User Guide

JetStream 52-Port Gigabit Stackable L3 Managed Switch

T3700G-52TQ

REV1.0.0
1910011776

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.

Industry Canada Statement

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

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

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。

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Explanation of the symbols on the product label

Symbol	Explanation
	AC voltage
	Indoor use only
	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.

CONTENTS

Package Contents

The following items should be found in your box:

- One T3700G-52TQ switch
- One Power Cord
- One Console Cable
- One USB Cable
- One Power Supply Module Slot Cover
- Two mounting brackets and other fittings
- Installation Guide
- Resource CD for T3700G-52TQ switch, including:
  - This User Guide
  - The Command Line Interface Guide
  - SNMP Mibs
  - 802.1X Client Software and its User Guide
  - 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 T3700G-52TQ 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

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

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

In this Guide the following conventions are used:

- The switch or T3700G-52TQ mentioned in this Guide stands for T3700G-52TQ JetStream 52-Port Gigabit Stackable L3 Managed Switch without any explanation.
- **Menu Name→Submenu Name→Tab page** indicates the menu structure. **System→System Info→System Summary** means the System Summary page under the System Info menu option that is located under the System menu.
- **Bold font** indicates a button, a toolbar icon, menu or menu item.

Symbols in this Guide：

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

More Info:

- The latest software, management app and utility can be found at Download Center at *http://www.tp-link.com/support.*

- The Installation Guide (IG) can be found where you find this guide or inside the package of the switch.
- Specifications can be found on the product page at *http://www.tp-link.com.*
- A Technical Support Forum is provided for you to discuss our products at *http://forum.tp-link.com*.
- Our Technical Support contact information can be found at the Contact Technical Support page at *http://www.tp-link.com/support*.

1.3 Overview of This Guide

Chapter	Introduction
Chapter 1 About This Guide	Introduces the guide structure and conventions.
Chapter 2 Introduction	Introduces the features, application and appearance of T3700G-52TQ switch.
Chapter 3 Login to the Switch	Introduces how to log on to T3700G-52TQ 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 manage the switch with a certain access level. • System Tools: Manage the configuration file of the switch. • Access Security: Provide different security measures for the user to enhance the configuration management security. • SDM Template: Manage the hardware TCAM resources.
Chapter 5 Stack	This module is used to configure the stack properties of the switch. Here mainly introduces: • Stack Info: View the detailed information of the stack. • Stack Config: Configure the current stack. • Auto Copy Software: Configure the Auto Copy Software function.
Chapter 6 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.

Chapter	Introduction
Chapter 7 VLAN	This module is used to configure VLANs to control broadcast in LANs. Here mainly introduces: • 802.1Q VLAN: Configure port-based VLAN. • MAC VLAN: Configure MAC-based VLAN without changing the 802.1Q VLAN configuration. • Protocol VLAN: Create VLANs in application layer to make some special data transmitted in the specified VLAN. • VLAN VPN: VLAN VPN allows the packets with VLAN tags of private networks to be encapsulated with VLAN tags of public networks at the network access terminal of the Internet Service Provider. • GVRP: GVRP allows the switch to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other switches, without having to individually configure each VLAN. • Private VLAN: Designed to save VLAN resources of uplink devices and decrease broadcast. Private VLAN mainly used in campus or enterprise networks to achieve user layer-2-separation and to save VLAN resources of uplink devices.
Chapter 8 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 9 Multicast	This module is used to configure multicast function of the switch. Here mainly introduces: • IGMP Snooping: Configure global parameters of IGMP Snooping function, port properties, VLAN and multicast VLAN. • MLD Snooping: Configure global parameters of MLD Snooping function, port properties, VLAN and multicast VLAN. • MVR: Configure the Multicast VLAN Registration (MVR) feature. • Multicast Table: View different types of multicast table.

Chapter	Introduction
Chapter 10 Routing	The module is used to configure several IPv4 unicast routing protocols. Here mainly introduces: • Interface: Configure and view different types of interfaces: VLAN, loopback and routed port. • Routing table: Displays the routing information summary. • Static Routing: Configure and view static routes. • DHCP Server: Configure the DHCP feature to assign IP parameters to specified devices. • DHCP Relay: Configure the DHCP relay feature. • Proxy ARP: Configure the Proxy ARP feature to enable hosts on the same network but isolated at layer 2 to communicate with each other. • ARP: Displays the ARP information. • RIP: Configure the RIP feature. RIP is an interior gateway protocol using UDP data packets to exchange routing information. • OSPF: Configure the Open Shortest Path protocol. • VRRP: Configure the Virtual Router Redundant Protocol.
Chapter 11 Multicast Routing	This module is used to configure several multicast routing protocols for multicast data forwarding. Here mainly introduces: • Global Config: • IGMP: Configure the IGMP features. • PIM DM: Configure the PIM DM features. • PIM SM: Configure the PIM SM features. • Static Mroute: Configure the static multicast routing features.
Chapter 12 QoS	This module is used to configure QoS function to provide different quality of service for various network applications and requirements. Here mainly introduces: • Class of Service: Configure priorities, port priority, 802.1P priority and DSCP priority. • DiffServ: Configure classes, policies and services to allow traffic to be classified into streams and given certain QoS treatment. • 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. • Auto VoIP: Configure the Auto VoIP feature to prioritize the transmission of voice traffic

Chapter	Introduction
Chapter 13 ACL	This module is used to configure match rules and process policies of packets to filter packets in order to control the access of the illegal users to the network. Here mainly introduces: • Time-Range: Configure the effective time for ACL rules. • ACL Config: Configure the ACL rules. • ACL Binding: Bind the ACL to a port/VLAN to take its effect on a specific port/VLAN.
Chapter 14 Network Security	This module is used to configure the multiple 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. • IP Source Guard: Configure IP source guard feature to filter IP packets in the LAN. • DoS Defend: Configure DoS defend feature to prevent DoS attack. • 802.1X: Configure common access control mechanism for LAN ports to solve mainly authentication and security problems. • AAA: Configure the authentication, authorization and accounting features.
Chapter 15 SNMP	This module is used to configure SNMP function to provide a management frame to monitor and maintain the network devices. Here mainly introduces: • SNMP Config: Configure global settings of SNMP function. • Notification: Configure notification function for the management station to monitor and process the events. • RMON: Configure RMON function to monitor network more efficiently.
Chapter 16 LLDP	This module is used to configure LLDP function to provide information for SNMP applications to simplify troubleshooting. Here mainly introduces: • Basic Config: Configure the LLDP parameters of the device. • Device Info: View the LLDP information of the local device and its neighbors • Device Statistics: View the LLDP statistics of the local device

Chapter	Introduction
Chapter 17 Maintenance	This module is used to assemble the commonly used system tools to manage the switch. Here mainly introduces: • System Monitor: Monitor the memory and CPU of the switch. • Log: View and configure the system log function. • Device Diagnose: Including Cable Test and Loopback. Cable Test tests the connection status of the cable connected to the switch; and Loopback tests if the port of the switch and the connected device are available. • Network Diagnose: Test if the destination is reachable and the account of router hops from the switch to the destination.
Appendix A Glossary	Lists the glossary used in this manual.

Return to CONTENTS

Chapter 2 Introduction

Thanks for choosing the T3700G-52TQ JetStream 52-Port Gigabit Stackable L3 Managed Switch!

2.1 Overview of the Switch

T3700G-52TQ is an L3 managed switch that features advanced L3 routing, 10Gbps wire-speed, physical stacking and removable power supply module and fan module, designed to meet the needs of convergence layer. T3700G-52TQ is ideal for large businesses, campuses or SMB networks requiring an outstanding, reliable and affordable 10 Gigabit solution.

T3700G-52TQ supports stacking of up to 8 units, thus providing flexible scalability and protective redundancy for your networks. Moreover, aiming to better protect your network, T3700G-52TQ supports 2 power supply modules. T3700G-52TQ can fully implement resilient scalable networks due to its advanced features such as OSPF, VRRP, IGMP and PIM DM/SM.

2.2 Appearance Description

2.2.1 Front Panel

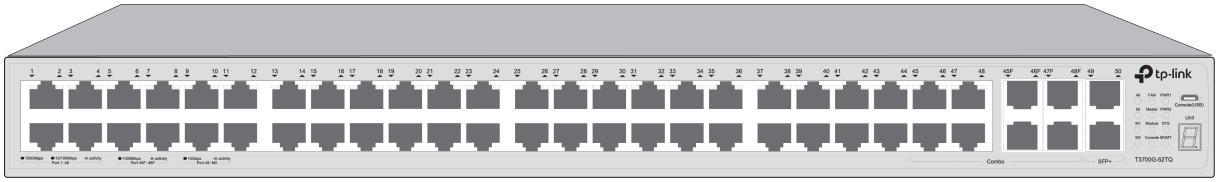


Figure 2-1 Front Panel

The following parts are located on the front panel of the switch:

- **LEDs**

LED	Status		Indication
PWR1	On	Green	The power supply module connected to the corresponding power slot works properly.
		Yellow	The power supply module connected to the corresponding power slot works improperly.
	Off		The corresponding power slot is not connected to any power supply module.
PWR2	On	Green	The power supply module connected to the corresponding power slot works properly.
		Yellow	The power supply module connected to the corresponding power slot works improperly.
	Off		The corresponding power slot is not connected to any power supply module.

LED	Status		Indication
SYS	Flashing (green)		The switch works properly.
	On/Off		The switch works improperly.
MGMT	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.
FAN	Green		The fan module works properly.
	Yellow		The fan module works improperly.
	Off		No fan module is connected to the switch.
Master	On		The switch works as master in the stack system, or does not join any stack system.
	Off		The switch works as member in the stack system.
Module	On(green)		An Interface Card is connected to the switch and works properly.
	On(yellow)		An Interface Card is connected to the switch, but works improperly.
	Off		No Interface Card is connected to the switch.
Console	On(green)		Data is being transmitted or received.
	Off		No data being transmitted or received for more than 6 minutes.
Link/Act (Port 1-48)	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.
49, 50	Green	On	A 10Gbps 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.

LED	Status		Indication
M1, M2	Green	On	A 10Gbps device is connected to the corresponding port of the Interface Card, but no activity.
		Flashing	Data is transmitting or received.
	Off		1. No Interface Card is connected. 2. No device is connected to the corresponding port of the Interface Card.

- **10/100/1000Mbps RJ45 Ports:** Port 1-48 designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding Link/Act LED.
- **SFP Port:** Port 45F-48F, designed to install the SFP transceiver. These four SFP transceiver slots are shared with the associated RJ45 ports. The associated two ports are referred as a "Combo" port, which means they cannot be used simultaneously, otherwise only RJ45 port works. The SFP ports support 1000M SFP module connection only.
- **SFP+ Port:** Port 49-50, designed to install the 10Gbps SFP+ transceiver or SFP+ cables. T3700G-52TQ also provides an interface card slot on the rear panel to install the expansion card (TX432 of TP-Link for example). If TX432 is installed, you get another two 10Gbps SFP+ ports.
- **Micro-USB Console Port:** Designed to connect with the USB port of a computer for monitoring and configuring the switch. The switch has an RJ-45 console port and a micro-USB console port available. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector.
- **Unit ID LED:** Designed to display the stack Unit ID of the switch. For the switch that does not join any stack system, it displays its default Unit ID. To modify the default unit number, please logon to the GUI of the switch and go to **Stack→Stack Management→Stack Config** page.

2.2.2 Rear Panel

The rear panel of T3700G-52TQ is shown as the following figure.

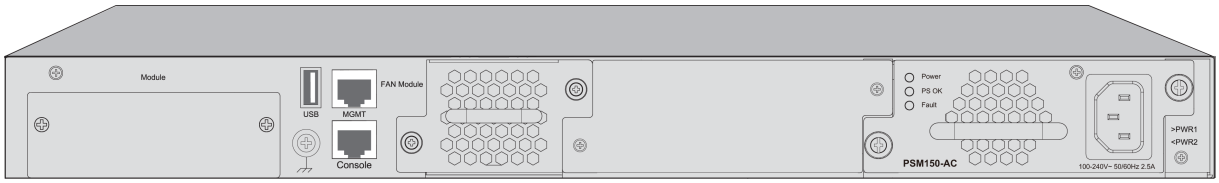


Figure 2-2 Rear Panel (1)

Note:

The Interface Card Slot and Power Supply Module2 are shipped with protective covers.

- **Interface Card Slot:** Designed to extend the interfaces. You can select an Interface Card (TX432 of TP-Link for example) for your switch if needed.

- **Grounding Terminal:** T3700G-52TQ 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. For detailed information, please refer to Installation Guide.
- **USB 2.0 Interface:** USB 2.0 interface is used to connecting peripheral equipment.
- **Management Port:** Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. It has a corresponding MGMT LED on the front panel. You need assign an IP address for the port to manage the switch.
- **RJ-45 Console Port:** Designed to connect with the serial port of a computer or terminal for monitoring and configuring the switch. The switch has an RJ-45 console port and a micro-USB console port available. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector.
- **Power Supply Module 1/2:** One AC Power Supply Module PSM150-AC has been installed in the switch. The malfunctioned PSM150-AC can be replaced with a TP-Link power supply module of the same model. Its input voltage is 100-240V~ 50/60Hz.
  The AC Power Supply Module is fully hot swappable, helping to ensure no system interruption during installation or replacement. For how to install/remove the Power Supply Module, please refer to **Installation Guide**.

With all the protective covers removed, and the Interface Card (TX432) & Power Supply Module (PSM150-AC) inserted, the rear panel of T3700G-52TQ is shown as the following figure.

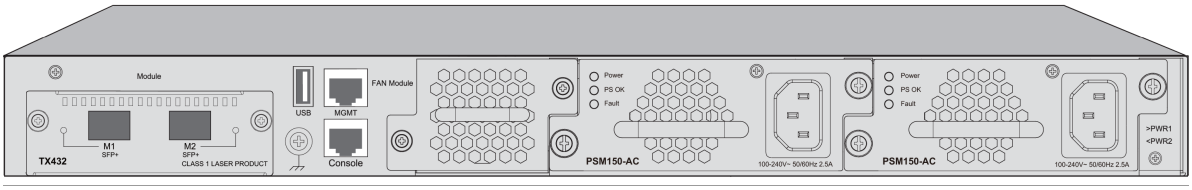


Figure 2-3 Rear Panel (2)

Return to CONTENTS

Chapter 3 Login to the Switch

3.1 Login

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

Figure 3-1 Web-browser

Tips:

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

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

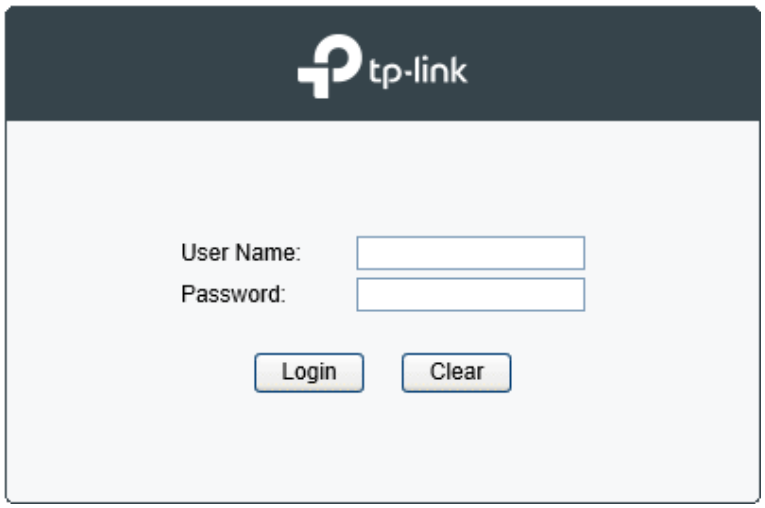


Figure 3-2 Login

3.2 Configuration

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

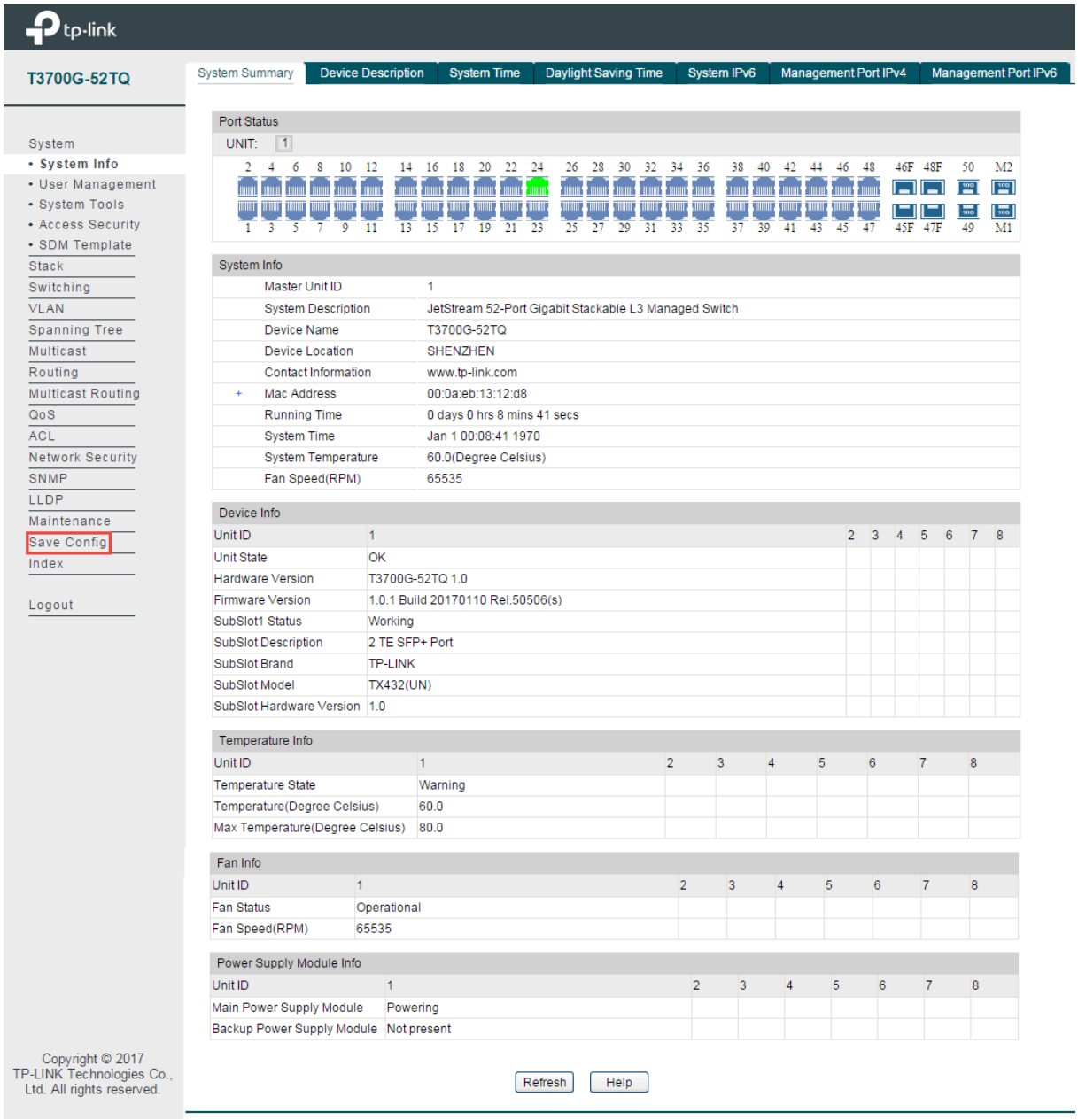


Figure 3-3 Main Setup-Menu

Note:

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

Return to CONTENTS

Chapter 4 System

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

4.1 System Info

The System Info, mainly for basic properties configuration, can be implemented on **System Summary**, **Device Description**, **System Time**, **Daylight Saving Time**, **System IPv6**, **Management Port IPv4** and **Management Port IPv6** 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 44 10/100/1000Mbps RJ45 ports, 4 1000Mbps SFP ports and 4 10000Mbps SFP+ ports of the switch. Ports 45, 46, 47 and 48 are Combo ports with SFP ports labeled 45F, 46F, 47F and 48F.

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

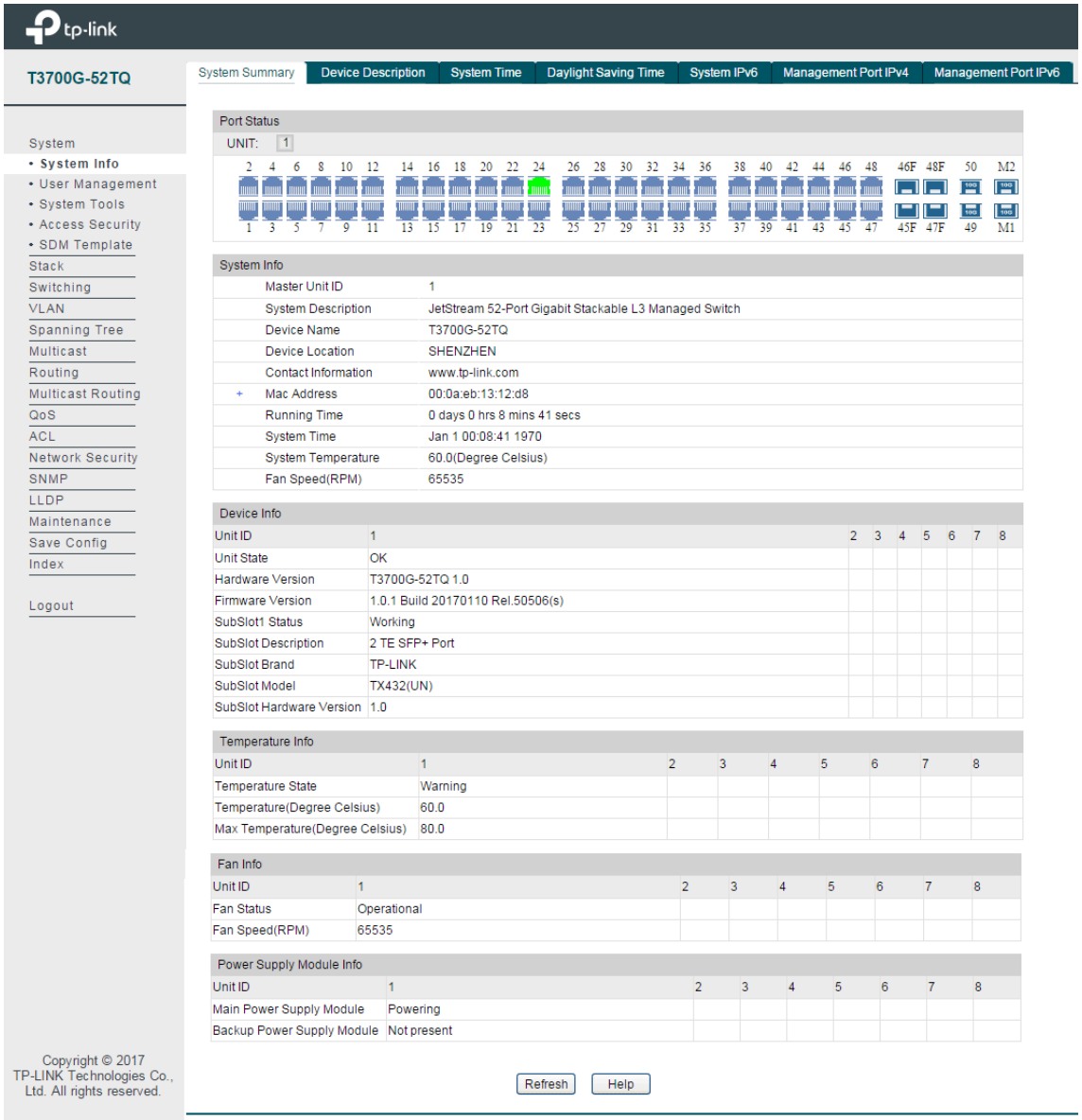


Figure 4-1 System Summary

➢ **Port Status**

UNIT: Select the unit ID of the desired member in the stack.

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.

Indicates the SFP+ port is not connected to a device.

Indicates the SFP+ port is at the speed of 10000Mbps.

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

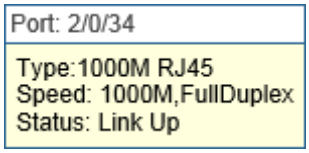


Figure 4-2 Port Information

- **Port Info**

Port:	Displays the port number of the switch.
Type:	Displays the type of the port.
Rate:	Displays the maximum transmission rate of the port.
Status:	Displays the connection status of the port.

Click a port to display the bandwidth utilization on this port. The actual rate divided by theoretical maximum rate is the bandwidth utilization. Figure 4-3 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.

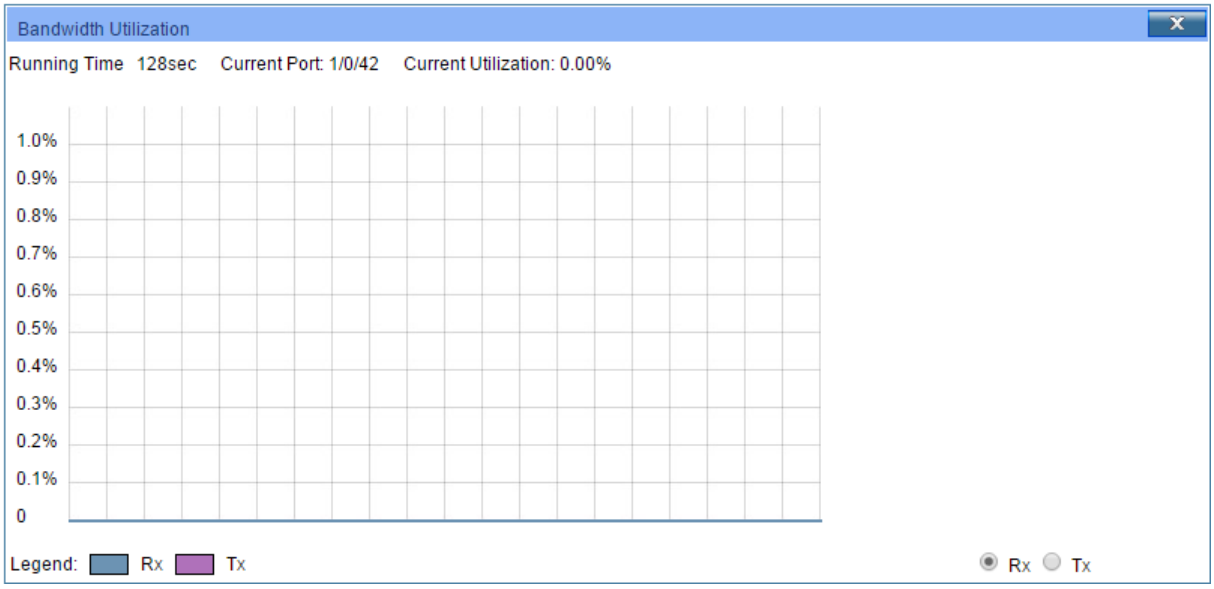


Figure 4-3 Bandwidth Utilization

- **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.

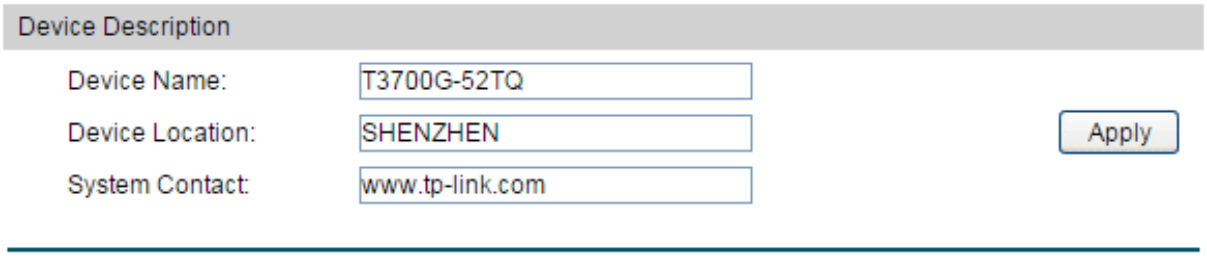


Figure 4-4 Device Description

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 like ACL.

You can manually set the system time, get UTC automatically if it has connected to an NTP server or synchronize with PC's clock as the system time.

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

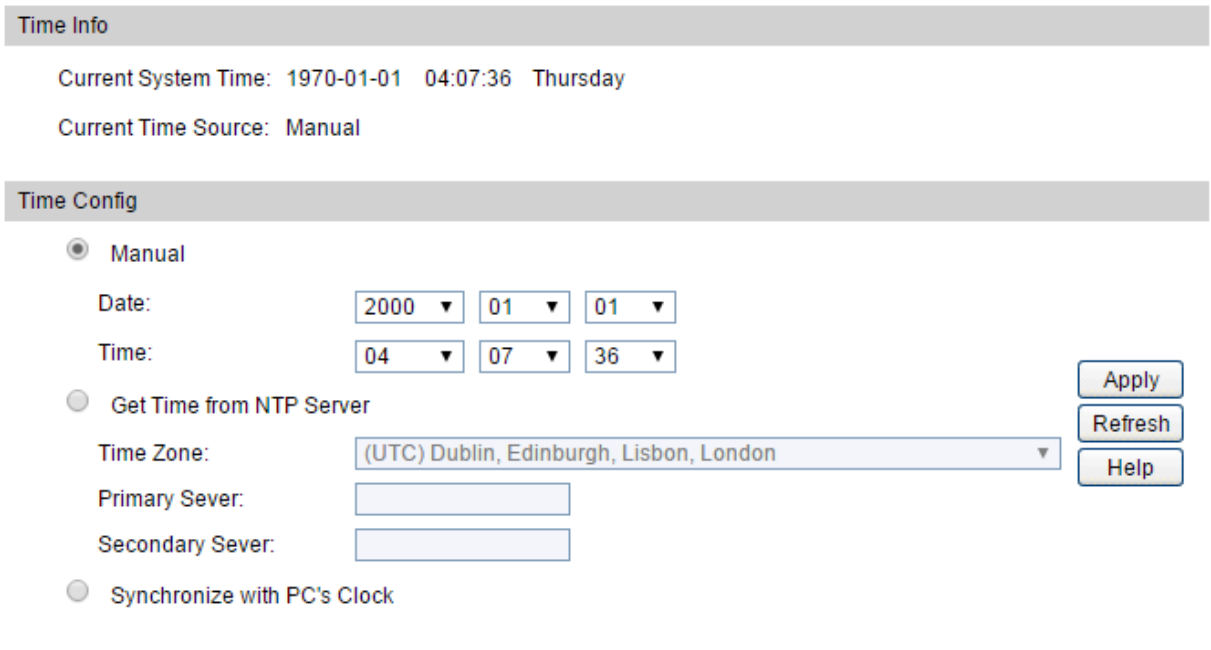


Figure 4-5 System Time

The following entries are displayed on this screen:

➢ **Time Info**

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

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

➢ **Time Config**

Manual:	When this option is selected, you can set the date and time manually.
Get Time from NTP Server:	When this option is selected, you can configure the time zone and the IP Address for the NTP Server. The switch will get UTC automatically if it has connected to an NTP Server. • **Time Zone:** Select your local time. • **Primary/Secondary NTP 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.

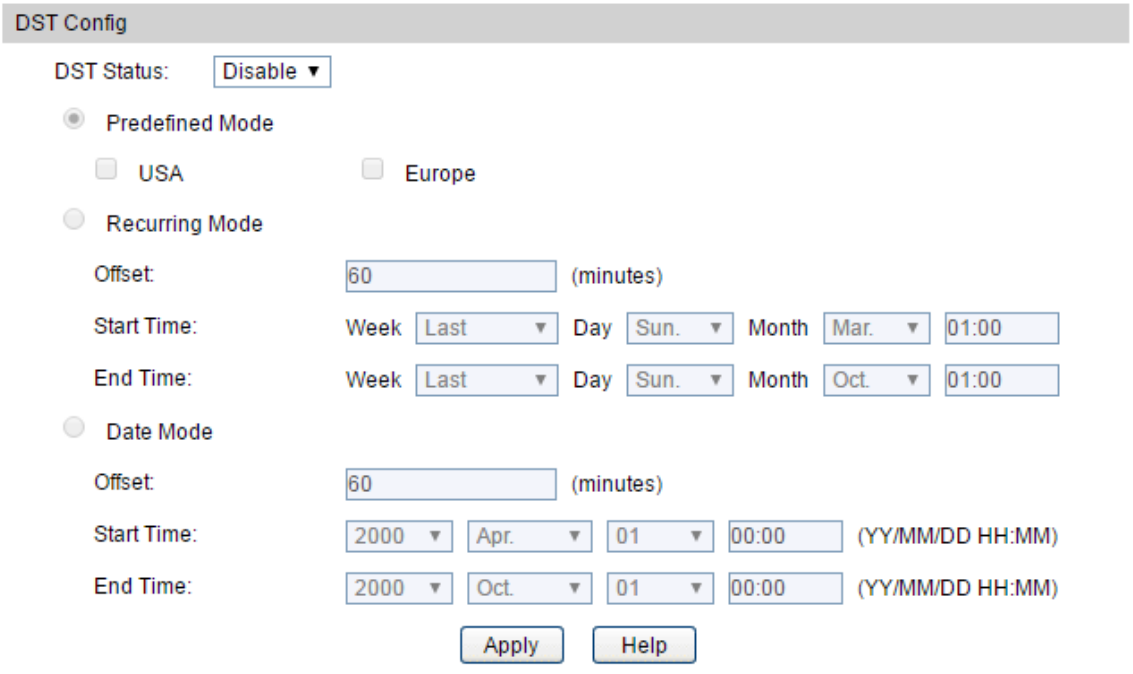


Figure 4-6 Daylight Saving Time

The following entries are displayed on this screen:

- **DST Config**

DST Status: Enable or disable DST.

Predefined Mode: Select a predefined DST configuration:

- USA: Second Sunday in March, 02:00 ~ First Sunday in November, 02:00.
- Europe: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00.

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 one-off 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:

When the DST is disabled, the predefined mode, recurring mode and date mode cannot be configured.

4.1.5 System IPv6

On this page you can configure IPv6 address on the switch and login the switch through the address to access the IPv6 applications. Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), is designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

Choose the menu **System** → **System Info** → **System IPv6** to load the following page.

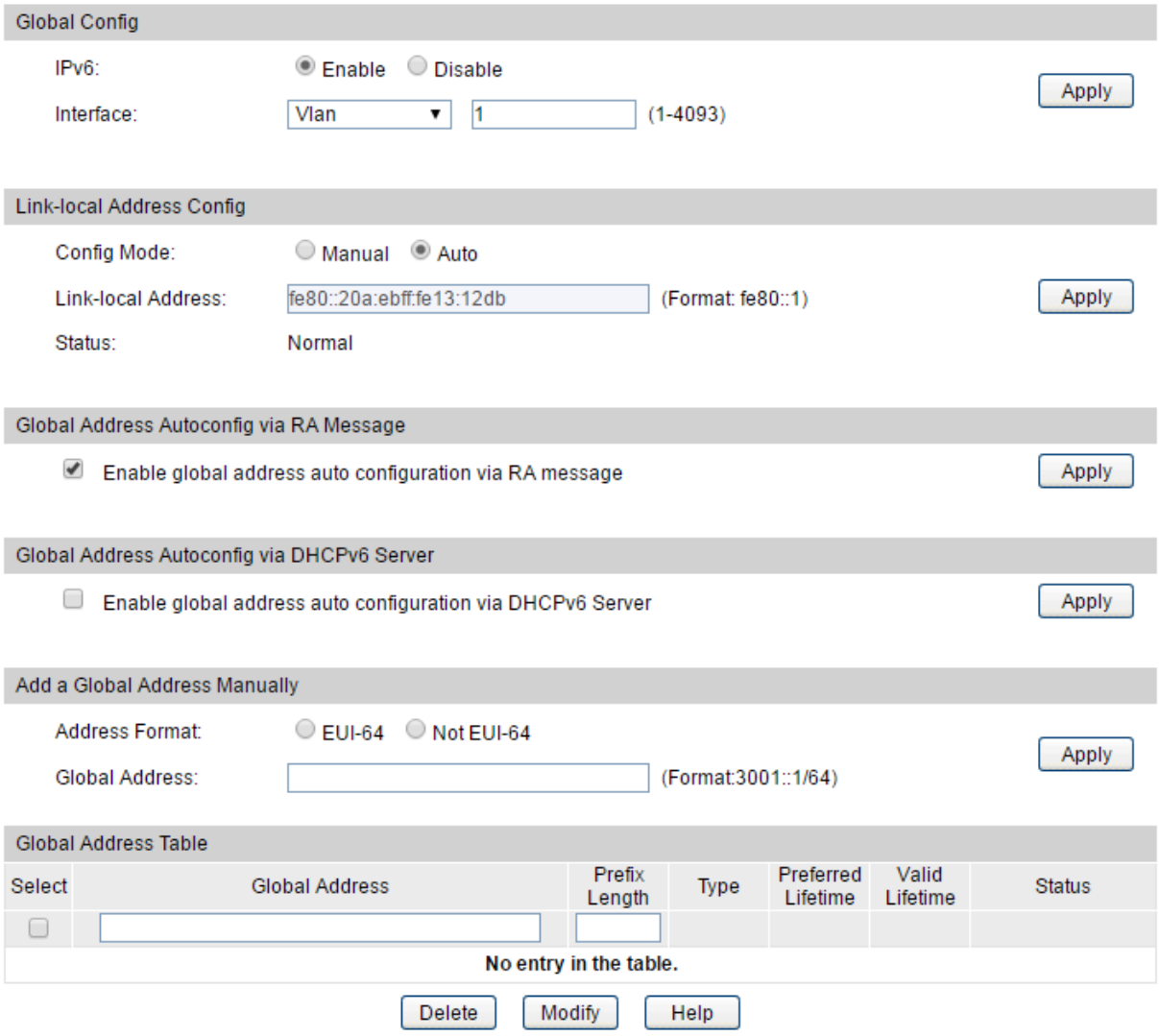


Figure 4-7 System IPv6

The following entries are displayed on this screen:

- **Gobal Config**

  IPv6: Enable or disable IPv6 function globally on the switch.

  Interface: Choose the interface ID to set IPv6 function. You can set interface type as VLAN Port or Routed Port.

- **Link-local Address Config**

  Config Mode: Select the link-local address configuration mode.

  - Manual: When this option is selected, you should assign a link-local address manually.
  - Auto: When this option is selected, the switch will generate a link-local address automatically.

  Link-local Address: Enter a link-local address.

Status: Displays the status of the link-local address.

- Normal: Indicates that the link-local address is normal.
- Try: Indicates that the link-local address may be newly configured.
- Repeat: Indicates that the link-local address is duplicate. It is illegal to access the switch using the IPv6 address (including link-local and global address).

➢ **Global Address Autoconfig via RA Message**

Enable global address auto configuration via RA message: When this option is enabled, the switch automatically configures a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.

➢ **Global Address Autoconfig via DHCPv6 Server**

Enable global address auto configuration via DHCPv6 Server: When this option is enabled, the system will try to obtain the global address from the DHCPv6 Server.

➢ **Add a Global Address Manually**

Address Format: You can select the global address format according to your requirements.

- EUI-64: Indicates that you only need to specify an address prefix, and then the system will create a global address automatically.
- Not EUI-64: Indicates that you have to specify an intact global address.

Global Address: When selecting the mode of EUI-64, please input the address prefix here, otherwise, please input an intact IPv6 address here.

➢ **Global Address Table**

Select: Select the desired entry to delete or modify the corresponding global address.

Global Address: Modify the global address.

Prefix Length: Modify the prefix length of the global address.

Type： Displays the configuration mode of the global address.

- Manual: Indicates that the corresponding address is configured manually.
- Auto: Indicates that the corresponding address is created automatically using the RA message or obtained from the DHCPv6 Server.

Preferred Lifetime： Displays the preferred time of the global address.

Valid Lifetime: Displays the valid time of the global address.

Status: Displays the status of the global address.

- Normal: Indicates that the global address is normal.
- Try: Indicates that the global address may be newly configured.
- Repeat: Indicates that the corresponding address is duplicate. It is illegal to access the switch using this address.

4.1.6 Management Port IPv4

The Management Port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network. Use this page to configure network information on the management port.

Choose the menu **System** → **System Info** → **Management Port IPv4** to load the following page.

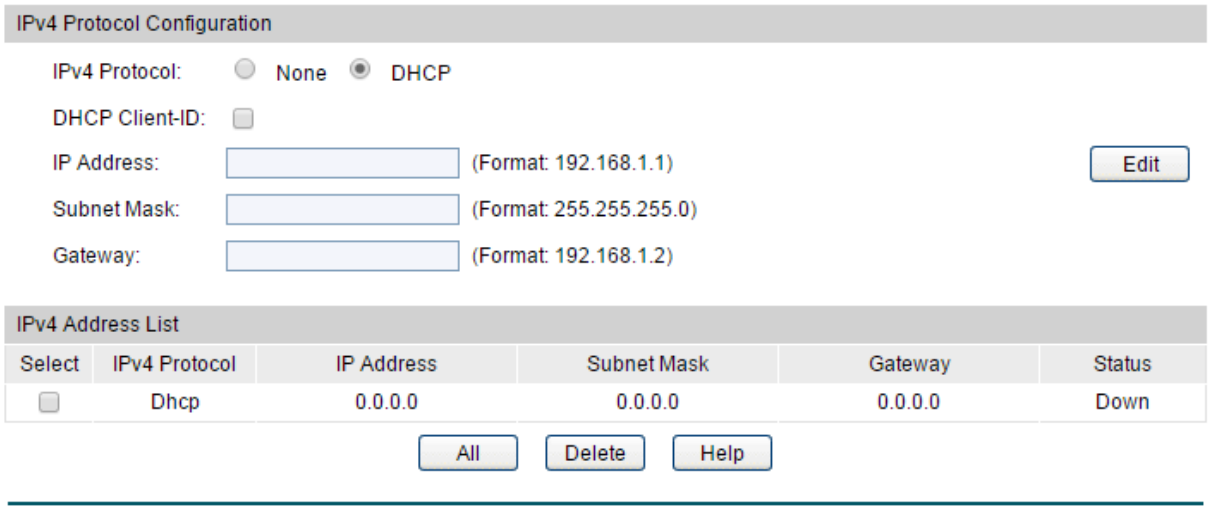


Figure 4-8 Management Port IPv4

The following entries are displayed on this screen:

➢ **IPv4 Protocol Configuration**

IPv4 Protocol: Specify IPv4 Address allocate mode of the management port.

- None: Setup manually.
- DHCP: Allocated through DHCP.

DHCP Client-ID: The DHCP Client-ID (Option 61) is used by DHCP clients to specify their unique identifier. This value is expected to be unique for all clients in an administrative domain.

IP Address: Specify the IP address of the interface when the Management Port Configuration Protocol is None.

Subnet Mask: Specify the Subnet Mask of the interface when the Management Port Configuration Protocol is None.

Gateway: Specify the Gateway of the interface when the Management Port Configuration Protocol is None.

➢ **IPv4 Address List**

Select: Select the interfaces to modify or delete.

IPv4 Protocol: Specify IPv4 Address allocate mode of the management port.

- None: Setup manually.
- DHCP: Allocated through DHCP.

IP Address: Specify the IP address of the interface when the Management Port Configuration Protocol is None.

Subnet Mask: Specify the Subnet Mask of the interface when the Management Port Configuration Protocol is None.

Gateway: Specify the Gateway of the interface when the Management Port Configuration Protocol is None.

Status: Displays interface current working status: up or down.

4.1.7 Management Port IPv6

The Management Port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network. Use this page to configure IPv6 network information on the management port.

Choose the menu **System** → **System Info** → **Management Port IPv6** to load the following page.

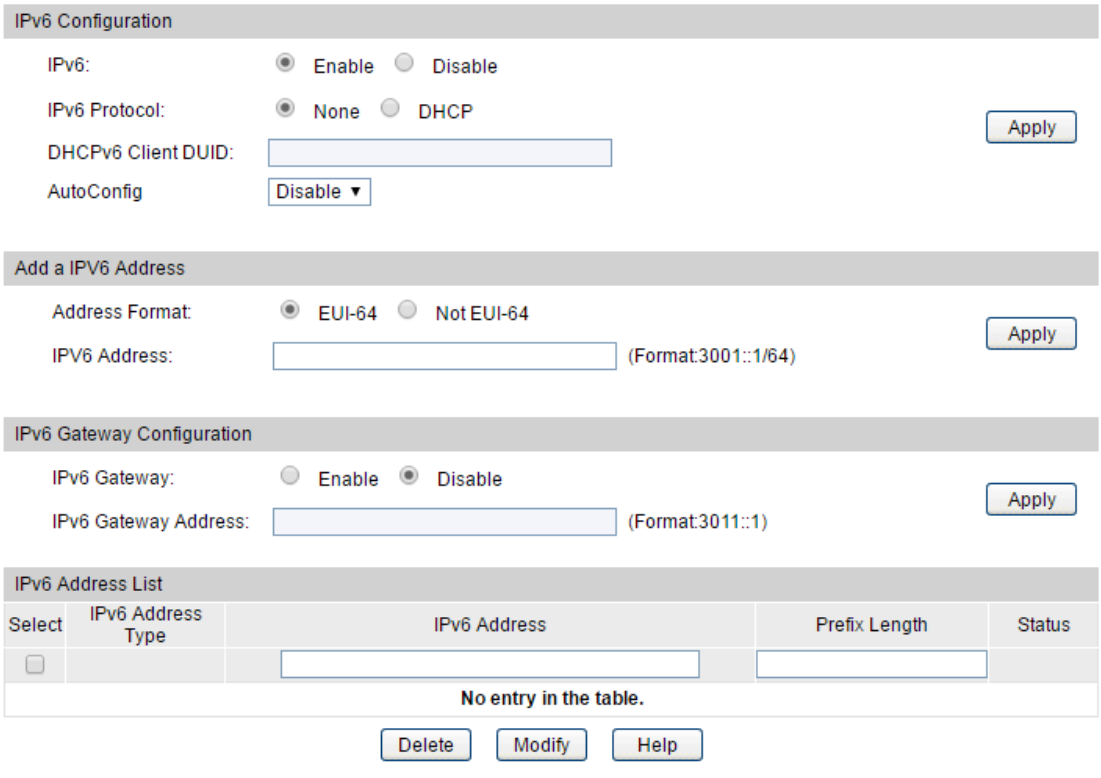


Figure 4-9 Management Port IPv6

The following entries are displayed on this screen:

- **IPv6 Configuration**

IPv6:	Enable or disable IPv6 function globally on the management port.
IPv6 Protocol:	Specify IPv6 network information allocate mode of the management port. • None: Setup manually. • DHCP: Allocated through DHCP.
DHCPv6 Client DUID:	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
AutoConfig:	Choose whether to allow to enable the IPv6 stateless address autoconfiguration mode via the RA message on the management port.

- **Add a IPv6 Address**

Address Format:	You can select the IPv6 address format according to your requirements. • EUI-64: Indicates that you only need to specify an address prefix, and then the system will create a IPv6 address automatically. • Not EUI-64: Indicates that you have to specify an intact IPv6 address.
IPV6 Address:	When selecting the mode of EUI-64, please input the address prefix here, otherwise, please input an intact IPv6 address here.

- **IPv6 Gateway Configuration**

IPv6 Gateway:	Choose whether to set the IPv6 Gateway Address.
IPv6 Gateway Address:	Please input the IPv6 gateway address here.

- **IPv6 Address List**

Select:	Select the interfaces to modify or delete.
IPv6 Address Type:	Displays IPv6 Address type: Link Local, Global or Router.
IPv6 Prefix:	Displays the IPv6 prefix.
Prefix Length:	Displays the prefix length of IPv6 Address.

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.

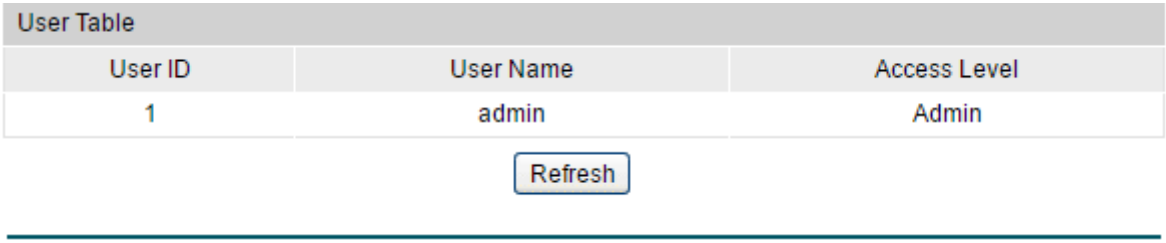


Figure 4-10 User Table

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 two access levels: Guest and Admin. The guest only can view the settings without the right to configure the switch; the admin can configure all the functions of the switch. 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.

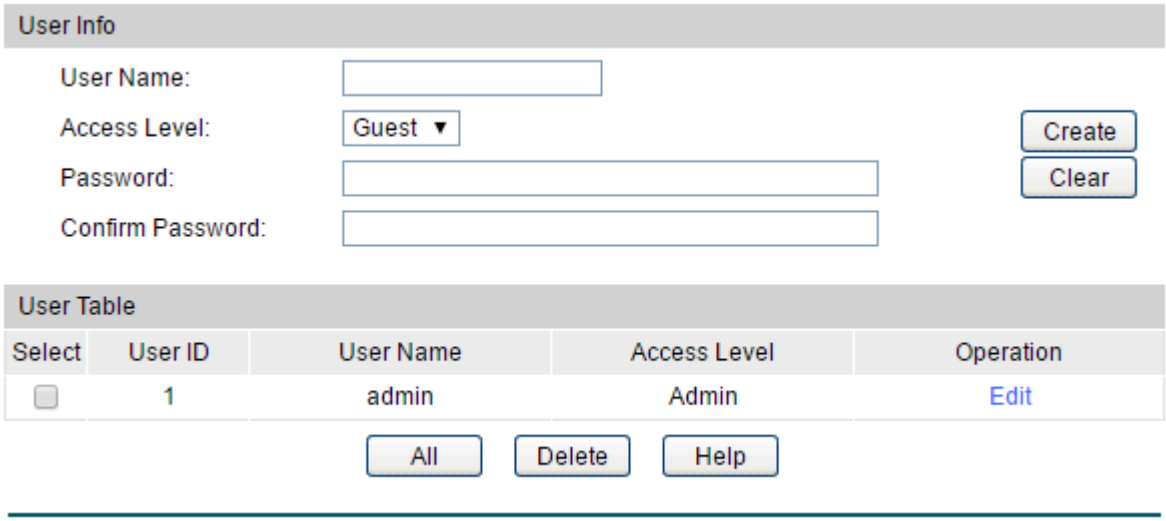


Figure 4-11 User Config

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.

- **Guest:** Guest only can view the settings without the right to edit and modify.
- **Admin:** Admin can edit, modify and view all the settings of different functions.

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 cannot be deleted.
User ID, User 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 **Apply** button to make the modification effective.

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 and the configuration file of the switch. When the switch is powered on, it will start up with the startup image. If the startup fails, the switch will try to start up with the backup image. If this startup fails too, the switch will changes to bootutil state, in which circumstance the switch's Web interface is unavailable and you can enter into the bootutil menu of the switch through the console connection.

When the startup process is finished, the switch will read the startup-config file. If it fails, the switch will try to read the backup-config file. If it fails too, the switch will be restored to factory settings.

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

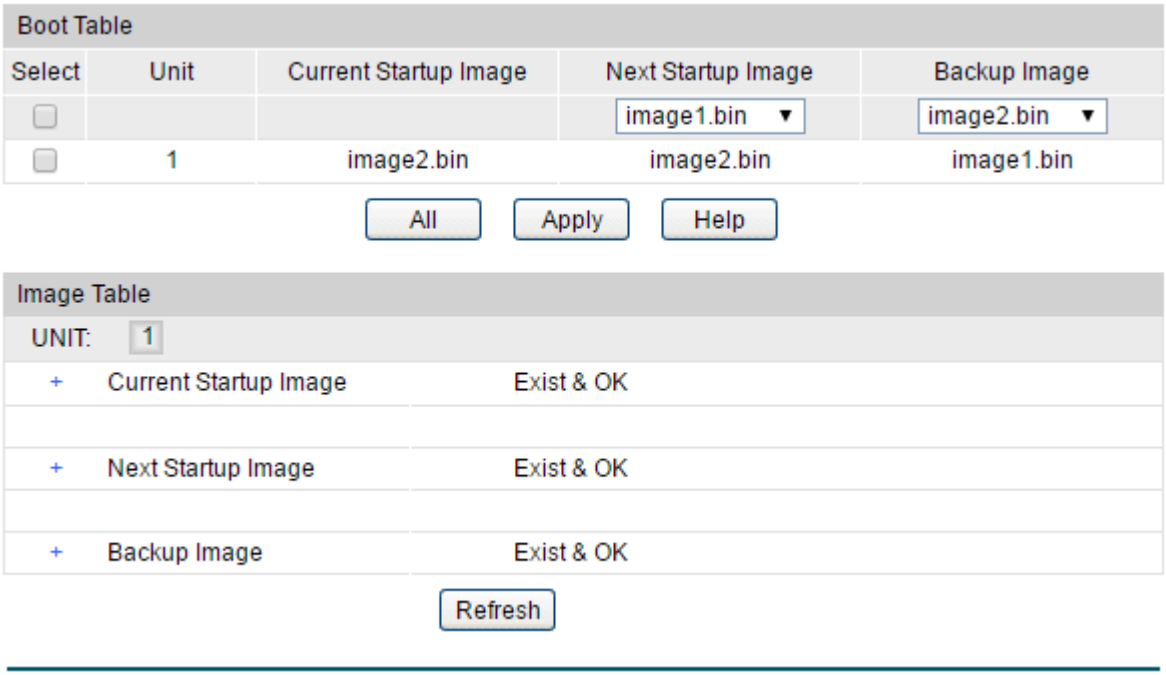


Figure 4-12 Boot Config

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.

- **Image Table**

  Image Name: The name of the image.

  Flash Version: The flash version of the image.

  Software Version: The software version of the 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.

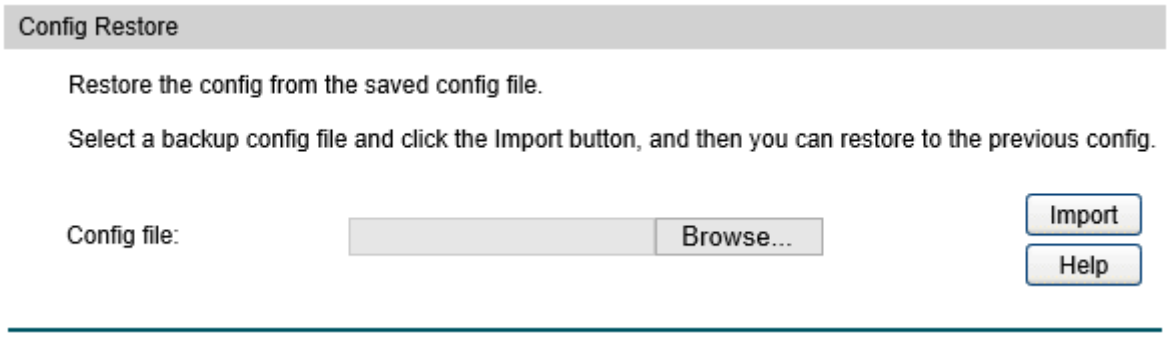


Figure 4-13 Config Restore

The following entries are displayed on this screen:

➢ **Config Restore**

Import: Click the **Import** button to restore the backup configuration file. It will take effect after the switch automatically reboots.

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 the configuration file is restored successfully, the device will reboot to make the configuration change effective.
4. Wrong uploaded configuration file may cause the switch unmanaged.

4.3.3 Config Backup

On this page you can download the current configuration of the specified unit in the stack 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.

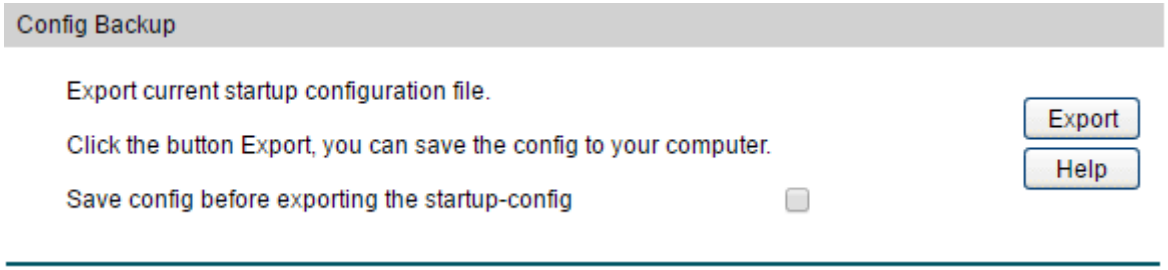


Figure 4-14 Config Backup

The following entries are displayed on this screen:

➢ **Config Backup**

Export: 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:

1. It will take a few minutes to backup the configuration. Please wait without any operation.
2. Check the checkbox to copy running-config to startup-config before exporting the startup-config.

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.

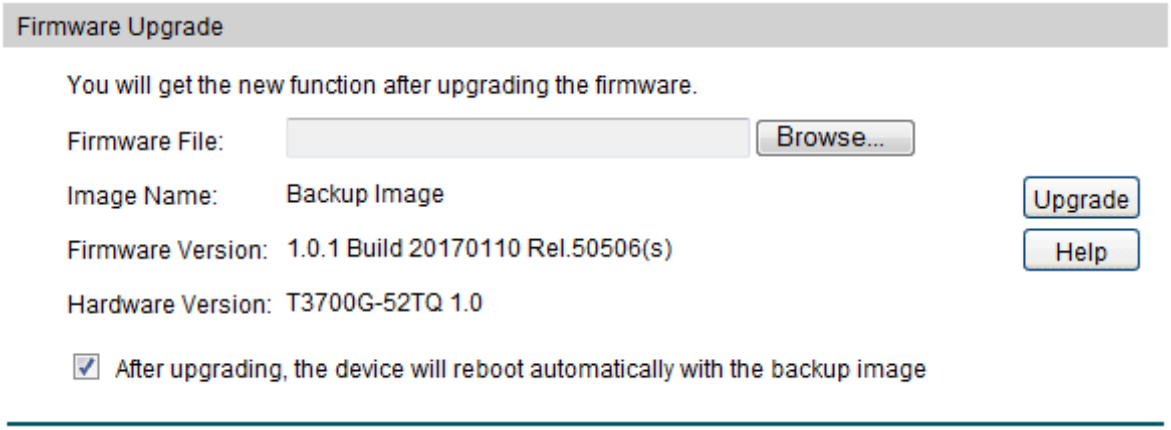


Figure 4-15 Firmware Upgrade

Note:

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

4.3.5 System Reboot

On this page you can reboot the specified unit switch in the stack 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 4-16 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 specified unit in the stack 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 4-17 System Reset

Note:

The System Reset option will restore the configuration to default and your current settings will be lost.

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. The definitions of Admin and Guest refer to 4.2 User Management. This function only applies to Web, SNMP, Telnet, SSL and SSH.

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

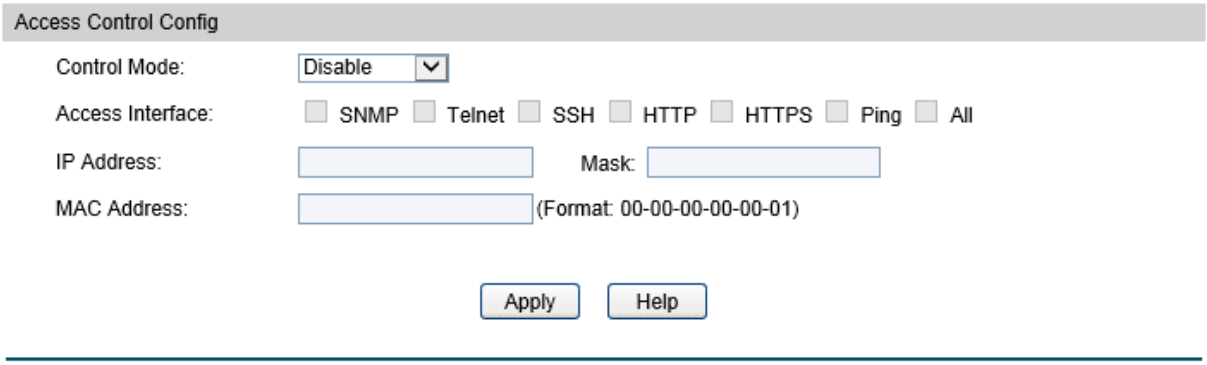


Figure 4-18 Access Control

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 managing the switch.
- **MAC-based:** Select this option to limit the MAC Address of the users for managing the switch.
- **Port-based:** Select this option to limit the ports for managing the switch.

Access Interface: Select the interface for Access Control to apply.

IP Address& Mask: These fields can be available for configuration only when IP-based mode is selected. Only the users within the IP-range you set here are allowed for managing the switch.

MAC Address: The field can be available for configuration only when MAC-based mode is selected. Only the user with this MAC Address you set here is allowed for managing the switch.

Port: The field can be available for configuration only when Port-based mode is selected. Only the users connected to these ports you set here are allowed for managing the switch.

4.4.2 HTTP Config

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

On this page you can configure the HTTP function.

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

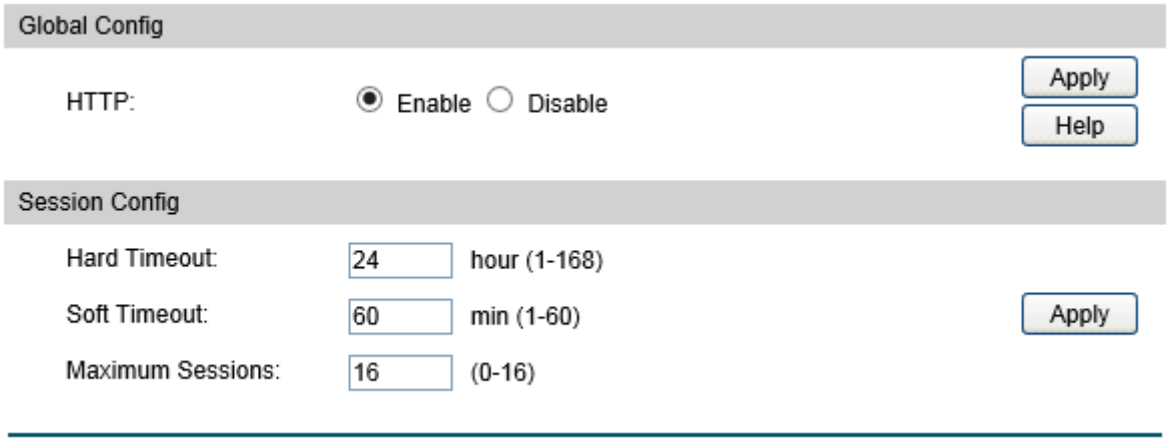


Figure 4-19 HTTP Config

The following entries are displayed on this screen:

- **Global Config**

  HTTP: Enable or disable the HTTP function on the switch.

- **Session Config**

  Hard Timeout: Configure hard timeout of HTTP sessions.

  Soft Timeout: Configure soft timeout of HTTP sessions.

  Maximum Sessions: Configure maximum allowable number of HTTP sessions.

4.4.3 HTTPS Config

SSL (Secure Sockets Layer), a security protocol, is to provide a secure connection for the application layer protocol (e.g. HTTP) communication based on TCP. SSL is widely used to secure the data transmission between the Web browser and servers. It is mainly applied through ecommerce and online banking.

SSL mainly provides the following services:

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

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

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

trusted certificate authority" or "Certificate Errors". Please add this certificate to trusted certificates or continue to this website.

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

On this page you can configure the HTTPS function.

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

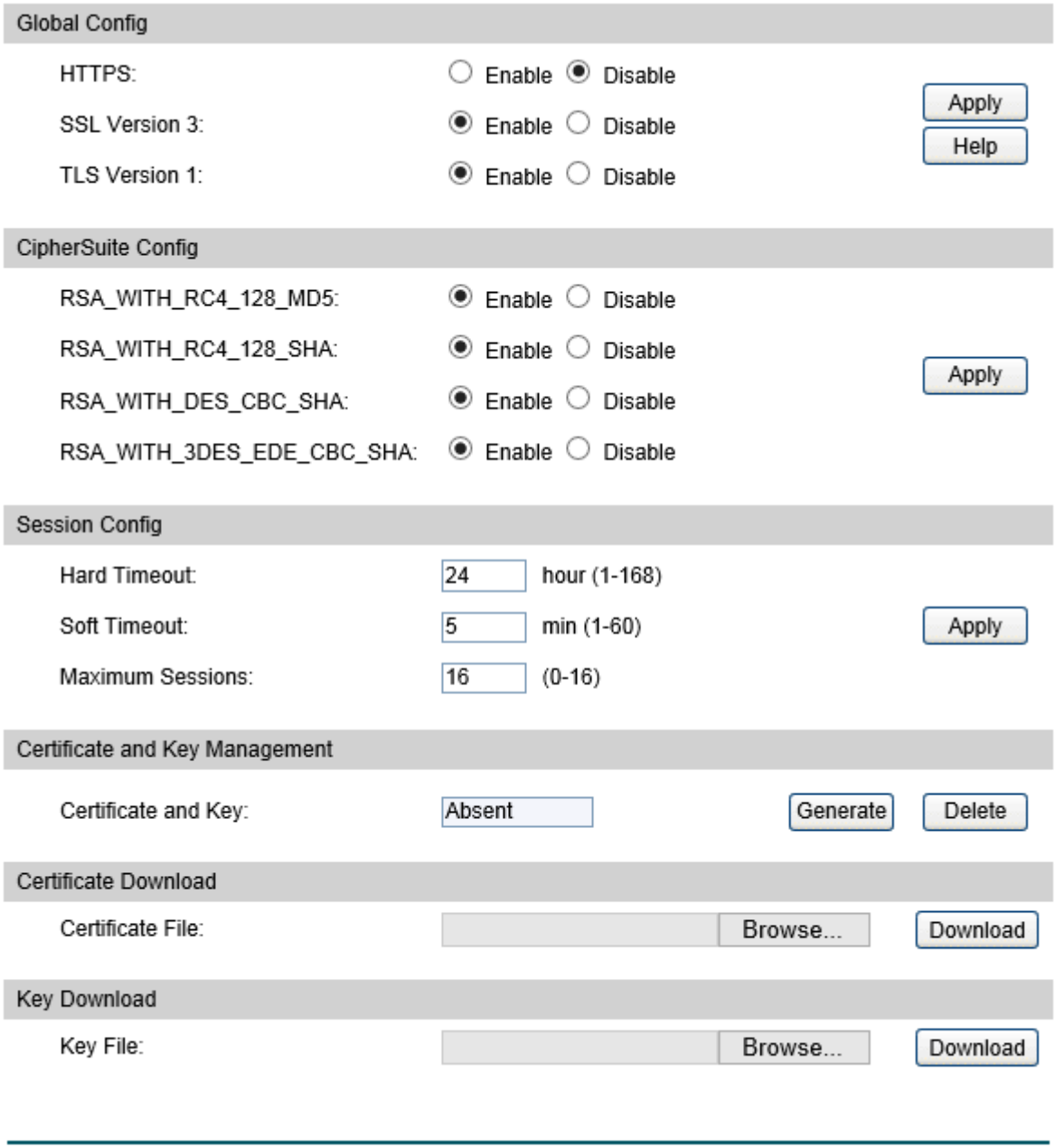


Figure 4-20 HTTPS Config

The following entries are displayed on this screen:

- **Global Config**

  HTTPS: Enable or 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**

Hard Timeout: Configure hard timeout of HTTP sessions.

Soft Timeout: Configure soft timeout of HTTP sessions.

Maximum Sessions: Configure maximum allowable number of HTTP sessions.

- **Certificate and Key Management**

You can get the status of the DSA and RSA keys, which can also be generated or deleted here with the Generate and Delete buttons.

Certificate and Key: The status of SSL certificate and key file (PEM Encoded) on the device, which might be Present or Absent.

- **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. HTTPS function can not be enabled until the SSL certificate and key are present.
2. The SSL certificate and key downloaded must match each other; otherwise the HTTPS connection will not work.

3. To establish a secured connection using https, please enter https:// into the URL field of the browser.
4. 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.

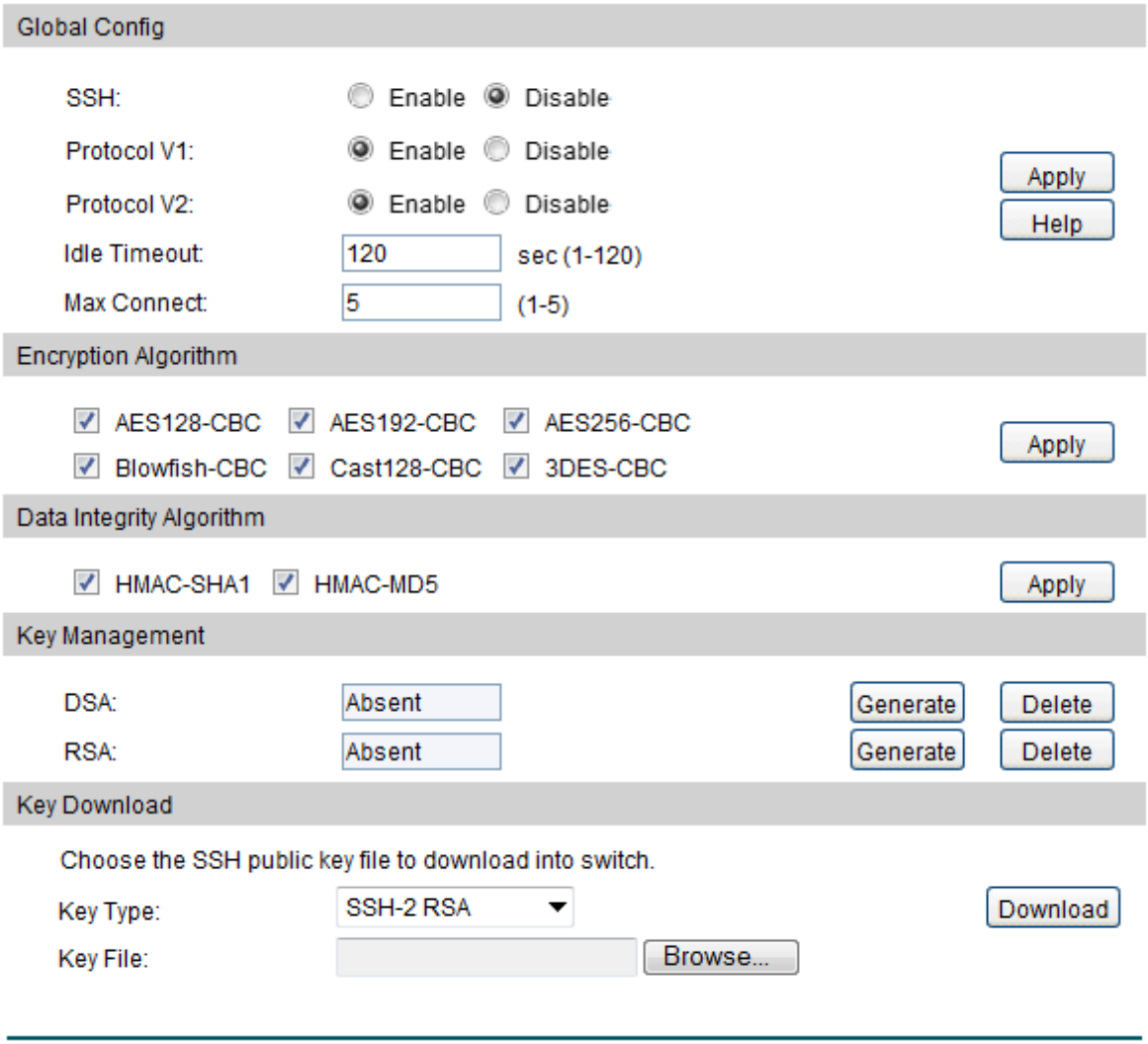


Figure 4-21 SSH Config

The following entries are displayed on this screen:

- **Global Config**

SSH: Enable or disable SSH function.

Protocol V1: Enable or disable SSH V1 to be the supported protocol.

Protocol V2: Enable or 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.

  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 Management**

  You can get the status of the DSA and RSA keys, which can also be generated or deleted here with the Generate and Delete buttons.

  DSA: The status of SSH-2 DSA key file (PEM Encoded) on the device, which might be Present or Absent.

  RSA: The status of SSH-1 RSA or SSH-2 RSA key file (PEM Encoded) on the device, which might be Present or Absent.

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

- **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.

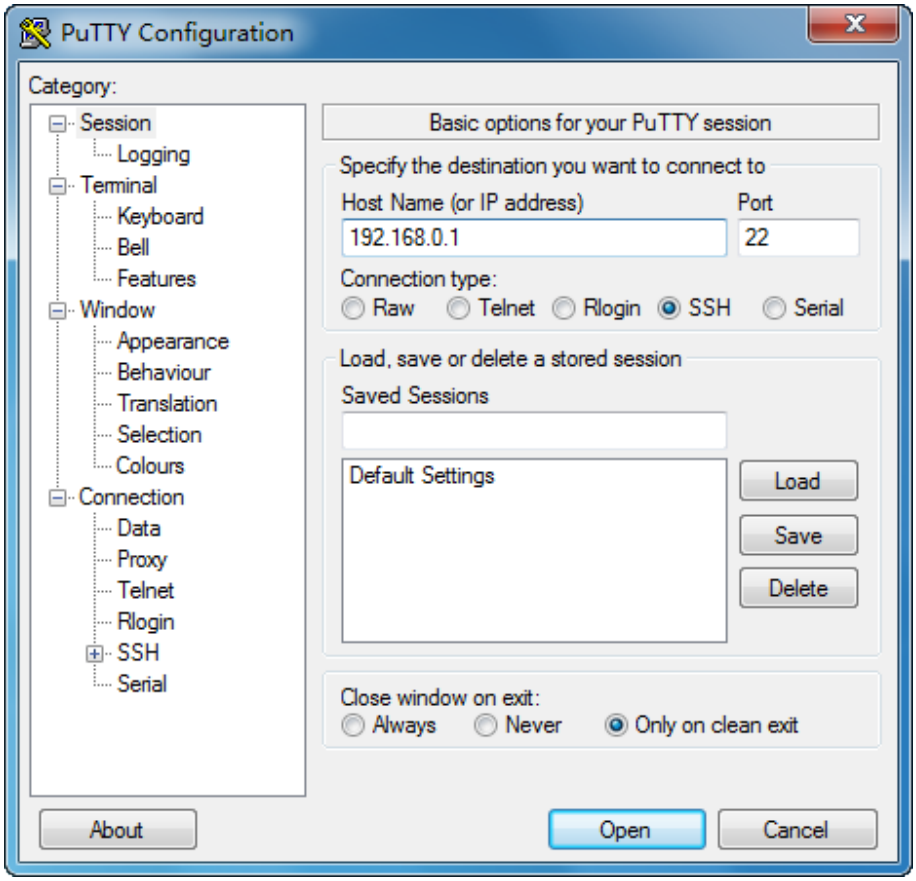
Application Example for SSH:

➢ **Network Requirements**

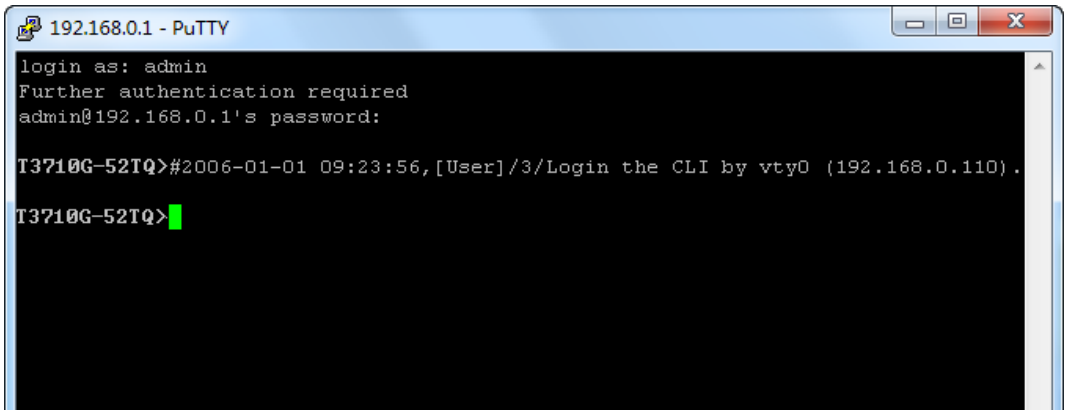
1. Log on to the switch via password authentication using SSH and the SSH function is enabled on the switch.
2. PuTTY client software is recommended.

➢ **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.



4.4.5 Telnet Config

On this page you can enable or disable Telnet function globally on the switch.

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

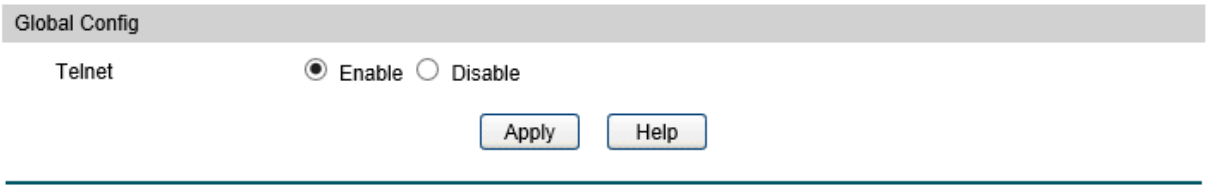


Figure 4-22 Access Control

The following entries are displayed on this screen:

➢ **Global Config**

Telnet: Enable or disable Telnet function globally on the switch.

4.5 SDM Template

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

4.5.1 SDM Template Config

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

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

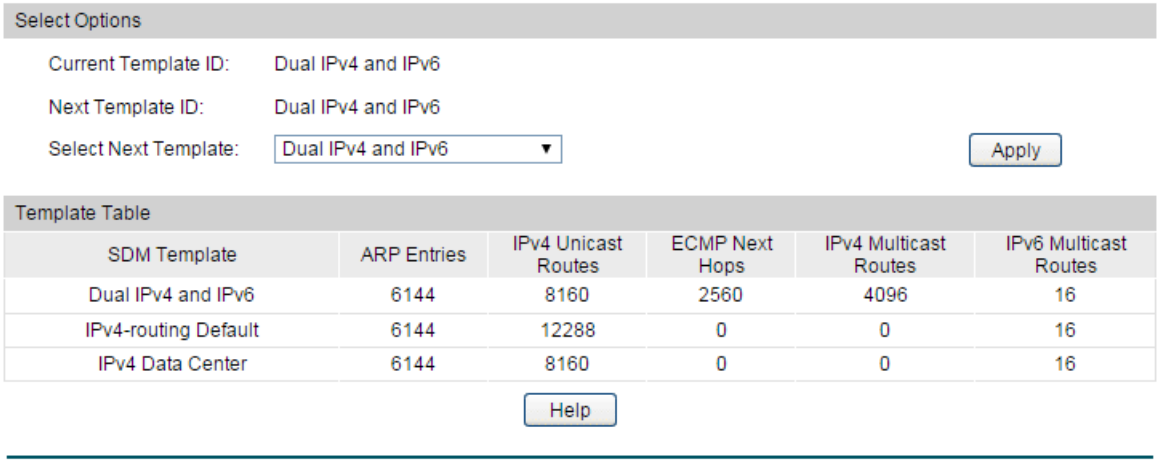


Figure 4-23 SDM Template Config

- **Select Options**

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

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

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

- **Template Table**

SDM Template: Displays the template name.

ARP Entries: The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.

IPv4 Unicast Routes: The maximum number of IPv4 unicast forwarding table entries.

ECMP Next Hops: The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.

IPv4 Multicast Routes: The maximum number of IPv4 multicast forwarding table entries.

IPv6 Multicast Routes: The maximum number of IPv6 multicast forwarding table entries.

Return to CONTENTS

Chapter 5 Stack

The stack technology is to connect multiple stackable devices through their stack ports, forming a stack which works as a unified system and presents as a single entity to the network in Layer 2 and Layer 3 protocols. It enables multiple devices to collaborate and be managed as a whole, which improves the performance and simplifies the management of the devices efficiently.

- **Advantages**

The stack delivers the following benefits:

1. Simplified management. After stack establishment, the user can log in the stack system through any stack ports of stackable devices, and manage it as a single device. You only need to configure the stack system once instead of operating repetitive configuration on multiple devices. Various ways such as CONSOLE, SNMP, TELNET and WEB are available for users to manage the stack.
2. High reliability. The stack is highly reliable in following aspects:
   1）The stack system is comprised of multiple devices among which one member device works as the stack master to take charge of the operation, management and maintenance of the stack, while the other stack members process services and keep a copy configuration file in accordance with the master for providing backup simultaneously. Once the stack master becomes unavailable, the remaining stack members elect a new master among themselves instantly and automatically, which can ensure uninterrupted services and furthermore making 1:N backup feasible. Due to the real-time configuration and data synchronization being strictly executed, the new master can take over the previous master to manage and maintain the stack system smoothly without affecting its normal operation.
   2）Distributed LACP (Link Aggregation Control Protocol) supports link aggregation across devices. Since the whole stack system presents as a single device on the network, external devices can implement LACP with the stack system by connecting to several stack member devices simultaneously. Among the links between the stack system and external devices, load distribution and backup can be realized to increase the reliability of the stack system and to simplify dramatically the network topology as Figure 5-1 shows.

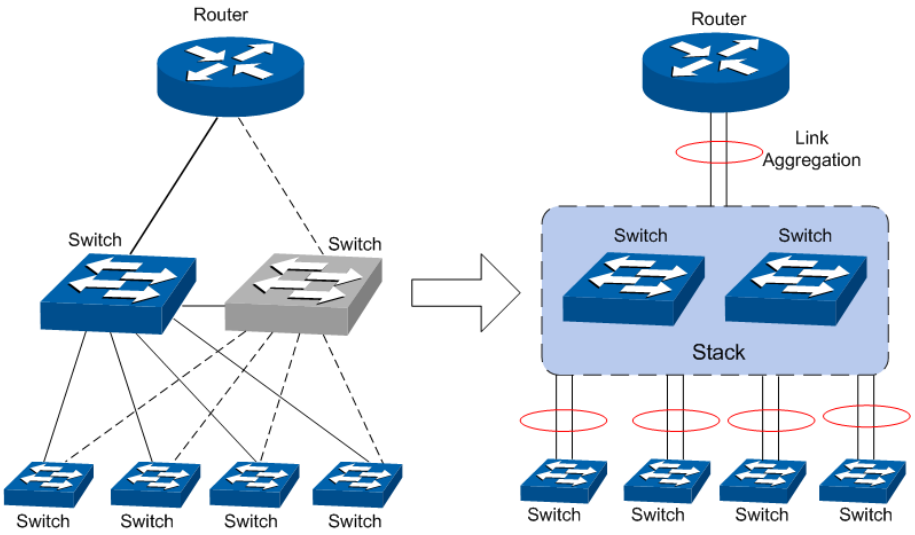


Figure 5-1 Distributed LACP

In a ring connected stack, it can still operate normally by transforming into a daisy chained stack when link failure occurs, which further ensures the normal operation of load distribution and backup across devices and links as Figure 5-2 shows.

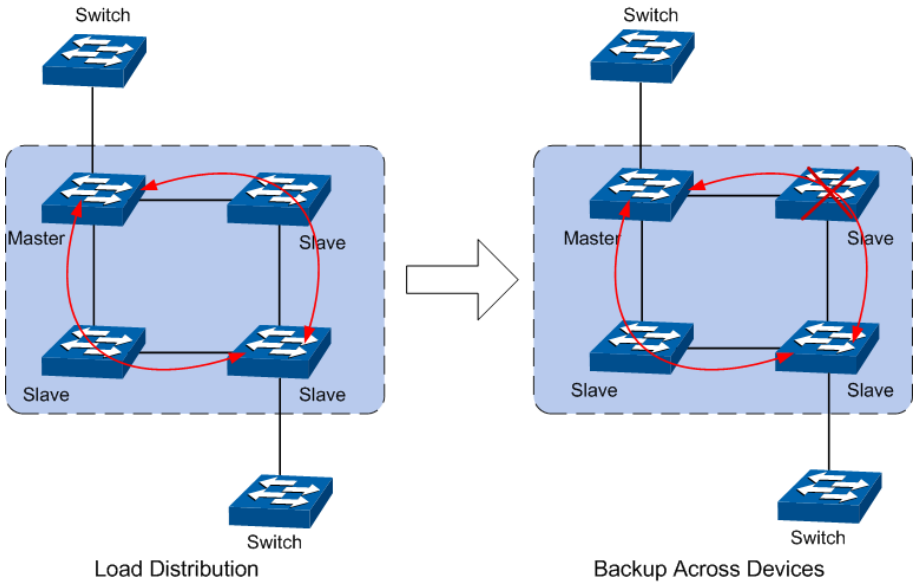


Figure 5-2 Load Distribution and Backup across Devices

3. Network scalability. Each member device in the stack system is able to process protocol packets and forward data individually, which enables you to increase the port number and bandwidth of the stack system by adding new member devices. The users are free to add or remove stack members without affecting the normal running of the stack, which enables them to protect the existed resources furthest during network upgrades.

➢ **Application Diagram**

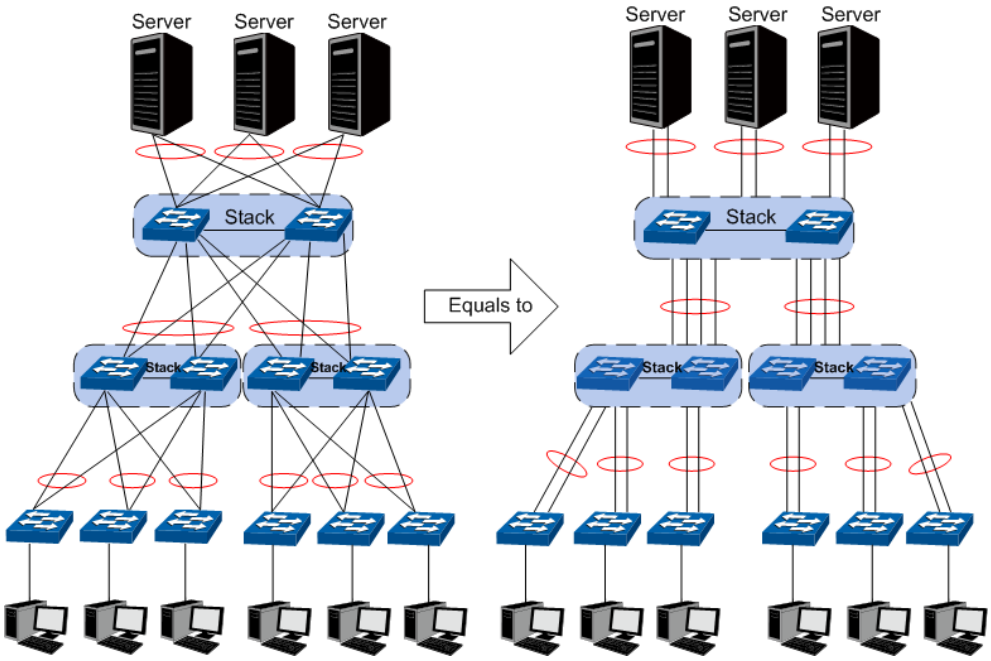


Figure 5-3 Application Diagram

➢ **Stack Introduction**

1. Stack Elements

1）Stack Role

Each device in the stack system is called stack member. Each stack member processes services packets and plays a role which is either master or member in the stack system. The differences between master and member are described as below:

- **Master:** Indicates the device is responsible for managing the entire stack system.
- **Member:** Indicates the device provides backup for the master. If the master fails, the stack will elect a new master from the remaining members to succeed the previous master.

2）Stack Event

Stack event indicates the global events which might happen during stack operation process, with two options:

- **Merge:** It occurs when two independent stacks merge into one stack because of stack link establishment, as shown in the following figure:

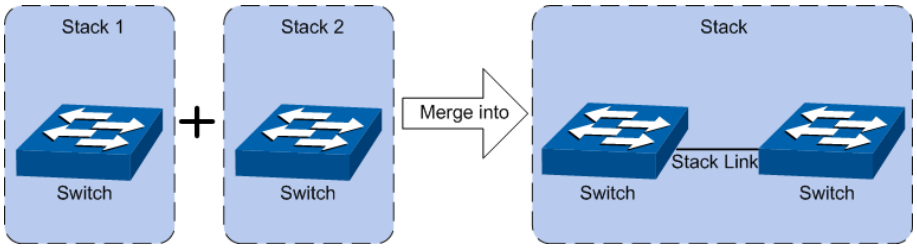


Figure 5-4 Stack Merge

When stack merge occurs, the previous masters compete to be the new master. The stack members of the defeated stack will join the winner stack as a member to form a new stack. Master will assign Unit Number to the newly joined members and compare their configuration files. The members with different configurations files with the master will download the configuration files of the master and re-configure.

- **Split:** It occurs when stack splits into two or more stacks because of stack link failures, as shown in the following figure:

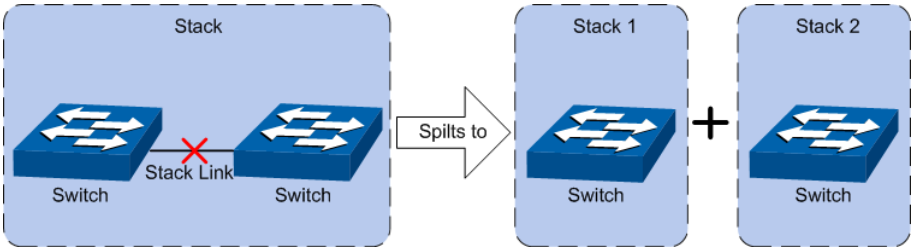


Figure 5-5 Stack Split

After stack partition occurs, each newly established stack elects their own new master and use the MAC address of the master as its stack MAC address. However, stack partition probably brings about routing and forwarding problems on the network since the partitioned stacks keep operating with the previous IP address by default, which results in same IP address being reused in the same LAN.

2. Operation Procedure

Stack management involves these four stages: Connecting the stack members, Topology collection, Master election, and Stack management and maintenance.

1）Connecting the stack members

To establish a stack, please physically connect the stack ports of the member devices with cables. The stack ports of T3700G-52TQ can be used for stack connection or as normal Ethernet Gigabit port. When you want to establish a stack, the stack mode of the related ports should be configured as "Enable". If the stack mode of the port is "Disable", then the port will work as a normal Ethernet port.

Stack typically adopts a daisy chain topology or ring topology as shown in Figure 5-6:

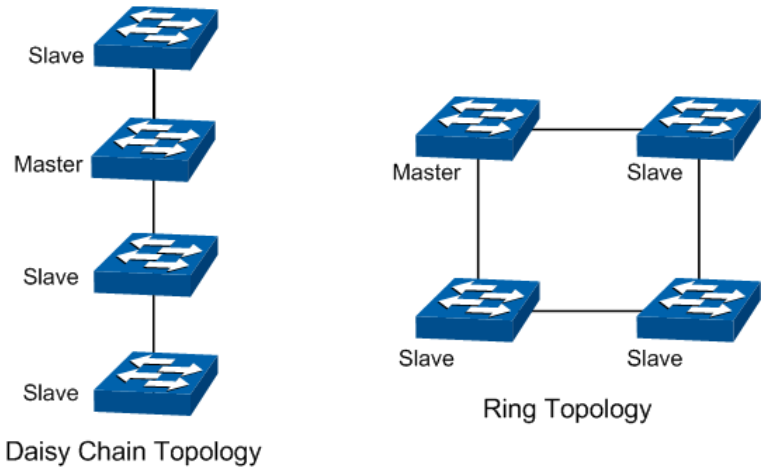


Figure 5-6 Stack Connect Topology

- The daisy chain topology is mainly used in a network where member devices are distributively located.
- The ring topology is more reliable than the daisy chain topology. In a daisy chained stack, link failure can cause stack split. While in a ring connected stack, the system is able to operate normally with a new daisy chained topology.

Note:

Establish a stack of ring or daisy chain topology with eight T3700G-52TQ switches at most.

2）Topology Collection

Each member in the stack collects the topology of the whole stack by exchanging stack discovery packets with its neighbors. Discovery packet carries topology information including stack port connection status, unit number, priorities, MAC addresses, etc.

Each member keeps a local record of the known topology information. When the device initializes, it only possesses the record of its own topology information. Periodically the stack members send out their known topology information through the stack ports to its neighbors. When the neighbors receive the information, they will update their local topology information. After a period of time of broadcasting and updating information, all the stack members can collect the complete topology information (known as topology convergence).

Then the switch enters the master election stage.

3）Master Election

After all members have obtained topology information (known as topology convergence), the stack enters the master election stage. A stack always has one stack master, while the other stack members are members. Master election determines the stack role of the stack members.

Master election is held each time the topology changes, for example, when stack merge or split occurs, or the stack or the current master is reset.

The master is elected based on the following rules and in the order listed:

1. The switch that is currently the stack master.
2. The switch with the highest stack member priority value.
3. The switch with the lowest MAC address.

After master election, the stack forms and enters into stack management and maintenance stage.

Note:

1. The priority value ranges from 1 to 15. The higher the value is, the more likely the member will be elected as the master. By default, the member priority of the switch is 5. We recommend you manually assign the highest priority value to the switch that you prefer to be the stack master before stack establishment.
2. The switch is non-preemptible when it joins the stack in cold-start mode, and the process is illustrated as bellow: the switch has no stack role at its start, and it sends out

discovery messages to collect the topology of the current stack system. After the topology collection, the switch obtains its role according to the rules above. The switch will become stack member if there is already a master in the stack. The master will resume its role even if the newly joined switch has a higher priority.

4）Stack Management and Maintenance

After the stack is established, all the stack members are integrated into a virtual device in the network and managed by the master. The following section briefly introduces the concepts and rules involved in stack management stage.

- **Unit Number:** When the stack is running, unit number is used to identify and manage member devices. Unit number is unique in a stack system. The factory default unit number of switch is 1. In order to keep its uniqueness, before establishing stack you are kindly recommended to prepare a unit number assignment scheme and then manually configure it on each member device.

  During unit number assignment process, the master prioritizes the member devices already carrying manually assigned unit number. If the unit number has not been used by other stack members the member device will keep it. Otherwise, the unit number is configured based on the following rules and in the order listed:

  1. The device which was managed by the current master before the configuration will resume its unit number.
  2. The device with manually assigned unit number is prior to the device whose unit number assignment mode is “Auto”.
  3. The device with the highest stack member priority value.
  4. The device with the lowest MAC address.

  Note:

  1. You can get the current unit number of the switch from the unit number LED on the front panel of the switch.
  2. When the stack is running, if you want to change the unit number manually, only the unit numbers which have not been occupied by the other member devices are available for you to choose from.

- **Port Number Format:**

  The format of port number should be Unit Number/Slot Number/Port Number. Among them:

  (1) Unit Number: The default unit number of the switch is 1. If a device has joined stack system, the unit number which the device possesses in the stack system will be kept using as its unit number after the device leaves the stack system.

  (2) Slot Number: Indicates the number of the slot the interface card is in. For T3700G-52TQ, the front panel ports belong to slot 0. Slot number starting from 1 each represents an interface card slot.

  (3) Physical Port Number: The physical port number on the switch which can be obtained through the front panel of the switch.

For instance: Port number 2/0/3 indicates the physical port3 on the switch whose unit number is 2.

- **Configuration Files Application Rules:** It includes global configuration and interface configuration two parts.

  (1) The global configurations of all stack members are the same. Besides, each member device keeps pace with the global configuration of the master device which enables the stack system to work just like a single entity in the network. The stack system adopts the following methods to ensure the synchronization of global configuration files:

  When the stack initializes, the master device will compare the configuration files of each stack member and reconfigure the device whose global configuration is different from its own, so as to ensure the global configuration of the stack members are exactly the same.

  When the stack is work normally, any global configuration of users will be recorded to the current configuration files of master and then be synchronized to the other members in the stack.

  (2) Each stack member only saves the configuration of its own ports. Even when user sets the configuration for all ports, the configuration will also be saved and implemented only on the related stack member which the ports belong to.

- **Stack Maintenance**

  Stack maintenance mainly functions to monitor the join and leave of member devices, collect the new topology at any times and maintain the current topology.

  When the stack is operating normally, packets are transmitted constantly between stack members. The switch can quickly judge the link status of the stack port via monitoring the response of the packets. When the switch detects the link status changes, it will recollect system topology and update topology database to ensure the normal operation of the stack.

  The events that will change the link status of the stack port which thus affecting the system topology include: stack member failure or leave, new member's coming, link failure or failure recovery, etc.

  When the master switch fails, the stack system elects a new master from the remaining members to succeed the previous master.

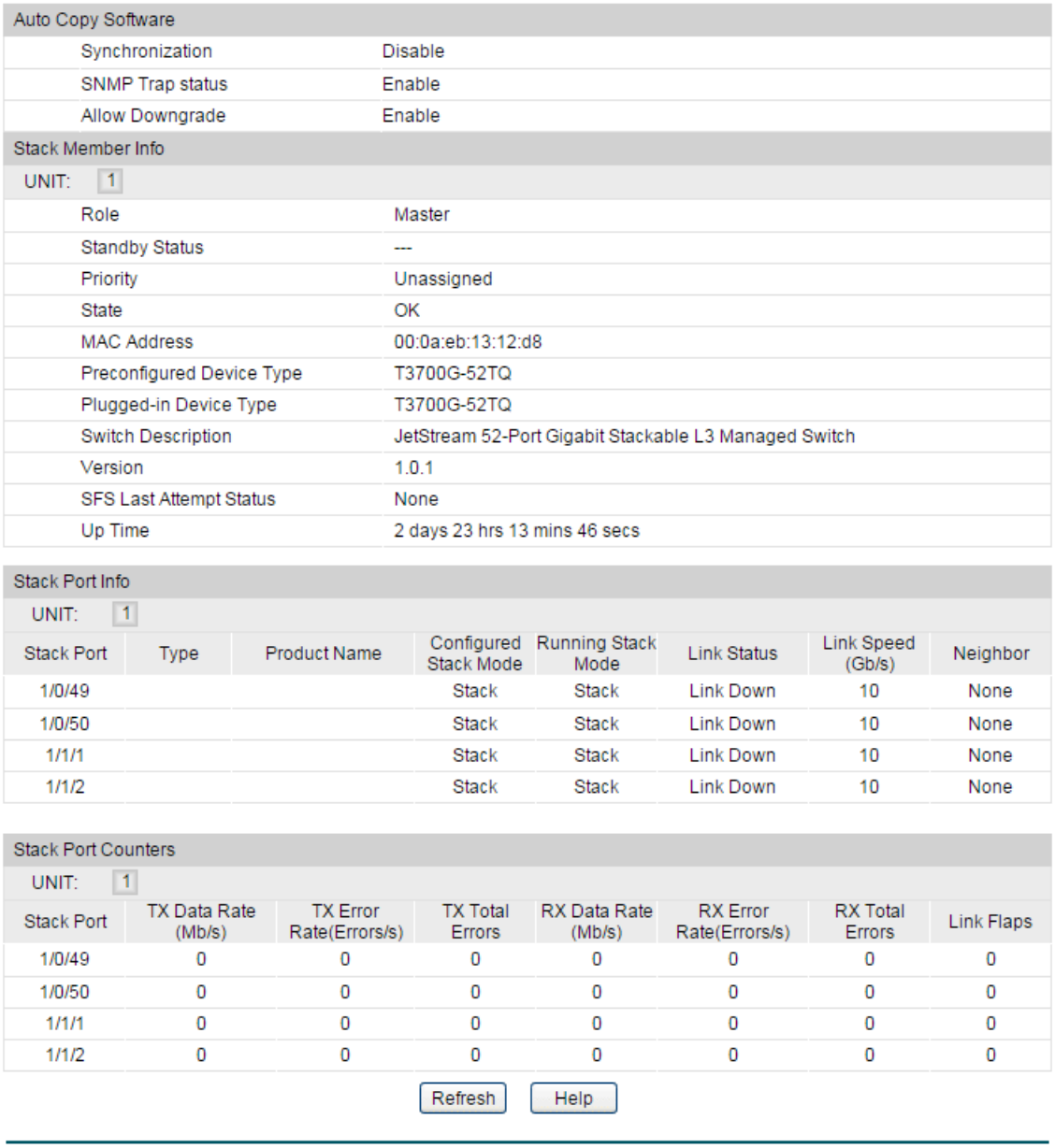
5.1 Stack Management

Before configuring the stack, we highly recommend you to prepare the configuration planning with a clear set of the role and function of each member device. Some configuration needs device reboot to take effect, so you are kindly recommended to configure the stack at first, next connect the devices physically after powering off them, then you can power them on and the devices will join the stack automatically. After stack is established, users can log in the stack system through any member devices to configure and manage it.

The stack management can be implemented on **Stack Info**, **Stack Config** and **Auto Copy Software** pages.

5.1.1 Stack Info

On this page you can view the basic parameters of the stack function. Choose the menu **Stack → Stack Management → Stack Info** to load the following page.



Auto Copy Software

Synchronization	Disable
SNMP Trap status	Enable
Allow Downgrade	Enable

Stack Member Info

UNIT: 1

Role	Master
Standby Status	---
Priority	Unassigned
State	OK
MAC Address	00:0a:eb:13:12:d8
Preconfigured Device Type	T3700G-52TQ
Plugged-in Device Type	T3700G-52TQ
Switch Description	JetStream 52-Port Gigabit Stackable L3 Managed Switch
Version	1.0.1
SFS Last Attempt Status	None
Up Time	2 days 23 hrs 13 mins 46 secs

Stack Port Info

UNIT: 1

Stack Port	Type	Product Name	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gb/s)	Neighbor
1/0/49			Stack	Stack	Link Down	10	None
1/0/50			Stack	Stack	Link Down	10	None
1/1/1			Stack	Stack	Link Down	10	None
1/1/2			Stack	Stack	Link Down	10	None

Stack Port Counters

UNIT: 1

Stack Port	TX Data Rate (Mb/s)	TX Error Rate(Errors/s)	TX Total Errors	RX Data Rate (Mb/s)	RX Error Rate(Errors/s)	RX Total Errors	Link Flaps
1/0/49	0	0	0	0	0	0	0
1/0/50	0	0	0	0	0	0	0
1/1/1	0	0	0	0	0	0	0
1/1/2	0	0	0	0	0	0	0

Refresh Help

Figure 5-7 Stack Info

Configuration Procedure:

View the basic parameters of the stack function.

Entry Description:

- **Auto Copy Software**

Synchronization: Displays the status of the Auto Copy Software function.

SNMP Trap status: Displays the SNMP trap status of the Auto Copy Software function.

Allow Downgrade:	Displays the status of allowing downgrade of the new members in the Auto Copy Software function.

- **Stack Member Info**

UNIT:	Displays the unit number of the switch.
Role:	Displays the stack role of the switch in the stack. There are two options: Master and Member.
Priority:	Displays the member priority of the switch. The higher the value is, the more likely the member will be elected as the master.
State:	Displays the state of the switch.
MAC Address	Displays the unique identification of the switch.
Preconfigured Device Type:	Displays the device type of the pre-configured switch.
Plugged-in Device Type:	Displays the device type of the plugged-in switch.
Switch Description:	Displays the description of the switch.
Version:	Displays the current software version of the switch.
SFS Last Attempt Status:	Displays the status of the last stack firmware synchronization.
Up Time:	Displays the system up time of the switch.

- **Stack Port Info:**

Stack Port:	Displays the stack port number.
Type:	Displays the transceiver type of the stack port
Product Name:	Displays the transceiver product name of the stack port.
Configured Stack Mode：	Displays the configured mode of the stack port.
Running Stack Mode：	Displays the running mode of the stack port.
Link Status：	Displays the link status of the stack port.
Link Speed:	Displays the link speed of the stack port.
Neighbor:	Displays the unit id of the switch directly linked on the stack port.

5.1.2 Stack Config

On this page you can configure the basic parameters of the stack function.

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

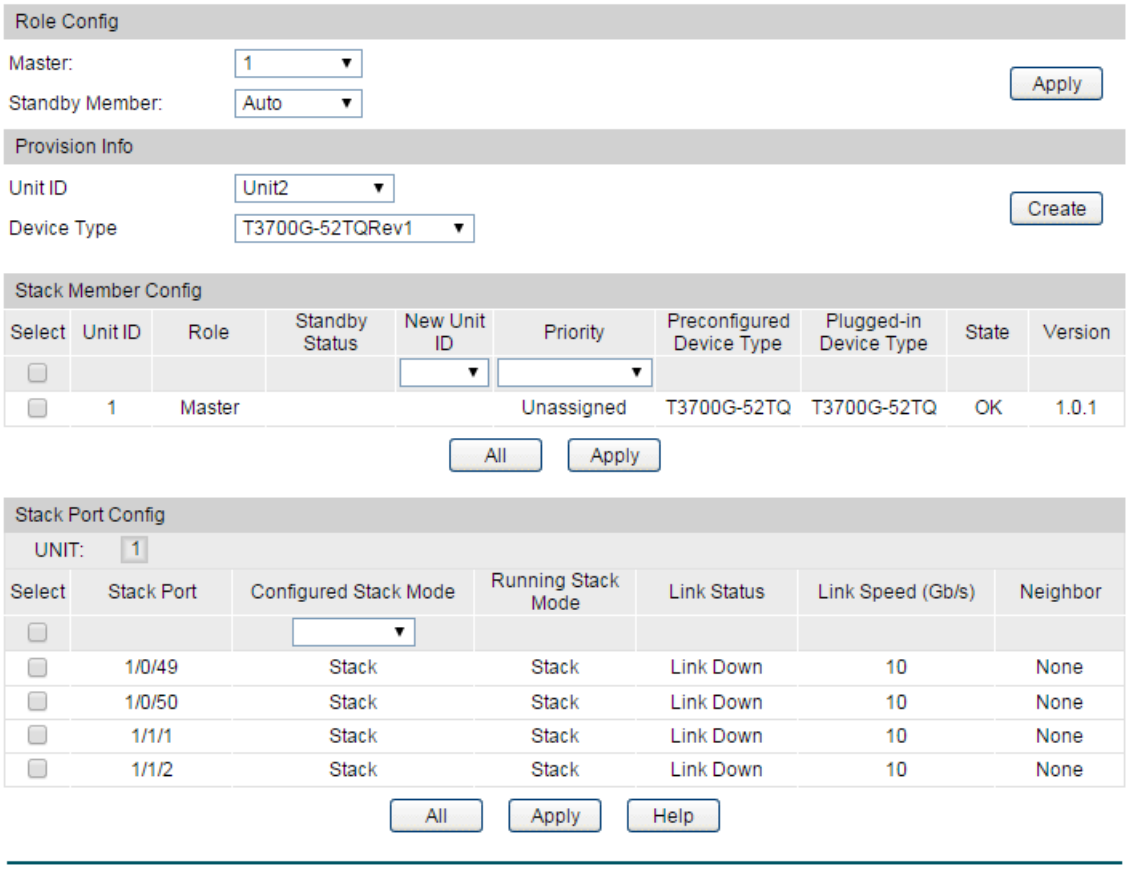


Figure 5-8 Stack Config

Configuration Procedure:

1) Set the role of a specified switch in the stack.
2) Configure the provisioned member switch.
3) Configure the Unit ID and Priority for the Stack Member.
4) Configure the SFP+ port's stacking feature.

Entry Description:

- **Role Config**

  Master: Set the switch as master.

  Standby Member: Set the switch as standby member.

- **Provision Info**

  Unit ID: Configure the switch number of the provisioned switch.

  Device Type: Configure the switch type of the provisioned switch.

- **Stack Member Config**

  Unit ID: Displays the switch number of the provisioned switch.

  Role: Displays the role of the switch in the stack: master or member.

  Standby Status: Displays the standby status of the switch.

New Unit ID:	Configure a new unit number of the switch.
Priority:	Configure the priority used in master election. Large first. The priority change will not take effect until next election.
Preconfigured Device Type:	Displays the switch type of the provisioned switch.
Plugged-in Device Type:	Displays the device type of the plugged-in switch.
State:	Displays the state of the switch.
Version:	Displays the software version of the switch.

- **Stack Port Config**

Select:	Select the SFP+ port.
Stack Port:	Displays the ports that can be configured as stack ports.
Configured Stack Mode :	Configure the SFP+ port to be an Ethernet port or a stack port.
Running Stack Mode:	Displays whether the port is an Ethernet port or a stack port at the moment.
Link Status:	Displays the link status of the stack port.
Link Speed (Gb/s):	Displays the link speed of the stack port.
Neighbor:	The unit id of the switch directly links on the stack port.

5.1.3 Auto Copy Software

To resolve the code mismatch in stack attaching, the new members will copy software from the master.

Choose the menu **Stack** → **Stack Management** → **Auto Copy Software** to load the following page.

Figure 5-9 Auto Copy Software

Configuration Procedure:

View and configure the Auto Copy Software function.

Entry Description:

Synchronization:	Enable or disable the Auto Copy Software function.

SNMP Trap status: Enable or disable SNMP trap of the Auto Copy Software function.

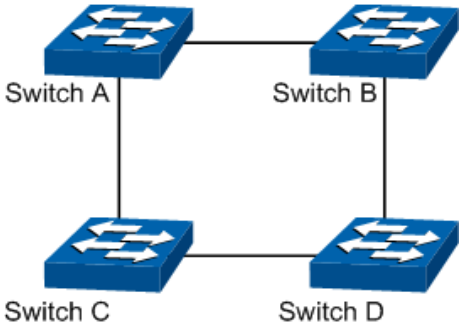
Allow Downgrade: Enable or disable downgrade of the new members in the Auto Copy Software function. If you choose enable, the member's software version is allowed to downgrade when copying software from the master.

5.2 Application Example for Stack

➢ **Network Requirements**

Establish a stack of ring topology with four T3700G-52TQ switches.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A, B, C and D before physically connecting them:

Step	Operation	Description
1	Configure stack mode.	Required. On **Stack Management** → **Stack Config** page, configure the port's stack mode as "Stack" in **Stack Port Config** section.
2	Configure unit ID.	Optional. On **Stack Management** → **Stack Config** page, configure the unit ID of switch A, B, C and D as 1, 2, 3 and 4 respectively in **Stack Member Config** section.
3	Configure the role of the switch in the stack.	Optional. On **Stack Management** → **Stack Config** page, configure the role of switch A as Master, the role of switch B, C, D as Member in **Role Config** section.
4	Configure the Auto Copy Software function.	Optional. On **Stack Management** → **Auto Copy Software** page, enable Auto Copy Software function.

- Connect the switches:

Connect switch A, B, C and D as the network diagram shows, and then power the switches on to establish a stack.

Return to CONTENTS

Chapter 6 Switching

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

6.1 Port

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

6.1.1 Port Config

On this page, you can configure port status, speed mode, duplex mode, flow control and jumbo frames for ports.

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

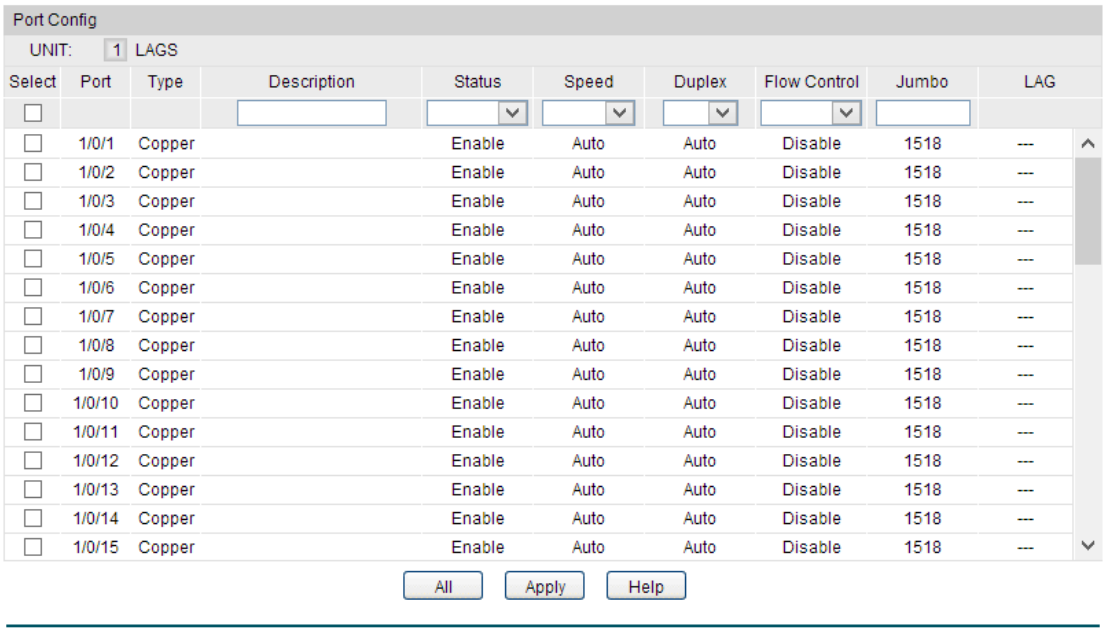


Figure 6-1 Port Config

Configuration Procedure:

Select and configure your desired ports or LAGs. Then click **Apply** to make the settings effective.

Entry Description:

UNIT: Click **1** to configure physical ports. Click **LAGS** to configure LAGs.

Type: Displays the port type. **Copper** indicates an Ethernet port, and **Sfp** indicates a fiber port.

Description:	Give a port description for identification.
Status:	With this option enabled, the port forwards packets normally. Otherwise, the port discards all the received packets. By default, it is enabled.
Speed:	Select the appropriate speed mode for the port. When **Auto** is selected, the port autonegotiates speed mode with the connected device. The default setting is **Auto**. This value is recommended if both ends of the line support autonegotiation.
Duplex:	Select the appropriate duplex mode for the port. There are three options: **Half**, **Full** and **Auto**. When Auto is selected, the port autonegotiates duplex mode with the connected device. The default setting is Auto.
Flow Control:	With this option enabled, the switch synchronizes the data transmission speed with the peer device, thus avoiding the packet loss caused by congestion. By default, it is disabled.
Jumbo	With this option properly configured, the port can send jumbo frames. The default MTU (Maximum Transmission Unit) size for frames received and sent on all ports is 1518 bytes. You can specify the MTU size up to 13312 bytes, thus allowing the port to send jumbo frames.
LAG:	Displays the LAG 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. We recommend that you set the ports on both ends of a link as the same speed and duplex mode.

6.1.2 Port Mirror

This function allows the switch to forward packet copies of the monitored ports to a specific monitoring port. Then you can analyze the copied packets to monitor network traffic and troubleshoot network problems.

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

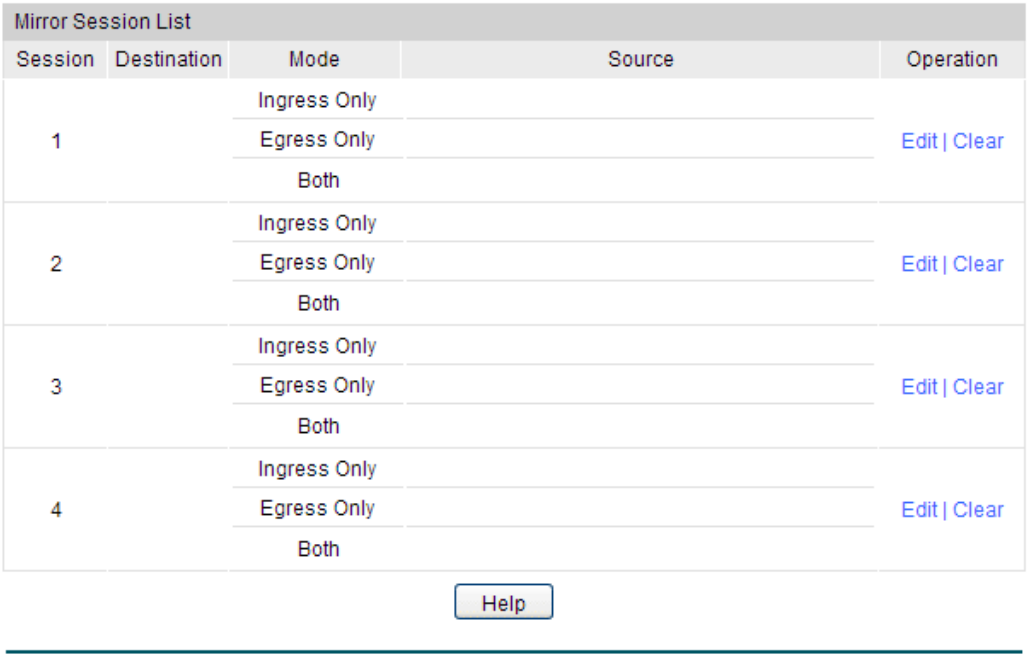


Figure 6-2 Mirror Session List

The above page displays a mirror session, and no more session can be created. Click **Edit** to configure the mirror session on the following page.

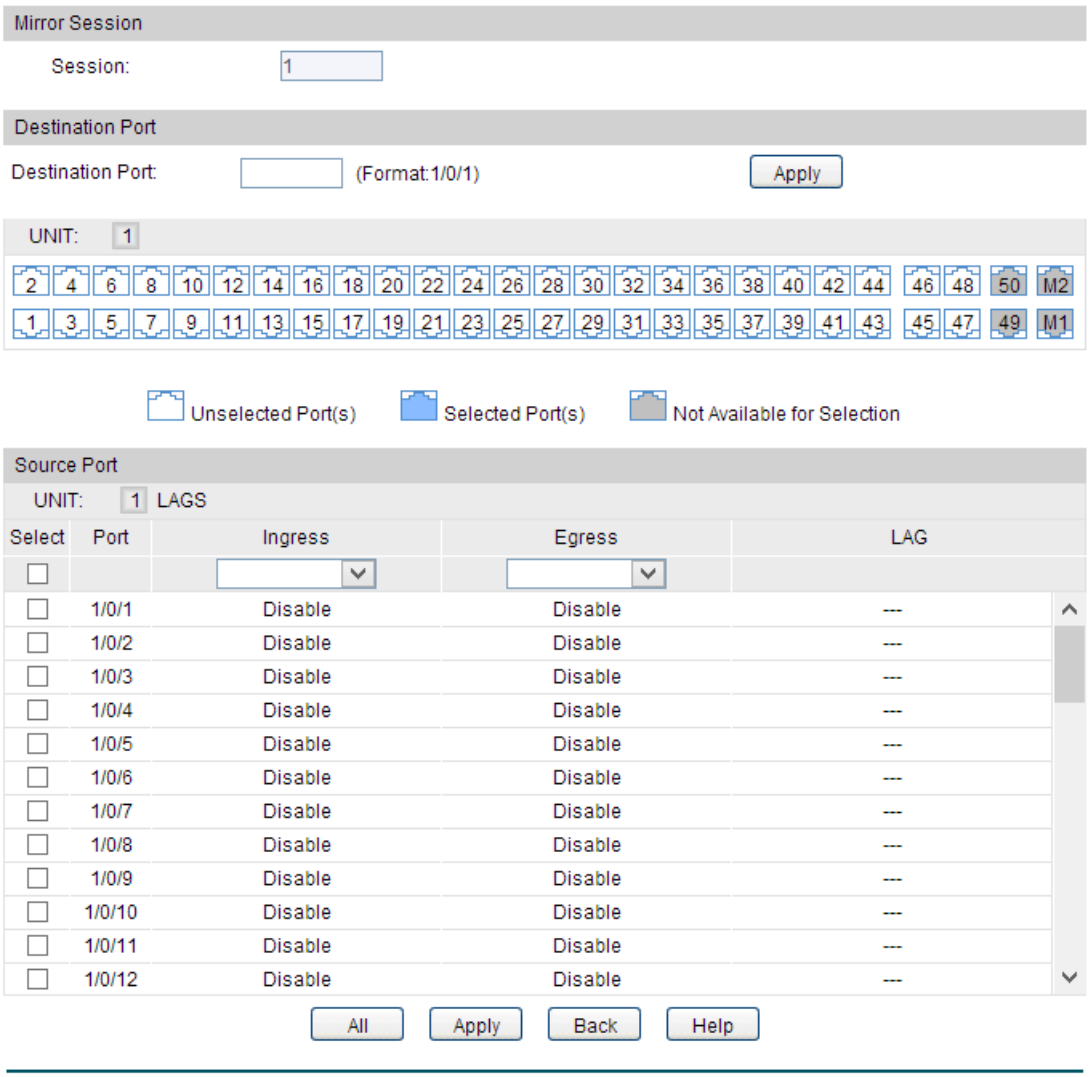


Figure 6-3 Port Mirror Config

Configuration Procedure:

1) In the **Destination Port** section, specify a monitoring port for the mirror session, and click **Apply**.

2) In the **Source Port** section, select one or multiple monitored ports for configuration. The set the parameters and click **Apply** to make the settings effective.

Entry Description:

Session: Displays session number.

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

Ingress: With this option enabled, the packets received by the monitored port will be copied to the monitoring port. By default, it is disabled.

Egress: With this option enabled, the packets sent by the monitored port will be copied to the monitoring port. By default, it is disabled.

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

Note:

1. The member port of a LAG cannot be set as a monitoring port or monitored port.
2. A port cannot be set as the monitoring port and monitored port at the same time.

6.1.3 Port Security

You can use this feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets.

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

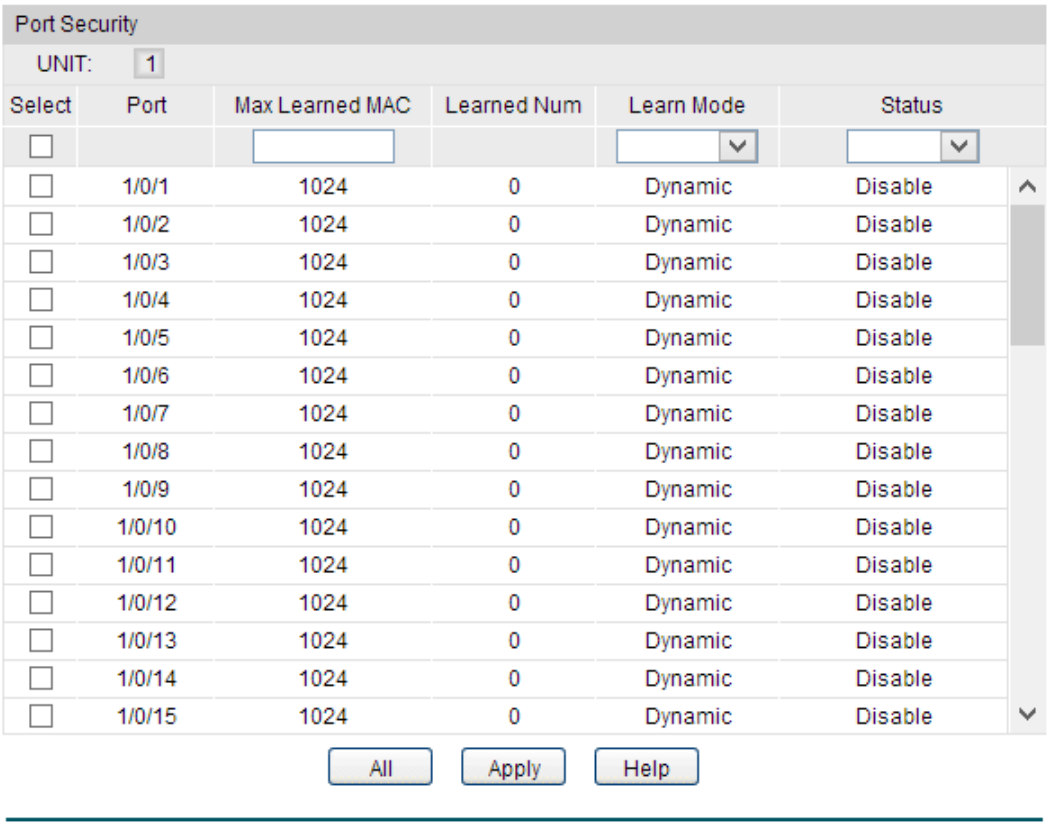


Figure 6-4 Port Security

Configuration Procedure:

1) Select one or multiple ports for security configuration.
2) Specify the maximum number of the MAC addresses that can be learned on the port, and then select the learn mode of the MAC addresses.
3) Select the status of the port security feature.
4) Click **Apply** to make the settings effective.

Entry Description:

Max Learned MAC:	Specify the maximum number of MAC addresses that can be learned on the port. When the learned MAC address number reaches the limit, the port will stop learning.
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:** The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting. • **Static:** The learned MAC addresses are 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.
Status:	Enable or disable the port security feature on the port. By default, it is disabled.

Note:

1. Port Security cannot be enabled on the member port of a LAG, and the port with Port Security enabled cannot be added to a LAG.
2. On one port, Port Security and 802.1X cannot be enabled at the same time.ort Security function is disabled when the 802.1X function is enabled.

6.1.4 Protected Ports

This feature is used to restrict the communication between the specific ports. A port that is a member of a protected ports group is a protected port. Protected ports in the same protected ports group cannot forward traffic to each other, even if they are in the same VLAN. But the protected ports can forward traffic to the unprotected ports and the ports that are in a different group.

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

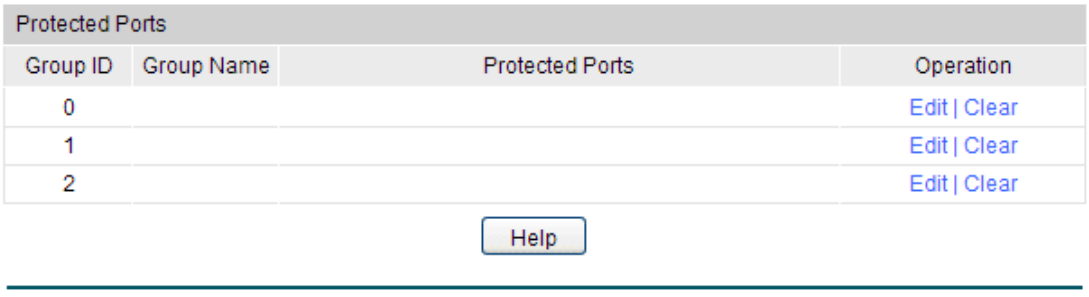
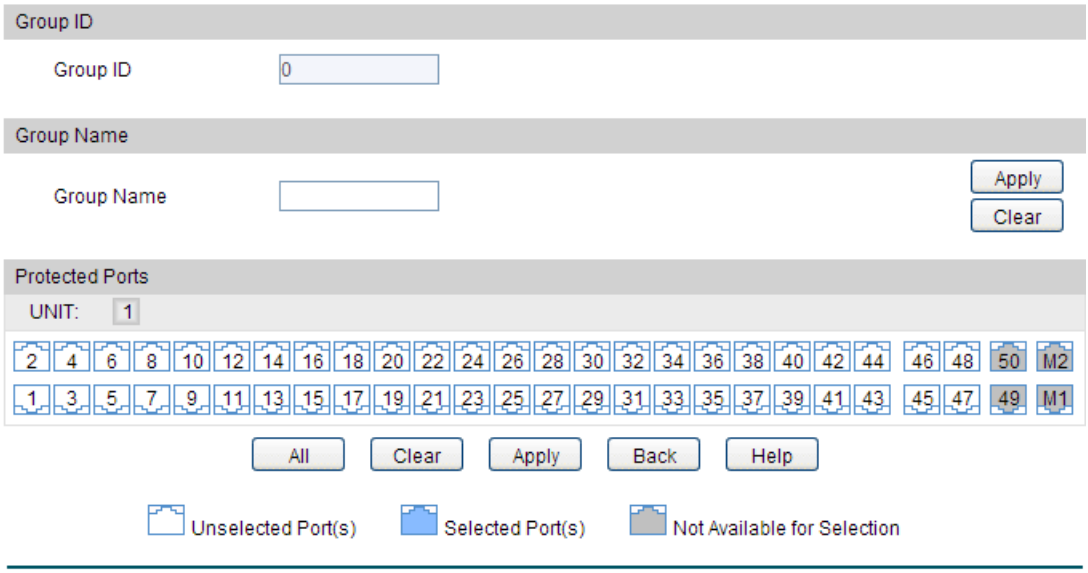


Figure 6-5 Port Isolation Config

The above page displays the information of protected ports groups. Click **Edit** to configure the group on the following page.



Configuration Procedure:

Select and configure your desired ports or LAGs. Then click **Apply** to make the settings effective.

Entry Description:

Group:	Displays the ID of the group for configuration.
Group Name:	Give a group name for identification.
Protected Ports:	Select member ports in this group. Protected ports in the same group cannot forward traffic to each other, even if they are in the same VLAN. But the protected ports can forward traffic to the unprotected ports and the ports that are in a different group.

6.1.5 Loopback Detection

Loopback Detection allows the switch to detect loops in the network. When a loop is detected on a port, the switch will display an alert on the management interface and further block the corresponding port according to your configurations.

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

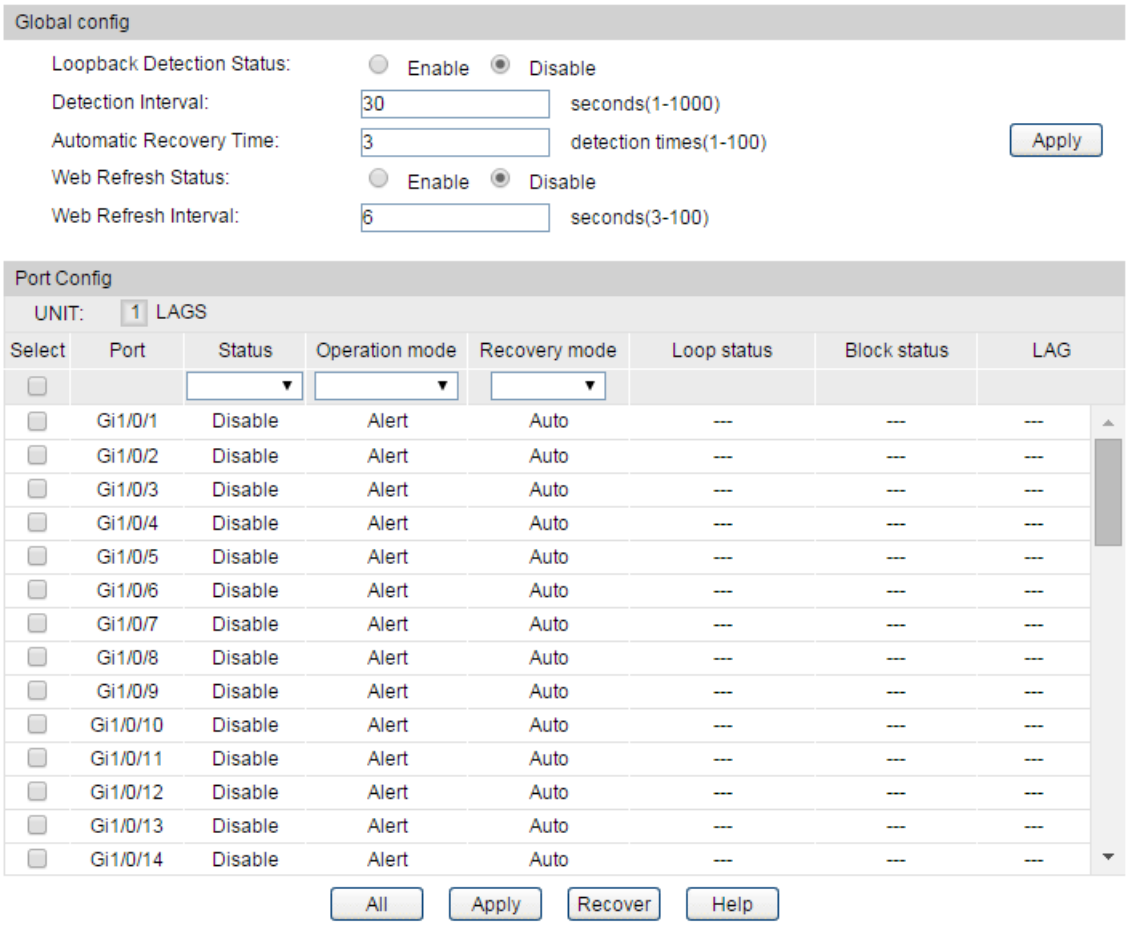


Figure 6-7 Loopback Detection Config

Configuration Procedure:

1) In the **Global Config** section, enable loopback detection and configure the global parameters. Then click **Apply** to make the settings effective.
2) In the **Port Config** section, select one or multiple ports for configuration. Then set the parameters and click **Apply** to make the settings effective.
3) View the loopback detection information on this page.

Entry Description:

➢ **Global Config**

LoopbackDetection Status:	Enable loopback detection globally.
Detection Interval:	Set the interval of sending loopback detection packets. The value ranges from 1 to 1000 seconds and the default value is 30 seconds.

Automatic Recovery Time:	Set the recovery time globally, after which the blocked port in Auto Recovery mode can automatically recover to normal status. It should be integral times of detection interval. The value ranges from 1-100 and is 3 by default
Web Refresh Status:	With this option enabled, the switch refreshes the web timely. By default, it is disabled.
Web Refresh Interval:	If you enabled web refresh, set the refresh interval between 3 and 100 seconds. The default value is 6 seconds.

➢ **Port Config**

Status:	Enable loopback detection for the port.
Operation Mode:	Select the operation mode when a loopback is detected on the port: ● **Alert:** The switch will display alerts. It is the default setting. ● **Port based:** In addition to displaying alerts, the switch will block the port on which the loop is detected.
Recovery Mode:	If you select **Port Based** as the operation mode, you also need to configure the recovery mode for the blocked port: ● **Auto:** The blocked port will automatically recover to normal status after the automatic recovery time. It is the default setting. ● **Manual:** You need to manually release the blocked port. Click the **Recovery** button to release the selected port.
Loop Status:	Displays whether a loop is detected on the port.
Block Status:	Displays whether the port is blocked.
LAG:	Displays the LAG number the port belongs to.

Note:

1. Recovery Mode is not selectable when Alert is chosen in Operation Mode.
2. To avoid broadcast storm, we recommend that you enable storm control before loopback detection is enabled.

6.1.6 Default Settings

Feature	Default Settings
Port Config	Type: Copper Status: Enable Speed: Auto Duplex: Auto Flow Control: Disable Jumbo: 1518
Port Mirror	Ingress: Disable Egress: Disable
Port Security	Max Learned MAC: 1024 Learned Num: 0 Learned Mode: Dynamic Status: Disable
Loopback Detection	Loopback Detection Status: Disable Detection Interval: 30 seconds Automatic Recovery Time: 3 detection times Web Refresh Status: Disable Web Refresh Interval: 6 seconds Port Status: Disable Operation mode: Alert Recovery mode: Auto

Return to CONTENTS

6.2 LAG

With the LAG (Link Aggregation Group) function, you can aggregate multiple physical ports into a logical interface to increase link bandwidth and configure the backup ports to enhance the connection reliability. You can configure LAG in two ways:

- **Static LAG**: The member ports are manually added to the LAG.
- **LACP (Link Aggregation Control Protocol)**: The switch uses LACP to implement dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. LACP extends the flexibility of the LAG configuration.

For the functions like **IGMP Snooping, 802.1Q VLAN, MAC VLAN, Protocol VLAN, VLAN-VPN, GVRP, Voice VLAN, STP, QoS, DHCP Snooping** and **Flow-Control**, the member pot of a LAG follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

The port which is enabled with **Port Security, Port Mirror, MAC Address Filtering** or **802.1X** cannot be added to LAG, and the member port of a LAG cannot be enabled with these functions.

The configuration guidelines are as follows:

- Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should be set as LACP mode.
- Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.
- A port cannot be added to more than one LAG at the same time.
- LACP does not support half-duplex links.
- One static LAG supports up to eight member ports. All the member ports share the traffic evenly. If an active link fails, the other active links share the traffic evenly.
- One LACP LAG supports more than eight member ports, but at most eight of them can be active. Using LACP protocol, the switches negotiate parameters and determine the active ports. When an active link fails, the link with the highest priority among the inactive links will replace the faulty link and start to forward data.
- 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.

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.

6.2.1 LAG Table

On this page, you can view the information of the current LAG of the switch and configure the Load-balancing Algorithm.

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

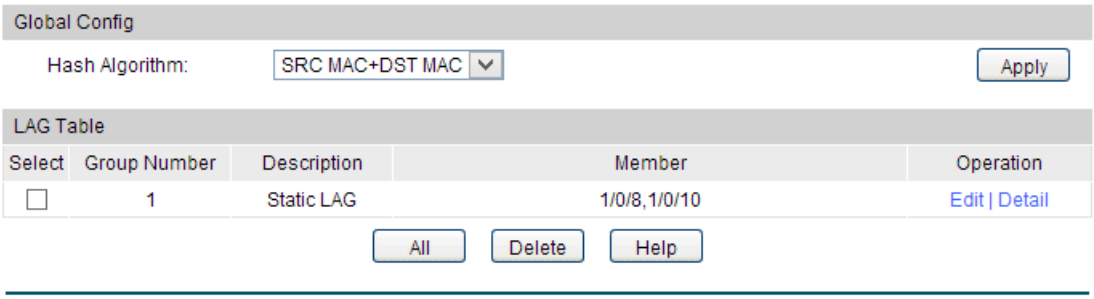


Figure 6-8 LAG Table

Configuration Procedure:

In the **Global Config** section, select the load-balancing algorithm. Click **Apply** to make the settings effective.

In **LAG Table**, view the information of the current LAG .

Entry Description:

Hash Algorithm: Select the Hash Algorithm, based on which the switch can choose the port to send the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. There are six options:

- **SRC MAC**: The computation is based on the source MAC addresses of the packets.
- **DST MAC**: The computation is based on the destination MAC addresses of the packets.
- **SRC MAC+DST MAC**: The computation is based on the source and destination MAC addresses of the packets.
- **SRC IP**: The computation is based on the source IP addresses of the packets.
- **DST IP**: The computation is based on the destination IP addresses of the packets.
- **SRC IP+DST IP**: The computation is based on 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.

Description: Displays the description of LAG.

Member: Displays the LAG member.

Operation: Click **Edit** to modify the settings of the LAG.

Click **Detail** to get the detailed information of the LAG.

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

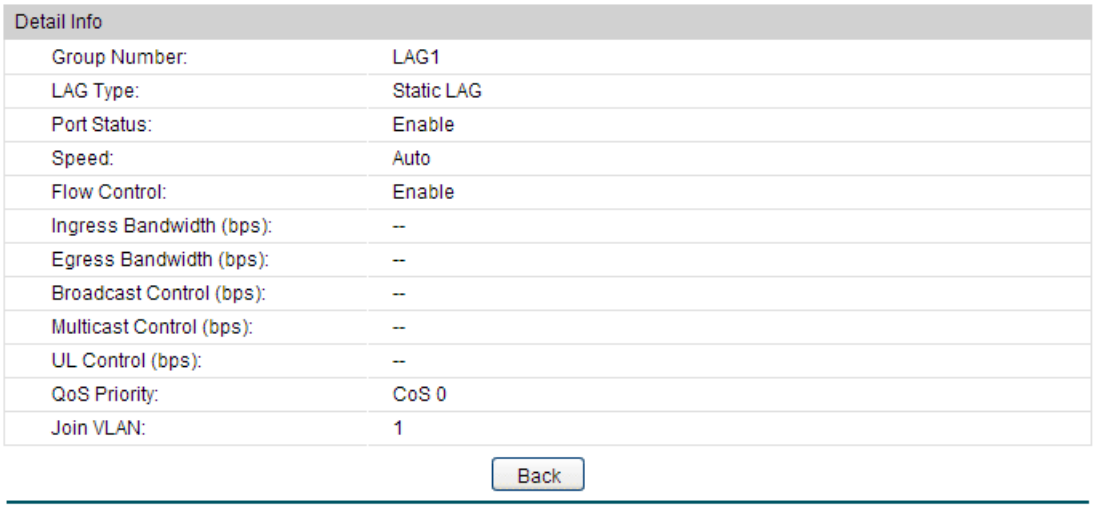


Figure 6-9 Detail Information

6.2.2 Static LAG

On this page, you can manually configure the LAG. The LACP feature is disabled for the member ports of the manually added Static LAG.

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

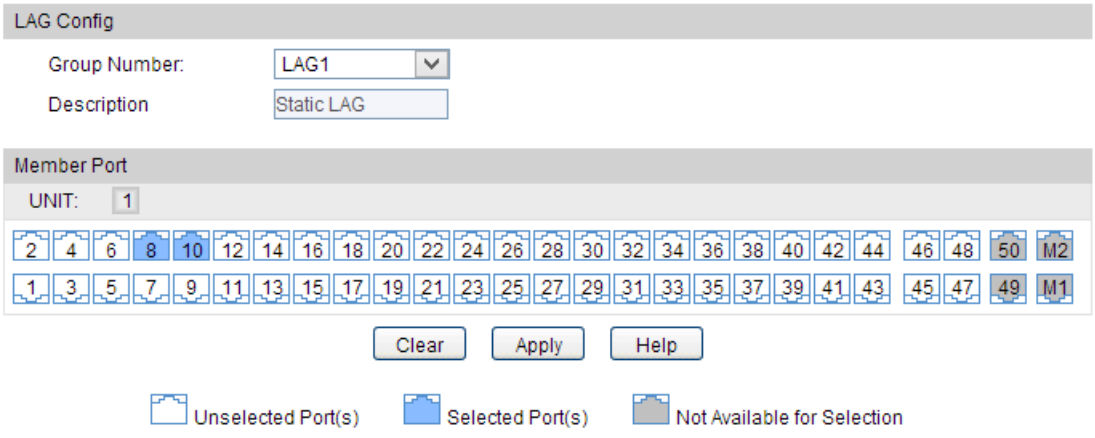


Figure 6-10 Static LAG Config

Configuration Procedure:

Select and configure your desired ports or LAGs. Then click **Apply**.

Entry Description:

Group Number: Select a Group Number for the LAG.

Description: Displays the description of the LAG for identification.

➢ **Member Port**

UNIT: Select the unit ID of the desired member in the stack.

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

Tips:

1. Load-balancing algorithm is effective only for outgoing traffic. If the data stream is not well shared by each link, you can change the algorithm of the outgoing interface.
2. Please properly choose the load-balancing algorithm to avoid data stream transferring only on one physical link. For example, if the destination device of the packets is a server with the fixed MAC address and IP address, you can set the algorithm as "SRC MAC+SRC IP" to allow the switch to determine the forwarding port based on the source MAC addresses and source IP addresses of the received packets.

6.2.3 LACP Config

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

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

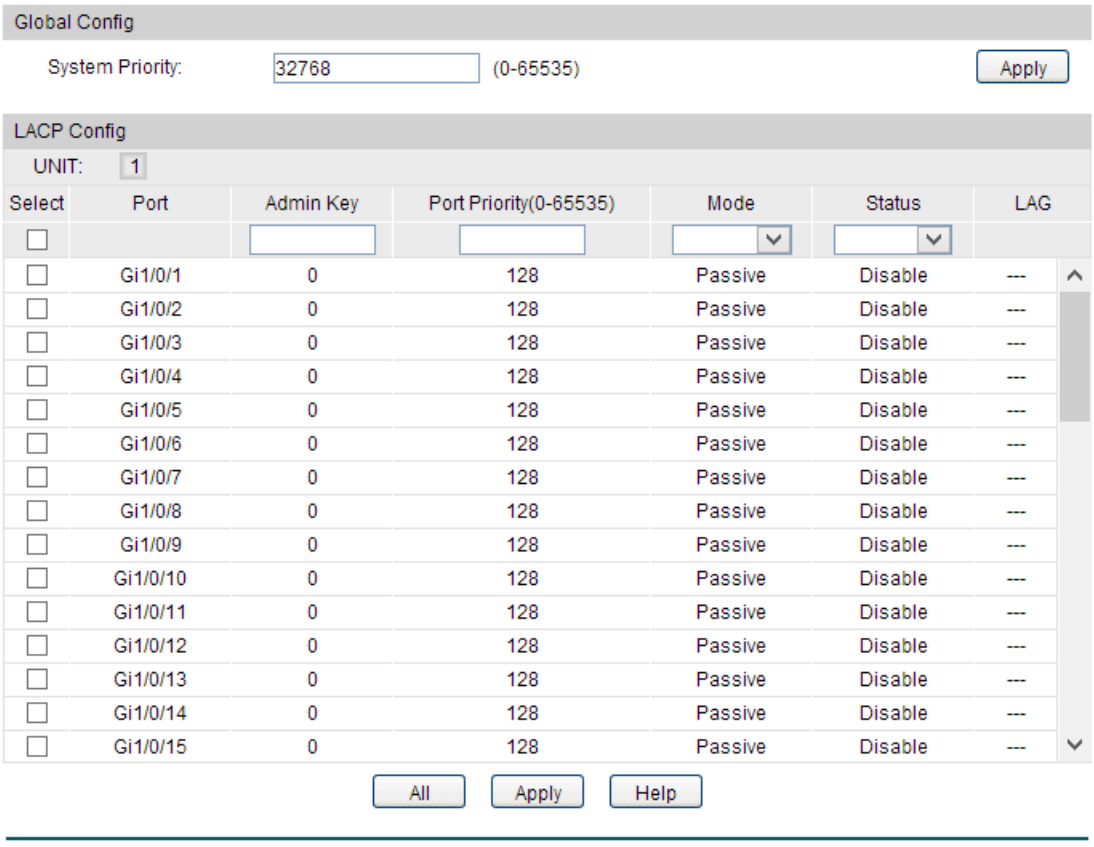


Figure 6-11 LACP Config

Configuration Procedure:

1) In the **LAG Config** section, select a LAG for configuration.

2) In the **Member Port** section, select the member ports for the LAG. It is multi-optional.

3) Click **Apply**.

Entry Description:

System Priority: Specify the system priority for the switch. A smaller value means a higher priority.

To keep active ports consistent at both ends, you can set the priority of one device to be higher than that of the other device. The device with higher priority will determine its active ports, and the other device can select its active ports according to the selection result of the device with higher priority. If the two ends have the same system priority value, the end with a smaller MAC address has the higher priority.

Admin Key: Specify the Admin Key which you can regard as the group number of the LAG.

Note that the group number of other static LAGs cannot be set as an Admin Key. The valid value ranges from 1 to 64.

Port Priority: Specify the Port Priority. A smaller value means a higher port priority.

The port with higher priority in an LAG will be selected as the active port to forward data. If two ports have the same priority value, the port with a smaller port number has the higher priority.

Mode: Select the LACP mode for the port.

In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. The LACP mode determines whether the port will take the initiative to send the LACPDU. There are two modes:

Passive: The port will not send LACPDU before receiving the LACPDU from the peer end.

Active: The port will take the initiative to send LACPDU.

Status: Enable the LACP function of the port. By default, it is disabled.

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

6.2.4 Default Settings

Feature	Default Settings
Global Config	Hash Algorithm: SRC MAC + DST MAC

LACP	System Priority: 32768 Admin Key: 0 Port Priority: 0 Mode: Passive Status: Disable

6.3 Traffic Monitor

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

6.3.1 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.

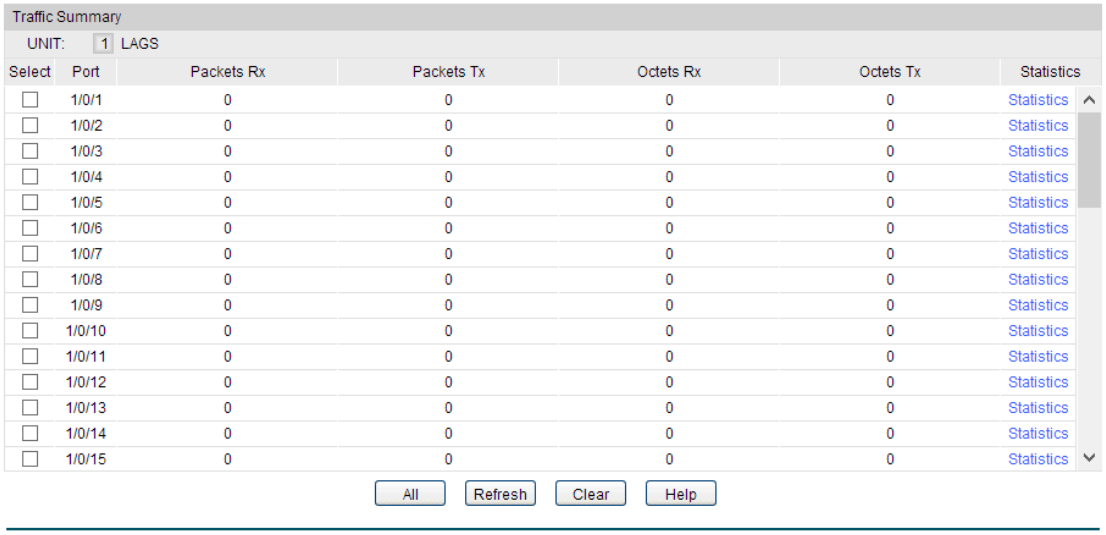


Figure 6-12 Traffic Summary

Configuration Procedure:

1) To get the real-time traffic summary, enable auto refresh in the **Auto Refresh** section, or click **Refresh** at the bottom of the page.

2) In the **Traffic Summary** section, click **1** to show the information of the physical ports, and click **LAGS** to show the information of the LAGs.

Entry Description:

➢ **Auto Refresh**

Auto Refresh: With this potion enabled, the switch refreshes the web timely.

Refresh Rate: Specify the refresh interval in seconds.

➢ **Traffic Summary**

Port: Displays the port number.

Packets Rx: Displays the number of packets received on the port. 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. 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.

6.3.2 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.

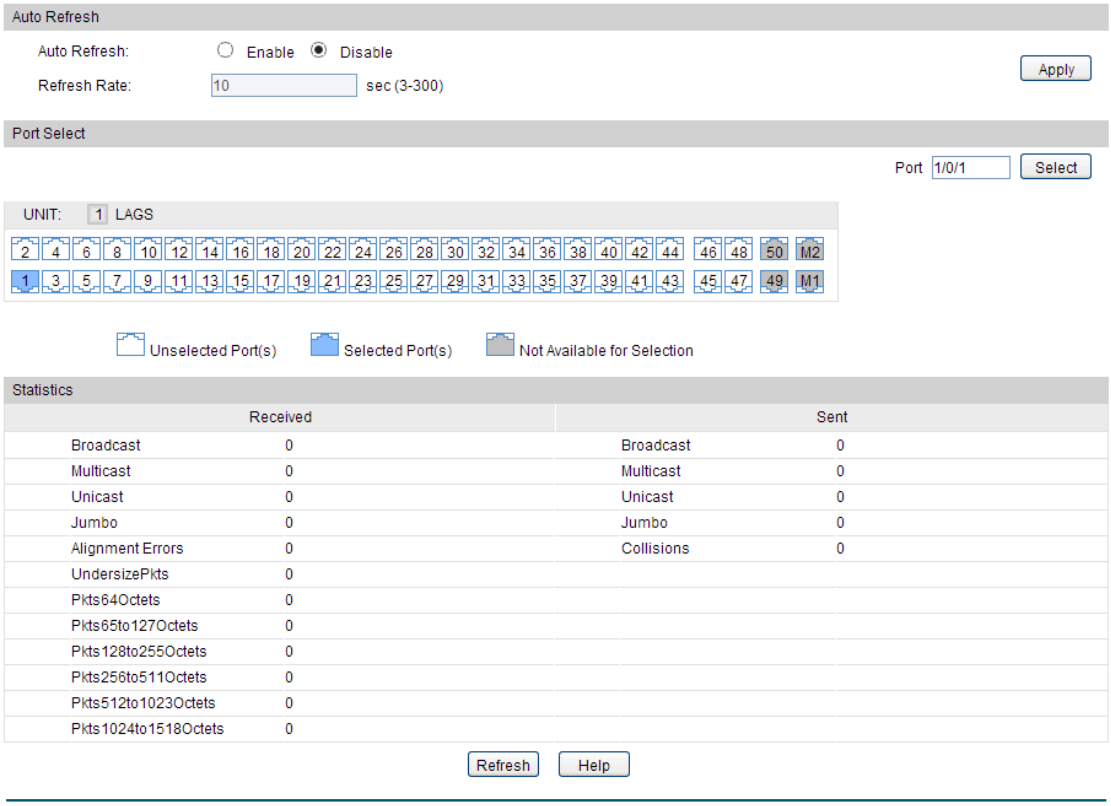


Figure 6-13 Traffic Statistics

Configuration Procedure:

1) To get the real-time traffic summary, enable auto refresh in the **Auto Refresh** section, or click **Refresh** at the bottom of the page.

2) In the **Traffic Summary** section, click **1** to show the information of the physical ports, and click **LAGS** to show the information of the LAGs.

Entry Description:

- **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.

- **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 sent on the port. Error frames are not counted in.
Multicast:	Displays the number of good multicast packets received or sent on the port. Error frames are not counted in.
Unicast:	Displays the number of good unicast packets received or sent on the port. Error frames are not counted in.
Jumbo	Displays the number of jumbo frames received or sent on the port.
Alignment Errors:	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.
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 more than 1023 bytes long.

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

6.4 MAC Address

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

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

Type	**Configuration Way**	**Aging out**	**Being kept after reboot** (if the configuration is saved)	**Relationship between the bound MAC address and the port**
Static 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 6-1 Types and features of Address Table

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

6.4.1 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.

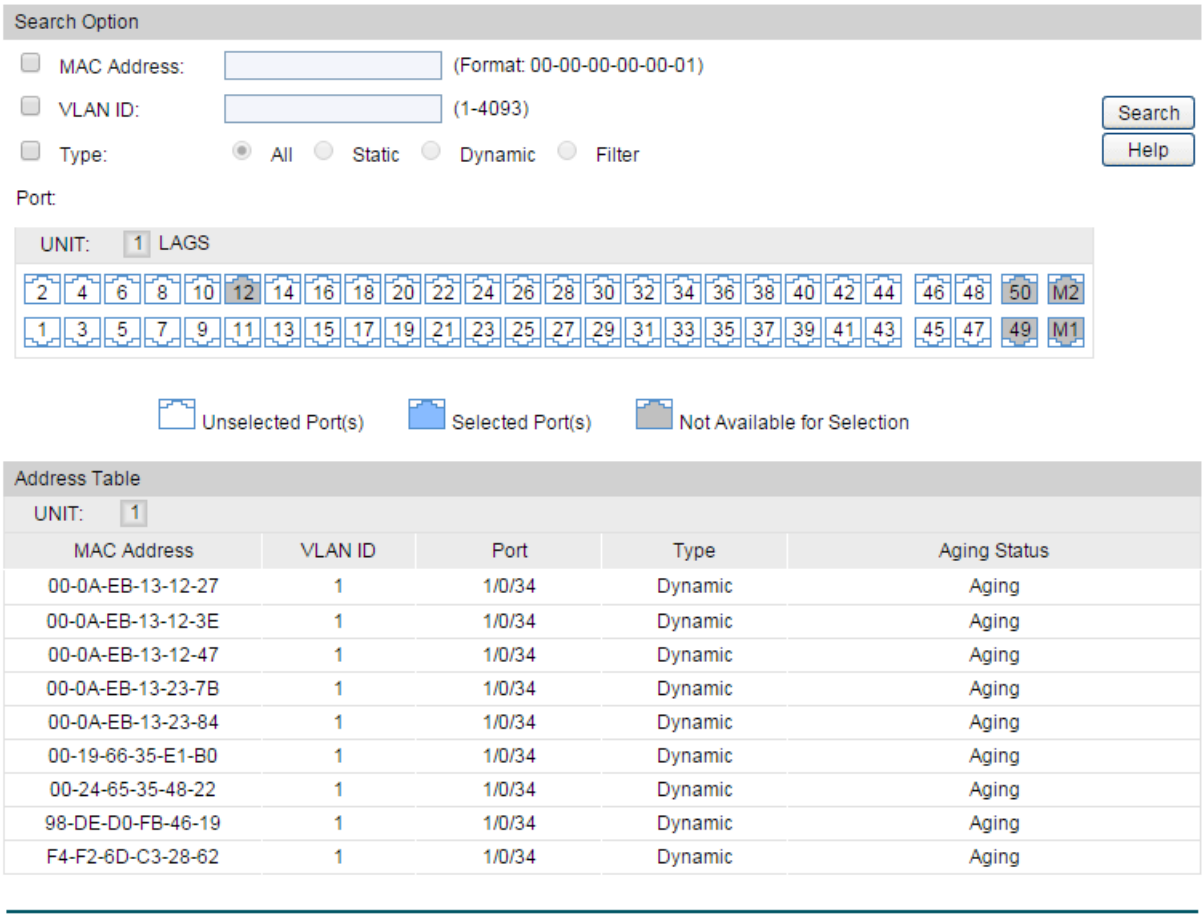


Figure 6-14 Address Table

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.

Port: Select the corresponding port number or link-aggregation number 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.
- **Filtering:** This option allows the address table to display the filtering address entries only.

UNIT: Select the unit ID of the desired member in the stack.

➢ **Address Table**

UNIT: Select the unit ID of the desired member in the stack.

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 or link-aggregation number of the MAC address.

Type: Displays the Type of the MAC address.

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

6.4.2 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.

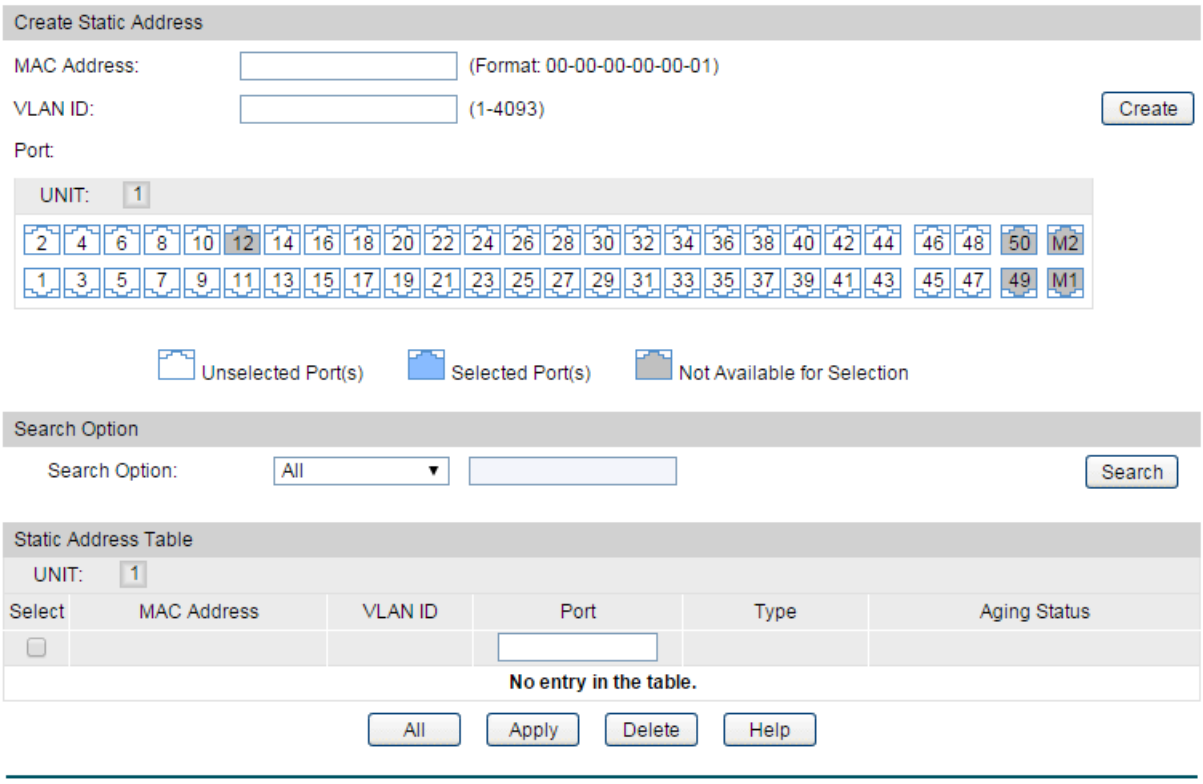


Figure 6-15 Static Address

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.

UNIT: Select the unit ID of the desired member in the stack.

Port: Select a port to be bound.

➢ **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**

UNIT: Select the unit ID of the desired member in the stack.

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.

6.4.3 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.

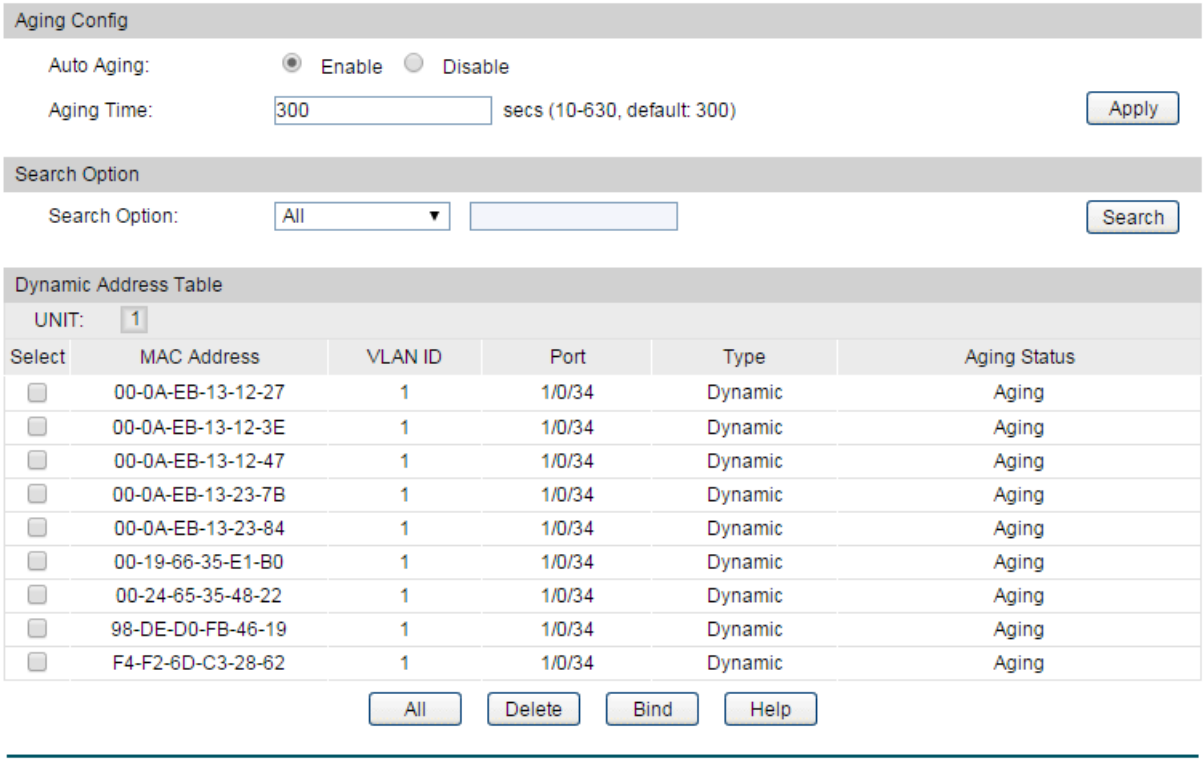


Figure 6-16 Dynamic Address

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 or link-aggregation number of your desired entry.

➢ **Dynamic Address Table**

UNIT: Select the unit ID of the desired member in the stack.

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 or link-aggregation 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.

6.4.4 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.

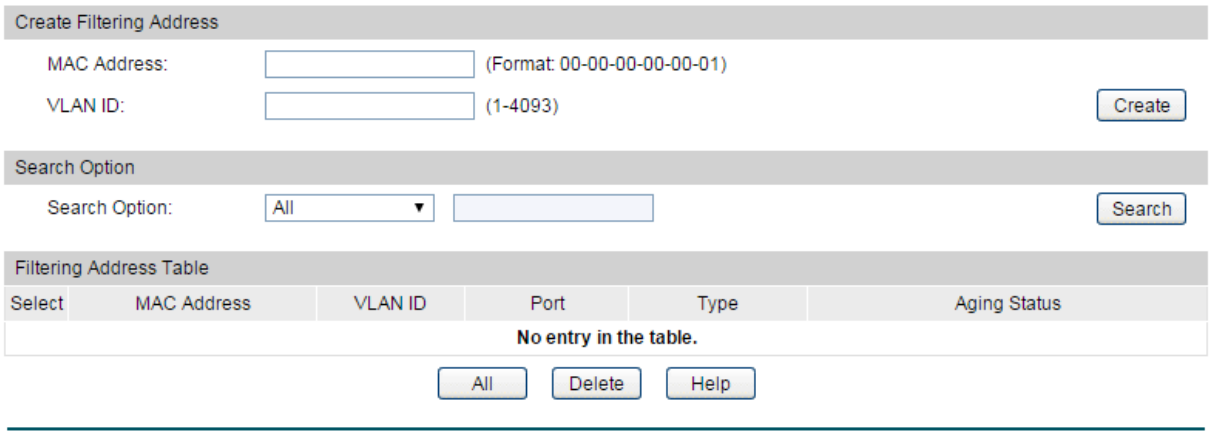


Figure 6-17 Filtering Address

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:

1. The MAC address in the Filtering Address Table cannot be added to the Static Address Table or bound to a port dynamically.
2. This MAC address filtering function is not available if the 802.1X feature is enabled.

Return to CONTENTS

Chapter 7 VLAN

The traditional Ethernet is a data network communication technology basing 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 Layer3 switch, etc. The following figure illustrates a VLAN implementation.

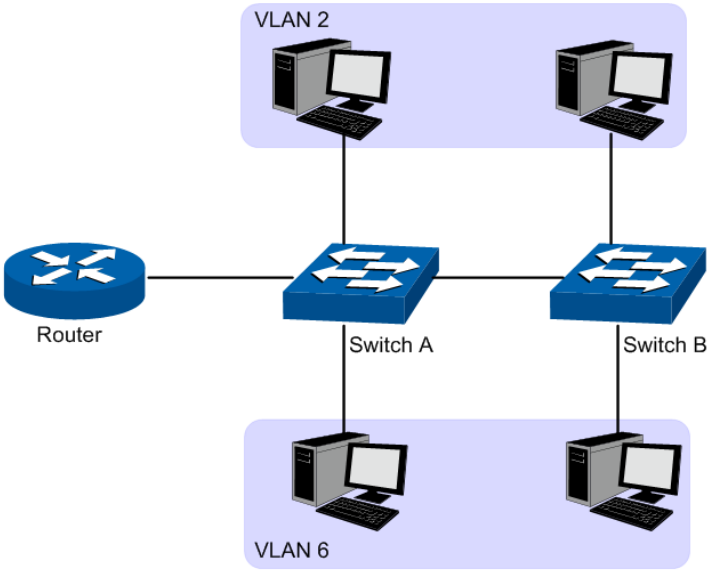


Figure 7-1 VLAN implementation

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 need not 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 segment. This switch supports three ways, namely, 802.1Q VLAN, MAC VLAN and Protocol VLAN, to classify VLANs. VLAN tags in the packets are necessary for the switch to identify packets of different VLANs. The switch can analyze the received untagged packets on the port and match the packets with the MAC VLAN, Protocol VLAN and 802.1Q VLAN in turn. If a packet is matched, the switch will add a corresponding VLAN tag to it and forward it in the corresponding VLAN.

7.1 802.1Q 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.

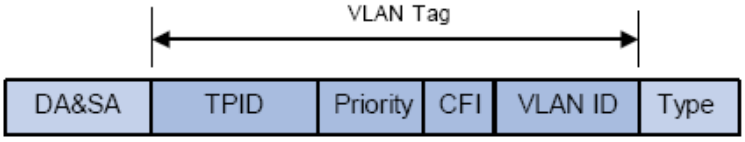


Figure 7-2 Format of VLAN Tag

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

(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 an 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 three types:

(1) **ACCESS:** The ACCESS port can be added in a single VLAN, and the egress rule of the port is UNTAG. The PVID is same as the current VLAN ID. If the ACCESS port is added to another VLAN, it will be removed from the current VLAN automatically.

(2) **TRUNK:** The TRUNK port can be added in multiple VLANs. The egress rule of the port is UNTAG if the arriving packet's VLAN tag is the same as the port's PVID, otherwise the egress rule is TAG. The TRUNK port is generally used to connect the cascaded network devices for it can receive and forward the packets of multiple VLANs.

(3) **GENERAL:** The GENERAL port can be added in multiple VLANs and set various egress rules according to the different VLANs. The default egress rule is UNTAG. The PVID can be set as the VID number of any valid VLAN.

➢ **PVID**

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 rowspan="2">Forwarding Packets</th></tr>
<tr><th>Untagged Packets</th><th>Tagged Packets</th></tr>
<tr><td>Access</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>If the VID of packet is the same as the PVID of the port, the packet will be received.
If the VID of packet is not the same as the PVID of the port, the packet will be dropped.</td><td>The packet will be forwarded after removing its VLAN tag.</td></tr>
<tr><td>Trunk</td><td>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,</td><td>If the arriving packet's VLAN tag is the same as the port's PVID, the packet will be forwarded after removing its VLAN tag, otherwise the packet will be forwarded with its current VLAN</td></tr>
</table>

		the packet will be dropped.	tag.
General			If the egress rule of port is TAG, the packet will be forwarded with its current VLAN tag. If the egress rule of port is UNTAG, the packet will be forwarded after removing its VLAN tag.

Table 7-1 Relationship between Port Types and VLAN Packets Processing

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

7.1.1 VLAN Config

On this page, you can view the current created 802.1Q VLAN.

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

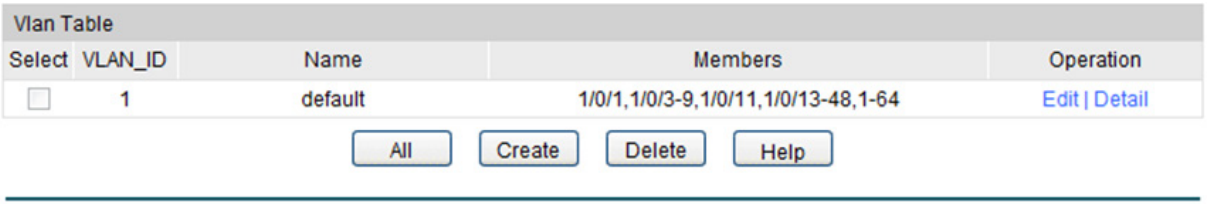


Figure 7-3 VLAN Table

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

The following entries are displayed on this screen:

➢ **VLAN Table**

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

VLAN ID: Displays the ID number of VLAN.

Name: Displays the user-defined name of 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** button to modify the settings of the corresponding VLAN. Click **Create** button to create a new VLAN.

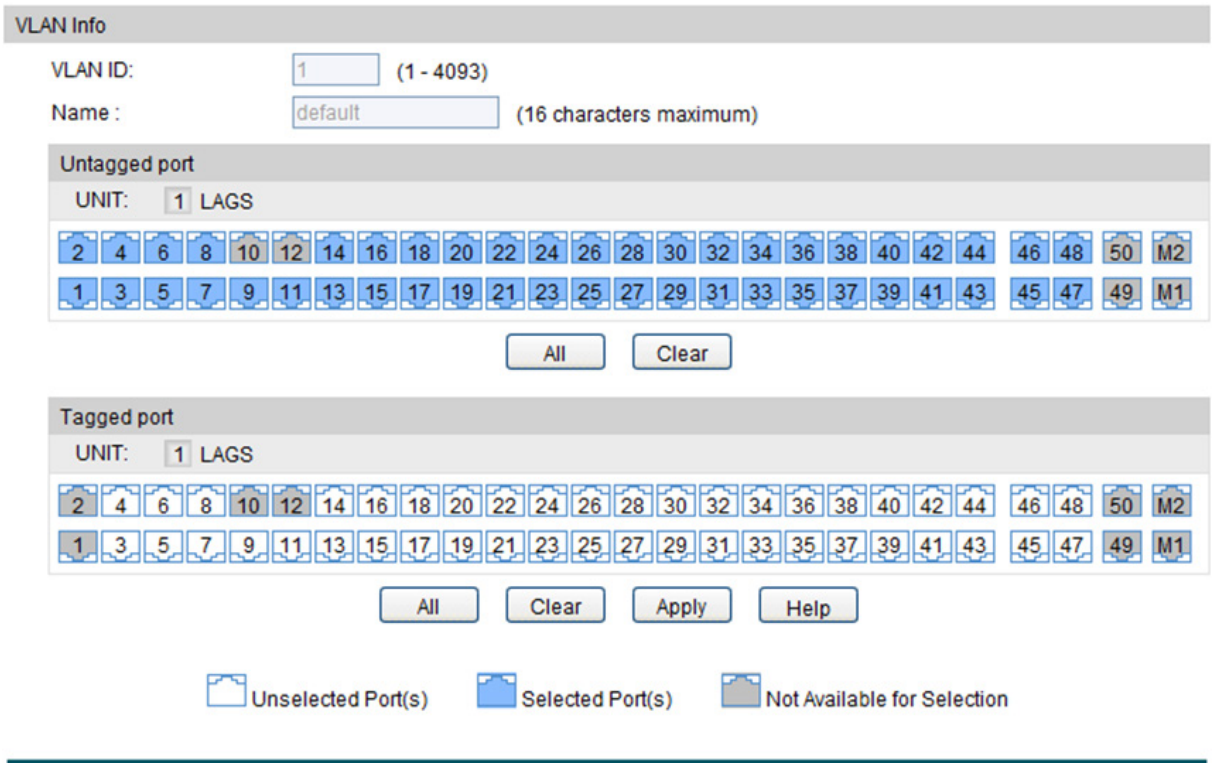


Figure 7-4 Create or Modify 802.1Q VLAN

The following entries are displayed on this screen:

➢ **VLAN Info**

VLAN ID:	Enter the ID number of VLAN.
Name:	Displays the user-defined name of VLAN.
Untagged port:	Displays the untagged port which is ACCESS, TRUNK or GENERAL.
UNIT:	Select the unit ID of the desired member in the stack.
Tagged port:	Displays the tagged port which is TRUNK or GENERAL.

7.1.2 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.

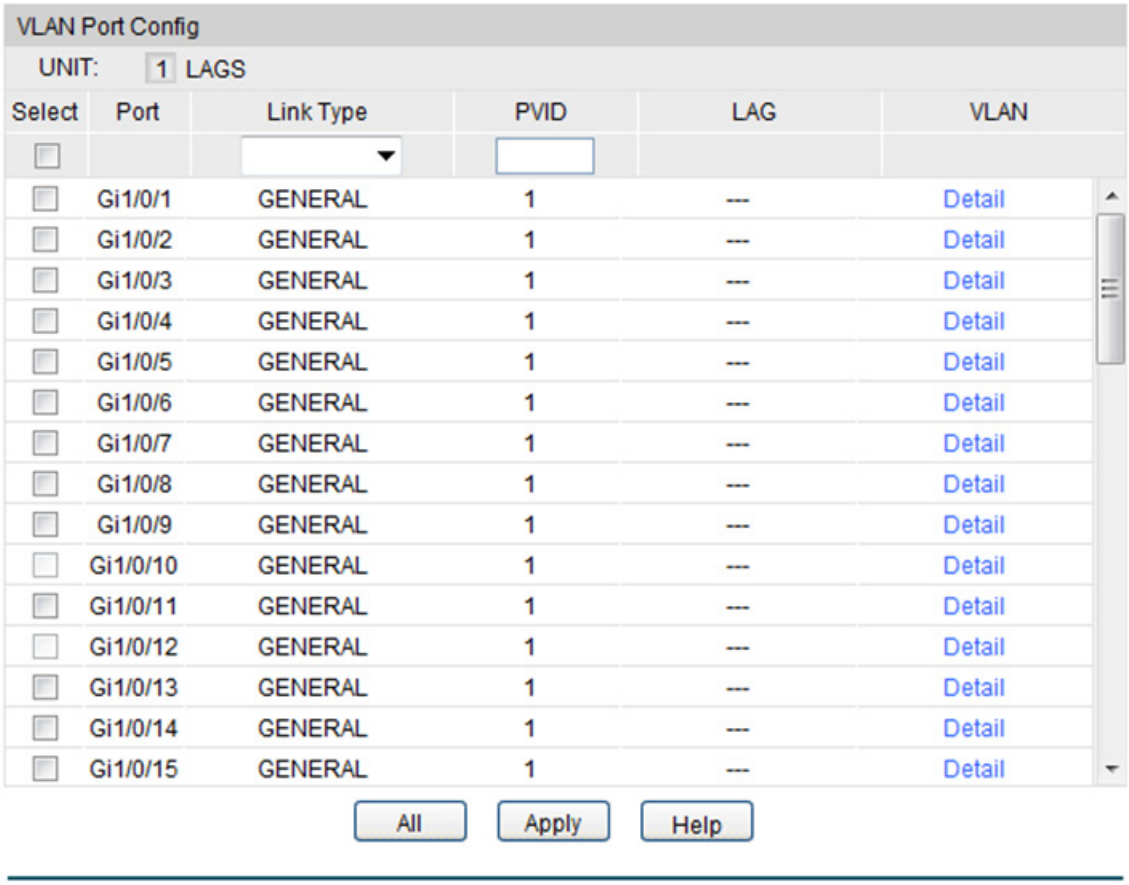


Figure 7-5 802.1Q VLAN – Port Config

The following entries are displayed on this screen:

➢ **VLAN Port Config**

UNIT: Select the unit ID of the desired member in the stack.

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

Port: Displays the port number.

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

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

PVID: Enter the PVID number of the port.

LAG: Displays the LAG to which the port belongs.

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

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

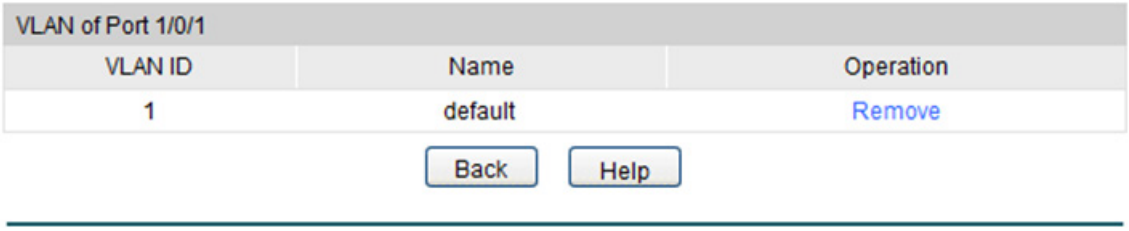


Figure 7-6 View the Current VLAN of Port

The following entries are displayed on this screen:

➢ **VLAN of Port**

VLAN ID: Displays the ID number of VLAN.

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.

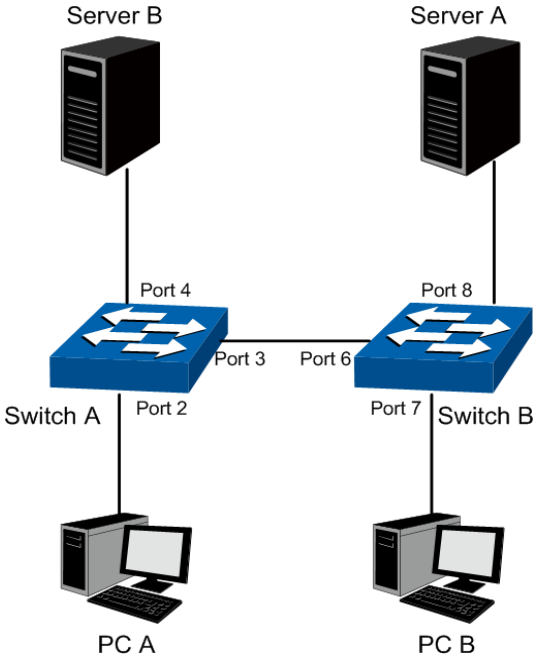
7.2 Application Example for 802.1Q VLAN

➢ **Network Requirements**

- Switch A is connecting to PC A and Server B;
- Switch B is connecting to PC B and Server A;
- PC A and Server A is in the same VLAN;

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

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

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

- Configure switch B

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

7.3 MAC VLAN

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

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

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

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

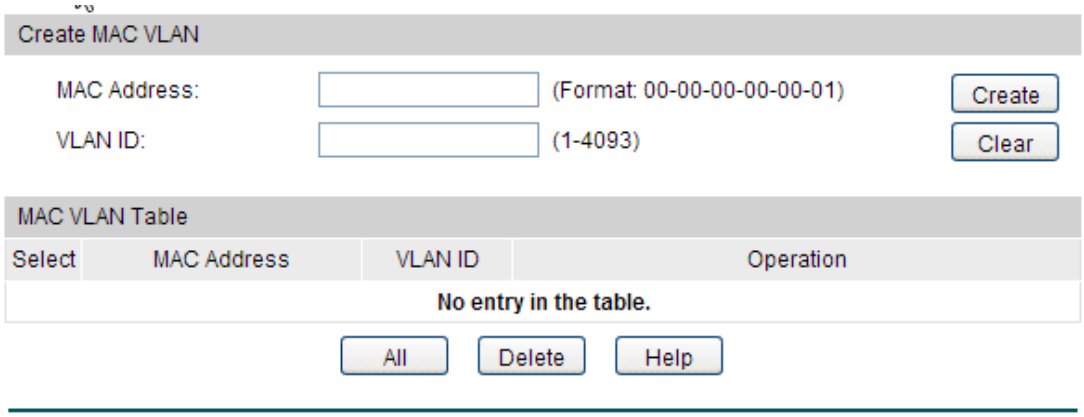


Figure 7-7 Create and View MAC VLAN

Configuration Procedure:

Specify a MAC address and a VLAN ID. Then click **Create** to make the settings effective.

Entry Description:

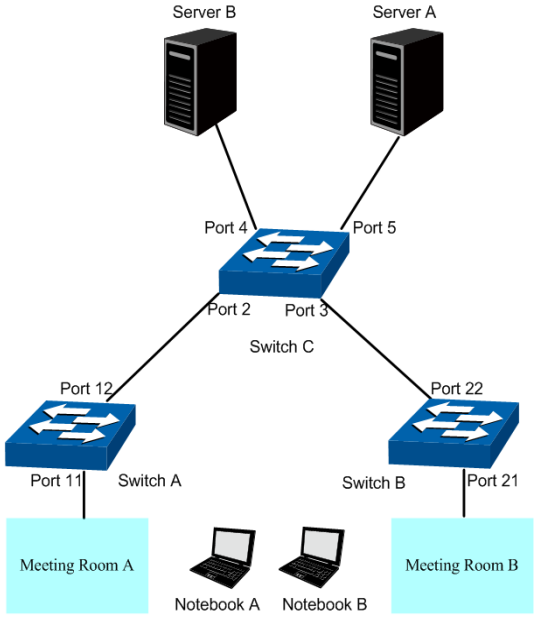
MAC Address:	Enter the MAC address.
VLAN ID:	Enter the ID number of the MAC VLAN. This VLAN should be one of the 802.1Q VLANs the ingress port belongs to.

7.4 Application Example for MAC VLAN

➢ **Network Requirements**

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

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

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

Step	Operation	Description
4	Configure MAC VLAN 10	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN10 with the MAC address as 00-19-56-8A-4C-71.
5	Configure MAC VLAN 20	On **VLAN→MAC VLAN→MAC VLAN** page, create MAC VLAN10 with the MAC address as 00-19-56-82-3B-70.

- Configure switch B

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

- Configure switch C

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

7.5 Protocol VLAN

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

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

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

Table 7-2 Protocol types in common use

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

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

7.5.1 Protocol Group Table

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

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

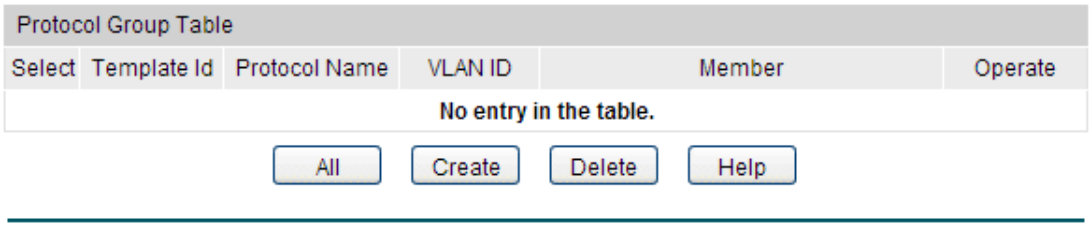


Figure 7-9 Protocol Group Table

Entry Description:

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

Template Id Displays the template ID of the protocol group.

Protocol Name: Displays the protocol of the protocol group.

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

Member: Displays the member of the protocol group.

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

7.5.2 Protocol Group

On this page, you can configure the Protocol Group.

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

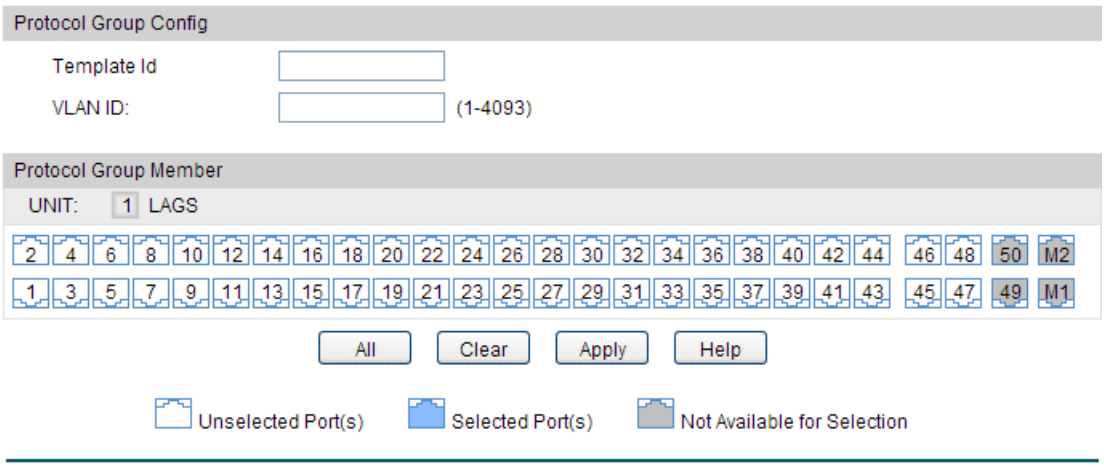


Figure 7-10 Configure Protocol Group

Configuration Procedure:

1) Specify a Template ID and a VLAN ID.
2) Add your desired ports into this protocol group.
3) Click **Apply** to make the settings effective.

Entry Description:

Template Id: Specify a template ID for this group.

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

7.5.3 Protocol Template

The Protocol Template should be created before configuring the Protocol VLAN. You can add your desired Protocol Template on this page.

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

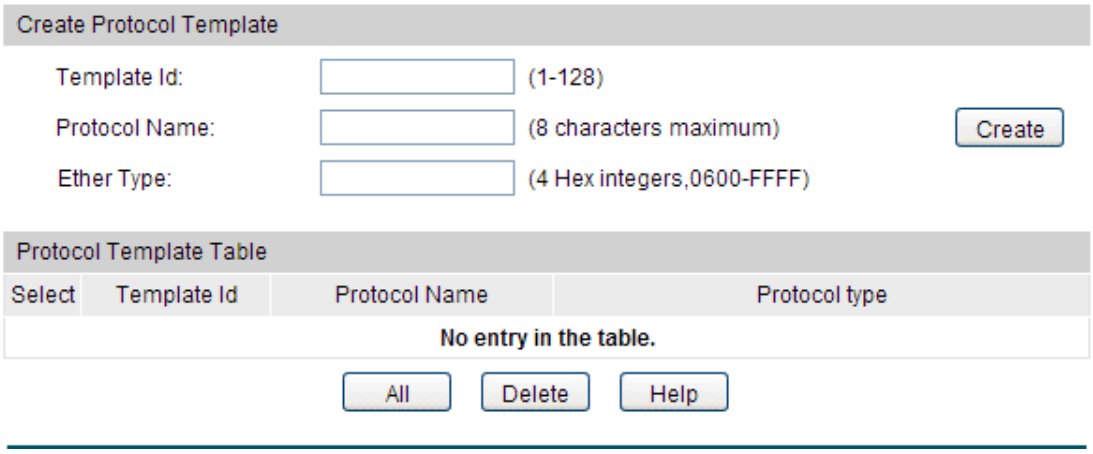


Figure 7-11 Create and View Protocol Template

Configuration Procedure:

1) Specify a template ID and a name for the protocol template.
2) Enter the ethernet type filed of your desired protocol.
3) Click **Create** to make the settings effective.

Entry Description:

Template Id	Give a template ID for the protocol template.
Protocol Name:	Give a name for the protocol template.
Ether Type:	Enter the Ethernet protocol type field in the protocol template.

Note:

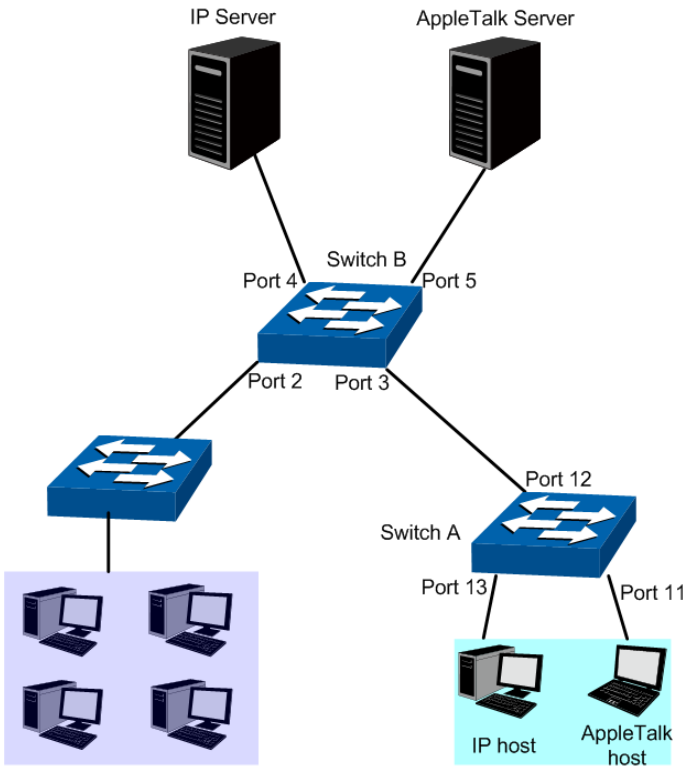
The Protocol Template bound to VLAN cannot be deleted.

7.6 Application Example for Protocol VLAN

➢ **Network Requirements**

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

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure switch A

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

- Configure switch B

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

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

7.7 VLAN VPN

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

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

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

（2） Saves public network VLAN ID resource.

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

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

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

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

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

Table 7-3 Values of Ethernet frame protocol type in common use

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

7.7.1 VLAN-VPN Config

On this page, you can configure the VLAN-VPN feature.

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

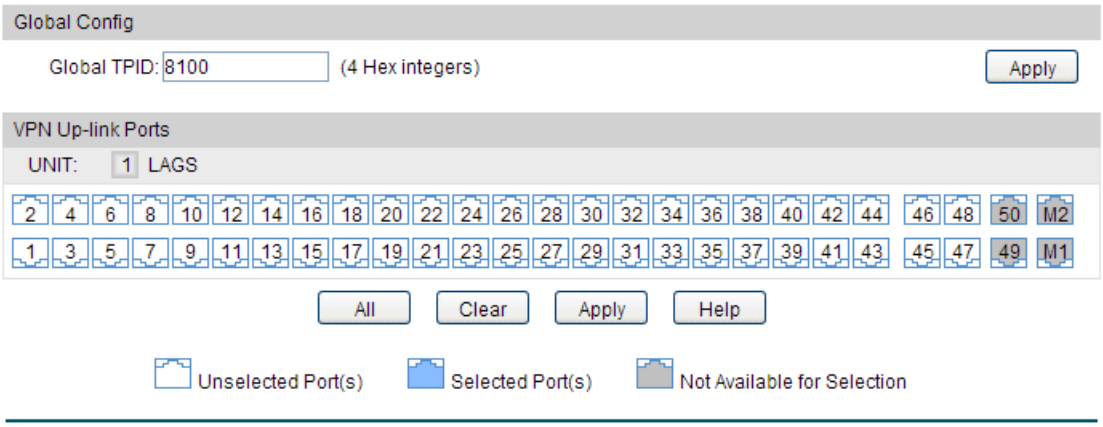


Figure 7-12 VPN Global Config

Configuration Procedure:

1) In the **Global Config** section, configure the global TPID according to your need.
2) **In the VPN Up-Link Ports** section, select your desired ports as the VPN up-link ports.
3) Click **Apply** to make the settings effectivce.

Entry Description:

Global TPID: Enter the global TPID (Tag Protocol Identifier). The default setting is 8100.

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

7.7.2 Default Settings

Feature	Default Settings
Global TPID	8100

7.8 GVRP

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

➢ **GARP**

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

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

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

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

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

- **Hold Timer:** When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer, puts all registration information it receives before the timer times out into one Join message and sends out the message after the timer times out.

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

➢ **GVRP**

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

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

7.8.1 GVRP Config

On this page, you can configure the GVRP feature.

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

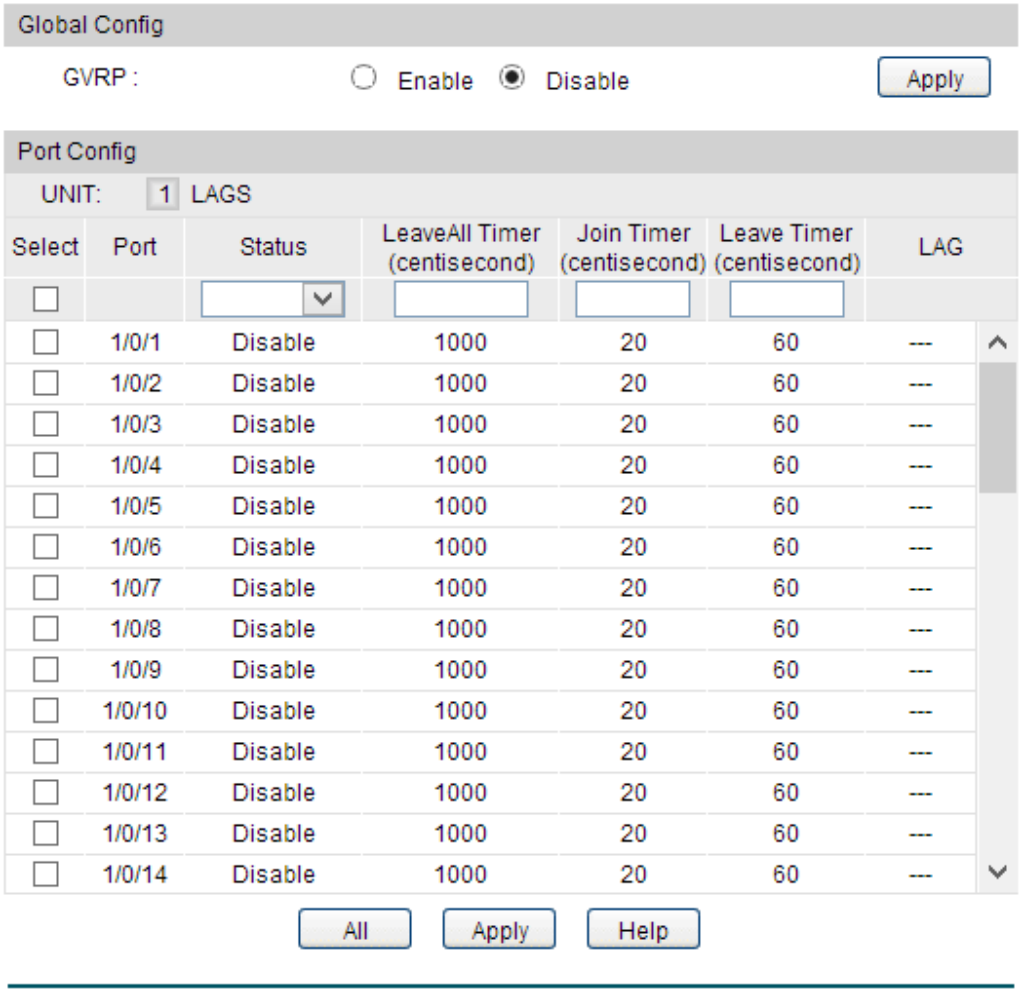


Figure 7-16 GVRP Config

Configuration Procedure:

Specify a MAC address and a VLAN ID. Then click **Create** to make the settings effective.

1) Globally enable the GVRP feautre.
2) Configure the parameters for ports.
3) Click **Apply** to make the settings effective.

Entry Description:

- **Global Config**

  GVRP: Enable the GVRP function. By default, it is disabled.

- **Port Config**

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

  Port: Displays the port number.

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

LeaveAll Timer: Once the LeaveAll Timer is set, the port with GVRP enabled can send a LeaveAll message after the timer times out, so that other GARP ports can re-register all the attribute information. After that, the LeaveAll timer will start to begin a new cycle. The LeaveAll Timer ranges from 200 to 6000 centiseconds.

Join Timer: To guarantee the transmission of the Join messages, a GARP port sends each Join message two times. The Join Timer is used to define the interval between the two sending operations of each Join message. The Join Timer ranges from 10 to 100 centiseconds.

Leave Timer: Once the Leave Timer is set, the GARP port receiving a Leave message will start its Leave timer, and deregister the attribute information if it does not receive a Join message again before the timer times out. The Leave Timer ranges from 20 to 600 centiseconds.

LAG: Displays the LAG to which the port belongs.

Note:

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

7.8.2 Default Settings

Feature	Default Settings
Global	GVRP: Disable
Port Conifg	Status: Disable LeaveAll Timer (centisecond): 1000 Join Timer (centisecond): 20 Leave Timer (centisecond): 60

7.9 Private VLAN

Private VLANs, designed to save VLAN resources of uplink devices and decrease broadcast, are sets of VLAN pairs that share a common primary identifier. To guarantee user information security, the ease with which to manage and account traffic for service providers, in campus network, service providers usually require that each individual user is Layer-2 separated. VLAN feature can solve this problem. However, as stipulated by IEEE 802.1Q protocol, a device can only support up to 4094 VLANs. If a service provider assigns one VLAN per user, the VLANs will be far from enough; as a result, the number of users this service provider can support is limited.

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

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

- **The Elements of a Private VLAN**

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

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

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

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

- Isolated VLAN—Members in an isolated VLAN are isolated with each other. Each isolated VLAN must bind to a primary VLAN.
- Community VLAN—Members in a community VLAN can communicate with each other directly. Each community VLAN must bind to a primary VLAN.

- **Features of Private VLAN**

1. A Private VLAN contains one Primary VLAN and one Secondary VLAN.
2. A VLAN cannot be set as the Primary VLAN and Secondary VLAN simultaneously.
3. A Secondary VLAN can only join one private VLAN.
4. A Primary VLAN can be associated with multi-Secondary VLANs to create multi-Private VLANs.

➢ **Private VLAN Implementation**

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

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

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

7.9.1 PVLAN Config

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

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

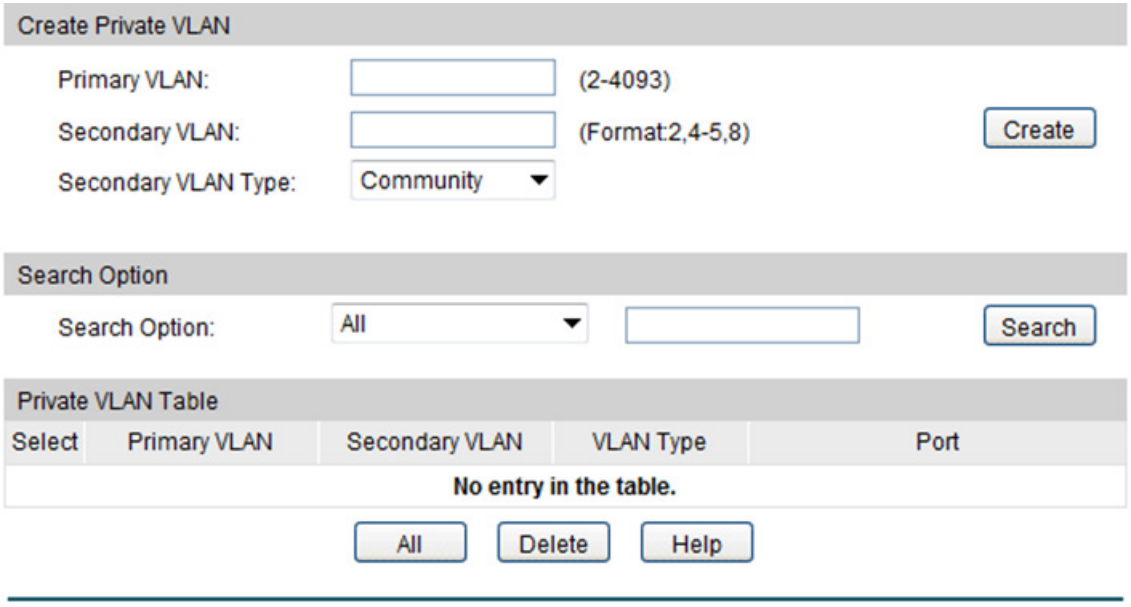


Figure 7-17 Create Private VLAN

The following entries are displayed on this screen:

➢ **Create Private VLAN**

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

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

➢ **Search Option**

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

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

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

➢ **Private VLAN Table**

Select:	Select the entry to delete. It is multi-optional.
Primary VLAN:	Displays the Primary VLAN ID number of the Private VLAN.
Secondary VLAN:	Displays the Secondary VLAN ID number of the Private VLAN.
Port:	Displays the Port number of the Private VLAN.

7.9.2 Port Config

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

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

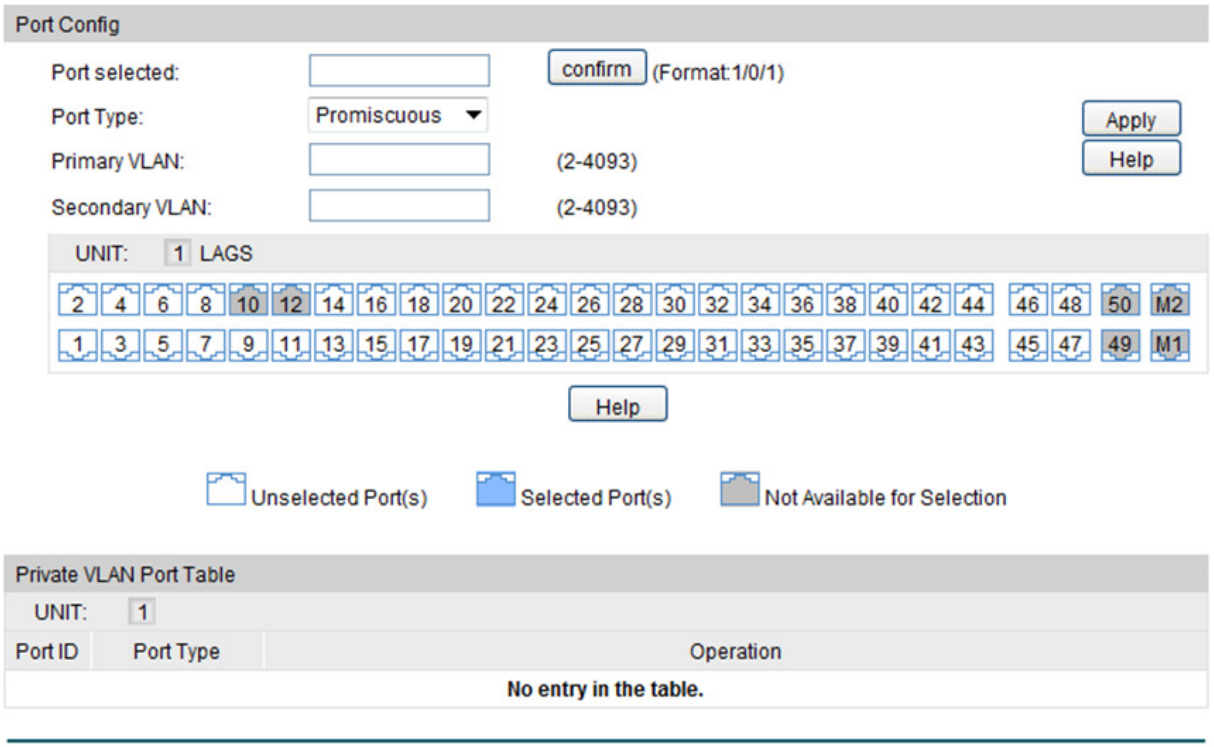


Figure 7-18 Create and View Protocol Template

The following entries are displayed on this screen:

➢ **Port Config**

Port selected:	Select the desired port for configuration. You can input one or select from the port table down the blank.
Port Type:	Select the Port Type from the pull-down list for the port.

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

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

UNIT: Select the unit ID of the desired member in the stack.

➢ **Private VLAN Port Table**

UNIT: Select the unit ID of the desired member in the stack.

Port ID: Displays the port number.

Port Type: Displays the corresponding Port Type.

Note:

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

Configuration Procedure:

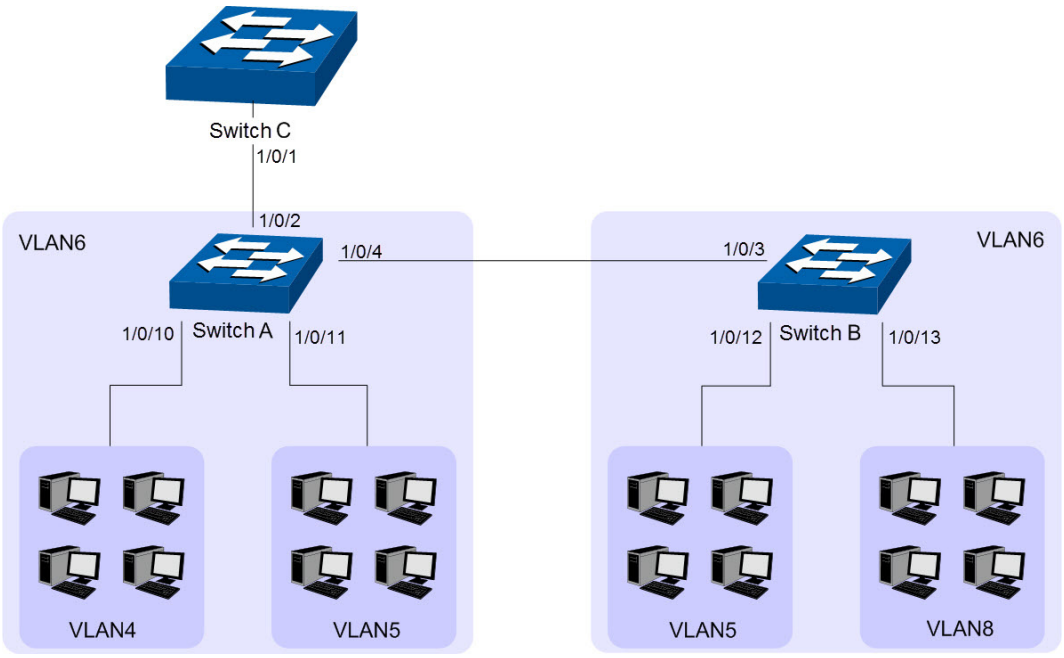
Step	Operation	Description
1	Create Private VLAN.	Required. On the **VLAN→Private VLAN→PVLAN Config** page, enter the Primary VLAN and Secondary VLAN, select one type of secondary VLAN and then click the **Create** button.
2	Add ports to Private VLAN	Required. On the **VLAN→Private VLAN→Port Config**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

7.10 Application Example for Private VLAN

➢ **Network Requirements**

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

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch C

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

- Configure switch A

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

- Configure switch B

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

Return to CONTENTS

Chapter 8 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): The value of the priority and MAC address of the switch. It is used to select the root bridge. The bridge ID is composed of a 2-byte priority and a 6-byte MAC address. The priority is allowed to be configured manually on the switch, and the switch with the lowest priority value will be elected as the root bridge. If the priority of all the switches are the same, the switch with the lowest MAC address is selected as the root bridge.

Root Bridge: The root of a spanning tree. There is only one root bridge in each spanning tree, and the root bridge has the lowest bridge ID. Configure the switch with the best performance 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 LAN segment. BPDUs are forwarded to the network segment through the designated bridge.

Path Cost: The path cost reflects the link speed of the port. The smaller the value, the higher link speed the port has.

The path cost can be manually configured on each port. If not, the path cost value is automatically calculated according to the link speed as shown below:

Link Speed	Path Cost Value
10Mb/s	2,000,000
100Mb/s	200,000
1Gb/s	2,0000
10Gb/s	2000

Table 8-1 Default path cost value

Root Path Cost: The root path cost is the accumulated path costs from the root bridge to the other switches. When the root bridge sends its BPDU, the root path cost value is 0. When a connected switch receives this BPDU, it increments the path cost of its local incoming port. Then it forwards this BPDU to the downstream switch, with the updated root path cost. The value of the accumulated root path cost increases as the BPDU propagates further.

Root Port: The port selected on non-root bridges to provide the lowest root path cost. There is only one root port in each non-root bridge.

Designated Port: The port selected for each LAN segment to provide the lowest root path cost from that LAN segment to the root bridge.

Port Priority: The port priority can be set to an integral multiple of 16 in the range of 0~240. The lower value priority has the higher priority. The port with the higher priority has more chance to be chosen as the root port.

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 the 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 and 2 are the designated ports of switch A and port 4 is the designated port of switch B; port 6 is the blocked port of switch C.

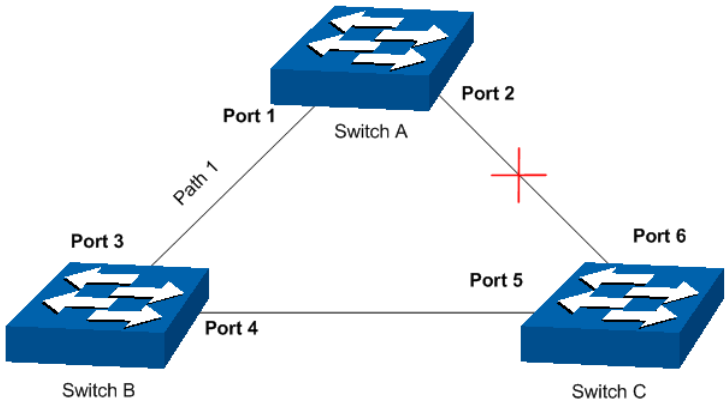


Figure 8-1 Basic STP diagram

➢ **STP Timers**

Hello Time:

Hello Time is 2 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 of the port itself, the switch discards the BPDU and does not change the BPDU of the port itself. 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.
2	The switch compares the BPDUs of all the ports, and selects the BPDU with the highest priority as the switch's BPDU.

Table 8-2 Comparing BPDUs

- Selecting the root bridge

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

- Selecting the root port

The non-root switch will go through the following steps when selecting a root port:

1) Choose the port that provides the lowest root path cost as the root port.
2) If multiple ports provide the same root path cost, the port which is connected to the neighboring switch (the switch will go through to reach the root bridge) with the smallest bridge ID will be selected as the root port
3) If multiple ports go through the same neighboring switch, the port with the highest priority will be selected as the root port.
4) If the priorities are the same between the ports, the port with the smallest port number will be selected as the root port.

- Selecting the designated bridge and designated port

Here are the steps taken by switches in selecting the designated bridge and designated port for each LAN segment:

1) Choose the switch with the lowest root path cost from the LAN segment to the root bridge as the designated bridge. The port through which the designated bridge is attached to the LAN segment is the designated port.
2) If multiple switches have the same root path cost, the one with the smallest bridge ID will be chosen as the designated bridge. The port through which the designated bridge is attached to the LAN segment is the designated port.
3) If it happens that there are more than one port through which the designated bridge is attached to the LAN segment, the port with the highest priority will be selected as the designated port.
4) If the priorities of the ports on the same designated bridge are still the same, the port with the smallest port number will be selected as the designated port.

Tips：

In a stable STP 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 alternate port can rapidly transit to the new root port once the old root port failed.
- The backup port can rapidly transit to the new designated port once the old designated port failed.
- 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-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 consists of multiple interconnected switches. These switches have the same region name, the same revision level and the same VLAN-Instance mapping table.

MSTI (Multiple Spanning Tree Instance): The MST instance is a spanning tree running in the MST region. Multiple MST instances can be established in one MST region and they are independent of each other. Each spanning tree is referred to as a multiple spanning tree instance.

VLAN-Instance Mapping: VLAN-Instance Mapping describes the mapping relationship between VLANs and instances. Multiple VLANs can be mapped to a same instance, but one VLAN can be mapped to only one instance.

IST (Internal Spanning Tree)**:** A special MST instance with an instance ID of 0. By default, all the VLANs are mapped to IST.

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.

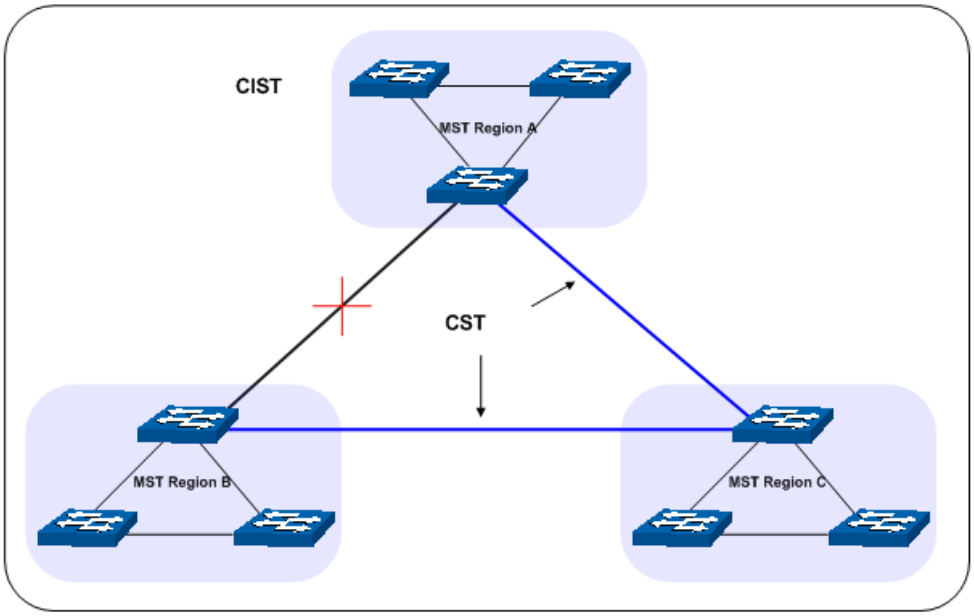


Figure 8-2 Basic MSTP diagram

➢ **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 trees 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: The port selected on non-root bridges to provide the lowest root path cost. There is only one root port in each non-root bridge.
- Designated Port: The port selected for each LAN segment to provide the lowest root path cost from that LAN segment to the root bridge
- 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: If a port is not selected as the designated port for it receives better BPDUs from another switch, it will become an alternate port.

  In RSTP/MSTP, the alternate port is the backup for the root port. It is blocked when the root port works normally. Once the root port fails, the alternate port will become the new root port.

  In STP, the alternate port is always blocked.
- Backup Port: If a port is not selected as the designated port for it receives better BPDUs from the switch it belongs to, it will become a backup port.

  In RSTP/MSTP, the designated port is the backup for the designated port. It is blocked when the designated port works normally. Once the root port fails, the backup port will become the new designated port.

  In STP, the backup port is always blocked.
- Disabled: Indicates the port that is not participating in the STP.

The following diagram shows the different port roles.

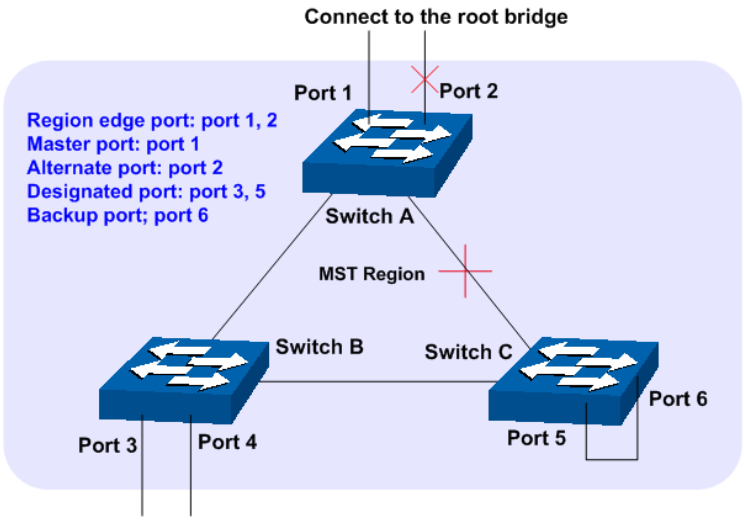


Figure 8-3 Port roles

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**.

8.1 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.

8.1.1 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. 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.

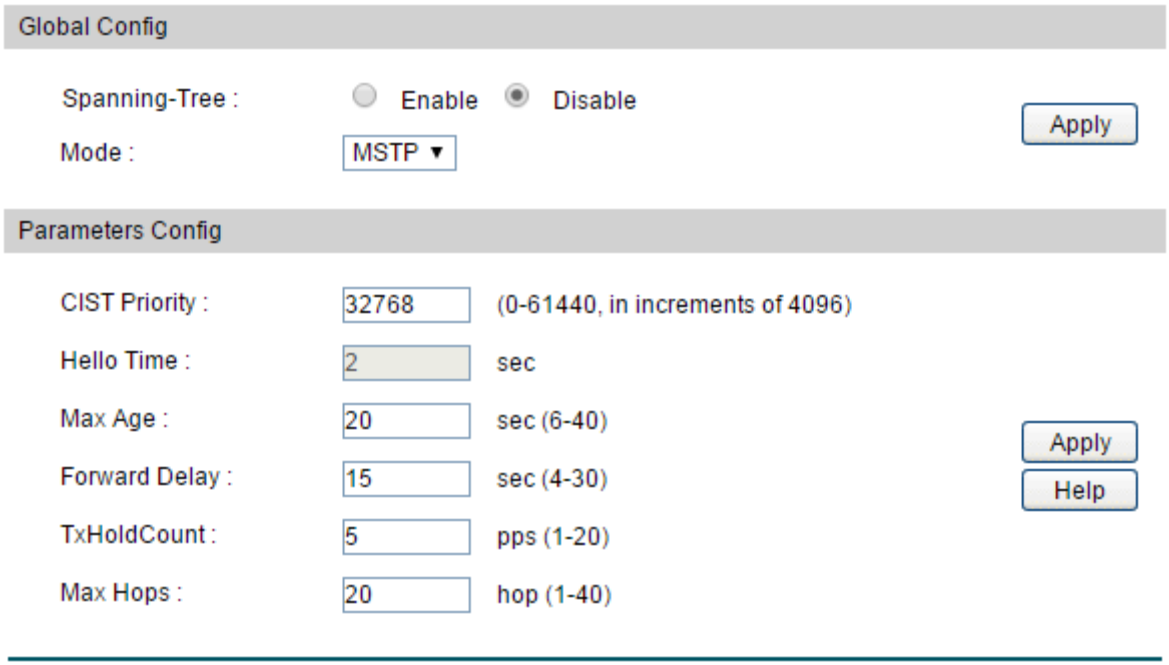


Figure 8-4 STP Config

Configuration Procedure:

1) Enable spanning tree function, select the STP mode, and click **Apply**.
2) Configure the related parameters and click **Apply**.

Entry Description:

➢ **Global Config**

Spanning Tree: Enable or disable STP function globally on the switch.

Mode: Select the desired STP mode on the switch.

- **STP:** Specify the spanning tree mode as STP (Spanning Tree Protocol).
- **RSTP:** Specify the spanning tree mode as RSTP (Rapid Spanning Tree Protocol).
- **MSTP:** Specify the spanning tree mode as MSTP (Multiple Spanning Tree Protocol).

➢ **Parameters Config**

CIST Priority: Specify the CIST priority of the switch. The valid values are from 0 to 61440, which are divisible by 4096.By default, it is 32768. The switch with the lower value has the higher priority.

CIST priority is usually a parameter configured in MSTP, which means the priority of a switch in CIST. The switch with the highest priority will be elected as the root bridge in CIST.

In STP/RSTP, CIST priority means the priority of a switch in the spanning tree. The switch with the highest priority is elected as the root bridge.

Hello Time Hello Time is 2 seconds, it's the interval to send BPDUs.

Max Age: Specify the maximum time the switch can wait without receiving a BPDU before attempting to regenerate a spanning tree. The valid values are from 6 to 40 in seconds, and the default value is 20.

Forward Delay: Specify the time for the port to transit its state after the network topology is changed. The valid values are from 4 to 30 in seconds, and the default value is 15.

TxHoldCount: Specify the maximum BPDU transmission rate of a port. The valid values are from 1 to 20, and the default value is 5.

Max Hops: Specify the maximum number of hops that occur in a specific region before the BPDU is discarded. The valid values are from 1 to 40, and the default value is 20.

Max Hops is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

Note:

1. To prevent frequent network flapping, make sure that Hello Time, Forward Delay, and Max Age conform to the formulas: 2*(Hello Time + 1) <= Max Age, 2*(Forward Delay - 1) >= Max Age.
2. 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.
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.

8.1.2 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.

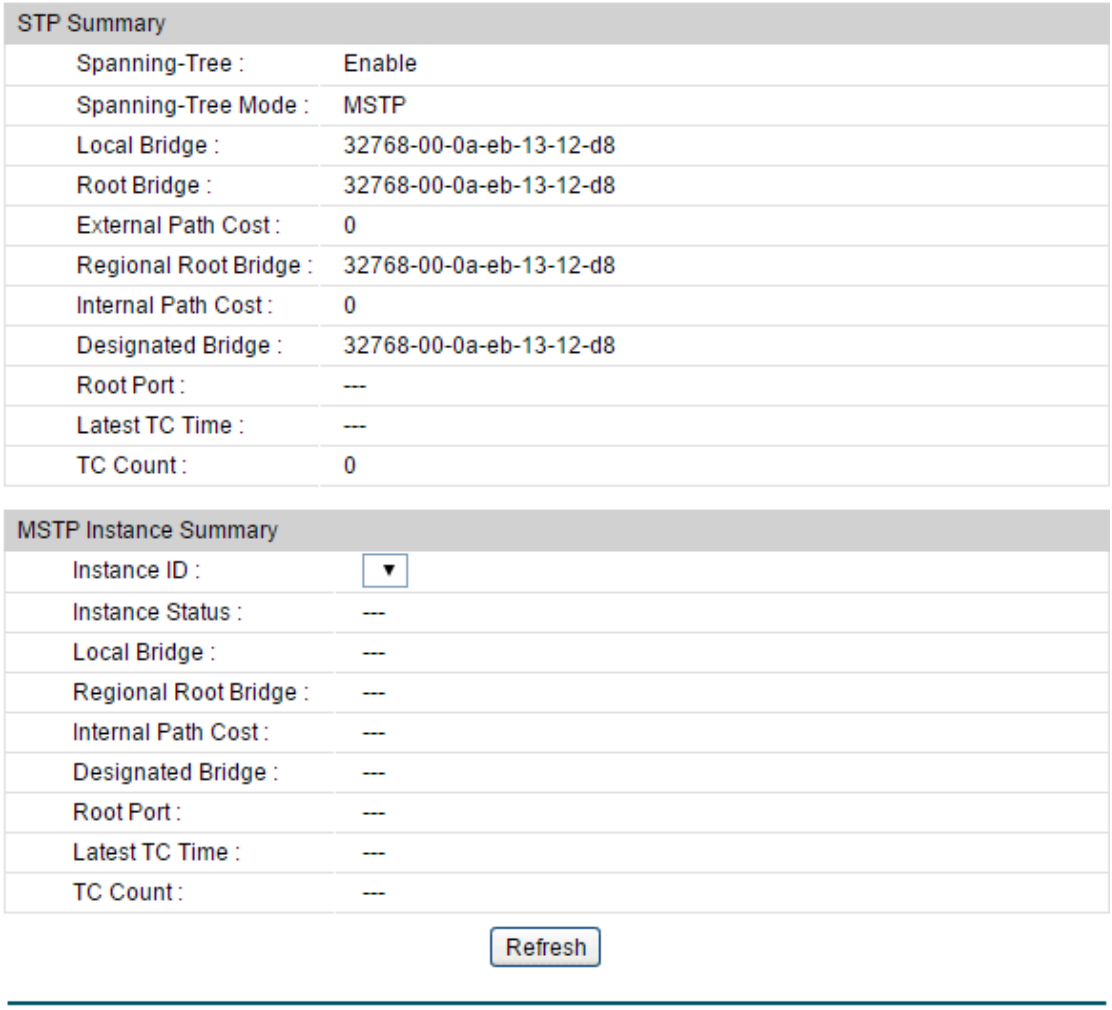


Figure 8-5 STP Summary

8.2 Port Config

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

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

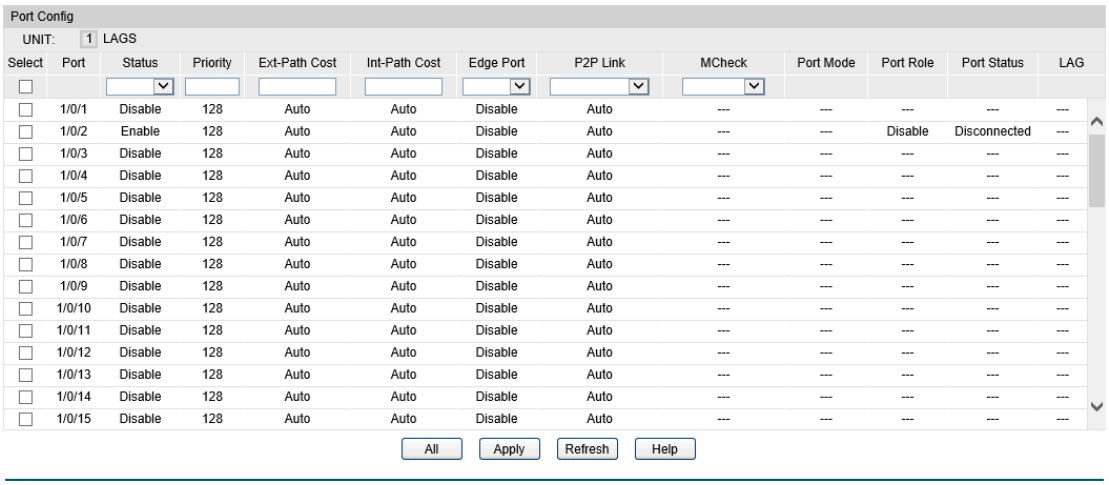


Figure 8-6 Port Config

Configuration Procedure:

Configure the parameters of the ports for CIST.

Entry Description:

➢ **Port Config**

UNIT: Select the desired unit or LAGs.

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

Port: Displays the port number of the switch.

Status: Enable or disable spanning tree function on the desired port.

Priority: Enter the value of port priority from 0 to 240 divisible by 16, and the default value is 128.

The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in CIST.

Ext-Path Cost: Enter the value of the external path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed.

In MSTP, External path cost is the path cost of the port in CST. The port with the lowest external root path cost will be elected as the root port in CIST.

In STP/RSTP, external path cost indicates the path cost of the port in the spanning tree. The port with the lowest external root path cost will be elected as the root port.

Int-Path Cost: Enter the value of the internal path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed.

Internal path cost is the path cost of the port in IST. The port with the lowest internal root path cost will be elected as the root port in IST.

Note: Internal path cost is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

Edge Port: Enable or disable Edge Port. By default, it is disabled.

The edge port can transit its state from blocking to forwarding directly. If the port is connected to an end device, like a PC, it is recommended to set the port as an edge port.

P2P Link: Select the P2P link status. If the two ports in the P2P link are a root port and a designated port, they can transit their states to forwarding directly.

Three options are supported: Auto, Open(Force) and Close(Force). By default, it is Auto.

Auto: The switch automatically detects if the port is connected to a P2P link, then determines the status is Open or Close.

Open(Force): The port is manually identified as connected to a P2P link.

Close(Force): The port is manually identified as not connected to a P2P link

MCheck: Select whether to do MCheck operation on the port. Unchange means no MCheck operation.

If a port on an MSTP-enabled device is connected to a STP/RSTP-enabled device, the port switches to the STP/RSTP compatible mode. If the STP/RSTP-enabled device is powered off or disconnected from the MSTP-enabled device, the port cannot switch back to MSTP mode. In this case, you can switch the port to MSTP mode by enabling MCheck operation.

Note: MCheck is configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

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

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

- **Root Port:** Indicates the port that has the lowest root 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:** The port receives and sends BPDUs, and forwards user data.
- **Learning:** The port receives and sends BPDUs, and drops the other packets.
- **Blocking:** The port only receives BPDUs and drops the other packets.
- **Disconnected:** The port is enabled with spanning tree function but not connected to any device.

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. 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.

8.3 MSTP Instance

MSTP combines VLANs and spanning tree together via VLAN-instance mapping table (VLAN-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-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.

8.3.1 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.

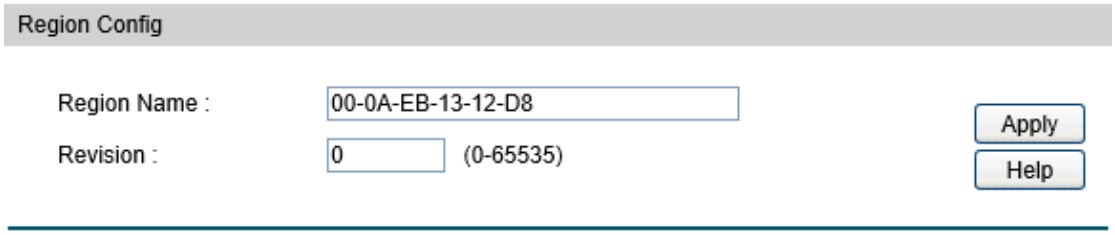


Figure 8-7 Region Config

Configuration Procedure:

Set the name and revision level to specify an MSTP region.

Entry Description:

➢ **Region Config**

Region Name: Configure the name for an MST region using up to 32 characters. By default, it is the MAC address of the switch.

Revision: Enter the revision from 0 to 65535 for MST region identification. By default, it is 0.

8.3.2 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.

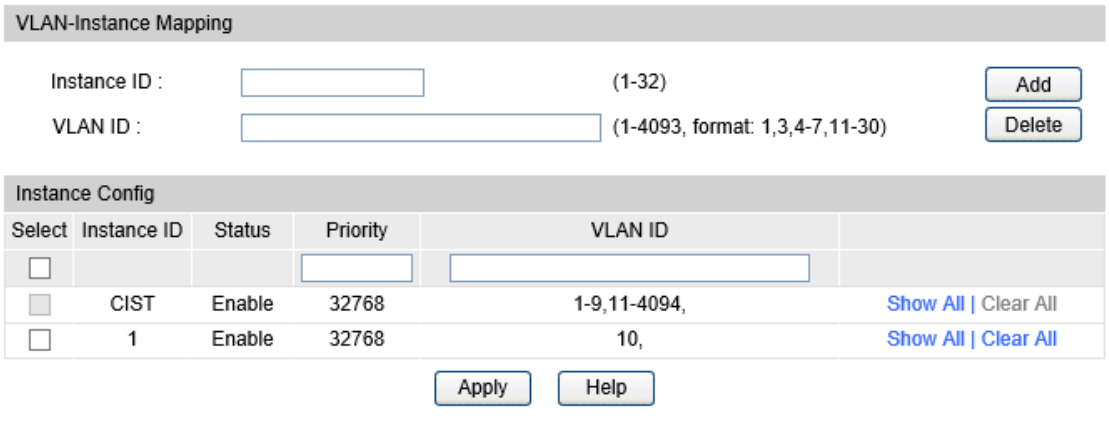


Figure 8-8 Instance Config

Configuration Procedure:

1) Enter the instance ID and the corresponding VLAN ID, and click **Add**.
2) Configure the priority of the switch in the desired instance, and click **Apply**.

Entry Description:

- **VLAN-Instance Mapping**

Instance ID:	Enter the corresponding instance ID.
VLAN ID:	Enter the desired VLAN ID. Click 'Add' button, the new VLAN ID will be added to the corresponding instance and the previous VLAN won't be replaced. Click 'Delete' button, the VLAN will be delete from the corresponding instance.

- **Instance Config**

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 a value from 0 to 61440 to specify the priority of the switch, which is divisible by 4096, and the default value is 32768. The switch with the lower value has the higher priority, and the switch with the highest priority will be elected as the root bridge in the desired instance.
VLAN ID:	Enter the VLAN ID mapped to the corresponding instance ID. After the modification, the previous VLAN will be cleared and mapped to the CIST.
Show All:	Click the **Show All** button to show all VLAN IDs mapped to the instance.
Clear All:	Click the **Clear All** button to clear up all VLAN from the instance. The cleared VLAN will be automatically mapped to the CIST.

Note:

In a network with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. If you want to announce a specific VLAN through GVRP, please be sure to map the VLAN to the CIST when configuring the MSTP VLAN-instance mapping table. For detailed introduction of GVRP, please refer to **GVRP** function page.

8.3.3 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 instances 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.

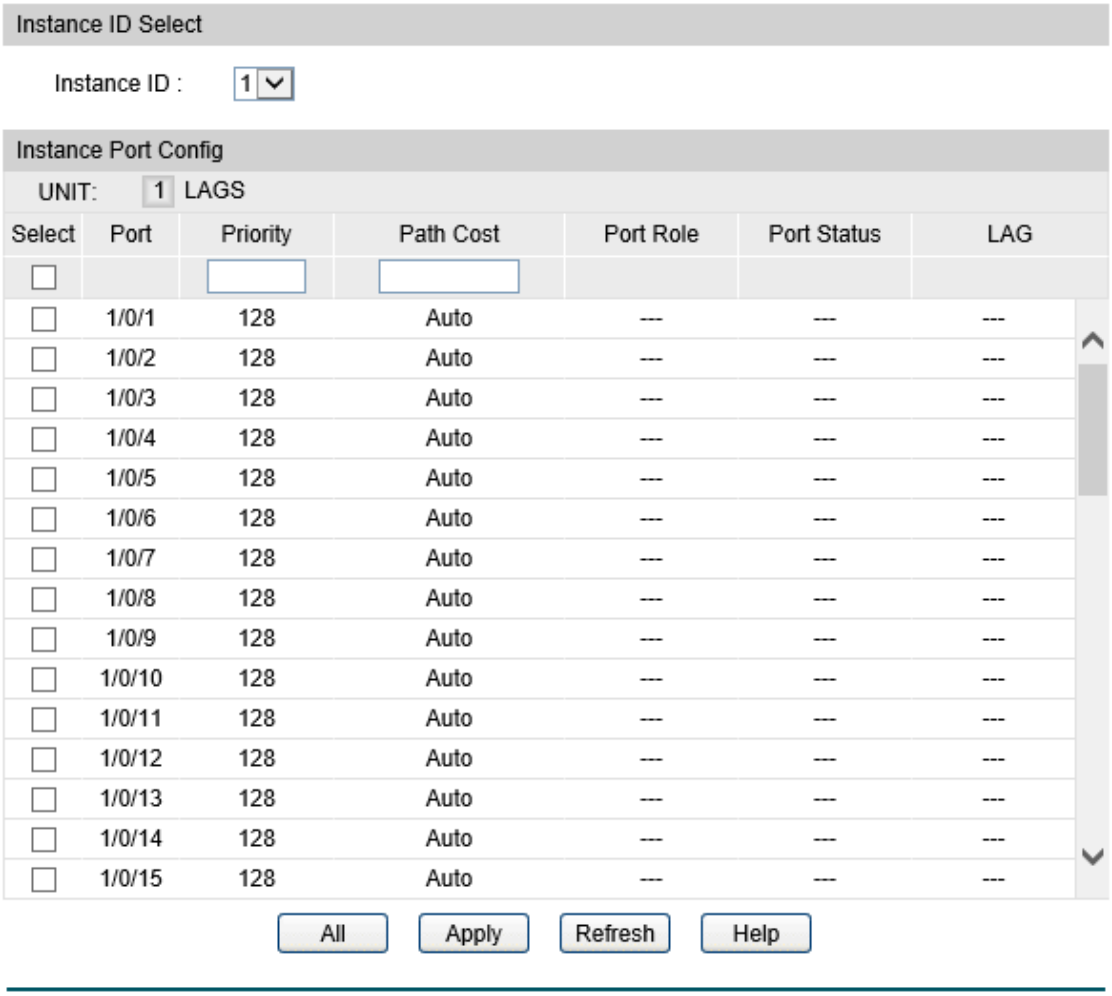


Figure 8-9 Instance Port Config

Configuration Procedure:

1) Select the desired instance ID for its port configuration.
2) Configure port parameters in the desired instance.

➢ **Instance ID Select**

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

➢ **Instance Port Config**

UNIT: Select the desired unit or LAGs.

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 value of port priority from 0 to 240, which is divisible by 16, and the default value is 128.

The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in the desired instance.

Path Cost: Enter the value of the path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed.

It is the path cost of the port in the desired instance. The port with the lowest path cost will be elected as the root of the desired instance.

Port Role: Displays the role that the port plays in the desired instance.

Root Port: Indicates the port is the root port.

Designated Port: Indicates the port is the designated port.

Alternate Port: Indicates the port is a backup of a root port.

Backup Port: Indicates the port is a backup of a designated port.

Disabled: Indicates the port is not participating in the spanning tree.

Port Status: Displays the port status.

Forwarding: The port receives and sends BPDUs, and forwards user data.

Learning: The port receives and sends BPDUs, and drops the other packets.

Blocking: The port only receives BPDUs and drops the other packets.

Disconnected: The port is enabled with spanning tree function but not connected to any device.

LAG: Displays the LAG 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 Spanning Tree parameters.	Required. Enable Spanning Tree function on the switch and configure MSTP parameters on **Spanning Tree→STP Config→STP Config** page.

3	Configure CIST parameters for ports	Required. Configure CIST parameters for ports on **Spanning Tree→Port Config→Port Config** page.
4	Configure the MST region	Required. Create the MST region, VLAN-Instance mapping and the priority of the switch in the corresponding 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.

8.4 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.

8.4.1 Port Protect

STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains Loop Protect, Root Protect, BPDU Protect, BPDU Filter, TC Protect and BPDU flood functions.

- **Loop Protect**

Loop Protect function is used to prevent loops caused by link congestions or link failures. It is recommended to enable this function on root ports and alternate ports.

If the switch cannot receive BPDUs because of link congestions or link failures, the root port will become a designated port and the alternate port will transit to forwarding status, so loops will occur.

With Loop Protect function enabled, the port will temporarily transit to blocking state when the port does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.

- **Root Protect**

Root Protect function is used to ensure that the desired root bridge will not lose its position. It is recommended to enable this function on the designated ports of the root bridge.

Generally, the root bridge will lose its position once receiving higher-priority BPDUs caused by wrong configurations or malicious attacks. In this case, the spanning tree will be regenerated, and traffic needed to be forwarded along high-speed links may be lead to low-speed links.

With root protect function enabled, when the port receives higher-priority BDPUs, it will temporarily transit to blocking state. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.

- **TC Protect**

TC Protect function is used to prevent the switch from frequently removing MAC address entries and TC-BPDU flooding.

A switch removes MAC address entries upon receiving TC-BPDUs (the packets used to announce changes in the network topology). If a user maliciously sends a large number of TC-BPDUs 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.

With TC Protect function enabled, the port will drop the received TC-BPDUs and will not forward them.

- **BPDU Protect**

BPDU Protect function is used to prevent the port from receiving BPUDs. It is recommended to enable this function on edge ports.

Normally edge ports do not receive BPDUs, but if a user maliciously attacks the switch by sending BPDUs, the system automatically configures these ports as non-edge ports and regenerates the spanning tree.

With BPDU protect function enabled, the edge port will be shut down when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it.

- **BPDU Filter**

BPDU filter function is to prevent BPDU flooding in the network. It is recommended to enable this function on edge ports.

If a switch receives malicious BPDUs, it forwards these BPDUs to the other switches in the network, and the spanning tree will be continuously regenerated. In this case, the switch occupies too much CPU or the protocol status of BPDUs is wrong.

With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs, preventing the switch from being attacked by BPDUs.

- **BPDU Flood**

BPDU flood function is to control BPDUs forwarding when spanning tree function is globally disabled.

Generally, if a port receives BPDUs, it will forward them to all the other ports. With BPDU flood function enabled, the port can only forward BPDUs to other BPDU-flood-enabled ports.

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

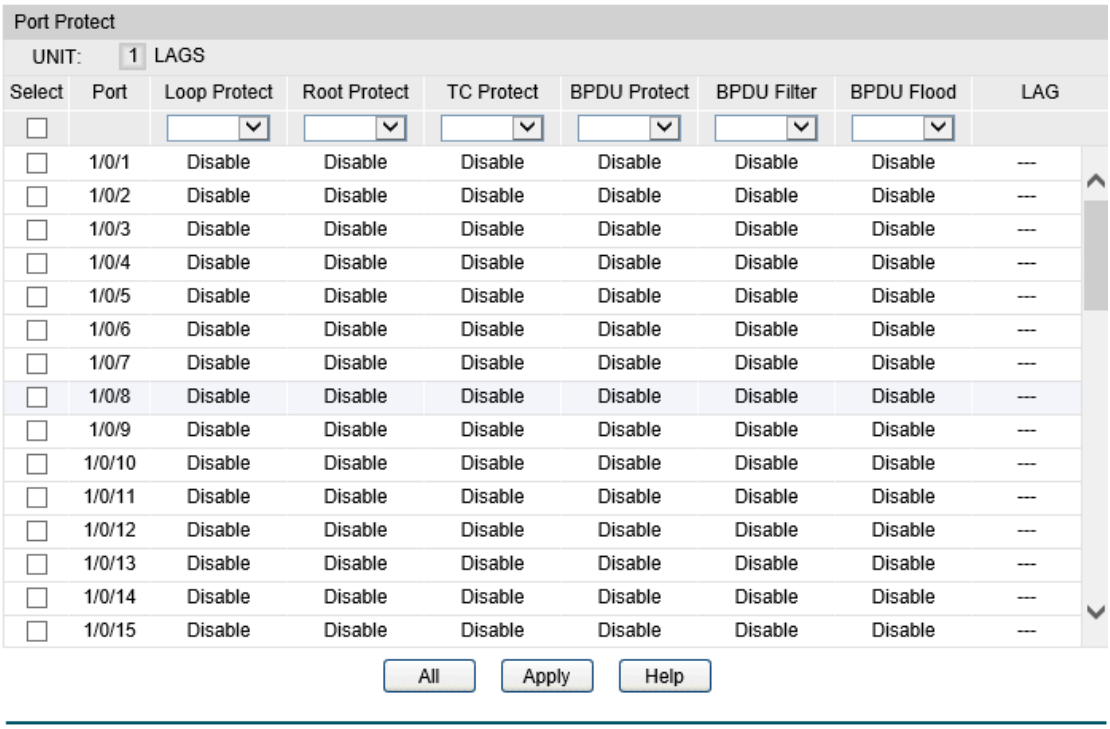


Figure 8-10 Port Protect

Configuration Procedure:

Configure the Port Protect features for the selected ports, and click **Apply**.

Entry Description:

➢ **Port Protect**

UNIT: Select the desired unit or LAGs.

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

Port: Displays the port number of the switch.

Loop Protect: Enable or disable the Loop Protect function. It is recommended to enable this function on root ports and alternate ports.

Loop Protect function is used to prevent loops caused by link congestions or link failures. With Loop Protect function enabled, the port will temporarily transit to blocking state when it does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.

Root Protect: Enable or disable the Root Protect function. It is recommended to enable this function on the designated ports of the root bridge.

Root Protect function is used to ensure that the desired root bridge will not lose its position. With root protect function enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.

TC Protect: Enable or disable the TC Protect function. It is It is recommended to enable this function on the ports of non-root switches.

TC Protect function is used to prevent the switch from frequently removing MAC address entries. With TC protect function enabled, the switch will drop TC-BPDUs.

BPDU Protect: Enable or disable the BPDU Protect function. It is It is recommended to enable this function on edge ports.

BPDU Protect function is used to prevent the edge port from receiving BPUDs. With BPDU protect function enabled, the edge port will be shut down when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it.

BPDU Filter: Enable or disable the BPDU Filter function. It is It is recommended to enable this function on edge ports.

BPDU filter function is to prevent BPDU flooding in the network. With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs, preventing the switch from being attacked by BPDUs.

BPDU Flood Enable or disable the BPDU Flood function.

With BPDU flood function enabled, the port can only forward BPDUs to other BPDU-flood-enabled ports.

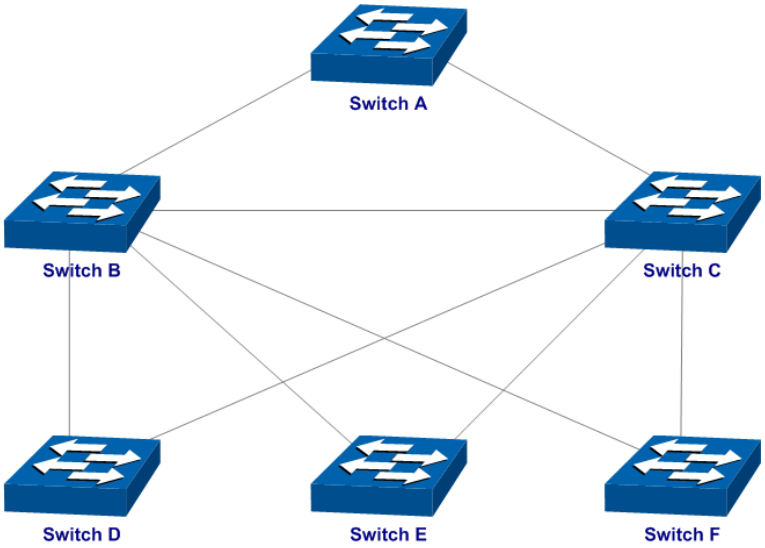
LAG: Displays the LAG which the port belongs to.

8.5 Application Example for MSTP 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 Instance 1 with B as the root bridge. The data in VLAN102, 104 and 106 are transmitted in Instance 2 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 Trunk, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.
2	Enable MSTP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→Port 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-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-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 Trunk, and add the ports to VLAN101-VLAN106. The detailed instructions can be found in the section 802.1Q VLAN.

Step	Operation	Description
2	Enable MSTP function	On **Spanning Tree→STP Config→STP Config** page, enable STP function and select MSTP version. On **Spanning Tree→Port 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-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-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 Switch B in Instance 1 as 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 Trunk, 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→Port 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-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.

5	Configure switch C as the designated 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 Switch C in Instance 2 as 0.

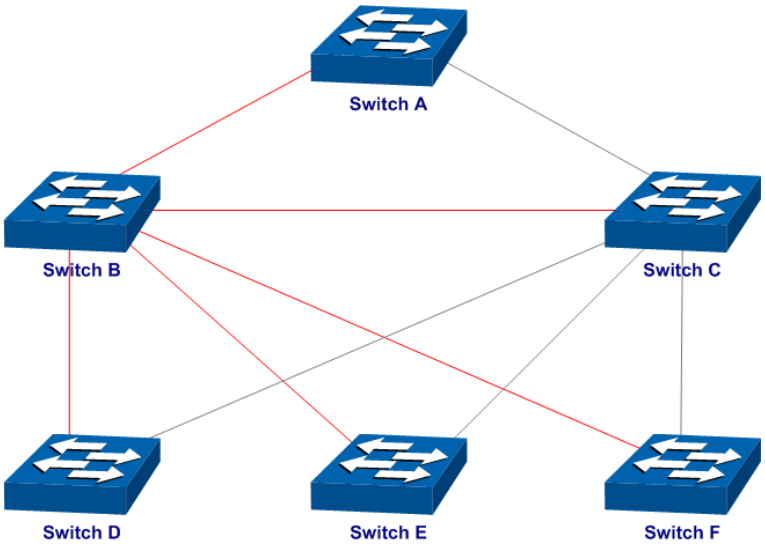
- Configure switch D:

Step	Operation	Description
1	Configure ports	On **VLAN→802.1Q VLAN** page, configure the link type of the related ports as Trunk, 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→Port 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-Instance mapping table of the MST region	On **Spanning Tree→MSTP Instance→Instance Config** page, configure VLAN-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.

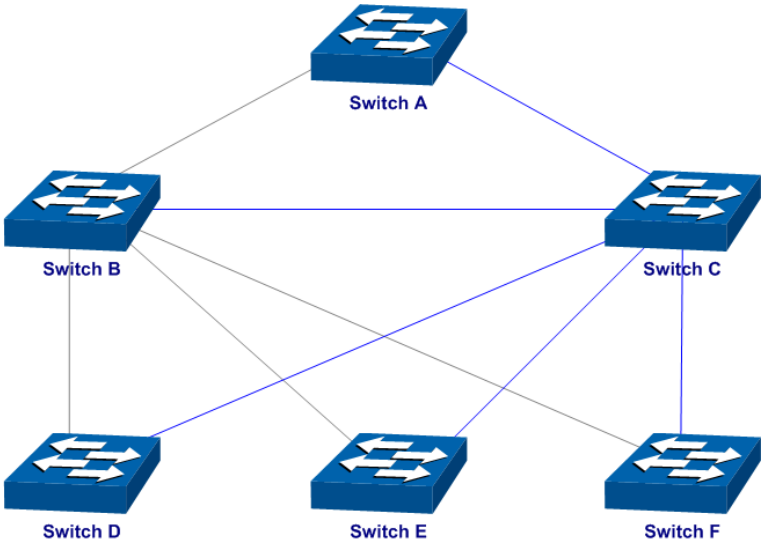
- The configuration procedure for switch E and F is the same with that for switch D.

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

- For Instance 1 (VLAN 101, 103 and 105), the red paths in the following figure are connected links; the gray paths are the blocked links.



- For Instance 2 (VLAN 102, 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 9 Multicast

➢ Multicast Overview

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

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

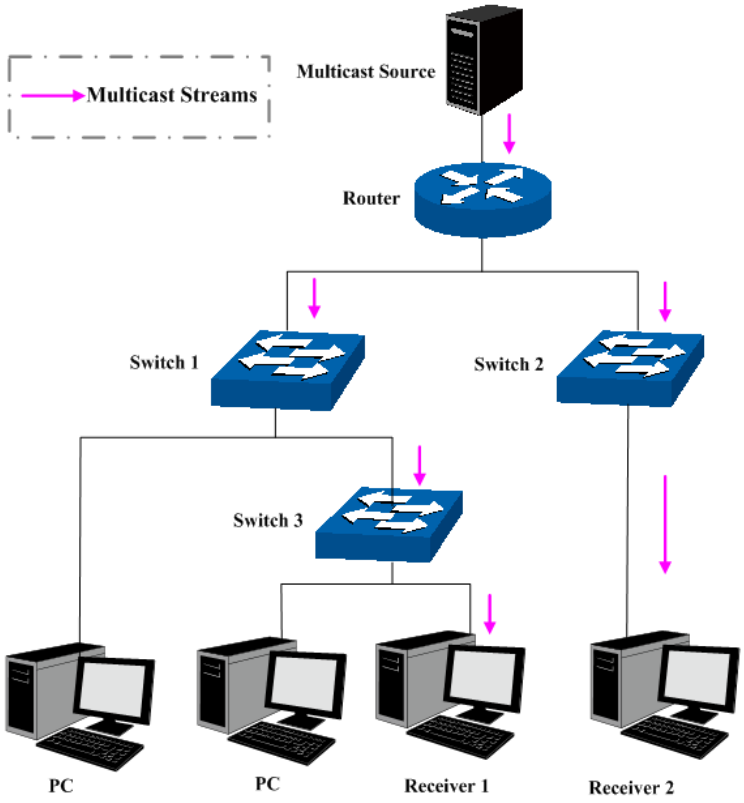


Figure 9-1 Information transmission in the multicast mode

Features of multicast:

1. The number of receivers is not certain. Usually point-to-multipoint transmission is needed;
2. Multiple users receiving the same information form a multicast group. The multicast information sender just need to send the information to the network device once;

3. Each user can join and leave the multicast group at any time;

4. Real time is highly demanded and certain packets drop is allowed.

➢ **Multicast Address**

1. Multicast IP Address:

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

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

Table 9-1 Range of the special multicast IP

2. 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 the following figure.

Figure 9-2 Mapping relationship between multicast IP 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 address.

➢ **Multicast Address Table**

The switch is forwarding multicast packets based on the multicast address table. As the transmission of multicast packets cannot span the VLAN, the first part of the multicast address table is VLAN ID, based on which the received multicast packets are forwarded in the VLAN owning the receiving port. The multicast address table is not mapped to an egress port but a group port list. When forwarding a multicast packet, the switch looks up the multicast address table based on the destination multicast address of the multicast packet. If the corresponding

entry cannot be found in the table, the switch will broadcast the packet in the VLAN owning the receiving port. If the corresponding entry can be found in the table, it indicates that the destination address should be a group port list, so the switch will duplicate this multicast data and deliver each port one copy. The general format of the multicast address table is described as Figure 9-3 below.

VLAN ID	Multicast IP	Port

Figure 9-3 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 four submenus: **IGMP Snooping**, **Multicast IP, Multicast Filter**, **Packet Statistics**.

9.1 IGMP Snooping

- **IGMP Snooping Process**

The switch, running IGMP Snooping, listens to the IGMP messages transmitted between the host and the router, and tracks the IGMP messages and the registered port. When receiving IGMP report message, the switch adds the port to the multicast address table; when the switch listens to IGMP leave message from the host, the router sends the Group-Specific Query message of the port to check if other hosts need this multicast, if yes, the router will receive IGMP report message; if no, the router will receive no response from the hosts and the switch will remove the port from the multicast address table. The router regularly sends IGMP query messages. After receiving the IGMP query messages, the switch will remove the port from the multicast address table if the switch receives no IGMP report message from the host within a period of time.

- **IGMP Messages**

The switch, running IGMP Snooping, processes the IGMP messages of different types as follows.

1. IGMP Query Message

IGMP query message, sent by the router, falls into two types, IGMP general query message and IGMP group-specific-query message. The router regularly sends IGMP general message to query if the multicast groups contain any member. When receiving IGMP leave message, the receiving port of the router will send IGMP group-specific-query message to the multicast group and the switch will forward IGMP group-specific-query message to check if other members in the multicast group of the port need this multicast.

When receiving IGMP general query message, the switch will forward them to all other ports in the VLAN owning the receiving port. The receiving port will be processed: if the receiving port

is not a router port yet, it will be added to the router port list with its router port time specified; if the receiving port is already a router port, its router port time will be directly reset.

When receiving IGMP group-specific-query message, the switch will send the group-specific query message to the members of the multicast group being queried.

2. IGMP Report Message

IGMP report message is sent by the host when it applies for joining a multicast group or responses to the IGMP query message from the router.

When receiving IGMP report message, the switch will send the report message via the router port in the VLAN as well as analyze the message to get the address of the multicast group the host applies for joining. The receiving port will be processed: if the receiving port is a new member port, it will be added to the multicast address table with its member port time specified; if the receiving port is already a member port, its member port time will be directly reset.

3. IGMP Leave Message

The host, running IGMPv1, does not send IGMP leave message when leaving a multicast group, as a result, the switch cannot get the leave information of the host momentarily. However, after leaving the multicast group, the host does not send IGMP report message any more, so the switch will remove the port from the corresponding multicast address table when its member port time times out. The host, running IGMPv2 or IGMPv3, sends IGMP leave message when leaving a multicast group to inform the multicast router of its leaving.

When receiving IGMP leave message, the querier will forward IGMP group-specific-query message to check if other members in the multicast group of the port need this multicast and reset the member port time to the leave time. When the leave time times out, the switch will remove the port from the corresponding multicast group. If no other member is in the group after the port is removed, the switch will send IGMP leave message to the router and remove the whole multicast group.

- **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.

Leave Time: Indicates the interval between the switch receiving a leave message from a host and the switch removing the host from the multicast groups. The default value is 1 second.

The IGMP Snooping function can be implemented on **Snooping Config**, **Port Config**, **VLAN Config** and **Multicast VLAN** pages.

9.1.1 Snooping Config

To configure the IGMP Snooping on the switch, please firstly configure IGMP global configuration and related parameters on this page.

If the multicast address of the received multicast data is not in the multicast address table, the switch will broadcast the data in the VLAN. When Unknown Multicast Discard feature is enabled, the switch drops the received unknown multicast so as to save the bandwidth and enhance the process efficiency of the system. Please configure this feature appropriate to your needs.

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

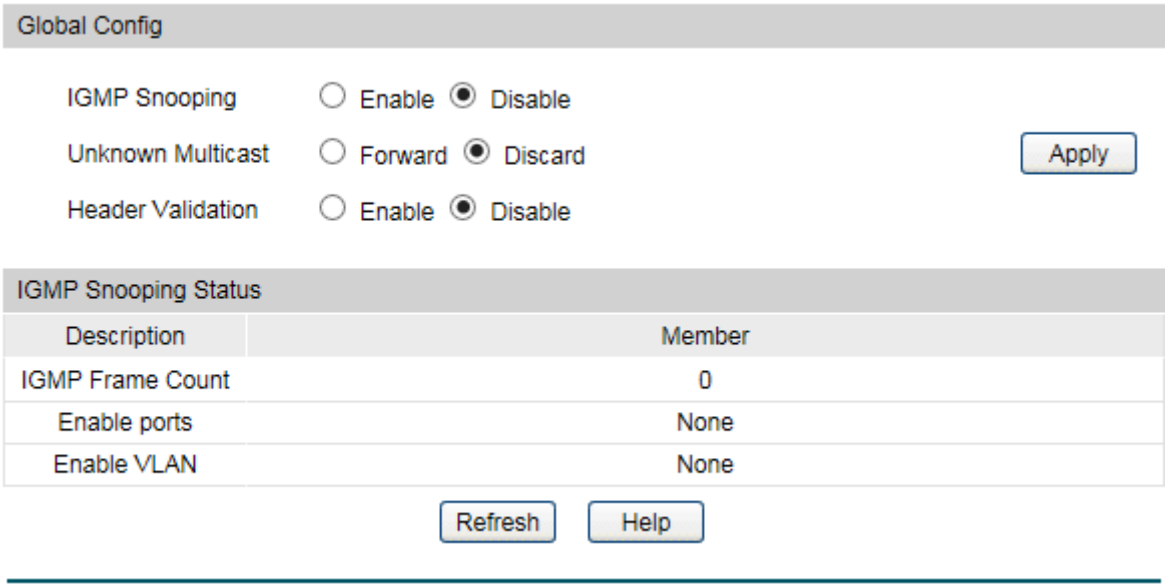


Figure 9-4 Basic Config

The following entries are displayed on this screen:

- **Global Config**

  IGMP Snooping: Enable or disable IGMP Snooping function globally on the switch.

  Unknown Multicast: Configure the way how the switch processes the multicast data sent to unknown multicast groups as Forward or Discard. Unknown multicast groups are multicast groups whose destination multicast address is not in the multicast forwarding table of the switch.

  Header Validation: Select Enable/Disable the validation of 2 IGMP header fields ToS (Type of Service) and Router Alert options. The fields validated depend on the IGMP version being used. Regardless of whether open the validation, TTL(Time To Live) must be 1.

  •IGMPv2 - Router Alert fields are validated.

  •IGMPv3 - ToS and Router Alert fields are validated

- **IGMP Snooping Status**

  Description: Displays IGMP Snooping status.

  Member: Displays the member of the corresponding status.

9.1.2 Port Config

On this page you can configure the IGMP feature for ports of the switch.

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

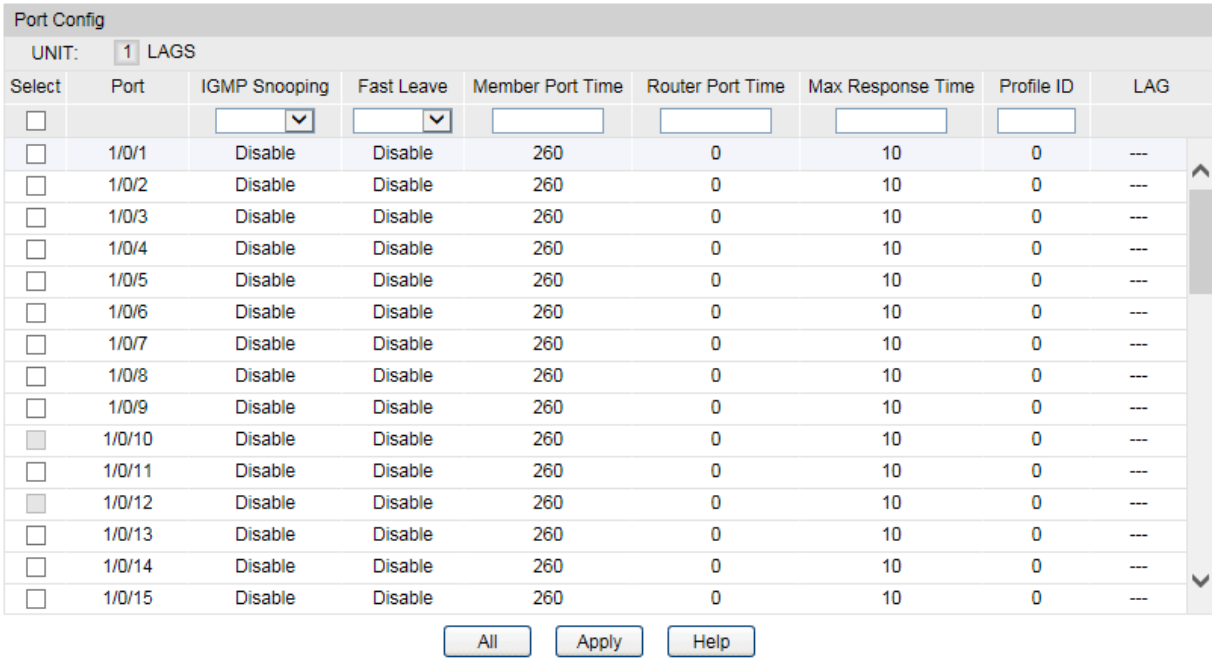


Figure 9-5 Port Config

The following entries are displayed on this screen:

➢ **Port Config**

UNIT: Select the unit ID of the desired member in the stack.

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

Port: Displays the port of the switch.

IGMP Snooping: Enable or disable IGMP Snooping for the desired port.

Fast Leave: Enable or 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.

Member Port Time: Member ports are ports connected to multicast group members on the switch. A port is considered to be a member port when it is added to a multicast group. The member port ages if the switch does not receive IGMP membership report message from the member port within the member port time. The switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds.

Router Port Time: Router ports are ports connected to Layer 3 devices on the switch. The router port ages if the switch does not receive

	IGMP query message from the router port within the router port time. The switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds.
Max Response Time:	Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.
Profile ID:	Enter the profile ID you create to bind the profile to the port. One port can only be bound to one profile.
LAG:	Displays the LAG number which the port belongs to.

Note:

1. Fast Leave on the port is effective only when the host supports IGMPv2 or IGMPv3.
2. When both Fast Leave feature and Unknown Multicast Discard feature are enabled, the leaving of a user connected to a port owning multi-user will result in the other users intermitting the multicast business.

9.1.3 VLAN Config

Multicast groups established by IGMP Snooping are based on VLANs. On this page you can configure different IGMP parameters for different VLANs.

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

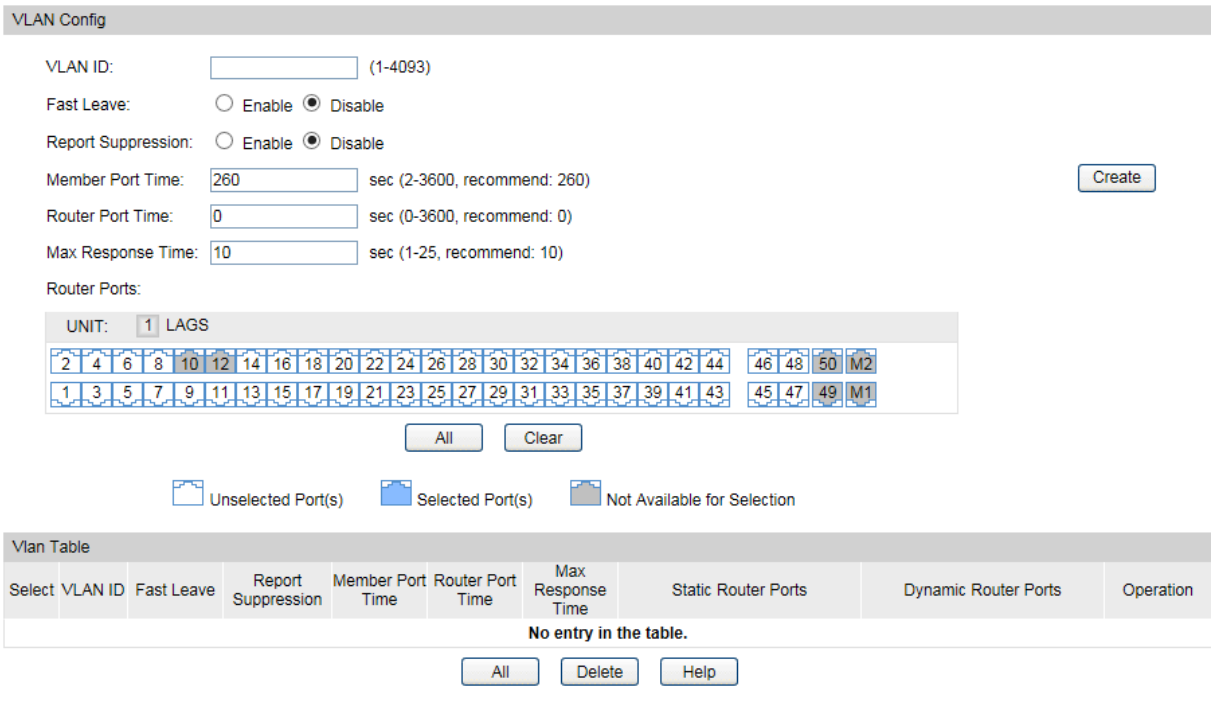


Figure 9-6 VLAN Config

The following entries are displayed on this screen:

➢ **VLAN Config**

VLAN ID:	Enter the VLAN ID to enable IGMP Snooping for the desired VLAN.

Fast Leave:	Enable or disable Fast Leave feature in this VLAN. If Fast Leave is enabled, the switch will immediately remove this port from the multicast group upon receiving IGMP leave messages.
Report Suppression:	If this function is enabled, the switch will only forward the first IGMP report message to Layer 3 devices and suppress subsequent IGMP report messages from the same multicast group during one query interval, which reduces the number of IGMP packets.
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.
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.
Max Response Time:	Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.
Router Ports:	Enter the static router port which is mainly used in the network with stable topology.
UNIT:	Select the unit ID of the desired member in the stack.

- **VLAN Table**

Select:	Select the desired VLAN ID for configuration. It is multi-optional.
VLAN ID:	Displays the VLAN ID.
Fast Leave:	Displays the fast leave feature of the VLAN.
Report Suppression:	Displays the report suppression feature of the VLAN.
Member Port Time:	Displays the member port time of the VLAN.
Router Port Time:	Displays the router port time of the VLAN.
Max Response Time:	Displays the max response 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.

Configuration procedure:

Step	Operation	Description
1	Enable IGMP Snooping function	Required. Enable IGMP Snooping globally on the switch on **Multicast→IGMP Snooping→Snooping Config page**.
2	Configure the multicast parameters for VLANs	Optional. Configure the multicast parameters for VLANs on **Multicast→IGMP Snooping→VLAN Config page.** If a VLAN has no multicast parameters configuration, it indicates the IGMP Snooping is not enabled in the VLAN, thus the multicast data in the VLAN will be broadcasted.

9.1.4 Querier Config

In an IP multicast network that runs IGMP, a Layer 3 multicast device works as an IGMP querier to send IGMP queries and manage the multicast table. But IGMP is not supported by the devices in Layer 2 network. IGMP Snooping Querier can act as an IGMP Router in Layer 2 network. It can help to create and maintain multicast forwarding table on the switch with the Query messages it generates.

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

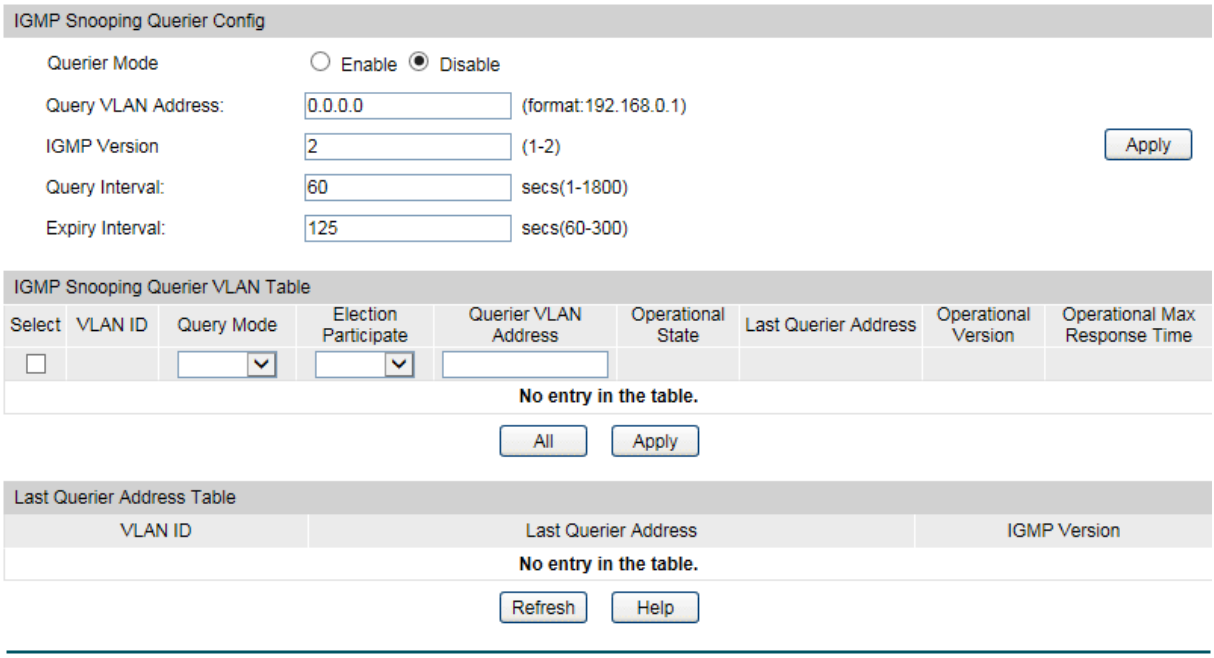


Figure 9-7 Querier Config

The following entries are displayed on this screen:

- **IGMP Snooping Querier Config**

Querier Mode:	Enter the Query mode which for the IGMP snooping querier on the device. When enabled, the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from the switches that want to receive IP multicast traffic. The IGMP snooping feature listens to these IGMP reports to establish appropriate forwarding.
Query VLAN Address:	Enter the General Query Message source IP address.
IGMP Version:	Enter the IGMP version used in periodic IGMP queries.
Query Interval:	Enter the time interval of sending a general query frame by IGMP Snooping Querier.
Expiry Interval:	Enter the Expiry Interval which is amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

- **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 Mode:	Displays the Querier Mode of VLAN.
Election Participate:	Displays the Election Participate of VLAN.
Querier VLAN Address:	Displays the General Query Message source IP address.
Operational State:	Displays the Operational State.
Last Querier Address:	Displays the Last Querier Address.
Operational Version:	Displays the Operational Version.
Operational Max Response Time:	Displays the value of Operational Max Response Time.

- **Last Querier Address Table**

VLAN ID:	Displays the VLAN ID.
Last Querier Address:	Displays the Last Querier Address.
IGMP Version:	Displays the Last Querier Version.

9.1.5 Profile Config

On this page you can configure an IGMP profile.

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

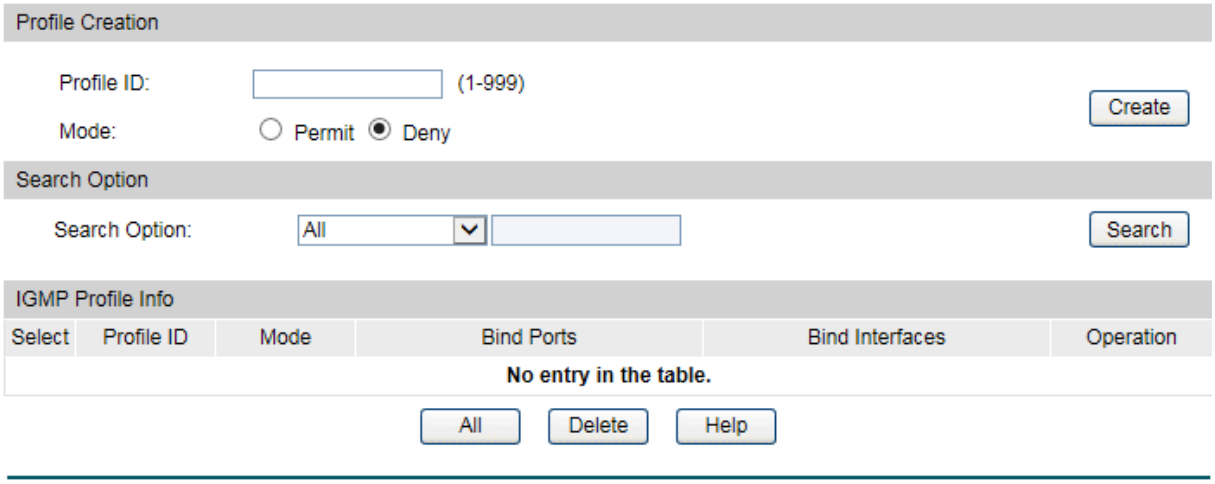


Figure 9-8 Profile Create

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**

  Profile ID: Enter the profile ID the desired entry must carry.

- **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.

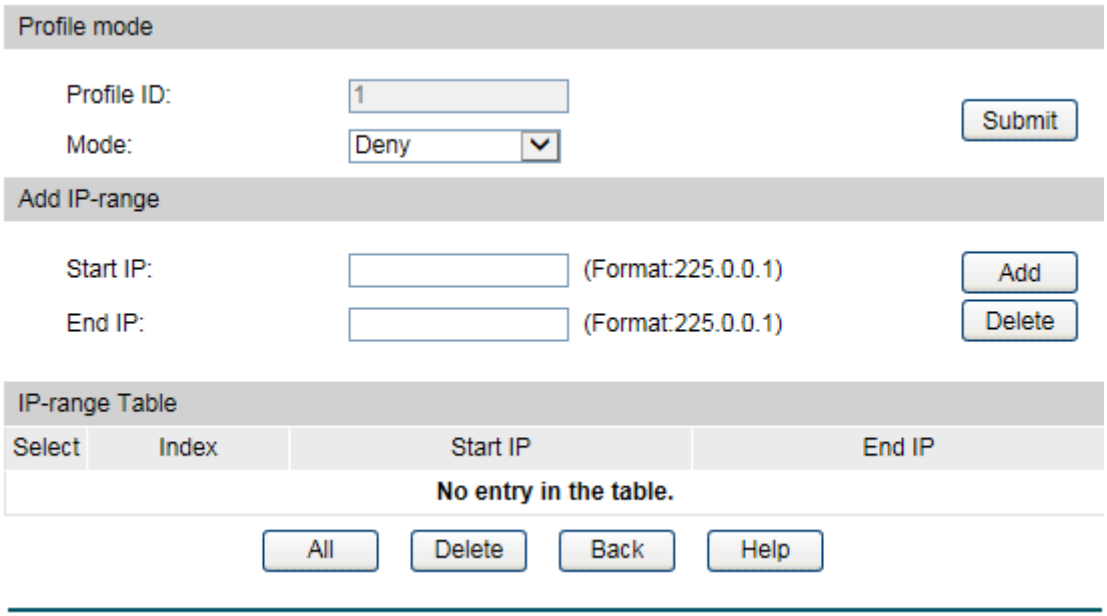


Figure 9-9 Profile Config

- **Profile Mode**

Profile ID: Displays the Profile ID.

Mode: Configure the filtering mode 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 the start IP address of the IP range.

End IP: Enter the end IP address of the IP range.

- **IP-range Table**

Select: Select to delete the IP range entry.

Index: Displays the index of the IP range.

Start IP: Displays the start IP address of the IP range.

End IP: Displays the end IP address of the IP range.

9.2 MLD Snooping

➢ **MLD Snooping**

Multicast Listener Discovery (MLD) snooping is applied for efficient distribution of IPv6 multicast data to clients and routers in a Layer 2 network. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. The list is constructed and maintained by snooping IPv6 multicast control packets. MLD snooping performs a similar function in IPv6 as IGMP snooping in IPv4.

The switch, running MLD Snooping, listens to the MLD messages transmitted between the host and the router, and tracks the MLD messages and the registered port. When receiving MLD report message, the switch adds the port to the multicast address table; when the switch listens to MLD Done message from the host, the router sends the Multicast-Address-Specific Query message of the port to check if other hosts need this multicast, if yes, the switch will receive MLD report message; if no, the switch will receive no response from the hosts and the switch will remove the port from the multicast address table. The router regularly sends MLD query messages. After receiving the MLD query messages, the switch will remove the port from the multicast address table if the switch receives no MLD report message from the host within a period of time.

➢ **MLD Snooping Fundamentals**

1. MLD Messages

MLD Queries： MLD Queries include General Queries and Multicast-Address-Specific Queries (MASQs) and are sent out from the MLD router.

MLD Reports： When a host wants to join a multicast group or responds to the MLD queries, it will send out an MLD report.

MLD Done Messages： When a host wants to leave a multicast group, it will send out an MLD Done message to inform the IPv6 multicast routers of its leave.

2. Relevant Ports of the Switch

Router Port: Indicates the switch port that links toward the MLD router.

Member Port: Indicates the switch port that links toward the multicast members.

3. Timers

Router Port Aging Time: Within this time, if the switch does not receive MLD queries from the router port, it will delete this port from the router port list. The default value is 300 seconds.

Member Port Aging Time: Within this time, if the switch does not receive MLD reports from the member port, it will delete this port from the MLD multicast group. The default value is 260 seconds.

General Query Interval: The interval between the multicast router sends out general queries.

➢ **MLD Snooping Process**

1. General Query

The MLD router regularly sends MLD general queries to query if the multicast groups contain any members. When receiving MLD general queries, the switch will forward them to all other ports in the VLAN. The receiving port will be processed: if the receiving port is not a router port yet, it will be added to the router port list with its router port aging time specified; if the receiving port is already a router port, its router port aging time will be directly reset.

2. Membership Report

The host will send MLD report messages when it applies for joining a multicast group or responds to the MLD query message from the router.

When receiving MLD report message, the switch will forward the report message via the router port in the VLAN, and analyze the message to get the address of the multicast group the host applies for joining. If the multicast group does not exist, it will create the group entry. The receiving port will be processed: if the receiving port is a new member port, it will be added to the forward list of the multicast group with its member port aging time specified; if the receiving port is already a member port, its member port aging time will be directly reset.

3. Member Leave

The host will send MLD Done message when leaving a multicast group to inform the router of its leaving.

When Immediate Leave is not enabled in a VLAN and a Done message is received on a port of this VLAN, the switch will generate MASQs on this port to check if there are other members in this multicast group. The user can control when a port membership is removed for an exiting address in terms of the number and interval of MASQs. If there is no Report message received from this port during the switch maximum response time, the port on which the MASQ was sent is deleted from the multicast group. If the deleted port is the last member of the multicast group, the multicast group is also deleted. The switch will send Done message to the router ports of the VLAN.

In IPv6，Layer 2 switches can use Multicast Listener Discovery (MLD) Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data. This list is constructed by snooping IPv6 multicast control packets.

The MLD Snooping function can be implemented on **Snooping Config**, **Port Config**, **VLAN Config**, **Querier Config** and **Profile Config** pages.

9.2.1 Snooping Config

To configure the MLD Snooping on the switch, please firstly configure MLD global configuration and related parameters on this page.

Chose the menu **Multicast→MLD Snooping→Snooping Config** to load the following page.

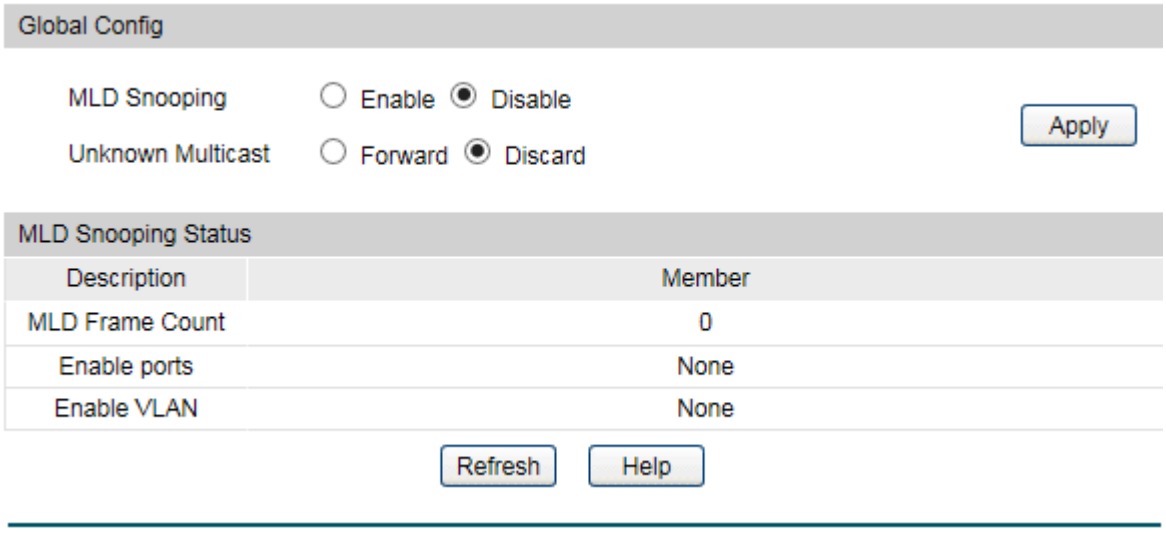


Figure 9-10 MLD Snooping Config

The following entries are displayed on this screen:

- **Global Config**

  MLD Snooping: Enable or disable MLD Snooping function globally.

  Unknown Multicast: Choose to forward or drop unknown multicast data.

  Unknown IPv6 multicast packets refer to those packets without corresponding forwarding entries in the IPv6 multicast table:

  When unknown multicast filter is enabled, the switch will discard all received unknown IPv6 multicast packets;

  When unknown multicast filer is disabled, all unknown IPv6 multicast packets are flooded in the ingress VLAN.

- **MLD Snooping Status**

  Description: Displays MLD Snooping status.

  Member: Displays the member of the corresponding status.

9.2.2 Port Config

On this page you can configure MLD Snooping function with each single port.

Choose the menu **Multicast→MLD Snooping→Port Config** to load the following page.

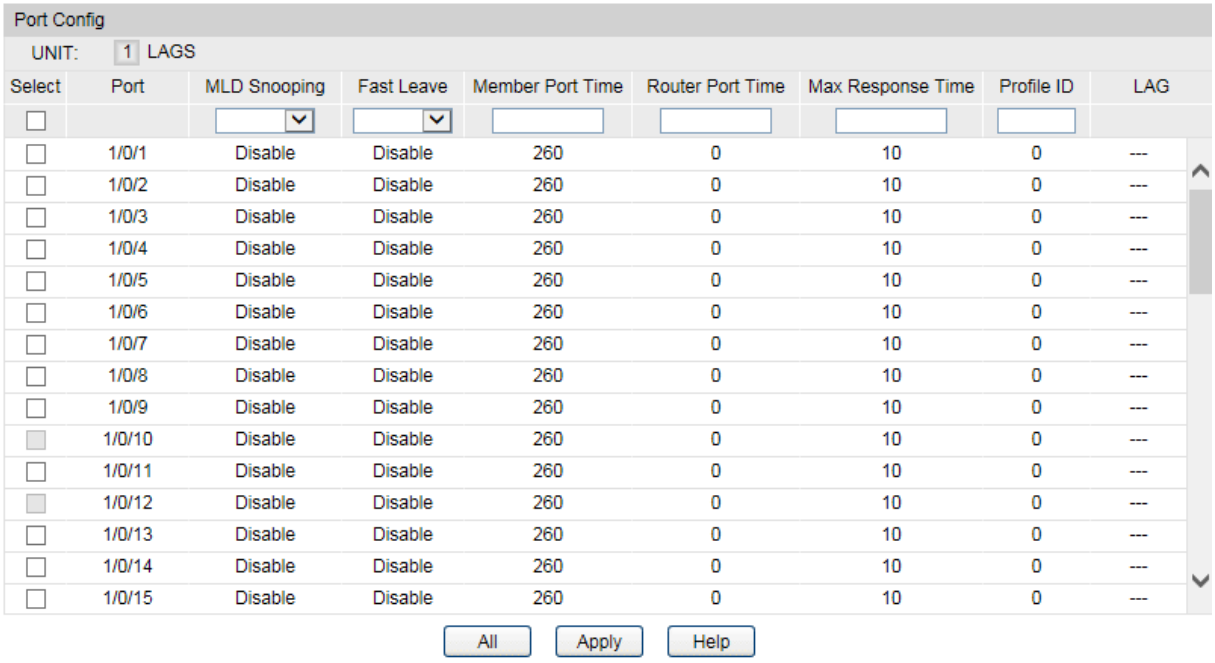


Figure 9-11 Port Config

The following entries are displayed on this screen:

➢ **Port Config**

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

Select: Select the port you want to configure.

Port: Displays the port number.

MLD Snooping: Select Enable/Disable MLD Snooping for the desired port.

Fast Leave: Select Enable/Disable Fast Leave feature for the desired port. If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD done messages.

Member Port Time: Member ports are ports connected to multicast group members on the switch. A port is considered to be a member port when it is added to a multicast group. The member port ages if the switch does not receive MLD membership report message from the member port within the member port time. The switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds.

Router Port Time: Router ports are ports connected to Layer 3 devices on the switch. The router port ages if the switch does not receive IGMP query message from the router port within the router

port time. The switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds.

Max Response Time: Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.

Profile ID: Enter the profile ID you create to bind the profile to the port. One port can only be bound to one profile.

LAG: Displays the LAG number.

9.2.3 VLAN Config

Multicast groups established by MLD Snooping are based on VLANs. On this page you can configure different MLD parameters for different VLANs.

Choose the menu **Multicast→MLD Snooping→VLAN Config** to load the following page.

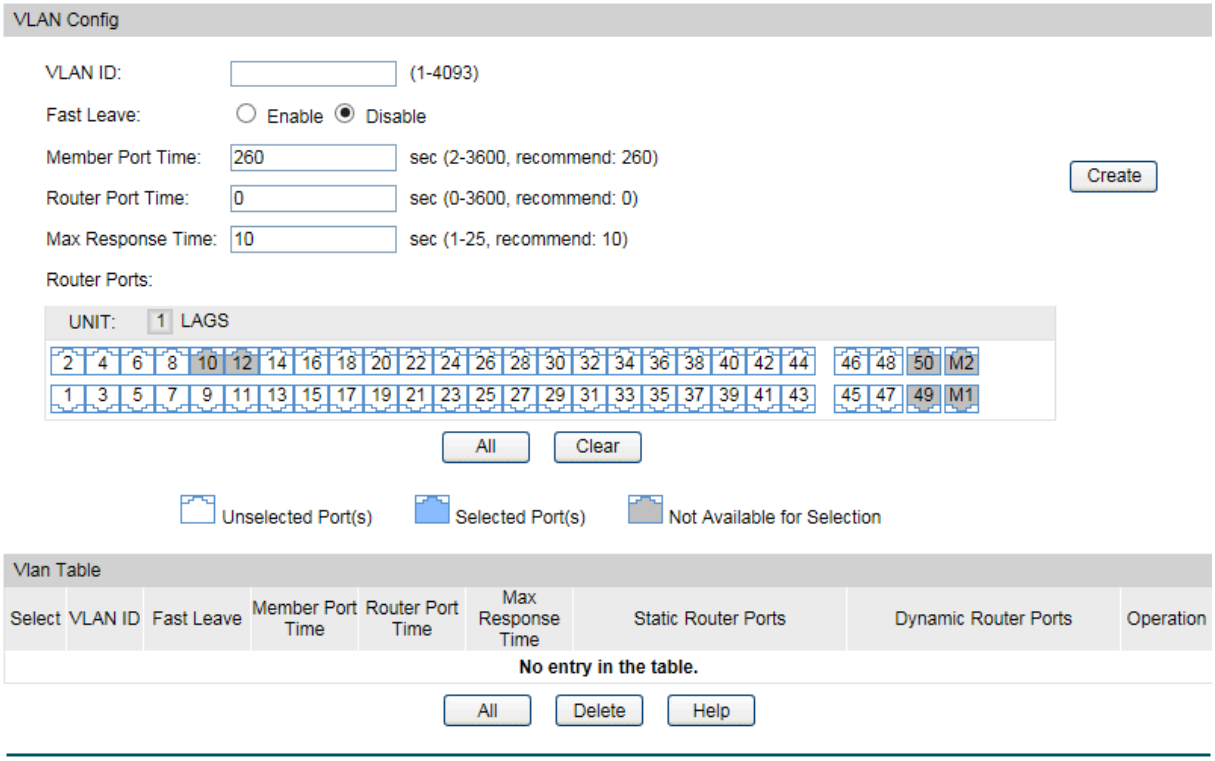


Figure 9-12 VLAN Config

The following entries are displayed on this screen:

➢ **VLAN Config**

VLAN ID: Enter the VLAN ID to enable MLD Snooping for the desired VLAN.

Fast Leave: Enable or disable Fast Leave feature in this VLAN. If Fast Leave is enabled, the switch will immediately remove this port from the multicast group upon receiving MLD leave messages.

Member Port Time: Specify the aging time of the member port. Within this time, if the switch doesn't receive MLD report message from the member port, it will consider this port is not a member port any more.

Router Port Time: Specify the aging time of the router port. Within this time, if the switch doesn't receive MLD query message from the router port, it will consider this port is not a router port any more.

Max Response Time: Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.

Router Ports: Enter the static router port which is mainly used in the network with stable topology.

UNIT: Select the unit ID of the desired member in the stack.

- **VLAN Table**

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

VLAN ID: Displays the VLAN ID.

Fast Leave: Displays the fast leave feature of the VLAN.

Member Port Time: Displays the member port time of the VLAN.

Router Port Time: Displays the router port time of the VLAN.

Max Response Time: Displays the max response 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.

Configuration procedure:

Step	Operation	Description
1	Enable MLD Snooping function	Required. Enable MLD Snooping globally on the switch on **Multicast→MLD Snooping→Snooping Config page**.
2	Configure the multicast parameters for VLANs	Optional. Configure the multicast parameters for VLANs on **Multicast→MLD Snooping→VLAN Config page.** If a VLAN has no multicast parameters configuration, it indicates the MLD Snooping is not enabled in the VLAN, thus the multicast data in the VLAN will be broadcasted.

9.2.4 Querier Config

In an IP multicast network that runs MLD, a Layer 3 multicast device works as an MLD querier to send MLD queries and manage the multicast table. But MLD is not supported by the devices in

Layer 2 network. MLD Snooping Querier can act as an MLD Router in Layer 2 network. It can help to create and maintain multicast forwarding table on the switch with the Query messages it generates.

Choose the menu **Multicast→MLD Snooping→Querier Config** to load the following page.

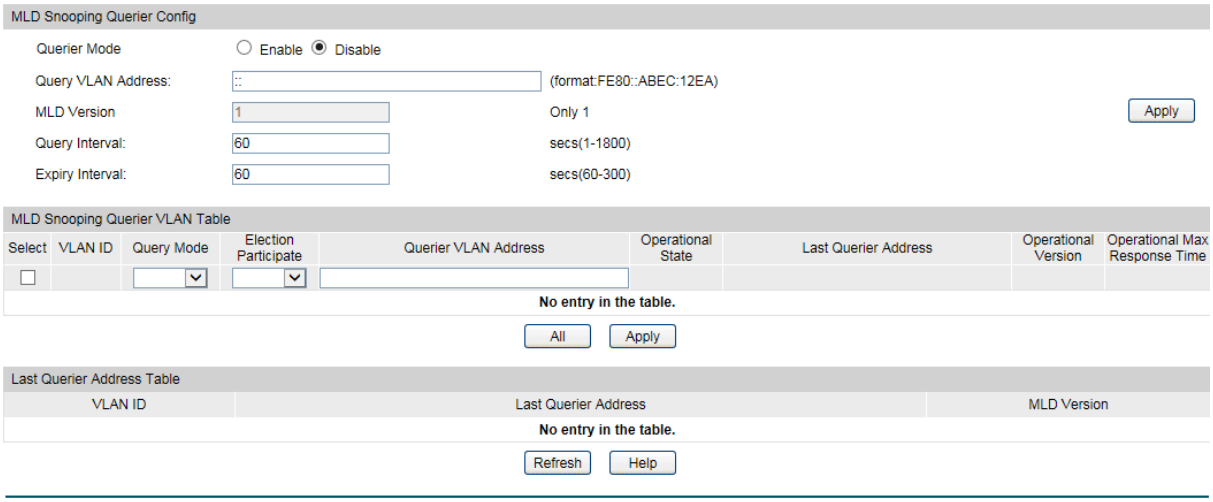


Figure 9-13 Packet Statistics

The following entries are displayed on this screen:

- **MLD Snooping Querier Config**

Querier Mode: Enter the Query mode which for the MLD snooping querier on the device. When enabled, the MLD snooping querier sends out periodic MLD queries that trigger MLD report messages from the switches that want to receive IP multicast traffic. The MLD snooping feature listens to these MLD reports to establish appropriate forwarding.

Query VLAN Address: Enter the General Query Message source IP address.

MLD Version: Enter the MLD version used in periodic MLD queries.

Query Interval: Enter the time interval of sending a general query frame by MLD Snooping Querier.

Expiry Interval: Enter the Expiry Interval which is amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

- **MLD Snooping Querier Table**

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

VLAN ID: Displays the ID of the VLAN that enables MLD Snooping Querier.

Query Mode: Displays the Querier Mode of VLAN.

Election Participate: Displays the Election Participate of VLAN.

Querier VLAN Address:	Displays the General Query Message source IP address.
Operational State:	Displays the Operational State.
Last Querier Address:	Displays the Last Querier Address.
Operational Version:	Displays the Operational Version.
Operational Max Response Time:	Displays the value of Operational Max Response Time.

➢ **Last Querier Address Table**

VLAN ID:	Displays the VLAN ID.
Last Querier Address:	Displays the Last Querier Address.
MLD Version:	Displays the Last Querier Version.

9.2.5 Profile Config

On this page you can configure an MLD profile.

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

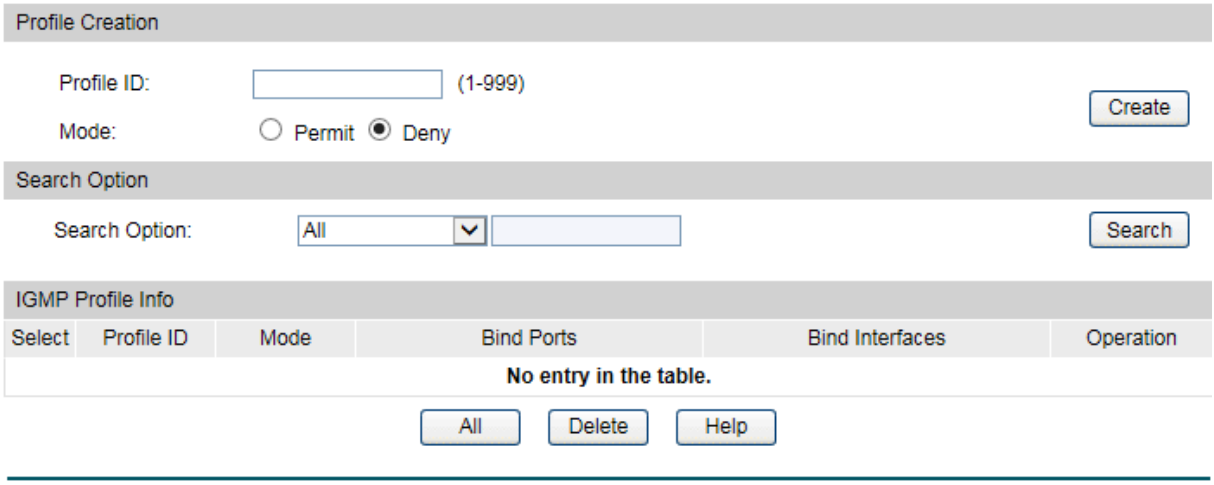


Figure 9-14 Profile Create

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**

Profile ID: Enter the profile ID the desired entry must carry.

➢ **MLD 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.

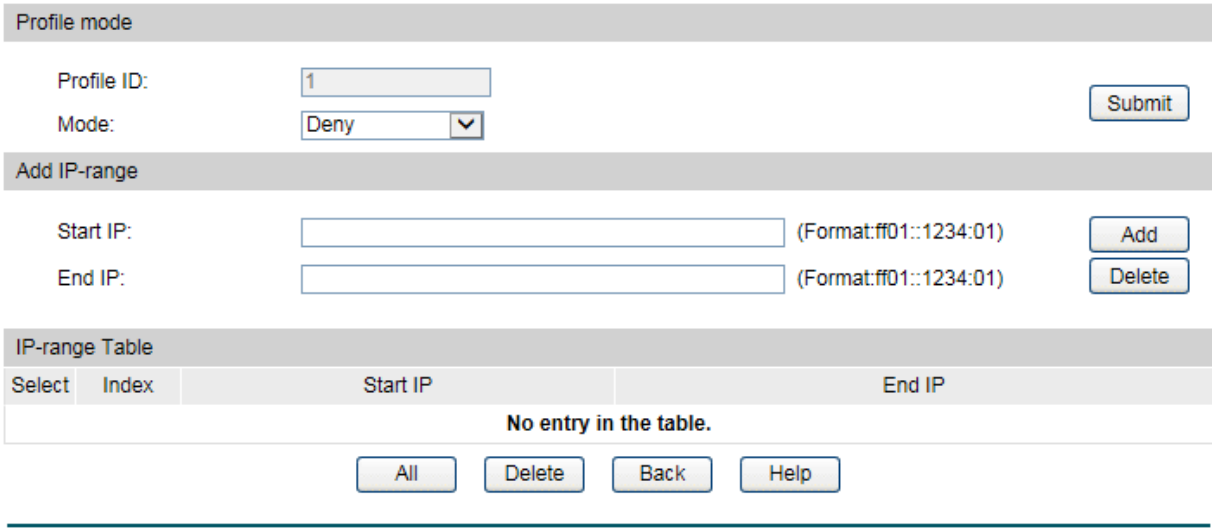


Figure 9-15 Profile Config

➢ **Profile Mode**

Profile ID: Displays the Profile ID.

Mode: Configure the filtering mode 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 the start IP address of the IP range.

End IP: Enter the end IP address of the IP range.

➢ **IP-range Table**

Select: Select to delete the IP range entry.

Index: Displays the index of the IP range.

Start IP: Displays the start IP address of the IP range.

End IP: Displays the end IP address of the IP range.

9.3 MVR

Multicast VLAN Registration (MVR) allows a single multicast VLAN to be shared for multicast member ports in different VLANs. In IGMP snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

Only one MVR multicast VLAN per switch or per stack is supported.

9.3.1 MVR Config

Use this page to view and configure the global settings for Multicast VLAN Registration (MVR).

Choose the menu **Multicast→MVR→MVR Config** to load the following page.

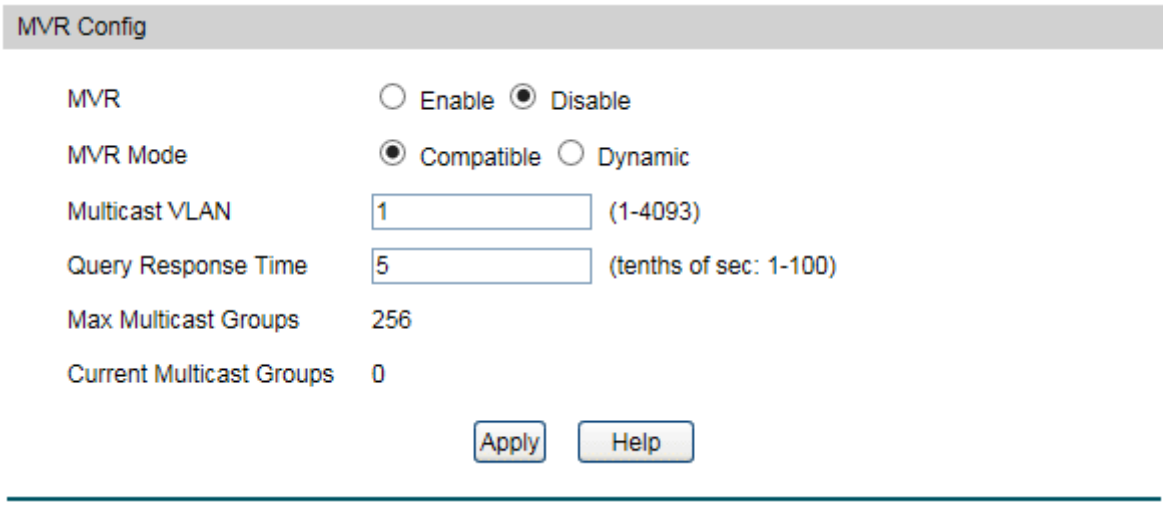


Figure 9-16 MVR Global Config

The following entries are displayed on this screen:

- **MVR Config**

MVR:	Before configuring functions related to MVR, click Enable to enable MVR function globally.
MVR Mode:	Select the MVR mode. **Compatible**: The switch working in Compatible mode does not learn multicast groups, which means the MVR switch does not forward IGMP reports from the hosts to the IGMP router. So the IGMP router has to be statically configured to transmit all the required multicast streams to the MVR switch. **Dynamic**: The MVR switch learns existing multicast groups by snooping the IGMP queries from the IGMP router and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN.
Multicast VLAN:	Specify the VLAN on which the multicast data will be received.
Query Response Time:	Set the maximum time wait for the IGMP membership report on a receiver port. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR response time for an IGMP group membership report before removing the port from the multicast group. The value ranges from 1 to 100 tenths of seconds.
Max Multicast Groups:	Displays the max number of multicast groups that MVR supports.
Current Multicast Groups:	Displays the current number of the MVR groups.

9.3.2 Interface Config

Use this page to configure MVR settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click Edit. The same MVR settings are applied to all selected interfaces.

Choose the menu **Multicast→MVR→Interface Config** to load the following page.

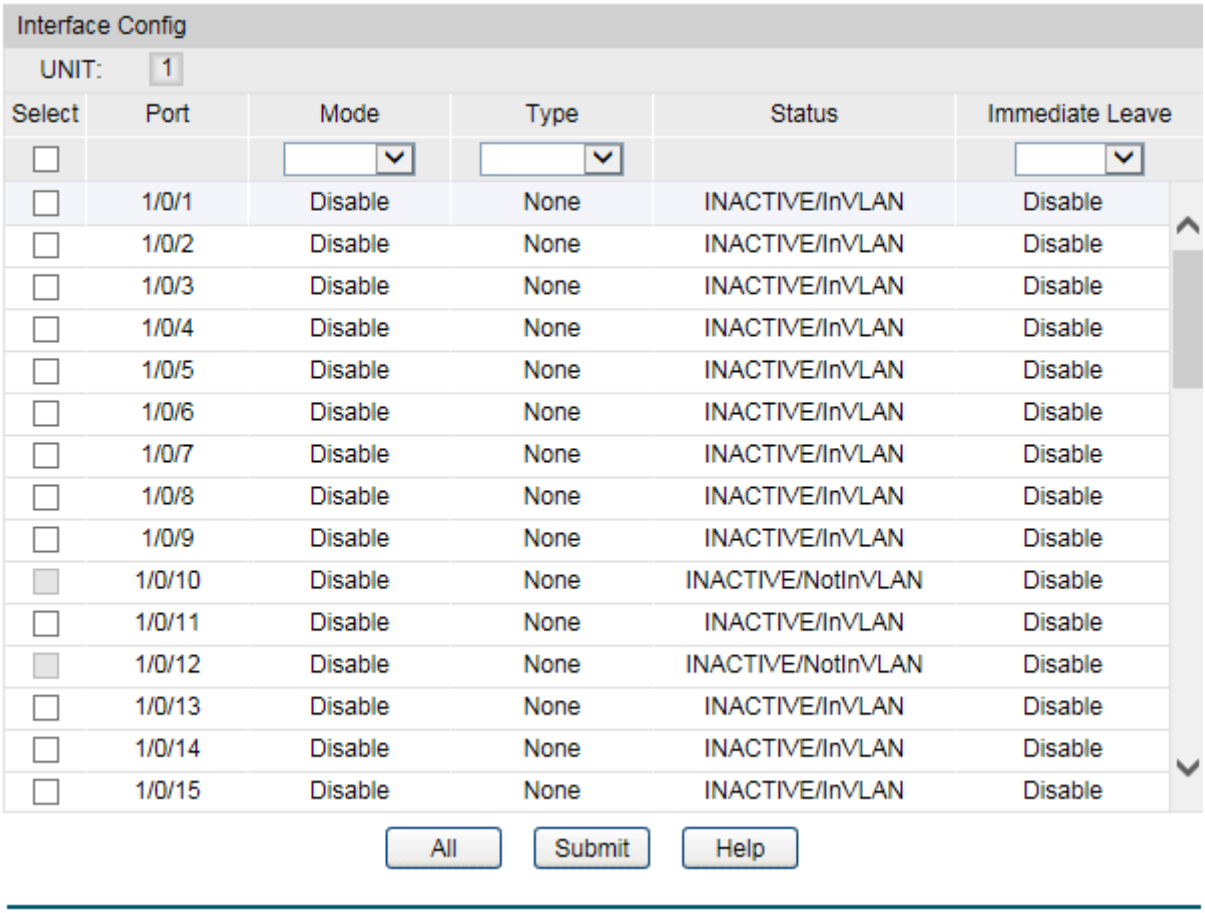


Figure9-17 MVR Interface Config

The following entries are displayed on this screen:

➢ **Interface Config**

UNIT: Select the unit ID of the desired member in the stack.

Select: Select the desired port to configure MVR settings on the specific interface. It is multi-optional.

Port: Displays the port number of the switch.

Mode: Enable or disable MVR on this port.

Type: Configure an port as one of the following type:

None: Non-MVR port.

Source: Configure the uplink ports that receive and send multicast data as source ports. All source ports belong to the multicast VLAN.

Receiver: The port where a listening port is connected to the switch. Receiver ports cannot belong to the multicast VLAN.

Status: Displays the port's status.

INACTIVE/InVLAN: The port is part of a VLAN but inactive.

INACTIVE/NotInVLAN: The port is not part of any VLAN and inactive.

ACTIVE/InVLAN: The port is part of a VLAN and active.

Immediate Leave: Enable or disable the immediate leave function on this port. When immediate leave is enabled, the receiver port will be removed for the multicast group when an IGMP leave message is received on this port, without sending an IGMP query message and waiting for the IGMP group membership report.

This function should only be enabled on receiver ports to which a single receiver device is connected.

9.3.3 Member Config

Use this page to view or configure MVR groups. MVR maintains two types of group entries in its database, Static and Dynamic. Static entries are configured by the administrator and Dynamic entries are learned by MVR on the source ports.

Choose the menu **Multicast→MVR→Member Config** to load the following page.

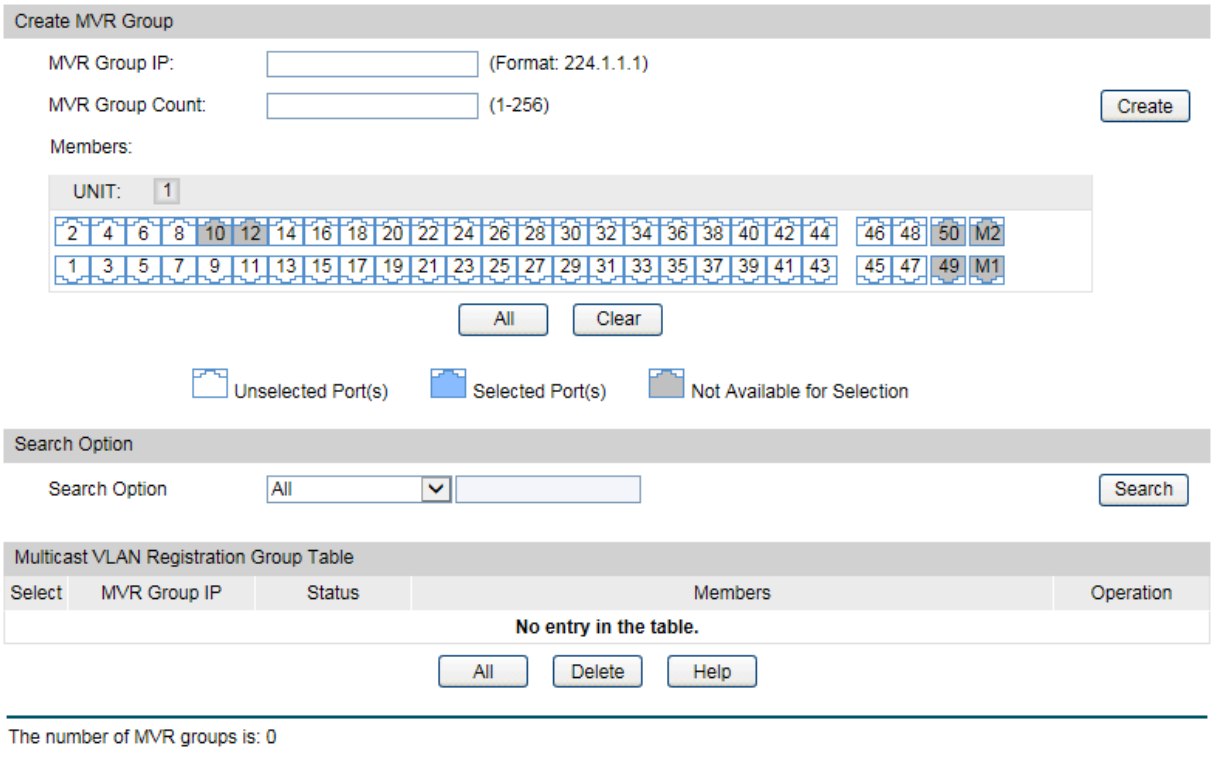


Figure9-18 MVR Member Config

The following entries are displayed on this screen:

- **Create MVR Group**

  MVR Group IP: Configure an IP multicast address on the switch or use the MVR Group Count parameter to create a contiguous series of MVR group addresses. Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have required to receive data on that multicast address.

  MVR Group Count: Specify the number of the contiguous multicast IP group addresses.

  Members: Statically configure the ports to receive multicast traffic sent to the multicast VLAN and the IP multicast address specified above.

- **Multicast VLAN Registration Group Table**

  MVR Group IP: Displays the IP multicast address.

  Status: Displays the status of the multicast group.

  Members: Displays the multicast members in this group.

  Operation: Click Edit to modify this multicast group's parameters.

9.3.4 Traffic

This page shows statistical information about IGMP packets intercepted by MVR.

Choose the menu **Multicast→MVR→Traffic** to load the following page.

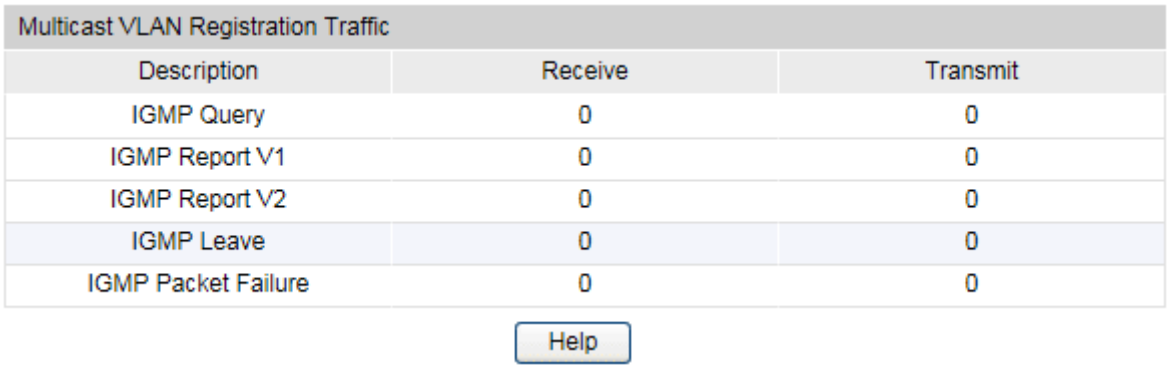


Figure9-19 MVR Traffic

The following entries are displayed on this screen:

- **Multicast VLAN Registration Traffic**

  IGMP Query: Displays the port number of the switch.

  IGMP Report V1: Displays the number of packets of IGMP Report V1.

  IGMP Report V2: Displays the number of packets of IGMP Report V2.

IGMP Leave: Displays the number of packets of IGMP Leave.

IGMP Packet Failure: Displays the number of packets of IGMP Packet Failure.

9.4 Multicast Table

You can view different types of multicast table in the follow pages.

9.4.1 Summary

On this page you can view the summary of the multicast table and multicast entries.

Choose the menu **Multicast→Multicast Table→Summary** to load the following page.

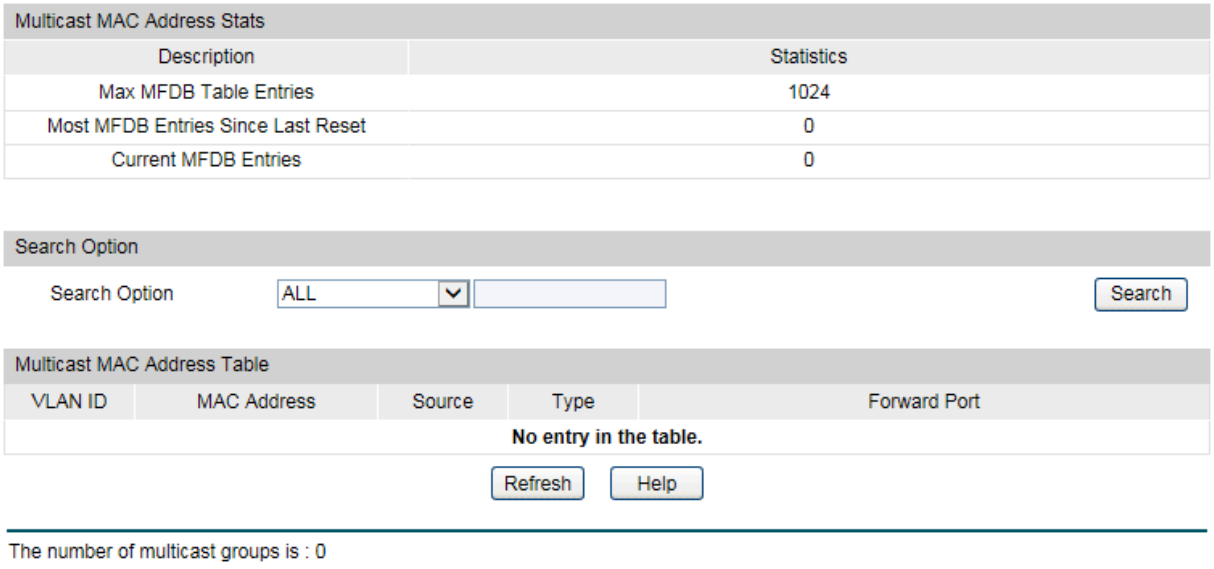


Figure 9-20 Multicast Table

The following entries are displayed on this screen:

➢ **Multicast MAC Address Stats**

Max MFDB Table Entries: Displays the Max MFDB Table Entries.

Most MFDB Entries Since Last Reset: Displays the Most MFDB Entries.

Current MFDB Entries: Displays the Current MFDB Entries.

➢ **Search Option**

Select the rules for displaying multicast MAC table to find the desired entries quickly.

All: Displays all multicast MAC entries.

VLAN ID: Enter the VLAN ID the desired entry must carry.

MAC Address: Enter the multicast MAC address the desired entry must carry.

Source: Enter the source the desired entry must carry.

Type: Enter the type the desired entry must carry.

Forward Port: Enter the forward port number the desired entry must carry.

- **Multicast MAC Address Table**

VLAN ID: Displays the VLAN ID of the multicast MAC entries.

MAC Address: Displays the MAC address of the multicast MAC entries.

Source: Displays the source of the multicast MAC entries.

Type: Displays the type of the multicast MAC entries.

Forward Port: Displays the forward port of the multicast MAC entries.

9.4.2 Static Config

On this page you can configure the static multicast table. The multicast groups configured here are not learned by IGMP Snooping and independent of multicast filter.

Choose the menu **Multicast→Multicast Table→Static Config** to load the following page.

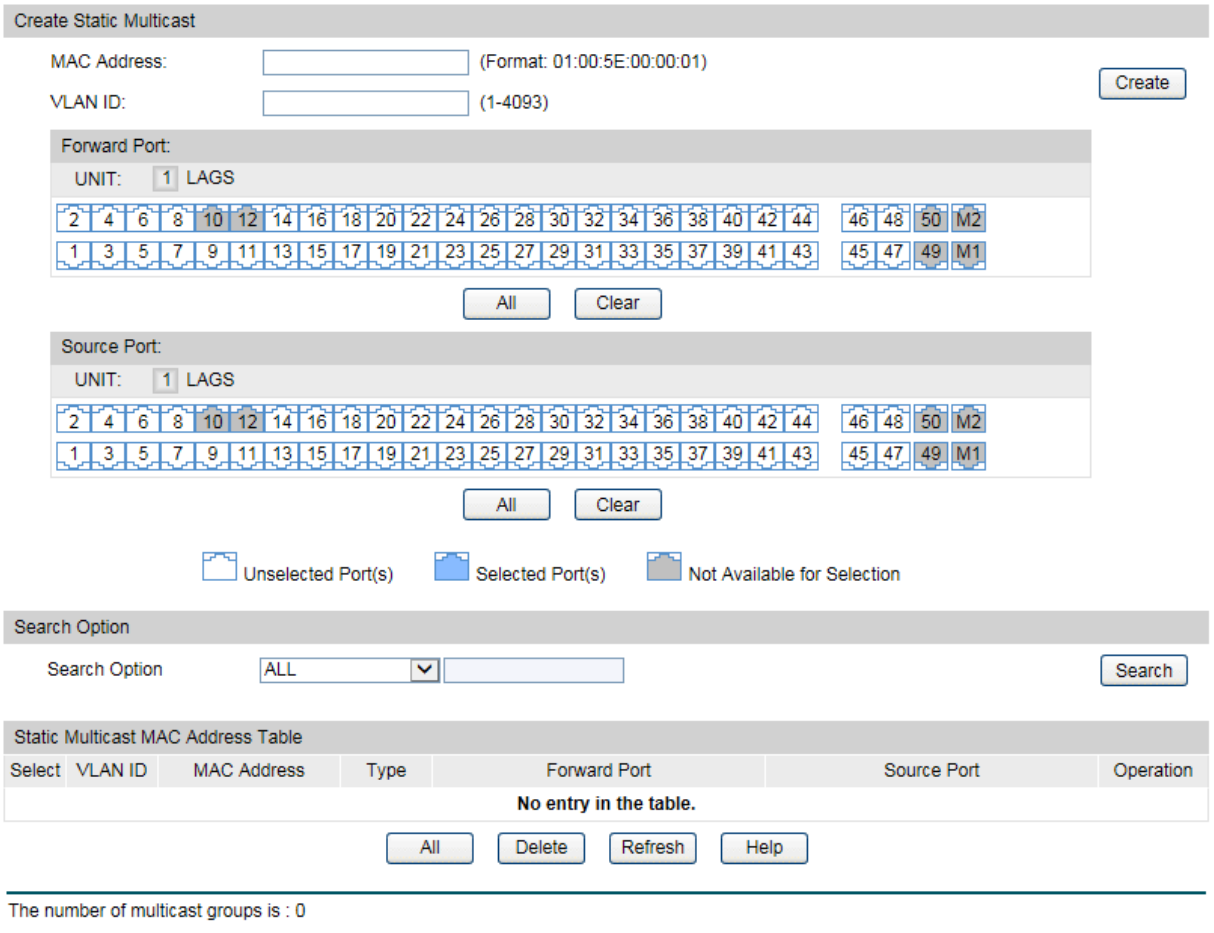


Figure 9-21 Static Multicast Table

The following entries are displayed on this screen:

- **Create Static Multicast**

  MAC Address: Enter the multicast MAC address to create multicast MAC entry.

  VLAN ID: Enter the VLAN ID to add multicast MAC entry for the desired VLAN.

  Forward Port: Select the forward port of multicast MAC entry.

  Source Port: Select the source port of multicast MAC entry.

- **Search Option**

  Search Option: Select the rules for displaying multicast MAC table to find the desired entries quickly.

  • All: Displays all multicast MAC entries.

  • VLAN ID: Enter the VLAN ID the desired entry must carry.

  • MAC Address: Enter the multicast MAC address the desired entry must carry.

  • Forward Port: Enter the forward port number the desired entry must carry.

  • Source Port: Enter the source port number the desired entry must carry.

- **Static Multicast MAC Address Table**

  VLAN ID: Displays the VLAN ID of the multicast MAC entries.

  MAC Address: Displays the MAC address of the multicast MAC entries.

  Type: Displays the type of the multicast MAC entries.

  Forward Port: Displays the forward port of the multicast MAC entries.

  Source Port: Displays the source port of the multicast MAC entries.

9.4.3 IGMP Snooping

In an MAC multicast environment, all receivers can join a multicast group. On this page you can view the information of the multicast groups for IGMP Snooping already on the switch.

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

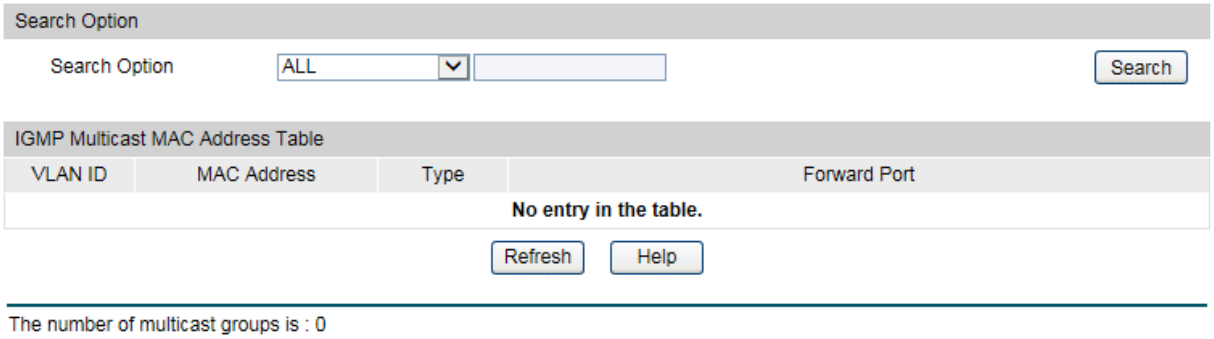


Figure 9-22 IGMP Multicast Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying multicast MAC table to find the desired entries quickly.

• All: Displays all multicast MAC entries.

• VLAN ID: Enter the VLAN ID the desired entry must carry.

• MAC Address: Enter the multicast MAC address the desired entry must carry.

• Forward Port: Enter the forward port number the desired entry must carry.

➢ **IGMP Multicast MAC Address Table**

VLAN ID: Displays the VLAN ID of the multicast MAC entries.

MAC Address: Displays the MAC address of the multicast MAC entries.

Type: Displays the type of the multicast MAC entries.

Forward Port: Displays the forward port of the multicast MAC entries.

9.4.4 MLD Snooping

On this page you can view the summary of the multicast table and multicast entries.

Choose the menu **Multicast→Multicast Table→Summary** to load the following page.

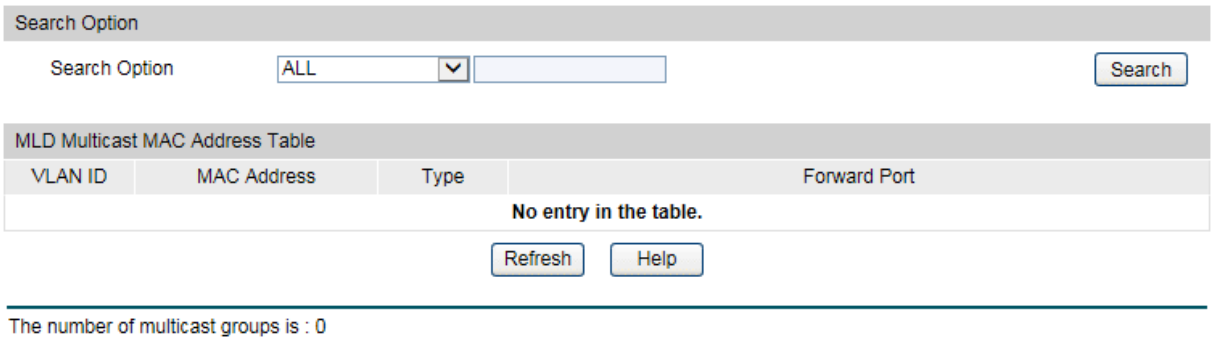


Figure 9-23 MLD Multicast Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying multicast MAC table to find the desired entries quickly.

All: Displays all multicast MAC entries.

• VLAN ID: Enter the VLAN ID the desired entry must carry.

• MAC Address: Enter the multicast MAC address the desired entry must carry.

• Forward Port: Enter the forward port number the desired entry must carry.

➢ **MLD Multicast MAC Address Table**

VLAN ID: Displays the VLAN ID of the multicast MAC entries.

MAC Address: Displays the MAC address of the multicast MAC entries.

Type: Displays the type of the multicast MAC entries.

Forward Port: Displays the forward port of the multicast MAC entries.

9.4.5 SSM Groups

This page displays information about IGMP snooping and MLD snooping for source specific multicast.

Choose the menu **Multicast→Multicast Table→SSM Groups** to load the following page.

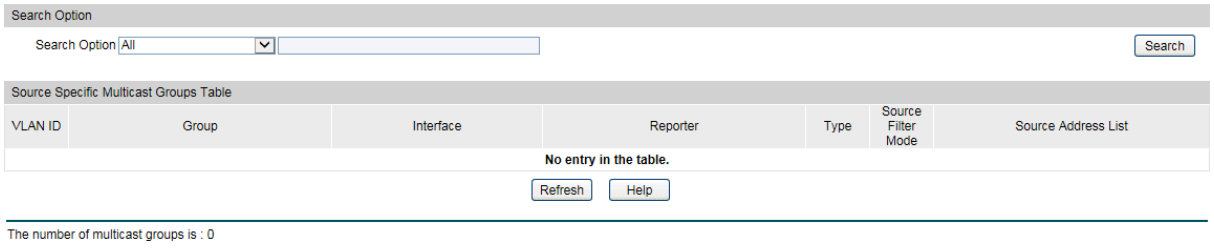


Figure 9-24 SSM Group

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying source specific multicast table to find the desired entries quickly.

All: Displays all source specific multicast entries.

• VLAN ID: Enter the VLAN ID the desired entry must carry.

• Group: Enter the group the desired entry must carry.

• Interface: Enter the interface the desired entry must carry.

• Reporter: Enter the reporter the desired entry must carry.

• Type: Enter the type the desired entry must carry.

• Source Filter Mode: Enter the source filter mode the desired entry must carry.

• Source Address List: Enter the source address list the desired entry must carry.

➢ **Source Specific Multicast Groups Table**

VLAN ID: Displays the VLAN ID of the entries.

Group: Displays the Group of the entries.

Interface: Displays the Interface of the entries.

Reporter: Displays the Reporter of the entries.

Type: Displays the type of the entries.

Source Filter Mode: Displays the Source Filter Mode of the entries.

Source Address List: Displays the Source Address List of the entries.

9.4.6 SSM Entries

This page displays the entries in the multicast forwarding database (MFDB) for source specific multicast, that were added because they were discovered by the IGMP Snooping or MLD Snooping feature.

Choose the menu **Multicast→Multicast Table→SSM Entries** to load the following page.

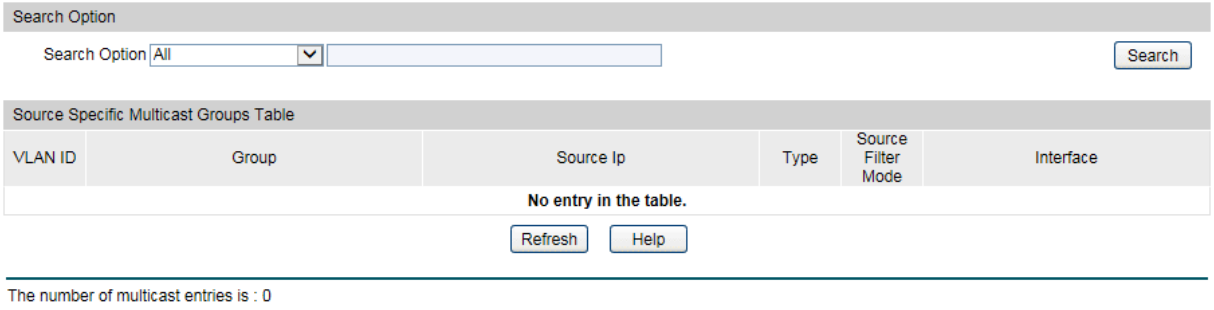


Figure 9-25 SSM Group Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying source specific multicast table to find the desired entries quickly.

• All: Displays all source specific multicast entries.

• VLAN ID: Enter the VLAN ID the desired entry must carry.

• Group: Enter the group the desired entry must carry.

• Source Ip: Enter the source ip the desired entry must carry.

• Type: Enter the type the desired entry must carry.

• Source Filter Mode: Enter the source filter mode the desired entry must carry.

• Interface: Enter the interface the desired entry must carry.

➢ **Source Specific Multicast Groups Table**

VLAN ID: Displays the VLAN ID of the entries.

Group: Displays the Group of the entries.

Source IP Displays the Source IP of the entries.

Type: Displays the type of the entries.

Source Filter Mode: Displays the Source Filter Mode of the entries.

Interface: Displays the Interface of the entries.

9.4.7 SSM Status

This page displays statistics about the source specific multicast forwarding database (SSMFDB).

Choose the menu **Multicast→Multicast Table→SSM Status** to load the following page.

IGMP Snooping

Description	Statistics
Total Entries	512
Most SSM FDB Entries Ever Used	0
Current Entries	0

MLD Snooping

Description	Statistics
Total Entries	256
Most SSM FDB Entries Ever Used	0
Current Entries	0

Refresh Help

Figure 9-26 SSM Status

The following entries are displayed on this screen:

- **IGMP Snooping**

Total Entries:	Displays the Max MFDB Table Entries.
Most SSM FDB Entries Ever Used:	Displays the Most SSM FDB Entries Ever Used of source specific multicast.
Current Entries:	Displays the Current Entries of source specific multicast.

- **MLD Snooping**

Total Entries:	Displays the Max MFDB Table Entries.
Most SSM FDB Entries Ever Used:	Displays the Most SSM FDB Entries Ever Used of source specific multicast.
Current Entries:	Displays the Current Entries of source specific multicast.

Return to CONTENTS

Chapter 10 Routing

Routing is the method by which the host or gateway decides where to send the datagram. Routing is the task of finding a path from a sender to a desired destination. It may be able to send the datagram directly to the destination, if that destination is on one of the networks that are directly connected to the host or gateway. However, what if the destination is not directly reachable? The host or gateway will attempt to send the datagram to a gateway that is nearer to the destination. The goal of a routing protocol is very simple: It is to supply the information that is needed to do routing. This chapter describes how to configure the IPv4 unicast routing on the T3700G-52TQ.

10.1 Interface

Interface is a virtual interface in Layer 3 mode and mainly used for realizing the Layer 3 connectivity between VLANs or routed ports. Each VLAN interface is corresponding to one VLAN. Each routed port is corresponding to one port. Loopback Interface is purely software implemented. Interface has its own IP address and subnet mask to identify the subnet it belongs to, and it works as the gateway of the subnet to forward Layer 3 IP packets.

Choose the menu **Routing** → **Interface** → **Interface Config** to load the following page.

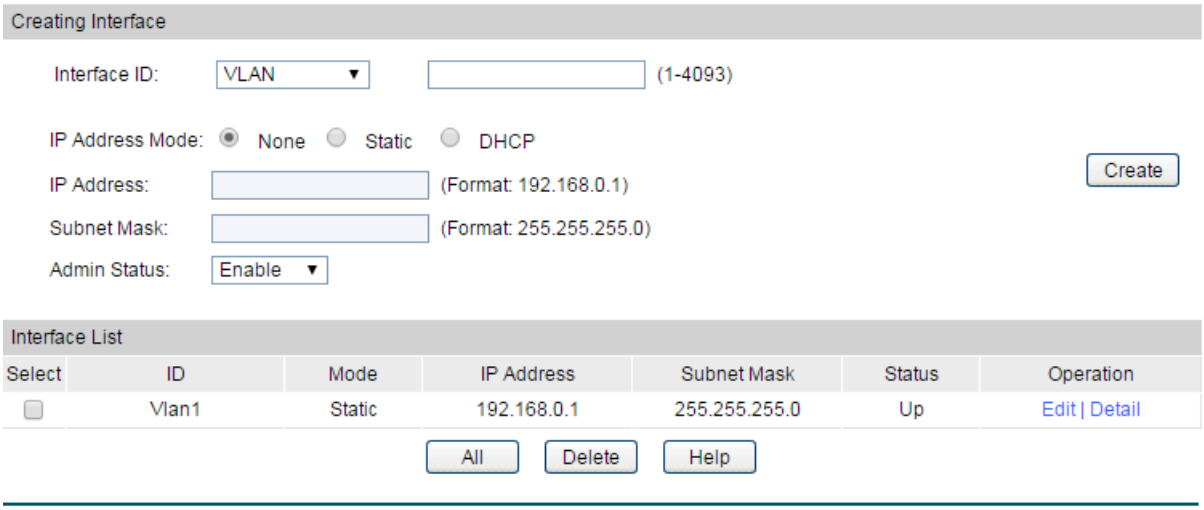


Figure 10-1 Interface Config

Configuration Procedure:

1) In the **Creating Interface** section, specify an interface ID and configure relevant parameters for the interface according to your actual needs. Then click **Create**.

2) In the **Interface List** section, you can view the corresponding interface entry you create.

Entry Description:

➢ **Create Interface**

Interface ID: Enter the ID of the interface corresponding to VLAN ID, loopback ID, or routed port.

IP Address Mode:	Specify the IP address assignment mode of the interface. **None**: without ip. **Static**: setup manually. **DHCP**: allocated through DHCP.
IP Address:	Specify the IP address of the interface.
Subnet Mask:	Specify the subnet mask of the interface's IP address.
Admin Status:	Enable or disable the interface's Layer 3 capabilities.

➢ **Interface List**

Select :	Select the interfaces to modify or delete.
ID:	Displays the ID of the interface.
Mode:	Displays IP address allocation mode. **None**: without ip. **Static**: setup manually. **DHCP**: allocated through DHCP.
IP Address:	Displays the IP address of the interface.
Subnet Mask:	Displays the subnet mask of the interface.
Status:	Displays interface current working status. Working status is up when admin status is enable, line protocol is up and IP Address is set.
Operation:	You can configure the interface by clicking the "**Edit**", or check Detail information by clicking "**Detail**".

In the Figure 10-1 Interface Config, click **Edit** to display the following figure:

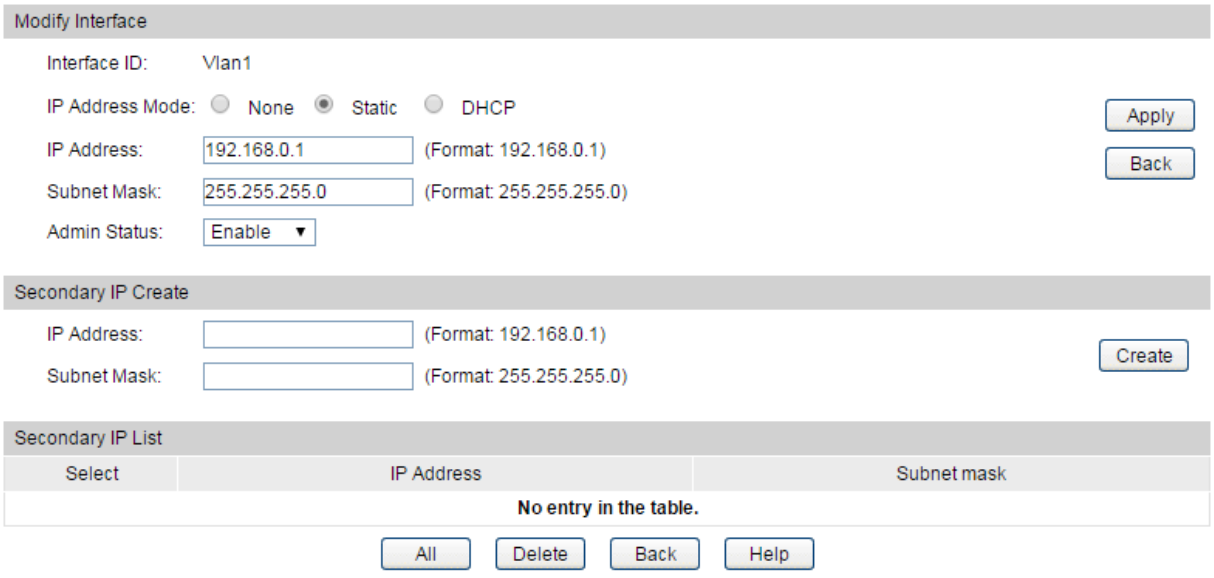


Figure 10-2 Interface Modify

Configuration Procedure:

1) In the **Modify Interface** section, specify an interface ID and configure relevant parameters for the interface according to your actual needs. Then click **Apply**.

2) In the **Secondary IP Create** section, configure the secondary IP for the specified interface which allows you to have two logical subnets using one physical subnet. Then click **Create**.

3) In the **Secondary IP List** section, you can view the corresponding secondary IP entry you create.

Entry Description:

Interface ID:	Displays ID of the interface, including VLAN ID, loopback interface and routed port.
IP Address Mode:	View and modify the IP address allocation mode. **None**: without ip. **Static**: setup manually. **DHCP**: allocated through DHCP.
IP Address:	View and modify the IP address of the interface.
Subnet Mask:	View and modify the subnet mask of the interface.
Admin Status:	View and modify the Admin status. Choose '**Disable**' to disable the interface's Layer 3 capabilities.

In the Figure 10-1 Interface Config, click **Detail** to display the following figure:

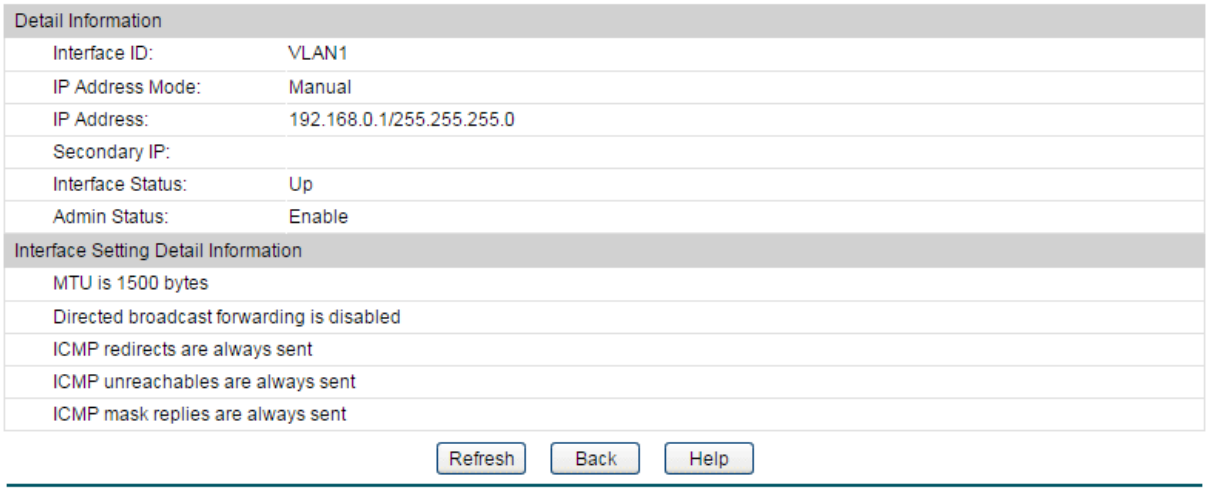


Figure 10-3 Detail Information

➢ **Detail Information**

Interface ID:	Displays ID of the interface, including VLAN ID, loopback interface and routed port.

IP Address Mode: Displays the IP address allocation mode.

None: without ip.

Static: setup manually.

DHCP: allocated through DHCP.

IP Address: Displays the IP address and subnet mask of the interface.

Secondary IP: Displays the secondary IP address and subnet mask of the interface.

Interface Status: Displays the interface current working status, which is up when Admin Status is enable, line protocol is up and IP address is set.

Admin Status: Displays the Admin status. Choose '**Disable**' to disable the interface's Layer 3 capabilities.

- **Interface Setting Detail Information**

Displays the detailed setting information of the interface.

10.2 Routing Table

This page displays the routing information summary generated by different routing protocols.

Choose the menu **Routing** → **Routing Table** → **Routing Table** to load the following page.

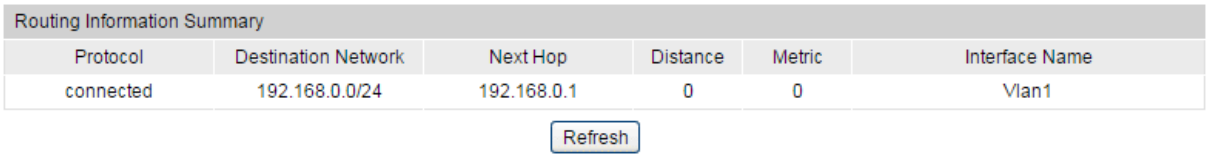


Figure 10-4 Routing Table

- **Routing Information Summary**

Protocol Displays the protocol of the route.

Destination Network: Displays the destination and subnet of the route.

Next Hop: Displays the IP address to which the packet should be sent next.

Distance: Displays the administrative distance which is a rating of the trustworthiness of a routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route which has the smallest distance will be recorded in the IP routing table.

Metric: Displays the metric of the route.

Interface name: Displays the description of the egress interface.

10.3 Static Routing

Static routes are special routes manually configured by the administrator and cannot change automatically with the network topology accordingly. Hence, static routes are commonly used in a relative simple and stable network. Proper configuration of static routes can greatly improve network performance.

10.3.1 Static Routing

Choose the menu **Routing** → **Static Routing** → **Static Routing Config** to load the following page.

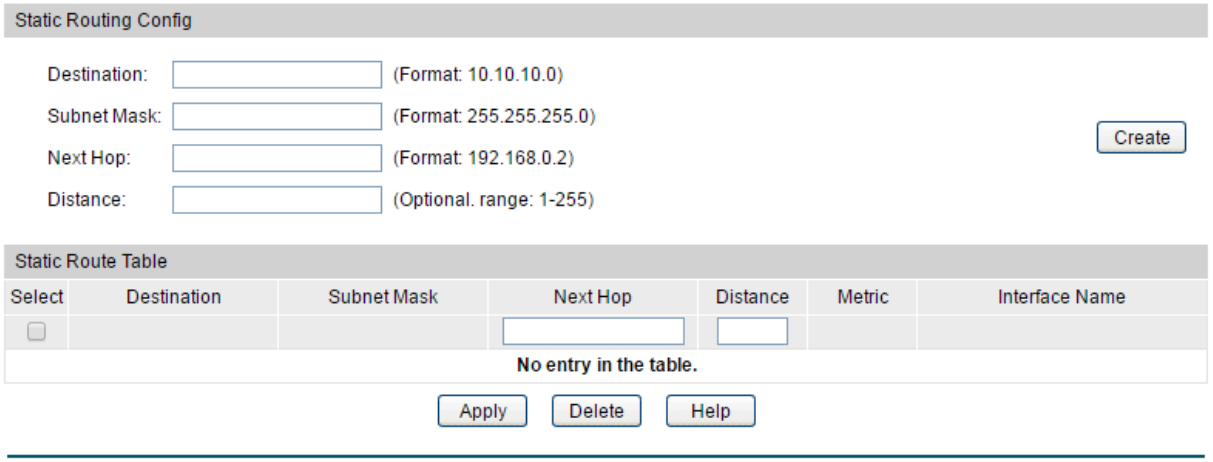


Figure 10-5 Static Routing Config

Configuration Procedure:

1) In the **Static Routing Config** section, configure corresponding parameters to add a static route. Then click **Create**.

2) In the **Static Route Table** section, you can view the corresponding interface entry you create.

Entry Description:

- **Static Routing Config**

  Destination: Specify the destination IP address of the packets.

  Subnet Mask: Specify the subnet mask of the destination IP address.

  Next Hop: Enter the IP address to which the packet should be sent next.

  Distance: Specify the administrative distance which is a rating of the trustworthiness of a routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route which has the smallest distance will be recorded in the IP routing table.

- **Static Route Table**

  Select: Specify the static route entries to modify.

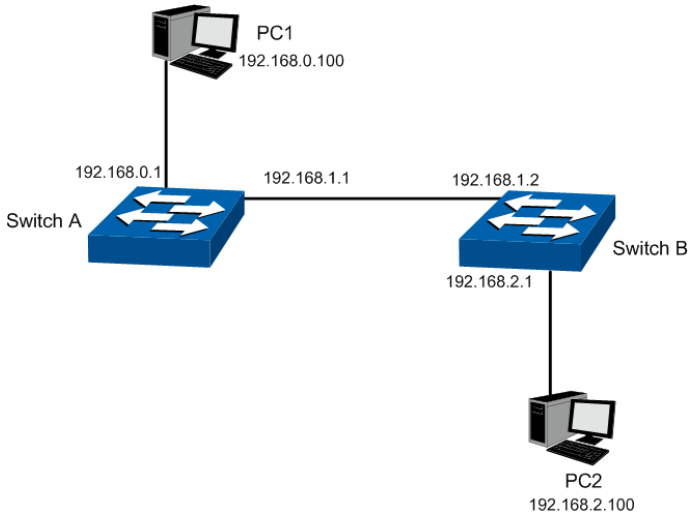
Destination Address:	Displays the destination IP address of the packets.
Subnet Mask:	Displays the subnet mask of the destination IP address.
Next Hop:	Displays the IP address to which the packet should be sent next.
Distance:	Specify the administrative distance which is a rating of the trustworthiness of a routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route which has the smallest distance will be recorded in the IP routing table.
Metric:	Displays the metric of the route.
Interface Name:	Displays the name of the VLAN interface.

10.3.2 Application Example for Static Routing

➢ **Network Requirements**

- A small enterprise network is divided into three VLANs: VLAN10, VLAN20 and VLAN30. Their VLAN IDs are 10, 20 and 30 respectively.
- PC1 is in VLAN10 and PC2 is in VLAN30. PC1 and PC2 are reachable for each other.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch A

Steps	Operation	Note
1	Add interface VLAN 10	Required. On page **Routing→Interface→Interface Config**, add interface VLAN 10 with the mode as static, the IP address as 192.168.0.1, the mask as 255.255.255.0 and the interface name as VLAN10.

2	Add interface VLAN 20	Required. On page **Routing→Interface→Interface Config**, add interface VLAN 20 with the mode as static, the IP address as 192.168.1.1, the mask as 255.255.255.0 and the interface name as VLAN20.
3	Add static route entry	Required. On page **Routing→Static Routing→Static Routing Config**, add a static route entry with the destination as 192.168.2.0, the subnet mask as 255.255.255.0 and the next hop as 192.168.1.2.

- Configure Switch B

Steps	Operation	Note
1	Add interface VLAN 20	Required. On page **Routing→Interface→Interface Config**, add interface VLAN 20 with the mode as static, the IP address as 192.168.1.2, the mask as 255.255.255.0 and the interface name as VLAN20.
2	Add interface VLAN 30	Required. On page **Routing→Interface→Interface Config**, add interface VLAN 30 with the mode as static, the IP address as 192.168.2.1, the mask as 255.255.255.0 and the interface name as VLAN30.
3	Add static route entry	Required. On page **Routing→Static Routing→Static Routing Config**, add a static route entry with the destination as 192.168.0.0, the subnet mask as 255.255.255.0 and the next hop as 192.168.1.1.

- Configure the PCs

Configure the default gateway of PC1 as 192.168.0.1 and the default gateway of PC2 as 192.168.2.1.

10.4 DHCP Server

DHCP module is used to configure the DHCP functions of the switch, including two submenus, **DHCP Server** and **DHCP Relay**.

➢ **Overview**

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP is adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of DHCP participants so the administrator can manage the parameters of the host in the network.

As workstations and personal computers proliferate on the Internet, the administrative complexity of maintaining a network is increased by an order of magnitude. The assignment of local network resources to each client represents one such difficulty. In most environments,

delegating such responsibility to the user is not plausible and, indeed, the solution is to define the resources in uniform terms, and to automate their assignment.

The DHCP dealt with the issue of assigning an internet address to a client, as well as some other resources.

➢ **DHCP Elements**

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to DHCP clients. Generally a DHCP server can allocate configuration parameters to more than one client. Figure 10-6 shows you the model.

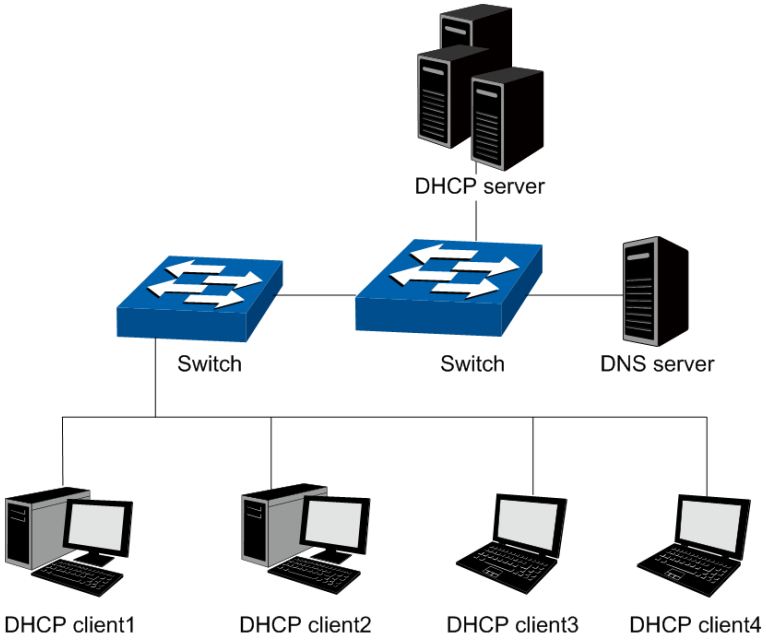


Figure 10-6 DHCP model

To meet the different requirements of DHCP clients, DHCP server is always designed to supply hosts with the configuration parameters in three policies.

1) Manual Assignment: For the specific DHCP clients (e.g., web server), the configuration parameters are manually specified by the administrator and are assigned to these clients via a DHCP server.

2) Automatic Assignment: The DHCP server must supplies the configuration parameters to DHCP client with the lease time continued for ever.

3) Dynamic Assignment: A network administrator assigns a range of IP addresses to DHCP server, and each client computer on the LAN is configured to request an IP address from the DHCP server with a fixed period of time (e.g., 2 hours), allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.

➢ **The Process of DHCP**

DHCP uses UDP as its transport protocol. DHCP messages from a client to a server are sent to the 'DHCP server' port (67), and DHCP messages from a server to a client are sent to the 'DHCP client' port (68). DHCP clients and servers both construct DHCP messages by filling in fields in the fixed format section of the message and appending tagged data items in the variable length option area. The process is shown as follows.

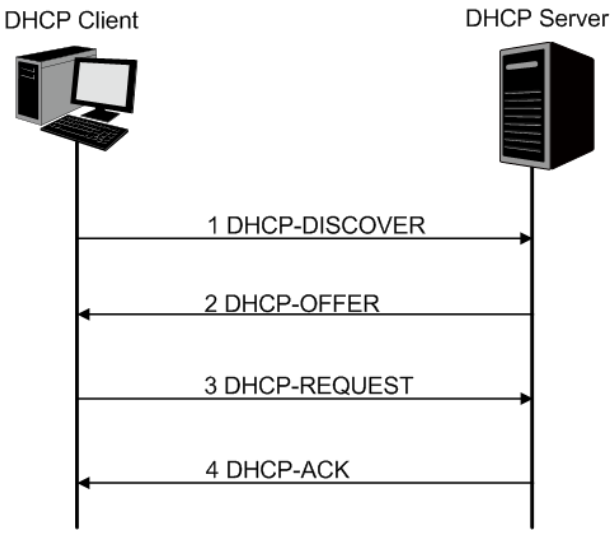


Figure 10-7 The Process of DHCP

1) DHCP discover: the client broadcasts messages on the physical subnet to discover available DHCP servers in the LAN. Network administrators can configure a local router (e.g. a relay agent) to forward DHCP-DISCOVER messages to a DHCP server in a different subnet.

2) DHCP offer: Each server who received the DHCP-DISCOVER message may respond a DHCP-OFFER message that includes configuration parameters (in the example below, IP address) to the client. The server unicast the DHCP-OFFER message to the client (using the DHCP/BOOTP relay agent if necessary) if possible, or may broadcast the message to a broadcast address on the client's subnet.

3) DHCP request: A client can receive DHCP offers from multiple servers, but it will accept only one DHCP-OFFER and broadcast a DHCP-REQUEST message which includes the server's identifier and the IP address offered by the server. Based on the server's identifier, servers are informed whose offer the client has accepted.

4) DHCP acknowledgement: The server selected in the DHCP-REQUEST message commits the binding for the client to persistent storage and responds with a DHCP-ACK message containing the configuration parameters for the requesting client. If the selected server is unable to satisfy the DHCP-REQUEST message (e.g., the requested IP address has been allocated), the server should respond with a DHCP-NAK message.

5) In Dynamic assignment policy, the DHCP client is assigned an IP address with a lease time (e.g. 2 hours) from the DHCP server. This IP address will be reclaimed by the DHCP server when its lease time expires. If the client wants to use the IP address continually, it should unicast a DHCP-REQUEST message to the server to extend its lease.

After obtaining parameters via DHCP, a host should be able to exchange packets with any other host in the networks.

➢ **The Format of DHCP Message**

Figure 10-6 DHCP model gives the process of DHCP and Figure 10-8 describes each field in the DHCP message. The numbers in parentheses indicate the size of each field in octets. The names for the fields given in the figure will be used throughout this document to refer to the fields in DHCP messages.

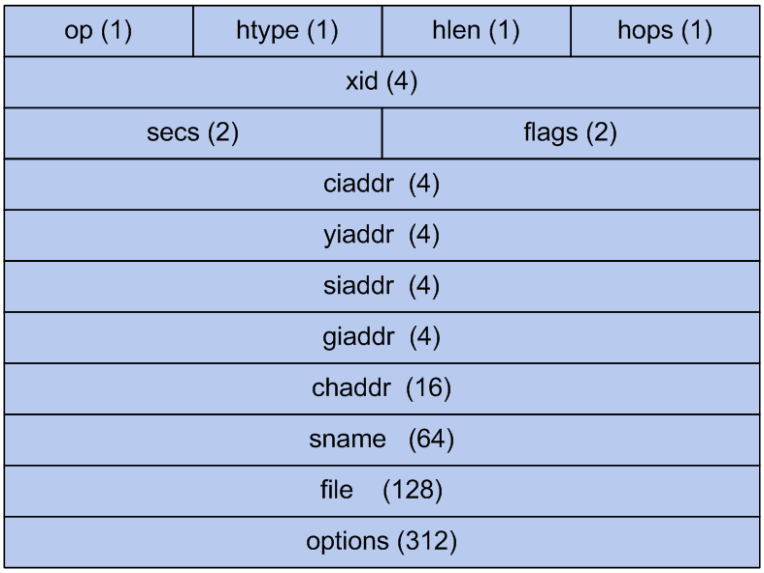


Figure 10-8 The Format of DHCP Message

1) op：Message type, '1' = BOOT-REQUEST, '2' = BOOT-REPLY.
2) htype：Hardware address type, '1' for ethernet.
3) hlen：Hardware address length, '6' for ethernet.
4) hops：Clients set this field to zero and broadcast the DHCP-REQUEST message , optionally used by relay-agents when booting via a relay-agent.
5) xid：Transaction ID, a random number chosen by the client, used by the client and server to associate messages.
6) secs：Filled in by client, seconds elapsed since client started trying to boot.
7) flags：A client that cannot receive unicast IP datagrams until its protocol software has been configured with an IP address should set the first bit in the 'flags' field to 1 in any DHCP-DISCOVER or DHCP-REQUEST message that client sends. A client that can receive unicast IP datagrams before its protocol software has been configured should clear the first bit to 0. A server or relay agent sending or relaying a DHCP message directly to a DHCP client should examine the first bit in the 'flags' field. If this bit is set to 1, the DHCP message should be sent as an IP broadcast and if the bit is cleared to 0, the message should be sent as an IP unicast. The remaining bits of the flags field are reserved for future use and must be set to zero by clients and ignored by servers and relay agents.
8) ciaddr：Client IP address, filled in by client in DHCPREQUEST when verifying previously allocated configuration parameters.
9) yiaddr：'your' (client) IP address, configuration parameters allocated to the client by DHCP server.
10) siaddr：IP address of next server to use in bootstrap, returned in DHCPOFFER, DHCPACK and DHCPNAK by server.
11) giaddr：Relay agent IP address, used in booting via a relay-agent.
12) chaddr：Client hardware address.
13) sname：Optional server host name, null terminated string.

14) file：Boot file name, null terminated string, "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER.

15) options：Optional parameters field. See the options documents (RFC 2132) for a list of defined options. We will introduce some familiar options in the next section.

➢ **DHCP Option**

This section defines a generalized use of the 'options' field for giving information useful to a wide class of machines, operating systems and configurations. Sites with a single DHCP server that is shared among heterogeneous clients may choose to define other, site-specific formats for the use of the 'options' field. Figure 10-9 gives the format of options field.

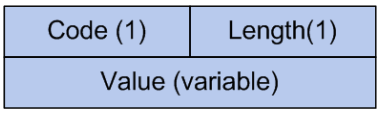


Figure 10-9 DHCP Option

All options begin with a Code octet, which uniquely identifies the option followed by the length octet. The value of the length octet does not include the Code and Length octets. The common options are illustrated as below.

1) option 1：Subnet Mask option. The subnet mask option is option1 which identifies the assigned IP address with network, and its length is 4 octets.

2) option 3：Router option. The router option is option 3 which specifies an IP address for routers on the client's subnet.

3) option 6：DNS option. The DNS option is option 6, and it assigns the IP address of domain name server to the client which allows the client can use the web service in the internet.

4) option 12：Host Name option. The option12 is used to specify the name of the client, which may be requested by the DHCP server for authentication.

5) option 50：Requested IP Address option. The option 50 is used in a DHCP-REQUEST message to allow the client to request the particular IP address.

6) option 51：Lease Time option. In DHCP-OFFER and DHCP-ACK message, the DHCP server uses this option to specify the lease time in which the clients can use the IP address legally.

7) option 53：Message Type option. This option is used to convey the type of the DHCP message. Legal values for this option show in Table 10-1:

Value	Message Type
1	DHCP-DISCOVER
2	DHCP-OFFER
3	DHCP-REQUEST
4	DHCP-DECLINE
5	DHCP-ACK
6	DHCP-NAK
7	DHCP-RELEASE
8	DHCP-INFORM

Table 10-1 Option 53

8) option 54：Server Identifier option. DHCP servers include option 54 in the DHCP-OFFER message in order to allow the client to distinguish between lease offers. DHCP clients use the option in a DHCP-REQUEST message to indicate which lease offers is being accepted.

9) option 55：Parameter Request List option. This option is used by a DHCP client to request values for specified configuration parameters.

10) option 61：Client hardware address.

11) option 66：TFTP server name option. This option is used to identify a TFTP server.

12) option 67：Boot-file name option. This option is used to identify a boot-file.

13) option 150：TFTP server address option. This option is used to specify the address of the TFTP server which assigns the boot-file to the client.

For particulars of DHCP option, please refer to RFC 2132. In the next section, DHCP Server and DHCP Relay function on this switch will be introduced in detail.

➢ **Application Environment of DHCP Server**

DHCP Server assigns IP address to the client efficiently in the following environment.

1) More and more device proliferates in the network, and it is a hard work to configure the IP parameter for every device manually.

2) There are not enough network resources to assign to every device exclusively.

3) Only a little device need static IP address to connect the network.

➢ **Details of DHCP Server on T3700G-52TQ**

A typical application of **T3700G-52TQ** working at DHCP Server function is shown below. It can be altered to meet the network requirement.

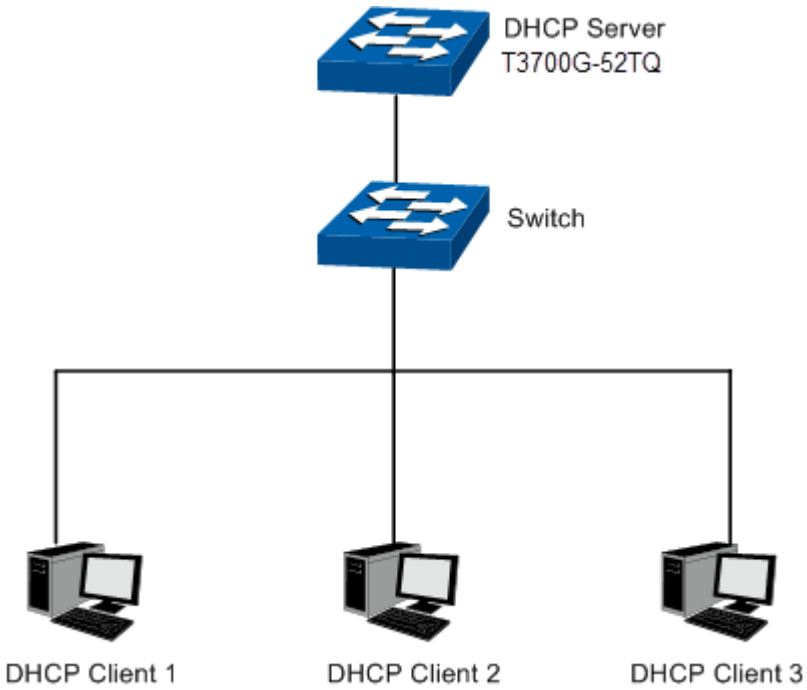


Figure 10-10 DHCP Server Application

To guarantee the process of assigning IP address fluency and in safety, and to keep the network run steadily, the DHCP Server function on T3700G-52TQ performs the following tasks.

- Create different IP pool for every VLAN. The device in different VLAN can get the IP address in different subnet.
- When receiving a DHCP-DISCOVER packet from the client, the switch judges the VLAN which the ingress port belong to, and chooses the IP in the same subnet with the VLAN interface to assign to the client.
- With a DHCP Relay running between the client and the server, when receiving a DHCP-DISCOVER packet transmitting from the Relay, the switch will choose the IP from the IP pool in the same subnet with the Relay's IP to assign to the client. If the IP pool is not configured on the switch or the configured IP pool doesn't match the Relay's network segment, the client may not get network parameters successfully.
- The switch can detect the IP address automatically before assigning it to avoid conflict.

➢ **IP Detection**

To avoid IP conflict, the switch will detect the IP address to be assigned in LAN through Ping test.

The DHCP server will send the Ping test packet with the destination IP being the IP address to be assigned. If the server receives the Reply packet from the destination host in the ping time, it means that the IP address has been used, and the server will choose another IP as destination IP to test again. The server will assign the IP address if the server not receives the Reply packet in the Ping time.

➢ **Policy of IP Assignment**

The switch chooses the IP assigned to clients based on the rules shown as follows.

1) First, the server will choose the IP which has been bound to the client manually.
2) Then, the server will assign the IP which has been assigned to the client once.
3) For the next, the server will assign the IP which is specified in the DHCP-DISCOVER packet from the client.
4) At last, the server will choose the first IP from the IP pool which has not been assigned.

➢ **Tips for Configure DHCP Server Function on T3700G-52TQ**

1) Configure the Excluded IP address which cannot be assigned by the switch, e.g. web server's IP, broadcast IP of subnet and gateway's IP.
2) Specify IP address for specific clients, and then the switch will supply these IP address to them only for ever.
3) Configure the IP pool in which the IP address can be assigned to the clients.

The DHCP Server, allowing the clients in all VLANs to get the IP address from the server automatically, is implemented on the **DHCP Server**, **Pool Setting**, **DHCP Options Set**, **Binding Table** and **Packet Statistics** pages.

10.4.1 DHCP Server

This page allows you to enable the DHCP Server function, configure the Excluded IP Address which cannot be assigned by the switch in every network.

Choose the menu **Routing→DHCP Server→DHCP Server** to load the following page.

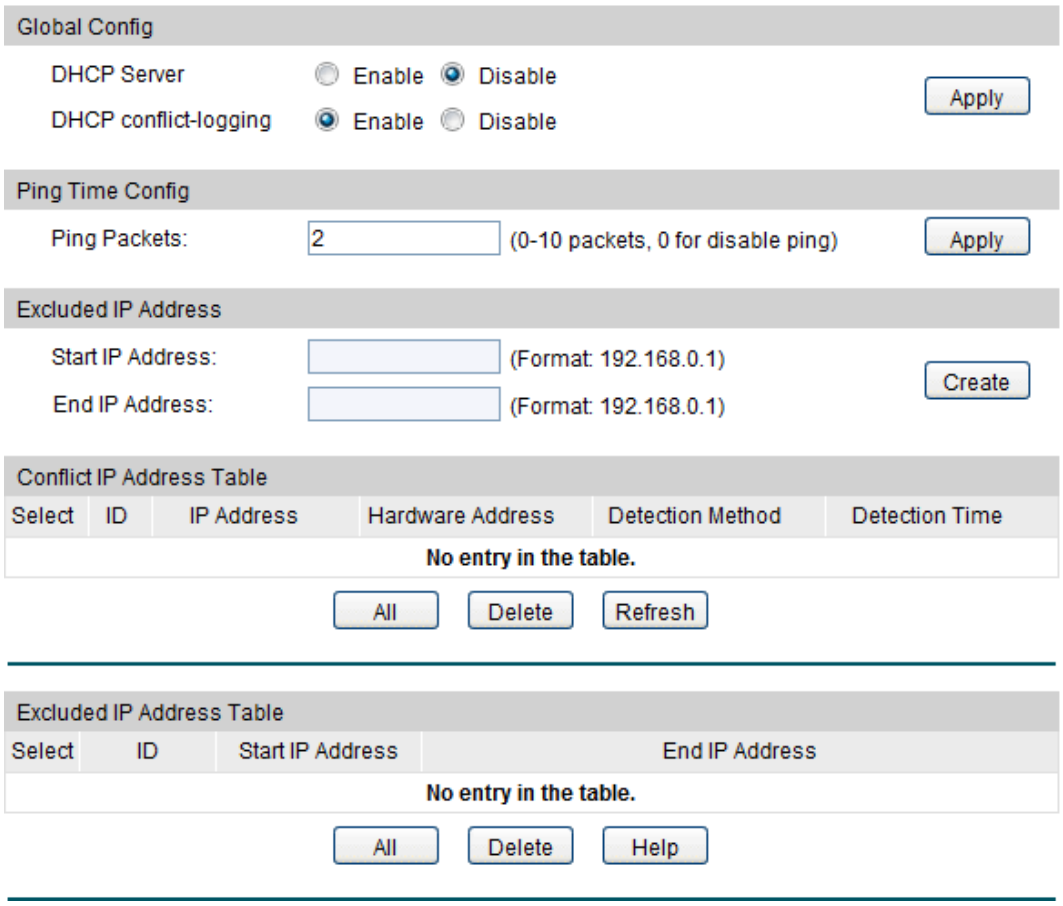


Figure10-11 DHCP Server

Configuration Procedure:

1) In the **Global Config** section, enable or disable DHCP Server and DHCP Conflict-logging. Then click **Apply**.
2) In the **Ping Time Config** section, configure Ping Packets for ping tests. Click **Apply**.
3) In the **Excluded IP Address** section, enter the **Start IP Address** and **End IP Address** to specify the range of reserved IP addresses. Click **Create**.
4) In the **Conflict IP Address Table** section, you can view the list of the IP addresses that should not be assigned to DHCP clients for ping conflict checked.
5) In the **Excluded IP Address Table** section, you can view the list of the IP addresses that should not be assigned to DHCP clients.

Entry Description:

- **Global Config**

DHCP Server:	Enable or disable DHCP Server. By default, it is disabled.
DHCP Conflict-logging:	Enable or disable DHCP Conflict-logging. By default, it is enabled.

➢ **Ping Time Config**

Ping Packets: The number of packets to be sent.

➢ **Excluded IP Address**

Start IP Address: The first one of the IP addresses that should not be assigned.

End IP Address: The last one of the IP addresses that should not be assigned.

10.4.2 Pool Setting

This page shows you how to configure the IP pool in which the IP address can be assigned to the clients in the network.

Choose the menu **Routing→DHCP Server→Pool Setting** to load the following page.

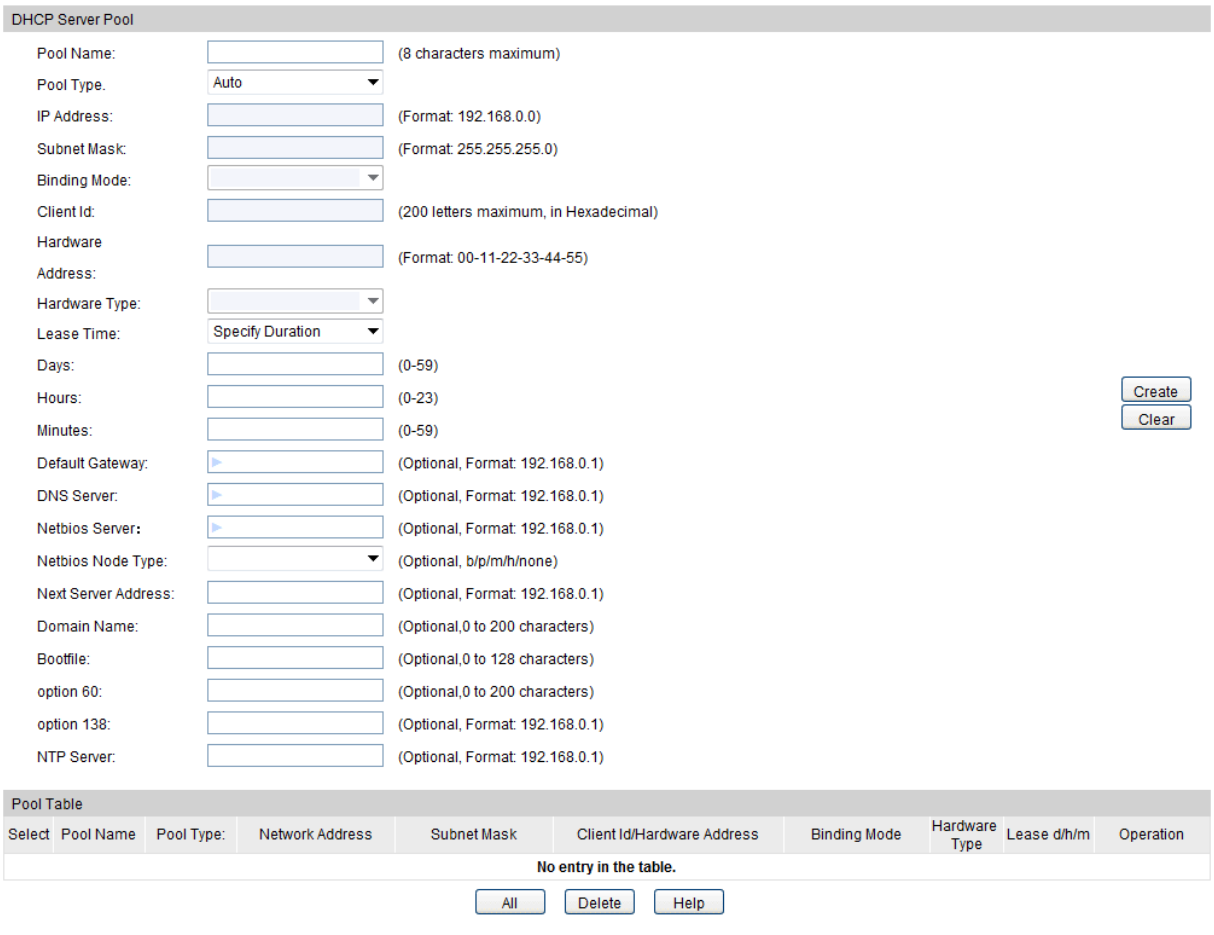


Figure 10-12 Pool Setting

Configuration Procedure:

1) Enter the pool name and choose the pool type.

2) Configure the pool parameters according to your actual needs. Click **Create**.

Entry Description:

Pool Name: Specify a pool name for identification.

Pool Type:	Specify the pool type.
IP Address:	Specify the IP address to be bound.
Subnet Mask:	Specify the corresponding subnet mask of the IP address in the pool.
Binding Mode:	Select a binding mode: **Client Id**: Bind the IP address to the client ID. **Client Id in ASCii**: Bind the IP address to the client ID in ASCII format. **Hardware Address**: Bind the IP address to the MAC address of the client.
Client ID:	If you select Client ID as the binding mode, enter the client ID in this field.
Hardware Address:	If you select Hardware Address as the binding mode, enter the MAC address in this field.
Hardware Type:	If you select Hardware Address as the binding mode, select a hardware type. The hardware type includes Ethernet and IEEE802.
Lease Time:	Specify the lease time of IP addresses in the pool.
Days:	Specify the days of the lease time of IP addresses in the pool.
Hours:	Specify the hours of the lease time of IP addresses in the pool.
Minutes:	Specify the minutes of the lease time of IP addresses in the pool.
Default Gateway:	Specify the IP address of the default gateway for a client.
DNS Server:	Specify the IP address of the DNS server for a client.
Netbios Server：	Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses.

Netbios Node Type:	Specify the Netbios type for the clients, which is the way of inquiring IP address resolution. The following options are provided: b-node Broadcast: The client sends query message via broadcast. p-node Peer-to-Peer: The client sends query message via unicast. m-node Mixed: The client sends query message via broadcast first. If it fails, the client will try again via unicast. h-node Hybrid: The client sends query message via unicast first. If it fails, the client will try again via broadcast.
Next Server Address:	Specify the IP address of a TFTP server for the clients. If needed, the clients can get the configuration file from the TFTP server for auto installation.
Domain Name:	Specify the domain name that the clients should use when resolving host names via DNS.
Bootfile:	Specify the name of the bootfile. If needed, the clients can get the bootfile from the TFTP server for auto installation.
option 60:	Specify the option 60 for device identification. Mostly it is used under the scenario where the APs (Access Points) apply for different IP addresses from different servers according to the needs. If an AP requests option 60, the server will respond a packet containing the option 60 configured here. And then the AP will compare the received option 60 with its own. If they are the same, the AP will accept the IP address assigned by the server, otherwise the assigned IP address will not be accepted. .
option 138:	Specify the option 138, which can be configured as the management IP address of an AC (Access Control) device. If the APs in the local network request this option, the server will respond a packet containing this option to inform the APs of the AC's IP address.
NTP Server:	Specify the Network Time Protocol Server for a client.

10.4.3 DHCP Options Set

Choose the menu **Routing→DHCP Server→DHCP Options Set** to load the following page.

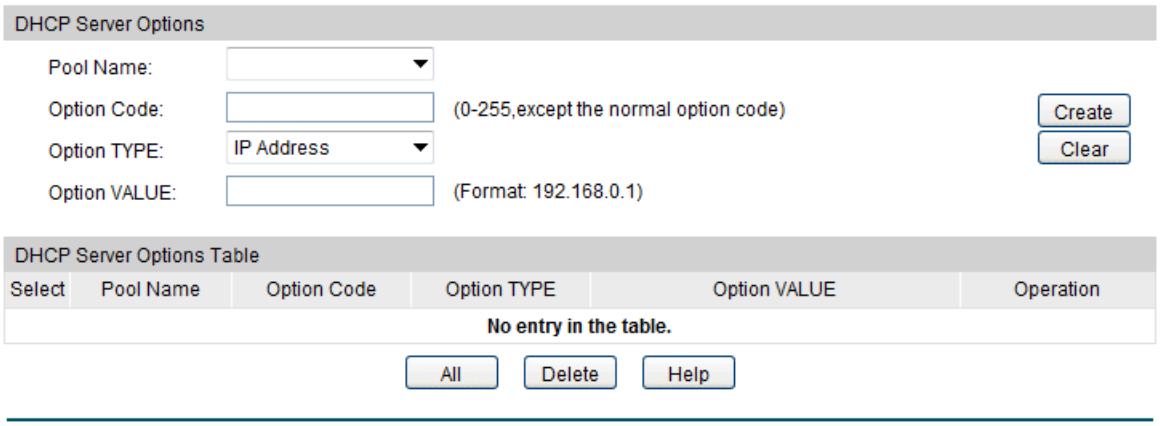


Figure 10-13 Manual Binding

Configuration Procedure:

1) Select a DHCP server pool from the drop-down list.

2) Configure the extend option in the pool according to your actual needs.

3) Click **Create**.

Entry Description:

Pool Name:	Select the IP Pool containing the IP address to be bound.
Option Code:	Specify the extend option code.
Option TYPE:	Specify the extend option type.
Option VALUE:	Specify the extend option value.

10.4.4 Binding Table

Choose the menu **Routing→DHCP Server→Binding Table** to load the following page.

Figure 10-14 DHCP Server Binding Table

Configuration Procedure:

View the information about the clients attached to the server.

Entry Description:

ID:	Displays the ID of the client.
IP Address:	Displays the IP address that the switch has allocated to the client.
Client ID / Hardware Address:	Displays the MAC address of the client.

Type:	Displays the type of this binding entry.
Lease Time Left(s):	Displays the lease time of the client left.

10.4.5 Packet Statistics

Choose the menu **Routing→DHCP Server→Packet Statistics** to load the following page.

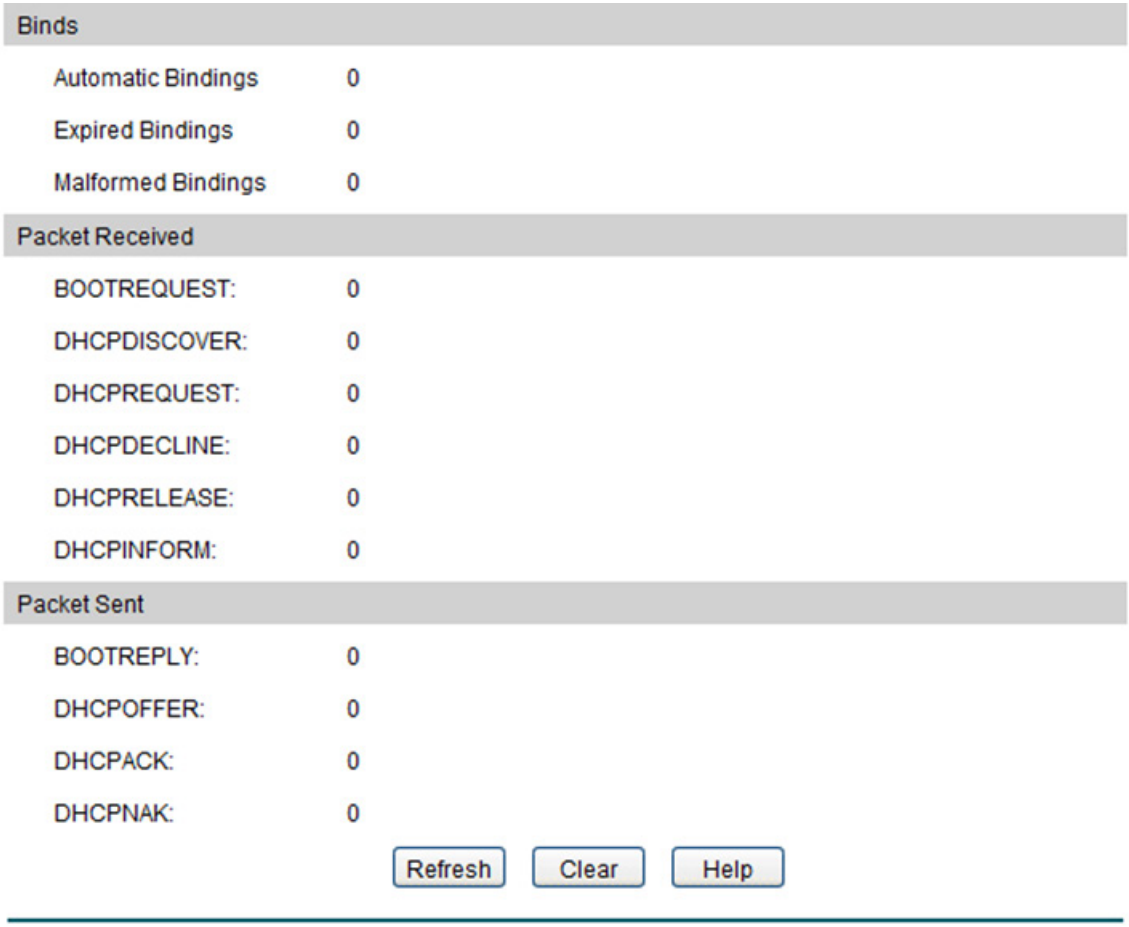


Figure10-15 Statistics

Configuration Procedure:

View the DHCP packets the switch received or sent.

Entry Description:

- **Binds**

Automatic Bindings:	Displays the DHCP Server auto bindings.
Expired Bindings:	Displays the DHCP Server expired bindings.
Malformed Bindings:	Displays the DHCP Server malformed binding.

- **Packets Received**

BOOTREQUEST:	Displays the Bootp Request packet received.
DHCPDISCOVER:	Displays the Discover packet received.

DHCPREQUEST: Displays the Request packet received.

DHCPDECLINE: Displays the Decline packet received.

DHCPRELEASE: Displays the Release packet received.

DHCPINFORM: Displays the Inform packet received.

➢ **Packets Sent**

BOOTREPLY: Displays the Bootp Reply packet sent.

DHCPOFFER: Displays the Offer packet sent.

DHCPACK: Displays the Ack packet sent.

DHCPNAK: Displays the Nak packet sent.

Configuration Procedure (using VLAN interface as an example):

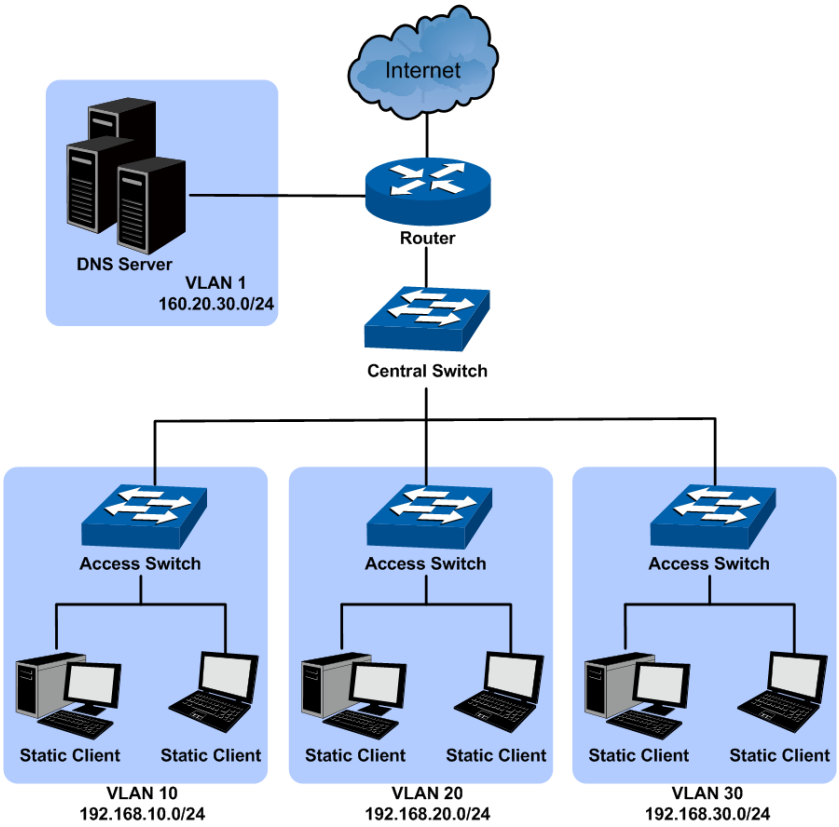
Step	Operation	Description
1	Set the link type for port.	Required. On the **VLAN→802.1Q VLAN→Port Config** page, set the link type for the port basing on its connected device.
2	Create VLAN.	Required. On the **VLAN→802.1Q VLAN→VLAN Config** page, click the **Create** button to create a VLAN. Enter the VLAN ID and the description for the VLAN. Meanwhile, specify its member ports.
3	Create VLAN interface.	Required. On the **Routing→Static Routing→Static Routing Config** page, create the interface IP address of the VLAN.
4	Enable DHCP Server.	Required. On the **Routing→DHCP Server→DHCP Server** page, enable the DHCP Server function.
5	Configure Excluded IP Address.	Optional. On the **Routing→DHCP Server→DHCP Server** page, configure the Excluded IP Address which cannot be assigned by the switch.
6	Configure IP Pool.	Required. On the **Routing→DHCP Server→Pool Setting** page, configure the parameters of IP Pool.

10.4.6 Application Example for DHCP Server and Relay

➢ **Network Requirements**

- Every building in the campus belongs to separate VLANs with different network segments.
- The access points in each building are divided into two parts. One part is the fixed computers with static IP addresses in the teachers' offices; the other is the classroom, in which most clients are laptops with dynamic IP addresses obtained from the DHCP server.
- DNS Server is in VLAN 1 and its IP address is 160.20.30.2.

➢ **Network Diagram**



Use T3700G-52TQ as the central switch and enable its DHCP server function to allocate IP addresses to clients in the network. Enable the DHCP relay function on each access switch in VLAN 10, 20 and 30. For details about DHCP relay, please refer to 10.5 DHCP Relay.

➢ **Configuration Procedure**

- Configure Central Switch

Step	Operation	Note
1	Create VLAN	Required. On page **VLAN→802.1Q VLAN→VLAN Config**, create VLAN10, VLAN20 and VLAN30, and configure their ports.
2	Create VLAN interface	Required. On page **Routing→Interface→Interface Config**, configure VLAN interface 192.168.10.1/24 for VLAN10, 192.168.20.1/24 for VLAN20, and 192.168.30.1 for VLAN30.
3	Enable DHCP Server	Required. On page **Routing→DHCP Server→DHCP Server**, enable DHCP Server function under the Global Config.
4	Configure the IP address pool	Required. On page **Routing→DHCP Server→Pool Setting**, configure IP address pool parameters for each VLAN interface. Take VLAN10 as an example, configure its Network Address as 192.168.10.0, Subnet Mask as 255.255.255.0, Default gateway as 192.168.10.1 (the IP address of the VLAN interface), DNS Server as 160.20.30.2,customize the Pool Name, Lease Time and other parameters.

Step	Operation	Note
5	Configure the reserved addresses	Required. On page **Routing→DHCP Server→DHCP Server**, under the Excluded IP Address, configure reserved IP addresses for the fixed computers in each VLAN.

- Configure Access Switch

Step	Operation	Note
1	Enable DHCP Relay.	Required. On the **Routing→DHCP Server→Global Config** page, **enable** the DHCP Server function, and the DHCP Relay function will be enabled at the same time.
2	Configure Option 82 support.	Optional. On the **Routing→DHCP Relay→Global Config** page, configure the Option 82 parameters.
3	Configure DHCP Server.	Required. On the **Routing→DHCP Relay→DHCP Server** page, specify the DHCP Server with the IP address of the central switch.

10.5 DHCP Relay

➢ **Application Environment of DHCP Relay**

In DHCP model, DHCP clients broadcast its DHCP request, so the DHCP sever and clients must be on the same subnet, which require the DHCP server is available in every subnet. It is costly to build so much DHCP Server. DHCP relay agent solves the problem. Via a relay agent, DHCP clients request an IP address from the DHCP server in another subnet, and DHCP clients in different subnets can share the same DHCP server in the internet.

➢ **Details of DHCP Relay on T3700G-52TQ**

A typical application of T3700G-52TQ working at DHCP Relay function is shown below. It can be altered to meet the network requirement.

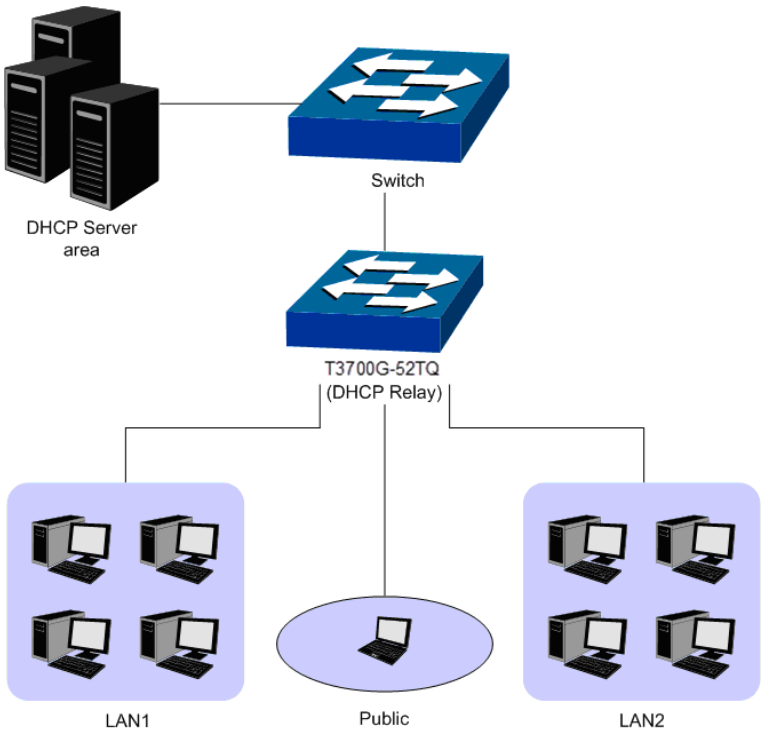


Figure 10-16 DHCP Relay Application

To allow all clients in different VLAN request IP address from one server successfully, the DHCP Relay function can transmit the DHCP packet between clients and server in different VLANs, and all clients in different VLANs can share one DHCP Server.

- When receiving DHCP-DISCOVER and DHCP-REQUEST packets, the switch will fill the giaddr field with the interface IP of the receiving port, optionally insert the option 82 information, and then forward the packet to the server.
- When receiving DHCP-OFFER and DHCP-REQUEST packets from the server, the switch will delete the option 82 information and forward the packet to the interface which receives the request.

The process will be shown as follows.

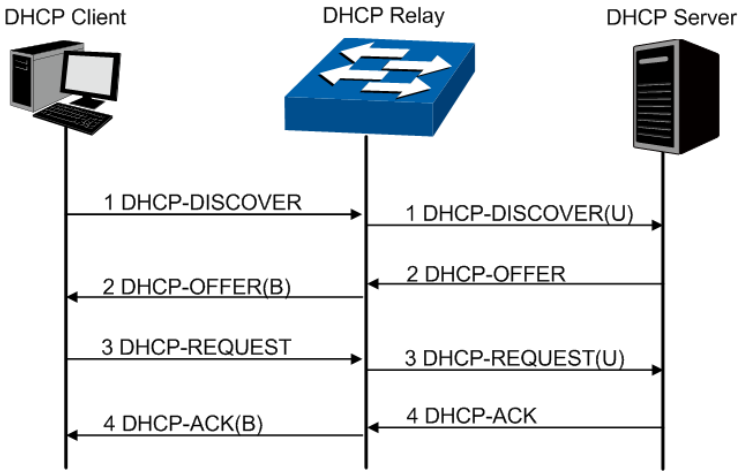


Figure 10-17 DHCP Relay Process

➢ **DHCP Relay Configuration**

1) Configure the Option 82 parameters to record the information of the clients. You are suggested to configure the option82 on the nearest Relay of the client.

2) Specify the DHCP Server which assigns IP addresses actually.

➢ **Option 82**

On this switch, Option 82 is used to record the location of the DHCP Client, the ethernet port and the VLAN, etc. Upon receiving the DHCP-REQUEST packet, the switch adds the Option 82 field to the packet and then transmits the packet to DHCP Server. The Server can be acquainted with the location of the DHCP Client via Option 82, so as to locate the DHCP Client, and assign the distribution policy of IP addresses and the other parameters for fulfilling the security control and account management of the client.

Option 82 can contain 255 sub-options at most. If Option 82 is defined, at least one sub-option should be defined. This Switch supports two sub-options, Circuit ID and Remote ID. Since there is no universal standard about the content of Option 82, different manufacturers define the sub-options of Option 82 to their need. For this Switch, the sub-options are defined as follows:

The Circuit ID is defined to be the number and VLAN of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of DHCP Relay device which receives the DHCP Request packets from DHCP Clients. Furthermore these two parameters also can be manually configured.

The format of Option 82 defined on the switch by default is given in the following figure. The numbers in parentheses indicate the size of each field in octets. By default, sub-option1 is Circuit ID option recording the VLAN and ethernet port information, while sub-option2 is Remote ID option recording the MAC address information of the client. You can define the sub-options manually.

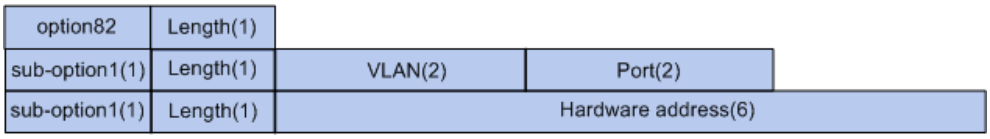


Figure10-18 Option 82

Note:

The option 82 parameters configured on the switch should base on and meet the requirement of the network.

The DHCP Relay, allowing the clients to get the IP address from the server in another subnet, is implemented on the **DHCP Relay** page. When the DHCP Server is enabled, the DHCP Relay will be enabled too.

10.5.1 Global Config

This page allows you to enable the DHCP Relay function.

Choose the menu **Routing→DHCP Relay→Global Config** to load the following page.

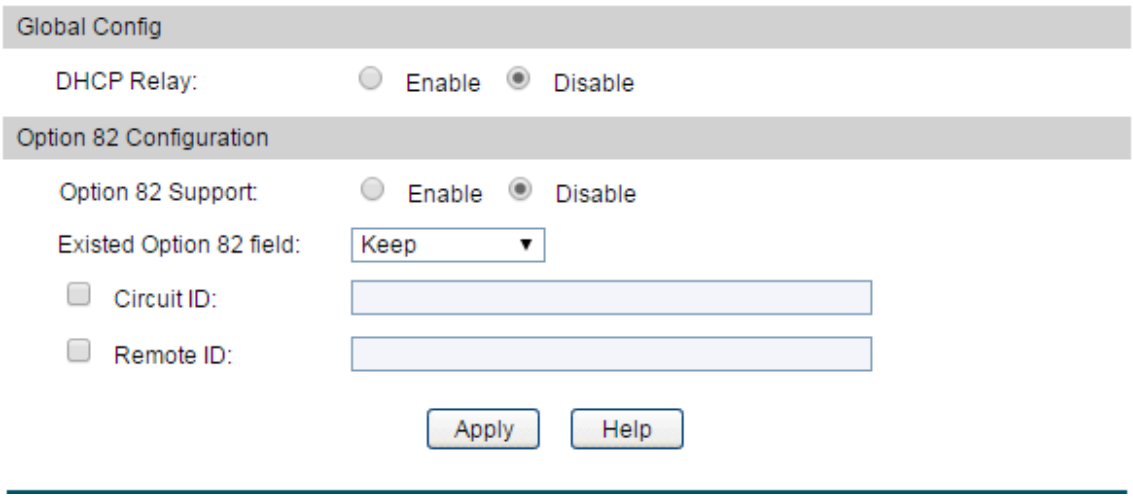


Figure 10-19 Global Config

Configuration Procedure:

1) In the **Global Config** section, enable DHCP Relay.
2) (Optional) In the **Option 82 Configuration** section, configure Option 82.
3) Click **Apply**.

Entry Description:

DHCP Relay: Enable or disable DHCP Relay.

Option 82 Support: Select whether to enable Option 82 or not. By default, it is disabled. Option 82 is used to record the locations of the DHCP client, its Ethernet port and the VLAN, etc. If you need to record the accurate location of a client, you can enable Option 82 on the relay device closest to the client.

Existed Option 82 Field: Select the operation for the Option 82 field of the DHCP request packets.

Keep: Indicates keeping the Option 82 field of the packets.

Replace: Indicates replacing the Option 82 field of the packets with the switch defined one. By default, the Circuit ID is defined to be the VLAN and the number of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of the DHCP Relay device which receives the DHCP Request packets.

Drop: Indicates discarding the packets that include the Option 82 field.

Circuit ID: Enter the customized circuit ID, which contains up to 32 characters. The circuit ID configurations of the switch and the DHCP server should be compatible with each other.

Remote ID: Enter the customized remote ID, which contains up to 32 characters. The remote ID configurations of the switch and the DHCP server should be compatible with each other.

10.5.2 DHCP Server

This page enables you to configure DHCP Servers on the specified interface.

Choose the menu **Routing→DHCP Relay→DHCP Server** to load the following page.

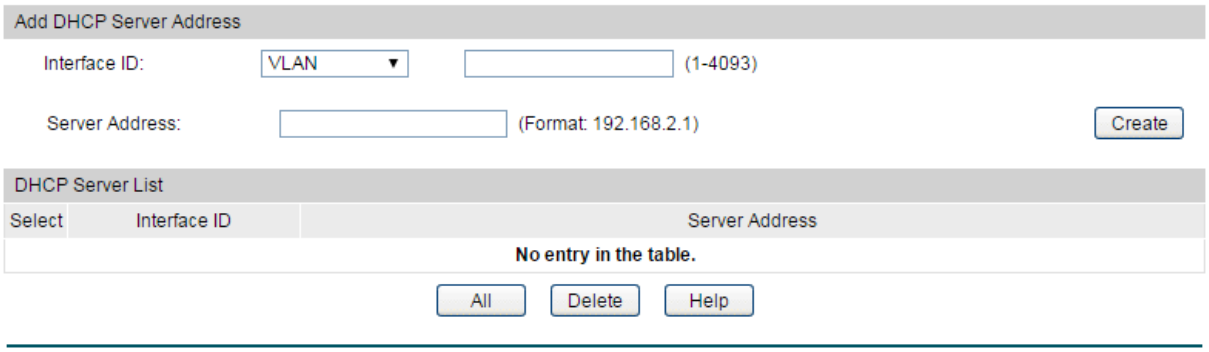


Figure 10-20 DHCP Server

Configuration Procedure:

1) In the **Add DHCP Server Address** section, select the interface type and enter the interface ID, and then enter the server address of the interface.
2) Click **Create** to specify the DHCP server for the interface.

Entry Description:

- **Add DHCP Server Address**

  Interface ID: Select the interface type and enter the interface ID.

  Server Address: Enter the DHCP server IP address.

- **DHCP Server List**

  Select: Select the desire DHCP server item.

  Interface ID: Displays the interface ID.

  Server Address: Displays the DHCP server address.

Configuration Procedure:

Step	Operation	Description
1	Enable DHCP Relay.	Required. On the **Routing→DHCP Relay→Global Config** page, **enable** DHCP Relay function.
2	Configure Option 82 support.	Optional. On the **Routing→DHCP Relay→Global Config** page, configure the Option 82 parameters.

3	Configure DHCP Server.	Required. On the **Routing→DHCP Relay→DHCP Server** page, specify the DHCP Server with IP address.

10.6 Proxy ARP

Proxy ARP functions to realize the Layer 3 connectivity between the hosts within the same network segment but isolated at Layer 2.

When an ARP request of a host is to be forwarded to another host in the same network segment but isolated at Layer 2, to realize the connectivity, the device connecting the two virtual networks should be able to respond to this request. This can be achieved by the device running proxy ARP.

Within the same network segment, hosts connecting with different layer 3 ports can communicate with each other through Layer 3 forwarding by using proxy ARP function. The following example simply illustrates how proxy ARP works.

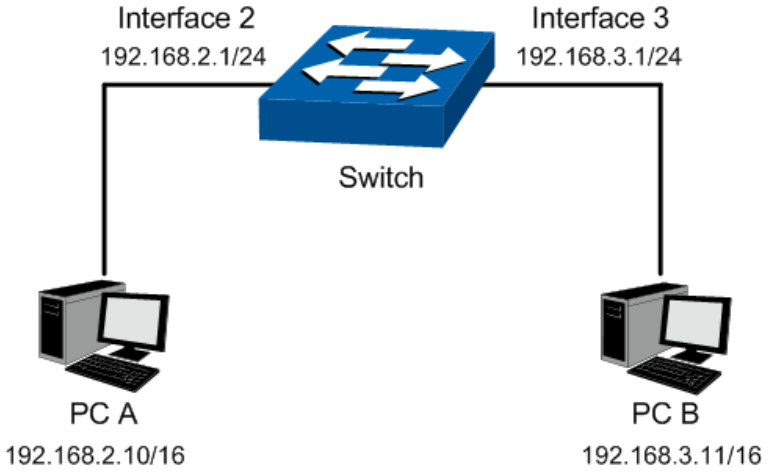


Figure 10-21 ARP Application

Within the same network segment, hosts connecting with the same layer 3 port can communicate with each other through Layer 3 forwarding by using local proxy ARP function. The following example simply illustrates how local proxy ARP works.

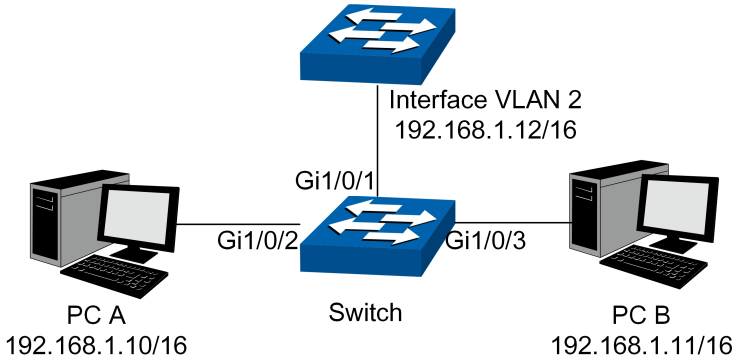


Figure 10-22 Local ARP Application

10.6.1 Proxy ARP

On this page you can enable Proxy ARP function for the layer 3 port.

Choose the menu **Routing→Proxy ARP→Proxy ARP** to load the following page.

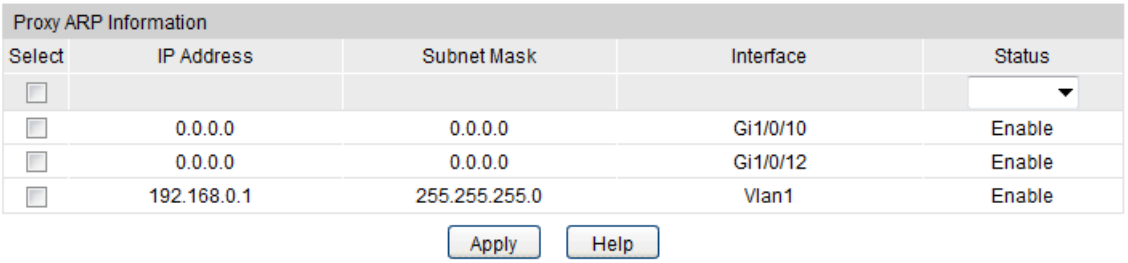


Figure 10-22 Proxy ARP

Configuration Procedure:

Enable Proxy ARP for the VLAN interface or routed port.

Entry Description:

IP Address/ Subnet Mask:	Displays the IP Address and Subnet Mask of the VLAN interface or routed port.
Interface:	Displays the VLAN interface ID of the VLAN interface or the port number of the routed port.
Status:	Enable or disable Proxy ARP

10.6.2 Local Proxy ARP

On this page you can enable Local Proxy ARP function for the layer 3 port.

Choose the menu **Routing→Proxy ARP→Local Proxy ARP** to load the following page.

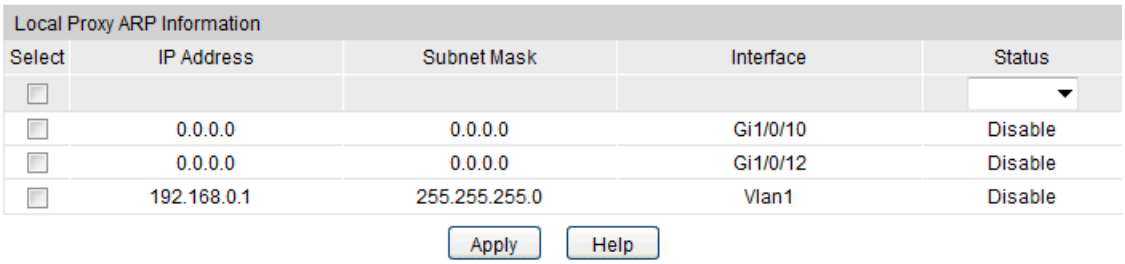


Figure 10-22 Proxy ARP

Configuration Procedure:

Enable Local Proxy ARP for the VLAN interface or routed port.

Entry Description:

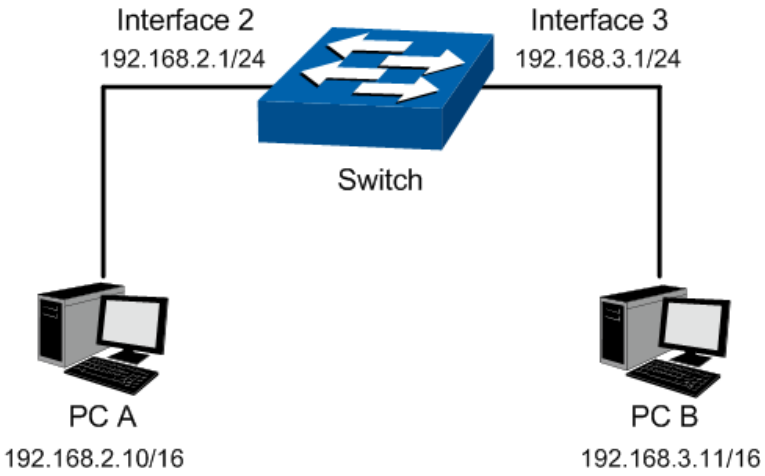
IP Address/ Subnet Mask:	Displays the IP Address and Subnet Mask of the VLAN interface or routed port.
Interface:	Displays the VLAN interface ID of the VLAN interface or the port number of the routed port.
Status:	Enable or disable Local Proxy ARP

10.6.3 Application Example for Proxy ARP

➢ **Network Requirements**

1. PC A and PC B are in the same network segment but belong to VLAN2 and VLAN3 respectively.
2. The IP address of PC A is 192.168.2.10/16 and the IP address of PC B is 192.168.3.11/16.
3. PC A and PC B can interconnect with each other by using Proxy ARP function.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure the Switch

Step	Operation	Description
1	Create VLAN	Required. On page **VLAN→802.1Q VLAN→VLAN Config**, create VLAN 2 and VLAN 3, and configure their ports.
2	Create VLAN Interface 2	Required. On **Routing→Interface→Interface Config** page, create VLAN Interface 2 with its IP address as 192.168.2.1, subnet mask as 255.255.255.0 and interface name as VLAN2.
3	Create VLAN Interface 3	Required. On **Routing→Interface→Interface Config** page, create VLAN Interface 3 with its IP address as 192.168.3.1, subnet mask as 255.255.255.0 and interface name as VLAN3.
4	Enable Proxy ARP	Required. On **Routing→Proxy ARP→Proxy ARP** page, enable Proxy ARP feature for VLAN interface 2 and VLAN interface 3.

10.7 ARP

This page displays the ARP table information and you can configure static ARP here.

10.7.1 ARP Table

Choose the menu **Routing** → **ARP** → **ARP Table** to load the following page.

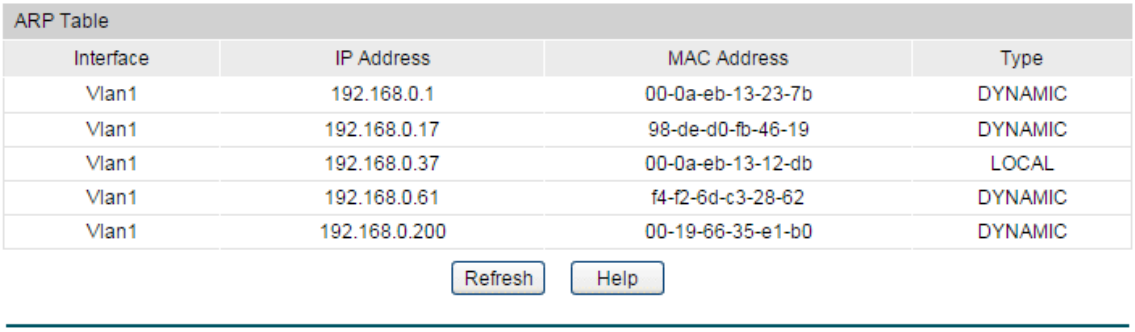


Figure 10-4 ARP Table

Configuration Procedure:

View all the dynamic and static ARP entries.

Entry Description:

Interface:	Displays the network interface of an ARP entry.
IP Address:	Displays the IP address of an ARP entry.
MAC Address:	Displays the MAC address of an ARP entry.
Type:	Displays the type of an ARP entry. **STATIC:** A static ARP entry that will always be remained. **DYNAMIC:** A dynamic ARP entry that will be deleted after aging time.

10.7.2 Static ARP

You can add desired static ARP entries by mannually specifying the IP addresses and MAC addresses.

Choose the menu **Routing** → **ARP** → **Static ARP** to load the following page.

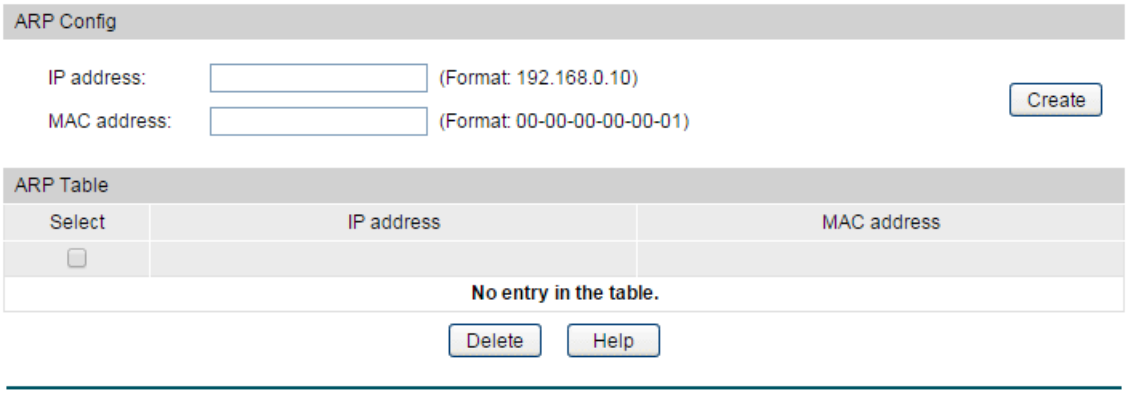


Figure 10-5 Static ARP

Configuration Procedure:

In the **ARP Config** section, enter the IP address and MAC address and click **Create**.

Entry Description:

- **ARP Config**

IP Address:	Specify the IP address of an ARP entry.
MAC Address:	Specify the MAC address of an ARP entry.

- **ARP Table**

Select:	Specify the static ARP entries to modify.
IP Address:	Displays the IP address of an ARP entry.
MAC Address:	Displays the MAC address of an ARP entry.

10.8 RIP

Note：

Router mentioned in this chapter refers to the traditional router or the switch running routing protocols.

RIP (Routing Information Protocol) is intended for use within the IP-based Internet. This protocol is most useful as an Interior Gateway Protocol (IGP). RIP was designed to work with moderate-size networks using reasonably homogeneous technology. Thus it is suitable as an IGP for many campuses and for regional networks using serial lines whose speeds do not vary widely. It is not intended for use in more complex environments.

RIP is a distance vector routing protocol, using UDP packets for exchanging information through port 520.

RIP uses “hop” to measure the distance to a destination. The hop count from a router to a directly connected network is 0. The hop count from a router to a directly connected router is 1. To limit convergence time, the range of RIP metric value is from 0 to 15. A metric value of 16 (or greater) is considered infinite, which means the destination network is unreachable. That is why RIP is not suitable for large-scaled networks.

RIP prevents routing loops by implementing the split horizon and poison reverse functions.

- **RIP routing table**

An RIP router has a routing table containing routing entries of all reachable destinations, and each routing entry contains:

- Destination address: IP address of a host or a network.
- Next hop: IP address of the adjacent router’s interface to reach the destination.
- Egress interface: Packet outgoing interface.
- Metric: Cost from the local router to the destination.
- Route time: Time elapsed since the routing entry was last updated. The time is reset to 0 every time the routing entry is updated.

- **RIP timers**

RIP employs three timers: update, timeout and garbage-collect.

- Update timer: defines the interval between routing updates.
- Timeout timer: defines the route aging time. If no update for a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- Garbage-collect: timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the garbage-collect timer expires, the route will be deleted from the routing table.

- **Routing loops prevention**

RIP is a distance vector (D-V) routing protocol. Since an RIP router advertises its own routing table to neighbors, routing loops may occur.

RIP uses the following mechanisms to prevent routing loops.

- Counting to infinity: The metric value of 16 is defined as unreachable. When a routing loop occurs, the metric value of the route will increment to 16.
- Split horizon: A router does not send the routing information learned from a neighbor to this neighbor to prevent routing loops and save bandwidth.
- Poison reverse: A router sets the metric of routes received from a neighbor to 16 and sends back these routes to the neighbor to help delete such information from the neighbor's routing table.
- Triggered updates: A router advertises updates once the metric of a route is changed rather than after the update period expires to speed up network convergence.

- **Operation of RIP**

The following procedure describes how RIP works.

1) After RIP is enabled, the router sends request messages to neighboring routers. Neighboring routers return Response messages including information about their routing tables.
2) After receiving such information, the router updates its local routing table, and sends triggered update messages to its neighbors. All routers on the network do the same to keep the latest routing information.
3) By default, an RIP router sends its routing table to neighbors every 30 seconds.
4) RIP ages out routes by adopting an aging mechanism to keep only valid routes.

- **RIP Version**

RIP has two versions, RIPv1 and RIPv2.

RIPv1, a classful routing protocol, supports message advertisement via broadcast only. RIPv1 protocol messages do not carry mask information, which means it can only recognize routing information of natural networks such as Class A, B, and C. That is why RIPv1 does not support discontinuous subnets.

RIPv2 is a classless routing protocol. Compared with RIPv1, RIPv2 has the following advantages.

- Supporting route tags. Route tags are used in routing policies to flexibly control routes.
- Supporting masks, route summarization and Classless Inter-Domain Routing (CIDR).
- Supporting designated next hops to select the best next hops on broadcast networks.
- Supporting multicast routing update to reduce resource consumption.
- Supporting plain text authentication and MD5 authentication to enhance security.

Note：

RIPv2 has two types of message transmission: broadcast and multicast. Multicast is the default type using 224.0.0.9 as the multicast address. The interface working in the RIPv2 broadcast mode can also receive RIPv1 messages.

➢ **RIP Message Format**

1) RIPv1 message format

A RIPv1 message consists of a header and up to 25 route entries. The following figure shows the format of RIPv1 message.

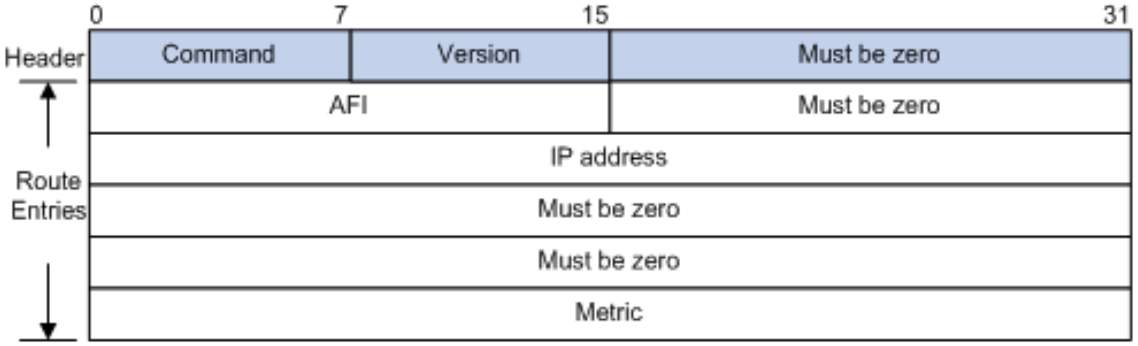


Figure 10-24 RIPv1 Message Format

The detailed explanations of each field are stated as following:

- Command: Type of message. 1 indicates request, and 2 indicates response.
- Version: Version of RIP, 0x01 for RIPv1.
- AFI: Address Family Identifier, 2 for IP.
- IP Address: Destination IP address of the route. It can be a natural network, subnet or a host address.
- Metric: Cost of the route.

2) RIPv2 message format

The format of RIPv2 message is shown as the following figure. It is similar to RIPv1.

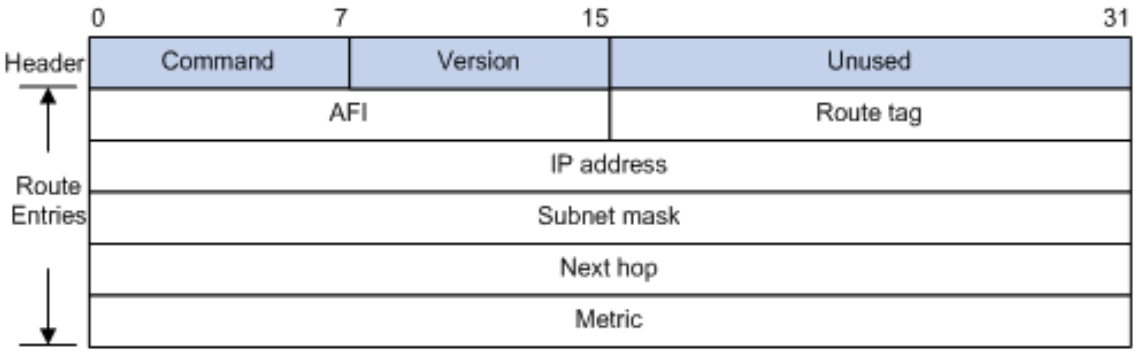


Figure 10-25 RIPv2 Message Format

The detailed explanations of each field are stated as following:

- Version: Version of RIP. For RIPv2 the value is 0x02.
- Route Tag: Route Tag.
- IP Address: Destination IP address. It can be a natural network address, subnet address or host address.
- Subnet Mask: Mask of the destination address.
- Next Hop: If set to be 0.0.0.0, it indicates that the originator of the route is the best next hop; otherwise it indicates a next hop better than the originator of the route.

➢ **RIPv2 authentication**

RIPv2 sets the AFI field of the first route entry as 0xFFFF to identify authentication information. See Figure 10-26.

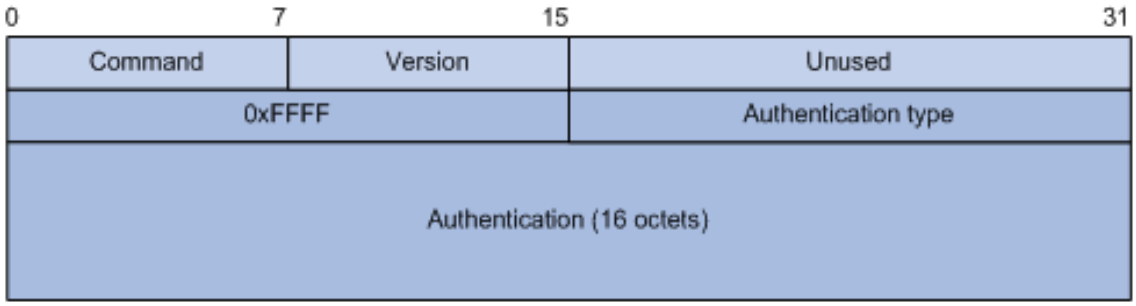


Figure 10-26 RIPv2 Authentication Message

- Authentication Type: A value of 2 represents plain text authentication, while a value of 3 indicates MD5 authentication.
- Authentication: Authentication data, including password information when plain text authentication is adopted or including key ID, MD5 authentication data length and sequence number when MD5 authentication is adopted.

Note：

RFC 1723 only defines plain text authentication. For more information about MD5 authentication, please see RFC 2453 RIP Version 2.

This function includes three submenus: **Basic Config**, **Interface Config** and **RIP Database**.

10.8.1 Basic Config

RIP (Routing Information Protocol) is a dynamic router protocol with Distance Vector Algorithms. You could configure the protocol below to active as you like.

Choose the menu **Routing→RIP→Basic Config** to load the following page.

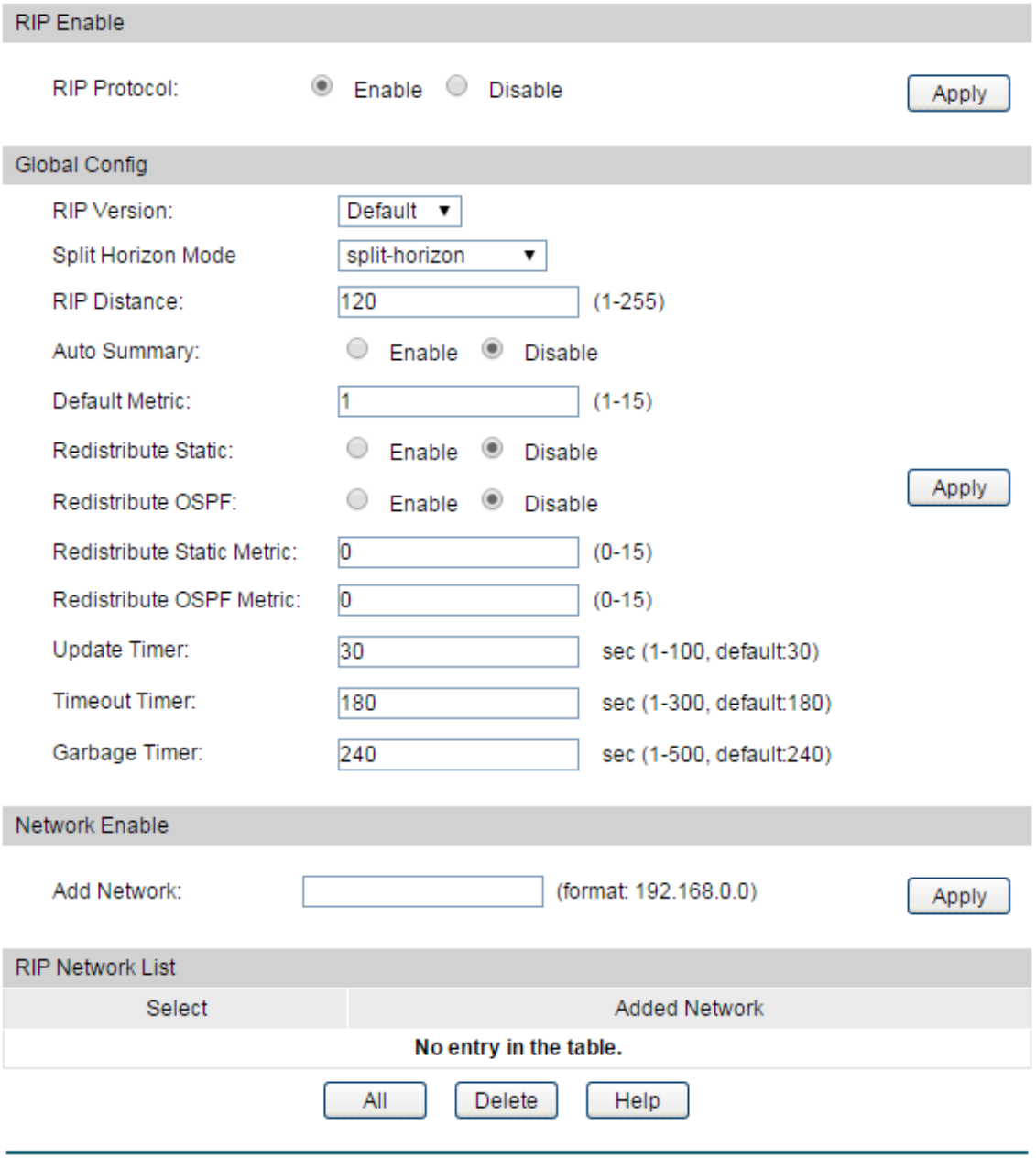


Figure 10-27 RIP Basic Config

The following entries are displayed on this screen:

- **RIP Enable**

  RIP Protocol: Choose to enable or disable the RIP function. By default it is enable.

➢ **Global Config**

RIP Version: Choose the global RIP version.

- Default: send with RIP version 1 and receive with both RIP version 1 and 2.
- RIPv1: send and receive RIP version 1 formatted packets via broadcast.
- RIPv2: send and receive RIP version 2 packets using multicast.

Split Horizon Mode: Choose the Split Horizon Mode.

- None: no special processing for this case.
- split-horizon: a route will not be included in updates sent to the router from which it was learned.
- Poison Reverse: a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

RIP Distance: Set the RIP router distance.

Auto Summary: If you select enable groups of adjacent routes will be summarized into single entries, in order to reduce the total number of entries The default is disable.

Default Metric: Set the default metric for the redistributed routes. The valid values are (1 to 15).

Redistribute Static: Choose to distribute Static router entries to RIP, the default is disable.

Redistribute OSPF: Choose to distribute OSPF router entries to RIP, the default is disable.

Redistribute Static Metric: Set the metric of redistributed Static routes. The valid values are (0 to 15).

Redistribute OSPF Metric: Redistribute OSPF Metric. Set the metric of redistributed OSPF routes. The valid values are (0 to 15).

Update Timer: The timer interval to generate a complete response to every neighboring gateway.

Timeout Timer: Upon expiration of the timeout, the route is no longer valid and set to unreachable.

Garbage Timer: Upon expiration of the garbage-collection timer, the route is finally removed from the tables.

➢ **Network Enable**

You could add the network to enable RIP protocol here, so the interface in the network would enable RIP protocol.

➢ **RIP Network List**

Display the network enabled in the list. You could choose to delete the network here.

10.8.2 Interface Config

On this page, you can configure advanced parameters for the RIP.

Choose the menu **Routing→RIP→Interface Config** to load the following page.

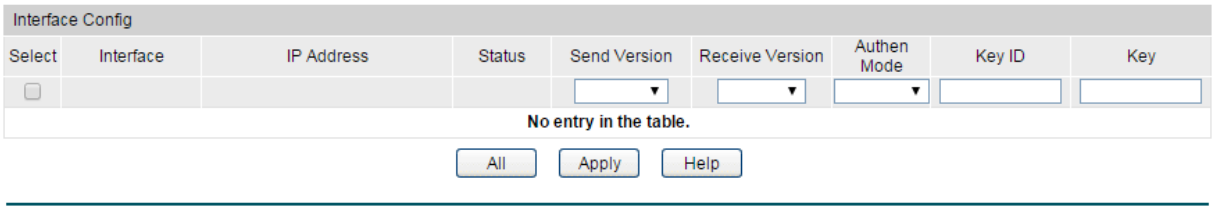


Figure 10-28 RIP Interface Config

The following entries are displayed on this screen:

➢ **Interface Config**

Select: Select the interface for which data is to be configured.

Interface: Displays the Interface ID.

IP Address: The interface IP address. You cannot change it here.

Status: The interface RIP status (up or down) is decided by the network status. You cannot change it here.

Send Version: Select the version of RIP control packets the interface should send from the pulldown menu.

- RIPv1: send RIP version 1 formatted packets via broadcast.
- RIPv2: send RIP version 2 packets using multicast.
- RIP-1c: send RIP version 2 packets using broadcast.

Receive Version: Select what RIP control packets the interface will accept from the pulldown menu.

- RIPv1: accept only RIP version 1 formatted packets.
- RIPv2: accept only RIP version 2 formatted packets.
- Both: accept both RIP version 1 and RIP version 2 formatted packets.

Authen Mode: Select an authentication type.

- **None**: This is the initial interface state. If you select this option from the pulldown menu no authentication protocols will be run
- **Simple**: If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
- **MD5**: If you select 'MD5' you will be prompted to enter both an authentication key and an authentication ID. All routers on the network must be configured with the same key and ID.

Key ID: Enter the RIP Authentication Key ID for the specified interface. If you choose not to use authentication or to use 'simple' you will not be prompted to enter the key ID.

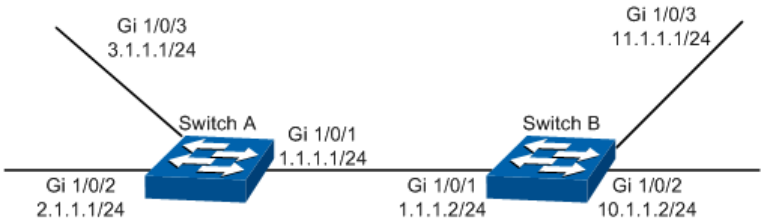
Key: Enter the RIP Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' or 'MD5' the key may be up to 16 octets long.

10.8.3 Application Example for RIP

➢ **Network Requirements**

- IP addresses of Switch A's three interfaces are 1.1.1.1/24, 2.1.1.1/24, 3.1.1.1/24 respectively. IP addresses of Switch B's three interfaces are 1.1.1.2/24, 10.1.1.1/24, 11.1.1.1/24 respectively.
- RIP is required to be enabled in all interfaces of Switch A and B. Network shall be interconnected between Switch A and B with the use of RIPv2.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch A

Step	Operation	Note
1	Enable RIP	Required. On page **Routing→RIP→Basic Config**, enable RIP, select RIPv2 as RIP version.
2	Enable the network segments where the interfaces are located	Required. On page **Routing→RIP→Basic Config** Network Enable part, add network segments 1.1.1.0, 2.1.1.0, 3.1.1.0, and enable RIP in these network segments. These network segments will be displayed in RIP Network List after they are successfully added.

- Configure Switch B

Step	Operation	Note
1	Enable RIP	Required. On page **Routing→RIP→Basic Config**, enable RIP, select RIPv2 as RIP version.

2	Enable the network segments where the interfaces are located	Required. On page **Routing→RIP→Basic Config** Network Enable part, add network segments 1.1.1.0, 10.1.1.0, 11.1.1.0, and enable RIP in these network segments. These network segments will be displayed in RIP Network List after they are successfully added.

10.9 OSPF

OSPF (Open Shortest Path First) is a routing protocol based on link state and also an internal gateway protocol, which is developed and recommended by IETF. The OSPF protocol standard in current use for IPv4 network is OSPF Version 2, which is defined specifically in RFC2328 and will be introduced generally in this Guide.

➢ **Introduction**

1. OSPF Features

OSPF protocol is a popular routing protocol in networking with the following features.

- Fast convergence – It could send update packets immediately upon the change of network topology, to quickly synchronize the update for the routers in the autonomous system.
- Due to the rapid convergence, OSPF routing protocol acts with great speediness and stability in the large-scale network, and is not prone to some harmful routing information.
- OSPF protocol introduces the concept of area – to manage the autonomous system by area, which means the routers only need to synchronize the link state database with the other routers in the same area. Thus, the smaller link state database requires lower memory consumption from the routers, and the less routing information to manage also releases certain CPU resources for the routers and meanwhile reduces the network bandwidth occupied by the routing information.
- OSPF protocol supports multiple equal-cost routes to one destination for load balance, thus to perform more efficient data forwarding.
- OSPF supports VLSM route addressing by variable-length subnet mask.
- OSPF supports the message authentication based on interfaces, thus to guarantee the security of message interaction and routing calculation.
- OSPF supports using the reserved multicast address in the link of specific network type, to reduce the influence on the other irrelevant routers.

2. OSPF Common Scenario

OSPF protocol is usually applied in the large complex network environment. Shown as below is the instance diagram of a large company, where the large network is divided by department. OSPF protocol works as the fundamental routing protocol among routers, which could guarantee not only the message interaction but also the network independence among departments.

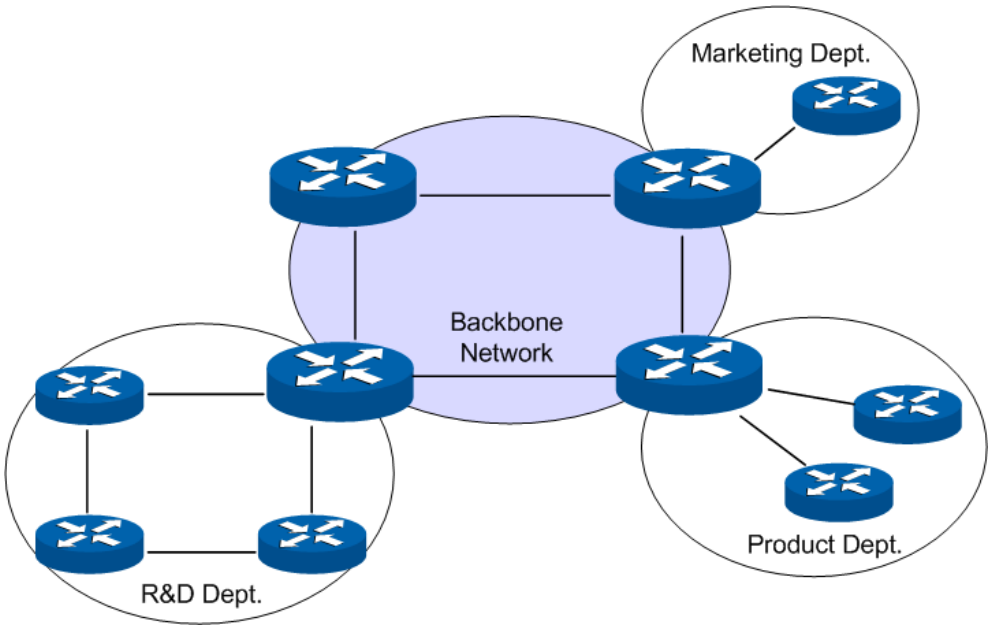


Figure 10-30 Common Scenario for OSPF routing protocol

The network topology is more prone to changes in an autonomous system of larger size. The network adjustment of any one router could destabilize the whole network and cause massive OSPF packets to be forward repeatedly, and all the routers need to recalculate the routes, which would waste lots of network resources. In this case, area partition would be an effective solution. The routers only need to maintain the same link state database in their own area, and then the ABR would collect the routing information from different areas and advertise to other areas. For more details about area partition, please refer to the following chapters.

➢ **OSPF Principles**

This section would introduce in details the working principles of OSPF protocol. First of all, let's get to know some basic concepts about the OSPF routing protocol.

1. Autonomous System

Autonomous System, short for AS, is a set of routers using the same routing protocol to exchange routing information. OSPF, working within an AS, is an internal gateway protocol.

2. Router ID

A router running OSPF protocol identifies its uniqueness by its router ID – a 32-bit unsigned integer, which could be manually assigned by the administrator or automatically selected by the router itself. In case different routers might obtain the same ID in automatic selection, you are recommended to configure router ID manually.

In RFC protocol, two means of automatically electing router ID are recommended:

- If the loopback interfaces are configured, the highest IP address among them will be selected as the router ID.
- If no loopback interface is configured, the highest IP address among those of active router interfaces will be selected as the router ID.

The good stability of loopback interfaces (always in active state as long as the router boots) ensures that every time the router boots it would automatically elect the loopback interface IP

address as the router ID which is thus always invariant outward. To ensure the uniqueness of the router ID, it is recommended to manually configure the router ID or the loopback interface.

In the automatic election, the router would in the first place select the highest loopback interface IP address as the router ID. If the router doesn't pre-define the loopback interfaces, it would select the highest physical interface IP address as the router ID.

3. OSPF Network Types

OSPF, a dynamic routing protocol running in the network layer, would apply different working mechanism according to the features of different data link layers. There are four sorts of relationships between the working mechanism of OSPF routing protocol and network type.

1) **Broadcast:** When the network type is Ethernet or FDDI, OSPF protocol would broadcast the Hello, LSU and LSAck packets. For instance, the Hello packet is multicast to the other OSPF routers in the LAN and the destination address is the reserved 224.0.0.5, while the other routers forward the link state update and acknowledgement data to OSPF DR with the reserved multicast address as 224.0.0.6. In such broadcast type of network the DD and LSR packets are unicast.

2) **NBMA (Non-Broadcast Multi-Access):** In such type of network as frame relay, ATM or X.25, where the routers need extra configuration to find neighbors, the OSPF protocol packets are unicast.

3) **P2MP (Point-to-MultiPoint):** In general, P2MP type of network is converted from NBMA, where the Hello packet is multicast (224.0.0.5), LSU and LSAck packets are multicast (224.0.0.5) or unicast, DD and LSR packets are unicast.

4) **P2P (Point-to-Point):** When the link layer protocol is PPP or HDLC, the link always connects a pair of routers, who could generally establish an adjacency relationship after becoming valid neighbors. In this type of network, the protocol packets are multicast (224.0.0.5).

Our switches are all Ethernet ones. The network type of all the interfaces defaults to Broadcast, and it also supports to be configured as P2P type that can automatically find neighbors. To ensure the communication of multi-point networking, it's not recommended to manually configure the network type of interfaces. In the following guide, we will mainly take the broadcast type of interface for example to introduce the working principle of OSPF protocol.

4. Designated Router and Backup Designated Router

On broadcast networks or NBMA networks, usually there are multiple routers running OSPF protocol at the same time. If the neighbor relationship between any two routers is adjacency, the change of one router could result in the repeated forwarding of route updates and a waste of network resources.

DR (Designated Router) and BDR (Backup Designated Router) defined by OSPF protocol would maintain the entire network, while the other routers only need to establish adjacency relationships with DR and BDR. DR is responsible to flood the routing information in the network to all the neighbors. When DR fails, BDR will become the new DR, which avoids network block during the DR re-election. Then a new BDR needs to be re-elected for sure, but the process would not affect the communication even though it still requires quite a long time. Once DR and

BDR are determined in a network, unless they become invalid, any new routers joining or exiting would not cause re-election.

As shown below, on a network of five routers, ten adjacency relations need to be established if one between every two routers, but only seven adjacencies are required if DR and BDR are introduced. To conclude, on a network of N routers, N*(N-1)/2 adjacencies are required in general, but the adjacencies required will be (N-2)*2+1 if DR and BDR are introduced. Therefore, the more routers on the network, the more significant the advantages will be.

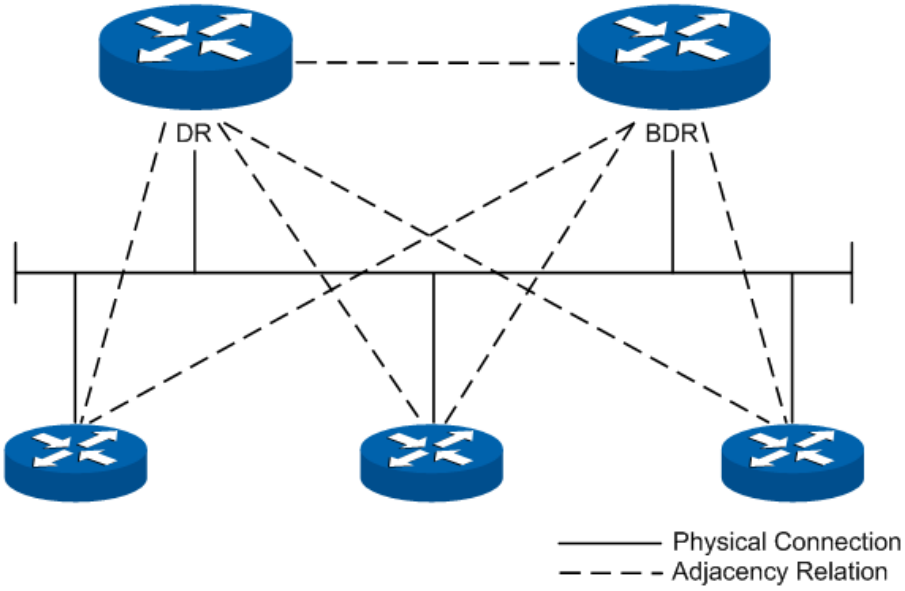


Figure 10-31 Diagram of DR/BDR Adjacency Relation

DR or BDR is determined by the interface priority and router ID. First of all, whether a router could be the DR or BDR on a network is decided by its interface priority. The one of highest priority would be elected as DR or BDR; while if all the interfaces are of the same priority, it would then be decided by the router ID. In conclusion, DR or BDR is the feature of a certain interface of the router which indicates the status of the router in a network segment rather than the features of the router on the network. Every network segment needs to elect a DR and a BDR to synchronize the routing information. The configuration of router interface parameters needs to be done on the basis of network planning.

- **OSPF Working Process**

In the following, we would take the example of two routers initiating interface OSPF protocol to introduce the working process of OSPF routing protocol in the Ethernet model.

1) The router interface initiates the OSPF protocol, and then the interfaces in the same network segment would discover neighbors by sending Hello packets. If the interfaces are connected on the same public data link, and the area IDs, authentication information, network subnet, Hello data interval and neighbor router dead-interval are all matched, the two routers would put each other in its neighbor table.

2) If the receiver discovers its own ID on the neighbor table of the Hello packet, a successful mutual communication would be established. And then they will elect DR and BDR according to such parameters as the interface priority and the router ID, while if DR and BDR already exist in the network, they will be accepted.

3) After DR and BDR are determined, the master and slave one will be elected between the DR/BDR and the other routers on the network, and then the link state database synchronization will start.

4) On the network the routers and DR/BDR will mutually unicast the link state data to advertise LSA, until all the routers establish an identical link state database. During the synchronization of link state database, if the database description packet sent contains an updated LSA or a LSA the receiver doesn't have, the receiver would send request for the details of this LSA via LSR packets. In other words, in any phase of DD exchange, as long as the received DD packet contains new LSA information, the receiver could send LSA request for synchronization. The routers receiving the LSR packet will unicast the LSU packet carrying LSA to the other end.

5) After two routers have finished the synchronization of link state database, a complete adjacency relation will be established.

6) When the intra-area routers have an identical link state database, each of them will calculate a loop-free topology through SPF algorithm with itself as the root thus to describe the shortest forward path to every network node it knows, and create a routing table according to the topology of shortest forward path and provide a basis for data forwarding.

7) After the establishment of routing table, if the network remains stable, the neighbors would discover and maintain their neighbor relationships by sending out Hello packets at regular intervals. And the adjacent routers would recalculate the routing table by periodical LSA update in order to maintain valid entries in the routing table.

8) Any new routers joining the network will accept the current DR/BDR and synchronize the link state database with them until a complete adjacency relation is established. During synchronizing the link state database, DR/BDR will obtain LSA from the newly-joint routers and then flood this LSA to the adjacent routers who then will flood it to the other ports till the entire network.

1. Work Flow Diagram

The diagram below takes two routers for example to introduce in the Ethernet module the detailed steps of two routers from failure state to complete adjacency state and the relevant packet types involved in the process.

Note:

To facilitate the description the diagram below shows the LSA synchronization after the DD exchange, while in reality these two processes are simultaneous.

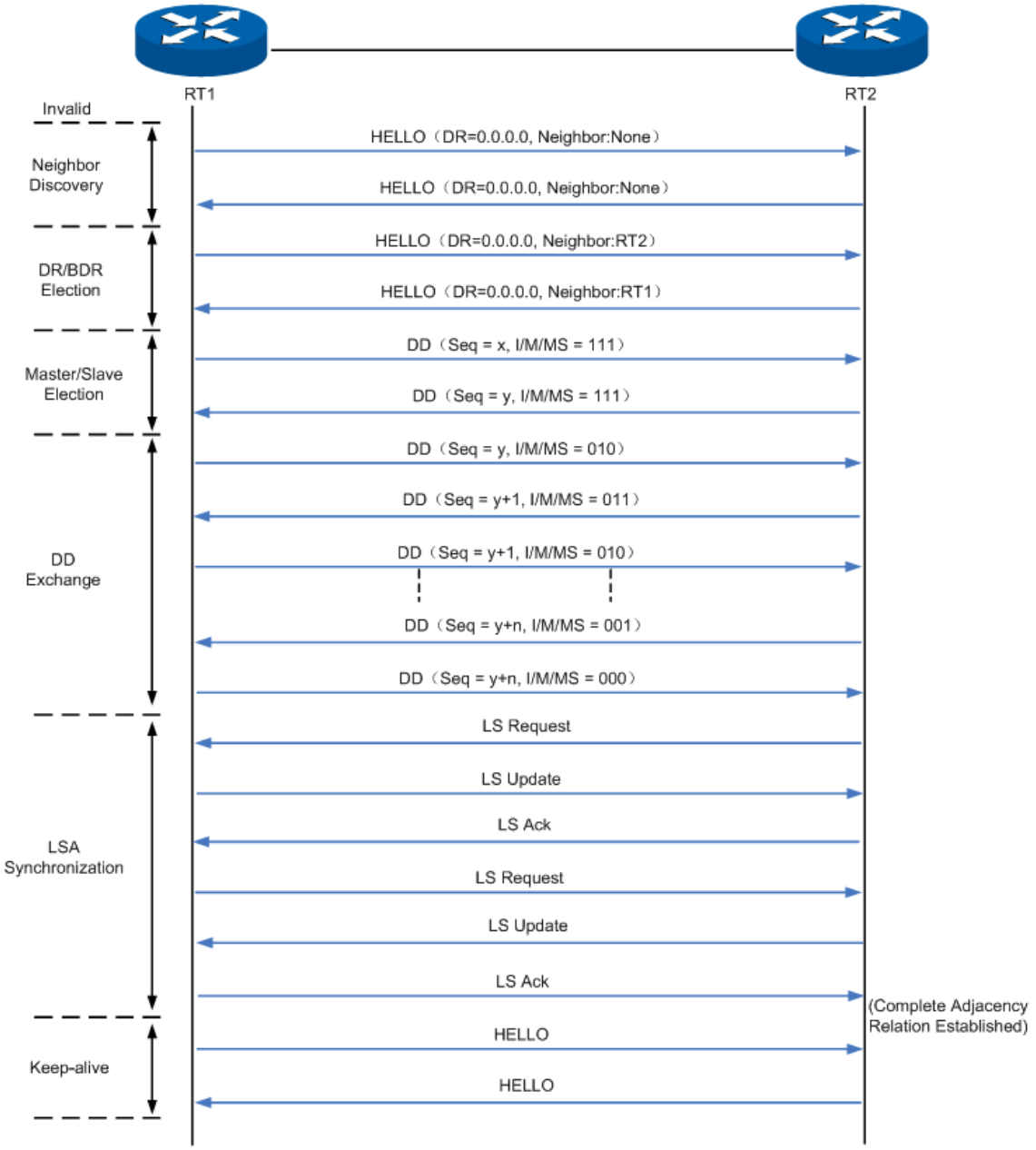


Figure 10-32 Steps to Establish a Complete Adjacency Relation

2. Flooding

As Figure 10-32 shows, two random routers will synchronize the link state database via LSA request, LSA update and LSA acknowledgement packets. But in the actual module of router network, how do the routers flood the change of local network to the entire network through LSA update packets? Figure 10-33 will introduce in details the flooding of the LSA update packets on the broadcast network.

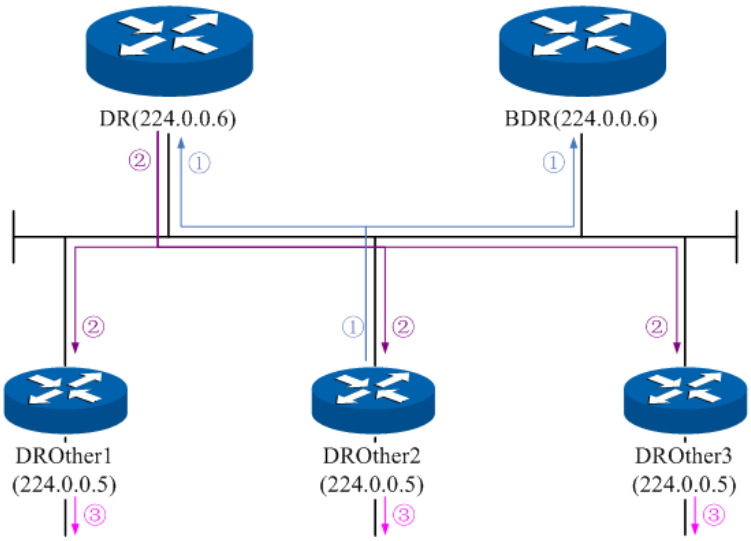


Figure 10-33 Flooding of the LSA

1) DROthers multicast the LSA update of its directly-connected network to DR and BDR.

2) After receiving the LSA update, DR floods it to all the adjacent routers.

3) After receiving the LSA update from DR, the adjacent routers flood it to the other OSPF interfaces in their own areas.

➢ **Area and Route Summarization**

OSPF protocol gets every router in the network to obtain a complete network topology through adjacency relationship, thus to calculate the routing table and accomplish the forwarding of network data. As the network grows in size, every router has to spend plenty of resources to store LSDB and calculate routing table, so any delicate changes in the network topology will require the routers in the entire network to re-synchronize and re-calculate, which will cause the network to be in the state of frequent "oscillation".

In order to run effectively and efficiently in a large-scale network, OSPF protocol can divide the routers in an autonomous system into logic areas identified by Area ID. After the area partition, the intra-area routers will accomplish the route addressing and data forwarding according to the standard OSPF routing protocol. While the boundary routers of multiple areas will have to summarize the information from the routers of all areas to the backbone area that is identified as Area 0, and then the backbone area will advertise these summary to the other areas. As below is the model of area partition.

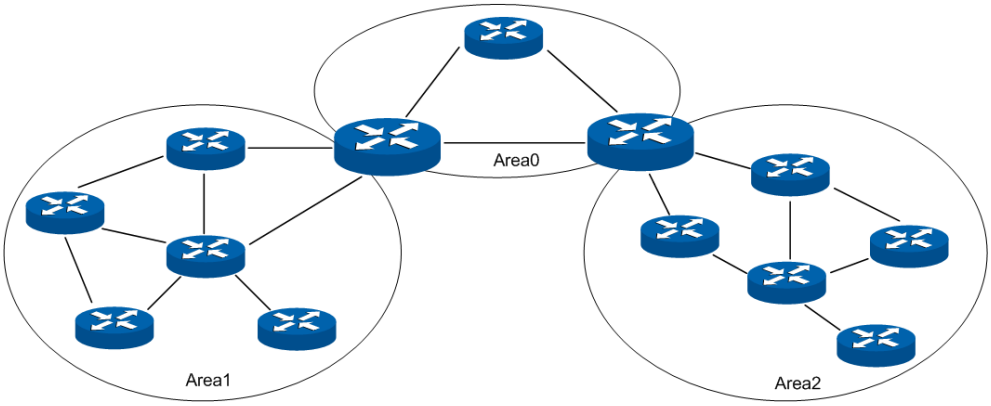


Figure 10-34 Area Model

As shown above, a large-scale network is divided into three areas: Area 0, Area 1 and Area 2. Area 1 and Area 2 exchange the routing information via Backbone Area, which has to maintain its network connectivity at all time. The non-backbone Area 1 and Area 2 cannot communicate directly with each other, but they can exchange routing information through the backbone Area 0. On large-scale networks, an appropriate area partition can help greatly to save network resources and enhance the speed of the routing.

After the area partition in the network, routers of different type need to accomplish different tasks. Different areas need to transmit the routing information to the backbone area in different ways, due to their different locations relative to the backbone area. In the following, we will introduce the details involved after the area partition.

1. Router Type

As Figure 10-35 shows, after the area partition of the network, the routers need to accomplish different tasks due to their locations in different areas, according to which the routers can be classified into 4 types: Internal Router (IR), Backbone Router (BR), Area Boundary Router (ABR) and Autonomous System Boundary Router (ASBR).

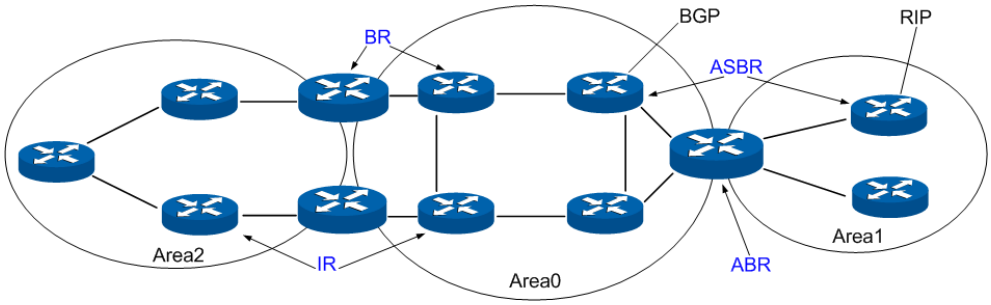


Figure 10-35 Classification of Routers

Responsibilities of different routers divide as Table 10-2.

Router Name	Features	Responsibility
IR	All the routing interfaces belong to the same area	Flood and exchange its all link and interface information with the adjacent routers in the same area, thus to synchronize the link state database with the intra-area routers.
BR	At least one routing interface belongs to the backbone area	Summarize the routing topology information from all areas in AS via ABR and forward the communication data for all areas.
ABR	Connect one or more areas to the backbone area	Maintain independent link state databases for different areas, and deliver the topology information of each area to the other areas via the backbone area.

ASBR	Connect with the routers outside the OSPF AS by other routing protocol	Maintain independent routing tables for different routing protocols, import the routing information learned by other routing protocol to OSPF domain through a certain standard, and then establish a uniform routing table.

Table 10-2 Router Types

2. Virtual Link

In practice, some physical restrictions might keep ABR of some areas from directly connecting to the backbone area, which can be solved by configuring an OSPF virtual link. Virtual link sketch is shown as below.

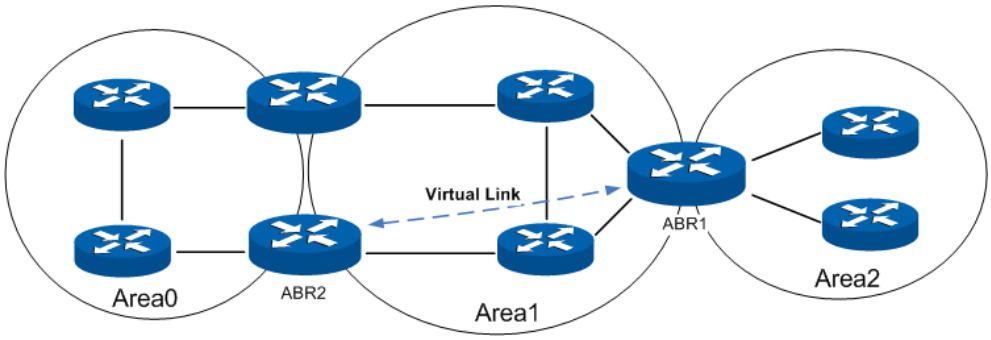


Figure 10-36 Virtual Link Sketch

As in Figure 10-36, ABR of Area 2 has no physical link to connect directly with the backbone area, in which case Area 2 could not communicate with others without configuring a virtual link. Then a virtual link between ABR1 and ABR2, passing through Area 1, could provide a logical link for Area 2 to connect with the backbone area.

A virtual link is a point-to-point connection between two ABRs. Hence, simply configuring the virtual link parameters on two ordinary router interfaces makes two ends of the virtual link. Two ABR directly forward the OSPF packets to each other's interface IP address, while the OSPF routers between them transmit these packets as regular IP packets.

In general, configuring a virtual link is a temporary means to fix the problems of network topology, which usually would to certain degree complicate the network. Therefore, when networking in reality, a virtual link should be avoided if possible.

3. Route Types

OSPF prioritize routes into four levels:

1) Intra-area route

2) Inter-area route

3) Type-1 external route: It has high credibility and its cost is comparable with the cost of an OSPF internal route. The cost from a router to the destination of the Type-1 external route equals to the cost from the router to the corresponding ASBR plus that from the ASBR to the destination of the external route.

4) Type-2 external route: It has low credibility, so OSPF considers the cost from the ASBR to the destination of the Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from the internal router to the destination of

the Type-2 external route equals to that from the ASBR to the destination of the Type-2 external route. If two routes to the same destination have the same cost, then take the cost from the router to the ASBR into consideration.

Intra-area route and inter-area route describe the internal network structure of the autonomous system, while the external routes tell how to select the route to the destination outside the autonomous system.

4. Stub Area and NSSA Area

An area that can connect to the autonomous system and forward the communication data to external areas only through ABR could be set as Stub Area. Once an area is set to be Stub Area, ABR would no longer flood the external routing information described by the AS-External LSA to it, and meanwhile a default route with a target network 0.0.0.0 would be generated. This default routing would be announced to the other routers in the area. All the packets forwarded to external areas would be sent to ABR and then be forwarded outwards through it. Since there is no need to learn about the routing information from other areas, the size of the routing table of the routers in the stub area as well as the number of the routing message transferred would be reduced greatly.

NSSA (Not-So-Stubby-Area) has a lot in common with stub area, but is not completely the same. NSSA doesn't allow ABR to import the external routing information described by AS-External LSA, either. But it does allow ASBR in the area to spread in the NSSA the routing information as Type-7 LSA, which is learned by other routing protocols. Upon receiving it, ABR in the area would transform it to AS-External LSA and then flood to the whole autonomous system.

5. Route Summarization

Route summarization is to summarize routing information with the same prefix with a single summarization route and then distribute it to other area. Via ABR route summarization a Summary LSA will be distributed to other areas, while via ASBR route summarization an AS-External LSA will be distributed to the entire AS. Therefore, route summarization will greatly reduce the size of LSBD.

ABR Route Summarization: When the network reaches a certain size, to configure route summarization on the ABR could summarize the intra-area route to be a wider one and then distribute it to other areas, which could receive less the routing entries. As Figure 10-37 shows, in Area 1 ABR1 can configure a summarization route 192.161.0.0/16 and advertise it to the backbone area, while in Area 2 ABR2 can configure an summarization route 192.162.0.0/16 and advertise it to the backbone area.

Please pay attention to that, if the network is planned to be discontinuous subnets, you need to configure the route summarization with great caution; otherwise, it might cause some unreachable network conditions. As Figure 10-38 shown, configuring the summarization route 192.161.0.0/16 on ABR1 and ABR2 might result in the inaccessible routing. Under such circumstance, it is suggested to configure route summarization on only one ABR.

ASBR Route Summarization: If a route summarization is configured on an ASBR, the AS-External LSA in the specified address range will be summarized. When NSSA is configured, Type-7 LSA in the specified address range will also be summarized. Following a similar principle with ABR route summarization, ASBR summarizes routes of different type.

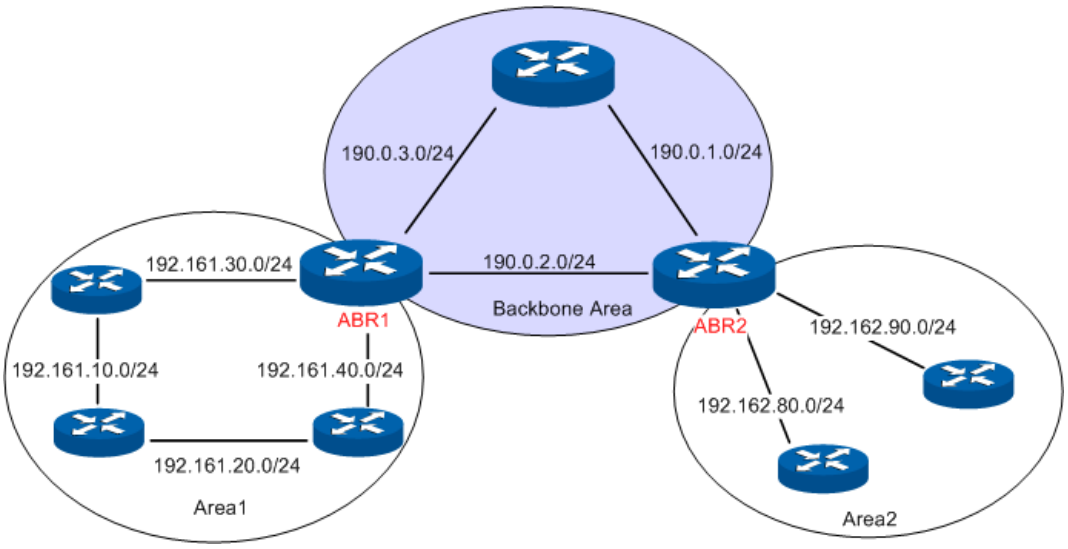


Figure 10-37 ABR Route Summarization

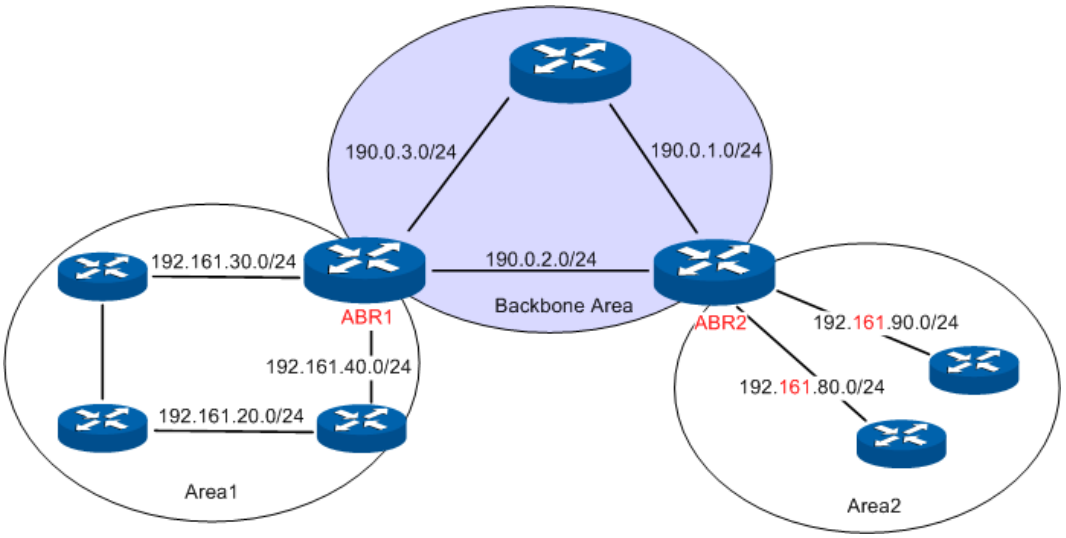


Figure 10-38 Discontinuous Network Segment

➢ **Link State Database**

When the routers in the network completely synchronize the link state database through LSA exchanges, they can calculate the shortest path tree by basing themselves as the root node. The OSPF protocol routing calculation is simply presented as below.

1) Each OSPF router would generate LSA according to its own link state or routing information, and then send it through the update packets to the other OSPF routers in the network. LSA is to describe the network topology and the routing information. For instance, Router-LSA describes the link state of routers; Summary-LSA describes the inter-area route; and so on.

2) Each OSPF router collects LSA advertised by the other routers to form an LSDB. All the Router-LSA and Network-LSA in the LSDB describe the entire intra-area network topology, while the other types of LSA describe the route to a certain destination in other areas or external AS.

3) When all the routers in the network completely synchronize their LSDB, each OSPF router will calculate a loop-free topology by SPF algorithm to describe the shortest path to every

destination in the network as it knows. This loop-free topology is so-called the SPF algorithm tree.

4) Each router will establish its own routing table according to the SPF algorithm tree.

➢ **OSPF Protocol Packet Type**

During the entire learning process, OSPF routing protocol uses five types of packet, all of which are IP packets. The packets with 89 as its IP header protocol segment are OSPF ones. This device abides by the standard RFC protocol. And we are going to introduce the packet formats involved in the course of OSPF routing protocol running according to the definition by RFC documentation, and attached with the images and the meaning of key segments.

1. OSPF Header

In the course of routing learning, OSPF uses five types of packet, which have the same OSPF header, as shown below.

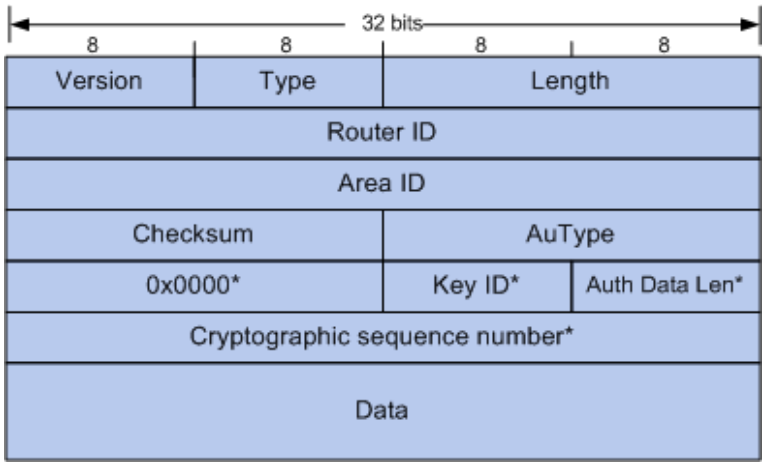


Figure 10-39 OSPF Header

1) **Version:** The version number of OSPF run by this device. For instance, the OSPF run by our IPv4 devices is of Version 2, and that run by IPv6 devices is of Version 3.

2) **Type:** The type of this packet. There are totally five types of OSPF packets, as shown in the table below.

Type Code	Packet Name
1	Hello Packet
2	Database Description Packet
3	Link State Request Packet
4	Link State Update Packet
5	Link State Acknowledgement Packet

Table 10-3 OSPF Packet Type

3) **Router ID:** ID of the router sending this packet.

4) **Area ID：** ID of the area that the router interface sending this packet belongs to.

5) **Authentication Type:** The authentication type applied by this packet. The segment marked with * in the rear is regarded as essential information of authentication, as shown in the table below.

Type Code	Authentication Name	Features
0	Non-Authentication	The 64-bit authentication information fields behind are all 0.
1	Plain-text Authentication	The 64-bit authentication information behind is the password to authenticate.
2	MD5 Ciphertext Authentication	The Key ID, authentication data length and encryption serial number work together to perform MD5 Ciphertext Authentication

Table 10-4 Authentication Type

2. HELLO Packet

OSPF routers send Hello packets to each other to find neighbor routers in the network and to maintain the mutual adjacency relationship. Only when two routers send Hello packets carrying the same interface parameters, can they become neighbors.

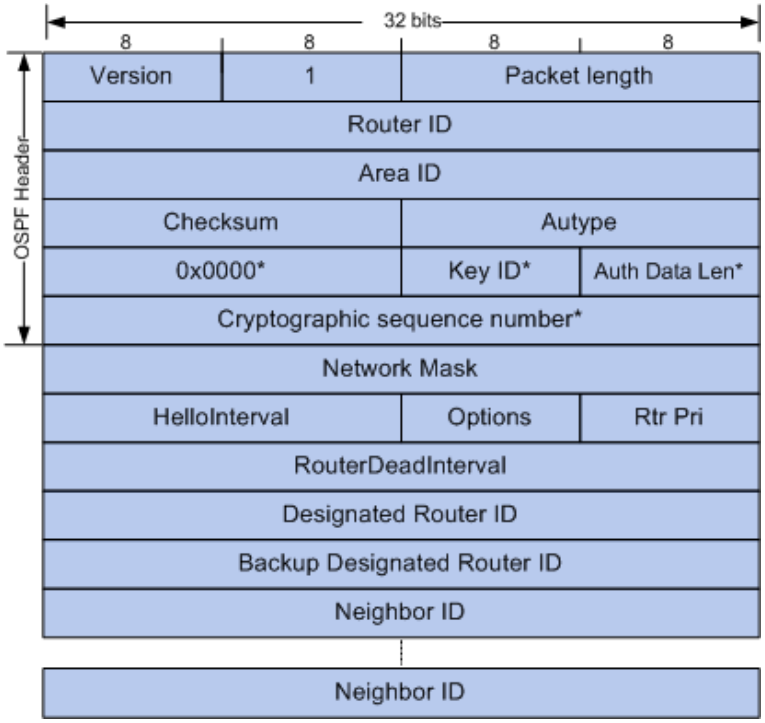


Figure 10-40 HELLO Packet

1) **Netmask:** Netmask of the router interface forwarding Hello packet. Only when the netmask of the forwarding interface and that of the receiving interface coincide, can these two routers be neighbors.

2) **Hello Interval:** Interval of a sequence of Hello packets sending by the forwarding interface. Only the routers with the same Hello interval can become neighbors.

3) **Router Priority:** This field decides the election result for DR/BDR in the network segment. The greatest value means the highest priority of the advertising router and also the possibility of being elected as the DR in the segment, while the value 0 means no election right.

4) **Router Dead Interval:** When the receiving router doesn't receive another Hello packet update from the advertising router within the specified age time, it will delete the advertising router from its neighbor table. Only routers with the coincident dead interval can be neighbors.

5) **Designated Router ID:** The interface IP of the router specified by the advertising router in the advertising interface network.

6) **Backup Designated Router ID:** The interface IP of the backup router specified by the advertising router in the advertising interface network.

7) **Neighbor:** All the neighbor tables of the advertising router, listing the neighbor interface IP addresses in each interface network segment.

3. DD Packet

Two routers after becoming neighbors will send to each other the header of all routing information in its link state database through the DD packets, in which way the receiving router could synchronize the database.

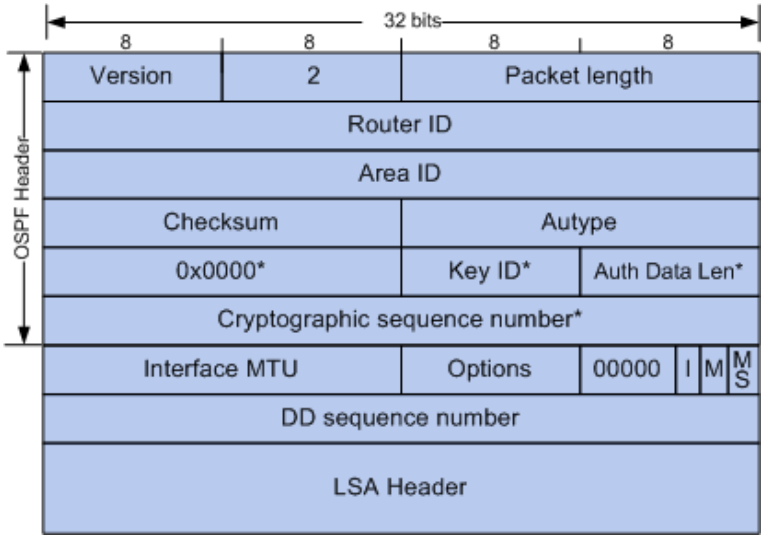


Figure 10-41 DD Packet

1) **Interface MTU:** Size in bytes of the largest IP packet that can be sent out by the routing interface of the advertising router.

2) **I:** The Initial bit. During the synchronization of link state database between two routers, it may require multiple DD packets to be forwarded, among which the first DD packet will set its initial bit to 1, while the others 0.

3) **M:** The More bit. When the forwarded DD packet is not the last one database, it will set its More Bit to 1, while the last DD packet will set the M-Bit to be 0.

4) **MS:** The Master/Slave bit. Before the synchronization of the link state database between two routers, master/slave router needs to be elected, which in general is decided by such parameters as the router priority, router ID and etc. After the election, the master router will dominate the process of database synchronization. The DD packet forwarded by the master router would set its MS bit to 1, while that by the slave router would set the MS bit to 0.

5) **DD Sequence Number:** After the master/slave router having been elected, the master router randomly determines the sequence number of the first DD packet, and then the sequence number of the following DD packets increments by one. In this way, the whole synchronization process will carry on in good order.

6) **LSA header:** The LSA header of the whole or partial link state database of the advertising router, whose uniqueness identifies a LSA.

4. LSR Packet

During the synchronization of the link state database between two routers, if one router finds an updated LSA or an LSA it doesn't have in the DD packet forwarded, it could send a LSR packet to request for a complete LSA.

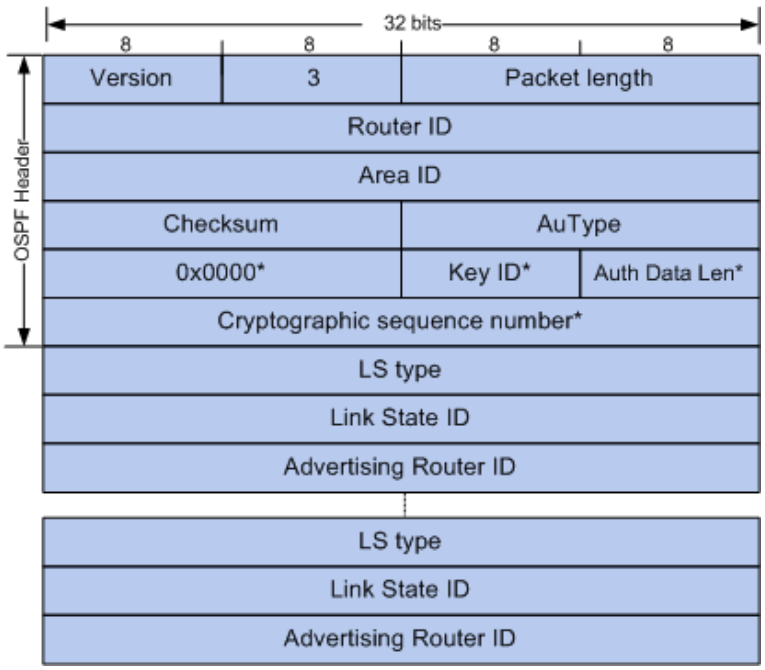


Figure 10-42 LSR Packet

1) **Link State Type:** The type of LSA. There are 11 types of LSA in total: Router LSA, Network LSA, Network Summarization LSA, ASBR Summarization LSA, and so on. In the following, all these would be introduced in details.

2) **Link State ID:** It has different meanings for different types of LSA. The Link State ID of Router LSA stands for the ID of advertising router; that of Network LSA stands for the interface IP address of the DR; and that of Network Summarization LSA stands for the IP address of the network or subnet advertised; and etc.

3) **Advertising Router:** Router ID of the router advertising this LSA.

5. LSU Packet

When one router receives an LSR, it would send an LSU packet to inform the other the complete LSA information. The router receiving the LSA update will re-encapsulate this LSA and then flood it.

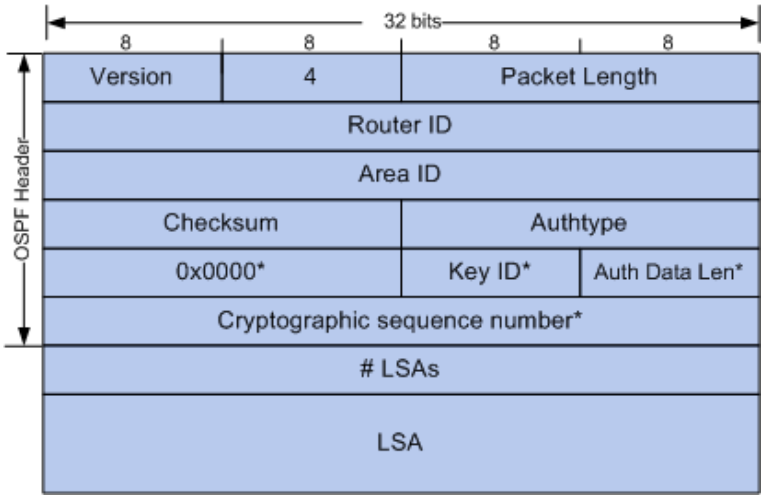


Figure 10-43 LSU Packet

1) **LSA Quantity:** The quantity of LSA included in the LSU.

2) **LSA:** A complete description of LSA.

6. LSAck Packet

When receiving a LSU, the router will send to the router forwarding the LSU packet a LSAck packet including the LSA header it receives to confirm whether the data received is correct.

7. LSA

OSPF protocol defines area and multiple router types. Via various sorts of LSA, different types of router complete routing update caused by network changes. OSPF protocol defines 11 types of LSA, which all have the same LSA header. As shown below, every LSA is unique in the network, and could be identified uniquely by the key field of LSA header.

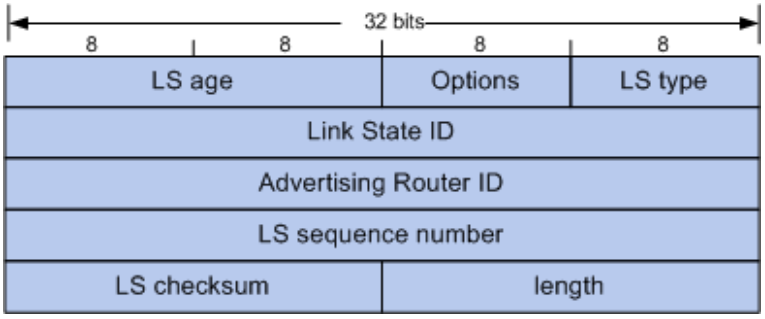


Figure 10-44 LSA Header

1) **Age:** The time passed since the LSA is generated. When the age goes over the threshold value set by the router system, which is one hour, and the router doesn't receive an LSA update, it will delete this LSA.

2) **Type:** The type of LSA. Table 10-5 enumerates several common features of LSA.

3) **Link State ID:** It has different meanings for different types of LSA. For details please refer to the RFC documentation.

4) **Advertising Router:** ID of the router advertising this LSA.

5) **Sequence Number:** It indicates the uniqueness of a certain LSA, whose update would be flooded to the network by adding 1 to the sequence number.

In the table below are the features of 6 types of common LSA.

Type Code	Name	Features
1	Router LSA	Originates from all the routers, and describes the router interface which itself has already run the OSPF features and then spreads in its advertising area.
2	Network LSA	Originates from DR, and describes the link state of all routers in its connected network segment and then diffuses in its advertising area.
3	Network Summary LSA	Originates from ABR, and describes the routers of all segments in the area and then advertises to the backbone area, the routers in which area will re-summarize and then announce to the other area.
4	ASBR Summary LSA	Originates from ABR, and describes the routers from ABR to ASBR and advertises the path to ASBR to the area ABR connects.
5	AS External LSA	Originates from ASBR, and describes the external route and the accessible network obtained by other routing protocols. This type of LSA will be flooded to the entire autonomous system.
6	NSSA External LSA	Originates from ASBR in the NSSA. The content of this LSA is the same as that of AS external LSA, but it would be advertised only to NSSA. ABR can transform this type of routing information to AS external LSA and then flood it to the entire AS.

Table 10-5 Types of LSA

➢ **OSPF Features Supported by the Switches**

This switch, supporting standard OSPF routing features, is applicable to multiple network environments and able to meet the common networking requirements in the Ethernet scene. The OSPF features supported are listed as follows.

1) Multi-process – The switch can establish multiple routing processes, independent of each other and having independent database. Each routing interface belongs only to one specific process. In short, multi-process on one switch is to divide one switch into several independent switches logically.

2) Area Partition – The switch can divide an autonomous system into different areas according to the user-specified principle. The routers in the same area only need to synchronize LSA with the other routers in its area, which can save routing resources and lower routing performance requirements, thus to reduce networking cost.

3) Configuration of multiple equal-cost routes to balance load and backup lines.

4) Route redistribution –OSPF can import routing information learned by other routing protocols or other OSPF processes.

5) Plaintext authentication and MD5 authentication supported when two neighbor routers in the same area are performing message interaction, which can improve the security.

6) Customized configuration of multiple interface parameters, including the interface cost, the retransmit interval, the transmit delay, the router priority, the router dead time, the hello interval and authentication key, etc. in order to satisfy multiple network requirements with flexibility.

7) Configuration of virtual link – When a network being divided into several areas, it can connect the areas physically located far away to the backbone network through virtual link.

8) Configuration of Stub Area and NSSA.

9) ABR route summarization – to summarize the intra-area routing information with the same prefix with a single route and then distribute it to other areas.

➢ **Configuration Introduction**

OSPF protocol defines various parameters to guarantee the normal operation of the OSPF function. The configurations of all the routers in the AS should be unitedly planned, which adds complexity to the implement of the OSPF function to some extent. However, in a practical scenario, most of these parameters need no configurations unless there are special requirements. Users can keep the default values of these parameters and configure the basic ones. The necessary steps to configure OSPF protocol is shown below:

1) Enable routing features on the switches. The routing features are enabled by default.

2) Create the routing interfaces and configure their IP parameters.

3) Plan the areas to which the subnets (routing interfaces) of the switches belong.

4) Configure the OSPF processes on each switch.

5) Configure the routing interfaces and the areas they belong to under the corresponding OSPF processes.

The OSPF routing protocol will run normally after the above configurations. A special topology network requires further reading of introductions to the web configuration pages below to optimize the corresponding parameters.

10.9.1 Process

Choose the menu **Routing→OSPF→Process** to load the following page.

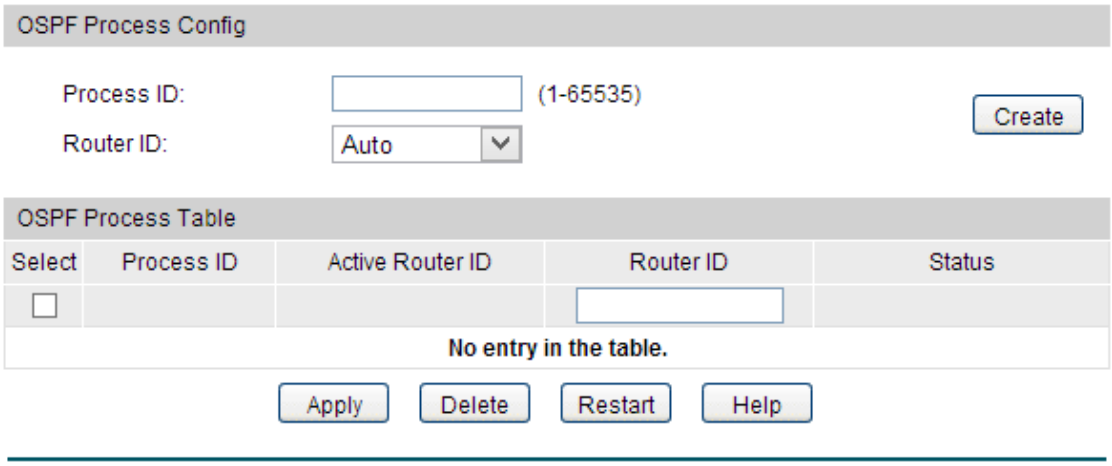


Figure10-45 OSPF Process

Configuration Procedure:

1) Specify a Process ID.
2) Configure the router ID.
3) Click **Apply**.

Entry Description:

➢ **OSPF Process Config**

Process ID: The 16 bit integer that uniquely identifies the OSPF process, ranging from 1 to 65535.

Router ID: The 32 bit unsigned integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS).

➢ **OSPF Process Table**

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

Process ID: Displays the configured OSPF process.

Active Router ID: Displays the active router ID that is currently used by the process.

Router ID: Displays the router ID that you configured before. When you change the router ID of a process, it will not take effect until you restart the process.

Status: Displays the status of the process.

- Running: The process is running and its router ID has been configured or auto selected.
- Pending: The process has no router ID and cannot start.

10.9.2 Basic

Choose the menu **Routing→OSPF→Basic** to load the following page.

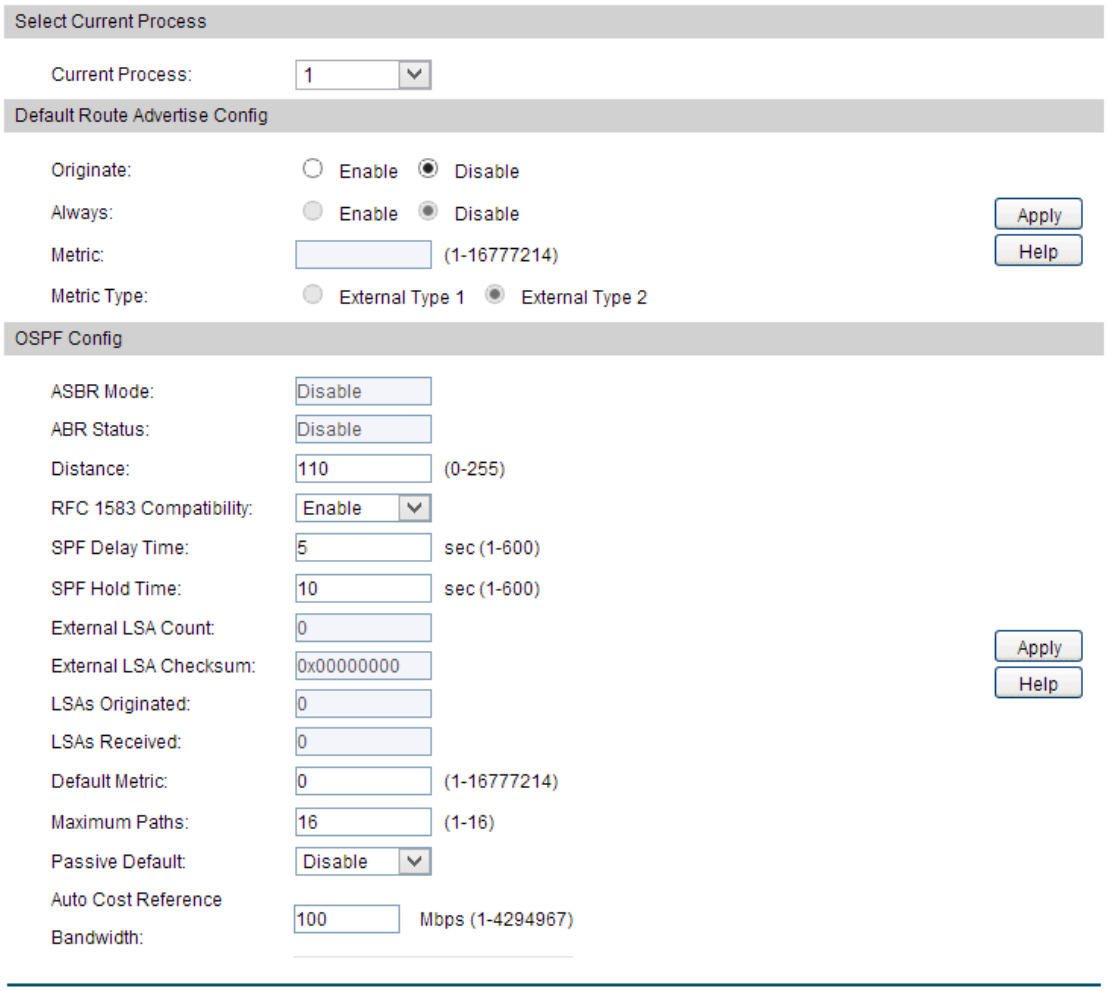


Figure 10-46 OSPF Base

Configuration Procedure:

1) Select a process to configure.
2) Configure the relevant parameters and functions.
3) Click **Apply**.

Entry Description:

➢ **Select Current Process**

Current Process: Select the desired OSPF process for configuration.

➢ **Default Route Advertise Config**

Originate: When this parameter is Enable, OSPF originates an AS-External LSA advertising a default route (0.0.0.0/0.0.0.0).

Always: If Originate is Enable, but the Always option is DISABLE, OSPF will only originate a default route if the router already has a default route in its routing table. Set Always to ENABLE to force OSPF to originate a default route regardless of whether the router has a default route.

Metric: Specify the metric of the default route. The valid value ranges from 1 to 16777214 and the default is 1.

Metric Type: Set the OSPF metric type of the default route. Two types are supported: External Type 1 and External Type 2. The default value is External Type 2.

- **OSPF Config**

ASBR Mode: The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an AS-External LSA advertising the default route.

ABR Status: The router is an Area Border Router if it has active non-virtual interfaces in two or more OSPF areas.

Distance: Specify OSPF route distance. When more than two protocols have routes to the same destination, only the route which have smallest distance will be inserted to IP routing table. The valid value ranges from 0 to 255 and the default is 110.

RFC 1583 Compatibility: Select the preference rules that will be used when choosing among multiple AS-external LSAs advertising the same destination. If you select Enable, the preference rules will be those defined by RFC 1583. Else the preference rules will be those defined in RFC 2328, which will prevent routing loops when AS-external LSAs for the same destination have been originated from different areas. All routers in the OSPF domain must be configured the same. The default value is 'Enable'.

SPF Delay Time: The number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. The valid value ranges from 1 to 600 seconds and the default is 5.

SPF Hold Time: The minimum time in seconds between two consecutive SPF calculations. The valid value ranges from 1 to 600 seconds and the default is 10.

External LSA Count: The number of AS-External LSAs in the link state database.

External LSA Checksum: The sum of the LS checksums of the AS-External LSAs contained in the link-state database.

LSAs Originated: This value represents the number of LSAs originated by this router.

LSAs Received:	The number of LSAs received from other routers in OSPF domain.
Default Metric:	Set a default for the metric of redistributed routes. The valid value ranges from 1 to 16777214.
Maximum Paths:	Set the number of paths that OSPF can report for a given destination. The valid value ranges from 1 to 16 and the default is 16.
Reference Bandwidth:	Specify the reference bandwidth in megabits per second. The valid value ranges from 1 to 4294967 Mbps and the default is 100Mbps.
Passive Default:	Configure the global passive mode settings for all OSPF interfaces. Configuring this field will overwrite any present interface level passive mode settings. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks. The default value is 'Disable'.

10.9.3 Network

You can configure networks contained by an area on this page. The interfaces, whose IP address fall into the networks, will be imported to the associated area.

Choose the menu **Routing→OSPF→Network** to load the following page.

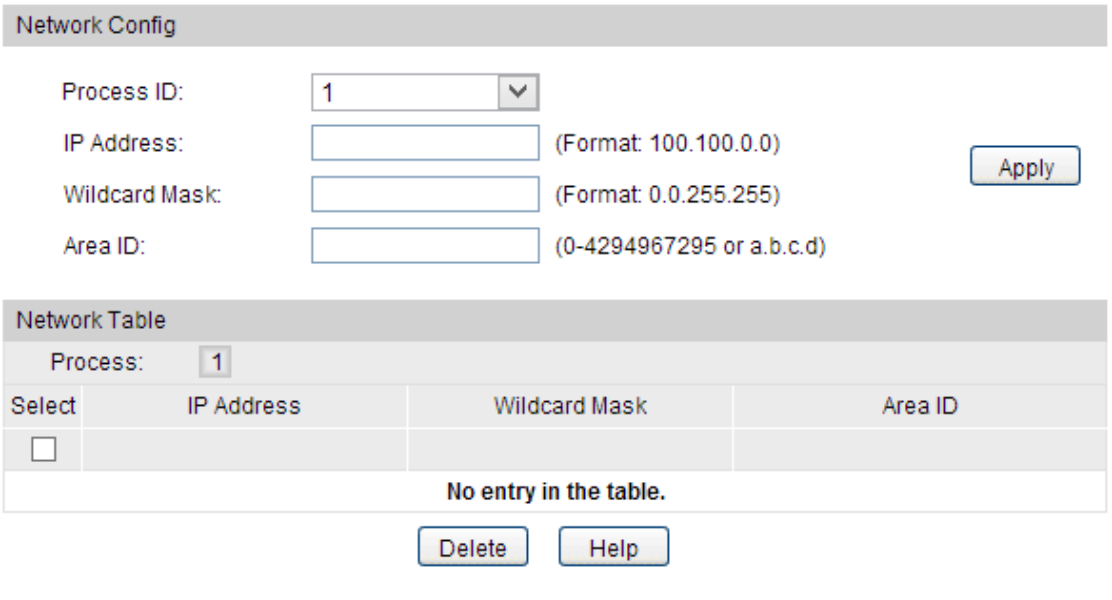


Figure 10-47 OSPF Network

Configuration Procedure:

1) Select a process to configure.
2) Configure the IP address, wildcard mask and area ID.
3) Click **Apply**.

Entry Description:

- **Network Config**

Process ID: Select the desired OSPF process for configuration.

IP Address: The IP address of the network.

Wildcard Mask: The wildcard mask of the network. Normal subnet mask is also supported.

Area ID: The 32 bit unsigned integer that uniquely identifies the area to which a router interface connects. If you assign an Area ID which does not exist, the area will be created with default values. It can be in decimal format or dotted decimal format.

- **Network Table**

Process: Select one OSPF Process to display its network list.

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

IP Address: Displays the IP address of the network.

Wildcard Mask: Displays the wildcard mask of the network.

Area ID: Displays the area to which the network belongs.

10.9.4 Interface

Choose the menu **Routing→OSPF→Interface** to load the following page.

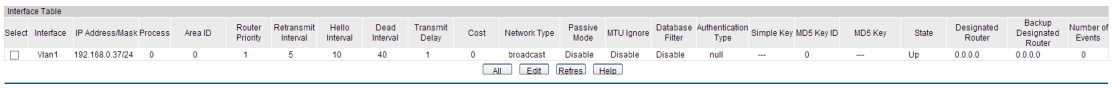


Figure10-48 OSPF Interface

Entry Description:

- **Interface Table**

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

Interface: The interface for which data is to be displayed or configured.

IP Address/Mask: The IP address and subnet mask of the interface.

Process: The process to which the interface belongs.

Area ID: The area to which a router interface connects.

Router Priority: The router priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network. The default is 1.

Retransmit Interval: The retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. The valid value ranges from 1 to 65535 seconds and the default is 5 seconds.

Hello Interval: The hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 10 seconds.

Dead Interval: The dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 40.

Transmit Delay: The Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid value ranges from 1 to 65535 seconds and the default is 1 second.

Cost: The link cost. OSPF uses this value in computing shortest paths. The valid value ranges from 1 to 65535.

Network Type: The OSPF network type on the interface. The default network type for Ethernet interfaces is broadcast.

Passive Mode: Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.

MTU Ignore: Disables OSPF MTU mismatch detection on received database description packets. Default value is Disable (MTU mismatch detection is enabled).

Database Filter: To prevent outgoing link-state advertisements (LSAs) flooding out of an OSPF interface. The default is Disable, all outgoing LSAs are flooded out of the interface.

Authentication Type: Displays the authentication type of the interface. One of the following:

- **null**: No authentication.
- **simple**: Use simple password.
- **md5**: Use md5 message-digest algorithm.

Simple Key: Displays the active simple password of the interface.

MD5 Key ID: Displays the active MD5 key ID of the interface.

MD5 Key: Displays the active MD5 key of the interface.

State: Displays the current state of the selected router interface. One of the following:

- **Down:** This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.
- **Loopback:** In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router-LSAs as single host routes, whose destination is the interface IP address.
- **Waiting:** The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
- **DR:** This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a Network LSA for the network node. The Network LSA will contain links to all routers (including the Designated Router itself) attached to the network.
- **BDR:** This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
- **DR Other:** The interface is connected to a broadcast on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

Designated Router: The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router.

Backup Designated Router: The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router.

Number of Events: This is the number of times the specified OSPF interface has changed its state.

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

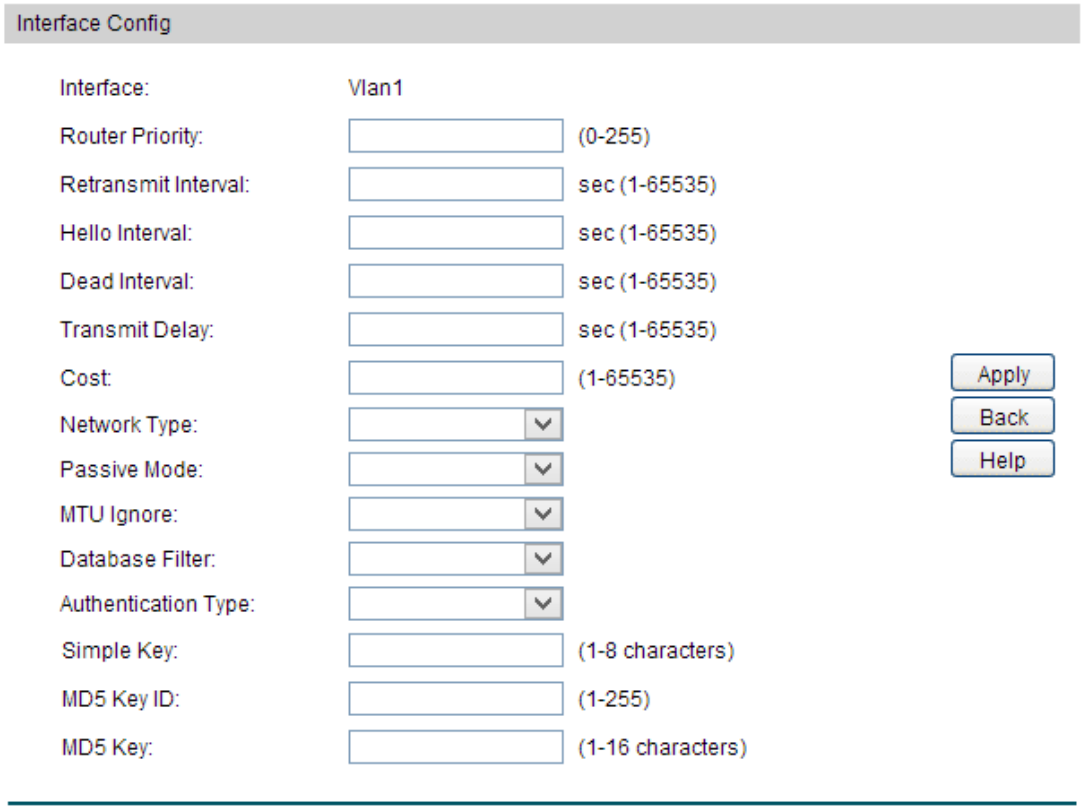


Figure 10-49 Interface Config

Configuration Procedure:

1) Configure the OSPF parameters of the interface.
2) Click **Apply**.

Entry Description:

➢ **Interface Config**

Interface: Displays the interface ID for configuration.

Router Priority: The router priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network. The default is 1.

Retransmit Interval:	The retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. The valid value ranges from 1 to 65535 seconds and the default is 5 seconds.
Hello Interval:	The hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 10 seconds.
Dead Interval:	The dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 40 seconds.
Transmit Delay:	The Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid value ranges from 1 to 65535 seconds and the default is 1 second.
Cost:	The link cost. OSPF uses this value in computing shortest paths. The valid value ranges from 1 to 65535.
Network Type:	Sets the OSPF network type. The default network type for Ethernet interfaces is broadcast.
Passive Mode:	Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.
MTU Ignore:	Disables OSPF MTU mismatch detection on received database description packets. Default value is Disable (MTU mismatch detection is enabled).
Database Filter:	To prevent outgoing link-state advertisements (LSAs) flooding out of an OSPF interface. The default is Disable, all outgoing LSAs are flooded out of the interface.
Authentication Type:	The authentication type of interface. The choices are: • **null**: No authentication. • **simple**: Use simple password. • **md5**: Use md5 message-digest algorithm.
Simple Key:	Displays the active simple password of the interface.
MD5 Key ID:	Displays the active MD5 key ID of the interface.
MD5 Key:	Displays the active MD5 key of the interface.

10.9.5 Area

Choose the menu **Routing→OSPF→Area** to load the following page.

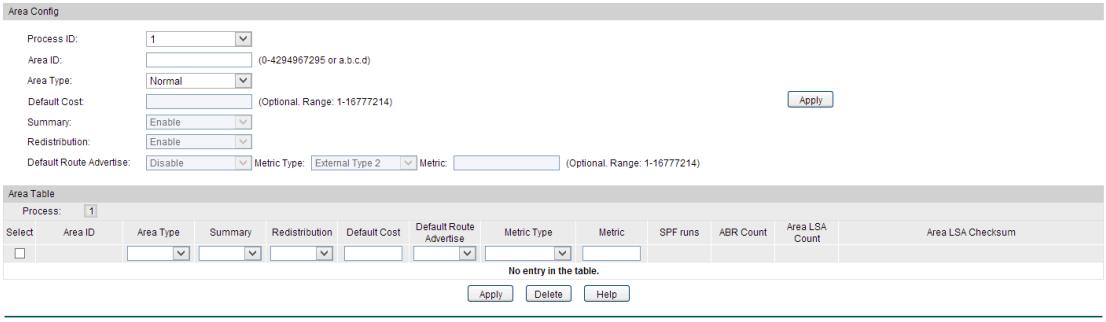


Figure10-50 OSPF Area

Configuration Procedure:

1) Select a process, and configure the OSPF parameters of the area.

2) Also you can selelct an entry in the Area Table, and change the configuration of the area.

3) Click **Apply**.

Entry Description:

➢ **Area Config**

Process ID:	Select the desired OSPF process for configuration.
Area ID:	The 32 bit unsigned integer that uniquely identifies the area. It can be in decimal format or dotted decimal format.
Area Type:	OSPF area type: Normal, Stub, or NSSA.
Default Cost:	The metric value you want to apply for the default Summary-LSA advertised into the stub area. The valid value ranges from 1 to 16777214.
Summary:	Set whether or not the specified Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas. It is always Enable in Normal areas. The default is Enable.
Redistribution:	Set whether or not the external routes will be redistributed to the area. It is always Enable in Normal areas and always Disable in Stub areas.
Default Route Advertise:	Enable or disable advertising default route (0.0.0.0/0.0.0.0) into NSSA area by sending a NSSA-External LSA. It is only available in NSSA area.
Metric Type:	Set the OSPF metric type of the default route. Two types are supported: External Type 1 and External Type 2. The default value is External Type 2.
Metric:	Specify the metric of the default route. The valid value ranges from 1 to 16777214 and the default is 1.

- **Area Table**

Process:	Select one OSPF Process to display its area list.
Select:	Select the desired item for configuration. It is multi-optional.
Area ID:	Displays the configured area.
Area Type:	Displays the type of the area and it can be modified.
Summary:	Displays the Summary parameter and it can be modified.
Redistribution:	Displays the Redistribution parameter and it can be modified.
Default Cost:	Displays the stub cost of the area and it can be modified.
Default Route Advertise:	Displays the Default Route Advertise status and it can be modified.
Metric Type:	Displays the type of default route and it can be modified.
Metric:	Displays the metric of default route and it can be modified.
SPF runs:	Displays the number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
ABR Count:	Displays the total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count:	Displays the total number of link-state advertisements in this area's link-state database, excluding AS-External LSAs.
Area LSA Checksum:	Displays the 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers.

10.9.6 Area Aggregation

You can configure address ranges for an area on this page. The address range is used to consolidate or summarize routes for an area at an area boundary. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries, a single route is advertised for each address range.

Choose the menu **Routing→OSPF→Area Aggregation** to load the following page.

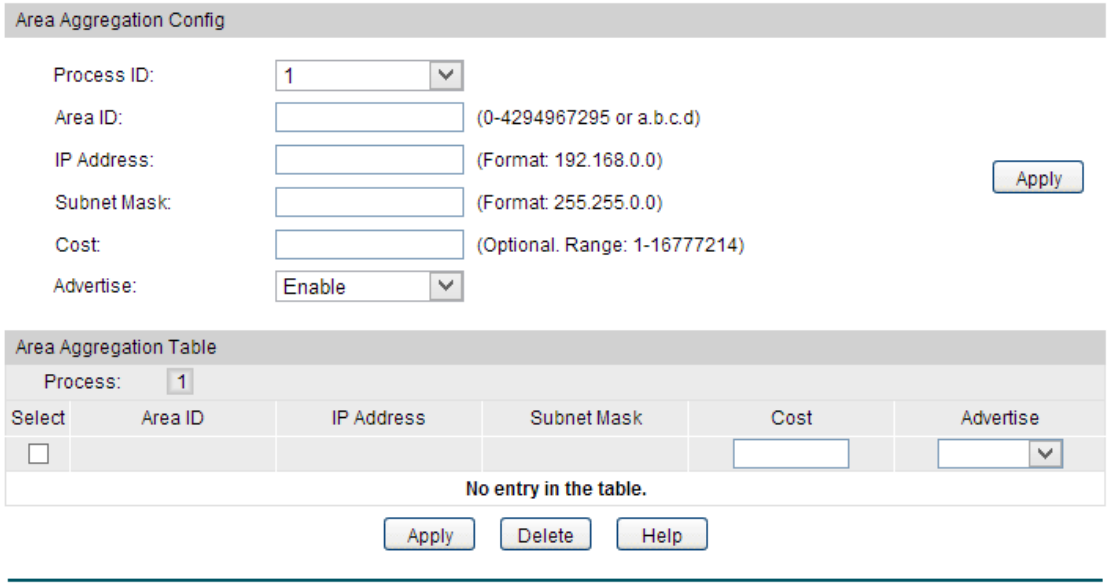


Figure10-51 OSPF Area Aggregation

Configuration Procedure:

1) Select a process.
2) Configure the relevant parameters.
3) Click **Apply**.

Entry Description:

➢ **Area Aggregation Config**

Process ID:	Select the desired OSPF process for configuration.
Area ID:	The 32 bit unsigned integer that uniquely identifies the area. It can be in decimal format or dotted decimal format.
IP Address:	The IP address of the address range.
Subnet Mask:	The subnet mask of the address range.
Cost:	Specify the path cost to the address range. If not specified, it will be dynamic calculated by OSPF. The valid value ranges from 1 to 16777214.
Advertise:	Set whether or not the area address range will be advertised outside the area via a Network-Summary LSA. The default is Enable.

➢ **Area Aggregation Table**

Process: Select one OSPF Process to display its address range list.

Area ID: Displays the area to which the address range belongs.

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

IP Address: Displays the IP address of the address range.

Subnet Mask: Displays the subnet mask of the address range.

Cost: Displays the path cost to the address range and it can be modified.

Advertise: Displays the Advertise parameter and it can be modified.

10.9.7 Virtual Link

Choose the menu **Routing→OSPF→Virtual Link** to load the following page.

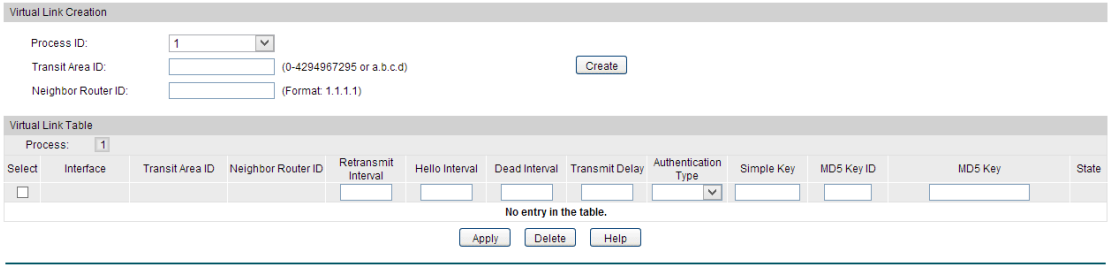


Figure10-52 Virtual Link

Configuration Procedure:

1) Select a process.
2) Configure the relevant parameters.
3) Click **Apply**.

Entry Description:

➢ **Virtual Link Creation**

Process ID: Select the desired OSPF process for configuration.

Transit Area ID: The ID of the transit area. Virtual links can be configured between any pair of area border routers having interfaces to a common (non-backbone) area. Here the common area is named Transit Area.

Neighbor Router ID: The router ID of the neighbor portion of a virtual link.

➢ **Virtual Link Table**

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

Interface: Displays the virtual interface. When you create a virtual link, actually a virtual interface is created.

Transit Area ID: Displays the transit area ID of the virtual link.

Neighbor Router ID: Displays the neighbor router ID of the virtual link.

Retransmit Interval: The retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. The valid value ranges from 1 to 65535 seconds and the default is 5 seconds.

Hello Interval: The hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 10 seconds.

Dead Interval: The dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 40.

Transmit Delay: The Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid value ranges from 1 to 65535 seconds and the default is 1 second.

Authentication Type: You may select an authentication type other than none by clicking on the 'Authentication Type' button. The choices are:

- **null**: No authentication.
- **simple**: Use simple password.
- **md5**: Use md5 message-digest algorithm.

Simple Key: Displays the active simple password of the interface.

MD5 Key ID: Displays the active MD5 key ID of the interface.

MD5 Key: Displays the active MD5 key of the interface.

State: Displays the current state of the selected router interface. One of:

- **Down:** This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.
- **P2P:** In this state, the interface is operational, and connects either to a physical point-to-point network or to a virtual link. Upon entering this state, the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.

10.9.8 Route Redistribution

Choose the menu **Routing→OSPF→Route Redistribution** to load the following page.

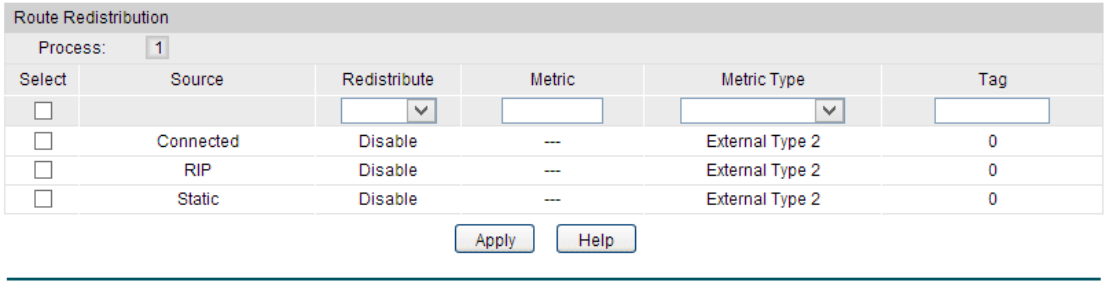


Figure10-53 Route Redistribution

Configuration Procedure:

1) Select a Source to be enabled with Route Redistribution.
2) Enable Route Redistribution and configure the relevant parameters.
3) Click **Apply**.

Entry Description:

➢ **Route Redistribution**

Process: Select one OSPF Process to display its route redistribution list.

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

Source: The available source routes for redistribution by OSPF. The valid values are 'Static', 'RIP', 'Connected', and other OSPF processes.

Redistribute: This option enables or disables the redistribution for the selected source protocol.

Metric: Set the metric value to be used as the metric of redistributed routes. The valid value ranges from 1 to 16777214 and the default is equal to Default Metric configured on Basic page.

Metric Type: Set the OSPF metric type of redistributed routes. The default is External Type 2.

Tag: Set the tag field in routes redistributed. The valid value ranges from 0 to 4294967295 and the default is 0.

10.9.9 Neighbor Table

Choose the menu **Routing→OSPF→Neighbor Table** to load the following page.

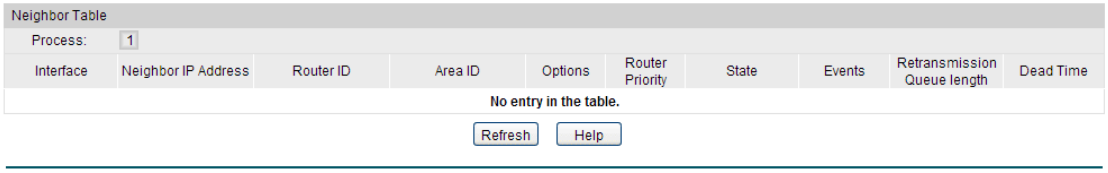


Figure10-55 Neighbor Table

Entry Description:

➢ **Neighbor Table**

Process: Select one OSPF Process to display its neighbor list.

Interface: Displays the interface for which neighbor list is to be displayed.

Neighbor IP Address: The IP address of the neighboring router's interface to the attached network.

Router ID: A 32 bit integer in dotted decimal format representing the neighbor.

Area ID: The area ID of the OSPF area associated with the interface.

Options: An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets.

Router Priority: The router priority of the neighbor.

State: The state of the neighbor:

- Down: This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to 'Down' neighbors, although at a reduced frequency.
- Attempt: This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval.
- Init: In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface.
- 2-Way: In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater.
- ExStart: This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
- Exchange: In this state the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.
- Loading: In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
- Full: In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in Router LSAs and Network LSAs.

Events: The number of times this neighbor relationship has changed state, or an error has occurred.

Retransmission Queue length:	An integer representing the current length of the retransmission queue of the specified neighbor router ID of the specified interface.
Dead Time:	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

10.9.10 Link State Database

Choose the menu **Routing→OSPF→Link State Database** to load the following page.

Figure10-56 Link State Database

Entry Description:

- **Link State Database**

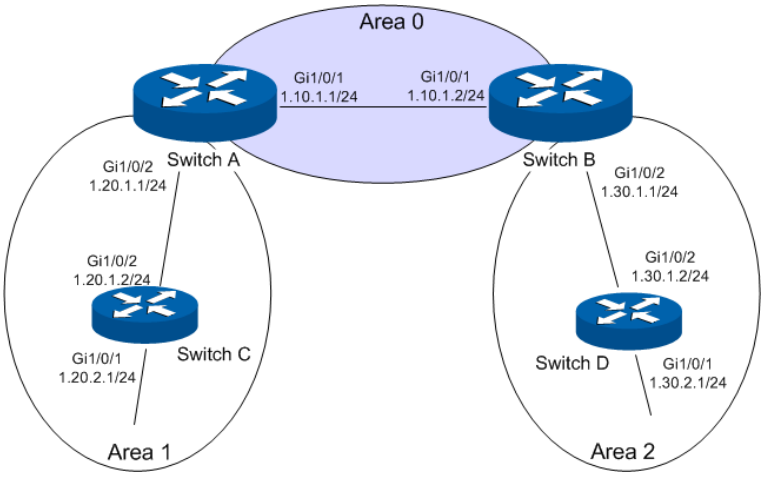
Process:	Select one OSPF Process to display its link state database.
Area ID:	Displays the ID of the area to which the LSA belongs.
Advertising Router:	Displays the ID of the router that advertising the LSA.
LSA Type:	The format and function of the link state advertisement. One of the following: Router, Network, Network-Summary, ASBR-Summary, External (Type 5), NSSA-External (Type 7).
Link State ID:	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age:	The time since the link state advertisement was first originated, in seconds.
Sequence:	The sequence number field is an unsigned 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum:	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
Options:	The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement.

10.9.11 Application Example for OSPF

➢ **Network Requirements**

1. The AS is divided into three areas and all switches in the AS run OSPF.
2. Switch A and Switch B act as ABRs to forward routing information between areas.
3. Each switch can learn routing information to all the network segments in the AS after the configuration.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch A

Step	Operation	Description
1	Create routing interfaces and their IP addresses	Required. On page **Routing→Interface→Interface Config**, create routed port 1/0/1 with the IP 1.10.1.1/24 and routed port 1/0/2 with the IP 1.20.1.1/24.
2	Create OSPF process	Required. On page **Routing→OSPF→Process**, Create OPSF process 1 and configure the Router ID as 1.1.1.1.
3	Create networks in the area	Required. On page **Routing→OSPF→Network**, configure network 1.10.1.0/24 in area 0 and configure network 1.20.1.0/24 in area 1.
4	Configure area aggregation	Optional. On page **Routing→OSPF→Area Aggragation**, configure the aggregation address as 1.20.0.0/16 in area 1.

- Configure Switch B

Step	Operation	Description
1	Create routing interfaces and their IP addresses	Required. On page **Routing→Interface→Interface Config**, create routed port 1/0/1 with the IP 1.10.1.2/24 and routed port 1/0/2 with the IP 1.30.1.1/24.

2	Create OSPF process	Required. On page **Routing→OSPF→Process**, Create OPSF process 1 and configure the Router ID as 2.2.2.2.
3	Create networks in the area	Required. On page **Routing→OSPF→Network**, configure network 1.10.1.0/24 in area 0 and configure network 1.30.1.0/24 in area 2.
4	Configure area aggregation	Optional. On page **Routing→OSPF→Area Aggragation**, configure the aggregation address as 1.30.0.0/16 in area 2.

- Configure Switch C

Step	Operation	Description
1	Create routing interfaces and their IP addresses	Required. On page **Routing→Interface→Interface Config**, create routed port 1/0/1 with the IP 1.20.2.1/24 and routed port 1/0/2 with the IP 1.20.1.2/24.
2	Create OSPF process	Required. On page **Routing→OSPF→Process**, Create OPSF process 1 and configure the Router ID as 3.3.3.3.
3	Create networks in the area	Required. On page **Routing→OSPF→Network**, configure network 1.20.0.0/16 in area 1.

- Configure Switch D

Step	Operation	Description
1	Create routing interfaces and their IP addresses	Required. On page **Routing→Interface→Interface Config**, create routed port 1/0/1 with the IP 1.30.2.1/24 and routed port 1/0/2 with the IP 1.30.1.2/24.
2	Create OSPF process	Required. On page **Routing→OSPF→Process**, Create OPSF process 2 and configure the Router ID as 4.4.4.4.
3	Create networks in the area	Required. On page **Routing→OSPF→Network**, configure network 1.30.0.0/16 in area 2.

10.10 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. Generally, all hosts in a LAN (Local Area Network) would set a default route. Packets which are sent by the host and whose destination address does not belong to the local network segment will be sent to the gateway via the default route. Therefore, communication between the host and external network can be established. Once the gateway fails, all hosts of this network segment whose default next hop is the gateway will stop communicating with external network.

VRRP is developed to solve the problem mentioned above and designed for LAN with multicast or broadcast function, such as Ethernet. Virtual router acts as a backup group which consists of one master router and several backup routers.

The virtual router (also a backup group) has its own IP address. This IP address can be the same as the interface address of any router in the backup group. In this case, the virtual router is also called IP address owner. All physical routers in the backup group have their own IP addresses. Hosts in LAN only recognize the IP address of the virtual router, but not that of the master router or backup routers. The IP address of the virtual router is assigned as the default gateway for the participating routers. Hosts in LAN communicate with external network via the virtual router. Once the master router in backup group fails, another router will be selected to replace it from the backup group through election protocol and thus provides routing service for hosts. Therefore, communication between hosts and external network can be established without interruption.

- **Advantages of VRRP**

VRRP owns the following advantages:

1. Simplified network management. In LAN with multicast or broadcast function, such as Ethernet, even though a device fails, with the help of VRRP, highly-reliable default link can still be provided and network interruption can be avoided after a single link fails without reconfiguration of dynamic routing or router discovery protocols, or default gateway configuration on every end-host.
2. Small network overhead. The single message that VRRP defines is the VRRP advertisement, which can only be sent by the master router.

- **Typical Networking Application Diagram**

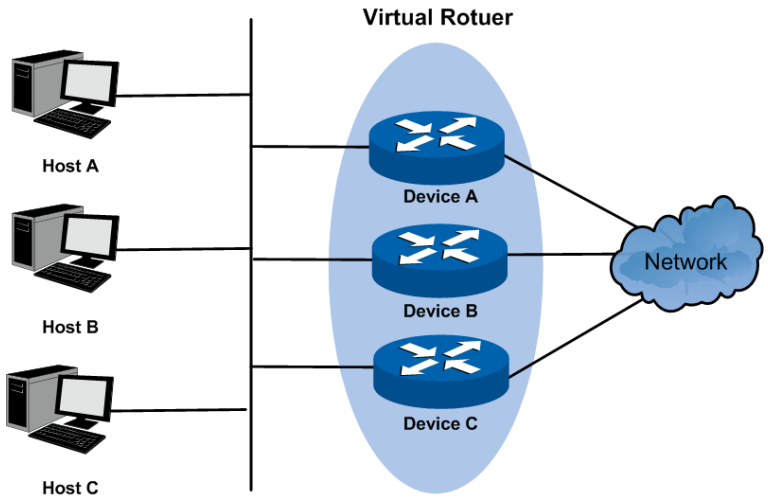


Figure 10-57 Typical Networking Application Diagram

- **VRRP Operating Principle**

1. Working Process

VRRP backup group, or virtual router, consists of a group of physical routers with the same VRID (virtual route identifier). A virtual router owns one or more virtual IP addresses and one virtual MAC address, in the format 00-00-5E-00-01-{VRID}. The IP address of the virtual

router is assigned as the default gateway for the hosts within the LAN. Communication with external network can be realized via the virtual router.

Master router is selected from the physical routers in the virtual router group according to VRRP priority. The elected master router provides routing service to the hosts in LAN, and sends VRRP messages periodically to publicize its configuration information like priority and operating condition to other routers in backup group. Other physical routers in the backup group work as backup routers. They monitor the VRRP packets sent by the master router. A new master router will be elected among them to take the role of the master router if master router fails.

2. Master Election

Initially-created routers work in Backup state and learn other members' priorities in the virtual router via VRRP packets. The one with the highest priority is elected as master router. If the priority values are the same, the router with the highest interface IP address is selected as the master.

- In preemptible mode, when backup router receives VRRP packet, it will compare its priority with that of the advertisement packet. If of higher priority, the backup router will become the master router; otherwise, it will maintain Backup state.
- In non-preemptible mode, physical routers in the backup group will maintain Master or Backup state as long as the master router functions normally. Even if backup router is given higher priority, it cannot become a master router in non-preempt mode.

The VRRP priority ranges from 0 to 255 (the bigger the number is, the higher the priority is). Configurable range is 1-254. The priority value 0 is reserved for the current master when it gives up its role as master router. For example, when master router receives shutdown message, it would send VRRP packet with priority 0 to the backup group which the interface belongs to. The priority of the IP address owner must be 255. Therefore, if there exists an IP address owner in the backup group and it works normally, it must be the master router.

3. State Transition

VRRP defines three state modes: Initialize, Master and Backup. Only in Master state can master router provide service for forwarding request via virtual IP address and forward VRRP packet.

When the system just starts, it comes to Initialize state. If the virtual router is not given a virtual IP address, the system would maintain Initialize state. If the virtual IP address is configured properly, when the system receives startup message from interface, it would transition to the Backup state (in which case its priority is not 255) or Master state (in which case its priority is 255). Routers in master or backup state can change to Initialize state only when they receive shutdown message from interface. In Initialize state, router cannot deal with VRRP packet.

If the master router functions properly, it will periodically send VRRP packets informing backup routers in the backup group that it functions properly. VRRP timer can be manually configured to customize the intervals that master router sends VRRP packet. If the backup router waits for a period longer than three times the advertisement timer and fails to receive VRRP packets from the master router, they will assume that the master router is

dead and initiate an election process by transitioning to the Master state and forwarding VRRP packets.

To avoid frequent Master-Backup state transition among routers in the backup group and provide enough time for backup routers to collect necessary information, backup router would not preempt to be master as soon as it receives packets with lower priority value. It would wait for a certain time, which is called preempt-mode delay time, and then send packets to take place of the former master. Users can customize the preempt-mode delay time.

4. Authentication Methods

VRRP provides three authentication methods:

- No authentication: the eligibility of VRRP packets is not verified and no security insurance is provided. In a safe network, no authentication can be set as authentication method.
- Simple text password: in a network where security is possible to be threatened, simple text password is recommended. The router which forwards the VRRP packets fills the authentication data in the VRRP packets. The router which has received the VRRP packets compares the data with that in local configuration. If they are the same, the VRRP packet received is considered legitimate. If not, it would be considered as illegitimacy.
- MD5 authentication: in a highly-unsecured network, MD5 authentication is recommended. The router which sends the VRRP packets conducts digest operation on VRRP packets using authentication data and MD5 algorithm. The result is saved in Authentication Header. The router which has received the VRRP packet conducts the same digest operation and compares the result with the content in Authentication Header. If they match, the VRRP packet received is considered legitimate. If not, it would be considered as illegitimacy.

➢ **Interface Tracking**

This function enhances the backup function. If interface tracking is enabled, when the master router's other interfaces which are not in this backup group (for example, the uplink interface) fail, it would lower its priority value automatically. Therefore, router with more available interfaces and better performance can be elected as master router; and the stability of backup group is increased.

When the router interface connecting the uplink fails, the backup group cannot recognize uplink breakdown. If this router is in Master state, hosts in the LAN cannot visit external network. This problem can be solved with the help of interface tracking function. When the interface connecting the uplink is down, the router will automatically lower its priority, making priority of other routers in the backup group higher than its priority value. As a result, the backup router with the highest priority becomes master.

➢ **Load Balancing**

One router can work in more than one backup group, which makes it possible that a router can be master router in one backup group and backup router in other backup groups.

Load balancing means multiple routers undertake workloads simultaneously. Therefore, two or more backup groups are needed to realize load balancing. Each backup group consists of one master router and several backup routers. Master router can vary from one backup group to the others.

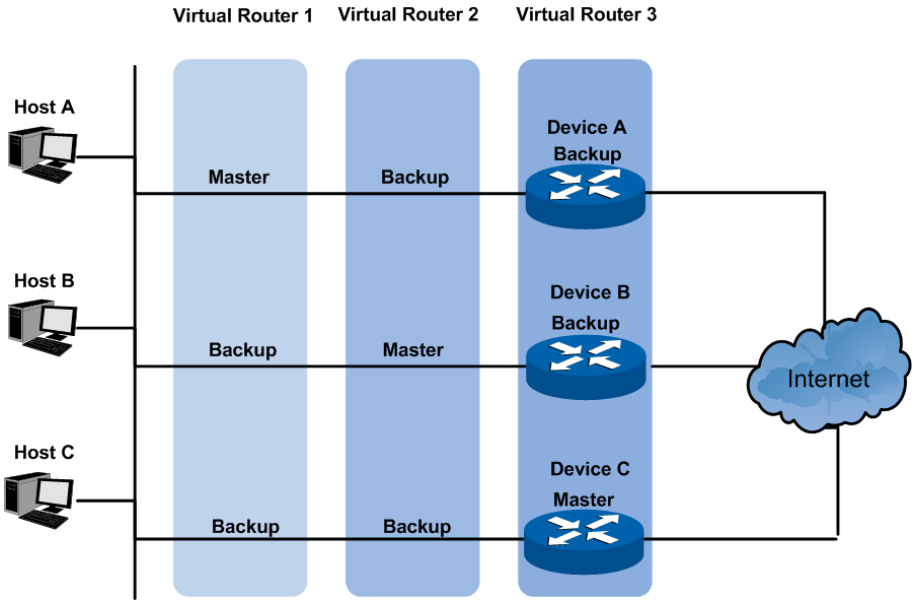


Figure 10-58 VRRP Load Balancing

A router owns different priority in different backup groups when it participates in multiple VRRP backup groups simultaneously.

In Figure 10-58, there exist three backup groups:

- Backup Group 1, corresponding to Virtual Router 1. Device A is the master router; Device B and C are backup routers.
- Backup Group 2, corresponding to Virtual Router 2. Device B is the master router; Device A and C are backup routers.
- Backup Group 3, corresponding to Virtual Router 3. Device C is the master router; Device A and B are backup routers.

To realize the workload balancing among Device A, B and C, the default gateway of the hosts associated with the LAN should be set as Virtual Router 1, 2 and 3 respectively. When it comes to priority configuration, it would be better that the VRRP priority values of the three virtual routers are different in order to prevent one router from being more than one master simultaneously.

➢ **VRRP Configuration**

Before configuring VRRP, users should plan well to specify the role and function of the devices in backup groups. Every switch in backup group should be configured, which is the precondition to construct a backup group.

10.10.1 Basic Config

VRRP (Virtual Routing Redundancy Protocol) is a function on the switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will

forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts.

Choose the menu **Routing** → **VRRP** → **Basic Config** to load the following page.

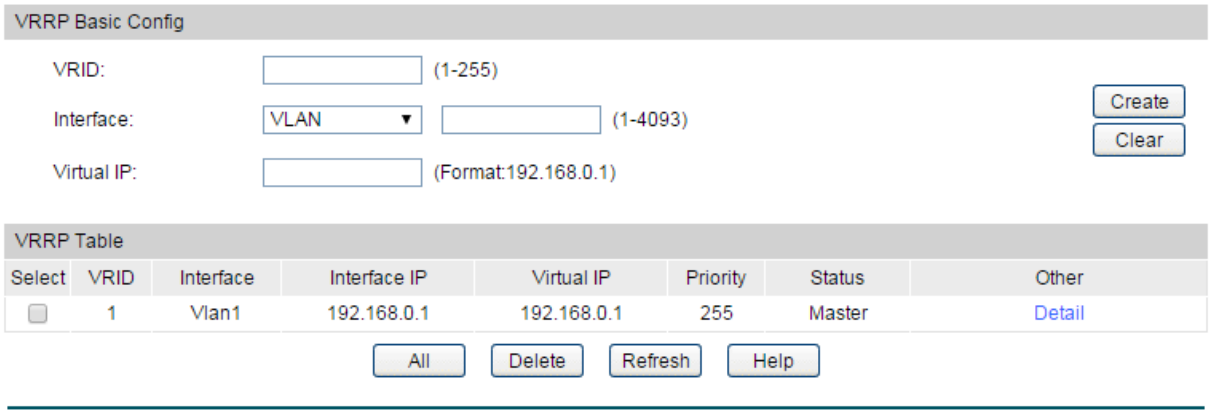


Figure10-59 VRRP Basic Config

Configuration Procedure:

1) Enter the VRID to identify the VRRP group.
2) Select an interface and assign a virtual IP address for the VRRP group.
3) Click **Create**.

Entry Description:

- **VRRP Basic Config**

VRID:	Enter the VRID only if you are creating a new VRRP group. The VRID ranges from 1 to 255.
Interface:	Select the VLAN interface ID or router interface ID for the new VRRP group.
Virtual IP:	Assign a virtual IP address for the new VRRP group. It must be on the same network segment as the IP address of the interface where the VRRP group is configured.
Create:	Click the button to add a new VRRP group.
Clear:	Click the button to clear the configuration.

- **VRRP Table**

Select:	Select one or more items.
VRID:	Displays the VRID associated with the VRRP group.
Interface:	Displays the Interface ID associated with the VRRP group.
Interface IP:	Displays the IP Address associated with the selected interface.

Virtual IP:	Displays the primary Virtual IP associated with the VRRP group.
Priority:	Displays the priority associated with the VRRP group.
Status:	Displays the status associated with the VRRP group.
Other:	Displays more information about the VRRP group.
All:	Select all the VRRP items.
Delete:	Delete the selected items.
Refresh:	Update the status of the VRRP items.

Click **Detail** to view the detailed information of the specified VRRP group. If you do not configure the tracked interface, the track information will not display here.

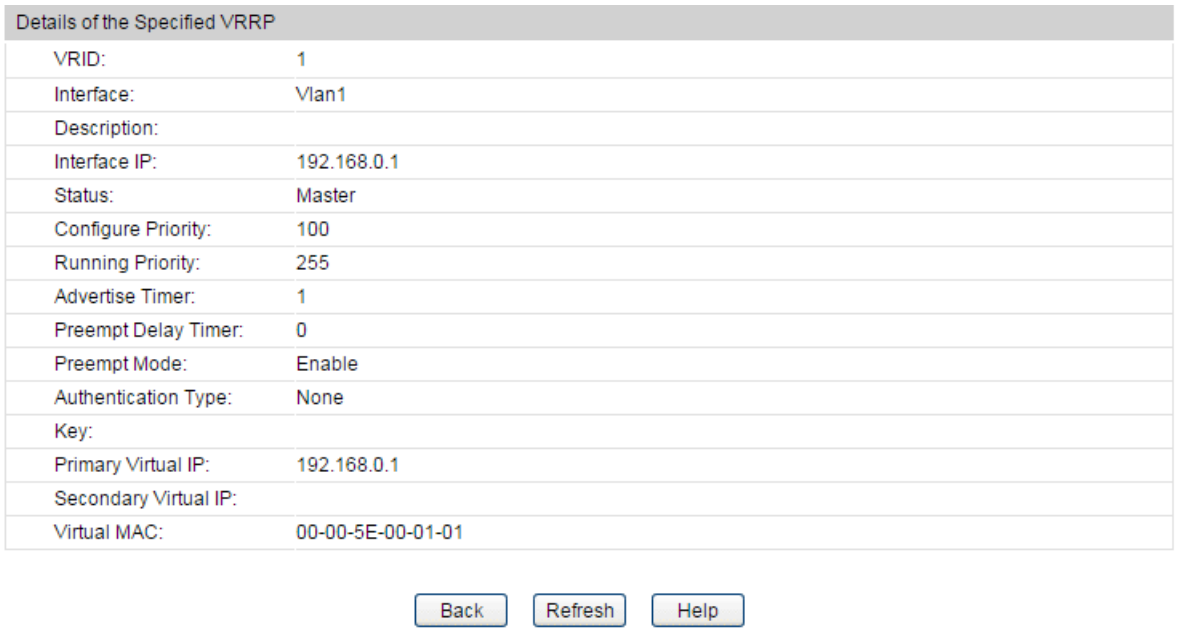


Figure 10-60 Detailed Specified VRRP Information

Entry Description:

VRID:	Displays the VRID associated with the VRRP group.
Interface:	Displays the Interface ID associated with the VRRP group.
Description:	Displays the description associated with the VRRP group.
Interface IP:	Displays the IP Address associated with the selected interface.
Status:	Displays the status associated with the VRRP group.
Configure Priority:	Displays the configured priority associated with the VRRP group. It ranges from 1 to 255.

Running Priority:	Displays the running priority associated with the VRRP group. It ranges from 1 to 255.
Advertise Timer:	Displays the advertise timer associated with the VRRP group. It ranges from 1 to 255.
Preempt Delay Timer:	Displays the preempt delay timer associated with the VRRP group. It ranges from 0 to 255.
Preempt Mode:	Displays the preempt mode associated with the VRRP group.
Authentication Type:	Displays the authentication type associated with the VRRP group.
Key:	Displays the key associated with authentication type. If the authentication type is 'normal', it will display '--'.
Primary Virtual IP:	Displays the primary virtual IP associated with the VRRP group.
Virtual MAC:	Displays the Virtual MAC address associated with the VRRP group.
Tracked Interface:	Displays the tracked interface ID.
Reduced Priority:	Displays the reduced priority when the tracked interface is 'down'.
Back:	Click the button to go back to the VRRP Basic Config page.
Refresh:	Click the button to refresh this page.

10.10.2 Advanced Config

You can modify most of features of the VRRP on this page, including the description, priority, preempt mode, advertisement. But you cannot add or delete a VRRP group.

Choose the menu **Routing** → **VRRP** → **Advanced Config** to load the following page.

Figure10-61 VRRP Advanced Config

Configuration Procedure:

Select your desired VRRP group and configure corresponding parameters according to your needs. Then click **Apply**.

Entry Description:

Select:	Select one or more items.

VRID: Displays the VRID associated with the VRRP group.

Interface: Displays the Interface ID associated with the VRRP group.

Description: Give a description for the VRRP group. It can contain up to 8 characters. Only numbers, letters, and underlines are allowed.

Priority: Set the priority for the device associated with the VRRP group. It ranges from 1 to 254. The one with greater value owns the higher priority.

Advertise Timer: Specify the interval at which the VRRP packets are sent. It ranges from 1 to 255 seconds.

Preempt Mode: With this option enabled, a backup router will preempt the master status if it has a priority greater than the current master router's priority. By default, it is enabled.

Delay Time: Specify the time that a backup router has to wait for before setting itself as the master when the current master is considered to be unavailable. It ranges from 0 to 255 seconds.

Authentication: Select the authentication type for the Virtual Router. By default, it is None.

- None: No authentication will be performed.
- Simple: Authentication will be performed using a text password.
- MD5: Authentication of MD5 will be performed using a text password. This authentication mode has a higher security than Simple mode.

Key: If you select Simple or MD5 as authentication mode, enter the key.

10.10.3 Virtual IP Config

You can configure virtual IP for the virtual routers on this page. The virtual IP must be in the subnet of an interface corresponding with the virtual router, can be added, deleted or modified for the special virtual router.

Choose the menu **Routing** → **VRRP** → **Virtual IP Config** to load the following page.

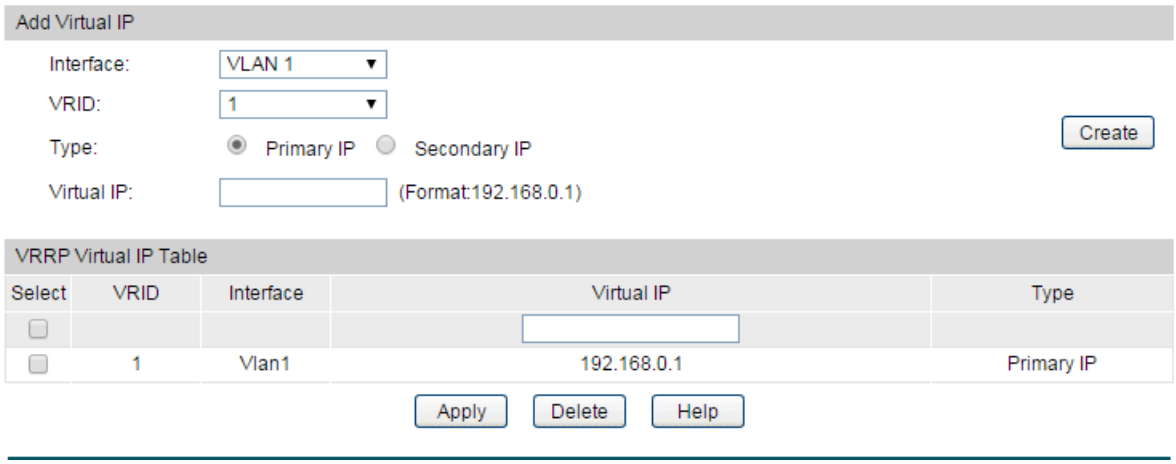


Figure10-62 Virtual IP Config

Configuration Procedure:

Select the interface and VRID associated with your desired VRRP group and add one or more virtual IP addresses for the VRRP group. Then Click **Create**.

Entry Description:

- **Add Virtual IP**

Interface:	Select the interface associated with your desired VRRP group.
VRID:	Select the VRID associated with your desired VRRP group.
Type:	Set the type of the virtual IP address.
Virtual IP:	Add an IP address for the VRRP group. You can add up to 32 virtual IP addresses associated with the VRRP group.

- **VRRP Virtual IP Table**

Select:	Select one or more items.
VRID:	Displays the VRID associated with the VRRP group.
Interface:	Displays the Interface ID associated with the VRRP group.
Virtual IP:	Displays the virtual IP address associated with the VRRP group.
Type:	Displays the type of the virtual IP address.

Note:

Up to 32 virtual IPs can be configured for each VRRP group.

10.10.4 Track Config

You can configure track information for virtual routers. When the uplink interface of the master router is down, service will be interrupted since VRRP cannot detect the status change of interfaces outside the VRRP group. You can configure interface tracking to track the uplink interface. In this way, the priority of the master router can be reduced when the tracked interface is down, and the backup router will take over traffic. This ensures continuity for network communication.

Choose the menu **Routing** → **VRRP** → **Track Config** to load the following page.

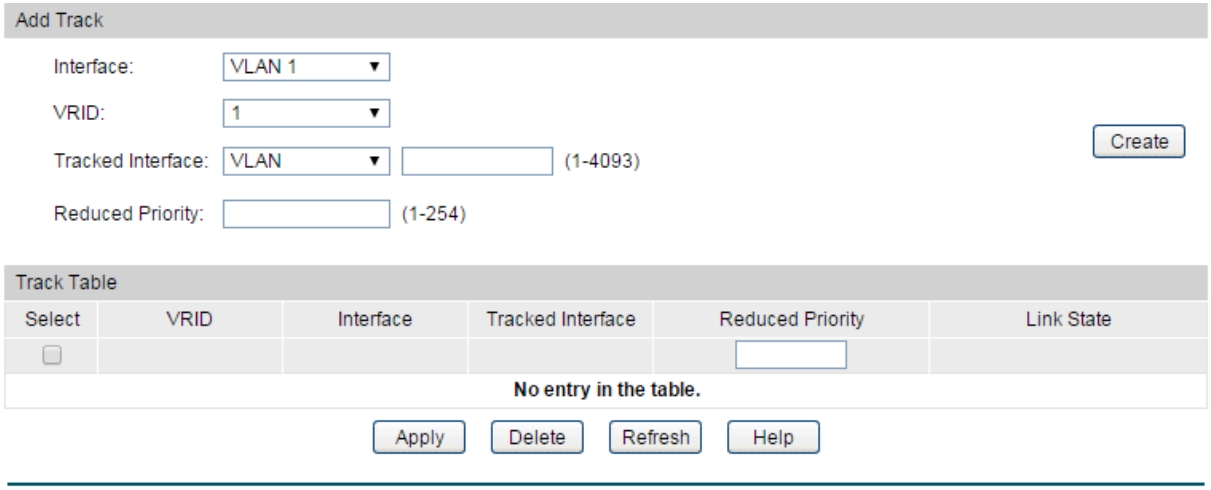


Figure10-63 Track Config

Configuration Procedure:

Select the interface and VRID associated with your desired VRRP group and add track information for the VRRP group. Then Click **Create**.

Entry Description:

- **Add Track**

Interface:	Select the interface associated with your desired VRRP group.
VRID:	Select the VRID associated with your desired VRRP group.
Tracked Interface:	Specify the interface to be tracked.
Reduced Priority:	Specify the priority to reduce if the tracked interface is down. After reducing this value, the priority of the master router should be smaller than the priority of the backup router.

- **Track Table**

Select:	Select one or more items.
VRID:	Displays the VRID associated with your desired VRRP group.

Interface: Displays the Interface ID associated with your desired VRRP group.

Tracked Interface: Displays the Interface ID tracked by the VRRP group.

Reduced Priority: Displays the reduced priority associated with the interface tracked by the VRRP group.

Link State: Displays the status of the interface tracked by the VRRP group.

Apply: Change the selected reduced priority. A new reduced priority should be provided if the **Apply** button is clicked.

Delete: Delete the selected interface.

Refresh: Update the link state of the tracked interface.

Note:

1. IP owner cannot track any interface.
2. Up to 20 interfaces can be tracked for each VRRP group.
3. When tracking the uplink interface, the devices in the VRRP group must work in preemption mode.

10.10.5 Virtual Router Statistics

You can view global and detailed statistics of VRRP groups.

Choose the menu **Routing** → **VRRP** → **Virtual Router Statistics** to load the following page.

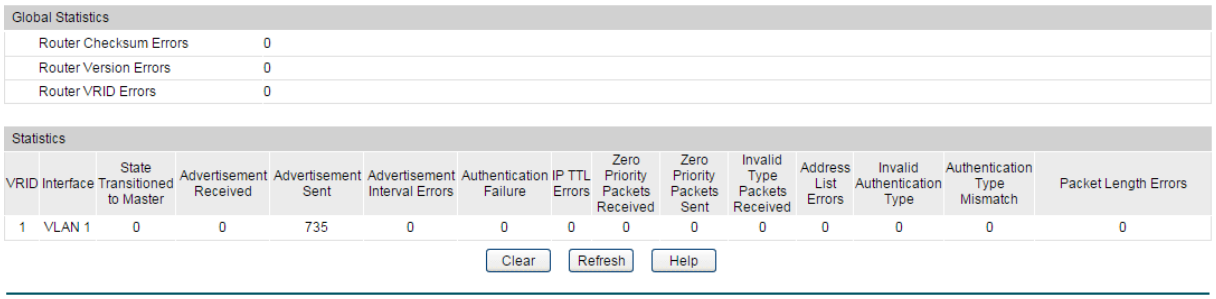


Figure10-64 Virtual Router Statistics

➢ **Global Statistics**

Router Checksum Errors: Displays the total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors: Displays the total number of VRRP packets received with an unknown or unsupported version number.

Router VRID Errors: Displays the total number of VRRP packets received with an invalid VRID for this virtual router.

➢ **Statistics**

Displays specified virtual router statistics. It lists all the statistics for the specified VRRP group and can be reset for your convenience when doing statistics.

VRID:	Displays the VRID associated with your desired VRRP group.
Interface:	Displays the Interface ID associated with your desired VRRP group.
Checksum Errors:	Displays the number of VRRP packets received with an invalid VRRP checksum value.
Version Errors:	Displays the number of VRRP packets received with an unknown or unsupported version number.
State Transitioned to Master:	Displays the number of times that this virtual router's state has transitioned to Master.
Advertisement Received:	Displays the number of VRRP advertisements received by this virtual router.
Advertisement Sent:	Displays the number of VRRP advertisements sent by this virtual router.
Advertisement Interval Errors:	Displays the number of the received VRRP advertisement packets whose advertisement interval was different from the one configured for the local virtual router.
Authentication Failure:	Displays the number of VRRP packets received that did not pass the authentication check.
IP TTL Errors:	Displays the number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
Zero Priority Packets Received:	Displays the number of VRRP packets received by the virtual router with a priority of '0'.
Zero Priority Packets Sent:	Displays the number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received:	Displays the number of VRRP packets received by the virtual router with an invalid value in the 'type' field.
Address List Errors:	Displays the number of packets received for which the address list does not match the locally configured list for the virtual router.
Invalid Authentication Type:	Displays the number of packets received with an unknown authentication type.
Authentication Type Mismatch:	Displays the number of packets received with an authentication type different to the locally configured authentication method.
Packet Length Errors:	Displays the number of packets received with a packet length less than the length of the VRRP header.
Clear:	Clear the statistics displayed on the web.
Refresh:	Refreshes the web page to show the latest VRRP information.

Configuration Procedure：

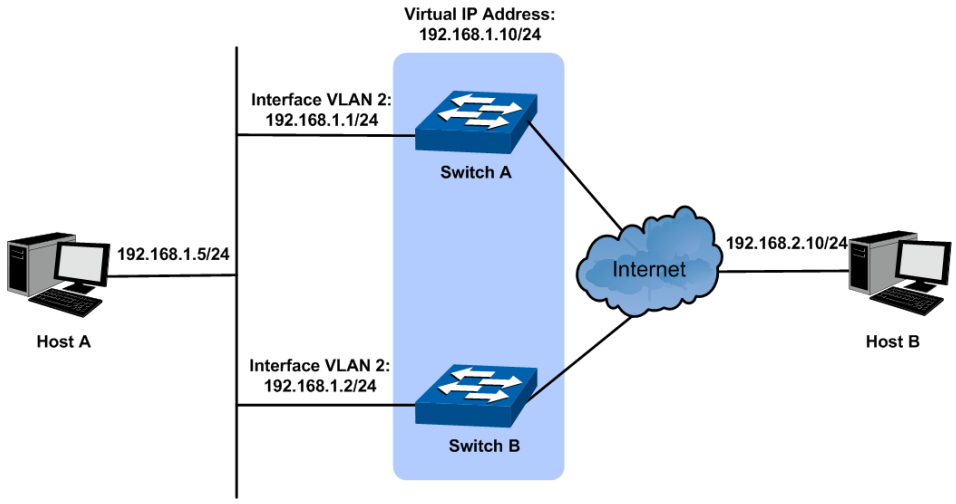
Steps	Operation	Note
1	Configure interface and its IP address.	Required. On page **Routing** → **Interface** → **Interface Config**, create a routing interface (either interface VLAN or routed port) and specify its IP address and subnet mask.
2	Add port to the interface.	Required. On page **VLAN** → **802.1Q VLAN** → **VLAN Config**, add the port connected to the client to the interface VLAN configured in Step 1.
3	Configure VRID and Virtual IP.	Required. On page **Routing** → **VRRP** → **Basic Config**, configure a VRID and Virtual IP for the interface in Step 1. The Virtual IP and the interface IP should be on the same LAN. The client should configure this Virtual IP as the default gateway.
4	Configure the priority.	Optional. On page **Routing** → **VRRP** → **Advanced Config**, configure the priority value to be used by the VRRP router in the election for the master Virtual Router.
5	Configure the Authentication Type.	Optional. On page **Routing** → **VRRP** → **Advanced Config**, configure the authentication type for the Virtual Router.

10.10.6 Application Example for VRRP

➢ **Network Requirements**

1. Host A needs to access Host B on the Internet. The default gateway of Host A is 192.168.1.10/24.
2. Switch A and Switch B are in the backup group with the Virtual IP address as 192.168.1.10/24.
3. When Switch A works normally, packets sent from Host A to Host B are forwarded by Switch A. When Switch A is down, packets sent from Host A to Host B are forwarded by Switch B.

➢ **Network Diagram**



➢ **Configuration Procedure**

- Configure Switch A

Steps	Operation	Note
1	Configure the interface and its IP address.	On page **Routing** → **Interface** → **Interface Config**, create the interface VLAN2, and configure its IP address as 192.168.1.1 and Subnet Mask as 255.255.255.0.
2	Add port to the interface.	On page **VLAN** → **802.1Q VLAN** → **VLAN Config**, add the port connected to the client to interface VLAN 2.
3	Create the VRRP group	On page **Routing** → **VRRP** → **Basic Config**, create a VRRP group with the VRID as 1, the interface as VLAN 2 and the Virtual IP as 192.168.1.10.
4	Configure VRRP priority	On page **Routing** → **VRRP** → **Advanced Config**, configure the VRRP priority of interface VLAN 2 as 110.

- Configure Switch B

Steps	Operation	Note
1	Configure the interface and its IP address.	On page **Routing** → **Interface** → **Interface Config**, create the interface VLAN2, and configure its IP address as 192.168.1.2 and Subnet Mask as 255.255.255.0.
2	Add port to the interface.	On page **VLAN** → **802.1Q VLAN** → **VLAN Config**, add the port connected to the client to interface VLAN 2.
3	Create the VRRP group	On page **Routing** → **VRRP** → **Basic Config**, create a VRRP group with the VRID as 1, the interface as VLAN 2 and the Virtual IP as 192.168.1.10.

Return to CONTENTS

Chapter 11 Multicast Routing

- **Overview of Multicast Routing Protocols**

Note:

The router and router icon mentioned in this chapter represent the router in general or the switch that runs the layer 3 multicast routing protocols.

The multicast routing protocols run in layer 3 multicast devices and they create and maintain multicast routes to forward the multicast packets correctly and efficiently. The multicast routing protocols establish routes for the point-to-multipoint transmissions, known as the multicast distributing tree.

The multicast routing table consists of a group of (S, G) entries, and (S, G) route represents routing information from source S to group G. If no multicast source is specified, the entry will be described as (*, G) with * representing any multicast source. If the router supports multiple multicast routing protocols, its multicast routing table will contain multicast routes generated from multiple protocols.

Multicast routing protocols include protocols as IGMP, PIM, MSDP, DVMRP, and static multicast routing.

The domain mentioned in this guide refers to Autonomous System, which contains a group of routers exchanging routing information with the same routing protocol.

IGMP stands for Internet Group Management Protocol. It is responsible for members management of IP multicast in the TCP/IP, and is used to establish and maintain the multicast member relationships between the IP host and its directly neighboring multicast routers.

PIM (Protocol Independent Multicast) is a typical intra-domain multicast routing protocol among the AS. It provides IP multicast forwarding by leveraging static routes or unicast routing tables generated by any unicast routing protocols, such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) or Border Gateway Protocol (BGP).

MSDP (Multicast Source Discovery Protocol) is an intra-domain multicast resolution which aims at the connection of different PIM SM domains and is used to discover the multicast source information among different ASs.

DVMRP (Distance Vector Multicast Routing Protocol) is mainly applied in the multicast backbone network of the Internet.

The following mainly introduces IGMP, PIM and Static Multicast Routing.

- **Multicast Roles and Models**

There are several different roles in the multicast transmission:

- Multicast Source: The sender of the multicast information.
- Multicast Group Member: All the receivers of the multicast information.
- Multicast Group: The group consists of the multicast group members.

- Multicast Router(or the Layer 3 Multicast Device): The router or switch that supports the layer 3 multicast functions, which contains the multicast routing function and the management function of the multicast group members.

The multicast model divides into two types depending on whether there is an exact multicast source: ASM (Any-Source Multicast) and SSM (Source-Specific Multicast).

ASM (Any-Source Multicast): In the ASM model, any sender can be a multicast source sending multicast information to a multicast group address, and receivers can join a multicast group identified by the group address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the location of the multicast source in advance. However, they can join or leave the multicast group at any time. At any specified moment, the number of multicast source in the ASM should be no more than one, otherwise network congestion and malfunction of the multicast members may occur.

SSM (Source-Specific Multicast): In the SSM model, the receivers know the exact location of the multicast source. The SSM allows host to specify the multicast sources and it uses the multicast group address range different from that of the ASM. The SSM marks a multicast session with both multicast address and multicast source address, and it builds up dedicated multicast forwarding path for the receiver and its specified multicast source.

11.1 Global Config

The **Global Config** can be implemented on the **Global Config** and **Mroute Table** pages.

11.1.1 Global Config

You must enable IP multicast routing. Then the software can forward multicast packets, and the switch can populate its multicast routing table.

Choose the menu **Multicast Routing→Global Config→Global Config** to load the following page.

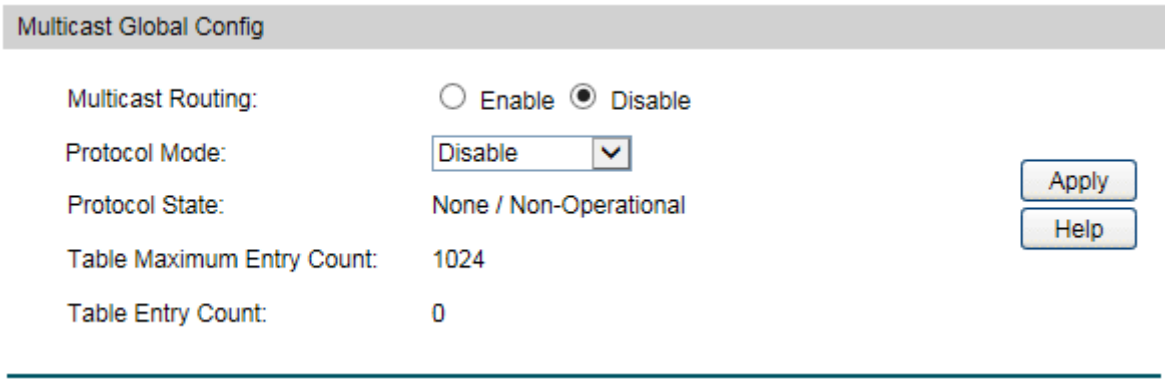


Figure 11-1 Multicast Routing Global Config

The following entries are displayed on this screen:

➢ **Multicast Global Config**

Multicast Routing: Enable or disable Multicast Routing function globally on the switch. The default is "disable".

Protocol Mode:	Select PIM DM or PIM SM from the radio button to set the administrative status in the router. The default is disable.
Protocol State:	The multicast routing protocol presently activated and operational state of the multicast forwarding module.
Table Maximum Entry Count:	The maximum number of entries in the IP Multicast routing table.
Table Entry Count:	The number of multicast route entries currently present in the Multicast route table.

11.1.2 Mroute Table

On this page you can get the desired mroute information through different search options.

Choose the menu **Multicast Routing→Global Config→Mroute Table** to load the following page.

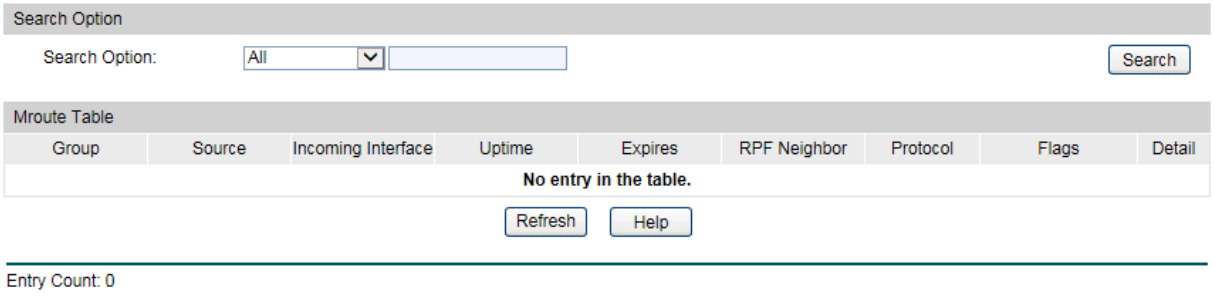


Figure 11-2 Mroute Table

The following entries are displayed on this screen:

- **Search Option**

All:	Select All to display all entries.
Group:	Select Group and enter the group of desired entry.
Source:	Select Source and enter the source of desired entry.

- **Mroute Table**

Group:	The destination group IP address.
Source:	The IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry.
Incoming Interface:	The incoming interface on which multicast packets for this source/group arrive.
Uptime:	The time in seconds since the entry was created.
Expires:	The time in seconds before this entry will age out and be removed from the table.
RPF Neighbor:	The IP address of the Reverse Path Forwarding neighbor.

Protocol:	The multicast routing protocol which created this entry. The possibilities are PIM DM and PIM SM.
Flags:	The value displayed in this field is valid if the multicast routing protocol running is PIM SM. The possible values are RPT or SPT. For other protocols an "------" is displayed.
Detail:	Displays the detailed information of the mroute entries.
Outgoing Interface:	Displays the outgoing interfaces on which multicast packets for this source/group are forwarded.

11.2 IGMP

➢ **Brief Introduction of IGMP**

IGMP stands for Internet Group Management Protocol. It is responsible for the management of IP multicast members in IPv4, and is used to establish and maintain the multicast member relationships between the IP host and its directly neighboring multicast routers.

So far, there are three IGMP versions:

- IGMPv1(defined in RFC 1112)
- IGMPv2(defined in RFC 2236)
- IGMPv3(defined in RFC 3376)

All IGMP versions support ASM model, and IGMPv3 can be directly applied in SSM model.

➢ **IGMPv1 Work Mechanism**

IGMPv1 is mainly based on the query-and-response mechanism to manage the multicast group members.

When there are multiple multicast routers in the subnet, all of them can receive IGMP membership report message. A specific router needs to be chosen from these routers through the querier election mechanism, and it will works as the querier to send IGMP query message.

In IGMPv1, the DR (Designated Router) is elected according to the multicast routing protocol (such as PIM) as the exclusive IGMP querier to forward the multicast information.

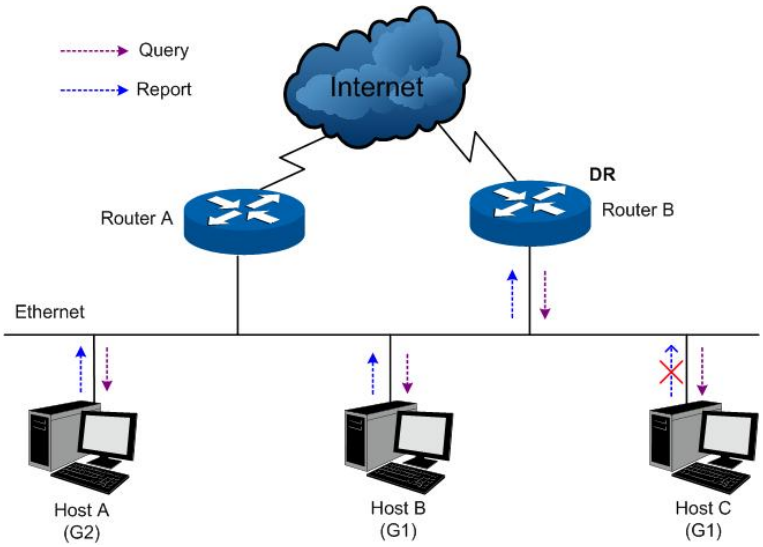


Figure 11-3 IGMP Query-and-Response

As shown in Figure 11-3, Suppose Host B and Host C expect to receive the multicast traffic sending to multicast group G1, and Host A expects to receive the multicast traffic sending to multicast group G2. The basic process of the host joining the multicast group and the IGMP querier (Router B) maintaining the multicast group membership is as below:

(1) Instead of waiting for the IGMP query message from the IGMP querier, the host will actively send IGMP membership report message to the multicast group it wants to join in.

(2) The IGMP querier will periodically send the IGMP query message to all the hosts and routers in the local network with the multicast address 224.0.0.1.

(3) After receiving the IGMP query message, the host that is interested in multicast group G1, either Host B or Host C (depending on whose latency timer runs out first) — for example Host B, will firstly multicast IGMP membership report message to G1 to declare it belongs to G1. As all the hosts and routers can receive this membership report message and the IGMP routers (Router A and Router B) already know there is a host interested in G1, Host C will not send its report message for G1 after it receives the report message of Host B. This is called the membership report preventing mechanism and it helps to reduce the traffic in the local network.

(4) At the same time, as Host A is interested in G2, it will multicast report message to G2 to declare it belongs to G2.

(5) Through the above query-and-response process, the IGMP router learns that there are group members of G1 and G2 in the local network. It will generate the multicast forwarding entries (*, G1) and (*, G2) via the multicast routing protocol, such as PIM, as the basis of the multicast traffic forwarding. The symbol * represents any multicast source.

(6) When multicast packets sending to G1 or G2 from the multicast source arrive at the IGMP router via multicast routing, the multicast forwarding entries (*, G1) and (*, G2) in the IGMP router will guide the multicast packets to the local network and the receiver hosts can receive them.

IGMPv1 doesn't specially define the leave group message. When a host running IGMPv1 leaves one multicast group, it wouldn't send the report message to this multicast group. If no member exists in the multicast group, the IGMP router will not receive any report message to this multicast group, thus it will delete this multicast group's corresponding multicast forwarding entries after a period of time.

- **IGMPv2 Work Process**

IGMPv2 adds the querier-election mechanism and leave-group mechanism based on IGMPv1.

1. Querier-Election Mechanism

The querier-election mechanism in IGMPv2 is illustrated as below:

(1) Every IGMP router will assume itself as the querier at its initialization, and send IGMP general query message to all the hosts and routers with the multicast address 224.0.0.1 in the local network.

(2) After the other IGMPv2 routers in the local network receive this IGMP general query message, it will compare the message's source IP address with its interface address. Through the comparison, the router with the smallest IP address will be elected as the querier and the other routers as the non-querier.

(3) All the non-queriers will start up a timer, known as the Other Querier Present Timer. This timer will be reset if the non-querier receives the IGMP query message before the timer runs out; otherwise the former querier will be assumed as invalid and a new querier-election will be initiated.

2. Leave-Group Mechanism

When a host leaves a multicast group in IGMPv2:

(1) The host will send leave group message to all the multicast routers in the local network with the multicast address 224.0.0.2.

(2) After receiving this leave group message, the querier will send group-specific query message to the multicast group that the host announces to leave. (The querying multicast group address is filled in the destination address field and the group address field of this group-specific query message.)

(3) When there are other members of this multicast group in the local network, these members will send their membership report messages after receiving the group-specific query message within the max response time set in the query message.

(4) If the querier receives the other member's membership report message of this multicast group within the max response time, the querier will continue to maintain the memberships of this multicast group; otherwise the querier will assume that there is no member in this multicast group and will no longer maintain its memberships.

➢ **IGMPv3 Work Process**

Compatible of and Inherited from IGMPv1 and IGMPv2, IGMPv3 further enhances the control capacity of the hosts and broaden the functions of the query and report messages.

1. Enhancement of the Hosts

IGMPv3 adds the filtering mode (INCLUDE/EXCLUDE) for the multicast source basing on the group-specific query. This mode allows the hosts to accept or reject multicast traffic from specified multicast sources when joining a multicast group.

When a host joins a multicast group:

- If it expects only the multicast data from specified multicast sources, such as S1, S2 … Its report message can be marked with INCLUDE Sources (S1, S2 …);
- If it doesn't expect any multicast data from the specified multicast sources, such as S2, S2… Its report message can be marked with EXLUDE Sources (S1,S2 …);

As shown in Figure 11-4, there are two multicast sources, Source 1(S1) and Source 2(S2), sending multicast data to multicast group G. Host B is only expecting the multicast data sending from Source 1 to G.

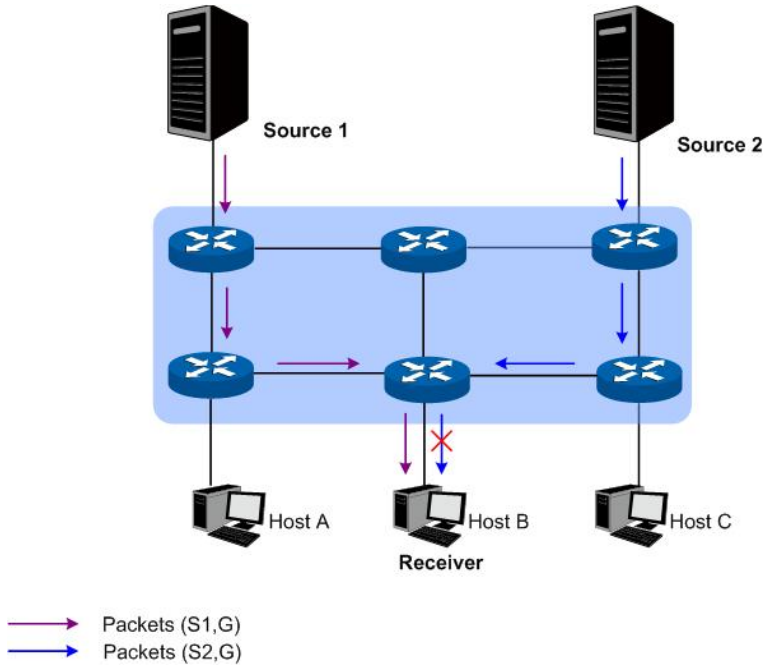


Figure 11-4 IGMPv3 Multicast Source Filtering

If the IGMP protocol running between the hosts and the multicast routers is IGMPv1 or IGMPv2, Host B will be unable to select its expecting sources when it joins the multicast group G. Thus whether needed or not, the multicast data from Source 1 and Source 2 will be transferred to Host B.

When IGMPv3 is running between the hosts and the multicast routers, Host B will only expect the multicast data sending from Source 1 to G, referred as (S1, G), or refuse to receive the multicast data sending from Source 2 to G, referred as (S2, G). Thus only the multicast data from Source 1 will be transferred to Host B.

2. Function Enhancement of the Query and Report Message

(1) Query message carrying source address

IGMPv3 supports source-specific query as well as the general query in IGMPv1 and the group-specific query in IGMPv2:

- The general query message carries neither group address nor source address;
- The group-specific query message carries the group address without the source address.
- The source-specific query message carries not only the group address, but also one or several source addresses.

(2) The report message carrying several group records

The destination address of IGMPv3 report message is 224.0.0.22. The IGMPv3 report message can carry one or several group records, which contains the list of multicast group addresses and multicast source addresses in each of them. The types of group records are listed as below:

- IS_IN: indicating the mapping relationship between the multicast group and the multicast source list is INCLUDE, which means the host will only receive the multicast data sending from the specified multicast source list to this multicast group. If the specified multicast source list is empty here, the host will leave this group.
- IS_EX: indicating the mapping relationship between the multicast group and the multicast source list is EXCLUDE, which means the host will only receive the multicast data sending to this multicast group with its source not in the specified source list.
- TO_IN: indicating the mapping relationship between the multicast group and the multicast source list changes from EXCLUDE to INCLUDE.
- TO_EX: indicating the mapping relationship between the multicast group and the multicast source list changes from INCLUDE to EXCLUDE.
- ALLOW: indicating the host expects to receive multicast data from more multicast sources besides the current ones. If the current mapping relationship is INCLUDE, these multicast sources will be added to the multicast source list; if the current mapping relationship is EXCLUDE, these multicast sources will be deleted from the multicast source list.
- BLOCK: indicating the host doesn't expect to receive multicast data from the specific multicast sources any longer. If the current mapping relationship is INCLUDE, these multicast sources will be deleted from the multicast source list; if the current mapping relationship is EXCLUDE, these multicast sources will be added to the multicast source list.

11.2.1 Global Config

IGMP stands for Internet Group Management Protocol. It is responsible for the management of IP multicast members in IPv4, and is used to establish and maintain the multicast member relationships between the IP host and its directly neighboring multicast routers.

Choose the menu **Multicast Routing→IGMP→Global Config** to load the following page.

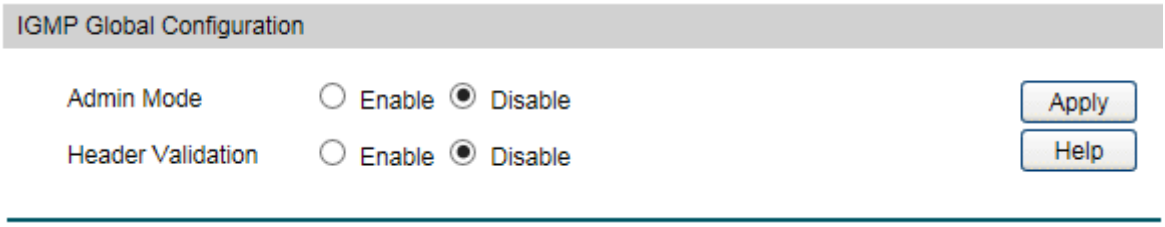


Figure 11-1 IGMP Global Config

The following entries are displayed on this screen:

➢ **Multicast Global Config**

Admin Mode: Select Enable/Disable IGMP function globally on the Switch.

Header Validation: Select Enable/Disable the validation of igmp header field Router Alert options. The fields validated for IGMPv2 and IGMPv3 only. Regardless of whether open the validation, TTL(Time To Live) must be 1.

11.2.2 Interface Config

Choose the menu **Multicast Routing→IGMP→Interface Config** to load the following page.

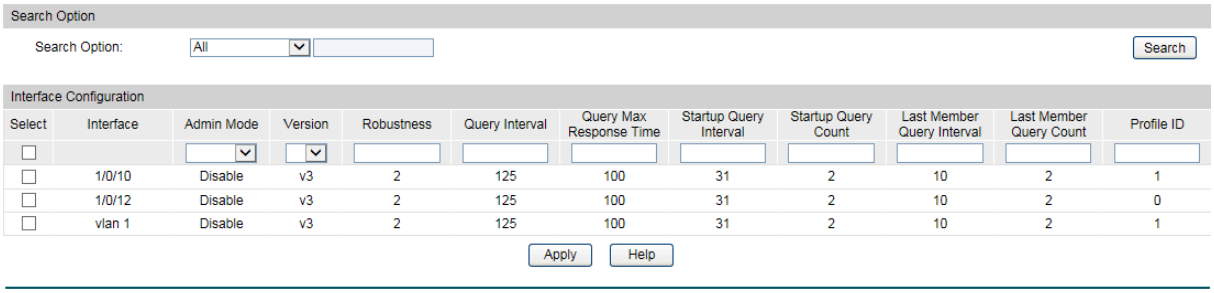


Figure 11-5 Interface Config

The following entries are displayed on this screen:

➢ **Search Option**

All: Displays all the interface entries.

Interface VLAN: Enter the VLAN ID the desired entry must carry.

Routed Port: Enter the routed port the desired entry must carry.

➢ **Interface Configuration**

Select: Select the interface for which parameters is to be configured.

Interface: The interface for which data is to be displayed or configured.

Admin Mode: The interface administrative status. You can select Enable/Disable the IGMP function for the interface.

Version: There are three versions for IGMP protocol.

- IGMPv1: the interface is now an IGMPv1 Router.
- IGMPv2: the interface is now an IGMPv2 Router.
- IGMPv3: the interface is now an IGMPv3 Router.

Robustness: Specify the robustness of the selected interface, ranging from 1 to 255. The default is 2.

Query Interval: Specify the IGMP query interval at which IGMP router sends out a general query, ranging from 1 to 3600 . The default is 125 seconds.

Query Max Response Time: When IGMP router sends out a query packet, the host should response within the specified Query Max Response Time, the value is in tenths of a second, ranging from 0 to 255 . The default is 100(10 seconds).

Startup Query Interval: When IGMP router starts up, it will send out a general query every Startup Query Interval, ranging from 1 to 300. The default is 31 seconds.

Startup Query Count: The number of general queries to be sent on startup, ranging from 1 to 20. The default is 2.

Last Member Query Interval: When the last member leaves a multicast group, IGMP router will send out a specific query every Last Member Query Interval, the value is in tenths of a second, ranging from 0 to 255. The default is 10(1 seconds).

Last Member Query Count: The number of queries to be sent on receiving a leave group report, ranging from 1 to 20. The default is 2.

Profile ID: The Profile ID bound to the selected interface, ranging from 0 to 999.The value 0 means bound to none.

11.2.3 Interface State

Choose the menu **Multicast Routing→IGMP→Interface State** to load the following page.

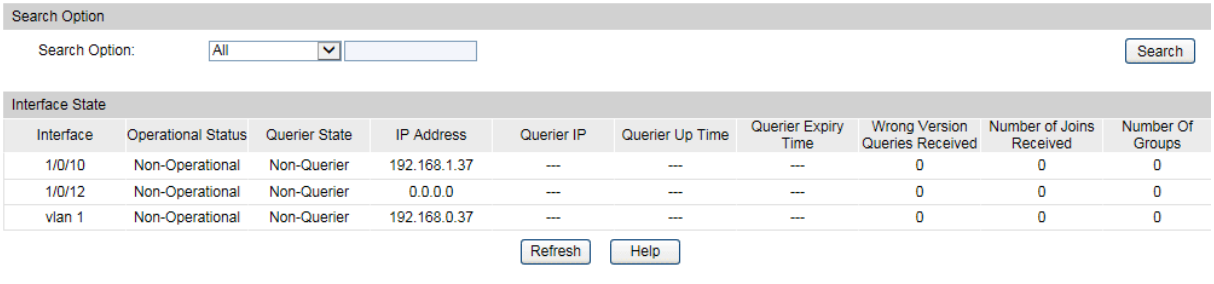


Figure 11-6 Interface State

The following entries are displayed on this screen:

➢ **Search Option**

All: Displays all interface entries.

Interface VLAN: Enter the VLAN ID the desired entry must carry.

Routed Port: Enter the routed port the desired entry must carry.

- **Interface State**

Interface: The interface for which data is to be displayed or configured.

Operational Status: The operational state of IGMP on the selected interface.

Querier State: Indicates whether the selected interface is in querier or non-querier mode.

IP Address: The IP address of the selected interface.

Querier IP: The address of the IGMP querier on the IP subnet to which the selected interface is attached.

Querier Up Time: Indicates whether the selected interface is in querier or non-querier mode.

Querier Expiry Time: The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this will be zero.

Wrong Version Queries Received: The current number of dynamic groups for the selected interface.

Number of Joins Received: The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.

Number of Groups: The current number of entries for the selected interface in the cache table.

11.2.4 Multicast Group Table

On this page you can view the information of the multicast groups already on the switch. Multicast IP addresses range from 224.0.0.1 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 Routing→IGMP→Multicast Group Table** to load the following page.

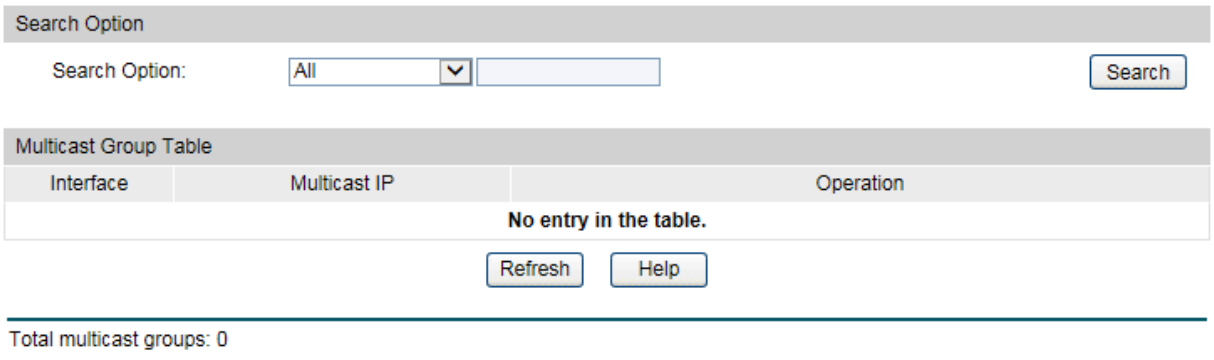


Figure 11-8 Multicast Group Table

The following entries are displayed on this screen:

➢ **Search Option**

Search Option: Select the rules for displaying multicast IP table to find the desired entries quickly.

- **All**: Displays all multicast IP entries.
- **Multicast IP:** Enter the multicast IP address the desired entry must carry.
- **Interface VLAN**: Enter the VLAN ID the desired entry must carry.
- **Routed Port**: Select the routed port the desired entry must carry.

➢ **Multicast Group Table**

Interface: Displays the VLAN ID the desired entry must carry.

Multicast IP: Displays the multicast IP address the desired entry must carry.

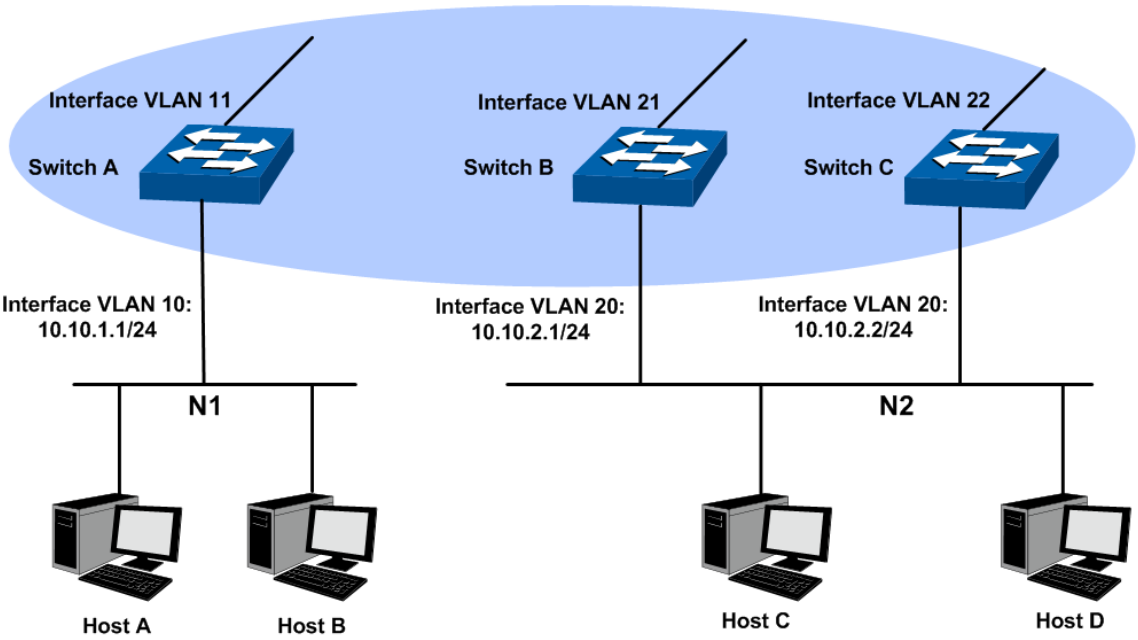
Operation: Click the Detail button to view the mode and source IP address of the multicast group.

11.2.5 Application Example for IGMP

➢ **Network Requirements**

1. Receivers of different organizations form the stub networks N1 and N2, and Host A and Host C are the multicast information receivers in N1 and N2 respectively. They receive the Video-On-Demand information through multicast.
2. In the PIM network, Switch A connects to N1; Switch B and Switch C connect to N2.
3. Switch A connects N1 through its interface VLAN 10, and connects the other devices in the PIM network through interface VLAN 11.
4. Switch B and Switch C connect to N2 through their interface VLAN 20 respectively. Switch B connects to the other devices in PIM through interface VLAN 21, and Switch C connects to the other devices in PIM through interface VLAN 22.
5. IGMPv3 is required between Switch A and N1. IGMPV2 is required among Switch B, Switch C and N2, with Switch B as the IGMP querier.

➢ **Network Diagram**



➢ **Configuration Procedure**

1) Configure the interface IP addresses and the unicast routing protocol

Configure the IP address and subnet mask of each interface as the diagram above. The detailed configuration steps are omitted here.

Configure the switches to access each other through OSPF protocol. Ensure the network-layer intercommunication among Switch A, Switch B and Switch C. The dynamic routing information is updated among the three switches via the unicast routing protocol. The detailed configuration steps are omitted here.

2) Enable the IP multicast routing, and enable the IGMP function on the interfaces of the user-side.

- Configure Switch A

Steps	Operation	Note
1	Enable IP multicast routing.	On page **Multicast Routing→ Global Config→ Global Config**, enable the multicast routing function.
2	Enable IGMP on user-side interface.	On page **Multicast Routing→ IGMP→ Interface Config**, enable IGMP (version 3) on interface VLAN 10.

- Configure Switch B

Steps	Operation	Note
1	Enable IP multicast routing.	On page **Multicast Routing→ Global Config→ Global Config**, enable the multicast routing function.

2	Enable IGMP on user-side interface.	On page **Multicast Routing→ IGMP→ Interface Config**, enable IGMP (version 2) on interface VLAN 20.

- Configure Switch C

Steps	Operation	Note
1	Enable IP multicast routing.	On page **Multicast Routing→ Global Config→ Global Config**, enable the multicast routing function.
2	Enable IGMP on user-side interface.	On page **Multicast Routing→ IGMP→ Interface Config**, enable IGMP (version 2) on interface VLAN 20.

11.3 PIM DM

In this section we firstly outline PIM protocol, RPF Check mechanism and the two modes of PIM, then introduce the working process of PIM DM.

PIM is a popular multicast routing protocol within the AS. Instead of relying on one specific unicast routing protocol, PIM uses the static routing or unicast routing table generated by any unicast routing protocol (including RIP, OSPF, IS-IS, BGP etc.) to perform routing for IP multicast data.

Unlike some other multicast routing protocols, PIM doesn't update routing information between routers or maintain an independent route forwarding table. PIM uses the RPF (Reverse Path Forwarding) check mechanism to forward the multicast data.

There are two types of multicast routing and forwarding tables in the multicast implementation:

- All the multicast route information will be summarized as a general multicast routing-table;
- The multicast forwarding-table is used to control the forwarding of the multicast packets directly.

The multicast routing table consists of a group of (S, G) entries, and (S, G) route represents routing information from source S to group G. If the router supports multiple multicast routing protocols, its multicast routing table will contain multicast routes generated from multiple protocols. The router will chose the optimal multicast route according to multicast routing and forwarding strategy, and send it to the multicast forwarding table.

The multicast routing protocol uses the RPF mechanism to establish the multicast routing entries, thus to guarantee the multicast data being transferred in the correct path.

➢ **RPF Mechanism**

PIM uses the unicast routing table to perform the RPF check. RPF mechanism ensures the multicast packets being forwarded correctly according to the multicast routing configuration, and avoids loops causing by various reasons.

1. RPF Check

The RPF check relies on unicast route or static multicast route. The unicast routing table aggregates the shortest paths to each destination network segments, and the static multicast routing table lists specified static RPF routing entries configured by the user manually. Instead of maintaining certain unicast routing independently, the multicast routing protocol relies on the current unicast routing information or static multicast routing in the network to establish multicast routing entries.

When performing the RPF check, the router will look up the unicast routing table and the static multicast routing table at the same time. The process is as below:

(1) Chose an optimal route from the unicast routing table and the static routing table respectively:

- The router looks up the unicast routing table with the IP address of the packet source as the destination address, and selects an optimal unicast route automatically. The output interface of the corresponding entry is the RPF interface, and the next hop is the RPF neighbor. The router will consider the traveling path of the multicast data sent from the RPF neighbor and received on the RPF interface as the shortest path from the multicast source S to the local network.
- The router looks up the static multicast routing table with the IP address of the packet source specified as the source address, and selects an optimal static multicast route automatically. The corresponding entry explicitly specifies the RPF interface and RPF neighbor.

(2) Select one from the two optimal routes as the RPF route：

According to the longest mask matching principle, the longest mask matching route between them will be selected; if the two routes have the same mask, the route with higher priority will be selected; if the two routes also have the same priority, then the static multicast route is prior to the unicast route.

2. RPF Mechanism Application

When the router receives multicast packets sent from multicast source S to multicast group G, it will look up the multicast forwarding table at first:

(1) If the corresponding entry (S, G) exists and the packet's actual arriving interface is the same as the input interface in the multicast forwarding table, the packet will be forwarded to all the output interfaces.

(2) If the corresponding entry (S, G) exists and the packet's actual arriving interface is different from the input interface in the multicast forwarding table, the router will perform RPF check on this packet:

- If the check result shows that the RPF interface is the same as the input interface in the current (S, G) entry, which indicates that the (S, G) entry is correct and the packet from the wrong path will be discarded;

- If the check result shows that the RPF interface is the different from the input interface in the current (S, G) entry, which indicates that the (S, G) entry is invalid and the router will correct the input interface to the packet's actual arriving interface, and forward this packet to all the output interfaces.

(3) If the corresponding entry (S, G) doesn't exist, the router will still perform the RPF check on this multicast packet. With the RPF interface as the input interface, the router will create corresponding entry with the RPF interface as the input interface combining related routing information, and send this entry to the multicast forwarding table:

- If the packet's actual arriving interface is exactly the RPF interface, the RPF check will pass and the packet will be forwarded to all the output interfaces;
- If the packet's actual arriving interface is not the RPF interface, the RPF check fails and this packet will be discarded.

➢ **PIM Modes**

PIM can be divided into two modes according to different routing mechanisms:

- PIM DM: Protocol Independent Multicast-Dense Mode
- PIM SM: Protocol Independent Multicast-Sparse Mode

➢ **PIM DM**

PIM DM (defined in RFC 3973) is a multicast routing protocol in dense mode. It uses Push Mode to transfer multicast packets and applies to small network with relatively dense multicast group members.

The working mechanism of PIM DM is illustrated as below:

- PIM DM assumes that there is at least one multicast group member in each subnet of the network, and the multicast packets will be flooded to all the nodes in the network. Then branches without receivers are pruned from the distribution tree, leaving only branches that contain receivers. This "flood-and-prune" process takes place periodically. The pruned branches can also resume to forwarding state periodically.
- When a new receiver on a previously pruned branch of the tree joins a multicast group, the PIM DM takes the Graft (see Grafting) mechanism to actively resume this node's function of forwarding multicast data, thus reducing the time it takes to resume to the forwarding state. Generally speaking, the packet forwarding tree in the dense mode is Source Tree (a forwarding tree with multicast source as the root, and multicast members as the branches). As the Source Tree is a forwarding tree with the shortest path from the multicast source to the receivers, it is also called Shortest Path Tree (SPT).

The working process of PIM DM can be summarized as follows：

- Neighbor Discovering
- SPT Building
- Grafting

➢ **Neighbor Discovering**

In PIM domain, routers periodically sends PIM Hello packets to all the PIM routers with the multicast address 224.0.0.13 to discover PIM neighbors, maintain the PIM neighboring relationships between the routers, thus to build and maintain the SPT.

➢ **SPT Building**

The SPT building process is also the "flood-and-prune" process:

(1) When the multicast source S is sending multicast packets to multicast group G in PIM DM domain, the multicast packets will firstly be flooded: After the multicast packet passes the router's RPF check, the router will create a corresponding (S, G) entry and forward this packet to all the nodes downstream in the network. All the routers in the PIM DM domain will create the (S, G) entry after this flooding process.

(2) Then branches without receivers downstream are pruned. The downstream branches with no receivers will send prune message to the upstream node to delete the corresponding interface in the output interface list of the multicast forwarding entry (S, G), and the multicast packets will no longer forwarded to the pruned branches.

Note:

The entry (S, G) contains the multicast source address S, the multicast group G, the list of output interfaces and input interfaces.

The prune process is initiated by the leaf router, as shown in Figure 11-11, the leaf router without receivers (such as the router directly connected to Host A) performs the prune actively, and the prune process will last until there are only necessary branches in the PIM DM domain. These branches form the SPT.

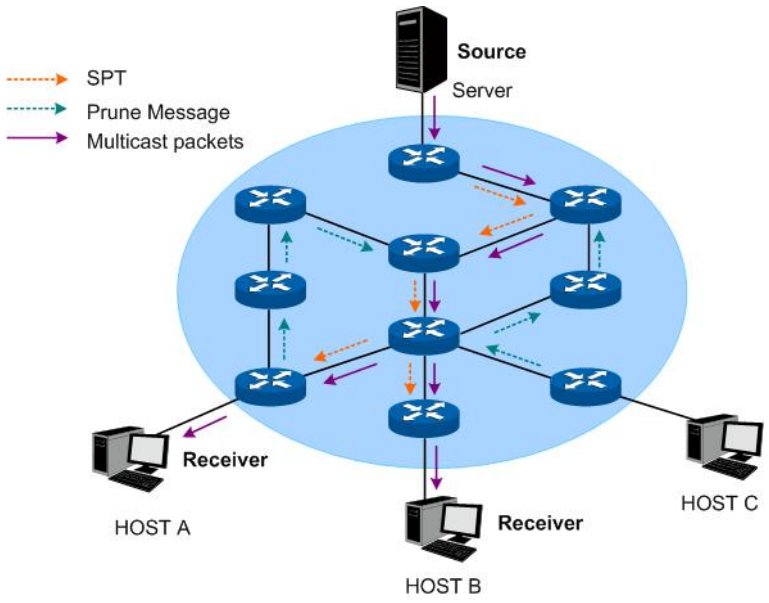


Figure 11-11 SPT Topology in PIM DM

The "flood-and-prune" process takes place periodically. The pruned nodes are provided with timeout mechanism, and the "flood-and-prune" process will resume after the pruned state times out.

➢ **Grafting**

When a new receiver on a previously pruned branch of the tree joins a multicast group, the PIM DM takes the Graft mechanism to actively resume this node's function of forwarding multicast data, thus reducing the time it takes to resume to the forwarding state. The process is illustrated as below:

(1) The branch that needs to receive the multicast data again will send a graft message to its upstream node up the distribution tree towards the source hop-by-hop, applying to rejoin the SPT;

(2) The upstream node turns the downstream node into forwarding state after receiving the graft message, and responses with a Graft-Ack message to confirm;

(3) If the downstream node sending the graft message doesn't receive the Graft-Ack message from its upstream node, it will keep sending graft messages until being confirmed.

➢ **Assert Mechanism**

If there are multiple multicast routers in one network segment, these routers may send the same multicast packets to this network segment repeatedly. To avoid this kind of situation, the Assert Mechanism is applied to select the exclusive router to forward the multicast data.

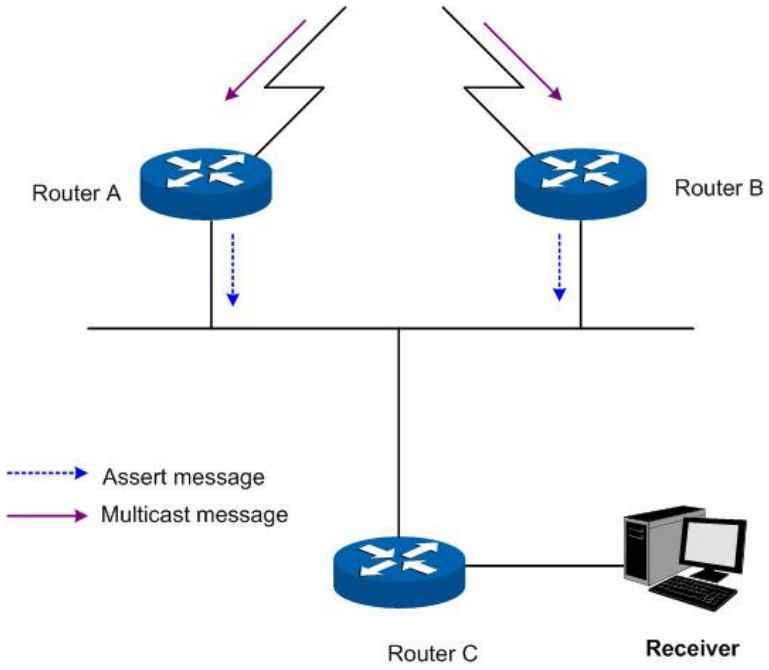


Figure 11-12 Assert Mechanism

As shown in Figure 11-12, the downstream node Router C will receive the same two (S, G) multicast packets from Router A and Router B in the local network after they receive them from the upstream nodes. Router A and Router B will also receive the multicast packets on their local interfaces sent from each other.

Meanwhile, Router A and Router B will send the Assert Messages through their local interfaces to all the PIM routers with the multicast address 224.0.0.13. The Assert Message contains the following information: the multicast source address S, the multicast group address G, the

priority and cost of the unicast route to the multicast source. The router to forward the multicast packets of (S, G) is elected based on the following rules and in the order listed:

(1) The router with the unicast route of the higher priority to the multicast source;

(2) The router with the unicast route of the smaller cost to the multicast source;

(3) The router with the local interface of the higher IP address.

11.3.1 PIM DM Interface

Choose the menu **Multicast Routing→PIM DM→PIM DM Interface** to load the following page.

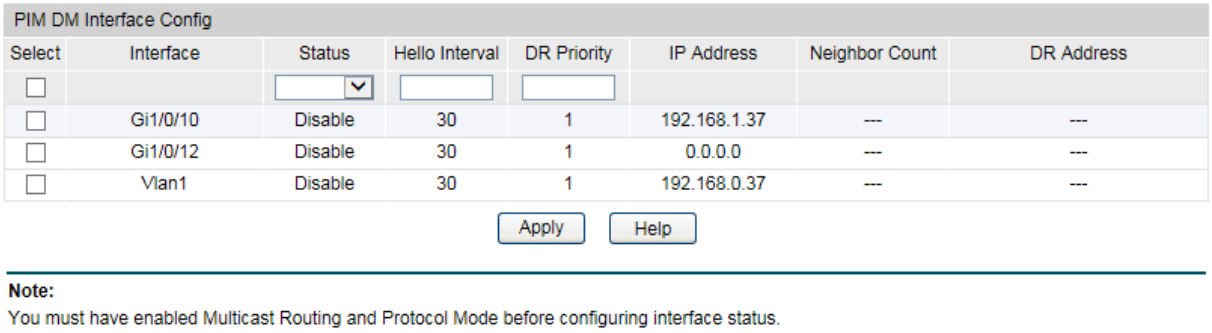


Figure 11-13 PIM DM Interface

The following entries are displayed on this screen:

➢ **PIM DM Interface Config**

The L3 interfaces can be configured as PIM DM mode by this page.

Select:	Select the desired PIM DM interface entry to modify.
Interface:	The interface for which data is to be displayed or configured. You must have configured at least one router interface before configuring or displaying data for a PIM DM interface.
Status:	Select enable or disable from the pull-down list to set the administrative status of PIM DM for the selected interface. The default is disable.
Hello Interval:	Specify the rate (time in seconds) at which PIM hello messages are transmitted from the selected interface. The valid value ranges from 1 to 18725 and the default is 30 seconds.
DR Priority:	Specify the DR priority for the selected interface. The valid value range from 0 to 4294967294. The default value is 1.
IP Address:	The IP address of this interface.
Neighbor Count:	The neighbor numbers of this interface.
DR Address:	The designated router on the selected PIM interface.

11.3.2 PIM DM Neighbor

PIM DM neighbor is automatically learned by sending and receiving Hello Packets when PIM DM is enabled.

Choose the menu **Multicast Routing→PIM DM→PIM DM neighbor** to load the following page.

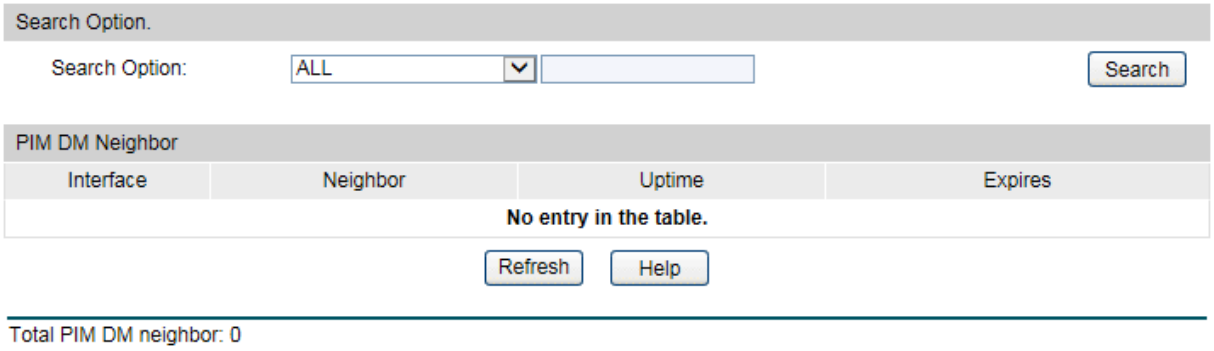


Figure 11-14 PIM DM neighbor

The following entries are displayed on this screen:

➢ **Search Option**

The L3 interfaces can be configured as PIM DM mode by this page.

Search Option:

- **ALL**: Displays all entries.
- **Neighbor**: Select Neighbor and enter the neighbor address of your desired entry.
- **Interface**：Select interface and enter the interface ID of your desired entry.

➢ **PIM DM Neighbor**

Interface: The physical interface on which PIM DM is enabled.

Neighbor: The IP address of the PIM neighbor for which this entry contains information.

Uptime: The time since the PIM neighbor (last) became a neighbor of the local switch.

Expires: The time remaining before the PIM neighbor will be aged out.

Configuration Procedure for PIM DM:

Step	Operation	Description
1	Configure interface	Required. Configure IP addresses and subnet masks of routing interfaces on **Routing→Interface→Interface Config** page.
2	Configure routing protocol	Required. Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all network can communicate with each other and update the routing information through a unicast routing protocol dynamically.
3	Enable multicast routing and PIM DM	Required. Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM DM on routing interfaces on **Multicast Routing→PIM DM→PIM DM Interface** page.

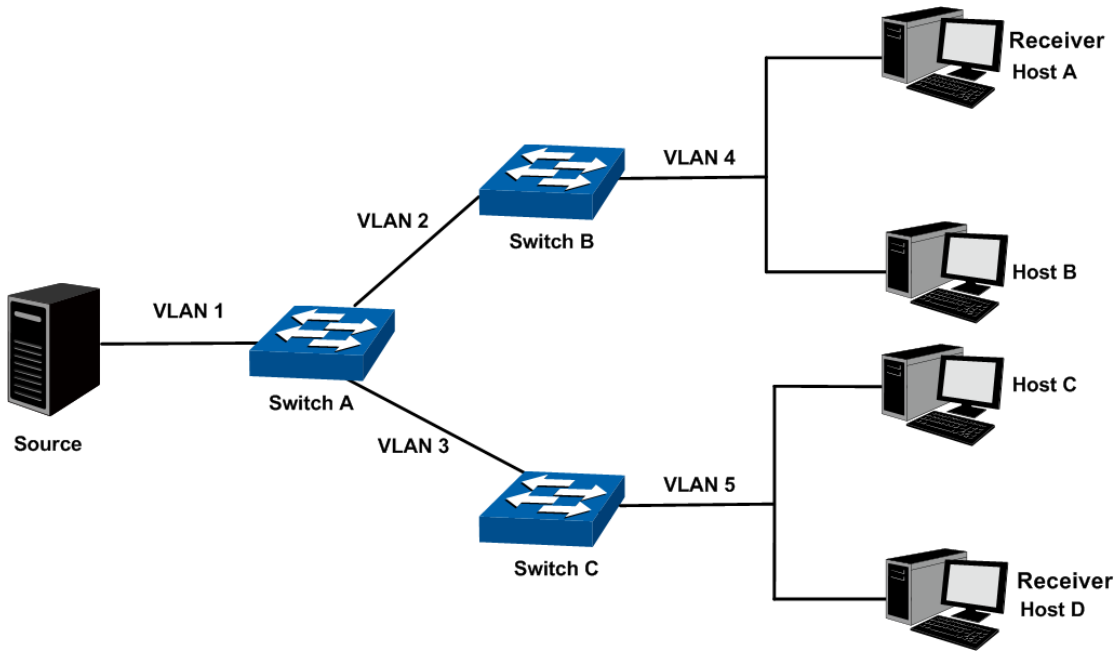
Step	Operation	Description
4	Enable IGMP	Required. Enable IGMP on the routing interfaces which connect to the receivers on **Multicast Routing→IGMP→Interface Config** page.

11.3.3 Application Example for PIM DM

➢ **Network Requirements**

1. Receivers receive VOD data through multicast. The whole network runs PIM DM as multicast routing protocol.
2. Host A and Host D act as multicast receivers.
3. Switch A connects to Switch B in VLAN 2, connects to Switch C in VLAN 3. The Source server connects to Switch A in VLAN 1.
4. Host A and B connect to Switch B in VLAN 4. Host C and D connect to Switch C in VLAN 5.
5. The VLAN interfaces connecting to hosts run IGMP protocol.

➢ **Network Diagram**



The IP addresses of VLAN interfaces in each switch are displayed below:

Switch A: VLAN interface 1: 192.168.1.2/24

VLAN interface 2: 192.168.2.2/24

VLAN interface 3: 192.168.3.2/24

Switch B: VLAN interface 2: 192.168.2.100/24

VLAN interface 4: 192.168.4.100/24

Switch C: VLAN interface 3: 192.168.3.100/24

VLAN interface 5: 192.168.5.100/24

➢ **Configuration Procedure**

- Configure Switch A:

Step	Operation	Description
1	Configure interface.	Configure IP addresses and subnet masks of VLAN interfaces 1, 2 and 3 on **Routing→ Interface→Interface Config** page.
2	Configure routing protocol.	Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all the switches can communicate with each other and update the routing information through a unicast routing protocol dynamically.
3	Enable multicast routing and PIM DM	Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM DM on VLAN interfaces 1, 2 and 3 on **Multicast Routing→PIM DM→PIM DM Interface** page.

- Configure Switch B and C:

Step	Operation	Description
1	Configure interface	Configure IP addresses and subnet masks of VLAN interfaces 2, 3, 4 and 5 on **Routing→Interface→Interface Config** page.
2	Configure routing protocol	Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all network can communicate with each other.
3	Enable multicast routing and PIM DM	Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM DM on VLAN interfaces 2, 3, 4 and 5 on **Multicast Routing→PIM DM→PIM DM Interface** page.
4	Enable IGMP	Enable IGMP on the VLAN interfaces 4 and 5 which connect to the receivers on **Multicast Routing→IGMP→Interface Config** page.

11.4 PIM SM

PIM DM uses the "flood-and-prune" mode to create the SPT for transferring multicast data. Although SPT has the short path, its building-up process is of low efficiency and does not apply to the large and medium-sized network.

PIM SM is a multicast routing protocol in sparse mode. It uses the "Pull Mode" to transfer multicast data and usually applies to large and medium-sized network with relatively sparse multicast group members.

The working mechanism of PIM SM is illustrated as below:

- PIM SM assumes that no hosts need to receive the multicast data, the multicast data will not be forwarded to the host unless there is an explicitly request for the traffic. The core task of PIM SM to realize multicast forwarding is to build and maintain the RPT (Rendezvous Point Tree). RPT selects a certain router in the PIM domain as the public RP (rendezvous point), through which the multicast data is transferred along the RPT to the receivers.

- The router connected to the receiver sends the join message to the RP of a certain multicast group. The path along which the join message is sent to the RP hop-by-hop forms a branch of RPT.
- When the multicast source is sending multicast data to a multicast group, the router directly connected to the multicast source firstly registers to the RP by sending the Register Message to the RP in unicast mode. The arrival of the register message at the RP triggers the establishment of the SPT. Then the multicast source sends the multicast data along the SPT to the RP. The multicast data will be duplicated and distributed to the receivers after they arrive at the RP.

Note:

The duplicating process only takes place at the branching point of the distributing tree, and this process automatically repeats until the packets arrives at the final receivers.

The work process of PIM SM can be generalized below:

- Neighbor Discovering
- DR Electing
- RP Discovering
- RPT Building
- Multicast Source Registering
- Switching from RPT to SPT
- Asserting

➢ **Neighbor Discovering**

The neighbor discovering mechanism of PIM SM and PIM DM is the same, for more details, refer to Neighbor Discovering.

➢ **DR Electing**

The DR (Designated Router) in the shared network is elected through the Hello message, and works as the exclusive router to forward multicast data in this shared network.

Whether the network connects to the multicast source or the network connects to the receivers, the DR must be elected if the network is a shared one. The DR is responsible for sending join message to the RP in the receiver side and sending register message to the RP in the multicast source side.

Note:

- The DR is elected between the multiple routers of the network segment by comparing the priorities and IP addresses carried in Hello packets. The elected DR has practical meaning in PIM SM; with PIM DM operation, the DR has meaning only if IGMPv1 is in use, the elected DR functions as the IGMP querier on account that IGMPv1 does not have an IGMP querier election process.

- The device working as DR should be enabled with the IGMP function; otherwise the receivers connected to it would be unable to join the multicast group via this DR.

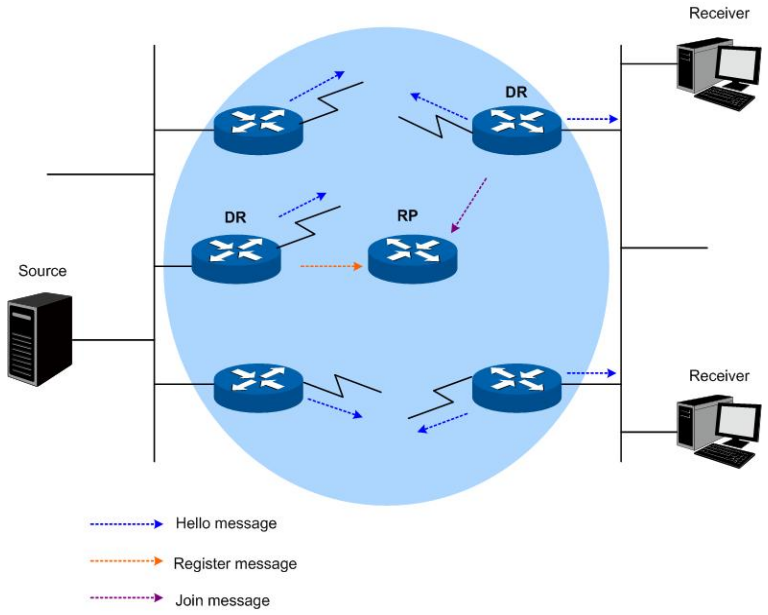


Figure 11-15 DR Elect

As shown in Figure 11-15, the DR election process is illustrated below:

(1) Routers in the shared network sends Hello message carrying DR-election priority to each other, and the router with the highest priority will be elected as the DR;

(2) If the routers have the same priorities, or at least one route in the network doesn't support carrying the DR-election priority in the Hello packet, the routers with the highest IP address will be elected as the DR.

When the DR fails, a new DR election process will be triggered if the other routers haven't received the hello packet from the DR before they time out.

➢ **RP Discovering**

RP is the core device in the PIM SM domain. In a small network with simple structure, the multicast data is so little that merely one RP is enough to forward it. In this network an RP can be statically designated among the routers in the PIM SM domain; in more circumstances, the PIM SM domain is of large scale and the forwarding data for the RP is huge. To release the burden of the RP and optimize the RPT topology, each multicast group should have its own RP. Thus the bootstrapping mechanism is needed to elect the RP dynamically. The BSR (BootStrap Router) should be configured in this mechanism.

BSR is the administrative core in the PIM SM. It collects the Advertisement Messages sent from the C-RP (Candidate-RP) in the network and selects certain C-RP information to compose a RP-Set (which is the mapping relationship database between the multicast group and the RP). The RP-Set is published to the whole PIM SM domain and all the routers (including DR) can calculate the required RP location according to the information offered by the RP-Set.

In a PIM SM domain (or administrative domain), there is only one BSR (for more details about BSR administrative domain, please refer to BSR Adminsitrative Domain) and several C-BSRs (Candidate-BSR). Once the BSR fails, a new BSR will be elected among the other C-BSRs to

avoid business disruption. Similarly, several C-RPs can be configured in one PIM SM domain, and each multicast group's corresponding RP can be calculated through the BSR mechanism. The location of RP and BSR in the network is shown below:

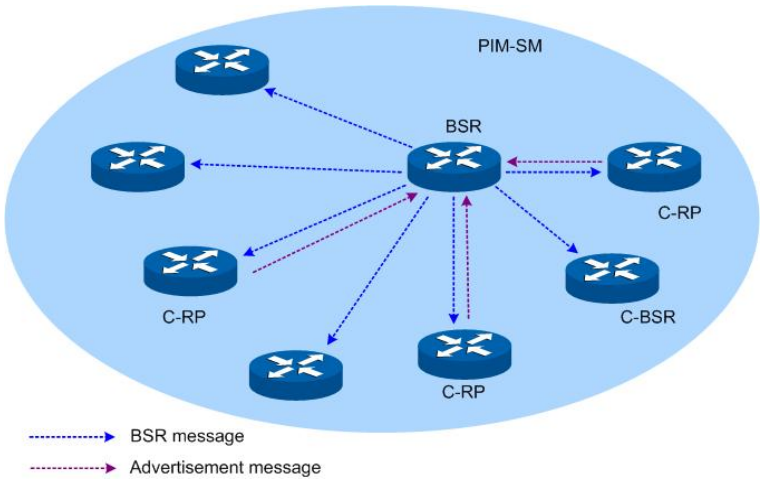


Figure 11-16 The Locations of C-RP, C-BSR and BSR

- **RPT Building**

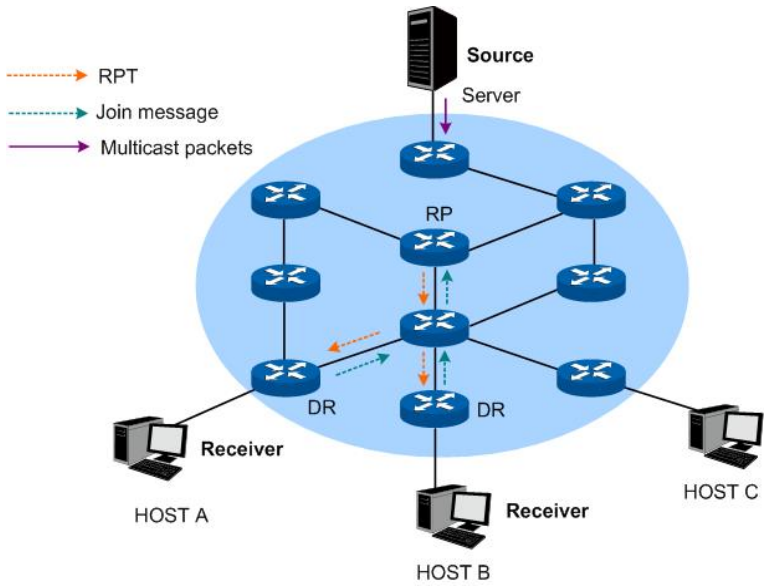


Figure 11-17 RPT Topology in PIM SM

As shown in Figure 11-17, the establishing process of RPT is illustrated below:

(1) When a receiver joins a multicast group G, it informs the directly connected DR with IGMP message;

(2) After receiving the IGMP message from multicast group G, the DR sends PIM join message toward the corresponding root, also known as the RP;

(3) The join message travels router-by-router toward the root, constructing a branch of the RPT as it goes. These routers generate (*, G) entries in their forwarding tables with * representing any multicast source. The RPT works with RP as the root node, and DR as the branch node.

When multicast data for multicast group G is sent to RP, it will travels along the constructed RPT to DR and finally arrives at the receivers.

When a receiver is no longer interested in the multicast group data, its directly connected DR will send prune message up the RPT toward the group's corresponding RP; after the upstream node receives this prune message, it will delete the link to the downstream node in its interface list and check if there are other receivers of this group. If there are no more receivers, the prune message will be sent upstream.

- **Multicast Source Registering**

The multicast source register is to inform its presence to the RP.

As shown in Figure 11-18, the process of the multicast source registering to RP is illustrated below:

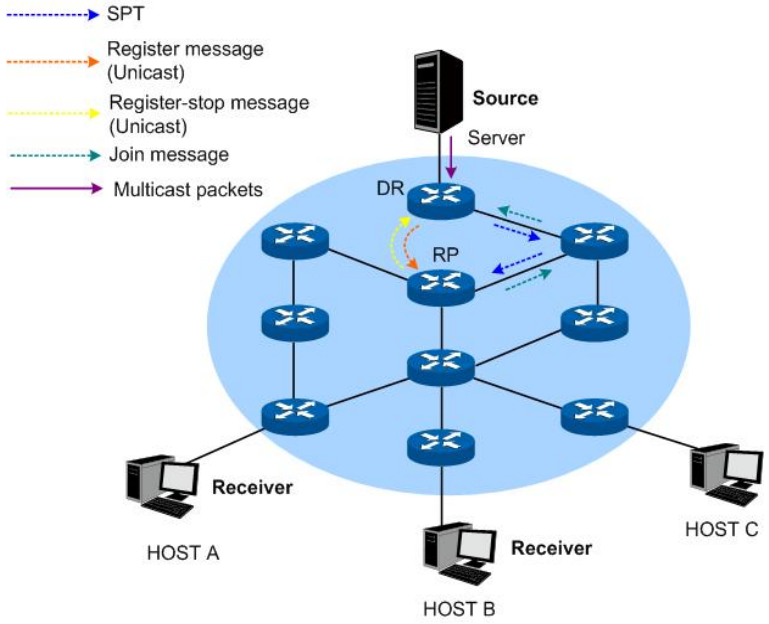


Figure 11-18 Multicast Source Register Topology in PIM SM

(1) When the multicast source S's directly connected DR receives a multicast packet sent from the multicast source to the multicast group G, the DR will encapsulate this packet into a register packet and send it to the corresponding RP in unicast way;

(2) After the RP receives the register packet, it will de-capsulate this packet and send the packaged multicast data to the receivers along the RPT, and meanwhile it will send join message to the multicast source hop-by-hop. The join message travels router-by-router toward the source from the RP, constructing a branch of the SPT as it goes. These routers generate (S, G) entries in their forwarding tables. The SPT works with multicast source as the root, and RP as the branch.

(3) The multicast data sent from the multicast source travels along the constructed SPT to RP, and is forwarded by the RP to the receivers along the RPT. When RP receives the multicast data from the RPT, it will send Register-Stop Message to the DR directly connected to the multicast source to finish the multicast source register process.

➢ **Switching from RPT to SPT**

Once receiver-side DR receives the multicast data from RP to multicast group G, the switching process from RPT to SPT will be triggered:

(1) The receiver-side DR sends (S, G) join message to the multicast source S hop-by-hop, and the join message finally arrives at the source-side DR. All routers the join message passes will generate the (S, G) entry in their forwarding tables, thus building up a branch of SPT;

(2) The receiver-side DR sends prune message toward the RP hop-by-hop. The RP will forward the received prune message toward the multicast source. The switching process from RPT to SPT is then accomplished.

After the switching from RPT to SPT, the multicast data will be sent from multicast source to the receivers directly. Through this switching process from RPT to SPT, PIM SM constructs the SPT in a more economical way than PIM DM does.

➢ **Asserting**

The assert mechanism of PIM SM and PIM DM is the same. For more details, refer to Assert Mechanism.

➢ **BSR Administrative Domain**

BSR is the administrative core in the PIM SM domain. The BSR is exclusive in one PIM SM domain and it advertises the RP-Set information in the whole PIM SM domain. All the multicast group information is forwarded inside the BSR's administrative network scope. When the PIM SM domain is relatively large, you can consider dividing the PIM SM domain into multiple BSR administrative domains, thus sharing the administrative pressure of single BSR and providing specialized services for specific multicast groups.

In geographical space, the BSR administrative domains are separated with each other and one router cannot belong to more than one BSR domain. In other words, the routers contained by the BSR domains are different from each other.

In multicast address, each BSR administrative domain provides services for specific multicast groups. These multicast group addresses usually have no intersection with each other, but they may also have crossings and overlaps, as shown in Figure 11-19.

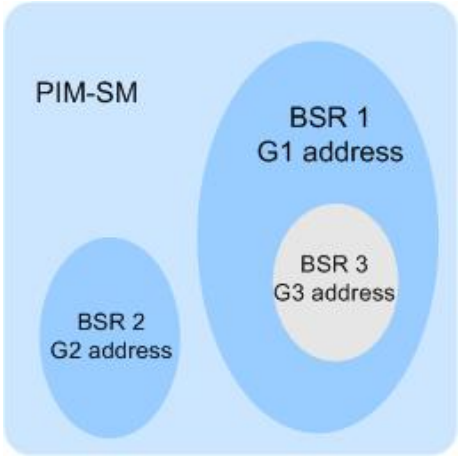


Figure 11-19 BSR Domain Divided by Multicast Address

Features of BSR administrative domain:

- Divide the BSR administrative domains by setting BSR border

Each BSR administrative domain has its own border, C-RP and BSR devices. These devices are only valid in their belonged domains, which means that the BSR mechanism and RP election are separated between their administrative domains.

- BSR messages cannot pass through the BSR border

The multicast messages (such as C-RP Hello Message and BSR BootStrap Message) of each BSR administrative domain cannot pass through the domain border.

11.4.1 PIM SM Interface

Choose the menu **Multicast Routing→PIM SM→PIM SM Interface** to load the following page.

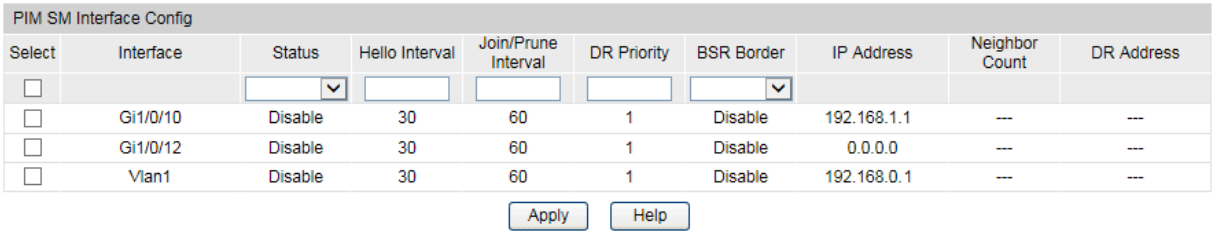


Figure11-20 PIM SM Interface

The following entries are displayed on this screen:

➢ **PIM SM Interface Config**

The L3 interfaces can be configured as PIM SM mode by this page.

Select:	Select the desired interface to configure.
Interface:	Displays the VLAN interface which you can configure.
Status:	Select to enable or disable PIM SM function on the interface.
Hello Interval:	Specify the rate (time in seconds) at which PIM hello messages are transmitted from the selected interface. The valid value ranges from 1 to 18725 seconds and the default is 30 seconds.
Join/Prune Interval:	Specify the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid value range from 1 to 18724 seconds and the default value is 60 seconds.
DR Priority:	Specify the DR priority for the selected interface. The valid value range from 0 to 4294967294. The default value is 1.
BSR Border:	Select to enable or disable the BSR border to define a PIM bootstrap message boundary for the PIM domain.
IP Address:	Displays the IP address of the interface.
Neighbor Count:	Displays the number of PIM neighbors of this interface.
DR Address	Displays the DR address of the interface.

11.4.2 PIM SM Neighbor

PIM SM neighbor is automatically learned by sending and receiving Hello Packets when PIM SM is enabled.

Choose the menu **Multicast Routing→PIM SM→PIM SM Neighbor** to load the following page.

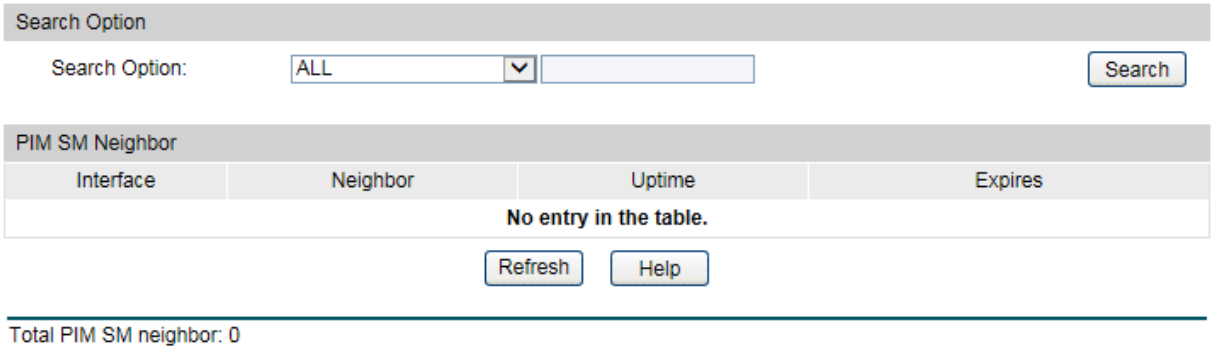


Figure 11-21 PIM SM neighbor

The following entries are displayed on this screen:

➢ **Search Option**

Search Option:

- ALL: Displays all entries.
- Neighbor: Select Neighbor and enter the neighbor address of your desired entry.
- Interface: Select Interface VLAN and enter the interface ID of your desired entry.
- Interface Routed Port: Select Interface Routed Port and enter the interface ID of your desired entry.

➢ **PIM SM Neighbor**

Interface: The physical interface on which PIM DM is enabled.

Neighbor: The IP address of the PIM neighbor for which this entry contains information.

Uptime: The time since the PIM neighbor (last) became a neighbor of the local switch.

Expires: The time remaining before the PIM neighbor will be aged out.

11.4.3 BSR

PIM SM uses a Bootstrap Router (BSR), which advertises information to other multicast routers about the rendezvous point (RP). In a given network, a set of routers can be administratively enabled as candidate bootstrap routers(C-BSR). If it is not apparent which router should be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, then the candidate with the highest IP address becomes the BSR.

Choose the menu **Multicast Routing→PIM SM→BSR** to load the following page.

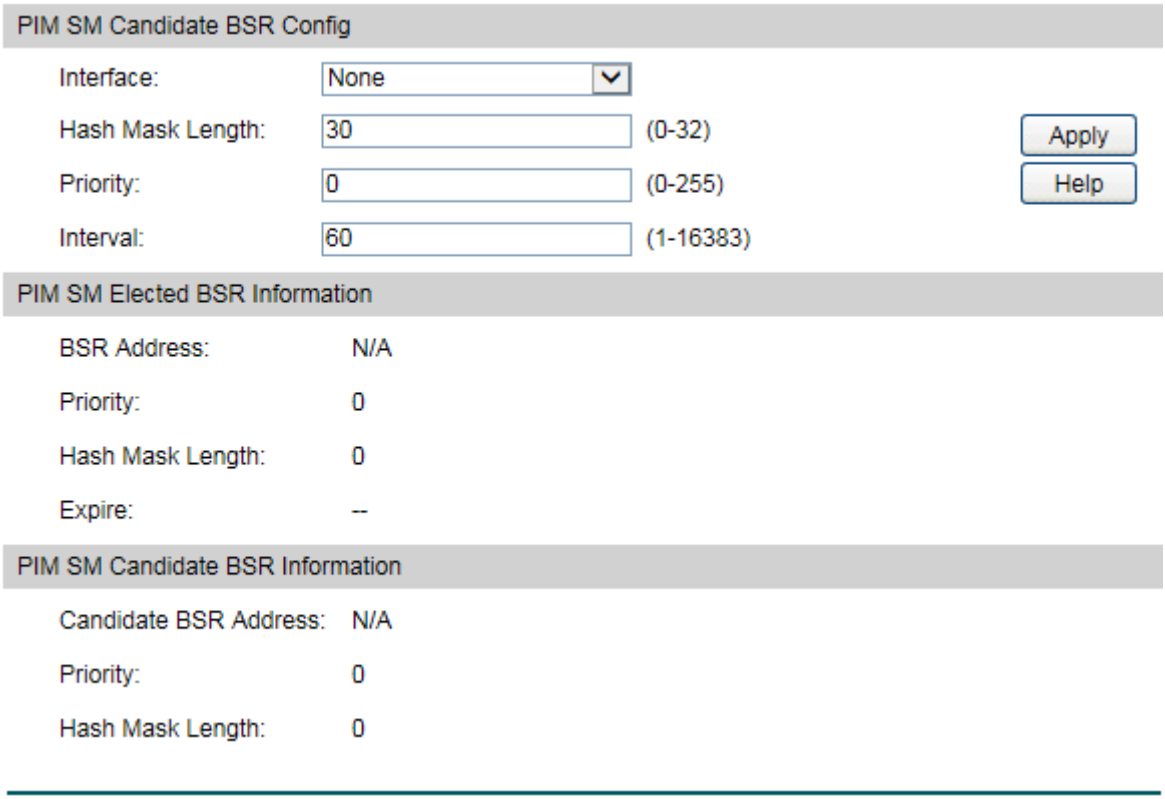


Figure 11-22 BSR

The following entries are displayed on this screen:

➢ **PIM SM Candidate BSR Config**

Configure the candidate BSR of current device.

Interface: Select the interface on this switch from which the BSR address is derived to make it a candidate. This interface must be enabled with PIM SM.

Hash Mask Length: specify the mask length that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP The valid value range from 0 to 32 and the default value is 30.

Priority: Specify the priority of the BSR. The BSR with the larger priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The valid value range from 0 to 255 and the default value is 64

Interval: The BSR Advertisement interval, ranging from 1 to 16383.

➢ **PIM SM Elected BSR Information**

BSR Address: Displays the elected BSR address.

Priority: Displays the priority of the elected BSR.

Hash Mask Length: Displays the hash mask length of the elected BSR.

Next BSR message time:	Displays the time of next BSR message sending if this is the elected BSR.
Expire:	Displays the expiry time of the elected BSR.

➢ **PIM SM Candidate BSR Information**

Candidate BSR Address:	Displays the Candidate BSR address.
Priority:	Displays the priority of the Candidate BSR.
Hash Mask Length:	Displays the hash mask length of the Candidate BSR.

11.4.4 RP

In the PIM SM mode, RP receives multicast data from the source and transmits the data down the shared tree to the multicast group members. You must have an RP if the interface is in sparse-dense mode, and you can manually assign static RP or config candidate RP to generate the RP.

Choose the menu **Multicast Routing→PIM SM→RP** to load the following page.

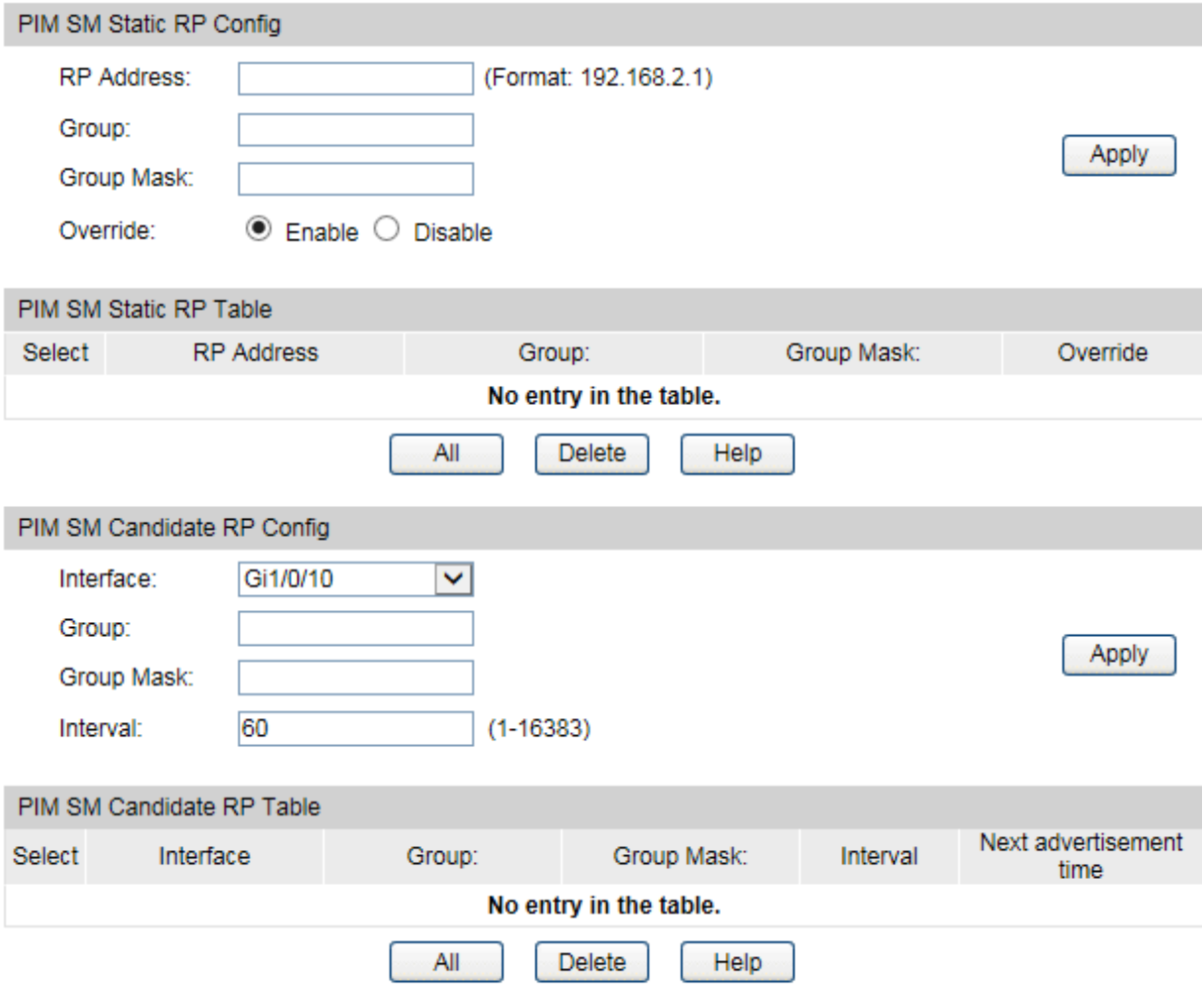


Figure 11-23 RP Config

The following entries are displayed on this screen:

➢ **PIM SM Static RP Config**

By default, no static RP address is configured. You could configure the IP address of RPs on all multilayer switches.

RP Address: Specify the IP address of the static RP.

Group: Group Address of the RP to be created or deleted.

Group Mask: Group Mask of the RP to be created or deleted.

Override: Select to enable or disable override mode. If the override mode is enabled, the static RP will take effect no matter the candidate RP is configured or not. Otherwise the static RP will be invalid when the candidate RP is configured.

➢ **PIM SM Static RP Table**

Displays the configured static RP of this PIM SM domain.

RP Address: Displays the ip address of static RP.

Group: Displays the group address.

Group Mask: Displays the group mask.

Override: Displays the override mode. If the override mode is enabled, the static RP will take effect no matter the candidate RP is configured or not. Otherwise the static RP will be invalid when the candidate RP is configured.

➢ **PIM SM Candidate RP Config**

Configure the candidate RP on this device. Candidate RPs periodically send multicast RP-announce messages to a particular group or group range to announce their availability.

Interface: Select the VLAN interface of the candidate RP.

Group: The group address transmitted in Candidate-RP-Advertisements.

Group Mask: The group address mask transmitted in Candidate-RP-Advertisements.

Interval: Specify the interval of advertisement message of the candidate RP in seconds. The default value is 60.

➢ **PIM SM Candidate RP Table**

Interface: Displays the VLAN interface of the candidate RP.

Group: Displays the group address transmitted in Candidate-RP-Advertisements.

Group Mask: Displays the group address mask transmitted in Candidate-RP-Advertisements.

Interval: Displays the interval of advertisement message of the candidate RP in seconds.

Next advertisement time: Displays the remaining time to send the next RP advertisement packet.

11.4.5 RP Mapping

Choose the menu **Multicast Routing→PIM SM→RP Mapping** to load the following page.

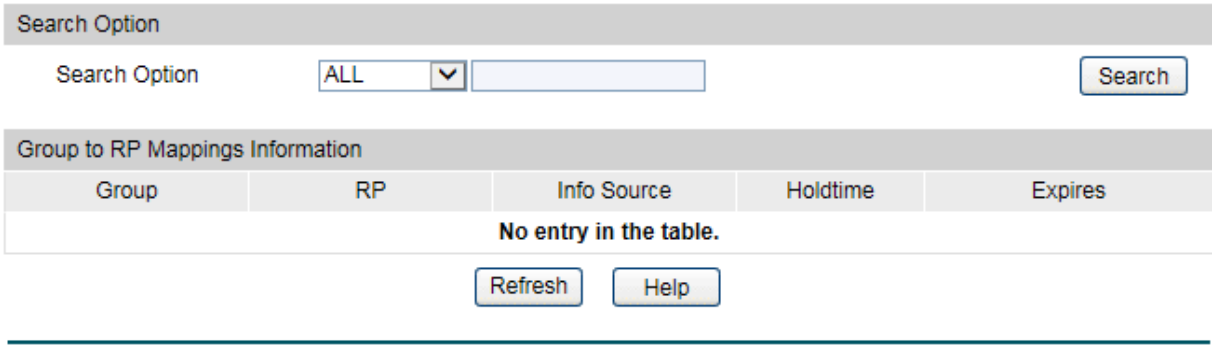


Figure 11-24 RP Mapping

The following entries are displayed on this screen:

➢ **Search Option**

Search Option:
- **ALL**: Select All to display all entries.
- **RP**: Select RP and enter the RP IP address of desired entry.

➢ **Group to RP Mappings Information**

Group: Displays the group address.

RP: Displays the RP address.

Info Source: Displays the BSR address which announce the RP information.

Holdtime: Displays the holdtime of the RP.

Expires Displays the expiry time of the RP. If RP is static, the expiry time will be Never.

11.4.6 RP Info

Choose the menu **Multicast Routing→PIM SM→RP Info** to load the following page.

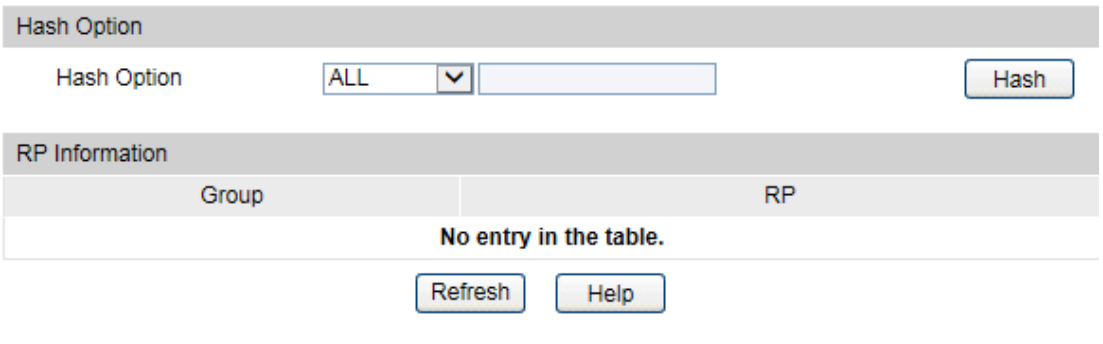


Figure 11-25 RP Info

The following entries are displayed on this screen:

➢ **Search Option**

Search Option:
- **ALL**: Select All to display all entries.
- **Group**: Select Group and enter the group IP address of desired entry.

➢ **RP Information**

Group: Displays the group address.

RP: Displays the RP address.

Configuration Procedure for PIM SM:

Step	Operation	Description
1	Configure interface.	Required. Configure IP addresses and subnet masks of routing interfaces on **Routing→ Interface→Interface Config** page.
2	Configure routing protocol.	Required. Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all the switches can communicate with each other and update the routing information through a unicast routing protocol dynamically.
3	Enable multicast routing and PIM SM.	Required. Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM SM on routing interfaces on **Multicast Routing→PIM SM→PIM SM Interface** page.
4	Configure static RP or configure candidate BSR and candidate RP.	Required. Configure static RP or configure a specified routing interface as candidate RP on **Multicast Routing→PIM SM→RP** page. Configure a specified routing interface as candidate BSR on **Multicast Routing→PIM SM→BSR** page.
5	Enable IGMP.	Required. Enable IGMP on the routing interfaces which connect to the receivers on **Multicast Routing→IGMP→Interface Config** page.

11.4.7 PIM SSM

While PIM-SM employs a specially-configured RP router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Source Specific Multicast (PIM-SSM) does not use an RP. It supports only source-route deliver trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly-connected LANs. The SSM service model can be implemented with a strict subset of the PIM-SM protocol mechanisms. Both regular IP Multicast and SSM semantics can coexist on a single router and both can be implemented using the PIM-SM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4, is reserved for SSM.

Choose the menu **Multicast Routing→PIM SM→PIM SSM** to load the following page.

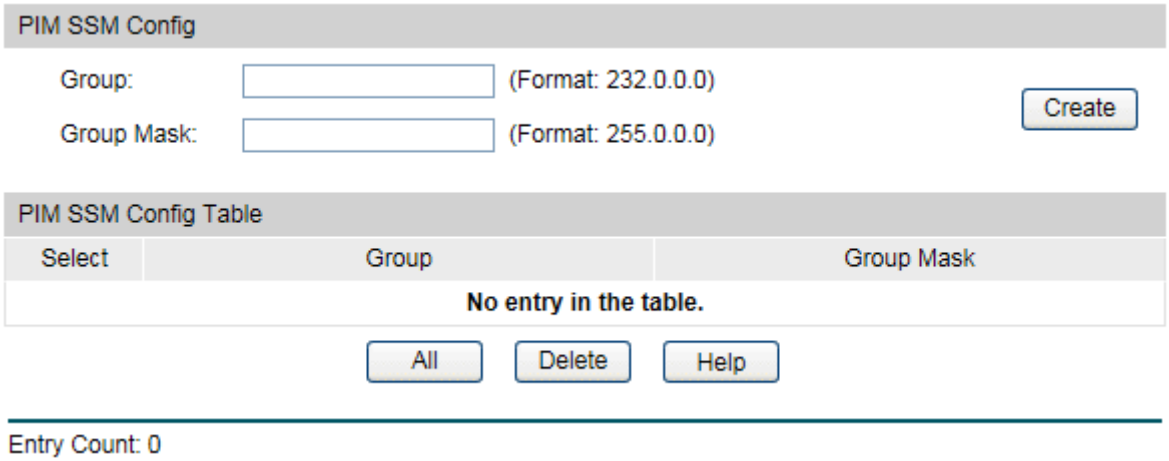


Figure 11-25 PIM SSM Config

The following entries are displayed on this screen:

- **PIM SSM Config**

  Group: Enter the source-specific multicast group ip-address.

  Group Mask: Enter the source-specific multicast group ip-address mask.

- **PIM SSM Config Table**

  Select: Enter the source-specific multicast group ip-address.

  Group: Displays the source-specific multicast group ip-address.

  Group Mask: Displays the source-specific multicast group ip-address mask.

11.4.8 Packet Statistics

Choose the menu **Multicast Routing→PIM SM→Packet Statistics** to load the following page.

Figure 11-25 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.

➢ **PIM SM Statistics**

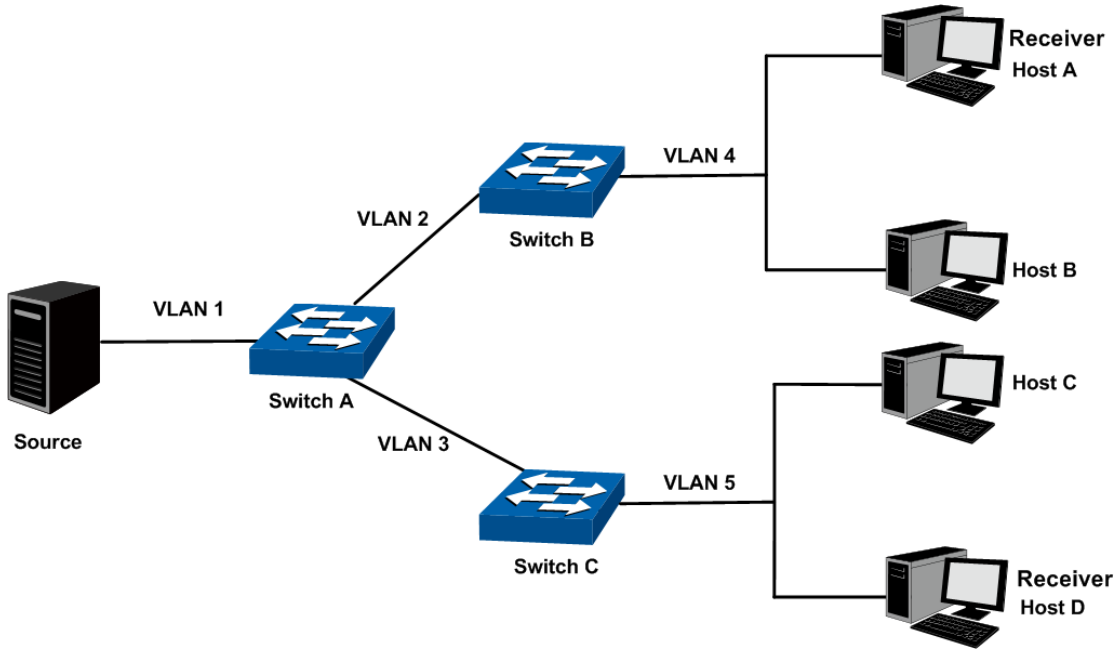
Interface:	The interface on which PIM SM is enabled.
Stat:	Rx: Packet Received in Protocol. Tx: Packet Sent from Protocol.
Hello:	Hello Format Packets Statistics.
Register:	Register Format Packets Statistics.
Reg-Stop:	Register-Stop Format Packets Statistics.
Join/Pru:	Join/Prune Format Packets Statistics.
BSR:	Bootstrap Format Packets Statistics.
Assert:	Assert Format Packets Statistics.
CRP:	Candidate-RP-Advertisement Format Packets Statistics.
Error Packet:	Err Packets Statistics.

11.4.9 Application Example for PIM SM

➢ **Network Requirements**

1. Receivers receive VOD data through multicast. The whole network runs PIM SM as multicast routing protocol.
2. Host A and Host D act as multicast receivers.
3. Switch A connects to Switch B in VLAN 2, connects to Switch C in VLAN 3. The Source server connects to Switch A in VLAN 1.
4. Host A and B connect to Switch B in VLAN 4. Host C and D connect to Switch C in VLAN 5.
5. All switches run PIM SM. The VLAN interfaces connected to hosts run IGMP protocol.
6. Specify VLAN interface 3 in switch A as candidate BSR and candidate RP.

➢ **Network Diagram**



The IP addresses of VLAN interfaces in each switch are displayed below:

Switch A: VLAN interface 1: 192.168.1.2/24

VLAN interface 2: 192.168.2.2/24

VLAN interface 3: 192.168.3.2/24

Switch B: VLAN interface 2: 192.168.2.100/24

VLAN interface 4: 192.168.4.100/24

Switch C: VLAN interface 3: 192.168.3.100/24

VLAN interface 5: 192.168.5.100/24

➢ **Configuration Procedure**

- Configure Switch A:

Step	Operation	Description
1	Configure interface.	Configure IP addresses and subnet masks of VLAN interfaces 1, 2 and 3 on **Routing→ Interface→Interface Config** page.
2	Configure routing protocol.	Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all the switches can communicate with each other and update the routing information through a unicast routing protocol dynamically.
3	Enable multicast routing and PIM SM.	Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM SM on VLAN interfaces 1, 2 and 3 on **Multicast Routing→PIM SM→PIM SM Interface** page.

4	Configure candidate BSR and candidate RP.	Configure VLAN interface 1 as candidate BSR on **Multicast Routing→PIM SM→BSR** page. Configure VLAN interface 1 as candidate RP on **Multicast Routing→PIM SM→RP** page.

- Configure Switch B and C:

Step	Operation	Description
1	Configure interface.	Configure IP addresses and subnet masks of VLAN interfaces 2, 3, 4 and 5 on **Routing→ Interface→Interface Config** page.
2	Configure routing protocol.	Configure the routing entries via static route or dynamic routing protocol like OSPF, and make sure all network can communicate with each other.
3	Enable multicast routing and PIM SM.	Enable multicast routing on **Multicast Routing→Global Config** page. Enable PIM SM on VLAN interfaces 2, 3, 4 and 5 on **Multicast Routing→PIM SM→PIM SM Interface** page.
4	Enable IGMP.	Enable IGMP on the VLAN interfaces 4 and 5 which connect to the receivers on **Multicast Routing→IGMP→Interface Config** page.

11.5 Static Mroute

When the multicast network topology is the same as that of the unicast network, receivers can receive the multicast data through the unicast route. But in some circumstances, the multicast network topology differs from that of unicast network or some routers in the network supports unicast only. Then you can configure static multicast routes to offer different transferring paths for multicast and unicast data separately. Notice the following two considerations:

- The static multicast routing functions only to affect the RPF check, but not to direct the forwarding of the multicast data, so it is also called RPF static routing;
- The static multicast routing only functions in the configured multicast router. It won't be broadcasted or imported into other routers in any way.

The static multicast routing is an important foundation for the RPF check. In the RPF check process, with static multicast routing configured, the router will choose one as the RPF route after comparing the optimal unicast route and the static multicast route selected respectively from the unicast routing table and the static multicast routing table.

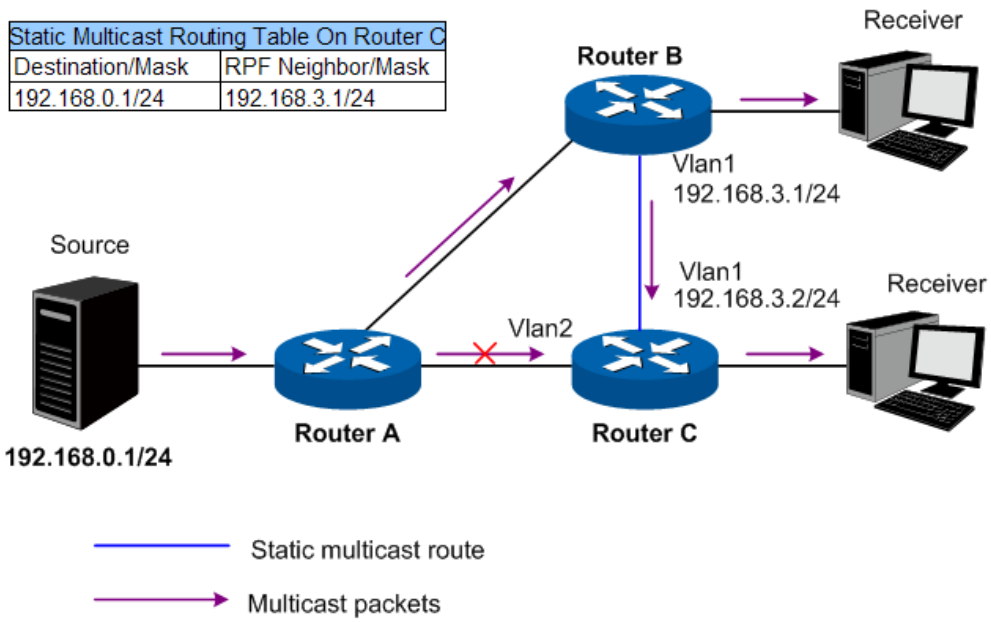


Figure 11-26 Static Multicast Routing

As shown in Figure 11-26, when no static multicast routing entry is configured, the RPF neighbor of Router C to the multicast source is Router A. The multicast packets sent from Source will be transferred along the path Router A→Router C, which is the same as the unicast path. When Router C is configured with static multicast routing and the RPF neighbor of Router C to Source is configured as Router B, the multicast data sent from Source will travel along a different path Router A→Router B→Router C.

11.5.1 Static Mroute Config

Choose the menu **Multicast Routing→Static Mroute→Static Mroute Config** to load the following page.

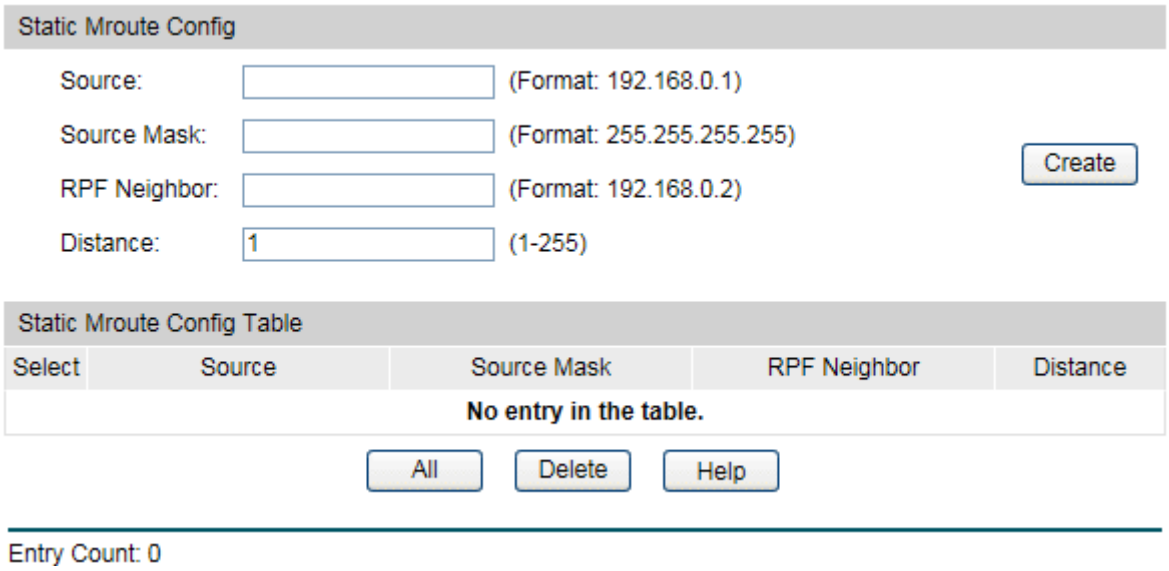


Figure 11-27 Static Mroute Config

The following entries are displayed on this screen:

- **Static Mroute Config**

Source:	Enter the IP address that identifies the multicast source of the entry you are creating.
Source Mask:	Enter the subnet mask to be applied to the Source.
RPF Neighbor:	Enter the IP address of the neighbor router on the path to the mroute source.
Distance:	Enter the Administrative distance of static mroute. The range is 0-255 and default is 0. The lower the distance, the better the preference.

- **Static Mroute Config Table**

Select:	Select the static mroute entry to modify.
Source:	Displays the IP address of the multicast source.
Source Mask:	Displays the subnet mask of source.
RPF Neighbor:	Displays the IP address of the neighbor router.
Distance:	Displays the Administrative distance of static mroute.

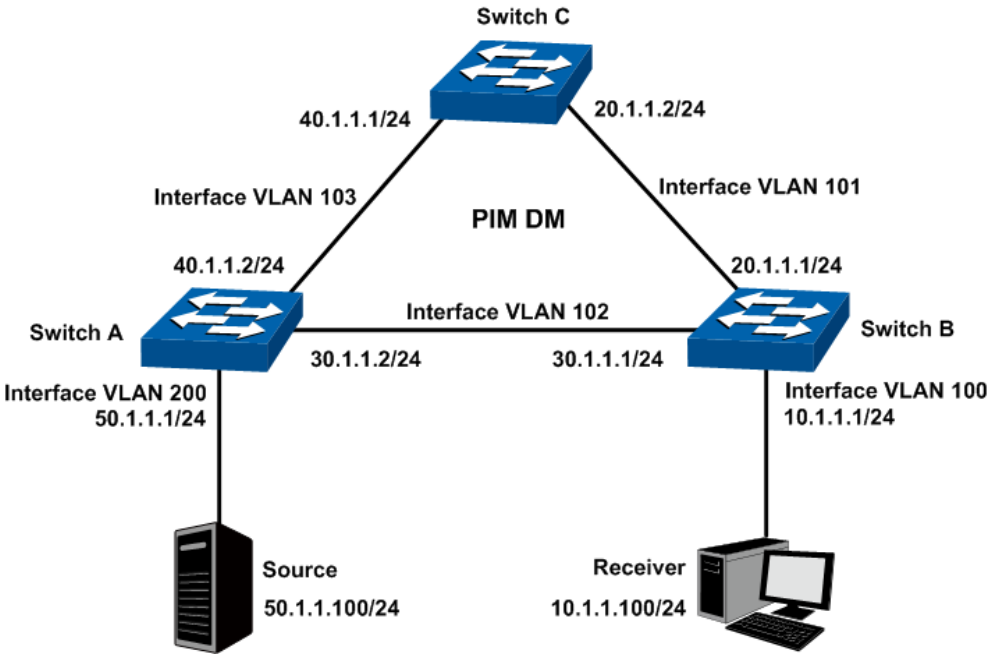
Click **delete** to delete the selected entry.

11.5.2 Application Example for Static Mroute

- **Network Requirements**

1. The network runs PIM DM and all the switches in the network support multicast features.
2. Switch A, Switch B and Switch C run OSPF protocol.
3. In normal circumstances, Receiver receives multicast data from Source through the path Switch A-Switch B, which is the same as the unicast route.
4. After the configuration takes effect, Receiver will receive multicast data from Source through the path Switch A-Switch C-Switch B.

➢ **Network Diagram**



➢ **Configuration Procedure**

1) Configure the interfaces and unicast routing protocol

Configure the VLAN interfaces and their IP addresses of Switch A, Switch B and Switch C on the page **Routing→ Interface→ Interface Config** according to the topology,

Configure the OSPF features on the switches in this PIM DM domain, making the switches accessible with each other at the network layer. Detailed configuration process is omitted here.

2) Configure the multicast routing features

- Configure Switch A

Step	Operation	Note
1	Enable IP multicast routing	Required. On page **Multicast Routing→Global Config→Global Config**, enable the Multicast Routing function globally.
2	Enable PIM DM	Required. On page **Multicast Routing→PIM DM→PIM DM Interface**, enable PIM DM on the VLAN interfaces 102, 103 and 200.

- Configure Switch B

Step	Operation	Note
1	Enable IP multicast routing	Required. On page **Multicast Routing→Global Config→Global Config**, enable the Multicast Routing function globally.
2	Enable PIM DM	Required. On page **Multicast Routing→PIM DM→PIM DM Interface**, enable PIM DM on the VLAN interfaces 100, 101 and 102.

Step	Operation	Note
3	Enable IGMP	Required. On page **Multicast Routing→IGMP→Interface Config**, enable the IGMP function on VLAN interface 100.
4	Configure static multicast routing	Required. On page **Multicast Routing→Static Mroute→Static Mroute Config**, configure a static multicast routing entry with the Source as 50.1.1.100, the Source Mask as 255.255.255.0 and the RPF Neighbor as 20.1.1.2.

- Configure Switch C

Step	Operation	Note
1	Enable IP multicast routing	Required. On page **Multicast Routing→Global Config→Global Config**, enable the Multicast Routing function globally.
2	Enable PIM DM	Required. On page **Multicast Routing→PIM DM→PIM DM Interface**, enable PIM DM on the VLAN interfaces 101 and 103.

3) Verify the configuration

On page **Multicast Routing→Global Config→Mroute Table** on Switch A, check the RPF neighbor of the entry whose Source is 50.1.1.100/24. The RPF neighbor should be 20.1.1.2 (the interface on Switch C) if the configuration is valid.

Return to CONTENTS

Chapter 12 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.

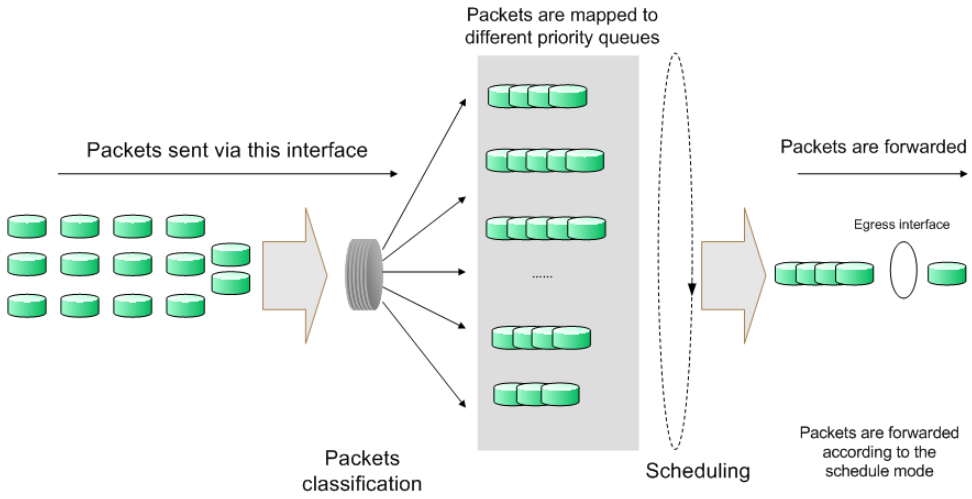


Figure 12-1 QoS function

- 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 three schedule modes: SP, WRR and SP+WRR.

➢ **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

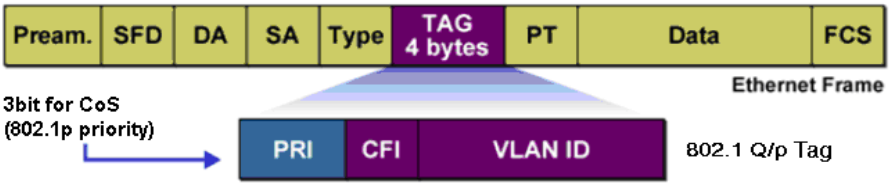


Figure 12-2 802.1Q frame

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

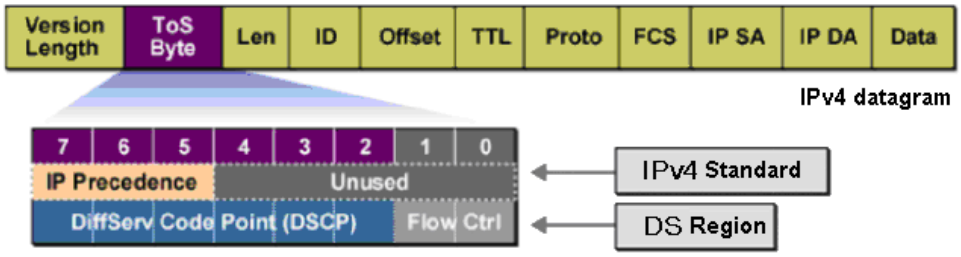


Figure 12-3 IP datagram

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 if 8021.1P Priority mode is enabled; 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 seven scheduling queues, ranging from TC0 to TC6. TC0 has the lowest priority while TC6 has the highest priority. The switch supports three schedule modes: SP, WRR and SP+WRR.

1. SP-Mode: Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. The switch has eight egress queues labeled as TC0, TC1, TC2 …TC6. In SP mode, their priorities increase in order. TC6 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.

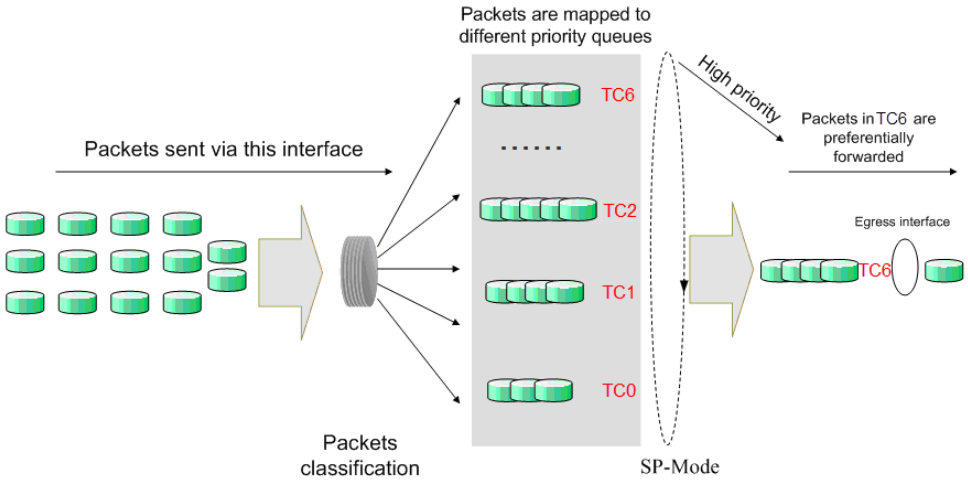


Figure 12-4 SP-Mode

2. WRR-Mode: Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. The weight value indicates the occupied proportion of the resource. WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time. In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of. The default weight value ratio of TC0, TC1, TC2, TC3, TC4, TC5 and TC6 is 1:2:3:4:5:6:7.

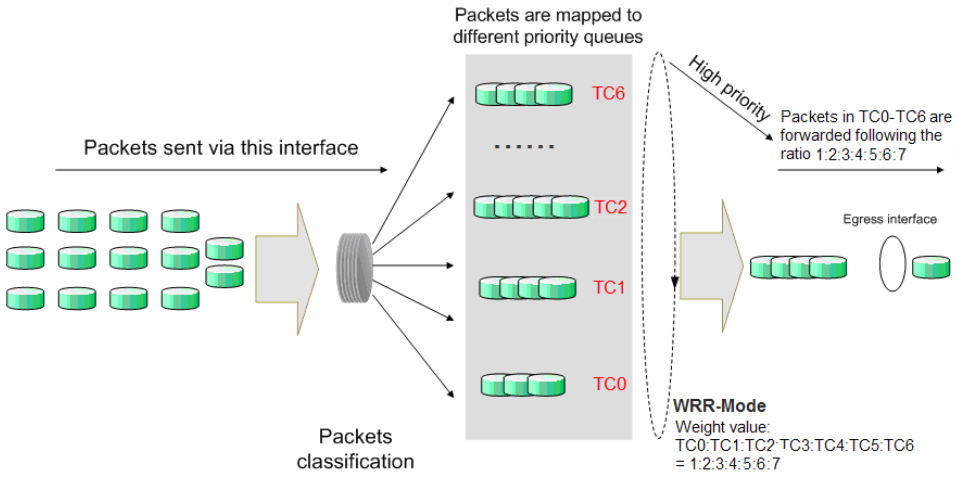


Figure 12-5 WRR-Mode

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, TC6 is in the SP group; TC0, TC1, TC2 to TC5 belong to the WRR group and the weight value ratio of TC0, TC1, TC2 to TC6 is 1:2:3:4:5:6:7. In this way, when scheduling queues, the switch allows TC6 to occupy the whole bandwidth following the SP mode and the TC0, TC1, TC2 to TC5 in the WRR group will take up the bandwidth according to their ratio 1:2:3:4:5:6.

The QoS module is mainly for traffic control and priority configuration, including five submenus: **Class of Service**, **DiffServ**, **Bandwidth Control, Voice VLAN** and **Auto VoIP**.

12.1 Class of Service

The Class of Service (CoS) queueing feature allows you configure certain aspects of switch queueing. It provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms. The switch implements three priority modes based on port, on 802.1P and on DSCP, and supports three queue scheduling algorithms.

The Class of Service function can be implemented on **Trust Mode**, **Port Priority**, **802.1P/CoS to Queue Mapping, DSCP to Queue Mapping** and **Schedule Mode** pages.

12.1.1 Trust Mode

On this page you can configure the trust mode. The switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode).

Choose the menu **QoS→Class of Service→Trust Mode** to load the following page.

Figure 12-6 Port Priority Config

Configuration Procedure:

Configure the trust mode according to your needs, then click **Apply**.

Entry Description:

Trust Mode: Configure the trust mode.

untrusted: untrusted mode. In this mode, data will be classified into different service based on the port priority and the 802.1p/CoS mapping.

trust 802.1p: trust 802.1p mode. In this mode, data will be classified into different service based on the 802.1p priority and the 802.1P/CoS mapping.

trust ip-dscp: trust ip-dscp mode. In this mode, data will be classified into different service based on the DSCP priority and the DSCP-mapping.

12.1.2 Port Priority

On this page you can configure the port priority.

Choose the menu **QoS→Class of Service→Port Priority** to load the following page.

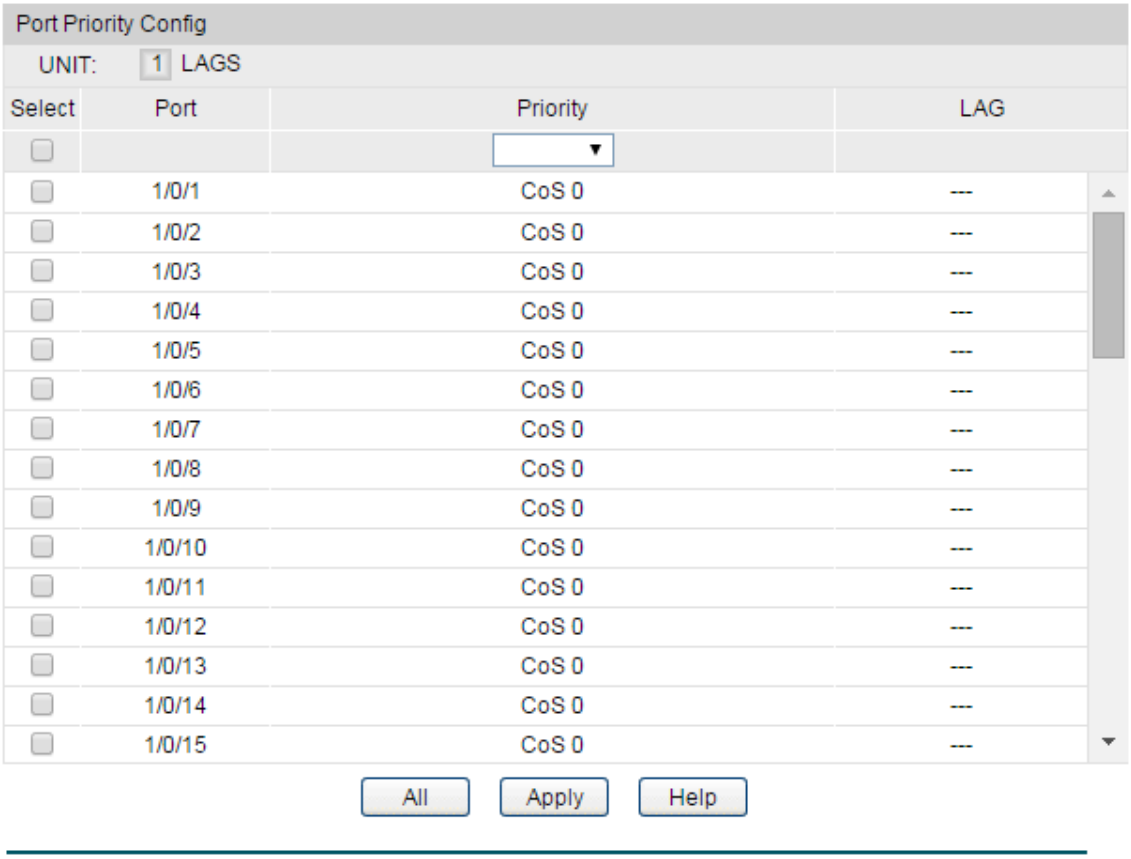


Figure 12-6 Port Priority Config

Configuration Procedure:

Select the desired port or LAG to set its priority. Click **Apply**.

Entry Description:

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 CoS queue that the port will be mapped to.

The packets are firstly mapped to CoS queues, then to TC queues according to the **802.1P/CoS to Queue Mapping** relations.

LAG: Displays the aggregation group which the port is in.

Note:

1) All the ports in the same LAG should be assigned with the same port priority.
2) To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

Configuration Procedure:

Step	Operation	Description
1	Enable the port Priority	Required. On **QoS→Class of Service→Trust Mode** page, select untrusted mode.
2	Select the port priority	Required. On **QoS→Class of Service→Port Priority** page, configure the port priority.
3	Configure the mapping relation between the CoS priority and TC	Required. On **QoS→Class of Service→802.1P/CoS to Queue Mapping** page, configure the mapping relation between the CoS and TC.
4	Select a schedule mode	Required. On **QoS→Class of Service→Schedule Mode** page, select a schedule mode.

12.1.3 802.1P/CoS to Queue Mapping

On this page you can configure the mapping relation between the 802.1P priority 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→Class of Service→802.1P/CoS to Queue Mapping** to load the following page.

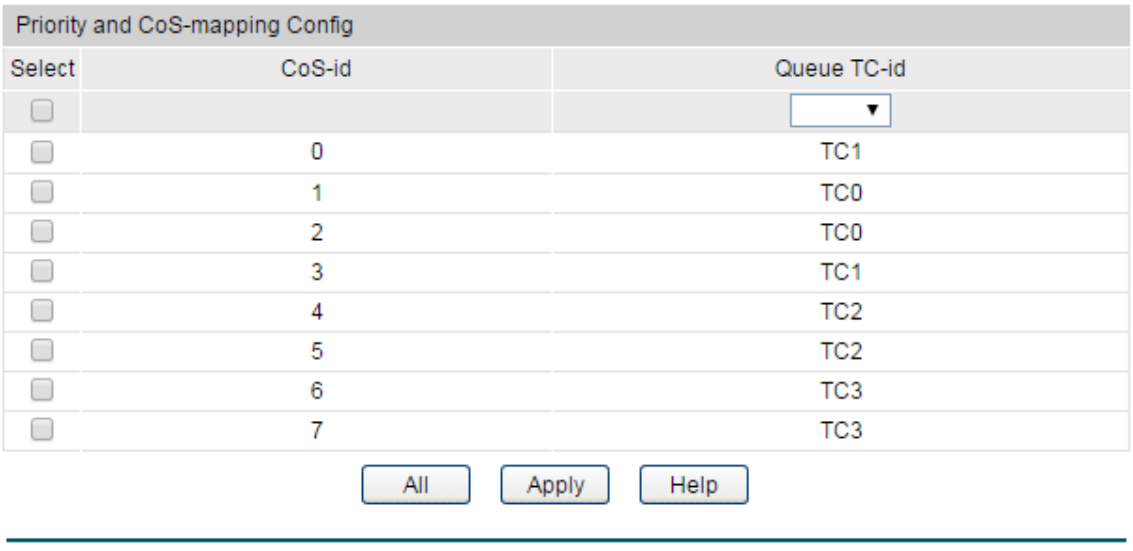


Figure 12-8 802.1P Priority

Configuration Procedure:

Configure the CoS-id-TC mapping relations. Click **Apply**.

Entry Description:

CoS-id: CoS-id is a value for the switch to establish mapping relations between the priorities and TC queues. The valid values are from 0 to 7 and correspond to the 802.1P priority levels.

Queue TC-id: Select a TC queue that you want the CoS-id to be mapped to.

The switch supports 7 TC queues, from TC0 for the lowest priority to TC 6 for the highest priority.

Note:

To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

Configuration Procedure:

Step	Operation	Description
1	Enable the 802.1P Priority	Required. On **QoS→Class of Service→Trust Mode** page, select trust 802.1p mode.
2	Configure the mapping relation between the 802.1P priority CoS and the TC	Required. On **QoS→Class of Service→802.1P/CoS to Queue Mapping** page, configure the mapping relation between the 802.1P priority CoS and the TC.
3	Select a schedule mode	Required. On **QoS→Class of Service→Schedule Mode** page, select a schedule mode.

12.1.4 DSCP to Queue Mapping

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 trust ip-dscp mode is selected, 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 trust 802.1p mode is selected; the untagged non-IP datagram are mapped based on port priority mode.

Choose the menu **QoS→Class of Service→DSCP to Queue Mapping** to load the following page.

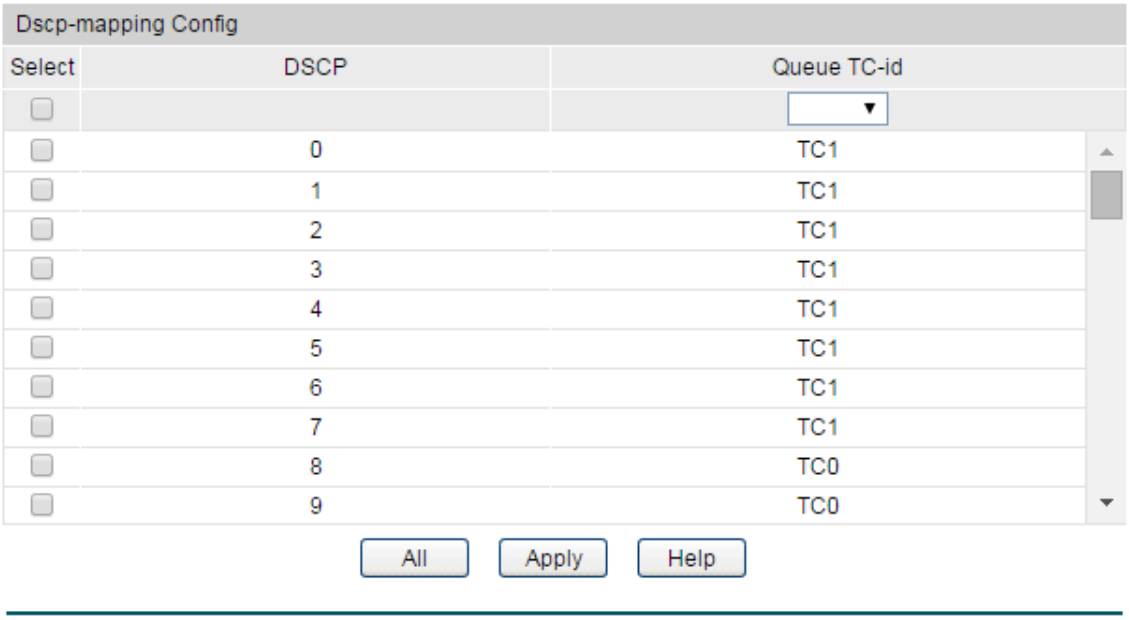


Figure 12-9 DSCP Priority

Configuration Procedure:

Configure the DSCP-TC mapping relations. Click **Apply**.

Entry Description:

DSCP: Select the desired DSCP priority.

DSCP priority represents the DSCP field in the IP packet header. It comprises 6 bits and the valid values are from 0 to 63.

Queue TC-id: Select a TC queue that the DSCP priority will be mapped to.

The switch supports 7 TC queues, from TC0 for the lowest priority to TC 6 for the highest priority.

Note:

To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

Configuration Procedure:

Step	Operation	Description
1	Enable DSCP Priority	Required. On **QoS→Class of Service→Trust Mode** page, select trust ip-dscp mode.
2	Configure the mapping relation between the DSCP priority and TC	Required. On **QoS→Class of Service→DSCP Priority** page, enable DSCP Priority and configure the mapping relation between the DSCP priority and TC.

3	Select a schedule mode	Required. On **QoS→Class of Service→Schedule Mode** page, select a schedule mode.

12.1.5 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…TC6.

Choose the menu **QoS→Class of Service→Schedule Mode** to load the following page.

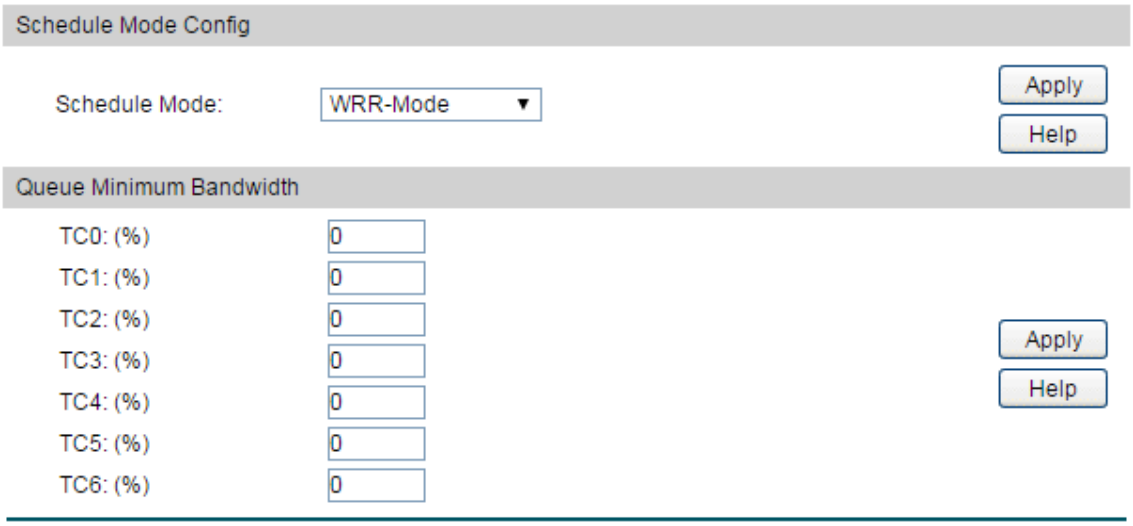


Figure 12-7 Schedule Mode

Configuration Procedure:

1) Select a schedule mode. Click **Apply**.
2) (Optional) Configure the weight value of the each TC queue if the schedule mode is WRR of SP+WRR. Click **Apply**.

Entry Description:

- **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 to TC6 is 1:2:3:4:5:6:7.

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, TC6 is in the SP group; TC0, TC1, TC2 to TC5 belong to the WRR group and the weight value ratio of TC0, TC1, TC2 to TC5 is 1:2:3:4:5:6. In this way, when scheduling queues, the switch allows TC6 to occupy the whole bandwidth following the SP mode and the TC0, TC1, TC2 to TC6 in the WRR group will take up the bandwidth according to their ratio 1:2:3:4:5:6:7.

- **Queue Minimum Bandwidth**

Queue Minimum Bandwidth: Set Minimum guaranteed bandwidth for TC0-TC6. Valid bandwidth range is 0% to 100%. Total queue minimum bandwidth value is 100%.

12.2 DiffServ

Differentiated Services (DiffServ) feature allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Packets are classified based on the criteria which is defined by a class. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet. The policy can be added to the ports after service configuration.

The DiffServ function can be implemented on **Global**, **Class Summary**, **Class Config, Policy Summary, Policy Config** and **Servive Config** pages.

12.2.1 Global

On this page you can configure the DiffServ Admin Mode and view the DiffServ Entry Table.

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

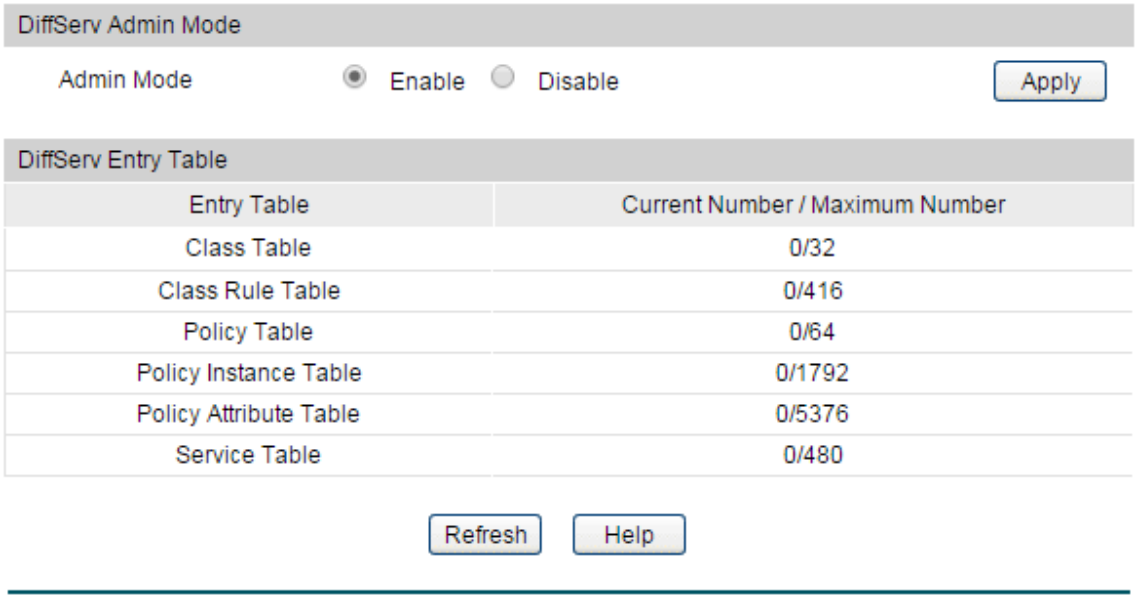


Figure 12-6 Global Config

Configuration Procedure:

Enable the DiffServ Admin Mode and click **Apply**.

Entry Description:

DiffServ Admin Mode: Enable or disable the administrative mode of DiffServ on the device. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.

Class Table: The current and maximum number of classifier entries in the table. DiffServ classifiers differentiate among traffic types.

Class Rule Table: The current and maximum number of class rule entries in the table. Class rules specify the match criteria that belong to a class definition.

Policy Table: The current and maximum number of policy entries in the table. The policy determines the traffic conditioning or service provisioning actions applied to a traffic class.

Policy Instance Table: The current and maximum number of policy-class instance entries in the table. A policy-class instance is a policy that is associated with an existing DiffServ class.

Policy Attribute Table: The current and maximum number of policy attribute entries in the table. A policy attribute entry attaches various policy attributes to a policy-class instance.

Service Table: The current and maximum number of service entries in the table. A service entry associates a DiffServ policy with an interface and inbound or outbound direction.

12.2.2 Class Summary

On this page you can configure DiffServ classes and view summary information about the classes that exist on the device.

Choose the menu **QoS→DiffServ→Class Summary** to load the following page.

Figure 12-6 Class Summary

Configuration Procedure:

Specify the name, type and protocol of the DiffServ Class, then click **Create**.

Entry Description:

Name:	Enter the class name. It ranges from 1 to 31 characters.
Type:	The class type.
Protocol:	The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.
Match Criteria:	Match criteria detail information of classes.

12.2.3 Class Config

Choose the menu **QoS→DiffServ→Class Config** to load the following page.

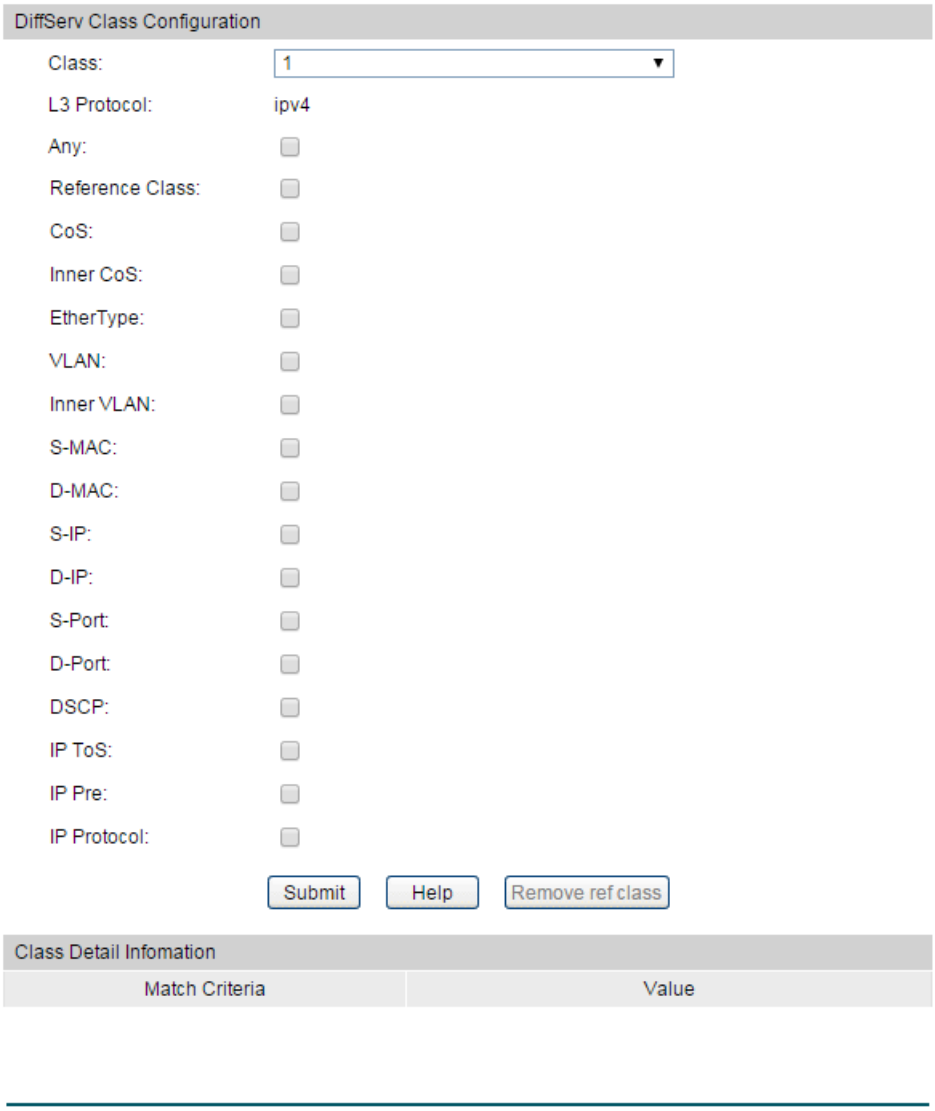


Figure 12-7 Class Config

Configuration Procedure:

Select a class from the drop-down list. Define the criteria to associate with a DiffServ class, then click **submit**.

Entry Description:

Class: The name of the class. To configure match criteria for a class, select its name from the menu.

L3 Protocol: The Layer 3 protocol to use for filtering class types, which is either IPv4 or IPv6.

Any: Select this option to specify that all packets are considered to match the specified class. There is no need to configure additional match criteria if Any is selected because a match will occur on all packets.

Reference Class:	Select this option to reference another class for criteria. The match criteria defined in the referenced class is as match criteria in addition to the match criteria you define for the selected class. After selecting this option, the classes that can be referenced are displayed. Select the class to reference. A class can reference at most one other class of the same type.
CoS:	Select this option to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.
Inner CoS:	Select this option to require the secondary CoS value in an Ethernet frame header to match the specified secondary CoS value.
EtherType:	Select this option to require the EtherType value in the Ethernet frame header to match the specified EtherType value.
VLAN:	Select this option to require a packet's VLAN ID to match a VLAN ID.
Inner VLAN:	Select this option to require a packet's VLAN ID to match a secondary VLAN ID.
S-MAC:	Select this option to require a packet's source MAC address to match the specified MAC address.
D-MAC:	Select this option to require a packet's destination MAC address to match the specified MAC address.
S-IP:	Select this option to require the source IP address in a packet header to match the specified values.
D-IP:	Select this option to require the destination IP address in a packet header to match the specified values.
S-IPv6:	Select this option to require the source IPv6 address in a packet header to match the specified values.
D-IPv6:	Select this option to require the destination IPv6 address in a packet header to match the specified values.
S-Port:	Select this option to require a packet's TCP/UDP source port to match the specified port number.
D-Port:	Select this option to require a packet's TCP/UDP destination port to match the specified port number.
DSCP:	Select this option to require the packet's IP DiffServ Code Point (DSCP) value to match the specified value.
IP ToS:	Select this option to require the packet's Type of Service (ToS) bits in the IP header to match the specified value.
IP Pre:	Select this option to require the packet's IP Precedence value to match the number configured in the IP Precedence Value field.

IP Protocol: Select this option to require a packet header's Layer 4 protocol to match the specified value.

Flow Label: Select this option to require an IPv6 packet's flow label to match the configured value.

12.2.4 Policy Summary

Choose the menu **QoS→DiffServ→Policy Summary** to load the following page.

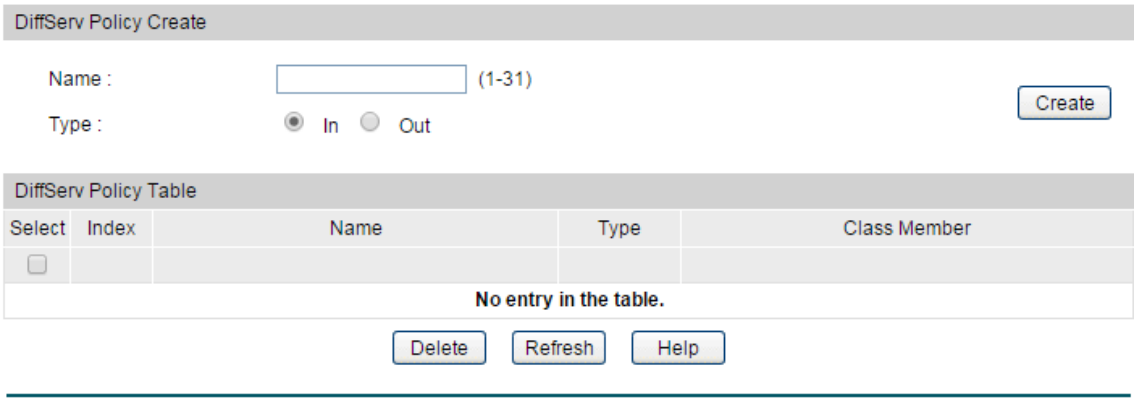


Figure 12-8 802.1P Priority

Configuration Procedure:

Create DiffServ policies and specify the traffic flow direction to which the policy is applied. Then click **Create**.

Entry Description:

- **DiffServ Policy Create**

  Name: Enter the DiffServ policy name. It ranges from 1 to 31 characters.

  Type: Specify the traffic flow direction to which the policy is applied.

- **DiffServ Policy Table**

  Name: The name of the DiffServ policy.

  Type: The traffic flow direction to which the policy is applied.

  Class Member: The DiffServ class or classes that have been added to the policy.

12.2.5 Policy Config

Choose the menu **QoS→DiffServ→Policy Config** to load the following page.

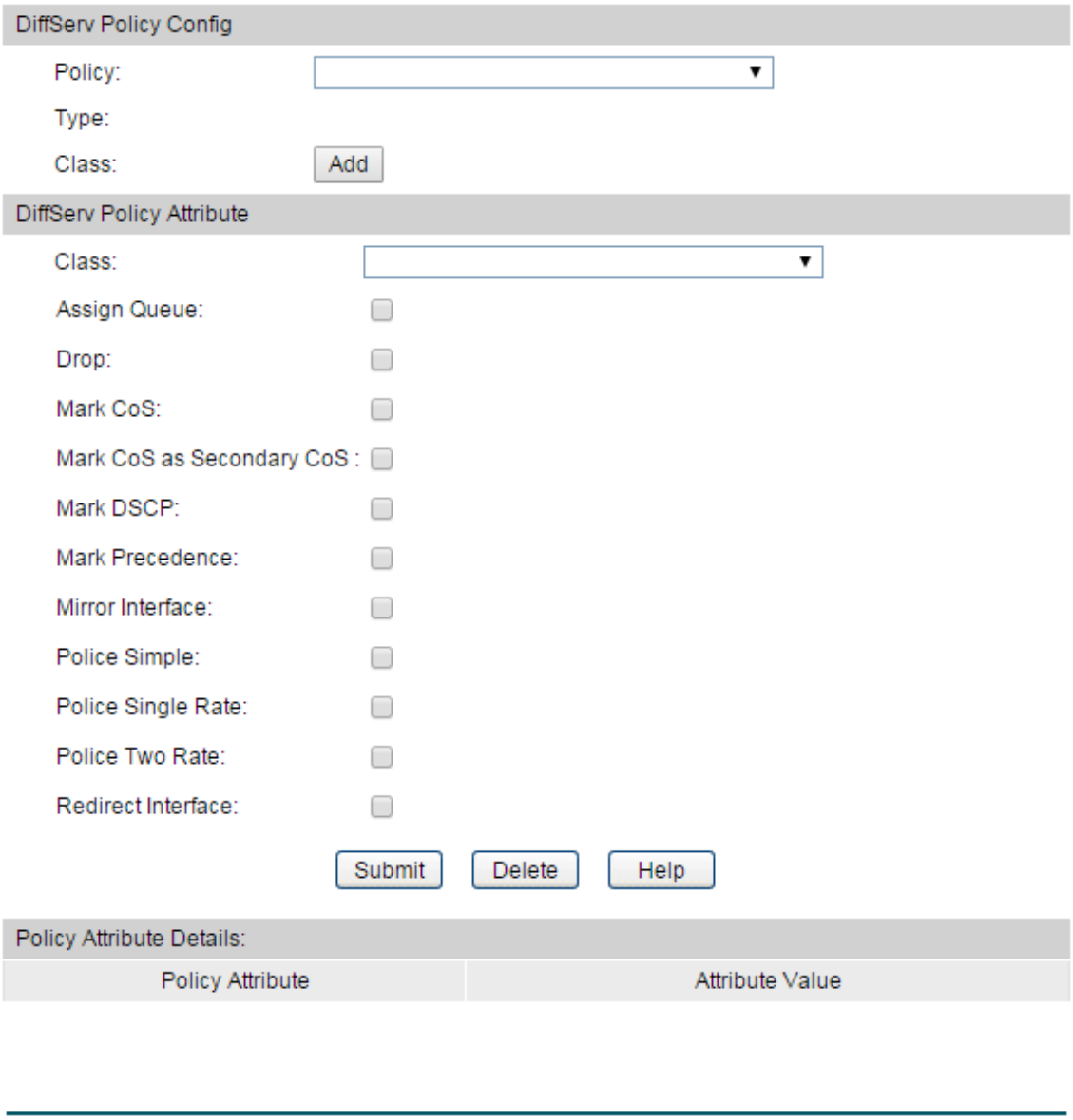


Figure 12-9 DSCP Priority

Configuration Procedure:

Add or remove a DiffServ policy-class association and configure the policy attributes.

Entry Description:

- **DiffServ Policy Config**

Policy: The name of the policy. To add a class to the policy, remove a class from the policy, or configure the policy attributes, you must first select its name from the menu.

Type: The traffic flow direction to which the policy is applied.

Class: The DiffServ class or classes associated with the policy. The policy is applied to a packet when a class match within that policy-class is found.

Add: Click this button to show the avaliable class list menu.

- **DiffServ Policy Attribute**

Class: Select a class to configure the policy attribute.

Assign Queue: Select this option to assign matching packets to a traffic queue. Use the Queue ID field to select the queue to which the packets of this policy-class are assigned.

Drop: Select this option to drop packets that match the policy-class.

Mark CoS: Select this option to mark all packets in a traffic stream with the specified Class of Service (CoS) queue value. Use the Class of Service field to select the CoS value to mark in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted.

Mark CoS as Secondary CoS : Select this option to mark the priority field of the 802.1p header in the outer tag of a double-VLAN tagged packet with the same CoS value that is included in the inner tag.

Mark DSCP: Select this option to mark all packets in the associated traffic stream with the specified IP DSCP value.

Mark Precedence: Select this option to mark all packets in the associated traffic stream with the specified IP Precedence value. After you select this option, use the IP Precedence Value field to select the IP Precedence to mark in packets that match the policy-class.

Mirror Interface: Select this option to copy the traffic stream to a specified egress port (physical or LAG) without bypassing normal packet forwarding. This action can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. Use the Interface menu to select the interface to which traffic is mirrored.

Police Simple: Select this option to enable the simple traffic policing style for the policy-class. The simple form of the police attribute uses a single data rate and burst size, resulting in two outcomes (conform and violate).

Police Single Rate: Select this option to enable the single-rate traffic policing style for the policy-class. The single-rate form of the police attribute uses a single data rate and two burst sizes, resulting in three outcomes (conform, exceed, and violate).

Police Two Rate: Select this option to enable the two-rate traffic policing style for the policy-class. The two-rate form of the police attribute uses two data rates and two burst sizes. Only the smaller of the two data rates is intended to be guaranteed.

Redirect Interface: Select this option to force a classified traffic stream to the specified egress port (physical port or LAG). Use the Interface field to select the interface to which traffic is redirected.

Note:

To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

12.2.6 Service Config

Choose the menu **QoS→DiffServ→Service Config** to load the following page.

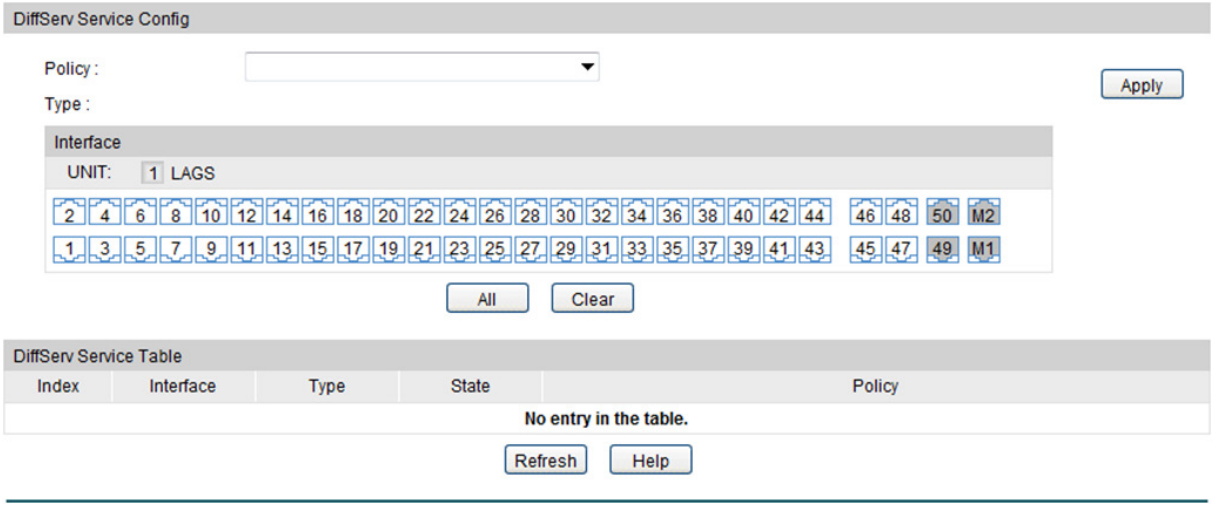


Figure 12-9 DSCP Priority

Configuration Procedure:

Add DiffServ policies to interfaces or remove policies from interfaces.

Entry Description:

- **DiffServ Service Config**

Policy: Select a policy.

Type: Displays the traffic flow direction to which the policy is applied.

Interface: Select one or more interfaces bound to the policy.

- **DiffServ Service Table**

Interface: Displays the interfaces that have an associated policy.

Type: Displays the traffic flow direction to which the policy is applied.

State: The status of the policy on the interface. A policy is Up if DiffServ is globally enabled, and if the interface is administratively enabled and has a link. Otherwise, the status is Down.

Policy: The DiffServ policy associated with the interface.

12.3 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.

12.3.1 Rate Limit

Rate limit functions to control the 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.

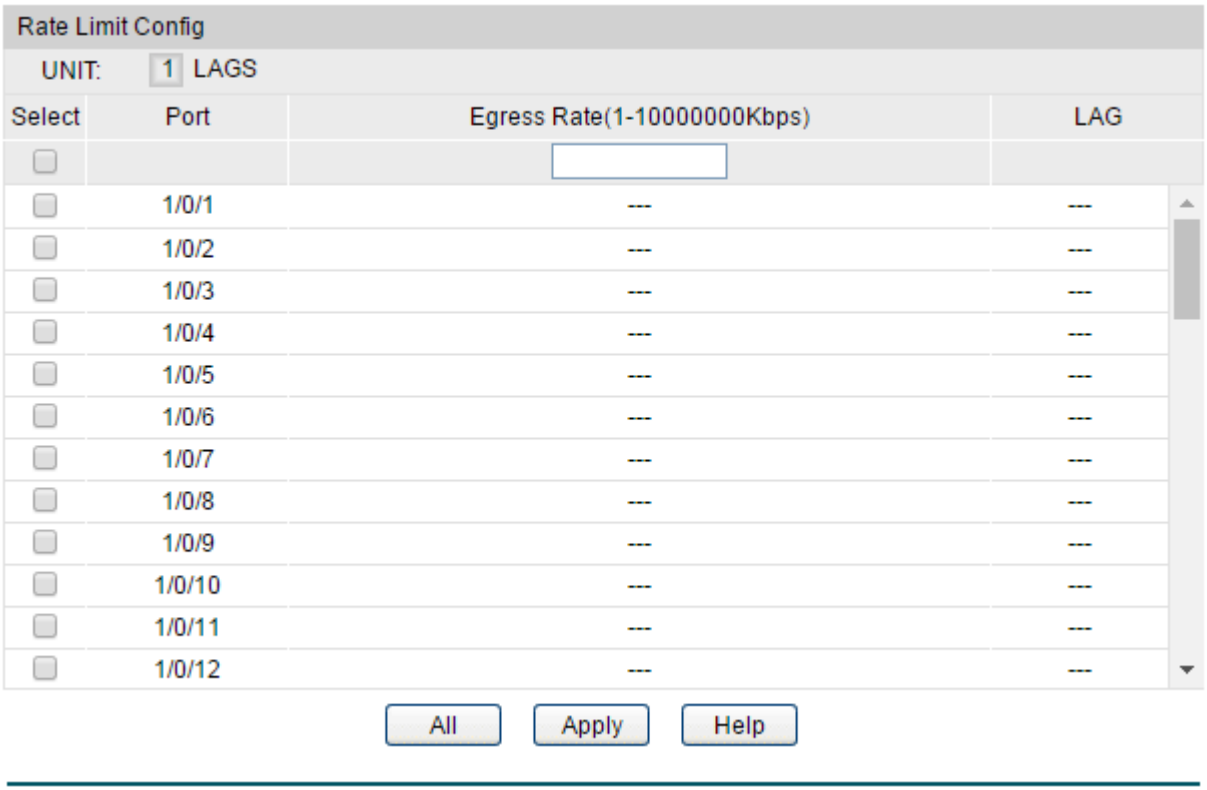


Figure 12-10 Rate Limit

Configuration Procedure:

1) Configure the upper rate limit for the port to send packets.
2) Click **Apply**.

Entry Description:

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.
Egress Rate:	Configure the bandwidth for sending packets on the port.
LAG:	Displays the LAG number which the port belongs to.

Note:

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.

12.3.2 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.

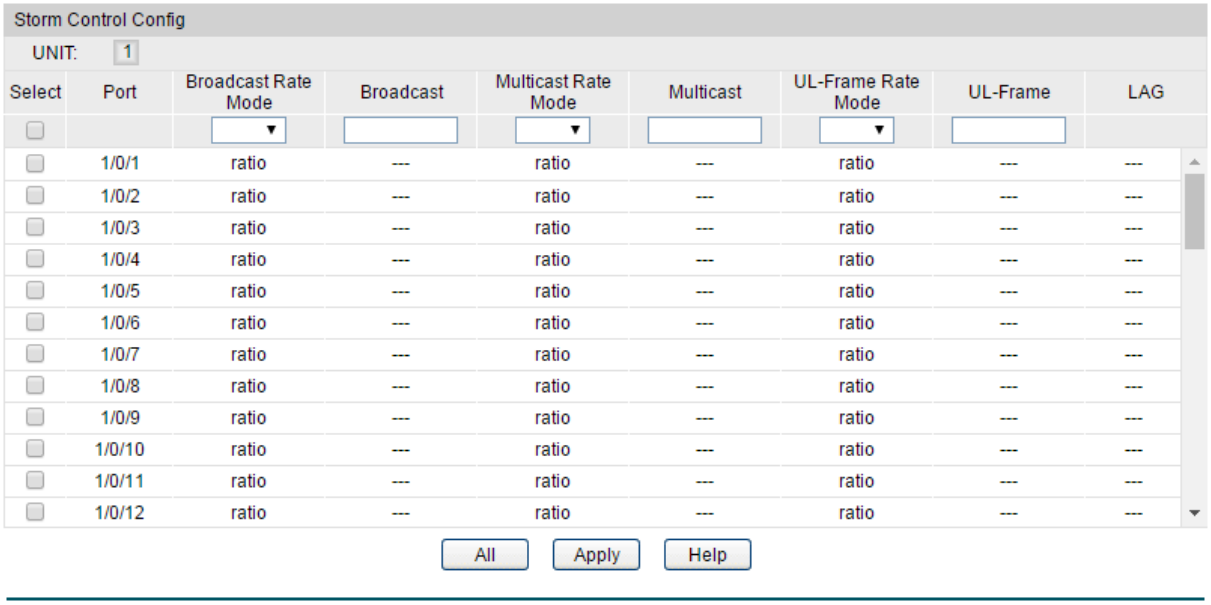


Figure 12-11 Storm Control

Configuration Procedure:

1) Select the port(s) and configure the upper rate limit for forwarding broadcast packets, multicast packets and UL frames.
2) Click **Apply**.

Entry Description:

UNIT:	Select the unit ID of the desired member in the stack.
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**: Specify the threshold in kbits per second. • **ratio**: Specify the threshold as a percentage of the bandwidth. • **pps**: Specify the threshold in packets per second.
Broadcast:	Enable or disable broadcast control feature for the port.
Mulitcast Rate Mode:	Select the multicast rate mode.
Multicast:	Input 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 function for the port.
UL-Frame Rate Mode:	Select the UL-Frame rate mode.
UL-Frame:	Input 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 function for the port.
LAG:	Displays the LAG number which the port belongs to.

12.4 Voice VLAN

➢ **Overview**

The voice VLAN feature is used to prioritize the transmission of voice traffic. Voice traffic is typically more time-sensitive than data traffic, and the voice quality can deteriorate a lot because of packet loss and delay. To ensure the high voice quality, you can configure the voice VLAN and set priority for voice traffic.

➢ **OUI Address (Organizationally Unique Identifier Address)**

The OUI address is used by the switch to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet complies with the OUI addresses in the switch, the switch identifies the packet as a voice packet and prioritizes it in transmission.

The Voice VLAN function can be implemented on **Global Config, Port Config** and **OUI Config** pages.

12.4.1 Global Config

Choose the menu **QoS→Voice VLAN→Global Config** to load the following page.

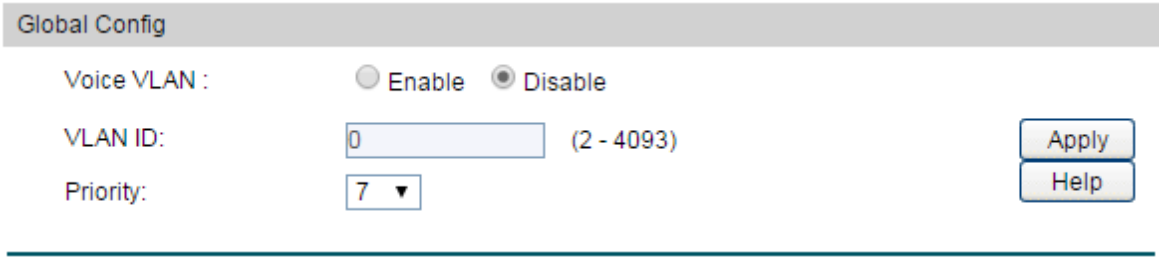


Figure 12-12 Global Configuration

Configuration Procedure:

1) Enable the voice VLAN feature, and enter a VLAN ID.
2) Specify a priority for the voice VLAN, and click **Apply**.

Note:

1. Before configuring the voice VLAN, you need to create a VLAN for voice traffic. For details about VLAN Configuration, please refer to 802.1Q VLAN.
2. VLAN 1 is a default VLAN and cannot be configured as the voice VLAN.
3. Only one VLAN can be set as the voice VLAN on the switch.

12.4.2 Port Config

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

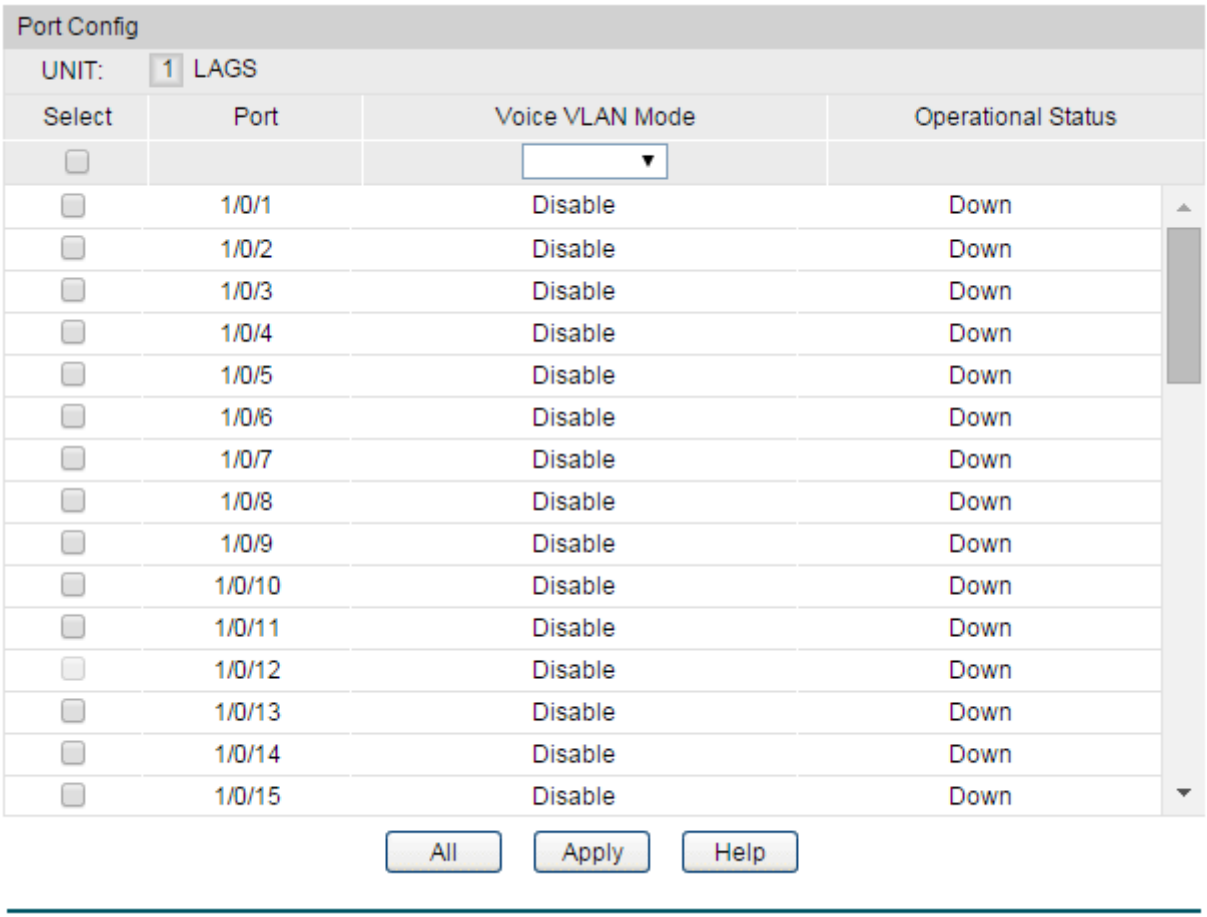


Figure 12-13 Port Config

Configuration Procedure:

1) Select your desired ports/LAGs and enable the Voice VLAN mode for selected ports.
2) Click **Apply**.

Entry Description:

Voice VLAN Mode: Enable or disable the administrative mode of OUI-based Voice VLAN on the interface.

Operational Status: Displays the current state of the ports that are connected to voice devices.

Up: The corresponding port is enabled with the voice VLAN mode and has a link.

Down: The corresponding port is not enabled with the voice VLAN mode or has no link.

12.4.3 OUI Config

If the OUI address of your voice device is not in the OUI table, you need to add the OUI address to the table.

Choose the menu **QoS→Voice VLAN→OUI Config** to load the following page.

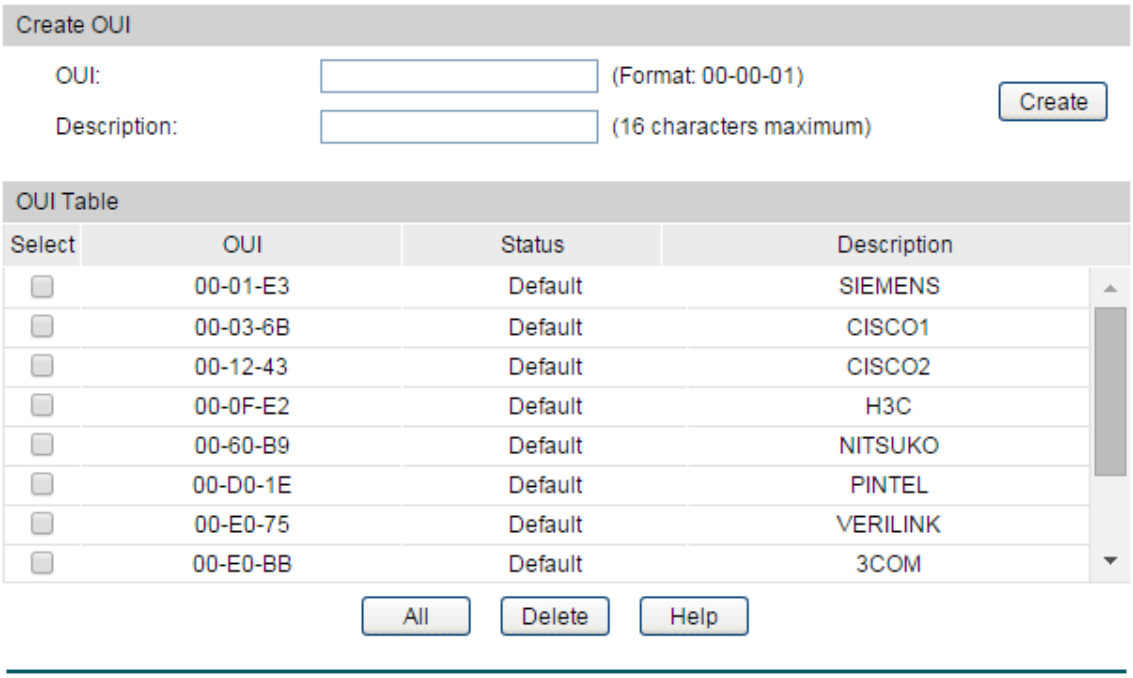


Figure 12-14 OUI Config

Configuration Procedure:

1) Enter an OUI address and give a description about the OUI address.
2) Click **Create** to add an OUI address to the table.

Entry Description:

OUI:	Enter the OUI address of your device.
Description:	Give an OUI address description for identification. The length is no more than 16 characters.

12.5 Auto VoIP

➢ **Overview**

The Auto VoIP feature is used to prioritize the transmission of voice traffic. Voice over Internet Protocol (VoIP) enables telephone calls over a data network, and the Auto VoIP feature helps provide a classification mechanism for voice packets. When Auto VoIP is configured on a port that receives both voice and data traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is heavy.

To apply the Auto VoIP configuration, you need to further configure LLDP and DiffServ. For details, see *LLDP* and *DiffServ*.

12.5.1 Auto VoIP Config

Before configuring Auto VoIP, you need to create a VLAN for voice traffic. For details about VLAN configuration, see *802.1Q VLAN*.

Choose the menu **QoS > Auto VoIP > Auto VoIP Config** to load the following page.

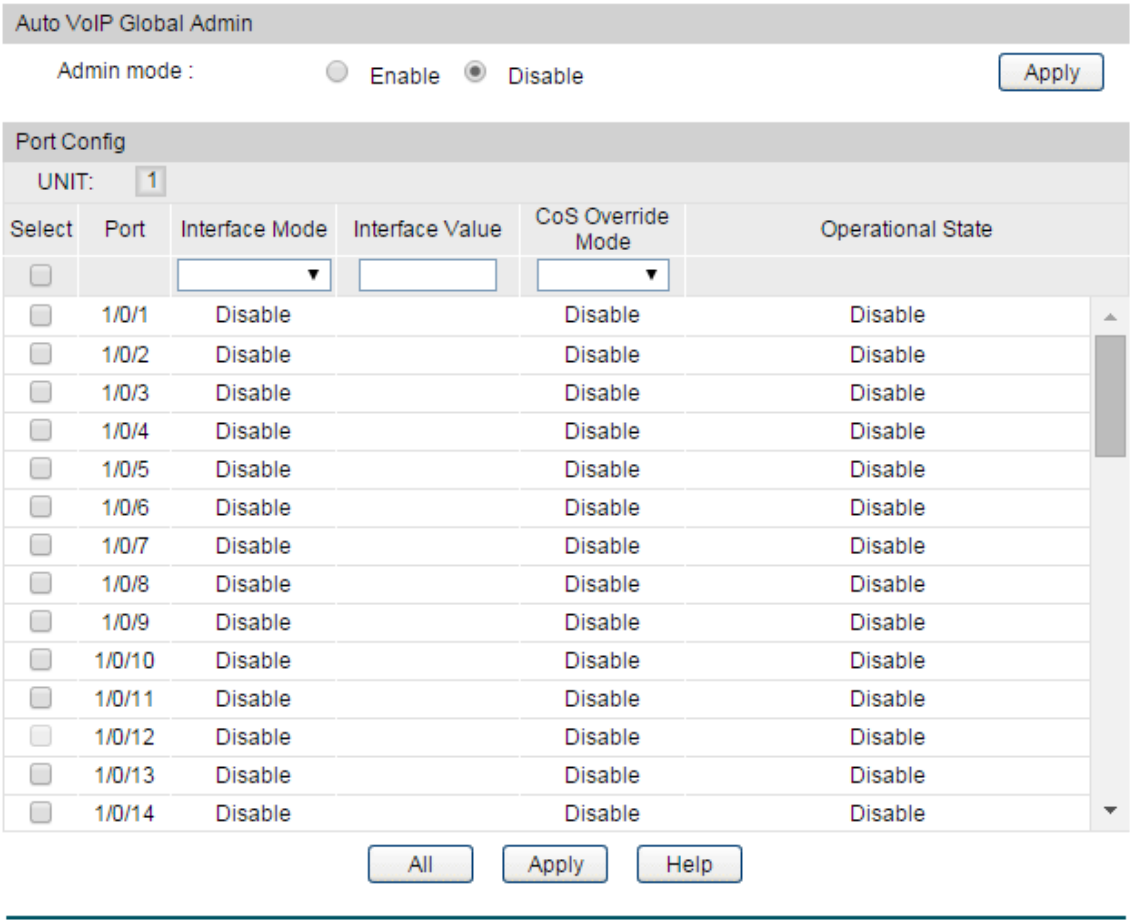


Figure 12-22 Auto VoIP Config

Configuration Procedure:

1) Enable the Admin mode of Auto VoIP.
2) Select your desired ports and choose the interface mode and enter corresponding interface value; choose the CoS override mode and click **Apply**.
3) Configure the corresponding module based on the interface mode.

Entry Description:

Admin Mode: Enable or disable the Admin mode of Auto VoIP.

UNIT: Select the unit ID of the desired member in the stack.

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

Port: Displays the port number of the switch.

Interface Mode: Indicates how an IP phone connected to the port should send voice traffic

• VLAN ID – Forward voice traffic in the specified Auto VoIP VLAN. If you choose VLAN ID, you need to configure LLDP-MED to instruct voice devices to send tagged voice traffic, and create a priority policy in DiffServ for voice traffic. For details, see *LLDP* and *DiffServ.*

• Dot1p – Tag voice traffic with the specified 802.1p priority value. If you choose Dot1p, you need to configure LLDP-MED to instruct voice devices to send tagged voice traffic, and set 802.1P Priority in **Class of Service**. For details, see *LLDP* and *Class of Service*.

• None – The IP phone sends voice traffic based on the configuration of itself.

• Untagged – Instruct the IP phone to send untagged voice traffic.

• Disable – Disable the Auto VoIP feature on the interface.

Interface Value: If you have selected VLAN ID or Dot1p as the Auto VoIP Interface Mode, specify the corresponding voice VLAN ID or the Dot1p priority value that the connected IP phone should use for voice traffic.

CoS Override Mode Enable or disable the Class of Service override mode

• Enabled – The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices.

• Disabled – The port trusts the priority value in the received frame.

Operating Status Displays operating status of the voice VLAN feature on the interface. To make it enabled, you must enable the voice VLAN both globally and on the interface. Additionally, the interface must be up and have a link.

Return to CONTENTS

Chapter 13 ACL

The fast growth of network size and traffic brings challenges to network security and bandwidth allocation. Packet filtering can prevent unauthorized access behaviors and improve bandwidth use.

ACL (Access Control List), which is based on rule matching, is primarily used for packet filtering. ACL accurately identifies and controls packets on the network to manage network access behaviors, prevent network attacks, and improve bandwidth use efficiency. In this way, ACL ensures security and high service quality on networks. It is usually applied in the following occasions:

To prevent various network attacks, such as IP (Internet Protocol), TCP (Transmission Control Protocol), and ICMP (Internet Control Message Protocol) packets attacks.

To manage network access behaviors, such as controlling access to a network or to specific resources on your network.

The ACL module is mainly for ACL configuration of the switch, including three submenus: **Time-Range**, **ACL Config** and **ACL Binding**.

13.1 Time-Range

If a configured ACL is needed to be effective in a specified time-range, a time-range should be firstly specified in the ACL. As the time-range based ACL takes effect only within the specified time-range, data packets can be filtered by differentiating the time-ranges.

On this switch absolute time and periodic time can be configured. Configure an absolute time section in the form of "the start date to the end date" to make ACLs effective; configure a periodic time section to make ACLs effective on the fixed days of the week.

The Time-Range configuration can be implemented on **Time-Range Summary** page.

13.1.1 Time-Range Summary

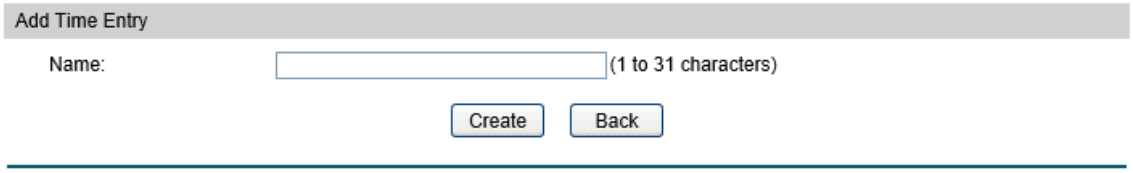
On this page you can view the current time-ranges.

Choose the menu **ACL** → **Time-Range** → **Time-Range Summary** to load the following page.

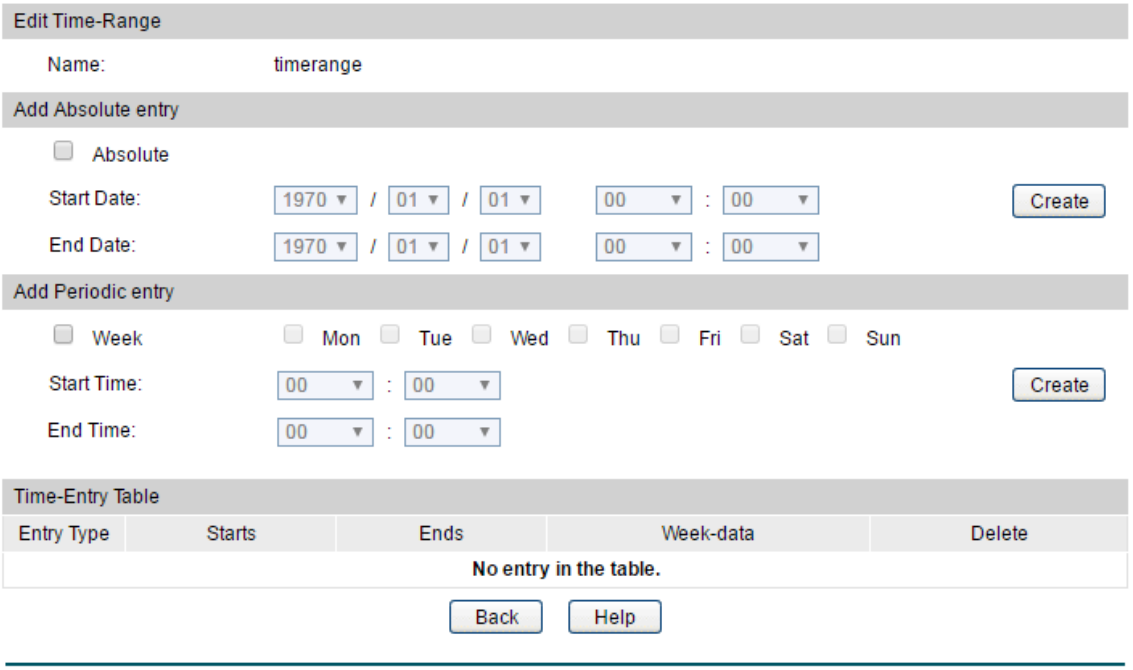
Figure 13-1 Time-Range Table

Configuration Procedure:

1) To add a new time range, click "**Add**" to load the following page. Then enter the name of the time-range for time identification and click "Create". You can view the entry in the Time-Range Table.



2) To edit the time range, click "**Edit**" in the Time-Range Table to load the following page. Then configure Absolute entry or Periodic entry according to your actual needs.



Entry Description:

Select: Select the desired entry to delete the corresponding time-range.

Time-Range Name: Displays the name of the time-range.

Time-Range Status: Shows whether the time range is Active or Inactive. A time range is inactive if the current day and time do not fall within any time range entries configured for the time range.

Absolute Entry: Shows whether an absolute time entry is currently configured for the time range.

Periodic Entry Count: The number of periodic time range entries currently configured for the time range.

Operation: Display and edit the information of this time-range.

Name: The name of the time-range.

Absolute: Select Absolute to configure absolute time-range. The ACL rule based on this time-range takes effect only when the system time is within the absolute time-range.

Start Date: Configure values for the Start Date and the Time of Day.

End Date: Configure values for the End Date and the Time of Day.

Week:	Select Week to configure week time-range. The ACL rule based on this time-range takes effect only when the system time is within the week time-range.
Start Time:	Configure values for the Start Time of Day.
End Time:	Configure values for the End Time of Day.
Entry Type:	The type of time range entry.
Starts:	For an Absolute entry, indicates the time, day, month, and year that the entry begins. For a Periodic entry, indicates the time that the entry begins.
Ends:	For an Absolute entry, indicates the time, day, month, and year that the entry ends. For a Periodic entry, indicates the time that the entry ends.
Week-data:	For a Periodic entry, indicates the day(s) of the week of the entry.
Delete:	Click the Delete button to delete the corresponding time-slice.

13.2 ACL Config

An ACL may contain a number of rules, and each rule specifies a different package range. Packets are matched in match order. Once a rule is matched, the switch processes the matched packets taking the operation specified in the rule without considering the other rules, which can enhance the performance of the switch.

Packets are classified based on match rules in order of the rules. For different types of ACL, you can define the rules based on source or destination IP address, source or destination MAC address, protocol type, port number and so on.

There are three types of ACL including **MAC ACL**, **Standard-IP ACL** and **Extend-IP ACL**.

13.2.1 ACL Summary

On this page, you can view the all the ACLs and their rules configured in the switch. The rules in an ACL are listed in an ascending order of configuration time, no matter what their rule IDs are. By default, a rule configured earlier is listed before a rule configured later. The switch matches a received packet with the rules in order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule.

In ACL rule table, you can view all the ACLs and their rules. You can also delete an ACL or an ACL rule, or change the matching order if needed.

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

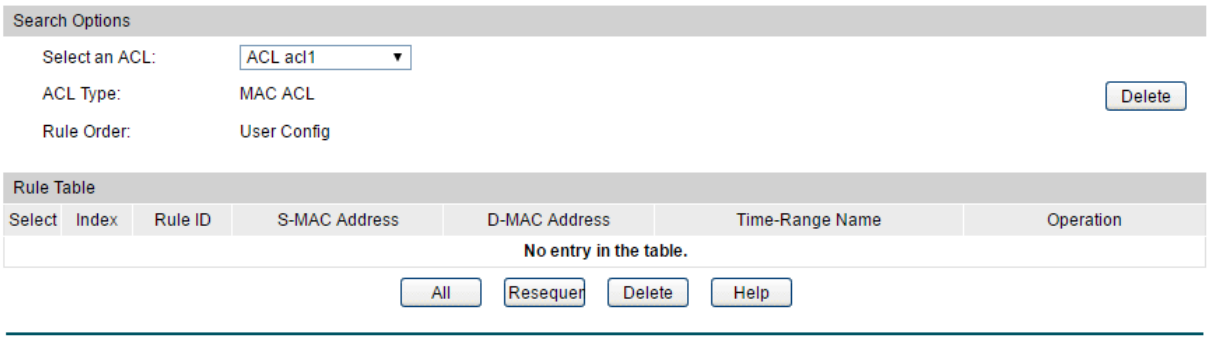


Figure 13-4 ACL Summary

Configuration Procedure:

Select an ACL ID from the drop-down list. You can view corresponding rules in the Rule Table.

13.2.2 ACL Create

On this page you can create ACLs.

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

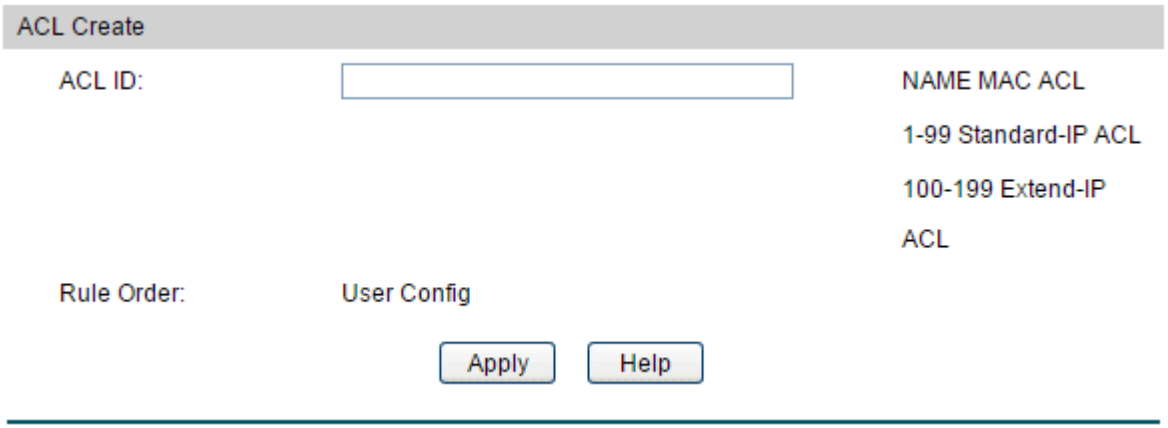


Figure 13-5 ACL Create

Configuration Procedure:

Enter an ID number in the ACL ID field, then click Apply.

Entry Description:

ACL ID:	Enter a number that is used to identify the ACL.
Rule Order:	User Config order is set to be match order in this ACL.

13.2.3 MAC ACL

MAC ACLs analyze and process packets based on a series of match conditions, which can be the source MAC addresses, destination MAC addresses and EtherType carried in the packets.

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

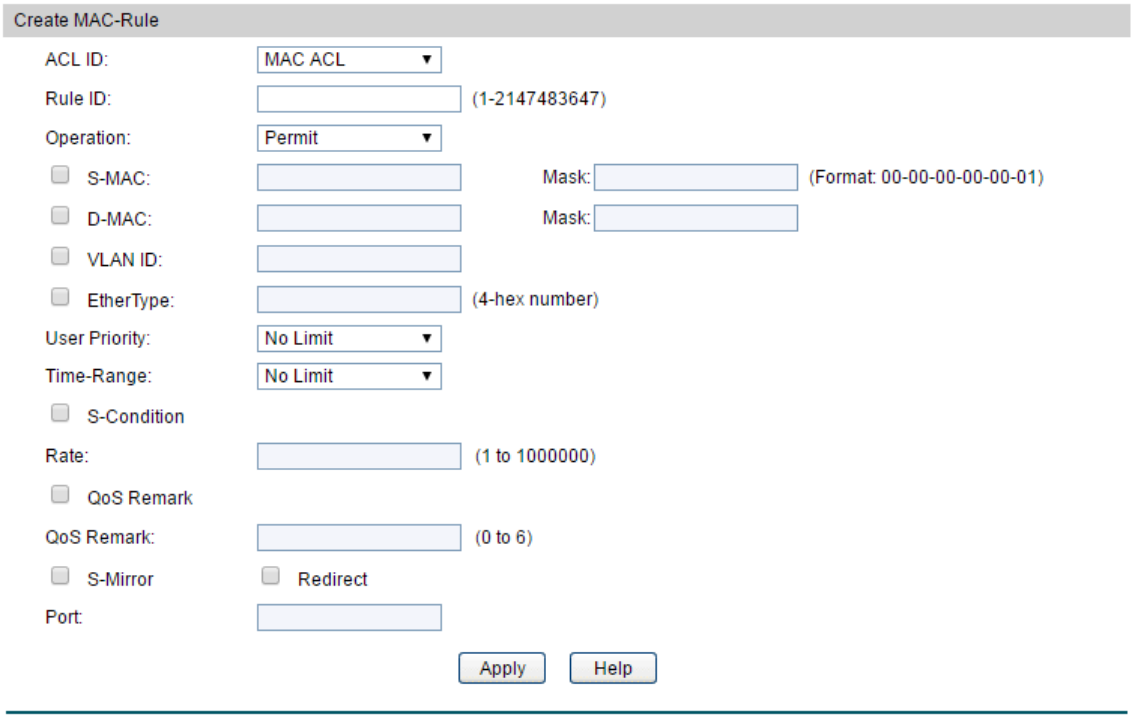


Figure 13-6 Create MAC Rule

Configuration Procedure:

1) Select an ACL ID from the drop-down list, enter a Rule ID, then specify the operation of the rule.

2) Select and define the rule's packet-matching criteria.

Entry Description:

ACL ID: Select the desired MAC ACL for configuration.

Rule ID: Enter the rule ID.

Operation: Select the operation for the switch to process packets which match the rules.

- **Permit:** Forward packets.
- **Deny:** Discard Packets.

S-MAC: Enter the source MAC address contained in the rule.

D-MAC: Enter the destination MAC address contained in the rule.

MASK: Enter MAC address mask. If it is set to 1, it must strictly match the address.

VLAN ID: Enter the VLAN ID contained in the rule.

EtherType: Enter EtherType contained in the rule.

User Priority: Select the user priority contained in the rule for the tagged packets to match.

Time-Range: Select the time-range for the rule to take effect.

S-Condition: Select S-Condition to limit the transmission rate of the data packets.

Rate: The transmission rate of the data packets. Valid values are (1 to 1000000) in Kbps.

Qos Remark: Select QoS Remark to forward the data packets based on the QoS settings.

S-Mirror: Select S-Mirror to mirror the data packets to the specific port.

Redirect: Select Redirect to change the forwarding direction of the data packets.

Port: Redirect or mirror the data packets to the specific port.

13.2.4 Standard-IP ACL

Standard-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Choose the menu **ACL** → **ACL Config** → **Standard-IP ACL** to load the following page.

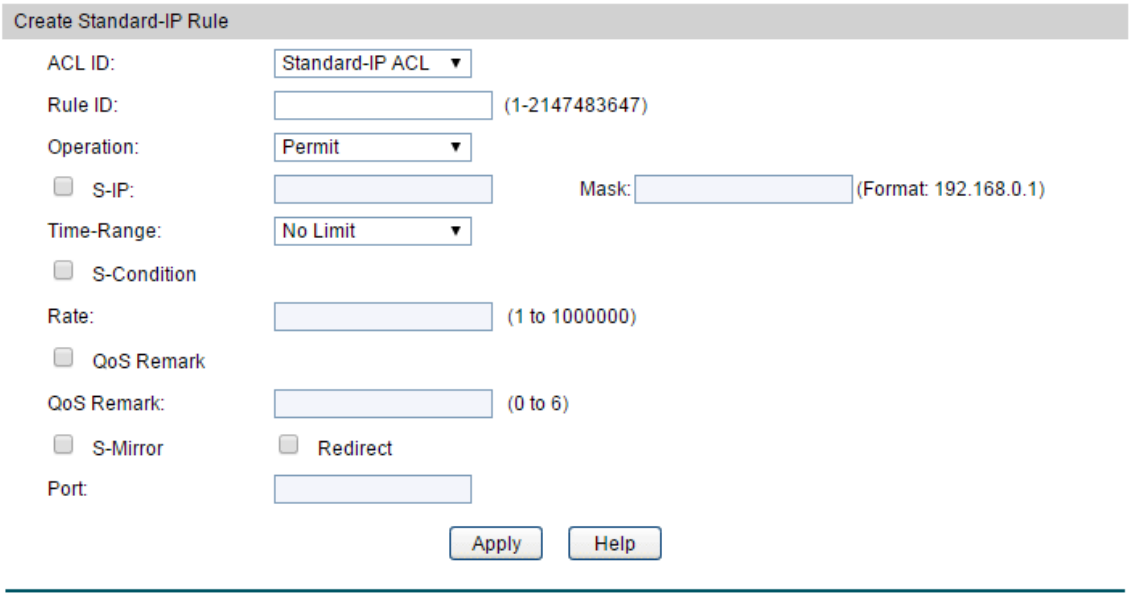


Figure 13-7 Create Standard-IP Rule

Configuration Procedure

1) Select an ACL ID from the drop-down list, enter a Rule ID, then specify the operation of the rule.

2) Select and define the rule's packet-matching criteria.

Entry Description

ACL ID: Select a Standard-IP ACL from the drop-down list.

Rule ID: Enter an ID number that is used to identify the rule. It cannot be the same as the existing Standard-IP Rule IDs.

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.

Mask: Enter IP address mask. If it is set to 1, it must strictly match the address.

Time-Range: Select the time-range for the rule to take effect.

S-Condition: Select S-Condition to limit the transmission rate of the data packets.

Rate: The transmission rate of the data packets. Valid values are (1 to 1000000) in Kbps.

Qos Remark: Select QoS Remark to forward the data packets based on the QoS settings.

S-Mirror: Select S-Mirror to mirror the data packets to the specific port.

Redirect: Select Redirect to change the forwarding direction of the data packets.

Port: Redirect or mirror the data packets to the specific port.

13.2.5 Extend-IP ACL

Extend-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses, destination IP addresses, IP protocol and other information of this sort carried in the packets.

Choose the menu **ACL** → **ACL Config** → **Extend-IP ACL** to load the following page.

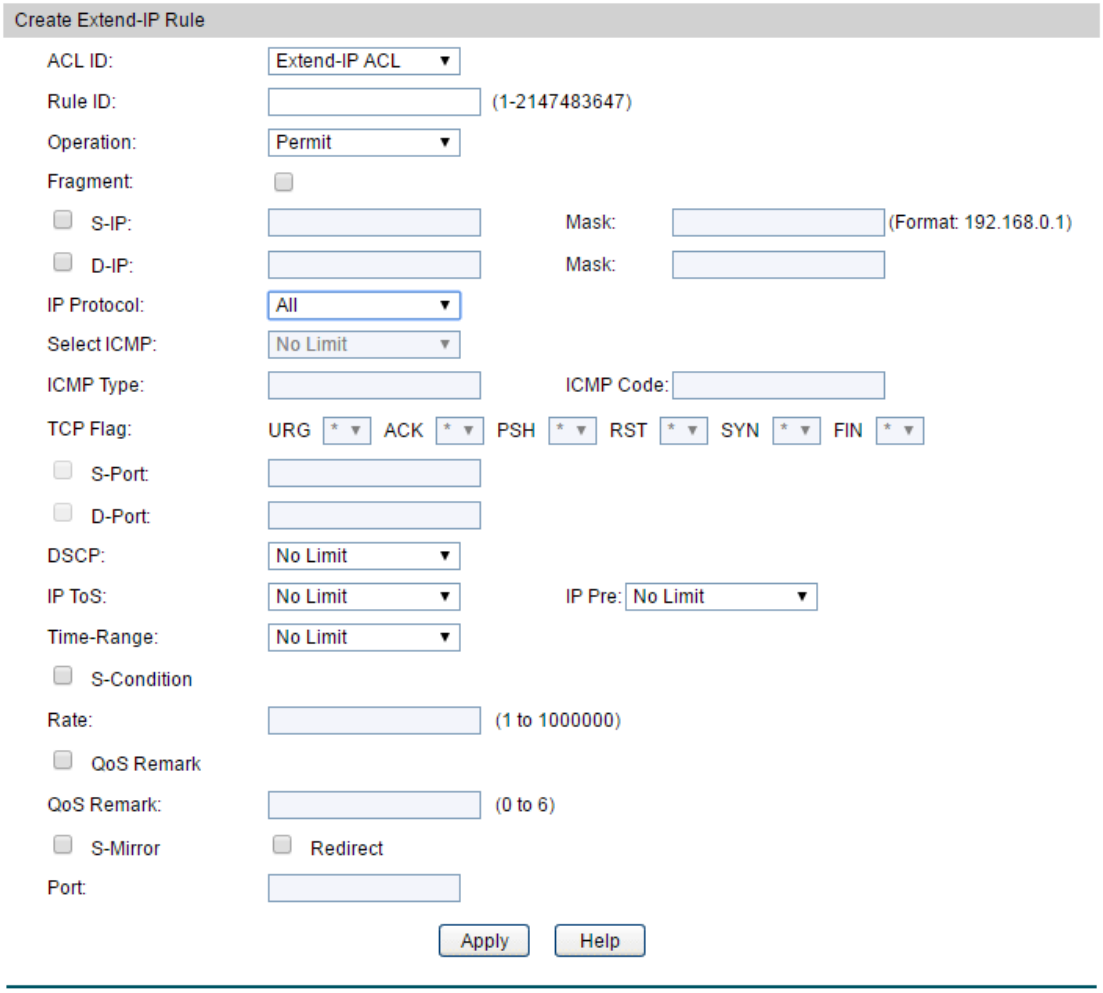


Figure 13-8 Create Extend-IP Rule

Configuration Procedure

1) Select an ACL ID from the drop-down list, enter a Rule ID, then specify the operation of the rule.

2) Select and define the rule's packet-matching criteria.

Entry Description

ACL ID: Select a Standard-IP ACL from the drop-down list.

Rule ID: Enter an ID number that is used to identify the rule. It cannot be the same as the existing Standard-IP Rule IDs.

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.
Select ICMP:	Configure the predefined ICMP type and code.
ICMP Type:	Configure the predefined ICMP type.
ICMP Code:	Configure the predefined ICMP code.
IP Protocol:	Select IP protocol contained in the rule.
TCP Flag:	Configure TCP flag when TCP is selected from the pull-down list of IP Protocol.
S-Port:	Configure TCP/IP source port contained in the rule when TCP/UDP is selected from the pull-down list of IP Protocol.
D-Port:	Configure TCP/IP destination port contained in the rule when TCP/UDP is selected from the drop-down list of IP Protocol.
DSCP:	Enter the DSCP information contained in the rule.
IP ToS:	Enter the IP ToS contained in the rule.
IP Pre:	Enter the IP Precedence contained in the rule.
Time-Range:	Select the time-range for the rule to take effect.
S-Condition:	Select S-Condition to limit the transmission rate of the data packets.
Rate:	The transmission rate of the data packets. Valid values are (1 to 1000000) in Kbps.
Qos Remark:	Select QoS Remark to forward the data packets based on the QoS settings.
S-Mirror:	Select S-Mirror to mirror the data packets to the specific port.
Redirect:	Select Redirect to change the forwarding direction of the data packets.
Port:	Redirect or mirror the data packets to the specific port.

13.3 ACL Binding

ACL Binding function can have the policy take its effect on a specific port/VLAN. The ACL will take effect only when it is bound to a port/VLAN. In the same way, the port/VLAN will receive the data packets and process them based on the ACL only when the ACL is bound to the port/VLAN.

The ACL Binding can be implemented on **Binding Table**, **Port Binding** and **VLAN Binding** pages.

13.3.1 Binding Table

On this page view the policy bound to port/VLAN.

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

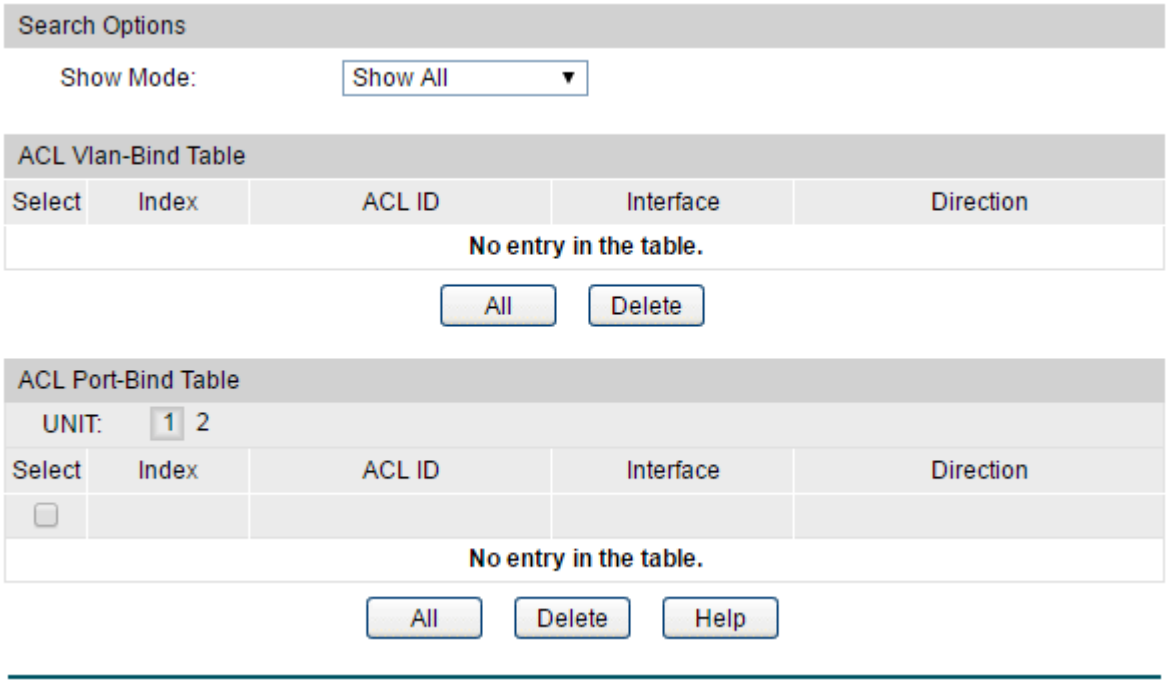


Figure13-12 Binding Table

Configuration Procedure

1) In the **ACL VLAN-Bind Table**, you can view VLAN binding entries.

2) In the **ACL Port-Bind Table**, you can view port binding entries.

3) You can also delete existing entries if needed.

Entry Description

➢ **Search Options**

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 or name of the binding ACL.

Interface: Displays the VLAN ID bound to the ACL.

Direction: Displays the binding direction.

➢ **ACL Port-Bind Table**

UNIT:	Select the unit ID of the desired member in the stack.
Select:	Select the desired entry to delete the corresponding binding ACL.
Index:	Displays the index of the binding ACL.
ACL ID:	Displays the ID or name of the binding ACL.
Interface:	Displays the port number bound to the ACL.
Direction:	Displays the binding direction.

13.3.2 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.

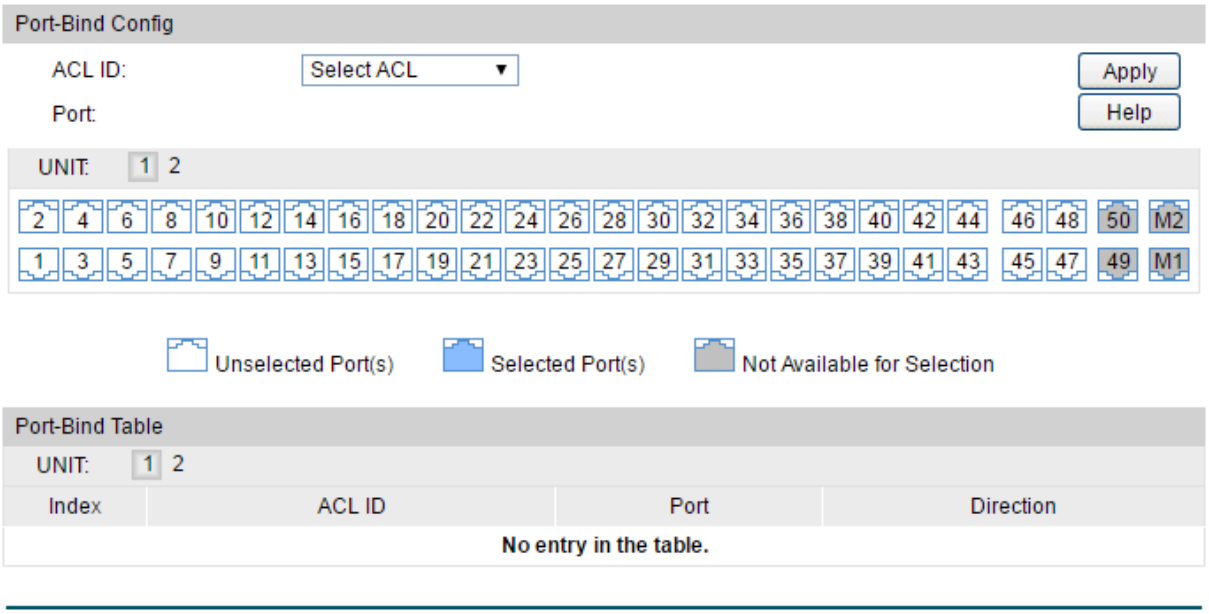


Figure13-13 Bind the ACL to the port

Configuration Procedure:

Select the ACL and port(s) you want to bind. Then click **Apply**.

Entry Description:

➢ **Port-Bind Config**

ACL ID:	Select the ID or the name of the ACL you want to bind.
Port:	Select the port you want to bind.

➢ **Port-Bind Table**

Index:	Displays the index of the binding ACL.

ACL ID: Displays the ID or name of the binding ACL.

Port: Displays the number of the port bound to the corresponding ACL.

Direction: Displays the binding direction.

13.3.3 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.

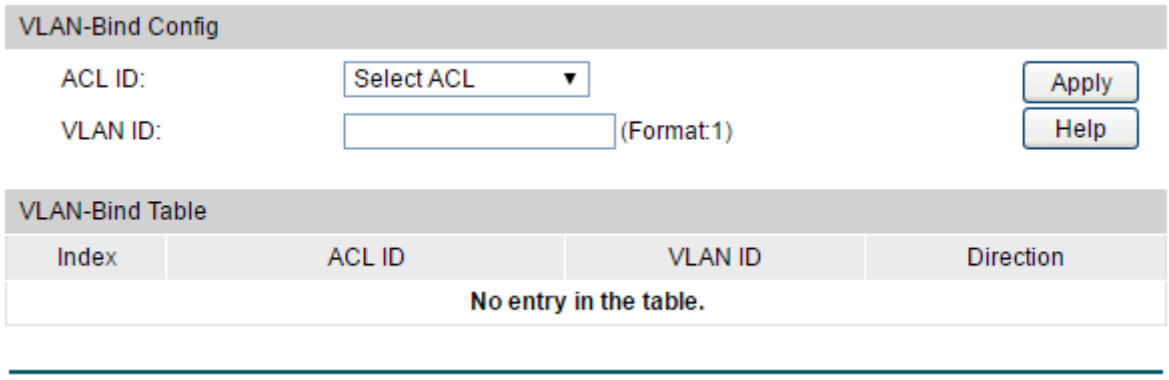


Figure13-14 Bind the ACL to the VLAN

Configuration Procedure:

Select the ACL and enter the VLAN ID. Then click **Apply**.

Entry Description:

- **VLAN-Bind Config**

  ACL ID: Select the ID or name 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 or name of the binding ACL.

  VLAN ID: Displays the ID of the VLAN bound to the corresponding ACL.

  Direction: Displays the binding direction.

ACL Configuration Procedure:

Step	Operation	Description
1	Configure effective time-range	Optional. On **ACL** → **Time-Range** →**Time-Range Summary** configuration page, configure the effective time-ranges for ACLs.

2	Configure ACL rules	Required. On **ACL** → **ACL Config** configuration pages, configure ACL rules to match packets.
3	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.

Return to CONTENTS

Chapter 14 Network Security

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

14.1 IP-MAC Binding

The IP-MAC Binding function allows you to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together. Basing on the IP-MAC binding table, ARP Inspection and IP Source Guard functions can control the network access and only allow the Hosts matching the bound entries to access the network.

The following two 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) 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.

The two methods are also considered as the sources of the IP-MAC Binding entries. The entries from different sources should be different from the other to avoid collision. Only the entry from the source with the higher priority will take effect. The priority of Manual is higher than that of Snooping.

The **IP-MAC Binding** function is implemented on the **Binding Table** and **Manual Binding** pages.

14.1.1 Binding Table

On this page, you can view the information of the bound entries.

Choose the menu **Network Security→IP-MAC Binding→Binding Table** to load the following page.

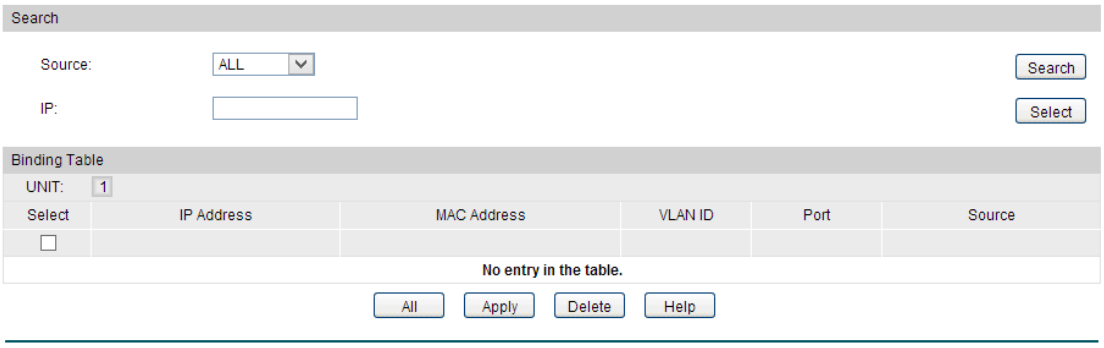


Figure 14-1 Binding Table

Configuration Procedure:

Select a source type and click **Search** to search the specified type of entry.

Entry Description:

Source:	Displays the Source of the entry. • **All:** All the bound entries will be displayed. • **Manual:** Only the manually added entries will be displayed. • **Snooping:** Only the entries formed via DHCP Snooping will be displayed.
IP	Click the Select button to quick-select the corresponding entry based on the IP address you entered.
UNIT:	Select the unit ID of the desired member in the stack.
Select:	Select the desired entry to modify the Host Name and Protect Type. It is multi-optional.
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.
Source:	Displays the Source of the entry.

14.1.2 Manual Binding

You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

Choose the menu **Network Security→IP-MAC Binding→Manual Binding** to load the following page.

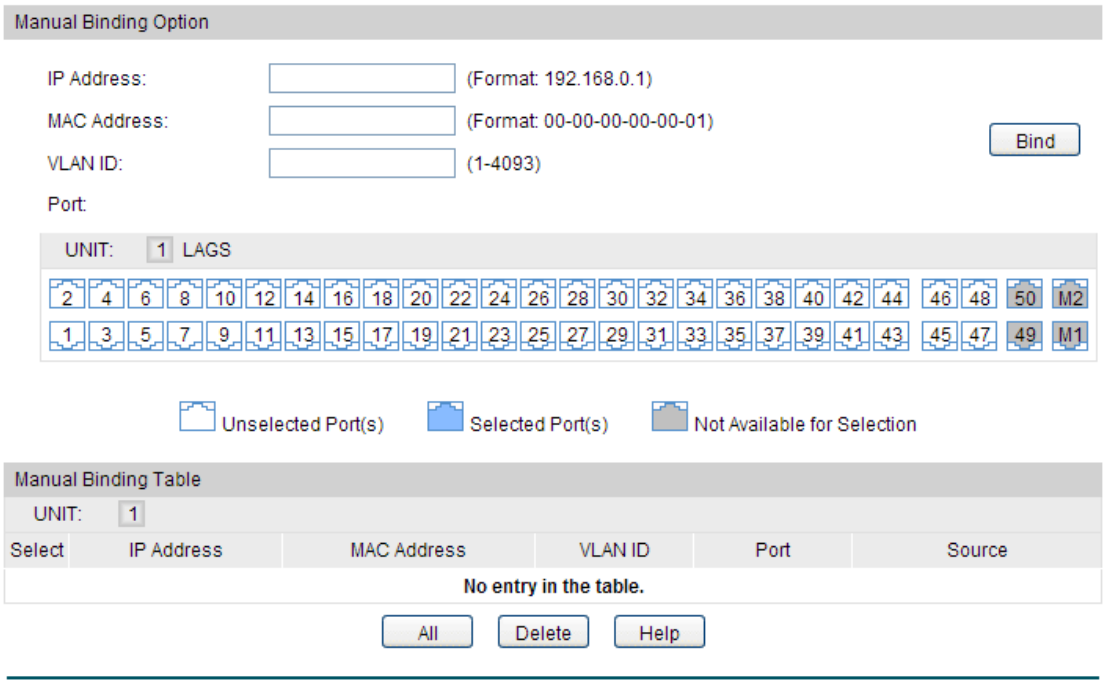


Figure 14-2 Manual Binding

Configuration Procedure:

Specify the IP address, MAC address, VLAN ID and port number, and click **Bind**.

Entry Description:

IP Address:	Enter the IP Address of the Host.
MAC Address:	Enter the MAC Address of the Host.
VLAN ID:	Enter the VLAN ID.
Port:	Select the number of port connected to the Host.
UNIT:	Select the unit ID of the desired member in the stack.

14.2 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. For details about the DHCP Server function, please refer to 10.4 DHCP Server.

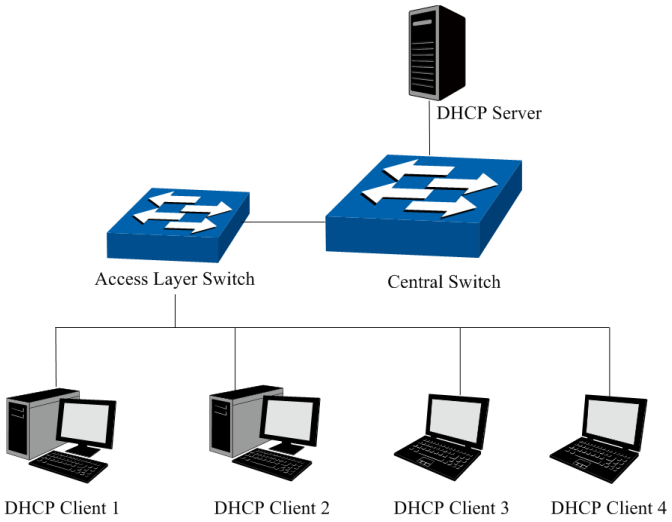


Figure 14-5 Network diagram for DHCP-snooping implementation

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.

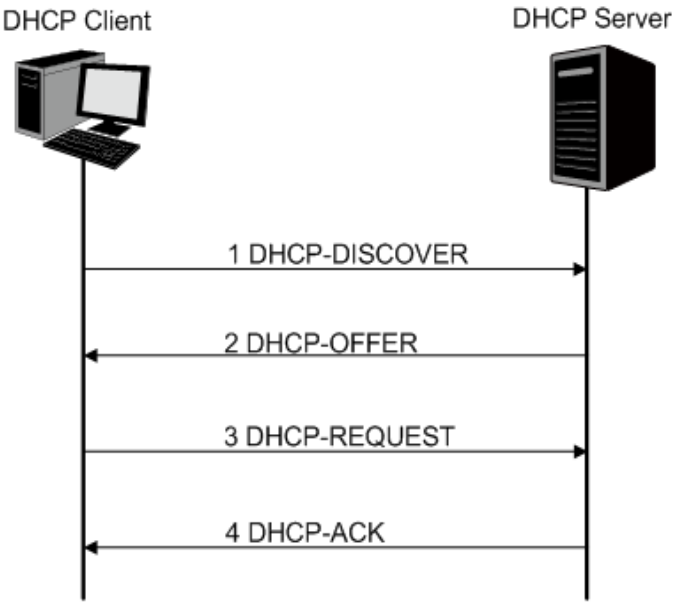


Figure 14-6 Interaction between a DHCP client and a DHCP server

(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.

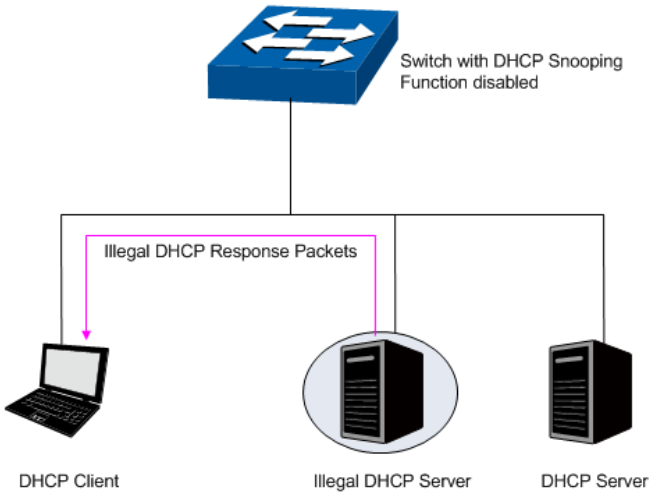


Figure 14-7 DHCP Cheating Attack Implementation Procedure

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.

14.2.1 Global Config

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

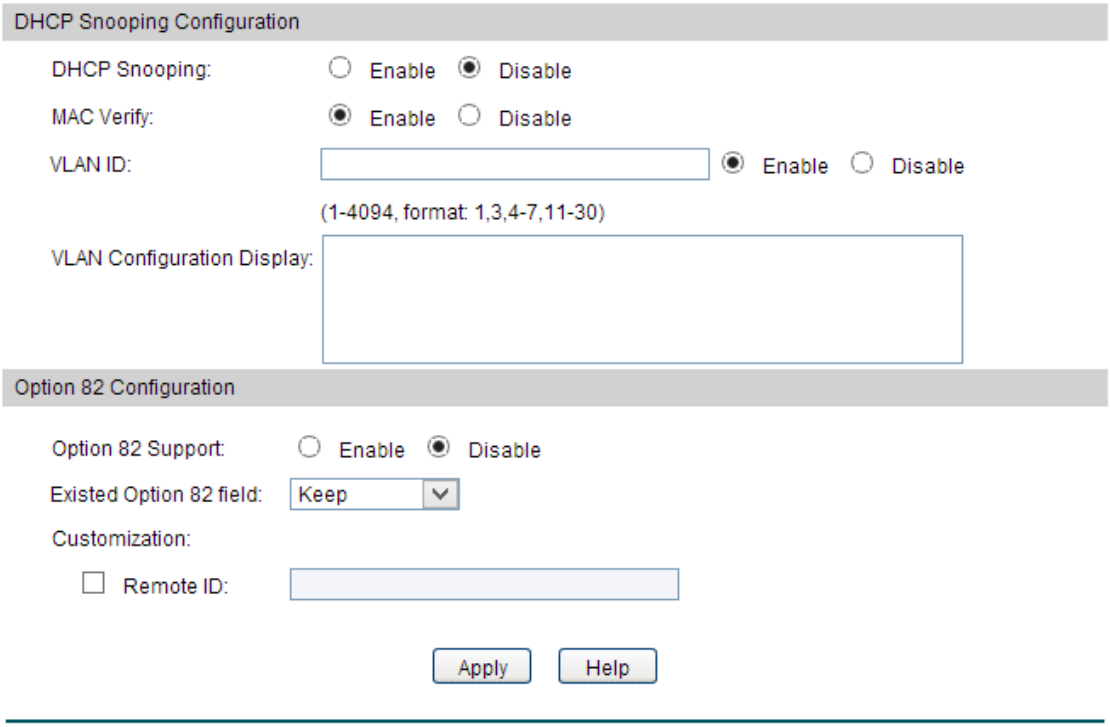


Figure 14-8 DHCP Snooping

Note:

If you want to enable the DHCP Snooping feature for the member port of LAG, please ensure the parameters of all the member ports are the same.

Configuration Procedure:

1) Enable DHCP Snooping globally and for the specified VLAN.
2) Configure Option 82.
3) Click **Apply**.

Entry Description:

DHCP Snooping:	Enable/Disable the DHCP Snooping function globally.
MAC Verify:	Enable or disable the MAC Verify feature. There are two fields in the DHCP packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCP packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCP server from being exhausted by forged MAC addresses.
VLAN ID:	Specify the VLAN ID in the format shown on the page.
VLAN Configuration Display:	Displays the VLANs that have been enabled with DHCP Snooping.

➢ **Option 82 Config**

Option 82 Support:	Enable/Disable the Option 82 feature.

Existed Option 82 field: Select the operation for the Option 82 field of the DHCP request packets from the Host.

- **Keep:** Indicates to keep the Option 82 field of the packets.
- **Replace:** Indicates to replace the Option 82 field of the packets with the switch defined one.
- **Drop:** Indicates to discard the packets including the Option 82 field.

Customization: Enable or Disable the switch to define the Option 82.

Remote ID: Enter the sub-option Remote ID for the customized Option 82.

14.2.2 Port Config

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

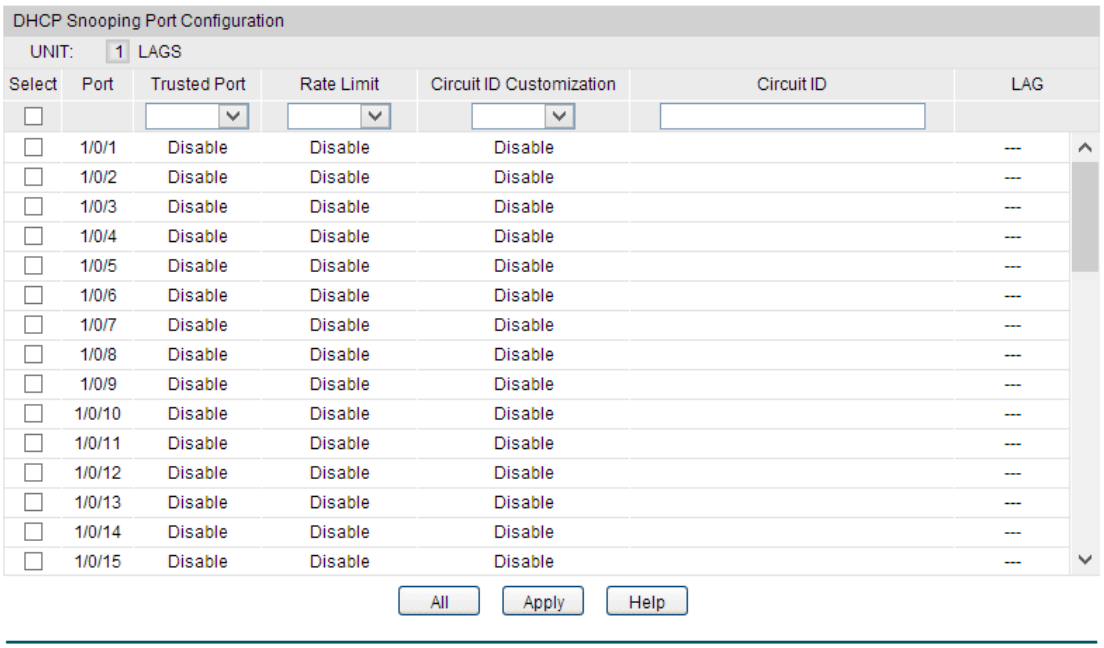


Figure 14-9 DHCP Snooping

Configuration Procedure:

Select one or more ports and configure the relevant parameters. Click **Apply**.

Entry Description:

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.

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.
Circuit ID Customization:	Enable or Disable the switch to define Circuit ID.
Circuit ID:	Enter the sub-option Circuit ID for the customized Option 82.
LAG:	Displays the LAG to which the port belongs to.

14.3 ARP Inspection

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 and so on. The following part will simply introduce these ARP attacks.

- **Imitating Gateway**

The attacker sends the MAC address of a forged Gateway to Host, and then the Host will automatically update the ARP table after receiving the ARP response packets, which causes that the Host cannot access the network normally. The ARP Attack implemented by imitating Gateway is illustrated in the following figure.

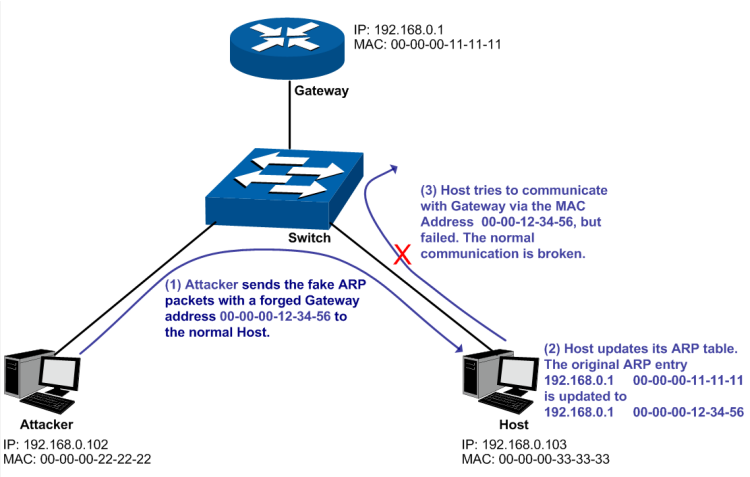


Figure 14-10 ARP Attack - Imitating Gateway

As the above figure shown, the attacker sends the fake ARP packets with a forged Gateway address to the normal Host, and then the Host will automatically update the ARP table after receiving the ARP packets. When the Host tries to communicate with Gateway, the Host will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

- **Cheating Gateway**

The attacker sends the wrong IP address-to-MAC address mapping entries of Hosts to the Gateway, which causes that the Gateway cannot communicate with the legal terminal Hosts

normally. The ARP Attack implemented by cheating Gateway is illustrated in the following figure.

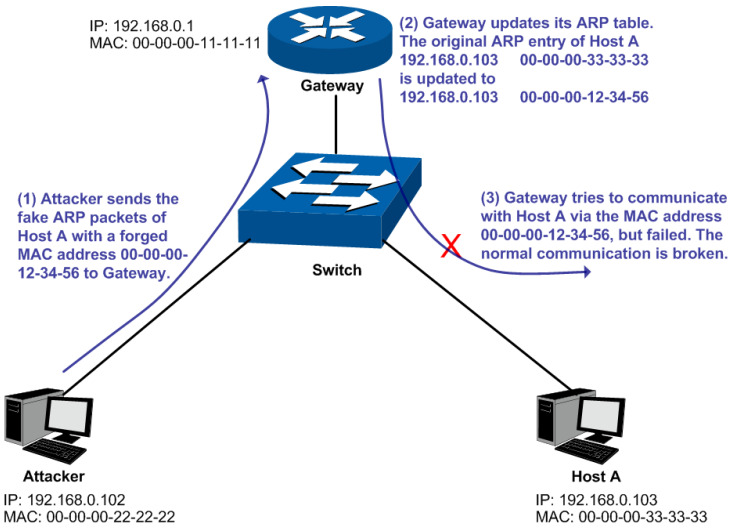


Figure 14-11 ARP Attack – Cheating Gateway

As the above figure shown, the attacker sends the fake ARP packets of Host A to the Gateway, and then the Gateway will automatically update its ARP table after receiving the ARP packets. When the Gateway tries to communicate with Host A in LAN, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

- **Cheating Terminal Hosts**

The attacker sends the false IP address-to-MAC address mapping entries of terminal Host/Server to another terminal Host, which causes that the two terminal Hosts in the same network segment cannot communicate with each other normally. The ARP Attack implemented by cheating terminal Hosts is illustrated in the following figure.

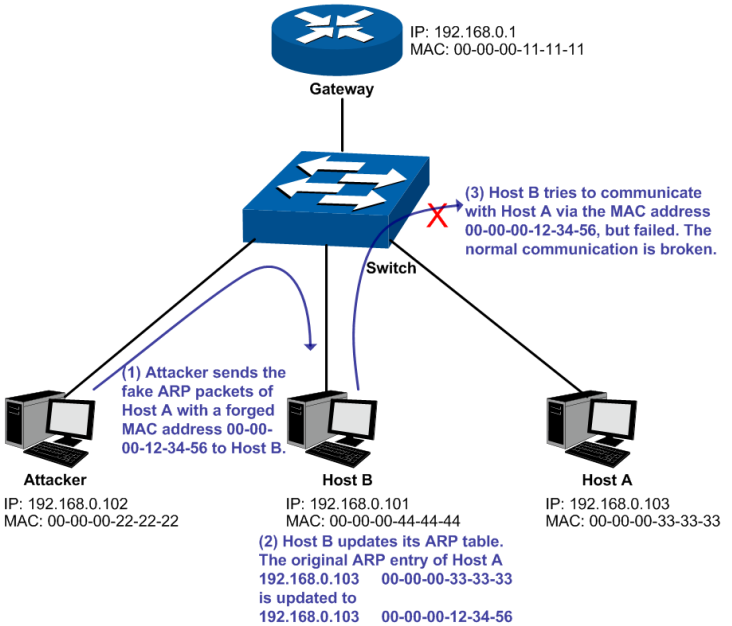


Figure 14-12 ARP Attack – Cheating Terminal Hosts

As the above figure shown, the attacker sends the fake ARP packets of Host A to Host B, and then Host B will automatically update its ARP table after receiving the ARP packets. When Host B tries to communicate with Host A, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

- **Man-In-The-Middle Attack**

The attacker continuously sends the false ARP packets to the Hosts in LAN so as to make the Hosts maintain the wrong ARP table. When the Hosts in LAN communicate with one another, they will send the packets to the attacker according to the wrong ARP table. Thus, the attacker can get and process the packets before forwarding them. During the procedure, the communication packets information between the two Hosts are stolen in the case that the Hosts were unaware of the attack. That is called Man-In-The-Middle Attack. The Man-In-The-Middle Attack is illustrated in the following figure.

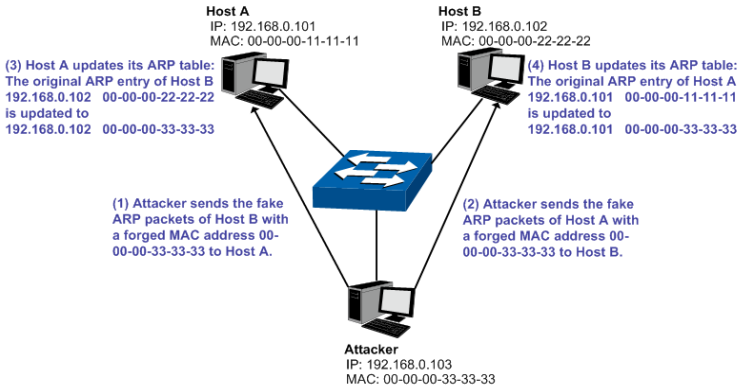


Figure 14-13 Man-In-The-Middle Attack

Suppose there are three Hosts in LAN connected with one another through a switch.

Host A: IP address is 192.168.0.101; MAC address is 00-00-00-11-11-11.

Host B: IP address is 192.168.0.102; MAC address is 00-00-00-22-22-22.

Attacker: IP address is 192.168.0.103; MAC address is 00-00-00-33-33-33.

1. First, the attacker sends the false ARP response packets.
2. Upon receiving the ARP response packets, Host A and Host B updates the ARP table of their own.
3. When Host A communicates with Host B, it will send the packets to the false destination MAC address, i.e. to the attacker, according to the updated ARP table.
4. After receiving the communication packets between Host A and Host B, the attacker processes and forwards the packets to the correct destination MAC address, which makes Host A and Host B keep a normal-appearing communication.
5. The attacker continuously sends the false ARP packets to the Host A and Host B so as to make the Hosts always maintain the wrong ARP table.

In the view of Host A and Host B, their packets are directly sent to each other. But in fact, there is a Man-In-The-Middle stolen the packets information during the communication procedure. This kind of ARP attack is called Man-In-The-Middle attack.

➢ **ARP Flooding Attack**

The attacker broadcasts a mass of various fake ARP packets in a network segment to occupy the network bandwidth viciously, which results in a dramatic slowdown of network speed. Meantime, the Gateway learns the false IP address-to-MAC address mapping entries from these ARP packets and updates its ARP table. As a result, the ARP table is fully occupied by the false entries and unable to learn the ARP entries of legal Hosts, which causes that the legal Hosts cannot access the external network.

The IP-MAC Binding function allows the switch to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together when the Host connects to the switch. Basing on the predefined IP-MAC Binding entries, the ARP Inspection functions to detect the ARP packets and filter the illegal ARP packet so as to prevent the network from ARP attacks.

The **ARP Inspection** function is implemented on the **ARP Detect**, **ARP Defend** and **ARP Statistics** pages.

14.3.1 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.

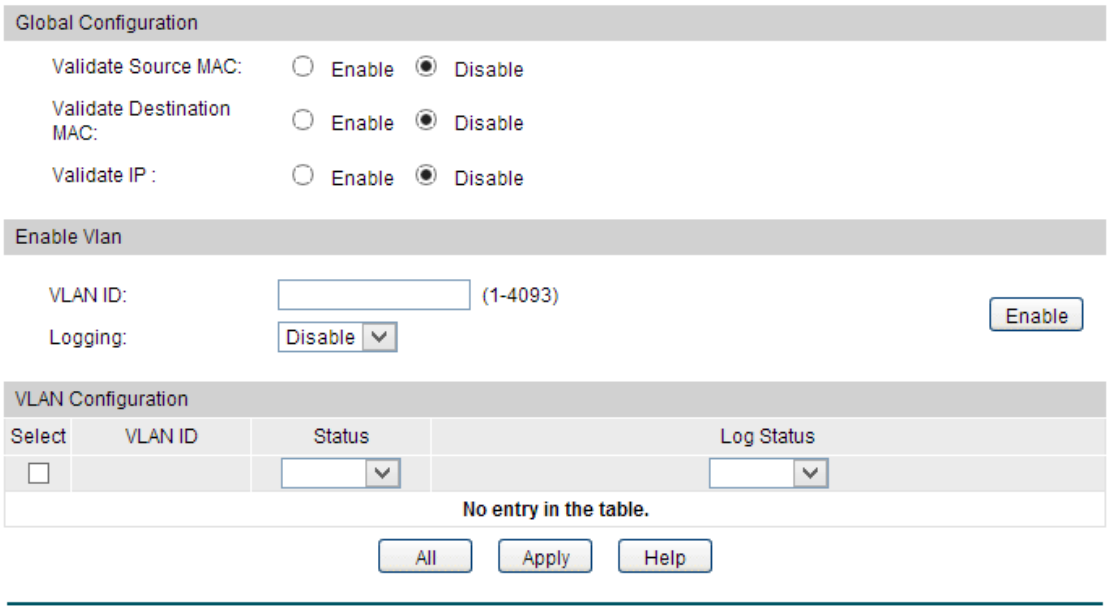


Figure 14-14 ARP Detect

Configuration Procedure:

1) In the **Global Configuration** section, enable or disable the following features.
2) In the **Enable VLAN** section, enable ARP Detect for the VLAN.

Entry Description:

Validate Source MAC:	Enable or disable the switch to check whether the source MAC address and the Sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.
Validate Destination MAC:	Enable or disable the switch to check whether the Destination MAC address and the Target MAC address are the same when receiving an ARP Reply packet. If not, the ARP packet will be discarded.
Validate IP:	Enable or disable the switch to check whether the Sender IP address of all ARP packets and the Target IP address of ARP Reply packets are legal. The illegal packets will be discarded.
VLAN ID	Enable/Disable the ARP Detect function, and click the **Apply** button to apply.
Logging:	With this option enabled, a log will be generated when an ARP packet is discarded.

14.3.2 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.

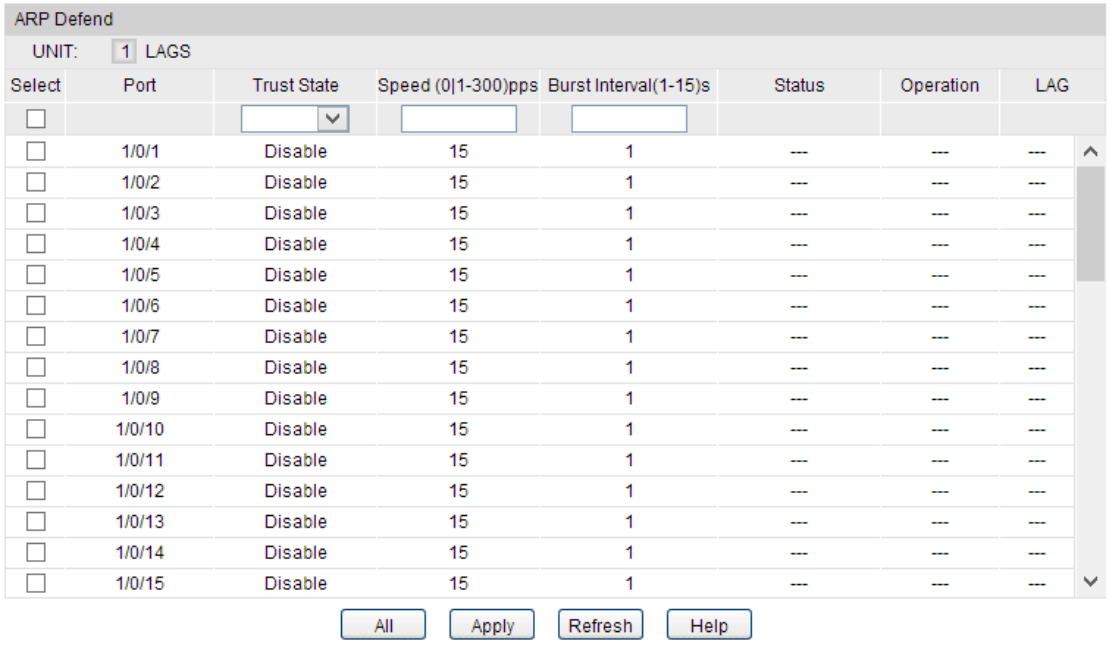


Figure 14-15 ARP Defend

Configuration Procedure:

Select one or more ports, and configure the relevant parameters. Then click **Apply.**

Entry Description:

UNIT:	Select the unit ID of the desired member in the stack.
Select:	Select your desired port for configuration. It is multi-optional.
Port:	Displays the port number.
Trust State:	Enable or disable this port to be a trusted port, on which the ARP packets will be forwarded directly without checked.
Speed(10-300)pps:	Enter a value to specify the maximum amount of the received ARP packets per second.
Burst Interval(1-15)s:	Enter a value to specify a time range. If the average speed of received ARP packets in this time range reach the limit, the port will be shut down.
Status	Displays the status of the ARP attack.
Operation:	Click the **Recover** button to restore the port to the normal status. The ARP Defend for this port will be re-enabled.
LAG:	Displays the LAG to which the port belongs to.

Note:

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

14.3.3 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.

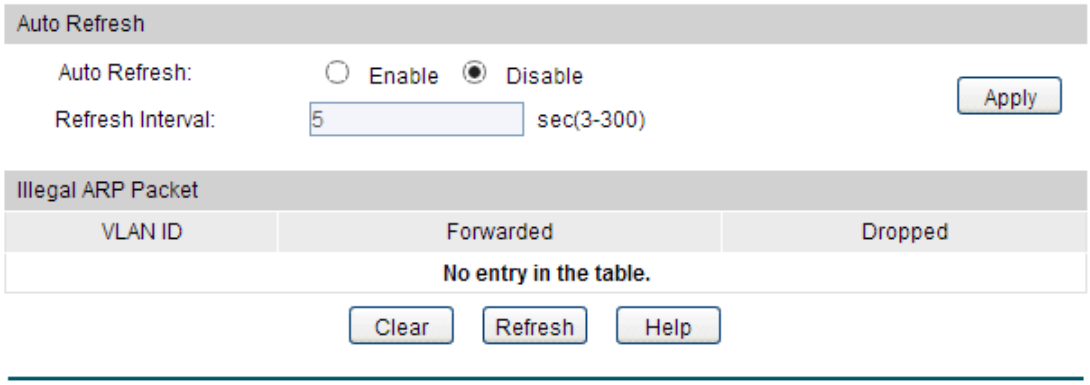


Figure 14-16 ARP Statistics

Configuration Procedure:

1) In the **Auto Refresh** section, configure the Auto Refresh feature.

2) In the Illegal ARP Packet section, view the statistics of ARP packets in each VLAN.

Entry Description:

Auto Refresh:	Enable or disable the Auto Refresh feature.
Refresh Interval:	Specify the refresh interval to display the ARP Statistics.
VLAN ID:	Displays the VLAN ID.
Forwarded:	Displays the number of forwarded packets in this VLAN.
Dropped:	Displays the number of dropped packets in this VLAN.

14.4 IP Source Guard

IP Source Guard is to filter the IP packets based on the IP-MAC Binding entries. Only the packets matched to the IP-MAC Binding rules can be processed, which can enhance the bandwidth utility.

Choose the menu **Network Security→IP Source Guard** to load the following page.

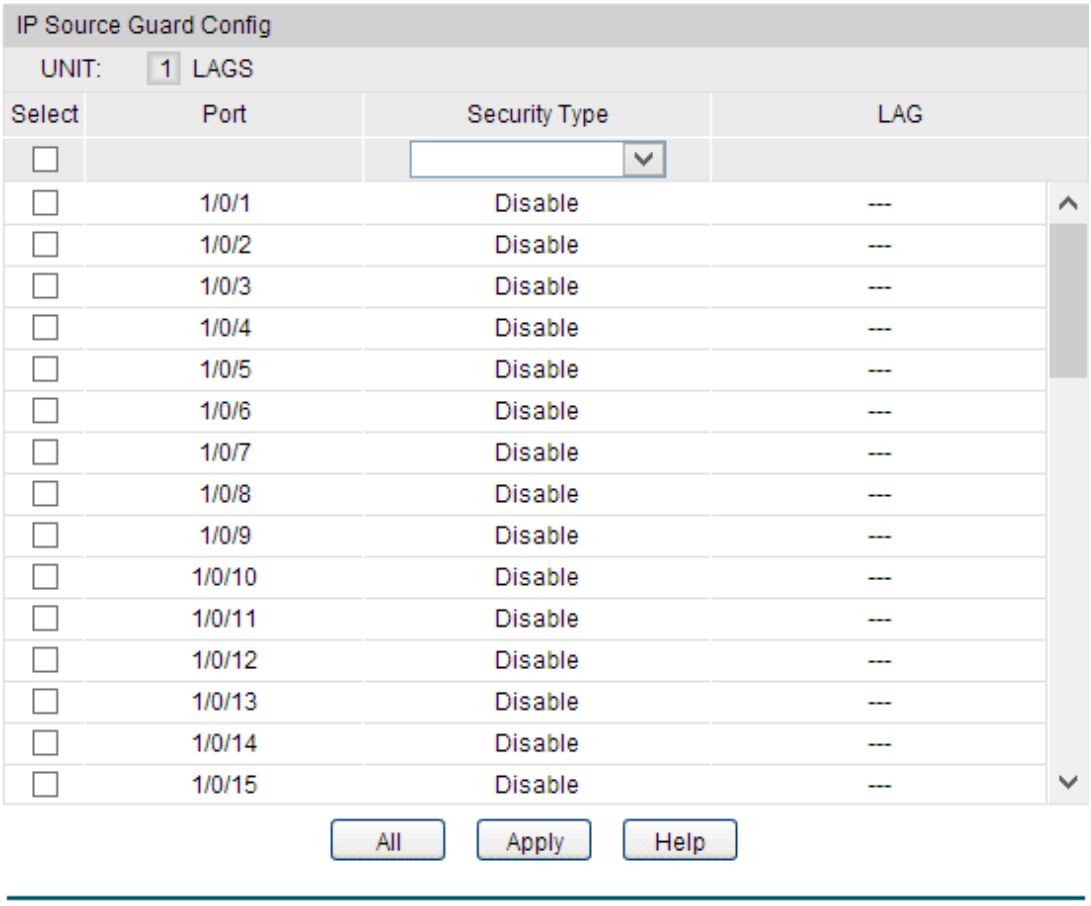


Figure 14-17 IP Source Guard

Configuration Procedure:

Select one or more ports, configure security type, and click **Apply**.

Entry Description:

UNIT:	Select the unit ID of the desired member in the stack.
Select:	Select your desired port for configuration. It is multi-optional.
Port:	Displays the port number.
Security Type:	Select Security Type for the port. • **Disable:** Select this option to disable the IP Source Guard feature for the port. • **SIP:** Only the packets with its source IP address and port number matched to the IP-MAC binding rules can be processed. • **SIP+MAC:** Only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed.
LAG:	Displays the LAG to which the port belongs to.

14.5 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 14-1 Defendable DoS Attack Types

14.5.1 DoS Defend

On this page, you can enable the DoS Defend type appropriate to your need.

Choose the menu **Network Security→DoS Defend→DoS Defend** to load the following page.

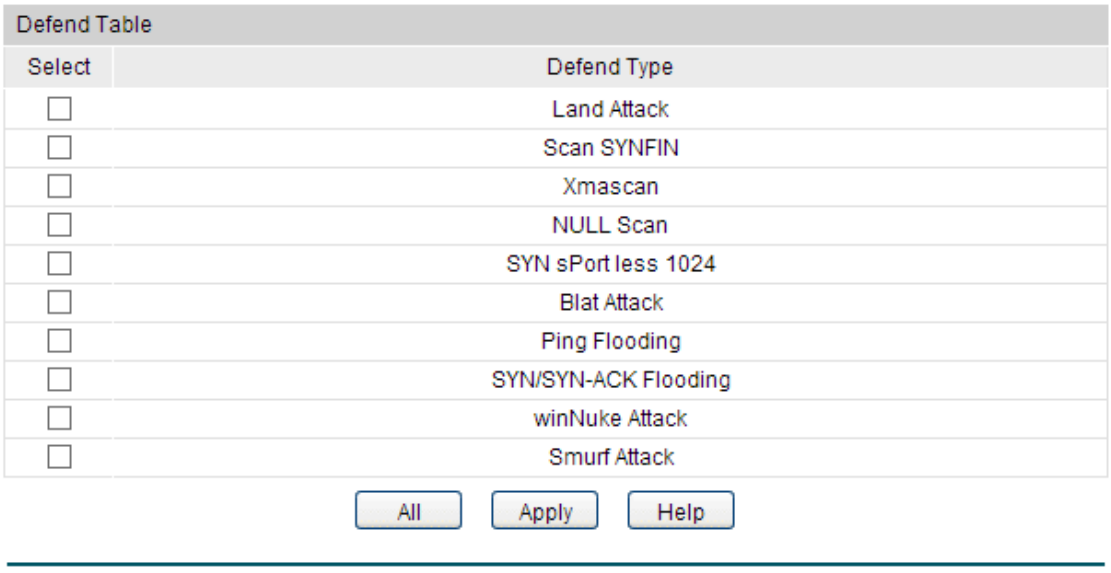


Figure 14-18 DoS Defend

Configuration Procedure:

Select one or more Defend Types to be enabled, and click **Apply**.

Entry Description:

Select:	Select the entry to enable the corresponding Defend Type.
Defend Type:	Displays the Defend Type name.

14.6 802.1X

The 802.1X protocol was developed by IEEE802 LAN/WAN committee to deal with the security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to solve mainly authentication and security problems.

802.1X is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access control devices. With the 802.1X protocol enabled, a supplicant can access the LAN only when it passes the authentication, whereas those failing to pass the authentication are denied when accessing the LAN.

➢ **Architecture of 802.1X Authentication**

802.1X adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system, as shown in the following figure.

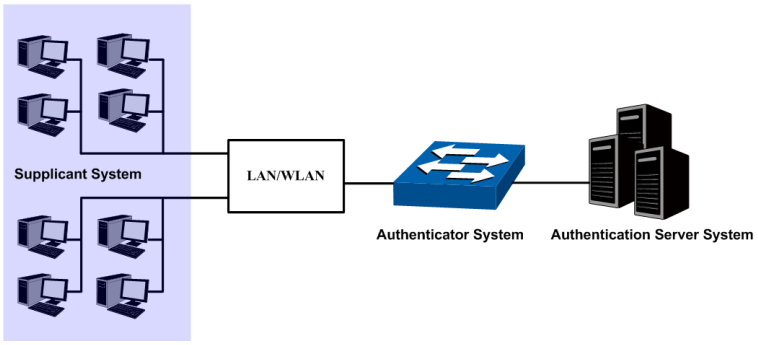


Figure 14-19 Architecture of 802.1X authentication

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 authentication way for the EAP relay mode. The following figure describes the basic EAP-MD5 authentication procedure.

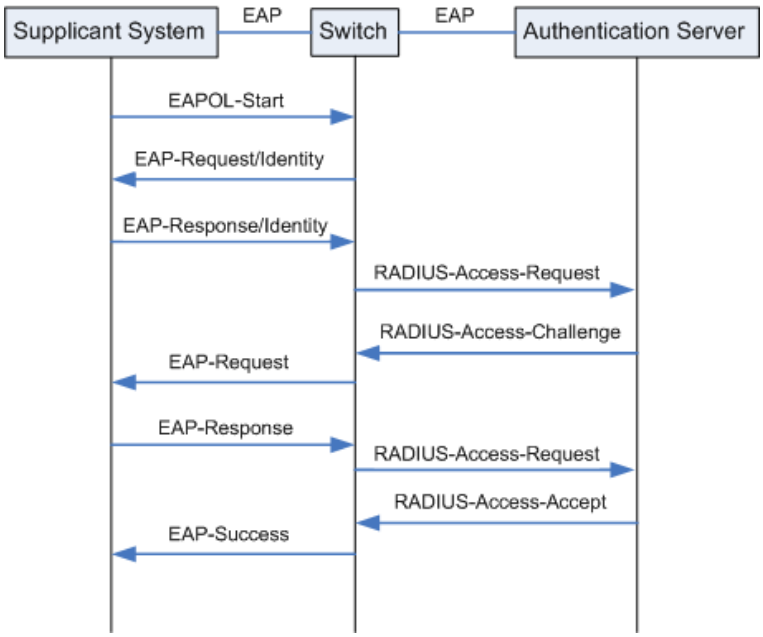


Figure 14-20 EAP-MD5 Authentication Procedure

(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.

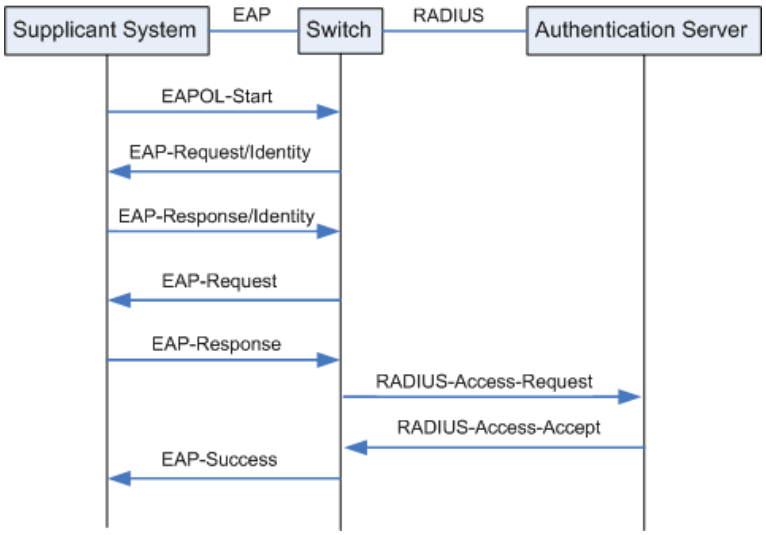


Figure 14-21 PAP Authentication Procedure

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.

14.6.1 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.

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

Figure 14-22 Global Config

Configuration Procedure:

Enable or disable 802.1X and the Accounting feature globally and click **Apply**.

14.6.2 Port Config

On this page, you can configure the 802.1X features for the ports basing on the actual network.

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

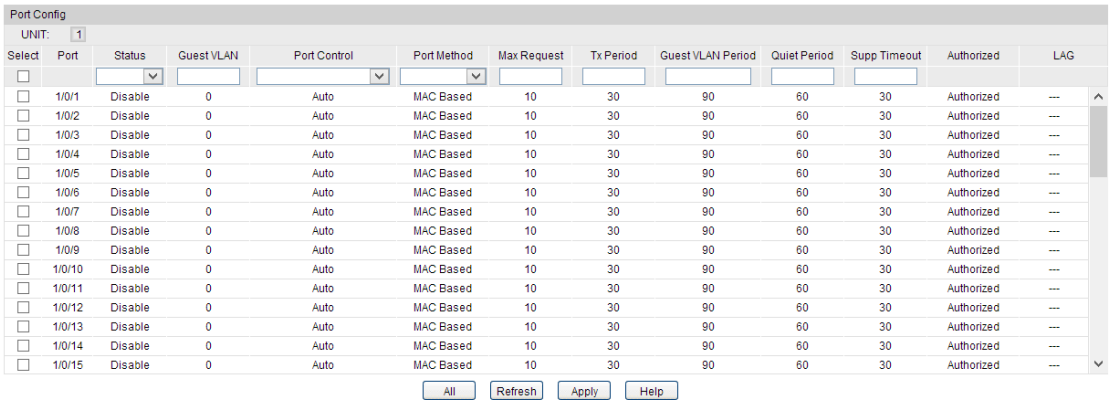


Figure 14-23 Port Config

Configuration Procedure:

Select one or more ports and configure the relevant parameters. Then click **Apply**.

Entry Description:

UNIT: Select the unit ID of the desired member in the stack.

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: Specify the VLAN ID needed to enable the Guest VLAN function, ranging from 0 to 4093. 0 indicates that the Guest VLAN function is disabled. The supplicants in the Guest VLAN can access the specified network sources.

Port Control: 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.

Port Method: 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.

Max Request: Specify the maximum number of attempts to send the authentication packet. It ranges from 1 to 10 times and the default is 10 times.

Tx Period: Specify the Dot1x transmit period on the specified port to determine when an EAP-Request/Identity packet is to be transmitted. It ranges from 1 to 65535 seconds and the default time is 30 seconds.

Guest VLAN Period: Specify the Guest VLAN Period of the port. Once set the Guest VLAN on the port, the port will be included in the Guest VLAN after the Guest VLAN Period. It ranges from 1 to 300 seconds and the default time is 90 seconds.

Quiet Period: Specify the Quiet Period. It ranges from 0 to 65535 seconds and the default time is 60 seconds.

The quiet period starts after the authentication fails. During the quiet period, the switch does not process authentication requests from the same client.

Supp Timeout: Specify the maximum time to wait for EAP-Response/MD5-challenge packet from the supplicant before timing out the supplicant.

It ranges from 1 to 65535 seconds and the default time is 30 seconds. If the switch does not receive any reply from the client within the specified time, it will resend the request.

Authorized: Displays the authentication status of the port.

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

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. In addition, the authentication parameters of the switch and the authentication server should be the same.

Configuration Procedure:

Step	Operation	Description
1	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.
2	Install the 802.1X client software.	Required. For the client computers, you are required to install the 802.1X software TpSupplicant provided on the CD. The installation guide is also provided on the CD.

3	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.
4	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.
5	Configure the parameters of the authentication server	Required. On the **Network Security→AAA→Radius Config** page, configure the parameters of the server.

14.7 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 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.

- **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.

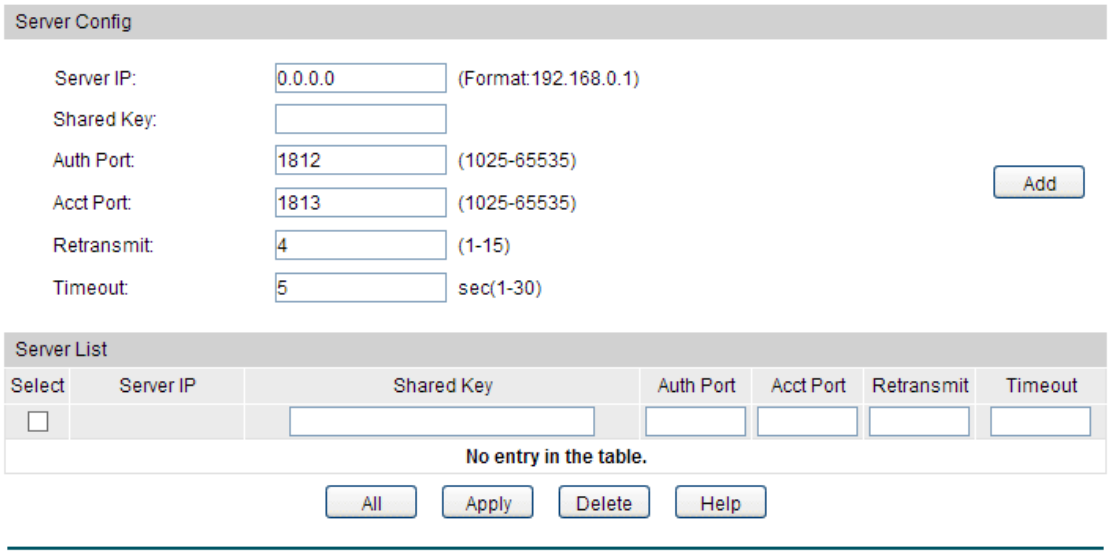
- **RADIUS/TACACS+ Server**

User can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

14.7.1 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.



Configuration Procedure:

Configure the RADIUS server's IP and other relevant parameters under the Server Config.

View, edit and delete the configured RADIUS servers in the Server List.

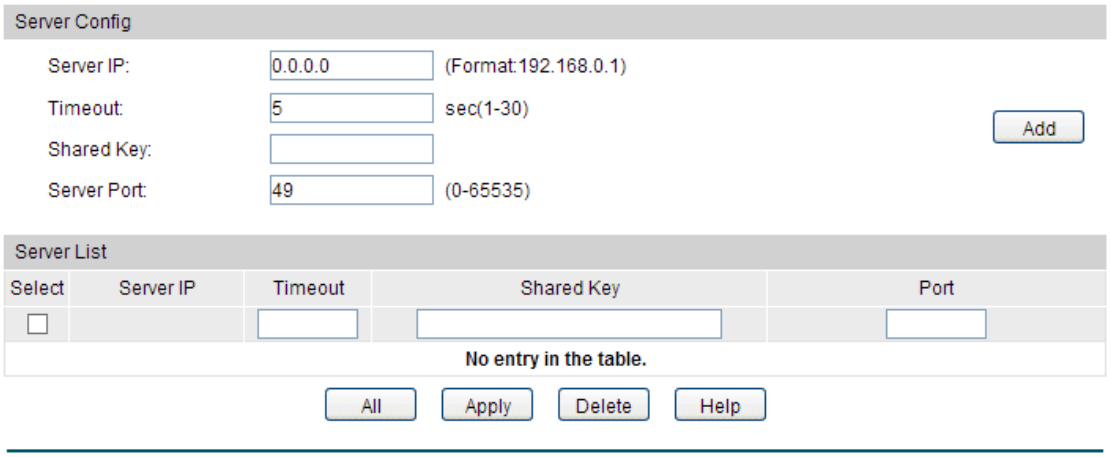
Entry Description:

Server IP:	Enter the IP of the server running the RADIUS secure protocol.
Shared Key:	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Auth Port:	Specify the UDP destination port on the RADIUS server for authentication requests.
Acct Port:	Specify the UDP destination port on the RADIUS server for accounting requests.
Retransmit:	Specify the number of times a request is resent to a server if the server does not respond.
Timeout:	Specify the time interval that the switch waits for the server to reply before resending.

14.7.2 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.



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.
Server Port:	Specify the TCP port used on the TACACS+ server for AAA.

14.7.3 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.

Choose the menu **Network Security→AAA→Authentication List** to load the following page.

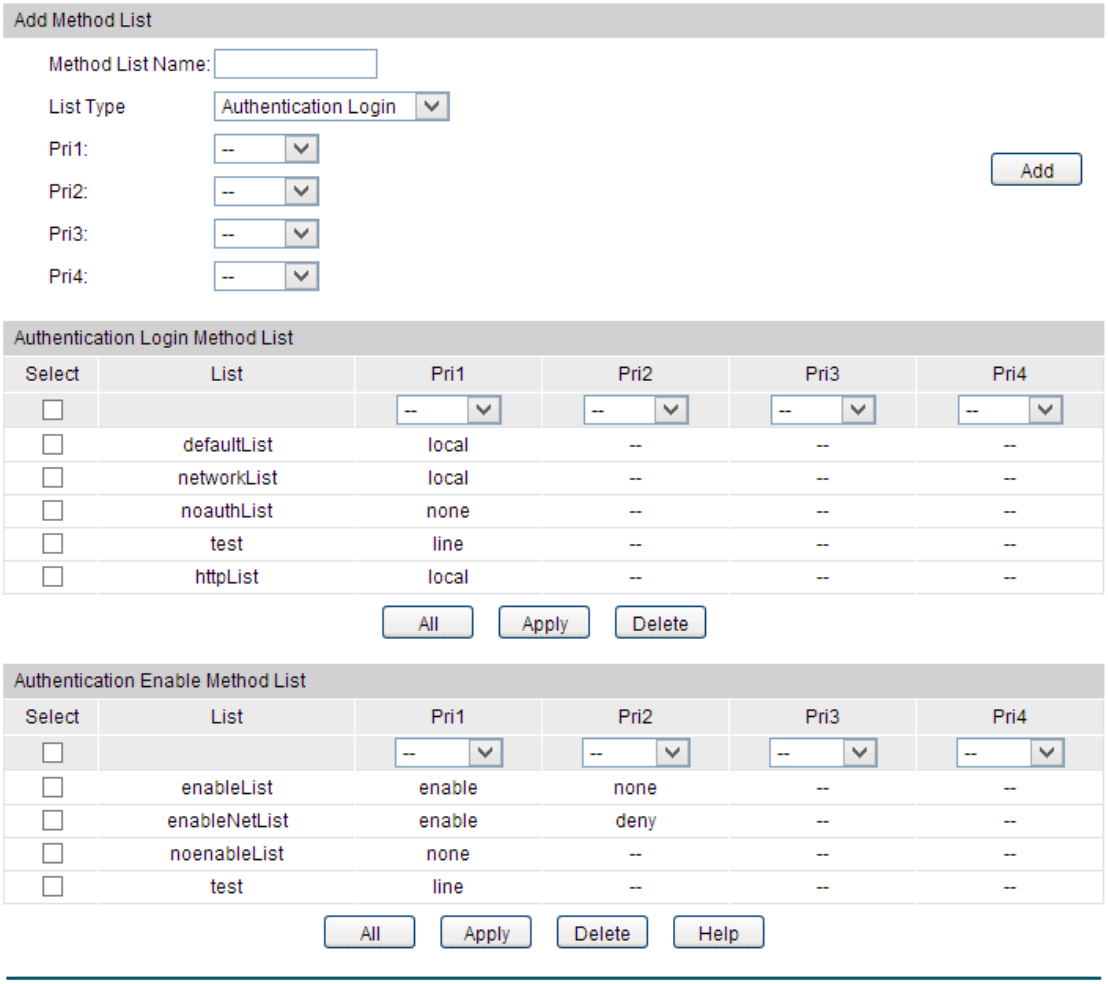


Figure 14-22 Authentication Method List Config

Configuration Procedure:

1) Enter the method list name.
2) Specify the authentication type as Login or Enable.
3) Configure the authencation method with priorities.

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. enable: Use the locally configured Enable password to verify the user's credentials. none: No authentication is used. line: Use the locally configured Line password to verify the user's credentials. radius: Use the remote RADIUS server/server groups for authentication. tacacs: Use the remote TACACS+ server/server groups for authentication. deny: Deny the authentication. Only Enable Method supports this option.

Tips:

If the Enable password is verified on the remote RADIUS server, the switch will send the Enable authentication with the default username as $enab15$. If the Enable password is verified locally, the Enable password should be previously set by the admin users using the command lines. For more details please refer to the command **enable password** in the Command Line Interface Guide on the resource CD.

14.7.4 Application Authentication List Config

Users can configure authentication method lists on the following access applications: console, telnet, ssh and http.

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

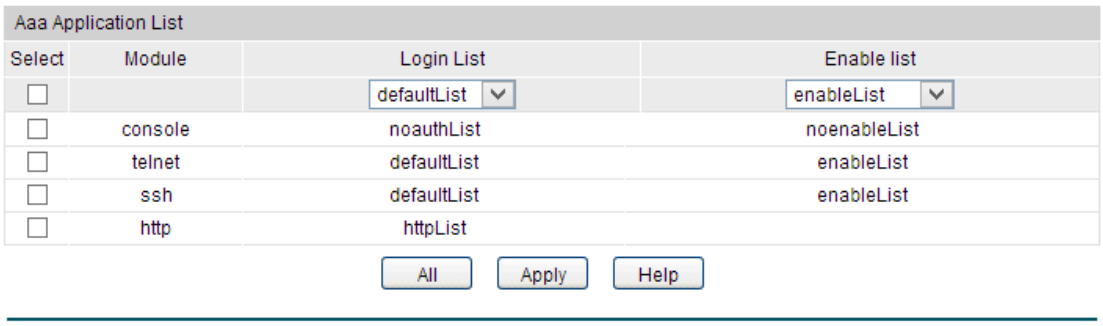


Figure 14-23 Application Authentication Settings

Configuration Procedure:

1) Select the application module.
2) Configure the authentication method list from the Login List drop-down menu. This option defines the authentication method for users accessing the switch.

3) Configure the authentication method list from the Enable List drop-down menu. Thisoption defines the authentication method for users requiring the administrator privilege.

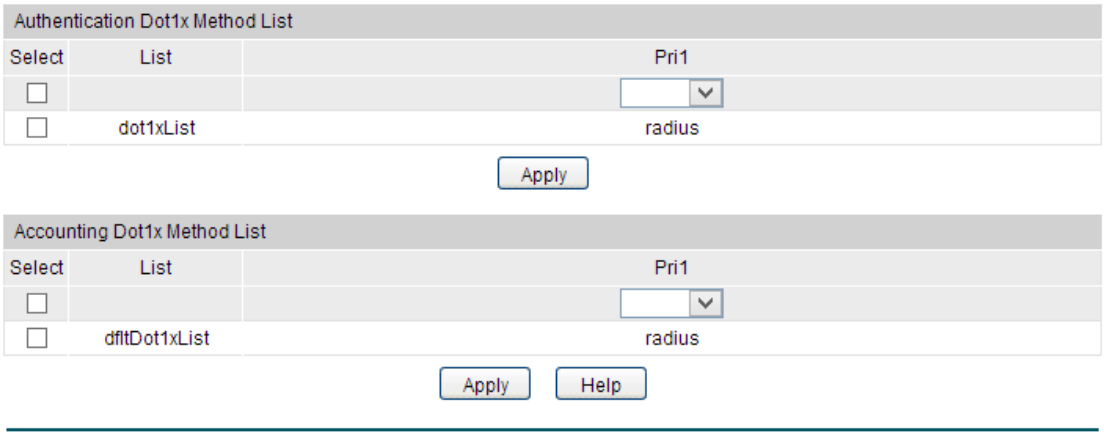
Entry Description:

Module:	Lists of the configurable applications on the switch.
Login List:	Configure an application for the login utilizing a previously configured method list.
Enable List:	Configure an application to promote the user level to admin-level users utilizing a previously configured method list.

14.7.5 802.1X Authentication Server Config

This page is used to configure the RADIUS server group used in 802.1X Authentication and Accounting.

Choose the menu **Network Security→AAA→Dot1x List** to load the following page.



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 Accounting Dot1x Method List Table.

14.7.6 Default Settings

Feature	Default Settings
RADIUS server	• Auth port is 1812. • Acct port is 1813. • Retransmit is 4 times. • Timeout is 5 seconds.

TACACA+ server	• Communication port is 49. • Timeout is 5 seconds.
Authentication login method list	The list contains local, and the default login username and passwords are both admin.
Authentication enable method list	The list is empty, which means users can prompt to administrator privilege without password.
Access application authentication	The application console/telnet/ssh/http use the default Login List and default Enable list.
802.1X authentication server and accounting server	802.1X authentication uses the radius server group. 802.1X accounting uses the radius server group.

Return to CONTENTS

Chapter 15 SNMP

➢ SNMP Overview

SNMP (Simple Network Management Protocol) has gained the most extensive application on the UDP/IP networks. SNMP provides a management frame to monitor and maintain the network devices. It is used for automatically managing the various network devices no matter the physical differences of the devices. Currently, the most network management systems are based on SNMP.

SNMP is simply designed and convenient for use with no need of complex fulfillment procedures and too much network resources. With SNMP function enabled, network administrators can easily monitor the network performance, detect the malfunctions and configure the network devices. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

➢ SNMP Management Frame

SNMP management frame includes three network elements: SNMP Management Station, SNMP Agent and MIB (Management Information Base).

SNMP Management Station: SNMP Management Station is the workstation for running the SNMP client program, providing a friendly management interface for the administrator to manage the most network devices conveniently.

SNMP Agent: Agent is the server software operated on network devices with the responsibility of receiving and processing the request packets from SNMP Management Station. In the meanwhile, Agent will inform the SNMP Management Station of the events whenever the device status changes or the device encounters any abnormalities such as device reboot.

MIB: MIB is the set of the managed objects. MIB defines a few attributes of the managed objects, including the names, the access rights, and the data types. Every SNMP Agent has its own MIB. The SNMP Management station can read/write the MIB objects basing 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.

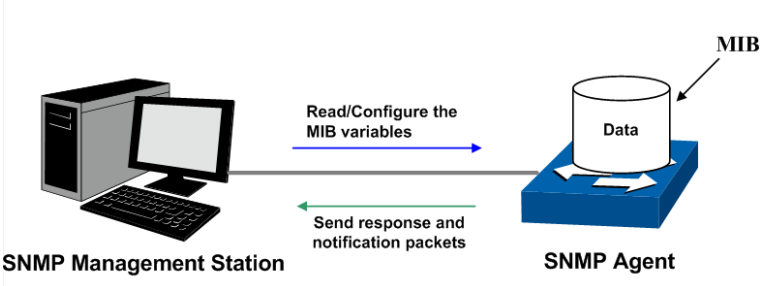


Figure15-1 Relationship among SNMP Network Elements

➢ **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: Basing 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}.

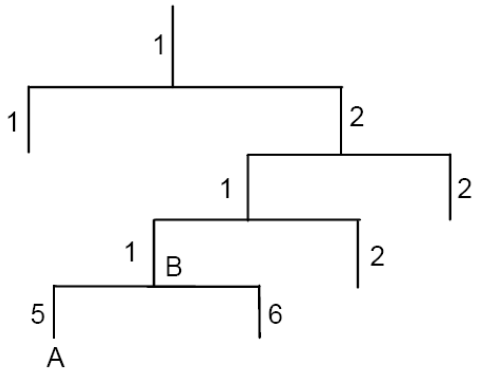


Figure15-2 Architecture of the MIB tree

➢ **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 an 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 an SNMP Group can manage the switch via the client program on management station. The specified User Name and the Auth/Privacy Password are used for SNMP Management Station to access the SNMP Agent, functioning as the password.

SNMP module is used to configure the SNMP function of the switch, including three submenus: **SNMP Config**, **Notification** and **RMON**.

15.1 SNMP Config

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

15.1.1 Global Config

Choose the menu **SNMP** → **SNMP Config** → **Global Config** to load the following page.

Figure 15-3 Global Config

Configuration Procedure:

Configure the local engine ID and remote engine ID.

Entry Description:

- **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 informs from Switch.

Note:

1. The total hexadecimal characters of Engine ID should be even.
2. Change the Local Engine ID could make local user and community invaild, please re-create new local users or community.
3. Change the Remote Engine ID could make remote user invaild, please re-create new remote users.

15.1.2 SNMP View

The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Choose the menu **SNMP** → **SNMP Config** → **SNMP View** to load the following page.

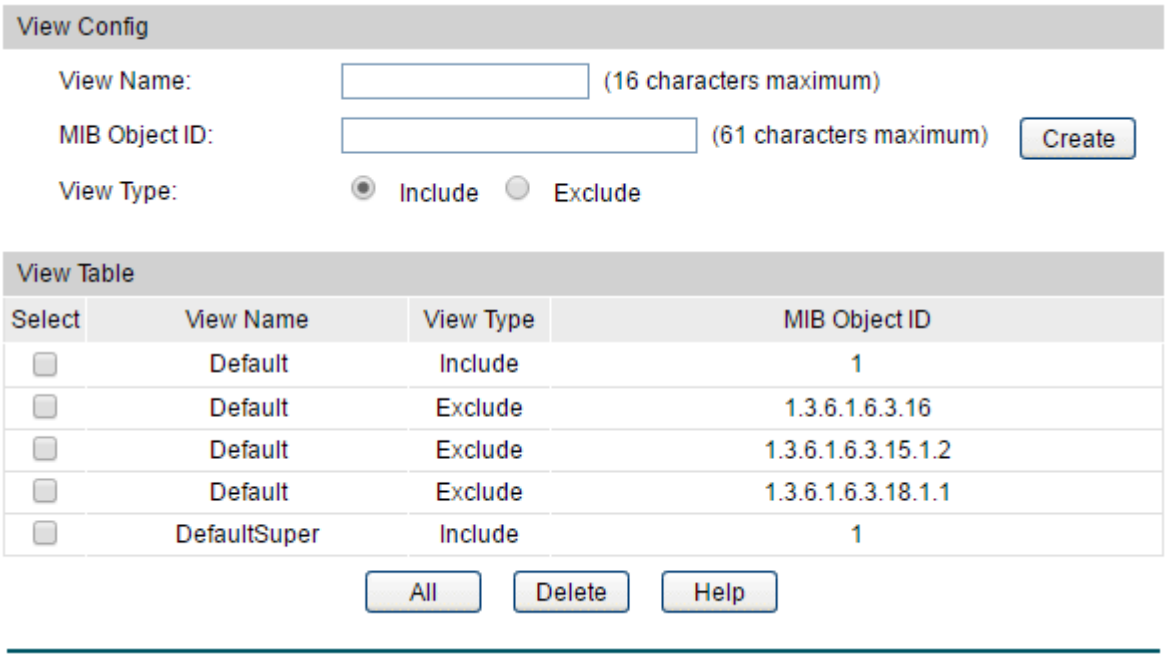


Figure15-4 SNMP View

Configuration Procedure:

Create an SNMP view, and configure the content of the view.

Entry Description:

➢ **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 vew entry.

15.1.3 SNMP Group

On this page, you can configure SNMP Group to control the network access by providing the users in various groups with different management rights via the Read View, Write View and Notify View.

Choose the menu **SNMP** → **SNMP Config** → **SNMP Group** to load the following page.

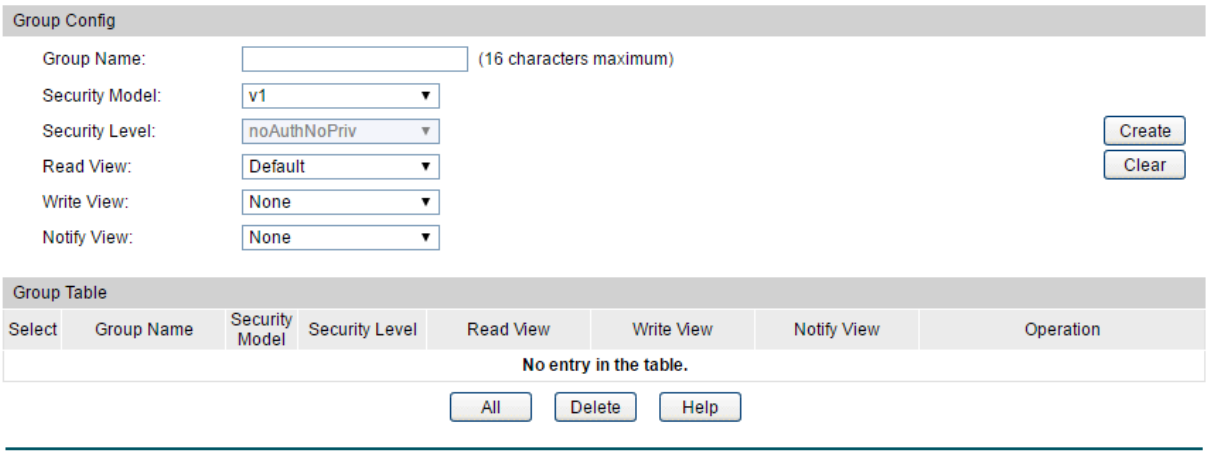


Figure15-5 SNMP Group

Configuration Procedure:

1) Set the group name and security model. If you choose SNMPv3 as the security model, you need to further configure security level.

2) Set the read, write and notify view of the SNMP Group. Click **Create**.

Entry Description:

➢ **Group Config**

Group Name: Enter the SNMP Group name. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group.

These three items of the Users in one group should 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 notification 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's 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 Default.

15.1.4 SNMP User

The User in an 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.

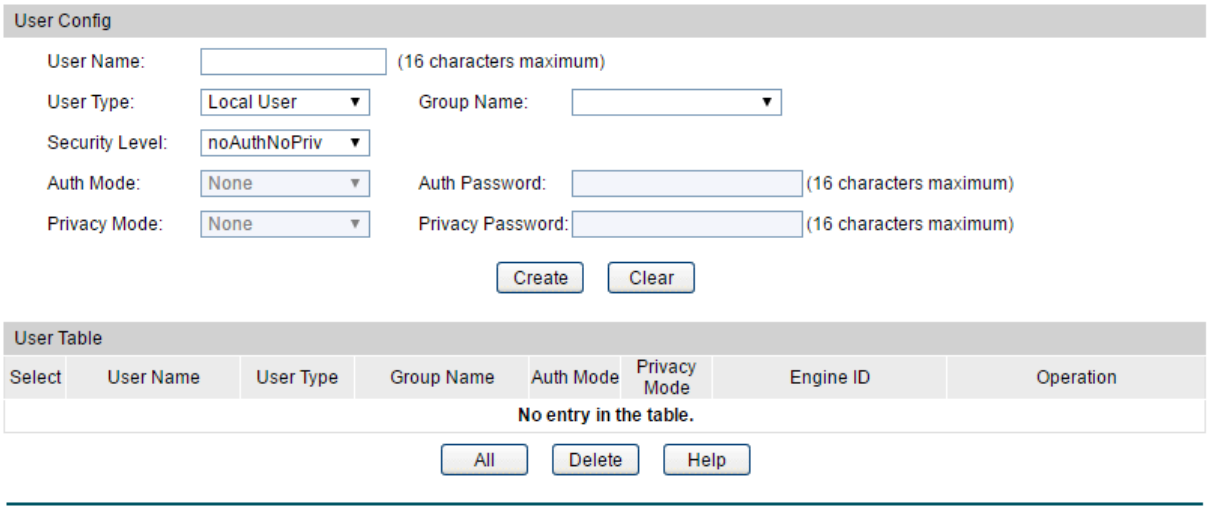


Figure15-6 SNMP User

Configuration Procedure:

1) Specify the user name, user type and the group which the user belongs to.

2) Set the security model. If you have chosen authNoPriv or authPriv as the security level, you need to set corresponding Auth Mode or Privacy Mode.

Entry Description:

➢ **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 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.

Auth Mode: Displays the Authentication Mode of the User.

Privacy Mode: Displays the Privacy Mode of the User.

Engine ID: Displays the Engine ID 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 Level.

15.1.5 SNMP Community

SNMP v1 and SNMP v2c adopt community name authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password. If SNMP v1 or SNMP v2c is employed, you can directly configure the SNMP Community on this page without configuring SNMP Group and User.

Choose the menu **SNMP** → **SNMP Config** → **SNMP Community** to load the following page.

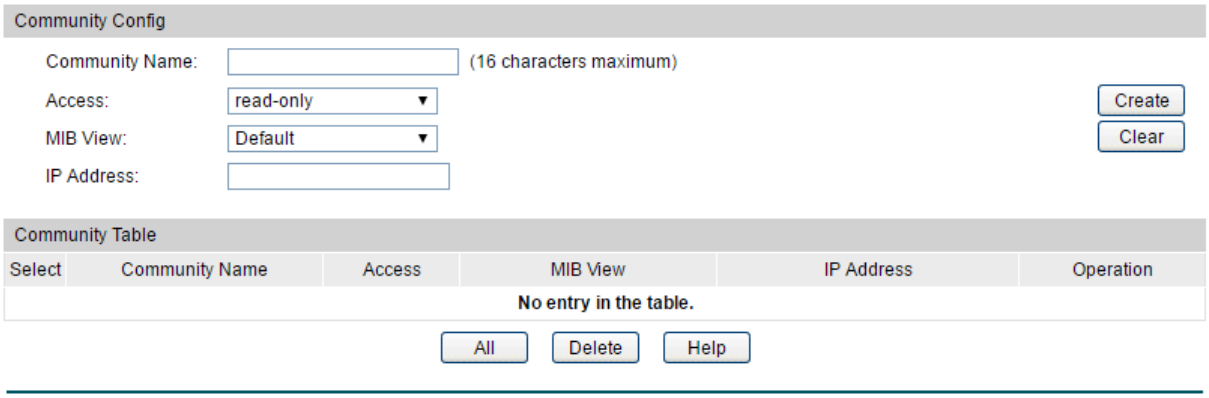


Figure 15-7 SNMP Community

Configuration Procedure:

Set the community name, access rights and the related view. Click **Create**.

Entry Description:

➢ **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.

IP Address: Enter the IP address which could connect the SNMP server. If null, all user could connect the SNMP server.

➢ **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.

IP Address: Displays the IP address of the SNMP Community.

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 Default.

Configuration Procedure:

- If SNMPv3 is employed, please take the following steps:

Step	Operation	Description
1	Create SNMP View.	Required. On the **SNMP→SNMP Config→SNMP View** page, create SNMP View of the management agent. The default View Name is Default and the default OID is 1.
2	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.
3	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:

<table>
<tr><th>Step</th><th colspan="2">Operation</th><th>Description</th></tr>
<tr><td>1</td><td colspan="2">Create SNMP View.</td><td>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.</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Configure access level for the User.</td><td>Create SNMP Community directly.</td><td rowspan="2">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.</td></tr>
<tr><td>Create SNMP Group and SNMP User.</td></tr>
</table>

15.2 Notification

With the Notification function enabled, the switch can initiatively report to the management station about the important events that occur on the Views (e.g., the managed device is rebooted), which allows the management station to monitor and process the events in time.

The notification information includes the following two types:

Trap：Trap is the information that the managed device initiatively sends to the Network management station without request.

Inform：Inform packet is sent to inform the management station and ask for the reply. The switch will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times. The Inform type, employed on SNMPv2c and SNMPv3, has a higher security than the Trap type.

The **Notification** can be configured on the **Notification Config** and **Traps Config** pages.

15.2.1 Notification Config

On this page, you can configure the notification function of SNMP.

Choose the menu **SNMP** → **Notification** → **Notification Config** to load the following page.

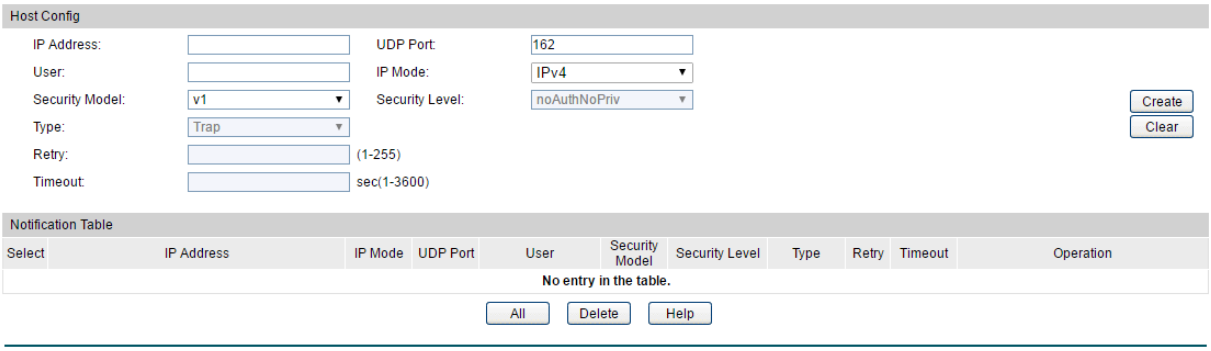


Figure15-8 Notification Config

Configuration Procedure:

1) Specify the IP address of the host, the UDP port that sends notifications, and choose the IP mode according to the network environment.
2) Specify the user name or community name used by the NMS, and configure the security model and security level based on the settings of the user or community.
3) Choose a notification type based on the SNMP version. If you choose the Inform type, you need to set retry times and timeout interval.
4) Click **Create**.

Entry Description:

- **Host Config**

IP Address:

If you set the **IP Mode** to IPv4, specify an IPv4 address for the host.

If you set the **IP Mode** to IPv6, specify an IPv6 address for the host.

UDP Port:

Specify a UDP port on the host to send notifications. The default is port 162. For communication security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.

IP Mode:

Choose an IP mode for the host, which should be coordinated with the **IP Address**.

User:

Specify the user name or community name used by the NMS.

Security Model:

Choose the corresponding SNMP version for the NMS.

The version should be consistent with settings of the user or community.

v1: The NMS uses SNMPv1.

v2: The NMS uses SNMPv2c.

v3: The NMS uses SNMPv3.

Security Level:

Choose the security level for the NMS that uses SNMPv3. The setting should be consistent with that of the specified user or community.

noAuthNoPriv: No authentication mode or privacy mode is applied to check or encrypt packets.

authNoPriv: An authentication mode is applied to check packets, but no privacy mode to encrypt packets.

authPriv: An authentication mode and a privacy mode are applied to check and encrypt packets.

Type: Choose a notification type for the NMS that uses SNMPv2c or SNMPv3; the default type is Trap.

- Trap: Set the switch to send Trap messages to the NMS. When the NMS receives a trap message, it will not send a response to the switch. Thus the switch cannot determine whether the trap is received or not, and the trap that is not received will not be resent.
- Inform: Set the switch to send Inform messages to the NMS. When the NMS receives an Inform message, it sends a response to the switch. If the switch does not receive a response within the Timeout interval, it will resend the Inform message. Therefore, Informs are more reliable than Traps.

Retry: Set the retry times for Informs; the default is 3. The switch will resend the Inform message if it does not receive response from the NMS within the timeout interval. It will stop sending Inform messages when the retry time reaches the limit.

Timeout: Set the length of time that the switch waits for a response from the NMS after sending an inform message; the default is 100 seconds. Set the length of time that the switch waits for a response from the NMS after sending an inform message; the default is 100 seconds.

➢ **Notification Table**

Select: Select the desired entry to delete the corresponding management station.

IP Address: Displays the IP Address of the management host.

UDP Port: Displays the UDP port used to send notifications.

User: Displays the User name of the management station.

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

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

Type: Displays the type of the notifications.

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

Timeout: 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.

15.2.2 Traps Config

On this page, you can configure the traps of SNMP.

Choose the menu **SNMP** → **Notification** → **Traps Config** to load the following page.

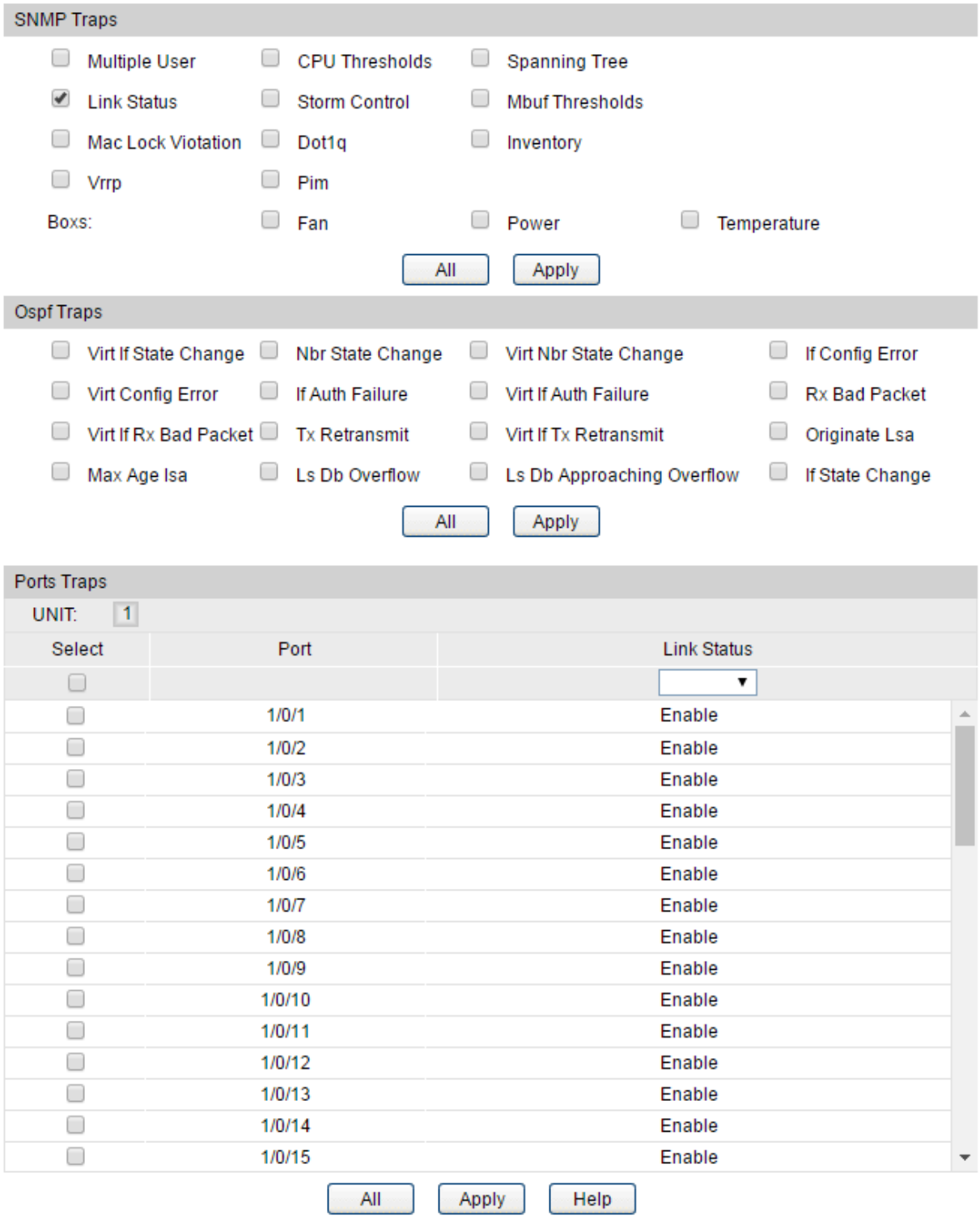


Figure15-9 Traps Config

Configuration Procedure:

Configure traps you desire to send to the SNMP server. Click **Apply**.

Entry Description:

- **SNMP Traps**

Multiple User:	Generates a trap when the same user ID is logged into the switch more than once at the same time.
CPU Thresholds:	Generates a trap when the CPU utilization is over 80%.
Spanning Tree:	Generates a trap when the status of STP changes.
Link Status:	Generates a trap when the up/down status of an interface changes.
Storm Control:	Generates a trap when the multicast or broadcast rate exceeds the predefined value.
Mbuf Thresholds	Generates a trap when the memory utilization is over 80%.
Mac Lock Violation:	Generates a trap when a packet with a disallowed MAC address is received on a locked port.
Dot1q:	Generates a trap when creating or deleting a VLAN.
Inventory:	Generates a trap for Inventory.
Vrrp:	Generates a trap for Virtual Routing Redundancy Protocol (VRRP) changes.
Pim:	Generates a trap for Protocol-Independent Multicast (PIM) changes.
Fan:	Generates a trap for fan.
Power:	Generates a trap for power.
Temperature:	Generates a trap for temperature.

- **OSPF Traps**

Virt If State Change:	Generates a trap when virtual interface state changes.
Nbr State Change:	Generates a trap when non-virtual neighbour state changes.
Virt Nbr State Change:	Generates a trap when virtual neighbour state changes.
If Config Error:	Generates a trap when configure mismatch errors occur on non-virtual interfaces.
Virt Config Error:	Generates a trap when configure mismatch errors occur on virtual interfaces.

If Auth Failure:	Generates a trap when authentication failures occur on non-virtual interfaces.
Virt If Auth Failure:	Generates a trap when authentication failures occur on virtual interfaces.
Rx Bad Packet:	Generates a trap when packet parse failures occur on non-virtual interfaces.
Virt If Rx Bad Packet:	Generates a trap when packet parse failures occur on virtual interfaces.
Tx Retransmit:	Generates a trap when packet retransmission occur on non-virtual interfaces.
Virt If Tx Retransmit:	Generates a trap when packet retransmission occur on virtual interfaces.
Originate Lsa:	Generates a trap when OSPF originates a new LSA.
Max Age lsa:	Generates a trap when one of the LSAs in the link-state database has aged to maxage.
Ls Db Overflow:	Generates a trap when the number of LSAs in the link-state database overflows.
Ls Db Approaching Overflow:	Generates a trap when the number of LSAs in the link-state database is approaching overflow.
If State Change:	Generates a trap when non-virtual interface state changes.

- **Port Traps**

Port:	Displays the port number of the switch.
Link status:	Enable or disable link status traps for the desired port. Allow SNMP Linkup and Linkdown traps.

15.3 RMON

RMON (Remote Monitoring) basing 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 **History, Event** and **Alarm** pages.

15.3.1 History

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

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

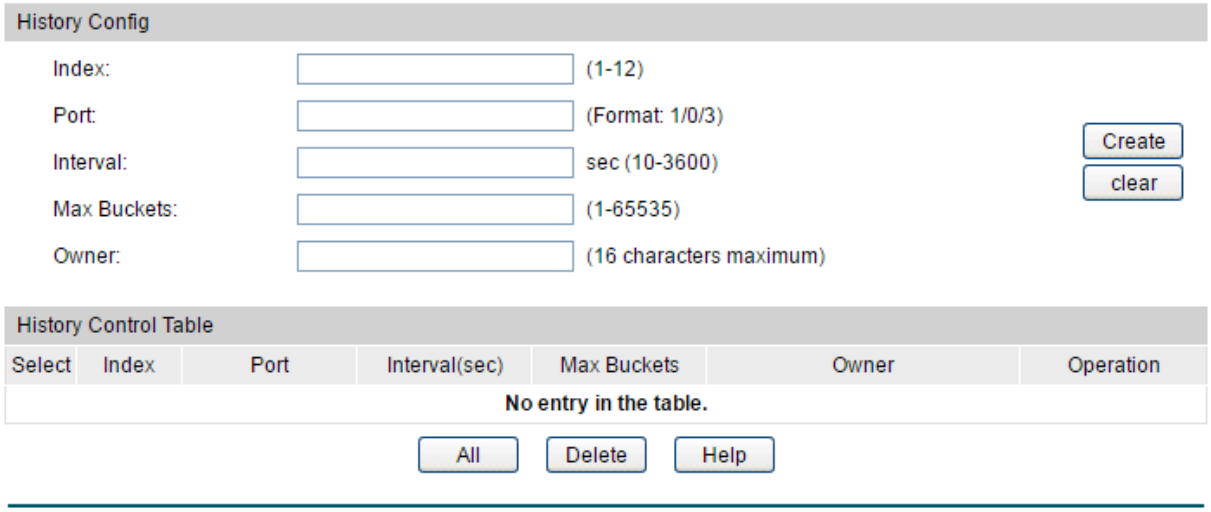


Figure 15-10 History Control

Configuration Procedure:

Configure the history group for RMON. Click **Create**.

Entry Description:

Index: Specify the index number of the entry.

Port: Specify the port from which the history samples were taken, in format as 1/0/1.

Interval: Specify the interval to take samplings from the port, ranging from 10 to 3600 seconds. The default is 1800 seconds.

Max Buckets Displays the maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 65535. The default is 50 buckets.

Owner: Enter the name of the device or user that defines the entry.

Operation: Click "Edit" to edit the history group entry.

15.3.2 Event

On this page, you can configure the RMON events.

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

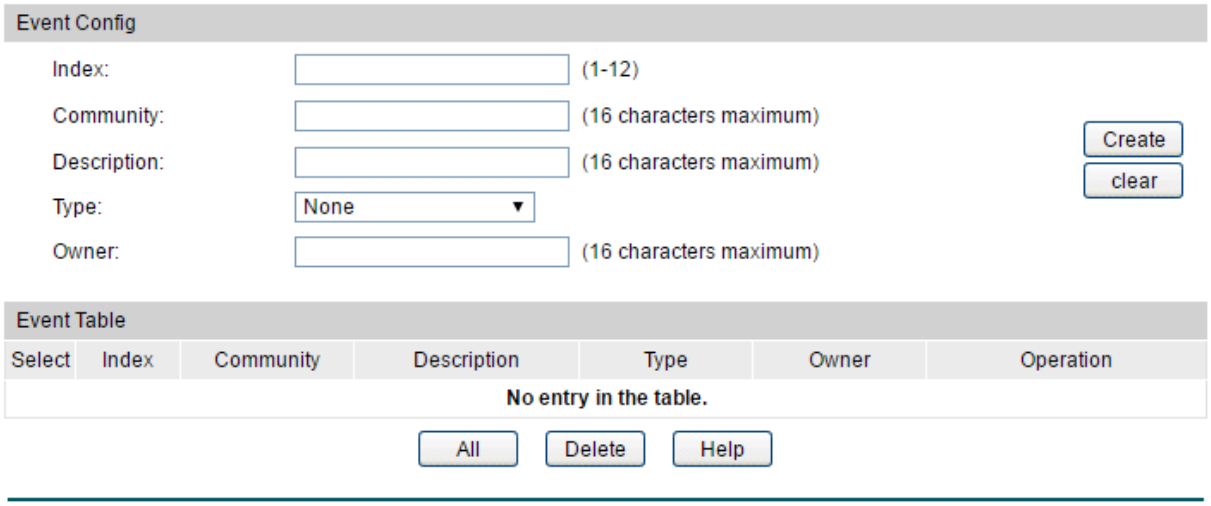


Figure15-11 Event Config

Configuration Procedure:

Configure the event group for RMON. Click **"Create"**.

Entry Description:

Index: Displays the index number of the entry.

Community: 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.

Operation: Click "Edit" to edit the event group entry.

15.3.3 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.

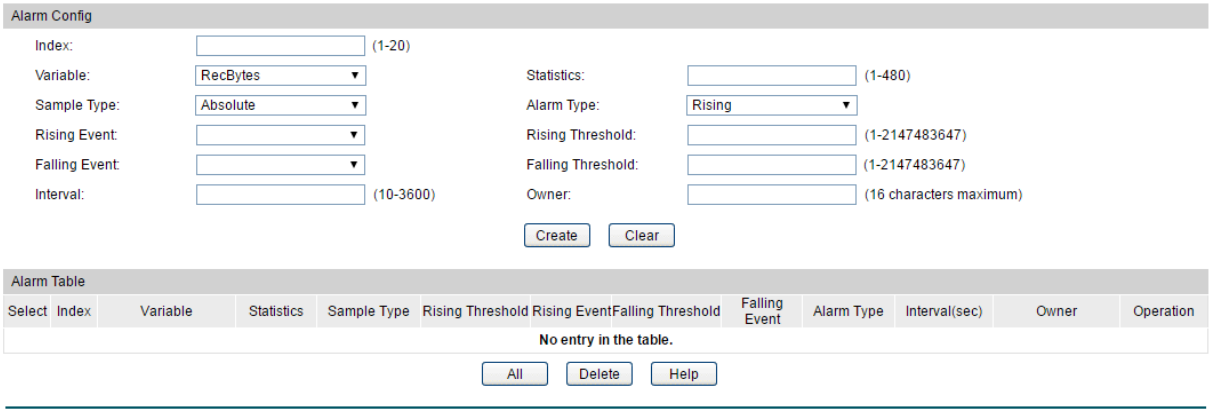


Figure 15-12 Alarm Config

Configuration Procedure:

1) Specify the index number of the alarm group, choose a variable to be monitored, and associate the entry with a statistics entry.

2) Set the sample type, the alarm type, the rising and falling event action and the corresponding threshold of the entry. Enter the alarm interval time.

3) Enter the owner name.

4) Click **Create**.

Entry Description:

Index: Displays the index number of the entry.

Variable: Select the alarm variables from the drop-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.

Alarm Type: Specify the type of the alarm.

- **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.
- **All:** The alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold.

Rising Event: Select the index of the corresponding event which will be triggered if the sampled value is larger than the rising Threshold.

Rising Threshold: Enter the rising counter value that triggers the rising threshold alarm, ranging from 1 to 2147483647.

Falling Event: Select the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold.

Falling Threshold: Enter the falling counter value that triggers the falling threshold alarm, ranging from 1 to 2147483647.

Interval: Enter the alarm interval time in seconds, ranging from 10 to 3600.

Owner: Enter the name of the device or user that defines the entry.

Operation: Click "Edit" to edit the alarm group entry.

Note:

When alarm variables exceed the Threshold on the same direction continuously for several times, an alarm event will only be generated on the first time, that is, the Rising Alarm and Falling Alarm are triggered alternately for that the alarm following to Rising Alarm is certainly a Falling Alarm and vice versa.

Return to CONTENTS

Chapter 16 LLDP

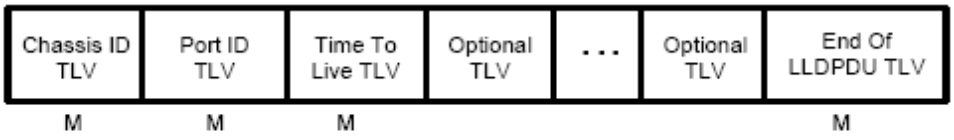
LLDP (Link Layer Discovery Protocol) is a Layer 2 protocol that is used for network devices to advertise their own device information periodically to neighbors on the same IEEE 802 local area network. The advertised information, including details such as device identification, capabilities and configuration settings, is represented in TLV (Type/Length/Value) format according to the IEEE 802.1ab standard, and these TLVs are encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit). The LLDPDU distributed via LLDP is stored by its recipients in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

An IETF Standard MIB, as well as a number of vendor specific MIBs, have been created to describe a network's physical topology and associated systems within that topology. However, there is no standard protocol for populating these MIBs or communicating this information among stations on the IEEE 802 LAN. LLDP protocol specifies a set. The device running LLDP can automatically discover and learn about the neighbors, allowing for interoperability between the network devices of different vendors. This protocol allows two systems running different network layer protocols to learn about each other.

The LLDP 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.

- **Basic Management TLV**

A set of TLVs considered to be basic to the management of the network stations are required for all LLDP implementations.

- **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.

Note:

For detailed introduction of TLV, please refer to IEEE 802.1ab standard.

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.
Max Frame Size TLV	The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

The LLDP module is mainly for LLDP function configuration of the switch, including four submenus: **Basic Config**, **Device Info, Device Statistics** and **LLDP-MED**.

16.1 Basic Config

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

16.1.1 Global Config

On this page you can configure the LLDP parameters of the device globally.

Choose the menu **LLDP** → **Basic Config** → **Global Config** to load the following page.

Figure 16-1 Global Configuration

Configuration Procedure:

Configure the global parameters here. Then click **Apply** to make the settings effective.

Entry Description:

Transmit Interval:	Indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent.
Hold Multiplier:	This parameter is a multiplier on the Transmit Interval that determines the actual TTL (Time To Live) value used in an LLDPDU. TTL = Hold Multiplier * Transmit Interval.
Reinit Delay:	Specify the delay time before LLDP is re-enabled on an interface.
Notification Interval:	Configure the interval of Trap message which will be sent from the local device to the network management system.

16.1.2 Port Config

On this page you can configure all ports' LLDP parameters.

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

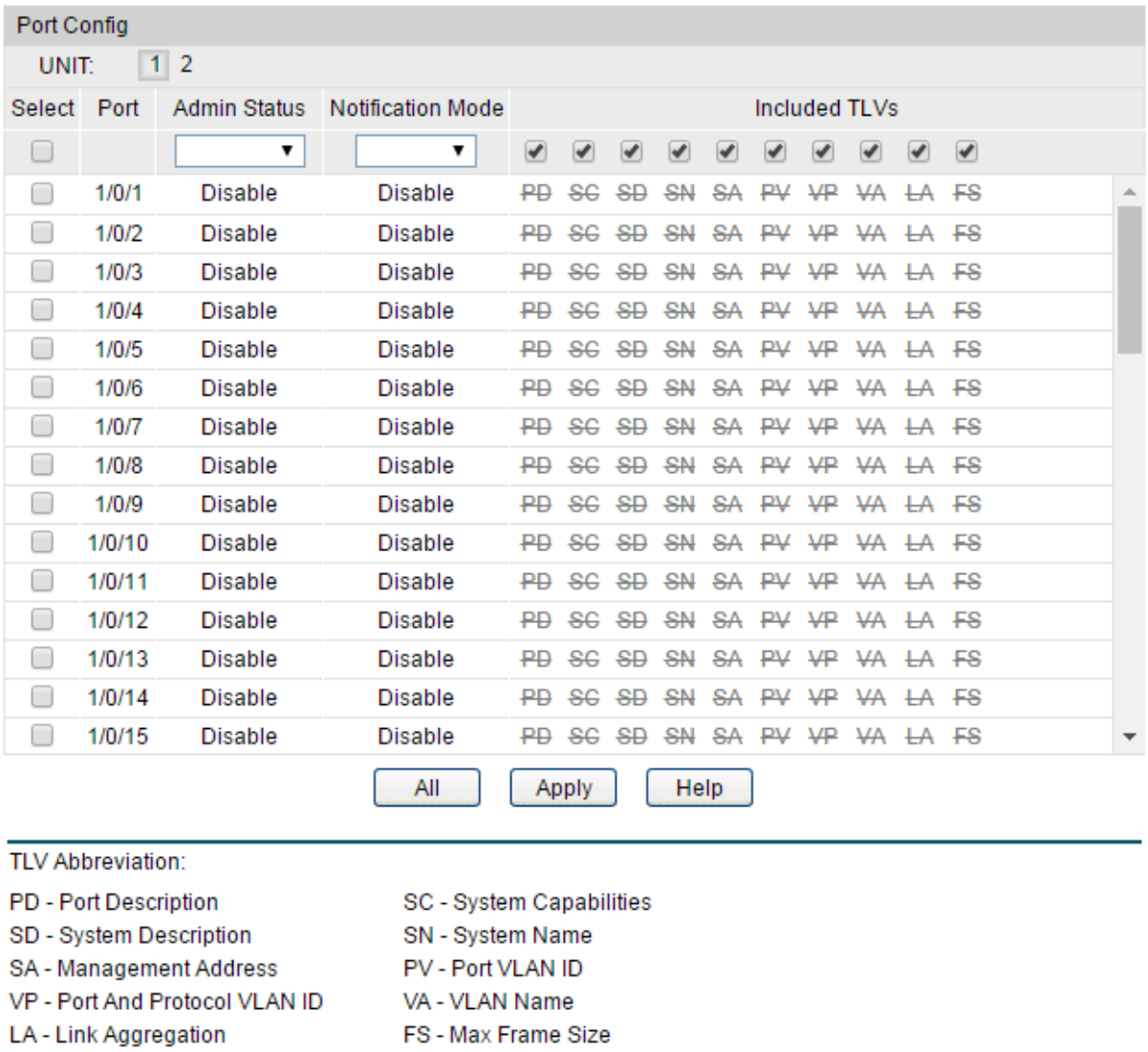


Figure 16-2 Port Configuration

Configuration Procedure:

Select your desired port and configure the relevant parameters here. Then click **Apply** to make the settings effective.

Entry Description:

UNIT:	Select the unit ID of the desired member in the stack.
Select:	Select the desired entry for configuration. It is multi-optional.
Port:	Displays the port number to be configured.
Admin Status:	Configure the ports' LLDP state.
Notification Mode:	Enable or disable the ports' SNMP notification.
Included TLVs:	Select TLVs to be included in outgoing LLDPDU. By default, no TLVs are included.

16.2 Device Info

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

16.2.1 Local Info

On this page you can view all ports' configuration and system information.

Choose the menu **LLDP** → **Device Info** → **Local Info** to load the following page.

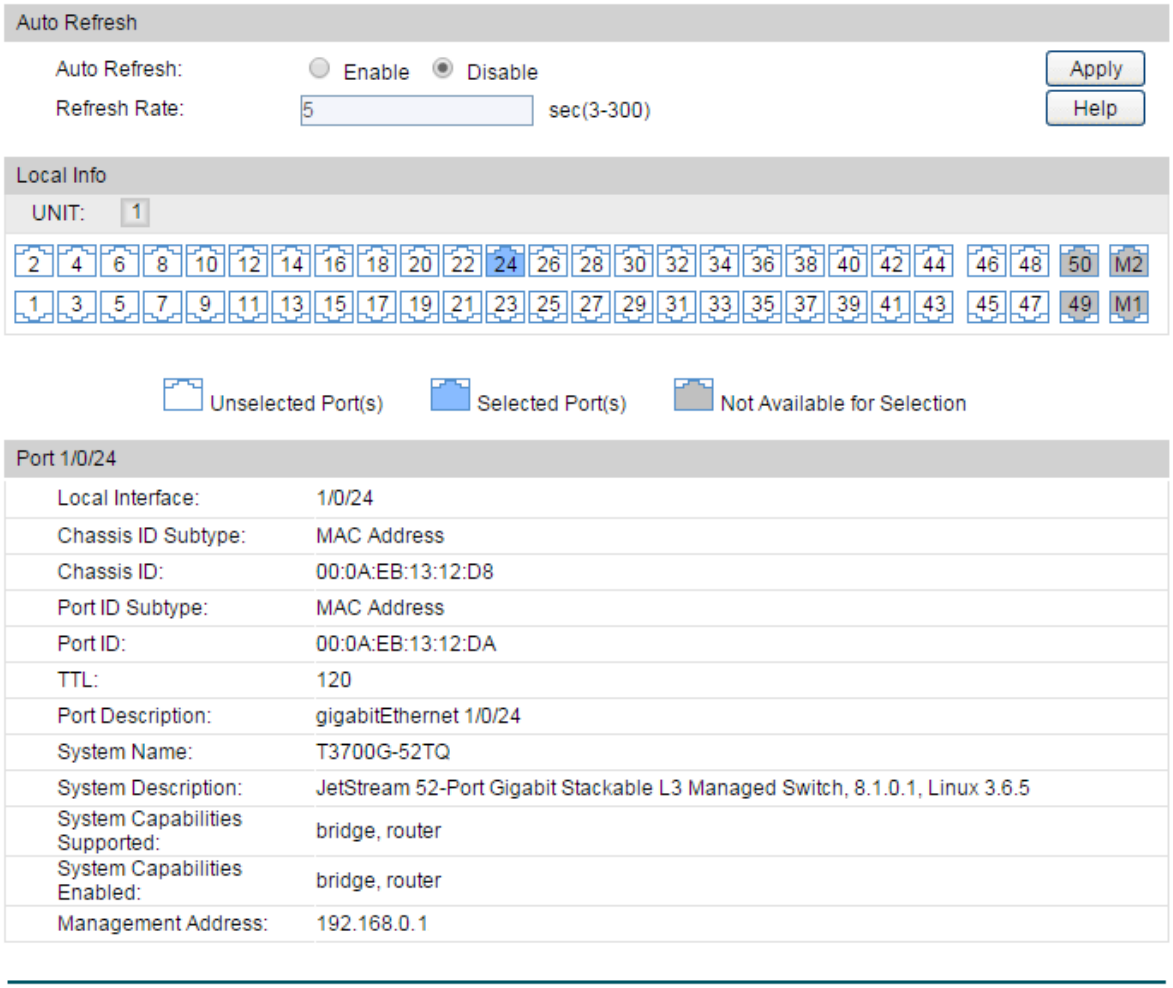


Figure 16-3 Local Information

Configuration Procedure:

1) Choose Enable or Disable **Auto Refresh** according to your needs.

2) Select the desired port to view the information of the corresponding port under the Local Info.

Entry Description:

Auto Refresh:	Enable/Disable the auto refresh function.
Refresh Rate:	Configure the auto refresh rate.
UNIT:	Select the unit ID of the desired member in the stack.

Local Interface:	Displays the local port number.
Chassis ID Subtype：	Indicates the basis for the chassis ID, and the default subtype is MAC address.
Chassis ID：	Indicates the specific identifier for the particular chassis in local device.
Port ID Subtype：	Indicates the basis for the port ID, and the default subtype is interface name.
Port ID：	Indicates the specific identifier for the port in local device.
TTL:	Indicates 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：	Displays local port's description.
System Name：	Indicates local device's administratively assigned name.
System Description：	Displays local device's system description.
System Capabilities Supported：	Displays the supported function of the local device.
System Capabilities Enabled：	Displays the primary function of the local device.
Management Address：	Displays the particular management address associated with local device.

16.2.2 Neighbor Info

On this page you can view the information of the neighbors.

Choose the menu **LLDP** → **Device Info** → **Neighbor Info** to load the following page.

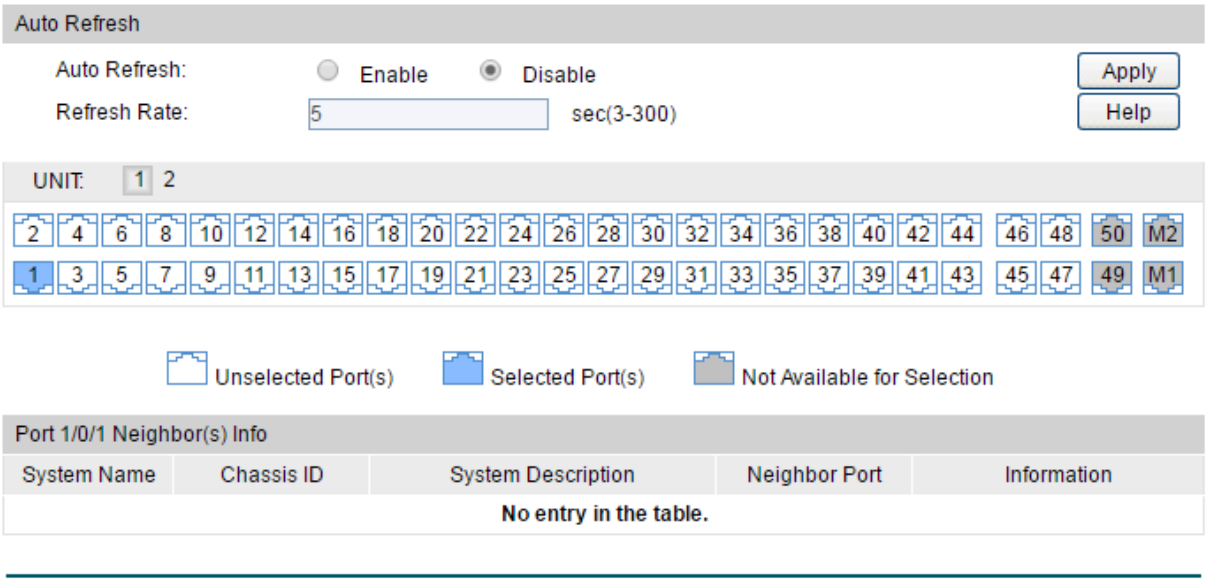


Figure 16-4 Neighbor Information

Configuration Procedure:

1) Choose Enable or Disable **Auto Refresh** according to your needs.

2) Select the desired port to view the information of neighbor connected to the corresponding port.

Entry Description:

Auto Refresh:	Enable/Disable the auto refresh function.
Refresh Rate:	Configure the auto refresh rate.
UNIT:	Select the unit ID of the desired member in the stack.
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.
Neighbor Port:	Displays the port number of the neighbor linking to local port.
Information:	Click to display the detail information of the neighbor.

16.3 Device Statistics

You can view the LLDP statistics of local device through this feature.

Choose the menu **LLDP** → **Device Statistics** → **Statistic Info** to load the following page.

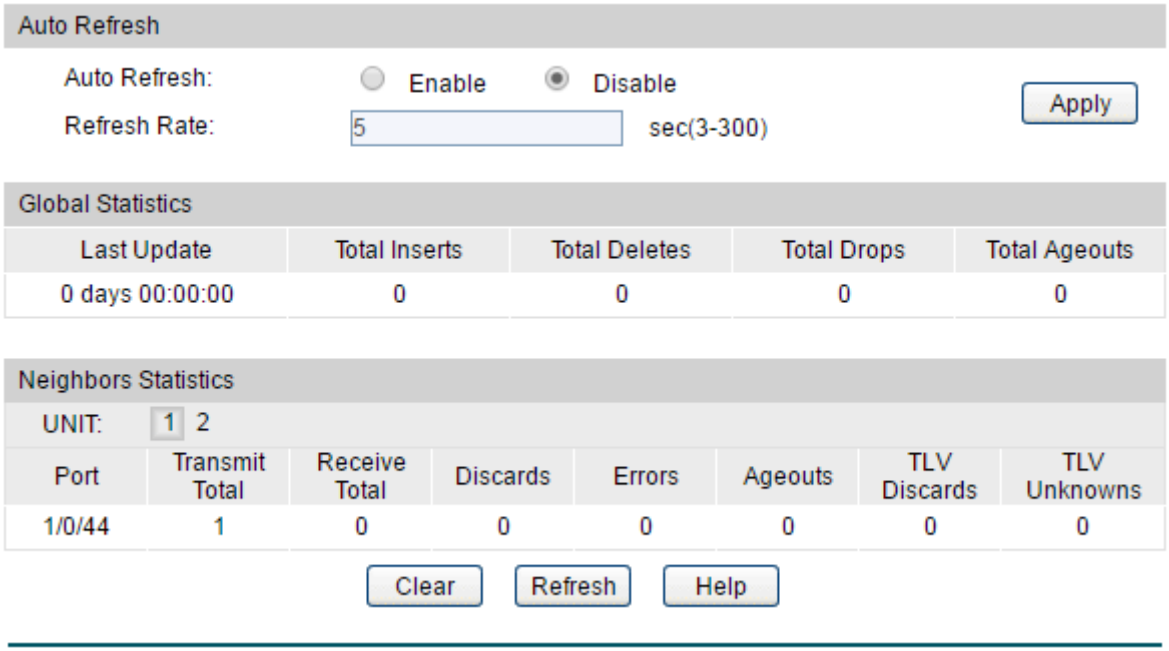


Figure 16-5 Device Statistics

Configuration Procedure:

1) Choose Enable or Disable **Auto Refresh** according to your needs.

2) View **Global Statistics** and **Neighbors Statistics** in the corresponding table.

Entry Description:

Auto Refresh:	Enable/Disable the auto refresh function.
Refresh Rate:	Configure the auto refresh rate.
Last Update:	Display latest update time of the statistics.
Total Inserts:	Display the number of neighbors during latest 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.
UNIT:	Select the unit ID of the desired member in the stack.
Port:	Display local device's port number.
Transmit Total:	Displays the number of LLDPDUs sent by this port.
Receive Total:	Displays the number of LLDPDUs received by this port.
Discards:	Displays the number of LLDPDUs discarded by this port.
Errors:	Displays the number of error LLDPDUs received by this port.
Ageouts:	Displays the number of overtime neighbors linking to this port.
TLV Discards:	Displays the number of TLVs dropped by this port.
TLV Unknowns:	Displays the number of unknown TLVs received by this port.

16.4 LLDP-MED

LLDP-MED is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy and inventory management.

- **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.
Inventory TLV	The Inventory TLV set contains seven basic Inventory management TLVs, that is, Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV and Asset ID TLV. If support for any of the TLVs in the Inventory Management set is implemented, then support for all Inventory Management TLVs shall be implemented.

LLDP-MED is configured on the **Global Config**, **Port Config**, **Local Info** and **Neighbor Info** pages.

16.4.1 Global Config

On this page you can configure the LLDP-MED parameters of the device globally.

Choose the menu **LLDP** → **LLDP-MED** → **Global Config** to load the following page.

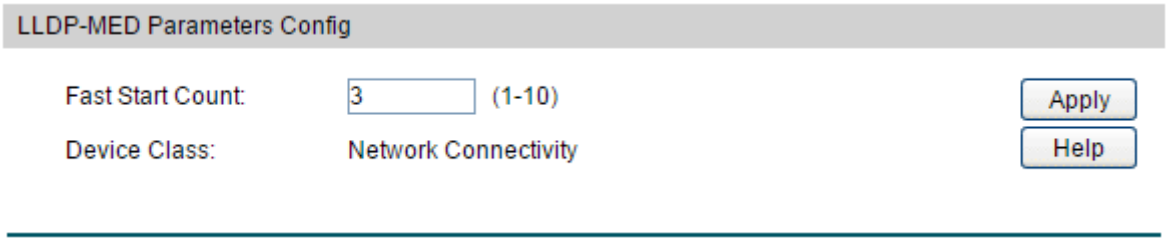


Figure 16-6 LLDP-MED Global Configuration

Configuration Procedure:

1) Configure the number of LLDP-MED frames which will be transmitted fast.

2) View Device Class of the device.

Entry Description:

Fast Start Count: When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted (the number of frames equals this parameter).

LLDP-MED fast start mechanism will be activated when LLDP-MED status changes from disable to enable. The device will transmit a specified number of LLDP-MED frames fast then the transmit interval will return to normal.

Device Class: LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices. In turn, Endpoint Devices are composed of three defined Classes: Class I, Class II and Class III. Bridge is a Network Connectivity Device.

16.4.2 Port Config

On this page you can configure all ports' LLDP-MED parameters.

Choose the menu **LLDP** → **LLDP-MED** → **Port Config** to load the following page.

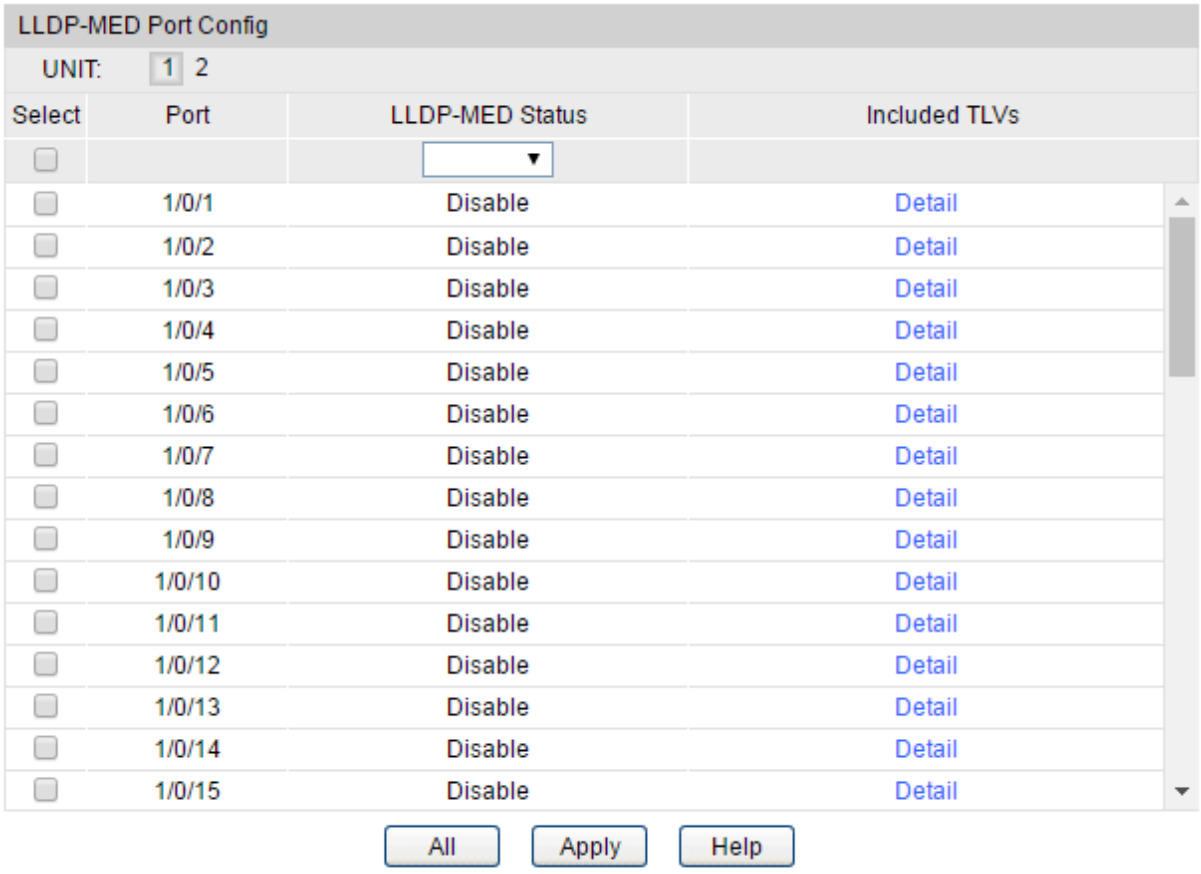


Figure 16-7 LLDP-MED Port Configuration

Configuration Procedure:

1) Select your desired port and enable LLDP-MED. Then click **Apply** to make the settings effective.

2) Click **Detail** to configure the included TLVs in outgoing LLDPDU on the following page.

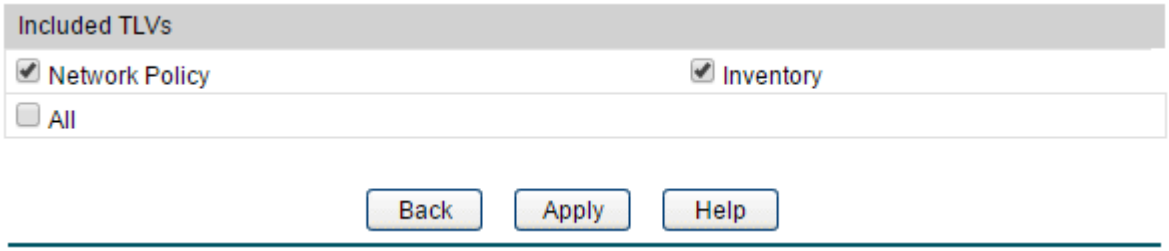


Figure 16-8 Configure TLVs of LLDP-MED Port

Entry Description:

UNIT: Select the unit ID of the desired member in the stack.

Select: Select the desired port to configure.

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.

Click the **Detail** button to display the included TLVs and select the desired TLVs.

16.4.3 Local Info

On this page you can view all ports' LLDP-MED configuration.

Choose the menu **LLDP** → **LLDP-MED** → **Local Info** to load the following page.

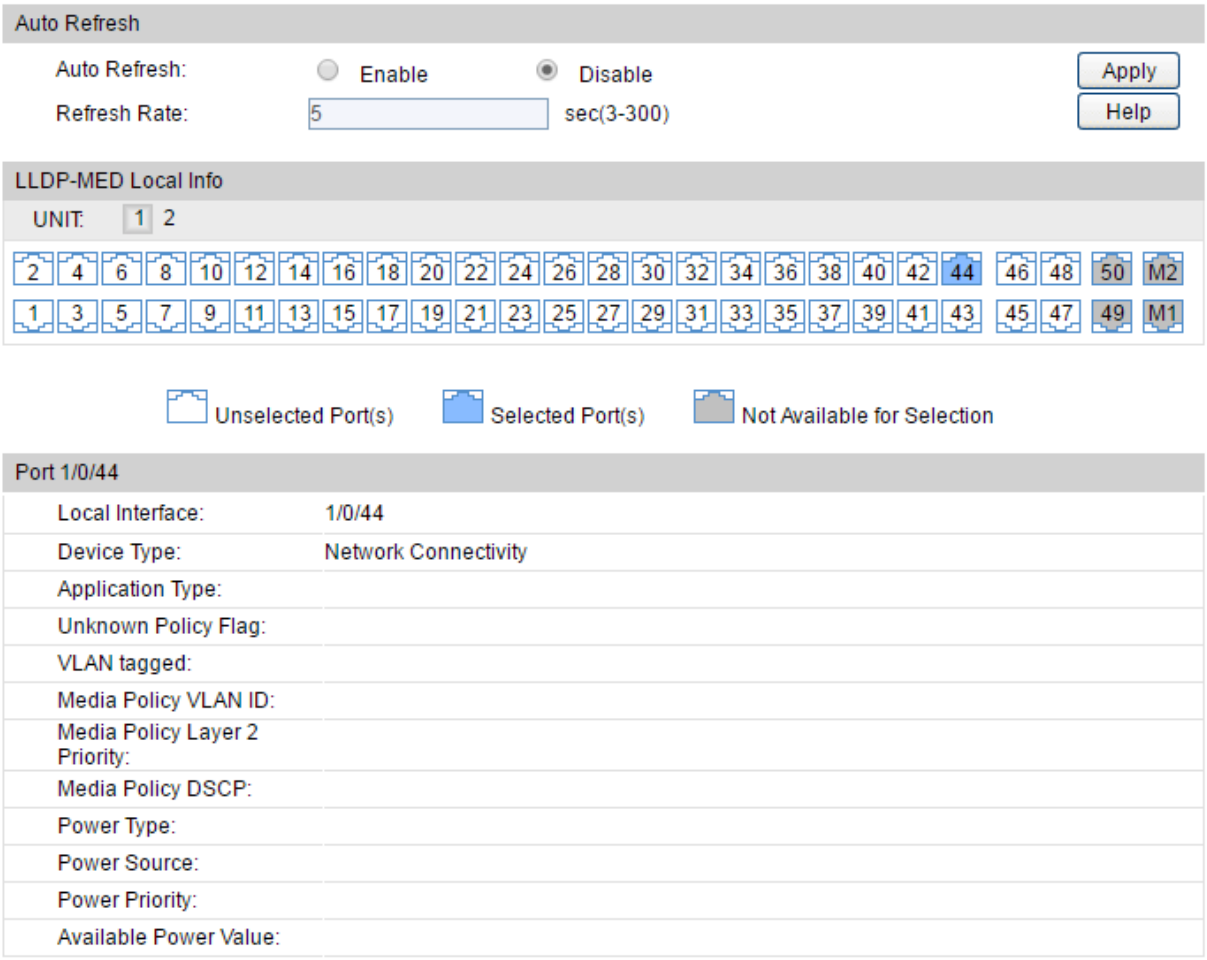


Figure 16-9 LLDP-MED Local Information

Configuration Procedure:

1) Choose Enable or Disable Auto Refresh according to your needs.

2) Select the desired port to view the local information of the corresponding port under the LLDP-MED Local Info.

Entry Description:

Auto Refresh: Enable/Disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

Local Interface: Enable/Disable the auto refresh function.

Device Type:	Specify the auto refresh rate.
Application Type:	Application Type indicates the primary function of the applications defined for the network policy.
Unknown Policy Flag:	Displays whether the local device will explicitly advertise the policy required by the device but currently unknown.
VLAN tagged:	Indicates the VLAN type the specified application type is using, 'tagged' or 'untagged'.
Media Policy VLAN ID:	Displays the application (eg. Voice VLAN) VLAN identifier (VID) for the port.
Media Policy Layer 2 Priority:	Displays the Layer 2 priority to be used for the specified application type.
Media Policy DSCP:	Displays the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474.
Power Source:	Displays the power source being utilized by a PSE or PD device.
Power Priority:	Power Priority represents the priority of the PD type device to the power being supplied by the PSE type device, or the power priority associated with the PSE type device's port that is sourcing the power via MDI.
Available Power Value:	Indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

16.4.4 Neighbor Info

On this page you can get the LLDP-MED information of the neighbors.

Choose the menu **LLDP** → **LLDP-MED** → **Neighbor Info** to load the following page.

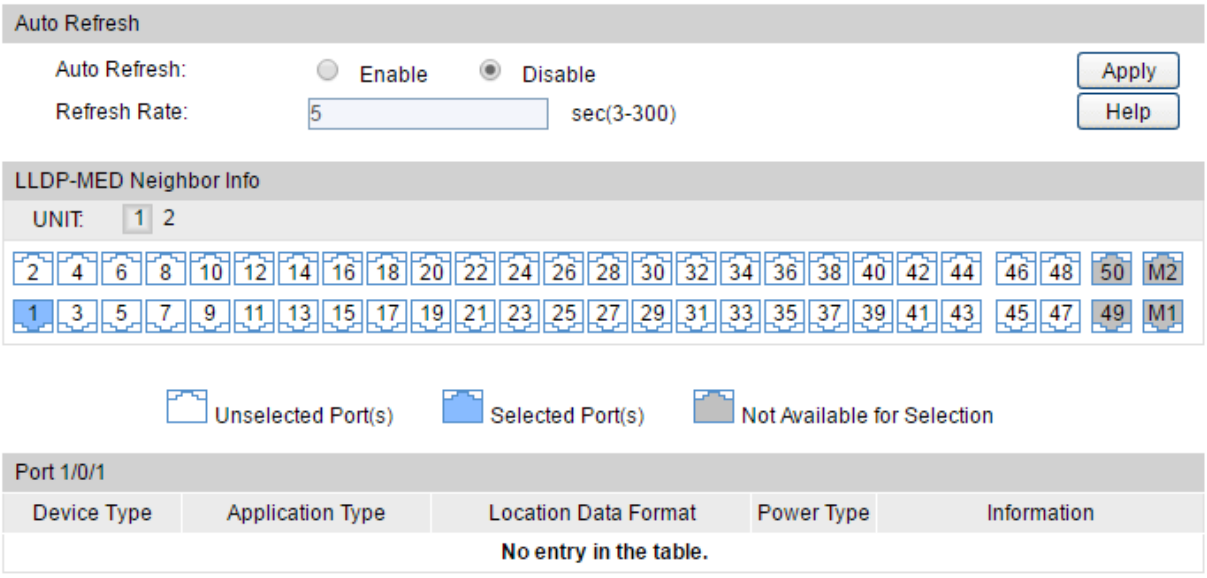


Figure 16-10 LLDP-MED Neighbor Information

Configuration Procedure:

1) Choose Enable or Disable **Auto Refresh** according to your needs.

2) Select the desired port to view the information of neighbor connected to the corresponding port under the LLDP-MED Neighbor Info.

Entry Description:

Auto Refresh:	Enable/Disable the auto refresh function.
Refresh Rate:	Specify the auto refresh rate.
Unit:	Select the unit ID of the desired member in the stack.
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, either Power Sourcing Entity (PSE) or Powered Device (PD).
Information:	Click the **Information** button to display the detailed information of the corresponding neighbor.

Return to CONTENTS

Chapter 17 Maintenance

Maintenance module, assembling the commonly used system tools to manage the switch, provides the convenient method to locate and solve the network problem.

(1) System Monitor: Monitor the utilization status of the memory and the CPU of switch.

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

(3) Device Diagnose: Cable Test tests the connection status of the cable to locate and diagnose the trouble spot of the network.

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

17.1 System Monitor

System Monitor functions to display the utilization status of the memory and the CPU of switch via the data graph. The CPU utilization rate and the memory utilization rate should fluctuate stably around a specific value. If the CPU utilization rate or the memory utilization rate increases markedly, please detect whether the network is being attacked.

The **System Monitor** function is implemented on the **CPU Monitor** and **Memory Monitor** pages.

17.1.1 CPU Monitor

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

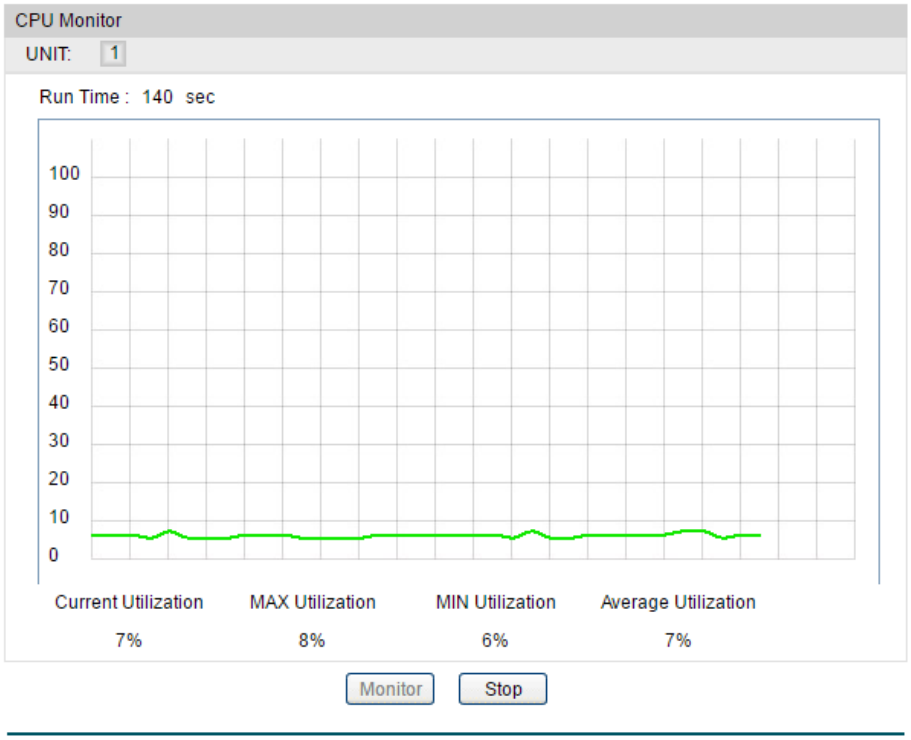


Figure17-1 CPU Monitor

UNIT: Select the unit ID of the desired member in the stack.

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

17.1.2 Memory Monitor

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

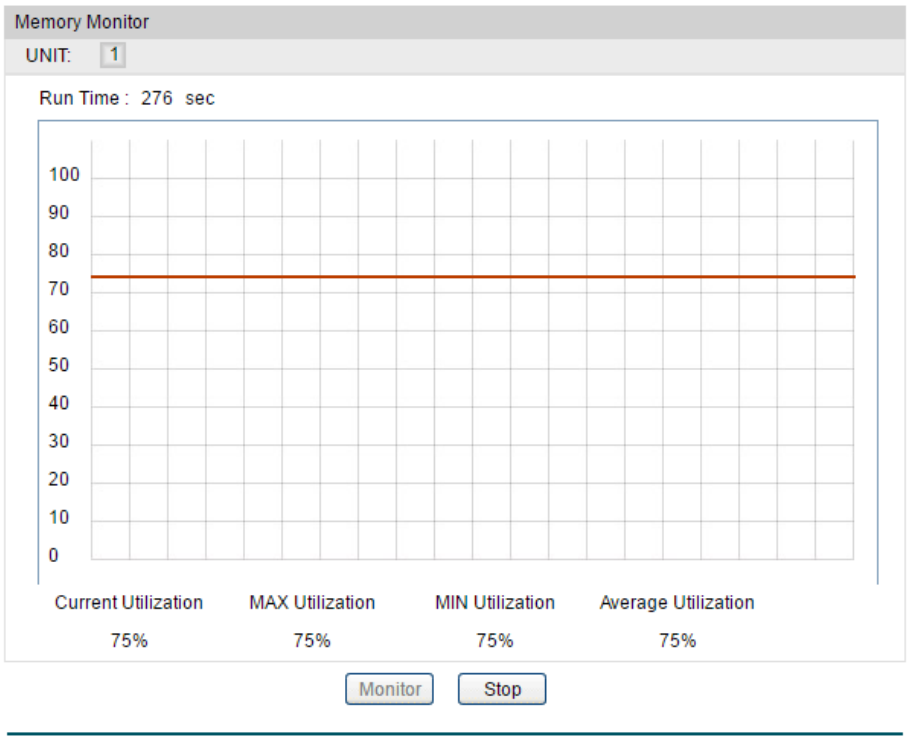


Figure17-2 Memory Monitor

UNIT: Select the unit ID of the desired member in the stack.

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

17.2 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

Severity	Level	Description
errors	3	Error conditions
warnings	4	Warnings conditions
notifications	5	Normal but significant conditions
informational	6	Informational messages
debugging	7	Debug-level messages

Table 17-1 Log Level

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

17.2.1 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.

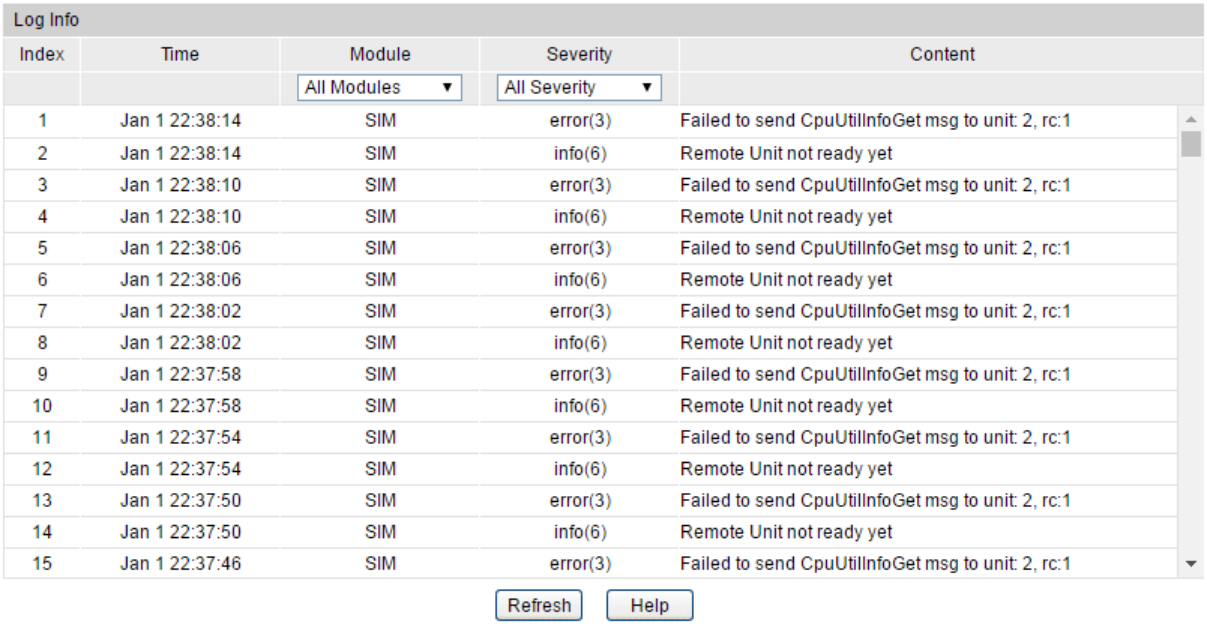


Figure17-3 Log Table

Configuration Procedure:

Select a module and a severity to view the corresponding log information.

Entry Description:

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:

1. There are 8 severity levels marked with value 0-7. The smaller value has the higher priority.
2. This page displays logs in the log buffer, and at most 1024 logs are displayed.

17.2.2 Local Log

Local Log is the log information saved in switch. By default, all system logs are saved in log buffer and the function of saving logs to the log file in the flash is disabled. On this page, you can set the output channel for logs.

Choose the menu **Maintenance** → **Log** → **Local Log** to load the following page.

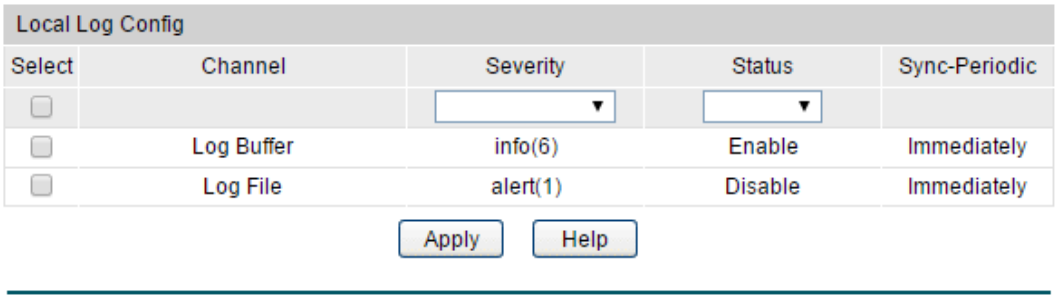


Figure17-4 Local Log

Configuration Procedure:

1) Select your desired channel and configure the corresponding severity and status.
2) Click **Apply** to make the settings effective.

Entry Description:

Channel:	Local log includes 2 channels: log buffer and log file. Log buffer indicates the RAM for saving system log. The channel is enabled by default. The information in the log buffer is displayed on the **Maintenance > Log> 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 **Maintenance > Log> 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 or disable the channel.
Sync-Periodic	Specify how frequent the log information would be synchronized to the log file.

17.2.3 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.

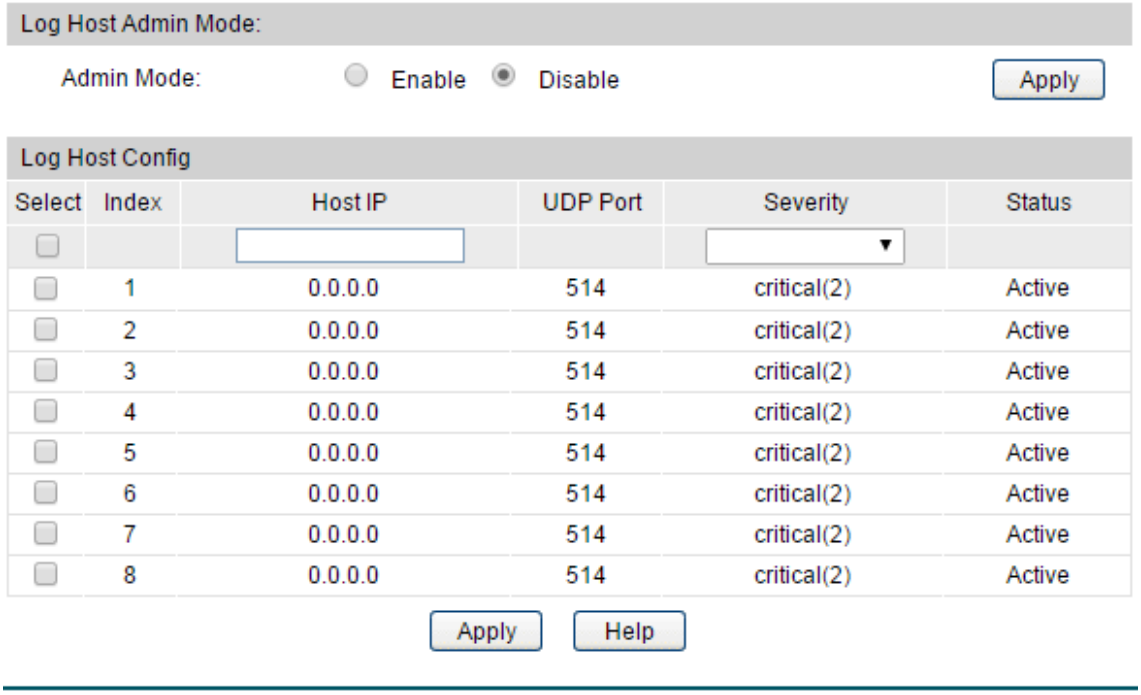


Figure17-5 Log Host

Configuration Procedure:

Select an entry to enable the status, and then set the host IP address and severity. Click **Apply** to make the settings effective.

Entry Description:

Admin Mode:	Enable or disable the log host. While enabled, syslog packets will be sent to the hosts. While disabled, no syslog packets will be sent to the hosts.
Index:	Displays the index of the log host. The switch supports 8 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:	Displays the status of the corresponding log host.

Note:

The Log Server software is not provided. If necessary, please download it on the Internet.

17.2.4 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.

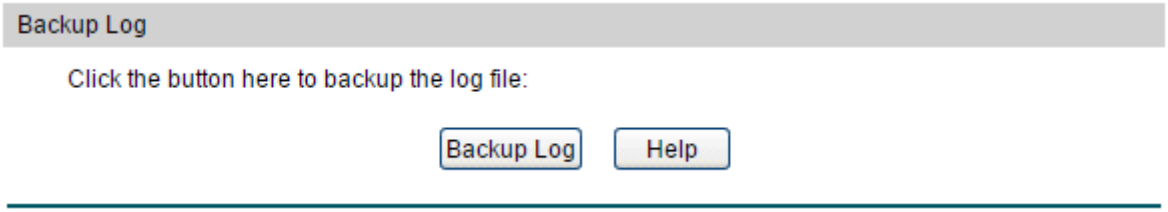


Figure17-6 Backup Log

Configuration Procedure:

Click **Backup Log** to save the system log as a file on your computer. If the switch system breaks down, you can check the file for troubleshooting.

Entry Description:

Backup Log: Click the **Backup Log** button to save the log as a file to your computer.

Note:

1. When a critical error results in the breakdown of the system, you can export the log file to get some related important information about the error for device diagnosis after the switch is restarted.
2. It will take a few minutes to backup the log file. Please wait without any operation.

17.3 Device Diagnose

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

17.3.1 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 Diagnose** → **Cable Test** to load the following page.

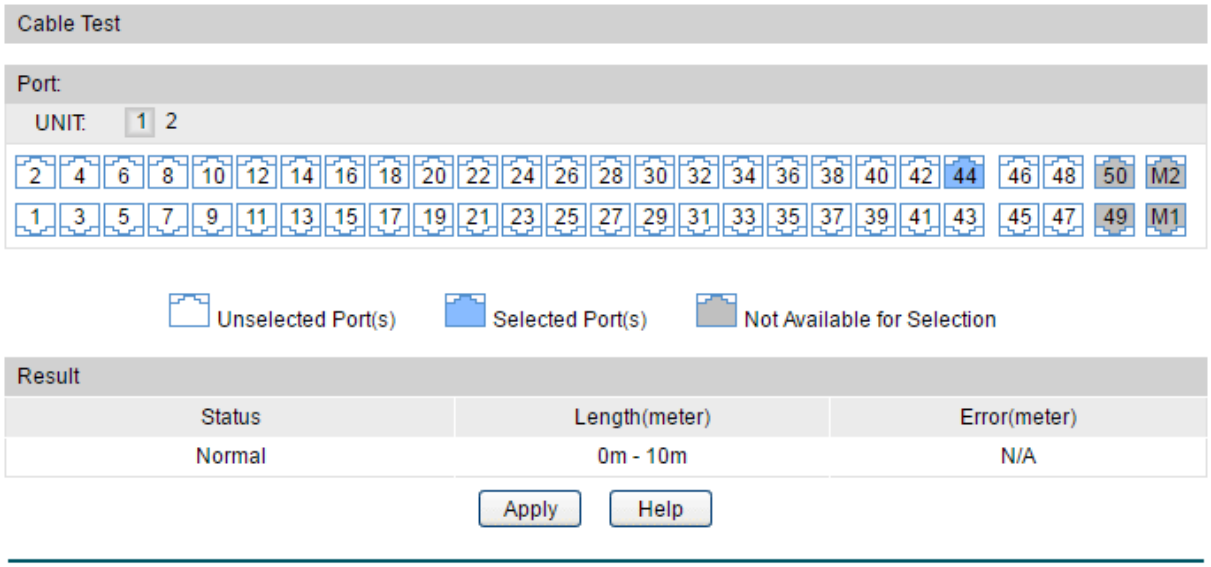


Figure17-7 Cable Test

Configuration Procedure:

1) In the **Port** section, select your desired port for the test.
2) In the **Result** section, click **Apply** and check the test results.

Entry Description:

Port: Select the port for cable testing.

UNIT: Select the unit ID of the desired member in the stack.

Status: Test the connection status of the cable connected to the port.

Length: If the connection status is normal, here displays the length range of the cable.

Error: If the connection status is short, close or crosstalk, here displays the length from the port to the trouble spot. The value makes sense only when the cable is longer than 30m.

Note:

1. The interval between two cable tests for one port must be more than 3 seconds.
2. The result is more reasonable when the cable pair is in the open status.
3. The test result is just for your information.
4. If the port is 100Mbps and its connection status is normal, cable test cannot get the length of the cable.

17.4 Network Diagnose

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

17.4.1 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 Diagnose** → **Ping** to load the following page.

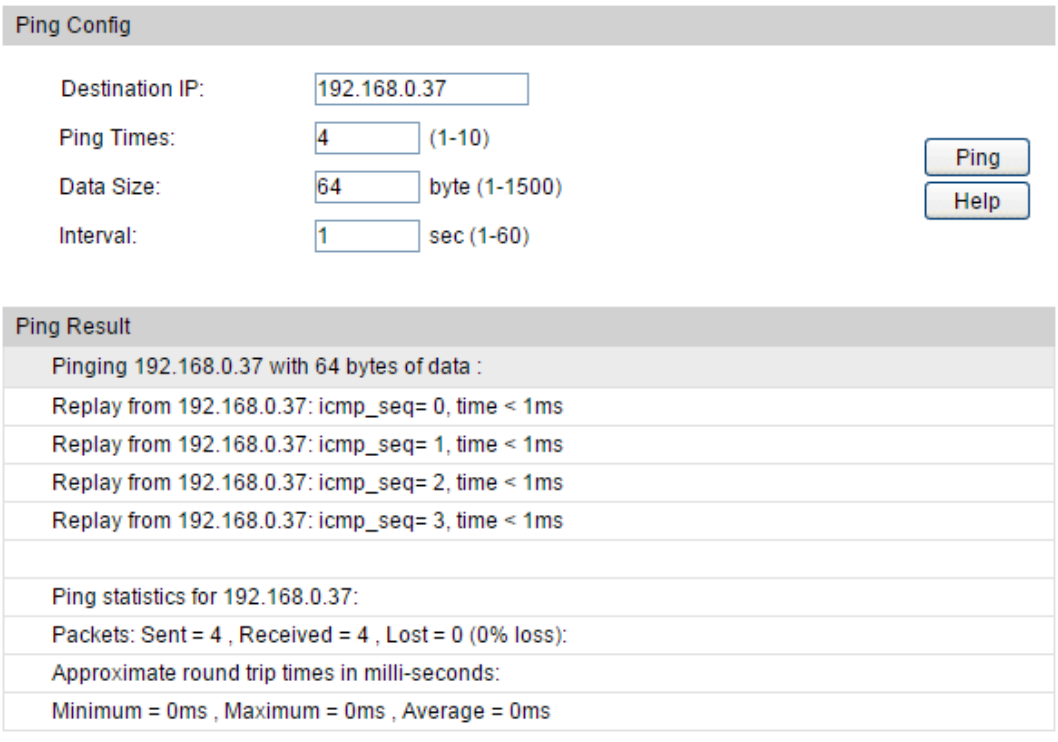


Figure17-8 Ping

Configuration Procedure:

1) In the **Ping Config** section, enter the IP address of the destination device for Ping test, set Ping times, data size and interval according to your needs, and then click Ping to start the test.

2) In the **Ping Result** section, check the test results.

Entry Description:

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.

17.4.2 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 Diagnose** → **Tracert** to load the following page.

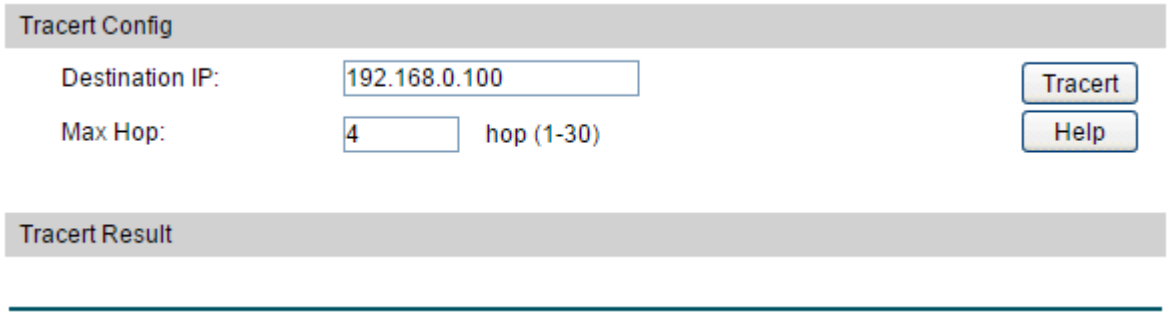


Figure17-9 Tracert

Configuration Procedure:

1) In the **Tracert Config** section, enter the IP address of the destination, set the max hop, and then click **Tracert** to start the test.

2) In the **Tracert Result** section, check the test results.

Entry Description:

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: Glossary

Access Control List (ACL)
ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

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.

Extensible Authentication Protocol over LAN (EAPOL)
EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)
Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)
The GARP provides a generic attribute dissemination capability that is used by participants in GARP Applications (GARP Participants) to register and de-register attribute values with other GARP Participants within a Bridged LAN. The definition of the attribute types, the values that they can carry, and the semantics that are associated with those values when registered, are specific to the operation of the GARP Application concerned.

Generic Multicast Registration Protocol (GMRP)
GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)
See Generic Attribute Registration Protocol.

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 802.1X
Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

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 acts as 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 for which 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.

Link Aggregation Control Protocol (LACP)
Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

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-member configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Port Authentication
See IEEE 802.1X.

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.

Secure Shell (SSH)
A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

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