

# **SICOM3000A Industrial Ethernet Switch**

## **Web Operation Manual**

Publication Date: Dec. 2021

Version: V1.0

***KYLAND***

**Disclaimer:**

Kyland Technology Co., Ltd. tries to keep the content in this manual as accurate and as up-to-date as possible. This document is not guaranteed to be error-free, and we reserve the right to amend it without notice.

**All rights reserved**

No part of this documentation may be excerpted, reproduced, translated, annotated or duplicated, in any form or by any means without the prior written permission of KYLAND Corporation.

**Copyright © 2021 Kyland Technology Co., Ltd.**

Website: <http://www.kyland.com>

FAX: +86-10-88796678

Email: support@kyland.com

# Contents

Preface .....	1
1 Product Introduction.....	6
1.1 Overview .....	6
1.2 Software Features.....	6
2 Switch Access.....	8
2.1 View Types.....	8
2.2 Switch Access by Console Port.....	9
2.3 Switch Access by Telnet.....	12
2.4 Switch Access by Web .....	13
3 Maintenance .....	17
4 Basic Configuration .....	22
4.1 System Information .....	22
4.2 System Configuration.....	22
4.3 CPU Load .....	23
4.4 Firmware Upgrade .....	23
4.4.1 Firmware Upgrade by HTTP.....	23
4.4.2 Firmware Upgrade by SFTP .....	24
4.5 Firmware Application Activate .....	26
5 IP Configuration .....	28
5.1 IP Address Configuration.....	28
5.2 ARP .....	31
5.2.1 Introduction.....	31
5.2.2 Web Configuration.....	31
5.3 DHCP Configuration.....	32
5.3.1 DHCP Server Configuration.....	34
5.3.2 DHCP Snooping .....	45
5.3.3 Option 82 Configuration.....	48
6 Clock System.....	51

6.1 Clock Configuration.....	51
6.2 SNTP .....	53
6.3 PTP .....	55
6.3.1 Introduction.....	55
6.3.2 Synchronization Principle .....	56
6.3.3 Web Configuration.....	57
6.3.4 Typical Configuration Example .....	63
7 Port Configuration.....	65
8 QoS Configuration .....	70
8.1 Introduction .....	70
8.2 Principle .....	71
8.3 Web Configuration .....	71
8.4 Typical Configuration Example.....	96
9 Security.....	99
9.1 User Management.....	99
9.1.1 Introduction.....	99
9.1.2 Web Configuration.....	99
9.2 Authentication login configuration.....	102
9.3 SSH Configuration .....	103
9.3.1 Introduction.....	103
9.3.2 Implementation .....	104
9.3.3 Web Configuration.....	104
9.3.4 Typical Configuration Example .....	105
9.4 SSL Configuration .....	107
9.4.1 Introduce.....	107
9.4.2 Web Configuration.....	107
9.5 Access Management.....	110
9.5.1 Introduction.....	110
9.5.2 Web Configuration.....	110
9.6 SNMP v1/SNMP v2c .....	112

9.6.1 Introduction.....	112
9.6.2 Implementation .....	112
9.6.3 Explanation.....	113
9.6.4 MIB Introduction .....	113
9.6.5 Web Configuration.....	114
9.6.6 Typical Configuration Example .....	118
9.7 SNMPv3.....	119
9.7.1 Introduce.....	119
9.7.2 Implementation .....	120
9.7.3 Web Configuration.....	120
9.7.4 Typical Configuration Example .....	130
9.8 RMON .....	131
9.8.1 Introduce.....	131
9.8.2 RMON Groups.....	132
9.8.3 Web Configuration.....	133
9.9 TACACS+ Configuration .....	139
9.9.1 Introduction.....	139
9.9.2 Web Configuration.....	140
9.9.3 Typical Configuration Example .....	142
9.10 RADIUS Configuration .....	143
9.10.1 Introduction.....	143
9.10.2 Web Configuration.....	143
9.10.3 Typical Configuration Example .....	147
10 Network .....	149
10.1 Port Security.....	149
10.1.1 Introduction.....	149
10.1.2 Web Configuration.....	149
10.2 IEEE802.1X Configuration .....	152
10.2.1 Introduction.....	152
10.2.2 Web Configuration.....	152

10.2.3 Typical Configuration Example .....	159
10.3 ACL .....	160
10.3.1 Overview.....	160
10.3.2 Implementation .....	160
10.3.3 Web Configuration.....	161
10.3.4 Typical Configuration Example .....	174
11 Port Aggregation .....	176
11.1 Static Aggregation .....	176
11.1.1 Introduction .....	176
11.1.2 Implementation .....	176
11.1.3 Web Configuration .....	177
11.1.4 Typical Configuration Example .....	178
11.2 LACP .....	178
11.2.1 Introduction .....	178
11.2.2 Implementation .....	179
11.2.3 Web Configuration .....	179
11.2.4 Typical Configuration Example .....	182
12 Loop Detect Configuration .....	183
12.1 Overview .....	183
12.2 Web Configuration .....	183
12.3 Typical Configuration Example .....	186
13 Industry Protocol.....	187
13.1 EtherNet/IP.....	187
13.1.1 Introduction.....	187
13.1.2 Web Configuration.....	187
13.2 ModbusTCP .....	187
13.2.1 Introduction.....	187
13.2.2 Web Configuration.....	188
13.3 PROFINET .....	188
13.3.1 Introduction.....	188

13.3.2 WEB Configuration .....	190
14 Multicast .....	191
14.1 IGMP Snooping .....	191
14.1.1 Introduction .....	191
14.1.2 Basic Concepts .....	191
14.1.3 Principle .....	192
14.1.4 Web Configuration .....	193
14.1.5 Typical Application Example .....	198
14.2 GMRP .....	199
14.2.1 GARP Introduction .....	199
14.2.2 GMRP Protocol .....	200
14.2.3 Web Configuration .....	201
14.2.4 Typical Application Example .....	203
14.3 Unregistered Multicast Action .....	204
15 LLDP .....	206
15.1 Introduction .....	206
15.2 Web Configuration .....	206
16 MEP .....	209
16.1 Web Configuration .....	209
17 ERPS Principle .....	235
17.1 Introduction .....	235
17.1.1 Basic Concept .....	235
17.1.2 Protocol Message .....	238
17.1.3 ERPS Protocol State .....	239
17.1.4 ERPS Timer .....	240
17.1.5 ERPS Operating Mechanism .....	240
17.1.6 ERPS Configuration Networking .....	242
17.2 Web Configuration .....	243
18 MAC Address Configuration .....	250
18.1 Introduction .....	250

18.2 Web Configuration .....	250
19 VLAN .....	253
19.1 VLAN Configuration .....	253
19.1.1 Introduction .....	253
19.1.2 Principle .....	253
19.1.3 Port-based VLAN .....	254
19.1.4 Web Configuration .....	256
19.1.5 Typical Configuration Example .....	260
19.2 PVLAN Configuration .....	262
19.2.1 Introduction .....	262
19.2.2 Explanation .....	262
19.2.3 Typical Configuration Example .....	263
19.3 GVRP .....	264
19.3.1 GARP Introduction .....	264
19.3.2 GVRP Introduction .....	265
19.3.3 Web Configuration .....	266
19.3.4 Typical Configuration Example .....	268
20 Redundancy .....	270
20.1 DT-Ring .....	270
20.1.1 Introduction .....	270
20.1.2 Concepts .....	270
20.1.3 Implementation .....	271
20.1.4 Explanation .....	274
20.1.5 Web Configuration .....	274
20.1.6 Typical Configuration Example .....	277
20.2 DRP .....	278
20.2.1 Overview .....	278
20.2.2 Concept .....	279
20.2.3 Implementation .....	280
20.3 DHP .....	285



20.3.1 Overview.....	285
20.3.2 Concepts .....	286
20.3.3 Implementation .....	287
20.3.4 Description.....	288
20.3.5 Web Configuration .....	288
20.3.6 Typical Configuration Example .....	292
20.4 RSTP/STP.....	292
20.4.1 Introduction.....	292
20.4.2 Concepts .....	292
20.4.3 BPDU .....	293
20.4.4 Implementation .....	294
20.4.5 Web Configuration.....	295
20.4.6 Typical Configuration Example .....	301
20.5 MSTP Configuration .....	302
20.5.1 Introduction.....	302
20.5.2 Basic Concepts.....	304
20.5.3 MSTP Implementation .....	308
20.5.4 Web Configuration.....	309
20.5.5 Typical Configuration Example .....	318
21 Alarm .....	322
21.1 Introduction .....	322
21.2 Web Configuration .....	322
22 Link Check.....	331
22.1 Introduction .....	331
22.2 Web Configuration .....	331
23 Log.....	333
23.1 Introduction .....	333
23.2 Web Configuration .....	333
24 Port Mirroring.....	336
24.1 Introduction .....	336

24.2 Explanation .....	336
24.3 Web Configuration .....	336
24.4 Typical Configuration Example .....	337
25 Diagnostics .....	339
25.1 Ping .....	339
Appendix: Acronyms .....	341

## Preface

This manual mainly introduces the access methods and software features of SICOM3000A industrial Ethernet switch, and details Web configuration methods.

### Content Structure

The manual contains the following contents:

Main Content	Explanation
1. Product Introduction	<ul style="list-style-type: none"> <li>➤ Overview</li> <li>➤ Software Features</li> </ul>
2. Switch Access	<ul style="list-style-type: none"> <li>➤ View Types</li> <li>➤ Switch Access by Console Port</li> <li>➤ Switch Access by Telnet</li> <li>➤ Switch Access by Web</li> </ul>
3. Maintenance	<ul style="list-style-type: none"> <li>➤ Reboot</li> <li>➤ Load Default</li> <li>➤ Save Current Configuration</li> <li>➤ Upload/Download Configuration File</li> </ul>
4. Basic Configuration	<ul style="list-style-type: none"> <li>➤ System Information</li> <li>➤ System Configuration</li> <li>➤ CPU Load</li> <li>➤ Firmware Upgrade (by HTTP, SFTP)</li> <li>➤ Firmware Application Active</li> </ul>
5. IP Configuration	<ul style="list-style-type: none"> <li>➤ IP Address Configuration</li> <li>➤ ARP Configuration</li> <li>➤ DHCP Configuration</li> </ul>
6. Clock System	<ul style="list-style-type: none"> <li>➤ Clock Configuration</li> <li>➤ SNTP</li> <li>➤ PTP</li> </ul>
7. Port Configuration	<ul style="list-style-type: none"> <li>➤ Configure port status</li> </ul>

	<ul style="list-style-type: none"> <li>➤ Port Statistics</li> </ul>
8. QoS Configuration	<ul style="list-style-type: none"> <li>➤ Port-based Queue Priority Mapping</li> <li>➤ 802.1Q Header-based Queue Priority Mapping</li> <li>➤ IEEE802.1p Remarking</li> <li>➤ DSCP-based Queue Priority Mapping</li> <li>➤ DSCP RE-Mapping</li> <li>➤ DSCP Class rule</li> <li>➤ QCL</li> <li>➤ Port-based Commit Access Rate</li> <li>➤ Queue-based Commit Access Rate</li> <li>➤ Port-based Queue scheduling</li> <li>➤ Port-based traffic shaping</li> <li>➤ Storm suppression</li> </ul>
9. Security	<ul style="list-style-type: none"> <li>➤ User Management</li> <li>➤ Authentication Login Configuration</li> <li>➤ SSH Configuration</li> <li>➤ SSL Configuration</li> <li>➤ Access Management</li> <li>➤ SNMP v1/v2c/v3</li> <li>➤ RMON Configuration</li> <li>➤ TACACS+ Configuration</li> <li>➤ RADIUS Configuration</li> </ul>
10. Network	<ul style="list-style-type: none"> <li>➤ Port Security</li> <li>➤ IEEE802.1X Configuration</li> <li>➤ ACL Configuration</li> </ul>
11. Port Aggregation	<ul style="list-style-type: none"> <li>➤ Static Aggregation</li> <li>➤ LACP Configuration</li> </ul>
12. Loop Detect Configuration	
13. Industry Protocol	<ul style="list-style-type: none"> <li>➤ EtherNet/IP</li> </ul>

	<ul style="list-style-type: none"> <li>➤ Modbus TCP</li> <li>➤ PROFINET</li> </ul>
14. Multicast	<ul style="list-style-type: none"> <li>➤ IGMP Snooping</li> <li>➤ GMRP</li> <li>➤ Unregistered Multicast Action</li> </ul>
15. LLDP	
16. MAC Address Configuration	
17. VLAN	<ul style="list-style-type: none"> <li>➤ VLAN Configuration</li> <li>➤ PVLAN Configuration</li> <li>➤ GVRP</li> </ul>
18. Redundancy	<ul style="list-style-type: none"> <li>➤ DT-Ring</li> <li>➤ DRP/DHP</li> <li>➤ RSTP/STP</li> <li>➤ MSTP</li> </ul>
19. Alarm	<ul style="list-style-type: none"> <li>➤ Power Alarm</li> <li>➤ Memory Usage Alarm、 CPU Usage Alarm</li> <li>➤ Port Alarm</li> <li>➤ DT-Ring Alarm</li> <li>➤ DRP Alarm</li> <li>➤ IP/MAC Conflict Alarm</li> <li>➤ CRC and Packet Loss Alarm</li> <li>➤ Port Rate Alarm</li> <li>➤ SFP Power Alarm</li> </ul>
20. Link Check	
21. Log	
22. Port Mirroring	
23. Diagnostics	Ping

**Conventions in the manual**




### 1. Text format conventions

Format	Explanation
< >	The content in < > is a button name. For example, click <Apply> button.
[ ]	The content in [ ] is a window name or a menu name. For example, click [File] menu item.
{ }	The content in { } is a portfolio. For example, {IP address, MAC address} means IP address and MAC address is a portfolio and they can be configured and displayed together.
→	Multi-level menus are separated by “→”. For example, Start → All Programs → Accessories. Click [Start] menu, click the sub menu [All programs], then click the submenu [Accessories].
/	Select one option from two or more options that are separated by “/”. For example “Addition/Deduction” means addition or deduction.
~	It means a range. For example, “1~255” means the range from 1 to 255.

### 2. CLI conventions

Format	Description
<b>Bold</b>	Commands and keywords, for example, <b>show version</b> , appear in <b>bold</b> font.
<i>Italic</i>	Parameters for which you supply values are in <i>italic</i> font. For example, in the <b>show vlan</b> <i>vlan id</i> command, you need to supply the actual value of <i>vlan id</i> .

### 3. Symbol conventions

Symbol	Explanation
 <b>Caution</b>	The matters need attention during the operation and configuration, and they are supplement to the operation description.
 <b>Note</b>	Necessary explanations to the operation description.
 <b>Warning</b>	The matters call for special attention. Incorrect operation might cause data loss or damage to devices.

## Product Documents

The documents of SICOM3000A industrial Ethernet switch include:

<b>Name of Document</b>	<b>Content Introduction</b>
SICOM3000A Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods.
SICOM3000A Industrial Ethernet Switch Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

## Document Obtainment

Product documents can be obtained by:

- CD shipped with the device
- Kyland website: [www.kyland.com](http://www.kyland.com)

# 1 Product Introduction

## 1.1 Overview

SICOM3000A includes a series of high-performance managed industrial Ethernet switches applied in the rail transportation industry. SICOM3000A conforms to EN50155, EN50121 and other industrial standards. The switch is a layer 2 switch that supports MSTP, RSTP, DT-Ring, IEC62439-6 redundancy protocols, guaranteeing the reliable operation of the system. It also supports the SFP optical module with digital diagnosis function, which can monitor the transmitting power and receiving power of the optical transceiver module in real time.

## 1.2 Software Features

SICOM3000A provides abundant software features, satisfying customers' various requirements.

- Redundancy protocols: STP/RSTP, MSTP, DT-Ring and DRP.
- Multicast protocols: IGMP Snooping, static multicast and GMRP.
- Switching attributes: VLAN, PVLAN, GVRP, QoS, and ARP.
- Bandwidth management: port static aggregation, LACP, port rate limiting, and port storm suppression.
- Security: user management, access management, SSH, SSL, TACACS+, RADIUS, IEEE802.1X, and ACL.
- Synchronization protocols: SNTP, PTP.
- Device management: software update, configuration file upload/download, log record and upload and U-disk configuration.
- Device diagnosis: port mirroring, LLDP, link check, and loop protection.
- Alarm function: power alarm, mem/cpu usage alarm, port alarm, ring alarm, CRC and Pkt Loss alarm, Port Rate alarm, IP/MAC address conflict alarm and SFP Power alarm.
- Network management: management by CLI, Telnet, Web and Kyvision network management software, DHCP, and SNMP v1/v2c/v3 network monitoring.



- Industry Protocol: EtherNet/IP、ModbusTCP、Profinet;
- .....

## 2 Switch Access

You can access the switch by:

- Console port
- Telnet/SSH
- Web browser
- Kyvision management software

Kyvision network management software is designed by Kyland. For details, refer to its user manual.

### 2.1 View Types

When logging into the Command Line Interface (CLI) by the console port or Telnet, you can enter different views or switch between views by using the following commands.

Table 1 View Types

View Prompt	View Type	View Function	Command for View Switching
SWITCH #	Privileged mode	View recently used commands. View software version. View response information for ping operation. Upload/Download configuration file. Restore default configuration. Reboot switch. Save current configuration. Display current configuration. Update software.	Input “ <b>configure terminal</b> ” to switch from privileged mode to configuration mode.  Input “ <b>exit</b> ” to return to the general mode.
SWITCH (config) #	Configuration mode	Configure all switch functions.	Input “ <b>exit</b> ” or “ <b>end</b> ” to return to the Privileged mode.

When the switch is configured through the CLI, "?" can be used to get command help. In the help information, there are different parameter description formats. For example, <1, 255>

means a number range; <xx:xx:xx:xx:xx:xx> means a MAC address; <word31> means the string range is 1~31. In addition, ↑ and ↓ can be used to scroll through recently used commands.

## 2.2 Switch Access by Console Port

You can access a switch by its console port and the hyper terminal of Windows OS or other software that supports serial port connection, such as HTT3.3. The following example shows how to use Hyper Terminal to access switch by console port.

1. Connect the 9-pin serial port of a PC to the console port of the switch with the DB9-M12 console cable.
2. Run the Hyper Terminal in Windows desktop. Click [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in Figure 1.

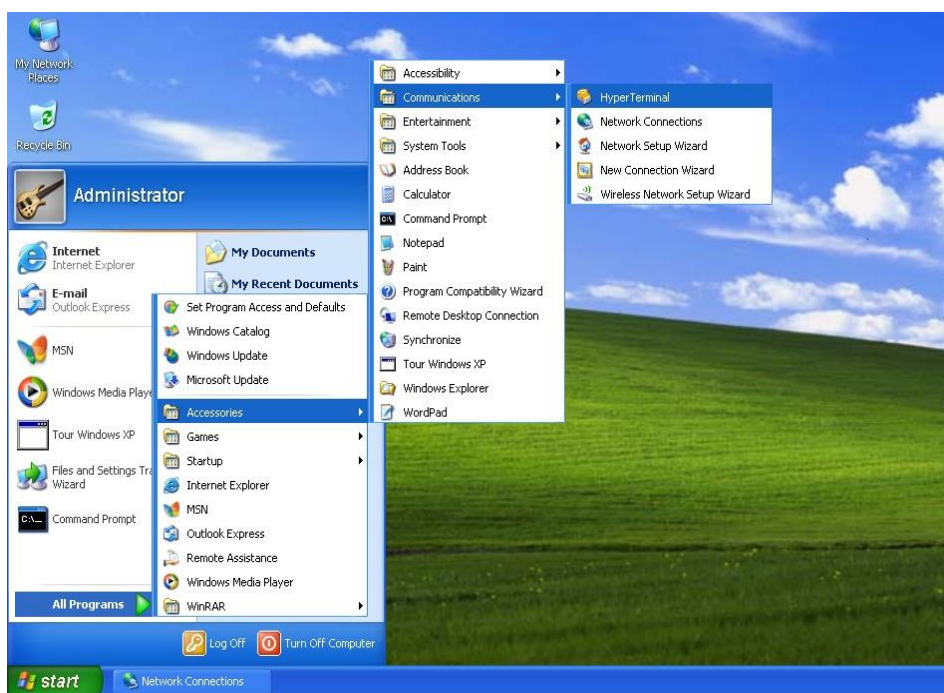


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in Figure 2.

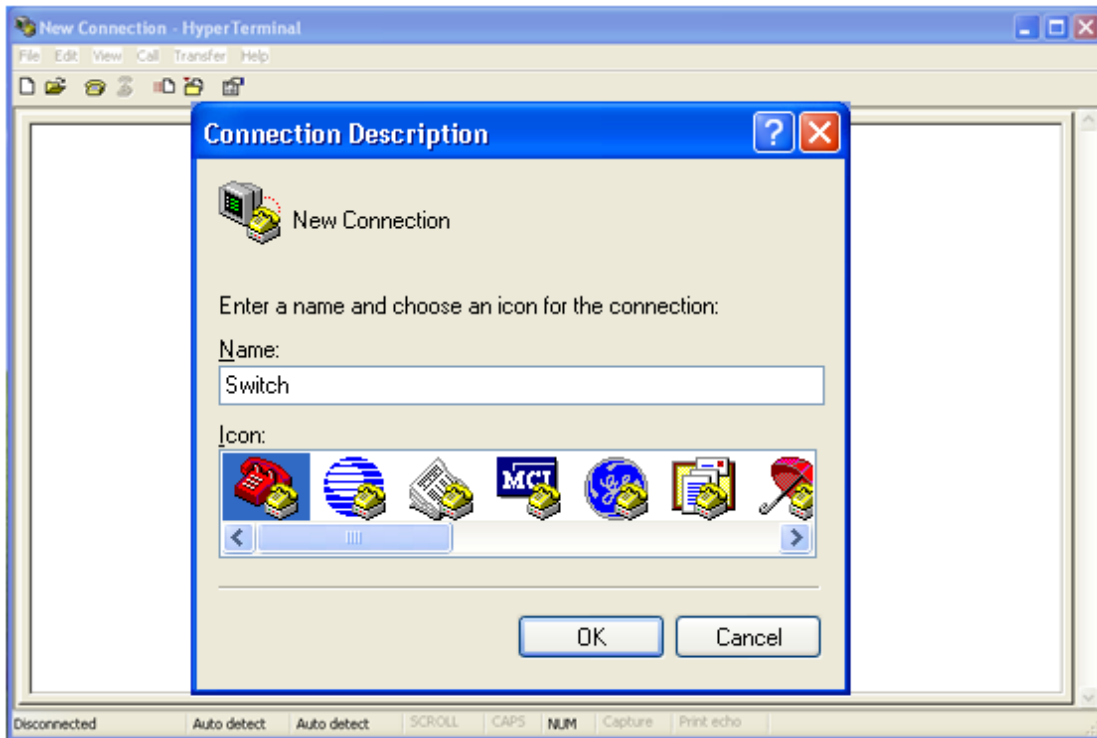


Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown in Figure 3.



Figure 3 Selecting the Communication Port



**Note:**

To confirm the communication port in use, right-click [My Computer] and click [Property] → [Hardware] → [Device Manager] → [Port].

5. Set port parameters (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None), as shown in Figure 4.

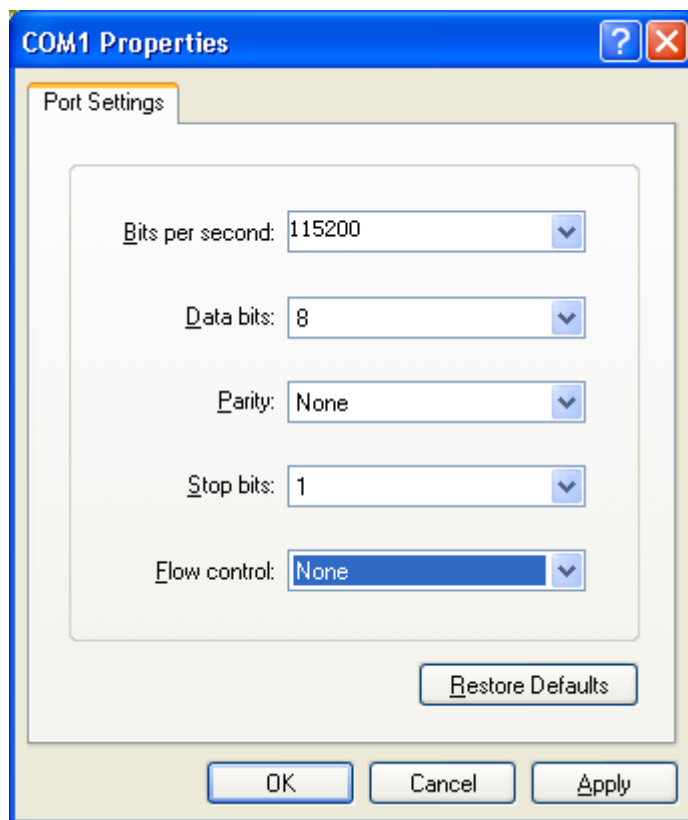


Figure 4 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input default username "admin", and password"123" to enter the privileged mode. You can also input other created username and password, as shown in Figure 5.

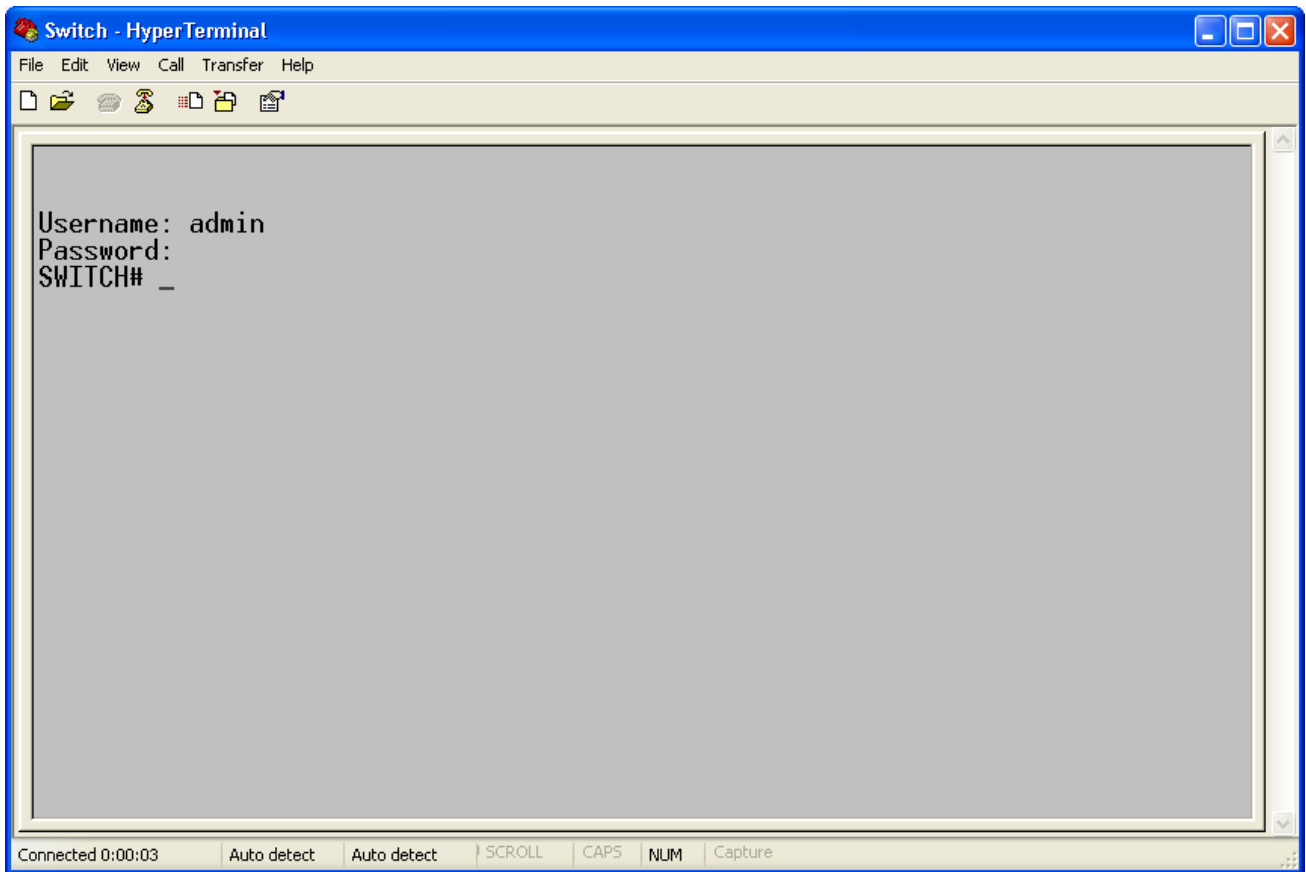


Figure 5 CLI

### 2.3 Switch Access by Telnet

The precondition for accessing a switch by Telnet is the normal communication between the PC and the switch.

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 6. The default IP address of a Kyland switch is 192.168.0.2.

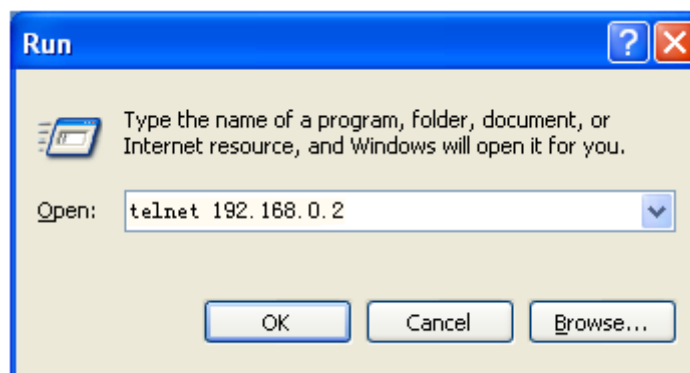


Figure 6 Telnet Access

**Note:**

To confirm the switch IP address, please refer to "5 IP Configuration" to learn how to obtain IP address.

2. In the Telnet interface, input username "admin", and password "123" to log in to the switch. You can also input other created users and password, as shown in Figure 7.

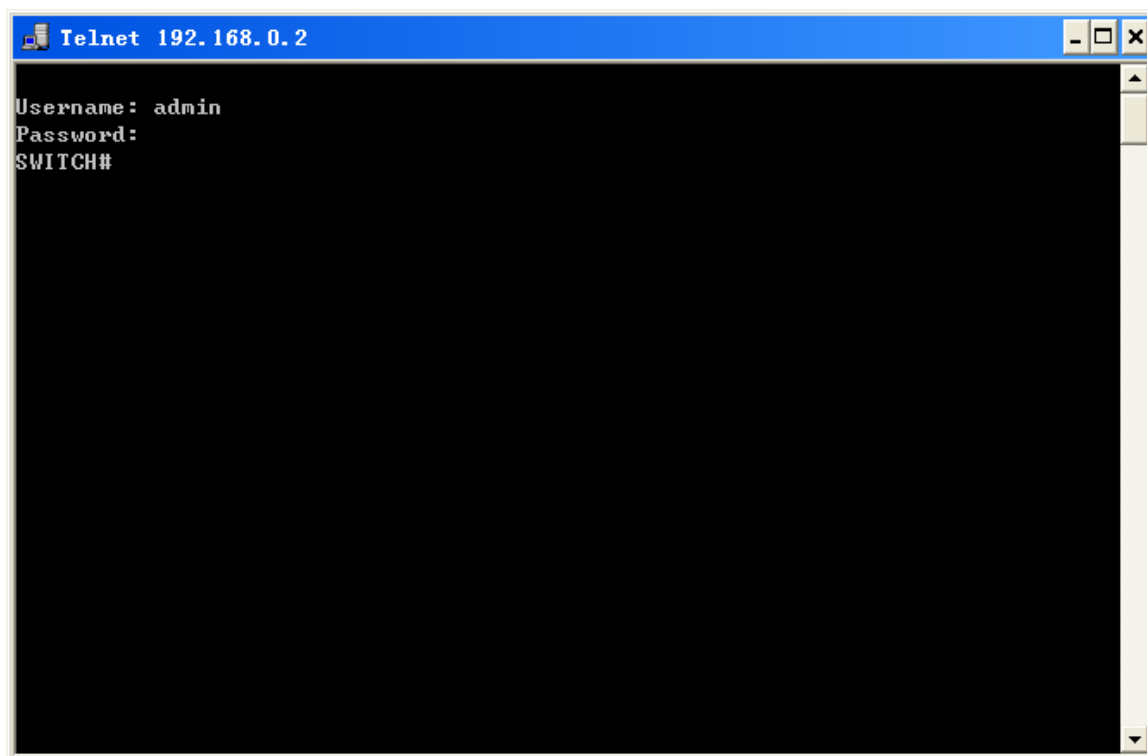


Figure 7 Telnet Interface

## 2.4 Switch Access by Web

The precondition for accessing a switch by Web is the normal communication between the PC and the switch.

**Note:**

IE8.0 or a later version is recommended for the best Web display results.

1. Input "IP address" in the browser address bar. The login interface is displayed, as shown in Figure 8. Input the default username "admin", password "123", or self-created username and password. Then click <Login>. You can also input other created users and password.

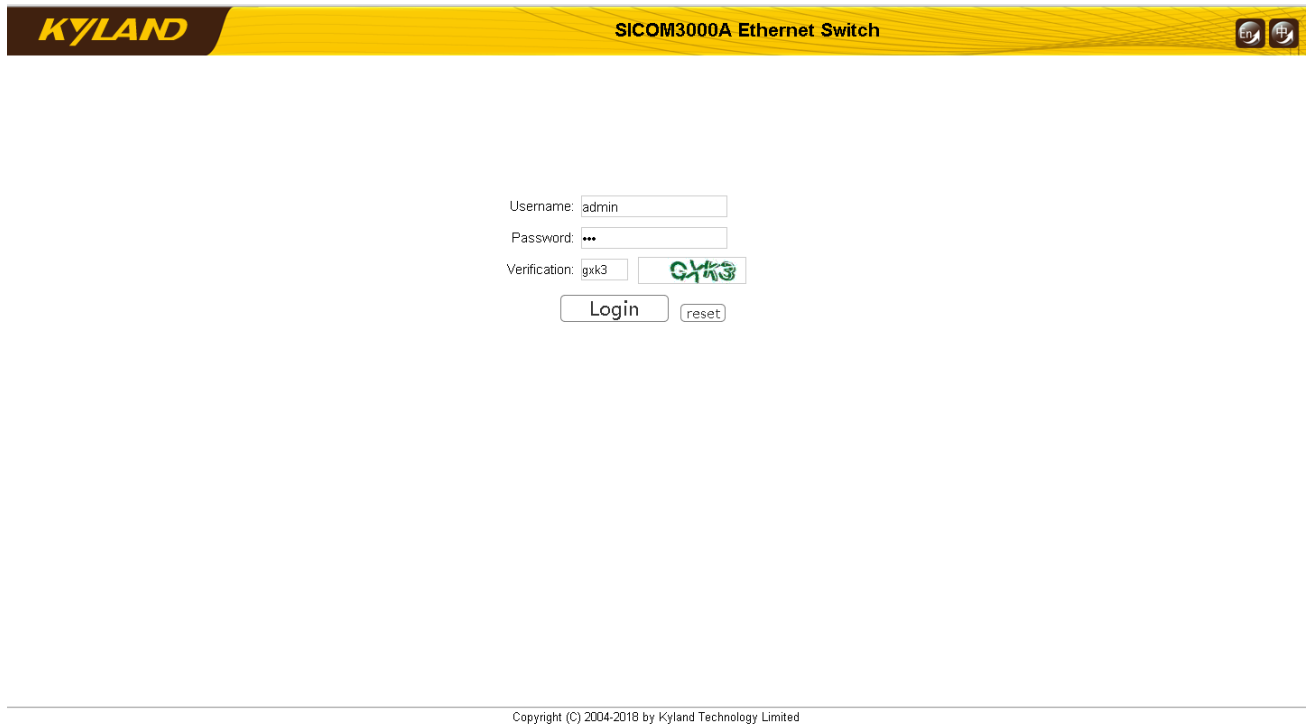




Figure 8 Web Login

You can click  or  to switch to the English or Chinese interface. The English login interface is displayed by default.



**Note:**

To confirm the switch IP address, please refer to “5 IP Configuration” to learn how to obtain IP address.

2. When you log in successfully, there is a navigation tree on the left of the interface, as shown in Figure 9.



**KYLAND** SICOM3000A Ethernet Switch

Auto-refresh  Refresh



### System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.301 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	SICOM3000A-2Gx8GE
Device MAC Address	00-1e-ed-1c-e8-e0
S/N	S30U0036Axxxxxxx
Time	
System Date	1970-01-01T10:27:53+00:00
System Uptime	0d 10:27:53
Software	
Software Version	R3001
Code Date	Jul 25 2018 09:02:04
Code Revision	Build-24.0.44.2.B1.4.3
Hardware Version	V1.0
Logic Version	V1.0.0

Copyright (C) 2004-2018 by Kyland Technology Limited

Figure 9 Web Interface

You can expand or collapse the navigation tree by clicking menu on the navigation tree. You

can click  to link to Figure 9, and click  to exit the Web interface.

As shown in Figure 10, the configuration/view page of each module provides multiple operation buttons and you can click a button to perform a relevant operation on the page. For example, you can click <Submit> to make the current configuration take effect, click <Reset> to cancel the current configuration and use the configuration that has taken effect, click <Cancel> to close the configuration page and return to the previous configuration page, or click <Refresh> to update information on the current page. You can also select "Auto-refresh" so that the information is automatically updated, at an interval of 4s, or click <Clear> to clear the current statistics and restart statistics.

**QoS Egress Port Tag Remarking Port 3** Port 3

Tag Remarking Mode Default

**PCP/DEI Configuration**

Default PCP 5

Default DEI 0

Submit Reset Cancel

**Access Management Statistics**    Auto-refresh     Refresh    Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	513	513	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	46	46	0
SSH	0	0	0

Figure 10 Configuration/Statistics Interface

### 3 Maintenance

1. Reboot the device, as shown in Figure 11.



Figure 11 Reboot

Before rebooting, please confirm whether to save current configuration. If you select "Yes", the switch runs the current configuration after reboot. If you select "No", the switch runs the previous saved configuration. If no configuration has been saved, the switch will restore the default configuration after reboot.

2. Restore the default configuration, as shown in Figure 12.



Figure 12 Restoring Default Configuration



**Caution:**

After you have restored the default settings, you need to restart the device to make settings take effect.

3. Save current running-config, as shown in Figure 13.

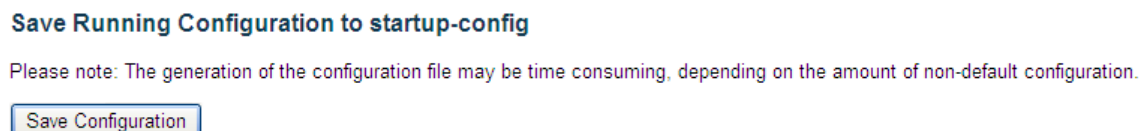


Figure 13 Save Current Configuration

4. Upload the file from the switch to local /server, as shown in Figure 14, Figure 15.

### Upload From Switch

Transport protocols	<input checked="" type="radio"/> Http <input type="radio"/> Sftp
---------------------	--

Select file to save.

Please note: running-config may take a while to prepare for upload.

File Name
<input type="radio"/> ram-log
<input checked="" type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Figure 14 Upload File –HTTP

### Upload From Switch

Transport protocols	<input type="radio"/> Http <input checked="" type="radio"/> Sftp
User name	admin
Password	123
Server IP address	192.168.0.23

Select file to save.

Please note: running-config may take a while to prepare for upload.

File Name
<input type="radio"/> ram-log
<input checked="" type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Figure 15 Upload File -SFTP

#### {User name, Password }

Range: {1~63 characters, 1~63 characters}

Description: Input the user name and password created on SFTP server.

#### Server IP address

Format: A.B.C.D

Description: Configure the IP address of the SFTP server.



**Caution:**

- When transferring files by SFTP, you need to configure SFTP user name, password, and SFTP server IP address.
- In the file transmission, keeps the SFTP server running.

You can save a file in the switch to the local /server. **ram-log** file records the log information, **running-config** is the current running configuration file of the switch, **default-config** is the default configuration file, and **startup-config** is the switch startup file. Select a file and click <Upload From Switch> to save the file to the local/server.

5. Download the configuration file from local /server to switch as a new startup file for the switch, as shown in Figure 16, Figure 17.

**Download To Switch**

**File To Download**

<b>Transport protocols</b>	<input checked="" type="radio"/> Http <input type="radio"/> Sftp	
<b>Local File</b>	D:\running-config	浏览...

**Destination File**

<b>File Name</b>
<input checked="" type="radio"/> startup-config

Download To Switch

Figure 16 Download Configuration File –HTTP

### Download To Switch

#### File To Download

Transport protocols	<input type="radio"/> Http <input checked="" type="radio"/> Sftp
User name	admin
Password	123
Server IP address	192.168.0.23
Server file name	running-config

#### Destination File

File Name	<input checked="" type="radio"/> startup-config
-----------	---

Figure 17 Download Configuration File –SFTP

### Local File

Function: Select the configuration file stored in local.

#### {User name, Password}

Range: {1~63 characters, 1~63 characters}

Description: Input the username and password created on SFTP server.

#### Server IP address

Format: A.B.C.D

Description: Configure the IP address of the SFTP server.

#### Server file name

Range: 1~63 characters

Description: Configure the configuration file name stored on SFTP server.



#### Caution:

- When transferring files by SFTP, you need to configure SFTP user name, password, and SFTP server IP address.
- In the file transmission, keeps the SFTP server running.

You can download the configuration file from local /server to switch as a new startup file for the switch. The new startup file will replace the original **startup-config** file. Click <Download

To Switch> to download the configuration file from local /server to switch.

## 6. USB Configuration

Download and upload configuration files via USB flash drive, as shown in Figure 18

### Auto Configuration

Please note: USB download/upload config file is startup-config.

**Auto Configuration**  Disable  Enable

After the state is enabled, the device automatically downloads the configuration file and takes effect when the device boots.

### Index USB File List

USB flash may not exist.

**USB File name**

To download or delete files, you need to enter the existing filename in the list of USB files.

Upload configuration file does not need to enter the file name.

Figure 18 USB Configuration

Automatic configuration: enable / disable

Description: After the automatic configuration switch is enabled, the device will automatically download the USB flash drive configuration file and take effect when the device starts.

USB flash drive file name: You need to enter the file name that exists in the USB flash drive file list to download or delete the configuration file. You do not need to enter a file name to upload the configuration file.

## 4 Basic Configuration

### 4.1 System Information

System information includes contact, system name, device type, MAC address, S/N, system time, and version information, as shown in Figure 19.

System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	Chongxin Creative Building, No.18 Shixing East Street, Shijingshan District, Beijing 100041, P.R.China
Hardware	
Device Type	Aquam8012A-3GE9P
Device MAC Address	00-01-c1-00-00-00
S/N	201501090000000001
Time	
System Date	2015-12-22T02:10:08+00:00
System Uptime	0d 01:20:57
Software	
Software Version	R0001
Code Date	Dec 7 2015 15:34:03
Code Revision	Build-24.0.11.2
Hardware Version	V1.0
Logic Version	V1.0.1

Figure 19 System Information

### 4.2 System Configuration

System configuration includes contact, system name, and location configuration, as shown in Figure 20.

System Configuration

System Contact	+86-10-88798888
System Name	SWITCH
System Location	No.901 Floor 8 to 12, Building No.2,S

Figure 20 System Configuration

#### System Contact

Range: 0~255 characters (ASCII characters from 32 to 126)

#### System Name

Range: 0~255 characters (alphabet A~Z / a~z, digits 0~9, minus sign -. The first character must be an alpha character, and the first or last character must not be a minus sign.



### System Location

Range: 0~255 characters (ASCII characters from 32 to 126)

### 4.3 CPU Load

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals, as shown in Figure 21.

CPU Load

Running Time	CPU Load
100ms	2%
1sec	0%
10sec	4%

Figure 21 CPU Load

### 4.4 Firmware Upgrade

Firmware upgrade may help the switch to improve its performance. For this series switches, Firmware upgrade includes Boot version update and system software version update. The Boot version should be updated before the system software version. If the Boot version does not change, you can update only the system software version. Firmware upgrade needs the assistance of HTTP/SFTP.

#### 4.4.1 Firmware Upgrade by HTTP

1. Upgrade firmware, as shown in Figure 22.

**Firmware Upgrade**

Transport protocols	<input checked="" type="radio"/> Http <input type="radio"/> Sftp
Upgrade Target	<input checked="" type="radio"/> Application <input type="radio"/> Bootloader
Upgrade Mode	<input checked="" type="radio"/> First <input type="radio"/> Second <input type="radio"/> All
Local File	D:\工作\工作\新建文件夹\SICOM300 <input type="button" value="浏览..."/>

Figure 22 Upgrade Firmware-HTTP

#### Upgrade Target

Options: Application/Bootloader

Function: Select the upgrade target.

**Upgrade Mode**

Options: First/Second/All

Description: Two software versions can be downloaded to the switch, and they can be the same or different. All indicates version 1 and version 2.

**Local File**

Function: Select the version file stored in local.

2. When the upgrade is completed as shown in Figure 23, please activate the software version and reboot the device, open the System Information page to check whether the upgrade succeeded and the new version is active.

Firmware update in progress



Completed!

Figure 23 Upgrade Successfully



**Warning:**

- When upgrade completes, activate the software version and reboot the device to make the new version take effect.
- If upgrade fails, do not reboot the device to avoid the loss of software file and startup anomaly.

**4.4.2 Firmware Upgrade by SFTP**

The Secure File Transfer Protocol (SFTP) is an SSH-based file transfer protocol. It provides encrypted file transfer to ensure security.

The following example uses MSFTP to describe the configuration of the SFTP server and the firmware upgrade process.

1. Add an SFTP user, as shown in Figure 24. Enter the user and password, for example, admin and 123. Set the port number to 22. Enter the path for saving the firmware version file in Root path. Click <Start> button.



Figure 24 Adding an SFTP User

2. Upgrade firmware, as shown in Figure 25.

### Firmware Upgrade

Transport protocols	<input type="radio"/> Http <input checked="" type="radio"/> Sftp
Upgrade Target	<input checked="" type="radio"/> Application <input type="radio"/> Bootloader
Upgrade Mode	<input type="radio"/> First <input type="radio"/> Second <input checked="" type="radio"/> All
User name	admin
Password	123
Server IP address	192.168.0.23
File name	Aquam8012A-1U-F0002.bin
<input type="button" value="Submit"/>	

Figure 25 Upgrade Firmware- SFTP

#### Upgrade Target

Options: Application/Bootloader

Function: Select the upgrade target.

#### Upgrade Mode

Options: First/Second/All

Description: Two firmware versions can be downloaded to the switch, and they can be the same or different. All indicates version 1 and version 2.

#### {User name, Password}

Range: {1~63 characters, 1~63 characters}

Description: Input the user name and password created on SFTP server.

**Server IP address**

Format: A.B.C.D

Description: Configure the IP address of the SFTP server.

**File name**

Range: 1~63 characters

Description: Configure the firmware update file name stored on SFTP server.

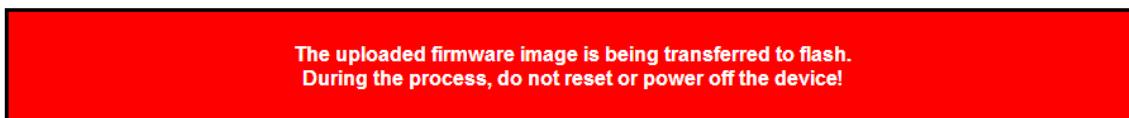


**Warning:**

The file name must contain an extension. Otherwise, the upgrade may fail.

3. When the upgrade is completed as shown in Figure 26, please activate the software version and reboot the device, open the System Information page to check whether the update succeeded and the new version is active.

Firmware update in progress



Completed!

Figure 26 Upgrade Successfully



**Warning:**

- In the firmware upgrade process, keeps the SFTP server running.
- When upgrade completes, reboot the device to activate the new version.
- If upgrade fails, do not reboot the device to avoid the loss of software file and startup anomaly.

## 4.5 Firmware Application Activate

Activate the firmware application, as shown in Figure 27.

### Fireware Application Activate

Select application file to activate.

Application Selected	Current Startup	Application Version	Version
<input checked="" type="radio"/>	✓	App-1	R0002
<input type="radio"/>		App-2	R0002

Figure 27 Activate the Firmware Application

Select one version and click <Activate Application> button, configuring the version to be active version that is the next startup version. Only one can be active version at a time.

Current Startup indicates the version is current running version.

## 5 IP Configuration

### 5.1 IP Address Configuration

1. View the switch IP address by using the console port.

Log in to the switch CLI through the console port. Run the "**show interface vlan 1**" command in the Privileged mode to view the switch IP address, as shown in the red circle of Figure 28.

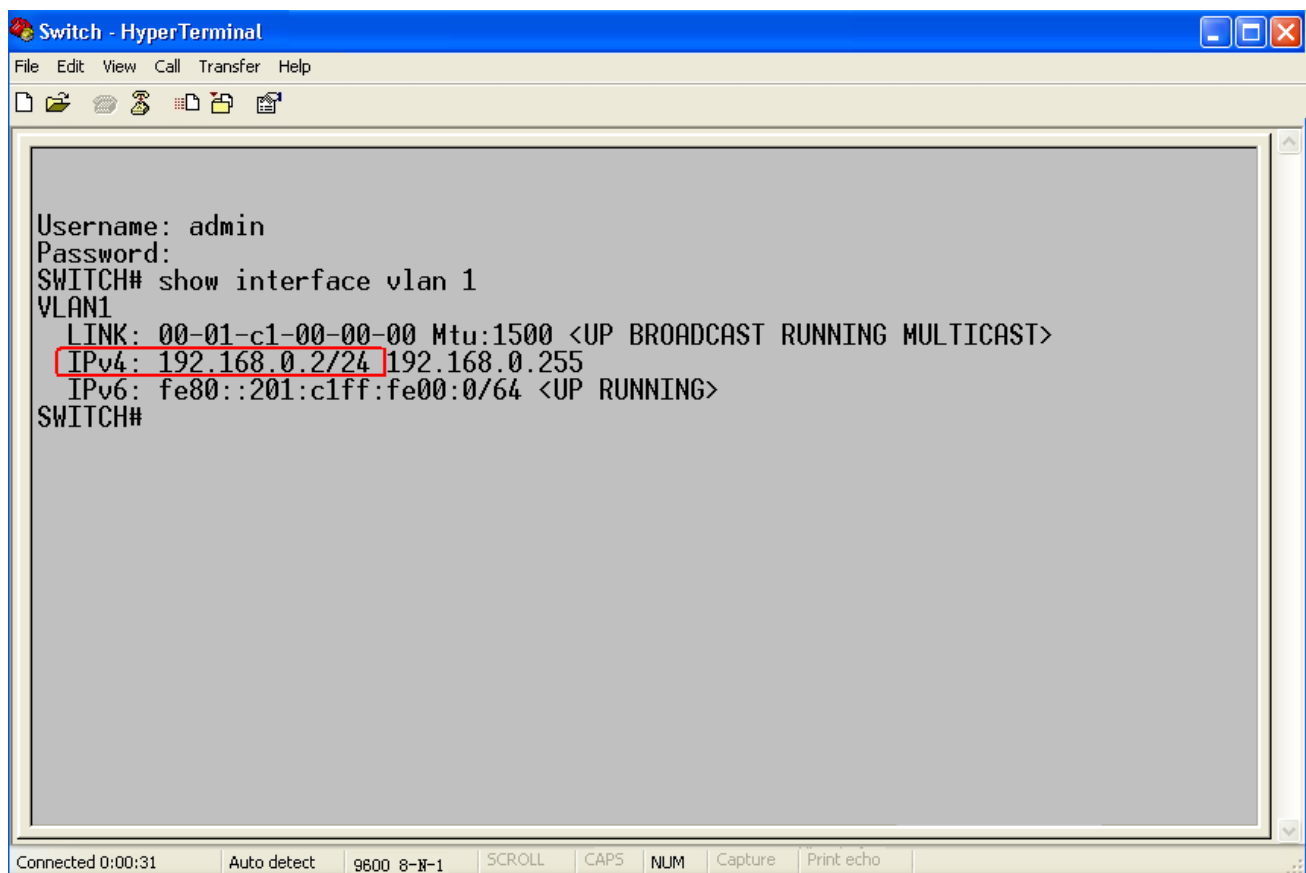


Figure 28 Display IP Address

2. Create IP interface.

Hosts in different VLANs cannot communicate with each other. Their communication packets need to be forwarded by a router or Layer 3 switch through a IP interface. This series switches support IP interfaces, which are virtual Layer 3 interfaces used for inter-VLAN communication. You can create one IP interface for each VLAN. The interface is used for forwarding Layer 3 packets of the ports in the VLAN.

3. Configure IP address

Switch IP address can be manually configured or automatically obtained, as shown in Figure 29.

**IP Configuration**

Mode Host

**IP Interfaces**

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	192.168.0.100/24	192.168.0.20	24		
<input type="checkbox"/>	2	<input type="checkbox"/>	0		192.168.1.20	24		
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	0					

Add Interface

**IP Routes**

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Submit Reset

Figure 29 Configure IP Address

**VLAN**

Function: Configure VLAN attribute of the IP interface, only ports in this VLAN will be able to access the IP interface.

**DHCPv4-Enable**

Options: Enable/Disable

Function: Disable DHCPv4, configure IP address and mask manually; enable DHCPv4, switch (as DHCP client) automatically obtains an IP address through DHCP. There should be a DHCP server in the network to assign IP addresses and mask to clients.

**DHCPv4-Fallback**

Range: 0~4294967295s

Function: If the value is not zero, the switch obtains the IP address attempt time over the Dynamic Host Configuration Protocol (DHCP). In this case, the IP address needs to be configured manually. After the attempt time expires, the IP address that is manually configured takes effect. If the value is 0, the switch repeatedly tries to acquire an IP address till it obtains an IP address over DHCP. In this case, the IP address does not need to be manually configured.

**DHCPv4-Current Address**

Function: Display the IP address and mask length that is automatically acquired from the DHCP server. If the switch fails to acquire an IP address over DHCP during the attempt time, the IP address and mask length that are manually configured are displayed in **Current Address**.

#### IPv4-Address

Format: A.B.C.D

Function: Manually configure IP address .

#### IPv4-Mask Length

Function: The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. Mask length is the number of "1" in subnet mask.

Click <Add Interface> to add a new IP interface, a maximum of 8 interfaces is supported.



#### Caution:

- Each IP interface supports one IP address.
  - IP addresses of different network segments should be configured for different IP interfaces.
- 

4. View IP interfaces, as shown in Figure 30.



**IP Interfaces**

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN2	LINK	00-01-c1-00-00-00	<BROADCAST MULTICAST>
VLAN2	IPv4	192.168.1.20/24	
VLAN2	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN3	LINK	00-01-c1-00-00-00	<BROADCAST RUNNING MULTICAST>
VLAN3	IPv6	fe80::201:c1ff:fe00:0/64	

**IP Routes**

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

**Neighbour Cache**

IP Address	Link Address
192.168.0.184	VLAN1:44-37-e6-88-6e-90
fe80::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN2:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN3:00-01-c1-00-00-00

Figure 30 View IP Interfaces

## 5.2 ARP

### 5.2.1 Introduction

The Address Resolution Protocol (ARP) resolves the mapping between IP addresses and MAC addresses by the address request and response mechanism. The switch can learn the mapping between IP addresses and MAC addresses of other hosts on the same network segment. It also supports static ARP entries for specifying mapping between IP addresses and MAC addresses. Dynamic ARP entries periodically age out, ensuring consistency between ARP entries and actual applications.

This series switches provide not only Layer 2 switching function, but also the ARP function for resolving the IP addresses of other hosts on the same network segment, enabling the communication between the NMS and managed hosts.

### 5.2.2 Web Configuration

1. Configure ARP aging time, as shown in Figure 31.

### Dynamic ARP timeout

timeout(min)	5
--------------	---

Figure 31 Configuring Aging Time

#### timeout

Range: 0 ~ 60min

Default: 5min

Function: Configure ARP aging time, when aging time is set to 0, aging is prohibited.

Description: ARP aging time is the duration from when a dynamic ARP entry is added to the table to when the entry is deleted from the table.

2. Add static ARP entry, as shown in Figure 32.

### Add/Del Static ARP

Delete	IPv4 Address	MAC Address
<input type="checkbox"/>	192.168.1.23	00-01-01-01-01-02
<input type="checkbox"/>	192.168.0.23	00-01-01-01-01-01

Add

Submit    Reset

Figure 32 Adding Static ARP Entry

#### ARP

Portfolio: {IP address, MAC address}

Format: {A.B.C.D, HHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure static ARP entry.



**Caution:**

In general, the switch automatically learns ARP entries. Manual configuration is not required.

Click <Add> to add a new static ARP entry, a maximum of 128 static ARP entries is supported.

### 5.3 DHCP Configuration

With the continuous expansion of network scale and the growing of network complexity,

under the conditions of the frequent movement of computers (such as laptops or wireless network) and the computers outnumbering the allocable IP addresses, the BootP protocol that is specially for the static host configuration has become increasingly unable to meet actual needs. For fast access and exit network and improving the utilization ratio of IP address resources, we do need to develop an automatic mechanism based on BootP to assign IP addresses. DHCP (Dynamic Host Configuration Protocol) was introduced to solve these problems.

DHCP employs a client-server communication model. The client sends a configuration request to the server, and then the server replies configuration parameters such as an IP address to the client, achieving the dynamic configuration of IP addresses. The structure of a DHCP typical application is shown in Figure 33.

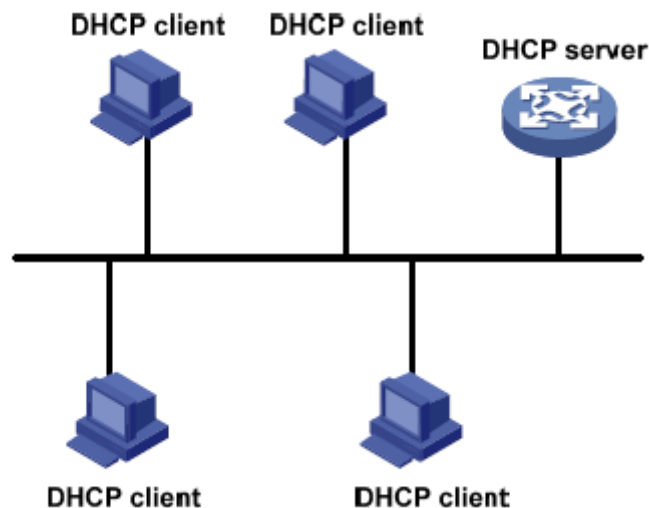


Figure 33 DHCP Typical Application



**Caution:**

In the process of dynamic obtainment of IP addresses, the messages are transmitted in the way of broadcast, so it is required that the DHCP client and the DHCP server are in a same segment. If they are in the different segments, the client can communicate with the server via a DHCP relay to get IP addresses and other configuration parameters.

DHCP supports two types of IP address allocation mechanisms.

Static allocation: the network administrator statically binds fixed IP addresses to few specific clients such as a WWW server and sends the binding IP addresses to clients by DHCP. The

tenancy term for static allocation is permanent.

Dynamic allocation: DHCP server dynamically allocates an IP address to a client. This allocation mechanism can allocate a permanent IP address or an IP address with a limited lease period to a client. When the lease expires, the client needs to reapply an IP address.

The network administrator can choose a DHCP allocation mechanism for each client.

### **5.3.1 DHCP Server Configuration**

#### **5.3.1.1 Introduction**

DHCP server is a provider of DHCP services. It uses DHCP messages to communicate with DHCP client to allocate a suitable IP address to the client and assign other network parameters to the client as required. In the following conditions, the DHCP server generally is used to allocate IP addresses.

- Large network scale. The workload of manual configuration is heavy and it is hard to manage the entire network.
- The hosts outnumber the assignable IP addresses, and it is unable to allocate a fixed IP address to each host.
- Only a few hosts in the network need fixed IP addresses.

#### **5.3.1.2 DHCP Address Pool**

The DHCP server selects an IP address from an address pool and allocates it together with other parameters to the client. The IP address allocation sequence is as follows:

1. The IP address statically bound to the client MAC address.
2. The IP address that is recorded in the DHCP server that it was ever allocated to the client.
3. The IP address that is specified in the request message sent from the client.
4. The first allocable IP address found in an address pool.
5. If there is no available IP address, check the IP address whose lease expires and that had conflicts in order. If found, allocate the IP address. If not, no process.

#### **5.3.1.3 Web Configuration**

1. Enable DHCP server, as shown in Figure 34.

### DHCP Server Mode Configuration

#### Global Mode

Mode  ▾

#### VLAN Mode

	VLAN Range	Mode
	1 - 2	Enabled
	6 - 20	Enabled
<input type="button" value="Cancel"/>	<input type="text"/> - <input type="text"/>	Enabled ▾

Figure 34 Enable DHCP Server

#### Global Mode

Options: Disabled/Enabled

Default: Disabled

Function: Select the current switch to the DHCP server to allocate an IP address to a client or not.

#### {VLAN Range, Mode}

Range: {1~4095, Disabled/Enabled}

Function: If the VLAN of a client that applies for an IP address is set to Enabled, the DHCP server allocates an IP address to the client. Otherwise, the DHCP server does not allocate an IP address to the client.

2. Create DHCP address pool, as shown in Figure 35.

**DHCP Server Pool Configuration**

**Pool Setting**

Delete	Name	Type	IP	Subnet Mask	Lease Time
<input type="checkbox"/>	<u>pool-1</u>	-	-	-	1 days 0 hours 0 minutes

Add New Pool

Submit    Reset

Figure 35 Create DHCP Address Pool

**Name**

Range: 1~32 characters

Function: configure the name of the IP address pool.

Click <Add New Pool> to create a new DHCP address pool.

3. Configure the DHCP address pool, click <Name> in Figure 35 to configure the DHCP address pool, as shown in Figure 36.

### DHCP Pool Configuration

Pool

Name

Setting

Pool Name	<input type="text" value="pool-1"/>
Type	Host <input type="button" value="v"/>
IP	<input type="text" value="192.168.0.6"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Lease Time	<input type="text" value="1"/> days (0-365)
	<input type="text" value="0"/> hours (0-23)
	<input type="text" value="0"/> minutes (0-59)
Domain Name	<input type="text" value="domain.com"/>
Broadcast Address	<input type="text"/>
Default Router	<input type="text" value="192.168.0.201"/>
	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
DNS Server	<input type="text" value="192.168.0.202"/>
	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
NTP Server	<input type="text" value="192.168.0.203"/>
	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
NetBIOS Node Type	None <input type="button" value="v"/>
NetBIOS Scope	<input type="text"/>
NetBIOS Name Server	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
NIS Domain Name	<input type="text"/>
NIS Server	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
	<input type="text" value="0.0.0.0"/>
Client Identifier	MAC <input type="button" value="v"/> <input type="text" value="00-11-22-33-44-55"/>
Hardware Address	<input type="text" value="00-11-22-33-44-55"/>
Client Name	<input type="text"/>
Vendor 1 Class Identifier	<input type="text"/>
Vendor 1 Specific Information	<input type="text"/>
Vendor 2 Class Identifier	<input type="text"/>
Vendor 2 Specific Information	<input type="text"/>
Vendor 3 Class Identifier	<input type="text"/>
Vendor 3 Specific Information	<input type="text"/>
Vendor 4 Class Identifier	<input type="text"/>
Vendor 4 Specific Information	<input type="text"/>

Figure 36 Configure IP Address Pool

**Name**

Function: select a created pool name.

**Type**

Options: None/Network/Host

Default: None

Function: Configure the address pool type. Network: the switch dynamically allocates IP addresses to multiple DHCP clients. Host: the switch supports static allocation of IP addresses to special DHCP clients.

**{IP, Subnet Mask}**

Function: Network indicates that you can configure the range of the IP address pool, and the address range is determined by the subnet mask. The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. It is generally configured to 255.255.255.0.

Host indicates that you can configure the IP address of the client statically bounded. Static IP address allocation is implemented by bounding the MAC address and IP address of the client. When the client with this MAC address requests for IP address, the DHCP server finds the IP address corresponding to the MAC address of the client and allocates the IP address to the client. The priority of this allocation mode is higher than that of dynamic IP address allocation, and the tenancy term is permanent.

**Lease Time**

Range: 0 day 0 hour 0 minute~365 days 23 hours 59 minutes

Default: 1 day 0 hour 0 minute

Description: Configure lease timeout of dynamic allocation. For different address pools, DHCP server can set different address lease time, but the addresses in the same DHCP address pool have the same lease time.

**Domain Name**

Range: 1~36 characters

Function: Configure the domain name of the IP address pool. When allocating an IP address



to a client, send the domain name suffix to the client too.

### **Broadcast Address**

Format: A.B.C.D

Function: Configure the client broadcast address allocated by DHCP server.

### **Default Routing**

Format: A.B.C.D

Function: Configure the client gateway address allocated by DHCP server.

Explanation: when the DHCP client visits the host that is in the different segment, the data must be forwarded via gateways. When the DHCP server allocates IP addresses to clients, it can specify gateway addresses at the same time. DHCP address pool can configure max 4 gateways.

### **DNS Server**

Format: A.B.C.D

Function: Configure the client DNS server address allocated by DHCP server.

Explanation: When visiting the network host via a domain name, the domain name needs to be resolved to an IP address, which is realized by DNS (Domain Name System). In order to let a DHCP client visit a network host via a domain name, when the DHCP server allocates IP addresses to clients, it can specify IP addresses of domain name servers at the same time. DHCP address pool can configure max 4 DNS servers.

### **NTP Server**

Format: A.B.C.D

Function: Configure the client NTP server address allocated by DHCP server.

### **NetBIOS Node Type**

Options: None/B-node/P-node/M-node/H-node

Default: None

Function: Configure the client NetBIOS node type allocated by DHCP server. When the DHCP client uses the NetBIOS protocol for communication on the network, a mapping must be established between the host name and IP address. Different node types obtain the mapping in different modes.

Description: The B-node obtains the mapping by broadcast. The P-node obtains the

mapping by sending a unicast packet to communicate with the WINS server. The M-node obtains the mapping by sending a broadcast packet the first time. If the M-node fails to obtain the mapping the first time, it obtains the mapping by sending a unicast packet to communicate with the WINS server the second time. The H-node obtains the mapping by sending a unicast packet to communicate with the WINS server the first time. If the H-node fails to obtain the mapping the first time, it obtains the mapping by sending a broadcast packet the second time.

**NetBIOS Scope**

Range: 1~36 characters

Function: Configure the NetBIOS name.

**NetBIOS Name Server**

Format: A.B.C.D

Function: Configure the client WINS server address allocated by the DHCP server.

Explanation: For the client running a Microsoft Windows operating system (OS), the Windows Internet Naming Service (WINS) server provides the service of resolving a host name into an IP address for the host that uses the NetBIOS protocol for communication. Therefore, most Windows OS-based clients require WINS configuration. To enable the DHCP client to resolve a host name into an IP address, specify the WINS server address when the DHCP server allocates an IP address to the client. DHCP address pool can configure max 4 WINS servers.

**NIS Domain Name**

Range: 1~36 characters

Function: Configure the client NIS domain name allocated by DHCP server.

**NIS Server**

Format: A.B.C.D

Function: Configure the client NIS server address allocated by DHCP server.

**Client Identifier**

Options: None/FQDN/MAC

Default: None

Function: When the pool type is host, specify client's unique identifier

**Hardware Address**

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: When the pool type is host, configure the MAC address of the client statically bounded.

**Client Name**

Range: 1~32 characters

Function: When the pool type is host, configure client user name.

**Vendor i Class Identifier**

Range: 1~64 characters

Function: Configure the client Vendor Class Identifier allocated by DHCP server.

**Vendor i Specific Information**

Range: 1~64 hexadecimal numbers

Function: Configure the client Vendor Specific Information allocated by DHCP server.

4. Configure excluded IP addresses (IP addresses are not allocated dynamically in the DHCP address pool), as shown in Figure 37.

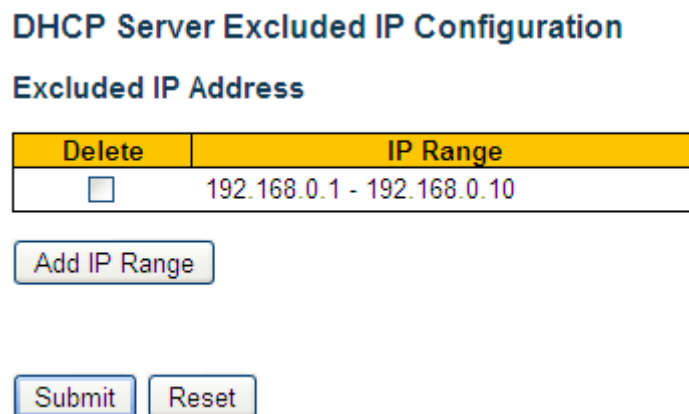


Figure 37 Configure Excluded IP Addresses

**IP Range**

Function: Configure the range of IP addresses are not allocated dynamically in the DHCP address pool. When allocating IP addresses, the DHCP server must eliminate the occupied IP address (for example, IP addresses of the gateway and DNS server). Otherwise, the same IP address may be allocated to two clients, causing IP address conflict.

Click <Add IP Range> to configure the range of IP addresses are not allocated dynamically.

5. View DHCP server statistics information, as shown in Figure 38.

**DHCP Server Statistics**

**Database Counters**

Pool	Excluded IP Address	Declined IP Address
1	1	0

**Binding Counters**

Automatic Binding	Manual Binding	Expired Binding
1	0	0

**DHCP Message Received Counters**

Discover	Request	Decline	Release	Inform
20	9	0	0	40

**DHCP Message Sent Counters**

Offer	ACK	NAK
5	5	2

Figure 38 View DHCP Server Statistics Information

6. View information about IP addresses allocated by the DHCP server, as shown in Figure 39.

**DHCP Server Binding IP**

**Binding IP Address**

Delete	IP	Type	State	Pool Name	Server ID
<input type="checkbox"/>	192.168.0.11	Automatic	Committed	pool-1	192.168.0.223

Figure 39 View Information about IP Addresses Allocated by the DHCP Server

7. View the IP addresses declined by DHCP clients, as shown in Figure 40.

**DHCP Server Declined IP**

**Declined IP Address**

Declined IP
192.168.0.11

Figure 40 View the IP addresses Declined by DHCP Clients

When a client detects that an IP address allocated by the server conflicts with a static IP address in the same network segment, it sends a decline packet to the server to reject this

IP address. The server records the IP address rejected by the client, and will not allocate this IP address to other clients within a certain period of time.

#### 5.3.1.4 Typical Configuration Example

As Figure 41 shows, switch A works as a DHCP server and switch B works as a DHCP client. The port 3 of Switch A connects to the port 4 of Switch B. The client sends out IP address request messages and the server can allocate an IP address to the client in two ways. The excluded IP address range is 192.168.0.1~192.168.0.10 when DHCP server dynamically allocates IP address.

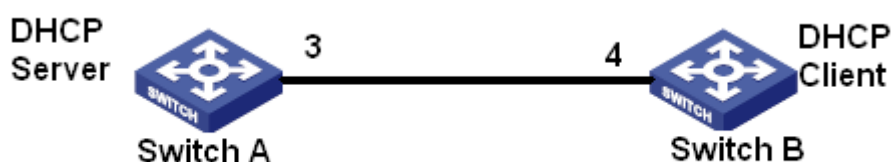


Figure 41 DHCP Typical Configuration Example

#### Statically allocate IP address

➤ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 34.
2. Create a DHCP IP pool: pool-1, as shown in Figure 35.
3. Set the pool type as Host; IP address as 192.168.0.6, mask as 255.255.255.0. Bind the MAC address of switch B: 00-11-22-33-44-55, as shown in Figure 36.

➤ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.
2. The switch B obtains the IP address of 192.168.0.6 and the subnet mask of 255.255.255.0 from the DHCP server, as shown in Figure 42.

IP Configuration

Mode

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	5	192.168.0.6/24	192.168.0.222	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Figure 42 DHCP Client Obtain IP Address-1

**Dynamically allocate IP address**

➤ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 34.
2. Create a DHCP IP pool: pool-1, as shown in Figure 35.
3. Set the pool type as Network; IP address as 192.168.0.6; mask as 255.255.255.0, as shown in Figure 36.
4. Configure excluded IP address range as 192.168.0.1~192.168.0.10, as shown in Figure 37.

➤ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.
2. DHCP server searches the assignable IP addresses in the address pool in order and allocates the first found assignable IP address and other network parameters to Switch B. The subnet mask is 255.255.255.0, as shown in Figure 43.

IP Configuration

Mode

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	5	192.168.0.11/24	192.168.0.222	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Figure 43 DHCP Client Obtain IP Address-2

### 5.3.2 DHCP Snooping

#### 5.3.2.1 Introduce

DHCP Snooping is a monitoring function of DHCP services on layer 2 and is a security feature of DHCP, ensuring the security of the client further. The DHCP Snooping security mechanism can control that only the trusted port can forward the request message of the DHCP client to the legal server, meanwhile, it can control the source of the response message of the DHCP server, ensuring the client to obtain an IP address from the valid server and preventing the fake or invalid DHCP server from allocating IP addresses or other configuration parameters to other hosts.

DHCP Snooping security mechanism divides port to trusted port and untrusted port.

Trusted port: it is the port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: it is the port that connects with the invalid DHCP server. Untrusted port does not forward the request messages of DHCP clients and the response messages of DHCP servers to prevent DHCP clients from obtaining invalid IP addresses.

#### 5.3.2.2 Web Configuration

1. Enable DHCP Snooping function, as shown in Figure 44.

### DHCP Snooping Configuration

Snooping Mode Enabled ▾

Figure 44 DHCP Snooping State

#### DHCP Snooping Mode

Options: Enable/Disable

Default: Disable

Function: Enable/Disable switch DHCP Snooping function.



**Caution:**

The switch working as DHCP server and client cannot enable DHCP Snooping function.

2. Configure trusted ports, as shown in Figure 45.

#### Port Mode Configuration

Port	Mode
*	<> ▾
1	Trusted ▾
2	Trusted ▾
3	Untrusted ▾
4	Trusted ▾
5	Trusted ▾
6	Trusted ▾
7	Trusted ▾
8	Trusted ▾
9	Trusted ▾
10	Trusted ▾
11	Trusted ▾
12	Trusted ▾

Figure 45 Configure Trust Port

#### Mode

Options: Trusted/Untrusted

Default: Untrusted

Function: set the port to a trusted port or an untrusted port. The ports that connect with valid DHCP servers directly or indirectly are trusted ports.





**Caution:**

The trusted port configuration and Port Trunk is mutually exclusive. The port joining in a trunk group cannot be set to a trusted port. The trusted port cannot join in a trunk group.

**5.3.2.3 Typical Configuration Example**

As Figure 46 shows, the DHCP client requests an IP address from the DHCP server. An unauthorized DHCP server exists in the network. Set port 1 to a trusted port by DHCP Snooping to forward the request message of the DHCP client to the DHCP server and forward the response message of the DHCP server to the DHCP client. Set port 3 to an untrusted port that cannot forward the request message of the DHCP client and the response message of the unauthorized DHCP server, ensuring that the client can obtain a valid IP address from the valid DHCP server.

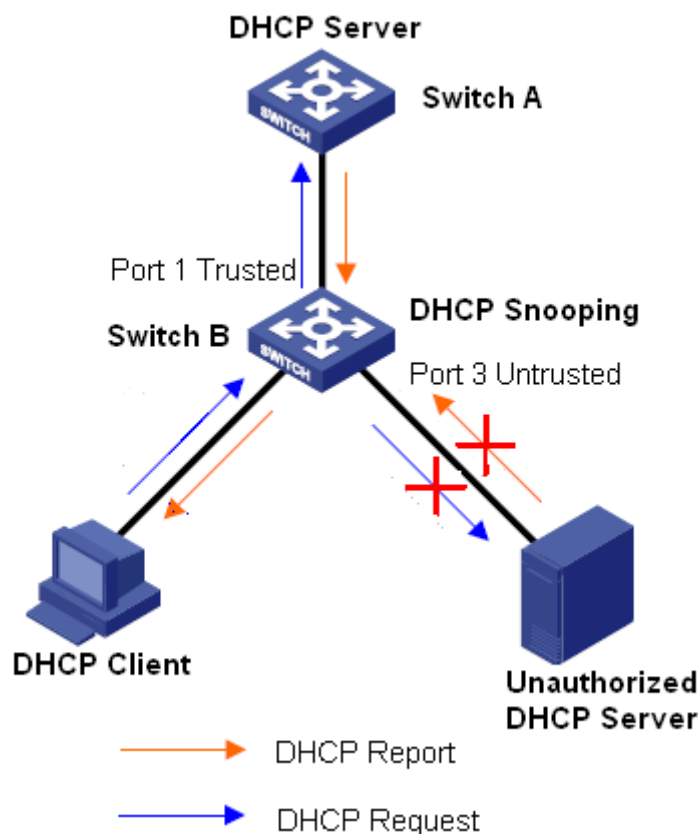


Figure 46 DHCP Snooping Typical Configuration Example

Switch B configuration:

- Enable DHCP Snooping function, as shown in Figure 44.
- Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as

shown in Figure 45.

Default: Trusted

### 5.3.3 Option 82 Configuration

Option 82 (Relay Agent Information Entry) records the client information. When the Option 82 supported DHCP Snooping receives the request message from the DHCP client, it add the corresponding Option 82 field into the messages and then forward the message to the DHCP server. The server supporting Option 82 can flexibly allocate addresses according to the Option 82 message.

Once Option 82 is enabled, the Option 82 field will be added into the message. The Option 82 field of this series switches contains two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

- Sub-option 1 contains the VLAN ID and number of the port that receives the request message from the DHCP client, as shown in Table 2.

Table 2 Sub-option 1 Field Format

Sub-option type (0x01)	Length (0x04)	VLAN ID	Port number
One byte	One byte	Two bytes	Two bytes

Sub-option type: the type of the sub-option 1 is 1.

Length: the number of bytes that VLAN ID and Port number occupy.

VLAN ID: On DHCP Snooping device, the VLAN ID of the port that receives the request message from the DHCP client.

Port number: On DHCP Snooping device, the number of the port that receives the request message from the DHCP client.

- The content of Sub-option 2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client, as shown in Table 3.

Table 3 Sub-option 2 Field Format-MAC Address

Sub-option type (0x02)	Length (0x06)	MAC Address
One byte	One byte	6 bytes

Sub-option type: the type of the sub-option 2 is 2

Length: the number of bytes that sub-option2 content occupies. MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the content of sub-option2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client.

### 5.3.3.1 DHCP Snooping Supports Option 82 Function

#### 1 Introduction

If DHCP Snooping device supports Option 82 function, when the DHCP Snooping receives a DHCP request message, it will process the request message according to whether the message contains Option 82 and the client policy, and then forward the processed message to the DHCP server. The specific processing method is shown in Table 4.

Table 4 Processing Modes for Request Messages (DHCP Snooping)

Receive the request message from the DHCP client	Configuration policy	DHCP Snooping device processing the request message
The request message contains Option 82	Drop	Drop the request message
	Keep	Keep the message format unchanged and forward the message
	Replace	Replace the Option 82 field in the message with the Option 82 field of the Snooping device and forward the new message
The request message does not contain Option 82	Drop/Keep/Replace	Add the Option 82 field of the Snooping device into the message and forward it

When the DHCP Snooping device receives the response message from the DHCP server, if the message contains Option 82 field, remove the Option 82 field and forward the message to the client

#### 2 Web Configuration

DHCP Snooping Option 82 configuration is shown in Figure 47.

**Option82 Configuration**

<b>Option82 Status</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Client Policy</b>	<input type="radio"/> Replace <input checked="" type="radio"/> Keep <input type="radio"/> Drop

Figure 47 DHCP Snooping Option82 Configuration

**Option82 Status**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable Option82 function on DHCP Snooping device.

**Client Policy**

Options: Drop/Replace/Keep

Default: Replace

Function: Configure client policy. The DHCP Snooping device processes the request message sent from the Client according to Client Policy, as shown in Table 4.

## 6 Clock System

### 6.1 Clock Configuration

Configure the time zone, as shown in Figure 48.

#### Time Zone Configuration

Time Zone Configuration	
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi <input type="button" value="v"/>
Acronym	china ( 0 - 16 characters )

Figure 48 Configure the Time Zone

#### Time Zone

Function: Select the local timezone.

#### Acronym

Function: Description the time zone.

Configure daylight saving time, as shown in Figure 49 and Figure 50.

To make full use of time and save energy, Daylight Saving Time (DST) can be used in summer. To be specific, adjust clock forward some time in summer. DST configuration includes recurring and Non-recurring configuration.

### Daylight Saving Time Configuration

Daylight Saving Time Mode		
Daylight Saving Time	Recurring	
Start Time settings		
Week	1	
Day	Mon	
Month	Apr	
Hours	10	
Minutes	0	
End Time settings		
Week	1	
Day	Mon	
Month	Oct	
Hours	9	
Minutes	0	
Offset settings		
Offset	60	(1 - 1440) Minutes

Figure 49 Configure Recurring DST

### Daylight Saving Time Configuration

Daylight Saving Time Mode		
Daylight Saving Time	Non-Recurring	
Start Time settings		
Month	Apr	
Date	1	
Year	2015	
Hours	10	
Minutes	0	
End Time settings		
Month	Oct	
Date	1	
Year	2015	
Hours	9	
Minutes	0	
Offset settings		
Offset	60	(1 - 1440) Minutes

Figure 50 Configure Non-Recurring DST

**Daylight Saving Time**

Options: Disabled/Recurring/Non-Recurring

Default: Disabled

Function: Enable or disable DST. After DST is enabled, clock will be adjusted forward some time in summer. Recurring means recurring time year by year.

**Start Time setting /End Time setting**

Function: After DST is enabled, configure the time segment for DST. In non-Recurring mode, you need to configure year, month, date, hour, and minute to specify the time segment for DST. As shown in Figure 50, the DST is configured to be executed in the period from 10:00 a.m. April 1, 2015 to 9:00 a.m. October 1, 2015. You can set the month, week, day, hour, and minute in cycle mode to specify the DST execution time range every year. For example, you can configure the DST to be executed from 10:00 a.m. on the first Monday in April to 9:00 a.m. on the first Monday in October every year in Figure 49.

**Offset**

Range: 1~1440min

Default: 1min

Function: Set the DST clock offset, that is, the time length that the clock is brought forward for the DST execution.



**Caution:**

- Start time should be different from end time.
- Start time indicates non-DST time. End time indicates DST time.

For example, run DST from 10:00:00 April 1st to 9:00:00 October 1st. The offset is 60 min. Non-DST time will run until 10:00:00 April 1st. Then the clock jumps to 11:00:00 to start DST. DST runs until 9:00:00 October 1st. Then the clock jumps back to 8:00:00 to run non-DST time.

**6.2 SNTP**

The Simple Network Time Protocol (SNTP) synchronizes time between server and client by

means of requests and responses. As a client, the switch synchronizes time from the server according to packets of the server.



**Caution:**

- To synchronize time by SNTP, there must be an active SNTP server.
- All the time information carried in the SNTP protocol is standard time information of time zone 0.

**SNTP Configuration**

<b>Mode</b>	Enabled <input type="button" value="v"/>
<b>Server Address</b>	192.168.0.184

Figure 51 Enable SNTP

**Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable SNTP.

**Server Address**

Format: A.B.C.D

Function: Configure the IP address of the SNTP server. Clients will synchronize time according to server packets.

Check whether the clock is synchronized from the server.

Click [Basic Configuration] → [System Information] to view the clock information, as shown in Figure 52.



System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	SICOM3000A-2GX8GE
Device MAC Address	00-1e-cd-1c-e8-e0
S/N	S30U0035Axxxxxxxxx
Time	
System Date	1970-01-02T00:30:08+00:00
System Uptime	1d 00:30:08
Software	
Software Version	R3001
Code Date	Jul 25 2018 09:02:04
Code Revision	Build-24.0.44.2.B1.4.3
Hardware Version	V1.0
Logic Version	V1.0.0

Figure 52 View the Clock Information

You can view the switch time information based on the server time, in combination with the selected time zone and DST configuration.

## 6.3 PTP

### 6.3.1 Introduction

The Precision Time Protocol (PTP) synchronizes independent clocks on distributed nodes of the measurement and control system with high precision and accuracy. The protocol synchronizes both phase and frequency with precision up to ±100ns. Note: In the series products, only SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L3GT, and SICOM3028GPT-L3FT support PTP.

#### PTP Concepts

##### 1. PTP domain

A network on which PTP is applied is a PTP domain. A PTP domain has only one master clock. All the other devices synchronize time from it.

##### 2. PTP port

A PTP-enabled port is called PTP port

##### 3. Clock node

The nodes in a PTP domain are clock nodes. PTP defines the following clock nodes:

### ➤ Boundary Clock (BC)

In a PTP domain, the BC node has one or multiple PTP ports participating in clock synchronization. If only one PTP port participates in clock synchronization, the port synchronizes time from uplink clock node or to downlink clock node. If multiple PTP ports take part in clock synchronization, one of these ports synchronizes time from uplink clock node and the other ports synchronize time to downlink clock nodes. When the BC serves as the clock source, it can deliver time to downlink clock nodes through multiple PTP ports.

### ➤ Transparent Clock (TC)

The TC node does not need to keep time with other clock nodes. It has multiple PTP ports. These ports only forward PTP packets and verify forwarding delay, but do not perform clock synchronization. Transparent transmission clocks fall into the following types:

End-to-End Transparent Clock (E2ETC): directly forwards non-PTP packets and participates in delay calculation of the entire link.

Peer-to-Peer Transparent Clock (P2PTC): directly forwards Sync, Follow\_Up, and Announce packets, terminates other PTP packets, and participates in delay calculation of each segment of a link.

Relationship between a pair of synchronous clock nodes:

- The node sending synchronization clock information is the master mode, while the nodes receiving the information are slave nodes.
- The clock of the master node is master clock, while the clock of a slave node is slaveclock.
- The port sending synchronization clock information is the master port, while the ports receiving the information are slave ports

## 6.3.2 Synchronization Principle

### 1. Selection of the grandmaster clock

All clock nodes select the grandmaster clock in the PTP domain by exchanging Announce packets with clock stratum and clock ID information. Then the master/slave relationship

between nodes and master/slave ports on the nodes are determined. With this process, a spanning tree with the grandmaster clock as the root is established throughout the PTP domain. Then the master clock periodically sends Announce packets to slave clocks. If a slave clock does not receive Announce packets from the master clock within a period, the master clock is considered invalid and new selection is started.

Announce packets contain the following information for grandmaster clock selection: grandmaster priority 1, clock stratum, clock accuracy, grandmaster priority 2, and clock ID.

The information is compared in the following procedure: the clock with lowest grandmaster priority 1 is elected as the grandmaster clock; if clocks have the same value for grandmaster priority 1, the clock with lowest clock stratum is elected as the grandmaster clock; similarly, if clocks have the same values for grandmaster priority 1, clock stratum, clock accuracy, grandmaster priority 2, the clock with lowest clock ID is elected as the grandmaster clock.

## 2. Synchronization principle

Master and slave clocks exchange synchronization packets, record sending and receiving time of packets, and calculate the total delay between master and slave clocks based on time difference. If the network path is symmetric, the unidirectional delay is half the total delay. A slave clock adjusts local time according to the time difference between master and slave clocks and unidirectional delay, implementing time synchronization from the master Clock

PTP supports two delay measurement mechanisms:

- Request-response mechanism: used for the end-to-end delay measurement of an entire link.
- Peer-to-peer mechanism: used for point-to-point delay measurement. Compared with the request\_response mechanism, the peer-to-peer mechanism measures the delay of each segment of a link.

### 6.3.3 Web Configuration

1. PTP Clock Configuration: as shown in Figure 53

**PTP Clock Configuration**

Delete	Clock Instance	Device Type	Profile
<input type="checkbox"/>	0	Ord-Bound	1588

Figure 53 PTP Clock Configuration

Clock Instance:

Range:0~3

Function: Configure PTP Instance

Device Type:

Range: Ord-Bound/P2pTransp/E2eTransp/Masteronly/Slaveonly

Function: Configure PTP Clock Type

Profile:

Range: No Profile/1588

Function: Select PTP Description File



**Caution:**

➤Profile 1588 cannot utilize with E2eTransp

2.Click Instance No.to enter PTP detailed configuration, as shown in Figure 54:

PTP Clock's Configuration

Port Enable and Configuration

Port Enable										Configuration
1	2	3	4	5	6	7	8	9	10	Ports Configuration
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Local Clock Current Time

PTP Time	Clock Adjustment method	System Clock Sync to PTP time	PTP time Sync to System Clock
1970-01-01T01:01:02+00:00 785,491,480	Internal Timer	False	False

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Clock Parent DataSet

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:1e:cd:ff:fe:1c:e8:e1	0	False	0	0	00:1e:cd:ff:fe:1c:e8:e1	Cl:251 Ac:Unknwn Va:65535	100	128

Clock Default DataSet

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	
0	Ord-Bound	False	10	00:1e:cd:ff:fe:1c:e8:e1	0	Cl:251 Ac:Unknwn Va:65535	
Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VLAN ID	PCP	DSCP
100	128	IPv4Multi	False	True	1	0	0

Clock Time Properties DataSet

UTC Offset	Valid	Leap59	Leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False	False	False	False	False	True	160

Submit Reset

Figure 54 PTP instance detailed configuration

2.1 Port enable and configuration

Port Enable:

Function: Select one port to enable PTP

Configuration:

Click Ports Configuration, to reach the PTP clock port data configuration page, as shown in Figure 545.

PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	DIm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
5	Isth	0	0.000,000,000	0	3	0	e2e	0	0	0	0	2

Submit Reset

Figure 55 Ports Configuration

Anv:

Range:-3~4

Function: The time interval for issuing announce messages in master state.

**Ato:**

Range:1~10

Function: The timeout for receiving announce messages on the port.

**Syv:**

Range:-7~4

Function: The time interval for issuing sync messages in master.

**Dlm:**

Range: p2p/e2e

Function: Configurable member delay mechanism. The delay mechanism used for the port:

e2e End to end delay measurement

p2p Peer to peer delay measurement.

Can be defined per port in an Ordinary/Boundary clock.

In a transparent clock, all ports use the same delay mechanism, determined by the clock type.

**MPR:**

Range: -7~5

Function: The interval for issuing Delay\_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave.

The interval for issuing Pdelay\_Req messages for the port in P2P mode.

**Delay Asymmetry:**

Range:-100000~100000ns

Function: Delay compensation for asymmetric links

**Ingress latency:**

Range:-100000~100000ns

Function: Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

**Egress Latency:**

Range:-100000~100000ns

Function: Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2

## 2.2 Clock Current Dataset

Shows the actual PTP time with nanosecond resolution, there are two methods: synchronize the System Clock to PTP Time or synchronize PTP Time to the System Clock. However, the two are mutually exclusive and cannot be selected as TRUE at the same time.

## 2.3 Clock Default Dataset

### **2 Step Flag:**

enable 2 step flag

### **Domain:**

configure domain id of PTP instance

### **Pri 1:**

Clock priority 1 [0..255] used by the BMC master select algorithm.

### **Pri 2;**

Clock priority 2 [0..255] used by the BMC master select algorithm.

### **Protocol:**

Range: Ethernet/IPv4Multi

Function: Transport protocol used by the PTP protocol engine.

Description: Ethernet PTP over Ethernet multicast/IPv4Multi PTP over IPv4 multicast

### **One-Way:**

If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

### **VLAN Tag Enable:**

Enables the VLAN tagging for the PTP frames.

Note: Packets are only tagged if the port is configured for vlan tagging for the configured VLAN

### **VlanID:**

Range:1-4094

### **PCP:**

Range: 0~7

Description: Priority Code Point value used for PTP frames.

**DSCP:**

Range: 0~63

Description: Differentiated Services Code Point value used for PTP frames.

2.3 Clock Time Properties Data Set

**UTC Offset:**

Range: 0-10000

**Valid:**

Range: TRUE/FALSE

**Leap59, Leap61:**

Description: leap second

**Time Trac、Freq Trac:**

Range: TRUE/FALSE

**PTP Time Scale:**

Range: TRUE/FALSE

**Time Source:**

The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

16 (0x10) ATOMIC\_CLOCK

32 (0x20) GPS

48 (0x30) TERRESTRIAL\_RADIO

64 (0x40) PTP

80 (0x50) NTP

96 (0x60) HAND\_SET

144 (0x90) OTHER



160 (0xA0) INTERNAL\_OSCILLATOR

3.PTP Status

Shows PTP clock configuration, as shown in Figure 56

PTP Clock Configuration

		Port List									
Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10
0	Ord-Bound										✓

Figure 56 PTP clock configuration

Shows PTP instance detailed configuration, as shown in Figure 57

PTP Clock's Configuration

Auto-refresh

Local Clock Current Time			
PTP Time	Clock Adjustment method	Ports Page	
1970-01-01T04:50:22+00:00 152,387,820	Internal Timer	Ports	

Clock Default DataSet															
ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP	DSCP	
0	Ord-Bound	False	10	00:1e:cd:ff:fe:1c:e8:e1	0	Cl:251 Ac:Unknwn Va:65535	100	128	IPv4Multi	False	True	1	0	0	

Clock Current DataSet					
stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
0	0.000,000,000	0.000,000,000	0	FREERUN	N.A.

Clock Parent DataSet							
Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1 Pri2
00:1e:cd:ff:fe:1c:e8:e1	0	False	0	0	00:1e:cd:ff:fe:1c:e8:e1	Cl:251 Ac:Unknwn Va:65535	100 128

Clock Time Properties DataSet							
UTC Offset	Valid	Leap59	Leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False	False	False	False	False	True	160

Figure 57 PTP instance detailed configuration

6.3.4 Typical Configuration Example

As shown in Figure 58, port 1 of Switch A is connected to port 2 of Switch B, and port 3 of Switch B is connected to port 4 of Switch C. Switch A is a master clock (BC clock type). Switch B uses P2PTC clock type. Switch C is a slave clock (BC clock type), and synchronizes time from Switch A by using PTP protocols.

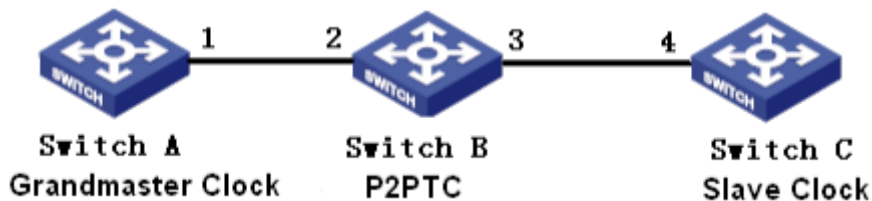


Figure 58 PTP Configuration Example

Configuration on Switch A:

1. Enable PTP on port 1 of Switch A.
2. Set the clock type to Boundary. Because Switch A is the master clock, it should have the best grandmaster priority1. In this example, set the grandmaster priority1 to 200 and the delay measurement mechanism to peer-to-peer, as shown in Figure 53、 Figure 54.

Configuration on Switch B:

3. Enable PTP on port 2 and port 3 of Switch B.
4. Set the clock type to P2PTC, the grandmaster priority1 to 210, and the delay measurement mechanism to peer-to-peer, as shown in Figure 53、 Figure 54.

Configuration on Switch C:

5. Enable PTP on port 4 of Switch C.
6. Set the clock type to Boundary, the grandmaster priority1 to 220, and the delay measurement mechanism to peer-to-peer, as shown in Figure 53、 Figure 54.

## 7 Port Configuration

1. Configure port status, port speed, flow control, and other information, as shown in Figure 59.

Port Configuration

Port	Link	Speed		Adv Duplex		Adv Speed			Flow Control			Maximum Frame Size	Excessive Collision Mode	Reset
		Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx			
*		<>	<>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	<>	<input type="checkbox"/>
1	100fdx	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
2	100fdx	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
3	100fdx	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
4	Down	Down	10Mbps HDX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
5	Down	Down	10Mbps FDX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
6	Down	Down	100Mbps HDX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
7	Down	Down	100Mbps FDX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
8	Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
9	Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
10	Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
11	Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
12	Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>

Submit    Reset

Figure 59 Port Configuration

### Link

Display the link status of ports.

Green: The port is in LinkUp state and can communicate normally.

Red: The port is in LinkDown state and cannot communicate normally.

### Speed-Current

Display the communication speed and duplex mode of ports.

### Speed-Configuration

Options: Disabled/Auto/10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX//1Gbps FDX

Default: Auto

Function: Configure the speed and duplex mode of ports. Disabled indicates the port is disabled and disallows data transmission. This option directly affects the hardware status of the port and triggers port alarms.

Description: The speed and duplex mode of ports can be automatically negotiated or forcibly set. When Auto is set, the port speed and duplex mode will be automatically negotiated

according to port connection status. You are advised to enable auto-negotiation for each port to avoid the connection problems caused by mismatched port configuration. If you want to force port speed/duplex mode, please make sure the same speed/duplex mode configuration in the connected ports at both ends.

**Caution:**

- The 10/100Base-TX port can be set to Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX.
- The 10/100/1000Base-TX port can be set to Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX.

**Adv Duplex**

Options: Fdx/Hdx

Function: Configure the auto-negotiation duplex mode of ports.

Description: Fdx indicates the port can receive and transmit data at the same time; Hdx indicates the port only receives or transmits data at the same time. When the port mode is set to Auto, the duplex mode of the port is determined by means of negotiation with the peer by default. The negotiated duplex mode can be either Fdx or Hdx. The parameter can be configured for a port to negotiate only one duplex mode, thereby controlling the negotiation of the duplex mode.

**Adv Speed**

Options: 10M/100M/1G

Function: Configure the auto-negotiation speed of ports.

Description: When the port mode is set to **Auto**, the port speed is determined by means of negotiation with the peer by default. The negotiated speed can be any rate within the port rate capability range. The parameter can be configured for a port to negotiate only some rates, thereby controlling the speed negotiation.

**Caution:**

The Adv Duplex configuration and Adv Speed configuration take effect only in auto mode.

**Flow Control**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable flow control function on the designated port.

Description: Once the flow control function is enabled, the port will inform the sender to slow the transmitting speed to avoid packet loss by algorithm or protocol when the port-received flow is bigger than the size of port cache. If the devices work in different duplex modes (half/full), their flow control is realized in different ways. If the devices work in full duplex mode, the receiving end will send a special frame (Pause frame) to inform the sending end to stop sending packets. When the sender receives the Pause frame, it will stop sending packets for a period of "wait time" carried in the Pause frame and continue sending packets once the "wait time" ends. If the devices work in half duplex mode, they support back pressure flow control. The receiving end creates a conflict or a carrier signal. When the sender detects the conflict or the carrier wave, it will take backoff to postpone the data transmission.

**Curr Rx/Curr Tx**

Function: Display the flow control status of the port.

**Maximum Frame Size**

Range: 1518~9600 bytes

Default: 9600 bytes

Function: Set the maximum size of a packet that is received by a port. Packets with the size larger than the value are discarded.

**Reset**

Options: Enabled/Disabled

Default: Disabled

Function: Reset the port or not.

2. View the port statistics, as shown in Figure 60.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1275387	11523	98799397	2629185	0	0	869612	0	609
2	184535	1092883	17294542	80989316	0	0	1226	0	125257
3	227	183345	26332	16672027	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Figure 60 Port Statistics

**Port**

Click <port> to enter the “detailed port statistics” page.

**Packets**

Display the number of packets that each port sends/receives.

**Bytes**

Display the number of bytes that each port sends/receives.

**Errors**

Display the number of error packets that each port sends/receives.

**Drops**

Display the number of packets that are discarded due to transmission/receiving conflicts.

**Filtered Received**

Display the number of packets that are filtered out by the receive end.

Click <port> to enter the “detailed port statistics” page.

3. View detailed port statistics, as shown in Figure 61.

Detailed Port Statistics Port 2 Port 2 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	11065	Tx Packets	11
Rx Octets	1034290	Tx Octets	1276
Rx Unicast	10	Tx Unicast	0
Rx Multicast	1110	Tx Multicast	11
Rx Broadcast	9945	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	3043	Tx 64 Bytes	0
Rx 65-127 Bytes	7529	Tx 65-127 Bytes	11
Rx 128-255 Bytes	365	Tx 128-255 Bytes	0
Rx 256-511 Bytes	83	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	45	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	11065	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	11
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	8073		

## Figure 61 Detailed Port Statistics

Select a port, and view the designated port detailed statistics.

## 8 QoS Configuration

### 8.1 Introduction

Quality of Service (QoS) enables differentiated services based on different requirements under limited bandwidths by means of traffic control and resource allocation on IP networks. QoS tries to satisfy the transmission of different services to reduce network congestion and minimize congestion's impact on the services of high priority.

Traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the main concepts of QoS deployment. They mainly complete the following functions:

**Traffic classification:** identifies an object based on certain matching rules. It is the basis and prerequisite of QoS.

**Traffic policing:** supervises the traffic rate of packets that are transmitted to a device. When the traffic rate exceeds the specified traffic rate, the device adopts restriction or penalty measures to protect network resources against damage. Traffic policing is classified into port-based traffic policing and queue-based traffic policing.

**Traffic shaping:** proactively adjusts traffic output rate. It aims at adapting traffic to available network resources of a downstream device to prevent unnecessary packet discarding and congestion. Traffic shaping is classified into port-based traffic shaping and queue-based traffic shaping.

**Congestion management:** This is mandatory for solving resource competition. Congestion management caches packets in queues and determines the sequence of packet forwarding based on a certain scheduling algorithm, achieving preferential forwarding for key services.

**Congestion avoidance:** Excessive congestion may result in damage on network resources. Congestion avoidance monitors the use of network resources. When detecting increasing congestion, the function adopts proactive packet discarding and tunes traffic volume to solve the overload.

Traffic policing, traffic shaping, congestion management, and congestion avoidance control the network traffic and allocated resources from different aspects. They are the specific



embodiment of QoS. For example, the switch supervises packets that are transmitted to a network based on the committed rate. It conducts shaping on the packets before the packets leave the switch. It conducts queue scheduling management in the case of congestion, and adopts congestion avoidance measures when the congestion is intensifying.

## 8.2 Principle

Each port of this series switches supports 8 cache queues, from 0 to 7 in priority ascending order.

When a frame reaches the port, the switch determines the queue for the frame according to the frame information and port. This series switches support traffic classification in the following queue mapping modes: port, 802.1Q header information, differentiated services code point (DSCP), and QoS control list (QCL), with the priority in ascending order.

When forwarding data, a port uses a scheduling mode to schedule the data in 8 queues and the bandwidth of each queue. This series switches support two scheduling modes: 6 Queues Weighted and SP (Strict Priority) .

WRR (Weighted Round Robin) schedules data flows based on weight ratio. Queues obtain their bandwidths based on their weight ratio. WRR prioritizes high-weight ratio queues. More bandwidths are allocated to queues with higher weight ratio.

SP mode forwards high-priority packets preferentially. It is mainly used for transmitting sensitive signals. If a frame enters the high-priority queue, the switch stops scheduling the low-priority queues and starts to process the data of the high-priority queue. When the high-priority queue contains no data, the switch starts to process the data of the queue with lower priority.

6 Queues Weighted indicates that queue 6 and queue 7 use the Strict Priority scheduling mode, and queue 0 ~ queue 5 use the WRR scheduling mode. Data in queue 7 is processed prior to data in queue 6. When both queue 7 and queue 6 are empty, data in queue 0 ~ queue 5 is scheduled based on the weight ratio.

## 8.3 Web Configuration

1. Configure port-based queue mapping mode, as shown in Figure 62.

### QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>
1	2	0	1	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source
9	0	0	0	0	Disabled	<input type="checkbox"/>	Source
10	0	0	0	0	Disabled	<input type="checkbox"/>	Source
11	0	0	0	0	Disabled	<input type="checkbox"/>	Source
12	0	0	0	0	Disabled	<input type="checkbox"/>	Source

Figure 62 Configure Port-based Queue Mapping Mode

#### CoS

Range: 0~7

Default: 0

Function: Configure port default CoS value.

Description: The CoS value determines the queue for storing packets. The CoS value ranges from 0 to 7, which respectively corresponds to queue 0 to queue 7. After a packet is transmitted to the switch, the switch allocates the CoS value to the packet. If the received packet is tag type and the tag classification is disabled, or the received packet is untag type, the CoS value in the packet is the default CoS value of the port that receives the packet.

#### PCP

Range: 0~7

Default: 0

Function: Configure the default PCP (Priority Code Point) value of the port.

Explanation: When a packet is untagged, the priority in the tag added to the packet is the default PCP value of the port.

#### DEI

Range: 0~1

Default: 0

Function: Configure the default DEI (Drop Eligible Indicator) value of the port.

Explanation: When a packet is untagged, the CFI in the tag added to the packet is the default DEI value of the port.

2. Configure 802.1Q frame header-based queue mapping mode

Click <Tag Class> in Figure 62 to enter 802.1Q frame header queue mapping mode configuration page, as shown in Figure 63.

**QoS Ingress Port Tag Classification Port 2** Port 2 ▾

**Tagged Frames Settings**

**Tag Classification** Enabled ▾

**(PCP, DEI) to (QoS class, DP level) Mapping**

PCP	DEI	QoS Class	DP Level
*	*	◇ ▾	◇ ▾
0	0	2 ▾	0 ▾
0	1	3 ▾	1 ▾
1	0	0 ▾	0 ▾
1	1	0 ▾	1 ▾
2	0	2 ▾	0 ▾
2	1	2 ▾	1 ▾
3	0	3 ▾	0 ▾
3	1	3 ▾	1 ▾
4	0	4 ▾	0 ▾
4	1	4 ▾	1 ▾
5	0	5 ▾	0 ▾
5	1	5 ▾	1 ▾
6	0	6 ▾	0 ▾
6	1	6 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Figure 63 Configure 802.1Q Frame Header Queue Mapping Mode

**Tag Classification**

Options: Enabled/Disabled

Default: Disabled

Function: Whether to enable the 802.1Q header information-based queue mapping mode. This queue mapping mode has a higher priority over the port-based queue mapping mode.



**Caution:**

The 802.1Q header information-based queue mapping mode is applicable only to tagged packets received by a port.

**(PCP, DEI) to (QoS class, DP level) Mapping**

Range: 0~7 (QoS class) 0~1 (DP Level)

Default: The PCP value range is 0, 1, 2, 3, 4, 5, 6, and 7, which are respectively mapped to the QoS classes 1, 0, 2, 3, 4, 5, 6, and 7. The DEI value range is 0 and 1, which are respectively mapped to the DP levels 0 and 1.

Function: Set the mapping from (PCP, DEI) to (CoS, DPL) based on PCP and DEI values in packets.

Description: The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0-7 respectively correspond to queues 0-7. After a packet is transmitted to the switch, the switch allocates the CoS value and DPL value to the packet. The CoS value and DPL value of the packet are (CoS, DPL) mapped from (PCP, DEI) if the received packet is tag type, and the tag classification is enabled.

You can select a port to configure the 802.1Q header information-based queue mapping mode in the upper right corner of the page.

3. Configure 802.1p remarking, as shown in Figure 64.

**QoS Egress Port Tag Remarking**

Port	Mode
1	Classified
2	Mapped
3	Default
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

Figure 64 Configure 802.1p Remarking

**Mode**

Option: Classified/Mapped/Default

Function: Displays the 802.1p retagging mode when an egress port forwards packets. 802.1p retagging is used to update the PCP value and DEI value in packets when an egress port forwards packets.



**Caution:**

If packets forwarded by an egress port are untagged, the 802.1p retagging function is unavailable.

Click <Port> to enter 802.1p remarking configuration page.

- Configure 802.1p remarking mode to Classified, as shown in Figure 65.

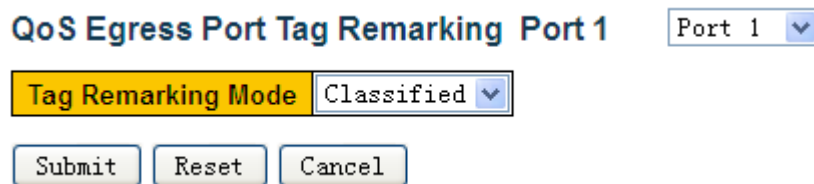


Figure 65 Configure 802.1p Remarking Mode to Classified

**Tag Remarking Mode**

Options: Classified/Mapped/Default

Default: Classified

Function: Configure 802.1p remarking mode. Classified: The PCP value and DEI value in packets are not updated when an egress port forwards the packets.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

- Configure 802.1p remarking mode to Default, as shown in Figure 66.

**QoS Egress Port Tag Remarking Port 3** Port 3 ▾

**Tag Remarking Mode** Default ▾

**PCP/DEI Configuration**

<b>Default PCP</b>	5 ▾
<b>Default DEI</b>	0 ▾

Figure 66 Configure 802.1p Remarking Mode to Default

**Tag Remarking Mode**

Options: Classified/Mapped/Default

Default: Classified

Function: Configure 802.1p remarking mode. Default: The PCP value and DEI value in packets are updated to the default values (set in the lower part of the page) of an egress port when the egress port forwards the packets.

**Default PCP**

Range: 0~7

Default: 0

Function: Set the default PCP value of an egress port.

**Default DEI**

Range: 0~1

Default: 0

Function: Set the default DEI value of an egress port.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

- Configure 802.1p remarking mode to Mapped, as shown in Figure 67.

**QoS Egress Port Tag Remarking Port 2** Port 2 ▾

**Tag Remarking Mode** Mapped ▾

**(QoS class, DP level) to (PCP, DEI) Mapping**

QoS Class	DP Level	PCP	DEI
*	*	◇ ▾	◇ ▾
0	0	1 ▾	0 ▾
0	1	1 ▾	1 ▾
1	0	0 ▾	0 ▾
1	1	0 ▾	1 ▾
2	0	3 ▾	0 ▾
2	1	2 ▾	1 ▾
3	0	3 ▾	0 ▾
3	1	4 ▾	1 ▾
4	0	4 ▾	0 ▾
4	1	4 ▾	1 ▾
5	0	5 ▾	0 ▾
5	1	5 ▾	1 ▾
6	0	6 ▾	0 ▾
6	1	6 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Figure 67 Configure 802.1p Remarking Mode to Mapped

**Tag Remarking Mode**

Options: Classified/Mapped/Default

Default: Classified

Function: Configure 802.1p remarking mode. Mapped: The PCP value and DEI value in packets are updated to the (PCP, DEI) mapped from (CoS, DPL) when an egress port forwards the packets. The mapping is configured in the lower part of the page.

**(QoS class, DP level) to (PCP, DEI) Mapping**

Range: 0~7 (PCP) 0~1 (DEI)

Default: The QoS class range is 0, 1, 2, 3, 4, 5, 6, and 7, which are respectively mapped to the PCP values 1, 0, 2, 3, 4, 5, 6, and 7. The DP level value range is 0 and 1, which are respectively mapped to the DEI values 0 and 1.

Function: Configure the mapping from (CoS, DPL) to (PCP, DEI) based on the CoS and DPL values in packets.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

4. Enable DSCP-based queue mapping mode, as shown in Figure 68.

### QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>
1	0	0	0	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input checked="" type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input checked="" type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source
9	0	0	0	0	Disabled	<input type="checkbox"/>	Source
10	0	0	0	0	Disabled	<input type="checkbox"/>	Source
11	0	0	0	0	Disabled	<input type="checkbox"/>	Source
12	0	0	0	0	Disabled	<input type="checkbox"/>	Source

Figure 68 Enable DSCP-based Queue Mapping Mode

### DSCP-Based

Options: Enabled/Disabled

Default: Disabled

Function: Whether to enable the DSCP-based queue mapping mode. This queue mapping mode has a higher priority over the 802.1Q header information-based queue mapping mode.

5. Enable the DSCP translation of an ingress port and the DSCP rewriting function of an egress port, as shown in Figure 69.



### QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Disable ▾	Disable ▾
2	<input type="checkbox"/>	Disable ▾	Disable ▾
3	<input checked="" type="checkbox"/>	All ▾	Enable ▾
4	<input type="checkbox"/>	Disable ▾	Disable ▾
5	<input type="checkbox"/>	Disable ▾	Disable ▾
6	<input type="checkbox"/>	Disable ▾	Disable ▾
7	<input type="checkbox"/>	Disable ▾	Disable ▾
8	<input type="checkbox"/>	Disable ▾	Disable ▾
9	<input type="checkbox"/>	Disable ▾	Disable ▾
10	<input type="checkbox"/>	Disable ▾	Disable ▾
11	<input type="checkbox"/>	Disable ▾	Disable ▾
12	<input type="checkbox"/>	Disable ▾	Disable ▾

Figure 69 Configure Port DSCP Function

#### Translate

Options: Enabled/Disabled

Default: Disabled

Function: Whether to translate the DSCP value in a packet received by an ingress port. If it is set to Enable, the DSCP value is translated according to the DSCP translation table (“Translate” column in Figure 71).

#### Classify

Options: Disable/DSCP=0/Selected/All

Default: Disable

Function: Selects the rewritten DSCP value of an egress port when Rewrite is set to Enable.

Disable: The DSCP value in packets is not rewritten when an egress port forwards the packets.

DSCP=0: When an egress port forwards packets, if the DSCP values in the packets are 0, the DSCP values in the packets are rewritten according to the classification in Figure 72.

Selected: When an egress port forwards packets, if the DSCP values in the packets are a selected value (“Classify” column in Figure 71), the DSCP values in the packets are rewritten

according to the classification in Figure 72.

All: When an egress forwards packets, the DSCP values in the packets are written according to the classification in Figure 72.

**Rewrite**

Options: Disable/Enable/Remap DP Unaware/Remap DP Aware

Default: Disable

Function: Set the rewriting mode of the DSCP value in packets when an egress port forwards the packets.

Disable: The DSCP values in packets are not rewritten when an egress port forwards the packets.

Enable: Whether the DSCP values in packets are rewritten is determined based on the classify configuration when an egress port forwards the packets.

Remap DP Unaware: The DSCP values in packets are rewritten based on the mapping (“Remap DP0” column in Figure 71) from (DSCP, DPL=0) to DSCP when an egress forwards the packets.

Remap DP Aware: The DSCP values in packets are rewritten based on the mapping (“Remap DP0” and “Remap DP1” columns in Figure 71) from (DSCP, DPL) to DSCP when an egress forwards the packets.

6. Configure DSCP-based queue mapping mode, as shown in Figure 70.

**DSCP-Based QoS Ingress Classification**

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input checked="" type="checkbox"/>	6	0
5	<input checked="" type="checkbox"/>	2	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0

Figure 70 Configure DSCP-based Queue Mapping Mode

## Trust

Options: Enabled/Disabled

Default: Disabled

Function: Whether to trust the DSCP value.

---

**Caution:**

The DSCP-based queue mapping mode is applicable only to the DSCP values in packets received by a port are trusted

---

## QoS Class

Range: 0~7

Default: 0

Function: Set the mapping from DSCP to CoS.

Description: The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0~7 respectively correspond to queues 0~7. After a packet with the DSCP value being a trusted value is transmitted to the switch, the switch allocates the CoS value to the packet according to the mapping from DSCP to CoS.

---

**Caution:**

If translate is enabled for an ingress port, the switch allocates the CoS value based on the translated DSCP value. Otherwise, the switch allocates the CoS value based on the original DSCP value in packets.

---

7. Configuring DSCP translation and rewriting, as shown in Figure 71.

### DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input checked="" type="checkbox"/>	<>	<>
0 (BE)	7	<input checked="" type="checkbox"/>	0 (BE)	0 (BE)
1	5	<input checked="" type="checkbox"/>	1	1
2	8 (CS1)	<input checked="" type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	8 (CS1)	4
5	5	<input type="checkbox"/>	9	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)

Figure 71 Configuring DSCP Translation and Rewriting

#### Translate

Range: 0~63

Function: Set the translation table of DSCP values.

#### Classify

Options: Enabled/Disabled

Default: Disabled

Function: When Classify is set to Selected in Figure 69, this parameter is used to set the selected DSCP value.



**Caution:**

When translate is enabled for an ingress port, the selected DSCP value is the DSCP value after translation. Otherwise, the selected DSCP value is the original DSCP value in packets.

#### Remap DP0/ Remap DP1

Range: 0~63

Function: Set the mapping from (DSCP, DPL) to DSCP values.

8. Configure DSCP classification, as shown in Figure 72.

### DSCP Classification

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	4	5
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Submit    Reset

Figure 72 Configure DSCP Classification

### DSCP DP0/DSCP DP1

Range: 0~63

Function: Set the mapping from (CoS, DPL) to DSCP values. The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0-7 respectively correspond to queues 0-7.

9. Configure QCL entry, as shown in Figure 73.

#### QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	2	Unicast	Any	Any	Any	Any	Any	Any	5	Default	Default	Default	Default	Default	⊕ ⊖ ⊕ ⊖ ⊕ ⊖ ⊕ ⊖
2	3	Any	Any	Any	10	4-5	Any	Any	6	Default	Default	6	0	Default	⊕ ⊖ ⊕ ⊖ ⊕ ⊖ ⊕ ⊖
3	4	Any	00-00-00-00-00-23	Any	Any	Any	Any	IPv4	7	1	9	Default	Default	Default	⊕ ⊖ ⊕ ⊖ ⊕ ⊖ ⊕ ⊖
5	Any	Any	Any	Any	Any	Any	Any	Any	1	Default	Default	Default	Default	Default	⊕ ⊖ ⊕ ⊖ ⊕ ⊖ ⊕ ⊖
4	Any	Any	Any	Untagged	Any	Any	Any	Any	4	Default	Default	Default	Default	Default	⊕ ⊖ ⊕ ⊖ ⊕ ⊖ ⊕ ⊖

Figure 73 Configure QCL Entry

The queue mapping of packets is implemented by matching QCL entries. Each entry consists of several conditions in the logical AND relationship. It is considered that a packet received by a member port matches a QCL entry only when the packet meets all the conditions. QCL entries are independent of each other.

When there are multiple QCL entries, the device compares a packet with the QCL entries one by one (from top to bottom). Once a match is found, the action is taken and no further comparison is conducted. Click <⊕> to add a new QCL entry; click <⊖> to edit the QCL

entry; click <⊗> to delete the QCL entry, click <⬆> to move up the current entry; click <⬇> to move down the current entry.

QCE is the ID of a QCL entry, which is numbered based on the entry creation time sequence.

10. Configuration QCL entry parameters

- Select a port on which the current QCL entry takes effect, as shown in Figure 74.

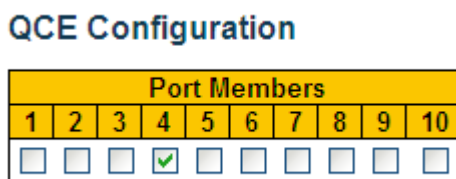


Figure 74 Select Port Member

**Port members**

Function: Select a port on which the current QCL entry takes effect. All ports are member ports by default.

- Configure QCL entry parameters, as shown in Figure 75.

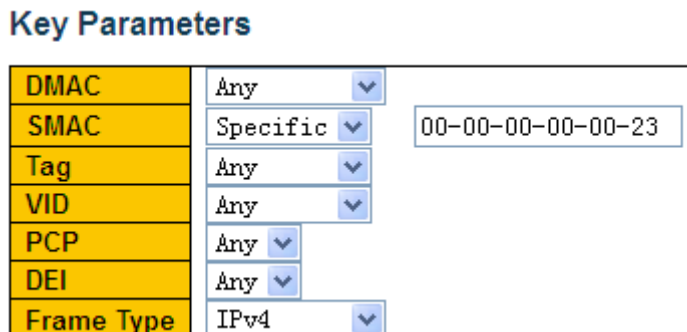


Figure 75 Configure QCL Entry Parameters

**DMAC**

Options: Any/ Unicast/ Multicast / Broadcast

Default: Any

Function: Set a condition--destination MAC address. When the destination MAC address in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

**SMAC**

Options: Any/ Specific

Default: Any

Function: Set a condition--source MAC address. When it is set to Specific, a MAC address needs to be set. When the source MAC address in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

### **Tag**

Options: Any/ Untagged/ Tagged

Default: Any

Function: Set a condition--tag. When a packet received by a member port meets settings of this parameter, the condition is matched successfully.

### **VID**

Options: Any/ Specific (1~4095) / Range (1~4095)

Default: Any

Function: Set a condition--VID. When it is set to Specific, the VID value needs to be set. When it is set to Range, the VID range needs to be set. When the VID in a packet received by a member port meets settings of this parameter, the condition is matched successfully. This parameter is unavailable when Tag is set to Untagged.

### **PCP**

Options: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

Default: Any

Function: Set a condition--PCP. When the PCP value in a packet received by a member port meets settings of this parameter, the condition is matched successfully. This parameter is unavailable when Tag is set to Untagged.

### **DEI**

Options: Any/0/1

Default: Any

Function: Set a condition--DEI. When the DEI value in a packet received by a member port meets settings of this parameter, the condition is matched successfully. This parameter is unavailable when Tag is set to Untagged.

### **Frame Type**

Options: Any/ EtherType/ LLC/ SNAP/ IPv4/ IPv6

Default: Any

Function: Select frame type.

- Configure the EtherType frame parameters, as shown in Figure 76.

**EtherType Parameters**

<b>Ether Type</b>	Specific ▾	Value: 0x0806
-------------------	------------	---------------

Figure 76 Configure the EtherType Frame Parameters

### Ether Type

Options: Any/ Specific (0x0600~0xFFFF)

Default: Any

Function: Set a condition--Ethernet type. When it is set to Specific, an Ethernet type needs to set. When an Ethernet packet received by a member port meets settings of this parameter, the condition is matched successfully.

- Configure the LLC frame parameters, as shown in Figure 77.

**LLC Parameters**

<b>DSAP Address</b>	Specific ▾	Value: 0x60
<b>SSAP Address</b>	Any ▾	
<b>Control</b>	Specific ▾	Value: 0x85

Figure 77 Configure the LLC Frame Parameters

### DSAP Address/SSAP Address/Control

Options: Any/Specific (0x00~0xFF)

Default: Any

Function: Set a condition--LLC packet parameters. When DSAP Address, SSAP Address, or Control is set to Specific, a specific value needs to be entered. When an LLC packet received by a member port meets settings of the parameters, the condition is matched successfully.



- Configure the SNAP frame parameters, as shown in Figure 78.

**SNAP Parameters**

PID

Figure 78 Configure the SNAP Frame Parameters

**PID**

Options: Any/ Specific (0x0000~0xFFFF)

Default: Any

Function: Set a condition--SNAP packet parameter. When it is set to Specific, a PID value needs to be entered. When the PID in an SNAP packet received by a member port meets settings of this parameter, the condition is matched successfully.

- Configure the IPv4/ IPv6 frame parameters, as shown in Figure 79.

**IPv4 Parameters**

Protocol	<input type="text" value="UDP"/>
SIP	<input type="text" value="Specific"/> <input type="text" value="Value: 192.168.1.100"/> <input type="text" value="Mask: 255.255.255.0"/>
IP Fragment	<input type="text" value="Any"/>
DSCP	<input type="text" value="Any"/>

**UDP Parameters**

Sport	<input type="text" value="Specific"/>	<input type="text" value="Value: 4154"/>
Dport	<input type="text" value="Any"/>	

Figure 79 Configure the IPv4 Frame Parameters

**Protocol**

Options: Any/ UDP/ TCP/ Other (0~255)

Default: Any

Function: Set a condition--IPv4 packet protocol type. When it is set to UDP or TCP, a source port ID and a destination port ID need to be set. When it is set to Other, a protocol ID needs to be set. When the protocol type in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

**Sport/ Dport**

Options: Any/ Specific (0~65535) / Range (0~65535)

Default: Any

Function: Set a condition--TCP/UDP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs

to be set. When the port IDs in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

**SIP**

Options: Any/ Specific

Default: Any

Function: Set a condition--source IP address and source IP address mask. When it is set to Specific, an IP address and IP address mask need to be set. When the SIP in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

**IP Fragment**

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP fragment packet. When the fragment in an IPv4 packet received by a member port meets settings of this parameter, the condition is matched successfully.

**DSCP**

Options: Any/ Specific (0~63) / Range (0~63)

Default: Any

Function: Set a condition--DSCP value. When it is set to Specific, a DSCP value needs to be entered. When it is set to Range, the DSCP range needs to be set. When the DSCP in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

➤ Configure the QCL action, as shown in Figure 80.

**Action Parameters**

CoS	5	▼
DPL	Default	▼
DSCP	9	▼
PCP	Default	▼
DEI	Default	▼
Policy		

Figure 80 Configure the QCL Action

**CoS**

Options: 0~7/ Default

Default: 0

Function: The CoS value determines the queue for storing packets. The CoS value ranges from 0 to 7, which corresponds to queue 0 to queue 7. The value Default indicates that the CoS value is 0. When a packet received by a member port matches the QCL entry, the switch allocates a CoS value to the packet.

**DPL**

Options: Default/ 0/ 1

Default: Default

Function: Change the DPL value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the DPL value in a packet is not changed.

**DSCP**

Options: Default/ 0~63

Default: Default

Function: Change the DSCP value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the DSCP value in a packet is not changed.

**PCP**

Options: Default/ 0~7

Default: Default

Function: Change the PCP value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the PCP value in a packet is not changed.

**DEI**

Options: Default/ 0/ 1

Default: Default

Function: Change the DEI value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the DEI

value in a packet is not changed.



**Caution:**

The PCP value and DEI value in a packet cannot be changed separately. That is, the PCP value and DEI value must be changed simultaneously or retain their original values.

➤ View QCL entries, as shown in Figure 81.

**QoS Control List Status**

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static 1	2	Any	5	Default	Default	Default	Default	Default	Default	No
Static 2	3	Any	6	Default	Default	6	0	Default	Default	No
Static 3	4	IPv4	7	1	9	Default	Default	Default	Default	No
Static 5	Any	Any	1	Default	Default	Default	Default	Default	Default	No
Static 4	Any	Any	2	Default	Default	Default	Default	Default	Default	No

Figure 81 View QCL Entries

**Conflict**

Options: No/Yes

Function: Displays the conflict status of a QCL entry. If resources for creating a QCL entry are insufficient, **Conflict** is set to **Yes** for this entry. Otherwise, **Conflict** is set to **No** for this entry.

Click <Resolve Conflict> to release resources required for a conflicting QCL entry so that the resource conflict is solved.

11. Configure ingress port policers, as shown in Figure 82.

### QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	2	Mbps ▾	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	200	fps ▾	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>

Figure 82 Configure Ingress Port Policers

#### Enable

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable ingress port policers. The traffic policing of a port is implemented by port rate limit or port flow control.

#### Rate, Unit

Range: 100~3276700kbps/ 1~3276Mbps/ 100~3276700fps/ 1~3276Kfps

Default: 500kbps

Function: Limit the rate of packets received by a port. Packets with the rate exceeding the value are discarded.

#### Flow Control

Options: Enabled/Disabled

Default: Disabled

Function: Whether to enable port flow control. After flow control is enabled for a port, when the traffic received by the port is larger than the limit value, the sender is instructed to slow down the transmission to prevent packet loss by means of algorithms or protocols.



**Note:**

The precondition for the flow control function taking effect is to enable the port flow control in Port Configuration page (The port should be in LinkUp status ).

12. Configure ingress queue policers, as shown in Figure 83.

**QoS Ingress Queue Policers**

Port	Queue 0	Queue 1	Queue 2		Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	20	Mbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 83 Configure Ingress Queue Policers

**Enable (E)**

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable ingress queue policers. You need to set the rate and unit after traffic policing is enabled for a queue.

**Rate, Unit**

Range: 100~3276700kbps/ 1~3276Mbps

Default: 500kbps

Function: Limit the rate of packets received by a queue of a port. Packets with the rate exceeding the value are discarded.

13. Configure port queue scheduling mode, as shown in Figure 84 and Figure 85.

**QoS Egress Port Schedulers**

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	6 Queues Weighted	13%	25%	25%	13%	13%	13%
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

Figure 84 View Port Queue Scheduling Mode

Click <Port> to enter the “port queue scheduling mode” configuration page.

**QoS Egress Port Scheduler and Shapers Port 6**

Scheduler Mode 6 Queues Weighted

Queue	Queue Shaper				Queue Scheduler	
	Enable	Rate	Unit	Excess	Weight	Percent
Q7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	--	--
Q6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	--	--
Q5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%
Q4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%
Q3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%
Q2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	40	25%
Q1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	40	25%
Q0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%

Figure 85 Configure Port Queue Scheduling Mode

**Scheduler Mode**

Options: Strict Priority/6 Queues Weighted

Default: Strict Priority

Function: Configure the egress-queue mode of the selected port.

**Queue Weight**

Range: 1~100

Default: 17

Function: Configure weight values of the queue.

You can select a port to configure the queue scheduling mode in the upper right corner of the page.

14. Configure egress port shapers, as shown in Figure 86.

Port Shaper			
Enable	Rate	Unit	Excess
<input checked="" type="checkbox"/>	4	Mbps	--

Figure 86 Configure Egress Port Shapers

**Enable**

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable egress port shapers. Traffic shaping of a port is implemented by port rate limit.

**Rate, Unit**

Range: 100~3281943kbps/ 1~3281Mbps

Default: 500kbps

Function: Limit the rate of packets transmitted by a port. Packets with the rate exceeding the value are discarded.

Click <Back> to close the current configuration page and return to the previous configuration page.

You can select a port to configure traffic shaping in the upper right corner of the page.

15. Configure the queue shapers, as shown in Figure 87.



Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	--	--
Q6	<input checked="" type="checkbox"/>	4	Mbps	<input type="checkbox"/>	--	--
Q5	<input checked="" type="checkbox"/>	8	Mbps	<input checked="" type="checkbox"/>	20	13%
Q4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%
Q3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%
Q2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	40	25%
Q1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	40	25%
Q0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	20	13%

Figure 87 Configure the Queue Shapers

**Enable**

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the queue shapers.

**Rate, Unit**

Range: 100~3281943kbps/ 1~3281Mbps

Default: 500kbps

Function: Limit the rate of packets transmitted by a queue of a port. Packets with the rate exceeding the value are discarded.

Click <Back> to close the current configuration page and return to the previous configuration page.

You can select a port to configure traffic shaping in the upper right corner of the page.

16. Configure port storm control, as shown in Figure 88.

**Global Storm Policer Configuration**

Frame Type	Enable	Rate	Unit
Unicast	<input checked="" type="checkbox"/>	1	kfps
Multicast	<input type="checkbox"/>	1	fps
Broadcast	<input type="checkbox"/>	1	fps

Submit    Reset

Figure 88 Configure Port Storm Control

Port storm control is to limit the port-received broadcast/unknown multicast/unknown unicast

packets. When the rate of broadcast/unknown multicast/unknown unicast packets received on the port exceeds the configured threshold, the system will discard excess broadcast/unknown multicast/unknown unicast packets to keep the broadcast/unknown multicast/unknown unicast traffic within the allowable range, ensuring normal network operation.

**Enable**

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable port storm control.

**Rate, Unit**

Range: 1~1024000fps/ 1~1024kfps

Default: 1fps

Function: Configure the threshold for port rate limiting and the packets that exceed the threshold will be dropped.

17. View queue counters, as shown in Figure 89.

**Queuing Counters**

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	1328270	897	0	0	0	0	0	0	0	0	0	0	0	0	0	6852
2	236399	1092247	0	0	0	0	0	0	0	0	0	0	0	0	0	693
3	284	222112	0	0	0	0	0	0	0	0	0	0	0	0	0	13096
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 89 View Queue Counters

Display the number of packets that each queue sends/receives.

Click <port> to enter the “detailed port statistics” page, as shown in Figure 61.

**8.4 Typical Configuration Example**

As shown in Figure 90, port1~port5 forward packet to port 6. Among them,

The packets received by port1 are Untag, and the packets entering port 1 are mapped to

queue 2.

The PCP value of port 2 received packet is 0, DEI value is 1, and the packets entering port 2 are mapped to queue 3.

The DSCP value of port 3 received packet is 4, and the packets entering port 3 are mapped to queue 6.

Port 4 maps all received packets with the source MAC address of 00-00-00-00-00-23 to queue 5 and changes the DSCP value in these packets to 9 for forwarding.

The DSCP value of port 5 received packet is 5, and the packets entering port 5 are mapped to queue 2.

Port6 adopts SP+WRR scheduling mode.

#### **Switch Configuration process:**

1. Set the CoS value of port 1 to 2, as shown in Figure 62.
2. Enable Tag Class of port 2, and map (PCP=0, DEI=1) to CoS=3, as shown in Figure 63.
3. Enable DSCP-Based port 3 and port 5, as shown in Figure 68.
4. Trust DSCP value 4 and 5, and map DSCP value 4 to queue 6 and DSCP value 5 to queue 2, as shown in Figure 70.
5. Configure a QCL entry of port 4, as shown in Figure 74.
6. Configure the QCL entry parameters: set Source MAC to 00-00-00-00-00-23, and frame type to IPv4, as shown in Figure 75.
7. Configure the QCL entry action parameters: set CoS value to 5 and DSCP value to 9, as shown in Figure 80.
8. Configure port 6 queue scheduling mode to 6 Queues Weighted, queue weight of Q0~Q5 to 20, 40, 40, 20, 20, 20, as shown in Figure 85.

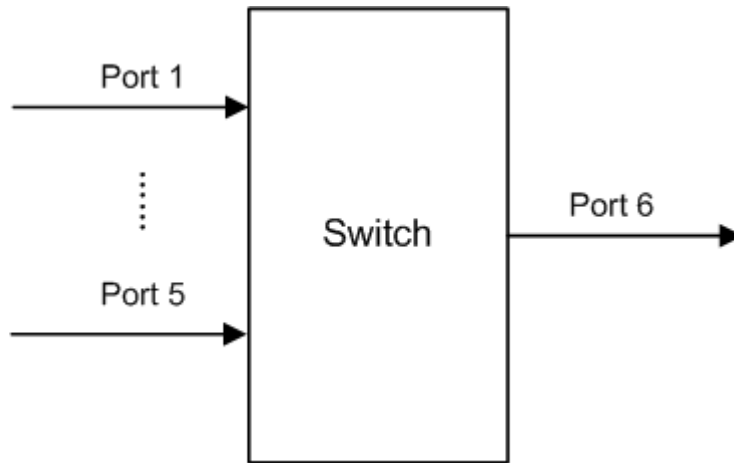


Figure 90 QoS Configuration Example

Port1 and port5 packets enter queue 2, port2 packets enter queue 3, port3 packets enter queue 6, port4 packets enter queue 5.

Queue 6 and queue 7 use the strict priority scheduling mode, and queue 0 to queue 5 use the WRR scheduling mode. Data in queue 6 is processed first when queue 6 is empty, data in queues 0 through 5 is scheduled by weight ratio.

The queue weight are 20, 40, 40, 20, 20, 20. So the bandwidth proportion allocated to the packets in ingress queue 2 is  $40 / (20+40+40+20+20+20) = 25\%$ , that allocated to the packets in ingress queue 3 is  $20 / (20+40+40+20+20+20) = 13\%$ , and that allocated to the packets in ingress queue 5 is  $20 / (20+40+40+20+20+20) = 13\%$ . Among them, port 1 and port 5 packets both go into queue 2, so they are forwarded according to the rule of First In, First out (FIFO), but the total bandwidth proportion of port 1 and port 5 must be 25%.

## 9 Security

### 9.1 User Management

#### 9.1.1 Introduction

To avoid security problems caused by illegitimate users, the series switches provide hierarchical user management. The switch provides different operation rights based on user levels, satisfying diversified access control requirements. Three user levels are available, as shown in Table 5.

Table 5 User Level

User Level	Privilege Level	Description
Guest	5~9	The lowest level, guest users can only view switch configuration.
System	10~14	Medium level, system users have certain access and configuration rights.  System users cannot access the following functions: user management, software update, reboot, load default, and file transmission.
Admin	15	Highest level, admin users have the rights to perform all functions.

#### 9.1.2 Web Configuration

1. Create new users, as shown in Figure 91.

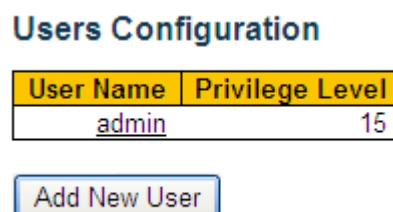


Figure 91 Create New Users

Click <Add New User> to configure different level user, the switch supports a maximum of 20 users.

2. Configure different levels of users, as shown in Figure 92.

Add User

User Settings	
User Name	aaa
Password	•••
Password (again)	•••
Privilege Level	10

Figure 92 Configure Different Level of User

**User Name**

Range: 1~31 characters

Function: Configure the user name.

**Password**

Range: 0~31 characters

Function: Configure the password to be used when the current user accesses the switch.

**Password (again)**

Range: 0~31 characters

Function: Confirm the access password.

**Privilege Level**

Range: 0~15

Function: Configure user level, users of different levels have different operation rights.

3. View the users list, as shown in Figure 93.

Users Configuration

User Name	Privilege Level
<a href="#">333</a>	3
<a href="#">555</a>	5
<a href="#">888</a>	8
<a href="#">aaa</a>	10
<a href="#">ddd</a>	13
<a href="#">admin</a>	15

Figure 93 Users List

Click <User Name> to modify current user configuration.

4. Edit the user settings, as shown in Figure 94.

**Edit User**

User Settings	
User Name	aaa
Password	•••
Password (again)	•••
Privilege Level	10 <input type="button" value="v"/>

Figure 94 Modify the User Configuration

You can modify user password and privilege level.

Click <Delete User> to delete current user.



**Note:**

- Default user admin cannot be deleted.
- The privilege level of admin is forced to 15, cannot be modified; but the default password (123) can be modified.

5. Configure groups privilege level, as shown in Figure 95.

### Privilege Level Configuration

Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
ALARM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DT-RING	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LINKCHECK	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10

Submit Reset

Figure 95 Configure groups privilege level

When the user privilege level is same or greater than a group privilege level, the user can access or configure the group. The access or configure right is based on the user privilege level.

## 9.2 Authentication login configuration

Configure access mode to switch, authentication mode and authentication order, as shown in Figure 96.



### Authentication Method Configuration

Client	Method		
console	no	no	no
telnet	tacacs	local	no
ssh	radius	tacacs	local
http	local	no	no

Figure 96 Authentication Login Configuration

#### Client

Options: console/telnet/ssh/http

Function: Select access mode to switch.

#### Method 1/Method 2/Method 3

Options: no/local/tacacs/radius

Default: local

Function: The methods from left to right are method 1, method 2, and method 3. Select the order of authentication. Authentication method 1 is first performed. If the authentication fails, authentication method 2 is conducted. If both authentications method 1 and authentication method 2 fail, authentication method 3 is conducted.

Description: **no** means authentication is disabled and login is not possible. **local** means using username and password set in local to perform authentication. **tacacs** means using the username and password set in TACACS+ server for authentication. **radius** means using the username and password set in RADIUS server for authentication.



**Caution:**

If tacacs/radius is selected for method 1 and method 2, it is recommended to configure method 3 as local. This will enable the management client to login switch via the local user if none of the configured remote authentication servers are alive.

## 9.3 SSH Configuration

### 9.3.1 Introduction

SSH (Secure Shell) is a network protocol for secure remote login. It encrypts all transmitted data to prevent information disclosure. When data is encrypted by SSH, users can only use

command lines to configure switches.

The series of switches support the SSH server function and allow the connection of multiple SSH users that log in to the switch remotely through SSH.

### 9.3.2 Implementation

In order to realize the SSH secure connection in the communication process, the server and the client experience the following five stages:

Version negotiation stage: currently, SSH consists of two versions: SSH1 and SSH2. The two parties negotiate a version to use.

Key and algorithm negotiation stage: SSH supports multiple types of encryption algorithms. The two parties negotiate an algorithm to use.

Authentication state: the SSH client sends an authentication request to the server and the server authenticates the client.

Session request stage: the client sends a session request to the server after passing the authentication.

Session stage: the client and the server start communication after passing the session request.

### 9.3.3 Web Configuration

1. Enable SSH protocol, as shown in Figure 97.

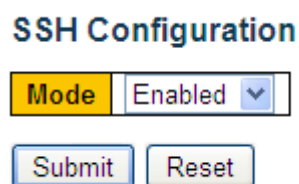


Figure 97 Enable SSH Protocol

#### Mode

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SSH protocol. If it is enabled, the switch works as the SSH server.

### 9.3.4 Typical Configuration Example

The Host works as the SSH client to establish a local connection to switch, as shown in Figure 98.

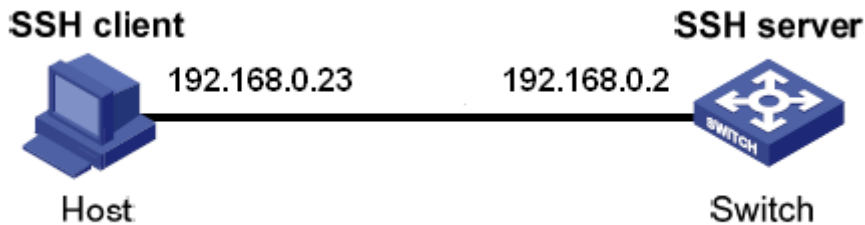


Figure 98 SSH Configuration Example

1. Enable SSH protocol, as shown in Figure 97.
2. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 99; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).

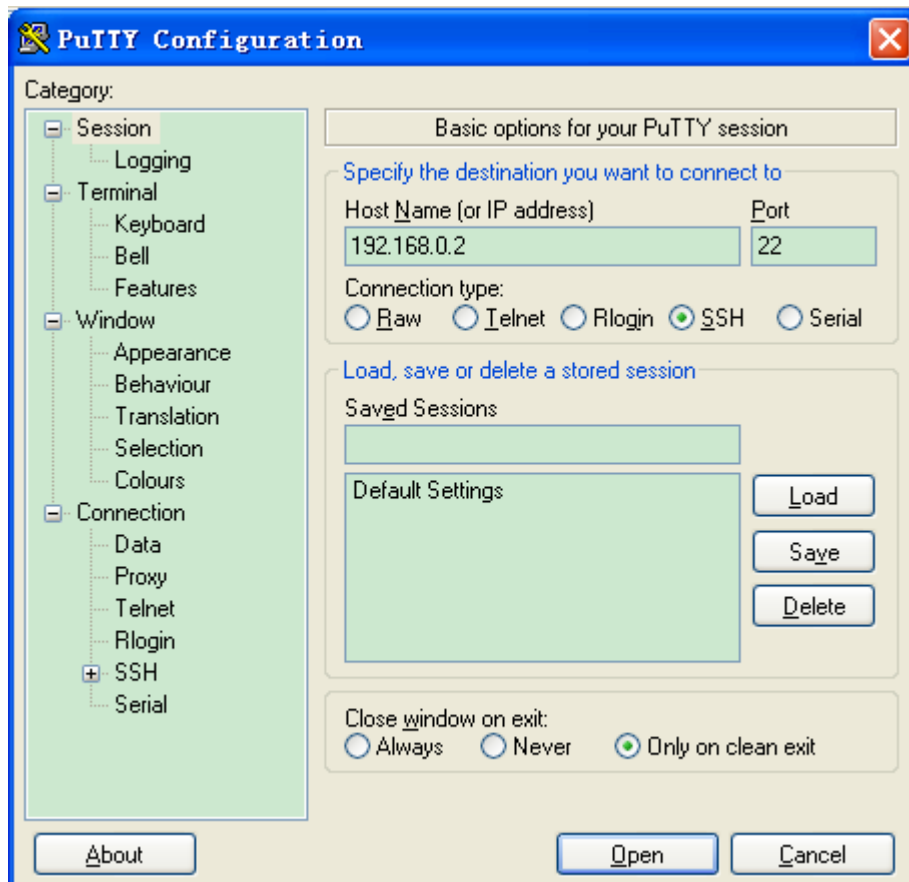


Figure 99 SSH Client Configuration

3. Click <Open> button and following warning message appears shown in Figure 100, click the <是(Y)> button.



Figure 100 Warning Message

4. Input the user name "admin" and the password "123" to enter the switch configuration interface, as shown in Figure 101.



Figure 101 Login Interface of the SSH Authentication

## 9.4 SSL Configuration

### 9.4.1 Introduce

SSL (Secure Socket Layer) is a security protocol and provides the security link for the TCP-based application layer protocol, such as HTTPS. SSL encrypts the network connection at the transport layer and uses the symmetric encryption algorithm to guarantee the data security, and uses the secret key authentication code to ensure the information reliability. This protocol is widely used in Web browser, receiving and sending emails, network fax, real time communication, and so on, providing an encryption protocol for the security transmission in the network.

Once a switch enables SSL, users must use the secure link https, such as https://192.168.0.2, to access the switch.

### 9.4.2 Web Configuration

1. Enable HTTPS protocol, as shown in Figure 102.

**HTTPS Configuration**

Mode	Enabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

Submit    Reset

Figure 102 Enable HTTPS Protocol

#### Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the HTTPS protocol. After enabling HTTPS, users can use http://ip address and the secure link https://ip address to access the switch.

#### Automatic Redirect

Options: Enabled/ Disabled

Default: Disabled

Function: Enabled means users must use the secure link `https://ip address` to access the switch. Disabled means users can use `http://ip address` and the secure link `https://ip address` to access the switch. The parameter “Automatic Redirect” can be configured only if the “Mode” is enabled.

**Certificate Maintain**

Options: None/Delete/Upload/Generate

Default: None

Function: Maintain the HTTPS certificate. The parameter “Certificate Maintain” can be configured only if the “Mode” is disabled. **Delete** is used to delete an existing HTTPS certificate from the switch. **Upload** is used to upload a correct HTTPS certificate to the switch by using the web browser or URL. **Generate** indicates that the switch automatically generates a correct HTTPS certificate.

**Certificate Status**

Options: Switch secure HTTP certificate is presented/Switch secure HTTP certificate is not presented/Switch secure HTTP certificate is generating

Function: Displays the HTTPS certificate status in the switch. **Switch secure HTTP certificate is presented** indicates that a certificate is available in the switch. In this case, you can log in to the Web Page of the switch over HTTPS. **Switch secure HTTP certificate is not presented** indicates that no certificate is available in the switch. In this case, you cannot log in to the Web page over HTTPS. **Switch secure HTTP certificate is generating** indicates that an HTTPS certificates is being generated.

2. Generate HTTPS certificate, as shown in Figure 103.

**HTTPS Configuration**

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Generate
Certificate Algorithm	RSA
Certificate Status	Switch secure HTTP certificate is not presented

Submit    Reset

Figure 103 Generate Certificate

**Certificate Algorithm**

Options: RSA/DSA

Default: RSA

Function: Select the algorithm for generating HTTPS certificate.

3. Upload HTTPS certificate, as shown in Figure 104, Figure 105.

### HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Upload
PassPhrase	●●●
Certificate Upload	Web Browser
File Upload	E:\参考资料\SSL\ssl 秘钥 <input type="button" value="浏览..."/>
Certificate Status	Switch secure HTTP certificate is not presented

Figure 104 Upload Certificate -Web Browser

### HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Upload
PassPhrase	●●●
Certificate Upload	URL
URL	
Certificate Status	Switch secure HTTP certificate is not presented

Figure 105 Upload Certificate -URL

### Pass Phrase

Function: It is used for encrypting the certification.

### Certificate Upload

Options: Web Browser/URL

Default: Web Browser

Function: Select the certificate upload method.

### File Upload

Function: Select the HTTPS certificate file stored in local.

### URL

Function: Configure the storage path of the HTTPS certificate file. The supported protocols are HTTP, HTTPS, TFTP, and FTP, the configuration format is as follows:

[http://10.10.10.10:80/new\\_image\\_path/new\\_image.dat](http://10.10.10.10:80/new_image_path/new_image.dat) or

FTP://username:password@10.10.10.10/new\_image\_path/new\_image.dat.

4. When the HTTPS certificate is presented in switch, input the username and password to successfully log into switch through HTTPS.

## 9.5 Access Management

### 9.5.1 Introduction

Access entries can be configured to manage access to the switch, so as to restrict the hosts that can access the switch as well as the access mode. A maximum of 16 access entries can be configured. A host that matches any of the access entries can successfully access the switch.

### 9.5.2 Web Configuration

1. Configure access management entry, as shown in Figure 106.

Access Management Configuration

Mode

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
<input type="checkbox"/>	1	192.168.0.10	192.168.0.250	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	192.168.1.5	192.168.1.50	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 106 Configure Access Management Entry

#### Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the switch access management. Disable: the access to the switch is not restricted.

#### VLAN ID

Range: 1~4094



Function: Configure the VLAN ID of access management entry.

**Start IP Address/End IP Address**

Function: Configure the IP address range of access management entry.

**HTTP/HTTPS**

Function: When HTTP/HTTPS is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over HTTP/HTTPS.

**SNMP**

Function: When SNMP is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over SNMP.

**TELNET/SSH**

Function: When TELNET/SSH is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over TELNET/SSH.

Click <Add New Entry> to configure the access management entry, the switch supports a maximum of 16 access management entries.

2. View access management statistics, as shown in Figure 107.

**Access Management Statistics**    Auto-refresh     Refresh    Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	513	513	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	46	46	0
SSH	0	0	0

Figure 107 View Access Management Statistics

3. Configure timeouts for switch access modes, as shown in Figure 108.

**Login Timeout**

Service Type	Timeout		
Command Line	10	min	0 sec
WEB	5	min	0 sec

Submit    Reset

Figure 108 Configure Timeouts for Switch Access Modes

**Timeout**

Range: (0~1440) min (0~3600) s

Default: 10 min for Command Line, 5 min for web

Function: Configure the login user timeout and disconnection time. The time starts counting when a user finishes all configurations, and the system will automatically exit the access mode when the time ends. When the time is set to 0, the user timeout and disconnection function is disabled. In this case, the server will not judge whether the user login times out and therefore the user will not exit the current login mode.

## 9.6 SNMP v1/SNMP v2c

### 9.6.1 Introduction

The Simple Network Management Protocol (SNMP) is a framework using TCP/IP to manage network devices. With the SNMP function, the administrator can query device information, modify parameter settings, monitor device status, and discover network faults.

### 9.6.2 Implementation

SNMP adopts the management station/agent mode. Therefore, SNMP involves two types of NEs: NMS and agent.

The Network Management Station (NMS) is a station running SNMP-enabled network management software client. It is the core for the network management of an SNMP network.

Agent is a process in the managed network devices. It receives and processes request packets from the NMS. When an alarm occurs, the agent proactively reports it to the NMS.

The NMS is the manager of an SNMP network, while agent is the managed device of the SNMP network. The NMS and agents exchange management packets through SNMP.

SNMP involves the following basic operations:

Get-Request

Get-Response

Get-Next-Request

Set-Request

Trap

The NMS sends Get-Request, Get-Next-Request, and Set-Request packets to agents to query, configure, and manage variables. After receiving these requests, agents reply with Get-Response packets. When an alarm occurs, an agent proactively reports it to the NMS with a trap packet.

**9.6.3 Explanation**

This series of switches support SNMP v2c. SNMP v2c is compatible with SNMPv1.

SNMP v1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the community name carried by an SNMP packet is not acknowledged by the switch, the request fails and an error message is returned.

SNMP v2c also uses community name for authentication. It is compatible with SNMP v1, and extends the functions of SNMP v1.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP version can be configured on an agent, so that it can use different versions to communicate with different NMSs.

**9.6.4 MIB Introduction**

Any managed resource is called managed object. The Management Information Base (MIB) stores managed objects. It defines the hierarchical relationships of managed objects and attributes of objects, such as names, access permissions, and data types. Each agent has its own MIB. The NMS can read/write MIBs based on permissions. Figure 109 shows the relationships among the NMS, agent, and MIB.

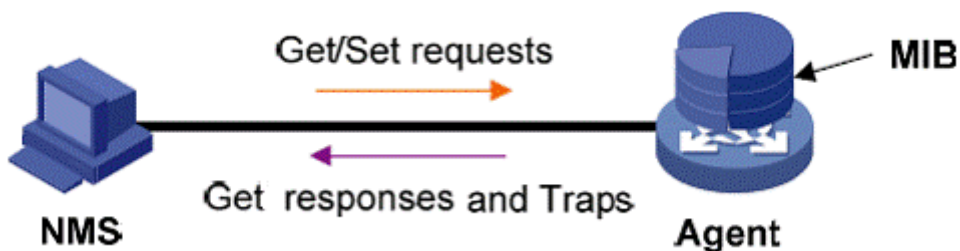


Figure 109 Relationship among NMS, Agent, and MIB

MIB defines a tree structure. The tree nodes are managed objects. Each node has a unique

Object Identifier (OID), which indicates the location of the node in the MIB structure. As shown in Figure 110, the OID of object A is 1.2.1.1.

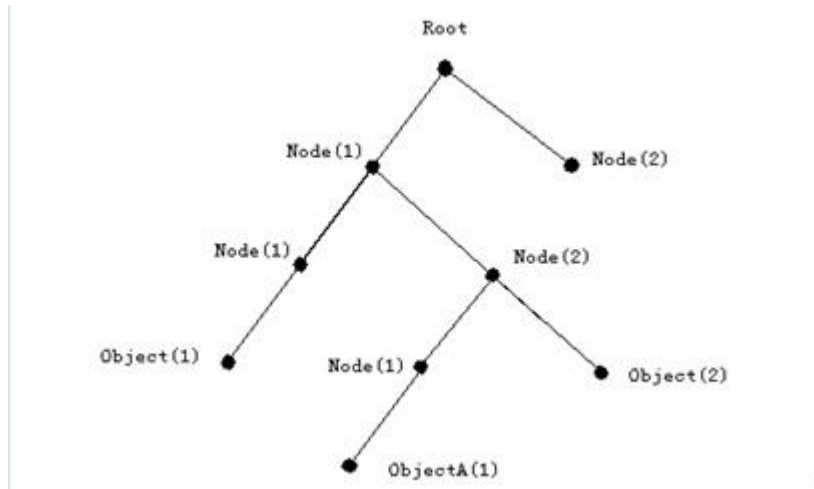


Figure 110 MIB Structure

### 9.6.5 Web Configuration

1. Enable SNMP protocol and select SNMP version, as shown in Figure 111.

#### SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Figure 111 Enable SNMP Protocol and Select SNMP Version

#### Mode

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SNMP.

#### Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Choose a SNMP version. SNMP v2c is compatible with SNMP v1; ; SNMP v3 is

compatible with SNMP v1 and SNMP v2c.

**Read-only Community**

Range: 0~255 characters

Default: public

Function: Configure the name of read-only community.

Description: The MIB information of the switch can be read only if the community name carried by an SNMP packet is identical with that configured on the switch.

**Read&write Community**

Range: 0~255 characters

Default: private

Function: Configure the name of read-write community.

Description: The MIB information of the switch can be read and written only if the community name carried by an SNMP packet is identical with that configured on the switch.

2. Configure global trap mode, as shown in Figure 112.

**Trap Configuration**

**Global Settings**

Mode

**Trap Destination Configurations**

Delete	Name	Enable	Version	Destination Address	Destination Port
<input type="checkbox"/>	111	Enabled	SNMPv2c	192.168.0.23	162

Figure 112 Configure Global Trap Mode

**Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable global trap mode.

Click <Add New Entry> to configure trap entry, the switch supports a maximum of 4 trap entries. Click <Name> to modify the trap entry.

3. Configure trap entry, as shown in Figure 113.

### SNMP Trap Configuration

Trap Config Name	111
Trap Mode	Enabled
Trap Version	SNMP v2c
Trap Community	Public
Trap Destination Address	192.168.0.23
Trap Destination Port	162
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

### SNMP Trap Event

System	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> Warm Start <input checked="" type="checkbox"/> Cold Start
Interface	Link up <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches <input checked="" type="checkbox"/> * Link down <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches LLDP <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches
Authentication	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> SNMP Authentication Fail
Switch	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> STP <input checked="" type="checkbox"/> RMON

Figure 113 Configure Trap Entry

#### Trap Config Name

Range: 1~255 characters

Function: Configure trap entry name.

#### Trap Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable the trap entry. After enabling the trap mode, switch can send trap message to NMS.

#### Trap Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Set the version of trap packets sent from the switch to the server.

### **Trap Community**

Range: 0~255 characters

Default: public

Function: Configure the community carried by trap message.

### **Trap Destination Address**

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages.

### **Trap Destination Port**

Range: 1~65535

Default: 162

Function: Configure the number of port for sending trap messages.

### **Trap Inform Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Whether to send a response to the switch after the server receives a trap packet.

### **Trap Inform Timeout**

Range: 0~2147s

Default: 3s

Function: Set the timeout time for sending trap packets. After sending a trap packet to the server, the switch retransmits the trap packet if it does not receive a response from the server within this period.

### **Trap Inform Retry Times**

Range: 0~255

Default: 5

Function: Set the number of timeout retransmission times of trap packets. If the accumulated number of transmission times exceeds the value of this parameter and the server does not respond yet, it is considered that transmitting the trap packet fails.

### **Warm Start/ Cold Start**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when switch warm starting/cold starting.

### **Link up/ Link down**

Options: none/specific/all switches

Default: none

Function: Whether to send a port up/down trap packet when the port status changes.

### **LLDP**

Options: none/specific/all switches

Default: none

Function: Whether to send a Link Layer Discovery Protocol (LLDP) trap packet when the neighbor status changes.

### **SNMP Authentication Fail**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when SNMP Authentication Failure.

### **STP**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when STP status changing.

## **9.6.6 Typical Configuration Example**

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. The NMS monitors and manages the Agent through SNMP v2c, and reads and writes the MIB node information of the Agent. When the Agent is faulty, it proactively sends trap packets to the NMS, as shown in Figure 114.



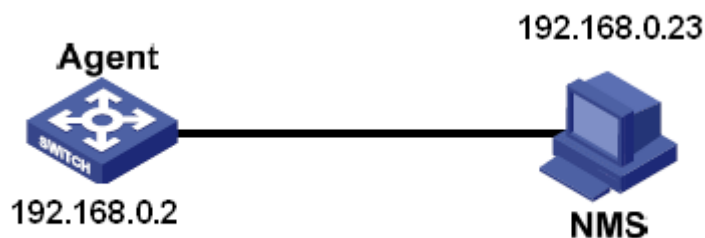


Figure 114 SNMP v2c Configuration Example

### Configuration on Agent:

1. Enable SNMP and v2c state; configure access rights with Read only community "public" and Read and write community "private", as shown in Figure 111.
2. Configure global trap mode, as shown in Figure 112.
3. Create trap entry 111, enable trap mode; set the trap version to SNMP v2c, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters, as shown in Figure 113.

If you want to monitor and manage Agent devices, run the corresponding management software in NMS, such as Kyvision developed by Kyland.

For details about operations of Kyvision, refer to the *Kyvision Operation Manual*.

## 9.7 SNMPv3

### 9.7.1 Introduce

SNMP v3 provides a User-Based Security Model (USM) authentication mechanism. You can configure authentication and encryption functions. Authentication is used for verifying the validity of packet sender, preventing illegitimate users' access. Encryption is used for encrypt packets transmitted between the NMS and the Agent, avoiding interception. The authentication and encryption functions can improve the security of communication between the SNMP NMS and the SNMP Agent.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP version can be configured on an agent, so that it can use different versions to communicate with different NMSs.

### 9.7.2 Implementation

SNMP v3 provides four configuration tables. Each table can contain 16 entries. These tables determine whether specific users can access MIB information.

You can create multiple users in the user table. Each user uses different security policies for authentication and encryption.

The group table is the collection of multiple users. In the group table, access rights are defined based on user groups. All the users of a group have the rights of the group.

The view table refers to the MIB view information, which specifies the MIB information that can be accessed by users. The MIB view may contain all nodes of a certain MIB subtree (that is, users are allowed to access all nodes of the MIB subtree) or contain none of the nodes of a certain MIB subtree (that is, users are not allowed to access any node of the MIB subtree).

You can define MIB access rights in the access table by group name, security model, and security level.

### 9.7.3 Web Configuration

1. Enable SNMP protocol and select SNMP version, as shown in Figure 115.

**SNMP System Configuration**

<b>Mode</b>	Enabled <input type="button" value="v"/>
<b>Version</b>	SNMP v3 <input type="button" value="v"/>
<b>Read Community</b>	public
<b>Write Community</b>	private
<b>Engine ID</b>	800007e5017f000001

Figure 115 Enable SNMP Protocol and Select SNMP Version

**Mode**

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SNMP.

**Version**

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Choose a SNMP version. SNMP v2c is compatible with SNMP v1; ; SNMP v3 is compatible with SNMP v1 and SNMP v2c.

**Engine ID**

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Set the engine ID for the SNMP v3 system. When the engine ID is changed, users corresponding to device IDs in the user table are cleared.

2. Configure global trap mode, as shown in Figure 116.

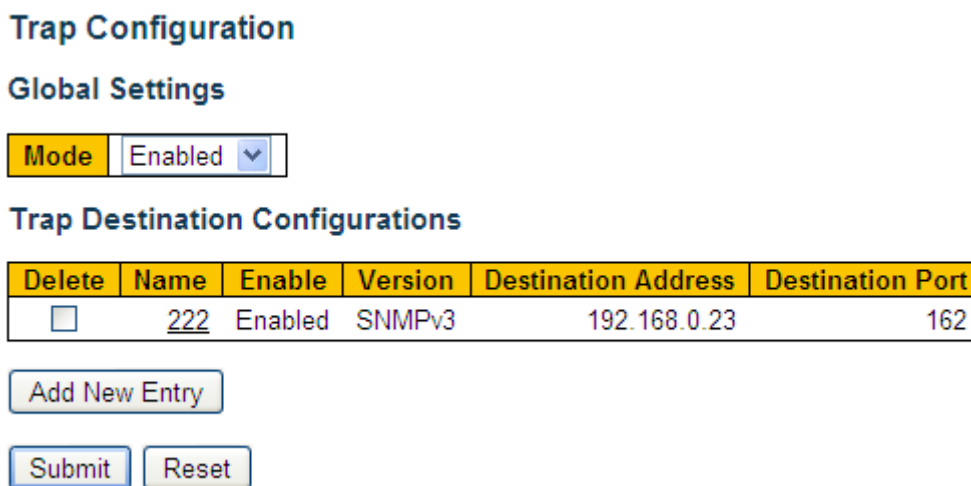


Figure 116 Configure Global Trap Mode

**Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable global trap mode.

Click <Add New Entry> to configure trap entry, the switch supports a maximum of 4 trap entries. Click <Name> to modify the trap entry.

3. Configure trap entry, as shown in Figure 117.

### SNMP Trap Configuration

Trap Config Name	222
Trap Mode	Enabled <input type="button" value="v"/>
Trap Version	SNMP v3 <input type="button" value="v"/>
Trap Community	Public
Trap Destination Address	192.168.0.23
Trap Destination Port	162
Trap Inform Mode	Enabled <input type="button" value="v"/>
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled <input type="button" value="v"/>
Trap Security Engine ID	Probe Fail
Trap Security Name	None <input type="button" value="v"/>

### SNMP Trap Event

System	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> Warm Start <input checked="" type="checkbox"/> Cold Start
Interface	Link up <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches <input checked="" type="checkbox"/> * Link down <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches LLDP <input type="radio"/> none <input type="radio"/> specific <input checked="" type="radio"/> all switches
Authentication	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> SNMP Authentication Fail
Switch	<input checked="" type="checkbox"/> * <input checked="" type="checkbox"/> STP <input checked="" type="checkbox"/> RMON

Figure 117 Configure Trap Entry

#### Trap Config Name

Range: 1~255 characters

Function: Configure trap entry name.

#### Trap Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable the trap entry. After enabling the trap mode, switch can send trap message to NMS.

#### Trap Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Set the version of trap packets sent from the switch to the server.

### **Trap Community**

Range: 0~255 characters

Default: public

Function: Configure the community carried by trap message.

### **Trap Destination Address**

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages.

### **Trap Destination Port**

Range: 1~65535

Default: 162

Function: Configure the number of port for sending trap messages.

### **Trap Inform Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Set whether to send a response to the switch after the server receives a trap packet.

### **Trap Inform Timeout**

Range: 0~2147s

Default: 3s

Function: Set the timeout time for sending trap packets. After sending a trap packet to the server, the switch retransmits the trap packet if it does not receive a response from the server within this period.

### **Trap Inform Retry Times**

Range: 0~255

Default: 5

Function: Set the number of timeout retransmission times of trap packets. If the accumulated number of transmission times exceeds the value of this parameter and the server does not respond yet, it is considered that transmitting the trap packet fails.

### **Trap Probe Security Engine ID**

Options: Enabled/Disabled

Default: Enabled

Function: Set the security engine ID carried in SNMP v3 trap packets. When it is set to Enabled, the switch automatically probes and acquires the security engine ID. When it is set to Disabled, the security engine ID is acquired from the value of Trap Security Engine ID.

### **Trap Security Engine ID**

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Configure the Trap Security Engine ID carried by trap message.

### **Warm Start/ Cold Start**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when switch warm starting/cold starting.

### **Link up/ Link down**

Options: none/specific/all switches

Default: none

Function: Whether to send a port up/down trap packet when the port status changes.

### **LLDP**

Options: none/specific/all switches

Default: none

Function: Whether to send an LLDP trap packet when the neighbor status changes.

### **SNMP Authentication Fail**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when SNMP Authentication Failure.

### **STP**

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when STP status changing.

4. Configure community, as shown in Figure 118.

### SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Figure 118 Configure Community

#### Community

Range: 1~32 characters

Function: Configure the community name at switch-side.

When SNMP v3 is selected, a community name can be set to enable the network management system (NMS) to access the switch over SNMPv1 and SNMPv2. In this case, the community name on the NMS must be consistent with that on the switch. The access permissions of a community name depend on the configuration of the group table and access table.

#### Source IP

Format: A.B.C.D

Function: Configure the NMS IP address.

#### Source Mask

Function: Network indicates that you can configure the range of the IP address pool, and the address range is determined by the subnet mask. The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. The NMS IP address is determined by Source IP and Source Mask.

Click <Add New Entry> to configure community, the switch supports a maximum of 16 communities.



Note:

By default, the community names public and private exist on the switch. There is no IP address restriction on the NMS.

4. Configure the user table, as shown in Figure 119.

**SNMPv3 User Configuration**

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
<input type="checkbox"/>	800007e5017f000001	1111	Auth, Priv	MD5	••••••••	DES	••••••••
<input type="checkbox"/>	800007e5017f000001	2222	Auth, Priv	SHA	••••••••	AES	••••••••

Figure 119 SNMP v3 User Table Configuration

**Engine ID**

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Set the user engine ID. If the user engine ID is different from the SNMPv3 system engine ID, the user is ineffective currently.

**User Name**

Range: 1~32 characters

Function: Create the user name.

**Security Level**

Options: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Function: Configure the security level of current user.

Description: NoAuth,NoPriv indicates that neither authentication nor encryption is required. Auth,NoPriv indicates that authentication is required but not encryption. Auth,Priv indicates that both authentication and encryption are required.

**Authentication Protocol**

Options: MD5/SHA

Function: Select an authentication algorithm. The authentication protocol and authentication password need to be set when Security Level is set to Auth, NoPriv or NoAuth, Priv.

**Authentication Password**

Range: 8~32 characters (MD5) 8~40 characters (SHA)

Function: Create the authentication password.

**Privacy Protocol**

Options: DES/AES



Function: Select a encryption protocol. The privacy protocol and privacy password need to be set when Security Level is set to Auth, Priv.

**Privacy Password**

Range: 8~32 characters

Function: Create the encryption password.

Click <Add New Entry> to configure user entry. A maximum of 16 users are supported.



Note:

By default, the user default\_user exists in the switch and the security level is NoAuth, NoPriv.

5. Configure the group table, as shown in Figure 120.

**SNMPv3 Group Configuration**

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group
<input type="checkbox"/>	usm	1111	group
<input type="checkbox"/>	usm	2222	group

Figure 120 SNMP v3 Group Table Configuration

**Security Model**

Default: v1/v2/usm

Description: Select the security model of current group(SNMP version). SNMP v3 adopts User-based Security Model (USM) .

**Security Name**

Range: all existing communities/user names, 1~32 characters

Function: Configure the security name. When the security model is v1/v2, the security name must be identical with community. When the security model is usm, the security name must be identical with the user name in the user table.

**Group Name**

Range: 1~32 characters

Function: Configure the name of the group table, users with same group name belong to one group.

Click <Add New Entry> to configure group table. A maximum of 16 groups are supported.



**Note:**

By default, the following group tables exist in the switch: {v1,public,default\_ro\_group}, {v1,private,default\_rw\_group}, {v2c,public,default\_ro\_group}, {v2c,private,default\_rw\_group}, and {usm,default\_user,default\_rw\_group}.

6. Configure the view table, as shown in Figure 121.

**SNMPv3 View Configuration**

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1
<input type="checkbox"/>	view1	included	.1.3.6.1.2.1.1.1

Figure 121 SNMP v3 View Table Configuration

**View Name**

Range: 1~32 characters

Function: Configure the view name.

**View Type**

Options: included/excluded

Default: included

Function: Included indicates that the current view includes all nodes of the MIB tree.

Excluded indicates that the current view does not include any nodes of the MIB tree.

**OID Subtree**

Function: MIB tree, indicated by the OID of the root node of the tree.

Click <Add New Entry> to configure view table. A maximum of 16 view entries are supported.



**Note:**

By default, the view default\_view exists in the switch and this view covers all nodes in subtree

1.

7. Configure the access table, as shown in Figure 122.

**SNMPv3 Access Configuration**

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼
<input type="checkbox"/>	group	usm	Auth, NoPriv	default_view ▼	None ▼

Figure 122 SNMP v3 Access Table Configuration

**Group Name**

Range: all existing group names, 1~32 characters

Function: Users in the group have the same access rights.

**Security Model**

Default: any/v1/v2/usm

Function: Set the security model (that is, SNMP version number) adopted when the current group accesses the switch. SNMPv3 adopts User-based Security Model (USM) and the value **any** indicates that any security model can be adopted. The group name and Security Model in access table should be identical with those in group table.

**Security Level**

Options: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Function: Select the security level of current group.

Description: NoAuth,NoPriv indicates that neither authentication nor encryption is required. Auth,NoPriv indicates that authentication is required but not encryption. Auth,Priv indicates that both authentication and encryption are required. When authentication/encryption is required, the user can access specified MIB information only if the authentication/encryption protocol and authentication/encryption password are identical with those configured in the user table.

The security levels are NoAuth,NoPriv, Auth,NoPriv and Auth,Priv in ascending order. The content with a lower security level is allowed to be accessed with a higher security level. For

example, if both authentication/encryption protocol and authentication/encryption password are correct, security level is configured as Auth,NoPriv can be successfully accessed with the Auth,NoPriv and Auth,Priv security level but cannot be accessed with the NoAuth,NoPriv security level.

**Read View Name**

Options: default\_view/None/all existing view names

Function: Select the name of read-only view.

**Write View Name**

Options: default\_view/None/all existing view names

Function: Select the name of write view.

Click <Add New Entry> to configure access table. A maximum of 16 access entries are supported.



**Note:**

By default, the following access tables exist in the switch: {default\_ro\_group, any, NoAuth,NoPriv, default\_view, None} and {default\_rw\_group, any, NoAuth,NoPriv, default\_view, default\_view}.

**9.7.4 Typical Configuration Example**

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. User 1111 and user 2222 manage the Agent through SNMP v3. Security level is set to AuthNoPriv, and the switch can perform read-only operation on all node information of the Agent. When an alarm occurs, the Agent sends trap v3 messages to the NMS proactively, as shown in Figure 123.

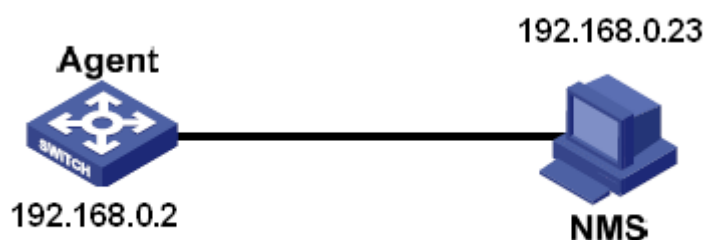


Figure 123 SNMP v3 Configuration Example

Configuration on the Agent:

1. Enable SNMP and v3 state, as shown in Figure 115.

2. Configure the SNMP v3 user table

Set a username to 1111, security level to Auth,Priv, authentication protocol to MD5, authentication password to aaaaaaaa, privacy protocol to DES, and privacy password to xxxxxxxx.

Set another username to 2222, security level to Auth,Priv, authentication protocol to SHA, authentication password to bbbbbbbb, privacy protocol to AES, and privacy password to yyyyyyyy, as shown in Figure 119.

3. Create group, set security model to usm, and add user 1111 and user 2222 to the group, as shown in Figure 120.

4. Configure the SNMP v3 access table

Set the group name to group, security model to usm, security level to Auth,NoPriv, read view to default\_view, and write view to None, as shown in Figure 122.

5. Enable the global trap mode, as shown in Figure 116.

6. Create trap entry 222, enable trap mode; set the trap version to SNMP v3, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters, as shown in Figure 117.

If you want to monitor and manage Agent devices, run the corresponding management software in NMS.

## 9.8 RMON

### 9.8.1 Introduce

Based on SNMP architecture, Remote Network Monitoring (RMON) allows network management devices to proactively monitor and manage the managed devices. An RMON network usually involves the Network Management Station and Agents. The NMS manages Agents and Agents can collect statistics on various types of traffic on these ports.

RMON mainly provides statistics and alarm functions. With the statistics function, Agents

can periodically collect statistics on various types of traffic on these ports, such as the number of packets received from a certain network segment during a certain period. Alarm function is that Agents can monitor the values of specified MIB variables. When a value reaches the alarm threshold (such as the number of packets reaches the specified value), Agent can automatically record alarm events in RMON log, or send a Trap message to the management device.

### 9.8.2 RMON Groups

RMON (RFC2819) defines multiple RMON groups. The series devices support statistics group, history group, event group, and alarm group in public MIB.

#### ➤ Statistics group

With the statistics group, the system collects statistics on all types of traffic on ports and stores the statistics in the Ethernet statistics table for further query by the management device. The statistics includes the number of network collisions, CRC error packets, undersized or oversized packets, broadcast and multicast packets, received bytes, and received packets. After creating a statistics entry on a specified port successfully, the statistics group counts the number of packets on the port and the statistics is a continuously accumulated value.

#### ➤ History group

History group requires the system to periodically sample all kinds of traffic on ports and saves the sampling values in the history record table for further query by the management device. The history group counts the statistics values of all kinds of data in the sampling interval.

#### ➤ Event group

Event group is used to define event indexes and event handing methods. Events defined in the event group is used in the configuration item of alarm group. An event is triggered when the monitored device meets the alarm condition. Events are addressed in the following ways:

Log: logs the events and related information in the event log table.

Trap: sends a Trap message to the NMS and inform the NMS of the event.

Log-Trap: logs the event and sends a Trap message to the NMS.

None: indicates no action.

➤ Alarm group

RMON alarm management can monitor the specified alarm variables. After alarm entries are defined, the system will acquire the values of monitored alarm variables in the defined period. When the value of an alarm variable is larger than or equal to the upper limit, a rising alarm event is triggered. When the value of an alarm variable is smaller than or equal to the lower limit, a falling alarm event is triggered. Alarms will be handled according to the event definition.



**Caution:**

If a sampled value of alarm variable exceeds the threshold multiple times in a same direction, then the alarm event is only triggered only the first time. Therefore the rising alarm and falling alarm are generated alternately.

**9.8.3 Web Configuration**

1. Configure statistics table, as shown in Figure 124.

**RMON Statistics Configuration**

Delete	ID	Data Source
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. 1000002

Figure 124 Configure RMON Statistics Table

**ID**

Range: 1~65535

Function: Configure the number of the statistics entry. Statistics group supports up to 128 entries.

**Data Source**

Range: 100000portid

Function: Select the port whose statistics are to be collected.

2. View statistics group status, as shown in Figure 125.

RMON Statistics Overview

Start from Control Index  with  entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000002	1024	6445055	29080	23081	965	0	0	0	0	0	0	7393	17565	756	691	181	2494

Figure 125 Overview statistics group status

Drop: the number of packets dropped by the port.

Octets: the number of bytes received by the port.

Pkts: the number of packets received by the port.

Broadcast: the number of broadcast packets received by the port.

Multicast: the number of multicast packets received by the port.

CRC Errors: the number of CRC error packets with a length of between 64 and 9600 bytes received by the port.

Undersize: the number of packets with less than 64 bytes received by the port.

Oversize: the number of packets with more than 9600 bytes received by the port.

Frag.: the number of CRC error packets with less than 64 bytes received by the port.

Jabb.: the number of CRC error packets with more than 9600 bytes received by the port.

Coll.: the number of collisions received by the port under half duplex mode.

64 Bytes: the number of packets with a length of 64 bytes received by the port.

65~127: the number of packets with a length of between 65 and 127 bytes received by the port.

128~255: the number of packets with a length of between 128 and 255 bytes received by the port.

256~511: the number of packets with a length of between 256 and 511 bytes received by the port.

512~1023: the number of packets with a length of between 512 and 1023 bytes received by the port.

1024~1588: the number of packets with a length of between 1024 and 1588 bytes received by the port.





**Note:**

The oversize depends on the parameter “Maximum Frame Size” in Port Configuration. Communication is normal when the port is in LinkUP state. In this example, the oversize is 9600 bytes.

3. Configure history table, as shown in Figure 126.

**RMON History Configuration**

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
<input type="checkbox"/>	2	.1.3.6.1.2.1.2.2.1.1.1000002	1800	50	50

Figure 126 Configure History Table

**ID**

Range: 1~65535

Function: Configure the number of the history entry. History group supports up to 256 entries.

**Data Source**

Options: 100000portid

Function: Select the port whose information is to be sampled.

**Interval**

Range: 1~3600s

Default: 1800s

Function: Configure the sampling period of the port.

**Buckets**

Range: 1~65535

Default: 50

Function: Configures the number of latest sampling values of port information stored in RMON.

4. View history group status, as shown in Figure 127.

**RMON History Overview**

Start from Control Index  and Sample Index  with  entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
2	37	21052	0	23497	223	198	25	0	0	0	0	0	0	0
2	38	21062	0	28051	304	293	11	0	0	0	0	0	0	0
2	39	21072	0	17795	200	183	17	0	0	0	0	0	0	0
2	40	21082	0	30628	329	315	14	0	0	0	0	0	0	0
2	41	21092	0	28780	317	298	19	0	0	0	0	0	0	0
2	42	21102	0	24672	272	243	29	0	0	0	0	0	0	0
2	43	21112	0	129168	437	304	13	0	0	0	0	0	0	1
2	44	21122	0	21179	238	224	14	0	0	0	0	0	0	0
2	45	21132	0	39616	398	351	47	0	0	0	0	0	0	0
2	46	21142	0	32798	337	309	23	0	0	0	0	0	0	0

Figure 127 Overview History Group Status

5. Configure event table, as shown in Figure 128.

**RMON Event Configuration**

Delete	ID	Desc	Type	Community	Event Last Time
<input type="checkbox"/>	1	aaa	logandtrap	public	71339
<input type="checkbox"/>	2	bbb	logandtrap	public	71319

Figure 128 Configure Event Table

**ID**

Range: 1~65535

Function: Configure the index number of the event entry. Event group supports up to 128 entries.

**Desc**

Range: 0~127 characters

Function: Describe the event.

**Type**

Options: none/log/snmptrap/logandtrap

Default: none

Function: Configure the event type for alarms, that is, the processing mode towards alarms.

**Community**

Range: 0~127 characters

Default: public

Function: Configure the community name for sending a trap event. The value shall be identical with that in SNMP.

**Last Event**

Function: Displays the value of sysUpTime when the event is used last time.

6. View event group status, as shown in Figure 129.

**RMON Event Overview**

Start from Control Index  and Sample Index  with  entries per page.

Event Index	LogIndex	LogTime	LogDescription
<u>1</u>	1	71179	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=172 >= 50 :1, 1
<u>1</u>	2	71339	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=186 >= 50 :1, 1
<u>2</u>	1	71159	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
<u>2</u>	2	71319	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
<u>2</u>	3	71419	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2

Figure 129 Overview Event Group Status

7. Configure alarm table, as shown in Figure 130.

**RMON Alarm Configuration**

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
<input type="checkbox"/>	1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	186	RisingOrFalling	50	1	20	2

Figure 130 Configure Alarm Table

**ID**

Range: 1~65535

Function: Configure the number of the alarm entry. Alarm group supports up to 256 entries.

**Interval**

Range: 1~2147483647s

Deault: 30s

Function: Configure the sampling period.

**Variable**

Format: A.100000portid

Range: A: 10~21

Function: Select the port MIB information to be monitored.

InOctets: A=10, the number of bytes received by the port.

InUcastPkts: A=11, the number of unicast packets received by the port.

InNUcastPkts: A=12, the number of broadcast and multicast packets received by the port.

InDiscards: A=13, the number of packets dropped by the port.

InErrors: A=14, the number of error packets received by the port.

InUnknownProtos: A=15, the number of unknown packets received by the port.

OutOctets: A=16, the number of bytes sent by the port.

OutUcastPkts: A=17, the number of unicast packets sent by the port.

OutNUcastPkts: A=18, the number of broadcast and multicast packets sent by the port.

OutDiscards: A=19, the number of discarded packets sent by the port.

OutErrors: A=20, the number of error packets sent by the port.

OutQLen: A=21, the length of packets in port outlet queue.

### **Sample Type**

Options: Absolute/Delta

Default: Delta

Function: choose the method of comparing the sampling value and threshold.

Description: Absolute: directly compare each sampling value to threshold; Delta: the sampling value minus the previous sampling value, then use the difference to compare with threshold.

### **Startup Alarm**

Options: Rising/Falling/RisingOrFalling

Default: RisingOrFalling

Function: choose the alarm type.

### **Rising Threshold**

Range: 1~2147483647

Function: Set a rising threshold. When the sampling value exceeds the rising threshold and the alarm type is RisingAlarm or RisOrFallAlarm, the alarm will be triggered and the rising event index will be activated.

### **Rising Index**

Range: 1~65535

Function: Set the index of a rising event. It is the handing method of a rising alarm.

### **Falling Threshold**

Range: 1~2147483647

Function: Set a falling threshold. When the sampling value is lower than the falling threshold and the alarm type is FallingAlarm or RisOrFallAlarm, the alarm will be triggered and the falling event index will be activated.

**Falling Index**

Range: 1~65535

Function: Set the index of a falling event. It is the handling method of a falling alarm.

8. View alarm group status, as shown in Figure 131.

**RMON Alarm Overview**

Start from Control Index  with  entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	195	RisingOrFalling	50	1	20	2

Figure 131 Overview Alarm Group Status

**9.9 TACACS+ Configuration**

**9.9.1 Introduction**

Terminal Access Controller Access Control System (TACACS+) is a TCP-based application. It adopts the client/server mode to implement the communication between Network Access Server (NAS) and TACACS+ server. The client runs on the NAS and user information is managed centrally on the server. The NAS is the server for users but client for the server. Figure 132 shows the structure.

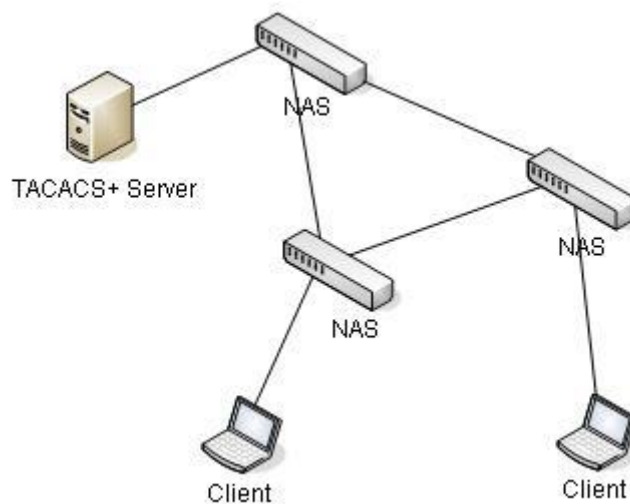


Figure 132 TACACS+ Structure

The protocol authenticates, authorizes, and charges terminal users that need to log in to the device for operations. The device serves as the TACACS+ client, and sends the user name and password to the TACACS+ server for authentication. The server receives TCP connection requests from users, responds to authentication requests, and checks the legitimacy of users. If a user passes authentication, it can log in to the device for operations.

### 9.9.2 Web Configuration

1. Configure global TACACS+ parameters, as shown in Figure 133.

#### TACACS+ Server Configuration

##### Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key	111	

Figure 133 Configure Global TACACS+ Parameter

#### Timeout

Range: 1~1000s

Default: 5s

Function: Set the overtime for response from the TACACS+ server. After sending a TACACS+ request packet, if the device still receives no response from the TACACS+ server after the specified time, authentication fails, and the device will consider the TACACS+ server is invalid.

#### Deadtime

Range: 0~1440min

Default: 0min

Function: Configures the period when the server is invalid. During this period, the device does not send TACACS+ request messages to the server. The value is 0 means disabling the function. You can enable this function only if more than one TACACS+ server has been configured.

#### Key

Range: 0~63 characters

Function: Set the key to improve the communication security between client and TACACS+ server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the TACACS+ server.

2. Configure the TACACS+ server, as shown in Figure 134.

**Server Configuration**

Delete	hostname	Port	Timeout	Key
<input type="checkbox"/>	192.168.0.23	49	5	aaa
<input type="checkbox"/>	192.168.0.32	45	5	

Add New Server

Submit Reset

Figure 134 TACACS+ Server Configuration

**Hostname**

Function: Configure the IP address or hostname of TACACS+ server. A maximum of 5 TACACS+ servers can be configured.

**Port**

Range: 0~65535

Default: 49

Function: Set TCP port of the TACACS+ server for authentication.

**Timeout**

Range: 1~1000s

Function: Set the overtime for response from the TACACS+ server. After sending a TACACS+ request packet, if the device still receives no response from the TACACS+ server after the specified time, authentication fails, and the device will consider the TACACS+ server is invalid.

**Key**

Range: 0~63 characters

Function: Set the key to improve the communication security between client and TACACS+ server. The two parties share the key to verify the legitimacy of packets. Both parties can

receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the TACACS+ server.

**Note:**

The priority of "Timeout" and "Key" in TACACS+ server configuration is higher than those in global configuration.

### 9.9.3 Typical Configuration Example

As shown in Figure 135, TACACS+ server can authenticate and authorize users by the switch. The server IP address is 192.168.0.23, and the shared key used when switch and server exchange packets is aaa.

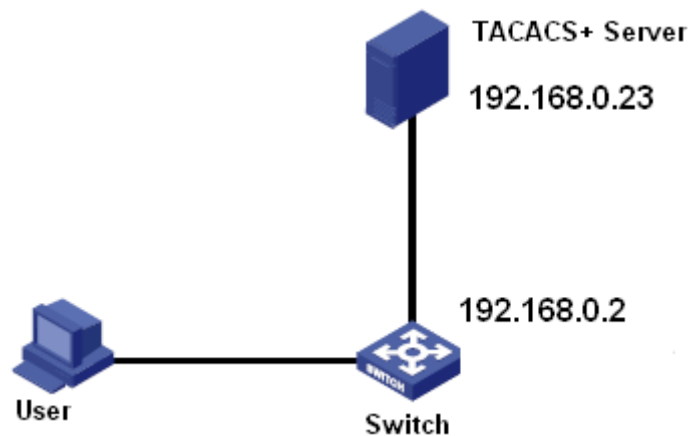


Figure 135 TACACS+ Authentication Example

1. TACACS+ server configuration. Set the server IP address to 192.168.0.23 and key to aaa, as shown in Figure 134.
2. When logging in to the switch through Web, select "Local", while logging in to the switch through telnet, select "Tacacs+", as shown in Figure 96.
3. Configure username and password "bbb", encrypt key "aaa" on TACACS+ server.
4. When logging in to the switch through Web, input the username "admin" and password "123" to pass the local authentication.
5. When logging in to the switch through Telnet, input the username and password "bbb" to pass the TACACS+ authentication.



## 9.10 RADIUS Configuration

### 9.10.1 Introduction

RADIUS (Remote Authentication Dial-In User Service) is a distributed information exchange protocol. It defines UDP-based RADIUS frame format and information transmission mechanism, protecting networks from unauthorized access. RADIUS is usually used in networks that require high security and remote user access.

RADIUS adopts client/server mode to achieve communication between the NAS (Network Access Server) and the RADIUS server. The RADIUS client runs on the NAS. The RADIUS server provides centralized management for user information. The NAS is the server for users but client for the RADIUS server. Figure 136 shows the structure.

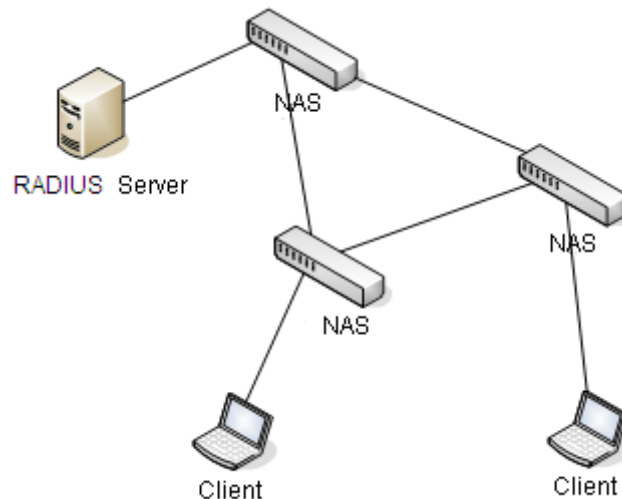


Figure 136 RADIUS Structure

The protocol authenticates terminal users that need to log in to the device for operation. Serving as the RADIUS client, the device sends user information to the RADIUS server for authentication and allows or disallows users to log in to the device according to authentication results.

### 9.10.2 Web Configuration

1. Configure global RADIUS parameters, as shown in Figure 137.

## RADIUS Server Configuration

### Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	111	
NAS-IP-Address	192.168.0.220	
NAS-IPv6-Address		
NAS-Identifier	222	

Figure 137 Configure Global RADIUS Parameters

#### Timeout

Range: 1~1000s

Default: 5s

Function: Set the overtime for response from the RADIUS server. After sending a RADIUS request packet, the device will retransmit a RADIUS request packet if it still receives no response from the RADIUS server after the specified time.

#### Retransmit

Range: 1~1000

Default: 3

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, authentication fails, and the device will consider the RADIUS server is invalid.

#### Deadtime

Range: 0~1440min

Default: 0min

Function: Configures the period when the server is invalid. During this period, the device does not send RADIUS request messages to the server. The value is 0 means disabling the function. You can enable this function only if more than one RADIUS server has been configured.

#### Key

Range: 0~63 characters

Function: Set the key to improve the communication security between client and RADIUS server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the RADIUS server.

**NAS-IP-Address**

Function: Configures the source address used for sending RADIUS request messages by the equipment. If no source address is specified, the interface address for sending messages will be regarded as the source address.

**NAS-Identifier**

Range: 0~253 characters

Function: Configures the identifier used for sending RADIUS request messages by the equipment.

2. Configure the RADIUS server, as shown in Figure 138.

**Server Configuration**

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="checkbox"/>	192.168.0.23	1812	1813	5	3	aaa
<input type="checkbox"/>	192.168.0.184	1812	1813	5	3	bbb

Figure 138 Configure the RADIUS Server

**Hostname**

Function: Configure the IP address or hostname of RADIUS server. A maximum of 5 RADIUS server can be configured.

**Auth Port**

Range: 0~65535

Default: 1812

Function: Set UDP port of the RADIUS server for authentication.

**Acct Port**

Range: 0~65535

Default: 1813

Function: Set UDP port of the RADIUS server for accounting. Since RADIUS uses different UDP ports for receiving and sending authentication and accounting messages, different port numbers must be configured for authentication and accounting.

**Timeout**

Range: 1~1000s

Function: Set the overtime for response from the RADIUS server. After sending a RADIUS request packet, the device will retransmit a RADIUS request packet if it still receives no response from the RADIUS server after the specified time.

**Retransmit**

Range: 1~1000

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, authentication fails, and the device will consider the RADIUS server is invalid.

**Key**

Range: 0~63 characters

Function: Set the key to improve the communication security between client and RADIUS server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the RADIUS server.



**Note:**

The priority of “Timeout”, “Retransmit”, and “Key” in RADIUS server configuration is higher than those in global configuration.

3. View RADIUS server status, as shown in Figure 139.

**RADIUS Server Status Overview**

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.0.23	1812	Ready	1813	Ready
2	192.168.0.184	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Figure 139 View RADIUS Server Status

Click the number to enter the “detailed RADIUS server statistics” page.

4. View detailed RADIUS server statistics, as shown in Figure 140.

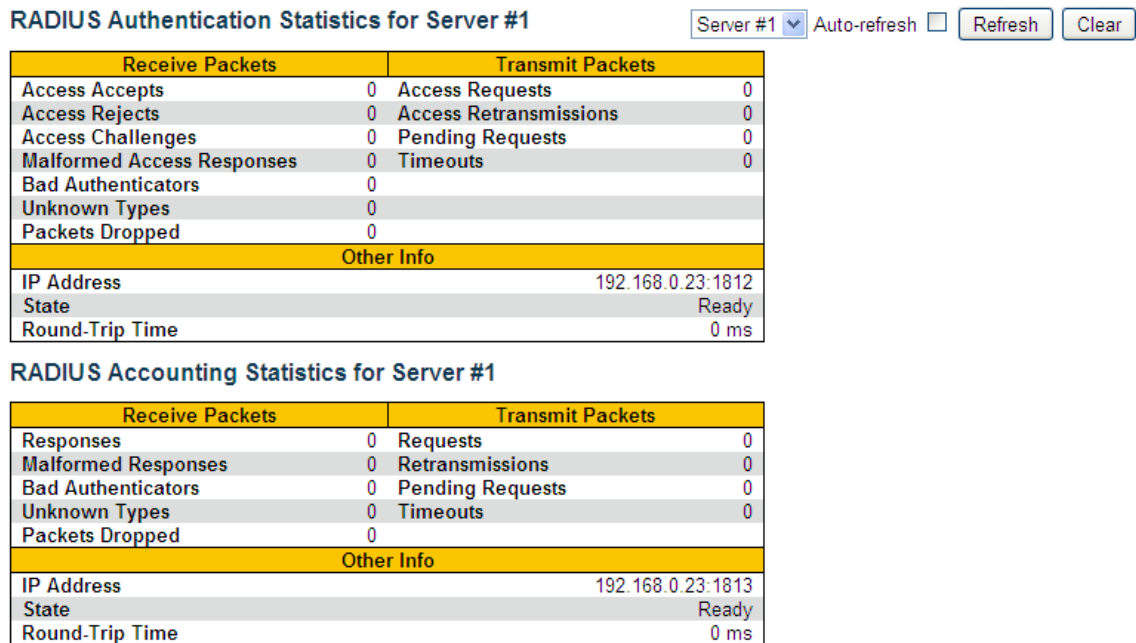


Figure 140 View Detailed RADIUS Server Statistics

Select a server, and view the designated server detailed statistics.

### 9.10.3 Typical Configuration Example

As shown in Figure 141, IEEE802.1X is enabled on port 1 of the switch. Then users can log in to the switch through port 1 after passing the authentication on the RADIUS server. The IP address of the server is 192.168.0.23. The key for packet exchange between the switch and the server is aaa.

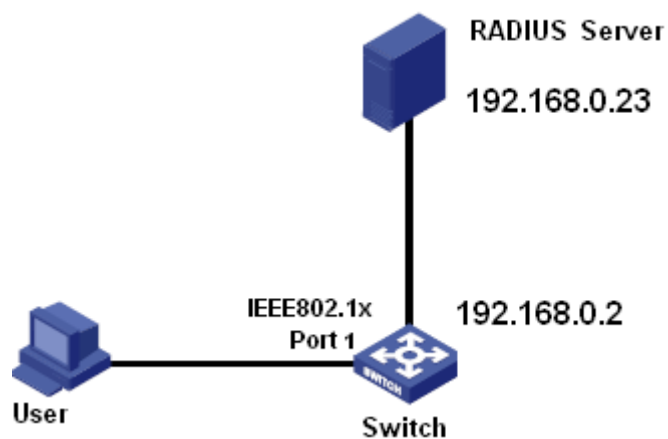


Figure 141 RADIUS Authentication Example

1. Set the IP address of the authentication server to 192.168.0.23 and password to aaa, as shown in Figure 138.
  2. IEEE802.1x settings: enable IEEE802.1X globally. Set authentication type to radius, admin state of port 1 to port-based 802.1X, keep default settings for the other parameters. For details, see section "10.2IEEE802.1X Configuration".
  3. Set both the user name and password on the RADIUS Server to ccc, encrypt key to aaa.
  4. Install and run 802.1x client software on a PC. Enter ccc for the user name and password.
- Then the user can pass the authentication and access the switch.

## 10 Network

### 10.1 Port Security

#### 10.1.1 Introduction

Port security limits the maximum number of users per port, which are uniquely identified by MAC addresses and vlan id. If the MAC address limit on the port is enabled, the maximum number of users on the port is MAC limit. If the number of MAC addresses on the port exceeds the maximum limit, the corresponding action is triggered.

#### 10.1.2 Web Configuration

Configure port-security mac limit parameters, as shown in Figure 142.

**System Configuration**

<b>Mode</b>	Enabled <input type="button" value="v"/>
<b>Aging Enabled</b>	<input checked="" type="checkbox"/>
<b>Aging Period</b>	<input type="text" value="3600"/> seconds

Figure 142 System Configuration

**Mode:**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable global mac limit function.

**Aging Enable:**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable global mac aging function.

**Aging Period:**

Range: 10~10000000s

Default: 3600s

Function: mac address can be aged by this period

1. Mac limit port configuration, as shown in Figure 143.

**Port Configuration**

Port	Mode	Limit	Action	State	Reopen
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Enabled	4	None	Ready	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen

Figure 143 Port Configuration

**Mode:**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable port mac limit function.

**Limit:**

Range:1~1024

Default:4

Function: Configure max number of mac limit.

**Action:**

Option: None/Trap/Shutdown/Trap&Shutdown

Default: None

Function:

Configure the action after the port learns more MAC addresses than the limit.

**State:**

Option: Disabled/Ready/Limit Reached/Shutdown

**Reopen:**



If a port is shutdown by this module, you may reopen it by clicking this button.



**Caution:**

- 1、 Both Port Mode and [Global Mode](#) must be set to Enabled for Limit Control to be in effect.
- 2、 Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

3.Port Security Switch Status, as shown in Figure 144.

**Port Security Switch Status**

**User Module Legend**

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

**Port Status**

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	L--	Ready	0	4
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

Figure 144 Port Security Switch Status

4.Port Security Status, as shown in Figure 145.

**Port Security Status Port 5**

MAC Address	VLAN ID	State	Time of Addition	Ageing Time(s)
54-e6-fc-6a-fe-a0	1	Forwarding	1970-01-01T07:19:41+00:00	3597

Figure 145 Port Status

## 10.2 IEEE802.1X Configuration

### 10.2.1 Introduction

To ensure WLAN security, IEEE802 LAN/WAN committee proposed the 802.1X protocol. As a common access control mechanism for LAN ports in Ethernet, 802.1X implements Ethernet authentication and security. 802.1X is a port-based network access control. Port-based network access control is to implement authentication and control on the ports of LAN access devices. If a user passes the authentication, it can access the resources in the LAN. If it cannot pass the authentication, it cannot access the resources in the LAN. 802.1X systems adopt the Client/Server structure, as shown in Figure 146. User authentication and authorization of port-based access control requires the following elements:

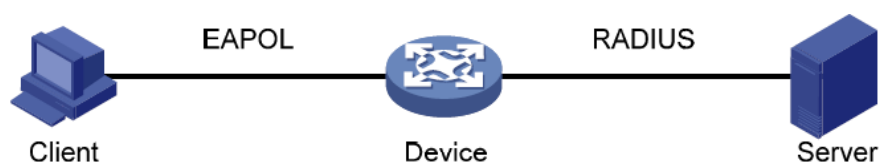


Figure 146 IEEE802.1X Structure

**Client:** usually indicates a user terminal. When a user wants to surf the Internet, it starts the client program and enters required user name and password. The client program will send a connection request. The client should support EAPOL (Extensible Authentication Protocol over LAN).

**Device:** indicates the authentication switch in an Ethernet system. It uploads and delivers user authentication information, and enables or disables a port based on the authentication result.

**Authentication server:** indicates the entity that provides authentication service for devices. It checks whether users have the permissions to use network services according to the identifiers (user names and passwords) sent by clients, and enables or disables ports according to authentication results.

### 10.2.2 Web Configuration

1. Configure global IEEE802.1X parameters, as shown in Figure 147.

## Network Access Server Configuration

### System Configuration

Mode	Enable
Reauthentication Enabled	<input checked="" type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Quiet Timer	10 seconds
RADIUS-Assigned QoS Enabled	<input checked="" type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input checked="" type="checkbox"/>
Guest VLAN Enabled	<input checked="" type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input checked="" type="checkbox"/>

Figure 147 Configure Global IEEE802.1X Parameters

#### Mode

Options: Enable/Disable

Default: Disable

Function: Enable/Disable global IEEE802.1x security function.

#### Reauthentication Enabled

Options: Enable/Disable

Default: Disable

Function: Configure whether regular re-authentication is required when authentication succeeds.

#### Reauthentication Period

Range: 1~3600s

Default: 3600s

Function: When authentication succeeds, set the time interval for re-authentication.

“Reauthentication Period” can be configured only if enabling “Reauthentication Enabled”.

#### EAPOL Timeout

Range: 1~65535s

Default: 30s

Function: Set the overtime for response from the client. After sending an identity EAPOL

request packet, the device will retransmit identity EAPOL request packet if it still receives no response from the client after the specified time.

### **Aging Period**

Range: 10~1000000s

Default: 300s

Function: Configure aging period. When Reauthentication is disabled, the time interval for re-authentication is 2\*aging period.

### **Quiet Timer**

Range: 10~1000000s

Default: 10s

Function: If authentication fails, the device enters to quiet period. During the quiet period, the device does not respond to authentication requests from the client.

### **RADIUS-Assigned QoS Enabled**

Options: Enable/Disable

Default: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-Assigned QoS Enabled** is checked on the server, the authorization information includes CoS information assigned for authorization. The equipment will modify the CoS value of the client authentication port based on the assigned value.

### **RADIUS-Assigned VLAN Enabled**

Options: Enable/Disable

Default: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-Assigned VLAN Enabled** is checked on the server, the authorization information includes VLAN information assigned for authorization. The equipment will add the client authentication port to the assigned VLAN.

### **Guest VLAN Enabled**

Options: Enable/Disable

Default: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. All users that access this port are authorized to access the resources in the guest VLAN.

### **Guest VLAN ID**

Range: 1~4095

Default: 1

Function: Configure guest VLAN ID.

### **Max. Reauth. Count**

Range: 1~255

Default: 2

Function: Set the maximum retransmission attempts for Identity EAPOL request packets. If the device still receives no response packets from the client after maximum retransmission attempts, the device will consider authentication fails.

### **Allow Guest VLAN if EAPOL Seen**

Options: Enable/Disable

Default: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. When disabled, the device adds the port to the guest VLAN only when this port has no EAPOL frame record.



#### **Caution:**

- The precondition for configuring “Guest VLAN ID”, “Max. Reauth. Count”, and “Allow Guest VLAN if EAPOL Seen” is enabling “Guest VLAN ID”.
  - It is recommended to disable “RADIUS-Assigned VLAN Enabled” and “Guest VLAN ID”, when the authentication port type is Trunk or Hybrid.
  - The CoS value assigned for authorization does not change or affect the configuration of the port. However, the priority of the COS value assigned for authorization is higher than a COS value configured by a user. In other words, what is valid after authentication is the CoS value assigned for authorization. If a user fails to be authenticated or goes offline, the CoS value configured by the user take effects.
-

- The VLAN assigned for authorization or the guest VLAN does not change or affect the configuration of the port. However, the VLAN assigned for authorization or the guest VLAN has a higher priority than a VLAN configured by a user.

After a user initiates authentication, and if the authentication is successful:

If the port enables **RADIUS-Assigned VLAN**, the port is added to the VLAN assigned by the RADIUS server.

If the port does not enable **RADIUS-Assigned VLAN**, the port is added to the VLAN configured by the user.

If a user fail to be authenticated or goes offline:

If the port enables **Guest VLAN** and **Allow Guest VLAN if EAPOL Seen**, the port is added to the VLAN.

If the port enables **Guest VLAN** but does not enable **Allow Guest VLAN if EAPOL Seen**, the port is added to the guest VLAN when no EAPOL fame record is available, and is added to the VLAN configured by the user when EAPOL frame record is available.

If the port does not enable **Guest VLAN**, the port is added to the VLAN configured by the user.

## 2. Configure IEEE802.1X port, as shown in Figure 148.

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate	Reinitialize
2	Port-based 802.1X	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Unauthorized	Reauthenticate	Reinitialize
3	MAC-based Auth.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Unauthorized	Reauthenticate	Reinitialize
4	Force Unauthorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
5	Force Unauthorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize

Submit Reset

Figure 148 Configure IEEE802.1X port

### Port

Options: all switch ports.

### Admin State

Options: Force Authorized/Force Unauthorized/Port-based 802.1X/MAC-based Auth.

Default: Force Authorized

Function: Select the port authentication mode.

Description: **Force Authorized** means port is always in an authorized state and allows users to access network resource without authentication.

**Force Unauthorized** means the port is always in unauthorized state and does not allow users to conduct authentication and the switch does not provide authentication services to clients that access the switch from this port. **MAC-based Auth** indicates that users using the port need to be authenticated respectively. When a user is offline, only the user cannot use the network. **Port-based 802.1X** indicates that users are authenticated based on port. After the first user using the port passes authentication, all the other users using the port do not need to be authenticated. However, when the first user is offline, the port is disabled and all the other users using the port cannot use the network.

#### **RADIUS-Assigned QoS Enabled**

Options: Enable/ Disable

Default: Disable

Function: Enable or disable RADIUS-Assigned QoS on port.

#### **RADIUS-Assigned VLAN Enabled**

Options: Enable/ Disable

Default: Disable

Function: Enable or disable RADIUS-Assigned VLAN on port.

#### **Guest VLAN Enabled**

Options: Enable/ Disable

Default: Disable

Function: Enable or disable guest VLAN on port.



**Note:**

This function is available only when **RADIUS-Assigned QoS/RADIUS-Assigned VLAN/Guest VLAN** is enabled at both the global and port levels.

---

**Port State**

Options: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth

Function: Display port authentication state. **Globally Disabled** indicates IEEE802.1X is disabled globally; **Authorized** indicates the user connected to the port passes authentication; **Unauthorized** indicates the user connected to the port fails to pass authentication; **Link Down** indicates the port is link down; x Auth/y Unauth indicates x users are authorized and y users are unauthorized when the port authentication mode is MAC-based Auth.

When the port authentication mode is MAC-based Auth or Port-based 802.1X, you can click <Reauthenticate>/<Reinitialize> button to reauthenticate. The port state changes to **Unauthorized** during reauthenticating.

3. View IEEE802.1X configuration, as shown in Figure 149.

**Network Access Server Switch Status**

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
<a href="#">1</a>	Force Authorized	Authorized			-	
<a href="#">2</a>	Port-based 802.1X	Unauthorized			-	
<a href="#">3</a>	MAC-based Auth.	Unauthorized			-	
<a href="#">4</a>	Force Unauthorized	Link Down			-	
<a href="#">5</a>	Force Unauthorized	Link Down			-	
<a href="#">6</a>	Force Authorized	Link Down			-	
<a href="#">7</a>	Force Authorized	Link Down			-	
<a href="#">8</a>	Force Authorized	Link Down			-	
<a href="#">9</a>	Force Authorized	Link Down			-	
<a href="#">10</a>	Force Authorized	Link Down			-	

Figure 149 View IEEE802.1X Configuration

Click <port> to enter the “IEEE802.1X statistics” page.

4. View IEEE802.1X statistics, as shown in Figure 150.



**NAS Statistics**

Port 1  Auto-refresh

**Port State**

Admin State	Port-based 802.1X
Port State	Authorized
QoS Class	-
Port VLAN ID	

**Port Counters**

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	4	Total	5
Response ID	1	Request ID	3
Responses	1	Requests	1
Start	1		
Logoff	1		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	1	Responses	2
Other Requests	4		
Auth. Successes	1		
Auth. Failures	0		
Last Supplicant Info			
MAC Address	44-37-e6-88-6e-90		
VLAN ID	1		
Version	1		
Identity	ccc		

Figure 150 View IEEE802.1X Statistics

Select a port, and view the designated port IEEE802.1X statistics.

**10.2.3 Typical Configuration Example**

As shown in Figure 151, client is connected to port 1 of the switch. Enable IEEE802.1x on port 1 and select Port-based 802.1X authentication mode. The username and password of the remote authentication are both ddd.

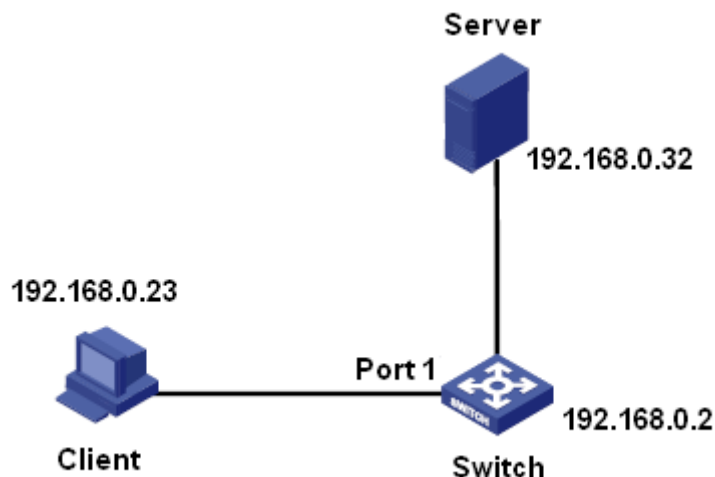


Figure 151 IEEE802.1x Configuration Example

You can refer to the typical configuration example in “9.10 RADIUS Configuration”.

## 10.3 ACL

### 10.3.1 Overview

With the development of network technologies, security issues have become increasingly prominent, calling for access control mechanism. With the Access Control List (ACL) function, the switch matches packets with the list to implement access control.

### 10.3.2 Implementation

The series switches filter packets according to the matched ACL. Each entry consists several conditions in the logical AND relationship. ACL entries are independent of each other.

The switch compares a packet with ACL entries in the ascending order of entry IDs. Once a match is found, the action is taken and no further comparison is conducted, as shown in the following figure.

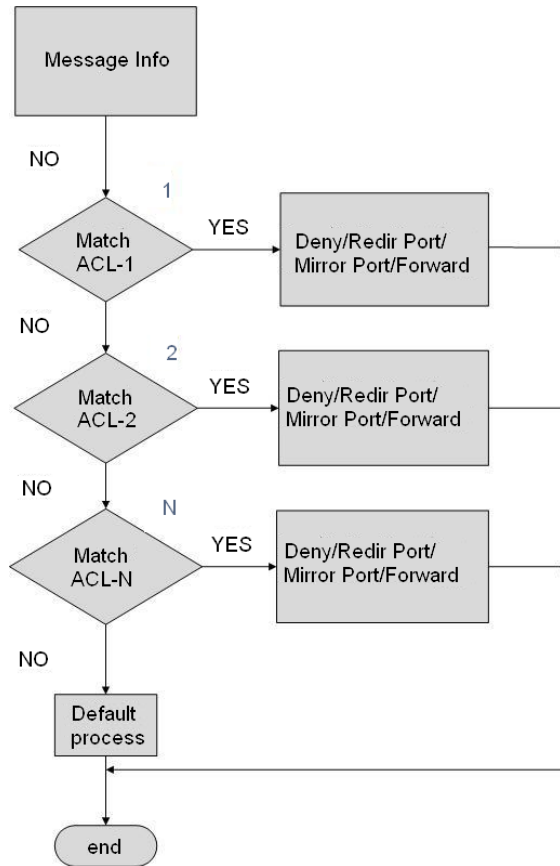


Figure 152 ACL Processing Flowchart



**Note:**

Default process indicates the processing mode towards packets matching no ACL entry.

**10.3.3 Web Configuration**

1. Configure ACL ports, as shown in Figure 153.



**Caution:**

The ACL port configuration specifies the processing mode of packets received by a port that do not match any ACL entry.

ACL Ports Configuration Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	111897
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Figure 153 Configure ACL Ports

**Policy ID**

Range: 0~255

Default: 0

Function: Configure the port policy ID.

**Action**

Options: Deny/Permit

Default: Permit

Function: Configure the action towards a packet that mismatches any ACL entry. Deny: Packets mismatching any entry will be denied. Permit: Packets mismatching any entry will be forwarded.

**Rate Limiter ID**

Range: Disabled/1~16

Default: Disabled

Function: whether to enable port rate limit function, and select rate limiter ID.

**EVC Policer**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port EVC policer.

**EVC Policer ID**

Range: 1~256

Default: 1

---

Function: After enabling EVC policer, configure port EVC policer ID.

---

**Caution:**

The port rate limit and EVC policy cannot be enabled simultaneously.

---

**Port Redirect**

Options: Disabled/ any port

Default: Disabled

Function: Enable/Disable port redirect function. After enabling port redirect function, packets mismatching any ACL entry will be forwarded to the specified port.

---

**Caution:**

Port redirection can be enabled only when Action is set to Deny.

---

**Mirroring**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port mirroring function. After enabling port mirroring function, packets mismatching any ACL entry will be forwarded to both the destination port and the mirroring destination port.

---

**Caution:**

The prerequisite for enabling ACL port mirroring is that a mirroring destination port must exist.

---

**Logging**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port logging function. Enabled: if a port receives a packet that does not match any ACL entry, the packet is written into the system log. Disabled: if a port receives a packet that does not match an ACL entry, the packet is not written into the system log.

**Shutdown**

Options: Enabled/Disabled

Default: Disabled

Function: whether to shutdown port or not. Enabled: if a port receives a packet that does not match any ACL entry, the port is shut down. Disabled: if a port receives a packet that does not match an ACL entry, the port is not shut down.

**Counter**

Function: Display the number of packets that mismatching any ACL entry that each port receives.

2. Configure ACL rate limiter, as shown in Figure 154.

**ACL Rate Limiter Configuration**

Rate Limiter ID	Rate	Unit
*	1	<> ▾
1	1	pps ▾
2	1	pps ▾
3	1	pps ▾
4	1	pps ▾
5	1	pps ▾
6	1	pps ▾
7	1	pps ▾
8	1	pps ▾
9	1	pps ▾
10	1	pps ▾
11	1	pps ▾
12	1	pps ▾
13	1	pps ▾
14	1	pps ▾
15	1	pps ▾
16	1	pps ▾

Submit Reset

Figure 154 Configure ACL Rate Limiter

**Rate Unit**

Range: 0~3276700 pps/ 0~1000000 Kbps (the step is 100)

Default: 1 pps

Function: Set the limited rate of a rate limiter ID.

3. Configure ACL entry, as shown in Figure 155.

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	2	Any	EType	Deny	Disabled	1	Disabled	0	+ ⊕ ⊖ ⊗
4	6	Any	Any	Permit	Disabled	Disabled	Disabled	0	+ ⊕ ⊖ ⊗
2	3	Any	Any	Permit	Disabled	Disabled	Disabled	0	+ ⊕ ⊖ ⊗
3	5	Any	IPv4/UDP 50	Permit	Disabled	Disabled	Disabled	0	+ ⊕ ⊖ ⊗

Figure 155 Configure ACL Entry

When there are multiple ACL entries, the device compares a packet with the ACL entries one by one (from top to bottom). Once a match is found, the action is taken and no further comparison is conducted.

Click <⊕> to add a new ACL entry; click <⊖> to edit the ACL entry; click <⊗> to delete the ACL entry, click <⬆> to move up the current entry; click <⬇> to move down the current entry.

ACE is the ID of an ACL entry, which is numbered based on the entry creation time sequence.

4. Configure the ACL entry parameters

- Configure the ACL entry parameters, as shown in Figure 156.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xFF
Frame Type	Ethernet Type

Figure 156 Configure the ACL Entry Parameters

**Ingress Port**

Option: All/ any port

Default: All

Function: Select a port on which the access control entry (ACE) takes effect.

**Policy Filter**

Options: Any/Specific

Default: Any

Function: Set an ACE condition--policy ID. When it is set to Specific, a policy value and policy bitmask need to be set. When the policy value of a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**Policy Value**

Range: 0~255

Function: Configure policy value.

**Policy Bitmask**

Range: 0x0~0xFF

Function: Set the policy bitmask. The policy value and policy bitmask are used for matching in the policy filtering. A policy bitmask is converted into binary digits and then right-aligned with the policy value (in binary mode). The value 1 indicates the same and the value 0 indicates that any value is allowed.

**Frame Type**

Options: Any/Ethernet Type/IPv4

Default: Any

Function: Set a condition--packet type. When the type of a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➤ Configure VLAN parameters, as shown in Figure 157.

**VLAN Parameters**

802.1Q Tagged	Any	▼
VLAN ID Filter	Specific	▼
VLAN ID	1	
Tag Priority	Any	▼

Figure 157 Configure VLAN Parameters

**802.1Q Tagged**

Options: Any/ Disabled/ Enabled



Default: Any

Function: Set a condition--802.1Q tag. The value Disabled indicates untagged packets and the value Enabled indicates tagged packets. When a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**VLAN ID Filter**

Options: Any/ Specific (1~4095)

Default: Any

Function: Set a condition--VID. When it is set to Specific, a VID value needs to be entered. When the VID in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully. When 802.1Q Tagged is set to Disabled, this parameter needs to be set to Any.

**Tag Priority**

Option: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

Default: Any

Function: Set a condition--tag priority. When the priority in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully. When 802.1Q Tagged is set to Disabled, this parameter needs to be set to Any.

➤ Configure EtherType frame parameters, as shown in Figure 158.

**MAC Parameters**

SMAC Filter	Specific
SMAC Value	02-02-02-02-02-02
DMAC Filter	Any

**Ethernet Type Parameters**

EtherType Filter	Any
------------------	-----

Figure 158 Configure EtherType Frame Parameters

**SMAC Filter**

Options: Any/ Specific

Default: Any

Function: Set a condition--source MAC address. When it is set to Specific, a source MAC address needs to be set. When the source MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**DMAC Filter**

Options: Any/ UC/ MC / BC/ Specific

Default: Any

Function: Set a condition--destination MAC address. When it is set to Specific, a destination MAC address needs to be set. When the destination MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**Ether Type Filter**

Options: Any/ Specific (0x600~0xFFFF, exclude 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6))

Default: Any

Function: Set a condition--Ethernet type. When it is set to Specific, an Ethernet type needs to set. When an Ethernet packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➤ Configure IPv4 frame parameters, as shown in Figure 159.

**MAC Parameters**

DMAC Filter	Any ▼
-------------	-------

**IP Parameters**

IP Protocol Filter	Other ▼
IP Protocol Value	0
IP TTL	Zero ▼
IP Fragment	Yes ▼
IP Option	Any ▼
SIP Filter	Any ▼
DIP Filter	Any ▼

Figure 159 Configure IPv4 Frame Parameters

**DMAC Filter**

Options: Any/ UC/ MC / BC

Default: Any

Function: Set a condition--destination MAC address. When the destination MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

### **IP Protocol Filter**

Options: Any/ ICMP/ UDP/ TCP/ Other (0~255)

Default: Any

Function: Set a condition--IPv4 packet protocol type. When it is set to ICMP, UDP, or TCP, relevant parameters need to be set. When it is set to Other, a protocol ID needs to be set. When the protocol type in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

### **IP TTL**

Options: Any/Non-zero/zero

Default: Any

Function: Set a condition--TTL field in IP packets. The value Non-zero indicates that the condition is matched when the IP TTL in an IPv4 packet is larger than 0, and the value Zero indicates that the condition is not matched when the IP TTL in an IPv4 packet is larger than 0.

### **IP Fragment**

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP fragment. When the IP fragment in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

### **IP Option**

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP option. When the IP option in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

### **SIP Filter**

Options: Any/Host/Network

Default: Any

Function: Set a condition--source IP address. When it is set to Host, an IP address needs to be set. When it is set to Network, an IP address and a subnet mask need to be set. When the source IP address in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**DIP Filter**

Options: Any/Host/Network

Default: Any

Function: Set a condition--destination IP address. When it is set to Host, an IP address needs to be set. When it is set to Network, an IP address and a subnet mask need to be set. When the destination IP address in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➤ Configure ICMP parameters, as shown in Figure 160.

**ICMP Parameters**

ICMP Type Filter	Any	▼
ICMP Code Filter	Any	▼

Figure 160 Configure ICMP Parameters

**ICMP Type Filter**

Options: Any/Specific (0~255)

Default: Any

Function: Set a condition--ICMP type. When it is set to Specific, an ICMP type needs to be set. When the ICMP type in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

**ICMP Code Filter**

Options: Any/Specific (0~255)

Default: Any

Function: Set a condition--ICMP code. When it is set to Specific, an ICMP code needs to be set. When the ICMP code in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

- Configure UDP parameters, as shown in Figure 161.

**UDP Parameters**

Source Port Filter	Any	▼
Dest. Port Filter	Any	▼

Figure 161 Configure UDP Parameters

**Source Port Filter/ Destination Port Filter**

Options: Any/ Specific (0~65535) / Range (0~65535)

Default: Any

Function: Set a condition--UDP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs to be set. When the UDP port IDs in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

- Configure TCP parameters, as shown in Figure 162.

**TCP Parameters**

Source Port Filter	Any	▼
Dest. Port Filter	Any	▼
TCP FIN	1	▼
TCP SYN	Any	▼
TCP RST	Any	▼
TCP PSH	Any	▼
TCP ACK	Any	▼
TCP URG	Any	▼

Figure 162 Configure TCP Parameters

**Source Port Filter/ Destination Port Filter**

Options: Any/ Specific (0~65535) / Range (0~65535)

Default: Any

Function: Set a condition--TCP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs to be set. When the TCP port IDs in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

**TCP FIN/SYN/RST/PSH/ACK/URG**

Options: Any/1/0

Default: Any

Function: Set a condition--TCP control fields. When the TCP control fields in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

➤ Configure ACL entry action, as shown in Figure 163.

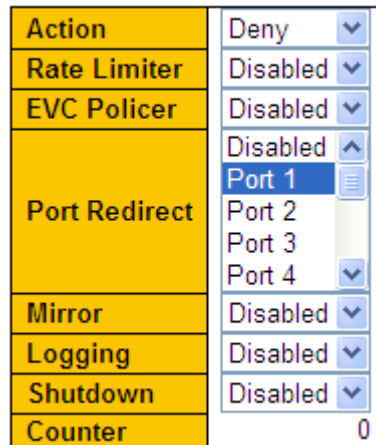


Figure 163 Configure ACL Entry Action

**Action**

Options: Deny/Permit/Filter

Default: Permit

Function: Specify the mode for an ingress port to process a packet that matches an ACE. The value Deny indicates discarding the packet, the value Permit indicates forwarding the packet, and the value Filter indicates filtering the packet and a filtering port needs to be selected.

**Rate Limiter**

Options: Disabled/1~16

Default: Disabled

Function: whether to enable port rate limit function, and select rate limiter ID.

**EVC Policer**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port EVC policer.

## EVC Policer ID

Range: 1~256

Default: 1

Function: After enabling EVC policer, configure port EVC policer ID.

---

**Caution:**

The port rate limit and EVC policy cannot be enabled simultaneously.

---

## Port Redirect

Options: Disabled/ any port

Default: Disabled

Function: Enable/Disable port redirect function. After enabling port redirect function, packets matching any entry will be forwarded to the specified port.

---

**Caution:**

Port redirection can be enabled only when Action is set to Deny.

---

## Mirroring

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port mirroring function. After enabling port mirroring function, packets matching any entry will be forwarded to both the destination port and the mirroring destination port.

---

**Caution:**

The prerequisite for enabling ACL port mirroring is that a mirroring destination port must exist.

---

## Logging

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port logging function.

Function: Enable/Disable port logging function. Enabled: if a port receives a packet that

match any ACL entry, the packet is written into the system log. Disabled: if a port receives a packet that match an ACL entry, the packet is not written into the system log.

**Shutdown**

Options: Enabled/Disabled

Default: Disabled

Function: whether to shutdown port or not. Enabled: if a port receives a packet that match any ACL entry, the port is shut down. Disabled: if a port receives a packet that match an ACL entry, the port is not shut down.

**Counter**

Function: Display the number of packets matching the ACE that each port receives.

➤ View ACL entries, as shown in Figure 164.

**ACL Status**

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
rp_mirror_cpu	1	EType	Filter	Disabled	Enabled	Yes	0	No
devSmacDrop	1	EType	Deny	Disabled	Disabled	No	0	No
bootp	1	IPv4/UDP 67-68	Filter	Disabled	Enabled	Yes	298	No
arp	1	ARP	Filter	Disabled	Enabled	Yes	199870	No
static	1	EType	Deny	Disabled	Disabled	No	0	No
static	4	Any	Permit	Disabled	Disabled	No	0	No
static	2	Any	Permit	Disabled	Disabled	No	0	No
static	3	IPv4/UDP 50	Permit	Disabled	Disabled	No	0	No
static	5	EType	Permit	Disabled	Disabled	No	0	No
static	6	IPv4/Other 0	Permit	Disabled	Disabled	No	0	No

Figure 164 View ACL Entries

**Conflict**

Options: No/Yes

Function: Displays the conflict status of an ACL entry. If resources for creating an ACL entry are insufficient, **Conflict** is set to **Yes** for this entry. Otherwise, **Conflict** is set to **No** for this entry.

**10.3.4 Typical Configuration Example**

Connect port 2 of the switch. Configure the port to receive packets only from source MAC address 02-02-02-02-02-02 and forward the packets through port 1.

Configuration steps:

1. Configure the port action to Deny, as shown in Figure 153.



2. Configure ACL entry, set ingress port to 2, frame type to Ethernet Type, as shown in Figure 156.
3. Set SMAC filter to 02-02-02-02-02-02, as shown in Figure 158.
4. Configuration ACL entry action to Deny, port redirect to port 1, as shown in Figure 163.
5. Keep all the other parameters default or empty.

# 11 Port Aggregation

## 11.1 Static Aggregation

### 11.1.1 Introduction

Port channel is to bind a group of physical ports that have the same configuration to a logical port to increase bandwidth and improve transmission speed. The member ports in a same group share traffic and serve as dynamic backups for each other, improving connection reliability.

Port group is a physical port group on the configuration layer. Only the physical ports that join in port group can participate in link aggregation and become a member of port channel. When physical ports in a port group meet certain conditions, they can conduct port aggregation and form a port channel and become an independent logical port, thereby increasing network bandwidth and providing link backup.

### 11.1.2 Implementation

As shown in Figure 165, three ports on Switch A and Switch B aggregate to form a port channel. The bandwidth of the port channel is the total bandwidth of these three ports.

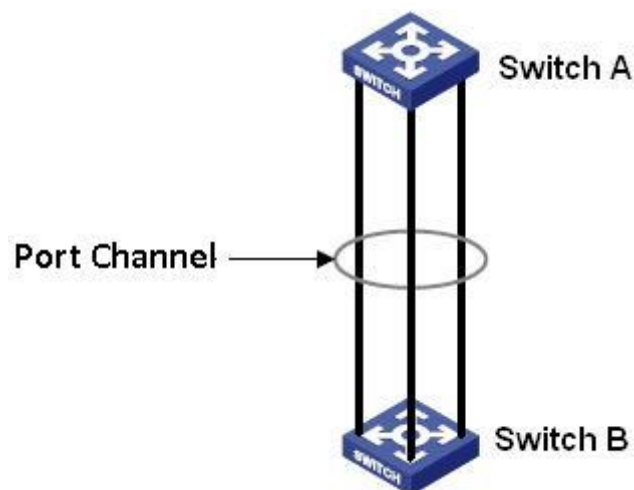


Figure 165 Port Channel

If Switch A sends packets to Switch B by way of the port channel, Switch A determines the member port for transmitting the traffic based on the calculation result of load sharing. When

one member port of the port channel fails, the traffic transmitted through the port is taken over by another normal port based on load sharing algorithm.



**Caution:**

- A port can be added to only one port group.
- Only full duplex ports can join an aggregation.
- The port in a port channel cannot be enabled LACP, and a port enabled LACP cannot be added to a port channel.
- Port channel and redundant port are mutually exclusive. The port in a port channel cannot be configured as a redundant port, and a redundant port cannot be added to a port channel.
- Redundant port in this document refers to DT-Ring ring port, DT-Ring backup port, DRP ring port, DRP backup port, RSTP port, and MSTP port.

**11.1.3 Web Configuration**

1. Configure load sharing mode of port channel, as shown in Figure 166.

**Aggregation Mode Configuration**

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Figure 166 Load Sharing Mode Configuration

**Hash Code Contributors**

Options: Source MAC Address/Destination MAC Address/IP Address/ TCP/UDP Port Number

Default: Source MAC Address/IP Address/ TCP/UDP Port Number

Function: Set the load sharing mode of port channel.

Description: Source MAC Address indicates source MAC address-based load sharing. Destination MAC Address indicates destination MAC address-based load sharing. IP Address indicates IP address-based load sharing. TCP/UDP Port Number indicates load sharing based on TCP/UDP port number.

2. Configure aggregation group port members, as shown in Figure 167.

### Aggregation Group Configuration

		Port Members											
Group ID		1	2	3	4	5	6	7	8	9	10	11	12
Normal		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 167 Configure Aggregation Group Port Members

#### Port Member

Function: Select aggregation group port members.

Description: All member ports in one aggregation group have the same configuration. The number of trunk groups depends on the number of switch ports. Each group can contain a maximum of 8 ports.

#### 11.1.4 Typical Configuration Example

As shown in Figure 165, add three ports (port 1, 2, and 3) of Switch A to port group 1 and three ports (port 1, 2, and 3) of switch B to port group 1. Use network cables to connect these ports to form a port channel, realizing load sharing among ports. (It is assumed that the three ports on Switch A and B have the same attributes respectively).

#### Configuration on switches:

1. Add port 1, 2, and 3 of switch A to port group 1, as shown in Figure 167.
2. Add port 1, 2, and 3 of switch B to port group 1, as shown in Figure 167.

### 11.2 LACP

#### 11.2.1 Introduction

Link Aggregation Control Protocol (LACP) is based on the IEEE802.3ad standard. It is used to exchange information with the peer port over Link Aggregation Control Protocol Data Unit (LACPDU), in order to select a member port in the dynamic aggregation group.

### 11.2.2 Implementation

A port enabled with LACP informs the peer port of its LACP priority of the local equipment, equipment MAC address, LACP priority of the port, port number and key value by sending an LACPDU message. The peer port negotiates with the local port after receiving the LACPDU message:

1. Compare the IDs of the equipment at both ends (equipment ID = equipment LACP priority+ equipment MAC address). At first, compare the LACP priorities. If the LACP priorities are the same, compare their MAC addresses. Select the equipment with a smaller ID as the master equipment.
2. Compare the port IDs of the master equipment (port ID = LACP priority of the port + port number). At first, compare the LACP priorities of the ports. If the port LACP priorities are the same, compare the port numbers. Select the port with a smaller ID as the reference port.
3. If this port and reference port have the same key values, and the same port attribute configurations in Up state, and the peer ports of this port and the reference port have the same key values and port attribute configurations, this port can become a member port of the dynamic aggregation group.

### 11.2.3 Web Configuration

1. Configure LACP port, as shown in Figure 168.

### LACP Port Configuration

Ports	LACP Enabled	Key	Role	Timeout	Prio
*	<input checked="" type="checkbox"/>	<>	<>	<>	32768
1	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
2	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
3	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
4	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
5	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
6	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
7	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
8	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
9	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
10	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768

Submit    Reset

Figure 168 Configure LACP Port

#### LACP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable LACP on port.

#### Key

Options: Auto/Specific (1~65535)

Default: Auto

Function: Configure the port key value. Auto means the key value depends on port speed, key=1 (10Mb), key=2 (100Mb), key=3 (1000Mb). Ports with different key values cannot be added to a aggregation group.

#### Role

Options: Active/Passive

Default: Active

Function: Selects the role state of LACP. An active port will actively send LACPDU messages to the peer port. A passive port will send LACPDU messages to the peer port after receiving LACPDU messages from the peer port.



**Caution:**

For two connected ports, at least one port should be active; otherwise, the two ports cannot exchange information with each other.

**Timeout**

Options: Fast/Slow

Default: Fast

Function: Configures the interval for the active port to send LACPDU messages. **Fast** indicates that the interval is 1s. **Slow** indicates that the interval is 30s.

**Prio**

Default: 1~65535

Default: 32768

Function: Configures the LACP priority of a port, which is used for selecting a reference port.

Port with a lower priority in the master equipment is selected as the reference port.

2. View LACP system status, as shown in Figure 169.

**LACP System Status**

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-01-c1-01-00-02	2	32768	0d 00:00:28	1,2

Figure 169 View LACP System Status

3. View LACP port status, as shown in Figure 170.

**LACP Status**

Ports	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	2	LLAG1	00-01-c1-01-00-02	1	32768
2	Yes	2	LLAG1	00-01-c1-01-00-02	2	32768
3	Yes	2	-	-	-	-
4	Yes	2	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Figure 170 View LACP Port Status

**LACP**

Options: Yes/No

Function: View LACP status of ports. Yes means LACP is enabled and the port is LinkUp. No means LACP is not enabled or the port is LinkDown.

4. View LACP port statistics, as shown in Figure 171.

**LACP Statistics**

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	333	326	0	0
2	222	221	0	0
3	0	7	0	0
4	0	7	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Figure 171 View LACP Port Statistics

**11.2.4 Typical Configuration Example**

As shown in Figure 165, add three ports (port 1, 2, and 3) of Switch A to port group 1 and three ports (port 1, 2, and 3) of switch B to port group 1. Use network cables to connect these ports to form a port channel, realizing load sharing among ports. (It is assumed that the three ports on Switch A and B have the same attributes respectively).

**Configuration on switches:**

1. Enable LACP on port 1, 2, and 3 of switch A, as shown in Figure 168.
2. Enable LACP on port 1, 2, and 3 of switch B, as shown in Figure 168.



## 12 Loop Detect Configuration

### 12.1 Overview

After loop detect is enabled for the port, loop detect packets would be sent out through the port to decide whether loops exist in the network connected to the port. The CPU send loop detect packets to the port periodically. If any port of the switch receives the loop detect packets, it is determined that the loops exist in the network. Shut down the port that is sending loop detect packets and the port would be linked up automatically after a while and continue detection. The time interval for sending loop detect packets and the port recover time can be configured in the software.

**Note:**

Loop detection and DT-Ring/DRP/RSTP/MSTP are mutually exclusive. A port enabled loop detection cannot be configured as a redundant port; a redundant port cannot be enabled loop detection.

---

### 12.2 Web Configuration

1. Configure the loop detect function of the port, as shown in Figure 172.

General Settings

Global Configuration

Enable Loop Protection	Enable <input type="button" value="v"/>
Transmission Time	5 <input type="text"/> seconds
Shutdown Time	180 <input type="text"/> seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> <input type="button" value="v"/>	<> <input type="button" value="v"/>
1	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
2	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
3	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
4	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
5	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
6	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
7	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
8	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
9	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
10	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
11	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
12	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>

Figure 172 Enable the Loop Detect Function of the Port

**Enable Loop Protection**

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global loop detect function of the port.

**Transmission Time**

Range: 1~10s

Default: 5s

Function: Configure the time interval for sending loop detect packets.

**Shutdown Time**

Range: 0~604800s

Default: 180s

Function: Configure the port recover time, 0 indicates the port cannot be linked up automatically until restarting device.

**Enable**

Options: Enable/Disable

Default: Enable

Function: Enable or disable the loop detection function of the port.

**Action**

Option: Shutdown Port/Shutdown Port and Log/Log Only

Default: Shutdown Port

Function: Specify the action to be performed when a port detects that a loop exists.

**Tx Mode**

Options: Enable/Disable

Default: Enable

Function: Whether to send loop detect packets or not.



**Caution:**

A port can accurately detect whether a loop exists only after the loop protection is enabled globally, the loop protection and Tx mode are enabled on the port.

2. View loop protection status, as shown in Figure 173.

**Loop Protection Status**

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	14	Down	-	2015-11-14T13:29:24+08:00
3	Shutdown	Enabled	8	Disabled	Loop	2015-11-14T13:30:55+08:00
4	Shutdown	Enabled	1	Down	-	2015-11-14T13:26:33+08:00
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

Figure 173 View Loop Protection Status

### Loop Protection Status

Options: --/Loop

Function: Loop detection status displays whether there are loops in the network when the loop detection function of the port is enabled. Loop indicates there are loops while -- indicated no loop exists.

### 12.3 Typical Configuration Example

Networking Requirements:

Port 3 of the switch is connected to the external network. When there are loops for the network, shut down port 3, as shown in Figure 174.

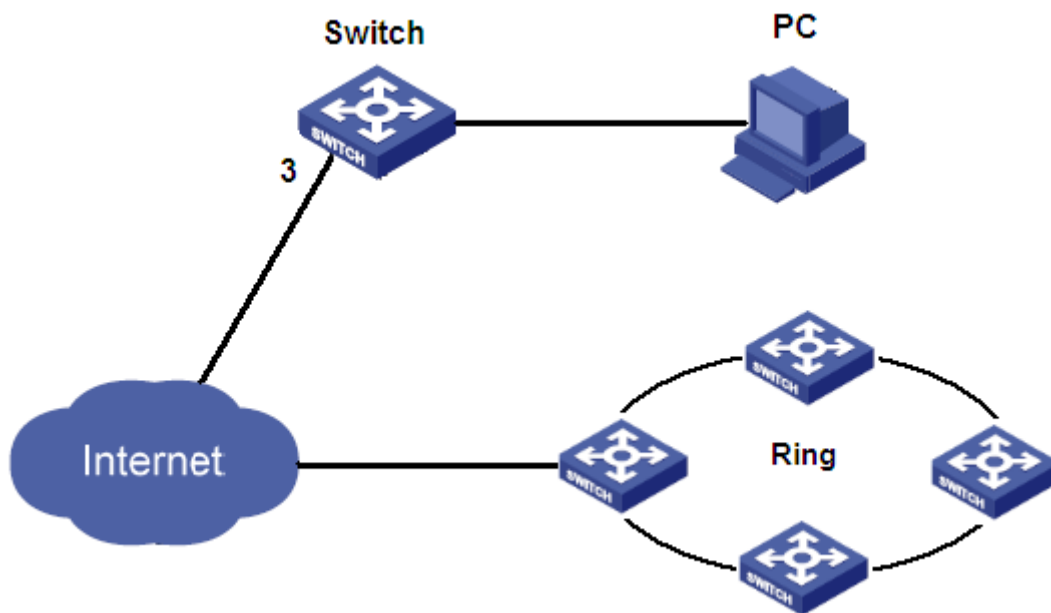


Figure 174 Loop Detect Instance

Specific configuration:

Enable the loop detection on port 3, as shown in Figure 172.

## 13 Industry Protocol

### 13.1 EtherNet/IP

#### 13.1.1 Introduction

EtherNet/IP is an industrial application layer protocol for industrial automation applications. It is based on standard TCP/IP and UDP/IP protocols and uses fixed Ethernet hardware and software to define an application layer protocol for configuring, accessing, and controlling industrial automation devices.

This series of switches enable users to set port state (enable/disable) using the EtherNet/IP protocol to obtain device information, port information, alarm information, DT-ring information, DRP information, and RSTP information.

#### 13.1.2 Web Configuration

Configure EtherNet/IP protocol, as shown in Figure 175.

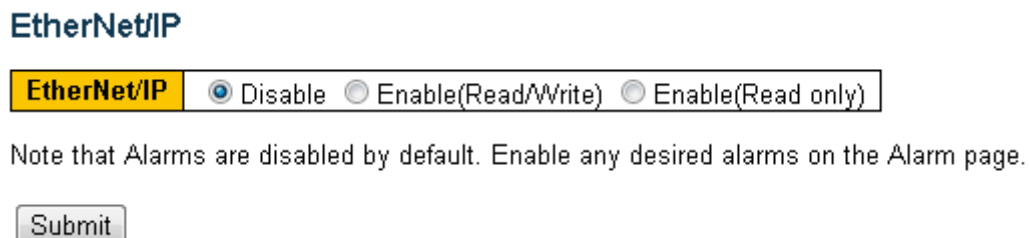


Figure 175 EtherNet/IP Configuration

**Option:** Disable/Enable(Read/Write)/Enable(Read Only)

**Default:** Disable

**Function:** Enable EtherNet/IP ,and utilize EtherNet/IP protocol to configure device state.

### 13.2 ModbusTCP

#### 13.2.1 Introduction

The ModbusTCP protocol is a Modbus protocol based on Ethernet TCP/IP. Modbus is an application layer message transmission protocol, which uses Master/Slave (Master/Slave) to communicate. Modbus is a simple client/server application protocol. The server analyzes,

processes requests, and sends replies to the client.

This series of switches enables users to set port status (enable/disable) using the ModbusTCP protocol to obtain device information, port information, alarm information, DT-ring information, DRP information, and RSTP information

### 13.2.2 Web Configuration

Configure Modbus TCP protocol, as shown in Figure 176.

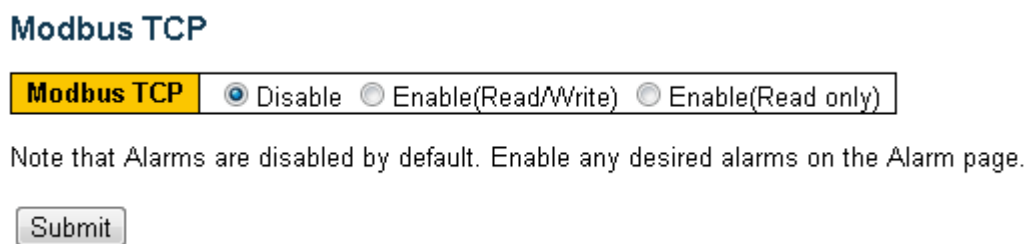


Figure 176 Modbus TCP Configuration

**Option:** Disable/Enable(Read/Write)/Enable(Read Only)

**Default:** Disable

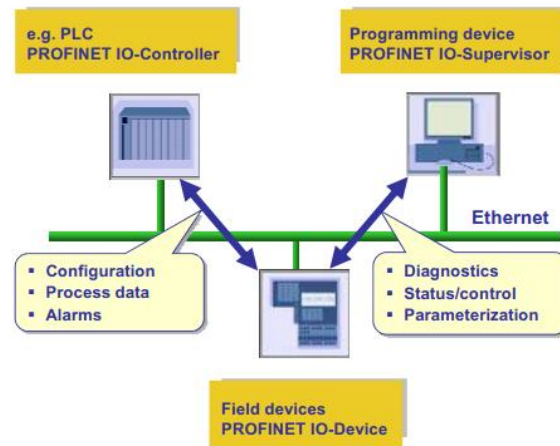
**Function:** Enable Modbus TCP, and utilize Modbus TCP protocol to configure device state.

## 13.3 PROFINET

### 13.3.1 Introduction

PROFINET is an industrial communication network based on Ethernet for all applications views from PROFIBUS International (PI). It covers the key markets and key technologies in automation both today and in the future. With PROFINET I/O implementation, production and process automation can be easily done. Besides, data exchanges on PROFINET I/O are done between I/O controller (PLC, etc.) and I/O devices (field devices).

There are three major roles in PROFINET I/O network structure. They are I/O controller, I/O supervisor, and I/O devices. It follows the provider and consumer model for data exchange. The detail descriptions are below.



**•I/O Controller**

I/O Controller is a role to control the I/O device. In PROFINET I/O networking, it may exist exact one controller. However, it allows several controllers to implement system redundancy. The typical controller is the programmable logic controller (PLC) where the automation program runs.

**•I/O Supervisor**

I/O supervisor may be a programming device which control I/O controller, personal computer, or HMI device for commissioning or diagnostic use.

**•I/O Device**

I/O device is a distributed field device which connected to one or more I/O controllers via PROFINET I/O. It sends switch data to controller periodically by supported cycle time.

PROFINET switch acts as a PROFINET I/O device. It supports many useful attributes for I/O controller to configure or monitor. The detail attributes are described under GSD file and following subject.

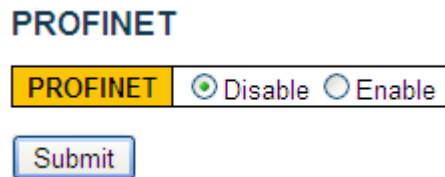
**•GSD**

A PROFINET switch as an I / O device needs to provide a GSD file description to ensure that the device can be identified by the controller. The GSDI / O file models the PROFINET switch equipment and uses GSDML language to form the file. In this way, the device can be

configured and simulated by STEP7 or TIA PORTAL software. A GSD file will describe the functions supported by the device in detail.

### 13.3.2 WEB Configuration

Configure PROFINET protocol, as shown in Figure 177



PROFINET

PROFINET  Disable  Enable

Submit

Figure 177 PROFINET Configuration

**Option:** Disable/Enable

**Default:** Disable

**Function:** Enable/Disable PROFINET protocol



## 14 Multicast

### 14.1 IGMP Snooping

#### 14.1.1 Introduction

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast protocol at the data link layer. It is used for managing and controlling multicast groups. IGMP Snooping-enabled switches analyze received IGMP packets, establish mapping between ports and MAC multicast addresses, and forward multicast packets according to the mapping.

There are three versions of the Internet Group Message Protocol (IGMP): IGMPv1, IGMPv2, and IGMPv3. IGMPv1 is defined in RFC1112, IGMPv2 is defined RFC2236, and IGMPv3 is defined in RFC3376.

IGMPv1 supports two types of packets (report and query packets) and defines the basic group member query and report process.

IGMPv2, on the basis of IGMPv1, provides the leave packet of the fast leave mechanism for group members. With this mechanism, when the last member leaves a multicast group, the router is instructed to conduct fast convergence. In comparison with IGMPv1, IGMPv2 supports two types of query packets: general query packet and group-specific query packet. The switch periodically sends a general query packet to query the membership. When a host leaves a multicast group, after the switch receives a leave message, the switch sends a group-specific query packet to determine whether all members leave the multicast group.

The host source filtering function is added to IGMPv3. This function enables a host to specify whether to receive or reject packets from some specific multicast group sources.

#### 14.1.2 Basic Concepts

Querier: periodically sends IGMP general query packets to query the status of the members in the multicast group, maintaining the multicast group information. When multiple queriers exist on a network, they automatically elect the one with the smallest IP address to be the querier. Only the elected querier periodically sends IGMP general query packets. The other

queriers only receive and forward IGMP query packets.

Router port: receives general query packets (on an IGMP-enabled switch) from the querier. Upon receiving an IGMP report, a switch establishes a multicast entry and adds the port that receives the IGMP report to the member port list. If a router port exists, it is also added to the member port list. Then the switch forwards the IGMP report to other devices through the router port, so that the other devices establish the same multicast entry.

IGMP snooping proxy: The IGMP snooping proxy function is configured on an edge device to reduce the number of IGMP report packets and leave packets received by an upstream device, thereby improving the overall performance of the upstream device. A device on which the IGMP snooping proxy function is configured functions as a host of its upstream device, and functions as a querier of its downstream host.

### 14.1.3 Principle

IGMP Snooping manages and maintains multicast group members by exchanging related packets among IGMP-enabled devices. The related packets are as follows:

General query packet: The querier periodically sends general query packets (destination IP address: 224.0.0.1) to confirm whether the multicast group has member ports. After receiving the query packet, a non-querier device forwards the packet to all its connected ports.

Specific query packet: If a device wants to leave a multicast group, it sends an IGMP leave packet. After receiving the leave packet, the querier sends a specific query packet (destination IP address: IP address of the multicast group) to confirm whether the group contains other member ports.

Membership report packet: If a device wants to receive the data of a multicast group, the device sends an IGMP report packet (destination IP address: IP address of the multicast group) immediately to respond to the IGMP query packet of the group.

Leave packet: If a device wants to leave a multicast group, the device will send an IGMP leave packet (destination IP address: 224.0.0.2).

### 14.1.4 Web Configuration

1. Enable IGMP Snooping, as shown in Figure 177.

#### IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Figure 177 Enabling IGMP Snooping

#### Snooping Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global IGMP Snooping protocol.

#### Unregistered IPMCv4 Flooding Enabled

Options: Enable/Disable

Default: Enable

Function: Configure unregistered multicast action. Enable: when receiving an unregistered multicast packet, the switch broadcasts the packet within the VLAN (all ports except the inlet port). Disable: when receiving an unregistered multicast packet, the switch discards it. Unregistered multicast packets refer to the multicast packets without corresponding forwarding entries on the switch.

#### IGMP SSM Range

Format: A.B.C.D/ 4~32

Default: 232.0.0.0/8

Function: Only hosts and routers with the address within the value of this parameter can run the service model of IGMP source specific multicast (SSM) provided that the hosts and routers support the IGMP SSM service model. The SSM service model provides users with a transmission service of specifying multicast sources for a client.

#### Leave Proxy Enabled

Options: Enabled/Disabled

Default: Disabled

Function: Specify whether to forward leave packets to the querier. When it is enabled, leave packets are not forwarded.

**Proxy Enabled**

Options: Enabled/Disabled

Default: Disabled

Function: Specify whether to forward leave packets and member report packets to the querier. When it is enabled, leave packets and member report packets are not forwarded.

2. Configure IGMP port, as shown in Figure 178.

**Port Related Configuration**

Port	Router Port	Throttling
*	<input checked="" type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	unlimited
2	<input checked="" type="checkbox"/>	unlimited
3	<input checked="" type="checkbox"/>	unlimited
4	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	unlimited

Figure 178 Configure IGMP Port

**Router Port**

Options: Enabled/Disabled

Default: Disabled

Function: Configure router port.

**Throttling**

Options: unlimited/1~10

Default: unlimited

Function: Whether to limit the number of multicast entries learnt by a port.

3. Configure IGMP Snooping VLAN, as shown in Figure 179.

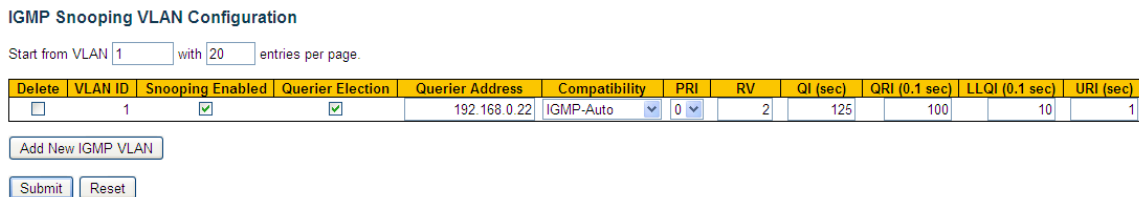


Figure 179 Configure IGMP Snooping VLAN

**VLAN ID**

Options: all created VLAN IDs

**Snooping Enabled**

Options: Enable/Disable

Default: Disable

Function: Enable or disable the VLAN IGMP Snooping function. The precondition of this function is to enable global IGMP Snooping function.

**Querier Election**

Options: Enable/Disable

Default: Enable

Function: Enable or disable the IGMP query function for the selected VLAN. The precondition of this function is to enable global IGMP Snooping function and the VLAN IGMP Snooping function.

Description: If there are multiple queriers in network, they will automatically select the one with the smallest IP address to be the querier. If there is only one device which enables IGMP query function, it will be the querier.

**Querier Address**

Format: A.B.C.D

Function: Configure the source IP address of sending the query packet. When no querier address is set, the IP address of the VLAN port is used as the querier address.

**Compatibility**

Options: IGMP-Auto/Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

Default: IGMP-Auto

Function: Configure IGMP version.

**PRI (Priority of Interface)**

Range: 0~7

Default: 0

Function: Configure the priority of IGMP control packet.

**RV (Robustness Variable)**

Range: 1~255

Default: 2

Function: Specify the robustness parameter of the IGMP query function.

Description: The larger the parameter, the worse the network environment. User can set a suitable robustness parameter according to the actual network.

**QI (Query Interval)**

Range: 1~31744s

Default: 125s

Function: Configure the interval of sending general query packet.

**QRI (Query Response Interval)**

Range: 0~31744 (unit: 0.1s)

Default: 100

Function: Configure the max response time of responding general query packet.

**LLQI (Last Member Query Interval)**

Range: 0~31744 (unit: 0.1s)

Default: 10

Function: Configure the max response time of responding specific query packet.

**Caution:**

QI, QRI, and LLQI configuration is valid only for querier.

---

**URI (Unsolicited Report Interval)**

Range: 0~31744s

Default: 1s

Function: Set the interval for a host to re-send a report packet for joining a multicast group

Click <Add New IGMP VLAN> to configure IGMP Snooping VLAN entry. A maximum of 32 IGMP Snooping VLAN entries are supported.

4. View IGMP Snooping status, as shown in Figure 180.

**IGMP Snooping Status**

**Statistics**

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v2	v2	ACTIVE	209	84	0	1541	140	78
2	v3	v3	ACTIVE	0	0	0	0	0	0
3	v3	v3	ACTIVE	0	0	0	0	0	0

**Router Port**

Port	Status
1	Both
2	Static
3	Static
4	Both
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Figure 180 View IGMP Snooping Status

**Router Port Status**

Options: Both/Static/Dynamic

Function: Display router port status. Static indicates that a port is statically configured as a router port, Dynamic indicates that a port is dynamically learnt as a router port, and Both indicates that a port is statically configured as a router port or dynamically learnt as a router port.

5. View the multicast member list, as shown in Figure 181.

VLAN ID	Groups	Port Members												
		1	2	3	4	5	6	7	8	9	10	11	12	
1	224.0.1.1	✓		✓										
1	225.10.24.3	✓		✓										
1	226.81.9.8	✓		✓										
1	239.2.11.71	✓		✓										
1	239.5.5.5	✓		✓										
1	239.77.124.213	✓		✓										
1	239.255.255.250	✓		✓										
1	239.255.255.254	✓		✓										

Figure 181 IGMP Snooping Member List

### 14.1.5 Typical Application Example

As shown in Figure 182, enable IGMP Snooping function in Switch 1, Switch 2, and Switch 3. Enable auto query on Switch 2 and Switch 3. The IP address of Switch 2 is 192.168.1.2 and that of Switch 3 is 192.168.0.2, so Switch 3 is elected to querier.

1. Enable IGMP Snooping.
2. Enable IGMP Snooping and auto-query.
3. Enable IGMP Snooping and auto-query.

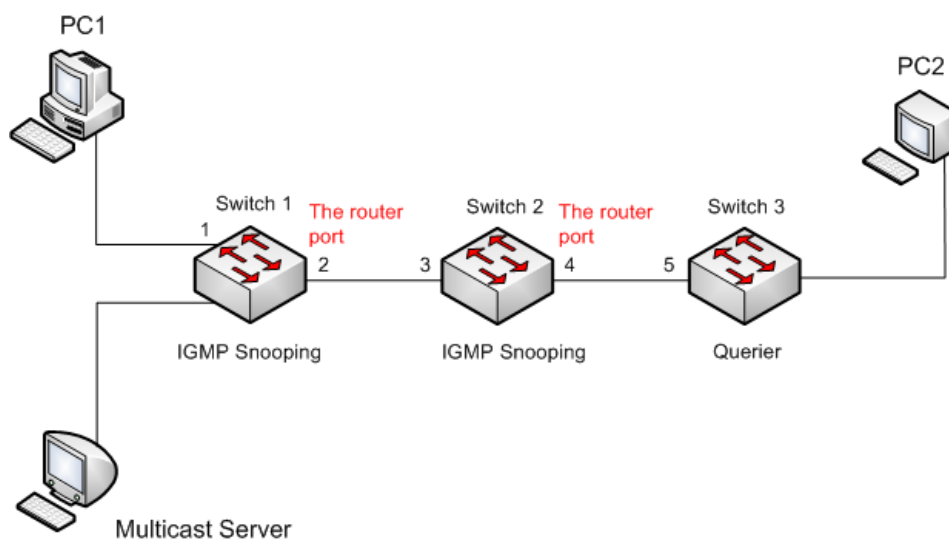


Figure 182 IGMP Snooping Application Example

- Because Switch 3 is elected as the querier, it periodically sends out a general query message.
- Port 4 of Switch 2 receives query message. It becomes router port. Meanwhile, Switch 2



forwards query message from port 3. Then port 2 of Switch 1 is elected to router port once it receives query message from Switch 2.

- When PC 1 joins in multicast group 225.1.1.1, it will send out IGMP report message, so port 1 and router port 2 of Switch 1 will also join in multicast group 225.1.1.1. Then, the IGMP report message will be forwarded to Switch 2 by router port 2, so port 3 and port 4 of Switch 2 will also join in 225.1.1.1, and then the IGMP report message will be forwarded to Switch 3 by router port 4, so port 5 of Switch 3 will join in 225.1.1.1 as well.
- When multicast server's multicast data reaches Switch 1, the data will be forwarded to PC1 by port 1; because router port 2 is also a multicast group member, so the multicast data will be forwarded by router port. In this way, when the data reaches port 5 of Switch 3, it will stop forwarding because there is no receiver any more, but if PC2 also joins in group 255.1.1.1, the multicast data will be forwarded to PC2.

## 14.2 GMRP

### 14.2.1 GARP Introduction

The Generic Attribute Registration Protocol (GARP) is used for spreading, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network. With GARP, the configuration information of a GARP member will spread the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

- When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn. A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.
- When a GARP application entity wants to cancel its own information on other switches,

the entity sends a Leave message.

- After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.



**Caution:**

An application entity indicates a GARP-enabled port.

---

GARP timers include Hold timer, Join timer, Leave timer, and LeaveAll timer.

- **Hold Timer:** When receiving a registration message, a GARP entity does not send a Join message immediately, but starts Hold timer. When the timer expires, the entity sends all the registration messages received within the preceding period in one Join message, reducing packet sending for better network stability.
- **Join Timer:** To ensure that Join messages are received by other application entities, a GARP application entity starts Join timer after sending a Join message. If receiving no JoinIn message before Join timer expires, the entity sends the Join message again. If receiving a JoinIn message before the timer expires, the entity does not send the second Join message.
- **Leave Timer:** When a GARP application entity wants to cancel the information about an attribute, the entity sends a Leave message. The entity receiving the message starts Leave timer. If receiving no Join message before the timer expires, the entity receiving the message cancels the information about the attribute.
- **LeaveAll Timer:** As a GARP application entity starts, it starts LeaveAll timer. When the timer expires, the entity sends a LeaveAll message, so that the other GARP application entities re-register all the attributes. Then the entity starts LeaveAll timer again for the new cycle.

### 14.2.2 GMRP Protocol

The GARP Multicast Registration Protocol (GMRP) is a multicast registration protocol based on GARP. It is used for maintaining the multicast registration information of switches. All GMRP-enabled switches can receive multicast registration information from other switches, update local multicast registration information dynamically, and spread local multicast

registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-enabled switches on a network.

If a switch or terminal wants to join or leave a multicast group, the GMRP-enabled port broadcasts the information to all the ports in the same VLAN.

**Explanation:**

Agent port: indicates the port on which GMRP and the agent function are enabled.

Propagation port: indicates the port on which only GMRP is enabled, but not the proxy function.

GMRP must have one or more agent port. Dynamically learned GMRP multicast entry and agent entry are forwarded by the propagation port to the propagation ports of the lower-level devices.

All GMRP timers on the same network must keep consistent to prevent mutual interference.

The timers should comply with the following rules: Hold timer < Join timer, 2 \* Join timer < Leave timer, and Leave timer < LeaveAll timer.

**14.2.3 Web Configuration**

1. GMRP global configuration, as shown in Figure 183.

**Global Configuration**

<b>GMRP Enabled</b>	<input checked="" type="checkbox"/>
<b>Hold timer</b>	100 ms
<b>Join timer</b>	500 ms
<b>Leave timer</b>	3000 ms
<b>Leave all timer</b>	10000 ms

Figure 183 GMRP Global Configuration

**GMRP Enabled:**

Option: Enable/Disabled

Default: Disabled

Function: Enable global gmrp function

**Timer:**

Option: Hold timer/join timer/Leave timer/Leave all timer

Default: 100/500/3000/10000ms

Function: Configure global gmrp timer value.

2.GMRP Port Configuration, as shown in Figure 184.

**Port Related Configuration**

	Port Members									
	1	2	3	4	5	6	7	8	9	10
GMRP Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agent Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 184 GMRP Port Configuration,

**GMRP Enabled:**

Option: Enabled/Disabled

Default: Disabled

Function: Enable port gmrp.

**Agent Enabled:**

Option: Enabled/Disabled

Default: Disabled

Function: Enable port gmrp agent.

3.Agent MAC Table Configuration, as shown in Figure 185.

**Agent MAC Table Configuration**

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	1	01-00-00-00-00-01	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	01-00-00-00-00-02	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 185 Agent MAC Table Configuration

Function: Configure static multicast mac address of agent, bound with port and vlan.

Note: You must enable global gmrp, port gmrp, and port gmrp proxy at the same time to configure this item.

4.GMRP MAC Table Status, as shown in Figure 186.

**GMRP MAC-Address Table**

MAC Type

Type	VLAN	MAC Address	Port Members													
			CPU	1	2	3	4	5	6	7	8	9	10			
Agent	1	01-00-00-00-00-01		✓												
Agent	2	01-00-00-00-00-02		✓												

Figure 186 GMRP MAC Table Status

**MAC Type:**

Option: All/Agent/Dynamic

Default: All

**14.2.4 Typical Application Example**

As shown in Figure 187, Switch A and Switch B are connected by port 2. Port 1 of Switch A is set to an agent port and generates two multicast entries:

- MAC address: 01-00-00-00-00-01, VLAN: 1
- MAC address: 01-00-00-00-00-02, VLAN: 2

After configuring different VLAN attributes on ports, observe the dynamic registration between switches and multicast information update.

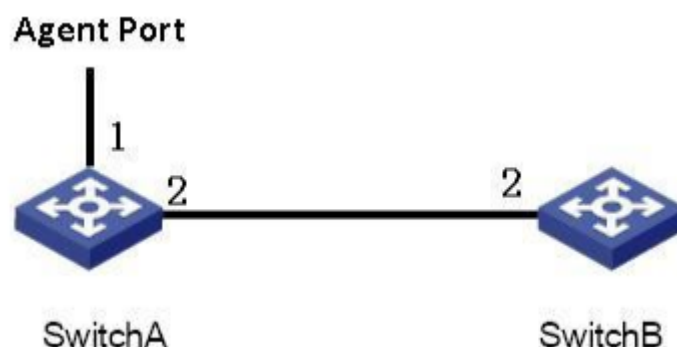


Figure 187 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as

shown in Figure 183.

2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; set the timers to default values, as shown in Figure 184.

3. Configure agent multicast entry. Set <MAC address, VLAN ID, Member port> to <01-00-00-00-00-01, 1, 1> and <01-00-00-00-00-02, 2, 1>, as shown in Figure 185.

Configuration on Switch B:

1. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 183.

2. Enable GMPR function in port 2; set the timers to default values, as shown in Figure 184.

Table 6 lists the dynamically learned GMRP multicast entries in Switch B.

Table 6 Dynamic Multicast Entries

View Prompt	View Type	View Function	Command for View Switching
SWITCH #	Privileged mode	View recently used commands. View software version. View response information for ping operation. Upload/Download configuration file. Restore default configuration. Reboot switch. Save current configuration. Display current configuration. Update software.	Input " <b>configure terminal</b> " to switch from privileged mode to configuration mode. Input " <b>exit</b> " to return to the general mode.
SWITCH (config) #	Configuration mode	Configure all switch functions.	Input " <b>exit</b> " or " <b>end</b> " to return to the Privileged mode.

### 14.3 Unregistered Multicast Action

Web configuration, as shown in Figure 188.

**Unregistered Multicast Action**

<b>L2 Unregistered Multicast</b>	<input type="radio"/> Discard	<input checked="" type="radio"/> Forward
<b>IP Unregistered Multicast</b>	<input type="radio"/> Discard	<input checked="" type="radio"/> Forward

Figure 188 Unregistered Multicast Action

**L2 Unregistered Multicast:**

Option: Discard/Forward

Default: Forward

**IP Unregistered Multicast:**

Option: Discard/Forward

Default: Forward

## 15 LLDP

### 15.1 Introduction

The Link Layer Discovery Protocol (LLDP) provides a standard link layer discovery mechanism. It encapsulates device information such as the capability, management address, device identifier, and interface identifier in a Link Layer Discovery Protocol Data Unit (LLDPDU), and advertises the LLDPDU to its directly connected neighbors. Upon receiving the LLDPDU, the neighbors save these information to MIB for query and link status check by the NMS.

### 15.2 Web Configuration

1. Configure LLDP, as shown in Figure 189.

#### LLDP Configuration

##### LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

##### LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FastEthernet 1/9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Submit Reset

Figure 189 Configure LLDP

#### Tx Interval



Range: 5~32768s

Default: 30s

Function: Configure the time interval for sending LLDP packets.

### **Tx Hold**

Range: 2~10 times

Default: 4 times

Function: Set the number of Tx holding times. Effective duration of an LLDP packet = Tx Interval x Tx Hold.

### **Tx Delay**

Range: 1~8192s

Default: 2s

Function: Set the transmission interval between a new LLDP packet and the previous LLDP packet after configuration information is changed. The value of Tx Delay cannot be larger than 1/4 of the value of Tx Interval.

### **Tx Reinit**

Range: 1~10s

Default: 2s

Function: After LLDP is disabled on a port or a switch is restarted, the switch sends an LLDP shutdown frame to a neighboring node to announce that the previous LLDP packet is invalid. Tx Reinit refers to the interval between transmission of the LLDP shutdown frame and re-initialization of an LLDP packet.

### **Mode**

Options: Enabled/Disabled/Rx only/Tx only

Default: Enabled

Function: Set the LLDP packet mode. The enabled mode indicates that the switch can send LLDP packets, and receive and identify LLDP packets; the disabled mode indicates that the switch neither sends LLDP packets nor receives LLDP packets; the only Rx mode indicates that the switch only receives and identifies LLDP packets; the only Tx mode indicates that the switch only sends LLDP packets.

### **Port Descr**

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry port description.

**Sys Name**

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system name.

**Sys Descr**

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system description.

**Sys Capa**

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system capability.

**Mgmt Addr**

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry management address.

2. View LLDP connection information, as shown in Figure 190.

**LLDP Neighbor Information**

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
FastEthernet 1/1	C0-A8-00-1A	20-03				
FastEthernet 1/2	00-01-C1-00-00-00	Fa 1/3	FastEthernet 1/3		Bridge(+)	192.168.0.223 (IPv4)

Figure 190 LLDP Information



**Caution:**

To display LLDP information, LLDP must be enabled on the two connected devices.

## 16 MEP

### 16.1 Web Configuration

1.The Maintenance Entity Point instances are configured here, as shown below.

Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
<input type="checkbox"/>	1	Port	Mep	Down	1	0		100	00-1E-CD-20-25-00	
<input type="checkbox"/>	2	Port	Mep	Down	2	2		100	00-1E-CD-20-25-01	

Figure 191 Maintenance Entity Point

#### Delete

Function: This box is used to mark a MEP for deletion in next Save operation.

#### Instance

Function: The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.

#### Domain

Configuration options: Port/EVC/VLAN

Default configuration: Port

Function: Select domain

Describe: **Port** is a MEP in the Port Domain. EVC is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created.

**VLAN** is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created. The current function does not support EVC mode

#### Mode

Configuration options: Mep/Mip

Default configuration: Mep

Describe: **MEP** is a Maintenance Entity End Point. **MIP** is a Maintenance Entity Intermediate Point.

#### Direction

Configuration options: Down/Up

Default configuration: Down

Describe: **Down** is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

**Up** is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

### **Residence Port**

Configuration range: Is the valid port number on the actual device.

Function: The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

### **Level**

Configuration range: 0~7

Describe: The MEG level of this MEP.

### **Flow Instance**

Describe: The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

### **Tagged VID**

Function:::An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

### **This MAC**

Function: **Port MEP**, The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

### **Alarm**

Function: There is an active alarm on the MEP.

2.Instance Configuration, as shown below.

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
2	ITU ICC	vlan2	ICC000MEG0000	1	100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 192 Instance Configuration

**Level**

Configuration range:0~7

Describe: ID of MEP

**Format**

Configuration options: ITU ICC /IEEE String/ITU CC ICC

Default configuration: ITU ICC

Function: This is the configuration of the Maintenance Association Identifier formats.

**Domain Name**

Describe: This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

**MEG Id**

Describe: This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

**MEP Id**

Describe: This value will become the transmitted two byte CCM MEP ID.

**Tagged VID**

Describe: This value will be the VID of a TAG added to the OAM PDU.

**Syslog**

Describe: This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

**cLevel**

Describe: Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

**cMEG**

Describe: Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

**cMEP**

Describe: Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

**cAIS**

Describe: Fault Cause indicating that AIS PDU is received.

**cLCK**

Describe: Fault Cause indicating that LCK PDU is received.

**cDEG**

Describe: Fault Cause indicating that server layer is indicating Signal Degraded.

**cSSF**

Describe: Fault Cause indicating that server layer is indicating Signal Fail.

**aBLK**

Describe: The consequent action of blocking service frames in this flow is active.

**aTSD**

Describe: The consequent action of indicating Trail Signal Degraded is calculated.

**aTSF**

Describe: The consequent action of indicating Trail Signal Fail to-wards protection is active.

3. Peer MEP Configuration, as shown below.

**Peer MEP Configuration**

Delete	Peer MEP ID	Unicast Peer MAC	cLOC	cRDI	cPeriod	cPriority
No Peer MEP Added						
<input type="button" value="Add New Peer MEP"/>						

Figure 193 Peer MEP Configuration

**Delete**

Describe: This box is used to mark a Peer MEP for deletion in next Save operation.

**Peer MEP ID**

Describe: This value will become an expected MEP ID in a received CCM.

**Unicast Peer MAC**

Describe: This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

**cLOC**

Describe: Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

**cRDI**

Describe: Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

**cPeriod**

Describe: Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

**cPriority**

Describe: Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

4.Functional Configuration, as shown below;

**Functional Configuration**

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
<input type="checkbox"/>	0	1 f/sec	<input type="checkbox"/>	<input type="checkbox"/>	0	Multi	L-APS	1

Figure 194 Functional Configuration

**Continuity Check**

**Enable**

Configuration options: Select / deselect

Function: Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

**Priority**

Configuration range: 1~9

Function: The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority'

has to be the same.

### **Frame rate**

Configuration options: 300 f/sec,100 /sec,10 f/sec,1 f/sec,6 f/min,1 f/min,6 f/hour

Default configuration: 1 f/sec

Describe: Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:

- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Function: Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

### **TLV**

Configuration options: Select / deselect

Enable/disable of TLV insertion in the CCM PDU.

### **APS Protocol**

#### **Enable**

Configuration options: Select / deselect

Function: Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

#### **Priority**

Function: The priority to be inserted as PCP bits in TAG (if any).

#### **Cast**

Configuration options: Multi/Uni

Default configuration: Multi

Function: Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be



taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

**Type**

Configuration options: L-APS/R-APS

Default configuration: R-APS

Describe: R-APS: APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Click fault management. This page allows the user to check and configure the fault management of the current MEP instance.

Please note that, the sub-tables of Link Trace, Link Trace State, Client, AIS and LOCK are not supported while the MEP entry is in MPLS (Link/Tunnel/PW/LSP) domain. as shown below;

**Loop Back**

Enable	DEI	Priority	Cast	Peer MEP	Unicast MAC	To Send	Size	Interval
<input type="checkbox"/>	<input type="checkbox"/>	0	Multi ▾	1	00-00-00-00-00-00	10	64	100

Figure 195 Loop Back

**Enable**

Configuration options: Select / Deselect

Function: Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

**DEI**

Configuration options: Select / Deselect

Function: The DEI to be inserted as PCP bits in TAG (if any).

**Priority**

Function: The priority to be inserted as PCP bits in TAG (if any).

**Cast**

Configuration options: Multi/Un

Function: -Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

### Peer MEP

Function: This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

### Unicast MAC

Function: This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

### To Send

Default configuration:10

Describe: The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.

### Size

Default configuration:64

Function: The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

**Switch RX frame MAX size:** The MAX frame size (all inclusive) accepted on the switch port of Bytes

**CPU RX frame MAX size:** The MAX frame size (all inclusive) possible to copy to CPU of Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

**Interval**

Function: The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)".

Loop Back State configuration, as shown below;

**Loop Back State**

Transaction ID	Transmitted	Reply MAC	Received	Out Of Order
1	0	00-00-00-00-00-00	0	0

Figure 196 Loop Back State

**Transaction ID**

Function: The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.

**Transmitted**

Function: The total number of LBM PDU transmitted.

**Reply MAC**

Function: The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.

**Received**

Function: The total number of LBR PDU received from this 'Reply MAC'.

**Out Of Order**

Function: The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace configuration, as shown below;

**Link Trace**

Enable	Priority	Peer MEP	Unicast MAC	Time To Live
<input checked="" type="checkbox"/>	0	1	00-00-00-00-00-00	1

Figure 197 Link Trace

**Enable**

Configuration options: Select / Deselect

Function: Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

**Priority**

Function: The priority to be inserted as PCP bits in TAG (if any).

**Peer MEP**

Function: This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

**Unicast MAC**

Function: This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

**Time To Live**

Function: This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State configuration, as shown below;

**Link Trace State**

Transaction ID	Time To Live	Mode	Direction	Forwarded	Relay	Last MAC	Next MAC
No Transactions							

Figure 198 Link Trace State

**Transaction ID**

Describe: The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

**Time To Live**

Describe: This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

**Mode**

Describe: Indicating if is was a MEP/MIP sending this LTR.

**Direction**

Describe: Indicating if MEP/MIP sending this LTR is ingress/egress.

**Forwarded**

Describe: Indicating if MEP/MIP sending this LTR has forwarded the LTM.

**Relay**

Describe: The Relay action can be one of the following

**MAC:** The was a hit on the LT Target MAC

**FDB:** LTM is forwarded based on hit in the Filtering DB

**MFDB:** LTM is forwarded based on hit in the MIP CCM DB

**Last MAC**

Describe: The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

**Next MAC**

Describe: The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal configuration, as shown below;

**Test Signal**

Tx	Rx	DEI	Priority	Peer MEP	Rate	Size	Pattern	Sequence Number
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	1	64	All Zero	<input type="checkbox"/>

Figure 199 Test Signal

**Tx,Rx**

Configuration options: Select / Deselect

Function: Test Signal based on transmitting TST PDU can be enabled/disabled.

**DEI**

Describe: The DEI to be inserted as PCP bits in TAG (if any).

**Priority**

Function: The priority to be inserted as PCP bits in TAG (if any).

**Peer MEP**

Function: The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

**Rate**

Describe: The TST frame transmission bit rate - in Mega bits pr. second. Limit is 2.5Gbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

### Size

Default configuration:64

Describe: The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

**Switch RX frame MAX size:** The MAX frame size (all inclusive) accepted on the switch port of Bytes

**CPU RX frame MAX size:** The MAX frame size (all inclusive) possible to copy to CPU of Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX

### Pattern

Default configuration: All Zero/All One/10101010

Default configuration: All Zero

Describe: **All Zero:** Pattern will be '00000000'; **All One:** Pattern will be '11111111';

**10101010:** Pattern will be '10101010'

Test Signal State configuration, as shown below;

**Test Signal State**

TX frame count	RX frame count	RX rate	Test time	Clear
0	0	0	0	<input checked="" type="checkbox"/>

Figure 200 Test Signal State

**TX frame count**

Function: The number of transmitted TST frames since last 'Clear'.

**RX frame count**

Function: The number of received TST frames since last 'Clear'.

**RX rate**

Function: The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

**Test time**

Function: The number of seconds passed since first TST frame received after last 'Clear'.

**Clear**

Function: This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration, as shown below;

**Client Configuration**

Flow										
Domain	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾	VLAN ▾
Instance	1	0	0	0	0	0	0	0	0	0
Level	2	0	0	0	0	0	0	0	0	0
AIS prio	2 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
LCK prio	4 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾

Figure 201 Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

**Domain**

Configuration range: VLAN / EVC

Describe: The domain of the client layer flow.

Function: For a MPLS MEP, the client domain can only be EVC or LSP. For a non-MPLS

MEP, the client flow domain can not be LSP. For a non-MPLS MEP, the client flow domain can not be mixed VLAN and EVC.

**Instance**

Describe: Client layer flow instance numbers.

**Level**

Function: Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

**AIS Prio**

Function: The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

**LCK Prio**

Function: The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS configuration, as shown below;

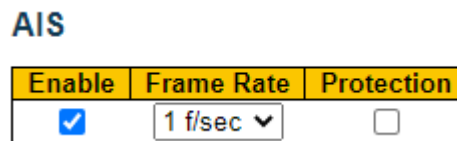


Figure 202 AIS

**Enable**

Configuration options: Select / Deselect

Function: Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

**Frame Rate**

Configuration options: 1 f / sec, 1 f / min

Function: Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

**Protection**

Configuration options: Select / Deselect

Function: Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.



LOCK configuration, as shown below;

**LOCK**

Enable	Frame Rate
<input checked="" type="checkbox"/>	1 f/sec ▼

Figure 203 LOCK

**Enable**

Configuration options: Select / Deselect

Function: Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disable.

**Frame Rate**

Configuration options: 1 f / sec, 1 f / min

Function: Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:

Click Performance Monitoring. This page allows the user to check and configure the Performance Monitor of the current MEP instance.

Performance Monitoring Data Set configuration, as shown below;

Enable
<input type="checkbox"/>

Figure 204 Performance Monitoring Data Set

**Enable**

Configuration options: Select / Deselect

Function: When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement configuration, as shown below;

**Loss Measurement**

Enable	Priority	Frame rate	Cast	Ended	FLR Interval	Loss Threshold
<input checked="" type="checkbox"/>	0	1 f/sec ▼	Multi ▼	Single ▼	5	0

Figure 205 Loss Measurement

**Enable**

Configuration options: Select / Deselect

Function: Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

**Priority**

Function: The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

**Frame rate**

Configuration options: 100 f/sec, 10 f/sec, 1 f/sec, 6 f/min, 1 f/min, 6 f/four

Function: Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

**Cast**

Configuration options: Multi / Uni

Describe: Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

**Ended**

Configuration options: Single / Dual

Describe:

- Single: Single ended Loss Measurement implemented on LMM/LMR.
- Dual: Dual ended Loss Measurement implemented on SW based CCM.

**FLR Interval**

Default configuration: 5(s)

Describe: This is the interval in seconds where the Frame Loss Ratio is calculated.

**Loss Threshold**

Function: Far end loss threshold count is incremented if a loss measurement is above this

threshold.

Loss Measurement State configuration, as shown below;

**Loss Measurement State**

Tx	Rx	Near End Loss Count	Far End Loss Count	Near End Loss Ratio	Far End Loss Ratio	Clear
0	0	0	0	0	0	<input type="checkbox"/>

Figure 206 Loss Measurement State

**Near End Loss Count**

Function: The accumulated near end frame loss count - since last 'clear'.

**Far End Loss Count**

Function: The accumulated far end frame loss count - since last 'clear'.

**Near End Loss Ratio**

Function: The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

**Far End Loss Ratio**

Function: The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

**Clear**

Function: Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability configuration, as shown below;

**Loss Measurement Availability**

Enable	Interval	FLR Threshold	Maintenance
<input type="checkbox"/>	0	0	<input type="checkbox"/>

Figure 207 Loss Measurement Availability

**Enable**

Configuration options: Select / Deselect

Function: Enable/disable of loss measurement availability.

**Interval**

Function: Availability interval - number of measurements with same availability in order to change availability state.

**FLR Threshold**

Function: Availability frame loss ratio threshold in per mille.

**Maintenance**

Configuration options: Select / Deselect

Function: Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status configuration, as shown below;

**Loss Measurement Availability State**

Near Availability Count	Far Availability Count	Near Unavailability Count	Far Unavailability Count	Near State	Far State
0	0	0	0	-	-

Figure 208 Loss Measurement Availability Status

**Near Avail Count**

Function: Near end availability count.

**Far Avail Count**

Function: Far end availability count.

**Near Unavail Count**

Function: Near end unavailability count.

**Far Unavail Count**

Function: Far end unavailability count.

**Near State**

Function: Near end availability state.

**Far State**

Function: Far end availability state.

Loss Measurement High Loss Interval configuration, as shown below;

**Loss Measurement High Loss Interval**

Enable	FLR Threshold	Consecutive Interval
<input type="checkbox"/>	0	0

Figure 209 Loss Measurement High Loss Interval

**Enable**

Configuration options: Select / Deselect

Function: Enable/disable of loss measurement high loss interval.

**FLR Threshold**

Function: High Loss Interval frame loss ratio threshold in per mille.

**Consecutive Interval:**

Function: High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval State configuration, as shown below:

**Loss Measurement High Loss Interval State**

Near Count	Far Count	Near Consecutive Count	Far Consecutive Count
0	0	0	0

Figure 210 Loss Measurement High Loss Interval State

**Near Count**

Function: Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

**Far Count**

Function: Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

**Near Consecutive Count**

Function: Near end high loss interval consecutive count.

**Far Consecutive Count**

Function: Far end high loss interval consecutive count.

Loss Measurement Signal Degrade configuration, as shown below:

**Loss Measurement Signal Degrade**

Enable	TX Minimum	FLR Threshold	Bad Threshold	Good Threshold
<input type="checkbox"/>	0	0	0	0

Figure 211 Loss Measurement Signal Degrade

**Enable**

Configuration options: Select / Deselect

Function: Enable/disable of loss measurement signal degrade.

**TX Minimum**

Function: Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

**FLR Threshold**

Function: Signal Degraded frame loss ratio threshold in per mille.

**Bad Threshold**

Function: Number of consecutive bad interval measurements required to set degrade state.

**Good Threshold**

Function: Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement configuration, as shown below;

Delay Measurement

Enable	Priority	Cast	Peer MEP	Ended	Tx Mode	Calc	Gap	Count	Unit	D2forD1	Counter Overflow Action
<input type="checkbox"/>	0	Multi	1	Single	Standardize	Flow	10	10	us	<input type="checkbox"/>	Keep

Figure 212 Delay Measurement

**Enable**

Configuration options: Select / Deselect

Function: Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

**Priority**

Function: The priority to be inserted as PCP bits in TAG (if any).

**Cast**

Configuration options: Multi / Uni

Function: Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

**Peer MEP**

Function: This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

**Ended**

Configuration options: Single/Dual

Single: Delay Measurement implemented on 1DM.

Dual: Delay Measurement implemented on DMM/DMR.

**Tx Mode**

Configuration options: Standardize / Proprietary

Describe:

**Standardize:** Y.1731 standardize way to transmit 1DM/DMR.

**Proprietary:** Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.

**Calc**

Configuration options: Flow / Round trip

Function: This is only used if the 'Way' is configured to Two-way.

**Round trip:** The frame delay calculated by the transmitting and receiving timestamps of initiators.  $\text{Frame Delay} = \text{RxTimeb} - \text{TxTimeStampf}$

**Flow:** The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes.  $\text{Frame Delay} = (\text{RxTimeb} - \text{TxTimeStampf}) - (\text{TxTimeStampb} - \text{RxTimeStampf})$

**Gap**

Function: The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

**Count**

Function: The number of last records to calculate. The range is 10 to 2000.

**Unit**

Configuration options: us / ns

Function: The time resolution.

**D2forD1**

Configuration options: Select / Deselect

Function: Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

**Counter Overflow Action**

Configuration options: Keep / Reset

Function: The action to counter when overflow happens.

Delay Measurement State configuration, as shown below:

Delay Measurement State														
	Tx	Rx	Rx Timeout	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way														
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	0	<input type="checkbox"/>

Figure 213 Delay Measurement State

**Tx**

Function: The accumulated transmit count - since last 'clear'.

**Rx**

Function: The accumulated receive count - since last 'clear'.

**Rx Timeout**

Function: The accumulated receive timeout count for two-way only - since last 'clear'.

**Rx Error**

Function: The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

**Av Delay Tot**

Function: The average total delay - since last 'clear'.

**Av Delay last N**

Function: The average delay of the last n packets - since last 'clear'.

**Delay Min.**

Function: The minimum delay - since last 'clear'.

**Delay Max**

Function: The maximum delay - since last 'clear'.

**Av Delay-Var Tot**

Function: The average total delay variation - since last 'clear'.

**Av Delay-Var last N**

Function: The average delay variation of the last n packets - since last 'clear'.

**Delay-Var Min**

Function: The minimum delay variation - since last 'clear'.

**Delay-Var Max**

Function: The maximum delay variation - since last 'clear'.

**Overflow**

Function: The number of counter overflow - since last 'clear'.

**Clear**

Function: Set of this check and save will clear the accumulated counters.



### Far-end-to-near-end one-way delay

Function: The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 enabled. 3. DMR received with D2forD1 enabled.

### Near-end-to-far-end one-way delay

Function: The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with D2forD1 enabled.

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Delay Measurement Bins configuration, as shown below;

Delay Measurement State														
	Tx	Rx	Rx Timeout	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way														
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 214 Delay Measurement Bins

### Measurement Bins for FD

Function: Configurable number of Frame Delay Measurement Bins per Measurement Interval.

- The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
- The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
- The default number of FD Measurement Bins per Measurement Interval supported is 3.

### Measurement Bins for IFDV

Function: Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.

- The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
- The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
- The default number of FD Measurement Bins per Measurement Interval supported is 2.

### Measurement Threshold

Function: Configurable the Measurement Threshold for each Measurement Bin.

- The unit for a measurement threshold is in microseconds (us).
- The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD configuration, as shown below;

**Delay Measurement Bins for FD**

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

Figure 215 Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Table 7 Delay Measurement Bins for FD

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV configuration, as shown below;

**Delay Measurement Bins for IFDV**

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

Figure 216 Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Table 8 Delay Measurement Bins for IFDV

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

5.TLV Configuration, as shown below.

### TLV Configuration

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

Figure 217 TLV Configuration

#### OUI First

Function: The transmitted first value in the OS TLV OUI field.

#### OUI Second

Function: The transmitted second value in the OS TLV OUI field.

#### OUI Third

Function: The transmitted third value in the OS TLV OUI field.

#### Sub-Type

Function: The transmitted value in the OS TLV Sub-Type field.

#### Value

Function: The transmitted value in the OS TLV Value field.

6.TLV Status Configuration, as shown below.

#### TLV Status

Peer MEP ID	CC Organization Specific						CC Port Status		CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX	Value	Last RX

Figure 218 TLV Status

#### CC Organization Specific-OUI First

Describe: The last received first value in the OUI field.

#### CC Organization Specific-OUI Second

Describe: The last received second value in the OS TLV OUI field.

**CC Organization Specific-OUI Third**

Describe: The last received third value in the OS TLV OUI field.

**CC Organization Specific-Sub-Type**

Describe: The last received value in the OS TLV Sub-Type field.

**CC Organization Specific-Value**

Describe: The last received value in the OS TLV Value field.

**CC Organization Specific-Last RX**

Describe: OS TLV was received in the last received CCM PDU.

**CC Port Status-Value**

Describe: The last received value in the PS TLV Value field.

**CC Port Status-Last RX**

Describe: PS TLV was received in the last received CCM PDU.

**CC Interface Status-Value**

Describe: The last received value in the IS TLV Value field.

**CC Interface Status-Last RX**

Describe: IS TLV was received in the last received CCM PDU.

7.Link State Tracking configuration, as shown below.

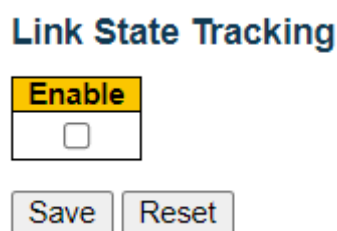


Figure 219 Link State Tracking

**Enable**

Configuration options: Select / Deselect

Function: When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

## 17 ERPS Principle

### 17.1 Introduction

In the 2-layer networks, STP protocol is generally used for network reliability, STP protocol is a standard ring network protection protocol developed by IEEE and is widely used, but practical applications is limited by network size and the convergence time is affected by the network topology. The general convergence time of STP is second level and is longer with large network diameter. Although adopting RSTP/MSTP can reduce the convergence time, it still cannot meet the requirements for businesses with high quality of service requirements such as 3G/NGN voice.

To reduce the convergence time and eliminate the effect of network size, the ERPS protocol arises. The ERPS is a link layer protocol specifically applied to Ethernet rings that is able to prevent broadcast storm caused by data rings; When a link on the Ethernet ring is disconnected, the backup link is quickly enabled to restore communication between the nodes on the ring network. Compared to the STP protocol, the ERPS protocol has a fast topological convergence rate (below 50ms) and the convergence time is independent of the number of nodes on the ring network.

#### 17.1.1 Basic Concept

Figure 259220 is the basic networking model of ERPS, and this section introduces some of the basic concepts in ERPS.

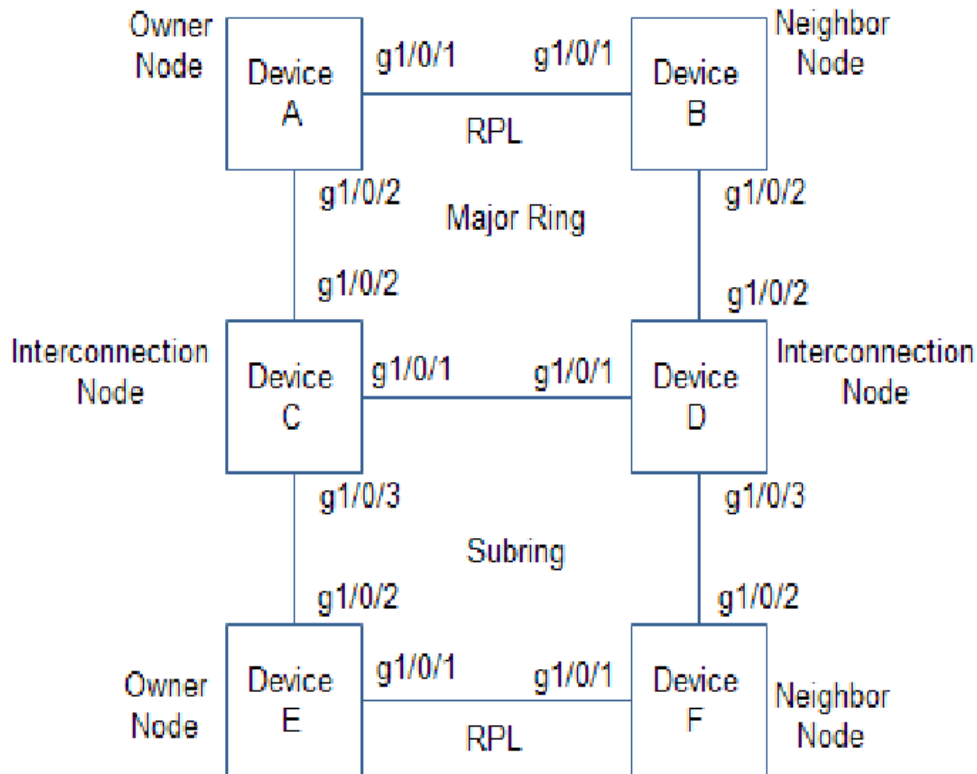


Figure 220 ERPS networking schematic diagram

1.ERPS Ring.

A ring Ethernet network topology is called an ERPS ring. The ERPS ring is divided into the major ring and the subring, and by default, the ERPS ring is major ring, the ERPS ring can be manually configured as a subring. An ERPS ring can be composed of a single major ring or multiple ring networks, there can be multiple major rings and multiple subrings in multiple ring networks. As shown in Figure 25920, The closed loop enclosed by the four nodes Device A, Device B, Device C, Device D is the major ring. The subring is composed by the three links of Device C and Device E, Device E and Device F and Device F and Device D, and is an unclosed ring.

The ERPS ring consists of many nodes. Some nodes use RPL (Ring Protection Link) to protect the ring network, and prevent loop to be generated. As shown in Figure 25920, the link between Device A and Device B, Device E and Device F is RPL.

2.Node Role

Each device on the ERPS ring is called a node. The node role is determined by the user's configuration and is divided into the following:

**Owner node:** Owner node, responsible for blocking and opening the port located in RPL on the node, preventing loop, and thus switching the link.

**Neighbor node:** Neighbor node, the node on the RPL which is connected with the Owner node, cooperate with the Owner node block and open the port on the RPL on the node to switch link.

**Interconnection node:** Interconnection node, for nodes connecting multiple rings in the multi-loop model, the interconnected node belongs to subring, and the major ring has no interconnected node. In the protocol message delivery mode of the link between the subloop interconnection nodes, the protocol message of the subring is terminated at the interconnection node, and the data message is not terminated.

**Normal node:** Normal node, all nodes except the three nodes described above are normal nodes. The normal node is responsible for receiving and forwarding the protocol and data messages in the link.

On the major ring, Device A is Owner node, Device B is Neighbor node, On the subring, Device E is Owner node, Device F is Neighbor node. Device C and Device D are Normal node.

### 3.Port Type

The ERPS ring member port types are determined by the user configuration and are divided into three types:

**RPL port:** Port at both ends of the PRL.

**Interconnection port:** The interconnection node port is the port responsible for connecting the subring to the major ring.

**Normal port:** Normal port is default port type and can receive and forward protocol and data messages in the link without special functions.

As shown in Figure 25920, the port Gigabit Ethernet 1/0/1 on the Device A, Device B, Device E and Device F is RPL port. the port Gigabit Ethernet 1/0/3 on the Device C and Device D is Interconnection port. the other ports are Normal port.

### 17.1.2 Protocol Message

R-APS (Ring Automatic Protection Switching) message is the protocol message of the ERPS. The protocol provides the setting function of the R-APS message level. The node does not handle a R-APS message level larger than itself. The node R-APS message level with the same instance on the same ring must be the same.

ERPS protocol message type and role are shown in Table 9.

Message type	Description
(NR, RB) (No Request, RPL Block) message	Sent by the Owner node in the Idle state, notifying the other nodes that the RPL port is blocked. After other nodes receive (NR, RB) messages, they release their own fault-free ports and update their respective MAC address table items. When the link is stable in the Idle state, the Owner node periodically sends the (NR, RB) messages
NR (No Request, Link recovery) message	When the link fault recovery, it is sent by the node of the recovery port, the WTR timer starts after Owner receives the NR message, and stops sending the NR message after receiving the (NR, RB) message at the node of the recovery port
SF (Signal Fail) message	When the link fails to send and receive signals, it is sent by the node where the fault port is located, and after the Owner and Neighbor nodes receive the SF message, release the respective RPL ports. Before the fault is eliminated, the SF message is periodically sent at the node of the fault port
MS (Manual Switch) message	Send by the node with MS mode, the port with MS mode is blocked, other nodes receive MS messages after releasing their fault-free port, update their respective



Message type	Description
	MAC address table items. Link in MS state, MS message is sent periodically
FS (Forced Switch) message	Send by the node with FS mode, the port with FS mode is blocked, other nodes receive FS messages after releasing their fault-free port, update their respective MAC address table items. Link in FS state, FS message is sent periodically
Flush message	If the subring topology changes, the interconnection node sends a flush message as a broadcast to notify the major ring to refresh the MAC address table item

### 17.1.3 ERPS Protocol State

The ERPS defines the following 6 states:

**Init state:** It is the Init state when ring port is incomplete (the number of ports of non-interconnected nodes is less than 2 or the number of ports of interconnected nodes is less than 1).

**Idle state:** After the ring initializes to the Idle state, when the Owner node enters the idle state, the other nodes then enter the Idle state. In which, the RPL port of Owner node and Neighbor node is blocked, that is RPL does not work; The Owner node sends the (NR, RB) message regularly.

**Protection state:** When a link of the ring network fails, after ring protection switches, the ring finally stabilized to the state. RPL port of the Owner and Neighbor node opens, that is RPL opens to ensure the entire ring network still work. When a node in the link enters the protection state, the other nodes then enter the protection state.

**MS state:** The traffic forwarding path can be manually switched in the MS state. When a node in the link performs MS operation, the other nodes then enter the MS state.

**FS state:** The traffic forwarding path can be forced to switch in the FS state. When a node in the link performs FS operation, the other nodes then enter the FS state.

**Pending state:** The pending state is an unstable state, which is a transition state of each state during switches.

The ring is Idle state when normal; The ring is Protection state after link fail.

#### 17.1.4 ERPS Timer

The ERPS timer is divided into three types:

**Hold-off timer:** The timer starts when the port detects the link fault, delaying the speed of fault reporting. When the link fails, wait for Hold-off to timeout and report if the failure still exists. This provides the opportunity to repair the link to the service layer, and avoid the unnecessary failure reporting. The timing of this timer affects the speed of link fault reporting and the switching performance of the link when the fault occurs.

**Guard timer:** The timer starts when the port detects a link recovery to prevent unnecessary shocks to the network from residual original R-APS messages caused by an online forwarding delay. The interface no longer processes all R-APS messages until this timer timeout. This timer has an impact on link recovery performance during multi-point failures.

**WTR timer:** In switch back mode, the timer starts when the Owner node receives the NR message in the Protection state to prevent frequent network shocks caused by the intermittent fault link on the network. before this timer timeout, RPL remains forward and the failure recovery point is temporarily blocked, if the Owner node receives a FS message that there is a fault link in the ring network, the timer is directly closed and RPL remains forward.

#### 17.1.5 ERPS Operating Mechanism

The ERPS determines the state of the link by the notified messages and processes them accordingly. The control message types of ERPS are mainly SF and NR. If link signal failure is detected, SF message is sent; if link recovery is detected, NR message is sent. If link state changes are detected, messages are sent continuously, and subsequent messages are sent every 5 seconds.

The link down alarm mechanism is shown in When the node in the link finds itself any port down of the ERPS ring, it blocks the fault port and immediately sends a SF message to notify the other nodes on the link has failed. Other nodes open the non-fault blocking port

after receiving this message and refresh the MAC address table item.

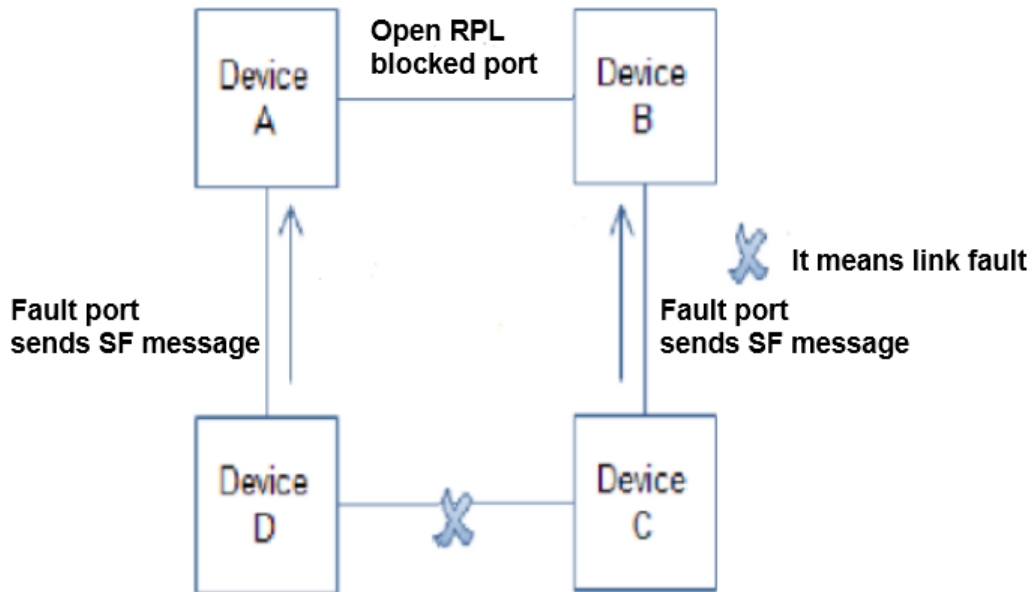


Figure 221 Link down alarm mechanism

The link recovery mechanism is shown in Figure 221. When the fault link recovery, the port in the previous fault state is blocked first, the Guard timer is started and the NR message is sent to notify the Owner node that the fault link has recovered.

After the Owner node receives the NR message, it starts the WTR timer. If the timer does not receive the SF message before the timer timeout, the Owner node blocks the RPL port and sends out the periodic (NR, RB) message; fault recovery node opens the temporarily blocked recovery port after receiving the (NR, RB) message; Neighbor node blocks the RPL port after receiving the (NR, RB) message, and link recovery.

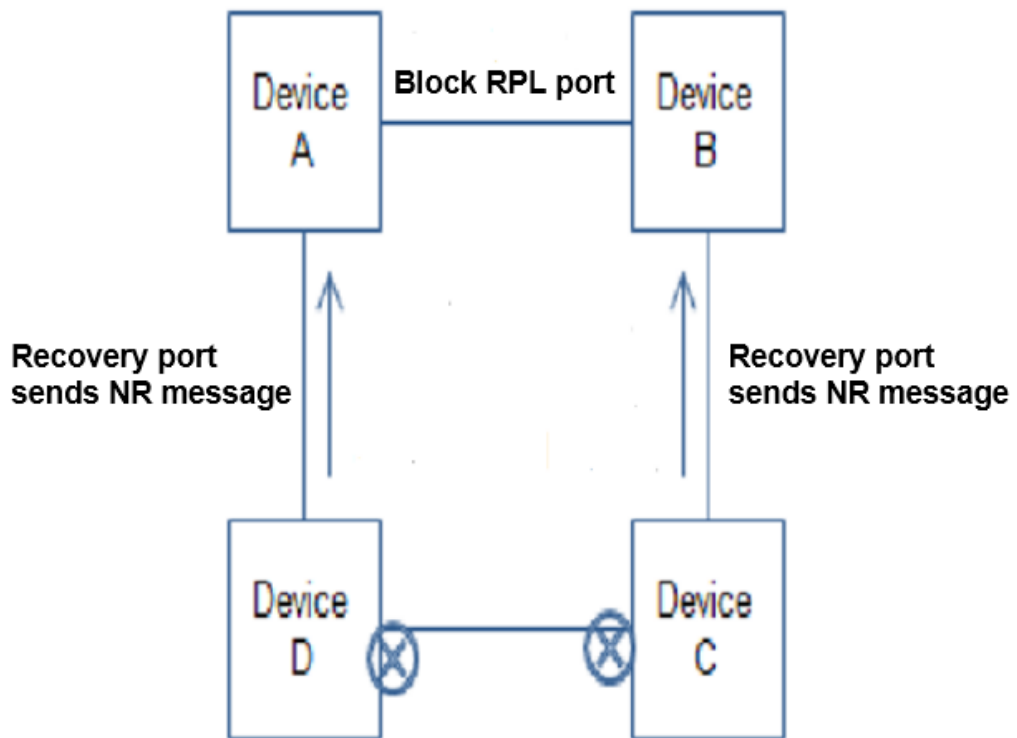


Figure 222 Link recovery mechanism

### 17.1.6 ERPS Configuration Networking

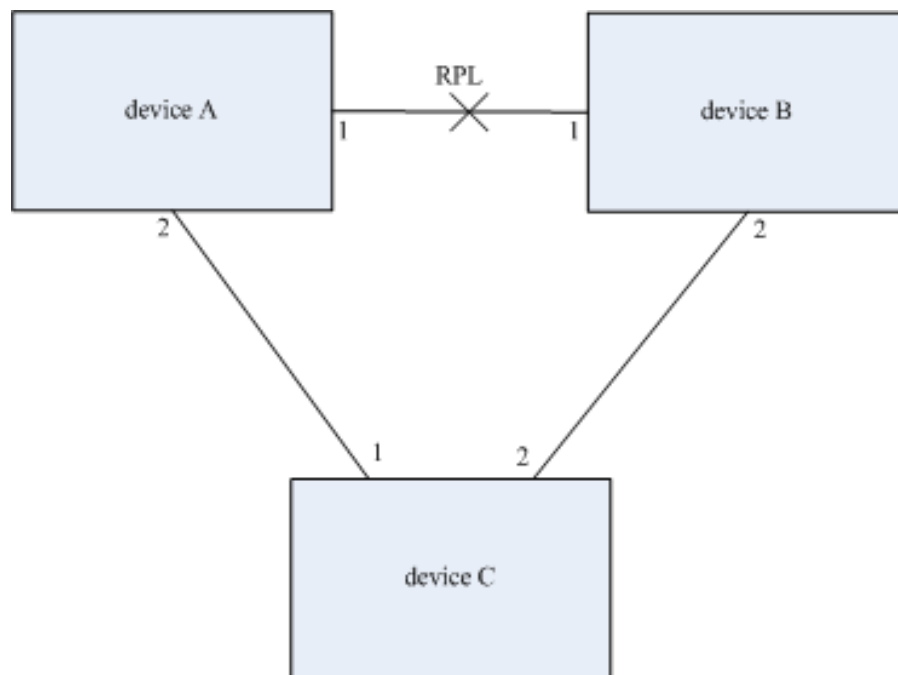


Figure 223 Schematic diagram of single ring

## 17.2 Web Configuration

1.Instance Data configuration, as shown below.

ERPS Configuration 1							
Instance Data							
ERPS ID	Port 0	Port 1	Port 0 SF MEP	Port 1 SF MEP	Port 0 APS MEP	Port 1 APS MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

Figure 224 Ethernet Ring Protection Switching

### ERPS ID

Configuration range: Integer value between 1 and 64

Function: The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page.

### Port 0

Function: Create ring port 0.

### Port 1

Function: Create ring port 1



**Caution:**

The connection sub-ring has only one ring port, port 0

### Port 0 SF MEP

Default configuration: 1

Function: The Port 0 Signal Fail reporting MEP.

### Port 1 SF MEP

Default configuration: 1

Function: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

### Port 0 APS MEP

Default configuration: 1

Function: The Port 0 APS PDU handling MEP.

**Port 1 APS MEP**

Default configuration: 1

Function: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

**Ring Type**

Configuration options: Major / sub

Default configuration: Major

Function: Type of Protecting ring. It can be either major ring or sub-ring.

**Interconnected Node**

Configuration options: Yes / No

Function: Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

**Virtual Channel**

Configuration options: Yes / No

Function: Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

**Major Ring ID**

Function: Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

**Alarm**

Function: There is an active alarm on the ERPS.

2.Instance Configuration, as shown below.

**Instance Configuration**


Configured	Guard Time	WTR Time	Hold Off Time	Version	Revertive	VLAN config
	500	1min ▾	0	v2 ▾	<input checked="" type="checkbox"/>	<a href="#">VLAN Config</a>

Figure 225 Instance Configuration

**Configured**

Configuration options: Red / Green

Function:

**Red:** This ERPS is only created and has not yet been configured - is not active.

**Green:** This ERPS is configured - is active.

**Guard Time**

Default configuration: 500

Function: Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages.

The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms

**WTR Time**

Configuration range: 1min~12min

Default configuration: 1min

Function: The Wait To Restore timing value to be used in revertive switching.

The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

**Hold Off Time**

Configuration range: 0s~10s

Function: The timing value to be used to make persistent check on Signal Fail before switching.

The range of the hold off timer is 0 to 10 seconds in steps of 100 ms

**Version**

Configuration options: V1 / V2

Function: ERPS Protocol Version - V1 or V2

**Revertive**

Configuration options: Select / Deselect

Function: In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.

In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

**VLAN config**

Function: VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group., as shown below.

**ERPS VLAN Configuration 1**

Delete	VLAN ID
Delete	1
Delete	2
Delete	0
Delete	0

Figure 226 VLAN configuration

**Delete**

Function: To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.

**VLAN ID**

Function: Indicates the ID of this particular VLAN.

**Add New Entry**

Configuration range: 1~4095

Function: Click to "Add New Entry" add a new VLAN ID.

The VLAN is enabled on the selected switch unit when you click on "Save". A VLAN without any port members will be deleted when you click "Save".

The Delete button can be used to undo the addition of new VLANs.

3.RPL Configuration, as shown below.



### RPL Configuration

RPL Role	RPL Port	Clear
None ▾	None ▾	<input type="checkbox"/>

Figure 227 RPL Configuration

#### RPL Role

Configuration options: None / RPL\_Owner / RPL\_Neighbour

Default configuration: None

Function: It can be either RPL owner or RPL Neighbor.

#### RPL Port

Configuration options: None / Port0 / Port1

Default configuration: None

Function: This allows to select the east port or west port as the RPL block.

#### Clear

Configuration options: Select / Deselect

Function: If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

4.Instance Command configuration, as shown below.

### Instance Command

Command	Port
None ▾	None ▾

Figure 228 Instance Command

#### Command

Configuration options: None / Manual Switch / Forced Switch / Clear

Default configuration: Clear

Function: Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

**Forced Switch:** Forced Switch command forces a block on the ring port where the command is issued.

**Manual Switch:** In the absence of a failure or FS, Manual Switch command forces a block

on the ring port where the command is issued.

**Clear:** The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

**Port**

Configuration options: None / Port0 / Port1

Default configuration: None

Function: Port selection - Port0 or Port1 of the protection Group on which the command is applied.

5.Instance State configuration, as shown below.

Instance State

Protection State	Port 0	Port 1	Transmit APS	Port 0 Receive APS	Port 1 Receive APS	WTR Remaining	RPL Un-blocked	No APS Received	Port 0 Block Status	Port 1 Block Status	FOP Alarm
Pending	OK	OK				0			Blocked	Blocked	

Save Reset

Figure 229 Instance State

**Protection State**

Describe: ERPS state according to State Transition Tables in G.8032.

**Port 0**

Describe:

**OK:** State of East port is ok

**SF:** State of East port is Signal Fail

**Port 1**

Describe:

**OK:** State of West port is ok

**SF:** State of West port is Signal Fail

**Transmit APS**

Describe: The transmitted APS according to State Transition Tables in G.8032.

**Port 0 Receive APS**

Describe: The received APS on Port 0 according to State Transition Tables in G.8032.

**Port 1 Receive APS**

Describe: The received APS on Port 1 according to State Transition Tables in G.8032.

**WTR Remaining**

Describe: Remaining WTR timeout in milliseconds.

**RPL Un-blocked**

Function: APS is received on the working flow.

**No APS Received**

Function: RAPS PDU is not received from the other end.

**Port 0 Block Status**

Function: Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

**Port 1 Block Status**

Function: Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

**FOP Alarm**

Function: Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

## 18 MAC Address Configuration

### 18.1 Introduction

When forwarding a packet, the switch searches for the forwarding port in the MAC address table based on the destination MAC address of the packet.

A MAC address can be either static or dynamic.

A static MAC address is configured by a user. It has the highest priority (not overridden by dynamic MAC addresses) and is permanently valid.

Dynamic MAC addresses are learned by the switch in data forwarding. They are valid only for a certain period. The switch periodically updates its MAC address table. When receiving a data frame to be forwarded, the switch learns the source MAC address of the frame, establishes a mapping with the receiving port, and queries the forwarding port in the MAC address table based on the destination MAC address of the frame. If a match is found, the switch forwards the data frame from the corresponding port. If no match is found, the switch broadcasts the frame in its broadcast domain.

Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, the switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC addresses do not involve the concept of aging time.

### 18.2 Web Configuration

1. Configure MAC address aging time, as shown in as shown below;

#### Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	300 seconds

Figure 230 MAC Address Aging Time Configuration

#### Disable Automatic Aging

Options: Enable/Disable

Default: Default

Function: Enable/Disable MAC address aging. Enable indicates you need to configure an aging time. Disable indicates the address dynamically learned does not age with time.

**Aging Time**

Range: 10~1000000s

Default: 300s

Function: Set the aging time for the dynamic MAC address entry.

2. Configure dynamic MAC address, as shown in as shown below;

**MAC Table Learning**

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 231 Configure Dynamic MAC Address

**Port Members**

Options: Auto/Disable

Default: Auto

Function: Whether a port dynamically learns an MAC address table. Auto indicates a port can dynamically learn the MAC address table. Disable indicates that a port is forbidden to dynamically learn the MAC address table. Secure: Enable port secure mac learning. Only static MAC entries are learned, all other frames are dropped.

3. Configure static MAC address, as shown in as shown below; .

**Static MAC Table Configuration**

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	00-12-34-56-78-90	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	1	01-01-01-01-01-01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	00-11-22-33-44-55	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Static Entry

Submit    Reset

Figure 232 Configure Static MAC Address

**VLAN ID**

Options: all created VLAN IDs

Default: VLAN 1

Function: Configuration the VLAN ID of static MAC address.

**MAC address**

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure MAC address. For unicast MAC address, the lowest bit in the first byte is 0. For multicast MAC address, the lowest bit in the first byte is 1.

**Port Members**

Function: Select ports to forward the packets with this destination MAC address.

Click <Add New Static Entry> to configure static MAC address entry. A maximum of 64 static MAC address entries are supported.

4. View MAC address table, as shown in as shown below;

Type	VLAN	MAC Address	Port Members													
			CPU	1	2	3	4	5	6	7	8	9	10	11	12	
Static	1	00-01-C1-00-00-00	✓													
Dynamic	1	00-01-C1-00-00-02					✓									
Static	1	00-12-34-56-78-90			✓											
Dynamic	1	00-1E-CD-11-01-B1	✓													
Static	1	01-01-01-01-01-01	✓	✓	✓	✓	✓									
Static	2	00-11-22-33-44-55													✓	
Static	2	01-01-01-01-01-02				✓	✓	✓								

Figure 233 View MAC address table

## 19 VLAN

### 19.1 VLAN Configuration

#### 19.1.1 Introduction

One LAN can be divided into multiple logical Virtual Local Area Networks (VLANs). A device can only communicate with the devices on the same VLAN. As a result, broadcast packets are restricted to a VLAN, optimizing LAN security.

VLAN partition is not restricted by physical location. Each VLAN is regarded as a logical network. If a host in one VLAN needs to send data packets to a host in another VLAN, a router or layer-3 device must be involved.

#### 19.1.2 Principle

To enable network devices to distinguish packets from different VLANs, fields for identifying VLANs need to be added to packets. At present, the most commonly used protocol for VLAN identification is IEEE802.1Q. Table 10 shows the structure of an 802.1Q frame.

Table 10 802.1Q Frame Structure

DA	SA	802.1Q header				Length/type	Data	FCS
		TPID	PRI	CFI	VID			

A 4-byte 802.1Q header, as the VLAN tag, is added to the traditional Ethernet data frame.

TPID: 16 bits. It is used to identify a data frame carrying a VLAN tag. The value is 0x8100.

The value of TPID specified in the 802.1Q protocol is 0x8100.

PRI: three bits, identifying the 802.1p priority of a packet.

CFI: 1 bit, specifies whether an MAC address is encapsulated in the standard format in different transmission media. The value 0 indicates that an MAC address is encapsulated in the standard format and the value 1 indicates that an MAC address is encapsulated in non-standard format.

VID: 12 bits, indicating the VLAN number. The value ranges from 1 to 4093. 0, 4094, and

---

4095 are reserved values.

---

**Note:**

- VLAN 1 is the default VLAN and cannot be manually created and deleted.
  - Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and deleted.
- 

The packet containing 802.1Q header is a tagged packet; the one without 802.1Q header is an untagged packet. All packets carry an 802.1Q tag in the switch.

### 19.1.3 Port-based VLAN

VLAN partition can be either port-based or MAC address-based. This series switches support port-based VLAN partition. VLAN members can be defined based on switch ports. After a port is added to a specified VLAN, the port can forward the packets with the tag for the VLAN.

#### 1. Port Mode

Ports fall into two types according to how they handle VLAN tags when they sends packets.

**Access:** In access mode, the port can be added to only one VLAN. By default, all switch ports are access ports and belong to VLAN1. Packets forwarded by an access port do not have VLAN tags. Access ports are usually used to connect to terminals that do not support 802.1Q.

**Trunk:** In trunk mode, the port can be added to many VLAN. Trunk port receives tag and untag packets. When sending PVID packets, the Trunk port can be set whether to carry the tag. It carries the tag when sending other packets. Trunk ports are usually used to connect network transmission devices.

**Hybrid:** In hybrid mode, the port can be added to many VLAN. You can set the type of packets to be received by a Hybrid port and whether the tag is carried when the Hybrid port sends packets. The Hybrid port can be used to connect network devices and user devices. The difference between a Hybrid port and a Trunk port is as follows: The Hybrid port does not carry the tag when sending packets from multiple VLANs and the Trunk port does not carry the tag only when sending PVID packets.



## 2. PVID

Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID. The default PVID of all ports is 1.



**Caution:**

- When configuring the PVID of a port, select one of the VLAN IDs allowed through the port; otherwise, the port may fail to forward packets.
- When the PVID tag is added to untagged packets, you can refer to PCP and DEI settings in Figure 62 for the default PRI and CFI values of a port.

Table 11 shows how the switch processes received and forwarded packets according to the port mode, and PVID.

Table 11 Different Processing Modes for Packets

Processing Received Packets		Processing Packets to Be Forwarded	
Untagged packets	Tagged packets	Port Mode	Packet Processing
Add PVID tags to packets: ➤ If the PVID is in the list of VLANs allowed through, accept the packet. ➤ If the PVID is not in the list of VLANs allowed through, discard the packet.	➤ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the packet. ➤ If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet.	Access	Forward the packet after removing the tag.
		Trunk	Forward the packet according to the “Egress Tagging” configuration: ➤ Untag Port VLAN: If the VLAN ID in a packet is the same as PVID, and in the list of VLANs allowed through, forward the packet after removing the tag. If the VLAN ID in a packet is different from PVID, and in the list of VLANs allowed through, keep the tag and forward the packet. ➤ Tag All: If the VLAN ID in a packet is in the list of VLANs allowed through, keep the tag and forward the packet.

		Hybrid	<p>Forward the packet according to the “Egress Tagging” configuration:</p> <ul style="list-style-type: none"> <li>➤ Untag Port VLAN: the same as above.</li> <li>➤ Tag All: the same as above.</li> <li>➤ Untag All: If the VLAN ID in a packet is in the list of VLANs allowed through, forward the packet after removing the tag.</li> </ul>
--	--	--------	--

### 19.1.4 Web Configuration

1. Created VLANs configuration, as shown in Figure 234.

#### Global VLAN Configuration

Allowed Access VLANs	1,2,100,200
Ethertype for C-Tag	88A8

Figure 234 Created VLANs configuration

#### Allowed Access VLANs

Options: 1~4093

Default: 1

Function: Configure allowed VLANs for access port. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

#### Ethertype for C-Tag

Options: 600-FFFF

Default: 88A8

Function: When the message carries double tags, the TPID value of the outer tag changes with the configuration.

2. Configure port VLAN, as shown in Figure 235.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	2	<>	<input checked="" type="checkbox"/>	<>	<>	2	1
1	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	2	1
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	2	
3	Access	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100	
4	Access	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100	
5	Access	200	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	200	
6	Access	200	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	200	
7	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1,2,100,200	
8	Hybrid	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-3	2
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Submit Reset

Figure 235 Configure Port VLAN

**Mode**

Options: Access/Trunk/Hybrid

Default: Access

Function: Select the mode for the specified port. Each port supports only one mode.

**Port VLAN (PVID)**

Range: 1~4094

Default: 1

Function: Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID.



**Caution:**

- The PVID of the Access port should be selected from the list of VLANs allowed by the Access port, see
- Configuration options: 1 ~ 4093
- Default configuration: 1
- Function: Parameter setting of "Allowed VLAN" in configuration;
- The PVID of the Trunk port / Hybrid port should be selected from the list of VLANs allowed by the port, see the "Allow VLAN" parameter configuration below.

**Port Type**

**C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a

C-tag.

**S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

**S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

### Ingress Filtering

Options: Enable/Disable

Default: Disable

Function: Enable/Disable ingress filtering function of the hybrid port. The ingress filtering is enabled forcibly for access port and trunk port, you cannot configure the parameter. Enable: If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet. Disable: If the VLAN ID in a packet is not in the list of VLANs allowed through, accept the packet and forward to MAC engine.

### Ingress Acceptance

Options: Tagged and Untagged/ Tagged Only/ Untagged Only

Default: Tagged and Untagged

Function: Set the type of packets to be received by a Hybrid port. It is forcibly set to Tagged and Untagged for the Access port and Trunk port and cannot be modified. The value Tagged and Untagged indicates that the Hybrid port can receive tagged packets and untagged packets; the value Tagged Only indicates that the Hybrid port receives only tagged packets and discards untagged packets; the value Untagged Only indicates that the Hybrid port receives only untagged packets and discards tagged packets.

### Egress Tagging

Options: Untag Port VLAN/ Unatg All/ Tag All

Default: Untag Port VLAN

Function: Set the packet transmission processing for the Trunk port or Hybrid port. The

egress tagging is configured to Unatg All forcibly for access port, you cannot configure the parameter. Untag Port VLAN: If the VLAN ID in a packet is the same as PVID, and in the list of VLANs allowed through, forward the packet after removing the tag. If the VLAN ID in a packet is different from PVID, and in the list of VLANs allowed through, keep the tag and forward the packet. Tag All: If the VLAN ID in a packet is in the list of VLANs allowed through, keep the tag and forward the packet. Untag All: If the VLAN ID in a packet is in the list of VLANs allowed through, forward the packet after removing the tag.

### **Allowed VLANs**

Range: 1-4094

Range: 1-4094

Function: Configure allowed VLANs for trunk/hybrid port. When the Access port allows only one VLAN, the value of this parameter is consistent with the value of Port VLAN and it cannot be changed. When this parameter is set to multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

### **Forbidden VLANs**

Range: 1-4094

Function: Configure forbidden VLANs for a port. After this parameter is set for a port, the port will never become a member port of the VLAN, including the dynamically registered VLAN through GVRP. When this parameter is set to multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

3. View all created VLANs and port members, as shown in Figure 236.

### VLAN Membership Status for Combined users

Start from VLAN  with  entries per page.

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
100	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
200	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 236 View All Created VLANs and Port Members

indicates that a port is a member port of the current VLAN;  indicates that the current VLAN belongs to forbidden VLANs of a port.

1 to 99 VLAN entries can be displayed on each page and 20 VLAN entries are displayed by default. You can specify the first VLAN entry ID on the first page.

4. View port VLAN configuration, as shown in Figure 237.

### VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	2	Untag All		No
2	C-Port	<input checked="" type="checkbox"/>	All	2	Untag All		No
3	C-Port	<input checked="" type="checkbox"/>	All	100	Untag All		No
4	C-Port	<input checked="" type="checkbox"/>	All	100	Untag All		No
5	C-Port	<input checked="" type="checkbox"/>	All	200	Untag All		No
6	C-Port	<input checked="" type="checkbox"/>	All	200	Untag All		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input type="checkbox"/>	All	1	Untag PVID		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No

Figure 237 View Port VLAN Configuration

## 19.1.5 Typical Configuration Example

As shown in Figure 238, the entire LAN is divided into 3 VLANs: VLAN2, VLAN100, and VLAN200. It is required that the devices in the same VLAN can communicate with each other, but different VLANs are isolated. The terminal PCs cannot distinguish tagged packets, so the ports connecting Switch A and Switch B with PCs are set to access port. VLAN2, VLAN100, and VLAN200 packets need to be transmitted between Switch A and Switch B, so

the ports connecting Switch A and Switch B should be set to trunk port, permitting the packets of VLAN 2, VLAN 100, and VLAN 200 to pass through. Table 12 shows specific configuration.

Table 12 VLAN Configuration

VLAN	Configuration
VLAN2	Set port 1 and port 2 of Switch A and B to access ports, and port 7 to trunk port.
VLAN100	Set port 3 and port 4 of Switch A and B to access ports, and port 7 to trunk port.
VLAN200	Set port 5 and port 6 of Switch A and B to access ports, and port 7 to trunk port.

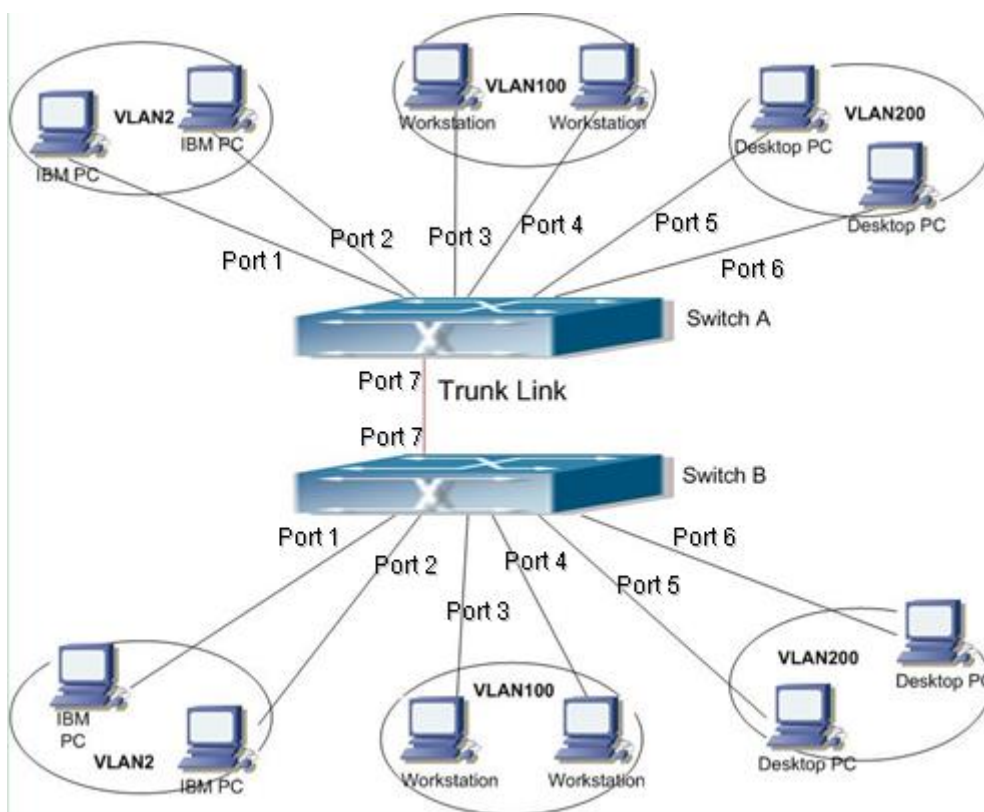


Figure 238 VLAN Application

**Configurations on Switch A and Switch B:**

1. Configure allowed access VLANs to 1, 2, 100, 200, as shown in Figure 234.
2. Configure ports 1, 2 as access ports, port VLAN as 2. Configure ports 3, 4 as access ports, port VLAN as 100. Configure ports 5, 6 as access ports, port VLAN as 200. Configure port 7 as trunk port, port VLAN as 1, allowed VLANs as 1, 2, 100, 200, as shown in Figure 235.
3. Keep all the other parameters default.

## 19.2 PVLAN Configuration

### 19.2.1 Introduction

PVLAN (Private VLAN) uses two layers isolation technologies to realize the complex port traffic isolation function, achieving network security and broadcast domain isolation.

The upper VLAN is a shared domain VLAN in which ports are uplink ports. The lower VLANs are isolation domains in which ports are downlink ports. Downlink ports can be assigned to different isolation domains and they can communicate with uplink port at the same time. Isolation domains cannot communicate to each other.

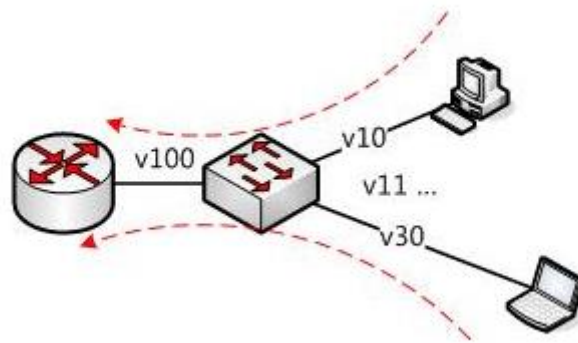


Figure 239 PVLAN Application

As shown in Figure 239, the shared domain is VLAN100 and the isolation domains are VLAN 10 and VLAN 30; the devices in the isolation domains can communicate with the device in the share domain, such as VLAN 10 can communicate with VLAN 100; VLAN 30 can also communicate with VLAN 100, but the devices in different isolation domains cannot communicate with each other, such as VLAN 10 cannot communicate with VLAN 30.

### 19.2.2 Explanation

PVLAN function can be implemented through special configuration on ports.

- The PVID of uplink ports are the same as shares domain VLAN ID; the PVID of downlink ports are the same as their own isolation domain VLAN ID.
- The uplink ports are set to hybrid and are assigned to the shares domain VLAN and all isolation domains; the downlink ports are set to hybrid and are assigned to the shared



domain VLAN and own isolation domain.

- The packets sent by PVLAN member ports are Untag.

### 19.2.3 Typical Configuration Example

Figure 240 shows PVLAN application. VLAN300 is a shared domain and port 1 and port 2 are uplink ports; VLAN100 and VLAN200 are isolation domains and ports 3, 4, 5, and 6 are downlink ports.

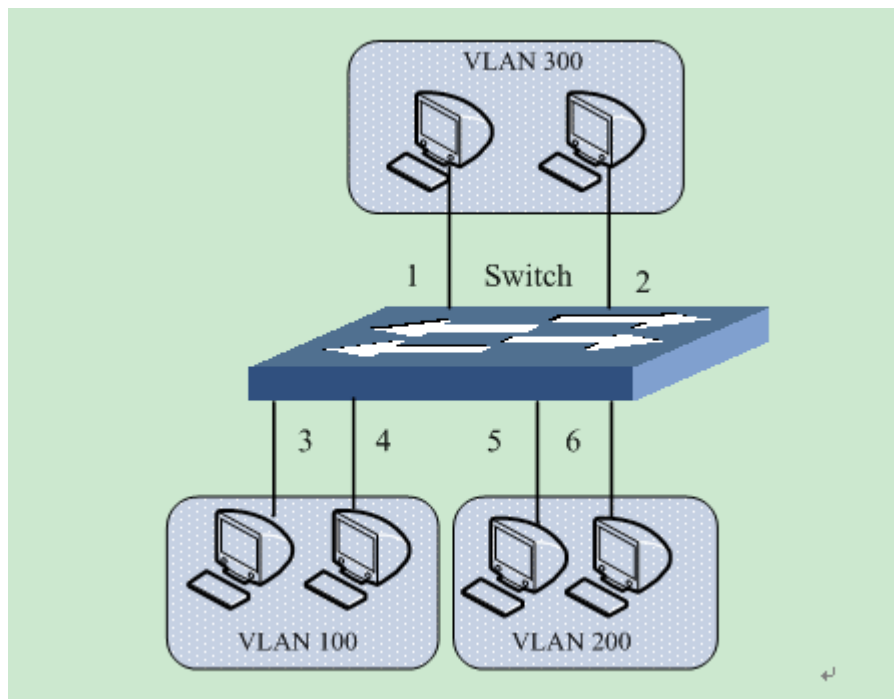


Figure 240 PVLAN Configuration Example

Switch configuration:

1. Configure ports 1, 2 to hybrid ports, port VLAN to 300, egress tagging to Untag All, allowed VLANs to 100,200,300.
2. Configure ports 3, 4 to hybrid ports, port VLAN to 100, egress tagging to Untag All, allowed VLANs to 100,300.
3. Configure ports 5, 6 to hybrid ports, port VLAN to 200, egress tagging to Untag All, allowed VLANs to 200,300, as shown in Figure 241.
4. Keep all the other parameters default.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Hybrid	300	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100,200,300	
2	Hybrid	300	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100,200,300	
3	Hybrid	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100,300	
4	Hybrid	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	100,300	
5	Hybrid	200	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	200,300	
6	Hybrid	200	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	200,300	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Submit Reset

Figure 241 PVLAN Ports Configuration

## 19.3 GVRP

### 19.3.1 GARP Introduction

The Generic Attribute Registration Protocol (GARP) is used for spreading, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network.

With GARP, the configuration information of a GARP member will spread the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn. A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.

When a GARP application entity wants to cancel its own information on other switches, the entity sends a Leave message.

After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.

**Note:**

An application entity indicates a GARP-enabled port.

GARP timers include Hold timer, Join timer, Leave timer, LeaveAll timer.

**Hold Timer:** when a GARP-enabled switch receives a registration message, it starts a Hold timer rather than sending out the Join message immediately. When the Hold timer times out, it will put all registration information received during this time in a same Join message and send it out, reducing the message quantity for network stability.

**Join Timer:** in order to guarantee that the Join message can be reliably transmitted to other switches, the GARP-enabled switch will wait for a time interval of a Join timer after sending the first Join message. If the switch does not receive a Join In message during this time, it will send out a Join message again, otherwise, it won't send the second message.

**Leave Timer:** when a GARP-enabled switch wishes other switches to cancel its attribute information, it sends out a Leave message. Other GARP-enabled switches that receive this message will enable a Leave timer. If they do not receive a Join message until the timer times out, they will cancel this attribute information.

**LeaveAll Timer:** When a switch enables GARP, it starts a LeaveAll timer at the same time. When the timer times out, the switch will send a LeaveAll message to other GARP-Enabled switches and let them re-register their all attribute information, and then restart the LeaveAll timer to begin a new cycle.

### 19.3.2 GVRP Introduction

GVRP (GARP VLAN Registration Protocol) is a GARP application and is based on the GARP working mechanism to maintain the VLAN dynamic registration information of the device and propagate the information to other devices.

The GVRP-enabled device can receive VLAN registration information from other devices and dynamically update the local VLAN registration information, and the device can propagate the local VLAN registration information to other devices, reaching the consistency of VLAN information in all devices in the same LAN. The VLAN registration information propagated by GVRP contains not only the manually configured local static registration

information, but also the dynamic registration information from other devices.



**Caution:**

GVRP port and port channel are mutually exclusive. The port in a port channel cannot be configured as a GVRP port; the GVRP port cannot be added to a port channel.

**19.3.3 Web Configuration**

1. Enable GVRP protocol and set the corresponding timers, as shown in Figure 242.

**GVRP Configuration**

Enable GVRP

Parameter	Value	
Join-timer:	500	(ms)
Leave-timer:	3000	(ms)
LeaveAll-timer:	10000	(ms)
Max VLANs:	20	

Figure 242 GVRP Protocol Configuration

**Enable GVRP**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable GVRP protocol.

**Join-timer**

Range: 100ms~327600ms

Default: 500ms

Function: Configure the join-timer value. The value must be a multiple of 100.

**Leave-timer**

Range: 100ms~327600ms

Default: 3000ms

Function: Configure the level-timer value. The value must be a multiple of 100.

**LeaveAll-timer**

Range: 100ms~327600ms

Default: 10000ms

Function: Configure the leave all-timer value. The value must be a multiple of 100.

Explanation: If LeaveAll timers of different devices time out at the same time, the devices will send out a LeaveAll message at the same time, which increases the message quantity. In order to avoid this, the actual running time of a LeaveAll timer is a random value and is longer than the time of one LeaveAll timer, and less than 1.5 times of a LeaveAll timer.

**Max VLANs**

Range: 1~4094

Default: 20

Function: Set the maximum number of VLANs that are dynamically registered with a GVRP port. The GVRP function needs to be disabled for the setting of this parameter.

2. Configure GVRP port, as shown in Figure 243.

**GVRP Port Configuration**

Port	Mode
*	<>
1	GVRP enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Submit    Reset

Figure 243 GVRP Port Setting

**Mode**

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port GVRP function.



**Caution:**

➤ A GVRP port should be configured as a Trunk port.

➤ A GVRP port is used to transmit the VLAN attributes of other GVRP ports in the up state.

3. Show statically configured and dynamically registered VLAN information, as shown in Figure 244.

### VLAN Membership Status for Combined users

Start from VLAN  with  entries per page.

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 244 VLAN Information

### 19.3.4 Typical Configuration Example

As Figure 245 shows, GVRP needs to be enabled on devices so that VLAN information is dynamically registered and updated between device A and device B.

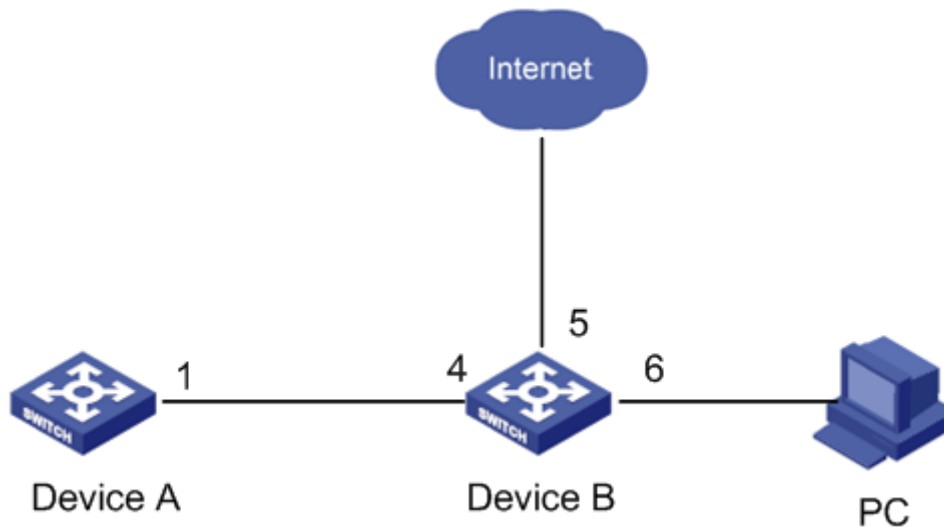


Figure 245 GVRP Configuration Example

Configuration of Device A are as follows:

1. Configure port 1 to trunk port, allowed VLANs to 1.
2. Enable global GVRP, as shown in Figure 242.
3. Enable GVRP on port 1, as shown in Figure 243.

Configuration of Device B are as follows:

1. Configure port 4 to trunk port, allowed VLANs to 1; configure port 5 to access port,

allowed VLANs to 5; configure port 6 to trunk port, allowed VLANs to 1, 6.

2. Enable global GVRP, as shown in Figure 242.

3. Enable GVRP on port 4, 5, 6, as shown in Figure 243.

Port 1 of Switch A can register the same VLAN information as that of port 5 and 6 of Switch B, as shown in Figure 244.

## 20 Redundancy

### 20.1 DT-Ring

#### 20.1.1 Introduction

DT-Ring and DT-Ring+ are Kyland-proprietary redundancy protocols. They enable a network to recover within 50ms when a link fails, ensuring stable and reliable communication.

DT rings fall into two types: port-based (DT-Ring-Port) and VLAN-based (DT-Ring-VLAN).

DT-Ring-Port: specifies a port to forward or block packets.

DT-Ring-VLAN: specifies a port to forward or block the packets of a specific VLAN. This allows multiple VLANs on a tangent port, that is, one port is part of different redundant rings based on different VLANs.

DT-Ring-Port and DT-Ring-VLAN cannot be used together.

#### 20.1.2 Concepts

**Master:** One ring has only one master. The master sends DT-Ring protocol packets and detects the status of the ring. When the ring is closed, the two ring ports on the master are in forwarding and blocking state respectively.



**Note:**

The first port whose link status changes to up when the ring is closed is in forwarding state.

The other ring port is in blocking state.

---

**Slave:** A ring can include multiple slaves. Slaves listen to and forward DT-Ring protocol packets and report fault information to the master.

**Backup port:** The port for communication between DT rings is called the backup port.

**Master backup port:** When a ring has multiple backup ports, the backup port with the larger MAC address is the master backup port. It is in forwarding state.

**Slave backup port:** When a ring has multiple backup ports, all the backup ports except the master backup port are slave backup ports. They are in blocking state.

**Forwarding state:** If a port is in forwarding state, the port can both receive and send data.



Blocking state: If a port is in blocking state, the port can receive and forward only DT-Ring protocol packets, but not other packets.

### 20.1.3 Implementation

#### DT-Ring-Port Implementation

The forwarding port on the master periodically sends DT-Ring protocol packets to detect ring status. If the blocking port of the master receives the packets, the ring is closed; otherwise, the ring is open.

Working process of switch A, Switch B, Switch C, and Switch D:

1. Configure Switch A as the master and the other switches as slaves.
2. Ring port 1 on the master is in forwarding state while ring port 2 is in blocking state. Both two ports on the slave are in forwarding state.
3. If link CD is faulty, as shown in Figure 246.
  - a) When link CD is faulty, port 6 and port 7 on the slave are in blocking state. Port 2 on the master changes to forwarding state, ensuring normal link communication.
  - b) When the fault is rectified, port 6 and port 7 on the slave are in forwarding state. Port 2 on the master changes to blocking state. Link switchover occurs and links restore to the state before CD is faulty.

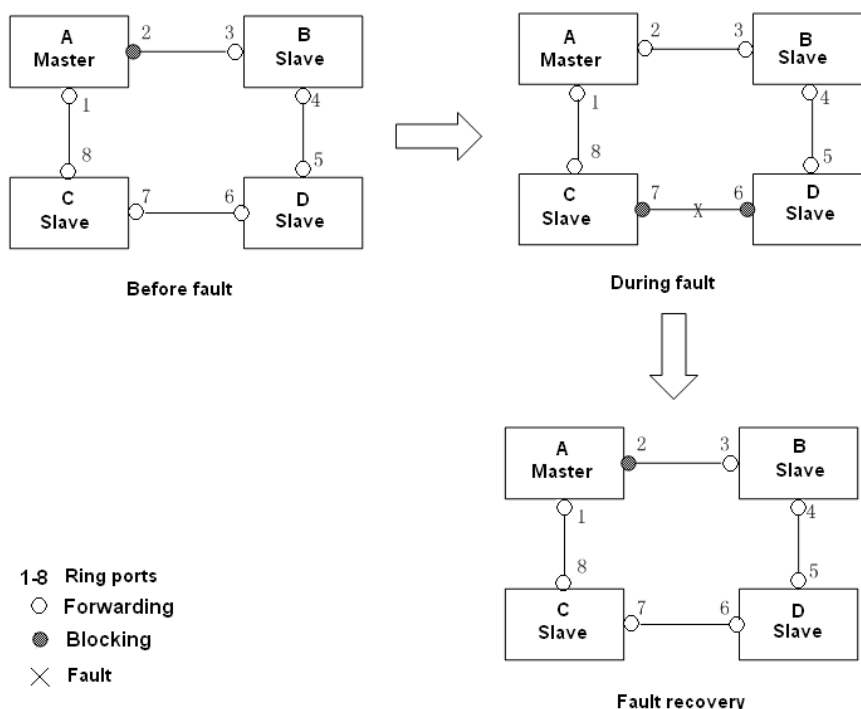


Figure 246 CD Link Fault

4. If link AC is faulty, as shown in Figure 247.

a) When link AC is faulty, port 1 is in blocking state and port 2 changes to forwarding state, ensuring normal link communication.

b) After the fault is rectified, port 1 is still in blocking state and port 8 is in forwarding state. No switchover occurs.

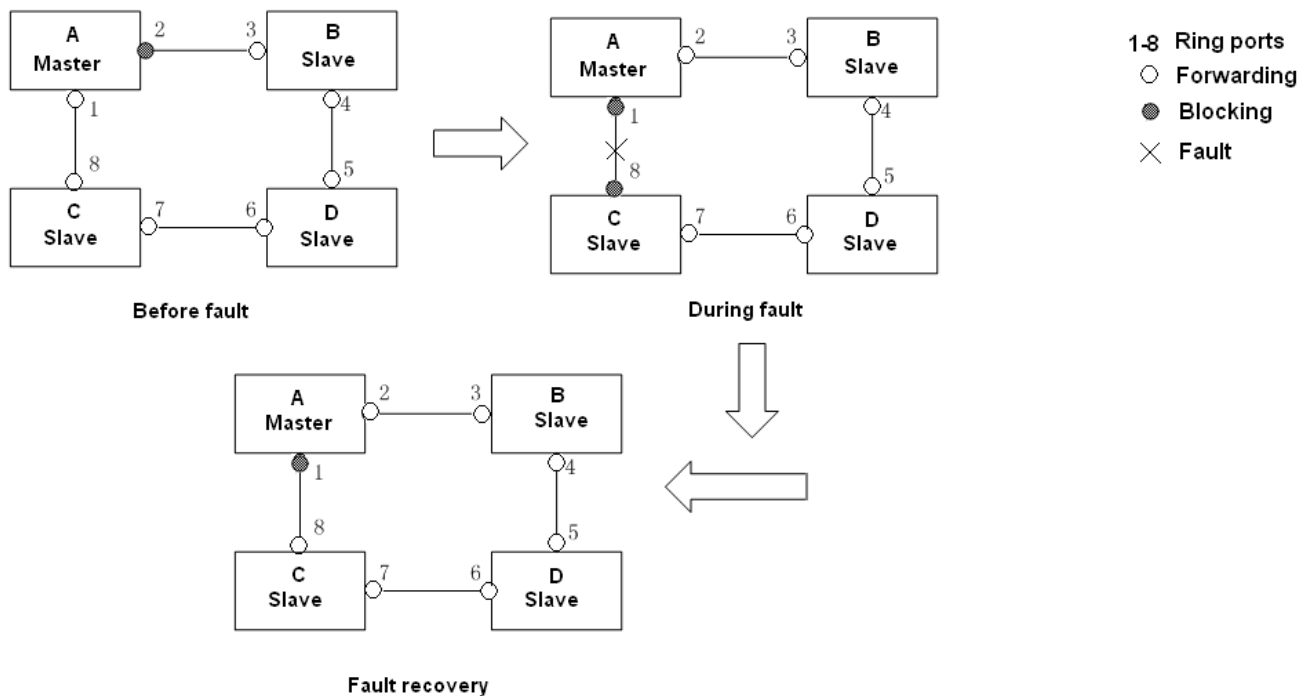


Figure 247 DT-Ring Link Fault



**Caution:**

Link status change affects the status of ring ports.

**DT-Ring-VLAN Implementation**

DT-Ring-VLAN allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-Ring-VLAN. Different DT-VLAN-Rings can have different masters. As shown in Figure 248, two DT-Ring-VLANs are configured.

Ring links of DT-Ring-VLAN 10: AB-BC-CD-DE-EA.

Ring links of DT-Ring-VLAN 20: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same

ports in the two rings, but use different logical links based on VLANs.

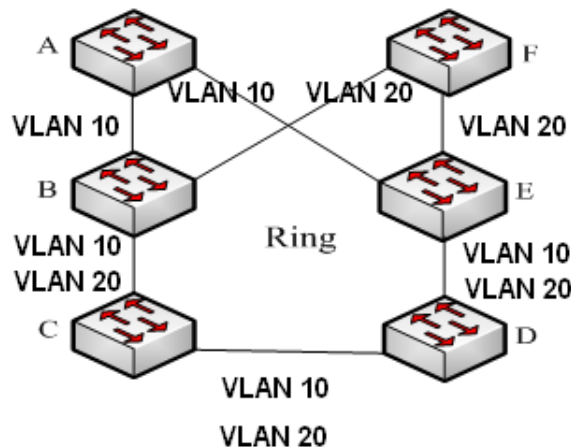


Figure 248 DT-Ring-VLAN



**Note:**

In each DT-Ring-VLAN logical ring, the implementation is identical with that of DT-Ring-Port.

**DT-Ring+ Implementation**

DT-Ring+ can provide backup for two DT rings, as shown in Figure 249. One backup port is configured respectively on Switch C and Switch D. Which port is the master backup port depends on the MAC addresses of the two ports. If the master backup port or its link fails, the slave backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

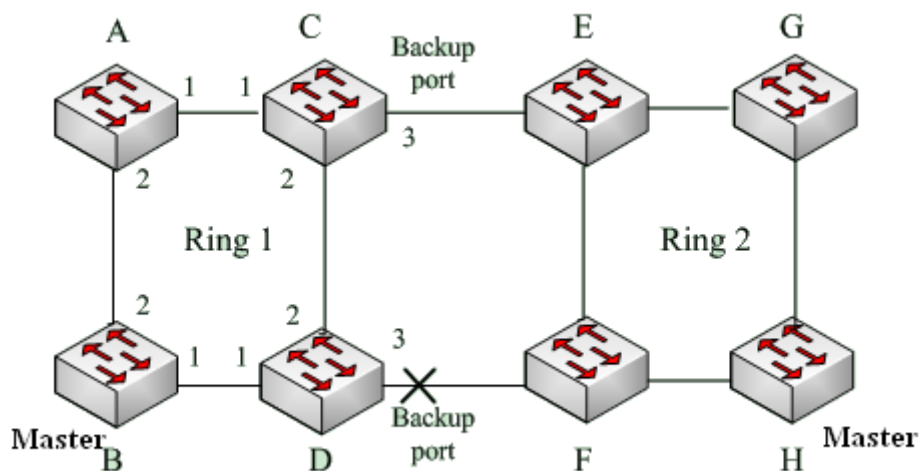


Figure 249 DT-Ring+ Topology



**Caution:**

Link status change affects the status of backup ports.

**20.1.4 Explanation**

DT-Ring configurations should meet the following conditions:

- All switches in the same ring must have the same domain number.
- Each ring can only have one master and multiple slaves.
- Only two ports can be configured on each switch for a ring.
- For two connected rings, backup ports can be configured only in one ring.
- A maximum of two backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring.
- DT-Ring-Port and DT-Ring-VLAN cannot be configured on one switch at the same time.

**20.1.5 Web Configuration**

1. Configure DT-Ring redundant ring mode, as shown in Figure 250.

**Global DT-Ring Configuration**

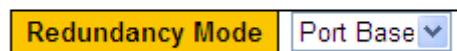


Figure 250 Redundant Ring Mode Configuration

**Redundancy Mode**

Options: Port Based/Vlan Based

Default: Port Based

Function: Choose DT-Ring redundant ring mode.



**Caution:**

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

2. Configure DT-Ring-Port and DT-Ring-VLAN, as shown in Figure 251 and Figure 252.

DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
<input type="checkbox"/>	1	a	Master	1	2	Enable	3	

Figure 251 DT-Ring-Port Configuration

DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
<input type="checkbox"/>	1	a	Master	1	2	Enable	3	1-3,5

Figure 252 DT-Ring-VLAN Configuration

**Domain ID**

Range: 1~32

Function: The domain ID is used to distinguish different rings. One switch supports a maximum of 16 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

**Domain Name**

Range: 1~31 characters

Function: Configure the domain name.

**Station Type**

Options: Master/Slave

Default: Master

Function: Select the switch role in a ring.

**Ring Port-1/Ring Port-2**

Options: all switch ports

Function: Select two ring ports.



**Caution:**

- DT-Ring ring port or backup port and port channel are mutually exclusive. A DT-Ring ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DT-Ring ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are

mutually exclusive, that is, the ring port and backup port of DT-Ring-Port cannot be configured as RSTP port, DRP-Port ring port, or DRP-Port backup port; RSTP port, DRP-Port ring port, and DRP-Port backup port cannot be configured as DT-Ring-Port ring port or backup port.

- It is not recommended that ports in the isolation group are configured as DT-Ring ports and backup ports at the same time, and DT-Ring ports and backup ports cannot be added to the isolation group.

### DT-Ring+

Options: Enable/Disable

Default: Disable

Function: Enable/disable DT-Ring+.

### Backup Port

Options: all switch ports

Function: Set a port to backup port.

Explanation: Enable DT-Ring+ before setting backup port.



**Caution:**

Do not configure a ring port as a backup port.

### VLAN ID

Options: all created VLANs

Function: Select the VLANs for the ring port. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

3. View and modify DT-Ring configuration, as shown in Figure 253.

DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
<input type="checkbox"/>	1	a	Master	1	2	Enable	3	--
<input checked="" type="checkbox"/>	1	a	Master	1	2	Enable	3	---
<input type="checkbox"/>	2	b	Slave	4	5	Disable	---	---

Submit Modify Delete Reset

Figure 253 DT-Ring Configuration

Select a DT-Ring entry, click <Modify> to edit the DT-Ring entry configuration; click <Delete> to delete the designated DT-Ring entry.

4. Click a DT-Ring entry in Figure 253 to show DT-Ring and port status, as shown in Figure 254.

### DT-Ring Information

Domain Id	1
Domain Name	a
Station Type	Master
Ring State	Close
Ring Port-1	1   Forwarding
Ring Port-2	2   Blocking
Change Time	1   <input type="button" value="Clear"/>
Vlan List	---

Auto-refresh

### DT-Ring+ Information

DT-Ring+	Enable
Backup Port	3
Device-0	
Backup Port	3   Blocking
Equipment IP	192.168.0.222
Equipment MAC	00-01-c1-00-00-00
Device-1	
Backup Port	3   Blocking
Equipment IP	192.168.0.221
Equipment MAC	00-22-11-11-11-01

Figure 254 DT-Ring State

### 20.1.6 Typical Configuration Example

As shown in Figure 249, switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

#### Configuration on Switch A:

1. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 251.

#### Configuration on Switch B:

2. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 251;

**Configuration on Switch C and Switch D:**

3. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to enable, backup port to 3, as shown in Figure 251;

**Configuration on Switch E, Switch F, and Switch G:**

4. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 251;

**Configuration on Switch H:**

5. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 251;

## 20.2 DRP

### 20.2.1 Overview

Kyland develops the Distributed Redundancy Protocol (DRP) for data transmission on ring-topology networks. It can prevent broadcast storms for ring networks. When a link or node is faulty, the backup link can take over services in real time to ensure continuous data transmission.

Compliant with the IEC 62439-6 standard, DRP uses the master election mechanism with no fixed master. DRP provides the following features:

➤ Network scale-independent recovery time

DRP achieves network scale-independent recovery time by optimizing the ring detection packet forwarding mechanism. DRP enables networks to recover within 20ms, with the introduction of real-time reporting interruption, improving reliability for real-time data transmission. This feature enables switches to provide higher reliability for the applications in the power, rail transit, and many other industries that require real-time control.

➤ Diversified link detection functions

To improve network stability, DRP provides diversified link detection functions for typical network faults, including fast disconnection detection, optical fiber unidirectional link detection, link quality inspection, and equipment health check, ensuring proper data transmission.



- Applicable to multiple network topologies

Besides rapid recovery for simple ring networks, DRP also supports complex ring topologies, such as intersecting rings and tangent rings. Additionally, DRP supports VLAN-based multiple instances, thereby suiting various network applications with flexible networking.

- Powerful diagnosis and maintenance functions

DRP provides powerful status query and alarm mechanisms for network diagnosis and maintenance, as well as mechanism for preventing unintended operation and incorrect configurations that may lead to ring network storms.

### 20.2.2 Concept

#### 1. DRP Modes

DRP involves two modes: DRP-Port-Based and DRP-VLAN-Based.

DRP-Port-Based: forwards or blocks packets based on specific ports.

DRP-VLAN-Based: forwards or blocks packets based on VLANs. If a port is in blocking state, only the data packets of the specified VLAN are blocked. Therefore, multiple VLANs can be configured on tangent ring ports. A port can belong to different DRP rings according to VLAN configurations.

#### 2. DRP Port Statuses

Forwarding state: If a port is in forwarding state, it can receive and forward data packets.

Blocking state: If a port is in blocking state, it can receive and forward DRP packets, but not other data packets.

Primary port: indicates the ring port (on the root) whose status is configured as forwarding forcibly by user when the ring is closed.



**Caution:**

- If no primary port is configured on the root, the first port whose link status changes to up when the ring is closed is in forwarding state. The other ring port is in blocking state.
- A port in blocking state on the Root can proactively send DRP packets.

#### 3. DRP Roles

DRP determines the roles of switches by forwarding Announce packets, preventing

redundancy rings to form loops.

INIT: indicates the device on which DRP is enabled and the two ring ports are in Link down state.

Root: indicates the device on which DRP is enabled and at least one ring port is in Link up state. In a ring, the Root is elected according to the vectors of Announce packets. It may change with the network topology. The Root sends its own Announce packets to other devices periodically. Statuses of ring ports: One ring port is in forwarding state and the other is in blocking state. Upon receiving the Announce packet of another device, the Root compares the vector of the packet with that of its own Announce packet. If the vector of the received packet is larger, the Root changes its role to Normal or B-Root according to the link status and CRC degradation of ports.

B-Root: indicates the device on which DRP is enabled, meeting at least one of the following conditions: one ring port is in Link up state while the other is in Link down, CRC degradation, the priority is not less than 200. The B-Root compares and forwards Announce packets. If the vector of a received Announce packet is smaller than that of its own announce packet, the B-Root changes its role to Root; otherwise, it forwards the received packet and does not change its own role. Statuses of ring ports: One ring port is in forwarding state.

Normal: indicates the device on which DRP is enabled and both ring ports are in Link up state without CRC degradation and the priority is less than 200. The Normal only forwards Announce packets, but does not check the content of packets. Statuses of ring ports: Both ring ports are in forwarding state.



**Note:**

CRC degradation: indicates that the number of CRC packets exceed the threshold in 15 minutes.

**20.2.3 Implementation**

Each switch maintains its own vector of Announce packet. The switch with the larger vector will be elected as the Root.

The vector of Announce packet contains the following information for role assignment.

Table 13 Vector of Announce Packet

Link	CRC degradation		Role	IP address of	MAC address
status	CRC degradation status	CRC degradation rate	priority	the device	of the device

Link status: The value is set to 1 if one ring port is in Link down state and set to 0 if both ring ports are in Link up state.

CRC degradation status: If CRC degradation occurs on one port, the value is set to 1. If CRC degradation does not occur on the two ring ports, the value is set to 0.

CRC degradation rate: The ratio of the number of CRC packets and the threshold in 15 minutes.

Role priority: The value can be set on the Web UI.

The parameters in Table 13 are compared in the following procedure:

1. The value of link status is checked first. The device with a larger link status value is considered to have a larger vector.
2. If the two compared devices have the same link status value, the values of CRC degradation status are compared. The device with a larger CRC degradation status value is considered to have a larger vector. If the CRC degradation status value of all compared devices is 1, the device with a larger CRC degradation rate value is considered to have a larger vector.
3. If the two compared devices have the same link status value and CRC degradation value, the values of role priority, IP addresses, and MAC addresses are compared sequentially. The device with a larger value is considered to have a larger vector.
4. The device with the larger vector is elected as the Root.



**Note:**

Only when CRC degradation status value is 1, the CRC degradation rate value participates in vector comparison. Otherwise, the vectors are compared regardless of CRC degradation rate value.

➤ Implementation of DRP-Port-Based mode

The roles of switches are as follows:

1. Upon startup, all switches are in INIT state. When the state of one port changes to Link up, the switch becomes the Root and sends Announce packets to the other switches in the ring for election.
2. The switch with the largest vector of Announce packet is elected as the Root. The ring port that links up first on the Root is in forwarding state and the other ring port is in blocking state. Among the other switches in the ring, the switch with one ring port in Link down or CRC degradation state is the B-Root. The switch with both ring ports in Link up state and no CRC degradation is the Normal.

The fault recovery procedure is shown in the following figure:

1. In the initial topology, A is the Root; port 1 is in forwarding state and port 2 in blocking state. B, C, and D are Normal(s), and their ring ports are in forwarding state.
2. When link CD is faulty, DRP changes the statuses of port 6 and port 7 to blocking. As a result, C and D become the Roots. Because A, C, and D are Roots at the moment, they all send Announce packets. The vectors of C and D are larger than that of A because port 7 and port 6 are in Link down status. In this case, if the vector of D is larger than that of C, D is elected as the Root and C becomes the B-Root. When receiving the Announce packet of D, A finds that the vector of D is larger than its own vector and both its ring ports are in Link up state. Therefore, A becomes a Normal and changes the status of port 2 to forwarding.
3. When link CD recovers, D is still the Root because its vector is larger than the vector of C.
  - If no primary port is configured on D, port 7 is still in blocking state and port 8 is in forwarding state.
  - If port 7 on D is configured as primary port, port 7 changes to forwarding state and port 8 is in blocking state.

DRP changes the state of port 6 to forwarding. As a result, C becomes a Normal. Therefore, the root node of this network do not change for link recovery.

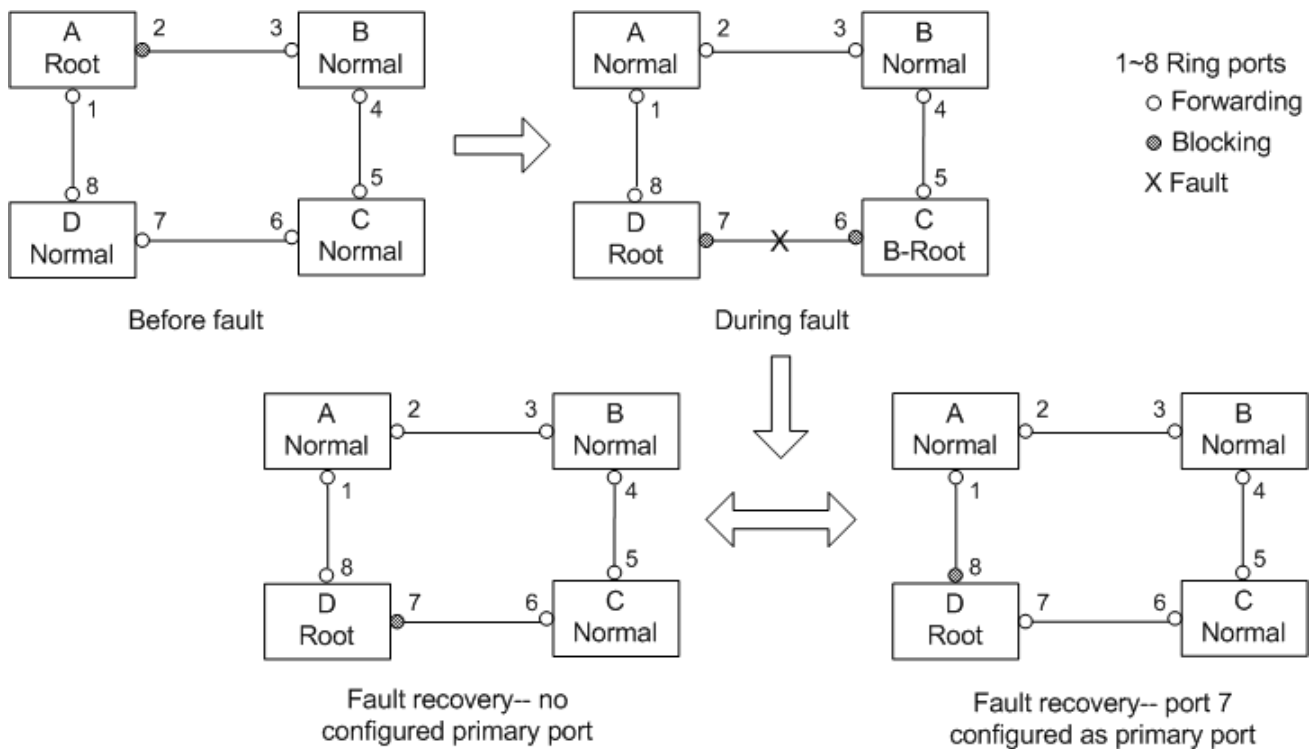


Figure 255 DRP Link Fault



**Note:**

In a DRP ring network, the roles of switches change upon a link fault, but do not change when the link recovers. This mechanism improves network security and reliability of data transmission.

➤ Implementation of DRP-VLAN-Based mode

DRP-VLAN-Based ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DRP-VLAN-Based. Different DRP-VLAN-Based ring can have different roots. As shown in the following figure, two DRP-VLAN-Based rings are configured.

Ring links of DRP-VLAN10/20-Based: AB-BC-CD-DE-EA.

Ring links of DRP-VLAN30-Based: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLANs

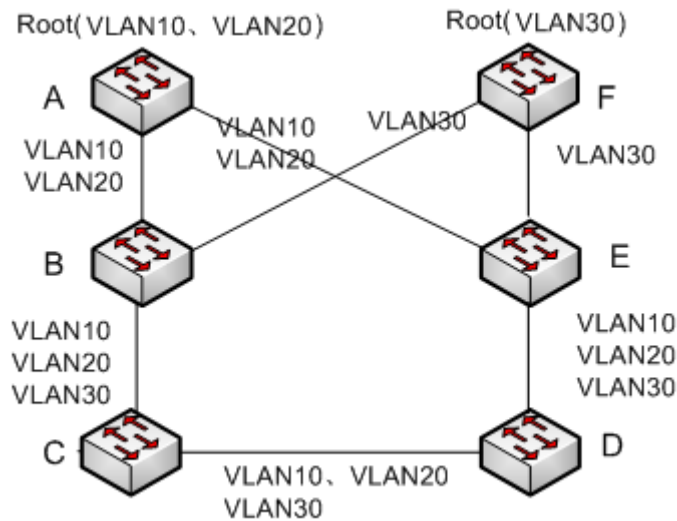


Figure 256 DRP-VLAN-Based



**Note:**

The port status and role assignment of each DRP-VLAN-Based ring are the same as those of DRP-Port-Based ring.

➤ DRP Backup

DRP can also provide backup for two DRP rings, preventing loops and ensuring normal communication between rings.

Backup port: indicates the communication port between DRP rings. Multiple backup ports can be configured, but must be in the same ring. The first backup port that links up is the master backup port, which is in forwarding state. All the other backup ports are slave. They are in blocking state.

As shown in Figure 257, one backup port can be configured on each switch. The master backup port is in forwarding state and the other backup ports are in blocking state. If the master backup port or its link is faulty, a slave backup port will be selected to forward data.

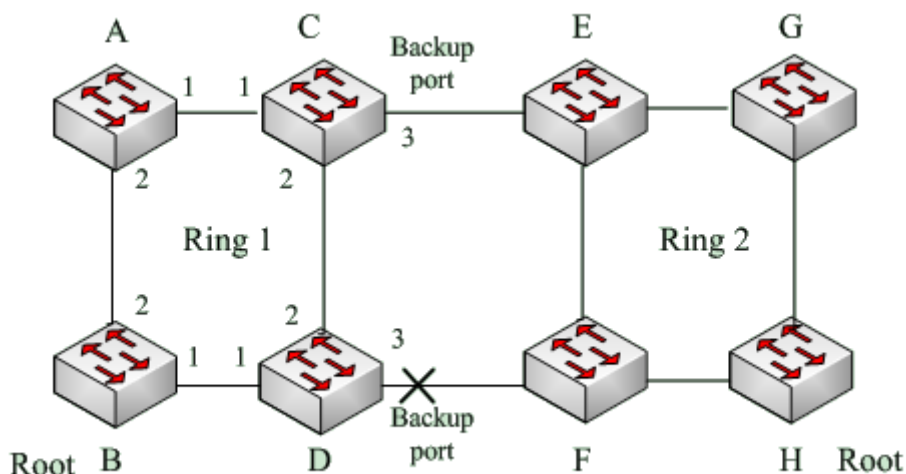


Figure 257 DRP Backup



**Caution:**

Link status change affects the status of backup ports.

## 20.3 DHP

### 20.3.1 Overview

As shown in Figure 258, A, B, C, and D are mounted to a ring. Dual Homing Protocol (DHP) achieves the following functions if it is enabled on A, B, C, and D:

- A, B, C, and D can communicate with each other, without affecting the proper running of devices in the ring.
- If the link between A and B is faulty, A can still communicate with B, C, and D by way of Device 1 and Device 2.

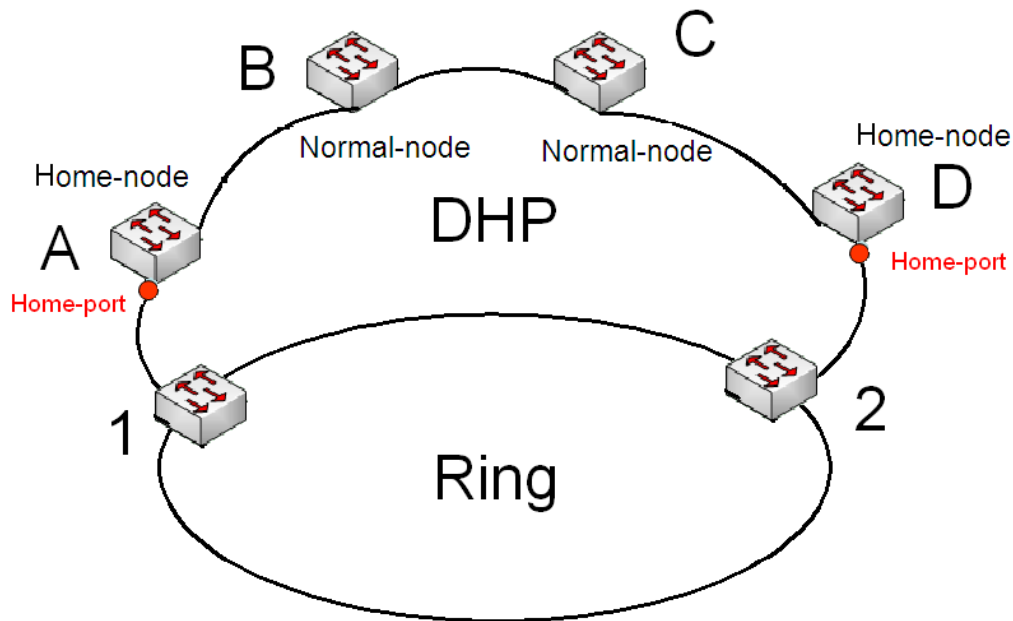


Figure 258 DHP Application

### 20.3.2 Concepts

The implementation of DHP is based on DRP. The role election and assignment mechanism of DHP is the same as that of DRP. DHP provides link backup through the configuration of Home-node, Normal-node, and Home-port.

Home-node: indicates the devices at both ends of the DHP link and terminates DRP packets.

Home-port: indicates the port connecting a Home node to the external network. A Home-port provides the following functions:

- Sending response packets to the Root upon receiving Announce packets from the Root. The Root identifies the ring status as closed if it receives response packets. If the Root does not receive response packets, it identifies the ring status as open.
- Blocking the DRP packets of external networks and isolating the DHP link from external networks.
- Sending entry clearing packets to connected devices on external networks upon a topology change of the DHP link.

Normal-node: indicates the devices in the DHP link, excluding the devices at both ends.

Normal-nodes transmit the response packets of Home-nodes.



### 20.3.3 Implementation

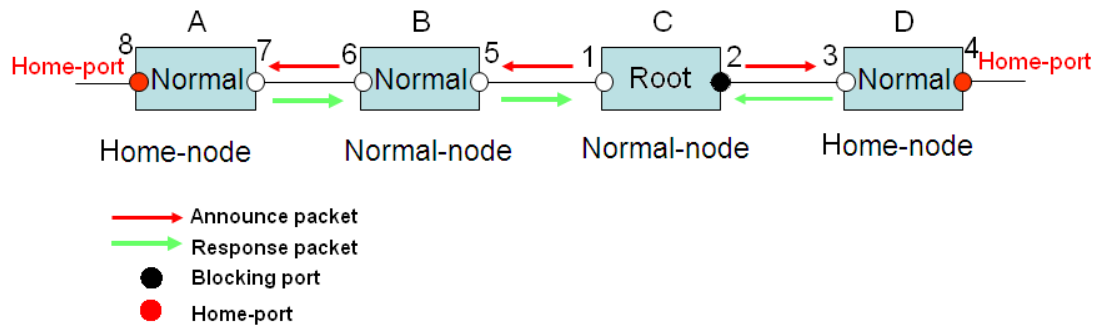


Figure 259 DHP Configuration

As shown in Figure 258, the configurations of A, B, C, and D in Figure 259 are as follows:

- DRP configuration: C is the Root; port 2 is in blocking state; A, B, and D are Normal; all the other ring ports are in forwarding state.
- DHP configuration: A and D are Home-nodes; port 8 and port 4 are Home-ports; B and C are Normal-nodes.

Implementation:

1. C, the Root, sends Announce packets through its two ring ports. Home-port 8 and Home-port 4 terminate the received Announce packets and send response packets to C. C identifies the ring status as closed. Port 2 is in blocking state.
2. When the link between A and B is blocked, the topology involves two links: A and B-C-D.
  - A is elected as the Root. Port 7 is in blocking state.
  - In link B-C-D, B is elected as the Root. Port 6 is in blocking state. C becomes the Normal. Port 2 is forwarding state. A can communicate with B, C, and D by way of Device 1 and Device 2, as shown in Figure 260.

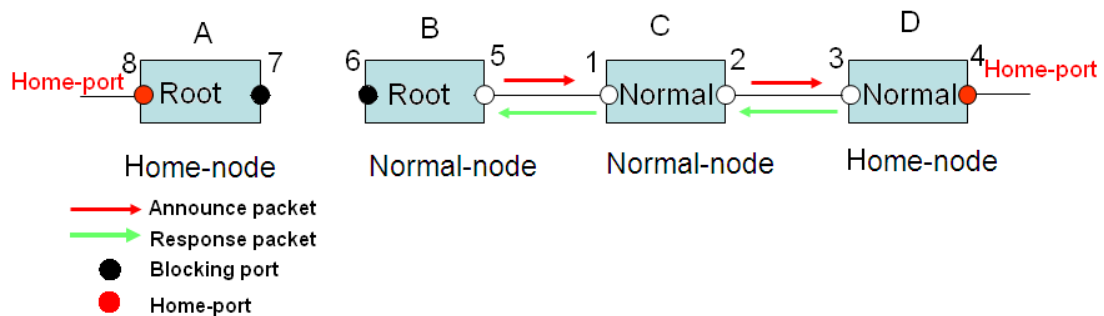


Figure 260 DHP Fault Recovery

### 20.3.4 Description

DRP configurations meet the following requirements:

- All switches in the same ring must have the same domain number.
- One ring contains only one Root, but can contain multiple B-Roots or Normal(s).
- Only two ports can be configured on each switch for a ring.
- For two connected rings, backup ports can be configured only in one ring.
- Multiple backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring.

### 20.3.5 Web Configuration

1. Configure the DRP redundancy mode, as shown in Figure 261.

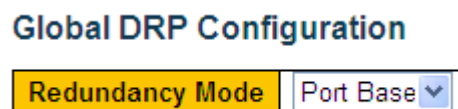


Figure 261 Configure the DRP Redundancy Mode

#### Redundancy Mode

Options: Port Based/Vlan Based

Default: Port Based

Function: Configure the DRP redundancy mode.



**Caution:**

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

2. Configure DRP-Port-Based and DRP-VLAN-Based, as shown in Figure 262 and Figure 263.

DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
<input type="checkbox"/>	1	a	1	2	Ring Port	Disable	--	100	128	3		

Submit Modify Delete Reset

Figure 262 DRP-Port-Based Configuration

DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
<input type="checkbox"/>	1	a	1	2	Ring Port	Disable	--	100	128	3	1-3,5	2

Submit Modify Delete Reset

Figure 263 DRP-VLAN-Based Configuration

**Domain ID**

Range: 1~32

Function: Each ring has a unique domain ID. One switch supports a maximum of 8 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

**Domain Name**

Range: 1~31 characters

Function: Configure the domain name.

**Ring Port-1/Ring Port-2**

Options: all switch ports

Function: Select two ring ports.



**Caution:**

- DRP ring port or backup port and port channel are mutually exclusive. A DRP ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DRP ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, the ring port and backup port of DRP-Port cannot be configured as RSTP port, DT-Ring-Port ring port, or DT-Ring-Port backup port; RSTP port, DT-Ring-Port ring port, and DT-Ring-Port backup port cannot be configured as DRP-Port ring port or backup port.
- It is not recommended that ports in an isolation group are configured as DRP ports and backup ports at the same time, and DRP ports and backup ports cannot be added to an isolation group.

**Primary Port**

Options: --/Ring Port-1/Ring Port-2

Default: --

Function: Configure the primary port. When the ring is closed, the primary port on root is in forwarding state.

**DHP Mode**

Options: Disable/Normal-Node/Home-Node

Default: Disable

Function: Disable DHP or configure the DHP mode.

**DHP Home Port**

Options: Ring-Port-1/Ring-Port-2/Ring-Port-1-2

Function: Configure the Home-port for a DHP Home-node.

Description: If there is only one device in DHP link, the both ring ports of the Home-node must be configured as the Home-port.

**CRC Threshold**

Range: 25~65535

Default: 100

Function: Configure the CRC threshold.

Description: This parameter is used in root election. The system counts the number of received CRCs. If the number of CRCs of one ring port exceeds the threshold, the system considers the port to have CRC degradation. As a result, the CRC degradation value is set to 1 in the vector of the Announce packet of the port.

**Role Priority**

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

**Backup Port**

Options: all switch ports

Function: Configure the backup port.



**Caution:**

Do not configure a ring port as a backup port.

**VLAN List**

Options: All created VLANs

Function: Select the VLANs managed by current DRP-VLAN-Based ring.

**Protocol Vlan ID**

Range: 1~4093

Description: The VLAN ID must be one of service VLAN.

Function: DRP packets with the VLAN ID serve as the basis for the diagnosis and maintenance of the DRP-VLAN-Based ring.

3. View and modify DRP configuration, as shown in Figure 264.

DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
<input type="checkbox"/>	1	a	1	2	Ring Port-1	Disable	---	100	128	3		0
<input checked="" type="checkbox"/>	1	a	1	2	Ring Port-1	Disable	---	100	128	3		
<input type="checkbox"/>	2	b	4	5	---	Disable	---	100	128	---		

Submit Modify Delete Reset

Figure 264 View and Modify DRP Configuration

Select a DRP entry, click <Modify> to edit the DRP entry configuration; click <Delete> to delete the designated DRP entry.

4. Click a DRP entry in Figure 264 to show DRP and port status, as shown in Figure 265.

**DRP Information**

Domain ID	1
Domain Name	a
Role State	ROOT
Ring State	Close
Ring Port-1	1   FORWARD
Ring Port-2	2   BLOCK
Primary Port	Ring Port-1
DHP Mode	Disable
DHP Home Port	---
CRC Threshold	100
Role Priority	128
Backup Port	3   INIT

Figure 265 DRP State

### 20.3.6 Typical Configuration Example

As shown in Figure 257, A, B, C, and D form Ring 1; E, F, G, and H form Ring 2; CE and DF are the backup links of Ring 1 and Ring 2.

#### Configuration on switch A and switch B:

1. Set Domain ID to 1 and Domain name to a. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 262.

#### Configuration on switch C and switch D:

2. Set Domain ID to 1, Domain name to a, and Backup port to 3. Select ring port 1 and ring port 2. Keep the default value for role priority, as shown in Figure 262;

#### Configuration on switch E, F, G, and H:

3. Set Domain ID to 2 and Domain name to b. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 262;

## 20.4 RSTP/STP

### 20.4.1 Introduction

Standardized in IEEE802.1D, the Spanning Tree Protocol (STP) is a LAN protocol used for preventing broadcast storms caused by link loops and providing link backup. STP-enabled devices exchange packets and block certain ports to prune "loops" into "trees", preventing proliferation and endless loops. The drawback of STP is that a port must wait for twice the forwarding delay to transfer to the forwarding state.

To overcome the drawback, IEEE creates 802.1w standard to supplement 802.1D.

IEEE802.1w defines the Rapid Spanning Tree Protocol (RSTP). Compared with STP, RSTP achieves much more rapid convergence by adding alternate port and backup port for the root port and designated port respectively. When the root port is invalid, the alternate port can enter the forwarding state quickly.

### 20.4.2 Concepts

Root bridge: serves as the root for a tree. A network has only one root bridge. The root bridge changes with network topology. The root bridge periodically sends BPDU to the other

devices, which forward the BPDU to ensure topology stability.

Root port: indicates the best port for transmission from the non-root bridges to the root bridge. The best port is the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.

Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.

Alternate port: indicates the backup port of the root port. If the root port fails, the alternate port becomes the new root port.

Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the new designated port and forwards data.

**20.4.3 BPDU**

To prevent loops, all the bridges of a LAN calculate a spanning tree. The calculation process involves transmitting BPDUs among devices to determine the network topology. Table 14 shows the data structure of a BPDU.

Table 14 BPDU

...	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	...
...	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	...

Root bridge ID: priority of the root bridge (2 bytes) +MAC address of the root bridge (6 bytes).

Root path cost: cost of the path to the root bridge.

Designated bridge ID: priority of the designated bridge (2 bytes) +MAC address of the designated bridge (6 bytes).

Designated port ID: port priority + port number.

Message age: duration that a BPDU can be spread in a network.

Max age: maximum duration that a BPDU can be saved on a device. When Message age is larger than Max age, the BPDU is discarded.

Hello time: interval for sending BPDUs.

Forward delay: status change delay (discarding--learning--forwarding).

#### 20.4.4 Implementation

The process for all bridges calculating the spanning tree with BPDUs is as follows:

##### 1. In the initial phase

Each port of all devices generates the BPDU with itself as the root bridge; both root bridge ID and designated bridge ID are the ID of the local device; the root path cost is 0; the designated port is the local port.

##### 2. Best BPDU selection

All devices send their own BPDUs and receive BPDUs from other devices. Upon receiving a BPDU, each port compares the received BPDU with its own.

- If the priority of its own BPDU is higher, then the port does not perform any operation.
- If the priority of the received BPDU is higher, then the port replaces the local BPDU with the received one.

Devices compare the BPDUs of all ports and figure out the best BPDU. Principles for comparing BPDUs are as follows:

- The BPDU with a smaller root bridge ID has a higher priority.
- If the root bridge IDs of two BPDUs are the same, their root path costs are compared. If the root path cost in a BPDU plus the path cost of the local port is smaller, then the priority of the BPDU is higher.
- If the root path costs of two BPDUs are also the same, the designated bridge IDs, designated port IDs, and IDs of the port receiving the BPDUs are further compared in order. The BPDU with a smaller ID has a higher priority. The BPDU with a smaller root bridge ID has a higher priority.

##### 3. Selection of the root bridge

The root bridge of the spanning tree is the bridge with the smallest bridge ID.

##### 4. Selection of the root port

A non-root-bridge device selects the port receiving the best BPDU as the root port.

##### 5. BPDU calculation of the designated port



Based on the BPDU of the root port and the path cost of the root port, a device calculates a designated port BPDU for each port as follows:

- Replace the root bridge ID with the root bridge ID of the BPDU of the root port.
- Replace the root path cost with the root path cost of the root port BPDU plus the path cost of the root port.
- Replace designated bridge ID with the ID of the local device.
- Replace the designated port ID with the ID of the local port.

#### 6. Selection of the designated port

If the calculated BPDU is better, then the device selects the port as the designated port, replaces the port BPDU with the calculated BPDU, and sends the calculated BPDU. If the port BPDU is better, then the device does not update the port BPDU and blocks the port.

Blocked ports can receive and forward only RSTP packets, but not other packets.

### 20.4.5 Web Configuration

1. Set the time parameters of the network bridge, as shown in Figure 266.

### STP Bridge Configuration

**Global Settings**

Global Enable Enable ▼

**Basic Settings**

Protocol Version	RSTP ▼
Bridge Priority	0 ▼
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

**Advanced Settings**

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

Save
Reset

Figure 266 Setting Time Parameters of the Network Bridge

#### Global Enable

Options: Enable/Disable

Default: Disable

Function: Disable or enable spanning tree.



**Caution:**

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

#### Protocol Priority

Options: MSTP/RSTP/STP

Default: MSTP

Function: Select the spanning tree protocol.

### Bridge Priority

Range: 0~61440. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

### Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

### Forward Delay

Range: 4~30s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

### Max Age

Range: 6~40s

Default: 20s

Function: Maximum duration that a BPDU can be saved on a device.

Description: If the value of message age in the BPDU is larger than the specified value, then the BPDU is discarded.



#### Caution:

- The values of Forward Delay Time, Hello Time and Max Age Time should meet the following requirements:  $2 * (\text{Forward Delay Time} - 1.0 \text{ seconds}) \geq \text{Max Age Time}$ ;  $\text{Max Age Time} \geq 2 * (\text{Hello Time} + 1.0 \text{ seconds})$ .
  - The default setting is recommended.
-

**Transmit Hold Count**

Range: 1~10

Default: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

**Edge Port BPDU Filtering**

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

**Edge Port BPDU Guard**

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

**Port Error Recovery**

Options: Enable/Disable

Default: Disable

Function: Control whether a port can automatically recover from the error state to the normal state.

**Port Error Recovery Timeout**

Range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure RSTP port, as shown in Figure 267.

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	<input type="checkbox"/>	<>		<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Specific	5	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Specific	10	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Submit Reset

Figure 267 Configure RSTP Port

**STP Enabled**

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP/RSTP on ports.



**Caution:**

- RSTP port and port channel are mutually exclusive. A RSTP port cannot be added to a port channel; a port in a port channel cannot be configured as a RSTP port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, a RSTP port cannot be configured as DRP-Port/DT-Ring-Port ring port, or DRP-Port/DT-Ring-Port backup port; DRP-Port/DT-Ring-Port ring port, and DRP-Port/DT-Ring-Port backup port cannot be configured as a RSTP port.
- It is not recommended that ports in an isolation group are configured as RSTP ports at the same time, and RSTP ports cannot be added to an isolation group

**Path Cost**

Options: Auto/Specific (1~200000000)

Default: Auto

Description: The path cost of a port is used to calculate the best path. The value of the

parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of the path cost parameter. To configure the value manually, select No for Cost Count.

**Priority**

Range: 0~240. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

**Admin Edge**

Options: Non-Edge/Edge

Default: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge port can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

**Auto Edge**

Options: Enable/Disable

Default: Enable

Function: Specify whether to enable the automatic detection function of an edge port.

**Restricted Role**

Options: Enable/Disable

Default: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

**Restricted TCN**

Options: Enable/Disable

Default: Disable

Function: A port with restricted TCN will not actively send TCN messages.

**BPDU Guard**

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

**Point-to-point**

Options: Auto/Forced True/Forced False

Default: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: **Auto** indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link and forced sharing refers that a link connected to a port is a shared link.

**20.4.6 Typical Configuration Example**

The priorities of Switch A, B, and C are 0, 4096, and 8192. Path costs of links are 4, 5, and 10, as shown in Figure 268

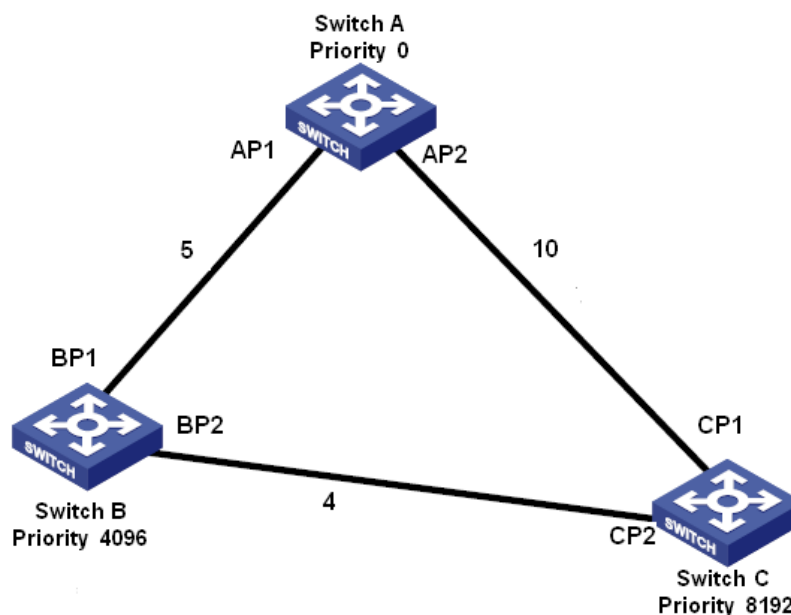


Figure 268 RSTP Configuration Example

Configuration on Switch A:

1. Set bridge priority to 0 and time parameters to default values, as shown in Figure 266.
2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 267.

Configuration on Switch B:

1. Set bridge priority to 4096 and time parameters to default values, as shown in Figure 266.
2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 267.

Configuration on Switch C:

1. Set bridge priority to 8192 and time parameters to default values, as shown in Figure 266.
2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 267.

- The priority of Switch A is 0 and its root ID is the smallest. Therefore, Switch A is the root bridge.
- The path cost from AP1 to BP1 is 5 and that from AP2 to BP2 is 14. Therefore, BP1 is the root port.
- The path cost from AP1 to CP2 is 9 and that from AP2 to CP1 is 10. Therefore, CP2 is the root port and BP2 is the designated port.

## 20.5 MSTP Configuration

### 20.5.1 Introduction

Although RSTP achieves rapid convergence, it also has the following defect just as the STP: all bridges in the LAN share one spanning tree and packets of all VLANs are forwarded along the spanning tree. As shown in Figure 269, certain configurations may block the link between switch A and switch C. Because switch B and switch D are not in VLAN 1, they cannot forward the packets of VLAN 1. As a result, the VLAN 1 port of switch A cannot communicate with that of switch C.



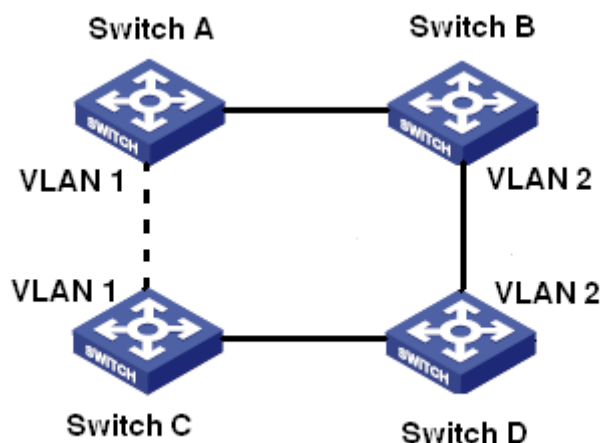


Figure 269 RSTP Disadvantage

To solve this problem, the Multiple Spanning Tree Protocol (MSTP) came into being. It achieves both rapid convergence and separate forwarding paths for the traffic of different VLANs, providing a better load sharing mechanism for redundant links.

MSTP maps one or multiple VLANs into one instance. Switches with the same configuration form a region. Each region contains multiple mutually independent spanning trees. The region serves as a switch node. It participates in the calculation with other regions based on the spanning tree algorithm, calculating an overall spanning tree. Based on this algorithm, the network in Figure 269 forms the topology shown in Figure 270. Both switch A and switch C are in Region1. No link is blocked because the region contains no loops. This is the same with Region2. Region1 and Region2 are similar to switch nodes. These two "switches" form a loop. Therefore, a link should be blocked.

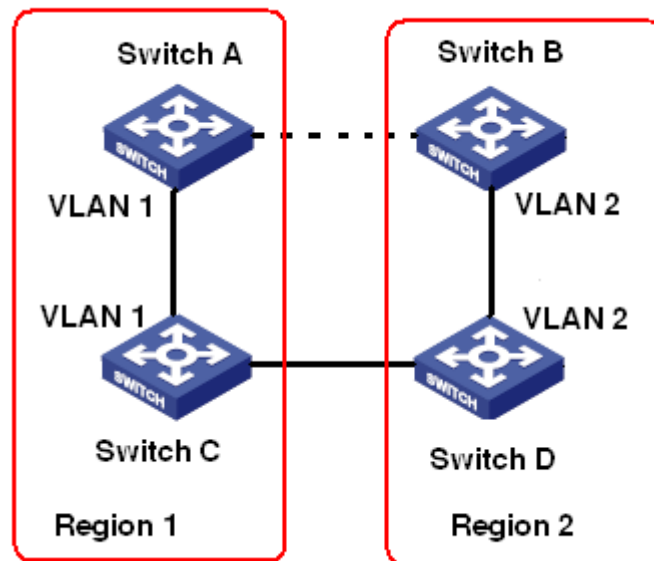


Figure 270 MSTP Topology

### 20.5.2 Basic Concepts

Learn MSTP concepts based on Figure 271 and Figure 274.

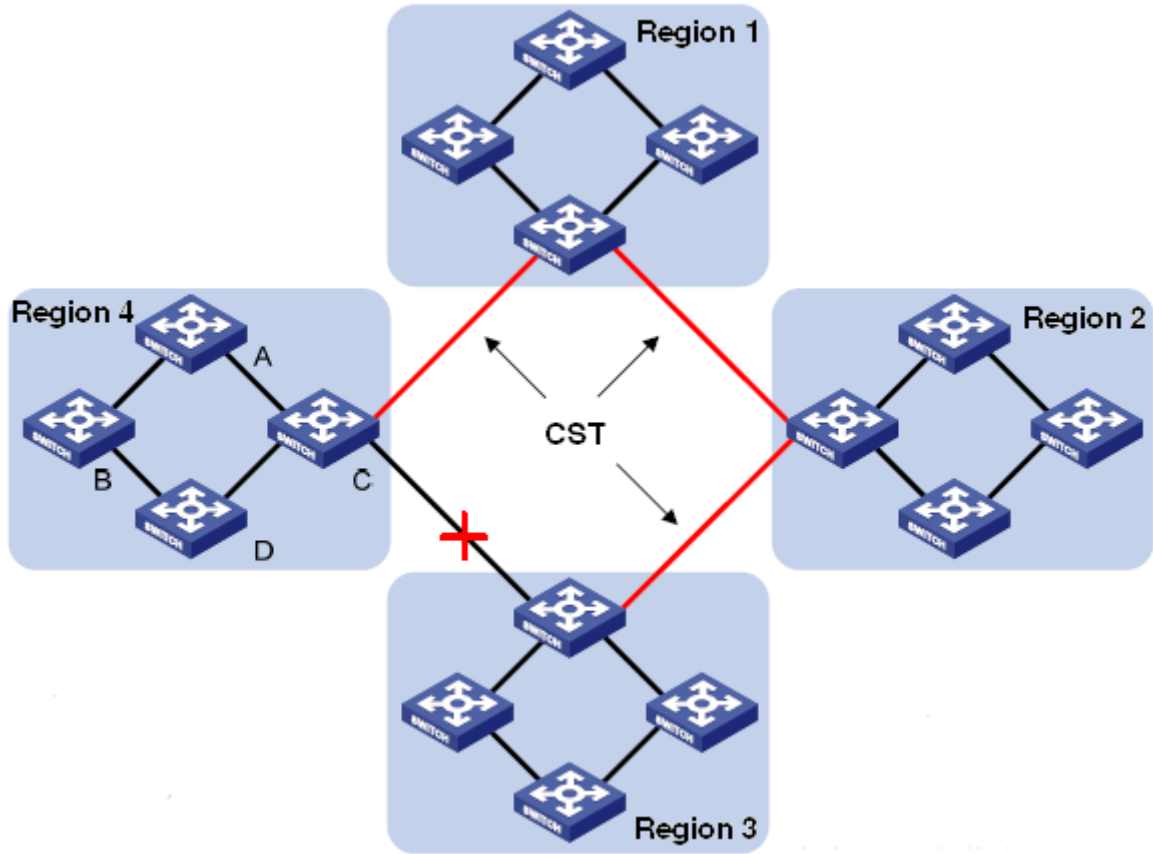


Figure 271 MSTP Concepts

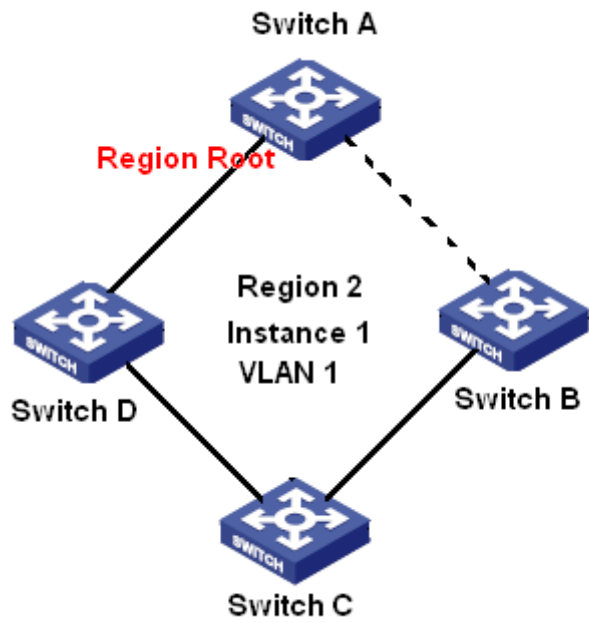


Figure 272 VLAN 1 Mapping to Instance 1

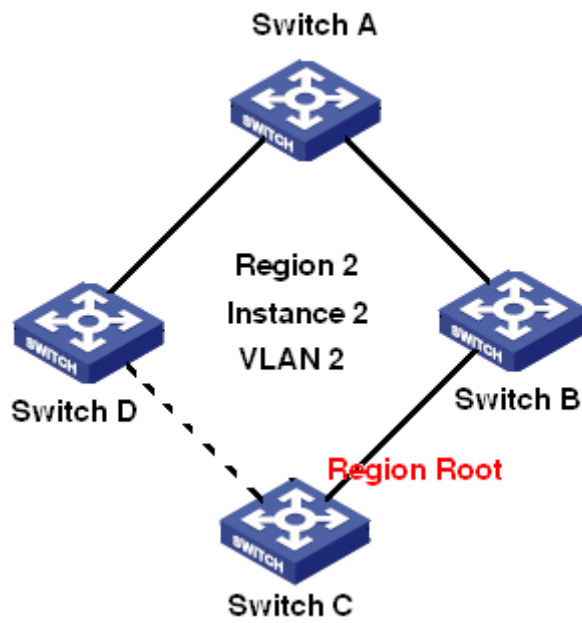


Figure 273 VLAN2 Mapping to Instance 2

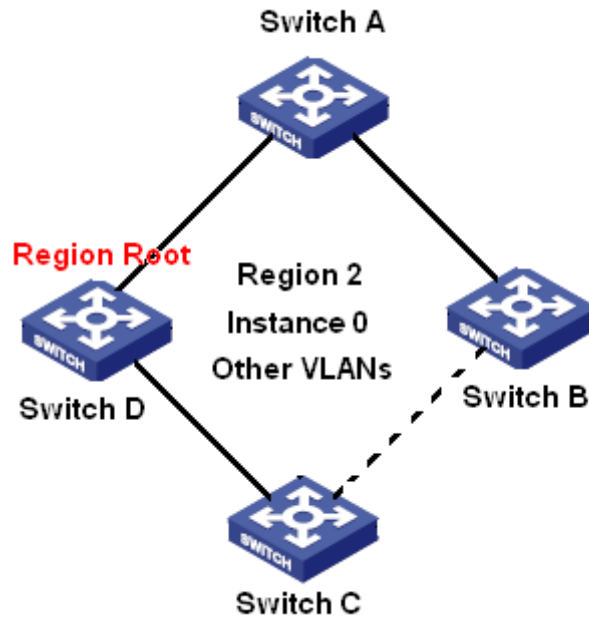


Figure 274 Other VLAN Mapping to Instance 0

Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 272 and Figure 273 ) or multiple VLANs with the same topology (as shown in Figure 274 ) can be mapped to one instance; that is, one VLAN can form a spanning tree and multiple VLANs can share one spanning tree. Different instances are mapped to different spanning trees. Instance 0 is the spanning tree for the devices of all regions, while the other instances are the spanning trees for the devices of a specific region.

Multiple Spanning Tree Region (MST region): Switches with the same MSTP region name, revision level, and VLAN-to-instance mapping are in the same MST region. As shown in Figure 271 , Region1, Region2, Region3, and Region4 are four different MST regions.

VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 271 , VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 272; VLAN 2 is mapped to instance 2, as shown in Figure 273. The other VLANs are mapped to instance 0, as shown in Figure 274.

Common and Internal Spanning Tree (CIST): indicates instance 0, that is, the spanning tree covering all the devices on a switching network. As shown in Figure 271 , the CIST comprises IST and CST.

Internal Spanning Tree (IST): indicates the CIST segment in the MST region, that is, instance 0 of each region, as shown in Figure 274.

**Common Spanning Tree (CST):** indicates the spanning tree connecting all MST regions in a switching network. If each MST region is a device node, the CST is the spanning tree calculated based on STP/RSTP by these device nodes. As shown in Figure 271, the red lines indicate the spanning tree.

**MSTI (Multiple Spanning Tree Instance):** one MST region can form multiple spanning trees and they are independent of each other. Each spanning tree is a MSTI, as shown in Figure 272 and Figure 273. IST is also a special MSTI.

**Common root:** indicates the root bridge of the CIST. The switch with the smallest root bridge ID in a network is the common root.

In an MST region, spanning trees have different topologies, and their regional roots can also be different. As shown in Figure 272, Figure 273, and Figure 274, the three instances have different regional roots. The root bridge of the MSTI is calculated based on STP/RSTP in the current MST region. The root bridge of the IST is the device that is connected to another MST region and selected based on the priority information received.

**Boundary port:** indicates the port that connects an MST region to another MST region, STP running region, or RSTP running region.

**Port state:** A port can be in either of the following states based on whether it is learning MAC addresses and forwarding traffic.

**Forwarding state:** indicates that a port learns MAC addresses and forwards traffic.

**Learning state:** indicates that a port learns MAC addresses but does not forward traffic.

**Discarding state:** indicates that a port neither learns MAC addresses nor forwards traffic.

**Root port:** indicates the best port from a non-root bridge to the root bridge, that is, the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port. The root port can be in forwarding, learning, or discarding state.

**Designated port:** indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports. The designated port can be in forwarding, learning, or discarding state.

**Master port:** indicates the port that connects an MST region to the common root. The port is

in the shortest path to the common root. From the CST, the master port is the root port of a region (as a node). The master port is a special boundary port. It is the root port for the CIST and master port for other instances. The master port can be in forwarding, learning, or discarding state.

Alternate port: indicates the backup port of the root port or master port. When the root port or master port fails, the alternate port becomes the new root port or master port. The master port can only be in discarding state.

Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the designated port and forwards data without any delay. The backup port can only be in discarding state.

### 20.5.3 MSTP Implementation

MSTP divides a network into multiple MST regions. CST is calculated between regions. Multiple spanning trees are calculated in a region. Each spanning tree is an MSTI. Instance 0 is the IST, and other instances are MSTIs.

#### 1. CIST calculation

- A device sends and receives BPDU packets. Based on the comparison of MSTP configuration messages, the device with the highest priority is selected as the common root of the CIST.
- An IST is calculated in each MST region.
- Each MST region is considered as a single device and CST is calculated between regions.
- CST and IST constitute the CIST of the entire network.

#### 2. MSTI calculation

In an MST region, MSTP generates different spanning trees for VLANs based on the mapping between VLANs and spanning trees. Each spanning tree is calculated independently. The calculation process is similar to that in STP.

In an MST region, VLAN packets are forwarded along corresponding MSTIs. Between MST regions, VLAN packets are forwarded along the CST.

### 20.5.4 Web Configuration

1. Set the time parameters of the network bridge, as shown in Figure 275.

**STP Bridge Configuration**

**Global Settings**

Global Enable:

---

**Basic Settings**

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

---

**Advanced Settings**

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input type="text"/>

Figure 275 Setting Time Parameters of the Network Bridge

#### Global Enable

Options: Enable/Disable

Default: Disable

Function: Disable or enable spanning tree.



**Caution:**

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

### Protocol Priority

Options: MSTP/RSTP/STP

Default: MSTP

Function: Select the spanning tree protocol.

### Bridge Priority

Range: 0~61440. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

### Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

### Forward Delay

Range: 4~30s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

### Max Age

Range: 6~40s

Default: 20s

Function: Maximum duration that a BPDU can be saved on a device.

Description: If the value of message age in the BPDU is larger than the specified value, then the BPDU is discarded.



#### Caution:

- The values of Forward Delay Time, Hello Time and Max Age Time should meet the following requirements:  $2 * (\text{Forward Delay Time} - 1.0 \text{ seconds}) \geq \text{Max Age Time}$ ;  $\text{Max Age Time} \geq 2 * (\text{Hello Time} + 1.0 \text{ seconds})$ .
-



- 
- The default setting is recommended.
- 

### Maximum Hop Count

Range: 6~40

Default: 20

Function: Configure the maximum hops of MST region. The maximum hops of MST region limit the scale of MST region; the maximum number of hops of regional root is the maximum number of hops of MST region.

Description: Starting from the root bridge of spanning tree in MST region, the hop number deducts 1 when the BPDU passes through a device in the region. Device drops the BPDU with the hop number of 0.



#### Caution:

- Only the maximum hop configuration of root bridge in MST region is valid. Non-root bridge device adopts the maximum hop configuration of root bridge.
  - The default setting is recommended.
- 

### Transmit Hold Count

Range: 1~10

Default: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

### Edge Port BPDU Filtering

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

### Edge Port BPDU Guard

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down

when receiving BPDU packets.

**Port Error Recovery**

Options: Enable/Disable

Default: Disable

Function: Control whether a port can automatically recover from the error state to the normal state.

**Port Error Recovery Timeout**

Range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure MSTI mapping, as shown in Figure 276.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	Region
Configuration Revision	0

---

MSTI Mapping

MSTI	VLANs Mapped	
MSTI1	10	↑ ↓
MSTI2		↑ ↓
MSTI3	30	↑ ↓
MSTI4	40	↑ ↓
MSTI5	11-15, 25	↑ ↓
MSTI6		↑ ↓
MSTI7		↑ ↓

Figure 276 Configure MSTI Mapping

**Configuration Name**

Range: 1-32 characters

Default: device MAC address

Function: Configure the name of MST region.

**Configuration Revision**

Options: 0~65535

Default: 0

Function: Configure the revision parameter of MSTP region.

Description: Revision parameter, MST region name, and VLAN mapping table codetermines the MST region that the device belongs to. When all configurations are the same, the devices are in same MST region.

**VLANs Mapped**

Range: 1~4094

Function: Configure the VLAN mapping table in MST region. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

Description: By default, all VLANs map to instance 0. One VLAN maps to only one spanning tree instance. If a VLAN with an existing mapping is mapped to another instance, the previous mapping is cancelled. If the mapping between the designated VLAN and instance is deleted, this VLAN will be mapped to instance 0.

3. Configure the bridge priority of the switch in designated instance, as shown in Figure 277.

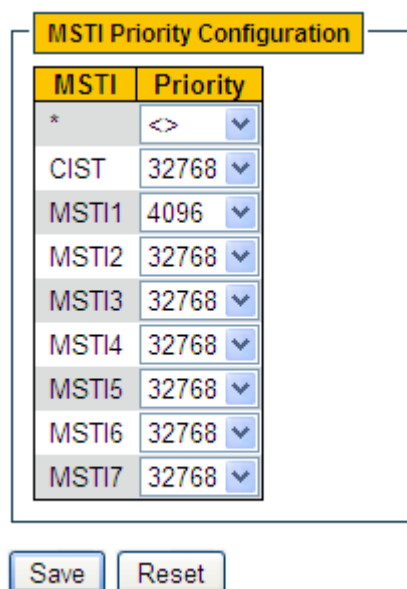


Figure 277 Configuring Bridge Priority in Designated Instance

**Priority**

Range: 0~61440 with the step length of 4096

Default: 32768

Function: Configure the bridge priority of the switch in designated instance.

Description: The bridge priority determines whether the switch can be elected to regional root of spanning tree instance. The smaller value is, the higher priority is. By setting a lower priority, a certain device can be designated to root bridge of spanning tree. The MSTP-enabled device can be configured with different priorities in different spanning tree instance.

Click <Save> to make current configurations take effect.

4. Configure CIST ports, as shown in Figure 278.

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	<input type="checkbox"/>	<>		<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Specific	5	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Specific	10	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Figure 278 Configure CIST Ports

### STP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP/RSTP on ports.



**Caution:**

- MSTP port and port channel are mutually exclusive. A MSTP port cannot be added to a port channel; a port in a port channel cannot be configured as a MSTP port.
- It is not recommended that ports in an isolation group are configured as MSTP ports at the same time, and MSTP ports cannot be added to an isolation group

**Path Cost**

Options: Auto/Specific (1~200000000)

Default: Auto

Description: The path cost of a port is used to calculate the best path. The value of the parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of the path cost parameter. To configure the value manually, select No for Cost Count.

**Priority**

Range: 0~240. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

**Admin Edge**

Options: Non-Edge/Edge

Default: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

**Auto Edge**

Options: Enable/Disable

Default: Enable

Function: Whether to enable the automatic detection function of an edge port.

**Restricted Role**

Options: Enable/Disable

Default: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

**Restricted TCN**

Options: Enable/Disable

Default: Disable

Function: A port with restricted TCN will not actively send TCN messages.

**BPDU Guard**

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

**Point-to-point**

Options: Auto/Forced True/Forced False

Default: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: Auto indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link, and forced sharing refers that a link connected to a port is a shared link.

5. Configure MSTI ports, as shown in Figure 279.



Figure 279 Select MSTI

**Select MSTI**

Range: MST1~MST7

Default: MST1

Function: Select a MSTI, click <Get> to enter the MSTI ports configuration page, as shown in following figure.

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<> ▼	<> ▼
1	Auto ▼	128 ▼
2	Auto ▼	128 ▼
3	Auto ▼	128 ▼
4	Auto ▼	128 ▼
5	Auto ▼	128 ▼
6	Auto ▼	128 ▼
7	Auto ▼	128 ▼
8	Auto ▼	128 ▼
9	Auto ▼	128 ▼
10	Auto ▼	128 ▼
11	Auto ▼	128 ▼
12	Auto ▼	128 ▼

Figure 280 Configure MSTI Ports

**Path Cost**

Options: Auto/Specific (1~200000000)

Default: Auto

Function: Configure the path cost of the port in the designated instance.

Description: Port path cost is used to calculate the optimum path. This parameter depends on bandwidth. The bigger bandwidth is, the lower cost is. Changing port path costs can change the transmission path between the device and root bridge, thereby changing port role. The MSTP-enabled port can be configured with different path costs in different spanning tree instances.

**Priority**

Range: 0~240. The step is 16.

Default: 128

Function: Configure the priority of the port in the designated instance.

Description: Port priority determines whether it will be elected to root port. In the same condition, the port with lower priority will be elected to root port. The MSTP-enabled ports

can be configured with different priorities and play different port roles in different spanning tree instances.

6. View bridge status, as shown in Figure 281.

**STP Bridges**

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
<u>CIST</u>	32768.00-01-C1-00-00-00	32768.00-01-C1-00-00-00	-	0	Steady	-
<u>MSTI1</u>	32769.00-01-C1-00-00-00	32769.00-01-C1-00-00-00	-	0	Steady	-
<u>MSTI3</u>	32771.00-01-C1-00-00-00	32771.00-01-C1-00-00-00	-	0	Steady	-
<u>MSTI4</u>	32772.00-01-C1-00-00-00	32772.00-01-C1-00-00-00	-	0	Steady	-
<u>MSTI5</u>	32773.00-01-C1-00-00-00	32773.00-01-C1-00-00-00	-	0	Steady	-

Figure 281 View Bridge Status

7. View STP ports status, as shown in Figure 282.

**STP Port Status**

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 01:03:13
2	DesignatedPort	Forwarding	0d 00:03:32
3	BackupPort	Discarding	0d 00:03:32
4	Disabled	Discarding	-
5	Non-STP	Discarding	-
6	Non-STP	Discarding	-
7	Non-STP	Discarding	-
8	Non-STP	Discarding	-
9	Non-STP	Discarding	-
10	Non-STP	Discarding	-
11	Non-STP	Discarding	-
12	Non-STP	Discarding	-

Figure 282 View STP Ports Status

8. View STP ports packets statistics, as shown in Figure 283.

**STP Statistics**

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1960	1180	0	0	0	0	0	0	0	0
2	164	0	0	0	3	0	0	0	0	0
3	3	0	0	0	164	0	0	0	0	0

Figure 283 View STP Ports Packets Statistics

**20.5.5 Typical Configuration Example**

As shown in Figure 284, Switch A, B, C, and D belong to the same MST region. The VLANs



marked in red indicate the VLAN packets can be transmitted through the links. After configurations are completed, VLAN packets can be forwarded along different spanning tree instances. VLAN 10 packets are forwarded along instance 1 and the root bridge of instance 1 is Switch A; VLAN 30 packets are forwarded along instance 3 and the root bridge of instance 3 is Switch B. VLAN 40 packets are forwarded along instance 4 and the root bridge of instance 4 is Switch C. VLAN 20 packets are forwarded along instance 0 and the root bridge of instance 0 is Switch B.

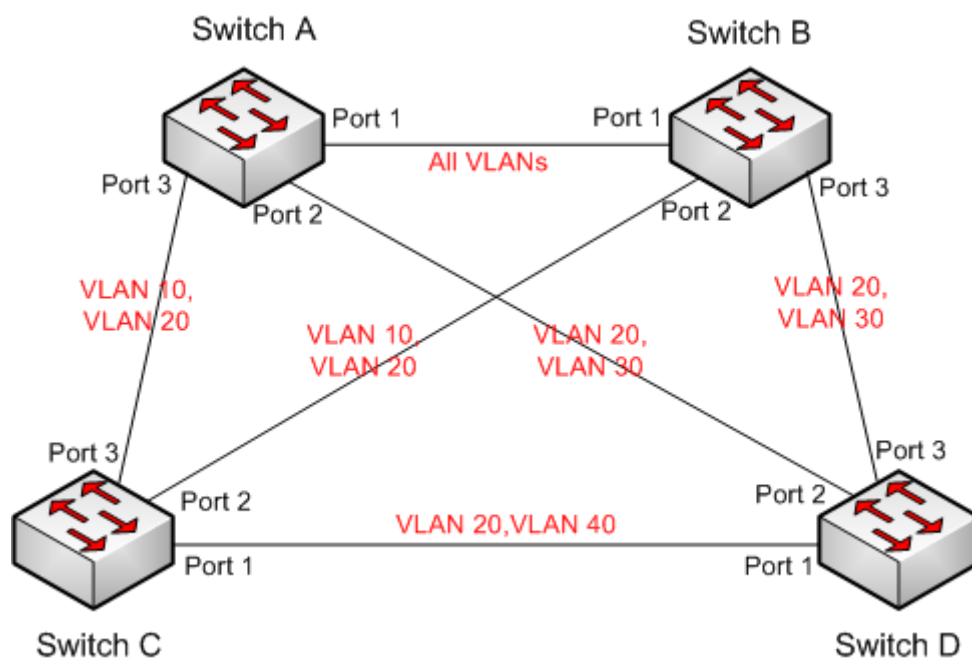


Figure 284 MSTP Typical Configuration Example

**Configuration on Switch A:**

1. Create VLAN 10, 20, and 30 on Switch A; set the ports and allow the packets of corresponding VLANs to pass through.
2. Enable global MSTP protocol, as shown in Figure 275.
3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 276.
4. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 276.
5. Set the switch bridge priority in MSTI 1 to 4096, and keep default priority in other instances, as shown in Figure 277.

**Configuration on Switch B:**

6. Create VLAN 10, 20, and 30 on Switch B; set the ports and allow the packets of corresponding VLANs to pass through.
7. Enable global MSTP protocol, as shown in Figure 275.
8. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 276.
9. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 276.
10. Set switch bridge priority in MSTI 3 and MSTI 0 to 4096, and keep default priority in other instances, as shown in Figure 277.

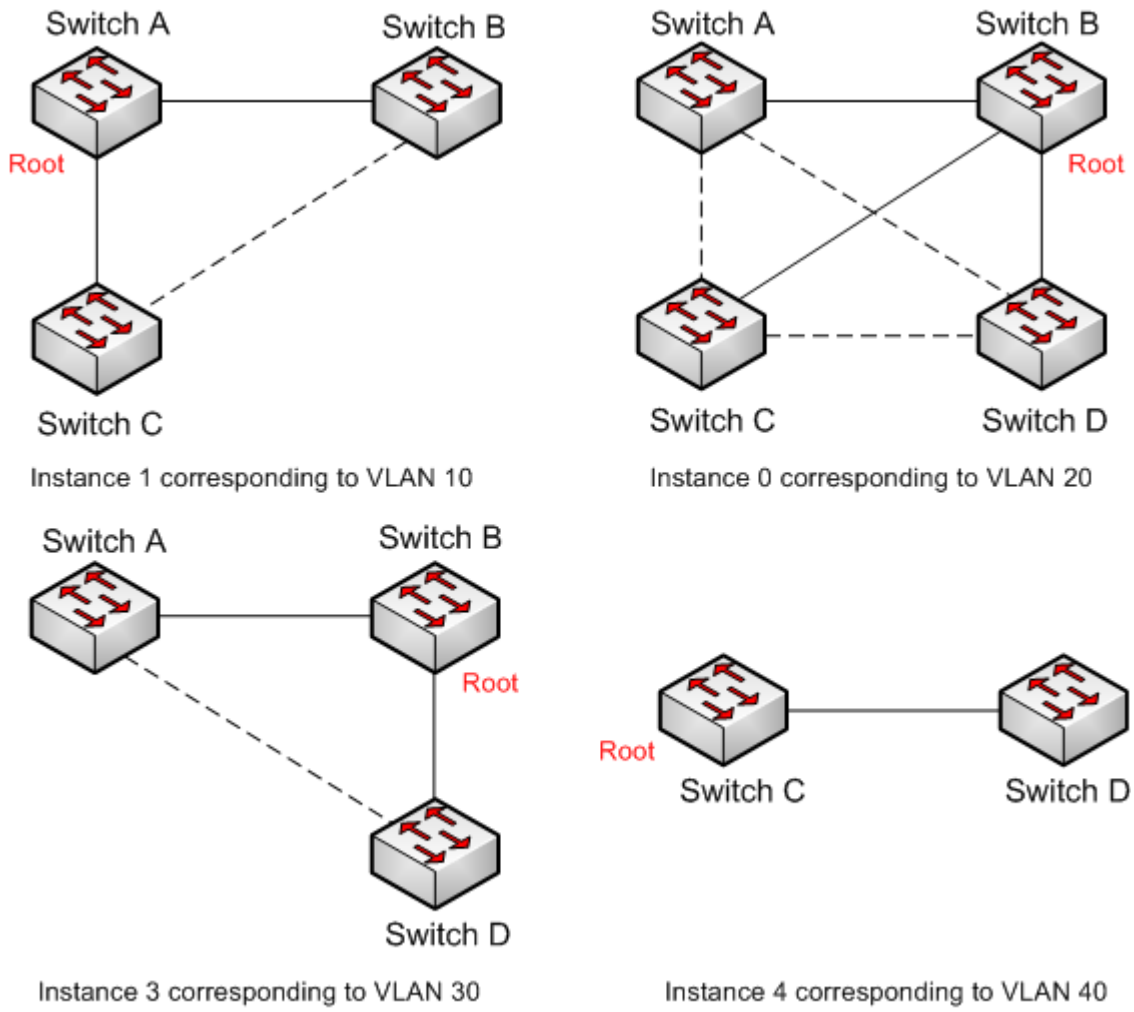
#### **Configuration on Switch C:**

11. Create VLAN 10, 20, and 40 on Switch C; set the ports and allow the packets of corresponding VLANs to pass through.
12. Enable global MSTP protocol, as shown in Figure 275.
13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 276.
14. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 276.
15. Set switch bridge priority in MSTI 4 to 4096, and keep default priority in other instances, as shown in Figure 277.

#### **Configuration on Switch D:**

16. Create VLAN 20, 30, and 40 on Switch D; set the ports and allow the packets of corresponding VLANs to pass through.
17. Enable global MSTP protocol, as shown in Figure 275.
18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 276.
19. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 276.

When MSTP calculation is completed, the MSTI of each VLAN is as follows:



.....Blocked link through MSTP calculation

Figure 285 Spanning Tree Instance of each VLAN

## 21 Alarm

### 21.1 Introduction

This series switches support the following types of alarms:

- Power alarm: If the function is enabled, then an alarm will be generated for a single power input.
- Memory/CPU Usage Alarm: If this function is enabled, an alarm is generated when the CPU / memory usage exceeds the specified threshold.
- IP/MAC conflict alarm: If the function is enabled, then an alarm will be triggered for an IP/MAC conflict.
- Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.
- Ring alarm: If this function is enabled, an alarm is triggered when the ring is open.
- CRC and Packet Loss alarm: If this function is enabled, an alarm is generated when the number of CRC error / packet loss of a port exceeds the specified threshold.
- Port Rate alarm: If this function is enabled, an alarm is generated when the incoming / outgoing traffic rate of a port exceeds the specified threshold.
- SFP Power Alarm;



**Caution:**

Only the master station of a DT ring and the root of a DRP support the ring alarm function.

### 21.2 Web Configuration

1. Configure and display power alarm, mem/cpu usage alarm, as shown in Figure 286.

#### Alarm Configuration

Alarm Type	Enable	Threshold	Margin Value	Status
Power Alarm	<input checked="" type="checkbox"/>	---	---	Power-1: Power Down   Power-2: Power On
Mem Usage Alarm	<input checked="" type="checkbox"/>	85 (50~100)	5 (1~20)	Normal
CPU Usage Alarm	<input checked="" type="checkbox"/>	85 (50~100)	5 (1~20)	Normal

Figure 286 Alarm configuration

#### Power Alarm

Options: Enable/Disable

Default: Disable

Function: Enable/Disable power alarm.

### **Status**

Options: Power On/Power Down

Description: Power On means the power is in connection state and works normally communication. Power Down means the power is disconnected or works abnormally.

### **Mem/CPU Usage Alarm**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable mem usage alarm.

### **Threshold (%)**

Range: 50~100

Default: 85

Function: Set the memory/ CPU usage threshold. When the memory/ CPU usage of the switch is higher than the threshold, an alarm is generated.

Margin Value (%)

Range: 1~20

Default: 5

Function: Set the memory/ CPU usage margin value.

Description: If the memory/ CPU usage fluctuates around the threshold, alarms may be generated and cleared repeatedly. To prevent this phenomenon, you can specify a margin value (5% by default). The alarm will be cleared only if the memory/ CPU usage is lower than the threshold by the margin value or more. For example, the memory usage threshold is set to 60% and the margin value is set to 5%. If the memory usage of the switch is lower than or equal to 60%, no alarm is generated. If the memory usage is higher than 60%, an alarm will be generated. The alarm will be cleared only if the memory usage is equal to or lower than 55%.

Alarm Status

Options: Normal /Alarm

Function: View the memory/ CPU usage status of switch. Alarm means the memory/ CPU usage exceeds the threshold and triggers alarm.

2. Configure and display IP/MAC conflict alarm, as shown in Figure 287.

**IP,MAC Conflict Alarm**

Alarm Name	Alarm Enable	Status	Check Time	
IP,MAC Conflict	<input checked="" type="checkbox"/>	IP:Conflict   Mac:No Conflict	300	180-600 secs

Figure 287 IP/MAC Conflict Alarm

**IP, MAC Conflict**

Options: Enable/Disable

Default: Enable

Function: Enable/Disable IP/MAC conflict alarm.

**Status**

Options: Conflict / No Conflict

Description: When an IP/MAC conflict occurs, Conflicts displayed; otherwise, No Conflicts displayed.

**Check Time**

Range: 180~600s

Default: 300s

Function: Configure the interval for detecting IP/MAC conflicts.

3. Configure and display DT-Ring ring alarm, as shown in Figure 288.

**DT-Ring Alarm Configuration**

Domain ID	Enable	Status
*	<input checked="" type="checkbox"/>	
1	<input checked="" type="checkbox"/>	DT-Ring Close
2	<input checked="" type="checkbox"/>	DT-Ring Open

Figure 288 DT-Ring Alarm

**DT-Ring Alarm Configuration**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable DT-Ring alarm.

**Status**

Options: DT-Ring Close / DT-Ring Open

Description: DT-Ring Close means DT-Ring is closed. DT-Ring Open means DT-Ring is open or in abnormal state.

4. Configure and display DRP ring alarm, as shown in Figure 289.

**DRP Alarm Configuration**

Domain ID	Enable	Status
*	<input checked="" type="checkbox"/>	
1	<input checked="" type="checkbox"/>	DRP Open
2	<input checked="" type="checkbox"/>	DRP Close

Figure 289 DRP Alarm

**DRP Alarm Configuration**

Options: Disable/Enable

Default: Disable

Function: Enable/Disable DRP alarm.

**Status**

Options: DRP Close / DRP Open

Description: DRP Close means DRP is closed. DRP Open means DRP is open or in abnormal state.

5. Configure and display port alarm, as shown in Figure 290.

### Port Alarm Configuration

Port	Enable	Status
*	<input checked="" type="checkbox"/>	
1	<input checked="" type="checkbox"/>	Link Up
2	<input checked="" type="checkbox"/>	Link Down
3	<input checked="" type="checkbox"/>	Link Down
4	<input type="checkbox"/>	---
5	<input type="checkbox"/>	---
6	<input type="checkbox"/>	---
7	<input type="checkbox"/>	---
8	<input type="checkbox"/>	---
9	<input type="checkbox"/>	---
10	<input type="checkbox"/>	---

Figure 290 Port Alarm

### Port Alarm Configuration

Options: Disable/Enable

Default: Disable

Function: Enable/Disable port alarm.

### Status

Options: Link Up/Link Down

Description: Link Up means the port is in connection state and supports normal communication. Link Down means the port is disconnected or in abnormal connection (communication failure).

6. Configure and display CRC and Packet loss alarm, as shown in Figure 291.



CRC and Pkt Loss

Port	CRC			Pkt Loss		
	Enable	Threshold	Status	Enable	Threshold	Status
*	<input type="checkbox"/>	<input type="text"/>	pps	<input type="checkbox"/>	<input type="text"/>	pps
1	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
2	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
3	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
4	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
5	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
6	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
7	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
8	<input checked="" type="checkbox"/>	1	pps Normal	<input checked="" type="checkbox"/>	1	pps Normal
9	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---
10	<input type="checkbox"/>	1	pps ---	<input type="checkbox"/>	1	pps ---

Submit

Figure 291 CRC and Packet loss alarm

**CRC/Pkt Loss Alarm**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable CRC/ Pkt loss alarm.

**Threshold**

Range: 1 to 1000000pps.

Function: Configure the threshold for the port CRC/ Pkt loss alarm.

**Alarm Status**

Options: Alarm/ Normal

Function: View the port CRC/ Pkt loss status. Alarm means the port CRC/ Pkt loss exceeds the threshold and triggers alarm.

7. Configure and display port rate alarm, as shown in Figure 292.

Port Rate Alarm

Port	Input Rate Alarm				Output Rate Alarm			
	Enable	Threshold	Unit	Status	Enable	Threshold	Unit	Status
*	<input type="checkbox"/>		<>		<input type="checkbox"/>		<>	
1	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
2	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
3	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
4	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
5	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
6	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
7	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
8	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
9	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---
10	<input type="checkbox"/>	1	bps	---	<input type="checkbox"/>	1	bps	---

Submit

Figure 292 Port rate alarm

**Input rate alarm/output rate alarm**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable port traffic alarm.

**Threshold**

Range: 1 to 1000000000bps or 1 to 1000000kbps.

Function: Configure the threshold for the port traffic.

**Alarm Status**

Options: Alarm/ Normal

Function: View the port traffic status. Alarm means the incoming / outgoing traffic rate exceeds the threshold and triggers alarm.

8. Configure and display SFP port RX Power alarm, as shown in Figure 293

**Soft Alarm**

Port	Enable	Threshold(-40.0~8.2)	Status
*	<input type="checkbox"/>		dBm
9	<input checked="" type="checkbox"/>	-22.0	dBm <b>Alarm</b>
10	<input type="checkbox"/>	-22.0	dBm ---

**Hard Alarm Mode**

**Hard Alarm Mode**

**Hard Alarm Status**

Port	RX Power Alarm			TX Power Alarm		
	Current Value	High Alarm State	Low Alarm State	Current Value	High Alarm State	Low Alarm State
9	-40.5	Normal	Alarm	-9.6	Normal	Normal

Figure 293 SFP port RX Power alarm

**Software Alarm**

Options: Enable/ Disable

Default: Disable

Function: Enable/ Disable SFP RX power alarm.

**Threshold**

Range: -40~8.2 (unit: dBm)

Default: -22.0dBm

Function: Configure the threshold for the SFP port RX power alarm.

**Alarm Status**

Options: NotSupportDDM/NotExist/Normal/Alarm

Description: software alarm refers to the port receiving optical power alarm, which requires the SFP to support DDM function. If the SFP is not inserted into the port, the status is NotExist. If the SFP is inserted, but DDM is not supported, the status is NotSupportDDM. If a ddm-supported SFP is inserted, the receiving optical power is lower than the threshold, then alarm will be generated, the status is Alarm. If a ddm-supported SFP is inserted, the receiving optical power is not lower than the threshold, then the status is normal.

**Hardware Alarm**

Options: Enable/ Disable

Default: Disable

Function: Enable/ Disable SFP power hardware alarm.

**Alarm Status**

Options: Alarm/ Normal

Function: View the SFP power hardware alarm status. Supports SFP Tx/Rx power alarm, but the SFP Tx power alarm threshold is not configurable.

## 22 Link Check

### 22.1 Introduction

Link check adopts periodic interaction of protocol packets to judge the link connectivity and display the port communication status. In case of a fault, the problem can be found and handled in time.

The port for which link status check is enabled sends link-check packets periodically (every 1s) to check the link status. If the port does not receive a link-check packet from the peer end within the receive timeout period (5s), it indicates that the link is abnormal and the port displays Rx fault state. If the port receives a link-check packet from the peer end and the packet shows that the link-check packet is received from local within the receive timeout period (5s), the port displays the normal state. If the port receives a link-check packet from the peer end but the packet shows that the link-check packet is not received from local within the receive timeout period (5s), the port displays Tx fault state. If the link to the port is down, the port displays link down state.

The port for which link status check is disabled works in passive mode. That is, it does not send a link-check packet in active mode. However, after receiving a link-check packet from the peer end, this port returns a link-check packet immediately to inform the peer end that it has received the link-check packet.

### 22.2 Web Configuration

Configure link check, as shown in Figure 294.

### Link Check Configuration

Port	Enable	Status
*	<input checked="" type="checkbox"/>	
1	<input checked="" type="checkbox"/>	Rx Fault
2	<input checked="" type="checkbox"/>	Normal
3	<input checked="" type="checkbox"/>	Normal
4	<input checked="" type="checkbox"/>	Down
5	<input type="checkbox"/>	---
6	<input type="checkbox"/>	---
7	<input type="checkbox"/>	---
8	<input type="checkbox"/>	---
9	<input type="checkbox"/>	---
10	<input type="checkbox"/>	---

Figure 294 Configure Link Check

#### Enable

Options: Disable/Enable

Default: Disable

Function: Enable/Disable link check on port.



**Caution:**

If the peer device does not support the function, the function shall be disabled on the connected port of the local device.

#### Status

Options: Up/Normal/--/Rx Fault/Tx Fault/Down

Description: If Link Check is enabled on a port and the port sends and receives data normally, Normal is displayed. If the peer end does not receive the detection packets from the device, Tx Fault is displayed. If the device does not receive detection packets from the peer end, Rx Fault is displayed. If port is link down, Down is displayed. If Link Check is not enabled on a port, -- is displayed. At the moment of link check being enabled on a link up port, up is displayed.

## 23 Log

### 23.1 Introduction

The log function mainly records system status, fault, debugging, anomaly, and other information. With appropriate configuration, the switch can upload logs into a Syslog-supported server in real time.

Log contains information about alarms, broadcast storm, reboot, memory, and information about users' operations.

### 23.2 Web Configuration

1. Configure system log, as shown in Figure 295.

**System Log Information** Auto-refresh

Search Level    
 Clearlevel

The total number of entries is:45  
 Start from ID

ID	Level	Time	Message
1	Informational	2015-08-07T15:13:13+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2015-08-07T15:13:15+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to up.
5	Notice	2015-08-07T15:13:17+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2015-08-07T16:37:22+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to down.
7	Notice	2015-08-07T16:37:23+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
8	Notice	2015-08-07T16:37:25+08:00	LINK-UPDOWN: Interface FastEthernet 1/3, changed state to up.
9	Notice	2015-08-07T16:37:26+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
10	Informational	2015-08-07T16:56:59+08:00	Power Alarm: entity id:1 state:Power Down
11	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Link Down
12	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:2 port:FastEthernet 1/2 state:Link Down
13	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:4 port:FastEthernet 1/4 state:Link Down
14	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:5 port:FastEthernet 1/5 state:Link Down
15	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:6 port:FastEthernet 1/6 state:Link Down
16	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:7 port:FastEthernet 1/7 state:Link Down
17	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:8 port:FastEthernet 1/8 state:Link Down
18	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:9 port:FastEthernet 1/9 state:Link Down
19	Informational	2015-08-07T16:57:39+08:00	Power Alarm: entity id:1 state:Disable
20	Informational	2015-08-07T16:57:42+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Disable

Figure 295 Configure System Log

#### Search Level

Options: Error/Warning/Notice/Information/All

Default: all

Function: Select the level of log information to be displayed.

**Clear level**

Options: Error/Warning/Notice/Information/All

Default: all


Function: Select the level of log information to be deleted. Click <Clear> to delete the designated level log information.

**The total number**

Function: Displays the number of logs that meet the query conditions.

**Start from ID**

Function: set the start ID of log entries on the current page. You can click Refresh to update log entries on the current page. 20 log entries can be displayed on each page.

Click  to view log entries on the next page. The start ID of the next page is the ID of the last log entry on the current page.

Click  to view log entries on the previous page.

Click  to view log entries on the last page. The end ID is the ID of the last log entry.

Click  to view log entries on the first page. The start ID is the ID of the first log entry.

2. Upload Log to server in real time, as shown in Figure 296.

**System Log Configuration**

Server Mode	Enabled
Server Address	192.168.0.184
Syslog Level	Informational
Write to Flash	Enabled

Figure 296 Upload Log in Real Time

**Server Mode**

Options: Disable/Enable

Default: Disable

Function: Enable/Disable uploading Log to server in real time.

**Server Address**

Function: Configure the IP address of the server that log information is uploaded to.



**Syslog Level**

Option: Error/Warning/Notice/Information

Default: Information

Function: Select the level of log information to be uploaded to server.

**Write to Flash**

Option: Enabled/Disabled

Default: Disabled

Function: whether to write log to flash or not.

You can install Syslog Server software, for example, Tftp32, on a PC to build a "Syslog Server".

Log information can be displayed in real time on the Syslog Server, as shown in Figure 297.

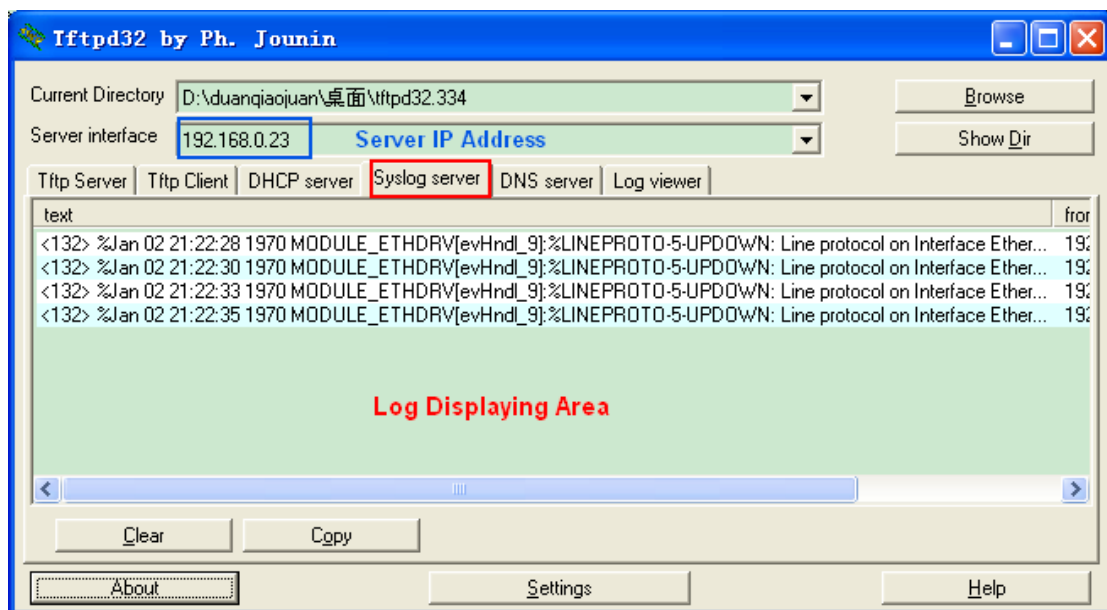


Figure 297 Uploading Log Information in Real Time

## 24 Port Mirroring

### 24.1 Introduction

With port mirroring function, the switch copies all received or transmitted data frames in a port (mirroring source port) to another port (mirroring destination port). The mirroring destination port is connected to a protocol analyzer or RMON monitor for network monitoring, management, and fault diagnosis.

### 24.2 Explanation

A switch supports only one mirroring destination port but multiple source ports.

Multiple source ports can be either in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

The source port and destination port cannot be the same port.



**Caution:**

The dynamic MAC address learning must be disabled on a destination port.

### 24.3 Web Configuration

1. Configure port mirror function, as shown in Figure 298.

#### Mirroring & Remote Mirroring Configuration

Mode	Enabled
Type	Mirror
VLAN ID	200
Reflector Port	Port 1

Figure 298 Configure Port Mirror Function

**Mode**

Options: Enable/Disable

Default: Disable

Function: Enable/Disable port mirror function.

**Type**

Options: Mirror

Function: Use port mirror function.

2. Select the mirroring destination and source port, as shown in Figure 299.

**Port Configuration**

Port	Source	Intermediate	Destination
1	Both	<input type="checkbox"/>	<input type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Rx only	<input type="checkbox"/>	<input type="checkbox"/>
4	Tx only	<input type="checkbox"/>	<input type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
7	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
8	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
9	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
10	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
11	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
12	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
CPU	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Submit    Reset

Figure 299 Select the Mirroring Destination and Source Port

**Source**

Options: Rx only/Tx only /Both

Function: Select the data to be mirrored in the mirroring source port.

Rx only: indicates only the received packets are mirrored in the source port.

Tx only: indicates only the transmitted packets are mirrored in the source port.

Both: indicates both transmitted and received packets are mirrored in the source port.

**Destination**

Function: Select a port to be the mirroring destination port. There is one and only one mirroring destination port.

**24.4 Typical Configuration Example**

As shown in Figure 300, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

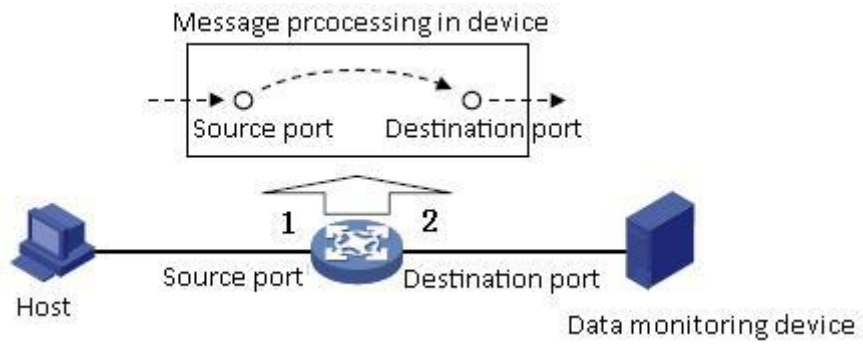


Figure 300 Port Mirroring Example

**Configuration process:**

1. Enable port mirror function, as shown in Figure 298.
2. Set port 2 to the mirroring destination port, port 1 to the mirroring source port and the port mirroring mode to both, as shown in Figure 299.

## 25 Diagnostics

### 25.1 Ping

Users can run the ping command to check whether the device of a specified address is reachable and whether the network connection is faulty during routine system maintenance.

1. Configure ping command, as shown in Figure 301.

**ICMP Ping**

IP Address	192.168.0.184
Ping Length	56
Ping Count	5
Ping Interval	1

Figure 301 Configure Ping Command

#### IP Address

Format: A.B.C.D

Description: Input the IP address of the destination device.

#### Ping Length

Range: 2~1452 bytes

Default: 56 bytes

Function: Specify the length of an ICMP request (excluding the IP and ICMP packet header) for transmission.

#### Ping Count

Range: 1~60

Default: 5

Function: Specify the number of times for sending an ICMP request.

#### Ping Interval

Range: 0~30s

Default: 1s

Function: Specify the interval for sending an ICMP request.

2. View ping output, as shown in Figure 302.

### ICMP Ping Output

```
PING server 192.168.0.184, 56 bytes of data.  
64 bytes from 192.168.0.184: icmp_seq=0, time=0ms  
64 bytes from 192.168.0.184: icmp_seq=1, time=0ms  
64 bytes from 192.168.0.184: icmp_seq=2, time=0ms  
64 bytes from 192.168.0.184: icmp_seq=3, time=0ms  
64 bytes from 192.168.0.184: icmp_seq=4, time=0ms  
Sent 5 packets, received 5 OK, 0 bad
```

[Back](#)

Figure 302 View Ping Output

The output of the ping command includes response of the destination device to each ICMP request packet and packet statistics collected during the running of the ping command.

## Appendix: Acronyms

<b>Acronym</b>	<b>Full Spelling</b>
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
EAPOL	Extensible Authentication Protocol over LAN
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit

LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
NetBIOS	Network Basic Input/Output System
NMS	Network Management Station
NTP	Network Time Protocol
OID	Object Identifier
PCP	Priority Code Point
PD	Powered Device
POE	Power Over Ethernet
PSE	Power Sourcing Equipment
PVLAN	Private VLAN
QCL	QoS Control List
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System



TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VLAN	Virtual Local Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin