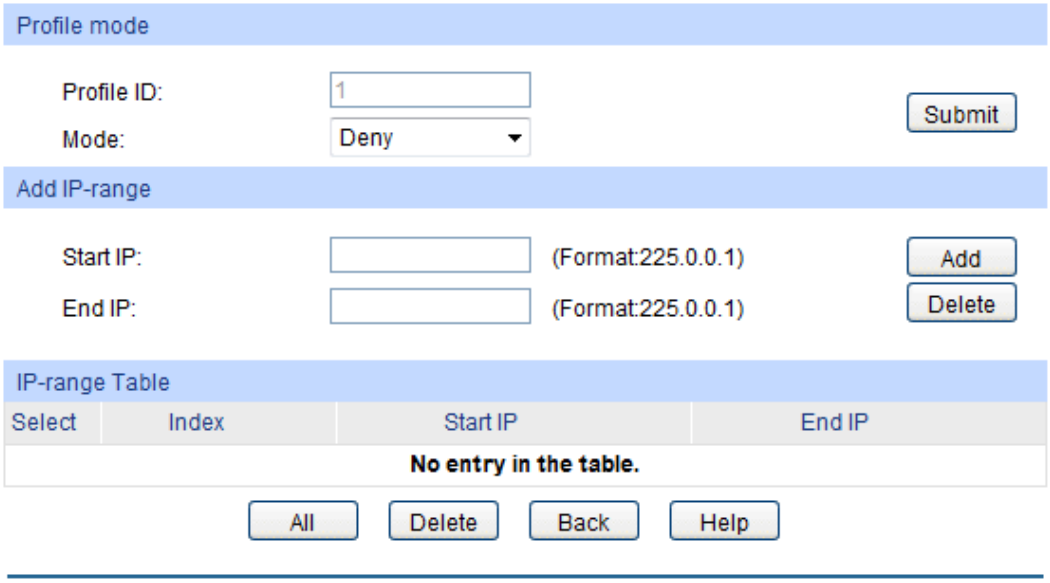
Mode: Displays the attribute of the profile.

- **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.

8.1.7 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.

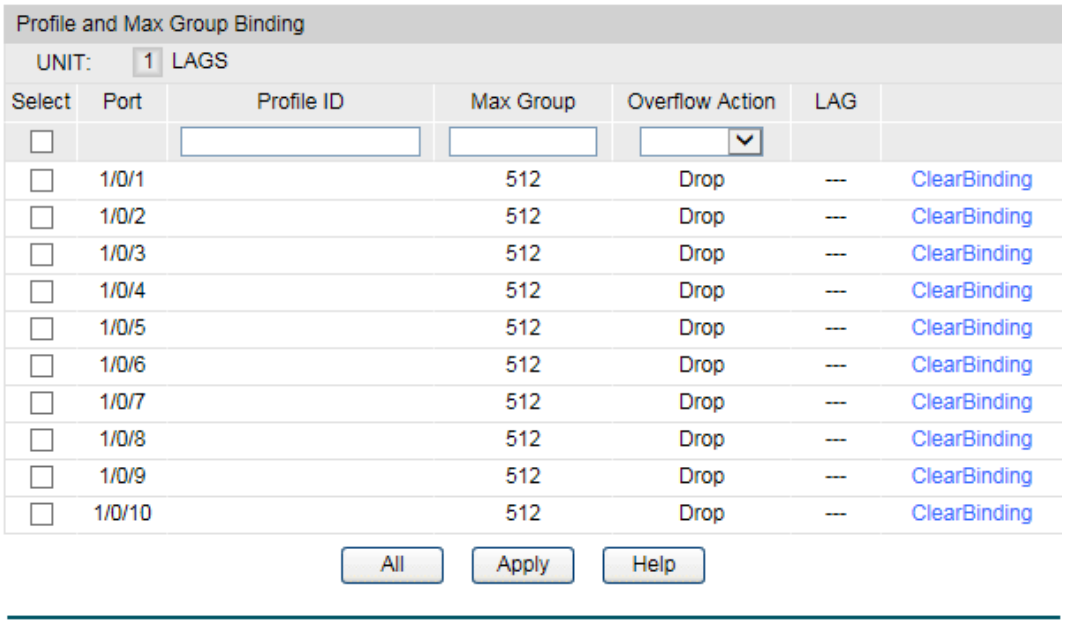


Figure 8-10 Profile Binding

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.

8.1.8 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.

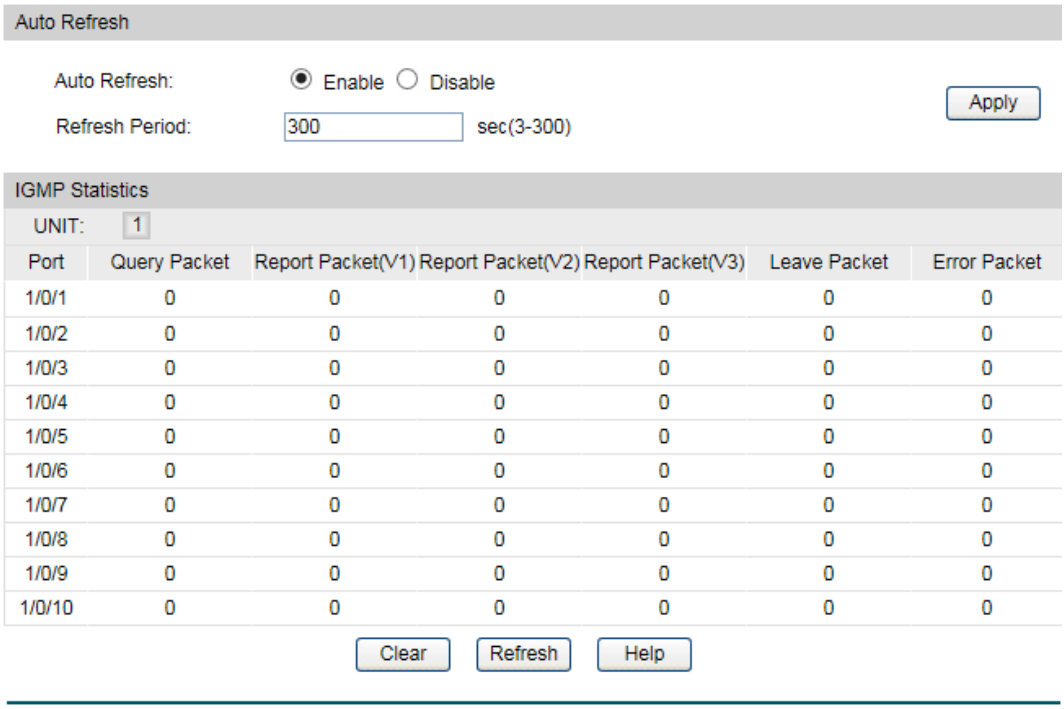


Figure 8-11 Packet Statistics

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.

8.2 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** and **Static IPv4 Multicast Table**.

8.2.1 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.

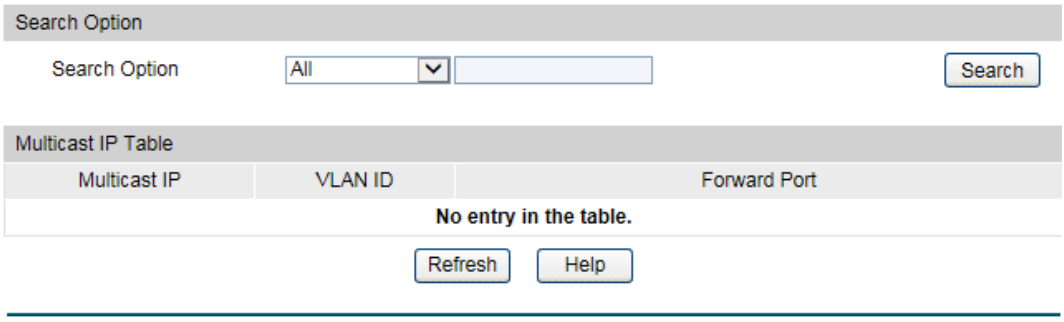


Figure 8-12 IPv4 Multicast Table

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.

8.2.2 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.

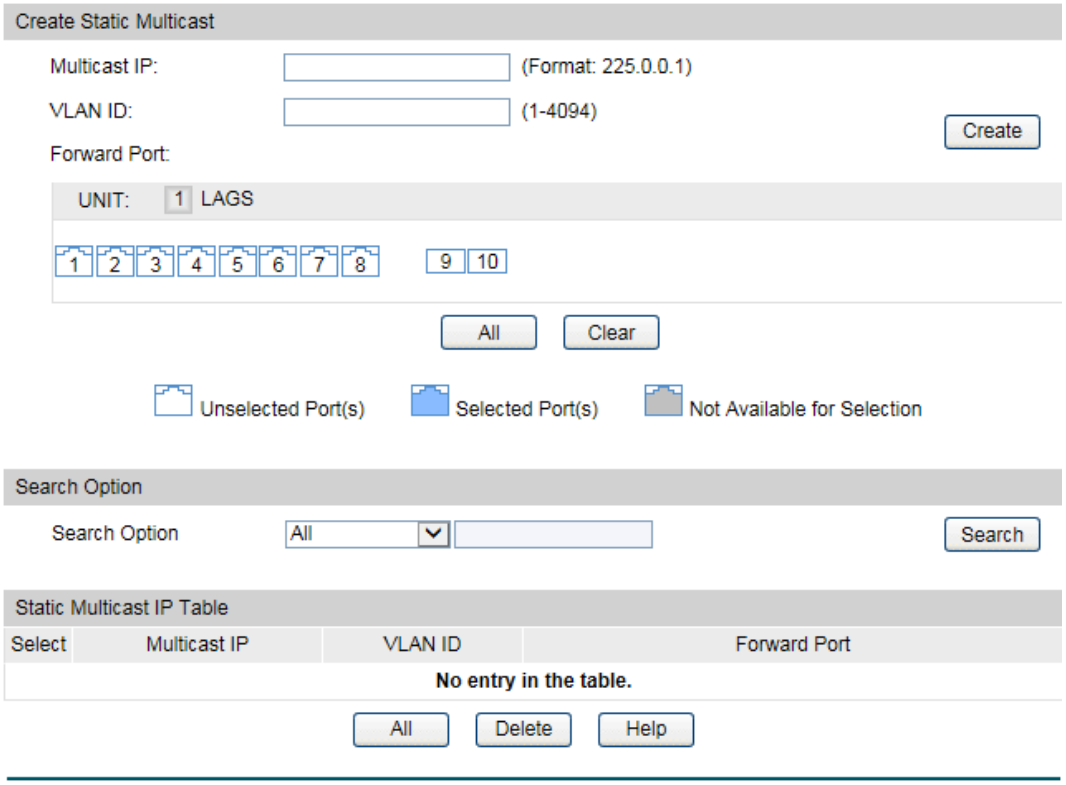


Figure 8-13 Static IPv4 Multicast Table

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.

Return to CONTENTS

Chapter 9 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.

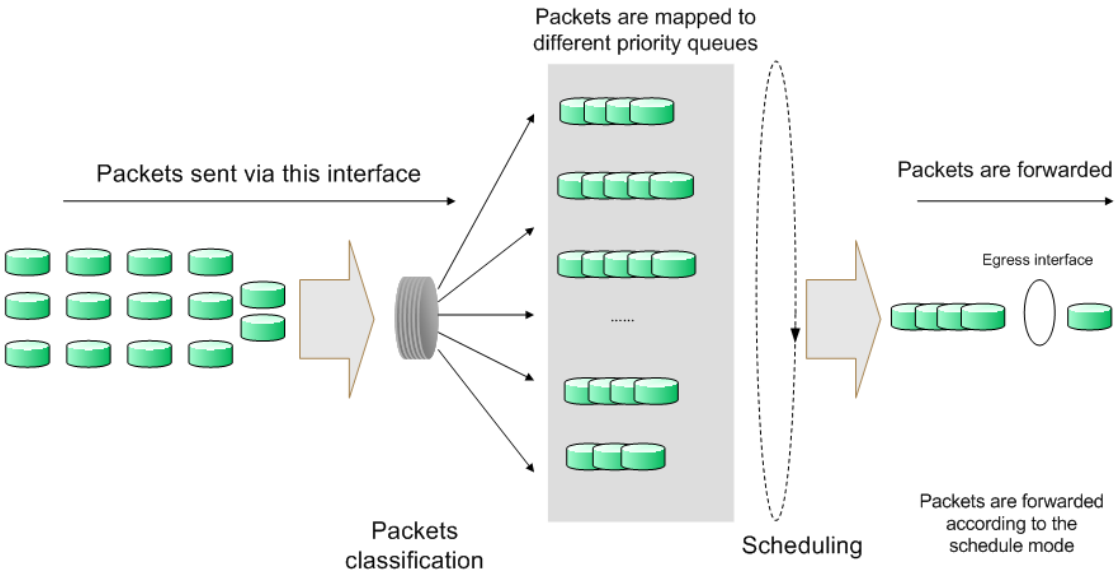


Figure 9-1 QoS function

- 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

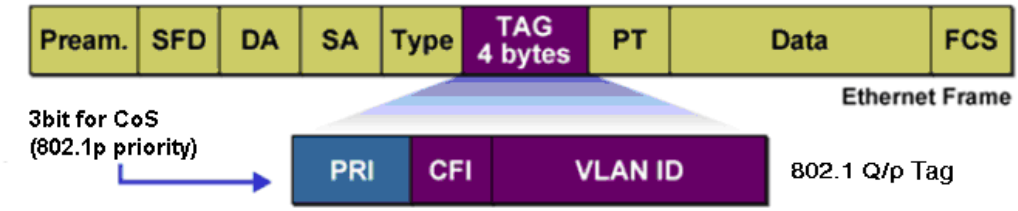


Figure 9-2 802.1Q frame

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

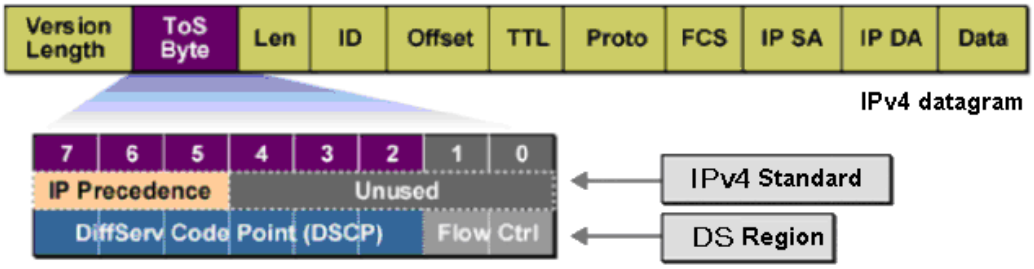


Figure 9-3 IP datagram

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 four scheduling queues, TC0, TC1, TC2 and TC3. TC0 has the lowest priority while TC3 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 four egress queues labeled as TC0, TC1, TC2 and TC3. In SP mode, their priorities increase in order. TC3 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.

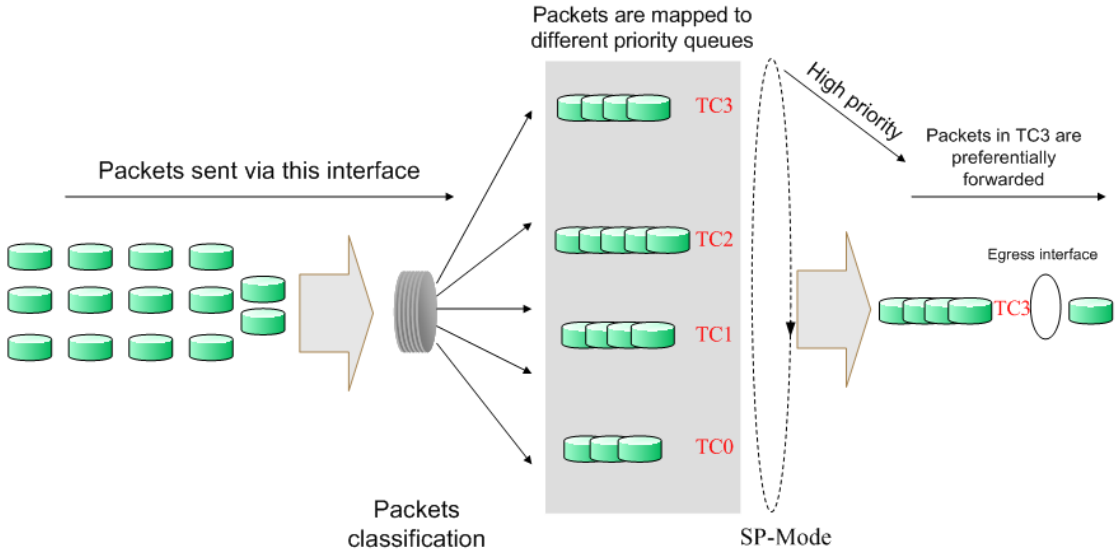


Figure 9-4 SP-Mode

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 and TC3 is 1:2:4:8.

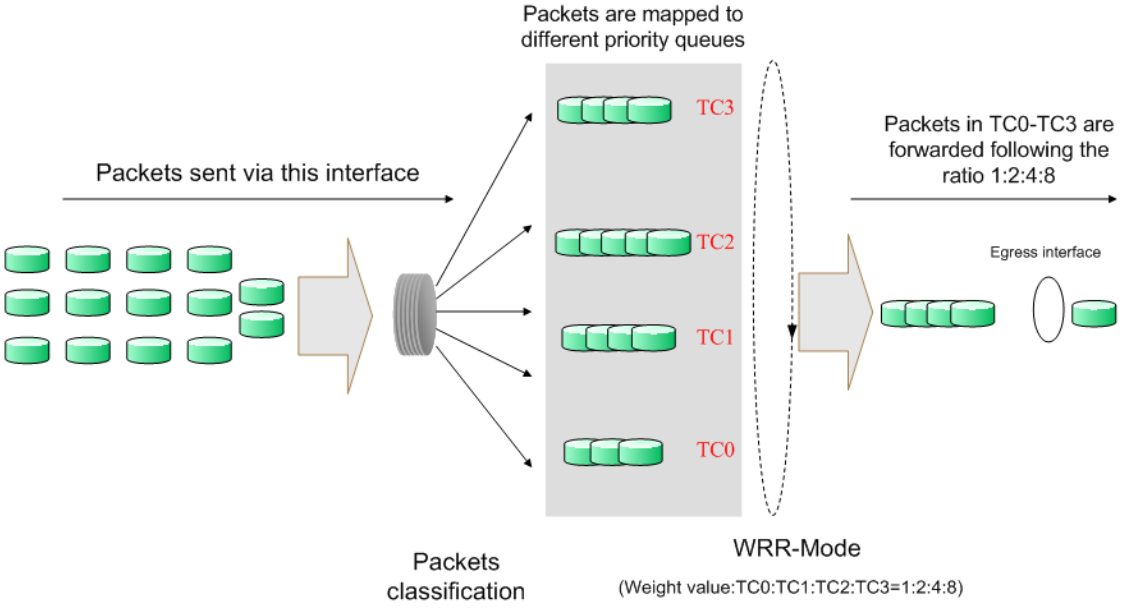


Figure 9-5 WRR-Mode

3. SP+WRR-Mode: Strict-Priority + Weight Round Robin Mode. In this mode, this 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, TC3 is in the SP group; TC0, TC1 and TC2

belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.

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.

The QoS module is mainly for traffic control and priority configuration, including three submenus: **DiffServ**, **Bandwidth Control** and **Voice VLAN**.

9.1 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**, **802.1P/Cos mapping**, **DSCP Priority** and **Schedule Mode** pages.

9.1.1 Port Priority

On this page you can configure the port priority.

Choose the menu **QoS→DiffServ→Port Priority** to load the following page.

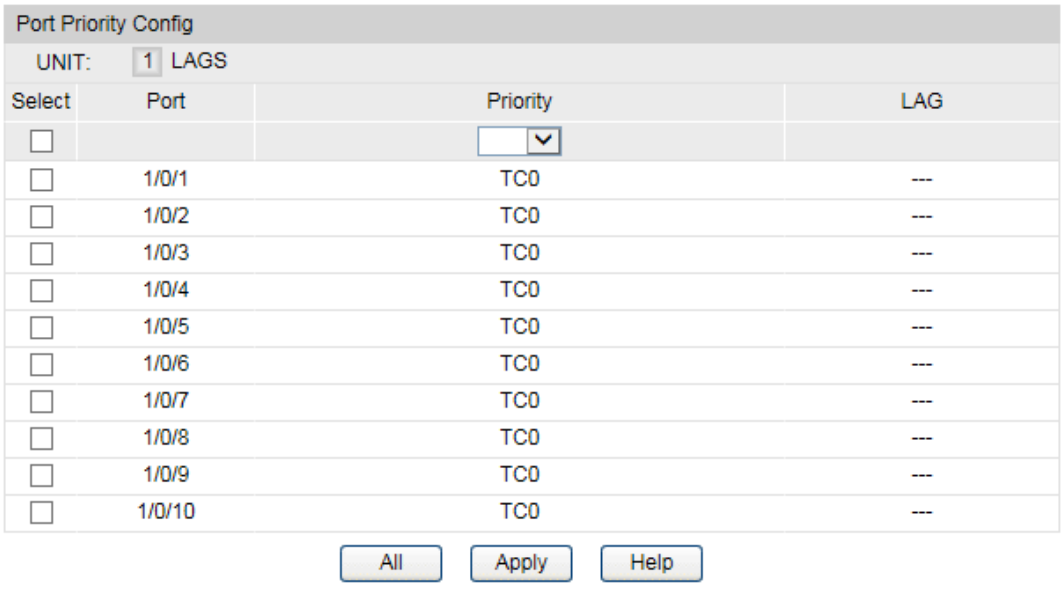


Figure 9-6 Port Priority Config for

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	Select a schedule mode	Required. On **QoS→DiffServ→Schedule Mode** page, select a schedule mode.

9.1.2 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… TC3.

Choose the menu **QoS→DiffServ→Schedule Mode** to load the following page.

Figure 9-7 Schedule Mode

The following entries are displayed on this screen:

- **Schedule Mode Config**

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 value ratio of TC0, TC1, TC2 and TC3 is 1:2:4:8.

SP+WRR-Mode: Strict-Priority + Weight Round Robin Mode. In this mode, this 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, TC3 is in the SP group; TC0, TC1 and TC2 belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.

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.

9.1.3 802.1P 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/CoS mapping** to load the following page.

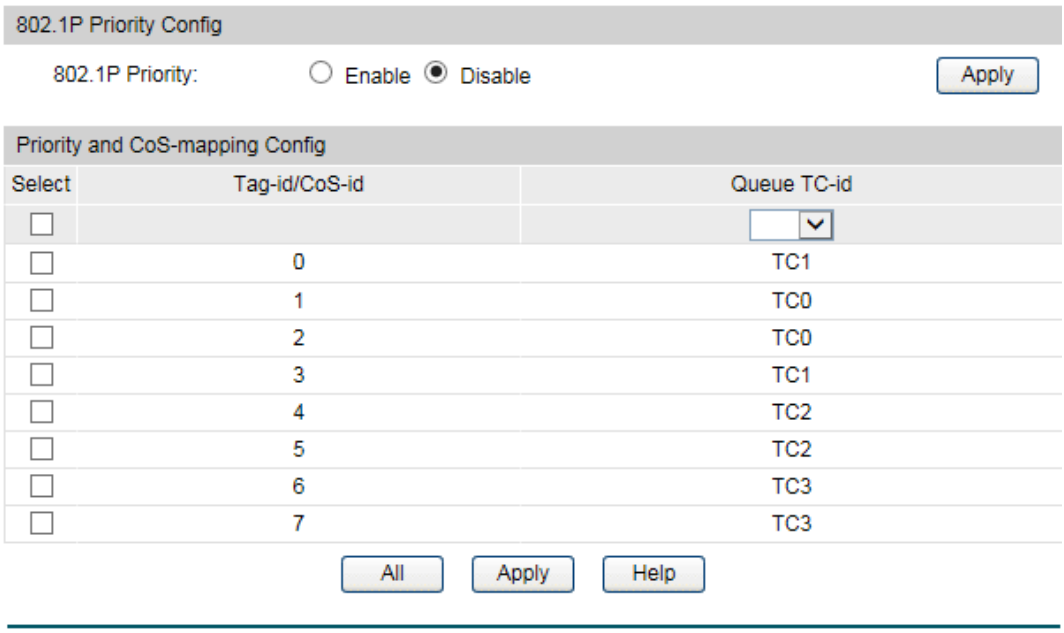


Figure 9-8 802.1P/CoS mapping

The following entries are displayed on this screen:

➢ **802.1P Priority Config**

802.1P Priority: Select Enable or Disable 802.1P Priority.

➢ **Priority and CoS-mapping Config**

Tag-id/Cos-id: Indicates the precedence level defined by IEEE802.1P 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 and TC3.

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/CoS mapping** 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.

9.1.4 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 8021.1P 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.

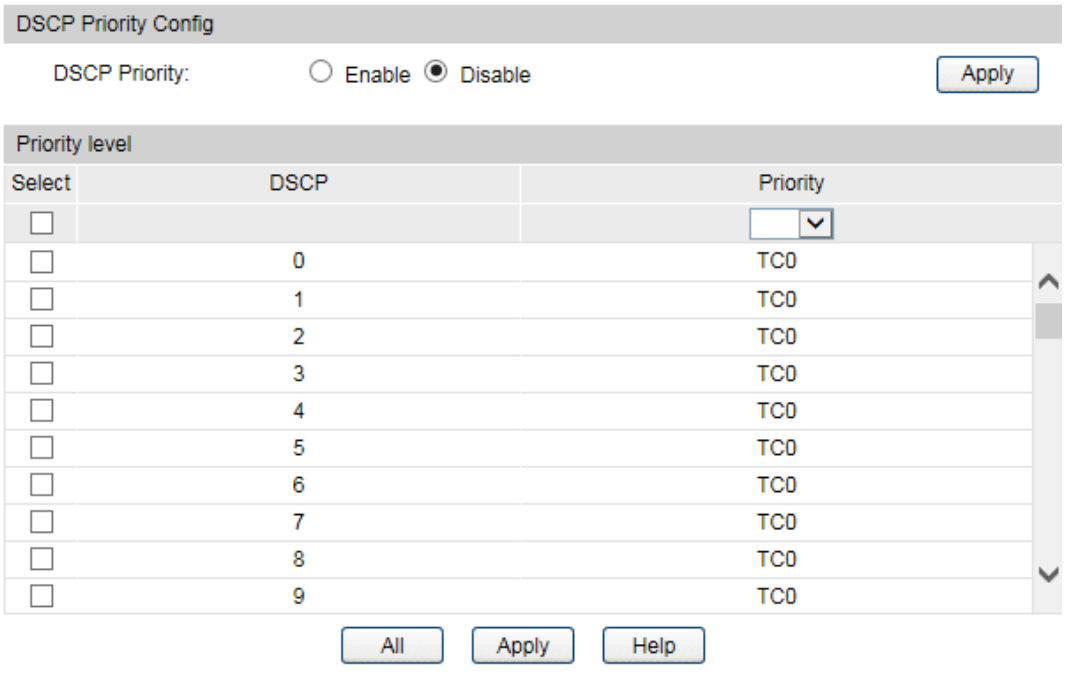


Figure 9-9 DSCP Priority

The following entries are displayed on this screen:

- **DSCP Priority Config**

  DSCP Priority: Select Enable or Disable DSCP Priority.

- **Priority Level**

  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 TC0 ~ TC3.

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 TC.
2	Select a schedule mode	Required. On **QoS→DiffServ→Schedule Mode** page, select a schedule mode.

9.2 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.

9.2.1 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.

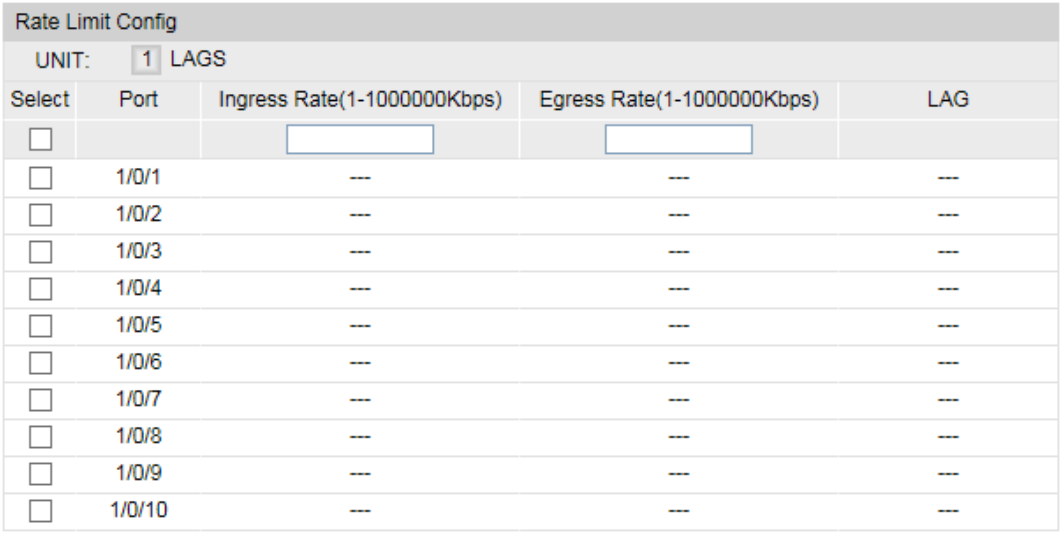


Figure 9-10 Rate Limit

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 select "Manual" to 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 select "Manual" to 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 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.

9.2.2 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.

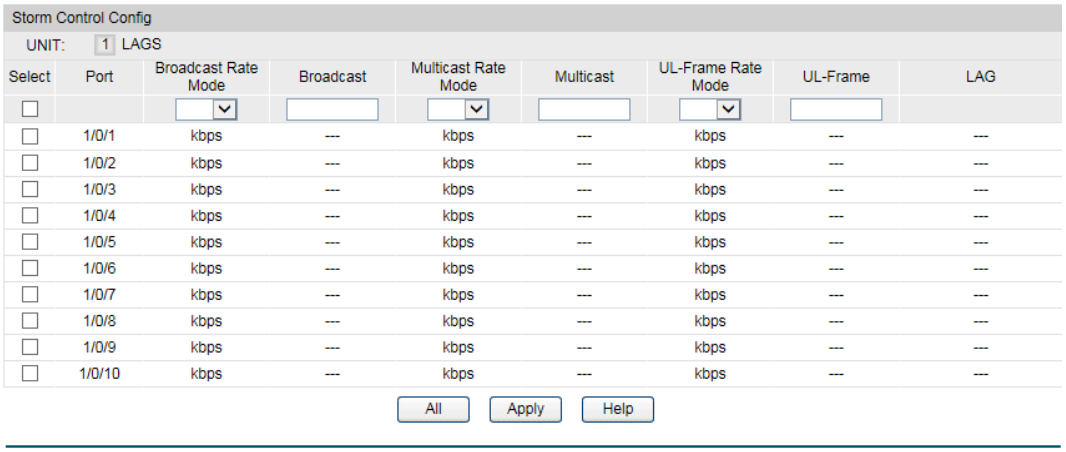


Figure 9-11 Storm Control

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.
Broadcast Rate Mode:	Select the broadcast rate mode, kbps or ratio. • **kbps**: Specify the threshold in kbits per second. • **ratio**: Specify the threshold as a percentage of the bandwidth.
Broadcast:	Select the bandwidth for receiving broadcast packets on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the broadcast control feature on the port.
Multicast Rate Mode:	Select the multicast rate mode, kbps or ratio. • **kbps**: Specify the threshold in kbits per second. • **ratio**: Specify the threshold as a percentage of the bandwidth.
Multicast:	Select the bandwidth for receiving multicast packets on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the multicast control feature on the port.
UL-Frame Rate Mode:	Select the UL-Frame rate mode, kbps or ratio. • **kbps**: Specify the threshold in kbits per second. • **ratio**: Specify the threshold as a percentage of the bandwidth.
UL-Frame:	Select the bandwidth for receiving UL-Frame on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the UL-Frame control feature on the port.
LAG:	Displays the LAG number which the port belongs to.

Note:

If you enable storm control feature for the ingress rate limit-enabled port, ingress rate limit feature will be disabled for this port.

9.3 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 9-1 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 9-2 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 9-3 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.

9.3.1 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.

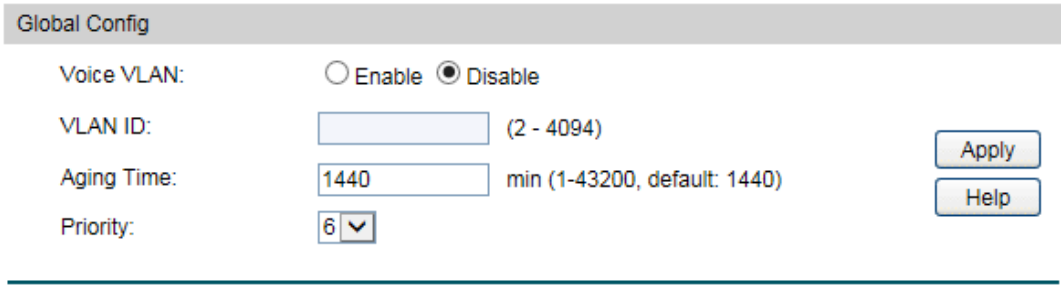


Figure 9-12 Global Configuration

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.

9.3.2 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.

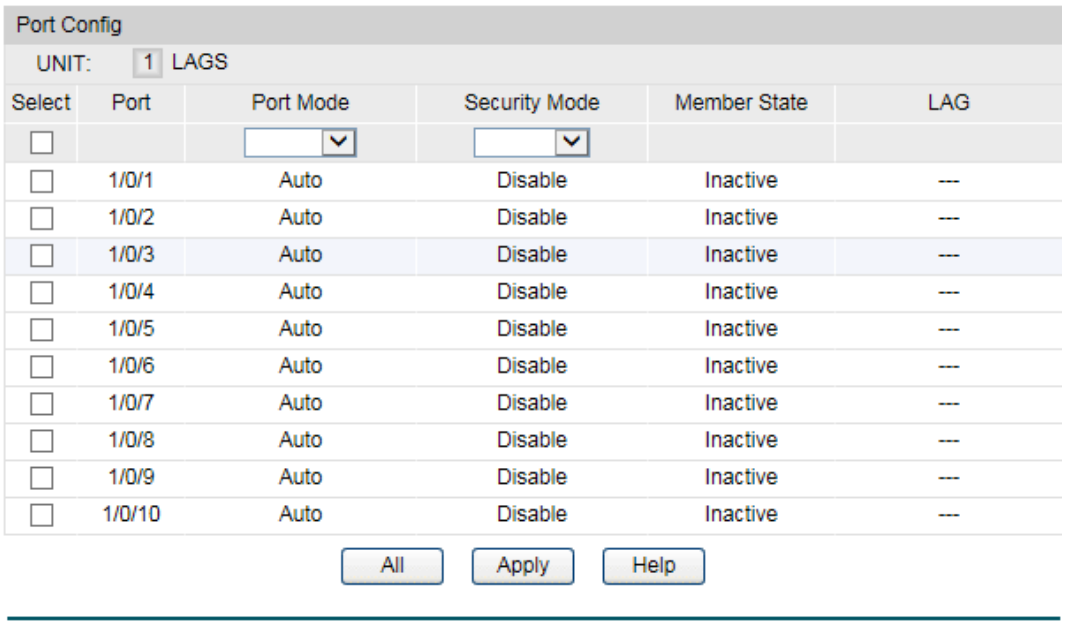


Figure 9-13 Port Config

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.

9.3.3 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.

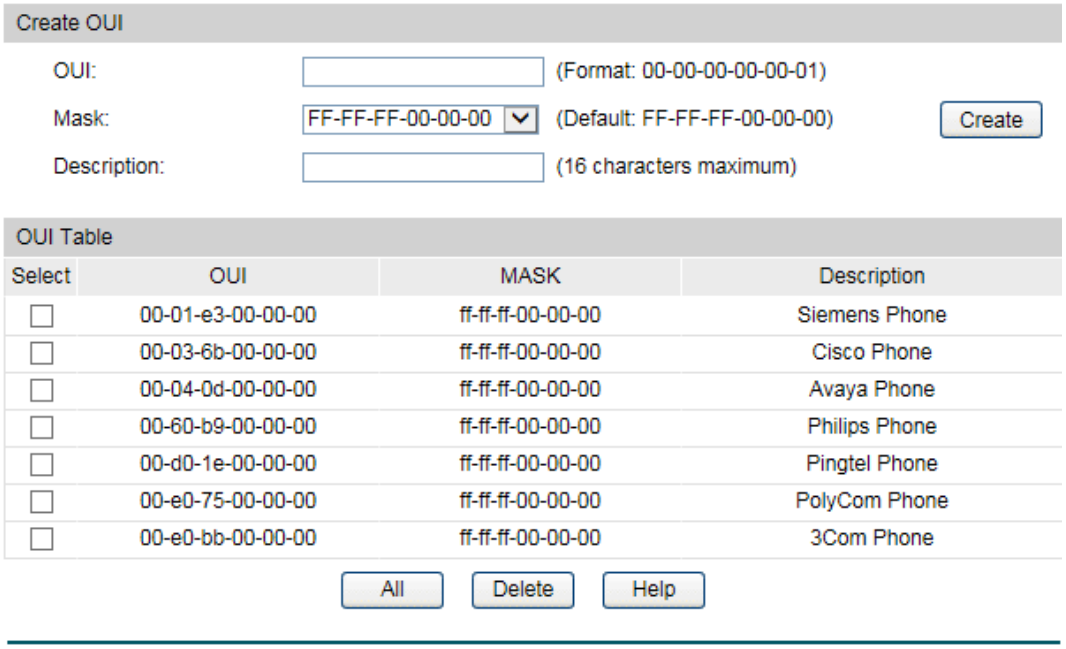


Figure 9-14 OUI Configuration

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	Configure the link type of the port	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, configure the link type of ports of the voice device.
2	Create VLAN	Required. On **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN.
3	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.
4	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.
5	Enable Voice VLAN	Required. On **QoS→Voice VLAN→Global Config** page, configure the global parameters of voice VLAN.

Return to CONTENTS

Chapter 10 PoE

Note:
Only T1500G-10MPS supports PoE function.

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 falls 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.

T1500G-10MPS 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.

PoE function can be configured in the two sections, **PoE Config** and **PoE Time-Range**.

10.1 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.

10.1.1 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.

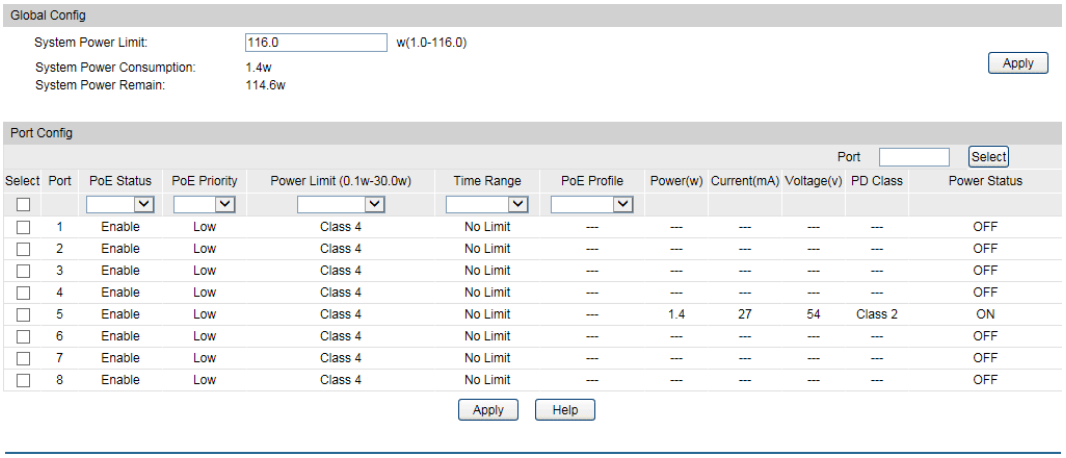


Figure 10-1 PoE Config

The following items are displayed on this screen:

- **Global Config**

  System Power Limit: Specify the max power the PoE switch can supply.

  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**

  Port Select: Click the **Select** button to quick-select the corresponding entry based on the port number you entered.

  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 PD linked to the port with lower priority will be disconnected.

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.

10.1.2 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.

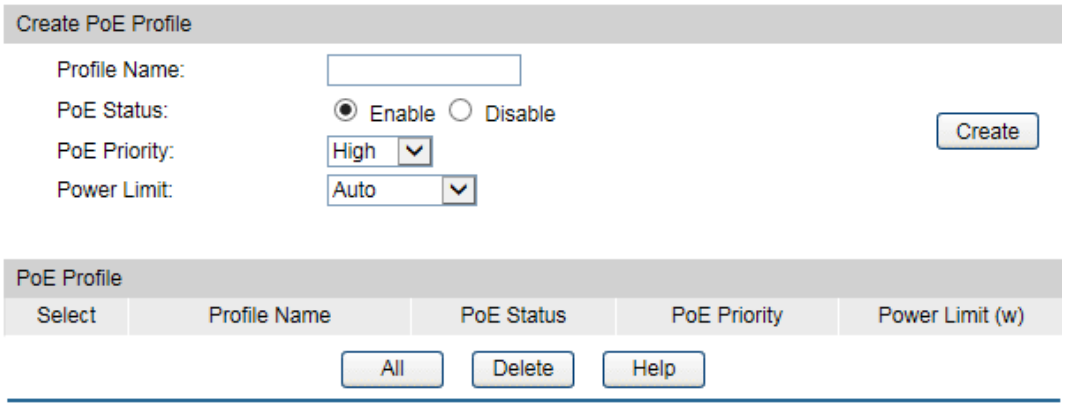


Figure 10-2 Profile Config

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.

10.2 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 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 the port based on this time range supply power; configure a week time section to make the port supply based on this time range on the fixed days of the week; configure a holiday section and select **Exclude Holiday** to make the port based on this time range not supply power on some special days. In each time-range, four time-slices can be configured.

The Time-Range configuration can be implemented on **PoE Time-Range Summary**, **PoE Time-Range Create** and **PoE Holiday Config** pages.

10.2.1 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.

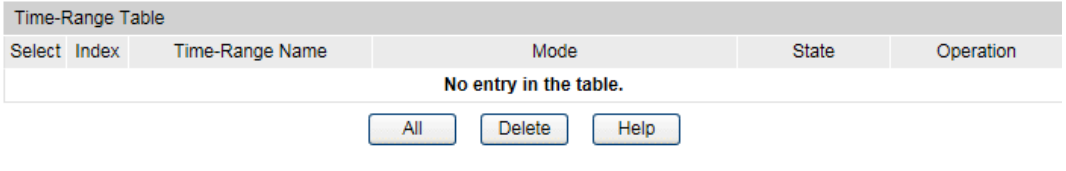


Figure 10-3 Time-Range Table

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 the time-range adopts. The mode can be one or a combination of the following modes: **Include/Exclude Holiday**, **Absolute** and **Periodic**.
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.

10.2.2 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.

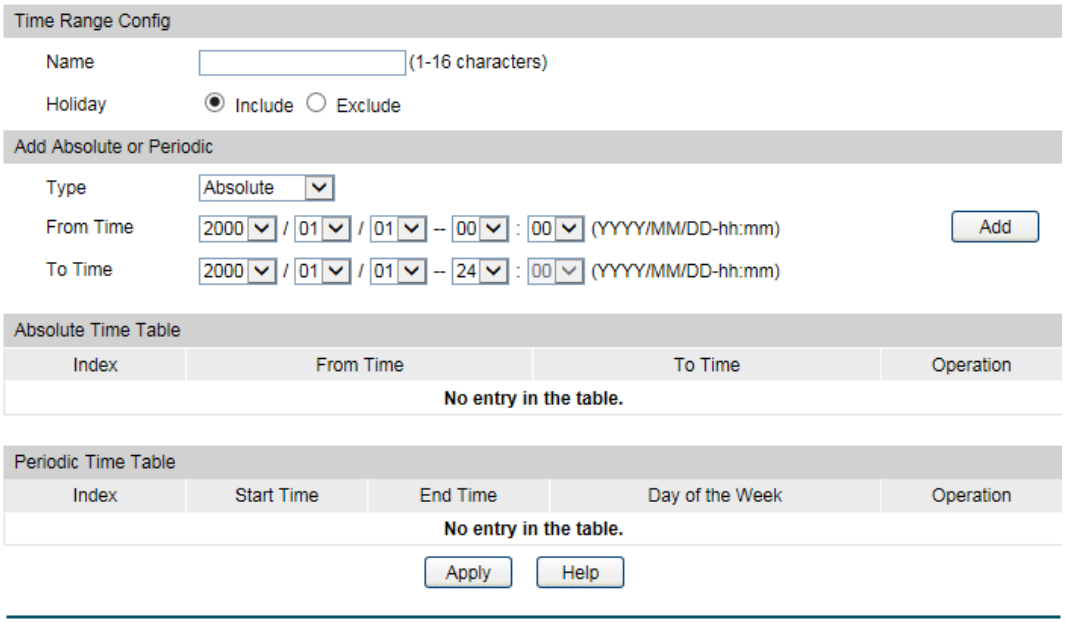


Figure 10-4 Time-Range Create

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.

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.

10.2.3 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 Create** to load the following page.

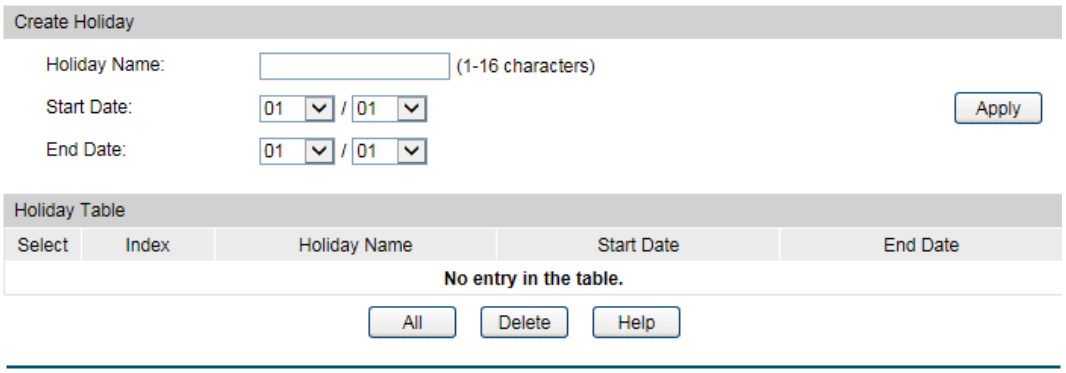


Figure 10-5 Holiday Configuration

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.

Return to CONTENTS

Chapter 11 ACL

11.1 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** and **Extend-IP ACL** pages.

11.1.1 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 11-1 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.

- **Rule Table**

Display the rule table of the ACL you have selected. Here you can edit the rules, view the details of them, and move them up and down.

11.1.2 ACL Create

On this page you can create ACLs.

Choose the menu **ACL→ACL Config→ACL Create** to load the following page.

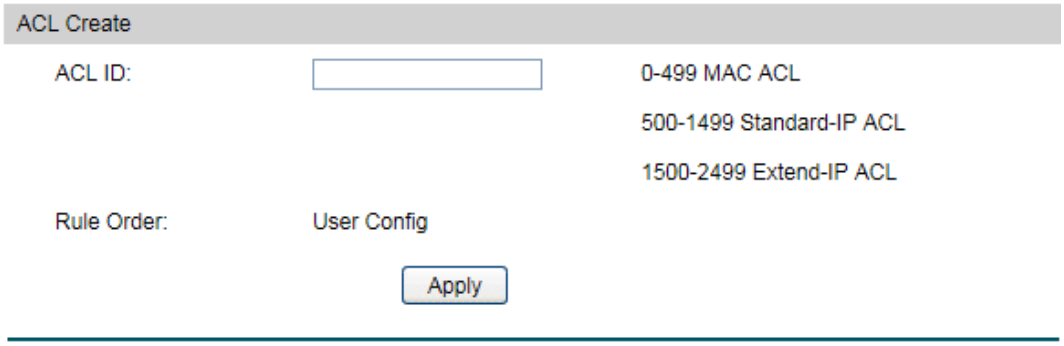


Figure 11-2 ACL Create

The following entries are displayed on this screen:

➢ **Create ACL**

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.

11.1.3 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.

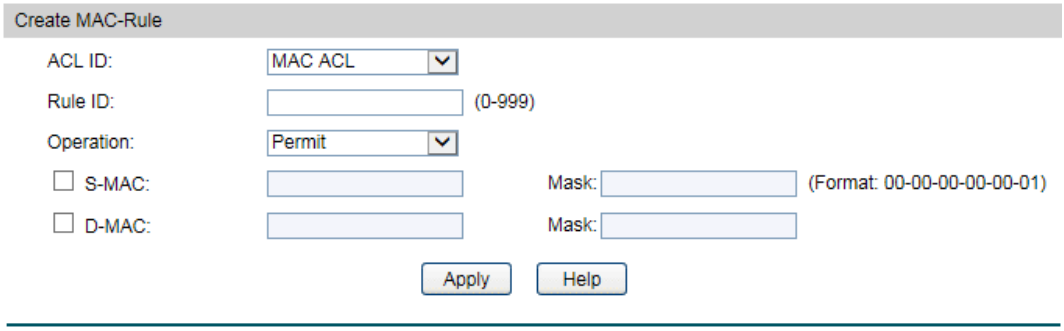


Figure 11-3 Create MAC Rule

The following entries are displayed on this screen:

➢ **Create MAC ACL**

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.

11.1.4 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.

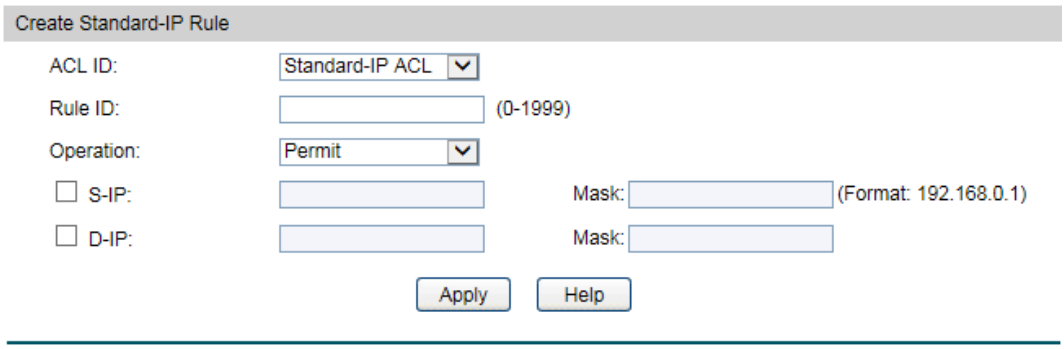


Figure 11-4 Create Standard-IP Rule

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.

11.1.5 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.

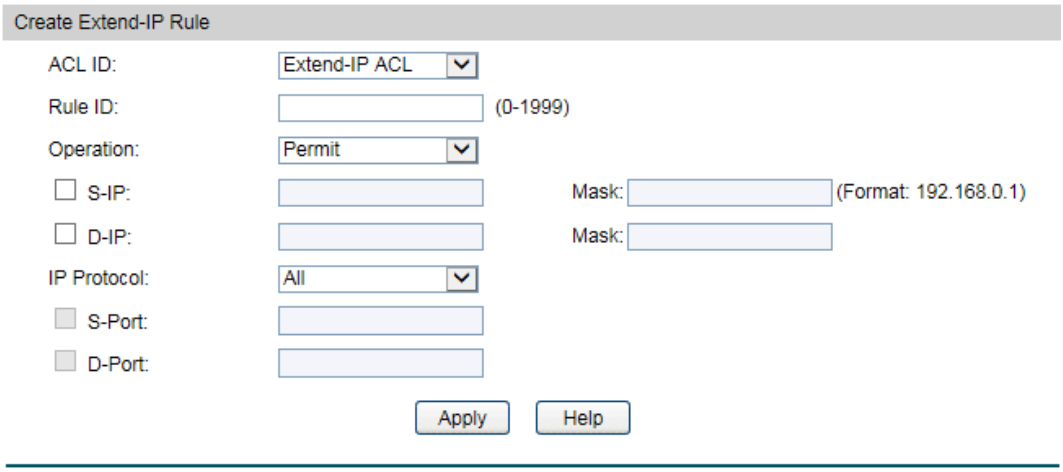


Figure 11-5 Create Extend-IP Rule

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.

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.

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.

11.2 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.

11.2.1 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.

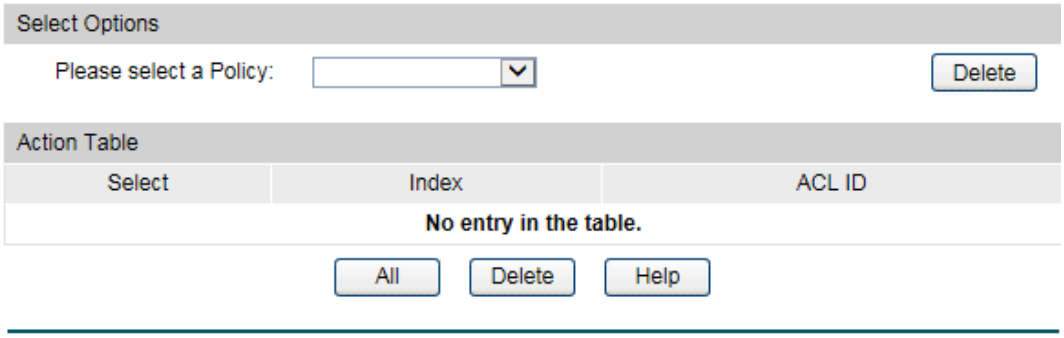


Figure 11-6 Policy Summary

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.

11.2.2 Policy Create

On this page you can create the policy.

Choose the menu **ACL→Policy Config→Policy Create** to load the following page.

Figure 11-7 Create Policy

The following entries are displayed on this screen:

- **Create Policy**

  Policy Name: Enter the name of the policy.

11.2.3 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.

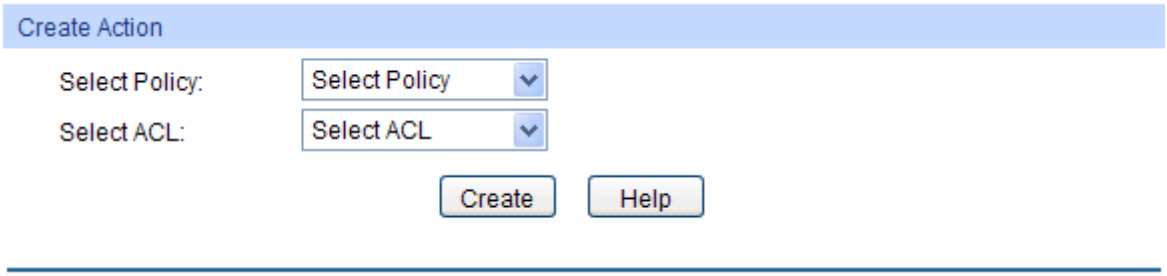


Figure 11-8 Action Create

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.

11.3 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.

11.3.1 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.

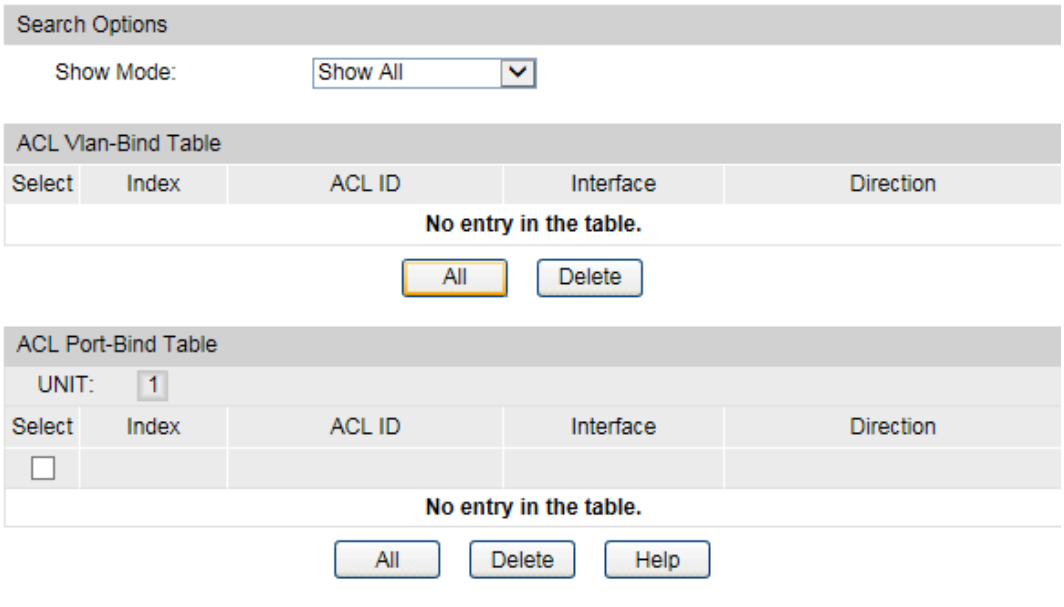


Figure 11-9 Binding Table

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.

11.3.2 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.

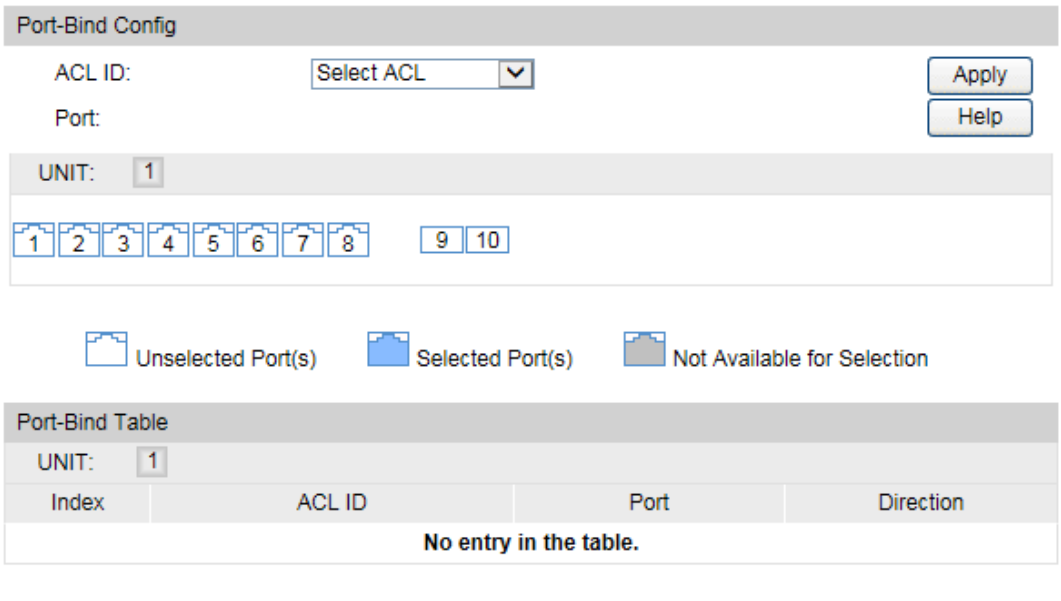


Figure 11-10 Bind the policy to the port

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.

11.3.3 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.

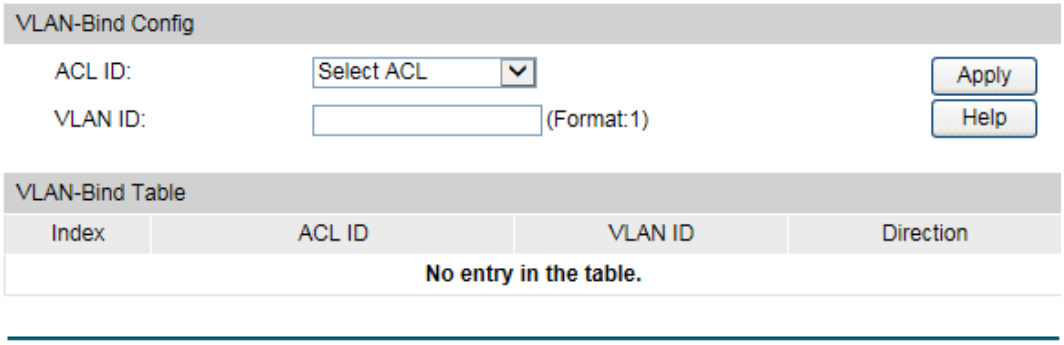


Figure 11-11 Bind the policy to the VLAN

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.

11.4 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.

11.4.1 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.

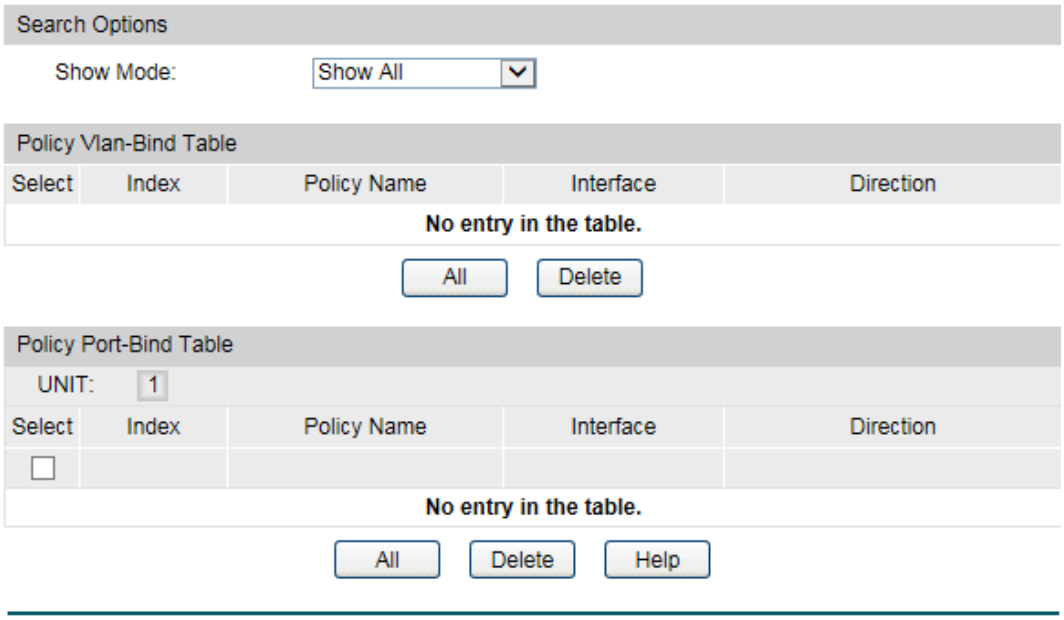


Figure 11-12 Binding Table

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.

11.4.2 Port Binding

On this page you can bind a policy to a port.

Choose the menu **ACL→Policy Binding→Port Binding** to load the following page.

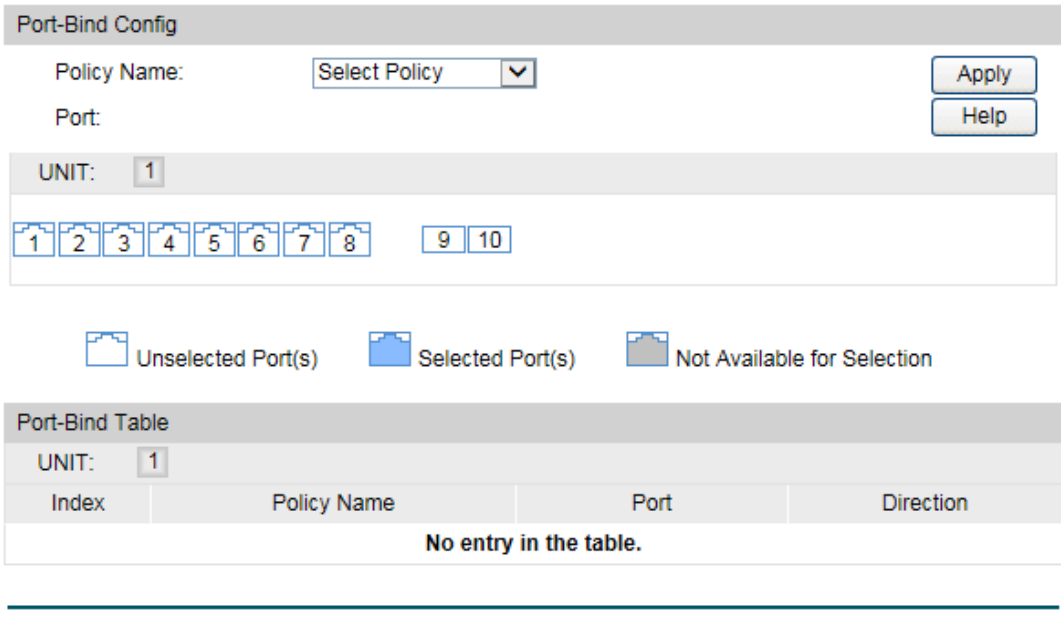


Figure 11-13 Bind the policy to the port

The following entries are displayed on this screen:

- **Port-Bind Config**

Policy Name: Select the name of the policy you want to bind.

Port: Enter 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.

11.4.3 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.

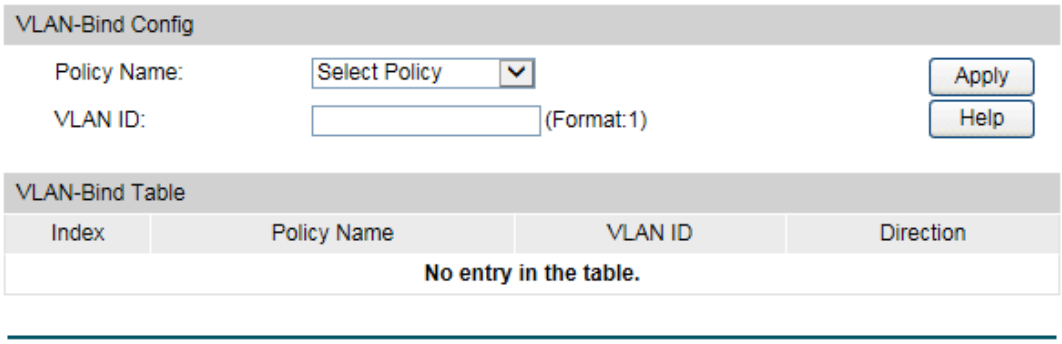


Figure 11-14 Bind the policy to the VLAN

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
3	Configure ACL rules	Required. On **ACL→ACL Config** configuration pages, configure ACL rules to match packets.
4	Configure Policy	Required. On **ACL→Policy Config** configuration pages, configure the policy to control the data packets those match the corresponding ACL rules.

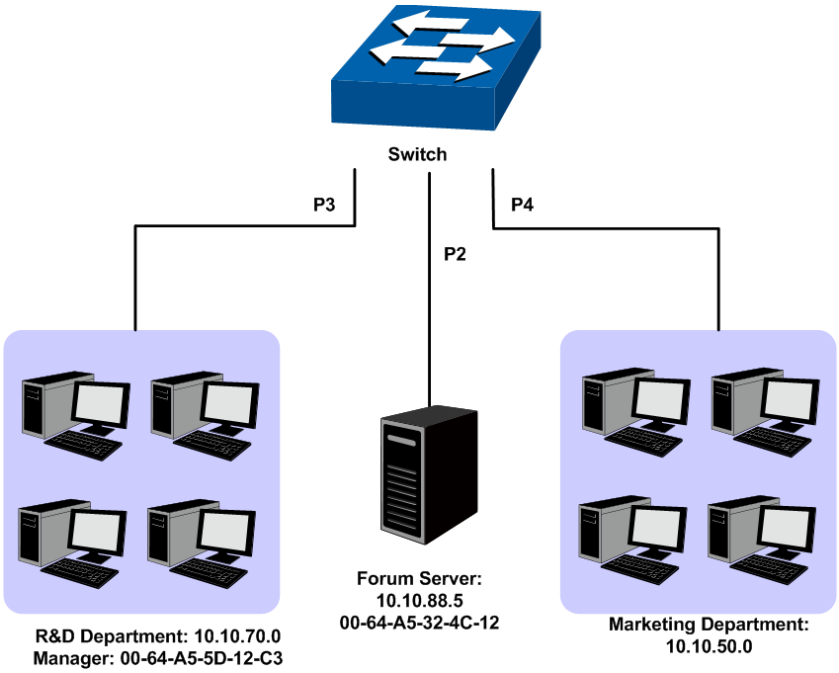
5	Bind the policy to the port/VLAN	Required. On **ACL→Policy Binding** configuration pages, bind the policy to the port/VLAN to make the policy effective on the corresponding port/VLAN.

11.5 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 10.10.70.0 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 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 12 Network Security

Network Security module is to provide the multiple protection measures for the network security, including five submenus: **IP-MAC Binding**, **DHCP Snooping**, **ARP Inspection**, **DoS Defend**, **802.1X** and **AAA**. Please configure the functions appropriate to your need.

12.1 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.

12.1.1 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.

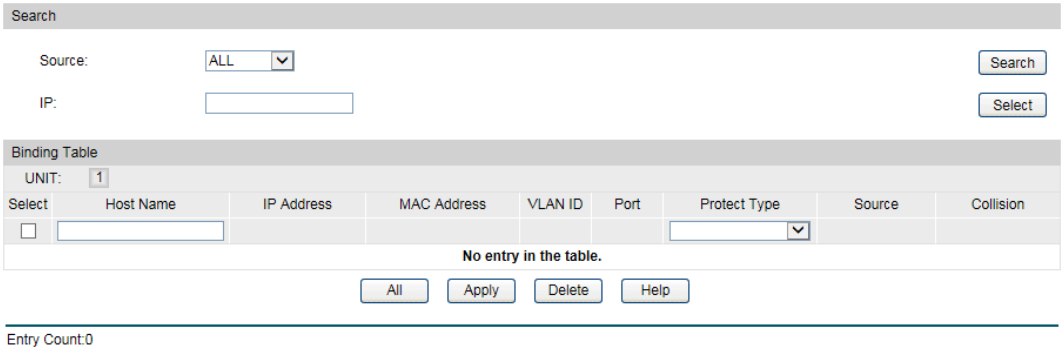


Figure 12-1 Binding Table

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.

12.1.2 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.

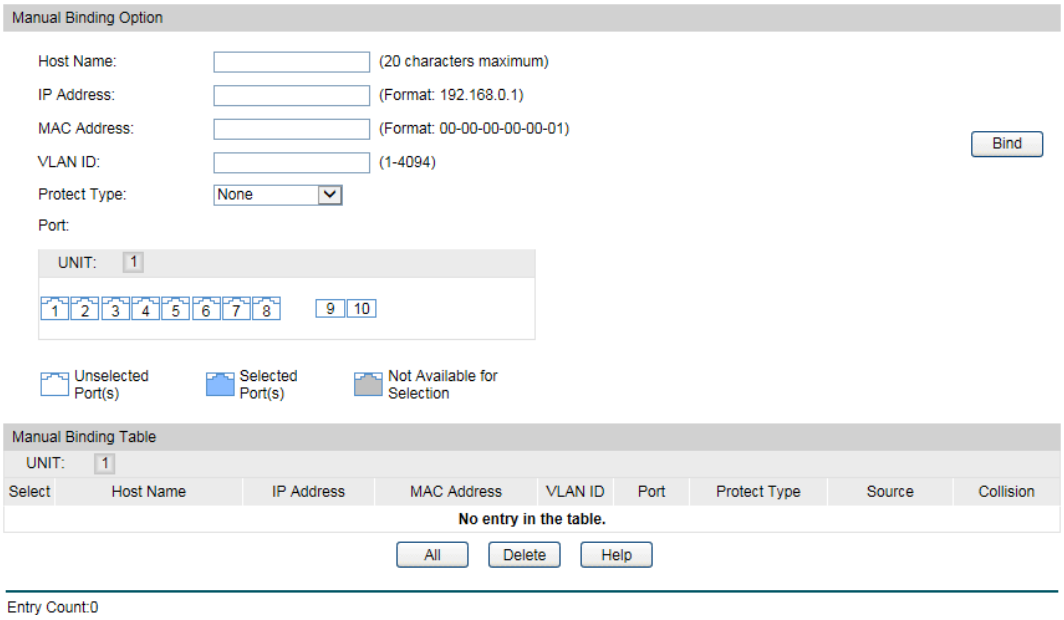


Figure 12-2 Manual Binding

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.

12.1.3 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.

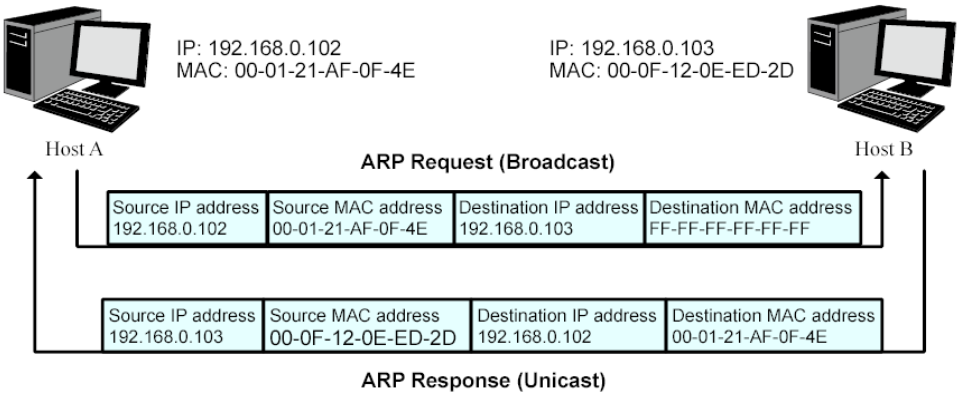


Figure 12-3 ARP Implementation Procedure

(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.

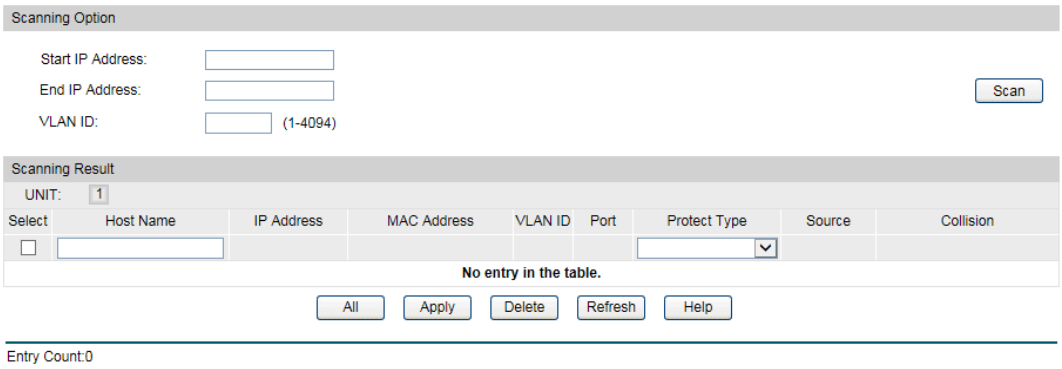


Figure 12-4 ARP Scanning

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.

12.2 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.

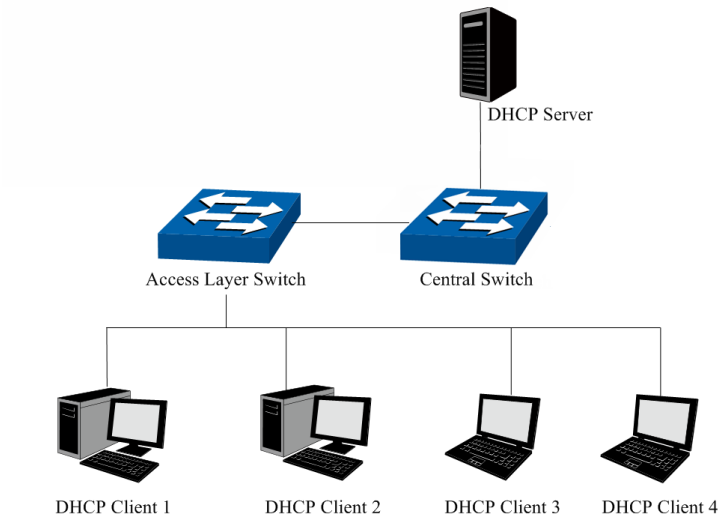


Figure 12-5 Network diagram for DHCP-snooping implementation

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.

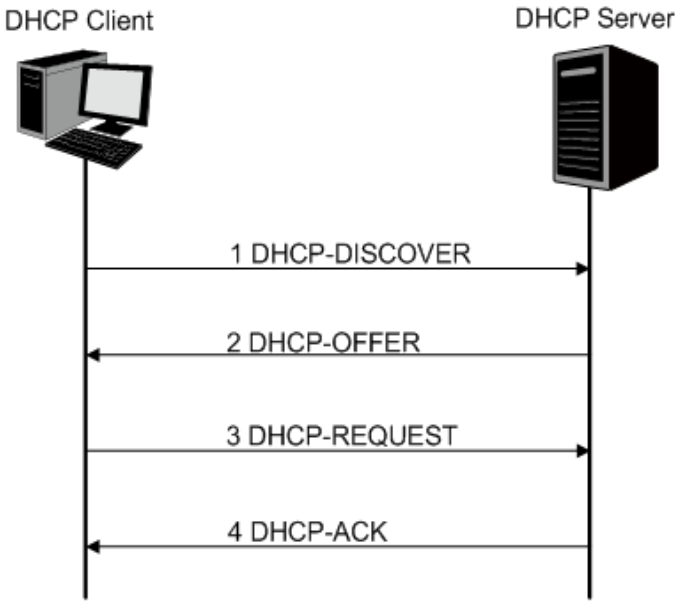


Figure 12-6 Interaction between a DHCP client and a DHCP server

(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.

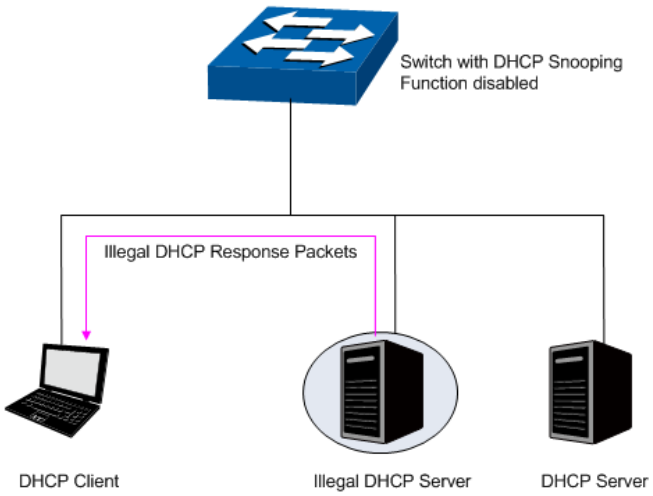


Figure 12-7 DHCP Cheating Attack Implementation Procedure

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.

12.2.1 Global Config

Choose the menu **Network Security→DHCP Snooping→Global Config** to load the following page.

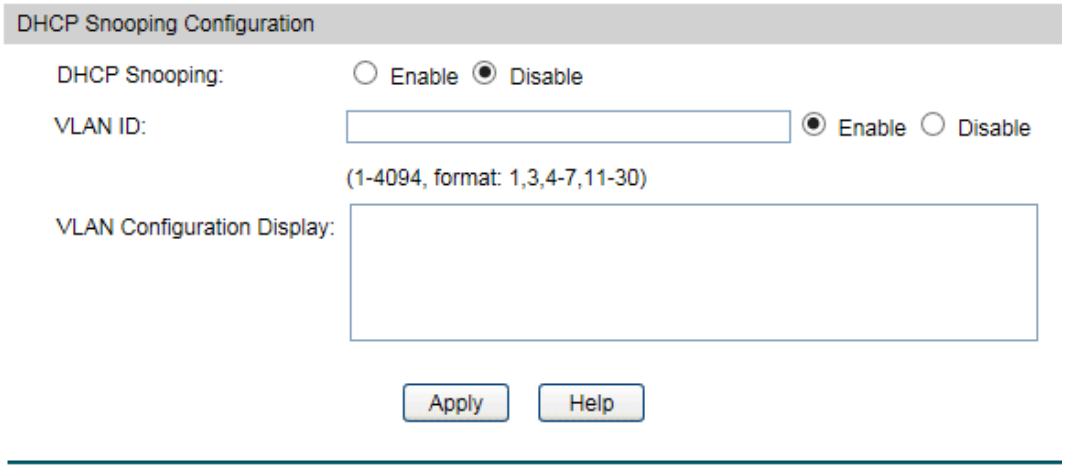


Figure 12-8 DHCP Snooping

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.

12.2.2 Port Config

Choose the menu **Network Security→DHCP Snooping→Port Config** to load the following page.

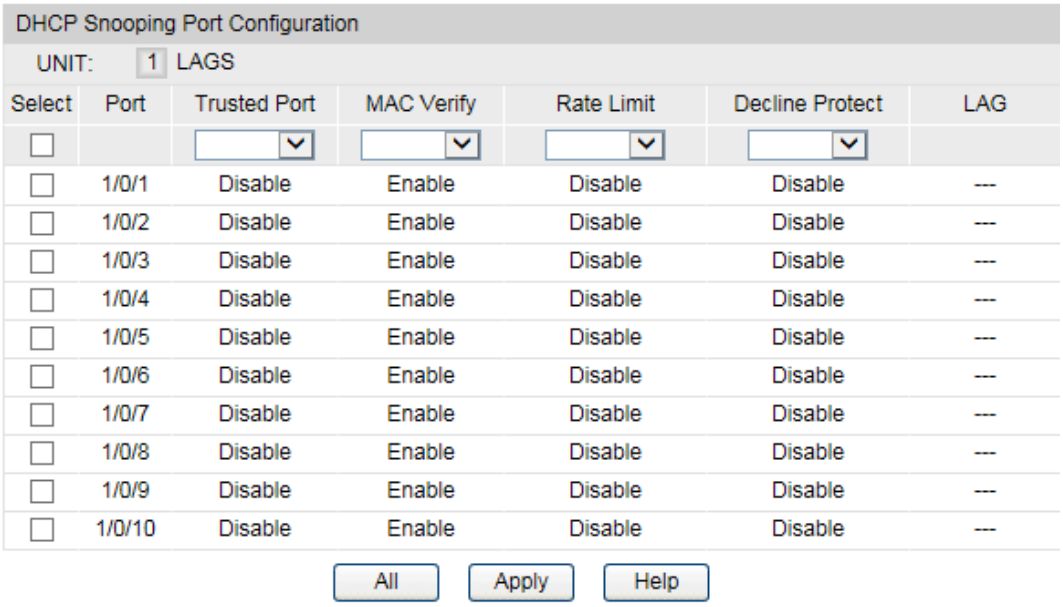


Figure 12-9 DHCP Snooping

➢ **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.

12.2.3 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.

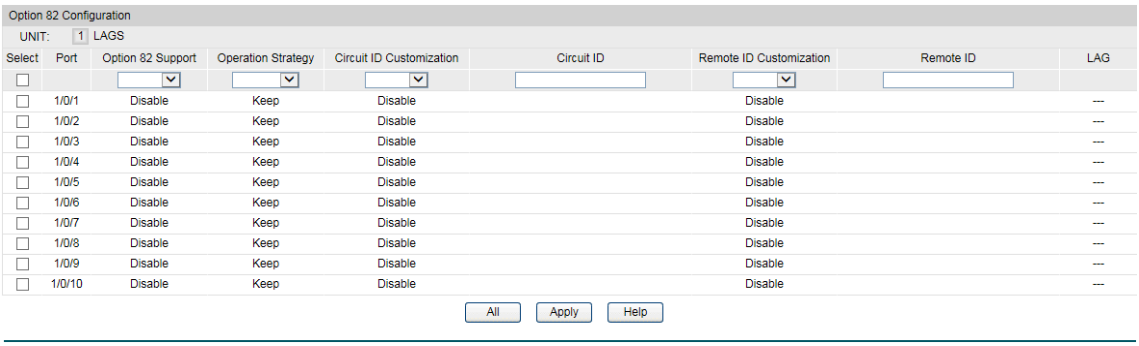


Figure 12-10 Option 82 Config

➢ **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.

12.3 ARP Inspection

According to the ARP Implementation Procedure stated in 12.1.3 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.

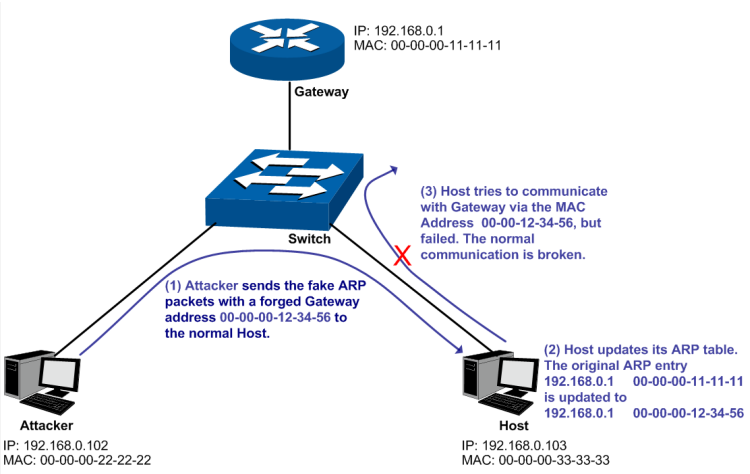


Figure 12-11 ARP Attack - Imitating Gateway

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.

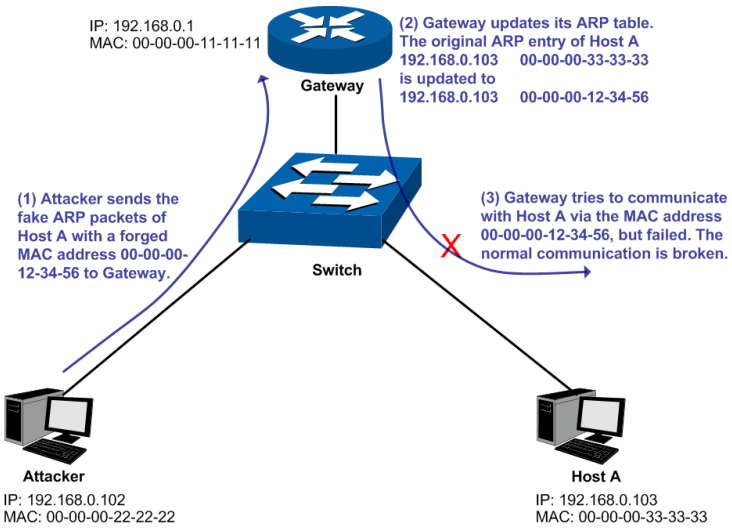


Figure 12-12 ARP Attack – Cheating Gateway

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.

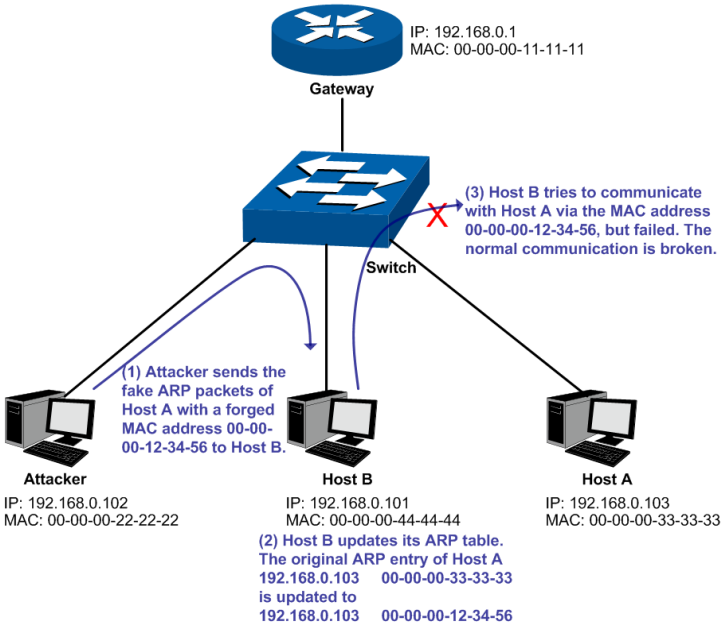


Figure 12-13 ARP Attack – Cheating Terminal Hosts

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.

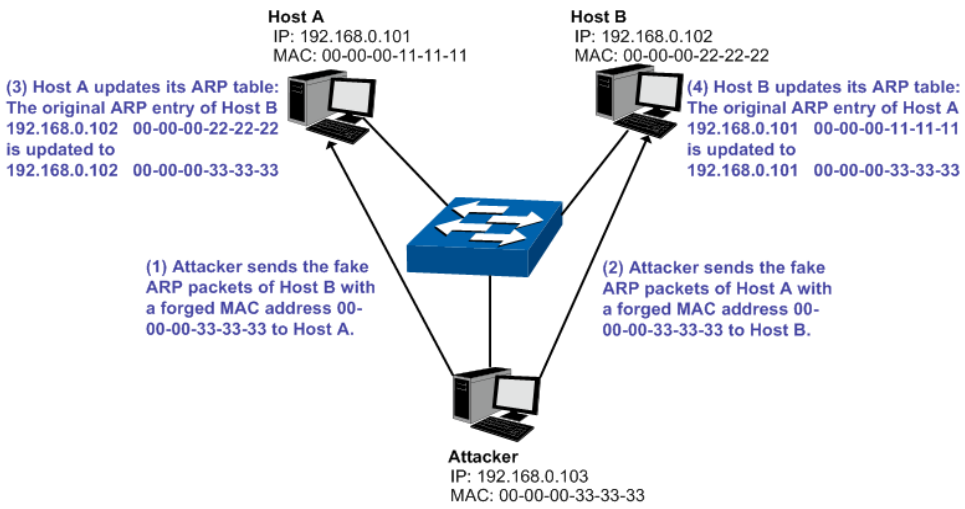


Figure 12-14 Man-In-The-Middle Attack

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.

12.3.1 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.

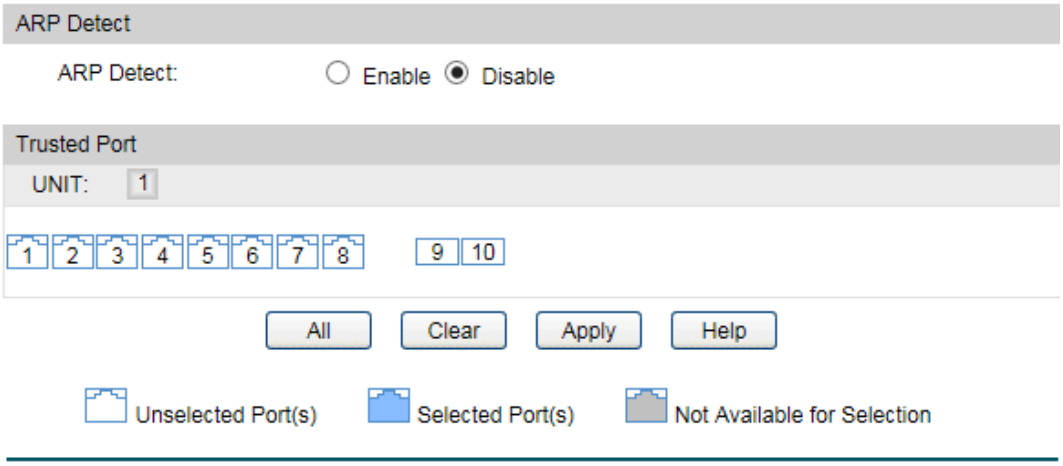


Figure 12-15 ARP Detect

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.

Step	Operation	Description
4	Enable ARP Detect feature.	Required. On the **Network Security→ARP Inspection→ARP Detect** page, enable the ARP Detect feature.

12.3.2 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.

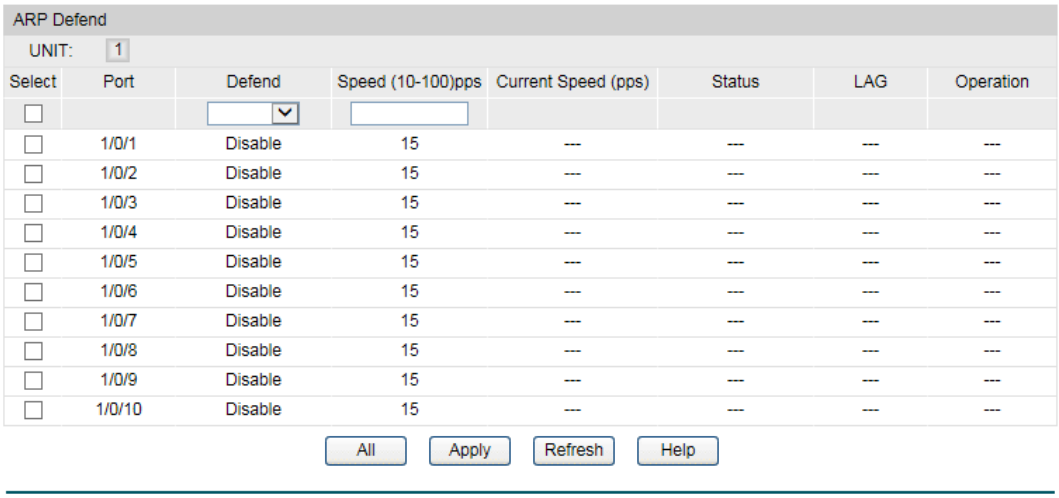


Figure 12-16 ARP Defend

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:

1. It's not recommended to enable the ARP Defend feature for the LAG member port.

2. ARP Detect and ARP Defend cannot be enabled at the same time.

12.3.3 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.

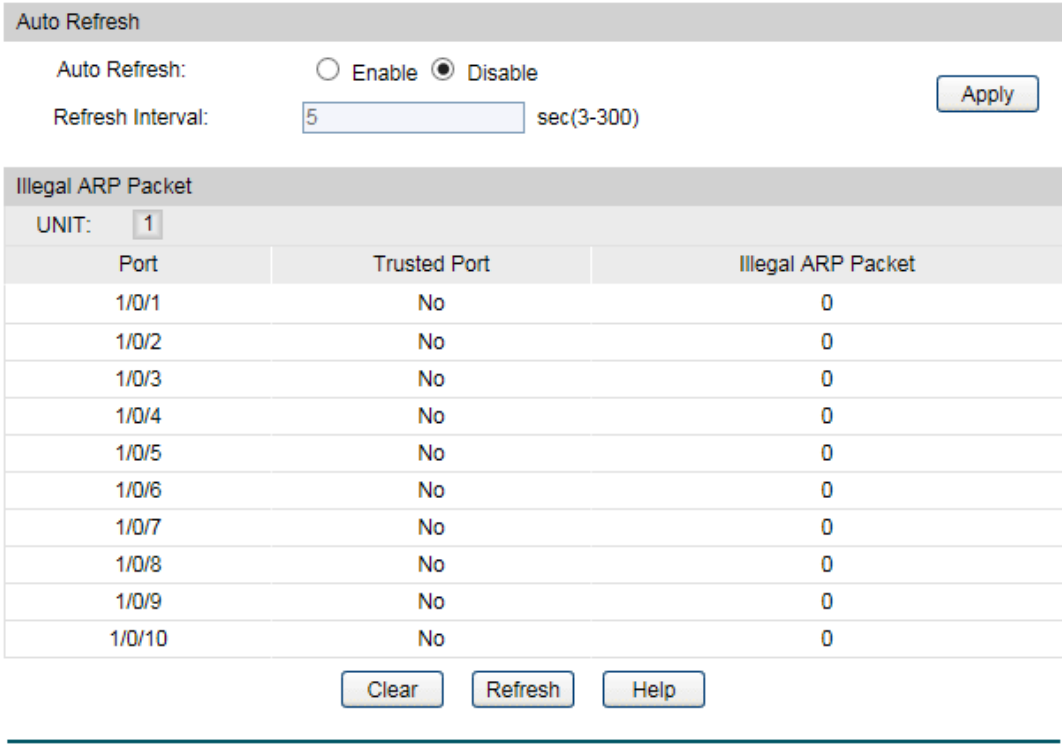


Figure 12-17 ARP Statistics

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.

12.4 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 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 12-1 Defendable DoS Attack Types

12.4.1 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.

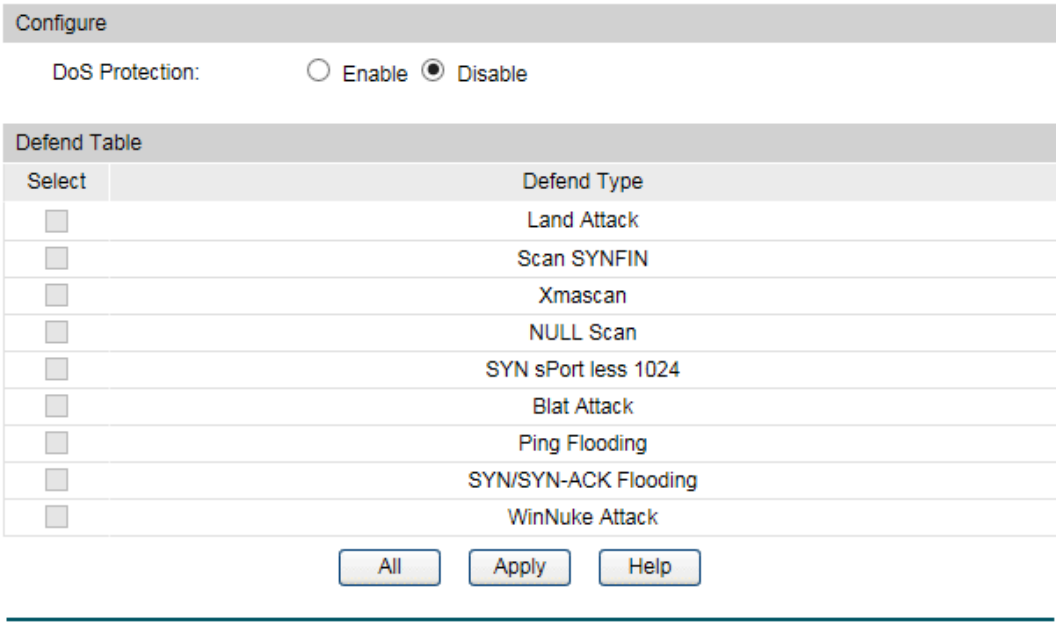


Figure 12-18 DoS Defend

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.

12.5 802.1X

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.

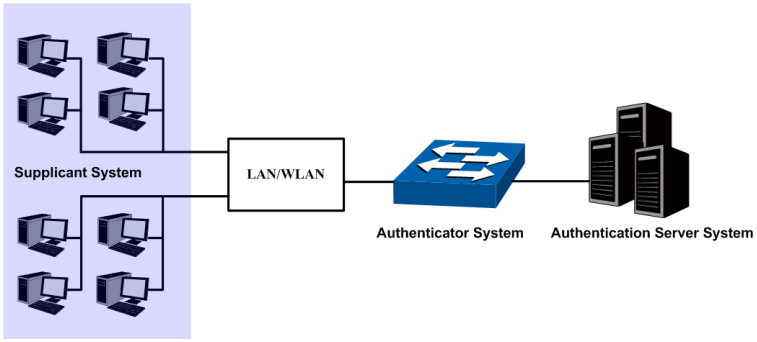


Figure 12-19 Architecture of 802.1X authentication

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 TP-Link 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 TP-Link 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.

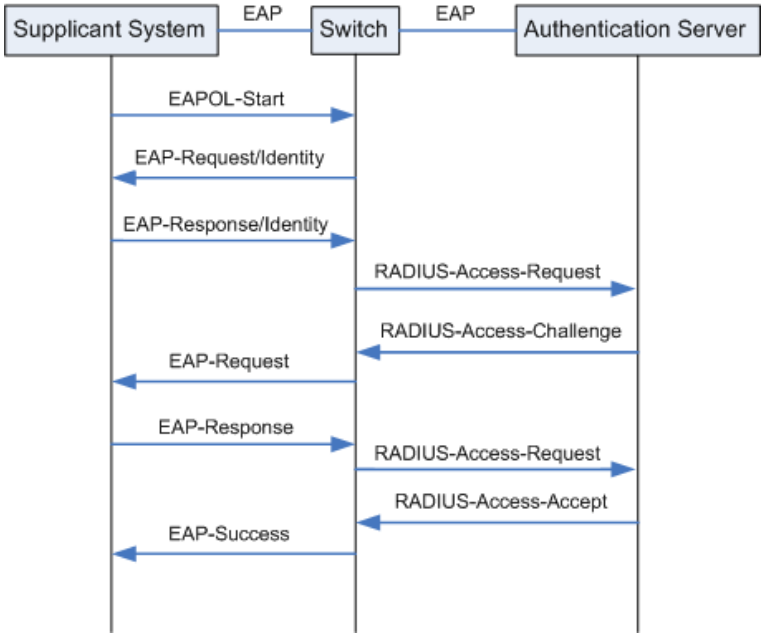


Figure 12-20 EAP-MD5 Authentication Procedure

(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.

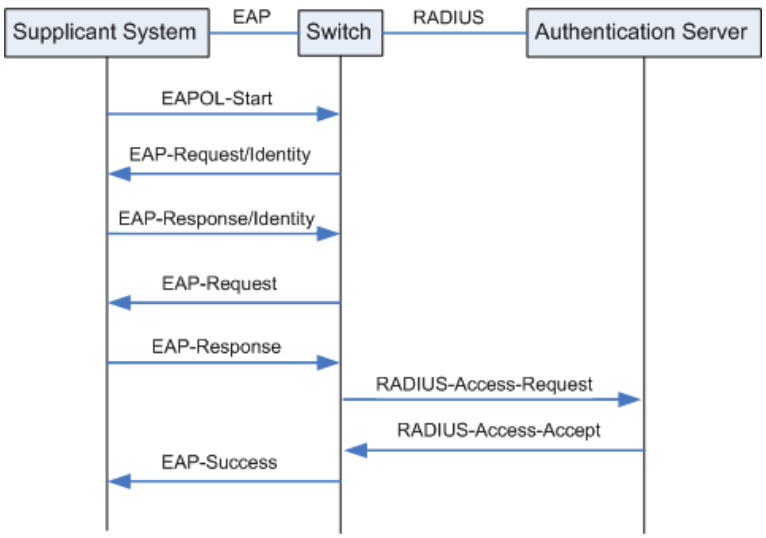


Figure 12-21 PAP Authentication Procedure

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.

12.5.1 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 instead of TP-Link 802.1X Client.

Choose the menu **Network Security→802.1X→Global Config** to load the following page.

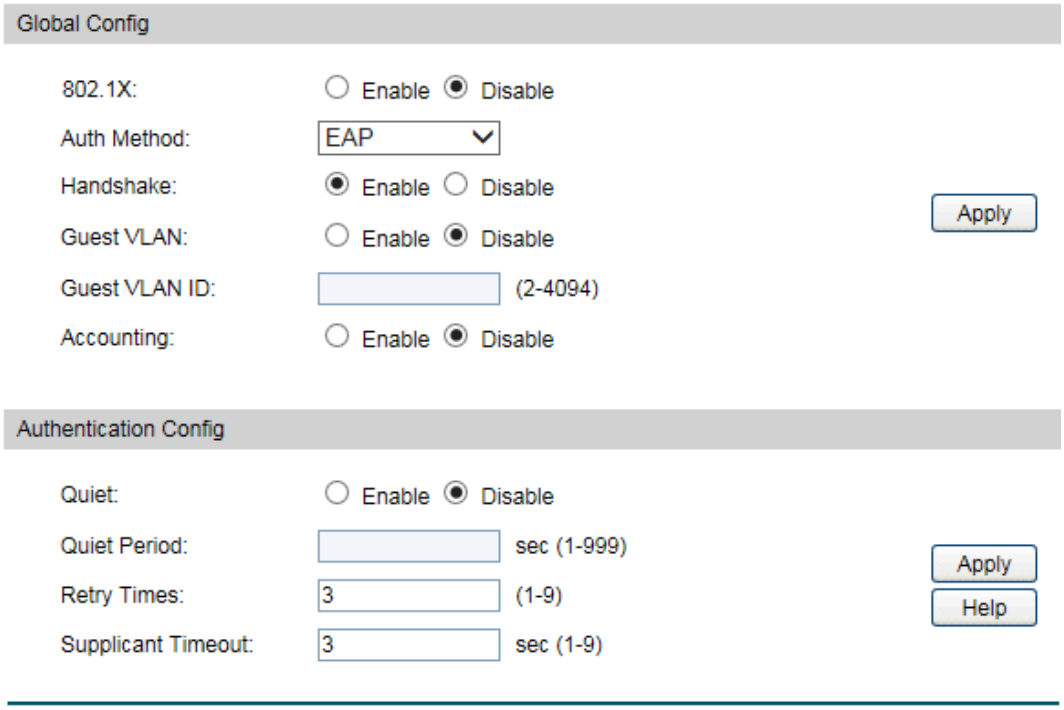


Figure 12-22 Global Config

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 TP-Link 802.1X Client and the switch. Please disable Handshake feature if you are using other client softwares instead of TP-Link 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.

12.5.2 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.

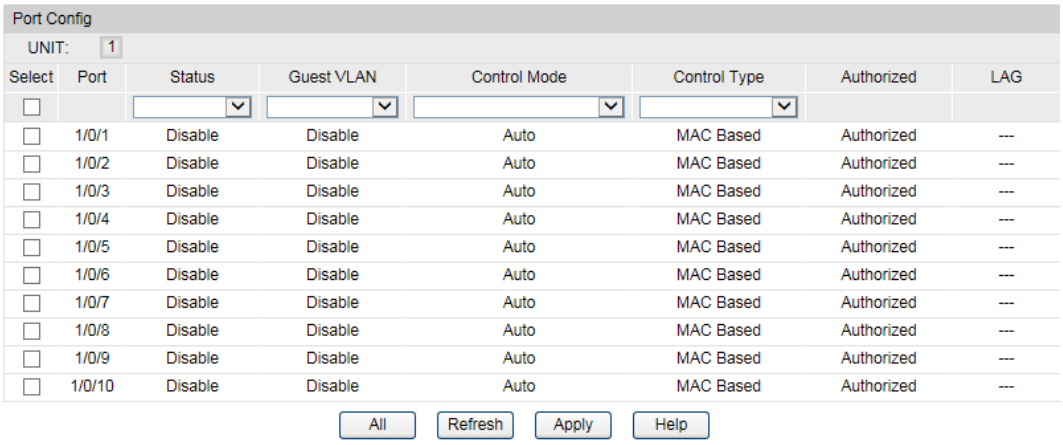


Figure 12-23 Port Config

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 TP-Link 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.

12.6 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.

12.6.1 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 12-24 AAA Global Config

➢ **Configuration Procedure**

Click Enable to enable the AAA function globally.

12.6.2 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 12-25 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 admin** in the Command Line Interface Guide on the resource CD.

12.6.3 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.

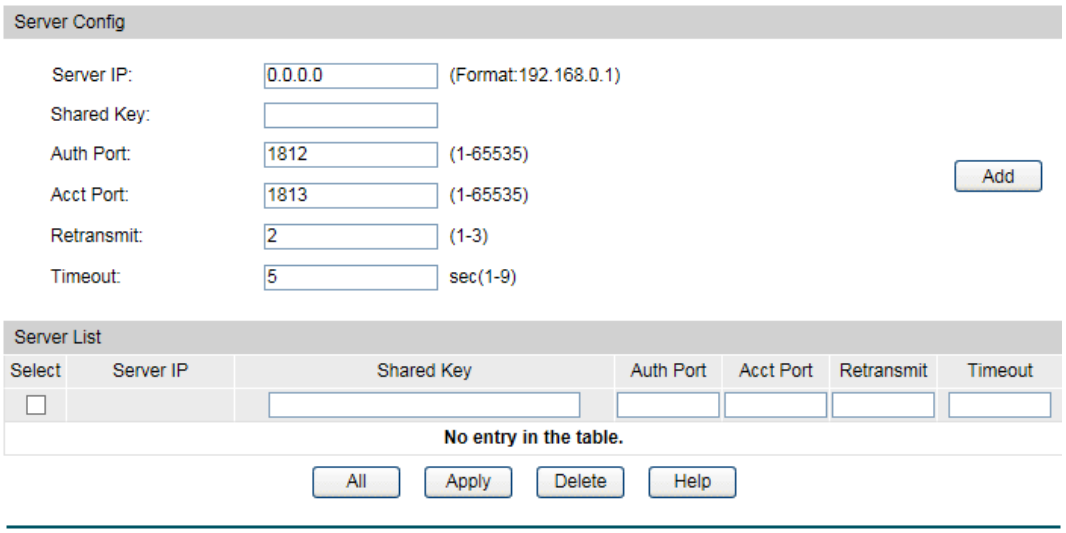


Figure 12-26 RADIUS Server Config

➢ **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.

12.6.4 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.

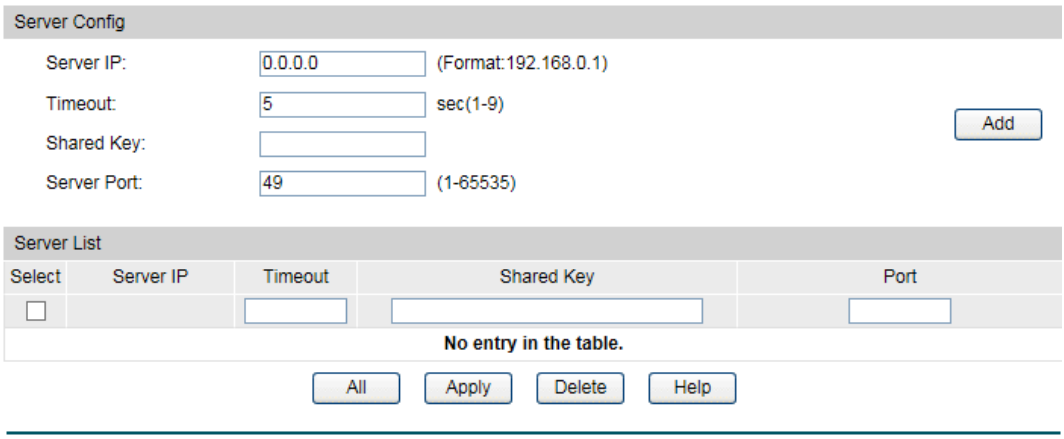


Figure 12-27 TACACS+ Server Config

➢ **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.

12.6.5 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.

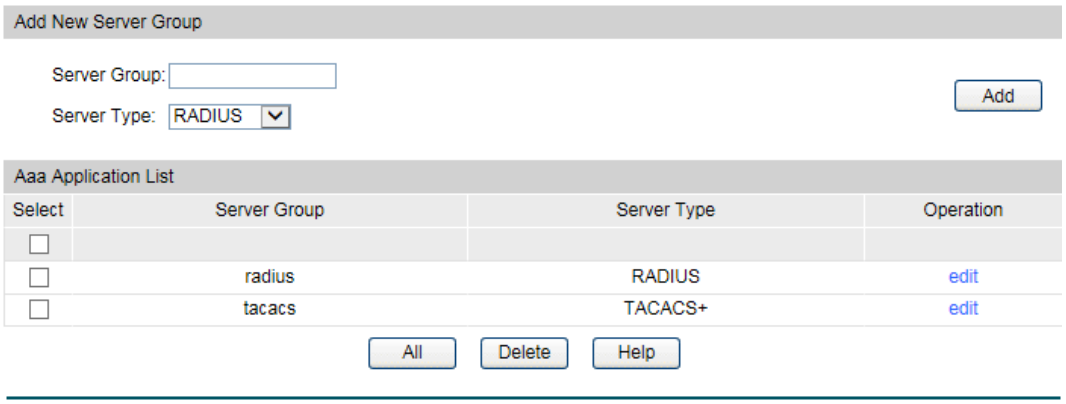


Figure 12-28 Create New Server Group

Figure 12-29 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 12-29)

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.

12.6.6 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.

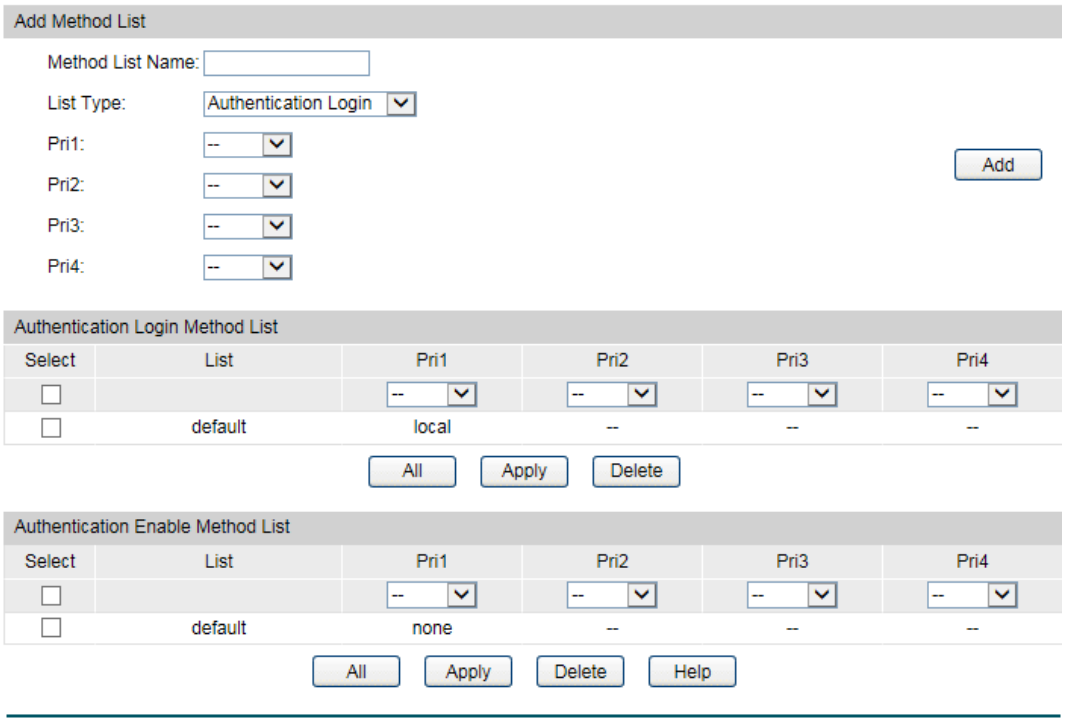


Figure 12-30 Authentication Method List Config

➢ **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 $enable$.

12.6.7 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.

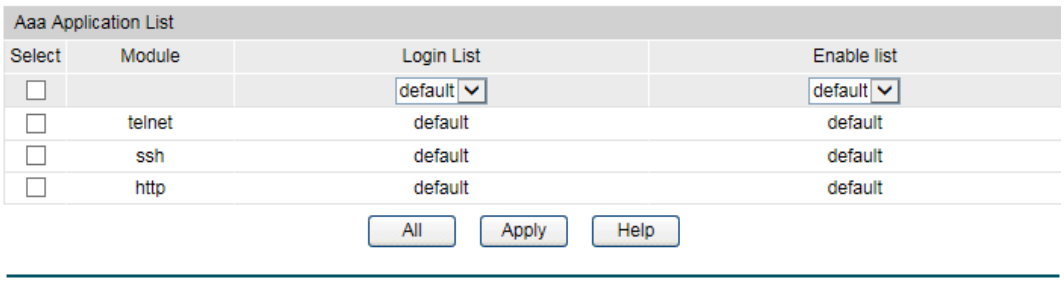


Figure 12-31 Application Authentication Settings

➢ **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.

12.6.8 802.1X 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.

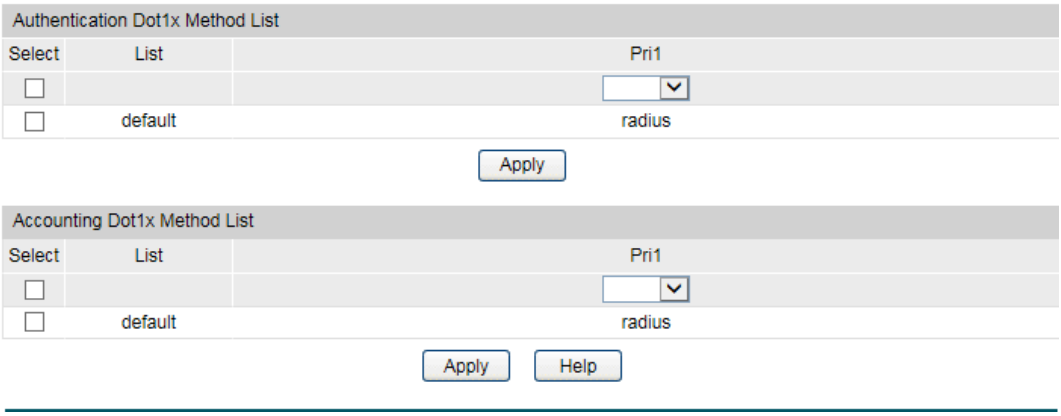


Figure 12-32 802.1X Config

➢ **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.

12.6.9 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 13 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.

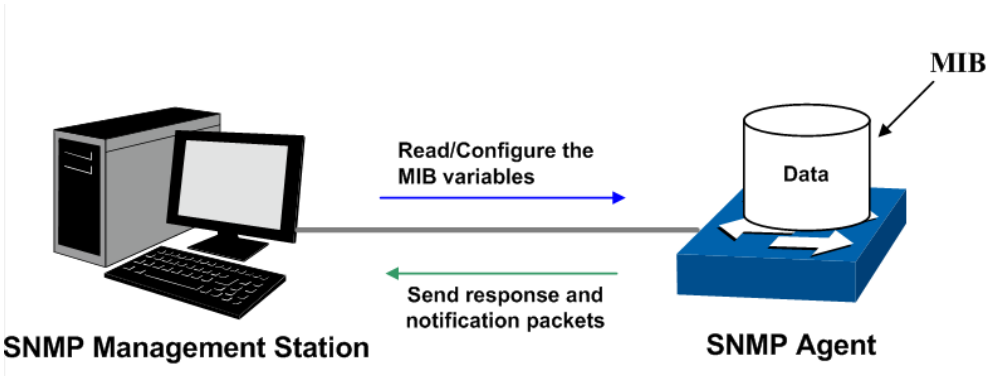


Figure 13-1 Relationship among SNMP Network Elements

➢ **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}.

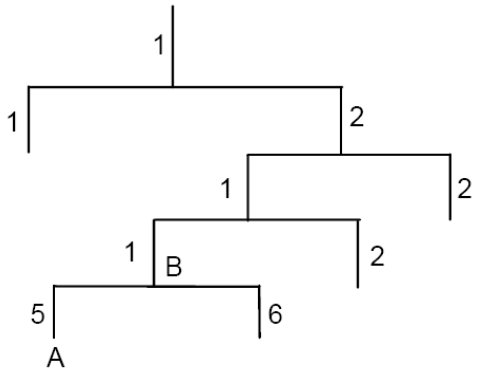


Figure 13-2 Architecture of the MIB tree

➢ **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**.

13.1 SNMP Config

The **SNMP Config** can be implemented on the **Global Config**, **SNMP View**, **SNMP Group**, **SNMP User** and **SNMP Community** pages.

13.1.1 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.

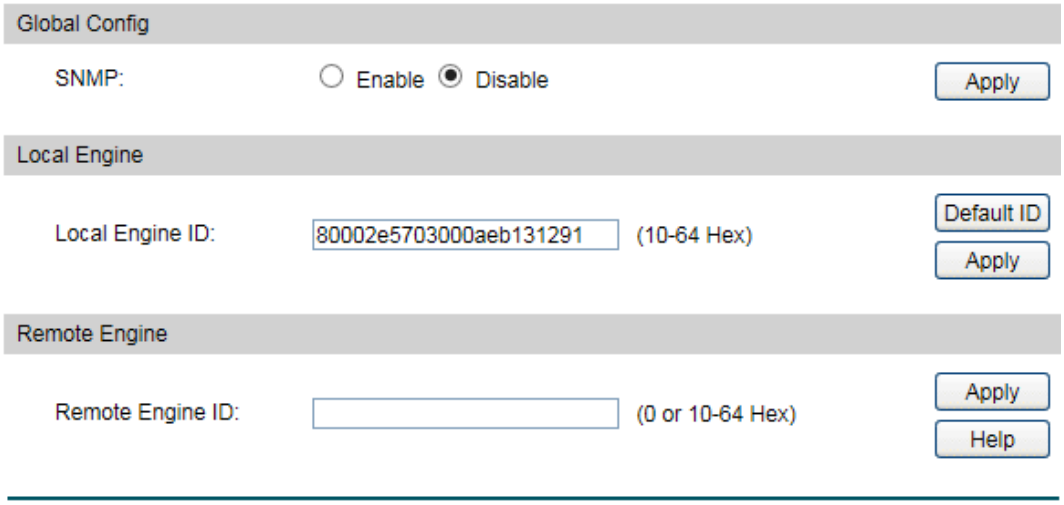


Figure 13-3 Global Config

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.

13.1.2 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.

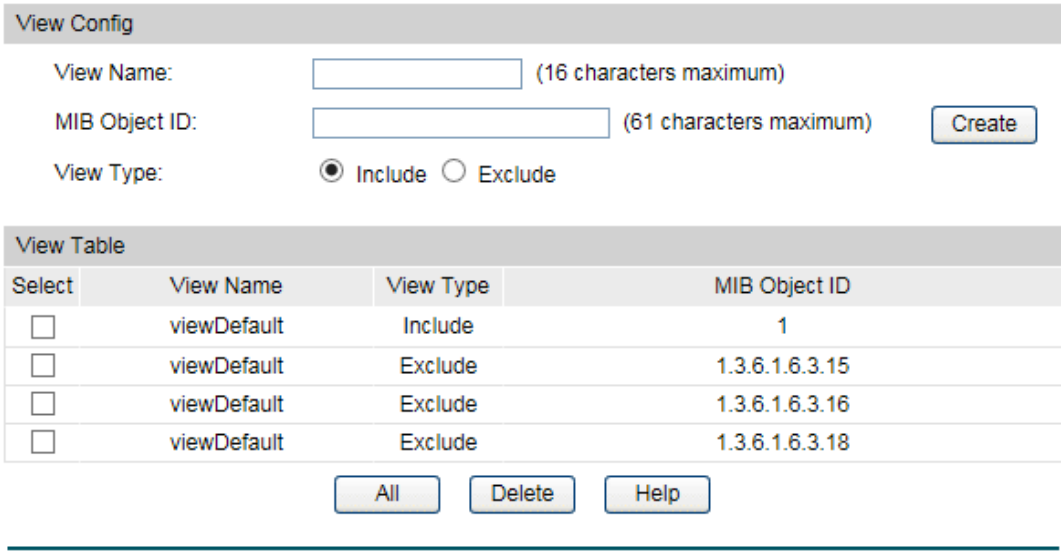


Figure 13-4 SNMP View

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.

13.1.3 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.

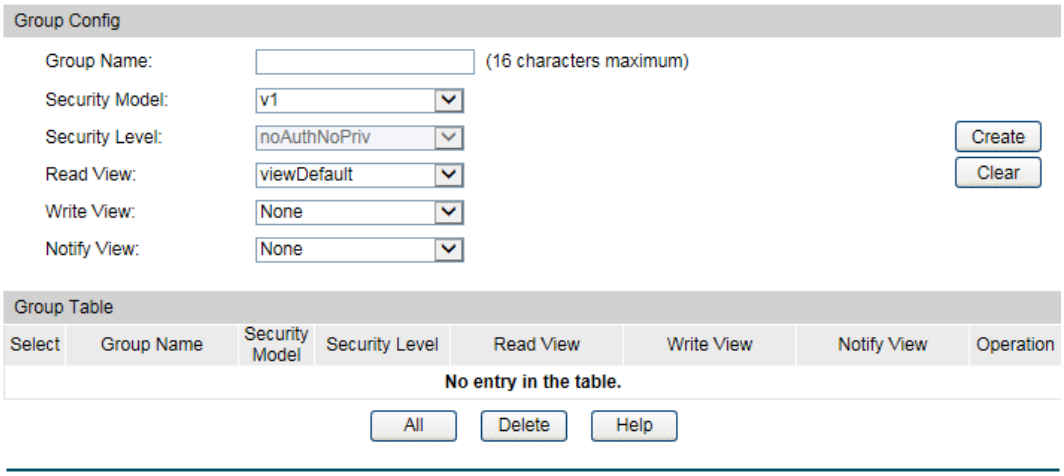


Figure 13-5 SNMP Group

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.

13.1.4 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.

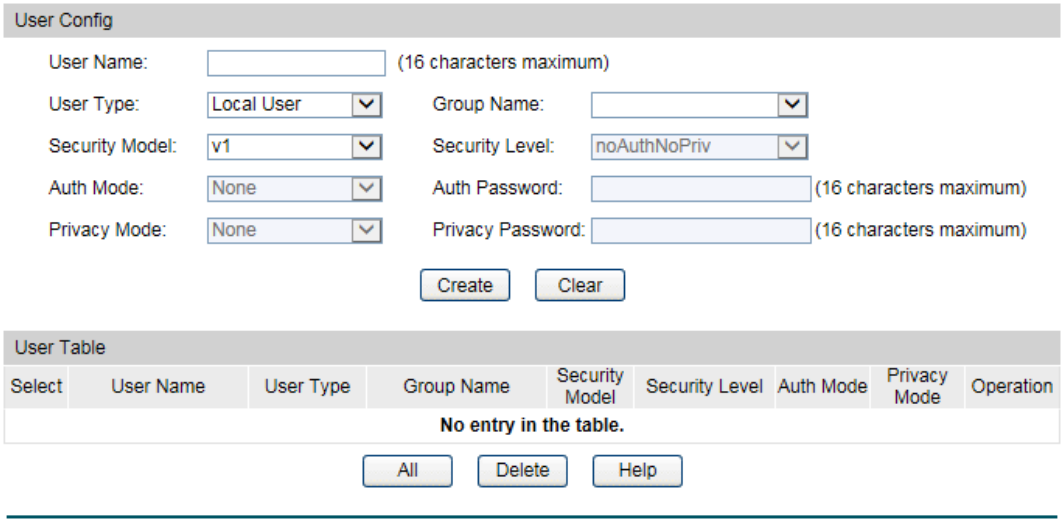


Figure 13-6 SNMP User

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.

13.1.5 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.

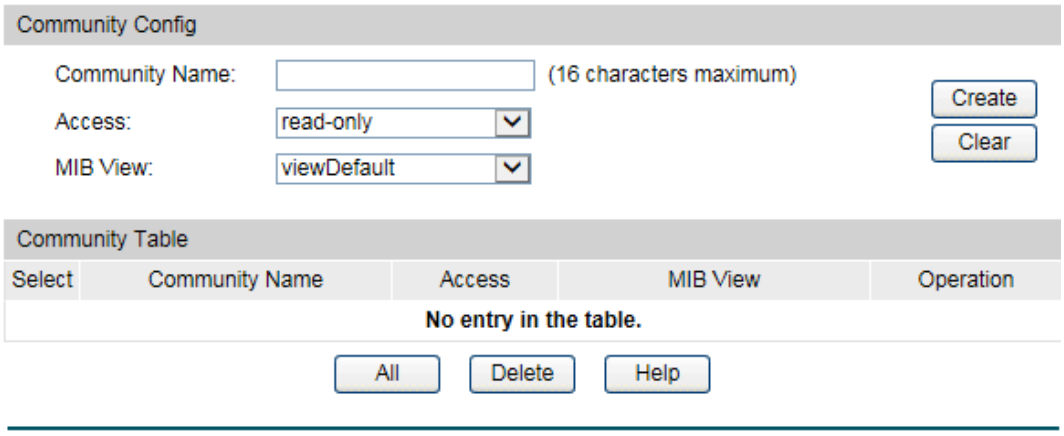


Figure 13-7 SNMP Community

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.

Step	Operation	Description
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.	

13.2 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** to load the following page.

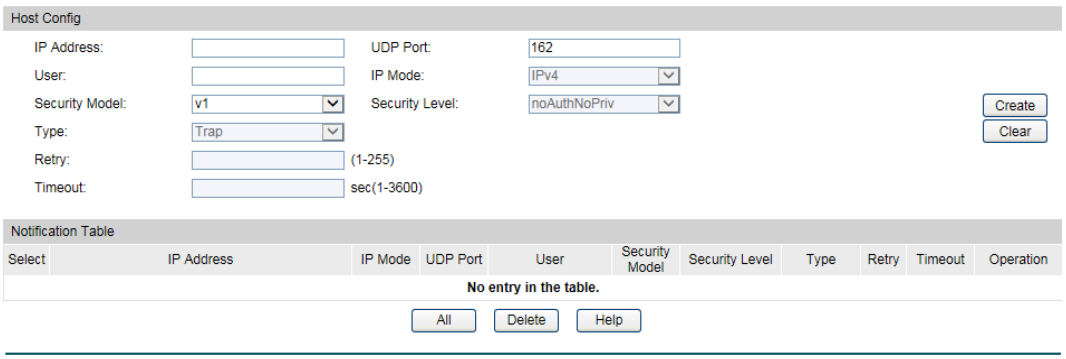


Figure 13-8 Notification Config

The following entries are displayed on this screen:

➢ **Create Notification**

IP Address: Enter the IP Address of the management Host.

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.

User: Enter the User name of the management station.

IP Mode: Select the IP mode of the IP address.

Security Model: Select the Security Model of the management station.

Security Level: Select the Security Level for the SNMP v3 User.

- **noAuthNoPriv:** No authentication and no privacy security level are used.
- **authNoPriv:** Only the authentication security level is used.
- **authPriv:** Both the authentication and the privacy security levels are used.

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.

➢ **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.

Timeout: Displays the maximum time for the switch to wait for the response from the management station before resending a request.

Retry: Displays the amount of times the switch resends an inform request.

Operation: Click the **Edit** button to modify the corresponding entry and click the **Modify** button to apply.

13.3 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.
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.

13.3.1 Statistics

On this page you can configure and view the statistics entry.

Choose the menu **SNMP→RMON→Statistics** to load the following page.

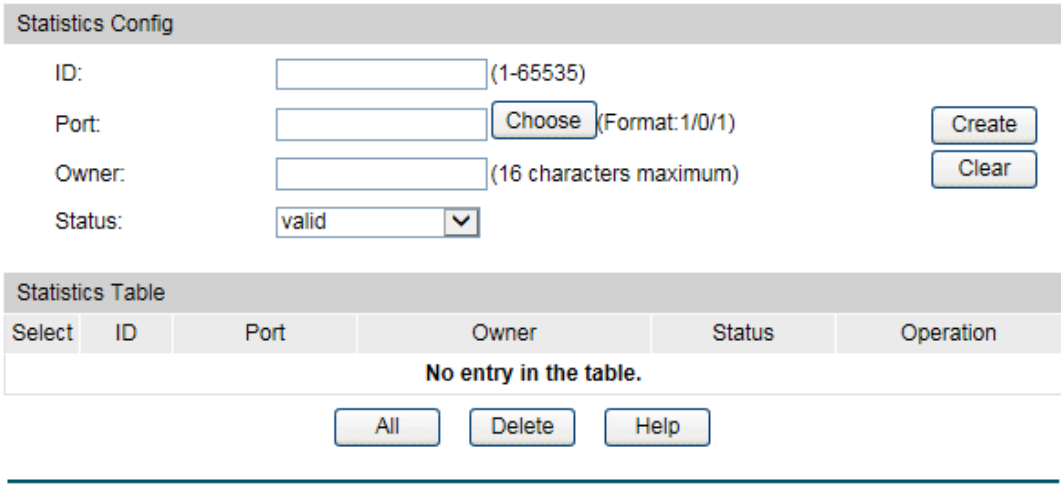


Figure 13-9 Statistics

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.

13.3.2 History

On this page, you can configure the History Group for RMON.

Choose the menu **SNMP→RMON→History** to load the following page.

History Control Table

Select	Index	Port	Interval(sec)	Max Buckets	Owner	Status
☐						
☐	1	1/0/1	1800	50	monitor	Disable
☐	2	1/0/1	1800	50	monitor	Disable
☐	3	1/0/1	1800	50	monitor	Disable
☐	4	1/0/1	1800	50	monitor	Disable
☐	5	1/0/1	1800	50	monitor	Disable
☐	6	1/0/1	1800	50	monitor	Disable
☐	7	1/0/1	1800	50	monitor	Disable
☐	8	1/0/1	1800	50	monitor	Disable
☐	9	1/0/1	1800	50	monitor	Disable
☐	10	1/0/1	1800	50	monitor	Disable
☐	11	1/0/1	1800	50	monitor	Disable
☐	12	1/0/1	1800	50	monitor	Disable

All Apply Help

Figure 13-10 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.

13.3.3 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 13-11 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.

13.3.4 Alarm

On this page, you can configure Statistic Group and Alarm Group for RMON.

Choose the menu **SNMP→RMON→Alarm** to load the following page.

Alarm Config

Select	Index	Variable	Statistics	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Alarm Type	Interval(sec)	Owner	Status
☐												
☐	1	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	2	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	3	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	4	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	5	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	6	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	7	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	8	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	9	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	10	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	11	RecBytes		Absolute	100		100		All	1800	monitor	Disable
☐	12	RecBytes		Absolute	100		100		All	1800	monitor	Disable

All Apply Help

Figure 13-12 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 14 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).

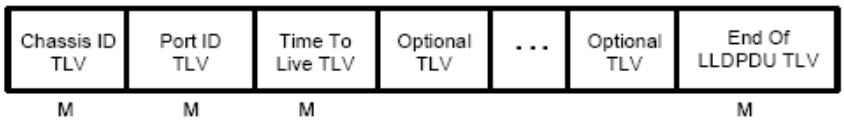
An IETF Standard MIB, as well as a number of vendor specific MIBs, have been created to describe a network's physical topology and associated systems within that topology. However, there is no standard protocol for populating these MIBs or communicating this information among stations on the IEEE 802 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.

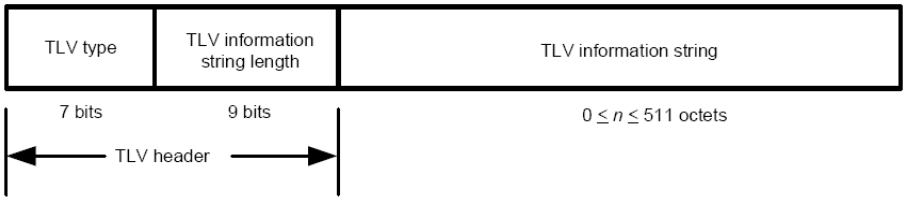
3) LLDPDU receipt mechanism

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 TP-Link switch, the following LLDP optional TLVs are supported.

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**.

14.1 Basic Config

LLDP is configured on the **Global Config** and **Port Config** pages.

14.1.1 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.

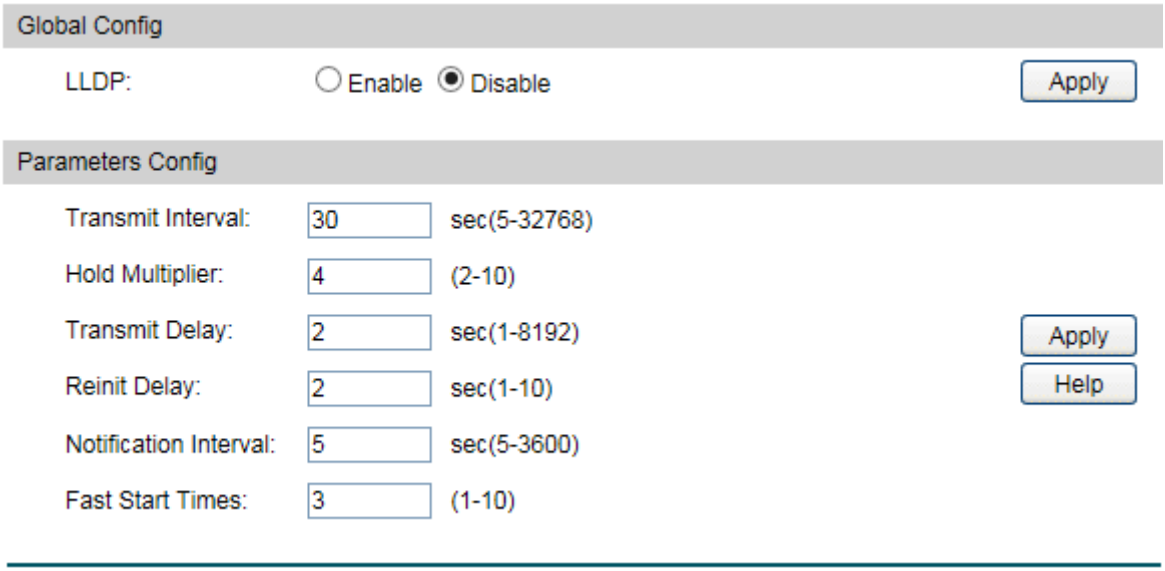


Figure 14-1 LLDP Global Configuration

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.

  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.

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 3.

Notification Interval: Specify the interval of Trap message which will be sent from local device to network management system. The default value is 5.

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.

14.1.2 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.

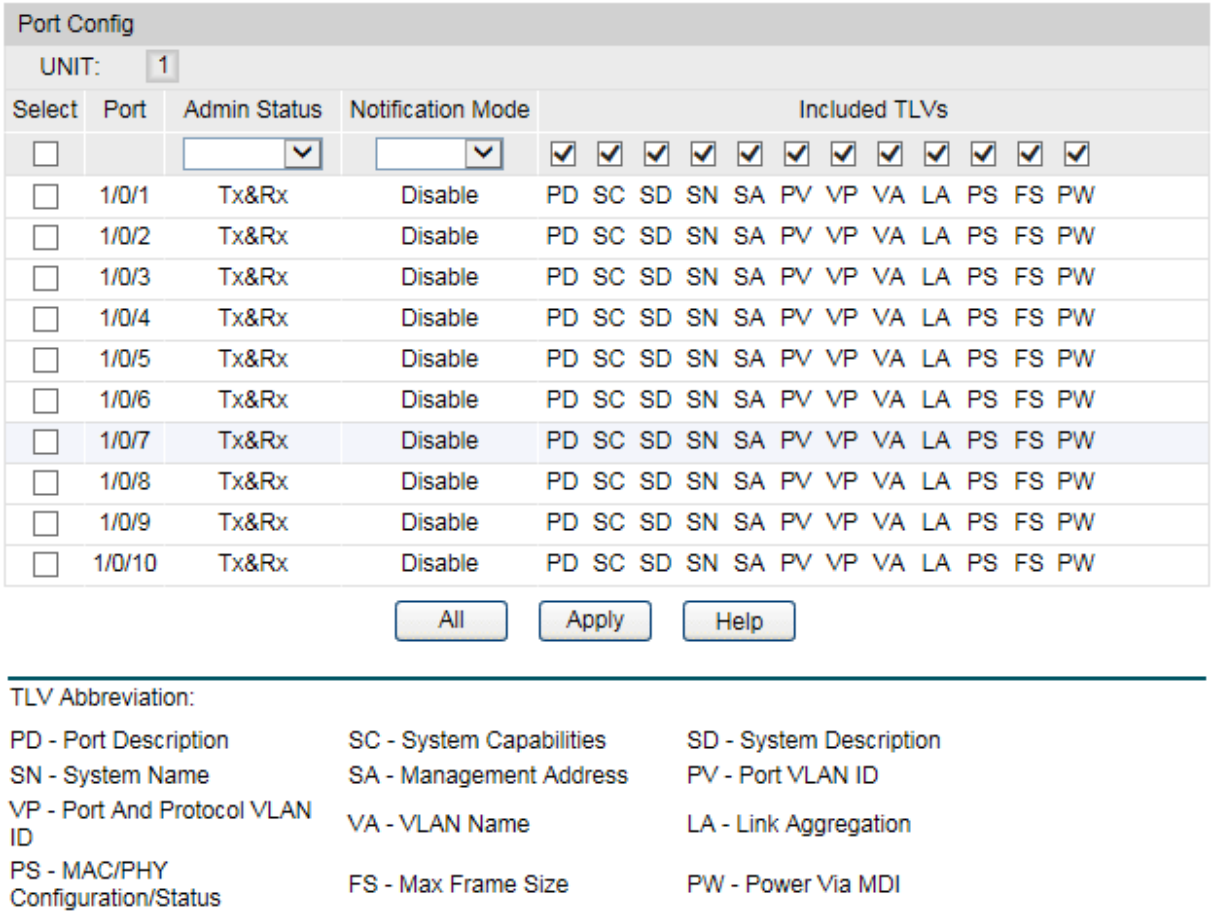


Figure 14-2 LLDP Port Config

The following entries are displayed on this screen:

- **LLDP Port Config**

Port Select:	Select the desired port 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.

14.2 Device Info

You can view the LLDP information of the local device and its neighbors on the **Local Info** and **Neighbor Info** pages respectively.

14.2.1 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.

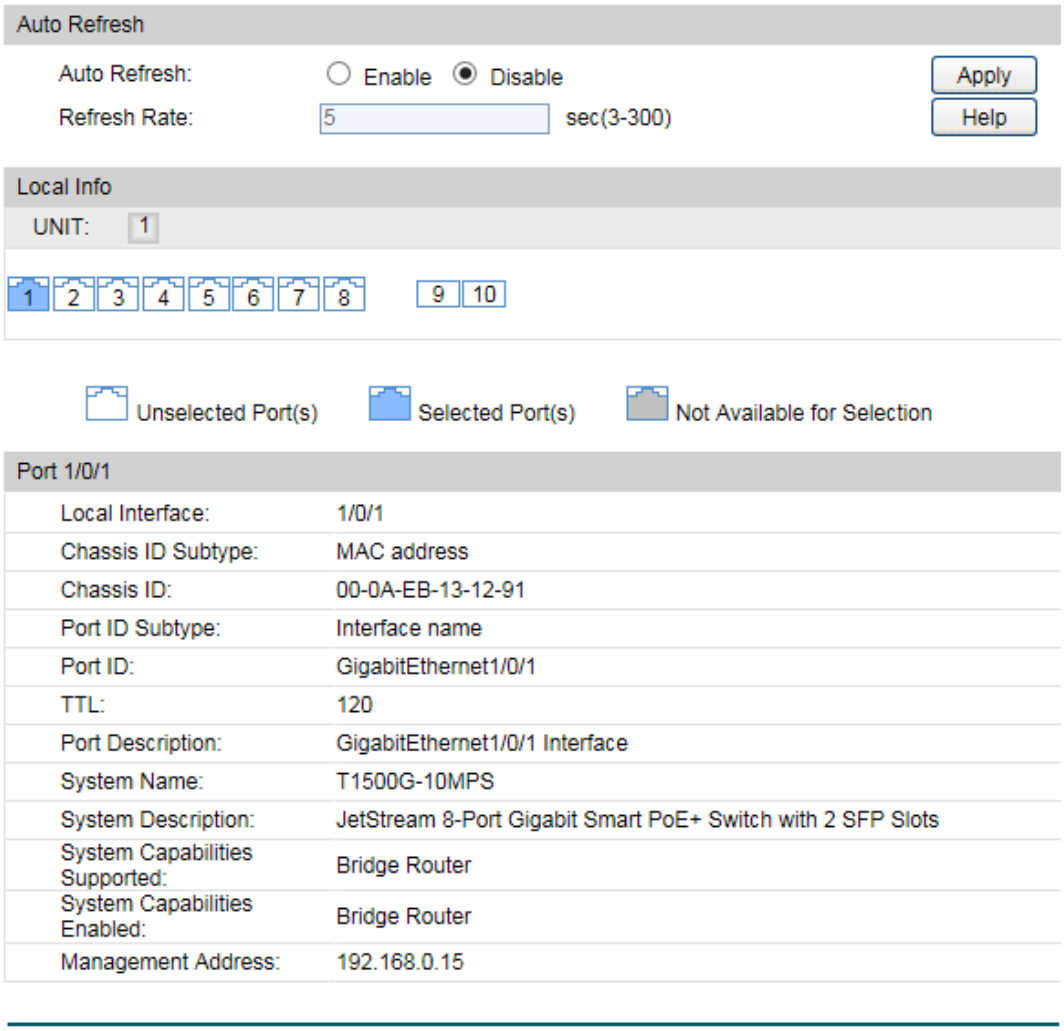


Figure 14-3 LLDP Local Information

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.

14.2.2 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.

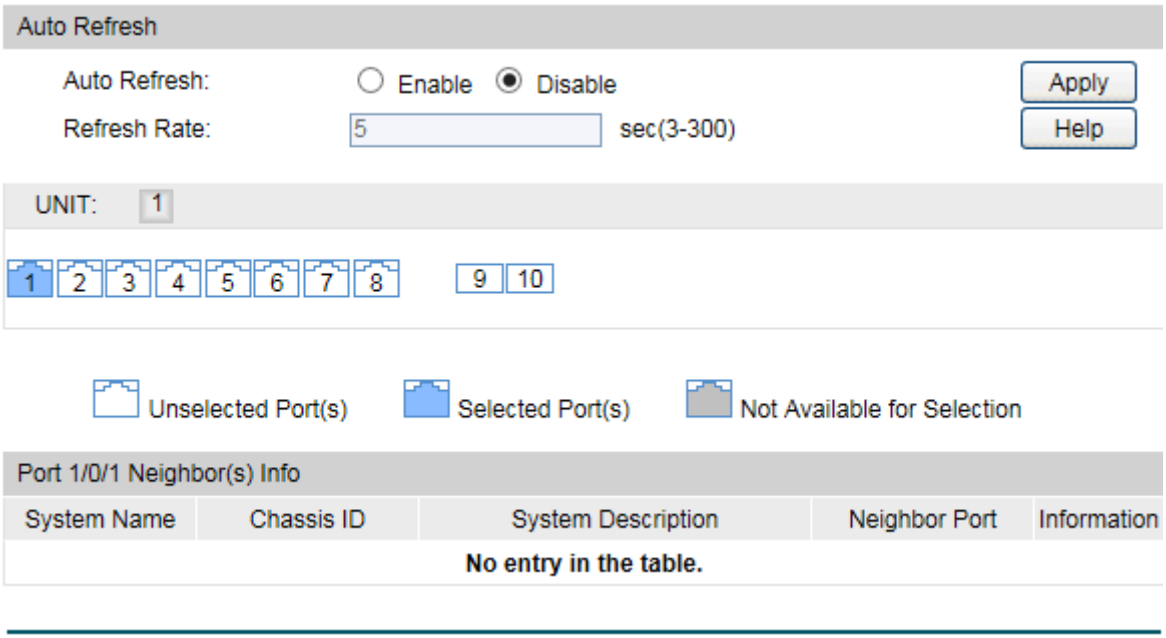


Figure 14-4 LLDP Neighbor Information

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**

Port Select: Select one port to display its neighbor information.

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.

System Name: Displays the system name of the neighbor device.

14.3 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.

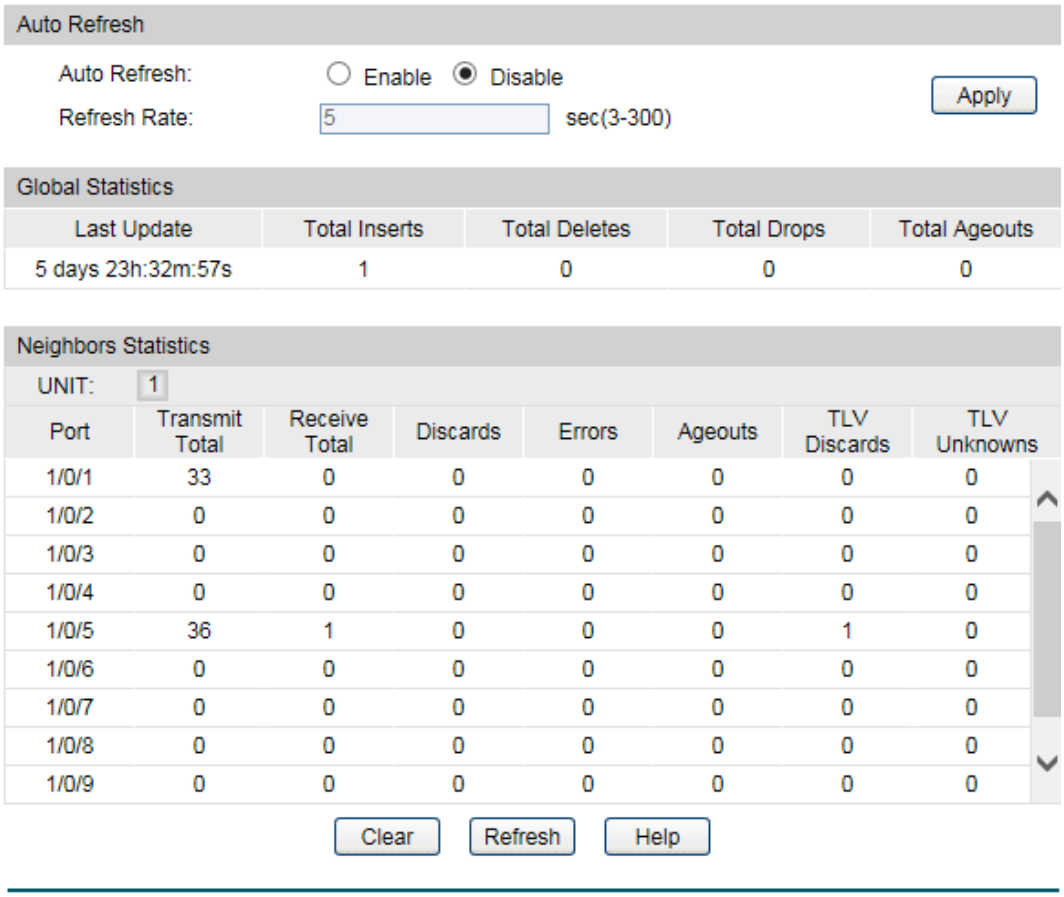


Figure 14-5 LLDP Statistic Information

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 Select:	Click the **Select** button to quick-select the corresponding port based on the port number you entered.
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.

14.4 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.

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.

14.4.1 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.

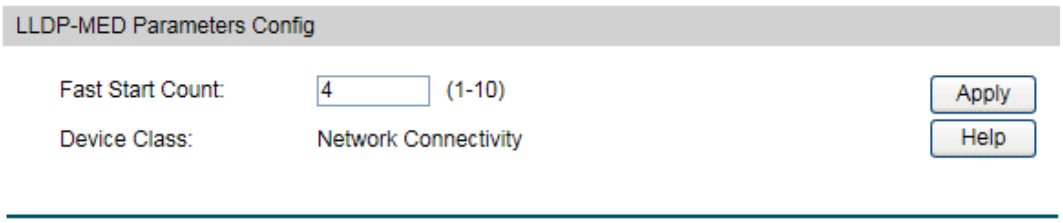


Figure 14-6 LLDP-MED Global Configuration

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.

14.4.2 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.

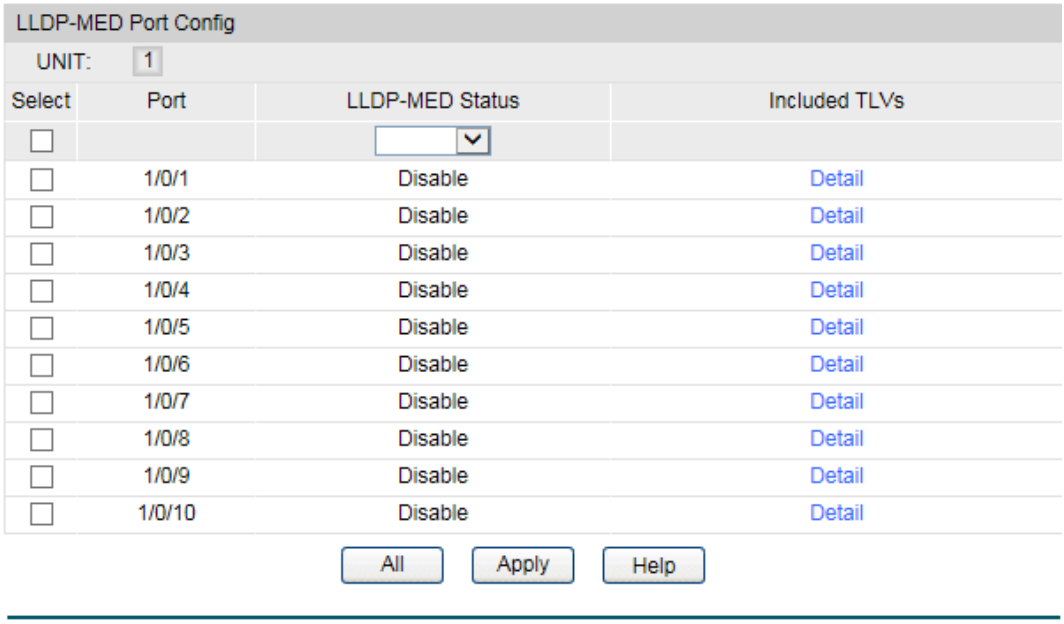


Figure 14-7 LLDP-MED Port Configuration

The following entries are displayed on this screen:

➢ **LLDP-MED Port Config**

Port: Displays local device's port number.

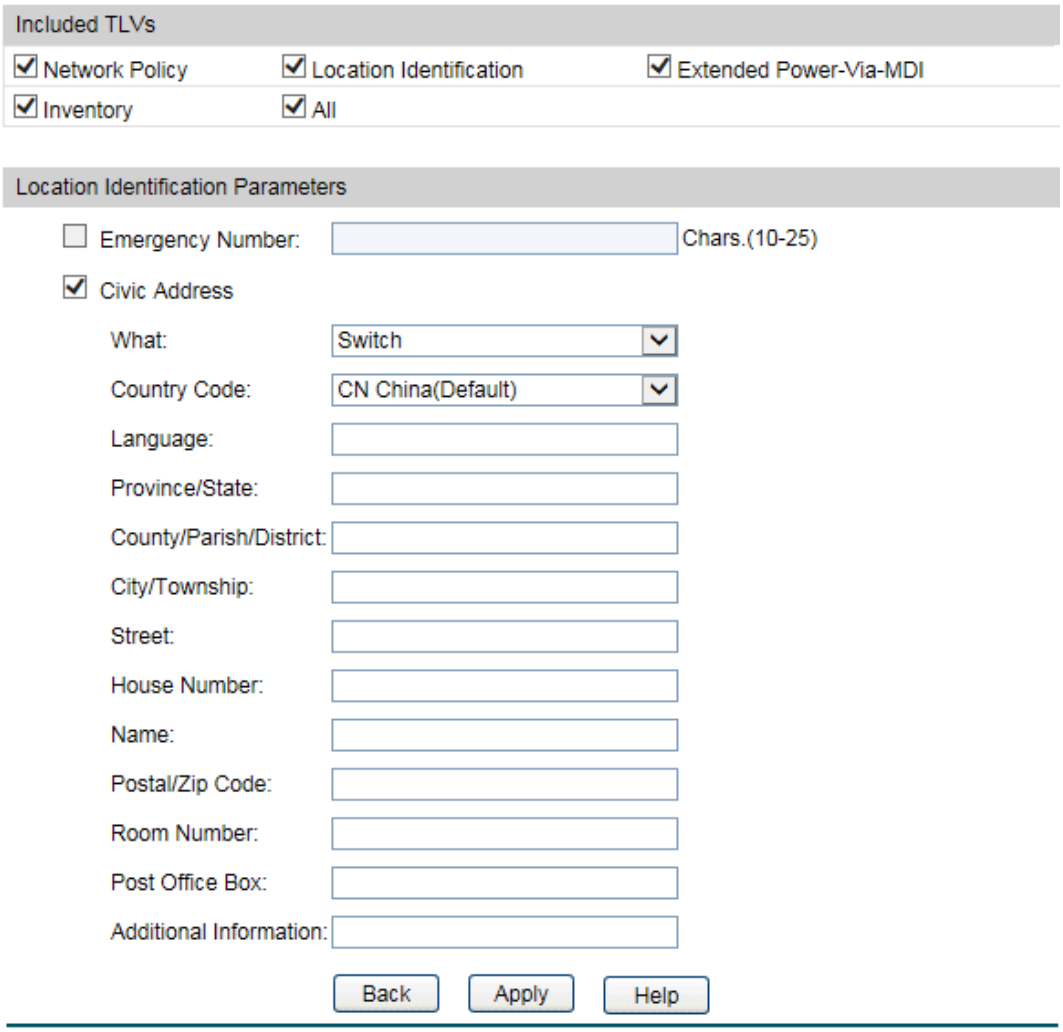
LLDP-MED Status: Configure the port's LLDP-MED status:

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.

14.4.3 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.

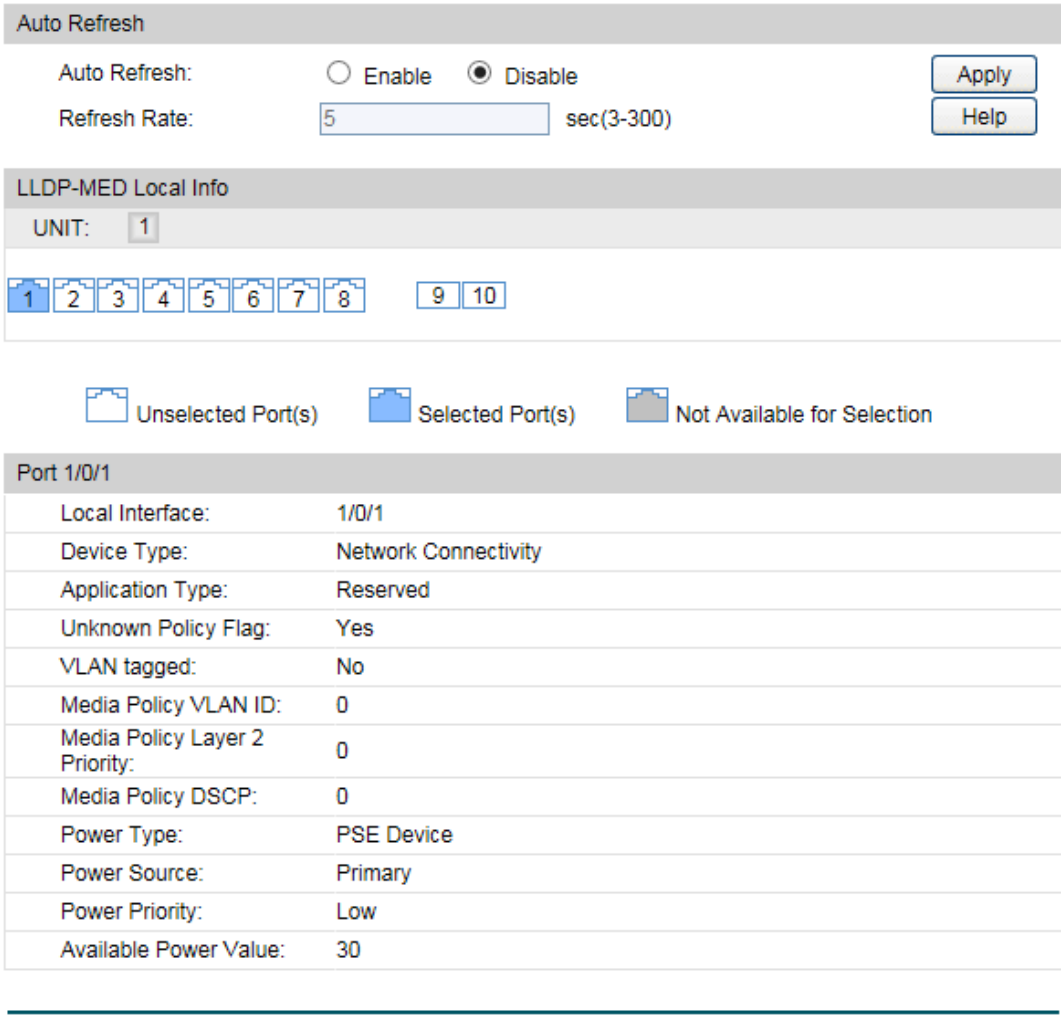


Figure 14-8 LLDP-MED Local Information

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.

14.4.4 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.

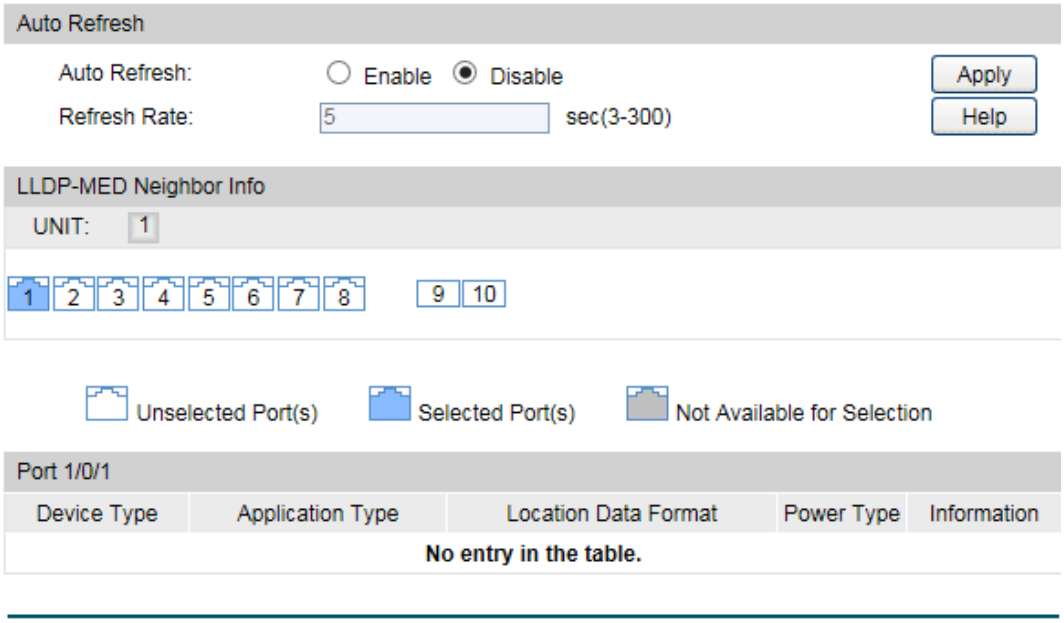


Figure 14-9 LLDP-MED Neighbor Information

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 15 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） Log: View the configuration parameters of the switch and find out the errors via the Logs.

（3） Device Diagnostics: Cable Test tests the connection status of the cable to locate and diagnoses the trouble spot of the network. Loopback tests whether the ports of the switch and its peer device are available.

（4） Network Diagnostics: Test whether the destination device is reachable and detect the route hops from the switch to the destination device.

15.1 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.

15.1.1 CPU Monitor

Choose the menu **Maintenance→System Monitor→CPU Monitor** to load the following page.

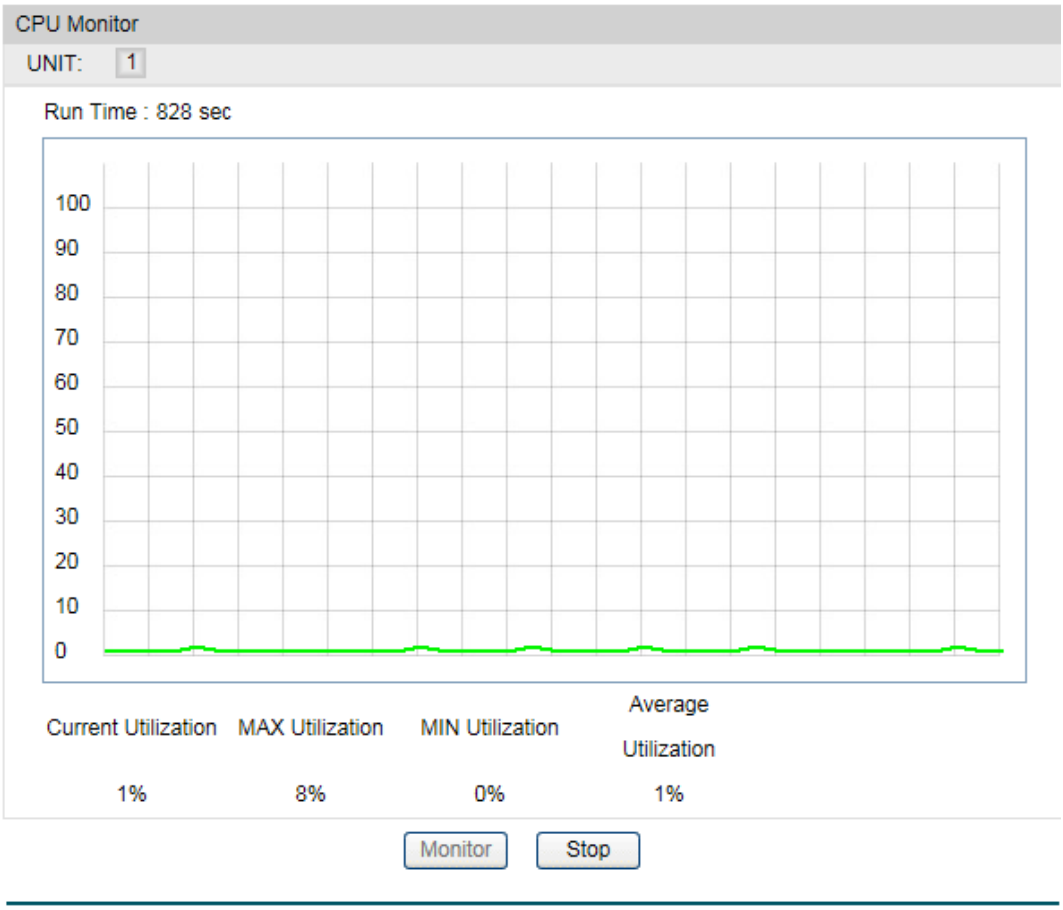


Figure 15-1 CPU Monitor

Click the **Monitor** button to enable the switch to monitor and display its CPU utilization rate every four seconds.

15.1.2 Memory Monitor

Choose the menu **Maintenance→System Monitor→Memory Monitor** to load the following page.

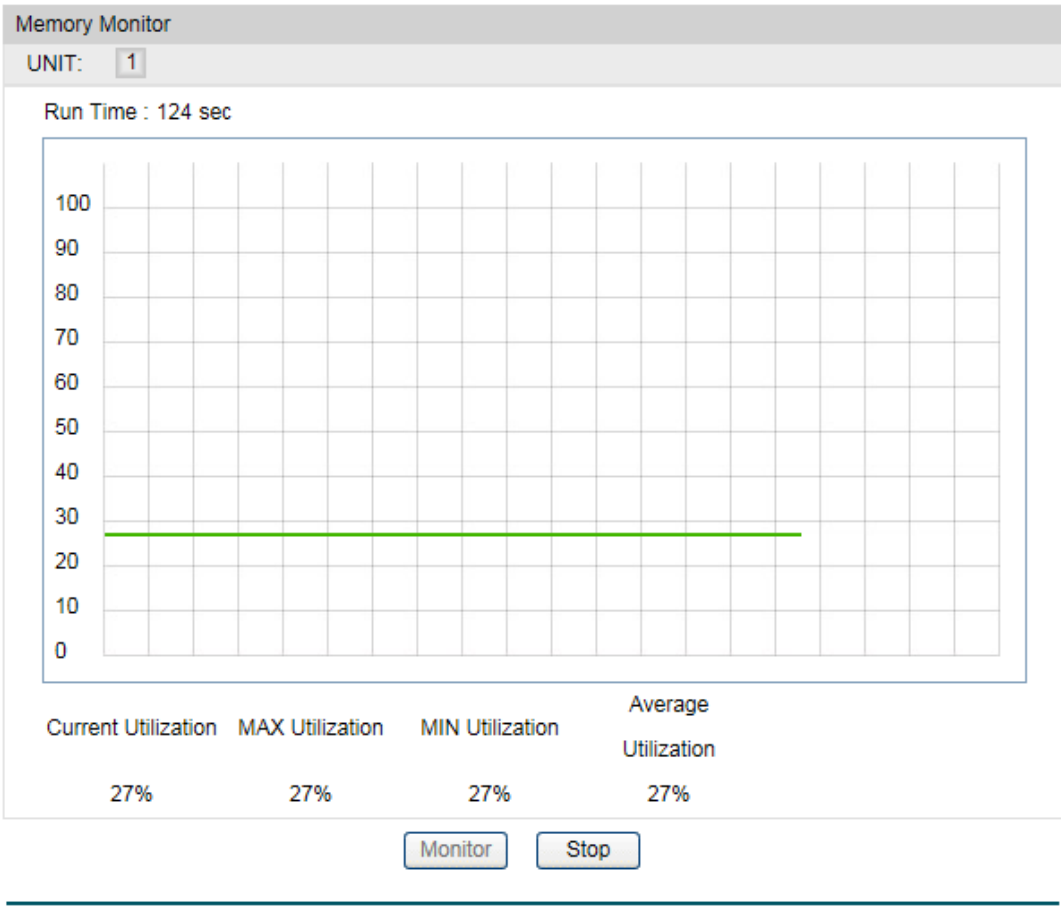


Figure 15-2 Memory Monitor

Click the **Monitor** button to enable the switch to monitor and display its Memory utilization rate every four seconds.

15.2 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
notifications	5	Normal but significant conditions
informational	6	Informational messages
debugging	7	Debug-level messages

Table 15-1 Log Level

The **Log** function is implemented on the **Log Table**, **Local Log**, **Remote Log** and **Backup Log** pages.

15.2.1 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.

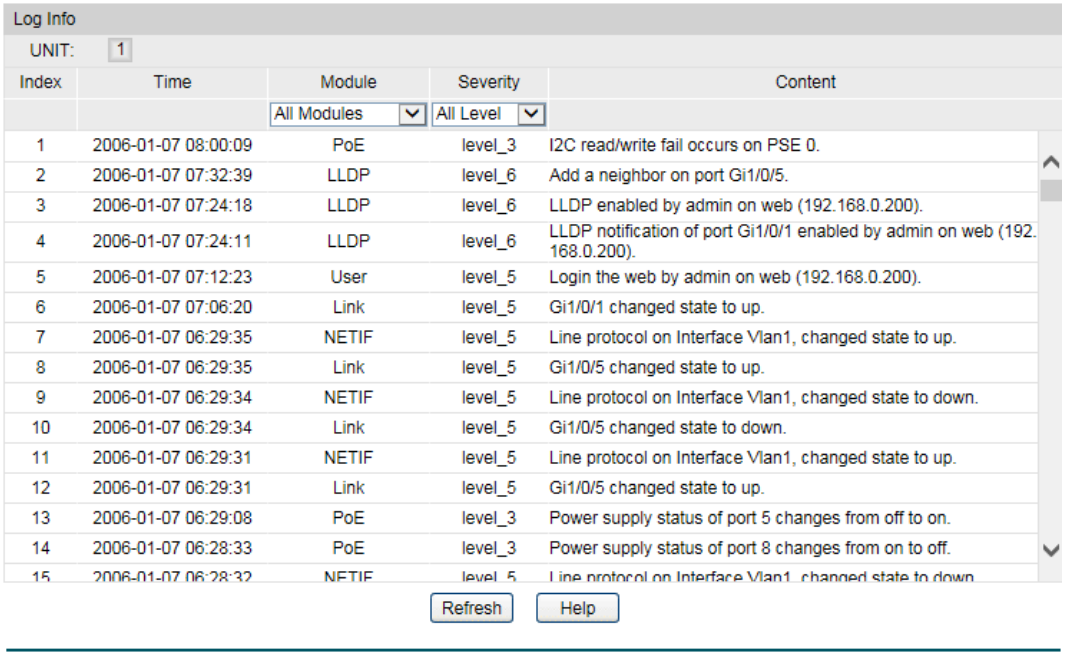


Figure 15-3 Log Table

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.

Module: Displays the module which the log information belongs to. You can select a module from the drop-down list to display the corresponding log information.

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:

3. The logs are classified into eight levels based on severity. The higher the information severity is, the lower the corresponding level is.
4. This page displays logs in the log buffer, and at most 1024 logs are displayed.

15.2.2 Local Log

Local Log is the log information saved in switch. By default, all system logs are saved in log buffer and the logs with severities from level_0 to level_2 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.

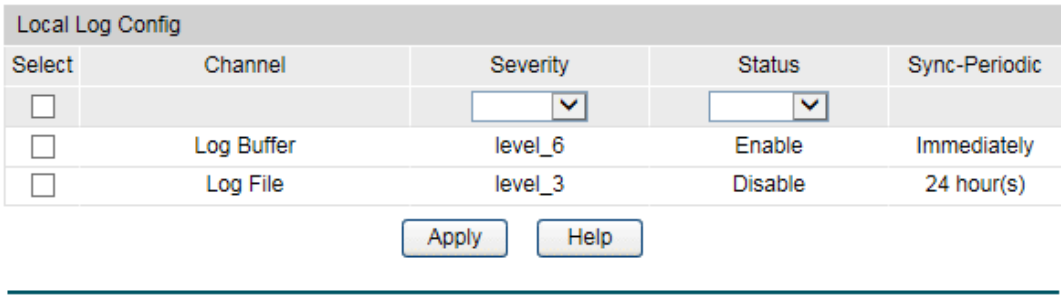


Figure 15-4 Local Log

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.

15.2.3 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.

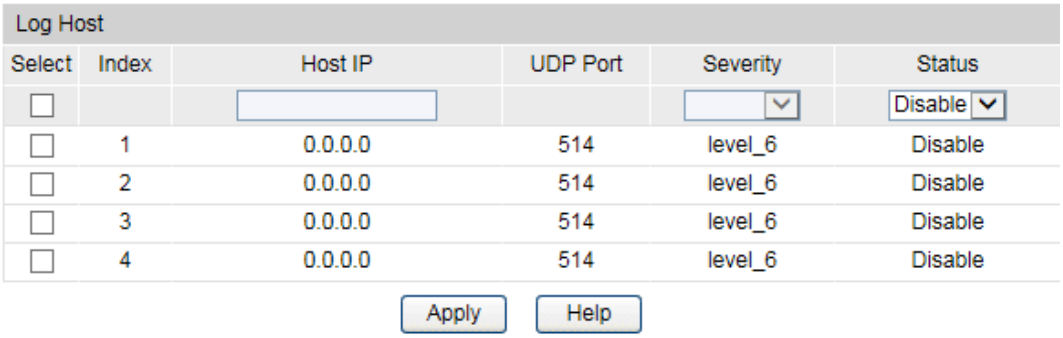


Figure 15-5 Log Host

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.

15.2.4 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.

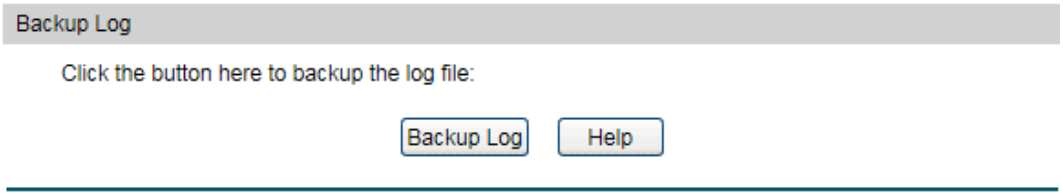


Figure 15-6 Backup Log

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:

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

15.3 Device Diagnostics

This switch provides Cable Test and Loopback functions for device diagnose.

15.3.1 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.

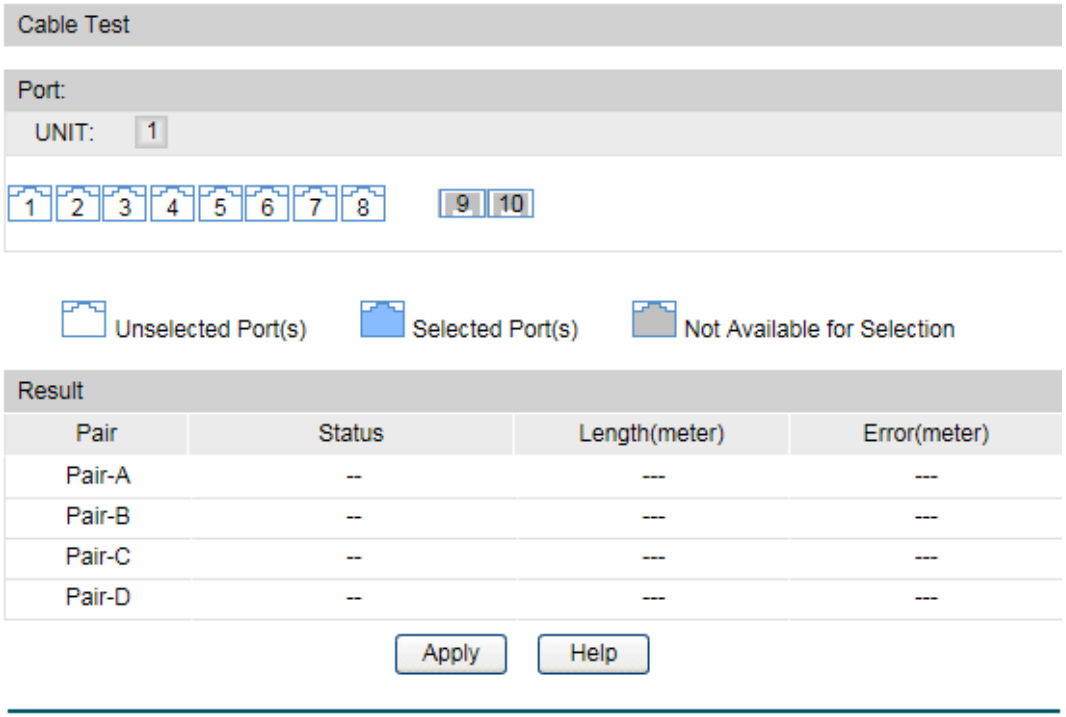


Figure 15-7 Cable Test

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 Length displayed here is the length of pair cable not that of the physical cable.
2. The test result is just for your reference.

15.4 Network Diagnostics

This switch provides Ping test and Tracert test functions for network Diagnostics.

15.4.1 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.

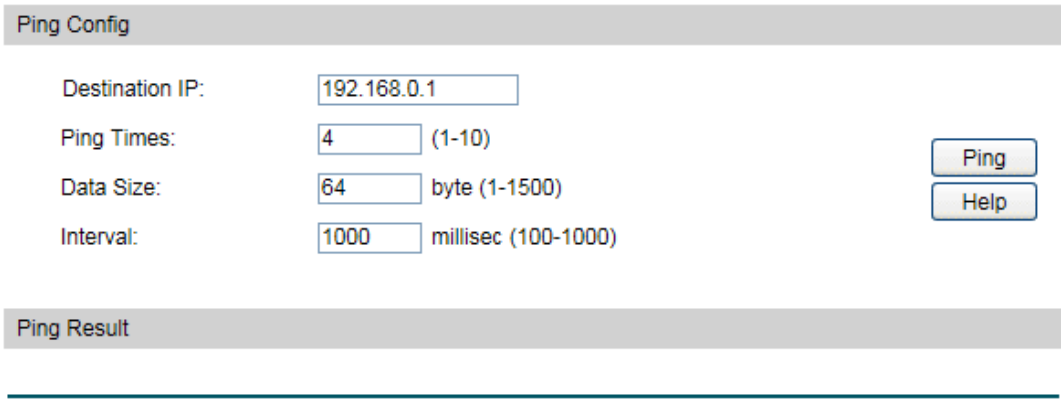


Figure 15-8 Ping

The following entries are displayed on this screen:

➢ **Ping Config**

Destination IP: Enter the IP address of the destination node for Ping test.

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.

15.4.2 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.

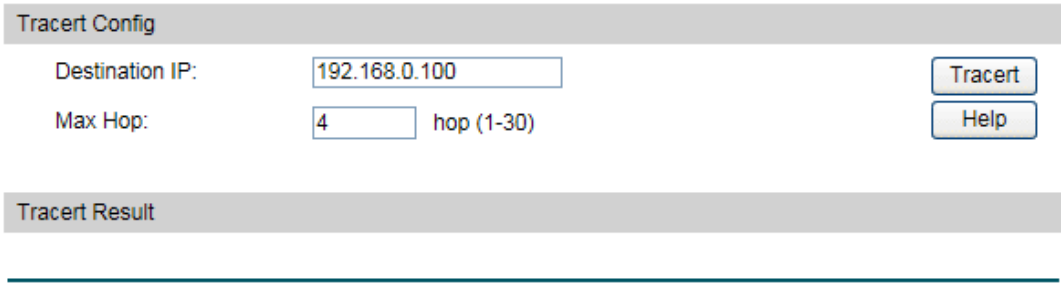


Figure 15-9 Tracert

The following entries are displayed on this screen:

- **Tracert Config**

  Destination IP: Enter the IP address of the destination device.

  Max Hop: Specify the maximum number of the route hops the test data can pass through.

Return to CONTENTS

Appendix A: Specifications

Standards	T1500G-10MPS: IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEEE802.3ad, IEEE802.3af, IEEE802.3at, IEEE802.3x, IEEE802.1p, IEEE802.1q, IEEE802.1x, IEEE802.1d, IEEE802.1s, IEEE802.1w T1500G-8T: IEEE802.3i, IEEE802.3u,IEEE802.3ab, IEEE802.3ad, IEEE802.3af, IEEE802.3x, IEEE802.1p, IEEE802.1q, IEEE802.1d, IEEE802.1x, IEEE802.1s, IEEE802.1w	
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 (maximum 100m)
	100Base-TX	2-pair UTP/STP of Cat. 5 or above (maximum 100m)
	100Base-FX (T1500G-10MPS)	MMF SFP Module
	100Base-LX10 (T1500G-10MPS)	SMF SFP Module
	100Base-BX10 (T1500G-10MPS)	SMF SFP Module
	1000Base-T	4-pair UTP/STP of Cat. 5e or above (maximum 100m)
	1000Base-SX (T1500G-10MPS)	MMF SFP Module
	1000Base-LX (T1500G-10MPS)	MMF or SMF SFP Module
	1000Base-LX10 (T1500G-10MPS)	SMF SFP Module

	1000Base-BX10 (T1500G-10MPS)	SMF SFP Module
LED	T1500G-10MPS: PWR, SYS, PoE MAX, FAN, Speed or PoE, SFP1, SFP2, PoE, Speed T1500G-8T: Power, System, 1-8	
Transmission Method	Store and Forward	
Packets Forwarding Rate	10Base-T：14881pps/port 100Base-X：148810pps/port 1000Base-T：1488095pps/port 1000Base-X : 1488095pps/port	
Operating Environment	Operating Temperature: 0℃ to 40℃	
	Storage Temperature: -40℃ to 70℃	
	Operating Humidity: 10% to 90% RH Non-condensing	
	Storage Humidity: 5% to 90% RH Non-condensing	

Return to CONTENTS

Appendix B: Glossary

Boot Protocol (BOOTP)
BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)
CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, or DSCP priority bit.

Differentiated Services Code Point (DSCP)
DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)
A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)
Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options..

IEEE 802.1D
Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q
VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p
An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.3ac
Defines frame extensions for VLAN tagging.

IEEE 802.3x
Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

Internet Group Management Protocol (IGMP)
A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP Snooping
Listening to IGMP Query and IGMP Report packets transferred between IP Multicast routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query
On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IP Multicast Filtering
It is a feature to allow or deny the Client to add the specified multicast group.

Multicast Switching
A process whereby the switch filters incoming multicast frames for services forwhich no attached host has registered, or forwards them to all ports contained within the designated multicast group.

Layer 2
Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation
See Port Trunk.

Management Information Base (MIB)
An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm
An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Network Time Protocol (NTP)
NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Port Mirroring
A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk
Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Authentication Dial-in User Service (RADIUS)
RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)
RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)
RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Simple Network Management Protocol (SNMP)
The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)
SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Algorithm (STA)
A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet
Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)
A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)
UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)
A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Return to CONTENTS