VERSITRON®

Your Copper to Fiber Connection

SGX288164M

28-Port Managed Switch

Web Management User's Manual

v1.00

© 2022

VERSITRON, Inc.

83 Albe Drive / Suite C

Newark, DE 19702

www.versitron.com

Copyright © VERSITRON, Inc. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies.

PROPRIETARY DATA

All data in this manual is proprietary and may not be disclosed, used or duplicated, for procurement or manufacturing purposes, without prior written permission by **VERSITRON**.

VERSITRON LIFETIME WARRANTY

All VERSITRON products are covered by a **Lifetime Warranty** against defects in materials and workmanship. This coverage is applicable to the original purchaser and is not transferable.

We repair, or at our option, replace parts/products that, during normal usage and operation, are proven to be defective during the time you own the products, provided that said products and parts are still manufactured and/or available. Such repair/replacement is subsequent to receipt of your product at our facility and our diagnostic evaluation and review of the unit. Advance replacements are not provided as part of the warranty coverage.

This warranty does not cover damage to products caused by misuse, mishandling, power surges, accident, improper installation, neglect, alteration, improper maintenance, or other causes which are not normal and customary applications of the products and for which they were not intended. No other warranty is expressed or implied, and VERSITRON is not liable for direct, indirect, incidental or consequential damages or losses.

In the unlikely event a warranty issue should arise, simply contact us at 302-894-0699 or 1-800-537-2296 or via email at fiberlink@versitron.com to obtain a Return Material Authorization (RMA) number, along with instructions for returning your product.

About This Manual

Copyright

Copyright © 2022 VERSITRON, Inc. All rights reserved.

The products and programs described in this manual are licensed products of VERSITRON, Inc. This manual contains proprietary information protected by copyright, and this manual and all accompanying hardware, software and documentation are copyrighted. No parts of this manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of VERSITRON, Inc.

Purpose

This manual gives specific information on how to operate and use the management functions of the SGX288164M.

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used throughout this manual to show information.

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

See the VERSITRON, Inc. warranty statement.

Disclaimer

VERSITRON, Inc. does not warrant that the hardware will work properly in all environments and applications, and marks no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. VERSITRON, Inc. disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of VERSITRON, Inc.. VERSITRON, Inc. assumes no responsibility for any inaccuracies that may be contained in this User's Manual. VERSITRON, Inc. makes no commitment to update or keep current the information in this User's Manual, and reserves the righter to make improvements to this User's Manual and /or to the products described in this User's Manual, at any time without notice.

Contents

1 Web Overview 5
1.1 Brief 5
1.2 Logging in to the Web interface 5
1.3 Basic Information 6
1.4 Logging out of the Web interface 7
1.5 Save Configuration 7
1.6 Introduction to the Web interface 7
1.7 Introduction to the Web-based functions 8
2 Interface 14
2.1 Port management 14
2.2 Port Ratelimit 16
2.3 Strom Control 18
2.4 Port Statistics 20
2.5 Port Mirror 21
2.6 Port Isolate 22
2.7 Link Aggregation 23
2.7.1 Overview 23
2.7.2 Configuring an Aggregation Group 24
2.7.3 Configuration Example 27
2.8 PoE Management 29
2.8.1 PoE Overview 29
2.8.2 PoE Configuration 30
3 L2-Swtich 33
3.1 VLAN 33
3.1.1 Introduction 33
3.1.2 Configuring a VLAN 36
3.2 QinQ 38

3.2.1 Overview 38
3.2.2 QinQ configuration 39
3.3 ERPS 41
3.2.1 Overview 41
3.2.3 Configure the ERPS 46
3.2.4 Single-ring configuration example 49
3.4 IGMP Snooping 53
3.3.1 Principle of IGMP snooping 53
3.3.2 Configure the IGMP Snooping 54
3.5 Spanning Tree 57
3.4.1 Overview 57
3.4.2 Spanning Tree Configuring 59
3.6 MAC Management 63
3.5.1 Overview 63
3.5.2 Configuring MAC addresses 64
3.5.3 MAC Address Configuration Examples 67
3.7 LLDP 68
3.7.1 Overview 68
3.7.2 Configuring LLDP 69
4.1 ACL 75
4.1.1 Overview 75
4.1.2 Configuring Acls 75
4.2 QoS 81
4.2.1 Overview 81
4.2.2 Configuring Qos 81
4.3 DHCP Snooping 87
4.3.1 Overview 87
4.3.2 Configuring DHCP Snooping 88

4.4 802.1X Authentication 91
4.1.1 Overview 91
4.4.2 Configuring 802.1X 97
4.4.3 802.1X Configuration Example 99
4.5 MAC Authentication 104
4.5.1 Overview 104
4.5.2 Configuring MAC authentication 104
4.5.3 Configuration Example 106
4.6 RADIUS 109
4.6.1 Overview 109
4.6.2 Configuring RADIUS 112
4.6.3 RADIUS Configuration Example 113
4.7 Port Security 114
4.7.1 Overview 114
4.7.2 Configuring Port Security 115
4.7.3 Configuration Example 117
4.8 IP Source Guard 119
4.8.1 Overview 119
4.8.2 Configuring IP Source Guard 119
4.8.3 Configuring ARP Check 121
5 System 122
5.1 Management IP Address 122
5.2 User Management 123
5.3 Service 125
5.3.1 Overview 125
5.3.2 Configuring service 126
5.4 SNMP 127
5.5 Date/Time 129

5.5.1 Date and Time interface 130
5.5.2 Configuing System Time 130
5.5.3 Configuing NTP Server 131
5.6 Configuration File Management 131
5.6.1 Back up configuration 131
5.6.2 Restore Configuration 132
5.6.3 Reset to Factory Defaults 132
5.7 System Upgrade 133
5.8 Log/Diagnosis 134
5.9 Reboot 135
6 Diagnosis 136
6.1 Network Utilities 136
6.1.1 Overview 136
6.1.2 Diagnostic tool operations 137
6.2 Dying Gasp 138
6.2.1 Overview 138
6.2.2 Configuring Dying Gasp 139
6.3 Optical Transceiver Information 139
6.3.1 Displaying Optical Transceiver Information 140
6.3.2 Displaying detail information 140

1 Web Overview

1.1 Brief

The device provides the Web-based network management function to facilitate the operations and maintenance on devices. Through this function, the administrator can visually manage and maintain network devices through the Web-based configuration interfaces. Figure 1-1 shows a Web-based network management operating environment:

Figure 1-1 Web-based network management operating environment

1.2 Logging in to the Web interface

The device is provided with the default Web login information. You can use the following default information to log in to the Web interface:

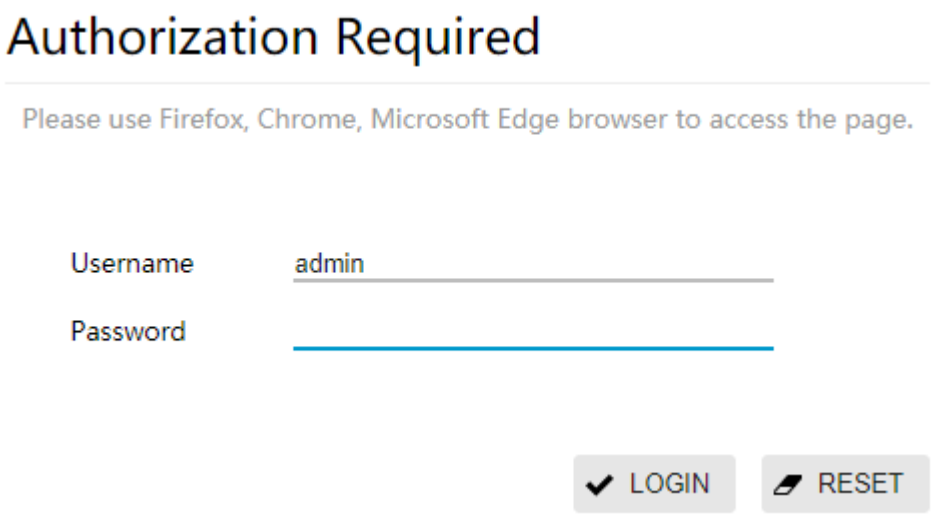
- Username: admin
- Password: admin
- IP address of the device: 192.168.2.1

To log in to the device through the Web interface:

1. Connect the Ethernet interface of the device to the PC using a crossover Ethernet cable.
2. Configure an IP address for the PC and ensure that the PC and device can communicate with each other properly.
3. Modify the IP address of the PC to one that is within the network segment 192.168.2.1/24 (except for 192.168.56.166), for example, 192.168.2.123.
4. Open the browser, and input the login information.

5. On the PC, open the browser, type the IP address http://192.168.2.1 in the address bar, press Enter and you can enter the login page of the Web interface, as shown in Figure 1-2. Input the username **admin** and password **admin**, and click Login.

Figure 1-2 Login page of the Web interface



1.3 Basic Information

After logging in to the Web interface, you will enter the Basic Information page, as shown in Figure 1-3. Table 1-1 which lists the configuration items of the basic information. The Host Name can be modified. After entering the new information, click the Apply button.

Figure 1-3 Basic Information page

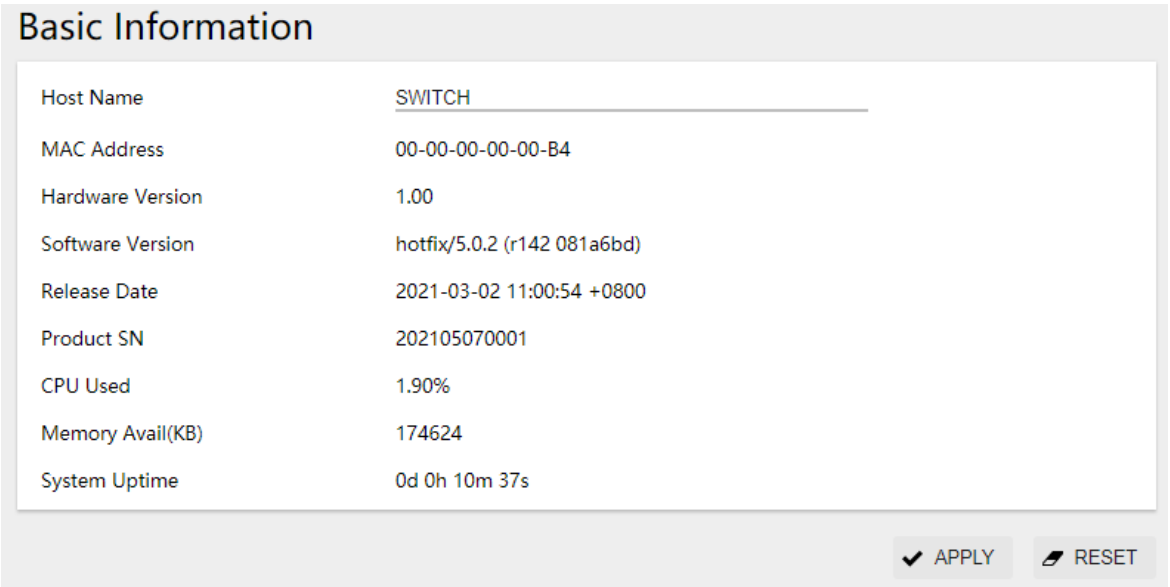


Table1-1 Basic Information configuration items

Item	Description
Host Name	Displays the device name. Allows user to change it.
MAC Address	Displays the device’ s MAC address.
Hardware Version	Displays the device’ s hardware version.
Software Version	Displays the device’ s software version.
Release Date	Displays the device software’ s release date.
Product SN	Displays the device’ s serial number.
CPU Used	Displays the device’ s cpu status.
Memory Avail	Displays the device’ s memory status.
System Uptime	Displays the time from last system start.

1.4 Logging out of the Web interface

Click the Logout button in the navigation area to quit Web-based network management. **The system does not save the current configuration before you log out of the Web interface. Therefore, we recommend that you save the current configuration before logout.**

NOTE:

- You cannot log out by directly closing the browser.

1.5 Save Configuration

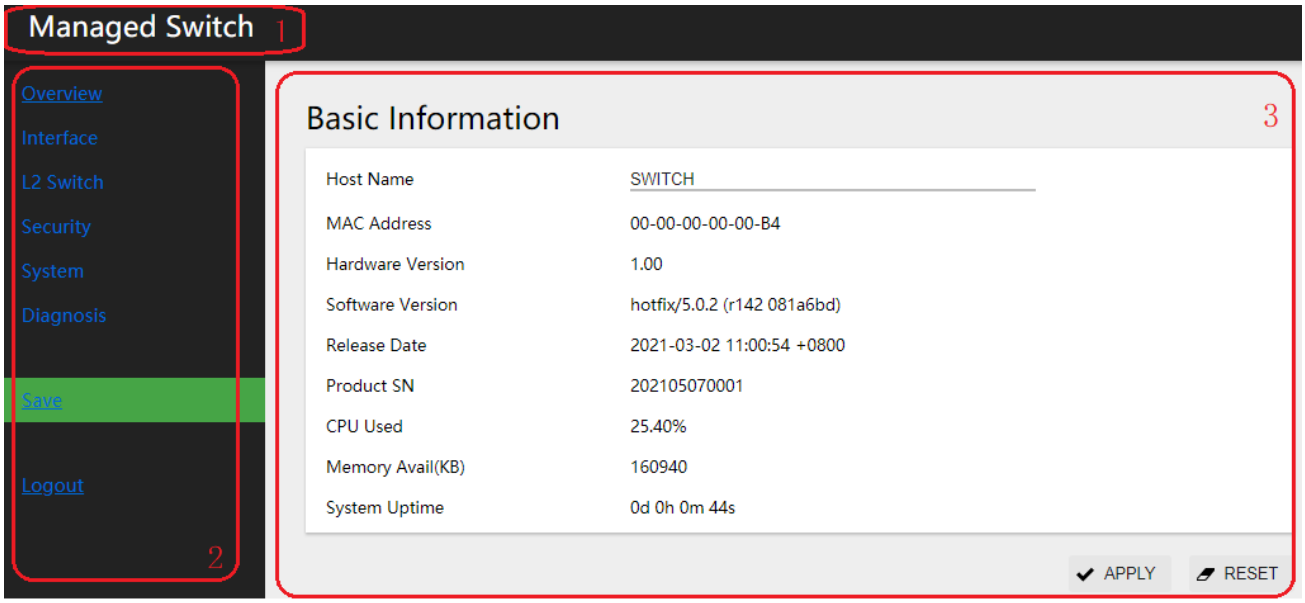
The save configuration module provides the function to save the current configuration to the configuration file for the next startup.

Click the Save button to save the current configuration to the configuration file.

1.6 Introduction to the Web interface

The Web interface is composed of three parts: navigation area, title area, and body area, as shown in Figure 1-4.

Figure 1-4 Web-based configuration interface



(1) Title area	(2) Navigation area	(3) Body area

- Item：Product Name
- Navigation area: Organizes the Web-based function menus in the form of a navigation area where you can select function menus as needed. The result is displayed in the body area. The Web network management functions not supported by the device are not displayed in the navigation area.
- Body area: The area where you can configure and display a function.

1.7 Introduction to the Web-based functions

Table 1-2 describes the Web-based network management functions in detail.

Table 1-2 Description of Web-based functions

Function menu		Description
Overview	Basic information	Displays device information.
Interface	Port management	Displays interface information and statistics. Allows to create, modify, delete, and enable/disable an interface.
	Port Ratelimit	Display and allows set the port ratelimit.
	Strom Control	Display and allows set strom control mode.
	Port Statistics	Display and allows clear port statistcs

	Port mirror		Display and allows create/remove a port mirroring group.	
	Port isolate		Allows user to create isolate port groups.	
	Link Aggregation	Global Configuration	Display and allows set Load balancing method.	
		Aggregation Port	Display the information of the Aggregation Port.	
		Aggregation Member	Allows set Aggregation Member ID and Aggregation mode.	
	PoE management	PoE Global Configuration	Display and allows set PoE supply power and enable/disable legacy mode.	
		PoE interface Configuration	Display the statistics of the PD devices. Allows Enable/Disable PoE for the PoE interface	
network	VLAN	VLAN	Allows user to create, modify and delete VLANs.	
		Interface	Allows user to create, modify, delete, and enable/disable an interface. Allows user to modify the VLANs to which a port belongs.	
	QinQ	Configuration	Display and allows create/remove port QinQ	
		Apply	Enable the QinQ function of the port	
	ERPS	Summary	Displays the detailed information of the ERPS	
		Configuration	ERPS Ring Configuration	Allows user to configure the ERPS Ring ID, east interface and west interface.

		ERPS Instance Configuration	Allows user to configure the ERPS RAPS VLAN, Data VLAN, Owner interface.
IGMP Snooping	Summary	Displays the detailed information of the IGMP Snooping	
	Configuration	IGMP Snooping	Allows user to enable/disable IGMP Snooping.
		IGMP Mrouter Interface	Allows user to configure IGMP Mrouter Interface.
		IGMP Static Group	Allows user to configure IGMP Static Group
Spanning Tree	Summary	Display the detailed information of the MSTP	
	Global Configuration	Display and allows set MSTP globe configuration	
	MST Configuration	Display and allows set the information of MST configuration	
	Instance	Allows create and remove MSTP Instance	
	Interface	Display and allows set MSTP interface configuration	
MAC management	MAC management	Allows set MAC Ageing Time.	
	Static MAC Address	Allows set Static MAC Address.	
	Filter MAC Address	Allows set Filter MAC Address.	
Global Configuration		Enable LLDP fuction, confiure system name and	

			system description	
	Port		Configure interface’ s parameters	
	Statistics		Show LLDP status of device	
Security	ACL	ACL	Allows create/remove/modify an ACL Rule.	
		Apply	Allows configure the port rule.	
	QoS	Summary	Display and allows configure QoS global configuration and Queue Weight.	
		Interface trust mode	Display and allows Configure interface trust mode.	
		CoS Map	Display and allows Configure CoS Map.	
		DSCP Map	Display and allows Configure DSCP Map.	
		Policy	Display and allows Configure QoS Policy.	
	DHCP Snooping	Enable/Disable	Enable/Disable DHCP Function.	
		DHCP Snooping Trust	Allows user to configure the status of the DHCP Snooping function and modify the trusted and untrusted attributes of a port.	
	802.1 X Authentication	Summary	Display 802.1x authentication profile	
		Configuration	Global Configuration	Enable/disable
			Port Configuration	Set 1x rules of the interface
	MAC Authentication	Summary	Displays MAC authentication profile	
		Configuration	Global Configuration	Enable/disable
			Port Configuration	Set MAC rules of the interface
	RADIUS	Global Configuration	RADIUS global configuration	

		Server	Show/configure RADIUS server configuration
	Port Security	Port Configuration	Allows user to configure port security function
		MAC Configuration	Allows user to configure MAC security function
	IP Source Guard	Summary	Display IP source guard summary
		Port Configuration	Allows user to configure port security function
		User Configuration	Allows user to configure VID, MAC address, IP address of the interface
System	Management IP Adderss		Allows user to Configures the management VLAN, IP address and mask.
	User management		Allows user to change the password.
	Service	Telnet Server	Allows user to Enable/Disable Telnet Server.
		SSH Server	Allows user to Enable/Disable SSH Server.
		HTTP Server	Allows user to Enable/Disable HTTP Server.
		HTTPS Server	Allows user to Enable/Disable HTTPS Server.
	SNMP	SNMPv1 / v2c	Display and allows configure snmpv1/v2c.
		SNMPv3	Display and allows configure snmpv3
	Date/Time		Displays and allows configuration of the system date and time.
	Configuration File	Backup	Allows user to back up the configuration file for the next startup to the host of the current user.

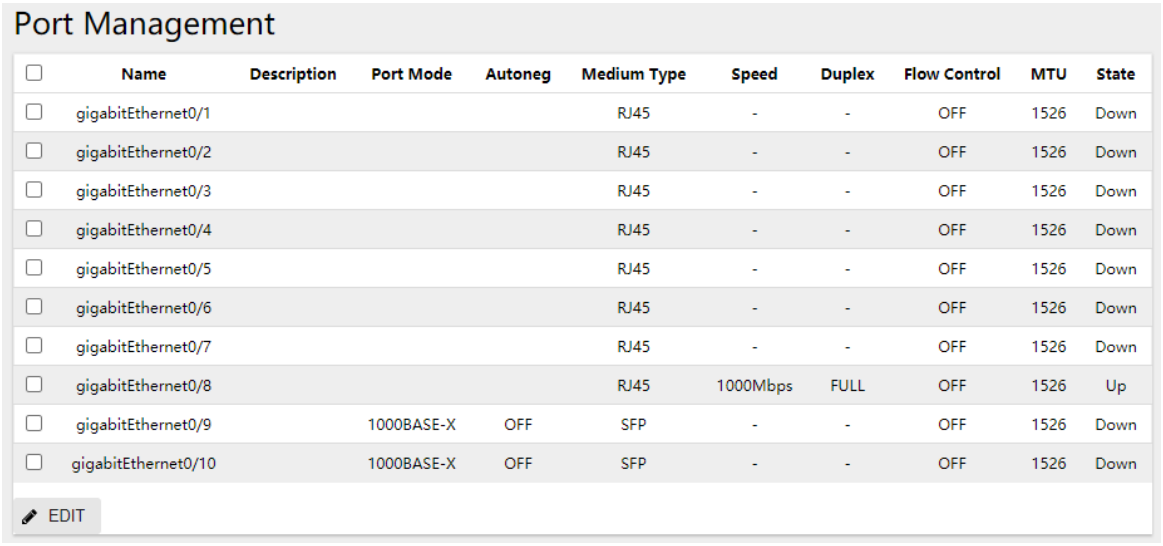
	Management	Restore	Allows user to upgrade the configuration file on the host of the current user to the device for the next startup.
		Reset to Factory Defaults	Allows user to restore the system to factory defaults.
	System Upgrade		Allows user to upload the file to be upgraded from the local host to upgrade the system software.
	Log		Allows user to generate a diagnostic information file, view the file or save the file to the local host.
	Reboot		Allows user to reboot the device.
Diagnosis	Network Utilities		Perform the ping/trace route operation and display the results.
	Dying Gasp		Enable\Disable the dying gasp function
	Optical Transceiver Information		Display optical module information, such as manufacturer, serial number, optical power, etc
Save	\		Allows user to save the current configuration to the configuration file for the next startup.
Logout	\		log out of the Web interface

2 Interface

2.1 Port management

You can use the interface management feature to view interface information, create/remove logical interfaces, change interface status, and reset interface parameters, as shown in Figure 2-1.

Figure 2-1 Port management page



Configuring interface management

1. Select Interface > Port Management in the navigation area to enter the port managemnet page as shown in Figure 2-1.

2. Select the interface to be configured, click Edit button to enter the page for configuring an interface, as shown in Figure 2-2. Table 2-1 describes the configuration items of configuring an interface

Figure 2-2 interface management page

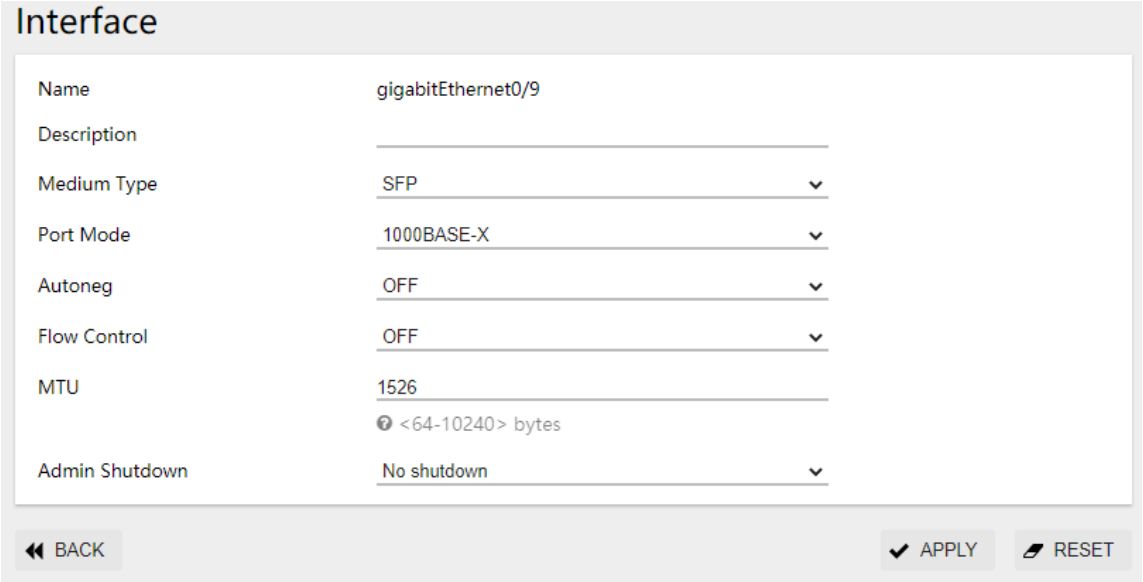


Table 2-1 Configuration items of configuring an interface

Item	Description
Name	The name of the logical interface.
Description	Set the description of a logical interface.
Medium type	Set the medium type of the Combo ports • RJ45：the mode of port is 10/100/1000BASE-T • SFP：the mode of port is 1000BASE-X Note: only for combo ports.
Speed	Set the port’ s transmission rate: • 10: indicates 10 Mbps • 100M：indicates 100 Mbps • 1000M：indicates 1000 Mbps • Auto: indicates auto-negotiation Note: only for copper ports.
Duplex	Set the port’ s duplex mode: • AUTO：indicates auto-negotiation • FULL：indicates full duplex • HALF：indicates half duplex Note: only for copper ports.
Port Mode	Set the port’ s mode • 100BASE-FX：indicates the port mode is 100BASE-FX.

	• 1000BASE-X：indicates the port mode is 1000BASE-X. • SGMII： indicates the port mode is SMGII. • 2500BASE-X：indicates the port mode is 2.5G BASE-X. • 10G BASE-X: indicates the port mode is 10G BASE-X. Note: only for fiber ports.
Autoneg	Enables or disables port’ s autoneg. The auto-negotiation function needs to be enabled or disabled at the same time as the peer end, otherwise a link failure will occur. Note: only for fiber ports.
Flow Control	Enables or disables flow control on the port.
MTU	Allows or forbids jumbo frames to pass through the port.
Admin Shutdown	Shutdown/no shutdown the port.

2.2 Port Ratelimit

Port-based rate limiting allows you to limit the speed at which network traffic is sent or received by a device that is connected to a port on your switch. Unlike 802.1p Quality of Service (QoS), port-based rate limiting does not prioritize information based on type. Rate limiting simply means that the switch will slow down traffic on a port to keep it from exceeding the limit that you set. If you set the rate limit on a port too low, you might see degraded video stream quality, sluggish response times during online activity, and other problems.

The best use of rate limiting is to keep low-priority devices that are connected to your switch from using too much of your bandwidth and slowing down your other connected devices. A combination of rate limiting and QoS can help you maximize your network’ s efficiency and prioritize devices and activities.

Configuring Port Ratelimit

1. Select Interface > Port Ratelimit in the navigation area to enter the port ratelimit page as shown in Figure 2-3.

2. Select the ports to be configured, as shown in Figure 2-4, type the number in the box. Table 2-2 describes the configuration items of configuring an interface.

3. Click the Apply button.

4. Click the Save button in the navigation area.

Figure 2-3 Port Ratelimit status page

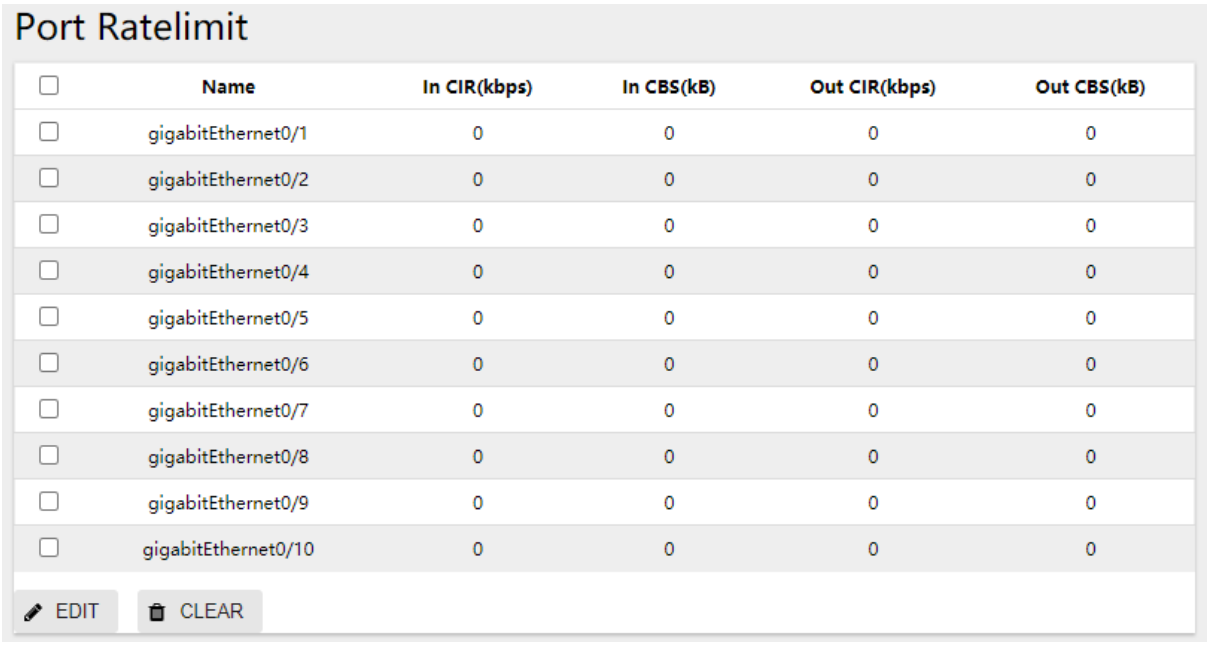
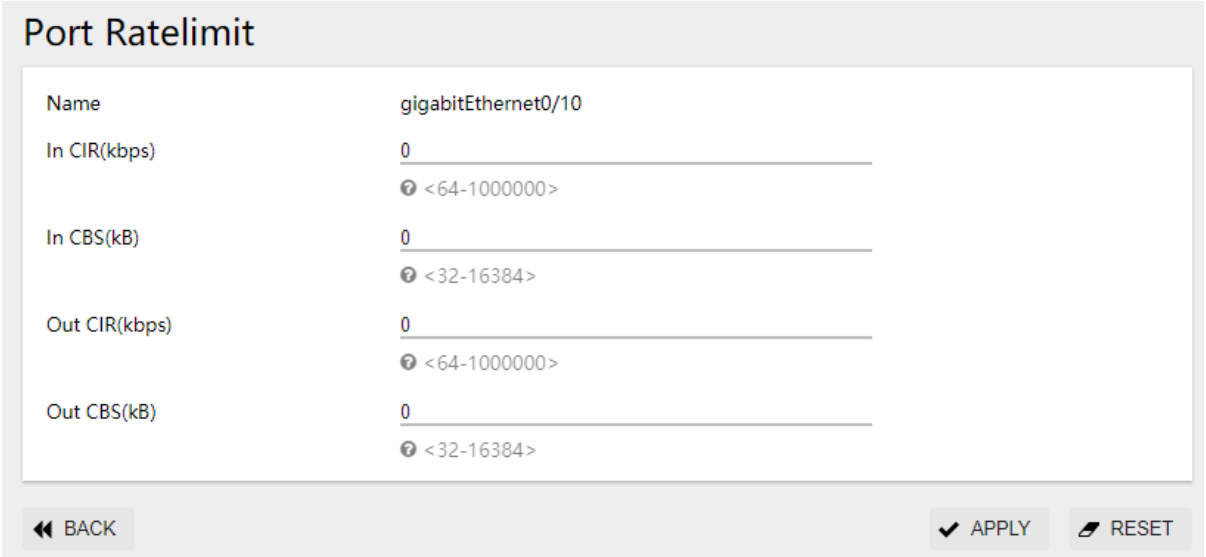


Figure 2-4 Port Ratelimit configuration page



NOTE:

- CBS embodies a rate-limit feature for policing traffic. When policing traffic with CBS, here recommends the burst value 4 times of the limit value. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

Table 2-2 Port Ratelimit Configuration items

Item	Description
In CIR (kbps)	Specify the rate limit in the inbound direction (KBits).
In CBS (KB)	Specify the burst size in the inbound direction (KBits).
Out CIR (kbps)	Specify the rate limit in the outbound direction (KBits).
Out CBS (KB)	Specify the burst size in the outbound direction (KBits).
Apply	Click to enable port ratelimit.
Clear	Click to clear the box.

2.3 Strom Control

A traffic storm occurs when a large amount of broadcast, multicast, or unicast packets congest a network.

You can use the storm suppression function to limit the size of a particular type of traffic (currently broadcast, multicast and unknown unicast traffic) on a per-interface basis in Ethernet port view or port group view.

In interface or port group view, you set the maximum broadcast, multicast or unknown unicast traffic allowed to pass through an interface or each interface in a port group. When the broadcast, multicast, or unknown unicast traffic on the interface exceeds the threshold, the system discards packets until the traffic drops below the threshold.

Configuring the Storm Control on an Ethernet Port

1. Select Interface > Strom Control in the navigation area to enter the storm control page as shown in Figure 2-5.

2. Select the ports to be configured, click Edit to enter the page shown in Figure 2-6.

3. Configure the type of the strom control and type the percentage in the box below. The description of the strom control is described in Table 2-3.

4. Click the Apply.

5. Click the Save in the navigation area.

Figure 2-5 Strom Control page

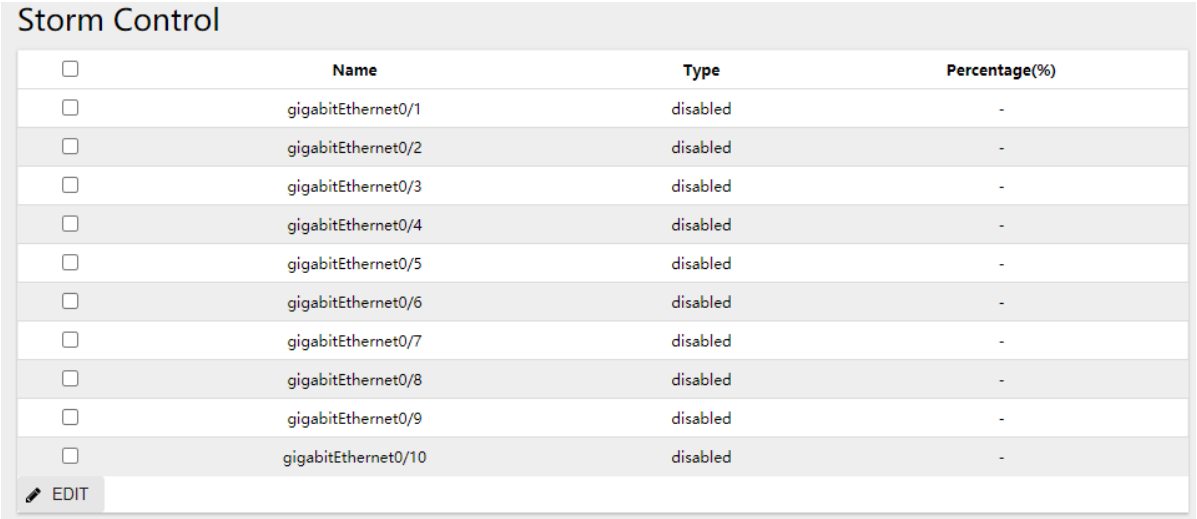


Figure 2-6 Strom Control Page

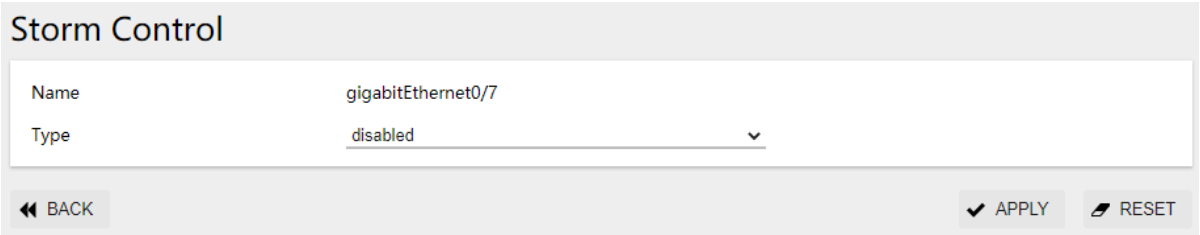


Table 2-3 Items of the strom control

Item		Description
Name		The logical interface
Type	disabled	Disable strom control
	broadcast	Selects the parameter used in broadcast suppression and sets its value in the percentage box.
	multicast	Selects the parameter used in multicast suppression and sets its value in the percentage box.
	unicast	Selects the parameter used in unicast suppression and sets its value in the percentage box.

	multicast-broadcast	Selects the parameter used in multicasta and broadcast suppression and sets its value in the percentage box.
	unicast-broadcast	Selects the parameter used in unicast and broadcast, suppression and sets its value in the percentage box.
	all	Selects the parameter used in unicast and unicast, broadcast, suppression and sets its value in the percentage box.
Percentage (%)		Indicates the maximum percentage of traffic to the total transmission capability of an Ethernet interface.

2.4 Port Statistics

The port statistics module displays statistics about the packets received and sent through interfaces.

Displaying port statistics

Select Interface > Port Statistics in the navigation area to enter the page shown in Figure 2-7. The page displays the port' s Rx Packets, Rx Bytes, Tx Packets, Tx Bytes. Table 2-4 describes the items of port statistics.

Figure 2-7 port statistics page

Port Statistics

Name	Rx Packets	Rx Bytes	Tx Packets	Tx Bytes	Rx pps	Rx bps	Tx pps	Tx bps	Clear
gigabitEthernet0/1	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/2	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/3	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/4	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/5	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/6	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/7	0	0	0	0	0	0	0	0	CLEAR
gigabitEthernet0/8	1,169	145,216	669	364,530	2	3,784	3	8,376	CLEAR

Table 2-4 Items of port statistics

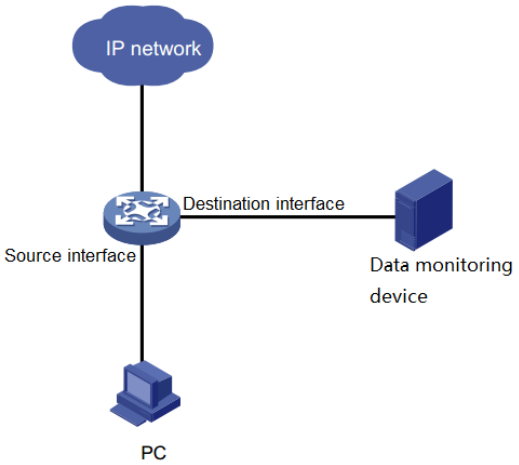
Item	Description

Name	The name of the logical interface.
Rx Packets	The packets number of the interface received.
Rx Bytes	The Bytes number of the interface received.
Tx Packets	The packets number of the interface transmited.
Tx Bytes	The Bytes number of the interface transmited.
Rx pps(pps)	The speed of the interface receiced, pps (bit per second).
Rx bps(bps)	The speed of the interface receiced, bps (bit per second).
Tx pps(pps)	The speed of the interface transmited, pps (bit per second).
Tx pps(bps)	The speed of the interface transmited, bps (bit per second).
Clear	Click to clear the statistics.

2.5 Port Mirror

Port mirroring is to copy the packets passing through one or multiple ports (called source interface) to a port (called the destination interface) on the local device. The source interface is connected with a monitoring device. By analyzing on the monitoring device, the packets mirrored to the destination interface, you can monitor the network and troubleshoot possible network problems.

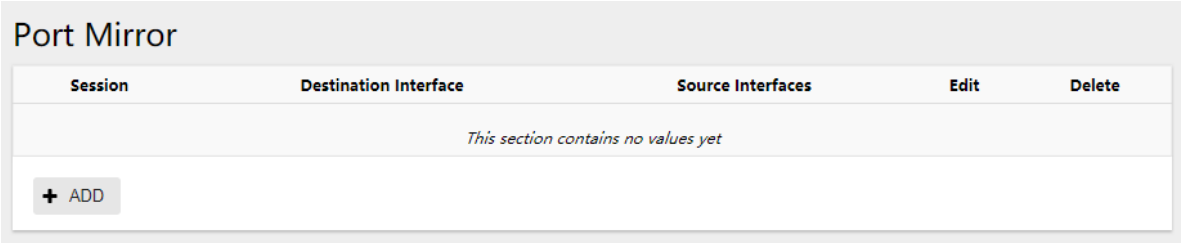
Figure2-8 A port mirroring implementation



Creating a mirroring group

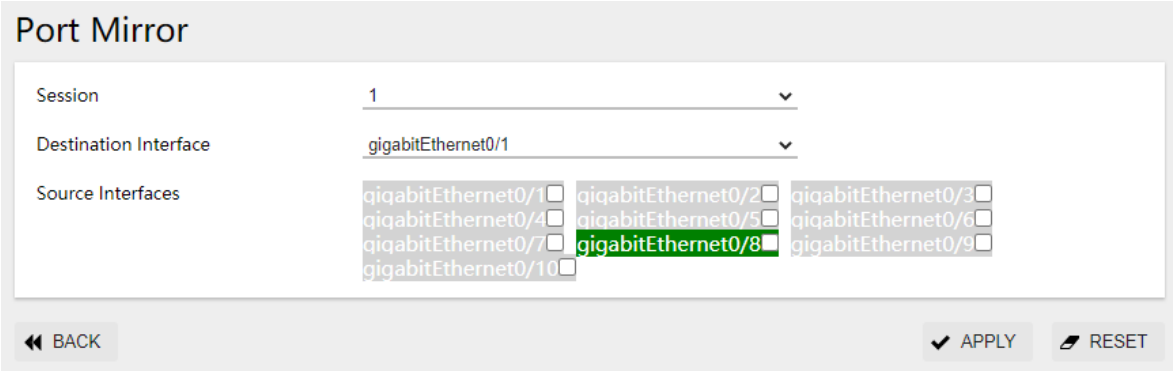
1. Select Interface > Port Mirror in the navigation area to enter the Port mirror page as shown in Figure 2-9.

Figure 2-9 Port Mirror Page



2. Click the +Add to enter the page for creating a mirroring port, as shown in Figure 2-10. Table 2-5 describes the configuration items of creating a mirroring group.

Figure 2-10 The page for creating a mirroring group



3. Configure the ‘Session’, ‘Destination Interface’, ‘Source Interfaces’.

4. Click Apply.

5. Click Save in the navigation area.

Table 2-5 Configuration items of creating a mirroring group

Item	Description
Session	ID of the mirroring group to be created
Destination Interface	the monitor port for the mirroring group
Source Interface	mirroring ports for the mirroring group

2.6 Port Isolate

Usually, Layer 2 traffic isolation is achieved by assigning ports to different VLANs. To save VLAN resources, port isolation is introduced to isolate ports within a VLAN, allowing for great flexibility and security.

1. Switch support multiple isolation groups which can be configured manually. These devices are referred to as multiple-isolation-group devices.

2. There is no restriction on the number of ports assigned to an isolation group.

3. Within the same VLAN, Layer 2 data transmission between ports within and outside the isolation group is supported.

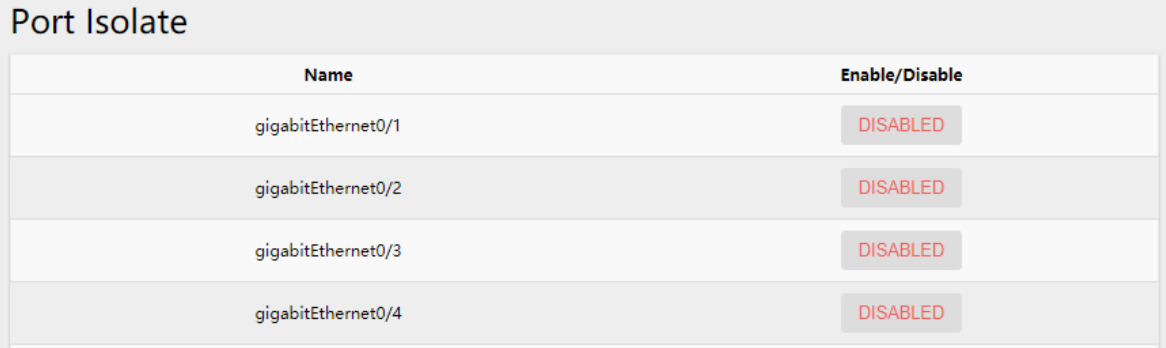
Configuring an Isolation Group

1. Select Interface > Port Isolate in the navigation area to enter the Port isolate page as shown in Figure 2-11.

2. Select the port to be isolated, click Enable/Disable button.

5. Click Save in the navigation area.

Figure 2-11 Port Isolate page



2.7 Link Aggregation

2.7.1 Overview

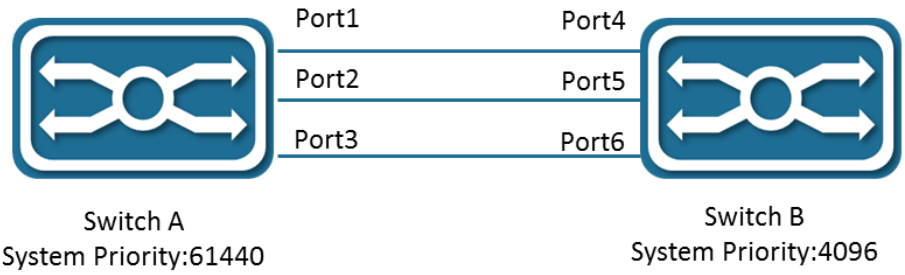
Link Aggregation

Ethernet link aggregation, most often simply called link aggregation, aggregates multiple physical Ethernet links into one logical link to increase link bandwidth beyond the limits of any one single link. This logical link is called an aggregate link. It allows for link redundancy because the member physical links dynamically back up one another.

As shown in Figure 2-11, Switch A and Switch B are connected with three physical Ethernet links. These physical Ethernet links are aggregated into an aggregate link, Link aggregation 1. The

bandwidth of this aggregate link can be as high as the total bandwidth of these three physical Ethernet links.

Figure 2-11 Port Isolate page



LACP

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables dynamic aggregation of physical links. It uses link aggregation control protocol data units (LACPDUs) for exchanging aggregation information between LACP-enabled devices.

There are two link aggregation modes: dynamic and static. Dynamic link aggregation uses LACP while static link aggregation does not. A link aggregation group operating in static mode is called a static link aggregation group, while a link aggregation group operating in dynamic mode is called a dynamic link aggregation group.

2.7.2 Configuring an Aggregation Group

Configuration procedure:

1. Select Interface > Link Aggregation in the navigation area to enter the Link Aggregation page as shown in Figure 2-12, The description of the link aggregation is described in Table 2-6.

Figure 2-12 Global Configure Page

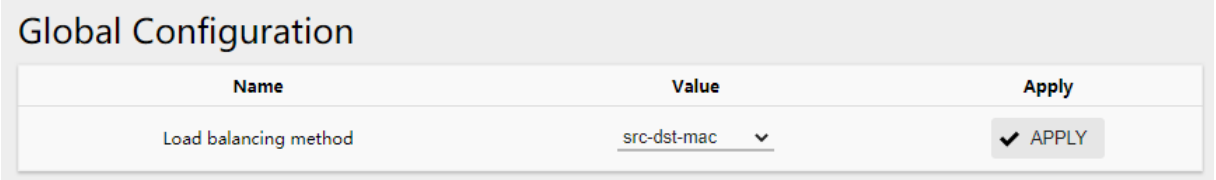


Table 2-6 description of global configure item

Item		Dedcription	
Global Configuration	Name	Load balancing method	
	Value	dst-mac	Equalize according to the destination MAC address
		src-mac	Equalize according to the source MAC address
		src-dst-mac	Equalize according to the destination MAC address and source MAC address
		dst-ip	Equalize according to the destination IP address
		srt-ip	Equalize according to the source IP address
		src-dst-ip	Equalize according to the destination IP address and source IP address
		dst-port	Equalize according to the L4 TCP/UDP destination port number
		src-port	Equalize according to the L4 TCP/UDP source port number
		src-dst-port	Equalize according to the L4 TCP/UDP destination port number and source port number
	Apply	Click to enable	

(2) In the Aggregation Member Configure page, configure the 'ID', 'MODE' of the port as shown in Figure 2-13, The description of the link aggregation is described in Table 2-7. Click Apply to Complete configuration.

Figure 2-13 Aggregation Member Configure page

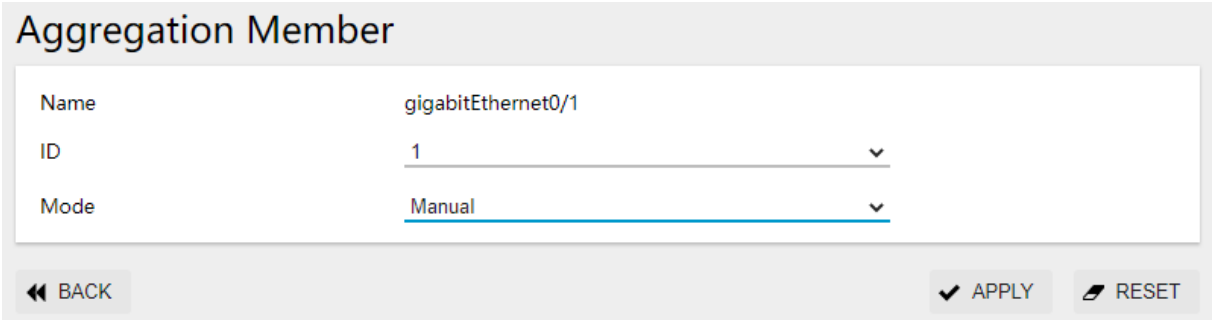


Table 2-7 description of Aggregation Member

Item		Dedcription	
Aggregation Member	Name	The device interface number	
	ID	The ID of the Aggregation Member	
	Mode	Manual	Manual mode
		Active	In this mode, the ports send LACP packets at regular intervals to the partner ports
		Passive	In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving the LACP packets from the partner port, the ports send LACP packets to the partner port.

After the configuration is complete, the aggregation port created is displayed on the Aggregation Port page, as shown in Figure 2-14. The description of Aggregation Port is described in Table 2-8.

Figure 2-14 Aggregation port page

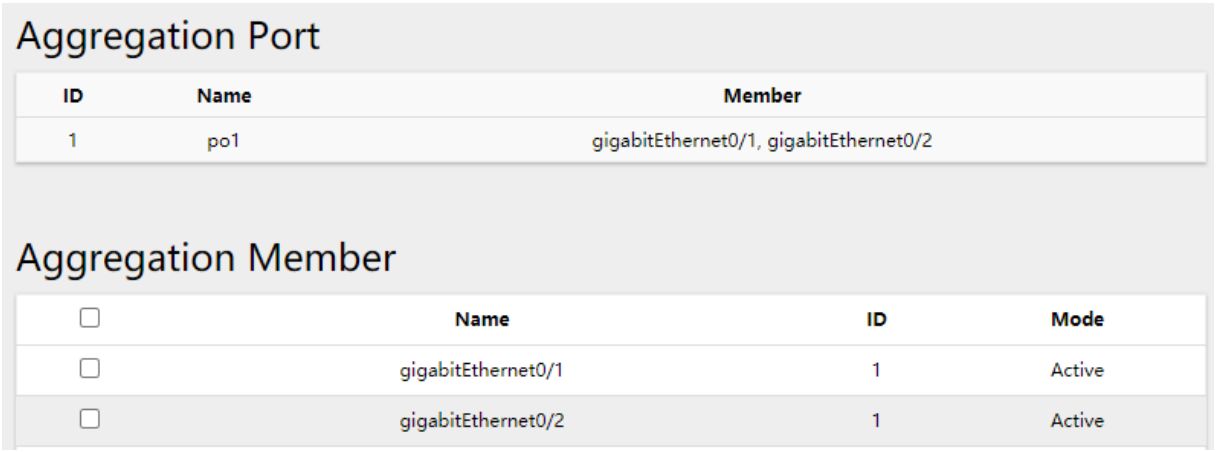


Table 2-8 description of Aggregation port

Item		Dedcription
Aggregation Port	ID	The ID of the Aggregation Port
	Name	The name of the Aggregation Port
	Member	The member ports of the Aggregation Port

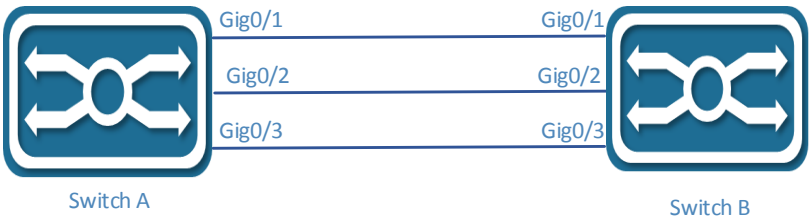
2.7.3 Configuration Example

1. Network Requirements

• As shown in Figure 2-15, aggregate the ports on each device to form a link aggregation group, balancing incoming/outgoing traffic across the member ports

• You can create a static or dynamic link aggregation group to achieve load balancing.

Figure 2-15 Network diagram



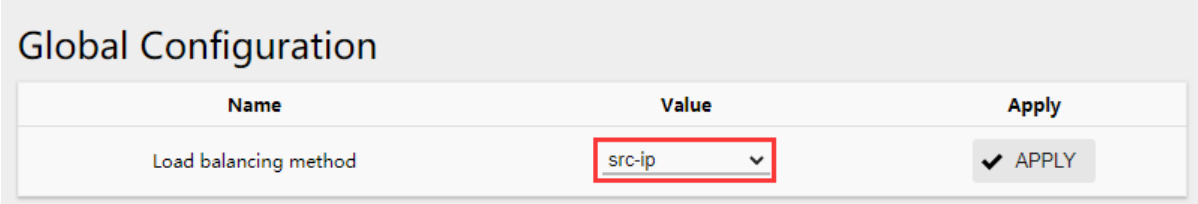
2. Configure procedure

Approach 1: Create static link aggregation

1. Select interface > Link aggregation from the navigation area to enter the Global Configuration page.

2. In the Global Configuration page, select the src-ip option for the load balancing method, click Apply to complete the configuration, as shown in Figure 2-16.

Figure 2-16 Global Configuation



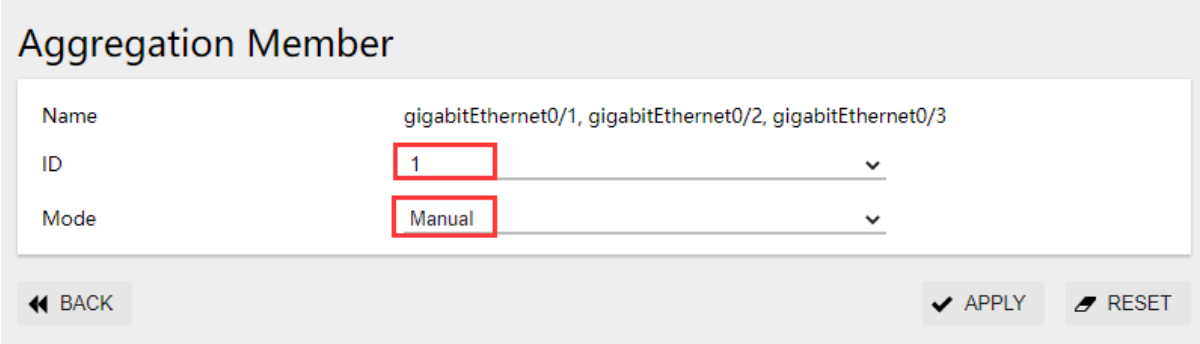
3. In the Aggregation Member area, check the box in front of the gigabitEthernet0/1, gigabitEthernet0/2, gigabitEthernet0/3, click the EDIT button to enter the page as shown in Figure 2-17.

1. Set the ID ‘1’.

2. Select the Manual option for the Mode.

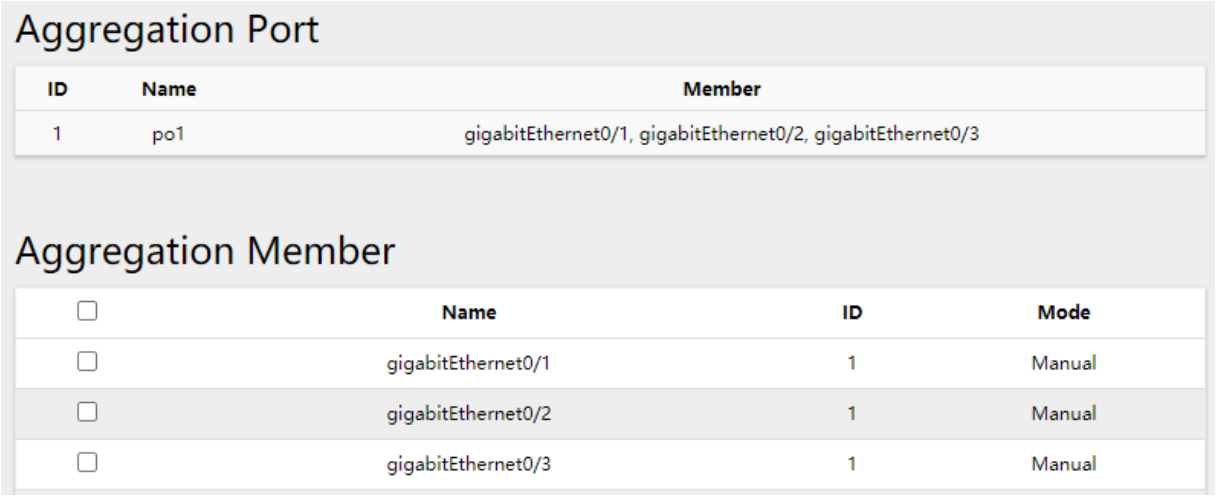
3. Click Apply.

Figure 2-17 Aggregation member static configuration



After the configuration is complete, the static aggregation port created is displayed on the Aggregation Port page, as shown in Figure 2-18.

Figure 2-18 static aggregation port



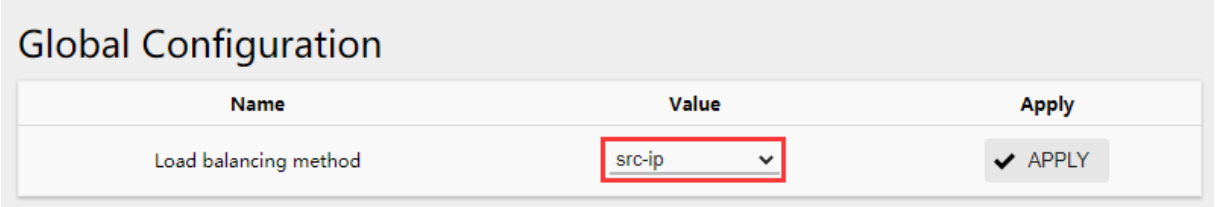
4. Click Save in the navigation area.

Approach 2: Create dynamic link aggregation

1. Select interface > Link aggregation from the navigation area to enter the Global Configuration page.

2. In the Global Configuration page, select the src-ip option for the load balancing mgigabitEthernetod, click【Apply】to complete the configuration, as shown in Figure 2-19.

Figure 2-19 Global Configuation



3. In the Aggregation Member page, configure the gigabitEthernet0/1, gigabitEthernet0/2, gigabitEthernet0/3. As shown in Figure 2-20.

a. Set the ID ‘1’ .

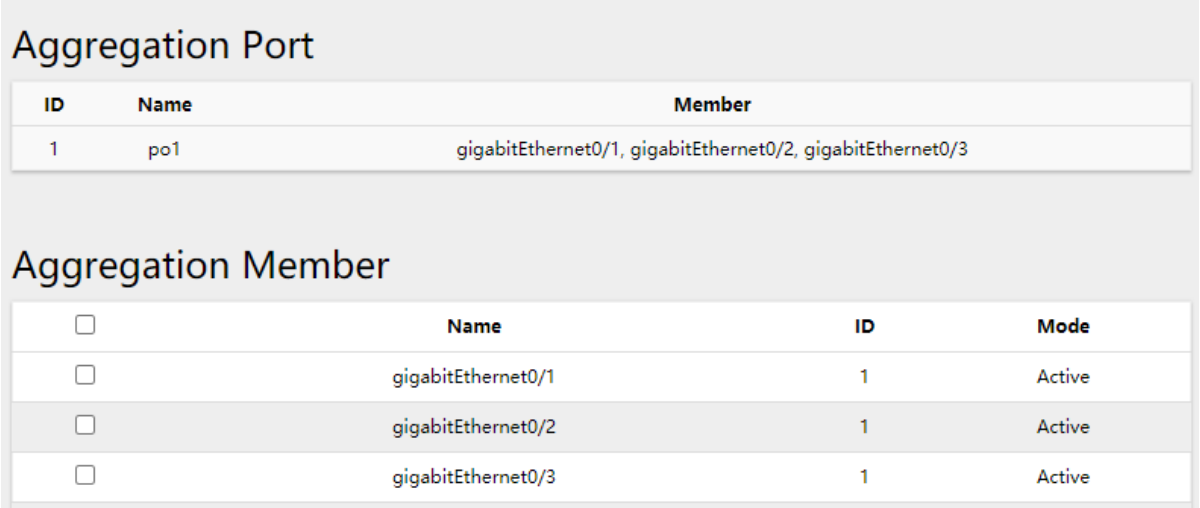
b. Select the Active option for the Mode.

c. Click Apply.

Figure 2-20 Aggregation member dynamic configuration

After the configuration is complete, the dynamic aggregation port created is displayed on *the* Aggregation Port page, as shown in *Figure 2-21.*

Figure 2-21 dynamic aggregation port



4. Click Save in the navigation area.

2.8 PoE Management (Not Applicable to the SGX288164M)

2.8.1 PoE Overview

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PDs) from Ethernet interfaces through twisted pair cables.

2.8.2 PoE Configuration

NOTE:

- Before configure PoE, make sure that the PoE power supply and PSE are operating normally; otherwise, you cannot configure PoE or the configured PoE function does not take effect.

1. Select Interface > PoE Management in the navigation area to enter the PoE Management page as shown in Figure 2-22, the Table 2-9 describes the items of PoE Global Configuration.

2. Type the max power supply in the Power supply text.

Figure 2-22 PoE Global Configuration

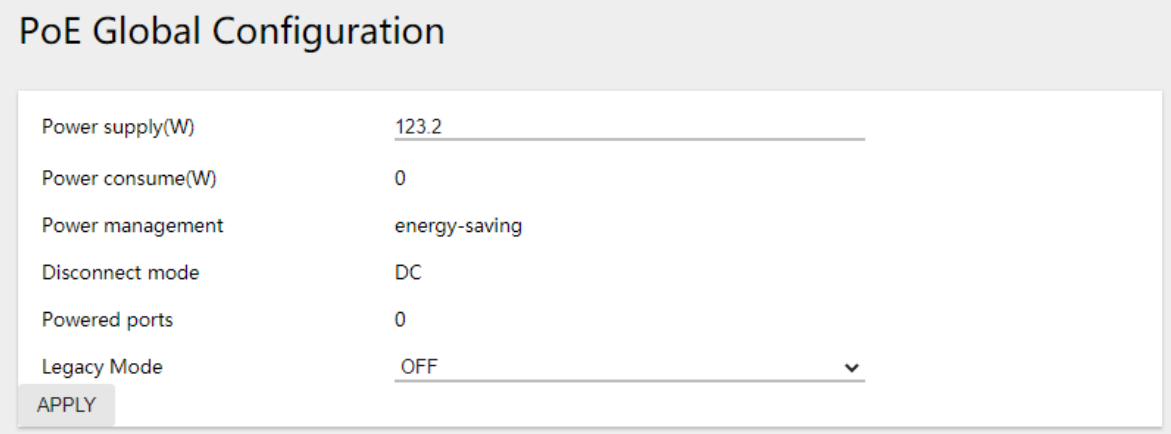


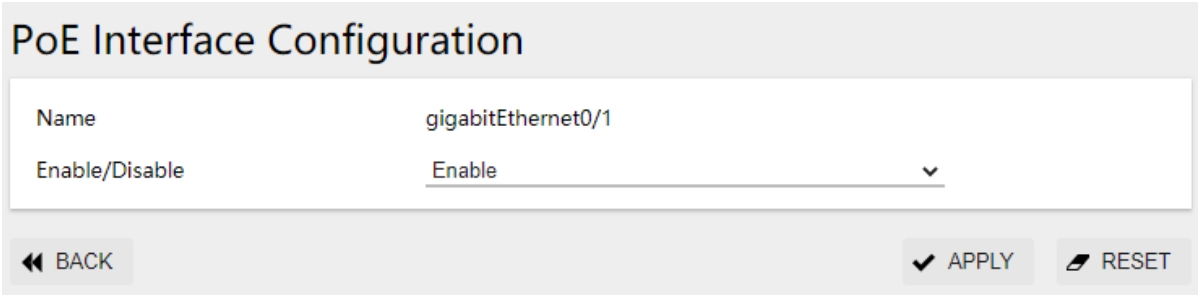
Table 2-9 description of PoE Global Configuration

Item	Description
Power supply	The maximum power that the PSE can provide to the connected PD. The default value=15.4w*port number of the switch. • When the sum of the power consumption of all powered PoE interfaces on a PSE exceeds the maximum power of the PSE, the system considers the PSE is overloaded. So, the Power supply must be configured correctly to avoid overload, Use the Equation below to calculate the Power supply. Power supply=PoE Power-10W.
Power consumes	Display the sum of the power consumption of all poe interface.

Power management	Display the mode of power management is engery-saving. In this mode, the power requested and allocated to the port is based on the actual port's (real time) power consumption.
Disconnect mode	Display the mode of disconnection is DC disconnect
Powered ports	Display the number of the powered ports.
Legacy Mode	ON/OFF，the default is OFF. OFF：Resistor detection only, only support the pd which has the valid decect resistor. ON：Resistor & legacy detection, support the pd which has the invalid decect resistor.

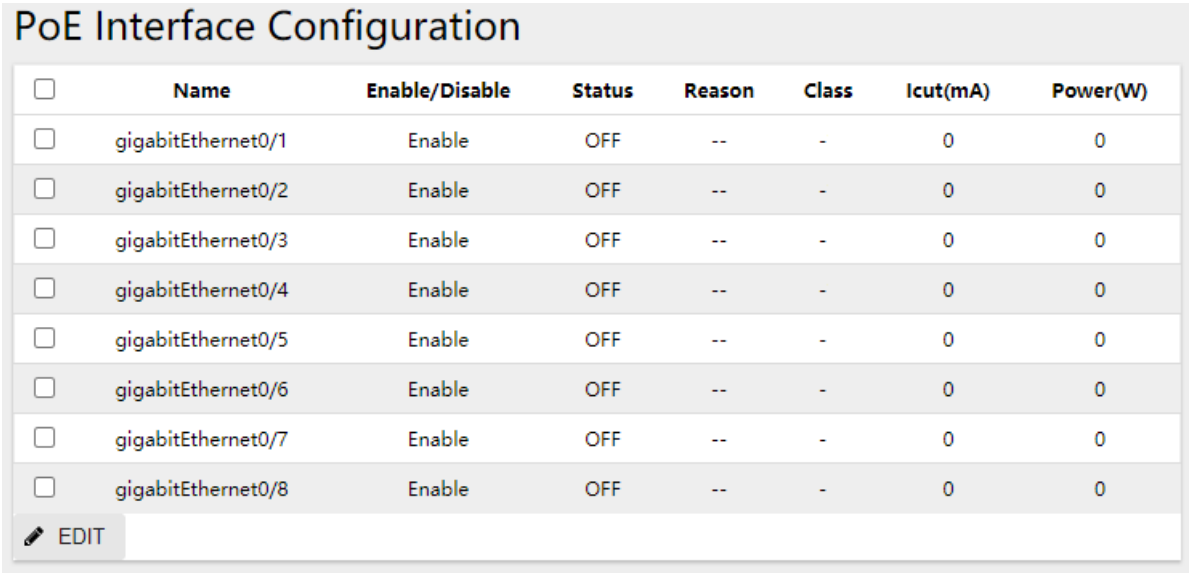
3. Select the port to be configured and click the Edit to enter the Edit Interface page of the interface, as shown in Figure 2-23. You can enable/disable PoE for the PoE interface.

Figure 2-23 PoE Interface Configuration



4. Click the Apply to complete the operation, and then the page will return to the PoE Interface Configuration page autoly, as shown in Figure 2-24. the Table 2-10 describes the items of the PoE Interface Configuration.

Figure 2-24 PoE Interface Configuration



5. Click the Save in the navigation area to save the configuration.

Table 2-10 the items of the PoE Interface Configuration

Item	Description
Enable/Disable	Enable/diable PoE for the PoE Interface.
Status	Display the status of the PoE interface.
Reason	The reason that the port cannot be powered. Short：short load，management: Insufficient power
Class	PD Classification
Icut	Current consumed by the PD
Power	Power consumption of the PD

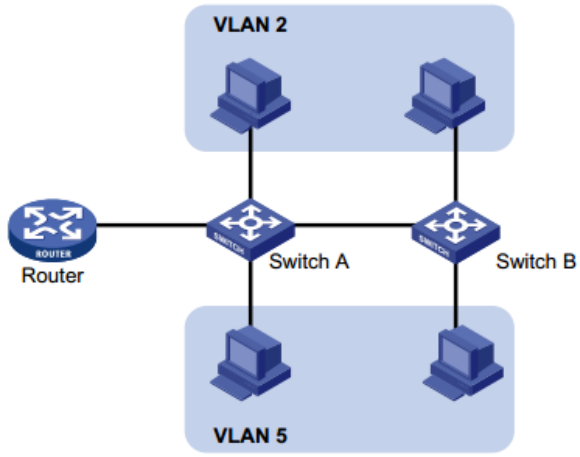
3 L2-Swtich

3.1 VLAN

3.1.1 Introduction

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared, collisions and excessive broadcasts are common on an network. To address the issue, virtual LAN (VLAN) was introduced. The idea is to break a LAN down into separate VLANs, that is, Layer 2 broadcast domains whereby frames are switched between ports assigned to the same VLAN. VLANs are isolated from each other at Layer 2. A VLAN is a bridging domain, and ll broadcast traffic is contained within it, as shown in Figure 3-1.

Figure 3-1 A VLAN diagram



A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same LAN, regardless of their physical locations. VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. For hosts in different VLANs to communicate, routers or Layer 3 switches are required.

- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

You can create VLANs based on:

- Port
- MAC address
- Protocol
- IP subnet
- Policy
- Other criteria

Because the Web interface is available only for port-based VLANs, this chapter introduces only port-based VLANs.

3.1.1.1 VLAN Mode

Depending on the tag handling mode, the VLAN Mode of a port can be one of the following three:

- Access :

An access port belongs to only one VLAN and usually connects to a user device.

- Trunk :

A trunk port can join multiple VLANs to receive and send traffic for them. It usually connects to a network device.

- Hybrid :

A hybrid port can join multiple VLANs to receive and send traffic for them. It can connect either a user device or a network device.

A hybrid port is different from a trunk port in that:

- A hybrid port allows traffic of multiple VLANs to pass through untagged.
- A trunk port allows only traffic of the default VLAN to pass through untagged.

3.1.1.2 Port link type

By default, VLAN 1 is the default VLAN for all ports. However, you can change the default VLAN for a port as required. When doing that, follow these guidelines:

- Because an access port can join only one VLAN, its default VLAN is the VLAN to which it belongs and cannot be configured.
- Because a trunk or hybrid port can join multiple VLANs, you can configure a default VLAN for the port.

3.1.1.3 Frame handling methods

Table 3-1 A port configured with a default VLAN handles a frame as follows:

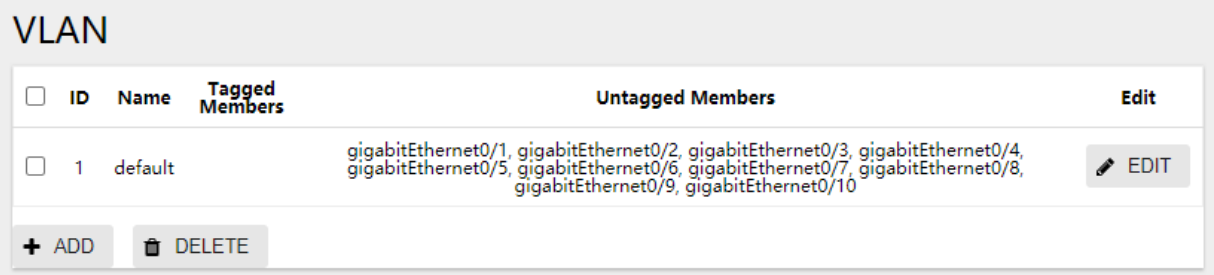
<table>
<tr><th rowspan="2">Port type</th><th colspan="2">Actions (in the inbound direction)</th><th rowspan="2">Actions (in the outbound direction)</th></tr>
<tr><th>Untagged frame</th><th>Tagged frame</th></tr>
<tr><td>Access</td><td>Tag the frame with the default VLAN tag.</td><td>• Receive the frame if its VLAN ID is the same as the default VLAN ID
• Drop the frame if its VLAN ID is different from the default VLAN ID.</td><td>Remove the default VLAN tag and send the frame.</td></tr>
<tr><td>Trunk</td><td rowspan="2">Check whether the default VLAN is carried on the port :
• If yes, tag the frame with the default VLAN tag.
• If not, drop the frame.</td><td rowspan="2">• Receive the frame if its VLAN is carried on the port.
• Drop the frame if its VLAN is not carried on the port.</td><td>• Remove the tag and send the frame if the frame Carries the default VLAN tag.
• Send the frame without removing the tag if its VLAN is carried on the port but is different from the default one.</td></tr>
<tr><td>Hybrid</td><td>Send the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration.</td></tr>
</table>

3.1.2 Configuring a VLAN

3.1.2.2 Creating a VLAN

1. Select L2 Switch > VLAN in the navigation area. The system automatically enters the page as shown in Figure 3-2.

Figure 3-2 VLAN configuration page



2. Click Add to enter the page for creating a VLAN, as shown in Figure 3-3. Table 3-2 describes the configuration items of creating a VLAN.

3. Type number into the ID box, select the Tagged Members to be assigned to these VLAN.

Figure 3-3 Create a VLAN

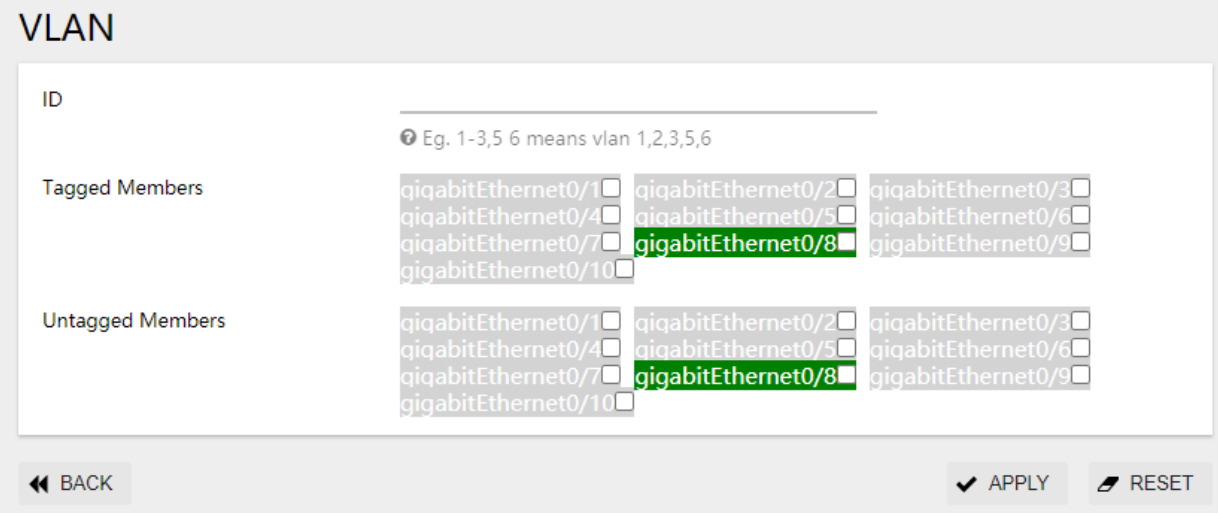


Table 3-2 Vlan configuration items

Item	Description
ID	This field displays the ID of the VLAN
name	By default, the description string of a VLAN is its VLAN ID, such as VLAN 0002.
Tagged Members	Indicates that the port sends the traffic of the VLAN without removing the VLAN tag.

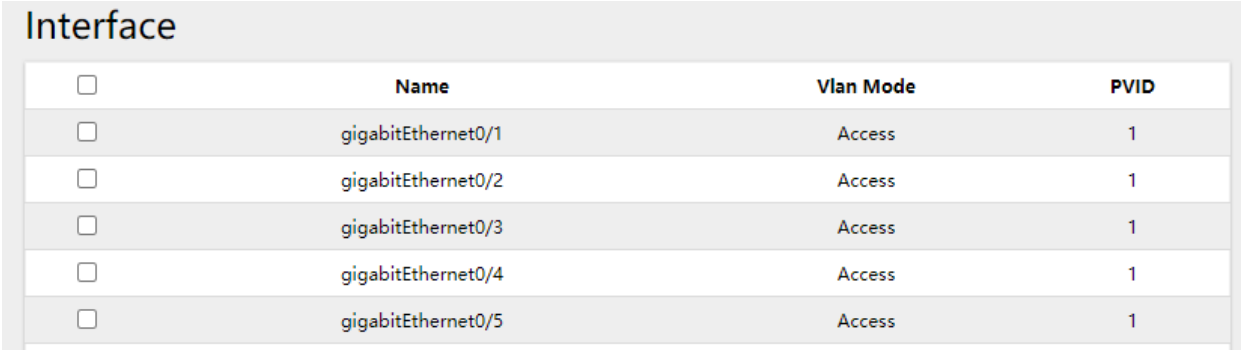
Untagged Members	Indicates that the port sends the traffic of the VLAN with the VLAN tag removed
Edit	Click to enter the VLAN editing page
Add	Click to enter the VLAN adding page
Delete	Select the VLAN ID, click to delete

4. Click the Save in the navigation area to save the configuration.

3.1.2.3 Configuring an interface

1. Select L2 Switch > VLAN > Interface in the navigation area. The system automatically enters the page as shown in Figure 3-4.

Figure 3-4 Interface page



2. Check the box in front of the ports to be configured, click Edit to enter the interface configuration page, as shown in Figure 3-5. Table 3-3 describes the configuration items of configuring a VLAN.

3. Configure the Vlan Mode, PVID, click Apply.

Figure 3-5 Interface configuration page

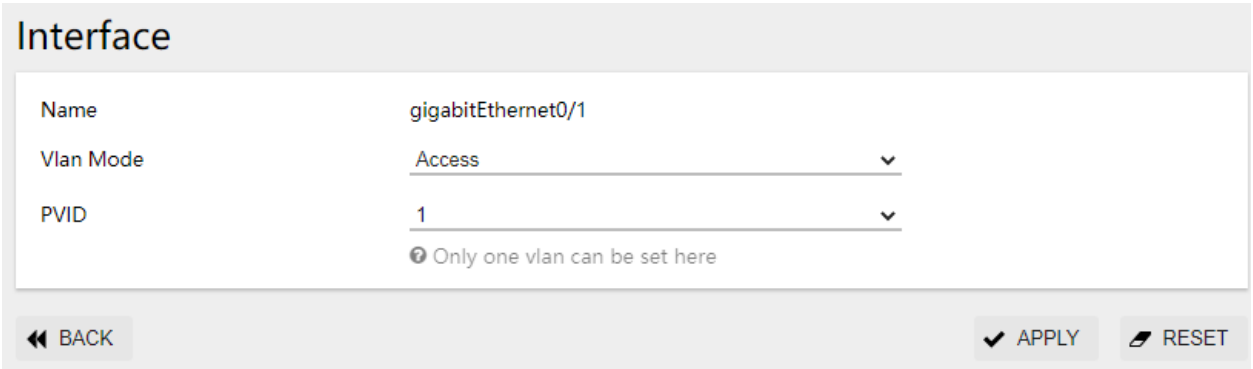


Table 3-3 The description of the Interface

Item		Description
Name		This field displays the port to be configured
VLAN Mode	Access	Sets the port' s VLAN Mode to access
	Trunk	Sets the port' s VLAN Mode to trunk
	Hybrid	Sets the port' s VLAN Mode to hybrid
PVID		Set the port' s default VLAN ID •The trunk ports at the two ends of a link must have the same PVID. Otherwise, the link cannot properly transmit packets
Native Vlan		VLAN (Native Vlan) , only exist in Trunk mode.

4. Click the Save in the navigation area to save the configuration.

3.2 QinQ

3.2.1 Overview

Introduction to QinQ

QinQ stands for 802.1Q in 802.1Q. QinQ is a flexible, easy-to-implement Layer 2 VPN technology based on IEEE 802.1Q. QinQ enables the edge device on a service provider network to insert an outer VLAN tag in the Ethernet frames from customer networks, so that the Ethernet frames travel across the service provider network (public network) with double VLAN tags. QinQ enables a service provider to use a single SVLAN to serve customers who have multiple CVLANs.

Background and benefits

The IEEE 802.1Q VLAN tag uses 12 bits for VLAN IDs. A device supports a maximum of 4094 VLANs. This is far from enough for isolating users in actual networks, especially in metropolitan area networks (MANs).

By tagging tagged frames, QinQ expands the available VLAN space from 4094 to 4094 × 4094. QinQ delivers the following benefits:

- Releases the stress on the SVLAN resource.
- Enables customers to plan their CVLANs without conflicting with SVLANs.

• Provides an easy-to-implement Layer 2 VPN solution for small-sized MANs or intranets.

• Allows the customers to keep their VLAN assignment schemes unchanged when the service provider upgrades the service provider network.

3.2.2 QinQ configuration

Creating a QinQ rule

1. Select L2 Switch > QinQ in the navigation area. The system automatically enters the page as shown in Figure 3-6. Table 3-4 describes the items of configuring a QinQ rule.

Figure 3-6 QinQ overview

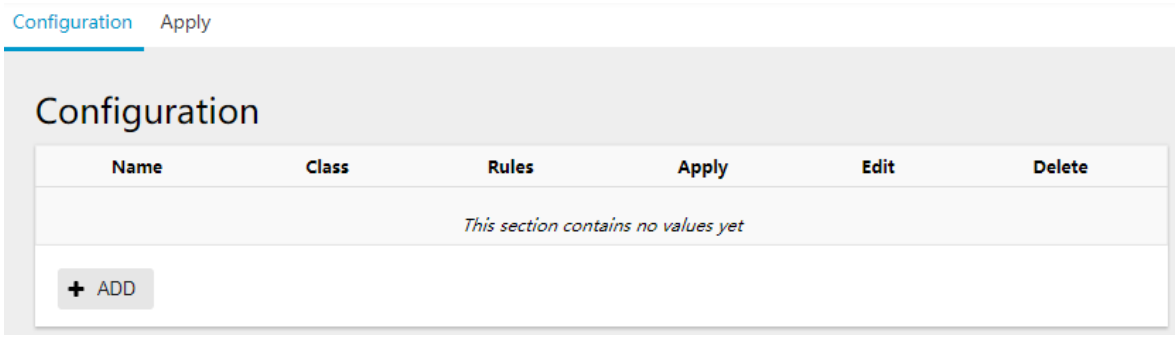


Table 3-4 The description of configuring a QinQ rule

Item	Description
Name	The name of QinQ rules
Class	QinQ category Stacking：Multi-layer tag mode Mapping：tag replacement mode
Rules	list of mapping rules
Apply	Application information of QinQ mapping
Edit	Click to eidt the QinQ rule
Delete	Click to delete the QinQ rule

2. Click Add to enter the page for creating a VPN rule, as shown in Figure 3-7. Table 3-5 describes the configuration items of creating a rule.

3. Type number into the Name, CVID, SVID box, click APPLY button.

Figure 3-7 Create a VLAN

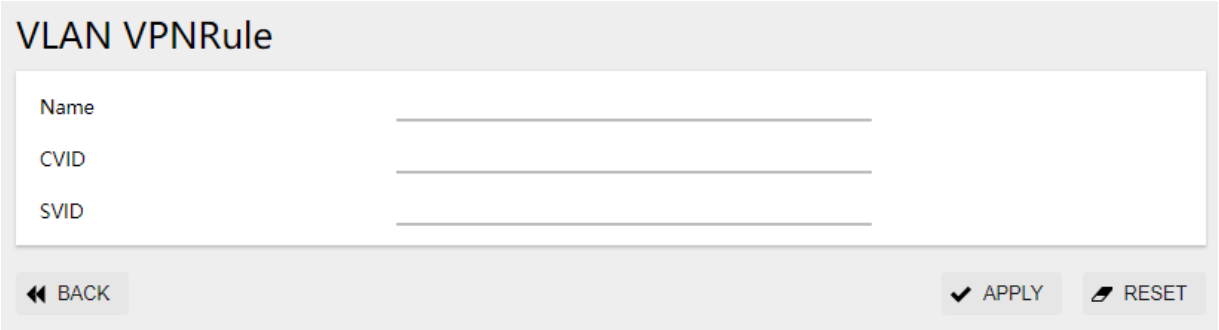


Table 3-5 Vlan configuration items

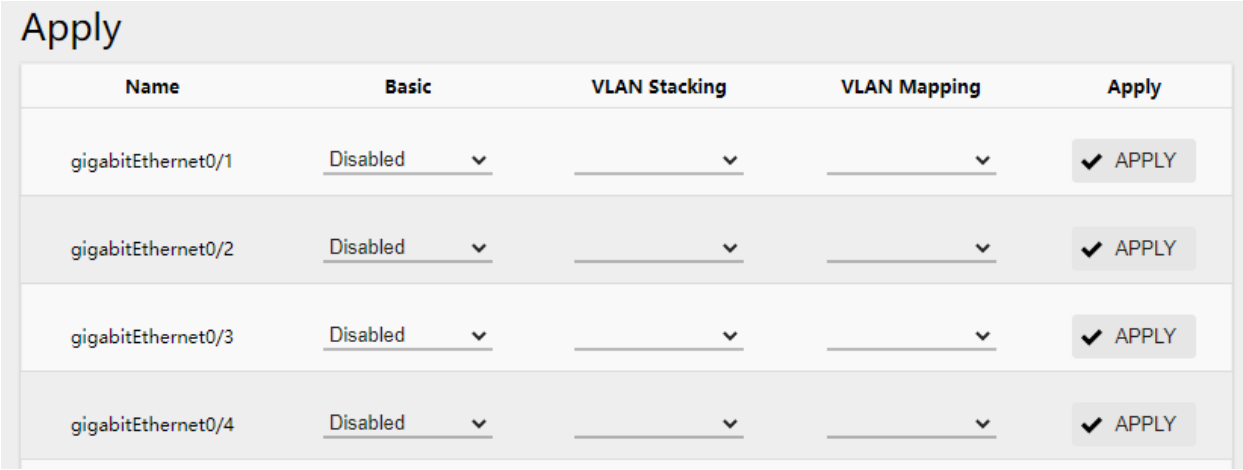
Item	Description
Name	The name of the VLAN VPNRule
CVID	The ID of the customer VLAN
SVID	The ID of the service provider VLAN

4. Click the Save in the navigation area to save the configuration.

Apply the rule to the interface

1. Select L2 Switch > QinQ > Apply in the navigation area. The system automatically enters the page as shown in Figure 3-8.

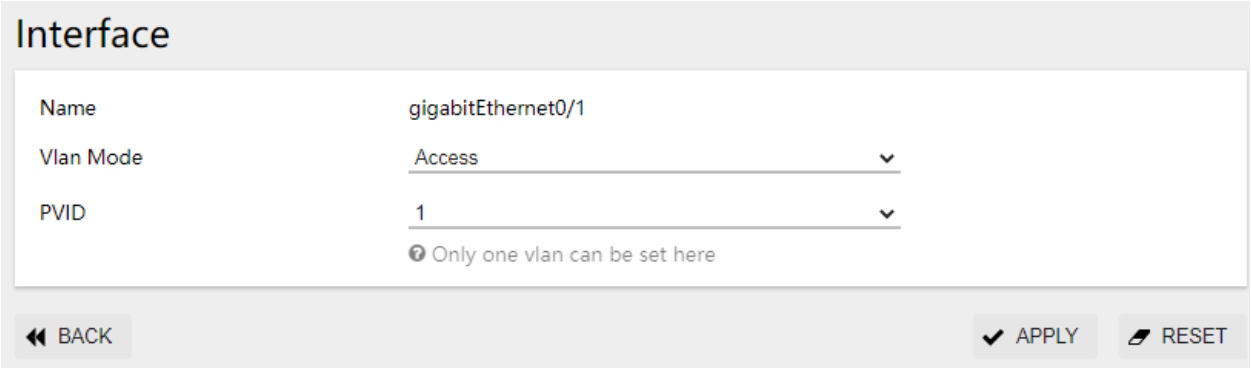
Figure 3-8 Interface page



2. Check the box in front of the ports to be configured, click Apply. to enter the interface configuration page, as shown in Figure 3-9.

3. Configure the Vlan Mode, PVID, click Apply.

Figure 3-9 Interface configuration page

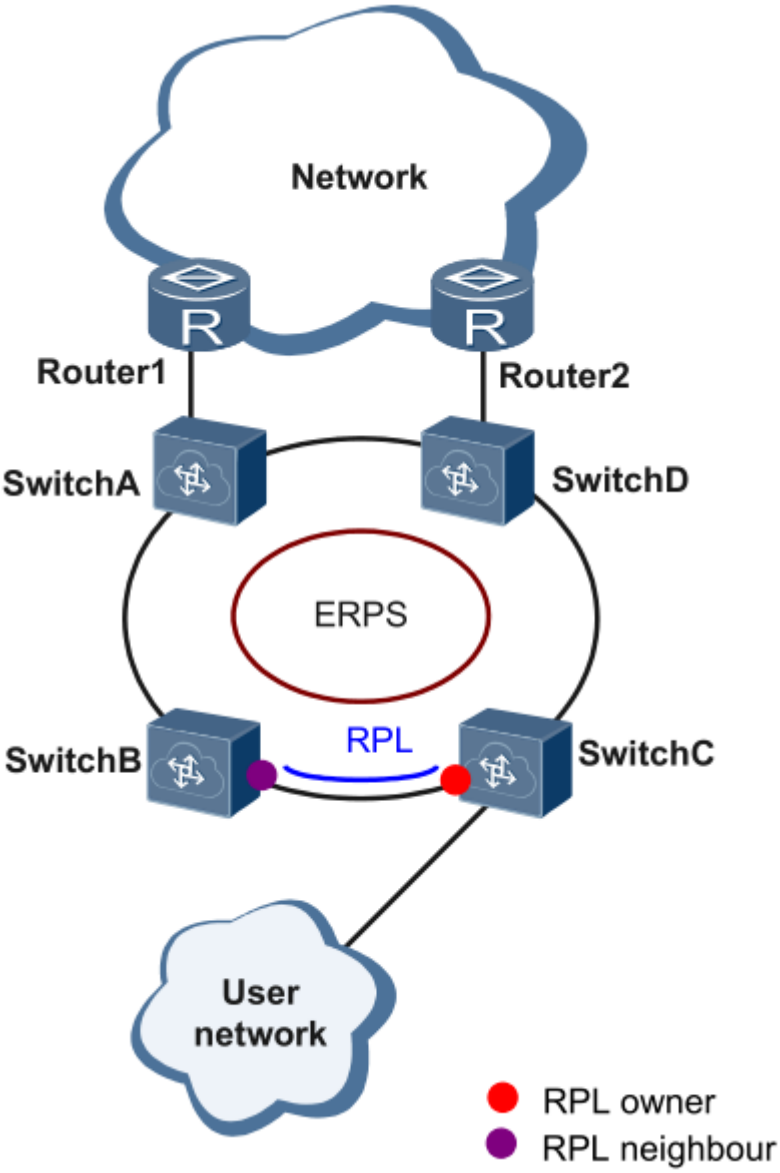


4. Click the Save in the navigation area to save the configuration.

3.3 ERPS

3.2.1 Overview

The ITU-T G.8032 ERPS feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.



Initial State

As the following figure, the devices on the ring have been configured, and all the link status is up. The RPL owner interface will be blocked by ERPS protocol to prevent loops. If a RPL neighbour interface is configured, it will also be blocked. Other interfaces are under the fordwarding state, can forward the traffic.

Link failure

When there is a link failure between SwitchD and SwitchE, the two interfaces on the link will be blocked by ERPS protocol, the RPL owner interface will be forwarded.

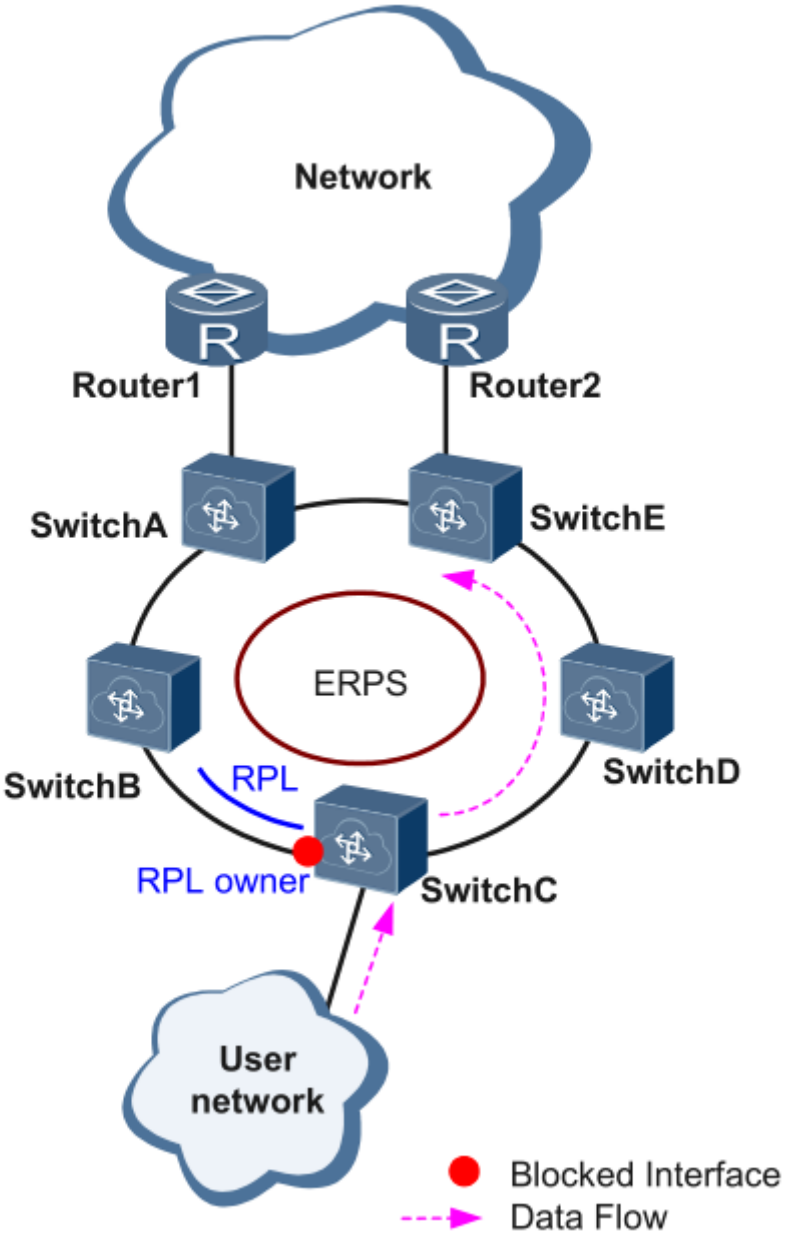
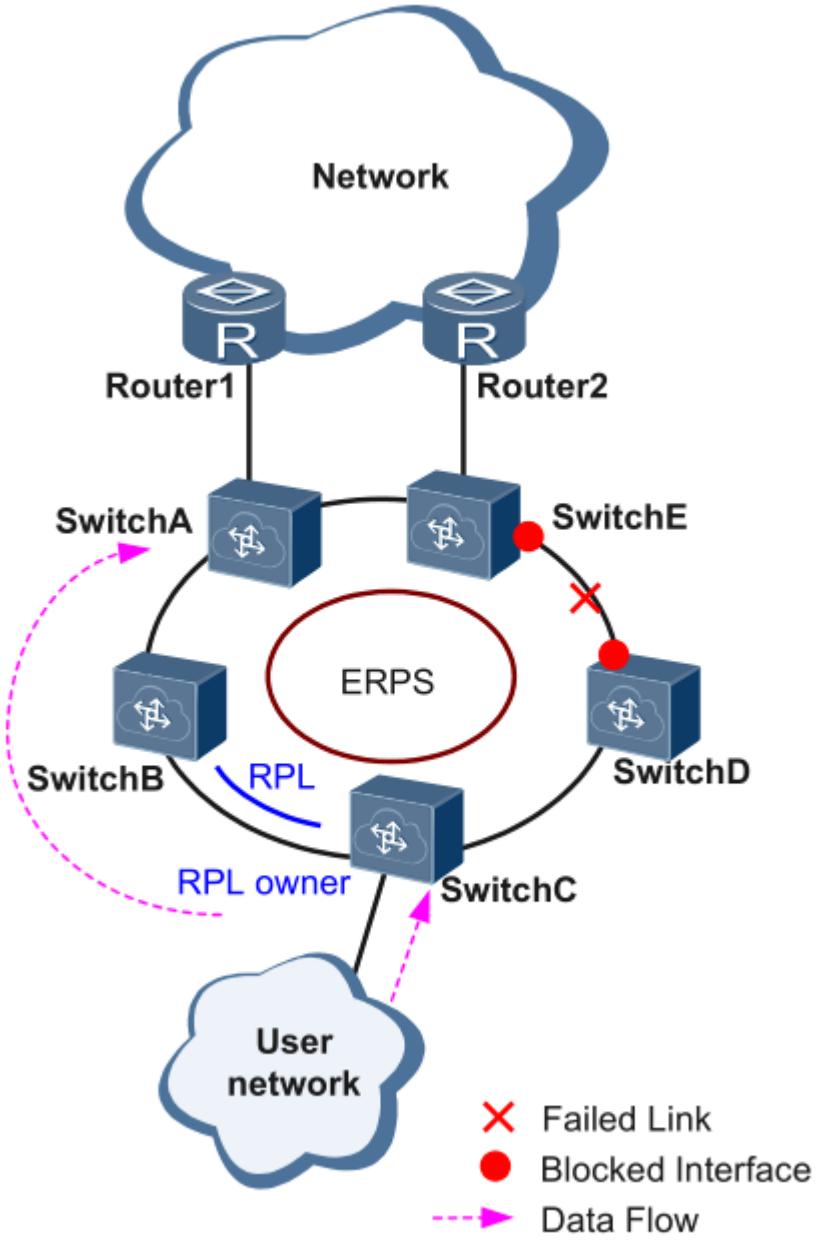


Figure 1 Link failure

Link restores

When the failure link is restored. When the erps ring is configured to revertive mode, the RPL owner interface will be blocked by ERPS protocol, the restored link will be configured to forwarding state to forward traffic.



Single-Ring :

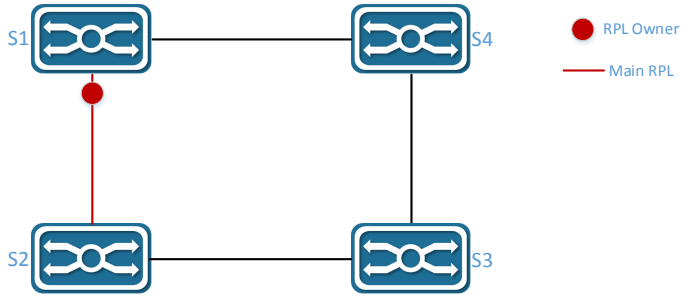
Only one ring in a network topology needs to be protected.

In Figure 3-10, the network topology has only one ring, only one ring protection link (RPL) owner node, and only one RPL. All nodes must belong to the same ring automatic protection switching (R-APS) virtual local area network (VLAN).

- All devices in the ring network must support ERPS.

- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-10 ERPS single ring



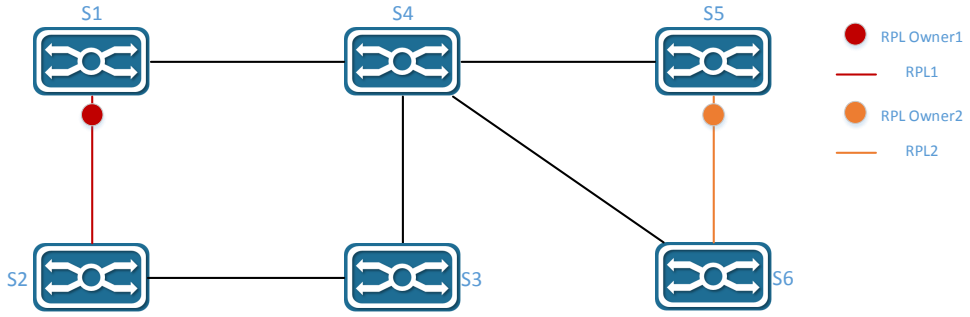
Tangent Rings :

The two rings in a network topology that share one device need to be protected.

In Figure 3-11, the two rings in the network topology share one device. Each ring has only one PRL owner node and only one RPL. The two rings belong to different R-APS VLANs.

- All devices in the ring network need to support ERPS.
- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-11 ERPS Tangent Rings



Intersecting Rings :

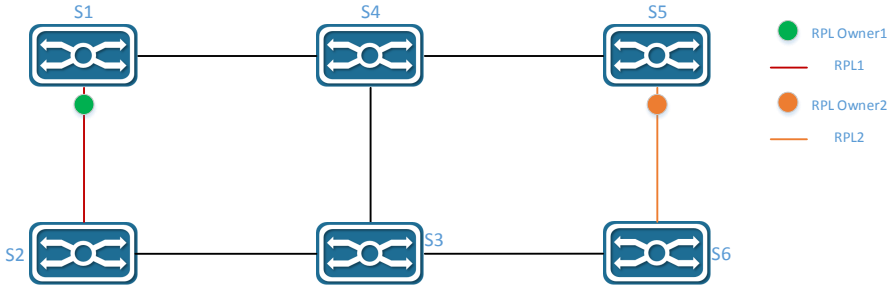
Two or more rings in a network topology share one link. (Each link between intersecting nodes must be a direct link without any intermediate node.)

In Figure 3-12, four rings exist in the network topology. Each ring has only one PRL owner node and only one RPL. The four rings belong to different R-APS VLANs.

- All devices in the ring network need to support ERPS.

- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-12 ERPS Intersecting Rings



3.2.3 Configure the ERPS

3.2.3.1 ERPS summary

Select L2 Switch > ERPS in the navigation area to enter the erps summary page as shown in Figure 3-13, The description of the ERPS summary is described in Table 3-6.

Figure 3-13 ERPS Summary Page

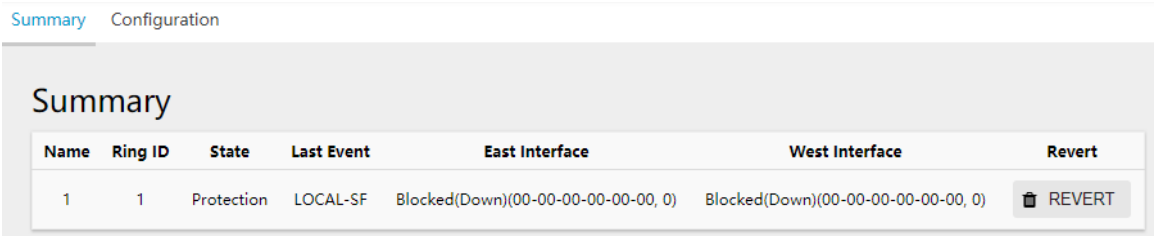


Table 3-6 ERPS ring description

Item	Description
Name	The name of the ERPS ring
Ring ID	The number of the ERPS ring
State	ERPS ring status, include： Idle： Stable state when all non-RPL links are available. In this state, the owner node blocks the RPL port and periodically sends NR-RB packets. The neighbor node blocks the RPL port. All nodes enter the idle state after the owner node enters the idle state. Pending： Transient state between the previous states Protection：

	State when a non-RPL link is faulty. In this state, the RPL link is unblocked to forward traffic. All nodes enter the protection state after a node enters the protection state.
Last Event	Recent state event RAPS-NR : remote failure recovery RAPS-NR-RB: remote switchback RAPS-SF : remote fault LOCAL-SF : local fault LOCAL-CLEAR-SF : local failure recovery WTR-EXP : local switchback
East Interface	The east interface of the ERPS ring
West Interface	The west interface of the ERPS ring
Revert	When the faulty link is restored, you can choose to manually revert immediately, otherwise the system will automatically revert after 5 minutes.

3.2.3.2 ERPS ring configuration

1. Select L2 Switch > ERPS > Configration > ERPS Ring Configuration, click +Add to to create erps ring, as shown in Figure 3-14. The description of the ERPS Ring Configuration is described in Table 3-7.

Figure 3-14 ERPS Ring Configuraiton

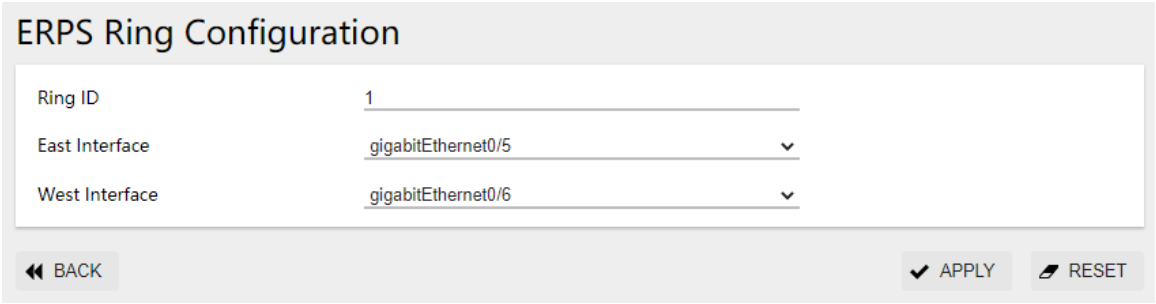
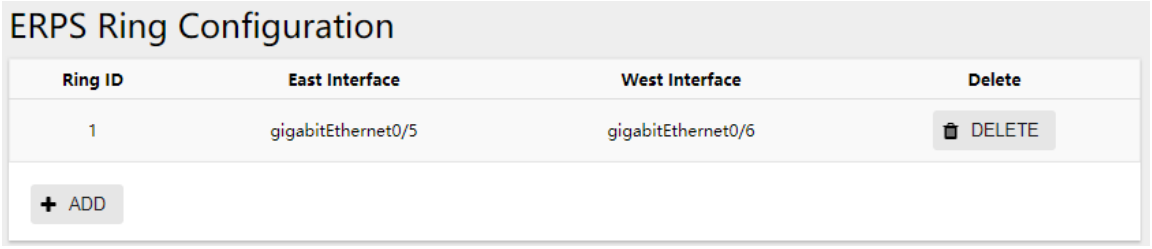


Table 3-7 Description of ERPS Ring

Item	Description
Ring ID	Can be any number. The ring number of each ERPS ring must be unique.
East Interface	Specify a port of the switch as the east port
West Interface	Specify a port of the switch as the west port

2. Click the Apply button, and the returned page is shown in Figure 3-15.

Figure 3-15 ERPS Ring Configuraiton



3.2.3.3 ERPS instance configuration

Select L2 Switch > ERPS > Configration > ERPS Instance Configuration, click +Add to create an erps instance, as shown in Figure 3-16. The description of the ERPS Instance Configuration summary is described in Table 3-8.

Figure 3-16 ERPS Instance Configuration

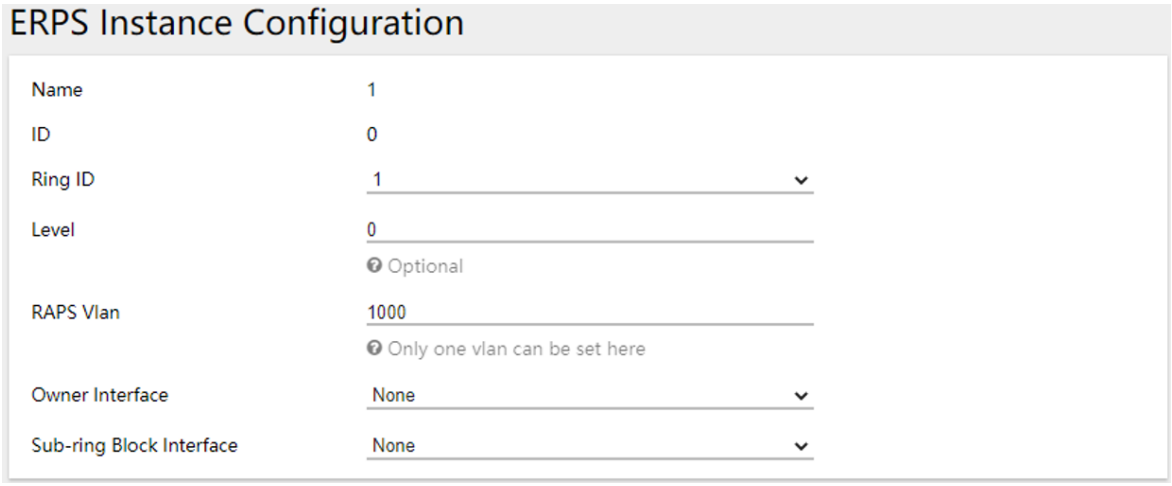


Table 3-8 Description of the ERPS Instance Configuration

Item	Description
Name	Instance name, in string format, unique, such as '1' or 'aa'
ID	Configure the VLAN Instance protected by the ERPS instance. By default, all VLANs belong to Instance 0. The default id is 0.
Ring ID	The associated ring ID must be the ring that has been created.
Level	ERPS priority, default is 0
RAPS VLAN	Each switch in the same ring must be configured with the same RAPS management VLAN for transmitting ERPS protocol packets. The RAPS management VLAN can be a virtual VLAN and needs to be distinguished from the data VLAN. It does not need to be created.
Ownerinterface	ERPS Owner interface can select either the east interface or the west

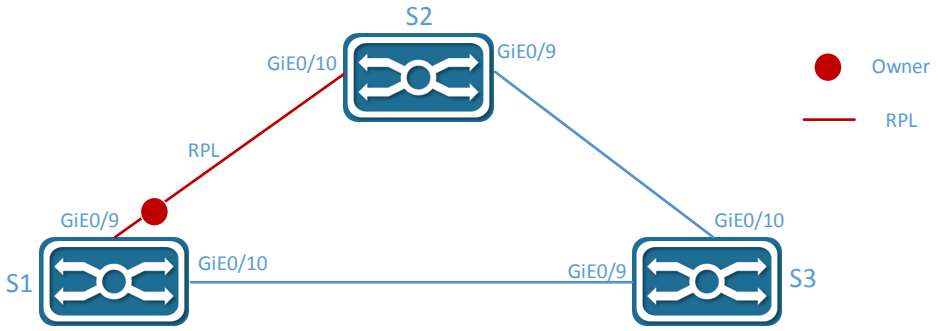
	interface as the Owner node. Each ERPS ring has one and only one interface configured as an RPL owner interface that controls the ports that need to be blocked.
Sub-ring Block Interface	The sub-ring blocked interface, one subring has only one blocking port. You can choose east or west. This parameter needs to be configured only for the tangent ring. The sub-rings of the two devices with tangent to the ring must be configured with the sub-ring blocking port.
Attached Instance	It only needs to be set when the sub-ring blocking port needs to be configured, and is set to the ring ID that is tangent to the current sub-ring.

3.2.4 Single-ring configuration example

Network Requirements:

In Figure 3-17, switches make up a ring network. Data traffic VLAN is 1-3. The backup link by default is between SWITCH 1 and SWITCH 2. If any link is failure, the network can recover quickly by forwarding the backup link.

Figure 3-17 ERPS network diagram

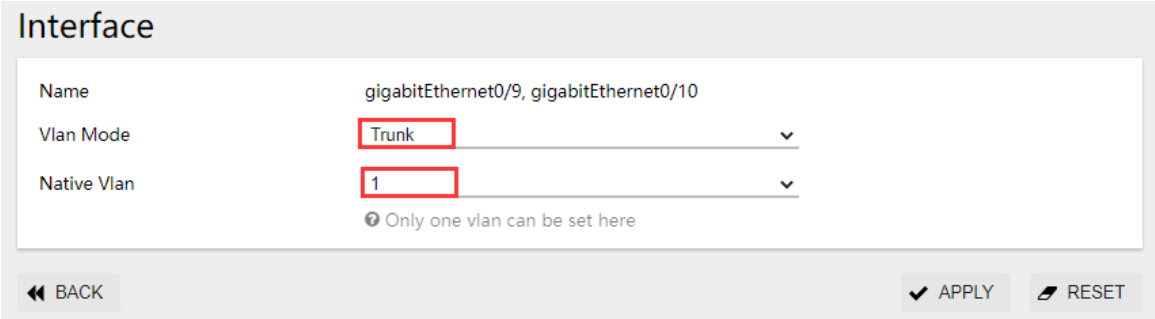


3.2.4.1 Configure Device S1

1. Configure the ports as trunk ports.

Select L2 Switch > VLAN > Interface, select gigabitEthernet0/9 and gigabitEthernet0/10, click Edit button to enter the interface configuration page. As shown in Figure 3-18, configure the Vlan mode of gigabitEthernet0/9 and gigabitEthernet0/10 in the Ethernet ring, Native Vlan is the default value 1.

Figure 3-18 Interface configuration page



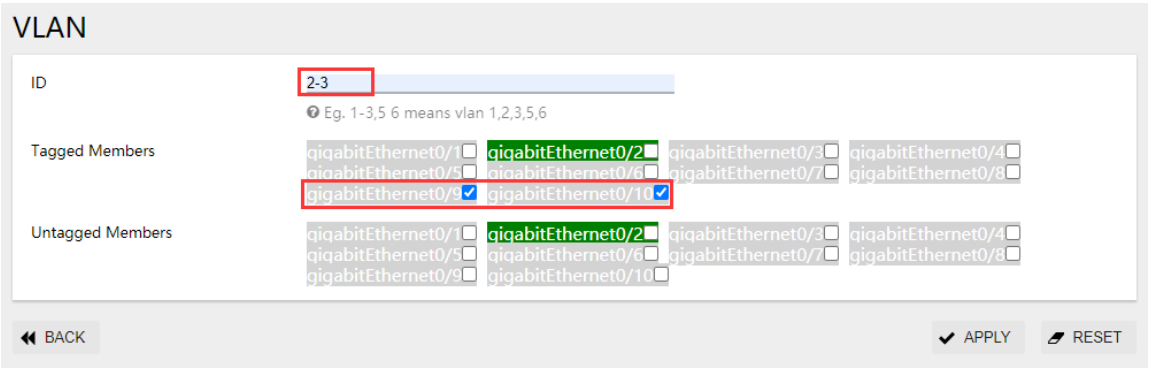
Click the Apply button, and the returned page is shown in Figure 3-19.

Figure 3-19 Interface page

2. Creating VLAN2 and VLAN3, select gigabitEthernet0/9 and gigabitEthernet0/10 to be assigned to these VLAN.

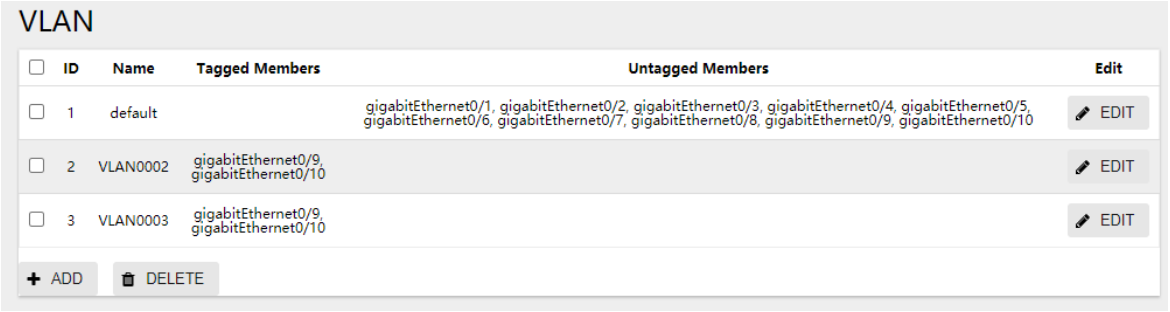
Select L2 Switch > VLAN, click Add button to enter the VLAN created page, as shown in Figure 3-20, type ‘2-3’ in the ID box, check the gigabitEthernet0/9 and gigabitEthernet0/10 box.

Figure 3-20 Creating VLAN2 and VLAN3



Click the Apply button, and the returned page is shown in Figure 3-21.

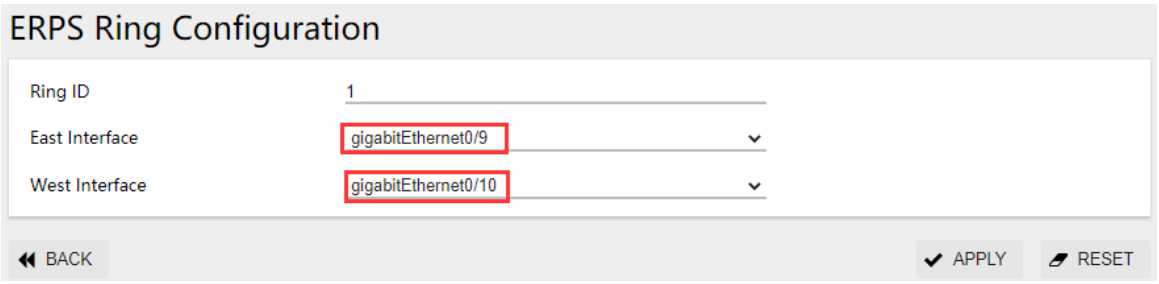
Figure3-21 VLAN page



3. Creating ERPS Ring

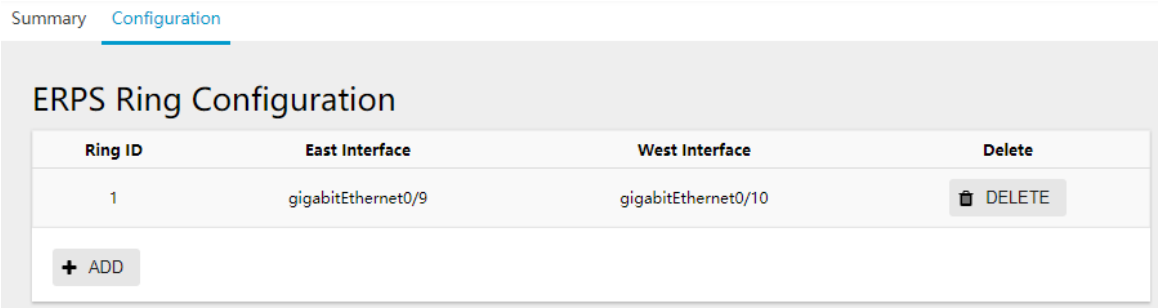
Select L2 Switch > ERPS > Configuration > ERPS Ring Configuration, click [+Add] button to enter the ERPS Ring Configuration page, as shown in Figure 3-22. Configure the Ring ID ‘1’, East Interface ‘gigabitEthernet0/9’, West Interface gigabitEthernet0/10.

Figure 3-22 ERPS Ring Configuration Page



Click the Apply button, and the returned page is shown in Figure 3-23.

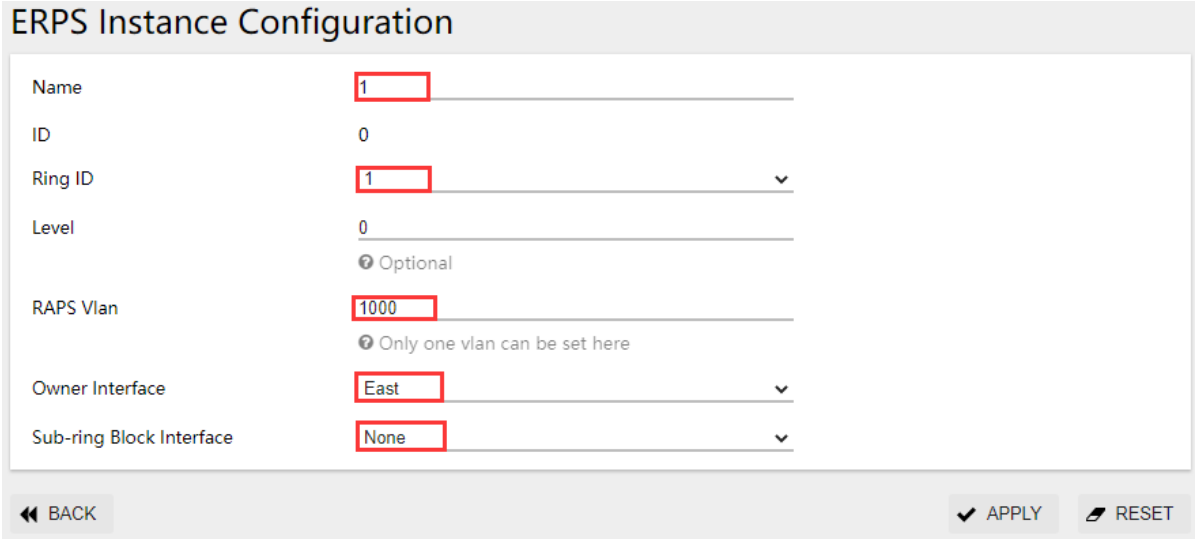
Figure 3-23 ERPS Ring 1 of Switch A



4. Creating ERPS Instance, configure Instance Name, Ring ID and other parameters.

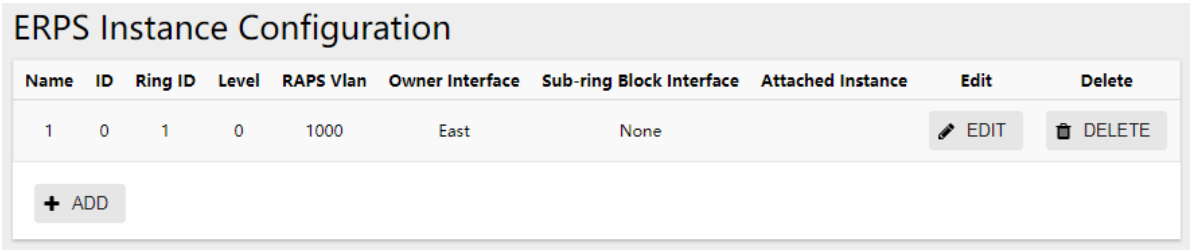
Select L2 Switch > ERPS > Configuration > ERPS Instance Configuration, click +Add button to enter the ERPS Instance Configuration page, As shown in Figure 3-24. Configure the Name ‘1’, Ring ID ‘1’, Level ‘0’, RAPS Vlan ‘1000’, Owner Interface ‘East’, Sub-ring Block Interface ‘None’.

Figure 3-24 ERPS Instance Configuration Page



Click the Apply button, and the returned page is shown in Figure 3-25.

Figure 3-25 ERPS Instance 1 of Switch 1



5. Click Save in the navigation area to save the configuration.

NOTE:

- In the case of a single ring, only one owner interface needs to be set. The device of owner interface is generally considered in the middle of the ring.

3.2.4.2 Configure Device S2 and S3

1. Configure the ports as trunk ports.

Select L2 Switch > VLAN > Interface, select gigabitEthernet0/9 and gigabitEthernet0/10, click Edit button to enter the interface configuration page. Configure the Vlan mode of gigabitEthernet0/9 and gigabitEthernet0/10 in the Ethernet ring, Native Vlan is the default value 1.

2. Creating VLAN2 and VLAN3, select gigabitEthernet0/9 and gigabitEthernet0/10 to be assigned to these VLAN.

Select L2 Switch > VLAN, click +Add button to enter the VLAN created page, type ‘2-3’ in the ID box, check the gigabitEthernet0/9 and gigabitEthernet0/10 box.

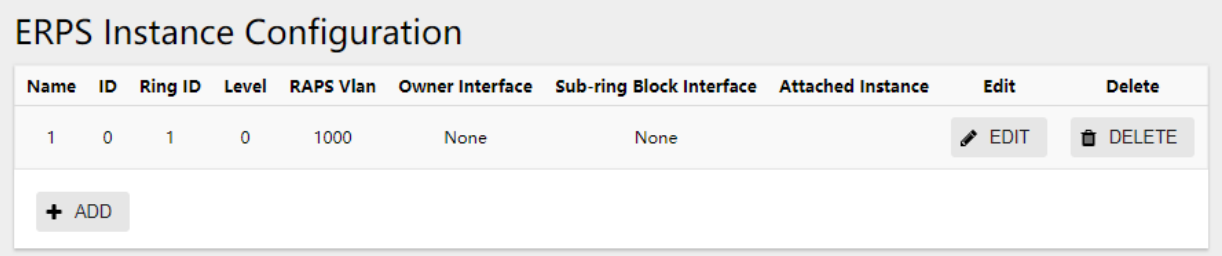
3. Creating ERPS Ring

Select L2 Switch > ERPS > Configuration > ERPS Ring Configuration, click +Add button to enter the ERPS Ring Configuration page. Configure the Ring ID ‘1’, East Interface ‘gigabitEthernet0/9’, West Interface gigabitEthernet0/10.

4. Creating ERPS Instance, configure Instance Name, Ring ID and other parameters.

Select L2 Switch > ERPS > Configuration > ERPS Instance Configuration, click +Add button to enter the ERPS Instance Configuration page, As shown in Figure 3-26. Configure the Name ‘1’, Ring ID ‘1’, Level ‘0’, RAPS Vlan ‘1000’, Owner Interface ‘None’, Sub-ring Block Interface ‘None’.

Figure 3-26 ERPS Instance 1 of Switch 2&3



5. Click Save in the navigation area to save the configuration

NOTE:

- Different from S1, S2 and S3 configure the Owner interface = None.

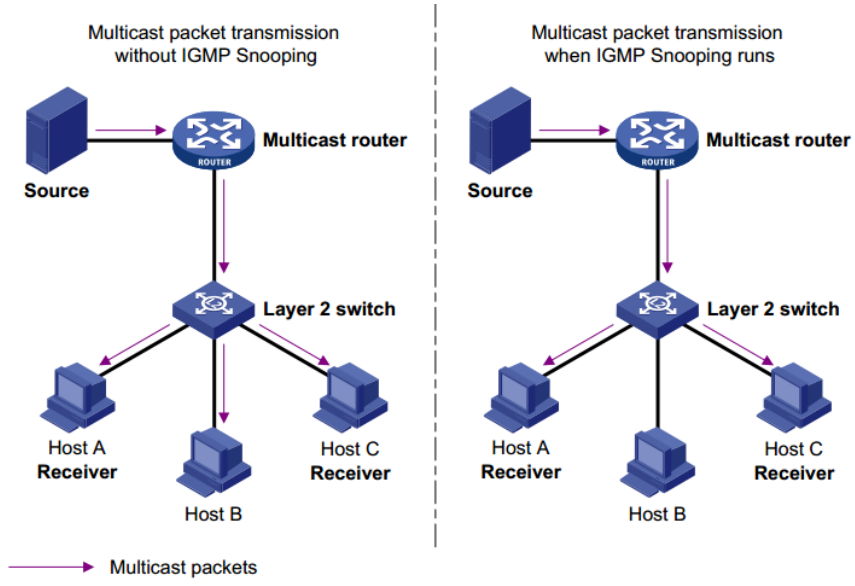
3.4 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

3.3.1 Principle of IGMP snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings. As shown in Figure 3-27, when IGMP snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. However, when IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

Figure 3-27 Multicast forwarding before and after IGMP snooping runs



3.3.2 Configure the IGMP Snooping

3.3.2.1 IGMP Snooping Summary

Select L2 Switch > IGMP Snooping > Summary in the navigation area to enter the summary page, as shown in Figure 3-28. Table 3-9 describes the IGMP snooping configuration items.

Figure 3-28 IGMP snooping summary

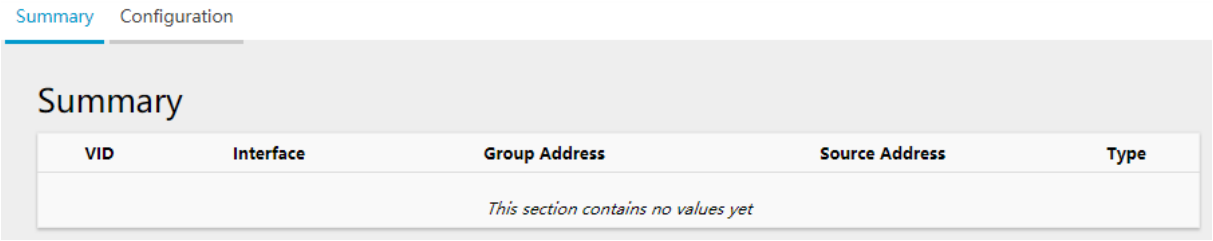


Table 3-9 IGMP snooping summary items

Item		Description
Summary	VID	VLAN ID
	Interface	Interface Name, where entry is learned from.
	Group Address	Group IP address.
	Source Address	Source IP address, for source specific group
	Type	Group type.

3.3.2.2 IGMP Snooping Global Configuration

1. Select L2 Switch > IGMP Snooping > Configuration > IGMP Snooping in the navigation area to enter the IGMP Snooping global configuration page shown in Figure 3-29. Table 3-10 describes the IGMP snooping configuration items.

2. Click the Enable/Disable button of 'IGMP Snooping' to enable/disable IGMP Snooping.

3. Click the Enable/Disable button of 'Discard Unknown Multicast' to enable/disable this function.

4. Click the Enable/Disable button of 'TC Suppression' to enable/disable this function.

Figure 3-29 IGMP Snooping Global Configuration

Table 3-10 IGMP snooping global configuration items

Item		Description
Name	IGMP Snooping	The global control for IGMP snooping.
	Discard Unknown Multicast	If this option is enabled, unknown multicast traffic will be dropped by switch.
	TC Suppression	If this option is enabled, topology change event will be ignored by switch

3.3.2.3 IGMP Mrouter Interface Configuration

1. Select L2 Switch > IGMP Snooping > Configuration > IGMP Mrouter Interface in the navigation area to enter the IGMP Mrouter Interface page shown in Figure 3-30. Table 3-11 describes the IGMP Mrouter Interface configuration items.

Figure 3-30 IGMP Mrouter Interface

Table 3-11 IGMP IGMP Mrouter Interface items

Item		Description
IGMP Mrouter Interface	VID	VLAN ID
	Interface	Interface Name.
	Delete	Click to delete this entry.

2. Click the +Add button to create an IGMP Mrouter Interface, as shown in Figure 3-31. Configure 'Vid', 'Name', click Apply.

Figure 3-31 Creating IGMP Mrouter Interface

3.3.2.4 IGMP Static Group Configuration

1. Select L2 Switch > IGMP Snooping > Configuration > IGMP Static Group in the navigation area to enter the IGMP Static Group page shown in Figure 3-32. Table 3-12 describes theIGMP Static Group configuration items.

Figure 3-32 IGMP Static Group

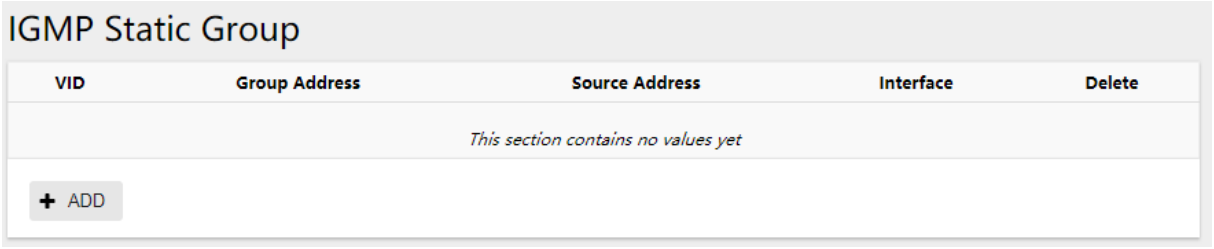
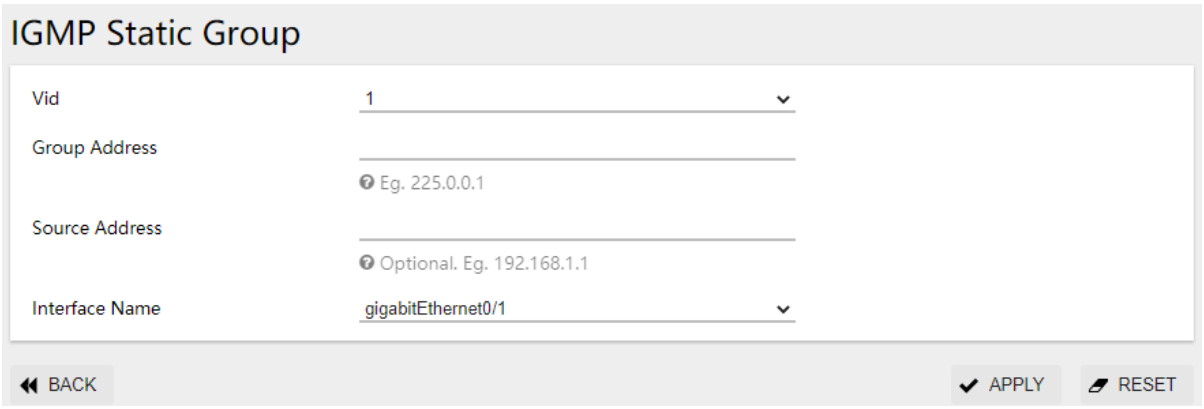


Table 3-12 IGMP IGMP Static Group items

Item		Description
IGMP Static Group	VID	VLAN ID
	Group Address	Group IP address
	Source Address	Source IP address
	Interface	Interface name.
	Delete	Click to delete this entry.

2. Click the +Add button to create an IGMP Static Group, as shown in Figure 3-33. Configure 'Vid', 'Group Address', 'Source Address', 'Interface Name', click Apply.

Figure 3-33 Creating IGMP Static Group



3.5 Spanning Tree

3.4.1 Overview

Spanning Tree Protocol (STP) is a Layer-2 management protocol. It cannot only selectively block redundant links to eliminate Layer-2 loops but also can back up links.

Like many protocols, STP is continuously updated from Rapid Spanning Tree Protocol (RSTP) to Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer-2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is completely compatible with 802.1D STP. Like traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes two times of the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP: Since all VLANs in a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be balanced among VLANs.
- MSTP, defined by the IEEE in 802.1s, resolves defects of STP and RSTP. It cannot only rapidly converge but also can enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

In general, STP/RSTP works based on ports while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

3.4.2 Spanning Tree Configuring

Display the Summary of the Spanning Tree

Select L2 Switch > Spanning Tree > Summary in the navigation area to enter the summary page, as shown in Figure 3-34. Table 3-13 describes the Spanning Tree Summary items.

Figure 3-34 Spanning Tree Summary Page

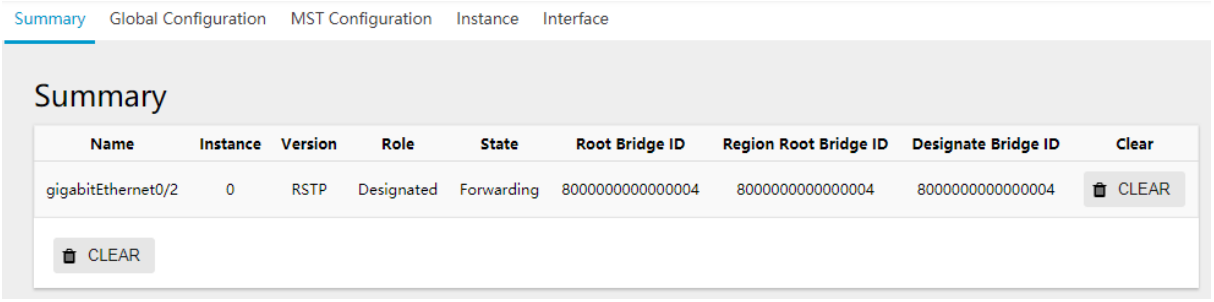


Table 3-13 Spanning Tree Summary items

Item		Description
Summary	Name	Interface name.
	Instance	Interface instance
	Version	Interface STP protocol version
	Role	Interface STP role
	State	Interface STP state
	Root Bridge ID	STP root bridge identity
	Region Root Bridge ID	MSTP region root bridge identity
	Designate Bridge ID	STP designate bridge identity
	Clear	Clear the protocol version and trigger a new negotiation

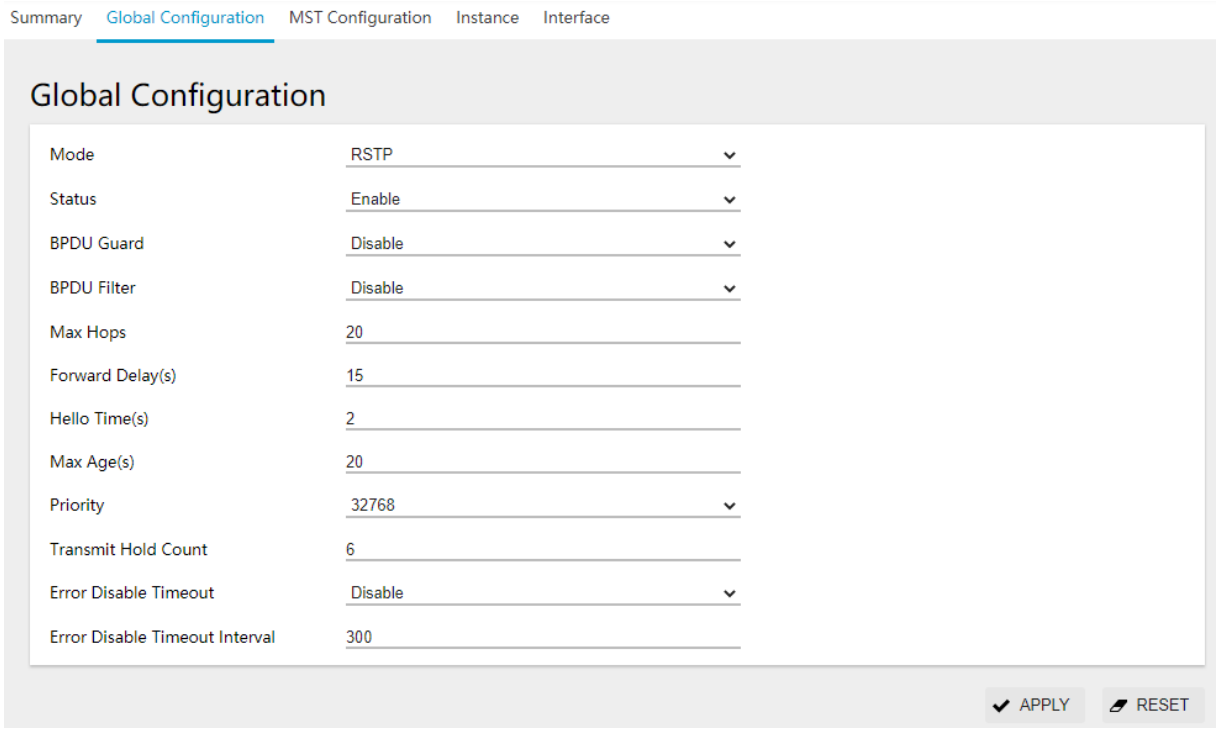
Configuring the Global Configuration

Select L2 Switch > Spanning Tree > Global Configuration in the navigation area to enter the Global Configuration page, as shown in Figure 3-35. Table 3-14 describes the Global Configuration items.

Table 3-14 Spanning Tree Summary items

Item		Description
Global Configuration	Mode	Set the working mode of STP, including STP, RSTP, and MSTP. STP: In STP mode, each port of the device sends STP BPDUs. RSTP: In RSTP mode, each port of the device will send out RSTP BPDUs. When it is connected to the device running STP, the port will automatically migrate to STP mode. MSTP: In MSTP mode, each port of the device sends MSTP BPDUs. When it is connected to the device running STP, the port is automatically migrated to work in STP mode.
	Status	Enable STP.
	BPDU Guard	Enable BPDU protection. Enable BPDU protection to prevent malicious attacks on the device and prevent network attacks.
	BPDU Filter	Enable BPDU filter
	Max Hops	Set the maximum hop count of the MST region. This parameter determines the size of the MST region. Only the parameters configured on the domain root will take effect in the domain, and the configuration on the non-domain root is invalid.
	Forward Delay	Set the delay time before an interface change to forwarding
	Hello Time	Hello timer interval
	Max Age	Set the maximum duration that messages are saved in the device
	Priority	Bridge priority
	Transmit Hold Count	Maximum number of BPDUs sent by the bridge per second
	Error Disable Timeout	Configuration error port auto disable function
	Error Disable Timeout Interval	Configuration error port is automatically disabled timeout.

Figure 3-35 Global Configuration Page



Configuring the MST Configuration

Select L2 Switch > Spanning Tree > MST Configuration in the navigation area to enter the MST Configuration page, as shown in Figure 3-36. Table 3-15 describes the MST Configuration items.

Figure 3-36 MST Configuration Page

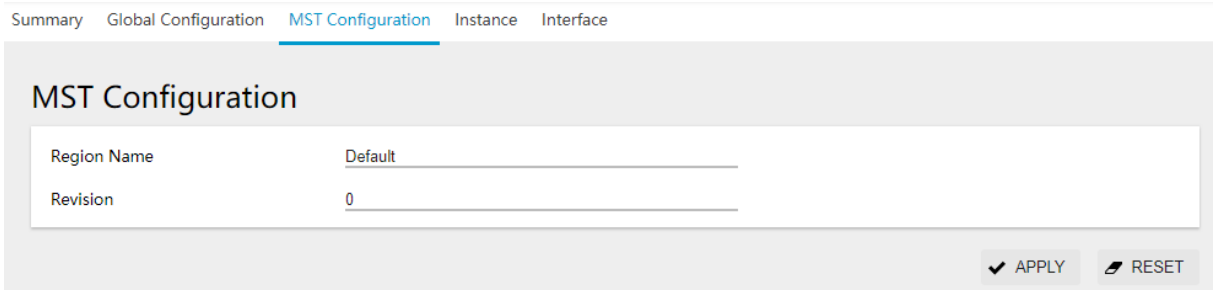


Table 3-15 Spanning Tree MST Configuration items

Item		Description
MST Configuration	Region Name	Set the domain name of the MST domain By default, the domain name of an MST region is Default.
	Revision	Set the revision level of the MST region

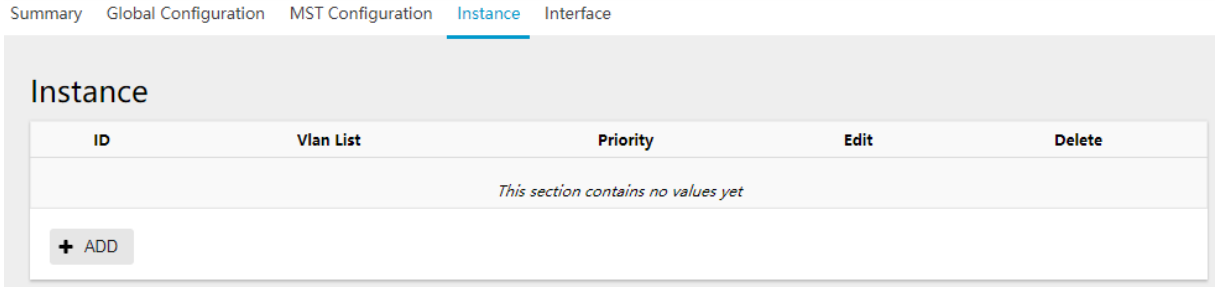
Configuring the Instance

Select L2 Switch > Spanning Tree > Instance in the navigation area to enter the Instance page, as shown in Figure 3-37. Table 3-16 describes the Instance items.

Table 3-16 Spanning Tree Instance items

Item		Description
Instance	ID	Instance ID
	VLAN List	Instance associated VLAN list
	Priority	Bridge priority in this instance
	Edit	Click to edit this entry
	Delete	Click to delete this entry

Figure 3-37 Spanning Tree Instance Page



Configuring the Interface

Select L2 Switch > Spanning Tree > Interface in the navigation area to enter the Interface page, as shown in Figure 3-38. Table 3-17 describes the Interface items.

Figure 3-38 Spanning Tree Interface Page

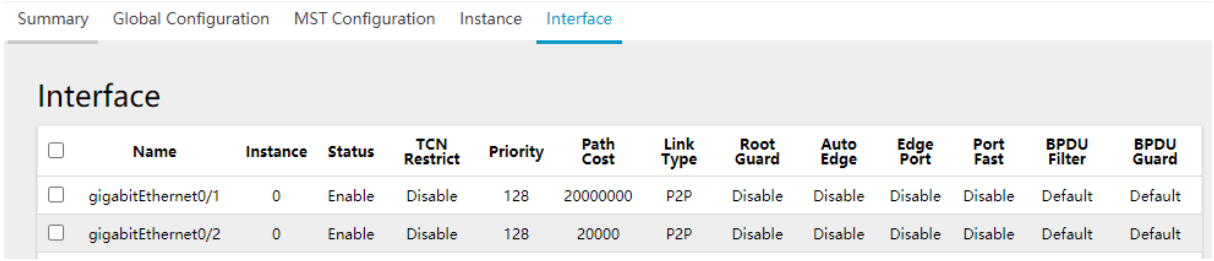


Table 3-17 Spanning Tree Interface items

Item		Description
Interface	Name	Interface name
	Instance	Interface’ s instance ID

Status	STP status
TCN Restrict	Configure the topology change notification packet suppression function.
Priority	Configuring interface priority
Path Cost	Configure interface path cost
Link Type	Configure interface link type
Root Guard	Configure the interface to enable root protection.
Auto Edge	Configure the interface to automatically recognize the function of the edge port.
Edge Port	Configure the interface as an edge port.
Port Fast	Configure the interface as a fast port.
BPDU Filter	Configure the interface to enable BPDU filtering.
BPDU Guard	Configure the interface to enable BPDU protection.

3.6 MAC Management

3.5.1 Overview

A device maintains a MAC address table for frame forwarding. Each entry in this table indicates the MAC address of a connected device, to which interface this device is connected and to which VLAN the interface belongs. A MAC address table consists of two types of entries: static and dynamic. Static entries are manually configured and never age out. Dynamic entries can be manually configured or dynamically learned and will age out.

Your device learns a MAC address after it receives a frame from a port, port A for example, as it executes the following steps.

1. Checks the frame for the source MAC address (MAC-SOURCE for example).

2. Looks up the MAC address table for an entry corresponding to the MAC address and do the following:

- If an entry is found for the MAC address, updates the entry.

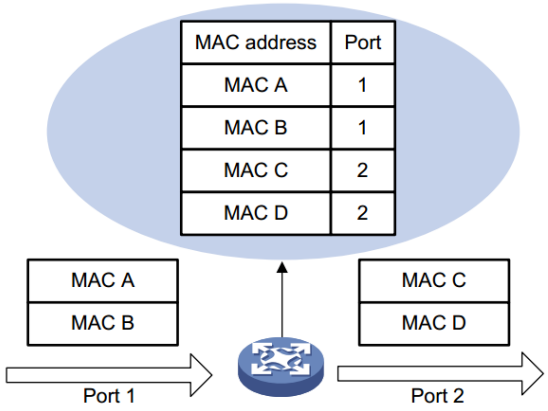
- If no entry containing the MAC address is found, adds an entry that contains the MAC address and the receiving port (port A) to the MAC address table.

3. After the MAC address (MAC-SOURCE) is learned, if the device receives a frame destined for MAC-SOURCE, the device looks up the MAC address table and then forwards the frame from port A.

When forwarding a frame, the device adopts the following forwarding modes based on the MAC address table:

- Unicast mode: If an entry matching the destination MAC address exists, the device forwards the frame directly from the sending port recorded in the entry.
- Broadcast mode: If the device receives a frame with the destination address being all Fs, or no entry matches the destination MAC address, the device broadcasts the frame to all the ports except the receiving port.

Figure 3-39 MAC address table of the device



3.5.2 Configuring MAC addresses

MAC addresses configuration includes the configuring and displaying of static MAC address, Filter MAC Address, and the setting of MAC address entry aging time.

Configuring a static MAC address

1. Select L2 Switch > MAC Mangement > Static MAC Address from the navigation area. The system automatically displays the Static MAC Address page, as shown in Figure 3-40.

2. Click +Add to enter the page for creating static MAC address, as shown in Figure 3-41. Table 3-18 shows the detailed configuration for creating a static MAC address.

3. Type in MAC address, for example ‘00eb.fc00.8877’, select the VID in the VLAN drop down list, select the Interface in the Interface drop list.

4. Click Apply to end the operation.

Figure 3-40 MAC static address page

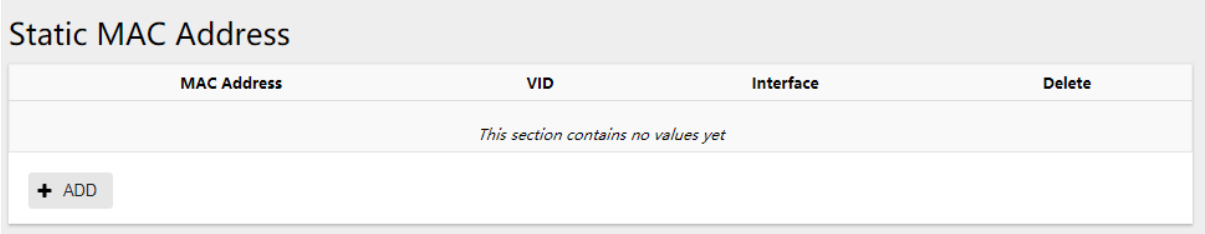


Figure 3-41 Creating static MAC address

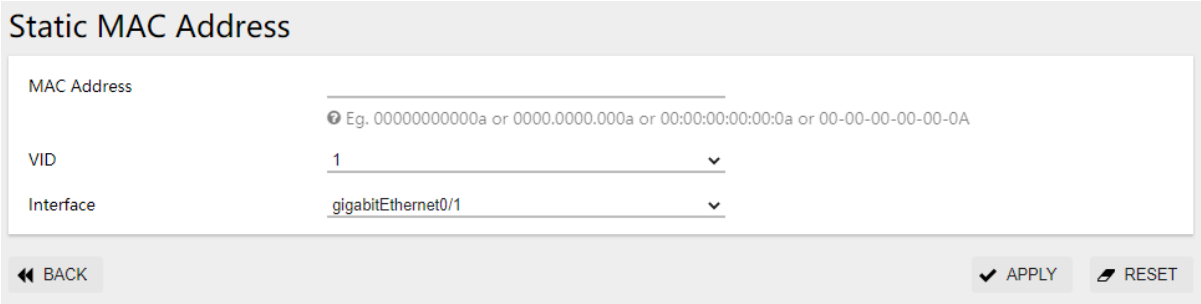


Table 3-18 Static MAC Address items

Item		Description
Static Mac Address	MAC Address	Set the MAC address to be added.
	VID	Sets the ID of the VLAN to which the MAC address belongs.
	Interface	Sets the port to which the MAC address belongs.

Configuring a Filter MAC address

1. Select L2 Switch > MAC Mangement > Filter MAC Address from the navigation area. The system automatically displays the Filter MAC Address page, as shown in Figure 3-42.

Figure 3-42 MAC static address page

2. Click +Add to enter the page for creating filter MAC address, as shown in Figure 3-43. Table 3-19 shows the detailed configuration for creating a fliter MAC address.

3. Type in MAC address, for example ‘00eb.fc00.8877’, select the VID in the VLAN drop down list.

4. Click Apply to end the operation.

Figure 3-43 Creating Filter MAC address

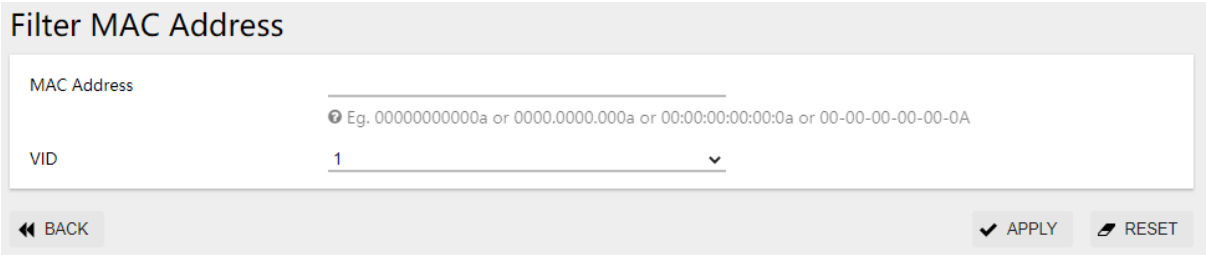


Table 3-19 Filter MAC Address items

Item		Description
Static Mac Address	MAC Address	Set the MAC address to be filtered.
	VID	Sets the ID of the VLAN to which the MAC address belongs.

Configuring MAC Aging Time

1. Select L2 Switch > MAC Mangement from the navigation area. The system automatically displays the Aging Times configuration page, as shown in Figure 3-44. Table 3-20 shows the detailed configuration of Ageing Times.

2. Type number in the Value box, for example ‘300’.

3. Click Apply to end the operation.

Figure 3-44 Ageing Times page

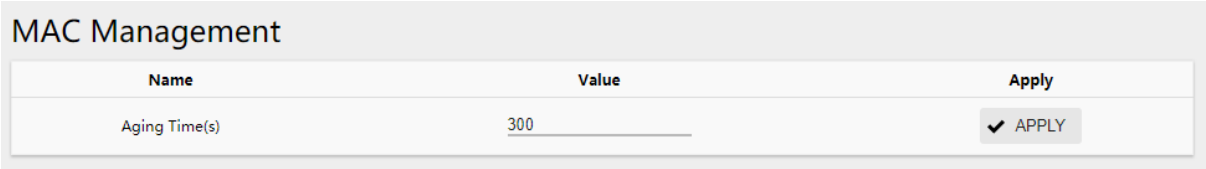


Table 3-20 Ageing Times items

Item		Description
Ageing Times	Value	Set the aging time for the MAC address, the default value is 300 seconds.
	Apply	Click to enable

3.5.3 MAC Address Configuration Examples

Network requirements:

It is required to add a static MAC address ‘000E.C6C1.C8AB’ under gigabitEthernet0/1 in VLAN 1, and filter the MAC address ‘000E.C6C1.C8CC’ in VLAN 10.

Configuration procedure

1. Create VLAN 10, Select L2 Switch > VLAN, click +Add button to enter the VLAN created page, type ‘10’ in the ID box.

2. Select L2 Switch > MAC Mangement > Filter MAC Address from the navigation area, and then click +Add. The page shown in Figure 3-45 appears.

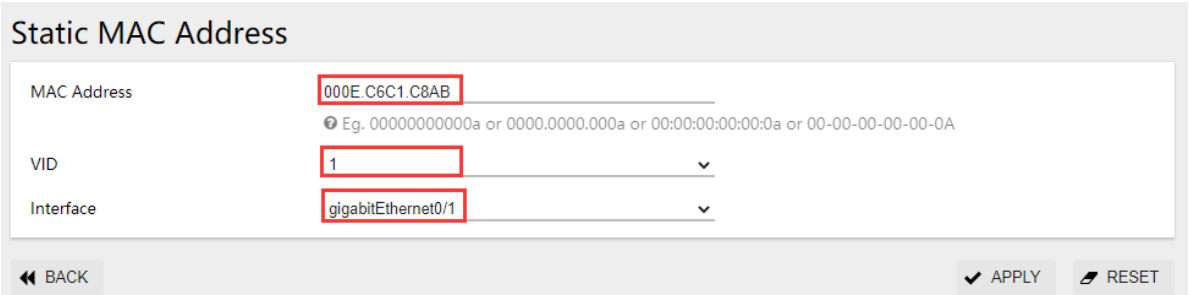
3. Type in MAC address ‘000E.C6C1.C8AB’.

4. Select ‘1’ in the VLAN drop down list.

5. Select ‘gigabitEthernet0/1’ in the Port drop down list.

6. Click Apply to end the operation.

Figure 3-45 Creating static MAC address



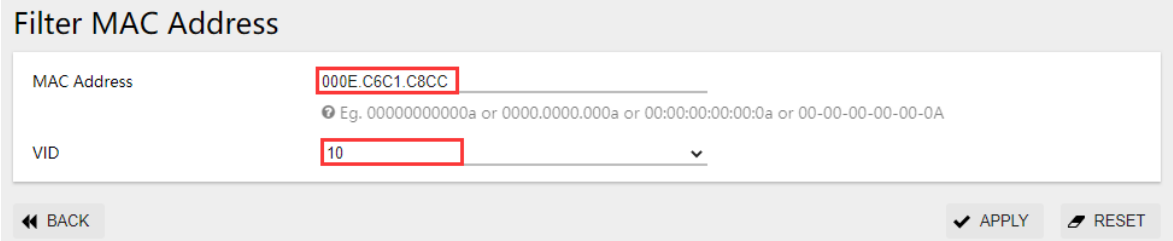
7. Select L2 Switch > MAC Mangement > Filter MAC Address from the navigation area, and then click +Add. The page shown in Figure 3-46 appears.

8. Type in MAC address ‘000E.C6C1.C8CC’ .

9. Select ‘10’ in the VLAN drop down list.

10. Click Apply to end the operation.

Figure 3-46 Creating Filter MAC address



11. Click the Save in the navigation area to save the configuration

3.7 LLDP

3.7.1 Overview

In a heterogeneous network, a standard configuration exchange platform ensures that different types of network devices from different vendors can discover one another and exchange configuration.

The Link Layer Discovery Protocol (LLDP) is specified in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices. Local device information includes its system capabilities, management IP address, device ID, port ID, and so on. The device stores the device information in LLDPDUs from the LLDP neighbors in a standard MIB. LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

3.7.2 Configuring LLDP

LLDP global Configuration

Select L2 Switch > LLDP > Global Configuration in the navigation area to enter the Global Configuration page, as shown in Figure 3-47. Table 3-21 describes the Global Configuration items.

Figure 3-47 LLDP Global Configuration

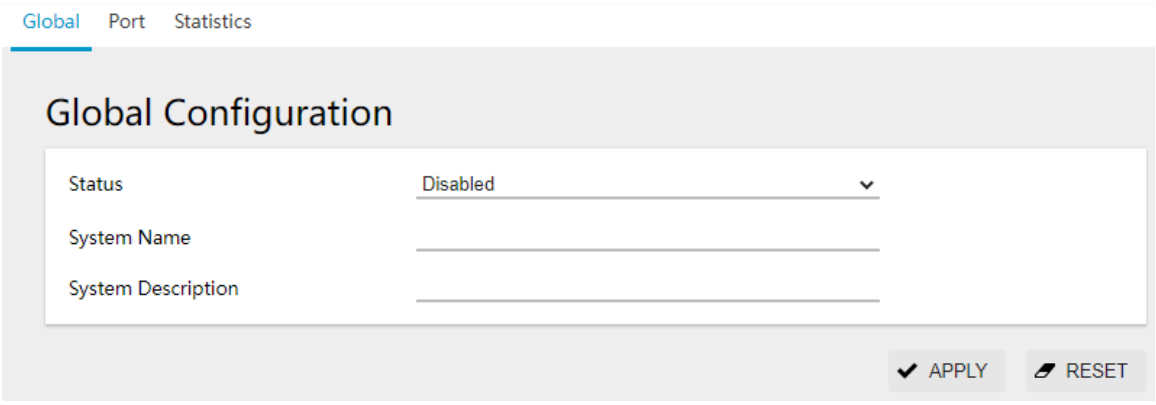


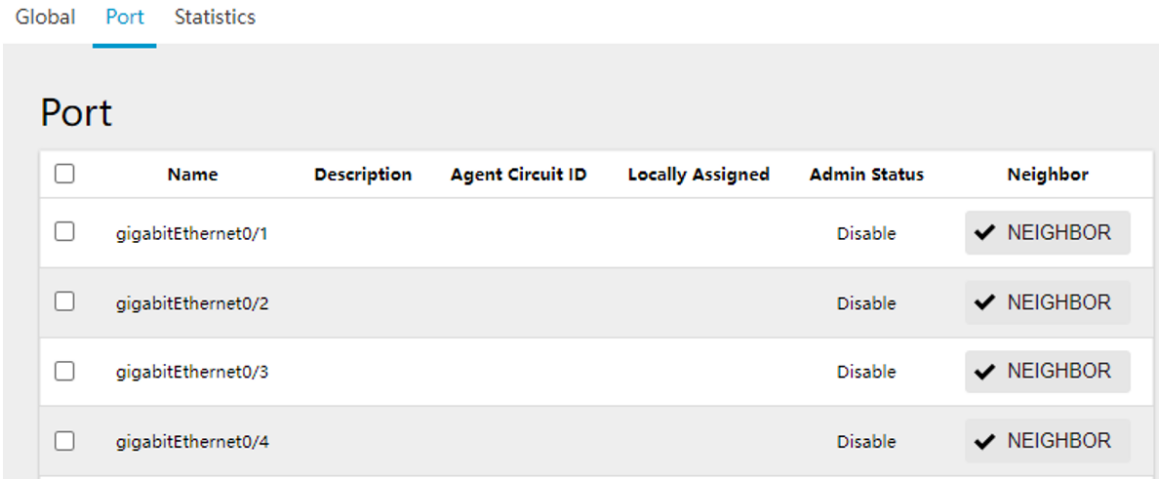
Table 3-21 LLDP Global Configuration Items

Item	Description
Status	Disabled: global enable off Enabled: global enable on
System Name	The name of the device, can be empty
System Description	Description of the system, can be empty

LLDP port setting

1. Select L2 Switch > LLDP > Port in the navigation area to enter the LLDP port status page, as shown in Figure 3-48.

Figure 3-48 LLDP port status



2. Select the interface to be configured, click Edit button to enter the page for configuring an interface, as shown in Figure 3-49. Table 3-22 describes the configuration items of configuring an interface.

Figure 3-49 LLDP port status

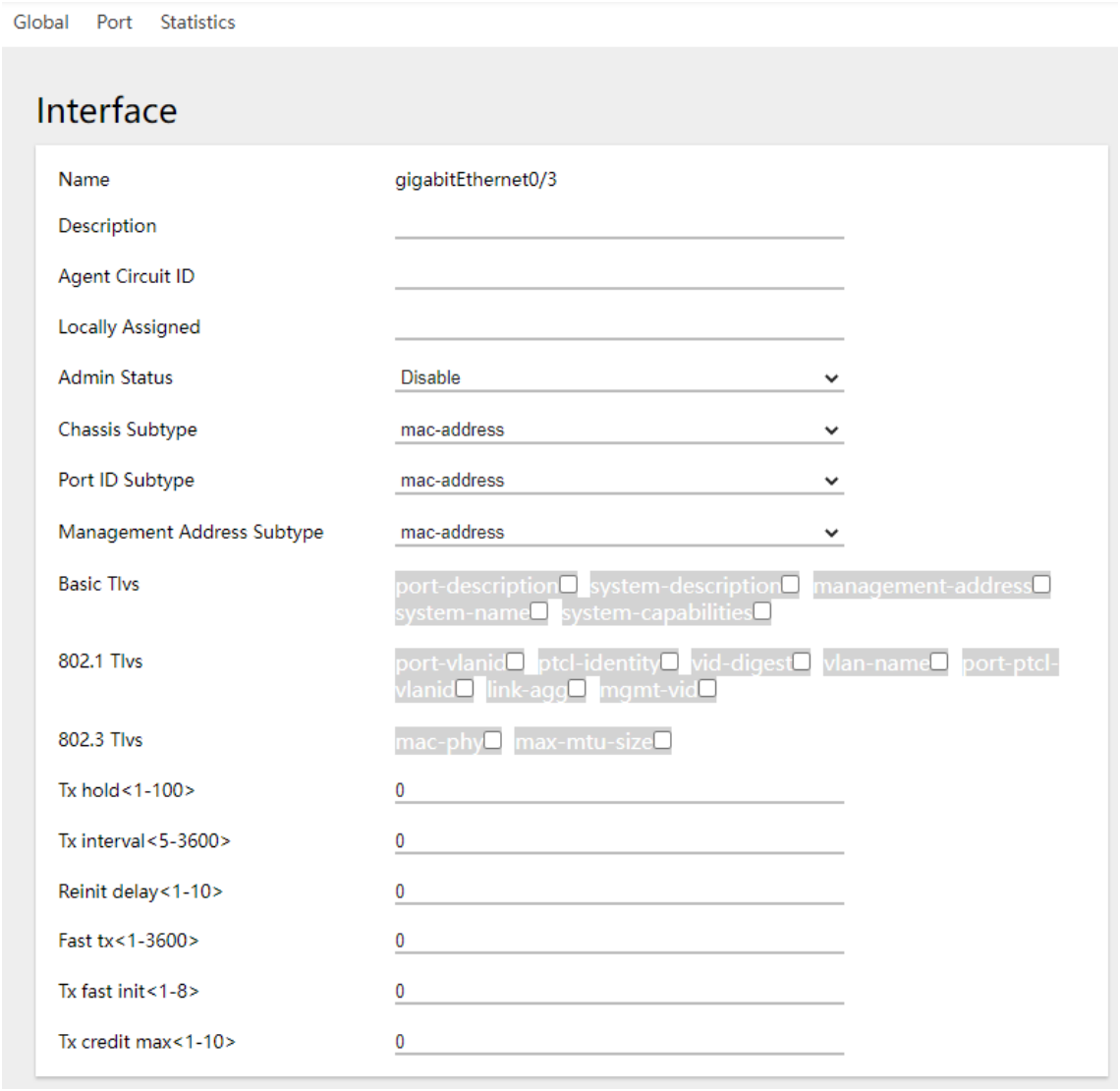


Table 3-22 LLDP port Configuration Items

Item	Description
Description	Description of the currently configured LLDP port
Agent Circuit ID	Agent circuit identification. Can be used as a value for port-id-tlv
Locally Assigned	Locally Assigned
Admin Status	Disabled: No LLDP packets are sent/receive on the interface TxOnly: LLDP packets are sent on the interface RxOnly: LLDP packets are received on the interface TxRx: LLDP packets are sent/receive on the interface
Chassis Subtype	Mac-address: indicates the MAC address If-alias: Indicates the interface alias

	If-name: indicates the interface name Ip-address: Indicates the IP address Locally-assigned: indicates local configuration
Port ID Subtype	Mac-address: indicates the MAC address If-alias: Indicates the interface alias If-name: indicates the interface name Ip-address: Indicates the IP address Agt -circuit-id: Indicates the agt-circuit-id Locally-assigned: indicates locally-assigned value
Management Address Subtype	Mac-address: Device MAC address Ip-address: Device IP address
Basic Tlvs	port-description: port descriptor system-description: system descriptor management-address: management address system-name: system name system-capabilities: system capabilities
802.1 Tlvs	port-vlanid: port's vlanid ptcl -identity: protocol id vid-digest: vid digest vlan-name: vlan name port-ptcl - vlanid: port protocol vlanid link- agg mgmt -vid: Link Aggregation Management vid
802.3 Tlvs	mac-phy: The rate and duplex status supported by the port, whether it supports port rate auto-negotiation, whether the auto-negotiation function is enabled, and the current rate and duplex status max - mtu -size: maximum mtu value
Tx hold	Transmission hold, the default value txFastInit is 4, used for packet TTL calculation; TTL= msgTxInterval * msgTxHold + 1

Tx interval	Transfer intervals, default is 30 s; admin can change this value to any value between5and 300.
Reinit delay	Indicates the amount of delay between when adminStatus becomes ' disabled' and when reinitialization is attempted. The default value of reinitDelay is 2 s.
Fast tx	Defines the time interval for the timer interval between two transfers within a fast transfer period (ie txFast is not zero). The default value for msgFastTx is 1; administrators can change this value to any value between 1 and 3600.
Tx fast init	This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transmission period.
Tx credit max	Configure the maximum value of txCredit. The default value is 5. Administrators can change this value to any value in the range 1 to 10.

View statistics

Select L2 Switch > LLDP > statistics in the navigation area to enter the LLDP port setting page, as shown in Figure 3-50. Table 3-23 describes the Global Configuration items.

Figure 3-50 LLDP port statistics

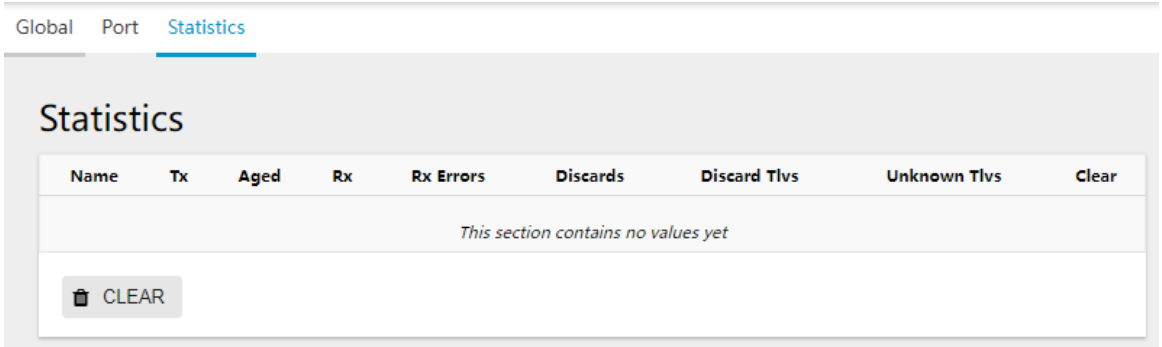


Table 3-23 LLDP port Configuration Items

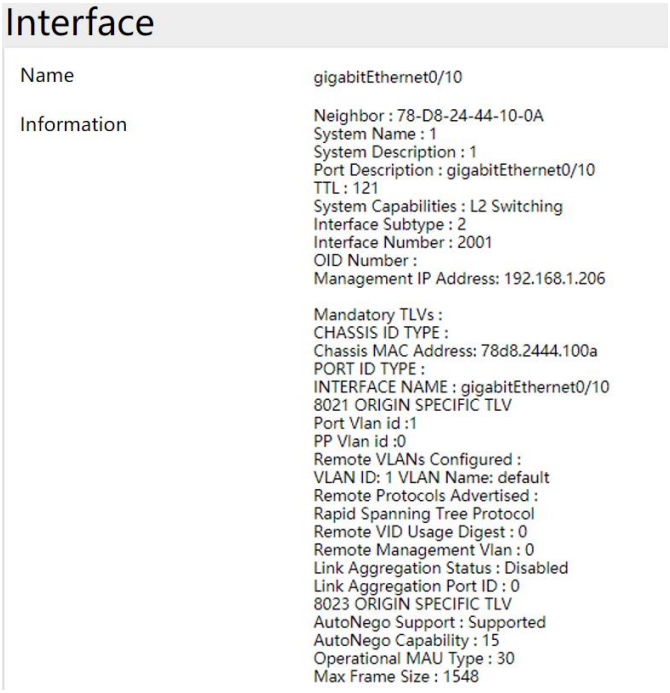
Item	Description
Item	Description of the currently configured LLDP port
Tx	The number of packets sented on the interface
Aged	The number of packets aged on the interface

Rx	The number of packets received on the interface
Rx Errors	The number of error packets received on the interface
Discards	The number of packets discarded on the interface
Discard Tlvs	The number of tlv packets of discarded on the interface
Unknown Tlvs	The number of unknown tlvs packets on the interface
CLEAR	Clear counters on the current interface

View neighbor information

On the current 'Port' tab, click the 'Neighbor' button of the corresponding port to enter the neighbor information view interface.

Figure 3-51 LLDP neighbor information



4 Security

4.1 ACL

4.1.1 Overview

An access control list (ACL) is a set of rules (or permit or deny statements) for identifying traffic based on criteria such as source IP address, destination IP address, and port number. ACLs are essentially used for packet filtering. A packet filter drops packets that match a deny rule and permits packets that match a permit rule. ACLs are also widely used by many modules, for example, QoS and IP routing, for traffic identification.

NOTE:

- Unless otherwise stated, ACLs refer to IPv4 ACLs throughout this document.

4.1.2 Configuring Acls

Configuring a rule for a basic IP ACL

1. Select Security > ACL from the navigation tree.

2. Click the +ADD to enter the rule configuration page and choose the ACL type 'IP' for a basic ACL as shown in Figure 4-1. Table 4-1 describes the configuration items of configuring an IP ACL.

Figure 4-1. Configuring a basic IP ACL

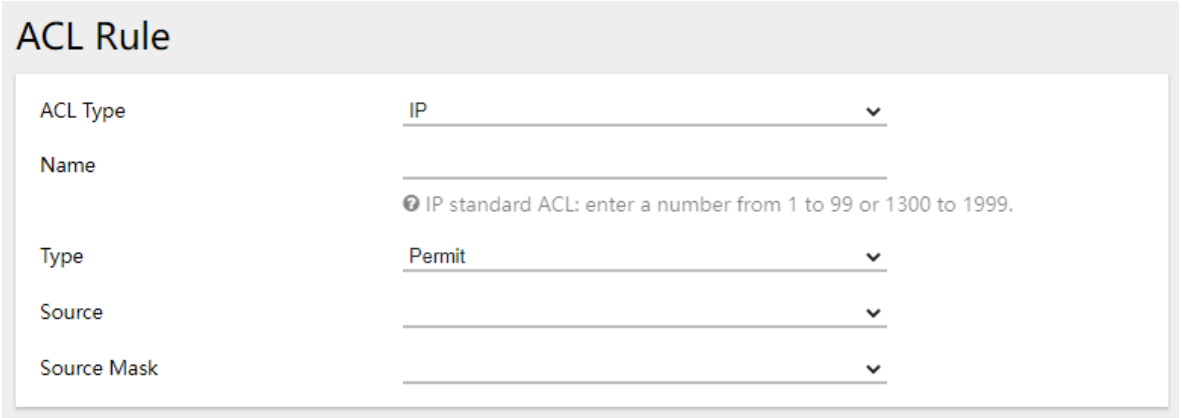


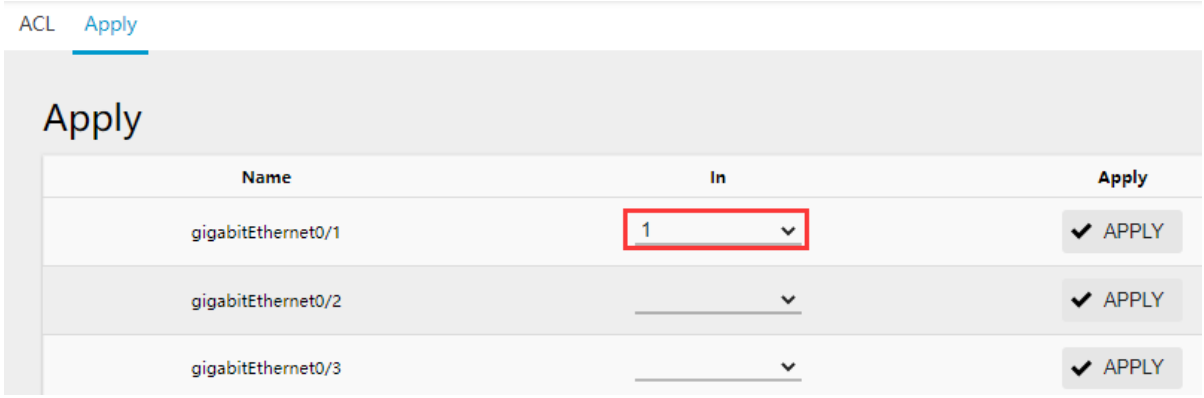
Table 4-1 The description of the basic IP ACL

Item		Description
ACL Type	IP	ACL of Standard IP
Name		The number of the rule, Between 1-99 or 1300-1999
Type	Permit	Allows matched packets to pass
	Deny	Drops matched packets
Source		Source IP address, such as 192.168.64.1
Source Mask		The IP mask is reversed. If it matches the first 24 bits of the IP address, the mask is 255.255.255.0, which needs to be set to 00.00.00.255 here.

3. Configure a rule for a basic ACL, and click Apply.

4. Click Apply tab to enter the ACL port configuration page, choose the ACL rules of the corresponding port, as shown in Figure 4-2, and click Apply.

Figure 4-2 Apply the ACL rule to the port



Configuring a rule for an IP-Extend ACL

1. Select Security > ACL from the navigation tree.

2. Click the +ADD to enter the rule configuration page and choose the ACL type 'IP-Extend' for an IP-Extend ACL as shown in Figure 4-3. Table 4-2 describes the configuration items of configuring an IP-Extend ACL.

Figure 4-3. Configuring an IP-Extend ACL

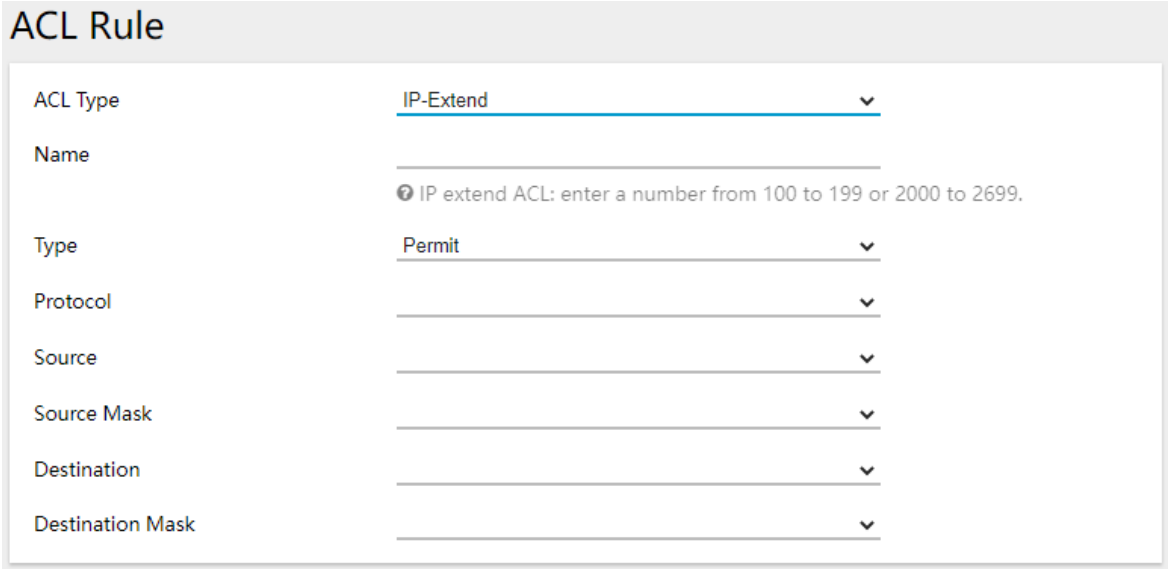


Table 4-2 The description of the IP-Extend ACL

Item		Description
ACL Type	IP-Extend	Extend ACL, Match the protocol number, source IP address, and destination IP address of IPv4 packets.
Name		The number of the rule, Between 100-199 or 2000-2699.
Type	Permit	Allows matched packets to pass
	Deny	Drops matched packets
Protocol		Support common protocol message options, including tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp, etc. Support all IPv4 packets IPv4 packets that support custom protocols
Source		Source IP address, such as 192.168.64.1
Source mask		The IP mask is reversed. If it matches the first 24 bits of the IP address, the mask is 255.255.255.0, which needs to be set to 00.00.00.255 here.
Destination		Destination IP address, such as 192.168.64.100
Destination mask		Enter a value to specify the subnet mask for the destination IP address. The IP mask is reversed.

3. Configure a rule for a basic ACL, and click Apply.

4. Click Apply tab to enter the ACL port configuration page, choose the ACL rules of the corresponding port, and click Apply.

Configuring a rule for a MAC-Extend ACL

1. Select Security > ACL from the navigation tree.

2. Click the +ADD to enter the rule configuration page and choose the ACL type 'MAC-Extend' for a MAC-Extend ACL as shown in Figure 4-4. Table 4-3 describes the configuration items of configuring a MAC-Extend ACL.

Figure 4-4. Configuring a MAC-Extend ACL

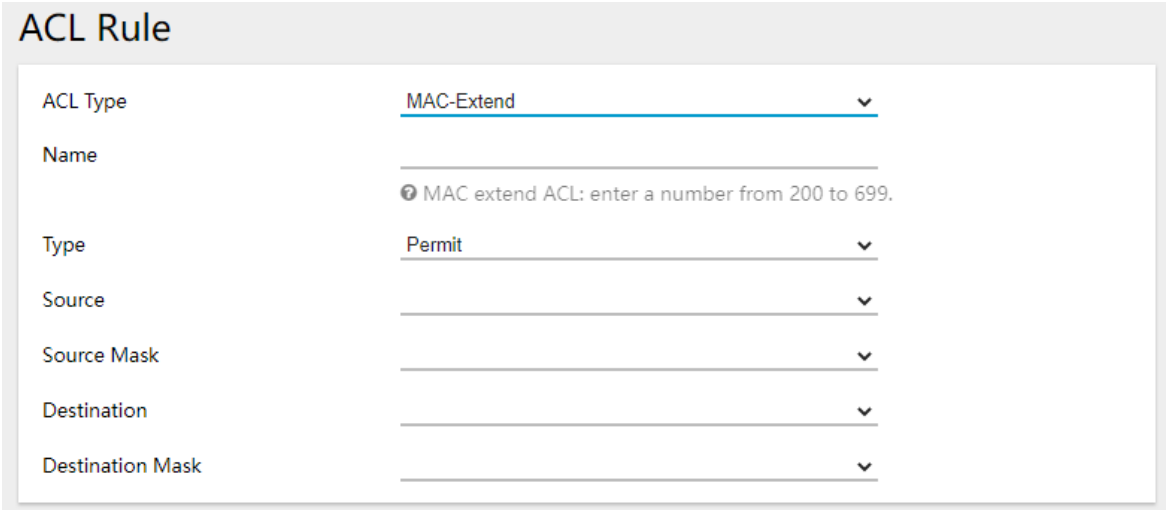


Table 4-3 The description of the MAC-Extend ACL

Item		Description
ACLType	MAC-Extend	Extended MAC ACL to match Layer 2 source MAC address and destination MAC address
Name		The number of the rule, Between 200-699
Type	Permit	Allows matched packets to pass
	Deny	Drops matched packets
Source		Source IP address, such as 192.168.64.1
Source mask		The IP mask is reversed. If it matches the first 24 bits of the IP address, the mask is 255.255.255.0, which needs to be set to 00.00.00.255 here.
Destination		Destination IP address, such as 192.168.64.100

Destination mask	Enter a value to specify the subnet mask for the destination IP address. The IP mask is reversed.

3. Configure a rule for a basic ACL, and click Apply.

4. Click Apply tab to enter the ACL port configuration page, choose the ACL rules of the corresponding port, and click Apply.

Configuring a rule for an IP-Name ACL

1. Select Security > ACL from the navigation tree.

2. Click the +ADD to enter the rule configuration page and choose the ACL type 'IP-Named' for an IP-Named ACL, as shown in Figure 4-5. Table 4-4 describes the configuration items of configuring a IP-Named ACL.

Figure 4-5. Configuring an IP-Named ACL

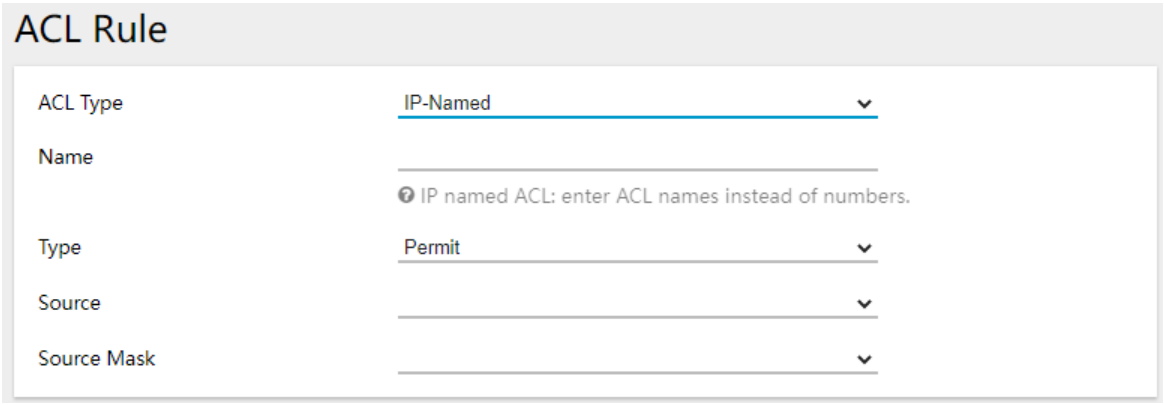


Table 4-4 The description of the IP-Named ACL

Item		Description
ACLType	IP-Named	Standard ACL, support name naming, the first character must be a letter
Name		String starting with a letter
Type	Permit	Allows matched packets to pass
	Deny	Drops matched packets
Source		Source IP address, such as 192.168.64.1
Source mask		The IP mask is reversed. If it matches the first 24 bits of the IP address, the mask is 255.255.255.0, which needs to be set to 00.00.00.255 here.

3. Configure a rule for a basic ACL, and click Apply.

4. Click Apply tab to enter the ACL port configuration page, choose the ACL rules of the corresponding port, and click Apply.

Configuring a rule for an IP-Name-Extend ACL

1. Select Security > ACL from the navigation tree.

2. Click the +ADD to enter the rule configuration page and choose the ACL type 'IP-Name-Extend' for an IP-Name-Extend ACL as shown in Figure 4-6. Table 4-5 describes the configuration items of configuring an IP-Name-Extend ACL.

Figure 4-6 Configuring an IP-Name-Extend ACL

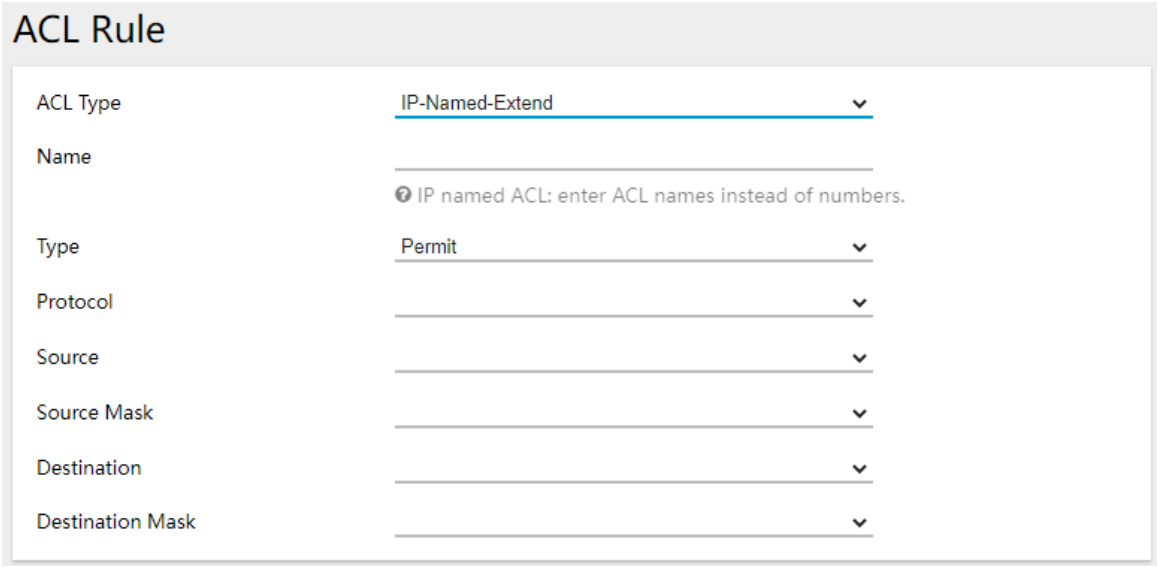


Table 4-5 The description of the IP-Name-Extend ACL

Item		Description
ACL Type	IP-Named -Extend	Extended ACL, support name naming, the first character must be a letter
Name		String starting with a letter
Type	Permit	Allows matched packets to pass
	Deny	Drops matched packets
Protocol		Support common protocol message options, including tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp, etc. Support all IPv4 packets IPv4 packets that support custom protocols

Source	Source IP address, such as 192.168.64.1
Source mask	The IP mask is reversed. If it matches the first 24 bits of the IP address, the mask is 255.255.255.0, which needs to be set to 00.00.00.255 here.
Destination	Destination IP address, such as 192.168.64.100
Destination mask	Enter a value to specify the subnet mask for the destination IP address. The IP mask is reversed.

3. Configure a rule for a basic ACL, and click Apply.

4. Click Apply tab to enter the ACL port configuration page, choose the ACL rules of the corresponding port, and click Apply.

4.2 QoS

4.2.1 Overview

Quality of Service (QoS) reflects the ability of a network to meet customer needs. In an internet, QoS evaluates the ability of the network to forward packets of different services. The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

4.2.2 Configuring Qos

Qos global Configuration

Select Security > Qos > Summary in the navigation area to enter the QoS summary page, as shown in Figure 4-7. Table 4-6 describes the QoS summary items.

Figure 4-7 QoS summary

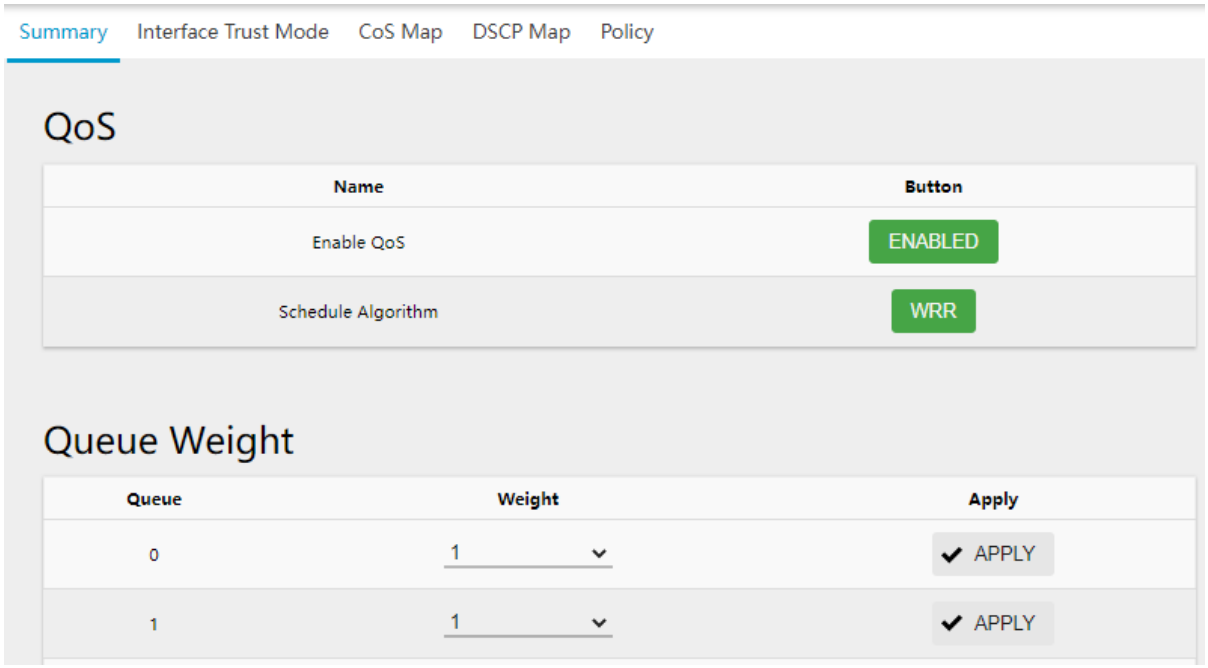


Table 4-6 Descriptions of QoS summary

Items		Description		
Summary	QoS	Enable QoS	Enable	Enable QOS, all QOS functions do not support configuration before enabling
			Disable	Disable QOS, when QOS is disabled, delete all QOS configurations
		Schedule Algorithm	Sp	Absolute priority scheduling, the queue ID is large, the priority is high, and the low-priority queue is processed after the high -priority queue is processed.
			Wrr	robin scheduling algorithm schedules each queue in turn according to the queue weight, from the largest to the smallest queue ID.
	Queue weight	Queue		< 0, 7 >
		weight		< 0, 32>, the larger the value, the higher the weight, and the higher the probability of preferential processing of packets in this queue under the condition of channel congestion, 0 means infinity.

Select Security > Qos > Interface Trust Mode in the navigation area to enter the QoS interface trust mode page, as shown in Figure 4-8. Table 4-7 describes the interface trust mode items.

Figure 4-8 Configuring Interface Trust

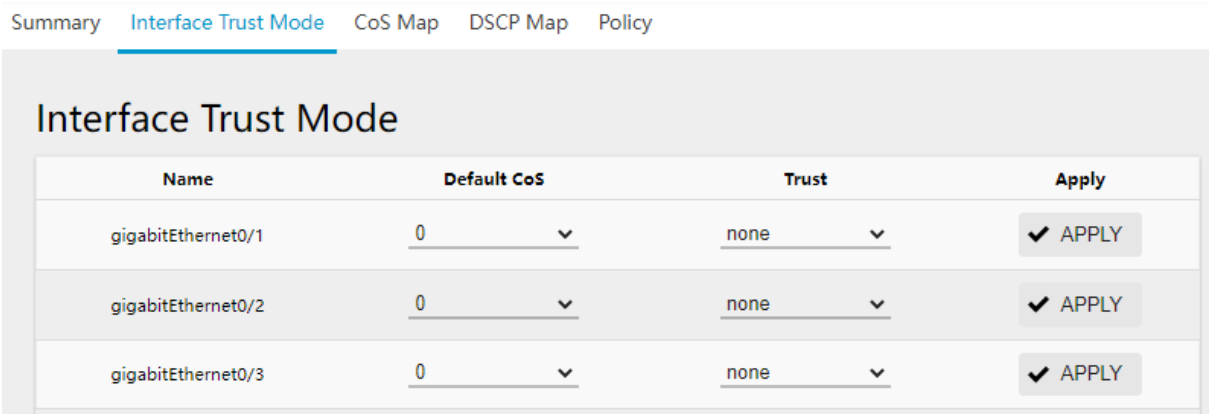


Table 4-7 QoS port trust parameter description

Items		Description
Interface trust	Name	The name of the interface
	Default CoS	< 0, 7>, when the configuration port is not trusted, or the configuration is trusted but the message does not meet the trust condition, the port default cos is used to mark the ingress message
	Trust	Support untrust, trust cos, trust dscp configuration. When in no trust mode, the entry stage modifies the cos field and dscp field of the message according to the default cos of the port; when trust cos is configured, the same as the no trust mode for untagged messages, and for tagged messages, choose the message with its own cos; When configuring trust dscp, for ip packets, select the packet with dscp, and for non-ip packets, it is the same as trust cos mode.
	Apply	Click to configure

Select Security > Qos > CoS Map in the navigation area to enter the QoS CoS Map page, as shown in Figure 4-9. Table 4-8 describes the CoS Map items.

Figure 4-9 Configuring CoS Map

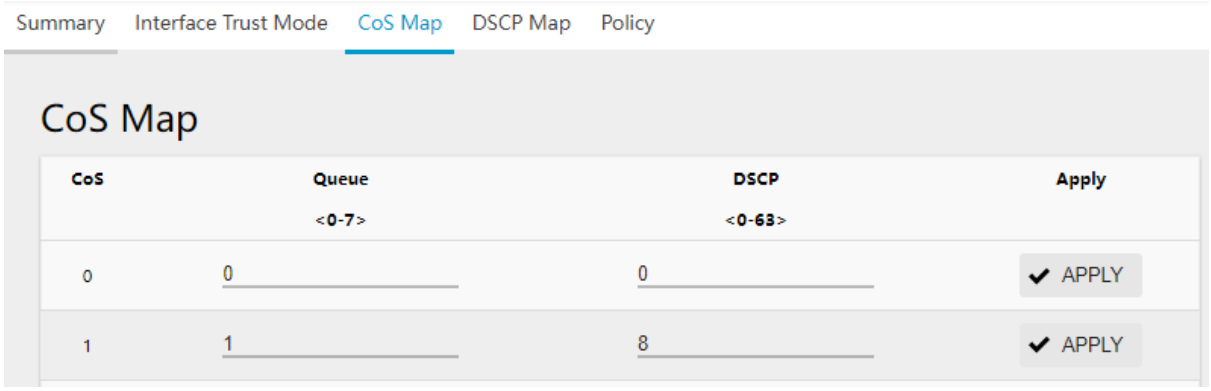


Table 4-8 QoS CoS mapping parameter description

Items		Description
CoS Map	CoS	<0, 7>
	Queue	< 0, 7>, Cos - queue mapping relationship, based on the cos marked on the port, modifying the packet egress queue takes effect when the port is configured as no trust, trust cos or trust dscp and non-ip packets.
	DSCP	cos-dscp mapping relationship takes effect when the port is configured as no trust, trust cos or trust dscp and is not ip packets. Modify the packet dscp value.
	Apply	Click to apply

Select Security > Qos > DSCP Map in the navigation area to enter the QoS DSCP Map page, as shown in Figure 4-10. Table 4-9 describes the DSCP Map items.

Figure 4-10 Configuring DSCP Map

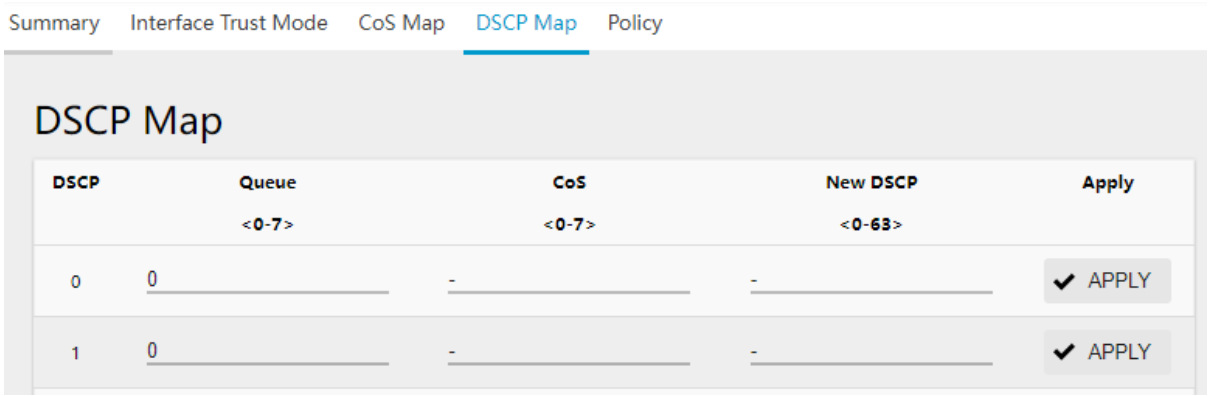


Table 4-9 QoS DSCP parameter description

Items		Description
DSCP Map	DSCP	<0, 63>
	Queue	< 0, 7>, dsp-queue mapping relationship, which takes effect when the port is configured as trust dscp and ip packets, modify the packet export queue
	CoS	< 0, 7>, dscp-cos mapping relationship, which takes effect when the port is configured as trust dscp and ip packets, modify the cos field of the packet
	Nes DSCP	< 0, 63 >, dscp-dscp mapping relationship, which takes effect when the port is configured as trust dscp and ip packets, first perform dscp-dscp mapping, and then perform dscp-cos mapping
	Apply	Click to apply

Select Security > Qos > Policy in the navigation area to enter the QoS Policy page, as shown in Figure 4-11. Table 4-10 describes the QoS Policy items.

Figure 4-11 Configuring Qos Policy

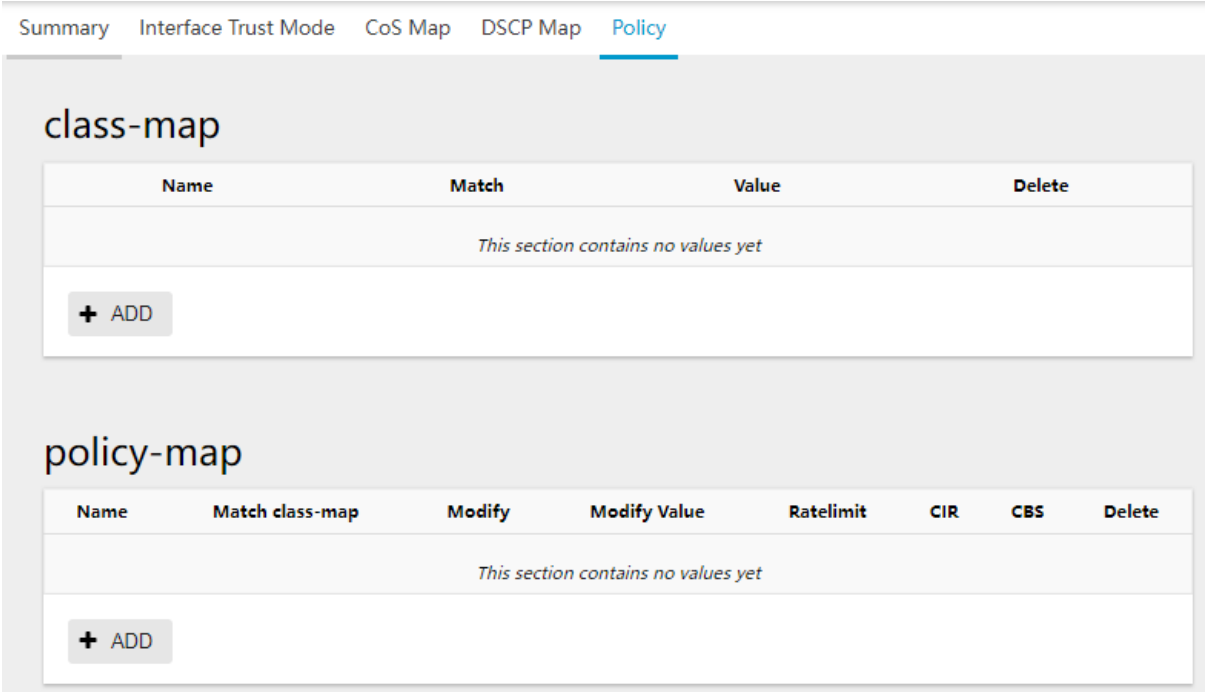


Table 4-10 QoS Policy Parameter Description

Items		Description	
Policy	class-map	Name	Create a category, define the category name
		Match	Define match type, support associated ACL; Support packet etype, dscp, cos, l4port, vlan field matching
		Value	stream match type
		Delete	delete category
	Policy-map	Name	Create a policy, define a policy name
		Match class-map	Select the class-map associated with the policy
		Modify	policy, supports modifying cos, dscp, vlan and other actions
		Modify value	Strategy action to a corresponding value
		Ratelimit	Action 2 corresponding to the strategy, speed limit
		CIR	Speed limit waterline, unit kbps
		CBS	burst capability, unit Kbyte
		Delete	delete policy

Select Security > Qos > Policy > Apply in the navigation area to enter the QoS Policy Apply page, as shown in Figure 4-12. Table 4-11 describes the QoS Policy Apply items.

Figure 4-12 Qos Apply

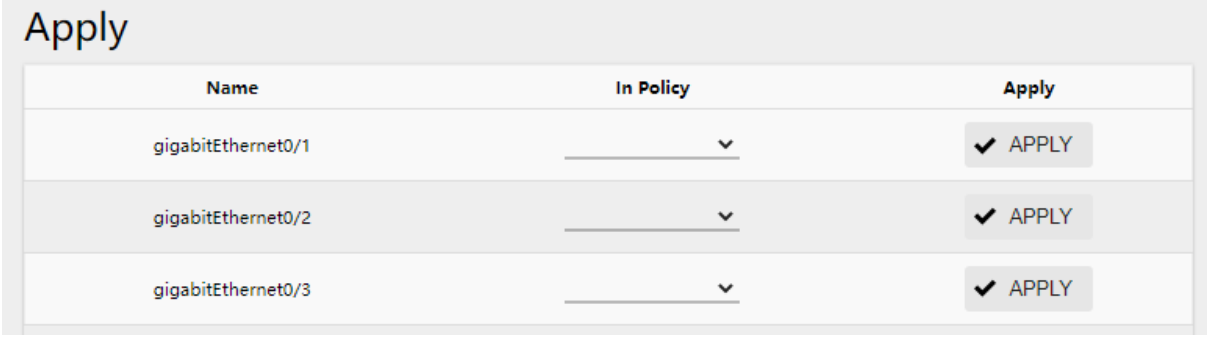


Table 4-11Description of Qos Apply

Items		Description
Apply	Name	Interface to be applied
	In Policy	Select the policy
	Apply	policy takes effect on the por

4.3 DHCP Snooping

4.3.1 Overview

DHCP snooping (Dynamic Host Configuration Protocol) is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Trusted Sources

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server. The default trust state of all interfaces is untrusted.

DHCP Snooping Limit Rate

Configure the number of DHCP packets per second that an interface can receive, to reduce or eliminate the impact of DHCP packet attack from this interface.

MAC Address Verification

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on

untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

Option-82 Insertion

DHCP Option82 option is also called DHCP relay agent information option, one of many dhcp options. The Option82 option is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation strategy. The addition and stripping of options are implemented by the relay component.

DHCP Database

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces. When the Ip verify source function is enabled on the interface, database entries act as valid users on the interface.

4.3.2 Configuring DHCP Snooping

Configuring DHCP Snooping globally

1. Select Security > DHCP Snooping from the navigation tree.

2. Click the Global Configuration tap of the current page to enter the page, as shown in Figure 4-13. Table 4-12 describes the configuration items of configuring DHCP Globally.

Figure 4-13 DHCP Snooping global configuration

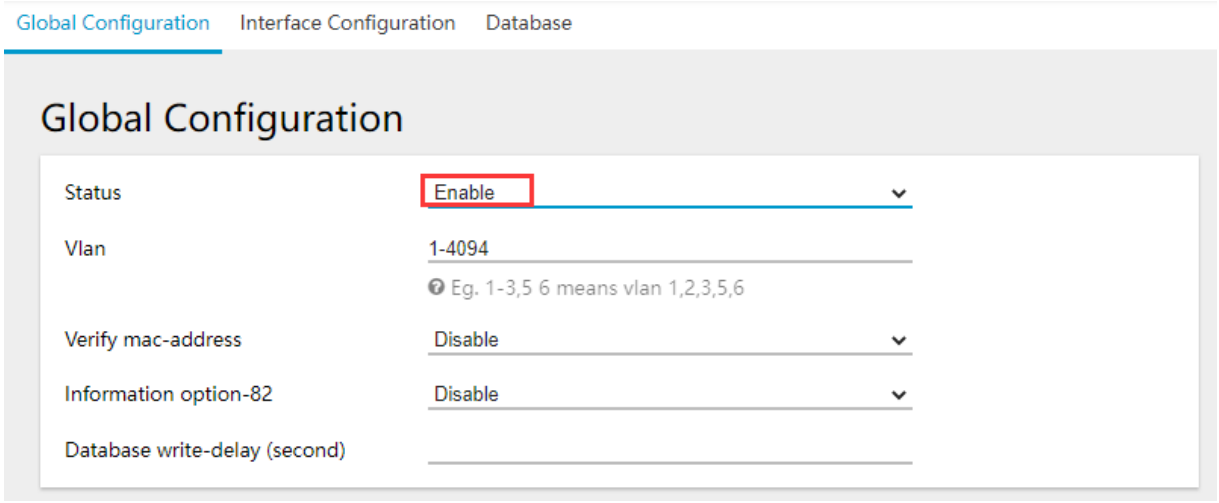


Table 4-12 The description of DHCP Snooping global configuration

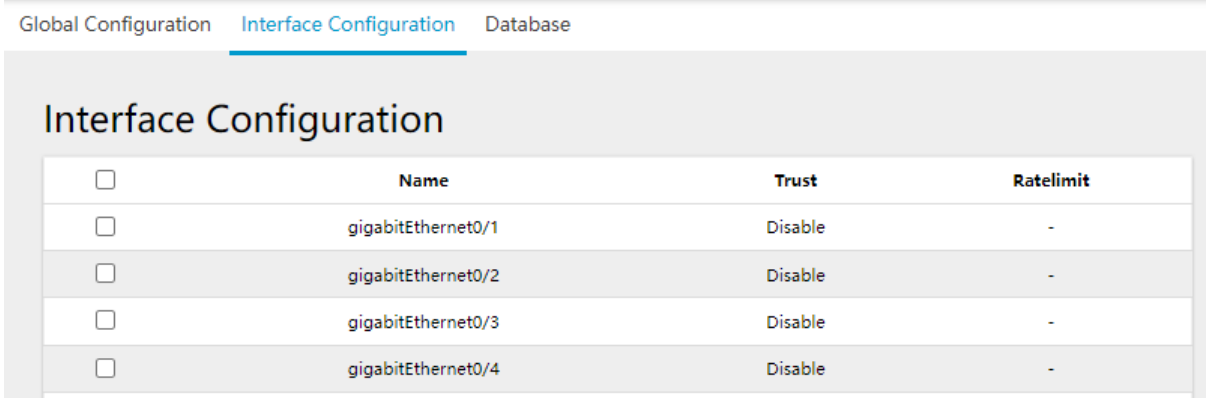
Item	Description
Status	Enable/Disable the DHCP Snooping globally
Vlan	Enable/Disable the DHCP Snooping on the vlans
Vefify mac-address	Verify the source MAC address and the client hardware address is matched in DHCP packets
Information option-82	Enable/Disable option-82 insertion
Database write-delay(s)	Configure the interval time database writing to flash

Configuring DHCP Snooping ports

1. Select Security > DHCP Snooping from the navigation tree.

2. Click the Interface Configuration tap of the current page to enter the DHCP Snooping interfae configuration status page, as shown in Figure 4-14.

Figure 4-14 DHCP Snooping interfae configuration status



3. Check the ports to be configured, click EDIT to enter the interface configuration page as shown in Figure 4-15. Table 4-13 describes the configuration items of configuring DHCP snooping interface configuration.

Figure 4-15 DHCP Snooping global configuration

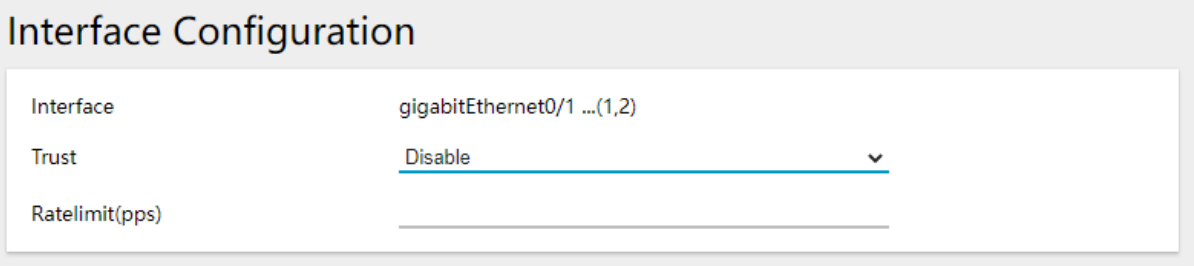


Table 4-13 The description of DHCP snooping interface configuration

Item	Description
Trust	determines whether traffic sources are trusted or untrusted
Ratelimit(pps)	Configure the number of DHCP packets per second that an interface can receive

NOTE:

- Due to hardware limitations, for DHCP rate limit, when the limit value is not 0, the software rate limit is used, and when the limit value is 0, the hardware rate limit is used. Software rate limit will consume CPU resources.

Configuring DHCP Snooping databse

1. Select Security > DHCP Snooping from the navigation tree.

2. Click the Database tap of the current page to enter the database page, as shown in Figure 4-16. Table 4-14 describes the configuration items of configuring DHCP Snooping database.

Figure 4-16 DHCP Snooping database

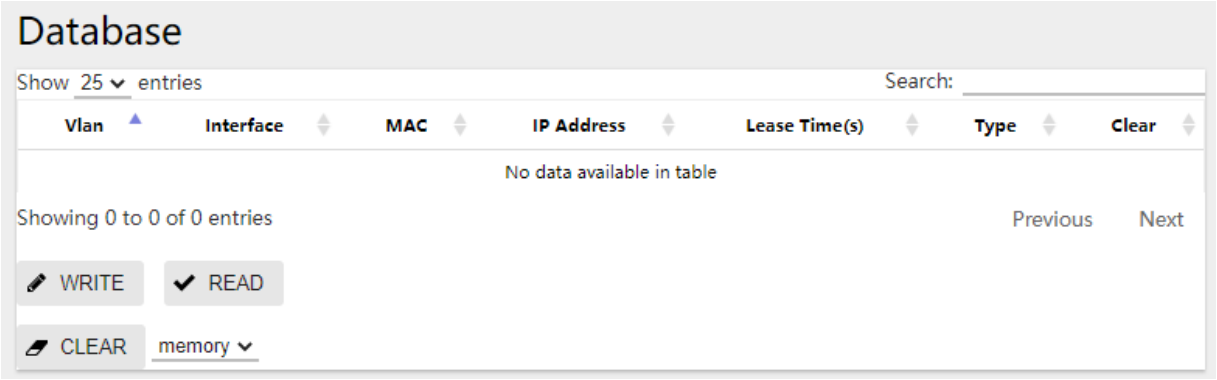


Table 4-14 The description of DHCP Snooping database

Item	Description
Search	Search database entries by fuzzy match the intput strings
WRITE	Write database entries to flash
READ	Read database entries from flash
CLEAR	Clear database entries, you can narrow the scope by selecting keywords

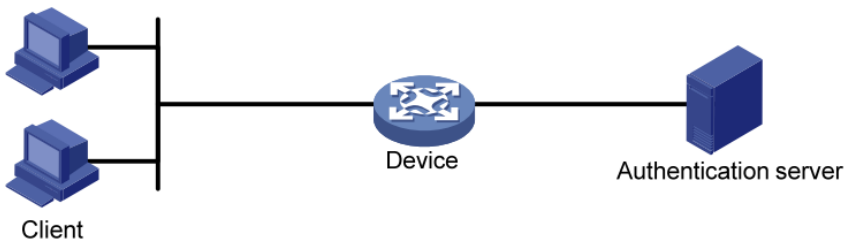
4.4 802.1X Authentication

4.1.1 Overview

The 802.1X protocol was proposed by the IEEE 802 LAN/WAN committee for security of wireless LANs (WLAN). It has been widely used on Ethernet as a common port access control mechanism. As a port-based access control protocol, 802.1X authenticates and controls accessing devices at the port level. A device connected to an 802.1X-enabled port of an access control device can access the resources on the LAN only after passing authentication.

4.4.1.1 Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: Client, Device, and Server, as shown in below.



- Client is an entity seeking access to the LAN. It resides at one end of a LAN segment and is authenticated by Device at the other end of the LAN segment. Client is usually a user-end device such as a PC. 802.1X authentication is triggered when an 802.1X-capable client program is launched on Client. The client program must support Extensible Authentication Protocol over LAN (EAPOL).
- Device, residing at the other end of the LAN segment, authenticates connected clients. Device is usually an 802.1X-enabled network device and provides access ports (physical or logical) for clients to access the LAN.
- Server is the entity that provides authentication services to Device. Server, normally running RADIUS (Remote Authentication Dial-in User Service), serves to perform authentication, authorization, and accounting services for users.

4.4.1.2 Authentication modes of 802.1x

The 802.1X authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the client, device, and authentication server. Client Device Server

- Between the client and the device, EAP protocol packets are encapsulated using EAPOL to be transferred on the LAN.
- Between the device and the RADIUS server, EAP protocol packets can be exchanged in two modes: EAP relay and EAP termination. In EAP relay mode, EAP packets are encapsulated in EAP over RADIUS (EAPOR) packets on the device, and then relayed by device to the RADIUS server. In EAP termination mode, EAP packets are terminated at the device, converted to RADIUS packets either with the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) attribute, and then transferred to the RADIUS server.

4.4.1.3 Basic concepts of 802.1x

These basic concepts are involved in 802.1X: controlled port/uncontrolled port, authorized state/unauthorized state, and control direction.

Controlled port and uncontrolled port

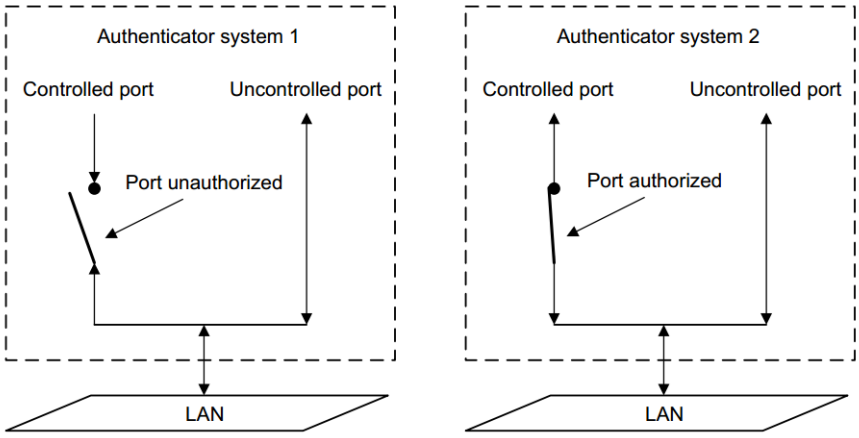
A device provides ports for clients to access the LAN. Each port can be regarded as aunity of two logical ports: a controlled port and an uncontrolled port. Any packets arriving at the port are visible to both logical ports.

- The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol packets to pass, guaranteeing that the client can always send and receive authentication packets.
- The controlled port is open to allow data traffic to pass only when it is in the authorized state.

Authorized state and unauthorized state

A controlled port can be in either authorized state or unauthorized state, which depends on the authentication result, as shown in Figure 4-17.

Figure 4-17 Authorized/unauthorized state of a controlled port



You can control the port authorization status of a port by setting port authorization mode to one of the following:

- Force-Authorized: Places the port in authorized state, allowing users of the port to access the network without authentication.

- Force-Unauthorized: Places the port in unauthorized state, denying any access requests from users of the port.
- Auto: Places the port in the unauthorized state initially to allow only EAPOL packets to pass, and turns the port into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

Control direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the client or just the traffic from the client.

802.1X authentication triggering

802.1X authentication can be initiated by either a client or the device.

Unsolicited triggering of a client

A client can initiate authentication unsolicitedly by sending an EAPOL-Start packet to the device. The destination address of the packet is 01-80-C2-00-00-03, the multicast address specified by the IEEE 802.1X protocol.

Some devices in the network may not support multicast packets with the above destination address, and unable to receive authentication requests of clients as a result. To solve this problem, the device also supports EAPOL-Start packets using a broadcast MAC address as the destination address.

Unsolicited triggering of the device

The device can trigger authentication by sending EAP-Request/Identity packets to unauthenticated clients periodically (every 30 seconds by default). This method can be used to authenticate clients that cannot send EAPOL-Start packets unsolicitedly to trigger authentication, for example, a client running the 802.1X client application provided by Windows XP.

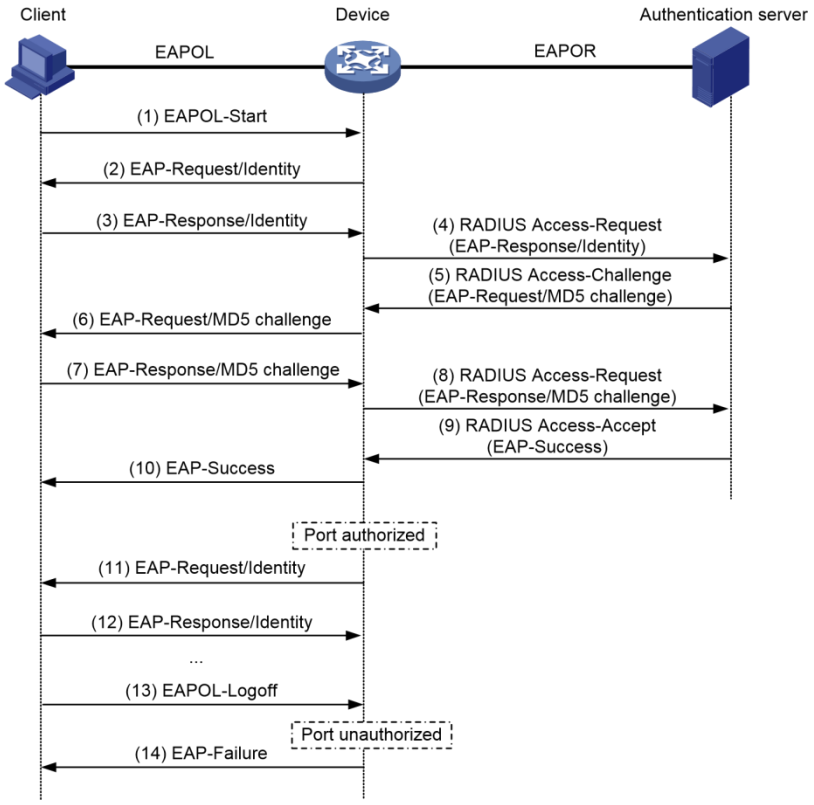
Authentication process of 802.1x

An 802.1X device communicates with a remote RADIUS server in two modes: EAP relay and EAP termination. The following describes the 802.1X authentication procedure in the two modes, which is triggered by the client in the examples.

EAP relay

EAP relay is defined in IEEE 802.1X. In this mode, EAP packets are carried in an upper layer protocol, such as RADIUS, so that they can go through complex networks and reach the authentication server. Generally, relaying EAP requires that the RADIUS server support the EAP attributes of EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying the EAPMessage attribute respectively.

Figure 4-18 shows the message exchange procedure with EAP-MD5



1. When a user launches the 802.1X client software and enters the registered username and password, the 802.1X client software generates an EAPOL-Start frame and sends it to the device to initiate an authentication process.

2. Upon receiving the EAPOL-Start frame, the device responds with an EAPRequest/Identity packet for the username of the client.

3. When the client receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the device.

4. Upon receiving the EAP-Response/Identity packet, the device relays the packet in a RADIUS Access-Request packet to the authentication server.

5. When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the device.

6. After receiving the RADIUS Access-Challenge packet, the device relays the contained EAP-Request/MD5 Challenge packet to the client.

7. When receiving the EAP-Request/MD5 Challenge packet, the client uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the device.

8. After receiving the EAP-Response/MD5 Challenge packet, the device relays the packet through a RADIUS Access-Request packet to the authentication server.

9. When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the device a RADIUS Access-Accept packet.

10. Upon receiving the RADIUS Access-Accept packet, the device opens the port to grant the access request of the client. After the client gets online, the device periodically sends handshake requests to the client to check whether the client is still online. By default, if two consecutive handshake attempts end up with failure, the device concludes that the client has gone offline and

performs the necessary operations, guaranteeing that the device always knows when a client goes offline.

11. The client can also send an EAPOL-Logoff frame to the device to go offline unsolicitedly. In this case, the device changes the status of the port from authorized to unauthorized and sends an EAP-Failure packet to the client.

4.4.2 Configuring 802.1X

Displaying 802.1X Summary

Select Security > 802.1x Authentication > Summary from the navigation area. The system automatically displays the 802.1X summary, as shown in Figure 4-19. Table 4-15 describes the Spanning Tree Summary items.

Figure 4-19 The summary of the 802.1X

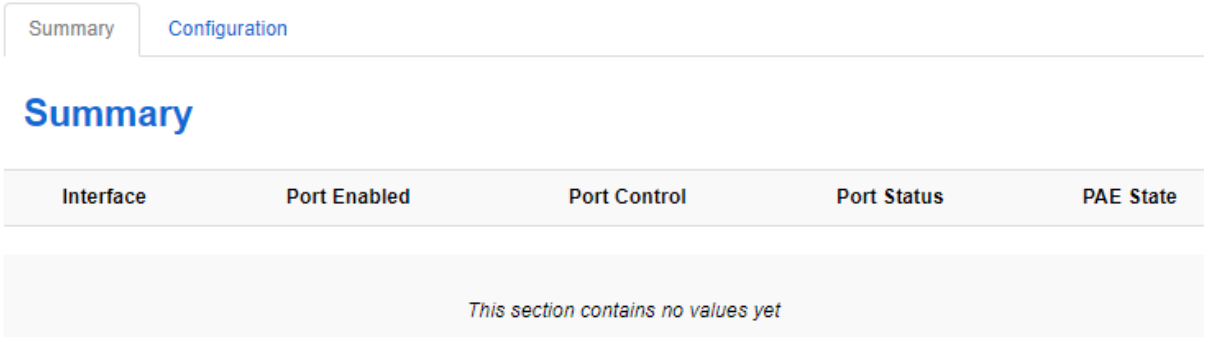


Table 4-15 The 802.1X summary items

Item	Description
Interface	Physical interface name
Port Enabled	802.1X authentication enable state on the interface.
Port Control	802.1X authentication control mode on the interface.
Port Status	802.1X authentication current authentication state on the interface.
PAE State	Port Access Entity state

Configuring 802.1X

Select Security > 802.1x Authentication > Configuration from the navigation area. The system automatically displays the 802.1X Global Configuration and Port Configuration, as shown in Figure 4-20 and Figure 4-21. Table 4-16 describes the Global Configuration and Port Configuration items.

Figure 4-20 802.1X Global Configuration

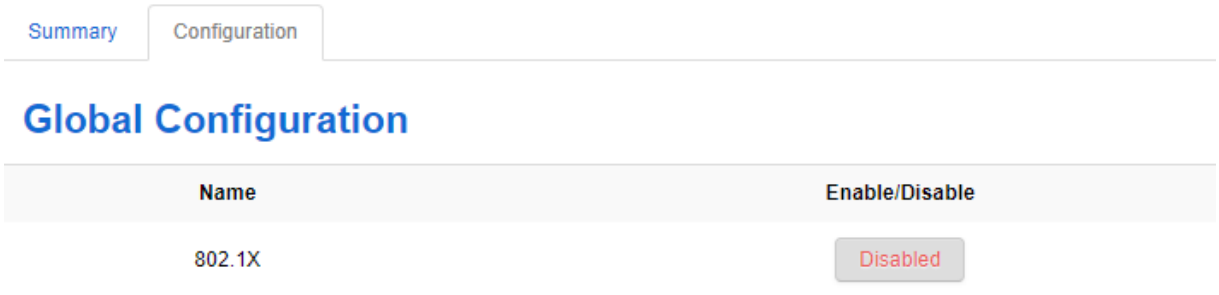


Figure 4-21 802.1X Port Configuration

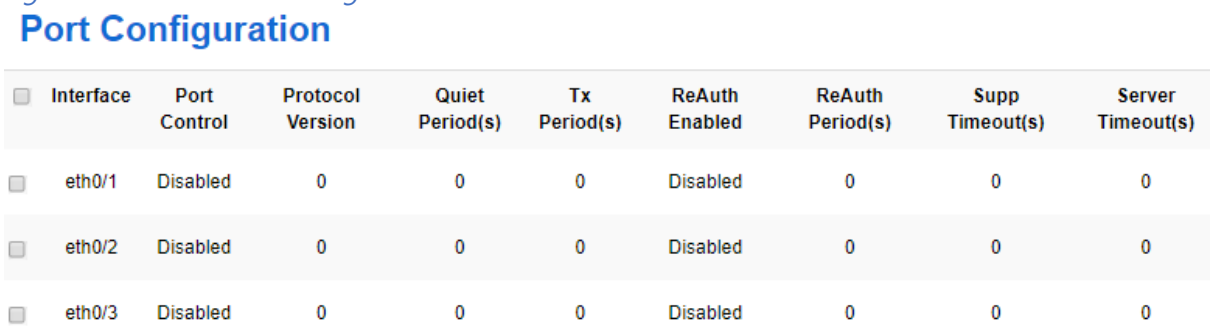


Table 4-16 The 802.1X Configuration items

Item		Description
Global Configuration	Enable/Disable	Enables the 802.1X feature on your switch.
Portl Configuration	Interface	Physical interface name
	Port Control	Port control mode
	Protocol Version	Eapol protocol version, default version 2
	Quiet Period(s)	Sets the number of seconds that the switch remains in the quiet-periodfollowing a failed authentication exchange with the client. The range is 0 to 65,535 seconds; the default is 60.

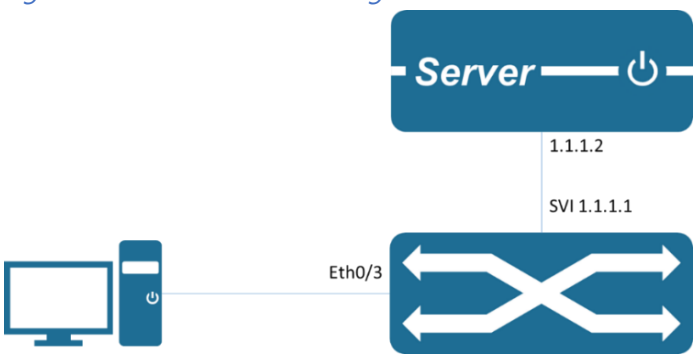
	When the switch cannot authenticate the client, the switch remains idle for a set period, and then tries again. The idle time is determined by the quiet-period value.
Tx Period(s)	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30.
ReAuth Enabled	Enables periodic reauthentication of the client
ReAuth Period(s)	Specifies the number of seconds between reauthentication attempts or have the switch use a RADIUS-provided session timeout. The range is 1 to 65,535; the default is 3600 seconds. This command affects the behavior of the switch only if periodic reauthentication is enabled.
Supp Timeout(s)	Sets the number of seconds that the switch waits for a response to an EAP-Request/MD5 Challenge frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30.
Server Timeout(s)	Sets the number of seconds that the switch waits for a response to a RADIUS Access-Request packet from the server. The range is 1 to 65,535 seconds; the default is 30.

4.4.3 802.1X Configuration Example

Network requirements

- As shown in Figure 4-22 the access user is authenticated on GigabitEthernet0/3 to control access to the Internet.
- The IP address of the RADIUS server group is 1.1.1.2.
- Set the shared key for the system to exchange packets with the RADIUS server as name.

Figure 4-22 802.1X Network diagram



Configuration procedure

1. Configuring the server

Server:

Configure NAS authentication device 1.1.1.1 and communication key name.

In this example, freeradius is used as the server. The main configuration is as follows:

vim /etc/freeRADIUS/3.0/clients.conf

Add

client 1.1.1.1 {

ipaddr = 1.1.1.1

secret = name

}

Add the user account test password test.

cat /etc/freeRADIUS/3.0/mods-config/files/authorize | grep 'password'

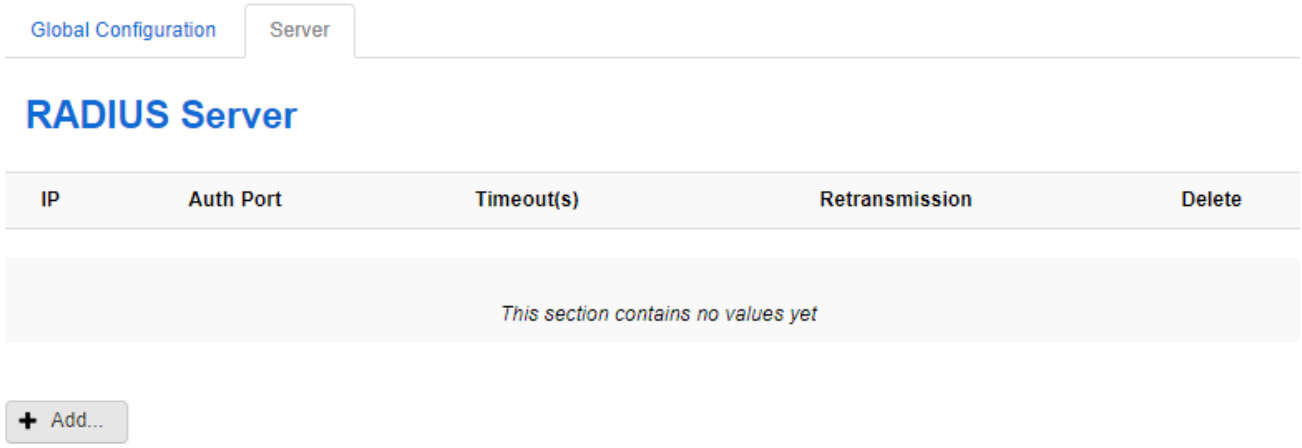
test Cleartext-Password: = 'test'

The sever should support the corresponding authentication method, such as EAP-MSCHAPv2.

2. Configure the RADIUS server

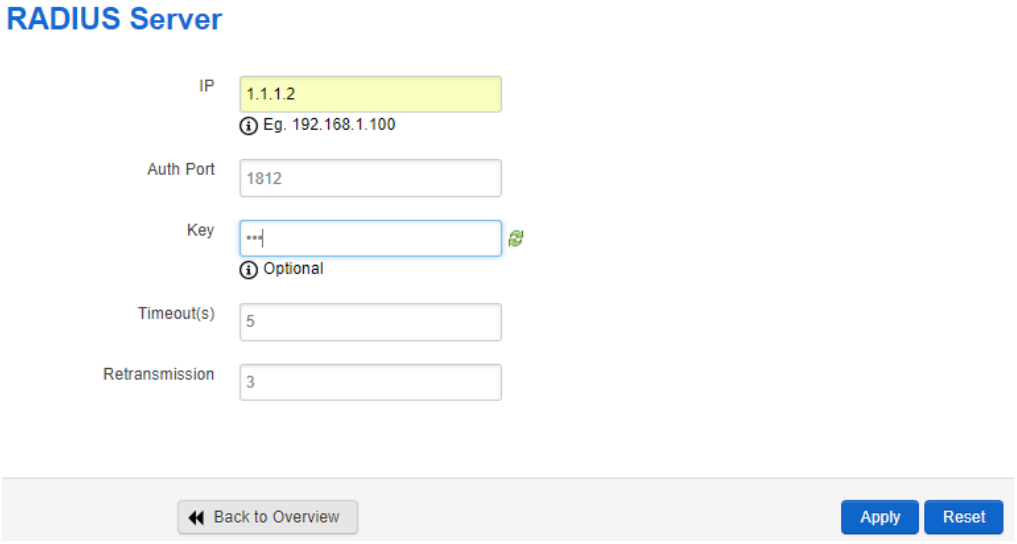
1) Select Security > RADIUS > Sever from the navigation area. The system automatically displays the RADIUS Sever Page, as shown in Figure 4-23.

Figure 4-23 RADIUS Sever



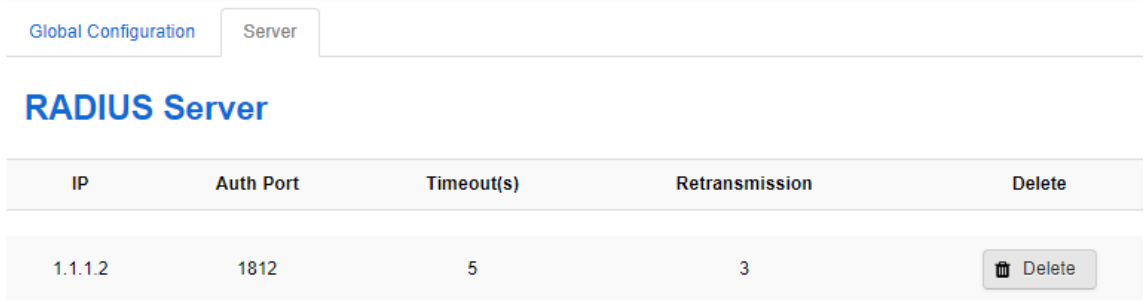
2) Click the +Add button to enter the RADIUS Sever Configuration page as shown in Figure 4-24. Configure the IP ‘1.1.1.2’, the Auth port ‘1812’, tpye the password in the Key box, the timeout period is the default 5S, and the number of retransmissions is 3.

Figure 4-24 RADIUS Sever Configuration



3) Click Apply to end the configuration. The system automatically returns the RADIUS Sever Displayed page, as shown in Figure 4-25 you can see the RADIUS server created.

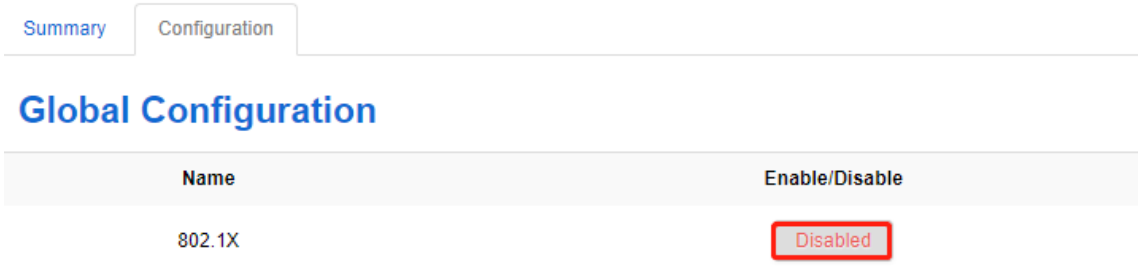
Figure 4-25 RADIUS server created



3. Enable 802.1X authentication Globally

Select Security > 802.1X > Configuraiton from the navigation area. The system automatically displays the 802.1X Global Configuration Page, as shown in Figure 4-26. Click the enable button to enable 802.1X authentication Globally.

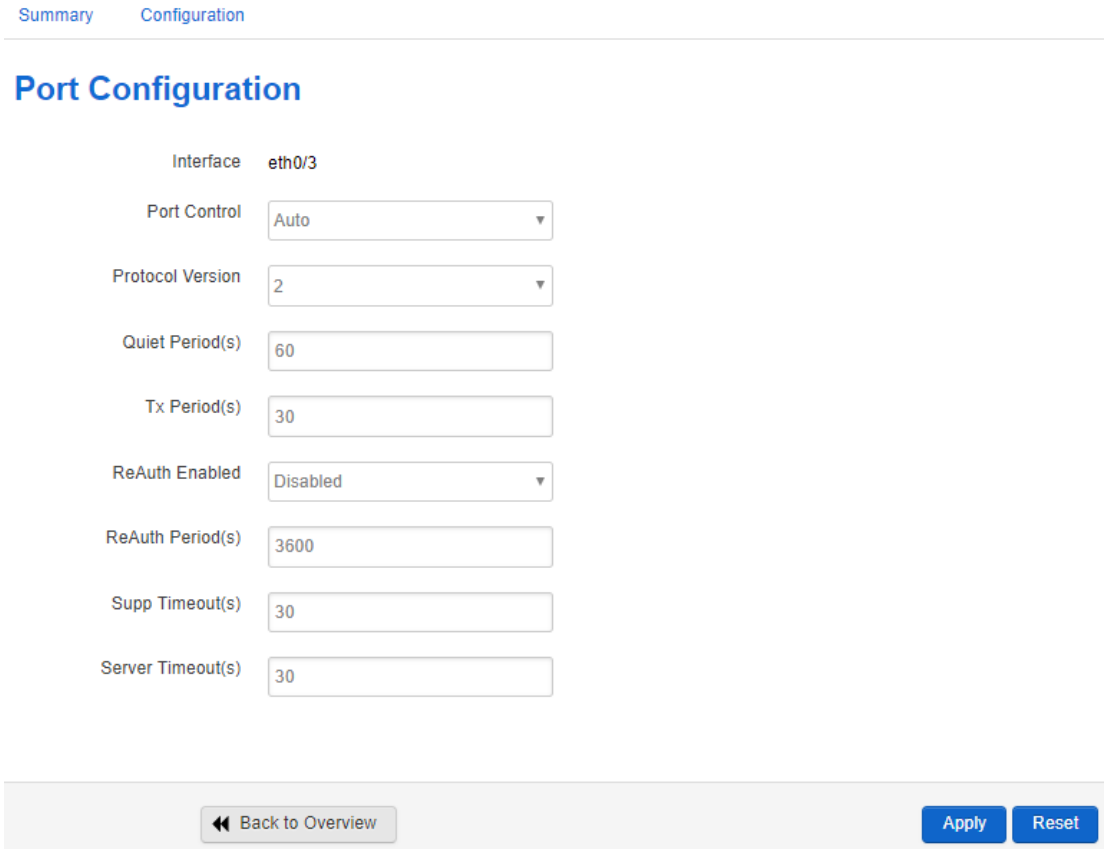
Figure 4-26 RADIUS server created



4. Configure gigabitEthernet0/3 to enable 802.1X authentication

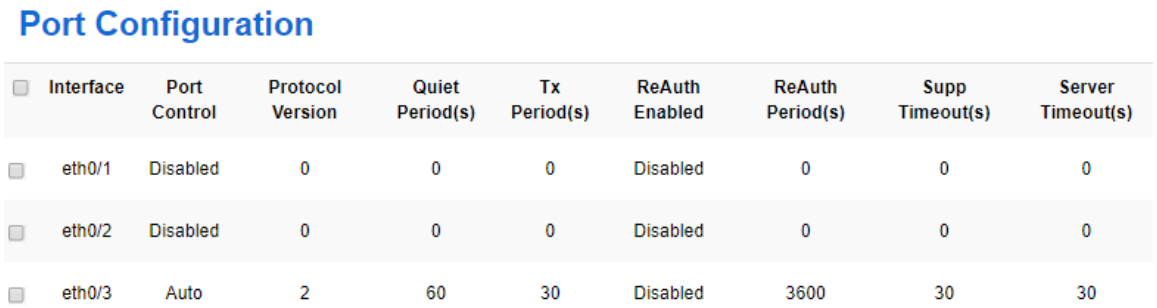
1. Select Security > 802.1X > Port Configuraiton from the navigation area. The system automatically displays the 802.1X Port Configuration Displayed Page, as shown in Figure 4-19. Select interface gigabitEthernet0/3, click Edit to enter the Port Configuration Page, as shown in Figure 4-27. Configure Port Control 'Auto', Protocol Version '2', Quite Period '60', Tx Period '30', ReAuth Enabled 'disable', ReAuth Period '3600', Supp Timeout '30', Server Timeout '30'.

Figure 4-27 802.1X Port Configuration



2. Click Apply to end the configuration. The system automatically returns the Port Configuration Displayed page, as shown in Figure 4-28, you can see the interface gigabitEthernet0/3 was enabled.

Figure 4-28 802.1X Port Configuration Displayed page



5. Configure the authentication client

Enable the 802.1X authentication client and log in using the account test.

The client should support the corresponding authentication method, such as the EAP-MSCHAPv2 method.

4.5 MAC Authentication

4.5.1 Overview

Authentication of MAC addresses is supported using a RADIUS server that contains a database of all valid users.

When the mac-auth option is enabled on any interface, all source MAC addresses from any incoming frame are sent for authentication. If the username and password of the source address are configured in the RADIUS server, then authentication succeeds, otherwise it fails. When authentication succeeds, the source MAC is added to the forwarding table with forwarding enabled. In the case of failure, the source MAC either is added to the forwarding table as discarded or is added to a restricted VLAN.

NOTE:

- If the configured static MAC is the same as the silent MAC, the MAC silent function after the MAC address authentication fails will be invalid.

4.5.2 Configuring MAC authentication

Displaying MAC Authentication Summary

Select Security > MAC Authentication > Summary from the navigation area. The system automatically displays the MAC Authentication summary, as shown in Figure 4-29. Table 4-17 describes the MAC Authentication Summary items.

Figure 4-29 The MAC Authentication Summary

Table 4-17 The MAC Authentication Summay items

Item		Description
Summary	VID	User’ s VLAN ID
	MAC	User’ s MAC
	MAC Address Aging	enable MAC aging
	Forwarding	MAC forwarding status
	Interface	User's port
	Timestamp	MAC generation time
	Delete	Click to delete

Configuring MAC Authentication

Select Security > MAC Authentication > Configuration from the navigation area. The system automatically displays the MAC Authentication Global Configuration and Port Configuration, as shown in Figure 4-30 and Figure 4-31. Table 4-18 describes the Global Configuration and Port Configuration items.

Figure 4-30 MAC Authentication Global Configuration

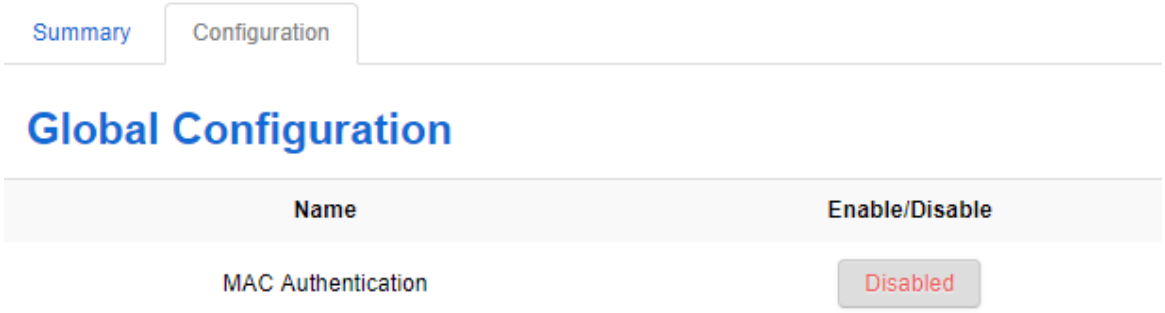


Figure 4-31 MAC Authentication Port Configuration

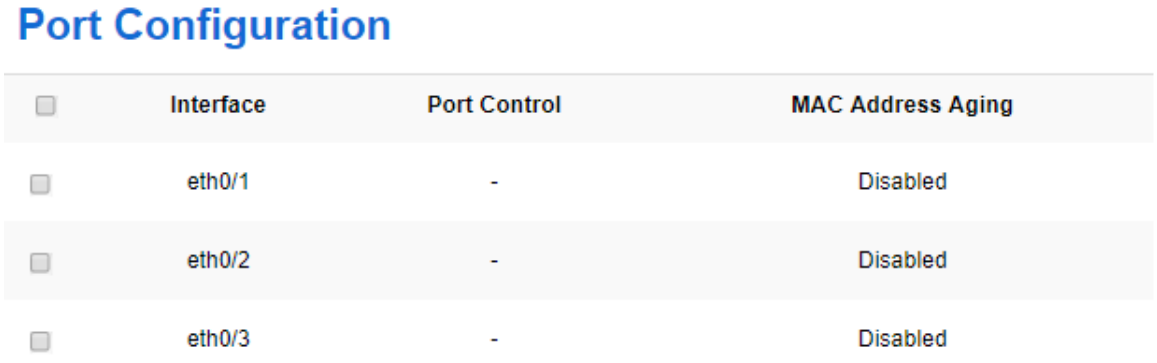


Table 4-18 The MAC Authentication Configuration items

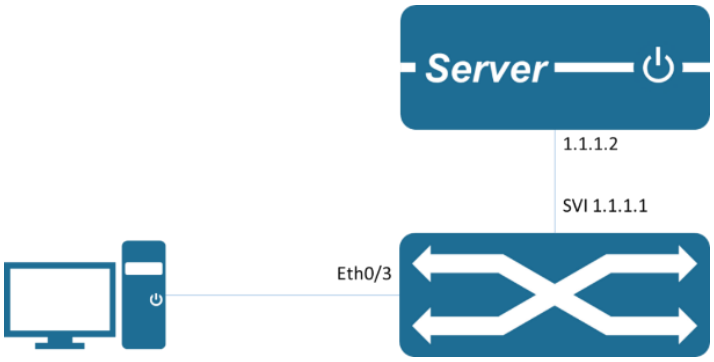
Item	Description	
Global Configuration	Enable/Disable	Enables the 802.1X feature on your switch.
Portl Configuration	Interface	Physical interface name
	Port Control	Port control mode
	MAC Address Aging	Enable mac aging

4.5.3 Configuration Example

Network requirements

- As shown in Figure 4-32 the access user is authenticated on GigabitEthernet0/3 to control access to the Internet.
- The IP address of the RADIUS server group is 1.1.1.2.
- Set the shared key for the system to exchange packets with the RADIUS server as name.

Figure 4-32 802.1X Network diagram



Configuration procedure

1. Configuring the server

Server:

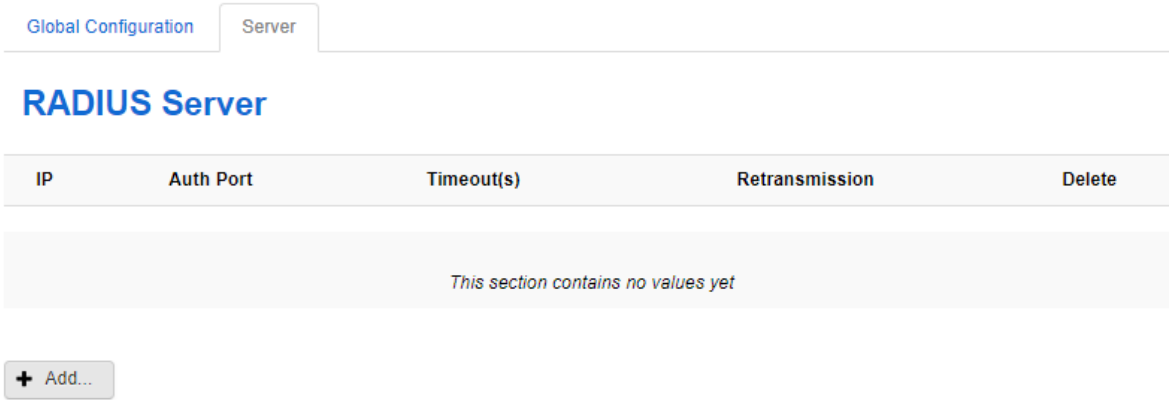
Configure NAS authentication device 1.1.1.1 and communication key name.

Add the client MAC address as a user account and password to the user database.

2. Configure the RADIUS server

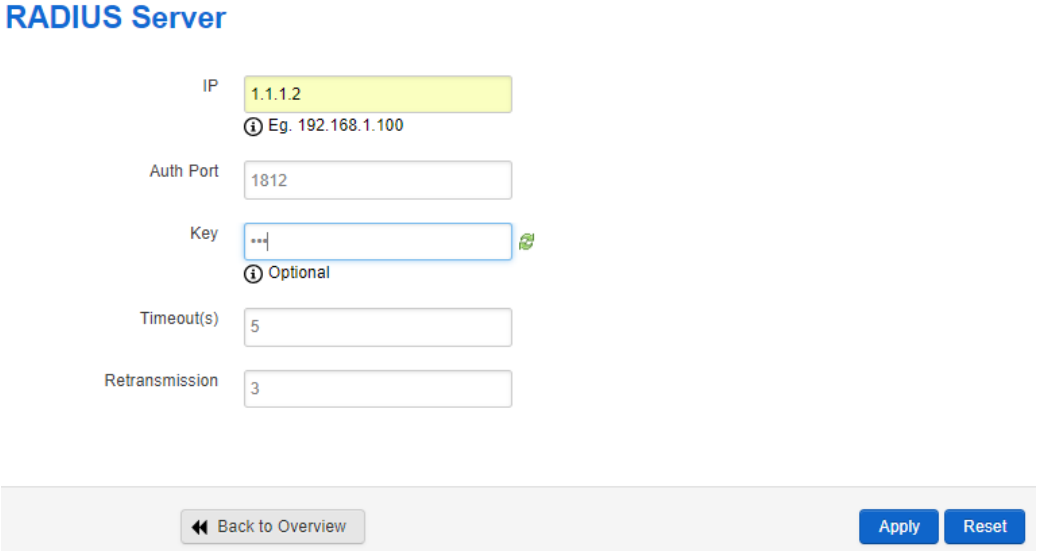
1) Select Security > RADIUS > Sever from the navigation area. The system automatically displays the RADIUS Sever Page, as shown in Figure 4-33.

Figure 4-33 RADIUS Sever



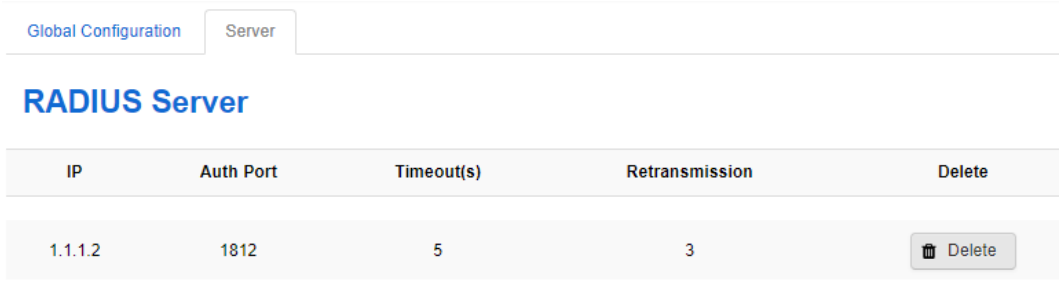
2) Click the +Add button to enter the RADIUS Sever Configuration page as shown in Figure 4-34. Configure the IP ‘1.1.1.2’, the Auth port ‘1812’, tpye the password in the Key box, the timeout period is the default 5S, and the number of retransmissions is 3.

Figure 4-34 RADIUS Sever Configuration



3) Click Apply to end the configuration. The system automatically returns the RADIUS Sever Displayed page, as shown in Figure 4-35 you can see the RADIUS server created.

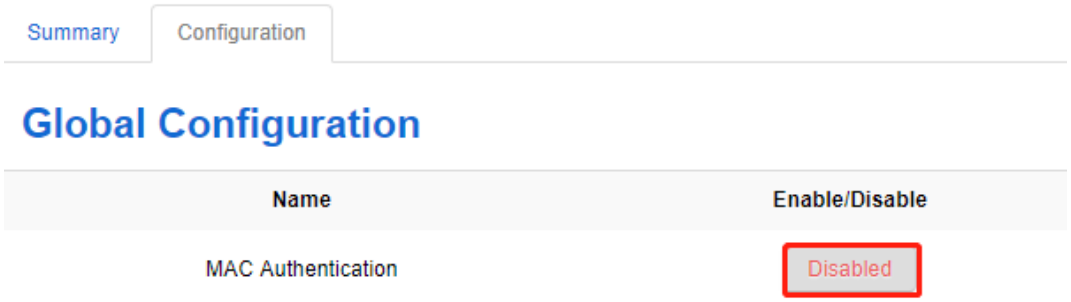
Figure 4-35 RADIUS server created



3. Enable MAC Authentication Globally

Select Security > MAC Authentication > Configuraiton from the navigation area. The system automatically displays the MAC Authentication Global Configuration Page, as shown in Figure 4-36. Click the enable button to enable MAC authentication Globally.

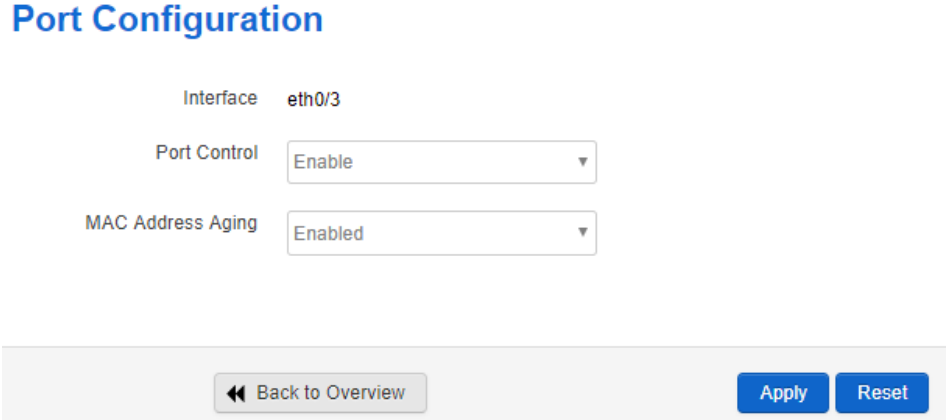
Figure 4-36 Enable MAC Authentication



4. Configure gigabitEthernet0/3 to enable MAC authentication

1. Select Security > MAC Authentication > Port Configuraiton from the navigation area. The system automatically displays the MAC Port Configuration Displayed Page, as shown in Figure 4-31. Select interface gigabitEthernet0/3, click Edit to enter the Port Configuration Page, as shown in Figure 4-37. Configure Port Control ‘Enable’, MAC Address Aging ‘Enable’.

Figure 4-37 MAC Port Configuration



2. Click Apply to end the configuration. The system automatically returns the Port Configuration Displayed page, as shown in Figure 4-38, you can see the interface gigabitEthernet0/3 was enabled.

Figure 4-38 MAC Port Configuration Displayed page

Port Configuration

	Interface	Port Control	MAC Address Aging
☐	eth0/1	-	Disabled
☐	eth0/2	-	Disabled
☐	eth0/3	Enable	Enabled

5. Configure Client access automatic authentication

Start the client, access the network, and trigger MAC authentication.

4.6 RADIUS

4.6.1 Overview

Remote Authentication Dial-In User Service (RADIUS) is protocol for implementing Authentication, Authorization, and Accounting (AAA).

RADIUS is a distributed information interaction protocol using the client/server model. RADIUS can protect networks against unauthorized access and is often used in network environments where both high security and remote user access are required. RADIUS uses UDP, and its packet format and message transfer mechanism are based on UDP. It uses UDP port 1812 for authentication and 1813 for accounting.

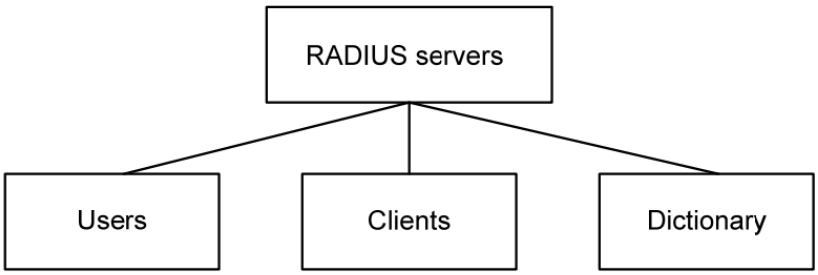
RADIUS was originally designed for dial-in user access. With the diversification of access methods, RADIUS has been extended to support more access methods, for example, Ethernet access and ADSL access. It uses authentication and authorization in providing access services and uses accounting to collect and record usage information of network resources.

Client/server model

- Client: The RADIUS client runs on the NASs located throughout the network. It passes user information to designated RADIUS servers and acts on the responses (for example, rejects or accepts user access requests).
- Server: The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access. It listens to connection requests, authenticates users, and returns the processing results (for example, rejecting or accepting the user access request) to the clients.

In general, the RADIUS server maintains three databases: Users, Clients, and Dictionary, as shown in Figure 4-39.

Figure 4-39 RADIUS server components



- Users: Stores user information such as the usernames, passwords, applied protocols, and IP addresses.
- Clients: Stores information about RADIUS clients, such as the shared keys and IP addresses.
- Dictionary: Stores information about the meanings of RADIUS protocol attributes and their values.

Security and authentication mechanisms

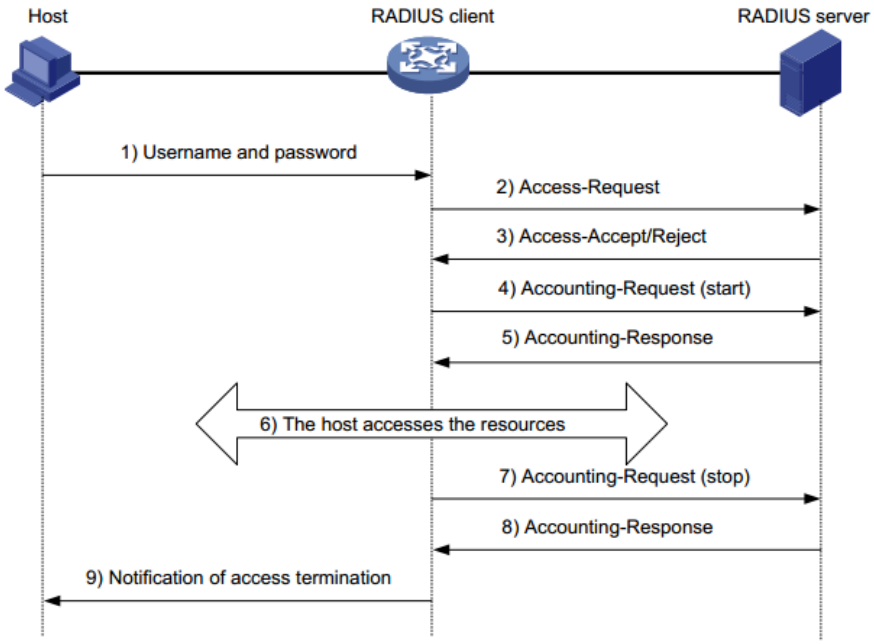
Information exchanged between a RADIUS client and the RADIUS server is authenticated with a shared key, which is never transmitted over the network. This enhances the information exchange security. In addition, to prevent user passwords from being intercepted on insecure networks, RADIUS encrypts passwords before transmitting them.

A RADIUS server supports multiple user authentication methods, for example, the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) of the Point-to-Point Protocol (PPP). Moreover, a RADIUS server can act as the client of another AAA server to provide authentication proxy services.

Basic message exchange process of RADIUS

Figure 4-40 illustrates the interaction of the host, the RADIUS client, and the RADIUS server.

Figure 4-40 Basic message exchange process of RADIUS



The following is how RADIUS operates:

1. The host initiates a connection request carrying the username and password to the RADIUS client.

2. Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.

3. The RADIUS server authenticates the username and password. If the authentication succeeds, it sends back an Access-Accept message containing the user ‘s authorization information. If the authentication fails, it returns an Access-Reject message.

4. The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.

5. The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.

6. The user accesses the network resources.

7. The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.

8. The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.

9. The user stops access to network resources

NOTE:

- XPTN series switch do not support RADIUS accounting function

4.6.2 Configuring RADIUS

RADIUS global configuration

Select Security > RADIUS > Global Configuration from the navigation area. The system automatically displays the RADIUS Global Configuration, as shown in Figure 4-41. Table 4-19 describes the RADIUS Global Configuration items.

Figure 4-41 The RADIUS Global Configuration

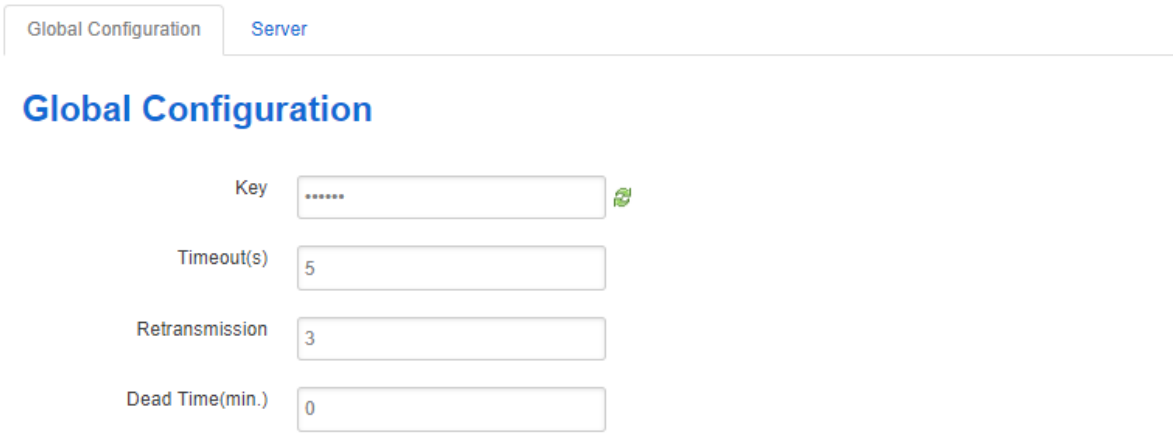


Table 4-19 The RADIUS Global Configuration items

Item		Description
Global Configuration	Key	Global default password configuration; onfigurable, unreadable; optional configuration
	Timeout	Global server timeout; optional configuration
	Retransmission	Global server retransmissions; optional configuration
	Dead Time	Server death duration; optional configuration; default 0, indicating that the server will be revived immediately after death

RADIU Server configuration

Select Security > RADIUS > Server from the navigation area. The system automatically displays the RADIUS Server Configuration, as shown in Figure 4-42. Table 4-20 describes the RADIUS Server Configuration items.

Figure 4-42 The RADIUS Server Configuration

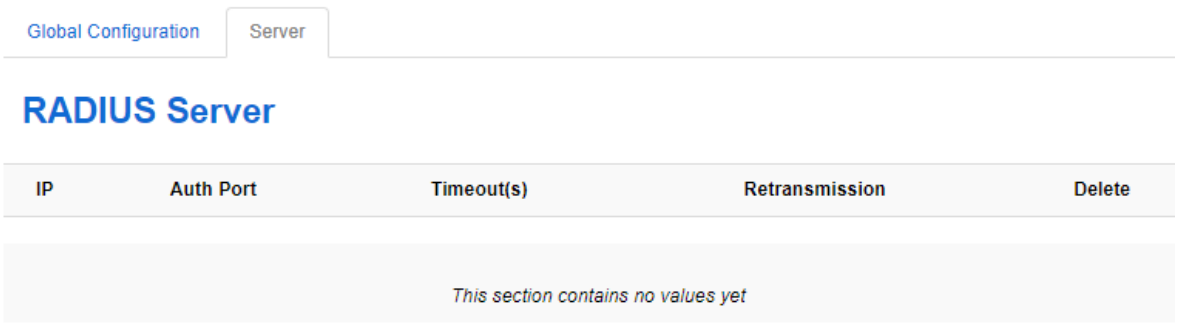


Table 4-20 The RADIUS Server Configuration items

Item	Description
IP	Server IP address
Auth Port	Server authentication port number; default 1812
Key	Server key; global configuration when not configured
Timeout	Server timeout; default 5s
Retransmission	Server retransmission times, default 3 times

4.6.3 RADIUS Configuration Example

For details about RADIUS Configuration, refer to 4.1.3 802.1X Configuration Example

4.7 Port Security

4.7.1 Overview

The Port Security function restricts the number of valid MAC addresses on the port to limit the access of illegal users to the port. The illegal MAC packets will be directly discarded.

The legal MAC can be generated statically or dynamically. The static legal MAC is generated through user command line configuration; the dynamic legal MAC is dynamically generated through the MAC address learning function.

When the number of secure addresses on the port has reached the configured value of the maximum number of secure addresses, the new MAC access port will be recognized as an illegal MAC and a violation event will be generated. The user can configure the actions to be taken when the violation event occurs, respectively restrict or shutdown the port.

Restrict: Prohibit illegal MAC data from passing, and generate alarm log prompt information. Illegal MAC will prohibit access to the port within the MAC address aging time. It can be restored through shutdown and no shutdown ports.

Shutdown: The port is forced to be down, and the port recovery time can be configured. The port will automatically recover when the time is up; it can also be recovered by the shutdown, no shutdown command.

If you want to convert a dynamic security user to a static security user, you can enable the sticky function on the port. When the sticky function is enabled on the port, the dynamic users learned on the port will exist as static users. If the configuration is saved, the device will still exist after restarting the device.

NOTE:

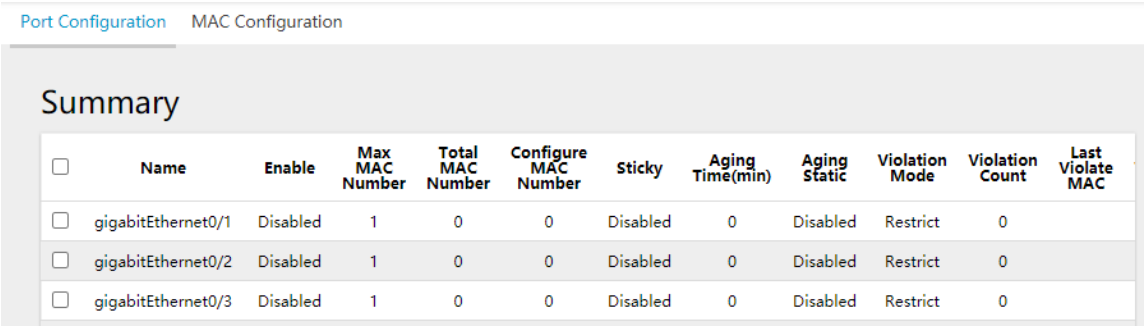
- Only support L2 port configuration port security, such as ordinary physical port, aggregation port.
- Only support port security configuration in access mode.
- Does not support aggregation port member ports to configure port security functions.
- Does not support SPAN destination port configuration port security function.
- Does not support configuring port security functions on ports that have been configured with static MAC addresses.

4.7.2 Configuring Port Security

Port Configuration

Select Security > Port security in the navigation area to enter the Port security page as shown in Figure 4-43.

Figure 4-43 Port Security statistic page



Check the box in front of the interface, click Edit to enter the Port Configuration page, as shown in Figure 4-44. The items of the port configuration are described in Table 4-21.

Figure 4-44 Port Security configuration page

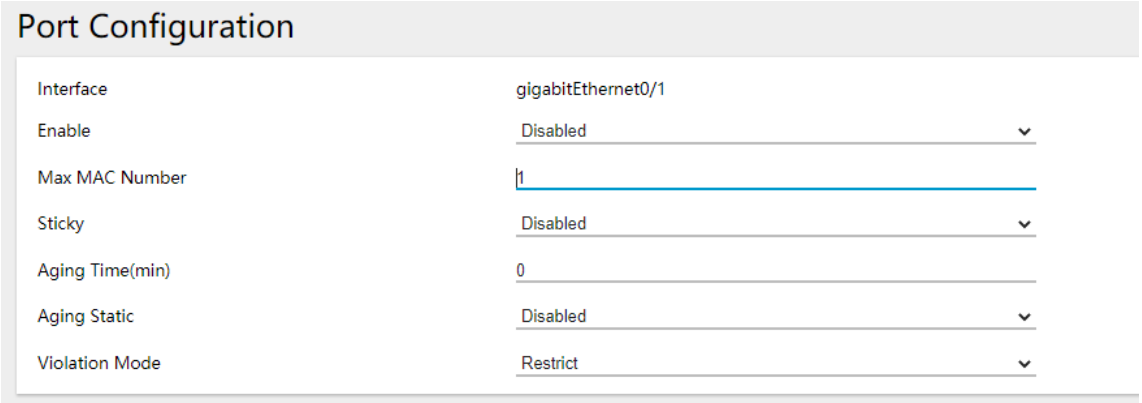


Table 4-21 the items of the port security configuration

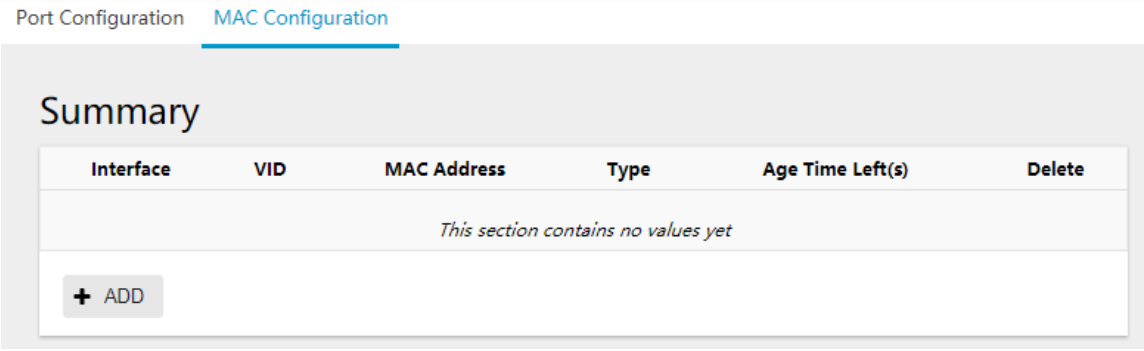
Item		Description
Port Configuration	Enable	Enable/disable port Security of the interface.
	Max MAC Number	Configure the maximum number of secure MAC addresses for the port, the default maximum number of secure addresses is 1, the range is <1-1024>
	Sticky	Turn on/off the Sticky function.

	Aging Time(min)	Configure the security address aging time, in minutes. The default aging time is 0, which means that the aging function is turned off. Aging tiem range <0-1440> The default aging function only takes effect for dynamic and sticky security addresses.
	Aging Static	Enable the static security address aging function.
	Violation Mode	Configure port security violation handling, default violation mode is Restrict. Restrict：Prohibit illegal user data from passing, and log prompt Shutdown：shutdown interface，and resume passing after errdisable recovery time.

MAC Configuration

Select Security > Port security > MAC Configuration in the navigation area to enter the Port security page as shown in Figure 4-45.

Figure 4-45 Mac configuration summary



Click +ADD to enter the page of MAC Configuration page as shown in Figure 4-46.

Figure 4-46 Mac configuration page

The items of the mac configuration are described in Table 4-22.

Table 4-22 the items of the mac configuration

Item		Description
MAC Configuration	Interface	Select the interface to be configured.
	VID	Specify the management VLAN ID.
	MAC Address	Configure a static security address, the format of the security address: XXXX.XXXX.XXXX The security address cannot be a broadcast or multicast Address.
	Type	Configure the MAC address as dynamic or static.
	Age time left	The remaining aging time of the current MAC address, in seconds.
	Delete	Delete the current MAC address, only valid for static addresses and dynamic addresses with sticky enabled.

4.7.3 Configuration Example

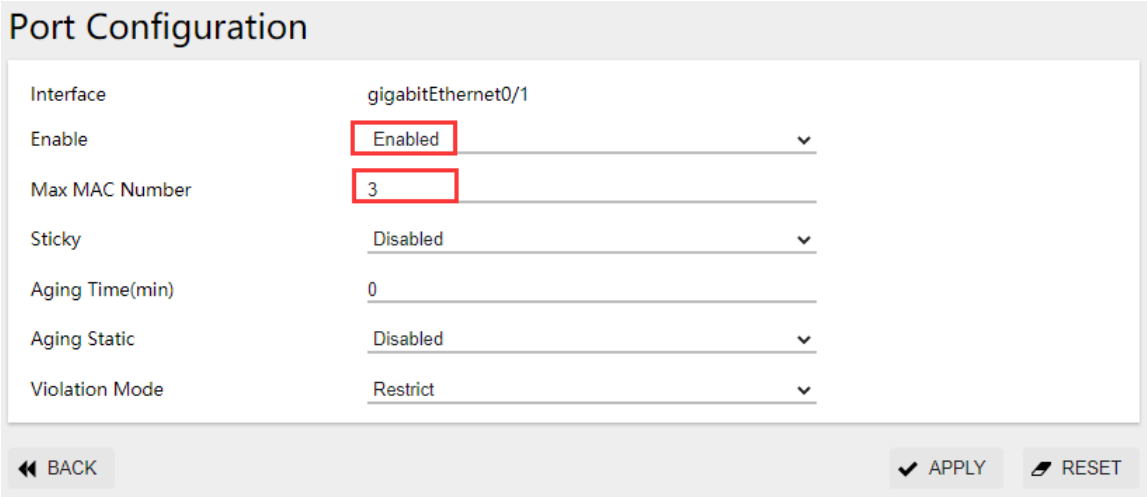
Network requirements :

Limit the number of legal users on interface GigabitEthernet 0/1 to 3, and illegal users whose MACs are 0001.0001.0001, 0001.0001.0002, and 0001.0001.0003 cannot access the device.

Configuration procedure :

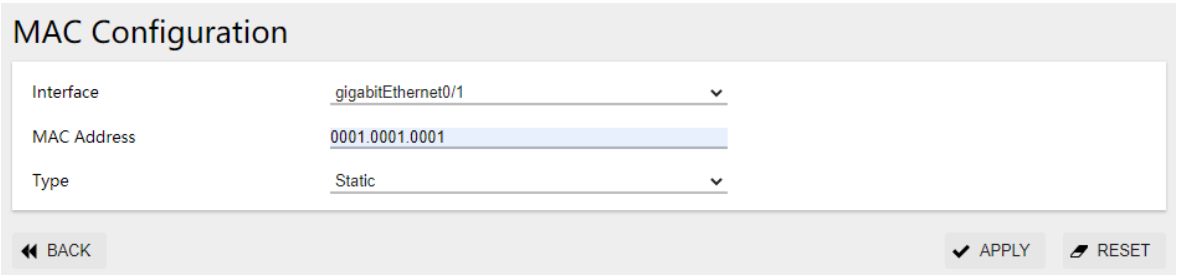
(1) Select Security > Port Security from the navigation area, check the box in front of the gigabitEthernet 0/1, click EDIT to enter the page of Port Configuration, as shown in Figure 4-47.

Figure 4-47 Port Security configuration page



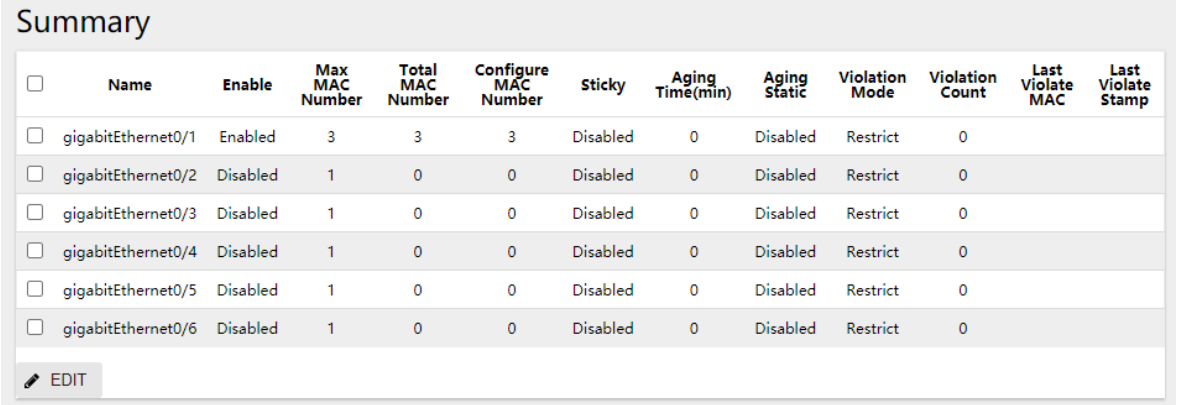
(2) Click MAC Configuration in the current page, click +ADD to enter MAC configuration page, as shown in Figure 4-48. Text the mac address 0001.0001.0001, 0001.0001.0002, and 0001.0001.0003 into the MAC Address table separately, click Apply.

Figure 4-48 Mac configuration



(3) The rules were created successfully in the summary page as shown in Figure 4-49.

Figure 4-49 Port Security statistic page



(4) Click Save in the navigation area.

4.8 IP Source Guard

4.8.1 Overview

IP Source Guard：

The IP Source Guard binding function allows IP packets conforming to the IP+MAC binding to pass through the port, and non-conforming packets are directly discarded, thereby achieving the purpose of preventing IP/MAC spoofing attacks.

The binding entries of IP Source Guard mainly come from two sources: user static configuration and dynamic acquisition in the IP DHCP snooping environment.

User static configuration: mainly for host users whose IP addresses are statically configured in the local area network.

IP DHCP snooping dynamic acquisition: mainly respond to the host users who dynamically acquire the IP address through DHCP in the local area network.

IP/MAC spoofing attack: Illegal MAC users send IP packets with legal source IP to realize the legalization of access identity.

ARP Check：

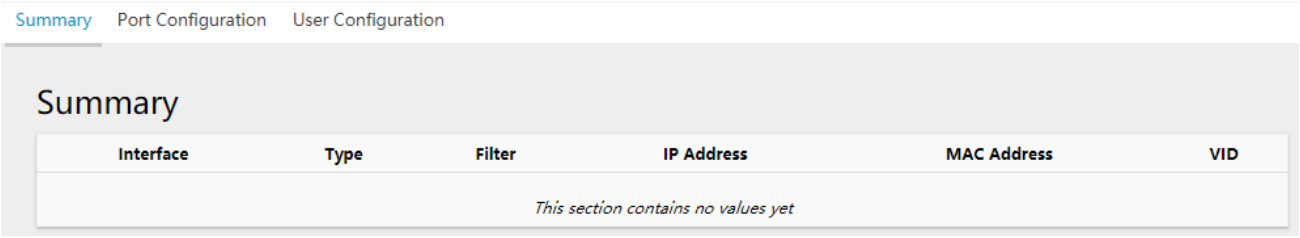
The Arp-check (ARP packet check) function filters all ARP packets under the port and discards all illegal ARP packets, which can effectively prevent ARP spoofing in the network and improve the stability of the network.

In the divice that supports the Arp-check function, the Arp-check function can generate corresponding ARP filtering information based on the legal user information (IP+MAC) generated by the security application modules such as IP Source Guard, so as to realize the illegal ARP packets filtering in the network.

4.8.2 Configuring IP Source Guard

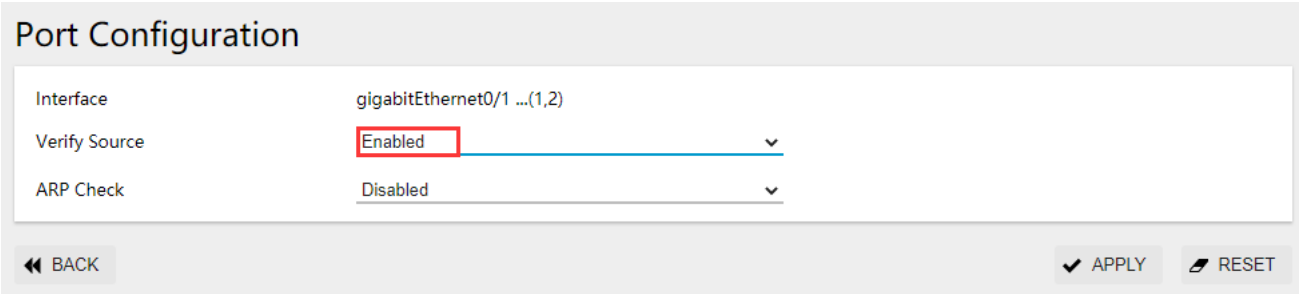
(1) Select Security > IP Source Guard in the navigation area to enter the IP Source Guard Summary page as shown in Figure 4-50.

Figure 4-50 IP source guard Summary



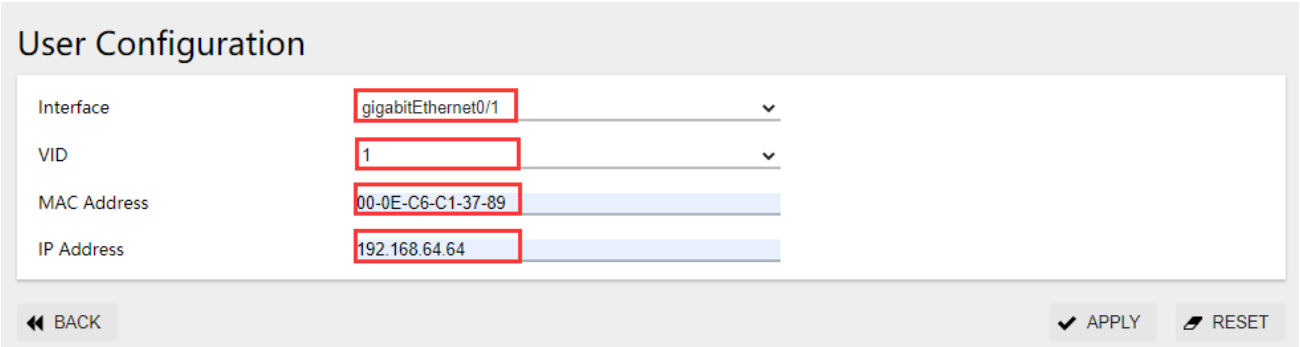
(2) Click Port Configuration in the current page, check the box in front of the interface to be configured, click EDIT to enter the port configuration page was shown in Figure 4-51, enable Verify Source function.

Figure 4-51 IP source guard port configuration



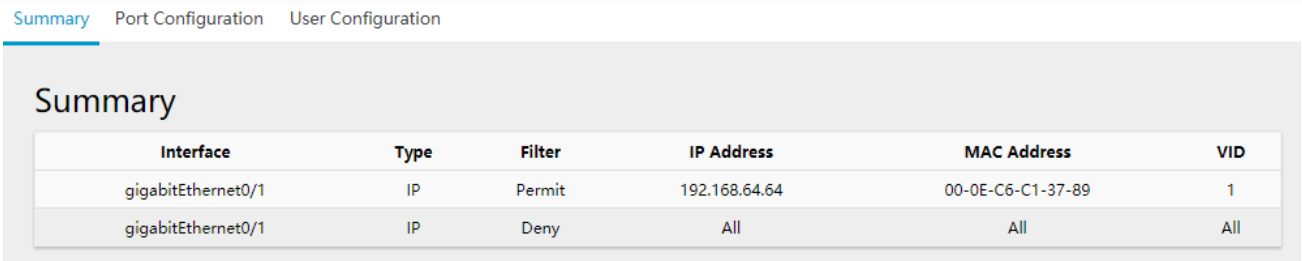
(3) Select User Configuration in current page, click +ADD to enter the user configuration page, as shown in Figure 4-52.

Figure 4-52 IP source guard user configuration



(4) Click APPLY button, the rules created were displayed in summary page as shown in Figure 4-53.

Figure 4-53 IP source guard rules Summary

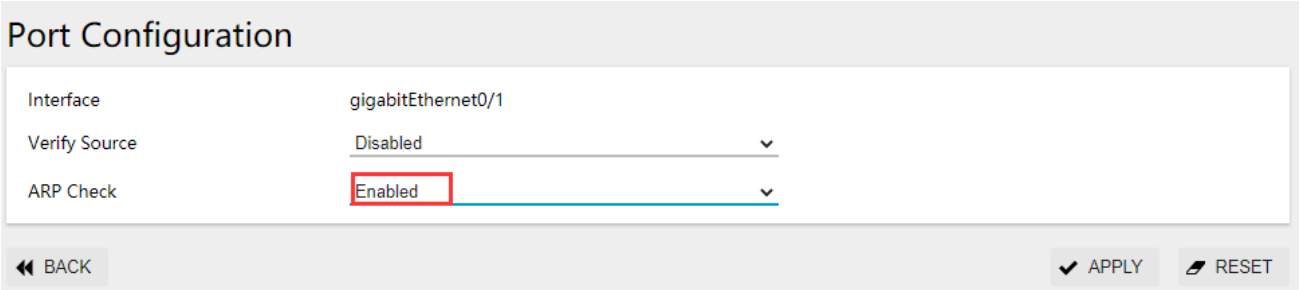


4.8.3 Configuring ARP Check

(1) Select Security > IP Source Guard in the navigation area to enter the IP Source Guard Summary page as shown in Figure 4-54.

(2) Click Port Configuration in the current page, check the box in front of the interface to be configured, click EDIT to enter the port configuration page was shown in Figure 4-12, enable ARP check function.

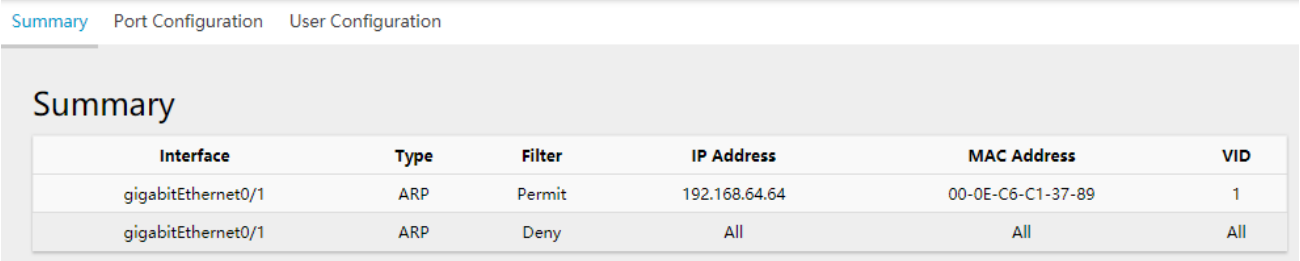
Figure 4-54 IP Source Guard ARP Check



(3) Select User Configuration in current page, click +ADD to enter the user configuration page, as shown in Figure 4-52.

(4) Click APPLY button, the rules created were displayed in summary page as shown in Figure 4-55.

Figure 4-55 ARP Check rules



5 System

5.1 Management IP Address

Select System > Management IP Address from the navigation area to enter the Management IP Address page, as shown in Figure 5-1. Table 5-1 lists the configuration items of the Management IP Address.

Figure 5-1 Management Information page

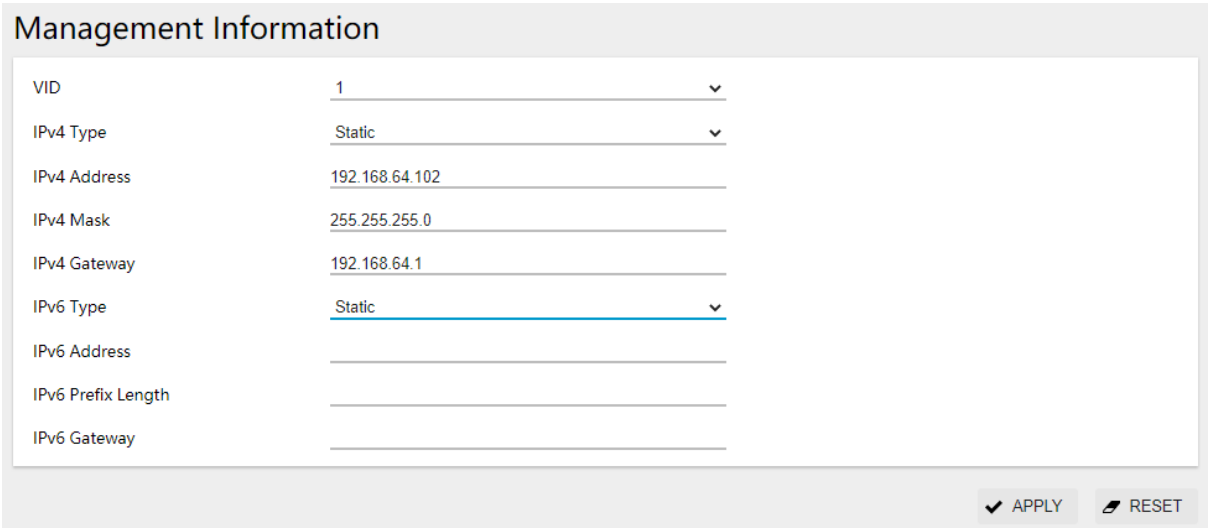


Table 5-1 Management Information configuration items

Item	Description
VID	Specify the management VLAN ID. The default management VLAN is 1.
IPv4 Type	None：IPv4 management address is not used. Static：Select this option to manually specify an IPv4 address and the mask length DHCP：Select the option to get an IPv4 address through DHCP.
IPv4 Address	Specify the IPv4 management address. The default IP is 192.168.2.1.
IPv4 Mask	Specify the IPv4 management mask. The default mask is 255.255.255.0.
IPv4 Gateway	Specify the IPv4 management gateway.
IPv6 Type	None：IPv6 management address is not used. Static：Select this option to manually specify an IPv6 address and the mask length.

	DHCP：Select the option to get an IPv6 address through DHCP.
IPv6 Address	Specify the IPv6 management address.
IPv6 Prefix Length	Specify the IPv6 management address prefix length.
IPv6 Gateway	Specify the IPv6 management gateway.

5.2 User Management

In the user management part, you can:

- Set the username, password.
- Create a new user.

Select System > User Management from the navigation area to enter the User Management page, as shown in Figure 5-2. Table 5-2 lists the configuration items of the User Management.

Figure 5-2 User Management page

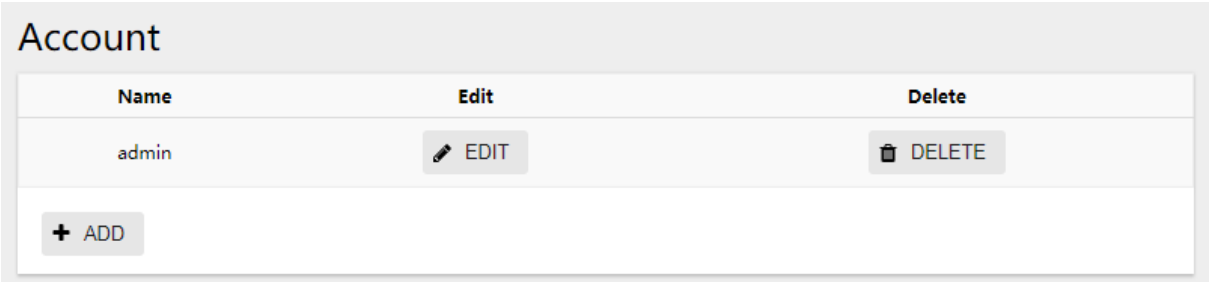


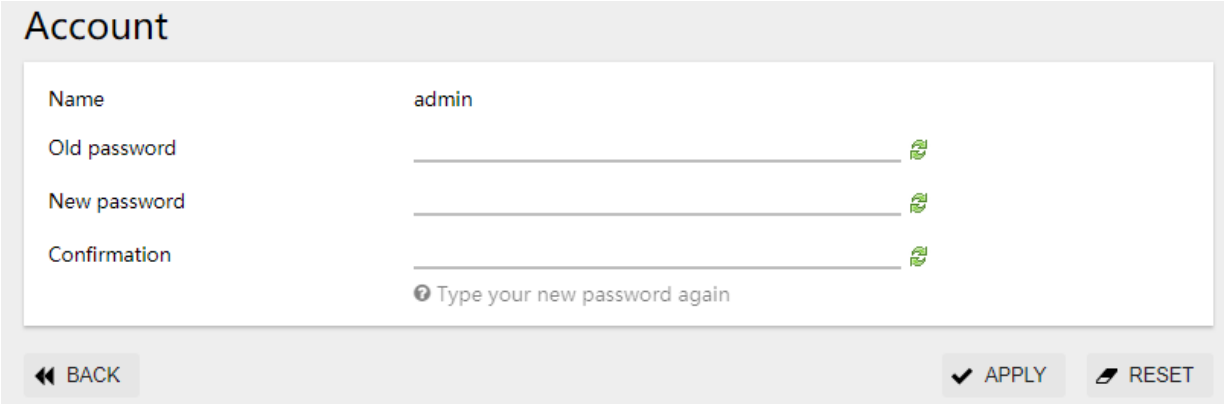
Table 5-2 Account configuration items

Item		Description
Account	Name	User name
	Edit	Click to change the password
	Delete	Click to delete the user account
	+Add...	Click to create a new user

Setting the password

1. Select System > User Management from the navigation area to enter the User Management page, as shown in Figure 5-3.

Figure 5-3 User Management page



2. Type Old password in the Old password box, the default password is admin.

3. Type new password in the New password box.

4. Type the same password again in the Confirmation box.

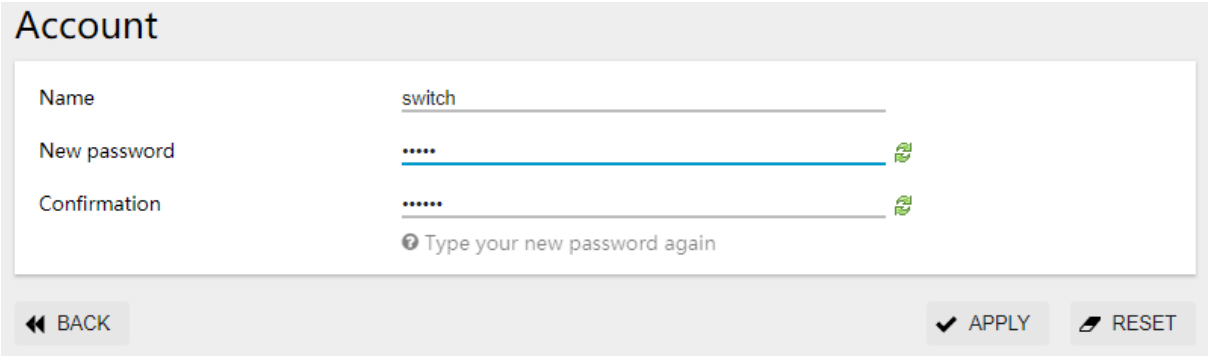
5. Click Apply.

6. Click Save in the navigation area.

Creating a new user

1.Select System > User Management from the navigation area to enter the User Management page, as shown in Figure 5-4.

Figure 5-4 User Management page



2. Type a new user name in the Name box.

3. Type new password in the New password box.

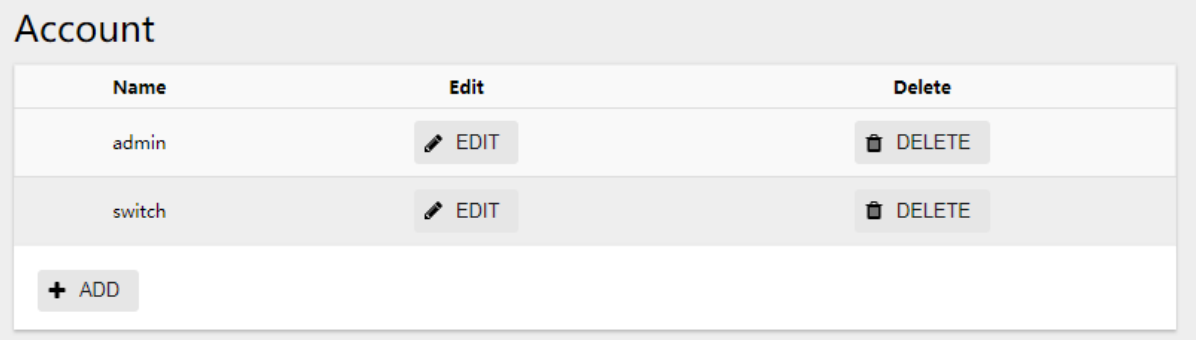
4. Input the same password again in the Confirmation box.

5. Click Apply.

6. Click Save in the navigation area.

7. The new user account was created in the Account page as shown in Figure 5-5.

Figure 5-5 User Management page



5.3 Service

5.3.1 Overview

The service management module provides the following types of services: FTP, Telnet, SSH, SFTP, HTTP and HTTPS. You can enable or disable the services as needed. In this way, the performance and security of the system can be enhanced, thus secure management of the device can be achieved.

Telnet Server

The Telnet protocol is an application layer protocol that provides remote login and virtual terminal functions on the network.

SSH Server

Secure Shell (SSH) offers an approach to securely logging in to a remote device. By encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception

HTTP Server

The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite. You can log in to the device using the HTTP protocol with HTTP service enabled, accessing and controlling the device with Web-based network management.

HTTPS Server

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol. The SSL protocol of HTTPS enhances the security of the device in the following ways:

- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;
- Encrypts the data exchanged between the HTTPS client and the device to ensure the data security and integrity, thus realizing the security management of the device;
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.

5.3.2 Configuring service

(1) Select System > Telnet Server from the navigation area to enter the Telnet Sever configuration page, as shown in Figure 5-6.

(2) Click ENABLED/DISABLED to enable/disable Telnet/SSH service.

(3) When HTTPS Server is enabled, the certificate and private key should be uploaded, as shown in figure. If no certificate is specified, the device will use the default certificate.

Figure 5-6 Server page

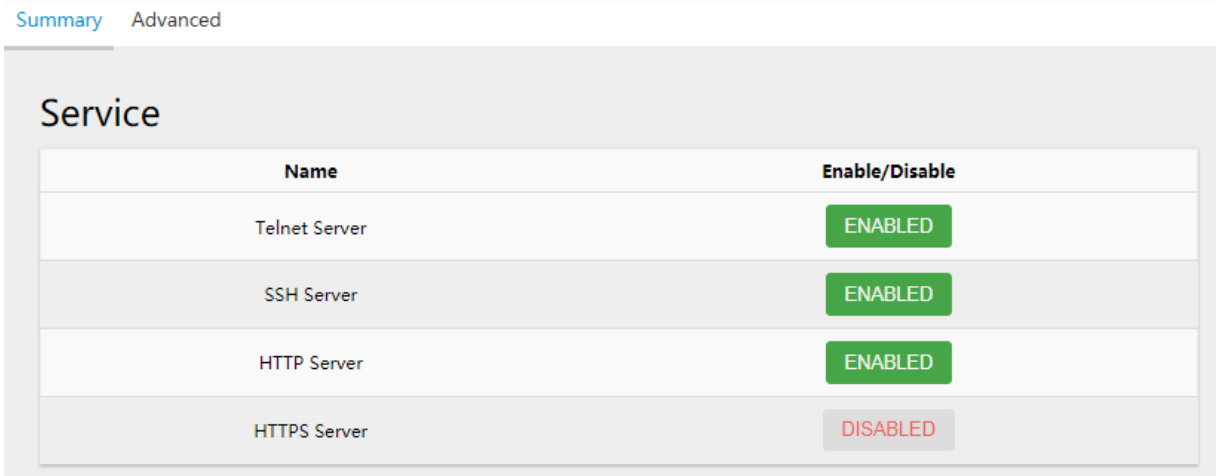
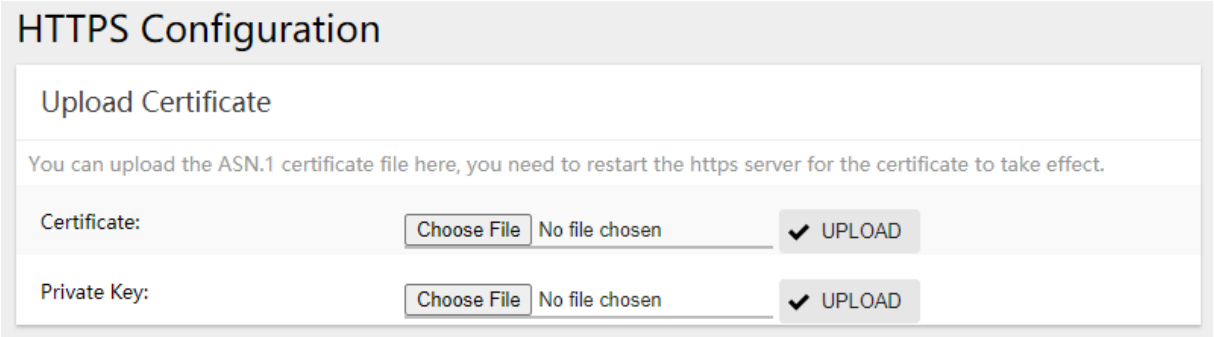


Figure 5-7 HTTPS Configuration Page



5.4 SNMP

Simple Network Management Protocol (SNMP) offers the communication rules between a management device and the managed devices on the network; it defines a series of messages, methods, and syntaxes to implement the access and management from the management device to the managed devices. SNMP has the following characteristics:

- Automatic network management. SNMP enables network administrators to search and modify information, find and diagnose network problems, plan for network growth, and generate reports on network nodes.
- SNMP shields the physical differences between various devices and thus realizes automatic management of products from different manufacturers. Offering only the basic set of functions, SNMP makes the management tasks independent of both the physical features of the managed devices and the underlying networking technology. Thus, SNMP achieves effective management of devices from different manufacturers, especially in small, high-speed, and low-cost network environments.

SNMP mechanism

An SNMP enabled network comprises Network Management Station (NMS) and agent.

- An NMS is a station that runs the SNMP client software. It offers a user-friendly interface, making it easier for network administrators to perform most network management tasks.
- An agent is a program on the device. It receives and handles requests sent from the NMS. Only under certain circumstances, such as interface state change, will the agent inform the

NMS. NMS manages an SNMP enabled network, whereas agents are the managed network device. NMS and agents exchange management information through the SNMP protocol.

SNMP provides the following four basic operations:

- Get operation: NMS gets the value of a certain variable of the agent through this operation.
- Set operation: NMS can reconfigure the value of one or more objects in the agent MIB (Management Information Base) by means of this operation.
- Trap operation: The agent sends traps to the NMS through this operation.
- Inform operation: The NMS sends traps to other NMSs through this operation.

SNMP Community Configuration

Select System > Service from the navigation area to enter the SNMP Community page, as shown in Figure 5-7. Click +Add... button to add new SNMP Community. Table 5-4 lists the configuration items of the SNMP configuration.

Figure 5-7 SNMP Community page

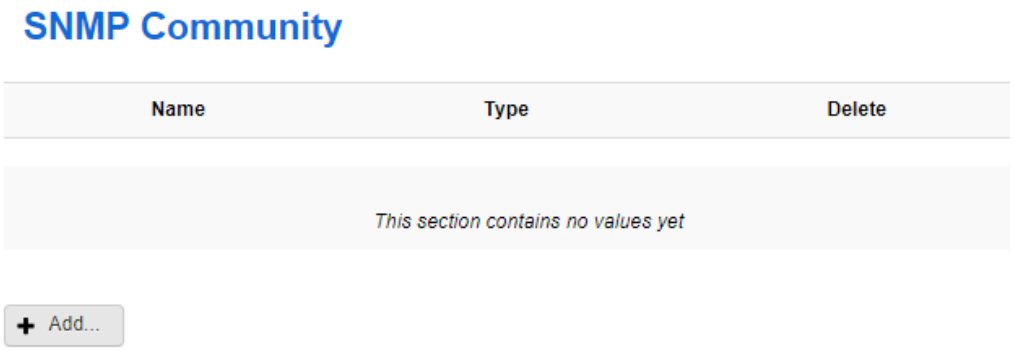


Table 5-4 SNMP Community configuration items

Item		Description
SNMP Community	Name	Display the community string.
	Type	Display the community type.
	Delete	Click this button to delete this community.
	Add	Click this button to add a new community.

SNMP Server Configuration

Select System > Service from the navigation area to enter the SNMP Sever page, as shown in Figure 5-8. Click +Add… button to add new SNMP Sever. Table 5-5 lists the configuration items of the SNMP configuration.

Figure 5-8 SNMP Sever page

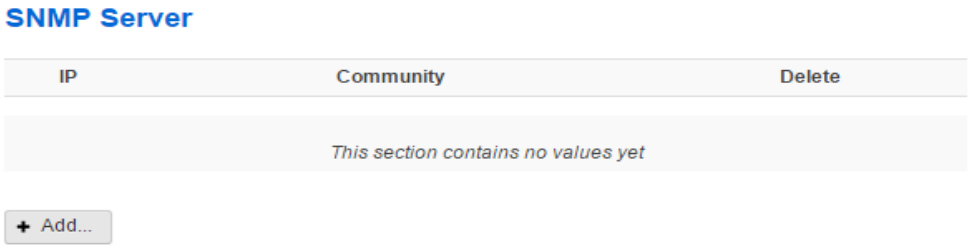


Table 5-5 SNMP Sever configuration items

Item		Description
SNMP Sever	IP	Display the server IP.
	Community	Display the community string.
	Delete	Click this button to delete this server.
	Add…	Click this button to add a new server.

5.5 Date/Time

The system time module allows you to display and set the device system time on the Web interface. The device supports setting system time through manual configuration and automatic synchronization of NTP server time.

An administrator cannot keep time synchronized among all the devices within a network by changing the system clock on each device, because this is a timeconsuming task and cannot guarantee clock precision.

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP allows quick clock synchronization within the entire

network and ensures a high clock precision so that the devices can provide diverse applications based on consistent time.

5.5.1 Date and Time interface

Select System > Date and Time from the navigation area. The system time configuration page appears by default, as in Figure 5-9. The current system time and clock status are displayed. Table 5-6 shows the network time configuration items.

Figure 5-9 System time configuration page

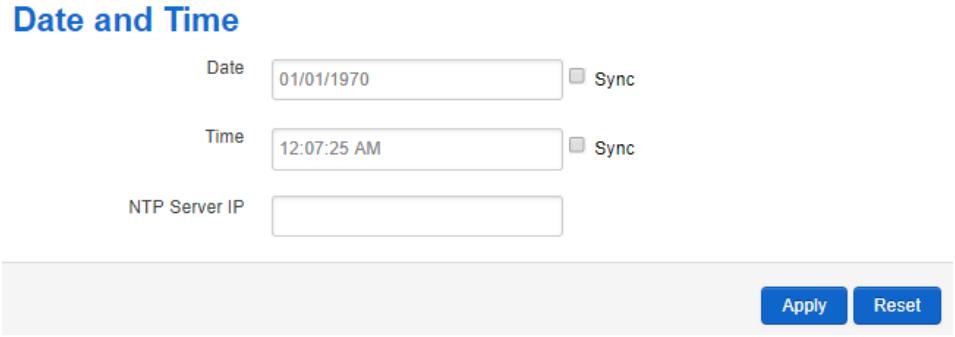


Table 5-6 System time configuration items

Item	Description
Date	System date
Time	System time
NTP Server IP	Set the NTP server IP address

5.5.2 Configuing System Time

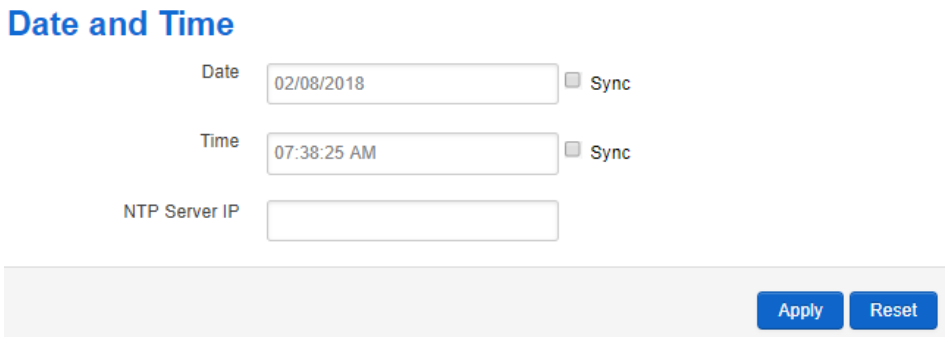
1. Select System > Date and Time from the navigation area. The system time configuration page appears by default, as shown in Figure 5-10.

2. Type 02/08/2018 in the Date box, and type 07:38:25 AM in the Time box. Check the Sync box of the date and time, the time of the pc will be set.

3. Click Apply.

4. Click Save of the navigation area.

Figure 5-10 System time configuration page



5.5.3 Configuing NTP Server

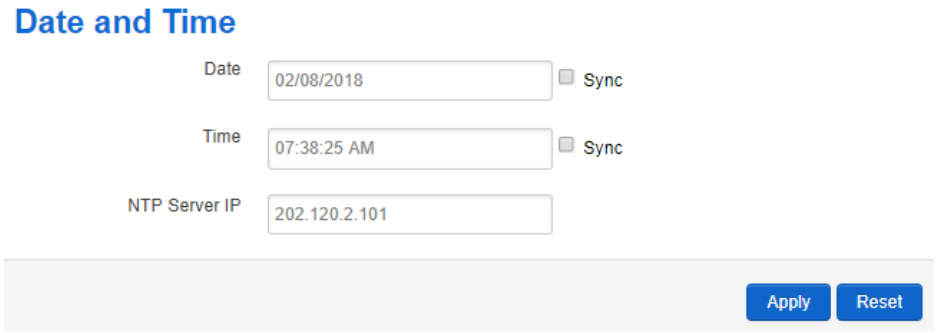
1. Select System > Date and Time from the navigation area. The system time configuration page appears by default, as shown in Figure 5-11.

2. Type 202.120.2.101 in the NTP Server IP box.

3. Click Apply.

4. Click Save of the navigation area.

Figure 5-11 NTP Server Time time configuration page

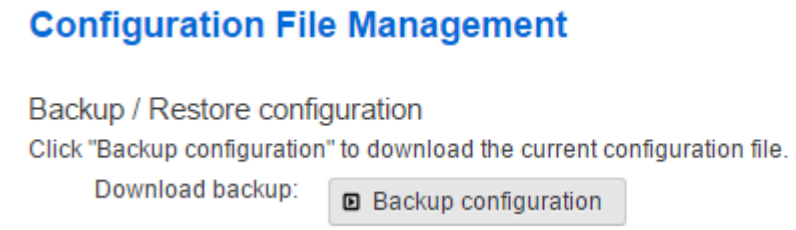


5.6 Configuration File Management

5.6.1 Back up configuration

Select System > Configuration File Management from the navigation area to enter the backup configuration page, as shown in Figure 5-12.

Figure 5-12 Configuration File Management page

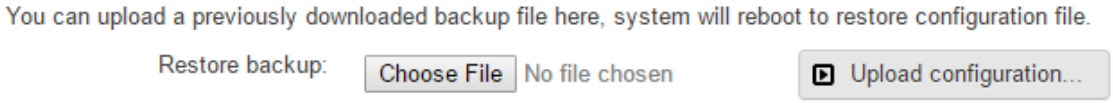


Click the Backup configuration button, a file download dialog box appears. You can save the file locally.

5.6.2 Restore Configuration

Select Device > Configuration File Management from the navigation area to enter the Restore configuration page, as shown in Figure 5-13.

Figure 5-13 Restore Configuration page

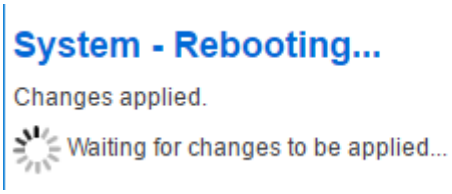


Backup / Restore configuration steps:

1. After you click the Choose File button in this figure, the file upload dialog box appears. You can select the *. conf file to be uploaded, and then click OK.

2. Click the Upload configuration button, then the device will be reboot, as shown in Figure 5-14.

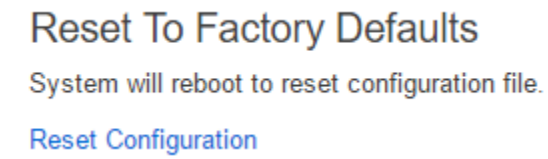
Figure 5-14 Rebooting page



5.6.3 Reset to Factory Defaults

1. Select Device > Configuration File Management > Reset To Factory Defaults from the navigation area to enter the Reset to Factory Defaults page, as shown in Figure 5-15.

Figure 5-15 Reset to Factory Defaults page



2. Click the Reset Configuration button to apply. This operation restores the system to factory defaults, delete the current configuration file, and reboot the device.

5.7 System Upgrade

Software upgrade allows you to obtain a target application file from the current host and set the file as the main boot file or backup boot file to be used at the next reboot.

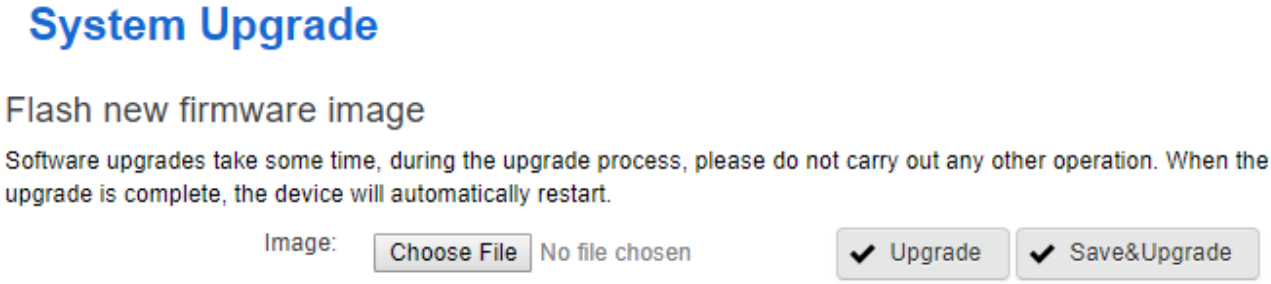
NOTE:

- A software upgrade takes some time. Do not perform any operation on the web interface during the upgrading procedure; otherwise, the upgrade operation may be interrupted.

---

1. Select System -> System Upgrade from the navigation area to enter the page as shown in Figure 5-16.

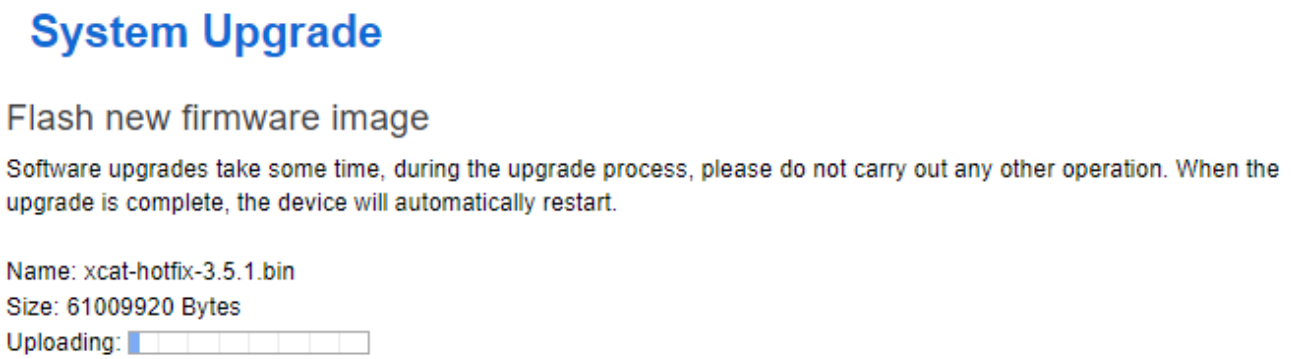
Figure 5-16 System Upgrade page



2. Click Choose File, when you click Create Diagnostic Information File, the system begins to generate the diagnostic information file, and after the file is generated, the page is as shown in Figure 5-17. Click Upgrade to Download, and the File Download dialog box appears. You can select to open this file or save this file to the local host.

3. Click Upgrade or Save & Upgrade to complete the software upgrade. After the upgrade is finished, the device will be rebooted.

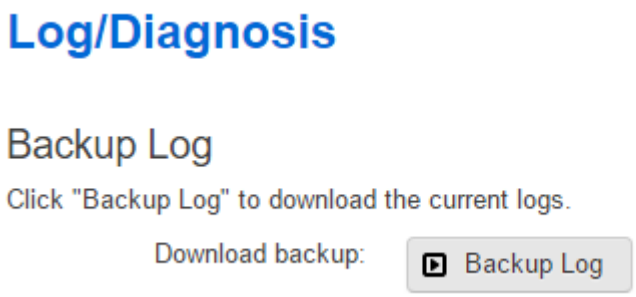
Figure 5-17 Flash new firmware image page



5.8 Log/Diagnosis

Each functional module has its own running information, and generally, you need to view the output information for each module one by one. To receive as much information as possible in one operation during daily maintenance or when system failure occurs, the diagnostic information module allows you to save the running statistics of multiple functional modules to a file, and then you can locate problems faster by checking this file.

Figure 5-18 Backup log page



1. Select Device > Log/Diagnosis from the navigation area to enter the page as shown in Figure 5-18.

2. When you click Backup Log button, the system begins to generate the diagnostic information file, and after the file is generated, the File Download dialog box appears. You can save this file to the local host.

5.9 Reboot

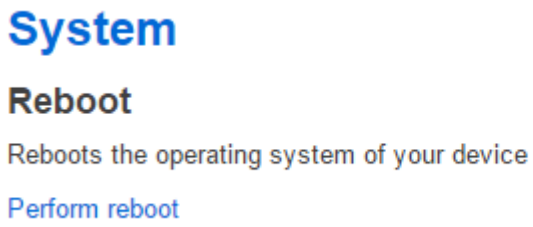
NOTE:

- Before rebooting the device, save the configuration; otherwise, all unsaved configurations are lost after device reboot. After the device reboots, you must re-log in to the Web interface.

1. Select System> Reboot from the navigation area to enter the page as shown in Figure 5-19.

2. Click Perform reboot to reboot the device.

Figure 5-19 Device reboot page



6 Diagnosis

6.1 Network Utilities

6.1.1 Overview

Ping

You can use the ping function to check whether a device with a specified address is reachable, and to examine network connectivity. A successful execution of the ping command involves the following steps:

1. The source device sends an ICMP echo request (ECHO-REQUEST) to the destination device.

2. The destination device responds by sending an ICMP echo reply (ECHO-REPLY) to the source device after receiving the ICMP echo request.

3. The source device displays related statistics after receiving the reply. Output of the ping command falls into the following:

- The ping command can be applied to the destination’ s host name or IP address. If the destination’ s host name is unknown, the prompt information is displayed.
- If the source device does not receive an ICMP echo reply within the timeout time, it displays the prompt information and the statistics during the ping operation. If the source device receives an ICMP echo reply within the timeout time, it displays the number of bytes of the echo reply, the message sequence number, Time to Live (TTL), the response time, and the statistics during the ping operation. Statistics during the ping operation include number of packets sent, number of echo reply messages received, percentage of messages not received, and the minimum, average, and maximum response time.

Traceroute

By using the traceroute command, you can display the Layer 3 devices involved in delivering a packet from source to destination. This function is useful for identification of failed node(s) in the event of network failure.

The traceroute command involves the following steps in its execution:

1. The source device sends a packet with a TTL value of 1 to the destination device.

2. The first hop (the Layer 3 device that first receives the packet) responds by sending a TTL-expired ICMP message to the source, with its IP address encapsulated. In this way, the source device can get the address of the first Layer 3 device.

3. The source device sends a packet with a TTL value of 2 to the destination device.

4. The second hop responds with a TTL-expired ICMP message, which gives the source device the address of the second Layer 3 device.

This process continues until the ultimate destination device is reached. In this way, the source device can trace the addresses of all the Layer 3 devices involved to get to the destination device. The traceroute command can be applied to the destination’ s host name or IP address. If the destination’ s host name is unknown, the prompt information is displayed

6.1.2 Diagnostic tool operations

ping operation

1. Select Diagnostic > Network Utilities from the navigation tree to enter the IPv4&IPv6 Ping configuration page.

2. Type in the IPv4 address of the destination device in the text box.

3. Click PING to execute the ping command, and you see the result in the box below.

Figure 6-1 Network Utilities page

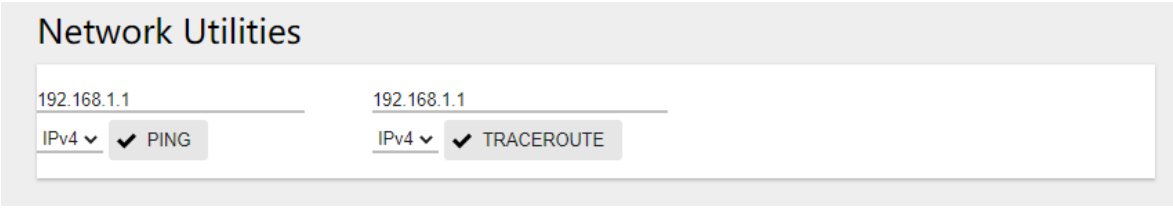


Figure 6-2 The ping result

```
PING 192.168.1.116 (192.168.1.116) 56(84) bytes of data.
64 bytes from 192.168.1.116: icmp_req=1 ttl=128 time=0.712 ms
64 bytes from 192.168.1.116: icmp_req=2 ttl=128 time=0.604 ms
64 bytes from 192.168.1.116: icmp_req=3 ttl=128 time=0.624 ms
64 bytes from 192.168.1.116: icmp_req=4 ttl=128 time=0.590 ms
64 bytes from 192.168.1.116: icmp_req=5 ttl=128 time=0.545 ms

--- 192.168.1.116 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.545/0.615/0.712/0.055 ms
```

Traceroute operation

1. Select Diagnostic > Network Utilities from the navigation tree.

2. Type the destination IP address in the text box.

3. Click TRACEROUTE to execute the trace route command, and you see the result in the box below, as shown in Figure 6-3.

Figure 6-3 The trace route result

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.1.1  0.777 ms
 2  192.168.2.1  1.444 ms
 3  100.64.0.1  4.197 ms
 4  218.104.229.169  4.049 ms
 5  218.106.149.197  26.020 ms
 6  219.158.114.117  16.973 ms
 7  219.158.103.42  23.279 ms
 8  219.158.20.222  25.190 ms
 9  219.158.10.62  28.488 ms
10  219.158.33.174  23.111 ms
11  108.170.241.1  23.096 ms
12  108.170.235.11  26.870 ms
13  8.8.8.8  23.630 ms
```

6.2 Dying Gasp

6.2.1 Overview

The networking devices rely on a temporary back-up power supply on a capacitor, which allows for a gradual shutdown and the generation of the dying-gasp message. This temporary power supply is designed to last from 10 to 20 milliseconds to perform these tasks.

According to the definition in 802.3ah, when a device power failure event occurs, the device sends an OAM event message to its connected device. Since OAM is a point-to-point protocol, the power failure event message will not be sent to the next device that supports OAM. Continue to forward again. The device that receives a power failure event will output a power failure LOG prompt message.

In addition to the OAM alarm information, the power-off device will also send a trap message to the smmp server.

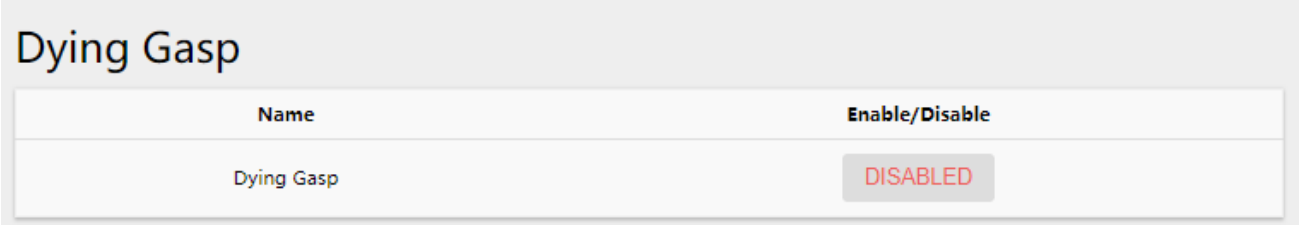
Node information	Data
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

6.2.2 Configuring Dying Gasp

1. Select Diagnosis > Dying gasp from the navigation area to enter the page of dying gasp configuration page as shown in Figure 6-4.

2. Click Enable/Disable tap to apply dying gasp.

Figure 6-4 Dying gasp configuration page



6.3 Optical Transceiver Information

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to troubleshoot fiber cables and fiber transceivers at remote sites. To solve this problem, Ethernet switches provide digital diagnostics and monitoring (DDM) functions on SFP optical fiber links and allow users to measure optical parameters and its performance from a central site. This function

can greatly facilitate the troubleshooting process for optical fiber links and reduce costs for onsite debugging.

6.3.1 Displaying Optical Transceiver Information

Select Diagnosis > Optical Transceiver Information from the navigation area. The system automatically displays the optical transceiver information, as shown in Figure 6-5. Table 6-1 describes the optical transceiver information items.

Figure 6-5 optical transceiver information

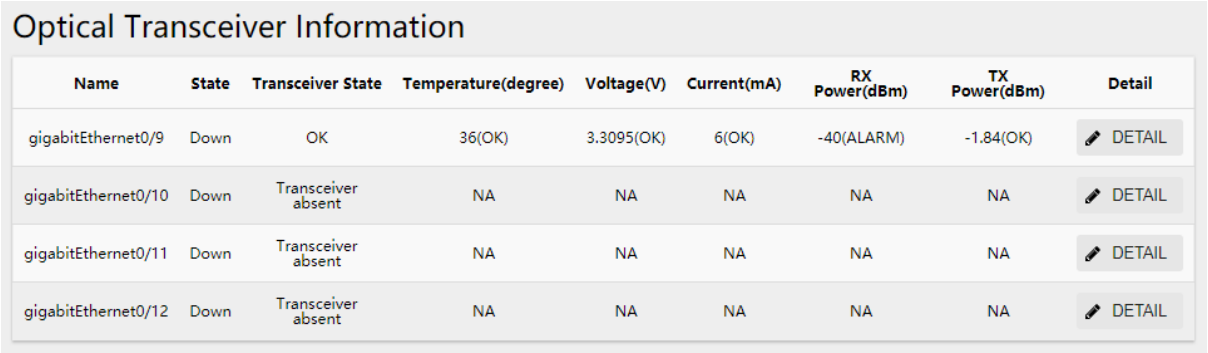


Table 6-1 optical transceiver information items

Item	Description
Name	Switch port number that the SFP is plugged into.
State	The state of the fiber interface, up/down.
Transceiver State	The absent of the transceiver.
Temperature(degree)	SFP casing temperature
Voltage(V)	Voltage supply to the transceiver.
Current(mA)	Current consumed by transceiver.
Rx Power(dBm)	The amount of light being received from the fiber optic cable
TX Power(dBm)	The amount of light being transmitted into the fiber optic cable
Detail	Click to show the detail information of the transceiver.

6.3.2 Displaying detail information

Click DETAIL of the interface to enter the page of transceiver detail inforamation. As shown in Figure 6-6.

Figure 6-6 transceiver detail information

Interface-gigabitEthernet0/9

Transceiver Type	10GBASE-SR-SFP+
Connector Type	LC
Wavelength(nm)	850
Link Length: 62.5/125 um OM1 fiber(m)	30
Link Length: 50/125 um OM2 fiber(m)	80
Link Length: 50/125 um OM3 fiber(m)	300
Digital Diagnostic Monitoring	YES
Vendor Serial Number	WT1703230020
Alarm	RX Channel power low; RX Channel loss of signal;
Vendor Name	OEM
Vendor OUI	0030d3
Vendor Part Number	SFP-XG-SX-MM850
Vendor Revision	1.0
Manufacturing Date	2017-03-27
Encoding	64B/66B