

SICOM3005A Industrial Ethernet Switches

Web Operation Manual

Publication Date: Jul. 2014

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 © 2014 Kyland Technology Co., Ltd.

Publication: Kyland Technology Co., Ltd

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

FAX: +86-10-88796678

Email: support@kyland.com

Contents

Preface	1
1. Product Introduction.....	5
1.1 Overview	5
1.2 Software Features	5
2. Switch Access.....	6
2.1 View Types	6
2.2 Console Port Access	7
2.3 Telnet Access.....	10
2.4 Web Access.....	11
3. Device Management.....	14
4. Device Status.....	15
4.1 Basic Information.....	15
4.2 Port Status	15
4.3 Port Statistics.....	16
5. Basic Configuration.....	18
5.1 IP Address	18
5.2 Device Information	19
5.3 Port Configuration	20
5.4 Change Password	22
5.5 Software Update.....	22
5.5.1 Software Update by FTP	22
5.5.2 Software Update by TFTP	27
5.6 Upload & Download.....	29
6. LLDP.....	32
6.1 Introduction.....	32
6.2 Web Configuration.....	32
7. ARP	34
7.1 Introduction.....	34

7.2 Explanation.....	34
7.3 Web Configuration.....	34
8. QoS Configuration	37
8.1 Introduction.....	37
8.2 Principle.....	37
8.3 Web Configuration.....	38
8.4 Typical Configuration Example	41
9. Port Trunk	43
9.1 Introduction.....	43
9.2 Implementation	43
9.3 Explanation.....	44
9.4 Web Configuration.....	44
9.5 Typical Configuration Example	46
10. MAC Aging Time	47
10.1 Introduction.....	47
10.2 Web Configuration.....	47
11. Port Rate.....	48
11.1 Introduction	48
11.2 Implementation	48
11.3 Web Configuration	49
11.4 Typical Configuration Example	50
12. Redundant	51
12.1 DT-Ring	51
12.1.1 Introduction	51
12.1.2 Concepts	51
12.1.3 Implementation.....	52
12.1.4 Explanation	56
12.1.5 Web Configuration.....	56
12.1.6 Typical Configuration Example.....	61
12.2 RSTP/STP Configuration.....	62

12.2.1 Introduction	62
12.2.2 Basic Concepts	62
12.2.3 Configuration BPDU	63
12.2.4 Implementation.....	63
12.2.5 Web Configuration.....	65
12.2.6 Typical Configuration Example	68
12.3 RSTP/STP Transparent Transmission	69
12.3.1 Introduction	69
12.3.2 Web Configuration.....	70
12.3.3 Typical Configuration Example	70
12.4 DRP	71
12.4.1 Overview	71
12.4.2 Concepts	72
12.4.3 Implementation.....	73
12.4.4 Description	77
12.5 DHP	77
12.5.1 Overview	77
12.5.2 Concepts	78
12.5.3 Implementation.....	79
12.5.4 Web Configuration.....	80
12.5.5 Typical Configuration Example	83
13. Multicast	84
13.1 GMRP.....	84
13.1.1 GARP Introduction	84
13.1.2 GMRP Protocol	85
13.1.3 Explanation	85
13.1.4 Web Configuration.....	86
13.1.5 Typical Configuration Example	89
13.2 Static FDB Multicast	91
13.2.1 Introduction	91

13.2.2 Web Configuration.....	91
13.3 IGMP Snooping	93
13.3.1 Introduction	93
13.3.2 Basic Concepts	93
13.3.3 Principle	93
13.3.4 Web Configuration.....	94
13.3.5 Typical Application Example	95
14. Diagnosis.....	97
14.1 Port Mirroring.....	97
14.1.1 Introduction	97
14.1.2 Explanation	97
14.1.3 Web Configuration.....	97
14.1.4 Typical Configuration Example	98
14.2 Link Check.....	99
14.2.1 Introduction	99
14.2.2 Web Configuration.....	99
14.3 Virtual Cable Tester	100
14.3.1 Introduction	100
14.3.2 Implementation.....	100
14.3.3 Web Configuration.....	101
15. SNTP	103
15.1 Introduction.....	103
15.2 Web Configuration.....	103
16. Security.....	106
16.1 SSH.....	106
16.1.1 Introduction	106
16.1.2 Secret Key.....	106
16.1.3 Implementation.....	106
16.1.4 Web Configuration.....	107
16.1.5 Typical Configuration Example	111

16.2 Dot1x	119
16.2.1 Introduction	119
16.2.2 Web Configuration.....	119
16.2.3 Typical Configuration Example	122
16.3 Port Security.....	123
16.3.1 Introduction	123
16.3.2 Web Configuration.....	123
16.3.3 Typical Configuration Example	125
16.4 AAA Configure	125
16.4.1 Introduction	125
16.4.2 Implementation.....	125
16.4.3 Web Configuration.....	126
16.5 TACACS+ Configure.....	127
16.5.1 Introduction	127
16.5.2 Web Configuration.....	128
16.5.3 Typical Configuration Example	130
16.6 SSL Configure	131
16.6.1 Introduction	131
16.6.2 Web Configuration.....	131
17. VLAN	133
17.1 VLAN Configuration.....	133
17.1.1 Introduction	133
17.1.2 Principle	133
17.1.3 Port-based VLAN	134
17.1.4 Web Configuration.....	135
17.1.5 Typical Configuration Example	138
17.2 PVLAN.....	139
17.2.1 Introduction	139
17.2.2 Web Configuration.....	140
17.2.3 Typical Configuration Example	142

17.3 GVRP	143
17.3.1 Introduction	143
17.3.2 Port Mode.....	143
17.3.3 Web Configuration.....	144
17.3.4 Typical Configuration Example.....	146
18. RMON.....	147
18.1 Introduction.....	147
18.2 RMON Group	147
18.3 Web Configuration.....	148
19. Unicast Configuration	154
19.1 Introduction.....	154
19.2 Web Configuration	154
20. Alarm and Syslog.....	156
20.1 Alarm	156
20.1.1 Introduction	156
20.1.2 Web Configuration.....	156
20.2 Syslog.....	158
20.2.1 Introduction	158
20.2.2 Web Configuration.....	159
21. SNMP	163
21.1 SNMPv2	163
21.1.1 Introduction	163
21.1.2 Implementation.....	163
21.1.3 Explanation	164
21.1.4 MIB Introduction	164
21.1.5 Web Configuration.....	165
21.1.6 Typical Configuration Example.....	167
21.2 SNMPv3	168
21.2.1 Introduction	168
21.2.2 Implementation.....	168

21.2.3 Web Configuration.....	169
21.2.4 Typical Configuration Example.....	172
22. DHCP	174
22.1 DHCP Server Configuration	175
22.1.1 Introduction	175
22.1.2 DHCP Address Pool.....	175
22.1.3 Web Configuration.....	176
22.1.4 Typical Configuration Example.....	182
22.2 DHCP Snooping	184
22.2.1 Introduction	184
22.2.2 Web Configuration.....	185
22.2.3 Typical Configuration Example.....	186
22.3 Option 82 Configuration.....	187
22.3.1 DHCP Snooping Supports Option 82 Function	188
22.3.2 DHCP Server Supports Option 82 Function	191
23. Serial Card Management.....	194
24. Appendix: Acronyms	195

Preface

This manual mainly introduces the access methods and software features of SICOM3005A industrial Ethernet switches, and introduces the Web configuration methods in detail.

Content Structure

The manual contains the following contents:

Main Content	Explanation
1. Product Introduction	<ul style="list-style-type: none"> ➤ Overview ➤ Software Features
2. Switch access	<ul style="list-style-type: none"> ➤ View Type ➤ Access switch by Console port ➤ Access switch by Telnet ➤ Access switch by Web
3. Device Management	<ul style="list-style-type: none"> ➤ Reboot ➤ Logout
4. Device status	<ul style="list-style-type: none"> ➤ Basic Information ➤ Port Status ➤ Port Statistics
5. Basic configuration	<ul style="list-style-type: none"> ➤ IP address ➤ Device Information ➤ Port Configuration ➤ Change Password ➤ Software Update(FTP, TFTP) ➤ Upload & Download
6. LLDP	
7. ARP	
8. QoS configuration	
9. Port Trunk	
10. MAC Aging Time	

11. Port Rate	
12. Redundant	<ul style="list-style-type: none"> ➤ DT-Ring Configuration ➤ RSTP/STP Configuration ➤ RSTP/STP Transparent Transmission ➤ DRP
13. Multicast	<ul style="list-style-type: none"> ➤ GMRP ➤ Static FDB Multicast ➤ IGMP Snooping
14. Diagnosis	<ul style="list-style-type: none"> ➤ Port Mirroring ➤ Link Check ➤ Virtual Cable Tester
15. SNTP	
16. Security	<ul style="list-style-type: none"> ➤ SSH ➤ Dot1x ➤ Port Security ➤ AAA Configuration ➤ TACACS+ Information ➤ SSL Configuration
17. VLAN	<ul style="list-style-type: none"> ➤ VLAN Configuration ➤ PVLAN ➤ GVRP
18. RMON	
19. Unicast Configuration	
20. Alarm and Syslog	<ul style="list-style-type: none"> ➤ Alarm ➤ Syslog
21. SNMP	<ul style="list-style-type: none"> ➤ SNMP v2 ➤ SNMP v3
22. DHCP	<ul style="list-style-type: none"> ➤ DHCP server configuration ➤ DHCP Snooping

➤ Option82 configuration

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 group. For example, {IP address, MAC address} means that IP address and MAC address are a group 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 submenu [All programs], then click the submenu [Accessories].
/	Select one from two or more options that are separated by "/". For example "Add/Subtract" means addition or subtraction.
~	It means a range. For example, "1~255" means a range from 1 to 255

2. CLI conventions

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

3. Symbol conventions

Symbol	Explanation
 Caution	The matters need attention during the operation and configuration, and it is a supplement to the operation content
 Note	Necessary explanations to operation contents
 Warning	The matters that call for special attention. Incorrect operation might cause data loss or damage to devices

Product Documents

The documents of SICOM3005A Switching Serial Port Server include:

Document	Description
SICOM3005A Switching Serial Port Server Hardware Installation Manual	Describes the appearance, structure, hardware specifications, and mounting and dismounting methods of SICOM3005A .
SICOM3005A Industrial Ethernet Switches Web Operation Manual	Introduces the switch software functions, Web configuration methods and steps of all functions.
SICOM3005A Serial Port Server Web Operation Manual	Describes the software functions, configuration methods, and configuration steps of SICOM3005A Serial Port Server.

Document Obtainment

Product documents can be obtained by:

- CD shipped with the device.
- Kyland website: www.kyland.com.

1. Product Introduction

1.1 Overview

The switch is green DIN-rail industrial Ethernet switches applied in the wind power, distribution network automation, power, and intelligent transportation industries. The switch supports IEC62439-6 and VCT. The Reset button allows one-touch recovery. The brilliant performance of the switches satisfies the needs of many industries.

1.2 Software Features

This series switches provide abundant software features, satisfying customers' various requirements.

- Redundancy protocols: RSTP/STP, DT-Ring, and IEC62439-6
- Multicast protocols: IGMP Snooping, GMRP, and static multicast
- Switching attributes: VLAN, PVLAN, GVRP, QoS, and ARP
- Bandwidth management: port trunk, and port rate limiting
- Synchronization protocol: SNTP
- Security: IEEE802.1X, TACACS+, SSH, SSL, port security, and AAA
- Device management: FTP/TFTP software update, FTP/TFTP file transmission, and log recording and uploading
- Device diagnosis: port mirroring, LLDP, VCT, and link status detection
- Alarming: port alarm, power alarm, and ring alarm
- Network management: management by CLI, Telnet, Web, and Kyvision network management software, and SNMP network monitoring
- ...

2. Switch Access

There are some ways to access a switch.

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

Kyvision network management software is designed by Kyland. Please refer to its user manual for more information.

2.1 View Types

When logging into CLI (Command Line Interface) by Console port or Telnet, user can enter different views or switch between different views by using different commands, as shown in Table 1.

Table 1: View Switching

View Prompt	View Type	View Function	Command for View Switching
SWITCH>	General mode	<ul style="list-style-type: none"> ➤ Show currently used commands ➤ Show IP address ➤ Show software version ➤ View response information for ping operation 	Input " enable " to enter the Privileged mode
SWITCH #	Privileged mode	<ul style="list-style-type: none"> ➤ Show switch configuration information ➤ Upload/download configuration file ➤ Upload/download log record ➤ Restore default configuration 	<ul style="list-style-type: none"> ➤ Input "configure terminal" to switch from the Privileged mode to the Configuration mode; ➤ Input "exit" to return to the General mode

		<ul style="list-style-type: none"> ➤ View response information for ping operation ➤ Restart the switch ➤ Save current configuration ➤ Software update ➤ Upload/download file through xmodem protocol 	
SWITCH(config) #	Configuration mode	Configure all switch functional modules	Input " exit " or " end " to return to the Privileged mode

When a switch is configured by command lines, "?" can be used to get command help. In the help information, there are different parameter descriptions, for example, <1, 255> means a number range; <H.H.H.H> means an IP address; <H:H:H:H:H:H> means a MAC address; word<1,31> means a string range. In addition, ↑ and ↓ can be used to scroll through the last used commands.

2.2 Console Port Access

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

1. Use DB9-RJ45 cable to connect the DB9 port of a PC and the switch Console port.
2. Run the Hyper Terminal in Windows desktop. Click [Start]→[All Programs]→[Accessories]→[Communications]→[Hyper Terminal], as shown in Figure 1.

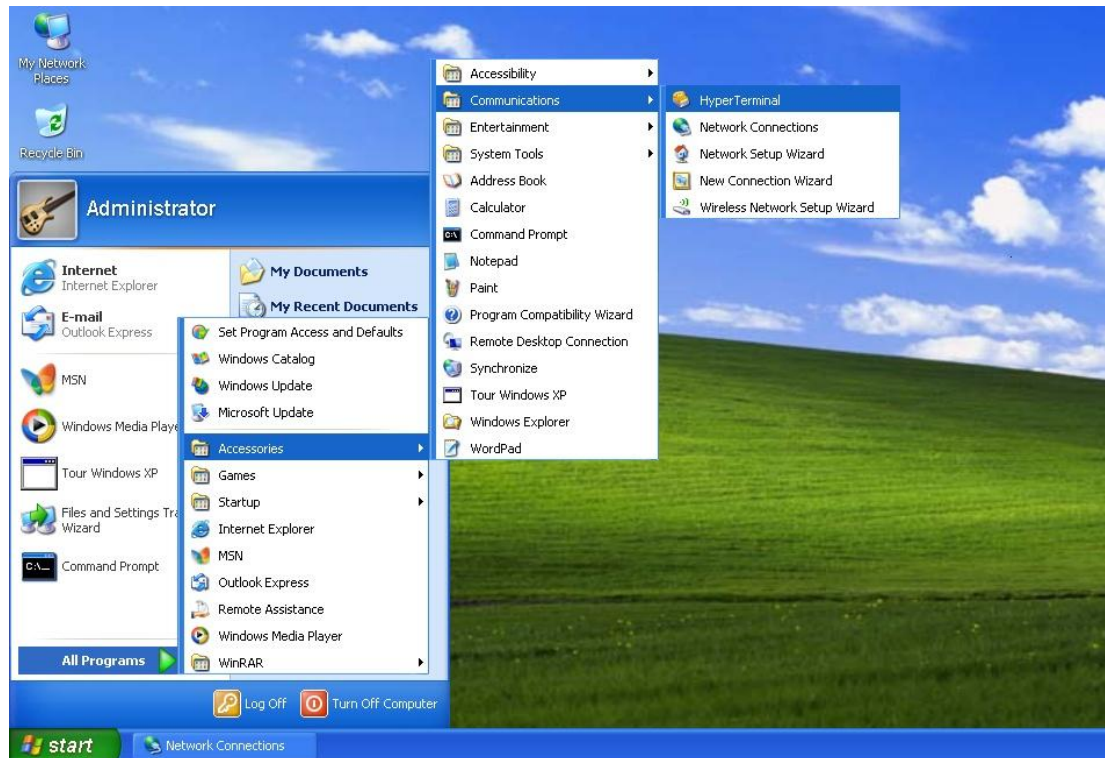


Figure 1: Hyper Terminal

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

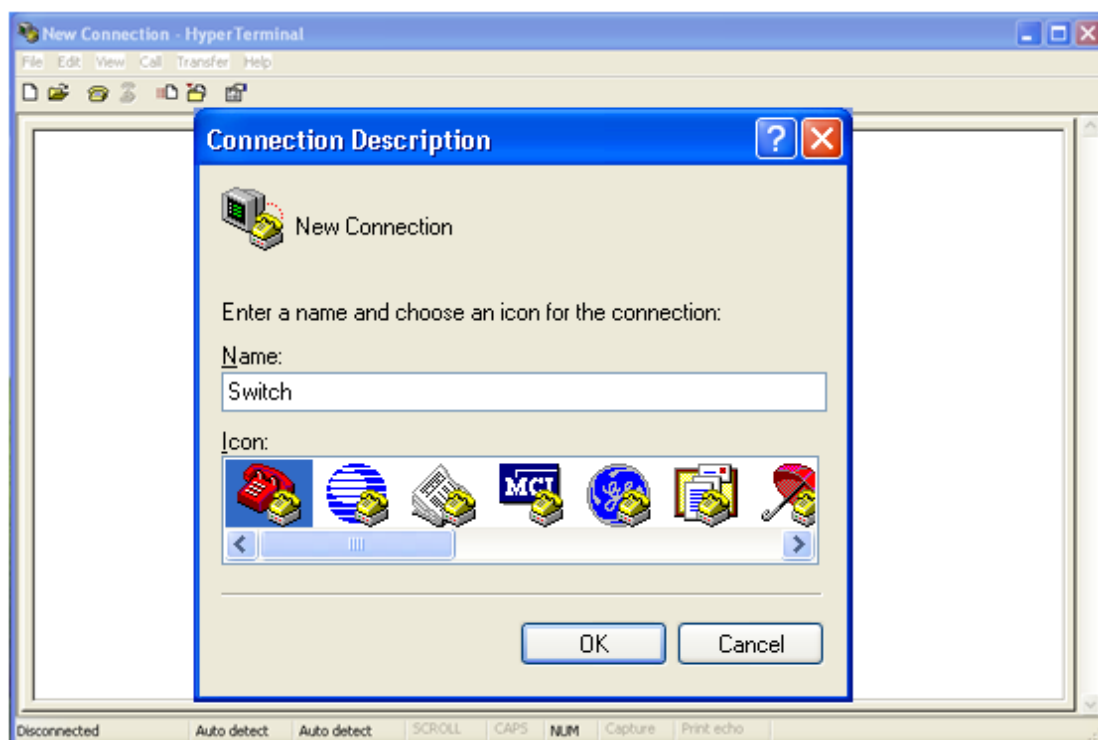


Figure 2: New Connection

4. Connect a correct communication port, as shown in Figure 3.

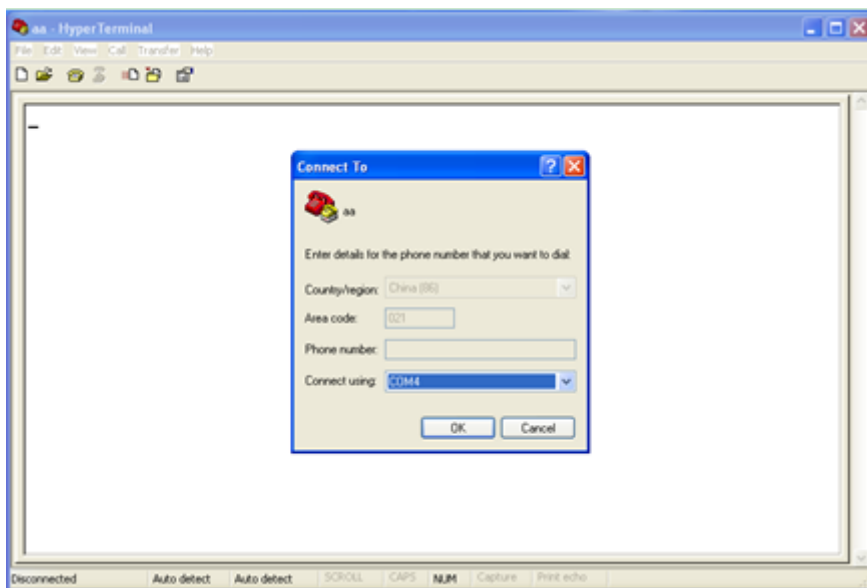


Figure 3: Select communication port



Note:

To confirm communication port, please right click [My Computer]→[Property]→[Hardware]→[Device Manager]→[Port] to check the Console port-used communication port.

5. Serial port setting as shown in Figure 4. Bits per second (Baud rate): 115200; Data bits: 8; Parity: None; Stop bits: 1; Flow control: None

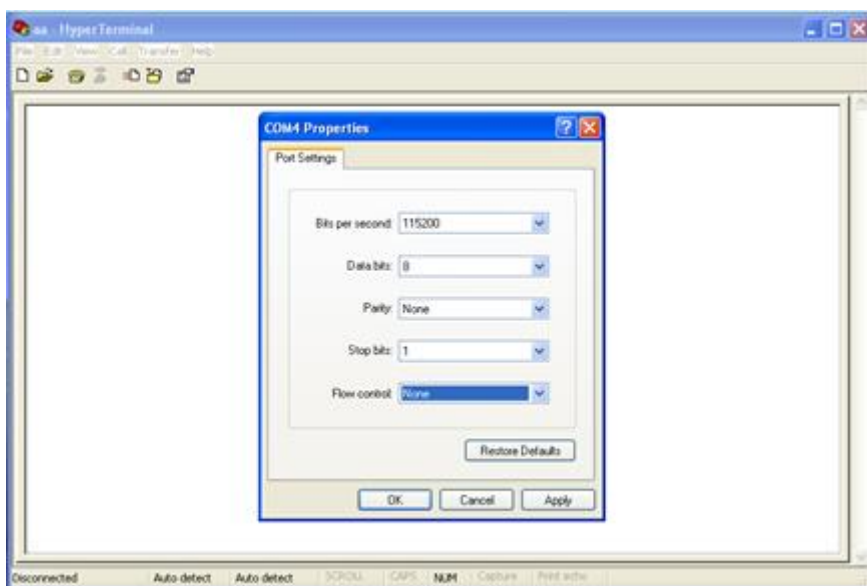


Figure 4: Port Setting

6. Click <OK> button to enter the switch CLI. Input password "admin" and press <Enter> to

enter the General mode, as shown in Figure 5.

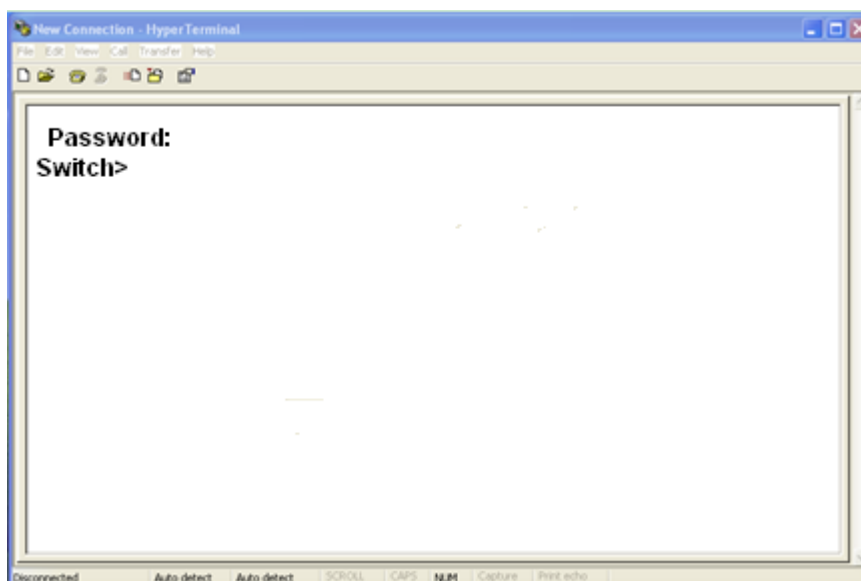


Figure 5: CLI

2.3 Telnet Access

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

1. Type "**telnet** IP address" in the RUN dialog box, as shown in Figure 6.

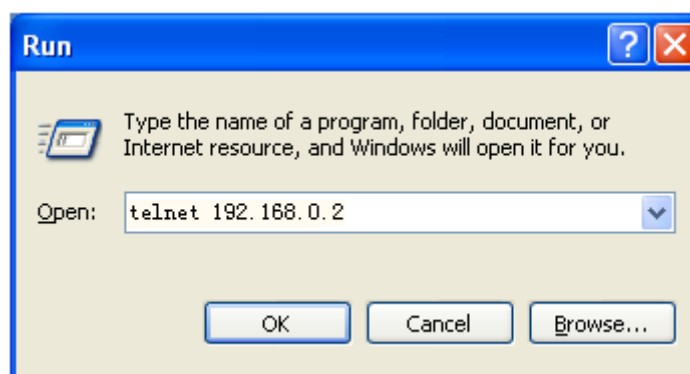


Figure 6: Telnet Access



Note:

To confirm the switch IP address, please refer to "5.1 IP Address" to learn how to obtain the IP address.

2. In the Telnet interface, input "admin" in User, and "123" in Password. Click <Enter> to log in to the switch, as shown in Figure 7.

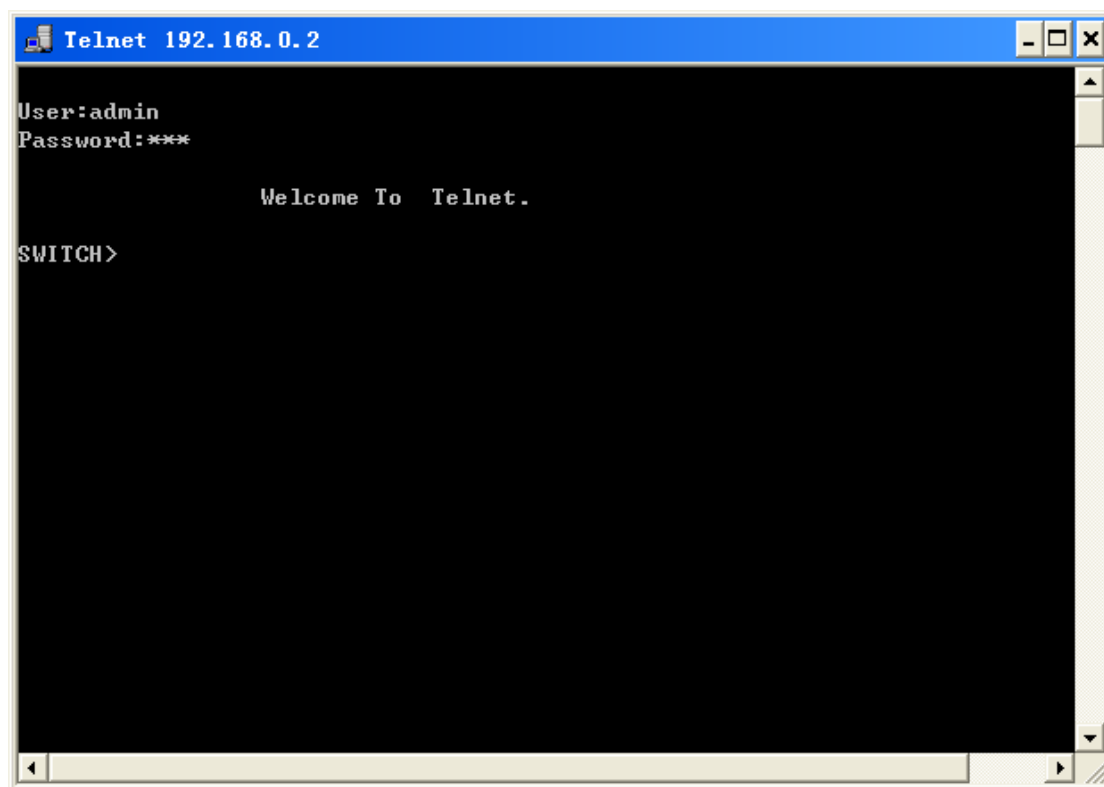


Figure 7: Telnet Interface

2.4 Web Access

The precondition of accessing switch by Web is the normal communication of PC and switch.



Note:

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

By default, HTTP protocol is used for Web login. If HTTPS protocol is used for login, please refer to "16.6 SSL" for more details.

1. Input "*IP address*" in the browser address bar. The login interface is displayed, as shown in Figure 8. Input the default user name "admin" and password "detmold". Click <Sign in>.

Layer 2 Switch

中文

User Name: admin

Password: [masked]

☐ Save the password

Sign in

Serial Number : S30P0001XXXXXXXX

System Name : SWITCH

Location : Chongxin Mansion Building, Xijing Road 3#, Shijingshan District, Beijing

Contact : +86-10-88798888

KYLAND TECHNOLOGY CO., LTD. All Rights Reserved 2013.

Figure 8: Web Login

The default setting is the English login interface. Click <中文> button to change to the Chinese login interface.



Note:

To confirm the switch IP address, please refer to "5.1 IP Address" to learn how to obtain the IP address.

2. After the success of Web login, there is a navigation tree on the left of the interface, as shown in Figure 9.

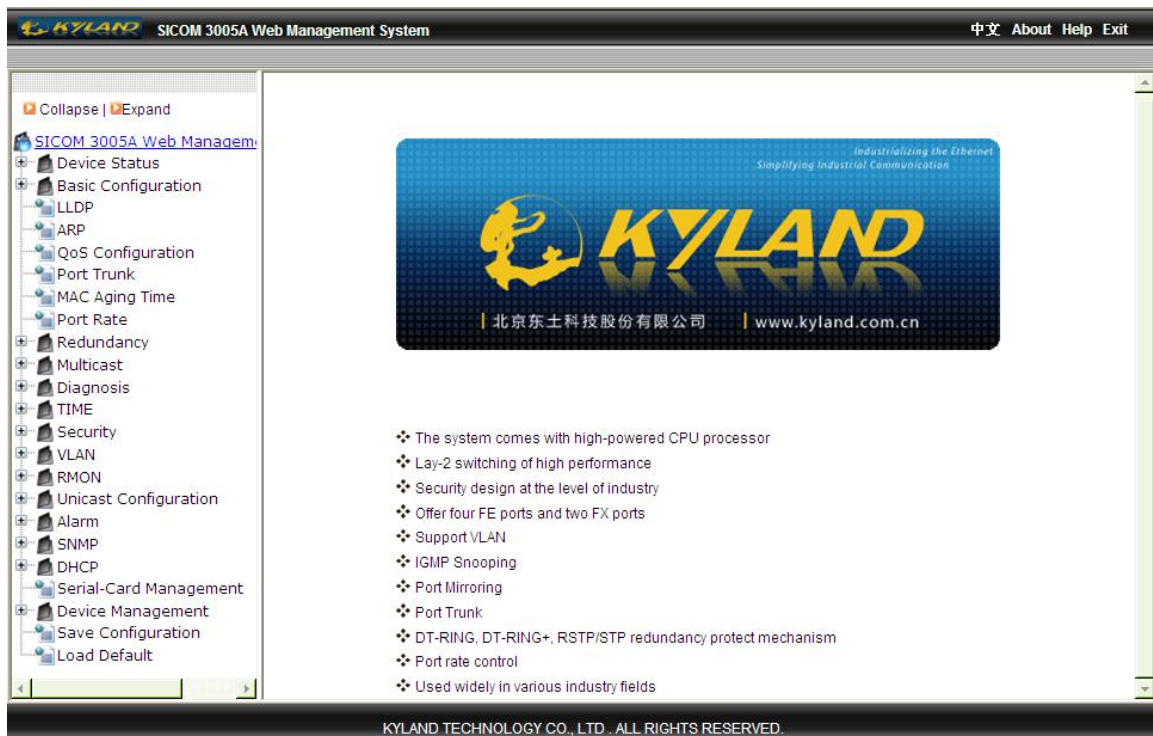


Figure 9 : Web Interface

You can expand or collapse the navigation tree by clicking <Expand> or <Collapse> on the top of the navigation tree. You can perform corresponding operations by clicking [Save Settings] or [Load Default] in the top menu. In the upper right corner, you can click <中文> to switch to the Chinese interface and <Logout> to exit the Web interface.

**Caution:**

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

3. Device Management

Click [Device Management]→[Reboot]/[Logout]. You can reboot the device or exit the Web interface. Before rebooting the device, you need to save the current settings as required. If you have saved the settings, the switch automatically configures itself with the saved settings after restart. If you have not saved any settings, the switch restores the factory default settings after restart.

4. Device Status

4.1 Basic Information

The switch basic information contains MAC address, SN, IP address, subnet mask, gateway, system name, device model, software version, BootROM version, as shown in Figure 10.

Item	Information
MAC Address	00-15-7E-0A-40-80
SN	S30P0001XXXXXXXX
IP Address	192.168.0.222
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	SWITCH
Device Model	SICOM3005A
Software Version	R0001 (2014-7-11 19:54)
BootRom Version	V2.1.18 (2014-4-4 10:59)

Figure 10: Switch Basic Information

4.2 Port Status

Port status interface can automatically display port number, port type, administration status, link status, speed, duplex, flow control, as shown in Figure 11.

Port	Type	Administration Status	Link	Speed	Duplex	Flow Control
1	FE	Enable	Down	---	---	---
2	FE	Enable	Down	---	---	---
3	FE	Enable	Down	---	---	---
4	FE	Enable	Up	100M	Full-Duplex	Off
5	FX	Enable	Down	---	---	---
6	FX	Enable	Down	---	---	---
S-CH	S-CH	Enable	Up	100M	Full-Duplex	Off

Figure 11: Port Status

Port

Show port number printed on the switch front panel

Type

FE: 10/100Base-TX RJ45 port

FX: 100Base-FX port

S-CH is a serial port that adopts an RJ45 interface. It is used to manage internal serial port

cards. The S-CH port is not used to transmit protocol packets. Some functions, including VLAN, QoS, port rate, port mirroring, and static FDB multicast can be configured through the S-CH port and other functions cannot be configured through it.

Administration Status

Show the administration status of ports

Enable: the port is available and permits data transmission

Disable: the port is locked without data transmission

Link

Show the link status of ports

Up: the port is in LinkUp state and can communicate normally

Down: the port is in LinkDown state and cannot communicate normally

Speed

Show the communication speed of LinkUp ports

Duplex

Show the duplex mode of LinkUp ports

Full-duplex: the port can receive and transmit data at the same time

Half-duplex: the port only receives or transmits data at the same time

Flow Control

Show the flow control status of LinkUp ports.

**Note:**

Please refer to "5.3 Port Configuration" for the details of duplex and flow control.

4.3 Port Statistics

The Port Statistics interface displays the number of bytes and packets that each port sends, and the number of bytes and packets that each port receives, CRC errors, and the number of packets whose lengths are less than 64 bytes, as shown in Figure 12.

<input type="checkbox"/> All	Port	Type	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
<input type="checkbox"/>	1	FE	0	0	0	0	0	0
<input type="checkbox"/>	2	FE	0	0	0	0	0	0
<input type="checkbox"/>	3	FE	0	0	0	0	0	0
<input type="checkbox"/>	4	FE	759144	1835	2273575	27670	0	0
<input type="checkbox"/>	5	FX	0	0	0	0	0	0
<input type="checkbox"/>	6	FX	0	0	0	0	0	0
<input type="checkbox"/>	S-CH	S-CH	2107159	26472	20400	300	0	0

Clear

Figure 12: Port Statistics

You can click <Clear> to restart statistics collection.

5. Basic Configuration

5.1 IP Address

1. Show switch IP address by using Console port

Use Console port to log into switch command line interface, input "**show interface**" command in the General mode to check the switch IP address. As Figure 13 shows, the IP address is circled in red.

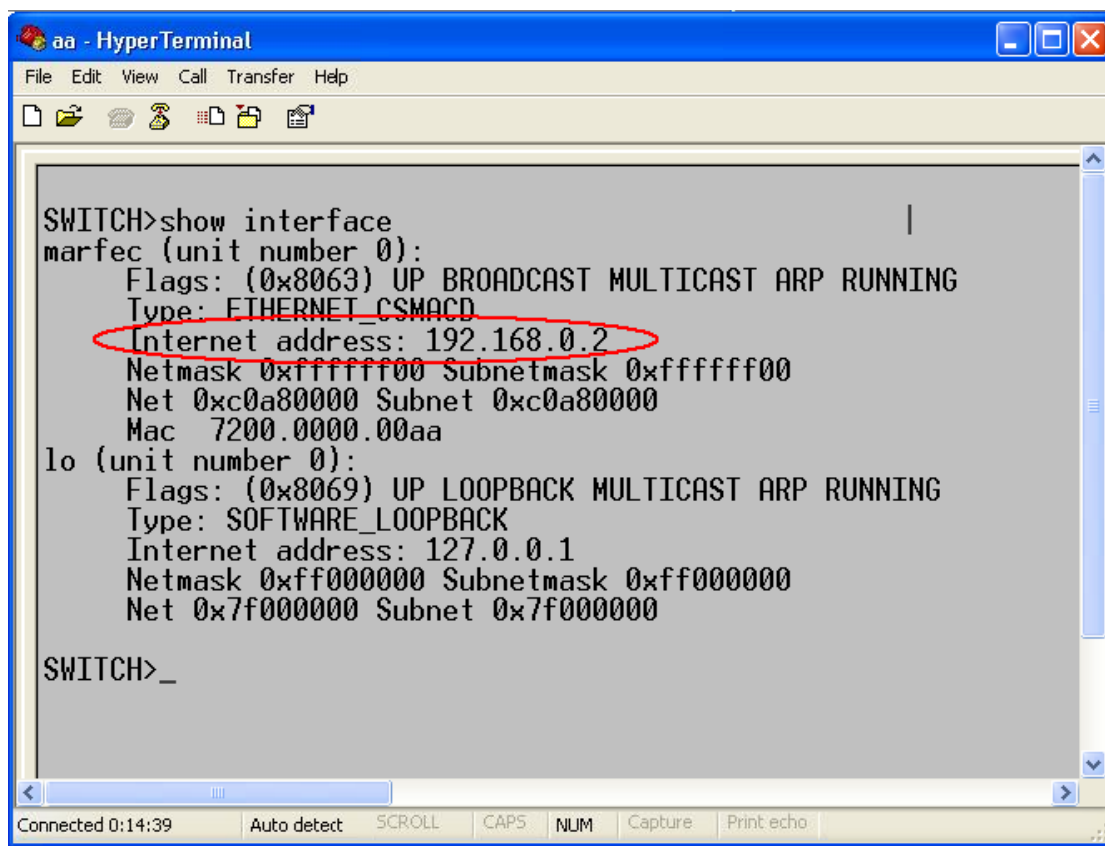


Figure 13: Show IP Address

2. IP address configuration

Switch IP address and gateway can be manually or automatically configured. As Figure 14 shows, when "Auto IP Configuration" is disabled, the switch IP address and gateway need to be manually configured; when "Auto IP Configuration" is enabled, switch can automatically obtain an IP address by DHCP protocol and there must be a DHCP Server in the network to assign IP addresses, subnet mask addresses and gateway addresses to clients. For more details, please refer to "22.1 DHCP Server Configuration".

MAC Address	00-72-74-79-71-75
Auto IP Configuration	<input checked="" type="radio"/> Disable <input type="radio"/> DHCP Client IP
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
GateWay	192.168.1.4

Figure 14: IP Address

**Caution:**

- IP address and gateway must be in the same segment, otherwise, the IP address cannot be modified.
- For this series switches, the change in IP address will take effect immediately after modification without the need of reboot.

5.2 Device Information

Device information includes the project name, switch name, location and contact, as shown in Figure 15.

Project Name	PRJNAME
Switch Name	SWITCH
Location	Chongxin Mansion Building, Xijing Road 3#, Shijingshan Distri
Contact	+86-10-88798888

Figure 15: Device Information

Project Name

Configuration range: 1~64 characters

Switch Name

Configuration range: 1~32 characters

Location

Configuration options: character/Chinese character

Configuration range: 1~255 characters (One Chinese character occupies two characters)

Contact

Configuration options: character/Chinese character

Configuration range: 1~32 characters (One Chinese character occupies two characters)

5.3 Port Configuration

Port configuration can configure port status, port speed, flow control and other information, as shown in Figure 16.

Port	Type	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control
1	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> 10M <input type="radio"/> 100M	<input checked="" type="radio"/> Half <input type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On
2	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> 10M <input type="radio"/> 100M	<input checked="" type="radio"/> Half <input type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On
3	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> 10M <input type="radio"/> 100M	<input checked="" type="radio"/> Half <input type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On
4	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On
5	FX	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input checked="" type="radio"/> 10M <input type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On
6	FX	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="radio"/> Off <input type="radio"/> On

Figure 16: Port Configuration

Administration Status

Configuration options: Enable/Disable

Default: Enable

Function: Enable means that the port is open and permits data transmission; Disable means that the port is blocked without data transmission. This option can directly disable the port in hardware and trigger port alarms. When it is disabled, the port's operation state cannot be set.

Operation Status

Configuration options: Enable/Disable

Default: Enable

Function: configure the port operation state.

Explanation: The port is disabled by protocols.

Auto

Configuration options: Enable/Disable

Default: Enable

Function: configure the auto-negotiation status of ports

Function: When Auto is enabled, the port speed and duplex mode will be automatically negotiated according to port connection status; when Auto is disabled, the port speed and duplex mode can be configured by user.


Caution:

100Base-FX ports are forced to disable auto-negotiation.

Speed

Configuration options: 10M/100M

Function: forced port speed

Explanation: When the Auto is disabled, the port speed can be configured by user.

Duplex

Configuration options: Half/Full

Function: configure the duplex mode of ports

Explanation: When the Auto is disabled, the port duplex mode can be configured by user.


Caution:

- 10/100Base-TX ports can be configured to auto-negotiation, 10M&full duplex, 10M&half duplex, 100M&full duplex, 100M&half duplex.
- 100Base-FX ports are forced to 100M&full duplex.

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

Flow Control

Configuration options: Off/On

Default: Off

Function: Open/Close flow control function in the designated port.

Explanation: 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. For the devices working in different duplex mode (half/full), their flow control is realized in different ways. For the device working in full duplex mode, the receiving end will send a special frame (Pause frame) to inform the sending end to stop sending messages, when the sender receives the Pause frame, it will stop sending messages for a period of "wait time" carried in the Pause frame and continue sending messages once the "wait time" ends. For the device working in the half duplex mode, it supports back pressure flow control. It is that the receiving end intentionally 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.

5.4 Change Password

Users can change the password for the "admin" account, the password is 1~32 characters. The operation is shown in Figure 17.

User Name	admin
Old Password	●●●●●●
New Password	●●●
Confirm Password	●●●

Figure 17: Change Password

5.5 Software Update

Switch can obtain more performances by software update. For this series switches, software updates contains BootROM software version update and system software version update. First, update the BootROM software version, and then update the system software version. If no change in the BootROM version, users can only update the system software version. The software version update needs FTP/TFTP server.

5.5.1 Software Update by FTP

Install an FTP server. We will use WFTPD software as an example to introduce FTP server

configuration and software update.

1. Click [Security]→[Users/rights] to open "Users/Rights Security Dialog"; Click <New User> button to create a new FTP user, as shown in Figure 18. Create a user name and password, for example, user name "admin", and password "123", click <OK>.

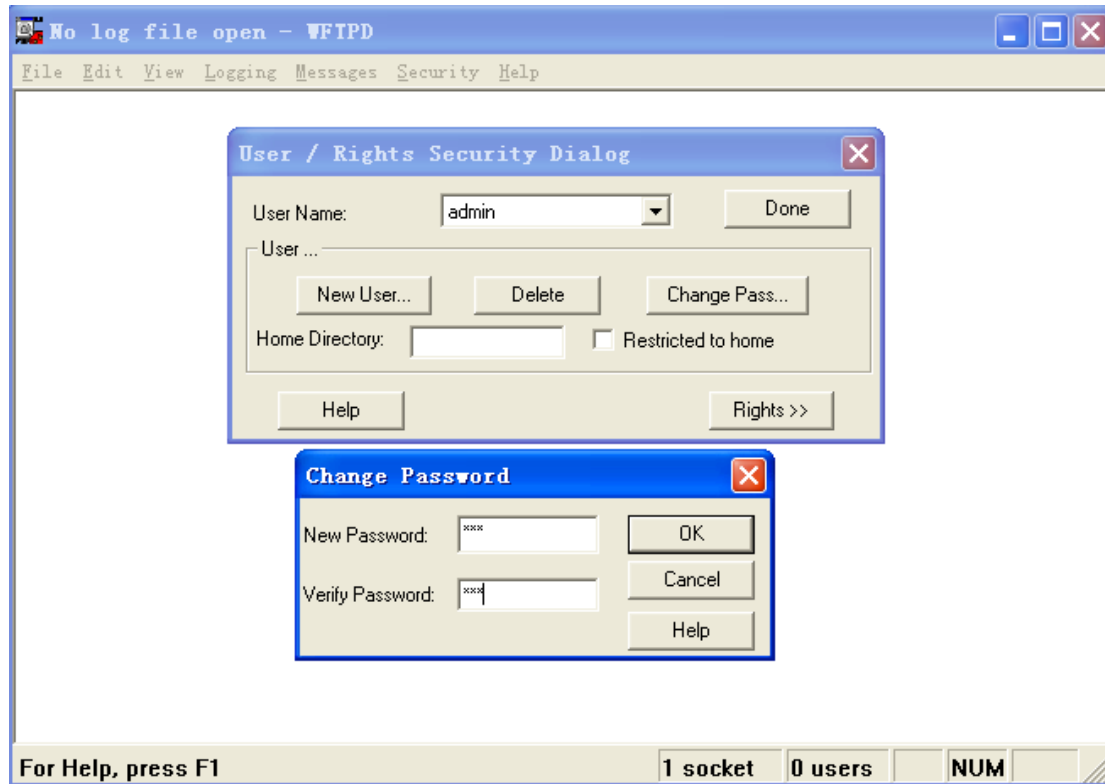


Figure 18: Create a new FTP user

2. Input the storage path of the update file in the space of "Home Directory", as shown in Figure 19, click <Done>

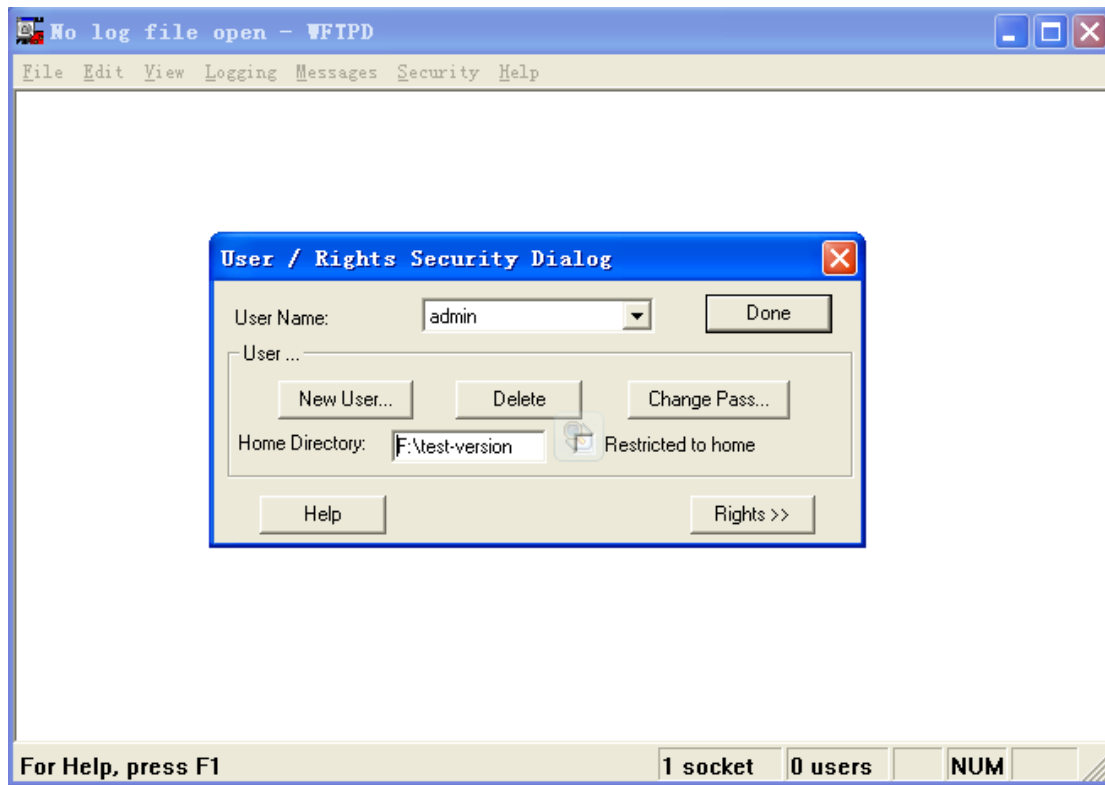


Figure 19: File storage path

3. To update the BootROM software, input the following command in the Privileged mode.

Switch#**update ftp-mode bootrom** *File_name Ftp_server_ip_address User_name Password*

Table 2 lists the parameter descriptions.

Table 2: Parameters for BootROM Update by FTP

Parameter	Description
<i>File_name</i>	Name of the BootROM version
<i>Ftp_server_ip_address</i>	IP address of the FTP server
<i>User_name</i>	Created FTP user name
<i>Password</i>	Created FTP password

4. Figure 20 shows the software update page. Enter the IP address of the FTP server, file name (on the server), FTP user name, and password. Click <Apply>.

Update Mode	<input checked="" type="radio"/> Ftp Mode <input type="radio"/> Tftp Mode
Server IP Address	192.168.0.23
File Name	SICOM3009A-T0008.bin
User Name	admin
Password	...

Figure 20 Software Update by FTP



Warning:

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

5. Make sure the normal communication of FTP server and switch, as shown in Figure 21.

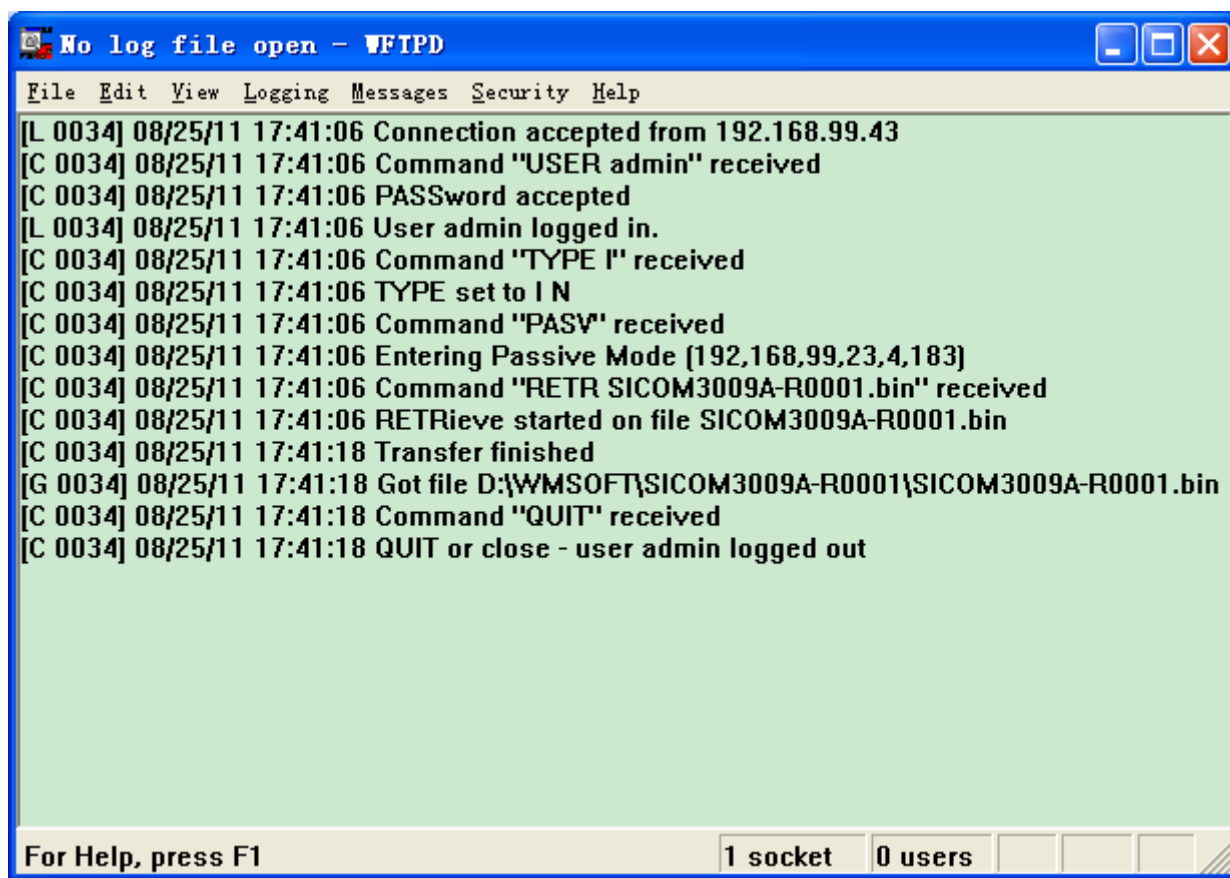


Figure 21: Normal communication of FTP server and switch



Caution:

To display update log information as shown in the preceding figure, you need to click [Logging]→[Log Option] in WFTPD and select Enable Logging and the log information to be

displayed.

6. Wait for the update to complete, as shown in Figure 22.

Result

The software is updating, do not cut off power supply or proceed any other operations.
please wait 3-4 minutes...

Figure 22: Wait for update to complete

7. When update completes as shown in Figure 23, please reboot the device and open the Basic Information to check if update succeeded and the new version is active.

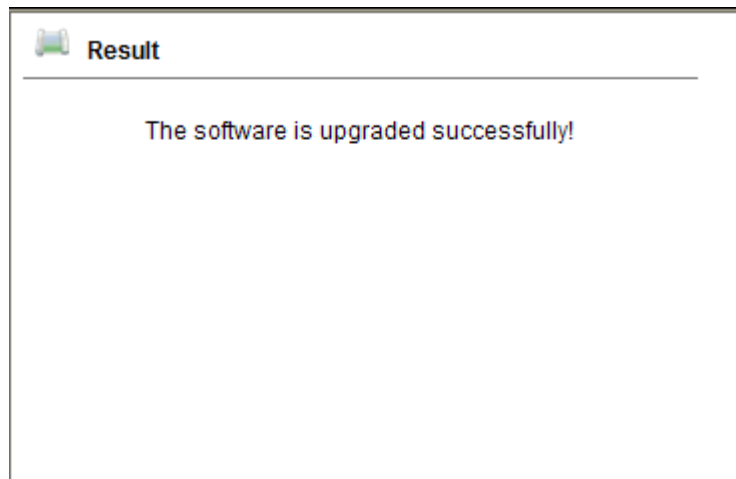


Figure 23: Successful software update by FTP



Warning:

- In the software update process, keep the FTP server software running.
- When update completes, reboot the device to activate the new version.
- If update fails, do not reboot the device to avoid the loss of software file and the switch cannot be started normally.

5.5.2 Software Update by TFTP

Install TFTP server. We will use TFTPd software in this example to introduce TFTP server configuration and software update, as shown in Figure 24.

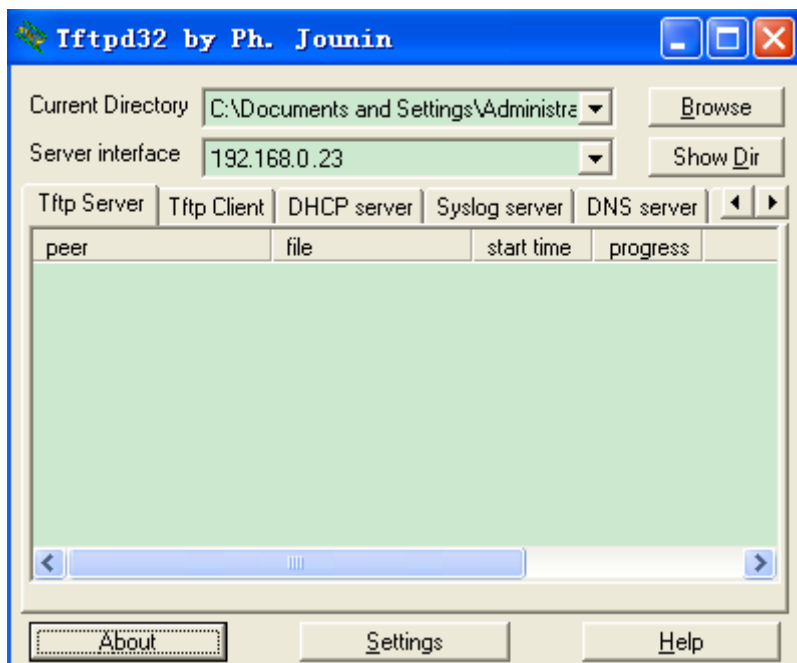


Figure 24: TFTP server configuration

1. In Current Directory, choose the storage path of the update file on server; input the server IP address in Server interface.
2. To update the BootROM software, input the following command in the Privileged mode.

Switch#**update tftp-mode bootrom** *File_name* *Tftp_server_ip_address*

Table 3 lists the parameter descriptions.

Table 3: Parameters for BootROM Update by TFTP

Parameter	Description
<i>File_name</i>	Name of the BootROM version
<i>Tftp_server_ip_address</i>	IP address of the TFTP server

3. As Figure 25 shows, input TFTP server IP address, file name on server, click <Apply> button, and wait for update to complete.

Update Mode	<input type="radio"/> Ftp Mode <input checked="" type="radio"/> Tftp Mode
Server IP Address	192.168.0.23
File Name	SICOM3009A-T0008.bin
User Name	
Password	

Figure 25: Software update by TFTP



Caution:

If software is updated by TFTP, there is no need of user name and password.

4. Make sure the normal communication of TFTP server and switch, as shown in Figure 26.

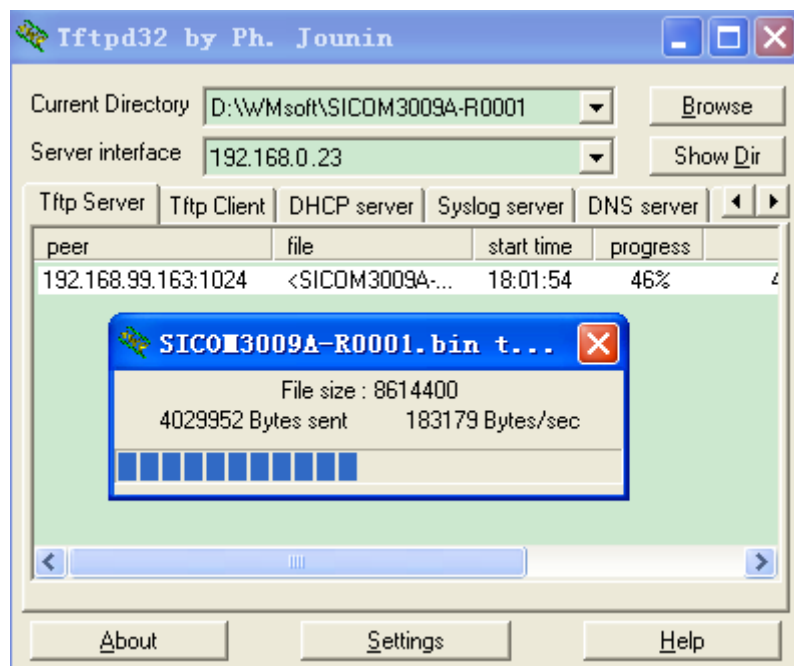


Figure 26: Normal communication of TFTP server and switch

5. Wait for the update to complete, as shown in Figure 27.

Result

The software is updating, do not cut off power supply or proceed any other operations.
please wait 3-4 minutes...

Figure 27: Wait for update

6. When update completes as shown in Figure 28, please reboot the device and open the Basic Information to check if update succeeded and the new version is active.

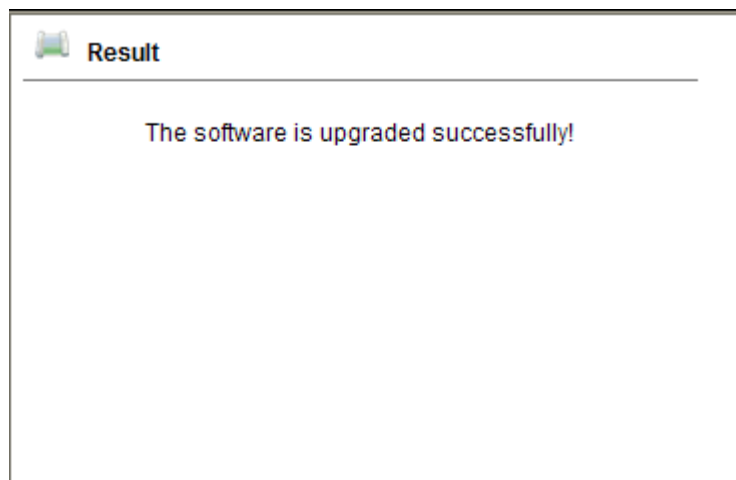


Figure 28: Successful software update by TFTP



Warning:

- In the software update process, keep the TFTP server software running.
- When update completes, reboot the device to activate the new version.
- If update fails, do not reboot the device, so as to avoid the loss of software file and the switch cannot be started normally.

5.6 Upload & Download

Configuration backup function can save current switch configuration files on the server.

When the switch configuration is changed, users can download the original configuration files from the server to switch by FTP/TFTP protocol.

File uploading is to upload the switch configuration files to the server and save them to *.doc and *.txt files. File downloading is to download the saved configuration files from the server to switch, as shown in Figure 29 to Figure 32.

**Caution:**

After configuration file is downloaded to the switch, you need to restart the switch to make the configuration take effect.

Transfer Mode	<input checked="" type="radio"/> Ftp Mode <input type="radio"/> Tftp Mode
Function Selection	<input checked="" type="radio"/> Upload File to PC <input type="radio"/> Download File to Switch <input type="radio"/> Download help file
Server IP Address	<input type="text" value="192.168.0.23"/>
File Name	<input type="text" value="config.txt"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="..."/>

Figure 29: Configuration file upload in FTP mode

Transfer Mode	<input checked="" type="radio"/> Ftp Mode <input type="radio"/> Tftp Mode
Function Selection	<input type="radio"/> Upload File to PC <input checked="" type="radio"/> Download File to Switch <input type="radio"/> Download help file
Server IP Address	<input type="text" value="192.168.0.23"/>
File Name	<input type="text" value="config.txt"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="..."/>

Figure 30: Configuration file download in FTP mode

Transfer Mode	<input type="radio"/> Ftp Mode <input checked="" type="radio"/> Tftp Mode
Function Selection	<input checked="" type="radio"/> Upload File to PC <input type="radio"/> Download File to Switch <input type="radio"/> Download help file
Server IP Address	<input type="text" value="192.168.0.23"/>
File Name	<input type="text" value="config.txt"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Figure 31: Configuration file upload in TFTP mode

Transfer Mode	<input type="radio"/> Ftp Mode <input checked="" type="radio"/> Tftp Mode
Function Selection	<input type="radio"/> Upload File to PC <input checked="" type="radio"/> Download File to Switch <input type="radio"/> Download help file
Server IP Address	<input type="text" value="192.168.0.23"/>
File Name	<input type="text" value="config.txt"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Figure 32: Configuration file download in TFTP mode

6. LLDP

6.1 Introduction

LLDP (Link Layer Discovery Protocol) provides a standard Link layer discovery method, which can encapsulate the main capabilities, management address, device identifier, interface identifier and other information of the local device into LLDPDU (Link Layer Discovery Protocol Data Unit), and then send the LLDPDU to its connected neighbors. Once the neighbors receive the information, they will save them in their MIB for the future query and link status judgment by the network management system.

6.2 Web Configuration

1. Enable LLDP protocol, as shown in Figure 33.

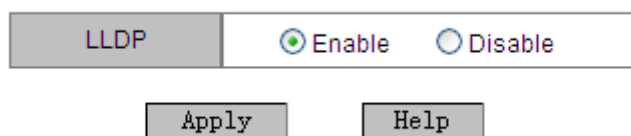


Figure 33: Enable LLDP

LLDP

Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable LLDP protocol.

Explanation: If LLDP is enabled, the switch will send LLDP messages to its neighbor devices, meanwhile, receive and process the LLDP messages from the neighbor devices. If LLDP is disabled, the switch neither sends nor processes LLDP messages.

Once LLDP protocol is enabled, LLDP information can display the information of the neighbor device, including the connected local port on the switch and the remote port on the neighbor device, the IP address, MAC address, System name(Switch Name) and system description(Device Model) of the neighbor device, as shown in Figure 34.

LLDP Information

Local Port	Remote Port	Neighbor IP	Neighbor MAC	Remote System Name	Remote System Description
Port_2	Port_1	192.168.0.222	00-15-7e-0a-40-80	SWITCH	SICOM3005A

Figure 34: LLDP information



Caution:

LLDP information can be displayed only after LLDP protocol is enabled in both connected devices. This protocol is the link layer discovery protocol and it is enabled by default.

7. ARP

7.1 Introduction

ARP (Address Resolution Protocol) uses address request and response mechanism to resolve the mapping relationship of IP address and MAC address. The switch not only can dynamically learn the IP address-and-MAC address mapping relationships of other hosts that are in the same segment with the switch, but also can configure static ARP entries to specify the fixed mapping relationships of IP and MAC addresses. Dynamic ARP entries need periodic aging to ensure the consistency between entries and the practical applications.

This series switches not only provide layer 2 switching function, but also support ARP function to realize the IP address resolution of other hosts that are in the same segment with switches, achieving intercommunication with the network management system and other management hosts.

7.2 Explanation

ARP entries are divided to dynamic ARP entries and static ARP entries.

Dynamic entries are automatically generated and maintained by the exchange of ARP messages, and they can be aged and renewed by new ARP messages and covered by static ARP entries.

Static entries are manually configured and maintained, and cannot be aged and covered by dynamic ARP entries.

Max 512 ARP entries are supported, along with max 256 static entries. When the number of ARP entries exceeds 512, the new entry will cover the old dynamic entry.

7.3 Web Configuration

1. Configure ARP aging time, as shown in Figure 35.

ARP Aging Time

ARP Aging Time	20	(10-60min)
----------------	----	------------

Apply
Help

Figure 35: Configure aging time

ARP Aging Time

Configuration range: 10~60min

Default: 20min

Function: configure ARP aging time.

Explanation: The ARP aging time begins once a dynamic ARP entry adds into the address table. When the time ends, this dynamic entry will be deleted from the table.

2. Configure static ARP address entry, as shown in Figure 36.

ARP Address Configuration

IP address	192.168.0.12
MAC address	ea-23-47-83-84-95

Apply
Help

Figure 36: Configure static ARP entry

ARP address

Group configuration: {IP address, MAC address}

Configuration format: {A.B.C.D, HH-HH-HH-HH-HH-HH} (H is a hexadecimal number)

Function: configure static ARP address resolution entry.



Caution:

- The IP address set in the static ARP entry must be in the same segment with the switch IP address.
- When the switch IP address is set in the static ARP entry, the system will automatically correspond to the switch MAC address.
- Generally, switch can automatically learn ARP entries without the need of static entry configuration by the administrator.

3. Show or delete ARP address entry, as shown in Figure 37.

ARP Address List

Index	IP address	MAC address	Flags
<input type="radio"/>	192.168.0.5	00-E0-CD-31-71-02	dynamic
<input type="radio"/>	192.168.0.6	00-1E-CD-00-00-11	dynamic
<input type="radio"/>	192.168.0.12	EA-23-47-83-84-95	static
<input type="radio"/>	192.168.0.23	44-37-E6-88-6E-90	dynamic

Figure 37: ARP address mapping table

ARP address

Group displaying: {IP address, MAC address, Flags}

Function: show ARP entries, including static and dynamic entries.

Method: Select a static entry and click <Delete> to delete this entry.



Caution:

Dynamic ARP entries cannot be deleted.

8. QoS Configuration

8.1 Introduction

QoS (Quality of Service) is a mechanism that utilizes flow control and resource allocation to offer different services to multi traffics that have different demands on the limited bandwidth in the IP network, according with the transmission features of different traffics as far as possible, reducing network congestion and minimizing the influence of network congestion on the high priority traffics.

QoS mainly concerns traffic identification, congestion management and congestion avoidance. They mainly complete the following functions:

Traffic identification: identity objects according to certain matching rules, such as the priority identifier in the message, the remarked priority based on port and VLAN, and so on. Traffic identification is the premise of QoS.

Congestion management: an indispensable measure to solve resource competition. Generally, it is to put messages in queues for caching, and use certain scheduling algorithm to arrange the message forwarding sequence, so as to guarantee the top forwarding priority of key traffics.

Congestion avoidance: excessive congestion will damage network resources. Congestion avoidance supervises the usage of network resources. When it is found that the congestion has aggravated, the messages will be dropped to adjust flow, solving the network overload.

8.2 Principle

Each port of this series switches has 4 caching queues (0, 1, 2, and 3) and the priority gradually increases. When a frame arrives at a port, it will be stored in a queue according to the mapping relationship of the queue and the priority value.

This series switches support three types of queue mapping modes: port, DSCP, and 802.1p.

- If the Ingress Type of a port is set to Port, the port default priority determines a queue to save a message. The mapping relationship of port default priority and queue is consistent

with that of 802.1p priority and queue.

- DSCP value depends on the ToS/DSCP part of the message. The mapping relationship of this priority and queue can be configured.
- If the message is a tagged message, 802.1p value depends on the priority of 802.1Q Tag in the message. When the message is an untagged message, 802.1p value depends on the port default priority. The mapping relationship of 802.1p priority and queue can be configured.

When ports forward data, the scheduling mode determines how to schedule data in four queues and bandwidth occupied by each queue. This series switches support two types of QoS queue scheduling modes: WRR (Weighted Round Robin) and SP (Strict Priority).

- WRR scheduling mode is to schedule data streams according to the weight ratio. The bandwidth is allocated to each queue according to the weight ratio and mode bandwidth is allocated to the queue with high weight ratio.
- SP mode can strictly guarantee the preferential forwarding of the high priority messages and mainly used for the transmission of sensitive signals. Once a frame adds into the high priority queue, the SP mechanism stops the scheduling of low priority queue and processes the data in the high priority queue. Only when the high priority queue is empty, it starts processing data in the lower priority queue in turn.

8.3 Web Configuration

1. QoS port configuration, as shown in Figure 38.

Port Configure

Port	Type	Ingress Type			Egress Type	
1	FE	<input checked="" type="radio"/> Port	<input type="radio"/> 802.1P	<input type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR
2	FE	<input type="radio"/> Port	<input checked="" type="radio"/> 802.1P	<input type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR
3	FE	<input type="radio"/> Port	<input checked="" type="radio"/> 802.1P	<input type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR
4	FE	<input type="radio"/> Port	<input type="radio"/> 802.1P	<input checked="" type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR
5	FX	<input type="radio"/> Port	<input checked="" type="radio"/> 802.1P	<input type="radio"/> DSCP	<input type="radio"/> SP	<input checked="" type="radio"/> WRR
6	FX	<input type="radio"/> Port	<input checked="" type="radio"/> 802.1P	<input type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR
S-CH	S-CH	<input type="radio"/> Port	<input checked="" type="radio"/> 802.1P	<input type="radio"/> DSCP	<input checked="" type="radio"/> SP	<input type="radio"/> WRR

SP: Strict Priority WRR: Weight Round Robin 8:4:2:1

Figure 38: QoS Port Configuration

Ingress Type

Configuration options: Port/802.1P/DSCP

Default: 802.1P

Function: configure the port priority mapping mode.

Explanation: Select only one type of priority mapping mode for each port.

Egress Type

Configuration options: SP/WRR

Default: SP

Function: configure the scheduling mode for a port.

Explanation: SP is to preferentially process the data in the high priority queue; WRR is that different queues have different weight configuration. This series switches adopts the fixed weight ratio: queue 3, 2, 1, 0 correspond to the weight ratio of 8:4:2:1.

2. Configure the mapping relationship of 802.1p priority/port priority to queue, as shown in Figure 39.

802.1P Priority 0~7

Priority	0	1	2	3	4	5	6	7
Queue	0 ▼	0 ▼	1 ▼	1 ▼	2 ▼	2 ▼	3 ▼	3 ▼

Figure 39: 802.1p priority-queue mapping table

802.1P Priority 0~7

Group configuration: {Priority, Queue}

Configuration range: {0~7, 0~3}

Default: priority 0 and 1 map to queue 0; priority 2 and 3 map to queue 1; priority 4 and 5 map to queue 2; priority 6 and 7 map to queue 3;

Function: Map 802.1P priority/port priority to queue

3. Configure the mapping relationship of DSCP priority to queue, as shown in Figure 40.

DSCP Priority 0~63

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	0	16	1	32	2	48	3
1	0	17	1	33	2	49	3
2	0	18	1	34	2	50	3
3	0	19	1	35	2	51	3
4	0	20	1	36	2	52	3
5	0	21	1	37	2	53	3
6	0	22	1	38	2	54	3
7	0	23	1	39	2	55	3
8	0	24	1	40	2	56	3
9	0	25	1	41	2	57	3
10	0	26	1	42	2	58	3
11	0	27	1	43	2	59	3
12	0	28	1	44	2	60	3
13	0	29	1	45	2	61	3
14	0	30	1	46	2	62	3
15	0	31	1	47	2	63	3

Queue : 0--LOWEST, 1--SECLow, 2--SECHIGH, 3--HIGHEST

Apply
Help

Figure 40: DSCP priority-queue mapping table

DSCP Priority 0~63

Group configuration: {Priority, Queue}

Configuration range: {0~63, 0~3}

Default: priority 0~15 maps to queue 0; priority 16~31 maps to queue 1; priority 32~47 maps to queue 2; priority 48~63 maps to queue 3;

Function: Map DSCP priority to queue

8.4 Typical Configuration Example

As Figure 41 shows, port 1, 2, 3, 4 forward messages to port 5. Among them, the default priority of port 1 is 6 and the port 1 received messages are mapped to queue 3; the port 2 received messages carry an 802.1P priority of 2 and are mapped to queue 1; the port 3 received messages carry a 802.1P priority of 4 and are mapped to queue 2; the port 4 received messages carry a DSCP priority of 6 and are mapped to queue 3; port 5 adopts WRR scheduling mode.

Switch configuration steps:

1. Set the ingress type of port 1 to "Port", the ingress type of port 2 and port 3 to "802.1P" and the ingress type of port 4 to DSCP; set the egress type of port 5 to WRR, as shown in Figure 38.
2. Respectively map the 802.1P priority 2, 4 and 6 to queue 1, 2 and 3, as shown in Figure 39.
3. Map the DSCP priority 6 to queue 3, as shown in Figure 40.

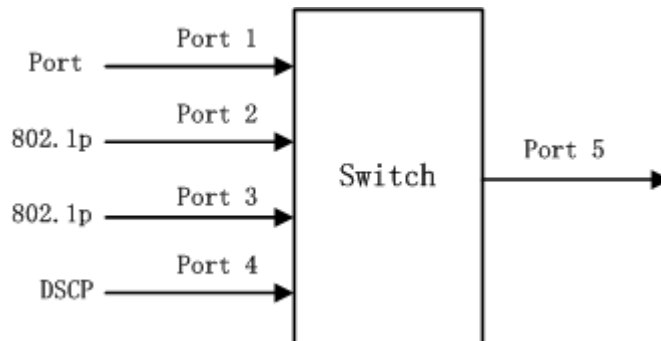


Figure 41: QoS configuration example

The messages from port 1 and port 4 add into the queue 3; the messages from port 2 add into the queue 1; and the messages from port 3 add into the queue 2. Then according to the corresponding relationship between queue and weight ratio, (the weight ratio of queue 1 is 2; the weight ratio of queue 2 is 4; the weight ratio of queue 3 is 8), we learn that the bandwidth ratio allocated to the messages in queue 1 is $2/(2+4+8)$; the bandwidth ratio allocated to the messages in queue 2 is $4/(2+4+8)$; the bandwidth ratio allocated to the messages in queue 3 is $8/(2+4+8)$. Besides, the messages from port 1 and port 4 all enter the queue 3, so they are forwarded based on the rule of "First come, First go", but certainly the total bandwidth ratio

allocated to the messages from port 1 and port 4 must be $8/(2+4+8)$.

9. Port Trunk

9.1 Introduction

Port trunk is to bind a group of physical ports that have the same configuration to a logical port. The member ports in a Trunk group not only can share the flow to, but also can become a dynamic backup of each other to enhance the connection reliability.

9.2 Implementation

As Figure 42 shows, three ports in Switch A aggregate to a Trunk group and the bandwidth of the Trunk group is the total bandwidth of three ports.

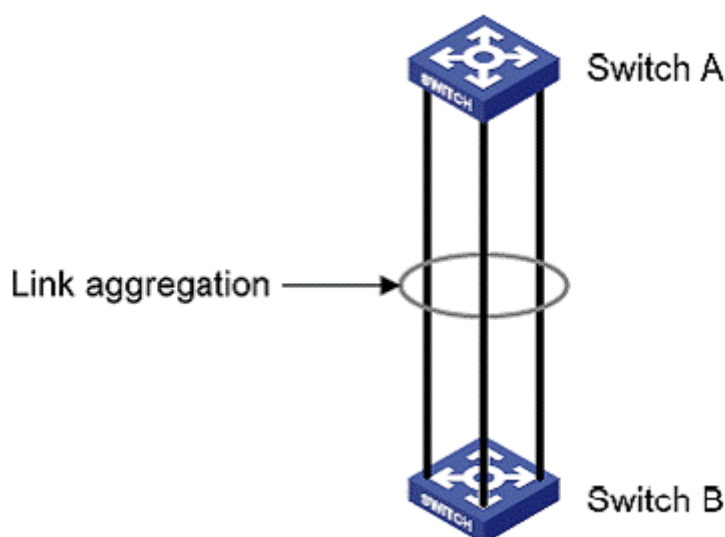


Figure 42: Port Trunk

When Switch A would like to transmit a flow to Switch B via the link aggregation, the trunk group in Switch A will conduct flow allocation algorithm according to the way of flow sharing, then one member port will be selected to transmit the flow according to the algorithm results. If a failed connection occurs in one port in the trunk group, the flow borne by this port will be allocated to other normally connected ports by flow allocation algorithm again.

9.3 Explanation

Port Trunk and the following port operations are mutually exclusive:

- The mutual exclusion of Port Trunk and port redundancy protocol. A port joining Trunk group cannot be configured to a redundancy port, while a redundancy port cannot join a Trunk group.
- The mutual exclusion of Port Trunk and port multicast protocol. A port joining a Trunk group cannot enable a multicast protocol, while a multicast protocol-enabled port cannot join a Trunk group.
- The mutual exclusion of Port Trunk and port GVRP mode configuration. A port joining a Trunk group cannot enable GVRP mode, while a GVRP mode-enabled port cannot join a Trunk group.
- The mutual exclusion of Port Trunk and port unicast configuration. A port joining a Trunk group cannot be added into a static unicast entry, while a port added into a static unicast entry cannot join a Trunk group.
- The mutual exclusion of Port Trunk and DHCP Snooping Trust-Port. A port joining Trunk group cannot be set to a Trust-Port, while a Trust-Port cannot join a Trunk group.
- The mutual exclusion of Port Trunk and Port mirroring. A port joining Trunk group cannot be set to a mirror source/destination port, while a mirror source/destination port cannot join a Trunk group.

**Caution:**

A port can only join one Trunk group.

9.4 Web Configuration

1. Select the port trunk mode, as shown in Figure 43.



Figure 43: Port Trunk Mode Setting

Port Trunk Mode

Configuration options: XOR/HASH

Default: HASH

Function: set port trunk mode

Explanation: Port Trunk Mode determines the way of flow sharing of Trunk Group.

2. Set Trunk group, as shown in Figure 44.

Trunk ID		1				
Port	1	2	3	4	5	6
Type	FE	FE	FE	FE	FX	FX
Select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 44: Trunk Group Configuration

Trunk ID

Configuration range: 1 to 16

Function: Set the Trunk Group ID

Explanation: The series switches support max 16 trunk groups and each trunk group supports max four member ports.

3. Show Trunk group list, as shown in Figure 45.

Trunk List
trunk-1
trunk-2

Figure 45: Trunk Group List

Click a Trunk group in the list shown in Figure 45 to check group members, modify Trunk group configuration and delete Trunk group, as shown in Figure 46.

Trunk ID		<input type="text" value="1"/>				
Port	1	2	3	4	5	6
Type	FE	FE	FE	FE	FX	FX
Select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 46: Detailed configuration of Trunk Group

Modify the members of Trunk group (Add new ports or delete the existing ports). Click <Apply> to activate the changes; click <Delete> to delete the Trunk group.

9.5 Typical Configuration Example

As Figure 42 shows, three ports (port 1, 2, 3) of Switch A respectively connect to three ports (port 1, 2, 3) of Switch B to form a Trunk Group 1, so as to realize the flow sharing between the ports.

Switch configuration steps:

1. Create Trunk Group 1 in Switch A and select port 1, 2 and 3 to be group members, as shown in Figure 44.
2. Create Trunk Group 1 in Switch B and select port 1, 2 and 3 to be group members, as shown in Figure 44.

10. MAC Aging Time

10.1 Introduction

Each port of a switch has the function of auto-learning addresses. That is to learn the source address of the port-received frame, including source MAC address and switch port number, and store it in the address table. Aging time starts once the dynamic address adds into the address table. If all switch ports do not receive the frame with this source address within once to twice aging time, the address will be deleted from the dynamic forwarding address table. Static MAC address table is not affected by the aging time.

10.2 Web Configuration

Configure MAC Aging Time, as shown in Figure 47.



MAC Aging Time(s)	300	(15-3600)
Apply		Help

Figure 47: MAC Aging Time

MAC Aging Time

Configuration range: 15~3600s

Default: 300s

Explanation: this value must be a multiple of 15. Users can adjust the aging time according to the specific situation to effectively implement the MAC aging function.

11. Port Rate

11.1 Introduction

Port rate configuration is to limit the amount of port-received/transmitted messages and drop the data that is over the limitation. Ingress ports limit the rate of the selected messages, while egress ports limit the rate of all messages.

The rate limitation of five types of messages in ingress ports:

- Unknown Unicast Frame (UUF): the message whose destination MAC address has not been learned or has not been statically added.
- Unknown Multicast Frame (UMF): the message whose destination MAC address has not been statically added or has not been learned by IGMP Snooping and GMRP.
- Broadcast Frame (BF): the message with the destination MAC address of FF:FF:FF:FF:FF:FF.
- Multicast Frame (MF): the message whose destination MAC address has been statically added or has been learned by IGMP Snooping and GMRP.
- Unicast Frame (UF): the unicast message whose destination MAC address has been learned or been statically added.

11.2 Implementation

Token bucket can be considered as a container to save a certain number of tokens. The mechanism puts tokens into the bucket at a predetermined rate and the bucket has a specified capacity. If the amount of tokens exceeds the capacity of the bucket, which will overflow, the mechanism will stop accumulating tokens. Each token allows sending a certain number of bits. When a packet is transmitted, a number of tokens that is equivalent to the length of the packet in bits are removed. If there are insufficient tokens in the bucket, the packet may be transmitted until there are sufficient tokens in the bucket or may be dropped. Port rate configuration uses token buckets to control flow. If port rate is set in a port, the messages in this port will be processed by Token Bucket before forwarding. If there are

sufficient tokens, the messages will be transmitted, or else they will be dropped.

11.3 Web Configuration

1. Add port rate configuration, as shown in Figure 48.

Port Rate Configuration

Port ID	Bucket	PacketType	IngressRate	EgressRate
1	0	<input checked="" type="checkbox"/> UUF <input checked="" type="checkbox"/> UMF <input checked="" type="checkbox"/> BF <input type="checkbox"/> MF <input type="checkbox"/> UF	70 (64-200000Kbps)	80 (64-1000000Kbps)

UUF--unknown unicast frame, UMF--unknown multicast frame, BF--broadcast frame MF--multicast frame UF--unicast frame

Figure 48: Port Rate Configuration

Port ID

Configuration options: all switch ports

Bucket

Configuration range: 0~4

Function: Set an index for a token bucket. Each port can set 5 different token buckets.

Packet Type

Configuration options: UUF/UMF/BF/MF/UF

Function: choose the types of packets that need to limit the rate in a token bucket. Multiple types of packets can be chosen at the same time

Ingress Rate

Configuration range: 64~200000Kbps

Function: limit the ingress rate of port-received packets and the packets that exceed the limitation will be dropped

Explanation: The ingress rate of Fast Ethernet port is in the range of 64~100000Kbps

The ingress rate of Gigabit Ethernet port is in the range of 64~200000Kbps

Egress Rate

Configuration range: 64~1000000Kbps

Function: limit the egress rate of port-transmitted packets and the egress rate is shared by 5 token buckets in a port.

Explanation: The egress rate of Fast Ethernet port is in the range of 64~100000Kbps

The egress rate of Gigabit Ethernet port is in the range of 64~1000000Kbps

2. Delete port rate configuration.

Select an index of a Token bucket of the selected port shown in Figure 48, and click <Delete> to delete the packet rate limiting configuration of this bucket of the port.



Caution:

Once a packet ingress rate setting is deleted from a token bucket in a port, the port's egress rate setting is deleted as well. If other token buckets of this port need an egress rate, it needs to be reset.

3. Show port rate configuration list, as shown in Figure 49.

Port Rate Configuration List
(The configuration is the same with the last time if you do nothing this time !)
(1、 unknown unicast frame; 2、 unknown multicast frame; 3、 broadcast frame; 4、 multicast frame; 5、 unicast frame;)

Port ID	Bucket	PacketType	IngressRate	EgressRate
1	0	1 2 3	64Kbps	64Kbps
	1	4	66Kbps	
	2	5	68Kbps	
	3	NULL	disable	
	4	NULL	disable	
2	0	NULL	disable	disable
	1	NULL	disable	
	2	NULL	disable	
	3	NULL	disable	
	4	NULL	disable	
3	0	NULL	disable	disable
	1	NULL	disable	
	2	NULL	disable	
	3	NULL	disable	
	4	NULL	disable	

Figure 49: Port rate configuration list

In the Packet Type, 1 means UUF (Unknown unicast frame), 2 means UMF (Unknown multicast frame), 3 means BF (Broadcast frame), 4 means MF (multicast frame), 5 means UF (Unicast frame).

11.4 Typical Configuration Example

Limit the ingress rate of UUF, UMF and BF in port 1 to 70Kbps and set the egress rate of port 1 to 80Kbps, and they are processed in the Token bucket 0.

Configuration steps: select port 1, token bucket 0, and the packet types of UUF, UMF and BF; set the ingress rate to 70Kbps and the egress rate to 80Kbps, as shown in Figure 48.

12. Redundant

12.1 DT-Ring

12.1.1 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.

12.1.2 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.

Primary port: indicates the ring port (on the master) whose status is configured as forwarding forcibly by user when the ring is closed.

**Note:**

If no primary port is configured on the master, 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.

12.1.3 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 the following figure:
 - 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.

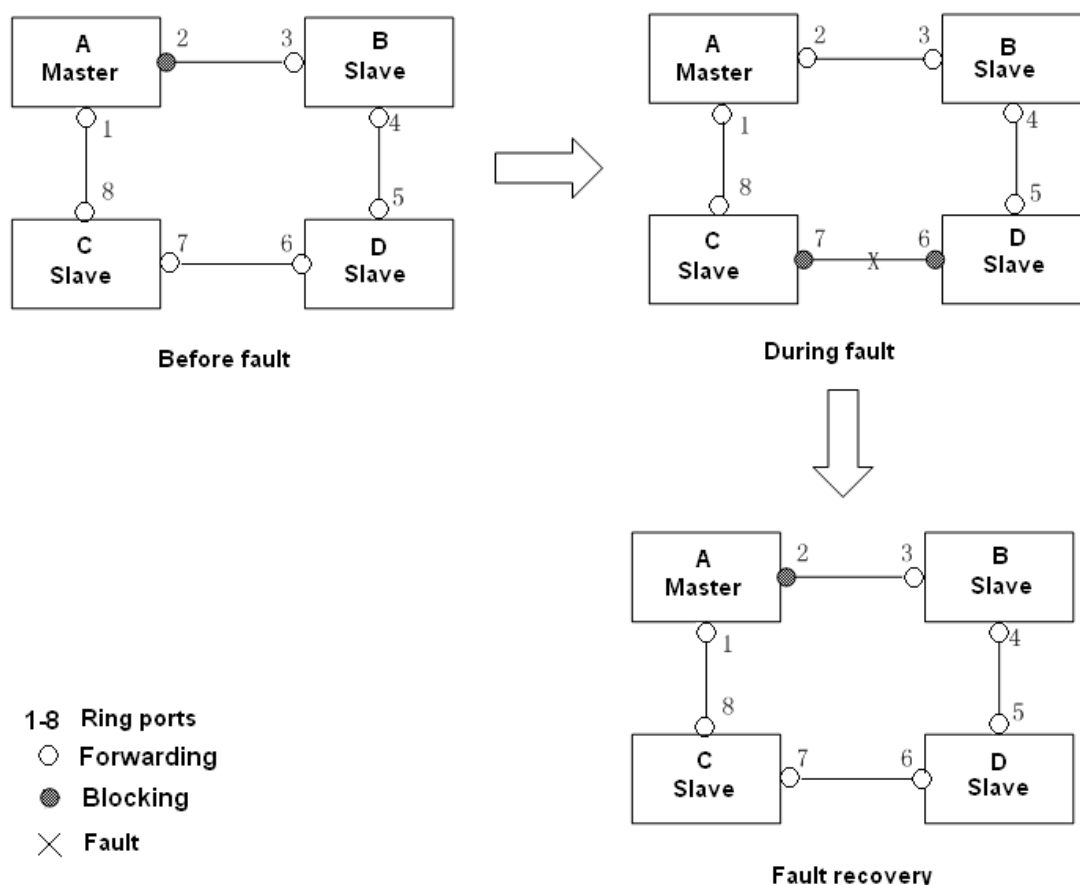


Figure 50 CD Link Fault



Note:

If port 1 on master A is configured as the primary port, the fault and fault recovery processes are identical with those described above.

4. If link AC is faulty, as shown in the following figure:

- 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,
 - If no primary port is configured on master A, port 1 is still in blocking state and port 8 is in forwarding state. No switchover occurs.
 - If port 1 on master A is configured as primary port. When the ring is closed, primary port must be in forwarding state. Therefore, port 1 changes to forwarding state. Port 8 is in forwarding state and port 2 is in blocking state. Link switchover occurs.

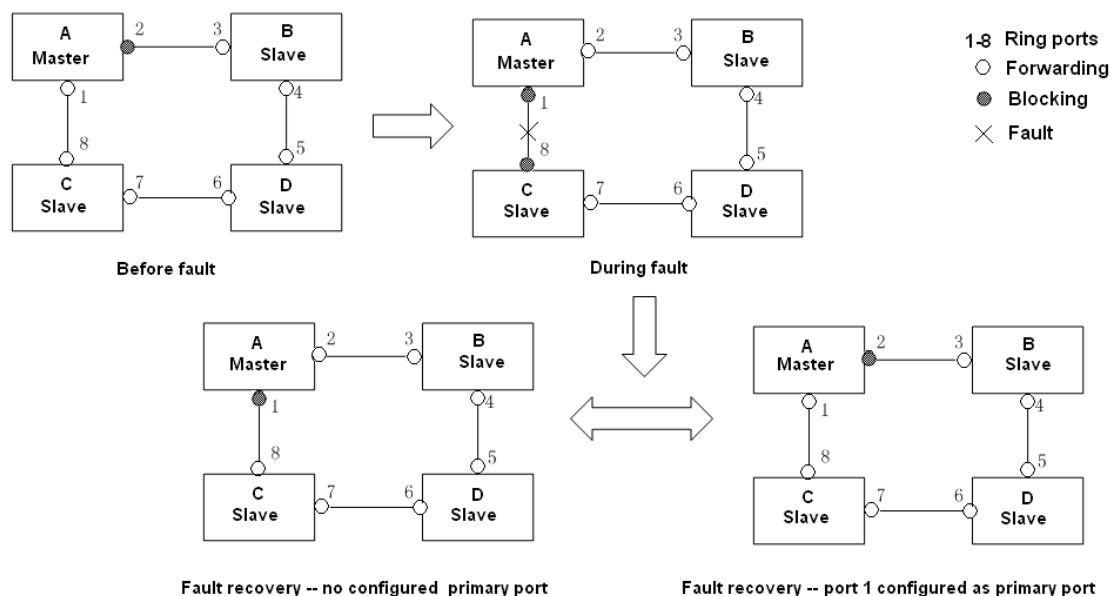


Figure 51 DT-Ring Link Fault



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 the following figure, 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.

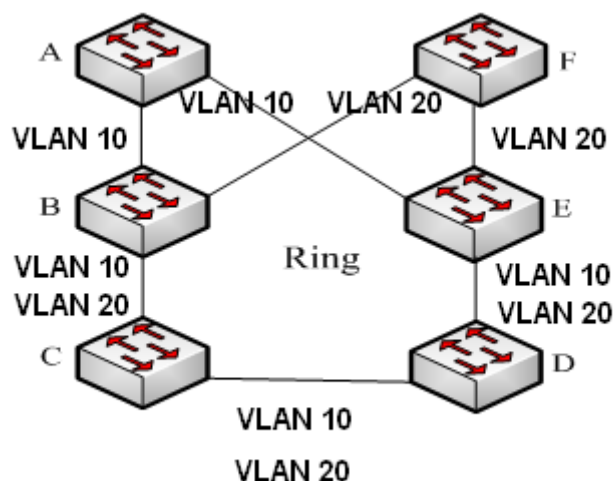


Figure 52 DT-Ring-VLAN



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 the following figure. 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.

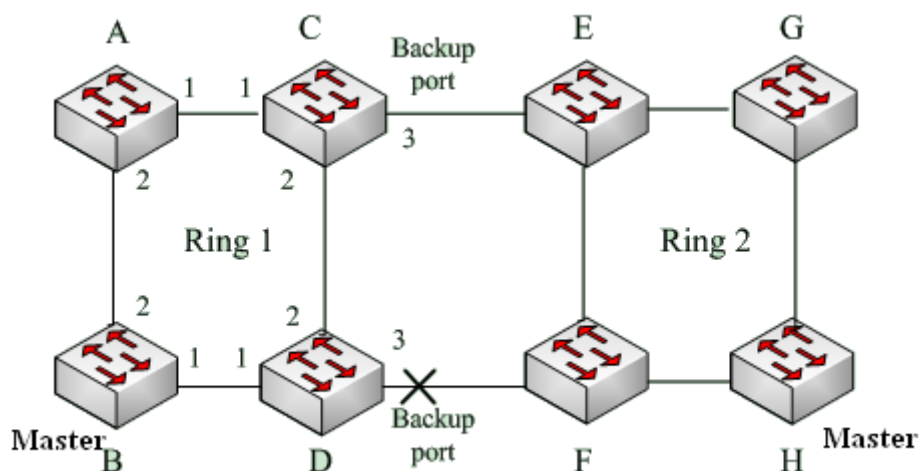


Figure 53 DT-Ring+ Topology



Caution:

Link status change affects the status of backup ports.

12.1.4 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.

12.1.5 Web Configuration

1. Configure redundancy mode, as shown in the following figure.

Figure 54 Configuring Redundancy Mode and Ring Status Detection

Select Redundancy Mode

Options: DT-RING-PORT/DT-RING-VLAN

Default: DT-RING-PORT

Function: Select the redundancy mode.

Check Loop Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable ring status detection.

Description: After ring status detection is enabled, the switch automatically detects ring status. When a non-ring port receives DT-Ring packets, the port will be locked. Therefore,

use the function with caution.

2. Create DT-Ring, as shown in the following figure.

DT-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	DT-RING+ Status	Backup Port	Change times	Ring State
<div style="display: flex; justify-content: center; gap: 20px;"> Add Help </div>							

Figure 55 Creating a DT-Ring

Click <Add> to create DT-Ring and set related parameters.

3. Configure DT-Ring-Port and DT-Ring-VLAN, as shown in the following figures.

DT-RING

Redundancy	DT-RING
Domain ID	1
Domain name	a
Station Type	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Ring Port1	1
Ring Port2	2
Primary Port	1

DT-RING+

DT-RING+	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Backup Port	3

Apply
Help

Figure 56 DT-Ring-Port Configuration

DT-RING

Redundancy	DT-RING
Domain ID	1
Domain name	a
Station Type	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Ring Port1	1
Ring Port2	2
Primary Port	1

DT-RING+

DT-RING+	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Backup Port	3

Add VLAN List

VLAN Choose	VID	VLAN Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	2	2

Apply
Help

Figure 57 DT-Ring-VLAN Configuration

Redundancy

Forcible configuration: DT-RING

Domain ID

Range: 1~32

Function: Differentiate rings. A maximum of 16 port-based rings or 8 VLAN-based rings can be configured on one switch.

Domain name

Range: 1-31 characters

Function: Configure the domain name.

Station Type

Options: Master/Slave

Default: Master

Function: Select the role of the switch in the current ring.

Ring Port1/Ring Port2

Options: All switch ports

Function: Select two ring ports.

Primary Port

Options: Disable/All switch ports

Default: Disable

Function: Configure the primary port.

Description: When the ring is closed, the primary port is in forwarding state.



Caution:

- The primary port takes effect only when the ring is closed.
- The primary port must be one of the two ring ports on the master.

DT-RING+

Options: Enable/Disable

Default: Disable

Function: Enable or disable the DT-Ring+ function.

Backup Port

Options: All switch ports

Function: Select one port as the backup port.

Description: You can configure a backup port only after the DT-Ring+ function is enabled.

Add VLAN List

Options: All created VLAN lists

Function: Select the VLAN whose packets are allowed through on the current ring port.



Caution:

- A ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a ring port or backup port.
- A ring port or backup port cannot be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a ring port or backup port.
- STP cannot be enabled on a ring port or a backup port. An STP-enabled port cannot be

configured as a ring port or backup port.

- DT-Ring and DRP are mutually exclusive. One switch cannot be configured to be on a DT-Ring and a DRP ring at the same time.

After the configurations are completed, created rings are listed in the DT-RING List, as shown in the following figure.

DT-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	DT-RING+ Status	Backup Port	Change times	Ring State
<u>a-1</u>	master	1,2	1	Enable	3	1	RING-CLOSE
<u>b-2</u>	slave	4,5	Disable	Enable	6	0	----

Figure 58 DT-Ring List

4. View and modify DT-Ring configuration.

Click the DT-Ring options in the preceding figure. You can view and modify the configurations of the ring, as shown in the following figure.

DT-RING Configuration

Redundancy	DT-RING
Domain ID	<input type="text" value="1"/>
Domain Name	<input type="text" value="a"/>
Station Type	<input type="text" value="master"/> ▼
Ring Port1	<input type="text" value="1"/> ▼
Ring Port2	<input type="text" value="2"/> ▼
Primary Port	<input type="text" value="1"/> ▼

DT-RING+	<input type="text" value="Enable"/> ▼
Backup Port	<input type="text" value="3"/> ▼

Figure 59 Querying and Modifying DT-Ring Configuration

Click <Apply> for changes to take effect after modification. Click <Delete> to delete the DT-Ring configuration entry.

5. View the status of DT-Ring and ports, as shown in the following figure.

DT-RING State List	
Redundancy	DT-RING
Ring Port 1	forwarding
Ring Port 2	blocking
Ring State	RING-CLOSE
Clean Change times	CLEAN

Redundancy	DT-RING+
Equipment IP	192.168.0.222
Equipment MAC	00-15-7E-0A-40-80
Backup Port Status	blocking
Equipment IP	192.168.0.223
Equipment MAC	00-1E-CD-11-01-B1
Backup Port Status	blocking

Figure 60 DT-Ring Status

12.1.6 Typical Configuration Example

As shown in Figure 53, 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:

1. Domain ID: 1; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 56.

Configuration on switch B:

2. Domain ID: 1; Domain name: Ring; Station Type: Master; Ring Port 1 and 2; no primary port; DT-Ring+: Disable; Backup Port: none, as shown in Figure 56.

Configuration on switch C and switch D:

3. Domain ID: 1; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Enable; Backup Port: 3, as shown in Figure 56.

Configuration on switch E, switch F and switch G:

4. Domain ID: 2; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 56.

Configuration on switch H:

5. Domain ID: 2; Domain name: Ring; Station Type: Master; Ring Port 1 and 2; no primary port; DT-Ring+: Disable; Backup Port: none, as shown in Figure 56.

12.2 RSTP/STP Configuration

12.2.1 Introduction

STP (Spanning Tree Protocol) is based on IEEE802.1D standard and is a protocol of providing link backup to avoid loop and broadcast storm in LAN. The STP-enabled device selectively blocks some ports by mutual information exchange to prune the ring network to loop-free tree network, so as to avoid packet storm in the network. The disadvantage of STP is that it does not support rapid port state transition and ports must wait for twice Forward delay time before transiting to a forwarding state.

In order to solve this disadvantage, IEEE802.1w standard was launched as the supplement of 802.1D standard and defined RSTP (Rapid Spanning Tree Protocol). RSTP protocol made the following improvements based on STP protocol to improve the convergence rate: set an Alternate port for the root port and set a Backup port for the designated port; when the root port is out of running, its Alternate port will enter forwarding state without delay.

12.2.2 Basic Concepts

Root bridge: it works like a tree root in the tree network. There is one and only one root bridge in the entire network. The root bridge changes with the network topology and is not fixed. Root bridge periodically sends out configuration BPDU, and other devices forward this configuration BPDU to guarantee the topology stability.

Root port: the optimum port for the data transmission from a non-root bridge to the root bridge, along with smallest path cost. It is responsible for the communication with the root bridge. There is only one root port on a non-root bridge and there is not root port on the root bridge.

Designated port: a port on the designated bridge and it is responsible for forwarding configuration BPDU to other device or LAN. All ports in the root bridge are designated ports.

Alternate port: the backup port of the root port. When the root port breaks down, the alternate port will become the new root port

Backup port: the backup port of the designated port. When the designated port breaks down,

the backup port will rapidly become the new designated port and forward data.

12.2.3 Configuration BPDU

In order to avoid loops in network, all bridges on LAN calculate a spanning tree together. They confirm the network topology by delivering BPDU messages between them, as shown in Table 4.

Table 4: BPDU Data

...	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: 2 bytes of root bridge priority plus 6 bytes of root bridge MAC address

Root path cost: the cost of the shortest path to the root bridge

Designated bridge ID: 2 bytes of designated bridge priority plus 6 bytes of designated bridge MAC address

Designated port ID: port priority plus port number

Message age: age of the configuration BPDU while it propagates in the network

Max age: the maximum age of configuration BPDU maintained in the device. When Message Age > Max age, drop the BPDU

Hello time: the time interval of sending BPDU

Forward delay: the state transition delay (discarding—learning or learning --forwarding)

12.2.4 Implementation

The specific process of spanning tree calculation by using BPDU message:

1. Initial state: each device port generates a BPDU with itself as the root bridge. Root bridge ID is the device ID, root path cost is 0, designated bridge ID is the device ID, and designated port is the local port.
2. Select the optimum configuration BPDU. Each device sends out its configuration BPDUs, meanwhile it also receives configuration BPDUs from other devices. Once receiving a configuration BPDU, each port will compare it with its own configuration BPDU.
 - If the priority of the configuration BPDU generated by the local port is higher than its

received configuration BPDU, the device does not perform any processing.

- If the priority of the configuration BPDU generated by the local port is lower than its received configuration BPDU, the device will replace the content of configuration BPDU generated by the local port with the content of the received configuration BPDU.

Device elects the optimum configuration BPDU after comparing the configuration BPDUs of all ports. The principles of BPDU comparison:

- The configuration BPDU with the smallest root bridge ID has the highest priority.
- If the root bridge IDs are the same, compare the root path cost. The comparison method: the root path cost of the configuration BPDU plus the corresponding path cost of the port. The configuration BPDU with a smaller value has a higher priority.
- If the root path costs are the same, compare designated bridge ID, designated port ID, the ID of port that receives this configuration BPDU in turn. The configuration BPDU with a smaller value has a higher priority.

3. Select a root bridge. The root bridge of a spanning tree is the one with the smallest bridge ID.

4. Select root ports. The port that can receive the optimum configuration BPDU on the non-root bridge device is the root port.

5. Calculate a configuration BPDU of the designated port. According to the configuration BPDU and the path cost of the root port, the configuration BPDU of the designated port is calculated for each port.

- Root bridge ID is replaced by that of the configuration BPDU of the root port.
- Root path cost is replaced by that of the configuration BPDU of the root port plus the corresponding path cost of the root port.
- Designated bridge ID is replaced by the device ID.
- Designated port ID is replaced by the port ID.

6. Select designated port.

If the calculated configuration BPDU is superior, the device will elect this port to the designated port and the configuration BPDU of the designated port will be replaced by the calculated configuration BPDU that will be forwarded.

If the configuration BPDU of the port is superior, device won't renew the configuration BPDU

of the port and block this port. Blocked ports can receive and forward only RSTP packets, but not other packets.

12.2.5 Web Configuration

1. Enable global STP/RSTP protocol, as shown in Figure 61.

Protocol Settings

Protocol Types	<input type="radio"/> Disable <input checked="" type="radio"/> RSTP <input type="radio"/> STP
-----------------------	---

Figure 61: Enable RSTP/STP Protocol

Protocol Types

Configuration options: Disable/RSTP/STP

Default: Disable

Function: enable/disable spanning tree protocol (RSTP or STP)

2. Configure the time parameters of the network bridge, as shown in Figure 62.

Spanning Tree Priority	<input style="width: 100%;" type="text" value="32768"/> (0-65535)
Hello Time	<input style="width: 100%;" type="text" value="2"/> (1-10s)
Max Age Time	<input style="width: 100%;" type="text" value="20"/> (6-40s)
Forward Delay Time	<input style="width: 100%;" type="text" value="15"/> (4-30s)
Message-age Increment	<input type="radio"/> Compulsion <input checked="" type="radio"/> Default

Apply

Help

Figure 62: Configure Time Parameters of the bridge BPDU

Spanning Tree Priority

Configuration range: 0~65535 with the step length of 4096

Default: 32768

Function: configure bridge priority

Explanation: the bridge priority is used to elect the root bridge. The smaller the value is, the higher the priority is.

Hello Time

Configuration range: 1~10s

Default: 2s

Function: set the time interval of sending configuration BPDU

Max Age Time

Configuration range: 6~40s

Default: 20s

Explanation: when the message age of BPDU is longer than the max age time, drop this BPDU.

Forward Delay Time

Configuration range: 4~30s

Default: 15s

Function: the time of state transition (Discarding—Learning or Learning---Forwarding)

Message-age Increment

Configuration options: Compulsion/Default

Default: Default

Function: set how to modify the message age when a BPDU passes through a bridge.

Explanation: On Compulsion mode, the message age plus one. On Default mode, the message age plus max (max age time/16, 1)

Forward Delay Time, Max Age Time and Hello Time should accord to the following relationship:

$2 \times (\text{Forward Delay Time} - 1.0 \text{ seconds}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time} + 1.0 \text{ seconds})$.

3. Configure the RSTP protocol-enabled port, as shown in Figure 63.

Port Settings

PortType	Protocol Status	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
1	FE <input checked="" type="radio"/> Enable <input type="radio"/> Disable	128	200000	<input checked="" type="radio"/> Yes <input type="radio"/> No
2	FE <input checked="" type="radio"/> Enable <input type="radio"/> Disable	128	2000000	<input type="radio"/> Yes <input checked="" type="radio"/> No
3	FE <input checked="" type="radio"/> Enable <input type="radio"/> Disable	128	2000000	<input checked="" type="radio"/> Yes <input type="radio"/> No
4	FE <input checked="" type="radio"/> Enable <input type="radio"/> Disable	128	2000000	<input type="radio"/> Yes <input checked="" type="radio"/> No
5	FX <input type="radio"/> Enable <input checked="" type="radio"/> Disable	128	200000	<input type="radio"/> Yes <input type="radio"/> No
6	FX <input type="radio"/> Enable <input checked="" type="radio"/> Disable	128	200000	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

Help

Figure 63: Configure the RSTP protocol-enabled port

Protocol Status

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable the spanning tree protocol in port.



Caution:

- Port mirroring and STP are mutually exclusive. The mirroring source/destination port cannot enable STP, while STP-enabled port cannot be set to the mirroring source/destination port.
- Port Trunk and STP are mutually exclusive. The port joining Trunk group cannot enable STP, while STP-enabled port cannot join Trunk group.
- An STP-enabled port can not be configured as a ring port or backup port. STP can not be enabled on a ring port or a backup port.

Port Priority

Configuration range: 0~255 with the step length of 16

Default: 128

Function: Set the port priority to determine the port role

Path Cost

Configuration range: 1~200000000

Default: 2000000 (10M port), 200000 (100M port), 20000 (1000M port)

Explanation: port path cost is used to calculate the optimum path. This value is subject to the bandwidth. The more bandwidth, the lower the cost is. The transmission path from the local device to the root bridge can be changed by changing the port path cost, so as to change the port role. If users would like to change this value by themselves, please choose "No" in Cost Count.

Cost Count

Configuration range: Yes/No

Default: Yes

Explanation: if choose Yes, the port path cost adopts the default value; if choose No, users can configure the port path cost by themselves.

12.2.6 Typical Configuration Example

The priorities of Switch A, B C are 0, 4096, 8192 respectively, and the path costs of three links are 4, 5 and 10 respectively, as shown in Figure 64.

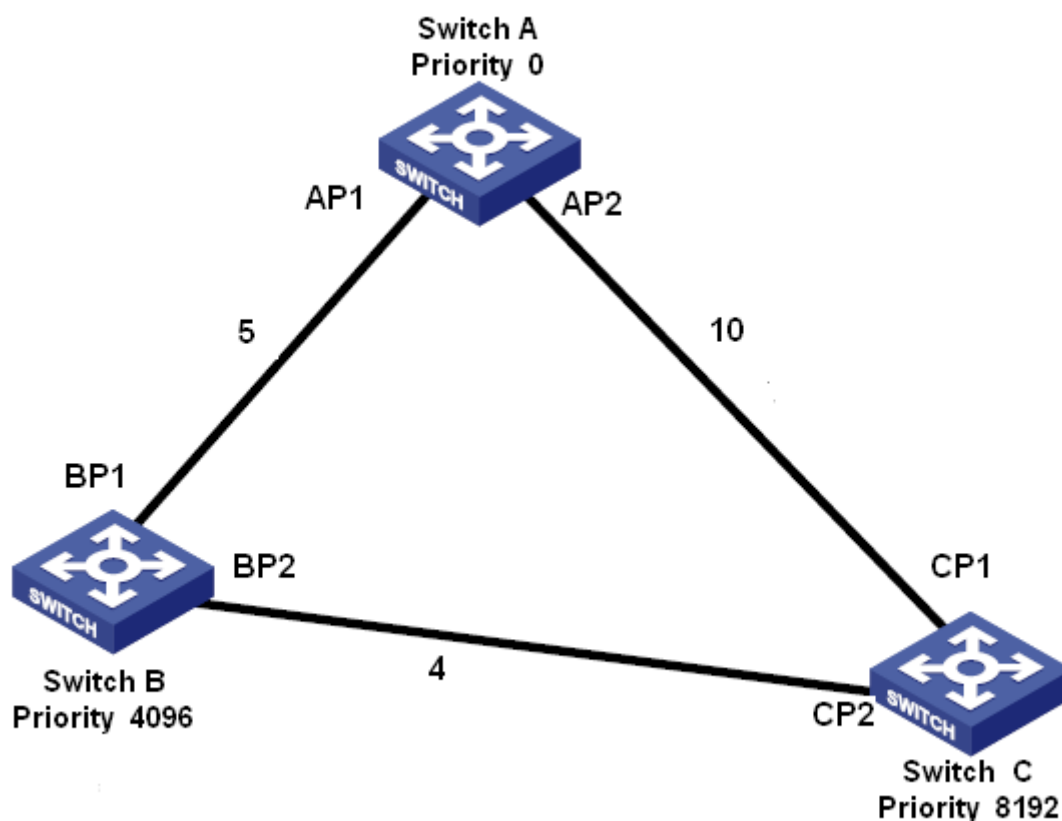


Figure 64: RSTP Example

Switch A Configuration:

1. Set the priority to 0 and the time parameters to the defaults, as shown in Figure 62.
2. Set the path cost of port 1 to 5, and the path cost of port 2 to 10, as shown in Figure 63.

Switch B Configuration:

3. Set the priority to 4096 and the time parameters to the defaults, as shown in Figure 62.
4. Set the path cost of port 1 to 5, and the path cost of port 2 to 4, as shown in Figure 63.

Switch C Configuration:

5. Set the priority to 8192 and the time parameters to the defaults, as shown in Figure 62.

6. Set the path cost of port 1 to 10, and the path cost of port 2 to 4, as shown in Figure 63.
- The priority of Switch A is 0 and has the smallest bridge ID, so it is elected to the root bridge.
 - The path cost from AP1 to BP1 is 5, and the path cost from AP2 to BP2 is 14, so the BP1 is elected to the root port.
 - The path cost from AP1 to CP2 is 9, and the path cost from AP2 to CP1 is 10, so the CP2 is elected to the root port and BP2 is the designated port.

12.3 RSTP/STP Transparent Transmission

12.3.1 Introduction

RSTP protocol is compliant with IEEE standard and DRP/DT-Ring is the private redundant protection protocol of Kyland, but RSTP protocol and DRP/DT-Ring cannot coexist. In order to solve this problem, Kyland develops a RSTP/STP transparent transmission function that can retain other redundant protocols on the switch, meanwhile, transparently transmit RSTP protocol messages, meeting the industrial communication requirements.

When switches that run other redundant protocols enable RSTP transparent transmission function on their ports, they can receive and forward RSTP protocol messages. The RSTP transparent transmission function-enabled switches can be regarded as a transparent link.

In Figure 65, Switch A, B, C and D form a DT-Ring/DRP ring network. After enabling port transparent transmission function in Switch A, B, C and D ports, Switch E and F can receive RSTP protocol messages from each other, detect loops and calculate spanning trees.

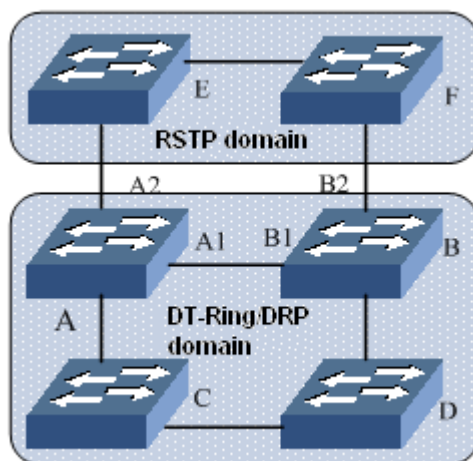


Figure 65: RSTP Transparent Transmission Application

12.3.2 Web Configuration

Configure the RSTP transparent transmission function on port, as shown in Figure 66.

Port	Type	RSTP/STP Transparent Transmission	
1	FE	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
2	FE	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
3	FE	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
4	FE	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
5	FX	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
6	FX	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

Figure 66: RSTP Transparent Transmission Configuration

RSTP/STP Transparent Transmission

Configuration options: Enable/Disable

Default: Disable

Function: Enable RSTP transparent transmission function on port.



Caution:

The RSTP protocol-enabled port cannot enable RSTP transparent transmission function.

12.3.3 Typical Configuration Example

As Figure 65 shows, Switch A, B, C and D form a DRP ring; Switch E and F forms a RSTP

ring, in which the DRP ring form a transparent transmission link to transmit the RTSP protocol messages sent from Switch E or F.

- Switch A, B, C and D form a DRP redundant ring, and the configuration steps are introduced in the "DRP Configuration".
- Enable RSTP protocol in the corresponding ports in Switch E and F (See Figure 61 and Figure 63).
- Enable RSTP transparent transmission function in the A1, A2, A3, B1, B2, B3, C1, C2, D1, D2 ports in Switch A, B, C and D (See Figure 66).

12.4 DRP

12.4.1 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.

12.4.2 Concepts

1. 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.



Caution:

A port in blocking state on the Root can proactively send DRP packets.

2. 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 more 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.

12.4.3 Implementation

The vector of Announce packet

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 5 Vector of an Announce Packet

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

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 5 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.

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 as follows:

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, as shown in the following figure.

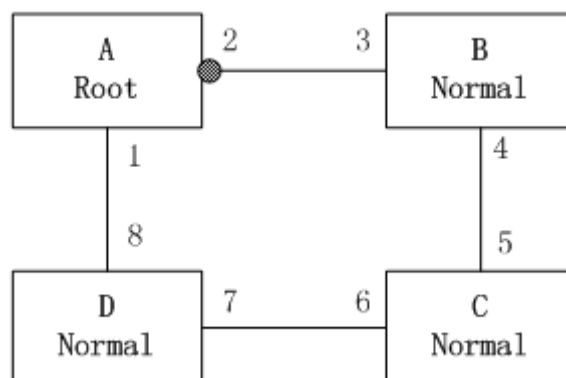


Figure 67 DRP Topology

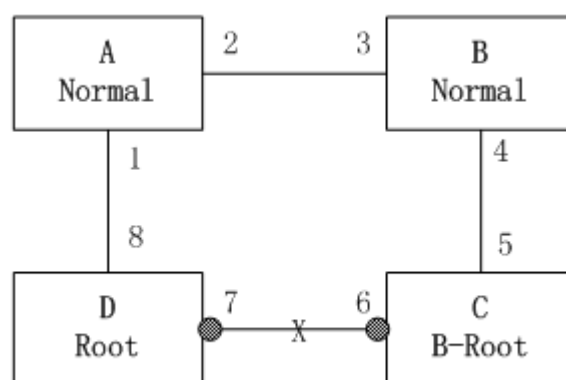


Figure 68 Link Fault

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 state. 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, as shown in the preceding figure.

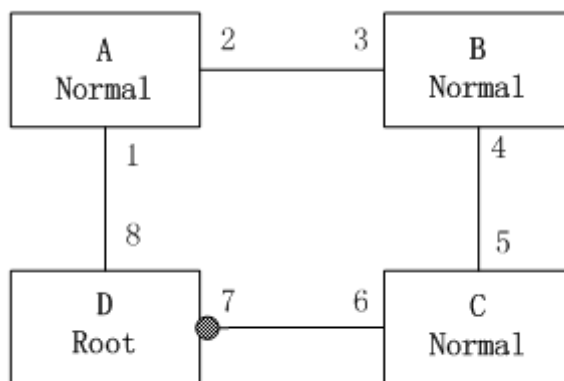


Figure 69 Link Recovery

3. When link CD recovers, D is still the Root because its vector is larger than the vector of C. Because D is the Root, port 7 is in blocking state. In this case, port 6 is in Link up state, so DRP changes the state of port 6 to forwarding. As a result, C becomes a Normal. Therefore, the roles of switches do not change for link recovery.

**Note:**

On 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.

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 the following figure, 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.

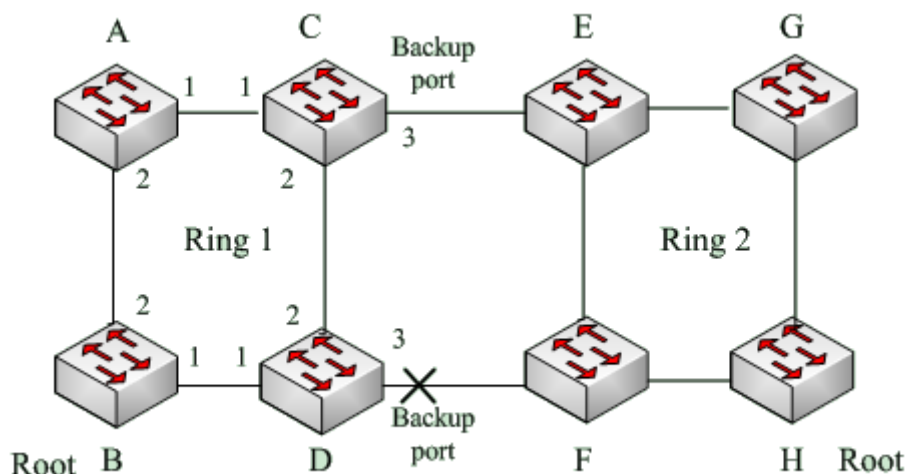


Figure 70 DRP Backup

**Caution:**

Link status change affects the status of backup ports.

12.4.4 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.

12.5 DHP

12.5.1 Overview

As shown in the following figure, 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.

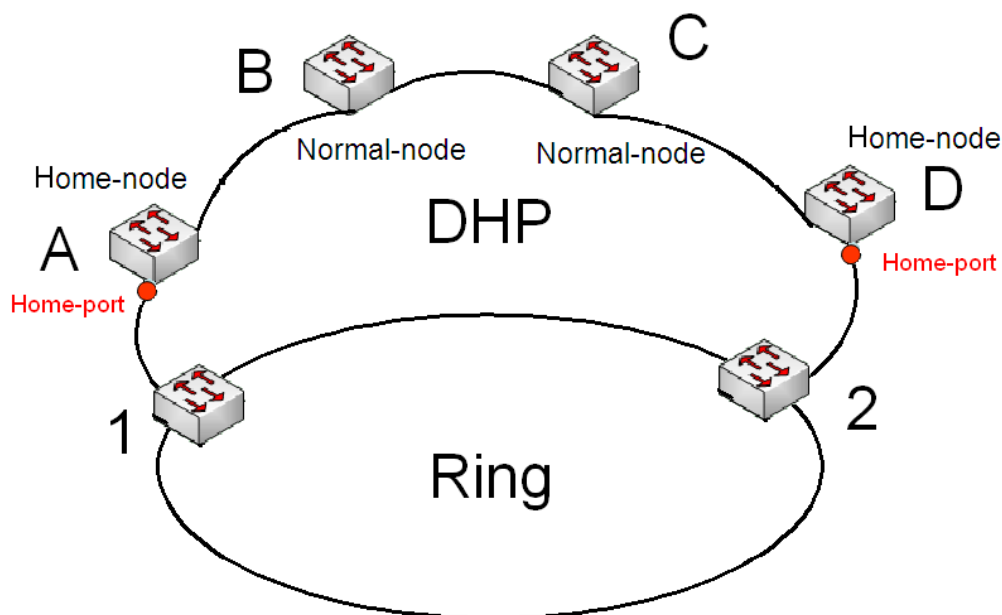


Figure 71 DHP Application

12.5.2 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.

12.5.3 Implementation

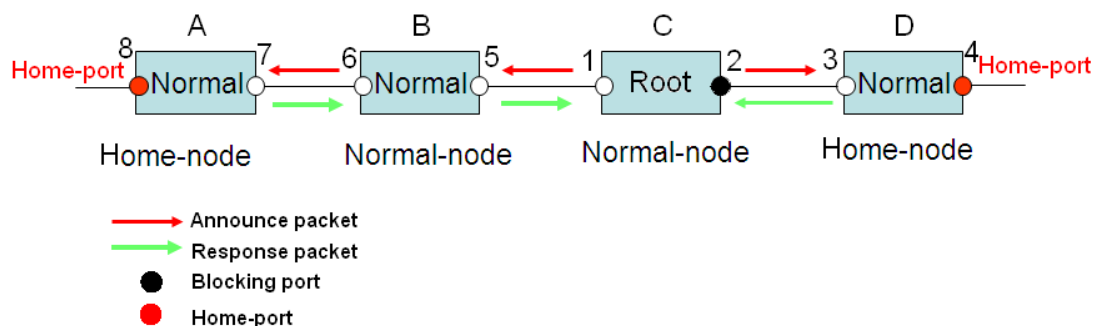


Figure 72 DHP Configuration

As shown in the Figure 72, the configurations of A, B, C, and D in Figure 71 are as follows:

- DRP configuration: C is the Root; port 2 is in blocking state; A, B, and D are Normals; 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 the following figure.

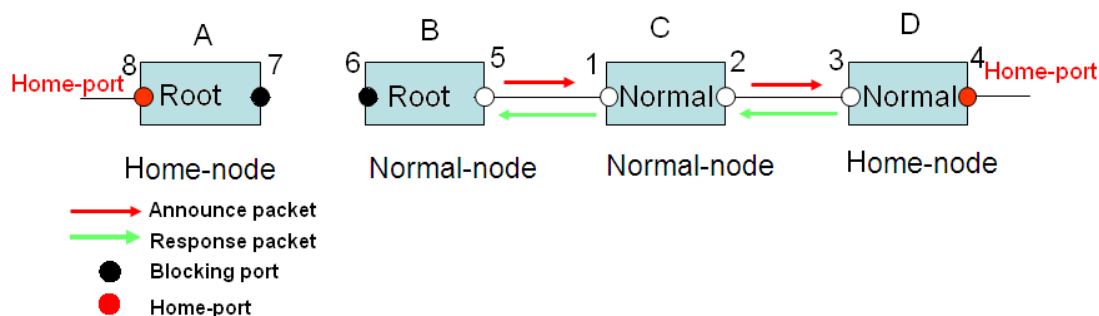


Figure 73 DHP Fault Recovery

12.5.4 Web Configuration

1. DRP configuration, as shown in Figure 74.

DRP Setting

Redundancy	DRP
Domain ID	<input type="text" value="1"/>
Domain Name	<input type="text" value="a"/>
DHP Mode	<input type="text" value="Home Node"/> ▼
Home Port	<input type="text" value="Ring Port 1"/> ▼
Role Priority	<input type="text" value="128"/> (0~255)
CRC Threshold	<input type="text" value="100"/> (25~65535)
Ring Port 1	<input type="text" value="1"/> ▼
Ring Port 2	<input type="text" value="2"/> ▼
Backup Port	<input type="text" value="3"/> ▼

Figure 74: DRP Configuration

Redundancy

Forced configuration: DRP

Domain ID

Range: 1~32

Description: Each ring has a unique domain ID. On one switch, a maximum of 16 DRP rings can be configured.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

DHP Mode

Options: Disable/Normal-node/Home-node

Default: Disable

Function: Disable DHP or configure the DHP mode.

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.

Role-Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

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.

Ring Port 1/Ring Port 2

Options: all switch ports

Function: Select two ring ports.

Backup Port

Options: all switch ports

Function: Configure the backup port.



Caution:

Do not configure a ring port as a backup port.

After you have completed setting the parameters, the created entry will be displayed in the DRP List, as shown in the following figure.

DRP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status
<u>1-a</u>	ROOT	1,2	3	Ring-Close

Figure 75: DRP List

**Caution:**

- A DRP ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a DRP ring port or backup port.
- A DRP ring port or backup port cannot be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a DRP ring port or backup port.
- STP cannot be enabled on a DRP ring port or backup port. An STP-enabled port cannot be configured as a DRP ring port or backup port.
- DT-Ring and DRP are mutually exclusive. One switch cannot be configured to be on a DT-Ring and a DRP ring at the same time.

2. View and modify DT-Ring configuration

Click the DRP entry in Figure 75. You can view and modify the parameter settings of the entry, as shown in the following figure.

DRP Setting

Redundancy	DRP
Domain ID	<input type="text" value="1"/>
Domain Name	<input type="text" value="a"/>
DHP Mode	<input type="text" value="Home Node"/> ▼
Home Port	<input type="text" value="Ring Port 1"/> ▼
Role Priority	<input type="text" value="128"/> (0~255)
CRC Threshold	<input type="text" value="100"/> (25~65535)
Ring Port 1	<input type="text" value="1"/> ▼
Ring Port 2	<input type="text" value="2"/> ▼
Backup Port	<input type="text" value="3"/> ▼

Figure 76 Querying and Modifying a DRP-Port-Based Entry

After modification is completed, click <Apply> to make the modification take effect. You can delete the DRP entry by clicking <Delete>.

3. View the roles and port status of a DRP ring, as shown in the following figure.

DRP Status

Role Status	ROOT
Ring Port 1	FORWARD
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	Ring-Close
IP Address	192.168.0.221
MAC Address	00-15-7E-0A-40-80

Figure 77 DRP-Port-Based Status Query

12.5.5 Typical Configuration Example

As shown in Figure 70, 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 Ring. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 74.

Configuration on switch C and switch D:

2. Set Domain ID to 1, Domain name to Ring, and Backup port to 3. Select ring port 1 and ring port 2. Keep the default value for role priority, as shown in Figure 74.

Configuration on switch E, F, G, and H:

3. Set Domain ID to 2 and Domain name to Ring. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 74.

13. Multicast

13.1 GMRP

13.1.1 GARP Introduction

GARP (Generic Attribute Registration Protocol) is used to distribute, propagate and register certain information (such as VLAN, multicast address) between switches in a network. GARP application is divided to GVRP and GMRP. GVRP will be introduced in "17.3 GVRP". Through GARP mechanism, the configuration information of a GARP member can be rapidly propagated in the entire switching network. The GARP member uses join/leave message to inform other GARP members to register or cancel its attribute information, meanwhile, it can register or cancel the attribute information of other members according to their join/leave messages.

There are three types of messages in GARP: Join, Leave, LeaveAll

- If a GARP-enabled switch wishes other switches to register its certain attribute information, it will send out a Join message. The Join message is divided to two types: Join Empty and Join In. Sending Join In message to declare a registered attribution and sending Join Empty message to declare a non-registered attribute.
- When a GARP-enabled switch wishes other switches to cancel its certain attribute information, it will send out a Leave message.
- When a switch enables GARP, it starts a LeaveAll timer at the same time. When the timer times out, the switch will send out 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.

13.1.2 GMRP Protocol

GMRP (GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP and is used to maintain the multicast registration information of a switch. All GMRP-enabled switches can receive the multicast registration information from other switches, and dynamically renew the local multicast registration information; meanwhile, they can propagate the local multicast registration information to other switches. This information exchanging mechanism guarantees the consistency of the multicast information of all GMPR-supported switches in a same network.

Once a switch or a terminal registers or deregisters a multicast group, the GMPR-enabled port will broadcast this information to other ports in the same VLAN.

13.1.3 Explanation

Agent port: the port that enable GMRP function and agent function.

Propagation port: the port that only enables GMRP function, and does not enable agent function.

Dynamically learned GMRP multicast entry and agent entry are forwarded by the

propagation port to the proration ports of the lower-level devices.

All GMRP timers in the same network must keep consistent to avoid potential interference between them. The timers should follow the rule: hold timer < join timer, 2*join timer < leave timer, leave timer < leaveall timer.

13.1.4 Web Configuration

1. Enable global GMRP protocol, as shown in Figure 78.

Protocol Configure	
GMRP State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LeaveAll Timer	<input type="text" value="10000"/> ms
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 78: GMRP Global Configuration

GMRP State

Configuration options: Enable/Disable

Default: Disable

Function: enable/disable global GMRP function. This function cannot be used with IGMP-Snooping function.

LeaveAll Timer

Configuration range: 100ms~327600ms

Default: 10000ms

Function: the time interval of sending leave all message. It must be a multiple of 100.

Explanation: if the LeaveAll timers of different devices time out at the same time, multiple LeaveAll messages will be sent out at the same time, which increases the message quantity.

In order to avoid this problem, the actual running time of a LeaveAll timer is a random value, which is longer than the time of a LeaveAll timer, and less than 1.5 times of a LeaveAll timer.

2. Set GMRP function for each port, as shown in Figure 79.

Port Configure

PortType	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
1 FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	100 ms	500 ms	3000 ms
2 FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	100 ms	500 ms	3000 ms
3 FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	100 ms	500 ms	3000 ms
4 FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	100 ms	500 ms	3000 ms
5 FX	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	100 ms	500 ms	3000 ms
6 FX	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	100 ms	500 ms	3000 ms

Figure 79: Port GMRP Configuration

GMRP Enable

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable GMRP function on port

Agent Enable

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable GMRP agent function on port



Caution:

- Agent ports cannot propagate agent entries.
- The premise of enabling GMRP agent function on port is to enable GMRP function on port.

Hold Timer

Configuration range: 100ms~327600ms

Default: 100ms

Explanation: This value must be a multiple of 100. It is better to set a same time of Hold timers for all GMRP-enabled ports

Join Timer

Configuration range: 100ms~327600ms

Default: 500ms

Explanation: This value must be a multiple of 100. It is better to set a same time of Join timers for all GMRP-enabled ports

Leave Timer

Configuration range: 100ms~327600ms

Default: 3000ms

Explanation: This value must be a multiple of 100. It is better to set a same time of Leave timers for all GMRP-enabled ports

3. Add a GMRP agent entry, as shown in Figure 80.

GMRP Agent Set

MAC	01-00-00-00-00-01
VLAN ID	1 (1-4093)

Port List

NOTE: Multicast propagation port cannot be set as member port!

Member Port List

1	
---	--

Apply

<<

>>

Source Port List

--	--

Help

Figure 80: GMRP agent entry configuration

MAC

Configuration format: HH-HH-HH-HH- HH - HH (H is a hexadecimal number)

Function: configure the MAC address of the multicast group, and the lowest bit of the highest byte is 1.

VLAN ID

Configuration options: all existing VLAN IDs

Function: configure a VLAN ID for the GMRP agent entry

Explanation: GMRP agent entry can only be forwarded from the propagation port whose VLAN ID is the same as that of the agent entry.

Member Port List

Select member ports for the agent entry and select from agent ports.

Source Port List

Configuration options: all GMRP Agent-enabled ports

4. Show, modify and delete GMRP agent entry, as shown in Figure 81.

GMRP Agent List

Index	MAC	VLAN ID	Member Port
<input type="radio"/> 1	01-00-00-00-00-01	1	1
<input type="radio"/> 2	01-00-00-00-00-02	2	1

Add
Delete
Modify
Help

Figure 81: GMRP agent entry operations

It displays the agent AMC address, VLAN ID, member ports. Choose an entry, click <Delete> button to delete the entry; click <Modify> to modify the member ports of the agent entry.

5. Check the multicast members of the agent entry in the connected neighbor device, as shown in Figure 82. But it should meet the following conditions:

- The connected devices both enable GMRP function.
- The two ports that connect two devices must be propagation ports.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	2

Figure 82: GMRP Dynamic multicast table

GMRP Dynamic Multicast List

Group displaying: {Index, Multicast MAC, VLAN ID, Member Port}

Function: show GMRP dynamic multicast entries

13.1.5 Typical Configuration Example

As Figure 83 shows, switch A and Switch B are connected by port 2. Port 1 of switch A is set to an agent port and contains two multicast entries:

MAC address: 01-00-00-00-00-01, VLAN: 1

MAC address: 01-00-00-00-00-02, VLAN: 2

Observe the dynamic registration between switches and multicast information update by setting different VLAN attribute for ports

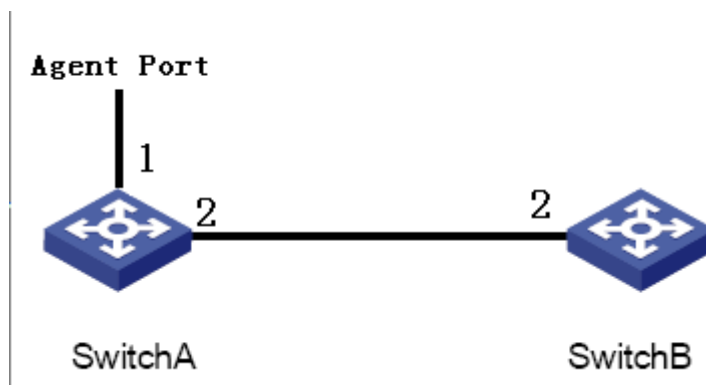


Figure 83: GMRP networking

Switch A configuration:

1. Enable global GMRP function in Switch A; LeaveAll timer uses the default value, as shown in Figure 78.
2. Enable GMRP function and agent function in port 1; only enable GMPR function in port 2; the timers all use default values, as shown in Figure 79.
3. Configure the agent multicast entry. <MAC address, VLAN ID, Member port> configure to {01-00-00-00-00-01, 1, 1} and {01-00-00-00-00-02, 2, 1}, as shown in Figure 80.

Switch B configuration:

4. Enable global GMRP function in switch B; LeaveAll timer uses the default value, as shown in Figure 78.
5. Enable GMPR function in port 2; the timers all use default values, as shown in Figure 79.

Dynamic GMRP multicast entries in Switch B are shown in Table 6.

Table 6: Dynamic Multicast Entries

Attribute of Switch A port 2	Attribute of Switch B port 2	Switch B-received Multicast Entries
Untag1	Untag1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Untag2	Untag2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2

Untag1	Untag2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2
--------	--------	--

13.2 Static FDB Multicast

13.2.1 Introduction

Multicast address table can be statically configured. An entry is added into the multicast address table in the form of {Multicast MAC address, VLAN ID, Multicast member port}, and a multicast message will be forwarded to the corresponding member port according to the entry

13.2.2 Web Configuration

1. Enable static FDB multicast, as shown in Figure 84.

FDB Multicast Status

☒ Enable
☐ Disable

Apply

Help

Figure 84: Enable Static FDB Multicast

FDB Multicast Status

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable static multicast. Static Multicast and IGMP Snooping can not be enabled at the same time.

2. Add a static multicast entry, as shown in Figure 85.

Static FDB Multicast List Configuration

MAC	01-01-01-01-01-01
VLAN ID	1 (1-4093)

Port List

Port	1	2	3	4	5	6	S-CH
Type	FE	FE	FE	FE	FX	FX	S-CH
Select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply
Help

Figure 85: Add Static Multicast Address Entry

MAC

Configuration format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: configure multicast group address. The lowest bit of the highest byte is 1.

VLAN ID

Configuration options: all existing VLAN IDs

Function: set the VLAN ID of the static multicast entry. Only VLAN member ports can forward this multicast message.

Port List

Function: choose the member ports of the multicast address. If a host connected to a port would like to receive a certain multicast group data, statically add this port into the multicast group and become a static member port.

3. Show, modify and delete static multicast entry, as shown in Figure 86.

Static FDB Multicast List

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	01-01-01-01-01-01	1	1,2,3

Add
Delete
Modify
Help

Figure 86: Static Multicast Entry Operations

Static FDB multicast list displays MAC address, VLAN ID and member ports. Choose an entry, click <Delete> to delete the entry; click <Modify> to modify the member ports of the entry.

13.3 IGMP Snooping

13.3.1 Introduction

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast protocol running in data link layer and is used to manage and control multicast group. The IGMP Snooping-enabled switch analyzes the received IGMP message to establish mapping relationships of port and MAC multicast address, and forward multicast messages according to these mapping relationships.

13.3.2 Basic Concepts

Querier: periodically sending general IGMP query messages to inquire whether multicast group members are active, so as to maintain multicast group information. If there are multiple queriers in network, they will automatically elect the one with the smallest IP address to be querier. Only the elected querier can periodically send out IGMP query messages, while other non-querier devices can receive and forward query messages, instead of sending out query messages.

Router port: in IGMP-enabled device, the port that receives the IGMP query message from the querier is the router port. When an IGMP report arrives, the device need to create a multicast entry and the port that receives the IGMP report becomes a member port. In addition, if there is a router port, add it into the member port list. Meanwhile, the device will forward the IGMP report message from the router port to other devices, so as to establish a same multicast entry in other devices.

13.3.3 Principle

IGMP Snooping conducts management and maintenance of multicast group members through sending related messages between IGMP devices. It mainly contains following important messages:

General query message: the querier periodically sends out a general query message with the fixed destination IP address of 224.0.0.1 to confirm the existence of multicast group member ports. When the non-querier device receives the general query message, it also

forwards the message to all connected ports.

Specified query message: if a host wishes to leave a multicast group, it will send an IGMP leave message. When the querier receives this message, it will send out an IGMP specified query message (its destination IP is the IP address of the multicast group that the host wants to leave) to check whether there is other members in this multicast group.

Member report message: if a host wishes to receive a certain multicast group data, it will respond to IGMP query message by sending IGMP member report message (its destination IP address is the IP address of the multicast group that the host would like to join in).

Leave group message: if a host wishes to leave a multicast group, it will send an IGMP leave message with the fixed destination IP address of 224.0.0.2.

13.3.4 Web Configuration

1. Enable IGMP Snooping protocol and enable Auto-query, as shown in Figure 87.

IGMP Snooping Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Query Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Cross Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 87: Enable IGMP Snooping

IGMP Snooping Status

Configuration options: Enable/Disable

Default: Disable

Function: enable/disable IGMP Snooping function. This function cannot use together with Static Multicast/GMRP function.

Auto Query Status

Configuration options: Enable/Disable

Default: Disable

Function: the switch participates the querier election or not.

Explanation: Only when the IGMP Snooping is enabled can auto-query function be enabled.



Caution:

At least one switch enables auto-query function.

IGMP Cross Status

Options: Enable/Disable

Default: Disable

Function: If the function is enabled, report and leave packets can be forwarded by the DT-Ring ports.

2. Show IGMP member list, as shown in Figure 88.

IGMP Member List		
MAC	VLAN ID	Member
01-00-5E-7F-FF-FE	1	6
01-00-5E-51-09-08	1	6
01-00-5E-00-01-01	1	6
01-00-5E-0A-18-03	1	6
01-00-5E-7F-FF-FA	1	4 6

Figure 88: IGMP Snooping Member List

IGMP Member List

Group Displaying: {MAC, VLAN ID, Member}

Function: show the FDB multicast table that are dynamically learned by IGMP Snooping. VLAN ID is the VLAN ID of the member port.

13.3.5 Typical Application Example

As Figure 89 shows, enable IGMP Snooping function in Switch 1, Switch 2, Switch 3; switch 2 and switch 3 enable Auto Query. The IP address of Switch 2 is 192.168.1.2; the IP address of Switch 3 is 192.168.0.2, so Switch 3 is elected to the querier.

1. Enable IGMP Snooping function in Switch 1.
2. Enable IGMP Snooping and auto-query functions in Switch 2 .
3. Enable IGMP Snooping and auto-query functions in Switch 3.

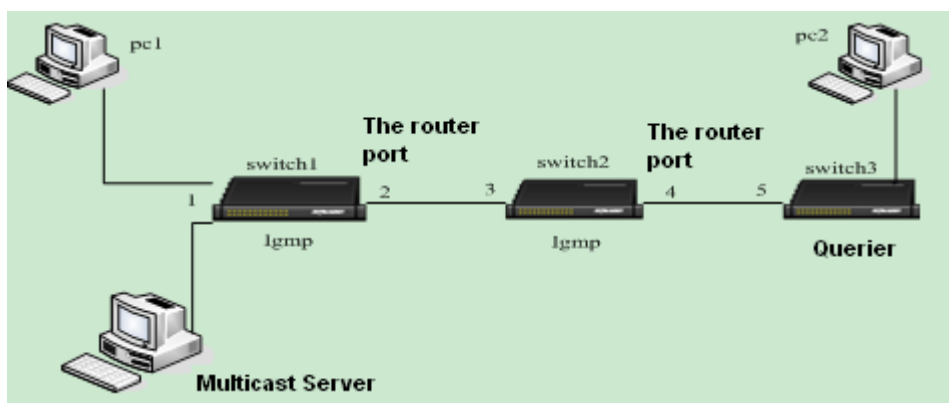


Figure 89: IGMP Snooping Application Example

- Because Switch 3 is elected to the querier, it will periodically send out a general query message, and then port 4 of Switch 2 will receive the query message, so it is elected to a router port, then the query message will be forwarded from the port 3 of Switch 2, and the port 2 of Switch 1 will receive the message and it will be elected to a router port.
- When PC 1 joins in the multicast group 225.1.1.1, it will send IGMP report messages of the multicast group to Switch 1, so port 1 and router port 2 of Switch 1 will also join in the multicast group 225.1.1.1; then, IGMP report messages will be forwarded to Switch 2 from the router port 2, so the port 3 and port 4 of Switch 2 will also join in multicast group 225.1.1.1, and then IGMP report messages will be forwarded to Switch 3 from the router port 4, so port 5 of Switch 3 will join in the multicast group 225.1.1.1 as well.
- When the multicast data from the multicast server reaches Switch 1, the data will be forwarded to pc1 by port 1; because router port 2 also enter the multicast group, so the multicast data will be forwarded from the router port 2. In this way, when the data reaches port 5 of Switch 3, the forwarding will stop because there is no receiver any more, but if pc2 also enter 255.1.1.1, the multicast data will be forwarded to pc2, too.

14. Diagnosis

14.1 Port Mirroring

14.1.1 Introduction

Port mirroring function is that the switch copies all received or transmitted data frames in a port (mirroring source port) to another port (mirroring destination port), and the mirroring destination port connects with a protocol analyzer or RMON monitor for network monitoring, management and fault diagnosis.

14.1.2 Explanation

A switch supports only one mirroring destination port, but there is no such restriction on mirroring source ports and it supports one or multiple source ports. Multiple source ports can be in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

Source port and destination port cannot be the same port.



Caution:

- Port mirroring and Port Trunk are mutually exclusive. The mirroring source/destination port cannot be added into a Trunk group, while the ports joining a Trunk group cannot be set to a mirroring destination/source port .
- Port mirroring and redundant protocol configuration are mutually exclusive. The mirroring destination/source port can neither enable redundant protocols nor be set to a redundant port, while the redundant protocol-enabled port and redundant port cannot be set to a mirroring source/destination port.

14.1.3 Web Configuration

1. Select the mirroring destination port, as shown in Figure 90.



Monitoring Port 2

Figure 90: Mirroring Destination Port

Monitoring Port

Configuration options: NULL/ one switch port

Default: NULL

Function: Select a port to be the mirroring destination port. There is one and only one mirroring destination port.

2. Select mirroring source ports and the mirroring mode, as shown in Figure 91.

Port ID	Type	Monitored	Mode
1	FE	<input checked="" type="checkbox"/>	<input type="radio"/> RX <input type="radio"/> TX <input checked="" type="radio"/> RX & TX
2	FE	<input type="checkbox"/>	<input checked="" type="radio"/> RX <input type="radio"/> TX <input type="radio"/> RX & TX
3	FE	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> RX <input type="radio"/> TX <input type="radio"/> RX & TX
4	FE	<input checked="" type="checkbox"/>	<input type="radio"/> RX <input checked="" type="radio"/> TX <input type="radio"/> RX & TX
5	FX	<input type="checkbox"/>	<input checked="" type="radio"/> RX <input type="radio"/> TX <input type="radio"/> RX & TX
6	FX	<input type="checkbox"/>	<input checked="" type="radio"/> RX <input type="radio"/> TX <input type="radio"/> RX & TX
S-CH	S-CH	<input type="checkbox"/>	<input checked="" type="radio"/> RX <input type="radio"/> TX <input type="radio"/> RX & TX

Apply Help

Figure 91: Mirroring Source Port

Mode

Configuration options: RX/TX/RX&TX

Function: Select the data to be mirrored.

TX only mirror the transmitted messages of the source port

RX only mirror the received messages of the source port

TX&RX mirror both transmitted and received messages of the source port

14.1.4 Typical Configuration Example

As Figure 92 shows, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received messages on port 1 are mirrored to port 2

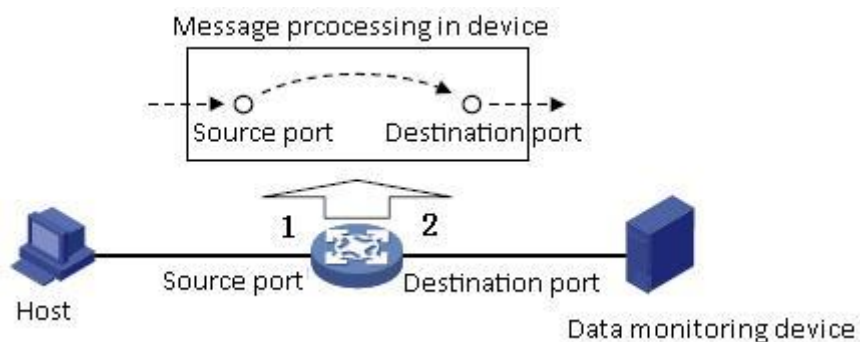


Figure 92: Port Mirroring Example

Configuration process:

1. Set port 2 to the mirroring destination port, as shown in Figure 90.
2. Set port 1 to the mirroring source port and the port mirroring mode is set to RX&TX, as shown in Figure 91.

14.2 Link Check

14.2.1 Introduction

Link Check detects the data transmission of redundancy protocol-enabled ports. Link Check helps to detect the anomaly for timely processing when a fault occurs.

14.2.2 Web Configuration

Link Check configuration, as shown in Figure 93.

Link Check

Port	Type	Administration Status		Run Status
1	FE	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	Receive Fault
2	FE	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	Receive Fault
3	FE	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	Normal Link
4	FE	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Disable
5	FX	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Disable
6	FX	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Disable

Figure 93: Link Check

Administration Status

Configuration options: Enable/Disable

Default: Enable

Explanation: The function can be enabled only on a redundant protocol-enabled port.



Caution:

If the peer device does not support the function, the function shall be disabled on the connected port of the local device.

Run Status

Configuration options: Normal Link/Receive Fault/Disable/Send Fault

Explanation: If Link Check is enabled on a redundant port and the port sends and receives data normally, Normal Link is displayed. If the peer end does not receive the detection packets from the device, Send Fault is displayed. If the device does not receive detection packets from the peer end, Receive Fault is displayed. If Link Check is not enabled on a port, Disable is displayed.

14.3 Virtual Cable Tester

14.3.1 Introduction

VCT (Virtual Cable Tester) uses Time Domain Reflectometry (TDR) to detect Twisted-pair status. It transmits a pulse signal to the cable and detects the reflection of the pulse signal to detect the cable fault. If a failover occurs in the cable, parts of or all pulse energy will be reflected back to the sending source when the transmitted pulse signal reaches the end of the cable or the fault point, and VCT technology can measure the signal arrival time at the fault point and the time of getting back to the sending source, then calculates the distance according to the time.

14.3.2 Implementation

VCT technology can detect the media of link connecting the Ethernet copper ports and send back the detection result. VCT can detect the following types of cable faults:

Short: it means short circuit. It is that two or more wires are shorted.

Open: it means open circuit. There might be broken wires on the cable.

Normal: it means normal cable connection.

Imped: it means impedance mismatch. For example, the impedance of the Cat.5 cable is 100 ohm, the impedance of the terminators at the both ends of the cable must be 100 ohm to avoid wave reflection and data error.

Fail: it means VCT test fails.



Note:

The color of the cable for RJ45 connector meets the 568B standard: 1-orange and white, 2-orange, 3-green and white, 4-blue, 5-blue and white, 6-green, 7-brown and white, and 8-brown. (1, 2), (3, 6), (4, 5), (7, 8) are four cable pairs.

14.3.3 Web Configuration

Detect a cable, as shown in Figure 94.

<input type="checkbox"/> All	Detecting Port	Type	cable-pair	Status	Length(m)
<input type="checkbox"/>	1	FE	(1,2)	Open	1
			(3,6)	Open	1
<input type="checkbox"/>	2	FE	(1,2)	no history	no history
			(3,6)	no history	no history
<input type="checkbox"/>	3	FE	(1,2)	Normal	Unknown
			(3,6)	Normal	Unknown
<input type="checkbox"/>	4	FE	(1,2)	no history	no history
			(3,6)	no history	no history

[Note]: 1. The port will be link down while being tested.
2. If the result is "Normal" or "Mismatch", the length can not be tested.

Test

Link Down

Link Up

Figure 94: VCT Detection

Detecting Port

Configuration options: all switch copper ports

Method: select a port, and then click <Test> to detect the cable pair state of the current port.

Type

Show the port port.

Cable-pair

For 10/100Base-T(X) RJ45 port, only (1, 2) and (3, 6) cable pairs are tested; for 10/100/1000Base-T(X) RJ45 port, (1, 2), (3, 6), (4, 5), (7, 8) cable pairs are tested.

Status

Displaying options: Open/Short/Normal/ Mismatch/Fail

Function: show the cable pair state of the current port, including open circuit, short circuit, normal connection, impedance mismatch, testing fail.

Length

Function: Show the distance between the port and the fault point. There is light deviation about the VCT technology. The distance of the normal cable pair is unknown.

Click <Test> to detect the cable pair state of the selected ports and then display the test result; click <Link Down> to detect the cable pair state of all link down ports and then display the test result; click <Link Up> to detect the cable pair state of all link up ports and then display the test result.

**Caution:**

The port will be link down while testing.

15. SNTP

15.1 Introduction

SNTP (Simple Network Time Protocol) calibrates time by requests and responses between servers and clients. Switches work as clients to calibrate time according to the messages from the server. Four SNTP servers are supported at the same time, but only one server is in active state.

The request from the SNTP client is gradually sent to each server in the form of unicast, and the server that firstly responds will enter an active state, and other servers are in inactive state.

**Caution:**

- The switch cannot serve as the SNTP server.
- To synchronize time by SNTP, there must be an active SNTP server.

15.2 Web Configuration

1. Enable SNTP protocol and configure SNTP server, as shown in Figure 95.

SNTP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Server IP	<input type="text" value="192.168.0.23"/>
Interval Time	<input type="text" value="16"/> (16-16284s)
Time Zone	<input type="text" value="GMT+8(Beijing Time)"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 95: SNTP Configuration

SNTP Status

Configuration options: Enable/Disable

Default: Disable

Function: enable/disable SNTP protocol

Server IP

Configuration format: A.B.C.D

Function: configure the IP address of the SNTP server and the client calibrates time according to the messages from this server

Interval Time

Configuration range: 16~16284s

Function: set the interval of the SNTP client sending a synchronous request to the SNTP server

Time Zone

Configuration options: GMT, GMT+1, GMT+2, GMT+3, GMT+4, GMT+5, GMT+6, GMT+7, GMT+8, GMT+9, GMT+10, GMT+11, GMT+12, GMT-1, GMT-2, GMT-3, GMT-4, GMT-5, GMT-6, GMT-7, GMT-8, GMT-9, GMT-10, GMT-11

Function: choose the local time zone

2. Choose the client-and-server time synchronization form, as shown in Figure 96.

Last synchronization Time	2011.08.05 15:40:52
Device Time	2011.08.05 15:40:53
Update	<input checked="" type="radio"/> Automatism <input type="radio"/> Manual <input type="button" value="Apply"/>

Figure 96: Time Synchronization Form

Last synchronization time

Displaying format: yyyy.mm.dd hh.mm.ss

Default: 0000.00.00 00.00.00

Function: show the time obtained from the server

Device Time

Displaying format: yyyy.mm.dd hh.mm.ss

Function: show the local time of the device

Update

Configuration options: Automatism/Manual

Default: Automatism

Function: choose the client-and-server time synchronization form

3. Show SNTP configuration information, as shown in Figure 97.

Number	Server IP	Server Status	Time Zone	Interval Time	Synchronization
<input type="checkbox"/> 1	192.168.0.23	active	+ 8	16	<input type="button" value="Synch"/>
<input type="checkbox"/> 2	192.168.0.56	repose	+ 8	20	<input type="button" value="Synch"/>

Figure 97: SNTP Configuration Information

Number

Select the number to delete the corresponding server configuration.

Server Status

Displaying options: active/repose

The server in active state provides SNTP time to the client. There is one and only one server that is in active state, and others are in repose at the same time.

Synchronization

Function: click <Synch> button in the "Manual" synchronization form

16. Security

16.1 SSH

16.1.1 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 switch supports the SSH server function and allows the connection of multiple SSH users that log in to the switch remotely through SSH, but only one user can connect to the switch at a time.

16.1.2 Secret Key

The unencrypted message is called plaintext, and the encrypted message is called cipher text. Encryption or decryption is under the control of the secret key. A secret key is a specific character string and is the only parameter to control the transformation between plain text and cipher text, working as a Key. Encryption can change plain text to cipher text, while decryption can change cipher text to plain text.

The key-based security authentication needs secret keys, and each end of the communication has a pair of secret keys, private key and public key. Public key is used to encrypt data, and the legal owner of private key can use the private key to decrypt the data to guarantee the data security.

16.1.3 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

16.1.4 Web Configuration

➤ SSH server configuration steps:

1. Disable SSH Status.
2. Click <Destroy> to destroy the old key pair, as shown in Figure 98.

SSH State		<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Authentication Retry Times	<input type="text" value="10"/>	(1-10)	
Time Out	<input type="text" value="300"/>	(60-300)s	
Local Key Pair	<input type="button" value="Create"/> <input type="button" value="Destroy"/>		
Local Key Value	<div>NULL</div>		

Figure 98: Destroy the Old Key Pair

3. Click <Create> to create a new key pair, as shown in Figure 99.

SSH State	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Authentication Retry Times	10	(1-10)
Time Out	300	(60-300)s
Local Key Pair	<input type="button" value="Create"/> <input type="button" value="Destroy"/>	
Local Key Value	Public key portion is: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAg wCcvfc9zy00UPW0Dmbtydi0EHsWPP VTh8sf/tBreFoGLXnA/OmW/hy664E	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Figure 99: Create a new key pair

4. Enable SSH protocol and configure the SSH server, as shown in Figure 100.

SSH State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Authentication Retry Times	10	(1-10)
Time Out	300	(60-300)s
Local Key Pair	<input type="button" value="Create"/> <input type="button" value="Destroy"/>	
Local Key Value	Public key portion is: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAg wCcvfc9zy00UPW0Dmbtydi0EHsWPP VTh8sf/tBreFoGLXnA/OmW/hy664E	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Figure 100: SSH server configuration

SSH State

Configuration options: Enable/Disable

Default: Disable

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

Authentication Retry Times

Configuration range: 1~10

Default: 10

Function: set the number of attempts to log into SSH server

Time Out

Configuration range: 60~300

Default: 300

Function: set the time that the SSH client connection lasts when there is no data transmission. When the time is out, the connection automatically disconnects.

Local Key Pair

Configuration options: Create/Destroy

Function: create or destroy the local key pair of the SSH server. Please create a local key pair before enabling SSH server; destroy the old key pair before creating a new key pair.

Local Key Value

Function: show the local key value. Click <Create> to automatically generate the key value.

➤ SSH key configuration steps:

1. SSH key configuration, as shown in Figure 101.

Key Configure

Key Name	333
Key Type	<input checked="" type="radio"/> RSA
Key Value	<pre>fPxH9tPc79dmB7fkXB1dhCmTAipzE jGVikqp d9R4V4dD0dRQhNo5oxvN9J es4JvvveXkvVOId918R5p0TxoYa8 LlopqJjsI/Vb0cyDJV1D/Fdw== rsa-key-20110706</pre>

Format of Key Value: [algo-name] [pubkey] [keyinfo]
 [algo-name] : ssh-rsa | ssh-dsa
 [pubkey] : base64 code, less than 2048Byte
 [keyinfo] : more info for this key

Figure 101: SSH key configuration

Key Name

Configuration range: 3~20 characters

Function: set the key name and support max 3 keys

Key Type

Fixed configuration: RSA

Explanation: this series switches only support RSA key algorithm

Key Value

Configuration format: {algorithm name, public key, key info}

Algorithm name: ssh-rsa | ssh-dsa

Public key: it is based on 64 codes and the length is less than 2048 bytes

Key info: more info for the key

Function: configure the public key corresponding to the client

Explanation: Generally, the public key is generated by Puttygen software and is copied to the key value of the server; the private key is saved in the client.

2. Show public key list and delete the selected key, as shown in Figure 102.

Public Key List

Index	Key Name	Key Type
<input type="checkbox"/> 1	111	RSA
<input checked="" type="checkbox"/> 2	222	RSA
<input type="checkbox"/> 3	333	RSA

Figure 102: Show key list

➤ SSH user configuration steps:

1. SSH user configuration, as shown in Figure 103.

SSH User Manager

User Name		<input type="text" value="ddd"/>
Authentication Type	<input type="radio"/> Public Key	<input type="text" value="111"/> ▼
	<input checked="" type="radio"/> Password	<input type="password" value="•••"/>

Figure 103: SSH user configuration

User Name

Configuration range: 3~20 characters

Function: create a user name and support max 4 users

Authentication Type

Configuration options: Public Key/Password

Default: Public key

Function: set user authentication types. If choose "Public Key", choose one key from the

public key list; if choose "Password", input 3~8 characters to be password.

2. Show SSH user list and delete the selected user, as shown in Figure 104.

SSH User List

Index	User Name	Authen-Type	Password/Key
<input type="checkbox"/> 1	aaa	Public Key	111
<input type="checkbox"/> 2	bbb	Public Key	222
<input type="checkbox"/> 3	ccc	Public Key	333
<input type="checkbox"/> 4	ddd	Password	44/E1yyNEjdEc

Figure 104: Show User List

16.1.5 Typical Configuration Example

The Host works as the SSH client to establish a local connection with Switch, as shown in Figure 105.

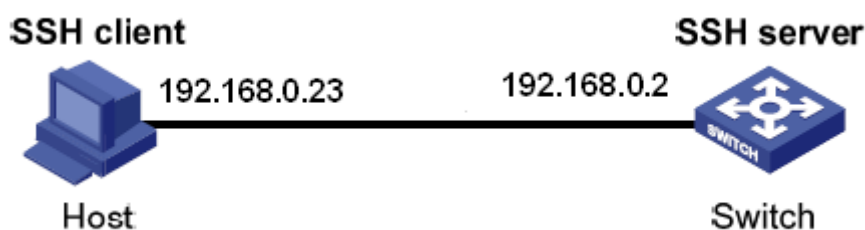


Figure 105: SSH configuration example

➤ SSH user chooses the authentication type of "Password":

1. Destroy the old key pair of the server, create a new key pair and start SSH server, see Figure 98, Figure 99, and Figure 100.
2. Set the SSH user name to ddd; choose the authentication type of "Password", set the password to 444, see Figure 103.
3. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 106; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).

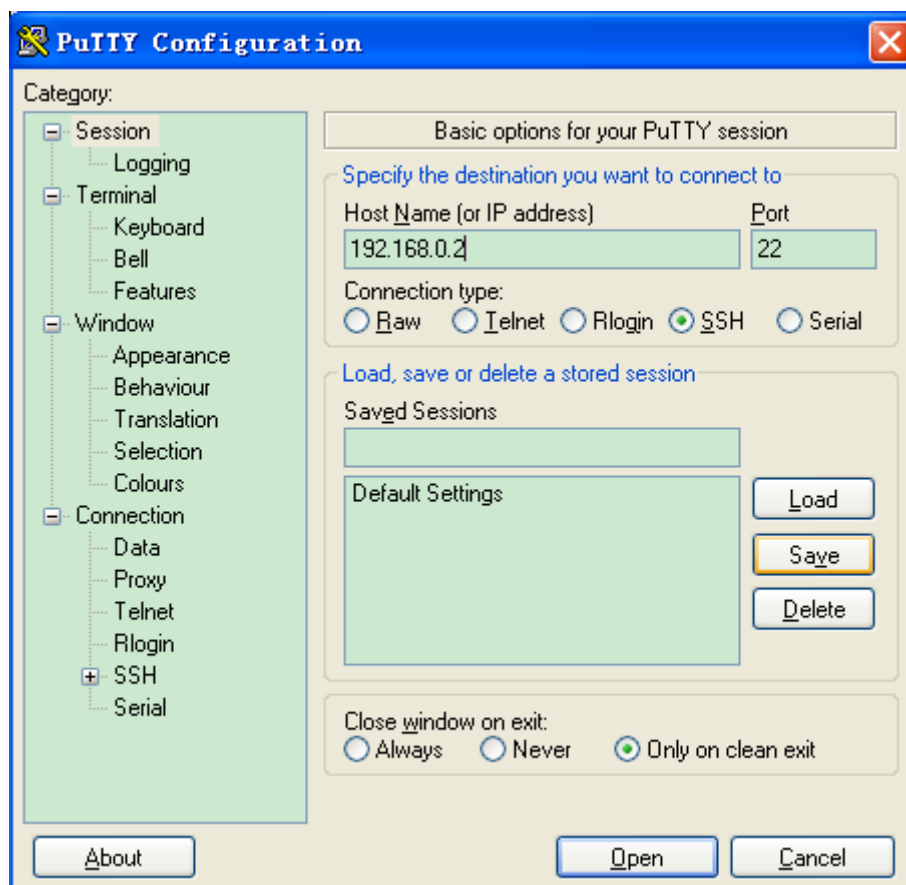


Figure 106: SSH client configuration

- Click <Open> button and the following warning message appears shown in Figure 107, click the <是(Y)> button.



Figure 107: Warning message

5. Input the user name "ddd" and the password "444" to enter the switch configuration interface, as shown in Figure 108.

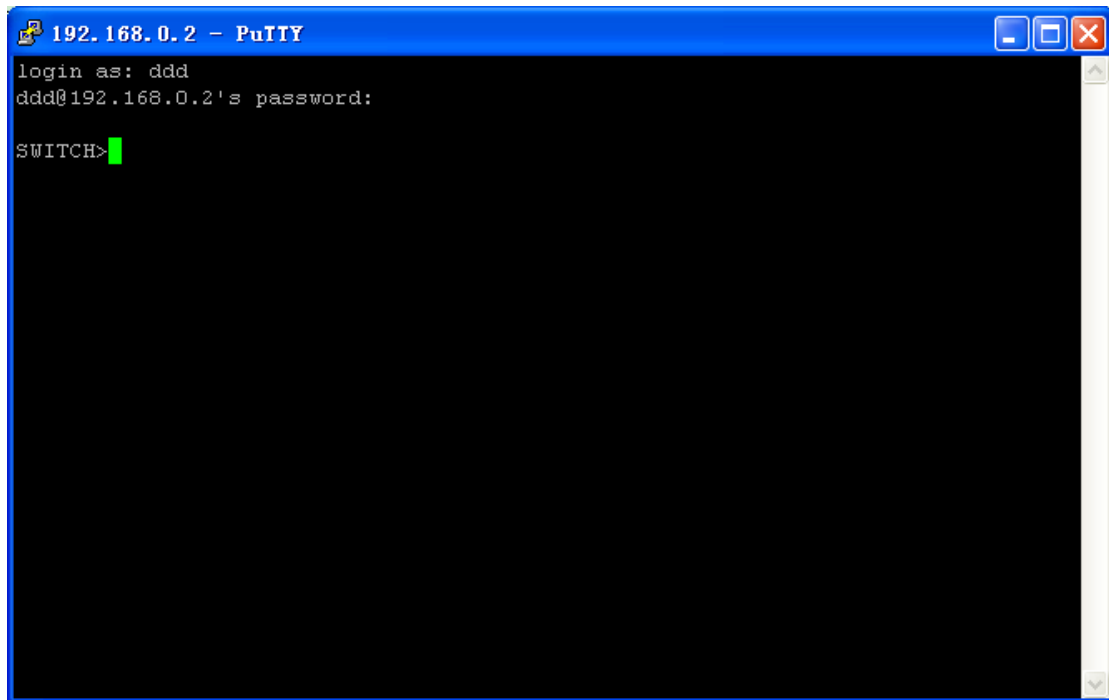


Figure 108: Login interface of the SSH password authentication

- SSH user chooses the authentication type of "Public Key":
 1. Destroy the old key pair of the server, create a new key pair and start the SSH server, see Figure 98, Figure 99 and Figure 100.
 2. Configure SSH client, see Figure 101; run PuTTYGen.exe in the client, click <Generate> button to generate the client key pair, as shown in Figure 109.

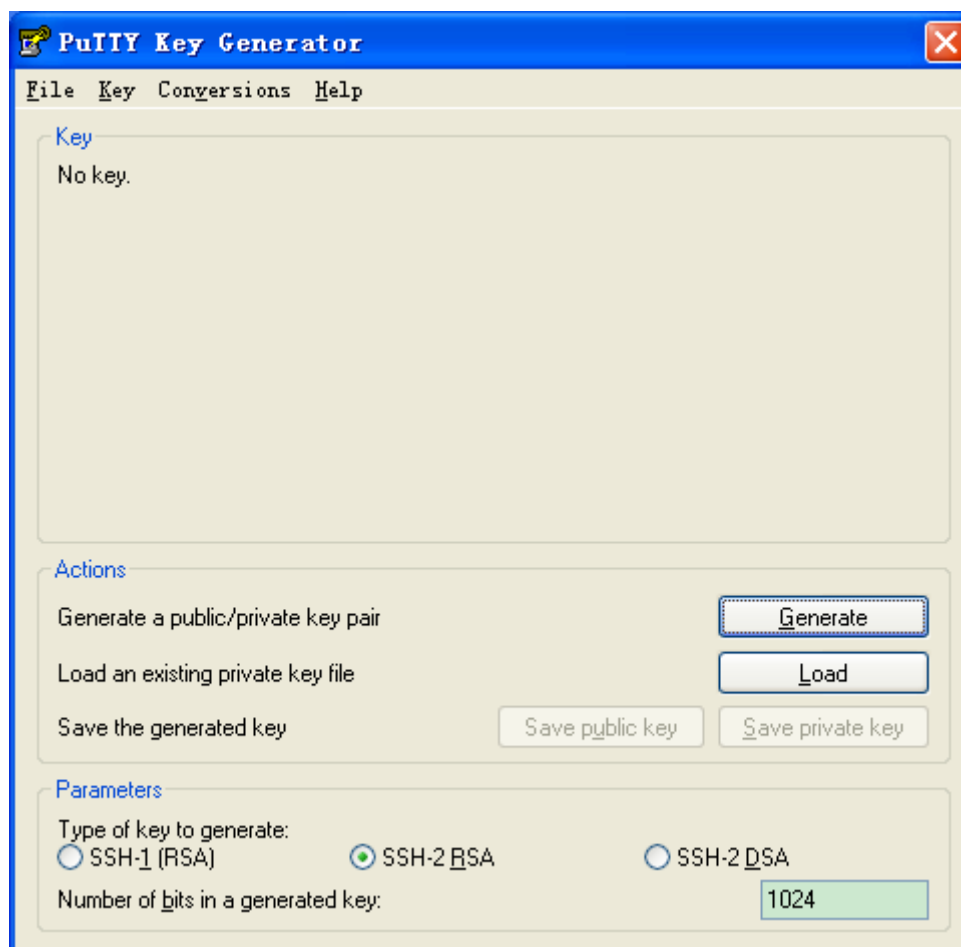


Figure 109: Generate the client key

3. In the generation process, please move the mouse in the screen, otherwise, the progress bar does not move forward and the generation stops, as shown in Figure 110.

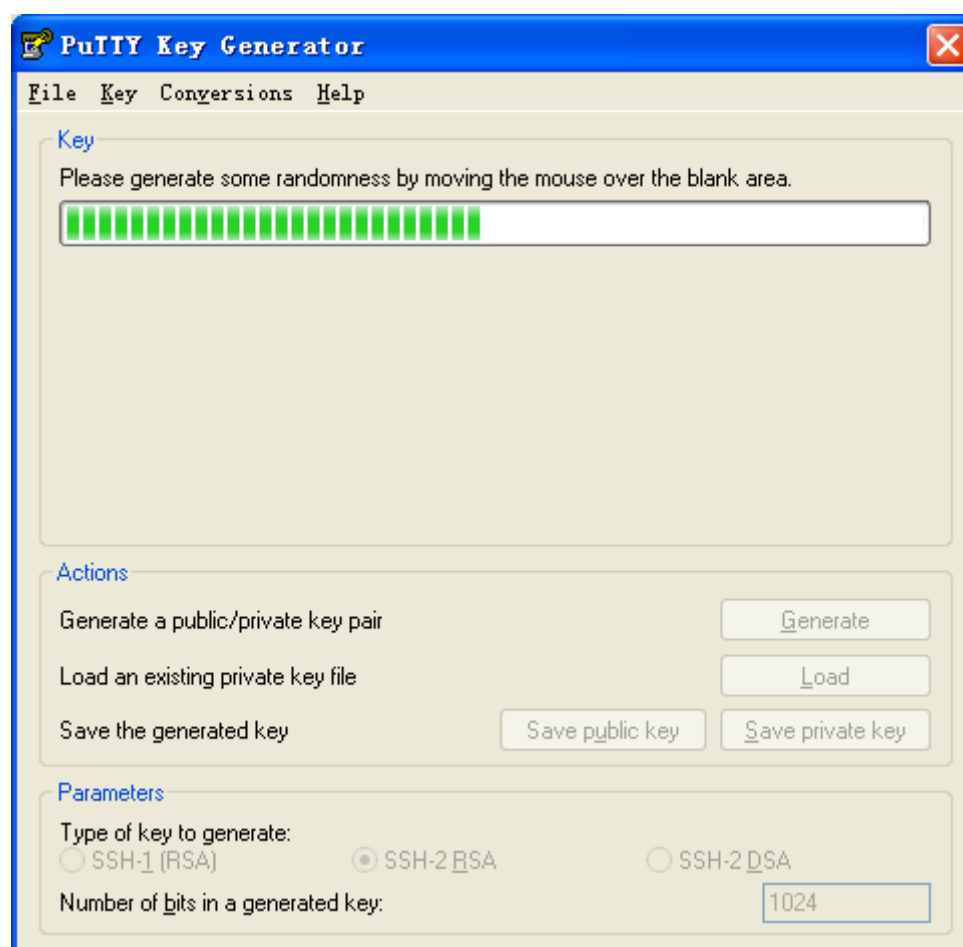


Figure 110: Key Generation

4. As Figure 111 shows, click <Save private key> to save the private key, and copy the public key to the space of Key Value in the SSH Key Configuration interface and input the key name, as shown in Figure 101.

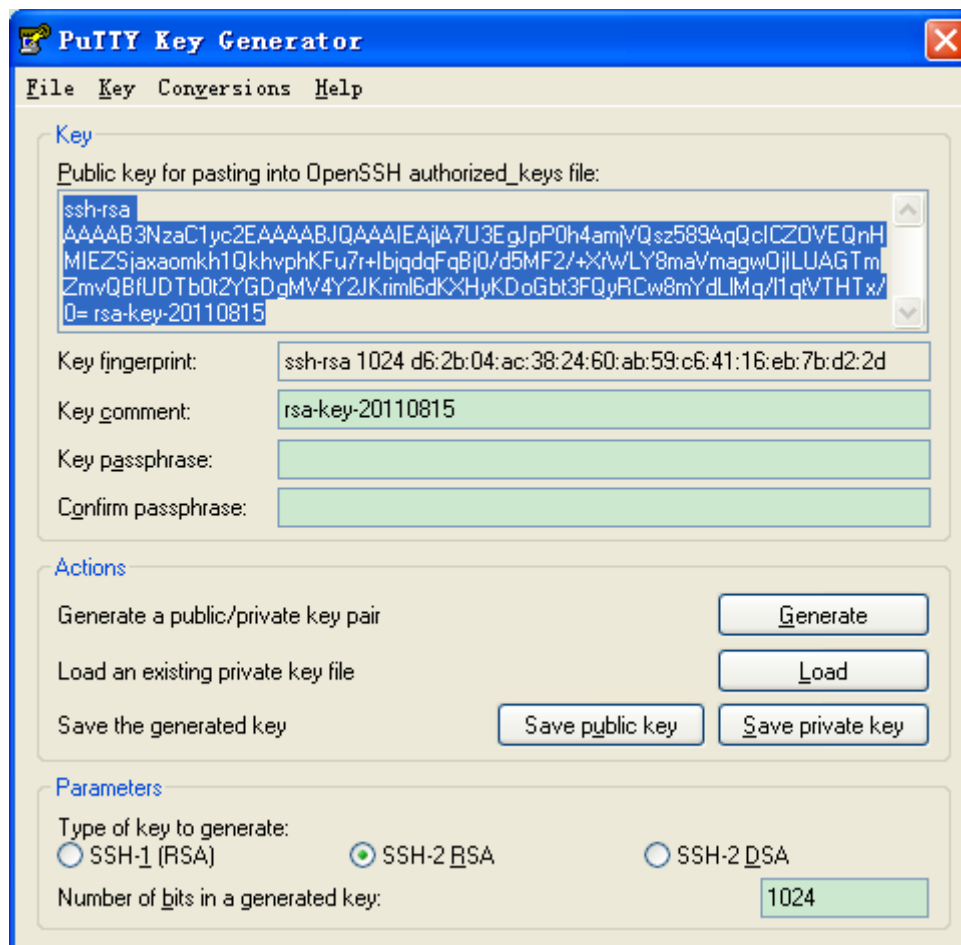


Figure 111: Generate the key value

5. Configure the SSH user name to ddd, and select the authentication type of "Public Key", choose the corresponding key name, as shown in Figure 103.
6. Establish a connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 112; input the IP address of the SSH server "192.168.0.2" in the space of Host Name (or IP address)

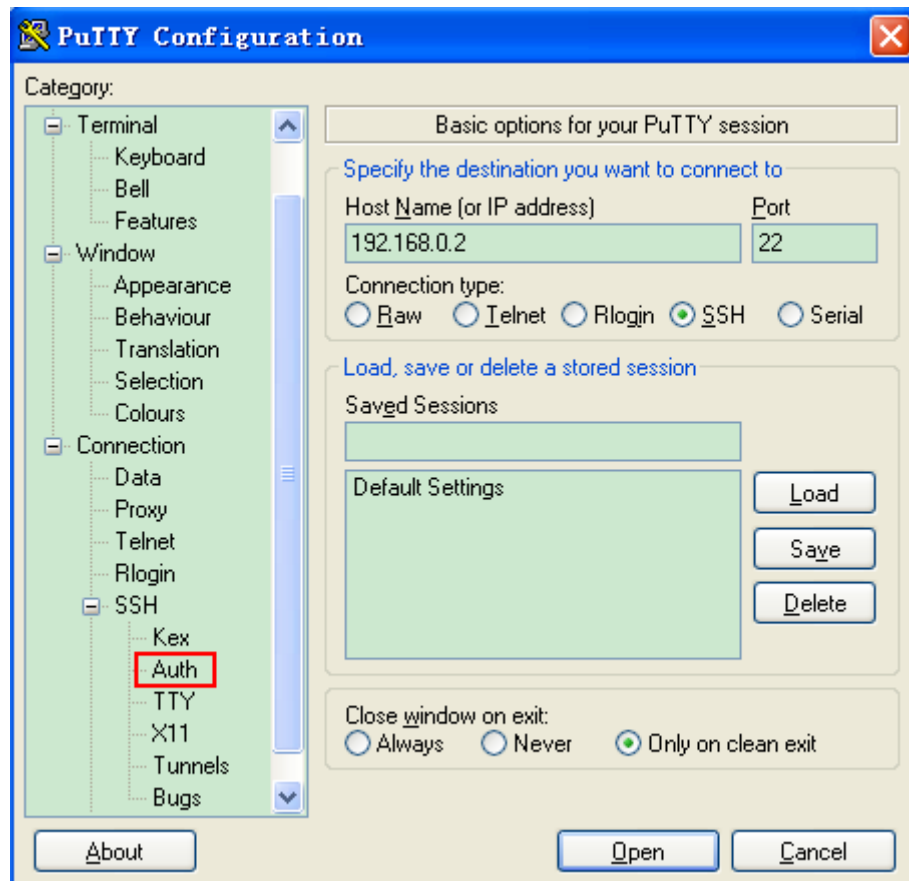


Figure 112: SSH client configuration of the "Public Key" authentication

7. Click [SSH]→[Auth] in the left side of the Figure 112, and the screen shown in Figure 113 appears, click <Browse> and choose the private file saved in the step 4.

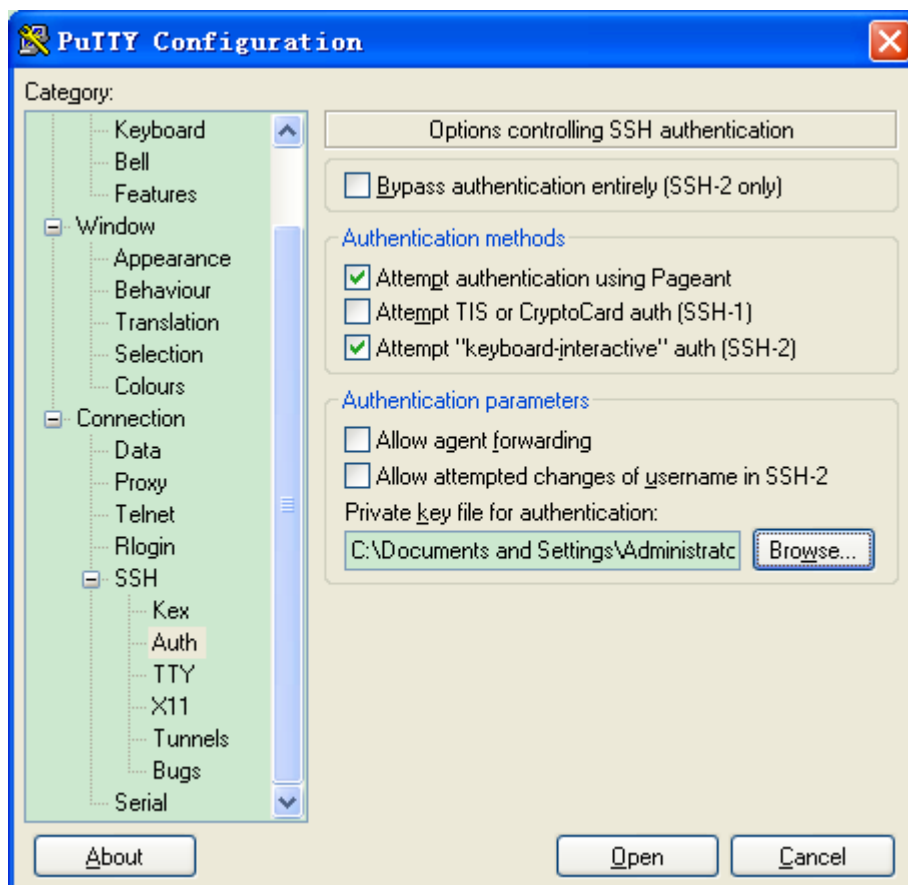


Figure 113: Choose the key file

8. Click <Open> button; input the user name to enter the switch configuration interface, as shown in Figure 114.

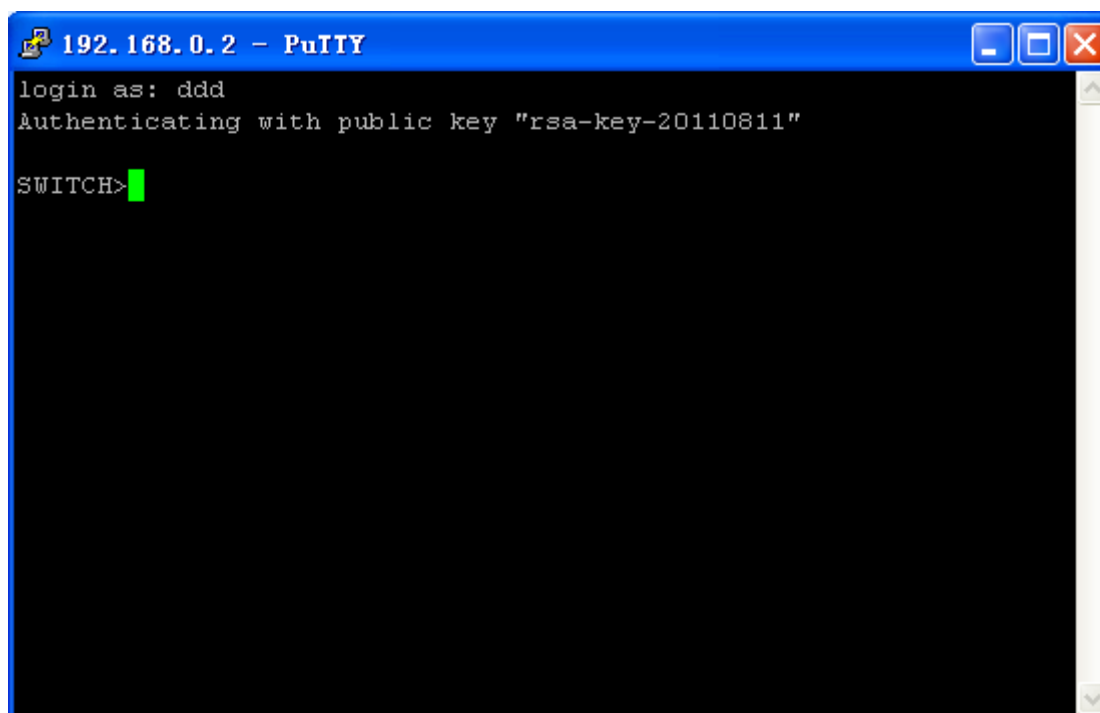


Figure 114: Login interface of the SSH public key authentication

16.2 Dot1x

16.2.1 Introduction

In order to solve the WLAN security problem, IEEE802LAN/WAN committee put forwarded the 802.1X protocol. IEEE802.1X protocol is used in Ethernet as a common access control mechanism, mainly solving authentication and security problems of Ethernet. 802.1X protocol is a kind of Port-Based Network Access Control protocol. Port-Based Network Access Control is to authenticate and control accessing devices on the port. The device connected to an 802.1X-enabled port can access the resources in LAN only after passing authentication. The 802.1X-enabled systems is a typical Client/Server structure. 802.1X application requires three elements:

Client: generally, it is a user terminal device. When users want to get online, they need to activate the Client program and input the username and password, and then the client program will send out the request for connection.

Authenticator: in Ethernet system, it means the authentication switch that is mainly in charge of the transmission of authentication information and authentication result, and it can enable or disable ports according to authentication results.

Authentication server: it is to provide authentication services. It verifies identifiers (Username and password) sent from the client to judge whether the user has right to use the network services, and it will send Enable/Disable Port command to the switch according to the authentication result.

16.2.2 Web Configuration

1. Enable global Dot1x function, as shown in Figure 115.

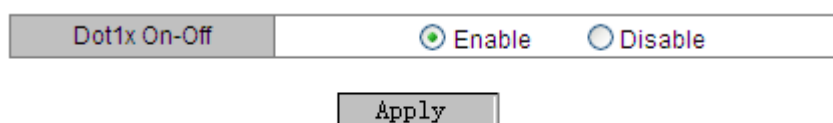


Figure 115: Enable global Dot1x

Dot1x On-Off

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable global Dot1x security function

2. Dot1x information configuration on port, as shown in Figure 116.

PortID	UserName	UserPassword
3	ccc	ccc

Figure 116: Dot1x information

Port ID

Configuration options: all switch ports

Function: choose the port to enable Dot1x function

User Name

Configuration range: 1-16 characters

Function: configure the user name bound to the port

User Password

Configuration range: 1-16 characters

Function: configure the user password bound to the port

3. Configure authentication method and authentication timeout, as shown in Figure 117.

Dot1x Method	<input checked="" type="radio"/> Local <input type="radio"/> Remote
Server Timeout	30 (1-30s)

Figure 117: Configure authentication method and timeout

Dot1x Method

Configuration options: Local/Remote

Default: Local

Function: choose the Dot1x authentication method

Explanation: If choose Local, user needs to manually add authentication username and

password on switch. If choose Remote, user needs to pass TACACS+ server authentication with the user name and password set on TACACS+ server.

Server Timeout

Configuration range: 1-30s

Default: 30s

Function: configure the authentication timeout. If user does not pass the authentication within this time, it is assumed that the authentication fails and user enters the quiet state.

4. Configure Dot1x-enabled ports, as shown in Figure 118.

PortID	Type	State	Mode	Reauthentication	Reauthentication Period	Quiet Period
1	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> ForceUnauthorized <input type="radio"/> Auto <input type="radio"/> ForceAuthorized	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	3600	60
2	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> ForceUnauthorized <input checked="" type="radio"/> Auto <input type="radio"/> ForceAuthorized	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	3600	60
3	FE	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> ForceUnauthorized <input type="radio"/> Auto <input checked="" type="radio"/> ForceAuthorized	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	3600	60
4	FE	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> ForceUnauthorized <input checked="" type="radio"/> Auto <input type="radio"/> ForceAuthorized	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	3600	60
5	FX	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> ForceUnauthorized <input checked="" type="radio"/> Auto <input type="radio"/> ForceAuthorized	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	3600	60
6	FX	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> ForceUnauthorized <input checked="" type="radio"/> Auto <input type="radio"/> ForceAuthorized	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	3600	60

Figure 118: The Dot1x-enabled port configuration

State

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable Dot1x protocol on port. When this function is enabled, user can log into switch from this port only after passing authentication.

Mode

Configuration options: ForceUnauthorized/Auto/ForceAuthorized

Default: Auto

Function: choose the authentication mode of the port

Explanation: ForceUnauthorized means that the port is always in an unauthorized state and does not allow user authentication and the authenticator does not offer the authentication service to clients that would like to access the network through this port; Auto means the initial state of the port is an unauthorized mode and the port does not allow users to access network resources, but if a user passes authentication, the port will be switched to the authorized state and allows user to access network resources. ForceAuthorized means that the port is always in an authorized state and allows user to access network resources

without passing authentication.

Reauthentication

Configuration: Enable/Disable

Default: Disable

Function: When the authentication is passed, the periodical reauthentication is required or not.

Reauthentication Period

Configuration range: 60~7200s

Default: 3600s

Function: When the authentication is passed, set the time interval of reauthentication.

Quiet Period

Configuration range: 10~120s

Default: 60s

Function: If authentication fails, the silent period(QuietPeriod) starts. During the silent period, the server does not respond to authentication requests from the client. After the silent period ends, the server starts to accept authentication requests again.

16.2.3 Typical Configuration Example

As Figure 119 shows, Dot1x client connects with switch port 3; enable Dot1x protocol in port 3 and choose Auto authentication mode; the local authentication username and password are both ccc and the remote authentication username and password are both ddd, other settings use the default values.

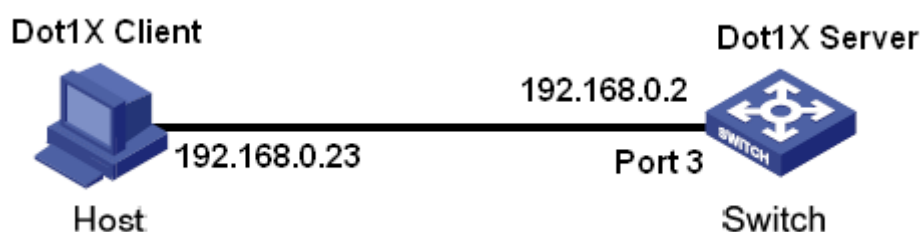


Figure 119: Dot1x configuration example

➤ Local authentication configuration

1. Enable global Dot1x protocol, as shown in Figure 115.

2. Configure the username and password of port 3 to ccc, as shown in Figure 116.
3. Choose the Dot1x method of Local, as shown in Figure 117.
4. Enable Dot1x protocol in port 3, and the authentication mode is set to Auto, as shown in Figure 118.
5. Install 802.1X authentication client software and run it, input username and password "ccc" to do authentication. User can access the switch after passing authentication.

➤ Remote authentication configuration

1. Enable global Dot1x protocol, as shown in Figure 115.
2. Choose the Dot1x method of Remote, as shown in Figure 117.
3. Enable Dot1x protocol in port 3, and the authentication mode is set to Auto, as shown in Figure 118.
4. Set the username and password to "ddd" on TACACS+ server.
5. Install 802.1X authentication client software and run it, input username and password "ddd" to do authentication. User can access the switch after passing authentication.

16.3 Port Security

16.3.1 Introduction

Port security is a MAC address-based security mechanism for network access control. This mechanism detects the source MAC addresses of the port-received frames to control the network access of unauthorized devices. The main function of port security is to let devices learn legal source MAC addresses by defining different types of port security modes.

16.3.2 Web Configuration

1. Select the port to enable Port Security function, as shown in Figure 120.

Port	Operation
FE-3 ▼	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 120: Enable Port Security

Port

Configuration options: all switch ports

Operation


Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable port security function

2. Port security address configuration, as shown in Figure 121.

The configuration

Port ID	MAC Address	VLAN ID (1~4093)
FE-3 	00-01-01-01-01-01	1

Apply
Add

Figure 121: Port security address configuration

Port ID

Configuration options: the ports that enable port security function

Function: select the port to bind to the security address

MAC Address

Function: set the MAC address that is bound to the port. Only the message whose source MAC address is this binding address can pass through this port, otherwise the message is dropped.

VLAN ID

Configuration range: all existing VLANs

Function: set the VLAN ID of the port



Caution:

Each port of the series switches can configure max 32 port security entries.

3. Show the port security list and delete the selected port security configuration, as shown in Figure 122.

The list of port safty

Number	Port ID	MAC Address	VLAN ID
<input type="radio"/>	3	00-01-01-01-01-01	1

Figure 122: Port security list

16.3.3 Typical Configuration Example

Bind the MAC address of 0x000101010000 to the port 1 in VLAN 2, then only the message with the source MAC address of 0x000101010000 can pass through the port 1 in VLAN 2.

Configuration steps:

1. Enable port security function in port 1, as shown in Figure 120.
2. Set the MAC address of port 1 to 0x000101010000, and the VLAN ID to 2, as shown in Figure 121.

16.4 AAA Configure

16.4.1 Introduction

AAA (Authentication, Authorization, Accounting) is a management mechanism for network security, providing authentication, authorization and accounting functions.

Authentication: confirm the identity of the remote accessing user and judge whether it is a legal user.

Authorization: grant different rights to different users and limit services that users can access to.

Accounting: record all operations performed by users when they use network services, including service type, start time, data flow. It is not only an accounting method, also the supervision of the network security.

16.4.2 Implementation

First, Authentication provides user authentication. It usually uses user name and password to verify user rights. The principle of authentication is that each user has a unique right to

obtain a standard, and AAA server checks the standard with user standards in the database one by one. If there is conformity, the user passes the authentication; if there is not, the server refuses the network connection request.

Next, user obtains rights to operate corresponding tasks by Authorization. For example, user is likely to execute some commands for operation after logging into system, so the Authorization process will detect whether the user has rights to execute these commands. Simply put, authorization process includes the activity type or quality confirmation, the resources or services allocated to users. Authorization happens in the process of authentication. Once a user passes the authentication, the corresponding rights will be authorized to the user.

Last is Accounting. It is to account the number of resources that are consumed in the user connection process. These resources contain the connecting time or the transmitted and received data flow in the user connection process, and so on.

The Accounting process can be executed according to statistics logs in the connection process and the user information, and the authorization control, bill and trend analysis, resource utilization, and capacity planning.

Currently, the network connection server interface coordinating with AAA server is TACACS+ protocol.

16.4.3 Web Configuration

1. Authentication method order configuration, as shown in Figure 123.

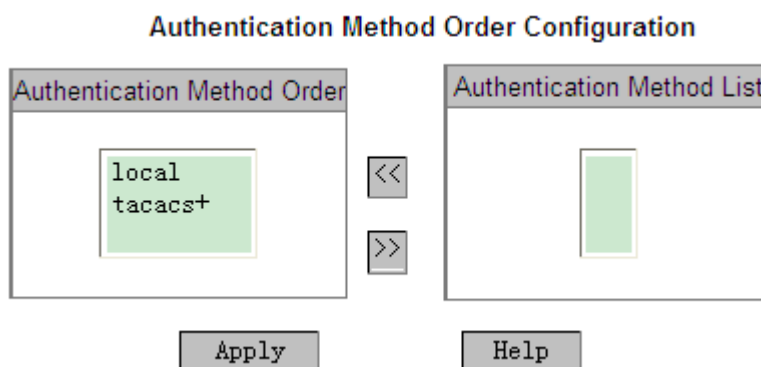


Figure 123: Configure authentication method

Authentication Method Order Configuration

Configuration options: local/tacacs+/local, tacacs+/tacacs+, local

Default: local

Function: choose the authentication order

Explanation: local: take the local authentication, which uses the user name and password created on device to login.

tacacs+: take the TACACS+ authentication, which uses the user name and password set on TACACS+ server

local, tacacs+: take the local authentication first, if cannot pass the authentication, then take TACACS+ authentication.

tacacs+, local: take the TACACS+ authentication first, if cannot pass the authentication, then take the local authentication.

2. TACACS+ authentication service configuration, as shown in Figure 124.

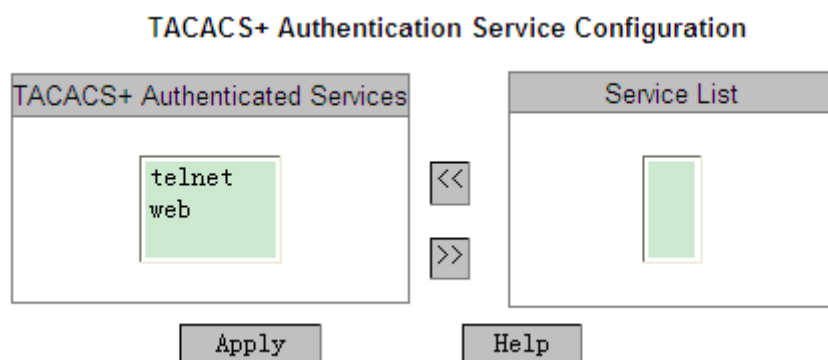


Figure 124: TACACS+ authentication service configuration

TACACS+ Authentication Service Configuration

Configuration options: telnet/web

Function: choose the login method of TACACS+ authentication

16.5 TACACS+ Configure

16.5.1 Introduction

TACACS+ (Terminal Access Controller Access Control System) is a kind of application based on TCP transmission protocol and uses client/server mode to achieve the communication between NAS (Network Access Server) and TACACS+ server. Clients run on

NAS and the server performs centralized management of user information. For users, NAS is a sever, but for TACACS+ server, NAS is a client. Figure 125 shows the structure.

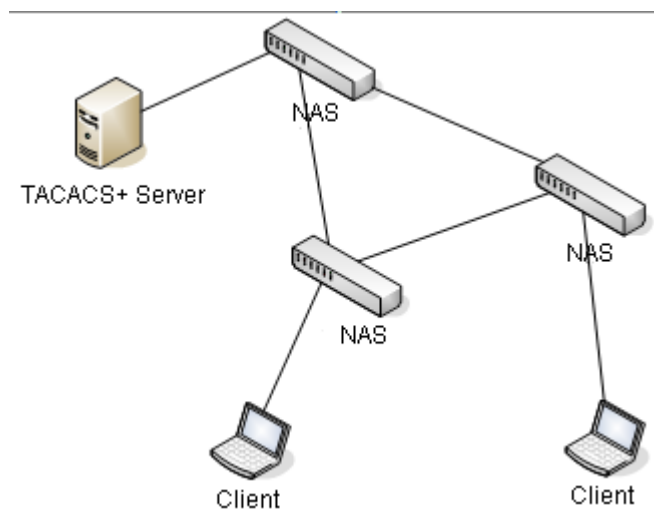


Figure 125: TACACS+ structure

This protocol is used to authenticate, authorize and charge the terminal user that would like to access the device to make operation. The device serves as a TACACS+ client, sending the username and password to the TACACS+ server for verification. The server establishes TCP connection with the client and responds to authentication requests, and verifies whether the user is a legal user. The user can log into the device to make operation only after it passed authentication and was authorized,

16.5.2 Web Configuration

1. Enable TACACS+ protocol, as shown in Figure 126.



Figure 126: Enable TACACS+ protocol

Protocol Status

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable TACACS+ protocol

2. TACACS+ server configuration, as shown in Figure 127.

Server Configuration

Server Attribute	<input checked="" type="radio"/> Primary <input type="radio"/> Secondary
Server Address	<input type="text" value="192.168.0.23"/>
TCP Port	<input type="text" value="45"/>
Encrypt	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Key Value	<input type="text" value="aaa"/>

Figure 127: TACACS+ server configuration

Server Attribute

Configuration options: Primary/Secondary

Default: Primary

Function: choose the server type

Server Address

Function: input the server IP address

TCP Port

Configuration range: 1~65535

Default: 49

Function: the number of the port that receives authentication requests from NAS

Encrypt

Configuration options: Enable/Disable

Default: Disable

Function: Encrypt messages or not. If it is enabled, it is required to input the key value.

Key Value

Configuration range: 1~32 characters

Function: configure key value

Explanation: set the key value to improve the communication security between client and TACACS+ server. Two parties share the key to verify the message legality. Only when the keys are same can both parties receive messages from each other and respond to messages, so please make sure the key set on the client is same as the key on TACACS+ server.

3. Show server list, as shown in Figure 128.

Server List

Index	Attribute	Server Address	TCP Port	Encrypt
<input type="checkbox"/> 1	Primary	192.168.0.23	49	Enable
<input type="checkbox"/> 2	Secondary	192.168.0.45	45	Disable

Figure 128: Server list

Show TACACS+ server list. The selected server configuration can be deleted or be modified.

16.5.3 Typical Configuration Example

As Figure 129 shows, the TACACS+ server can authenticate and authorize the user by using switch. The server IP address is 192.168.0.23, the shared key for the switch and server exchanging messages is aaa.

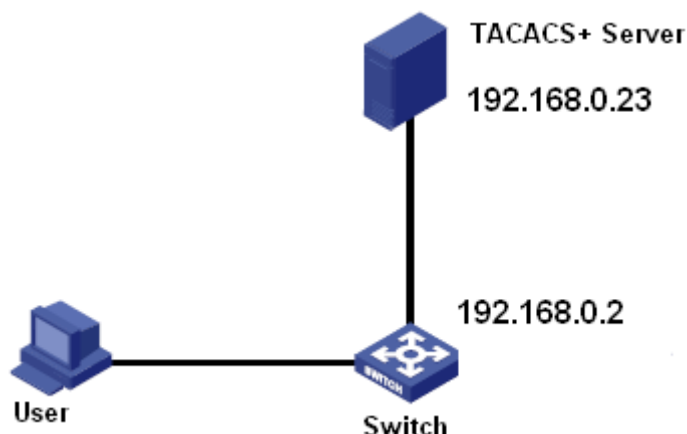


Figure 129: TACACS+ authentication example

1. Enable TACACS+ protocol, as shown in Figure 126.
2. Server configuration: IP address is 192.168.0.23, enable "Encrypt" and the Key Value is aaa, as shown in Figure 127. Web login uses Local authentication and Telnet login uses TACACS+ authentication, as shown in Figure 123 and Figure 124.
3. Configure the user name and password on TACACS+ server to bbb.
4. Input user name "admin" and password "123" and take local authentication to log into switch by Web.
5. Input user name and password "bbb" and take TACACS+ authentication to log into switch

by Telnet.

16.6 SSL Configure

16.6.1 Introduction

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.



Caution:

When using HTTPS protocol to access switch, please ensure SSL3.0 is used in the Internet options (open the browser, click [Tool]→[Internet Options]→[Advanced]→[Security], tick the "Use SSL3.0").

16.6.2 Web Configuration

1. Enable HTTPS protocol, as shown in Figure 130.



Figure 130: Enable HTTPS protocol

WEB Default Visit

Configuration options: HTTP/HTTPS

Default: HTTP

Function: choose the protocol to access Web browser.

Explanation: If choose HTTPS, use https://ip address to log into switch Web Interface.

2. Log into Web interface.

When a warning about authentication appears, please choose "Continue browsing the website", as shown in Figure 131.

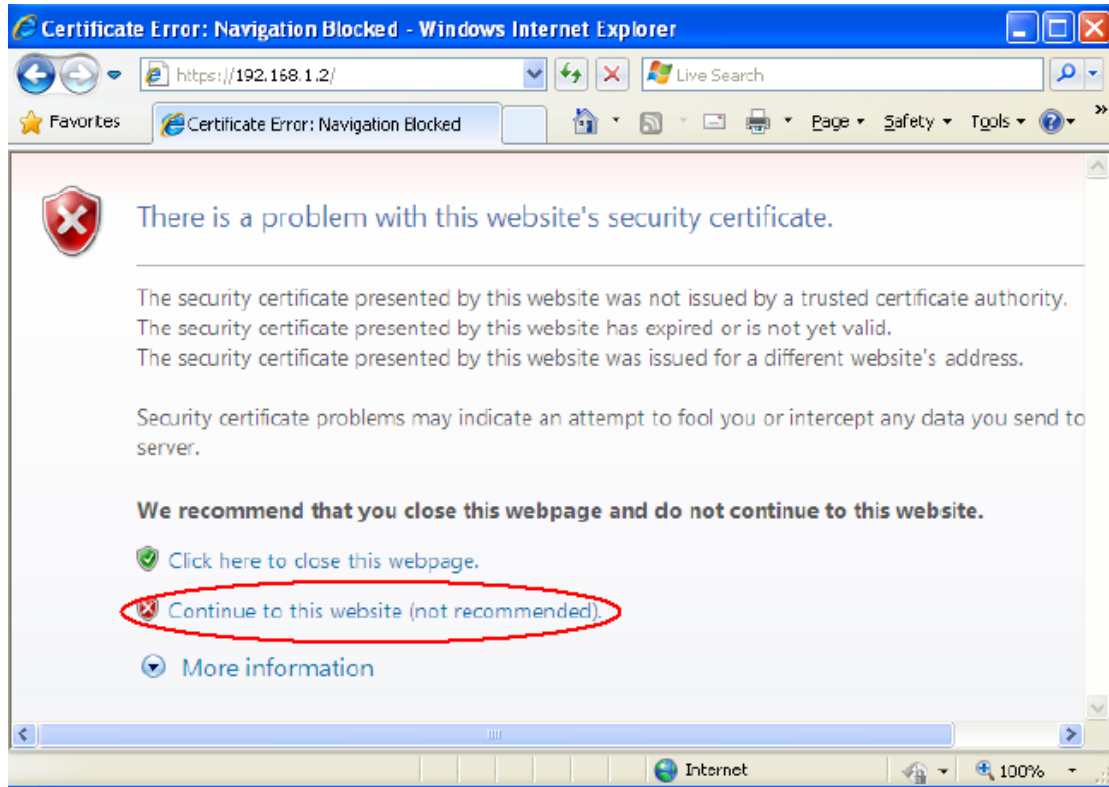


Figure 131: HTTPS logging interface

3. Input the username "admin" and password "123" to successfully log into switch through HTTPS.

17. VLAN

17.1 VLAN Configuration

17.1.1 Introduction

VLAN (Virtual Local Area Network) divides a LAN to multiple logic VLANs. The devices in a same VLAN can communicate to each other and the devices in different VLANs cannot conduct intercommunication, in this way, the broadcast messages are limited in a VLAN, highly improving LAN security.

VLAN partition is not restricted by the physical location. Each VLAN is regarded as a logical network. If a host in one VLAN would like to send data packets to a host in another VLAN, a router or a layer 3 device must be involved.

17.1.2 Principle

In order to let network devices distinguish different VLAN messages, it is needed to add a field into the message to identify VLAN. At present, the most common used protocol to identify VLAN is IEEE802.1Q protocol. The 802.1Q frame structure is shown in Table 7.

Table 7: 802.1Q Frame Structure

DA	SA	802.1Q Header				Length/Type	Data	FCS
		Type	PRI	CFI	VID			

A 4 bytes 802.1Q header is added into the traditional Ethernet data frame and it becomes the VLAN Tag.

Type: 16 bits, used to identify that the frame carries a VLAN Tag, and the value is 0x8100.

PRI: three bits, showing the 802.1p priority of the frame

CFI: one bit. 0 means Ethernet, 1 means token ring

VID: 12 bits, indicating VLAN ID and in the range of 1-4093. 0, 4094 and 4095 are reserved by protocol.

**Note:**

- VLAN 1 is the default VLAN and cannot be manually created and deleted by users.

-
- Reserved VLANs are reserved to realize specific functions by system and cannot be manually created and deleted by users.
-

The message containing 802.1Q header is a Tag message; if not, it is an Untag message. The messages in switch all carry an 802.1Q tag.

17.1.3 Port-based VLAN

VLAN partition consists of multiple types, such as port-based, MAC address-based. This series switches support the port-based VLAN partition. It defines VLAN members based on switch ports. It adds ports into the designated VLANs, and then the ports can forward the designated VLAN messages.

1. Port Type

According to the methods of port handling VLAN Tag during message forwarding, port can be divided to two types:

Untag port: the messages forwarded from this type of port do not have a Tag. Generally, this type of port is used to connect with the terminal equipment that does not support 802.1Q protocol. At default, all switch ports are Untag ports and belong to VLAN1.

Tag port: the messages forwarded from this type of port all carry a VLAN tag. This type of port is generally used to connect the network transmission devices.

2. PVID

Each port has a PVID attribute. When a port receives an Untag message, it will add a Tag into the message according to the PVID.

The port PVID is the VLAN ID of the Untag port. By default, all ports' PVID is VLAN 1.

After setting port type and PVID, there are several ways to process port-received and port-transmitted messages, as shown in Table 8.

Table 8: Different Processing Modes for Packets

Processing Received Packets		Processing Packets to Be Forwarded	
Untagged packets	Tagged packets	Port Type	Packet Processing
Add PVID tags to	➤ If the VLAN ID in a	Untag	Forward the packet after

untagged packets.	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.		removing the tag.
		Tag	➤ If the QoS priority of the ingress is set to port or 802.1p, keep the tag and forward the packet. ➤ If the QoS priority of the ingress is set to DSCP, replace the original tag with the combination of the queue mapped by the DSCP priority and the lowest bit of the ingress priority, and forward the packet with the new tag.

17.1.4 Web Configuration

1. Create a VLAN

Select ports to add into VLAN and make corresponding port configuration, as shown in Figure 132.

Add VLAN

VLAN Name:

VLAN ID:

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	<input checked="" type="checkbox"/>	<input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	FE	<input checked="" type="checkbox"/>	<input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	FE	<input type="checkbox"/>	<input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input type="radio"/> Disable
4	FE	<input type="checkbox"/>	<input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input type="radio"/> Disable
5	FX	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input checked="" type="radio"/> Enable <input checked="" type="radio"/> Disable
6	FX	<input type="checkbox"/>	<input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input type="radio"/> Disable
S-CH	S-CH	<input type="checkbox"/>	<input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input type="radio"/> Disable

Figure 132: VLAN Configuration

VLAN Name

Configuration range: 1~31 characters

Function: set VLAN name

VLAN ID

Configuration range: a number in the range of 2~4093

Function: Configure VLAN ID

Explanation: VLAN ID is used to distinguish different VLANs. This series switches support max 256 VLANs.

Tag

Configuration options: Tagged/Untagged

Function: select the port type in VLAN

Priority

Configuration range: 0~7

Default: 0

Function: set the port default priority. When adding an 802.1Q Tag into an untagged message, the PRI field is this priority value.

PVLAN

Configuration options: Enable/Disable

Default: Disable

Function: For Tag port, enable PVLAN or not. More information about PVLAN will be introduced in "17.2 PVLAN".



Caution:

- An Untag port can join only one VLAN and its VLAN ID is the port PVID. By default, it is VLAN 1, but a tag port can join multiple VLANs.
- When the Link Layer Discovery Protocol (LLDP) is enabled on both the serial port and the switch, the serial port sends VLAN information carried in an LLDP packet to the switch after the VLAN configuration succeeds. Upon receiving the LLDP packet, the switch automatically adds the S-CH port as a tagged port to this VLAN. The prerequisite of this operation is that

the VLAN on the switch is created and the S-CH port is not a member of this VLAN.

2. Show VLAN list, as shown in Figure 133.

PVLAN List	VLAN Group List
<input type="checkbox"/>	default---1
<input type="checkbox"/>	vlan---2

Apply
Help

Figure 133: Show VLAN List

PVLAN List

Function: If put a tick in the box, PVLAN function is enabled. More information will be introduced in "17.2 PVLAN".

3. Show the VLAN list of Untag ports and it is the port PVID, as shown in Figure 134.

Port Default VLAN ID

Port ID	VLAN ID
1	2
2	2
3	1
4	1
5	1
6	1
S-CH	1

Figure 134: Port PVID List



Caution:

If a port is added to all VLANs with Tag attribute, the PVID of the port is VLAN 1.

4. Modify/Delete VLAN

Click a VLAN in the Figure 133 to enter the corresponding screen in which the VLAN can be deleted or modified. Click <Delete> to delete the selected VLAN, as shown in Figure 135.

VLAN Name :

VLAN ID :

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	<input checked="" type="checkbox"/>	<input type="radio"/> tagged <input checked="" type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	FE	<input checked="" type="checkbox"/>	<input type="radio"/> tagged <input checked="" type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	FE	<input type="checkbox"/>	<input type="radio"/> tagged <input type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
4	FE	<input type="checkbox"/>	<input type="radio"/> tagged <input type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5	FX	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> tagged <input type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6	FX	<input type="checkbox"/>	<input type="radio"/> tagged <input type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
S-CH	S-CH	<input type="checkbox"/>	<input type="radio"/> tagged <input type="radio"/> Untagged	0 <input type="button" value="v"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure 135: Modify/Delete VLAN

17.1.5 Typical Configuration Example

As Figure 136 shows, the entire LAN is divided into 2 VLANs: VLAN2 and VLAN100. It is required that the devices in a same VLAN can communicate to each other, but different VLANs are isolated. The terminal PCs cannot distinguish Tag messages, so the ports on connecting Switch A and Switch B with PCs are set to Untag port. VLAN2 and VLAN100 messages need to be transmitted between Switch A and Switch B, so the ports connecting Switch A and Switch B should be set to Tag ports, permitting the messages of VLAN 2 and VLAN 100 to pass through. Table 9 shows specific configuration.

Table 9: VLAN Configuration

VLAN	Configuration
VLAN2	Set Switch A and B's port 1 and port 2 to Untag ports, port 5 to Tag port
VLAN100	Set Switch A and B's port 3 and port 4 to Untag ports, port 5 to Tag port

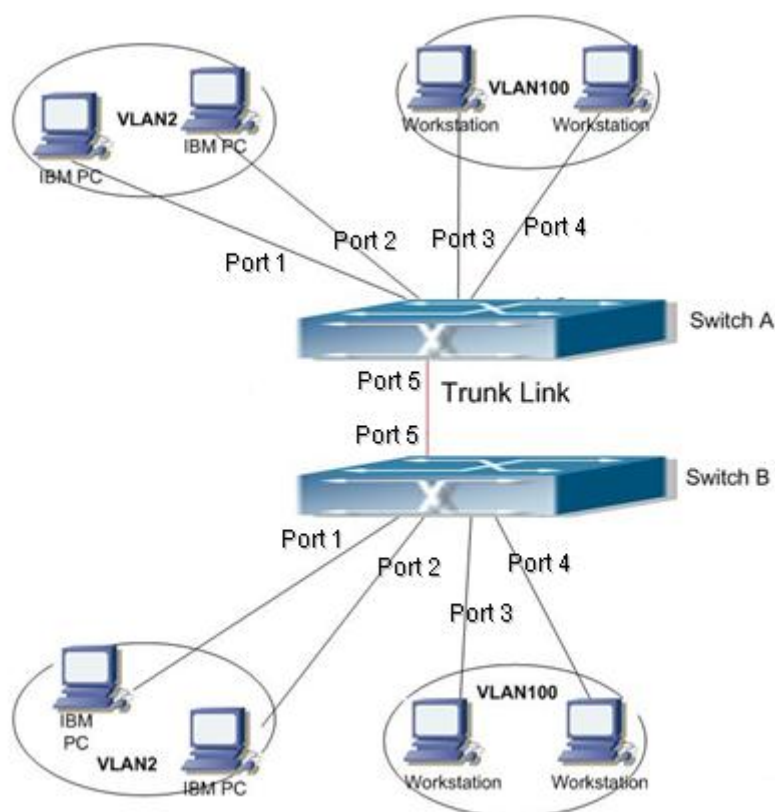


Figure 136: VLAN Application

Switch A and Switch B configuration are as follows:

1. Create VLAN 2, add port 1 and port 2 into VLAN 2 as Untag ports, and add port 5 into VLAN 2 as Tag port, as shown in Figure 132.
2. Create VLAN 100, add port 3 and port 4 into VLAN 100 as Untag ports, and add port 5 into VLAN 100 as Tag port, as shown in Figure 132.

17.2 PVLAN

17.2.1 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 the uplink port at the same time. Isolation domains cannot communicate to each other.

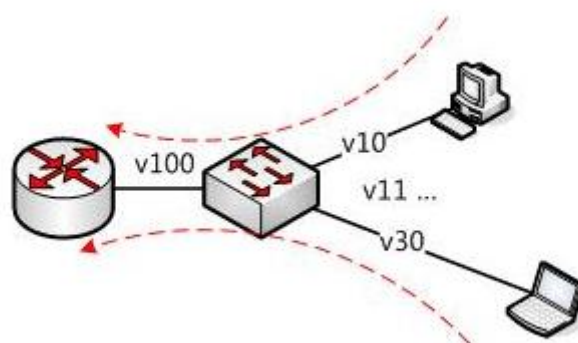


Figure 137: PVLAN Application

As Figure 137 shows, the shared domain is VLAN 100 and the isolation domains are VLAN 10 and VLAN 30; the devices in the isolation domains can communicate with the device in the shared domain, such as VLAN 10 can communicate with VLAN 100; VLAN 30 can also communicate with VLAN100, but the devices in different isolation domains cannot communicate to each other, such as VLAN 10 cannot communicate with VLAN 30.



Note:

When a PVLAN-enabled Tag port forwards a frame carrying a VLAN tag, the VLAN tag will be removed.

17.2.2 Web Configuration

1. Enable PVLAN function on port, as shown in Figure 138.

Add VLAN

VLAN Name:

VLAN ID:

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	<input checked="" type="checkbox"/>	<input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	FE	<input checked="" type="checkbox"/>	<input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	FE	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
4	FE	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
5	FX	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
6	FX	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
S-CH	S-CH	<input type="checkbox"/>	<input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="text" value="0"/> ▼	<input type="radio"/> Enable <input type="radio"/> Disable

Figure 138: Enable PVLAN function

In VLAN configuration interface, Tag ports can enable PVLAN function.

If the VLAN is a shared domain, the uplink port should be set to untagged, and the downlink port should be set to tagged.

If the VLAN is an isolation domain, the downlink port should be set to untagged, and the uplink port should be set to tagged.

2. Select VLAN members for PVLAN, as shown in Figure 139.

PVLAN List	VLAN Group List
<input type="checkbox"/>	default---1
<input checked="" type="checkbox"/>	vlan---100
<input checked="" type="checkbox"/>	vlan---200
<input checked="" type="checkbox"/>	vlan---300

Figure 139: PVLAN Member Configuration

PVLAN List

Configuration options: tick or not

Default: no tick

Function: Choose VLAN members for PVLAN

**Note:**

Both shared and isolation domains are member VLANs of PVLAN.

17.2.3 Typical Configuration Example

Figure 140 shows PVLAN application. VLAN300 is a shared domain and port 1 and port 2 are uplink ports; VLAN100 and VLAN200 are isolation domains and port 3, 4, 5 and 6 are downlink ports.

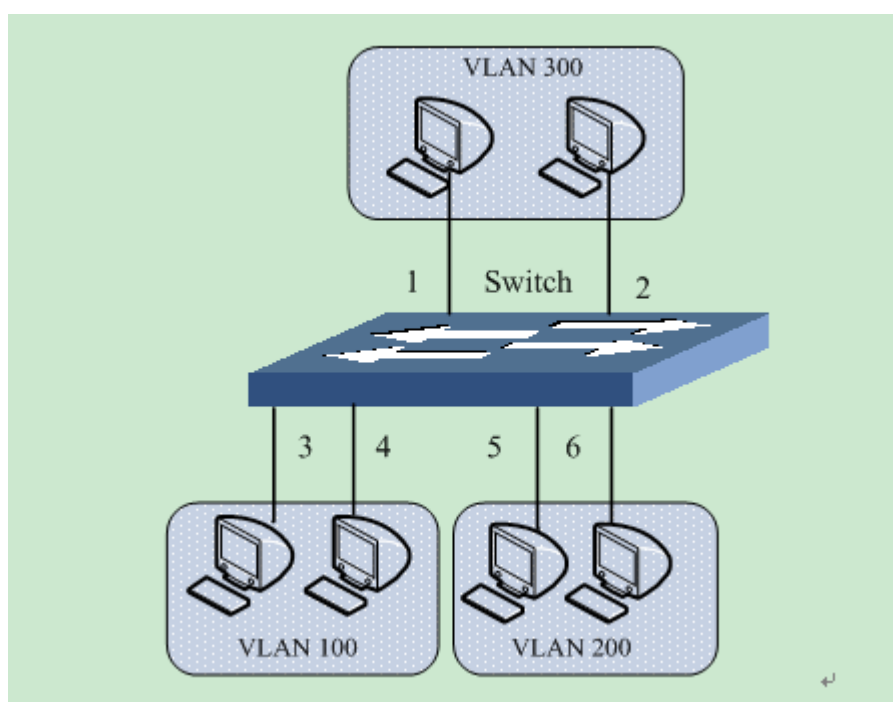


Figure 140: PVLAN Configuration Example

Switch Configuration:

1. Configure the shared domain of VLAN 300, as shown in Figure 138.

Port 1 and port 2 are set to Untagged and are assigned to the shared domain of VLAN 300;

Port 3 and port 4 are set to Tagged and are assigned to the shared domain of VLAN 300, and enable PVLAN;

Port 5 and port 6 are set to Tagged and are assigned to the shared domain of VLAN 300, and enable PVLAN;

2. Configure the isolation domain of VLAN 100, as shown in Figure 138.

Port 1 and port 2 are set to Tagged and are assigned to the isolation domain of VLAN 100,

and enable PVLAN;

Port 3 and port 4 are set to Untag ports and are assigned to the isolation domain of VLAN 100.

3. Configure the isolation domain of VLAN 200, as shown in Figure 138.

Port 1 and port 2 are set to Tagged and are assigned to the isolation domain of VLAN 200, and enable PVLAN;

Port 5 and port 6 are set to Untagged and are assigned to the isolation domain of VLAN 200.

4. Set VLAN300, VLAN100 and VLAN200 to PVLAN members, as shown in Figure 139.

17.3 GVRP

17.3.1 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.

17.3.2 Port Mode

There are three types of GVRP registration mode on a port: Normal, Fixed and Disable.

Normal: allow the port to dynamically register or deregister VLAN attribute, and propagate dynamic and static VLAN information.

Fixed: forbid the port dynamically registering or deregistering VLAN attribute, but allow the port to statically register or deregister VLAN information.

Disable: forbid the port dynamically or statically registering or deregistering VLAN attribute

and the port cannot propagate any VLAN information.



Caution:

GVRP port and Port Trunk are mutually exclusive. The GVRP-enabled port cannot join a Trunk group, while the port joining a Trunk group cannot enable GVRP.

17.3.3 Web Configuration

1. Enable GVRP protocol and set the corresponding timers, as shown in Figure 141.

Protocol Configuration

GVRP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LeaveAll Timer	<input type="text" value="10000"/> ms
Hold Timer	<input type="text" value="100"/> ms
Join Timer	<input type="text" value="500"/> ms
Leave Timer	<input type="text" value="3000"/> ms

Figure 141: GVRP Protocol Configuration

GVRP Status

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable GVRP protocol

LeaveAll Timer

Configuration range: 100ms~327600ms

Default: 10000ms

Function: set the time interval of sending leave all message. It 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.

Hold Timer

Configuration range: 100ms~327600ms

Default: 100ms

Explanation: This value must be a multiple of 100. It is better to set a same value of Hold timers on all GVRP-enabled ports

Join Timer

Configuration range: 100ms~327600ms

Default: 500ms

Description: This value must be a multiple of 100. It is better to set a same value of Join timers on all GVRP-enabled ports

Leave Timer

Configuration range: 100ms~327600ms

Default: 3000ms

Description: This value must be a multiple of 100. It is better to set a same value of Leave timers on all GVRP-enabled ports

2. Port configuration, as shown in Figure 142.

Port Setting

Port	Type	GVRP Mode		
1	FE	<input type="radio"/> Disable	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed
2	FE	<input type="radio"/> Disable	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed
3	FE	<input checked="" type="radio"/> Disable	<input type="radio"/> Normal	<input type="radio"/> Fixed
4	FE	<input checked="" type="radio"/> Disable	<input type="radio"/> Normal	<input type="radio"/> Fixed
5	FX	<input checked="" type="radio"/> Disable	<input type="radio"/> Normal	<input type="radio"/> Fixed
6	FX	<input checked="" type="radio"/> Disable	<input type="radio"/> Normal	<input type="radio"/> Fixed

Figure 142: GVRP Port Setting

GVRP Mode

Configuration options: Disable/Normal/Fixed

Default: Disable

Function: Set GVRP mode on port;



Caution:

- The port in Normal mode can only exist in the default VLAN (VLAN 1).
- Cannot carry on any VLAN operation on the port in Normal mode.

3. Show statically configured and dynamically registered VLAN information, as shown in Figure 143.

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag Port	GVRP Aware Port
1	1	default	1,2,3,4,5,6, S-CH		
2	2	vlan			3

Figure 143: VLAN Information

17.3.4 Typical Configuration Example

As Figure 144 shows, switch A and Switch B are connected by port 2. Port 1 of Switch A is set to Fixed mode to statically register VLAN information; port 2 is set to Normal mode and propagates the VLAN information of port 1. Port 2 of Switch B is set to Normal mode and registers the VLAN information of Switch A. In this way, port 2 of Switch B can register the same VLAN information as that in port 1 of Switch A.

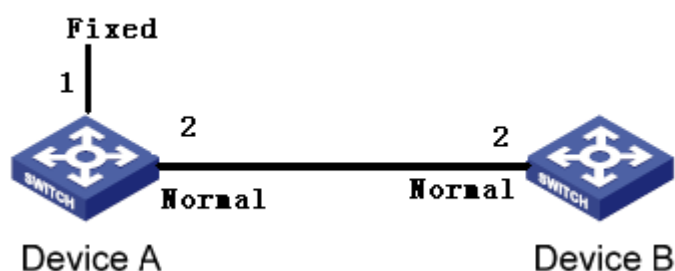


Figure 144: GVRP Configuration Example

Switch configuration are as follows:

1. Enable GVRP protocol on Switch A and Switch B, as shown in Figure 141.
2. Set the port 1 of Switch A to Fixed mode, and port 2 to Normal mode; set the port 2 of Switch B to Normal mode, as shown in Figure 142.
3. Port 2 of Switch B can register the same VLAN information as that of port 1 of Switch A.

18. RMON

18.1 Introduction

RMON (Remote Network Monitoring) is based on SNMP architecture and let network management devices more actively monitor and manage the managed devices. RMON includes NMS (Network Management Station) and Agent. NMS manages Agent and Agent can perform statistics of all kinds of traffic information on port.

RMON mainly realize statistics and alarm functions. Statistics function is that agent can periodically perform statistics of all kinds of traffic information on port, such as the amount of messages received in a certain network segment during a certain period. Alarm function is that agent can monitor the values of specified MIB variables. When a value reaches the alarm threshold (such as the amount of messages is up to the specified value), agent can automatically record alarm events in RMON log, or send a Trap message to the management device.

18.2 RMON Group

RMON (RFC2819) defines multiple RMON groups. This series devices support statistics group, history group, event group and alarm group of public MIB. Each group supports max 32 entries.

➤ Statistics Group

It is that the system can conduct statistics of all kinds of traffic information on port. The statistics information contains the number of network collisions, CRC error messages, undersized or oversized data messages, broadcast and multicast messages, received bytes, received messages, and so on. After successfully creating a statistics entry on a specified interface, the statistics group counts the number of messages on the current interface and the statistics result is a continuous accumulated value.

➤ History Group

History group stipulates that the system periodically take sampling of all kinds of traffic

information on port and saves the sampling values in the history record table, so as that the management device can view them at any time. The history group counts statistics values of all kinds of data in the sampling interval.

the port-received messages in each cycle and the cycle can be configured.

➤ 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. Event is triggered when the monitored device meets the alarm condition. There are several ways to handle events:

Log: logging the event and related information in the RMON log table

Trap: sending Trap to NMS and inform the happening of event

Log-Trap: logging and sending Trap

None: No action

➤ Alarm Group

RMON alarm management can monitor the specified alarm variables. After users define alarm entries, the system will gain the values of monitored alarm variables in a defined period. When the value of the alarm variable is bigger than or equal to the upper threshold, an upper alarm event is triggered. When the value of the alarm variable is lower than or equal to the lower threshold, a lower alarm event is triggered. Alarms will be handled according to the event definition.

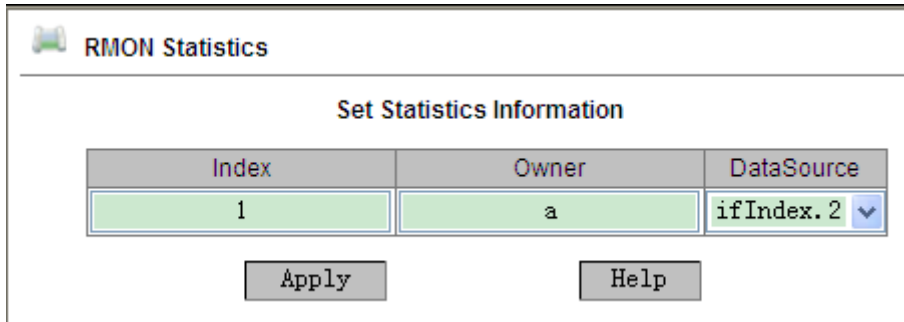


Caution:

If a sampled value of alarm variable exceeds the threshold multiple times in a same direction, only the first time can trigger alarm event. That means the rising alarm and falling alarm is alternate.

18.3 Web Configuration

1. Set statistics information, as shown in Figure 145.



The screenshot shows the 'RMON Statistics' window with a title bar. Below the title bar is a section titled 'Set Statistics Information'. It contains a table with three columns: 'Index', 'Owner', and 'DataSource'. The 'Index' column has a text input field with the value '1'. The 'Owner' column has a text input field with the value 'a'. The 'DataSource' column has a dropdown menu with 'ifIndex.2' selected. Below the table are two buttons: 'Apply' and 'Help'.

Index	Owner	DataSource
1	a	ifIndex.2

Apply Help

Figure 145: RMON Statistics Configuration

Index

Configuration range: 1~65535

Function: set a index of a statistics information entry

Owner

Configuration range: 1~32 characters

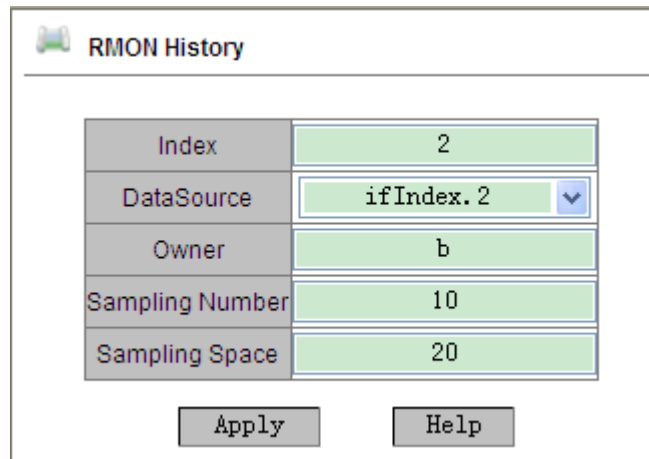
Function: set the name of a statistics information entry

Data Source

Configuration options: ifIndex.portid

Function: select the port to conduct statistics

2. History table configuration, as shown in Figure 146.



The screenshot shows the 'RMON History' window with a title bar. Below the title bar is a table with five rows: 'Index', 'DataSource', 'Owner', 'Sampling Number', and 'Sampling Space'. Each row has a corresponding text input field. The 'Index' field contains '2', the 'DataSource' field contains 'ifIndex.2' with a dropdown arrow, the 'Owner' field contains 'b', the 'Sampling Number' field contains '10', and the 'Sampling Space' field contains '20'. Below the table are two buttons: 'Apply' and 'Help'.

Index	2
DataSource	ifIndex.2
Owner	b
Sampling Number	10
Sampling Space	20

Apply Help

Figure 146: RMON History Configuration

Index

Configuration range: 1~65535

Function: set the index of history control entry

Data Source

Configuration options: ifIndex.portid

Function: select the port to take sampling

Owner

Configuration range: 1~32 characters

Function: set the name of a history control entry

Sampling Number

Configuration range: 1~65535

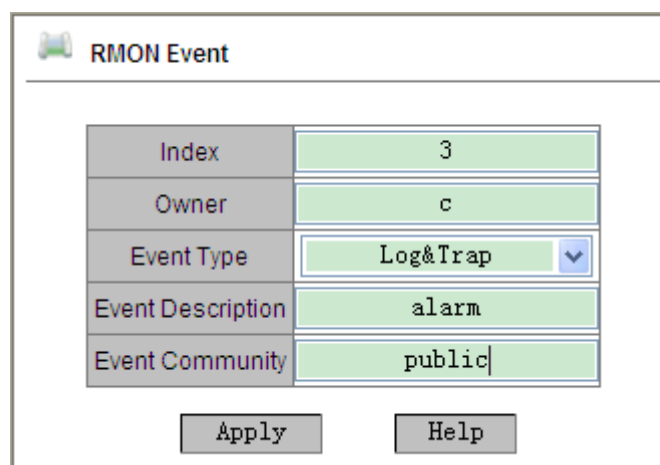
Function: set the times to take sampling

Sampling Space

Configuration range: 1~3600s

Function: set the interval to take sampling

3. Event control configuration, as shown in Figure 147.



The image shows a dialog box titled "RMON Event" with a small icon of a computer monitor. Inside the dialog, there is a table with five rows, each representing a configuration field. The fields are: Index (value 3), Owner (value c), Event Type (value Log&Trap with a dropdown arrow), Event Description (value alarm), and Event Community (value public). Below the table, there are two buttons: "Apply" and "Help".

Index	3
Owner	c
Event Type	Log&Trap ▼
Event Description	alarm
Event Community	public

Apply Help

Figure 147: RMON Event Control Configuration

Index

Configuration range: 1~65535

Function: set the index of a event control entry

Owner

Configuration range: 1~32 characters

Function: set the name of a event control entry

Event Type

Configuration options: NONE/LOG/Snmp-trap/log&Trap

Default: NONE

Function: set the event type when alarm happens. It is the alarm handling method.

Event Description

Configuration range: 1~127 characters

Function: set the event description

Event Community

Configuration range: 1~127 characters

Function: set the name of community sending trap events, which should be consistent with the community name of SNMP

4. Alarm control configuration, as shown in Figure 148.

MIB	(1213) IfInUcastPkts
Index	4
OID	1.3.6.1.2.1.2.2.1.11
Owner	
DataSource	ifIndex.2
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Apply
Help

Figure 148: RMON alarm control configuration

MIB

Function: choose the MIB information to do statistics, such as the number of unicast message in the ingress port

Index

Configuration range: 1~65535

Function: set the index of a alarm control entry

OID

Function: set the OID number of the current MIB node

Owner

Configuration range: 1~32 characters

Function: set the name of a alarm control entry

Data Source

Configuration options: ifIndex.portid

Function: choose the port to monitor

Sampling Type

Configuration options: Absolute/Delta

Default: Absolute

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

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.

Alarm Type

Configuration options: RisingAlarm/FallingAlarm/RisOrFallAlarm

Default: RisingAlarm

Function: choose the alarm type

Sampling Space

Configuration range: 1~65535

Function: set the sampling period which is better to be same as the sampling space in History configuration

Rising Threshold

Configuration range: 1~65535

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.

Falling Threshold

Configuration range: 1~65535

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.

Rising Event Index

Configuration range: 0~65535

Explanation: set the index of a rising event. It is the handling method of a rising alarm

Falling Event Index

Configuration range: 0~65535

Explanation: set the index of a falling event. It is the handling method of a falling alarm

19. Unicast Configuration

19.1 Introduction

When a switch forwards a message, it searches in the MAC address table to confirm the destination port number corresponding to the destination MAC address of the message.

MAC address is divided into static MAC address and dynamic MAC address.

Static MAC address is configured by users and has the highest priority (cannot be covered by dynamic MAC address) and is permanently valid.

Dynamic MAC address is learned by switch in the process of forwarding data frames, and is valid in a limited time, and is renewed periodically. When a switch receives data frames that need to be forwarded, first, it learns the source MAC addresses of data frames, and establishes mapping relationships with sending ports, and then searches in the MAC address table according to their destination MAC addresses. If there are matched entries, the switch will forward data frames from the corresponding ports. Otherwise, the switch will broadcast data frames in its broadcast domain.

This series switches support max 256 static unicast entries.

19.2 Web Configuration

1. Add static MAC address entry, as shown in Figure 149.

Set FDB Unicast

MAC	VLAN ID (1~4093)	Member Port
ec-de-12-34-56-78	2	2 ▼

Apply
Help

Figure 149: Add static unicast FDB entry

MAC

Configuration format: HH-HH-HH-HH-HH-HH (H means a hexadecimal number)

Function: configure unicast MAC address and the lowest bit in the highest byte is 0

VLAN ID

Function: set the VLAN ID of port

Member Port

Configuration options: all switch ports

Function: select a port to forward the message with this destination MAC address and the selects port must be in the above specified VLAN

2. Show static unicast MAC address list, as shown in Figure 150.

FDB Unicast Mac List			
Index	MAC	VLAN ID	Member Port
<input type="radio"/>	00-00-01-01-01-01	1	1
<input type="radio"/>	ec-de-12-34-56-78	1	2

Figure 150: Show Static FDB Table

Select an entry to delete or modify this entry.

3. Show dynamic unicast MAC address list, as shown in Figure 151.

Dynamic Unicast Mac List			
Index	MAC	VLAN ID	Member Port
1	00-14-78-2e-e5-61	1	3
2	00-19-e0-1b-69-59	1	3
3	00-19-e0-1b-f1-40	1	3
4	00-1d-7d-cf-77-6a	1	3
5	00-24-8c-73-3f-73	1	3
6	00-24-8c-7e-92-98	1	3
7	00-24-8c-9e-56-26	1	3
8	00-25-11-25-a7-96	1	3
9	00-25-11-4d-a3-0e	1	3
10	00-26-18-0b-39-ee	1	3
11	00-40-05-12-9d-a1	1	3

Figure 151: Dynamic unicast FDB table

20. Alarm and Syslog

20.1 Alarm

20.1.1 Introduction

This series switches support three types of alarms. When an alarm is triggered, the Alarm LED in the front panel goes ON.

Power alarm: if it is enabled, the alarm will be triggered for single power input

Port alarm: if it is enabled, the alarm will be triggered for Link Down of port.

Ring alarm: if it is enabled, the alarm will be triggered for an open ring.



Caution:

Only the master station of a DT ring supports the ring alarm function.

20.1.2 Web Configuration

1. Alarm setting, as shown in Figure 152.

Power Alarm

Alarm Name	Enable Alarm
Power Alarm	<input checked="" type="checkbox"/>

Port Alarm

Port	1	2	3	4	5	6
Type	FE	FE	FE	FE	FX	FX
Enable Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DT-RING Alarm

DT-RING ID	Enable Alarm
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

Apply
Help

Figure 152: Alarm setting

Power Alarm

Options: Enable/Disable

Default: Disable

Function: Enable/disable power alarm

Port Alarm

Options: Enable/Disable

Default: Disable

Function: Enable/disable port alarm.

DT-RING Alarm

Options: Enable/Disable

Default: Disable

Function: Enable or disable the DT-Ring function.

2. Show alarm status after alarm functions are enabled, as shown in Figure 153.

Power Alarm

Alarm Name	Alarm Status
power1	NONE
power2	WARN

Port Alarm

Port	1	2	3	4	5	6
Type	FE	FE	FE	FE	FX	FX
AlarmStatus	Link Up	Link Down	Link Down	-	-	-

DT-RING Alarm

DT-RING ID	Alarm Status
2	Ring Open
1	Ring Close

Figure 153: Show alarm status

Power Alarm Status

Options: NONE/WARN

Explanation: after the power alarm function is enabled, NONE is displayed for the power in power-on state, while WARN is displayed for the power in power-off state.

Port Alarm Status

Options: Link Up/Link Down

Explanation: after the port alarm function is enabled, Link Up is displayed for normal port connection, while Link Down displayed for port disconnection or abnormal connection.

DT-RING Alarm

Options: Ring Open/Ring Close

Explanation: after the port alarm function is enabled, Ring Open is displayed for an open ring, while Ring Close is displayed for a closed ring.

20.2 Syslog

20.2.1 Introduction

Logging function mainly records the switch system information and operation information for convenient fault location. It contains System log and Running log.

System log contains:

- Task suspension log
- Reboot caused by task suspension
- Reboot caused by pressing <Reset> button on switch front panel
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface
- System reboot

Running log contains:

- Port state change
- Power state change
- Ring state change
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface

Max 1024 logs are supported. When the number exceeds 1024, the new log will cover the old log.

20.2.2 Web Configuration

1. Logging function configuration, as shown in Figure 154.

Protocol Settings

Syslog	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RunLog	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Save in Flash	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Send to Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Remote-server IP	192.168.0.23

Figure 154: Log state configuration

Syslog

Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable syslog. Once it is enabled, syslog can be recorded.

RunLog

Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable RunLog. Once it is enabled, running log can be recorded.

Save in Flash

Configuration options: Enable/Disable

Default: Disable

Function: Save logs in Flash or not. Once it is enabled, the logs can be viewed on switch.

Send to Server

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable Send to Server

Explanation: Once it is enabled, switch logs can be uploaded to server by Syslog Server in real time.

Remote-server Ip

Configure the IP address of server to upload logs

Through Syslog Server (for example, Tftpd32), users can view logs in a timely manner, as shown in Figure 155.

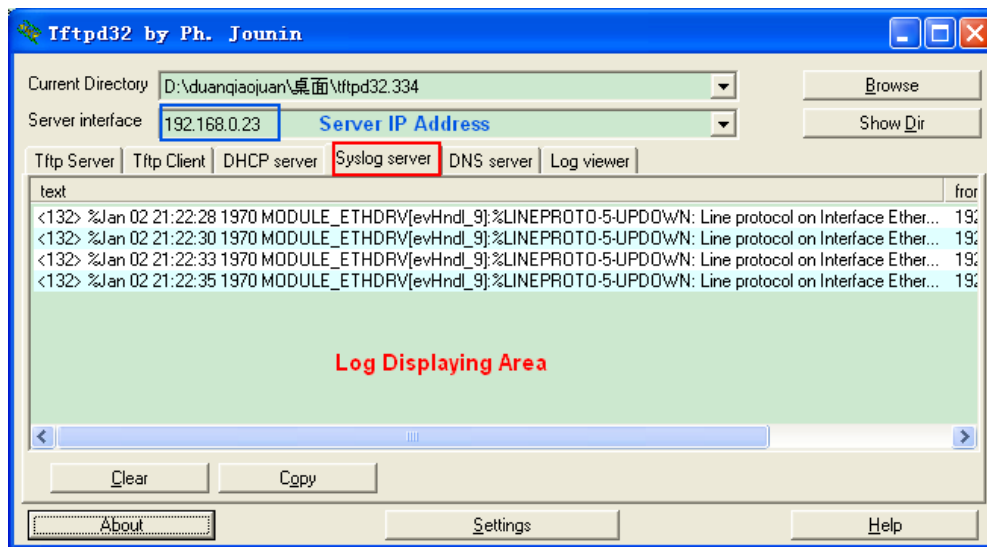


Figure 155: Send logs to server

2. Log uploading, as shown in Figure 156 and Figure 157.

Log Transmittal

Transfer Mode	<input checked="" type="radio"/> Ftp Mode <input type="radio"/> Tftp Mode
Server IP Address	192.168.0.23
File Name	log.txt
User Name	admin
Password	...

Figure 156: Upload logs by FTP mode

Log Transmittal

Transfer Mode	<input type="radio"/> Ftp Mode <input checked="" type="radio"/> Tftp Mode
Server IP Address	192.168.0.23
File Name	log.txt
User Name	
Password	

Figure 157: Upload logs by TFTP mode

Transfer Mode

Configuration options: Ftp Mode/Tftp Mode

Default: Ftp Mode

Function: Choose the mode to upload logs to server

Server IP Address

Configuration format: A.B.C.D

Function: Set the IP address of FTP/TFTP server

File Name

Configuration range: 1~32 characters

Function: set the file name saved in server

User Name

Configuration range: 1~32 characters

Function: Input FTP user name. There is no need to input user name when the file is uploaded by TFTP mode

Password

Configuration range: 1~32 characters

Function: Input FTP user password. There is no need to input password when the file is uploaded by TFTP mode

3. Show log, as shown in Figure 158.

Runlog

SEQ ID	EVENT TYPE	TIME	CONTENT
15	port link alarm	THU AUG 25 10:54:07 2011	Port alarm: entity id:3 state:Link down
14	software reboot	THU AUG 25 10:46:37 2011	software system reboot.
13	port link alarm	THU AUG 25 10:43:04 2011	Port alarm: entity id:3 state:Link up
12	port link alarm	THU AUG 25 10:42:37 2011	Port alarm: entity id:3 state:Link down
11	software reboot	THU JAN 01 21:38:15 1970	software system reboot.
10	power alarm	THU JAN 01 20:41:13 1970	Power alarm: entity id:2 state:Power down
9	port link alarm	THU JAN 01 16:25:42 1970	Port alarm: entity id:5 state:Link up
8	port link alarm	THU JAN 01 16:25:38 1970	Port alarm: entity id:5 state:Link down
7	port link alarm	THU JAN 01 16:23:01 1970	Port alarm: entity id:5 state:Link up
6	port link alarm	THU JAN 01 16:22:57 1970	Port alarm: entity id:5 state:Link down
5	port link alarm	THU JAN 01 00:00:13 1970	Port alarm: entity id:5 state:Link up
4	port link alarm	THU JAN 01 00:00:10 1970	Port alarm: entity id:2 state:Link up
3	port link alarm	THU JAN 01 00:00:06 1970	Port alarm: entity id:1 state:Link up
2	software reboot	THU JAN 01 07:37:14 1970	software system reboot.
1	port link alarm	THU JAN 01 07:37:05 1970	Port alarm: entity id:8 state:Link up
0	port link alarm	THU JAN 01 07:37:01 1970	Port alarm: entity id:8 state:Link down

Clear

Figure 158: Show Log

Log

Displaying portfolio: {SEQ ID, EVENT TYPE, TIME, CONTENT}

Function: show log records

Click <Clear> button to clear log informations.

**Caution:**

FTP/TFTP server must remain in online state when logs are uploading.

21. SNMP

21.1 SNMPv2

21.1.1 Introduction

SNMP (Simple Network Management Protocol) is a frame of using TCP/IP protocol suite to manage devices in a network. Network administrator can check device information, modify device parameters, monitor device status and locate network faults by SNMP function.

21.1.2 Implementation

SNMP protocol adopts manager/agent mode, so SNMP network contains NMS and Agent. NMS (Network Management Station) is a workstation running the SNMP-supported client network management software, playing a core role in SNMP network management.

Agent is a program in the managed device. It is responsible for receiving, processing requests from NMS. When an alarm happens, Agent will automatically inform the NMS.

NMS manages SNMP network, while Agent is managed by SNMP network. The management information exchange between NMS and Agent is through SNMP protocol.

SNMP provides 5 basic operations:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS sends query and configuration requests to Agent by Get-Request, Get-Next-Request and Set-Request messages. When Agent receives requests, it will send out Get-Response message as respond. When an alarm happens, Agent will automatically send Trap message to NMS to inform the occurrence of abnormal events.

21.1.3 Explanation

SNMP Agent of this series device supports SNMP v2 and SNMP v3 versions. SNMPv2 is compatible with SNMP v1.

SNMP v1 adopts Community Name Authentication. The community name works as a password and is used to restrict SNMP NMS accessing SNMP Agent. If the community name of the SNMP message cannot pass device authentication, this message will be dropped.

SNMP v2 also adopts community name authentication. It not only is compatible with SNMP v1, but also expands the functions of SNMP v1.

The precondition of mutual visiting of NMS and Agent is the matched SNMP version. Agent can be configured with multiple versions at the same time, and use different version to communicate with different NMS.

21.1.4 MIB Introduction

Any managed resource can be viewed as an object and it is called a managed object.

MIB (Management Information Base) is a collection of all managed objects. It defines the hierarchical relationships between managed objects and defines a series of attributes of objects, such as object name, access rights, data types, and so on. Each Agent has its own MIB. NMS can read or write objects in the MIB according to its rights. The relationship of NMS, Agent and MIB is shown in Figure 159.



Figure 159: NMS, Agent and MIB relationship

MIB defines a tree structure and each tree node is a managed object. Each tree node contains an OID (Object Identifier) that can indicate the node position in the MIB tree structure. As Figure 160 shows, the OID of the managed object A is 1.2.1.1.

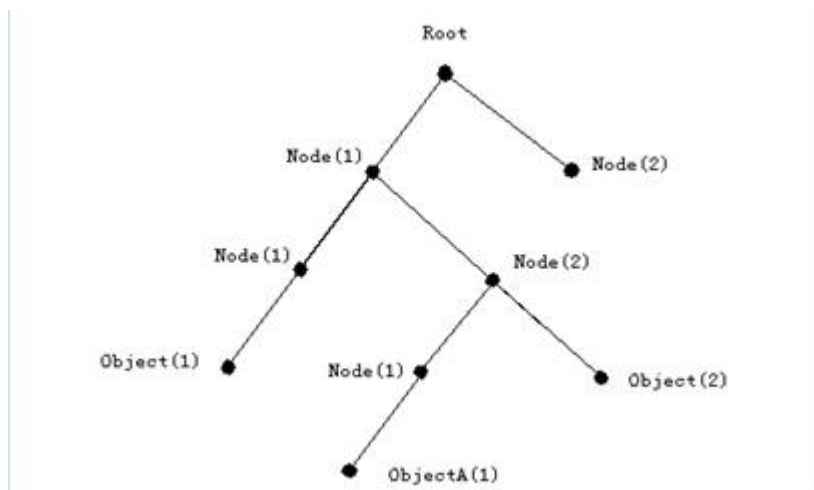


Figure 160: MIB tree structure

21.1.5 Web Configuration

1. Enable SNMP Protocol, as shown in Figure 161.

SNMP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
V2 Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 161: Enable SNMP and choose SNMP version

SNMP Status

Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable SNMP protocol

V2 Status

Configuration options: Enable/Disable

Default: Enable

Function: Enable SNMPv2 version that is compatible with SNMPv1

2. Configure access rights, as shown in Figure 162.

Read-Only Community	public (3-16)
Read-Write Community	private (3-16)
Request Port	161 (1-65535)

Figure 162: Access rights configuration

Read-Only Community

Configuration range: 3~16 characters

Default: public

Function: set the read-only community name.

Explanation: Only when the community name carried by the SNMP message sent from NMS is same as the community name set here can the NMS read MIB information.

Read-Write Community

Configuration range: 3~16 characters

Default: private

Function: set the read-write community name.

Description: Only when the community name carried by the SNMP message sent from NMS is same as the community name set here can the NMS read and write MIB information.

Request Port

Configuration range: 1~65535

Default: 161

Function: set the port to receive SNMP requests

3. Trap configuration, as shown in Figure 163.

Configure Trap

Trap on-off	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Trap Port ID	<input type="text" value="162"/> (1-65535)
Server IP Address1	<input type="text" value="192.168.0.23"/> (IP Addr)
Server IP Address2	<input type="text"/> (IP Addr)
Server IP Address3	<input type="text"/> (IP Addr)
Server IP Address4	<input type="text"/> (IP Addr)
Server IP Address5	<input type="text"/> (IP Addr)

Figure 163: Trap Configuration

Trap on-off

Configuration options: Enable/Disable

Default: Enable

Function: Enable/Disable the function of switch sending Trap messages

Trap Port ID

Configuration options: 1~65535

Default: 162

Function: Set the port ID of sending Trap messages

Server IP Address

Configuration format: A.B.C.D

Function: configure the server IP address of receiving Trap messages. Max 5 server IP addresses are supported.

4. Show management server IP address, as shown in Figure 164.

Management Station		
Server IP Address1	192.168.0.23	(IP Addr)
Server IP Address2		(IP Addr)
Server IP Address3		(IP Addr)

Figure 164: Management server IP address

There is no need to manually set the server IP addresses. They will be automatically displayed as long as run the network management software on server and read & write device MIB node information.

21.1.6 Typical Configuration Example

SNMP NMS connects with the switch through Ethernet. The IP address of NMS is 192.168.0.23 and the switch IP address is 192.168.0.2. NMS monitors and manages Agent by using SNMPv2 and it can read and write MIB information of Agent, and the Agent will automatically send Trap messages to NMS when failover occurs in Agent, as shown in Figure 165.

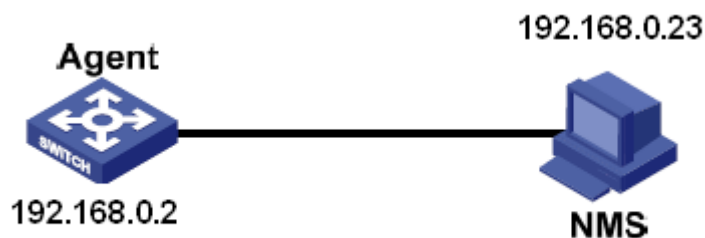


Figure 165: SNMPv2 Configuration Example

Agent configuration:

1. Enable SNMP protocol and v2 version, see Figure 161.
2. Configure access rights with the Read-Only community name "public" and Read-Write community name "private", and the request port is 161, as shown in Figure 162.
3. Enable Trap, the Trap port ID is set to 162 and the server IP address is 192.168.0.23, as shown in Figure 163.

If users would like to monitor and manage Agent, it is needed to run the corresponding management software, for example, Kyvision, in NMS.

Please refer to "Kyvision Management Software Operation Manual" to learn the specific operation of Kyvision software in NMS.

21.2 SNMPv3

21.2.1 Introduction

SNMPv3 provides a USM (User-Based Security Model) authentication mechanism. User can configure authentication and encryption functions. Authentication is used to verify the legality of the message sender to avoid the access from illegal users. Encryption is to encrypt the transmitted messages between NMS and Agent to avoid being eavesdropped. The combination of authentication and encryption improves the communication security between SNMP NMS and SNMP Agent.

21.2.2 Implementation

SNMPv3 has 4 configuration tables each of which can configure 16 entries. These tables codetermine whether the specified users based on context group can access MIB

information.

User table is used to create users. Each user can use different security policies to realize user authentication, encryption and other security functions.

Access table can access MIB node information by matching group name, context name, and by setting security model, security level

Group table is a collection of multiple users. Access rights are subject to a user group, the access rights of a group are applicable for all users in the group.

Context table are readable character strings to identify users. It has nothing to do with the specific security model.

21.2.3 Web Configuration

1. User table configuration, as shown in Figure 166.

Number	State	User Name	Authentication protocol	Authentication password
1	active	1111	<input type="radio"/> NONE <input checked="" type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	●●●●
2	active	3333	<input type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input checked="" type="radio"/> HMAC-SHA	●●●●
3	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
4	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
5	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
6	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
7	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
8	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
9	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
10	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
11	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	
12	----		<input checked="" type="radio"/> NONE <input type="radio"/> HMAC-MD5 <input type="radio"/> HMAC-SHA	

Figure 166: SNMPv3 user table configuration

User Name

Configuration range: 4~16 characters

Function: create user name

Authentication Protocol

Configuration options: NONE/HMAC-MD5/HMAC-SHA

Default: NONE

Function: choose a kind of authentication encryption algorithm

Authentication Password

Configuration range: 4~16 characters

Function: set a user password

2. Access table configuration, as shown in Figure 167.

Number	GroupName	ContextName	SecurityModel	SecurityLevel
1	1111	2222	<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input checked="" type="radio"/> AuthNoPriv
2	3333	4444	<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input checked="" type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
3			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
4			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
5			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
6			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
7			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
8			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
9			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
10			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
11			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
12			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
13			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
14			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
15			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv
16			<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2	<input type="radio"/> NoAuthNoPriv <input type="radio"/> AuthNoPriv

Figure 167: SNMPv3 access table configuration

Group Name

Configuration range: 4~16 characters

Function: set the name of group table. For this series switches, each group is only for a single user, so the group name must be the same as the user name set in the user table.

Context Name

Configuration range: 4~16 characters

Function: configure the context name

Security Model

Configuration range: SNMPv3/ SNMPv2

Explanation: SNMPv3 means using USM technology. SNMPv3 is selected forcibly.

Security Level

Configuration range: NoAuthNoPriv/AuthNoPriv

Default: NoAuthNoPriv

Function: authentication and encryption are needed or not when accessing MIB information.

Explanation: NoAuthNoPriv: needs neither authentication nor encryption; AuthNoPriv: need authentication, do not need encryption.

3. Context table configuration, as shown in Figure 168.

Number	ContextName
1	2222
2	4444
3	
4	
5	
6	
7	
8	
9	

Figure 168: SNMPv3 context table configuration

Context Name

Configuration range: 4~16 characters

Function: define a series of managed objects that can be accessed by SNMP. This name must be the same as the context name set in access table.

4. Group table configuration, as shown in Figure 169.

Number	SecurityName	SecurityModel
1	1111	<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
2	3333	<input checked="" type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
3		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
4		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
5		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
6		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
7		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
8		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c
9		<input type="radio"/> SNMP V3 <input type="radio"/> SNMP V2c

Figure 169: SNMPv3 group table

Security Name

Configuration range: 4~16 characters

Function: set the name of group table. For this series switches, each group is only for a

single user, so the security name must be the same as the user name set in user table.

Security Model

Configuration options: SNMPv3/SNMPv2c

Default: SNMPv3

Explanation: SNMPv3 means using USM technology. Currently, this parameter is forced to SNMPv3 model.

21.2.4 Typical Configuration Example

As Figure 170 shows, SNMP NMS connects with the switch via Ethernet, and the IP address of NMS is 192.168.0.23, the switch IP address is 192.168.0.2. The user with the name of 111 monitors and manages the Agent by SNMPv3, and the authentication protocol is HMAC-MD5, the security level is AuthNoPriv.

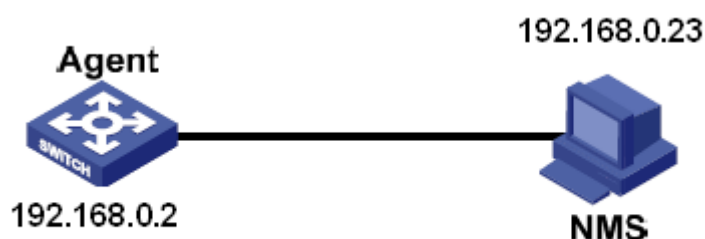


Figure 170: SNMPv3 configuration example

Agent Configuration:

1. Configure SNMPv3 user table. Set the user name to 1111, choose the authentication protocol of HMAC-MD5, and set the authentication password to "aaaa", as shown in Figure 166.
2. Configure SNMPv3 access table. Set the group name to 1111 and the context name to 2222, choose the Security Level of AuthNoPriv, as shown in Figure 167.
3. Configure SNMPv3 context table. Set the context name to 2222, as shown in Figure 168.
4. Configure SNMPv3 group table. Set the security name to 1111, as shown in Figure 169.

If users would like to monitor and manage Agent, it is needed to run the corresponding management software in NMS.

Please refer to "Kyvision Management Software Operation Manual" to learn the specific

operation of Kyvision software in NMS.

22. DHCP

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 171.

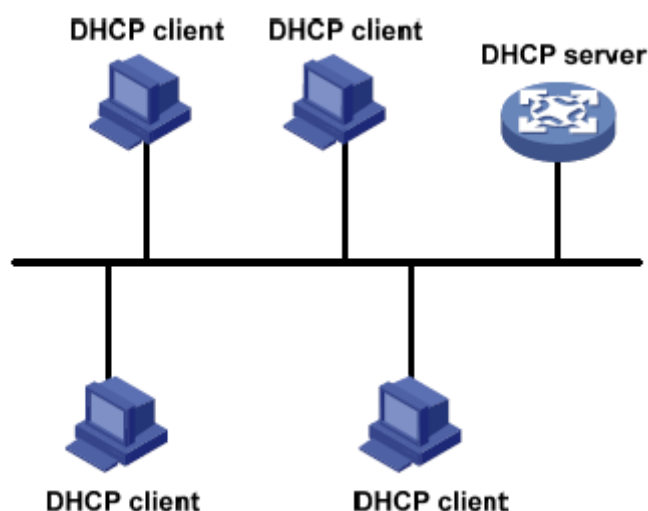


Figure 171: DHCP typical application



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. This series switches do

not support DHCP relay, so the client and the server must be in a same segment.

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. This allocation mechanism contains port IP address binding and MAC address binding.

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.

22.1 DHCP Server Configuration

22.1.1 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.

22.1.2 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 or the port ID connecting to the server.
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 a 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.

22.1.3 Web Configuration

1. Enable DHCP server, as shown in Figure 172.

Configuration Options	Configuration Information
DHCP server status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure 172: DHCP server state

DHCP server status

Configuration options: Enable/Disable

Default: Disable

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

2. Select the DHCP server mode, as shown in Figure 173.

DHCP server mode	<input type="radio"/> Common-Mode <input checked="" type="radio"/> Port-Mode
------------------	--

Figure 173: DHCP server mode

DHCP server mode

Configuration options: Common-mode/Port-mode

Default: Common mode

Explanation: Common mode contains dynamic IP address allocation and static MAC address binding. Port mode means the port desired IP setting.

3. Port-Mode configuration

When select Port-mode in the DHCP server mode, allocate static binding IP addresses to ports, as shown in Figure 174.

Port	Type	IP
1	FE	
2	FE	
3	FE	192.168.0.6
4	FE	
5	FX	
6	FX	

Apply Help

Figure 174: Port Desired IP Setting

Port desired IP setting is to statically configure an IP address to a port. When a port receives a request message from a client, the IP address bound to the port will be allocated to the client. This IP allocation mode has the highest priority and the lease period is 1000 days 23 hours and 59 minutes.

**Caution:**

The IP address bound to the port and the DHCP server must be in same segment.

When port mode is adopted for IP assignment, you need to configure the DHCP server, as shown in Figure 175.

Configuration Options		Configuration Information
DHCP server status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
DHCP server mode	<input type="radio"/> Common-Mode <input checked="" type="radio"/> Port-Mode	
DHCP server IP-pool name	<input type="text" value="pool"/>	
The domain name for the IP-Pool	<input type="text" value="domain"/>	
The starting IP address of the IP-Pool	<input type="text"/>	
The ending IP address of the IP-Pool	<input type="text"/>	
The subnet mask of the network-address	<input type="text" value="255.255.255.0"/>	
The default lease time of the IP address	Infinite: <input type="checkbox"/> 0 Days 1 Hours 0 Minutes	
The maximum lease time of the IP address	1 Days 0 Hours 0 Minutes	
The routers on the IP-Pool's subnet	IP Address 1:	<input type="text"/>
	IP Address 2:	<input type="text"/>
The dns-server for the IP-Pool's subnet	DNS1:	<input type="text"/>
	DNS2:	<input type="text"/>
Run	<input type="button" value="Run"/>	

Figure 175: Port mode server configuration

DHCP server IP-pool name

Configuration range: 1-15 characters

Function: configure the name of the IP address pool

The domain name for the IP-Pool

Configuration range: 1-60 characters

Function: configure the domain name of the IP address pool.

The subnet mask of the network-address

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.

**Caution:**

After configuration, click <Run> button to allocate correct IP addresses to clients.

4. Common-Mode Configuration

When DHCP server mode is set to Common-Mode, it contains static MAC address binding

and dynamic IP address allocation. In static MAC address binding, the system preferentially allocates the IP address bound to the MAC address, otherwise, dynamically allocate IP addresses in the address pool. The static MAC address binding configuration is shown in Figure 176 and Figure 177; dynamic IP address allocation configuration is shown in Figure 178.

Static Binding Between IP and MAC

IP address	192.168.0.36
MAC address	00-1e-cd-02-01-03

Figure 176: Static MAC address binding

Static MAC address binding is to bind the client MAC address to IP address. When the server receives an IP address request message whose source MAC address is the MAC address set here, the IP address bound to this MAC address will be allocated to the client. This kind of IP allocation mode requires server configuration as shown in Figure 178. After configuration, the list of "Static Binding between IP and MAC" shows the statically-configured binding relationships of MAC addresses and IP addresses. Tick in the box of Index to delete the corresponding binding entry.

The list of Static Binding Between IP and MAC

Index	IP Address	MAC Address
<input type="checkbox"/>	192.168.0.26	02-00-AA-BB-CC-05
<input type="checkbox"/>	192.168.0.36	00-1E-CD-02-01-03

Figure 177: Static MAC address binding list

Configuration Options		Configuration Information
DHCP server status		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP server mode		<input checked="" type="radio"/> Common-Mode <input type="radio"/> Port-Mode
DHCP server IP-pool name		pool
The domain name for the IP-Pool		domain
The starting IP address of the IP-Pool		192.168.0.3
The ending IP address of the IP-Pool		192.168.0.201
The subnet mask of the network-address		255.255.255.0
The default lease time of the IP address		Infinite: <input type="checkbox"/> 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
The routers on the IP-Pool's subnet	IP Address 1:	
	IP Address 2:	
The dns-server for the IP-Pool's subnet	DNS1:	
	DNS2:	
Run		Run

Figure 178: Common mode server configuration

DHCP server IP-pool name

Configuration range: 1-15 characters

Function: configure the name of the IP address pool

The domain name for the IP-Pool

Configuration range: 1-60 characters

Function: configure the domain name of the IP address pool

The starting IP address of the IP-Pool/The ending IP address of the IP-Pool

Configuration format: A.B.C.D (the starting IP address and the ending IP address must be in a same segment.

The subnet mask of the network-address

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. In the dynamic address allocation, the range of the IP address pool need to be set and the address range is determined by the subnet mask.

The default lease time of the IP address

Configuration range: 0 Days 0 Hours 1 Minutes – 1000 Days 23 Hours 59 Minutes/Infinite

Default: 0 Days 1 Hours 0 Minutes

Explanation: If the IP address request message sent from the client does not contain a valid lease time, the lease time of the IP address the server allocates to the client is the default value.

The maximum lease time of the IP address

Configuration range: 0 Days 0 Hours 1 Minutes – 1000 Days 23 Hours 59 Minutes

Default: 1 Days 0 Hours 0 Minutes

Explanation: When the client sends an IP address request message to the server, the lease time of the message cannot be longer than the maximum lease time of the IP address. 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.

The routers on the IP-Pool's subnet

Configuration range: the addresses that are in the same segment as the address pool.

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 two gateway addresses.

The dns-server for the IP-Pool's subnet

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. 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 two DNS addresses.

**Caution:**

After configuration, click <Run> button to allocate correct IP addresses to clients.

22.1.4 Typical Configuration Example

As Figure 179 shows, switch A works as a DHCP server and switch B works as a DHCP client. The port 3 of Switch A connects with 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 three ways.

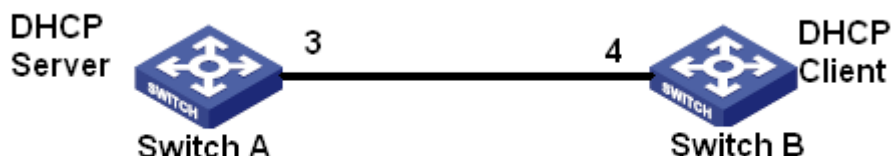


Figure 179: DHCP typical configuration example

Port IP binding:

➤ Switch A Configuration:

1. Enable DHCP server status, as shown in Figure 172.
2. Select Port-Mode in the DHCP server mode, as shown in Figure 173.
3. Set the “IP-pool name” to pool, set “the domain name for the IP- pool” to domain, set “the subnet mask” to 255.255.255.0, as shown in Figure 175.
4. Port 3 bind to the IP address of 192.168.0.6, as shown in Figure 174.
5. Click the <Run> button in the server configuration interface to run the server.

➤ Switch B configuration

1. Select DHCP Client IP in the IP address configuration of Switch B, as shown in Figure 14.
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 180.

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.6
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Figure 180: DHCP client obtain IP address-1

Static MAC address binding method

➤ Switch A configuration

1. Enable the DHCP server status, as shown in Figure 172.
2. Select Common-Mode in the DHCP server mode, as shown in Figure 173.
3. Set the “IP-pool name” to pool, set “the domain name for the IP- pool” to domain, set “the starting IP address of the IP-pool” to 192.168.0.3 and “the ending IP address of the IP-pool” to 192.168.0.201, set “the subnet mask” to 255.255.255.0 and the lease time uses the default value, as shown in Figure 175.
4. Bind the Switch B MAC address of 00-1E-CD-02-01-03 to the IP address of 192.168.0.36, as shown in Figure 176.
5. Click the <Run> button in the server configuration interface to run the server.

➤ Switch B configuration

1. Select DHCP Client IP in the IP address configuration of Switch B, as shown in Figure 14.
2. The switch B obtains the IP address of 192.168.0.36 and the subnet mask of 255.255.255.0 from the DHCP server, as shown in Figure 181

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.36
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Figure 181: DHCP client obtain IP address-2

Dynamic obtainment of IP address in address pool

➤ Switch A configuration

1. Enable DHCP server status, as shown in Figure 172.
2. Select Common-Mode in the DHCP server mode, as shown in Figure 173.
3. Set the “IP-pool name” to pool, set “the domain name for the IP- pool” to domain, set “the starting IP address of the IP-pool” to 192.168.0.3 and “the ending IP address of the IP-pool” to 192.168.0.201, set “the subnet mask” to 255.255.255.0 and the lease time uses the default value.

4. Click the <Run> button in the server configuration screen to run the server.

➤ Switch B configuration

1. Select DHCP Client IP in the IP address configuration of Switch B, as shown in Figure 14.
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 182.

MAC Address	00-1E-CD-02-01-03
Auto IP Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Client IP
IP Address	192.168.0.3
Subnet Mask	255.255.255.0
GateWay	0.0.0.0

Figure 182: DHCP client obtain IP address-3

22.2 DHCP Snooping

22.2.1 Introduction

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.

22.2.2 Web Configuration

1. Enable DHCP Snooping function, as shown in Figure 183.

DHCP Snooping Status

☒ Enable
 ☐ Disable

Apply

Help

Figure 183: DHCP Snooping state

DHCP Snooping Status

Configuration 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 184.

Trust-Port Settings

Port	Type	Protocol Status
1	FE	<input checked="" type="radio"/> Trust <input type="radio"/> Untrust
2	FE	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
3	FE	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
4	FE	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
5	FX	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
6	FX	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust

Apply

Help

Figure 184: Trusted port setting

Protocol Status

Configuration options: Trust/Untrust

Default: Untrust

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.

22.2.3 Typical Configuration Example

As Figure 185 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.

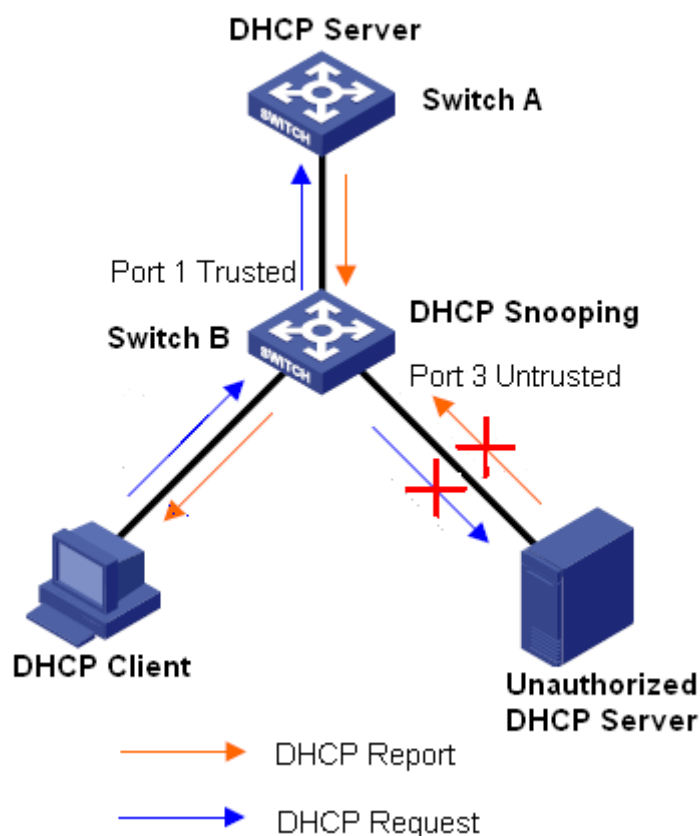


Figure 185: DHCP Snooping Typical Configuration Example

Switch B configuration:

- Enable DHCP Snooping function, as shown in Figure 183.
- Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as

shown in Figure 184.

22.3 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 needs to 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 10.

Table 10: 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 11, or the character string configured by users, as shown in Table 12.

Table 11: Sub-option 2 Field Format-MAC Address

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

Table 12: Sub-option 2 Field Format-Character String

Sub-option type (0x02)	Length (0x10)	Character string
One byte	One byte	16 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.

Character string: the content of Sub-option2 is 1~16 characters set by users. (The character is indicated by ASCII code and each character occupies one byte). The length is fixed to 16. If the configured length of the character string is less than 16 bytes, fill in the missing characters by 0.

22.3.1 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 13.

Table 13: 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; if the message does not contain Option 82 field, process the response message according to the server policy, as shown in Table 14.

Table 14: Processing Modes for Response Messages (DHCP Snooping)

Receive the response message from the DHCP server	Configuration policy	DHCP Snooping device processing the response message
The response message contains Option 82 field	Drop/Keep	Remove the Option 82 field in the response message and forward the message
The response message does not contain Option 82 field	Drop	Drop the response message
	Keep	Keep the message format unchanged and forward the message

2. Web Configuration

DHCP Snooping Option 82 configuration is shown in Figure 186.

Option82 Configuration

Option82 Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Client Policy	<input type="radio"/> Drop <input type="radio"/> Replace <input checked="" type="radio"/> Keep
Server Policy	<input type="radio"/> Drop <input checked="" type="radio"/> Keep
Remote-ID Type	<input type="radio"/> String <input checked="" type="radio"/> MAC
Remote-ID Content	<input type="text" value="00-22-55-AA-BB-04"/>

Figure 186: DHCP Snooping Option 82 configuration

Option82 Status

Configuration options: Enable/Disable

Default: Disable

Function: Enable/Disable Option82 function on DHCP Snooping device

Client Policy

Configuration options: Drop/Replace/Keep

Default: Keep

Function: Configure client policy. The DHCP Snooping device processes the request message sent from the Client according to Client Policy, as shown in Table 13.

Server Policy

Configuration options: Drop/Keep

Default: Keep

Function: Configure server policy. The DHCP Snooping device processes the response message sent from the server according to Server Policy, as shown in Table 14.

Remote-ID Type

Configuration options: String/MAC

Default: MAC

Function: configure the content of Sub-option2.

Explanation: MAC means that the content of sub-option2 is the MAC address of the DHCP Snooping device that receives the request message from the client. String means the content of the sub-option2 is the character string defined by user.

Remote-ID Content

Configuration option: MAC address/1~16 characters

Default: MAC address

Explanation: when the remote ID type is set to MAC, the Remote ID content is forced to the MAC address of the current Snooping device. When the remote ID type is set to String, the Remote ID content is configured by user. The configuration content is 1~16 characters (Each character occupies one byte)

22.3.2 DHCP Server Supports Option 82 Function

1. Introduction

If the DHCP Server is set to support Option82 function, when the DHCP server receives the DHCP request message, it will provides different address allocation solution according to whether the message contains Option82 field and server configuration.

The DHCP server includes the following variables:

- Class: each DHCP server can configure 32 classes. Each class contains three variables: IP address range and Match-always and relay agent information option.
- Match the variable of relay agent information option to the Option 82 field. When the variable value is same as the Option82 field, it is assumed that they are matched, or else they are unmatched.
- If Match-always is enabled, it is assumed that the value of relay agent information option always matches to the Option82 filed without the need of judgment. If the Match-always is disabled, it is needed to judge whether the value of relay agent information option matches to the Option82 filed

According the configuration of the above variables, the server processes the request message as shown in Table 15.

Table 15: Processing Modes for Request Messages (Option82-enabled DHCP Server)

Receive the request message from the DHCP client	Configuration Policy		DHCP server processing the request message
The request message contains Option82 field	Enable Match-always		Add Option82 field into the response message, and allocate IP address and other parameters to the client
	Disable Match-always	Configure the value of relay agent information option	➤ The value of relay agent information option is matched to the Option82 field: Add Option82 field into the response message,

			<p>and allocate IP address and other parameters to the client</p> <p>➤ The value of relay agent information option is not matched to the Option82 field: the server does not allocate IP address to the client</p>
		Do not configure the value of relay agent information option	The server does not allocate IP address to the client
The request message does not contain Option82 field	Enable Match-always		The response message does not contain Option82 field, allocate IP address and other parameters to the client
	Disable Match-always		The server does not allocate IP address to the client

If the DHCP server does not support Option82 function, when the DHCP server receives the message that contains Option82 field, the response message does not contain Option82 field, and the server can allocate IP address and other parameters to the client. Under this condition, the server processes the request message as shown in Table 16.

Table 16: Processing Modes for Request Messages (Option82-disabled DHCP Server)

Receive the request message from the DHCP client	DHCP server processing the request message
The request message contains Option82 field	The server does not allocate IP address and other parameters to the client
The request message does not contain Option82	The response message does not contain Option82

field	field, and the server allocate IP address and other parameter to the client
-------	---

23. Serial Card Management

The series switches support dual systems, that is, switch system and serial port system.

The switch system mainly implements the exchange of Ethernet data. For detailed operations, see related chapters in this document. The serial card system achieves conversion between Ethernet and serial protocol data. For detailed operations, refer to the *SICOM3005A Serial Port Server Web Operation Manual*. In the switch system, you can view the management IP and MAC addresses of the serial card system, as shown in Figure 187.

S-CH ID	VLAN ID	IP Address	MAC
1	1,2	<u>192.168.0.3</u>	00-1e-cd-00-01-23

Figure 187 Show the management IP Address of the Serial Card

24. Appendix: Acronyms

Acronym	Full Spelling
AAA	Authentication, Authorization, Accounting
ARP	Address Resolution Protocol
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services CodePoint
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transport Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MAC	Media Access Control
MIB	Management Information Base
NAS	Network Access Server
NMS	Network Management Station
OID	Object Identifier
PAE	Port Access Entity
PVLAN	Private VLAN

QoS	Quality of Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
UDP	User Datagram Protocol
USM	User-Based Security Model
VCT	Virtual Cable Tester
VLAN	Virtual Local Area Network
WRR	Weighted Round Robin