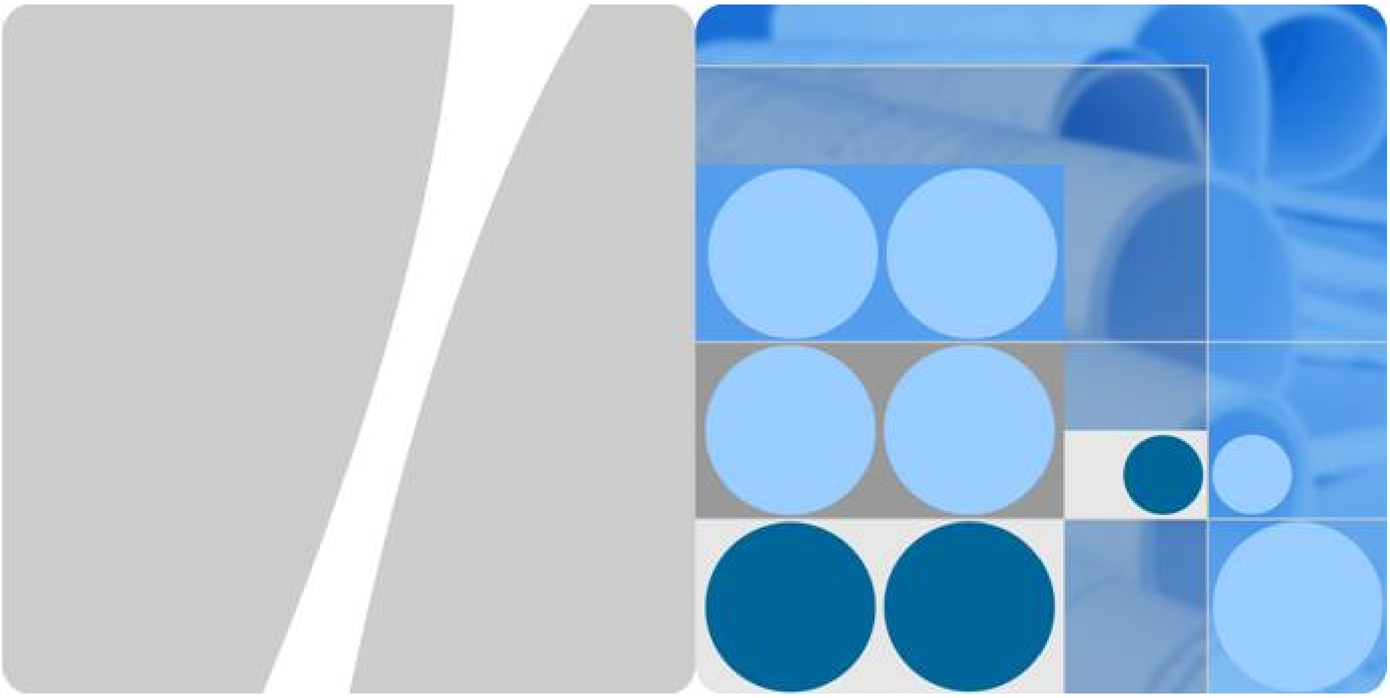


Quidway S2700&S3700&S5700&S6700 Series Ethernet Switches

V100R006C00

Web System Guide

Issue 01

Date 2011-07-15

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2011. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the configuration and maintenance of S2700,S2752,S3700,S5700, and S6700 through the web network management system. The web network management system provides the functions of viewing device information and managing the entire system, interfaces, services, ACL, QoS, routes, security, and tools.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
⚠ CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
🔑 TIP	Indicates a tip that may help you solve a problem or save time.
📖 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 01 (2011-07-15)

Initial commercial release.

Contents

About This Document....ii

1 Client Configuration....1

1.1 Logging In to the Web System Client....2

1.2 Web User Management....3

1.2.1 Adding a User Account....3

1.2.2 Changing Password....3

1.2.3 Deleting a User Account....4

1.3 Understanding the Web System Client User Interface....4

1.3.1 Window Layout....4

1.3.2 Navigation Tree....5

1.3.3 Buttons....8

1.3.4 GUI Elements....9

1.4 User Timeout....10

1.5 Saving Configuration....11

1.6 Logging Out of the Web System....11

2 Device Summary....12

2.1 Panel....13

2.2 Switch Information....13

2.3 Switch Health....14

2.4 Trends....15

3 System Management....17

3.1 Initialize....19

3.2 Reboot....19

3.3 Software Upgrade....21

3.4 Patch....22

3.4.1 Run Patch....22

3.4.2 Uninstall Patch....24

3.5 File System Management....24

3.5.1 File System Management....24

3.5.2 Recycle Bin....27

3.6 System Configuration....28

3.6.1 System Time....28

3.6.2 System Settings....29
3.7 PoE....30
3.7.1 Global Parameter Settings....31
3.7.2 Interface Parameter Settings....32
3.7.3 PoE Power Supply Information....34
3.8 DNS....35
3.8.1 Dynamic DNS Entry Table....35
3.8.2 DNS Settings....36
3.8.3 Domain Name Settings....37
3.8.4 Enable Dynamic Domain Name Resolution....38
3.9 Stacking....39
4 Interface Management....43
4.1 Ethernet....44
4.1.1 Basic Attributes....44
4.1.2 Statistics on Interface....47
4.2 Eth-Trunk....48
4.2.1 Eth-Trunk....49
4.2.2 System LACP Priority....56
4.3 VLANIF....57
4.4 LoopBack....60
5 Service Management....63
5.1 VLAN....65
5.1.1 VLAN....65
5.1.2 Hybrid Port....67
5.1.3 Access Port....69
5.1.4 Trunk Port....70
5.1.5 VLANIF Port....72
5.2 MAC....76
5.2.1 MAC Table....76
5.2.2 MAC Aging Time....77
5.2.3 MAC Learning....78
5.2.4 Static MAC Table....81
5.2.5 Blackhole MAC Table....83
5.2.6 Sticky MAC....84
5.3 STP....87
5.3.1 STP Information....87
5.3.2 STP Global....88
5.3.3 STP Interface....92
5.3.4 MST Region....95
5.4 Voice VLAN....97
5.4.1 Voice VLAN....97
5.4.2 Voice VLAN OUI....99

5.4.3 Aging Time....100
5.5 DHCP....101
5.5.1 DHCP....101
5.5.2 Configure Global Address Pool....102
5.5.3 Configure VLANIF Interface Address Pool....105
5.5.4 Configure DHCP Delay....110
5.6 ARP....112
5.6.1 ARP Table....112
5.6.2 Static ARP Table....114
5.6.3 ARP Attribute....117
5.7 VRRP....118
5.7.1 VRRP....118
5.7.2 VRRP Attribute....121
5.8 IGMP Snooping....122
5.8.1 Global IGMP Snooping....122
5.8.2 Configure IGMP Snooping in VLAN....123
6 ACL....126
6.1 Effective Period....127
6.2 ACL....129
7 QoS....148
7.1 Traffic Management....149
7.1.1 Traffic Classifier....149
7.1.2 Traffic Behavior....153
7.1.3 Traffic Policy....161
7.1.4 Apply Traffic Policy....163
7.2 Interface-based Rate Limit....164
7.2.1 View Rate Limit....164
7.2.2 Configure Rate Limit....165
7.3 Traffic Shaping....166
7.3.1 View Traffic Shaping....166
7.3.2 Configure Traffic Shaping....167
7.4 Congestion Management....168
7.4.1 View Scheduling....168
7.4.2 Configure Scheduling....169
7.5 Priority Mapping....170
7.5.1 Priority Mapping....170
7.5.2 Trust Priority....177
8 IP Routing....181
8.1 IPv4 Route....182
8.1.1 IPv4 Routing Tables....182
8.1.2 IPv4 Static Route....182

8.1.3 Global Parameter Settings....184

9 Security....186

9.1 Port Isolation....187

9.1.1 Bidirectional Isolation....187

9.1.2 Unidirectional Isolation....189

9.2 Static User Binding....191

9.2.1 View Static User Binding....191

9.2.2 Configure Static User Binding....192

9.3 AAA....194

9.3.1 AAA Scheme....194

9.3.2 Service Scheme....197

9.3.3 RADIUS Configurations....199

9.3.4 Domain....205

9.3.5 User....207

9.4 802.1x....211

9.4.1 802.1X Global Settings....211

9.4.2 802.1X Interface Settings....214

9.5 MAC Authen....217

9.5.1 Global Configuration....217

9.5.2 MAC Authentication on Interface....220

10 Tools....223

10.1 Ping....224

10.2 Tracert....225

10.3 VCT....226

Copyright © Huawei Technologies Co., Ltd.

1 Client Configuration

About This Chapter

To facilitate the maintenance and configuration of the S2700,S2752,S3700,S5700, and S6700, Huawei provides the Web network management system (short for Web system). You can log in to the Web system client to maintain and configure devices through the graphic user interface (GUI).

This chapter describes basic operations that you can perform on the Web system. It helps you quickly understand the operations and functions on the Web system.

1.1 Logging In to the Web System Client
Before configuring the switch, you must log in to the Web system client.

1.2 Web User Management
The switch provides default user name and password for your first login. To facilitate user management, the Web system enables you to add user accounts, change password, and delete user accounts.

1.3 Understanding the Web System Client User Interface
The following sections help you understand the Web system client user interface and improve your operation efficiency.

1.4 User Timeout
If you do not perform any operations on the Web system GUI for a long time, you are logged out and the login page is displayed.

1.5 Saving Configuration
After performing configuration, you need to save the configuration data.

1.6 Logging Out of the Web System
To protect security of user accounts and switches, log out of the Web system immediately after you finish the configurations.

Copyright © Huawei Technologies Co., Ltd.

1.1 Logging In to the Web System Client

Before configuring the switch, you must log in to the Web system client.

Context

- Before logging in to the Web system client, ensure that the switch has been commissioned and the Web system server is enabled on the switch.
- The Web system client connects to the switch through HTTP; therefore, you must log in to the Web system client through HTTP.
- The Web system client supports the Microsoft Internet Explorer 6 (IE6) and Firefox 3.0, or later versions. The Web system client described in this document uses the IE6.

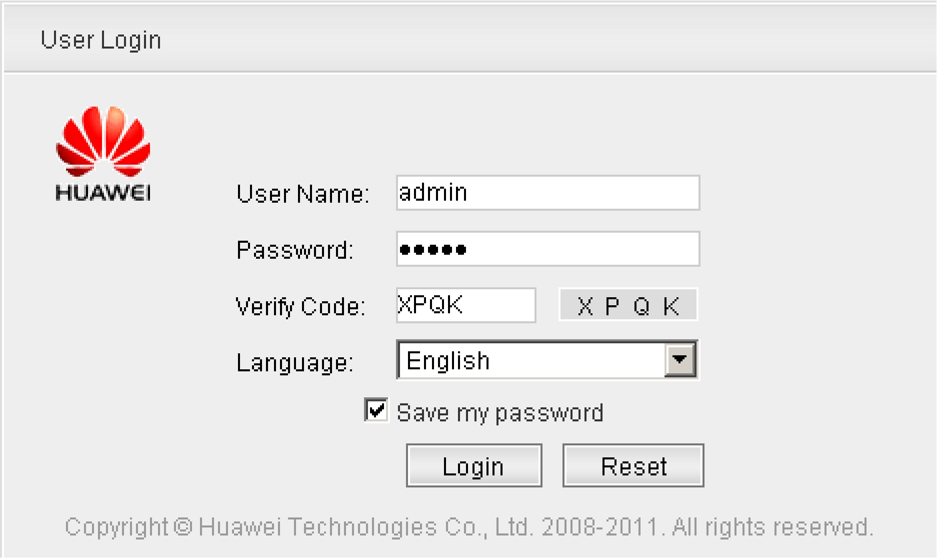
Procedure

Step 1 Open Microsoft Internet Explorer 6.0 on the client.

Step 2 Enter the universal resource locator (URL) of the Web system client in the address bar and press **Enter**. The **User Login** dialog box is displayed, as shown in **Figure 1-1**.

The URL is in the format **http://IP/view/login.html**, for example, **http://10.164.19.131/view/login.html**.

Figure 1-1 Login



User Login

User Name: admin

Password: •••••

Verify Code: XPQK X P Q K

Language: English

☑ Save my password

Copyright © Huawei Technologies Co., Ltd. 2008-2011. All rights reserved.

Step 3 Enter values in **User Name**, **Password**, and **Verify Code**.

- The local switch provides a default account. The user name and password of the account are **admin**.
- To create, change, or delete user names and passwords, choose **Security** > **AAA** > **User**.
- If your user level is 0, you can view only the **Ping** and **Tracert** pages after logging in to the client.

Step 4 Choose a language, for example, **English**.

- The Web system client of the current version supports Chinese and English.
- After logging in to the client, you can select another language from the **Language** drop-down list on the top right corner of the page.

Step 5 Click **Login**.

📖 **NOTE**

If you select **Save my password** before clicking **Login**, you do not need to enter the user name and password at next login.

After you log in to the Web system, the main page is displayed. For details about the main page, see **1.3.1 Window Layout**.

----End

1.2 Web User Management

The switch provides default user name and password for your first login. To facilitate user management, the Web system enables you to add user accounts, change password, and delete user accounts.

The following sections describe the operations of user management. To configure user management, choose **Security** > **AAA** > **User Management**.

1.2.1 Adding a User Account

You can add user accounts. Then the switch can authenticate and authorize the users who log in to the switch according to the user information you configured.

Context

You can add user accounts only when your user level is greater than 0.

Procedure

Step 1 Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.

Step 2 Click **New** to open the **Create User** page.

Step 3 Enter **User Name**, **Password**, and **Confirm Password** and set the access type to **http**. Retain the default values of other parameters.

Step 4 Click **OK**.

----End

1.2.2 Changing Password

You can change passwords in the web system.

Context

You can change the passwords only when your user level is greater than 0.

Procedure

Step 1 Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.

Step 2 Select a record that you want to modify and click ✎ to open the **Modify User** page.

Step 3 Enter **Password** and **Confirm Password**.

Step 4 Click **OK**.

----End

1.2.3 Deleting a User Account

You can delete user accounts from the Web system.

Context

You can delete user accounts only when your user level is greater than 0.

Procedure

Step 1 Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.

Step 2 Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

Step 3 Click **OK**.

----End

1.3 Understanding the Web System Client User Interface

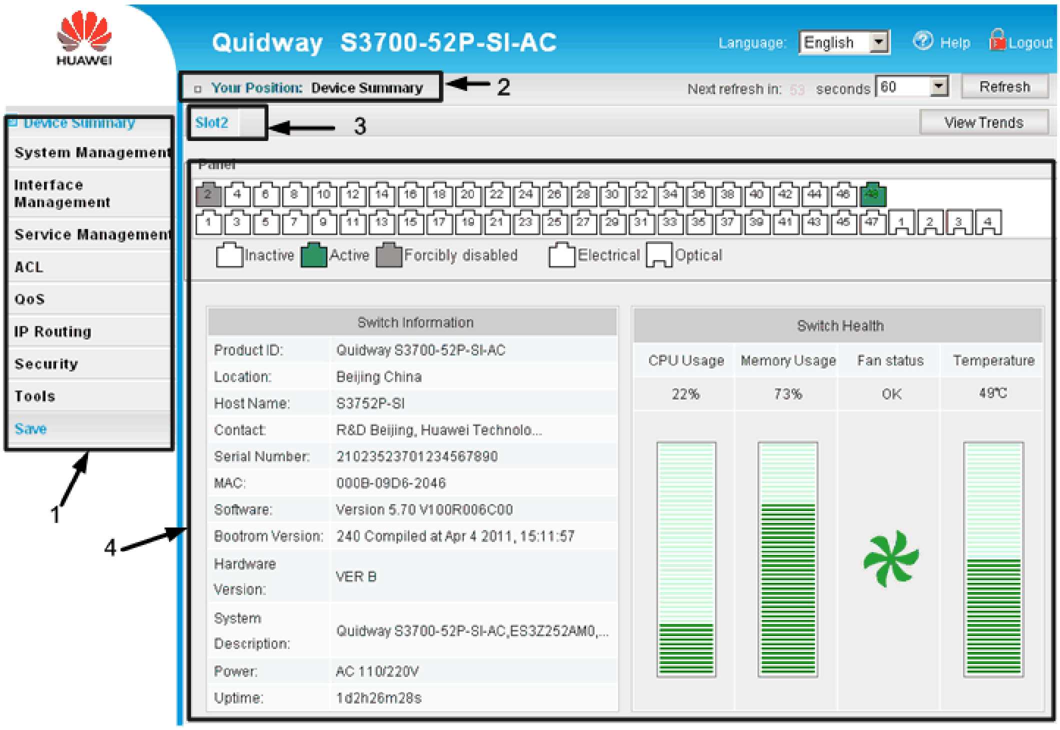
The following sections help you understand the Web system client user interface and improve your operation efficiency.

1.3.1 Window Layout

The layout and style of the Web system client GUI are described in the section.

Figure 1-2 shows a typical operation user interface of the Web system.

Figure 1-2 Device Summary



Switch Information

Product ID:	Quidway S3700-52P-SI-AC
Location:	Beijing China
Host Name:	S3752P-SI
Contact:	R&D Beijing, Huawei Technolo...
Serial Number:	21023523701234567890
MAC:	000B-09D6-2046
Software:	Version 5.70 V100R006C00
Bootrom Version:	240 Compiled at Apr 4 2011, 15:11:57
Hardware Version:	VER B
System Description:	Quidway S3700-52P-SI-AC,ES3Z252AM0,...
Power:	AC 110/220V
Uptime:	1d2h26m28s

Switch Health

CPU Usage	Memory Usage	Fan status	Temperature
22%	73%	OK	49℃

No.	Description
1	Navigation tree
2	Your location
3	Tabs
4	Configuration area

1.3.2 Navigation Tree

The navigation tree consists of nine nodes: Device Summary, System Management, Interface Management, Service Management, ACL, QoS, IP Routing, Security, and Tool.

Each node has subnodes, as described in **Table 1-1**.

Table 1-1 Description of the Web system navigation tree

Node	Subnode	Description
Device Summary	Panel	Displays information about the device panel.
	Switch Information	Displays the product type, location, software version, and hardware version of the switch.
	Switch Health	Displays the current CPU usage, memory usage, temperature, and fan status of the switch.
	Trends	Displays the CPU usage, memory usage, temperature, and port usage of the switch according to your selection.

Node	Subnode	Description
System Management	Factory Defaults	Restores the factory settings of the switch.
	Restart	Chooses the configuration file for next startup of the switch.
	Software Upgrade	Upgrades the software of the switch.
	Patch	Loads the patch file to the switch through TFTP.
	File System Management	Manages files, including uploading files to the switch, downloading files from the switch, and restoring or permanently deleting files in the recycle bin.
	System Configuration	Sets the system information such as system time and maintenance information.
	PoE	Configures and queries global PoE information and PoE on interfaces.
	DNS	Configures and queries dynamic DNS entries, DNS server, domain name suffix, and dynamic domain name resolution function.
	Stacking	Configures and queries the stacking function. **NOTE** The S2700EI, S2700SI or S2752EI switches do not support the function.
Interface Management	Ethernet	Configures and queries basic attributes of interfaces and traffic statistics on the interfaces.
	Eth-Trunk	Configures and queries Eth-Trunk interfaces and LACP priority.
	VLANIF	Configures and queries VLANIF interfaces. **NOTE** The S2700EI,S2700SI or S2752EI switches do not support the function.
	LoopBack	Configures and queries the loopback interfaces.
Service Management	VLAN	Configures and queries VLANs, interfaces, and VLANIF interfaces.
	MAC	Configures and queries MAC address table, MAC address aging time, MAC address learning function, static MAC address entries, blackhole MAC address entries, and sticky MAC function.
	STP	Configures and queries global STP information, STP on interfaces, and domains. **NOTE** The S2700SI series switches do not support this function.

Node	Subnode	Description
	Voice VLAN	Configures and queries voice VLAN, OUI, and aging time. **NOTE** The S2700SI series switches do not support this function.
	DHCP	Configures and queries DHCP global address pool, address pool on VLANIF interface, and DHCP relay. **NOTE** The S2700SI, S2700EI switches do not support the function.
	ARP	Configures and queries ARP entries, static ARP entries, and ARP parameters. **NOTE** The S2700EI,S2700SI or S2752EI switches do not support the function.
	VRRP	Configures and queries VRRP information. **NOTE** The S2700EI, S2700SI, S2752EI, S5700SI or S3700SI switches do not support the function.
	IGMP Snooping	Configures and queries global IGMP information and IGMP snooping of VLANs.
ACL	Effective Period	Configures and queries the ACL effective period.
	ACL	Configures and queries ACL information.
QoS	Traffic Management	Configures and queries the traffic classifier-based QoS function, including traffic classification, traffic behavior, traffic policy, and application of traffic policy.
	Limit Rate	Configures and queries the interface rate limiting function.
	Traffic Shaping	Configures and queries the traffic shaping function.
	Congestion Management	Configures and queries congestion management on interfaces. **NOTE** The S5700SI,S2700EI,S2700SI or S2752EI switches do not support the function.
	Priority Mapping	Configures and queries the priority mapping and trusted interface functions. **NOTE** The S2700EI,S2700SI or S2752EI switches do not support the function.
IP Routing	IPv4 Route	Configures and queries IPv4 routes, including IPv4 static routes and global IPv4 routing information.

Node	Subnode	Description
Security	Port isolation	Configures and queries isolation mode and isolation directions. **NOTE** The S2700SI series switches do not support this function.
	Static user binding	Configures and queries static user binding information. **NOTE** The S2700SI series switches do not support this function.
	AAA **NOTE** The AAA configuration function is equivalent to the user management function of S2700SI and S2700EI.	Configures and queries the security functions, including authentication, authorization, and accounting (AAA), service templates, RADIUS templates, RADIUS authentication and accounting servers, RADIUS authorization servers, domain management, and user data management.
	802.1X	Configures and queries global 802.1X parameters and 802.1X parameters on interfaces. **NOTE** The S2700SI or S2700EI switches do not support the function.
	MAC Authen	Configures and queries global MAC address authentication and MAC address authentication on interfaces. **NOTE** The S2700SI or S2700EI switches do not support the function.
Tool	Ping	The ping function.
	Tracert	The tracert function.
	VCT	The VCT function.

1.3.3 Buttons

The buttons that you usually use on the Web system GUI are described in this section.

Table 1-2 describes the buttons and functions.

Table 1-2 Button description

Button	Function
OK	Saves configurations or confirms the displayed information. **NOTE** If you click **OK** on a pop-up dialog box, the dialog box is closed.

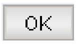
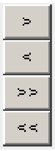
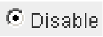
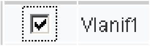
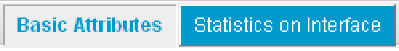
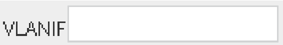
Button	Function
Apply	Saves configurations or confirms the displayed information. **NOTE** If you click **Apply** on a pop-up dialog box, the dialog box is not closed.
Query	Displays information that you queried.
Configure	Configures a selected record.
Cancel	Cancels the current configuration.
Refresh	Refreshes the current page.
New	Creates a record on the current page.
Delete	Deletes a selected record.
📝	Modifies a selected record.
Details	Displays details about a selected record.
Clear Configuration	Deletes the configuration data of a selected record.

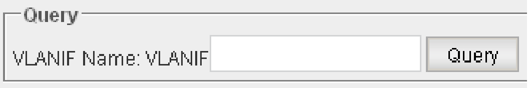
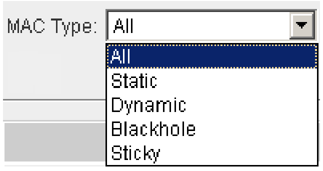
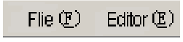
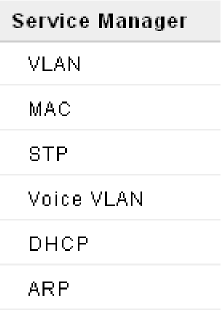
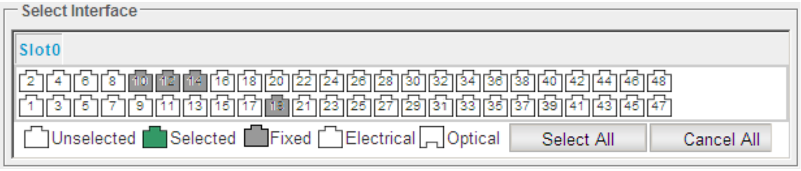
1.3.4 GUI Elements

The elements that you usually use on the Web system GUI are described in this section.

Table 1-3 describes the elements that you usually use on the Web system GUI.

Table 1-3 GUI elements

Name	Element
Button	
Move button	
Option button	
Check box	
Tab	
Text box	

Name	Element
Group box	
Drop-down list box	 MAC Type: All All Static Dynamic Blackhole Sticky
Menu	
Navigation tree	 Service Manager VLAN MAC STP Voice VLAN DHCP ARP
Sort button	Default: ▽ Descending: ▼ Ascending: ▲
Time setting	📅
Mandatory option	*
Interface panel	 Select Interface Slot0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 Unselected Selected Fixed Electrical Optical Select All Cancel All

1.4 User Timeout

If you do not perform any operations on the Web system GUI for a long time, you are logged out and the login page is displayed.

Figure 1-1 shows the login page. If you need to continue operations, log in again.

NOTE

- By default, the timeout time of a login user is 20 minutes.
- The timeout time is set on the **3.6.2 System Settings** page.

1.5 Saving Configuration

After performing configuration, you need to save the configuration data.

⚠ **CAUTION**

If you do not save the configuration data, the configuration that you made will be lost after reboot.

To save configurations, you can:

- Click **OK** or **Apply** to save the configuration data to memory.
- Click Save in the navigation tree to save all the configuration data to the configuration file.

1.6 Logging Out of the Web System

To protect security of user accounts and switches, log out of the Web system immediately after you finish the configurations.

You can log out of the Web system in either of the following ways:

- Click ☒ on the top right corner of the page to close the browser.
- Click 🔒Logout on any page of the Web system.

2 Device Summary

About This Chapter

The following sections describe the subnodes under the **Device Summary** node, including **Panel**, **Switch Information**, **Switch Health**, and **Trends**.

2.1 Panel
This subnode provides information about the device panel.

2.2 Switch Information
This subnode displays the product type, location, software version, and hardware version of the switch.

2.3 Switch Health
This subnode displays the current CPU usage, memory usage, temperature, and fan status of the switch.

2.4 Trends
This subnode displays the CPU usage, memory usage, temperature, and port usage of the switch according to your selection. **The S2700EI or S2700SI switches do not support the function.**

2.1 Panel

This subnode provides information about the device panel.

Context

The panel area on the Web system page displays information about each port of the selected switch, including:

- Number of ports
- Operating mode of each port

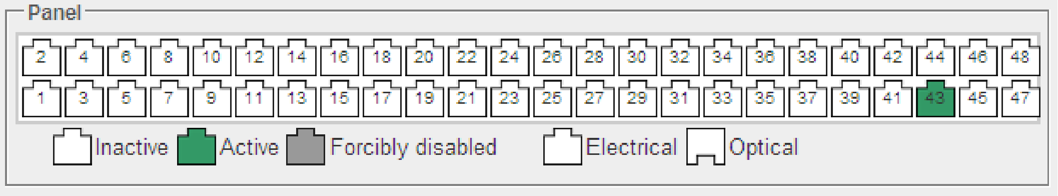
NOTE

You can place the cursor on a port to view the type, rate, and status of the port.

Procedure

Step 1 Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the **Panel** tab page, as shown in **Figure 2-1**.

Figure 2-1 Panel



Step 2 Select a refresh interval from the drop-down list before **Refresh**. The value Manual indicates not refresh. The default interval is 60 seconds.

Step 3 Click **Refresh**. Then the Web system synchronizes data with the switch and refreshes the information on the page.

NOTE

If you click a port icon, the configuration information of each port is displayed. For details about the displayed information, see **Configure basic attributes**.

----End

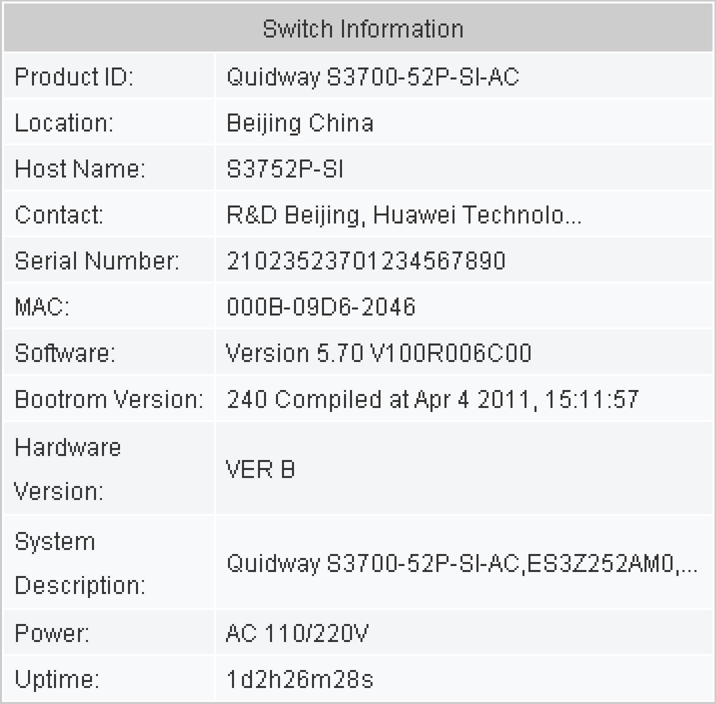
2.2 Switch Information

This subnode displays the product type, location, software version, and hardware version of the switch.

Procedure

Step 1 Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the **Switch Information** tab page, as shown in **Figure 2-2**.

Figure 2-2 Switch Information



Switch Information	
Product ID:	Quidway S3700-52P-SI-AC
Location:	Beijing China
Host Name:	S3752P-SI
Contact:	R&D Beijing, Huawei Technolo...
Serial Number:	210235237012345 67890
MAC:	000B-09D6-2046
Software:	Version 5.70 V100R006C00
Bootrom Version:	240 Compiled at Apr 4 2011, 15:11:57
Hardware Version:	VER B
System Description:	Quidway S3700-52P-SI-AC,ES3Z252AM0,...
Power:	AC 110/220V
Uptime:	1d2h26m28s

----End

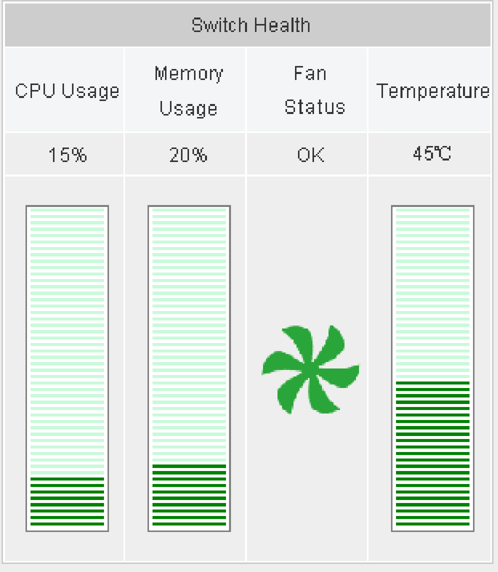
2.3 Switch Health

This subnode displays the current CPU usage, memory usage, temperature, and fan status of the switch.

Procedure

Step 1 Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the **Switch Health** tab page, as shown in **Figure 2-3**.

Figure 2-3 Switch Health



Switch Health

CPU Usage	Memory Usage	Fan Status	Temperature
15%	20%	OK	45℃

----End

2.4 Trends

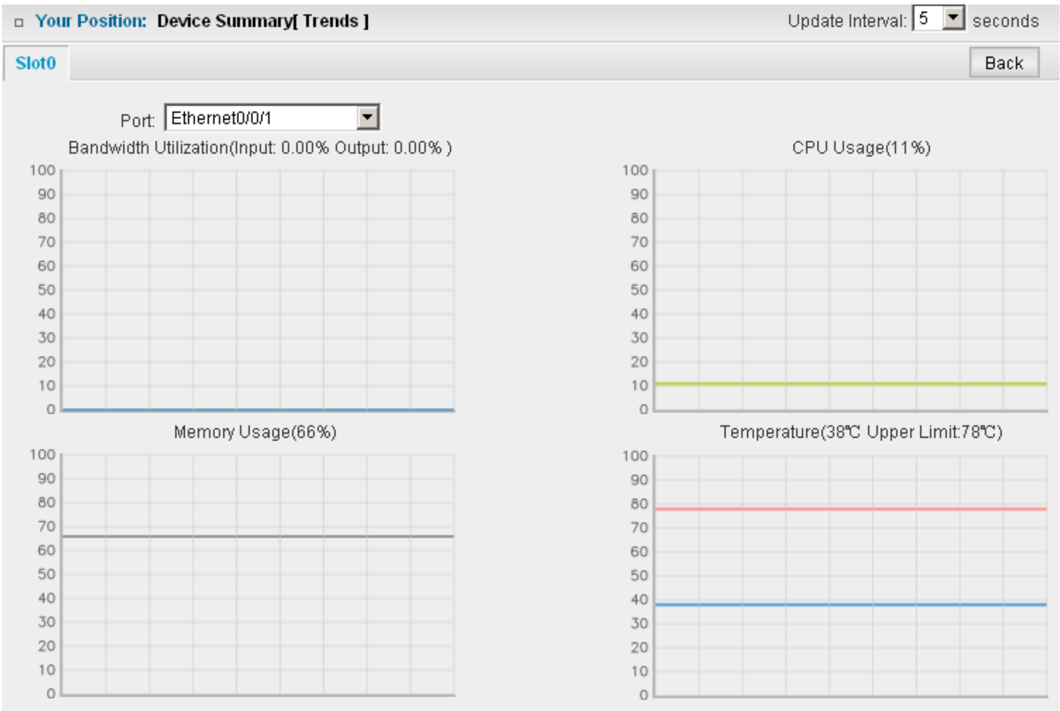
This subnode displays the CPU usage, memory usage, temperature, and port usage of the switch according to your selection. **The S2700EI or S2700SI switches do not support the function.**

Procedure

Step 1 Click **Device Summary** in the navigation tree to open the **Device Summary** page.

Step 2 Click **View Trends** on the top right corner of the page to open the **Trends** page, as shown in **Figure 2-4**.

Figure 2-4 Trends



Your Position: Device Summary[Trends]
Update Interval: 5 seconds
Slot0
Back
Port: Ethernet0/0/1
Bandwidth Utilization(Input: 0.00% Output: 0.00%)
CPU Usage(11%)
Memory Usage(66%)
Temperature(38℃ Upper Limit:78℃)
100
90
80
70
60
50
40
30
20
10
0

Step 3 Choose an index that you want to view.

Step 4 Click **Back** on the top right corner of the page to return to the **Device Summary** page.

----End

3 System Management

About This Chapter

This chapter describes the functions of system Management. The system configuration manager provides the following functions. You can query and configure the required functions.

3.1 Initialize
You can restore the factory settings of the system if necessary.

3.2 Reboot
You can specify the configuration file loaded to the switch at next startup.

3.3 Software Upgrade
When you upgrade software through TFTP, you need to upload the upgrade file on the TFTP server to the switch. After upgrade, the system restarts and uses the loaded file.

3.4 Patch
The following sections describe the functions of running and uninstalling patches.

3.5 File System Management
The following sections describe how to manage files, including uploading files to the switch, downloading files from the switch, and restoring or permanently deleting files in the recycle bin.

3.6 System Configuration
The following sections describe the configurations of the system time and system information.

3.7 PoE
The PoE configurations include global parameters, interface parameters, and PoE device information.

3.8 DNS
The following sections describe the configurations of dynamic DNS entries, domain name server, domain name suffix, and enabling dynamic domain name resolution.

3.9 Stacking
The stacking function connects multiple stacking-capable devices together to logically function as one device. Up to nine devices can be connected through stack cables in a ring or bus topology. All stacked devices logically function as one device to forward packets. There are three roles of the devices in a stack: master switch, standby switch, and slave switch. All of the three types of switches are called member switches. The Ethernet switches in a stack function as a device. You

Copyright © Huawei Technologies Co., Ltd.

can manage all the switches in a stack by using the master switch. **The S2700SI, S2700EI, S2752EI switches do not support the stacking function.**

3.1 Initialize

You can restore the factory settings of the system if necessary.

Context

If improper configurations have been performed on the switch, you can restore the factory settings of the switch.

WARNING

After you restore the factory settings of the switch, all the configurations that you have made on the switch will be deleted and cannot be restored.

Procedure

Step 1 Choose **System Management** > **Initialize** in the navigation tree to open the **Initialize** page.

Step 2 Click **Initialize**. A confirm dialog box is displayed.

Step 3 Click **OK**. After a reboot, you can log in to the Web system.

----End

3.2 Reboot

You can specify the configuration file loaded to the switch at next startup.

Context

The specified configuration file takes effect at next startup. Ensure that the configuration data is saved on the device before the reboot.

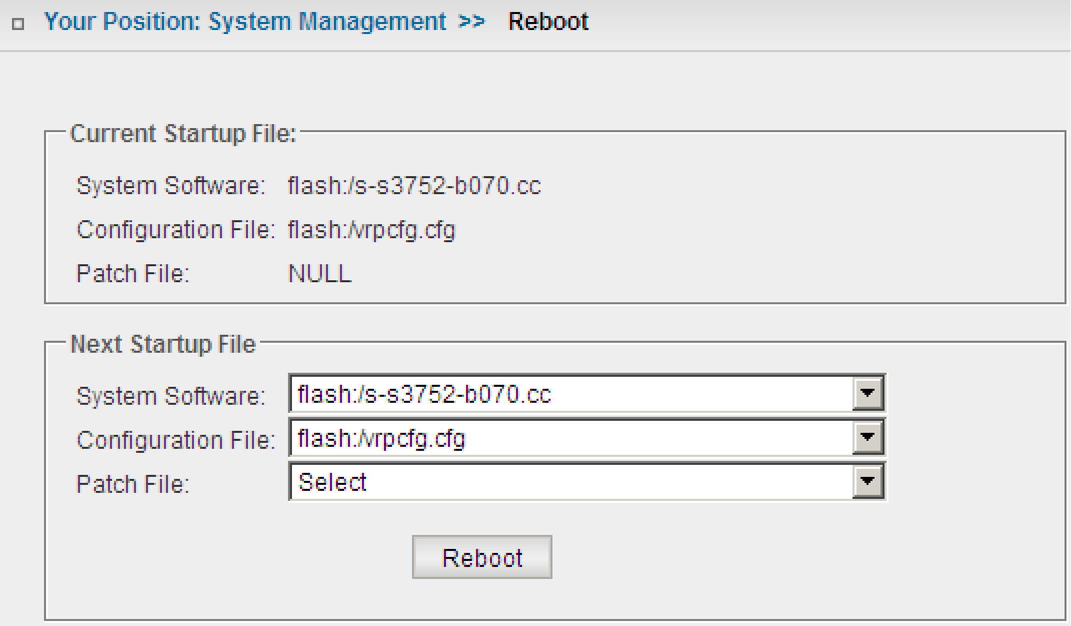
CAUTION

During the reboot, you are disconnected from the switch. If you have not saved the configuration data, the configuration data is lost after the reboot. Therefore, save the configuration before you reboot the system.

Procedure

Step 1 Choose **System Management** > **Reboot** in the navigation tree to open the **Reboot** page, as shown in **Figure 3-1**.

Figure 3-1 Reboot



Your Position: System Management >> Reboot

Current Startup File:

System Software: flash:/s-s3752-b070.cc

Configuration File: flash:/vrpcfg.cfg

Patch File: NULL

Next Startup File

System Software: flash:/s-s3752-b070.cc

Configuration File: flash:/vrpcfg.cfg

Patch File: Select

Table 3-1 describes the parameters on the **Reboot** page.

Table 3-1 Reboot

Parameter	Description
System Software	Specifies the system software for next startup.
Configuration File	Specifies the configuration file for next startup.
Patch File	Specifies the patch file for next startup.

Step 2 Select desired options from the drop-down lists and click **Reboot**. A pop-up dialog box is displayed, notifying you that communication between the system and the device will be interrupted during the reboot.

Step 3 Click **Yes** in the displayed dialog box.A dialog box is displayed to prompt you to save the configuration.

Step 4 Click **Save**. The system will reboot and save the configurations.

⚠ **WARNING**

If you click **Ignore**, the switch will reboot, but unsaved configurations will be lost.

----End

3.3 Software Upgrade

When you upgrade software through TFTP, you need to upload the upgrade file on the TFTP server to the switch. After upgrade, the system restarts and uses the loaded file.

Context

The Trivial File Transfer Protocol (TFTP) is a file transfer protocol.

The TFTP client supports file upload and download by using TFTP. TFTP uses the User Datagram Protocol (UDP) to transmit files, simplifying the transmission process.

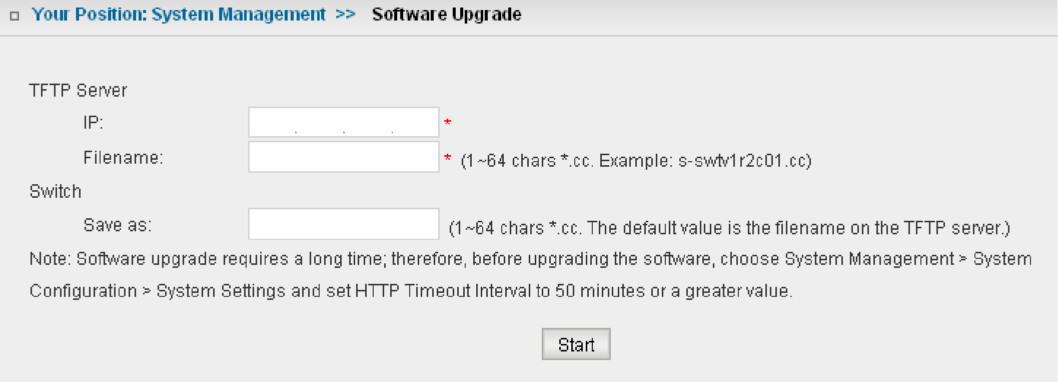
CAUTION

- Ensure that configurations are saved before upgrading software.
- Do not power off the switch during the upgrade.
- Software upgrade requires a long time; therefore, before upgrading the software, choose **System Management** > **System Configuration** > **System Settings** and set **Http Timeout Interval** to 50 minutes or a greater value.

Procedure

Step 1 Choose **System Management** > **Software Upgrade** in the navigation tree to open the **Software Upgrade** page, as shown in **Figure 3-2**.

Figure 3-2 Software Upgrade



Your Position: System Management >> Software Upgrade

TFTP Server

IP: *

Filename: * (1~64 chars *.cc. Example: s-swtv1r2c01.cc)

Switch

Save as: (1~64 chars *.cc. The default value is the filename on the TFTP server.)

Note: Software upgrade requires a long time; therefore, before upgrading the software, choose System Management > System Configuration > System Settings and set HTTP Timeout Interval to 50 minutes or a greater value.

Table 3-2 describes the parameters on the **Software Upgrade** page.

Table 3-2 Software Upgrade

Parameter		Description
TFTP Server	IP	Indicates the IP address of the TFTP server, for example, **10.10.10.1**. This parameter is mandatory.
	Filename	Indicates the name of the system software file that you want to load. The system software file is stored on the TFTP server and has the extension **.cc**, for example, **s-swtv1r2c01.cc**. This parameter is mandatory.
Switch	Save as	Indicates the name of the system software file loaded to the switch. The value is a string without spaces. The file name extension is **.cc**. If you do not specify the file name, the loaded file retains the original name.

Step 2 Set parameters and click **Start**. The system prompts you to save the configurations.

Step 3 After the upgrade, the system displays the login page.

Step 4 Enter the user name, password, and verification code to log in to the Web system.

----End

3.4 Patch

The following sections describe the functions of running and uninstalling patches.

3.4.1 Run Patch

If system software running on the switch has a few bugs, Huawei provides patches to remove the bugs in this version. You can install patches on the device.

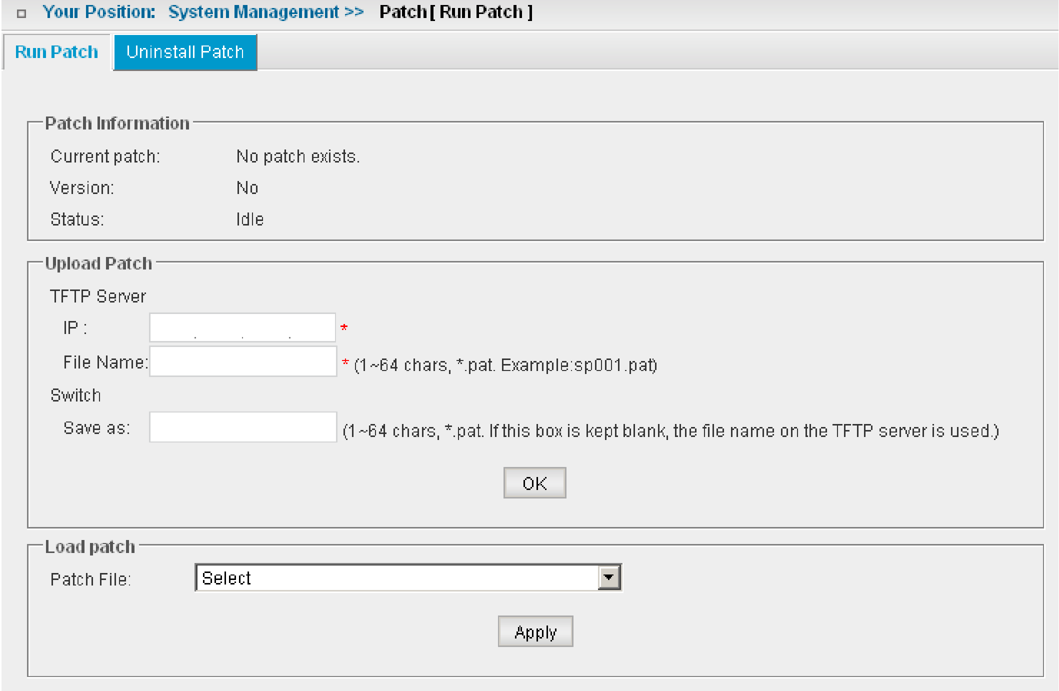
Context

- Before installing patches, you need to save patch files to the flash memory of the switch. Patch files are loaded to the switch by using TFTP.
- A patch is a kind of software compatible with the system software. It is used to remove critical bugs from system software. A patch file can contain a maximum of 20 patches. The patch file name extension is .pat.

Procedure

Step 1 Choose **System Management** > **Patch** > **Run Patch** in the navigation tree to open the **Run Patch** page, as shown in **Figure 3-3**.

Figure 3-3 Run Patch



Your Position: System Management >> Patch [Run Patch]

Run Patch | Uninstall Patch

Patch Information

Current patch: No patch exists.

Version: No

Status: Idle

Upload Patch

TFTP Server

IP : . . . *

File Name: * (1~64 chars, *.pat. Example:sp001.pat)

Switch

Save as: (1~64 chars, *.pat. If this box is kept blank, the file name on the TFTP server is used.)

OK

Load patch

Patch File: Select

Apply

Table 3-3 describes the parameters on the page.

Table 3-3 Run Patch

Parameter		Description
Patch Information		Information about patches is displayed on the page, including: ● Patches that have been loaded ● Patch version ● Running status of the patch
Upload Patch	IP	Indicates the IP address of the TFTP server, for example, **10.10.10.1**. This parameter is mandatory.
	File Name	Indicates the name of the patch file. The value is a string without spaces. The file name extension is .pat. This parameter is mandatory.
	Save as	Indicates the name of the system software file uploaded from the TFTP server. The value is a string without spaces. The loaded file name extension is .pat. If you do not specify the file name, the loaded file retains the original name.
Load patch		Indicates the name of the loaded files. This parameter is mandatory.

Step 2 If the patch to be loaded has not been uploaded, set parameters in the **Upload patch** area and click **OK**. You can view the name of the uploaded patch from the **Load patch** drop-down list box.

Step 3 Select the patch that you want to load from the **Load patch** drop-down list box. Click **Apply**. The system displays a message in **Patch information**, showing the loaded patch files.

----End

3.4.2 Uninstall Patch

If a patch is not needed, uninstall the patch to delete it from the memory permanently.

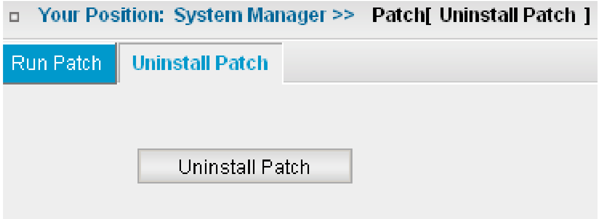
Context

- The patch that you want to delete must exist in the memory.
- After the patch is uninstalled, the patch is deleted from the memory.

Procedure

Step 1 Choose **System Management** > **Patch** > **Uninstall Patch** in the navigation tree to open the **Uninstall Patch** page, as shown in **Figure 3-4**.

Figure 3-4 Uninstall Patch



Step 2 Click **Uninstall Patch**. The system asks you whether to uninstall the patch.

Step 3 The system displays a message indicating whether the patch is uninstalled successfully.

----End

3.5 File System Management

The following sections describe how to manage files, including uploading files to the switch, downloading files from the switch, and restoring or permanently deleting files in the recycle bin.

3.5.1 File System Management

You can upload, download, and delete files.

Context

The TFTP client allows you to upload and download files by using TFTP.

NOTE

The switch connected to the Web system supports only the TFTP mode.

Procedure

- Upload files.

  You can upload files from the TFTP server to the switch.

  1. Choose **System Management** > **File System Management** > **File System Management** in the navigation tree to open the **File System Management** page.
  2. Click **Upload** to open the **Upload file to the switch** page, as shown in **Figure 3-5**.

Figure 3-5 Upload file to the switch

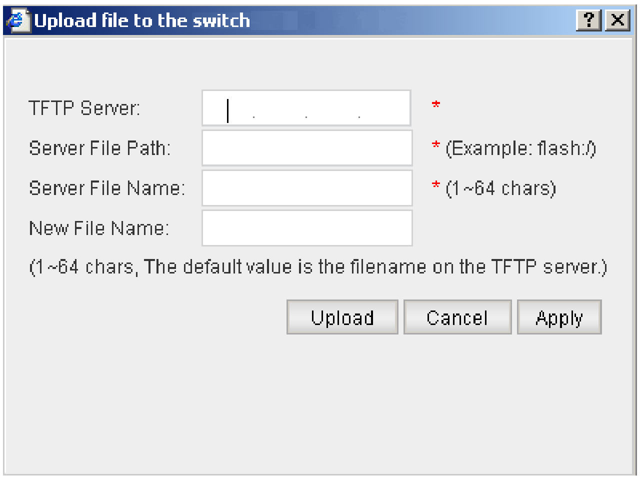


Table 3-4 describes the parameters on the **Upload file to the switch** page.

Table 3-4 Upload file to the switch

Parameter	Description
TFTP Server	Indicates the IP address of the TFTP server, for example, **10.10.10.1**. This parameter is mandatory.
Server File Path	Indicates the path where the files are stored on the switch, for example, **flash:/**. This parameter is mandatory.
Server File Name	Indicates the name of the file that you want to upload. This parameter is mandatory.

Parameter	Description
New File Name	Indicates the new name of the uploaded file. The value is a string without spaces. If you do not specify the new name, the file retains the original name. By default, the file name is unchanged. This parameter is optional.

3. Set parameters and click **Start**. The system displays the upload process page. After the file is uploaded, the system displays a message indicating the successful upload.

   NOTE

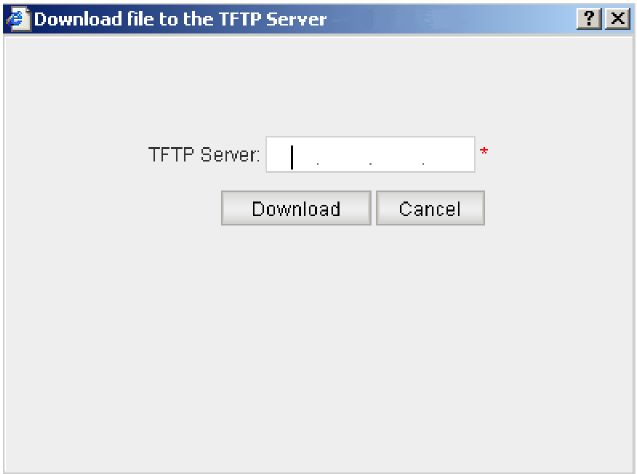
   - If you do not want to close the page after uploading a file, click **Apply**. You can upload other files.
   - If you want to close the page, click **Cancel**.

- Download files.

  You can download files from the switch to the TFTP server.

  1. Choose **System Management** > **File System Management** > **File System Management** in the navigation tree to open the **File System Management** page.
  2. Select the file you want to download and click **Download** to open the **Download file to the TFTP Server** page, as shown in **Figure 3-6**.

     Figure 3-6 Download files to the TFTP Server

  3. Enter the IP address of the TFTP server and click **Download**. The download progress is displayed. When the downloading is complete, the system displays a success message.

- Move files to the recycle bin.

  After files are moved to the recycle bin, they still exist on the switch. You can restore the files in the recycle bin.

WARNING

- The *version*_web.zip file is the Web system file and cannot be deleted. If this file is deleted, the Web system becomes unavailable. In the file name, *version* indicates the version of the Web system software.
- The *version*.cc file is the device software package and cannot be deleted. If this file is deleted, the Web system becomes unavailable. In the file name, *version* indicates the device software version to which the Web system is applied.
- The *name*.cfg file is the Web system configuration file and cannot be deleted. If this file is deleted, the Web system becomes unavailable. In the file name, *name* indicates the configuration file name.
- The *name*.pat file is the Web system patch file and cannot be deleted. If this file is deleted, the Web system becomes unavailable. In the file name, *name* indicates the patch file name.

1. Choose **System Management** > **File System Management** > **File System Management** in the navigation tree to open the **File System Management** page.
2. Select the file you want to move to the recycle bin.

   NOTE

   - To select a file, click the check box of the file.
   - To move files to the recycle bin in batches, click the check boxes of the files.
3. Click **Move to Recycle Bin**, and the system asks you whether to move the file to the recycle bin.
4. Click **OK**.

- Delete files permanently.

  You can permanently delete files from the switch.

CAUTION

The files deleted permanently cannot be restored.

1. Choose **System Management** > **File System Management** > **File System Management** in the navigation tree to open the **File System Management** page.
2. Select the file you want to delete.

   NOTE

   - To select a file, click the check box of the file.
   - To delete files in batches, click the check boxes of the files.
3. Click **Delete Permanently**, and the system asks you whether to delete the file.
4. Click **OK**.

----End

3.5.2 Recycle Bin

You can restore or permanently delete the files in the recycle bin.

Context

The files in the recycle bin can be restored or deleted permanently.

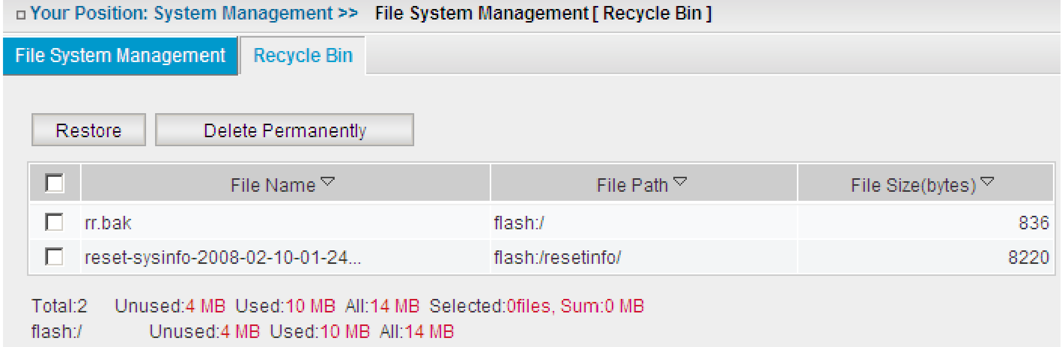
WARNING

The files deleted from the recycle bin cannot be restored.

Procedure

Step 1 Choose **System Management** > **File System Management** > **Recycle Bin** in the navigation tree to open the **Recycle Bin** page, as shown in **Figure 3-7**.

Figure 3-7 Recycle Bin


Your Position: System Management >> File System Management [Recycle Bin]
File System Management
Recycle Bin
Restore
Delete Permanently

☐	File Name ▽	File Path ▽	File Size(bytes) ▽
☐	rr.bak	flash:/	836
☐	reset-sysinfo-2008-02-10-01-24...	flash:/resetinfo/	8220

Total:2 Unused:4 MB Used:10 MB All:14 MB Selected:0files, Sum:0 MB
flash:/ Unused:4 MB Used:10 MB All:14 MB

Step 2 Select the file that you want to restore and click **Restore**.

NOTE

- To delete a file from the switch, select the file and click **Delete Permanently**.
- If an error occurs during file restoration or deletion, the system displays an error message.

----End

3.6 System Configuration

The following sections describe the configurations of the system time and system information.

3.6.1 System Time

You can set the local time zone manually.

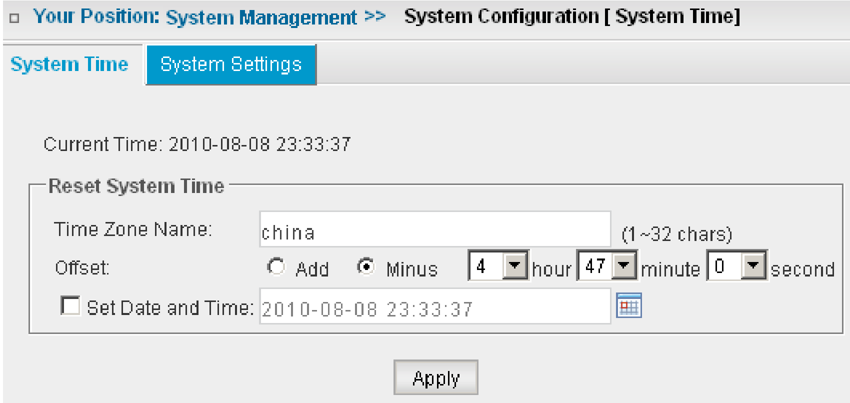
Context

To ensure effective communication between the switch and other devices, set the system time correctly.

Procedure

Step 1 Choose **System Management** > **System Configuration** > **System Time** in the navigation tree to open the **System Time** page, as shown in **Figure 3-8**.

Figure 3-8 System Time



□ Your Position: System Management >> System Configuration [System Time]

System Time | System Settings

Current Time: 2010-08-08 23:33:37

Reset System Time

Time Zone Name: china (1~32 chars)

Offset: ○ Add ● Minus 4 hour 47 minute 0 second

□ Set Date and Time: 2010-08-08 23:33:37

Apply

Table 3-5 describes the parameters on the **System Time** page.

Table 3-5 System Time

Parameter		Description
Current Time		Indicates the current date and time.
Reset System Time	Time Zone Name	Indicates the name of timezone.
	Offset	Indicates the difference between the current time and Universal Time Coordinated (UTC). This parameter is used to increase or decrease the time difference.
	Set Date and Time	Indicates the date and time that you want to specify. Select the **Set Date and Time** check box, and then click ▦ to set the date and time.

Step 2 Set the parameters.

Step 3 Click **Apply**, and then the new date and time is displayed.

----End

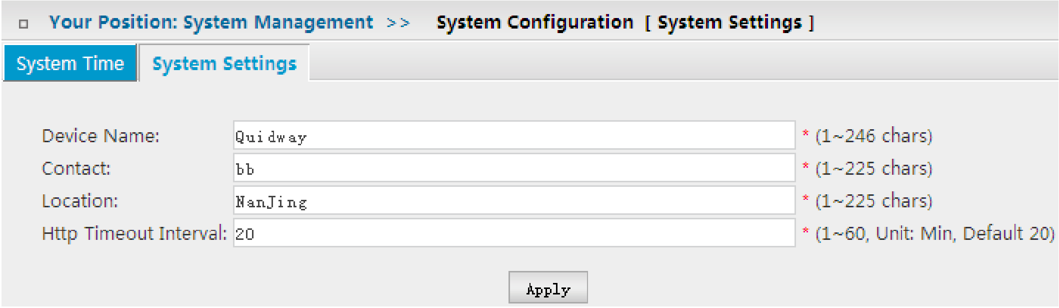
3.6.2 System Settings

You can configure the basic information for the system, including device name, maintenance contact information, and location.

Procedure

Step 1 Choose **System Management** > **System Configuration** > **System Settings** in the navigation tree to open the **System Settings** page, as shown in **Figure 3-9**.

Figure 3-9 System Settings



□ Your Position: System Management >> System Configuration [System Settings]

Device Name: Quidway * (1~246 chars)
Contact: bb * (1~225 chars)
Location: NanJing * (1~225 chars)
Http Timeout Interval: 20 * (1~60, Unit: Min, Default 20)

Table 3-6 describes the parameters on the **System Settings** page.

Table 3-6 System Settings

Parameter	Description
Device Name	Indicates the device name.
Contact	Indicates the maintenance contact information, for example, **RD Beijing, huawei Technologies co.,Ltd.**. The value is a string of case-sensitive characters.
Location	Indicates the physical location of the device, for example, **Beijing China**. The value is a string of case-sensitive characters.
HTTP Timeout Interval	Specifies the timeout of the HTTP connection.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

3.7 PoE

The PoE configurations include global parameters, interface parameters, and PoE device information.

The switch supports the Power Over Ethernet (PoE) function. After being configured with the PoE power supply and the boards that support the PoE function, the switch can provide 48 V

DC power for the remote powered device (PD) such as the IP phone, WLAN AP, and network camera through the twisted pair.**The S2700SI or S3700SI switches do not support the function.**

3.7.1 Global Parameter Settings

You can set global PoE parameters.

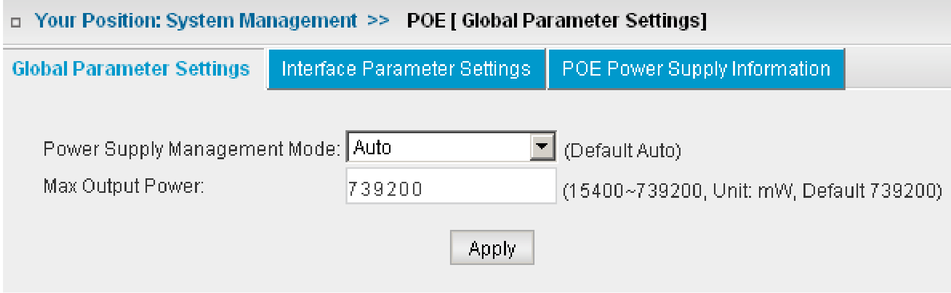
Context

Currently, the network devices are deployed flexibly; therefore, the cabling of power supply is complicated. To simplify cabling, you can configure the PoE function on the switch.

Procedure

Step 1 Choose **System Management** > **PoE** > **Global Parameter Settings** in the navigation tree to open the **Global Parameter Settings** page, as shown in **Figure 3-10**.

Figure 3-10 Global Parameter Settings



Your Position: System Management >> POE [Global Parameter Settings]
Global Parameter Settings
Interface Parameter Settings
POE Power Supply Information
Apply

Power Supply Management Mode: Auto (Default Auto)

Max Output Power: 739200 (15400~739200, Unit: mW, Default 739200)

Table 3-7 describes the parameters on the **Global Parameter Settings** page.

Table 3-7 Global Parameter Settings

Parameter	Description
Power Supply Management Mode	Indicates the mode of power supply management: ● Auto When providing power at almost full capacity, the switch provides power first for the PD connected to the interface of the highest priority. ● Manual When providing power at almost full capacity, the switch keeps the original power supply way, even if a new PD is connected to an interface with high priority. By default, the power supply is in automatic mode.
Max Output Power	Indicates the maximum output power of an interface. **NOTE** The configured maximum PoE power of the entire switch must be greater than the total power allocated to the boards.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

3.7.2 Interface Parameter Settings

You can set the PoE parameters on an interface.

Context

- Currently, the network devices are deployed flexibly; therefore, the cabling of power supply is complicated. To simplify cabling, you can configure the PoE function on the switch.
- By default, the PoE function is enabled on all interfaces.

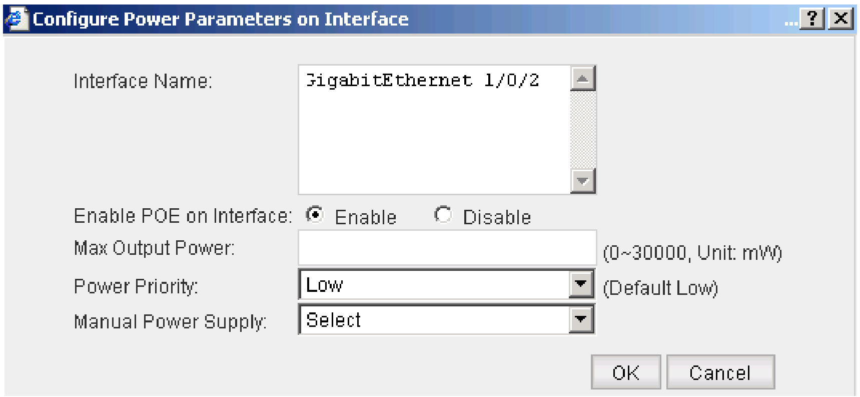
Procedure

- Query power supply information on interfaces.
  1. Choose **System Management** > **PoE** > **Interface Parameter Settings** in the navigation tree to open the **Interface Parameter Settings** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/sub-card ID/port number)**.

4. Click **Query** to display all matching records.

- Set power parameters on an interface.
  1. Choose **System Management** > **PoE** > **Interface Parameter Settings** in the navigation tree to open the **Interface Parameter Settings** page.
  2. Select a record and click **Configure**. The **Configure Power Parameters on Interface** page is displayed, as shown in **Figure 3-11**.

Figure 3-11 Configure Power Parameters on Interface



Interface Name: GigabitEthernet 1/0/2

Enable POE on Interface: ● Enable ○ Disable

Max Output Power: (0~30000, Unit: mW)

Power Priority: Low (Default Low)

Manual Power Supply: Select

Table 3-8 describes the parameters on the **Configure Power Parameters on Interface** page.

Table 3-8 Configure Power Parameters on Interface

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. NOTE If only one interface is selected, the configuration of the interface is displayed on the **Configure Power Parameters on Interface** page. If multiple interfaces are selected, the default settings of the interfaces are displayed.
Enable POE on Interface	Indicates whether to enable the PoE function on the interface. The options are **Enable** and **Disable**. By default, the PoE function is enabled. The PoE parameters take effect only after the PoE function is enabled.
Max Output Power	Indicates the maximum output power of an interface.

Parameter	Description
Power Priority	Indicates the power priority of an interface. The options are Low, High, and Critical. By default, the power priority of a PoE interface is low.
Manual Power Supply	Indicates the manual power supply mode. The options are power on and power off. The default setting is power on. You can manually power on and power off the PD connected to an interface. **NOTE** Before powering on or off a PD, ensure that: ● The PD is connected to an interface. ● The PoE function is enabled on the interface. ● If the PD on an interface has been powered on, an error message is displayed after you power on the PD again. ● If the PD on an interface has been powered off, an error message is displayed after you power off the PD again.

3. Set the parameters.
4. Click **OK**.

----End

3.7.3 PoE Power Supply Information

You can view PoE information.

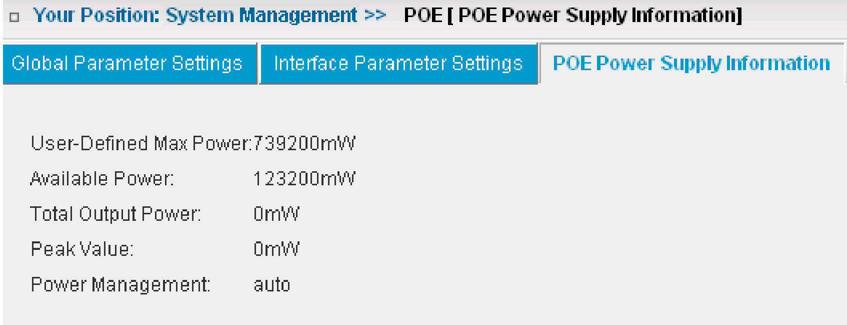
Context

None.

Procedure

Step 1 Choose **System Management** > **PoE** > **PoE Power Supply Information** in the navigation tree to open the **PoE Power Supply Information** page, as shown in **Figure 3-12**. The PoE information is displayed.

Figure 3-12 PoE Power Supply Information



Your Position: System Management >> POE [POE Power Supply Information]
Global Parameter Settings
Interface Parameter Settings
POE Power Supply Information

User-Defined Max Power:739200mW
Available Power: 123200mW
Total Output Power: 0mW
Peak Value: 0mW
Power Management: auto

NOTE

If the PoE information is modified, the latest PoE information is displayed.

----End

3.8 DNS

The following sections describe the configurations of dynamic DNS entries, domain name server, domain name suffix, and enabling dynamic domain name resolution.

In addition to distinguishing devices by IP addresses, TCP/IP provides the Domain Name System (DNS) to name hosts by using character strings. DNS uses a hierarchical naming method to specify a meaningful name for a device on the network. In addition, a DNS server is required on the network to bind IP addresses to domain names. The DNS server enables users to use simple domain names instead of complex IP addresses.

3.8.1 Dynamic DNS Entry Table

You can view the dynamic DNS entries.

Context

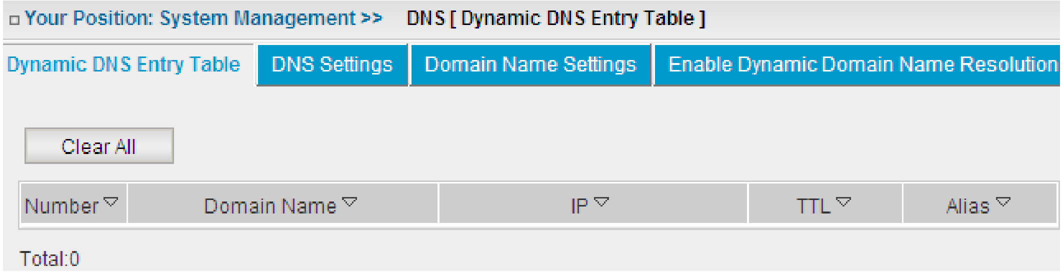
WARNING

The deleted dynamic DNS entries cannot be restored; therefore, perform the deletion operation with caution.

Procedure

Step 1 Choose **System Management** > **DNS** > **Dynamic DNS Entry Table** in the navigation tree to open the **Dynamic DNS Entry Table** page, as shown in **Figure 3-13**.

Figure 3-13 Dynamic DNS Entry Table


□ Your Position: System Management >> DNS [Dynamic DNS Entry Table]
Dynamic DNS Entry Table
DNS Settings
Domain Name Settings
Enable Dynamic Domain Name Resolution
Clear All

Number	Domain Name	IP	TTL	Alias

Total:0

Step 2 View dynamic DNS entries. To delete all dynamic DNS entries, click **Clear All**. The system asks you whether to delete all dynamic DNS entries. The deleted dynamic DNS entries cannot be restored.

Step 3 Click **OK**.

----End

3.8.2 DNS Settings

Dynamic domain name resolution requires a special DNS server. This server maps domain names to IP addresses and processes the resolution requests of clients.

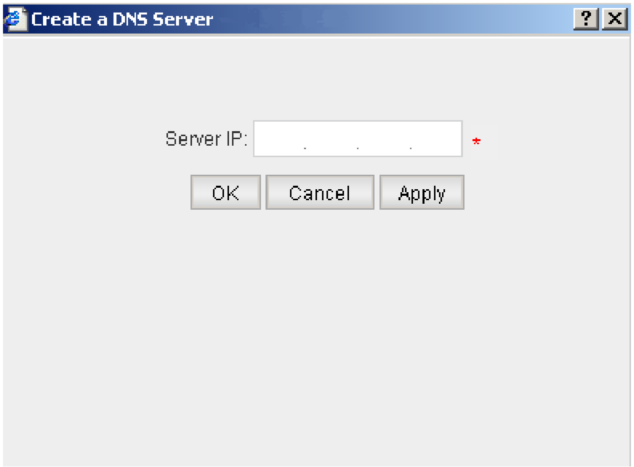
Context

After receiving a resolution request, the DNS server checks whether the domain name belongs to its authorized sub-domain. If yes, the server translates the domain name into an IP address according to the database, and then sends the result to the client. If the server cannot resolve the domain name, it performs the resolution operation specified in the request sent by the client.

Procedure

- Create a DNS server.
  1. Choose **System Management** > **DNS** > **DNS Settings** in the navigation tree to open the **DNS Settings** page.
  2. Click **New** to open the **Create a DNS Server** page, as shown in **Figure 3-14**.

Figure 3-14 Create a DNS Server



Server IP: . . . *

3. Set parameters.
4. Click **OK**.

- Delete a DNS server.
  1. Choose **System Management** > **DNS** > **DNS Settings** in the navigation tree to open the **DNS Settings** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.
  3. Click **OK**.

----End

3.8.3 Domain Name Settings

The system provides the domain name suffix list. You can preset domain name suffixes.

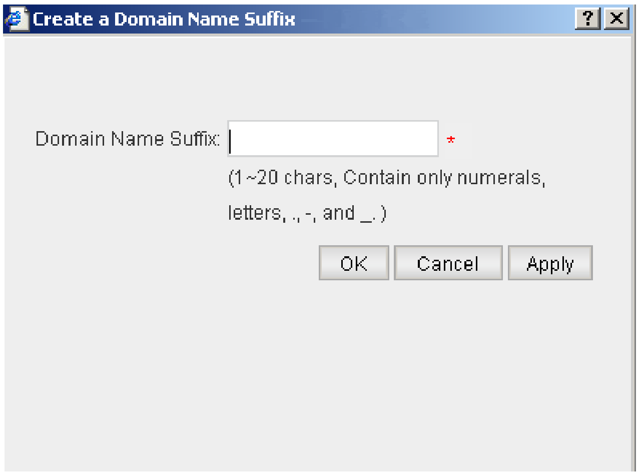
Context

- Users only need to enter partial content of a domain name, and then the system adds a suffix to the domain name for resolution.
- For example, you have set the domain name suffix **com** in the suffix list. If a user wants to visit **huawei.com**, the user only needs to enter **huawei**. Then the system adds the suffix **com** to **huawei.com**.

Procedure

- Create a domain name suffix.
  1. Choose **System Management** > **DNS** > **Domain Name Settings** in the navigation tree to open the **Domain Name Settings** page.
  2. Click **New** to open the **Create a Domain Name Suffix** page, as shown in **Figure 3-15**.

Figure 3-15 Create a Domain Name Suffix



Create a Domain Name Suffix

Domain Name Suffix: *

(1~20 chars, Contain only numerals, letters, ., -, and _.)

Table 3-9 describes the parameters on the **Create a Domain Name Suffix** page.

Table 3-9 Create a Domain Name Suffix

Parameter	Description
Domain Name Suffix	Indicates the new domain name suffix, for example, **com**.

3. Set parameters.
4. Click **OK**.

- Delete a domain name suffix.
  1. Choose **System Management** > **DNS** > **Domain Name Settings** in the navigation tree to open the **Domain Name Settings** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.
  3. Click **OK**

----End

3.8.4 Enable Dynamic Domain Name Resolution

To use the dynamic domain name resolution function, you must enable it first.

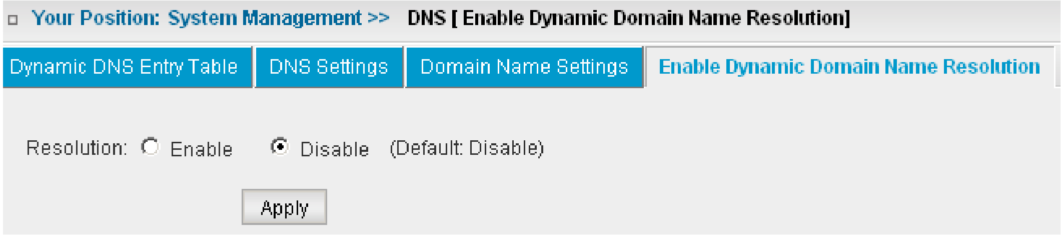
Context

Dynamic domain name resolution requires a special DNS server. This server maps domain names to IP addresses and processes the resolution requirement of clients.

Procedure

Step 1 Choose **System Management** > **DNS** > **Enable Dynamic Domain Name Resolution** in the navigation tree to open the **Enable Dynamic Domain Name Resolution** page, as shown in **Figure 3-16**.

Figure 3-16 Enable Dynamic Domain Name Resolution



Your Position: System Management >> DNS [Enable Dynamic Domain Name Resolution]

Resolution: ○ Enable ● Disable (Default: Disable)

Table 3-10 describes the parameters on the **Enable Dynamic Domain Name Resolution** page.

Table 3-10 Enable Dynamic Domain Name Resolution

Parameter	Description
Resolution	Indicates whether to enable the resolution function. You can set the DNS parameters before enabling the resolution function, but the DNS parameters take effect only after you enable the resolution function.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

3.9 Stacking

The stacking function connects multiple stacking-capable devices together to logically function as one device. Up to nine devices can be connected through stack cables in a ring or bus topology. All stacked devices logically function as one device to forward packets. There are three roles of the devices in a stack: master switch, standby switch, and slave switch. All of the three types of switches are called member switches. The Ethernet switches in a stack function as a device. You can manage all the switches in a stack by using the master switch. **The S2700SI, S2700EI, S2752EI switches do not support the stacking function.**

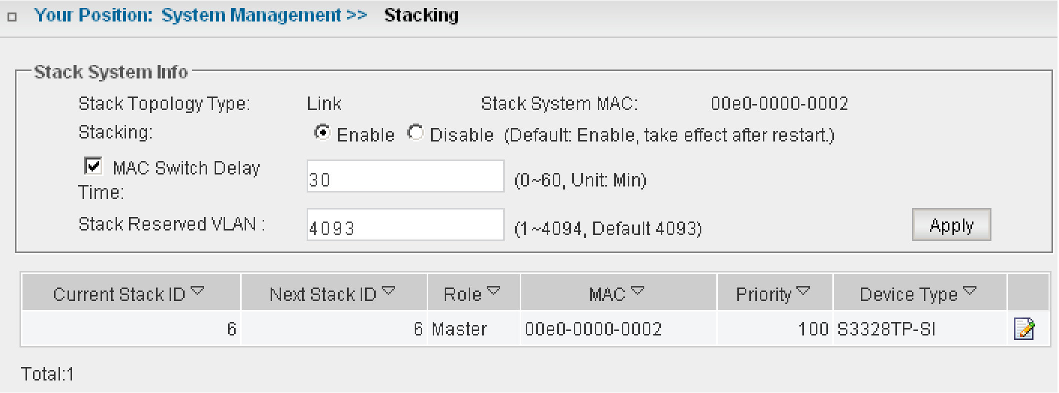
Context

- After the stacking function is enabled on a switch and another switch attempts to connect to this one, if the configurations that the stack does not support exist on the stacking-enabled switch, the system displays a message indicating that some configurations are not supported by the stack. As a result, the new switch cannot be added to the stack. The new switch can be added to the stack only after these configurations are deleted.
- Before the stack is established, each switch is an independent entity. Each switch has its own IP address and functions individually. Therefore, you need to manage each switch separately. After the stack is established, all the member switches are presented as one unified logical entity. In this manner, you can manage and maintain all the member switches in a stack by using one IP address. The stacking protocol elects the master switch, standby switch, and slave switch in a stack. Then, data can be backed up and the active/standby switchover can be implemented.

Procedure

- Configure the stack.
  1. Choose **System Management** > **Stacking** in the navigation tree to open the **Stacking** page, as shown in **Figure 3-17**.

Figure 3-17 Stacking



□ Your Position: System Management >> Stacking

Stack System Info

Stack Topology Type: Link

Stack System MAC: 00e0-0000-0002

Stacking: ● Enable ○ Disable (Default: Enable, take effect after restart.)

☑ MAC Switch Delay Time: 30 (0~60, Unit: Min)

Stack Reserved VLAN : 4093 (1~4094, Default 4093)

Current Stack ID	Next Stack ID	Role	MAC	Priority	Device Type	
6	6	Master	00e0-0000-0002	100	S3328TP-SI	

Total:1

Table 3-11 describes the parameters on the **Stacking** page.

Table 3-11 Stacking

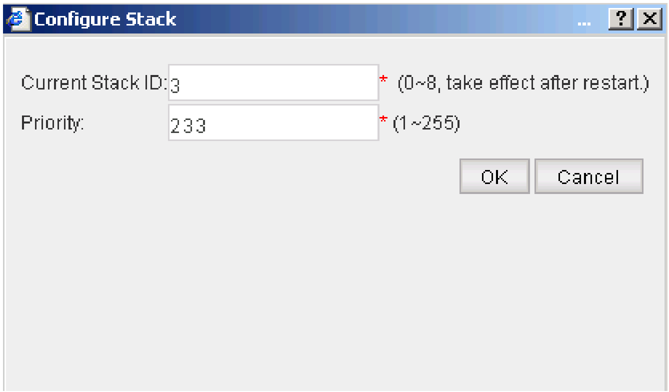
Parameter	Description
Stack Topology Type	Indicates the topology type of the stack. This parameter cannot be set.
Stack System MAC	Indicates the MAC address of the stack. This parameter cannot be set.
Stacking	Indicates whether to enable the stacking function on the interface. The options are **Enable** and **Disable**. By default, the PoE function is enabled. NOTE ● If the stacking parameters are set before you enable the stacking function, you must restart the device to make the parameters effective. ● On the S6700 switches, this parameter has a fixed value **Enable**.

Parameter	Description
MAC Switch Delay Time	Indicates the delay of MAC address switching. This parameter takes effect after the device is restarted. After a switchover occurs between the master and slave switches, the MAC address of the stack is switched to be that of the newly-elected master switch if the previous master switch does not rejoin the stack after the switchover times out. The MAC address switchover time of any member switch in a stack is the same as that of the master switch. **NOTE** ● By default, the MAC address switchover timer is disabled. The system performs the MAC address switchover immediately after the active/standby switchover occurs between switches. ● If the value of the MAC address switchover timer is set to 0, it indicates that MAC address switchover will not be performed.
Stack Reserved VLAN	Indicates the reserved VLAN of the stack. By default, a stack specifies VLAN 4093 as the reserved VLAN. A reserved VLAN is used for exchanging the stack protocol packets only.

2. Set the parameters.
3. Click **OK**.

- Modify the stack.
  1. Choose **System Management** > **Stacking** in the navigation tree to open the **Stacking** page.
  2. Click 📝 to open the **Configure Stack** page, as shown in **Figure 3-18**.

Figure 3-18 Configure Stack



Current Stack ID: 3 * (0~8, take effect after restart.)
Priority: 233 * (1~255)

Table 3-12 describes the parameters on the **Configure Stack** page.

Table 3-12 Configure Stack

Parameter	Description
Current Stack ID	Indicates the stack ID. This parameter takes effect after the device is restarted. Stack IDs can be configured before or after the stack is established. By default, all the stack IDs of member switches in a stack are 0. If stack IDs are not configured for member switches before the stack is established, the stack assigns stack IDs to member switches after being established. After the stack is established successfully, all the configurations of the stack can be performed on the master switch only.
Priority	Indicates the priority of the stack. The stack priority can be configured before or after the stack is established. If the stack is established, this parameter must be set on the master switch; otherwise, it is set on each switch.

3. Set the parameters.
4. Click **OK**.

----End

4 Interface Management

About This Chapter

This chapter describes interface configurations. The interfaces that can be managed include Ethernet interfaces, Eth-Trunk interfaces, VLANIF interfaces, and loopback interfaces. You can configure the interfaces and view configuration information.

4.1 Ethernet
The switch provides Ethernet interfaces and GigabitEthernet interfaces. Configure these interfaces as required.

4.2 Eth-Trunk
An Eth-Trunk is composed of Ethernet links. The Eth-Trunk interface does not exist physically.

4.3 VLANIF
When a switch needs to communicate with the devices at the network layer, you can create a logical interface based on a VLAN on the switch, namely, a VLANIF interface. The VLANIF interface does not exist physically. **The S2700SI, S2700EI, or S2752EI switches do not support this function.**

4.4 LoopBack
A loopback interface is a logical interface. It is always Up. The loopback interface is usually used in loopback test.

4.1 Ethernet

The switch provides Ethernet interfaces and GigabitEthernet interfaces. Configure these interfaces as required.

4.1.1 Basic Attributes

You can configure and query the basic attributes of Ethernet interfaces.

Context

To identify an interface, you can set the description of the interface. You can query and configure Ethernet interfaces as required.

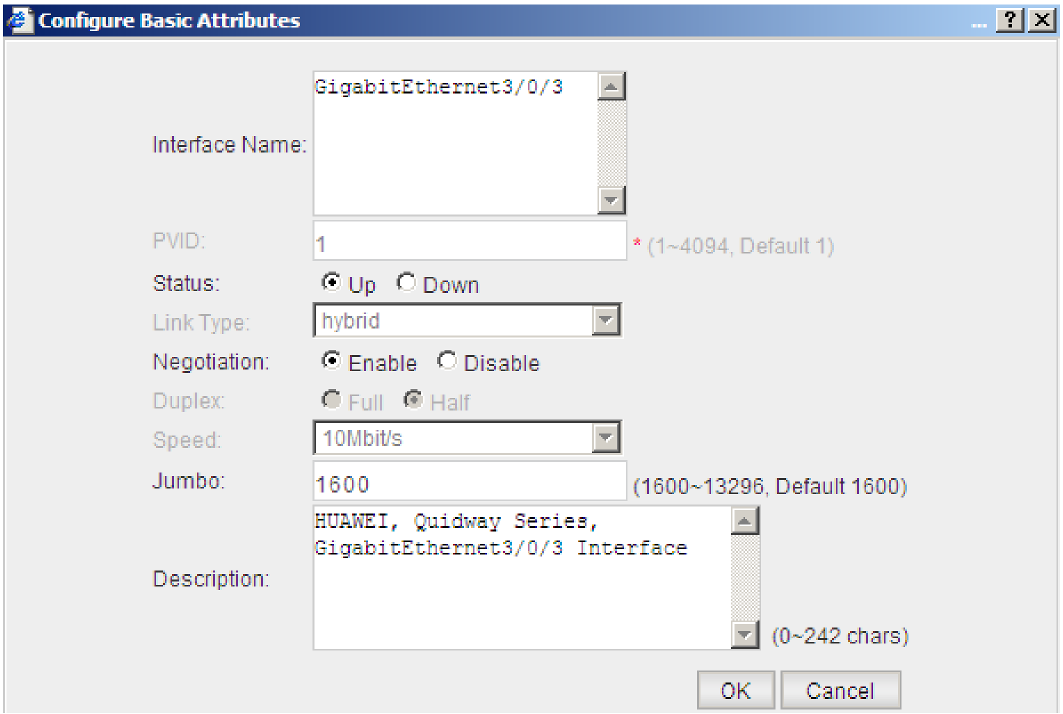
Procedure

- Query basic attributes.
  1. Choose **Interface Management** > **Ethernet** > **Basic Attributes** in the navigation tree to open the **Basic Attributes** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/subcard ID/interface number)**.
  4. Click **Query** to display all matching records.

     NOTE

     To view real-time interface information, click on the **Basic Attributes** tag page to refresh the page.
- Configure basic attributes.
  1. Choose **Interface Management** > **Ethernet** > **Basic Attributes** in the navigation tree to open the **Basic Attributes** page.
  2. Select a record and click **Configure**. The **Configure Basic Attributes** page is displayed, as shown in **Figure 4-1**.

Figure 4-1 Configure Basic Attributes



Interface Name: GigabitEthernet3/0/3

PVID: 1 * (1~4094, Default 1)

Status: ● Up ○ Down

Link Type: hybrid

Negotiation: ● Enable ○ Disable

Duplex: ○ Full ● Half

Speed: 10Mbit/s

Jumbo: 1600 (1600~13296, Default 1600)

Description: HUAWEI, Quidway Series, GigabitEthernet3/0/3 Interface (0~242 chars)

Table 4-1 describes the parameters on the **Configure Basic Attributes** page.

Table 4-1 Configure Basic Attributes

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. **NOTE** If only one interface is selected, the configuration of the interface is displayed on the **Configure Basic Attributes** page. If multiple interfaces are selected, the default settings of the interfaces are displayed.
PVID	Indicates the default VLAN of the interface. This parameter cannot be modified.
Status	Indicates the status of the interface, which can be enabled or disabled. By default, the status of an interface is enabled. This parameter is mandatory.
Link Type	The value cannot be changed.

Parameter	Description
Negotiation	Indicates whether auto-negotiation is enabled. This parameter is mandatory. By default, auto-negotiation is enabled, and the duplex mode or interface rate cannot be configured. If auto-negotiation is disabled, the **Duplex** and **Speed** parameters can be configured.
Duplex	Indicates the duplex mode of the interface, including full duplex and half duplex. By default, the full duplex mode is enabled on interfaces. This parameter is mandatory. To enable an interface to send and receive packets at the same time, enable the full duplex mode on the interface. To disable an interface from sending and receiving packets at the same time, enable the half duplex mode on the interface. **NOTE** A GE electrical interface can work in full duplex, half duplex, or auto-negotiation mode. However, if the speed is set to 1000 Mbit/s, the duplex mode must be full duplex or auto-negotiation. A GE optical interface operates in full duplex mode by default. You can configure it to operate in full duplex mode or auto-negotiation mode.
Speed	Indicates the interface speed, including 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s. This parameter is mandatory. **NOTE** The speed on a GE electrical interface can be 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s. If the duplex mode is set to half duplex, the interface speed cannot be 1000 Mbit/s. The speed on a GE optical interface can only be 1000 Mbit/s. You can set the speed to 1000 Mbit/s or enable auto-negotiation.

Parameter	Description
Jumbo	Indicates the length of a jumbo frame. This parameter is optional. NOTE On the S3700SI and S3700EI switches, the value ranges from 1600 to 13296. On the S5700EI switches, the value ranges from 1600 to 9712. On the S5700SI switches, the value ranges from 1600 to 10224. On the S6700 switches, the value ranges from 1536 to 12288. The S2700SI, S2700EI, or S2752EI switches do not support this parameter.
Description	Indicates the description of the interface. This parameter is mandatory.

3. Set parameters.
4. Click **OK**.

----End

4.1.2 Statistics on Interface

You can view traffic statistics on interfaces, update the statistics, or clear the statistics.

Context

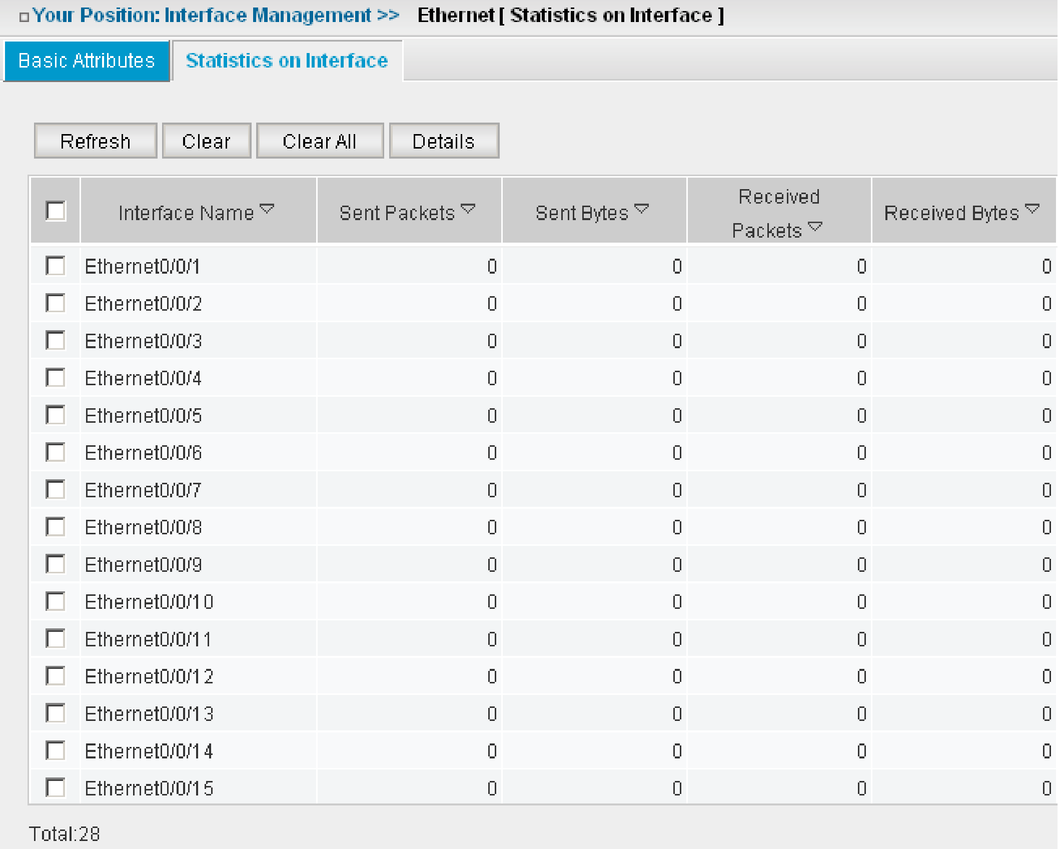
⚠ **CAUTION**

The cleared traffic statistics cannot be restored; therefore, confirm the operation before clearing the traffic statistics.

Procedure

Step 1 Choose **Interface Management** > **Ethernet** > **Statistics on Interface** in the navigation tree to open the **Statistics on Interface** page, as shown in **Figure 4-2**.

Figure 4-2 Statistics on Interface


Your Position: Interface Management >> Ethernet [Statistics on Interface]
Basic Attributes
Statistics on Interface
Refresh
Clear
Clear All
Details

□	Interface Name	Sent Packets	Sent Bytes	Received Packets	Received Bytes
□	Ethernet0/0/1	0	0	0	0
□	Ethernet0/0/2	0	0	0	0
□	Ethernet0/0/3	0	0	0	0
□	Ethernet0/0/4	0	0	0	0
□	Ethernet0/0/5	0	0	0	0
□	Ethernet0/0/6	0	0	0	0
□	Ethernet0/0/7	0	0	0	0
□	Ethernet0/0/8	0	0	0	0
□	Ethernet0/0/9	0	0	0	0
□	Ethernet0/0/10	0	0	0	0
□	Ethernet0/0/11	0	0	0	0
□	Ethernet0/0/12	0	0	0	0
□	Ethernet0/0/13	0	0	0	0
□	Ethernet0/0/14	0	0	0	0
□	Ethernet0/0/15	0	0	0	0

Total:28

Step 2 Select a record and click **Details** to view details about the record.

NOTE

- To obtain latest traffic statistics, click **Refresh**.
- To clear traffic statistics on a specified interface and refresh the page, click **Clear**.
- To clear traffic statistics on all interfaces and refresh the page, click **Clear All**.

On the **Details** page, you can refresh and clear the traffic statistics.

----End

4.2 Eth-Trunk

An Eth-Trunk is composed of Ethernet links. The Eth-Trunk interface does not exist physically.

The Eth-Trunk has the following advantages:

- Increasing bandwidth: The bandwidth of an Eth-Trunk interface is the total bandwidth of all member interfaces.
- Improving reliability: When a link fails, traffic is automatically switched to other links. This ensures reliability of the entire Eth-Trunk.

4.2.1 Eth-Trunk

An Eth-Trunk load balances incoming and outgoing traffic among multiple links and improves the bandwidth and connection reliability between two switches.

Context

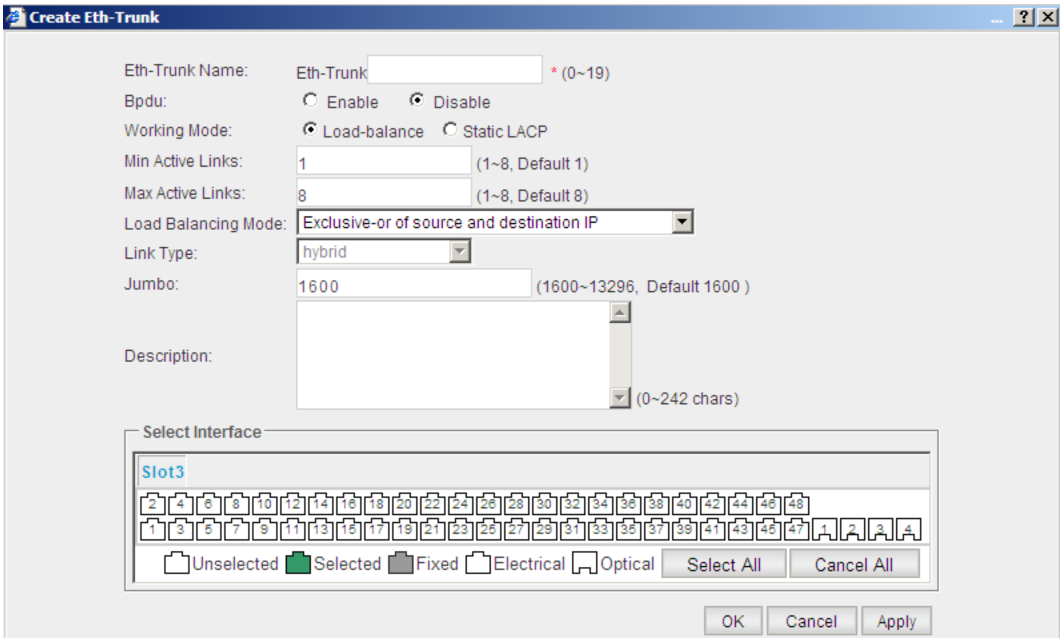
You can configure Eth-Trunks in the following scenarios:

- The bandwidth is insufficient when two switches are connected through only one link.
- The connection reliability cannot meet requirement when two switches are connected through only one link.

Procedure

- Query Eth-Trunk information.
  1. Choose **Interface Management** > **Eth-Trunk** > **Eth-Trunk** in the navigation tree to open the **Eth-Trunk** page.
  2. Enter the interface name, for example, **12**.
  3. Click **Query** to display all matching records.
- Create an Eth-Trunk.
  1. Choose **Interface Management** > **Eth-Trunk** > **Eth-Trunk** in the navigation tree to open the **Eth-Trunk** page.
  2. Click **New** to open the **Create Eth-Trunk** page, as shown in **Figure 4-3**.

Figure 4-3 Create Eth-Trunk



Create Eth-Trunk

Eth-Trunk Name: Eth-Trunk * (0~19)

Bpdu: ○ Enable ● Disable

Working Mode: ● Load-balance ○ Static LACP

Min Active Links: 1 (1~8, Default 1)

Max Active Links: 8 (1~8, Default 8)

Load Balancing Mode: Exclusive-or of source and destination IP

Link Type: hybrid

Jumbo: 1600 (1600~13296, Default 1600)

Description: (0~242 chars)

Select Interface

Slot3

Table 4-2 describes the parameters on the **Create Eth-Trunk** page.

Table 4-2 Create Eth-Trunk

Parameter	Description
Eth-Trunk Name	Indicates the name of an Eth-Trunk. This parameter is mandatory. **NOTE** ● On the S2700SI switches, the value ranges from 0 to 2. On the S2700EI switches, the value ranges from 0 to 13. On the S3700 and S5700 switches, the value ranges from 0 to 19. On the S6700 switches, the value ranges from 0 to 63. ● After creating an Eth-Trunk, you can create another Eth-Trunk on the same **Create Eth-Trunk** page. Enter an Eth-Trunk name and click anywhere on the page. Set parameters of the new Eth-Trunk after the page is refreshed.
BPDU	Indicates whether to enable BPDU. The options are **Enable** and **Disable**. By default, BPDU is disabled. **NOTE** S2700SI, S2700EI, and S2752EI switches you can configure BPDU on **System LACP Priority** page.

Parameter	Description
Working Mode	Indicates the working mode of the Eth-Trunk, including: ● Manual load balancing mode When the bandwidth or the reliability between two devices needs to be increased and one device does not support LACP, you should create an Eth-Trunk in manual load balancing mode and add member interfaces to the Eth-Trunk. ● Static LACP mode The links between two devices can implement redundancy backup. When a fault occurs on some links, the backup links replace the faulty ones to keep data transmission uninterrupted. The default mode is manual load balancing. NOTE ● Check whether the Eth-Trunk contains member interfaces before you set the working mode of the Eth-Trunk. If the Eth-Trunk contains member interfaces, the working mode of the Eth-Trunk cannot be changed. ● The working modes on the local end and remote end must be the same. ● Before configuring a static LACP mode, you must enable BPDU.
Min Active Links	Indicates the lower threshold of the number of active interfaces. You can specify the lower threshold of active interfaces in the Eth-Trunk. If the number of active interfaces is smaller than this value, the status of the Eth-Trunk becomes Down. NOTE ● The lower threshold must be not greater than the upper threshold. ● The lower thresholds of active member interfaces can be set to different values for the local end and remote end. If the lower thresholds at the two ends are different, the greater one is used.

Parameter	Description
Max Active Links	Indicates the upper threshold of the number of active interfaces. **NOTE** ● The lower threshold must be not greater than the upper threshold. ● The upper thresholds of active member interfaces can be set to different values for the local end and remote end. If the upper thresholds at the two ends are different, the smaller one is used. ● In manual load balancing mode, this parameter has a fixed value 8.
LACP Timeout	Indicates the timeout period for receiving LACP packets on an interface in static LACP mode: This parameter is valid only when the static LACP mode is enabled. The timeout can be set to 3 seconds for fast mode or 30 seconds for slow mode.
preempt Delay	Indicates whether to enable the preempt delay function in static LACP mode. By default, the preempt delay function is enabled. This parameter is valid only when the static LACP mode is enabled.
Preempt Delay	Specifies the delay for LACP priority preemption. This parameter is valid only when the static LACP mode and preempt delay functions are enabled.
Load Balancing Mode	Indicates the load balancing mode of Eth-Trunk, including: ● Based on destination IP addresses ● Based on destination MAC addresses ● Based on source IP addresses ● Based on the "Exclusive-OR" result of the source and destination IP addresses ● Based on source MAC addresses ● Based on the "Exclusive-OR" result of the source and destination MAC addresses By default, load balancing is based on the "Exclusive-OR" result of the source and destination IP addresses.

Parameter	Description
Link Type	Indicates the link type of an interface. The value cannot be changed.
Jumbo	Indicates the length of a Jumbo frame. This parameter is optional. **NOTE** The value of the S3700SI and S3700EI switches ranges from 1600 to 13296 seconds. The value of the S5700EI switches ranges from 1600 to 9712 seconds. The value of the S5700SI switches ranges from 1600 to 10224 seconds. The value of the S6700 switches ranges from 1536 to 12288 seconds. The S2700SI, S2700EI, or S2752EI switches do not support this parameter.
Description	Indicates the description of the created Eth-Trunk.
Select Interface	Adds member interfaces to the Eth-Trunk. An Eth-Trunk contains a maximum of eight member interfaces. **NOTE** ● Member interfaces of an Eth-Trunk must have the same interface type. ● A member interface cannot be an Eth-Trunk.

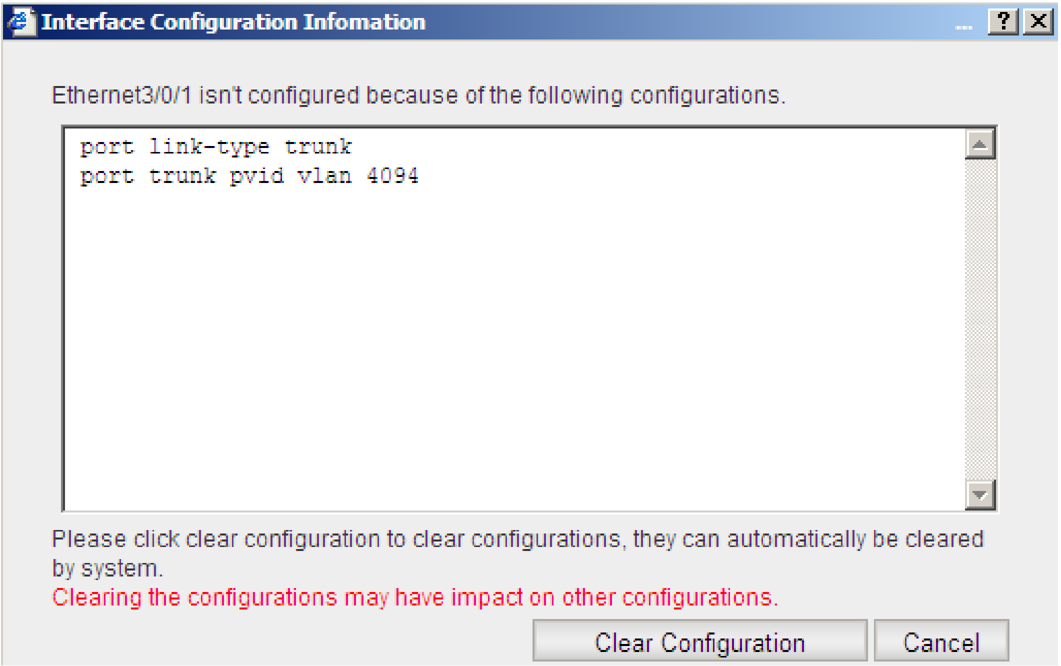
3. Set parameters.

NOTE

When selecting the interface,

- if this interface is configured by other Eth-Trunks, it is unavailable and cannot be selected;
- if this interface is not configured, you can select it;
- if this interface does not join the Eth-Trunk and is configured by other modules on the Web network management page, the **Configure Basic Attributes** page is displayed, as shown in **Figure 4-4**. You can clear the original configurations of this interface.

Figure 4-4 Interface Configuration Information



Ethernet3/0/1 isn't configured because of the following configurations.

```
port link-type trunk
port trunk pvid vlan 4094
```

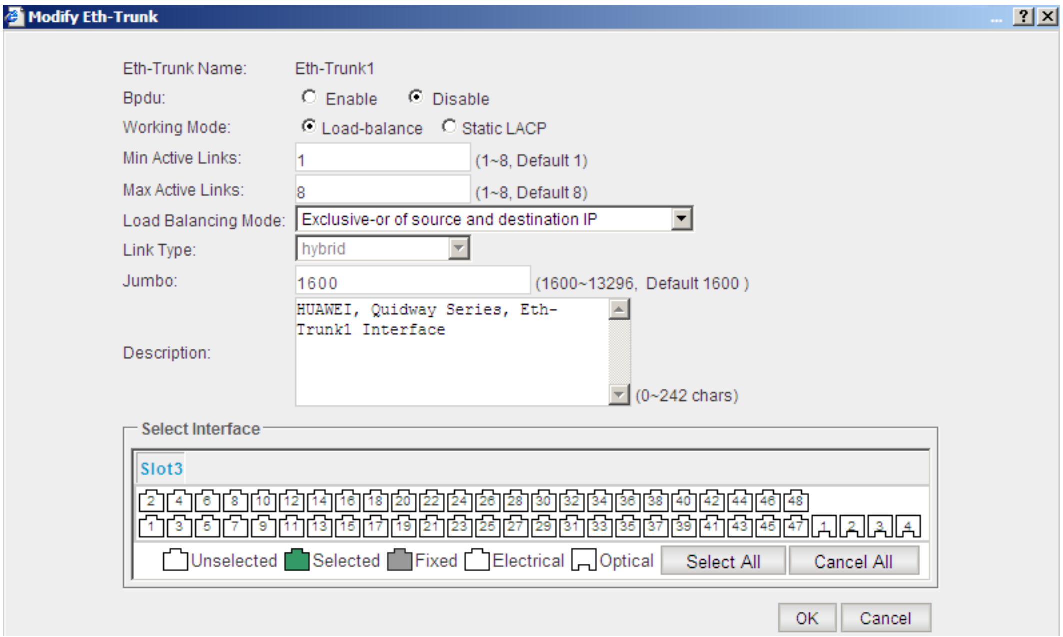
Please click clear configuration to clear configurations, they can automatically be cleared by system.

Clearing the configurations may have impact on other configurations.

4. Click **OK**.

- Modify Eth-Trunk
  1. Choose **Interface Management** > **Eth-Trunk** > **Eth-Trunk** in the navigation tree to open the **Eth-Trunk** page.
  2. Select a record that you want to modify and click ✎ to open the **Modify Eth-Trunk** page, as shown in **Figure 4-5**.

Figure 4-5 Modify Eth-Trunk



Eth-Trunk Name: Eth-Trunk1

Bpdu: ○ Enable ● Disable

Working Mode: ● Load-balance ○ Static LACP

Min Active Links: 1 (1~8, Default 1)

Max Active Links: 8 (1~8, Default 8)

Load Balancing Mode: Exclusive-or of source and destination IP

Link Type: hybrid

Jumbo: 1600 (1600~13296, Default 1600)

Description: HUAWEI, Quidway Series, Eth-Trunk1 Interface (0~242 chars)

NOTE

- **Table 4-2** describes the parameters on the **Modify Eth-Trunk** page.
- The Eth-Trunk name cannot be modified.
- Before changing the working mode of an Eth-Trunk, ensure that the Eth-Trunk does not contain any member interfaces.

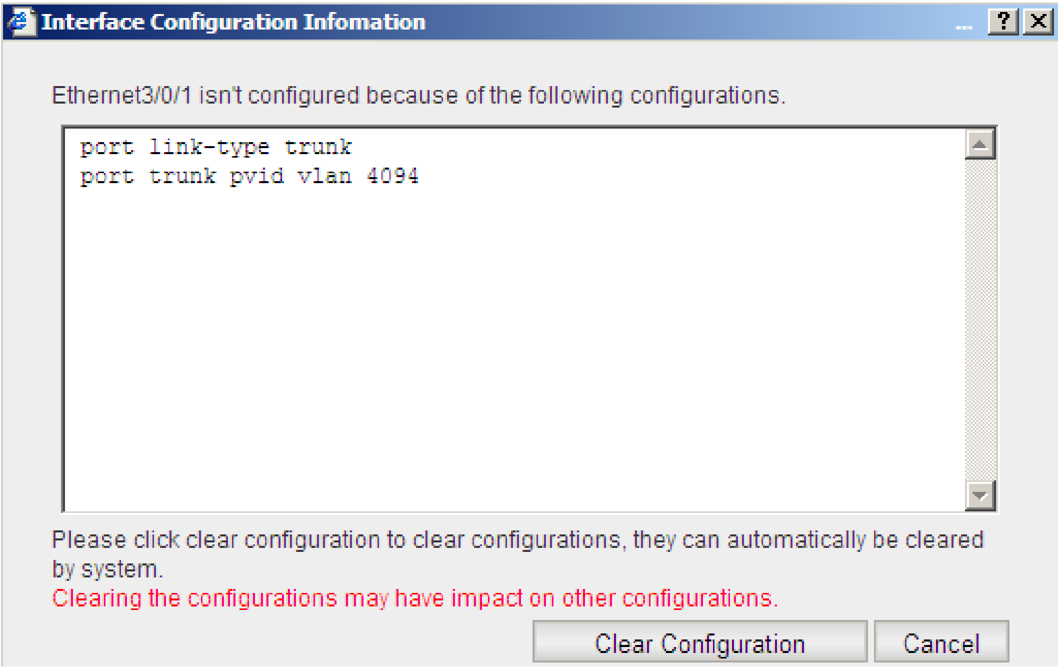
3. Set parameters.

NOTE

When selecting the interface,

- if this interface is configured by other Eth-Trunks, it is unavailable and cannot be selected;
- if this interface is not configured, you can select it;
- if this interface is configured by modules on the Web network management page, excluding Eth-Trunks, the **Configure Basic Attributes** page is displayed, as shown in **Figure 4-6**. You can clear the original configurations of this interface.

Figure 4-6 Interface Configuration Information



Ethernet3/0/1 isn't configured because of the following configurations.

```
port link-type trunk
port trunk pvid vlan 4094
```

Please click clear configuration to clear configurations, they can automatically be cleared by system.

Clearing the configurations may have impact on other configurations.

4. Click **OK**.

- Delete Eth-Trunk
  1. Choose **Interface Management** > **Eth-Trunk** > **Eth-Trunk** in the navigation tree to open the **Eth-Trunk** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

4.2.2 System LACP Priority

You can configure the LACP priorities in the system.

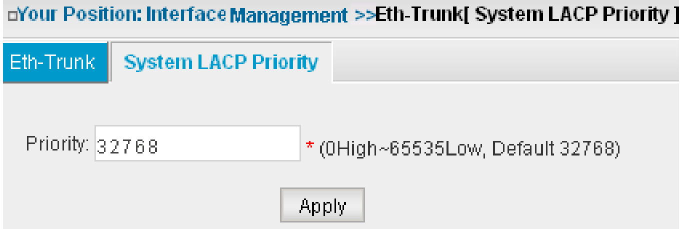
Context

Only the Eth-Trunk in static LACP mode needs to be configured with the LACP priority. The default LACP priority is 32768.

Procedure

Step 1 Choose **Interface Management** > **Eth-Trunk** > **System LACP Priority** in the navigation tree to open the **System LACP Priority** page, as shown in **Figure 4-7**.

Figure 4-7 System LACP Priority


Your Position: Interface Management >>Eth-Trunk[System LACP Priority]
Eth-Trunk
System LACP Priority
Apply

Priority: 32768 * (0High~65535Low, Default 32768)

Table 4-3 describes the parameters on the **System LACP Priority** page.

Table 4-3 System LACP Priority

Parameter	Description
Priority	Indicates the system LACP priority. This parameter is mandatory. NOTE A smaller value indicates a higher priority.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

4.3 VLANIF

When a switch needs to communicate with the devices at the network layer, you can create a logical interface based on a VLAN on the switch, namely, a VLANIF interface. The VLANIF interface does not exist physically. **The S2700SI, S2700EI, or S2752EI switches do not support this function.**

Context

A VLANIF interface is a Layer 3 interface and can be configured with an IP address. Before creating a VLANIF interface, you must create a VLAN. With a VLANIF interface, the switch can communicate with the devices at the network layer.

CAUTION

If a VLANIF interface whose IP address is the same as the switch address is deleted or shut down, you cannot log in to the Web system. In this case, you need to change the IP address of the VLANIF interface. After changing the VLANIF address, you must log in to the switch with the new address.

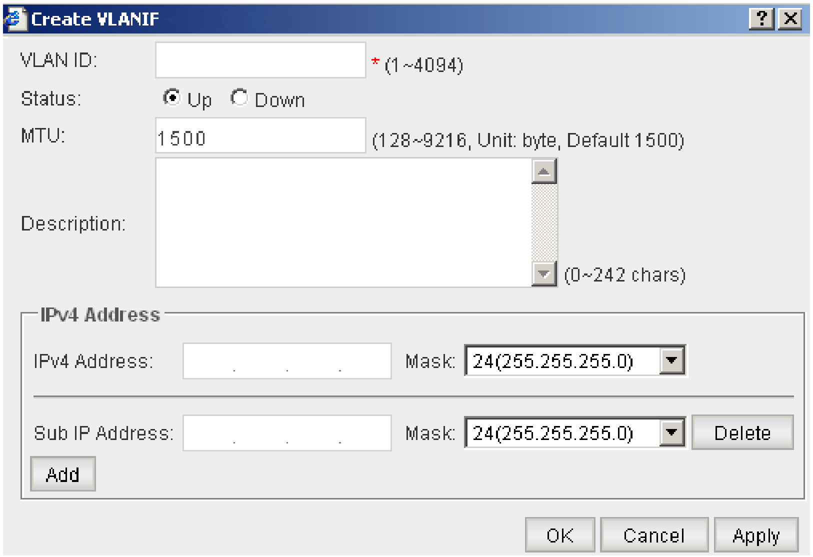
Procedure

- Query VLANIF interface information.
  1. Choose **Interface Management** > **VLANIF** in the navigation tree to open the **VLANIF** page.
  2. Enter the number of the interface that you want to query, for example, **10**. If you do not enter any interface number, all VLANIF interfaces are displayed.
  3. Click **Query** to display all matching records.
  4. Select a record and click **Details** to view details about the record.

     NOTE

     To view real-time interface information, click on the **VLANIF** tag page to refresh the page.
- Create a VLANIF interface.
  1. Choose **Interface Management** > **VLANIF** in the navigation tree to open the **VLANIF** page.
  2. Click **New** to open the **Create VLANIF** page, as shown in **Figure 4-8**.

Figure 4-8 Create VLANIF



Create VLANIF

VLAN ID: * (1~4094)

Status: ● Up ○ Down

MTU: 1500 (128~9216, Unit: byte, Default 1500)

Description: (0~242 chars)

IPv4 Address

IPv4 Address: . . . Mask: 24(255.255.255.0)

Sub IP Address: . . . Mask: 24(255.255.255.0)

Table 4-4 describes the parameters on the **Create VLANIF** page.

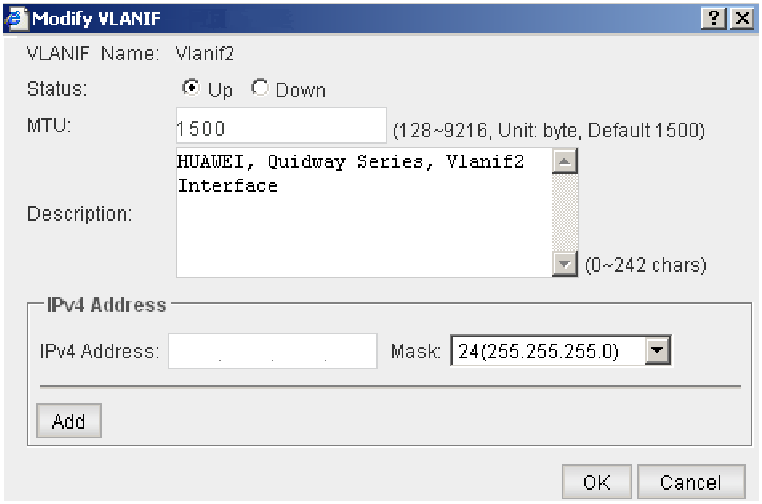
Table 4-4 Create VLANIF

Parameter		Description
VLAN ID		Indicates the VLAN ID corresponding to the new VLANIF interface. This parameter is mandatory.
Status		Indicates the status of the VLANIF interface, which can be enabled or disabled. By default, a VLANIF interface is Up. This parameter is mandatory.
MTU		Indicates the MTU of the VLANIF interface.
Description		Indicates the description of the VLANIF interface.
IPv4 Address	IPv4 Address	Indicates the IPv4 address of the VLANIF interface, for example, **10.10.10.1**.
	Mask	Indicates the mask of the IP address. Select a mask from the drop-down list box.
	Sub IP Address	Indicates the secondary IP address of the VLANIF interface.
	Mask	Indicates the mask of the secondary IP address. Select a mask from the drop-down list box. **NOTE** The **Add** and **Delete** buttons are used to add and delete secondary IP addresses.

3. Set parameters.
4. Click **OK**.

- Modify the VLANIF interface configuration.
  1. Choose **Interface Management** > **VLANIF** in the navigation tree to open the **VLANIF** page.
  2. Select a record that you want to modify and click ✎ to open the **Modify VLANIF** page, as shown in **Figure 4-9**.

Figure 4-9 Modify VLANIF



Modify VLANIF

VLANIF Name: Vlanif2

Status: ● Up ○ Down

MTU: 1500 (128~9216, Unit: byte, Default 1500)

Description: HUAWEI, Quidway Series, Vlanif2 Interface (0~242 chars)

IPv4 Address

IPv4 Address: . . . Mask: 24(255.255.255.0)

NOTE

- Table 4-4 describes the parameters on the **Modify VLANIF** page.
- The VLANIF interface name cannot be changed.

3. Set parameters.
4. Click **OK**.

- Delete a VLANIF interface.

1. Choose **Interface Management** > **VLANIF** in the navigation tree to open the **VLANIF** page.
2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

3. Click **OK**.

----End

4.4 LoopBack

A loopback interface is a logical interface. It is always Up. The loopback interface is usually used in loopback test.

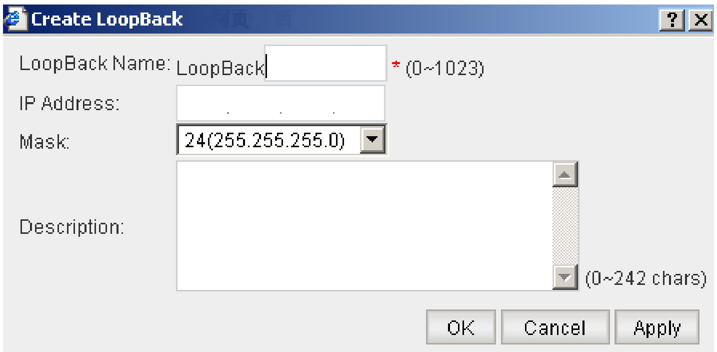
Context

According to the TCP/IP protocol suite, the IP addresses in the network segment 127.0.0.0 are loopback addresses. The interfaces that are configured with these addresses are loopback interfaces. A switch has a default loopback interface loopback 0. A loopback interface can receive all the packets sent to the local switch.

Procedure

- Query loopback interface information.
  1. Choose **Interface Management** > **LoopBack** in the navigation tree to open the **LoopBack** page.
  2. Enter the number of the interface that you want to query, for example, **12**.
  3. Click **Query** to display all matching records.
- Create a loopback interface.
  1. Choose **Interface Management** > **LoopBack** in the navigation tree to open the **LoopBack** page.
  2. Click **New** to open the **Create LoopBack** page, as shown in **Figure 4-10**.

Figure 4-10 Create LoopBack



LoopBack Name: LoopBack * (0~1023)

IP Address: . . .

Mask: 24(255.255.255.0)

Description: (0~242 chars)

Table 4-5 describes the parameters on the **Create LoopBack** page.

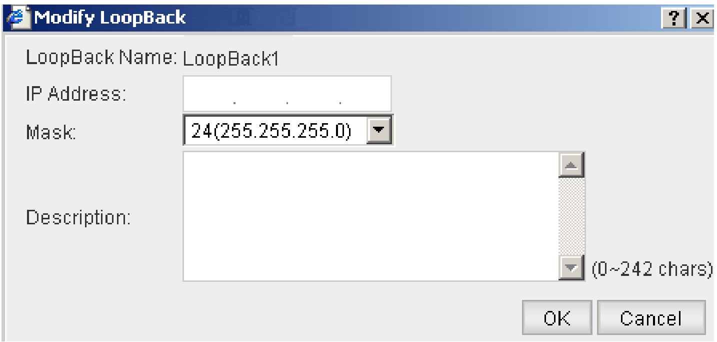
Table 4-5 Create LoopBack

Parameter	Description
LoopBack Name	Indicates the number of the loopback interface. This parameter is mandatory.
IP Address	Indicates the IP address of the loopback interface, for example, **10.10.10.1**.
Mask	Indicates the mask of the IP address. Select a mask from the drop-down list box, for example, **24 (255.255.255.0)**.
Description	Indicates the description of the loopback interface.

  3. Set parameters.
  4. Click **OK**.
- Modify the loopback interface configuration.
  1. Choose **Interface Management** > **LoopBack** in the navigation tree to open the **LoopBack** page.

2. Select a record that you want to modify and click 📝 to open the **Modify LoopBack** page, as shown in **Figure 4-11**.

Figure 4-11 Modify LoopBack



Modify LoopBack

LoopBack Name: LoopBack1

IP Address: . . .

Mask: 24(255.255.255.0)

Description:

(0~242 chars)

NOTE

- **Table 4-5** describes the parameters on the **Modify LoopBack** page.
- The loopback interface name cannot be changed.

3. Set parameters.
4. Click **OK**.

- Delete a loopback interface.
  1. Choose **Interface Management** > **LoopBack** in the navigation tree to open the **LoopBack** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete VLANIF interfaces in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5 Service Management

About This Chapter

This chapter describes service management for the switch. The Web system provides management functions for VLAN, MAC address, STP, voice VLAN, DHCP, ARP, VRRP, and IGMP snooping services. You can query and configure the required services.

5.1 VLAN
The following sections describe how to configure and query VLANs, hybrid interfaces, access interfaces, trunk interfaces, and VLANIF interfaces.

5.2 MAC
Each switch maintains a MAC address table (MAC table for short). The MAC table records MAC addresses of all the devices connected to interfaces of the switch. When forwarding a data frame, the switch searches the MAC table for the outbound interface according to the destination MAC address of the frame. This reduces the number of broadcast frames.

5.3 STP
The following sections describe how to query the STP information and set the global STP parameters, STP parameters on an interface, and parameters of an MST region. **The S2700SI switches do not support the STP function.**

5.4 Voice VLAN
A voice VLAN is assigned to voice data flows. You can create a voice VLAN and add the interface connected to a voice device to the voice VLAN. Then voice data flows can be transmitted on the voice VLAN. **The S2700SI switches do not support the voice VLAN function.**

5.5 DHCP
The switch supports Dynamic Host Configuration Protocol (DHCP) applications based on the global address pool or an address pool configured on a VLANIF interface. The switch also provides security guarantee for DHCP services and supports DHCP relay. **The S2700EI, S2700SI, S2752EI switches do not support the function.**

5.6 ARP
The following sections describe configurations of static ARP and dynamic ARP. **The S2700SI, S2700EI or S2752EI switches do not support the ARP function.**

5.7 VRRP

The following sections describe configurations of VRRP groups and VRRP parameters. **The S2700SI, S2700EI,S2752EI, S5700SI or S3700SI switches do not support the VRRP function.**

5.8 IGMP Snooping
The following sections describe configurations of IGMP snooping on a switch.

5.1 VLAN

The following sections describe how to configure and query VLANs, hybrid interfaces, access interfaces, trunk interfaces, and VLANIF interfaces.

A local area network (LAN) can be divided into several logical LANs. Each logical LAN is a broadcast domain, which is called a virtual LAN (VLAN). To put it simply, devices on a LAN are logically grouped into different LAN segments, regardless of their physical locations. VLANs isolate broadcast domains on a LAN.

5.1.1 VLAN

You can create, query, modify, and delete VLANs. In addition, you can create VLANs in a batch.

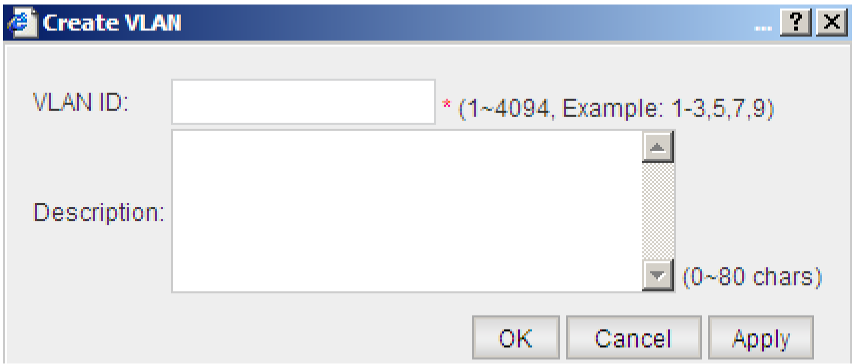
Context

- The switch supports 4094 VLANs from VLAN 1 to VLAN 4094.
- VLANs can isolate the hosts that require no communication with each other, which improves network security, reduces broadcast traffic, and suppresses broadcast storms.

Procedure

- Query VLAN information.
  1. Choose **Service Management** > **VLAN** > **VLAN** in the navigation tree to open the **VLAN** page.
  2. Enter a VLAN ID. If you do not enter any VLAN ID, all VLANs are displayed.
  3. Click **Query** to display all matching records.
- Create a VLAN.
  1. Choose **Service Management** > **VLAN** > **VLAN** in the navigation tree to open the **VLAN** page.
  2. Click **New** to open the **Create VLAN** page, as shown in **Figure 5-1**.

Figure 5-1 Create VLAN



Create VLAN

VLAN ID: * (1~4094, Example: 1-3,5,7,9)

Description: (0~80 chars)

Table 5-1 describes the parameters on the page.

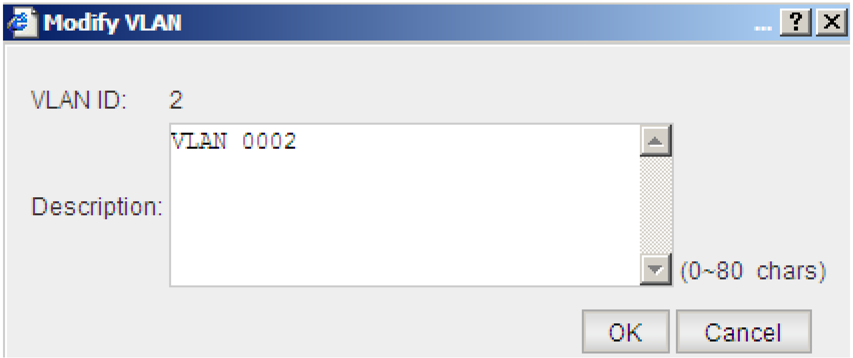
Table 5-1 Create VLAN

Parameter	Description
VLAN ID	Indicates the IDs of VLANs. The value ranges from 1 to 4094. This parameter is mandatory. You can enter multiple VLAN IDs, for example, **1-3,5,7,9**. VLAN 1 is the default VLAN, and the system will not re-create it.
Description	Indicates the description of a VLAN. This parameter is optional. When you create VLANs in a batch, keep the description empty.

3. Set parameters.
4. Click **OK**.

- Modify VLAN
  1. Choose **Service Management** > **VLAN** > **VLAN** in the navigation tree to open the **VLAN** page.
  2. Click the 📝 icon to open the **Modify VLAN** page, as shown in **Figure 5-2**.

Figure 5-2 Modify VLAN



Modify VLAN

VLAN ID: 2

Description: VLAN 0002

(0~80 chars)

NOTE

- **Table 5-1** describes the parameters on the page.
- The VLAN ID cannot be changed.

  3. Set parameters.
  4. Click **OK**.

- Delete a VLAN.
  1. Choose **Service Management** > **VLAN** > **VLAN** in the navigation tree to open the **VLAN** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

NOTE

- To select a record, click the check box of the record. You can delete multiple or all recordings simultaneously.
- VLAN 1 is the default VLAN and cannot be deleted.

3. Click **OK**.

----End

5.1.2 Hybrid Port

You can query, modify, or delete the configuration of a hybrid interface.

Context

A hybrid interface can connect to either a user host or a switch, and it can connect to an access link or a trunk link. A hybrid interface permits frames from multiple VLANs to pass and can remove VLAN tags of outgoing frames.

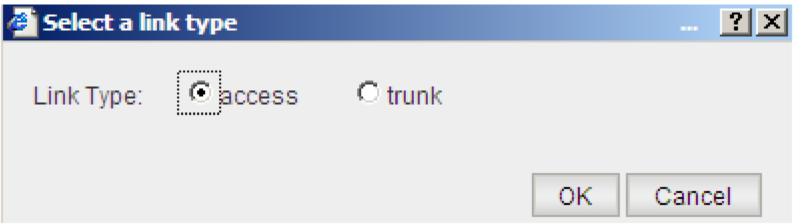
Procedure

- Query a hybrid interface.
  1. Choose **Service Management** > **VLAN** > **Hybrid port** in the navigation tree to open the **Hybrid port** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/subcard ID/interface number)**.
  4. Click **Query** to display all matching records.
- Modify the link type.
  1. Choose **Service Management** > **VLAN** > **Hybrid port** in the navigation tree to open the **Hybrid port** page.
  2. Select the interface whose link type you want to change.

     NOTE

     - To select a record, click the check box of the record.
     - To modify records in batches, click the check boxes of the records.
  3. Click **Change Link Type**. A dialog box is displayed to notify you that the VLANs need to be cleared first.
  4. Click **OK**. The **Select a link type** window is displayed, as shown in **Figure 5-3**.

     Figure 5-3 Select a link type

     Select a link type

     Link Type: ● access ○ trunk

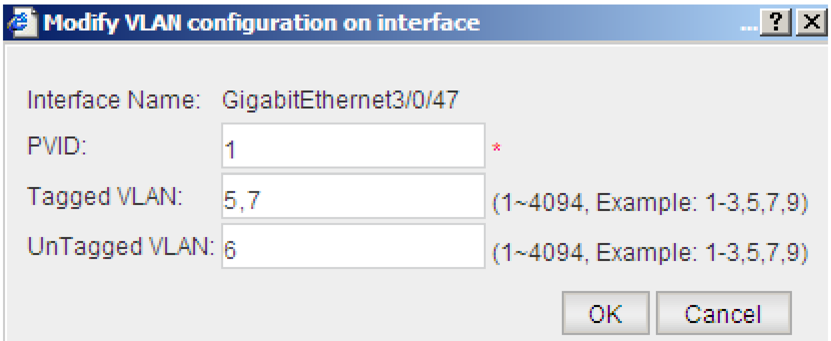
  5. Select the link type, access or trunk.
  6. Click **OK**.

- Clear the VLAN configuration.
  1. Choose **Service Management** > **VLAN** > **Hybrid port** in the navigation tree to open the **Hybrid port** page.
  2. Select the interface configured by the VLAN that you want to clear.

     NOTE

     - To select a record, click the check box of the record.
     - To delete interfaces in batches, click the check boxes of the files.
  3. Click **Delete VLANs**. A dialog box is displayed asking whether to delete VLANs.
  4. Click **OK**.
- Modify the hybrid interface configuration.
  1. Choose **Service Management** > **VLAN** > **Hybrid port** in the navigation tree to open the **Hybrid port** page.
  2. Click the ✎ icon to open the **Modify VLAN configuration on interface** page, as shown in **Figure 5-4**.

Figure 5-4 Modify VLAN configuration on interface



Interface Name: GigabitEthernet3/0/47

PVID: 1 *

Tagged VLAN: 5,7 (1~4094, Example: 1-3,5,7,9)

UnTagged VLAN: 6 (1~4094, Example: 1-3,5,7,9)

Table 5-2 describes the parameters on the page.

Table 5-2 Modify VLAN configuration

Parameter	Description
Interface Name	Indicates the name of the interface where you want to modify the configuration. This parameter cannot be modified.
PVID	The value ranges from 1 to 4094. This parameter is mandatory.
Tagged VLAN	Indicates the IDs of VLANs. The value ranges from 1 to 4094. This parameter is optional. You can enter multiple VLAN IDs, for example, **1-3,5,7,9**.
UnTagged VLAN	Indicates the IDs of VLANs. The value ranges from 1 to 4094. This parameter is optional. You can enter multiple VLAN IDs, for example, **1-3,5,7,9**.

NOTE

A VLAN supports either tagged mode or untagged mode.

3. Set parameters.
4. Click **OK**.

----End

5.1.3 Access Port

You can query, modify, or delete the configuration of an access interface.

Context

An access interface is connected to user hosts. It is mainly used to connect to access links, and the Ethernet frames transmitted on the access link do not contain VLAN tags. If an access interface is configured with a default VLAN, the access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the default VLAN ID. The access link transmits only the Ethernet frames with the default VLAN ID.

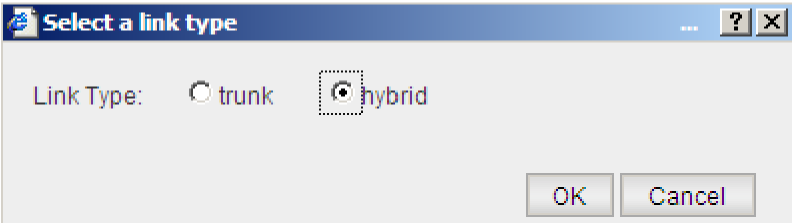
Procedure

- Query an access interface.
  1. Choose **Service Management** > **VLAN** > **Access Port** in the navigation tree to open the **Access Port** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/subcard ID/interface number)**.
  4. Click **Query** to display all matching records.
- Modify the link type.
  1. Choose **Service Management** > **VLAN** > **Access Port** in the navigation tree to open the **Access Port** page.
  2. Select the interface whose link type you want to change.

     NOTE

     - To select a record, click the check box of the record.
     - To modify records in batches, click the check boxes of the records.
  3. Click **Change Link Type**. A dialog box is displayed asking "Clear VLANs on the interface first. Do you want to clear VLANs?"
  4. Click **OK**. The **Select a link type** window is displayed, as shown in **Figure 5-5**.

Figure 5-5 Select a link type



Link Type: ○ trunk ● hybrid

5. The link type includes trunk and hybrid.
6. Click **OK**.

- Clear the VLAN configuration.
  1. Choose **Service Management** > **VLAN** > **Access Port** in the navigation tree to open the **Access Port** page.
  2. Select the interface configured by the VLAN that you want to clear.

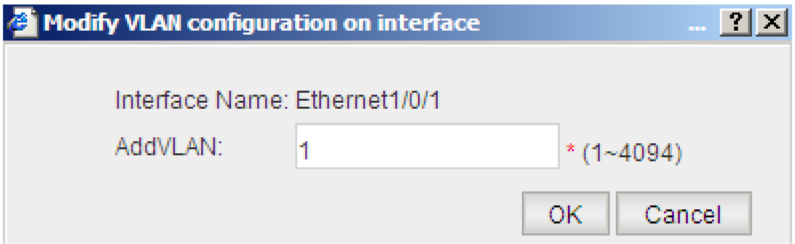
     📖 **NOTE**

     - To select a record, click the check box of the record.
     - To delete interfaces in batches, click the check boxes of the files.
  3. Click **Delete VLANs**. A dialog box is displayed asking whether to delete VLANs.
  4. Click **OK**.
- Add to a VLAN.
  1. Choose **Service Management** > **VLAN** > **Access Port** in the navigation tree to open the **Access Port** page.
  2. Select an interface to be added to the VLAN.

     📖 **NOTE**

     - To select a record, click the check box of the record.
     - To add interfaces in batches, click the check boxes of the records.
  3. Enter the ID of the VLAN to which you want to add the interface.
  4. Click **Add**.
- Modify the Access interface
  1. Choose **Service Management** > **VLAN** > **Access Port** in the navigation tree to open the **Access Port** page.
  2. Click the 📝 icon to open the **Modify VLAN configuration on interface** page, as shown in **Figure 5-6**.

Figure 5-6 Modify VLAN configuration on interface



Modify VLAN configuration on interface

Interface Name: Ethernet1/0/1

AddVLAN: 1 * (1~4094)

  3. Enter the interface IDs added to the VLAN.
  4. Click **OK**.

----End

5.1.4 Trunk Port

You can query, modify, or delete the configuration of a trunk interface.

Context

A trunk interface connects to a packet switching device and serves a trunk link. A trunk interface allows frames from multiple VLANs to pass.

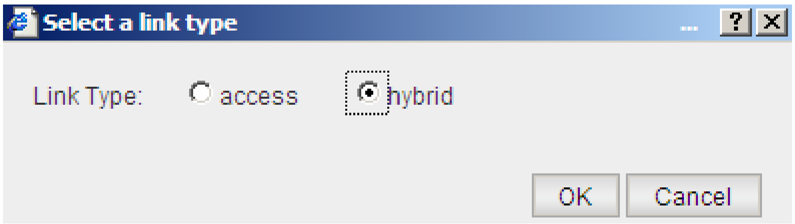
Procedure

- Query a trunk interface.
  1. Choose **Service Management** > **VLAN** > **Trunk port** in the navigation tree to open the **Trunk port** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/subcard ID/interface number)**.
  4. Click **Query** to display all matching records.
- Modify the link type.
  1. Choose **Service Management** > **VLAN** > **Trunk port** in the navigation tree to open the **Trunk port** page.
  2. Select the interface whose link type you want to change.

     NOTE

     - To select a record, click the check box of the record.
     - To modify records in batches, click the check boxes of the records.
  3. Click **Change Link Type**. A dialog box is displayed asking "Clear VLANs on the interface first. Do you want to clear VLANs?"
  4. Click **OK**. The **Select a link type** window is displayed, as shown in **Figure 5-7**.

     Figure 5-7 Select a link type



Select a link type

Link Type: ○ access ● hybrid

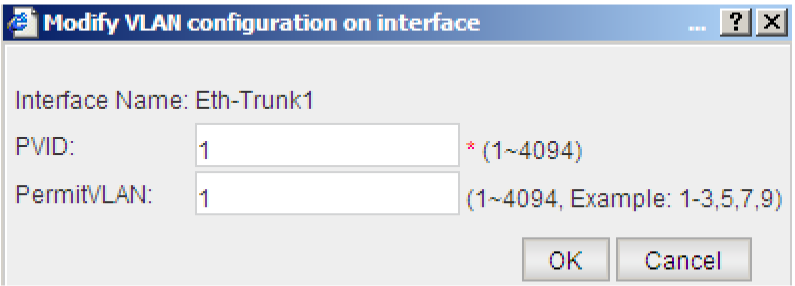
  5. The link type includes access and hybrid.
  6. Click **OK**.
- Clear the VLAN configuration.
  1. Choose **Service Management** > **VLAN** > **Trunk port** in the navigation tree to open the **Trunk port** page.
  2. Select the interface configured by the VLAN that you want to clear.

     NOTE

     - To select a record, click the check box of the record.
     - To delete interfaces in batches, click the check boxes of the files.
  3. Click **Delete VLANs**. A dialog box is displayed asking whether to delete VLANs.
  4. Click **OK**.

- Modify a Trunk interface.
  1. Choose **Service Management** > **VLAN** > **Trunk port** in the navigation tree to open the **Trunk port** page.
  2. Click the 📝 icon to open the **Modify VLAN configuration on interface** page, as shown in **Figure 5-8**.

Figure 5-8 Modify VLAN configuration on interface



Interface Name: Eth-Trunk1

PVID: 1 * (1~4094)

PermitVLAN: 1 (1~4094, Example: 1-3,5,7,9)

Table 5-3 describes the parameters on the page.

Table 5-3 Modify VLAN configuration

Parameter	Description
Interface Name	Indicates the name of the interface where you want to modify the configuration. This parameter cannot be modified.
PVID	The value ranges from 1 to 4094. This parameter is mandatory.
PermitVLAN	Indicates the IDs of VLANs. The value ranges from 1 to 4094. This parameter is optional. You can enter multiple VLAN IDs, for example, **1-3,5,7,9**.

  3. Set parameters.
  4. Click **OK**.

----End

5.1.5 VLANIF Port

When a switch needs to communicate with the devices at the network layer, you can create a logical interface based on a VLAN on the switch, namely, a VLANIF interface. The VLANIF interface is a configured interface and does not exist physically. **The S2700SI,S2700EI,and S2752EI switches do not support this function.**

Context

A VLANIF interface is an interface at the network layer and can be configured with an IP address. Before configuring a VLANIF interface, you must create the corresponding VLAN. The switch then uses the VLANIF interface to communicate with the devices at the network layer.

CAUTION

- You can also access this page by choosing **Interface Management** > **VLANIF port** page. The navigation path provided here enables you to configure VLANIF interfaces directly after configuring VLANs.
- If the IP address of a VLANIF is the switch address, deleting or shutting down the VLANIF interface disables you from logging in to the Web network management system. If the VLANIF address is changed, use the new address to log in to the Web network management system.

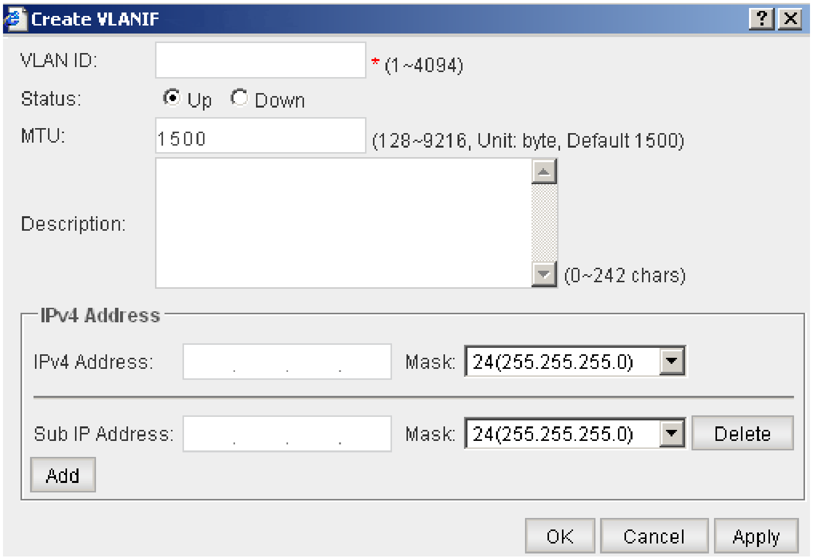
Procedure

- Query VLANIF interface information.
  1. Choose **Service Management** > **VLAN** > **VLANIF port** in the navigation tree to open the **VLANIF port** page.
  2. Enter the number of the interface that you want to query, for example, **10**. If you do not enter any interface number, all VLANIF interfaces are displayed.
  3. Click **Query** to display all matching records.
  4. Select a record and click **Details** to view details about the record.

     NOTE

     To view real-time interface information, click on the **VLANIF port** tag page to refresh the page.
- Create a VLANIF interface.
  1. Choose **Service Management** > **VLAN** > **VLANIF port** in the navigation tree to open the **VLANIF port** page.
  2. Click **New** to open the **Create VLANIF** page, as shown in **Figure 5-9**.

Figure 5-9 Create VLANIF



Create VLANIF

VLAN ID: * (1~4094)

Status: ● Up ○ Down

MTU: 1500 (128~9216, Unit: byte, Default 1500)

Description: (0~242 chars)

IPv4 Address

IPv4 Address: . . . Mask: 24(255.255.255.0)

Sub IP Address: . . . Mask: 24(255.255.255.0)

Table 5-4 describes the parameters on the page.

Table 5-4 Create VLANIF

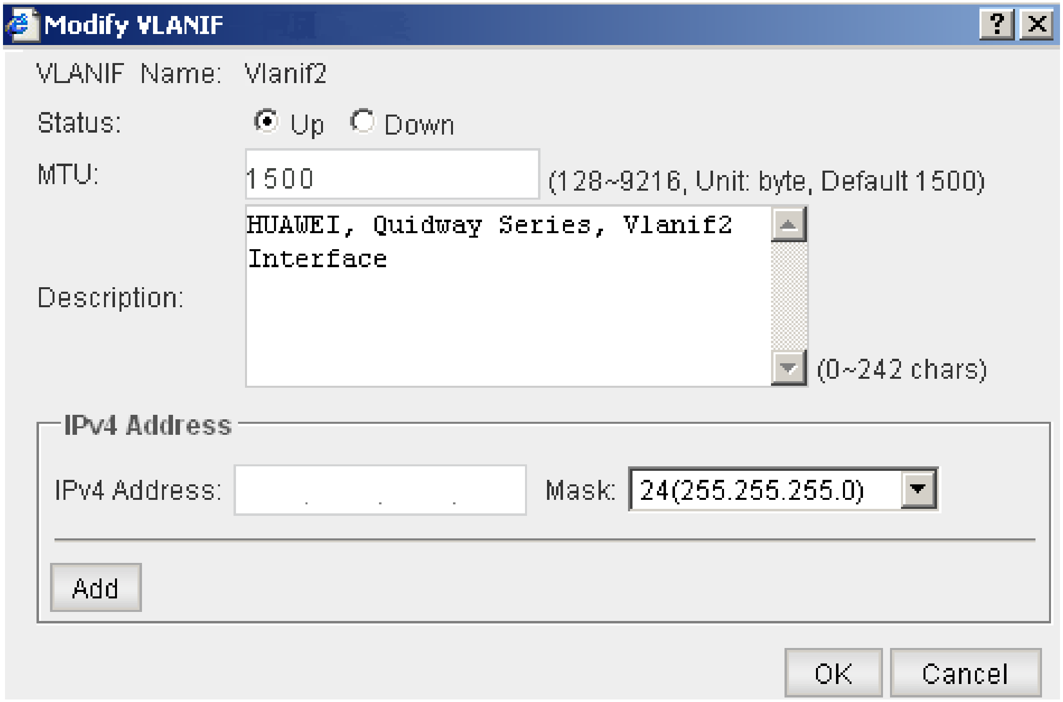
Parameter		Description
VLAN ID		Indicates the VLAN ID of the new VLANIF interface. This parameter is mandatory.
Status		Indicates the status of the VLANIF interface, which can be enabled or disabled. This parameter is mandatory. By default, the status of a VLANIF interface is Up.
MTU		Indicates the Maximum Transmission Unit (MTU) of the VLANIF interface.
Description		Indicates the description of the new VLANIF interface.
IPv4 Address	IPv4 Address	Indicates the IPv4 address of the VLANIF interface, for example, **10.10.10.1**.
	Mask	Indicates the mask of the IP address. Select a subnet mask from the drop-down list box.
	Sub IP Address	Indicates the secondary IP address of the VLANIF interface.

Parameter		Description
	Mask	Indicates the mask of the secondary IP address. Select a subnet mask from the drop-down list box. NOTE The **Add** and **Delete** buttons are used to add and delete secondary IP addresses. You can delete a secondary IP address as well as add another secondary IP address.

3. Set parameters.
4. Click **OK**.

- Modify the VLANIF interface configuration.
  1. Choose **Service Management** > **VLAN** > **VLANIF port** in the navigation tree to open the **VLANIF port** page.
  2. Select a record that you want to modify and click ✎ to open the **Modify VLANIF** page, as shown in **Figure 5-10**.

Figure 5-10 Modify VLANIF



Modify VLANIF

VLANIF Name: Vlanif2

Status: ◉ Up ○ Down

MTU: 1500 (128~9216, Unit: byte, Default 1500)

Description: HUAWEI, Quidway Series, Vlanif2 Interface (0~242 chars)

IPv4 Address

IPv4 Address: . . .

Mask: 24(255.255.255.0)

NOTE

- **Table 5-4** describes the parameters on the page.
- The VLANIF interface name cannot be changed.

  3. Set parameters.
  4. Click **OK**.

- Delete a VLANIF interface.
  1. Choose **Service Management** > **VLAN** > **VLANIF port** in the navigation tree to open the **VLANIF port** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.2 MAC

Each switch maintains a MAC address table (MAC table for short). The MAC table records MAC addresses of all the devices connected to interfaces of the switch. When forwarding a data frame, the switch searches the MAC table for the outbound interface according to the destination MAC address of the frame. This reduces the number of broadcast frames.

5.2.1 MAC Table

You can enter the search criteria to search entries in the MAC table.

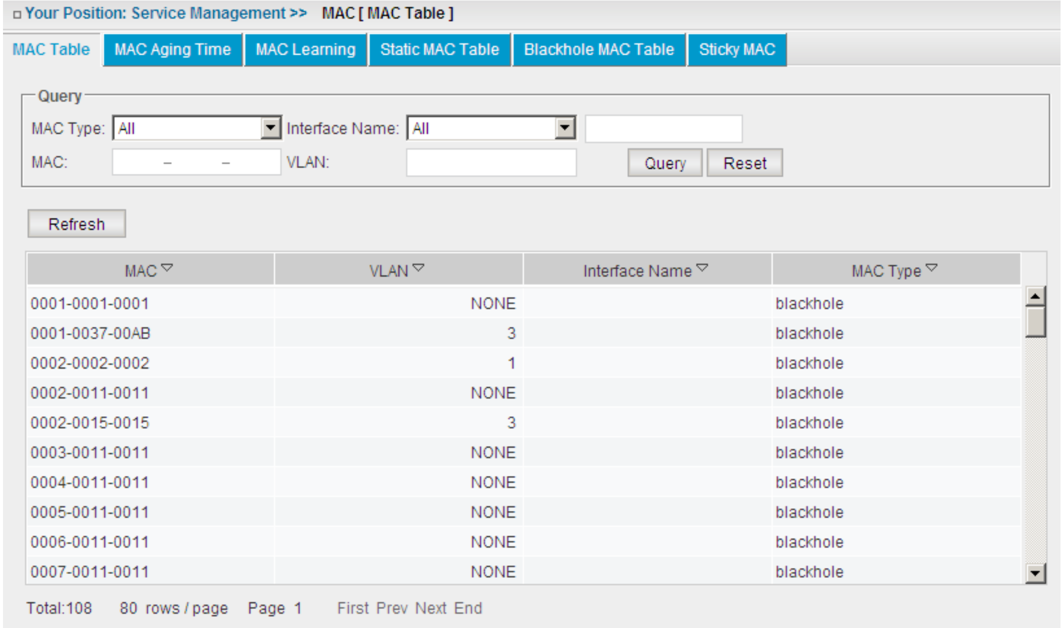
Context

The MAC table stores MAC addresses, VLAN IDs, and outbound interfaces learned by a switch. When forwarding an Ethernet frame, the switch searches the MAC table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

Procedure

Step 1 Choose **Service Management** > **MAC** > **MAC Table** in the navigation tree to open the **MAC Table** page, as shown in **Figure 5-11**.

Figure 5-11 MAC Table



Query

MAC Type: All
Interface Name: All
MAC: - -
VLAN:

MAC	VLAN	Interface Name	MAC Type
0001-0001-0001	NONE		blackhole
0001-0037-00AB	3		blackhole
0002-0002-0002	1		blackhole
0002-0011-0011	NONE		blackhole
0002-0015-0015	3		blackhole
0003-0011-0011	NONE		blackhole
0004-0011-0011	NONE		blackhole
0005-0011-0011	NONE		blackhole
0006-0011-0011	NONE		blackhole
0007-0011-0011	NONE		blackhole

Total:108 80 rows / page Page 1

Table 5-5 describes the parameters on the **MAC Table** page.

Table 5-5 MAC Table

Parameter	Description
MAC Type	Searches MAC entries based on the MAC entry type. The options are **All**, **Static**, **Dynamic**, **Blackhole**,and **Sticky**.
Interface Name	Searches MAC based on interfaces. Enter the interface type and number, for example, **Eth-Trunk12**.
MAC	Searches MAC entries based on MAC addresses.
VLAN	Searches MAC entries based on VLAN IDs.

Step 2 Set the search criteria.

Step 3 Click **Query**. The search results are displayed.

----End

5.2.2 MAC Aging Time

The MAC table needs to be updated constantly because the network topology always changes. The entries automatically generated in a MAC table are not always valid. Each entry has a lifecycle. If an entry is not updated within the lifecycle, it is deleted. This lifecycle is called the aging time. If an entry is updated before its lifecycle ends, the aging timer of the entry is reset.

Context

You need to set the aging time properly. If the aging time is excessively long or short, the switch may broadcast a large number of data frames because their destination MAC addresses cannot be found in the MAC table. This degrades the performance of the switch.

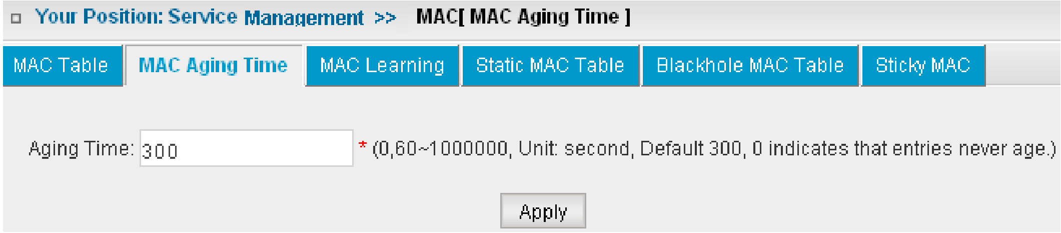
- If the aging time is excessively long, the switch may save a large number of useless MAC entries, and new MAC entries cannot be added because the number of MAC entries is limited. As a result, the switch cannot update the MAC table according to network changes.
- If the aging time is excessively short, the switch may delete valid MAC entries, and therefore the forwarding performance is degraded.

Generally, the default aging time (300s) is recommended.

Procedure

Step 1 Choose **Service Management** > **MAC** > **MAC Aging Time** in the navigation tree to open the **MAC Aging Time** page, as shown in **Figure 5-12**.

Figure 5-12 MAC Aging Time



Aging Time: 300 * (0,60~1000000, Unit: second, Default 300, 0 indicates that entries never age.)

Table 5-6 describes the parameters on the **MAC Aging Time** page.

Table 5-6 MAC Aging Time

Parameter	Description
Aging Time	Indicates the aging time of MAC entries.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.2.3 MAC Learning

A switch can learn source MAC addresses of data frames. After learning the interface connected to the destination host, the switch sends data frames to the interface instead of broadcasting data frames to all interfaces in the VLAN. **The S2700SI,S2700EI or S2752EI switches do not support the function.**

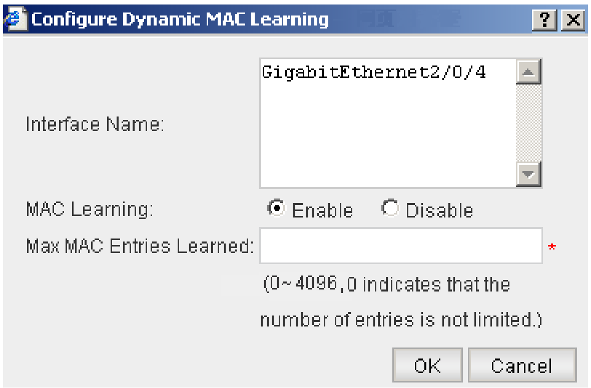
Context

By learning MAC addresses, a switch can obtain MAC addresses of devices on the network connected to an interface.

Procedure

- Query MAC address learning on an interface.
  1. Choose **Service Management** > **MAC** > **MAC Learning** in the navigation tree to open the **MAC Learning** page.
  2. Set the search criteria.
  3. Click **Query**. The search results are displayed.
- Configure MAC address learning on an interface.
  1. Choose **Service Management** > **MAC** > **MAC Learning** in the navigation tree to open the **MAC Learning** page.
  2. In the **Configure MAC Learning on Interface** group box, select a record and click **Configure**. The **Configure MAC Learning** page is displayed, as shown in **Figure 5-13**.

Figure 5-13 Configure Dynamic MAC Learning



Interface Name: GigabitEthernet2/0/4

MAC Learning: ● Enable ○ Disable

Max MAC Entries Learned: *

(0~4096,0 indicates that the number of entries is not limited.)

Table 5-7 describes the parameters on the **Configure MAC Learning** page.

Table 5-7 Configure Dynamic MAC Learning

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. NOTE If only one interface is selected, the configuration of the interface is displayed. If multiple interfaces are selected, the default settings of the interfaces are displayed.
MAC Learning	Indicates whether to enable MAC address learning.

Parameter	Description
Max MAC Entries Learned	Indicates the maximum number of MAC addresses that an interface can learn. This parameter limits the number of entries in the MAC table.

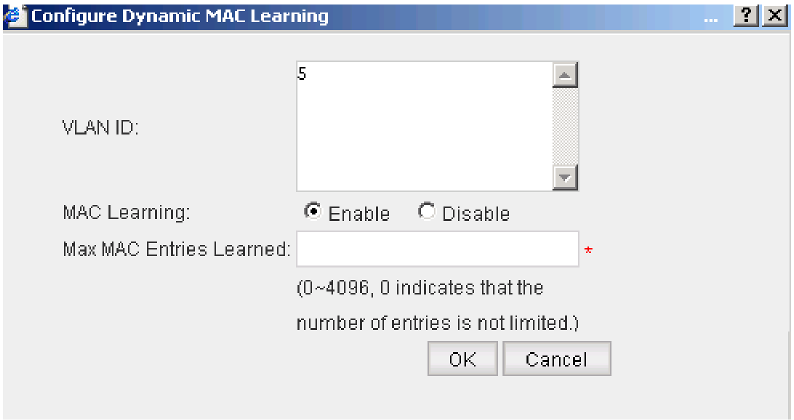
3. Set the parameters.
4. Click **OK**.

NOTE

To cancel the MAC address learning limit on an interface, select the corresponding record and click **Cancel Limit**.

- Query MAC address learning on a VLAN.
  1. Choose **Service Management** > **MAC** > **MAC Learning** in the navigation tree to open the **MAC Learning** page.
  2. Set the search criteria.
  3. Click **Query**. The search results are displayed.
- Configure MAC address learning on a VLAN.
  1. Choose **Service Management** > **MAC** > **MAC Learning** in the navigation tree to open the **MAC Learning** page.
  2. In the **Configure MAC Learning on VLAN** group box, select a record and click **Configure**. The **Configure MAC Learning** page is displayed, as shown in **Figure 5-14**.

Figure 5-14 Configure Dynamic MAC Learning



Configure Dynamic MAC Learning

VLAN ID: 5

MAC Learning: ● Enable ○ Disable

Max MAC Entries Learned: *

(0~4096, 0 indicates that the number of entries is not limited.)

Table 5-7 describes the parameters on the **Configure MAC Learning** page.

  3. Set the parameters.
  4. Click **OK**.

NOTE

To cancel the MAC address learning limit in a VLAN, select the corresponding record and click **Cancel Limit**.

----End

5.2.4 Static MAC Table

Static MAC entries are manually configured and never age.

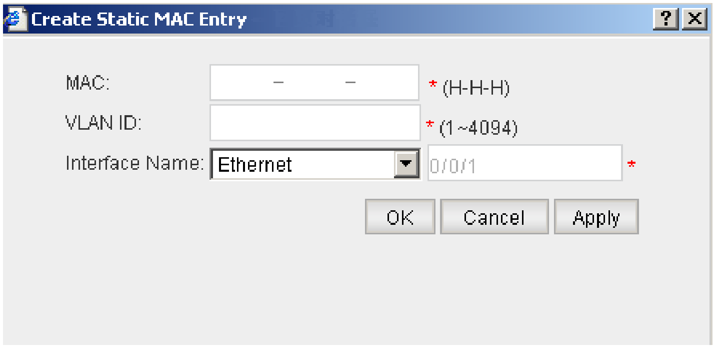
Context

.

Procedure

- Search static MAC entries.
  1. Choose **Service Management** > **MAC** > **Static MAC Table** in the navigation tree to open the **Static MAC Table** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Create a static MAC entry.
  1. Choose **Service Management** > **MAC** > **Static MAC Table** in the navigation tree to open the **Static MAC Table** page.
  2. Click **New** to open the **Create Static MAC Entry** page, as shown in **Figure 5-15**.

Figure 5-15 Create Static MAC Entry


Create Static MAC Entry

MAC: - - * (H-H-H)

VLAN ID: * (1~4094)

Interface Name: Ethernet 0/0/1 *

Table 5-8 describes the parameters on the **Create Static MAC Entry** page.

Table 5-8 Create Static MAC Entry

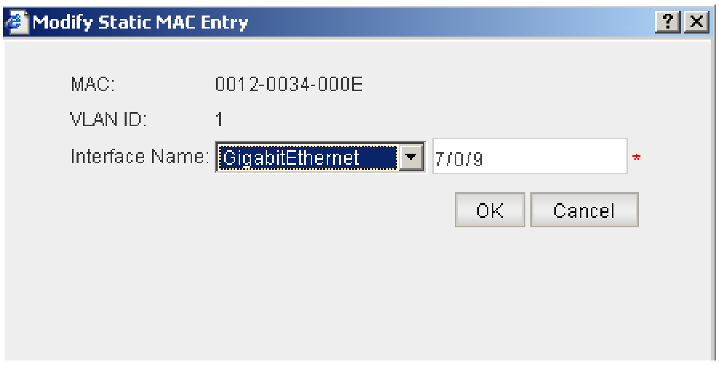
Parameter	Description
MAC	Indicates a MAC address in the format H-H-H. This parameter is mandatory.
VLAN ID	Indicates the IDs of VLANs. This parameter is mandatory.

Parameter	Description
Interface Name	Indicates the name of an interface, for example, **Eth-Trunk12**. This parameter is mandatory. NOTE The interface must be a member of the specified VLAN.

3. Set parameters.
4. Click **OK**.

- Modify a static MAC entry.
  1. Choose **Service Management** > **MAC** > **Static MAC Table** in the navigation tree to open the **Static MAC Table** page.
  2. Click ✎ to open the **Modify Static MAC Entry** page, as shown in **Figure 5-16**.

Figure 5-16 Modify Static MAC Entry



Modify Static MAC Entry

MAC: 0012-0034-000E

VLAN ID: 1

Interface Name: GigabitEthernet 7/0/9 *

NOTE

- **Table 5-8** describes the parameters on the **Modify Static MAC Entry** page.
- The VLAN ID and MAC address cannot be modified.

  3. Set parameters.
  4. Click **OK**.

- Delete a static MAC entry.
  1. Choose **Service Management** > **MAC** > **Static MAC Table** in the navigation tree to open the **Static MAC Table** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.2.5 Blackhole MAC Table

Blackhole MAC entries are used to discard data frames with the specified source or destination MAC addresses. They are manually configured and never age.

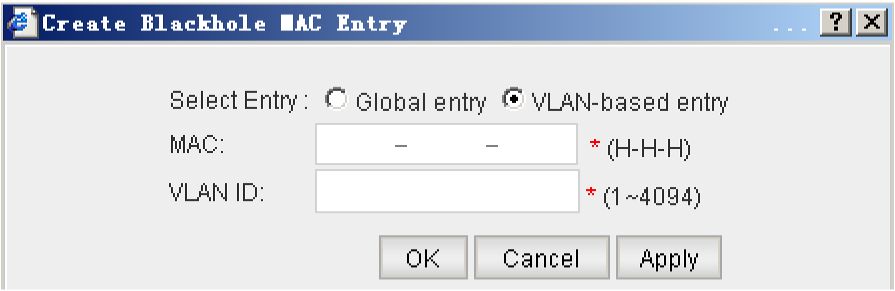
Context

A switch can learn 32 K MAC entries, including at most 1024 non-dynamic MAC entries.

Procedure

- Create a blackhole MAC entry.
  1. Choose **Service Management** > **MAC** > **Blackhole MAC Table** in the navigation tree to open the **Blackhole MAC Table** page.
  2. Click **New** to open the **Create Blackhole MAC Entry** page, as shown in **Figure 5-17**.

Figure 5-17 Create Blackhole MAC Entry



Create Blackhole MAC Entry

Select Entry : ○ Global entry ● VLAN-based entry

MAC: – – * (H-H-H)

VLAN ID: * (1~4094)

Table 5-9 describes the parameters on the **Create Blackhole MAC Entry** page.

Table 5-9 Create Blackhole MAC Entry

Parameter	Description
Select Entry	Indicates the type of a blackhole MAC entry. This parameter is mandatory. The options are: ● Global entry ● VLAN-based entry By default, **Global entry** is selected. NOTE S2700SI, S2700EI or S2752EI switches do not support the **Global entry** parameter.
MAC	Indicates a blackhole MAC address, in the format H-H-H.

Parameter	Description
VLAN ID	Indicates the IDs of VLANs. This parameter is mandatory. This parameter is available only when **VLAN-based entry** is selected.

3. Set parameters.
4. Click **OK**.

- Delete a blackhole MAC entry.
  1. Choose **Service Management** > **MAC** > **Blackhole MAC Table** in the navigation tree to open the **Blackhole MAC Table** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.2.6 Sticky MAC

You can configure the sticky MAC function on an interface. **The S2700SI switches do not support the sticky MAC function.**

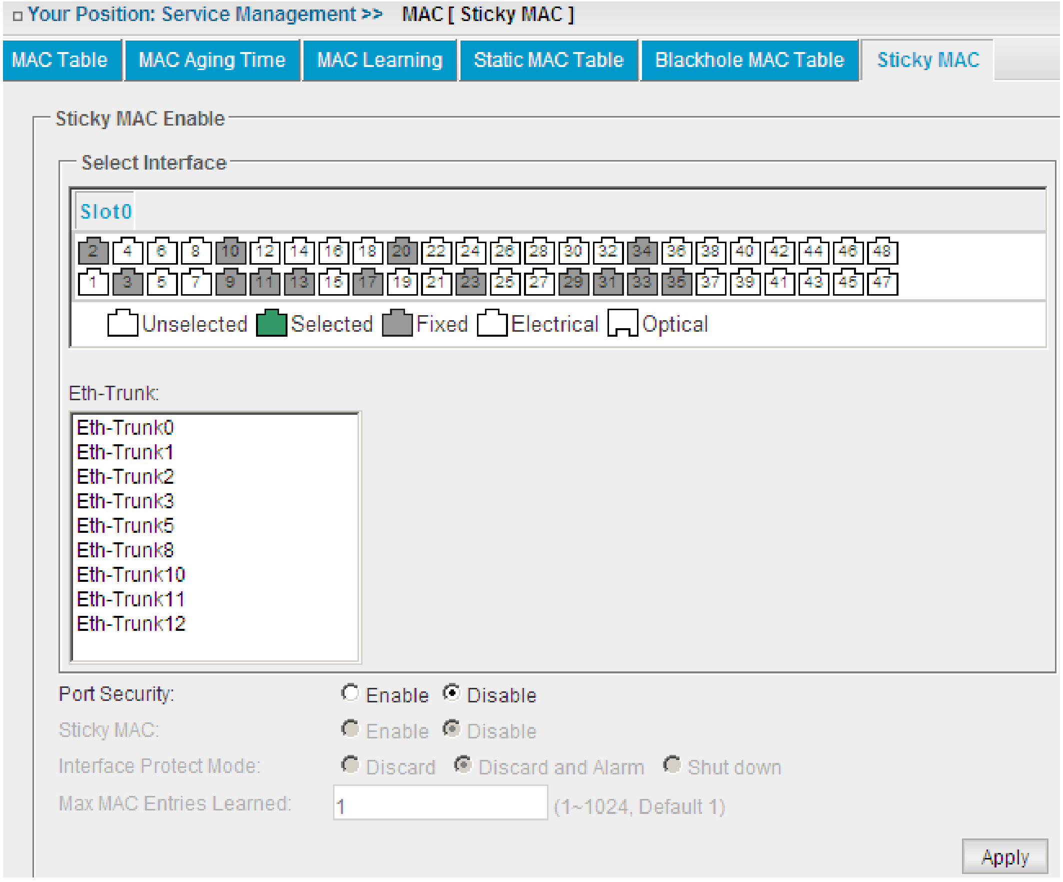
Context

After the sticky MAC function is enabled on an interface, the dynamic MAC addresses learned by the interface change to Sticky MAC addresses.

Procedure

- Enable the sticky MAC function.
  1. Choose **Service Management** > **MAC** > **Sticky MAC** in the navigation tree to open the **Sticky MAC** page.as shown in **Figure 5-18**.

Figure 5-18 Sticky MAC



Eth-Trunk:

- Eth-Trunk0
- Eth-Trunk1
- Eth-Trunk2
- Eth-Trunk3
- Eth-Trunk5
- Eth-Trunk8
- Eth-Trunk10
- Eth-Trunk11
- Eth-Trunk12

Port Security: ○ Enable ● Disable

Sticky MAC: ○ Enable ● Disable

Interface Protect Mode: ○ Discard ● Discard and Alarm ○ Shut down

Max MAC Entries Learned: 1 (1~1024, Default 1)

Table 5-10 describes the parameters in the **Sticky MAC Enable** group box on this page.

Table 5-10 Sticky MAC Enable

Parameter	Description
Port Security	Indicates whether to enable port security. The options are **Enable** and **Disable**. By default, port security is disabled. The following parameters are available only when **Enable** is selected.

Parameter	Description
Sticky MAC Enable	Indicates whether to enable the Sticky MAC function. The options are **Enable** and **Disable**. By default, the sticky MAC function is disabled. **NOTE** If the number of sticky MAC addresses on an interface does not reach the limit, the newly learned MAC addresses are converted to static MAC addresses. When the number of sticky MAC addresses reaches the limit, non-sticky MAC entries are deleted when new MAC addresses are learned.
Interface Protect Mode	Indicates the interface protection mode, that is, the action performed when the number of learned MAC addresses reaches the limit. The options are: ● Discard The interface discards all the subsequent packets whose source MAC addresses are not in the MAC table. ● Discard and Alarm The interface discards all the subsequent packets whose source MAC addresses are not in the MAC table and sends a trap. ● Shutdown The interface does not perform any action. If the sticky MAC function is disabled, the interface does not send a trap when the number of learned MAC addresses reaches the threshold even if you select the **Discard and Alarm** option. In this case, the interface only discards new packets whose source MAC addresses are not in the MAC table.
Max MAC Entries Learned	Indicates the maximum number of MAC addresses that an interface can learn. This parameter limits the number of entries in the MAC table.

2. Set the parameters.
3. Click **Apply** to complete the configuration.

----End

5.3 STP

The following sections describe how to query the STP information and set the global STP parameters, STP parameters on an interface, and parameters of an MST region. **The S2700SI switches do not support the STP function.**

The Spanning Tree Protocol (STP) is applicable to ring networks. It uses certain algorithms to implement path redundancy and prune a ring network into a tree-type network. This prevents increase and infinite circulation of packets in the ring network.

5.3.1 STP Information

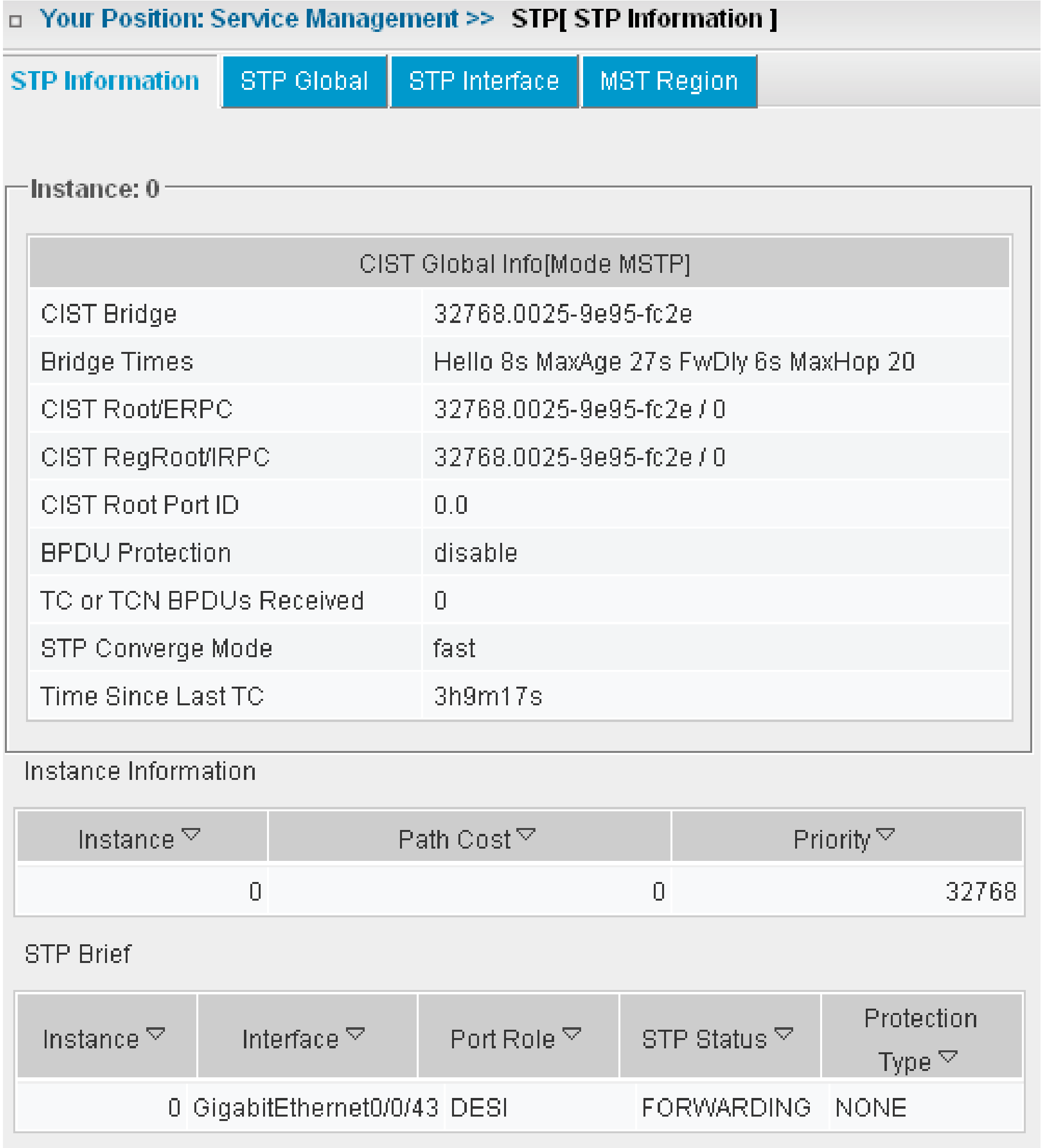
You can view STP information on the **STP Information** page.

Procedure

Step 1 Choose **Service Management** > **STP** > **STP Information** in the navigation tree to open the **STP Information** page.

Step 2 Detailed STP information is displayed, as shown in **Figure 5-19**.

Figure 5-19 STP Information



□ Your Position: Service Management >> STP[STP Information]
STP Information
STP Global
STP Interface
MST Region

Instance: 0

CIST Global Info[Mode MSTP]	
CIST Bridge	32768.0025-9e95-fc2e
Bridge Times	Hello 8s MaxAge 27s FwDly 6s MaxHop 20
CIST Root/ERPC	32768.0025-9e95-fc2e / 0
CIST RegRoot/IRPC	32768.0025-9e95-fc2e / 0
CIST Root Port ID	0.0
BPDU Protection	disable
TC or TCN BPDUs Received	0
STP Converge Mode	fast
Time Since Last TC	3h9m17s

Instance Information

Instance ▽	Path Cost ▽	Priority ▽
0	0	32768

STP Brief

Instance ▽	Interface ▽	Port Role ▽	STP Status ▽	Protection Type ▽
0	GigabitEthernet0/0/43	DESI	FORWARDING	NONE

----End

5.3.2 STP Global

You can set global STP parameters on the **STP Global** page.

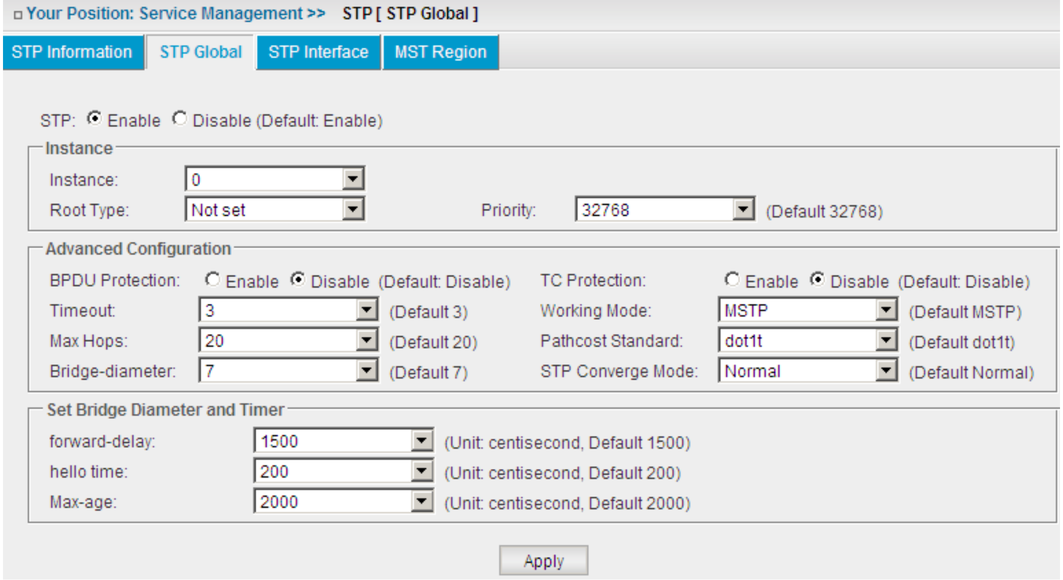
Context

On certain networks, you need to modify STP parameters of some switches to optimize their performance.

Procedure

Step 1 Choose **Service Management** > **STP** > **STP Global** in the navigation tree to open the **STP Global** page, as shown in **Figure 5-20**.

Figure 5-20 STP Global



Your Position: Service Management >> STP [STP Global]

STP Information | STP Global | STP Interface | MST Region

STP: ● Enable ○ Disable (Default: Enable)

Instance

Instance: 0

Root Type: Not set

Priority: 32768 (Default 32768)

Advanced Configuration

BPDU Protection: ○ Enable ● Disable (Default: Disable)

Timeout: 3 (Default 3)

Max Hops: 20 (Default 20)

Bridge-diameter: 7 (Default 7)

TC Protection: ○ Enable ● Disable (Default: Disable)

Working Mode: MSTP (Default MSTP)

Pathcost Standard: dot1t (Default dot1t)

STP Converge Mode: Normal (Default Normal)

Set Bridge Diameter and Timer

forward-delay: 1500 (Unit: centisecond, Default 1500)

hello time: 200 (Unit: centisecond, Default 200)

Max-age: 2000 (Unit: centisecond, Default 2000)

Table 5-11 describes the parameters on the **STP Global** page.

Table 5-11 STP Global

Parameter		**Description**
STP		Indicates whether to enable STP. The options are **Enable** and **Disable**. By default, STP is Enable.
Instance	Instance	Indicates the ID of a multi-spanning tree instance (MSTI). You can select any MSTI ID ranging from 0 to 48. NOTE S2700EI or S2752EI series switches MSTI ID ranging from 0 to 16.

Parameter		Description
	Root Type	Indicates the root type of the switch. The options are: ● Not set The root type is not set. ● Primary The switch is configured as root switch of the MSTI. ● Secondary The switch is configured as the backup root switch of the MSTI. By default, the **Not set** option is selected.
	Priority	Specifies the priority of the switch. The priority is a major basis for the spanning tree calculation. You can set different priorities for a switch in different MSTIs. NOTE In an instance, if **Root Type** is **Not set**, you can select a priority from the drop-down list box. If **Root Type** is **Primary** or **Secondary**, the priority cannot be set.
Advanced Configuration	BPDU Protection	Indicates whether to enable BPDU protection. The options are **Enable** and **Disable**. By default, BPDU protection is disabled. After BPDU protection is enabled , the switch shuts down the edge interfaces that receive BPDUs and notifies the NMS. .The shutdown interfaces can only be manually started by the network administrator.
	TC Protection	Indicates whether to enable topology change (TC) protection. The options are **Enable** and **Disable**. By default, TC protection is disabled. The TC protection function prevents topology changes caused by incorrect configuration or malicious attacks.
	Timeout	Indicates the timeout interval. The timeout interval is calculated based on the hello interval and hello time multiplier.
	Working Mode	Indicates the working mode of STP. The options are: ● MSTP The switch sends MSTP BPDUs in this mode. ● STP The switch sends STP BPDUs in this mode. ● RSTP The switch sends RSTP BPDUs in this mode. The default mode is MSTP.

Parameter		Description
	Max Hops	Indicates the maximum hop count of the spanning tree in an MST region. The default value is 20. This parameter limits the network scale of the spanning tree in the MST region. A configuration message has the maximum hop count on the root bridge. The hop count decreases by 1 every time the configuration message passes a switch. When the hop count decreases to 0, the configuration message is discarded; therefore, switches with larger hop count from the root bridge cannot participate in the spanning tree calculation. This limits the network scale in an MST region.
	Pathcost Standard	Indicates the algorithm used to calculate the path cost. The options are: ● dot1t Indicates the algorithm defined in IEEE 802.1t. ● dot1d-1998 Indicates the algorithm defined in IEEE 802.1d. ● legacy Indicates Huawei proprietary algorithm. The default algorithm is **dot1t**.
	Bridge-diameter	Indicates the network diameter in the MST region. The default value is 7. The network diameter refers to the maximum number of devices between any two devices on a network. The network diameter reflects the network scale.
	STP Converge Mode	Indicates the STP convergence mode. The options are: ● Fast In this mode, the switch deletes the useless MAC address entries and ARP entries directly. ● Normal In this mode, the switch sets the remaining aging time of the MAC address entries and the ARP entries to 0 and ages them. If the number of ARP aging detection times is greater than 0, the switch carries out aging detection of the ARP entries. The default mode is **Normal**.
Set Bridge Diameter and Timer	forward-delay	Indicates the delay of port status transition. The default value is 1500.
	hello time	Indicates the interval for sending hello packets. The root bridge sends hello packets at this interval to check whether faulty links exist. The default value is 200.

Parameter		Description
	Max-age	Indicates the maximum lifetime of a configuration message. This parameter determines whether a configuration message has expired. The default value is 2000.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.3.3 STP Interface

You can set STP parameters on an interface.

Context

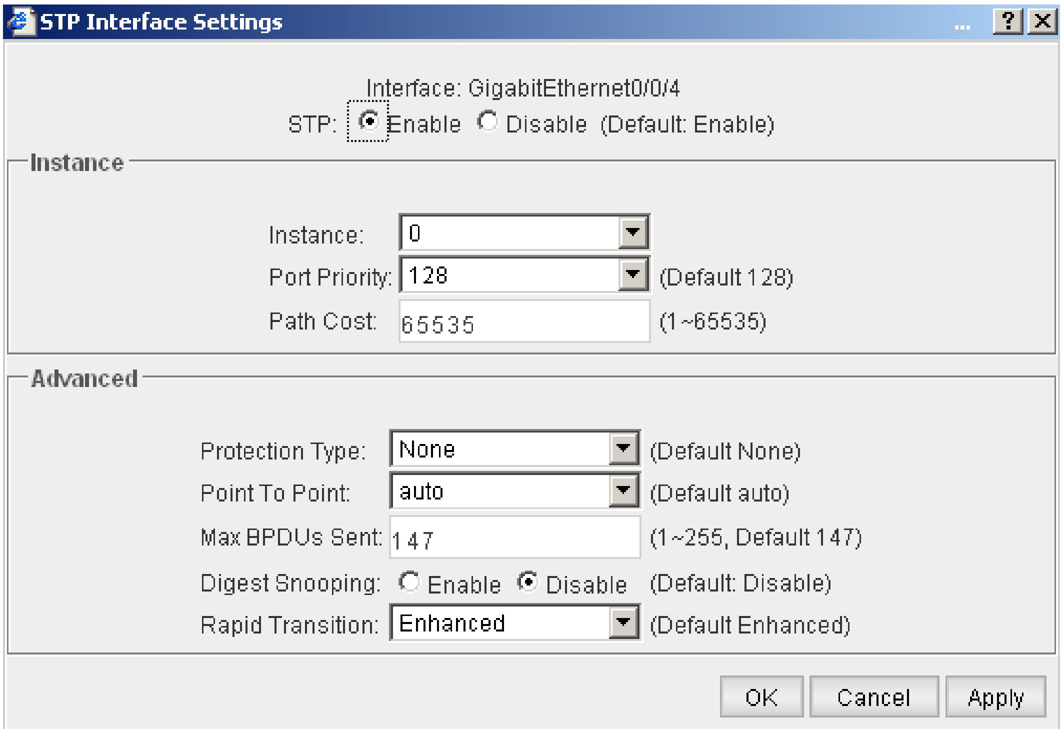
On certain networks, you need to modify STP parameters of some switches to optimize their performance.

Procedure

Step 1 Choose **Service Management** > **STP** > **STP Interface** in the navigation tree to open the **STP Interface** page.

Step 2 Select an interface and click **Configure** to open the **STP Interface Settings** page, as shown in **Figure 5-21**.

Figure 5-21 STP Interface Settings



Interface: GigabitEthernet0/0/4

STP: ● Enable ○ Disable (Default: Enable)

Instance

Instance: 0

Port Priority: 128 (Default 128)

Path Cost: 65535 (1~65535)

Advanced

Protection Type: None (Default None)

Point To Point: auto (Default auto)

Max BPDUs Sent: 147 (1~255, Default 147)

Digest Snooping: ○ Enable ● Disable (Default: Disable)

Rapid Transition: Enhanced (Default Enhanced)

Table 5-12 describes the parameters on the **STP Interface Settings** page.

Table 5-12 STP Interface Settings

Parameter		Description
Interface		Indicates the name of an interface. It is displayed automatically and cannot be modified after you select an interface. You can select only one interface each time.
STP		Indicates whether to enable STP. By default, STP is enabled. When STP is disabled on an interface, the interface does not take part in the spanning tree calculation and is always in Forwarding state. NOTE Loops may occur when STP is disabled on an interface.
Instance	Instance	Indicates the ID of an MSTI. You can select any MSTI ID ranging from 0 to 48. NOTE S2700EI or S2752EI series switches MSTI ID ranging from 0 to 16.
	Port Priority	Indicates the priority of the interface. The priority of an interface affects its role in the specified MSTI. You can set different priorities for an interface in different MSTIs so that traffic of VLANs can be load balanced among different physical links. NOTE When the priority of an interface changes, MSTP recalculates the role of the interface and changes the status of the interface.
	Path Cost	Indicates the path cost of the interface. The value range varies according to the calculation algorithm of path costs. The value ranges from 1 to 200000 when Huawei proprietary algorithm is used; the value ranges from 1 to 65535 when the algorithm defined in IEEE 802.1D is used; the value ranges from 1 to 200000000 when the algorithm defined in IEEE 802.1t is used. The path cost is the basis for calculating the spanning tree. If you set different path costs for an interface in different MSTIs, traffic of different VLANs is load balanced among multiple physical links. NOTE When the path cost of an interface changes, the MSTP recalculates the spanning tree based on the new path cost.

Parameter		Description
Advanced	Protection Type	Indicates the protection type on an interface. The options are: ● None No protection type is adopted. ● Edge port When the spanning tree is recalculated, edge ports transit to the Forwarding state directly, which reduces the status transition time. If an Ethernet port is not connected to any Ethernet port of the switch, you need to configure the Ethernet port as an edge port. ● Root protection Root protection prevents topology changes caused by incorrect configurations or malicious attacks. ● Loop protection When link congestion occurs or a unidirectional link is generated, the port connected to the link cannot receive BPDUs from the upstream switch. In this case, the local switch selects a new root port, the original root port becomes the designated port, and the blocked port transits to the Forwarding state. Loop is then generated on the switching network. To prevent this problem, you can enable loop protection.
	Point To Point	Indicates the point-to-point connection type of the interface. The options are: ● auto The interface automatically detects whether it is connected to a point-to-point link. ● force-true The interface is connected to a point-to-point link. ● force-false The interface is not connected to a point-to-point link. The default value is **auto**.
	Max BPDUs Sent	Indicates the maximum number of BPDUs that an interface can send in a hello interval. A larger value indicates more BPDUs sent in a hello interval and therefore more system resources occupied. A proper value of this parameter can limit the rate of sending BPDUs and prevent excessive bandwidth usage when network flapping occurs.

Parameter		Description
	Digest Snooping	Indicates whether to enable digest snooping. By default, digest snooping is disabled. NOTE You can configure digest snooping to make the BPDU key of a Huawei device the same as that of a third-party device.
	Rapid Transition	Indicates the rapid status transition mode. The options are **Normal** and **Enhanced**. The default value is **Enhanced**.

Step 3 Set the parameters.

Step 4 Click **OK**.

NOTE

Select a record on the **STP Interface Settings** page and click **Details**. Detailed STP settings of the interface are displayed.

----End

5.3.4 MST Region

You can modify the configuration of an MST region.

Context

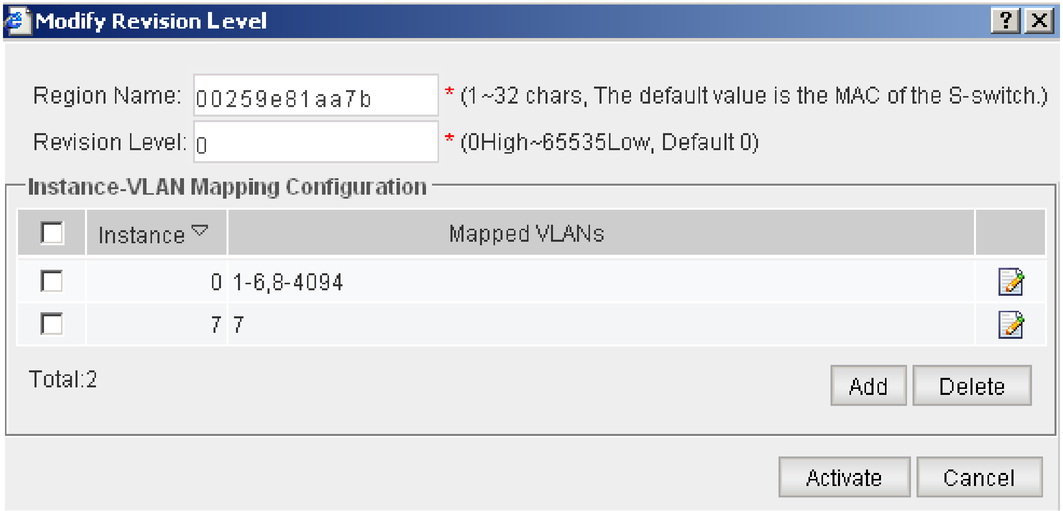
You need to modify the configuration of an MST region when you want to add a switch that is not enabled with STP to the MST region or move a switch enabled with STP from one MST region to another.

Procedure

Step 1 Choose **Service Management** > **STP** > **MST Region** in the navigation tree to open the **MST Region** page.

Step 2 Click **Modify** to open the **Modify Revision level** page, as shown in **Figure 5-22**.

Figure 5-22 Modify Revision level



Region Name: 00259e81aa7b * (1~32 chars, The default value is the MAC of the S-switch.)

Revision Level: 0 * (0High~65535Low, Default 0)

□	Instance	Mapped VLANs
□	0	1-6,8-4094
□	7	7

Total:2

Table 5-13 describes the parameters on the **Modify Revision level** page.

Table 5-13 Modify Revision level

Parameter	Description
Region Name	Indicates the name of an MST region. The default value is the MAC address of the main control board of the switch. The MST region name, the VLAN mapping table, and the MSTP revision level identify the region that the switch belongs to.
Revision Level	Indicates the MSTP revision level of the MST region. The MST region name, the VLAN mapping table, and the MSTP revision level identify the region that the switch belongs to.
Instance-VLAN Mapping Configuration	Indicates the mappings between MSTIs and VLANs. You can add, modify, or delete a mapping. The following step is to add a mapping.

Add an instance-VLAN mapping.

1. Click **Add** to open the **Add Instance-VLAN Mapping** page.
2. Set the parameters.

NOTE

You need to set the following parameters:

- **Instance**: select an instance ID.
- **VLAN**: enter a VLAN ID.

3. Click **Add**.

Step 3 Set the parameters.

Step 4 Click **Activate** to complete the configuration.

----End

5.4 Voice VLAN

A voice VLAN is assigned to voice data flows. You can create a voice VLAN and add the interface connected to a voice device to the voice VLAN. Then voice data flows can be transmitted on the voice VLAN. **The S2700SI switches do not support the voice VLAN function.**

By configuring a voice VLAN, you can set quality of service (QoS) parameters for voice data flows to increase the priority of the voice service and improve the quality of calls.

5.4.1 Voice VLAN

You can set parameters of a voice VLAN.

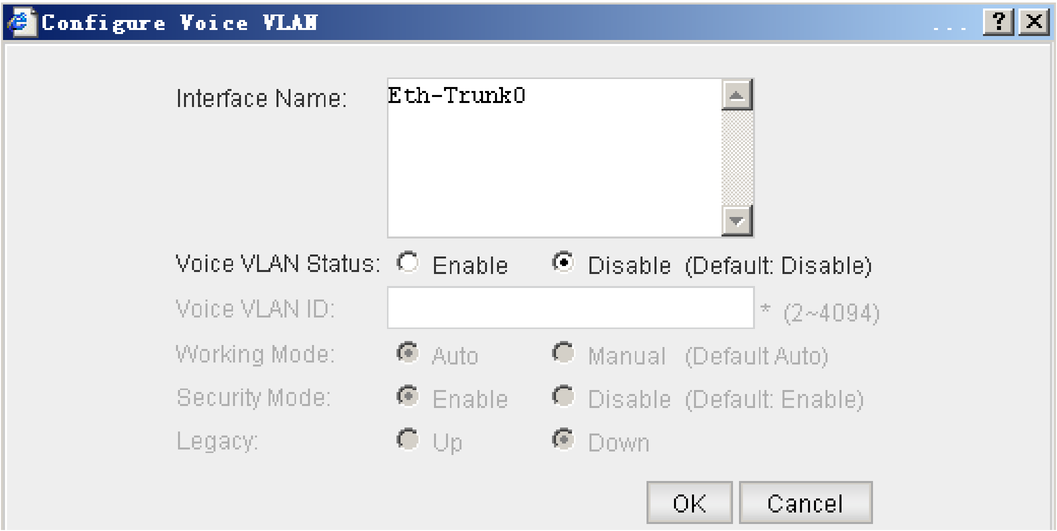
Context

- A voice VLAN is assigned to voice data flows. You can create a voice VLAN and add the interface connected to a voice device to the voice VLAN. Then voice data flows can be transmitted in the voice VLAN.
- After a voice VLAN is configured, interfaces connected to IP voice devices can be added to or deleted from the voice VLAN automatically or manually and voice data flows can be transmitted in the voice VLAN.

Procedure

- Query voice VLAN information.
  1. Choose **Service Management** > **Voice VLAN** > **Voice VLAN** in the navigation tree to open the **Voice VLAN** page.
  2. Set the search criteria.
  3. Click **Query** to display all the matching records.
- Configure a voice VLAN.
  1. Choose **Service Management** > **Voice VLAN** > **Voice VLAN** in the navigation tree to open the **Voice VLAN** page.
  2. Select an interface and click **Configure** to open the **Configure Voice VLAN** page, as shown in **Figure 5-23**.

Figure 5-23 Configure Voice VLAN



Interface Name: Eth-Trunk0

Voice VLAN Status: ○ Enable ● Disable (Default: Disable)

Voice VLAN ID: * (2~4094)

Working Mode: ● Auto ○ Manual (Default Auto)

Security Mode: ● Enable ○ Disable (Default: Enable)

Legacy: ○ Up ● Down

Table 5-14 describes the parameters on the **Configure Voice VLAN** page.

Table 5-14 Configure Voice VLAN

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. **NOTE** If only one interface is selected, the configuration of the interface is displayed on the **Configure Voice VLAN** page. If multiple interfaces are selected, the default settings of the interfaces are displayed.
Voice VLAN Status	Indicates whether to enable the voice VLAN function. The options are **Enable** and **Disable**. By default, the value is **Disable**.
Voice VLAN ID	Indicates the ID of the voice VLAN. This parameter is mandatory when the voice VLAN function is enabled.
Working Mode	Indicates the working mode of the voice VLAN. The options are **Auto** and **Manual**. This parameter is valid only when the voice VLAN function is enabled.
Security Mode	Indicates whether to enable the security mode. The options are **Enable** and **Disable**. By default, the value is **Disable**. This parameter is valid only when the voice VLAN function is enabled.
Legacy	Whether an interface can communicate with third-party voice devices. The options are **Up** and **Down**.

3. Set the parameters.

4. Click **OK**.

----End

5.4.2 Voice VLAN OUI

A switch checks whether an incoming flow is a voice data flow according to the source MAC address of the data flow. If the source MAC address of the data flow matches the organizationally unique identifier (OUI) address set in the system, the switch considers the data flow as a voice data flow. When an interface receives a voice data flow, the interface is added to the voice VLAN automatically. The voice flows with the voice VLAN tag sent from the voice device connected to the interface can be forwarded by the interface.

Context

You can set an OUI address. The OUI is the first 24 bits of a MAC address. The institute of Electrical and Electronics Engineers (IEEE) assigns an OUI to each vendor and you can identify the vendor of a device according to the OUI. You can set the mask of the OUI on the switch to adjust the length of the MAC address that the switch matches with the OUI.

Procedure

- Create a voice VLAN OUI.
  1. Choose **Service Management** > **Voice VLAN** > **Voice VLAN OUI** in the navigation tree to open the **Voice VLAN OUI** page.
  2. Click **New** to open the **Create a Voice VLAN OUI** page, as shown in **Figure 5-24**.

Figure 5-24 Create a Voice VLAN OUI

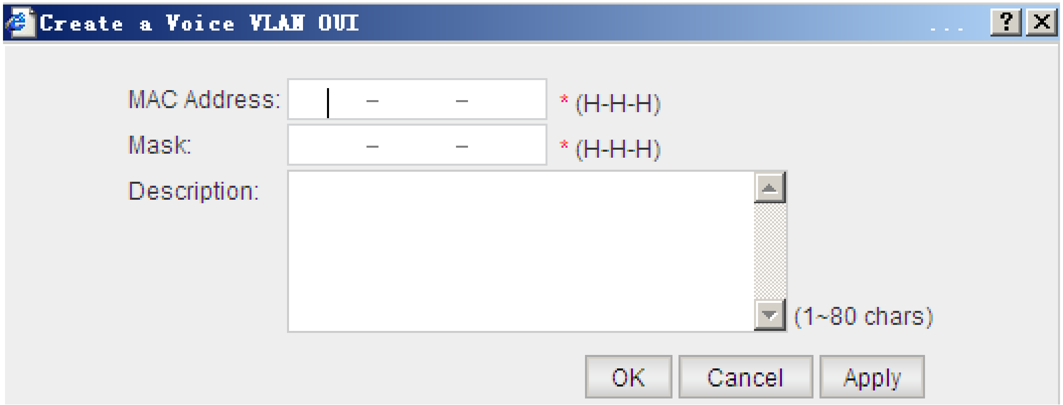


Table 5-15 describes the parameters on the **Create a Voice VLAN OUI** page.

Table 5-15 Create a Voice VLAN OUI

Parameter	Description
MAC Address	Indicates the MAC address of voice packets. This parameter is mandatory. The value is in the format **H-H-H**.

Parameter	Description
Mask	Indicates the mask of the OUI address. This parameter is mandatory. The value is in the format **H-H-H**.
Description	Indicates the description of the OUI address.

3. Set parameters.
4. Click **OK**.

- Delete a voice VLAN OUI.
  1. Choose **Service Management** > **Voice VLAN** > **Voice VLAN OUI** in the navigation tree to open the **Voice VLAN OUI** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.4.3 Aging Time

You can set the aging time of an interface in the voice VLAN.

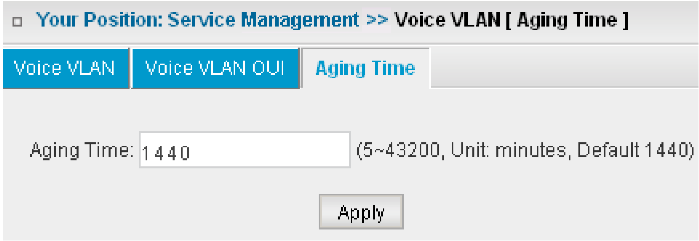
Context

If an interface has not updated the OUI address (no voice data flows pass through) when the aging time expires, the interface is deleted from the voice VLAN. By default, the aging time is set to 1440 minutes.

Procedure

Step 1 Choose **Service Management** > **Voice VLAN** > **Aging Time** in the navigation tree to open the **Aging Time** page, as shown in **Figure 5-25**.

Figure 5-25 Aging Time



Your Position: Service Management >> Voice VLAN [Aging Time]

Aging Time: 1440 (5~43200, Unit: minutes, Default 1440)

Table 5-16 describes the parameters on the **Aging Time** page.

Table 5-16 Aging Time

Parameter	Description
Aging Time	Indicates the aging time of an interface in the voice VLAN. The default value is 1440 minutes.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.5 DHCP

The switch supports Dynamic Host Configuration Protocol (DHCP) applications based on the global address pool or an address pool configured on a VLANIF interface. The switch also provides security guarantee for DHCP services and supports DHCP relay. **The S2700EI, S2700SI, S2752EI switches do not support the function.**

DHCP is a technology used to dynamically manage and configure clients in a concentrated manner. DHCP adopts the client/server model. The client applies to the server for configurations such as the IP address, subnet mask, and default gateway, and the server replies with corresponding configurations according to policies.

5.5.1 DHCP

You can set DHCP parameters only after enabling global DHCP.

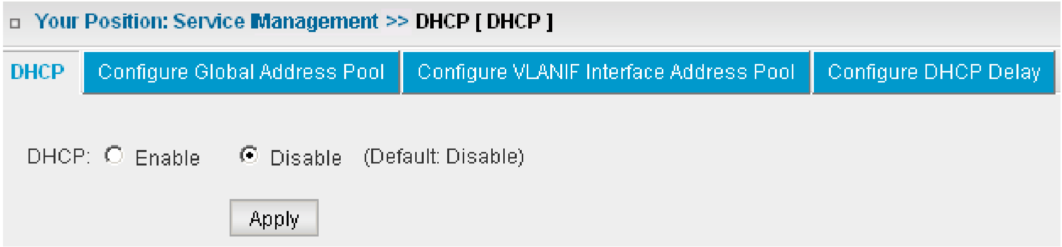
Context

You must enable DHCP before configuring the DHCP server and DHCP relay.

Procedure

Step 1 Choose **Service Management** > **DHCP** > **DHCP** in the navigation tree to open the **DHCP** page, as shown in **Figure 5-26**.

Figure 5-26 DHCP


□ Your Position: Service Management >> DHCP [DHCP]
DHCP
Configure Global Address Pool
Configure VLANIF Interface Address Pool
Configure DHCP Delay
Apply

DHCP: ○ Enable ● Disable (Default: Disable)

Table 5-17 describes the parameters on the **DHCP** page.

Table 5-17 DHCP

Parameter	Description
DHCP	Indicates whether to enable DHCP. By default, DHCP is disabled.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.5.2 Configure Global Address Pool

A DHCP server can allocate IP addresses to clients by using the global address pool.

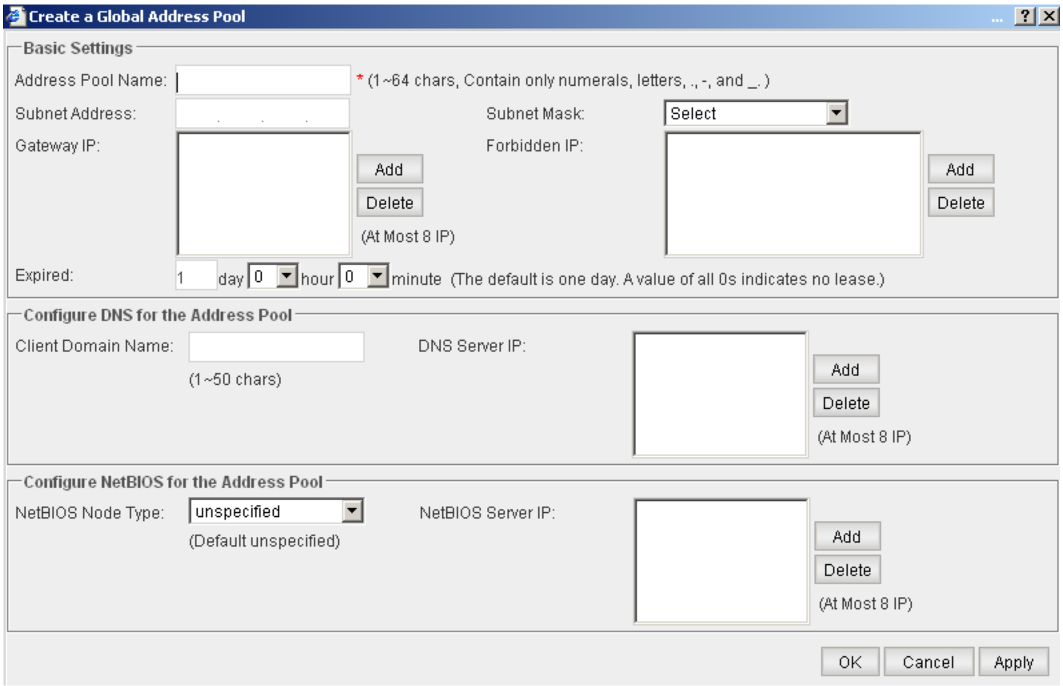
Context

- You need to configure a DHCP server based on the global address pool to enable computers to obtain IP addresses from the switch dynamically.
- A DHCP server based on the global address pool works with a DHCP relay agent.

Procedure

- Create a global address pool.
  1. Choose **Service Management** > **DHCP** > **Configure Global Address Pool** in the navigation tree to open the **Configure Global Address Pool** page.
  2. Click **New** to open the **Create a Global Address Pool** page, as shown in **Figure 5-27**.

Figure 5-27 Create a Global Address Pool



Create a Global Address Pool

Basic Settings

Address Pool Name: * (1~64 chars, Contain only numerals, letters, ., -, and _.)

Subnet Address: . . .

Subnet Mask: Select

Gateway IP: (At Most 8 IP)

Forbidden IP:

Expired: 1 day 0 hour 0 minute (The default is one day. A value of all 0s indicates no lease.)

Configure DNS for the Address Pool

Client Domain Name: (1~50 chars)

DNS Server IP: (At Most 8 IP)

Configure NetBIOS for the Address Pool

NetBIOS Node Type: unspecified (Default unspecified)

NetBIOS Server IP: (At Most 8 IP)

Table 5-18 describes the parameters on the **Create a Global Address Pool** page.

Table 5-18 Create a Global Address Pool

Parameter		Description
Basic Settings	Address Pool Name	Indicates the name of an address pool.
	Subnet Address	Indicates the IP subnet of the address pool.
	Subnet Mask	Indicates the mask of the IP subnet. Select a mask from the drop-down list box, for example, **24 (255.255.0.0)**.
	Gateway IP	Indicates the IP address of a gateway. You can configure a maximum of eight gateway IP addresses.
	Expired	Indicates the lease of dynamic IP addresses. The default lease is one day. The value range is as follows: ● **day**: an integer ranging from 0 to 999 ● **hour**: an integer ranging from 0 to 23 ● **minute**: an integer ranging from 0 to 59 NOTE Different address pools can have different IP address leases, but addresses in one pool have the same lease.
	Forbidden IP	Indicates the IP address that will not be dynamically allocated to users. Some IP addresses are allocated to applications such as the DNS server and cannot be allocated to users. You can specify these IP addresses as forbidden IP addresses. NOTE To add a forbidden IP address, click **Add**. To delete a forbidden IP address, select it and click **Delete**.
Configure DNS for the Address Pool	Client Domain Name	Indicates the domain name allocated by the DHCP server to the client.

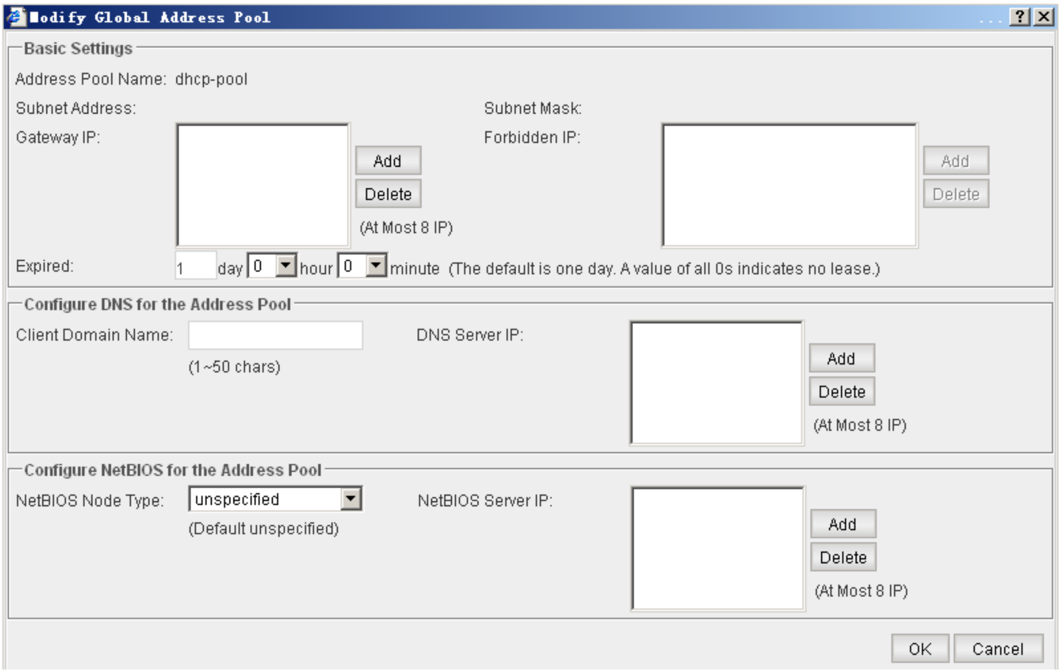
Parameter		Description
	DNS Server IP	Indicates the IP address of a DNS server. You can configure a maximum of eight DNS server addresses. **NOTE** To add a DNS server address, click **Add**. To delete a DNS server address, select it and click **Delete**.
Configure NetBIOS for the Address Pool	NetBIOS Node Type	Indicates the type of a NetBIOS node. The options are: ● unspecified The NetBIOS node type is not specified. ● b-node The NetBIOS node obtains the mapping between the host name and IP address in broadcast mode. b represents broadcast. ● p-node The NetBIOS node obtains the mapping between the host name and IP address by communicating with the NetBIOS server. p represents peer to peer. ● m-node The NetBIOS node is a p-type node with some broadcast features. m represents mixed. ● h-node The NetBIOS node is a b-type node using the peer-to-peer communication mechanism. h represents hybrid. The default value is **unspecified**.
	NetBIOS Server IP	Indicates the IP address of a NetBIOS server. You can configure a maximum of eight NetBIOS server addresses. **NOTE** To add a NetBIOS server address, click **Add**. To delete a NetBIOS server address, select it and click **Delete**.

3. Set parameters.
4. Click **OK**.

- Modify a global address pool.
  1. Choose **Service Management** > **DHCP** > **Configure Global Address Pool** in the navigation tree to open the **Configure Global Address Pool** page.

2. Click 📝 to open the **Modify Global Address Pool** page, as shown in **Figure 5-28**.

Figure 5-28 Modify Global Address Pool



Modify Global Address Pool

Basic Settings

Address Pool Name: dhcp-pool

Subnet Address:

Subnet Mask:

Gateway IP:

Forbidden IP:

(At Most 8 IP)

Expired: 1 day 0 hour 0 minute (The default is one day. A value of all 0s indicates no lease.)

Configure DNS for the Address Pool

Client Domain Name: (1~50 chars)

DNS Server IP: (At Most 8 IP)

Configure NetBIOS for the Address Pool

NetBIOS Node Type: unspecified (Default unspecified)

NetBIOS Server IP: (At Most 8 IP)

NOTE

- **Table 5-18** describes the parameters on the **Modify Global Address Pool** page.
- The address pool name cannot be modified.

3. Set parameters.
4. Click **OK**.

- Delete a global address pool.

1. Choose **Service Management** > **DHCP** > **Configure Global Address Pool** in the navigation tree to open the **Configure Global Address Pool** page.
2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

3. Click **OK**.

----End

5.5.3 Configure VLANIF Interface Address Pool

If a DHCP server based on a VLANIF interface address pool is configured, all the users going online through this interface obtain IP addresses from the VLANIF interface address pool.

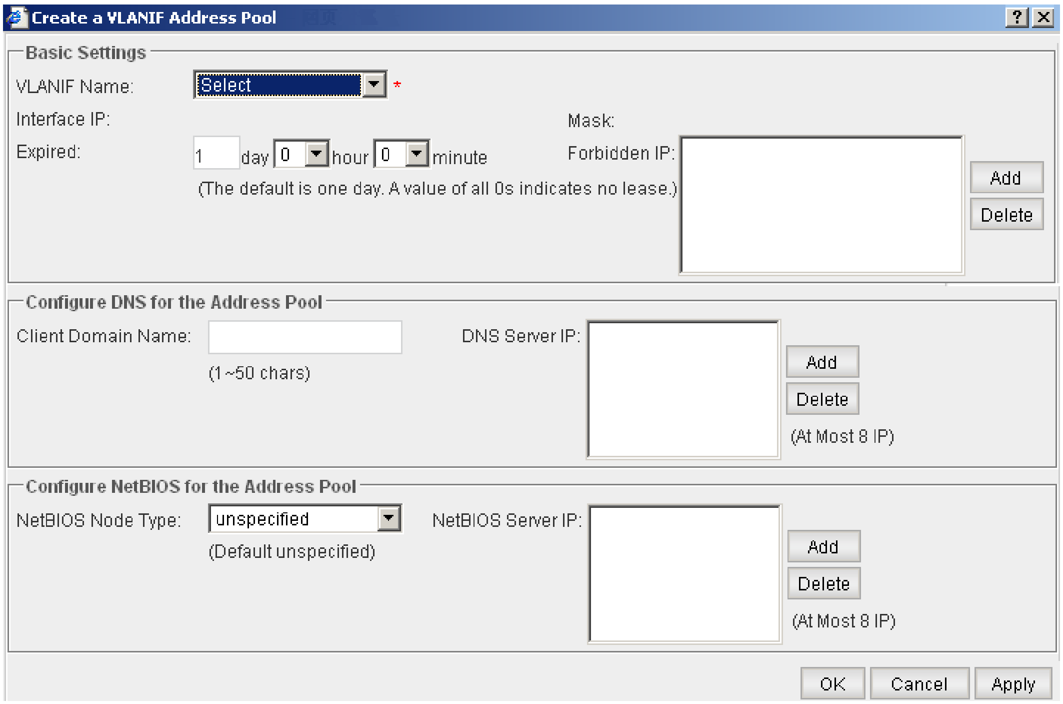
Context

- Before configuring an address pool on a VLANIF interface, you must enable DHCP.
- You can configure an address pool on a VLANIF interface when a device supports switched Ethernet interfaces. IP addresses cannot be configured on switched Ethernet interfaces directly; therefore, you need to create a VLANIF interface and configure a DHCP address pool on the VLANIF interface.
- The interface address pool takes precedence over the global address pool. If an address pool is configured on an interface, clients obtain IP addresses preferentially from the interface address pool even if a global address pool is configured.

Procedure

- Query information about a VLANIF interface address pool.
  1. Choose **Service Management** > **DHCP** > **Configure VLANIF Interface Address Pool** in the navigation tree to open the **Configure VLANIF Interface Address Pool** page.
  2. Set the search criteria.
  3. Click **Query** to display all the matching records.
- Create a VLANIF address pool.
  1. Choose **Service Management** > **DHCP** > **Configure VLANIF Interface Address Pool** in the navigation tree to open the **Configure VLANIF Interface Address Pool** page.
  2. Click **New** to open the **Create a VLANIF Address Pool** page, as shown in **Figure 5-29**.

Figure 5-29 Create a VLANIF Address Pool



Create a VLANIF Address Pool

Basic Settings

VLANIF Name: Select *

Interface IP:

Mask:

Expired: 1 day 0 hour 0 minute

(The default is one day. A value of all 0s indicates no lease.)

Forbidden IP:

Configure DNS for the Address Pool

Client Domain Name:

(1~50 chars)

DNS Server IP:

(At Most 8 IP)

Configure NetBIOS for the Address Pool

NetBIOS Node Type: unspecified

(Default unspecified)

NetBIOS Server IP:

(At Most 8 IP)

Table 5-19 describes the parameters on the **Create a VLANIF Address Pool** page.

Table 5-19 Create a VLANIF Address Pool

Parameter		Description
Basic Settings	VLANIF Name	Indicates the name of a VLNAIF interface. Select a name from the drop-down list box. NOTE The VLANIF interfaces in the drop-down list box are created in the **Interface Management** module.
	Interface IP	Indicates the IP address of the selected VLANIF interface. The value is displayed automatically after you select a VLANIF interface.
	Mask	Indicates the subnet mask of the selected VLANIF interface. The value is displayed automatically after you select a VLANIF interface.
	Expired	Indicates the lease of dynamic IP addresses. The default lease is one day. The value range is as follows: ● **day**: an integer ranging from 0 to 999 ● **hour**: an integer ranging from 0 to 23 ● **minute**: an integer ranging from 0 to 59 NOTE Different address pools can have different IP address leases, but addresses in one pool have the same lease.
	Forbidden IP	Indicates the IP address that will not be dynamically allocated to users. Some IP addresses are allocated to applications such as the DNS server and cannot be allocated to users. You can specify these IP addresses as forbidden IP addresses. NOTE To add a forbidden IP address, click **Add**. To delete a forbidden IP address, select it and click **Delete**.
Configure DNS for the Address Pool	Client Domain Name	Indicates the domain name allocated by the DHCP server to the client.

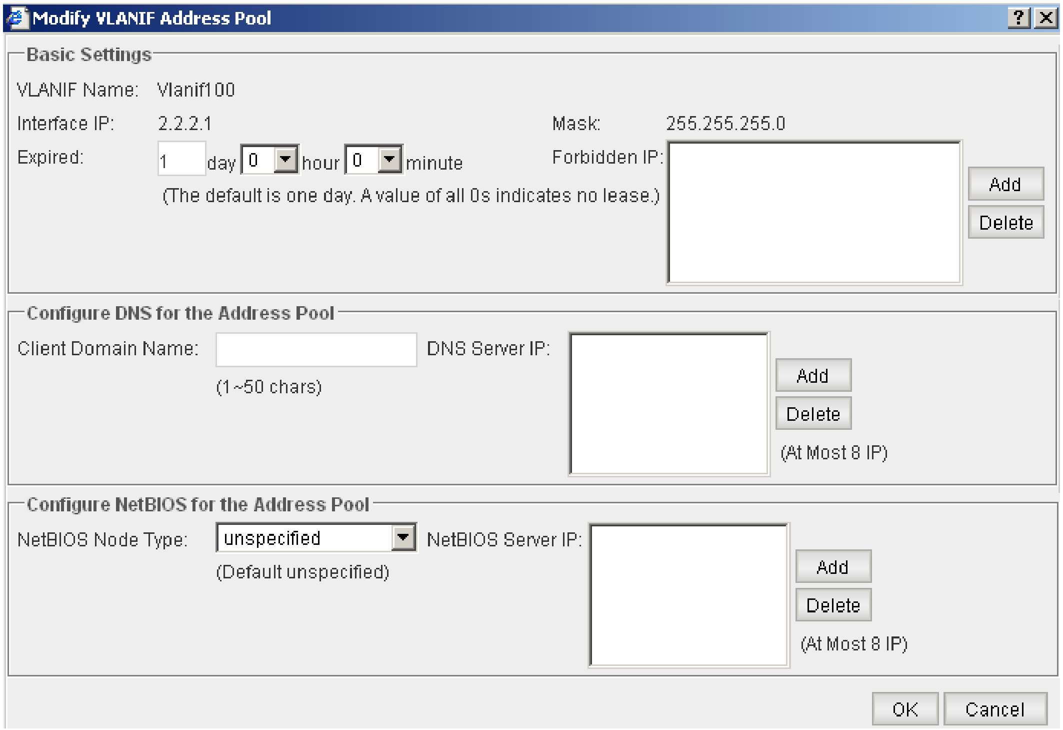
Parameter		Description
	DNS Server IP	Indicates the IP address of a DNS server. You can configure a maximum of eight DNS server addresses. **NOTE** To add a DNS server address, click **Add**. To delete a DNS server address, select it and click **Delete**.
Configure NetBIOS for the Address Pool	NetBIOS Node Type	Indicates the type of a NetBIOS node. The options are: ● unspecified The NetBIOS node type is not specified. ● b-node The NetBIOS node obtains the mapping between the host name and IP address in broadcast mode. b represents broadcast. ● p-node The NetBIOS node obtains the mapping between the host name and IP address by communicating with the NetBIOS server. p represents peer to peer. ● m-node The NetBIOS node is a p-type node with some broadcast features. m represents mixed. ● h-node The NetBIOS node is a b-type node using the peer-to-peer communication mechanism. h represents hybrid. The default value is **unspecified**.
	NetBIOS Server IP	Indicates the IP address of a NetBIOS server. You can configure a maximum of eight NetBIOS server addresses. **NOTE** To add a NetBIOS server address, click **Add**. To delete a NetBIOS server address, select it and click **Delete**.

3. Set the parameters.
4. Click **OK**.

- Modify VLANIF Address Pool

1. Choose **Service Management** > **DHCP** > **Configure VLANIF Interface Address Pool** in the navigation tree to open the **Configure VLANIF Interface Address Pool** page.
2. Click ✎ to open the **Modify VLANIF Address Pool** page , as shown in **Figure 5-30**.

Figure 5-30 Modify VLANIF Address Pool



Modify VLANIF Address Pool

Basic Settings

VLANIF Name: Vlanif100

Interface IP: 2.2.2.1

Mask: 255.255.255.0

Expired: 1 day 0 hour 0 minute

(The default is one day. A value of all 0s indicates no lease.)

Forbidden IP:

Configure DNS for the Address Pool

Client Domain Name:

(1~50 chars)

DNS Server IP:

(At Most 8 IP)

Configure NetBIOS for the Address Pool

NetBIOS Node Type: unspecified

(Default unspecified)

NetBIOS Server IP:

(At Most 8 IP)

NOTE

- **Table 5-19** describes the parameters on the **Modify VLANIF Address Pool** page.
- The name, IP address, subnet mask of the selected VLANIF interface cannot be modified.

3. Set the parameters.
4. Click **OK**.

- Delete a VLANIF Address Pool
  1. Choose **Service Management** > **DHCP** > **Configure VLANIF Interface Address Pool** in the navigation tree to open the **Configure VLANIF Interface Address Pool** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click check boxes of the records.
  3. Click **OK**.

----End

5.5.4 Configure DHCP Delay

By using a DHCP relay agent, the DHCP clients on a local area network (LAN) can communicate with the DHCP servers on other network segments, and obtain IP addresses from them. The DHCP clientson different network segments can also use one DHCP server. This reduces costs and achieves centralized device management.

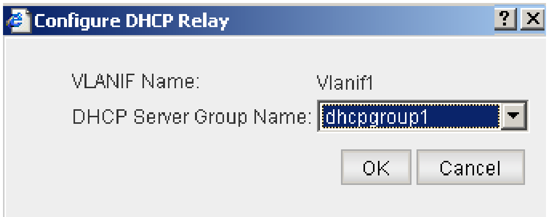
Context

- Before configuring the DHCP relay function, you must configure DHCP servers.
- DHCP relay is introduced to transmit packets between DHCP clients and a DHCP server that are on different network segments. A DHCP relay agent can transparently transmit DHCP broadcast packets between DHCP clients and a DHCP server that are on different network segments.
- In applications, the DHCP relay function is generally implemented on a VLANIF interface of a switch. This interface needs to be configured with an IP relay address to specify the DHCP server. An IP relay address refers to the IP address of the DHCP server specified on the DHCP relay agent. After the DHCP relay function is enabled on an interface, the DHCP broadcast packets received on the interface are sent to the specified server.
- If no DHCP server is configured on a network, the DHCP relay function can be enabled on a switch. In this manner, the DHCP Request packet from clients can be transmitted to the DHCP server on another network through the DHCP relay agent. To enable clients to obtain IP addresses, the DHCP server must use a global address pool. That is, the interface of the server connected to the DHCP relay agent cannot be configured with any address pool.

Procedure

- Query DHCP relay information.
  1. Choose **Service Management** > **DHCP** > **Configure DHCP Delay** in the navigation tree to open the **Configure DHCP Delay** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Configure DHCP relay.
  1. Choose **Service Management** > **DHCP** > **Configure DHCP Delay** in the navigation tree to open the **Configure DHCP Delay** page.
  2. Select a record and click **Configure** to open the **Configure DHCP Relay** page, as shown in **Figure 5-31**.

Figure 5-31 Configure DHCP Relay



Configure DHCP Relay

VLANIF Name: Vlanif1

DHCP Server Group Name: dhcpgroup1

Table 5-20 describes the parameters on the **Configure DHCP Relay** page.

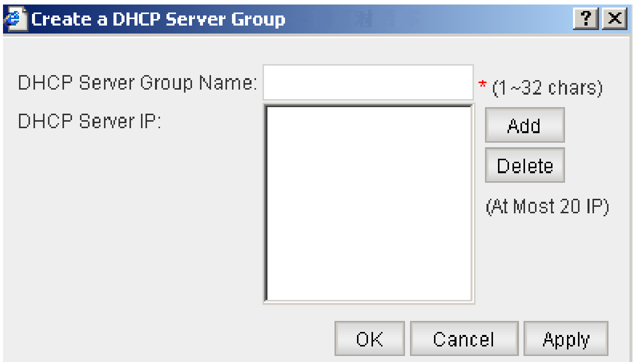
Table 5-20 Configure DHCP Relay

Parameter	Description
VLANIF Name	Indicates the name of a VLANIF interface. The VLANIF interface name cannot be modified. You can select multiple interfaces each time.
DHCP Server Group Name	Indicates the name of a DHCP server group. Select a configured DHCP server from the drop-down list box. If a DHCP server based on an interface address pool is configured, all the users going online through this interface obtain IP addresses from the interface address pool.

3. Set parameters.
4. Click **OK**.

- Delete the DHCP delay configuration.
  1. Choose **Service Management** > **DHCP** > **Configure DHCP Delay** in the navigation tree to open the **Configure DHCP Delay** page.
  2. Select a record and click **Clear Configuration**. The system asks you whether to delete the record.
  3. Click **OK**.
- Create a DHCP server group.
  1. Choose **Service Management** > **DHCP** > **Configure DHCP Delay** in the navigation tree to open the **Configure DHCP Delay** page.
  2. Click **New** to open the **Create a DHCP Server Group** page, as shown in **Figure 5-32**.

Figure 5-32 Create a DHCP Server Group


Create a DHCP Server Group

DHCP Server Group Name: * (1~32 chars)

DHCP Server IP:

Table 5-21 describes the parameters on the **Create a DHCP Server Group** page.

Table 5-21 Create a DHCP Server Group

Parameter	Description
DHCP Server Group Name	Indicates the name of a DHCP server group.
DHCP Server IP	Indicates the IP address of a DHCP server. You can configure a maximum of 20 DHCP servers in a DHCP server group. **NOTE** To add a DHCP server address, click **Add**. To delete a DHCP server address, select it and click **Delete**.

3. Set parameters.
4. Click **OK**.

- Delete a DHCP server group.
  1. Choose **Service Management** > **DHCP** > **Configure DHCP Delay** in the navigation tree to open the **Configure DHCP Delay** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.6 ARP

The following sections describe configurations of static ARP and dynamic ARP. **The S2700SI, S2700EI or S2752EI switches do not support the ARP function.**

On a LAN, a host or a network device must know the logical address (IP address) of another host or network device to send data to it. Only the logical address, however, is not enough. Since IP packets are encapsulated in frames for transmission across a physical network, the physical address of the destination device must also be known. Therefore, the mapping from a logical address to a physical address is required. The Address Resolution Protocol (ARP) is introduced to map IP addresses to physical addresses (Ethernet MAC addresses).

5.6.1 ARP Table

You can query ARP entries in the ARP table.

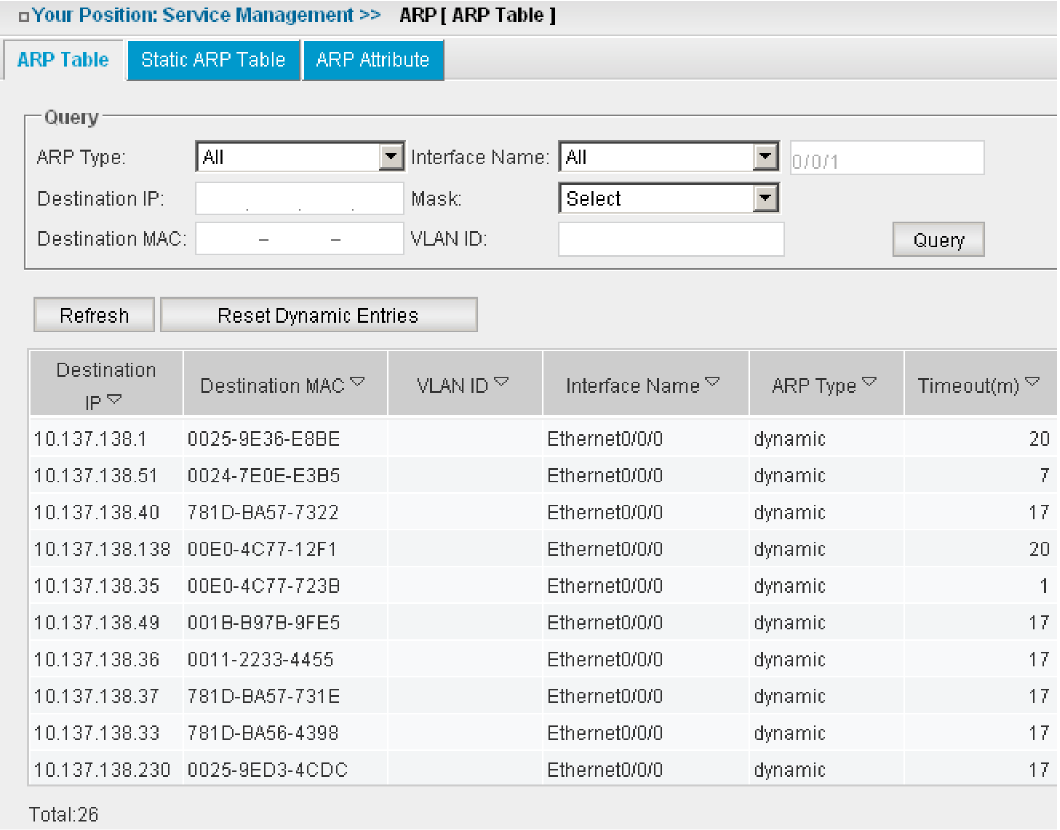
Context

- If two devices on an Ethernet network need to communicate with each other, they must know MAC addresses of each other. Each device maintains a table of mappings from IP addresses to MAC addresses, that is, an ARP table.
- The ARP table of a switch contains static and dynamic ARP entries. Static ARP entries are maintained manually, and dynamic ARP entries age based on the aging timer.

Procedure

- Query the ARP table.
  1. Choose **Service Management** > **ARP** > **ARP Table** in the navigation tree to open the **ARP Table** page, as shown in **Figure 5-33**.

Figure 5-33 ARP Table



ARP Type: All
Interface Name: All
0/0/1
Destination IP: . . .
Mask: Select
Destination MAC: – –
VLAN ID:

Destination IP	Destination MAC	VLAN ID	Interface Name	ARP Type	Timeout(m)
10.137.138.1	0025-9E36-E8BE		Ethernet0/0/0	dynamic	20
10.137.138.51	0024-7E0E-E3B5		Ethernet0/0/0	dynamic	7
10.137.138.40	781D-BA57-7322		Ethernet0/0/0	dynamic	17
10.137.138.138	00E0-4C77-12F1		Ethernet0/0/0	dynamic	20
10.137.138.35	00E0-4C77-723B		Ethernet0/0/0	dynamic	1
10.137.138.49	001B-B97B-9FE5		Ethernet0/0/0	dynamic	17
10.137.138.36	0011-2233-4455		Ethernet0/0/0	dynamic	17
10.137.138.37	781D-BA57-731E		Ethernet0/0/0	dynamic	17
10.137.138.33	781D-BA56-4398		Ethernet0/0/0	dynamic	17
10.137.138.230	0025-9ED3-4CDC		Ethernet0/0/0	dynamic	17

Total:26

Table 5-22 describes the parameters on the **ARP Table** page.

Table 5-22 ARP Table

Parameter	Description
ARP Type	Indicates the type of ARP entries. You can search for static entries, dynamic entries, or all entries.

Parameter	Description
Destination IP	Indicates the destination IP address in an ARP entry, for example, **10.10.10.1**.
Mask	Indicates the mask of the destination IP address, for example, **24(255.255.0.0)**. You can specify the destination IP address and mask to search for ARP entries of a network segment.
Destination MAC	Indicates the destination MAC address in an ARP entry, for example, **0022-0022-0022**.
VLAN ID	Indicates the VLAN ID in an ARP entry.
Interface Name	Indicates the interface in an ARP entry. First select an interface type from the drop-down list box. The options are **All**, **Ethernet**, **GigabitEthernet**, and **XGigabitEthernet**. Then enter the interface number in the text box, for example, **0/0/1**. To specify an Eth-Trunk, enter the interface name in the text box, for example, **Eth-Trunk12**.

2. Set the search criteria.
3. Click **Query**. The search results are displayed.

- Delete all dynamic entries.

  You can click **Reset Dynamic Entries** to delete all dynamic ARP entries.

  1. Choose **Service Management** > **ARP** > **ARP Table** in the navigation tree to open the **ARP Table** page.
  2. Click **Reset Dynamic Entries**. The system asks you whether to delete all dynamic entries.
  3. Click **OK**.

     NOTE

     You can click **Refresh** to display new ARP entries after deleting the original dynamic entries.

----End

5.6.2 Static ARP Table

You can query and configure static ARP entries.

Context

ARP entries can be maintained dynamically or manually. Manually configured mappings from IP addresses to MAC addresses are static ARP entries. You can query, add, modify, and delete ARP entries manually.

CAUTION

Static ARP entries are always valid when a switch works normally. When a VLAN is deleted, the ARP entries of the VLAN are also deleted.

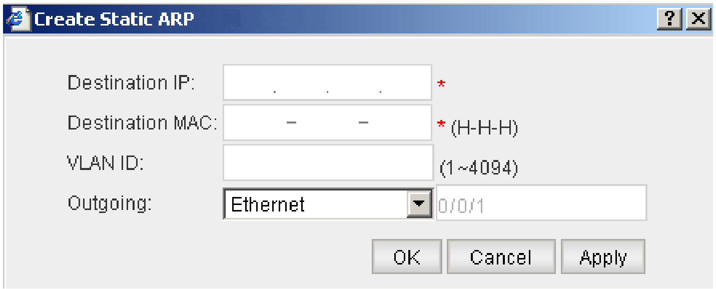
Procedure

- Query static ARP entries.
  1. Choose **Service Management** > **ARP** > **Static ARP Table** in the navigation tree to open the **Static ARP Table** page.

     NOTE

     - Table 5-22 describes the parameters on the **Static ARP Table** page.
     - The **Static ARP Table** page does not contain the **ARP Type** drop-down list box.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Create a static ARP entry.
  1. Choose **Service Management** > **ARP** > **Static ARP Table** in the navigation tree to open the **Static ARP Table** page.
  2. Click **New** to open the **Create Static ARP** page, as shown in Figure 5-34.

Figure 5-34 Create Static ARP



Destination IP: . . . *

Destination MAC: – – * (H-H-H)

VLAN ID: (1~4094)

Outgoing: Ethernet 0/0/1

Table 5-23 describes the parameters on the **Create Static ARP** page.

Table 5-23 Create Static ARP

Parameter	Description
Destination IP	Indicates the destination IP address in the new ARP entry, for example, **10.10.10.1**. NOTE This parameter cannot be set to the virtual IP address of a VRRP group on a VLANIF interface. Otherwise, an incorrect host route will be created, causing forwarding errors.

Parameter	Description
Destination MAC	Indicates the Ethernet MAC address mapping the IP address. The value is in the format **H-H-H**.
VLAN ID	Indicates the VLAN ID corresponding to the IP address. NOTE ● If you enter a VLAN ID, the created ARP entry is in the specified VLAN. ● The VLANIF interface of the VLAN must be in the same network segment as the destination IP address.
Outgoing	Indicates name of the outbound interface of ARP packets, for example, **Ethernet0/0/1**. NOTE The interface must be a member of the specified VLAN.

3. Set parameters.

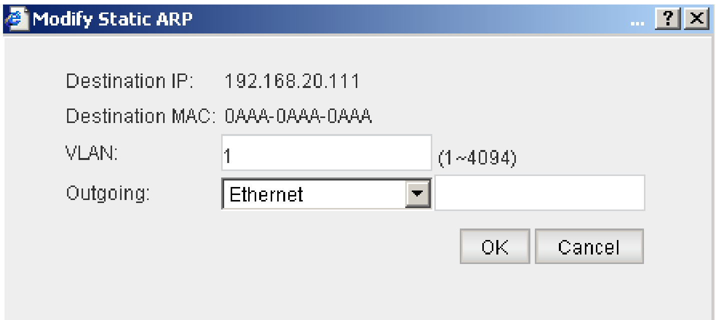
   NOTE

   The destination IP address and the IP address of the outbound interface must be in the same network segment.

4. Click **OK**.

- Modify a static ARP entry.
  1. Choose **Service Management** > **ARP** > **Static ARP Table** in the navigation tree to open the **Static ARP Table** page.
  2. Click 📝 to open the **Modify Static ARP** page, as shown in **Figure 5-35**.

Figure 5-35 Modify Static ARP



Destination IP: 192.168.20.111
Destination MAC: 0AAA-0AAA-0AAA
VLAN: 1 (1~4094)
Outgoing: Ethernet

NOTE

- **Table 5-23** describes the parameters on the **Modify Static ARP** page.
- The destination IP address, destination MAC address, and VLAN ID cannot be changed.

3. Set parameters.

4. Click **OK**.

- Delete Static ARP

1. Choose **Service Management** > **ARP** > **Static ARP Table** in the navigation tree to open the **Static ARP Table** page.
2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

   NOTE

   - To select a record, click the check box of the record.
   - To delete records in batches, click the check boxes of the records.
3. Click **OK**.

----End

5.6.3 ARP Attribute

You can set parameters of dynamic ARP entries, such as the number of aging detection times and aging time.

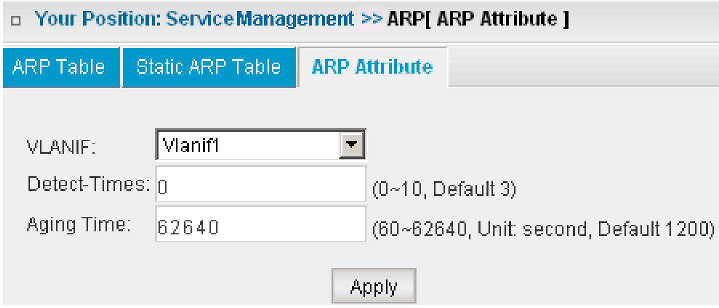
Context

You can set ARP parameters to use ARP entries flexibly.

Procedure

Step 1 Choose **Service Management** > **ARP** > **ARP Attribute** in the navigation tree to open the **ARP Attribute** page, as shown in **Figure 5-36**.

Figure 5-36 ARP Attribute



VLANIF: Vlanif1

Detect-Times: 0 (0~10, Default 3)

Aging Time: 62640 (60~62640, Unit: second, Default 1200)

Table 5-24 describes the parameters on the **ARP Attribute** page.

Table 5-24 ARP Attribute

Parameter	Description
VLANIF	Indicates the name of a VLANIF interface.

Parameter	Description
Detect-Times	Indicates the number of aging detection times. When a dynamic ARP entry expires, the switch sends aging detection packets to the corresponding host. If the host does not respond after the specified number of detection times, the ARP entry is deleted. A proper number of aging detection times can reduce address resolution errors caused by slow update of ARP entries. **NOTE** If this parameter is set to 0, the switch deletes expired ARP entries directly.
Aging Time	Indicates the aging time of ARP entries. The default value is 1200 seconds. A proper aging time can reduce address resolution errors caused by slow update of ARP entries.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.7 VRRP

The following sections describe configurations of VRRP groups and VRRP parameters. **The S2700SI, S2700EI,S2752EI, S5700SI or S3700SI switches do not support the VRRP function.**

The Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol. VRRP integrates multiple routing devices into a virtual router and uses certain mechanisms to switch services to other routers when the next hop router fails, ensuring continuous and reliable communication.

5.7.1 VRRP

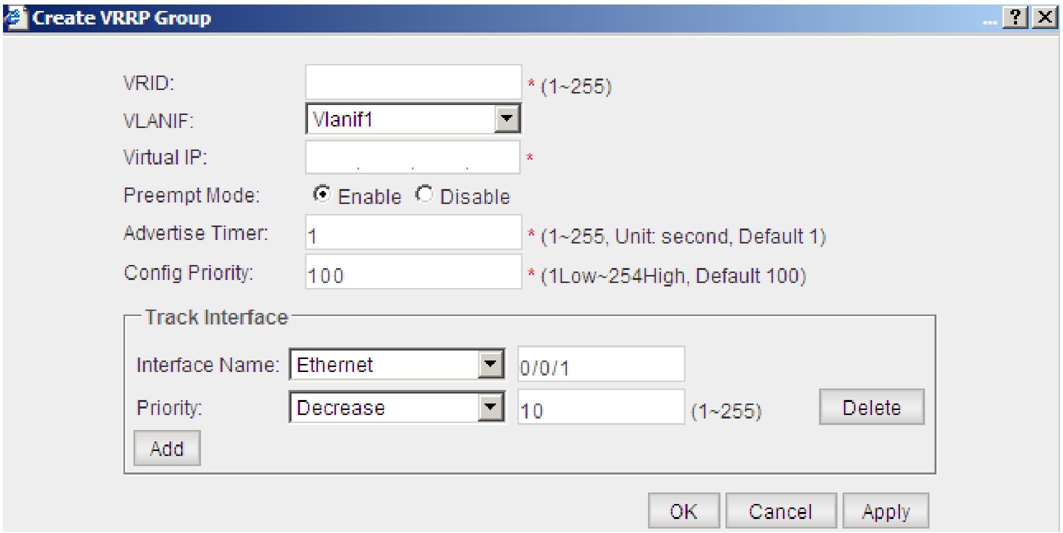
VRRP helps to obtain a more reliable default route without changing the networking or configuring any routing protocol.

Procedure

- Query VRRP group information.
  1. Choose **Service Management** > **VRRP** > **VRRP** in the navigation tree to open the **VRRP** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.

- Create a VRRP group.
  1. Choose **Service Management** > **VRRP** > **VRRP** in the navigation tree to open the **VRRP** page.
  2. Click **New** to open the **Create VRRP Group** page, as shown in **Figure 5-37**.

Figure 5-37 Create VRRP Group



VRID: * (1~255)
VLANIF: Vlanif1
Virtual IP: . . . *
Preempt Mode: ● Enable ○ Disable
Advertise Timer: 1 * (1~255, Unit: second, Default 1)
Config Priority: 100 * (1Low~254High, Default 100)
Interface Name: Ethernet 0/0/1
Priority: Decrease 10 (1~255)

Table 5-25 describes the parameters on the **Create VRRP Group** page.

Table 5-25 Create VRRP Group

Parameter	Description
VRID	Indicates the ID of a virtual router. This parameter is mandatory.
VLANIF	Select a VLANIF interface that requires VRRP configuration. The VLANIF interface must exist in the system.
Virtual IP	Indicates the virtual IP address of the VRRP group, for example, **192.168.70.111**. This parameter is mandatory. **NOTE** The virtual IP address can be an idle IP address in the network segment of the VRRP group or the IP address of an interface in the VRRP group.
Preempt Mode	Indicates whether to adopt the preemption mode. If **Enable** is selected, you need to set the **preempt Delay** parameter. If **Disable** is selected, the **preempt Delay** parameter is invalid.

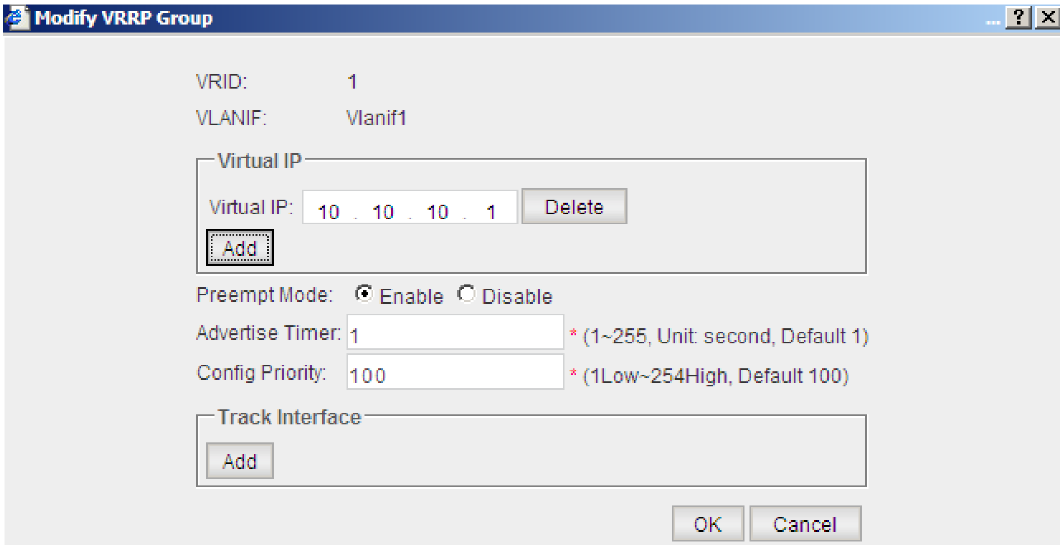
Parameter		Description
Advertise Timer		Indicates the interval for sending VRRP Advertisement packets. This parameter is mandatory. The master device sends VRRP Advertisement packets to backup devices at intervals to notify the backup devices that it works normally. If the backup devices do not receive any VRRP Advertisement packet within an interval, the backup device with the highest priority becomes the master.
Config Priority		Indicates the priority of a member switch. The role of each switch in a VRRP group is determined by its priority. The switch with the highest priority becomes the master.
Track Interface	Interface Name	Indicates the name and type of the tracked interface, for example, **Ethernet0/0/1**.
	Priority	Indicates whether to increase or decrease the VRRP priority of the tracked interface when the tracked interface is Down. NOTE If the preemption mode is disabled, this parameter cannot be set to **Increase**.

3. Set parameters.
4. Click **OK**.

- Modify the configuration of a VRRP group.
  1. Choose **Service Management** > **VRRP** > **VRRP** in the navigation tree to open the **VRRP** page.
  2. Click 📝 to open the **Modify VRRP Group** page, as shown in **Figure 5-38**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-38 Modify VRRP Group



VRID: 1

VLANIF: Vlanif1

Virtual IP: 10 . 10 . 10 . 1

Preempt Mode: ● Enable ○ Disable

Advertise Timer: 1 * (1~255, Unit: second, Default 1)

Config Priority: 100 * (1Low~254High, Default 100)

NOTE

- Table 5-25 describes the parameters on the **Modify VRRP Group** page.
- The VRID and VLANIF interface name cannot be changed.

3. Set parameters.
4. Click **OK**.

- Delete a VRRP group.
  1. Choose **Service Management** > **VRRP** > **VRRP** in the navigation tree to open the **VRRP** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

5.7.2 VRRP Attribute

Before modifying VRRP parameters, you must configure VRRP. If you do not modify VRRP parameters, the system uses the default parameter settings of VRRP.

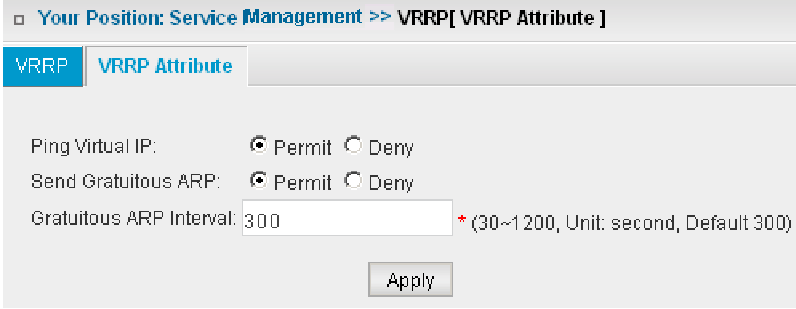
Context

If you do not modify VRRP parameters, the system uses the default parameter settings of VRRP.

Procedure

Step 1 Choose **Service Management** > **VRRP** > **VRRP Attribute** in the navigation tree to open the **VRRP Attribute** page, as shown in Figure 5-39.

Figure 5-39 VRRP Attribute



Your Position: Service Management >> VRRP[VRRP Attribute]

Ping Virtual IP: ● Permit ○ Deny

Send Gratuitous ARP: ● Permit ○ Deny

Gratuitous ARP Interval: 300 * (30~1200, Unit: second, Default 300)

Table 5-26 describes the parameters on the **VRRP Attribute** page.

Table 5-26 VRRP Attribute

Parameter	Description
Ping Virtual IP	Indicates whether the ping command can ping the virtual IP address of the VRRP group. The default value is **Permit**.
Send Gratuitous ARP	Indicates whether to allow the virtual router to send gratuitous ARP packets. To enable the network elements connected to the virtual router to learn the virtual IP address of the VRRP group, the virtual router needs to send gratuitous ARP packets to the network elements. The default value is **Permit**.
Gratuitous ARP Interval	Indicates the interval for sending gratuitous ARP packets.

Step 2 Set parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.8 IGMP Snooping

The following sections describe configurations of IGMP snooping on a switch.

After IGMP snooping is configured on a switch, the switch sets up a Layer 2 multicast forwarding table by listening to the IGMP messages sent between a router and hosts. The switch uses the Layer 2 multicast forwarding table to manage and control forwarding of multicast packets, implementing Layer 2 multicast.

5.8.1 Global IGMP Snooping

You can enable or disable global IGMP snooping.

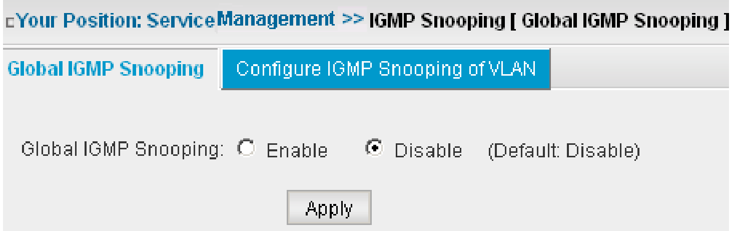
Context

By default, IGMP snooping is disabled on a switch. You need to enable global IGMP snooping on the switch before using this function.

Procedure

Step 1 Choose **Service Management** > **IGMP Snooping** > **Global IGMP Snooping** in the navigation tree to open the **Global IGMP Snooping** page, as shown in **Figure 5-40**.

Figure 5-40 Global IGMP Snooping



Your Position: Service Management >> IGMP Snooping [Global IGMP Snooping]
Global IGMP Snooping
Configure IGMP Snooping of VLAN
Apply

Global IGMP Snooping: ○ Enable ● Disable (Default: Disable)

Table 5-27 describes the parameters on the **Global IGMP Snooping** page.

Table 5-27 Global IGMP Snooping

Parameter	Description
Global IGMP Snooping	Indicates whether to enable global IGMP snooping. If global IGMP snooping is disabled, IGMP snooping cannot be enabled in a VLAN. The options are **Enable** and **Disable**. By default, global IGMP snooping is disabled.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

5.8.2 Configure IGMP Snooping in VLAN

You can query and configure IGMP snooping information in VLANs.

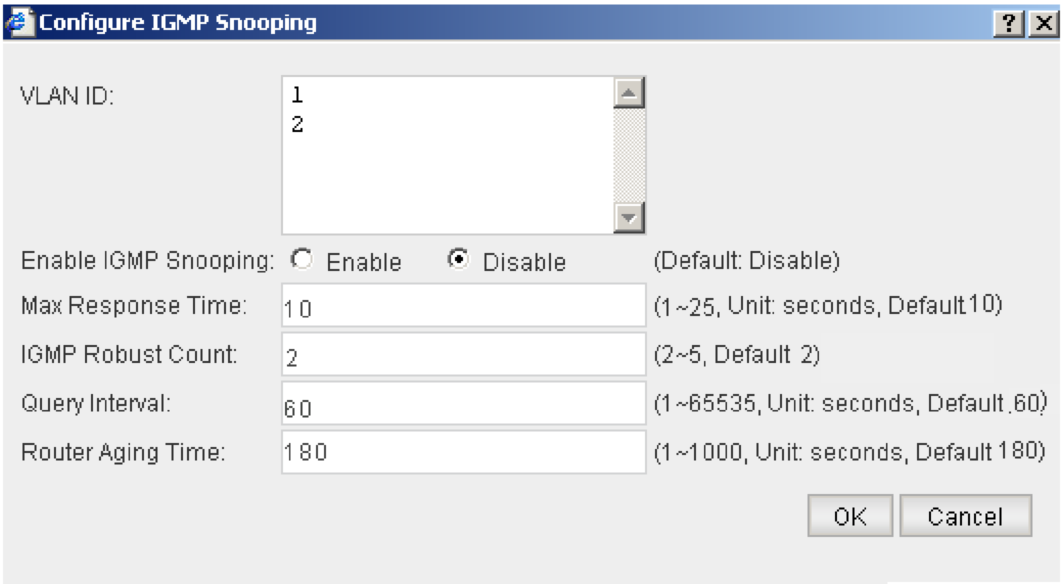
Context

By default, IGMP snooping is disabled on a switch. You need to enable global IGMP snooping on the switch before using this function. By default, IGMP snooping is disabled in a VLAN after global IGMP snooping is enabled. Therefore, you need to enable IGMP snooping in the VLAN.

Procedure

- Query IGMP snooping information.
  1. Choose **Service Management** > **IGMP Snooping** > **Configure IGMP Snooping of VLAN** in the navigation tree to open the **Configure IGMP Snooping of VLAN** page.
  2. Set the search criteria.
  3. Click **Query** to display all the matching records.
- Configure IGMP snooping in a VLAN.
  1. Choose **Service Management** > **IGMP Snooping** > **Configure IGMP Snooping of VLAN** in the navigation tree to open the **Configure IGMP Snooping of VLAN** page.
  2. Select a record and click **Configure** to open the **Configure IGMP Snooping** page, as shown in **Figure 5-41**.

Figure 5-41 Configure IGMP Snooping



Configure IGMP Snooping

VLAN ID: 1, 2

Enable IGMP Snooping: ○ Enable ● Disable (Default: Disable)

Max Response Time: 10 (1~25, Unit: seconds, Default10)

IGMP Robust Count: 2 (2~5, Default 2)

Query Interval: 60 (1~65535, Unit: seconds, Default 60)

Router Aging Time: 180 (1~1000, Unit: seconds, Default 180)

Table 5-28 describes the parameters on the **Configure IGMP Snooping** page.

Table 5-28 Configure IGMP Snooping

Parameter	Description
VLAN ID	Indicates the ID of a VLAN. The VLAN ID cannot be changed. You can select multiple VLANs each time. **NOTE** The VLAN must exist. If only one VLAN is selected, the IGMP configuration in the VLAN is displayed on the **Configure IGMP Snooping** page. If multiple VLANs are selected, the default IGMP snooping configuration is displayed.

Parameter	Description
Enable IGMP Snooping	Indicates whether to enable IGMP snooping. The options are **Enable** and **Disable**. NOTE ● Before enabling IGMP snooping in a VLAN, enable global IGMP snooping. ● After IGMP snooping is enabled in a VLAN, this function takes effect only on Ethernet interfaces in this VLAN.
Max Response Time	Indicates the maximum response time of IGMP Query messages. ● The maximum response time controls the deadline for a host to send an IGMP Membership Report message. A proper maximum response time enables hosts to rapidly respond to IGMP Query messages and prevent the congestion caused by a large number of Response messages sent at the same time. ● You can adjust the aging time of member interfaces by setting the maximum response time.
IGMP Robust Count	Indicates the IGMP robustness variable. By setting the IGMP robustness variable, you can: ● Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network. ● Adjust the aging time of member interfaces.
Query Interval	Indicates the interval for sending IGMP Query messages.
Router Aging Time	Indicates the aging time of a router interface.

3. Set the parameters.
4. Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

6 ACL

About This Chapter

The following sections describe how to view, add, modify, delete ACLs and ACL effective period, and configure the ACL function. The S2700SI switches do not support the ACL function.

The access control list (ACL) is used to identify flows. A network device filters packets according to certain rules. It must identify packets first, and then permits or denies the packets according to the policy that you have configured.

6.1 Effective Period
By configuring the effective period, you can apply an ACL to packets in a certain period of time.

6.2 ACL
An ACL classifies packets according to matching rules. The rules can be source addresses, destination addresses, or the port numbers of the packets. The S2700SI series switches do not support the ACL.

6.1 Effective Period

By configuring the effective period, you can apply an ACL to packets in a certain period of time.

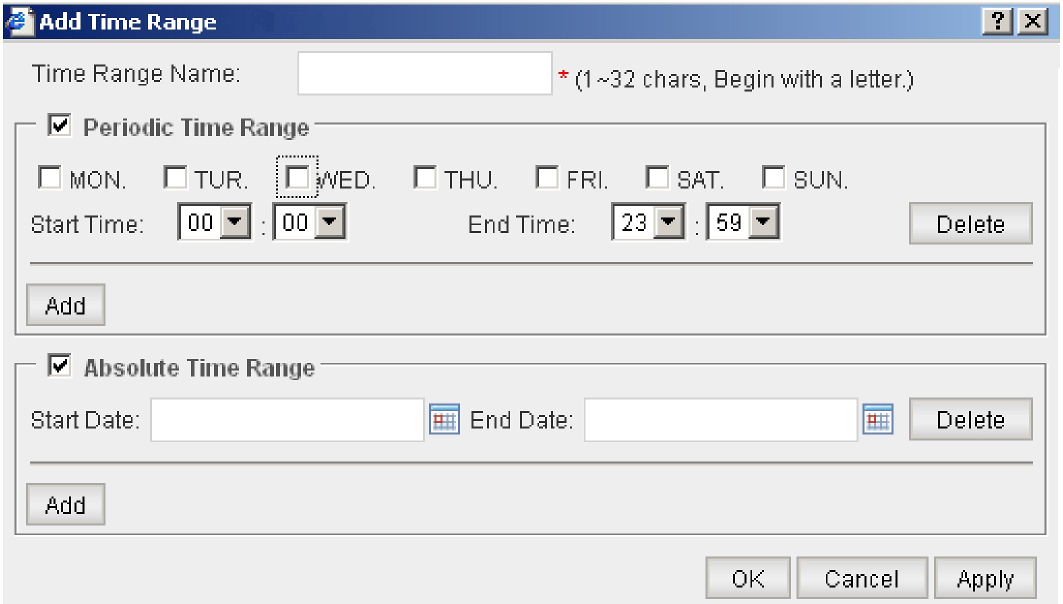
Context

- An effective period describes a special period of time. In practice, users may want certain ACL rules to be valid during a certain period but be invalid out of the period. That is, the ACL rules are used to filter packets based on the period of time. To implement this function, users can set one or multiple periods, and apply the periods to a rule. Then, packets are filtered based on the set periods.
- An effective period can contain periodic time ranges and absolute time ranges. A periodic time range takes effect on a certain day in a week. An absolute time range contains the start time and the end time.

Procedure

- Query the time range.
  1. Choose **ACL** > **Effective Period** to open the **Effective Period** page.
  2. Enter the name of the time range in the text box, for example, **test**.
  3. Click **Query** to display all matching records.
- Add a time range.
  1. Choose **ACL** > **Effective Period** to open the **Effective Period** page.
  2. Click **New** to open the **Add Time Range** page, as shown in **Figure 6-1**.

Figure 6-1 Add Time Range



Add Time Range

Time Range Name: * (1~32 chars, Begin with a letter.)

☑ Periodic Time Range

□ MON. □ TUR. □ WED. □ THU. □ FRI. □ SAT. □ SUN.

Start Time: 00 : 00 End Time: 23 : 59

☑ Absolute Time Range

Start Date: End Date:

Table 6-1 describes the parameters on the **Add Time Range** page.

Table 6-1 Add Time Range

Parameter	Description
Time Range Name	Indicates the name of the created effective period.
Periodic Time Range	Indicates the periodic time range. A periodic time range takes effect on a certain day in a week. You can create multiple periodic time ranges by clicking **New** or delete all the periodic time ranges by clicking **Delete**. NOTE If only one periodic time range is created in an effective period, the effective period takes effect when the current time is within the periodic time range.
Absolute Time Range	Indicates the absolute time range. An absolute time range contains the start time and the end time. You can create multiple absolute time ranges by clicking **New** or delete all the absolute time ranges by clicking **Delete**. NOTE If only one absolute time range is created in an effective period, the effective period takes effect when the current time is within the absolute time range.

3. Set parameters.

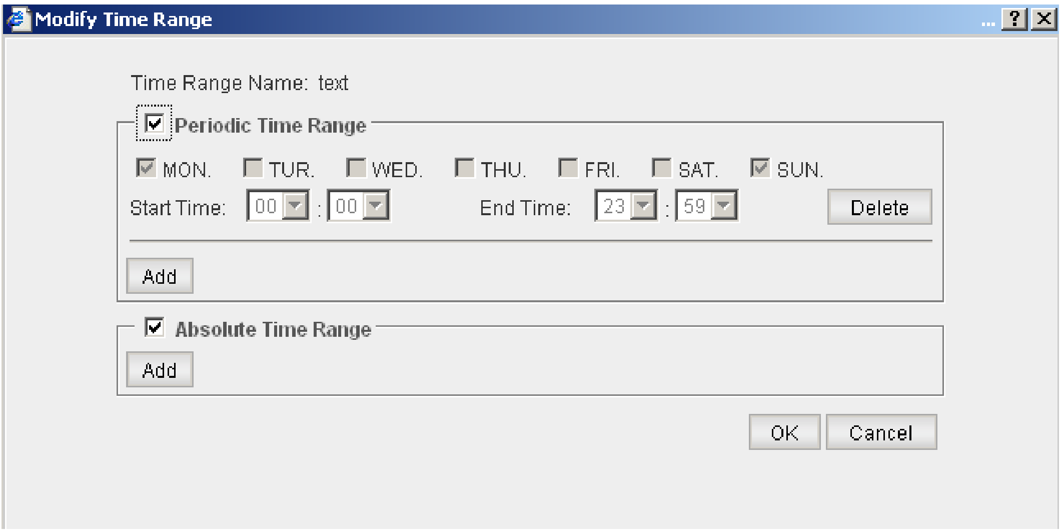
   NOTE

   - If an effective period contains an absolute time range and a periodic time range, the effective period takes effect only when the current time is within the absolute time range and the periodic time range.
   - The start time and end time of the absolute time range can be earlier than the current time.
   - The **Periodic Time Range** and **Absolute Time Range** parameters cannot be kept blank simultaneously.

4. Click **OK**.

- Modify a time range.
  1. Choose **ACL** > **Effective Period** to open the **Effective Period** page.
  2. Click 📝 to open the **Modify Time** page, as shown in **Figure 6-2**.

Figure 6-2 Modify Time Range



Modify Time Range

Time Range Name: text

☑ Periodic Time Range

☑ MON. □ TUR. □ WED. □ THU. □ FRI. □ SAT. ☑ SUN.

Start Time: 00 : 00 End Time: 23 : 59

☑ Absolute Time Range

NOTE

- **Table 6-1** describes the parameters on the **Modify Time** page.
- The effective period name cannot be modified.
- The periodic time range and absolute time range can only be deleted, but cannot be modified.

3. Set parameters.
4. Click **OK**.

- Delete a time range.
  1. Choose **ACL** > **Effective Period** to open the **Effective Period** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

6.2 ACL

An ACL classifies packets according to matching rules. The rules can be source addresses, destination addresses, or the port numbers of the packets. The S2700SI series switches do not support the ACL.

Context

ACLs are classified into the following types:

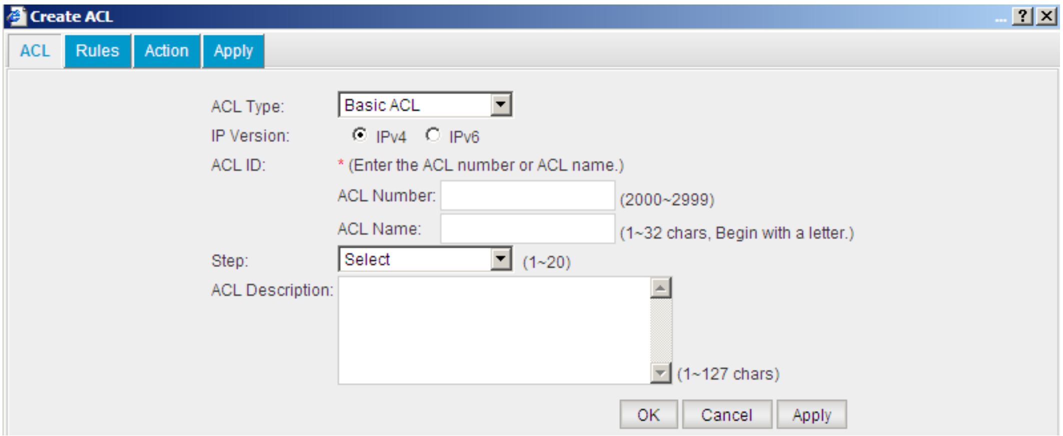
- Basic ACL: matching packets based on source IP addresses at Layer 3

- Advanced ACL: matching packets based on the Layer 3 or Layer 4 information of packets, such as source IP addresses, destination IP addresses, type of the protocol over IP, and the protocol feature
- Layer 2 ACL: matching packets based on Layer 2 information of packets, such as source MAC addresses, destination MAC addresses, VLAN priorities, and the Layer 2 protocol type

Procedure

- Query an ACL.
  1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Create an ACL.
  1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
  2. Click **New** to open the **Create ACL** page.
  3. Click the **ACL** tab, as shown in **Figure 6-3**.

Figure 6-3 Create ACL



ACL Type: Basic ACL
IP Version: ● IPv4 ○ IPv6
ACL ID: * (Enter the ACL number or ACL name.)
ACL Number: (2000~2999)
ACL Name: (1~32 chars, Begin with a letter.)
Step: Select (1~20)
ACL Description: (1~127 chars)

Table 6-2 describes the parameters on the page.

Table 6-2 Create ACL

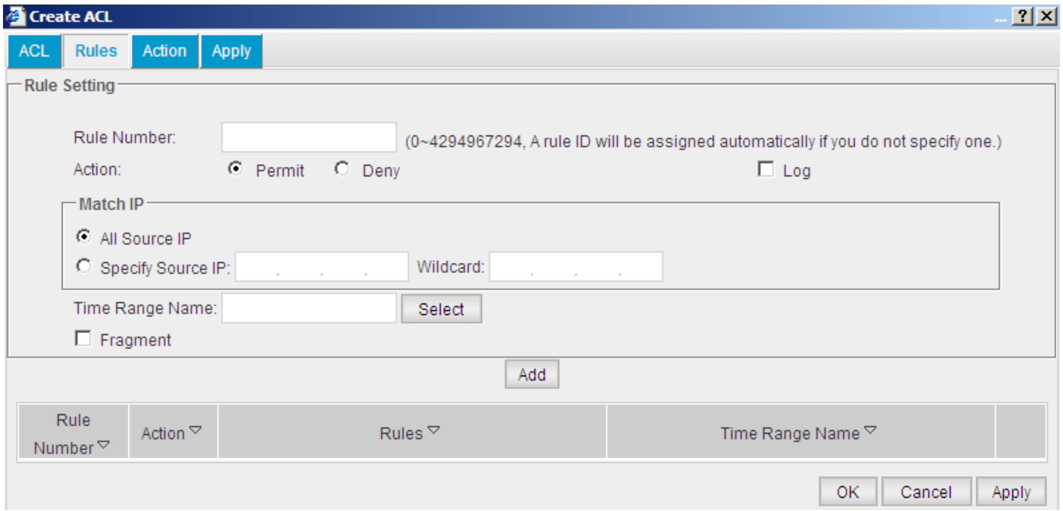
Parameter	Description
ACL Type	Indicates the ACL type, including: ● Basic ACL ● Advanced ACL ● Layer 2 ACL

Parameter		Description
IP Version		To create an IPv4 or IPv6 ACL, click the **IPv4** or **IPv6** check box. NOTE If you select Layer 2 ACL, the IP version cannot be set.
ACL ID	ACL Number	Indicates the number of an ACL. It identifies an ACL. The value of the ACL number is an integer, including: ● 2000-2999: basic ACL ● 3000-3999: advanced ACL ● 4000-4999: Layer 2 ACL NOTE ● When you modify an ACL, the ACL number cannot be changed. ● An ACL number or ACL name is required to identify an ACL.
	ACL Name	Indicates the name of an ACL. The ACL name must be unique. NOTE ● The ACL name is a string starting with a letter. Spaces or quotation marks are not allowed. The keyword **all** is not allowed. ● An ACL number or ACL name is required to identify an ACL. ● When you modify an ACL, the ACL name cannot be changed.
Step		Indicates the interval between two rule IDs. NOTE The **Step** text box is unavailable after you set **IP Version** to **IPv6**.
ACL Description		Indicates the description of an ACL. This parameter is optional. NOTE The **Description** text box of the ACL is unavailable after you set **IP Version** to **IPv6**.

4. Click the **Rules** tab.

   If the ACL is a basic ACL, the rule page is displayed, as shown in **Figure 6-4**.

Figure 6-4 Create Basic ACL Rule



Rule Number: (0~4294967294, A rule ID will be assigned automatically if you do not specify one.)

Action: ● Permit ○ Deny □ Log

Match IP

● All Source IP

○ Specify Source IP: . . . Wildcard: . . .

Time Range Name: Select

□ Fragment

[Table 6-3](#) describes the parameters on the page.

Table 6-3 Create Basic ACL Rule

Parameter		Description
Rule Number		Indicates the number of a rule. **NOTE** If you do not specify a rule number, the system automatically allocates a number for the rule. The rule number cannot be changed.
Action		Indicates whether to permit or deny packets. The default action is to permit.
Log		Indicates whether to record logs when packets are permitted. To record logs when packets are permitted, click the check box. **NOTE** The basic ACL and basic IPv6 ACL in the S2700EI switches do not support this parameter.
Match IP	All Source IP	Indicates that packets from any IP address are permitted.
	Specify Source IP	Enter the specified IP address and the reverse mask. By default, all source IP addresses are specified. **NOTE** ● To create an IPv4 ACL, enter the reverse mark. ● To create an IPv6 ACL, enter the prefix length.

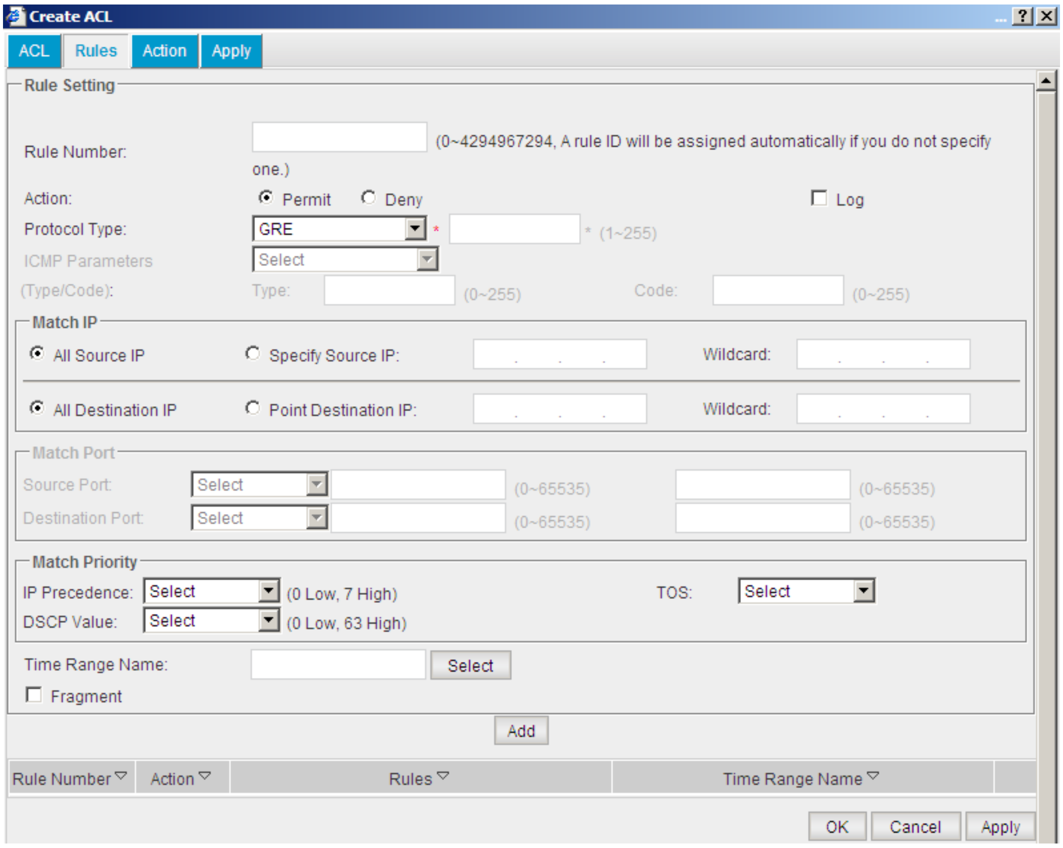
Parameter	Description
Time Range Name	Click **Select** to set the time range name. NOTE The time range name is displayed on the configuration result page.
Fragment	Indicates that the rule is valid for only non-initial fragments. NOTE The basic ACL and basic IPv6 ACL in the S2700EI switches do not support this parameter.

NOTE

- The rule page displays all the rules of the ACL. Click a record to view the details about the record or modify the record. To deselect a record, click it again. You can add rules on the rule page.
- When you modify the ACL rule, the ACL number and rule number cannot be modified.

If the ACL is an advanced ACL, the rule page is displayed, as shown in **Figure 6-5**.

Figure 6-5 Create an Advanced ACL Rule



Rule Number: (0~4294967294, A rule ID will be assigned automatically if you do not specify one.)

Action: ● Permit ○ Deny □ Log

Protocol Type: GRE * (1~255)

ICMP Parameters (Type/Code): Select Type: (0~255) Code: (0~255)

● All Source IP ○ Specify Source IP: . . . Wildcard: . . .

● All Destination IP ○ Point Destination IP: . . . Wildcard: . . .

Source Port: Select (0~65535) (0~65535)

Destination Port: Select (0~65535) (0~65535)

IP Precedence: Select (0 Low, 7 High) TOS: Select

DSCP Value: Select (0 Low, 63 High)

Time Range Name: Select

□ Fragment

Table 6-4 describes the parameters on the page.

Table 6-4 Create Advanced Rule

Parameter	Description
Rule Number	Indicates the number of a rule. **NOTE** If you do not specify a rule number, the system automatically allocates a number for the rule. The rule number cannot be changed.
Action	Indicates whether to permit or deny packets. The default action is to permit.
Log	Indicates whether to record logs when packets are permitted. **NOTE** The advanced ACL and advanced IPv6 ACL of the S2700EI switches do not support this parameter.
Protocol Type	Indicates the type of the protocol. The advanced ACL supports the following protocols: ● IGMP ● GRE ● IP ● IPINIP ● OSPF ● TCP ● UDP ● ICMP ● Customized **NOTE** The text box is valid only when the protocol type can be defined by users. The advanced IPv6 ACL supports the following protocols: ● GRE ● ICMPv6 ● IPv6 ● OSPF ● TCP ● UDP ● Customized **NOTE** The text box is valid only when the protocol type can be defined by users.

Parameter		Description
ICMP Parameters (Type/Code)		Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. The IGMP packets can be matched based on: ● Type: filters packets based on ICMP message type. ● Code: indicates the message code of the ICMP message type. **NOTE** The advanced ACL and advanced IPv6 ACL of the S2700EI switches do not support this parameter.
Match IP	All Source IP	Indicates that packets from any IP address are permitted.
	Specify Source IP	Enter the specified IP address and the reverse mask. By default, all source IP addresses are specified. **NOTE** ● To create an IPv4 ACL, enter the reverse mark. ● To create an IPv6 ACL, enter the prefix length.
	All Destination IP	Indicates that packets from any IP address are permitted.
	Point Destination IP	Enter the specified IP address and the reverse mask. By default, all destination IP addresses are specified. **NOTE** ● To create an IPv4 ACL, enter the reverse mark. ● To create an IPv6 ACL, enter the prefix length.
Match Port	Source Port	This parameter is valid only when the protocol type is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. Select a matching source port from the drop-down list box. The value can be equal, greater, smaller, or in the range. Enter the TCP or UDP port number in the text box.

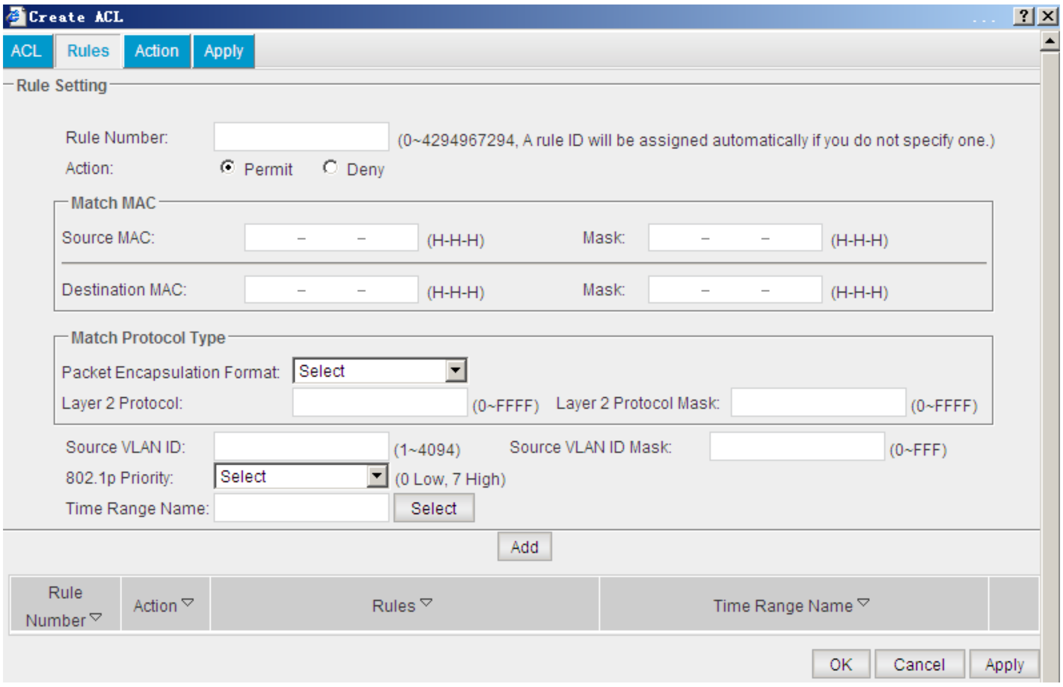
Parameter		Description
	Destination Port	This parameter is valid only when the protocol type is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. Select a matching destination port from the drop-down list box. The value can be equal, greater, smaller, or in the range. Enter the TCP or UDP port number in the text box.
Match Priority	IP Precedence	Indicates that packets are filtered based on the precedence field. By default, this parameter is empty. **NOTE** The advanced IPv6 ACL of the S5700SI switches does not support this parameter.
	DSCP Value	Specifies the Differentiated Services CodePoint (DSCP). **NOTE** ● If you set the IP precedence or TOS, the DSCP priority cannot be set. ● If you set the DSCP priority, the IP precedence or TOS cannot be set. ● The advanced IPv6 ACL of the S5700SI switches does not support this parameter.
	TOS	Indicates that packets are filtered based on the type field. This parameter is optional. **NOTE** The advanced IPv6 ACL of the S5700SI switches does not support this parameter.
Time Range Name		Click **Select** to set the time range name. **NOTE** The time range name is displayed on the configuration result page.
Fragment		Indicates that the rule is valid for only non-initial fragments. **NOTE** The advanced ACL and advanced IPv6 ACL of the S2700EI switches do not support this parameter.

NOTE

- The rule page displays all the rules of the ACL. Click a record to view the details about the record or modify the record. To deselect a record, click it again. You can add rules on the rule page.
- When you modify the ACL rule, the ACL number and rule number cannot be modified.

If the ACL is a basic ACL, the rule page is displayed, as shown in **Figure 6-6**.

Figure 6-6 Create Layer 2 ACL Rule



Rule Setting

Rule Number: (0~4294967294, A rule ID will be assigned automatically if you do not specify one.)

Action: ● Permit ○ Deny

Match MAC

Source MAC: - - (H-H-H) Mask: - - (H-H-H)

Destination MAC: - - (H-H-H) Mask: - - (H-H-H)

Match Protocol Type

Packet Encapsulation Format: Select

Layer 2 Protocol: (0~FFFF) Layer 2 Protocol Mask: (0~FFFF)

Source VLAN ID: (1~4094) Source VLAN ID Mask: (0~FFF)

802.1p Priority: Select (0 Low, 7 High)

Time Range Name: Select

Table 6-5 describes the parameters on the page.

Table 6-5 Create Layer 2 ACL Rule

Parameter		Description
Rule Number		Indicates the number of a rule. **NOTE** If you do not specify a rule number, the system automatically allocates a number for the rule. The rule number cannot be changed.
Action		Indicates whether to permit or deny packets. The default action is to permit.
Match MAC	Source MAC	Indicates the source MAC address used by the ACL rule. The value is in H-H-H format.
	Mask	Indicates the mask of the source MAC address used by the ACL rule. The value is in the format H-H-H. The default value contains only Fs.
	Destination MAC	Indicates the destination MAC address used by the ACL rule. The value is in H-H-H format.

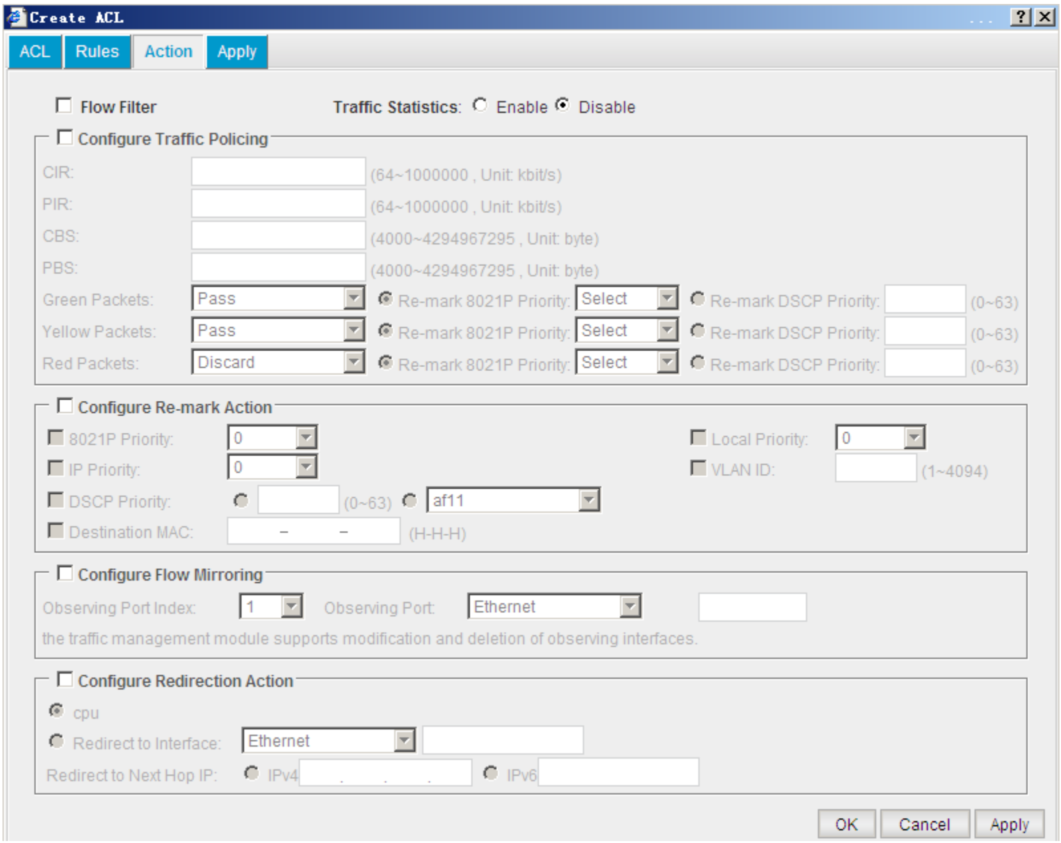
Parameter		Description
	Mask	Indicates the mask of the destination MAC address used by the ACL rule. The value is in the format H-H-H. The default value contains only Fs.
Match Protocol Type	Packet Encapsulation Format	Indicates the encapsulation format of protocol packets. The value can be ether-ii, 802.3, or snap.
	Layer 2 Protocol	Indicates the type of Layer 2 protocols.
	Layer 2 Protocol Mask	Indicates the mask of the Layer 2 protocol.
Source VLAN ID		Indicates the source VLAN ID.
Source VLAN ID Mask		Indicates the mask of the source VLAN ID. The value is in hexadecimal notation. It ranges from 0 to 0xFFF. The default value is 0xFFF.
802.1p Priority		Indicates the 802.1p priority of the ACL. By default, this parameter is empty.
Time Range Name		Click **Select** to set the time range name. **NOTE** The time range name is displayed on the configuration result page.

NOTE

- The rule page displays all the rules of the ACL. Click a record to view the details about the record or modify the record. To deselect a record, click it again. You can add rules on the rule page.
- When you modify the ACL rule, the ACL number and rule number cannot be modified.

5. Click the **Action** tab, as shown in **Figure 6-7**.

Figure 6-7 Create ACL Action



□ Flow Filter Traffic Statistics: ○ Enable ● Disable

□ Configure Traffic Policing

CIR: (64~1000000 , Unit: kbit/s)
PIR: (64~1000000 , Unit: kbit/s)
CBS: (4000~4294967295 , Unit: byte)
PBS: (4000~4294967295 , Unit: byte)
Green Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)
Yellow Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)
Red Packets: Discard ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

□ Configure Re-mark Action

□ 8021P Priority: 0 □ Local Priority: 0
□ IP Priority: 0 □ VLAN ID: (1~4094)
□ DSCP Priority: ● (0~63) ○ af11
□ Destination MAC: - - (H-H-H)

□ Configure Flow Mirroring

Observing Port Index: 1 Observing Port: Ethernet
the traffic management module supports modification and deletion of observing interfaces.

□ Configure Redirection Action

● cpu
○ Redirect to Interface: Ethernet
Redirect to Next Hop IP: ○ IPv4 . . . ○ IPv6

Table 6-6 describes the parameters on the page.

Table 6-6 Create ACL Action

Parameter		Description
Flow Filter		Indicates whether to enable the Flow Filter. This parameter is optional.
Traffic Statistics		Indicates whether to enable the traffic statistics. The value can be **Enable** or **Disable**. By default, the value is **Disable**.
Configure Traffic Policing	CIR	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.

Parameter			Description
	PIR		Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through. **NOTE** ● The value of PIR cannot be smaller than the value of CIR. By default, the value of PIR is equal to the value of CIR. ● The S2700EI and S2700SI switches do not support this parameter.
	CBS		Specifies the committed burst size (CBS), which is the committed burst volume of traffic that can pass through.
	PBS		Specifies the peak burst size (PBS), which is the peak burst volume of traffic that can pass through. The default value of PBS is related to the value of PIR. **NOTE** The S2700SI and S2700EI switches do not support this parameter.
	Green Packets **NOTE** The S2700SI and S2700EI switches do not support this parameter.	Green Packets	Indicates whether green packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**. **NOTE** The S5700SI switches cannot be modified.
		Re-mark 802.1P Priority	Indicates whether to re-mark the 802.1p priority. **NOTE** The S5700SI switches do not support this parameter.
		Re-mark DSCP Priority	Indicates whether to re-mark the DSCP priority. **NOTE** The S5700SI switches do not support this parameter.
	Yellow Packets	Yellow Packets	Indicates whether yellow packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**.
		Re-mark 802.1P Priority	Indicates whether to re-mark the 802.1p priority.

Parameter			Description
	NOTE The S2700SI and S2700EI switches do not support this parameter.	Re-mark DSCP Priority	Indicates whether to re-mark the DSCP priority.
	Red Packets **NOTE** The S2700SI and S2700EI switches do not support this parameter.	Red Packets	Indicates whether red packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **discard**.
		Re-mark 802.1P Priority	Indicates whether to re-mark the 802.1p priority.
		Re-mark DSCP Priority	Indicates whether to re-mark the DSCP priority.
Configure Re-mark Action	802.1P Priority		Select the check box of 802.1p to configure the 802.1p priority.
	Local Priority		Select the check box of the local priority to configure the local priority. **NOTE** You cannot set both the 802.1p priority and the local priority for redirection in a traffic behavior.
	IP Priority		Select the check box of the IP precedence to configure the IP precedence.
	DSCP Priority		Select the check box of DSCP to configure the DSCP priority.

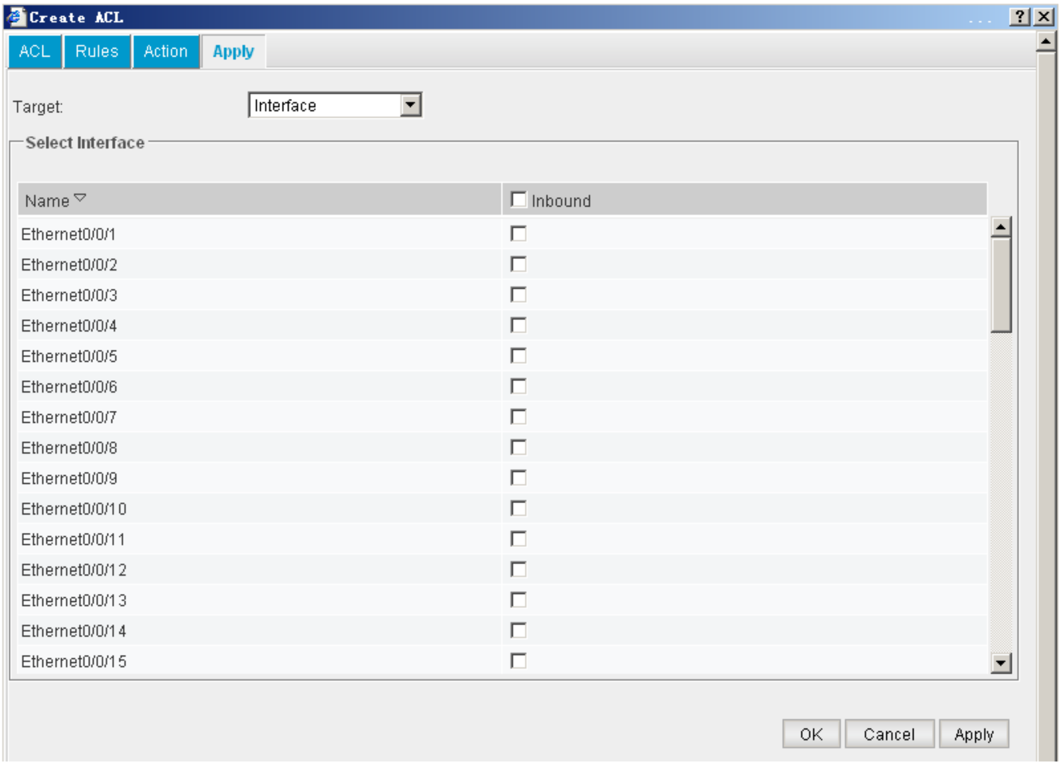
Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Destination MAC	Select the corresponding check box to configure the destination MAC address. The value is in the format H-H-H. Each H represents four hexadecimal digits. **NOTE** The S5700I, S2700SI, and S2700EI switches do not support this parameter.
	VLAN ID	Select the check box of VLAN ID to configure VLAN ID.
	Inner VLAN	Select the check box of the inner VLAN to configure the inner VLAN. **NOTE** The S5700I,S2700EI S2700SI, S2752EI, and S3700 switches do not support this parameter.
Configure Flow Mirroring	Observing Port Index	Indicates the ID of the observing interface where all matching flows are mirrored.
	Observing Port	Indicates the observing interface where all matching flows are mirrored, for example, **Ethernet 0/0/1**.
Configure Redirection Action **NOTE** The S2700SI and S2700EI switches do not support this parameter.	CPU	Indicates that packets are redirected to the CPU.
	Redirect to Interface	Indicates the interface where packets are redirected, for example, **Ethernet 0/0/1**.
	Redirect to Next Hop IP	1. Select an IP address type. The value can be IPv4 and IPv6. 2. Configure the redirected next hop address according to the IP address type. **NOTE** ● You cannot configure both the next hop address where packets are redirected and the re-marked destination MAC address. ● The S5700SI switches do not support this parameter.

6. Click the **Apply** tab.

   – If the object is interface, the **Target** field is displayed as **Interface**, as shown in **Figure 6-8**.

Figure 6-8 Apply an ACL to an interface



Target: Interface

Select Interface

Name	□ Inbound
Ethernet0/0/1	□
Ethernet0/0/2	□
Ethernet0/0/3	□
Ethernet0/0/4	□
Ethernet0/0/5	□
Ethernet0/0/6	□
Ethernet0/0/7	□
Ethernet0/0/8	□
Ethernet0/0/9	□
Ethernet0/0/10	□
Ethernet0/0/11	□
Ethernet0/0/12	□
Ethernet0/0/13	□
Ethernet0/0/14	□
Ethernet0/0/15	□

Table 6-7 describes the parameters on the page.

Table 6-7 Apply an ACL to an interface

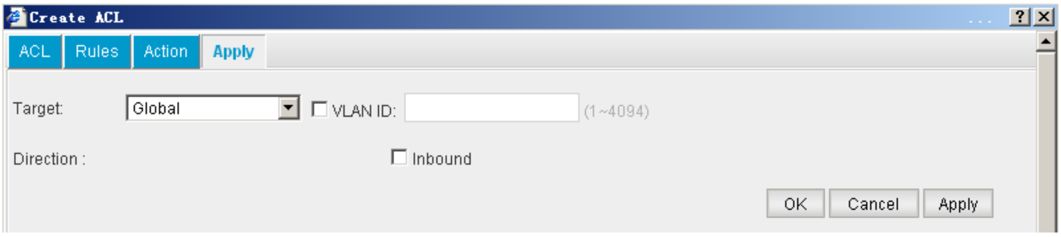
Parameter	Description
Name	Indicates all the interfaces on the device.
Inbound	● You can select all ACLs. You can specify all inbound interfaces by clicking the check boxes of all inbound interfaces. ● You can select an ACL. You can specify an inbound interface by clicking the check box of an inbound interface. ● You can select multiple interfaces. You can specify multiple inbound interfaces by clicking the check boxes of multiple inbound interfaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Outbound NOTE The S2700EI and S3700 series switches do not support this parameter.	● You can select all ACLs. You can select all outbound interfaces by clicking the check box of all outbound interfaces. ● You can select an ACL. You can specify an outbound interface by clicking the check box of an outbound interface. ● You can select multiple interfaces. You can specify multiple outbound interfaces by clicking the check boxes of multiple outbound interfaces. NOTE You can select the inbound and outbound interfaces or one of them at one time.

- If the object is interface, the **Target** field is displayed as **Global**, as shown in **Figure 6-9**.

Figure 6-9 Apply an ACL Globally



Target: Global
□ VLAN ID: (1~4094)
Direction : □ Inbound

Table 6-8 describes the parameters on the page.

Table 6-8 Apply an ACL Globally

Parameter	Description
VLAN ID	● If the check box of VLAN is not selected and the VLAN ID text box is not available, the ACL is not applied to any VLAN. ● If the check box of VLAN is selected, the ACL is applied to VLAN. This parameter is mandatory.
Direction NOTE The S2700EI and S3700 series switches do not support this parameter.	NOTE You can select the inbound and outbound interfaces or one of them at one time.

7. Set parameter on each tab page.

8. Click **OK**.

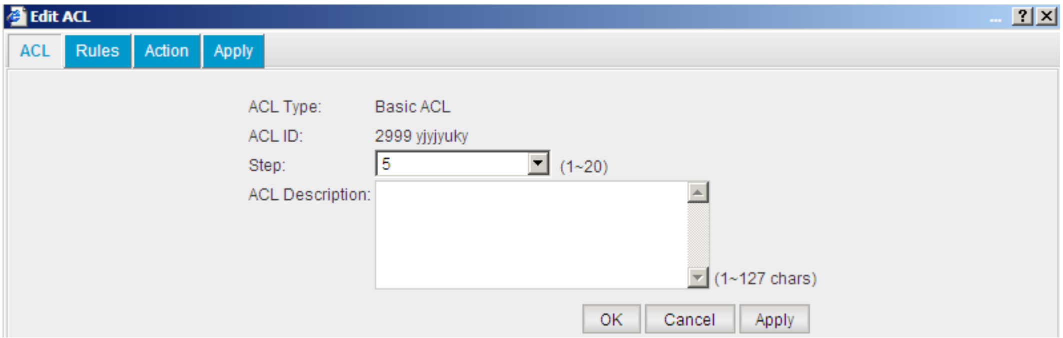
   NOTE

   - If no ACL is created, the system prompts you to create an ACL when you click the **rule** tab.
   - If no ACL is created, the system prompts you to create an ACL when you click the **action** or the **application** tab.
   - If an ACL rule is not created, the system displays a message indicating an empty ACL when you click the **Apply** tab.

- Edit an ACL.

1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
2. Click the 📝 icon to open the **Edit ACL** page.
3. Click the **ACL** tab, as shown in **Figure 6-10**.

Figure 6-10 Edit ACL



ACL Type: Basic ACL
ACL ID: 2999 yjyjyuky
Step: 5 (1~20)
ACL Description: (1~127 chars)

NOTE

- **Table 6-2** describes the parameters on the page.
- The ACL type and ACL identifier cannot be modified.
- The IPv6 ACL cannot be modified.

4. Click the **Rules** tab. The procedure for modifying a rule is similar to the procedure for creating a rule.
5. Click the **Action** tab. The **Action** tab page does not display the created action. The procedure for modifying a rule is similar to the procedure for creating a rule.
6. Click the **Apply** tab. The **Action** tab page displays the object to which the rule is applied.

   NOTE

   - The **Apply** tab page displays the object to which the ACL is applied.
   - If no new action is created, the system prompts you to create action when you click the **Apply** tab.
   - If an action is created, the new action will replace the original action and be delivered to objects when you click the **Apply** tab.

7. Modify the configuration parameter on the tab page.
8. Click **OK**.

NOTE

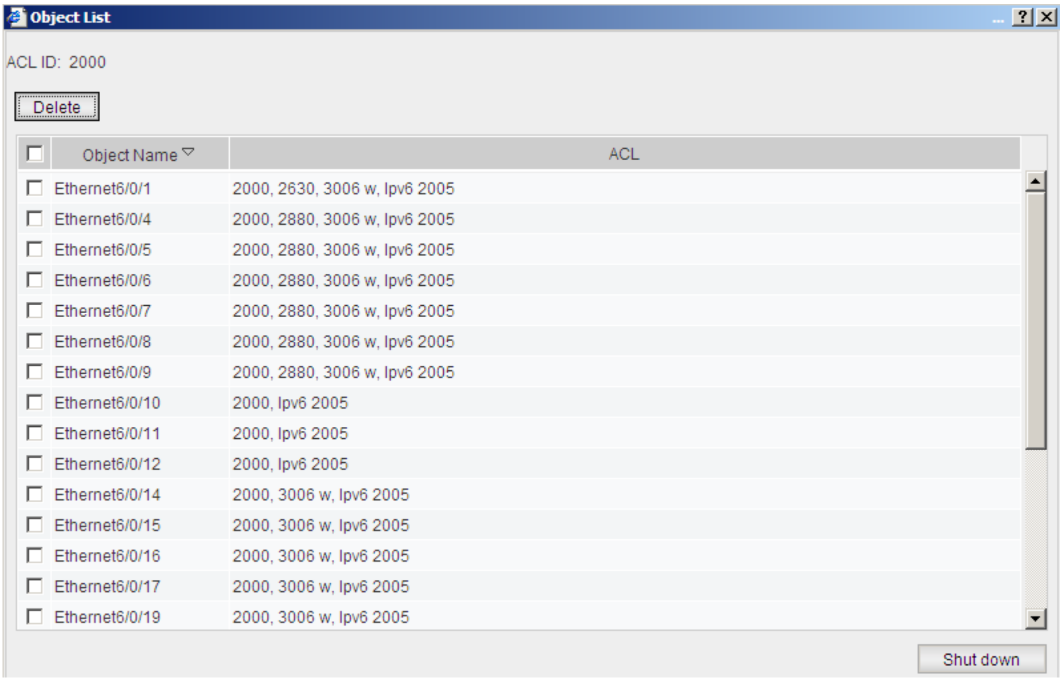
If an ACL rule is not created, the system displays a message indicating an empty ACL when you click the **Apply** tab.

- Delete an ACL.
  1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**. If the operation succeeds, the system returns to the **ACL Configuration** page; otherwise, an error message is displayed.
- Check basic ACL objects.
  1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
  2. Select a record that you want to check and click **Objects** to open the **Object List** page, as shown in **Figure 6-11**.

Figure 6-11 Object List



ACL ID: 2000

□ Object Name	ACL
□ Ethernet6/0/1	2000, 2630, 3006 w, Ipv6 2005
□ Ethernet6/0/4	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/5	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/6	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/7	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/8	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/9	2000, 2880, 3006 w, Ipv6 2005
□ Ethernet6/0/10	2000, Ipv6 2005
□ Ethernet6/0/11	2000, Ipv6 2005
□ Ethernet6/0/12	2000, Ipv6 2005
□ Ethernet6/0/14	2000, 3006 w, Ipv6 2005
□ Ethernet6/0/15	2000, 3006 w, Ipv6 2005
□ Ethernet6/0/16	2000, 3006 w, Ipv6 2005
□ Ethernet6/0/17	2000, 3006 w, Ipv6 2005
□ Ethernet6/0/19	2000, 3006 w, Ipv6 2005

Table 6-9 describes the parameters on the page.

Table 6-9 Check Basic ACL Object

Parameter	Description
Object Name	Indicates all objects that this ACL is applied to.

Parameter	Description
ACL	Indicates all ACLs applied to this object.

- Delete basic ACL objects.
  1. Choose **ACL** > **ACL** in the navigation tree to open the **ACL Configuration** page.
  2. Select the ACL whose objects you want to delete and click **Objects** to open the **Object List** page.
  3. Select the object name and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  4. Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

7 QoS

About This Chapter

This chapter describes the implementation principle of class-based QoS, and configuration methods of traffic management, interface-based rate limit, traffic shaping, priority mapping, and congestion management. The S2700SI switches do not support the QoS function.

By matching packets with the rules, the class-based QoS technology groups the packets sharing common features into one class and provides the same QoS level for traffic of the same type. In this manner, the class-based QoS technology provides differentiated services.

7.1 Traffic Management
The following sections describe the configuration methods of class-based QoS traffic management, including the configurations of the traffic classifier, traffic behavior, traffic policy, and application of the traffic policy.

7.2 Interface-based Rate Limit
The interface-based rate limit technology limits the rate of incoming and outgoing packets of an interface.

7.3 Traffic Shaping
Traffic shaping is also called queue shaping. The queue shaping technology limits traffic in a defined range by setting the shaping rate of packets of the entire queue. This prevents downstream traffic congestion.

7.4 Congestion Management
To ensure that delay-sensitive services have higher QoS level than non-delay-sensitive services, you can perform congestion management when temporary congestion occurs or increase bandwidth when the network is always congested. Congestion management technology sends flows of packets in queues by using queue scheduling technologies and scheduling algorithms. **The S5700SI, S2700SI, S2700EI or S2752EI series switches do not support this function.**

7.5 Priority Mapping
You can configure priority mappings and trusted interfaces. **The S2700SI, S2700EI or S2752EI series switches do not support this function.**

7.1 Traffic Management

The following sections describe the configuration methods of class-based QoS traffic management, including the configurations of the traffic classifier, traffic behavior, traffic policy, and application of the traffic policy.

7.1.1 Traffic Classifier

A traffic classifier is used to identify packets with certain features according to rules, and is the prerequisite and basis for providing differentiated services.

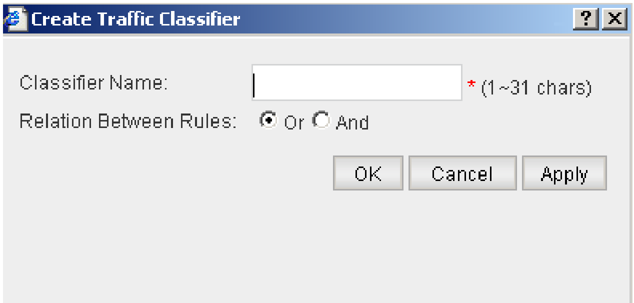
Context

By matching packets with the rules, the class-based QoS technology classifies packets according to certain rules and provides the same QoS level for traffic of the same type. In this manner, the class-based QoS technology provides differentiated services. A traffic classifier matches the packet header information with certain rules so that the packets sharing common features are grouped into one class.

Procedure

- Create a traffic classifier.
  1. Choose **QoS** > **Traffic Management** > **Traffic Classifier** in the navigation tree to open the **Traffic Classifier** page.
  2. Click **New** to open the **Create Traffic Classifier** page, as shown in **Figure 7-1**.

Figure 7-1 Create Traffic Classifier



Classifier Name: * (1~31 chars)
Relation Between Rules: ● Or ○ And

Table 7-1 describes the parameters on the **Create Traffic Classifier** page.

Table 7-1 Create Traffic Classifier

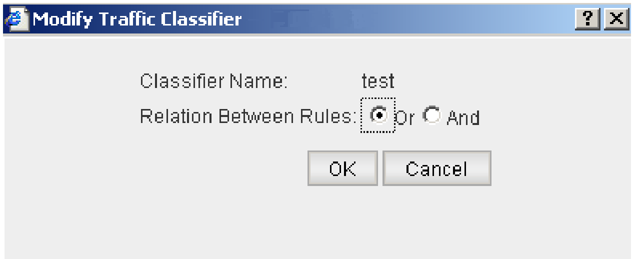
Parameter	Description
Classifier Name	Indicates the name of a traffic classifier. This parameter is mandatory.

Parameter	Description
Relation Between Rules	Indicates the relationship between rules, which can be **AND** or **OR**. By default, the value is **OR**.

3. Set parameters.
4. Click **OK**.

- Modify Traffic Classifier
  1. Choose **QoS** > **Traffic Management** > **Traffic Classifier** in the navigation tree to open the **Traffic Classifier** page.
  2. Click 📝 to open the **Modify Traffic Classifier** page, as shown in **Figure 7-2**.

Figure 7-2 Modify Traffic Classifier



Modify Traffic Classifier

Classifier Name: test

Relation Between Rules: ● Or ○ And

NOTE

- **Table 7-1** describes the parameters on the **Modify Traffic Classifier** page.
- The traffic classifier name cannot be modified.

  3. Set parameters.
  4. Click **OK**.

- Delete a traffic classifier.
  1. Choose **QoS** > **Traffic Management** > **Traffic Classifier** in the navigation tree to open the **Traffic Classifier** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

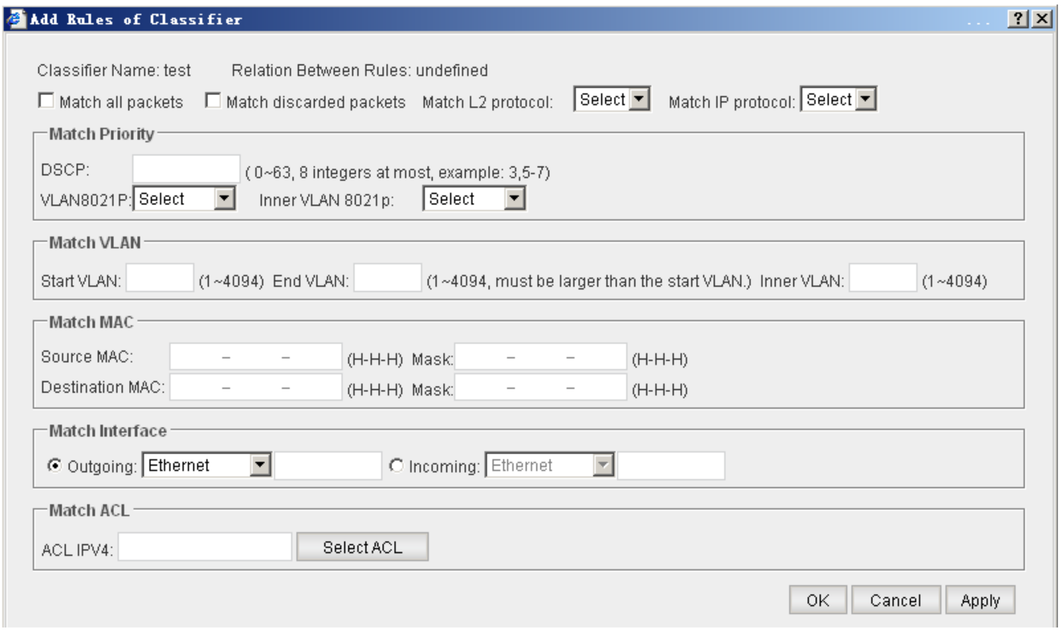
     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.

  3. Click **OK**.

- Add rules to the traffic classifier.
  1. Choose **QoS** > **Traffic Management** > **Traffic Classifier** in the navigation tree to open the **Traffic Classifier** page.
  2. Select the traffic classifier in which rules need to be added and click **New** to open the **Add Rules of Classifier** page, as shown in **Figure 7-3**.

Figure 7-3 Add Rules of Classifier



Add Rules of Classifier

Classifier Name: test   Relation Between Rules: undefined

□ Match all packets □ Match discarded packets Match L2 protocol: Select Match IP protocol: Select

Match Priority

DSCP: (0~63, 8 integers at most, example: 3,5-7)

VLAN8021P: Select Inner VLAN 8021p: Select

Match VLAN

Start VLAN: (1~4094) End VLAN: (1~4094, must be larger than the start VLAN.) Inner VLAN: (1~4094)

Match MAC

Source MAC: - - (H-H-H) Mask: - - (H-H-H)

Destination MAC: - - (H-H-H) Mask: - - (H-H-H)

Match Interface

● Outgoing: Ethernet ○ Incoming: Ethernet

Match ACL

ACL IPV4: Select ACL

Table 7-2 describes the parameters on the **Add Rules of Classifier** page.

Table 7-2 Add Rules of Classifier

Parameter	Description
Classifier Name	Indicates the name of a traffic classifier, which is set by the user.
Relation Between Rules	Indicates the relationship between rules, which is set by the user.
Match all packets	Indicates that all the packets are matched.
Match discarded packets	Indicates that discarded packets are matched. **NOTE** The S5700SI, S2700SI and S2700EI switches do not support this parameter.
Match L2 protocol	Indicates the matching rule based on the Layer 3 protocol type (Layer 2 encapsulated protocol fields), including: ● arp Indicates the ARP protocol. ● ip Indicates the IP protocol. ● mpls Indicates the MPLS protocol. ● rarp Indicates the RARP protocol.

Parameter		Description
Match IP protocol		Indicates the matching IP protocol, which can be IPv4 or IPv6.
Match Priority	DSCP	Indicates the matching rule based on DSCP priorities.
	VLAN8021p	Indicates the matching rule based on 802.1p priorities of VLAN packets.
	Inner VLAN 8021p	Indicates the matching rule based on 802.1p priorities in inner VLAN tags of QinQ packets. **NOTE** S5700SI switches do not support this parameter.
Match VLAN	Start VLAN	Indicates the start outer VLAN ID.
	End VLAN	Indicates the end outer VLAN ID.
	Inner VLAN	Indicates the inner VLAN ID. **NOTE** The S5700SI switches do not support this parameter.
Match MAC	Source MAC	Indicates the matching rule based on source MAC addresses. The value is in the format H-H-H. Each H represents four hexadecimal digits.
	Destination MAC	Indicates the matching rule based on destination MAC addresses. The value is in the format H-H-H. Each H represents four hexadecimal digits.
	Mask	Indicates the mask of the source MAC address. The value is in the format H-H-H. Each H represents four hexadecimal digits. If this parameter is not specified, the default value is FFFF-FFFF-FFFF. That is, all the MAC addresses are matched.
Match Interface	Outgoing	Indicates the matching rule based on outbound interfaces, for example, **Ethernet0/0/1**. **NOTE** ● This matching rule takes effect for only unicast packets. ● The outbound interface for classifying traffic must be different from the inbound interface where the traffic policy is applied; otherwise, the traffic policy cannot be used. ● The S5700SI, S2700SI and S2700EI switches do not support this parameter.
	Incoming	Indicates the matching rule based on inbound interfaces, for example, **Ethernet0/0/1**.

Parameter		Description
Match ACL	ACL IPv4	Indicates the matching rule based on IPv4 ACLs. Click **Select ACL** to select ACLs. You can select multiple ACLs.

📖 **NOTE**

The sequence of matching rules in a traffic classifier affects the flow matching sequence.

For example, if the matching rules based on 802.1p priorities of VLAN packets and inner VLAN tags are set, the system first matches flows with 802.1p priorities of VLAN packets and then inner VLAN tags. If multiple matching rules are configured, the system matches flows according to the matching rules one by one.

3. Set parameters.
4. Click **OK**.

- Delete rules.
  1. Choose **QoS** > **Traffic Management** > **Traffic Classifier** in the navigation tree to open the **Traffic Classifier** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     📖 **NOTE**

     You can delete rules in a batch.
  3. Click **OK**.

----End

7.1.2 Traffic Behavior

A traffic behavior contains actions of traffic policing, re-marking, flow mirroring, redirection, and traffic statistics. You can configure the traffic behavior as required.

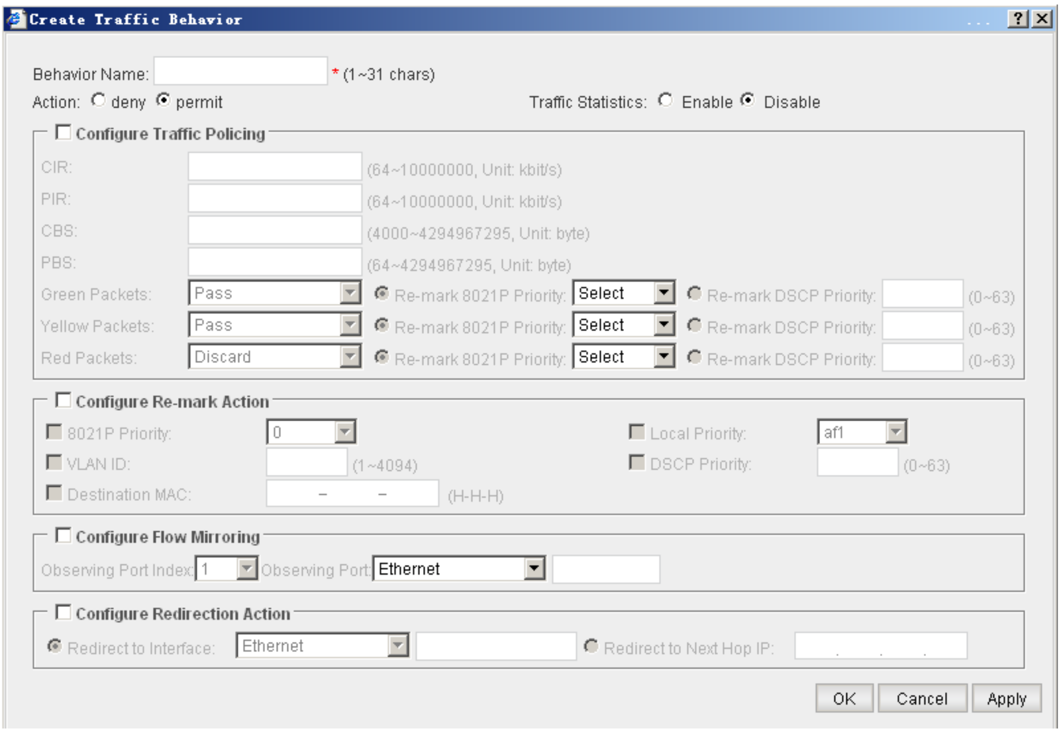
Context

The switch supports traffic behaviors of traffic policing, re-marking, flow mirroring, redirection, and traffic statistics.

Procedure

- Create a traffic behavior.
  1. Choose **QoS** > **Traffic Management** > **Traffic Behavior** in the navigation tree to open the **Traffic Behavior** page.
  2. Click **New** to open the **Create Traffic Behavior** page, as shown in **Figure 7-4**.

Figure 7-4 Create Traffic Behavior



Create Traffic Behavior

Behavior Name: * (1~31 chars)

Action: ○ deny ● permit

Traffic Statistics: ○ Enable ● Disable

□ Configure Traffic Policing

CIR: (64~10000000, Unit: kbit/s)

PIR: (64~10000000, Unit: kbit/s)

CBS: (4000~4294967295, Unit: byte)

PBS: (64~4294967295, Unit: byte)

Green Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

Yellow Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

Red Packets: Discard ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

□ Configure Re-mark Action

□ 8021P Priority: 0 □ Local Priority: af1

□ VLAN ID: (1~4094) □ DSCP Priority: (0~63)

□ Destination MAC: - - (H-H-H)

□ Configure Flow Mirroring

Observing Port Index: 1 Observing Port: Ethernet

□ Configure Redirection Action

● Redirect to Interface: Ethernet ○ Redirect to Next Hop IP: . . .

Table 7-3 describes the parameters on the **Create Traffic Behavior** page.

Table 7-3 Create Traffic Behavior

Parameter		Description
Behavior Name		Indicates the name of a traffic behavior. This parameter is mandatory.
Action		Indicates the traffic action used to control packets. The action can be **deny** or **permit**. By default, the action is **permit**.
Traffic Statistics		Indicates whether to enable the traffic statistics. The value can be **Enable** or **Disable**. By default, the value is **Disable**.
Configure Traffic Policing	CIR	Indicates the CIR, which is the allowed rate at which traffic can pass through.
	PIR	Indicates the PIR, which is the peak rate at which traffic can pass through. **NOTE** ● The value of PIR cannot be smaller than the value of CIR. By default, the value of PIR is equal to the value of the CIR. ● The S2700EI or S2700SI switches do not support this parameter.

Parameter			Description
	CBS		Indicates the CBS, which is the maximum size of burst traffic that can pass through.
	PBS		Indicates the PBS, which is the peak size of burst traffic that can pass through. The default value of PBS is related to the value of PIR. **NOTE** S2700EI and S2700SI switches do not support this parameter.
	Green Packets **NOTE** S2700SI and S2700EI switches do not support this parameter.	Green Packets	Indicates whether green packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**. **NOTE** S5700SI switches cannot be modified.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority. **NOTE** The S5700SI switches do not support this parameter.
		Re-mark DSCP Priority	Indicates Re-mark DSCP Priority. **NOTE** S5700SI switches do not support this parameter.
	Yellow Packets **NOTE** S2700SI and S2700EI switches do not support this parameter.	Yellow Packets	Indicates whether yellow packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority.
		Re-mark DSCP Priority	Indicates Re-mark DSCP Priority.
	Red Packets	Red Packets	Indicates whether red packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **discard**.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority.

Parameter			Description
	NOTE S2700SI and S2700EI switches do not support this parameter.	Re-mark DSCP Priority	Indicates Re-mark DSCP Priority.
Configure Re-mark Action	802.1P Priority		Indicates the 802.1p priority.
	Local Priority		Indicates the local priority. **NOTE** You cannot set both the 802.1p priority and the local priority for redirection in a traffic behavior.
	DSCP Priority		Indicates the DSCP priority.
	Destination MAC		Indicates the destination MAC address. The value is in the format H-H-H. Each H represents four hexadecimal digits. **NOTE** S5700SI, S2700SI and S2700EI switches do not support this parameter.
	VLAN ID		Indicates the VLAN ID.
	Inner VLAN		Indicates the inner VLAN ID. **NOTE** S5700SI, S2700EI, S2700SI and S2752EI switches do not support this parameter.
Configure Flow Mirroring	Observing Port Index		Indicates the ID of the observing interface where all matching flows are mirrored.
	Observing Port		Indicates the observing interface where all matching flows are mirrored, for example, **Ethernet0/0/1**.
Configure Redirection Action	Redirect to Interface		Indicates the interface where packets are redirected, for example, **Ethernet0/0/1**.

Parameter		Description
NOTE The S5700 SI, S2700 EI and S2700 SI switches do not support this parameter.	Redirect to Next Hop IP	Indicates the next hop address where packets are redirected, for example, **10.10.10.1**. **NOTE** You cannot configure both the next hop address where packets are redirected and the re-marked destination MAC address.

3. Set parameters.

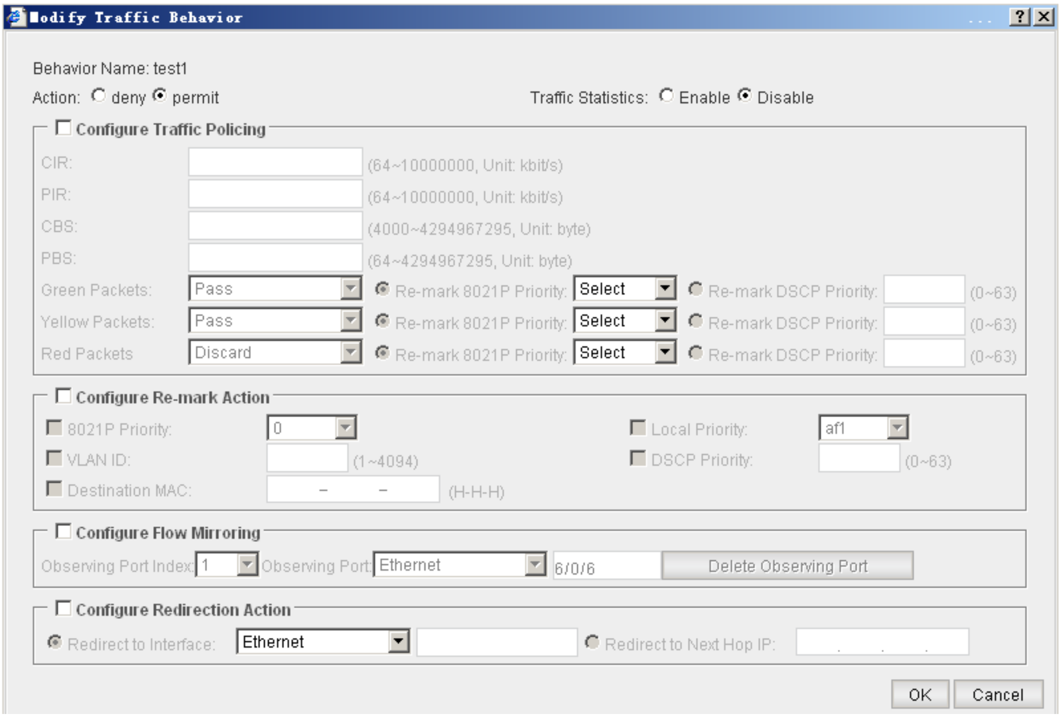
   NOTE

   To delete configuration of an item, deselect the checkbox of the item.

4. Click **OK**.

- Modify a traffic behavior.
  1. Choose **QoS** > **Traffic Management** > **Traffic Behavior** in the navigation tree to open the **Traffic Behavior** page.
  2. Click 📝 to open the **Modify Traffic Behavior** page, as shown in **Figure 7-5**.

Figure 7-5 Modify Traffic Behavior



Modify Traffic Behavior

Behavior Name: test1

Action: ○ deny ● permit

Traffic Statistics: ○ Enable ● Disable

□ Configure Traffic Policing

CIR: (64~10000000, Unit: kbit/s)

PIR: (64~10000000, Unit: kbit/s)

CBS: (4000~4294967295, Unit: byte)

PBS: (64~4294967295, Unit: byte)

Green Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

Yellow Packets: Pass ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

Red Packets Discard ● Re-mark 8021P Priority: Select ○ Re-mark DSCP Priority: (0~63)

□ Configure Re-mark Action

□ 8021P Priority: 0 □ Local Priority: af1

□ VLAN ID: (1~4094) □ DSCP Priority: (0~63)

□ Destination MAC: - - (H-H-H)

□ Configure Flow Mirroring

Observing Port Index: 1 Observing Port: Ethernet 6/0/6

□ Configure Redirection Action

● Redirect to Interface: Ethernet ○ Redirect to Next Hop IP: . . .

NOTE

- Table 7-4 describes the parameters on the **Modify Traffic Behavior** page.
- The traffic classifier name cannot be modified.

Table 7-4 Modify Traffic Behavior

Parameter			Description
Behavior Name			Shows the name of a traffic behavior.
Action			Indicates the traffic action used to control packets. The action can be **deny** or **permit**. By default, the action is **permit**.
Traffic Statistics			Indicates whether to enable the traffic statistics. The value can be **Enable** or **Disable**. By default, the value is **Disable**.
Configure Traffic Policing	CIR		Indicates the CIR, which is the allowed rate at which traffic can pass through.
	PIR		Indicates the PIR, which is the peak rate at which traffic can pass through. NOTE ● The value of PIR cannot be smaller than the value of CIR. By default, the value of PIR is equal to the value of the CIR. ● The S2700EI or S2700SI switches do not support this parameter.
	CBS		Indicates the CBS, which is the maximum size of burst traffic that can pass through.
	PBS		Indicates the PBS, which is the peak size of burst traffic that can pass through. The default value of PBS is related to the value of PIR. NOTE S2700EI and S2700SI switches do not support this parameter.
	Green Packets	Green Packets	Indicates whether green packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**. NOTE S5700SI switches cannot be modified.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority. NOTE The S5700SI switches do not support this parameter.

Parameter			Description
	NOTE S2700SI and S2700EI switches do not support this parameter.	Re-mark DSCP Priority	Indicates Re-mark DSCP Priority. **NOTE** S5700SI switches do not support this parameter.
	Yellow Packets **NOTE** S2700SI and S2700EI switches do not support this parameter.	Yellow Packets	Indicates whether yellow packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **pass**.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority.
		Re-mark DSCP Priority	Indicates Re-mark DSCP Priority.
	Red Packets **NOTE** S2700SI and S2700EI switches do not support this parameter.	Red Packets	Indicates whether red packets are allowed to pass through. The action can be **pass** or **discard**. By default, the action is **discard**.
		Re-mark 8021P Priority	Indicates the re-marked 802.1p priority.
		Re-mark DSCP Priority	Indicates Re-mark DSCP Priority.
Configure Re-mark Action	8021P Priority		Indicates the 802.1p priority.
	Local Priority		Indicates the local priority. **NOTE** You cannot set both the 802.1p priority and the local priority for redirection in a traffic behavior.
	DSCP Priority		Indicates the DSCP priority.
	Destination MAC		Indicates the destination MAC address. The value is in the format H-H-H. Each H represents four hexadecimal digits. **NOTE** S5700SI, S2700SI and S2700EI switches do not support this parameter.

Parameter		Description
	VLAN ID	Indicates the VLAN ID.
	Inner VLAN	Indicates the inner VLAN ID. NOTE S5700SI, S2700EI, S2700SI and S2752EI switches do not support this parameter.
Configure Flow Mirroring	Observing Port Index	Indicates the ID of the observing interface where all matching flows are mirrored.
	Observing Port	Indicates the observing interface where all matching flows are mirrored, for example, **Ethernet0/0/1**.
	Delete Observing Port	Deletes the binding between an observing interface index and an observing interface. NOTE If an observing interface index is not bound to any observing interface, this button is unavailable.
Configure Redirection Action NOTE The S5700SI, S2700EI and S2700SI switches do not support this parameter.	Redirect to Interface	Indicates the interface where packets are redirected, for example, **Ethernet0/0/1**.
	Redirect to Next Hop IP	Indicates the next hop address where packets are redirected, for example, **10.10.10.1**. NOTE You cannot configure both the next hop address where packets are redirected and the re-marked destination MAC address.

3. Set parameters.
4. Click **OK**.

- Delete a traffic behavior.
  1. Choose **QoS** > **Traffic Management** > **Traffic Behavior** in the navigation tree to open the **Traffic Behavior** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.

3. Click **OK**.

----End

7.1.3 Traffic Policy

A traffic policy is a QoS policy in which traffic classifiers are bound to traffic behaviors.

Context

A traffic policy can be used on an interface, globally, on an LPU, or in a VLAN so that traffic classifiers bound to traffic behaviors in the traffic policy are used on the interface, globally, on the LPU, or in the VLAN.

Procedure

- Create a traffic policy.
  1. Choose **QoS** > **Traffic Management** > **Traffic Policy** in the navigation tree to open the **Traffic Policy** page.
  2. Click **New** to open the **Create Traffic Policy** page, as shown in **Figure 7-6**.

Figure 7-6 Create Traffic Policy

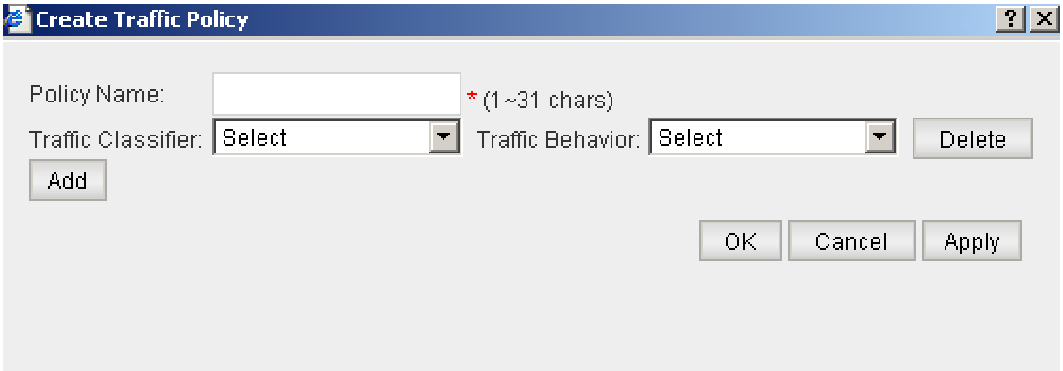


Table 7-5 describes the parameters on the **Create Traffic Policy** page.

Table 7-5 Create Traffic Policy

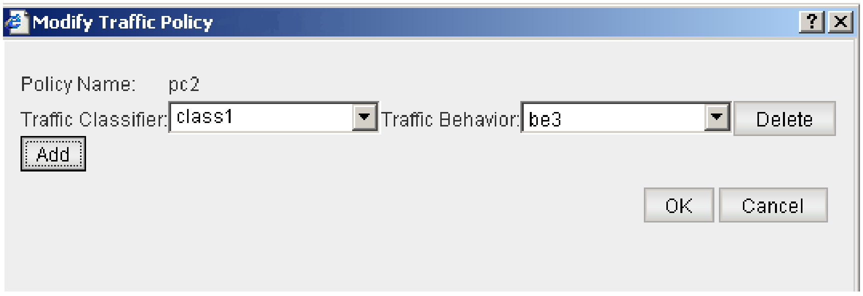
Parameter	Description
Policy Name	Indicates the name of a traffic policy. This parameter is mandatory.
Traffic Classifier	Indicates the name of a traffic classifier. NOTE In a traffic policy, you can configure multiple binding relationships between traffic classifiers and traffic behaviors and each traffic classifier can be bound to only one traffic behavior.

Parameter	Description
Traffic Behavior	Indicates the name of a traffic behavior. **NOTE** In a traffic policy, you can configure multiple binding relationships between traffic classifiers and traffic behaviors and each traffic classifier can be bound to only one traffic behavior.

3. Set parameters.
4. Click **OK**.

- Modify a traffic policy.
  1. Choose **QoS** > **Traffic Management** > **Traffic Policy** in the navigation tree to open the **Traffic Policy** page.
  2. Click 📝 to open the **Modify Traffic Policy** page, as shown in **Figure 7-7**.

Figure 7-7 Modify Traffic Policy



Modify Traffic Policy

Policy Name: pc2

Traffic Classifier: class1

Traffic Behavior: be3

NOTE

- **Table 7-5** describes the parameters on the **Modify Traffic Policy** page.
- The traffic policy name cannot be modified.

  3. Set parameters.
  4. Click **OK**.

- Delete a traffic policy.
  1. Choose **QoS** > **Traffic Management** > **Traffic Policy** in the navigation tree to open the **Traffic Policy** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

  3. Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

7.1.4 Apply Traffic Policy

A traffic policy takes effect only after being applied.

Context

None.

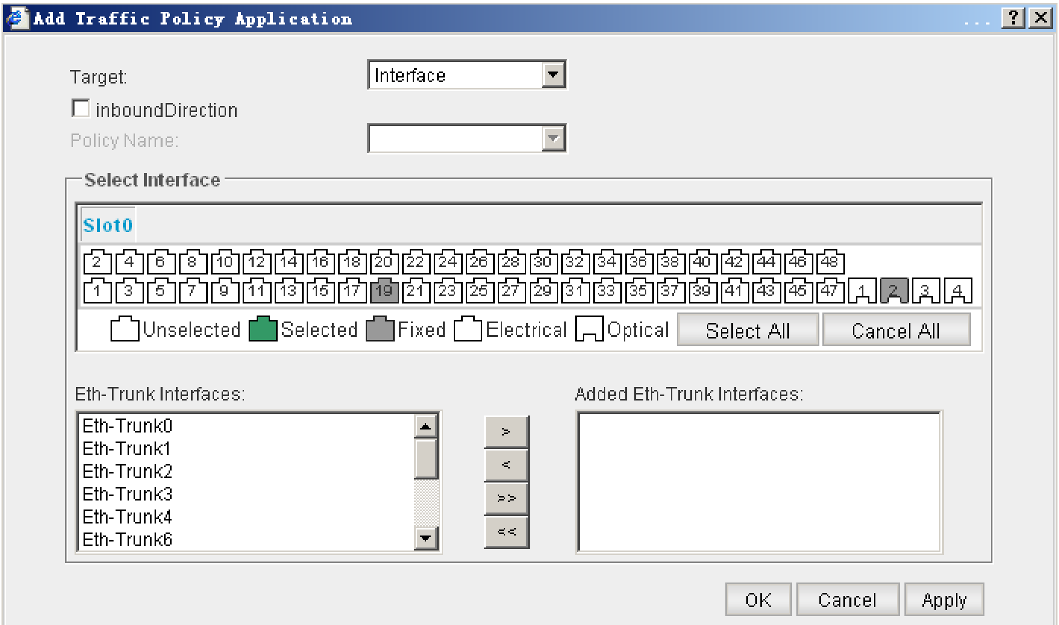
Procedure

- Query information about the traffic policy application.

  When you enter the **Apply Traffic Policy** page, you query only the traffic policy applied globally. This is because querying the traffic policy applied to an interface takes much time.

  1. Choose **QoS** > **Traffic Management** > **Apply Traffic Policy** in the navigation tree to open the **Apply Traffic Policy** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Add a traffic policy application.
  1. Choose **QoS** > **Traffic Management** > **Apply Traffic Policy** in the navigation tree to open the **Apply Traffic Policy** page.
  2. Click **New** to open the **Add Traffic Policy Application** page, as shown in **Figure 7-8**.

Figure 7-8 Add Traffic Policy Application



Add Traffic Policy Application

Target: Interface

□ inboundDirection

Policy Name:

Select Interface

Slot0

Eth-Trunk Interfaces:

Eth-Trunk0
Eth-Trunk1
Eth-Trunk2
Eth-Trunk3
Eth-Trunk4
Eth-Trunk6

Added Eth-Trunk Interfaces:

Table 7-6 describes the parameters on the **Add Traffic Policy Application** page.

Table 7-6 Add Traffic Policy Application

Parameter	Description
Target	Indicates the name of the configured traffic policy. The value can be **interface**, **VLAN**, or **global**. ● If the traffic policy is applied to an interface, you need to select an interface on the displayed page. ● If the traffic policy is applied to an interface, you need to enter the VLAN ID on the displayed page. ● If the traffic policy is applied globally, the page for global application of the traffic policy is displayed.
inbound Direction	Indicates the inbound direction.
outbound Direction	Indicates the outbound direction. NOTE Only S5700EI and S5700SI switches support this parameter.
Select Interface	Indicates the interface where the traffic policy is applied.

3. Set parameters.
4. Click **OK**.

- Delete a traffic policy application.
  1. Choose **QoS** > **Traffic Management** > **Apply Traffic Policy** in the navigation tree to open the **Apply Traffic Policy** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - Click the check box of the selected record.
     - You can also move records to the recycle bin in batches. That is, click the check boxes of the records.
  3. Click **OK**.

----End

7.2 Interface-based Rate Limit

The interface-based rate limit technology limits the rate of incoming and outgoing packets of an interface.

7.2.1 View Rate Limit

You can view detailed information about interface-based rate limit.

Context

You can select an interface to view the rate limit information.

Procedure

Step 1 Choose **QoS** > **Limit Rate** > **View Rate Limit** in the navigation tree to open the **View Rate Limit** page.

Step 2 Select any interface.

Step 3 The rate limit values are displayed.

NOTE

You can select only one interface.

----End

7.2.2 Configure Rate Limit

The interface-based rate limit function is used to limit the rate of outgoing traffic or incoming traffic on a physical interface.

Context

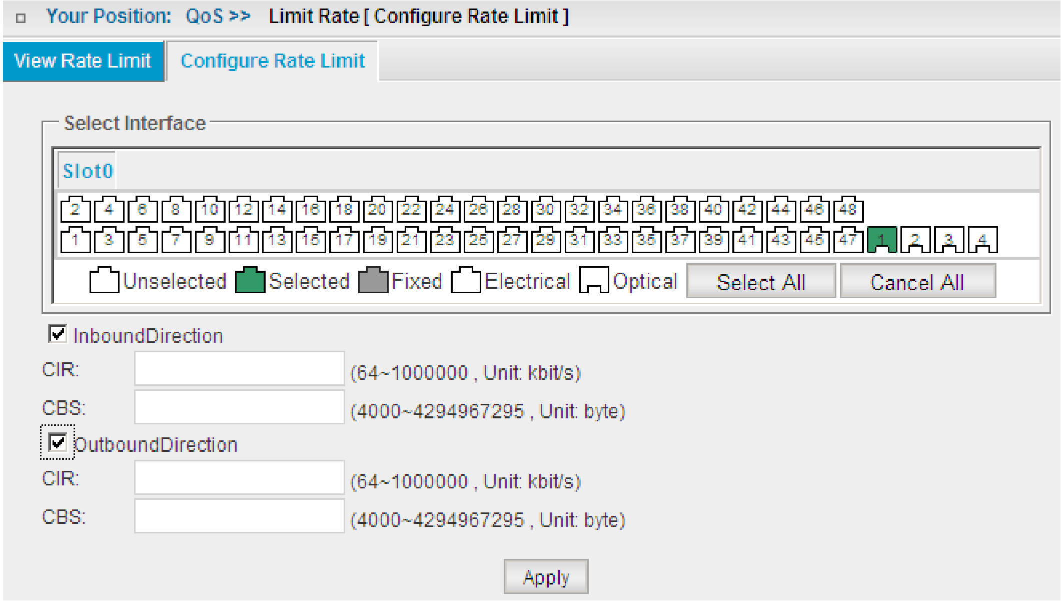
Before sending traffic from an interface, you can configure rate limit on the interface in the outbound direction. This function controls all outgoing packets.

Before sending traffic from an interface, you can configure rate limit on the interface in the inbound direction. This function controls all incoming packets.

Procedure

Step 1 Choose **QoS** > **Limit Rate** > **Configure Rate Limit** in the navigation tree to open the **Configure Rate Limit** page, as shown in **Figure 7-9**.

Figure 7-9 Configure Rate Limit



☑ InboundDirection

CIR: (64~1000000 , Unit: kbit/s)

CBS: (4000~4294967295 , Unit: byte)

☑ OutboundDirection

CIR: (64~1000000 , Unit: kbit/s)

CBS: (4000~4294967295 , Unit: byte)

Table 7-7 describes the parameters on the **Configure Rate Limit** page.

Table 7-7 Configure Rate Limit

Parameter		Description
Select Interface		Indicates the interface where rate limit is configured. You can select multiple interfaces.
Inbound Direction	CIR	Indicates the CIR in the inbound direction.
	CBS	Indicates the CBS in the inbound direction.
Outbound Direction	CIR	Indicates the CIR in the outbound direction.
	CBS	Indicates the CBS in the outbound direction.

Step 2 Select the interfaces that you want to configure.

Step 3 Click **Inbound** or **Outbound** and set the values of CIR and CBS.

Step 4 Click **Apply** to complete the configuration.

----End

7.3 Traffic Shaping

Traffic shaping is also called queue shaping. The queue shaping technology limits traffic in a defined range by setting the shaping rate of packets of the entire queue. This prevents downstream traffic congestion.

7.3.1 View Traffic Shaping

You can view traffic shaping information about an interface.

Context

- The switch supports queue shaping and interface shaping.
- You can select an interface to view the traffic shaping information. You can select only one interface.

Procedure

Step 1 Choose **QoS** > **Traffic Shaping** > **View Traffic Shaping** in the navigation tree to open the **View Traffic Shaping** page.

Step 2 Select any interface.

Step 3 The traffic shaping information about the interface is displayed.

NOTE

You can select only one interface.

----End

7.3.2 Configure Traffic Shaping

You can configure the traffic shaping function.

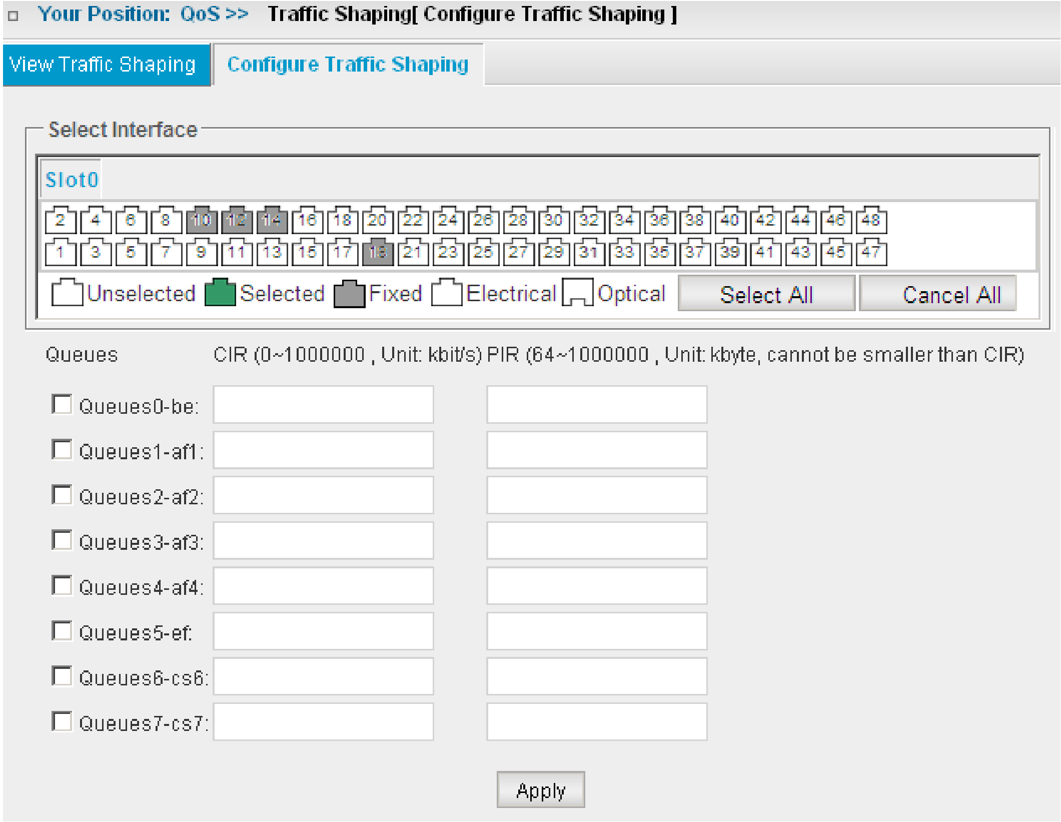
Context

When the rate of an interface on a downstream device is smaller than the rate of an interface on an upstream device or the burst traffic occurs, traffic congestion may occur on the interface of the downstream device. In this case, you can configure traffic shaping on the interface of the upstream device in the outbound direction so that traffic is sent at an even rate and the congestion problem of the downstream device is solved.

Procedure

Step 1 Choose **QoS** > **Traffic Shaping** > **Configure Traffic Shaping** in the navigation tree to open the **Configure Traffic Shaping** page, as shown in **Figure 7-10**.

Figure 7-10 Configure Traffic Shaping



□ Your Position: QoS >> Traffic Shaping[Configure Traffic Shaping]

Select Interface

Slot0

Queues CIR (0~1000000 , Unit: kbit/s) PIR (64~1000000 , Unit: kbyte, cannot be smaller than CIR)

□ Queues0-be:
□ Queues1-af1:
□ Queues2-af2:
□ Queues3-af3:
□ Queues4-af4:
□ Queues5-ef:
□ Queues6-cs6:
□ Queues7-cs7:

Table 7-8 describes the parameters on the **Configure Traffic Shaping** page.

Table 7-8 Configure Traffic Shaping

Parameter	Description
Select Interface	Indicates the interface where traffic shaping needs to be configured. You can select multiple interfaces.
Queues	Indicates the queue. NOTE S2700EI series switches only support 0 to 3 queues.
CIR	Indicates the CIR.
PIR	Indicates the PIR of an interface. The default value is the bandwidth of the interface and the value cannot be smaller than the value of the CIR. NOTE S2700EI series switches do not support PIR.
CBS	Indicates the committed burst size. NOTE Only S2700EI series switches support CBS.

Step 2 Select the interfaces that you want to configure.

Step 3 Select the queue that you want to configure and set the values of CIR, PIR, and CBS.

NOTE

If you do not select the queue, the configurations of the queue are deleted.

Step 4 Click **Apply** to complete the configuration.

----End

7.4 Congestion Management

To ensure that delay-sensitive services have higher QoS level than non-delay-sensitive services, you can perform congestion management when temporary congestion occurs or increase bandwidth when the network is always congested. Congestion management technology sends flows of packets in queues by using queue scheduling technologies and scheduling algorithms. **The S5700SI, S2700SI, S2700EI or S2752EI series switches do not support this function.**

7.4.1 View Scheduling

You can view the queue scheduling mode on an interface.

Context

Queue scheduling technologies include PQ scheduling, DRR scheduling and WRR scheduling.

Procedure

Step 1 Choose **QoS** > **Congestion Management** > **View Scheduling** in the navigation tree to open the **View Scheduling** page.

Step 2 Select any interface.

Step 3 The scheduling information about the interface is displayed.

NOTE

You can select only one interface.

----End

7.4.2 Configure Scheduling

When congestion occurs on a network, queue scheduling solves the resource preemption problem among multiple packets.

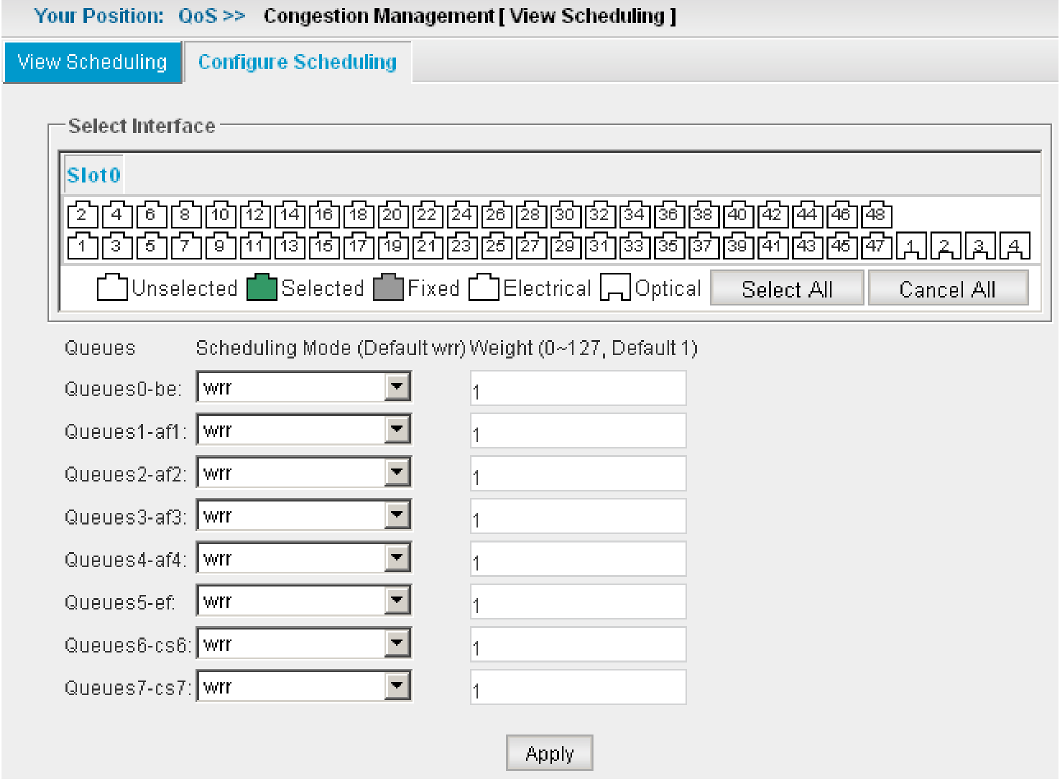
Context

- Congestion management technology prevents intermittent congestion on networks by using queue scheduling technologies.
- Queue scheduling technologies include PQ scheduling, DRR scheduling and WRR scheduling.

Procedure

Step 1 Choose **QoS** > **Congestion Management** > **Configure Scheduling** in the navigation tree to open the **Configure Scheduling** page, as shown in **Figure 7-11**.

Figure 7-11 Configure Scheduling



Queues	Scheduling Mode (Default wrr)	Weight (0~127, Default 1)
Queues0-be:	wrr	1
Queues1-af1:	wrr	1
Queues2-af2:	wrr	1
Queues3-af3:	wrr	1
Queues4-af4:	wrr	1
Queues5-ef:	wrr	1
Queues6-cs6:	wrr	1
Queues7-cs7:	wrr	1

Table 7-9 describes the parameters on the **Configure Scheduling** page.

Table 7-9 Configure Scheduling

Parameter	Description
Select Interface	Indicates the interface where scheduling needs to be configured. You can select multiple interfaces.
Queues	Indicates the queue where scheduling needs to be configured.
Scheduling Mode	Indicates the queue scheduling mode, including: ● PQ In PQ mode, the switch schedules packets based on priorities of queues in a strict manner. The weight is not used in this mode. ● DRR In RR mode, the switch schedules packets circularly based on priorities of queues. Based on RR scheduling, DRR scheduling is used to schedule packet flows of all the queues according to the maximum bandwidth assigned by the switch to the queues. ● WRR Based on RR scheduling, WRR scheduling is used to schedule packet flows based on weights of queues. The default value is wrr.
Weight	Indicates the weight used to schedule packet flows in queues.

Step 2 Select the interfaces that you want to configure.

Step 3 Set the scheduling mode and weight for the queue.

Step 4 Click **Apply** to complete the configuration.

----End

7.5 Priority Mapping

You can configure priority mappings and trusted interfaces. **The S2700SI, S2700EI or S2752EI series switches do not support this function.**

7.5.1 Priority Mapping

You can configure priority mappings on switches.

Context

When packets are sent to the inbound or outbound interface of a device, the device determines the queues and priorities of packets according to DSCP or the IP precedence field. The S3700 and S5700 switches support priority mappings for incoming packets. The S6700 series switches support priority mappings for incoming packets and outgoing packets.

Procedure

- Create a Diff-Serv domain name.

  NOTE

  You can create a Diff-Serv domain name on the S6700 switches.

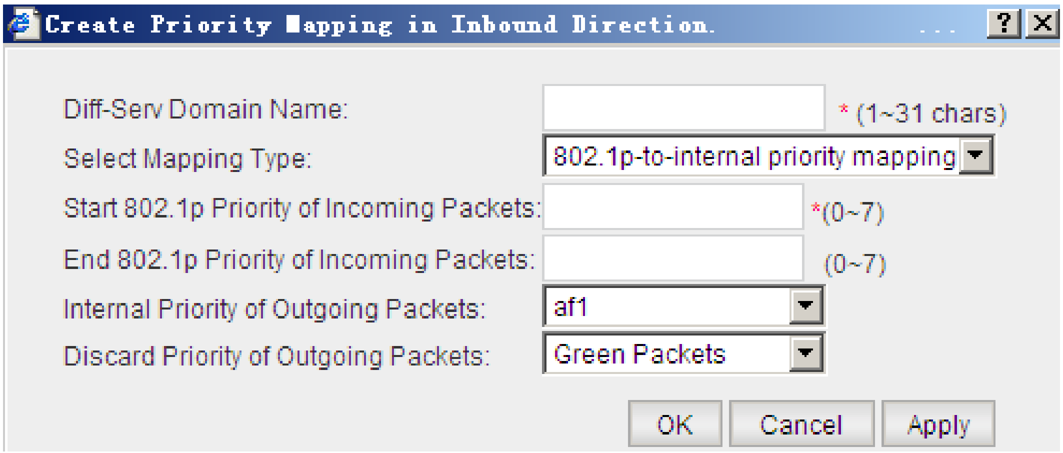
  1. Choose **QoS** > **Priority Mapping** to open the **Priority Mapping in Inbound Direction** page.

     NOTE

     - By default, the Diff-Serv domain name is default.
     - The maximum of eight Diff-Serv domain names can be created.
     - You can create a Diff-Serv domain name in the same way on the **Priority Mapping in Outbound Direction** page.

  2. Click **New**. The **Create Priority Mapping in Inbound Direction** is displayed, as shown in **Figure 7-12**.

Figure 7-12 Create Priority Mapping in Inbound Direction



Create Priority Mapping in Inbound Direction

Diff-Serv Domain Name: * (1~31 chars)

Select Mapping Type: 802.1p-to-internal priority mapping

Start 802.1p Priority of Incoming Packets: *(0~7)

End 802.1p Priority of Incoming Packets: (0~7)

Internal Priority of Outgoing Packets: af1

Discard Priority of Outgoing Packets: Green Packets

Table 7-10 describes the parameters on the page.

Table 7-10 Create Priority Mapping in Inbound Direction

Parameter	Description
Diff-Serv Domain Name	The value is a string of 1 to 31 characters.
Select Mapping Type	Mapping types include **802.1p-to-internal Priority Mapping** and **DSCP-to-internal Priority Mapping**.
Start 802.1p Priority of Incoming Packets	Indicates the start 802.1p priority ranging from 0 to 7. This parameter is mandatory.
End 802.1p Priority of Incoming Packets	Indicates the end 802.1p priority ranging from 0 to 7.
Internal Priority of Outgoing Packets	Indicates the internal priority including seven options. This parameter is mandatory.

Parameter	Description
Discard Priority of Outgoing Packets	Indicates the discard priority including **Green Packets**, **Yellow Packets**, and **Red Packets**. This parameter is mandatory.

NOTE

Select Mapping Type

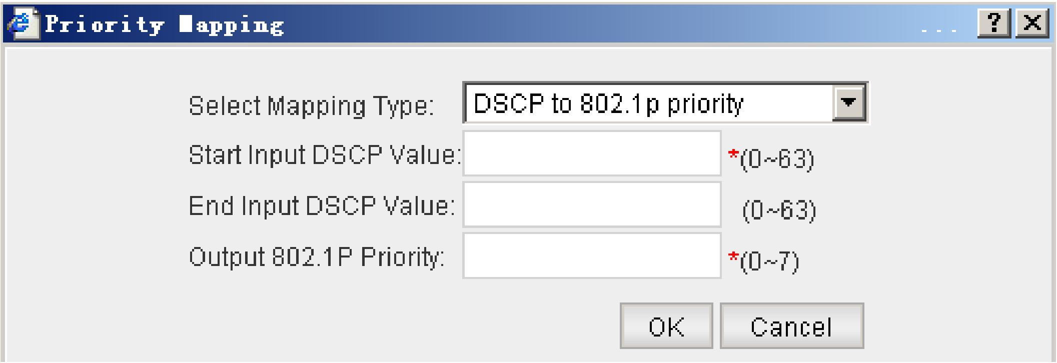
- For example, select **802.1p-to-internal Priority Mapping** as the default value.
- When **DSCP-to-internal Priority Mapping** is selected,

  the page displays a list including **Start DSCP Priority of Incoming Packets**, **End DSCP Priority of Incoming Packets**, **Internal Priority of Outgoing Packets** and **Discard Priority of Outgoing Packets**.
- The values of **Start DSCP Priority** and **End DSCP Priority** range from 0 to 63.
- The values of **Internal Priority** and **Discard Priority** are consistent with that of **802.1p-to-internal Priority Mapping**.

3. Set parameters.
4. Click **OK**.

- Configure priority mapping.
  - The S3700 and S5700 switches support this function.
    1. Choose **QoS** > **Priority Mapping** to open the **Priority Mapping** page.
    2. Click **Configure** to open the **Priority Mapping** page, as shown in **Figure 7-13**.

Figure 7-13 Priority Mapping



Priority Mapping

Select Mapping Type: DSCP to 802.1p priority

Start Input DSCP Value: *(0~63)

End Input DSCP Value: (0~63)

Output 802.1P Priority: *(0~7)

Table 7-11 describes the parameters on the page.

Table 7-11 Priority Mapping

Parameter	Description
Select Mapping Type	Indicates the priority mapping type.

Parameter	Description
Start Input DSCP Value	Specifies the start DSCP value of the incoming packets. The value ranges from 0 to 63. This parameter is mandatory. Specifies the start IP precedence value of the incoming packets. The value ranges from 0 to 7.
End Input DSCP Value	Specifies the end DSCP value of the incoming packets. The value ranges from 0 to 63. Specifies the end IP precedence value of the incoming packets. The value ranges from 0 to 7.
Output 802.1P Priority	Specifies the 802.1p priority of the outgoing packets. The value is an integer that ranges from 0 to 7. This parameter is mandatory. Specifies the discard priority of the outgoing packets. The value is an integer that ranges from 0 to 2. Specifies the DSCP priority of the outgoing packets. The value is an integer that ranges from 0 to 63.

NOTE

Configure the priority mappings as follows:

- To map the DSCP field to the 802.1p field, set the start DSCP value, end DSCP value, and specified 802.1p field of outgoing packets.
- To map the DSCP field to the discard priority, set the start DSCP value, end DSCP value, and discard priority.
- To map the DSCP field to the DSCP field, set the start DSCP value, end DSCP value, and DSCP value of outgoing packets.
- To map the IP precedence field to the 802.1p field, set the start IP precedence value, end IP precedence value, and specified 802.1p field of outgoing packets.
- To map the IP precedence field to the IP precedence field, set the start IP precedence value, end IP precedence value, and specified IP precedence value of outgoing packets.

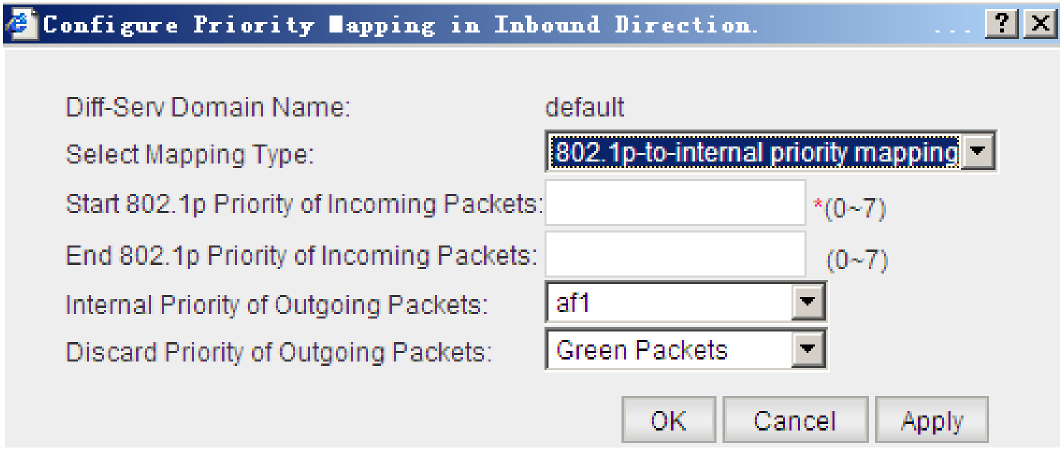
The following is an example for mapping the DSCP field to the 802.1p field.

3. Set parameters.
4. Click **OK**.

– The S6700 switches support this function.

1. Choose **QoS** > **Priority Mapping** > **Priority Mapping in Inbound Direction** to open the **Priority Mapping in Inbound Direction** page.
2. Select a record and click **Configure** to open the **Configure Priority Mapping in Inbound Direction** page, as shown in **Figure 7-14**.

Figure 7-14 Configure Priority Mapping in Inbound Direction



Diff-Serv Domain Name: default

Select Mapping Type: 802.1p-to-internal priority mapping

Start 802.1p Priority of Incoming Packets: *(0~7)

End 802.1p Priority of Incoming Packets: (0~7)

Internal Priority of Outgoing Packets: af1

Discard Priority of Outgoing Packets: Green Packets

Table 7-12 describes the parameters on the page.

Table 7-12 Configure Priority Mapping in Inbound Direction

Parameter	Description
Diff-Serv Domain Name	Indicates the current Diff-Serv domain name. This parameter cannot be modified.
Select Mapping Type	Mapping types include **802.1p-to-internal Priority Mapping** and **DSCP-to-internal Priority Mapping**.
Start 802.1p Priority of Incoming Packets	Indicates the start 802.1p priority ranging from 0 to 7. This parameter is mandatory.
End 802.1p Priority of Incoming Packets	Indicates the end 802.1p priority ranging from 0 to 7.
Internal Priority of Outgoing Packets	Indicates the internal priority including seven options. This parameter is mandatory.
Discard Priority of Outgoing Packets	Indicates the discard priority including **Green Packets**, **Yellow Packets**, and **Red Packets**. This parameter is mandatory.

NOTE

Select Mapping Type

- For example, select **802.1p-to-internal Priority Mapping** as the default value.
- When **DSCP-to-internal Priority Mapping** is selected,

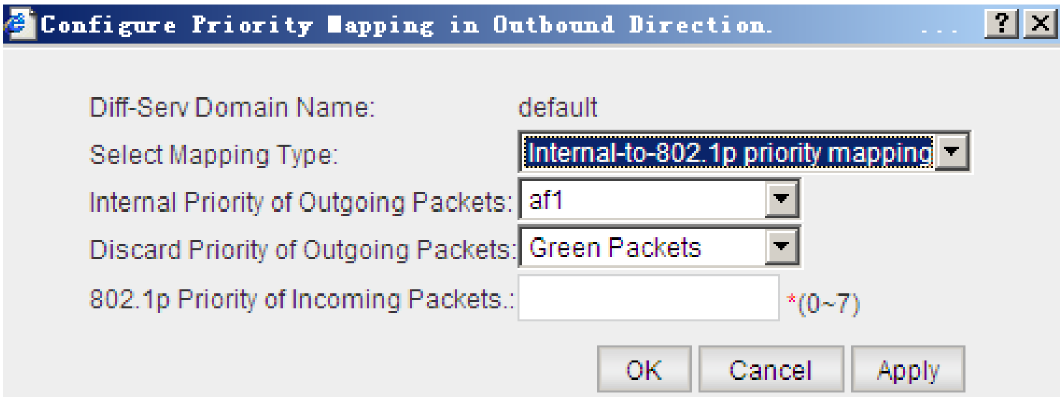
  the page displays a list including **Start DSCP Priority**, **End DSCP Priority**, **Internal Priority**, and **Discard Priority**.
- The values of **Start DSCP Priority** and **End DSCP Priority** range from 0 to 63.
- The values of **Internal Priority** and **Discard Priority** are consistent with that of **802.1p-to-internal Priority Mapping**.

3. Set parameters.
4. Click **OK**.

– The S6700 switches support this function.

1. Choose **QoS** > **Priority Mapping** > **Priority Mapping in Outbound Direction** to open the **Priority Mapping in Outbound Direction** page.
2. Select a record and click **Configure** to open the **Configure Priority Mapping in Outbound Direction** page, as shown in **Figure 7-15**.

Figure 7-15 Configure Priority Mapping in Outbound Direction



Diff-Serv Domain Name: default

Select Mapping Type: Internal-to-802.1p priority mapping

Internal Priority of Outgoing Packets: af1

Discard Priority of Outgoing Packets: Green Packets

802.1p Priority of Incoming Packets.: *(0~7)

Table 7-13 describes the parameters on the page.

Table 7-13 Configure Priority Mapping in Outbound Direction

Parameter	Description
Diff-Serv Domain Name	Indicates the current Diff-Serv domain name. This parameter cannot be modified.
Select Mapping Type	Mapping types include **Internal-to-802.1p Priority Mapping** and **Internal-to-DSCP Priority Mapping**.
Internal Priority of Outgoing Packets	Indicates the internal priority including seven options. This parameter is mandatory.

Parameter	Description
Discard Priority of Outgoing Packets	Indicates the discard priority including **Green Packets**, **Yellow Packets**, and **Red Packets**. This parameter is mandatory.
802.1p Priority of Incoming Packets	Indicates the start 802.1p priority ranging from 0 to 7. This parameter is mandatory.

NOTE

Select Mapping Type

- For example, select **Internal-to-802.1p Priority Mapping** as the default value.
- When **Internal-to-DSCP Priority Mapping** is selected,

  the page displays a list including **Internal Priority**, **Discard Priority**, and **DSCP Priority**.
- The DSCP value ranges from 0 to 63.
- The values of **Internal Priority**, **Discard Priority** are consistent with that of **Internal-to-DSCP Priority Mapping**.

3. Set parameters.
4. Click **OK**.

- Delete priority mapping.
  1. Choose **QoS** > **Priority Mapping** to open the **Priority Mapping** page.

     NOTE

     The S6700 switches can delete priority mapping on the **Priority Mapping in Inbound Direction** or **Priority Mapping in Outbound Direction** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.
- Delete Diff-Serv Domain Name

  NOTE

  The S6700 series switches can delete a Diff-Serv domain name.

  1. Choose **QoS** > **Priority Mapping** > **Priority Mapping** to open the **Priority Mapping in Inbound Direction** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - You can delete a Diff-Serv domain name in the same way on the **Priority Mapping in Outbound Direction** page.
     - By default, the Diff-Serv domain name is default. You cannot delete the default name.

3. Click **OK**.

----End

7.5.2 Trust Priority

You can query, add, modify, and delete the trust relations on interfaces.

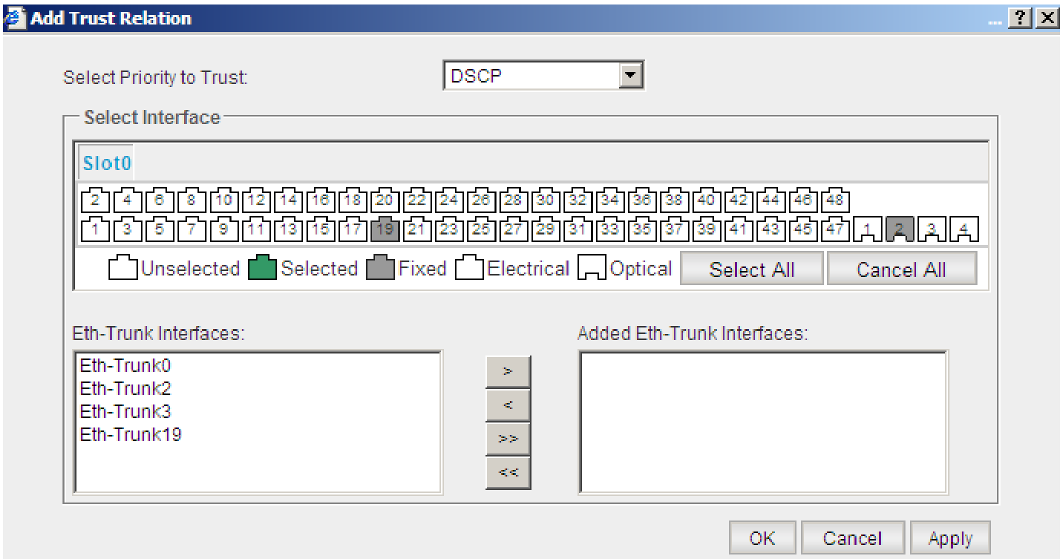
Context

You can select the type of a trusted priority.

Procedure

- Query a trust relation.
  1. Choose **QoS** > **Priority Mapping** > **Trust Priority** to open the **Trust Priority** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Add a trust relation.
  - This function is only **supported by S3700 and S5700 series switches.**
    1. Choose **QoS** > **Priority Mapping** > **Trust Priority** to open the **Trust Priority** page.
    2. Click **New** to open the **Add Trust Relation** page, as shown in **Figure 7-16**.

Figure 7-16 Add Trust Relation



Add Trust Relation

Select Priority to Trust: DSCP

Eth-Trunk Interfaces:
Eth-Trunk0
Eth-Trunk2
Eth-Trunk3
Eth-Trunk19

Added Eth-Trunk Interfaces:

Table 7-14 describes the parameters on the page.

Table 7-14 Add Trust Relation

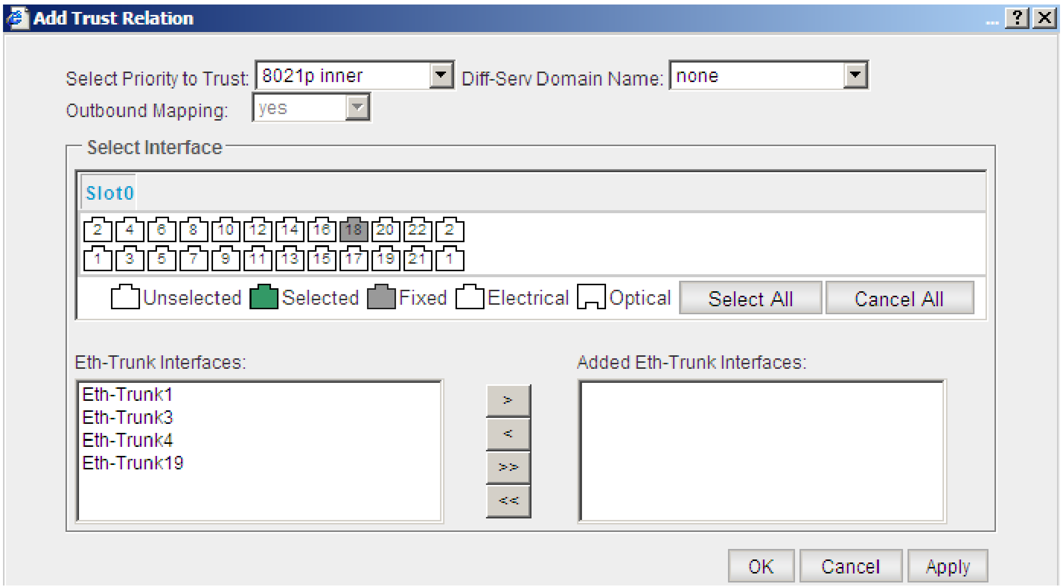
Parameter	Description
Select Interface	Indicates the interface that you want to configure. You can select multiple interfaces.
Select Priority to Trust	Indicates the type of a trusted priority, including: ● DSCP ● IP-Preference ● 8021P

3. Set parameters.
4. Click **OK**.

- This function is only supported by S6700 series switches.

1. Choose **QoS** > **Priority Mapping** > **Trust Priority** to open the **Trust Priority** page.
2. Click **New** to open the **Add Trust Relation** page, as shown in **Figure 7-17**.

Figure 7-17 Add Trust Relation



Add Trust Relation

Select Priority to Trust: 8021p inner
Diff-Serv Domain Name: none
Outbound Mapping: yes

Select Interface

Eth-Trunk Interfaces:
Eth-Trunk1
Eth-Trunk3
Eth-Trunk4
Eth-Trunk19

Added Eth-Trunk Interfaces:

Table 7-15 describes the parameters on the page.

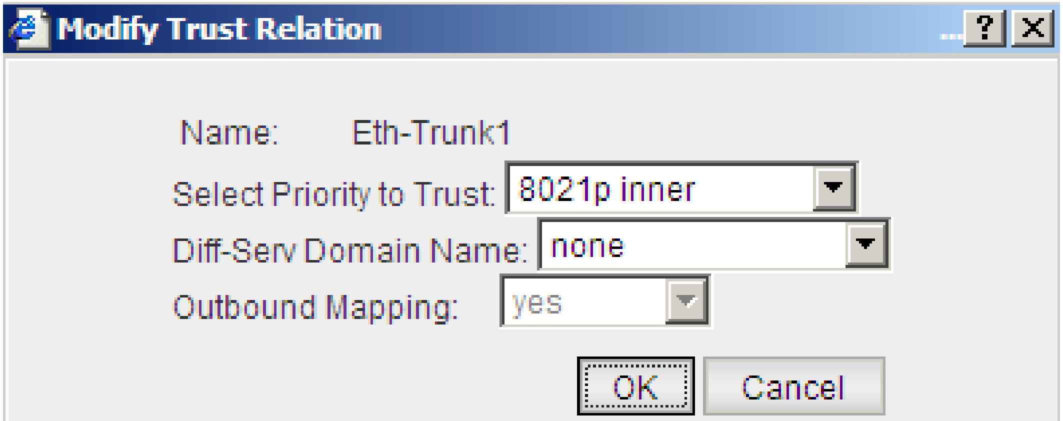
Table 7-15 Add Trust Relation

Parameter	Description
Select Priority to Trust	Indicates the type of a trusted priority, including: ● 8021P inner ● 8021P outer ● DSCP
Diff-Serv Domain Name	Indicates the name of the Diff-Serv domain.
Outbound Mapping	Indicates the type of a trusted priority, including: ● yes ● no
Select Interface	Indicates the interface that you want to configure. You can select multiple interfaces.

3. Set parameters.
4. Click **OK**.

- This function is only supported by S6700 series switches.
  1. Choose **QoS** > **Priority Mapping** > **Trust Priority** to open the **Trust Priority** page.
  2. Select a record that you want to modify and click 📝 to open the **Modify Trust Relation** page, as shown in **Figure 7-18**.

Figure 7-18 Modify Trust Relation



Name: Eth-Trunk1

Select Priority to Trust: 8021p inner

Diff-Serv Domain Name: none

Outbound Mapping: yes

Table 7-16 describes the parameters on the page.

Table 7-16 Modify Trust Relation

Parameter	Description
Name	You cannot modify this parameter.

Parameter	Description
Select Priority to Trust	Indicates the type of a trusted priority, including: ● 8021P inner ● 8021P outer ● DSCP
Diff-Serv Domain Name	Indicates the name of the Diff-Serv domain.
Outbound Mapping	Indicates the type of a trusted priority, including: ● yes ● no

3. Click **OK**.

- Delete a trusted priority.
  1. Choose **QoSPriority MappingTrust Priority** to open the **Trust Priority** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches,click the check boxes of records.
  3. Click **OK**.

----End

8 IP Routing

About This Chapter

This document describes the configurations of IP routing.

Routers are used to select routes for packets on the Internet. A router selects a proper route for a received packet according to the destination address and sends the packet to the next hop router. The last-hop router on the route sends the packet to the destination host.

8.1 IPv4 Route
The following sections describe the basic knowledge and configuration methods of IPv4 routing tables, IPv4 static routes, and global parameters.

8.1 IPv4 Route

The following sections describe the basic knowledge and configuration methods of IPv4 routing tables, IPv4 static routes, and global parameters.

8.1.1 IPv4 Routing Tables

A router forwards packets by using a routing table. Each router saves a routing table. Each entry in the routing table contains a physical interface of the router, and the router sends packets to the physical interfaces.

Context

You can query information about all routing tables through the Web system, including information about dynamic and static routing tables.

Procedure

Step 1 Choose **IP Routing** > **IPv4 Route** > **IPv4 Routing Tables** in the navigation tree to open the **IPv4 Routing Tables** page.

Step 2 Set the search criteria.

Step 3 Click **Query** to display all matching records.

----End

8.1.2 IPv4 Static Route

Static routes are manually configured by network administrators. After static routes are configured, networks can communicate through these routes. However, the static routes cannot be automatically updated when one network fails. In this case, only administrators can update them.

Context

It is recommended that you specify the next hop address when configuring a static route on the switch. You need to specify the next hop; otherwise, the next hop cannot be determined because most physical interfaces of the switch are Ethernet interfaces of the broadcast type and one outbound interface can be associated with multiple next hop addresses. If the outbound interface is specified, you must specify the next hop address of the interface.

Procedure

- Create an IPv4 static route.
  1. Choose **IP Routing** > **IPv4 Route** > **IPv4 Static Route** in the navigation tree to open the **IPv4 Static Route** page.
  2. Click **New** to open the **Create an IPv4 Static Route** page, as shown in **Figure 8-1**.

Figure 8-1 Create an IPv4 Static Route

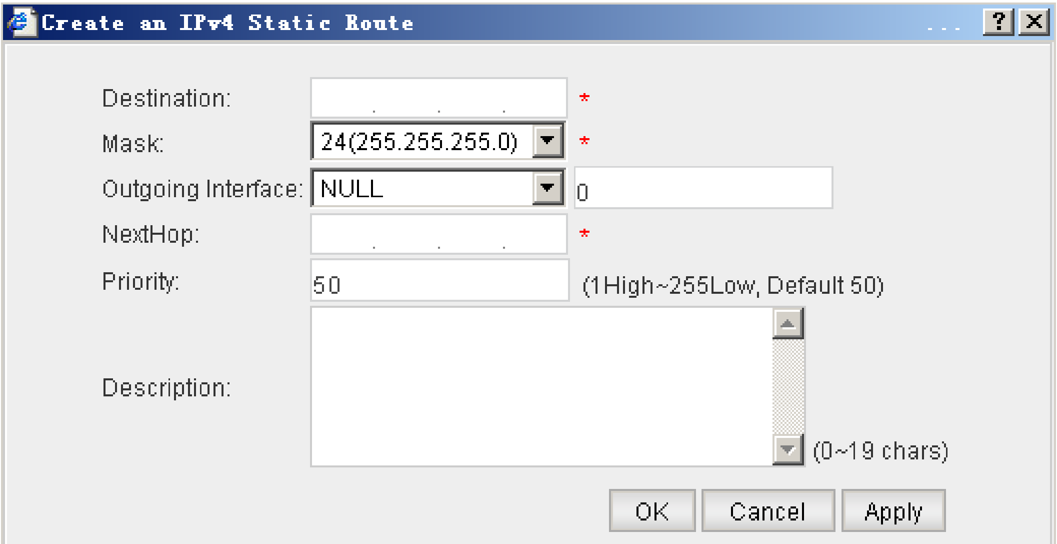


Table 8-1 describes the parameters on the **Create an IPv4 Static Route** page.

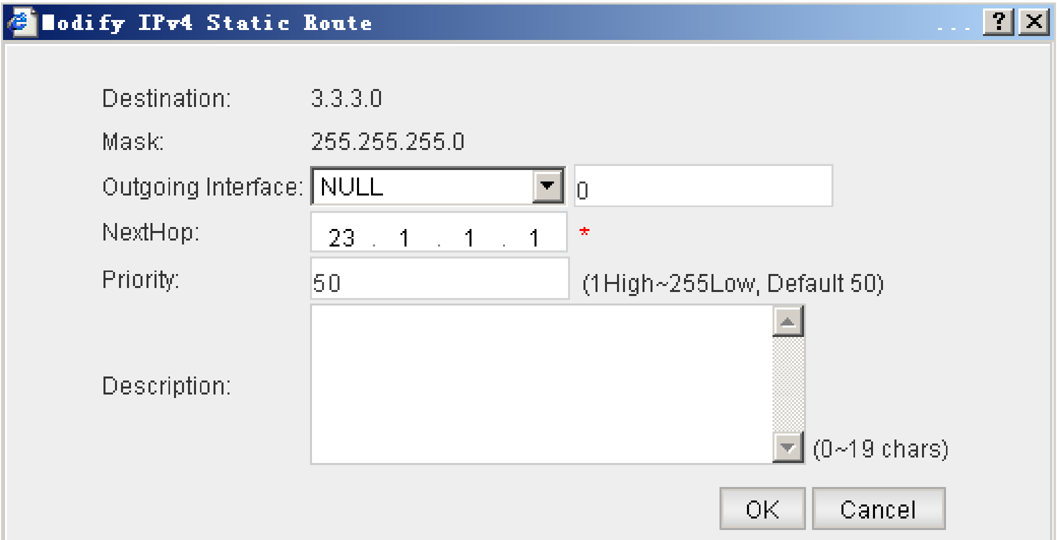
Table 8-1 Create an IPv4 Static Route

Parameter	Description
Destination	Indicates the destination IP address or the destination network address of an IP packet, for example, **10.10.10.1**. This parameter is mandatory.
Mask	Indicates the network mask that is used with the destination address to identify the address of the network segment where the destination host or router resides. The address of the network segment where the destination host or router resides can be calculated according to the AND operation on the destination address and network mask, for example, **255.255.0.0**. This parameter is mandatory.
Outgoing Interface	Indicates the interface on a router from which IP packets are forwarded, for example, **Vlanif1**.
NextHop	Indicates the next-hop router address that IP packets pass through, for example, **10.10.10.2**. This parameter is mandatory
Priority	Indicates the priority of a route. Packets may reach the same destination address through multiple routes. These routes may be discovered by different routing protocols, or statically configured. The route with the highest priority (smallest value) is selected as the optimal route. This parameter is optional.
Description	Indicates the description of an IPv4 static route. This parameter is optional.

3. Set parameters.
4. Click **OK**.

- Modify an IPv4 static route.
  1. Choose **IP Routing** > **IPv4 Route** > **IPv4 Static Route** in the navigation tree to open the **IPv4 Static Route** page.
  2. Click ✎ to open the **Modify IPv4 Static Route** page, as shown in **Figure 8-2**.

Figure 8-2 Modify IPv4 Static Route



Modify IPv4 Static Route

Destination: 3.3.3.0
Mask: 255.255.255.0
Outgoing Interface: NULL 0
NextHop: 23 . 1 . 1 . 1 *
Priority: 50 (1High~255Low, Default 50)
Description: (0~19 chars)

NOTE

- **Table 8-1** describes the parameters on the **Modify IPv4 Static Route** page.
- The destination IP address and subnet mask cannot be changed.

  3. Set parameters.
  4. Click **OK**.

- Delete an IPv4 static route.
  1. Choose **IP Routing** > **IPv4 Route** > **IPv4 Static Route** in the navigation tree to open the **IPv4 Static Route** page.
  2. Select a record that you want to delete and click **Delete**.

NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

  3. Click **OK**.

----End

8.1.3 Global Parameter Settings

You can set and query global parameters of an IPv4 static route.

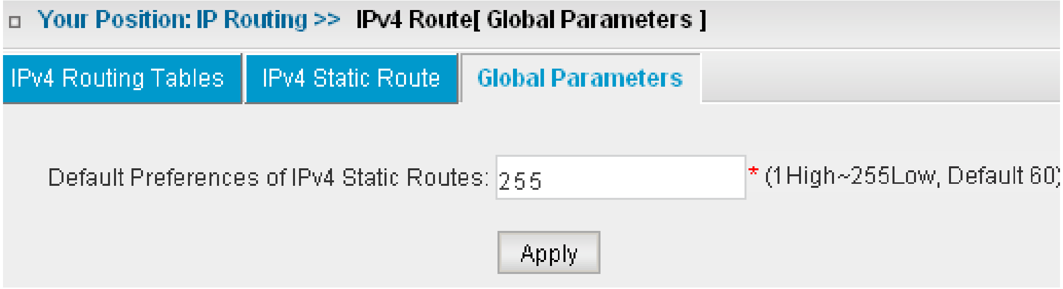
Context

By default, the priority of an IPv4 static route is 60. If the priority of an IPv4 static route is not specified, the default priority is used. If you change the default priority, the new default priority is valid for only new IPv4 static routes.

Procedure

Step 1 Choose **IP Routing** > **IPv4 Route** > **Global Parameter Settings** in the navigation tree to open the **Global Parameter Settings** page, as shown in **Figure 8-3**.

Figure 8-3 Global Parameters



Your Position: IP Routing >> IPv4 Route[Global Parameters]

Default Preferences of IPv4 Static Routes: 255 * (1 High~255Low, Default 60)

Table 8-2 describes the parameters on the **Global Parameter Settings** page.

Table 8-2 Global Parameter Settings

Parameter	Description
Default Preferences of IPv4 Static Routes	Indicates the default priority of an IPv4 static route. The value ranges from 1 to 255. The value 1 indicates the highest priority and the value 255 indicates the lowest priority. The default value is 60. This parameter is mandatory.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

9 Security

About This Chapter

This chapter describes concepts and configurations of security management, including port isolation, static user binding, AAA, 802.1x authentication, and MAC address authentication.

9.1 Port Isolation
You can configure and query the port isolation mode, bidirectional isolation, and unidirectional isolation. **The S2700SI series switches do not support this function.**

9.2 Static User Binding
Static user binding is configured manually and supports binding methods of IP+port, MAC+port, IP+MAC+port, IP+port+VLAN, MAC+port+VLAN, and IP+MAC+port+VLAN. **The S2700SI series switches do not support this function.**

9.3 AAA
Authentication, Authorization, and Accounting (AAA) is used to manage network security. **The AAA configuration function is equivalent to the user management function of S2700SI and S2700EI.**

9.4 802.1x
You can configure 802.1x parameters globally or on an interface. **The S2700SI or S2700EI series switches do not support the function.**

9.5 MAC Authen
You can configure MAC address authentication globally or on an interface. **The S2700SI or S2700EI series switches do not support the function.**

Copyright © Huawei Technologies Co., Ltd.

9.1 Port Isolation

You can configure and query the port isolation mode, bidirectional isolation, and unidirectional isolation. **The S2700SI series switches do not support this function.**

If you want to prevent members in a group from communicating with each other but allow them to access the public devices, such as the printer and the server, you can set the port isolation mode to isolation at both Layer 2 and Layer 3 or Layer 2 isolation and Layer 3 communication.

9.1.1 Bidirectional Isolation

You can create, query, modify, or delete an isolation mode or a bidirectional isolation configuration.

Context

- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate.
- The switch supports 64 VLANs from VLAN 1 to VLAN 64.

Procedure

- Configure an isolation mode.

  NOTE

  - The default mode is L2, namely, ports are isolated at Layer 2 but can communicate at Layer 3.
  - After the isolation mode is selected, the bidirectional isolation and unidirectional isolation configurations are applied to this mode.
  - Configuring the isolation mode is not affected by switching the bidirectional isolation and unidirectional isolation labels.
  - The S2700 switches do not support the function.

  1. Choose **Security** > **Port isolation** in the navigation tree to open the **Port isolation** page.
  2. Choose the isolation mode. The isolation can be L2 or ALL. L2 is Layer 2 isolation and Layer 3 communication. ALL is the isolation at both Layer 2 and Layer 3.
  3. Click **Apply**.

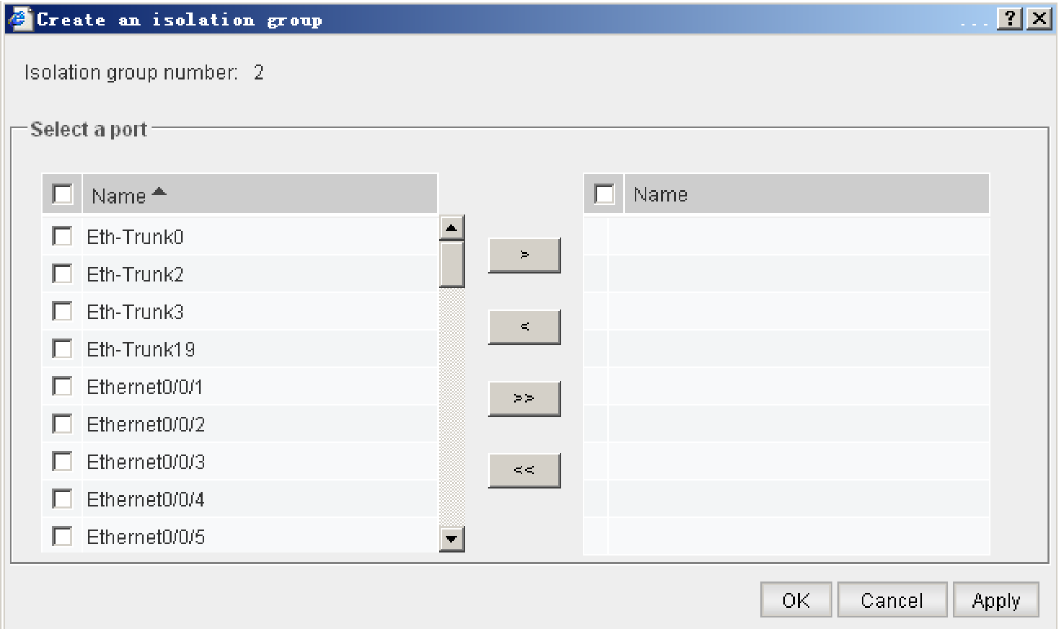
- Query an isolation group.

  1. Choose **Security** > **Port isolation** > **Bidirectional isolation** in the navigation tree to open the **Bidirectional isolation** page.
  2. Enter a number in the text box of isolation group number.
  3. Click **Query** to display all matching records.

- Create an isolation group.

  1. Choose **Security** > **Port isolation** > **Bidirectional isolation** in the navigation tree to open the **Bidirectional isolation** page.
  2. Click **New** to open the **Create an isolation group** page, as shown in **Figure 9-1**.

Figure 9-1 Create an isolation group



Create an isolation group

Isolation group number: 2

Table 9-1 describes the parameters on the page.

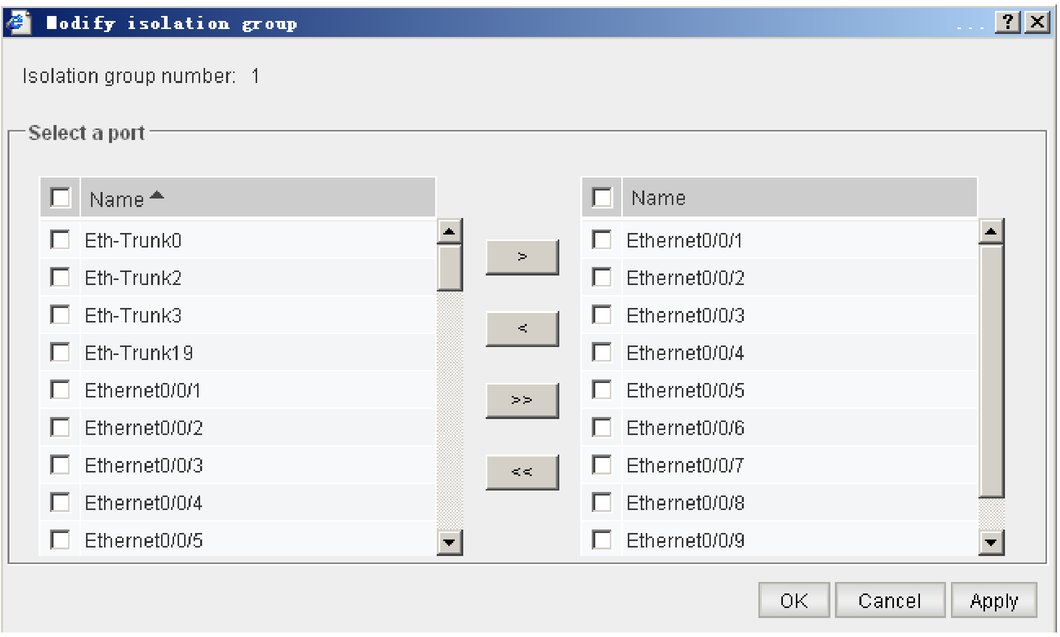
Table 9-1 Create an isolation group

Parameter	Description
Isolation group number	Indicates the value that the system generates automatically. The value ranges from 1 to 64. When creating an isolation group, the system assigns the minimum in existing numbers to the new isolation group.
Port list	Select the interface that you want to add to the isolation group on the port list on the left. Click > to display the new interface on the right list.

3. Select an interface.
4. Click **OK**.

- Modify an isolation group.
  1. Choose **Security** > **Port isolation** > **Bidirectional isolation** in the navigation tree to open the **Bidirectional isolation** page.
  2. Click the corresponding ✎ icon to open the **Modify isolation group** page, as shown in **Figure 9-2**.

Figure 9-2 Modify isolation group



Isolation group number: 1

Select a port

□	Name ▲
□	Eth-Trunk0
□	Eth-Trunk2
□	Eth-Trunk3
□	Eth-Trunk19
□	Ethernet0/0/1
□	Ethernet0/0/2
□	Ethernet0/0/3
□	Ethernet0/0/4
□	Ethernet0/0/5

□	Name
□	Ethernet0/0/1
□	Ethernet0/0/2
□	Ethernet0/0/3
□	Ethernet0/0/4
□	Ethernet0/0/5
□	Ethernet0/0/6
□	Ethernet0/0/7
□	Ethernet0/0/8
□	Ethernet0/0/9

Table 9-1 describes the parameters on the page.

3. Select an interface.
4. Click **OK**.

- Delete an isolation group.
  1. Choose **Security** > **Port isolation** > **Bidirectional isolation** in the navigation tree to open the **Bidirectional isolation** page.
  2. Select the isolation group that you want to delete. You can delete an isolation group or multiple isolation groups.
  3. Click **Delete**. The system asks you whether to delete the record.
  4. Click **OK** on the dialog box.

----End

9.1.2 Unidirectional Isolation

You can create, query, modify, and clear a unidirectional port isolation configuration.

Context

You can configure or delete the unidirectional isolation between the current interface and a specified interface. If interface A is isolated from interface B, packets sent from interface A cannot reach interface B, but packets sent from interface B can reach interface A.

NOTE

E interfaces, GE interfaces, XGE interfaces, and Eth-Trunk interfaces can be isolated from one another. But an interface cannot be isolated from itself or from the management interface unidirectionally. In addition, an Eth-Trunk cannot be isolated unidirectionally from its member interfaces.

Procedure

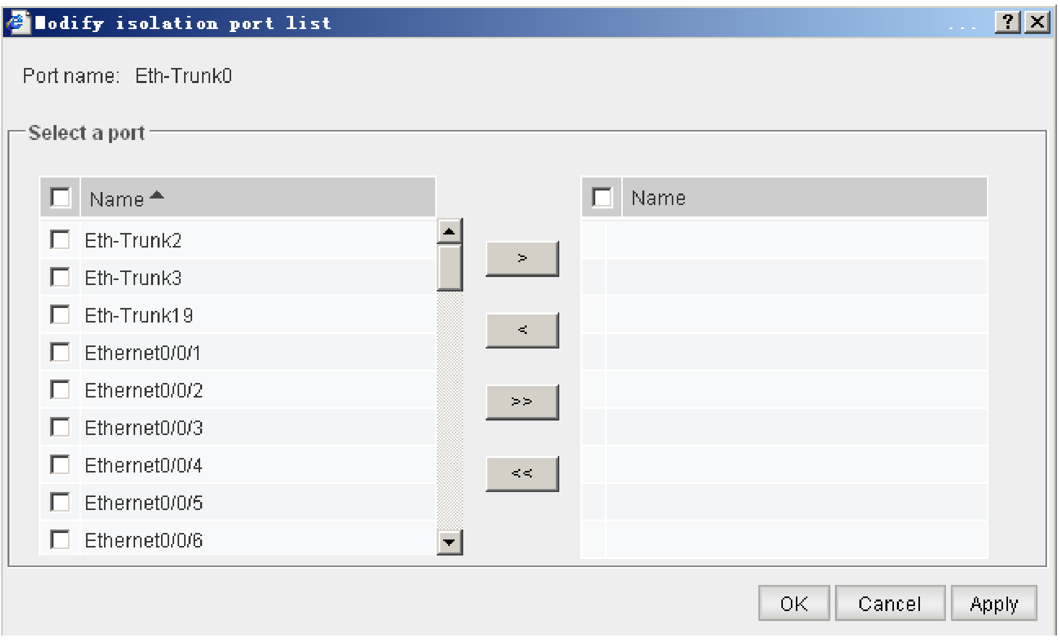
- Query a unidirectional isolation.
  1. Choose **Security** > **Port isolation** > **Unidirectional isolation** in the navigation tree to open the **Unidirectional isolation** page.
  2. Select an interface type from the drop-down list box.
  3. Enter the interface number, for example, **0/0/1 (stack ID/subcard ID/interface number)**.
  4. Click **Query** to display all matching records.
- Configure a unidirectional port isolation.

  NOTE

  You can configure and modify unidirectional isolation in the same method.

  1. Choose **Security** > **Port isolation** > **Unidirectional isolation** in the navigation tree to open the **Unidirectional isolation** page.
  2. Click the corresponding 📝 icon to open the **Modify isolation port list** page, as shown in **Figure 9-3**.

Figure 9-3 Modify isolation port list



Port name: Eth-Trunk0

Select a port

□	Name
□	Eth-Trunk2
□	Eth-Trunk3
□	Eth-Trunk19
□	Ethernet0/0/1
□	Ethernet0/0/2
□	Ethernet0/0/3
□	Ethernet0/0/4
□	Ethernet0/0/5
□	Ethernet0/0/6

□	Name

Table 9-2 describes the parameters on the page.

Table 9-2 Modify isolation port list

Parameter	Description
Port name	Indicates the name of the interface where you want to modify the configuration. This parameter cannot be modified.

Parameter	Description
Select the interface	Select the interface that you want to add to the isolation group on the port list on the left. Click > to display the new interface on the right list.

3. Select an interface.
4. Click **OK**.

- Clear a unidirectional isolation.
  1. Choose **Security** > **Port isolation** > **Unidirectional isolation** in the navigation tree to open the **Unidirectional isolation** page.
  2. Select the interface configured with unidirectional isolation that you want to delete. You can delete an interface or multiple interfaces.
  3. Click **Clear**. The system asks you whether to delete the record.
  4. Click **OK** on the dialog box.

----End

9.2 Static User Binding

Static user binding is configured manually and supports binding methods of IP+port, MAC+port, IP+MAC+port, IP+port+VLAN, MAC+port+VLAN, and IP+MAC+port+VLAN. **The S2700SI series switches do not support this function.**

9.2.1 View Static User Binding

You can view static user bindings on the **Static user binding** page. You can query information according to the search criteria.

Context

The switch supports the static bindings of IP+port, MAC+port, IP+MAC+port, IP+port+VLAN, MAC+port+VLAN, and IP+MAC+port+VLAN.

Procedure

Step 1 Choose **Security** > **Static user binding** in the navigation tree to open the **Static user binding** page, as shown in **Figure 9-4**.

Figure 9-4 Static user binding

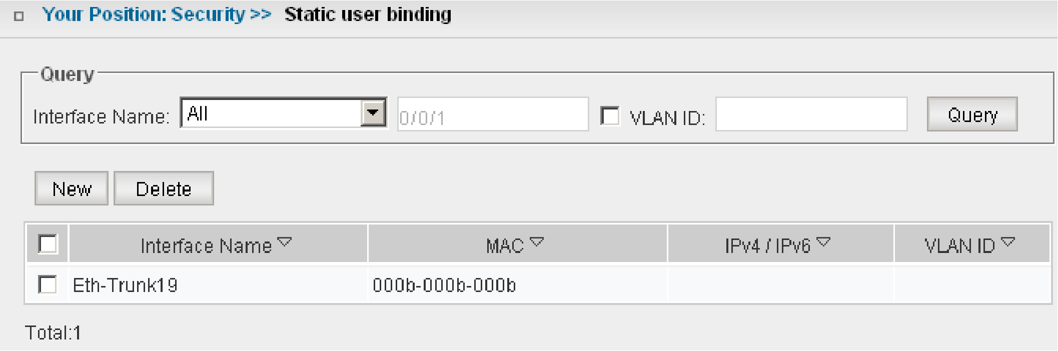


Table 9-3 describes the parameters on the page.

Table 9-3 Search criteria for static user binding

Parameter	Description
Interface Name	Indicates the interface type and name that you want to query.
VLAN ID	● If the check box of VLAN is not selected and the VLAN ID text box is not available, all VLANs are queried. ● When the check box of VLAN is selected, you can enter the VLAN ID that you want to query.

Step 2 Set the search criteria.

Step 3 Click **Query** Search results are displayed.

----End

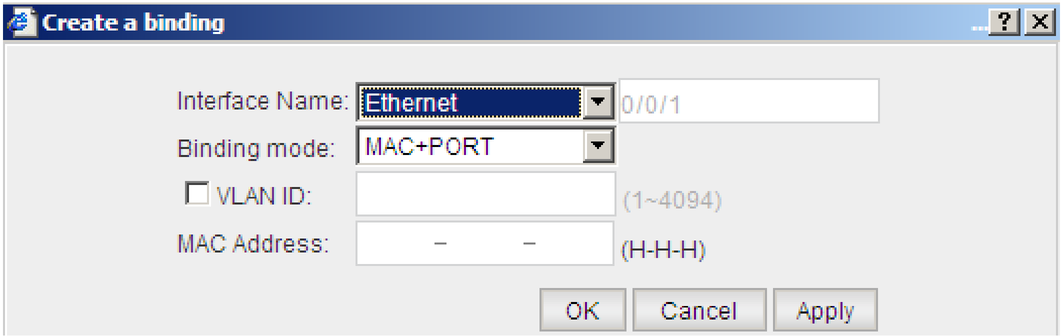
9.2.2 Configure Static User Binding

You can configure static user binding.

Procedure

- Create a binding.
  1. Choose **Security** > **Static user binding** in the navigation tree to open the **Static user binding** page.
  2. Click **New** to open the **Create a binding** page, as shown in **Figure 9-5**.

Figure 9-5 Create a binding



Create a binding

Interface Name: Ethernet 0/0/1

Binding mode: MAC+PORT

□ VLAN ID: (1~4094)

MAC Address: - - (H-H-H)

Table 9-4 describes the parameters on the page.

Table 9-4 Create a binding

Parameter	Description
Interface Name	Indicates the type and name of the interface that you want to bind. ● Interface types include **Ethernet**, **GigabitEthernet**, **XGigabitEthernet**, and **Eth-Trunk**. ● The interface type and name are mandatory.
Binding mode	The binding modes in the drop-down list box include: ● MAC+port ● IP+port ● IP+MAC+port Select one binding mode from the modes above. This parameter is mandatory.
VLAN ID	● If the check box of VLAN is not selected and the VLAN ID text box is not available, the VLAN is not bound. ● If the check box of VLAN is selected, VLAN is bound. This parameter is mandatory.
Binding Information	● If you select MAC+port, the binding information is displayed in the text box of the MAC address. ● If you select IP+port, the binding information is displayed in the text box of the IPv4/IPv6 address. You can choose the IPv4 or IPv6 address. ● If you select IP+MAC+port, the binding information is displayed in the text boxes of the MAC and IPv4/IPv6 address.

3. Set parameters.
4. Click **OK**.

- Delete a binding.
  1. Choose **Security** > **Static user binding** in the navigation tree to open the **Static user binding** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
     - When you delete IP+port or IP+port+VLAN binding, all binding information about this IP address is deleted.
     - When you delete MAC+port or MAC+port+VLAN binding, all binding information about this MAC address is deleted.
     - When you delete IP+MAC+port binding, all binding information about this IP+MAC is deleted.
     - When you delete IP+MAC+port+VLAN binding, all binding information about this IP +MAC+VLAN is deleted.
  3. Click **OK**.

----End

9.3 AAA

Authentication, Authorization, and Accounting (AAA) is used to manage network security. **The AAA configuration function is equivalent to the user management function of S2700SI and S2700EI.**

Generally, AAA uses the client/server model. In this model, the client runs on the resource side that is managed through AAA, whereas the server collects and keeps all user information. This model features good extensibility and facilitates concentrated management over user information.

9.3.1 AAA Scheme

You can add, modify, and delete an authentication scheme, authorization scheme, or accounting scheme. **The S2700EI and S2700SI switches do not support this function.**

Context

Authentication, authorization, and accounting are three independent service processes.

- In the authentication process, a device authenticates the user name, password, or user information of an access request or a service request. The device, however, neither delivers authorization information to the user nor triggers the accounting process. In AAA, a device can adopt only authentication.
- In the authorization process, a device sends authorization requests to the authorization server. After users pass authorization, the device sends authorization information to users. If the authorization scheme is **none**, users do not need to be authorized. In this case, users passing authentication have the default authority granted by the system.

- In the accounting process, a device sends accounting-start packets, accounting-update packets, or accounting-stop packets to the accounting server. In AAA, an accounting scheme is optional. If you do not configure an accounting scheme.

Procedure

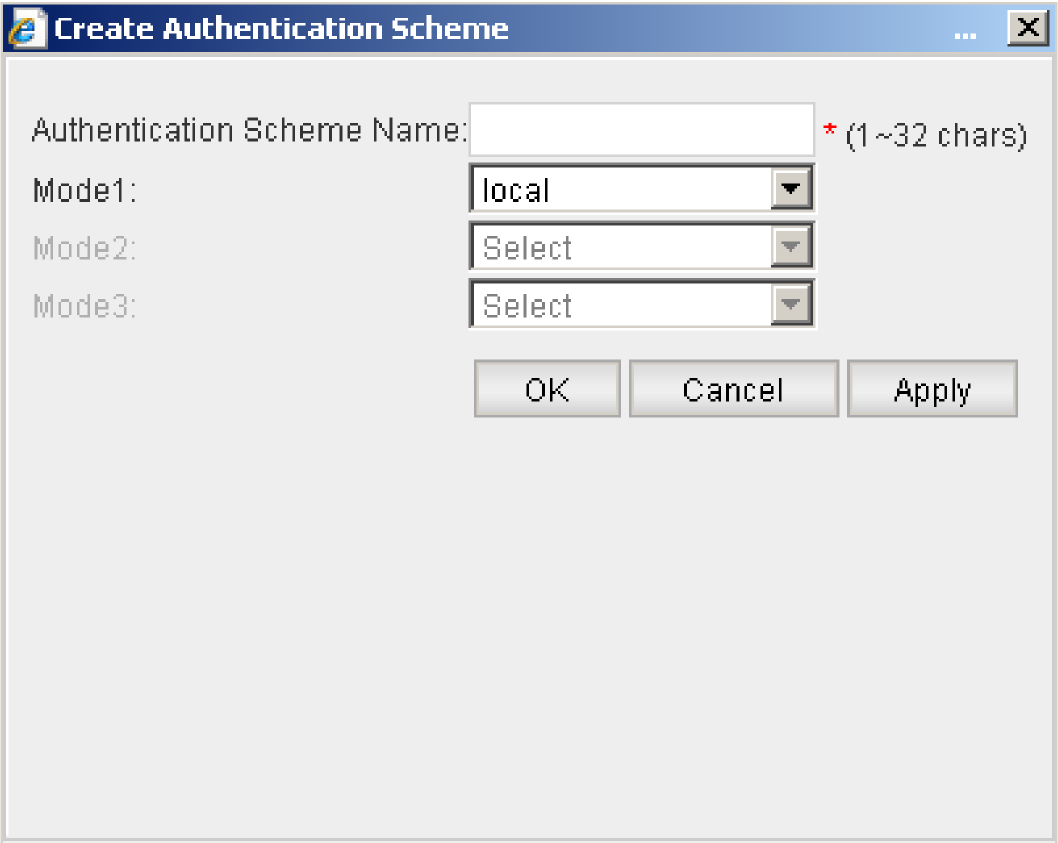
- Create an authentication scheme.

  NOTE

  You can create an authentication scheme, authorization scheme, or accounting scheme. Here the authentication scheme is used as an example.

  1. Choose **Security** > **AAA** > **AAA Scheme** in the navigation tree to open the **AAA Scheme** page.
  2. Click **New** to open the **Create Authentication Scheme** page, as shown in **Figure 9-6**.

Figure 9-6 Create Authentication Scheme



Create Authentication Scheme

Authentication Scheme Name: * (1~32 chars)

Mode1: local

Mode2: Select

Mode3: Select

Table 9-5 describes the parameters on the **Create Authentication Scheme** page.

Table 9-5 Create Authentication Scheme

Item	Description
Authentication Scheme Name	Indicates the name of an authentication scheme.
Authentication Scheme Mode	Indicates the authentication mode. There are four authentication modes for you to select. NOTE ● The options are **none**, **hwtacacs**, **radius**, and **local**. ● You can use the combination of authentication modes. If the authentication mode is **none** or **local**, you cannot configure an authentication scheme.
Authorization Scheme Mode	Indicates the authorization mode. There are four authorization modes for you to select. NOTE ● The options are **none**, **hwtacacs**, **radius**, and **local**. ● You can use the combination of authorization modes. If the authentication mode is **none**, you cannot configure an authorization scheme.
Accounting Scheme Mode	Indicates the accounting mode. There are three accounting modes for you to select. NOTE The options are **none**, **hwtacacs**, **radius**.

3. Set parameters.
4. Click **OK**.

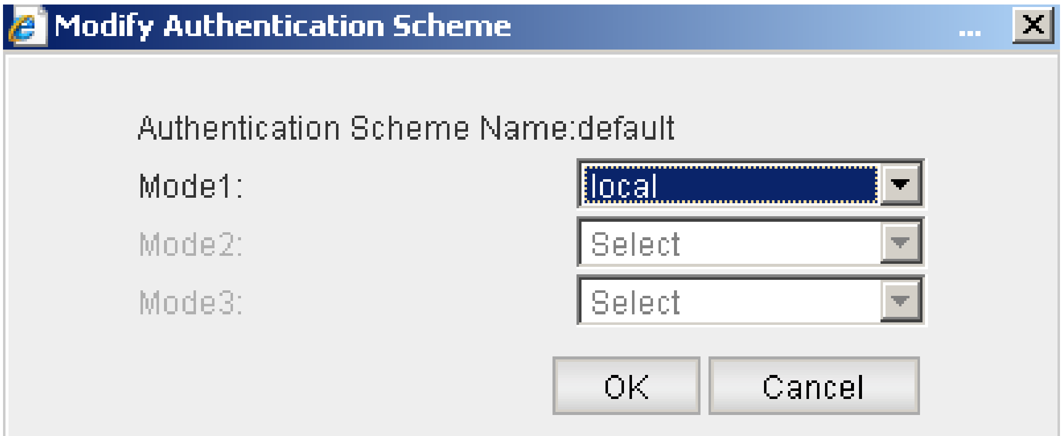
- Modify an authentication scheme.

NOTE

You can modify an authentication scheme, authorization scheme, or accounting scheme. Here the authentication scheme is used as an example.

1. Choose **Security** > **AAA** > **AAA Scheme** in the navigation tree to open the **AAA Scheme** page.
2. Click to open the **Modify Authentication Scheme** page, as shown in **Figure 9-7**.

Figure 9-7 Modify Authentication Scheme



Authentication Scheme Name:default

Mode1: local

Mode2: Select

Mode3: Select

NOTE

- **Table 9-5** describes the parameters on the **Modify Authentication Scheme** page.
- The authentication scheme name cannot be changed.

3. Set the authentication type as required.
4. Click **OK**.

- Delete an authentication scheme.
  1. Choose **Security** > **AAA** > **AAA Scheme** in the navigation tree to open the **AAA Scheme** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

9.3.2 Service Scheme

Access users must obtain authorization information before going online. Authorization information about users can be managed by configuring a service scheme. **The S2700EI or S2700SI series switches do not support this function.**

Context

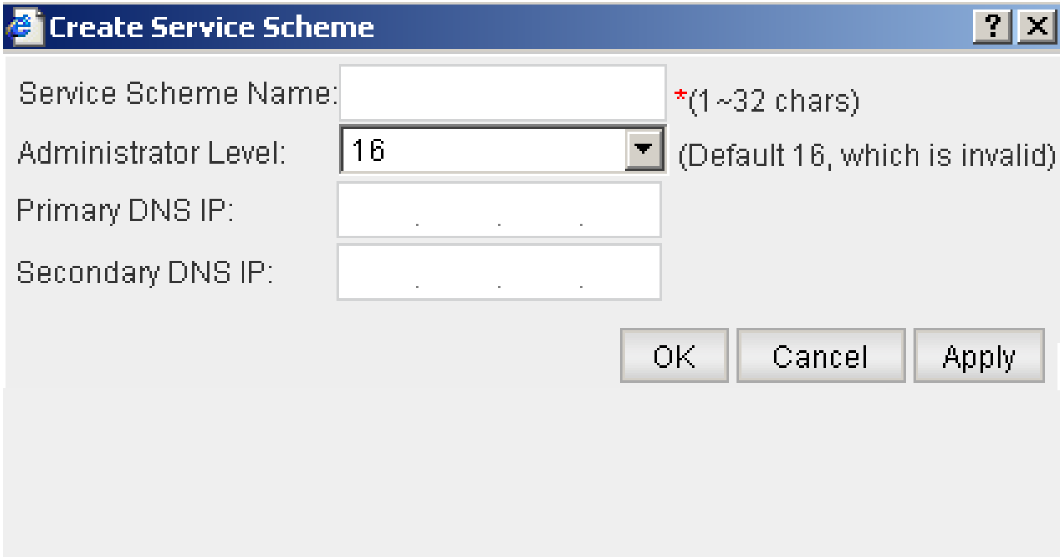
A service scheme is a set of authorization information about users. After a service scheme is created, you can set attributes of users in the service scheme view.

Procedure

- Create a service scheme.
  1. Choose **Security** > **AAA** > **Service Scheme** in the navigation tree to open the **Service Scheme** page.

2. Click **New** to open the **Create Service Scheme** page, as shown in **Figure 9-8**.

Figure 9-8 Create Service Scheme



Create Service Scheme

Service Scheme Name: *(1~32 chars)

Administrator Level: 16 (Default 16, which is invalid)

Primary DNS IP: . . .

Secondary DNS IP: . . .

Table 9-6 describes the parameters on the **Create Service Scheme** page.

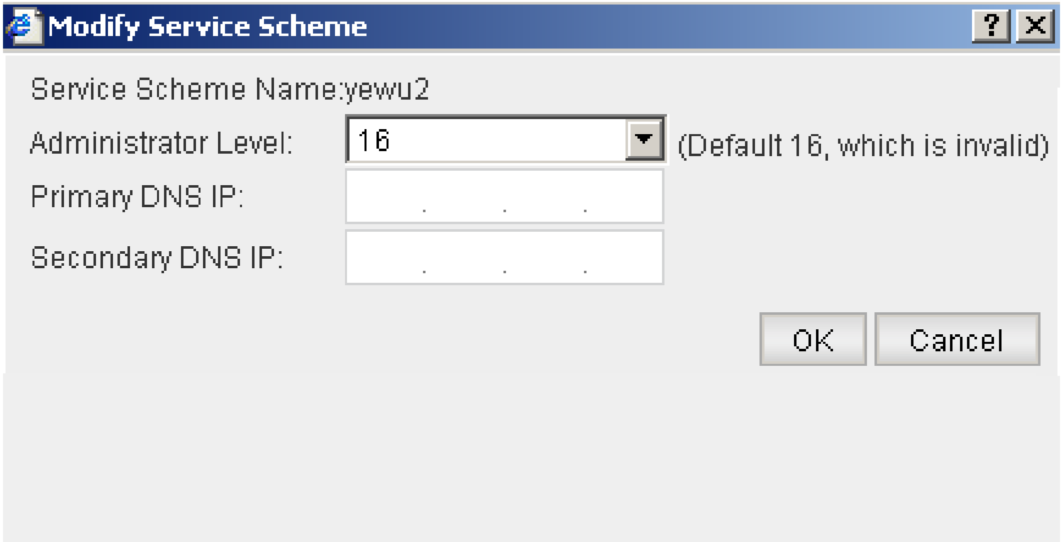
Table 9-6 Create Service Scheme

Parameter	Description
Service Scheme Name	Indicates the name of a new service scheme.
Administrator Level	Indicates the administrator level for a user to log in to the switch.
Primary DNS IP	Indicates the IP address of the primary DNS server, for example, **10.10.10.1**.
Secondary DNS IP	Indicates the IP address of the secondary DNS server, for example, **10.10.10.2**.

3. Set parameters.
4. Click **OK**.

- Modify a service scheme.
  1. Choose **Security** > **AAA** > **Service Scheme** in the navigation tree to open the **Service Scheme** page.
  2. Click 📝 to open the **Modify Service Scheme** page, as shown in **Figure 9-9**.

Figure 9-9 Modify Service Scheme



Modify Service Scheme

Service Scheme Name:yewu2

Administrator Level: 16 (Default 16, which is invalid)

Primary DNS IP: . . .

Secondary DNS IP: . . .

NOTE

- **Table 9-6** describes the parameters on the **Modify Service Scheme** page.
- The service scheme name cannot be modified.

3. Set parameters.
4. Click **OK**.

- Delete a service scheme.
  1. Choose **Security** > **AAA** > **Service Scheme** in the navigation tree to open the **Service Scheme** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

9.3.3 RADIUS Configurations

You can create, modify, and delete the RADIUS server template, authentication/accounting server, and authorization server. Before configuring a RADIUS authentication/ accounting server, you must create a RADIUS server template. A RADIUS server builds a unique database to store user names and passwords for authentication and accounting. The RADIUS authorization server receives authorization information sent by users and sends authorization information to users after users pass authorization. **The S2700SI and S2700EI switches do not support this function.**

Context

When a user logs in to a network device such as a switch or a network access server (NAS), the user name and password are sent to the NAS. After the RADIUS client (an NAS server) on the network receives the user name and password, it sends an authentication request to the RADIUS server. If the request is valid, the RADIUS server completes authentication and sends the required authorization information to the RADIUS client. If the request is invalid, the RADIUS server sends the authorization failure information to the RADIUS client.

NOTE

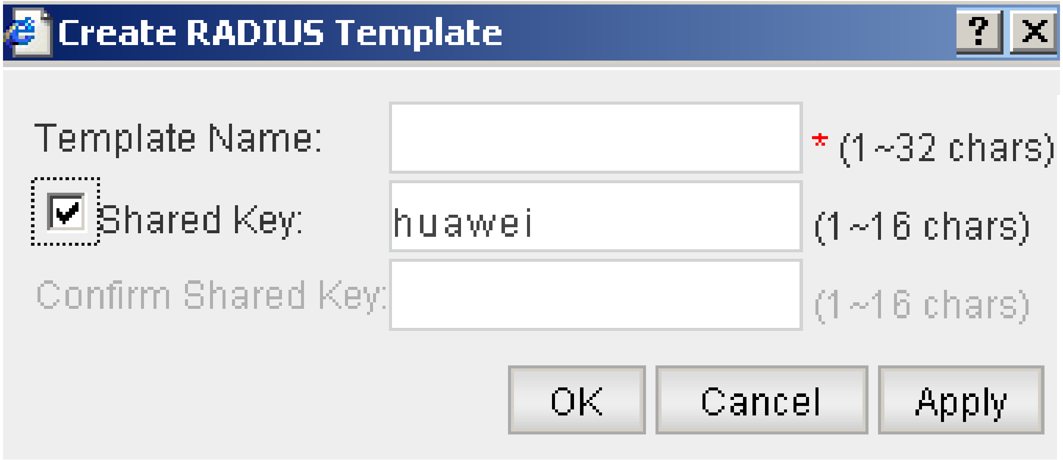
> Most RADIUS configurations have default values. You can perform configurations according to networking requirements. You can modify the RADIUS configuration only when the RADIUS server template is not in use.

The RADIUS authorization server is mainly used to authorize users when users select services dynamically.

Procedure

- Create a RADIUS server template.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Click **New** to open the **Create RADIUS Template** page, as shown in **Figure 9-10**.

Figure 9-10 Create RADIUS Template



Create RADIUS Template

Template Name: * (1~32 chars)

☑ Shared Key: huawei (1~16 chars)

Confirm Shared Key: (1~16 chars)

Table 9-7 describes the parameters on the page.

Table 9-7 Create a RADIUS Server Template

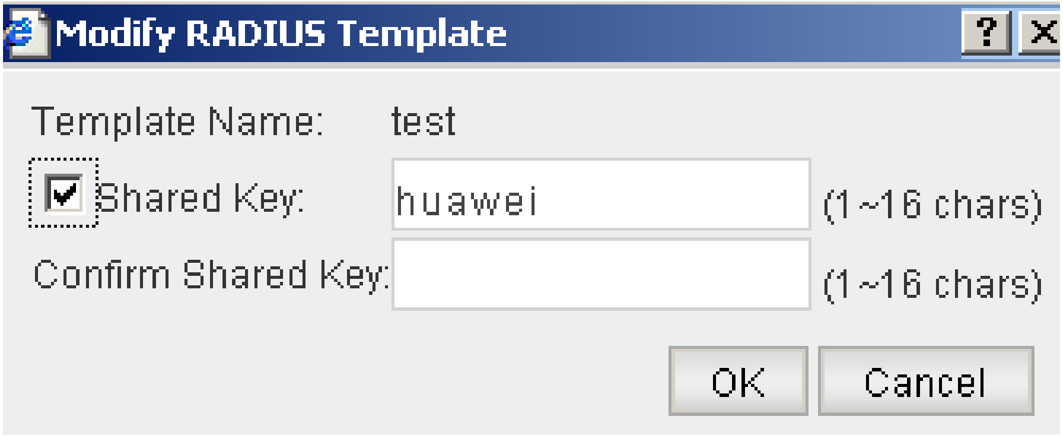
Parameter	Description
Template Name	Indicates the name of a new RADIUS server template.

Parameter	Description
Shared Key	When sending authentication packets, the switch and the RADIUS server encrypt important data such as the password to ensure the security of data transmission over the network. To ensure the validity of the authenticator and the authenticated end, the switch and the RADIUS server must be configured with the same key. The value is a string without spaces. By default, the shared key of a RADIUS server is huawei.
Confirm Shared Key	Indicates the confirmed shared key. The format is the same as that of the shared key.

3. Set parameters.
4. Click **OK**.

- Modify a RADIUS server template.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Click 📝 to open the **Modify RADIUS Template** page, as shown in **Figure 9-11**.

Figure 9-11 Modify RADIUS Template



Modify RADIUS Template

Template Name: test

☑ Shared Key: huawei (1~16 chars)

Confirm Shared Key: (1~16 chars)

NOTE

- **Table 9-7** describes the parameters on the page.
- The template name cannot be modified.

  3. Set parameters.
  4. Click **OK**.

- Delete a RADIUS server template.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

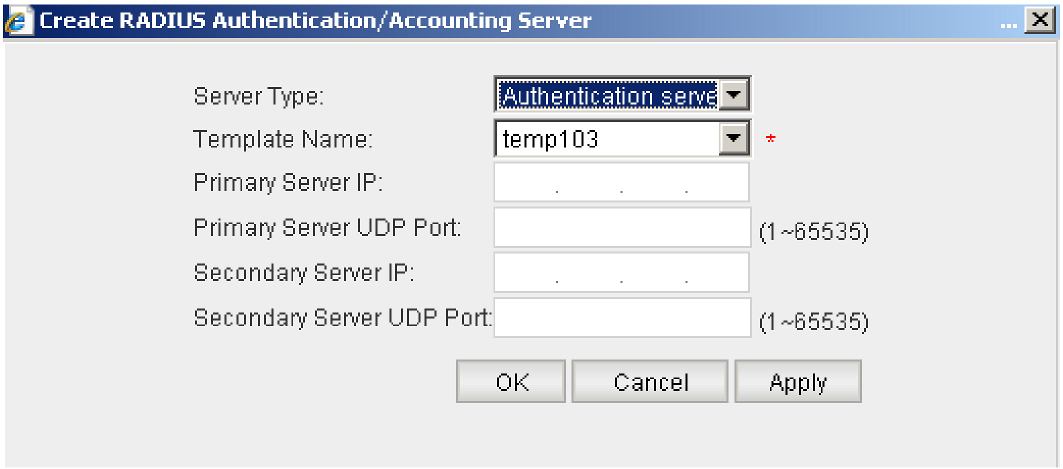
NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

3. Click **OK**.

- Create a RADIUS authentication/accounting server.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Click **New** to open the **Create RADIUS Authentication/Accounting Server** page, as shown in **Figure 9-12**.

Figure 9-12 Create RADIUS Authentication/Accounting Server



Create RADIUS Authentication/Accounting Server

Server Type: Authentication serve

Template Name: temp103 *

Primary Server IP: . . .

Primary Server UDP Port: (1~65535)

Secondary Server IP: . . .

Secondary Server UDP Port: (1~65535)

Table 9-8 describes the parameters on the page.

Table 9-8 Create RADIUS Authentication/Accounting Server

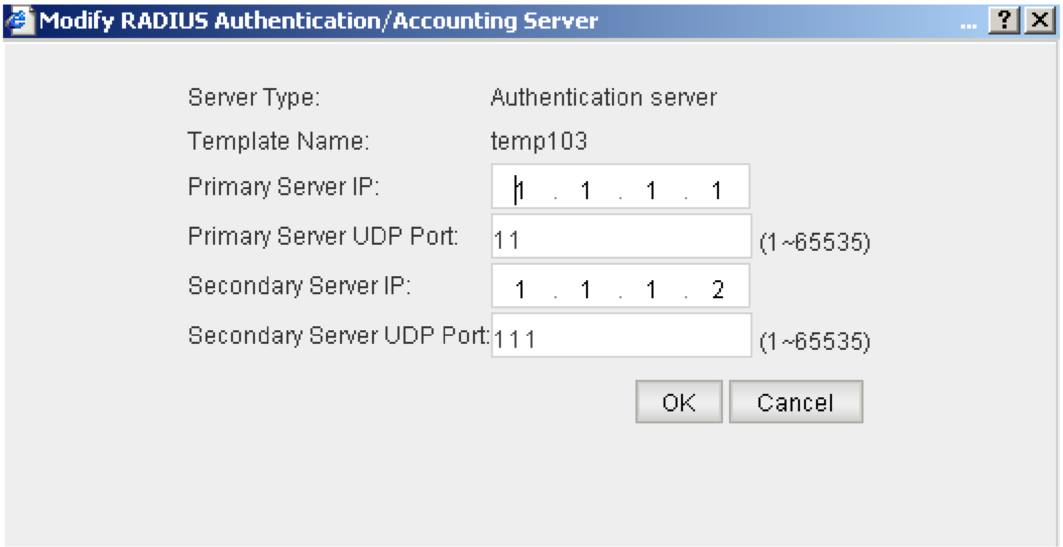
Parameter	Description
Server Type	Indicates the server type.
Template Name	Indicates the RADIUS server template name. This parameter is mandatory.
Primary Server IP	Indicates the IP address of the primary server, for example, **10.10.10.1**. NOTE ● The IP address of the primary authentication/accounting server must be different from that of the secondary authentication/accounting server; otherwise, the system displays a message indicating that the configuration fails. ● **Primary Server IP** and **Secondary Server IP** cannot be empty at the same time.
Primary Server UDP Port	Indicates the UDP port number of the primary server.

Parameter	Description
Secondary Server IP	Indicates the IP address of the secondary server, for example, **10.10.10.2**. NOTE ● The IP address of the primary authentication/accounting server must be different from that of the secondary authentication/ accounting server; otherwise, the system displays a message indicating that the configuration fails. ● **Primary Server IP** and **Secondary Server IP** cannot be empty at the same time.
Secondary Server UDP Port	Indicates the UDP port number of the secondary server.

3. Set parameters.
4. Click **OK**.

- Modify a RADIUS authentication/accounting server.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Click 📝 to open the **Modify RADIUS Authentication/Accounting Server** page, as shown in **Figure 9-13**.

Figure 9-13 Modify RADIUS Authentication/Accounting Server



Server Type: Authentication server
Template Name: temp103
Primary Server IP: 1 . 1 . 1 . 1
Primary Server UDP Port: 11 (1~65535)
Secondary Server IP: 1 . 1 . 1 . 2
Secondary Server UDP Port: 111 (1~65535)

NOTE

Table 9-8 describes the parameters on the page.

  3. Set parameters.
  4. Click **OK**.

- Delete a RADIUS authentication/accounting server.

1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

   NOTE

   - To select a record, click the check box of the record.
   - To delete records in batches, click the check boxes of the records.
3. Click **OK**.

- Create a RADIUS authorization server.

1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
2. Click **New** to open the **Create RADIUS Authorization Server** page, as shown in **Figure 9-14**.

Figure 9-14 Create RADIUS Authorization Server

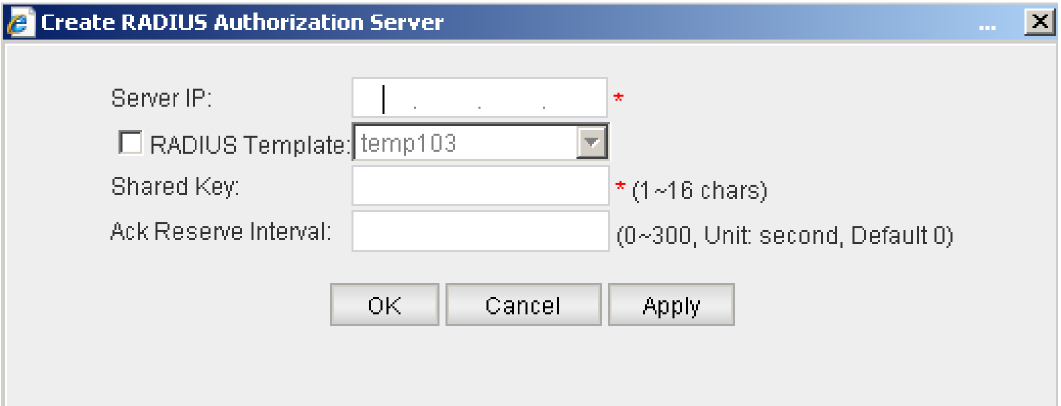


Table 9-9 describes the parameters on the page.

Table 9-9 Create RADIUS Authorization Server

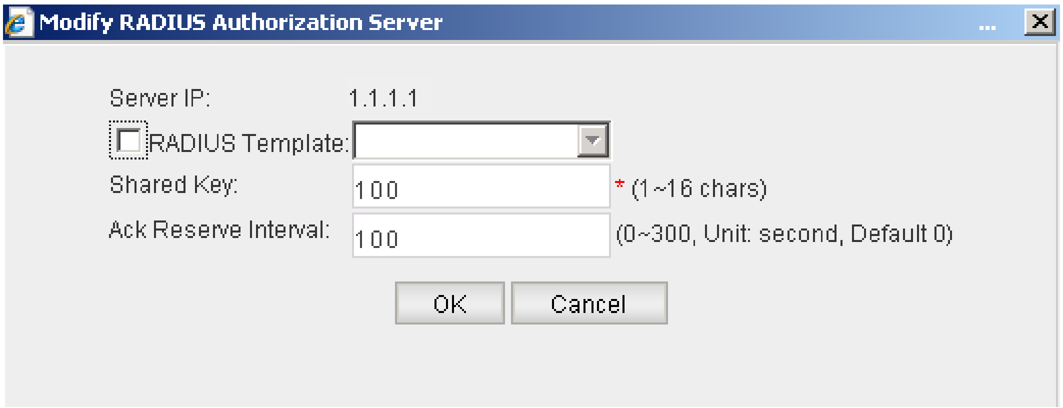
Parameter	Description
Server IP	Indicates the IP address of the authorization server, for example, **10.10.10.1**. This parameter is mandatory.
RADIUS Template	Indicates the RADIUS server template name. This parameter is optional.
Shared Key	To apply the shared key, select the check box of the shared key. This parameter is mandatory. By default, the shared key of a RADIUS server is huawei.
Ack Reserve Interval	Indicates the duration in which an authorization acknowledgment packet is reserved. This parameter is optional.

3. Set parameters.

4. Click **OK**.

- Modify a RADIUS authorization server.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Click ✎ to open the **Modify RADIUS Authorization Server** page, as shown in **Figure 9-15**.

Figure 9-15 Modify RADIUS Authorization Server



Modify RADIUS Authorization Server

Server IP: 1.1.1.1

□ RADIUS Template:

Shared Key: 100 * (1~16 chars)

Ack Reserve Interval: 100 (0~300, Unit: second, Default 0)

NOTE

- **Table 9-9** describes the parameters on the page.
- The IP address of the authorization server cannot be changed.

  3. Set parameters.
  4. Click **OK**.

- Delete a RADIUS authorization server.
  1. Choose **Security** > **AAA** > **RADIUS Config** in the navigation tree to open the **RADIUS Config** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

NOTE

- To select a record, click the check box of the record.
- To delete records in batches, click the check boxes of the records.

  3. Click **OK**.

----End

9.3.4 Domain

The switch manages users based on domains. You can configure the default authorization scheme, RADIUS template, authentication scheme, and accounting scheme in a domain. **The S2700EI and S2700SI series switches do not support this function.**

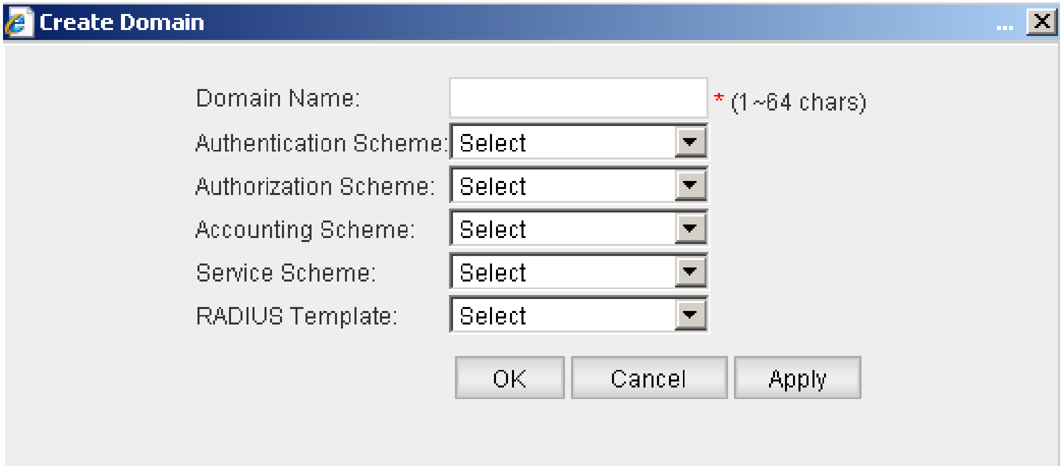
Context

If no AAA schemes are applied to a new domain, the default authentication scheme and accounting scheme are adopted. By default, the new domain is not bound to any authorization scheme.

Procedure

- Create a domain.
  1. Choose **Security** > **AAA** > **Domain** in the navigation tree to open the **Domain** page.
  2. Click **New** to open the **Create Domain** page, as shown in **Figure 9-16**.

Figure 9-16 Create Domain


Create Domain

Domain Name: * (1~64 chars)

Authentication Scheme: Select

Authorization Scheme: Select

Accounting Scheme: Select

Service Scheme: Select

RADIUS Template: Select

Table 9-10 describes the parameters on the **Create Domain** page.

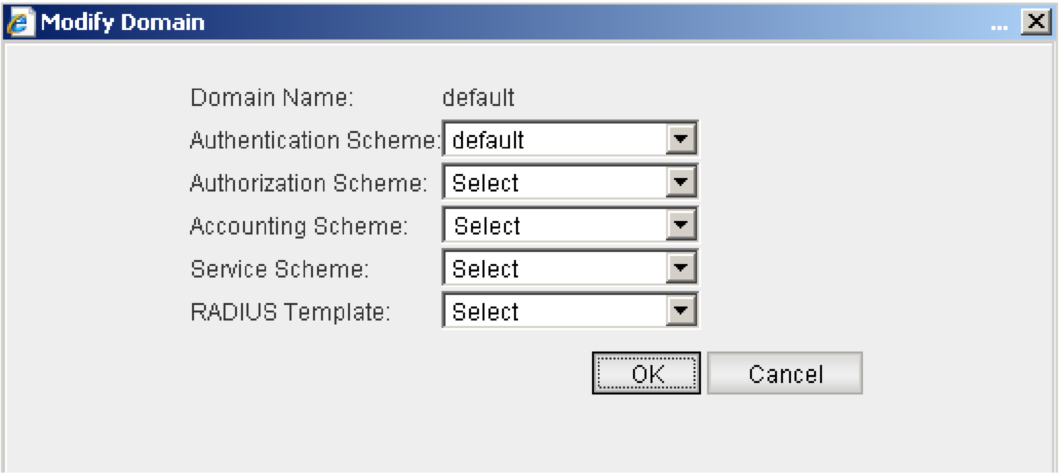
Table 9-10 Create Domain

Parameter	Description
Domain Name	Indicates the name of a new RADIUS server template.
Authentication Scheme	Indicates the authentication scheme of the system.
Authorization Scheme	Indicates the authorization scheme of the system.
Accounting Scheme	Indicates the accounting scheme of the system.
Service Scheme	Indicates the service scheme of the system.
RADIUS Template	Indicates the RADIUS server of the system.

  3. Set parameters.
  4. Click **OK**.
- Modify a domain.

1. Choose **Security** > **AAA** > **Domain** in the navigation tree to open the **Domain** page.
2. Click ✎ to open the **Modify Domain** page, as shown in **Figure 9-17**.

Figure 9-17 Modify Domain



Modify Domain

Domain Name: default

Authentication Scheme: default

Authorization Scheme: Select

Accounting Scheme: Select

Service Scheme: Select

RADIUS Template: Select

NOTE

- **Table 9-10** describes the parameters on the **Modify Domain** page.
- The domain name cannot be modified.

3. Set parameters.
4. Click **OK**.

- Delete a domain.
  1. Choose **Security** > **AAA** > **Domain** in the navigation tree to open the **Domain** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

9.3.5 User

You can create a local database to maintain user information and manage users on the local switch.

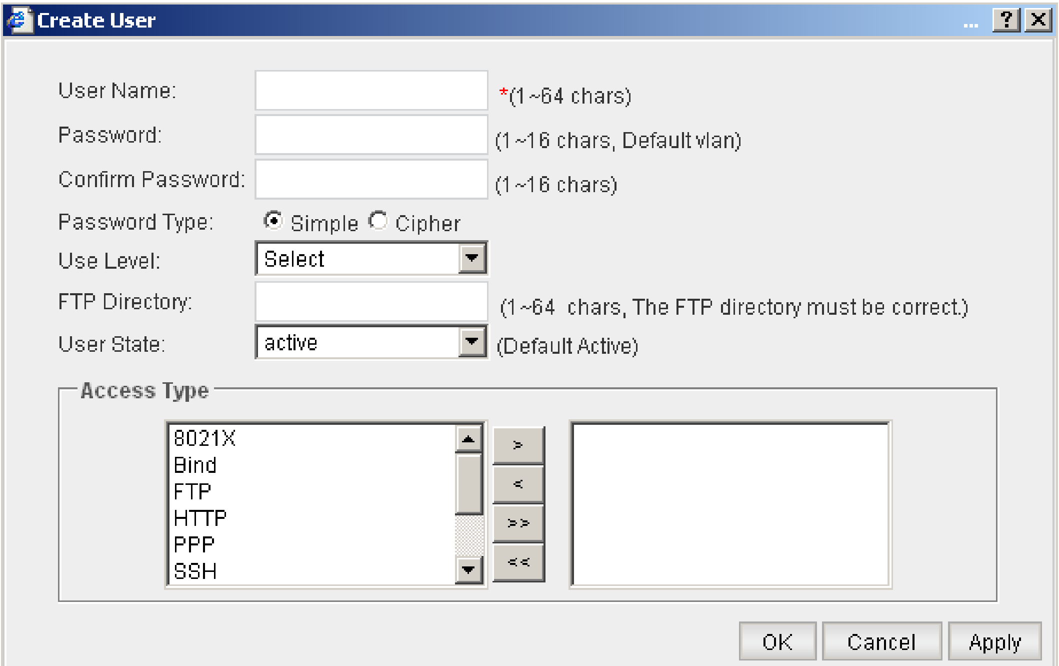
Context

- You need to create a local user account and configure attributes of the local user so that the switch can authenticate and authorize the local user that logs in according to the local user information.
- The following operations can be performed only by users with the user level higher than 0.

Procedure

- Create a user.
  1. Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.
  2. Click **New** to open the **Create User** page, as shown in **Figure 9-18**.

Figure 9-18 Create User



Create User

User Name: *(1~64 chars)

Password: (1~16 chars, Default vlan)

Confirm Password: (1~16 chars)

Password Type: ● Simple ○ Cipher

Use Level: Select

FTP Directory: (1~64 chars, The FTP directory must be correct.)

User State: active (Default Active)

Access Type

Table 9-11 describes the parameters on the **Create User** page.

Table 9-11 Create User

Parameter	Description
User Name	Indicates a new user name.
Password	Indicates the password.
Confirm Password	Confirms the password. It must be the same as the password.
Password Type	Indicates the password type. The password can be in plain text or cipher text. By default, the password is in cipher text.

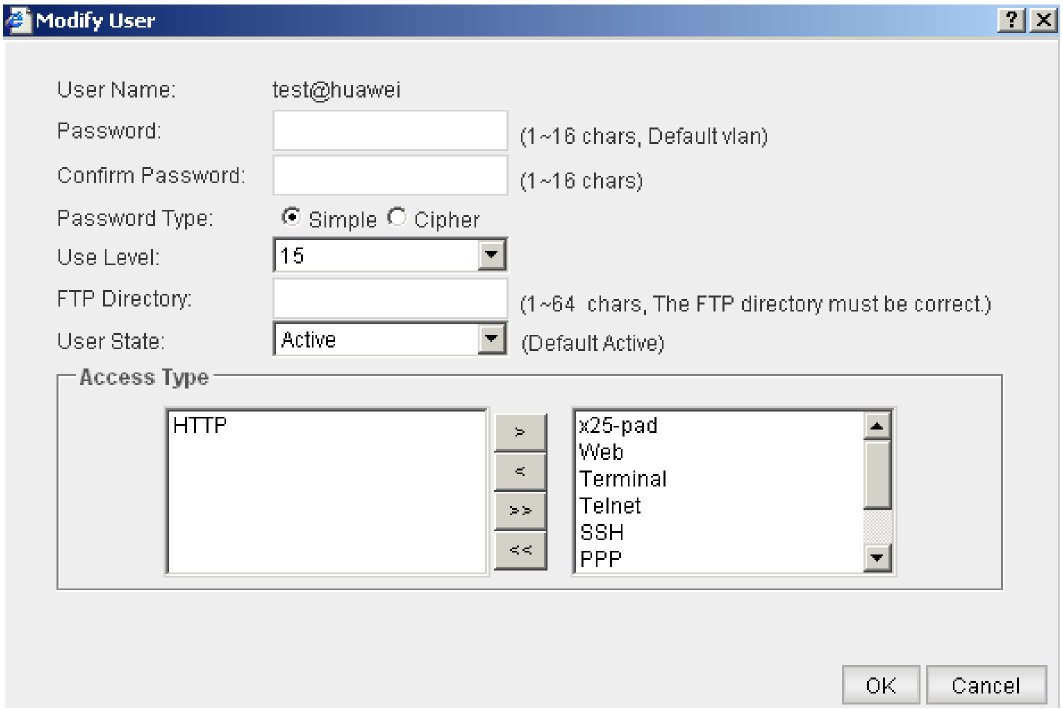
Parameter	Description
Use Level	Indicates the user level. The value ranges from 0 to 15. A greater value indicates a higher user level. Users of different levels have different authorities. A user can run the commands of the same level or lower levels. Users at level 2 can run the commands at levels 0, 1, and 2. Users at level 15 can run commands at all levels.
FTP Directory	Indicates the FTP directory, for example, **flash:/**. NOTE If the access type of a local user is set to FTP, this parameter is mandatory; otherwise, FTP users cannot log in.
User State	Indicates the user status, including: ● Active ● Block By default, the value is **Active**. NOTE ● If a local user is in **Active** state, a switch accepts and processes the authentication request of the user. ● If a local user is in **block** state, the authentication request from this user is denied.
Access Type	Indicates the access type. After you specify the access type of a user, only the users using the specified access type can log in. The steps are as follows: Select the access type in the right list box and click >. The selected access type is displayed in the right list box. By default, a user can log in by using any access type. NOTE ● You can hold **shift** or **ctrl** to select multiple access types or click >> to select all the access types. ● If you do not specify any value, all options are selected by default. If you deselect all options, the default settings are restored (all access types are supported).

Copyright © Huawei Technologies Co., Ltd.

3. Set parameters.
4. Click **OK**.

- Modify a user.
  1. Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.
  2. Click ✎ to open the **Modify User** page, as shown in **Figure 9-19**.

Figure 9-19 Modify User



Modify User

User Name: test@huawei

Password: (1~16 chars, Default vlan)

Confirm Password: (1~16 chars)

Password Type: ● Simple ○ Cipher

Use Level: 15

FTP Directory: (1~64 chars, The FTP directory must be correct.)

User State: Active (Default Active)

Access Type

HTTP

x25-pad
Web
Terminal
Telnet
SSH
PPP

NOTE

- **Table 9-11** describes the parameters on the **Modify User** page.
- The user name cannot be modified.

3. Set parameters.
4. Click **OK**.

- Delete a user.
  1. Choose **Security** > **AAA** > **User** in the navigation tree to open the **User** page.
  2. Select a record that you want to delete and click **Delete**. The system asks you whether to delete the record.

     NOTE

     - The current user cannot be deleted.
     - To select a record, click the check box of the record.
     - To delete records in batches, click the check boxes of the records.
  3. Click **OK**.

----End

9.4 802.1x

You can configure 802.1x parameters globally or on an interface. **The S2700SI or S2700EI series switches do not support the function.**

IEEE 802.1x, or 802.1x in brief, is a port-based network access control protocol. 802.1x was originated from IEEE 802.11 for wireless local area network (WLAN) access and was first introduced to solve the problem of access authentication of WLAN users. Later, the 802.1x protocol was applied on the Ethernet as a common access control mechanism on LAN interfaces to solve problems of authentication and security on the Ethernet.

Port-based network access control indicates that authentication and control are implemented for access devices on an interface of a LAN access control device. A user device can access LAN resources only after it passes authentication.

9.4.1 802.1X Global Settings

802.1x parameters can be set before global 802.1x authentication is enabled, but take no effect. After global 802.1x authentication is enabled, 802.1x parameters can be set before of each interface takes effect.

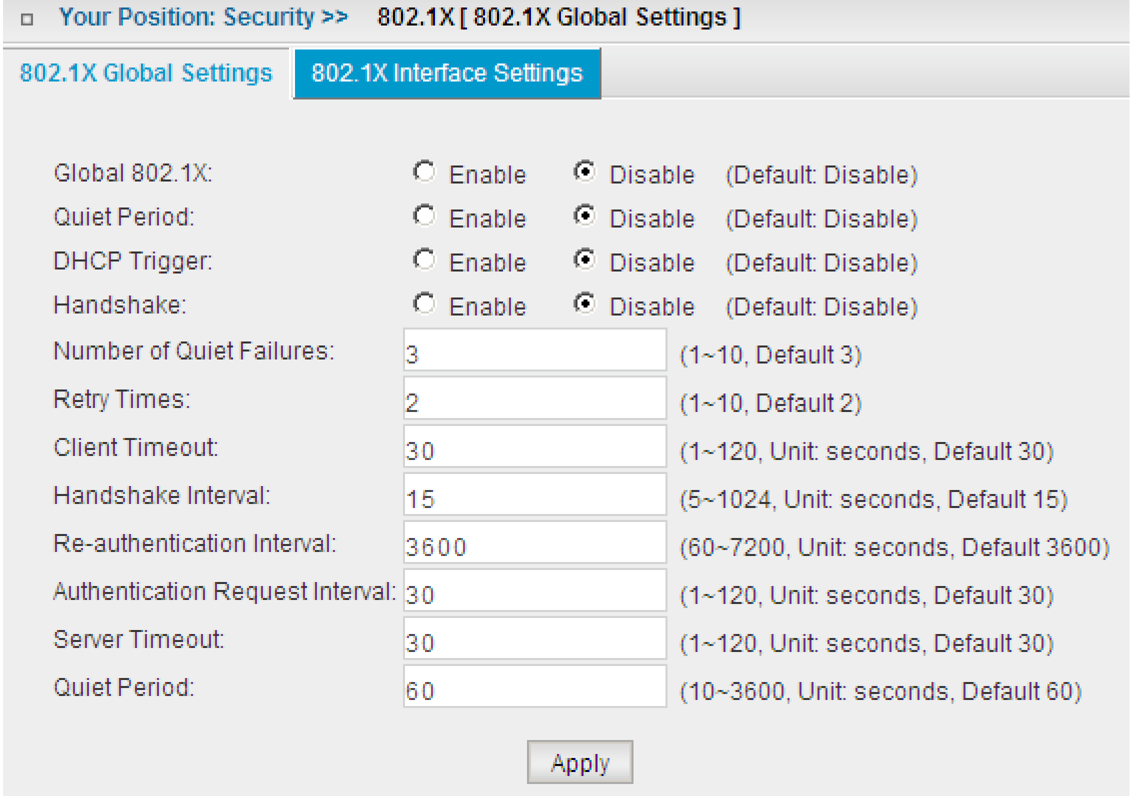
Context

You can configure 802.1x authentication to authenticate and control access devices connected to an interface of a LAN access control device.

Procedure

Step 1 Choose **Security** > **802.1X** > **802.1X Global Settings** in the navigation tree to open the **802.1X Global Settings** page, as shown in **Figure 9-20**.

Figure 9-20 802.1X Global Settings



□ Your Position: Security >> 802.1X [802.1X Global Settings]

802.1X Global Settings | 802.1X Interface Settings

Global 802.1X: ○ Enable ● Disable (Default: Disable)

Quiet Period: ○ Enable ● Disable (Default: Disable)

DHCP Trigger: ○ Enable ● Disable (Default: Disable)

Handshake: ○ Enable ● Disable (Default: Disable)

Number of Quiet Failures: 3 (1~10, Default 3)

Retry Times: 2 (1~10, Default 2)

Client Timeout: 30 (1~120, Unit: seconds, Default 30)

Handshake Interval: 15 (5~1024, Unit: seconds, Default 15)

Re-authentication Interval: 3600 (60~7200, Unit: seconds, Default 3600)

Authentication Request Interval: 30 (1~120, Unit: seconds, Default 30)

Server Timeout: 30 (1~120, Unit: seconds, Default 30)

Quiet Period: 60 (10~3600, Unit: seconds, Default 60)

Table 9-12 describes the parameters on the **802.1X Global Settings** page.

Table 9-12 802.1X Global Settings

Parameter	Description
Global 802.1X	Indicates whether to enable global 802.1x authentication. The options are **Enable** and **Disable**. By default, the value is **Disable**. 802.1x parameters can be set before global 802.1x authentication is enabled, but take no effect. After global 802.1x authentication is enabled, 802.1x parameters can be set before of each interface takes effect.

Parameter	Description
Quiet Period	Indicates whether to enable the quiet timer function. The options are **Enable** and **Disable**. By default, the value is **Disable**. NOTE If a user fails to pass 802.1x authentication after the quiet timer function is enabled, the system keeps the user quiet for a period. In this manner, the impact caused by frequent authentication is prevented. During the quite period, the switch discards 802.1x authentication request packets from the user.
DHCP Trigger	Indicates whether to enable the switch to trigger 802.1x authentication after receiving DHCP messages. The options are **Enable** and **Disable**. By default, the value is **Disable**. The switch is enabled to trigger 802.1x authentication after receiving DHCP messages. If a user fails to pass authentication, the user cannot dynamically obtain an IP address from the DHCP server.
Handshake	Indicates whether to enable the handshake function. The options are **Enable** and **Disable**. By default, the value is **Disable**. NOTE Not all clients support the handshake function. If a client does not support the handshake function, the switch will not receive handshake response packets within the handshake interval. In this case, you need to disable the handshake function to prevent the switch from disconnecting users by mistake.
Number of Quiet Failures	Indicates the number of authentication failures before the 802.1x user enters the quiet state.
Retry Times	Indicates the number of retransmission times. If the switch does not receive a response after sending an authentication request to a user, the switch retransmits the authentication request to the user. If the switch still fails to receive the response when the number of sent authentication requests reaches the limit, the switch does not send the authentication request to the user any more.
Client Timeout	Indicates the timeout interval of the response from the client.
Handshake Interval	Indicates the interval of handshakes between the switch and the 802.1x client.

Parameter	Description
Re-authentication Interval	Indicates the re-authentication interval. After a user passes 802.1x authentication, the switch sends a re-authentication request to the authentication server after a period. The re-authentication interval is controlled by the re-authentication timer.
Authentication Request Interval	Indicates the interval for sending authentication requests.
Server Timeout	Indicates the timeout interval of the response from the server. If the authentication server does not respond to an authentication request within the timeout interval, the switch retransmits the authentication request to the authentication server.
Quiet Period	Indicates the value of the quiet timer. If a user fails to pass 802.1x authentication, the authentication device waits until the quiet timer expires and re-initiates authentication requests. During the quiet period, the authentication device does not process authentication requests from the user.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

9.4.2 802.1X Interface Settings

You can query, set, and delete 802.1x parameters of an interface.

Context

You can configure 802.1x authentication to authenticate and control access devices connected to an interface of a LAN access control device.

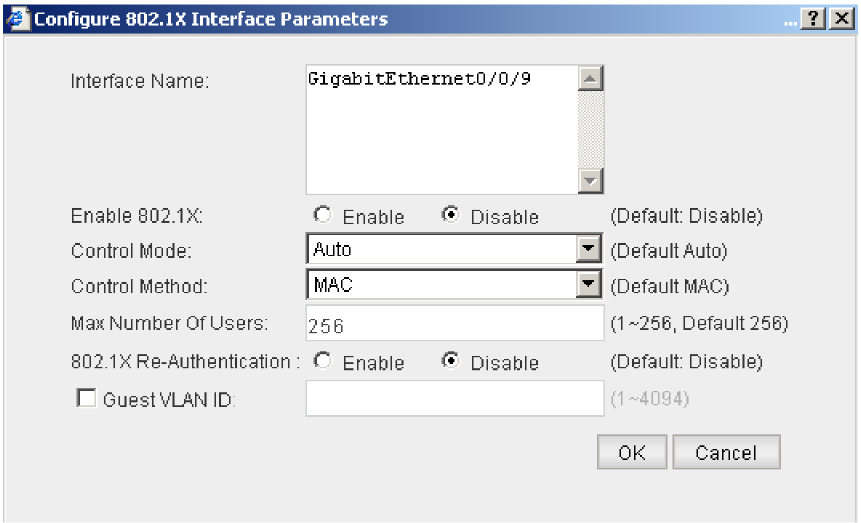
⚠ **CAUTION**

If 802.1x authentication is enabled on an interface, MAC address authentication or direct authentication cannot be enabled on the interface. If MAC address authentication or direct authentication is enabled on an interface, 802.1x authentication cannot be enabled on the interface.

Procedure

- Query information about 802.1x parameters on an interface.
  1. Choose **Security** > **802.1X** > **802.1X Interface Settings** in the navigation tree to open the **802.1X Interface Settings** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Set 802.1x parameters on an interface.
  1. Choose **Security** > **802.1X** > **802.1X Interface Settings** in the navigation tree to open the **802.1X Interface Settings** page.
  2. Select a record and click **Configure**. The **Configure 802.1X Interface Parameters** page is displayed, as shown in **Figure 9-21**.

Figure 9-21 Configure 802.1X Interface Parameters



Configure 802.1X Interface Parameters

Interface Name: GigabitEthernet0/0/9

Enable 802.1X: ○ Enable ● Disable (Default: Disable)

Control Mode: Auto (Default Auto)

Control Method: MAC (Default MAC)

Max Number Of Users: 256 (1~256, Default 256)

802.1X Re-Authentication : ○ Enable ● Disable (Default: Disable)

□ Guest VLAN ID (1~4094)

Table 9-13 describes the parameters on the **Configure 802.1X Interface Parameters** page.

Table 9-13 Configure 802.1X Interface Parameters

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. NOTE If only one interface is selected, the configuration of the interface is displayed on the **Configure 802.1X Interface Parameters** page. If multiple interfaces are selected, the default settings of the interfaces are displayed.

Parameter	Description
Enable 802.1X	Indicates whether to enable 802.1x authentication. The options are **Enable** and **Disable**. By default, the value is **Disable**. **NOTE** The 802.1x configuration takes effect only after 802.1x authentication is enabled globally and on an interface.
Control Mode	Indicates the access control mode of an interface. The options are as follows: ● Auto ● Authorized-force ● Unauthorized-force By default, the value is **Auto**.
Control Method	Indicates the access control mode of an interface: ● MAC ● Interface By default, the MAC address-based access control method is used. **NOTE** ● If the value is **Interface**, only one user can access the interface. ● If the value is **MAC**, a guest VLAN can be configured but takes no effect.
Max Number Of Users	Indicates the maximum number of access users on the specified interface. If no interface is specified, all interfaces support the same number of access users.
802.1X Re-Authentication	Indicates whether to enable 802.1x re-authentication. The options are **Enable** and **Disable**. By default, the value is **disabled**.
Guest VLAN ID	Indicates the ID of a guest VLAN. To configure a guest VLAN, select the check box before **Guest VLAN ID** and enter a VLAN ID. **NOTE** Only one guest VLAN can be configured on the interface.

3. Set parameters.
4. Click **OK**.

- Clear the configuration of 802.1x parameters on an interface.
  1. Choose **Security** > **802.1X** > **802.1X Interface Settings** in the navigation tree to open the **802.1X Interface Settings** page.
  2. Select a record and click **Clear Configuration**. The system asks you whether to delete the record.
  3. Click **OK**.

----End

9.5 MAC Authen

You can configure MAC address authentication globally or on an interface. **The S2700SI or S2700EI series switches do not support the function.**

You can configure the following authentication methods for MAC address authentication on the switch:

- Remote Authentication Dial-In User Service (RADIUS) authentication
- Local authentication

9.5.1 Global Configuration

The configuration of MAC address authentication takes effect on each interface only after global MAC address authentication is enabled.

Context

MAC address authentication can be configured on an interface before global MAC address authentication is configured, but does not take effect on the interface. After global MAC address authentication is enabled, MAC address authentication enabled on an interface takes effect immediately.

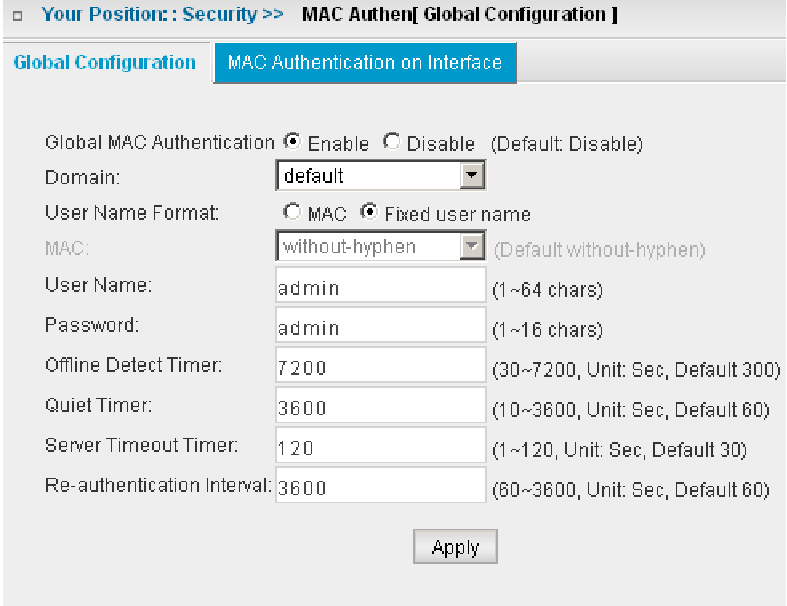
NOTE

MAC address authentication and 802.1x authentication cannot be enabled on the same interface.

Procedure

Step 1 Choose **Security** > **MAC Authen** > **Global Configuration** in the navigation tree to open the **Global Configuration** page, as shown in **Figure 9-22**.

Figure 9-22 Global Configuration



Your Position: : Security >> MAC Authen[Global Configuration]
Global Configuration
MAC Authentication on Interface
Apply

Global MAC Authentication ● Enable ○ Disable (Default: Disable)
Domain: default
User Name Format: ○ MAC ● Fixed user name
MAC: without-hyphen (Default without-hyphen)
User Name: admin (1~64 chars)
Password: admin (1~16 chars)
Offline Detect Timer: 7200 (30~7200, Unit: Sec, Default 300)
Quiet Timer: 3600 (10~3600, Unit: Sec, Default 60)
Server Timeout Timer: 120 (1~120, Unit: Sec, Default 30)
Re-authentication Interval: 3600 (60~3600, Unit: Sec, Default 60)

Table 9-14 describes the parameters on the **Global Configuration** page.

Table 9-14 Global Configuration

Parameter	Description
Global MAC Authentication	Indicates whether to enable global MAC address authentication. Authentication parameters can be set before global MAC address authentication is enabled, but take no effect. After global MAC address authentication is enabled, the authentication parameters of each interface take effect immediately. The options are **Enable** and **Disable**. By default, the value is **Disable**.
Domain	Indicates the domain for MAC address authentication.
User Name Format	Indicates the user name format. The options are as follows: ● MAC ● Fixed user name

Parameter	Description
MAC	Indicates the format of MAC addresses. The parameter is valid when MAC addresses of users are used as user names. The options are as follows: ● with-hyphen ● without-hyphen By default, the value is **without-hyphen**.
User Name	Indicates the user name. The value is valid when the fixed user name is used for MAC address authentication. Fixed user name: All users use the user names and passwords pre-configured on a switch; therefore, whether users can pass authentication depends on correctness of the user names and passwords and the maximum number of users allowed to use the user name.
Password	Indicates the password of the user. The value is valid when the fixed user name is used for MAC address authentication. Set the value of this parameter according to the user name format.
Offline Detect Timer	Indicates the value of the offline-detect timer, that is, the interval for the switch to detect whether a user is offline. When detecting that a user goes offline, the switch immediately instructs the RADIUS server to stop charging the user.
Quiet Timer	Indicates the value of the quiet timer. If a user fails to pass MAC address authentication, the switch waits for a period set by the quiet timer. Then the switch processes authentication requests from the user. During the quiet period, the switch does not process authentication requests from the user.
Server Timeout Timer	Indicates the timeout interval for the response from the RADIUS server. During MAC address authentication, if the connection between the switch and the RADIUS server expires, the switch forbids the user to access the Internet through the connected interface. In this case, the user can connect to another interface of the switch for re-authentication.

Parameter	Description
Re-authentication Interval	Indicates the re-authentication interval. After a user passes MAC address authentication, the switch sends an re-authentication request to the authentication server after a period. The re-authentication interval is controlled by the re-authentication timer.

Step 2 Set the parameters.

Step 3 Click **Apply** to complete the configuration.

----End

9.5.2 MAC Authentication on Interface

You can query, set, and delete MAC address authentication parameters on an interface.

Context

MAC address authentication can be configured on an interface before global MAC address authentication is configured, but does not take effect on the interface. After global MAC address authentication is enabled, MAC address authentication configured on an interface takes effect immediately.

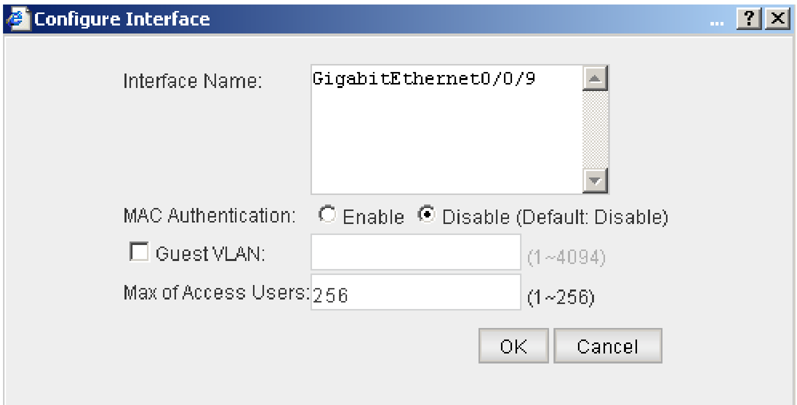
NOTE

MAC address authentication and 802.1x authentication cannot be configured on the same interface.

Procedure

- Query the configuration of MAC address authentication on an interface.
  1. Choose **Security** > **MAC Authen** > **MAC Authentication on Interface** in the navigation tree to open the **MAC Authentication on Interface** page.
  2. Set the search criteria.
  3. Click **Query** to display all matching records.
- Configure Interface
  1. Choose **Security** > **MAC Authen** > **MAC Authentication on Interface** in the navigation tree to open the **MAC Authentication on Interface** page.
  2. Select a record and click **Configure**. The **Configure Interface** page is displayed, as shown in **Figure 9-23**.

Figure 9-23 Configure Interface



Configure Interface

Interface Name: GigabitEthernet0/0/9

MAC Authentication: ○ Enable ● Disable (Default: Disable)

□ Guest VLAN: (1~4094)

Max of Access Users: 256 (1~256)

Table 9-15 describes the parameters on the **Configure Interface** page.

Table 9-15 Configure Interface

Parameter	Description
Interface Name	Indicates the name of an interface. The interface name cannot be modified. You can select multiple interfaces each time. NOTE If only one interface is selected, the configuration of the interface is displayed on the **Configure Interface** page. If multiple interfaces are selected, the default settings of the interfaces are displayed.
MAC Authentication	Indicates whether to enable MAC address authentication. The options are **Enable** and **Disable**. By default, the value is **Disable**.
Guest VLAN	Indicates the ID of a guest VLAN. To configure a guest VLAN, select the check box before **Guest VLAN ID** and enter a VLAN ID.
Max of Access Users	Indicates the maximum number of access users on the specified interface enabled with MAC address authentication. If no interface is specified, all interfaces can connect to access users of the same number.

3. Set parameters.
4. Click **OK**.

- Clear the configuration of MAC address authentication parameters on an interface.

1. Choose **Security** > **MAC Authen** > **MAC Authentication on Interface** in the navigation tree to open the **MAC Authentication on Interface** page.
2. Select a record that you want to clear and click **Clear Configuration**.

   NOTE

   - To select a record, click the check box of the record.
   - To delete records in batches, click the check boxes of the records.
3. Click **OK**.

----End

10 Tools

About This Chapter

This document describes the commands for maintaining and diagnosing the switch, that is, ping, tracert, and VCT.

10.1 Ping
The ping command is used to check network connectivity and host reachability.

10.2 Tracert
You can use the tracert command to test the gateways that packets pass through from the source host to the destination host. The tracert command is used to check network connectivity and locate network faults.

10.3 VCT
The VCT function controls the hardware interfaces and displays the cable status on the GUI so that you can conveniently and quickly locate faults and check lengths of cables.

Copyright © Huawei Technologies Co., Ltd.

10.1 Ping

The ping command is used to check network connectivity and host reachability.

Context

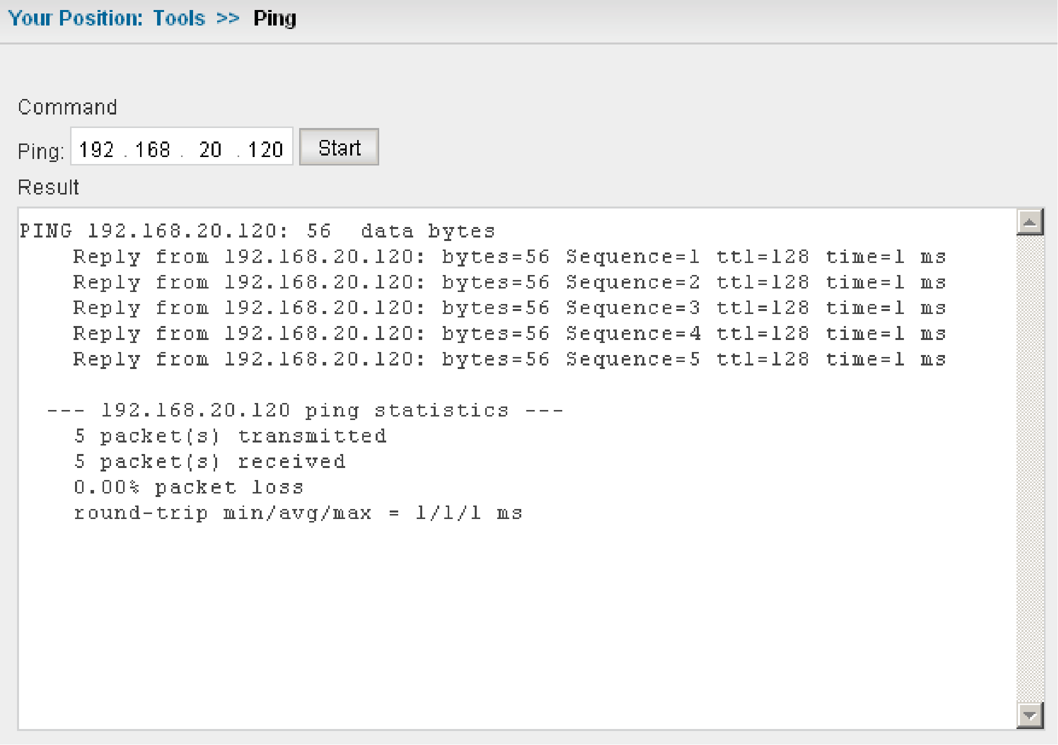
The ping command is used to check network connectivity and host reachability.

Procedure

Step 1 Choose **Tools** > **Ping** in the navigation tree to open the **Ping** page.

Step 2 Enter the IP address in the **ping** text box and click **Start**. The network connection information is displayed, as shown in **Figure 10-1**.

Figure 10-1 Ping



Ping: 192 . 168 . 20 . 120

```
PING 192.168.20.120: 56  data bytes
    Reply from 192.168.20.120: bytes=56 Sequence=1 ttl=128 time=1 ms
    Reply from 192.168.20.120: bytes=56 Sequence=2 ttl=128 time=1 ms
    Reply from 192.168.20.120: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 192.168.20.120: bytes=56 Sequence=4 ttl=128 time=1 ms
    Reply from 192.168.20.120: bytes=56 Sequence=5 ttl=128 time=1 ms

  --- 192.168.20.120 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

NOTE

If no response packets are received within the timeout interval, the following information is displayed:

```
Request time out
```

The preceding information shows that a link is faulty.

----End

10.2 Tracert

You can use the tracert command to test the gateways that packets pass through from the source host to the destination host. The tracert command is used to check network connectivity and locate network faults.

Context

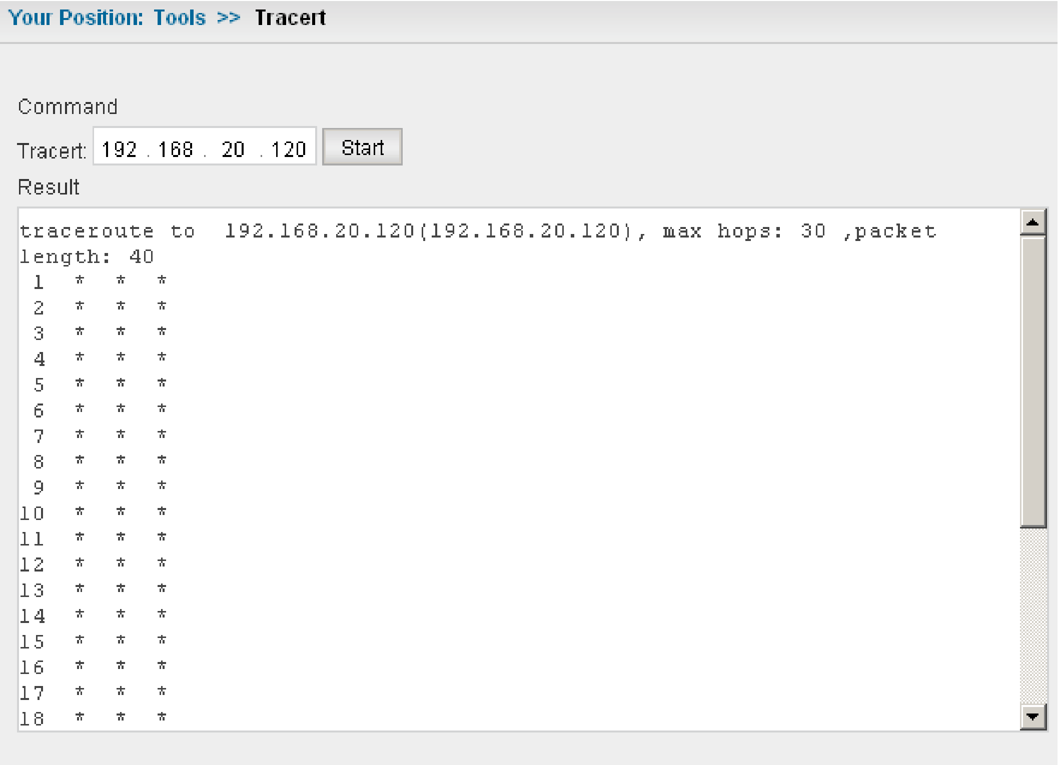
The **Tracert** command, also called **Trace Route** helps you check the IP addresses and the number of gateways between the source and the destination. Tracert is used to check network connectivity and locate network faults.

Procedure

Step 1 Choose **Tools** > **Tracert** in the navigation tree to open the **Trace Route** page.

Step 2 Enter the IP address in the **tracert** text box and click **Start**. The Layer 3 devices where packets pass through between the source host and the destination host are displayed, as shown in **Figure 10-2**.

Figure 10-2 Trace Route



Tracert: 192 . 168 . 20 . 120

```
traceroute to  192.168.20.120(192.168.20.120), max hops: 30 ,packet
length: 40
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
 9  *  *  *
10  *  *  *
11  *  *  *
12  *  *  *
13  *  *  *
14  *  *  *
15  *  *  *
16  *  *  *
17  *  *  *
18  *  *  *
```

NOTE

- The output of the **tracert** command includes IP addresses of all the gateways through which the packet reaches the destination. If one gateway sends back a packet indicating TTL timeout, * is displayed.
- The tracert test may takes a long time.

----End

10.3 VCT

The VCT function controls the hardware interfaces and displays the cable status on the GUI so that you can conveniently and quickly locate faults and check lengths of cables.

Context

The VCT function helps to detect the type of a network cable fault and locate the faulty point. In this manner, network cable faults can be conveniently located.

Procedure

Step 1 Choose **Tools** > **VCT** in the navigation tree to open the **VCT** page.

Step 2 Select an interface. You can select only one interface each time.

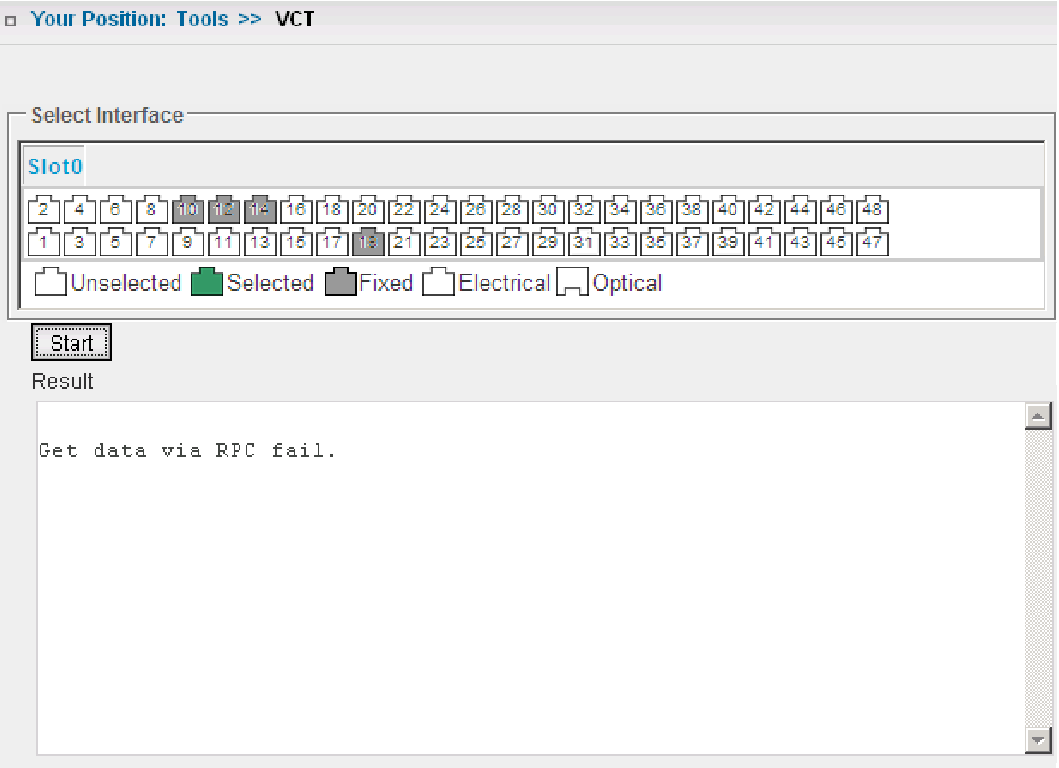
Step 3 Click **Start**.

CAUTION

The system displays a message requesting you to confirm the operation.

Step 4 Click **OK**. The returned information is displayed, as shown in **Figure 10-3**.

Figure 10-3 VCT



```
Get data via RPC fail.
```

----End