

# **SICOM3000/3004/3005/3006 Series Industrial Ethernet Switches Web Operation Manual**



**Kyland Technology Co., LTD.**

Publication Date: Sept. 2012

Version: V2.0

Customer Service Hotline: (+8610) 88796676

FAX: (+8610) 88796678

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

E-mail: [support@kyland.biz](mailto:support@kyland.biz)

**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.

**Copyright © 2012 KYLAND Technology CO., LTD.**

**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.

## Contents

Preface .....	1
1 Product Introduction .....	5
1.1 Overview .....	5
1.2 Product Models .....	5
1.3 Software Features .....	6
2 Switch Access .....	7
2.1 View Types .....	7
2.2 Access through Console Port .....	8
2.3 Access through Telnet .....	11
2.4 Access through Web .....	12
3 Device Management .....	15
4 Device Status .....	16
4.1 Basic Information .....	16
4.2 Port Status .....	16
4.3 Port Statistics .....	18
4.4 System Operating Information .....	18
5 Basic Configuration .....	19
5.1 IP Address .....	19
5.2 Basic Information .....	20
5.3 Port Configuration .....	21
5.4 Password Change .....	24
5.5 Software Update .....	24
5.5.1 Software Update through FTP .....	25
5.6 Software Version Query .....	30
5.7 Configuration Upload/Download .....	30
6 Advanced Configuration .....	32
6.1 Port Rate Limiting .....	32
6.1.1 Overview .....	32
6.1.2 Web Configuration .....	32

6.1.3	Typical Configuration Example .....	34
6.2	VLAN.....	34
6.2.1	Overview.....	34
6.2.2	Principle.....	34
6.2.3	Port-based VLAN.....	35
6.2.4	Web Configuration .....	37
6.2.5	Typical Configuration Example .....	41
6.3	PVLAN .....	43
6.3.1	Overview.....	43
6.3.2	Web Configuration .....	44
6.3.3	Typical Configuration Example .....	45
6.4	Port Mirroring .....	46
6.4.1	Overview.....	46
6.4.2	Description.....	46
6.4.3	Web Configuration .....	47
6.4.4	Typical Configuration Example .....	48
6.5	Port Trunk .....	49
6.5.1	Overview.....	49
6.5.2	Implementation .....	49
6.5.3	Description.....	50
6.5.4	Web Configuration .....	51
6.5.5	Typical Configuration Example .....	53
6.6	Link Check .....	53
6.6.1	Overview.....	53
6.6.2	Web Configuration .....	53
6.7	Static Multicast .....	54
6.7.1	Overview.....	54
6.7.2	Web Configuration .....	54
6.8	IGMP Snooping.....	57
6.8.1	Overview.....	57

6.8.2	Concepts .....	57
6.8.3	Principle .....	58
6.8.4	Web Configuration .....	58
6.8.5	Typical Configuration Example .....	60
6.9	ACL .....	61
6.9.1	Overview .....	61
6.9.2	Web Configuration .....	61
6.9.3	Typical Configuration Example .....	63
6.10	ARP .....	63
6.10.1	Overview .....	63
6.10.2	Description .....	64
6.10.3	Web Configuration .....	64
6.11	SNMP .....	66
6.11.1	Overview .....	66
6.11.2	Implementation .....	66
6.11.3	Description .....	67
6.11.4	MIB .....	67
6.11.5	Web Configuration .....	68
6.11.6	Typical Configuration Example .....	70
6.12	DT-Ring .....	71
6.12.1	Overview .....	71
6.12.2	Concepts .....	72
6.12.3	Implementation .....	72
6.12.4	Web Configuration .....	76
6.12.5	Typical Configuration Example .....	81
6.13	RSTP/STP .....	81
6.13.1	Overview .....	81
6.13.2	Concepts .....	82
6.13.3	BPDU .....	82
6.13.4	Implementation .....	83

6.13.5 Web Configuration .....	85
6.13.6 Typical Configuration Example .....	88
6.14 RSTP/STP Transparent Transmission.....	89
6.14.1 Overview.....	89
6.14.2 Web Configuration .....	90
6.14.3 Typical Configuration Example .....	91
6.15 QoS.....	92
6.15.1 Overview.....	92
6.15.2 Principle.....	92
6.15.3 Web Configuration .....	93
6.15.4 Typical Configuration Example .....	98
6.16 MAC Address Aging Time .....	99
6.16.1 Overview.....	99
6.16.2 Web Configuration .....	100
6.17 LLDP .....	100
6.17.1 Overview.....	100
6.17.2 Web Configuration .....	101
6.18 SNTP .....	101
6.18.1 Overview.....	101
6.18.2 Web Configuration .....	102
6.19 MSTP .....	104
6.19.1 Overview.....	104
6.19.2 Concepts .....	106
6.19.3 Implementation .....	110
6.19.4 Web Configuration .....	111
6.19.5 Typical Configuration Example .....	120
6.20 Alarm.....	123
6.20.1 Overview.....	123
6.20.2 Web Configuration .....	123
6.21 Port Traffic Alarm.....	126

6.21.1 Overview.....	126
6.21.2 Web Configuration .....	127
6.22 GMRP .....	128
6.22.1 GARP .....	128
6.22.2 GMRP .....	129
6.22.3 Description.....	130
6.22.4 Web Configuration .....	130
6.22.5 Typical Configuration Example .....	134
6.23 RMON .....	135
6.23.1 Overview.....	135
6.23.2 RMON Groups .....	136
6.23.3 Web Configuration .....	137
6.24 Unicast Address Configuration and Query .....	142
6.24.1 Overview.....	142
6.24.2 Web Configuration .....	142
Appendix: Acronyms .....	145

## Preface

This manual mainly introduces the access methods and software features of SICOM3000/3004/3005/3006 series industrial Ethernet switches, and details Web configuration methods.

## Content Structure

The manual contains the following contents:

Chapter	Content
1. Product Introduction	<ul style="list-style-type: none"><li>➤ Overview</li><li>➤ Product models</li><li>➤ Software features</li></ul>
2. Switch Access	<ul style="list-style-type: none"><li>➤ View types</li><li>➤ Access through Console Port</li><li>➤ Access through Telnet</li><li>➤ Access through Web</li></ul>
3. Device Management	<ul style="list-style-type: none"><li>➤ Restart</li><li>➤ Logout</li></ul>
4. Device Status	<ul style="list-style-type: none"><li>➤ Basic information</li><li>➤ Port status</li><li>➤ Port statistics</li></ul>
5. Basic Configuration	<ul style="list-style-type: none"><li>➤ IP address</li><li>➤ Basic information</li><li>➤ Port configuration</li><li>➤ Password change</li><li>➤ Software update (FTP)</li><li>➤ Software version query</li><li>➤ Configuration upload/download</li></ul>
6. Advanced Configuration	<ul style="list-style-type: none"><li>➤ Port rate limiting</li><li>➤ VLAN</li></ul>

	<ul style="list-style-type: none"> <li>➤ PVLAN</li> <li>➤ Port mirroring</li> <li>➤ Port trunk</li> <li>➤ Link check</li> <li>➤ Static multicast</li> <li>➤ IGMP Snooping</li> <li>➤ ACL</li> <li>➤ ARP</li> <li>➤ SNMP</li> <li>➤ DT-Ring</li> <li>➤ RSTP/STP</li> <li>➤ RSTP/STP transparent transmission</li> <li>➤ QoS</li> <li>➤ MAC address aging time</li> <li>➤ LLDP</li> <li>➤ SNTP</li> <li>➤ MSTP</li> <li>➤ Alarm</li> <li>➤ Port traffic alarm</li> <li>➤ GMRP</li> <li>➤ RMON</li> <li>➤ Unicast address configuration and query</li> </ul>
--	---

## Conventions in the manual

### 1. Text format conventions




Format	Description
< >	The content in < > is a button name. For example, click <Apply> button.
[ ]	The content in [ ] is a window name or a menu name. For example, click [File] menu item.

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

## 2. CLI conventions

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

## 3. Symbol conventions

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

## Product Documents

The documents of SICOM3000/3004/3005/3006 series industrial Ethernet switches include:

Document	Content
SICOM3000 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3000.
SICOM3004 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3004.
SICOM3005 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3005.
SICOM3006 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3006.
SICOM3000/3004/3005/3006 Series Industrial Ethernet Switches Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

### Document Obtainment

Product documents can be obtained by:

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

# 1 Product Introduction

## 1.1 Overview

The series switches are applied in the wind power, distribution network automation, power, intelligent transportation, and many other industries. They support RSTP, MSTP, DT-Ring, and redundant power supply, securing reliable operation. SICOM3004/3006 are embedded boards that can be installed in other devices for integration.

## 1.2 Product Models

The series switches include four models: SICOM3000, SICOM3004, SICOM3005, and SICOM3006. They provide extensive interfaces to suit customers' different needs. For details, see the following table.

Table 1 Product Models

Model	Gigabit	100M		Remarks
	SFP Slot	RJ45 Port	SC/ST/FC Port	
SICOM3000-2GX-2S/M-6T	2	6	2	--
SICOM3000-2GX-8T	2	8	--	--
SICOM3000-2S/M-6T	--	6	2	--
SICOM3000-1S/M-7T	--	7	1	--
SICOM3000-8T	--	8	--	--
SICOM3000-MA-C-2GX-2S/M-6T	2	6	2	For coal mining industry, conformal coating
SICOM3004-4T	--	4	--	Bare board
SICOM3004-2S/M-2T	--	2	2	Bare board
SICOM3005-2S/M-4T	--	4	2	--
SICOM3005-1S/M-4T	--	4	1	--

SICOM3005-6T	--	6	--	--
SICOM3006-6T	--	6	--	Bare board
SICOM3006-2S/M-4T	--	4	2	Bare board
SICOM3006-4S/M-2T	--	2	4	Bare board

### 1.3 Software Features

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

- Redundancy protocols: RSTP/STP, DT-Ring, and MSTP
- Multicast protocols: IGMP Snooping, GMRP, and static multicast
- Switching attributes: VLAN, PVLAN, QoS, and ARP
- Bandwidth management: port trunk, port rate limiting
- Security: ACL
- Synchronization protocol: SNTP
- Device management: FTP software update, configuration upload/download
- Device diagnosis: port mirroring, LLDP, link check
- Alarm function: port alarm, power alarm, ring alarm, IP/MAC address conflict alarm, and port traffic alarm
- Network management: management by CLI, Telnet, Web and Kyvision network management software, and SNMP network monitoring
- ...

## 2 Switch Access

You can access the switch by:

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

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

### 2.1 View Types

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

Table 2 View Types

View Prompt	View Type	View Function	Command for View Switching
SWITCH>	User view	View recently used commands. View software version.	Input " <b>enable</b> " to enter the management view.
SWITCH #	Management view	View the IP address. View the switch configuration. Upload/Download configuration/log file. Restore default configuration. Save current configuration. Update software. Restart the switch.	Input " <b>configure terminal</b> " to enter the configuration view from the management view. Input " <b>exit</b> " to return to the user view.
SWITCH(config)#	Configuration view	Configure switch functions.	Input " <b>exit</b> " or " <b>end</b> " to return to the management view.

When the switch is configured through the CLI, "?" can be used to get command help. In the help information, there are different parameter

description formats. For example, <1, 255> means a number range; <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 recently used commands.

## 2.2 Access through Console Port

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

1. Connect the serial port of a PC to the console port of the switch with a DB9-RJ45 cable.
2. Run the Hyper Terminal in Windows desktop. Click [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in the following figure.

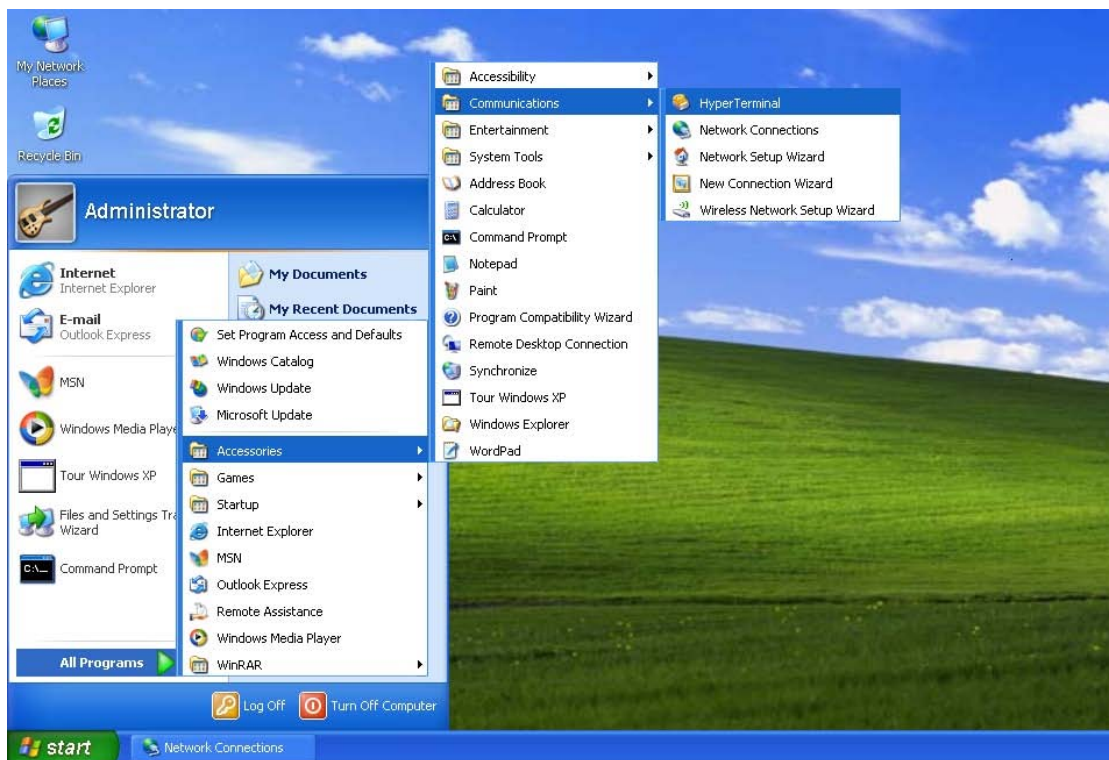


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in the following figure.

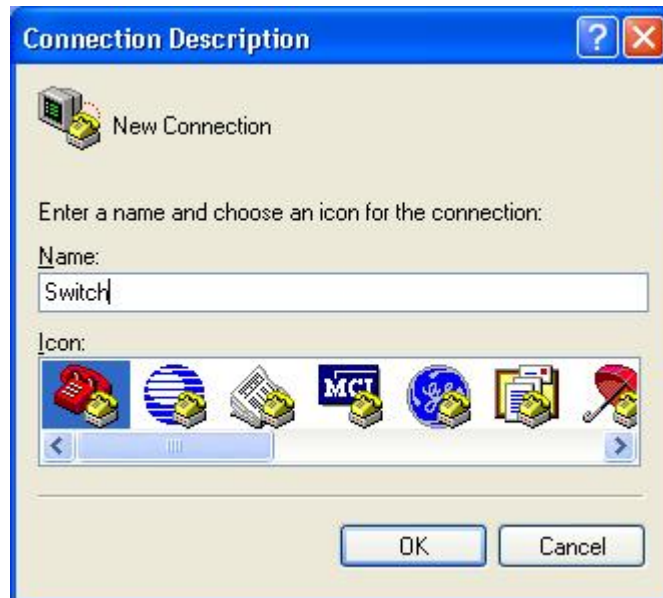


Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown in the following figure.



Figure 3 Selecting the Communication Port

**Note:**

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

5. Set port parameters (Bits per second: 9600, Data bits: 8, Parity: None, Stop

bits: 1, and Flow control: None), as shown in the following figure.

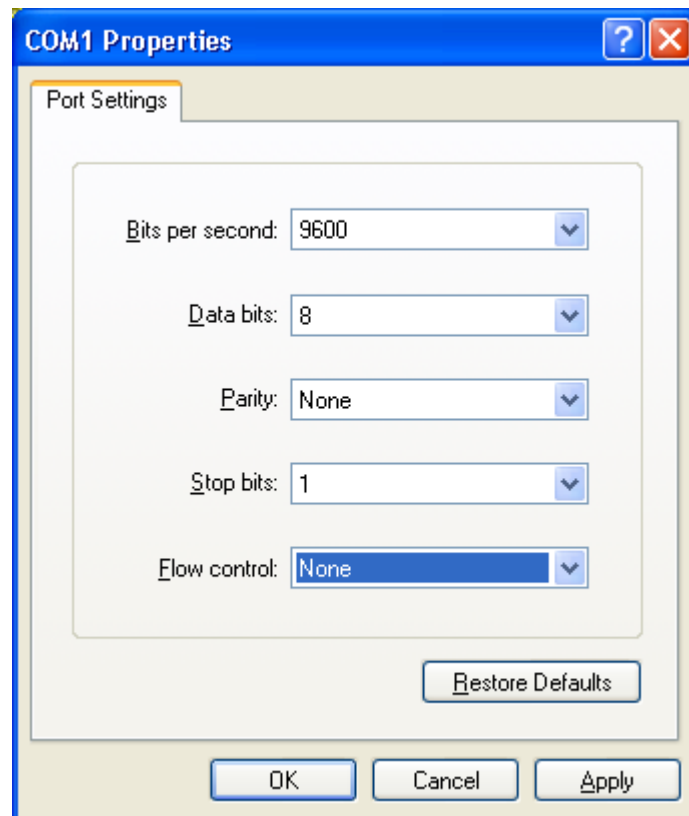


Figure 4 Setting Port Parameters

6. Click <OK>. The switch CLI is displayed. Input password "admin" and press <Enter> to enter the user view, as shown in the following figure.

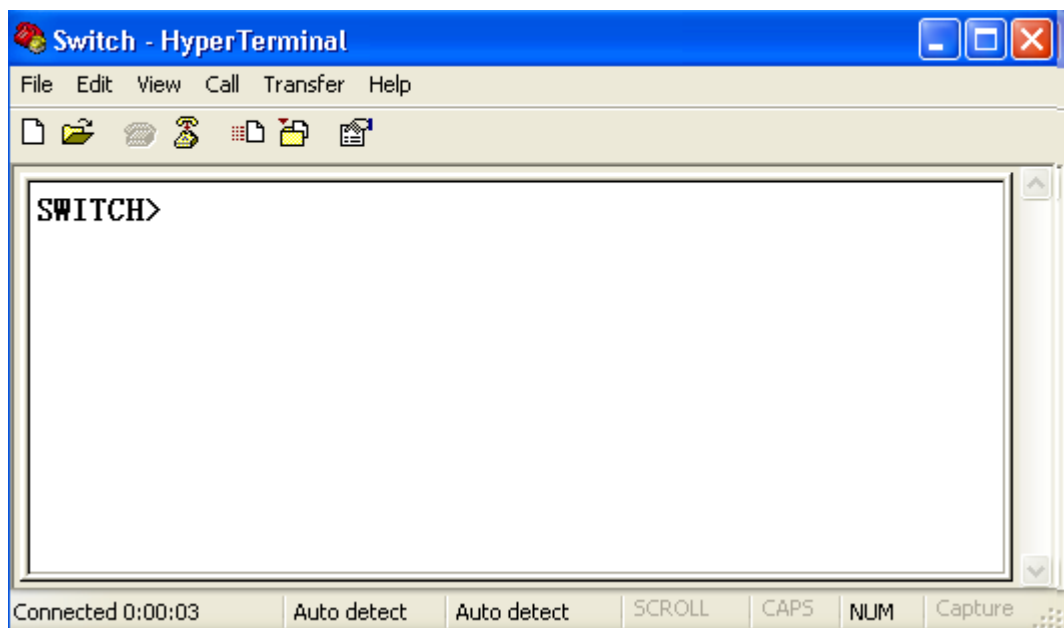


Figure 5 CLI

## 2.3 Access through Telnet

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

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in the following figure.

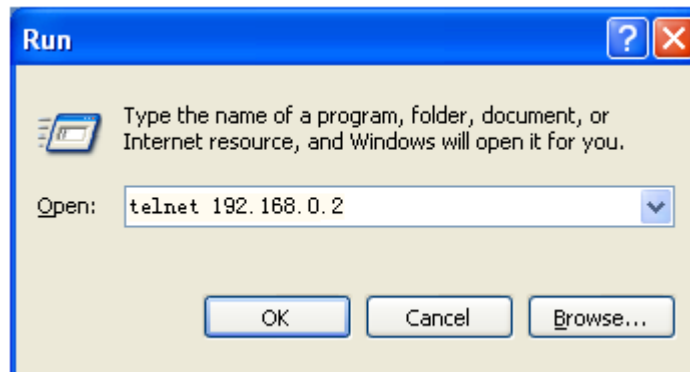


Figure 6 Telnet Access



**Note:**

For details about how to confirm the switch IP address, see section 5.1 IP Address.

2. In the Telnet interface, input "admin" in User, and "123" in Password. Press <Enter> to log in to the switch, as shown in the following figure.

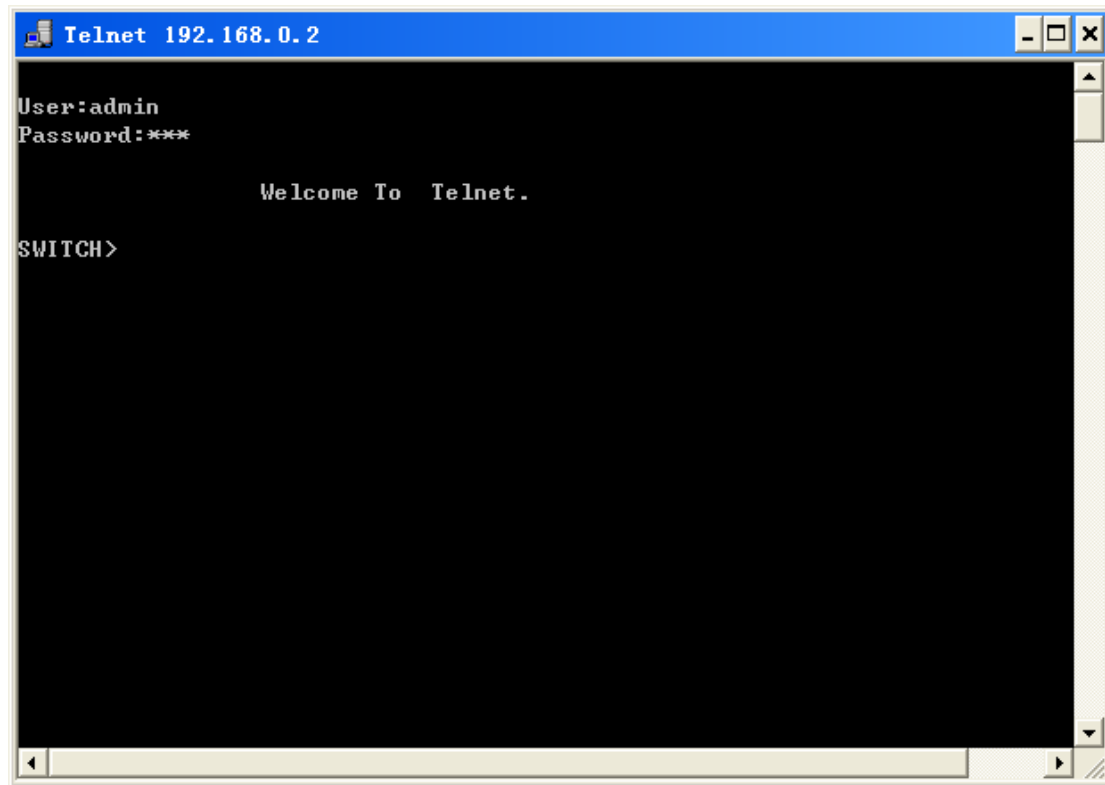


Figure 7 Telnet Interface

## 2.4 Access through Web

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.

1. Input "IP address" in the browser address bar. The login interface is displayed, as shown in the following figure. Input the default user name "admin" and password "123". Click <Login>.

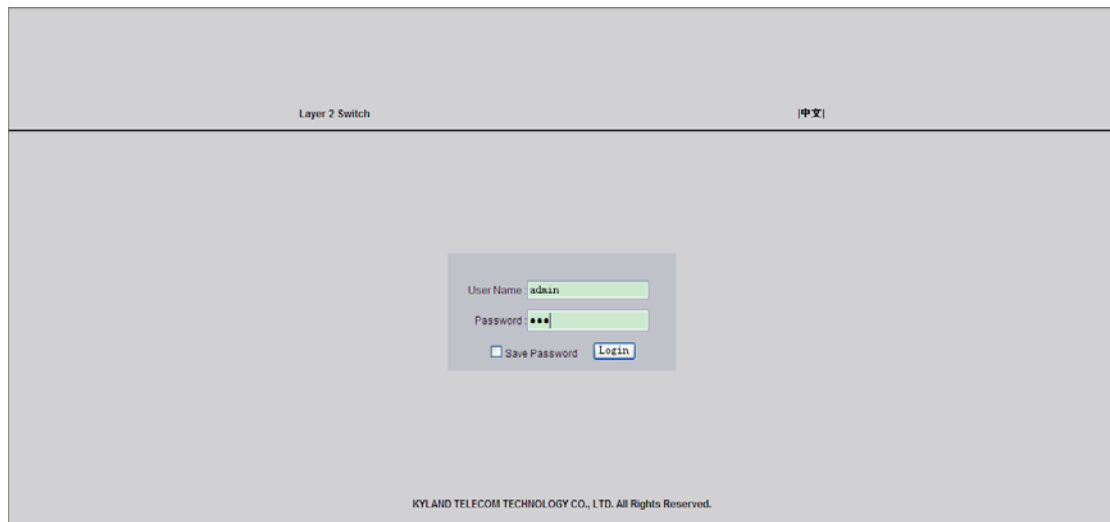


Figure 8 Web Login

The English login interface is displayed by default. You can click <中文> to change to the Chinese login interface.



**Note:**

For details about how to confirm the switch IP address, see section 5.1 IP Address.

---

2. After you log in successfully, there is a navigation tree on the left of the interface, as shown in the following figure.

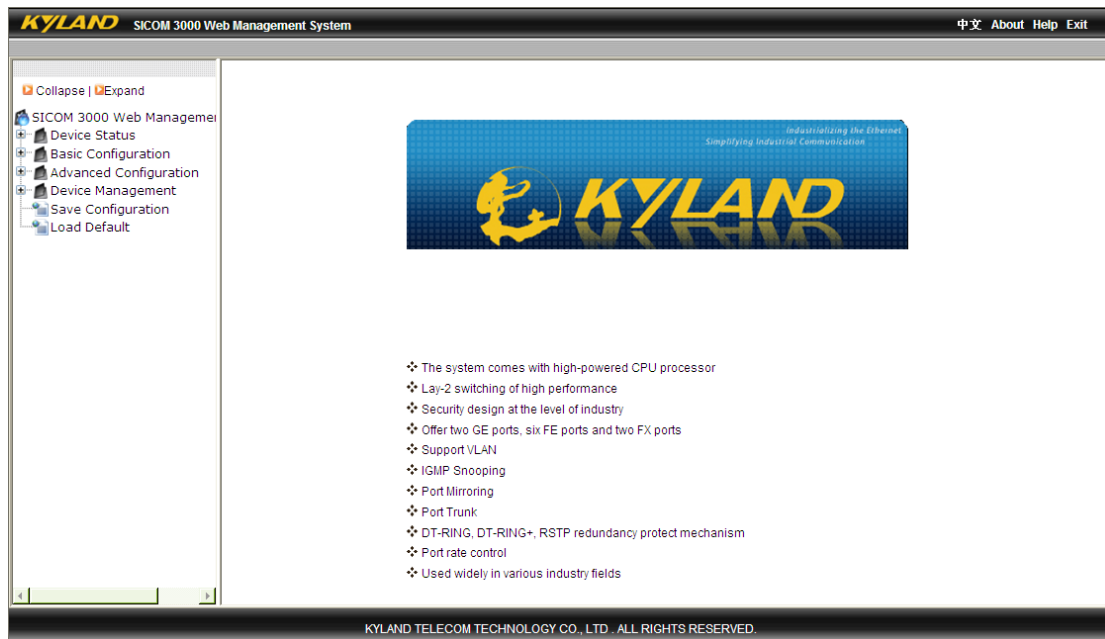


Figure 9 Web Interface

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 Configuration] or [Load Default] in the top menu. In the upper right corner, you can click <中文> to switch to the Chinese interface and <Exit> 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 includes the MAC address, SN, IP address, subnet mask, gateway, system name, device model, and software version, as shown in the following figure.

Item	Information
MAC Address	00-0A-93-05-00-10
SN	S3A2M070015
IP Address	192.168.0.22
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	Switch
Device Model	SICOM3000_2GX_2S_SC_6T
Software Version	ID:1 V1.5.37 (2012-5-12 22:58)
FW Version	v1.1.8 (2010-11-11 14:24)

Figure 10 Basic Information

### 4.2 Port Status

Port status page displays the port number, administration status, link status, speed, duplex, and flow control, as shown in the following figure.

Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
FE1	Enable	Enable	Down	---	---	---	---	---
FE2	Enable	Enable	Down	---	---	---	---	---
FE3	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE5	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE6	Enable	Enable	Down	---	---	---	---	---
FX7	Enable	Enable	Down	---	---	---	---	---
FX8	Enable	Enable	Down	---	---	---	---	---
GE1	Enable	Enable	Down	---	---	---	---	---
GE2	Enable	Enable	Down	---	---	---	---	---

Figure 11 Port Status

#### Port ID

Display the type and ID of ports.

FE: 10/100Base-TX RJ45 port

FX: 100Base-FX port

GE: Gigabit RJ45 port

GX: Gigabit SFP slot

### **Administration Status**

Display the administration status of ports.

Enable: The port is available and permits data transmission.

Disable: The port is locked without data transmission.

### **Operation Status**

Display the operation status of ports.

#### **Link**

Display 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**

Display the communication speed of LinkUp ports.

#### **Duplex**

Display 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**

Display the flow control status of LinkUp ports.

#### **RX**

Options: Enable/Disable

Enable: The port can receive data.

Disable: The port cannot receive data.

#### **TX**

Options: Enable/Disable

Enable: The port can transmit data.

Disable: The port cannot transmit data.

**Note:**

For details about port settings, see section 5.3 Port Configuration.

### 4.3 Port Statistics

Port statistics cover the number of bytes/packets that each port sends/receives, CRC errors, and number of packets with less than 64 bytes, as shown in the following figure.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
FE1	Enable	Down	0	0	0	0	0	0
FE2	Enable	Down	0	0	0	0	0	0
FE3	Enable	Up	56719	723	0	0	0	0
FE4	Enable	Up	115687	908	31371	214	0	0
FE5	Enable	Up	19224	132	74839	815	0	0
FE6	Enable	Down	0	0	0	0	0	0
FX7	Enable	Down	0	0	0	0	0	0
FX8	Enable	Down	0	0	0	0	0	0
GE1	Enable	Down	0	0	0	0	0	0
GE2	Enable	Down	0	0	0	0	0	0

Reset

Figure 12 Port Statistics

You can click <Reset> to restart statistics collection.

### 4.4 System Operating Information

System operating information includes the device runtime and CPU usage, as shown in the following figure.

Device Operating	
Device Operating Time:	0Days,20H:41M:37S
CPU:	0%(short-term), 1%(long-term)

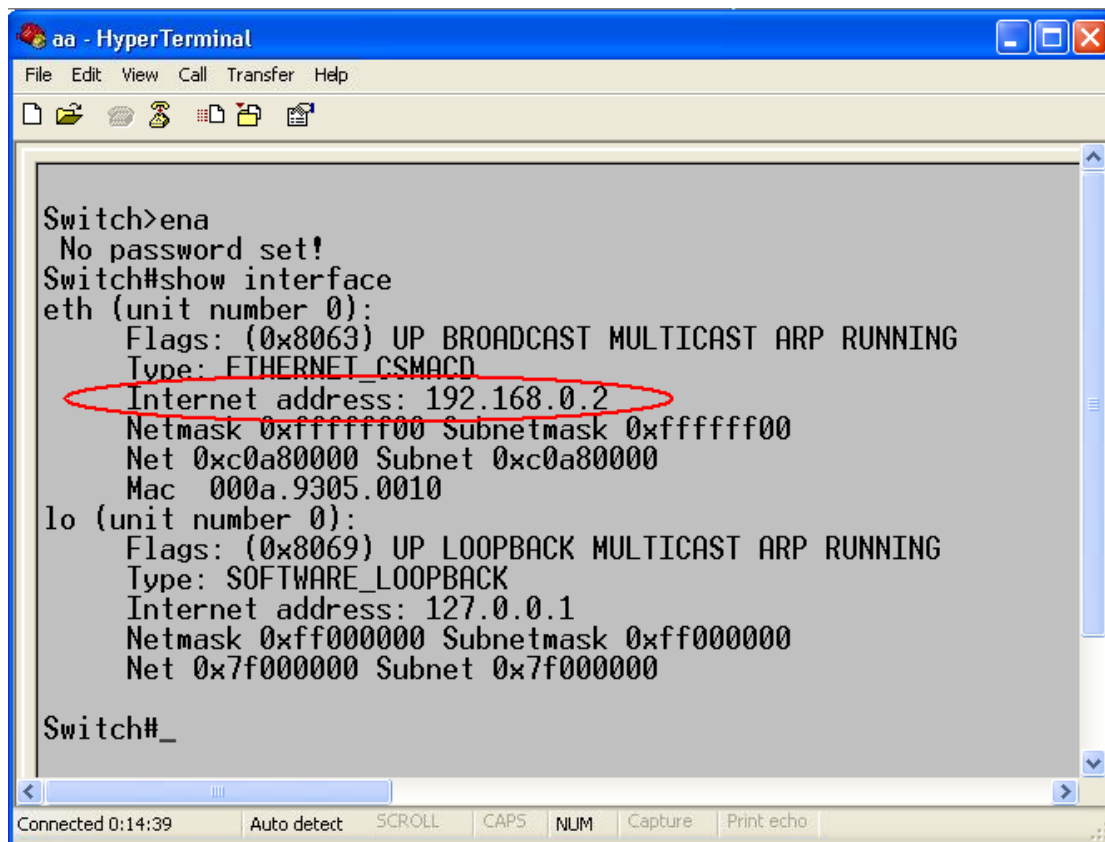
Figure 13 System Operating Information

## 5 Basic Configuration

### 5.1 IP Address

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

Log in to the switch CLI through the console port. Run the "**show interface**" command in the management view to view the switch IP address. As shown in the following figure, the IP address is circled in red.



```
Switch>ena
No password set!
Switch#show interface
eth (unit number 0):
  Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 192.168.0.2
  Netmask 0xffffffff Subnetmask 0xffffffff
  Net 0xc0a80000 Subnet 0xc0a80000
  Mac 000a.9305.0010
lo (unit number 0):
  Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
  Type: SOFTWARE_LOOPBACK
  Internet address: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  Net 0x7f000000 Subnet 0x7f000000

Switch#_
```

Figure 14 Viewing IP Address

2. Set the IP address.

Switch IP address and gateway can be configured manually, as shown in the following figure.

MAC Address	00-0A-93-05-00-10
IP Address	192.168.0.4
Subnet Mask	255.255.255.0
GateWay	192.168.0.1

Apply Help

Figure 15 IP Address

**Caution:**

- IP address and gateway must be in the same network segment; otherwise, the IP address cannot be modified.
- For the series switches, the change in IP address will take effect only after the device is restarted.

## 5.2 Basic Information

Basic information includes the project name, switch name, location, contact, and system time, as shown in the following figure.

Project Name	PRJNAME
System Name	Switch
Location	Chongxin Mansion Buil
Contact	+86-10-88798888

Apply Help

Figure 16 Device Information

**Project Name**

Range: 1~64 characters

**System Name**

Range: 1~32 characters

**Location**

Value: English/Chinese characters

Range: 1~255 characters (One Chinese character occupies the position of two English characters.)

### Contact

Value: English/Chinese characters

Range: 1~32 characters (One Chinese character occupies the position of two English characters.)

## 5.3 Port Configuration

In port configuration, you can configure port status, port speed, flow control, and other information, as shown in the following figures.

Port ID	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FE1	Disable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE2	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FE3	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FX7	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX8	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
GE1	Enable	Enable	Disable	1000M	Full	Off	Enable	Enable	Noreset
GE2	Enable	Enable	Disable	1000M	Full	Off	Enable	Enable	Noreset

Figure 17 Port Configuration

Port ID	Port Description	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FX1	Null	Disable	Disable	Disable	100M	Full	Off	Disable	Disable	Noreset
FX2	5	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FE3	a	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	-	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Null	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Null	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset

Figure 18 Port Configuration (SICOM3005)

### Administration Status

Options: Enable/Disable

Default: Enable

Function: Allow data transmission on port or not.

Description: Enable indicates the port is enabled and permits data transmission; Disable indicates the port is disabled and disallows data

transmission. This option directly affects the hardware status of the port and triggers port alarms.

### **Operation Status**

Description: When the administration status is Enable, the operation status is set to Enable forcibly; when the administration status is Disable, the operation status is set to Disable forcibly.

### **Auto**

Options: Enable/Disable

Default: Enable

Function: Configure the auto-negotiation status of ports.

Description: When Auto is set to Enable, the port speed and duplex mode will be automatically negotiated according to port connection status; when Auto is set to Disable, the port speed and duplex mode can be configured.



#### **Caution:**

100Base-FX ports are set to Disable forcibly.

---

### **Speed**

Options: 10M/100M/1000M

Function: Configure the speed of ports forcibly.

Description: When Auto is set to Disable, the port speed can be configured.

### **Duplex**

Options: Half/Full

Function: Configure the duplex mode of ports.

Description: When Auto is set to Disable, the port duplex mode can be configured.

---



#### **Caution:**

- 10/100Base-TX ports can be set to auto-negotiation, 10M&full duplex, 10M&half duplex, 100M&full duplex, or 100M&half duplex.
-

- 100Base-FX ports are set to 100M&full duplex.
  - 1000M fiber ports can be set to auto-negotiation and 1000M&full duplex.
- 

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

### **Flow Control**

Options: Off/On

Default: Off

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

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

### **RX**

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

Description: Enable indicates the port can receive data; Disable indicates the port cannot receive data.

## TX

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

Description: Enable indicates the port can transmit data; Disable indicates the port cannot transmit data.

## Reset

Options: Reset/Noreset

Default: Noreset

Function: Reset the port or not.

## 5.4 Password Change

You can change the password for user name "admin", as shown in the following figure.

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

Figure 19 Changing the Password

## 5.5 Software Update

Software updates may help the switch to improve its performance. For this series switches, software updates include BootROM software version update and system software version update. The BootROM software version should be updated before the system software version. If the BootROM version does not change, you can update only the system software version.

The software version update requires an FTP server.

### 5.5.1 Software Update through FTP

Install an FTP server. The following uses WFTPD software as an example to introduce FTP server configuration and software update.

1. Click [Security] → [Users/Rights]. The "Users/Rights Security Dialog" dialog box is displayed. Click <New User> to create a new FTP user, as shown in the following figure. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.

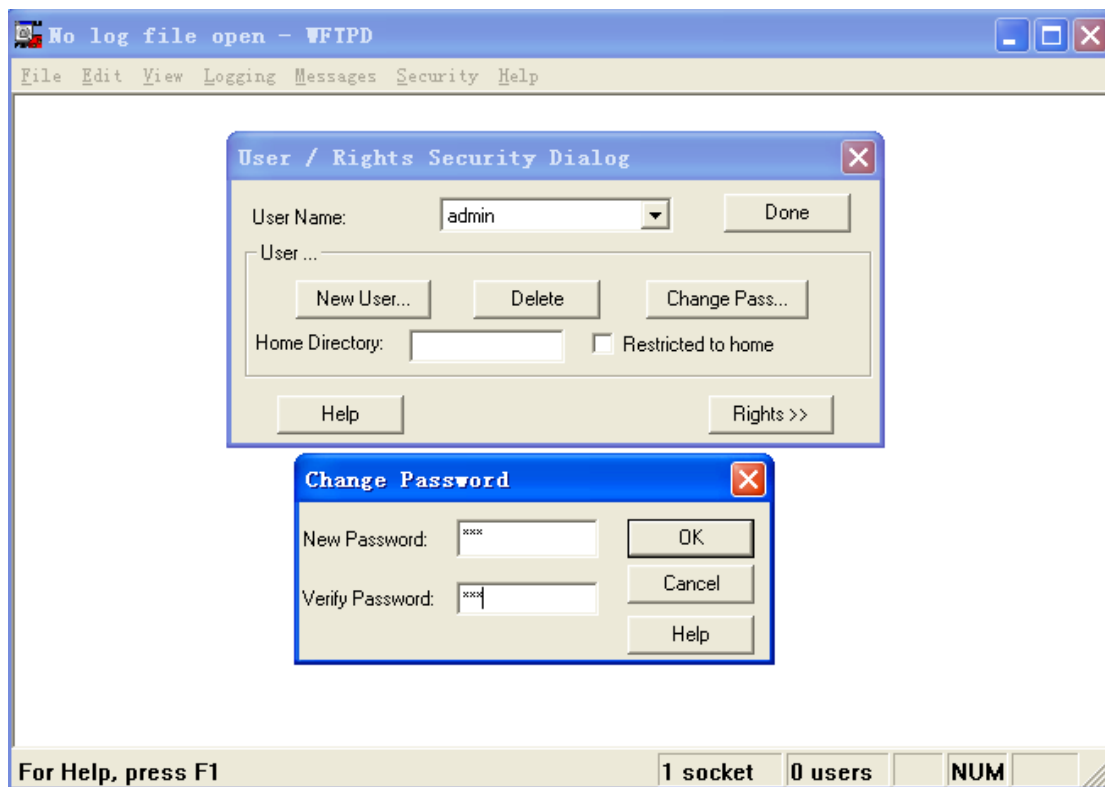


Figure 20 Creating a New FTP User

2. Input the storage path of the update file in "Home Directory", as shown in the following figure. Click <Done>.

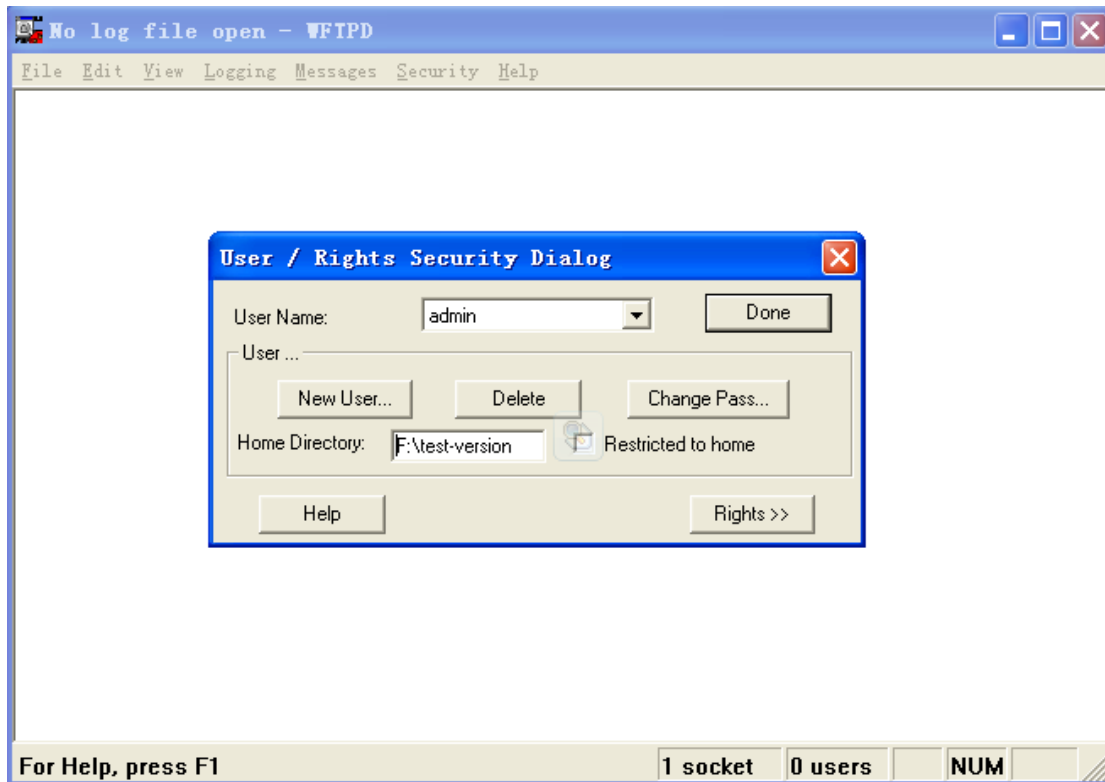


Figure 21 File Location

- To update the BootROM software, input the following command in the management view.

Switch#**update bootrom** *File\_name* *Ftp\_server\_ip\_address* *User\_name*  
*Password*

The following table lists the parameter descriptions.

Table 3 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

- The following figure 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>.

SoftwareID	2
FTP Server IP Address	192.168.0.23
FTP File Name	icom-3024p-1.5.37.bin
FTP User Name	admin
FTP Password	•••

Apply Help

Figure 22 Software Update through FTP



**Warning:**

- Only the software version in inactive state can be used for update through Web.
- The file name must contain an extension. Otherwise, the update may fail.

5. Ensure normal communication between the FTP server and the switch, as shown in the following figure.

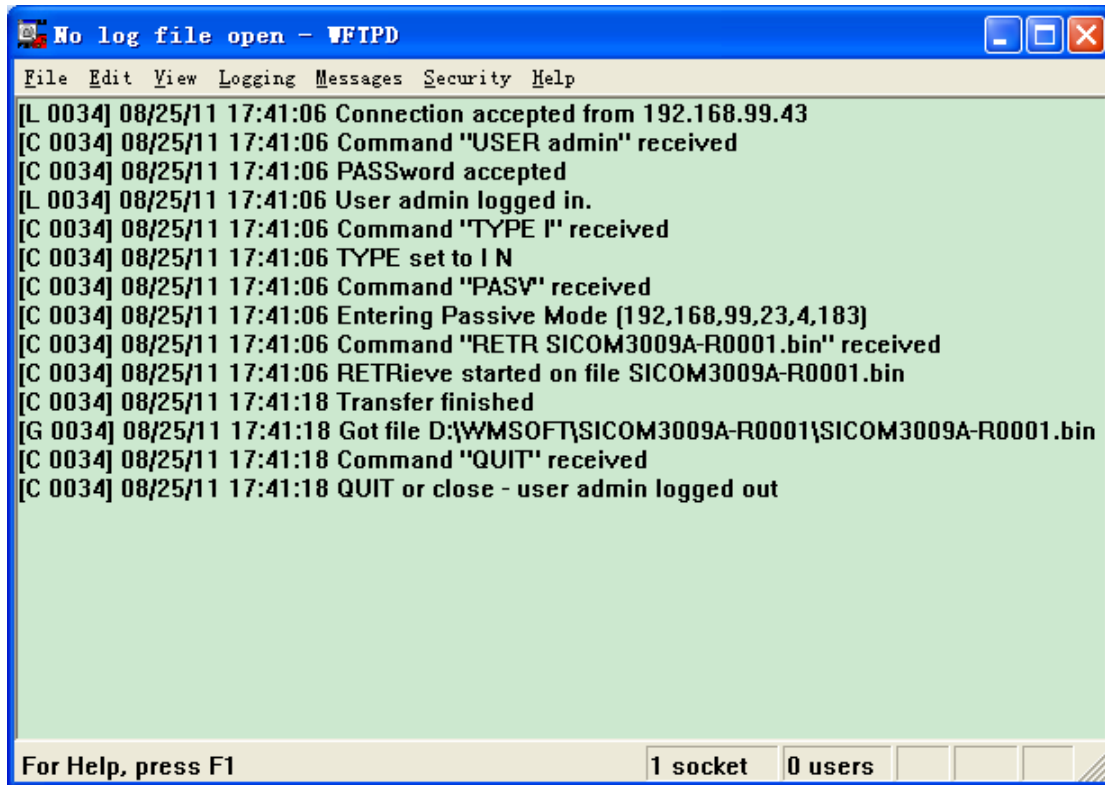


Figure 23 Normal Communication between FTP Server and Switch



**Caution:**

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

6. Wait for the update to complete, as shown in the following figure.

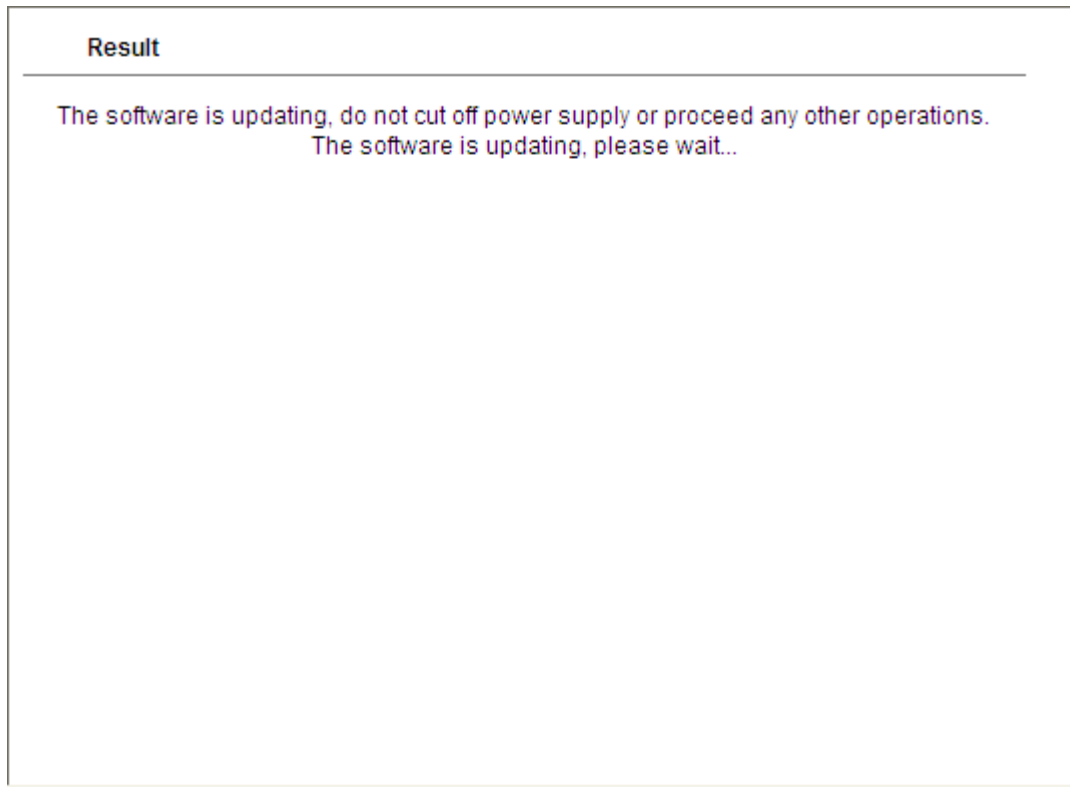


Figure 24 Update Process

7. When the update is completed as shown in the following figure, please reboot the device and open the Switch Basic Information page to check whether the update succeeded and the new version is active.



Figure 25 Successful Software Update through FTP

**Warning:**

- In the software update process, keep the FTP server software running.
- When update completes, reboot the device to make the new version take effect.
- If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

## 5.6 Software Version Query

Two software versions can be downloaded to the switch, but only one can be in active state at a time. In the Web UI, you can update only the inactive version.

By querying software versions, you can learn the IDs, release dates, and statuses of the two versions, as shown in the following figure.

ID	Version	Date	Status
1	v1.5.37	2012-5-12 22:58	Active
2	v1.5.33	2011-12-27 13:31	Inactive

Apply Help

Figure 26 Software Version Query

## 5.7 Configuration Upload/Download

Configuration backup function can save current switch configuration files on the server. When the switch configuration is changed, you can download the original configuration files from the server to switch through FTP.

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 the following figures.

**Caution:**

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

Select Mode	Upload file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	•••

Apply Help

Figure 27 Configuration File Upload

Select Mode	Download file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	•••

Apply Help

Figure 28 Configuration File Download

## 6 Advanced Configuration

### 6.1 Port Rate Limiting

#### 6.1.1 Overview

Port rate limiting is to limit the rate packets received or transmitted by a port and discard the packets whose rate exceeds the threshold. The function takes effect on all packets at the egress but only certain types of packets at the ingress.

The following packets are controlled at the ingress.

- Unknown unicast packets: indicate the unicast packets not added statically and the packets whose MAC addresses are not learned.
- Unknown multicast packets: indicate the multicast packets not added statically and the packets not learned through IGMP Snooping or GMRP.
- Broadcast packets: indicate the packets with the destination MAC address of FF:FF:FF:FF:FF:FF.
- Reserved multicast packets: indicate the packets with MAC addresses in the range of 0x0180c2000000 to 0x0180c200002f.
- Multicast packets: indicate the packets added statically or learned through IGMP Snooping or GMRP.
- Unicast packets: indicate the unicast packets added statically or whose source MAC addresses are learned.

#### 6.1.2 Web Configuration

1. Select the packet types for rate control, as shown in the following figure.

The restricted speed is disabled when it is set to 0.

Set Packet Type for Rate Control

Type	Service	Broadcast	Remark
Unicast	<input type="checkbox"/>	<input type="checkbox"/>	Unicast packet type and address added statically or learned through source MAC.
Multicast	<input type="checkbox"/>	<input type="checkbox"/>	Multicast packet type and address added statically or learned through IGMP snooping.
Broadcast	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Broadcast address.
RSVM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	MAC control frame between 0x0180c2000000~0x0180c200002f.
MLF, DLF	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Multicast packet and address not added statically and not learned through IGMP snooping or source MAC.

Figure 29 Packet Types for Rate Control

The receiver classifies rate control into two types: service rate control and broadcast rate control. Each packet can be added to only one rate control type.

2. Configure port rate control, as shown in the following figure.

Port ID	Service	Broadcast	OutRate
FE1	0 Kbps	0 Kbps	0 Kbps
FE2	70 Kbps	80 Kbps	90 Kbps
FE3	0 Kbps	0 Kbps	0 Kbps
FE4	0 Kbps	0 Kbps	0 Kbps
FE5	0 Kbps	0 Kbps	0 Kbps
FE6	0 Kbps	0 Kbps	0 Kbps
FX7	0 Kbps	0 Kbps	0 Kbps
FX8	0 Kbps	0 Kbps	0 Kbps
GE1	0 Kbps	0 Kbps	0 Kbps
GE2	0 Kbps	0 Kbps	0 Kbps

Apply Help

Figure 30 Port Rate Control

### Service/Broadcast

Range: 64~1000000Kbps

Function: Configure rate control for packets on the port. Packets whose rate is higher than the specified value are discarded.

Description: The ingress rate for a 100M port ranges from 64 to 100000Kbps.

The ingress rate for a 1000M port ranges from 64 to 100000Kbps.

### OutRate

Range: 64~1000000Kbps

Function: Limit the rate of packets forwarded by a port.

Description: The egress rate for a 100M port ranges from 64 to 100000Kbps.

The ingress rate for a 1000M port ranges from 64 to 100000Kbps.

**Caution:**

If a rate value is set to 0, rate control is disabled on the port.

---

### 6.1.3 Typical Configuration Example

Set the rate threshold of reserved multicast, unknown multicast, and unicast packets on port 2 to 70Kbps, broadcast packets to 80Kbps, and outgoing rate to 90Kbps.

Configuration steps:

1. Select reserved multicast, unknown multicast, and unicast packets in the Service column, and broadcast packets in the Broadcast column, as shown in Figure 29.
2. On port 2, set the service rate threshold to 70Kbps, broadcast rate threshold to 80Kbps, and outgoing rate to 90Kbps, as shown in Figure 30.

## 6.2 VLAN

### 6.2.1 Overview

One LAN can be divided into multiple logical Virtual Local Area Networks (VLANs). A device can only communicate with the devices on the same VLAN. As a result, broadcast packets are restricted to a VLAN, optimizing LAN security.

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

### 6.2.2 Principle

To enable network devices to distinguish packets from different VLANs, fields for identifying VLANs need to be added to packets. At present, the most commonly used protocol for VLAN identification is IEEE802.1Q. The following

table shows the structure of an 802.1Q frame.

Table 4 802.1Q Frame Structure

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

A 4-byte 802.1Q header, as the VLAN tag, is added to the traditional Ethernet data frame.

Type: 16 bits. It is used to identify a data frame carrying a VLAN tag. The value is 0x8100.

PRI: three bits, identifying the 802.1p priority of a packet.

CFI: one bit. 0 indicates Ethernet, and 1 indicates token ring.

VID: 12 bits, indicating the VLAN number. The value ranges from 1 to 4093. 0, 4094, and 4095 are reserved values.



**Note:**

- VLAN 1 is the default VLAN and cannot be manually created and deleted.
- Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and deleted.

The packet containing 802.1Q header is a tagged packet; the one without 802.1Q header is an untagged packet. All packets carry an 802.1Q tag in the switch.

### 6.2.3 Port-based VLAN

VLAN partition can be either port-based or MAC address-based. This series switches support port-based VLAN partition. VLAN members can be defined based on switch ports. After a port is added to a specified VLAN, the port can forward the packets with the tag for the VLAN.

## 1.Port Type

Ports fall into two types according to how they handle VLAN tags when they forward packets.

- **Untag port:** Packets forwarded by an Untag port do not have VLAN tags. Untag ports are usually used to connect to terminals that do not support 802.1Q. By default, all switch ports are Untag ports and belong to VLAN1.
- **Tag port:** All packets forwarded by a Tag port carry a VLAN tag. Tag ports are usually used to connect network transmission devices.

## 2.PVID

Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID.

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

The following table shows how the switch processes received and forwarded packets according to the port type and PVID.

Table 5 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 untagged packets.	<ul style="list-style-type: none"> <li>➤ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the packet.</li> <li>➤ If the VLAN ID in a packet is not in the list of VLANs allowed through,</li> </ul>	Untag	Forward the packet after removing the tag.
		Tag	Keep the tag and forward the packet.

	discard the packet.		
--	---------------------	--	--

## 6.2.4 Web Configuration

1. Configure the VLAN transparent transmission mode, as shown in the following figure.

Ingress VLAN Filter : Nonmember Drop ▼ Untagged Port VLAN List

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

Apply Add Help

Figure 31 Configuring VLAN Transparent Transmission Mode

### Ingress VLAN Filter

Options: Nonmember Drop/Nonmember Forward

Default: Nonmember Drop

Function: Configure the VLAN transparent transmission mode.

Description: The transparent transmission mode indicates whether the switch checks incoming packets on a port. If Nonmember Drop is selected, a packet is discarded when the VLAN tag of the packet is different from the VLAN of the port. If Nonmember Forward is selected, a packet is accepted when the VLAN tag of the packet is identical with that of any other connected port on the switch; otherwise, the packet is discarded.

2. Create a VLAN.

Click <Add> in Figure 31 to create a VLAN. As shown in the following figure, select the ports to be added to the VLAN and set port parameters.

VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
FE1	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
FE2	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
FE3	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
FE4	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
FE5	<input type="text" value="Tagged"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
FE6	<input type="text" value="Untagged"/> ▾	<input type="text" value="1"/> ▾	<input type="text" value="Disable"/> ▾
FX7	<input type="text" value="Untagged"/> ▾	<input type="text" value="4"/> ▾	<input type="text" value="Disable"/> ▾
FX8	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
GE1	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾
GE2	<input type="text" value="-----"/> ▾	<input type="text" value="0"/> ▾	<input type="text" value="Disable"/> ▾

Figure 32 VLAN Configuration

**VLAN Name**

Range: 1~31 characters

Function: Set the VLAN name.

**VLAN ID**

Range: 2~4093

Function: Configure the VLAN ID.

Description: VLAN ID is used to distinguish different VLANs. This series switches support a maximum of 256 VLANs.

**VLAN Member**

Options: Tagged/Untagged

Function: Select the type of the port in the VLAN.

**Priority**

Range: 0~7

Default: 0

Function: Set the default priority of the port. When adding an 802.1Q tag to an

untagged packet, the value of the PRI field is the priority.

## PVLAN

Options: Enable/Disable

Default: Disable

Function: To add a Tag port to a VLAN, you need to enable or disable PVLAN.

For details about PVLAN, see the next chapter.



### Caution:

An Untag port can be added to only one VLAN. The VLAN ID is the PVID of the port. The default value is 1. A Tag port can be added to multiple VLANs.

3. View the VLAN list, as shown in the following figure.

Ingress VLAN Filter: Nonmember Drop ▼ Untagged Port VLAN List

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

Apply Add Help

Figure 33 Viewing VLAN List

## PVLAN List

Options: Select/Deselect

Function: Enable or disable the PVLAN function. For details, see the next chapter.

4. View the PVIDs of ports.

Click <Untagged Port VLAN List> in Figure 33. The following page is displayed.

Port ID	VLAN ID
FE1	1
FE2	1
FE3	1
FE4	1
FE5	1
FE6	2
FX7	2
FX8	1
GE1	1
GE2	1

Figure 34 Port PVID List



**Caution:**

Each port must have an Untag attribute. If it is not set, the Untag port is in VLAN 1 by default.

---

5. Modify/Delete VLAN.

Click a VLAN list in Figure 33. You can modify or delete a created VLAN. Click <Delete> at the bottom. You can delete a VLAN directly, as shown in the following figure.

VLAN Name :

VLAN ID :

Port ID	VLAN Member	Priority	PVLAN
FE1	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
FE2	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
FE3	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
FE4	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
FE5	<input type="text" value="Tagged"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
FE6	<input type="text" value="Untagged"/> ▼	<input type="text" value="1"/> ▼	<input type="text" value="Disable"/> ▼
FX7	<input type="text" value="Untagged"/> ▼	<input type="text" value="4"/> ▼	<input type="text" value="Disable"/> ▼
FX8	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
GE1	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼
GE2	<input type="text" value="-----"/> ▼	<input type="text" value="0"/> ▼	<input type="text" value="Disable"/> ▼

Figure 35 Modifying/Deleting a created VLAN

### 6.2.5 Typical Configuration Example

As shown in the following figure, the entire LAN is divided into 3 VLANs: VLAN2, VLAN100 and VLAN200. 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 packets, so the ports on connecting Switch A and Switch B with PCs are set to Untag port. VLAN2, VLAN100 and VLAN200 packets need to be transmitted between Switch A and Switch B, so the ports connecting Switch A and Switch B should be set to Tag ports, permitting the packets of VLAN 2, VLAN 100 and VLAN 200 to pass through. The following table shows specific configuration.

Table 6 VLAN Configuration

Item	Configuration
VLAN2	Set port 1 and port 2 of Switch A and B to Untag ports, and port 7 to Tag

	port.
VLAN100	Set port 3 and port 4 of Switch A and B to Untag ports, and port 7 to Tag port.
VLAN200	Set port 5 and port 6 of Switch A and B to Untag ports, and port 7 to Tag port.

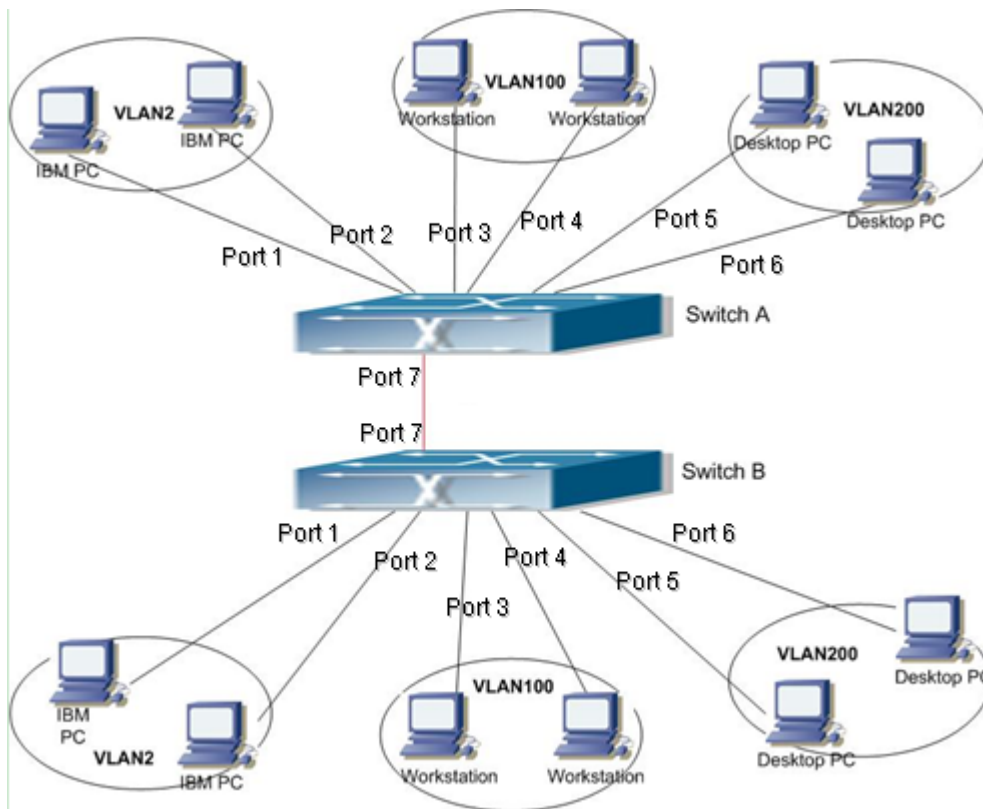


Figure 36 VLAN Application

**Configurations on Switch A and Switch B:**

1. Create VLAN 2, add port 1 and port 2 to VLAN 2 as Untag ports, and add port 7 into VLAN 2 as Tag port, as shown in Figure 32.
2. Create VLAN 100, add port 3 and port 4 to VLAN 100 as Untag ports, and add port 7 into VLAN 100 as Tag port, as shown in Figure 32.
3. Create VLAN 200, add port 5 and port 6 into VLAN 200 as Untag ports, and add port 7 into VLAN 200 as Tag port, as shown in Figure 32.

## 6.3 PVLAN

### 6.3.1 Overview

Private VLAN (PVLAN) 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 with each other.

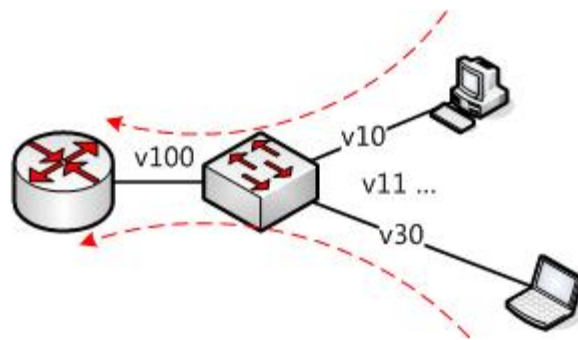


Figure 37 PVLAN Application

As shown in the preceding figure, 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.

### 6.3.2 Web Configuration

1. Enable PVLAN on the port, as shown in the following figure.

VLAN Name:

VLAN ID:

Port ID	VLAN Member	Priority	PVLAN
FE1	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Enable"/>
FE2	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Enable"/>
FE3	<input type="text" value="Untagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE4	<input type="text" value="Untagged"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
FE5	<input type="text" value="Tagged"/>	<input type="text" value="0"/>	<input type="text" value="Enable"/>
FE6	<input type="text" value="Tagged"/>	<input type="text" value="1"/>	<input type="text" value="Enable"/>
FX7	<input type="text" value="-----"/>	<input type="text" value="4"/>	<input type="text" value="Disable"/>
FX8	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
GE1	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>
GE2	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="Disable"/>

Figure 38 Enabling PVLAN

You can enable PVLAN on a Tag port in VLAN.

If the VLAN is a shared domain, the uplink port is an Untag port and the downlink port shall be added to the VLAN as a Tag port.

If the VLAN is an isolation domain, the downlink port is an Untag port and the uplink port shall be added to the VLAN as a Tag port.

2. Select the member VLANs of PVLAN, as shown in the following figure.

Ingress VLAN Filter:

Untagged Port VLAN List

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 39 Selecting PVLAN Members

**PVLAN List**

Options: Select/Deselect

Default: Deselect

Function: Select PVLAN members.

**Note:**

Both shared and isolation domains are member VLANs of PVLAN.

**6.3.3 Typical Configuration Example**

Figure 40 shows a 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.

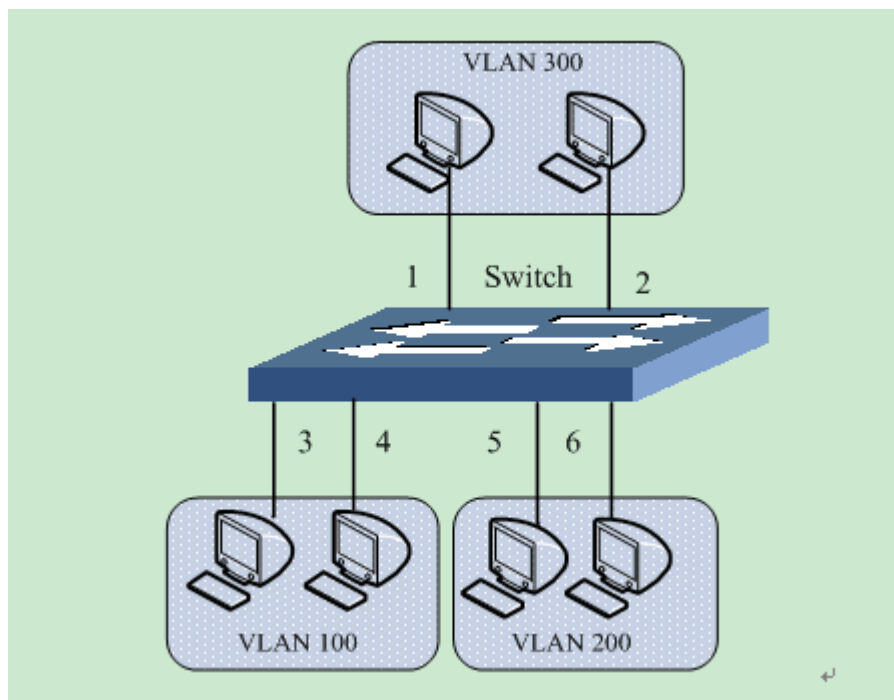


Figure 40 PVLAN Configuration Example

Configuration steps:

1. Configure the shared domain, VLAN 300, as shown in Figure 38.

Set port 1 and port 2 to Untag ports and add them to VLAN 300.

Set port 3 and port 4 to Tag ports and add them to VLAN 300. Enable PVLAN

on the two ports.

Set port 5 and port 6 to Tag ports and add them to VLAN 300. Enable PVLAN on the two ports.

2. Configure VLAN 100, an isolation domain, as shown in Figure 38.

Set port 1 and port 2 to Tag ports and add them to VLAN 100. Enable PVLAN on the two ports.

Set port 3 and port 4 to Untag ports and add them to VLAN 100.

3. Configure VLAN 200, an isolation domain, as shown in Figure 38.

Set port 1 and port 2 to Tag ports and add them to VLAN 200. Enable PVLAN on the two ports.

Set port 5 and port 6 to Untag ports and add them to VLAN 200.

4. Set VLAN300, VLAN100 and VLAN200 to PVLAN members, as shown in Figure 39.

## 6.4 Port Mirroring

### 6.4.1 Overview

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

### 6.4.2 Description

A switch supports only one mirroring destination port but multiple source ports. Multiple source ports can be either in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

The source port and destination port cannot be the same port.



#### **Caution:**

➤ Port mirroring and Port Trunk are mutually exclusive. The mirroring

---

---

source/destination port cannot be added into a Trunk group, while the ports added to a Trunk group cannot be set to a mirroring destination/source port.

- Port mirroring and port redundancy are mutually exclusive. The mirroring destination/source port cannot be set to a redundant port, while the redundant port cannot be set to a mirroring source/destination port.
- 

### 6.4.3 Web Configuration

1. Select the mirroring destination port, as shown in the following figure.



Figure 41 Selecting a Mirroring Port

#### Mirroring Port

Options: Disable/A switch port

Default: Disable

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

2. Select mirroring source ports and the mirroring mode, as shown in the following figure.

Mirrored Port	Mode
<input type="checkbox"/> FE1	RX
<input type="checkbox"/> FE2	RX
<input checked="" type="checkbox"/> FE3	RX
<input type="checkbox"/> FE4	RX
<input checked="" type="checkbox"/> FE5	TX
<input checked="" type="checkbox"/> FE6	RX & TX
<input type="checkbox"/> FX7	RX
<input type="checkbox"/> FX8	RX
<input type="checkbox"/> GE1	RX
<input type="checkbox"/> GE2	RX

Figure 42 Mirroring Source Port

**Mode**

Options: RX/TX/RX&amp;TX

Function: Select the data to be mirrored.

TX indicates only the transmitted packets are mirrored in the source port.

RX indicates only the received packets are mirrored in the source port.

TX&amp;RX indicates both transmitted and received packets are mirrored in the source port.

**6.4.4 Typical Configuration Example**

As shown in the following figure, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

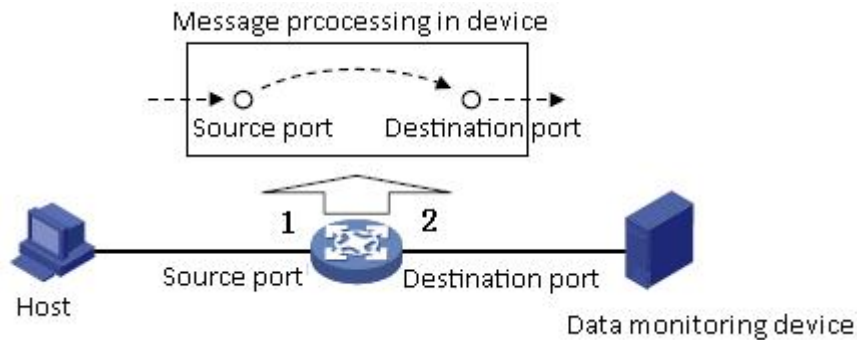


Figure 43 Port Mirroring Example

Configuration steps:

1. Set port 2 to the mirroring destination port, as shown in Figure 41.
2. Set port 1 to the mirroring source port and the port mirroring mode to TX&RX, as shown in Figure 42.

## 6.5 Port Trunk

### 6.5.1 Overview

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 can not only share the load, but also become a dynamic backup for each other to enhance connection reliability.

### 6.5.2 Implementation

As shown in the following figure, three ports in Switch A aggregate to a trunk group and the bandwidth of the trunk group is the total bandwidth of three ports.

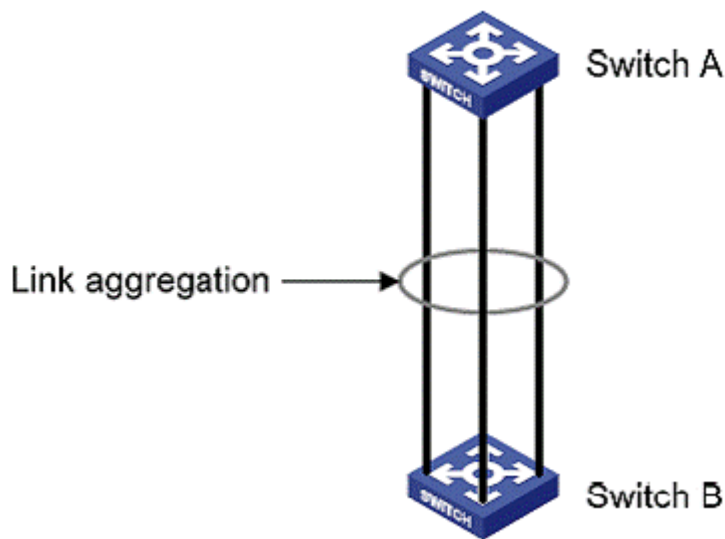


Figure 44 Port Trunk

If Switch A sends packets to Switch B by way of the aggregated link, Switch A determines the member port for transmitting the traffic based on the calculation result of load sharing. When one member port of the aggregated link fails, the traffic transmitted through the port is taken over by another normal port based on traffic sharing algorithm.

### 6.5.3 Description

Port trunk and the following port operations are mutually exclusive:

- Port trunk is mutually exclusive with port redundancy. A port added to a trunk group cannot be configured as a redundant port, while a redundant port cannot be added to a trunk group.
- Port trunk is mutually exclusive with port mirroring. A port added to a trunk group cannot be configured as a mirroring destination/source port.

In addition, the following operations are not recommended.

- Enable GMRP on a trunk port.
- Add a GMRP-enabled port to a trunk group.
- Add a trunk port to a static unicast/multicast entry.
- Add a port in a static unicast/multicast entry to a trunk group.

**Caution:**

- Gigabit ports of the series switches do not support port trunk.
- A port can be added to only one trunk group.

## 6.5.4 Web Configuration

### 1. Add Port Trunk.

Click <Add> to add a trunk group, as shown in the following figure.

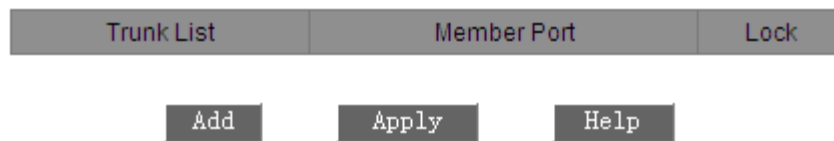


Figure 45 Adding a Trunk Group

### 2. Configure the trunk group, as shown in the following figure.

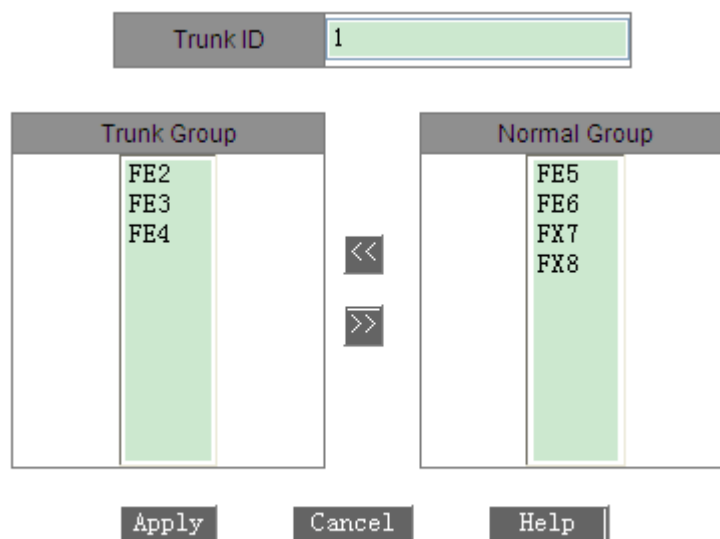


Figure 46 Configuring the Trunk Group

#### Trunk ID

Range: 1~2

Function: Set the trunk group ID.

Description: The series switches support a maximum of 2 trunk groups. Each

group can contain a maximum of 4 ports.

3. View trunk group list, as shown in the following figure.

Trunk List	Member Port	Lock
trunk--1	FE2 FE3 FE4	<input type="checkbox"/>
trunk--2	FE5 FE6	<input type="checkbox"/>

Figure 47 Trunk Group List

### Lock

Lock the member ports of a trunk group. After locked member ports are deleted from a trunk group, you must enable the ports manually to unlock the ports.

Click a trunk group in Figure 47. You can modify or delete the trunk group, as shown in the following figure.

Trunk ID

Trunk Group	Normal Group
FE2 FE3 FE4	FX7 FX8

Figure 48 Modifying/Deleting a Trunk Group

After modifying group member settings (add a new port to the group or delete a port member from the group), click <Apply> to make the modification take effect. If you click <Delete>, you can delete the group.

## 6.5.5 Typical Configuration Example

As shown in Figure 44, port 2, port 3, and port 4 of Switch A are connected to those of Switch B respectively, forming trunk group 1 to achieve load balancing among ports.

Configuration steps:

1. Create trunk group 1 on Switch A and add port 2, port 3, and port 4 to the group, as shown in Figure 46.
2. Create trunk group 1 on Switch B and add port 2, port 3, and port 4 to the group, as shown in Figure 46.

## 6.6 Link Check

### 6.6.1 Overview

Link Check detects the data transmission of redundancy protocol (STP/RSTP/DT-Ring)-enabled ports. When a fault occurs, link check helps to detect the anomaly for timely processing.

### 6.6.2 Web Configuration

The following figure shows the link check configuration.

Link Check			
Port	Administration Status		Run Status
FE1	Enable	▼	Receive Fault
FE2	Enable	▼	Receive Fault
FE3	Enable	▼	Receive Fault
FE4	Enable	▼	Normal Link
FE5	Enable	▼	Receive Fault
FE6	Enable	▼	Receive Fault
FX7	Enable	▼	Receive Fault
FX8	Disable	▼	Disable
GX1	Enable	▼	Receive Fault
GX2	Disable	▼	Disable

Apply

Figure 49 Link Check Configuration

## Administration Status

Options: Enable/Disable

Default: Enable

Description: 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

Options: Normal Link/Receive Fault/Disable/Send Fault

Description: If Link Check is enabled on a ring 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.

## 6.7 Static Multicast

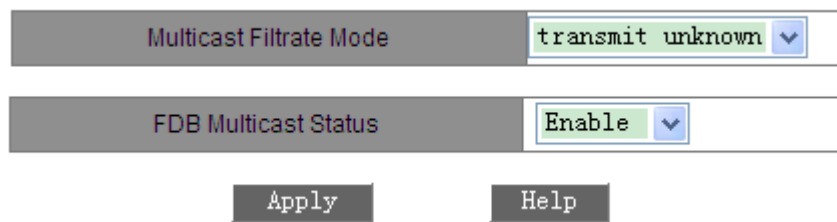
### 6.7.1 Overview

You can configure the static multicast address table. You can add an entry to the table in <multicast MAC address, VLAN ID, multicast member port> format. When receiving multicast packets, the switch searches the table for the corresponding member port to forward the packets.

The device supports up to 256 multicast entries.

### 6.7.2 Web Configuration

1. Enable static multicast, as shown in the following figure.



Multicast Filtrate Mode: transmit unknown ▼

FDB Multicast Status: Enable ▼

Apply Help

Figure 50 Enabling Static Multicast

**Multicast Filtrate Mode**

Options: transmit unknown/drop unknown

Default: transmit unknown

Function: Configure the processing mode for unknown multicast packets.

Description: Unknown multicast packets are packets not manually added or learned through IGMP Snooping and GMRP

transmit unknown indicates unknown multicast packets are broadcasted in the corresponding VLANs; drop unknown indicates unknown multicast packets are discarded.

**FDB Multicast Status**

Options: Enable/Disable

Default: Disable

Function: Enable or disable static multicast. Static multicast and IGMP Snooping cannot be enabled at the same time.

2. Add a static multicast entry, as shown in the following figure.

**Static FDB Multicast List Configuration**

MAC	010101010101
VLAN ID	1 (1-4093)

**Port List**

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2" style="background-color: #cccccc;">Member Port List</th> </tr> <tr> <td style="width: 30%;"></td> <td style="width: 70%;"> <div style="background-color: #d9ead3; padding: 2px;">FE1</div> <div style="background-color: #d9ead3; padding: 2px;">FE3</div> <div style="background-color: #d9ead3; padding: 2px;">FE5</div> </td> </tr> </table>	Member Port List			<div style="background-color: #d9ead3; padding: 2px;">FE1</div> <div style="background-color: #d9ead3; padding: 2px;">FE3</div> <div style="background-color: #d9ead3; padding: 2px;">FE5</div>	<div style="background-color: #cccccc; padding: 5px; margin: 5px 0;">&lt;&lt;</div> <div style="background-color: #cccccc; padding: 5px; margin: 5px 0;">&gt;&gt;</div>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2" style="background-color: #cccccc;">Source Port List</th> </tr> <tr> <td style="width: 30%;"></td> <td style="width: 70%;"> <div style="background-color: #d9ead3; padding: 2px;">FE2</div> <div style="background-color: #d9ead3; padding: 2px;">FE4</div> <div style="background-color: #d9ead3; padding: 2px;">FE6</div> <div style="background-color: #d9ead3; padding: 2px;">FX7</div> <div style="background-color: #d9ead3; padding: 2px;">FX8</div> <div style="background-color: #d9ead3; padding: 2px;">GE1</div> <div style="background-color: #d9ead3; padding: 2px;">GE2</div> </td> </tr> </table>	Source Port List			<div style="background-color: #d9ead3; padding: 2px;">FE2</div> <div style="background-color: #d9ead3; padding: 2px;">FE4</div> <div style="background-color: #d9ead3; padding: 2px;">FE6</div> <div style="background-color: #d9ead3; padding: 2px;">FX7</div> <div style="background-color: #d9ead3; padding: 2px;">FX8</div> <div style="background-color: #d9ead3; padding: 2px;">GE1</div> <div style="background-color: #d9ead3; padding: 2px;">GE2</div>
Member Port List										
	<div style="background-color: #d9ead3; padding: 2px;">FE1</div> <div style="background-color: #d9ead3; padding: 2px;">FE3</div> <div style="background-color: #d9ead3; padding: 2px;">FE5</div>									
Source Port List										
	<div style="background-color: #d9ead3; padding: 2px;">FE2</div> <div style="background-color: #d9ead3; padding: 2px;">FE4</div> <div style="background-color: #d9ead3; padding: 2px;">FE6</div> <div style="background-color: #d9ead3; padding: 2px;">FX7</div> <div style="background-color: #d9ead3; padding: 2px;">FX8</div> <div style="background-color: #d9ead3; padding: 2px;">GE1</div> <div style="background-color: #d9ead3; padding: 2px;">GE2</div>									

Apply
Cancel

Figure 51 Adding a Static Multicast Entry

**MAC**

Portfolio: HHHHHHHHHHHH (H is a hexadecimal number.)

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

**VLAN ID**

Options: All existing VLANs

Function: Set the VLAN ID of the entry. Only the member ports of the VLAN can forward the multicast packets.

**Member Port List**

Select member ports for the multicast address. If hosts connected to a port need to receive the packets from a multicast address, you can configure the port as the member port of the multicast address.

3. View, modify, or delete a static multicast entry, as shown in the following figure.

**Static FDB Multicast List**

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	01-01-01-01-01-01	1	FE1 FE3 FE5
<input type="radio"/>	01-02-02-02-02-02	2	FE2 FE4 FE6

Figure 52 Operations on a Static Multicast Entry

The static multicast address list contains the MAC address, VLAN ID, and member port. To delete an entry, select the entry and click <Delete>. To modify an entry, select the entry and click <Modify>.

## 6.8 IGMP Snooping

### 6.8.1 Overview

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast protocol at the data link layer. It is used for managing and controlling multicast groups. IGMP Snooping-enabled switches analyze received IGMP packets, establish mapping between ports and MAC multicast addresses, and forward multicast packets according to the mapping.

### 6.8.2 Concepts

- Querier: periodically sends IGMP general query packets to query the status of the members in the multicast group, maintaining the multicast group information. When multiple queriers exist on a network, they automatically elect the one with the smallest IP address to be the querier. Only the elected querier periodically sends IGMP general query packets. The other queriers only receive and forward IGMP query packets.
- Router port: receives general query packets (on an IGMP-enabled switch) from the querier. Upon receiving an IGMP report, a switch establishes a multicast entry and adds the port that receives the IGMP report to the member port list. If a router port exists, it is also added to the member port

list. Then the switch forwards the IGMP report to other devices through the router port, so that the other devices establish the same multicast entry.

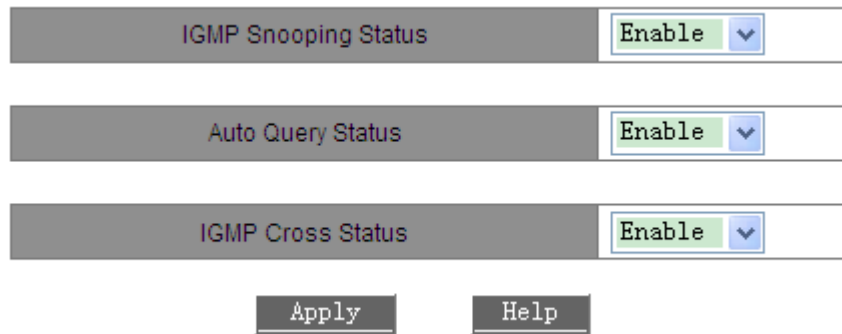
### **6.8.3 Principle**

IGMP Snooping manages and maintains multicast group members by exchanging related packets among IGMP-enabled devices. The related packets are as follows:

- General query packet: The querier periodically sends general query packets (destination IP address: 224.0.0.1) to confirm whether the multicast group has member ports. After receiving the query packet, a non-querier device forwards the packet to all its connected ports.
- Specific query packet: If a device wants to leave a multicast group, it sends an IGMP leave packet. After receiving the leave packet, the querier sends a specific query packet (destination IP address: IP address of the multicast group) to confirm whether the group contains other member ports.
- Membership report packet: If a device wants to receive the data of a multicast group, the device sends an IGMP report packet (destination IP address: IP address of the multicast group) immediately to respond to the IGMP query packet of the group.
- Leave packet: If a device wants to leave a multicast group, the device will send an IGMP leave packet (destination IP address: 224.0.0.2).

### **6.8.4 Web Configuration**

1. Enable IGMP Snooping, as shown in the following figure.



The screenshot shows a web interface with three rows of settings. Each row has a label on the left and a dropdown menu on the right. The first row is 'IGMP Snooping Status' with a dropdown set to 'Enable'. The second row is 'Auto Query Status' with a dropdown set to 'Enable'. The third row is 'IGMP Cross Status' with a dropdown set to 'Enable'. Below these rows are two buttons: 'Apply' and 'Help'.

Figure 53 Enabling IGMP Snooping

### IGMP Snooping Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable IGMP Snooping. IGMP Snooping and static multicast/GMRP cannot be enabled at the same time.

### Auto Query Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable auto query for querier election.

Description: The auto query function can be enabled only if IGMP Snooping is enabled.



#### Caution:

On a network, the auto query function shall be enabled on one switch at least.

### 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. View the multicast member list, as shown in the following figure.

IGMP Member List		
MAC	VLAN ID	Member
01-00-5E-00-01-01	1	FE5
01-00-5E-7F-FF-FE	1	FE5
01-00-5E-51-09-08	1	FE5
01-00-5E-0A-18-03	1	FE4 FE5
01-00-5E-7F-FF-FA	1	FE4 FE5

Figure 54 IGMP Snooping Member List

### IGMP Member List

Combination: {MAC address, VLAN ID, member port}

In the FDB multicast table dynamically learned through IGMP Snooping, the VLAN ID is the VLAN ID of member ports.

### 6.8.5 Typical Configuration Example

As shown in the following figure, IGMP Snooping is enabled on Switch 1, Switch 2, and Switch 3. Auto query is enabled on Switch 2 and Switch 3. The IP address of Switch 2 is 192.168.1.2 and that of Switch 3 is 192.168.0.2. Therefore, Switch 3 is elected as the querier.

1. Enable IGMP Snooping on Switch 1.
2. Enable IGMP Snooping and auto query on Switch 2.
3. Enable IGMP Snooping and auto query on Switch 3.

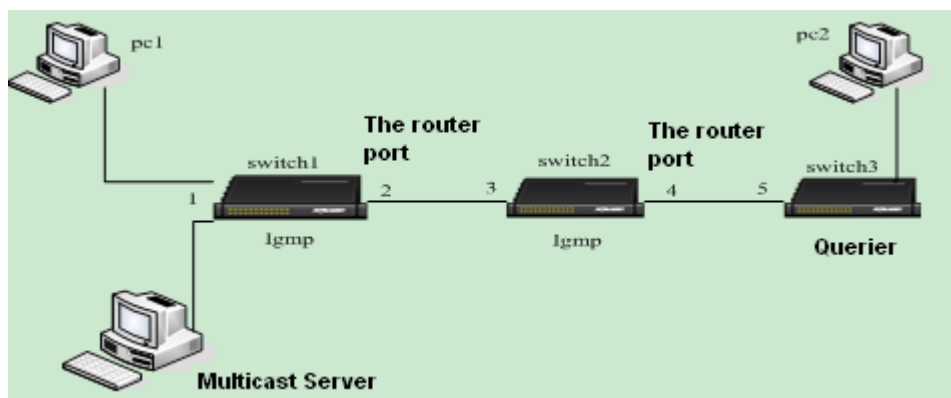


Figure 55 IGMP Snooping Configuration Example

- As the querier, Switch 3 periodically sends general query packets. Port 4 of

Switch 2 receives the packets and is thus elected as the routing port. Meanwhile, Switch 2 forwards the packets through port 3. Then port 2 of Switch 1 receives the packets and is thus elected as the routing port.

- When PC 1 is added to multicast group 225.1.1.1 and send IGMP report packets, port 1 and port 2 (routing port) of Switch 1 are added to multicast group 225.1.1.1. Meanwhile, IGMP report packets are forwarded to Switch 2 through port 2. Then port 3 and port 4 of Switch 2 are also added to multicast group 225.1.1.1. Switch 2 forwards the report packets to Switch 3 through port 4. As a result, port 5 of Switch 3 is also added to multicast group 225.1.1.1.
- When receiving multicast data, Switch 1 forwards the data to PC 1 through port 1. As port 2 is also a multicast group member, it also forwards multicast data. As the process proceeds, multicast data finally reaches port 5 of Switch 3 because no further receiver is available. If PC 2 is also added to multicast group 225.1.1.1, multicast data is also forwarded to PC 2.

## **6.9 ACL**

### **6.9.1 Overview**

With the Access Control List (ACL) function, the switch filters received packets according to the matched rules defined in the ACL, preventing illegitimate users' access and saving network resources.

### **6.9.2 Web Configuration**

1. Configure the ACL mode for ports, as shown in the following figure.

**Set Port ACL**

Port	Mode
FE1	Accept ▼
FE2	Reject ▼
FE3	None ▼
FE4	None ▼
FE5	None ▼
FE6	None ▼
FX7	None ▼
FX8	None ▼

Figure 56 ACL Mode Configuration

**Mode**

Options: None/Accept/Reject

Default: None

Function: Configure the ACL mode, that is, the processing mode towards matched packets.

2. Set parameters for the ACL entry, as shown in the following figure.

**Set Port ACL MAC**

Port	Configure MAC
FE1 ▼	000000010101

Figure 57 Configuring an ACL Entry

**Port**

Options: all switch ports

Function: Configure the port on which the ACL entry takes effect.

**Configure MAC**

Format: {HHHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure the source MAC address for the ACL entry.

Description: Each port supports a maximum of 24 ACL entries.

3. View the ACL.

**Port ACL MAC List**

Index	Port	MAC
<input type="radio"/>	FE1	00-00-00-01-01-01
<input type="radio"/>	FE2	00-00-00-02-02-02

Figure 58 ACL Entries

### 6.9.3 Typical Configuration Example

Port 1 accepts only the packets whose source MAC address is 00-00-00-01-01-01.

Configuration steps:

1. Select Accept for the ACL mode of port 1, as shown in Figure 56.
2. Set the source MAC address of ACL entry for port 1 to 00-00-00-01-01-01, as shown in Figure 57.

## 6.10 ARP

### 6.10.1 Overview

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

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

## 6.10.2 Description

ARP entries fall into dynamic and static ones.

Dynamic entries are generated and maintained based on the exchange of ARP packets. Dynamic entries can age out, be updated by a new ARP packet, or be overwritten by a static ARP entry.

Static entries are manually configured and maintained. They never age out or are overwritten by dynamic ARP entries.

The switch supports up to 512 ARP entries (256 static ones at most). When the number of ARP entries is larger than 512, new entries automatically overwrite old dynamic ones.

## 6.10.3 Web Configuration

1. Configure ARP aging time, as shown in the following figure.

**ARP Aging Time**

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

Apply
Help

Figure 59 Configuring Aging Time

### ARP Aging Time

Range: 10~60 minutes

Default: 20 minutes

Function: Configure ARP aging time.

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

2. Add a static ARP entry, as shown in the following figure.

**ARP address**

IP address	192.168.0.12
MAC address	ea2347838495

Apply
Help

Figure 60 Adding a Static ARP Entry

**ARP address**

Portfolio: {IP address, MAC address}

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

Function: Configure static ARP entry.

**Caution:**

- The IP address of a static ARP entry must be on the same network segment with the IP address of the switch.
- If the IP address of a static entry is the IP address of the switch, the system automatically maps the IP address to the MAC address of the switch.
- In general, the switch automatically learns ARP entries. Manual configuration is not required.

3. View or delete an ARP entry, as shown in the following figure.

**ARP address**

Number	IP address	MAC address	Flags
<input type="radio"/>	192.168.0.11	00-1E-CD-17-97-14	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

Add Delete Help

Figure 61 ARP Address Table

**ARP Address**

Portfolio: {IP address, MAC address, flag}

Function: Display ARP entries, including static and dynamic ones.

Operation: Select a static entry in the Number column. Click <Delete>. You can delete the entry.

**Caution:**

You cannot delete dynamic ARP entries.

---

## 6.11 SNMP

### 6.11.1 Overview

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

### 6.11.2 Implementation

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

- The Network Management Station (NMS) is a station running SNMP-enabled network management software client. It is the core for the network management of an SNMP network.
- Agent is a process in the managed network devices. It receives and processes request packets from the NMS. When an alarm occurs, the agent proactively reports it to the NMS.

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

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

The NMS sends Get-Request, Get-Next-Request, and Set-Request packets to

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

### 6.11.3 Description

This series switches support SNMPv2. SNMPv2 is compatible with SNMPv1. SNMPv1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the community name carried by an SNMP packet is not acknowledged by the switch, the packet is discarded.

SNMPv2 also uses community name for authentication. It is compatible with SNMPv1, and extends the functions of SNMPv1.

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

### 6.11.4 MIB

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



Figure 62 Relationship among NMS, Agent, and MIB

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

has a unique Object Identifier (OID), which indicates the location of the node in the MIB structure. As shown in the following figure, the OID of object A is 1.2.1.1.

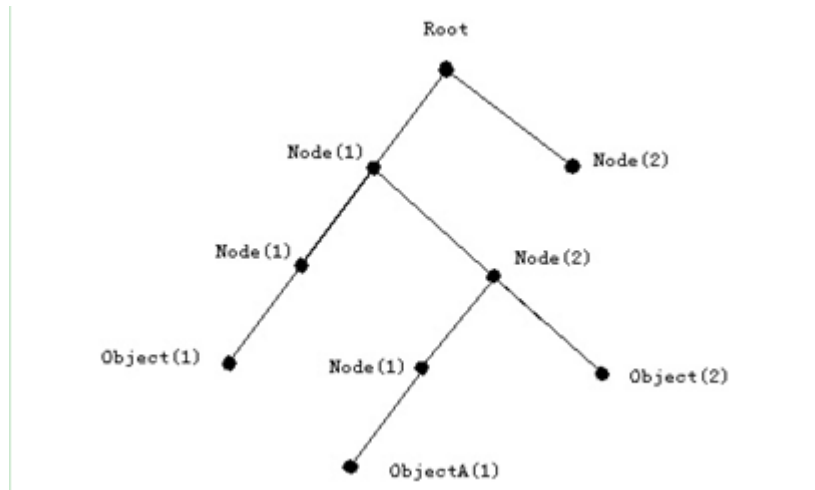


Figure 63 MIB Tree Structure

### 6.11.5 Web Configuration

1. Enable SNMP, as shown in the following figure.

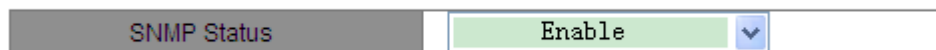


Figure 64 Enabling SNMP

#### SNMP Status

Options: Enable/Disable

Default: Enable

Function: Enable or disable SNMP.

2. Configure access rights, as shown in the following figure.

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

Figure 65 Access Rights Configuration

#### Read-Only Community

Range: 3~16 characters

Default: public

Function: Configure the name of read-only community.

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

### Read-Write Community

Range: 3~16 characters

Default: private

Function: Configure the name of read-write community.

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

### Request Port

Range: 1~65535

Default: 161

Function: Configure the number of the port for receiving SNMP requests.

3. Set trap parameters, as shown in the following figure.

**Trap Settings**

Trap on-off	<input type="text" value="Enable"/>
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 66 Trap Configuration

### Trap on-off

Options: Enable/Disable

Default: Enable

Function: Enable or disable trap sending.

### Trap Port ID

Options: 1~65535

Default: 162

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

### Server IP Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages. You can configure a maximum of five servers.

4. View the IP address of the management server, as shown in the following figure.

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

Figure 67 IP Address of Management Server

The IP address of management server does not need to be configured manually. The switch automatically displays it only if the NMS is running on the server and reads and writes the MIB node information of the device.

### 6.11.6 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. The NMS monitors and manages the Agent through SNMPv2, and reads and writes the MIB node information of the Agent. When the Agent is faulty, it proactively sends trap messages to the NMS, as shown in the following figure.

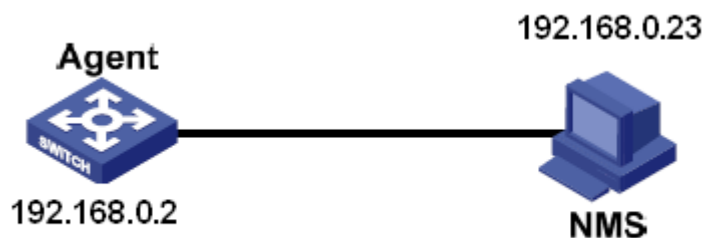


Figure 68 SNMPv2 Configuration Example

Configuration on the Agent:

1. Enable SNMP, as shown in Figure 64.
2. Configure access rights. Set read-only community name to public, read-write community name to private, and request port to 161, as shown in Figure 65.
3. Enable trap sending, set trap port number to 162, and IP address of server to 192.168.0.23, as shown in Figure 66.

To monitor and manage the status of the Agent, you need to run the management software, for example, Kyvision, on the NMS.

For operations on Kyvision, refer to the *Kyvision Operation Manual*.

## 6.12 DT-Ring

### 6.12.1 Overview

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-Ring fall into two types: port-based ring (DT-Port-Ring) and VLAN-based ring (DT-VLAN-Ring).

- DT-Port-Ring: specifies a port to forward or block packets.
- DT-VLAN-Ring: 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-Port-Ring and DT-VLAN-Ring cannot be used together.

### 6.12.2 Concepts

- Master station: One ring has only one master station. The master station sends DT-Ring packets and detects the current status of the ring.
- Master port: On the master station, the first port whose link status changes to up is called the master port. It is in forwarding state.
- Slave port: On the master station, the port whose link status changes to up later is called the slave port. When the ring is closed, the slave port is in blocking state. When a ring is open due to a link or port failure, the status of the slave port changes to forwarding.
- Slave station: A ring can include multiple slave stations. Slave stations listen to and forward DT-Ring packets and report fault information to the master station.
- Backup port: The port for communication between DT rings is called the backup port.
- Master Backup Port: When there are multiple backup ports in a ring, the master backup port is the backup port corresponding to a bigger device MAC address and it is in Forwarding state
- Slave Backup Port: When there are multiple backup ports in a ring, all the other ports (except the master backup port) are slave backup ports and they are in blocking state.
- Forwarding state: port can forward and receive data
- Blocking state: port can receive and forward only DT-Ring packets, but cannot receive or forward other data packets.

### 6.12.3 Implementation

#### 1. DT-Ring implementation

The master port on the master station periodically sends DT-Ring packets to detect ring status. If the slave port of the master station receives the packets, the ring is closed; otherwise, the ring is open.

When a ring is closed, the master port of the master station is in forwarding state, the slave port in blocking state, and all ring ports of slave stations are in forwarding state.

A ring may be open in the following cases:

- The master port of the master station fails. The statuses of the slave port on the master station and all ring ports of slave stations change to forwarding.
- The slave port of the master station fails. The statuses of the master port on the master station and all ring ports of slave stations change to forwarding.
- Another port or link fails. The statuses of the two ports of the master station and all up ports of slave stations change to forwarding.

DT-Ring configurations should meet the following conditions:

- All switches in the same ring must have the same domain number.
- Each ring can have only one master station and multiple slave stations.
- 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.
- DT-Port-Ring and DT-VLAN-Ring cannot be configured on one switch at the same time.

The following figure shows the working process of switch A, B, C, D.

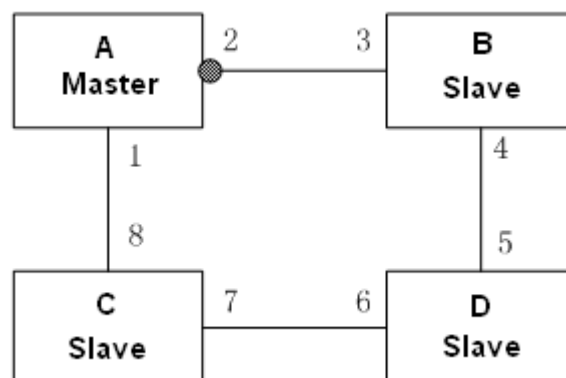


Figure 69 DT-Ring Topology

1. Configure Switch A as the master station, and others as slave stations.
2. Because Ring port 1 on the master station links up first, it is in

Forwarding state, and ring port 2 is in Blocking state. The two ring ports of each slave are in Forwarding state.

- When link CD (connecting Switch C to Switch D) fails, as shown in the following figure, port 2 switches to Forwarding state, and port 6 and port 7 are in Blocking state.

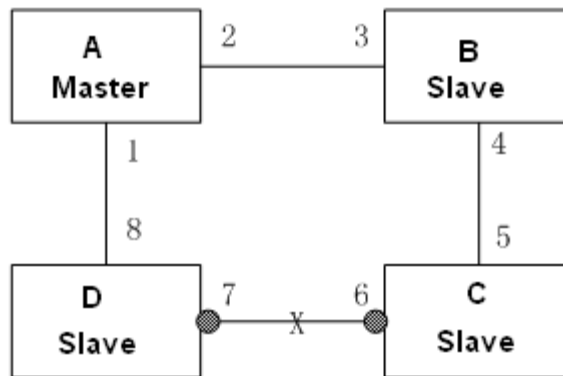


Figure 70 DT-Ring Link Fault



**Caution:**

The change in link status affects the roles and status of ring ports.

## 2. 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.

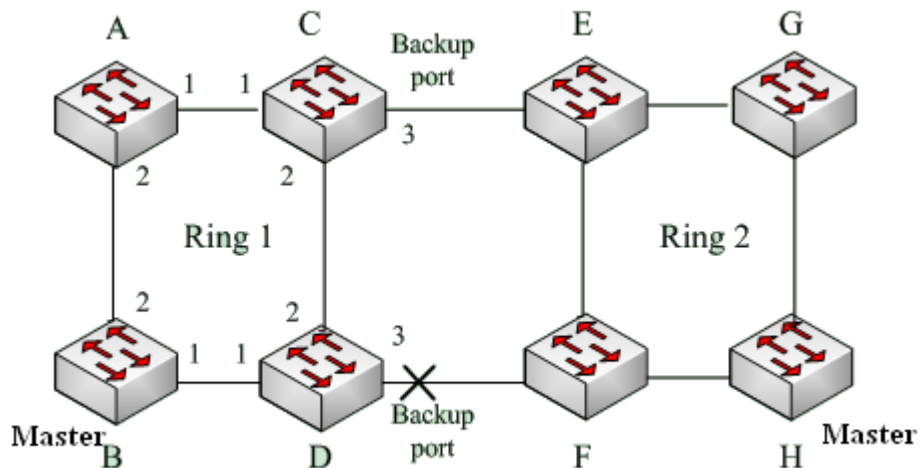


Figure 71 DT-Ring+ Topology

**Caution:**

The change in link status affects the status of backup ports.

### 3. DT-VLAN-Ring implementation

DT-VLAN-Ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-VLAN-Ring. Different DT-VLAN-Rings can have different master stations. As shown in the following figure, two DT-VLAN-Rings are configured.

Ring links of DT-VLAN-Ring10: AB-BC-CD-DE-EA

Ring links of DT-VLAN-Ring20: 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 VLAN.

Redundancy	DT-RING	
Domain ID	1	
Domain Name	a	
Station Type	Master	
Ring Port1	FE1	
Ring Port2	FE2	

DT-RING+		
DT-RING+	Enable	
Backup Port	FE3	

Add VLAN List		
VLAN Choose	VLAN ID	VLAN Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	2	vlan

Apply
Cannel
Help

Figure 72 DT-VLAN-Ring

#### 6.12.4 Web Configuration

1. Configure redundant ring mode and ring status detection, as shown in the following figure.

Select Redundancy Mode	DT-RING-PORT
Check Loop Status	Disable

Apply
Help

Figure 73 Redundant Ring Mode Configuration

##### Select Redundancy Mode

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

Default: DT-RING-PORT

Function: Select the redundancy mode.

##### Check Loop Status

Options: Disable/Enable

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 a DT ring, as shown in the following figure.

**DT-RING List**

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

Figure 74 Creating a DT Ring

Click <Add> and configure the DT ring.

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

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="FE1"/> ▼
Ring Port2	<input type="text" value="FE2"/> ▼

DT-RING+	
DT-RING+	<input type="text" value="Enable"/> ▼
Backup Port	<input type="text" value="FE3"/> ▼

Apply
Cancel
Help

Figure 75 DT-Ring Configuration

Redundancy	DT-RING	
Domain ID	1	
Domain Name	a	
Station Type	Master	
Ring Port1	FE1	
Ring Port2	FE2	

DT-RING+		
DT-RING+	Enable	
Backup Port	FE3	

Add VLAN List		
VLAN Choose	VLAN ID	VLAN Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	2	vlan

Apply	Cannel	Help
-------	--------	------

Figure 76 DT-VLAN-Ring Configuration

**Redundancy**

Forced configuration: DT-RING

**Domain ID**

Configuration rang: 1~32

Function: The domain ID is used to distinguish different rings. One switch supports a maximum of 16 port-based rings or 8 VLAN-based rings.

**Domain name**

Range: 1~31 characters

Function: Configure the domain name.

**Station Type**

Options: Master/Slave

Default: Master

Function: Select the switch role in a ring.

**Ring port 1/Ring port 2**

Options: all switch ports

Function: Select two ring ports.



**Caution:**

- Port trunk and ring are mutually exclusive. The port added to a trunk group cannot be configured as a ring port, and a ring port cannot be added to a trunk group.
- Port mirroring and port redundancy are mutually exclusive. The mirroring destination/source port cannot be set to a redundant port, while the redundant port cannot be set to a mirroring source/destination port.

### DT-Ring+

Options: Enable/Disable

Default: Disable

Function: Enable/disable DT-Ring+.

### Backup port

Options: all switch ports

Function: Set a port to backup port.

Explanation: Enable DT-Ring+ before setting backup port.

### Add VLAN list

Options: all created VLANs

Function: Select the VLANs for the ring port.

After setting is completed, DT-Ring List shows all created rings, as shown in the following figure.

DT-RING List

Domain ID	Station Type	Ring Port(1,2)	DT-RING+ Status	Backup Port	Change times
a-1	master	FE1,FE2	Enable	FE3	1
b-2	slave	FE4,FE5	Enable	FE6	0

Add

Help

Figure 77 DT-Ring List

## 4. View and modify DT-Ring configuration.

Click a DT-Ring entry in Figure 77 to show its ring configuration and modify it, as shown in the following figure.

**DT-RING Configuration**

Redundancy	DT-RING
Domain ID	1
Domain Name	a
Station Type	master
Ring Port1	FE1
Ring Port2	FE2
DT-RING+	Enable
Backup Port	FE3

Figure 78 DT-Ring Configuration

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

## 5. View DT-Ring and port status, as shown in the following figure.

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

Redundancy	DT-RING+
Equipment IP	192.168.0.22
Equipment MAC	00-0A-93-05-00-10
Backup Port Status	blocking
Equipment IP	192.168.1.22
Equipment MAC	00-11-22-33-44-44
Backup Port Status	blocking

Figure 79 DT-Ring State

### 6.12.5 Typical Configuration Example

As shown in Figure 71, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

#### Configuration on Switch A:

1. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 75.

#### Configuration on Switch B:

2. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 75.

#### Configuration on Switch C and Switch D:

3. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Enable; Backup port: port 3, as shown in Figure 75.

#### Configuration on Switch E, Switch F, and Switch G:

4. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 75.

#### Configuration on Switch H:

5. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 75.

## 6.13 RSTP/STP

### 6.13.1 Overview

Standardized in IEEE802.1D, the Spanning Tree Protocol (STP) is a LAN protocol used for preventing broadcast storms caused by link loops and providing link backup. STP-enabled devices exchange packets and block certain ports to prune "loops" into "trees", preventing proliferation and endless loops. The drawback of STP is that a port must wait for twice the forwarding

delay to transfer to the forwarding state.

To overcome the drawback, IEEE creates 802.1w standard to supplement 802.1D. IEEE 802.1w defines the Rapid Spanning Tree Protocol (RSTP). Compared with STP, RSTP achieves much more rapid convergence by adding alternate port and backup port for the root port and designated port respectively. When the root port is invalid, the alternate port can enter the forwarding state in no time.

### **6.13.2 Concepts**

- Root bridge: serves as the root for a tree. A network has only one root bridge. The root bridge changes with network topology. The root bridge periodically sends BPDU to the other devices, which forward the BPDU to ensure topology stability.
- Root port: indicates the best port for transmission from the non-root bridges to the root bridge. The best port is the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.
- Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.
- Alternate port: indicates the backup port of the root port. If the root port fails, the alternate port becomes the new root port.
- Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the new designated port and forwards data.

### **6.13.3 BPDU**

To prevent loops, all the bridges of a LAN calculate a spanning tree. The calculation process involves transmitting BPDUs among devices to determine the network topology. The following table shows the data structure of a BPDU.

Table 7 BPDU

...	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	...
...	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	...

Root bridge ID: priority of the root bridge (2 bytes)+MAC address of the root bridge (6 bytes).

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

Designated bridge ID: priority of the designated bridge (2 bytes)+MAC address of the designated bridge (6 bytes).

Designated port ID: port priority+port number.

Message age: duration that a BPDU can be spread in a network.

Max age: maximum duration that a BPDU can be saved on a device. When Message age is larger than Max age, the BPDU is discarded.

Hello time: interval for sending BPDUs.

Forward delay: status change delay (discarding--learning--forwarding).

#### 6.13.4 Implementation

The process for all bridges calculating the spanning tree with BPDUs is as follows:

1. In the initial phase, each port of all devices generates the BPDU with itself as the root bridge; both root bridge ID and designated bridge ID are the ID of the local device; the root path cost is 0; the designated port is the local port.
2. Best BPDU selection: All devices send their own BPDUs and receive BPDUs from other devices. Upon receiving a BPDU, each port compares the received BPDU with its own.
  - If the priority of its own BPDU is higher, the port does not perform any

operation.

- If the priority of the received BPDU is higher, the port replaces the local BPDU with the received one.

Devices compare the BPDUs of all ports and figure out the best BPDU.

Principles for comparing BPDUs are as follows:

- The BPDU with a smaller root bridge ID has a higher priority.
- If the root bridge IDs of two BPDUs are the same, their root path costs are compared. If the root path cost in a BPDU plus the path cost of the local port is smaller, the priority of the BPDU is higher.
- If the root path costs of two BPDUs are also the same, the designated bridge IDs, designated port IDs, and IDs of the port receiving the BPDUs are further compared in order. The BPDU with a smaller ID has a higher priority. The BPDU with a smaller root bridge ID has a higher priority.

3. Selection of the root bridge: The root bridge of the spanning tree is the bridge with the smallest bridge ID.

4. Selection of the root port: A non-root-bridge device selects the port receiving the best BPDU as the root port.

5. BPDU calculation of the designated port: Based on the BPDU of the root port and the path cost of the root port, a device calculates a designated port BPDU for each port as follows:

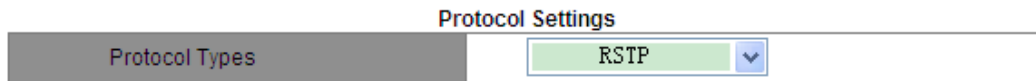
- Replace the root bridge ID with the root bridge ID of the BPDU of the root port.
- Replace the root path cost with the root path cost of the root port BPDU plus the path cost of the root port.
- Replace designated bridge ID with the ID of the local device.
- Replace the designated port ID with the ID of the local port.

6. Selection of the designated port: If the calculated BPDU is better, the device selects the port as the designated port, replaces the port BPDU with the calculated BPDU, and sends the calculated BPDU. If the port BPDU is better, the device does not update the port BPDU and blocks the port.

Blocked ports can receive and forward only RSTP packets, but not other packets.

### 6.13.5 Web Configuration

1. Enable STP/RSTP, as shown in the following figure.



The image shows a web configuration interface. At the top, there is a tab labeled 'Protocol Settings'. Below it, there is a section titled 'Protocol Types'. In this section, a dropdown menu is set to 'RSTP'.

Figure 80 Enabling RSTP/STP

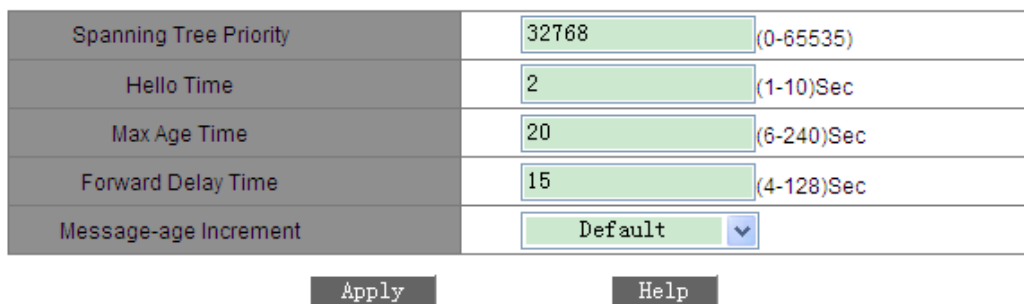
#### Protocol Types

Options: Disable/RSTP/STP

Default: Disable

Function: Disable or enable RSTP or STP.

2. Set the time parameters of the network bridge, as shown in the following figure.



Spanning Tree Priority	32768	(0-65535)
Hello Time	2	(1-10)Sec
Max Age Time	20	(6-240)Sec
Forward Delay Time	15	(4-128)Sec
Message-age Increment	Default	

Below the table, there are two buttons: 'Apply' and 'Help'.

Figure 81 Setting Time Parameters of the Network Bridge

#### Spanning Tree Priority

Range: 0~65535. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

#### Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

**Max Age Time**

Range: 6~240s

Default: 20s

Description: If the value of message age in the BPDU is larger than the specified value, the BPDU is discarded.

**Forward Delay Time**

Range: 4~128s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

**Message-age Increment**

Options: Compulsion/Default

Default: Default

Function: Configure the value to be added to message age when a BPDU passes through a network bridge.

Description: In compulsion mode, the value is 1.

In default mode, the value is  $\max(\max \text{ age time}/16, 1)$ .

Forward Delay Time, Max Age Time, and Hello Time shall meet the following requirements:

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

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

3. Enable RSTP on ports, as shown in the following figure.

Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
FE1	Enable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
FE2	Enable <input type="button" value="v"/>	128	2000000	No <input type="button" value="v"/>
FE3	Enable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
FE4	Enable <input type="button" value="v"/>	128	2000000	No <input type="button" value="v"/>
FE5	Disable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
FE6	Disable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
FX7	Disable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
FX8	Disable <input type="button" value="v"/>	128	2000000	Yes <input type="button" value="v"/>
GE1	Disable <input type="button" value="v"/>	128	200000	Yes <input type="button" value="v"/>
GE2	Disable <input type="button" value="v"/>	128	200000	Yes <input type="button" value="v"/>

Figure 82 Port Settings

**Protocol State**

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP on ports.

**Caution:**

- Port mirroring and STP are mutually exclusive. STP cannot be enabled on a mirroring source or destination port. An STP-enabled port cannot be configured as a mirroring source or destination port.
- Port Trunk and STP are mutually exclusive. STP cannot be enabled on a port added to a trunk group. An STP-enabled port cannot be added to a trunk group.

**Port Priority**

Range: 0~255. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

**Path Cost**

Range: 1~200000000

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

Description: The path cost of a port is used to calculate the best path. The value of the parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of this parameter. To configure the value manually, select No for Cost Count.

### Cost Count

Range: Yes/No

Default: Yes

Description: Yes indicates the path cost of the port adopts the default value. No indicates you can configure the path cost.

### 6.13.6 Typical Configuration Example

The priority of Switch A, B, and C are 0, 4096, and 8192. Path costs of links are 4, 5, and 10, as shown in the following figure.

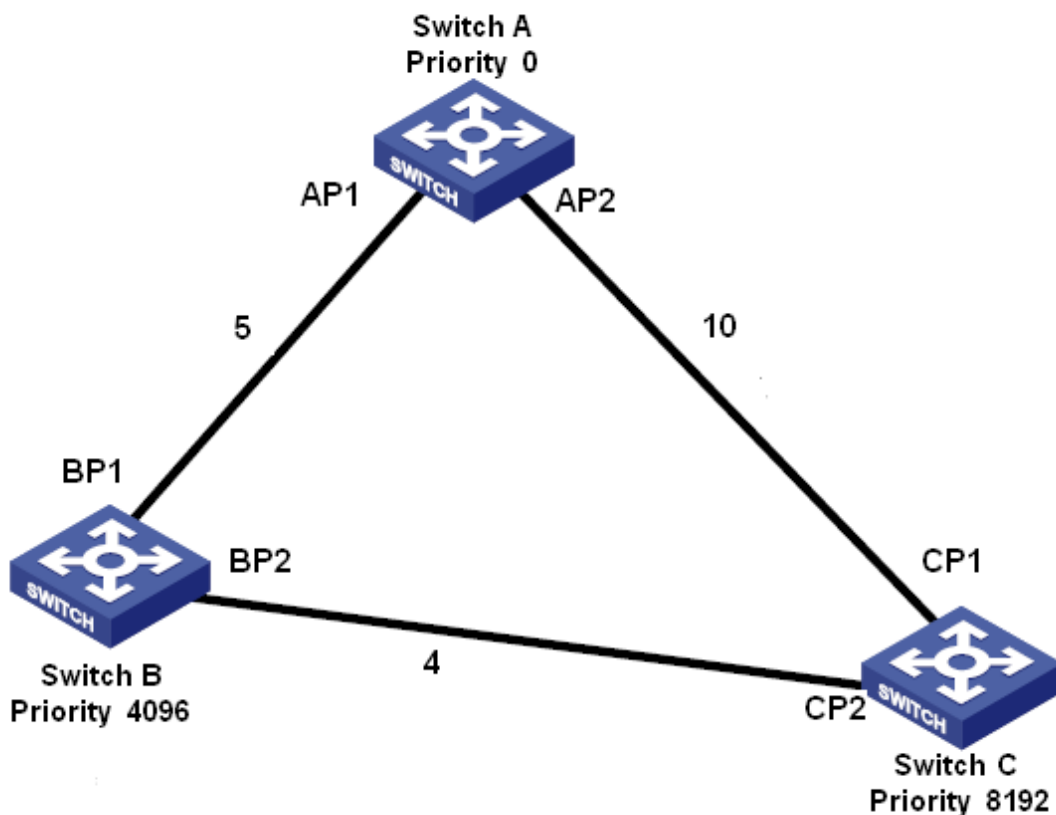


Figure 83 RSTP Configuration Example

Configuration on Switch A:

1. Set priority to 0 and time parameters to default values, as shown in Figure 81.
2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 82.

Configuration on Switch B:

1. Set priority to 4096 and time parameters to default values, as shown in Figure 81.
2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 82.

Configuration on Switch C:

1. Set priority to 8192 and time parameters to default values, as shown in Figure 81.
2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 82.

- The priority of Switch A is 0 and its root ID is the smallest. Therefore, Switch A is the root bridge.
- The path cost from AP1 to BP1 is 5 and that from AP2 to BP2 is 14. Therefore, BP1 is the root port.
- The path cost from AP1 to CP2 is 9 and that from AP2 to CP1 is 10. Therefore, CP2 is the root port and BP2 is the designated port.

## **6.14 RSTP/STP Transparent Transmission**

### **6.14.1 Overview**

RSTP is compliant with IEEE standard. DT-Ring is the private redundant protection protocol of Kyland, but cannot coexist with RSTP on the same network. To solve the problem, Kyland develops the RSTP transparent transmission function. The function enables the switch to keep other redundant protocols while transparently transmit RSTP packets, meeting industrial

communication requirements.

Switches running other redundant protocols can receive and forward RSTP packets only if the RSTP transparent transmission function is enabled. RSTP transparent transmission-enabled switches can be regarded as a transparent link.

As shown in the following figure, Switch A, Switch B, Switch C, and Switch D form a DT ring. The transparent transmission function is enabled on these four switches, so that Switch E and Switch F can receive RSTP packets from each other.

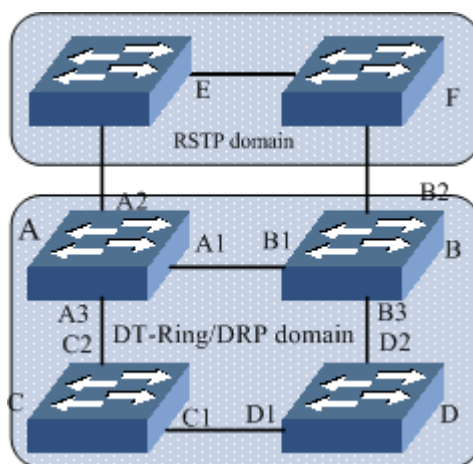


Figure 84 RSTP Transparent Transmission

### 6.14.2 Web Configuration

Configure RSTP transparent transmission on ports, as shown in the following figure.

Port	RSTP Transparent Transmission	
FE1	Disable	▼
FE2	Disable	▼
FE3	Disable	▼
FE4	Disable	▼
FE5	Enable	▼
FE6	Enable	▼
FX7	Disable	▼
FX8	Disable	▼
GE1	Disable	▼
GE2	Disable	▼

Figure 85 RSTP Transparent Transmission Configuration

**RSTP Transparent Transmission**

Options: Enable/Disable

Default: Disable

Function: Enable or disable RSTP transparent transmission on ports.

**Caution:**

RSTP transparent transmission cannot be enabled on an RSTP-enabled port.

**6.14.3 Typical Configuration Example**

As shown in Figure 84, Switch A, Switch B, Switch C, and Switch D form a DT ring, and Switch E and Switch F form an RSTP ring. In the RSTP ring, the entire DT ring serves as a transparent link to forward RSTP packets of Switch E and Switch F.

- Configure Switch A, Switch B, Switch C, and Switch D as a DT ring. For details, see DT-Ring Configuration.
- Enable RSTP on the involved ports of Switch E and Switch F, as shown in Figure 80 and Figure 82.

- Enable RSTP transparent transmission on ports A1, A2, A3, B1, B2, B3, C1, C2, D1, and D2, as shown in Figure 85.

## **6.15 QoS**

### **6.15.1 Overview**

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

QoS mainly involves service identification, congestion management, and congestion avoidance.

Service identification: Objects are identified based on certain match rules. For example, The objects can be priority tags carried by packets, priority mapped by ports and VLANs, or priority information mapped by quintuples. Service identification is the precondition for QoS.

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

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

### **6.15.2 Principle**

Each port of the switch has four cache queues, from 0 to 3 in priority ascending order.

You can configure the mapping between priority and queues. When a frame

reaches the port, the switch determines the queue for the frame according to the information in the frame header. The switch supports three queue mapping modes for priority identification: highest priority, TOS/DIFF, and 802.1p.

- If the highest priority is configured on a port, packets to be forwarded are put in queue 3.
- The TOS/DIFF value depends on the TOS/DSCP in packets. You can configure the mapping between priority and queues.
- When a packet is tagged, the 802.1p value depends on the priority of 802.1Q in the packet. When a packet is untagged, the 802.1p value depends on the default priority of the port. You can configure the mapping between the 802.1p priority and queues.

When forwarding data, a port uses a scheduling mode to schedule the data of four queues and the bandwidth of each queue. The switch supports two scheduling modes: Weighted Round Robin (WRR) and preempt mode.

- WRR schedules data flows based on weight ratio. Queues obtain their bandwidths based on their weight ratio. WRR prioritizes high-weight ratio queues. More bandwidths are allocated to queues with higher weight ratio.
- Hq-preempt mode forwards high-priority packets preferentially. It is mainly used for transmitting sensitive signals. If a frame enters the high-priority queue, the switch stops scheduling the low-priority queues and starts to process the data of the high-priority queue. When the high-priority queue contains no data, the switch starts to process the data of the queue with lower priority.

### 6.15.3 Web Configuration

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



Figure 86 QoS Mode

**QoS Mode**

Options: Disable/WRR/Hq-preempt

Default: Hq-preempt

Function: Configure the scheduling mode of a port.

**IP TOS/DSCP**

Options: DSCP MODE/IP TOS MODE

Default: DSCP MODE

Function: DSCP and IP TOS share the same field. DSCP mode indicates the DSCP priority-queue mapping mode and IP TOS mode indicates the IP TOS priority-queue mapping mode.

2. Configure the queue weight ratio, as shown in the following figure.

**Weight of Priority Queues**

3--HIGHEST	2--SECHIGH	1--SECLOW	0--LOWEST
8	4	2	1

Figure 87 Configuring Queue Weight Ratio

**{3-HIGHEST,2-SECHIGH,1-SECLOW,0-LOWEST}**

Range: {1~55, 1~55, 1~55, 1~55}

Default: {8, 4, 2, 1}

Function: Configure the queue weight ratio by obeying the following rules:

Weight of queue 3  $\geq 2 \times$  Weight of queue 2, Weight of queue 2  $\geq 2 \times$  Weight of queue 1, Weight of queue 1  $\geq 2 \times$  Weight of queue 0

3. Configure QoS port priority mapping mode, as shown in the following figure.

**Set the Port Priority**

Port	Highest priority	TOS/DIFF	802.1P Priority
FE1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FE2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FE5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FE6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FX8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

Help

Figure 88 Setting QoS Port Priority Mapping Mode

**Set the Port Priority**

Options: Highest priority/TOS/DIFF/802.1p Priority

Default: 802.1p Priority

Function: Configure port priority mapping mode.

Description: Only one priority mapping mode can be selected for each port.

4. Configure 802.1p priority-queue mapping.

Click <802.1p Priority> in Figure 86 to configure the 802.1p priority-queue mapping, as shown in the following figure.

**802.1P Priority 0~7**

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

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

Figure 89 802.1p Priority-Queue Mapping

### 802.1p Priority

Portfolio: {Priority, Queue}

Range: {0~7, 0~3}

Default: Priority 0 and 1 are mapped to queue 0; priority 2 and 3 are mapped to queue 1.

Priority 4 and 5 are mapped to queue 2; priority 6 and 7 are mapped to queue 3.

Function: Configure the mapping between 802.1p priority and queue.

5. Configure IP TOS priority-queue mapping.

Click <IP TOS Priority> in Figure 86 to configure the DSCP priority-queue mapping, as shown in the following figure.

**IP TOS Priority 0~7**

Priority	Queue
IP TOS 0	0
IP TOS 1	0
IP TOS 2	1
IP TOS 3	1
IP TOS 4	2
IP TOS 5	2
IP TOS 6	3
IP TOS 7	3

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

Figure 90 IP TOS Priority-Queue Mapping

**IP TOS Priority**

Portfolio: {Priority, Queue}

Range: {0~7, 0~3}

Default: Priority 0 to 7 are mapped to queue 0.

Function: Configure the mapping between IP TOS priority and queue.

6. Configure DSCP priority-queue mapping.

Click <DSCP Priority> in Figure 86 to configure the DSCP priority-queue mapping, as shown in the following figure.

DSCP Priority 0~63

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

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

Apply

Back

Figure 91 DSCP Priority-Queue Mapping

**DSCP Priority**

Portfolio: {DSCP, Qos Queue}

Range: {0~63, 0~3}

Default: Priority 0 to 63 are mapped to queue 0.

Function: Configure the mapping between DSCP priority and queue.

**6.15.4 Typical Configuration Example**

As shown in the following figure, port 1, port 2, port 3, and port 4 forward packets to port 5. The highest priority mode is configured on port 1. Packets from port 1 are mapped to queue 3. The 802.1p priority carried by packets from port 2 is 2, which is mapped to queue 1. The 802.1p priority carried by packets from port 3 is 4, which is mapped to queue 2. The DSCP priority carried by packets from port 4 is 6, which is mapped to queue 3. Port 5 adopts the WRR

scheduling mode.

Configuration steps:

1. Select WRR (default value) for QoS mode and DSCP for IP TOS/DSCP, as shown in Figure 86.
2. Configure highest priority-queue mapping on port 1, 802.1p on port 2 and port 3, and TOS/DIFF on port 4, as shown in Figure 88.
3. Configure 802.1p priority 2 and 4 to map to queue 1 and queue 2 respectively, as shown in Figure 89.
4. Configure DSCP priority 6 to map to queue 3, as shown in Figure 91.

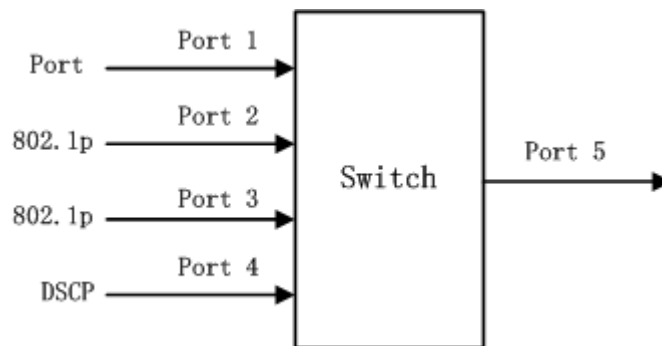


Figure 92 QoS Configuration Example

Packets received through port 1 and port 4 are put into queue 3; packets received through port 2 are put into queue 1; packets received through port 3 are put into queue 2. According to the mapping between queues and weights, the weight of queue 1 is 2, the weight of queue 2 is 4, and the weight of queue 3 is 8. As a result, the packets in queue 1 enjoy  $2/(2+4+8)$  bandwidth, those in queue 2 enjoy  $4/(2+4+8)$  bandwidth, and those in queue 3 enjoy  $8/(2+4+8)$  bandwidth. Packets received through port 1 and port 4 are put into queue 3 and forwarded according to the FIFO mechanism. The total bandwidth ratio of port 1 and port 4 is  $8/(2+4+8)$ .

## 6.16 MAC Address Aging Time

### 6.16.1 Overview

Ports of the switch can learn addresses automatically. The switch adds the

source addresses (source MAC address, switch port number) of received frames to the address table. Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, the switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC address table does not involve the concept of aging time.

### 6.16.2 Web Configuration

Configure MAC address aging time, as shown in the following figure.



Figure 93 MAC Address Aging Time

### MAC Aging Time

Range: 15~3600 seconds

Default: 300 seconds

Description: The value must be a multiple of 15. You can adjust the aging time as required.

## 6.17 LLDP

### 6.17.1 Overview

The Link Layer Discovery Protocol (LLDP) provides a standard link layer discovery mechanism. It encapsulates device information such as the capability, management address, device identifier, and interface identifier in a Link Layer Discovery Protocol Data Unit (LLDPDU), and advertises the LLDPDU to its directly connected neighbors. Upon receiving the LLDPDU, the neighbors save these information to MIB for query and link status check by the NMS.

## 6.17.2 Web Configuration

View LLDP connection information, as shown in the following figure.

LLDP Information			
Local Port	Remote Port	Neighbor IP	Neighbor MAC
3	4	192.168.0.51	08:00:3e:32:53:22
5	14	192.168.183.53	00:1e:cd:12:21:15

Figure 94 LLDP Information

In LLDP information, you can view the information about neighboring devices, including port number of the neighboring device connected to the local switch, IP address and MAC address of the neighboring device.



### Caution:

To display LLDP information, LLDP must be enabled on the two connected devices. LLDP is a link-layer detection protocol enabled by default.

## 6.18 SNTP

### 6.18.1 Overview

The Simple Network Time Protocol (SNTP) synchronizes time between server and client by means of requests and responses. As a client, the switch synchronizes time from the server according to packets of the server. In this case, a maximum of four SNTP servers can be configured, but only one can be active at a time. The switch can also serve as the SNTP server to provide time synchronization for clients.

The SNTP client sends a request to each server one by one through unicast. The server that responds first is in active state. The other servers are in inactive state.

**Caution:**

To synchronize time by SNTP, there must be an active SNTP server.

### 6.18.2 Web Configuration

1. Enable SNTP. Select the server and set related parameters, as shown in the following figure.

SNTP State	Enable	▼
Server IP	192.168.0.23	
Interval Time	16	(16-16284Sec)
time zone	GMT + 8	▼

Figure 95 SNTP Configuration

#### SNTP State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable SNTP.

#### Server IP

Format: A.B.C.D

Function: Set the IP address of the SNTP server. The client synchronizes time from the server based on the packets sent by the server.

#### Interval Time

Options: 16~16284s

Function: Configure the interval for sending synchronization requests from the SNTP client to the server.

#### time zone

Options: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, -12

Default: 0

Function: Select the local time zone.

2. Select the synchronization mode between the client and the server, as shown in the following figure.

Server Time	2012.06.28 13:55:02		
Device Time	2012.06.28 13:55:16		
update	<input type="text" value="automatism"/>	<input type="button" value="Apply"/>	

Figure 96 Time Synchronization Mode

### Server Time

Function: Display the latest time obtained from the server.

### Device Time

Function: Display the time of the device.

### update

Options: automatism/manual

Default: automatism

Function: Select the time synchronization mode between the device and the server.

3. View SNTP configuration, as shown in the following figure.

Number	Server IP	Server State	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	192.168.1.23	repose	+ 0	20	<input type="button" value="Synch"/>

Figure 97 SNTP Configuration

### Server State

Options: active/repose

Description: The active server provides SNTP time for the client. Only one server can be in active state at a time.

### Synchronization

To synchronize time manually, click <Synch>.

4. Configure the switch as the SNTP server, as shown in the following figure.

SNTP State	Enable	▼
time zone	GMT	+ 8 ▼

Apply Help

Local IP	192.168.0.22
Device Time	2012.06.28 14:21:27
Time Zone	8

Figure 98 Configuring the Switch as the SNTP Server

**SNTP State**

Options: Enable/Disable

Default: Disable

Function: Enable or disable the SNTP server function.

**time zone**

Options: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, and -12

Default: +8

Function: Select the server time zone.

**6.19 MSTP****6.19.1 Overview**

Although RSTP achieves rapid convergence, it also has the following defect just as the STP: all bridges in the LAN share one spanning tree and packets of all VLANs are forwarded along the spanning tree. As shown in the following figure, certain configurations may block the link between switch A and switch C. Because switch B and switch D are not in VLAN 1, they cannot forward the packets of VLAN 1. As a result, the VLAN 1 port of switch A cannot communicate with that of switch C.

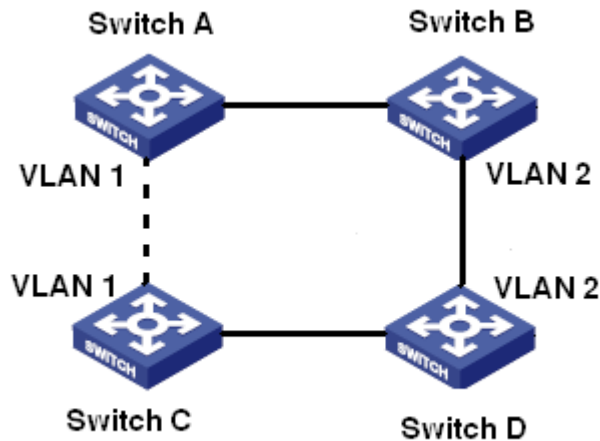


Figure 99 RSTP Defect

To solve this problem, the Multiple Spanning Tree Protocol (MSTP) came into being. It achieves both rapid convergence and separate forwarding paths for the traffic of different VLANs, providing a better load sharing mechanism for redundant links.

MSTP maps one or multiple VLANs into one instance. Switches with the same configuration form a region. Each region contains multiple mutually independent spanning trees. The region serves as a switch node. It participates in the calculation with other regions based on the spanning tree algorithm, calculating an overall spanning tree. Based on this algorithm, the network in Figure 99 forms the topology shown in Figure 100. Both switch A and switch C are in Region1. No link is blocked because the region contains no loops. This is the same with Region2. Region1 and Region2 are similar to switch nodes. These two "switches" form a loop. Therefore, a link should be blocked.

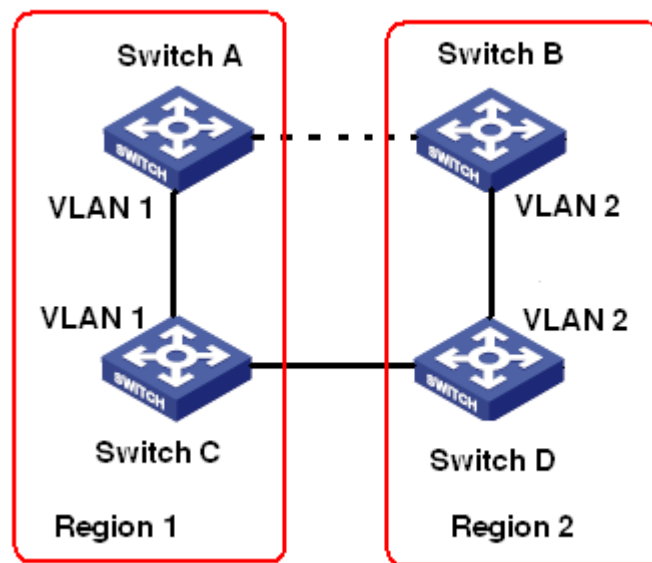


Figure 100 MSTP Topology

### 6.19.2 Concepts

Learn MSTP concepts based on the following figures.

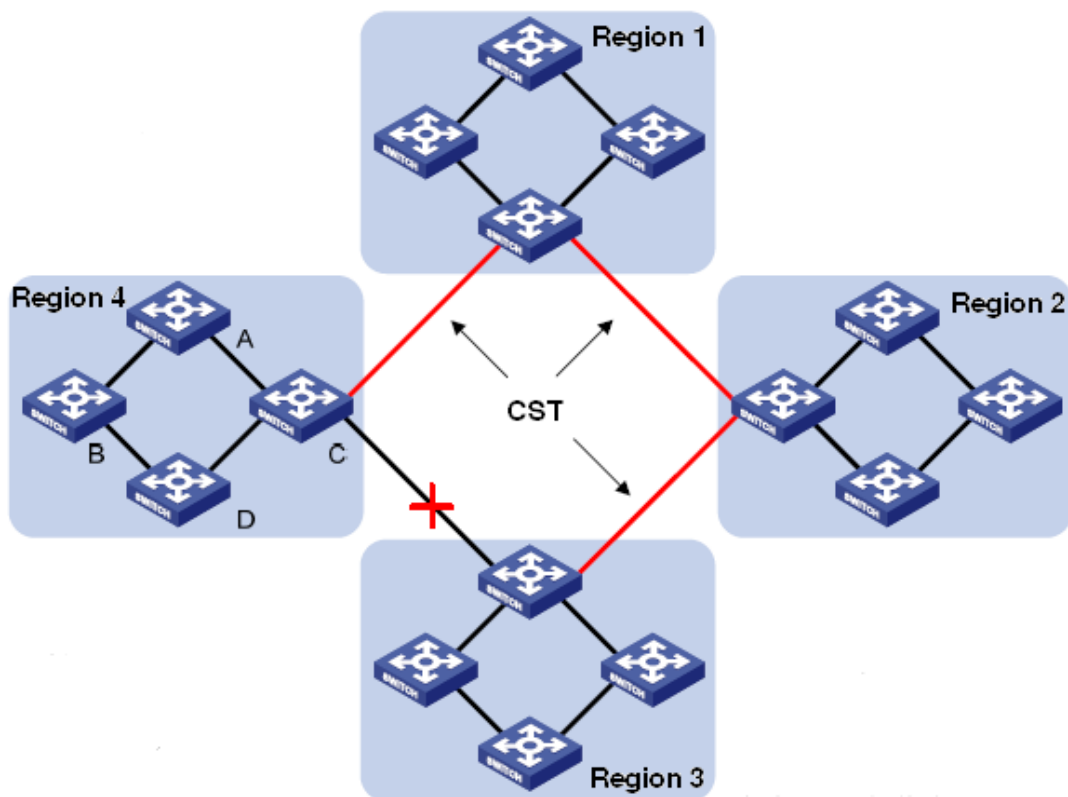


Figure 101 MSTP Concepts

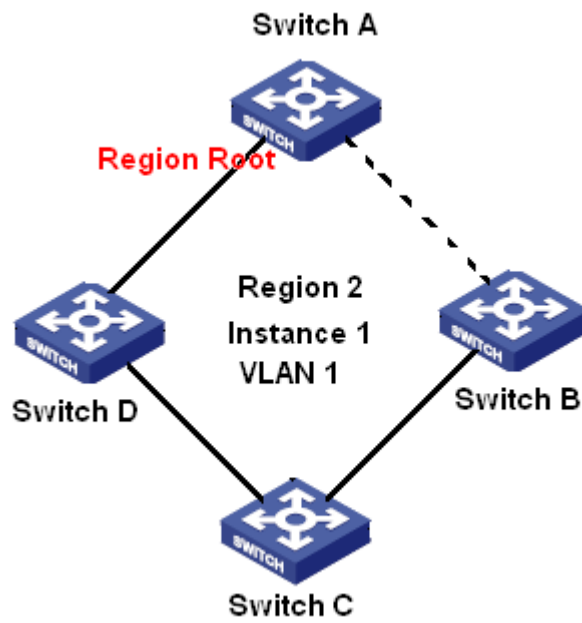


Figure 102 VLAN 1 Mapped to Instance 1

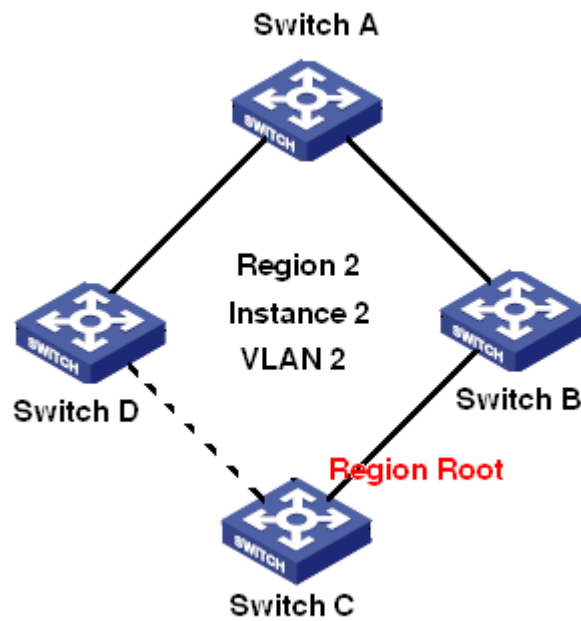


Figure 103 VLAN 2 Mapped to Instance 2

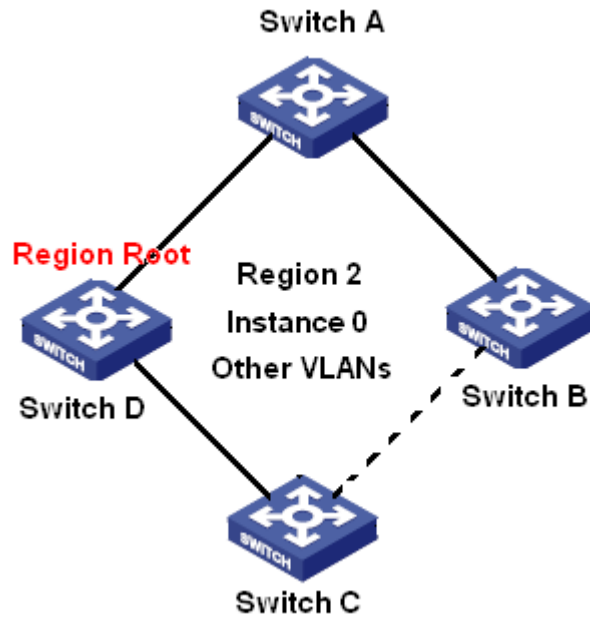


Figure 104 Other VLANs Mapped to Instance 0

- Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 102 and Figure 103) or multiple VLANs with the same topology (as shown in Figure 104) can be mapped to one instance; that is, one VLAN can form a spanning tree and multiple VLANs can share one spanning tree. Different instances are mapped to different spanning trees. Instance 0 is the spanning tree for the devices of all regions, while the other instances are the spanning trees for the devices of a specific region.
- Multiple Spanning Tree Regions (MST regions): Switches with the same MSTP region name, revision level, and VLAN-to-instance mapping are in the same MST region. As shown in Figure 101, Region1, Region2, Region3, and Region4 are four different MST regions.
- VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 101, VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 102; VLAN 2 is mapped to instance 2, as shown in Figure 103. The other VLANs are mapped to instance 0, as shown in Figure 104.
- Common and Internal Spanning Tree (CIST): indicates instance 0, that is, the spanning tree covering all the devices on a switching network. As shown

in Figure 101, the CIST comprises IST and CST.

- Internal Spanning Tree (IST): indicates the CIST segment in the MST region, that is, instance 0 of each region, as shown in Figure 104.
- Common Spanning Tree (CST): indicates the spanning tree connecting all MST regions in a switching network. If each MST region is a device node, the CST is the spanning tree calculated based on STP/RSTP by these device nodes. As shown in Figure 101, the red lines indicate the spanning tree.
- MSTI (Multiple Spanning Tree Instance): one MST region can form multiple spanning trees and they are independent of each other. Each spanning tree is a MSTI, as shown in Figure 102 and Figure 103. IST is also a special MSTI.
- Common root: indicates the root bridge of the CIST. The switch with the smallest root bridge ID in a network is the common root.
- Regional root: In an MST region, spanning trees have different topologies, and their regional roots can also be different. As shown in Figure 102, Figure 103, and Figure 104, the three instances have different regional roots.

The root bridge of the MSTI is calculated based on STP/RSTP in the current MST region.

The root bridge of the IST is the device that is connected to another MST region and selected based on the priority information received.

- Boundary port: indicates the port that connects an MST region to another MST region, STP running region, or RSTP running region.
- Port state: A port can be in either of the following states based on whether it is learning MAC addresses and forwarding traffic.
- Forwarding state: indicates that a port learns MAC addresses and forwards traffic.

Learning state: indicates that a port learns MAC addresses but does not forward traffic.

Discarding state: indicates that a port neither learns MAC addresses nor forwards traffic.

- Root port: indicates the best port from a non-root bridge to the root bridge, that is, the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.

The root port can be in forwarding, learning, or discarding state.

- Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.

The designated port can be in forwarding, learning, or discarding state.

- Master port: indicates the port that connects an MST region to the common root. The port is in the shortest path to the common root. From the CST, the master port is the root port of a region (as a node). The master port is a special boundary port. It is the root port for the CIST and master port for other instances.

The master port can be in forwarding, learning, or discarding state.

- Alternate port: indicates the backup port of the root port or master port. When the root port or master port fails, the alternate port becomes the new root port or master port.

The master port can only be in discarding state.

- Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the designated port and forwards data without any delay.

The backup port can only be in discarding state.

### **6.19.3 Implementation**

MSTP divides a network into multiple MST regions. CST is calculated between regions. Multiple spanning trees are calculated in a region. Each spanning tree is an MSTI. Instance 0 is the IST, and other instances are MSTIs.

#### **1. CIST calculation**

- A device sends and receives BPDUs. Based on the comparison of MSTP configuration messages, the device with the highest priority is selected as the common root of the CIST.
- An IST is calculated in each MST region.
- Each MST region is considered as a single device and CST is calculated between regions.
- CST and IST constitute the CIST of the entire network.

## 2. MSTI calculation

In an MST region, MSTP generates different spanning trees for VLANs based on the mapping between VLANs and spanning trees. Each spanning tree is calculated independently. The calculation process is similar to that in STP.

In an MST region, VLAN packets are forwarded along corresponding MSTIs. Between MST regions, VLAN packets are forwarded along the CST.

### 6.19.4 Web Configuration

1. Enable MSTP, as shown in the following figure.

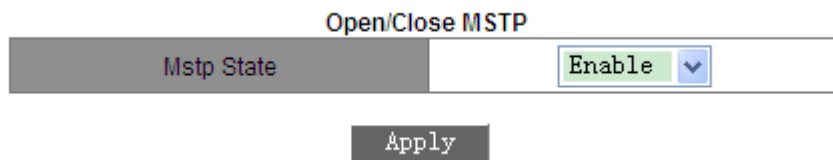


Figure 105 Enabling MSTP

#### Mstp State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable MSTP.

2. Configure MSTP operation mode, as shown in the following figure.

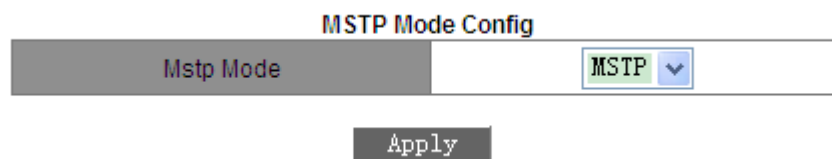


Figure 106 Configuring MSTP Mode

## Mstp Mode

Options: MSTP/STP

Default: MSTP

Function: Configure the mode of switch running spanning tree.

Description: In STP mode, all switch ports can send only STP BPDU packets. In MSTP mode, all switch ports send out MSTP BPDU packets, but if the switch is connected to an STP-enabled device, the port will automatically change to STP mode.

3. Force port to work in MSTP mode, as shown in the following figure.

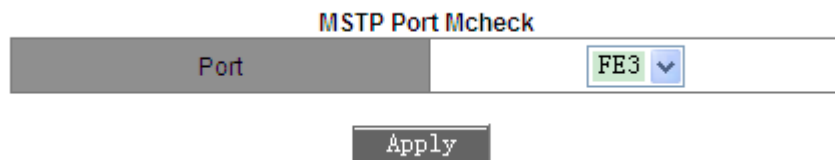


Figure 107 Forcing Port to Work in MSTP Mode

## Port

Options: all switch ports

Function: When an MSTP-enabled port is connected to an STP-enabled device, the connected port will automatically change to STP mode. If the STP-enabled device is removed, the port will not automatically go back to MSTP mode. If you want the switch to go back to MSTP mode in such a condition, configure this function for the port. Then if the port receives an STP message again, the port will automatically change to STP mode again.



### Caution:

This configuration will take effect only when the switch runs in MSTP mode; otherwise, it is invalid.

4. Configure the MSTP state of port, as shown in the following figure.

**Open/Close Port MSTP**

Operation type	Add ▼
Port	FE3 ▼

Apply

Figure 108 Configuring MSTP on Port

**Operation type**

Options: Add/Del

Default: Add

Function: Enable/Disable MSTP on a port.

Description: Add is to enable MSTP on the port; Del is to disable MSTP on the port. If MSTP is enabled globally, MSTP is enabled on all ports by default.

5. Set MST region parameters, as shown in the following figure.

**MSTP Region Config**

OperationType	Set ▼
MSTP Region Name Config	000a93050010
MSTP Revisionlevel Config	0

Apply

Figure 109 Configuring MST Region Parameters

**Operation Type**

Options: Set/Default

Function: Select the operation type of MST region parameters.

**MSTP Region Name Config**

Range: 1~32 characters

Default: device MAC address

Function: Configure the name of MST region.

**MSTP Revision level Config**

Options: 0~65535

Default: 0

Function: Configure the revision parameter of MSTP region.

Description: Revision parameter, MST region name, and VLAN mapping table codetermines the MST region that the device belongs to. When all configurations are the same, the devices are in same MST region.

6. Configure VLAN mapping table, as shown in the following figure.

**Add/Del Instance**

OperationType	Add ▼
MSTP Instance ID	3
Vlan List	5

**Apply**

**Instance List**

Instance ID	Vlan List
0	1 6 - 4094
2	2
3	3 - 5

Figure 110 Configuring VLAN Mapping Table

### Operation Type

Options: Add/Del

Function: Configure the operation type of VLAN mapping table.

### Portfolio: <MSTP Instance ID, Vlan List>

Range: <0~16, 1~4094>

Default: <0, 1~4094>

Function: Configure the VLAN mapping table in MST region.

Description: By default, all VLANs map to instance 0. One VLAN maps to only one spanning tree instance. If a VLAN with an existing mapping is mapped to another instance, the previous mapping is cancelled. If the mapping between the designated VLAN and instance is deleted, this VLAN will be mapped to instance 0.



#### Caution:

<Del> cannot delete the VLAN list of instance 0.

After setting is completed, the "Instance List" shows the mapping between VLAN and instance.

7. Configure the bridge priority of the switch in designated instance, as shown in the following figure.

**MSTP MST Priority**

OperationType	Add ▼
MSTP Instance ID	0 ▼
MSTP Bridge Priority	32768

**Apply**

Figure 111 Configuring Bridge Priority in Designated Instance

### Operation Type

Options: Add/Default

Function: Select the operation type of the bridge priority for the switch in a designated instance.

### MSTP Instance ID

Options: all created instances

### MSTP Bridge Priority

Range: 0~61440 with the step of 4096

Default: 32768

Function: Configure the bridge priority of the switch in designated instance.

Description: The bridge priority determines whether the switch can be elected to regional root of spanning tree instance. The smaller value is, the higher priority is. By setting a lower priority, a certain device can be designated to root bridge of spanning tree. The MSTP-enabled device can be configured with different priorities in different spanning tree instance.

8. Configure port priority and path cost in the designated instance, as shown in the following figure.

**MSTP MST Port Cost and Priority**

OperationType	Add ▼
MSTP Instance ID	0 ▼
Port	FE3 ▼
Priority	128
MSTP Port Pathcost	200000

Apply

Figure 112 Setting Port Priority and Path Cost in Designated Instance

**Operation Type**

Options: Add/Default

Function: Select the operation type of the priority and path cost of the port in a designated instance.

**MSTP Instance ID**

Options: all created instances

**Port**

Options: all switch ports

**Priority**

Range: 0~240 with step of 16

Default: 128

Function: Configure the priority of the port in the designated instance.

Description: Port priority determines whether it will be elected to root port. In the same condition, the port with lower priority will be elected to root port. The MSTP-enabled ports can be configured with different priorities and play different port roles in different spanning tree instances.

**MSTP Port Path cost**

Range: 1~2000000000

Default: as listed in the following tables.

Table 8 Default Path Cost of Common Port

Port Type	Default Path Cost	Recommended Range
-----------	-------------------	-------------------

10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000

Table 9 Default Path Cost of Aggregation Port

Port Type	Number of Aggregation Ports	Recommended
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

Function: Configure the path cost of the port in the designated instance.

Description: Port path cost is used to calculate the optimum path. This parameter depends on bandwidth. The bigger bandwidth is, the lower cost is. Changing port path costs can change the transmission path between the device and root bridge, thereby changing port role. The MSTP-enabled port can be configured with different path costs in different spanning tree instances.

9. Set MSTP time parameters, as shown in the following figure.

**MSTP Time Config**

OperationType	Set <input type="button" value="v"/>
MSTP Forward Time Config	<input type="text" value="15"/>
MSTP Hello Time	<input type="text" value="2"/>
MSTP Maxage Time	<input type="text" value="20"/>
MSTP Max Hop	<input type="text" value="20"/>

Figure 113 Setting MSTP Time Parameters

### Operation Type

Options: Set/Default

Function: Select the operation type of MSTP time parameters.

### MSTP Forward Time Config

Options: 4~30s

Default: 15s

Function: Configure the time interval for port state transition (Discarding — Learning or Learning — Forwarding).

### **MSTP Hello Time**

Range: 1~10s

Default: 2s

Function: Configure the time interval for sending BPDUs.

### **MSTP Max age Time**

Range: 6~40s

Default: 20s

Function: Set the maximum age of BPDU packets.



#### **Caution:**

- The values of MSTP Forward Time Config, MSTP Hello Time, and MSTP Max age Time should meet the following requirements:  
$$2 \times (\text{MSTP Forward Time Config} - 1.0 \text{ seconds}) \geq \text{MSTP Max age Time}$$
$$\text{MSTP Max age Time} \geq 2 \times (\text{MSTP Hello Time} + 1.0 \text{ seconds})$$
- The default settings are recommended.

### **MSTP Max Hop**

Range: 1~40

Default: 20

Function: Configure the maximum hops of MST region. The maximum hops of MST region limit the scale of MST region; the maximum number of hops of regional root is the maximum number of hops of MST region.

Description: Starting from the root bridge of spanning tree in MST region, the hop number deducts 1 when the BPDU passes through a device in the region.

Device drops the BPDU with the hop number of 0.



#### **Caution:**

- Only the maximum hop configuration of the root bridge in MST region is valid.  
Non-root bridge devices adopt the maximum hop of the root bridge.

➤ The default settings are recommended.

10. Configure MSTP fast transfer, as shown in the following figure.

**MSTP Fast Transfer Config**

OperationType	Add ▼
Port	FE3 ▼
MSTP Port Link Type	AUTO ▼
Set/Cancel Marginal Port	Ordinary port ▼

**Apply**

Figure 114 Configuring MSTP Fast Transfer

### Operation Type

Options: Add/Default

Function: Select the operation type of MSTP fast transfer.

### MSTP Port Link Type

Options: AUTO/Force True/Force False

Default: AUTO

Function: Set the link type of the port. If the port is connected to a point-to-point link, fast state transfer is available on the port.

Description: **AUTO** means the switch will automatically detect link type according to port duplex state. When the port works in full duplex mode, MSTP protocol will automatically assume that the link connected to the port is a point-to-point link. When the port works in half-duplex mode, MSTP protocol will automatically assume that the link connected to the port is a shared link.

**Force True** means the link connected to the local port is a point-to-point link.

**Force False** means the link connected to the local port is a shared link.

### Set/Cancel Marginal Port

Options: Marginal port/Ordinary port

Default: Ordinary port

Function: Configure the port as marginal or ordinary port.

Description: When the port is directly connected to terminals, but not connected to other devices or shared network segments, this port is a marginal port. A marginal port can transfer from blocking to forwarding without delay. Once the marginal port receives a BPDU, the port will change to ordinary port again.

### 6.19.5 Typical Configuration Example

As shown in the following figure, Switch A, B, C, and D belong to the same MST region. The VLANs marked in red indicate the VLAN packets can be transmitted through the links. After configurations are completed, VLAN packets can be forwarded along different spanning tree instances. VLAN 10 packets are forwarded along instance 1 and the root bridge of instance 1 is Switch A; VLAN 30 packets are forwarded along instance 3 and the root bridge of instance 3 is Switch B. VLAN 40 packets are forwarded along instance 4 and the root bridge of instance 4 is Switch C. VLAN 20 packets are forwarded along instance 0 and the root bridge of instance 0 is Switch B.

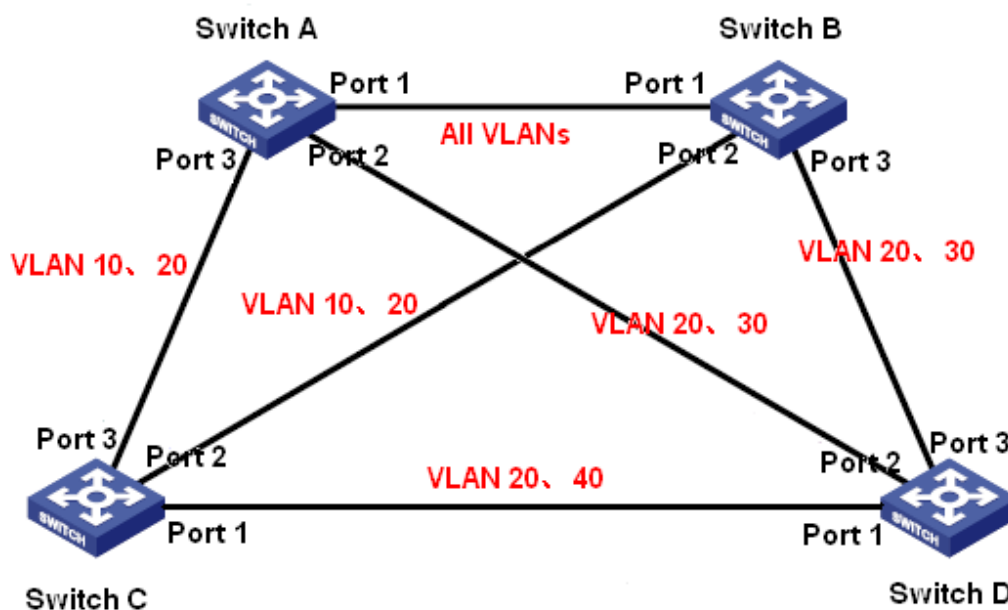


Figure 115 MSTP Typical Configuration Example

#### Configuration on Switch A:

1. Create VLAN 10, 20, and 30 on Switch A. Configure the ports to allow the packets of respective VLANs to pass through.
2. Enable global MSTP protocol, as shown in Figure 105.
3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 109.
4. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 110.
5. Set the switch bridge priority in instance 1 to 4096, and keep default priority in other instances, as shown in Figure 111.

**Configuration on Switch B:**

6. Create VLAN 10, 20, and 30 on Switch B. Configure the ports to allow the packets of respective VLANs to pass through.
7. Enable global MSTP protocol, as shown in Figure 105.
8. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 109.
9. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 110.
10. Set switch bridge priority in instance 3 and instance 0 to 4096, and keep default priority in other instances, as shown in Figure 111.

**Configuration on Switch C:**

11. Create VLAN 10, 20 and 40 on Switch C. Configure the ports to allow the packets of respective VLANs to pass through.
12. Enable global MSTP protocol, as shown in Figure 105.
13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 109.
14. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 110.
15. Set the switch bridge priority in instance 4 to 4096, and keep default priority in other instances, as shown in Figure 111.

**Configuration on Switch D:**

16. Create VLAN 20, 30 and 40 on Switch D. Configure the ports to allow the packets of respective VLANs to pass through.
17. Enable global MSTP protocol, as shown in Figure 105.
18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 109.
19. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 110.

When MSTP calculation is completed, the MSTI of each VLAN is as follows:

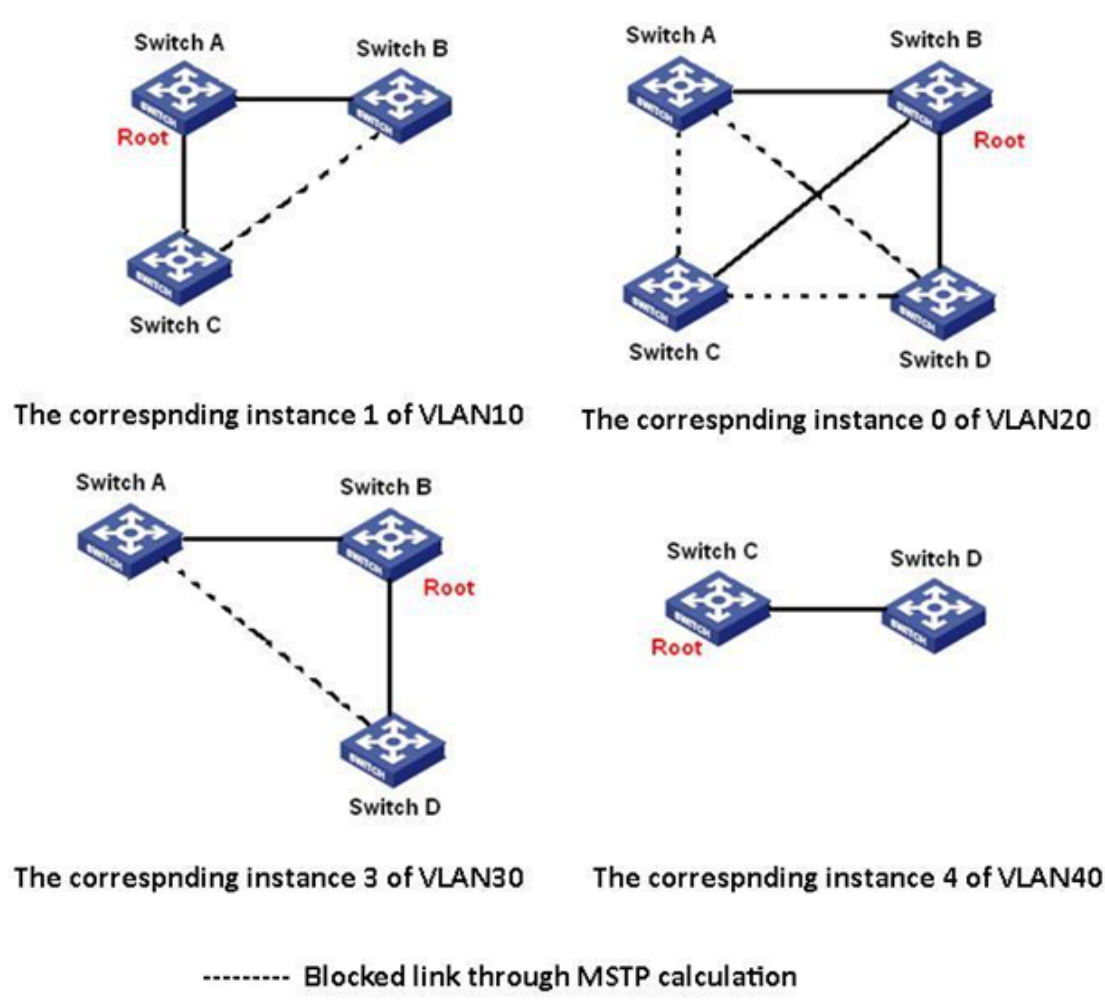


Figure 116 Spanning Tree Instance of each VLAN

## 6.20 Alarm

### 6.20.1 Overview

This series switches support the following types of alarms:

- IP/MAC conflict alarm: If the function is enabled, an alarm will be generated for an IP/MAC conflict.
- Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.
- Ring alarm: If this function is enabled, an alarm is triggered when the ring is open.
- Power alarm: If the function is enabled, an alarm will be generated for a single power input.



**Caution:**

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

### 6.20.2 Web Configuration

1. Set alarm parameters, as shown in the following figures.

IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	<input checked="" type="checkbox"/>	300 (180~600sec.)

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	<input checked="" type="checkbox"/>	FE2	<input checked="" type="checkbox"/>	FE3	<input checked="" type="checkbox"/>	FE4	<input checked="" type="checkbox"/>
FE5	<input checked="" type="checkbox"/>	FE6	<input checked="" type="checkbox"/>	FX7	<input type="checkbox"/>	FX8	<input type="checkbox"/>
GE1	<input type="checkbox"/>	GE2	<input type="checkbox"/>	-	-	-	-

DT-RING Alarm

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

Apply

Help

Figure 117 Alarm Setting

**IP, MAC Conflict**

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	<input checked="" type="checkbox"/>	300 (180~600sec.)

**Power Alarm**

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

**Port Alarm**

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FX1	<input checked="" type="checkbox"/>	FX2	<input checked="" type="checkbox"/>	FE3	<input checked="" type="checkbox"/>	FE4	<input type="checkbox"/>
FE5	<input type="checkbox"/>	FE6	<input checked="" type="checkbox"/>	-	-	-	-

**DT-RING Alarm**

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

Figure 118 Alarm Setting (SICOM3005)

**IP, MAC Conflict**

Options: Select/Deselect

Default: Select

Function: Enable or disable IP/MAC conflict alarm.

**Alarm Time**

Range: 180~600s

Default: 300s

Function: Configure the interval for detecting IP/MAC conflicts.

**Power Alarm**

Options: Select/Deselect

Default: Select

Function: Enable or disable power alarm.

**Port Alarm**

Options: Select/Deselect

Default: Deselect

Function: Enable or disable port alarm.

### DT-RING Alarm

Options: Select/Deselect

Default: Deselect

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

2. After the alarm function is enabled, the alarm information is as follows:

Basic Vision	
Alarm Title	Alarm Status
IP Alarm	Alarm
MAC Alarm	Normal

Port Alarm							
Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Down	FE2	Link Down	FE3	Link Down	FE4	Link Up
FE5	Link Down	FE6	Link Up	FX7	-	FX8	-
GE1	-	GE2	-	-	-	-	-

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

Figure 119 Alarm Information

Basic Vision	
Alarm Title	Alarm Status
power	WARN
IP Alarm	Normal
MAC Alarm	Normal

Port Alarm							
Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FX1	Link Down	FX2	Link Down	FE3	Link Up	FE4	-
FE5	-	FE6	Link Up	-	-	-	-

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

Figure 120 Alarm Information (SICOM3005)

**power**

Options: Normal/WARN

Description: After the power alarm is enabled, Normal is displayed for dual power inputs while WARN is displayed for a single power input.

**IP/MAC Alarm**

Options: Normal/Alarm

Description: When an IP/MAC conflict occurs, Alarm is displayed; otherwise, Normal is displayed.

**Port Alarm**

Options: Link Up/Link Down

Description: After port alarm is enabled, Link Up is displayed for a port connected properly. Link Down is displayed for a port disconnected or connected abnormally.

**DT-RING Alarm**

Options: Ring Open/Ring Close

Description: After ring alarm is enabled, Ring Open is displayed for an open ring while Ring Close is displayed for a closed ring.

**6.21 Port Traffic Alarm****6.21.1 Overview**

With the port traffic alarm function, the switch generates an alarm if the traffic rate of a port exceeds the specified threshold or a CRC error occurs.

---

**Caution:**

- The traffic alarm function is based on a port. Such an alarm is generated only if the function is enabled on a port.
  - The traffic alarm function is direction-specific. Incoming and outgoing traffic corresponds to different alarms.
  - If a CRC error occurs, a CRC error alarm is generated.
-

## 6.21.2 Web Configuration

1. Configure port traffic alarm, as shown in the following figure.

Port	FE1
Alarm Type	Input Rate
Alarm Status	enable
Alarm Threshold	1000 kbps

Figure 121 Configuring Port Traffic Alarm

### Alarm Type

Options: Input Rate/Output Rate/CRC Error

Function: Configure the port traffic alarm type.

### Alarm Status

Options: enable/disable

Default: disable

Function: Enable or disable the alarm type.

### Alarm Threshold

Range: 1~10000000000bps or 1~1000000kbps

Function: Configure the port traffic alarm threshold.

2. View port traffic alarm information, as shown in the following figure.

Port	Input Rate		Alarm Status	Output Rate		Alarm Status	Error CRC	Alarm Status
FE1	enable	1000kbps	normal	enable	100bps	normal	disable	-
FE2	disable	-	-	disable	-	-	disable	-
FE3	disable	-	-	disable	-	-	enable	normal
FE4	disable	-	-	disable	-	-	enable	normal
FE5	enable	1000bps	alarm	enable	1000kbps	normal	disable	-
FE6	disable	-	-	disable	-	-	disable	-
FX7	disable	-	-	disable	-	-	disable	-
FX8	disable	-	-	disable	-	-	disable	-

Figure 122 Port Traffic Alarm Information

## 6.22 GMRP

### 6.22.1 GARP

The Generic Attribute Registration Protocol (GARP) is used for spreading, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network. GARP applications include GVRP and GMRP.

With GARP, the configuration information of a GARP member will spread the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

- When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn. A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.
- When a GARP application entity wants to cancel its own information on other switches, the entity sends a Leave message.
- After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.



**Note:**

An application entity indicates a GARP-enabled port.

---

GARP timers include Hold timer, Join timer, Leave timer, and LeaveAll timer.

- **Hold Timer:** When receiving a registration message, a GARP entity does not send a Join message immediately, but starts Hold timer. When the timer

expires, the entity sends all the registration messages received within the preceding period in one Join message, reducing packet sending for better network stability.

- **Join Timer:** To ensure that Join messages are received by other application entities, a GARP application entity starts Join timer after sending a Join message. If receiving no JoinIn message before Join timer expires, the entity sends the Join message again. If receiving a JoinIn message before the timer expires, the entity does not send the second Join message.
- **Leave Timer:** When a GARP application entity wants to cancel the information about an attribute, the entity sends a Leave message. The entity receiving the message starts Leave timer. If receiving no Join message before the timer expires, the entity receiving the message cancels the information about the attribute.
- **LeaveAll Timer:** As a GARP application entity starts, it starts LeaveAll timer. When the timer expires, the entity sends a LeaveAll message, so that the other GARP application entities re-register all the attributes. Then the entity starts LeaveAll timer again for the new cycle.

### 6.22.2 GMRP

The GARP Multicast Registration Protocol (GMRP) is a multicast registration protocol based on GARP. It is used for maintaining the multicast registration information of switches. All GMRP-enabled switches can receive multicast registration information from other switches, update local multicast registration information dynamically, and spread local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-enabled switches on a network.

If a switch or terminal wants to join or leave a multicast group, the GMRP-enabled port broadcasts the information to all the ports in the same VLAN.

### 6.22.3 Description

Agent port: indicates the port on which GMRP and the agent function are enabled.

Propagation port: indicates the port on which only GMRP is enabled, but not the agent function.

Dynamically learned GMRP multicast entry and agent entry are forwarded by the propagation port to the propagation ports of the lower-level devices.

All GMRP timers on the same network must keep consistent to prevent mutual interference. The timers should comply with the following rules: Hold timer < Join timer,  $2 * \text{Join timer} < \text{Leave timer}$ , and  $\text{Leave timer} < \text{LeaveAll timer}$ .

### 6.22.4 Web Configuration

1. Enable the global GMRP protocol, as shown in the following figure.

Protocol Configure	
GMRP State	Enable ▼
LeaveAll Timer	10000 ms

Apply Help

Figure 123 GMRP Global Configuration

#### GMRP State

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global GMRP function. The function and IGMP Snooping cannot be used at the same time.

#### LeaveAll Timer

Range: 100ms~327600ms

Default: 10000ms

Function: Set the interval for sending LeaveAll messages. The value must be a multiple of 100.

Description: If the LeaveAll timers of different devices expire at the same time,

multiple LeaveAll messages will be sent simultaneously, increasing unnecessary packets. To prevent this problem, the actual timeout of a LeaveAll timer is a random value between the specified value and 1.5 times the specified value.

2. Configure GMRP function on each port, as shown in the following figure.

**Port Configure**

Port	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
FE1	Enable ▼	Enable ▼	100 ms	500 ms	3000 ms
FE2	Enable ▼	Disable ▼	100 ms	500 ms	3000 ms
FE3	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
FE4	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
FE5	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
FE6	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
FX7	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
FX8	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
GE1	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms
GE2	Disable ▼	Disable ▼	100 ms	500 ms	3000 ms

Figure 124 Port GMRP Configuration

### GMRP Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the GMRP function on the port.

### Agent Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the GMRP agent function on the port.



#### Caution:

- Agent port cannot propagate agent entry.
- To enable the GMRP agent function on a port, you need to enable the GMRP function first.

### Hold Timer

Range: 100ms~327600ms

Default: 100ms

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

### Join Timer

Range: 100ms~327600ms

Default: 500ms

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

### Leave Timer

Range: 100ms~327600ms

Default: 3000ms

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

3. Add a GMRP agent entry, as shown in the following figure.

**GMRP Agent Set**

MAC	<input style="width: 95%;" type="text" value="010000000001"/>	
VLAN ID	<input style="width: 95%;" type="text" value="1"/>	(1-4093)

**Port List**

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

**Member Port List**

	FE1	
--	-----	--

Apply

<<

>>

**Source Port List**

--	--	--

Help

Figure 125 GMRP Agent Entry Configuration

## MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

Function: Configure the MAC address of multicast group. The lowest bit of the first byte is 1.

### VLAN ID

Options: all created VLAN numbers

Function: Configure the VLAN ID for the GMRP agent entry.

Description: GMRP agent entry can only be forwarded from the propagation port with the VLAN ID same as this entry's VLAN ID.

### Member Port List

Select the member port for the agent entry. You can select the port only from GMRP agent-enabled ports.

### Source Port List

Options: all GMRP agent-enabled ports

4. View, modify, or delete a GMRP agent entry, as shown in the following figure.

**GMRP Agent List**

Index	MAC	VLAN ID	Member Port
<input type="radio"/> 1	01-00-00-00-00-01	1	FE1
<input type="radio"/> 2	01-00-00-00-00-02	2	FE1

Figure 126 GMRP Agent Entry Operations

A GMRP agent entry consists of the MAC address, VLAN ID, and member port the agent. To delete an entry, select the entry and click <Delete>. To modify an entry, select the entry and click <Modify>.

5. View the multicast members of this agent entry on the connected neighbor device are displayed, as shown in the following figure.

The following conditions shall be met.

- GMRP is enabled on the inter-connected devices.
- The two ports that connect the devices must be propagation ports, and the VLAN ID of the propagation port on the local device must be identical with

that in the agent entry.

GMRP Dynamic Multicast List			
Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	FE3

Figure 127 GMRP Dynamic Multicast Table

### GMRP Dynamic Multicast List

Portfolio: {Index, Multicast MAC, VLAN ID, Member Port}

Function: View GMRP dynamic multicast entries.

### 6.22.5 Typical Configuration Example

As shown in the following figure, Switch A and Switch B are connected through port 2. Port 1 of Switch A is set to an agent port and generates two multicast entries:

- MAC address: 01-00-00-00-00-01, VLAN: 1
- MAC address: 01-00-00-00-00-02, VLAN: 2

After configuring different VLAN attributes on ports, observe the dynamic registration between switches and multicast information update.

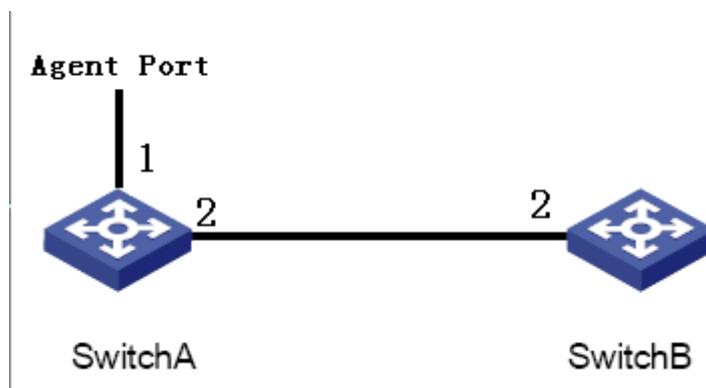


Figure 128 GMRP Networking

#### Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as shown in Figure 123.
2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; set the timers to default values, as shown in Figure 124.

3. Configure agent multicast entry. Set <MAC address, VLAN ID, Member port> to <01-00-00-00-00-01, 1, 1> and <01-00-00-00-00-02, 2, 1>, as shown in Figure 125.

#### **Configuration on Switch B:**

1. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 123.
2. Enable GMPR function on port 2; set the timers to default values, as shown in Figure 124.

The following table lists the dynamically learned GMRP multicast entries on Switch B.

Table 10 Dynamic Multicast Entries

Attribute of Port 2 on Switch A	Attribute of Port 2 on Switch B	Multicast Entries Received on Switch B
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

## **6.23 RMON**

### **6.23.1 Overview**

Based on SNMP architecture, Remote Network Monitoring (RMON) allows network management devices to proactively monitor and manage the

managed devices. An RMON network usually involves the Network Management Station and Agents. The NMS manages Agents and Agents can collect statistics on various traffic of ports.

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

### **6.23.2 RMON Groups**

RMON (RFC2819) defines multiple RMON groups. The series devices support statistics group, history group, event group, and alarm group in public MIB. Each group supports up to 32 entries.

#### **➤ Statistics group**

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

#### **➤ History group**

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

### ➤ Event group

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

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

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

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

None: indicates no action.

### ➤ Alarm group

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



#### Caution:

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

## 6.23.3 Web Configuration

1. Configure the statistics table, as shown in the following figure.

**Set Statistics Information**

Index	Owner	DataSource
1	a	ifIndex.2 ▼

Figure 129 RMON Statistics

**Index**

Range: 1~65535

Function: Configure the number of the statistics entry.

**Owner**

Range: 1~32 characters

Function: Configure the name of the statistics entry.

**Data Source**

Options: ifIndex.portid

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

2. Configure the history table, as shown in the following figure.

Index	<input type="text" value="2"/>
DataSource	<input type="text" value="ifIndex.2"/> ▼
Owner	<input type="text" value="b"/>
Sampling Number	<input type="text" value="10"/>
Sampling Space	<input type="text" value="20"/>

Figure 130 RMON History Table

**Index**

Range: 1~65535

Function: Configure the number of the history entry.

**Data Source**

Options: ifIndex.portid

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

**Owner**

Range: 1~32 characters

Function: Configure the name of the history entry.

**Sampling Number**

Range: 1~65535

Function: Configure the sampling times of the port.

**Sampling Space**

Range: 1~3600s

Function: Configure the sampling period of the port.

3. Configure the event table, as shown in the following figure.

Index	<input type="text" value="3"/>
Owner	<input type="text" value="c"/>
Event Type	<input type="text" value="LogandTrap"/> ▼
Event Description	<input type="text" value="alarm"/>
Event Community	<input type="text" value="public"/>

Figure 131 RMON Event Table

### Index

Range: 1~65535

Function: Configure the index number of the event entry.

### Owner

Range: 1~32 characters

Function: Configure the name of the event entry.

### Event Type

Options: NONE/LOG/Snmp-Trap/Log and Trap

Default: NONE

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

### Event Description

Range: 1~127 characters

Function: Describe the event.

### Event Community

Range: 1~127 characters

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

4. Configure the alarm table, as shown in the following figures.

Index	<input type="text" value="4"/>
OID	<input type="text" value="1.3.6.1.2.1.2.2.1.11"/>
Owner	<input type="text" value="d"/>
DataSource	<input type="text" value="ifIndex.2"/> ▼
Sampling Type	<input type="text" value="Absolute"/> ▼
Alarm Type	<input type="text" value="RisingAlarm"/> ▼
Sampling Space	<input type="text" value="20"/>
Rising Threshold	<input type="text" value="100"/>
Falling Threshold	<input type="text" value="20"/>
Rising EventIndex	<input type="text" value="3"/>
Falling EventIndex	<input type="text" value="3"/>

Figure 132 RMON Alarm Table

**Index**

Range: 1~65535

Function: Configure the number of the alarm entry.

**OID**

Indicates the OID of the current MIB node.

**Owner**

Range: 1~32 characters

Function: Configure the name of the alarm entry.

**Data Source**

Options: ifIndex.portid

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

**Sampling Type**

Options: Absolute/Delta

Default: Absolute

Function: Configure the comparison mode for the sampling value and threshold.

Description: Absolute indicates comparing the sampling value with the threshold. Delta indicates comparing the sampling value deducted by the last

sampling value with the threshold.

**Alarm Type**

Options: RisingAlarm/FallingAlarm/RisOrFallAlarm

Default: RisingAlarm

Function: Select the alarm type, including the rising edge alarm, falling edge alarm, and both rising edge and falling edge alarms.

**Sampling Space**

Range: 1~65535

Function: Configure the sampling period. The value should be identical with that in the history table.

**Rising Threshold**

Range: 1~65535

Function: Configure the rising edge threshold. When the sampling value exceeds the threshold and the alarm type is set to RisingAlarm or RisOrFallAlarm, an alarm is generated and the rising event index is triggered.

**Falling Threshold**

Range: 1~65535

Function: Configure the falling edge threshold. When the sampling value is lower than the threshold and the alarm type is set to FallingAlarm or RisOrFallAlarm, an alarm is generated and the falling event index is triggered.

**Rising Event Index**

Range: 0~65535

Function: Configure the index of the rising event, that is, processing mode for rising edge alarms.

**Falling Event Index**

Range: 0~65535

Function: Configure the index of the falling event, that is, processing mode for falling edge alarms.

## 6.24 Unicast Address Configuration and Query

### 6.24.1 Overview

When forwarding a packet, the switch searches for the forwarding port in the MAC address table based on the destination MAC address of the packet.

A MAC address can be either static or dynamic.

A static MAC address is configured by a user. It has the highest priority (not overridden by dynamic MAC addresses) and is permanently valid.

Dynamic MAC addresses are learned by the switch in data forwarding. They are valid only for a certain period. The switch periodically updates its MAC address table. When receiving a data frame to be forwarded, the switch learns the source MAC address of the frame, establishes a mapping with the receiving port, and queries the forwarding port in the MAC address table based on the destination MAC address of the frame. If a match is found, the switch forwards the data frame from the corresponding port. If no match is found, the switch broadcasts the frame in its broadcast domain.

The switch supports a maximum of 256 static unicast entries.

### 6.24.2 Web Configuration

1. Add a static MAC address entry, as shown in the following figure.

**Set FDB Unicast**

MAC	VLAN ID (1~4093)	Member Port
ecde12345678	2	FE2 ▼

Apply
Help

Figure 133 Adding a Static FDB Unicast Entry

#### MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

Function: Configure the unicast MAC address. The lowest bit in the first byte is 0.

**VLAN ID**

Options: all created VLAN IDs

**Member Port**

Options: all switch ports

Function: Select the port for forwarding packets destined for the MAC address.

The port must be in the specified VLAN.

2. View the static unicast address list, as shown in the following figure.

**FDB Unicast Mac List**

Index	MAC	VLAN ID	Member Port
<input type="radio"/>	ec:de:12:34:56:78	2	FE2
<input type="radio"/>	00:00:01:01:01:01	1	FE1

Figure 134 Viewing Static FDB Table

Select an entry. You can delete or modify the entry.

3. View the dynamic unicast address list, as shown in the following figure.

Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	00:00:5e:00:01:01	1	FE6
2	00:00:5e:00:01:42	1	FE6
3	c8:9c:dc:a9:00:1c	1	FE6
4	d0:27:88:68:97:a8	1	FE6
5	c8:9c:dc:57:3e:96	1	FE6
6	00:24:8c:74:97:4b	1	FE6
7	00:24:8c:7e:92:9e	1	FE6
8	c8:9c:dc:a8:c0:8e	1	FE6
9	f0:7d:68:fa:b5:84	1	FE6
10	d4:be:d9:b9:4d:0d	1	FE6
11	d0:27:88:45:ff:b5	1	FE6
12	00:1d:7d:cf:77:6a	1	FE6
13	00:24:8c:9e:56:26	1	FE6
14	d0:27:88:45:ff:25	1	FE6
15	00:1a:92:d6:e7:7f	1	FE6
16	00:40:05:12:9d:a1	1	FE6
17	00:79:63:00:72:00	1	FE6
18	d0:27:88:46:0a:e8	1	FE6
19	00:1a:92:74:fe:8a	1	FE6
20	00:50:c2:22:60:e0	1	FE6

Figure 135 Dynamic Unicast FDB Table

## Appendix: Acronyms

Acronym	Full Spelling
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
CST	Common Spanning Tree
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management Station
OID	Object Identifier
QoS	Quality of Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol

SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
ToS	Type of Service
VLAN	Virtual Local Area Network
WRR	Weighted Round Robin