



User Guide

T2500G-10TS (TL-SG3210)

1910012119 REV1.1.0

May 2017

CONTENTS

Package Contents	1
Chapter 1 About This Guide	2
1.1 Intended Readers.....	2
1.2 Conventions.....	2
1.3 Overview of This Guide	3
Chapter 2 Introduction.....	7
2.1 Overview of the Switch	7
2.2 Appearance Description.....	7
2.2.1 Front Panel	7
2.2.2 Rear Panel.....	8
Chapter 3 Login to the Switch	9
3.1 Login.....	9
3.2 Configuration.....	9
Chapter 4 System	11
4.1 System Info	11
4.1.1 System Summary.....	11
4.1.2 Device Description.....	13
4.1.3 System Time.....	13
4.1.4 Daylight Saving Time	14
4.1.5 System IP	16
4.1.6 System IPv6	17
4.2 User Management	26
4.2.1 User Table.....	26
4.2.2 User Config	26
4.3 System Tools.....	28
4.3.1 Boot Config	28
4.3.2 Config Restore	28
4.3.3 Config Backup.....	29
4.3.4 Firmware Upgrade	29
4.3.5 System Reboot	30
4.3.6 System Reset	30
4.4 Access Security.....	31

4.4.1	Access Control	31
4.4.2	HTTP Config.....	32
4.4.3	HTTPS Config.....	33
4.4.4	SSH Config.....	36
4.4.5	Telnet Config.....	42
Chapter 5	Switching.....	43
5.1	Port.....	43
5.1.1	Port Config	43
5.1.2	Port Mirror	44
5.1.3	Port Security.....	46
5.1.4	Port Isolation.....	48
5.1.5	Loopback Detection	49
5.2	LAG.....	51
5.2.1	LAG Table	51
5.2.2	Static LAG.....	53
5.2.3	LACP Config	54
5.3	Traffic Monitor.....	55
5.3.1	Traffic Summary	55
5.3.2	Traffic Statistics	56
5.4	MAC Address.....	58
5.4.1	Address Table	59
5.4.2	Static Address.....	60
5.4.3	Dynamic Address.....	61
5.4.4	Filtering Address	63
5.5	L2PT.....	64
5.5.1	L2PT Config	65
Chapter 6	VLAN.....	67
6.1	802.1Q VLAN	68
6.1.1	VLAN Config	70
6.1.2	Port Config	72
6.2	MAC VLAN.....	74
6.2.1	MAC VLAN.....	74
6.3	Protocol VLAN.....	76
6.3.1	Protocol Group Table	76

6.3.2	Protocol Group	77
6.3.3	Protocol Template.....	78
6.4	Application Example for 802.1Q VLAN.....	79
6.5	Application Example for MAC VLAN.....	80
6.6	Application Example for Protocol VLAN	82
6.7	VLAN VPN.....	84
6.7.1	VPN Config.....	85
6.7.2	VLAN Mapping	87
6.8	GVRP.....	88
Chapter 7	Spanning Tree	92
7.1	STP Config.....	97
7.1.1	STP Config.....	97
7.1.2	STP Summary.....	99
7.2	Port Config	99
7.3	MSTP Instance.....	101
7.3.1	Region Config.....	102
7.3.2	Instance Config.....	102
7.3.3	Instance Port Config.....	104
7.4	STP Security	105
7.4.1	Port Protect.....	106
7.4.2	TC Protect	108
7.5	Application Example for STP Function	108
Chapter 8	DHCP	113
8.1	DHCP Relay	117
8.1.1	Global Config.....	120
8.1.2	DHCP VLAN Relay.....	121
Chapter 9	Multicast.....	122
9.1	IGMP Snooping	126
9.1.1	Snooping Config	128
9.1.2	VLAN Config	129
9.1.3	Port Config	130
9.1.4	IP-Range.....	132
9.1.5	Multicast VLAN	133
9.1.6	Static Multicast IP	136

9.1.7	IGMP Snooping Querier	137
9.1.8	Packet Statistics	139
9.1.9	IGMP Authentication.....	141
9.2	MLD Snooping.....	142
9.2.1	Global Config.....	144
9.2.2	VLAN Config	145
9.2.3	Filter Config.....	146
9.2.4	Port Config	147
9.2.5	Static Multicast.....	148
9.2.6	Querier Config.....	149
9.2.7	Packet Statistics	150
9.3	Multicast Table.....	152
9.3.1	IPv4 Multicast Table	152
9.3.2	IPv6 Multicast Table	153
Chapter 10	QoS.....	154
10.1	DiffServ.....	157
10.1.1	Port Priority	157
10.1.2	DSCP Priority.....	158
10.1.3	802.1P/CoS Mapping.....	160
10.1.4	Schedule Mode.....	161
10.2	Bandwidth Control	162
10.2.1	Rate Limit	162
10.2.2	Storm Control.....	163
10.3	Voice VLAN	165
10.3.1	Global Config.....	167
10.3.2	Port Config	168
10.3.3	OUI Config.....	169
Chapter 11	ACL.....	171
11.1	Time-Range.....	171
11.1.1	Time-Range Summary.....	171
11.1.2	Time-Range Create	172
11.1.3	Holiday Config.....	173
11.2	ACL Config	174
11.2.1	ACL Summary	174

11.2.2	ACL Create.....	174
11.2.3	MAC ACL.....	175
11.2.4	Standard-IP ACL.....	176
11.2.5	Extend-IP ACL.....	177
11.3	Policy Config.....	178
11.3.1	Policy Summary.....	178
11.3.2	Policy Create	179
11.3.3	Action Create	180
11.4	Policy Binding.....	181
11.4.1	Binding Table.....	181
11.4.2	Port Binding.....	182
11.4.3	VLAN Binding.....	182
11.5	Application Example for ACL	183
Chapter 12 Network Security.....		186
12.1	IP-MAC Binding.....	186
12.1.1	Binding Table.....	186
12.1.2	Manual Binding.....	188
12.1.3	ARP Scanning.....	189
12.2	DHCP Snooping.....	191
12.2.1	DHCP Snooping.....	194
12.2.2	Option 82	195
12.3	ARP Inspection.....	197
12.3.1	ARP Detect.....	201
12.3.2	ARP Defend.....	202
12.3.3	ARP Statistics.....	203
12.4	DoS Defend.....	204
12.4.1	DoS Defend.....	205
12.5	802.1X.....	206
12.5.1	Global Config.....	210
12.5.2	Port Config	212
12.6	AAA.....	215
12.6.1	Global Config.....	216
12.6.2	Privilege Elevation	216
12.6.3	RADIUS Server Config.....	216

12.6.4	TACACS+ Server Config	217
12.6.5	Authentication Server Group Config.....	218
12.6.6	Authentication Method List Config.....	220
12.6.7	Application Authentication List Config.....	221
12.6.8	802.1X Authentication Server Config.....	222
12.6.9	Default Settings.....	223
12.7	PPPoE.....	224
Chapter 13SNMP.....		227
13.1	SNMP Config	229
13.1.1	Global Config.....	229
13.1.2	SNMP View	230
13.1.3	SNMP Group	231
13.1.4	SNMP User	233
13.1.5	SNMP Community.....	234
13.2	Notification.....	237
13.2.1	Notification Config.....	237
13.3	RMON.....	239
13.3.1	History Control.....	240
13.3.2	Event Config	241
13.3.3	Alarm Config.....	242
Chapter 14LLDP.....		244
14.1	Basic Config.....	248
14.1.1	Global Config.....	248
14.1.2	Port Config.....	249
14.2	Device Info.....	250
14.2.1	Local Info	250
14.2.2	Neighbor Info.....	251
14.3	Device Statistics.....	252
14.4	LLDP-MED	253
14.4.1	Global Config.....	254
14.4.2	Port Config	255
14.4.3	Local Info	257
14.4.4	Neighbor Info.....	258
Chapter 15Maintenance.....		260

15.1	System Monitor	260
15.1.1	CPU Monitor.....	260
15.1.2	Memory Monitor	261
15.2	Log	262
15.2.1	Log Table	263
15.2.2	Local Log	264
15.2.3	Remote Log.....	265
15.2.4	Backup Log	265
15.3	Device Diagnostics.....	266
15.4	Network Diagnostics.....	267
15.4.1	Ping	267
15.4.2	Tracert	268
15.5	DLDP.....	269
	Appendix A: Glossary	273

Package Contents

The following items should be found in your box:

- One T2500G-10TS switch
- One power cord
- One console cable
- One USB cable
- Two mounting brackets and other fittings
- Installation Guide
- Resource CD for T2500G-10TS switch, including:
 - This User Guide
 - The CLI Reference Guide
 - SNMP Mibs
 - 802.1X Client Software
 - 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 T2500G-10TS 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 T2500G-10TS mentioned in this Guide stands for T2500G-10TS JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots without any explanation.
- **Menu Name**→**Submenu Name**→**Tab page** indicates the menu structure. **System**→**System Info**→**System Summary** means the System Summary page under the System Info menu option that is located under the System menu.
- **Bold font** indicates a button, a toolbar icon, menu or menu item.

Symbols in this Guide:

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

More Info:

- The 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 T2500G-10TS switch.
Chapter 3 Login to the switch	Introduces how to log on to T2500G-10TS Web management page.
Chapter 4 System	<p>This module is used to configure system properties of the switch. Here mainly introduces:</p> <ul style="list-style-type: none"> ● System Info: Configure the description, system time and network parameters of the switch. ● User Management: Configure the user name and password for users to log on to the Web management page with a certain access level. ● System Tools: Manage the configuration file of the switch. ● Access Security: Provide different security measures for the login to enhance the configuration management security.
Chapter 5 Switching	<p>This module is used to configure basic functions of the switch. Here mainly introduces:</p> <ul style="list-style-type: none"> ● 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. ● L2PT: Configure the Layer 2 Protocol Tunneling feature.

Chapter	Introduction
Chapter 6 VLAN	<p>This module is used to configure VLANs to control broadcast in LANs. Here mainly introduces:</p> <ul style="list-style-type: none"> ● 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.
Chapter 7 Spanning Tree	<p>This module is used to configure spanning tree function of the switch. Here mainly introduces:</p> <ul style="list-style-type: none"> ● STP Config: Configure and view the global settings of spanning tree function. ● Port Config: Configure CIST parameters of ports. ● MSTP Instance: Configure MSTP instances. ● STP Security: Configure protection function to prevent devices from any malicious attack against STP features.
Chapter 8 DHCP	<p>This module is used to configure DHCP function of the switch. The switch can work as DHCP relay, and here mainly introduces DHCP relay function.</p> <ul style="list-style-type: none"> ● Global Config: Enable DHCP Relay and configure Option 82. ● DHCP VLAN Relay: Specify DHCP server for the VLAN.
Chapter 9 Multicast	<p>This module is used to configure multicast function of the switch. Here mainly introduces:</p> <ul style="list-style-type: none"> ● IGMP Snooping: Configure global parameters of IGMP Snooping function, port properties, VLAN and multicast VLAN. ● MLD Snooping: Configure global parameters of MLD Snooping function, port properties, VLAN and multicast VLAN. ● Multicast Table: View the information of IPv4 and IPv6 multicast groups already on the switch.

Chapter	Introduction
Chapter 10 QoS	<p>This module is used to configure QoS function to provide different quality of service for various network applications and requirements. Here mainly introduces:</p> <ul style="list-style-type: none"> ● DiffServ: Configure priorities, port priority, 802.1P priority and DSCP priority. ● Bandwidth Control: Configure rate limit feature to control the traffic rate on each port; configure storm control feature to filter broadcast, multicast and UL frame in the network. ● Voice VLAN: Configure voice VLAN to transmit voice data stream within the specified VLAN so as to ensure the transmission priority of voice data stream and voice quality.
Chapter 11 ACL	<p>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:</p> <ul style="list-style-type: none"> ● Time-Range: Configure the effective time for ACL rules. ● ACL Config: ACL rules. ● Policy Config: Configure operation policies. ● Policy Binding: Bind the policy to a port/VLAN to take its effect on a specific port/VLAN.
Chapter 12 Network Security	<p>This module is used to configure the multiple protection measures for the network security. Here mainly introduces:</p> <ul style="list-style-type: none"> ● IP-MAC Binding: Bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together. ● ARP Inspection: Configure ARP inspection feature to prevent the network from ARP attacks. ● DoS Defend: Configure DoS defend feature to prevent DoS attack. ● 802.1X: Configure common access control mechanism for LAN ports to solve mainly authentication and security problems. ● AAA: Configure the AAA function protect the device from unauthorized operations. ● PPPoE Config: Configure the PPPoE Circuit-ID Insertion function to support the authentication, authorization, and accounting (AAA) access requests on an Ethernet interface.
Chapter 13 SNMP	<p>This module is used to configure SNMP function to provide a management frame to monitor and maintain the network devices. Here mainly introduces:</p> <ul style="list-style-type: none"> ● 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	Introduction
Chapter 14 LLDP	<p>This module is used to configure LLDP function to provide information for SNMP applications to simplify troubleshooting. Here mainly introduces:</p> <ul style="list-style-type: none"> ● Basic Config: Configure the LLDP parameters of the device. ● Device Info: View the LLDP information of the local device and its neighbors. ● Device Statistics: View the LLDP statistics of the local device. ● LLDP-MED: Configure the LLDP-MED features.
Chapter 15 Maintenance	<p>This module is used to assemble the commonly used system tools to manage the switch. Here mainly introduces:</p> <ul style="list-style-type: none"> ● System Monitor: Monitor the memory and CPU of the switch. ● Log: View configuration parameters on the switch. ● Device Diagnostics: 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 Diagnostics: Test if the destination is reachable and the account of router hops from the switch to the destination. ● DLDP: Monitor the physical configuration of the cables and detect whether a unidirectional link exists.
Appendix A Glossary	Lists the glossary used in this manual.

[Return to CONTENTS](#)

Chapter 2 Introduction

2.1 Overview of the Switch

Designed for workgroups and departments, T2500G-10TS from TP-Link provides wire-speed performance and full set of layer 2 management features. It provides a variety of service features and multiple powerful functions with high security.

The EIA-standardized framework and smart configuration capacity can provide flexible solutions for a variable scale of networks. ACL, 802.1x, IP Source Guard and Dynamic ARP Inspection provide robust security strategy. QoS and IGMP snooping/filtering optimize voice and video application. Link aggregation (LACP) increases aggregated bandwidth, optimizing the transport of business critical data. SNMP, RMON, WEB/Telnet/SSH Log-in bring abundant management policies. T2500G-10TS switch integrates multiple functions with excellent performance, and is friendly to manage, which can fully meet the need of the users demanding higher networking performance.

2.2 Appearance Description

2.2.1 Front Panel

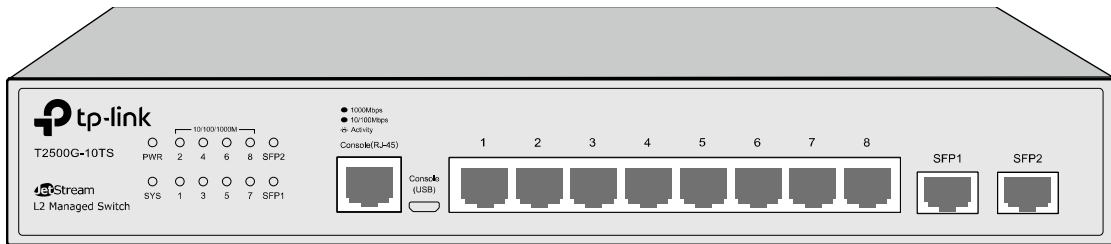


Figure 2-1 Front Panel

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

Name	Status	Indication	
PWR	On	Power is on.	
	Flashing	Power supply is abnormal.	
	Off	Power is off or power supply is abnormal.	
SYS	On	The switch is working abnormally.	
	Flashing	The switch is working normally.	
	Off	The switch is working abnormally.	
10/100/1000M	On	Green	A 1000Mbps device is connected to the corresponding port, but no activity.
		Yellow	A 10/100Mbps device is connected to the corresponding port, but no activity.
	Flashing	Data is being transmitted or received.	
	Off	Not linked.	

Name	Status	Indication
SFP1, SFP2	On	A 1000Mbps device is connected to the corresponding port, but no activity.
	Flashing	Data is being transmitted or received.
	Off	Not linked.

- **Console (RJ-45) Port:** Designed to connect with the serial port of a computer or terminal for monitoring and configuring the switch.
- **Console (USB) Port:** Designed to connect with the USB port of a computer for monitoring and configuring the switch. The switch has an RJ-45 console port and a micro-USB console port available. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector.
- **10/100/1000Mbps RJ45 Ports:** Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each 10/100/1000Mbps RJ45 port has a corresponding 10/100/1000M LED.
- **SFP Ports:** Designed to install the SFP module. T2500G-10TS features 2 individual SFP ports and supports 1000M SFP module connection only.

2.2.2 Rear Panel

The rear panel of T2500G-10TS features a power socket and a Grounding Terminal (marked with⊕).

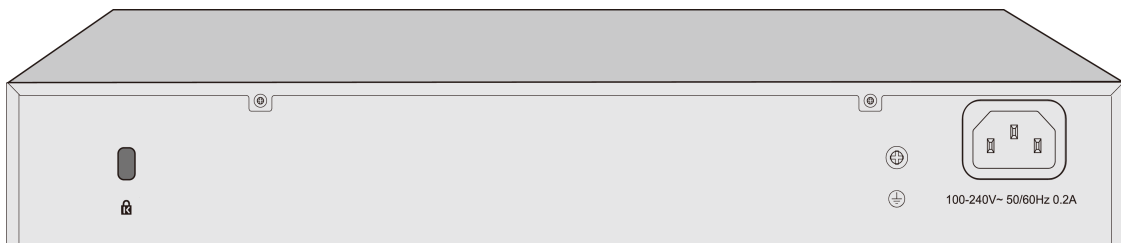


Figure 2-2 Rear Panel

- **Kensington Security Slot:** Secure the lock (not provided) into the security slot to prevent the device from being stolen.
- **Grounding Terminal:** T2500G-10TS 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 detail information, please refer to Installation Guide.
- **AC Power Socket:** Connect the female connector of the power cord here, and the male connector to the AC power outlet. Please make sure the voltage of the power supply meets the requirement of the input voltage (100-240V~ 50/60Hz 0.2A).

[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.

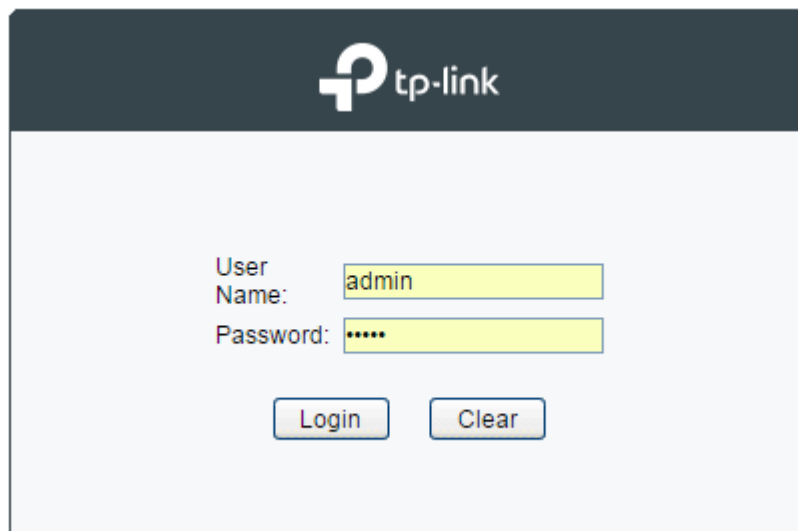


Figure 3-2 Login

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.

T2500G-10TS

System Summary | **Device Description** | System Time | Daylight Saving Time | System IP | System IPv6

System

- **System Info**
- User Management
- System Tools
- Access Security

Switching

VLAN

Spanning Tree

DHCP

Multicast

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

Logout

Copyright © 2017
TP-LINK Technologies Co., Ltd.
All rights reserved.

System Info

System Description:	JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots
Device Name:	T2500G-10TS
Device Location:	SHENZHEN
System Contact:	www.tp-link.com
Hardware Version:	T2500G-10TS 1.0
Firmware Version:	1.0.0 Build 20170315 Rel.31543(s)
Bootloader Version:	TP-LINK BOOTUTIL(v1.0.0)
IP Address:	192.168.0.25
Subnet Mask:	255.255.255.0
Default Gateway:	
MAC Address:	00-0A-EB-13-A2-26
Serial Number:	2111001000001
System Time:	2006-01-26 08:01:44
Run Time:	25 day - 0 hour - 1 min - 52 sec

Refresh Help

Figure 3-3 Main Setup-Menu

Note:

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

[Return to CONTENTS](#)

Chapter 4 System

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

4.1 System Info

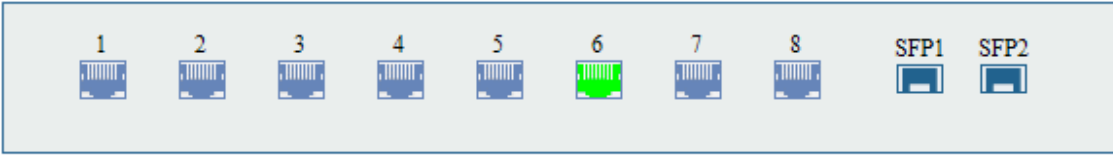
The System Info, mainly for basic properties configuration, can be implemented on **System Summary**, **Device Description**, **System Time**, **Daylight Saving Time**, **System IP** and **System IPv6** pages.

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 8 10/100/1000Mbps RJ45 ports and 2 SFP ports of the switch. Ports 1-8 are 10/100/1000Mbps ports, and SFP1 and SFP2 are individual SFP ports.

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



System Info	
System Description:	JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots
Device Name:	T2500G-10TS
Device Location:	SHENZHEN
System Contact:	www.tp-link.com
Hardware Version:	T2500G-10TS 1.0
Firmware Version:	1.0.0 Build 20170315 Rel.31543(s)
Bootloader Version:	TP-LINK BOOTUTIL(v1.0.0)
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Default Gateway:	
MAC Address:	00-0A-EB-13-A2-26
Serial Number:	2111001000001
System Time:	2006-01-05 07:06:54
Run Time:	3 day - 23 hour - 7 min - 2 sec

Figure 4-1 System Summary

➤ **Port Status**



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



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



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



Indicates the SFP port is not connected to a device.



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

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

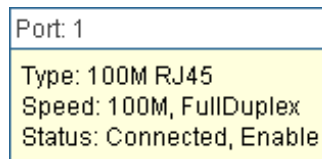


Figure 4-2 Port Information

➤ **Port Info**

Port: Displays the port number of the switch.

Type: Displays the type of the port.

Rate: Displays the maximum transmission rate of the port.

Status: Displays the connection status of the port.

Click a port to display the bandwidth utilization on this port. The actual rate divided by theoretical maximum rate is the bandwidth utilization. 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 abnormalities.

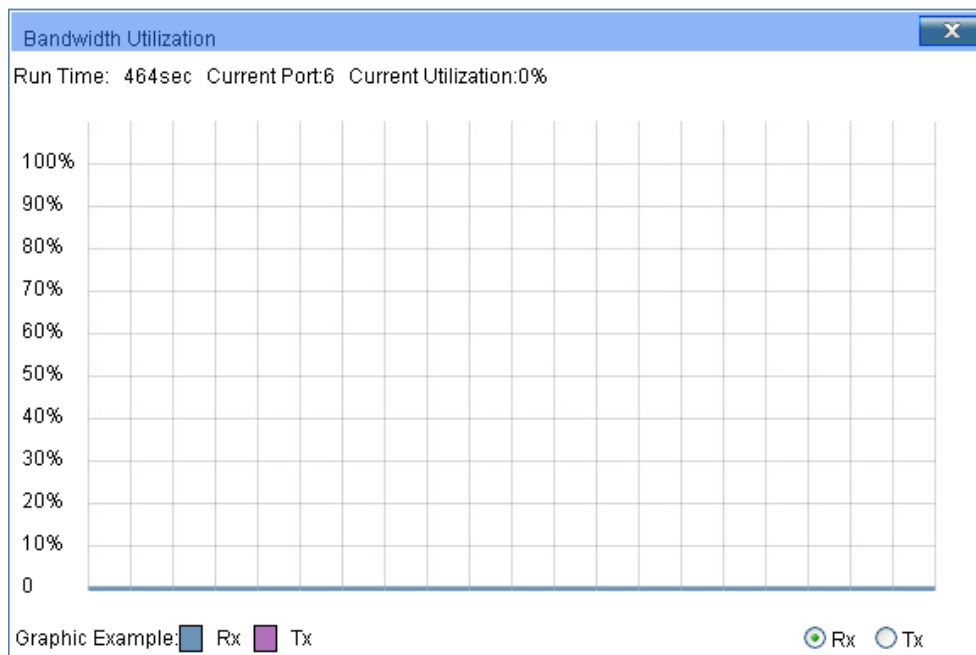


Figure 4-3 Bandwidth Utilization

➤ **Bandwidth Utilization**

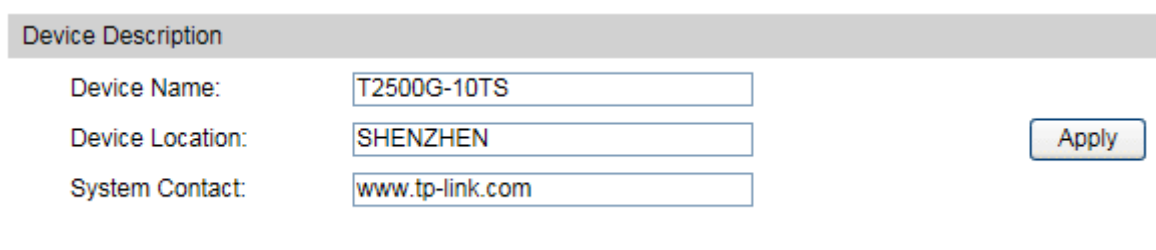
Rx: Select Rx to display the bandwidth utilization of receiving packets on this port.

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.



Device Description	
Device Name:	<input type="text" value="T2500G-10TS"/>
Device Location:	<input type="text" value="SHENZHEN"/>
System Contact:	<input type="text" value="www.tp-link.com"/>

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.

Time Info

Current System Date: 2006-01-01 12:02:27 Sunday
Current Time Source: Manual

Time Config

Manual

Date:

Time:

Get Time from NTP Server

Time Zone:

Primary Sever:

Secondary Sever:

Update Rate: hour(s)

Synchronize with PC's Clock

Figure 4-5 System Time

The following entries are displayed on this screen:

➤ **Time Info**

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

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

➤ **Time Config**

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

Get Time from NTP Server: When this option is selected, you can configure the time zone and the IP Address for the NTP Server. The switch will get UTC automatically if it has connected to an NTP Server.

- **Time Zone:** Select your local time.
- **Primary/Secondary 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.

DST Config

DST Status:

Predefined Mode

USA Australia Europe New Zealand

Recurring Mode

Offset: (minutes)

Start Time: Week Day Month

End Time: Week Day Month

Date Mode

Offset: (minutes)

Start Time: (MM/DD HH:MM)

End Time: (MM/DD HH:MM)

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

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

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

Date Mode:

Specify the DST configuration in Date mode. This configuration is 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:

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

4.1.5 System IP

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

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

MAC Address:	00-0A-EB-13-12-6A
IP Address Mode:	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> BOOTP
Management VLAN:	1 (VLAN ID: 1-4094)
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Default Gateway:	

Figure 4-7 System IP

The following entries are displayed on this screen:

➤ IP Config

MAC Address:

Displays MAC Address of the switch.

IP Address Mode:

Select the mode to obtain IP Address for the switch.

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

- Management VLAN:** Enter the ID of management VLAN, the only VLAN through which you can get access to the switch. By default VLAN1 owning all the ports is the Management VLAN and you can access the switch via any port on the switch. However, if another VLAN is created and set to be the Management VLAN, you may have to reconnect the management station to a port that is a member of the Management VLAN.
- IP Address:** Enter the system IP of the switch. The default system IP is 192.168.0.1 and you can change it appropriate to your needs.
- Subnet Mask:** Enter the subnet mask of the switch.
- Default Gateway:** Enter the default gateway of the switch.



Note:

1. Changing the IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.
2. The switch only possesses an IP address. The IP address configured will replace the original IP address.
3. If the switch gets the IP address from DHCP server, you can see the configuration of the switch in the DHCP server; if DHCP option is selected but no DHCP server exists in the network, the switch will keep obtaining IP address from DHCP server until success.
4. If DHCP or BOOTP option is selected, the switch will get network parameters dynamically from the Internet, which means that its IP address, subnet mask and default gateway cannot be configured.
5. By default, the IP address is 192.168.0.1.

4.1.6 System IPv6

IPv6 (Internet Protocol version 6), also called IPng (IP next generation), was developed by the IETF (Internet Engineering Task Force) as the successor to IPv4 (Internet Protocol version 4). Compared with IPv4, IPv6 increases the IP address size from 32 bits to 128 bits; this solves the IPv4 address exhaustion problem.

➤ **IPv6 features**

IPv6 has the following features:

1. **Adequate address space:** The source and destination IPv6 addresses are both 128 bits (16 bytes) long. IPv6 can provide 3.4×10^{38} addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.
2. **Header format simplification:** IPv6 cuts down some IPv4 header fields or move them to IPv6 extension headers to reduce the load of basic IPv6 headers, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of basic IPv6 headers is 40 bytes and is only twice that of IPv4 headers (excluding the Options field).

3. **Flexible extension headers:** IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the handling efficiency. The Options field in IPv4 packets contains 40 bytes at most, while the size of IPv6 extension headers is restricted by that of IPv6 packets.
4. **Built-in security:** IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and improves the interoperability between different IPv6 applications.
5. **Automatic address configuration:** To simplify the host configuration, IPv6 supports stateful and stateless address configuration.
 - Stateful address configuration means that a host acquires an IPv6 address and related information from a server (for example, DHCP server).
 - Stateless address configuration means that a host automatically configures an IPv6 address and related information on basis of its own link-layer address and the prefix information advertised by a router.

In addition, a host can generate a link-local address on basis of its own link-layer address and the default prefix (FE80::/64) to communicate with other hosts on the link.

6. **Enhanced neighbor discovery mechanism:** The IPv6 neighbor discovery protocol is a group of Internet control message protocol version 6 (ICMPv6) messages that manages the information exchange between neighbor nodes on the same link. The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP) message, Internet Control Message Protocol version 4 (ICMPv4) router discovery message, and ICMPv4 redirection message to provide a series of other functions.

➤ Introduction to IPv6 address

1. IPv6 address format

An IPv6 address is represented as a series of 16-bit hexadecimal, separated by colons (:). An IPv6 address is divided into eight groups, and the 16 bits of each group are represented by four hexadecimal numbers which are separated by colons, for example, 2001:0d02:0000:0000:0014: 0000:0000:0095. The hexadecimal letters in IPv6 addresses are not case-sensitive.

To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

- Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in shorter format as 2001:d02:0:0:14:0:0:95.
- Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address. For example, the above-mentioned address can be represented in the shortest format as 2001:d02::14:0:0:95.

**Note:**

Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. Otherwise, the device is unable to determine how many zeros double-colons represent when converting them to zeros to restore a 128-bit IPv6 address.

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is represented in "IPv6 address/prefix length" format, where "IPv6 address" is an IPv6 address in any of the above-mentioned formats and "prefix length" is a decimal number indicating how many leftmost bits from the preceding IPv6 address are used as the address prefix.

2. IPv6 address classification

IPv6 addresses fall into three types: unicast address, multicast address, and anycast address.

- **Unicast address:** An identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.
- **Multicast address:** An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address. There are no broadcast addresses in IPv6. Their function is superseded by multicast addresses.
- **Anycast address:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols' measure of distance).

The type of an IPv6 address is designated by the first several bits called format prefix. The following table lists the mappings between address types and format prefixes.

Type		Format Prefix (binary)	IPv6 Prefix ID
Unicast address	Unassigned address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site-local address	1111111011	FEC0::/10
	Global unicast address (currently assigned)	001	2xxx::/4 or 3xxx::/4

	Reserved type (to be assigned in future)	Other formats	
Multicast address		11111111	FF00::/8
Anycast address	Anycast addresses are taken from unicast address space and are not syntactically distinguishable from unicast addresses.		

Table 4-1 Mappings between address types and format prefixes

IPv6 unicast address can be classified into several types, including global unicast address, link-local address, and site-local address. The two most common types are introduced below:

- Global unicast address

A Global unicast address is an IPv6 unicast address that is globally unique and is routable on the global Internet.

Global unicast addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Except for addresses that start with binary 000, all global unicast addresses have a 64-bit interface ID. The IPv6 global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). The figure below shows the structure of a global unicast address.

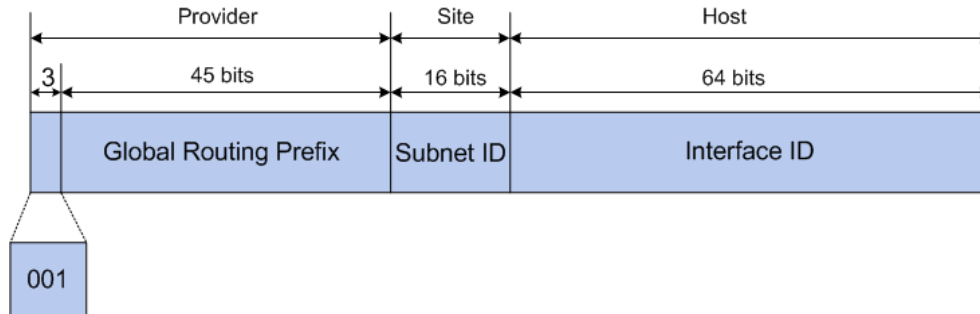


Figure 4-8 Global Unicast Address Format

An interface ID is used to identify interfaces on a link. The interface ID must be unique to the link. It may also be unique over a broader scope. In many cases, an interface ID will be the same as or based on the link-layer address of an interface. Interface IDs used in global unicast and other IPv6 address types must be 64 bits long and constructed in the modified extended universal identifier (EUI)-64 format.

For all IEEE 802 interface types (for example, Ethernet and FDDI interfaces), Interface IDs in the modified EUI-64 format are constructed in the following way:

the first three octets (24 bits) are taken from the Organizationally Unique Identifier (OUI) of the 48-bit link-layer address (the media access control, or MAC, address) of the interface, the fourth and fifth octets (16 bits) are a fixed hexadecimal value of FFFE, and the last three octets (24 bits) are taken from the last three octets of the MAC address. The construction of the interface ID is completed by setting the universal/local (U/L)

bit--the seventh bit of the first octet--to a value of 0 or 1. A value of 0 indicates a locally administered identifier; a value of 1 indicates a globally unique IPv6 interface identifier.

Take MAC address 0012:0B0A:2D51 as an example. Insert **FFFE** to the middle of the address to get 0012:0BFF:FE0A:2D51. Then set the U/L bit to 1 to obtain an interface ID in EUI-64 format as 0212:0BFF:FE0A:2D51.

- Link-local address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need globally unique addresses to communicate. The figure below shows the structure of a link-local address.

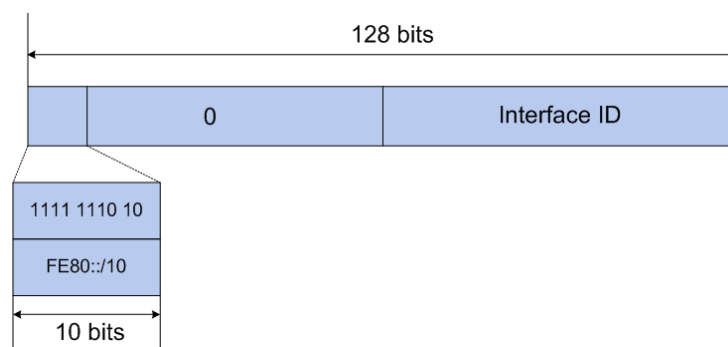


Figure 4-9 Link-local Address Format

IPv6 devices must not forward packets that have link-local source or destination addresses to other links.



Note:

You can configure multiple IPv6 addresses per interface, but only one link-local address.

➤ **IPv6 Neighbor Discovery**

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

1. IPv6 Neighbor Solicitation Message

A value of 135 in the Type field of the ICMP packet header identifies a neighbor solicitation (NS) message. Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link. After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement (NA) message, which has a value of 136 in the Type field of the ICMP packet header, on the local link. After the source node receives the neighbor advertisement, the source node and destination node can communicate.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified.

Neighbor solicitation messages are also used in the stateless autoconfiguration process to verify the uniqueness of unicast IPv6 addresses before the addresses are assigned to an interface. Duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed). Specifically, a node sends a neighbor solicitation message with an unspecified source address and a tentative link-local address in the body of the message. If another node is already using that address, the node returns a neighbor advertisement message that contains the tentative link-local address. If another node is simultaneously verifying the uniqueness of the same address, that node also returns a neighbor solicitation message. If no neighbor advertisement messages are received in response to the neighbor solicitation message and no neighbor solicitation messages are received from other nodes that are attempting to verify the same tentative address, the node that sent the original neighbor solicitation message considers the tentative link-local address to be unique and assigns the address to the interface.

Every IPv6 unicast address (global or link-local) must be verified for uniqueness on the link; however, until the uniqueness of the link-local address is verified, duplicate address detection is not performed on any other IPv6 addresses associated with the link-local address.

2. IPv6 Router Advertisement Message

Router advertisement (RA) messages, which have a value of 134 in the Type field of the ICMP packet header, are periodically sent out each configured interface of an IPv6 router.

RA messages typically include the following information:

- One or more onlink IPv6 prefixes that nodes on the local link can use to automatically configure their IPv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed
- Default router information (whether the device sending the advertisement should be used as a default router and, if so, the amount of time, in seconds, the device should be used as a default router)
- Additional information for hosts, such as the hop limit and maximum transmission unit (MTU) a host should use in packets that it originates

RAs are also sent in response to device solicitation messages. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup or anytime needed so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

Hosts discover and select default devices by listening to Router Advertisements (RAs).

Stateless address autoconfiguration means that the node automatically configures an IPv6 address and other information for its interface according to the address prefix and other configuration parameters in the received RA messages.

3. IPv6 Neighbor Redirect Message

A value of 137 in the type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Devices send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination.

A device will send an IPv6 ICMP redirect message when the following conditions are satisfied:

- The receiving interface is the forwarding interface.
- The selected route itself is not created or modified by an IPv6 ICMP redirect message.
- The selected route is not the default route.
- The forwarded IPv6 packet does not contain any routing header.

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

Global Config

IPv6: Enable Disable

Link-local Address Config

Config Mode: Manual Auto

Link-local Address: (Format: fe80::1)

Status: Normal

Global Address Autoconfig via RA Message

Enable global address auto configuration via RA message

Global Address Autoconfig via DHCPv6 Server

Enable global address auto configuration via DHCPv6 Server

Add a Global Address Manually

Address Format: EUI-64 Not EUI-64

Global Address: (Format:3001::1/64)

Global Address Table

Select	Global Address	Prefix Length	Type	Preferred Lifetime/Valid Lifetime	Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>			

Figure 4-10 System IPv6

The following entries are displayed on this screen:

➤ **Global Config**

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

➤ **Link-local Address Config**

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

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

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

- Status:** Displays the status of the link-local address.
- **Normal:** Indicates that the link-local address is normal.
 - **Try:** Indicates that the link-local address may be newly configured
 - **Repeat:** Indicates that the link-local address is duplicate. It is illegal to access the switch using the IPv6 address (including link-local and global address).
- **Global Address Autoconfig via RA Message**
- Enable global address auto configuration via RA message:** When this option is enabled, the switch automatically configures a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.
- **Global Address Autoconfig via DHCPv6 Server**
- Enable Global Address Autoconfig via DHCPv6 Server:** When this option is enabled, the system will try to obtain the global address from the DHCPv6 Server.
- **Add a global address manually**
- Address Format:** You can select the global address format according to your requirements.
- **EUI-64:** Indicates that you only need to specify an address prefix, and then the system will create a global address automatically.
 - **Not EUI-64:** Indicates that you have to specify an intact global address.
- Global Address:** When selecting the mode of EUI-64, please input the address prefix here, otherwise, please input an intact IPv6 address here.
- **Global address Table**
- Select:** Select the desired entry to delete or modify the corresponding global address.
- Global Address:** Modify the global address.
- Prefix Length:** Modify the prefix length of the global address.
- Type:** Displays the configuration mode of the global address.
- **Manual:** Indicates that the corresponding address is configured manually
 - **Auto:** Indicates that the corresponding address is created automatically using the RA message or obtained from the DHCPv6 Server.

Preferred Lifetime /Valid Lifetime:

Displays the preferred time and valid time of the global address.

Status:

Displays the status of the global address.

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



Tips:

After adding a global IPv6 address to your switch manually here, you can configure your PC's global IPv6 address in the same subnet with the switch and login to the switch via its global IPv6 address.

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.

User Table		
User ID	User Name	Access Level
1	admin	Admin

Figure 4-11 User Table

4.2.2 User Config

On this page you can configure the access level of the user to log on to the Web management page. The switch provides four access levels: Admin, Operator, Power User and User. "Admin" means that you can edit, modify and view all the settings of different functions. "Operator" means that you can edit, modify and view most of the settings of different functions. "Power User" means that you can edit, modify and view some of the settings of different functions. "User" means that you can only view some of the settings of different functions without the right to edit or modify. The Web management pages contained in this guide are subject to the admin's login without any explanation.

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

The screenshot displays the 'User Config' interface. At the top, there is a 'User Info' section with four input fields: 'User Name', 'Access Level' (a dropdown menu currently set to 'Operator'), 'Password', and 'Confirm Password'. To the right of these fields are two buttons: 'Create' and 'Clear'. Below this is a 'User Table' section containing a table with the following data:

Select	User ID	User Name	Access Level	Operation
<input type="checkbox"/>	1	admin	Admin	Edit

Below the table are two buttons: 'Delete' and 'Help'.

Figure 4-12 User Config

The following entries are displayed on this screen:

➤ **User Info**

User Name: Create a name for users' login.

Access Level: Select the access level to login.

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

Password: Type a password for users' login.

Confirm Password: Retype the password.

➤ **User Table**

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

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

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

4.3 System Tools

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

4.3.1 Boot Config

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

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

Select	Current Startup Image	Next Startup Image	Backup Image
<input type="checkbox"/>	image1.bin	image1.bin	image2.bin

Apply Help

Figure 4-13 Boot Config

The following entries are displayed on this screen:

➤ **Boot Table**

- Select:** Select the unit(s).
- Current Startup Image:** Displays the current startup image.
- Next Startup Image:** Select the next startup image.
- Backup Image:** Select the backup boot image.

4.3.2 Config Restore

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

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

Config Restore

Restore the config from the saved config file

Select a backup config file and click the Restore Config button, and then you can restore to the previous config.

Config file: Browse...

Restore Config Help

Figure 4-14 Config Restore

The following entries are displayed on this screen:

➤ **Config Restore**

Restore Config: Click the **Restore Config** 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 being restored, the current settings of the switch will be lost. Wrong uploaded configuration file may cause the switch unmanaged.

4.3.3 Config Backup

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

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

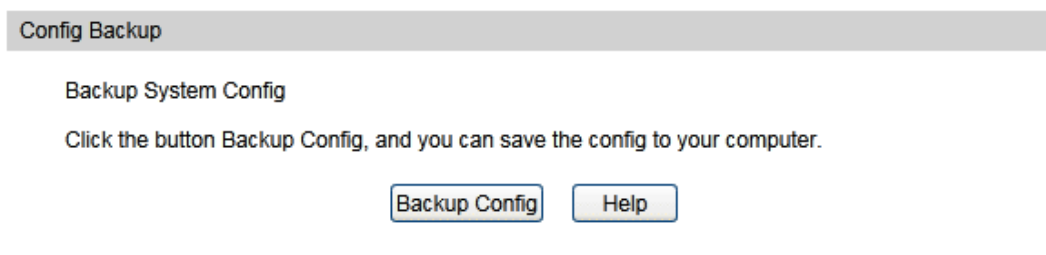


Figure 4-15 Config Backup

The following entries are displayed on this screen:

➤ **Config Backup**

Backup Config: Click the Backup Config button to save the current configuration as a file to your computer. You are suggested to take this measure before upgrading.



Note:

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

4.3.4 Firmware Upgrade

The switch system can be upgraded via the Web management page. To upgrade the system is to get more functions and better performance. Go to <http://www.tp-link.com> to download the updated firmware.

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

Firmware Upgrade

You will get the new function after upgrading the firmware.

Firmware File: Browse...

Image Name: Backup Image

Firmware Version: 1.0.0 Build 20170315 Rel.31543(s)

Hardware Version: T2500G-10TS 1.0

After upgrading, the device will reboot automatically with the backup image

Figure 4-16 Firmware Upgrade

 **Note:**

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

4.3.5 System Reboot

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

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

System Reboot

Save Config:

Reboot:

Figure 4-17 System Reboot

 **Note:**

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

4.3.6 System Reset

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

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

System Reset

Reset:

Figure 4-18 System Reset

 **Note:**

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

4.4 Access Security

Access Security provides different security measures for the remote login so as to enhance the configuration management security. It can be implemented on **Access Control**, **SSL Config** and **SSH 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](#).

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

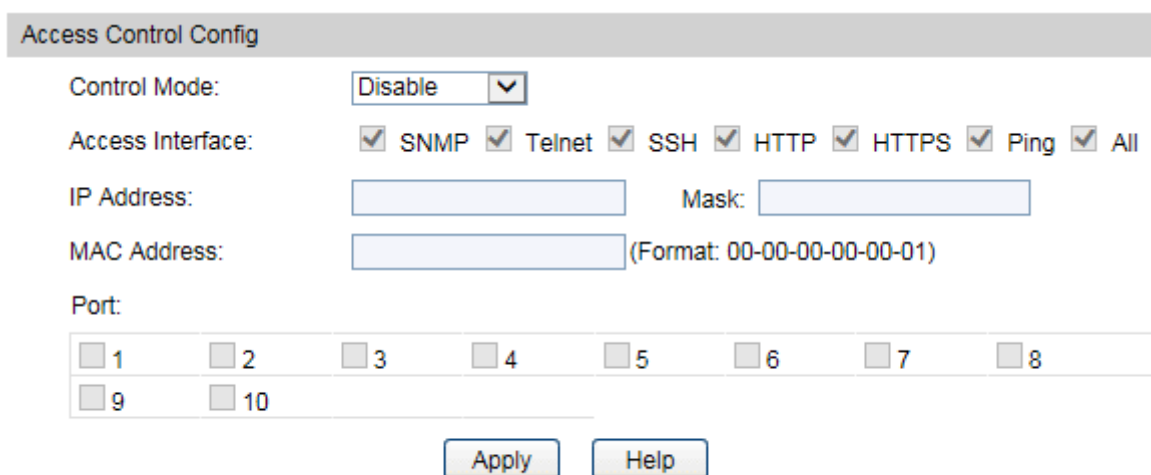


Figure 4-19 Access Control

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.

- **IP-based:** Select this option to limit the IP-range of the users for login.
- **MAC-based:** Select this option to limit the MAC Address of the users for login.
- **Port-based:** Select this option to limit the ports for login.

Access Interface:

Select the interface for access control to apply.

IP Address & Mask:

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

MAC Address: The field 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 login.

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

4.4.2 HTTP Config

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

On this page you can configure the HTTP function.

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

Global Config

HTTP: Enable Disable

Session Config

Session Timeout: min (5-30)

Access User Number

Number Control: Enable Disable

Admin Number: (1-16)

Guest Number: (0-15)

Figure 4-20 HTTP Config

The following entries are displayed on this screen:

➤ **Global Config**

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

➤ **Session Config**

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

➤ **Access User Number**

Number Control: Select Enable or disable the Number Control function.

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

Guest Number:

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

4.4.3 HTTPS Config

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

SSL mainly provides the following services:

1. Authenticate the users and the servers based on the certificates to ensure the data are transmitted to the correct users and servers;
2. Encrypt the data transmission to prevent the data being intercepted;
3. Maintain the integrity 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://\[3001::1\]](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.

The screenshot displays the HTTPS configuration page, organized into several sections:

- Global Config:** Contains three rows of settings, each with radio buttons for 'Enable' (selected) and 'Disable', and an 'Apply' button on the right.
 - HTTPS: Enable Disable
 - SSL Version 3: Enable Disable
 - TLS Version 1: Enable Disable
- CIPHERSUITE:** Contains four rows of settings, each with radio buttons for 'Enable' (selected) and 'Disable', and an 'Apply' button on the right.
 - RSA_WITH_RC4_128_MD5: Enable Disable
 - RSA_WITH_RC4_128_SHA: Enable Disable
 - RSA_WITH_DES_CBC_SHA: Enable Disable
 - RSA_WITH_3DES_EDE_CBC_SHA: Enable Disable
- Session Config:** Contains one row with a text input field for 'Session Timeout' (value: 10) and a label 'min (5-30)', with an 'Apply' button on the right.
- Access User Number:** Contains three rows of settings, each with radio buttons for 'Enable' and 'Disable' (selected), and an 'Apply' button on the right.
 - Number Control: Enable Disable
 - Admin Number: (1-16)
 - Guest Number: (0-15)
- Certificate Download:** Contains one row with a text input field for 'Certificate File', a 'Browse...' button, and a 'Download' button.
- Key Download:** Contains one row with a text input field for 'Key File', a 'Browse...' button, and a 'Download' button.

Figure 4-21 HTTPS Config

The following entries are displayed on this screen:

➤ **Global Config**

HTTPS: Select 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**

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

➤ **Access User Number**

Number Control: Select Enable or disable the Number Control function.

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

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

➤ **Certificate Download**

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

➤ **Key Download**

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



Note:

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

4.4.4 SSH Config

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

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

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

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

The screenshot displays the SSH configuration interface, organized into four main sections:

- Global Config:** Contains radio buttons for 'SSH' (Disable selected), 'Protocol V1' (Enable selected), and 'Protocol V2' (Enable selected). It also includes input fields for 'Idle Timeout' (120 sec) and 'Max Connect' (5), along with 'Apply' and 'Help' buttons.
- Encryption Algorithm:** Features checkboxes for AES128-CBC, AES192-CBC, AES256-CBC, Blowfish-CBC, Cast128-CBC, and 3DES-CBC, all of which are checked. An 'Apply' button is present.
- Data Integrity Algorithm:** Features checkboxes for HMAC-SHA1 and HMAC-MD5, both checked. An 'Apply' button is present.
- Key Download:** Includes a dropdown menu for 'Key Type' (SSH-2 RSA/DSA selected) and a 'Browse...' button for 'Key File'. A 'Download' button is also present.

Figure 4-22 SSH Config

The following entries are displayed on this screen:

➤ **Global Config**

- SSH:** Select Enable or disable SSH function.
- Protocol V1:** Select Enable or disable SSH V1 to be the supported protocol.
- Protocol V2:** Select 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.
- AES128-CBC:** Select the checkbox to enable the AES128-CBC algorithm of SSH.
- AES192-CBC:** Select the checkbox to enable the AES192-CBC algorithm of SSH.
- AES256-CBC:** Select the checkbox to enable the AES256-CBC algorithm of SSH.
- Blowfish-CBC:** Select the checkbox to enable the Blowfish-CBC algorithm of SSH.
- Cast128-CBC:** Select the checkbox to enable the Cast128-CBC algorithm of SSH.
- 3DES-CBC:** Select the checkbox to enable the 3DES-CBC algorithm of SSH.

➤ **Data Integrity Algorithm**

Configure SSH data integrity algorithms.


- HMAC-SHA1:** Select the checkbox to enable the HMAC-SHA1 algorithm of SSH.
- HMAC-MD5:** Select the checkbox to enable the HMAC-MD5 algorithm of SSH.

➤ **Key Download**

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

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

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

 **Note:**

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

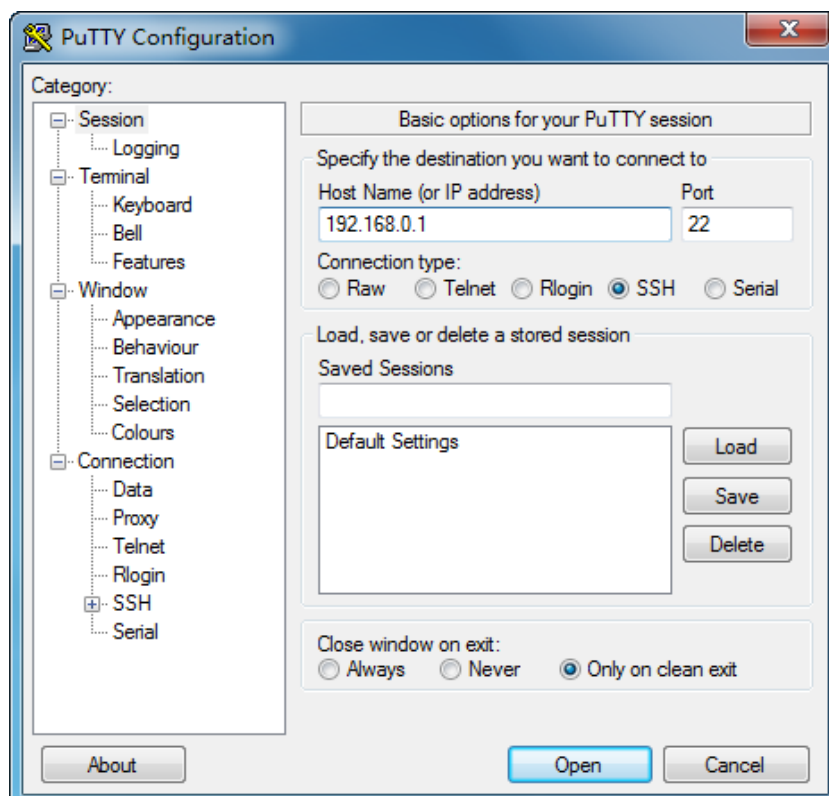
Application Example 1 for SSH:

➤ **Network Requirements**

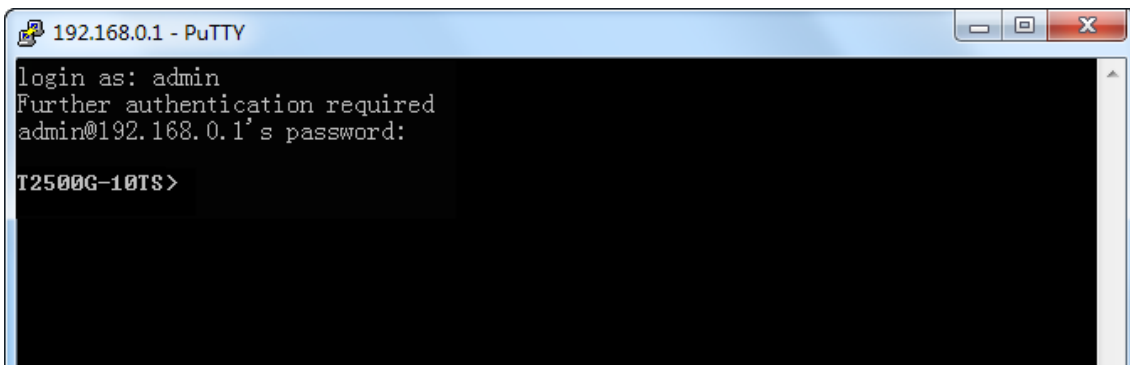
1. Log on to the switch via password authentication using SSH and the SSH function is enabled on the switch.
2. PuTTY client software is recommended.

➤ **Configuration Procedure**

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



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



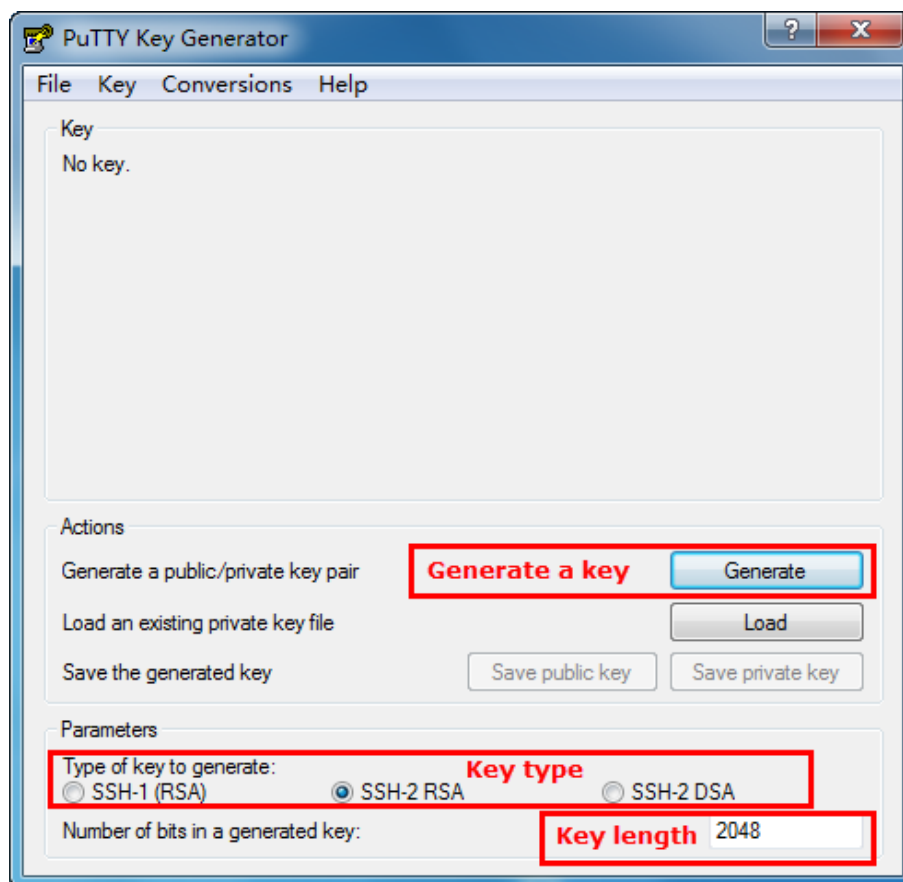
Application Example 2 for SSH:

➤ Network Requirements

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

➤ Configuration Procedure

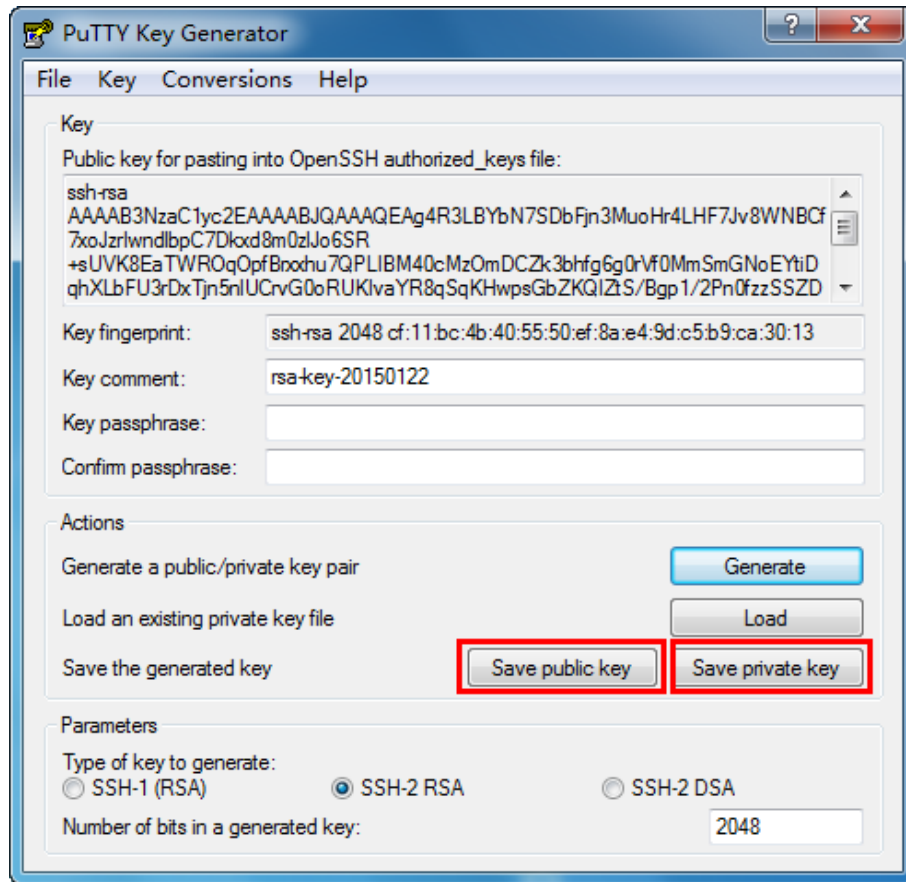
1. Select the key type and key length, and generate SSH key.



⚠ Note:

1. The key length is in the range of 512 to 3072 bits.

2. During the key generation, randomly moving the mouse quickly can accelerate the key generation.
2. After the key is successfully generated, please save the public key and private key to the computer.



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

Key Download

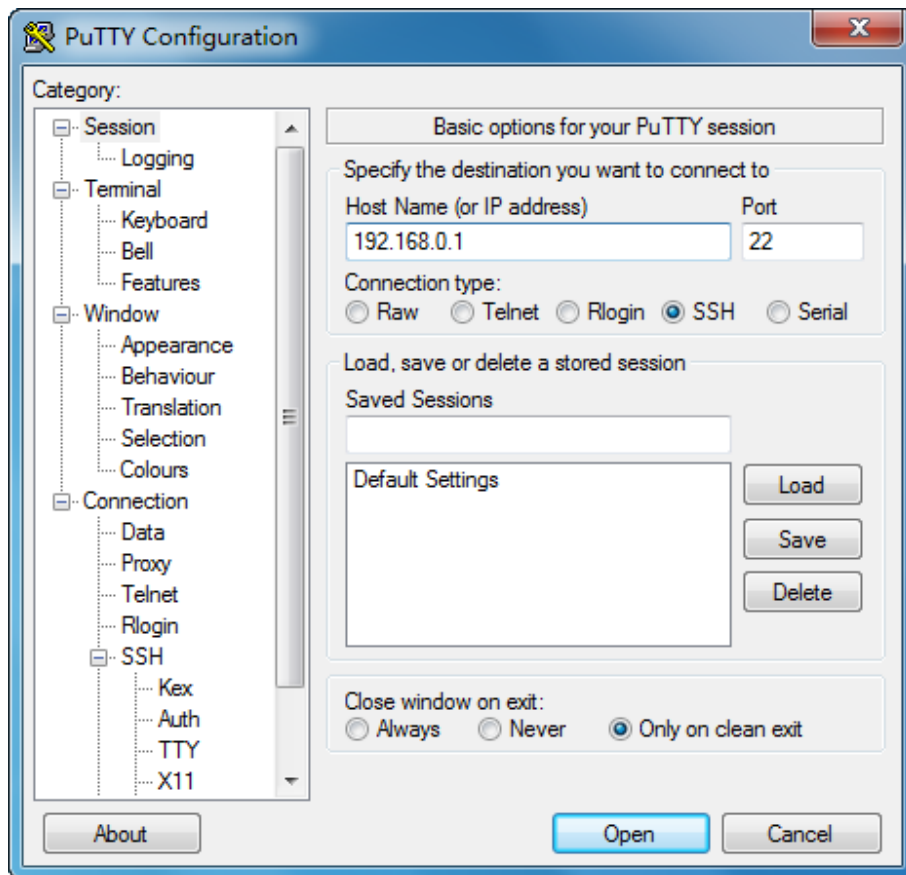
Choose the SSH public key file to download into switch.

Key Type:

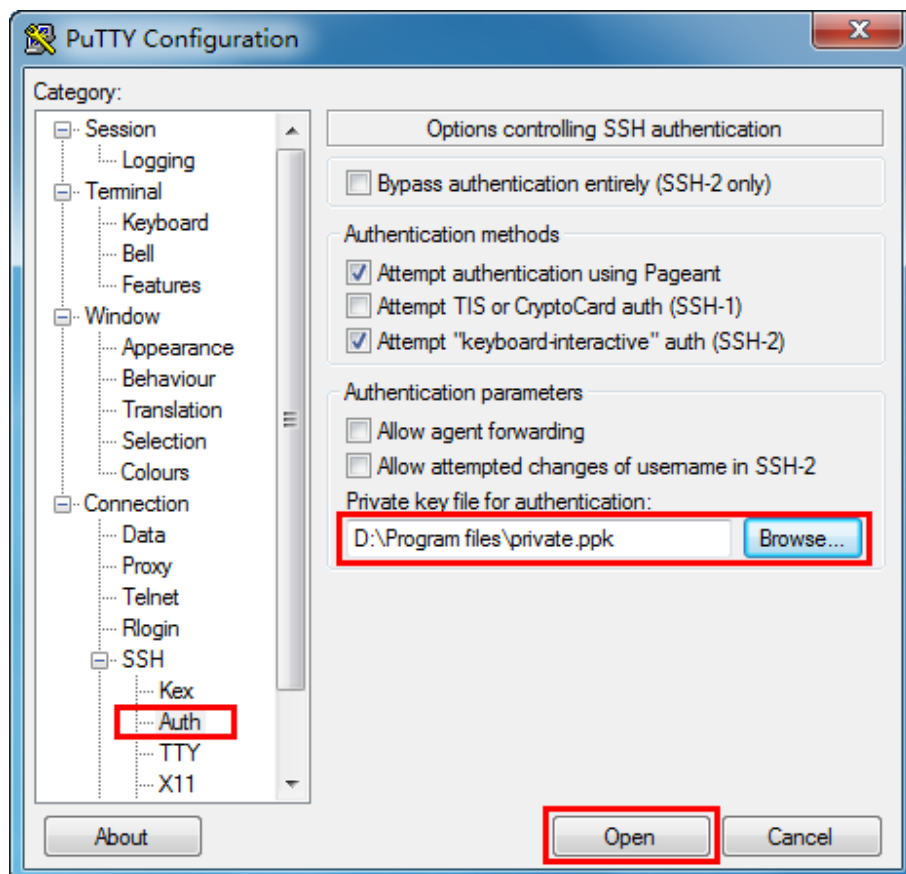
Key File:

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

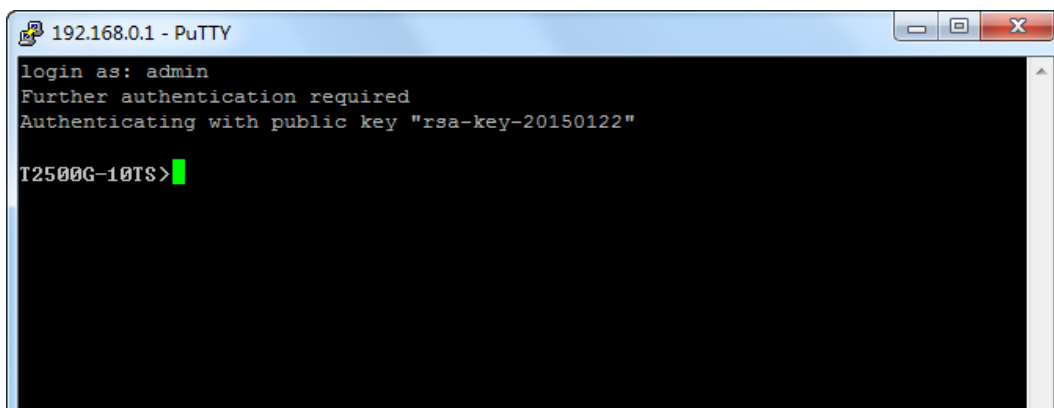
4. After the public key and private key are downloaded, please log on to the interface of PuTTY and enter the IP address for login.



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



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



4.4.5 Telnet Config

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

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

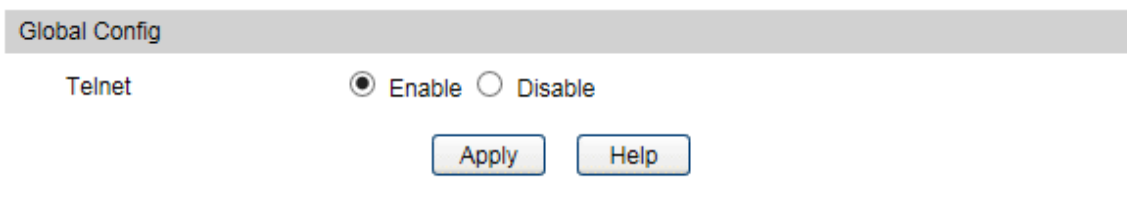


Figure 4-23 Access Control

The following entries are displayed on this screen:

➤ **Global Config**

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

[Return to CONTENTS](#)

Chapter 5 Switching

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

5.1 Port

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

5.1.1 Port Config

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

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

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

Port Config							
						Port <input type="text"/>	Select
Select	Port	Description	Status	Speed and Duplex	Flow Control	LAG	
<input type="checkbox"/>		<input type="text"/>	Disable	10MHD	Disable		
<input type="checkbox"/>	1		Enable	Auto	Disable	---	
<input type="checkbox"/>	2		Enable	Auto	Disable	---	
<input type="checkbox"/>	3		Enable	Auto	Disable	---	
<input type="checkbox"/>	4		Enable	Auto	Disable	---	
<input type="checkbox"/>	5		Enable	Auto	Disable	---	
<input type="checkbox"/>	6		Enable	Auto	Disable	---	
<input type="checkbox"/>	7		Enable	Auto	Disable	---	
<input type="checkbox"/>	8		Enable	Auto	Disable	---	
<input type="checkbox"/>	9		Enable	1000MFD	Disable	---	
<input type="checkbox"/>	10		Enable	1000MFD	Disable	---	

Figure 5-1 Port Config

The following entries are displayed on this screen.

➤ Port Config

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

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

Port: Displays the port number.

Description: Give a description to the port for identification.

Status: Allows you to Enable or disable the port. When Enable is selected, the port can forward the packets normally.

Speed and Duplex: Select the Speed and Duplex mode for the port. The device connected to the switch should be in the same Speed and Duplex mode with the switch. When "Auto" is selected, the Speed and Duplex mode will be determined by auto-negotiation.

Flow Control: Allows you to Enable or disable the Flow Control feature. When Flow Control is enabled, the switch can synchronize the speed with its peer to avoid the packet loss caused by congestion.

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

 **Note:**

1. The switch cannot be managed through the disabled port. Please enable the port which is used to manage the switch.
2. The parameters of the port members in a LAG should be set as the same.

5.1.2 Port Mirror

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

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

Mirror Group List				
Group	Mirroring	Mode	Mirrored Port	Operation
1	0	Ingress	---	Edit
		Egress	---	
2	0	Ingress	---	Edit
		Egress	---	
3	0	Ingress	---	Edit
		Egress	---	
4	0	Ingress	---	Edit
		Egress	---	

[Help](#)

Figure 5-2 Port Mirror Config

The following entries are displayed on this screen.

➤ **Mirror Session List**

Group: Displays the mirror group number.

- Mirroring:** Displays the mirroring port number.
- Mode:** Displays the mirror mode. The value will be "Ingress" or "Egress".
- Mirrored Port:** Displays the mirrored ports.
- Operation:** You can configure the mirror group by clicking **Edit**.

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

Mirror Group

Number:

Mirroring Port

Mirroring Port:

Mirrored Port

Port

Select	Port	Ingress	Egress	LAG
<input type="checkbox"/>		<input type="text" value="Disable"/> <input type="button" value="v"/>	<input type="text" value="Disable"/> <input type="button" value="v"/>	
<input type="checkbox"/>	1	Disable	Disable	---
<input type="checkbox"/>	2	Disable	Disable	---
<input type="checkbox"/>	3	Disable	Disable	---
<input type="checkbox"/>	4	Disable	Disable	---
<input type="checkbox"/>	5	Disable	Disable	---
<input type="checkbox"/>	6	Disable	Disable	---
<input type="checkbox"/>	7	Disable	Disable	---
<input type="checkbox"/>	8	Disable	Disable	---
<input type="checkbox"/>	9	Disable	Disable	---
<input type="checkbox"/>	10	Disable	Disable	---

Figure 5-3 Port Mirror Config

The following entries are displayed on this screen:

- **Mirror Group**
 - Number:** Select the mirror group you want to config.
- **Mirroring Port**
 - Mirroring Port:** Select a physical port from the port panel as the mirroring port.
- **Mirrored Port**
 - Select:** Select the desired port as a mirrored port. It is multi-optional.
 - Port:** Displays the port number.

Ingress:	Select Enable or disable the Ingress feature. When the Ingress is enabled, the incoming packets received by the mirrored port will be copied to the mirroring port.
Egress:	Select Enable or disable the Egress feature. When the Egress is enabled, the outgoing packets sent by the mirrored port will be copied to the mirroring port.
LAG:	Displays the LAG number which the port belongs to. The LAG member cannot be selected as the mirrored port or mirroring port.

**Note:**

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

5.1.3 Port Security

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

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

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

Port Security					
Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
<input type="checkbox"/>		<input type="text"/>		Dynamic <input type="button" value="v"/>	Disable <input type="button" value="v"/>
<input type="checkbox"/>	1	64	0	Dynamic	Disable
<input type="checkbox"/>	2	64	0	Dynamic	Disable
<input type="checkbox"/>	3	64	0	Dynamic	Disable
<input type="checkbox"/>	4	64	0	Dynamic	Disable
<input type="checkbox"/>	5	64	0	Dynamic	Disable
<input type="checkbox"/>	6	64	0	Dynamic	Disable
<input type="checkbox"/>	7	64	0	Dynamic	Disable
<input type="checkbox"/>	8	64	0	Dynamic	Disable
<input type="checkbox"/>	9	64	0	Dynamic	Disable
<input type="checkbox"/>	10	64	0	Dynamic	Disable

Figure 5-4 Port Security

The following entries are displayed on this screen:

➤ **Port Security**

- Select:** Select the desired port for Port Security configuration. It is multi-optional.
- Port:** Displays the port number.
- Max Learned MAC:** Specify the maximum number of MAC addresses that can be learned on the port.
- Learned Num:** Displays the number of MAC addresses that have been learned on the port.
- Learn Mode:** Select the Learn Mode for the port.
- **Dynamic:** When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time.
 - **Static:** When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted.
 - **Permanent:** When Permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.
- Status:** Enable or disable the Port Security feature for the port.

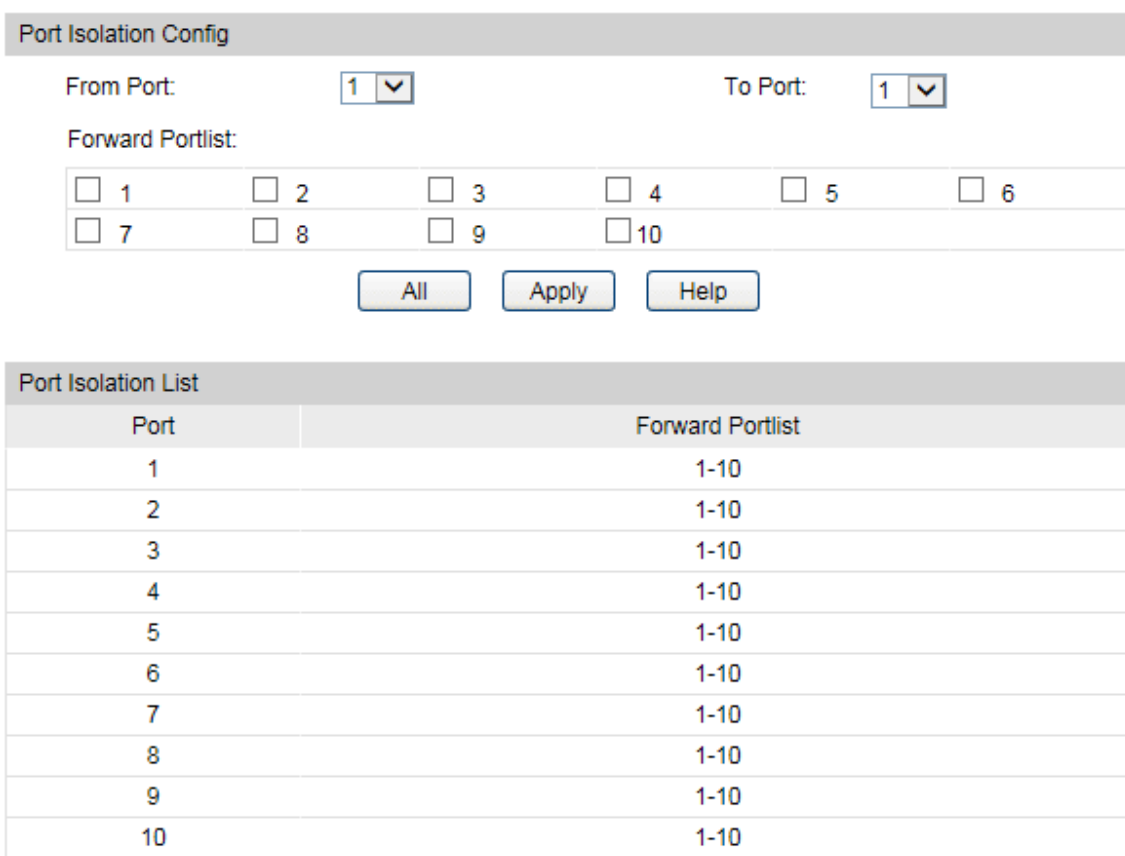
 **Note:**

1. The Port Security function is disabled for the LAG port member. Only the port is removed from the LAG, will the Port Security function be available for the port.
2. The Port Security function is disabled when the 802.1X function is enabled.

5.1.4 Port Isolation

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

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



The screenshot shows two web pages. The top page is titled "Port Isolation Config" and features two dropdown menus for "From Port" and "To Port", both set to "1". Below these is a "Forward Portlist" section with checkboxes for ports 1 through 10. At the bottom of this section are three buttons: "All", "Apply", and "Help". The bottom page is titled "Port Isolation List" and contains a table with two columns: "Port" and "Forward Portlist".

Port	Forward Portlist
1	1-10
2	1-10
3	1-10
4	1-10
5	1-10
6	1-10
7	1-10
8	1-10
9	1-10
10	1-10

Figure 5-5 Port Isolation Config

The following entries are displayed on this screen:

➤ **Port Isolation Config**

From/To Port: Select the port number to set its forward list.

Forward Portlist: Select the port(s) to be forwarded to.

➤ **Port Isolation List**

Port: Display the port number.

Forward Portlist: Display the forward list.

5.1.5 Loopback Detection

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

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

Global config

Loopback Detection Status: enable disable

Detection Interval: seconds(1-1000)

Automatic Recovery Time: detection times(1-100) Apply

Web Refresh Status: enable disable

Web Refresh Interval: seconds(3-100)

Port config

Port Select

Select	Port	Status	Operation mode	Recovery mode	Loop status	Block status	Block VLAN	LAG
<input type="checkbox"/>		disable ▾	Alert ▾	Auto ▾				
<input type="checkbox"/>	1	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	2	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	3	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	4	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	5	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	6	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	7	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	8	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	9	Disable	Alert	Auto	---	---	---	---
<input type="checkbox"/>	10	Disable	Alert	Auto	---	---	---	---

Apply
Manual Recover
Help

Figure 5-6 Loopback Detection Config

The following entries are displayed on this screen:

➤ Global Config

LoopbackDetection Status:

Enable Loopback Detection function globally.

Detection Interval:

Set the interval of sending loopback detection packets.

The valid values are 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/VLAN in Auto Recovery mode can automatically recover to normal status.

The valid values are from 1 to 100 seconds and the default value is 3 seconds.

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 3 seconds.
➤ Port Config	
Port Select:	Click the Select button to quick-select the corresponding port based on the port number you entered.
Select:	Select the desired port for Loopback Detection configuration. It is multi-optional.
Port:	Displays the port number.
Status:	Enable or disable Loopback Detection function for the port.
Operation Mode:	Select the mode how the switch processes the detected loops. <ul style="list-style-type: none"> • Alert: When a loop is detected, the switch will send a trap message and generate an entry on the log file. It is the default setting. • Port Based: When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will totally block the port on which the loop is detected and no packets can pass through the port. • VLAN Based: When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.
Recovery Mode:	If you select Port Based or VLAN Based as the operation mode, you also need to configure the recovery mode for the blocked port/VLAN: <ul style="list-style-type: none"> • Auto: The blocked port/VLAN 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/VLAN. Click the Recover button to release the corresponding port/VLAN.
Loop Status:	Displays whether a loop is detected on the port.
Block Status:	Displays whether the port is blocked.
Block VLAN:	View the information about the blocked VLAN.
LAG:	Displays the LAG number the port belongs to.
Manual Recover:	Manually remove the block status of selected ports.

**Note:**

1. Recovery Mode is not selectable when Alert is chosen in Operation Mode.
2. Loopback Detection must coordinate with storm control.

5.2 LAG

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

For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes **STP, QoS, GVRP, VLAN, port attributes, MAC Address Learning mode** and other associated settings. The further explains are as following:

- If the ports, which are enabled for the **GVRP, 802.1Q VLAN, Voice VLAN, STP, QoS, Port Isolation, DHCP Snooping** and **Port Configuration (Speed, Flow Control)**, are in a LAG, their configurations should be the same.
- The ports, which are enabled for the **Port Security, Port Mirror, MAC Address Filtering, Static MAC Address Binding, 802.1X Authentication, IP Source Guard**, and **half-duplex** cannot be added to the LAG.
- It's not suggested to add the ports with **ARP Inspection** and **DoS Defend** enabled to the LAG.

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

**Tips:**

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

Depending on different aggregation modes, aggregation groups fall into two types: **Static LAG** and **LACP Config**. The LAG function is implemented on the **LAG Table, Static LAG** and **LACP Config** configuration pages.

5.2.1 LAG Table

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

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

Select	Group Number	Description	Member	Operation
No trunk exists.				

Figure 5-7 LAG Table

The following entries are displayed on this screen:

➤ **Global Config**

Hash Algorithm:

Select the applied scope of aggregate hash arithmetic, which results in choosing a port to transfer the packets.

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

➤ **LAG Table**

Select:

Select the desired LAG. It is multi-optional.

Group Number:

Displays the LAG number here.

Description:

Displays the description of LAG.

Member:

Displays the LAG member.

Operation:

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

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

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

Detail Info	
Group Number:	LAG1
LAG Type:	Static
Port Status:	Enable
Rate:	1000MFullDuplex
Port mirror:	Disable
Ingress Bandwidth (bps):	--
Egress Bandwidth (bps):	--
Broadcast Control (bps):	--
Multicast Control (bps):	--
UL Control (bps):	--
QoS Priority:	CoS 0
Join VLAN:	1

[Back](#)

Figure 5-8 Detail Information

5.2.2 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.

LAG Config	
Group Number:	<input type="text" value="LAG1"/>
Description:	<input type="text"/>

Member Port					
<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10		

[Apply](#) [Clear](#) [Help](#)

Figure 5-9 Static LAG Config

The following entries are displayed on this screen:

➤ **LAG Config**

- Group Number:** Select a Group Number for the LAG.
- Description:** Give a description to the LAG for identification.

➤ **LAG Table**

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



Tips:

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

5.2.3 LACP Config

LACP (Link Aggregation Control Protocol) is defined in IEEE802.3ad/802.1ax and enables the dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. The switch can dynamically group similarly configured ports into a single logical link, which will highly extend the bandwidth and flexibly balance the load.

With the LACP feature enabled, the port will notify its partner of the system priority, system MAC, port priority, port number and operation key (operation key is determined by the physical properties of the port, upper layer protocol and admin key). The device with higher priority will lead the aggregation and disaggregation. System priority and system MAC decide the priority of the device. The smaller the system priority, the higher the priority of the device is. With the same system priority, the device owning the smaller system MAC has the higher priority. The device with the higher priority will choose the ports to be aggregated based on the port priority, port number and operation key. Only the ports with the same operation key can be selected into the same aggregation group. In an aggregation group, the port with smaller port priority will be considered as the preferred one. If the two port priorities are equal, the port with smaller port number is preferred. After an aggregation group is established, the selected ports can be aggregated together as one port to transmit packets.

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

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

Global Config

System Priority: (0 - 65535)

LACP Config

Select	Port	Admin Key	Port Priority (0-65535)	Mode	Status	LAG
<input type="checkbox"/>		<input style="width: 50px;" type="text"/>	<input style="width: 50px;" type="text"/>	Passive <input type="button" value="v"/>	Disable <input type="button" value="v"/>	
<input type="checkbox"/>	1	1	32768	Passive	Disable	---
<input type="checkbox"/>	2	1	32768	Passive	Disable	---
<input type="checkbox"/>	3	1	32768	Passive	Disable	---
<input type="checkbox"/>	4	1	32768	Passive	Disable	---
<input type="checkbox"/>	5	1	32768	Passive	Disable	---
<input type="checkbox"/>	6	1	32768	Passive	Disable	---
<input type="checkbox"/>	7	1	32768	Passive	Disable	---
<input type="checkbox"/>	8	1	32768	Passive	Disable	---
<input type="checkbox"/>	9	1	32768	Passive	Disable	---
<input type="checkbox"/>	10	1	32768	Passive	Disable	---

Figure 5-10 LACP Config

The following entries are displayed on this screen:

➤ **Global Config**

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

➤ **LACP Config**

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

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

Port: Displays the port number.

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

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

Status: Enable or disable the LACP feature for your selected port.

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

5.3 Traffic Monitor

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

5.3.1 Traffic Summary

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

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

Auto Refresh

Auto Refresh: Enable Disable

Refresh Rate: sec (3-300)

Traffic Summary

Port	Packets Rx	Packets Tx	Octets Rx	Octets Tx	Statistics
1	38,213	13,007	6,500,501	7,556,404	Statistics
2	0	0	0	0	Statistics
3	0	0	0	0	Statistics
4	0	0	0	0	Statistics
5	0	0	0	0	Statistics
6	0	0	0	0	Statistics
7	0	0	0	0	Statistics
8	0	0	0	0	Statistics
9	0	0	0	0	Statistics
10	0	0	0	0	Statistics

Figure 5-11 Traffic Summary

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Allows you to Enable or disable refreshing the Traffic Summary automatically.

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

➤ **Traffic Summary**

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

Port: Displays the port number.

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

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

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

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

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

5.3.2 Traffic Statistics

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

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

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Rate: sec (3-300)

Statistics

Received		Sent	
Broadcast	24,547	Broadcast	0
Multicast	1,040	Multicast	155
Unicast	12,717	Unicast	12,879
Alignment Errors	0	Collisions	0
UndersizePkts	0		
Pkts64Octets	23,132		
Pkts65to127Octets	2,611		
Pkts128to255Octets	6,543		
Pkts256to511Octets	921		
Pkts512to1023Octets	5,097		
PktsOver1023Octets	0		

Refresh
Help

Figure 5-12 Traffic Statistics

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Allows you to Enable or disable refreshing the Traffic Summary automatically.

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

➤ **Statistics**

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

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

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

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

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

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

Alignment Errors: 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.

5.4 MAC Address

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

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

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

Table 5-1 Types and features of Address Table

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

5.4.1 Address Table

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

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

Search Option

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Port:

Type: All Static Dynamic Filtering

MAC Address	VLAN ID	Port	Type	Aging Status
00-0A-EB-13-12-DB	1	1	Dynamic	Aging
00-0A-EB-13-23-7B	1	1	Dynamic	Aging
00-0A-EB-13-23-97	1	1	Dynamic	Aging
00-14-78-00-00-00	1	1	Dynamic	Aging
00-14-78-A8-CB-BE	1	1	Dynamic	Aging
00-19-66-35-E1-B0	1	1	Dynamic	Aging
30-B5-C2-57-32-96	1	1	Dynamic	Aging

Total MAC Address: 7

Figure 5-13 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 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.

➤ **Address Table**

- MAC Address:** Displays the MAC address learned by the switch.
- VLAN ID:** Displays the corresponding VLAN ID of the MAC address.
- Port:** Displays the corresponding Port number of the MAC address.
- Type:** Displays the Type of the MAC address.
- Aging Status:** Displays the Aging status of the MAC address.

5.4.2 Static Address

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

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

Create Static Address

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Port:

Search Option

Search Option:

Static Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
<input type="checkbox"/>			<input type="text" value="Port 1"/> <input type="button" value="v"/>		

Total MAC Address: 0

Figure 5-14 Static Address

The following entries are displayed on this screen:

➤ **Create Static Address**

- MAC Address:** Enter the static MAC Address to be bound.
- VLAN ID:** Enter the corresponding VLAN ID of the MAC address.
- Port:** Select a port from the pull-down list 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**

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 be 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.
4. This static MAC address bound function is not available if the 802.1X feature is enabled.

5.4.3 Dynamic Address

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

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

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

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

Aging Config

Auto Aging: Enable Disable

Aging Time: sec (10-630, default: 300)

Search Option

Search Option:

Dynamic Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
<input type="checkbox"/>	00-0A-EB-13-12-DB	1	1	Dynamic	Aging

Total MAC Address: 1

Figure 5-15 Dynamic Address

The following entries are displayed on this screen:

➤ **Aging Config**

Auto Aging: Allows you to Enable or disable the Auto Aging feature.

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

➤ **Search Option**

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

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

➤ **Dynamic Address Table**

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

MAC Address: Displays the dynamic MAC Address.

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

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

Type: Displays the Type of the MAC address.

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

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



Tips:

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

5.4.4 Filtering Address

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

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

Create Filtering Address

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Search Option

Search Option:

Filtering Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
<input type="button" value="All"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

Total MAC Address: 0

Figure 5-16 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.

5.5 L2PT

L2PT (Layer 2 Protocol Tunneling) is a feature for service providers to transmit packets from different customers across their ISP networks and maintain Layer 2 protocol configurations of each customer. The supported Layer 2 protocols are STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) and PVST+(Per VLAN Spanning Tree Plus).

When L2PT is enabled and the switch receives the specified Layer 2 protocol packets from the UNI port, the switch encapsulates these packets with a special MAC address and sends them across the service-provider network through the NNI port. The devices in the ISP network do not process these packets but forward them as normal packets. The switch on the outbound side of the ISP network receives these packets on its NNI port and restore their MAC address to their original Layer 2 protocol destination MAC address.

The L2PT protocol is usually used with VLAN VPN feature. Thus the NNI ports that connecting to the ISP network are configured as VPN Up-link ports.

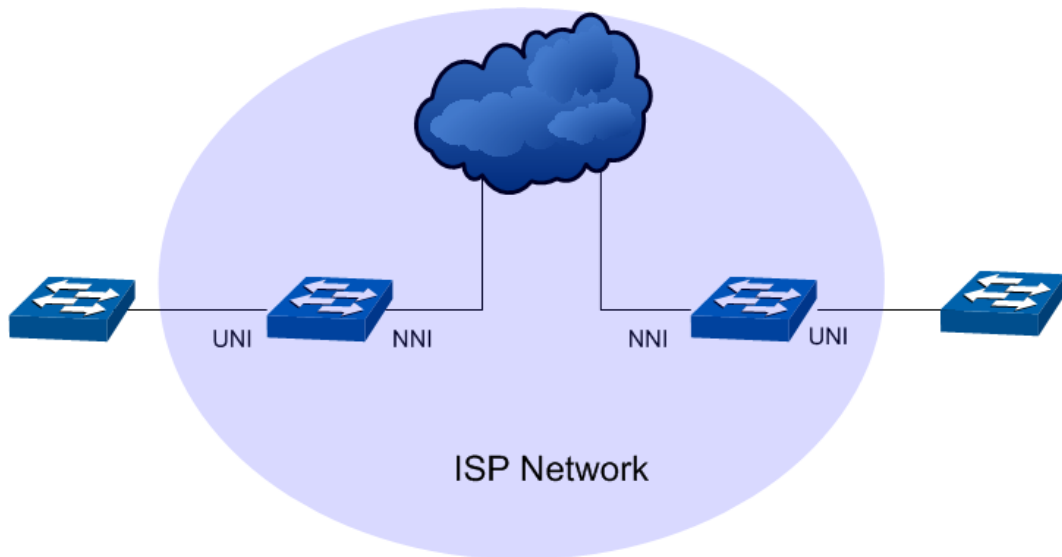


Figure 5-1 A Typical L2PT Topology

5.5.1 L2PT Config

Choose the menu **Switching**→**L2PT**→**L2PT Config** to load the following page.

Global Config

Layer 2 Protocol Tunneling: Enable Disable Apply

Port Config

Select	Port	Type	Protocol	Threshold (0-1000)	LAG
<input type="checkbox"/>		<input type="text" value="NONE"/> ▼	<input type="text" value="---/---/---/---/---/"/> ▼	<input type="text" value=""/>	
<input type="checkbox"/>	1	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	2	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	3	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	4	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	5	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	6	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	7	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	8	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	9	NONE	---/---/---/---/---/	---/---/---/---/---/	---
<input type="checkbox"/>	10	NONE	---/---/---/---/---/	---/---/---/---/---/	---

Apply
Help

Figure 5-2 L2PT Config

Configuration Procedure:

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

Entry Explanation:

UNIT:1/LAGS:

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

Select: Specify the port(s) to configure its L2PT feature. It is multi-optional.

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

- **None:** Disable the L2PT on this port.
- **UNI:** Specify the port's type as UNI if it is connecting to the user's local network.
- **NNI:** Specify the port's type as NNI if it is connecting to the ISP network.

Protocol: Specify the layer 2 protocol types of the packets that can be transparently transmitted on the selected port:

- **STP:** Enable protocol tunneling for the STP packets.
- **GVRP:** Enable protocol tunneling for the GVRP packets.
- **01000CCCCC:** Enable protocol tunneling for the CDP/VTP/PAgP/UDLD packets with their destination MAC address as 01-00-0C-CC-CC-CC.
- **01000CCCCCD:** Enable protocol tunneling for the PVST+ packets with the destination MAC address as 01-00-0C-CC-CC-CD.
- **LACP:** Enable protocol tunneling for the LACP packets.
- **ALL:** All the above layer 2 protocols are supported for tunneling.

Threshold (0-1000) Configure the threshold for packets-per-second accepted for encapsulation. Packets beyond the threshold will be dropped. If no protocol is specified, the threshold applies to each Layer 2 protocol types. The valid ranges are from 0 to 1000.

LAG: Displays the port's aggregation group.

[Return to CONTENTS](#)

Chapter 6 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.

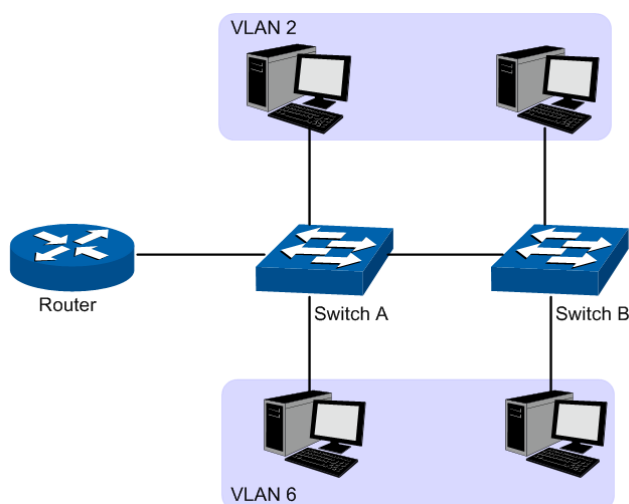


Figure 6-1 VLAN implementation

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

1. Broadcasts are confined to VLANs. This decreases bandwidth utilization and improves network performance.
2. Network security is improved. VLANs cannot communicate with one another directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 switches are used.
3. Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you 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.

6.1 802.1Q VLAN

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

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

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

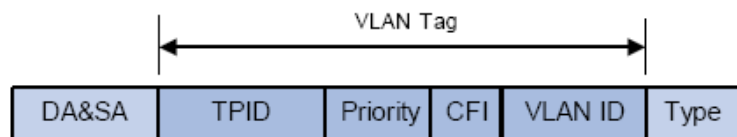


Figure 6-2 Format of VLAN Tag

1. TPID: TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100.
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, and the egress rule of the port 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. When the packets are forwarded by the TRUNK port, its VLAN tag will not be changed.
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 VLAN the port belongs to.

➤ **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.

Port Type	Receiving Packets		Forwarding Packets
	Untagged Packets	Tagged Packets	
Access	When untagged packets are received, the port will add the default VLAN tag, i.e. the PVID of the ingress port, to the packets.	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.	The packet will be forwarded after removing its VLAN tag.
Trunk		If the VID of packet is allowed by the port, the packet will be received. If the VID of packet is forbidden by the port, the packet will be dropped.	The packet will be forwarded with its current VLAN 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 6-1 Relationship between Port Types and VLAN Packets Processing

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

6.1.1 VLAN Config

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

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

VLAN Table				
Select	VLAN ID	Description	Members	Operation
<input type="checkbox"/>	1	Default VLAN	1-10	Edit Detail

VLAN ID

Total VLAN: 1

Figure 6-3 VLAN Table

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

The following entries are displayed on this screen:

➤ **VLAN Table**

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

- 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.

VLAN Create

VLAN ID: (2-4094)

Description: (16 characters maximum)

VLAN Members

	Port				
	Port				<input style="width: 50px;" type="text"/> <input type="button" value="Select"/>
Select	Port	Link Type	Egress Rule	LAG	
<input type="checkbox"/>	1	ACCESS	UNTAG	---	
<input type="checkbox"/>	2	ACCESS	UNTAG	---	
<input type="checkbox"/>	3	ACCESS	UNTAG	---	
<input type="checkbox"/>	4	ACCESS	UNTAG	---	
<input type="checkbox"/>	5	ACCESS	UNTAG	---	
<input type="checkbox"/>	6	ACCESS	UNTAG	---	
<input type="checkbox"/>	7	ACCESS	UNTAG	---	
<input type="checkbox"/>	8	ACCESS	UNTAG	---	
<input type="checkbox"/>	9	ACCESS	UNTAG	---	
<input type="checkbox"/>	10	ACCESS	UNTAG	---	

Figure 6-4 Create or Modify 802.1Q VLAN

The following entries are displayed on this screen:

➤ **VLAN Config**

- VLAN ID:** Enter the ID number of VLAN.
- Description:** Give a description to the VLAN for identification.
- Check:** Click the **Check** button to check whether the VLAN ID you entered is valid or not.

➤ **VLAN Members**

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

Select: Select the desired port to be a member of VLAN or leave it blank. It's multi-optional.

Port: Displays the port number.

Link Type: Displays the Link Type of the port. It can be reset on Port Config screen.

Egress Rule: Select the Egress Rule for the VLAN port member. The default egress rule is UNTAG.

- **TAG:** All packets forwarded by the port are tagged. The packets contain VLAN information.
- **UNTAG:** Packets forwarded by the port are untagged.

LAG: Displays the LAG to which the port belongs.

6.1.2 Port Config

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

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

The screenshot shows the 'VLAN Port Config' interface. At the top, there is a 'Port' input field and a 'Select' button. Below this is a table with columns: Select, Port, Link Type, PVID, LAG, and VLAN. The 'Link Type' column has a dropdown menu currently set to 'ACCESS'. The table lists ports 1 through 10, all with 'ACCESS' link type and '1' PVID. Each row has a 'Select' checkbox and a 'Detail' link. At the bottom of the table are 'Apply' and 'Help' buttons.

Select	Port	Link Type	PVID	LAG	VLAN
<input type="checkbox"/>		ACCESS			
<input type="checkbox"/>	1	ACCESS	1	--	Detail
<input type="checkbox"/>	2	ACCESS	1	--	Detail
<input type="checkbox"/>	3	ACCESS	1	--	Detail
<input type="checkbox"/>	4	ACCESS	1	--	Detail
<input type="checkbox"/>	5	ACCESS	1	--	Detail
<input type="checkbox"/>	6	ACCESS	1	--	Detail
<input type="checkbox"/>	7	ACCESS	1	--	Detail
<input type="checkbox"/>	8	ACCESS	1	--	Detail
<input type="checkbox"/>	9	ACCESS	1	--	Detail
<input type="checkbox"/>	10	ACCESS	1	--	Detail

Figure 6-5 802.1Q VLAN – Port Config

The following entries are displayed on this screen:

➤ **VLAN Port Config**

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

- Select:** Select the desired port 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, and the egress rule of the port is TAG. The PVID can be set as the VID number of any VLAN the port belongs to.
 - **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 VLAN the port belongs to.
- 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.

VLAN of Port 1		
		VLAN ID <input type="text"/> <input type="button" value="Select"/>
VLAN ID	VLAN Name	Operation
1	Default VLAN	Remove

Figure 6-6 View the Current VLAN of Port

The following entries are displayed on this screen:

➤ **VLAN of Port**

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

6.2 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.

6.2.1 MAC VLAN

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

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

Figure 6-7 Create and View MAC VLAN

The following entries are displayed on this screen:

➤ **VLAN Table**

MAC Address: Enter the MAC address.

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

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

➤ **MAC VLAN Table**

MAC Select: Click the **Select** button to quick-select the corresponding entry based on the MAC address you entered.

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

MAC Address: Displays the MAC address.

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

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

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

Configuration Procedure:

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

3	Create MAC VLAN.	Required. On the VLAN→MAC VLAN page, create the MAC VLAN. For the device in a MAC VLAN, it's required to set its connected port of switch to be a member of this VLAN so as to ensure the normal communication.
---	------------------	--

6.3 Protocol VLAN

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

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

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

Table 6-2 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.

6.3.1 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.

Protocol Group Table				
Select	Protocol	VLAN ID	Member	Operation
No entry in the group table.				
<input type="button" value="Create"/> <input type="button" value="All"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

Figure 6-8 Create Protocol VLAN

The following entries are displayed on this screen:

➤ **Protocol Group Table**

- Select:** Select the desired entry. It is multi-optional.
- Protocol Name:** Displays the protocol of the protocol group.
- VLAN ID:** Displays the corresponding VLAN ID of the protocol group.
- Member:** Displays the member of the protocol group.
- Operate:** Click the **Edit** button to modify the settings of the entry. And click the **Apply** button to apply your settings.

6.3.2 Protocol Group

On this page, you can configure the Protocol Group.

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

Protocol Group Config	
Protocol:	<input type="text" value="IP"/> (802.3Ethernet,0800)
VLAN ID:	<input type="text"/> (1-4094)

Protocol Group Member					
<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10		
<input type="button" value="Apply"/> <input type="button" value="All"/> <input type="button" value="Clear"/> <input type="button" value="Help"/>					

Figure 6-9 Create and View Protocol Template

The following entries are displayed on this screen:

➤ **Protocol Group**

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

➤ **Protocol Template Table**

Select your desired port for Protocol VLAN Group.

6.3.3 Protocol Template

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

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

The screenshot shows a web interface for creating and viewing protocol templates. At the top is a 'Create Protocol Template' section with three input fields: 'Protocol Name' (with a note '(8 characters maximum)'), 'Ether Type' (with a note '(4 Hex integers)'), and 'Frame Type' (a dropdown menu currently showing 'Ethernet II'). A 'Create' button is positioned to the right of the 'Ether Type' field. Below this is a 'Protocol Template Table' section containing a table with five rows of existing templates. Each row has a 'Select' checkbox, an 'ID', a 'Protocol Name', an 'Ether Type', and a 'Frame Type'. At the bottom of the table are three buttons: 'All', 'Delete', and 'Help'.

Select	ID	Protocol Name	Ether Type	Frame Type
<input type="checkbox"/>	1	IP	0800	802.3Ethernet
<input type="checkbox"/>	2	ARP	0806	802.3Ethernet
<input type="checkbox"/>	3	RARP	8035	802.3Ethernet
<input type="checkbox"/>	4	IPX	8137	SNAP
<input type="checkbox"/>	5	AT	809B	SNAP

Figure 6-10 Create and View Protocol Template

The following entries are displayed on this screen:

➤ **Create Protocol Template**

- Protocol Name:** Give a name for the Protocol Template.
- Frame Type:** Select a Frame Type for the Protocol Template.
- Ether Type:** Enter the Ethernet protocol type field in the protocol template.
- DSAP:** Enter the DSAP field when selected LLC.
- SSAP:** Enter the SSAP field when selected LLC.

➤ **Protocol Template Table**

- Select:** Select the desired entry. It is multi-optional.
- ID** Displays the Protocol Template ID.
- Protocol Name:** Displays the Protocol Name.
- Protocol Type:** Displays the Protocol type.

**Note:**

The Protocol Template bound to VLAN cannot be deleted.

Configuration Procedure:

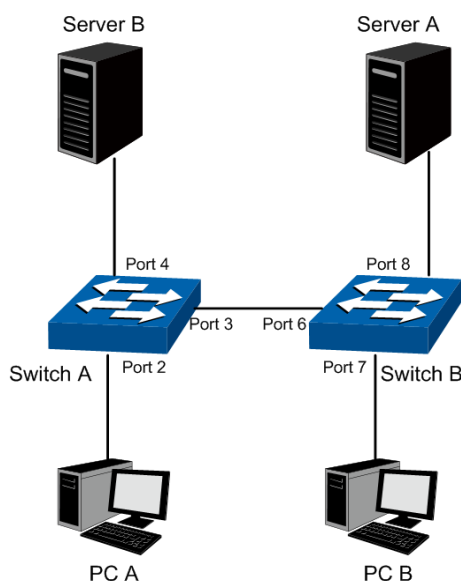
Step	Operation	Description
1	Set the link type for port.	Required. On the VLAN→802.1Q VLAN→Port Config page, set the link type for the port basing on its connected device.
2	Create VLAN.	Required. On the VLAN→802.1Q VLAN→VLAN Config page, click the Create button to create a VLAN. Enter the VLAN ID and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

6.4 Application Example for 802.1Q VLAN

➤ Network Requirements

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

➤ **Network Diagram**



➤ **Configuration Procedure**

- Configure switch A

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

- Configure switch B

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

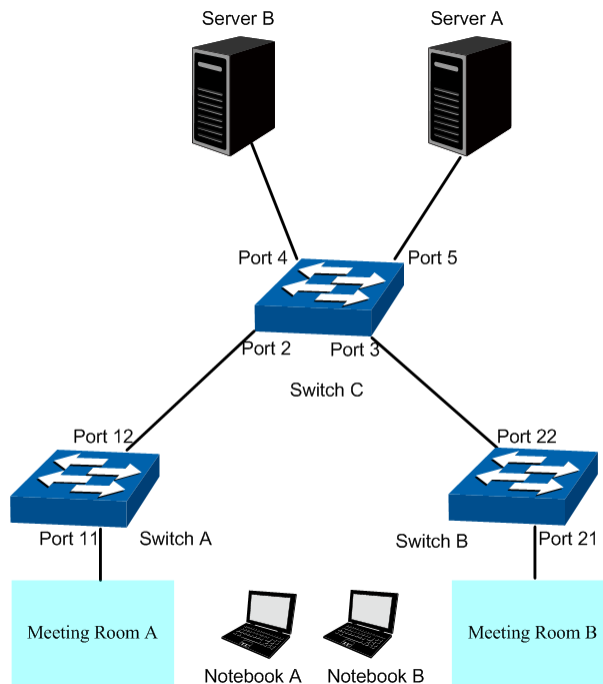
6.5 Application Example for MAC VLAN

➤ **Network Requirements**

- Switch A and switch B are connected to meeting room A and meeting room B respectively, and the two rooms are for all departments;

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

➤ **Network Diagram**



➤ **Configuration Procedure**

- Configure switch A

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

Step	Operation	Description
6	Port Enable	Required. On the VLAN→MAC VLAN→Port Enable page, select and enable Port 11 and Port 12 for MAC VLAN feature.

- Configure switch B

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

- Configure switch C

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

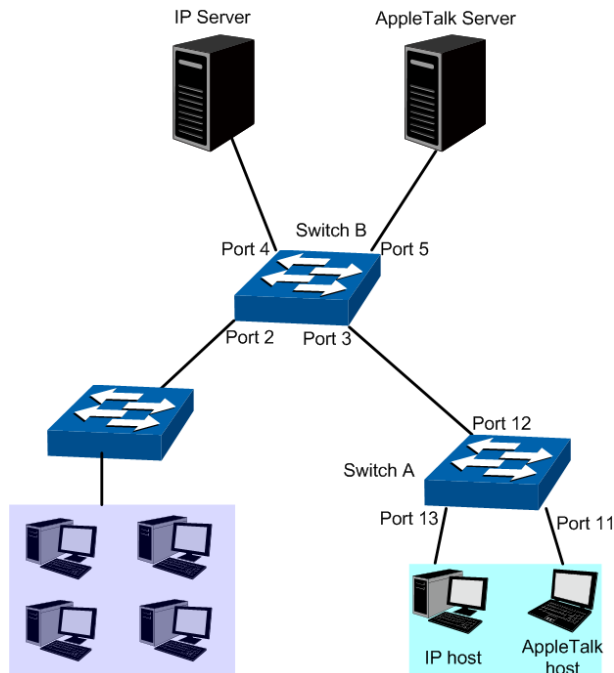
6.6 Application Example for Protocol VLAN

➤ Network Requirements

- Department A is connected to the company LAN via Port12 of switch A;
- Department A has IP host and AppleTalk host;

- IP host, in VLAN10, is served by IP server while AppleTalk host is served by AppleTalk server;
- Switch B is connected to IP server and AppleTalk server.

➤ **Network Diagram**



➤ **Configuration Procedure**

- Configure switch A

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

- Configure switch B

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

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

6.7 VLAN VPN

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

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

1. Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.
2. Saves public network VLAN ID resource.
3. You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
4. When the network of the Internet Service Provider is upgraded, the user's network with a relative independence can still work normally without changing the current configurations.

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

The position of the TPID field in an Ethernet packet is the same as the position of the protocol type field in the packet without VLAN Tag. Thus, to avoid confusion happening when the switch

forwards or receives a packet, you must not configure the following protocol type values listed in the following table as the TPID value.

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

Table 6-3 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.

6.7.1 VPN Config

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

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

Global Config

VPN Mode: Enable Disable

Global TPID: (4 Hex integers)

VPN Up-link Ports

1 2 3 4 5 6
 7 8 9 10

Port Config

Port

Select	Port	Missdrop	LAG
<input type="checkbox"/>		disable ▾	
<input type="checkbox"/>	1	Disable	---
<input type="checkbox"/>	2	Disable	---
<input type="checkbox"/>	3	Disable	---
<input type="checkbox"/>	4	Disable	---
<input type="checkbox"/>	5	Disable	---
<input type="checkbox"/>	6	Disable	---
<input type="checkbox"/>	7	Disable	---
<input type="checkbox"/>	8	Disable	---
<input type="checkbox"/>	9	Disable	---
<input type="checkbox"/>	10	Disable	---

Figure 6-11 VPN Global Config

The following entries are displayed on this screen:

➤ **Global Config**

VPN Mode: Allows you to Enable or disable the VLAN-VPN function.

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

➤ **VPN Up-link Ports**

Select the desired port as the VPN Up-link port. It's required to set the port connected to the operators' backbone networks to be up-link port.

➤ **Port Config**

Enable the VLAN-VPN missdrop function for the desired port. Click Apply.

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

6.7.2 VLAN Mapping

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

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

VLAN Mapping Config

Port:

C VLAN: (1-4094)

SP VLAN: (1-4094)

SP PRI: (0-7)

Description: (16 characters maximum)

VLAN Mapping Table

Select	Port	C VLAN	SP VLAN	PRI	Description	Operation
Not any entries in the table.						

Figure 6-12 Create VLAN Mapping Entry

The following entries are displayed on this screen:

➤ **VLAN Mapping Config**

- Port:** Select the mapping port.
- C VLAN:** Enter the ID number of the Customer VLAN. C VLAN refers to the VLAN to which the packet received by switch belongs.
- SP VLAN:** Enter the ID number of the Service Provider VLAN.
- SP PRI:** Enter the Service Provider Priority.
- Description:** Give a description to the VLAN Mapping entry or leave it blank.

➤ **VLAN Mapping Table**

- Select:** Select the desired entry to edit or delete the corresponding VLAN Mapping entry. It is multi-optional.
- Port:** Displays the mapping port.
- C VLAN:** Displays the ID number of the Customer VLAN. C VLAN refers to the VLAN to which the packet received by switch belongs.
- SP VLAN:** Displays the ID number of the Service Provider VLAN.
- SP PRI:** Displays the Service Provider Priority.

Description:	Displays a description to the VLAN Mapping entry.
Operation:	Click the Edit button to modify the settings of the entry and click the Modify button to apply.

6.8 GVRP

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

➤ GARP

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

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

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

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

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

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

- **LeaveAll Timer:** Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveAll message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

➤ **GVRP**

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

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

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

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

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

Global Config

GVRP: Enable Disable Apply

Port Config

Select	Port	Status	Registration Mode	LeaveAll Timer (centisecond)	Join Timer (centisecond)	Leave Timer (centisecond)	LAG
<input type="checkbox"/>		Disable <input type="button" value="v"/>	Normal <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	1	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	2	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	3	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	4	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	5	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	6	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	7	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	8	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	9	Disable	Normal	1000	20	60	---
<input type="checkbox"/>	10	Disable	Normal	1000	20	60	---

Apply
Help

Figure 6-13 GVRP Config



Note:

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

The following entries are displayed on this screen:

➤ **Global Config**

GVRP: Allows you to Enable or disable the GVRP function.

➤ **Port Config**

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

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

Port: Displays the port number.

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

Registration Mode: Select the Registration Mode for the port.

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

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

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

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

LAG: Displays the LAG to which the port belongs.



Note:

LeaveAll Timer $\geq 10 \times$ Leave Timer, Leave Timer $\geq 2 \times$ Join Timer

Configuration Procedure:

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

[Return to CONTENTS](#)

Chapter 7 Spanning Tree

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

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

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

➤ STP Elements

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

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

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

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

Bridge Priority: The bridge priority can be set to a value in the range of 0–61440. The lower value priority has the higher priority. The switch with the higher priority has more chance to be chosen as the root bridge.

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

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

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

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

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

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

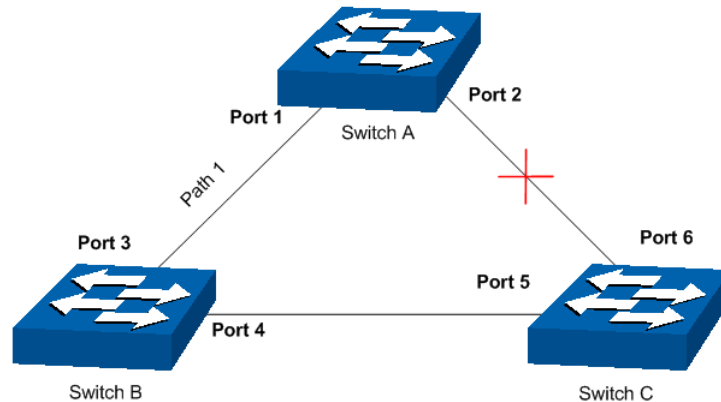


Figure 7-1 Basic STP diagram

➤ STP Timers

Hello Time:

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

Max. Age:

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

Forward Delay:

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

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

➤ BPDU Comparing Principle in STP mode

Assuming two BPDUs: BPDU X and BPDU Y

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

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

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

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

➤ **STP Generation**

- In the beginning

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

- Comparing BPDUs

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

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

Table 7-1 Comparing BPDUs

- Selecting the root bridge

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

- Selecting the root port and designate port

The operation is taken in the following way:

Step	Operation
1	For each switch (except the one chosen as the root bridge) in a network, the port that receives the BPDU with the highest priority is chosen as the root port of the switch.
2	Using the root port BPDU and the root path cost, the switch generates a designated port BPDU for each of its ports. <ul style="list-style-type: none"> ● Root ID is replaced with that of the root port; ● Root path is replaced with the sum of the root path cost of the root port and the path cost between this port and the root port; ● The ID of the designated bridge is replaced with that of the switch; ● The ID of the designated port is replaced with that of the port.
3	The switch compares the resulting BPDU with the BPDU of the desired port whose role you want to determine. <ul style="list-style-type: none"> ● If the resulting BPDU takes the precedence over the BPDU of the port, the port is chosen as the designated port and the BPDU of this port is replaced with the resulting BPDU. The port regularly sends out the resulting BPDU; ● If the BPDU of this port takes the precedence over the resulting BPDU, the BPDU of this port is not replaced and the port is blocked. The port only can receive BPDUs.

Table 7-2 Selecting root port and designated port



Tips :

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

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

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

➤ RSTP Elements

Edge Port: Indicates the port connected directly to terminals.

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

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

Features of MSTP:

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

➤ MSTP Elements

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

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

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

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

The following figure shows the network diagram in MSTP.

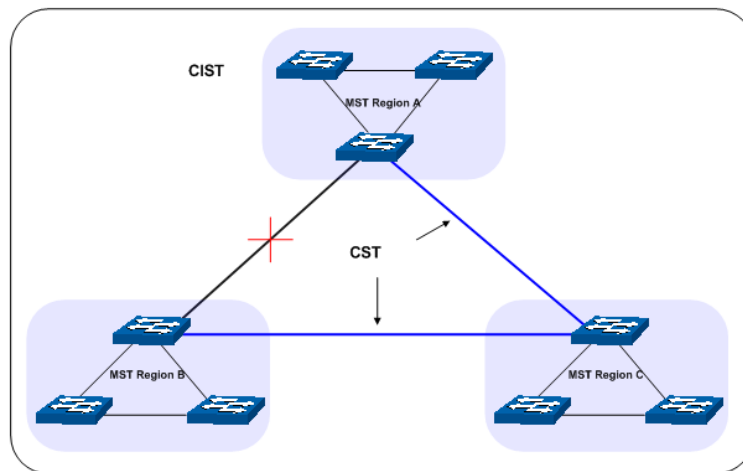


Figure 7-2 Basic MSTP diagram

➤ MSTP

MSTP divides a network into several MST regions. The CST is generated between these MST regions, and multiple spanning trees can be generated in each MST region. Each spanning tree is called an instance. As well as STP, MSTP uses BPDUs to generate spanning tree. The only difference is that the BPDUs for MSTP carry 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 BPDUs as well as learn MAC address.
- Learning: In this status the port can receive/send BPDUs and learn MAC address.
- Blocking: In this status the port can only receive BPDUs.
- Disconnected: In this status the port is not participating in the STP.

➤ Port Roles

In an MSTP, the following roles exist:

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

The following diagram shows the different port roles.

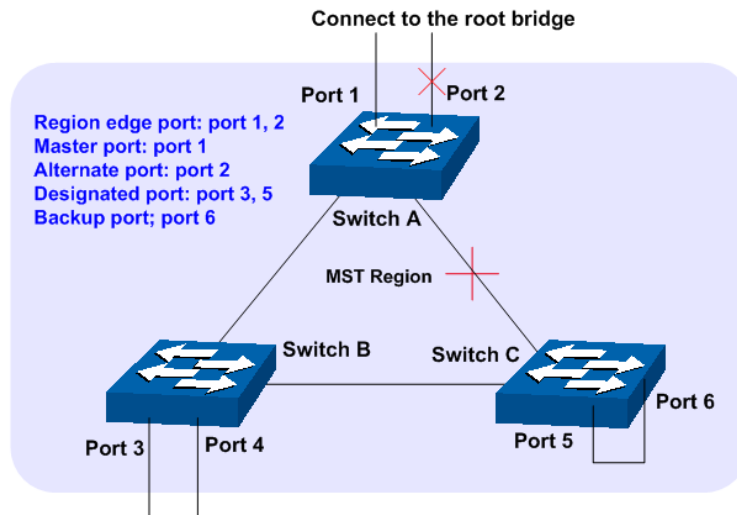


Figure 7-3 Port roles

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

7.1 STP Config

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

7.1.1 STP Config

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

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

Global Config

STP: Enable Disable Apply

Version: STP ▾

Parameters Config

CIST Priority: (0-61440)

Hello Time: sec (1-10)

Max Age: sec (6-40)

Forward Delay: sec (4-30)

TxHoldCount: pps (1-20)

Max Hops: hop (1-40)

Apply
Help

Figure 7-4 STP Config

The following entries are displayed on this screen:

➤ **Global Config**

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

Version: Select the desired STP version on the switch.

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

➤ **Parameters Config**

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

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

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

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

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

Max Hops: Enter a value from 1 to 40 to set the maximum number of hops that occur in a specific region before the BPDU is discarded. The default value is 20 hops.



Note:

1. The forward delay parameter and the network diameter are correlated. A too small forward delay parameter may result in temporary loops. A too large forward delay may cause a network unable to resume the normal state in time. The default value is recommended.
2. An adequate hello time parameter can enable the switch to discover the link failures occurred in the network without occupying too much network resources. A too large hello time parameter may result in normal links being regarded as invalid when packets drop occurred in the links, which in turn result in spanning tree being regenerated. A too small hello time parameter may result in duplicated configuration being sent frequently, which

increases the network load of the switches and wastes network resources. The default value is recommended.

3. A too small max age parameter may result in the switches regenerating spanning trees frequently and cause network congestions to be falsely regarded as link problems. A too large max age parameter result in the switches unable to find the link problems in time, which in turn handicaps spanning trees being regenerated in time and makes the network less adaptive. The default value is recommended.
4. If the TxHold Count parameter is too large, the number of MSTP packets being sent in each hello time may be increased with occupying too much network resources. The default value is recommended.

7.1.2 STP Summary

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

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

STP Summary	
STP Status:	Disable
STP Version:	---
Local Bridge:	---
Root Bridge:	---
External Path Cost:	---
Region Root:	---
Internal Path Cost:	---
Designated Bridge:	---
Root Port:	---
Latest TC Time:	---
TC Count:	0

MSTP Instance Summary	
Instance ID	1 ▾
Instance Status:	Disable
Local Bridge:	---
Region Root:	---
Internal Path Cost:	---
Designated Bridge:	---
Root Port:	---
Latest TC Time:	---
TC Count:	---

Figure 7-5 STP Summary

7.2 Port Config

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

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

The screenshot shows a web interface titled "Port Config". At the top right, there is a "Port" input field with a "Select" button. Below this is a table with the following columns: Select, Port, Status, Priority, ExtPath Cost, IntPath Cost, Edge Port, P2P Link, MCheck, STP Version, Port Role, Port Status, and LAG. The table contains 10 rows of data, all with "Disable" status and "128" priority. Below the table are three buttons: "Apply", "Refresh", and "Help".

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Link	MCheck	STP Version	Port Role	Port Status	LAG
<input type="checkbox"/>		Disable	128	Auto	Auto	Disable	Auto	Unchange	---	---	---	---
<input type="checkbox"/>	1	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	2	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	3	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	4	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	5	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	6	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	7	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	8	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
<input type="checkbox"/>	10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---

Figure 7-6 Port Config

The following entries are displayed on this screen:

➤ **Port Config**

- Port Select:** Click the **Select** button to quick-select the corresponding port based on the port number you entered.
- Select:** Select the desired port for STP configuration. It is multi-optional.
- Port:** Displays the port number of the switch.
- Status:** Select Enable /Disable STP function for the desired port.
- Priority:** Enter a value from 0 to 240 divisible by 16. Port priority is an important criterion on determining if the port connected to this port will be chosen as the root port. The lower value has the higher priority.
- ExtPath Cost:** ExtPath Cost is used to choose the path and calculate the path costs of ports in different MST regions. It is an important criterion on determining the root port. The lower value has the higher priority.
- IntPath Cost:** IntPath Cost is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority.
- Edge Port:** Enable or disable Edge Port. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.
- P2P Link:** Select the P2P link status. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.
- MCheck:** Select Enable to perform MCheck operation on the port. Unchange means no MCheck operation.
- STP Version:** Displays the STP version of the port.

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

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

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



Note:

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

7.3 MSTP Instance

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

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

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

7.3.1 Region Config

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

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

Region Config

Region Name:

Revision: (0-65535)

Figure 7-7 Region Config

The following entries are displayed on this screen:

➤ **Region Config**

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

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

7.3.2 Instance Config

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

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

Instance Table						
					Instance ID <input type="text"/>	<input type="button" value="Select"/>
Select	Instance	Status	Priority	VLAN ID		
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	1	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	2	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	3	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	4	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	5	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	6	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	7	Disable	32768	<input type="button" value="Clear"/>		
<input type="checkbox"/>	8	Disable	32768	<input type="button" value="Clear"/>		
CIST		Enable	32768	1-4094,		

VLAN-Instance Mapping

VLAN ID: (1-4094)

Instance ID: (0-8, 0 is the cist)

Figure 7-8 Instance Config

The following entries are displayed on this screen:

➤ **Instance Table**

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

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

Instance: Displays Instance ID of the switch.

Status: Displays status of the instance.

Priority: Enter the priority of the switch in the instance. It is an important criterion on determining if the switch will be chosen as the root bridge in the specific instance.

VLAN ID: Enter the VLAN ID which belongs to the corresponding instance ID. After modification here, the previous VLAN ID will be cleared and mapped to the CIST.

Clear: Click the **Clear** button to clear up all VLAN IDs from the instance ID. The cleared VLAN ID will be automatically mapped to the CIST.

➤ **VLAN-Instance Mapping**

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

Instance ID: Enter the corresponding instance ID.



Note:

In a network with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. If you want to broadcast packets of 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.

7.3.3 Instance Port Config

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

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

Port Config							
Instance ID		1	Port				Select
Select	Port	Priority	Path Cost	Port Role	Port Status	LAG	
<input type="checkbox"/>							
<input type="checkbox"/>	1	128	Auto	---	---	---	
<input type="checkbox"/>	2	128	Auto	---	---	---	
<input type="checkbox"/>	3	128	Auto	---	---	---	
<input type="checkbox"/>	4	128	Auto	---	---	---	
<input type="checkbox"/>	5	128	Auto	---	---	---	
<input type="checkbox"/>	6	128	Auto	---	---	---	
<input type="checkbox"/>	7	128	Auto	---	---	---	
<input type="checkbox"/>	8	128	Auto	---	---	---	
<input type="checkbox"/>	9	128	Auto	---	---	---	
<input type="checkbox"/>	10	128	Auto	---	---	---	

Figure 7-9 Instance Port Config

The following entries are displayed on this screen:

➤ **Port Config**

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

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

- Select:** Select the desired port to specify its priority and path cost. It is multi-optional.
- Port:** Displays the port number of the switch.
- Priority:** Enter the priority of the port in the instance. It is an important criterion on determining if the port connected to this port will be chosen as the root port.
- Path Cost:** Path Cost is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority.
- Port Role:** Displays the role of the port played in the MSTP Instance.
- Port Status:** Displays the working status of the port.
- LAG:** Displays the LAG number which the port belongs to.



Note:

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

Global configuration Procedure for Spanning Tree function:

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

7.4 STP Security

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

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

7.4.1 Port Protect

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

➤ Loop Protect

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

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

➤ Root Protect

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

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

➤ TC Protect

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

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

➤ BPDU Protect

Ports of the switch directly connected to PCs or servers are configured as edge ports to rapidly transit their states. When these ports receive BPDUs, the system automatically configures these ports as non-edge ports and regenerates spanning trees, which may cause

network topology jitter. Normally these ports do not receive BPDUs, but if a user maliciously attack the switch by sending BPDUs, network topology jitter occurs.

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

➤ **BPDU Filter**

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

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

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

Select	Port	Loop Protect	Root Protect	TC Protect	BPDU Protect	BPDU Filter	LAG
<input type="checkbox"/>		Disable	Disable	Disable	Disable	Disable	
<input type="checkbox"/>	1	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	2	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	3	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	4	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	5	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	6	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	7	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	8	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	9	Disable	Disable	Disable	Disable	Disable	---
<input type="checkbox"/>	10	Disable	Disable	Disable	Disable	Disable	---

Figure 7-10 Port Protect

The following entries are displayed on this screen:

➤ **Port Protect**

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

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

Port: Displays the port number of the switch.

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

Root Protect:	Root Protect is to prevent wrong network topology change caused by the role change of the current legal root bridge.
TC Protect:	TC Protect is to prevent the decrease of the performance and stability of the switch brought by continuously removing MAC address entries upon receiving TC-BPDUs in the STP network.
BPDU Protect:	BPDU Protect is to prevent the edge port from being attacked by maliciously created BPDUs
BPDU Filter:	BPDU Filter is to prevent BPDUs flood in the STP network.
LAG:	Displays the LAG number which the port belongs to.

7.4.2 TC Protect

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

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

TC Protect

TC Threshold: packet (1-100)

TC Protect Cycle: sec (1-10)

Apply

Help

Figure 7-11 TC Protect

The following entries are displayed on this screen:

➤ TC Protect

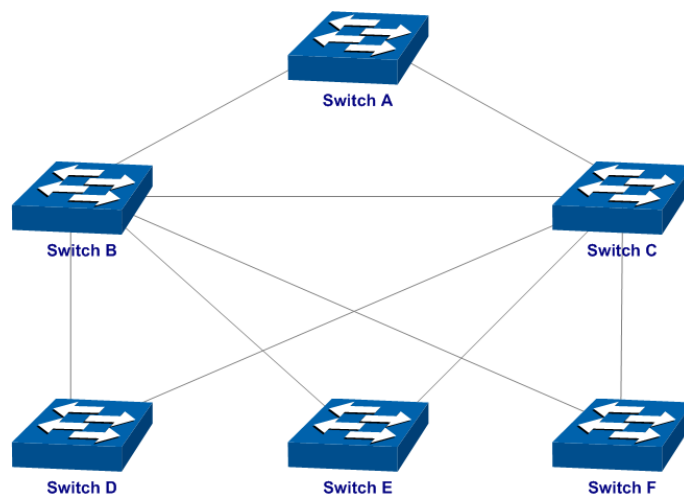
- TC Threshold:** Enter a number from 1 to 100. It is the maximum number of the TC-BPDUs received by the switch in a TC Protect Cycle. The default value is 20.
- TC Protect Cycle:** Enter a value from 1 to 10 to specify the TC Protect Cycle. The default value is 5.

7.5 Application Example for STP Function

➤ Network Requirements

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

➤ **Network Diagram**



➤ **Configuration Procedure**

- Configure switch A:

Step	Operation	Description
1	Configure ports	On VLAN→802.1Q VLAN 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→STP Config→Port Config page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On Spanning Tree→MSTP Instance→Region Config page, configure the region as TP-Link and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On Spanning Tree→MSTP Instance→Instance Config page, configure VLAN-to-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.

- Configure switch B:

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

- Configure switch C:

Step	Operation	Description
1	Configure ports	On VLAN → 802.1Q VLAN page, configure the link type of the related ports as 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 → STP Config → Port Config page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On Spanning Tree → MSTP Instance → Region Config page, configure the region as TP-Link and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On Spanning Tree → MSTP Instance → Instance Config page, configure VLAN-to-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.
5	Configure switch C as the root bridge of Instance 1	On Spanning Tree → MSTP Instance → Instance Config page, configure the priority of Instance 1 to be 4096.

Step	Operation	Description
6	Configure switch C as the root bridge of Instance 2	On Spanning Tree → MSTP Instance → Instance Config page, configure the priority of Instance 2 to be 0.

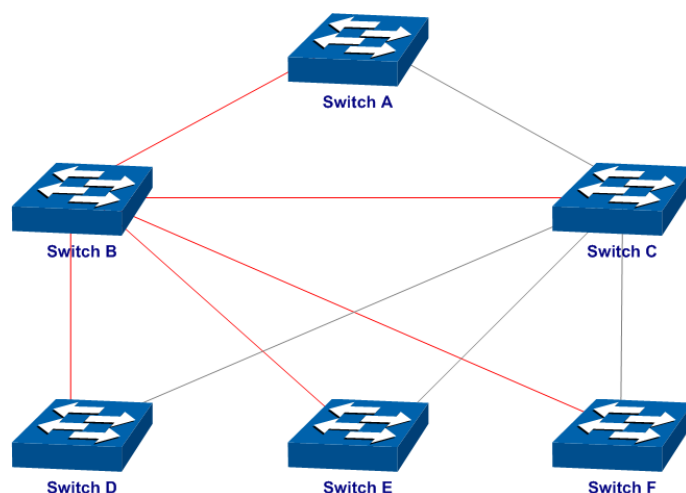
- Configure switch D:

Step	Operation	Description
1	Configure ports	On VLAN → 802.1Q VLAN page, configure the link type of the related ports as 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 → STP Config → Port Config page, enable MSTP function for the port.
3	Configure the region name and the revision of MST region	On Spanning Tree → MSTP Instance → Region Config page, configure the region as TP-Link and keep the default revision setting.
4	Configure VLAN-to-Instance mapping table of the MST region	On Spanning Tree → MSTP Instance → Instance Config page, configure VLAN-to-Instance mapping table. Map VLAN 101, 103 and 105 to Instance 1; map VLAN 102, 104 and 106 to Instance 2.

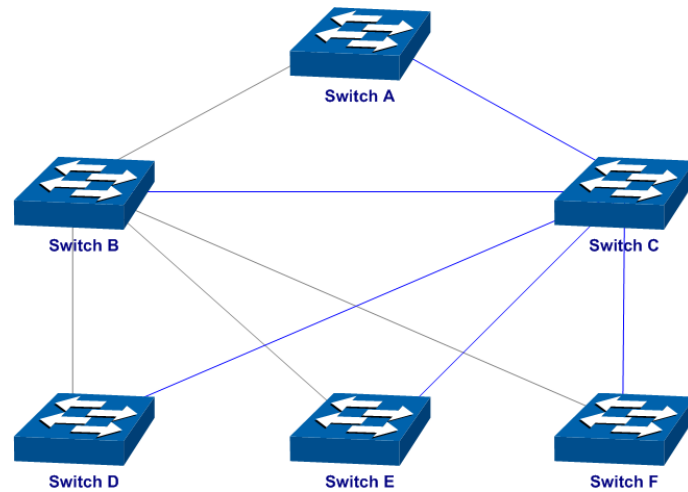
- The configuration procedure for switch E and F is the same with that for switch D.

➤ **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 8 DHCP

DHCP (Dynamic Host Configuration Protocol) is a client-server protocol which is widely used in LAN environments to dynamically assign host IP addresses from a centralized server.

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 8-1 shows you the model.

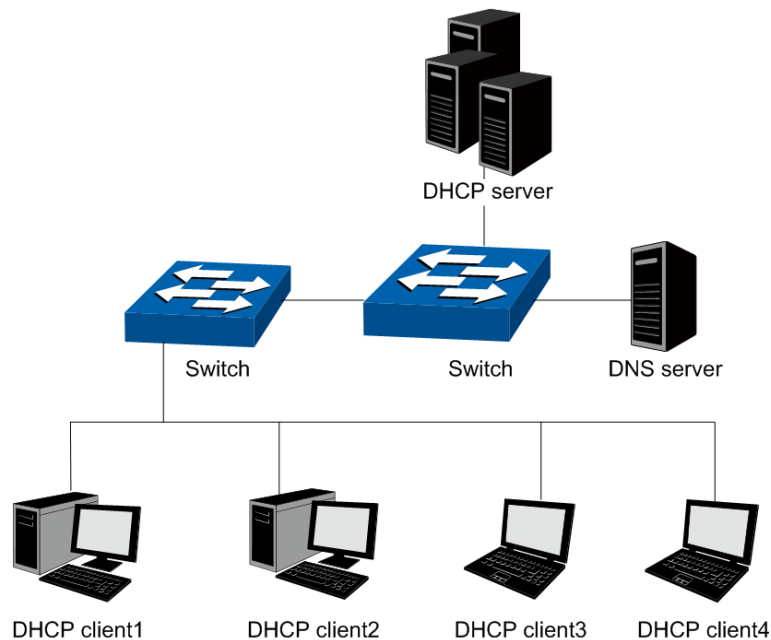


Figure 8-1 DHCP model

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 forever.
- 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.

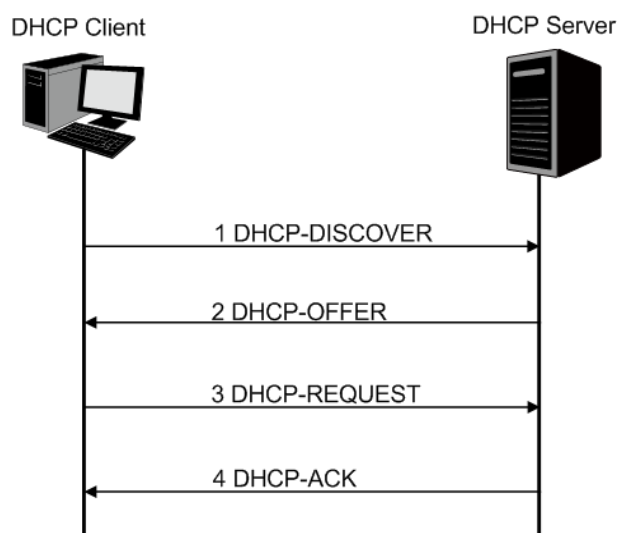


Figure 8-2 The Process of DHCP

- 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 8-1 DHCP model gives the process of DHCP and Figure 8-3 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.

op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (312)			

Figure 8-3 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 8-4 gives the format of options field.

Code (1)	Length(1)
Value (variable)	

Figure 8-4 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 8-1:

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 8-1 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.

8.1 DHCP Relay

The switch supports DHCP relay function, and in this section, DHCP relay function on this switch will be introduced in detail.

➤ Application Environment of DHCP Relay on T2500G-10TS

In DHCP model, DHCP clients broadcast their DHCP requests, which requires the DHCP sever and clients be in the same VLAN. Clients located in different VLANs with the DHCP server are unable to obtain their IP addresses dynamically.

DHCP relay agent solves the problem. With the help of a relay agent, a DHCP client can request an IP address from the DHCP server in another VLAN.

➤ Details of DHCP Relay on T2500G-10TS

A typical application of T2500G-10TS working at DHCP Relay function is shown below. It can be altered to meet the network requirement.

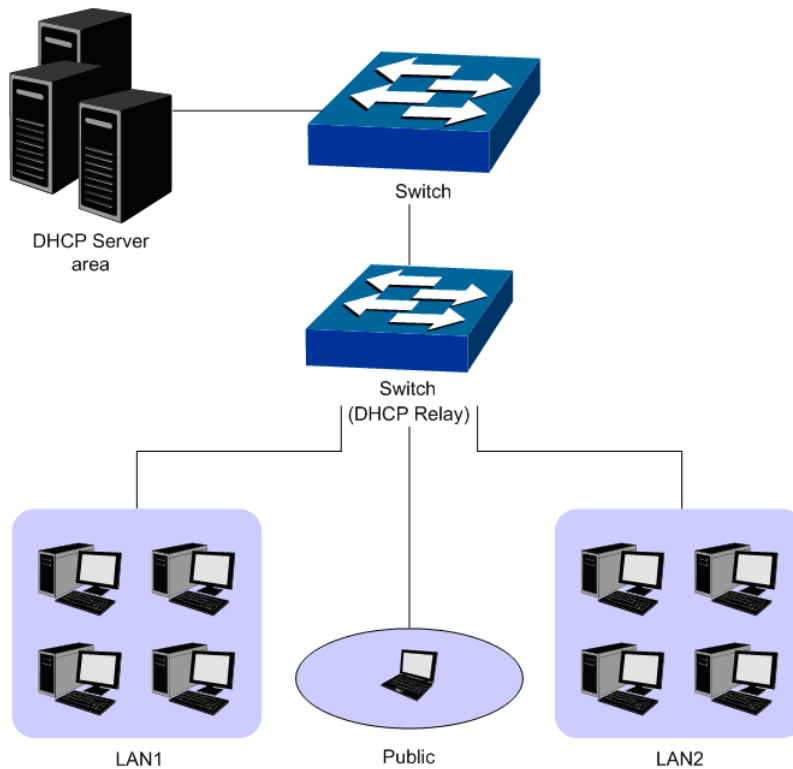


Figure 8-5 DHCP Relay Application

To allow all clients in different VLANs request IP address from one server successfully, the DHCP Relay function can transmit the DHCP packets between clients and server in different VLANs.

- When receiving DHCP-DISCOVER and DHCP-REQUEST packets, the switch will fill the giaddr field with its own management IP address, optionally insert the option 82 information, and then forward the packet to the server.
- When receiving DHCP-OFFER and DHCP-ACK packets from the server, the switch will delete the option 82 information and forward the packets to the port which receives the request.

The process is shown as follows.

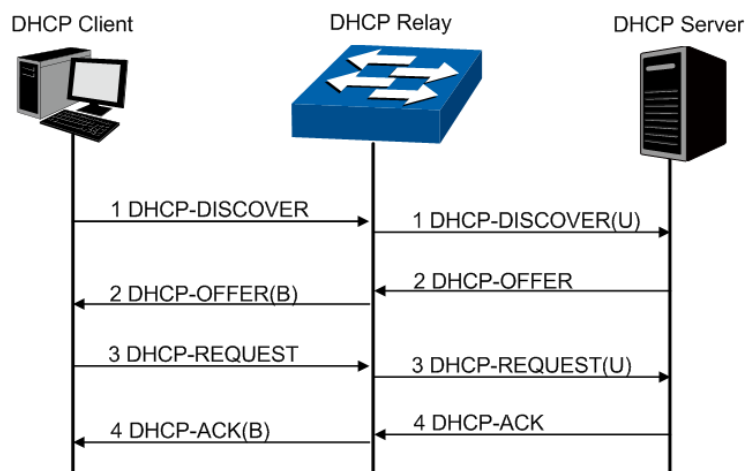


Figure 8-6 DHCP Relay Process

➤ **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.

option82	Length(1)		
sub-option1(1)	Length(1)	VLAN(2)	Port(2)
sub-option1(1)	Length(1)	Hardware address(6)	

Figure8-7 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 VLAN, is implemented on the **Global Config** and **DHCP VLAN Relay** page.

8.1.1 Global Config

Choose the menu **DHCP**→**DHCP Relay**→**Global Config** to load the following page.

Global Config

DHCP Relay: Enable Disable

Option 82 Config

Option 82 Support: Enable Disable

Existed Option 82 Field:

Option 82 Format:

Customization:

Circuit ID:

Remote ID:

Figure 8-8 Global Config

➤ Configuration Procedure:

- 1) In the **Global Config** section, enable DHCP Relay.

DHCP Relay: Enable or disable the DHCP Relay function.

- 2) (Optional) In the **Option 82 Config** section, configure Option 82.

Option 82 Support: Enable or disable the Option 82 feature.

Existed Option 82 Field: Select the operation for the existed Option 82 field of the DHCP request packets from the Host.

- Keep: Indicates to keep the Option 82 field of the packets.
- Replace: Indicates to replace the Option 82 field of the packets with the switch defined one.
- Drop: Indicates to discard the packets including the Option 82 field.

Option 82 Format: Select the format of option 82 sub-option value field.

- Normal: Indicates that the format of sub-option value field is TLV (type-length-value).
- Private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Customization: Enable or disable the switch to define the Option 82 field.

Circuit ID: Enter the sub-option Circuit ID for the customized Option 82 field.

Remote ID: Enter the sub-option Remote ID for the customized Option 82 field.

8.1.2 DHCP VLAN Relay

Choose the menu **DHCP→DHCP VLAN Relay→DHCP VLAN Relay** to load the following page.

Default Relay Agent Interface

Interface ID:

IP Address:

Add DHCP Server Address

VLAN ID: (1-4094)

Server Address: (Format: 192.168.2.1)

DHCP Server List

Select	VLAN ID	IP Address
--------	---------	------------

Figure 8-9 DHCP VLAN Relay

➤ **Configuration Procedure:**

- 1) In the **Default Relay Agent Interface** section, view the default relay agent interface information.
- 2) In the **Add DHCP Server Address** section, specify the VLAN in which the client needs IP addresses and the server address. Click **Add**.

VLAN ID: Specify the VLAN in which the hosts can get IP addresses from the DHCP server.

Server Address: Enter the IP address of the DHCP server.

Configuration Procedure:

Step	Operation	Description
1	Enable DHCP Relay.	Required. On the DHCP→DHCP Relay→Global Config page, enable the DHCP Relay function.
2	Configure Option 82 support.	Optional. On the DHCP→DHCP Relay→Global Config page, configure the Option 82 parameters.
3	Configure DHCP Server.	Required. On the DHCP→DHCP Relay→DHCP VLAN Relay page, specify the DHCP Server with IP address.

[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 Figure 9-1.

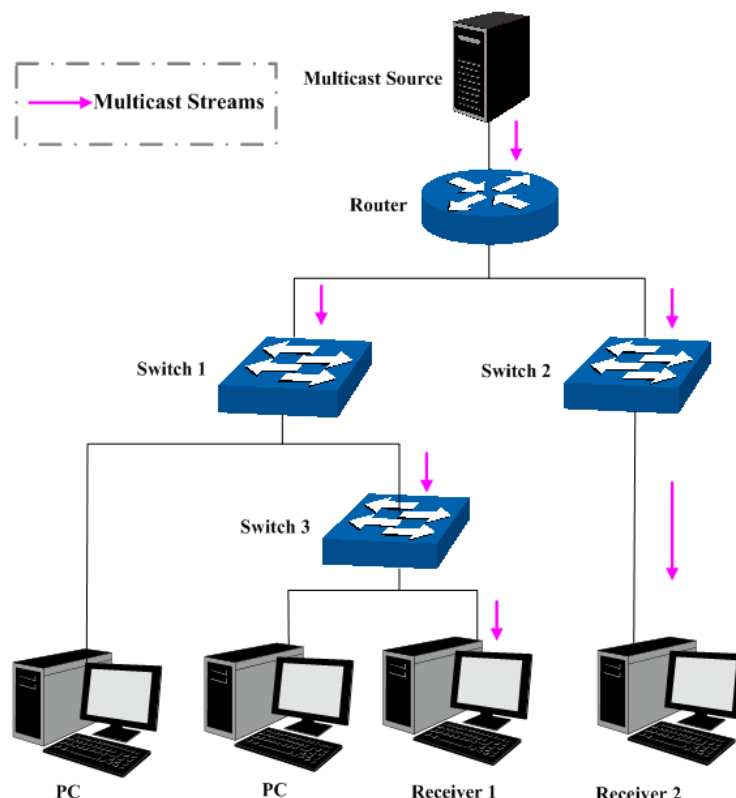


Figure 9-1 Information transmission in the multicast mode

Features of multicast:

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

3. Each user can join and leave the multicast group at any time;
4. Real time is highly demanded and certain packets drop is allowed.

➤ **IPv4 Multicast Address**

1. IPv4 Multicast IP Address:

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

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

Table 9-1 Range of the special multicast IP

2. IPv4 Multicast MAC Address:

When a unicast packet is transmitted in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transmitted in an Ethernet network, the destination is not a receiver but a group with uncertain number of members, so a multicast MAC address, a logical MAC address, is needed to be used as the destination address.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address begins with 01-00-5E while the low-order 23 bits of a multicast MAC address are the low-order 23 bits of the multicast IP address. The mapping relationship is described as Figure 9-2.

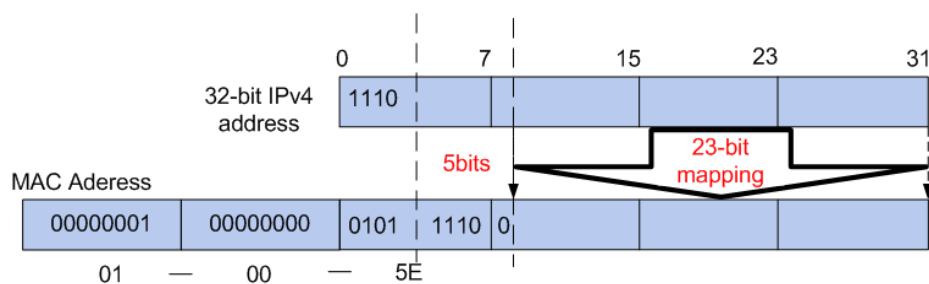


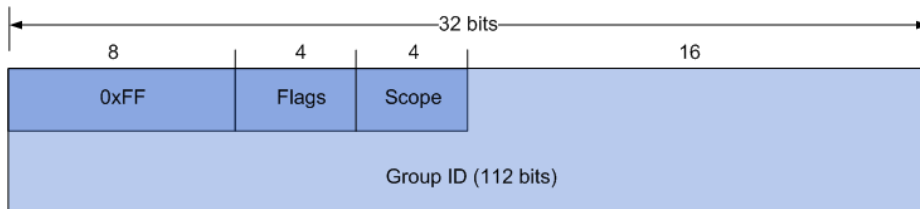
Figure 9-2 Mapping relationship between multicast IPv4 address and multicast MAC address

The high-order 4 bits of the IP multicast address are 1110, identifying the multicast group. Only 23 bits of the remaining low-order 28 bits are mapped to a multicast MAC address. In that way, 5 bits of the IP multicast address is not utilized. As a result, 32 IP multicast addresses are mapped to the same MAC addresses.

➤ **IPv6 Multicast Address**

1. IPv6 Multicast Address

An IPv6 multicast address is an identifier for a group of interfaces, and has the following format:



0xFF at the start of the address identifies the address as being a multicast address.

Flags have 4 bits. The high-order flag is reserved, and must be initialized to 0.

T=0 indicates a permanently-assigned multicast address assigned by the Internet Assigned Numbers Authority (IANA).

T=1 indicates a non-permanently-assigned multicast address.



Scope is a 4-bit value used to limit the scope of the multicast group. The values are as follows:

Value	Indication
0, 3, F	reserved
1	Interface-Local scope
2	Link-Local scope
4	Admin-Local scope
5	Site-Local scope
6, 7, 9-D	unassigned
8	Organization-local scope
E	Global scope

Table 9-2 Indications of the Scope

Reserved Multicast Addresses:

Address	Indication
FF01::1	All interface-local IPv6 nodes
FF02::1	All link-local IPv6 nodes
FF01::2	All interface-local IPv6 routers
FF02::2	All link-local IPv6 routers
FF05::2	All site-local IPv6 routers
FF0X::	X ranges from 0 to F. These multicast addresses are reserved and shall never be assigned to any multicast group.

Table 9-3 Reserved IPv6 Multicast Addresses

The solicited-node multicast address is a multicast group that corresponds to an IPv6 unicast or anycast address. It is usually used for obtaining the Layer 2 link-layer addresses of neighboring nodes within the local-link or applied in IPv6 Duplicate Address Detection. A node is required to join the associated Solicited-Node multicast addresses for all unicast and anycast addresses that have been configured for the node's interfaces.

IPv6 Solicited-Node Multicast Address Format:

FF02:0:0:0:0:1:FFXX:XXXX

The IPv6 solicited-node multicast address has the prefix FF02:0:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address.

2. IPv6 Multicast MAC Address

The high-order 16 bits of an IPv6 multicast MAC address begins with 0x3333 while the low-order 32 bits of an IPv6 multicast MAC address are the low-order 32 bits of the IPv6 multicast IP address. The mapping relationship is described as the following figure:

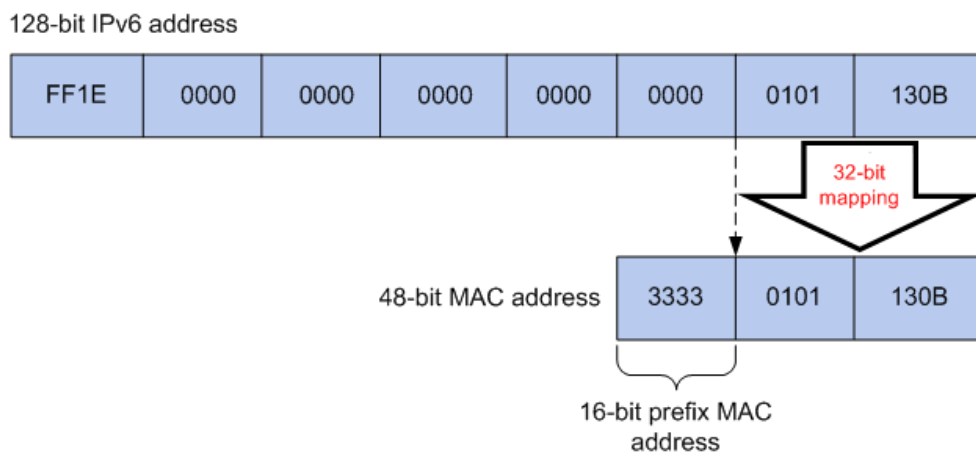


Figure 9-3 Mapping relationship between multicast IPv6 address and multicast IPv6 MAC address

The high-order 16 bits of the IP multicast address are 0x3333, identifying the IPv6 multicast group. The low-order 32 bits of the IPv6 multicast IP address are mapped to the multicast MAC address.

➤ Multicast Address Table

The switch is forwarding multicast packets based on the multicast address table. As the transmission of multicast packets cannot span the VLAN, the first part of the multicast address table is VLAN ID, based on which the received multicast packets are forwarded in the VLAN owning the receiving port. The multicast address table is not mapped to an egress port but a group port list. When forwarding a multicast packet, the switch looks up the multicast address table based on the destination multicast address of the multicast packet. If the corresponding entry cannot be found in the table, the switch will broadcast the packet in the VLAN owning the receiving port. If the corresponding entry can be found in the table, it indicates that the destination address should be a group port list, so the switch will duplicate this multicast data and deliver each port one copy. The general format of the multicast address table is described as Figure 9-4 below.

VLAN ID	Multicast IP	Port
---------	--------------	------

Figure 9-4 Multicast Address Table

➤ **IGMP Snooping**

In the network, the hosts apply to the near router for joining (leaving) a multicast group by sending IGMP (Internet Group Management Protocol) messages. When the up-stream device forwards down the multicast data, the switch is responsible for sending them to the hosts. IGMP Snooping is a multicast control mechanism, which can be used on the switch for dynamic registration of the multicast group. The switch, running IGMP Snooping, manages and controls the multicast group via listening to and processing the IGMP messages transmitted between the hosts and the multicast router, thereby effectively prevents multicast groups being broadcasted in the network.

➤ **MLD Snooping**

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

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

9.1 IGMP Snooping

➤ **IGMP Snooping Process**

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

➤ **IGMP Messages**

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

1. IGMP Query Message

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

When receiving IGMP general query message, the switch will forward them to all other ports in the VLAN owning the receiving port. The receiving port will be processed: if the receiving port is not a router port yet, it will be added to the router port list with its router port time specified; if the receiving port is already a router port, its router port time will be directly reset.

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

2. IGMP Report Message

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

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

3. 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 switch 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 the following pages: **Snooping Config**, **VLAN Config**, **Port Config**, **IP-Range**, **Multicast VLAN**, **Static Multicast IP** and **Packet Statistics**.

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.

Global Config

IGMP Snooping: Enable Disable

Unknown Multicast: Forward Discard

Report Message Suppression: Enable Disable

IGMP Snooping Status

Description	Member
Enabled Port	
Enabled VLAN	

Note:

IGMP Snooping will take effect only when Global Config, Port Config and VLAN Config are all enabled.

Figure 9-5 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:** Select the operation for the switch to process unknown multicast, Forward or Discard.
- Report Message Suppression:** If this function is enabled, the first Report Message from the listener will forward to the router ports while the subsequent Report Message will be suppressed to reduce the IGMP packets.

➤ **IGMP Snooping Status**

- Description:** Displays IGMP Snooping status.

Member: Displays the member of the corresponding status.

9.1.2 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.

The screenshot shows two parts of a web interface. The top part is titled "VLAN Config" and contains several input fields: "VLAN ID:" with a value of 1 and a range of (1-4094); "Router Port Time:" with a value of 300 and a range of sec (60-600, recommended: 300); "Member Port Time:" with a value of 260 and a range of sec (60-600, recommended: 260); "Leave Time:" with a value of 1 and a range of sec (1-30, recommended: 1); and "Static Router Ports:" with an empty field and a format of (Format: 1-3,6,8). A "Create" button is located to the right of the Member Port Time field. The bottom part is titled "VLAN Table" and features a table with columns: "Select", "VLAN ID", "Router Port Time", "Member Port Time", "Leave Time", and "Router Port". The "Select" column contains a checkbox. Above the table, there is a "VLAN ID" input field and a "Select" button. Below the table are three buttons: "Apply", "Delete", and "Help".

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.

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

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

Leave Time: Specify the interval between the switch receiving a leave message from a host and the switch removing the host from the multicast groups.

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

➤ **VLAN Table**

- VLAN ID Select:** Click the **Select** button to quick-select the corresponding VLAN ID based on the ID number you entered.
- Select:** Select the desired VLAN ID for configuration. It is multi-optional.
- VLAN ID:** Displays the VLAN ID.
- Router Port Time:** Displays the router port time of the VLAN.
- Member Port Time:** Displays the member port time of the VLAN.
- Leave Time:** Displays the leave time of the VLAN.
- Router Port:** Displays the router port of the VLAN.



Note:

The settings here will be invalid when multicast VLAN is enabled

Configuration procedure:

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

9.1.3 Port Config

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

When the switch receives IGMP report message, it examines the multicast filtering IP ID configured on the access port to determine if the port can join the multicast group. If the multicast IP is not filtered, the switch will add the port to the forward port list of the multicast group. Otherwise, the switch will drop the IGMP report message. In that way, you can control the multicast groups that users can access.

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

Port Config								
Select	Port	IGMP Snooping	Fast Leave	Filter	Action Mode	Bound IP-Range (ID)	Max Groups	LAG
<input type="checkbox"/>		Disable	Disable	Disable	Permit			
<input type="checkbox"/>	1	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	2	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	3	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	4	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	5	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	6	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	7	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	8	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	9	Disable	Disable	Disable	permit		256	---
<input type="checkbox"/>	10	Disable	Disable	Disable	permit		256	---

Figure 9-7 Port Config

The following entries are displayed on this screen:

➤ **Port Config**

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

Select: Select the desired port for 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.

Filter: Enable or disable multicast filtering feature on the port.

Action Mode: Select the action mode to process multicast packets when the multicast IP is in the filtering IP-range.

- Permit: Only the multicast packets whose multicast IP is in the IP-range will be processed.
- Deny: Only the multicast packets whose multicast IP is not in the IP-range will be processed.

Bound IP-Range (ID): Enter the IP-range ID the port will be bound to. The binding IP-range IDs of the port can be cleared by entering null value in this field and click **Apply** button to submit the configuration.

Max Groups: Specify the maximum number of multicast groups to prevent some ports taking up too much bandwidth.

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.
3. Multicast Filter feature can only have effect on the VLAN with IGMP Snooping enabled.
4. Multicast Filter feature has no effect on static multicast IP.
5. Up to 15 IP-Ranges can be bound to one port.

9.1.4 IP-Range

On this page you can figure the desired IP-ranges to be filtered.

Choose the menu **Multicast**→**IGMP Snooping**→**IP-Range** to load the following page.

Create IP-Range

IP-Range ID: (1-30)

Start Multicast IP: (Format: 225.0.0.1)

End Multicast IP: (Format: 225.0.0.1)

IP-Range Table

Select	IP-Range ID	Start Multicast IP	End Multicast IP
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>

Figure 9-8 Multicast Filter

The following entries are displayed on this screen:

➤ **Create IP-Range**

IP Range ID: Enter the IP-range ID.

Start Multicast IP: Enter start multicast IP of the IP-range you set.

End Multicast IP: Enter end multicast IP of the IP-range you set.

➤ **IP-Range Table**

IP-Range ID Select: Click the **Select** button to quick-select the corresponding IP-range ID based on the ID number you entered.

Select: Select the desired entry to delete or modify the corresponding IP-range. It is multi-optional.

IP-Range ID: Displays IP-range ID.

- Start Multicast IP:** Displays start multicast IP of the IP-range.
- End Multicast IP:** Displays end multicast IP of the IP-range.

9.1.5 Multicast VLAN

In old multicast transmission mode, when users in different VLANs apply for join the same multicast group, the multicast router will duplicate this multicast information and deliver each VLAN owning a receiver one copy. This mode wastes a lot of bandwidth.

The problem above can be solved by configuring a multicast VLAN. By adding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves the bandwidth since multicast streams are transmitted only within the multicast VLAN and also guarantees security because the multicast VLAN is isolated from user VLANs.

Before configuring a multicast VLAN, you should firstly configure a VLAN as multicast VLAN and add the corresponding ports to the VLAN on the **802.1Q VLAN** page. If the multicast VLAN is enabled, the multicast configuration for other VLANs on the **VLAN Config** page will be invalid, that is, the multicast streams will be transmitted only within the multicast VLAN.

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

Figure 9-9 Multicast VLAN

The following entries are displayed on this screen:

➤ **Multicast VLAN**

- Multicast VLAN:** Enable or disable Multicast VLAN feature.
- VLAN ID:** Enter the VLAN ID of the multicast VLAN.
- Router Port Time:** Specify the aging time of the router port. Within this time, if the switch doesn't receive IGMP query message from the router port, it will consider this port is not a router port any more.
- Member Port Time:** Specify the aging time of the member port. Within this time, if the switch doesn't receive IGMP report message from the member port, it will consider this port is not a member port any more.

Leave Time: Specify the interval between the switch receiving a leave message from a host, and the switch removing the host from the multicast groups.

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



Note:

1. The router port should be in the multicast VLAN, otherwise the member ports cannot receive multicast streams.
2. The Multicast VLAN won't take effect unless you first complete the configuration for the corresponding VLAN owning the port on the **802.1Q VLAN** page.
3. It is recommended to choose GENERAL as the link type of the member ports in the multicast VLAN.
4. Configure the link type of the router port in the multicast VLAN as TRUNK or configure the egress rule as TAG and the link type as GENERAL otherwise all the member ports in the multicast VLAN cannot receive multicast streams.

➤ **Configuration procedure:**

Step	Operation	Description
1	Enable IGMP Snooping function	Required. Enable IGMP Snooping globally on the switch and for the port on Multicast→IGMP Snooping→Snooping Config and Port Config page.
2	Create a multicast VLAN	Required. Create a multicast VLAN and add all the member ports and router ports to the VLAN on the VLAN→802.1Q VLAN page. <ul style="list-style-type: none"> • Configure the link type of the member ports as GENERAL. • Configure the link type of the router ports as TRUNK or configure the egress rule as tagged GENERAL.
3	Configure parameters for multicast VLAN	Optional. Enable and configure a multicast VLAN on the Multicast→IGMP Snooping→Multicast VLAN page. It is recommended to keep the default time parameters.
4	Look over the configuration	If it is successfully configured, the VLAN ID of the multicast VLAN will be displayed in the IGMP Snooping Status table on the Multicast→IGMP Snooping→Snooping Config page.

Application Example for Multicast VLAN:

➤ **Network Requirements**

Multicast source sends multicast streams via the router, and the streams are transmitted to user A and user B through the switch.

Router: Its WAN port is connected to the multicast source; its LAN port is connected to the switch. The multicast packets are transmitted in VLAN3.

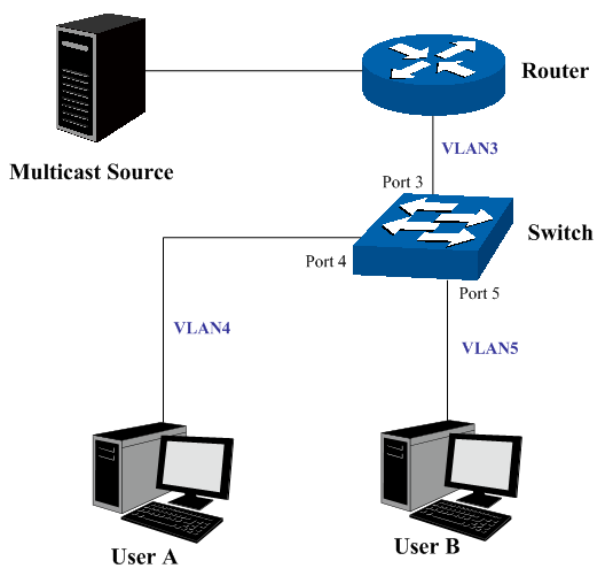
Switch: Port 3 is connected to the router and the packets are transmitted in VLAN3; port 4 is connected to user A and the packets are transmitted in VLAN4; port 5 is connected to user B and the packets are transmitted in VLAN5.

User A: Connected to Port 4 of the switch.

User B: Connected to port 5 of the switch.

Configure a multicast VLAN, and user A and B receive multicast streams through the multicast VLAN.

➤ **Network Diagram**



➤ **Configuration Procedure**

Step	Operation	Description
1	Create VLANs	Create three VLANs with the VLAN ID 3, 4 and 5 respectively, and specify the description of VLAN3 as Multicast VLAN on VLAN→802.1Q VLAN page.
2	Configure ports	On VLAN→802.1Q VLAN function pages. For port 3, configure its link type as GENERAL and its egress rule as TAG, and add it to VLAN3, VLAN4 and VLAN5. For port 4, configure its link type as GENERAL and its egress rule as UNTAG, and add it to VLAN3 and VLAN 4. For port 5, configure its link type as GENERAL and its egress rule as UNTAG, and add it to VLAN3 and VLAN 5.
3	Enable IGMP Snooping function	Enable IGMP Snooping function globally on Multicast→IGMP Snooping→Snooping Config page. Enable IGMP Snooping function for port 3, port4 and port 5 on Multicast→IGMP Snooping→Port Config page.

Step	Operation	Description
4	Enable Multicast VLAN	Enable Multicast VLAN, configure the VLAN ID of a multicast VLAN as 3 and keep the other parameters as default on Multicast→IGMP Snooping→Multicast VLAN page.
5	Check Multicast VLAN	3-5 and Multicast VLAN 3 will be displayed in the IGMP Snooping Status table on the Multicast→IGMP Snooping→Snooping Config page.

9.1.6 Static Multicast IP

Static Multicast IP table, isolated from dynamic multicast group and multicast filter, is not learned by IGMP Snooping. It can enhance the quality and security for information transmission in some fixed multicast groups.

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

Create Static Multicast

Multicast IP: (Format: 225.0.0.1)

VLAN ID: (1-4094)

Forward Port: (Format: 1-3,6,8)

Search Option

Search Option:

Static Multicast IP Table

Select	Multicast IP	VLAN ID	Forward Port
<input type="button" value="All"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>			

Figure 9-10 Static Multicast IP Table

The following entries are displayed on this screen:

➤ **Create Static Multicast**

- Multicast IP:** Enter static multicast IP address.
- VLAN ID:** Enter the VLAN ID of the multicast IP.
- Forward Port:** Enter the forward port of the multicast group.

➤ **Search Option**

- Search Option:** Select the rules for displaying multicast IP table to find the desired entries quickly.
- All: Displays all static multicast IP entries.
 - Multicast IP: Enter the multicast IP address the desired entry must carry.
 - VLAN ID: Enter the VLAN ID the desired entry must carry.
 - Port: Enter the port number the desired entry must carry.

➤ **Static Multicast IP Table**

- Select:** Select the desired entry to delete the corresponding static multicast IP. It is multi-optional.
- Multicast IP:** Displays the multicast IP.
- VLAN ID:** Displays the VLAN ID of the multicast group.
- Forward Port:** Displays the forward port of the multicast group.

9.1.7 IGMP Snooping Querier

In an IPv4 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→IGMP Snooping **Querier** to load the following page.

IGMP Snooping Querier Config

VLAN ID: (1-4094)

Query Interval: secs(1-300)

Max Response Time: secs(1-25)

General Query Source IP: (format:192.168.0.1)

Last Member Query Interval: secs(1-5) Add

Last Member Query Times: (1-5)

Last Member Query Source IP: (format:192.168.0.1)

IGMP Snooping Querier Table

Select	VLAN ID	Query Interval	Max Response Time	General Query Source IP	Last Member Query Interval	Last Member Query Times	Last Member Query Source IP
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

VLAN ID Select

Submit
Delete
Help

Figure 9-11 Packet Statistics

The following entries are displayed on this screen:

➤ **IGMP Snooping Querier Config**

- VLAN ID:** Enter the ID of the VLAN that enables IGMP Snooping Querier.
- Query Interval:** Enter the time interval of sending a general query frame by IGMP Snooping Querier.
- Max Response Time:** Enter the maximal time for the host to respond to a general query frame sent by IGMP Snooping Querier.
- General Query Source IP:** Enter the source IP of the general query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP.
- Last Member Query Interval:** Enter the time interval of sending specific query frames by IGMP Snooping Querier. A specific query will be sent on condition that "fast-leave" is not enabled and a leave frame is received.

Last Member Query Times: Enter the times of sending specific query frames by IGMP Snooping Querier. At receiving a leave frame, a specific query frame will be sent by IGMP Snooping Querier. If a report frame is received before sending specific frames number reaches "Last Member Query Times", the switch will still treat the port as group member and stop sending specific query frames to the port, otherwise the port will be removed from forward-ports of the IP multicast group.

Last Member Query Source IP: Enter the source IP of the specific query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP.

➤ **IGMP Snooping Querier Table**

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

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

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

Query Interval: Displays the Query Interval of the IGMP Snooping Querier.

Max Response Time: Displays the maximal time for the host to respond to a general query frame sent by IGMP Snooping Querier.

General Query Source IP: Displays the source IP of the general query frame sent by IGMP Snooping Querier.

Last Member Query Interval: Displays the time interval of sending specific query frames by IGMP Snooping Querier.

Last Member Query Times: Displays the times of sending specific query frames by IGMP Snooping Querier.

Last Member Query Source IP: Displays the source IP of the specific query frame sent by IGMP Snooping Querier.

9.1.8 Packet Statistics

On this page you can view the multicast data traffic on each port of the switch, which facilitates you to monitor the IGMP messages in the network.

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

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Period: sec (3-300)

IGMP Statistics

Port
Select

Port	Query Packet	Report Packet (V1)	Report Packet (V2)	Report Packet (V3)	Leave Packet	Error Packet
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

Refresh
Clear
Help

Figure 9-12 Packet Statistics

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable auto refresh feature.

Refresh Period: Enter the time from 3 to 300 in seconds to specify the auto refresh period.

➤ **IGMP Statistics**

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

Port: Displays the port number of the switch.

Query Packet: Displays the number of query packets the port received.

Report Packet (V1): Displays the number of IGMPv1 report packets the port received.

Report Packet (V2): Displays the number of IGMPv2 report packets the port received.

Report Packet (V3): Displays the number of IGMPv3 report packets the port received.

Leave Packet: Displays the number of leave packets the port received.

Error Packet: Displays the number of error packets the port received.

9.1.9 IGMP Authentication

IGMP Authentication (Internet Group membership Authentication Protocol) is a multicast authentication protocol used to authenticate users who want to join the limited multicast source. On this page you can configure IGMP Authentication feature for port.

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

Global Config

Accounting: Enable Disable

IGMP Authentication

Port

Select	Port	IGMP Authentication	LAG
<input type="checkbox"/>		Disable	
<input type="checkbox"/>	1	Disable	---
<input type="checkbox"/>	2	Disable	---
<input type="checkbox"/>	3	Disable	---
<input type="checkbox"/>	4	Disable	---
<input type="checkbox"/>	5	Disable	---
<input type="checkbox"/>	6	Disable	---
<input type="checkbox"/>	7	Disable	---
<input type="checkbox"/>	8	Disable	---
<input type="checkbox"/>	9	Disable	---
<input type="checkbox"/>	10	Disable	---

Figure 9-13 IGMP Authentication

The following entries are displayed on this screen:

➤ **Global Config**

Accounting: Enable or disable the IGMP Authentication Account feature.

➤ **IGMP Authentication**

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

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

Port: Displays the port number of the switch.

IGMP Authentication:

Select Enable or disable IGMP Authentication for the desired port.

LAG:

Displays the LAG number which the port belongs to.



Note:

The IGMP Authentication feature will take effect only when AAA function is enabled and the RADIUS server is configured. For how to enable AAA function and configure RADIUS server, please refer to [12.5 AAA](#).

9.2 MLD Snooping

➤ MLD Snooping

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

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

➤ MLD Snooping Fundamentals

1. MLD Messages

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

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

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

2. Relevant Ports of the Switch

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

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

3. Timers

Router Port Aging Time: Within this time, if the switch does not receive MLD queries from the router port, it will delete this port from the router port list. The default value is 260 seconds.

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

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

Last Listener Query Interval: The interval between the switch sends out MASQs.

Last Listener Query Count: The number of MASQs that the switch sends before aging out a multicast address when there is no MLD report response.

➤ **MLD Snooping Process**

1. General Query

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

2. Membership Report

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

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

3. Member Leave

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

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

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

The MLD Snooping function can be implemented on **Global Config, VLAN Config, Filter Config, Port Config, Static Multicast, Querier Config** and **Packet Statistics** pages.

9.2.1 Global 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**→**Global Config** to load the following page.

Global Config

MLD Snooping:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Report Message Suppression:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Unknown Multicast Filter:	<input checked="" type="radio"/> Forward	<input type="radio"/> Discard
Router Port Aging Time:	<input type="text" value="260"/> sec (1-1000)	<input type="button" value="Apply"/> <input type="button" value="Help"/>
Member Port Aging Time:	<input type="text" value="260"/> sec (200-1000)	
Last Listener Query Interval:	<input type="text" value="1"/> sec (1-5)	
Last Listener Query Count:	<input type="text" value="2"/> (1-7)	
Multicast VLAN:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Multicast VLAN ID:	<input type="text" value="1"/> (1-4094)	

Figure 9-14 Global Config

The following entries are displayed on this screen:

➤ Global Config

- | | |
|------------------------------------|--|
| MLD Snooping: | Enable or disable MLD Snooping function globally. |
| Report Message Suppression: | Enable or disable Report Message Suppression function globally. If this function is enabled, the first Report Message from the listener will forward to the router ports while the subsequent Report Message from the group will be suppressed to reduce the MLD traffic in the network. |
| Unknown Multicast Filter: | 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 filter is disabled, all unknown IPv6 multicast packets are flooded in the ingress VLAN. |
| Router Port Aging Time: | Enter the global router port aging time. If the router port does not receive Query Message in the aging time, it will be aged. |
| Member Port Aging Time: | Enter the global member port aging time. If the member port does not receive Report Message in the aging time, it will be aged. |

Last Listener Query Interval:

Enter the Last Listener Query interval time. When the multicast group has no more member ports, it will send the Specific Query Message with this interval time to check whether there is another listener.

Last Listener Query Count:


Enter the Last Listener Query numbers. When the multicast group has no more member ports, it will send this numbers of Specific Query Message to check whether there is another listener.

Multicast VLAN:

Enable or disable multicast VLAN function. When multicast VLAN is enabled, all multicast data will forward in this VLAN if this port belongs to the VLAN.

Multicast VLAN ID:

Enter the multicast VLAN ID.

 **Note:**

1. When Unknown Multicast Filter is configured, the Unknown Multicast function in IGMP Snooping is also configured at the same time.
2. Configurations of the Router Port Aging Time and Member Port Aging Time in [9.2.2 VLAN Config](#) override their global configurations here.
3. Before creating the Multicast VLAN, its corresponding VLAN should be configured in [9.2.2 VLAN Config](#).

9.2.2 VLAN Config

On this page you can configure MLD Snooping function with each single VLAN. You need to create VLAN if you want to enable MLD Snooping function in this VLAN.

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

VLAN Config

VLAN ID: (1-4094)

Router Port Aging Time: sec (0-1000)

Member Port Aging Time: sec (0, 200-1000) Create

Immediate Leave: Enable Disable

Static Router Ports: (Format: 1-3,6,8)

VLAN Table

Select	VLAN ID	Router Port Aging Time	Member Port Aging Time	Immediate Leave	Static Router Ports	Dynamic Router Ports
<input type="checkbox"/>		<input type="text" value=""/>	<input type="text" value=""/>	Enable ▾	<input type="text" value=""/>	

Figure 9-15 VLAN Config

The following entries are displayed on this screen:

➤ **VLAN Config**

VLAN ID:

Enter the VLAN ID you want to configure.

Router Port Aging Time:

Enter the router port aging time for this VLAN. It will override the global configured aging time.

Member Port Aging Time: Enter the member port aging time for this VLAN. It will override the global configured aging time.

Immediate Leave: Enable or disable immediate leave function for this VLAN. If this function is enabled, the multicast group member port will be deleted immediately if Done Message receive, not sending Specific Query for listener checking.

Static Router Ports: Enter the static router ports for this VLAN. Static router ports will not be aged.

➤ **VLAN Table**

Select: Select the VLAN ID you want to change.

VLAN ID: Displays the VLAN ID.

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

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

Immediate Leave: Displays the immediate leave function of this VLAN.

Static Router Ports: Displays the static router ports of this VLAN.

Dynamic Router Ports: Displays the dynamic router ports of this VLAN.



Note:

1. The VLAN configuration will take effect when global MLD Snooping function is enabled and the corresponding VLAN is created.
2. When the router port aging time or member port aging time is set for a VLAN, this value overrides the value configured globally.
3. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN. If the immediate leave function is enabled on a port with several listeners in the same IPv6 multicast group, these listeners will fail to receive the IPv6 multicast packets after one of them leave this group.

9.2.3 Filter Config

When the switch receives MLD report messages, it examines the multicast filtering ID and filter mode configured on the access port to determine if the port can join the multicast group. If the port can join the multicast group, the switch will add the port to the forward ports list of the multicast group. Otherwise, the switch will drop the MLD report messages. In that way, you can control the multicast groups that users can join in.

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

The screenshot shows two sections of a web interface. The top section, titled "Filter Config", contains three input fields: "Filter ID:" with a range "(1-30)", "Start Multicast IP:" with a format "(Format: FF03::AD45:3444)", and "End Multicast IP:" with a format "(Format: FF03::AD45:5432)". A "Create" button is located to the right of the IP fields. The bottom section, titled "Filter List", features a table with columns for "Select", "Filter ID", "Start Multicast IP", and "End Multicast IP". A "Select" button is positioned above the table, and "Apply", "Delete", and "Help" buttons are located below it.

Figure 9-16 Filter Config

The following entries are displayed on this screen:

➤ **Filter Config**

- Filter ID:** Enter the Filter ID which identifies the filter.
- Start Multicast IP:** Enter the start of the IP range.
- End Multicast IP:** Enter the end of the IP range.

➤ **Filter List**

- Select:** Select the filter ID you want to change.
- Filter ID:** Displays the filter ID number.
- Start Multicast IP:** Displays the start of the IP range.
- End Multicast IP:** Displays the end of the IP range.

 **Note:**

The max number of filter entries is 30.

9.2.4 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.


Port Config							
						Port <input type="text"/>	<input type="button" value="Select"/>
Select	Port	Filter	Filter Mode	Filter IDs	Max Groups	LAG	
<input type="checkbox"/>		<input type="button" value="Disable"/>	<input type="button" value="Accept"/>	<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	1	Disable	permit	---	256	---	
<input type="checkbox"/>	2	Disable	permit	---	256	---	
<input type="checkbox"/>	3	Disable	permit	---	256	---	
<input type="checkbox"/>	4	Disable	permit	---	256	---	
<input type="checkbox"/>	5	Disable	permit	---	256	---	
<input type="checkbox"/>	6	Disable	permit	---	256	---	
<input type="checkbox"/>	7	Disable	permit	---	256	---	
<input type="checkbox"/>	8	Disable	permit	---	256	---	
<input type="checkbox"/>	9	Disable	permit	---	256	---	
<input type="checkbox"/>	10	Disable	permit	---	256	---	

Figure 9-17 Port Config

The following entries are displayed on this screen:

➤ **Port Config**

- Select:** Select the port you want to configure.
- Port:** Displays the port number.
- Filter:** Choose to enable or disable filter function in this port.
- Filter Mode:** Choose the filter action mode. You can accept or refuse Report message with specific multicast groups specify by the filter IDs.
- Filter IDs:** Enter the filter IDs with this port. The filter IDs are configured in **Filer Config**. The format is 1,4,12.
- Max Groups:** Enter the maximum groups which the port can join as the member port. It ranges from 0 to 256.
- LAG:** Displays the LAG number.

 **Note:**

- If the Max Groups value is set less than the current value, some groups may be deleted to satisfy the restriction.
- The max number of filter entries on each port is 15.

9.2.5 Static Multicast

On this page you can configure static multicast groups. The multicast groups configured here are not learned by MLD Snooping and independent of dynamic multicast groups and multicast filters. The static multicast member ports won't age out.

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

Static Multicast Config

VLAN ID: (1-4094)

Multicast IP: (Format: FF03::C2D5:2313)

Member Ports: (Format: 1-3,6,8)

Static Multicast List

VLAN ID

Select	VLAN ID	Multicast IP	Member Ports
<input type="checkbox"/>			<input type="text"/>

Total Static Multicast IP: 0

Figure 9-18 Static Multicast

The following entries are displayed on this screen:

➤ **Static Multicast Config**

- VLAN ID:** Enter the VLAN ID.
- Multicast IP:** Enter the multicast IP address.
- Member Ports:** Enter the member ports of the static multicast group.

➤ **Static Multicast List**

- Select:** Select the static multicast group you want to change.
- VLAN ID:** Displays the VLAN ID.
- Multicast IP:** Displays the multicast group IP address.
- Member Ports:** Displays the member ports of the static multicast group.

9.2.6 Querier Config

In an IPv6 multicast network that runs MLD, a Layer 3 multicast device works as an MLD querier to send out MLD queries and manage the multicast table. But MLD is not supported by the devices in Layer 2 network. MLD Snooping Querier can act as an MLD Router in Layer 2 network. It can help to create and maintain multicast forwarding table on the switch with the Query messages it generates.

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

Figure 9-19 Querier Config


The following entries are displayed on this screen:

➤ **Querier Config**

- VLAN ID:** Enter the VLAN ID which you want to start Querier.
- Maximum Response Time:** Enter the value of Maximum Response Time field of the Query message.
- Query Interval:** Enter the Query message interval time. The Querier will send General Query Message with this interval.
- Query Source IP:** Enter the Query Message source IP address.

➤ **Querier List**

- Select:** Select the Querier you want to change.
- VLAN ID:** Displays the VLAN ID.
- Maximum Response Time:** Displays the value of Maximum Response Time field of the Query message.
- Query Interval:** Displays the Query message interval time.
- Query Source IP:** Displays the Query message source IP address.

 **Note:**
The MLD Snooping Querier doesn't participate in the MLD Querier Election, but an MLD Snooping Querier will affect the MLD Querier Election in the IPv6 network running MLD because of its relatively smaller IP address.

9.2.7 Packet Statistics

On this page you can view the MLD packets the switch received. It helps you to monitor the MLD Snooping function.

Choose the menu **Multicast**→**MLD Snooping**→**Packet Statistics** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable

Refresh Period: sec (3-300)

MLD Packet Statistics

Port	Received MLD Query	Received MLDv1 Report	Received MLDv2 Report	Received MLD Done	Send MLD Spec-Query	Error Packet
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

Figure 9-20 Packet Statistics

The following entries are displayed on this screen:

➤ **Auto Fresh**

Auto Fresh: Enable or disable auto fresh feature.

Fresh Period: Enter the time from 3 to 300 seconds to specify the auto fresh period.

➤ **MLD Packet Statistics**

Received MLD Query : Displays the number of MLD Query packets the switch has received.

Received MLDv1 Report: Displays the number of MLDv1 Report packets which the switch has received.

Received MLDv2 Report: Displays the number of MLDv2 Report packets which the switch has received.

Received MLD Done: Displays the number of MLD Done packets which the switch has received.

Send MLD Spec-Query: Displays the number of MLD Specific Query packets which the switch has sent.

Error Packet: Displays the number of error packets which the switch has received.

9.3 Multicast Table

In a network, receivers can join different multicast groups appropriate to their needs. The switch forwards multicast streams based on IPv4/IPv6 multicast address table.

The **Multicast Table** function is implemented on the **IPv4 Multicast Table** and **IPv6 Multicast Table** pages.

9.3.1 IPv4 Multicast Table

On this page you can view the information of the multicast groups already on the switch. Multicast IP addresses range from 224.0.0.0 to 239.255.255.255. The range for receivers to join is from 224.0.1.0 to 239.255.255.255.

Choose the menu **Multicast**→**Multicast Table**→**IPv4 Multicast Table** to load the following page.

Search Option

Multicast IP: (Format: 225.0.0.1)

VLAN ID: (1-4094)

Port:

Type: All Static Dynamic

Multicast IP Table

Multicast IP	VLAN ID	Forward Port	Type
--------------	---------	--------------	------

Total Multicast IP: 0

Figure 9-21 IPv4 Multicast Table

The following entries are displayed on this screen:

➤ **Search Option**

- Multicast IP:** Enter the multicast IP address the desired entry must carry.
- VLAN ID:** Enter the VLAN ID the desired entry must carry.
- Port:** Select the port number the desired entry must carry.
- Type:** Select the type the desired entry must carry.
- **All:** Displays all multicast IP entries.
 - **Static:** Displays all static multicast IP entries.
 - **Dynamic:** Displays all dynamic multicast IP entries.

➤ **Multicast IP Table**

- Multicast IP:** Displays multicast IP address.
- VLAN ID:** Displays the VLAN ID of the multicast group.

Forward Port: Displays the forward port of the multicast group.

Type: Displays the type of the multicast IP.

9.3.2 IPv6 Multicast Table

This page displays the IPv6 multicast groups already on the switch.

Choose the menu **Multicast**→**Multicast Table**→**IPv6 Multicast Table** to load the following page.

Search Option

Multicast IP: (Format: FF03::AD45:3444)

VLAN ID: (1-4094)

Port:

Type: All Static Dynamic

Multicast IP Table

Multicast IP	VLAN ID	Forward Ports	Type
--------------	---------	---------------	------

Total Multicast IP: 0

Figure 9-22 IPv6 Multicast Table

The following entries are displayed on this screen:

➤ **Search Option**

Multicast IP: Enter the multicast IP address the desired entry must carry.

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

Port: Select the port number the desired entry must carry.

Type: Select the type the desired entry must carry.

- **All:** Displays all multicast IP entries.
- **Static:** Displays all static multicast IP entries.
- **Dynamic:** Displays all dynamic multicast IP entries.

➤ **Multicast IP Table**

Multicast IP: Displays the multicast IP.

VLAN ID: Displays the VLAN ID.

Forward Ports: Displays the forward ports of the group.

Type: Displays the type of the group.



Note:

The max number of multicast entries is 256. The IPv4 multicast table and IPv6 multicast table share the total entry number of 256.

[Return to CONTENTS](#)

Chapter 10 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.

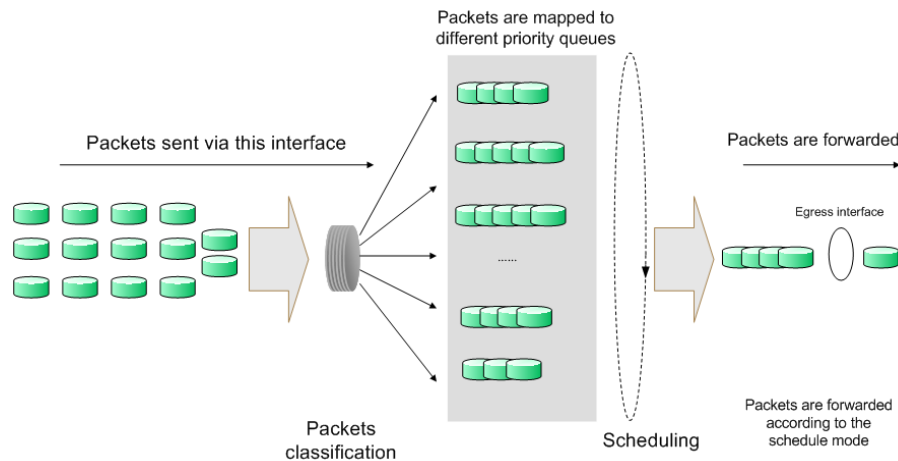


Figure 10-1 QoS function

- Traffic classification: Identifies packets conforming to certain characters according to certain rules.
- Map: The user can map the ingress packets to different priority queues based on the priority modes. This switch implements three priority modes based on port, on 802.1P and on DSCP.
- Queue scheduling algorithm: When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch supports four schedule modes: SP, WRR, SP+WRR and Equ.

➤ Priority Mode

This switch implements three priority modes based on port, on 802.1P and on DSCP. By default, the priority mode based on port is enabled and the other two modes are optional.

1. Port Priority

Port priority is just a property of the port. After port priority is configured, the data stream will be mapped to the egress queues according to the CoS of the port and the mapping relationship between CoS and queues.

2. 802.1P Priority

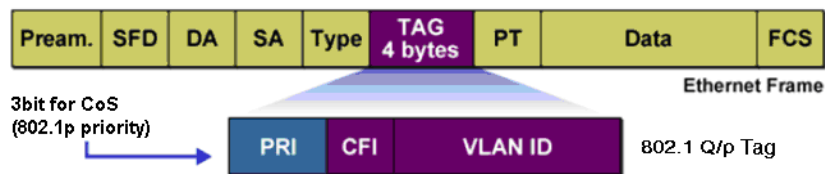


Figure 10-2 802.1Q frame

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

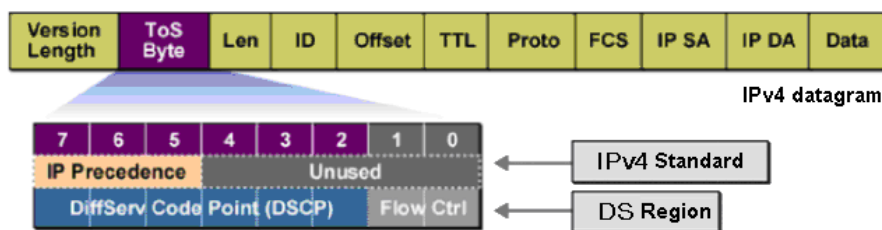


Figure 10-3 IP datagram

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 802.1P 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 four scheduling queues, TC0, TC1, TC2 and TC3. TC0 has the lowest priority while TC3 has the highest priority. The switch provides four schedule modes: SP, WRR, SP+WRR and Equ.

1. SP-Mode: Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. The switch has four egress queues labeled as TC0, TC1, TC2 and TC3. In SP mode, their priorities increase in order. TC3 has the highest priority. The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be "starved to death" because they are not served.

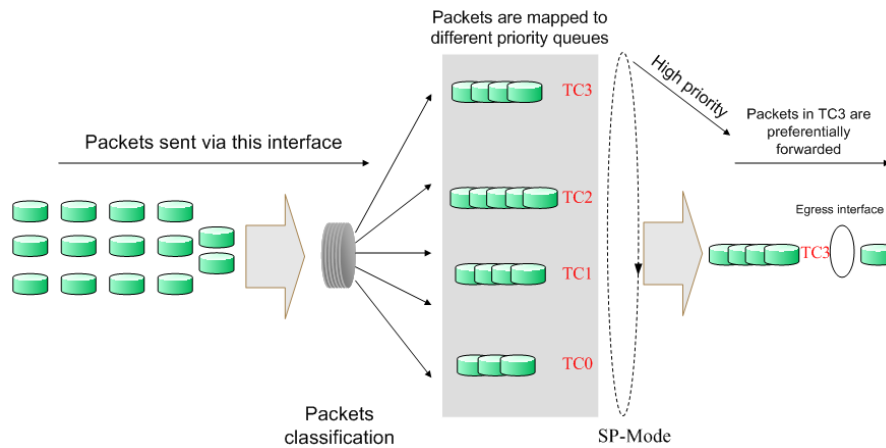


Figure 10-4 SP-Mode

2. WRR-Mode: Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. The weight value indicates the occupied proportion of the resource. WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time. In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of. The default weight value ratio of TC0, TC1, TC2 and TC3 is 1:2:4:8.

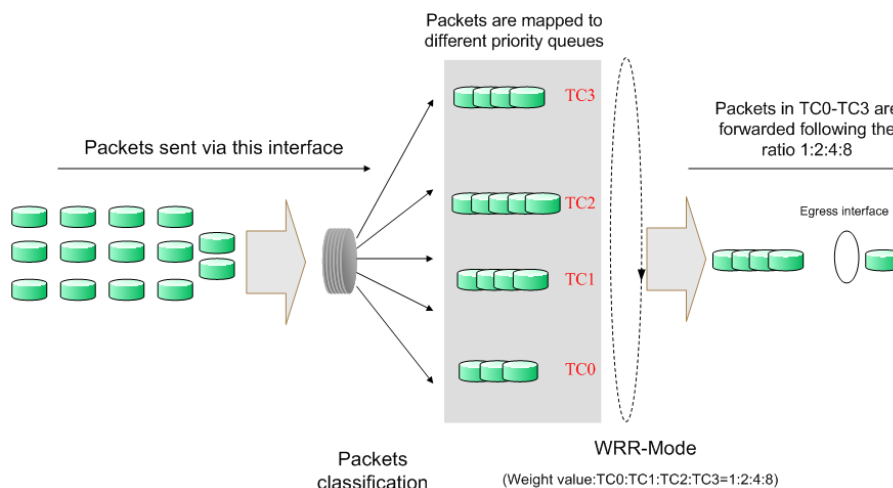


Figure 10-5 WRR-Mode

3. SP+WRR-Mode: Strict-Priority + Weight Round Robin Mode. In this mode, this switch provides two scheduling groups, SP group and WRR group. Queues in SP group and WRR group are scheduled strictly based on strict-priority mode while the queues inside WRR group follow the WRR mode. In SP+WRR mode, TC3 is in the SP group; TC0, TC1 and TC2 belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.
4. Equ-Mode: Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1.

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

10.1 DiffServ

This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function.

This switch implements three priority modes based on port, on 802.1P and on DSCP, and supports four queue scheduling algorithms. The port priorities are labeled as CoS0, CoS1... CoS7.

The DiffServ function can be implemented on **Port Priority**, **DSCP Priority**, **802.1P/CoS Mapping** and **Schedule Mode** pages.

10.1.1 Port Priority

On this page you can configure the port priority.

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

Port Priority Config			
Select	Port	Priority	LAG
<input type="checkbox"/>		CoS 0 ▾	
<input type="checkbox"/>	1	CoS 0	---
<input type="checkbox"/>	2	CoS 0	---
<input type="checkbox"/>	3	CoS 0	---
<input type="checkbox"/>	4	CoS 0	---
<input type="checkbox"/>	5	CoS 0	---
<input type="checkbox"/>	6	CoS 0	---
<input type="checkbox"/>	7	CoS 0	---
<input type="checkbox"/>	8	CoS 0	---
<input type="checkbox"/>	9	CoS 0	---
<input type="checkbox"/>	10	CoS 0	---

Figure 10-6 Port Priority Config

The following entries are displayed on this screen:

➤ **Port Priority Config**

- Select:** Select the desired port to configure its priority. It is multi-optional.
- Port:** Displays the physical port number of the switch.
- Priority:** Specify the priority for the port.
- LAG:** Displays the LAG number which the port belongs to.

**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	Select the port priority	Required. On QoS→DiffServ→Port Priority page, configure the port priority.
2	Configure the mapping relation between the CoS priority and TC	Required. On QoS→DiffServ→802.1P/CoS mapping page, configure the mapping relation between the CoS and TC.
3	Select a schedule mode	Required. On QoS→DiffServ→Schedule Mode page, select a schedule mode.

10.1.2 DSCP Priority

On this page you can configure DSCP priority. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority mode; non-IP datagram with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode if 802.1P Priority mode is enabled; the untagged non-IP datagram are mapped based on port priority mode.

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

DSCP Priority Config

DSCP Priority: Enable Disable Apply

Priority

DSCP: ▼ Priority: ▼

DSCP	Priority	DSCP	Priority
0	CoS0	1	CoS0
2	CoS0	3	CoS0
4	CoS0	5	CoS0
6	CoS0	7	CoS0
8	CoS1	9	CoS1
10	CoS1	11	CoS1
12	CoS1	13	CoS1
14	CoS1	15	CoS1
16	CoS2	17	CoS2
18	CoS2	19	CoS2

Apply
Help

Figure 10-7 DSCP Priority

The following entries are displayed on this screen:

➤ **DSCP Priority Config**

DSCP Priority: Enable or disable DSCP Priority.

➤ **Priority Level**

DSCP: Indicates the priority determined by the DSCP region of IP datagram. It ranges from 0 to 63.

Priority Level: Indicates the 802.1P priority the packets with tag are mapped to. The priorities are labeled as CoS0 ~ CoS7.

Note:
 To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

Configuration Procedure:

Step	Operation	Description
1	Configure the mapping relation between the DSCP priority and 802.1P priority	Required. On QoS→DiffServ→DSCP Priority page, enable DSCP Priority and configure the mapping relation between the DSCP priority and CoS.

Step	Operation	Description
2	Configure the mapping relation between the CoS and the TC	Required. On QoS→DiffServ→802.1P Priority page, configure the mapping relation between the CoS and the TC.
3	Select a schedule mode	Required. On QoS→DiffServ→Schedule Mode page, select a schedule mode.

10.1.3 802.1P/CoS Mapping

On this page you can configure the mapping relation between the 802.1P priority tag-id/CoS-id and the TC-id.

802.1P gives the Pri field in 802.1Q tag a recommended definition. This field, ranging from 0-7, is used to divide packets into 8 priorities. 802.1P Priority is enabled by default, so the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode but the untagged packets are mapped based on port priority mode. With the same value, the 802.1P priority tag and the CoS will be mapped to the same TC.

Choose the menu **QoS→DiffServ→802.1P/CoS Mapping** to load the following page.

Priority and CoS-mapping Config

Tag-id/CoS-id: Queue TC-id:

Tag-id/CoS-id	Queue TC-id	Tag-id/CoS-id	Queue TC-id
0	TC1	1	TC0
2	TC0	3	TC1
4	TC2	5	TC2
6	TC3	7	TC3

Figure 10-8 802.1P Priority

The following entries are displayed on this screen:

➤ **Priority and CoS-mapping Config**

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

Queue TC-id: Indicates the priority level of egress queue the packets with tag and CoS-id are mapped to. The priority levels of egress queue are labeled as TC0, TC1, TC2 and TC3. By default, the mapping relation between tag/cos and the egress queue is: 0-TC1, 1-TC0, 2-TC0, 3-TC1, 4-TC2, 5-TC2, 6-TC3, 7-TC3.

 **Note:**

To complete QoS function configuration, you have to go to the **Schedule Mode** page to select a schedule mode after the configuration is finished on this page.

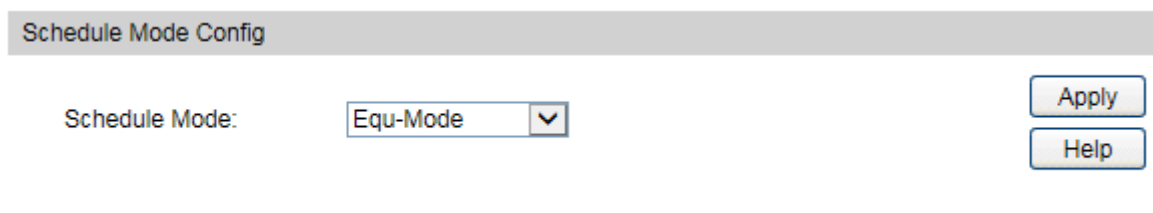
Configuration Procedure:

Step	Operation	Description
1	Configure the mapping relation between the 802.1P priority Tag/CoS and the TC	Required. On QoS→DiffServ→802.1P/CoS mapping page, configure the mapping relation between the 802.1P priority Tag/CoS and the TC.
2	Select a schedule mode	Required. On QoS→DiffServ→Schedule Mode page,, select a schedule mode.

10.1.4 Schedule Mode

On this page you can select a schedule mode for the switch. When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1...TC3.

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



Schedule Mode Config

Schedule Mode: Equ-Mode ▼

Apply

Help

Figure 10-9 Schedule Mode

The following entries are displayed on this screen:

➤ **Schedule Mode Config**

- SP-Mode:** Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.
- WRR-Mode:** Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. The weight value ratio of TC0, TC1, TC2 and TC3 is 1:2:4:8.

SP+WRR-Mode:

Strict-Priority + Weight Round Robin Mode. In this mode, this switch provides two scheduling groups, SP group and WRR group. Queues in SP group and WRR group are scheduled strictly based on strict-priority mode while the queues inside WRR group follow the WRR mode. In SP+WRR mode, TC3 is in the SP group; TC0, TC1 and TC2 belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.

Equ-Mode:

Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1.

10.2 Bandwidth Control

Bandwidth function, allowing you to control the traffic rate and broadcast flow on each port to ensure network in working order, can be implemented on **Rate Limit** and **Storm Control** pages.

10.2.1 Rate Limit

Rate limit functions to control the ingress/egress traffic rate on each port via configuring the available bandwidth of each port. In this way, the network bandwidth can be reasonably distributed and utilized.

Choose the menu **QoS**→**Bandwidth Control**→**Rate Limit** to load the following page.

Rate Limit Config					
				Port <input type="text"/>	<input type="button" value="Select"/>
Select	Port	Ingress Rate(Kbps)	Egress Rate(Kbps)	LAG	
<input type="checkbox"/>		<input type="text" value="128"/> <input type="button" value="v"/>	<input type="text" value="1024"/> <input type="button" value="v"/>		
<input type="checkbox"/>	1	---	---	---	
<input type="checkbox"/>	2	---	---	---	
<input type="checkbox"/>	3	---	---	---	
<input type="checkbox"/>	4	---	---	---	
<input type="checkbox"/>	5	---	---	---	
<input type="checkbox"/>	6	---	---	---	
<input type="checkbox"/>	7	---	---	---	
<input type="checkbox"/>	8	---	---	---	
<input type="checkbox"/>	9	---	---	---	
<input type="checkbox"/>	10	---	---	---	

Figure 10-10 Rate Limit

The following entries are displayed on this screen:

- **Rate Limit Config**

Port Select:	Click the Select button to quick-select the corresponding port based on the port number you entered.
Select:	Select the desired port for Rate configuration. It is multi-optional.
Port:	Displays the port number of the switch.
Ingress Rate (bps):	Configure the bandwidth for receiving packets on the port. You can select a rate from the dropdown list or select "Manual" to set Ingress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Ingress rate.
Egress Rate(bps):	Configure the bandwidth for sending packets on the port. You can select a rate from the dropdown list or select "Manual" to set Egress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Egress rate.
LAG:	Displays the LAG number which the port belongs to.



Note:

1. If you enable ingress rate limit feature for the storm control-enabled port, storm control feature will be disabled for this port.
2. When selecting "Manual" to set Ingress/Egress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Ingress/Egress rate. For example, if you enter 1000Kbps for egress rate, the system will automatically select 1024Kbps as the real Egress rate.
3. When egress rate limit feature is enabled for one or more ports, you are suggested to disable the flow control on each port to ensure the switch works normally.

10.2.2 Storm Control

Storm Control function allows the switch to filter broadcast, multicast and UL frame in the network. If the transmission rate of the three kind packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

Choose the menu **QoS**→**Bandwidth Control**→**Storm Control** to load the following page.

Select	Port	Broadcast Rate(bps)	Multicast Rate(bps)	UL-Frame Rate(bps)	LAG
<input type="checkbox"/>		128K	128K	128K	
<input type="checkbox"/>	1	---	---	---	---
<input type="checkbox"/>	2	---	---	---	---
<input type="checkbox"/>	3	---	---	---	---
<input type="checkbox"/>	4	---	---	---	---
<input type="checkbox"/>	5	---	---	---	---
<input type="checkbox"/>	6	---	---	---	---
<input type="checkbox"/>	7	---	---	---	---
<input type="checkbox"/>	8	---	---	---	---
<input type="checkbox"/>	9	---	---	---	---
<input type="checkbox"/>	10	---	---	---	---

Figure 10-11 Storm Control

The following entries are displayed on this screen:

➤ **Storm Control Config**

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

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

Port: Displays the port number of the switch.

Broadcast Rate (bps): Select the bandwidth for receiving broadcast packets on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the storm control function for the port.

Multicast Rate (bps): Select the bandwidth for receiving multicast packets on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the storm control function for the port.

UL-Frame Rate (bps): Select the bandwidth for receiving UL-Frame on the port. The packet traffic exceeding the bandwidth will be discarded. Select Disable to disable the storm control function for the port.

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

**Note:**

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

10.3 Voice VLAN

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

➤ OUI Address (Organizationally unique identifier address)

The switch can determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC address of a packet complies with the OUI addresses configured by the system, the packet is determined as voice packet and transmitted in voice VLAN.

An OUI address is a unique identifier assigned by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It comprises the first 24 bits of a MAC address. You can recognize which vendor a device belongs to according to the OUI address. The following table shows the OUI addresses of several manufacturers. The following OUI addresses are preset of the switch by default.

Number	OUI Address	Vendor
1	00-01-E3-00-00-00	Siemens phone
2	00-03-6B-00-00-00	Cisco phone
3	00-04-0D-00-00-00	Avaya phone
4	00-60-B9-00-00-00	Philips/NEC phone
5	00-D0-1E-00-00-00	Pingtel phone
6	00-E0-75-00-00-00	Polycom phone
7	00-E0-BB-00-00-00	3com phone

Table 10-1 OUI addresses on the switch

➤ Port Voice VLAN Mode

A voice VLAN can operate in two modes: automatic mode and manual mode.

Automatic Mode: In this mode, the switch automatically adds a port which receives voice packets to voice VLAN and determines the priority of the packets through learning the source MAC of the UNTAG packets sent from IP phone when it is powered on. The aging time of voice VLAN can be configured on the switch. If the switch does not receive any voice packet on the ingress port within the aging time, the switch will remove this port from voice VLAN. Voice ports are automatically added into or removed from voice VLAN.

Manual Mode: You need to manually add the port of IP phone to voice VLAN, and then the switch will assign ACL rules and configure the priority of the packets through learning the source MAC address of packets and matching OUI address.

In practice, the port voice VLAN mode is configured according to the type of packets sent out from voice device and the link type of the port. The following table shows the detailed information.

Port Voice VLAN Mode	Voice Stream Type	Link type of the port and processing mode
Automatic Mode	TAG voice stream	ACCESS: Not supported.
		TRUNK: Supported. The default VLAN of the port cannot be voice VLAN.
		GENERAL: Supported. The default VLAN of the port cannot be voice VLAN and the egress rule of the access port in the voice VLAN should be TAG.
	UNTAG voice stream	ACCESS: Supported.
		TRUNK: Not supported.
		GENERAL: Supported. The default VLAN of the port should be voice VLAN and the egress rule of the access port in the voice VLAN should be UNTAG.
Manual Mode	TAG voice stream	ACCESS: Not supported.
		TRUNK: Supported. The default VLAN of the port should not be voice VLAN.
		GENERAL: Supported. The default VLAN of the port cannot be voice VLAN and the egress rule of the access port in the voice VLAN should be TAG.
	UNTAG voice stream	ACCESS: Supported.
		TRUNK: Not supported.
		GENERAL: Supported. The default VLAN of the port should be voice VLAN and the egress rule of the access port in the voice VLAN should be UNTAG.

Table 10-2 Port voice VLAN mode and voice stream processing mode

➤ Security Mode of Voice VLAN

When voice VLAN is enabled for a port, you can configure its security mode to filter data stream. If security mode is enabled, the port just forwards voice packets, and discards other packets whose source MAC addresses do not match OUI addresses. If security mode is not enabled, the port forwards all the packets.

Security Mode	Packet Type	Processing Mode
Enable	UNTAG packet	When the source MAC address of the packet is the OUI address that can be identified, the packet can be transmitted in the voice VLAN. Otherwise, the packet will be discarded.
	Packet with voice VLAN TAG	
	Packet with other VLAN TAG	The processing mode for the device to deal with the packet is determined by whether the port permits the VLAN or not, independent of voice VLAN security mode.
Disable	UNTAG packet	Do not check the source MAC address of the packet and all the packets can be transmitted in the voice VLAN.
	Packet with voice VLAN TAG	
	Packet with other VLAN TAG	The processing mode for the device to deal with the packet is determined by whether the port permits the VLAN or not, independent of voice VLAN security mode.

Table 10-3 Security mode and packets processing mode



Note:

Don't transmit voice stream together with other business packets in the voice VLAN except for some special requirements.

The Voice VLAN function can be implemented on **Global Config**, **Port Config** and **OUI Config** pages.

10.3.1 Global Config

On this page, you can configure the global parameters of the voice VLAN, including VLAN ID, aging time, the transmission priority of the voice packets and so on.

Choose the menu **QoS**→**Voice VLAN**→**Global Config** to load the following page.

Global Config

Voice VLAN: Enable Disable

VLAN ID: (2-4094)

Aging Time: min (1-43200, default: 1440)

Priority: ▼

Figure 10-12 Global Configuration

The following entries are displayed on this screen:

➤ **Global Config**

Voice VLAN: Enable or disable Voice VLAN function.

VLAN ID: Enter the VLAN ID of the voice VLAN.

Aging Time: Specifies the living time of the member port in auto mode after the OUI address is aging out.

Priority: Select the priority of the port when sending voice data.

10.3.2 Port Config

Before the voice VLAN function is enabled, the parameters of the ports in the voice VLAN should be configured on this page.

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

Select	Port	Port Mode	Security Mode	Member State	LAG
<input type="checkbox"/>		<input type="text" value="Auto"/>	<input type="text" value="Disable"/>		
<input type="checkbox"/>	1	Auto	Disable	Inactive	---
<input type="checkbox"/>	2	Auto	Disable	Inactive	---
<input type="checkbox"/>	3	Auto	Disable	Inactive	---
<input type="checkbox"/>	4	Auto	Disable	Inactive	---
<input type="checkbox"/>	5	Auto	Disable	Inactive	---
<input type="checkbox"/>	6	Auto	Disable	Inactive	---
<input type="checkbox"/>	7	Auto	Disable	Inactive	---
<input type="checkbox"/>	8	Auto	Disable	Inactive	---
<input type="checkbox"/>	9	Auto	Disable	Inactive	---
<input type="checkbox"/>	10	Auto	Disable	Inactive	---

Figure 10-13 Port Config



Note:

1. To enable voice VLAN function for the LAG member port, please ensure its member state accords with its port mode.
2. If a port is a member port of voice VLAN, changing its port mode to be "Auto" will make the port leave the voice VLAN and will not join the voice VLAN automatically until it receives voice streams.

The following entries are displayed on this screen:

➤ **Port Config**

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

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

Port: Displays the port number of the switch.

- Port Mode:** Select the mode for the port to join the voice VLAN.
- **Auto:** In this mode, the switch automatically adds a port to the voice VLAN or removes a port from the voice VLAN by checking whether the port receives voice data or not.
 - **Manual:** In this mode, you can manually add a port to the voice VLAN or remove a port from the voice VLAN.
- Security Mode:** Configure the security mode for forwarding packets.
- **Disable:** All packets are forwarded.
 - **Enable:** Only voice data are forwarded.
- Member State:** Displays the state of the port in the current voice VLAN.
- LAG:** Displays the LAG number which the port belongs to.

10.3.3 OUI Config

The switch supports OUI creation and adds the MAC address of the special voice device to the OUI table of the switch. The switch determines whether a received packet is a voice packet by checking its OUI address. The switch analyzes the received packets. If the packets are recognized as voice packets, the access port will be automatically added to the Voice VLAN.

Choose the menu **QoS**→**Voice VLAN**→**OUI Config** to load the following page.

Create OUI

OUI: (Format: 00-00-00-00-00-01)

Mask: (Default: FF-FF-FF-00-00-00)

Description: (16 characters maximum)

OUI Table

Select	OUI	Mask	Description
<input type="checkbox"/>	00-01-e3-00-00-00	ff-ff-ff-00-00-00	Siemens Phone
<input type="checkbox"/>	00-03-6b-00-00-00	ff-ff-ff-00-00-00	Cisco Phone
<input type="checkbox"/>	00-04-0d-00-00-00	ff-ff-ff-00-00-00	Avaya Phone
<input type="checkbox"/>	00-60-b9-00-00-00	ff-ff-ff-00-00-00	Philips Phone
<input type="checkbox"/>	00-d0-1e-00-00-00	ff-ff-ff-00-00-00	Pingtel Phone
<input type="checkbox"/>	00-e0-75-00-00-00	ff-ff-ff-00-00-00	PolyCom Phone
<input type="checkbox"/>	00-e0-bb-00-00-00	ff-ff-ff-00-00-00	3Com Phone

Figure 10-14 OUI Configuration

The following entries are displayed on this screen:

➤ **Create OUI**

OUI: Enter the OUI address of the voice device.

Mask: Enter the OUI address mask of the voice device.

Description: Give a description to the OUI for identification.

➤ **OUI Table**

Select: Select the desired entry to view the detailed information.

OUI: Displays the OUI address of the voice device.

Mask: Displays the OUI address mask of the voice device.

Description: Displays the description of the OUI.

Configuration Procedure of Voice VLAN:

Step	Operation	Description
1	Configure the link type of the port	Required. On VLAN→802.1Q VLAN→Port Config page, configure the link type of ports of the voice device.
2	Create VLAN	Required. On VLAN→802.1Q VLAN→Port Config page, click the Create button to create a VLAN.
3	Add OUI address	Optional. On QoS→Voice VLAN→OUI Config page, you can check whether the switch is supporting the OUI template or not. If not, please add the OUI address.
4	Configure the parameters of the ports in voice VLAN.	Required. On QoS→Voice VLAN→Port Config page, configure the parameters of the ports in voice VLAN.
5	Enable Voice VLAN	Required. On QoS→Voice VLAN→Global Config page, configure the global parameters of voice VLAN.

[Return to CONTENTS](#)

Chapter 11 ACL

ACL (Access Control List) is used to filter packets by configuring match rules and process policies of packets in order to control the access of the illegal users to the network. Besides, ACL functions to control traffic flows and save network resources. It provides a flexible and secured access control policy and facilitates you to control the network security.

On this switch, ACLs classify packets based on a series of match conditions, which can be L2-L4 protocol key fields carried in the packets. A time-range based ACL enables you to implement ACL control over packets by differentiating the time-ranges.

The ACL module is mainly for ACL configuration of the switch, including four submenus: **Time-Range**, **ACL Config**, **Policy Config** and **Policy Binding**.

11.1 Time-Range

If a configured ACL is needed to be effective in a specified time-range, a time-range should be firstly specified in the ACL. As the time-range based ACL takes effect only within the specified time-range, data packets can be filtered by differentiating the time-ranges.

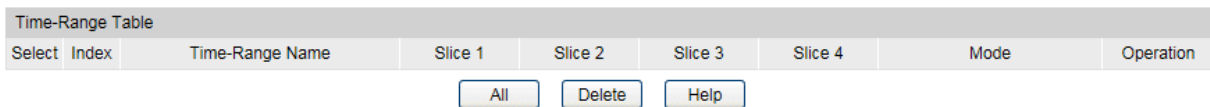
On this switch absolute time, week time and holiday can be configured. Configure an absolute time section in the form of "the start date to the end date" to make ACLs effective; configure a week time section to make ACLs effective on the fixed days of the week; configure a holiday section to make ACLs effective on some special days. In each time-range, four time-slices can be configured.

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

11.1.1 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.



Select	Index	Time-Range Name	Slice 1	Slice 2	Slice 3	Slice 4	Mode	Operation
--------	-------	-----------------	---------	---------	---------	---------	------	-----------

Figure 11-1 Time-Range Table

The following entries are displayed on this screen:

➤ **Time-Range Table**

Select: Select the desired entry to delete the corresponding time-range.

Index: Displays the index of the time-range.

Time-Range Name: Displays the name of the time-range.

Slice: Displays the time-slice of the time-range.

Mode: Displays the mode the time-range adopts.

Operation: Click the **Edit** button to modify the time-range. Click the **Detail** button to display the complete information of this time-range.

11.1.2 Time-Range Create

On this page you can create time-ranges.

Choose the menu **ACL**→**Time-Range**→**Time-Range Create** to load the following page.

Create Time-Range

Name:

Holiday

Absolute Start Date: 2000 / 01 / 01 End Date: 2000 / 01 / 01

Week Mon Tue Wed Thu Fri Sat Sun

Create Time-Slice

Start Time: 00 : 00

End Time: 24 : 00

Time-Slice Table

Index	Start Time	End Time	Delete
-------	------------	----------	--------

Figure 11-2 Time-Range Create



Note:

To successfully configure time-ranges, please firstly specify time-slices and then time-ranges.

The following entries are displayed on this screen:

➤ **Create Time-Range**

Name: Enter the name of the time-range for time identification.

Holiday: Select Holiday you set as a time-range. The ACL rule based on this time-range takes effect only when the system time is within the holiday.

Absolute: Select Absolute to configure absolute time-range. The ACL rule based on this time-range takes effect only when the system time is within the absolute time-range.

Week: Select Week to configure week time-range. The ACL rule based on this time-range takes effect only when the system time is within the week time-range.

➤ **Create Time-Slice**

Start Time: Set the start time of the time-slice.

- End Time:** Set the end time of the time-slice.
- **Time-Slice Table**
 - Index:** Displays the index of the time-slice.
 - Start Time:** Displays the start time of the time-slice.
 - End Time:** Displays the end time of the time-slice.
 - Delete:** Click the **Delete** button to delete the corresponding time-slice.

11.1.3 Holiday Config

Holiday mode is applied as a different secured access control policy from the week mode. On this page you can define holidays according to your work arrangement.

Choose the menu **ACL**→**Time-Range**→**Holiday Config** to load the following page.

Create Holiday

Start Date: /

End Date: / Create

Holiday Name:

Holiday Table

Select	Index	Holiday Name	Start Date	End Date
All Delete Help				

Figure 11-3 Holiday Configuration

The following entries are displayed on this screen:

- **Create Holiday**
 - Start Date:** Specify the start date of the holiday.
 - End Date:** Specify the end date of the holiday.
 - Holiday Name:** Enter the name of the holiday.
- **Holiday Table**
 - Select:** Select the desired entry to delete the corresponding holiday.
 - Index:** Displays the index of the holiday.
 - Holiday Name:** Displays the name of the holiday.
 - Start Date:** Displays the start date of the holiday.
 - End Date:** Displays the end date of the holiday.

11.2 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. Once a rule is matched,

The ACL Config function can be implemented on **ACL Summary**, **ACL Create**, **MAC ACL**, **Standard-IP ACL** and **Extend-IP ACL** pages.

11.2.1 ACL Summary

On this page, you can view the current ACLs configured in the switch.

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

Search Options

Select ACL:

ACL Type:

Rule Order:

Rule Table

Figure 11-4 ACL Summary

The following entries are displayed on this screen:

➤ Search Option

- Select ACL:** Select the ACL you have created
- ACL Type:** Displays the type of the ACL you select.
- Rule Order:** Displays the rule order of the ACL you select.

➤ Rule Table

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

11.2.2 ACL Create

On this page you can create ACLs.

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

Figure 11-5 ACL Create

The following entries are displayed on this screen:

➤ **Create ACL**

ACL ID: Enter ACL ID of the ACL you want to create.

Rule Order: User Config order is set to be match order in this ACL.

11.2.3 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, VLAN ID, and EtherType carried in the packets.

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

Figure11-6 Create MAC Rule

The following entries are displayed on this screen:

➤ **Create MAC-Rule**

ACL ID: Select the desired MAC ACL for configuration.

- Rule ID:** Enter the rule ID.
- Operation:** Select the operation for the switch to process packets which match the rules.
- **Permit:** Forward packets.
 - **Deny:** Discard Packets.
- S-MAC:** Enter the source MAC address contained in the rule.
- D-MAC:** Enter the destination MAC address contained in the rule.
- MASK:** Enter MAC address mask. If it is set to 1, it must strictly match the address.
- VLAN ID:** Enter the VLAN ID contained in the rule.
- EtherType:** Enter EtherType contained in the rule.
- User Priority:** Select the user priority contained in the rule for the tagged packets to match.
- Time-Range:** Select the time-range for the rule to take effect.

11.2.4 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.

The screenshot shows a web-based configuration interface for creating a Standard-IP ACL. The title is "Create Standard-IP Rule". The fields are as follows:

- ACL ID:** A dropdown menu with "Standard-IP ACL" selected.
- Rule ID:** An empty text input field.
- Operation:** A dropdown menu with "Permit" selected.
- S-IP:** An unchecked checkbox followed by an empty text input field and a "Mask:" label with an empty text input field.
- D-IP:** An unchecked checkbox followed by an empty text input field and a "Mask:" label with an empty text input field.
- Time-Range:** A dropdown menu with "No Limit" selected.

At the bottom of the form are two buttons: "Create" and "Help".

Figure11-7 Create Standard-IP Rule

The following entries are displayed on this screen:

➤ **Create Standard-IP Rule**

- ACL ID:** Select the desired Standard-IP ACL for configuration.
- Rule ID:** Enter the rule ID.

- Operation:** Select the operation for the switch to process packets which match the rules.
- **Permit:** Forward packets.
 - **Deny:** Discard Packets.
- Fragment:** Select if the rule will take effect on the fragment. When the fragment is selected, this rule will process all the fragments and the last piece of fragment will be always forwarded.
- S-IP:** Enter the source IP address contained in the rule.
- D-IP:** Enter the destination IP address contained in the rule.
- Mask:** Enter IP address mask. If it is set to 1, it must strictly match the address.
- Time-Range:** Select the time-range for the rule to take effect.

11.2.5 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.

Create Extend-IP Rule

ACL ID:	<input type="text" value="Extend-IP ACL"/>	
Rule ID:	<input type="text"/>	
Operation:	<input type="text" value="Permit"/>	
<input type="checkbox"/> S-IP:	<input type="text"/>	Mask: <input type="text"/>
<input type="checkbox"/> D-IP:	<input type="text"/>	Mask: <input type="text"/>
IP Protocol:	<input type="text" value="All"/>	
TCP Flag:	URG <input type="text" value="*"/> ACK <input type="text" value="*"/> PSH <input type="text" value="*"/> RST <input type="text" value="*"/> SYN <input type="text" value="*"/> FIN <input type="text" value="*"/>	
<input type="checkbox"/> S-Port:	<input type="text"/>	
<input type="checkbox"/> D-Port:	<input type="text"/>	
DSCP:	<input type="text" value="All"/>	
IP ToS:	<input type="text" value="All"/>	IP Pre: <input type="text" value="All"/>
Time-Range:	<input type="text" value="No Limit"/>	
<input type="button" value="Create"/> <input type="button" value="Help"/>		

Figure11-8 Create Extend-IP Rule

The following entries are displayed on this screen:

➤ **Create Extend-IP Rule**

ACL ID: Select the desired Extend-IP ACL for configuration.

Rule ID:	Enter the rule ID.
Operation:	Select the operation for the switch to process packets which match the rules. <ul style="list-style-type: none"> ● Permit: Forward packets. ● Deny: Discard Packets.
S-IP:	Enter the source IP address contained in the rule.
D-IP:	Enter the destination IP address contained in the rule.
Mask:	Enter IP address mask. If it is set to 1, it must strictly match the address.
IP Protocol:	Select IP protocol contained in the rule.
TCP Flag:	Configure TCP flag when TCP is selected from the pull-down list of IP Protocol.
S-Port:	Configure TCP/IP source port contained in the rule when TCP/UDP is selected from the pull-down list of IP Protocol.
D-Port:	Configure TCP/IP destination port contained in the rule when TCP/UDP is selected from the pull-down list of IP Protocol.
DSCP:	Enter the DSCP information contained in the rule.
IP ToS:	Enter the IP-ToS contained in the rule.
IP Pre:	Enter the IP Precedence contained in the rule.
Time-Range:	Select the time-range for the rule to take effect.

11.3 Policy Config

A Policy is used to control the data packets those match the corresponding ACL rules by configuring ACLs and actions together for effect. The operations here include stream mirror, stream condition, QoS remarking and redirect.

The Policy Config can be implemented on **Policy Summary**, **Police Create** and **Action Create** pages.

11.3.1 Policy Summary

On this page, you can view the ACL and the corresponding operations in the policy.

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

Select Options							
Select Policy:	<input type="text"/>	<input type="button" value="Delete"/>					

Action Table							
Select	Index	ACL ID	S-Mirror	S-Condition	Redirect	QoS Remark	Operation
			<input type="button" value="All"/>	<input type="button" value="Delete"/>	<input type="button" value="Help"/>		

Figure 11-9 Policy Summary

The following entries are displayed on this screen:

➤ **Search Options**

Select Policy: Select name of the desired policy for view. If you want to delete the desired policy, please click the **Delete** button.

➤ **Action Table**

Select: Select the desired entry to delete the corresponding policy.

Index: Enter the index of the policy.

ACL ID: Displays the ID of the ACL contained in the policy.

S-Mirror: Displays the source mirror port of the policy.

S-Condition: Displays the source condition added to the policy.

Redirect: Displays the redirect added to the policy.

QoS Remark: Displays the QoS remark added to the policy.

Operation: Click the **Edit** button to modify the action.

11.3.2 Policy Create

On this page you can create the policy.

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

Create Policy	
Policy Name:	<input type="text"/>
<input type="button" value="Create"/> <input type="button" value="Help"/>	

Figure 11-10 Create Policy

The following entries are displayed on this screen:

➤ **Create Policy**

Policy Name: Enter the name of the policy.

11.3.3 Action Create

On this page you can add ACLs and create corresponding actions for the policy.

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

Create Action

Select Policy:

Select ACL:

S-Mirror

Port:

S-Condition

Rate: Kbps(1-1000000)

Out of Band:

Redirect

Destination Port:

QoS Remark

DSCP:

Local Priority:

Figure 11-11 Action Create

The following entries are displayed on this screen:

➤ **Create Action**

- Select Policy:** Select the name of the policy.
- Select ACL:** Select the ACL for configuration in the policy.
- S-Mirror:** Select S-Mirror to mirror the data packets in the policy to the specific port.
- S-Condition:** Select S-Condition to limit the transmission rate of the data packets in the policy.
- **Rate:** Specify the forwarding rate of the data packets those match the corresponding ACL.
 - **Out of Band:** Specify the disposal way of the data packets those are transmitted beyond the rate.
- Redirect:** Select Redirect to change the forwarding direction of the data packets in the policy.
- **Destination Port:** Forward the data packets those match the corresponding ACL to the specific port.

QoS Remark: Select QoS Remark to forward the data packets based on the QoS settings.

- **DSCP:** Specify the DSCP region for the data packets those match the corresponding ACL.
- **Local Priority:** Specify the local priority for the data packets those match the corresponding ACL.

11.4 Policy Binding

Policy Binding function can have the policy take its effect on a specific port/VLAN. The policy will take effect only when it is bound to a port/VLAN. In the same way, the port/VLAN will receive the data packets and process them based on the policy only when the policy is bound to the port/VLAN.

The Policy Binding can be implemented on **Binding Table**, **Port Binding** and **VLAN Binding** pages.

11.4.1 Binding Table

On this page view the policy bound to port/VLAN.

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

Search Options					
Show Mode:	Show All ▼				
Policy Bind Table					
Select	Index	Policy Name	Interface	Direction	
All			Delete		Help

Figure 11-12 Binding Table

The following entries are displayed on this screen:

➤ **Search Options**

Show Mode: Select a show mode appropriate to your needs.

➤ **Policy Bind Table**

Select: Select the desired entry to delete the corresponding binding policy.

Index: Displays the index of the binding policy.

Policy Name: Displays the name of the binding policy.

Interface: Displays the port number or VLAN ID bound to the policy.

Direction: Displays the binding direction.

11.4.2 Port Binding

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

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

The screenshot shows a web interface for port binding. At the top is a grey header bar labeled "Port-Bind Config". Below it are two rows of configuration fields. The first row has "Policy Name:" followed by a dropdown menu with "Select Policy" and a downward arrow, and a "Bind" button. The second row has "Port:" followed by a text input field and the text "(Format: 1-3,6,8)", and a "Help" button. Below this is another grey header bar labeled "Port-Bind Table". Underneath is a table with four columns: "Index", "Policy Name", "Port", and "Direction".

Figure 11-13 Bind the policy to the port

The following entries are displayed on this screen:

➤ **Port-Bind Config**

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

Port: Enter the number of the port you want to bind.

➤ **Port-Bind Table**

Index: Displays the index of the binding policy.

Policy Name: Displays the name of the binding policy.

Port: Displays the number of the port bound to the corresponding policy.

Direction: Displays the binding direction.

11.4.3 VLAN Binding

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

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

The screenshot shows a web interface for VLAN binding. At the top is a grey header bar labeled "VLAN-Bind Config". Below it are two rows of configuration fields. The first row has "Policy Name:" followed by a dropdown menu with "Select Policy" and a downward arrow, and a "Bind" button. The second row has "VLAN ID:" followed by a text input field and the text "(Format: 1-3,6,8)", and a "Help" button. Below this is another grey header bar labeled "VLAN-Bind Table". Underneath is a table with four columns: "Index", "Policy Name", "VLAN ID", and "Direction".

Figure11-14 Bind the policy to the VLAN

The following entries are displayed on this screen:

➤ **VLAN-Bind Config**

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

VLAN ID: Enter the ID of the VLAN you want to bind.

➤ **VLAN-Bind Table**

Index: Displays the index of the binding policy.

Policy Name: Displays the name of the binding policy.

VLAN ID: Displays the ID of the VLAN bound to the corresponding policy.

Direction: Displays the binding direction.

Configuration Procedure:

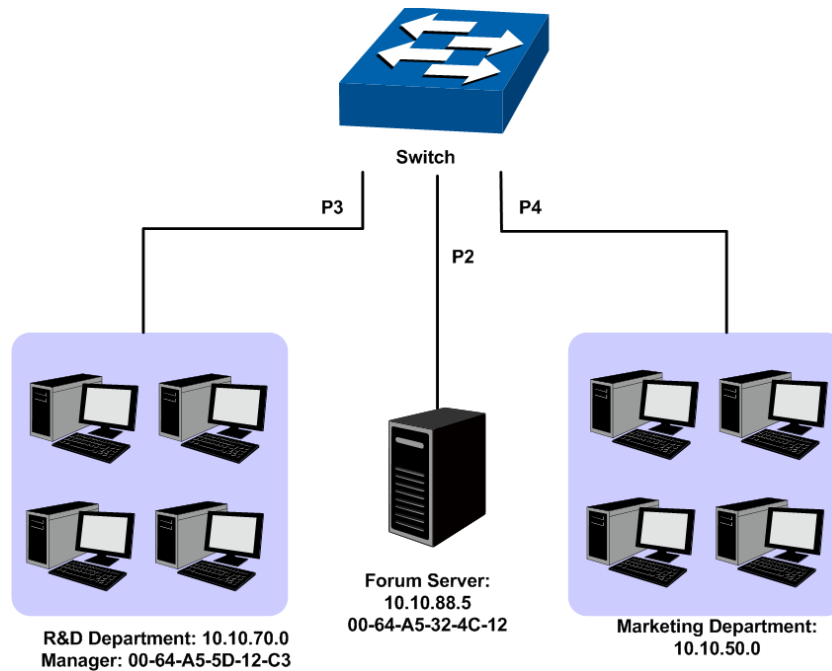
Step	Operation	Description
1	Configure effective time-range	Required. On ACL→Time-Range configuration pages, configure the effective time-ranges for ACLs.
2	Configure ACL rules	Required. On ACL→ACL Config configuration pages, configure ACL rules to match packets.
3	Configure Policy	Required. On ACL→Policy Config configuration pages, configure the policy to control the data packets those match the corresponding ACL rules.
4	Bind the policy to the port/VLAN	Required. On ACL→Policy Binding configuration pages, bind the policy to the port/VLAN to make the policy effective on the corresponding port/VLAN.

11.5 Application Example for ACL

➤ **Network Requirements**

1. The manager of the R&D department can access to the forum of the company without any forbiddance. The MAC address of the manager is 00-64-A5-5D-12-C3.
2. The staff of the R&D department can visit the forum during the working time.
3. The staff of the marketing department cannot visit the forum during the working time.
4. The R&D department and marketing department cannot communicate with each other.

➤ **Network Diagram**



➤ **Configuration Procedure**

Step	Operation	Description
1	Configure Time-range	On ACL→Time-Range page, create a time-range named work_time. Select Week mode and configure the week time from Monday to Friday. Add a time-slice 08:00–18:00.
2	Configure for requirement 1	On ACL→ACL Config→ACL Create page, create ACL 11. On ACL→ACL Config→MAC ACL page, select ACL 11, create Rule 1, configure the operation as Permit, configure the S-MAC as 00-64-A5-5D-12-C3 and mask as FF-FF-FF-FF-FF-FF, and configure the time-range as No Limit. On ACL→Policy Config→Policy Create page, create a policy named manager. On ACL→Policy Config→Action Create page, add ACL 11 to Policy manager. On ACL→Policy Binding→Port Binding page, select Policy manager to bind to port 3.

Step	Operation	Description
3	Configure for requirement 2 and 4	<p>On ACL→ACL Config→ACL Create page, create ACL 100.</p> <p>On ACL→ACL Config→Standard-IP ACL page, select ACL 100, create Rule 2, configure operation as Permit, configure S-IP as 10.10.70.0 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255, configure the time-range as work_time.</p> <p>On ACL→ACL Config→Standard-IP ACL page, select ACL 100, create Rule 1, configure operation as Deny, configure S-IP as 10.10.70.0 and mask as 255.255.255.0, configure D-IP as 10.10.50.1 and mask as 255.255.255.255, configure the time-range as No Limit.</p> <p>On ACL→ACL Config→Standard-IP ACL page, select ACL 100, create Rule 3, configure operation as Deny, configure S-IP as 10.10.70.1 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255, configure the time-range as No Limit.</p> <p>On ACL→Policy Config→Policy Create page, create a policy named limit1.</p> <p>On ACL→Policy Config→Action Create page, add ACL 100 to Policy limit1.</p> <p>On ACL→Policy Binding→Port Binding page, select Policy limit1 to bind to port 3.</p>
4	Configure for requirement 3 and 4	<p>On ACL→ACL Config→ACL Create page, create ACL 101.</p> <p>On ACL→ACL Config→Standard-IP ACL page, select ACL 101, create Rule 4, configure operation as Deny, configure S-IP as 10.10.50.0 and mask as 255.255.255.0, configure D-IP as 10.10.70.0 and mask as 255.255.255.0, configure the time-range as No Limit.</p> <p>On ACL→ACL Config→Standard-IP ACL page, select ACL 101, create Rule 5, configure operation as Deny, configure S-IP as 10.10.50.0 and mask as 255.255.255.0, configure D-IP as 10.10.88.5 and mask as 255.255.255.255, configure the time-range as work_time.</p> <p>On ACL→Policy Config→Policy Create page, create a policy named limit2.</p> <p>On ACL→Policy Config→Action Create page, add ACL 101 to Policy limit2.</p> <p>On ACL→Policy Binding→Port Binding page, select Policy limit2 to bind to port 4.</p>

[Return to CONTENTS](#)

Chapter 12 Network Security

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

12.1 IP-MAC Binding

The IP-MAC Binding function allows you to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together. Basing on the IP-MAC binding table, ARP Inspection and IP Source Guard functions can control the network access and only allow the Hosts matching the bound entries to access the network.

The following three IP-MAC Binding methods are supported by the switch.

1. **Manually:** You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.
2. **Scanning:** You can quickly get the information of the IP address, MAC address, VLAN ID and the connected port number of the Hosts in the LAN via the ARP Scanning function, and bind them conveniently. You are only requested to enter the IP address on the ARP Scanning page for the scanning.
3. **DHCP Snooping:** You can use DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

These three methods are also considered as the sources of the IP-MAC Binding entries. The entries from various sources should be different from one another to avoid collision. Among the entries in collision, only the entry from the source with the highest priority will take effect. These three sources (Manual, Scanning and Snooping) are in descending order of priority.

The **IP-MAC Binding** function is implemented on the **Binding Table**, **Manual Binding** and **ARP Scanning** pages.

12.1.1 Binding Table

On this page, you can view the information of the bound entries.

Choose the menu **Network Security**→**IP-MAC Binding**→**Binding Table** to load the following page.

Search Option

Source:

Binding Table

Host Name

Select	Host Name	IP Address	MAC Address	VLAN ID	Port	Protect Type	Source	Collision
<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		

Entry Count: 0

Figure 12-1 Binding Table

The following entries are displayed on this screen:

➤ **Search Option**

Source:

Select a Source from the pull-down list and click the **Search** button to view your desired entry in the Binding Table.

- **All:** All the bound entries will be displayed.
- **Manual:** Only the manually added entries will be displayed.
- **Scanning:** Only the entries formed via ARP Scanning will be displayed.
- **Snooping:** Only the entries formed via DHCP Snooping will be displayed.

➤ **Binding Table**

Host Name /IP Address /MAC Address Select:

Click the **Select** button to quick-select the corresponding entry based on the Host Name/IP Address/MAC Address you entered.

Select:

Select the desired entry to modify the Host Name/MAC Address/VLAN ID/Port /Protect Type. It is multi-optional.

Host Name:

Allows you to view and modify the Host Name.

IP Address:

Displays the IP Address of the Host.

MAC Address:

Allows you to view and modify the MAC Address of the Host.

VLAN ID:

Allows you to view and modify the VLAN ID.

Port:

Allows you to view and modify the number of port connected to the Host.

Protect Type:

Allows you to view and modify the Protect Type of the entry.

Source:

Displays the Source of the entry.

Collision:

Displays the Collision status of the entry.

- **Warning:** Indicates that the collision may be caused by the MSTP function.
- **Critical:** Indicates that the entry has a collision with the other entries.

**Note:**

1. Among the entries with Critical collision level, the one with the highest Source priority will take effect.
2. Among the conflicting entries with the same Source priority, only the last added or edited one will take effect.

12.1.2 Manual Binding

You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN.

Choose the menu **Network Security**→**IP-MAC Binding**→**Manual Binding** to load the following page.

Manual Binding Option

Host Name: (20 characters maximum)

IP Address: (Format: 192.168.0.1)

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Port: ▼

Protect Type: ▼

Manual Binding Table

Select	Host Name	IP Address	MAC Address	VLAN ID	Port	Protect Type	Collision
<input type="button" value="All"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>							

Entry Count: 0

Figure 12-2 Manual Binding

The following entries are displayed on this screen:

➤ **Manual Binding Option**

Host Name: Enter the Host Name.

IP Address: Enter the IP Address of the Host.

MAC Address: Enter the MAC Address of the Host.

VLAN ID: Enter the VLAN ID.

Port: Select the number of port connected to the Host.

Protect Type: Select the Protect Type for the entry.

➤ **Manual Binding Table**

- Select:** Select the desired entry to be deleted. It is multi-optional.
- Host Name:** Displays the Host Name here.
- IP Address:** Displays the IP Address of the Host.
- MAC Address:** Displays the MAC Address of the Host.
- VLAN ID:** Displays the VLAN ID here.
- Port:** Displays the number of port connected to the Host.
- Protect Type:** Displays the Protect Type of the entry.
- Collision:** Displays the Collision status of the entry.
 - **Warning:** Indicates that the collision may be caused by the MSTP function.
 - **Critical:** Indicates that the entry has a collision with the other entries.

12.1.3 ARP Scanning

ARP (Address Resolution Protocol) is used to analyze and map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations correctly. IP address is the address of the Host on Network layer. MAC address, the address of the Host on Data link layer, is necessary for the packet to reach the very device. So the destination IP address carried in a packet need to be translated into the corresponding MAC address.

ARP functions to translate the IP address into the corresponding MAC address and maintain an ARP Table, where the latest used IP address-to-MAC address mapping entries are stored. When the Host communicates with a strange Host, ARP works as the following figure shown.

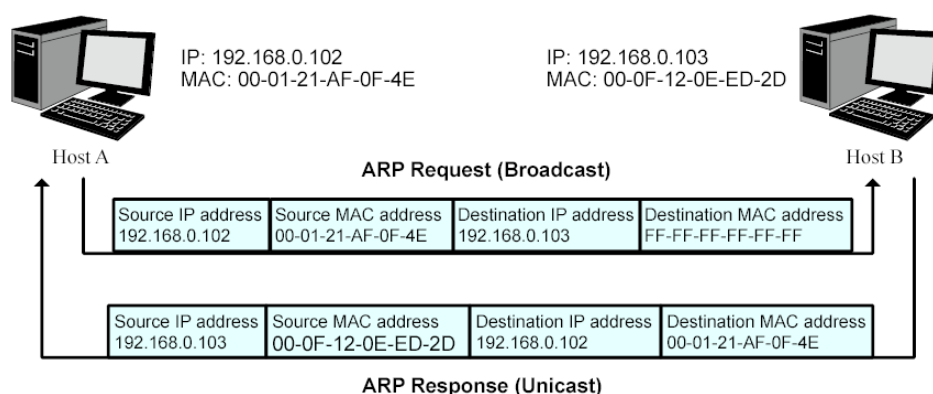


Figure 12-3 ARP Implementation Procedure

1. Suppose there are two hosts in the LAN: Host A and Host B. To send a packet to Host B, Host A checks its own ARP Table first to see if the ARP entry related to the IP address of Host B exists. If yes, Host A will directly send the packets to Host B. If the corresponding MAC address is not found in the ARP Table, Host A will broadcast ARP request packet, which contains the IP address of Host B, the IP address of Host A, and the MAC address of Host A, in the LAN.

2. Since the ARP request packet is broadcasted, all hosts in the LAN can receive it. However, only the Host B recognizes and responds to the request. Host B sends back an ARP reply packet to Host A, with its MAC address carried in the packet.
3. Upon receiving the ARP reply packet, Host A adds the IP address and the corresponding MAC address of Host B to its ARP Table for the further packets forwarding.

ARP Scanning function enables the switch to send the ARP request packets of the specified IP field to the Hosts in the LAN or VLAN. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN and the connected port number of the Host by analyzing the packet and bind them conveniently.

Choose the menu **Network Security**→**IP-MAC Binding**→**ARP Scanning** to load the following page.

Scanning Option

Start IP Address:

End IP Address: Scan

VLAN ID: (1-4094)

Scanning Result

Select	Host Name	IP Address	MAC Address	VLAN ID	Port	Protect Type	Collision
<input type="checkbox"/>	<input style="width: 150px;" type="text"/>					▼	

Refresh
Bind
Delete
Help

Entry Count: 0

Figure 12-4 ARP Scanning

The following entries are displayed on this screen:

➤ **Scanning Option**

- Start IP Address:** Specify the Start IP Address.
- End IP Address:** Specify the End IP Address.
- VLAN ID:** Enter the VLAN ID. If blank, the switch will send the untagged packets for scanning.
- Scan:** Click the **Scan** button to scan the Hosts in the LAN.

➤ **Scanning Result**

- Select:** Select the desired entry to be bound or deleted.
- Host Name:** Displays the Host Name here.
- IP Address:** Displays the IP Address of the Host.
- MAC Address:** Displays the MAC Address of the Host.
- VLAN ID:** Displays the VLAN ID here.
- Port:** Displays the number of port connected to the Host.

- Protect Type:** Displays the Protect Type of the entry.
- Collision:** Displays the Collision status of the entry.
- **Warning:** Indicates that the collision may be caused by the MSTP function.
 - **Critical:** Indicates that the entry has a collision with the other entries.

12.2 DHCP Snooping

Nowadays, the network is getting larger and more complicated. The amount of the PCs always exceeds that of the assigned IP addresses. The wireless network and the laptops are widely used and the locations of the PCs are always changed. Therefore, the corresponding IP address of the PC should be updated with a few configurations. DHCP (Dynamic Host Configuration Protocol, the network configuration protocol optimized and developed basing on the BOOTP, functions to solve the above mentioned problems.

➤ DHCP Working Principle

DHCP works via the "Client/Server" communication mode. The Client applies to the Server for configuration. The Server assigns the configuration information, such as the IP address, to the Client, so as to reach a dynamic employ of the network source. A Server can assign the IP address for several Clients, which is illustrated in the following figure.

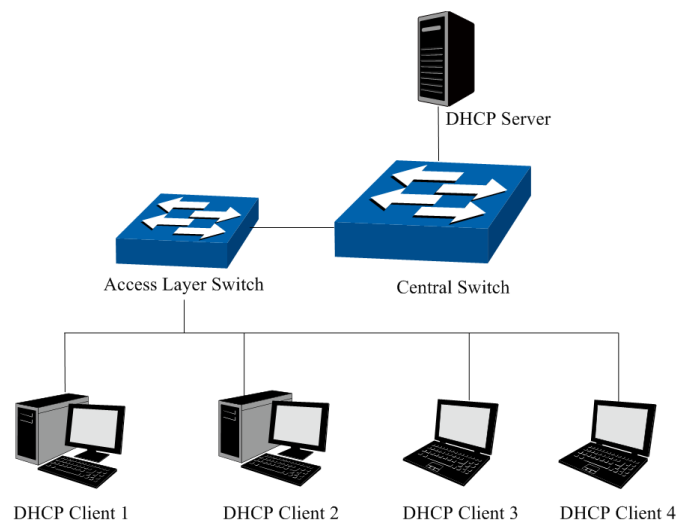


Figure 12-5 Network diagram for DHCP-snooping implementation

For different DHCP Clients, DHCP Server provides three IP address assigning methods:

1. Manually assign the IP address: Allows the administrator to bind the static IP address to the specific Client (e.g.: WWW Server) via the DHCP Server.
2. Automatically assign the IP address: DHCP Server assigns the IP address without an expiration time limitation to the Clients.
3. Dynamically assign the IP address: DHCP Server assigns the IP address with an expiration time. When the time for the IP address expired, the Client should apply for a new one.

The most Clients obtain the IP addresses dynamically, which is illustrated in the following figure.

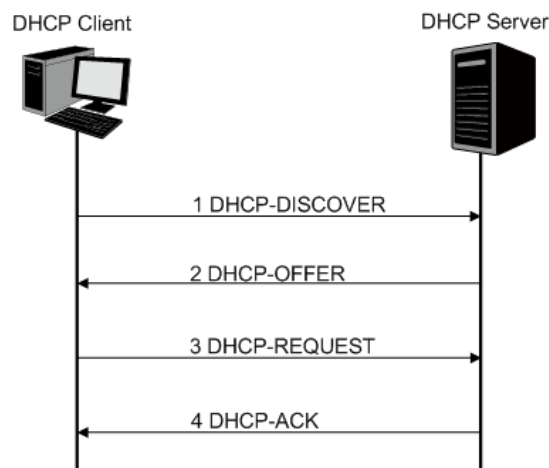


Figure 12-6 Interaction between a DHCP client and a DHCP server

1. DHCP-DISCOVER Stage: The Client broadcasts the DHCP-DISCOVER packet to find the DHCP Server.
2. DHCP-OFFER Stage: Upon receiving the DHCP-DISCOVER packet, the DHCP Server selects an IP address from the IP pool according to the assigning priority of the IP addresses and replies to the Client with DHCP-OFFER packet carrying the IP address and other information.
3. DHCP-REQUEST Stage: In the situation that there are several DHCP Servers sending the DHCP-OFFER packets, the Client will only respond to the first received DHCP-OFFER packet and broadcast the DHCP-REQUEST packet which includes the assigned IP address of the DHCP-OFFER packet.
4. DHCP-ACK Stage: Since the DHCP-REQUEST packet is broadcasted, all DHCP Servers on the network segment can receive it. However, only the requested Server processes the request. If the DHCP Server acknowledges assigning this IP address to the Client, it will send the DHCP-ACK packet back to the Client. Otherwise, the Server will send the DHCP-NAK packet to refuse assigning this IP address to the Client.

➤ Option 82

The DHCP packets are classified into 8 types with the same format basing on the format of BOOTP packet. The difference between DHCP packet and BOOTP packet is the Option field. The Option field of the DHCP packet is used to expand the function, for example, the DHCP can transmit the control information and network parameters via the Option field, so as to assign the IP address to the Client dynamically. For the details of the DHCP Option, please refer to RFC 2132.

Option 82 records the location of the DHCP Client. Upon receiving the DHCP-REQUEST packet, the switch adds the Option 82 to the packet and then transmits the packet to DHCP Server. Administrator can be acquainted with the location of the DHCP Client via Option 82 so as to locate the DHCP Client for fulfilling the security control and account management of Client. The Server supported Option 82 also can set the distribution policy of IP addresses and the other parameters according to the Option 82, providing more flexible address distribution way.

Option 82 can contain 255 sub-options at most. If Option 82 is defined, at least a sub-option should be defined. This switch supports two sub-options: Circuit ID and Remote ID. Since there is no universal standard about the content of Option 82, different manufacturers define the sub-options of Option 82 to their need. For this switch, the sub-options are defined as the following: The Circuit ID is defined to be the number of the port which receives the DHCP Request packets and its VLAN number. The Remote ID is defined to be the MAC address of DHCP Snooping device which receives the DHCP Request packets from DHCP Clients.

➤ DHCP Cheating Attack

During the working process of DHCP, generally there is no authentication mechanism between Server and Client. If there are several DHCP servers in the network, network confusion and security problem will happen. The common cases incurring the illegal DHCP servers are the following two:

- It's common that the illegal DHCP server is manually configured by the user by mistake.
- Hacker exhausted the IP addresses of the normal DHCP server and then pretended to be a legal DHCP server to assign the IP addresses and the other parameters to Clients. For example, hacker used the pretended DHCP server to assign a modified DNS server address to users so as to induce the users to the evil financial website or electronic trading website and cheat the users of their accounts and passwords. The following figure illustrates the DHCP Cheating Attack implementation procedure.

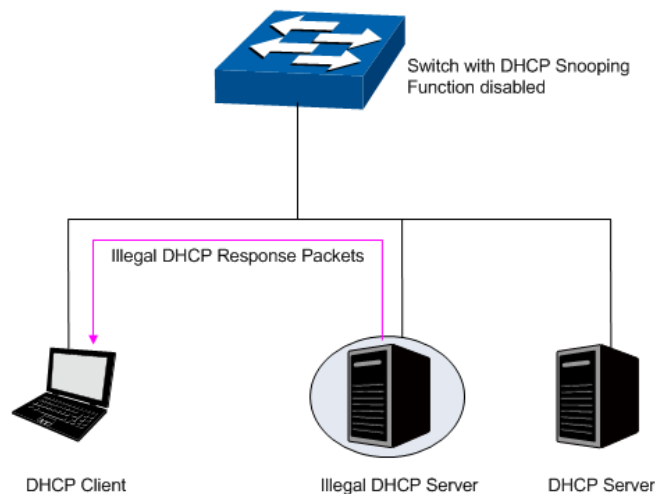


Figure 12-7 DHCP Cheating Attack Implementation Procedure

DHCP Snooping feature only allows the port connected to the DHCP Server as the trusted port to forward 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 packets on the distrusted port, so as to enhance the network security.

The **DHCP Snooping** function is implemented on the **DHCP Snooping** and **Option 82** pages.

12.2.1 DHCP Snooping

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

DHCP Snooping Config

DHCP Snooping: Enable Disable

Global Flow Control: pps

Decline Threshold: pps

Decline Flow Control: pps

Port Config

Port

Select	Port	Trusted Port	MAC Verify	Flow Control	Decline Protect	LAG
<input type="checkbox"/>		<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	
<input type="checkbox"/>	1	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	2	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	3	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	4	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	5	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	6	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	7	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	8	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	9	Enable	Disable	Disable	Disable	---
<input type="checkbox"/>	10	Enable	Disable	Disable	Disable	---

Figure 12-8 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.

The following entries are displayed on this screen:

➤ DHCP Snooping Config

- DHCP Snooping:** Enable or disable the DHCP Snooping function globally.
- Global Flow Control:** Select the value to specify the maximum amount of DHCP messages that can be forwarded by the switch per second. The excessive messages will be discarded.
- Decline Threshold:** Select the value to specify the minimum transmission rate of the Decline packets to trigger the Decline protection for the specific port.

Decline Flow Control: Select the value to specify the Decline Flow Control. The traffic flow of the corresponding port will be limited to be this value if the transmission rate of the Decline packets exceeds the Decline Threshold.

➤ **Port Config**

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

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

Port: Displays the port number.

Trusted Port: Enable or disable the port to be a Trusted Port. Only the Trusted Port can receive the DHCP packets from DHCP servers.

MAC Verify: Enable or disable the MAC Verify feature. There are two fields of the DHCP packet containing the MAC address of the Host. The MAC Verify feature is to compare the two fields and discard the packet if the two fields are different.

Flow Control: Enable or disable the Flow Control feature for the DHCP packets. The excessive DHCP packets will be discarded.

Decline Protect: Enable or disable the Decline Protect feature.

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

12.2.2 Option 82

You can configure Option 82 on the specified port.

Choose the menu **Network Security**→**DHCP Snooping**→**Option 82** to load the following page.

Option 82 Config

From Port: To Port:

Option 82 Support: Enable Disable

Existed Option 82 field:

Format:

Customization:

Circuit ID:

Remote ID:

Port	Option 82 Support	Operation Strategy	Format	Circuit ID	Remote ID	LAG
1	Disable	Keep	Normal	---	---	---
2	Disable	Keep	Normal	---	---	---
3	Disable	Keep	Normal	---	---	---
4	Disable	Keep	Normal	---	---	---
5	Disable	Keep	Normal	---	---	---
6	Disable	Keep	Normal	---	---	---
7	Disable	Keep	Normal	---	---	---
8	Disable	Keep	Normal	---	---	---
9	Disable	Keep	Normal	---	---	---
10	Disable	Keep	Normal	---	---	---

The following entries are displayed on this screen:

➤ **Option 82 Config**

From/To Port: Select the port or port range to which you want to apply the Option 82 feature.

Option 82 Support: Enable or disable the Option 82 feature.

Existed Option 82 field: Select the operation for the existed Option 82 field of the DHCP request packets from the Host. The option 82 field in DHCP reply packets will be remove when the option 82 feature is enable, no matter which operation is configured for the existed option 82 filed.

- **Keep:** Indicates to keep the Option 82 field of the packets.
- **Replace:** Indicates to replace the Option 82 field of the packets with the switch defined one.
- **Drop:** Indicates to discard the packets including the Option 82 field.

Format: Select the format of option 82 sub-option value field.

- **Normal:** Indicates that the format of sub-option value field is TLV (type-length-value).
- **Private:** Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Circuit ID: Enter the sub-option Circuit ID for the customized Option 82.

Remote ID: Enter the sub-option Remote ID for the customized Option 82.

12.3 ARP Inspection

According to the ARP Implementation Procedure stated in 12.1.3 ARP Scanning, it can be found that ARP protocol can facilitate the Hosts in the same network segment to communicate with one another or access to external network via Gateway. However, since ARP protocol is implemented with the premise that all the Hosts and Gateways are trusted, there are high security risks during ARP Implementation Procedure in the actual complex network. Thus, the cheating attacks against ARP, such as imitating Gateway, cheating Gateway, cheating terminal Hosts and ARP Flooding Attack, frequently occur to the network, especially to the large network such as campus network 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.

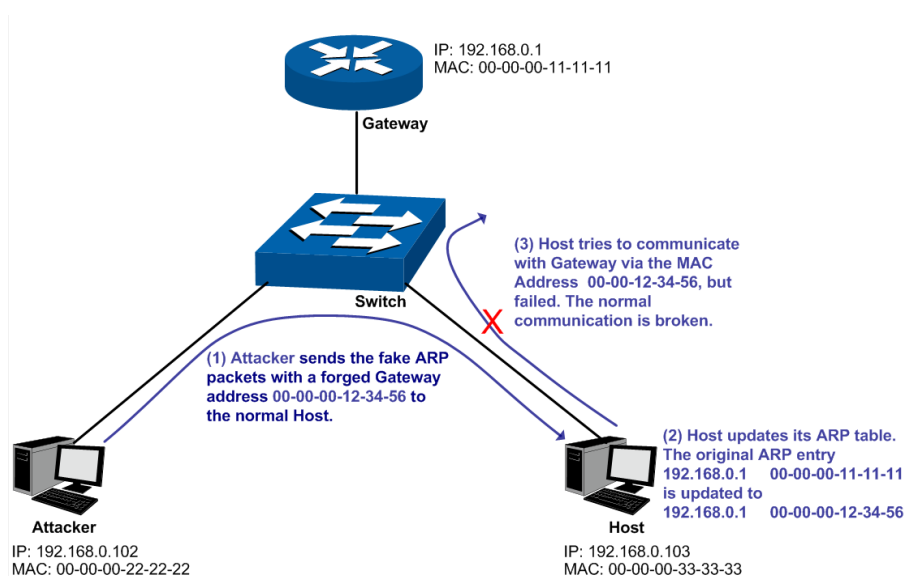


Figure 12-9 ARP Attack - Imitating Gateway

As the above figure shown, the attacker sends the fake ARP packets with a forged Gateway address to the normal Host, and then the Host will automatically update the ARP table after receiving the ARP packets. When the Host tries to communicate with Gateway, the Host will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

➤ Cheating Gateway

The attacker sends the wrong IP address-to-MAC address mapping entries of Hosts to the Gateway, which causes that the Gateway cannot communicate with the legal terminal Hosts

normally. The ARP Attack implemented by cheating Gateway is illustrated in the following figure.

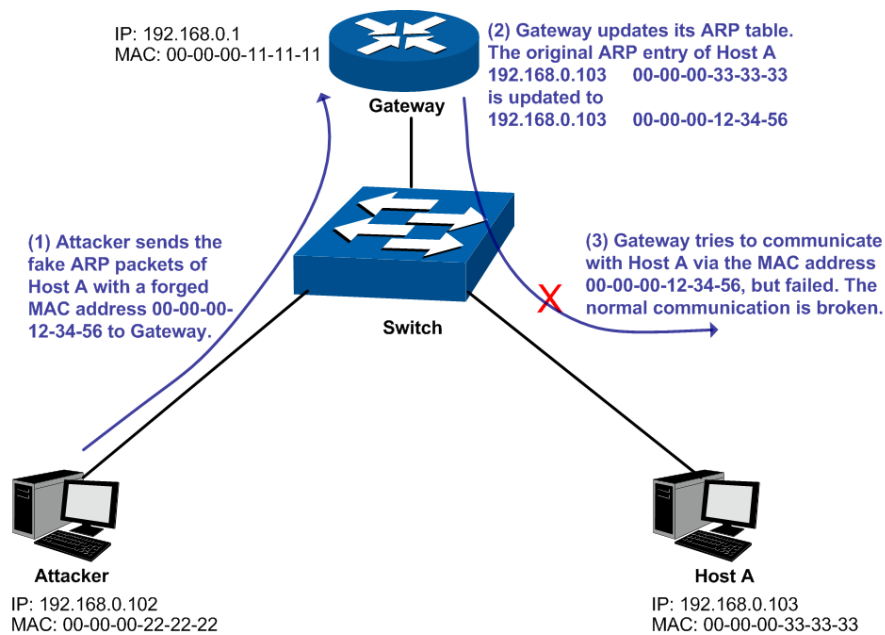


Figure 12-10 ARP Attack – Cheating Gateway

As the above figure shown, the attacker sends the fake ARP packets of Host A to the Gateway, and then the Gateway will automatically update its ARP table after receiving the ARP packets. When the Gateway tries to communicate with Host A in LAN, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

➤ **Cheating Terminal Hosts**

The attacker sends the false IP address-to-MAC address mapping entries of terminal Host/Server to another terminal Host, which causes that the two terminal Hosts in the same network segment cannot communicate with each other normally. The ARP Attack implemented by cheating terminal Hosts is illustrated in the following figure.

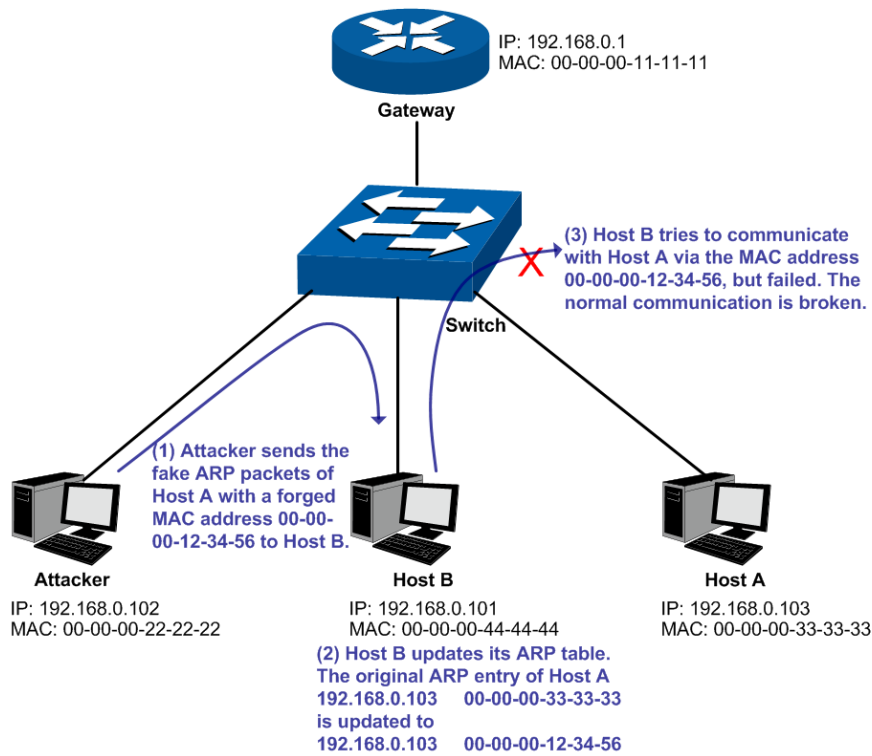


Figure 12-11 ARP Attack – Cheating Terminal Hosts

As the above figure shown, the attacker sends the fake ARP packets of Host A to Host B, and then Host B will automatically update its ARP table after receiving the ARP packets. When Host B tries to communicate with Host A, it will encapsulate this false destination MAC address for packets, which results in a breakdown of the normal communication.

➤ **Man-In-The-Middle Attack**

The attacker continuously sends the false ARP packets to the Hosts in LAN so as to make the Hosts maintain the wrong ARP table. When the Hosts in LAN communicate with one another, they will send the packets to the attacker according to the wrong ARP table. Thus, the attacker can get and process the packets before forwarding them. During the procedure, the communication packets information between the two Hosts are stolen in the case that the Hosts were unaware of the attack. That is called Man-In-The-Middle Attack. The Man-In-The-Middle Attack is illustrated in the following figure.

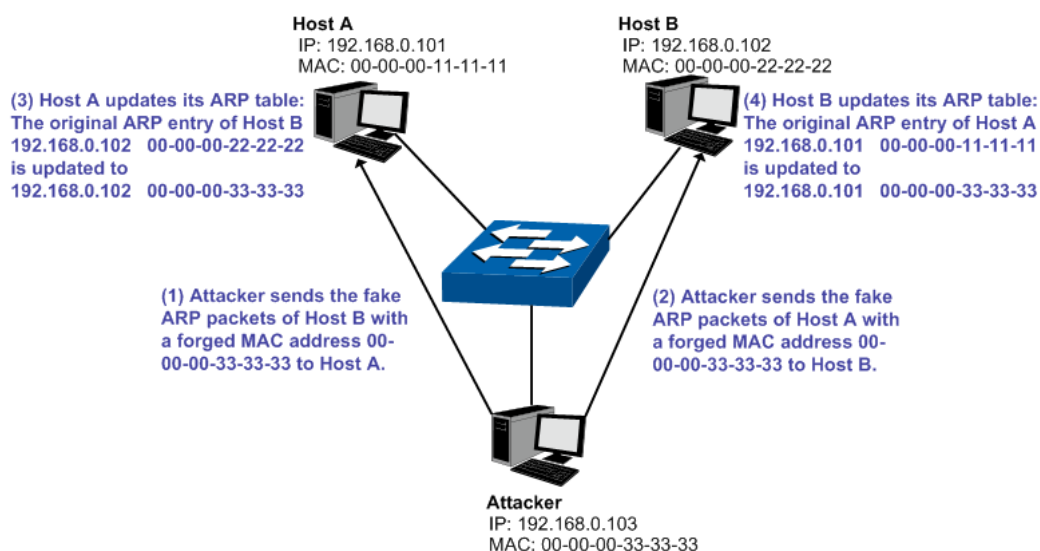


Figure 12-12 Man-In-The-Middle Attack

Suppose there are three Hosts in LAN connected with one another through a switch.

Host A: IP address is 192.168.0.101; MAC address is 00-00-00-11-11-11.

Host B: IP address is 192.168.0.102; MAC address is 00-00-00-22-22-22.

Attacker: IP address is 192.168.0.103; MAC address is 00-00-00-33-33-33.

1. First, the attacker sends the false ARP response packets.
2. Upon receiving the ARP response packets, Host A and Host B updates the ARP table of their own.
3. When Host A communicates with Host B, it will send the packets to the false destination MAC address, i.e. to the attacker, according to the updated ARP table.
4. After receiving the communication packets between Host A and Host B, the attacker processes and forwards the packets to the correct destination MAC address, which makes Host A and Host B keep a normal-appearing communication.
5. The attacker continuously sends the false ARP packets to the Host A and Host B so as to make the Hosts always maintain the wrong ARP table.

In the view of Host A and Host B, their packets are directly sent to each other. But in fact, there is a Man-In-The-Middle stolen the packets information during the communication procedure. This kind of ARP attack is called Man-In-The-Middle attack.

➤ **ARP Flooding Attack**

The attacker broadcasts a mass of various fake ARP packets in a network segment to occupy the network bandwidth viciously, which results in a dramatic slowdown of network speed. Meantime, the Gateway learns the false IP address-to-MAC address mapping entries from these ARP packets and updates its ARP table. As a result, the ARP table is fully occupied by the false entries and unable to learn the ARP entries of legal Hosts, which causes that the legal Hosts cannot access the external network.

The IP-MAC Binding function allows the switch to bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together when the Host connects to the switch. Basing on the predefined IP-MAC Binding entries, the ARP Inspection functions to detect the ARP packets and filter the illegal ARP packet so as to prevent the network from ARP attacks.

The **ARP Inspection** function is implemented on the **ARP Detect**, **ARP Defend** and **ARP Statistics** pages.

12.3.1 ARP Detect

ARP Detect feature enables the switch to detect the ARP packets basing on the bound entries in the IP-MAC Binding Table and filter the illegal ARP packets, so as to prevent the network from ARP attacks, such as the Network Gateway Spoofing and Man-In-The-Middle Attack, etc.

Choose the menu **Network Security**→**ARP Inspection**→**ARP Detect** to load the following page.

Note:

It's recommended to configure the up-linked port and LAG member as trusted port.

Figure 12-13 ARP Detect

The following entries are displayed on this screen:

➤ **ARP Detect**

ARP Detect: Enable or disable the ARP Detect function, and click the **Apply** button to apply.

➤ **Trusted Port**

Trusted Port: Select the port for which the ARP Detect function is unnecessary as the Trusted Port. The specific ports, such as up-linked port, routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ARP Trusted Port before enabling the ARP Detect function.

Configuration Procedure:

Step	Operation	Description
1	Bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together.	Required. On the IP-MAC Binding page, bind the IP address, MAC address, VLAN ID and the connected Port number of the Host together via Manual Binding, ARP Scanning or DHCP Snooping.
2	Enable the protection for the bound entry.	Required. On the Network Security→IP-MAC Binding→Binding Table page, specify a protect type for the corresponding bound entry.
3	Specify the trusted port.	Required. On the Network Security→ARP Inspection→ARP Detect page, specify the trusted port. The specific ports, such as up-linked port, routing port and LAG port, should be set as Trusted Port.
4	Enable ARP Detect feature.	Required. On the Network Security→ARP Inspection→ARP Detect page, enable the ARP Detect feature.

12.3.2 ARP Defend

With the ARP Defend enabled, the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP Attack flood.

Choose the menu **Network Security→ARP Inspection→ARP Defend** to load the following page.

ARP Defend Port

Select	Port	Defend	Speed (10-100) pps	Current Speed (pps)	Status	LAG	Operation
<input type="checkbox"/>		<input type="text" value="Disable"/> ▼	<input type="text"/>				
<input type="checkbox"/>	1	Disable	15	---	---	---	---
<input type="checkbox"/>	2	Disable	15	---	---	---	---
<input type="checkbox"/>	3	Disable	15	---	---	---	---
<input type="checkbox"/>	4	Disable	15	---	---	---	---
<input type="checkbox"/>	5	Disable	15	---	---	---	---
<input type="checkbox"/>	6	Disable	15	---	---	---	---
<input type="checkbox"/>	7	Disable	15	---	---	---	---
<input type="checkbox"/>	8	Disable	15	---	---	---	---
<input type="checkbox"/>	9	Disable	15	---	---	---	---
<input type="checkbox"/>	10	Disable	15	---	---	---	---

Figure 12-14 ARP Defend

The following entries are displayed on this screen:

➤ **ARP Defend**

- Port Select:** Click the **Select** button to quick-select the corresponding port based on the port number you entered.
- Select:** Select your desired port for configuration. It is multi-optional.
- Port:** Displays the port number.
- Defend:** Enable or disable the ARP Defend feature for the port.
- Speed:** Enter a value to specify the maximum amount of the received ARP packets per second.
- Current Speed:** Displays the current speed of the received ARP packets.
- Status:** Displays the status of the ARP attack.
- LAG:** Displays the LAG to which the port belongs to.
- Operation:** Click the **Recover** button to restore the port to the normal status. The ARP Defend for this port will be re-enabled.



Note:

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

12.3.3 ARP Statistics

ARP Statistics feature displays the number of the illegal ARP packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **Network Security**→**ARP Inspection**→**ARP Statistics** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Interval: sec (3-300)

Illegal ARP Packet

Port	Trusted Port	Illegal ARP Packet	Port	Trusted Port	Illegal ARP Packet
1	No	---	2	No	---
3	No	---	4	No	---
5	No	---	6	No	---
7	No	---	8	No	---
9	No	---	10	No	---

Refresh Clear Help

Figure 12-15 ARP Statistics

The following entries are displayed on this screen:

➤ **Auto Refresh**

- Auto Refresh:** Enable or disable the Auto Refresh feature.
- Refresh Interval:** Specify the refresh interval to display the ARP Statistics.

➤ **Illegal ARP Packet**

- Port:** Displays the port number.
- Trusted Port:** Indicates the port is an ARP Trusted Port or not.
- Illegal ARP Packet:** Displays the number of the received illegal ARP packets.

12.4 DoS Defend

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network.

With DoS Defend function enabled, the switch can analyze the specific fields of the IP packets and distinguish the malicious DoS attack packets. Upon detecting the packets, the switch will discard the illegal packets directly and limit the transmission rate of the legal packets if the over legal packets may incur a breakdown of the network. The switch can defend several types of DoS attack listed in the following table.

DoS Attack Type	Description
Land Attack	The attacker sends a specific fake SYN packet to the destination Host. Since both the source IP address and the destination IP address of the SYN packet are set to be the IP address of the Host, the Host will be trapped in an endless circle for building the initial connection. The performance of the network will be reduced extremely.
Scan SYNFIN	The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal. The switch can defend this type of illegal packet.
Xmascan	The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.
NULL Scan Attack	The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all the control fields set to 0 are considered as the illegal packets.
SYN sPort less 1024	The attacker sends the illegal packet with its TCP SYN field set to 1 and source port less than 1024.

DoS Attack Type	Description
Smurf Attack	By pretending to be a Host, the attacker broadcasts request packets for ICMP response in the LAN. When receiving the request packet, all the Hosts in the LAN will respond and send the reply packets to the actual Host, which will causes this Host to be attacked.
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.
winNuke Attack	Since the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this type of packets to the TCP port139 (NetBIOS) of the Host with the Operation System bugs, which will cause the Host with a blue screen.
Ping Of Death	ICMP ECHO Request Packet whose sum of "Fragment Offset" and "Total Length" fields in the IP header is greater than 65535 may cause Ping of Death attack. As the maximum packet length of an IPv4 packet including the IP header is 65,535 bytes, many computer systems could not properly handle this malformed or malicious ICMP ECHO Request Packet. Thus, the hosts may break down or reboot automatically when receive this kind of packet.

Table 12-1 Defendable DoS Attack Types

12.4.1 DoS Defend

On this page, you can enable the DoS Defend type appropriate to your need.

Choose the menu **Network Security**→**DoS Defend**→**DoS Defend** to load the following page.

Global Configure

DoS Defend: Enable Disable

Select	Defend Type
<input type="checkbox"/>	Land Attack
<input type="checkbox"/>	Scan SYNFIN
<input type="checkbox"/>	Xmascan
<input type="checkbox"/>	NULL Scan
<input type="checkbox"/>	SYN sPort less 1024
<input type="checkbox"/>	Blat Attack
<input type="checkbox"/>	Ping Flooding
<input type="checkbox"/>	SYN/SYN-ACK Flooding

Figure 12-16 DoS Defend

The following entries are displayed on this screen:

➤ **Defend Config**

DoS Defend: Allows you to Enable or disable DoS Defend function.

➤ **Defend Table**

Select: Select the entry to enable the corresponding Defend Type.

Defend Type: Displays the Defend Type name.

12.5 802.1X

The 802.1X protocol was developed by IEEE802 LAN/WAN committee to deal with the security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to solve mainly authentication and security problems.

802.1X is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access control devices. With the 802.1X protocol enabled, a supplicant can access the LAN only when it passes the authentication, whereas those failing to pass the authentication are denied when accessing the LAN.

➤ **Architecture of 802.1X Authentication**

802.1X adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system, as shown in the following figure.

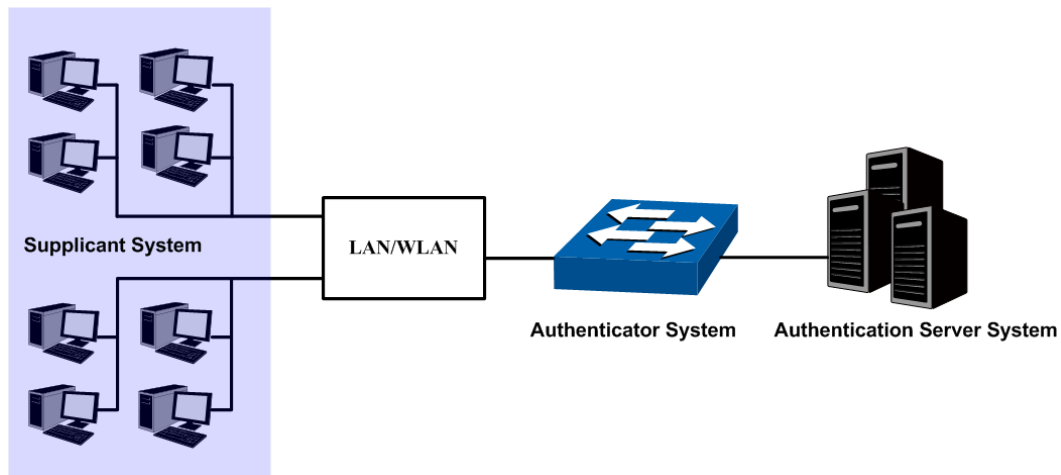


Figure 12-17 Architecture of 802.1X authentication

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.

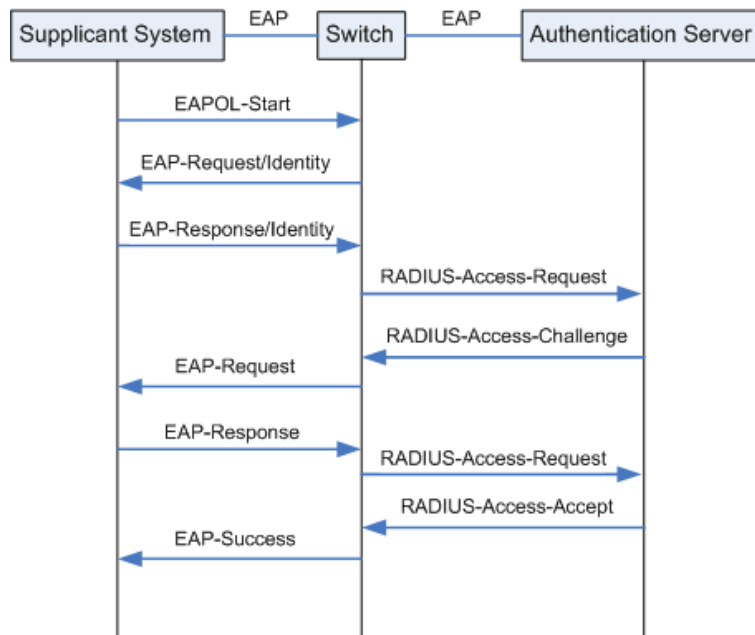


Figure 12-18 EAP-MD5 Authentication Procedure

- 1) A supplicant system launches an 802.1X client program via its registered user name and password to initiate an access request through the sending of an EAPOL-Start packet to the switch. The 802.1X client program then forwards the packet to the switch to start the authentication process.
- 2) Upon receiving the authentication request packet, the switch sends an EAP-Request/Identity packet to ask the 802.1X client program for the user name.
- 3) The 802.1X client program responds by sending an EAP-Response/Identity packet to the switch with the user name included. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.

- 4) Upon receiving the user name from the switch, the RADIUS server retrieves the user name, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS Access-Challenge packet. The switch then sends the key to the 802.1X client program.
- 5) Upon receiving the key (encapsulated in an EAP-Request/MD5 Challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-Response/MD5 Challenge packet) to the RADIUS server through the switch. (The encryption is irreversible.)
- 6) The RADIUS server compares the received encrypted password (contained in a RADIUS Access-Request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS Access-Accept packet and an EAP-Success packet) to the switch to indicate that the supplicant system is authorized.
- 7) The switch changes the state of the corresponding port to accepted state to allow the supplicant system access the network. And then the switch will monitor the status of supplicant by sending hand-shake packets periodically. By default, the switch will force the supplicant to log off if it cannot get the response from the supplicant for two times.
- 8) The supplicant system can also terminate the authenticated state by sending EAPOL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

2. EAP Terminating Mode

In this mode, packet transmission is terminated at authenticator systems and the EAP packets are mapped into RADIUS packets. Authentication and accounting are accomplished through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. This switch supports the PAP terminating mode. The authentication procedure of PAP is illustrated in the following figure.

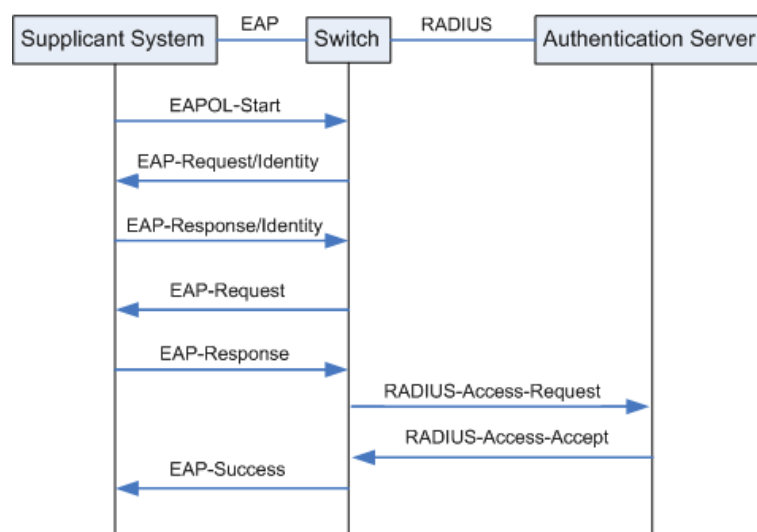


Figure 12-19 PAP Authentication Procedure

In PAP mode, the switch encrypts the password and sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS

server for further authentication. Whereas the randomly-generated key in EAP-MD5 relay mode is generated by the authentication server, and the switch is responsible to encapsulate the authentication packet and forward it to the RADIUS server.

➤ **802.1X Timer**

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way:

1. **Supplicant system timer (Supplicant Timeout):** This timer is triggered by the switch after the switch sends a request packet to a supplicant system. The switch will resend the request packet to the supplicant system if the supplicant system fails to respond in the specified timeout period.
2. **RADIUS server timer (Server Timeout):** This timer is triggered by the switch after the switch sends an authentication request packet to RADIUS server. The switch will resend the authentication request packet if the RADIUS server fails to respond in the specified timeout period.
3. **Quiet-period timer (Quiet Period):** This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the specified period before it processes another authentication request re-initiated by the supplicant system.

➤ **Guest VLAN**

Guest VLAN function enables the supplicants that do not pass the authentication to access the specific network resource.

By default, all the ports connected to the supplicants belong to a VLAN, i.e. Guest VLAN. Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated before accessing external resources. After passing the authentication, the ports will be removed from the Guest VLAN and be allowed to access the other resources.

With the Guest VLAN function enabled, users can access the Guest VLAN to install 802.1X client program or upgrade their 802.1x clients without being authenticated. If there is no supplicant past the authentication on the port in a certain time, the switch will add the port to the Guest VLAN.

With 802.1X function enabled and Guest VLAN configured, after the maximum number retries have been made to send the EAP-Request/Identity packets and there are still ports that have not sent any response back, the switch will then add these ports into the Guest VLAN according to their link types. Only when the corresponding user passes the 802.1X authentication, the port will be removed from the Guest VLAN and added to the specified VLAN. In addition, the port will back to the Guest VLAN when its connected user logs off.

The **802.1X** function is implemented on the **Global Config** and **Port Config** pages.

12.5.1 Global Config

On this page, you can enable the 802.1X authentication function globally and control the authentication process by specifying the Authentication Method, Guest VLAN and various Timers.

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

The image shows two configuration pages. The top page is titled "Global Config" and contains the following settings:

- 802.1X: Enable Disable
- Auth Method: (dropdown menu)
- Handshake: Enable Disable
- Guest VLAN: Enable Disable
- Guest VLAN ID: (1-4094)
- Accounting: Enable Disable
- VLAN Assignment: Enable Disable

An "Apply" button is located to the right of the Guest VLAN settings.

The bottom page is titled "Authentication Config" and contains the following settings:

- Quiet: Enable Disable
- Quiet Period: sec (1-999)
- Retry Times: (1-9)
- Supplicant Timeout: sec (1-9)

"Apply" and "Help" buttons are located to the right of the Quiet Period and Retry Times settings.

Figure 12-20 Global Config

The following entries are displayed on this screen:

➤ **Global Config**

802.1X:

Enable or disable the 802.1X function.

Auth Method:

Select the Authentication Method from the pull-down list.

- **EAP:** IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP protocol packets with authentication data can be encapsulated in the advanced protocol (such as RADIUS) packets to be transmitted to the authentication server.
- **PAP:** IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The transmission of EAP packets is terminated at the switch and the EAP packets are converted to the other protocol (such as RADIUS) packets for transmission.

Handshake:	Enable or disable the Handshake feature. The Handshake feature is used to detect the connection status of the TP-Link 802.1X Client with the switch. Please disable Handshake feature if you are using other client softwares instead of TP-Link 802.1X Client.
Guest VLAN:	Enable or disable the Guest VLAN feature.
Guest VLAN ID:	Enter your desired VLAN ID to enable the Guest VLAN feature. The supplicants in the Guest VLAN can access the specified network source.
Accounting:	Enable or disable the 802.1X accounting feature.
VLAN Assignment:	<p>Enable or disable the 802.1X VLAN assignment feature.</p> <p>802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.</p> <p>If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN.</p> <p>If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN.</p> <p>If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.</p>

➤ **Authentication Config**

Quiet:	Enable or disable the Quiet timer.
Quiet Period:	Specify a value for Quiet Period. Once the supplicant failed to the 802.1X Authentication, then the switch will not respond to the authentication request from the same supplicant during the Quiet Period.
Retry Times:	Specify the maximum transfer times of the repeated authentication request.
Supplicant Timeout:	Specify the maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant.

12.5.2 Port Config

On this page, you can configure the 802.1X features for the ports basing on the actual network. Choose the menu **Network Security**→**802.1X**→**Port Config** to load the following page.

Port Config

Port

Select	Port	Status	MAB	Guest VLAN	Control Mode	Control Type	Authorized	LAG
<input type="checkbox"/>		Disable ▾	Disable ▾	Disable ▾	Auto ▾	MAC Based ▾		
<input type="checkbox"/>	1	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	2	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	3	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	4	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	5	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	6	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	7	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	8	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	9	Disable	Disable	Disable	Auto	MAC Based	Yes	---
<input type="checkbox"/>	10	Disable	Disable	Disable	Auto	MAC Based	Yes	---

Figure 12-21 Port Config

The following entries are displayed on this screen:

➤ **Port Config**

- Port Select:** Click the **Select** button to quick-select the corresponding port based on the port number you entered.
- Select:** Select your desired port for configuration. It is multi-optional.
- Port:** Displays the port number.
- Status:** Enable or disable the 802.1X authentication feature for the port.
- MAB:** Enable or disable the MAB (MAC-Based Authentication Bypass) feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1X capability. For example, most printers, IP phones and fax machines do not have 802.1X capability.
- Guest VLAN:** Enable or disable the Guest VLAN feature for the port.
- Control Mode:** Specify the Control Mode for the port.
- **Auto:** In this mode, the port will normally work only after passing the 802.1X Authentication.
 - **Force-Authorized:** In this mode, the port can work normally without passing the 802.1X Authentication.
 - **Force-Unauthorized:** In this mode, the port is forbidden working for its fixed unauthorized status.

Control Type:

Specify the Control Type for the port.

- **MAC Based:** Any client connected to the port should pass the 802.1X Authentication for access.
- **Port Based:** All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1X Authentication.

Authorized:

Displays the authentication status of the port.

LAG:

Displays the LAG to which the port belongs to.

Configuration Procedure:

Step	Operation	Description
1	Install the 802.1X client software.	Required. For the client computers, you are required to install the TP-Link 802.1X Client provided on the CD. Please refer to the software guide in the same directory with the software for more information.
2	Configure the 802.1X globally.	Required. By default, the global 802.1X function is disabled. On the Network Security→802.1X→Global Config page, configure the 802.1X function globally.
3	Configure the 802.1X for the port.	Required. On the Network Security→802.1X→Port Config page, configure the 802.1X feature for the port of the switch basing on the actual network.
4	Connect an authentication server to the switch and do some configuration.	Required. Record the information of the client in the LAN to the authentication server and configure the corresponding authentication username and password for the client.
5	Enable the AAA function globally.	Required. On the Network Security→AAA→Global Config page, enable the AAA function globally.
6	Configure the parameters of the authentication server.	Required. On the Network Security→AAA→RADIUS Config page, configure the parameters of the RADIUS server.

**Note:**

1. The 802.1X function takes effect only when it is enabled globally on the switch and for the port.
2. The 802.1X function cannot be enabled for LAG member ports. That is, the port with 802.1X function enabled cannot be added to the LAG.
3. The 802.1X function should not be enabled for the port connected to the authentication server.

12.6 AAA

➤ Overview

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

Username and password pairs are used for login and privilege authentication. The authentication can be processed locally in the switch or centrally in the RADIUS/TACACS+ server(s). The local authentication username and password pairs can be configured in [4.2 User Management](#).

➤ Applicable Access Application

The authentication can be applied on the following access applications: Console, Telnet, SSH and HTTP.

➤ Authentication Method List

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

The administrator can set the authentication methods in a preferable order in the list. The switch uses the first listed method to authenticate users, if that method fails to respond, the switch selects the next authentication method in the method list. This process continues until there is a successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this circle, which means the secure server or the local switch denies the user's access, the authentication process stops and no other authentication methods are attempted.

➤ 802.1X Authentication

802.1X protocol uses the RADIUS to provide detailed accounting information and flexible administrative control over authentication process. The Dot1x List feature defines the RADIUS server groups in the 802.1X authentication.

➤ RADIUS/TACACS+ Server

Users can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

➤ Server Group

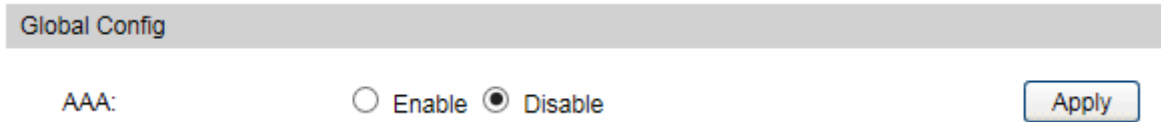
Users can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

The switch has two built-in authentication server group, one for RADIUS and the other for TACACS+. These two server groups cannot be deleted, and the user-defined RADIUS/TACACS+ server will join these two server groups automatically.

12.6.1 Global Config

This page is used to Enable or disable the AAA function globally.

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



Global Config

AAA: Enable Disable

Figure 12-1 AAA Global Config

➤ Configuration Procedure:

Click Enable to enable the AAA function globally.

12.6.2 Privilege Elevation

This page is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

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



Enable Admin

Enable Password:

Figure 12-2 Privilege Elevate

➤ Configuration Procedure:

Enter the Enable Password and click Enable button to elevate the current logged-in user from guest to admin. Only admin users can configure the following AAA settings.



Tips:

If the Enable password is verified locally, the Enable password should be previously set by the admin users using the command lines. For more details please refer to the command **enable admin password** in the Command Line Interface Guide on the resource CD.

12.6.3 RADIUS Server Config

This page is used to configure the authentication servers running the RADIUS security protocols.

Choose the menu **Network Security**→**AAA**→**RADIUS Config** to load the following page.

Server Config

Server IP: (Format:192.168.0.1)
 Shared Key:
 Auth Port: (1-65535)
 Acct Port: (1-65535)
 Retransmit: (1-3)
 Timeout: sec(1-9)
 NAS Identifier:

Server List

Select	Server IP	Shared Key	Auth Port	Acct Port	Retransmit	Timeout	NAS Identifier
<input type="checkbox"/>		<input type="checkbox"/> <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 12-3 RADIUS Server Config

➤ **Configuration Procedure:**

Configure the RADIUS server’s IP and other relevant parameters under the Server Config. View, edit and delete the configured RADIUS servers in the Server list.

➤ **Entry Description:**

- Server IP:** Enter the IP of the server running the RADIUS secure protocol.
- Shared Key:** Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
- Auth Port:** Specify the UDP destination port on the RADIUS server for authentication requests.
- Acct Port:** Specify the UDP destination port on the RADIUS server for accounting requests.
- Retransmit:** Specify the number of times a request is resent to a server if the server does not respond.
- Timeout:** Specify the time interval that the switch waits for the server to reply before resending.
- NAS Identifier:** Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

12.6.4 TACACS+ Server Config

This page is used to configure the authentication servers running the TACACS+ security protocols.

Choose the menu **Network Security**→**AAA**→**TACACS+ Config** to load the following page.

The screenshot displays the TACACS+ configuration interface. The top section, titled "Server Config", contains four input fields: "Server IP" with the value "0.0.0.0" and a format hint "(format:192.168.0.2)", "Timeout" with the value "5" and a unit hint "s(1-9)", "Shared Key" which is empty, and "Port" with the value "49" and a range hint "(1-65535)". An "Add" button is located to the right of the "Shared Key" field. Below this is the "Server List" section, which is a table with five columns: "Select", "Server IP", "Timeout", "Shared Key", and "Port". The table contains one row with empty input fields for each column, and a checkbox in the "Select" column. Below the table are three buttons: "Apply", "Delete", and "Help".

Figure 12-4 TACACS+ Server Config

➤ **Configuration Procedure:**

Configure the TACACS+ server's IP and other relevant parameters under the Server Config.

View, edit and delete the configured TACACS+ servers in the Server list.

➤ **Entry Description:**

Server IP: Enter the IP of the server running the TACACS+ secure protocol.

Shared Key: Enter the shared key between the TACACS+ server and the switch. The TACACS+ server and the switch use the key string to encrypt passwords and exchange responses.

Timeout: Specify the time interval that the switch waits for the server to reply before resending.

Port: Specify the TCP port used on the TACACS+ server for AAA.

12.6.5 Authentication Server Group Config

On this page users can group authentication servers running the same secure protocol for authentication. The switch has two built-in authentication server group, one for RADIUS and the other for TACACS+. These two server groups cannot be edited or deleted. The server entries in one group are tried in the order they are added.

Choose the menu **Network Security**→**AAA**→**Server Group** to load the following page.

Add New Server Group

Server Group:

Server Type:

Server Group List

Select	Server Group	Server Type	Operation
<input type="checkbox"/>			
<input type="checkbox"/>	radius	RADIUS	Edit
<input type="checkbox"/>	tacacs	TACACS+	Edit

Figure 12-5 Create New Server Group

Add Server IP

Server Group:

Server Type:

Server IP:

Server IP List

Select	Server Ip
<input type="checkbox"/>	
<input type="checkbox"/>	10.10.10.10

Figure 12-6 Add Server to Server Group

➤ **Configuration Procedure:**

- 1) Configure the Server Group name and Server Type to create a server group. (Figure 12-5)
- 2) Click **edit** in the Server Group List to configure the corresponding server group. (Figure 12-5)
- 3) Select Server IP you have previously created and click **Add** to add the server to the server group. (Figure 12-6)

View and delete the configured server groups in the Server Group List.

View and delete the configured servers in the Server List.

➤ **Entry Description:**

- Server Group:** Define a server group with a group name.
- Server Type:** Specify the server type as RADIUS or TACACS+.
- Server IP** Select the IP of the server you have previously configured.

**Note:**

1. The two built-in server groups radius and tacacs cannot be deleted or edited.
2. Up to 16 servers can be added to one server group.

12.6.6 Authentication Method List Config

Before you configure AAA authentication on a certain application, you should define an authentication method list first. An authentication method list describes the sequence and authentication method to be queried to authenticate a user.

The switch uses the first method listed to authenticate users, if that method fails to respond, the switch selects the next authentication method in the method list. This process continues until there is a successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this circle, which means the secure server or the local switch denies the user's access, the authentication process stops and no other authentication methods are attempted.

For example, if a user defines an authentication login method list as tacacs-radius-local, the switch will send an authentication request to the first TACACS+ server in the tacacs server group. If there is no response, the switch will send an authentication request to the second TACACS+ server in the tacacs server group and so on, until the tacacs server group list is exhausted. Then the RADIUS server group will be queried. If no authentication is accomplished in the RADIUS server list, the switch will authenticate the user locally. This forms a backup system for authentication.

Choose the menu **Network Security**→**AAA**→**Authentication List** to load the following page.

Add Method List

Method List Name:

List Type:

Pri1:

Pri2:

Pri3:

Pri4:

Authentication Login Method List

Select	Method List	Pri1	Pri2	Pri3	Pri4
<input type="checkbox"/>		<input type="text" value="--"/>	<input type="text" value="--"/>	<input type="text" value="--"/>	<input type="text" value="--"/>
<input type="checkbox"/>	default	local	--	--	--

Authentication Enable Method List

Select	Method List	Pri1	Pri2	Pri3	Pri4
<input type="checkbox"/>		<input type="text" value="--"/>	<input type="text" value="--"/>	<input type="text" value="--"/>	<input type="text" value="--"/>
<input type="checkbox"/>	default	none	--	--	--

Figure 12-7 Authentication Method List Config

➤ **Configuration Procedure:**

- 1) Enter the method list name.
- 2) Specify the authentication type as Login or Enable.
- 3) Configure the authentication method with priorities. The options are local, none, radius, tacacs or user-defined server groups.

View and delete the configured method priority list in the Authentication Login Method List and Authentication Enable Method List. .

➤ **Entry Description:**

Method List Name:	Define a method list name.
List Type:	Specify the authentication type as Login or Enable. Login stands for the Authentication Login Method List, and Enable stands for the Authentication Enable Method list.
Pri1, Pri2, Pri3, Pri4:	<p>Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.</p> <ul style="list-style-type: none">• local: Use the local database in the switch for authentication.• none: No authentication is used.• radius: Use the remote RADIUS server/server groups for authentication.• tacacs: Use the remote TACACS+ server/server groups for authentication.• user-defined server group: Use the user-defined server groups for authentication.



Tips:

If the Enable password is verified on the remote RADIUS server, the switch will send the Enable authentication with the default username as \$enable\$.

12.6.7 Application Authentication List Config

Users can configure authentication method lists on the following access applications: console, telnet, ssh and http.

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

Application Authentication Settings			
Select	Module	Login List	Enable List
<input type="checkbox"/>		default ▾	default ▾
<input type="checkbox"/>	console	default	default
<input type="checkbox"/>	telnet	default	default
<input type="checkbox"/>	ssh	default	default
<input type="checkbox"/>	http	default	default

Figure 12-8 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. This option defines the authentication method for users requiring the administrator privilege.

➤ **Entry Description:**

- Module:** Lists of the configurable applications on the switch.
- Login List:** Configure an application for the login utilizing a previously configured method list.
- Enable List:** Configure an application to promote the user level to admin-level users utilizing a previously configured method list.

12.6.8 802.1X Authentication Server Config

This page is used to configure the RADIUS server group used in 802.1X Authentication and Accounting.

Choose the menu **Network Security**→**AAA**→**Dot1x List** to load the following page.

Authentication Dot1x Method List		
Select	Method List	Pri1
<input type="checkbox"/>		radius
<input type="checkbox"/>	default	radius

Apply

Accounting Dot1x Method List		
Select	Method List	Pri1
<input type="checkbox"/>		radius
<input type="checkbox"/>	default	radius

Apply

Help

➤ **Configuration Procedure:**

- 1) Configure the 802.1X function both globally and on the supplicant-connected port. Please refer to [13.6 802.1X](#) for more details.
- 2) Go to **Network Security**→**AAA**→**Global Conifg** to enable AAA function.
- 3) Configure the 802.1X Aunthentication RADIUS server group in the Authentication Dot1x Method List Table.
- 4) Configure the 802.1X Accounting RADIUS server group in the Authentication Dot1x Method List Table.

12.6.9 Default Settings

Feature	Default Settings
Global AAA function	Disabled.
Enable password	No password is defined.
RADIUS server	<ul style="list-style-type: none"> • Auth port is 1812. • Acct port is 1813. • Retransmit is 2 times. • Timeout is 5 seconds. • NAS Identifier is the MAC address of the switch.
TACACA+ server	<ul style="list-style-type: none"> • Communication port is 1812. • Timeout is 5 seconds.
Server group	<p>Two server groups are preset: radius and tacacs.</p> <p>All RADIUS servers are added in the server group radius.</p> <p>All TACACS+ servers are added in the Server group tacacs.</p>
Authentication login method list	The list contains local, and the default login username and passwords are both admin.

Feature	Default Settings
Authentication enable method list	The list is empty, which means users can promote 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.

12.7 PPPoE

➤ PPPoE Tag Overview

The PPPoE ID-Insertion feature provides a way to extract a Vendor-specific tag as an identifier for the authentication, authorization, and accounting (AAA) access requests on an Ethernet interface. When enabled, the switch attaches a tag to the PPPoE discovery packets, which is called the PPPoE Vendor-Specific tag and it contains a unique line identifier. There are two formats of Vendor-specific tags: Circuit-ID format and Remote-ID format. The BRAS receives the tagged packet, decodes the tag, and uses the Circuit-ID/Remote-ID field of that tag as a NAS-Port-ID attribute in the RADIUS server for PPP authentication and AAA (authentication, authorization, and accounting) access requests. The switch will remove the Circuit-ID/Remote-ID tag from the received PPPoE Active Discovery Offer and Session-confirmation packets from the BRAS.

In this Chapter the switch will work as a DSLAM.

➤ PPPoE Tag Operation Process

The PPPoE ID insertion includes Circuit-ID tag and Remote-ID tag. The following process takes Circuit-ID insertion as an example:

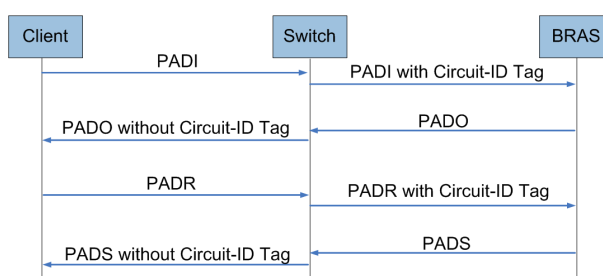


Figure 12-22 PPPoE Discovery Process

The PPPoE discovery process is illustrated below:

1. The client sends PADI (PPPoE Active Discovery Initiation) packets to the switch.
2. The switch intercepts PADI packets and inserts a unique Circuit-ID tag to them.
3. The switch forwards the PADI packets with Circuit-ID tag to the BRAS.
4. The BRAS responds with the PADO (PPPoE Active Discovery Offer) packets after receiving the PADI packets.

5. Upon receiving the PADO packets with the Circuit-ID tag, the switch will remove the tag and send the packets to the client. The switch will forward the PADO packets without the Circuit-ID tag directly.
6. The client sends PADR (PPPoE Active Discovery Request) packets according to the process.
7. The switch intercepts PADR packets and inserts a unique Circuit-ID tag to them.
8. The switch forwards the PADR packets with Circuit-ID tag to the BRAS.
9. The BRAS processes the received Circuit-ID tag in the PADR packets and extracts the Circuit-ID field to the RADIUS for accounting. And the BRAS allocates a PPP process session ID for this PPP session.
10. The BRAS responses with the PADS (PPPoE Active Discovery Session-confirmation) packets after receiving the PADR packets.
11. Upon receiving the PADS packets with the Circuit-ID tag, the switch will remove the tag and send the packets to the client. The switch will forward the PADS packets without the Circuit-ID tag directly.

On the **PPPoE ID Insertion** page, you can enable the PPPoE ID insertion function globally. Each port's PPPoE ID Insertion feature and type can be configured separately.

Choose the menu **Network Security**→**PPPoE**→**PPPoE ID Insertion** to load the following page.

Global Config

PPPoE ID Insertion: Enable Disable Apply

Port Config

Select	Port	Circuit-ID	Circuit-ID Type	UDF Value	Remote-ID	Remote-ID Value
<input type="checkbox"/>		Disable <input type="button" value="v"/>	IP <input type="button" value="v"/>	<input type="text"/>	Disable <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	1	Disable	IP	---	Disable	---
<input type="checkbox"/>	2	Disable	IP	---	Disable	---
<input type="checkbox"/>	3	Disable	IP	---	Disable	---
<input type="checkbox"/>	4	Disable	IP	---	Disable	---
<input type="checkbox"/>	5	Disable	IP	---	Disable	---
<input type="checkbox"/>	6	Disable	IP	---	Disable	---
<input type="checkbox"/>	7	Disable	IP	---	Disable	---
<input type="checkbox"/>	8	Disable	IP	---	Disable	---
<input type="checkbox"/>	9	Disable	IP	---	Disable	---
<input type="checkbox"/>	10	Disable	IP	---	Disable	---

Figure 12-23 PPPoE Circuit-ID Config

The following entries are displayed on this screen:

➤ **Global Config**

PPPoE ID Insertion: Enable or disable the PPPoE Circuit-ID Insertion function globally.

➤ **Port Config**

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

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

Port: Displays the port number.

Circuit-ID: Select Enable or disable the PPPoE Circuit-ID Insertion feature for the port.

Circuit-ID Type: Specify the Circuit-ID type for the port:

- **IP:** The IP address of the switch will be used to encode the Circuit-ID option. This is the default value.
- **MAC:** The MAC address of the switch will be used to encode the Circuit-ID option.
- **UDF:** The user specified string with the maximum length of 40 characters will be used to encode the Circuit-ID option.
- **UDF-ONLY:** The Circuit-ID option only contains user specified strings. The maximum length of the strings is 40 characters.

UDF Value: If the UDF is selected, specify a string with the maximum length of 40 characters to encode the Circuit-id option.

Remote-ID: Select Enable or disable the PPPoE Remote-ID Insertion feature for the port.

Remote-ID Value: A user specified string with the maximum length of 40.

[Return to CONTENTS](#)

Chapter 13 SNMP

➤ SNMP Overview

SNMP (Simple Network Management Protocol) has gained the most extensive application on the UDP/IP networks. SNMP provides a management frame to monitor and maintain the network devices. It is used for automatically managing the various network devices no matter the physical differences of the devices. Currently, the most network management systems are based on SNMP.

SNMP is simply designed and convenient for use with no need of complex fulfillment procedures and too much network resources. With SNMP function enabled, network administrators can easily monitor the network performance, detect the malfunctions and configure the network devices. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

➤ SNMP Management Frame

SNMP management frame includes three network elements: SNMP Management Station, SNMP Agent and MIB (Management Information Base).

SNMP Management Station: SNMP Management Station is the workstation for running the SNMP client program, providing a friendly management interface for the administrator to manage the most network devices conveniently.

SNMP Agent: Agent is the server software operated on network devices with the responsibility of receiving and processing the request packets from SNMP Management Station. In the meanwhile, Agent will inform the SNMP Management Station of the events whenever the device status changes or the device encounters any abnormalities such as device reboot.

MIB: MIB is the set of the managed objects. MIB defines a few attributes of the managed objects, including the names, the access rights, and the data types. Every SNMP Agent has its own MIB. The SNMP Management station can read/write the MIB objects 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.

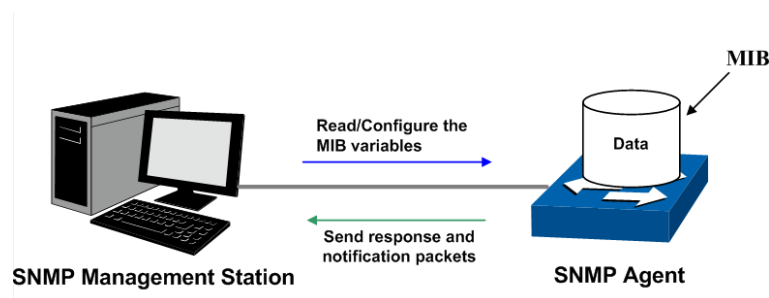


Figure 13-1 Relationship among SNMP Network Elements

➤ SNMP Versions

This switch supports SNMP v3, and is compatible with SNMP v1 and SNMP v2c. The SNMP versions adopted by SNMP Management Station and SNMP Agent should be the same. Otherwise, SNMP Management Station and SNMP Agent cannot communicate with each other normally. You can select the management mode with proper security level according to your actual application requirement.

SNMP v1: SNMP v1 adopts Community Name authentication. The community name is used to define the relation between SNMP Management Station and SNMP Agent. The SNMP packets failing to pass community name authentication are discarded. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password.

SNMP v2c: SNMP v2c also adopts community name authentication. It is compatible with SNMP v1 while enlarges the function of SNMP v1.

SNMP v3: 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}.

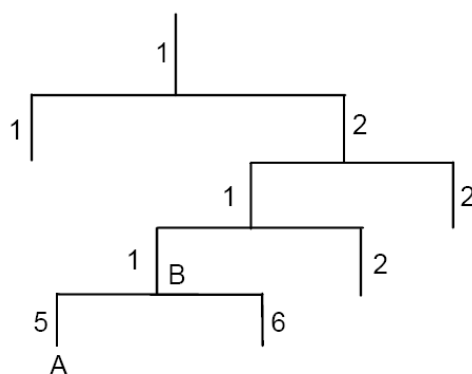


Figure 13-2 Architecture of the MIB tree

➤ SNMP Configuration Outline

1. Create View

The SNMP View is created for the SNMP Management Station to manage MIB objects. The managed object, uniquely identified by OID, can be set to under or out of the management of

SNMP Management Station by configuring its view type (included/excluded). The OID of managed object can be found on the SNMP client program running on the SNMP Management Station.

2. Create SNMP Group

After creating the SNMP View, it's required to create 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**.

13.1 SNMP Config

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

13.1.1 Global Config

To enable SNMP function, please configure the SNMP function globally on this page.

Choose the menu **SNMP**→**SNMP Config**→**Global Config** to load the following page.

The screenshot displays the 'Global Config' page for SNMP. It is organized into three distinct sections, each with a grey header bar:

- Global Config:** Contains a label 'SNMP:' followed by two radio buttons: 'Enable' (unselected) and 'Disable' (selected). An 'Apply' button is located to the right.
- Local Engine:** Contains a label 'Local Engine ID:' followed by a text input field containing the hexadecimal string '80002e5703000aeb13126a'. To the right of the input field is the text '(10-64 Hex)'. There are two buttons on the right: 'Default ID' and 'Apply'.
- Remote Engine:** Contains a label 'Remote Engine ID:' followed by an empty text input field. To the right of the input field is the text '(0 or 10-64 Hex)'. There are two buttons on the right: 'Apply' and 'Help'.

Figure 13-3 Global Config

The following entries are displayed on this screen:

➤ **Global Config**

SNMP: Enable or disable the SNMP function.

➤ **Local Engine**

Local Engine ID: Specify the switch's Engine ID for the remote clients. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the switch.

➤ **Remote Engine**

Remote Engine ID: Specify the Remote Engine ID for switch. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the remote device which receives informs from switch.



Note:

The amount of Engine ID characters must be even.

13.1.2 SNMP View

The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Choose the menu **SNMP**→**SNMP Config**→**SNMP View** to load the following page.

View Config

View Name: (16 characters maximum)

MIB Object ID: (61 characters maximum)

View Type: Include Exclude

View Table			
Select	View Name	View Type	MIB Object ID
<input type="checkbox"/>	viewDefault	Include	1
<input type="checkbox"/>	viewDefault	Exclude	1.3.6.1.6.3.15
<input type="checkbox"/>	viewDefault	Exclude	1.3.6.1.6.3.16
<input type="checkbox"/>	viewDefault	Exclude	1.3.6.1.6.3.18

Figure 13-4 SNMP View

The following entries are displayed on this screen:

➤ **View Config**

View Name: Give a name to the View for identification. Each View can include several entries with the same name.

MIB Object ID: Enter the Object Identifier (OID) for the entry of View.

View Type: Select the type for the view entry.

- **Include:** The view entry can be managed by the SNMP management station.
- **Exclude:** The view entry cannot be managed by the SNMP management station.

➤ **View Table**

Select: Select the desired entry to delete the corresponding view. All the entries of a View will be deleted together.

View Name: Displays the name of the View entry.

View Type: Displays the type of the View entry.

MIB Object ID: Displays the OID of the View entry.

13.1.3 SNMP Group

On this page, you can configure SNMP Group to control the network access by providing the users in various groups with different management rights via the Read View, Write View and Notify View.

Choose the menu **SNMP**→**SNMP Config**→**SNMP Group** to load the following page.

Group Config

Group Name: (16 characters maximum)

Security Model: v1

Security Level: noAuthNoPriv

Read View: viewDefault

Write View: None

Notify View: None

Create Clear

Group Table

Select	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Operation
--------	------------	----------------	----------------	-----------	------------	-------------	-----------

All Delete Help

Figure 13-5 SNMP Group

The following entries are displayed on this screen:

➤ **Group Config**

Group Name: Enter the SNMP Group name. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group.

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 viewDefault.

13.1.4 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.

User Config

User Name: (16 characters maximum)

User Type: Group Name:

Security Model: Security Level:

Auth Mode: Auth Password: (16 characters maximum)

Privacy Mode: Privacy Password: (16 characters maximum)

User Table

Select	User Name	User Type	Group Name	Security Model	Security Level	Auth Mode	Privacy Mode	Operation
--------	-----------	-----------	------------	----------------	----------------	-----------	--------------	-----------

Figure 13-6 SNMP User

The following entries are displayed on this screen:

➤ **User Config**

- User Name:** Enter the User Name here.
- User Type:** Select the type for the User.
 - **Local User:** Indicates that the user is connected to a local SNMP engine.
 - **Remote User:** Indicates that the user is connected to a remote SNMP engine.
- Group Name:** Select the Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.
- Security Model:** Select the Security Model for the User.
- Security Level:** Select the Security Level for the SNMP v3 User.

Auth Mode: Select the Authentication Mode for the SNMP v3 User.

- **None:** No authentication method is used.
- **MD5:** The port authentication is performed via HMAC-MD5 algorithm.
- **SHA:** The port authentication is performed via SHA (Secure Hash Algorithm). This authentication mode has a higher security than MD5 mode.

Auth Password: Enter the password for authentication.

Privacy Mode: Select the Privacy Mode for the SNMP v3 User.

- **None:** No privacy method is used.
- **DES:** DES encryption method is used.

Privacy Password: Enter the Privacy Password.

➤ **User Table**

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

User Name: Displays the name of the User.

User Type: Displays the User Type.

Group Name: Displays the Group Name of the User.

Security Model: Displays the Security Model of the User.

Security Level: Displays the Security Level of the User.

Auth Mode: Displays the Authentication Mode of the User.

Privacy Mode: Displays the Privacy Mode of the User.

Operation: Click the **Edit** button to modify the Group of the User and click the **Modify** button to apply.



Note:

The SNMP User and its Group should have the same Security Model and Security Level.

13.1.5 SNMP Community

SNMP v1 and SNMP v2c adopt community name authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password. If SNMP v1 or SNMP v2c is employed, you can directly configure the SNMP Community on this page without configuring SNMP Group and User.

Choose the menu **SNMP**→**SNMP Config**→**SNMP Community** to load the following page.

Community Config

Community Name: (16 characters maximum)

Access:

MIB View:

Community Table

Select	Community Name	Access	MIB View	Operation
<input type="button" value="All"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

Figure 13-7 SNMP Community

The following entries are displayed on this screen:

➤ **Community Config**

Community Name: Enter the Community Name here.

Access: Defines the access rights of the community.

- **read-only:** Management right of the Community is restricted to read-only, and changes cannot be made to the corresponding View.
- **read-write:** Management right of the Community is read-write and changes can be made to the corresponding View.

MIB View: Select the MIB View for the community to access.

➤ **Community Table**

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

Community Name: Displays the Community Name here.

Access: Displays the right of the Community to access the View.

MIB View: Displays the Views which the Community can access.

Operation: Click the **Edit** button to modify the MIB View and the Access right of the Community, and then click the **Modify** button to apply.



Note:

The default MIB View of SNMP Community is viewDefault.

Configuration Procedure:

- If SNMPv3 is employed, please take the following steps:

Step	Operation	Description
1	Enable SNMP function globally.	Required. On the SNMP→SNMP Config→Global Config page, enable SNMP function globally.
2	Create SNMP View.	Required. On the SNMP→SNMP Config→SNMP View page, create SNMP View of the management agent. The default View Name is viewDefault and the default OID is 1.
3	Create SNMP Group.	Required. On the SNMP→SNMP Config→SNMP Group page, create SNMP Group for SNMPv3 and specify SNMP Views with various access levels for SNMP Group.
4	Create SNMP User.	Required. On the SNMP→SNMP Config→SNMP User page, create SNMP User in the Group and configure the auth/privacy mode and auth/privacy password for the User.

- If SNMPv1 or SNMPv2c is employed, please take the following steps:

Step	Operation	Description			
1	Enable SNMP function globally.	Required. On the SNMP→SNMP Config→Global Config page, enable SNMP function globally.			
2	Create SNMP View.	Required. On the SNMP→SNMP Config→SNMP View page, create SNMP View of the management agent. The default View Name is viewDefault and the default OID is 1.			
3	<table border="1"> <tr> <td rowspan="2">Configure access level for the User.</td> <td>Create SNMP Community directly.</td> </tr> <tr> <td>Create SNMP Group and SNMP User.</td> </tr> </table>	Configure access level for the User.	Create SNMP Community directly.	Create SNMP Group and SNMP User.	<p>Required alternatively.</p> <ul style="list-style-type: none"> • 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.
Configure access level for the User.	Create SNMP Community directly.				
	Create SNMP Group and SNMP User.				

13.2 Notification

With the Notification function enabled, the switch can initiatively report to the management station about the important events that occur on the Views (e.g., the managed device is rebooted), which allows the management station to monitor and process the events in time.

The notification information includes the following two types:

Trap: Trap is the information that the managed device initiatively sends to the Network management station without request.

Inform: Inform packet is sent to inform the management station and ask for the reply. The switch will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times. The Inform type, employed on SNMPv2c and SNMPv3, has a higher security than the Trap type.

13.2.1 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.

Select	IP Address	IP Mode	UDP Port	User	Security Model	Security Level	Type	Timeout	Retry	Operation

Figure 13-8 Notification Config

The following entries are displayed on this screen:

➤ Create Notification

- IP Mode:** Select the IP mode.
- IP Address:** Enter the IP Address of the management Host.
- UDP Port:** Enter the number of the UDP port used to send notifications. The UDP port functions with the IP address for the notification sending. The default is 162.
- User:** Enter the User name of the management station.
- Security Model:** Select the Security Model of the management station.

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

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

Type: Select the type for the notifications.

- **Trap:** Indicates traps are sent.
- **Inform:** Indicates informs are sent. The Inform type has a higher security than the Trap type.

Retry: Specify the amount of times the switch resends an inform request. The switch will resend the inform request if it doesn't get the response from the management station during the **Timeout** interval, and it will terminate resending the inform request if the resending times reach the specified **Retry** times.

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

➤ **Notification Table**

Select: Select the desired entry to delete the corresponding management station.

IP Mode: Select the IP mode.

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.

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

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

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

13.3 RMON

RMON (Remote Monitoring) 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 Control**, **Event Config** and **Alarm Config** pages.

13.3.1 History Control

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

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

History Control Table					
Select	Index	Port	Interval (sec)	Owner	Status
<input type="checkbox"/>		Port 1 ▾	<input type="text"/>	<input type="text"/>	Disable ▾
<input type="checkbox"/>	1	Port 1	1800	monitor	Disable
<input type="checkbox"/>	2	Port 1	1800	monitor	Disable
<input type="checkbox"/>	3	Port 1	1800	monitor	Disable
<input type="checkbox"/>	4	Port 1	1800	monitor	Disable
<input type="checkbox"/>	5	Port 1	1800	monitor	Disable
<input type="checkbox"/>	6	Port 1	1800	monitor	Disable
<input type="checkbox"/>	7	Port 1	1800	monitor	Disable
<input type="checkbox"/>	8	Port 1	1800	monitor	Disable
<input type="checkbox"/>	9	Port 1	1800	monitor	Disable
<input type="checkbox"/>	10	Port 1	1800	monitor	Disable
<input type="checkbox"/>	11	Port 1	1800	monitor	Disable
<input type="checkbox"/>	12	Port 1	1800	monitor	Disable

Figure 13-9 History Control

The following entries are displayed on this screen:

➤ **History Control Table**

- Select:** Select the desired entry for configuration.
- Index:** Displays the index number of the entry.
- Port:** Specify the port from which the history samples were taken.
- Interval:** Specify the interval to take samplings from the port.
- Owner:** Enter the name of the device or user that defined the entry.
- Status:** Enable or disable the corresponding sampling entry.

13.3.2 Event Config

On this page, you can configure the RMON events.

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

Select	Index	User	Description	Type	Owner	Status
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>	Disable <input type="button" value="v"/>
<input type="checkbox"/>	1	public		None	monitor	Disable
<input type="checkbox"/>	2	public		None	monitor	Disable
<input type="checkbox"/>	3	public		None	monitor	Disable
<input type="checkbox"/>	4	public		None	monitor	Disable
<input type="checkbox"/>	5	public		None	monitor	Disable
<input type="checkbox"/>	6	public		None	monitor	Disable
<input type="checkbox"/>	7	public		None	monitor	Disable
<input type="checkbox"/>	8	public		None	monitor	Disable
<input type="checkbox"/>	9	public		None	monitor	Disable
<input type="checkbox"/>	10	public		None	monitor	Disable
<input type="checkbox"/>	11	public		None	monitor	Disable
<input type="checkbox"/>	12	public		None	monitor	Disable

Figure 13-10 Event Config

The following entries are displayed on this screen:

➤ Event Table

- Select:** Select the desired entry for configuration.
- Index:** Displays the index number of the entry.
- User:** Enter the name of the User or the community to which the event belongs.
- Description:** Give a description to the event for identification.
- Type:** Select the event type, which determines the act way of the network device in response to an event.
- **None:** No processing.
 - **Log:** Logging the event.
 - **Notify:** Sending trap messages to the management station.
 - **Log&Notify:** Logging the event and sending trap messages to the management station.
- Owner:** Enter the name of the device or user that defined the entry.
- Status:** Enable or disable the corresponding event entry.

13.3.3 Alarm Config

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

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

Select	Index	Variable	Port	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Alarm Type	Interval (sec)	Owner	Status
<input type="checkbox"/>		DropEvents		Absolute					All			Disable
<input type="checkbox"/>	1	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	2	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	3	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	4	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	5	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	6	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	7	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	8	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	9	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	10	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	11	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable
<input type="checkbox"/>	12	DropEvents	Port 1	Absolute	100	1	100	1	All	1800	monitor	Disable

Figure 13-11 Alarm Config

The following entries are displayed on this screen:

➤ **Alarm Table**

- Select:** Select the desired entry for configuration.
- Index:** Displays the index number of the entry.
- Variable:** Select the alarm variables from the pull-down list.
- Port:** Select the port on which the Alarm entry acts.
- Sample Type:** Specify the sampling method for the selected variable and comparing the value against the thresholds.
 - **Absolute:** Compares the values directly with the thresholds at the end of the sampling interval.
 - **Delta:** Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
- Rising Threshold:** Enter the rising counter value that triggers the Rising Threshold alarm.
- Rising Event:** Select the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold.
- Falling Threshold:** Enter the falling counter value that triggers the Falling Threshold alarm.
- Falling Event:** Select the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold.

Alarm Type:

Specify the type of the alarm.

- **All:** The alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold.
- **Rising:** When the sampled value exceeds the Rising Threshold, an alarm event is triggered.
- **Falling:** When the sampled value is under the Falling Threshold, an alarm event is triggered.

Interval:

Enter the alarm interval time in seconds.

Owner:

Enter the name of the device or user that defined the entry.

Status:

Enable or disable the corresponding alarm entry.

**Note:**

When alarm variables exceed the Threshold on the same direction continuously for several times, an alarm event will only be generated on the first time, that is, the Rising Alarm and Falling Alarm are triggered alternately for that the alarm following to Rising Alarm is certainly a Falling Alarm and vice versa.

[Return to CONTENTS](#)

Chapter 14 LLDP

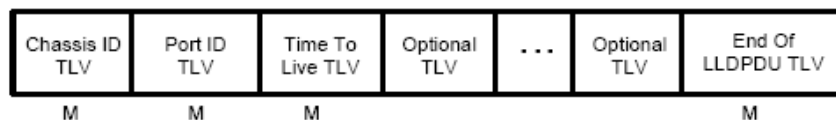
LLDP (Link Layer Discovery Protocol) is a Layer 2 protocol that is used for network devices to advertise their own device information periodically to neighbors on the same IEEE 802 local area network. The advertised information, including details such as device identification, capabilities and configuration settings, is represented in TLV (Type/Length/Value) format according to the IEEE 802.1ab standard, and these TLVs are encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit). The LLDPDU distributed via LLDP is stored by its recipients in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

An IETF Standard MIB, as well as a number of vendor specific MIBs, have been created to describe a network's physical topology and associated systems within that topology. However, there is no standard protocol for populating these MIBs or communicating this information among stations on the IEEE 802 LAN. LLDP protocol specifies a set. The device running LLDP can automatically discover and learn about the neighbors, allowing for interoperability between the network devices of different vendors. This protocol allows two systems running different network layer protocols to learn about each other.

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.

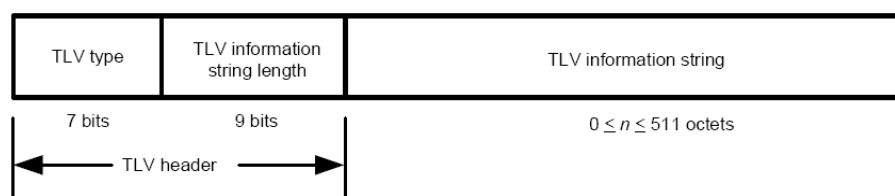
3) LLDPDU receipt mechanism

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 MAC address of the specific port that transmitted the LLDP frame.	Mandatory
3	Time To Live	Indicates the number of seconds that the neighbor device is to regard the local information to be valid.	Mandatory
4	Port Description	Identifies the description string of the port.	Optional
5	System Name	Identifies the system name.	Optional
6	System Description	Identifies the system description.	Optional
7	System Capabilities	Identifies the main functions of the system and the functions enabled.	Optional
8	Management Address	Identifies the management IP address, the corresponding interface number and OID (Object Identifier). The management IP address is specified by the user.	Optional
127	Organizationally Specific	Allows different organizations, such as IEEE 802.1, IEEE 802.3, IETF, as well as individual software and equipment vendors, to define TLVs that advertise information to remote device.	Optional

Optional TLVs are grouped into two categories including basic management TLV and Organizationally-specific TLV.

1) Basic Management TLV

A set of TLVs considered to be basic to the management of the network stations are required for all LLDP implementations.

2) Organizationally Specific TLV

Different organizations have defined various TLVs. For instance, Port VLAN ID TLV, Port and Protocol VLAN ID TLV, VLAN Name TLV And Protocol Identity TLV are defined by IEEE 802.1, while MAC/PHY Configuration/Status TLV, Power Via MDI TLV, Link Aggregation TLV and Maximum Frame TLV are defined by IEEE 802.3.

**Note:**

For detailed introduction of TLV, please refer to IEEE 802.1AB standard.

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

TLV	Description
Port Description TLV	The Port Description TLV allows network management to advertise the IEEE 802 LAN station's port description.
System Capabilities TLV	The System Capabilities TLV identifies the primary functions of the system and whether or not these primary functions are enabled.
System Description TLV	The System Description TLV allows network management to advertise the system's description, which should include the full name and version identification of the system's hardware type, software operating system, and networking software.
System Name TLV	The System Name TLV allows network management to advertise the system's assigned name, which should be the system's fully qualified domain name.
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher entities to assist discovery by network management.
Port VLAN ID TLV	The Port VLAN ID TLV allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
Port And Protocol VLAN ID TLV	The Port And Protocol VLAN ID TLV allows a bridge port to advertise a port and protocol VLAN ID.
VLAN Name TLV	The VLAN Name TLV allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation.
MAC/PHY Configuration/ Status TLV	The MAC/PHY Configuration/Status TLV identifies: a)The duplex and bit-rate capability of the sending IEEE 802.3 LAN node that is connected to the physical medium; b)The current duplex and bit-rate settings of the sending IEEE 802.3 LAN node; c)Whether these settings are the result of auto-negotiation during link initiation or of manual set override action.
Max Frame Size TLV	The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

TLV	Description
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

The LLDP module is mainly for LLDP function configuration of the switch, including three submenus: **Basic Config**, **Device Info** and **Device Statistics**.

14.1 Basic Config

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

14.1.1 Global Config

On this page you can configure the LLDP parameters of the device globally.

Choose the menu **LLDP**→**Basic Config**→**Global Config** to load the following page.

Figure 14-1 Global Configuration

The following entries are displayed on this screen:

➤ **Global Config**

LLDP: Enable or disable LLDP function globally.

LLDP Forward Message: Enable or disable the switch to forward LLDP messages when LLDP function is disabled.

➤ **Parameters Config**

Transmit Interval: Enter the interval for the local device to transmit LLDPDU to its neighbors. The default value is 30 seconds.

Hold Multiplier: Enter a multiplier on the Transmit Interval. It determines the actual TTL (Time To Live) value used in an LLDPDU. $TTL = \text{Hold Multiplier} * \text{Transmit Interval}$. The default value is 4.

- Transmit Delay:** Enter a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. The default value is 2 seconds.
- Reinit Delay:** This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The default value is 3 seconds.
- Notification Interval:** Specify the interval of Trap message which will be sent from local device to network management system. The default value is 5 seconds.
- Fast Start Count:** When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The default value is 3.

14.1.2 Port Config

On this page you can configure all ports' LLDP parameters.

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

LLDP Port Config

Port

Select	Port	Admin Status	Notification Mode	Included TLVs
<input type="checkbox"/>		Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>	
<input type="checkbox"/>	1	Tx&Rx	Disable	Detail
<input type="checkbox"/>	2	Tx&Rx	Disable	Detail
<input type="checkbox"/>	3	Tx&Rx	Disable	Detail
<input type="checkbox"/>	4	Tx&Rx	Disable	Detail
<input type="checkbox"/>	5	Tx&Rx	Disable	Detail
<input type="checkbox"/>	6	Tx&Rx	Disable	Detail
<input type="checkbox"/>	7	Tx&Rx	Disable	Detail
<input type="checkbox"/>	8	Tx&Rx	Disable	Detail
<input type="checkbox"/>	9	Tx&Rx	Disable	Detail
<input type="checkbox"/>	10	Tx&Rx	Disable	Detail

Figure 14-2 Port Configuration

The following entries are displayed on this screen:

➤ **LLDP Port Config**

Port Select: Select the desired port to configure.

- Admin Status:** Select the port's LLDP operating mode:
- **Tx&Rx:** Send and receive LLDP frames.
 - **Rx_Only:** Only receive LLDP frames.
 - **Tx_Only:** Only send LLDP frames.
 - **Disable:** Neither send nor receive LLDP frames.
- Notification Mode:** Enable or disable the ports' SNMP notification. If enabled, the local device will notify the trap event to SNMP server.
- Included TLVs:** Select TLVs to be included in outgoing LLDPDU.
- Details:** Click Details to display the included TLVs.

14.2 Device Info

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

14.2.1 Local Info

On this page you can see all ports' configuration and system information.

Choose the menu **LLDP**→**Device Info**→**Local Info** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Rate: sec(3-300)

Local Info

	Port	1	Select
Local Interface:	1		
Chassis ID Subtype:	Reserved		
Chassis ID:			
Port ID Subtype:	Reserved		
Port ID:			
TTL:	0		
Port Description:			
System Name:			
System Description:			
System Capabilities Supported:			
System Capabilities Enabled:			
Management Address:			

Refresh
Help

Figure 14-3 Local Information

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

➤ **Local Info**

Enter the desired port number and click **Select** to display the information of the corresponding port.

14.2.2 Neighbor Info

On this page you can get the information of the neighbors.

Choose the menu **LLDP→Device Info→Neighbor Info** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable

Refresh Rate: sec(3-300)

Neighbor Info

Port

Local Port	System Name	Chassis ID	System Description	Neighbor Port	Information
------------	-------------	------------	--------------------	---------------	-------------

Figure 14-4 Neighbor Information

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

➤ **Neighbor Info**

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

Local Port: Displays the local port number connecting to the neighbor device.

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

Chassis ID: Displays the Chassis ID of the neighbor device.

System Description: Displays the system description of the neighbor device.

Neighbor Port: Displays the he port number of the neighbor linking to local port.

Information: Click Information to display the detailed information of the neighbor device.

14.3 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.

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Rate: sec(3-300)

Global Statistics

Last Update	Total Inserts	Total Deletes	Total Drops	Total Ageouts
00:00:00:00	0	0	0	0

Neighbors Statistics

Port Select

Port	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Refresh Clear Help

Figure 14-5 Device Statistics

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

➤ **Global Statistics**

Last Update: Displays latest update time of the statistics.

Total Inserts:	Displays the number of neighbors inserted till last update time.
Total Deletes:	Displays the number of neighbors deleted by local device.
Total Drops:	Displays the number of neighbors dropped by local device.
Total Ageouts:	Displays the number of overtime neighbors in local device.
➤ Neighbor Statistics	
Port Select	Click the Select button to quick-select the corresponding port based on the port number you entered.
Port:	Displays local device's port number.
Transmit Total:	Displays the number of LLDPDUs sent by this port.
Receive Total:	Displays the number of LLDPDUs received by this port.
Discards:	Displays the number of LLDPDUs discarded by this port.
Errors:	Displays the number of error LLDPDUs received by this port.
Ageouts:	Displays the number of overtime neighbors linking to this port.
TLV Discards:	Displays the number of TLVs dropped by this port.
TLV Unknowns:	Displays the number of unknown TLVs received by this port.

14.4 LLDP-MED

LLDP-MED is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power via MDI, inventory management, and device location details.

➤ Elements

LLDP-MED Device: Refers to any device which implements this Standard.

LLDP-MED Device Type: LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices.

Network Connectivity Device: Refers to an LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. Bridge is a Network Connectivity Device.

Endpoint Device: Refers to an LLDP-MED Device at the network edge, providing some aspects of IP communications service, based on IEEE 802 LAN technology. Endpoint Devices may be a member of any of the Endpoint Device Classes. Endpoint Devices are composed of three defined Classes: Class I, Class II and Class III.

Generic Endpoint Device (Class I): The most basic class of Endpoint Device.

Media Endpoint Device (Class II): The class of Endpoint Device that supports media stream capabilities.

Communication Device Endpoint (Class III): The class of Endpoint Device that directly supports end users of the IP communication system.

Network Policy TLV	The Network Policy TLV allows both Network Connectivity Devices and Endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes that apply for a set of specific applications on that port.
Location Identification TLV	The Location Identification TLV provides for advertisement of location identifier information to Communication Endpoint Devices, based on configuration of the Network Connectivity Device it's connected to. You can set the Location Identification content in Location Identification Parameters. If Location Identification TLV is included and Location Identification Parameters isn't set, a default value is used in Location Identification TLV.
Extended Power-Via-MDI TLV	The Extended Power-Via-MDI TLV is intended to enable advanced power management between LLDP-MED Endpoint and Network Connectivity Devices, and it allows advertisement of fine grained power requirement details, Endpoint power priority, as well as both Endpoint and Network Connectivity Device power status.
Inventory TLV	The Inventory TLV set contains seven basic Inventory management TLVs, that is, Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV and Asset ID TLV. If support for any of the TLVs in the Inventory Management set is implemented, then support for all Inventory Management TLVs shall be implemented.

LLDP-MED is configured on the **Global Config**, **Port Config**, **Local Info** and **Neighbor Info** pages.

14.4.1 Global Config

On this page you can configure the LLDP-MED parameters of the device globally.

Choose the menu **LLDP**→**LLDP-MED**→**Global Config** to load the following page.

LLDP-MED Parameters Config

Fast Start Count: (1-10)

Device Class:

Figure 14-6 LLDP-MED Global Configuration

The following entries are displayed on this screen:

➤ **LLDP-MED Parameters Config**

Fast Start Count: When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted (the number of frames equals this parameter). The default value is 4.

Device Class: LLDP-MED devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices. In turn, Endpoint Devices are composed of three defined Classes: Class I, Class II and Class III. Bridge is a Network Connectivity Device.

14.4.2 Port Config

On this page you can configure all ports' LLDP-MED parameters.

Choose the menu **LLDP→LLDP-MED→Port Config** to load the following page.

Select	Port	LLDP-MED Status	Included TLVs
<input type="checkbox"/>		Disable	
<input type="checkbox"/>	1	Disable	Detail
<input type="checkbox"/>	2	Disable	Detail
<input type="checkbox"/>	3	Disable	Detail
<input type="checkbox"/>	4	Disable	Detail
<input type="checkbox"/>	5	Disable	Detail
<input type="checkbox"/>	6	Disable	Detail
<input type="checkbox"/>	7	Disable	Detail
<input type="checkbox"/>	8	Disable	Detail
<input type="checkbox"/>	9	Disable	Detail
<input type="checkbox"/>	10	Disable	Detail

Figure 14-7 LLDP-MED Port Configuration

The following entries are displayed on this screen:

➤ **LLDP-MED Port Config**

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.

Detail:

Click the **Detail** button to display the included TLVs and select the desired TLVs.

Included TLVs		
<input checked="" type="checkbox"/> Network Policy	<input checked="" type="checkbox"/> Location Identification	<input checked="" type="checkbox"/> Extended Power-Via-MDI
<input checked="" type="checkbox"/> Inventory	<input checked="" type="checkbox"/> All	

Location Identification Parameters	
<input type="checkbox"/> Emergency Number:	<input type="text"/> Chars.(10-25)
<input checked="" type="checkbox"/> Civic Address	
What:	<input type="text" value="Switch"/>
Country Code:	<input type="text" value="CN China(Default)"/>
Language:	<input type="text"/>
Province/State:	<input type="text"/>
County/Parish/District:	<input type="text"/>
City/Township:	<input type="text"/>
Street:	<input type="text"/>
House Number:	<input type="text"/>
Name:	<input type="text"/>
Postal/Zip Code:	<input type="text"/>
Room Number:	<input type="text"/>
Post Office Box:	<input type="text"/>
Additional Information:	<input type="text"/>

Figure 14-8 Configure TLVs of LLDP-MED Port

➤ **Included TLVs**

Select TLVs to be included in outgoing LLDPDU.

➤ **Location Identification Parameters**

Configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Emergency Number:

Emergency number is Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP.

Civic Address:

The Civic address is defined to reuse the relevant sub-fields of the DHCP option for Civic Address based Location Configuration Information as specified by IETF.

- What: This element describes which location the DHCP entry refers to. Currently, three options are defined: the location of the DHCP server (0: DHCP server), the location of the

network element believed to be closest to the client (1: Switch) or the location of the client (2: LLDP-MED Endpoint). Option (2) should be used, but may not be known. Options (0) and (1) should not be used unless it is known that the DHCP client is in close physical proximity to the server or network element.

- Country Code: The two-letters ISO 3166 country code in capital ASCII letters, e.g., CN or US.
- Language, Province/State, etc.: a part of civic address.

14.4.3 Local Info

On this page you can see all ports' LLDP-MED configuration.

Choose the menu **LLDP**→**LLDP-MED**→**Local Info** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Rate: sec(3-300)

LLDP-MED Local Info

Port Select

Local Interface:	1
Device Type:	Network Connectivity
Application Type:	Reserved
Unknown Policy Flag:	Yes
VLAN tagged:	No
Media Policy VLAN ID:	0
Media Policy Layer 2 Priority:	0
Media Policy DSCP:	0
Power Type:	0
Power Source:	0

Refresh
Help

Figure 14-9 LLDP-MED Local Information

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

➤ **Local-MED Local Info**

Select the desired port to display the information of the corresponding port.

Local Interface: Enable or 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.

14.4.4 Neighbor Info

On this page you can get the LLDP-MED information of the neighbors.

Choose the menu **LLDP**→**LLDP-MED**→**Neighbor Info** to load the following page.

Auto Refresh

Auto Refresh: Enable Disable Apply

Refresh Rate: sec(3-300)

LLDP-MED Neighbor Info

Port Select

Local Port	Device Type	Application Type	Location Data Format	Power Type	Information

Refresh
Help

Figure 14-10 LLDP-MED Neighbor Information

The following entries are displayed on this screen:

➤ **Auto Refresh**

Auto Refresh: Enable or disable the auto refresh function.

Refresh Rate: Specify the auto refresh rate.

➤ **LLDP-MED Neighbor Info**

Select the desired port to display LLDP-MED information of neighbors of the corresponding port:

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 15 Maintenance

Maintenance module, assembling the commonly used system tools to manage the switch, provides the convenient method to locate and solve the network problem.

1. System Monitor: Monitor the utilization status of the memory and the CPU of switch.
2. Log: View the configuration parameters of the switch and find out the errors via the Logs.
3. Cable Test: Test the connection status of the cable to locate and diagnose the trouble spot of the network.
4. Network Diagnostics: Test whether the destination device is reachable and detect the route hops from the switch to the destination device.
5. DLDP: Monitor the physical configuration of the cables and detect whether a unidirectional link exists.

15.1 System Monitor

System Monitor functions to display the utilization status of the memory and the CPU of switch via the data graph. The CPU utilization rate and the memory utilization rate should fluctuate stably around a specific value. If the CPU utilization rate or the memory utilization rate increases markedly, please detect whether the network is being attacked.

The **System Monitor** function is implemented on the **CPU Monitor** and **Memory Monitor** pages.

15.1.1 CPU Monitor

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

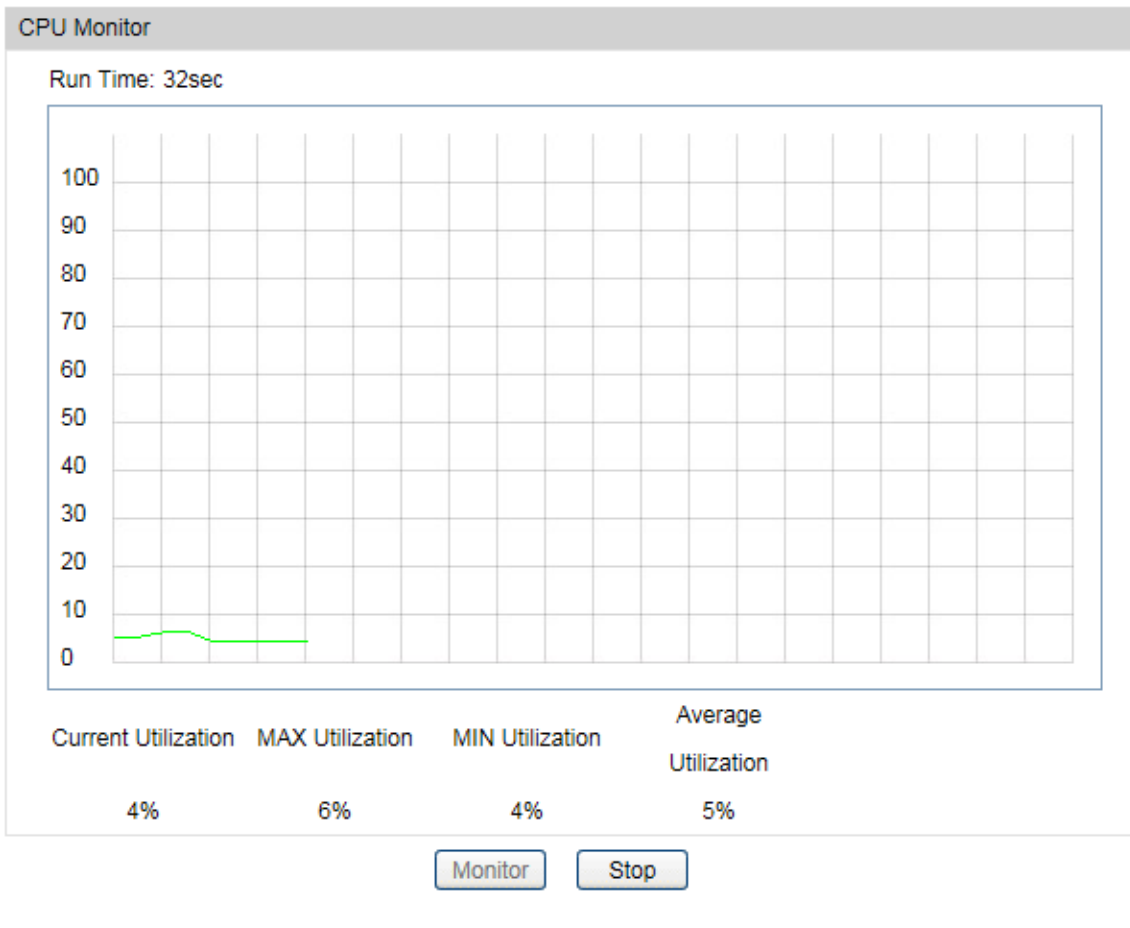


Figure 15-1 CPU Monitor

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

15.1.2 Memory Monitor

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

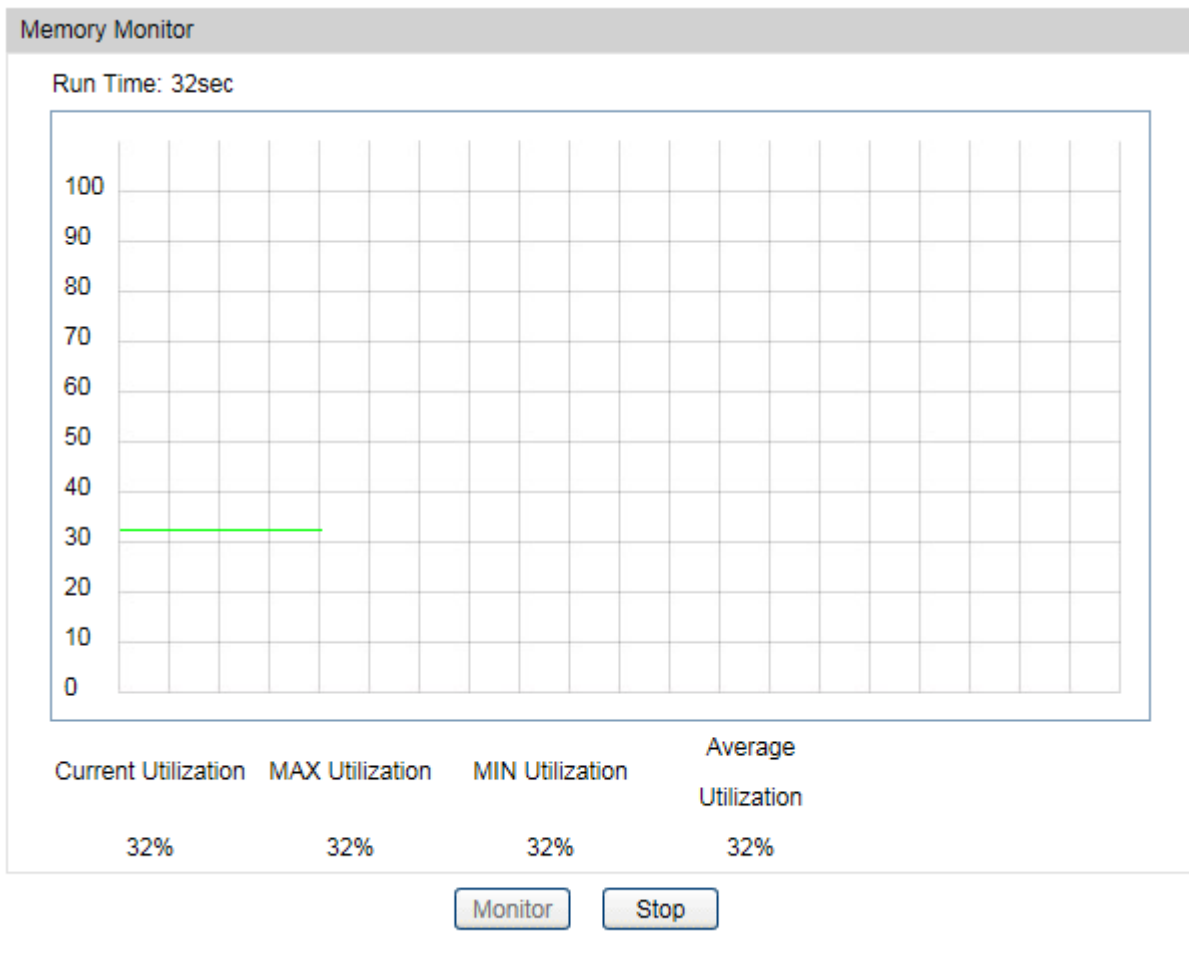


Figure 15-2 Memory Monitor

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

15.2 Log

The Log system of switch can record, classify and manage the system information effectively, providing powerful support for network administrator to monitor network operation and diagnose malfunction.

The Logs of switch are classified into the following eight levels.

Severity	Level	Description
emergencies	0	The system is unusable.
alerts	1	Action must be taken immediately.
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warnings conditions
notifications	5	Normal but significant conditions

Severity	Level	Description
informational	6	Informational messages
debugging	7	Debug-level messages

Table 15-1 Log Level

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

15.2.1 Log Table

The switch supports logs output to two directions, namely, log buffer and log file. The information in log buffer will be lost after the switch is rebooted or powered off whereas the information in log file will be kept effective even the switch is rebooted or powered off. Log Table displays the system log information in log buffer.

Choose the menu **Maintenance**→**Log**→**Log Table** to load the following page.

Log Info				
Index	Time	Module	Severity	Content
		All Module	All Level	
1	2006-01-05 08:18:54	CLI/TELNET/SSH	level_6	execute command 'conf ' by admin on vty0 (192.168.0.200).
2	2006-01-05 08:18:53	CLI/TELNET/SSH	level_6	execute command 'en ' by admin on vty0 (192.168.0.200).
3	2006-01-05 08:18:50	User	level_3	Login the CLI by admin on vty0 (192.168.0.200).
4	2006-01-05 07:51:37	User	level_3	Login the web by admin on web (192.168.0.200).
5	2006-01-05 07:09:14	User	level_6	Set session timeout: 30 by admin on web (192.168.0.200).
6	2006-01-05 07:06:53	User	level_3	Login the web by admin on web (192.168.0.200).
7	2006-01-05 06:49:45	User	level_3	Login the web by admin on web (192.168.0.200).
8	2006-01-02 14:31:45	User	level_3	Login the web by admin on web (192.168.0.200).
9	2006-01-01 18:26:14	User	level_3	Login the web by admin on web (192.168.0.200).
10	2006-01-01 12:32:52	User	level_3	Login the web by admin on web (192.168.0.200).
11	2006-01-01 12:20:18	User	level_3	Login the web by admin on web (192.168.0.200).
12	2006-01-01 08:25:03	User	level_3	Login the web by admin on web (192.168.0.200).
13	2006-01-01 08:03:18	System	level_6	Save config file ok by admin on web (192.168.0.200).
14	2006-01-01 08:03:08	VLAN	level_6	Set VLAN 1 as Management VLAN by admin on web (192.168.0.200).
15	2006-01-01 08:03:08	System	level_6	The IP Address of switch changed to 192.168.0.25 by admin on web (192.168.0.200).
16	2006-01-01 08:03:08	VLAN	level_6	Set VLAN 1 as Management VLAN by admin on web (192.168.0.200).

Figure 15-3 Log Table

The following entries are displayed on this screen:

> Log Info

Index: Displays the index of the log information.

Time: Displays the time when the log event occurs. The log can get the correct time after you configure on the **System**→**System Info**→**System Time** Web management page.

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

Severity: Displays the severity level of the log information. You can select a severity level to display the log information whose severity level value is the same or smaller.

Content: Displays the content of the log information.



Note:

1. The logs are classified into eight levels based on severity. The higher the information severity is, the lower the corresponding level is.
2. This page displays logs in the log buffer, and at most 511 logs are displayed.

15.2.2 Local Log

Local Log is the log information saved in switch. By default, all system logs are saved in log buffer and the logs with severities from level_0 to level_2 are saved in log file meanwhile. On this page, you can set the output channel for logs.

Choose the menu **Maintenance**→**Log**→**Local Log** to load the following page.

Local Log Config			
Select	Channel	Severity	Status
<input type="checkbox"/>		<input type="text" value=""/> ▼	<input type="text" value=""/> ▼
<input type="checkbox"/>	Log Buffer	level_6	Enable
<input type="checkbox"/>	Log File	level_2	Disable

Figure 15-4 Local Log

The following entries are displayed on this screen:

➤ **Local Log Config**

Select: Select the desired entry to configure the corresponding local log.

Log Buffer: Indicates the RAM for saving system log. The information in the log buffer is displayed on the Log Table page. It will be lost when the switch is restarted.

Log File: Indicates the flash sector for saving system log. The information in the log file will not be lost after the switch is restarted and can be exported on the Backup Log page.

Severity: Specify the severity level of the log information output to each channel. Only the log with the same or smaller severity level value will be output.

Status: Enable or disable the channel.

15.2.3 Remote Log

Remote log feature enables the switch to send system logs to the Log Server. Log Server is to centralize the system logs from various devices for the administrator to monitor and manage the whole network.

Choose the menu **Maintenance**→**Log**→**Remote Log** to load the following page.

Log Host					
Select	Index	Host IP	UDP Port	Severity	Status
<input type="checkbox"/>		<input type="text"/>		<input type="text" value="level_6"/> ▾	<input type="text" value="Disable"/> ▾
<input type="checkbox"/>	1	0.0.0.0	514	level_6	Disable
<input type="checkbox"/>	2	0.0.0.0	514	level_6	Disable
<input type="checkbox"/>	3	0.0.0.0	514	level_6	Disable
<input type="checkbox"/>	4	0.0.0.0	514	level_6	Disable

Figure 15-5 Log Host

The following entries are displayed on this screen:

➤ **Log Host**

Index: Displays the index of the log host. The switch supports 4 log hosts.

Host IP: Configure the IP for the log host.

UDP Port: Displays the UDP port used for receiving/sending log information. Here we use the standard port 514.

Severity: Specify the severity level of the log information sent to each log host. Only the log with the same or smaller severity level value will be sent to the corresponding log host.

Status: Enable or disable the log host.



Note:

The Log Server software is not provided. If necessary, please download it on the Internet.

15.2.4 Backup Log

Backup Log feature enables the system logs saved in the switch to be output as a file for device diagnosis and statistics analysis. When a critical error results in the breakdown of the system, you can export the logs to get some related important information about the error for device diagnosis after the switch is restarted.

Choose the menu **Maintenance**→**Log**→**Backup Log** to load the following page.

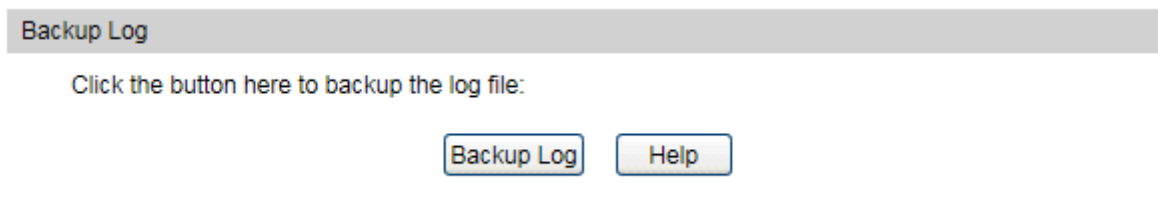



Figure 15-6 Backup Log

The following entry is displayed on this screen:

➤ **Backup Log**

Backup Log: Click the **Backup Log** button to save the log as a file to your computer.

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

15.3 Device Diagnostics

This switch provides Cable Test functions for device diagnostics.

Cable Test functions to test the connection status of the cable connected to the switch, which facilitates you to locate and diagnose the trouble spot of the network.

Choose the menu **Maintenance**→**Device Diagnostics**→**Cable Test** to load the following page.

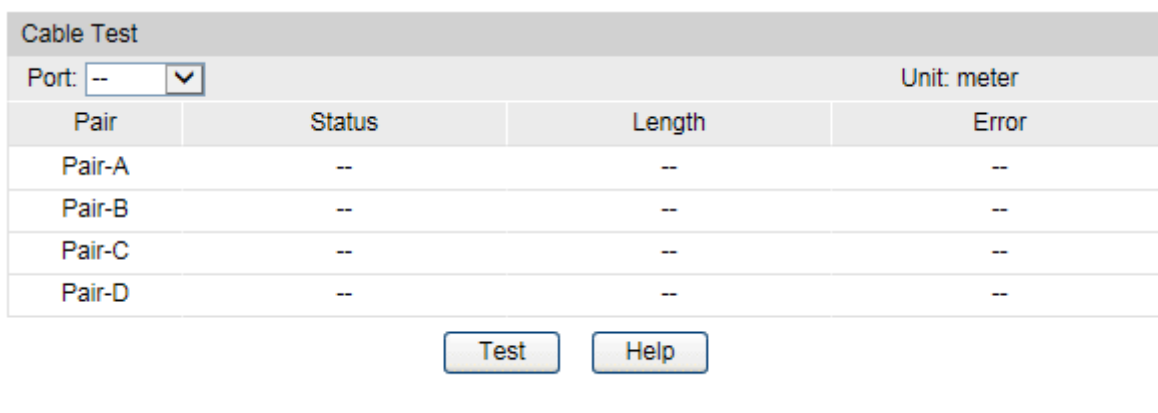


Figure 15-7 Cable Test

The following entries are displayed on this screen:

➤ **Cable Test**

Port: Select the port for cable testing.

Pair: Displays the Pair number.

Status: Displays the connection status of the cable connected to the port. The test results of the cable include normal, close, open or impedance.

Length: If the connection status is normal, here displays the length range of the cable.

Error: If the connection status is close, open or impedance, here displays the error length of the cable.

 **Note:**

1. The 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 reference.
4. If the port is 100Mbps and its connection status is normal, cable test can't get the length of the cable.

15.4 Network Diagnostics

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

15.4.1 Ping

Ping test function, testing the connectivity between the switch and one node of the network, facilitates you to test the network connectivity and reachability of the host so as to locate the network malfunctions.

Choose the menu **Maintenance**→**Network Diagnostics**→**Ping** to load the following page.

Ping Config	
Destination IP:	<input type="text" value="192.168.0.200"/>
Ping Times:	<input type="text" value="4"/> (1-10)
Data Size:	<input type="text" value="64"/> byte (1-1500)
Interval:	<input type="text" value="1000"/> millisec (100-1000)
<input type="button" value="Ping"/> <input type="button" value="Help"/>	

Ping Result
Pinging 192.168.0.200 with 64 bytes of data :
Reply from 192.168.0.200 : bytes=64 time<16ms TTL=64
Reply from 192.168.0.200 : bytes=64 time<16ms TTL=64
Reply from 192.168.0.200 : bytes=64 time<16ms TTL=64
Reply from 192.168.0.200 : bytes=64 time<16ms TTL=64
Ping statistics for 192.168.0.200:
Packets: Sent = 4 , Received = 4 , Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms , Maximum = 0ms , Average = 0ms

Figure 15-8 Ping

The following entries are displayed on this screen:

➤ **Ping Config**

Destination IP: Enter the IP address of the destination node for Ping test. Both IPv4 and IPv6 are supported.

Ping Times: Enter the amount of times to send test data during Ping testing. The default value is recommended.

Data Size: Enter the size of the sending data during Ping testing. The default value is recommended.

Interval: Specify the interval to send ICMP request packets. The default value is recommended.

➤ **Ping Result**

Here you can view the Ping result.

15.4.2 Tracert

Tracert test function is used to test the connectivity of the gateways during its journey from the source to destination of the test data. When malfunctions occur to the network, you can locate trouble spot of the network with this tracert test.

Choose the menu **Maintenance**→**Network Diagnostics**→**Tracert** to load the following page.

The screenshot shows a web interface for the Tracert function. It is divided into two main sections: 'Tracert Config' and 'Tracert Result'. The 'Tracert Config' section contains two input fields: 'Destination IP' with the value '192.168.0.100' and 'Max Hop' with the value '4'. To the right of these fields are two buttons: 'Tracert' and 'Help'. The 'Tracert Result' section is currently empty.

Figure 15-9 Tracert

The following entries are displayed on this screen:

➤ **Tracert Config**

Destination IP: Enter the IP address of the destination device. Both IPv4 and IPv6 are supported.

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

➤ **Tracert Result**

Here you can view the Tracert result.

15.5 DLDP

➤ DLDP Overview

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

➤ DLDP Operation Mechanism

1. DLDP Link States

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

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

Table 15-1 DLDP Link State

2. DLDP Work Process

The general DLDP work process chart is shown below:

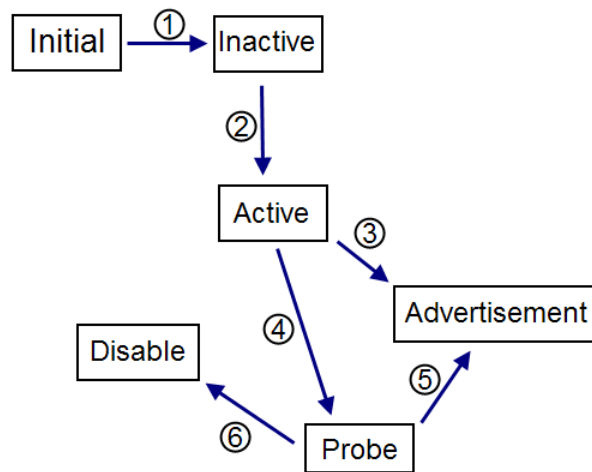


Figure 15-10 DLDP Process

The process is illustrated below

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

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

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

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

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

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

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

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

Choose the menu **Maintenance**→**DLDP**→**DLDP** to load the following page.

Global Config

DLDP State: Enable Disable

Adver Interval: seconds(1-30)

Shut Mode: ▼

Web Refresh State: Enable Disable

Web Refresh Interval: seconds(1-100)

Apply

Port Config

Port Select

Select	Port	DLDP State	Protocol State	Link State	Neighbor State
<input type="checkbox"/>		<input type="text" value=""/> ▼			
<input type="checkbox"/>	1	Disable	Initial	Link-Up	N/A
<input type="checkbox"/>	2	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	3	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	4	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	5	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	6	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	7	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	8	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	9	Disable	Initial	Link-Down	N/A
<input type="checkbox"/>	10	Disable	Initial	Link-Down	N/A

Apply
Reset
Help

Figure 15-11 DLDP Config

The following entries are displayed on this screen:

➤ **Global Config**

DLDP State: Enable or disable the DLDP function globally.

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

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

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

Web Refresh State: Enable or disable the web automatic refresh function.

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

➤ **Port Config**

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

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

Port: Port list of the switch.

DLDP State: Enable or disable DLDP on the selected port.

Protocol State: Displays the DLDP protocol state.

Link State: Displays the state of the links.

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

Configuration Procedure:

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

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-slave 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](#)

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.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

<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



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
	<p>RECYCLING</p> <p>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.</p> <p>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.</p>