3Com Baseline Switch 2900 Family
User Guide

Baseline Switch 2920-SFP Plus

Baseline Switch 2928-SFP Plus

Baseline Switch 2952-SFP Plus

Baseline Switch 2928-PWR Plus

Baseline Switch 2928-HPWR Plus

Manual Version:
6W102-20090810
www.3com.com

3Com Corporation
350 Campus Drive, Marlborough,
MA, USA 01752 3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

About This Manual

Organization

3Com Baseline Switch 2900 Family User Guide is organized as follows:

Part	Contents
1 Overview	Perform overview of 3Com baseline switch 2900 family.
2 Configuration Wizard	Perform quick configuration of the device.
3 IRF	Configure global parameters and stack ports, and display global settings, port settings, and topology summary of a stack.
4 Summary	Display the basic system information, port information, system resource state, and recent system operation logs.
5 Device Basic Information	Display and configure the system name and idle timeout period for logged-in users.
6 System Time	Display and configure the system date and time.
7 Log Management	Clear system logs, display and configure the loghost, display and refresh system logs. Display and configure the buffer capacity, and interval for refreshes system logs.
8 Configuration Management	Back up the configuration file or upload the configuration file to be used at the next startup from the host of the current user to the device. Save the current configuration to the configuration file to be used at the next startup. Restore the factory default settings.
9 Device Maintenance	Configure to upload upgrade file from local host, and upgrade the system software. Configure to reboot the device. Display the electronic label of the device. Generate diagnostic information file, and view or save the file to local host.
10 File Management	Manage files on the device, such as displaying the file list, downloading a file, uploading a file, and removing a file.
11 Port Management	Create, modify, delete, and enable/disable a port, and clear port statistics.
12 Port Mirroring	Create, remove, and configure a port mirroring group.
13 User Management	Create, modify, and remove an FTP or Telnet user, and display the brief information of FTP and Telnet users.
14 Loopback Test	Perform loopback tests on Ethernet interfaces.
15 VCT	Check the status of the cables connected to Ethernet ports.
16 Flow Interval	Set an interval for collecting traffic statistics on interfaces, and display the average rate at which the interface receives and sends packets within a specified time interval.
17 Storm Constrain	Display, create, modify, and remove the port traffic threshold, and display or set the interval for collecting storm constrain statistics.

Part	Contents
18 RMON	Configure RMON, and dissplay, create, modify, and clear RMON statistics.
19 Energy Saving	Display and configure the energy saving settings of an interface.
20 SNMP	Configure SNMP, and dissplay, create, modify, and clear SNMP statistics.
21 Interface Statistics	Display and clear the statistics information of an interface.
22 VLAN	Create VLANs, and display the VLAN-related details of a port.
23 VLAN Interface	Create VLAN interfaces, configure IP addresses for them, and Display information about VLAN interfaces by address type.
24 Voice VLAN	Configure the global voice VLAN or a voice VLAN on a port.
25 MAC Address	Create and remove MAC addresses, display MAC address information.
26 MSTP	Configure MSTP.
27 Link Aggregation and LACP	Create, modify and remove link aggregation groups, and set LACP priorities.
28 LLDP	Configure LLDP.
29 IGMP Snooping	Configure IGMP snooping globally or in a VLAN, or on a port.
30 Routing	Create an IPv4 static route, dlete the selected IPv4 static routes, and display the IPv4 active route table.
31 DHCP	Configure DHCP Relay or DHCP Snooping
32 Service Management	Enable or disable services, set related parameters, and displays the states of services.
33 Diagnostic Tools	Ping an IPv4 address, or perform trace route operations.
34 ARP	Add, modify, remove, and display ARP entries. Configure and display gratuitous ARP.
35 802.1X	Configure 802.1X globally or on a port, and display 802.1X configuration information globally or on a port.
36 AAA	Add and remove ISP domains, specify authentication /authorization /accounting methods for an ISP domain.
37 RADIUS	Display and configure RADIUS parameters.
38 User	Create, modify and remove a local user or a user group.
39 PKI	Add, modify, and delete a PKI entity or a PKI domain. Generate a key pair, destroy a key pair, retrieve a certificate, request a certificate, and delete a certificate.
40 Port Isolation Group	Configure a port isolation group, and display port isolation group information.
41 Authorized IP	Configure and display authorized IP.
42 ACL-QoS	Configure ACL rules and Qos Policy.
43 PoE	Configure a PoE interface, and display PSE information and PoE interface information.

Conventions

The manual uses the following conventions:

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
⚠ **Warning**	Means reader be extremely careful. Improper operation may cause bodily injury.
⚠ **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
✎ **Note**	Means a complementary description.

Related Documentation

In addition to this manual, each 3com Baseline Switch 2900 documentation set includes the following:

Manual	Description
3Com Baseline Switch 2900 Family Getting Started Guide	This guide provides all the information you need to install and use the 3Com Baseline Switch 2900 Family.

Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

Table of Contents

1 Overview

The 3Com baseline switch 2900 family can be configured through the command line interface (CLI), web interface, and SNMP/MIB. These configuration methods are suitable for different application scenarios.

- The web interface supports all switch 2900 series configurations.
- The CLI provides some configuration commands to facilitate your operation. To perform other configurations not supported by the CLI, use the web interface.

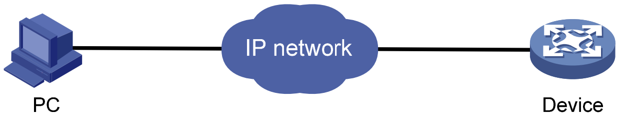
2 Configuration Through the Web Interface

Web-Based Network Management Operating Environment

3Com provides the Web-based network management function to facilitate the operations and maintenance on 3Com's network devices. Through this function, the administrator can visually manage and maintain network devices through the Web-based configuration interfaces.

Figure 2-1 shows a Web-based network management operating environment.

Figure 2-1 Web-based network management operating environment



Logging In to the Web Interface

Default Login Information

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

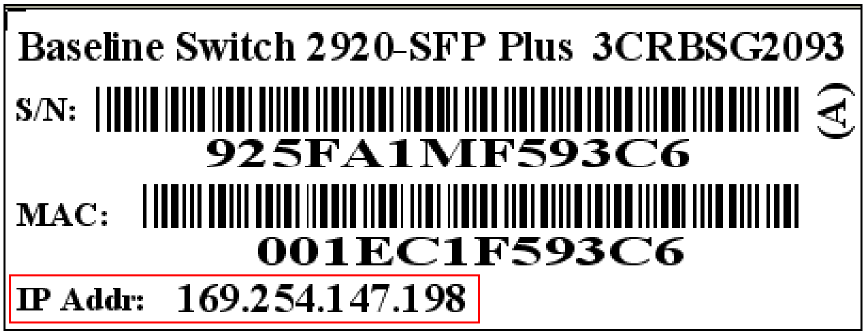
Table 2-1 The default Web login information

Information needed at login	Default value
Username	admin
Password	None
IP address of the device (VLAN-interface 1)	Default IP address of the device, depending on the status of the network where the device resides.

1) The device is not connected to the network, or no DHCP server exists in the subnet where the device resides

If the device is not connected to the network, or no DHCP server exists in the subnet where the device resides, you can get the default IP address of the device on the label on the right of the device rear panel, as shown in Figure 2-2. The default subnet mask is 255.255.0.0.

Figure 2-2 Default IP address of the device



Baseline Switch 2920-SFP Plus 3CRBSG2093

S/N: 925FA1MF593C6

MAC: 001EC1F593C6

IP Addr: 169.254.147.198

2) A DHCP server exists in the subnet where the device resides

If a DHCP server exists in the subnet where the device resides, the device will dynamically obtain its default IP address through the DHCP server. You can log in to the device through the console port, and execute the **summary** command to view the information of its default IP address.

```
<Sysname> summary
Select menu option:              Summary
IP Method:                       DHCP
IP address:                      10.153.96.86
Subnet mask:                     255.255.255.0
Default gateway:                 0.0.0.0
<Omitted>
```

Example

Assuming that the default IP address of the device is 169.254.147.198, follow these steps to log in to the device through the Web interface.

- Connect the device to a PC

Connect the GigabitEthernet interface of the device to a PC by using a crossover Ethernet cable (by default, all interfaces belong to VLAN 1).

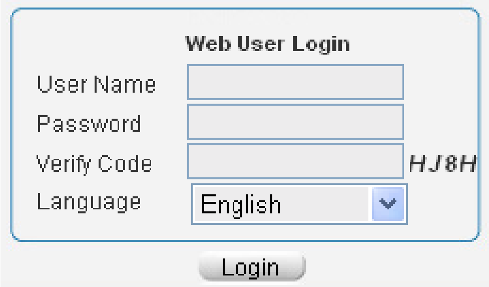
- Configure an IP address for the PC and ensure that the PC and device can communicate with each other properly.

Select an IP address for the PC from network segment 169.254.0.0/16 (except for the default IP address of the device), for example, 169.254.147.1.

- Open the browser, and input the login information.

On the PC, open the browser (it is recommended to use IE 5.0 or later), type the IP address http://169.254.147.198 in the address bar, and press **Enter** to enter the login page of the Web interface, as shown in Figure 2-3. Input the username **admin** and the verification code, leave the password blank, select the language (English and Chinese are supported at present), and click **Login**.

Figure 2-3 Login page of the Web interface



Web User Login

User Name

Password

Verify Code HJ8H

Language English

Caution

- The PC where you configure the device is not necessarily a Web-based network management terminal. A Web-based network management terminal is a PC used to log in to the Web interface and is required to be reachable to the device.
- After logging in to the Web interface, you can select **Device** > **Users** from the navigation tree, create a new user, and select **Wizard** or **Network** > **VLAN interface** to configure the IP address of the VLAN interface acting as the management interface. For detailed configuration, refer to the corresponding configuration manuals of these modules.
- If you click the verification code displayed on the Web login page, you can get a new verification code.
- Up to five users can concurrently log in to the device through the Web interface.

Logging Out of the Web Interface

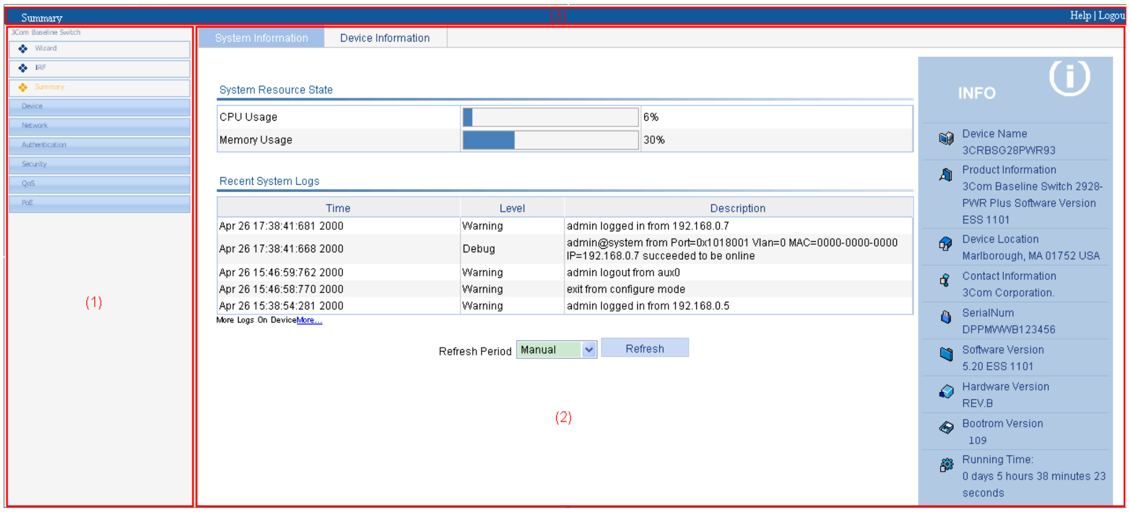
Click **Logout** in the upper-right corner of the Web interface, as shown in Figure 2-4 to quit the web console.

The system does not save the current configuration automatically. Therefore, you are recommended to save the current configuration before logout.

Introduction to the Web Interface

The Web interface is composed of three parts: navigation tree, title area, and body area, as shown in Figure 2-4.

Figure 2-4 Web-based configuration interface



System Resource State

CPU Usage		6%
Memory Usage		30%

Recent System Logs

Time	Level	Description
Apr 26 17:38:41:681 2000	Warning	admin logged in from 192.168.0.7
Apr 26 17:38:41:668 2000	Debug	admin@system from Port=0x1018001 Vlan=0 MAC=0000-0000-0000 IP=192.168.0.7 succeeded to be online
Apr 26 15:46:59:762 2000	Warning	admin logout from aux0
Apr 26 15:46:58:770 2000	Warning	exit from configure mode
Apr 26 15:38:54:281 2000	Warning	admin logged in from 192.168.0.5

More Logs On DeviceMore…

Device Name
3CRBSG28PWR93

Product Information
3Com Baseline Switch 2928-PWR Plus Software Version ESS 1101

Device Location
Marlborough, MA 01752 USA

Contact Information
3Com Corporation.

SerialNum
DPPMWWB123456

Software Version
5.20 ESS 1101

Hardware Version
REV.B

Bootrom Version
109

Running Time:
0 days 5 hours 38 minutes 23 seconds

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

- Navigation tree: Organizes the Web-based NM functions as a navigation tree, where you can select and configure functions as needed. The result is displayed in the body area.
- Body area: Allows you to configure and display features.
- Title area: Displays the path of the current configuration interface in the navigation tree; provides the **Help** button to display the Web related help information, and the **Logout** button to log out of the Web interface.

Caution

The Web network management functions not supported by the device will not be displayed in the navigation tree.

Web User Level

Web user levels, from low to high, are **visitor**, **monitor**, **configure**, and **management**. A user with a higher level has all the operating rights of a user with a lower level.

- Visitor: Users of this level can only use the network diagnostic tools **ping** and **Trace Route**. They can neither access the device data nor configure the device.
- Monitor: Users of this level can only access the device data but cannot configure the device.
- Configure: Users of this level can access device data and configure the device, but they cannot upgrade the host software, add/delete/modify users, or back up/restore configuration files.
- Management: Users of this level can perform any operations to the device.

Introduction to the Web-Based NM Functions

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

Note

User level in Table 2-2 indicates that users of this level or users of a higher level can perform the corresponding operations.

Table 2-2 Description of Web-based NM functions

Function menu			Description	User level
Wizard		IP Setup	Perform quick configuration of the device.	Management
IRF		Setup	Display global settings and port settings of a stack.	Configure
			Configure global parameters and stack ports.	Management
		Topology Summary	Display the topology summary of a stack.	Configure
		Device Summary	Display the control panels of stack members.	Configure
Summary		System Information	Display the basic system information, system resource state, and recent system operation logs.	Monitor
		Device Information	Display the port information of the device.	Monitor
Device	Basic	System Name	Display and configure the system name.	Configure
		Web Idle Timeout	Display and configure the idle timeout period for logged-in users.	Configure
	Device Maintenance	Software Upgrade	Configure to upload upgrade file from local host, and upgrade the system software.	Management
		Reboot	Configure to reboot the device.	Management
		Electronic Label	Display the electronic label of the device.	Monitor
		Diagnostic Information	Generate diagnostic information file, and view or save the file to local host.	Management
	System Time	System Time	Display and configure the system date and time.	Configure
	Syslog	Loglist	Display and refresh system logs.	Monitor
			Clear system logs.	Configure
		Loghost	Display and configure the loghost.	Configure
		Log Setup	Display and configure the buffer capacity, and interval for refreshes system logs.	Configure
	Configuration	Backup	Back up the configuration file to be used at the next startup from the device to the host of the current user.	Management
		Restore	Upload the configuration file to be used at the next startup from the host of the current user to the device.	Management

Function menu			Description	User level
		Save	Save the current configuration to the configuration file to be used at the next startup.	Configure
		Initialize	Restore the factory default settings.	Configure
	File Management	File Management	Manage files on the device, such as displaying the file list, downloading a file, uploading a file, and removing a file.	Management
	Port Management	Summary	Display port information by features.	Monitor
		Detail	Displays feature information by ports.	Monitor
		Setup	Create, modify, delete, and enable/disable a port, and clear port statistics.	Configure
	Port Mirroring	Summary	Display the configuration information of a port mirroring group.	Monitor
		Create	Create a port mirroring group.	Configure
		Remove	Remove a port mirroring group.	Configure
		Modify Port	Configure ports for a mirroring group.	Configure
	Users	Summary	Display the brief information of FTP and Telnet users.	Monitor
		Super Password	Configure a password for a lower-level user to switch from the current access level to the management level.	Management
		Create	Create an FTP or Telnet user.	Management
		Modify	Modify FTP or Telnet user information.	Management
		Remove	Remove an FTP or a Telnet user.	Management
		Switch To Management	Switch the current user level to the management level.	Visitor
	Loopback	Loopback	Perform loopback tests on Ethernet interfaces.	Configure
	VCT	VCT	Check the status of the cables connected to Ethernet ports.	Configure
	Flow Interval	Port Traffic Statistics	Display the average rate at which the interface receives and sends packets within a specified time interval.	Monitor
		Interval Configuration	Set an interval for collecting traffic statistics on interfaces.	Configure
	Storm Constrain	Storm Constrain	Display and set the interval for collecting storm constrain statistics. Display, create, modify, and remove the port traffic threshold.	Configure
	RMON	Statistics	Display, create, modify, and clear RMON statistics.	Configure
		History	Display, create, modify, and clear RMON history sampling information.	Configure
		Alarm	View, create, modify, and clear alarm entries.	Configure

Function menu			Description	User level
		Event	View, create, modify, and clear event entries.	Configure
		Log	Display log information about RMON events.	Configure
	Energy Saving	Energy Saving	Display and configure the energy saving settings of an interface.	Configure
	SNMP	Setup	Display and refresh SNMP configuration and statistics information.	Monitor
			Configure SNMP.	Configure
		Community	Display SNMP community information.	Monitor
			Create, modify and delete an SNMP community.	Configure
		Group	Display SNMP group information.	Monitor
			Create, modify and delete an SNMP group.	Configure
		User	Display SNMP user information.	Monitor
			Create, modify and delete an SNMP user.	Configure
		Trap	Display the status of the SNMP trap function and information about target hosts.	Monitor
			Enable or disable the SNMP trap function, or create, modify and delete a target host.	Configure
		View	Display SNMP view information.	Monitor
			Create, modify and delete an SNMP view.	Configure
	Interface Statistics	Interface Statistics	Display and clear the statistics information of an interface.	Configure
Net work	VLAN	Select VLAN	Select a VLAN range.	Monitor
		Create	Create VLANs.	Configure
		Port Detail	Display the VLAN-related details of a port.	Monitor
		Detail	Displays the member port information of a VLAN.	Monitor
		Modify VLAN	Modify the description and member ports of a VLAN.	Configure
		Modify Port	Change the VLAN to which a port belongs.	Configure
		Remove	Remove VLANs.	Configure
	VLAN Interface	Summary	Display information about VLAN interfaces by address type.	Monitor
		Create	Create VLAN interfaces and configure IP addresses for them.	Configure
		Modify	Modify the IP addresses and status of VLAN interfaces.	Configure
		Remove	Remove VLAN interfaces.	Configure
	Voice VLAN	Summary	Display voice VLAN information globally or on a port.	Monitor
		Setup	Configure the global voice VLAN.	Configure
		Port Setup	Configure a voice VLAN on a port.	Configure

Function menu			Description	User level
		OUI Summary	Display the addresses of the OUIs that can be identified by voice VLAN.	Monitor
		OUI Add	Add the address of an OUI that can be identified by voice VLAN.	Configure
		OUI Remove	Remove the address of an OUI that can be identified by voice VLAN.	Configure
	MAC	MAC	Display MAC address information.	Monitor
			Create and remove MAC addresses.	Configure
		Setup	Display and configure MAC address aging time.	Configure
	MSTP	Region	Display information about MST regions.	Monitor
			Modify MST regions.	Configure
		Global	Set global MSTP parameters.	Configure
		Port Summary	Displays the MSTP information of ports.	Monitor
		Port Setup	Set MSTP parameters on ports.	Configure
	Link Aggregation	Summary	Display information about link aggregation groups.	Monitor
		Create	Create link aggregation groups.	Configure
		Modify	Modify link aggregation groups.	Configure
		Remove	Remove link aggregation groups.	Configure
	LACP	Summary	Display information about LACP-enabled ports and their partner ports.	Monitor
		Setup	Set LACP priorities.	Configure
	LLDP	Port Setup	Display the LLDP configuration information, local information, neighbor information, statistics information, and status information of a port.	Monitor
			Modify LLDP configuration on a port.	Configure
		Global Setup	Display global LLDP configuration information.	Monitor
			Configure global LLDP parameters.	Configure
		Global Summary	Display global LLDP local information and statistics.	Monitor
		Neighbor Summary	Displays global LLDP neighbor information.	Monitor
	IGMP Snooping	Basic	Display global IGMP snooping configuration information or the IGMP snooping configuration information in a VLAN, and view the IGMP snooping multicast entry information.	Monitor
			Configure IGMP snooping globally or in a VLAN.	Configure
		Advanced	Display the IGMP snooping configuration information on a port.	Monitor
			Configure IGMP snooping on a port.	Configure
	IPv4 Routing	Summary	Display the IPv4 active route table.	Monitor
		Create	Create an IPv4 static route.	Configure

Function menu			Description	User level
		Remove	Delete the selected IPv4 static routes.	Configure
	DHCP	DHCP Relay	Display information about the DHCP status, advanced configuration information of the DHCP relay agent, DHCP server group configuration, DHCP relay agent interface configuration, and the DHCP client information.	Monitor
			Enable/disable DHCP, configure advanced DHCP relay agent settings, configure a DHCP server group, and enable/disable the DHCP relay agent on an interface.	Configure
		DHCP Snooping	Display the status, trusted and untrusted ports and DHCP client information of DHCP snooping.	Monitor
			Enable/disable DHCP snooping, and configure DHCP snooping trusted and untrusted ports.	Configure
	Service	Service	Displays the states of services: enabled or disabled.	Configure
			Enable/disable services, and set related parameters.	Management
	Diagnostic Tools	Ping	Ping an IPv4 address.	Visitor
		Trace Route	Perform trace route operations.	Visitor
	ARP Management	ARP Table	Display ARP table information.	Monitor
			Add, modify, and remove ARP entries.	Configure
		Gratuitous ARP	Displays the configuration information of gratuitous ARP.	Monitor
			Configure gratuitous ARP.	Configure
	ARP Anti-Attack	ARP Detection	Display ARP detection configuration information.	Monitor
			Configure ARP detection.	Configure
Authentication	802.1X	802.1X	Display 802.1X configuration information globally or on a port.	Monitor
			Configure 802.1X globally or on a port.	Configure
	AAA	Domain Setup	Display ISP domain configuration information.	Monitor
			Add and remove ISP domains.	Management
		Authentication	Display the authentication configuration information of an ISP domain.	Monitor
			Specify authentication methods for an ISP domain.	Management
		Authorization	Display the authorization method configuration information of an ISP domain.	Monitor
			Specify authorization methods for an ISP domain.	Management
		Accounting	Display the accounting method configuration information of an ISP domain.	Monitor
			Specify accounting methods for an ISP domain.	Management
	RADIUS	RADIUS Server	Display and configure RADIUS server information.	Management

Function menu			Description	User level
		RADIUS Setup	Display and configure RADIUS parameters.	Management
	Users	Local User	Display configuration information about local users.	Monitor
			Create, modify and remove a local user.	Management
		User Group	Display configuration information about user groups.	Monitor
			Create, modify and remove a user group.	Management
	PKI	Entity	Display information about PKI entities.	Monitor
			Add, modify, and delete a PKI entity.	Configure
		Domain	Display information about PKI domains.	Monitor
			Add, modify, and delete a PKI domain.	Configure
		Certificate	Display the certificate information of PKI domains and view the contents of a certificate.	Monitor
			Generate a key pair, destroy a key pair, retrieve a certificate, request a certificate, and delete a certificate.	Configure
		CRL	Display the contents of the CRL.	Monitor
			Receive the CRL of a domain.	Configure
Sec urity	Port Isolate Group	Summary	Display port isolation group information.	Monitor
		Modify	Configure a port isolation group.	Configure
	Authoriz ed IP	Summary	Display the configurations of authorized IP, the associated IPv4 ACL list, and the associated IPv6 ACL list.	Management
		Setup	Configure authorized IP.	Management
QoS	Time Range	Summary	Display time range configuration information.	Monitor
		Create	Create a time range.	Configure
		Remove	Delete a time range.	Configure
	ACL IPv4	Summary	Display IPv4 ACL configuration information.	Monitor
		Create	Create an IPv4 ACL.	Configure
		Basic Setup	Configure a rule for a basic IPv4 ACL.	Configure
		Advanced Setup	Configure a rule for an advanced IPv4 ACL.	Configure
		Link Setup	Create a rule for a link layer ACL.	Configure
		Remove	Delete an IPv4 ACL or its rules.	Configure
	Queue	Summary	Display the queue information of a port.	Monitor
		Setup	Configure a queue on a port.	Configure
	Line Rate	Summary	Display line rate configuration information.	Monitor
		Setup	Configure the line rate.	Configure

Function menu			Description	User level
	Classifier	Summary	Display classifier configuration information.	Monitor
		Create	Create a class.	Configure
		Setup	Configure the classification rules for a class.	Configure
		Remove	Delete a class or its classification rules.	Configure
	Behavior	Summary	Display traffic behavior configuration information.	Monitor
		Create	Create a traffic behavior.	Configure
		Setup	Configure actions for a traffic behavior.	Configure
		Port Setup	Configuring traffic mirroring and traffic redirecting for a traffic behavior	Configure
		Remove	Delete a traffic behavior.	Configure
	QoS Policy	Summary	Display QoS policy configuration information.	Monitor
		Create	Create a QoS policy.	Configure
		Setup	Configure the classifier-behavior associations for a QoS policy.	Configure
		Remove	Delete a QoS policy or its classifier-behavior associations.	Configure
	Port Policy	Summary	Display the QoS policy applied to a port.	Monitor
		Setup	Apply a QoS policy to a port.	Configure
		Remove	Remove the QoS policy from the port.	Configure
	Priority Mapping	Priority Mapping	Display priority mapping table information.	Monitor
			Modify the priority mapping entries.	Configure
	Port Priority	Port Priority	Display port priority and trust mode information.	Monitor
			Modify port priority and trust mode.	Configure
PoE	PoE	Summary	Display PSE information and PoE interface information.	Monitor
		Setup	Configure a PoE interface.	Configure

Introduction to the Controls on the Web Pages

Apply button

Click the button to submit and apply the input information.

Cancel button

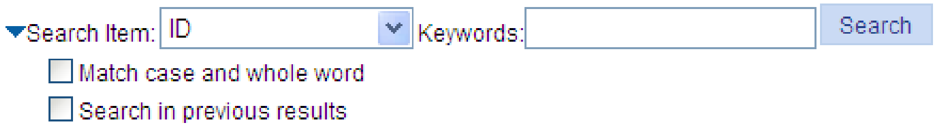
Click the button to cancel the input information. The page changes to the display page of the function or to the **Device Info** page.

Search button

Select an item to be queried, input the keyword, and click the **Query** button to display the items that meet the requirements.

The advance search function is also provided. You can click ▶ before **Search Item**, as shown in Figure 2-5. You can select **Match case and whole word**, that is, the item to be searched must completely match the keyword, or you can select **Search in previous results**. If you do not select exact search, fuzzy search is performed.

Figure 2-5 Advanced search



▼Search Item: ID Keywords: Search

□ Match case and whole word

□ Search in previous results

Refresh button

Click the button to refresh the display information of the current page.

Clear button

Click the button to clear all the items in a list or all statistics.

Remove button

Click the button to remove the selected items.

Select All button

Click the button to select all the items in a list, or all the ports on the device panel.

Select None button

Click the button to deselect all the items in a list, or all the ports on the device panel.

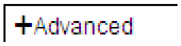
Restore button

Click the button to restore all the items in the current configuration page to the system default.

Expand button

As shown in Figure 2-6, click the plus sign before a corresponding item. You can see the collapsed contents.

Figure 2-6 Expand button



📝 icon

Click the icon to enter the modification page of an item to modify the configurations of the item.

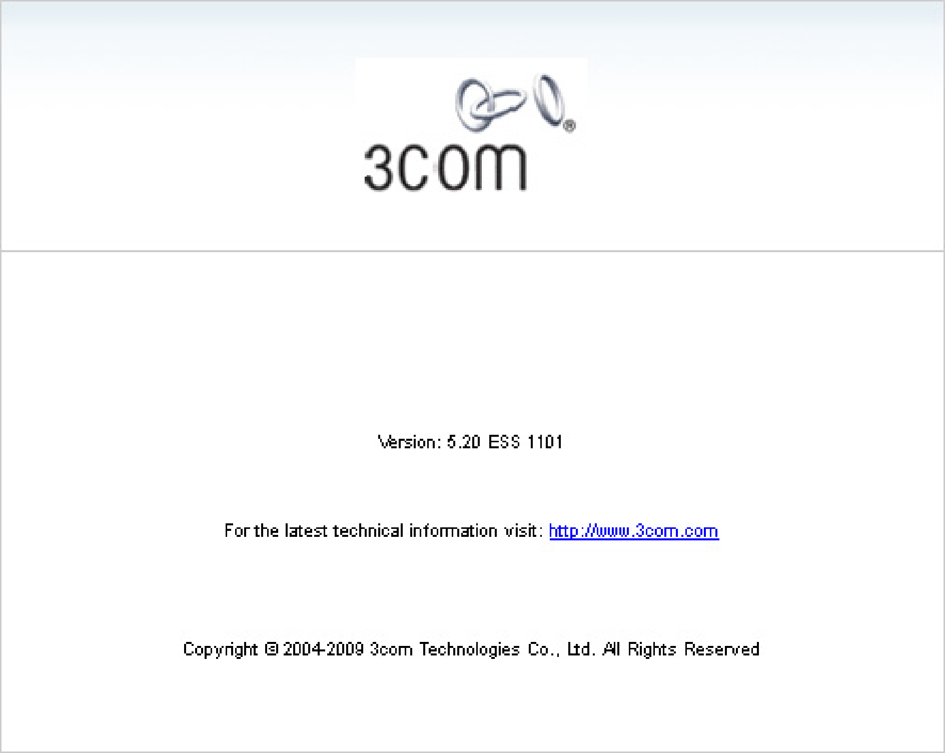
🗑 icon

Click the icon to delete the item corresponding to this icon.

Help button

Click the button to open the page, as shown in Figure 2-8.

Figure 2-7 About



Version: 5.20 ESS 1101

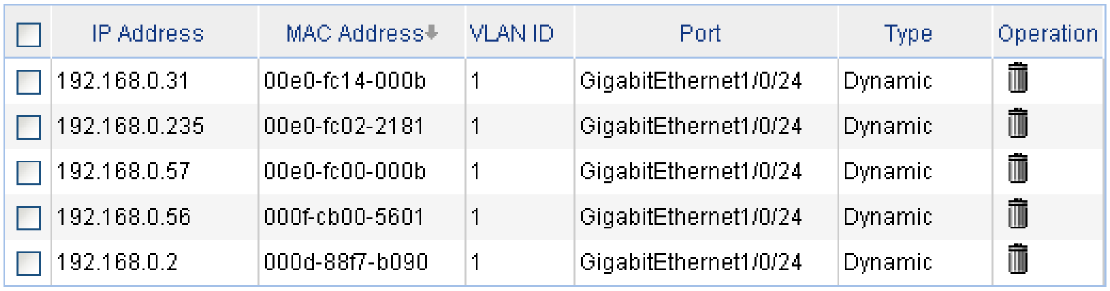
For the latest technical information visit: http://www.3com.com

Copyright © 2004-2009 3com Technologies Co., Ltd. All Rights Reserved

Sort display

On the page, you can click the blue items of each column to sort and display the records based on the item you selected.

Figure 2-8 Sort display



□	IP Address	MAC Address⇩	VLAN ID	Port	Type	Operation
□	192.168.0.31	00e0-fc14-000b	1	GigabitEthernet1/0/24	Dynamic	🗑
□	192.168.0.235	00e0-fc02-2181	1	GigabitEthernet1/0/24	Dynamic	🗑
□	192.168.0.57	00e0-fc00-000b	1	GigabitEthernet1/0/24	Dynamic	🗑
□	192.168.0.56	000f-cb00-5601	1	GigabitEthernet1/0/24	Dynamic	🗑
□	192.168.0.2	000d-88f7-b090	1	GigabitEthernet1/0/24	Dynamic	🗑

Configuration Guidelines

- The Web-based console supports Microsoft Internet Explorer 6.0 SP2 and higher, but it does not support the **Back**, **Next**, **Refresh** buttons provided by the browser. Using these buttons may result in abnormal display of Web pages.
- When the device is performing spanning tree calculation, you cannot log in to or use the Web interface.
- As the Windows firewall limits the number of TCP connections, when you use IE to log in to the Web interface, sometimes you may be unable to open the Web interface. To avoid this problem, it is recommended to turn off the Windows firewall before login.

- If the software version of the device changes, when you log in to the device through the Web interface, you are recommended to delete the temporary Internet files of IE; otherwise, the Web page content may not be displayed correctly.

3 Configuration Through the Command Line Interface

Note

- The 3Com baseline switch 2900 family can be configured through the command line interface (CLI), web interface, and SNMP/MIB, among which the web interface supports all switch 2900 series configurations. These configuration methods are suitable for different application scenarios. As a supplementary to the web interface, the CLI provides some configuration commands to facilitate your operation, which are described in this chapter. To perform other configurations not supported by the CLI, use the web interface.
- You will enter user view directly after you log in to the device. Commands in the document are all performed in user view.

Getting Started with the Command Line Interface

As a supplementary to the web interface, the CLI provides some configuration commands to facilitate your operation. For example, if you forget the IP address of VLAN-interface 1 and cannot log in to the device through the Web interface, you can connect the console port of the device to a PC, and reconfigure the IP address of VLAN-interface 1 through the CLI.

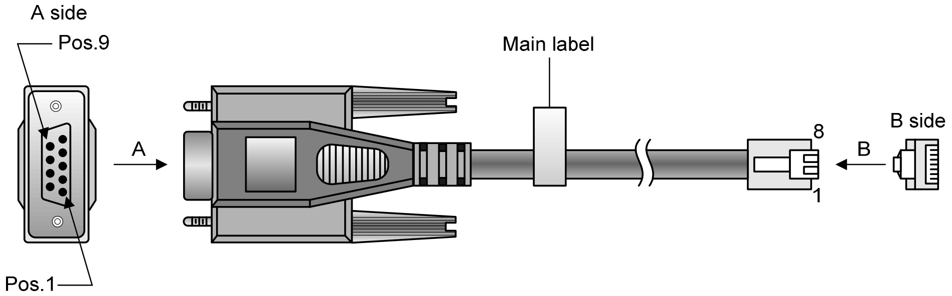
This section describes using the CLI to manage the device.

Setting Up the Configuration Environment

Set up the configuration environment as follows:

Step1 Take the console cable out of the package. (A console cable is an 8-core shielded cable. One end of the cable is a crimped RJ-45 connector, which is connected to the console port of the switch, and the other end is a DB-9 female connector, which is connected to the serial port on the console terminal, as shown below.)

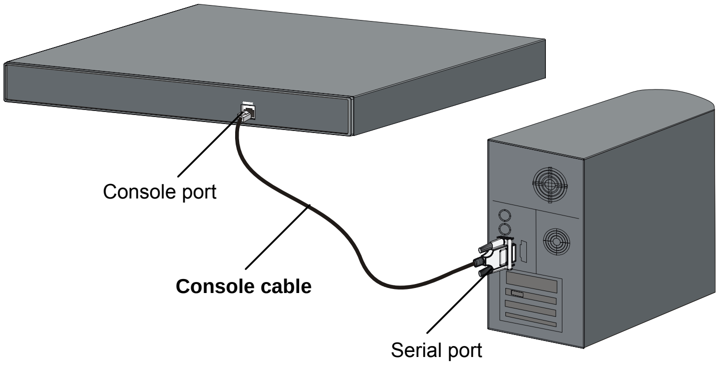
Figure 3-1 Console cable



Step2 Plug the DB-9 female connector of the console cable to the serial port of the console terminal or PC.

Step3 Connect the RJ-45 connector of the console cable to the console port of the switch. (as shown below)

Figure 3-2 Network diagram for configuration environment setup



Caution

Pay attention to the mark on the console port and be sure to plug the connector to the correct port.

Note

- When connecting a PC to a powered-on switch, you are recommended to connect the DB-9 connector of the console cable to the PC before connecting the RJ-45 connector to the switch.
- When disconnecting a PC from a powered-on switch, you are recommended to disconnect the DB-9 connector of the console cable from the PC after disconnecting the RJ-45 connector from the switch.

Setting Terminal Parameters

When setting up the configuration environment through the console port, the terminal or PC can use the terminal emulation program to communicate with the switch. You can run the HyperTerminal of the Windows operating system to connect to other PCs, network devices, and Telnet sites. For detailed information and the use of the HyperTerminal, refer to the HyperTerminal Help documentation in Help and Support Center on the PC running the Windows operating system.

In the following configuration procedure, Windows XP HyperTerminal is used to communicate with the switch.

1) Start the PC and run the terminal emulation program.

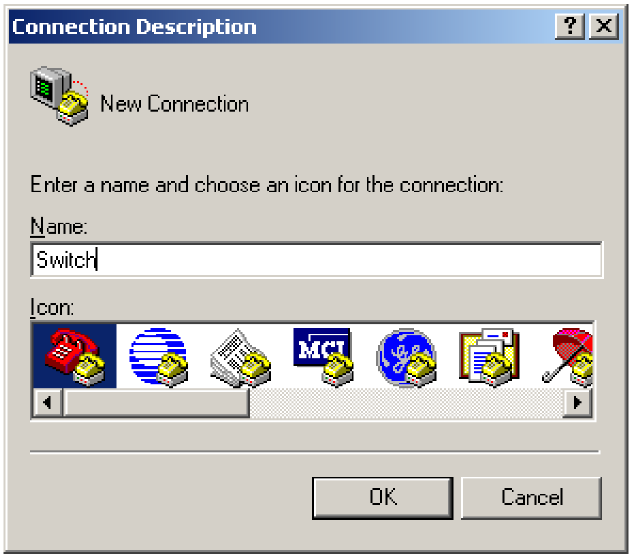
2) Set terminal parameters as follows:

- Bits per second: 38,400
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None
- Emulation: VT100

The specific procedure is as follows:

Step1 Select **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal** to enter the HyperTerminal window. The **Connection Description** dialog box appears, as shown below.

Figure 3-3 Connection description of the HyperTerminal

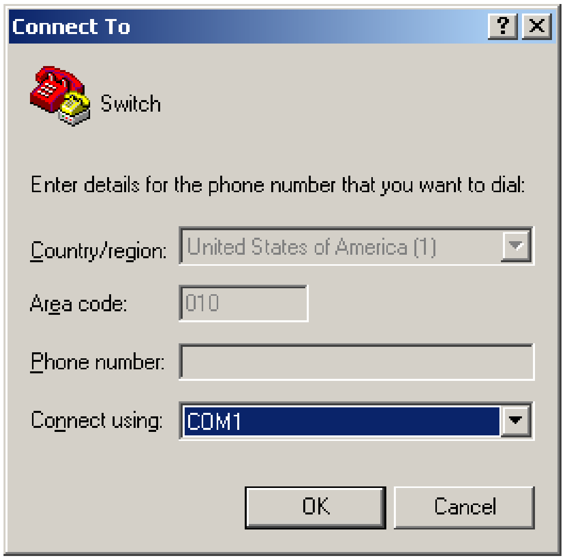


Enter a name and choose an icon for the connection:

Name: Switch

Step2 Type the name of the new connection in the **Name** text box and click **OK**. The following dialog box appears. Select the serial port to be used from the **Connect using** drop-down list.

Figure 3-4 Set the serial port used by the HyperTerminal connection



Connect To

Switch

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

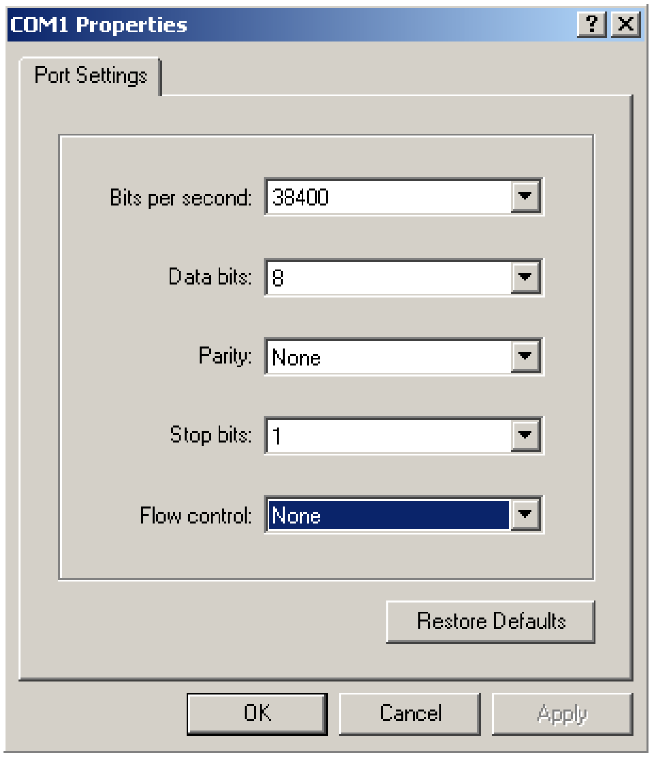
Area code: 010

Phone number:

Connect using: COM1

Step3 Click **OK** after selecting a serial port. The following dialog box appears. Set **Bits per second** to **38400**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**.

Figure 3-5 Set the serial port parameters



COM1 Properties

Port Settings

Bits per second: 38400

Data bits: 8

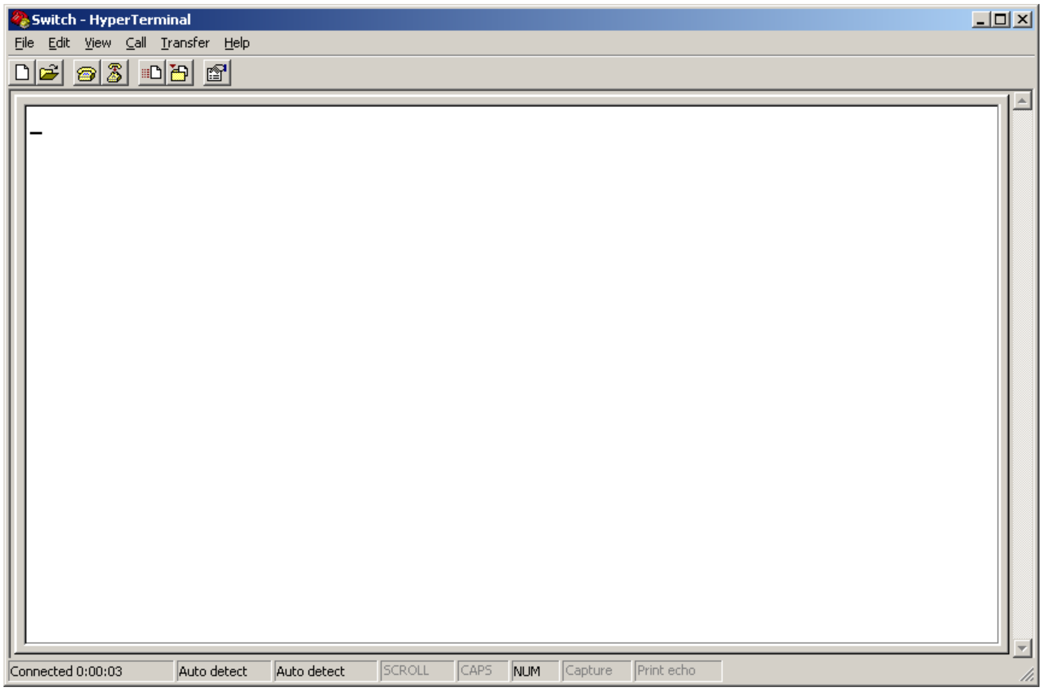
Parity: None

Stop bits: 1

Flow control: None

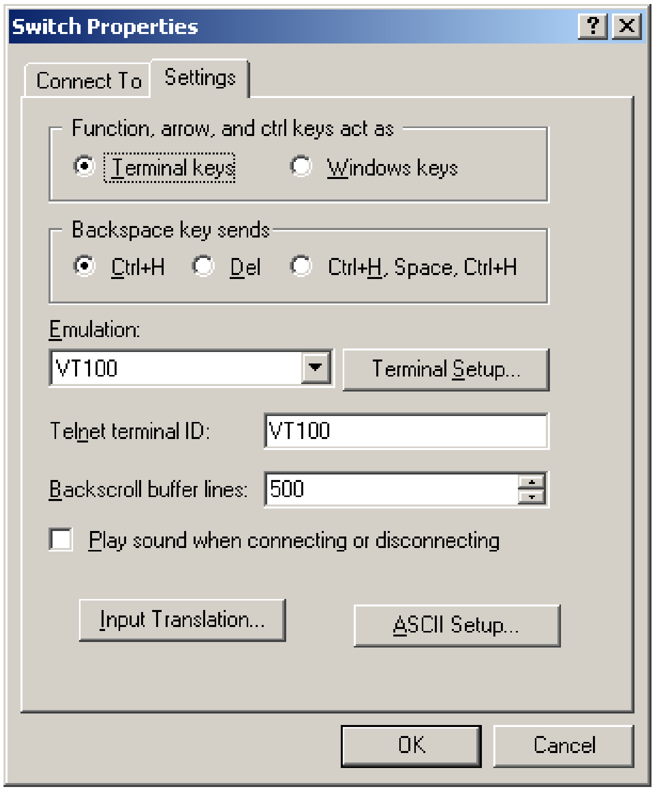
Step4 Click **OK** after setting the serial port parameters and the system enters the HyperTerminal window shown below.

Figure 3-6 HyperTerminal window



Step5 Click **Properties** in the HyperTerminal window to enter the **Switch Properties** dialog box. Click the **Settings** tab, set the emulation to **VT100**, and then click **OK**.

Figure 3-7 Set terminal emulation in Switch Properties dialog box



Function, arrow, and ctrl keys act as

● Terminal keys ○ Windows keys

Backspace key sends

● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

Logging In to the CLI

The login process requires a user name and password. The default user name for first time configuration is **admin**, no password is required. User names and passwords are case sensitive.

To logon to the CLI Interface:

Step1 Press **Enter**. The **Username** prompt displays:

```
Login authentication


Username:
```

Step2 Enter your User Name at the **Username** prompt.

```
Username:admin
```

Step3 Press **Enter**. The **Password** prompt display

```
Password:
```

The login information is verified, and displays the following CLI menu:

```
<3Com Baseline Switch>
```

If the password is invalid, the following message appears and process restarts.

```
% Login failed!
```

CLI Commands

This Command section contains the following commands:

To do…	Use the command…
Displays a list of CLI commands on the device	**?**
Reboot the device and run the default configuration	**initialize**
Specify VLAN-interface 1 to obtain an IP address through DHCP or manual configuration	**ipsetup** { **dhcp | ip address** *ip-address* { *mask* | *mask-length* } [**default-gateway** *ip-address*] }
Modify the login password of a user	**password**
Download the Boot ROM program or boot file from the TFTP server and specify it to be used at the next startup	**upgrade** *server-address source-filename* { **bootrom | runtime** }
Reboot the device and run the main configuration file	**reboot**
View the summary information of the device	**summary**
Ping a specified destination	**ping** *host*

initialize

Syntax

initialize

Parameters

None

Description

Use the **initialize** command to delete the configuration file to be used at the next startup and reboot the device with the default configuration being used during reboot.

Use the command with caution because this command deletes the configuration file to be used at the next startup and restores the factory default settings.

Examples

# Delete the configuration file to be used at the next startup and reboot the device with the default configuration being used during reboot.

```
<Sysname> initialize
 The startup configuration file will be deleted and the system will be rebooted.Continue?
[Y/N]:y
 Please wait...
```

ipsetup

Syntax

ipsetup { **dhcp** | **ip address** *ip-address* { *mask* | *mask-length* } [**default-gateway** *ip-address*] }

Parameters

dhcp: Specifies the interface to obtain an IP address through DHCP.

ip-address *ip-address*: Specifies an IP address for VLAN-interface 1 in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask, in the range of 0 to 32.

default-gateway *ip-address*: Specifies the IP address of the default gateway or the IP address of the outbound interface. With this argument and keyword combination configured, the command not only assigns an IP address to the interface, but also specifies a default route for the device.

Description

Use the **ipsetup dhcp** command to specify VLAN-interface 1 to obtain an IP address through DHCP.

Use the **ipsetup ip address** *ip-address* { *mask* | *mask-length* } command to assign an IP address to VLAN-interface 1.

By default, the device automatically obtains its IP address through DHCP; if fails, it uses the assigned default IP address. See Figure 2-2 for details.

If there is no VLAN-interface 1, either command creates VLAN-interface 1 first, and then specifies its IP address.

Examples

# Create VLAN-interface 1 and specify the interface to obtain an IP address through DHCP.

```
<Sysname> ipsetup dhcp
```

# Create VLAN-interface 1 and assign 192.168.1.2 to the interface, and specify 192.168.1.1 as the default gateway.

```
<Sysname> ipsetup ip-address 192.168.1.2 24 default-gateway 192.168.1.1
```

password

Syntax

password

Parameters

None

Description

Use the **password** command to modify the login password of a user.

Examples

# Modify the login password of user admin.

```
<Sysname> password
Change password for user: admin
Old password: ***
Enter new password: **
Retype password: **
The password has been successfully changed.
```

ping

Syntax

ping *host*

Parameters

host: Destination IP address (in dotted decimal notation), URL, or host name (a string of 1 to 20 characters).

Description

Use the **ping** command to ping a specified destination.

You can enter **Ctrl+C** to terminate a ping operation.

Examples

# Ping IP address 1.1.2.2.

```
<Sysname> ping 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/41/205 ms
```

The above information shows that IP address 1.1.2.2 is reachable and the echo replies are all returned from the destination. The minimum, average, and maximum roundtrip intervals are 1 millisecond, 41 milliseconds, and 205 milliseconds respectively.

quit

Syntax

quit

Parameters

None

Description

Use the **quit** command to log out of the system.

Examples

# Log out of the system.

```
<Sysname> quit
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
******************************************************************************

User interface aux0 is available.



Please press ENTER.
```

reboot

Syntax

reboot

Parameters

None

Description

Use the **reboot** command to reboot the device and run the main configuration file.

Note that:

- Use the command with caution because reboot results in service interruption.

- If the main configuration file is corrupted or does not exist, the device cannot be rebooted with the **reboot** command. In this case, you can specify a new main configuration file to reboot the device, or you can power off the device, and then power it on, and the system will automatically use the backup configuration file at the next startup.
- If you reboot the device when file operations are being performed, the system does not execute the command to ensure security.

Examples

# If the configuration does not change, reboot the device.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.........DONE!
 This command will reboot the device. Continue? [Y/N]:y
 Now rebooting, please wait...
```

# If the configuration changes, reboot the device.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.........DONE!
 This command will reboot the device. Current configuration will be lost in next startup if
you continue. Continue? [Y/N]:y
 Now rebooting, please wait...
```

summary

Syntax

summary

Parameters

None

Description

Use the **summary** command to view the summary information of the device, including the IP address of VLAN-interface 1, and software version information.

Examples

# Display summary information of the device.

```
<Sysname> summary
Select menu option:              Summary
IP Method:                       DHCP
IP address:                      10.153.96.86
Subnet mask:                     255.255.255.0
Default gateway:                 0.0.0.0

Current boot app is: flash:/2900_release.bin
Next main boot app is: NULL
Next backup boot app is: NULL

3Com Corporation
3Com Baseline Switch 2928-PWR Plus Software Version 5.20 ESS 1101
```

```
Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
3Com Baseline Switch 2928-PWR Plus uptime is 0 week, 0 day, 3 hours, 11 minutes

3Com Baseline Switch 2928-PWR Plus
128M    bytes DRAM
128M    bytes Nand Flash Memory
Config Register points to Nand Flash

Hardware Version is REV.B
CPLD Version is 001
Bootrom Version is  112
[SubSlot 0] 24GE+4SFP+POE Hardware Version is REV.B
```

upgrade

Syntax

upgrade *server-address source-filename* { **bootrom** | **runtime** }

Parameters

server-address: IP address or host name (a string of 1 to 20 characters) of a TFTP server.

source-filename: Software package name on the TFTP server.

bootrom: Specifies the Boot ROM file in the software package to be used at the next startup.

runtime: Specifies the boot file in the software package to be used at the next startup.

Description

Use the **upgrade** *server-address source-filename* **bootrom** command to upgrade the Boot ROM file. If the Boot ROM file in the downloaded software package is not applicable, the original Boot ROM program is still used at the next startup.

Use the **upgrade** *server-address source-filename* **runtime** command to upgrade the boot file. If the boot file in the downloaded software package is not applicable, the original boot file is still used at the next startup.

To make the downloaded package take effect, you need to reboot the device.

Note

The Switch 2900 series does not provide an independent Boot ROM file; instead, it integrates the Boot ROM file with the boot file together in a software package with the extension name of **.bin**.

Examples

# Download software package **main.bin** from the TFTP server and use the Boot ROM file in the package at the next startup.

```
<Sysname> upgrade 192.168.20.41 main.bin bootrom
```

# Download software package **main.bin** from the TFTP server and use the boot file in the package at the next startup.

```
<Sysname> upgrade 192.168.20.41 main.bin runtime
```

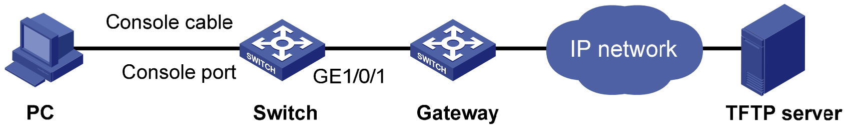
Configuration Example for Upgrading the Host Software Through the CLI

Network requirements

As shown in Figure 3-8, a Switch 2900 series switch is connected to the PC through the console cable, and connected to the gateway through GigabitEthernet 1/0/1. The IP address of the gateway is 192.168.1.1/24, and that of the TFTP server where the host software (suppose its name is **Switch2900.bin**) is located is 192.168.10.1/24. The route between the gateway and the switch is reachable.

The administrator upgrades the Boot ROM and the system boot file of the 2900 switch through the configuration PC and sets the IP address of the switch to 192.168.1.2/24.

Figure 3-8 Network diagram for upgrading the host software of the 2900 switch through CLI



Configuration procedure

1) Run the TFTP server program on the TFTP server, and specify the path of the program to be loaded. (Omitted)
2) Perform the following configurations on the switch.

# Configure the IP address of VLAN-interface 1 of the switch as 192.168.1.2/24, and specify the default gateway as 192.168.1.1.

```
<Switch> ipsetup ip-address 192.168.1.2 24 default-gateway 192.168.1.1
```

# Download the host software package **Switch2900.bin** on the TFTP server to the switch, and specify it as the boot file for the next system boot.

```
<Switch> upgrade 192.168.10.1 Switch2900.bin runtime
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP:   253700 bytes received in 2 second(s)
  File downloaded successfully.
   BootRom file updating finished!
```

# Download the host software package **Switch2900.bin** on the TFTP server to the switch, and specify it as the Boot ROM file for the next system boot.

```
<Switch> upgrade 192.168.10.1 Switch2900.bin bootrom
The file flash:/ Switch2900.bin exists. Overwrite it? [Y/N]:y
  Verifying server file...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait.../
  TFTP:  9711592 bytes received in 186 second(s)
  File downloaded successfully.
  The specified file will be used as the boot file at the next reboot.
```

# Reboot the switch.

```
<Switch> reboot
```

After getting the new application file, reboot the switch to have the upgraded application take effect.

Table of Contents

1 Configuration Wizard

Overview

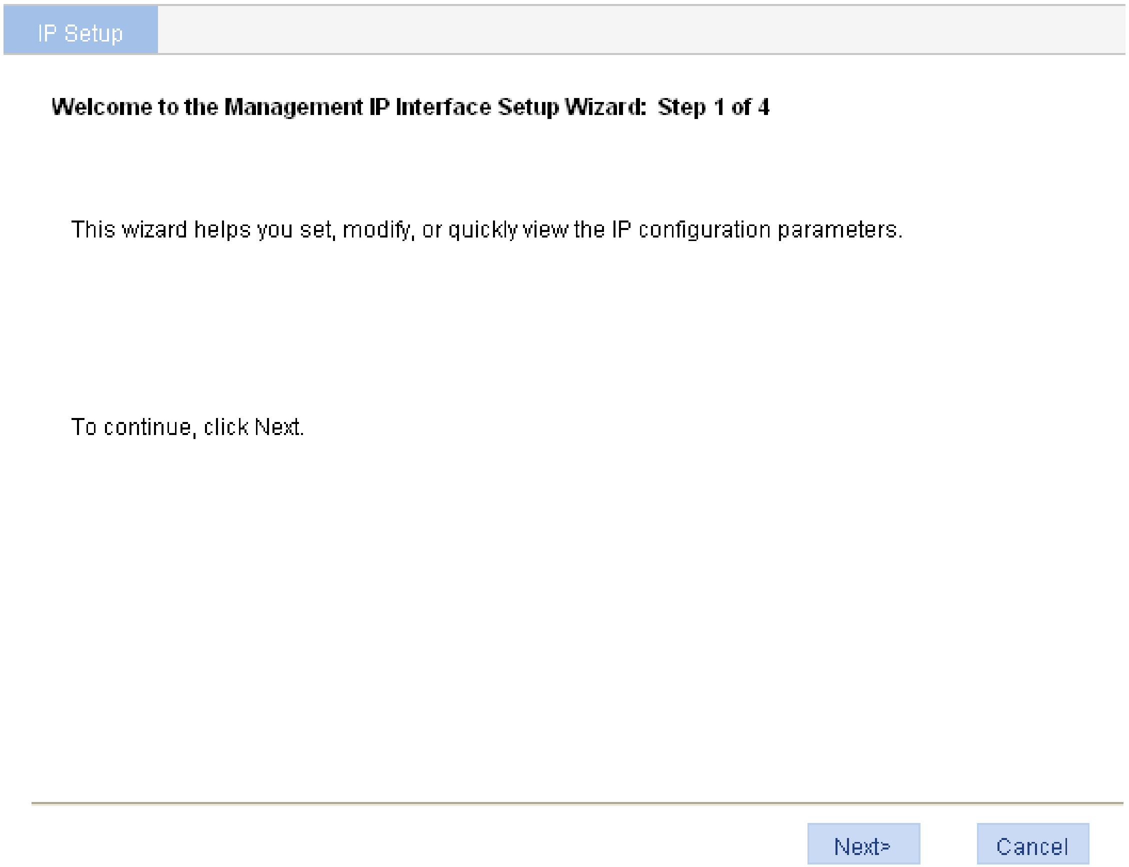
The configuration wizard guides you through the basic service setup, including the system name, system location, contact information, and management IP address (IP address of the VLAN interface).

Basic Service Setup

Entering the Configuration Wizard Homepage

From the navigation tree, select **Wizard** to enter the configuration wizard homepage, as shown in Figure 1-1.

Figure 1-1 Configuration wizard homepage



Welcome to the Management IP Interface Setup Wizard: Step 1 of 4

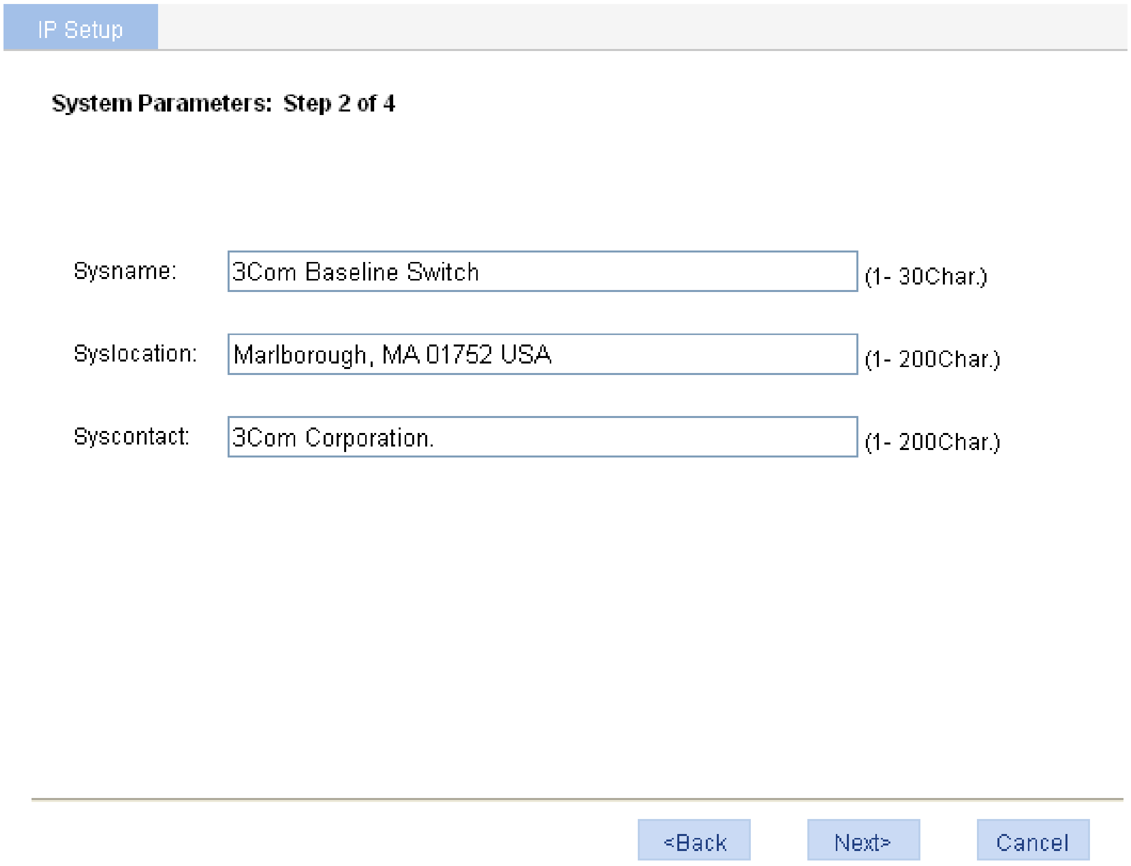
This wizard helps you set, modify, or quickly view the IP configuration parameters.

To continue, click Next.

Configuring System Parameters

In the wizard homepage, click **Next** to enter the system parameter configuration page, as shown in Figure 1-2.

Figure 1-2 System parameter configuration page



System Parameters: Step 2 of 4

Sysname: 3Com Baseline Switch (1- 30Char.)

Syslocation: Marlborough, MA 01752 USA (1- 200Char.)

Syscontact: 3Com Corporation. (1- 200Char.)

Table 1-1 describes the system parameter configuration items.

Table 1-1 System parameter configuration items

Item	Description
Sysname	Specify the system name. The system name appears at the top of the navigation tree. You can also set the system name in the **System Name** page you enter by selecting **Device** > **Basic**. For details, refer to *Device Basic Information Configuration*.
Syslocation	Specify the physical location of the system. You can also set the physical location in the setup page you enter by selecting **Device** > **SNMP**. For details, refer to *SNMP Configuration.*
Syscontact	Set the contact information for users to get in touch with the device vendor for help. You can also set the contact information in the setup page you enter by selecting **Device** > **SNMP**. For details, refer to *SNMP Configuration*.

Configuring Management IP Address

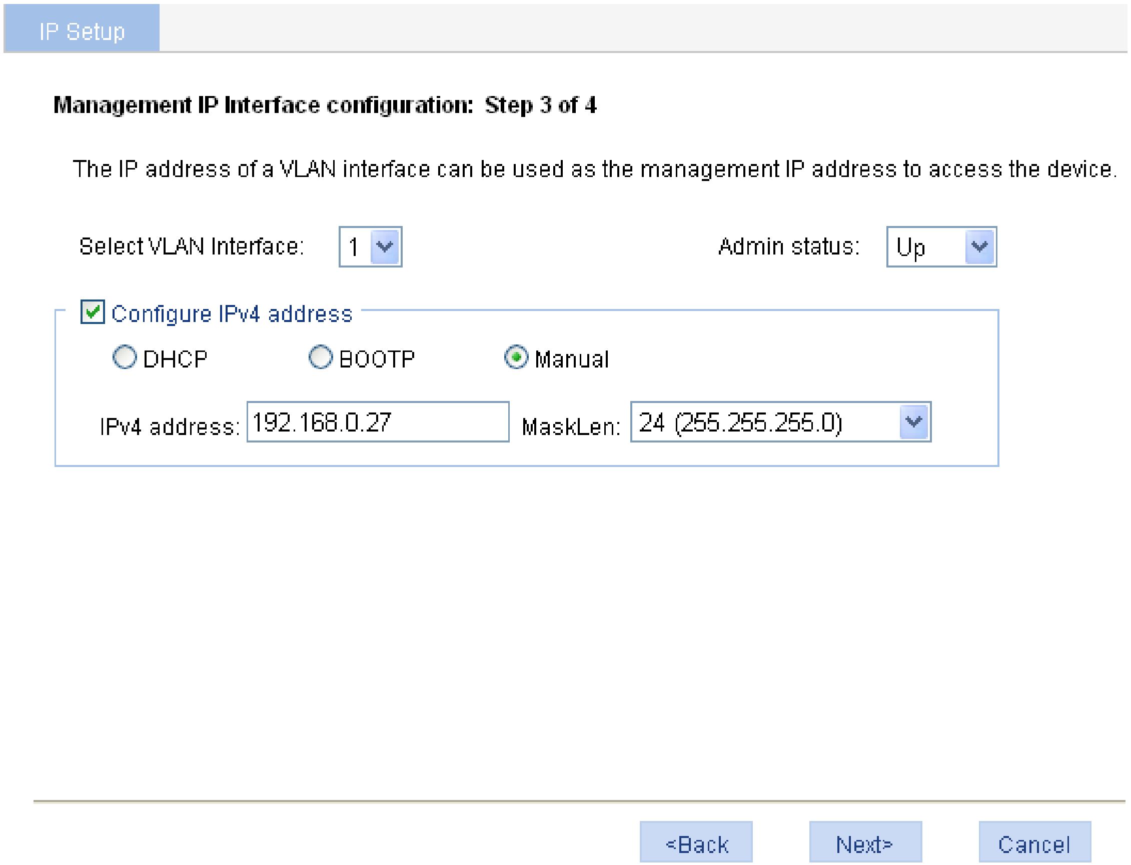
Caution

Modifying the management IP address used for the current login will tear down the connection to the device. Use the new management IP address to re-log in to the system.

A management IP address is the IP address of a VLAN interface, which can be used to access the device. You can also set configure a VLAN interface and its IP address in the page you enter by selecting **Network** > **VLAN Interface**. For configuration details, refer to *VLAN Interface Configuration*.

After finishing the configuration, click **Next** to enter the management IP address configuration page, as shown in Figure 1-3.

Figure 1-3 Management IP address configuration page



Management IP Interface configuration: Step 3 of 4

The IP address of a VLAN interface can be used as the management IP address to access the device.

Select VLAN Interface: 1

Admin status: Up

☑ Configure IPv4 address

○ DHCP ○ BOOTP ● Manual

IPv4 address: 192.168.0.27

MaskLen: 24 (255.255.255.0)

Table 1-2 describes the configuration items for configuring a management IP address.

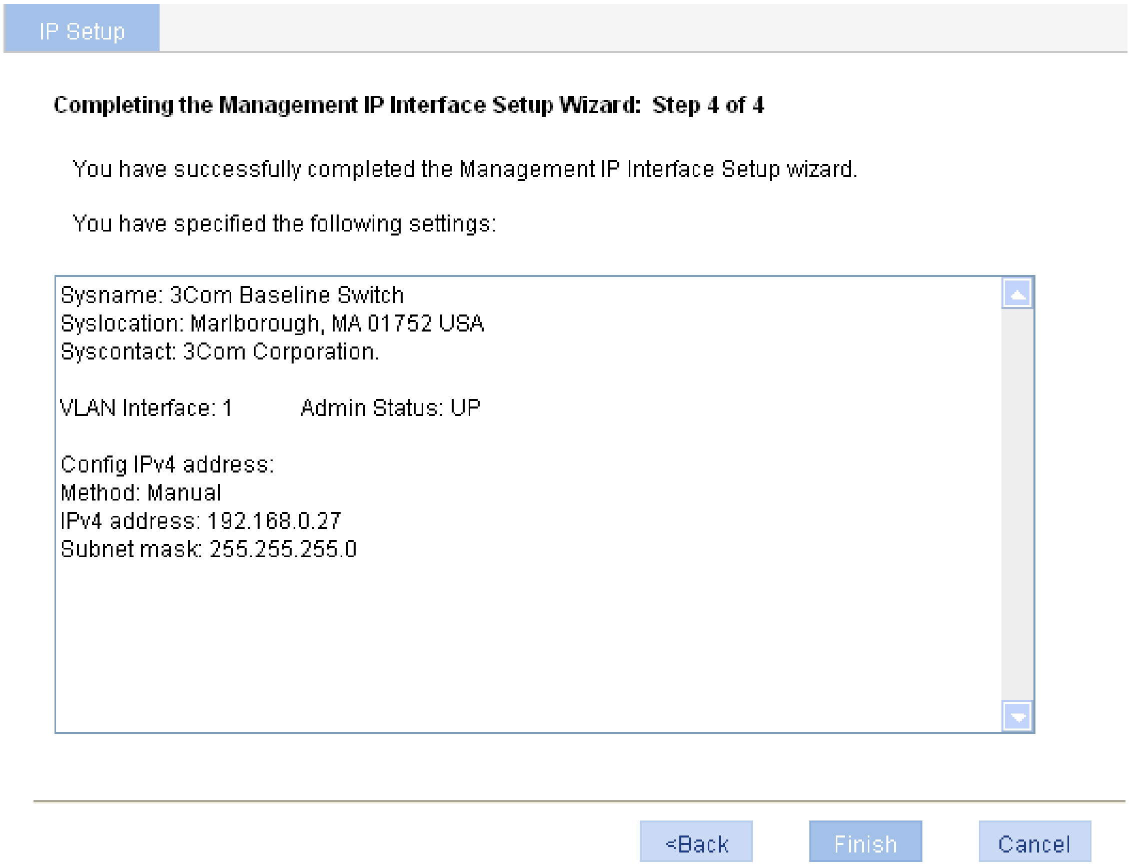
Table 1-2 Management IP address configuration items

Item	Description	
Select VLAN Interface	Select a VLAN interface. Available VLAN interfaces are those configured in the page you enter by selecting **Network** > **VLAN Interface** and selecting the **Create** tab.	
Admin Status	Enable or disable the VLAN interface. When errors occurred on the VLAN interface, disable the interface and then enable the port to bring the port to work properly. By default, the VLAN interface is down if no Ethernet ports in the VLAN is up. The VLAN is in the up state if one or more ports in the VLAN are up. **Highlight** *Disabling or enabling the VLAN interface does not affect the status of the Ethernet ports in the VLAN. That is, the port status does not change with the VLAN interface status.*	
Configure IPv4 address	DHCP	Configure how the VLAN interface obtains an IPv4 address. • DHCP: Specifies the VLAN interface to obtain an IPv4 address by DHCP. • BOOTP: Specifies the VLAN interface to obtain an IPv4 address through BOOTP. • Manual: Allows you to specify an IPv4 address and a mask length. **Highlight** *Support for IPv4 obtaining methods depends on the device model.*
	BOOTP	
	Manual	
	IPv4 address	Specify an IPv4 address and the mask length for the VLAN interface. These two text boxes are configurable if **Manual** is selected.
	MaskLen	

Finishing Configuration Wizard

After finishing the management IP address configuration, click **Next**, as shown in Figure 1-4.

Figure 1-4 Configuration finishes



Completing the Management IP Interface Setup Wizard: Step 4 of 4

You have successfully completed the Management IP Interface Setup wizard.

You have specified the following settings:

```
Sysname: 3Com Baseline Switch
Syslocation: Marlborough, MA 01752 USA
Syscontact: 3Com Corporation.

VLAN Interface: 1          Admin Status: UP

Config IPv4 address:
Method: Manual
IPv4 address: 192.168.0.27
Subnet mask: 255.255.255.0
```

The page displays your configurations. Review the configurations and if you want to modify the settings click **Back** to go back to the page. Click **Finish** to confirm your settings and the system performs the configurations.

Table of Contents

1 IRF

IRF Overview

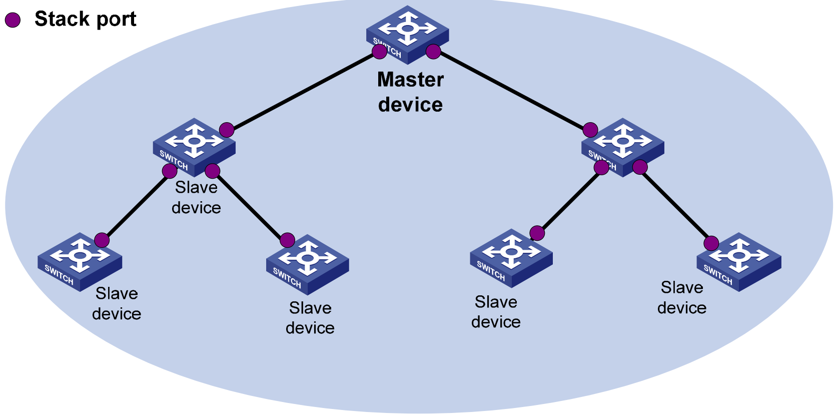
An Intelligent Resilient Framework (IRF) stack is a set of network devices. Administrators can group multiple network devices into a stack and manage them as a whole. Therefore, stack management can help reduce customer investments and simplify network management.

Introduction to Stack

A stack is a management domain that comprises several network devices connected to one another through stack ports. In a stack, there is a master device and several slave devices.

An administrator can manage all the devices in a stack through the master device. Figure 1-1 shows a network diagram for stack management.

Figure 1-1 Network diagram for stack management



- Master device: In a stack, the master device acts as the configuration interface in stack management. Management and monitoring of all the devices in the stack are performed through the master device.
- Slave devices: Managed devices in a stack.
- Stack port: Ports between stack devices.

Establishing a Stack

An administrator can establish a stack as follows:

- Configure a private IP address pool for a stack and create the stack on the network device which is to be configured as the master device.
- Configure ports between the stack devices as stack ports.
- The master device automatically adds the slave devices into the stack, and allocates a private IP address and a member ID for each slave device.

- The administrator can log in to any slave device from the master device of the stack, and perform various configurations for the slave device.

Configuring an IRF Stack

Configuration Task List

Perform the tasks in Table 1-1 to configure an IRF stack.

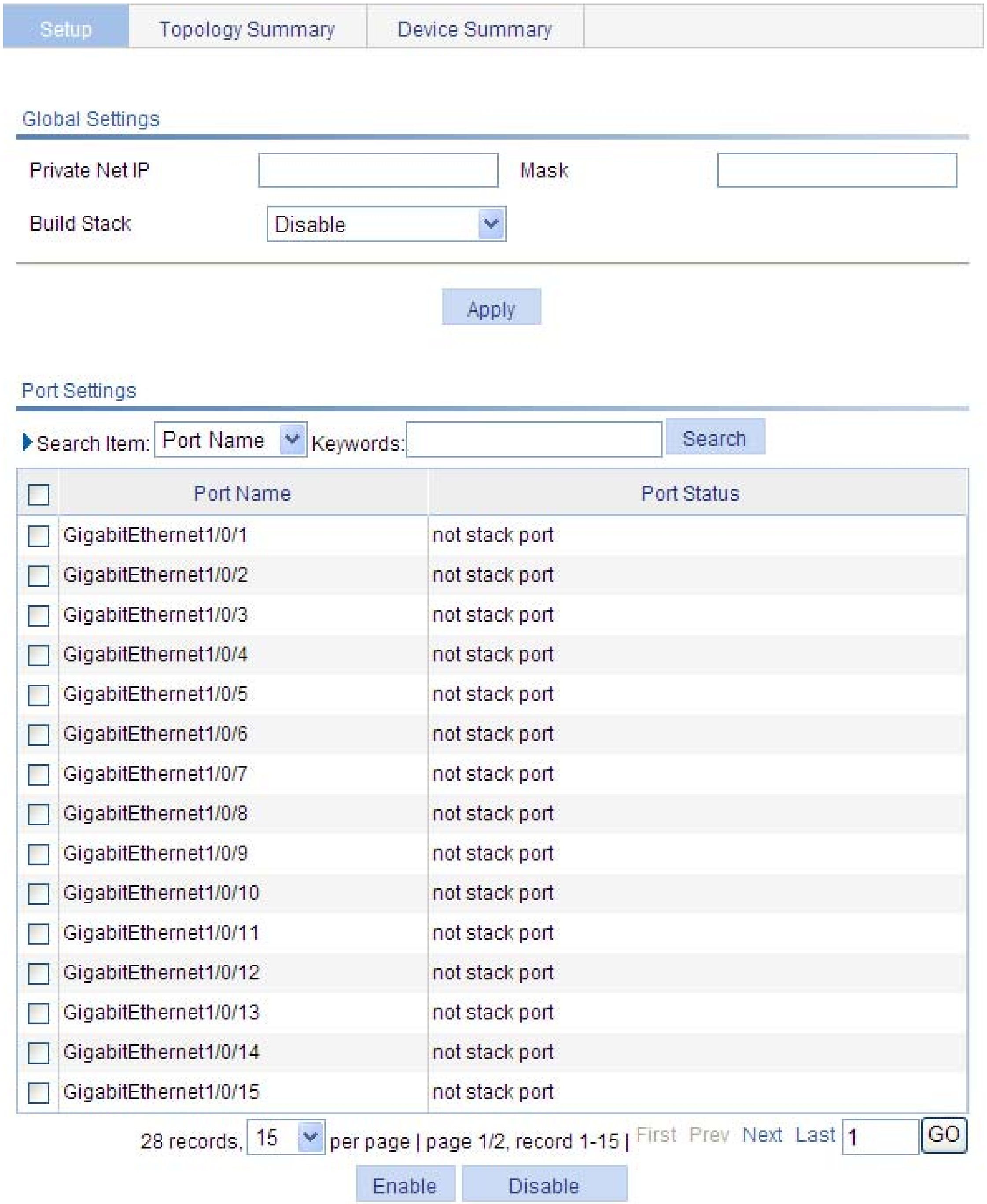
Table 1-1 Stack configuration task list

Task		Remarks
Configuring the master device of a stack	Configuring Global Parameters of a Stack	Required Configure a private IP address pool for a stack and establish the stack, and meantime the device becomes the master device of the stack. By default, no IP address pool is configured for a stack and no stack is established.
	Configuring Stack Ports	Required Configure the ports of the master device that connect to slave devices as stack ports. By default, a port is not a stack port.
Configuring slave devices of a stack	Configuring Stack Ports	Required Configure a port of a slave device that connects to the master device or another slave device as a stack port. By default, a port is not a stack port.
Displaying Topology Summary of a Stack		Optional Display the information of stack members.
Displaying Device Summary of a Stack		Optional Display the control panels of stack members. **Highlight** *Before viewing the control panel of a slave device, you must ensure that the username, password, and access right you used to log on to the master device are the same with those configured on the slave device; otherwise, the control panel of the slave device cannot be displayed.*
Logging Into a Slave Device From the Master		Optional Log in to the web network management interface of a slave device from the master device. **Highlight** *Before logging into a slave device, you must ensure that the username, password, and access right you used to log on to the master device are the same with those configured on the slave device; otherwise, you cannot log into the slave device. You can configure them by selecting **Device** and then clicking **Users** from the navigation tree.*

Configuring Global Parameters of a Stack

Select **IRF** from the navigation tree to enter the page shown in Figure 1-2. You can configure global parameters of a stack in the **Global Settings** area.

Figure 1-2 Set up



Private Net IP	
Mask	
Build Stack	Disable

Search Item: Port Name Keywords:

□	Port Name	Port Status
□	GigabitEthernet1/0/1	not stack port
□	GigabitEthernet1/0/2	not stack port
□	GigabitEthernet1/0/3	not stack port
□	GigabitEthernet1/0/4	not stack port
□	GigabitEthernet1/0/5	not stack port
□	GigabitEthernet1/0/6	not stack port
□	GigabitEthernet1/0/7	not stack port
□	GigabitEthernet1/0/8	not stack port
□	GigabitEthernet1/0/9	not stack port
□	GigabitEthernet1/0/10	not stack port
□	GigabitEthernet1/0/11	not stack port
□	GigabitEthernet1/0/12	not stack port
□	GigabitEthernet1/0/13	not stack port
□	GigabitEthernet1/0/14	not stack port
□	GigabitEthernet1/0/15	not stack port

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Table 1-2 describes configuration items of global parameters.

Table 1-2 Configuration items of global parameters

Item	Description
Private Net IP	Configure a private IP address pool for the stack. The master device of a stack must be configured with a private IP address pool to ensure that it can automatically allocate an available IP address to a slave device when the device joints the stack. **Highlight** *When you configure a private IP address pool for a stack, the number of IP addresses in the address pool needs to be equal to or greater than the number of devices to be added to the stack. Otherwise, some devices may not be able to join the stack automatically for lack of private IP addresses.*
Mask	
Build Stack	Enable the device to establish a stack. After you enable the device to establish a stack, the device becomes the master device of the stack and automatically adds the devices connected to its stack ports to the stack. **Highlight** *You can delete a stack only on the master device of the stack. The **Global Settings** area on a slave device is grayed out.*

Return to Stack configuration task list.

Configuring Stack Ports

Select **IRF** from the navigation tree to enter the page shown in Figure 1-2. You can configure stack ports in the **Port Settings** area.

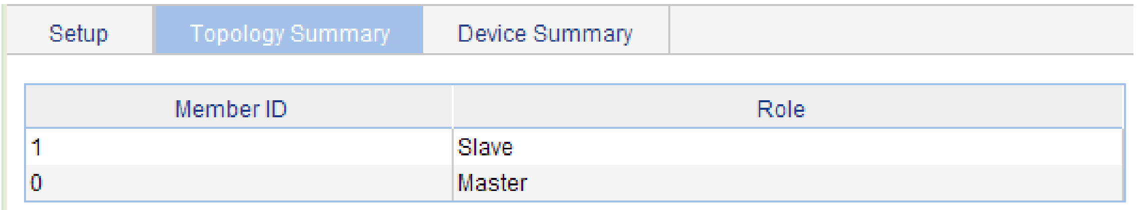
- Select the check box before a port name, and click **Enable** to configure the port as a stack port.
- Select the check box before a port name, and click **Disable** to configure the port as a non-stack port.

Return to Stack configuration task list.

Displaying Topology Summary of a Stack

Select **IRF** from the navigation tree and click the **Topology Summary** tab to enter the page shown in Figure 1-3.

Figure 1-3 Topology summary



Member ID	Role
1	Slave
0	Master

Table 1-3 describes the fields of topology summary.

Table 1-3 Fields of topology summary

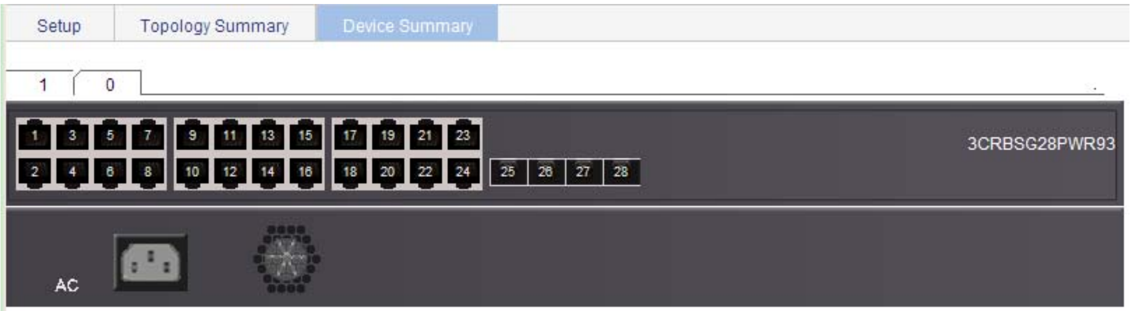
Fields	Description
Member ID	Member ID of the device in the stack: • Value 0 indicates that the device is the master device of the stack. • A value other than 0 indicates that the device is a slave device and the value is the member ID of the slave device in the stack.
Role	Role of the device in the stack: master or slave.

Return to Stack configuration task list.

Displaying Device Summary of a Stack

Select **IRF** from the navigation tree and click the **Device Summary** tab to enter the page shown in Figure 1-4. On this page, you can view interfaces and power socket layout on the panel of each stack member by clicking the tab of the corresponding member device.

Figure 1-4 Device summary (the master device)



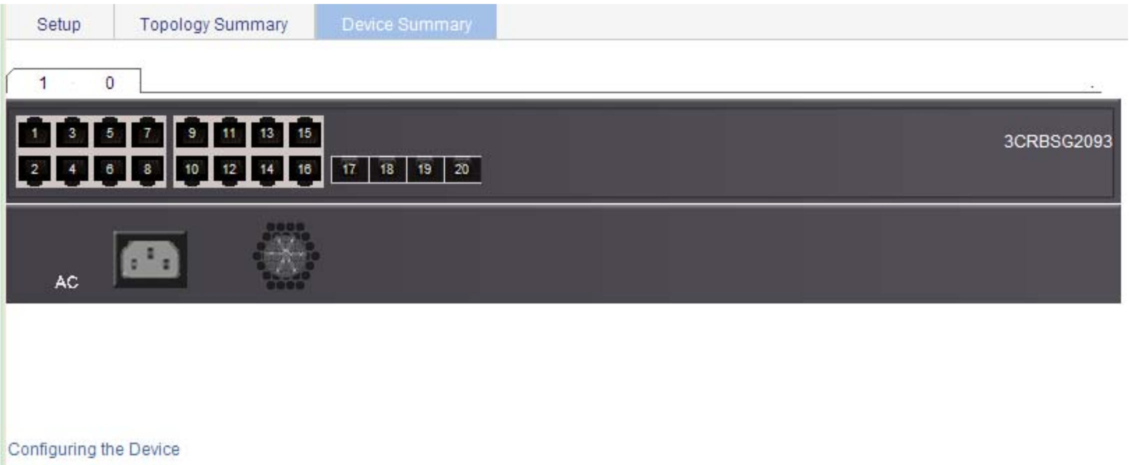
Return to Stack configuration task list.

Logging Into a Slave Device From the Master

Select **IRF** from the navigation tree, click the **Device Summary** tab, and click the tab of a slave device to enter the page shown in Figure 1-5.

Click the **Configuring the Device** hyperlink, you can log on to the web interface of the slave device to manage and maintain the slave device directly.

Figure 1-5 Device summary (a slave device)



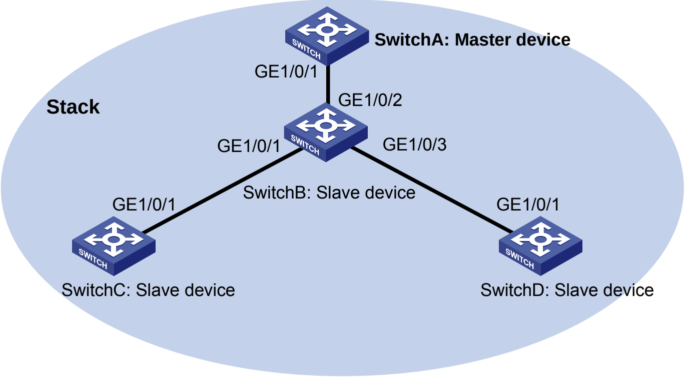
Return to Stack configuration task list.

IRF Stack Configuration Example

Network requirements

- As shown in Figure 1-6, Switch A, Switch B, Switch C, and Switch D are connected with one another.
- Create a stack, where Switch A is the master device, Switch B, Switch C, and Switch D are slave devices. An administrator can log in to Switch B, Switch C and Switch D through Switch A to perform remote configurations.

Figure 1-6 Network diagram for IRF stack



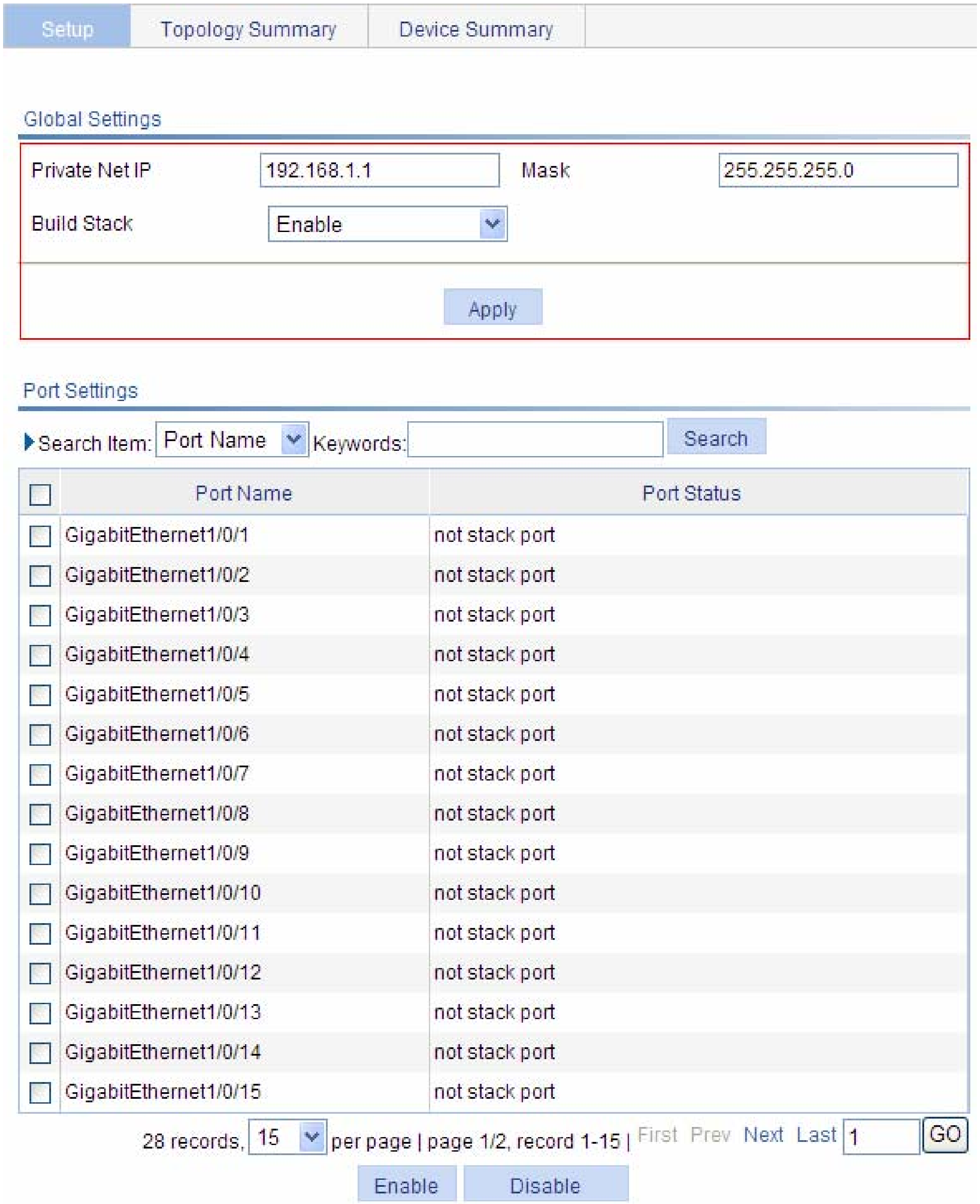
Configuration procedure

1) Configure the master device

# Configure global parameters for the stack on Switch A.

- Select **IRF** from the navigation tree of Switch A to enter the page of the **Setup** tab, and then perform the following configurations, as shown in Figure 1-7.

Figure 1-7 Configure global parameters for the stack on Switch A



Global Settings

Private Net IP	192.168.1.1	Mask	255.255.255.0
Build Stack	Enable		

Port Settings

Search Item: Port Name Keywords:

□	Port Name	Port Status
□	GigabitEthernet1/0/1	not stack port
□	GigabitEthernet1/0/2	not stack port
□	GigabitEthernet1/0/3	not stack port
□	GigabitEthernet1/0/4	not stack port
□	GigabitEthernet1/0/5	not stack port
□	GigabitEthernet1/0/6	not stack port
□	GigabitEthernet1/0/7	not stack port
□	GigabitEthernet1/0/8	not stack port
□	GigabitEthernet1/0/9	not stack port
□	GigabitEthernet1/0/10	not stack port
□	GigabitEthernet1/0/11	not stack port
□	GigabitEthernet1/0/12	not stack port
□	GigabitEthernet1/0/13	not stack port
□	GigabitEthernet1/0/14	not stack port
□	GigabitEthernet1/0/15	not stack port

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1

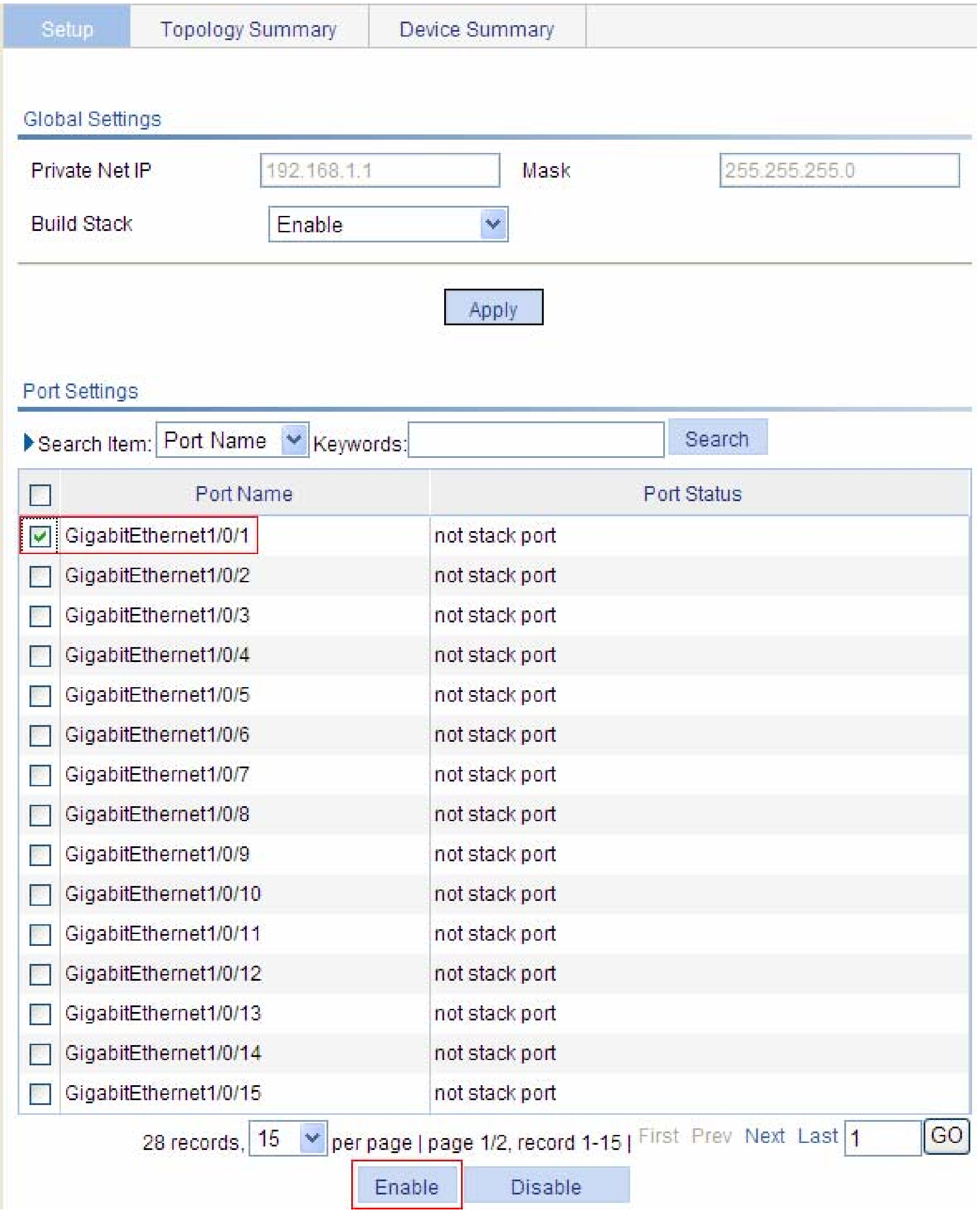
- Type **192.168.1.1** in the text box of **Private Net IP**.
- Type **255.255.255.0** in the text box of **Mask**.
- Select **Enable** from the **Build Stack** drop-down list.
- Click **Apply**.

Now, switch A becomes the master device.

# Configure a stack port on Switch A.

- On the page of the **Setup** tab, perform the following configurations, as shown in Figure 1-8.

Figure 1-8 Configure a stack port on Switch A



Global Settings

Private Net IP: 192.168.1.1 Mask: 255.255.255.0

Build Stack: Enable

Port Settings

Search Item: Port Name Keywords:

□	Port Name	Port Status
☑	GigabitEthernet1/0/1	not stack port
□	GigabitEthernet1/0/2	not stack port
□	GigabitEthernet1/0/3	not stack port
□	GigabitEthernet1/0/4	not stack port
□	GigabitEthernet1/0/5	not stack port
□	GigabitEthernet1/0/6	not stack port
□	GigabitEthernet1/0/7	not stack port
□	GigabitEthernet1/0/8	not stack port
□	GigabitEthernet1/0/9	not stack port
□	GigabitEthernet1/0/10	not stack port
□	GigabitEthernet1/0/11	not stack port
□	GigabitEthernet1/0/12	not stack port
□	GigabitEthernet1/0/13	not stack port
□	GigabitEthernet1/0/14	not stack port
□	GigabitEthernet1/0/15	not stack port

28 records, 15 per page | page 1/2, record 1-15 | 1

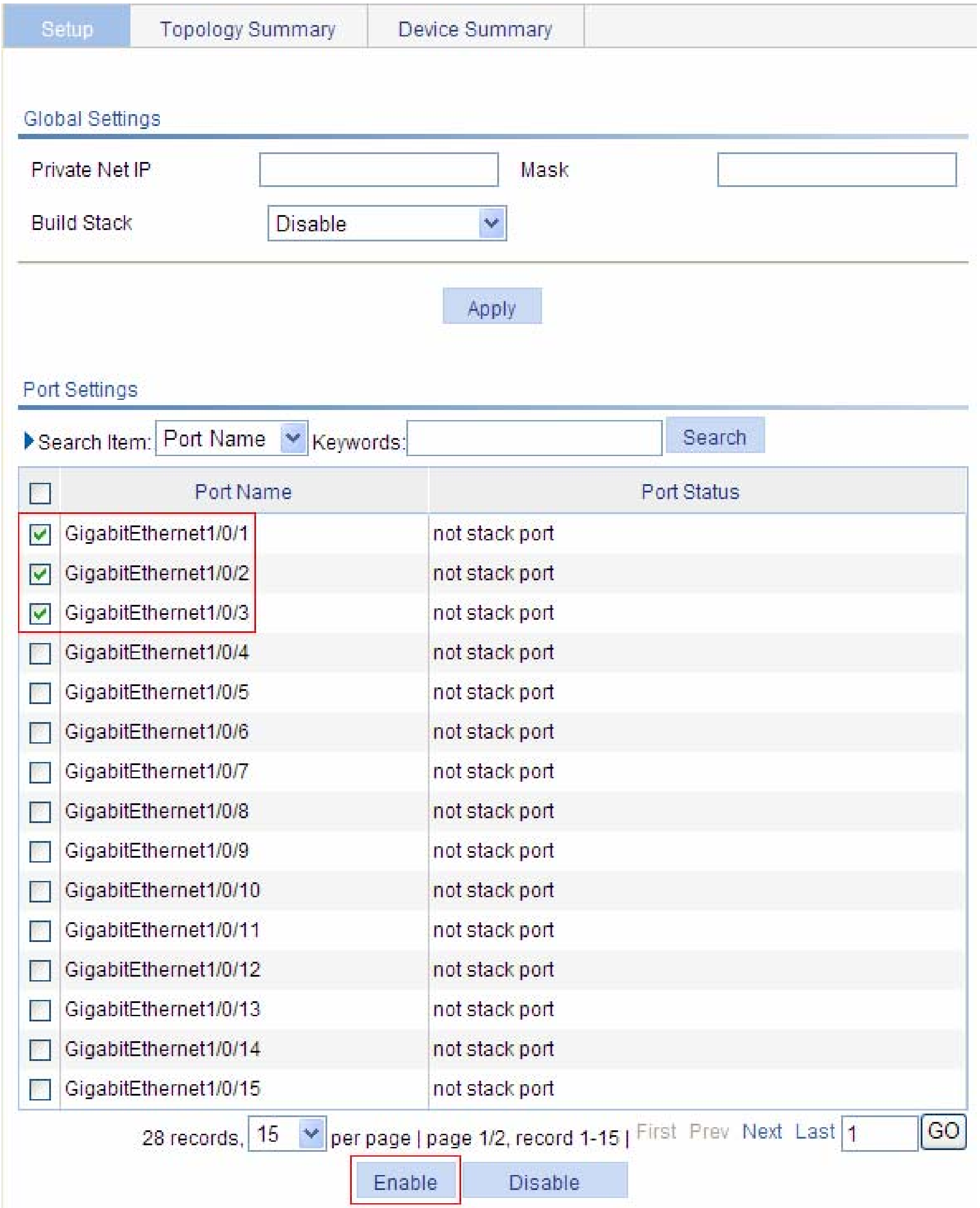
- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

2) Configure the slave devices

# On Switch B, configure local ports GigabitEthernet 1/0/2 connecting with switch A, GigabitEthernet 1/0/1 connecting with Switch C, and GigabitEthernet 1/0/3 connecting with Switch D as stack ports.

- Select **IRF** from the navigation tree of Switch B to enter the page of the **Setup** tab, and then perform the following configurations, as shown in Figure 1-9.

Figure 1-9 Configure stack ports on Switch B



Global Settings

Private Net IP:
Mask:
Build Stack: Disable

Port Settings

Search Item: Port Name Keywords:

☐	Port Name	Port Status
☑	GigabitEthernet1/0/1	not stack port
☑	GigabitEthernet1/0/2	not stack port
☑	GigabitEthernet1/0/3	not stack port
☐	GigabitEthernet1/0/4	not stack port
☐	GigabitEthernet1/0/5	not stack port
☐	GigabitEthernet1/0/6	not stack port
☐	GigabitEthernet1/0/7	not stack port
☐	GigabitEthernet1/0/8	not stack port
☐	GigabitEthernet1/0/9	not stack port
☐	GigabitEthernet1/0/10	not stack port
☐	GigabitEthernet1/0/11	not stack port
☐	GigabitEthernet1/0/12	not stack port
☐	GigabitEthernet1/0/13	not stack port
☐	GigabitEthernet1/0/14	not stack port
☐	GigabitEthernet1/0/15	not stack port

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

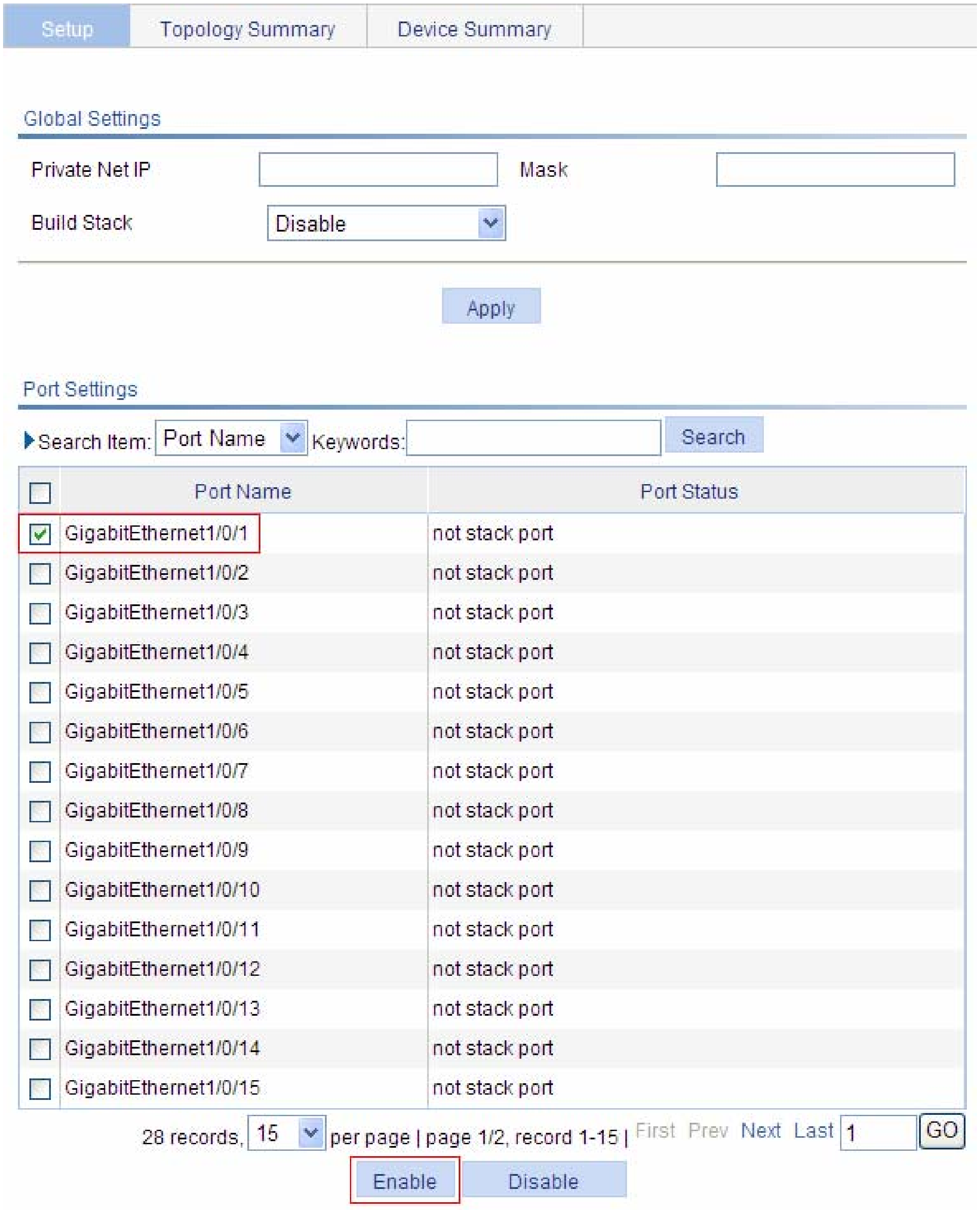
- In the **Port Settings** area, select the check boxes before **GigabitEthernet1/0/1**, **GigabitEthernet1/0/2**, and **GigabitEthernet1/0/3**.
- Click **Enable**.

Now, switch B becomes a slave device.

# On Switch C, configure local port GigabitEthernet 1/0/1 connecting with Switch B as a stack port.

- Select **IRF** from the navigation tree of Switch C to enter the page of the **Setup** tab, and then perform the following configurations, as shown in .

Figure 1-10 Configure a stack port on Switch C



Global Settings

Private Net IP:
Mask:
Build Stack: Disable

Port Settings

Search Item: Port Name Keywords:

□	Port Name	Port Status
☑	GigabitEthernet1/0/1	not stack port
□	GigabitEthernet1/0/2	not stack port
□	GigabitEthernet1/0/3	not stack port
□	GigabitEthernet1/0/4	not stack port
□	GigabitEthernet1/0/5	not stack port
□	GigabitEthernet1/0/6	not stack port
□	GigabitEthernet1/0/7	not stack port
□	GigabitEthernet1/0/8	not stack port
□	GigabitEthernet1/0/9	not stack port
□	GigabitEthernet1/0/10	not stack port
□	GigabitEthernet1/0/11	not stack port
□	GigabitEthernet1/0/12	not stack port
□	GigabitEthernet1/0/13	not stack port
□	GigabitEthernet1/0/14	not stack port
□	GigabitEthernet1/0/15	not stack port

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

Now, Switch C becomes a slave device.

# On Switch D, configure local port GigabitEthernet 1/0/1 connecting with Switch B as a stack port.

- Select **IRF** from the navigation tree of Switch D to enter the page of the **Setup** tab, and then perform the following configurations, as shown in Figure 1-10.
- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

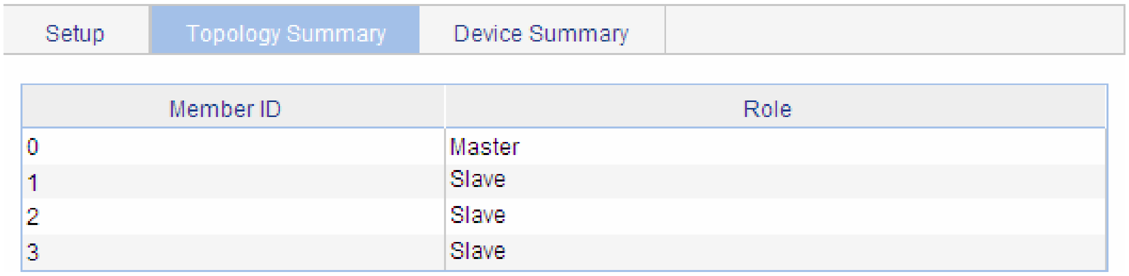
Now, Switch D becomes a slave device.

3) Verify the configuration

# Display the stack topology on Switch A.

- Select **IRF** from the navigation tree of Switch A and click the **Topology Summary** tab.
- You can view the information as shown in Figure 1-11.

Figure 1-11 Verify the configuration



Member ID	Role
0	Master
1	Slave
2	Slave
3	Slave

Configuration Guidelines

When configuring an IRF stack, note that:

1) If a device is already configured as the master device of a stack, you are not allowed to modify the private IP address pool on the device.

2) If a device is already configured as a slave device of a stack, the **Global Settings** area on the slave device is grayed out.

Table of Contents

1 Summary

Overview

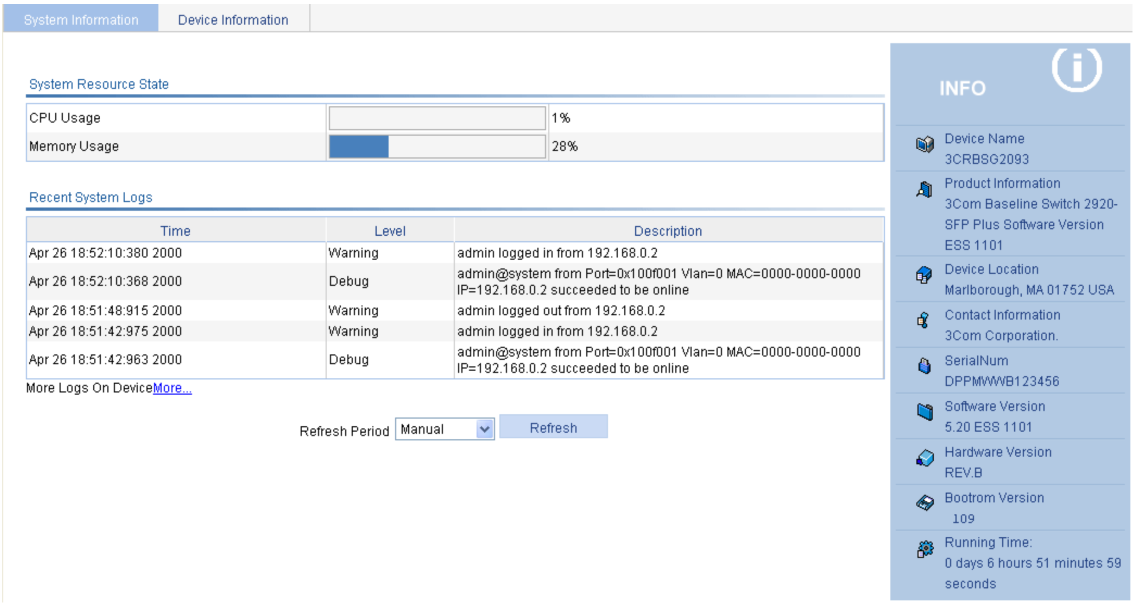
The device summary module helps you understand the system information, port information, power information, and fan information on the device. The system information includes the basic system information, system resources state, and recent system operation logs.

Displaying Device Summary

Displaying System Information

After you log in to the Web interface, the **System Information** page appears by default, as shown in Figure 1-1.

Figure 1-1 System information



System Resource State

CPU Usage		1%
Memory Usage		28%

Recent System Logs

Time	Level	Description
Apr 26 18:52:10:380 2000	Warning	admin logged in from 192.168.0.2
Apr 26 18:52:10:368 2000	Debug	admin@system from Port=0x100f001 Vlan=0 MAC=0000-0000-0000 IP=192.168.0.2 succeeded to be online
Apr 26 18:51:48:915 2000	Warning	admin logged out from 192.168.0.2
Apr 26 18:51:42:975 2000	Warning	admin logged in from 192.168.0.2
Apr 26 18:51:42:963 2000	Debug	admin@system from Port=0x100f001 Vlan=0 MAC=0000-0000-0000 IP=192.168.0.2 succeeded to be online

More Logs On DeviceMore...

Refresh Period Manual

Device Name
3CRBSG2093

Product Information
3Com Baseline Switch 2920-SFP Plus Software Version ESS 1101

Device Location
Marlborough, MA 01752 USA

Contact Information
3Com Corporation.

SerialNum
DPPMWWB123456

Software Version
5.20 ESS 1101

Hardware Version
REV.B

Bootrom Version
109

Running Time:
0 days 6 hours 51 minutes 59 seconds

Select from the **Refresh Period** drop-down list:

- If you select a certain period, the system refreshes the system information at the specified interval.
- If you select **Manual**, the system refreshes the information only when you click the **Refresh** button.

The system information page is divided into three sections, which display:

- Basic system information
- System resource state
- Recent system operation logs

Basic system information

The **INFO** area on the right of the page displays the basic system information including device name, product information, device location, contact information, serial number, software version, hardware version, BootROM version, and running time. The running time displays how long the device is up since the last boot.

You can configure the device location and contact information on the Setup page you enter by selecting **Device > SNMP**.

System resource state

The System Resource State displays the most current CPU usage and memory usage.

Recent system operation logs

Table 1-1 describes the fields in the recent system operation log table.

Table 1-1 Description about the recent system operation logs

Field	Description
Time	This field displays the time when the system operation logs are generated.
Level	This field displays the severity of the system operation logs.
Description	This field displays the description of the system operation logs.

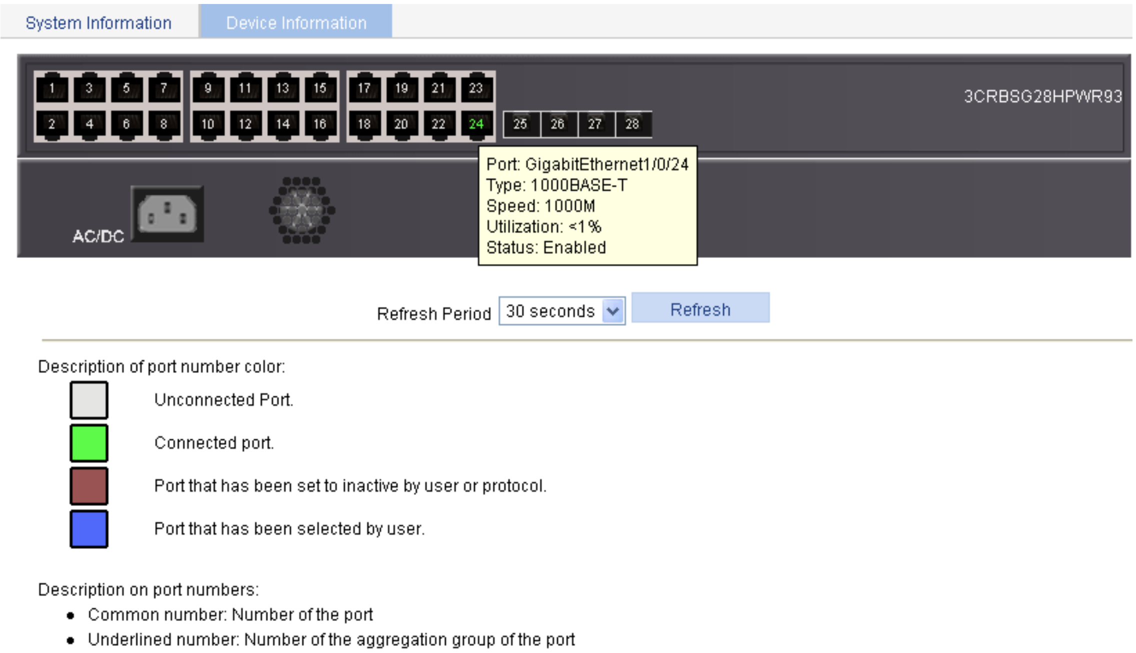
Note

- The **Summary** page displays up to five the most recent system operation logs about the login and logout events.
- For more system operation logs, you can click **More** to enter the **Log List** page. You can also enter this page by selecting **Device** > **Syslog**. For details, refer to *Log Management Configuration.*

Displaying Device Information

After you log in to the Web interface, you can click the **Device Information** tab to enter the page displaying the device ports. Hover the cursor over a port and the port details appears, including the port name, type, speed, utilization, and status, as shown in Figure 1-2. For the description about the port number and its color, see Figure 1-2. Similarly, you can also view the power type and working status and the fan working status.

Figure 1-2 Device information



Port: GigabitEthernet1/0/24
Type: 1000BASE-T
Speed: 1000M
Utilization: <1%
Status: Enabled

Refresh Period: 30 seconds

Description of port number color:

- ⬜ Unconnected Port.
- 🟩 Connected port.
- 🟥 Port that has been set to inactive by user or protocol.
- 🟦 Port that has been selected by user.

Description on port numbers:

- Common number: Number of the port
- Underlined number: Number of the aggregation group of the port

Select from the **Refresh Period** drop-down list:

- If you select a certain period, the system refreshes the information at the specified interval.
- If you select **Manual**, the system refreshes the information only when you click the **Refresh** button.

Table of Contents

1 Device Basic Information Configuration

Overview

The device basic information feature provides you the following functions:

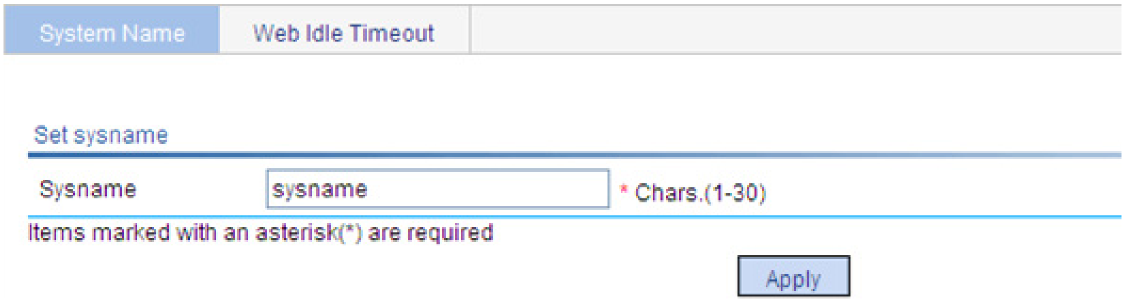
- Set the system name of the device. The configured system name will be displayed on the top of the navigation bar.
- Set the idle timeout period for a logged-in user. That is, the system will log an idle user off the Web for security purpose after the configured period.

Configuring Device Basic Information

Configuring System Name

Select **Device** > **Basic** from the navigation tree to enter the system name page, as shown in Figure 1-1.

Figure 1-1 System name



Sysname: sysname * Chars.(1-30)

Items marked with an asterisk(*) are required

Table 1-1 describes the system name configuration item.

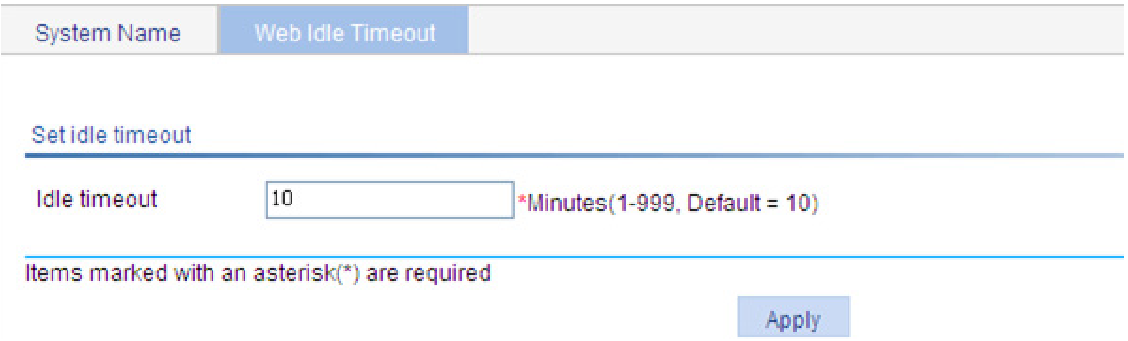
Table 1-1 System name configuration item

Item	Description
Sysname	Set the system name.

Configuring Idle Timeout Period

Select **Device** > **Basic** from the navigation tree to enter the idle timeout page, as shown in Figure 1-2.

Figure 1-2 Configuring idle timeout period



Set idle timeout

Idle timeout 10 *Minutes(1-999, Default = 10)

Items marked with an asterisk(*) are required

Table 1-2 describes the idle timeout period configuration item.

Table 1-2 Idle timeout period configuration item

Item	Description
Idle timeout	Set the idle timeout period for a logged-in user.

Table of Contents

1 System Time Configuration

Overview

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

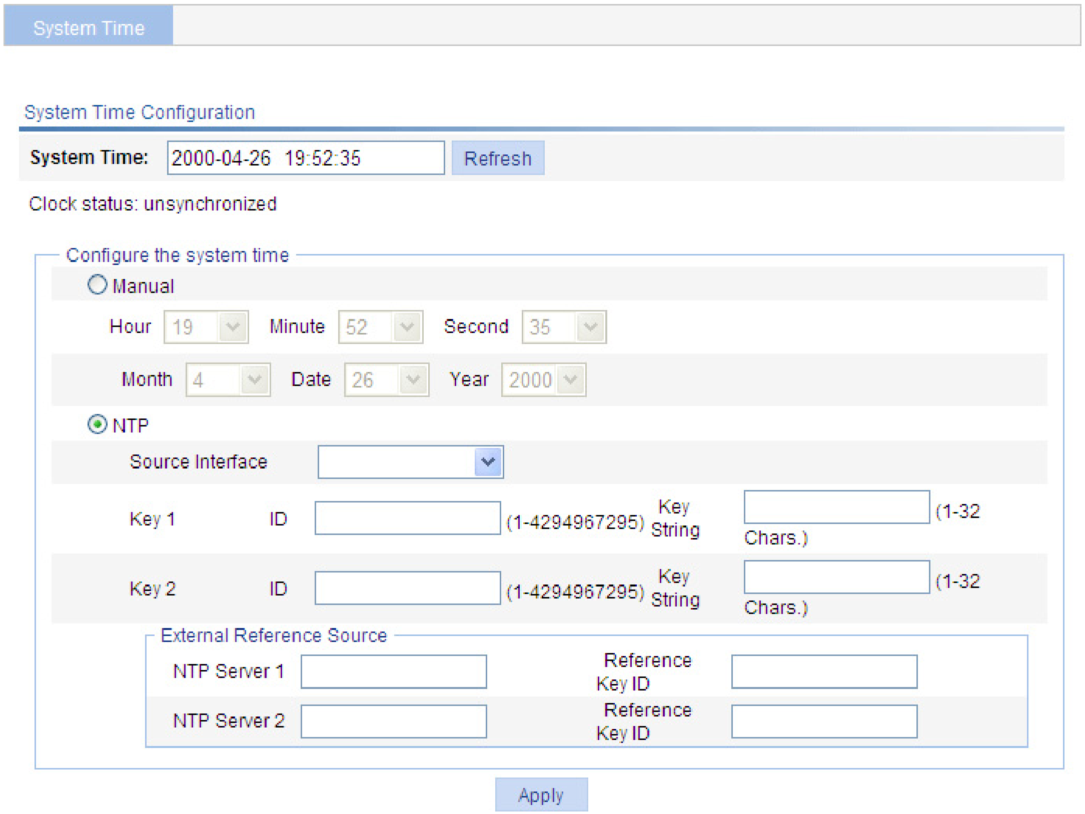
An administrator can by no means keep time synchronized among all the devices within a network by changing the system clock on each device, because this is a huge amount of workload and cannot guarantee the clock precision.

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP allows quick clock synchronization within the entire network and ensures a high clock precision so that the devices can provide diverse applications based on the consistent time.

Configuring System Time

Select **System** > **System Time** from the navigation tree to enter the system time configuration page, as shown in Figure 1-1. On the upper side of the interface, the current system time and clock status are displayed, and you can click **Refresh** to refresh the displayed content; on the lower side of the interface, you can set the system time.

Figure 1-1 System time configuration page



System Time: 2000-04-26 19:52:35 Refresh

Clock status: unsynchronized

Configure the system time

○ Manual

Hour 19 Minute 52 Second 35

Month 4 Date 26 Year 2000

● NTP

Source Interface

Key 1 ID (1-4294967295) Key String (1-32 Chars.)

Key 2 ID (1-4294967295) Key String (1-32 Chars.)

External Reference Source

NTP Server 1 Reference Key ID

NTP Server 2 Reference Key ID

Table 1-1 shows the system time configuration items.

Table 1-1 System time configuration items

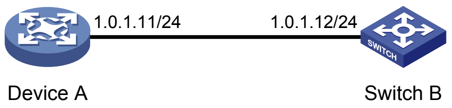
Item			Description
Manual			Select to manually configure the system time, including the setting of **Year**, **Month**, **Day**, **Hour**, **Minute**, and **Second.**
NTP	Source Interface		Set the source interface for an NTP message. If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, you can specify the source interface for NTP messages, so that the source IP address in the NTP messages is the primary IP address of this interface.
	Key 1		Set NTP authentication key. The NTP authentication feature should be enabled for a system running NTP in a network where there is a high security demand. This feature enhances the network security by means of client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication. You can set two authentication keys, each of which is composed of a key ID and key string. • ID is the ID of a key. • Key string is a character string for MD5 authentication key.
	Key 2		
	External Reference Source	NTP Server 1/Reference Key ID	Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. Only if the key provided by the server is the same with the specified key will the device synchronize its time to the NTP server. You can configure two NTP servers. The clients will choose the optimal reference source. **Highlight** *The IP address of an NTP server is a unicast address, and cannot be a broadcast or a multicast address, or the IP address of the local clock source.*
		NTP Server 2/Reference Key ID	

System Time Configuration Example

Network requirements

- As shown in Figure 1-2, the local clock of Device A is set as the reference clock.
- Switch B works in the client mode, and uses Device A as the NTP server.
- Configure NTP authentication on Device A and Switch B.

Figure 1-2 Network diagram for configuring system time



Configuration procedure

1) Configure Device A

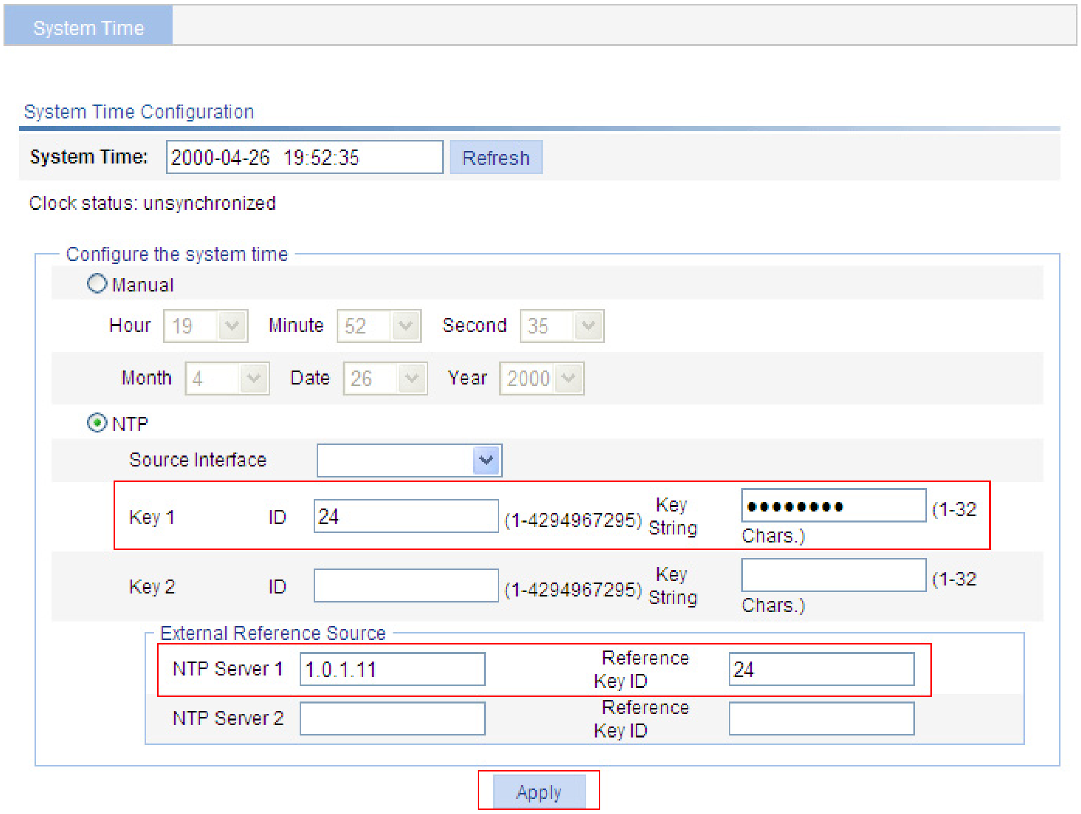
# Configure the local clock as the reference clock, with the stratum of 2. Enable NTP authentication, set the key ID to **24**, and specify the created authentication key **aNiceKey** is a trusted key. (Configuration omitted.)

2) Configure Switch B

# Configure Device A as the NTP server of Switch B.

- Select **System** > **System Time** from the navigation tree and perform the configurations as shown in Figure 1-3.

Figure 1-3 Configure Device A as the NTP server of Switch B



System Time: 2000-04-26 19:52:35

Clock status: unsynchronized

Configure the system time

○ Manual

Hour 19 Minute 52 Second 35

Month 4 Date 26 Year 2000

● NTP

Source Interface

Key 1 ID 24 (1-4294967295) Key String •••••••• (1-32 Chars.)

Key 2 ID (1-4294967295) Key String (1-32 Chars.)

External Reference Source

NTP Server 1 1.0.1.11 Reference Key ID 24

NTP Server 2 Reference Key ID

- Select **NTP**.
- Type **24** in the **ID** box, and type **aNiceKey** in the **Key String** text box for key 1.
- Type **1.0.1.11** in the **NTP Server 1** text box and type **24** in the **Reference Key ID** text box.
- Click **Apply**.

3) Verify the configuration

After the above configuration, you can see that the current system time on Device A is the same with that on Switch B.

Configuration Guidelines

When configuring system time, note that:

- A device can act as a server to synchronize the clock of other devices only after its clock has been synchronized. If the clock of a server has a stratum level higher than or equal to that of a client's clock, the client will not synchronize its clock to the server's.
- The synchronization process takes a period of time. Therefore, the clock status may be **unsynchronized** after your configuration. In this case, you can click **Refresh** to view the clock status and system time later on.

Table of Contents

1 Log Management

Overview

System logs contain a large amount of network and device information, including running status and configuration changes. System logs are an important way for administrators to know network and device status. With system log information, administrators can take corresponding actions against network problems and security problems.

System logs can be stored in the log buffer, or sent to the loghost.

Configuring Log Management

Configuration Task List

Perform the tasks in Table 1-1 to configure log management.

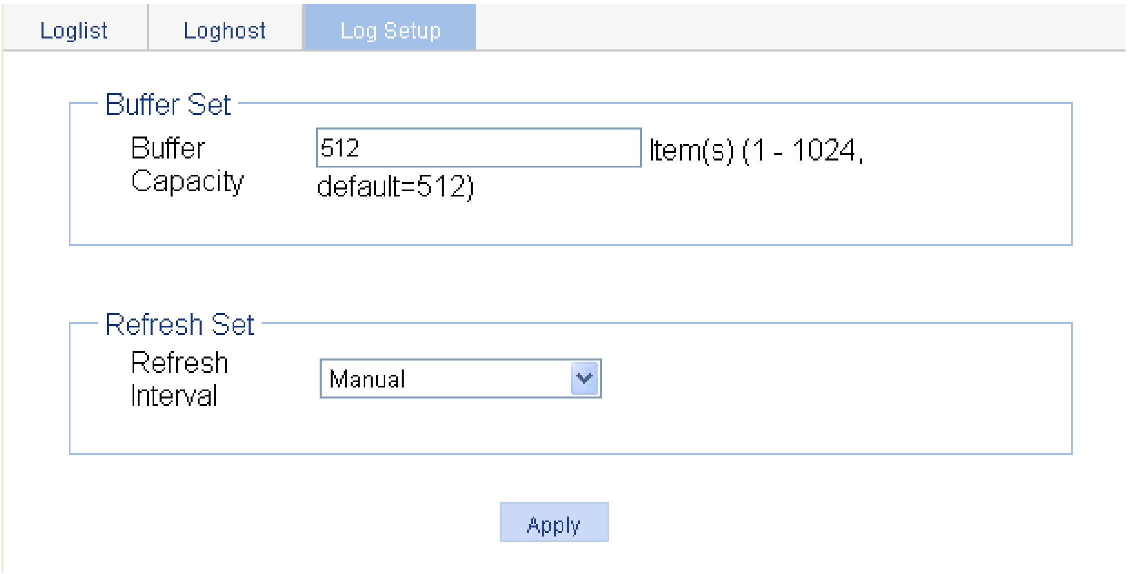
Table 1-1 Log management configuration task list

Task	Description
Setting Syslog Related Parameters	Optional • Set the number of logs that can be stored in the log buffer. • Set the refresh period of the log information displayed on the Web interface.
Displaying Syslog	Display detailed information of system logs.
Setting Loghost	Optional Set the loghost that can receive system logs.

Setting Syslog Related Parameters

Select **Device** > **Syslog** from the navigation tree, and click the **Logset** tab to enter the syslog configuration page, as shown in Figure 1-1.

Figure 1-1 Set system logs related parameters



Buffer Set

Buffer Capacity: 512 Item(s) (1 - 1024, default=512)

Refresh Set

Refresh Interval: Manual

Table 1-2 describes the syslog configuration items.

Table 1-2 Syslog configuration items

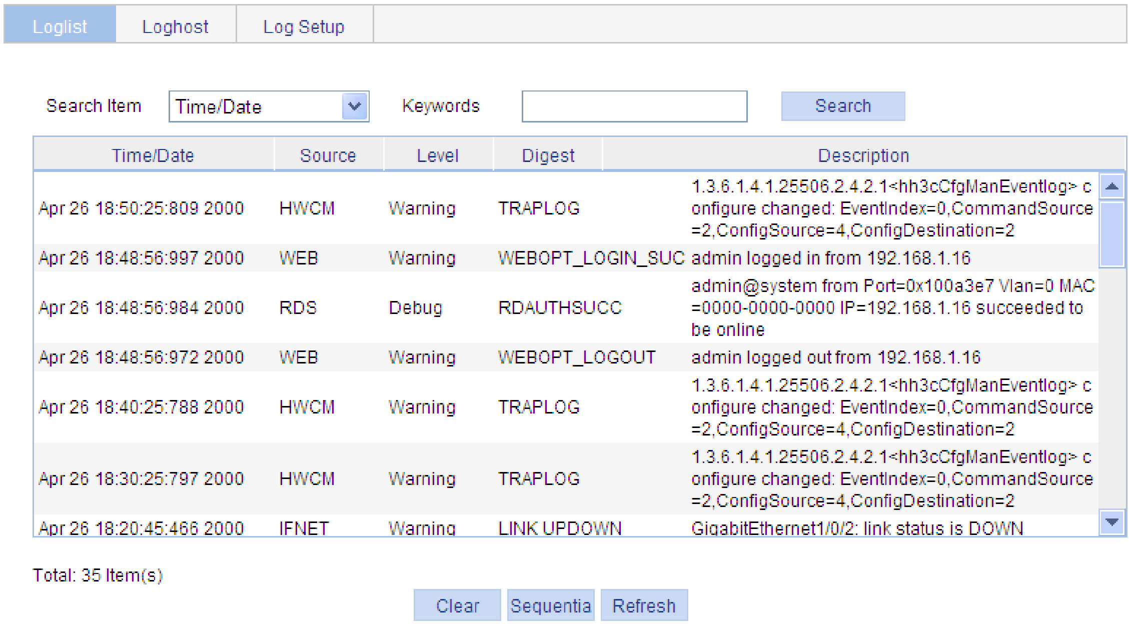
Item	Description
Log Buffer Size	Set the number of logs that can be stored in the log buffer.
Refresh Period	Set the refresh period on the log information displayed on the Web interface. You can select manual refresh or automatic refresh: • Manual: You need to click **Refresh** to refresh the Web interface when displaying log information. • Automatic: You can select to refresh the Web interface every 1 minute, 5 minutes, or 10 minutes.

Return to Log management configuration task list.

Displaying Syslog

Select **Device** > **Syslog** from the navigation tree to enter the syslog display page, as shown in Figure 1-2.

Figure 1-2 Display syslog



Time/Date	Source	Level	Digest	Description
Apr 26 18:50:25:809 2000	HWCM	Warning	TRAPLOG	1.3.6.1.4.1.25506.2.4.2.1<hh3cCfgManEventlog> configure changed: EventIndex=0,CommandSource=2,ConfigSource=4,ConfigDestination=2
Apr 26 18:48:56:997 2000	WEB	Warning	WEBOPT_LOGIN_SUC	admin logged in from 192.168.1.16
Apr 26 18:48:56:984 2000	RDS	Debug	RDAUTHSUCC	admin@system from Port=0x100a3e7 Vlan=0 MAC=0000-0000-0000 IP=192.168.1.16 succeeded to be online
Apr 26 18:48:56:972 2000	WEB	Warning	WEBOPT_LOGOUT	admin logged out from 192.168.1.16
Apr 26 18:40:25:788 2000	HWCM	Warning	TRAPLOG	1.3.6.1.4.1.25506.2.4.2.1<hh3cCfgManEventlog> configure changed: EventIndex=0,CommandSource=2,ConfigSource=4,ConfigDestination=2
Apr 26 18:30:25:797 2000	HWCM	Warning	TRAPLOG	1.3.6.1.4.1.25506.2.4.2.1<hh3cCfgManEventlog> configure changed: EventIndex=0,CommandSource=2,ConfigSource=4,ConfigDestination=2
Apr 26 18:20:45:466 2000	IFNET	Warning	LINK UPDOWN	GigabitEthernet1/0/2: link status is DOWN

Total: 35 Item(s)

Table 1-3 describes the syslog display items.

Table 1-3 Syslog display items

Item	Description
Time/Date	Displays the time/date when system logs are generated.
Source	Displays the module that generates system logs.
Level	Displays the severity level of system logs. For the detailed description of the severity levels, refer to Table 1-4.
Digest	Displays the brief description of system logs
Description	Displays the contents of system logs.

You can perform the following operations in the syslog display page:

- Click **Clear** to clear the log buffer.
- Click **Sequential Display** to change the order in which system logs are displayed, and then the **Sequential Display** button will be changed to **Reverse Display**. After you change the order in which system logs are displayed, the system logs are displayed in this order, unless you change it again.

Table 1-4 System logs severity level

Severity level	Description	Value
Emergency	The system is unavailable.	0
Alert	Information that demands prompt reaction	1
Critical	Critical information	2
Error	Error information	3
Warning	Warnings	4

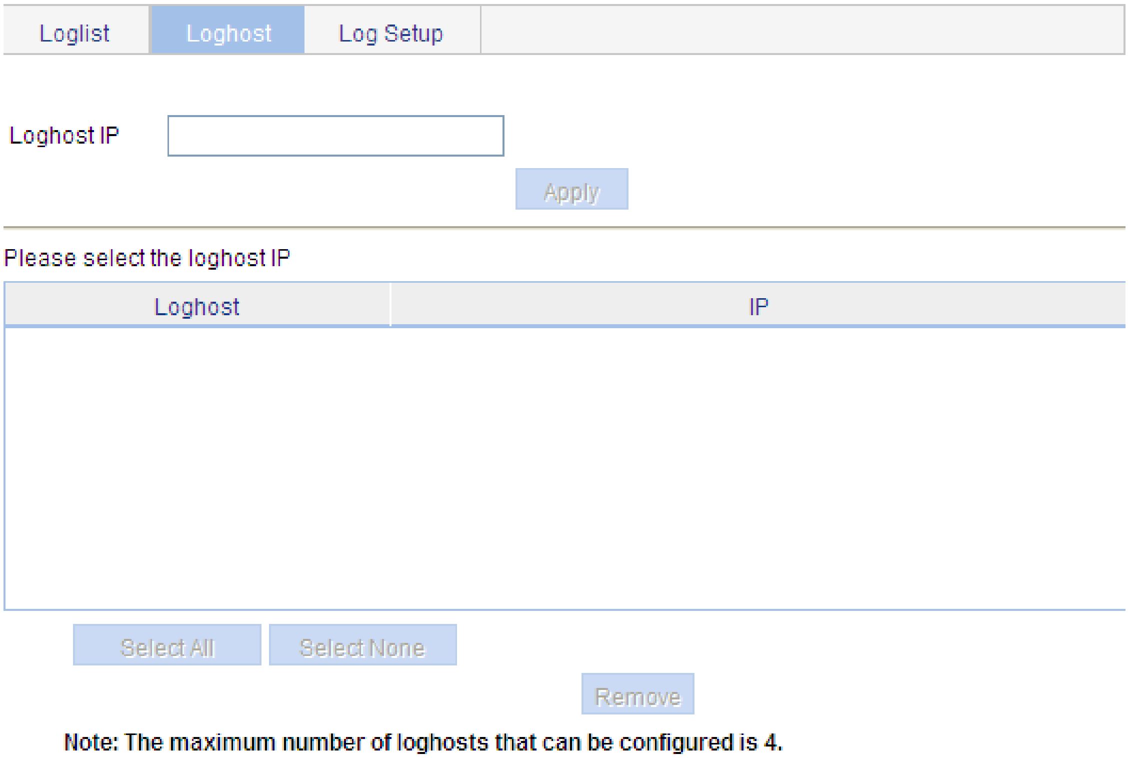
Severity level	Description	Value
Notification	Normal information that needs to be noticed	5
Informational	Informational information to be recorded	6
Debugging	Information generated during debugging	7
Note: A smaller value represents a higher severity level.		

Return to Log management configuration task list.

Setting Loghost

Select **Device** > **Syslog** from the navigation tree, and click the **Loghost** tab to enter the loghost configuration page, as shown in Figure 1-3.

Figure 1-3 Set loghost



Note: The maximum number of loghosts that can be configured is 4.

Table 1-5 describes the loghost configuration item.

Table 1-5 Loghost configuration item

Item	Description
Loghost IP	IP address of the loghost. • You can specify up to four loghosts. • You must input a valid IP address.

Return to Log management configuration task list.

Table of Contents

1 Configuration Management

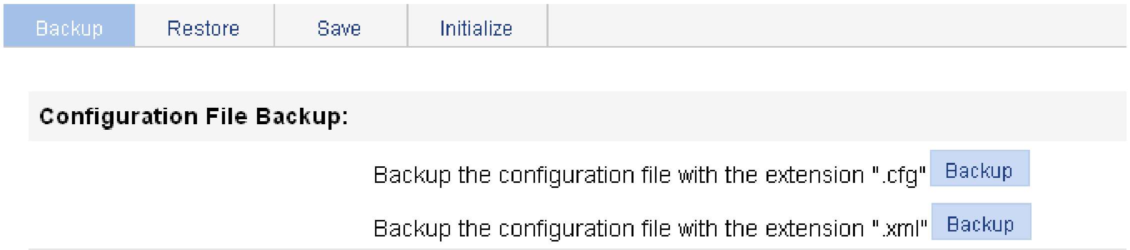
Back Up Configuration

Configuration backup provides the following functions:

- Open and view the configuration file (**.cfg** file or **.xml** file) for the next startup
- Back up the configuration file (**.cfg** file or **.xml** file) for the next startup to the host of the current user

Select **Device** > **Configuration** from the navigation tree to enter the backup configuration page, as shown in Figure 1-1.

Figure 1-1 Backup configuration page



Configuration File Backup:

Backup the configuration file with the extension ".cfg"

Backup the configuration file with the extension ".xml"

- After you click the upper **Backup** button in this figure, a file download dialog box appears. You can select to view the **.cfg** file or to save the file locally.
- After you click the lower **Backup** button in this figure, a file download dialog box appears. You can select to view the **.xml** file or to save the file locally.

Note

The switch uses both **.cfg** and **.xml** configuration files to save different types of configurations. When backing up or restoring the configuration file, you are recommended to back up or restore both of the two configuration files.

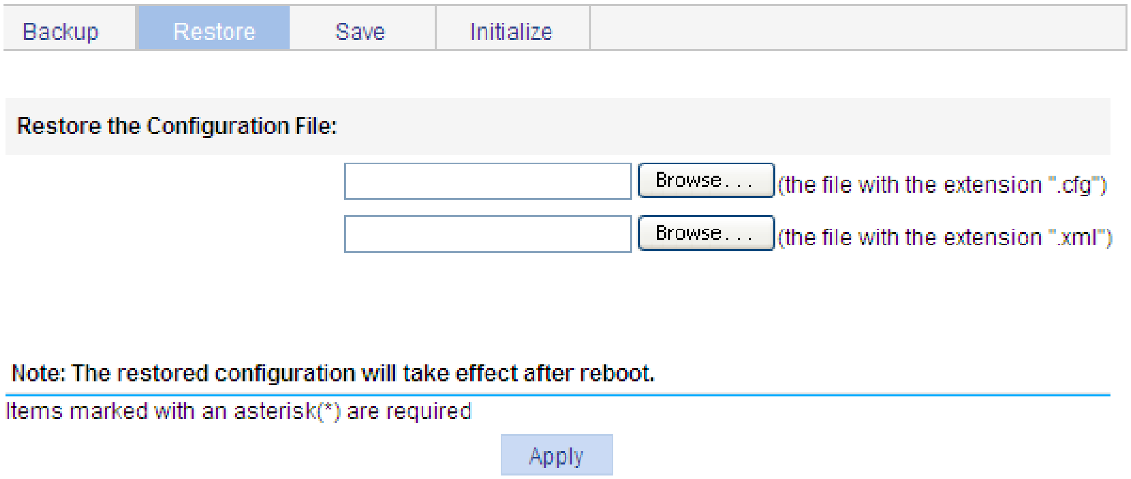
Restore Configuration

Configuration restore provides the following functions:

- Upload the **.cfg** file on the host of the current user to the device for the next startup
- Upload the **.xml** file on the host of the current user to the device for the next startup, and delete the previous **.xml** configuration file that was used for the next startup

Select **Device** > **Configuration** from the navigation tree, and then click the **Restore** tab to enter the configuration restore page, as shown in Figure 1-2.

Figure 1-2 Configuration restore page


Backup
Restore
Save
Initialize
Restore the Configuration File:
Browse...
(the file with the extension ".cfg")
Browse...
(the file with the extension ".xml")
Apply

Note: The restored configuration will take effect after reboot.

Items marked with an asterisk(*) are required

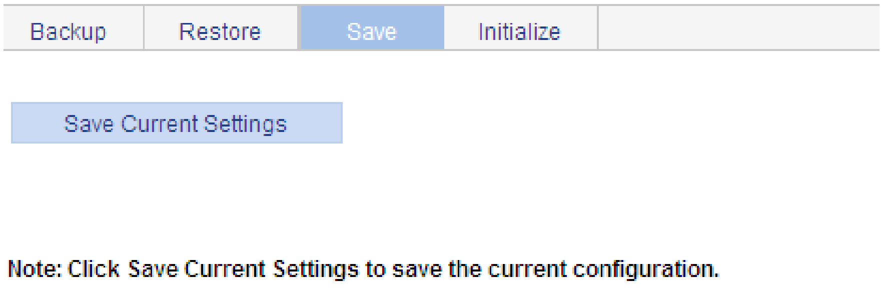
- After you click the upper **Browse** button in this figure, the file upload dialog box appears. You can select the **.cfg** file to be uploaded, and then click **Apply**.
- After you click the lower **Browse** button in this figure, the file upload dialog box appears. You can select the **.xml** file to be uploaded, and then click **Apply**.

Save Configuration

The save configuration module provides the function to save the current configuration to the configuration file (**.cfg** file or **.xml** file) for the next startup.

Select **Device** or **Configuration** from the navigation tree, and then click the **Save** tab to enter the save configuration confirmation page, as shown in Figure 1-3.

Figure 1-3 Save configuration confirmation



Note: Click Save Current Settings to save the current configuration.

Click the **Save Current Settings** button to save the current configuration to the configuration file.

Note

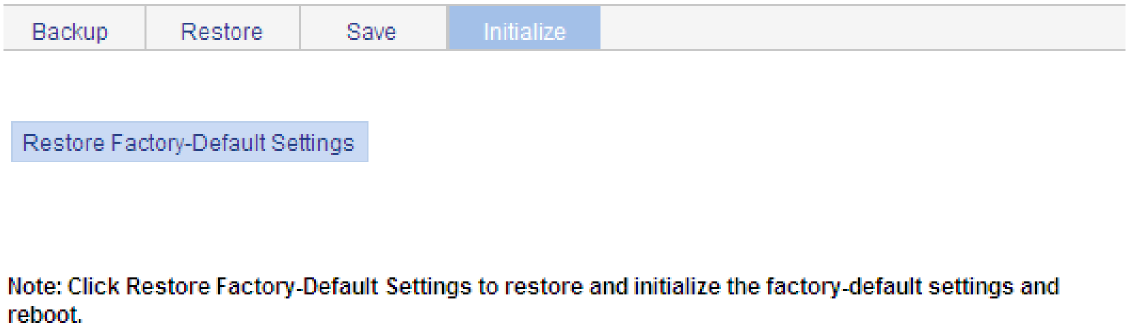
- Saving the configuration takes a period of time.
- The system does not support the operation of saving configuration of two or more consecutive users. If such a case occurs, the system prompts the latter users to try later.

Initialize

This operation will restore the system to factory defaults, delete the current configuration file, and reboot the device.

Select **Device** > **Configuration** from the navigation tree, and then click the **Initialize** tab to enter the initialize confirmation page as shown in Figure 1-4.

Figure 1-4 Initialize confirmation dialog box



Note: Click Restore Factory-Default Settings to restore and initialize the factory-default settings and reboot.

Click the **Restore Factory-Default Settings** button to restore the system to factory defaults.

Table of Contents

1 Device Maintenance

Software Upgrade

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

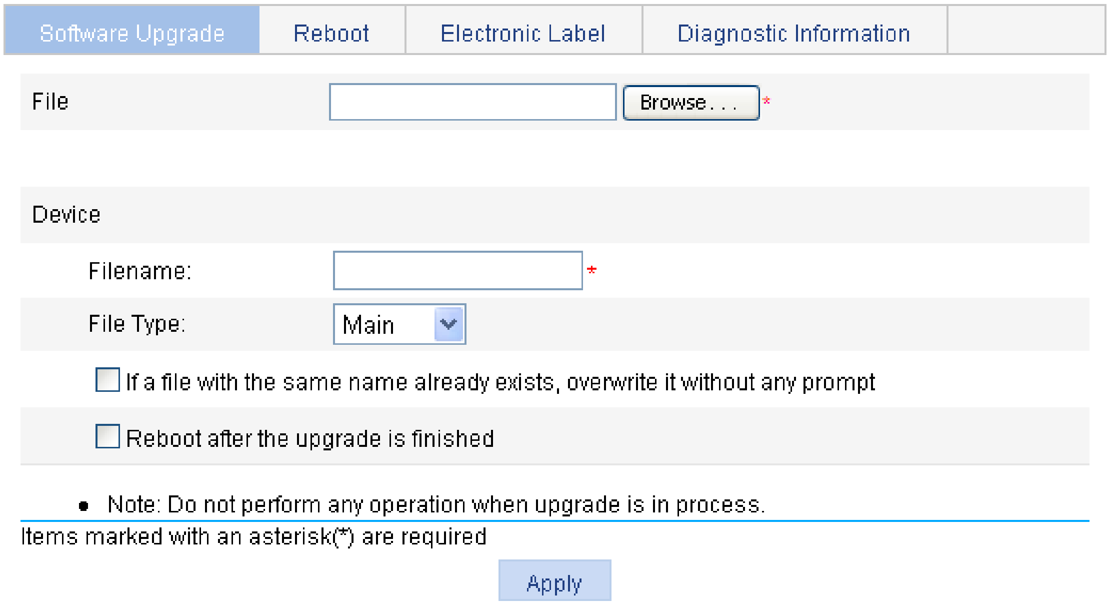
A boot file, also known as the system software or device software, is an application file used to boot the device. A main boot file is used to boot a device and a backup boot file is used to boot a device only when the main boot file is unavailable.

Caution

The software upgrade will take a period of time. During upgrading, do not perform any operation on the Web page. Otherwise, the software upgrade is interrupted.

Select **Device** > **Device Maintenance** from the navigation tree to enter the software upgrade configuration page, as shown in Figure 1-1.

Figure 1-1 Software upgrade configuration page



File *

Device

Filename: *

File Type: Main

□ If a file with the same name already exists, overwrite it without any prompt

□ Reboot after the upgrade is finished

- Note: Do not perform any operation when upgrade is in process.

Items marked with an asterisk(*) are required

Table 1-1 shows the detailed configuration for software upgrade.

Table 1-1 Software upgrade configuration items

Item	Description
File	Specifies the filename of the local application file, which must be with an extension **.bin**.
Filename	Specifies a filename for the file to be saved on the device. The filename must have an extension, which must be the same as that of the source application file.
File Type	Specifies the type of the boot file for the next boot: • Main • Backup
If a file with same name already exists, overwrite it without prompt.	Specifies whether to overwrite the file with the same name. If you do not select the option, when a file with the same name exists, a dialog box appears, telling you that the file already exists and you can not continue the upgrade.
Reboot after the upgrading finished.	Specifies whether to reboot the device to make the upgraded software take effect after the application file is uploaded.

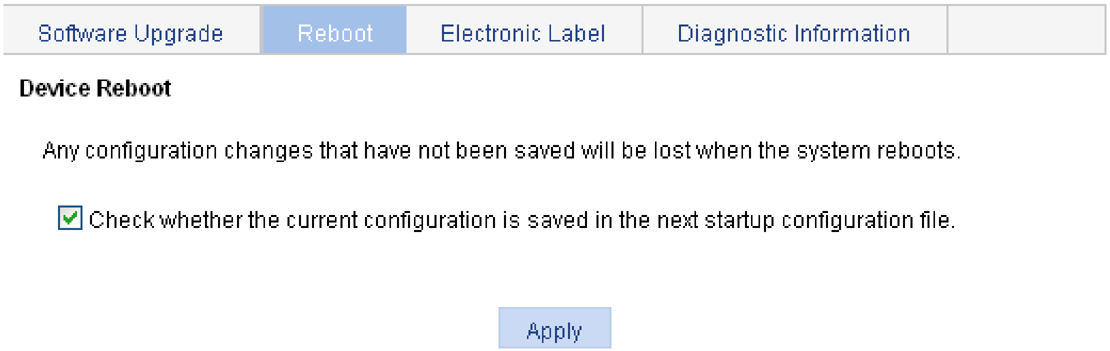
Device Reboot

Caution

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

Select **Device** > **Device Maintenance** from the navigation tree, click the **Reboot** tab to enter the device reboot configuration page, as shown in Figure 1-2.

Figure 1-2 Device reboot page



Device Reboot

Any configuration changes that have not been saved will be lost when the system reboots.

☑ Check whether the current configuration is saved in the next startup configuration file.

Click **Apply** to reboot the device. You can choose to check whether the current configuration has been saved to the configuration file to be used at the next startup.

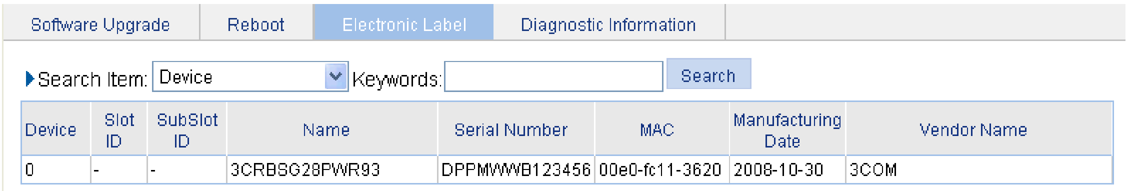
- If you select **Check configuration with next startup configuration file**, the system will check the configuration before rebooting the device. If the check succeeds, the system will reboot the device; if the check fails, a dialog box appears, telling you that the current configuration and the saved configuration are inconsistent, and the device will not be rebooted. In this case, you need to save the current configuration manually before you can reboot the device.
- If you do not select the check box, the system will reboot the device directly.

Electronic Label

Electronic label allows you to view information about the device electronic label, which is also known as the permanent configuration data or archive information. The information is written into the storage medium of a device or a card during the debugging and testing processes, and includes card name, product bar code, MAC address, debugging and testing date(s), manufacture name, and so on.

Select **Device** > **Device Maintenance** from the navigation tree, and click the **Electronic Label** tab to enter the page as shown in Figure 1-3.

Figure 1-3 Electronic label



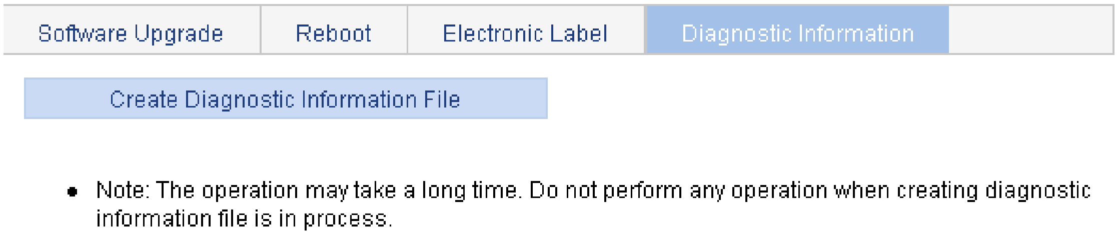
Device	Slot ID	SubSlot ID	Name	Serial Number	MAC	Manufacturing Date	Vendor Name
0	-	-	3CRBSG28PWR93	DPPMWWB123456	00e0-fc11-3620	2008-10-30	3COM

Diagnostic Information

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

Select **Device** > **Device Maintenance** from the navigation tree, and click the **Diagnostic Information** tab to enter the page as shown in Figure 1-4.

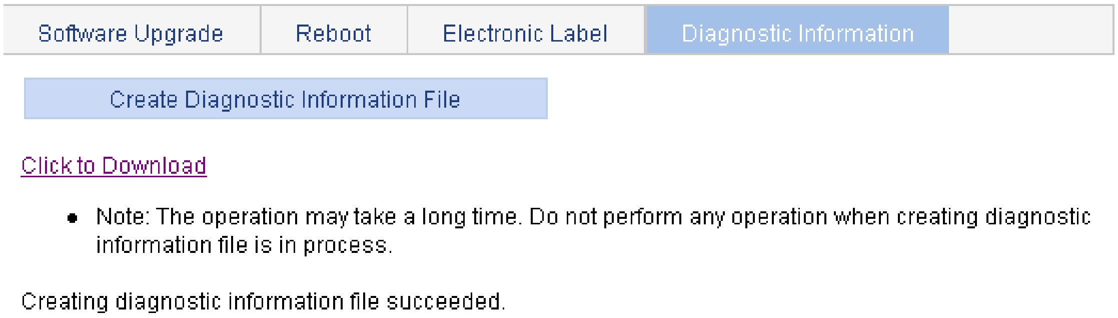
Figure 1-4 Diagnostic information



- Note: The operation may take a long time. Do not perform any operation when creating diagnostic information file is in process.

When you click **Create Diagnostic Information File**, the system begins to generate diagnostic information file, and after the file is generated, the page is as shown in Figure 1-5.

Figure 1-5 The diagnostic information file is created



- Note: The operation may take a long time. Do not perform any operation when creating diagnostic information file is in process.

Creating diagnostic information file succeeded.

Click **Click to Download**, and the **File Download** dialog box appears. You can select to open this file or save this file to the local host.

Note

- The generation of the diagnostic file will take a period of time. During this process, do not perform any operation on the Web page.
- After the diagnostic file is generated successfully, you can view this file by selecting **Device** > **File Management**, or downloading this file to the local host. For the details, refer to *File Management Configuration*.

Table of Contents

1 File Management

Overview

The device saves useful files (such as host software, configuration file) into the storage device, and the system provides the file management function for the users to manage those files conveniently and effectively. File management function provides the following operations:

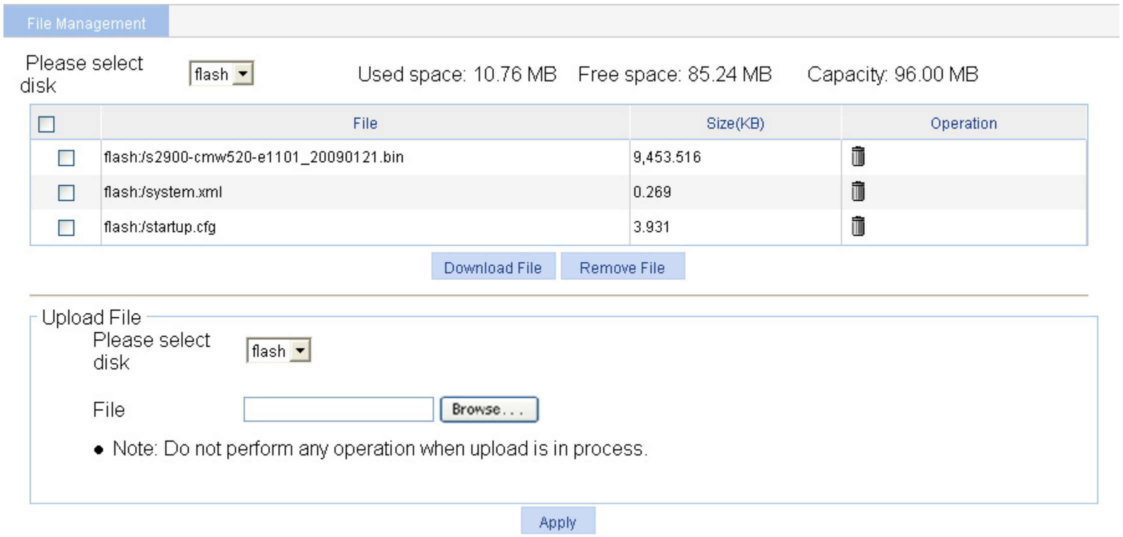
- Displaying File List
- Downloading a File
- Uploading a File
- Removing a File

File Management Configuration

Displaying File List

Select **Device** > **File Management** from the navigation tree to enter the file management page, as shown in Figure 1-1. On the top of this page, select a disk from the **Please select disk** drop-down list, and the used space, available space, and capacity of the disk will be displayed at the right of the drop-down list. The area below the drop-down list displays all files (displayed in the format of path + filename) saved on the disk and their sizes.

Figure 1-1 File management



Please select disk: flash

Used space: 10.76 MB   Free space: 85.24 MB   Capacity: 96.00 MB

□	File	Size(KB)	Operation
□	flash:/s2900-cmw520-e1101_20090121.bin	9,453.516	🗑
□	flash:/system.xml	0.269	🗑
□	flash:/startup.cfg	3.931	🗑

Please select disk: flash

File:

- Note: Do not perform any operation when upload is in process.

Downloading a File

Select **Device** > **File Management** from the navigation tree to enter the file management page, as shown in Figure 1-1. Select a file from the list, click the **Download File** button, and then a **File**

Download dialog box appears. You can select to open the file or to save the file locally. You can download only one file at one time.

Uploading a File

Select **Device** > **File Management** from the navigation tree to enter the file management page, as shown in Figure 1-1. In the **Upload File** area, select a disk from the **Please select disk** drop-down list to save the file, type the file path and filename in the **File** box, or click **Browse** to select a file. Click **Apply** to upload the file to the specified storage device.

⚠ **Caution**

Upload a file will take a period of time. During uploading, do not perform any operation on the Web page. Otherwise, the file upload is interrupted.

Removing a File

Select **Device** > **File Management** from the navigation tree to enter the file management page, as shown in Figure 1-1. You can remove a file by using one of the following ways:

- Click the 🗑 icon to remove a file.
- Select one or multiple files from the file list, and then click **Remove File**.

Table of Contents

1 Port Management Configuration

Overview

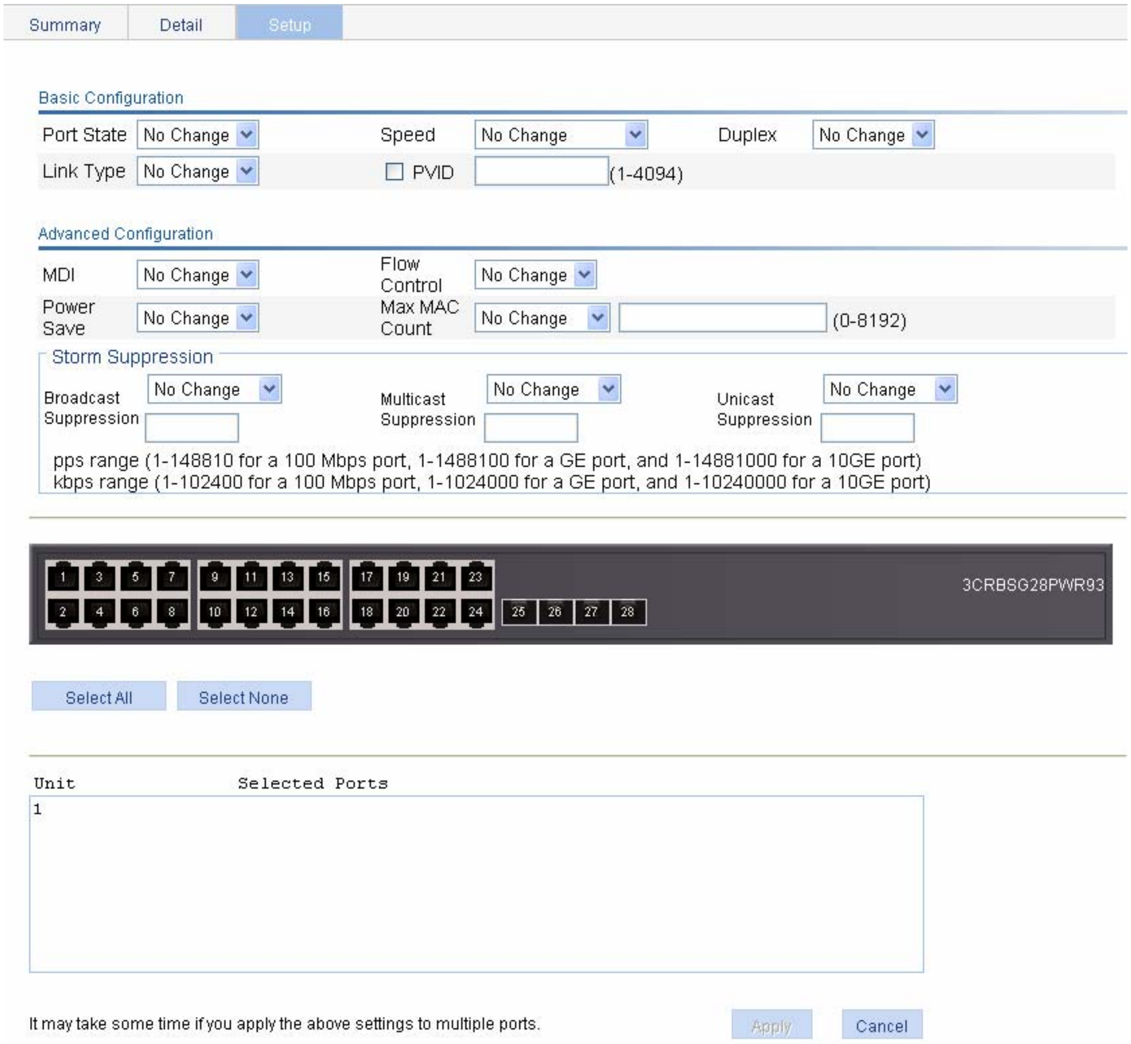
You can use the port management feature to set and view the operation parameters of a Layer 2 Ethernet port, including but not limited to its state, rate, duplex mode, link type, PVID, MDI mode, flow control settings, MAC learning limit, and storm suppression ratios.

Configuring a Port

Setting Operation Parameters for a Port

Select **Device** > **Port Management** from the navigation tree, and then select the **Setup** tab on the page that appears to enter the page as shown in Figure 1-1.

Figure 1-1 The **Setup** tab



Summary | Detail | Setup

Basic Configuration

Port State: No Change
Speed: No Change
Duplex: No Change
Link Type: No Change
□ PVID (1-4094)

Advanced Configuration

MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)

Storm Suppression

Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Select All | Select None

```
Unit                  Selected Ports
1
```

It may take some time if you apply the above settings to multiple ports.

Apply | Cancel

Table 1-1 describes the port configuration items.

Table 1-1 Port configuration items

Item	Description
Port State	Enable or disable the port. Sometimes, after you modify the operation parameters of a port, you need to disable and then enable the port to have the modifications take effect.
Speed	Set the transmission rate of the port. Available options include: • 10: 10 Mbps • 100: 100 Mbps • 1000: 1000 Mbps • Auto: auto-negotiation • Auto 10: auto-negotiated to 10 Mbps • Auto 100: auto-negotiated to 100 Mbps • Auto 1000: auto-negotiated to 1000 Mbps • Auto 10 100: auto-negotiated to 10 or 100 Mbps • Auto 10 1000: auto-negotiated to 10 or 1000 Mbps • Auto 100 1000: auto-negotiated to 100 or 1000 Mbps • Auto 10 100 1000: auto-negotiated to 10, 100, or 1000 Mbps **Highlight** *SFP optical ports do not support the **10** or **100** option.*
Duplex	Set the duplex mode of the port. • Auto: auto-negotiation • Full: full duplex • Half: half duplex **Highlight** *Ethernet electrical ports whose transmission rate is configured as 1000 Mbps and SFP optical ports do not support the **half** option.*
Link Type	Set the link type of the current port, which can be access, hybrid, or trunk. For details, refer to *VLAN Configuration*. **Highlight** *To change the link type of a port from trunk to hybrid or vice versa, you must first set its link type to access.*
PVID	Set the default VLAN ID of the interface. For details about setting the PVID, refer to *VLAN Configuration*. **Highlight** *To make sure a link properly transmits packets, the trunk or hybrid ports at the two ends of the link must have the same PVID.*

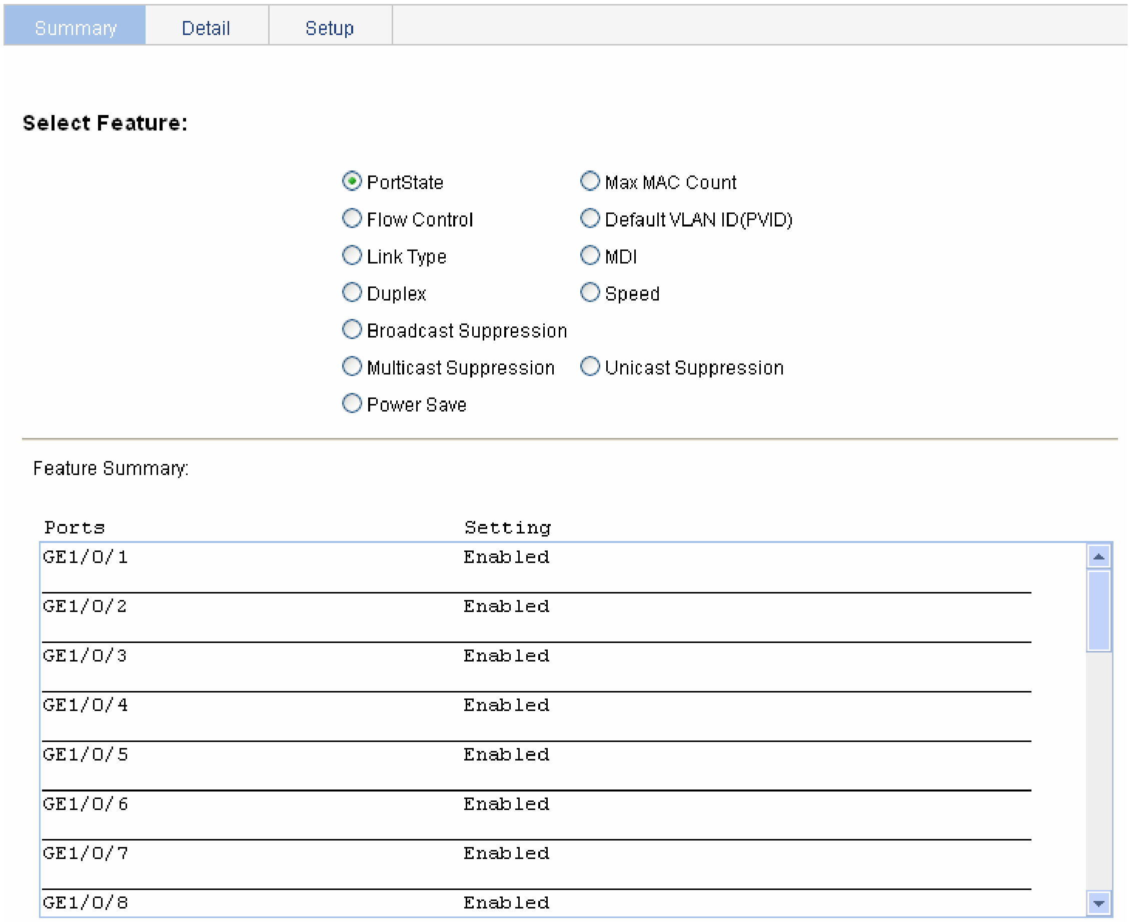
Item	Description
MDI	Set the Medium Dependent Interface (MDI) mode of the port. Two types of Ethernet cables can be used to connect Ethernet devices: crossover cable and straight-through cable. To accommodate these two types of cables, an Ethernet port can operate in one of the following three MDI modes: across, normal, and auto. An Ethernet port is composed of eight pins. By default, each pin has its particular role. For example, pin 1 and pin 2 are used for transmitting signals; pin 3 and pin 6 are used for receiving signals. You can change the pin roles by setting the MDI mode. • For an Ethernet port in across mode, pin 1 and pin 2 are used for transmitting signals; pin 3 and pin 6 are used for receiving signals. The pin roles are not changed. • For an Ethernet port in auto mode, the pin roles are decided through auto negotiation. • For an Ethernet port in normal mode, the pin roles are changed. Pin 1 and pin 2 are used for receiving signals; pin 3 and pin 6 are used for transmitting signals. To enable normal communication, you must connect the local transmit pins to the remote receive pins. Therefore, you should configure the MDI mode depending on the cable types. • Normally, the auto mode is recommended. The other two modes are used only when the device cannot determine the cable type. • When straight-through cables are used, the local MDI mode must be different from the remote MDI mode. • When crossover cables are used, the local MDI mode must be the same as the remote MDI mode, or the MDI mode of at least one end must be set to **auto**. **Highlight** *SFP optical ports do not support this feature.*
Flow Control	Enable or disable flow control on the port. With flow control enabled at both sides, when traffic congestion occurs on the ingress port, the ingress port will send a Pause frame notifying the egress port to temporarily suspend the sending of packets. The egress port is expected to stop sending any new packet when it receives the Pause frame. In this way, flow control helps to avoid dropping of packets. **Highlight** *Flow control works only after it is enabled on both the ingress and egress ports.*
Power Save	Enable or disable auto power down on the port. With auto power down enabled, when an Ethernet port does not receive any packet for a certain period of time, it automatically enters the power save mode and resumes its normal state upon the arrival of a packet. By default, auto power down is disabled.
Max MAC Count	Set the MAC learning limit on the port. Available options include: • User Defined: Select this option to set the limit manually. • No Limited: Select this option to set no limit.

Item	Description
Broadcast Suppression	Set broadcast suppression on the port. You can suppress broadcast traffic by percentage or by PPS as follows: • ratio: Sets the maximum percentage of broadcast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. • pps: Sets the maximum number of broadcast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. • kbps: Sets the maximum number of broadcast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. **Highlight** *Do not configure this item if the storm constrain function for broadcast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for broadcast traffic on a port, select* ***Device*** > ***Storm Constrain****.*
Multicast Suppression	Set multicast suppression on the port. You can suppress multicast traffic by percentage or by PPS as follows: • ratio: Sets the maximum percentage of multicast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. • pps: Sets the maximum number of multicast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. • kbps: Sets the maximum number of multicast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. **Highlight** *Do not configure this item if the storm constrain function for multicast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for multicast traffic on a port, select* ***Device*** > ***Storm Constrain****.*
Unicast Suppression	Set unicast suppression on the port. You can suppress unicast traffic by percentage or by PPS as follows: • ratio: Sets the maximum percentage of unicast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. • pps: Sets the maximum number of unicast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. • kbps: Sets the maximum number of unicast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below **Highlight** *Do not configure this item if the storm constrain function for unicast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for unicast traffic on a port, select* ***Device*** > ***Storm Constrain****.*
Selected Ports	Port or ports that you have selected from the chassis front panel, and for which you have set operation parameters

Viewing the Operation Parameters of a Port

Select **Device** > **Port Management** from the navigation tree. The **Summary** tab is displayed by default. Select the parameter you want to view by clicking the radio button before it to display the setting of this parameter for all the ports in the lower part of the page, as shown in Figure 1-2.

Figure 1-2 The **Summary** tab



Select Feature:

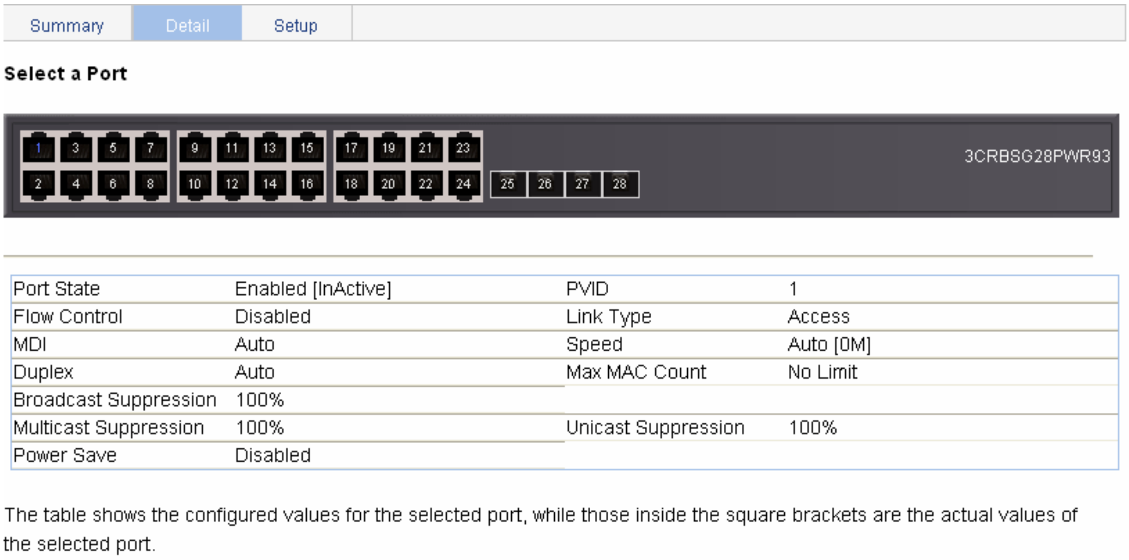
● PortState ○ Max MAC Count
○ Flow Control ○ Default VLAN ID(PVID)
○ Link Type ○ MDI
○ Duplex ○ Speed
○ Broadcast Suppression
○ Multicast Suppression ○ Unicast Suppression
○ Power Save

Feature Summary:

Ports	Setting
GE1/0/1	Enabled
GE1/0/2	Enabled
GE1/0/3	Enabled
GE1/0/4	Enabled
GE1/0/5	Enabled
GE1/0/6	Enabled
GE1/0/7	Enabled
GE1/0/8	Enabled

Select **Device** > **Port Management** from the navigation tree, select the **Details** tab on the page that appears, and then click the port whose operation parameters you want to view in the chassis front panel, as shown in Figure 1-3. The operation parameter settings of the selected port are displayed on the lower part of the page; those inside the square brackets are the actual values of the selected port

Figure 1-3 The **Details** tab



Select a Port

Port State	Enabled [InActive]	PVID	1
Flow Control	Disabled	Link Type	Access
MDI	Auto	Speed	Auto [0M]
Duplex	Auto	Max MAC Count	No Limit
Broadcast Suppression	100%		
Multicast Suppression	100%	Unicast Suppression	100%
Power Save	Disabled		

The table shows the configured values for the selected port, while those inside the square brackets are the actual values of the selected port.

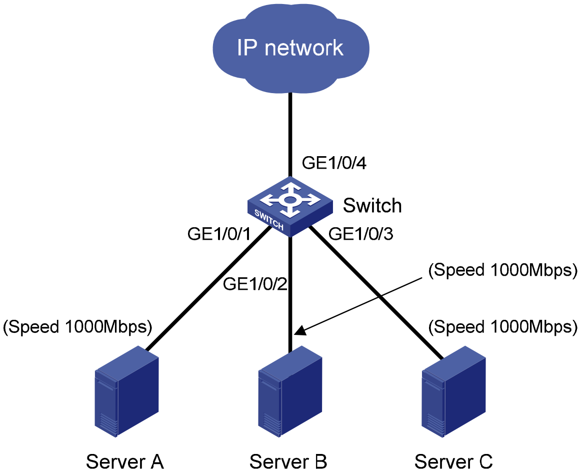
Port Management Configuration Example

Network requirements

As shown in Figure 1-4:

- Server A, Server B, and Server C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 or the switch respectively. The rates of the network adapters of these servers are all 1000 Mbps.
- The switch connects to the external network through GigabitEthernet 1/0/4 whose rate is 1000 Mbps.
- To avoid congestion at the egress port, GigabitEthernet 1/0/4, configure the auto-negotiation rate range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.

Figure 1-4 Network diagram for port rate configuration

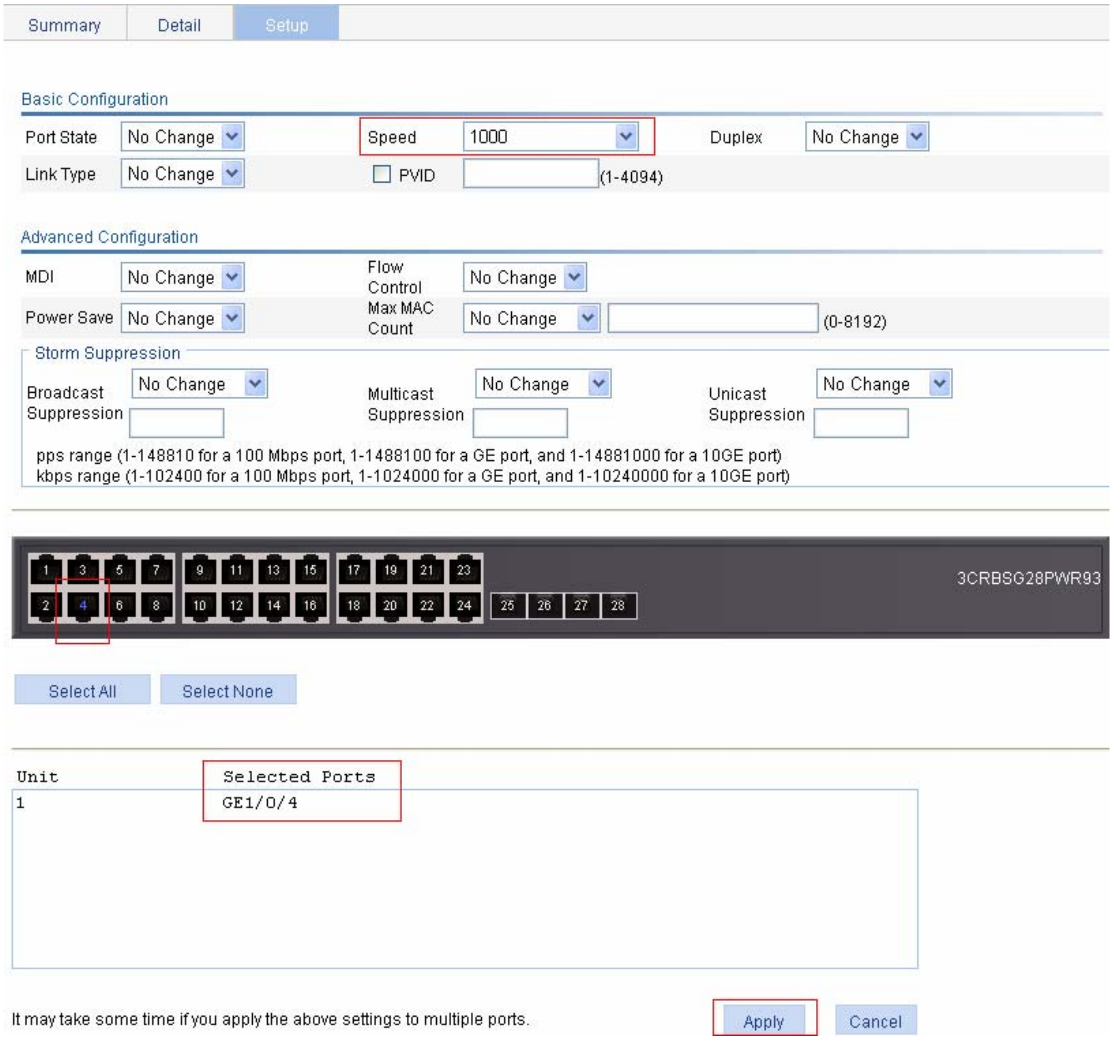


Configuration procedure

# Set the rate of GigabitEthernet 1/0/4 to 1000 Mbps.

- Select **Device** > **Port Management** from the navigation tree, click the **Setup** tab to enter the page shown in Figure 1-5, and make the following configurations:

Figure 1-5 Configure the rate of GigabitEthernet 1/0/4



Basic Configuration

Port State: No Change
Speed: 1000
Duplex: No Change
Link Type: No Change
□ PVID (1-4094)

Advanced Configuration

MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)

Storm Suppression

Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Unit	Selected Ports
1	GE1/0/4

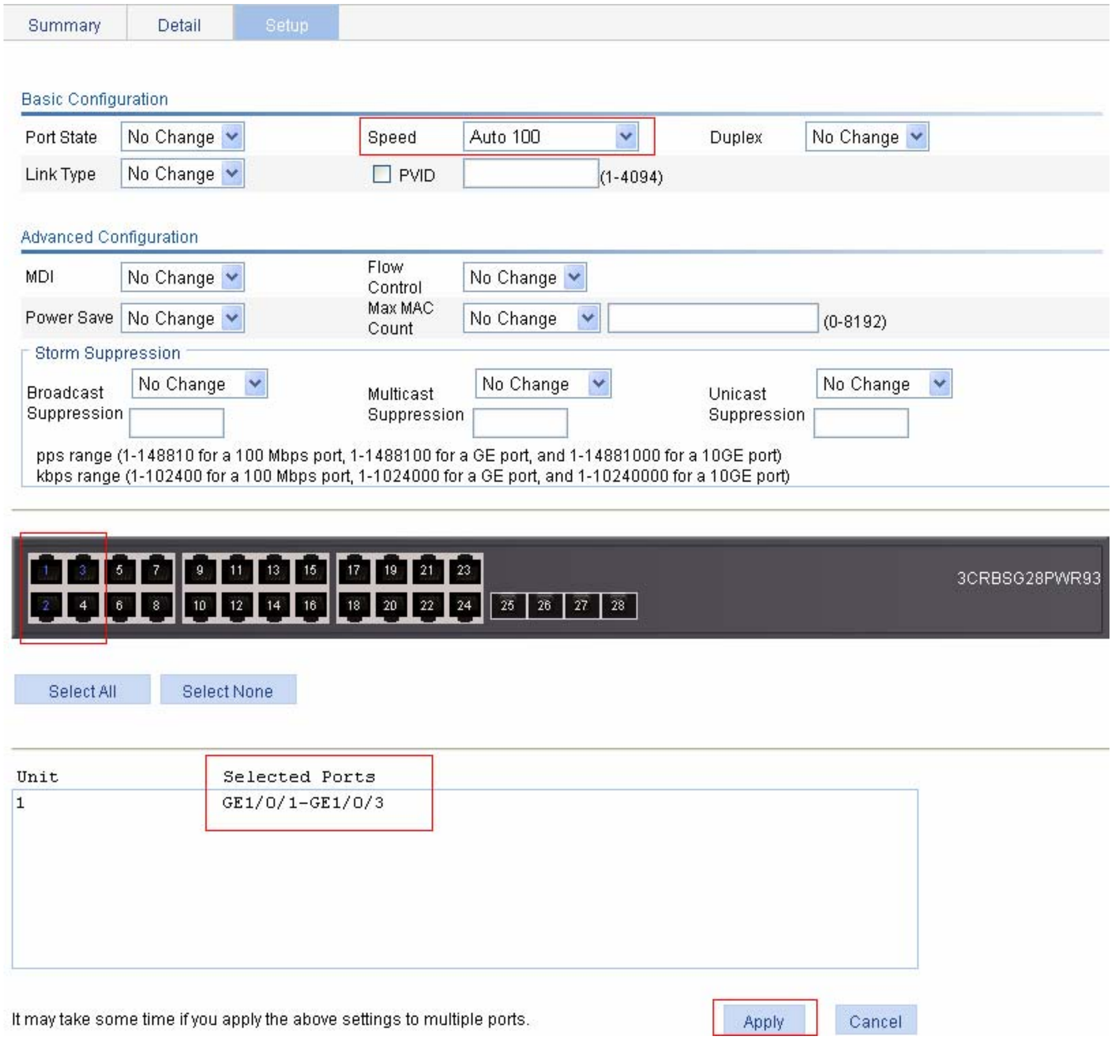
It may take some time if you apply the above settings to multiple ports.

- Select **100** in the **Speed** dropdown list.
- Select GigabitEthernet 1/0/4 on the chassis front panel.
- Click **Apply** to end the operation.

# Batch configure the auto-negotiation rate range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.

- Select **Auto 100** in the **Speed** dropdown list on the page shown in Figure 1-6.
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply** to end the operation.

Figure 1-6 Batch configure port rate



Port State: No Change
Speed: Auto 100
Duplex: No Change
Link Type: No Change
□ PVID (1-4094)

MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)

Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

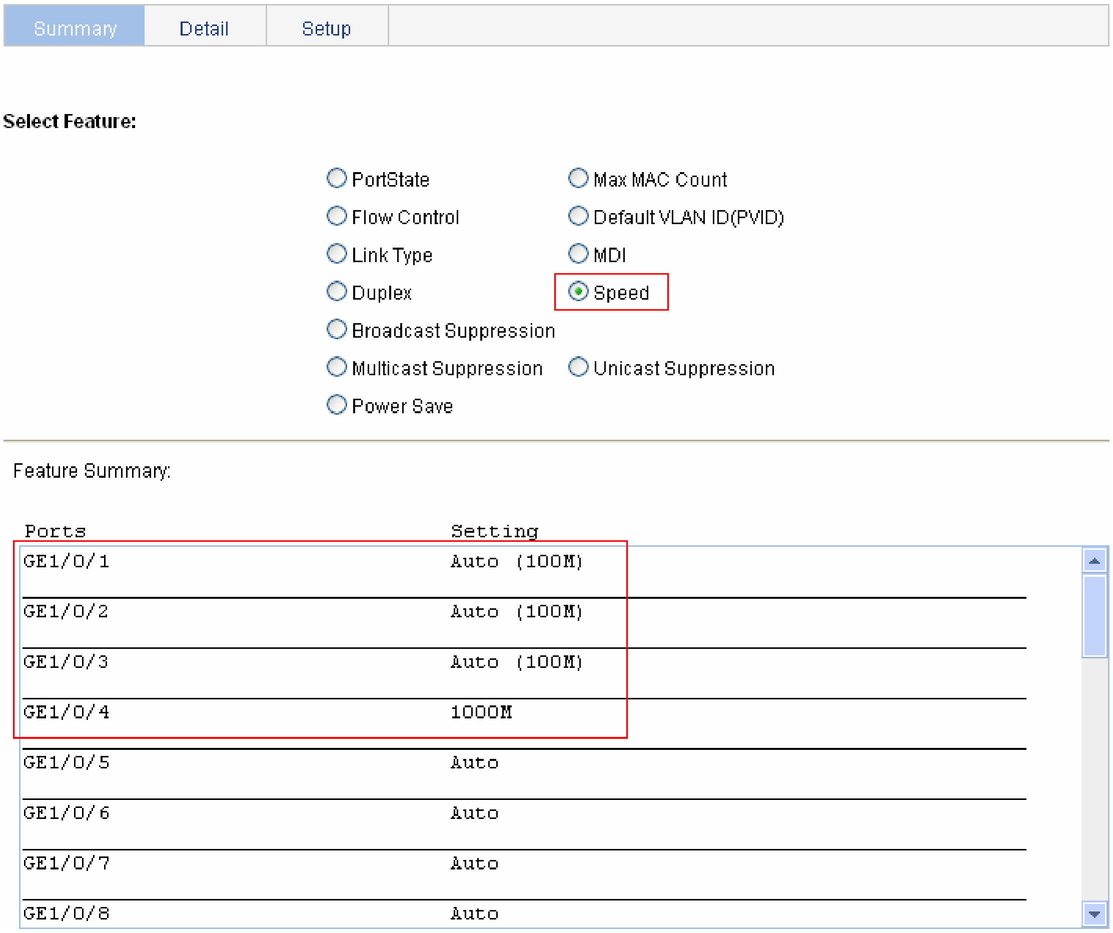
Unit	Selected Ports
1	GE1/0/1-GE1/0/3

It may take some time if you apply the above settings to multiple ports.

# Display the rate settings of ports.

- Click the **Summary** tab.
- Select the **Speed** option to display the rate information of all ports on the lower part of the page, as shown in Figure 1-7.

Figure 1-7 Display the rate settings of ports



Select Feature:

○ PortState ○ Max MAC Count
○ Flow Control ○ Default VLAN ID(PVID)
○ Link Type ○ MDI
○ Duplex ● Speed
○ Broadcast Suppression
○ Multicast Suppression ○ Unicast Suppression
○ Power Save

Feature Summary:

Ports	Setting
GE1/0/1	Auto (100M)
GE1/0/2	Auto (100M)
GE1/0/3	Auto (100M)
GE1/0/4	1000M
GE1/0/5	Auto
GE1/0/6	Auto
GE1/0/7	Auto
GE1/0/8	Auto

Table of Contents

1 Port Mirroring Configuration

Introduction to Port Mirroring

Port mirroring is to copy the packets passing through a port (called a mirroring port) to another port (called the monitor port) connected with a monitoring device for packet analysis.

You can select to port-mirror inbound, outbound, or bidirectional traffic on a port as needed.

Implementing Port Mirroring

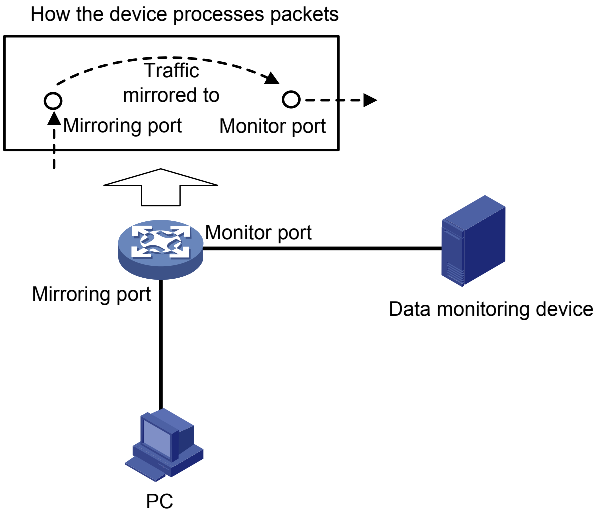
Port mirroring is implemented through local port mirroring groups. The following subsections describe how local port mirroring is implemented.

Local port mirroring

In local port mirroring, all packets (including protocol and data packets) passing through a port can be mirrored. Local port mirroring is implemented through a local mirroring group.

As shown in Figure 1-1, packets on the mirroring port are mirrored to the monitor port for the data monitoring device to analyze.

Figure 1-1 Local port mirroring implementation



Configuring Port Mirroring

Configuration Task List

Configuring local port mirroring

To configure local port mirroring, you must create a local mirroring group and then specify the mirroring ports and monitor port for the group.

Perform the tasks described in Table 1-1 to configure local port mirroring:

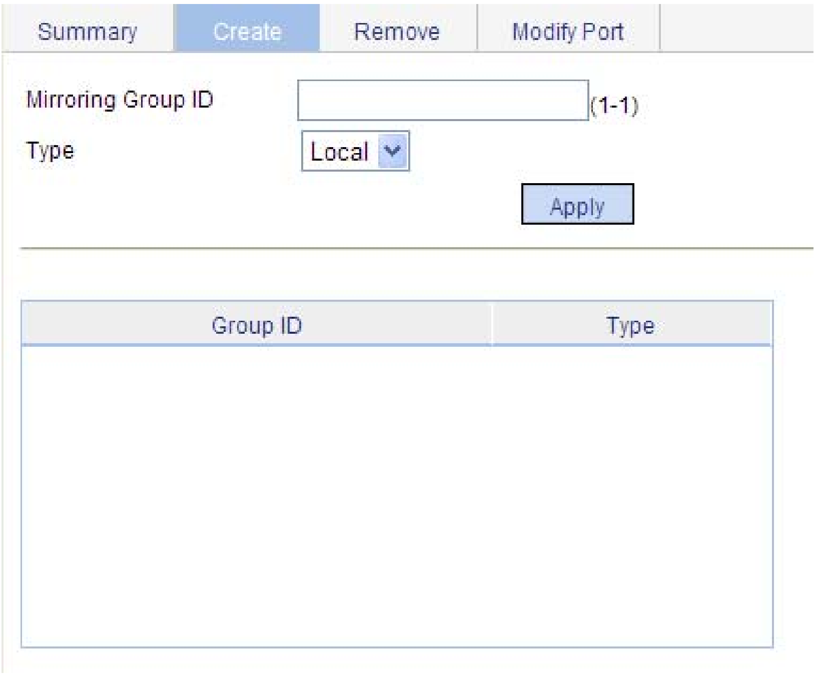
Table 1-1 Local port mirroring configuration task list

Task	Remarks
Create a local mirroring group	Required Refer to section Creating a Mirroring Group for details.
Configure the mirroring ports	Required Refer to section Configuring Ports for a Mirroring Group for details. During configuration, you need to select the port type **Mirror Port**. You can configure multiple mirroring ports for a mirroring group.
Configure the monitor port	Required Refer to section Configuring Ports for a Mirroring Group for details. During configuration, you need to select the port type **Monitor Port**. You can configure one only monitor port for a mirroring group.

Creating a Mirroring Group

Select **Device** > **Port Mirroring** from the navigation tree and click **Create** to enter the page for creating a mirroring group, as shown in Figure 1-2.

Figure 1-2 Create a mirroring group



Mirroring Group ID (1-1)

Type Local

Group ID	Type

Table 1-2 describes the configuration items of creating a mirroring group.

Table 1-2 Configuration items of creating a mirroring group

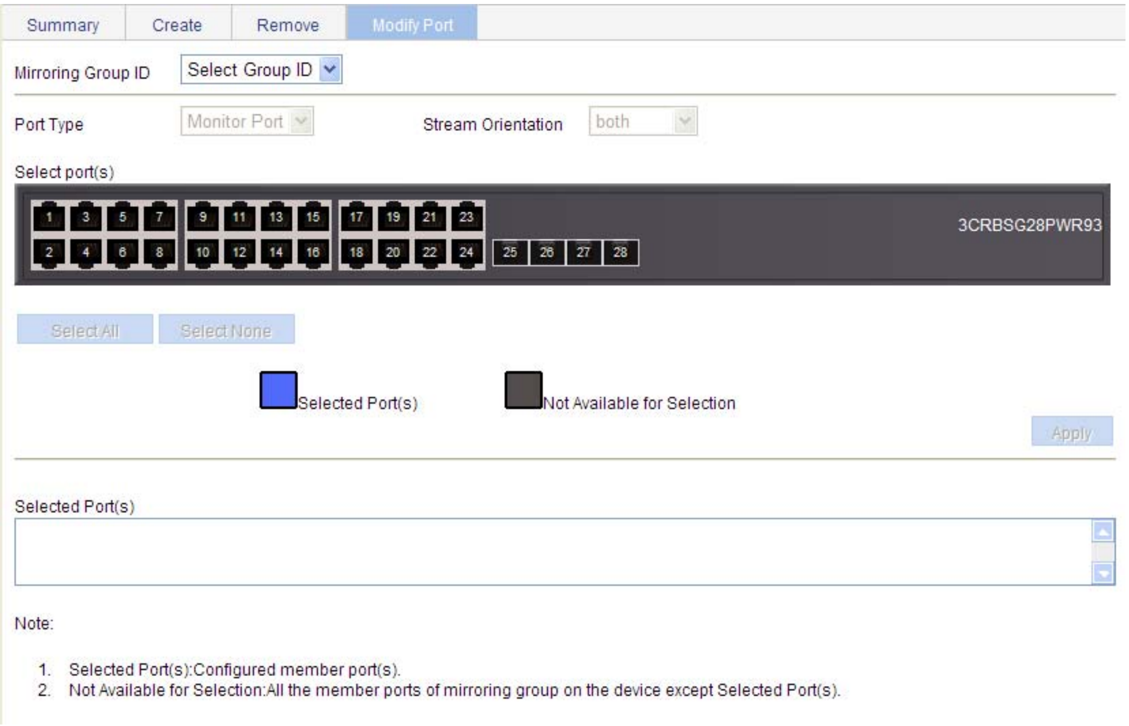
Item	Description
Mirroring Group ID	ID of the mirroring group to be created
Type	Specify the type of the mirroring group to be created: • **Local**: Creates a local mirroring group.

Return to Local port mirroring configuration task list.

Configuring Ports for a Mirroring Group

Select **Device** > **Port Mirroring** from the navigation tree and click **Modify Port** to enter the page for configuring ports for a mirroring group, as shown in Figure 1-3.

Figure 1-3 The Modify Port tab



Mirroring Group ID: Select Group ID

Port Type: Monitor Port   Stream Orientation: both

Select port(s)

🟦 Selected Port(s)   ■ Not Available for Selection

Selected Port(s)

Note:

1. Selected Port(s):Configured member port(s).
2. Not Available for Selection:All the member ports of mirroring group on the device except Selected Port(s).

Table 1-3 describes the configuration items of configuring ports for a mirroring group.

Table 1-3 Configuration items of configuring ports for a mirroring group

Item	Description	
Mirroring Group ID	ID of the mirroring group to be configured The available groups were created previously.	
Port Type	Set the type of the port to be configured	Configure ports for a local mirroring group: • **Monitor Port**: Configures the monitor ports for the local mirroring group. • **Mirror Port**: Configures mirroring ports for the local mirroring group.

Item	Description
Stream Orientation	Set the direction of the traffic monitored by the monitor port of the mirroring group This configuration item is available when **Mirror Port** is selected is the **Port Type** drop-down list. • **both**: Mirrors both received and sent packets on mirroring ports. • **inbound**: Mirrors only packets received by mirroring port. • **outbound**: Mirrors only packets sent by mirroring ports.
Select port(s)	Click the ports to be configured on the chassis front panel.

Return to Local port mirroring configuration task list.

Configuration Examples

Local Port Mirroring Configuration Example

Network requirements

The customer network is as described below:

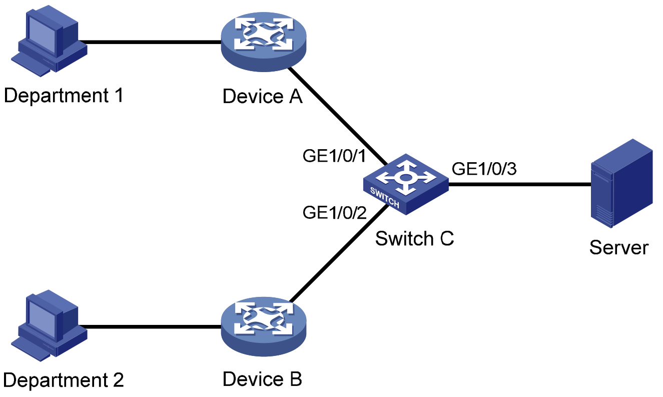
- Department 1 accesses Switch C through GigabitEthernet 1/0/1.
- Department 2 accesses Switch C through GigabitEthernet 1/0/2.
- Server is connected to GigabitEthernet 1/0/3 of Switch C.

Configure port mirroring to monitor the bidirectional traffic of Department 1 and Department 2 on the server.

To satisfy the above requirement through local port mirroring, perform the following configuration on Switch C:

- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as mirroring ports.
- Configure GigabitEthernet 1/0/3 as the monitor port.

Figure 1-4 Network diagram for local port mirroring configuration

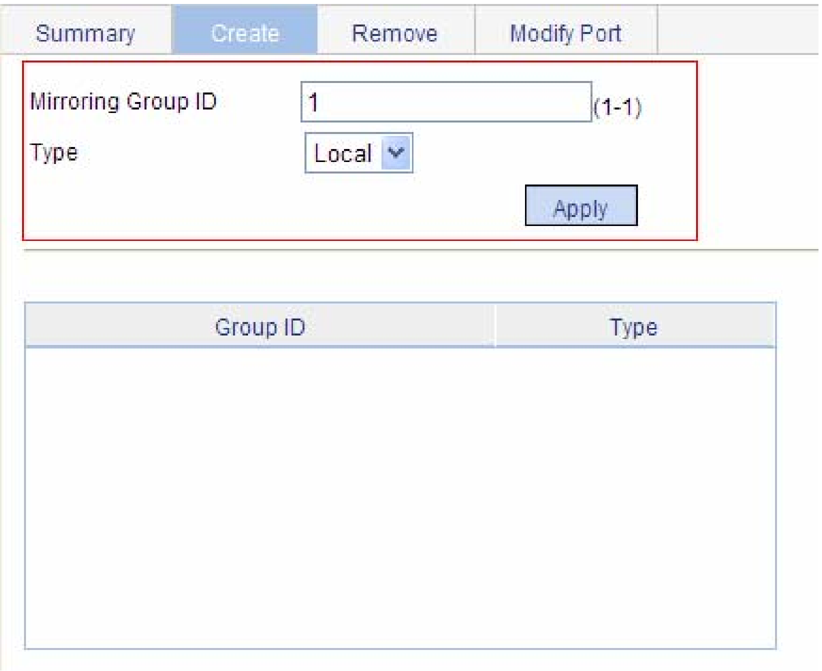


Configuration procedure

# Create a local mirroring group.

Select **Device** > **Port Mirroring** from the navigation tree and click **Create** to enter the page for creating mirroring groups, as shown in Figure 1-5.

Figure 1-5 Create a local mirroring group



Mirroring Group ID: 1 (1-1)

Type: Local

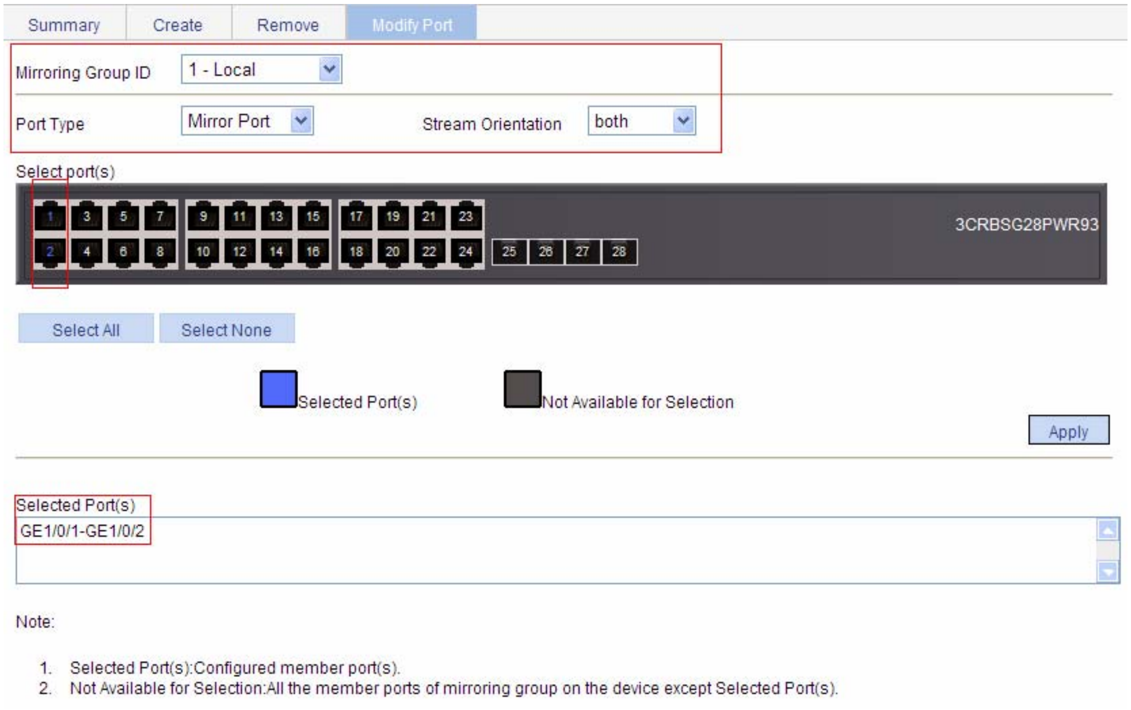
Group ID	Type

- Type in mirroring group ID **1**.
- Select **Local** in the **Type** drop-down list.
- Click **Apply**.

# Configure the mirroring ports.

Click **Modify Port** to enter the page for configuring ports for the mirroring group, as shown in Figure 1-6.

Figure 1-6 Configure the mirroring ports



Mirroring Group ID: 1 - Local

Port Type: Mirror Port

Stream Orientation: both

Select port(s)

🟦 Selected Port(s) ▨ Not Available for Selection

Selected Port(s)

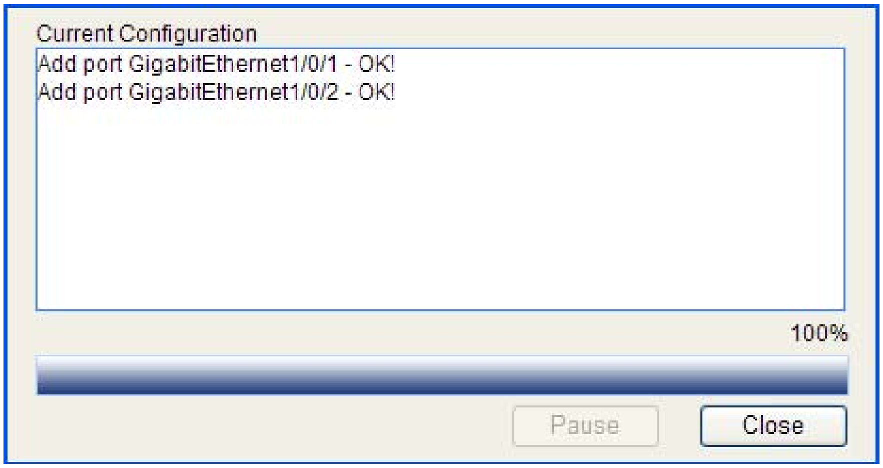
GE1/0/1-GE1/0/2

Note:

1. Selected Port(s):Configured member port(s).
2. Not Available for Selection:All the member ports of mirroring group on the device except Selected Port(s).

- Select **1 – Local** in the **Mirroring Group ID** drop-down list.
- Select **Mirror Port** in the **Port Type** drop-down list.
- Select **both** in the **Stream Orientation** drop-down list.
- Select GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the chassis front panel.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-7.

Figure 1-7 Configuration progress dialog box



Current Configuration

Add port GigabitEthernet1/0/1 - OK!
Add port GigabitEthernet1/0/2 - OK!

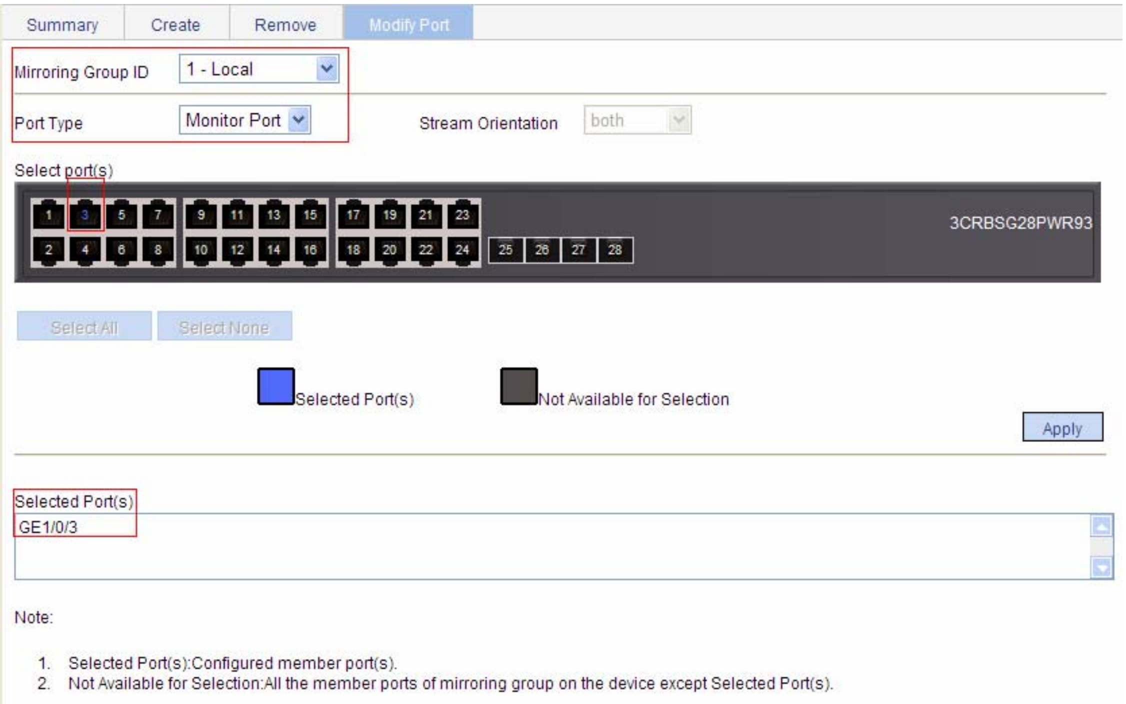
100%

- After the configuration process is complete, click **Close**.

# Configure the monitor port.

Click **Modify Port** to enter the page for configuring ports for the mirroring group, as shown in Figure 1-8.

Figure 1-8 Configure the monitor port



Mirroring Group ID: 1 - Local

Port Type: Monitor Port

Stream Orientation: both

Select port(s)

Selected Port(s)

GE1/0/3

Note:

1. Selected Port(s):Configured member port(s).
2. Not Available for Selection:All the member ports of mirroring group on the device except Selected Port(s).

- Select **1 – Local** in the **Mirroring Group ID** drop-down list.
- Select **Monitor Port** in the **Port Type** drop-down list.
- Select GigabitEthernet 1/0/3 on the chassis front panel.

- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

Configuration Guidelines

Pay attention to the following points during local port mirroring configuration:

- To ensure operation of your device, do not enable STP, MSTP, or RSTP on the monitor port.
- You can configure multiple mirroring ports but only one monitor port for a local mirroring group.

Table of Contents

1 User Management

Overview

In the user management part, you can:

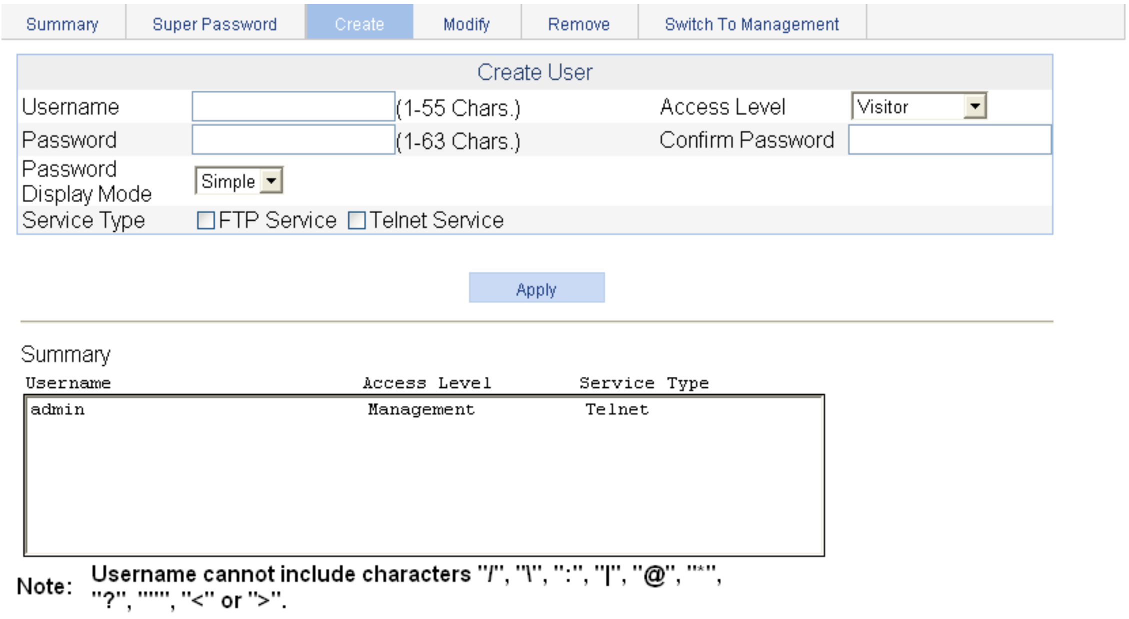
- Set the username, password, and access level for an FTP or Telnet user.
- Set the super password for switching the current Web user level to the management level.
- Switch the current Web user access level to the management level.

Users

Creating a User

Select **Device** > **Users** from the navigation tree, and click the **Create** tab to enter the page for creating local users, as shown in Figure 1-1.

Figure 1-1 Create a user



Create User

Username	(1-55 Chars.)	Access Level	Visitor
Password	(1-63 Chars.)	Confirm Password	
Password Display Mode	Simple		
Service Type	□FTP Service □Telnet Service		

Summary

Username	Access Level	Service Type
admin	Management	Telnet

Note: Username cannot include characters "/", "\", ":", "|", "@", "*", "?", """", "<" or ">".

Table 1-1 describes the configuration items for creating a user.

Table 1-1 Configuration items for creating a user

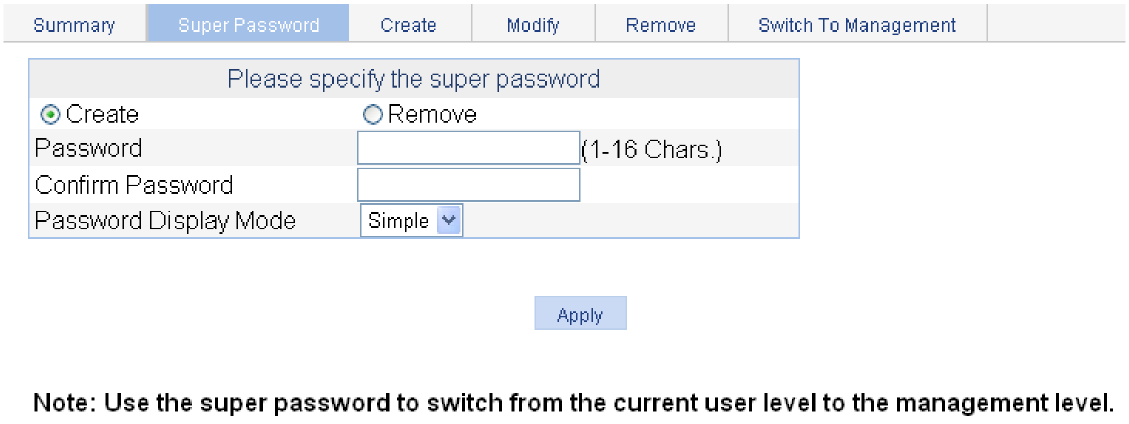
Item	Description
Username	Set the username for a user
Access Level	Set the access level for a user. Users of different levels can perform different operations. Web user levels, from low to high, are visitor, monitor, configure, and management. • Visitor: Users of visitor level can only use the network diagnostic tool ping and trace route. They can neither access the device data nor configure the device. • Monitor: Users of this level can only access the device data but cannot configure the device. • Configure: Users of this level can access data on the device and configure the device, but they cannot upgrade the host software, add/delete/modify users, or back up/restore the application file. • Management: Users of this level can perform any operations on the device.
Password	Set the password for a user • When the password mode is **Simple**, the input password is in plain text. • When the password mode is **Cipher**, the input password is either in plain text or cipher text with a length of 24 or 88. In this case, the input plain password with the length smaller than or equal to 16 will be converted to a cipher password with a length of 24; the input plain password with a length greater than 16 but smaller than 63 will be converted to a cipher password with a length of 88. When the length of the input password is 24, if the system can decrypt the password, it considers the password as a ciphertext password; if not, the system considers the password as a plaintext password. When the length of the input password is 88, if the system can decrypt the password, it considers the password as a ciphertext password; if not, the system prompts that the password is invalid.
Confirm Password	Input the same password again. Otherwise, the system prompts that the two passwords input are not consistent when you apply the configuration.
Password Display Mode	Set the password display mode. • Simple: The password will be saved in the configuration file in plain text. • Cipher: The password will be saved in the configuration file in cipher text, even if the password is input in plain text when configured. The plaintext password is not safe, and you are recommended to use the ciphertext password. No matter the password mode is set to **Simple** or **Cipher**, you must enter the password in the form of plain text for login authentication.
Service Type	Set the service type, including FTP and Telnet services. You must select either of them.

Setting the Super Password

In this part, users of the management level can specify the password for a lower-level user to switch from the current access level to the management level. If no such a password is configured, the switchover will fail.

Select **Device** > **Users** from the navigation tree, and click the **Super Password** tab to enter the super password configuration page.

Figure 1-2 Super password



Please specify the super password

● Create	○ Remove
Password	(1-16 Chars.)
Confirm Password	
Password Display Mode	Simple

Note: Use the super password to switch from the current user level to the management level.

Table 1-2 describes the configuration items of specifying a super password.

Table 1-2 Super password configuration items

Item	Description
Create/Remove	Set the operation type: • Create: Configure or modify the super password. • Remove: Remove the current super password.
Password	Set the password for a user to switch to the management level.
Confirm Password	Input the same password again. Otherwise, the system prompts that the two passwords input are not consistent when you apply the configuration.
Password Display Mode	Set the password display mode. • Simple: The password will be saved in the configuration file in plain text. • Cipher: The password will be saved in the configuration file in cipher text. The plaintext password is not safe, and you are recommended to use the ciphertext password.

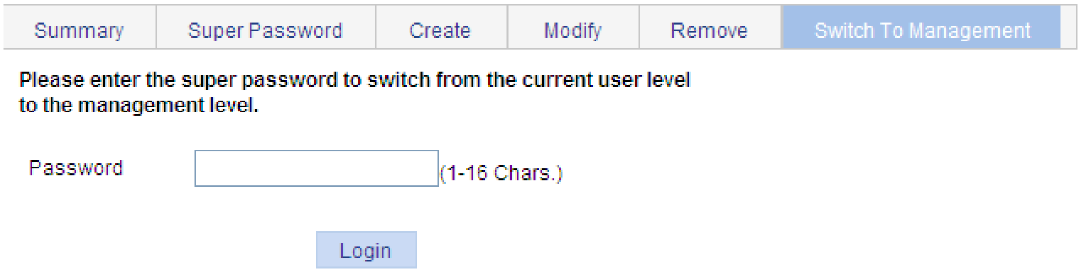
Switching the User Access Level to the Management Level

This function is provided for a user to switch the current user level to the management level. Note the following:

- Before switching, make sure that the super password is already configured. A user cannot switch to the management level without a super password.
- The access level switchover of a user is valid for the current login only. The access level configured for the user is not changed. When the user re-logs in to the Web interface, the access level of the user is still the original level.

Select **Device** > **Users** from the navigation tree, and click the **Switch To Management** tab to enter the access level switching page. Type the super password and click **Login**.

Figure 1-3 Switch to the management level.



Please enter the super password to switch from the current user level to the management level.

Password (1-16 Chars.)

Table of Contents

1 Loopback Test Configuration

Overview

You can check whether an Ethernet port works normally by performing the Ethernet port loopback test, during which the port cannot forward data packets normally.

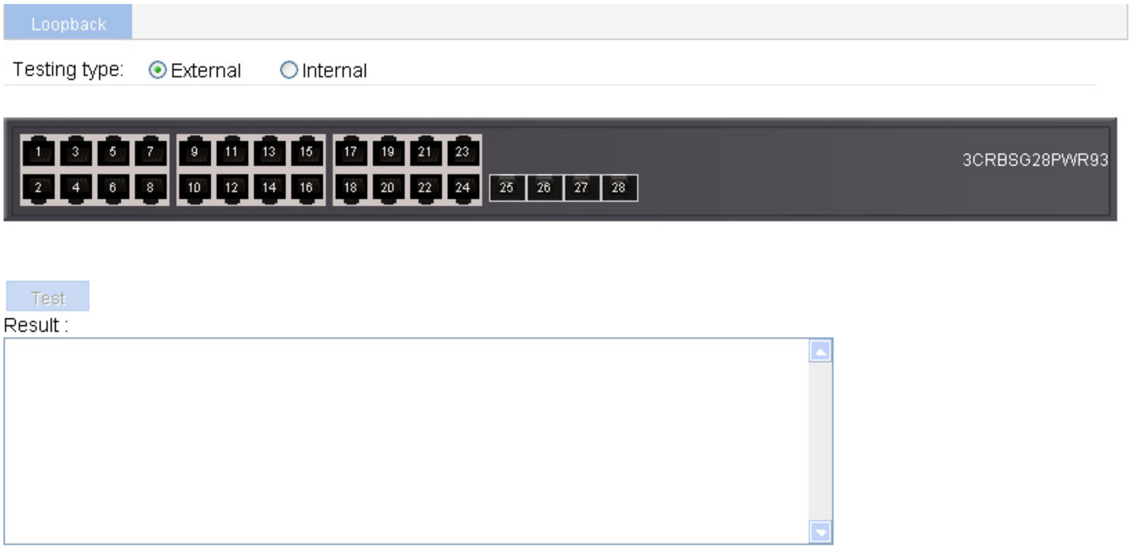
Ethernet port loopback test can be an internal loopback test or an external loopback test.

- In an internal loopback test, self loop is established in the switching chip to check whether there is a chip failure related to the functions of the port.
- In an external loopback test, a loopback plug is used on the port. Packets forwarded by the port will be received by itself through the loopback plug. The external loopback test can be used to check whether there is a hardware failure on the port.

Loopback Operation

Select **Device** > **Loopback** from the navigation tree to enter the loopback test configuration page, as shown in Figure 1-1.

Figure 1-1 Loopback test configuration page



Testing type: ● External ○ Internal

Result :

Table 1-1 describes the loopback test configuration items.

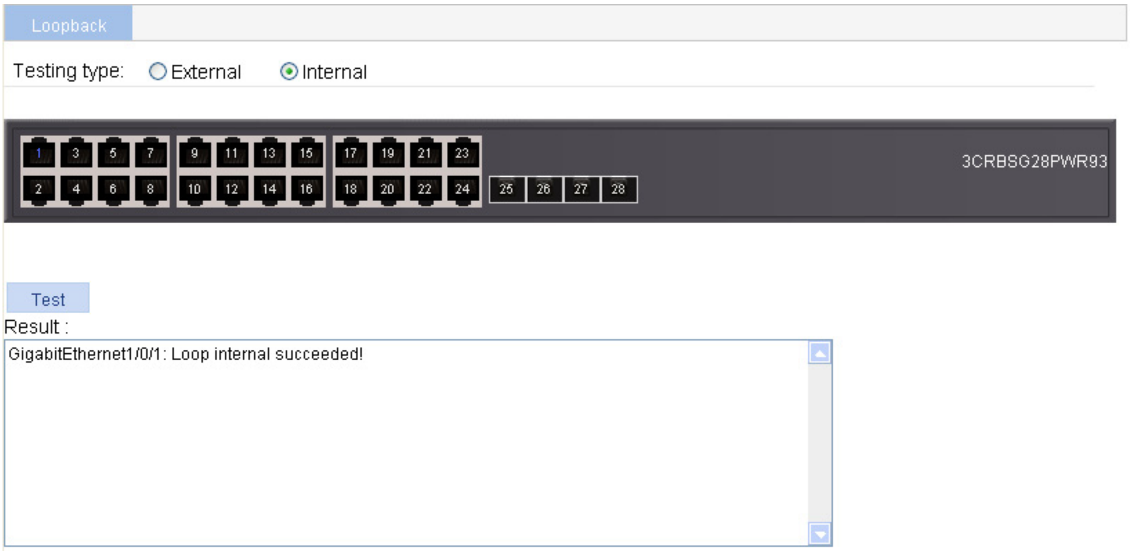
Table 1-1 Loopback test configuration items

Item		Description
Testing type	External	Sets the loopback test type, which can be **External** or **Internal**.
	Internal	

After selecting a testing type, you need to select a port on which you want to perform the loopback test from the chassis front panel.

After that, click **Test** to start the loopback test, and you can see the test result in the **Result** text box, as shown in Figure 1-2.

Figure 1-2 Loopback test result



GigabitEthernet1/0/1: Loop internal succeeded!

Configuration Guidelines

Note the following when performing a loopback test:

- You can perform an internal loopback test but not an external loopback test on a port that is physically down, while you can perform neither test on a port that is manually shut down.
- The system does not allow **Rate**, **Duplex**, **Cable Type** and **Port Status** configuration on a port under a loopback test.
- An Ethernet port works in full duplex mode when the loopback test is performed, and restores its original duplex mode after the loopback test.

Table of Contents

1 VCT

Overview

Note

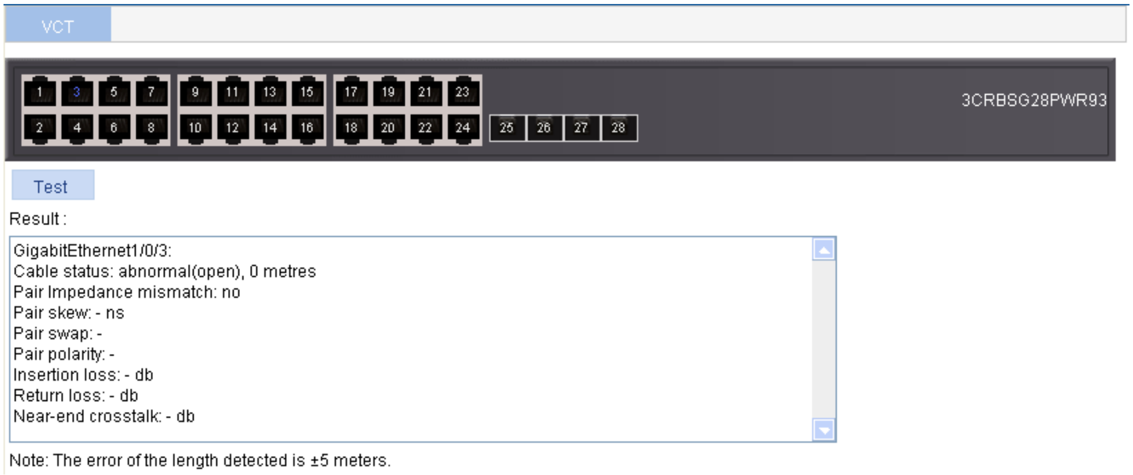
- The optical interface of a SFP port does not support this feature.
- A link in the up state goes down and then up automatically if you perform this operation on one of the Ethernet interfaces forming the link.

You can use the Virtual Cable Test (VCT) function to check the status of the cable connected to an Ethernet port on the device. The result is returned in less than 5 seconds. The test covers whether short circuit or open circuit occurs on the cable and the length of the faulty cable.

Testing Cable Status

Select **Device** > **VCT** from the navigation tree to enter the page for testing cable status. Select the port you want to test in the chassis front panel and then click **Test**. The test result is returned in less than 5 seconds and displayed in the **Result** text box, as shown in Figure 1-1.

Figure 1-1 Test the status of the cable connected to an Ethernet port



Result :

```
GigabitEthernet1/0/3:
Cable status: abnormal(open), 0 metres
Pair Impedance mismatch: no
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Note: The error of the length detected is ±5 meters.

Table 1-1 describes in details the cable test result.

Table 1-1 Description on the cable test result

Item	Description
Cable status	Status and length of the cable. The status of a cable can be normal, abnormal, abnormal(open), abnormal(short), or failure. • When a cable is normal, the cable length displayed is the total length of the cable. • When a cable is not normal, the cable length displayed is the length of the cable between the current port and the location where fault occurs. **Highlight** *The error of the length detected is within 5 meters.*

Table of Contents

1 Flow Interval Configuration

Overview

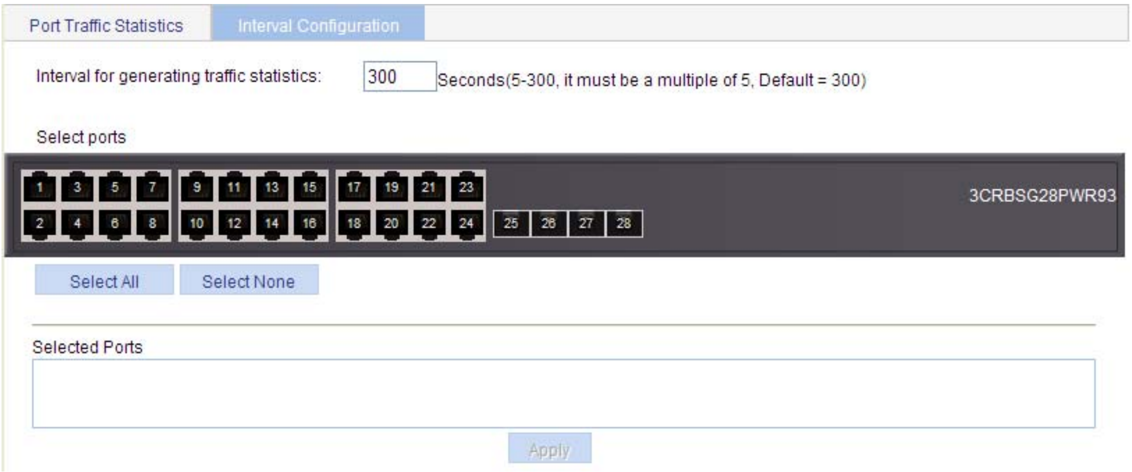
With the flow interval module, you can view the average receiving rate and average sending rate of a port over the specified interval.

Monitoring Port Traffic Statistics

Setting the Traffic Statistics Generating Interval

Select **Device** > **Flow interval** from the navigation bar, and click the **Interval Configuration** tab to enter the page shown in Figure 1-1.

Figure 1-1 The page for setting the traffic statistics generating interval



Interval for generating traffic statistics: 300 Seconds(5-300, it must be a multiple of 5, Default = 300)

Selected Ports

Table 1-1 describes the traffic statistics generating interval configuration items.

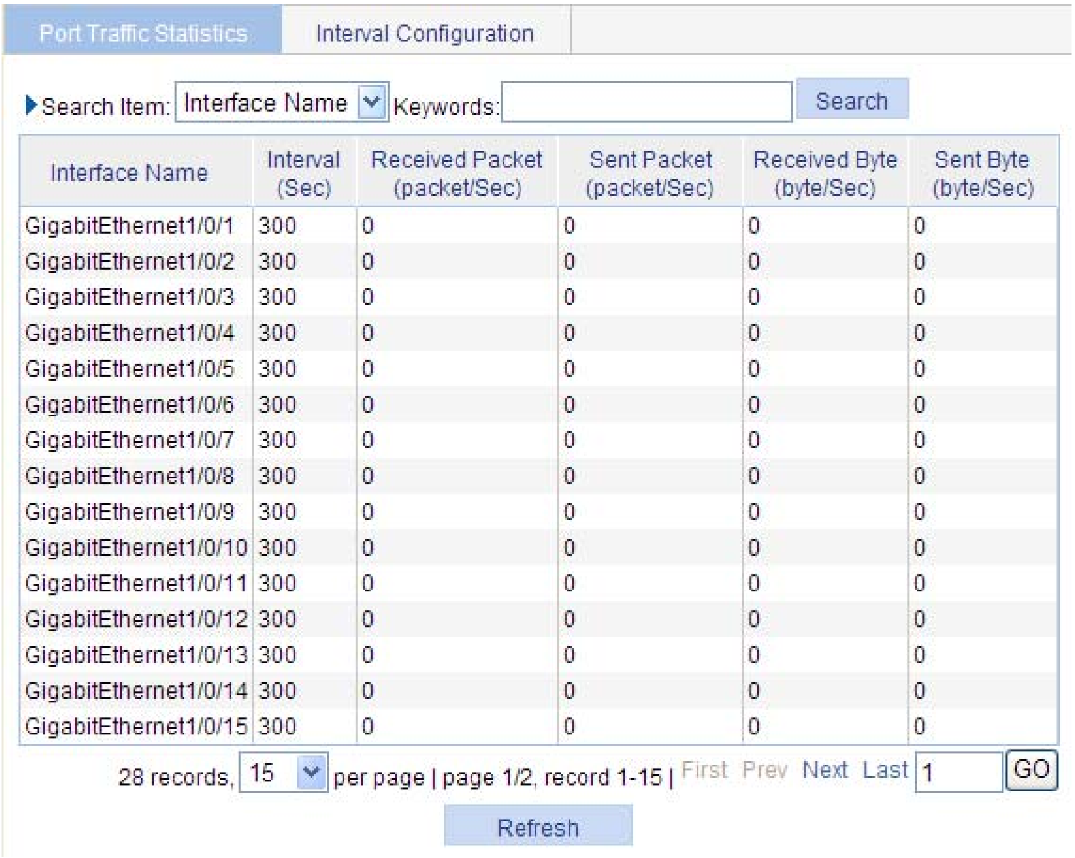
Table 1-1 Traffic statistics generating interval configuration items

Item	Remarks
Interval for generating traffic statistics	Set the interval for generating port traffic statistics.
Select ports	Select ports from the chassis front panel to apply the interval to them.

Viewing Port Traffic Statistics

Select **Device** > **Flow interval** from the navigation tree to enter the **Port Traffic Statistics** tab shown in Figure 1-2. On the tab, you can view the average receiving/sending rate (in both packets per second and bytes per second) of each port over the last interval.

Figure 1-2 Port traffic statistics



Search Item: Interface Name Keywords:

Interface Name	Interval (Sec)	Received Packet (packet/Sec)	Sent Packet (packet/Sec)	Received Byte (byte/Sec)	Sent Byte (byte/Sec)
GigabitEthernet1/0/1	300	0	0	0	0
GigabitEthernet1/0/2	300	0	0	0	0
GigabitEthernet1/0/3	300	0	0	0	0
GigabitEthernet1/0/4	300	0	0	0	0
GigabitEthernet1/0/5	300	0	0	0	0
GigabitEthernet1/0/6	300	0	0	0	0
GigabitEthernet1/0/7	300	0	0	0	0
GigabitEthernet1/0/8	300	0	0	0	0
GigabitEthernet1/0/9	300	0	0	0	0
GigabitEthernet1/0/10	300	0	0	0	0
GigabitEthernet1/0/11	300	0	0	0	0
GigabitEthernet1/0/12	300	0	0	0	0
GigabitEthernet1/0/13	300	0	0	0	0
GigabitEthernet1/0/14	300	0	0	0	0
GigabitEthernet1/0/15	300	0	0	0	0

28 records, 15 per page | page 1/2, record 1-15 | 1

Table of Contents

1 Storm Constrain Configuration

Overview

The storm constrain function limits traffic of a port within a predefined upper threshold to suppress packet storms in an Ethernet. With this function enabled on a port, the system detects the amount of broadcast traffic, multicast traffic, and unicast traffic reaching the port periodically. When a type of traffic exceeds the threshold for it, the function, as configured, blocks or shuts down the port, and optionally, sends trap messages and logs.

⚠ **Caution**

Alternatively, you can configure the storm suppression function to control a specific type of traffic. As the storm suppression function and the storm constrain function are mutually exclusive, do not enable them at the same time on an Ethernet port. For example, with broadcast storm suppression enabled on a port, do not enable storm constrain for broadcast traffic on the port. The storm suppression function is configured in **Device** > **Port Management**. For details, refer to *Port Management*.

With storm constrain enabled on a port, you can specify the system to act as follows when a certain type of traffic (broadcast, multicast, or unicast) exceeds the corresponding upper threshold:

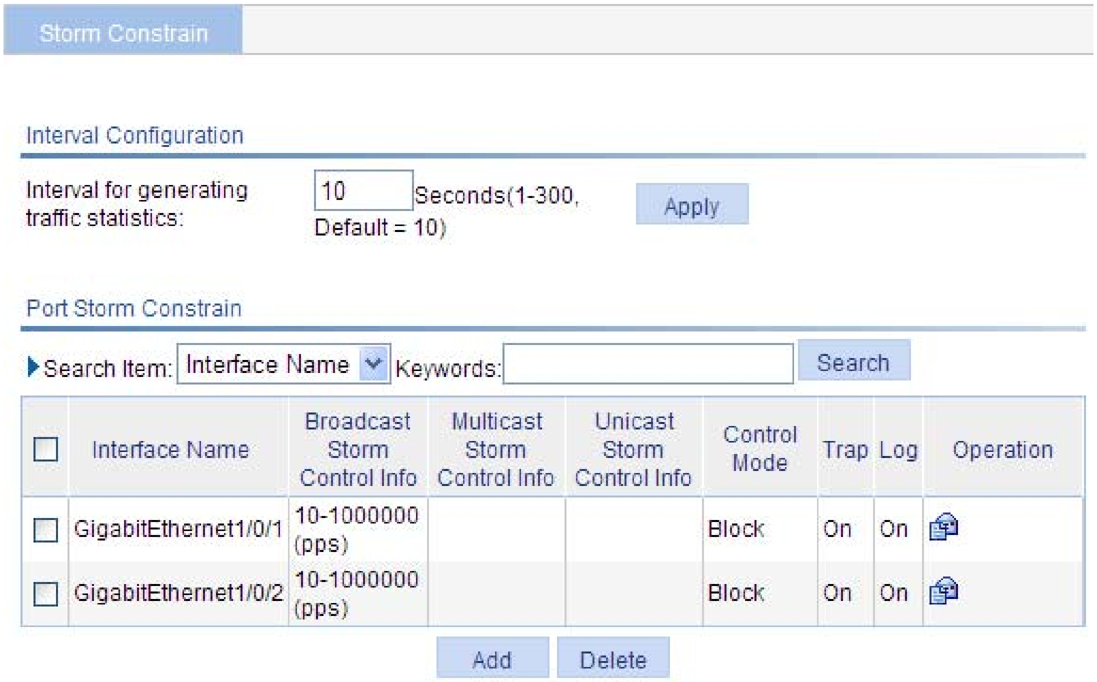
- Block: Block the port. In this case, the port is blocked and thus stops forwarding the traffic of this type until the type of traffic drops down below the lower threshold. Note that a port blocked by the storm constrain function can still forward other types of traffic and collect statistics for the blocked traffic.
- Shutdown: Shut down the port. In this case, the port is shut down and stops forwarding all types of traffic. To bring up the port, select **Device** > **Port Management** to configure the port, or cancel the storm constrain setting on the port.

Configuring Storm Constrain

Setting the Traffic Statistics Generating Interval

Select **Device** > **Storm Constrain** from the navigation tree to enter the page shown in Figure 1-1. In the **Interval for generating traffic statistics** text box, input the traffic statistics generating interval for storm constrain.

Figure 1-1 The Storm Constrain tab



Interval Configuration

Interval for generating traffic statistics: 10 Seconds(1-300, Default = 10)

Port Storm Constrain

Search Item: Interface Name Keywords:

□	Interface Name	Broadcast Storm Control Info	Multicast Storm Control Info	Unicast Storm Control Info	Control Mode	Trap	Log	Operation
□	GigabitEthernet1/0/1	10-1000000 (pps)			Block	On	On	✎
□	GigabitEthernet1/0/2	10-1000000 (pps)			Block	On	On	✎

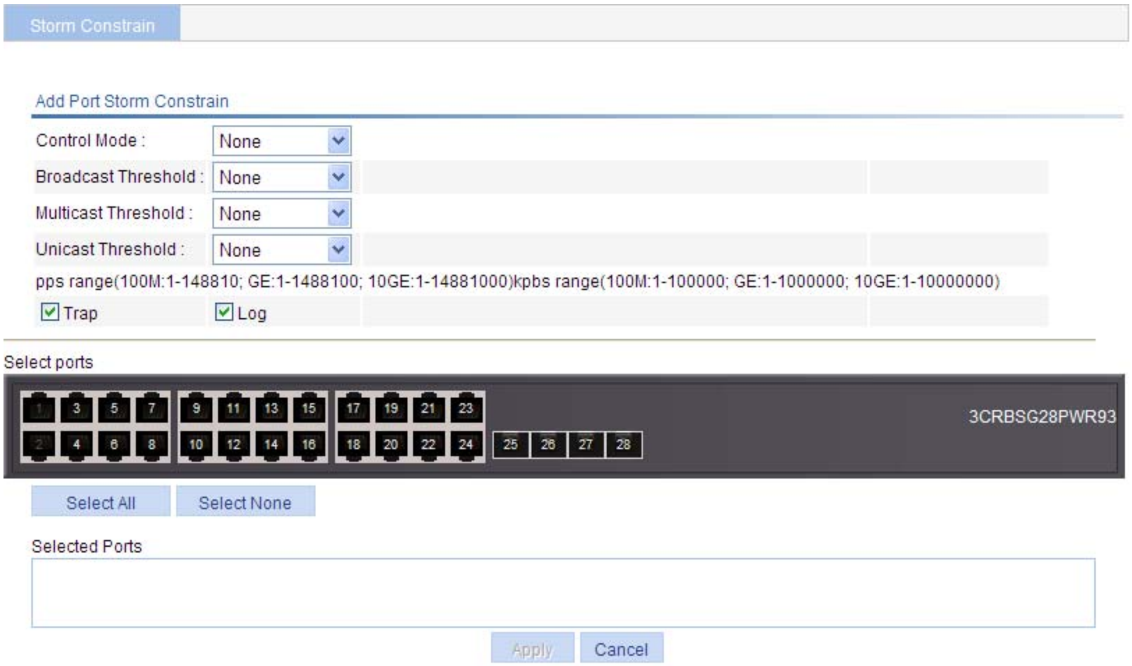
Note

- The traffic statistics generating interval set here is the interval used by the storm constrain function for measuring traffic against the traffic thresholds. It is different from the interval set in the flow interval module, which is used for measuring the average traffic sending and receiving rates over a specific interval.
- For network stability sake, set the traffic statistics generating interval for the storm constrain function to the default or a greater value.

Configuring Storm Constrain

Select **Device** > **Storm Constrain** from the navigation tree to enter the page shown in Figure 1-1. In the **Port Storm Constrain** area, the configured port storm constrain settings are displayed. Click **Add** to enter the page for adding port storm constrain configuration, as shown in Figure 1-2.

Figure 1-2 Add storm constrain settings for ports



Storm Constrain

Add Port Storm Constrain

Control Mode : None

Broadcast Threshold : None

Multicast Threshold : None

Unicast Threshold : None

pps range(100M:1-148810; GE:1-1488100; 10GE:1-14881000)kpbs range(100M:1-100000; GE:1-1000000; 10GE:1-10000000)

☑ Trap ☑ Log

Select ports

Selected Ports

[Table 1-1](#) describes the port storm constrain configuration items.

Table 1-1 Port storm constrain configuration items

Item	Remarks
Control Mode	Specify the action to be performed when a type of traffic exceeds the corresponding upper threshold. Available options include: • None: Perform no action. • Block: Block the traffic of this type on a port when the type of traffic exceeds the upper threshold. • Shutdown: Shut down the port when a type of traffic exceeds the traffic threshold. The port stops forwarding traffic as a result. **Highlight** *The storm constrain function, after being enabled, requires a full traffic statistics generating interval (in seconds) to collect traffic data, and analyzes the data in the next interval. Thus, it is normal that a period longer than one traffic statistics generating interval is waited for a control action to happen if you enable the function while the packet storm is present. Nevertheless, the action will be taken within two intervals.*
Broadcast Threshold	Set the broadcast, multicast, and unicast thresholds. • None: Perform no storm constrain for the selected port or ports. • pps: Specify the storm constrain upper threshold and lower threshold in packets per second (pps). **Highlight** • *On a port, you can set the thresholds for broadcast, multicast, and unicast traffic at the same time. To set storm constrain on a port successfully, you must specify the thresholds for at least a type of traffic.* • *When the* ***pps*** *option is selected, the upper threshold and lower threshold ranges depend on the interface type, as shown in the pps range description on the page.*
Multicast Threshold	
Unicast Threshold	

Item	Remarks
Trap	Select or clear the option to enable or disable the system to send trap messages both when an upper threshold is crossed and when the corresponding lower threshold is crossed after that.
Log	Select or clear the option to enable or disable the system to output logs both when an upper threshold is crossed and when the corresponding lower threshold is crossed after that.
Select ports	Select ports from the chassis front panel to apply the storm constrain settings to them.

Table of Contents

1 RMON

RMON Overview

Remote Monitoring (RMON) is used to realize the monitoring and management from the management devices to the managed devices on the network by implementing such functions as statistics and alarm. The statistics function enables a managed device to periodically or continuously track various traffic information on the network segments connecting to its ports, such as total number of received packets or total number of oversize packets received. The alarm function enables a managed device to monitor the value of a specified MIB variable, log the event and send a trap to the management device when the value reaches the threshold, such as the port rate reaches a certain value or the potion of broadcast packets received in the total packets reaches a certain value.

Both the RMON protocol and the Simple Network Management Protocol (SNMP) are used for remote network management:

- RMON is implemented on the basis of the SNMP, which is thus enhanced. RMON sends traps to the management device to notify the abnormality of the alarm variables by using the SNMP trap packet sending mechanism. Although trap is also defined in SNMP, it is usually used to notify the management device whether some functions on managed devices operate normally and the change of physical status of interfaces. Traps in RMON and those in SNMP have different monitored targets, triggering conditions, and report contents.
- RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. The RMON protocol defines that when an alarm threshold is reached on a managed device, the managed device sends a trap to the management device automatically, so the management device has no need to get the values of MIB variables for multiple times and compare them, and thus greatly reducing the communication traffic between the management device and the managed device. In this way, you can manage a large scale of network easily and effectively.

Working Mechanism

RMON allows multiple monitors (management devices). A monitor provides two ways of data gathering:

- Using RMON probes. Management devices can obtain management information from RMON probes directly and control network resources. In this approach, management devices can obtain all RMON MIB information.
- Embedding RMON agents in network devices such as routers, switches, and hubs to provide the RMON probe function. Management devices exchange data with RMON agents using basic SNMP operations to gather network management information, which, due to system resources limitation, may not cover all MIB information but four groups of information, statistics, history, alarm, and event, in most cases.

The 3Com device adopts the second way and realizes the RMON agent function. With the RMON agent function, the management device can monitor all the traffic flowing among the managed devices on all connected LAN segments; obtain information about error statistics and performance statistics for network management.

RMON Groups

Among the RMON groups defined by RMON specifications (RFC 2819), the realized public MIB of the device supports the statistics group, history group, alarm group, and event group.

Statistics group

The statistics group defines that the system collects statistics on various traffic information on an interface (at present, only Ethernet interfaces are supported) and saves the statistics in the Ethernet statistics table (ethernetStatsTable) for query convenience of the management device. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, and so on.

After the creation of a statistics entry on an interface, the statistics group starts to collect traffic statistics on the interface. The result of the statistics is a cumulative sum.

History group

The history group defines that the system periodically collects statistics on traffic information at an interface and saves the statistics in the history record table (ethernetHistoryTable) for query convenience of the management device. The statistics data includes bandwidth utilization, number of error packets, and total number of packets.

A history group collects statistics on packets received on the interface during each period, which can be configured through the command line interface (CLI).

Alarm group

The RMON alarm group monitors specified alarm variables, such as total number of received packets (etherStatsPkts) on an interface. After you define an alarm entry the system gets the value of the monitored alarm variable at the specified interval, when the value of the monitored variable is greater than or equal to the upper threshold, an upper event is triggered; when the value of the monitored variable is smaller than or equal to the lower threshold, a lower event is triggered. The event is then handled as defined in the event group.

Note

If the value of a sampled alarm variable overpasses the same threshold multiple times, only the first one can cause an alarm event. That is, the rising alarm and falling alarm are alternate.

Event group

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group and the private alarm group. The events can be handled in one of the following ways:

- Log: Logging event related information (the time of the event occurred, contents of the event, and so on) in the event log table of the RMON MIB of the device, and thus the management device can check the logs through the SNMP GET operation.
- Trap: Sending a trap to notify the occurrence of this event to the network management station (NMS).

- Log-Trap: Logging event information in the event log table and sending a trap to the NMS.
- None: No action.

Configuring RMON

Configuration Task List

Configuring the RMON statistics function

RMON statistics function can be implemented by either the statistics group or the history group, but the objects of the statistics are different. You can choose to configure a statistics group or a history group accordingly.

- A statistics object of the statistics group is a variable defined in the Ethernet statistics table, and the recorded content is a cumulative sum of the variable from the time the statistics entry is created to the current time. Perform the tasks in Table 1-1 to configure RMON Ethernet statistics function.
- A statistics object of the history group is the variable defined in the history record table, and the recorded content is a cumulative sum of the variable in each period. Perform the tasks in Table 1-2 to configure RMON history statistics function.

Table 1-1 RMON statistics group configuration task list

Task	Remarks
Configuring a Statistics Entry	Required You can create up to 100 statistics entries in a statistics table. After a statistics entry is created on an interface, the system collects statistics on various traffic information on the interface. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, and so on. The statistics are cleared after the device reboots. **Highlight** *Only one statistics entry can be created on one interface.*

Table 1-2 RMON history group configuration task list

Task	Remarks
Configuring a History Entry	Required You can create up to 100 history entries in a history table. After an entry is created, the system periodically samples the number of packets received/sent on the current interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table. **Highlight** *When you create an entry, if the value of the specified sampling interval is identical to that of the existing history entry, the system considers their configurations are the same and the creation fails.*

Configuring the RMON alarm function

- If you need to configure that the managed device sends a trap to the NMS when it triggers an alarm event, you should configure the SNMP agent as described in *SNMP Configuration* before configuring the RMON alarm function.
- As the alarm variables that can be configured through Web network management are MIB variables that defined in the history group or the statistics group, you must make sure that the RMON Ethernet statistics function or the RMON history statistics function is configured on the monitored Ethernet interface.

Perform the tasks in Table 1-3 to configure RMON alarm function.

Table 1-3 RMON alarm configuration task list

Task	Remarks
Configuring an Event Entry	Optional You can create up to 60 event entries for an event table. An event entry defines event indexes and the actions the system will take, including log the event, send a trap to the NMS, take no action, and log the event and send a trap to the NMS. **Highlight** *An entry cannot be created if the values of the specified alarm variable, sampling interval, sampling type, rising threshold and falling threshold are identical to those of an existing entry in the system.*
Configuring an Alarm Entry	Required You can create up to 60 alarm entries for an alarm table. With an alarm entry created, the specified alarm event will be triggered when an abnormity occurs, and the alarm event defines how to deal with the abnormity. **Highlight** *An entry cannot be created if the values of the specified event description, owners, and actions are identical to those of an existing entry in the system.*

Displaying RMON running status

After you configure the RMON statistics function or the alarm function, you can view RMON running status and verify the configuration by performing tasks in Table 1-4.

Table 1-4 Display RMON running status

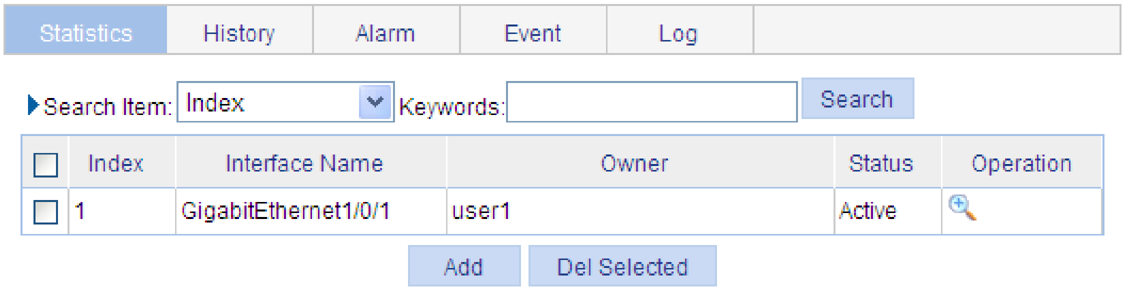
Task	Remarks
Displaying RMON Statistics Information	View the interface statistics during the period from the time the statistics entry is created to the time the page is displayed. The statistics are cleared after the device reboots.
Displaying RMON History Sampling Information	After you have created a history control entry on an interface, the system calculates the information of the interface periodically and saves the information to the etherHistoryEntry table. You can perform this task to view the entries in this table. And the number of history sampling records that can be displayed and the history sampling interval are specified when you configure the history group.

Task	Remarks
Displaying RMON Event Logs	If you have configured the system to log an event after the event is triggered when you configure the event group, the event is recorded into the RMON log. You can perform this task to display the details of the log table

Configuring a Statistics Entry

Select **Device** > **RMON** from the navigation tree to enter the page of the **Statistics** tab, as shown in Figure 1-1. Click **Add** to enter the page for adding a statistics entry, as shown in Figure 1-2.

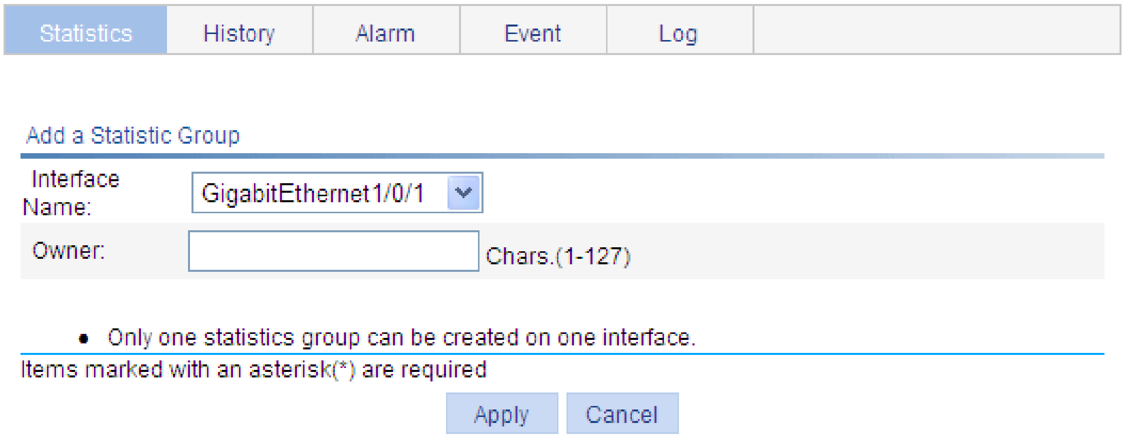
Figure 1-1 Statistics entry



Search Item: Index Keywords:

□	Index	Interface Name	Owner	Status	Operation
□	1	GigabitEthernet1/0/1	user1	Active	🔍

Figure 1-2 Add a statistics entry



Add a Statistic Group

Interface Name:	GigabitEthernet1/0/1
Owner:	Chars.(1-127)

- Only one statistics group can be created on one interface.

Items marked with an asterisk(*) are required

Table 1-5 describes the items for configuring a statistics entry.

Table 1-5 Statistics entry configuration items

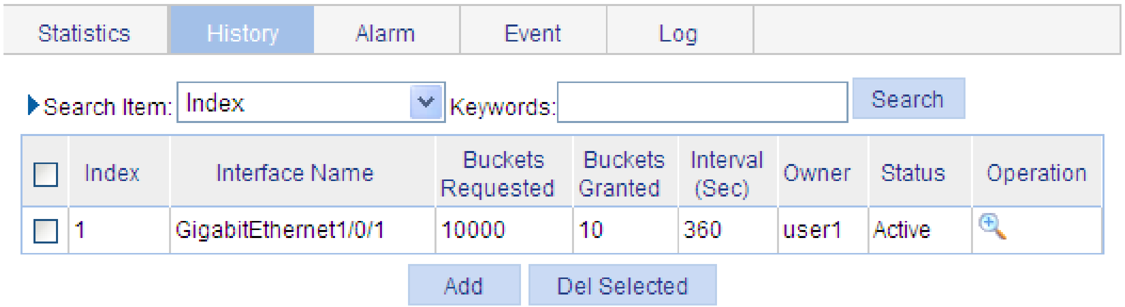
Item	Description
Interface Name	Select the name of the interface on which the statistics entry is created. Only one statistics entry can be created on one interface.
Owner	Set the owner of the statistics entry.

Return to RMON statistics group configuration task list.

Configuring a History Entry

Select **Device** > **RMON** from the navigation tree and click the **History** tab to enter the page, as shown in Figure 1-3. Click **Add** to enter the page for adding a history entry, as shown in Figure 1-4.

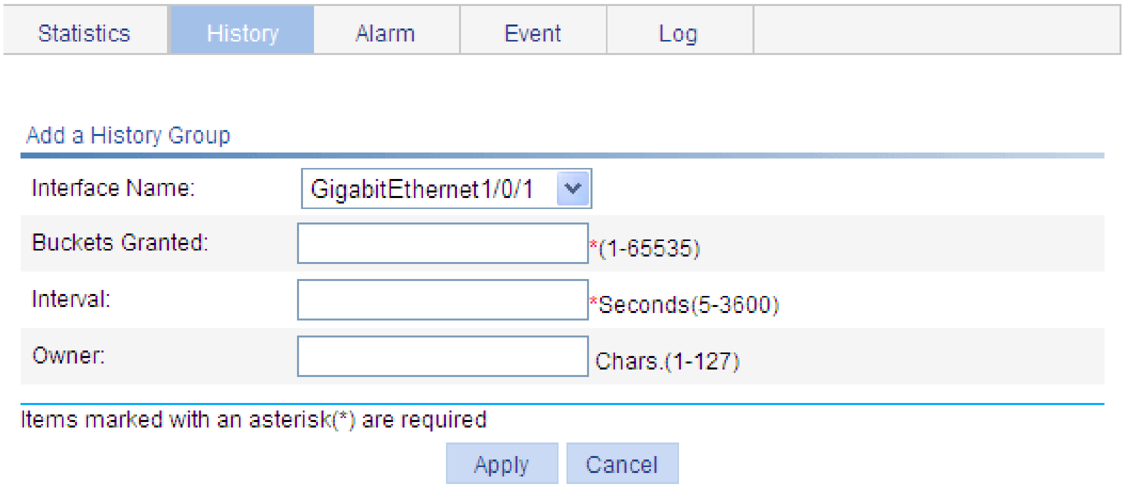
Figure 1-3 History entry



Search Item: Index Keywords:

□	Index	Interface Name	Buckets Requested	Buckets Granted	Interval (Sec)	Owner	Status	Operation
□	1	GigabitEthernet1/0/1	10000	10	360	user1	Active	🔍

Figure 1-4 Add a history entry



Add a History Group

Interface Name: GigabitEthernet1/0/1

Buckets Granted: *(1-65535)

Interval: *Seconds(5-3600)

Owner: Chars.(1-127)

Items marked with an asterisk(*) are required

Table 1-6 describes the items for configuring a history entry.

Table 1-6 History entry configuration items

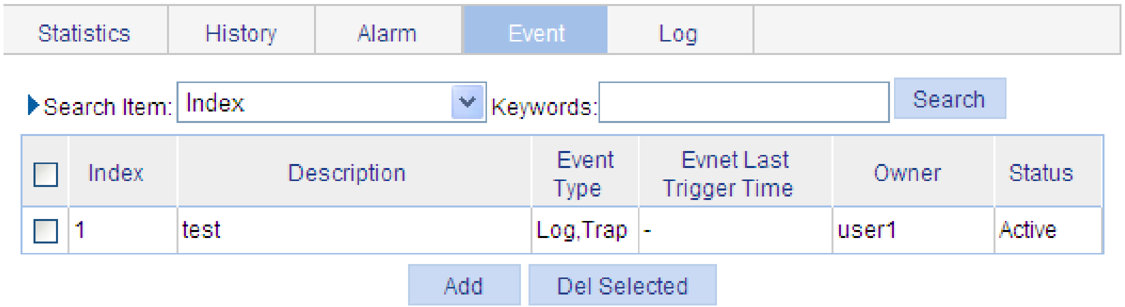
Item	Description
Interface Name	Select the name of the interface on which the history entry is created.
Buckets Granted	Set the capacity of the history record list corresponding to this history entry, namely, the maximum number of records that can be saved in the history record list. If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one. The statistics include total number of received packets on the current interface, total number of broadcast packets, total number of multicast packets in a sampling period, and so on.
Interval	Set the sampling period.
Owner	Set the owner of the entry.

Return to RMON history group configuration task list.

Configuring an Event Entry

Select **Device** > **RMON** from the navigation tree and click the **Event** tab to enter the page, as shown in Figure 1-5. Click **Add** to enter the page for adding an event entry, as shown in Figure 1-6.

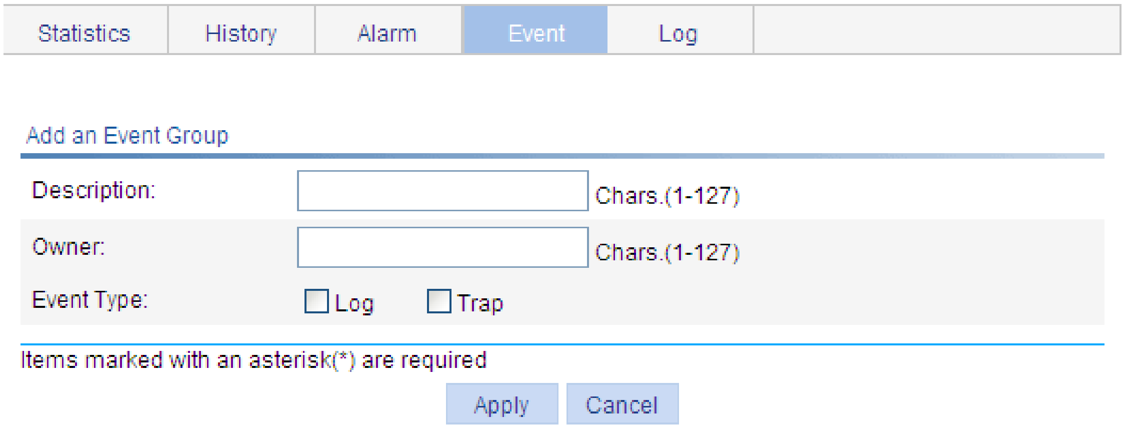
Figure 1-5 Event entry



Search Item: Index Keywords:

□	Index	Description	Event Type	Evnet Last Trigger Time	Owner	Status
□	1	test	Log,Trap	-	user1	Active

Figure 1-6 Add an event entry



Add an Event Group

Description: Chars.(1-127)

Owner: Chars.(1-127)

Event Type: □ Log □ Trap

Items marked with an asterisk(*) are required

Table 1-7 describes the items for configuring an event entry.

Table 1-7 Event entry configuration items

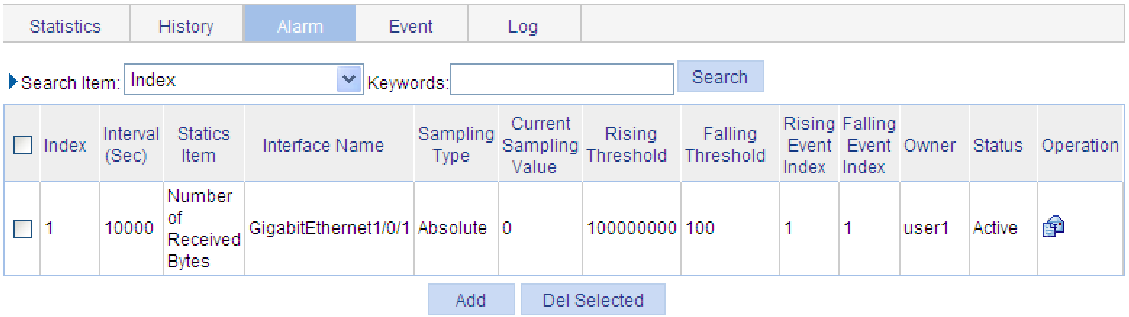
Item	Description
Description	Set the description for the event.
Owner	Set the owner of the entry.
Event Type	Set the actions that the system will take when the event is triggered: • Log: The system will log the event • Trap: The system will send a trap in the community name of **null**. If both **Log** and **Trap** are selected, the system will log the event and send a trap; If none of them is selected, the system will take no action

Return to RMON alarm configuration task list.

Configuring an Alarm Entry

Select **Device** > **RMON** from the navigation tree and click the **Alarm** tab to enter the page, as shown in Figure 1-7. Click **Add** to enter the page for adding an alarm entry, as shown in Figure 1-8.

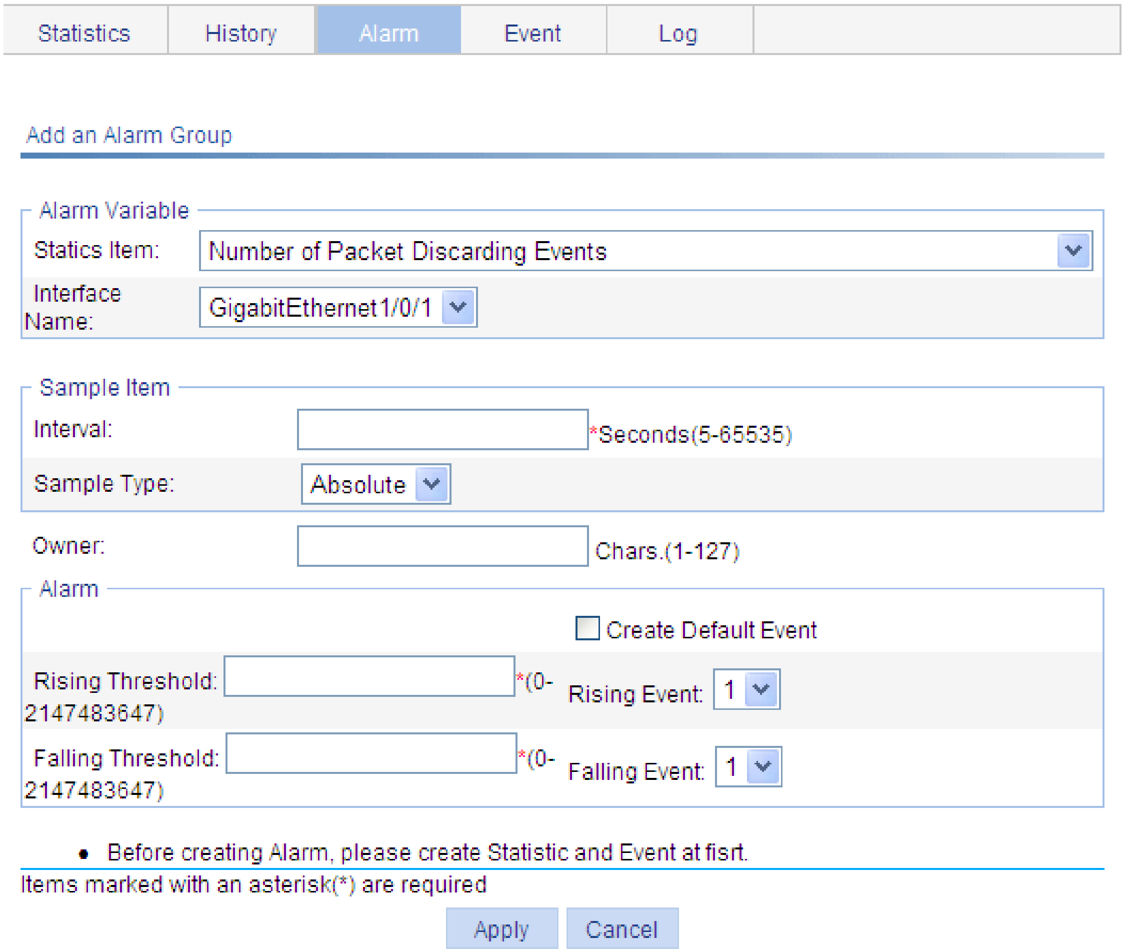
Figure 1-7 Alarm entry



Search Item: Index Keywords:

□	Index	Interval (Sec)	Statics Item	Interface Name	Sampling Type	Current Sampling Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Status	Operation
□	1	10000	Number of Received Bytes	GigabitEthernet1/0/1	Absolute	0	100000000	100	1	1	user1	Active	📋

Figure 1-8 Add an alarm entry



Add an Alarm Group

Alarm Variable

Statics Item: Number of Packet Discarding Events

Interface Name: GigabitEthernet1/0/1

Sample Item

Interval: *Seconds(5-65535)

Sample Type: Absolute

Owner: Chars.(1-127)

Alarm

□ Create Default Event

Rising Threshold: *(0-2147483647) Rising Event: 1

Falling Threshold: *(0-2147483647) Falling Event: 1

- Before creating Alarm, please create Statistic and Event at fisrt.

Items marked with an asterisk(*) are required

Figure 1-8 describes the items for configuring an alarm entry.

Table 1-8 Alarm entry configuration items

Item		Description
Alarm variable	Statics Item	Set the traffic statistics that will be collected and monitored, see Table 1-9 for details.
	Interface Name	Set the name of the interface whose traffic statistics will be collected and monitored.

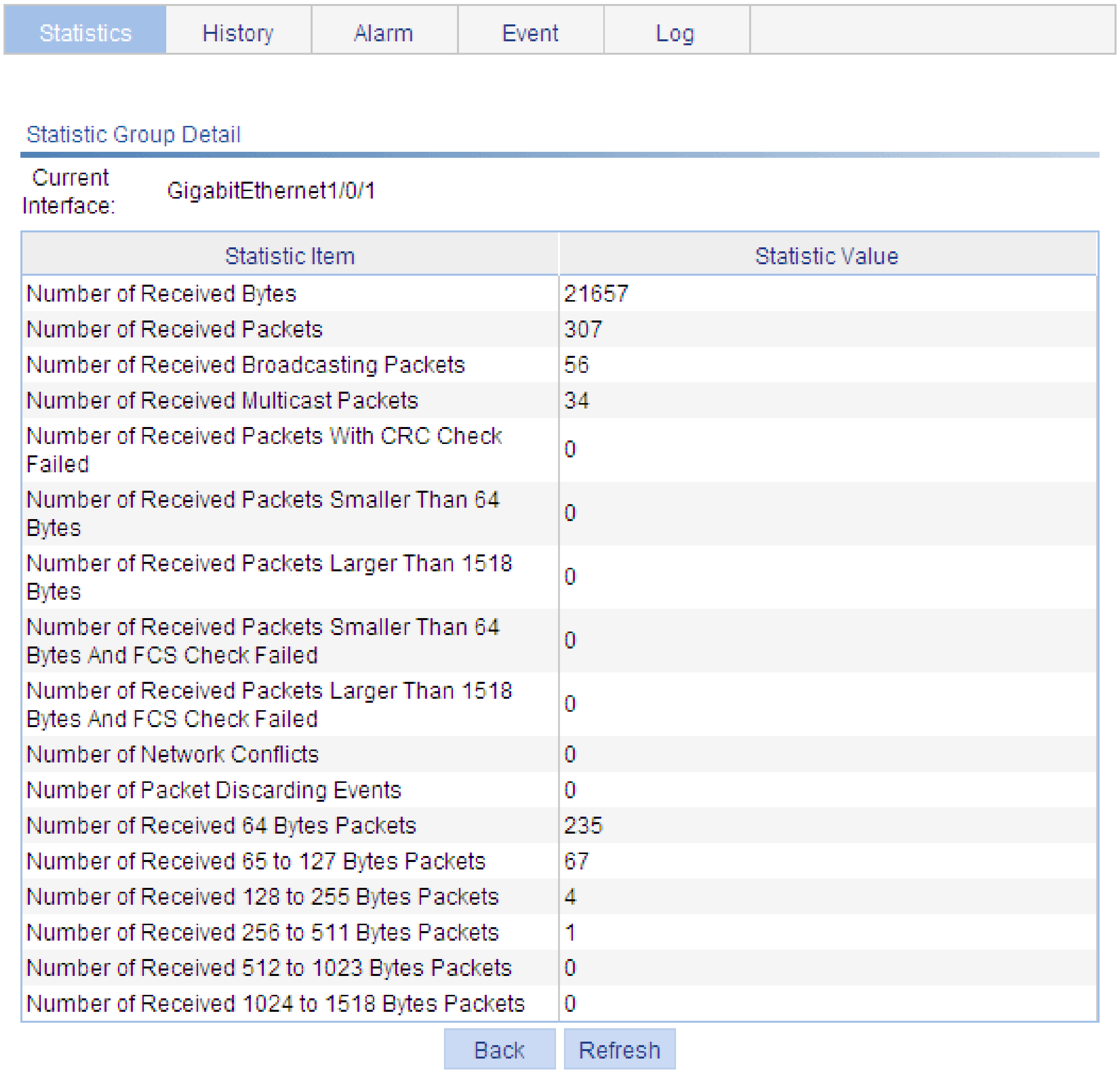
Item		Description
Sample Item	Interval	Set the sampling interval.
	Sample Type	Set the sampling type, including: • Absolute: Absolute sampling, namely, to obtain the value of the variable when the sampling time is reached. • Delta: Delta sampling, namely, to obtain the variation value of the variable during the sampling interval when the sampling time is reached.
Owner		Set the owner of the alarm entry.
Alarm	Create Default Event	Select whether to create a default event. The description of the default event is **default event**, the action is **log-and-trap**, and the owner is **default owner**. If there is no event, you can select to create the default event. And when the value of the alarm variable is higher than the alarm rising threshold or lower than the alarm falling threshold, the system will adopt the default action, that is, **log-and-trap**.
	Rising Threshold	Set the alarm rising threshold.
	Rising Event	Set the action that the system will take when the value of the alarm variable is higher than the alarm rising threshold. If the **Create Default Event** check box is selected, this option is not configurable.
	Falling Threshold	Set the alarm falling threshold.
	Falling Event	Set the action that the system will take when the value of the alarm variable is lower than the alarm falling threshold. If the **Create Default Event** check box is selected, this option is not configurable.

Return to RMON alarm configuration task list.

Displaying RMON Statistics Information

Select **Device** > **RMON** from the navigation tree to enter the page of the **Statistics** tab, as shown in Figure 1-1. Click the 🔍 icon of a statistics entry to enter the page as shown in Figure 1-9, which displays all statistics items on the current interface.

Figure 1-9 RMON statistics information



Statistic Group Detail

Current Interface: GigabitEthernet1/0/1

Statistic Item	Statistic Value
Number of Received Bytes	21657
Number of Received Packets	307
Number of Received Broadcasting Packets	56
Number of Received Multicast Packets	34
Number of Received Packets With CRC Check Failed	0
Number of Received Packets Smaller Than 64 Bytes	0
Number of Received Packets Larger Than 1518 Bytes	0
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	0
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	0
Number of Network Conflicts	0
Number of Packet Discarding Events	0
Number of Received 64 Bytes Packets	235
Number of Received 65 to 127 Bytes Packets	67
Number of Received 128 to 255 Bytes Packets	4
Number of Received 256 to 511 Bytes Packets	1
Number of Received 512 to 1023 Bytes Packets	0
Number of Received 1024 to 1518 Bytes Packets	0

Table 1-9 describes the fields of RMON statistics.

Table 1-9 Fields of RMON statistics

Item	Description
Number of Received Bytes	Total number of octets received by the interface, corresponding to the MIB node etherStatsOctets.
Number of Received Packets	Total number of packets received by the interface, corresponding to the MIB node etherStatsPkts.
Number of Received Broadcasting Packets	Total number of broadcast packets received by the interface, corresponding to the MIB node etherStatsBroadcastPkts.
Number of Received Multicast Packets	Total number of multicast packets received by the interface, corresponding to the MIB node etherStatsMulticastPkts.
Number of Received Packets With CRC Check Failed	Total number of packets with CRC errors received on the interface, corresponding to the MIB node etherStatsCRCAlignErrors.

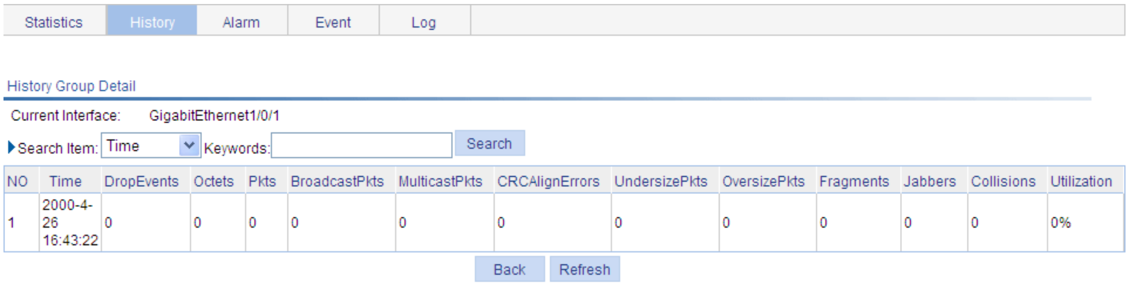
Item	Description
Number of Received Packets Smaller Than 64 Bytes	Total number of undersize packets (shorter than 64 octets) received by the interface, corresponding to the MIB node etherStatsUndersizePkts.
Number of Received Packets Larger Than 1518 Bytes	Total number of oversize packets (longer than 1518 octets) received by the interface, corresponding to the MIB node etherStatsOversizePkts.
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	Total number of undersize packets (shorter than 64 octets) with CRC errors received by the interface, corresponding to the MIB node etherStatsFragments.
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	Number of oversize packets (longer than 1518 octets) with CRC errors received by the interface, corresponding to the MIB node etherStatsJabbers.
Number of Network Conflicts	Total number of collisions received on the interface, corresponding to the MIB node etherStatsCollisions.
Number of Packet Discarding Events	Total number of drop events received on the interface, corresponding to the MIB node etherStatsDropEvents.
Number of Received 64 Bytes Packets	Total number of received packets with 64 octets on the interface, corresponding to the MIB node etherStatsPkts64Octets.
Number of Received 65 to 127 Bytes Packets	Total number of received packets with 65 to 127 octets on the interface, corresponding to the MIB node etherStatsPkts65to127Octets.
Number of Received 128 to 255 Bytes Packets	Total number of received packets with 128 to 255 octets on the interface, corresponding to the MIB node etherStatsPkts128to255Octets.
Number of Received 256 to 511 Bytes Packets	Total number of received packets with 256 to 511 octets on the interface, corresponding to the MIB node etherStatsPkts256to511Octets.
Number of Received 512 to 1023 Bytes Packets	Total number of received packets with 512 to 1023 octets on the interface, corresponding to the MIB node etherStatsPkts512to1023Octets.
Number of Received 1024 to 1518 Bytes Packets	Total number of received packets with 1024 to 1518 octets on the interface, corresponding to the MIB node etherStatsPkts1024to1518Octets.

Return to Display RMON running status.

Displaying RMON History Sampling Information

Select **Device** > **RMON** from the navigation tree and click the **History** tab to enter the page, as shown in Figure 1-3. Click the 🔍 icon of a history entry to enter the page as shown in Figure 1-10, which displays all history sampling information on the current interface.

Figure 1-10 RMON history sampling information



History Group Detail

Current Interface: GigabitEthernet1/0/1

Search Item: Time Keywords:

NO	Time	DropEvents	Octets	Pkts	BroadcastPkts	MulticastPkts	CRCAlignErrors	UndersizePkts	OversizePkts	Fragments	Jabbers	Collisions	Utilization
1	2000-4-26 16:43:22	0	0	0	0	0	0	0	0	0	0	0	0%

Table 1-10 describes the fields of RMON history sampling information.

Table 1-10 Fields of RMON history sampling information

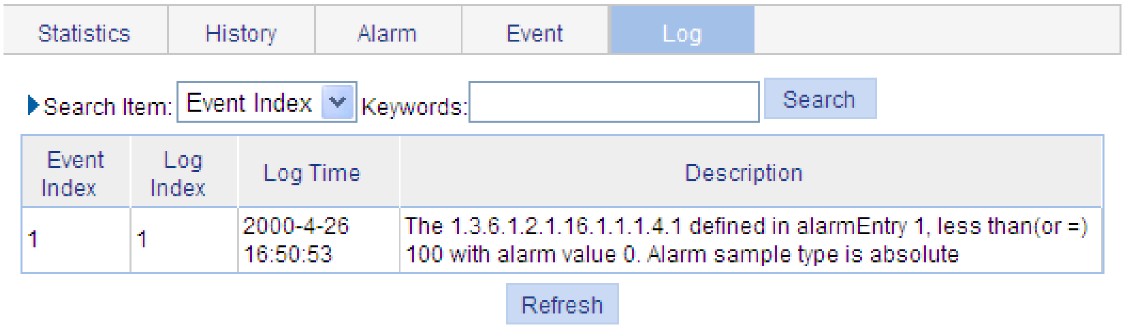
Item	Description
NO	Number of the entry in the system buffer Statistics are numbered chronologically when they are saved to the system buffer.
Time	Time at which the information is saved
DropEvents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.
Octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
Pkts	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
BroadcastPkts	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
MulticastPkts	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.
CRCAlignErrors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
UndersizePkts	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
OversizePkts	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
Fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
Jabbers	Number of jabbers received during the sampling period (Support for the field depends on the device model.), corresponding to the MIB node etherHistoryJabbers.
Collisions	Number of collision packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
Utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

Return to Display RMON running status.

Displaying RMON Event Logs

Select **Device** > **RMON** from the navigation tree and click the **Log** tab to enter the page, as shown in Figure 1-11, which displays log information for all event entries.

Figure 1-11 Log



Search Item: Event Index

Event Index	Log Index	Log Time	Description
1	1	2000-4-26 16:50:53	The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarmEntry 1, less than(or =) 100 with alarm value 0. Alarm sample type is absolute

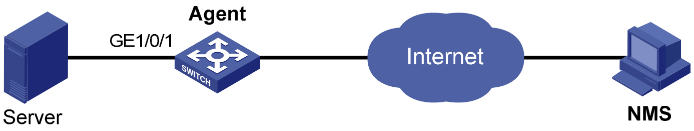
Return to Display RMON running status.

RMON Configuration Example

Network requirements

As shown in Figure 1-12, Agent is connected to a remote NMS across the Internet. Create an entry in the RMON Ethernet statistics table to gather statistics on Ethernet 1/0/1, and perform corresponding configurations so that the system will log the event when the number of bytes received on the interface exceed the specified threshold.

Figure 1-12 Network diagram for RMON

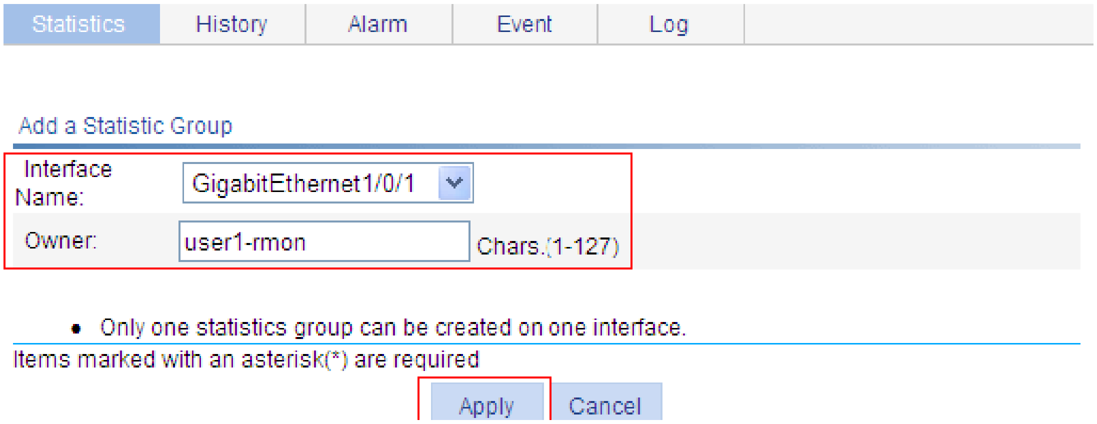


Configuration procedure

# Configure RMON to gather statistics for interface Ethernet 1/0/1.

- Select **Device** > **RMON** from the navigation tree to enter the page of the **Statistics** tab. Click **Add** and perform the following configurations, as shown in Figure 1-13.

Figure 1-13 Add a statistics entry



Add a Statistic Group

Interface Name: GigabitEthernet1/0/1

Owner: user1-rmon Chars.(1-127)

- Only one statistics group can be created on one interface.

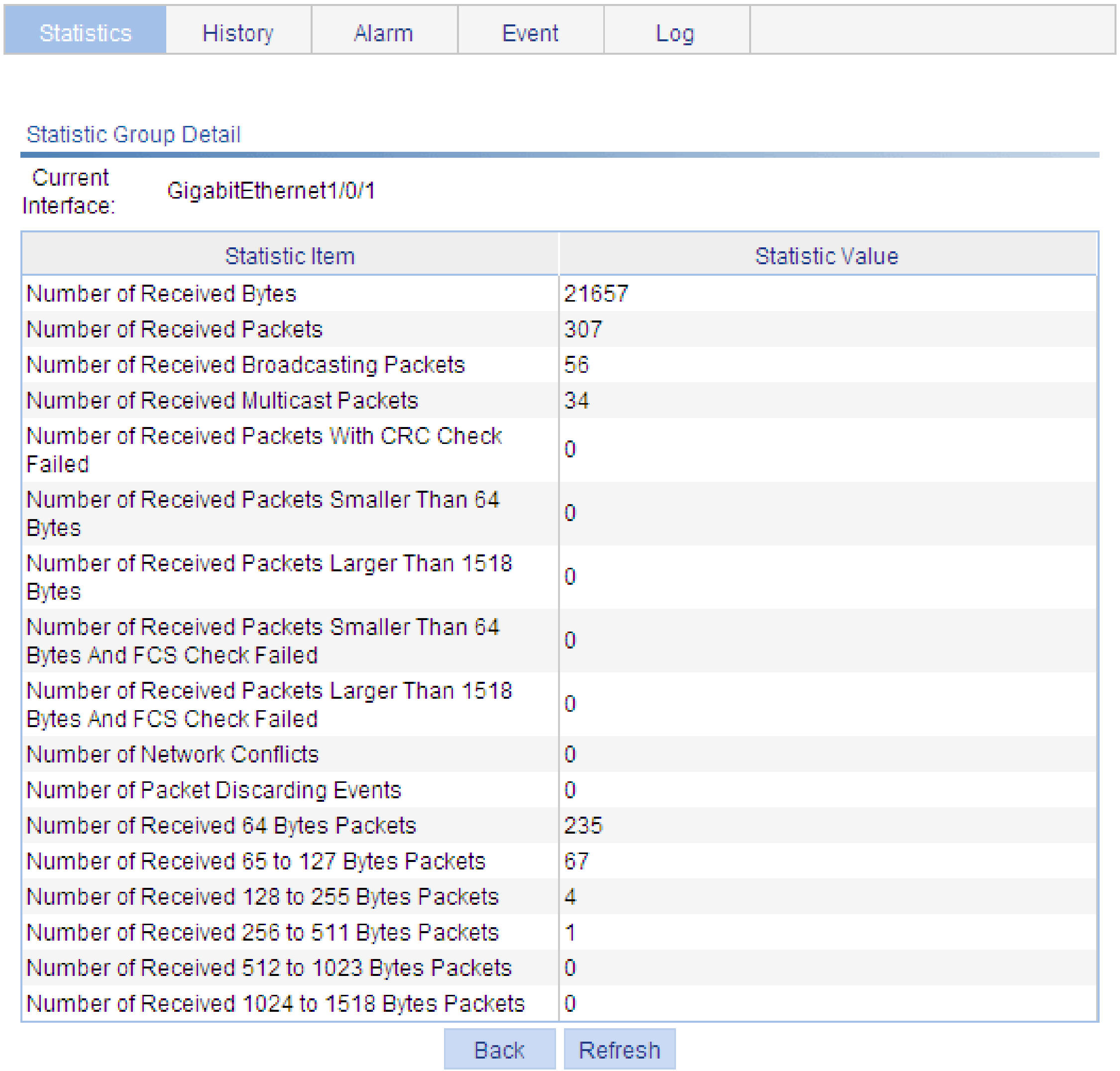
Items marked with an asterisk(*) are required

- Select **GigabitEthernet1/0/1** from the **Interface Name** drop-down box.
- Type **user1-rmon** in the text box of **Owner**.
- Click **Apply**.

# Display RMON statistics for interface Ethernet 1/0/1.

- Click the icon 🔍 corresponding to GigabitEthernet 1/0/1.
- You can view the information as shown in Figure 1-14.

Figure 1-14 Display RMON statistics



Statistic Group Detail

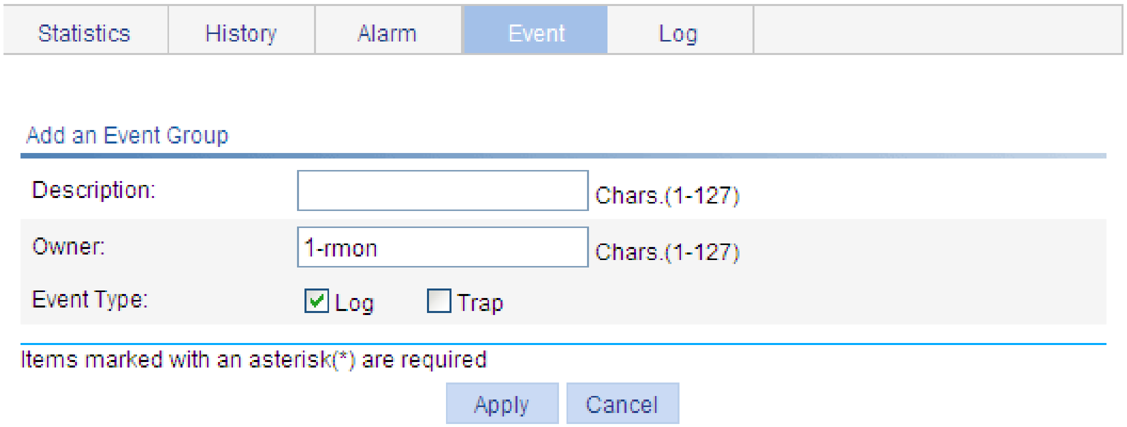
Current Interface: GigabitEthernet1/0/1

Statistic Item	Statistic Value
Number of Received Bytes	21657
Number of Received Packets	307
Number of Received Broadcasting Packets	56
Number of Received Multicast Packets	34
Number of Received Packets With CRC Check Failed	0
Number of Received Packets Smaller Than 64 Bytes	0
Number of Received Packets Larger Than 1518 Bytes	0
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	0
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	0
Number of Network Conflicts	0
Number of Packet Discarding Events	0
Number of Received 64 Bytes Packets	235
Number of Received 65 to 127 Bytes Packets	67
Number of Received 128 to 255 Bytes Packets	4
Number of Received 256 to 511 Bytes Packets	1
Number of Received 512 to 1023 Bytes Packets	0
Number of Received 1024 to 1518 Bytes Packets	0

# Create an event to start logging after the event is triggered.

- Click the **Event** tab, click **Add**, and then perform the following configurations, as shown in Figure 1-15.

Figure 1-15 Configure an event group



Add an Event Group

Description: Chars.(1-127)

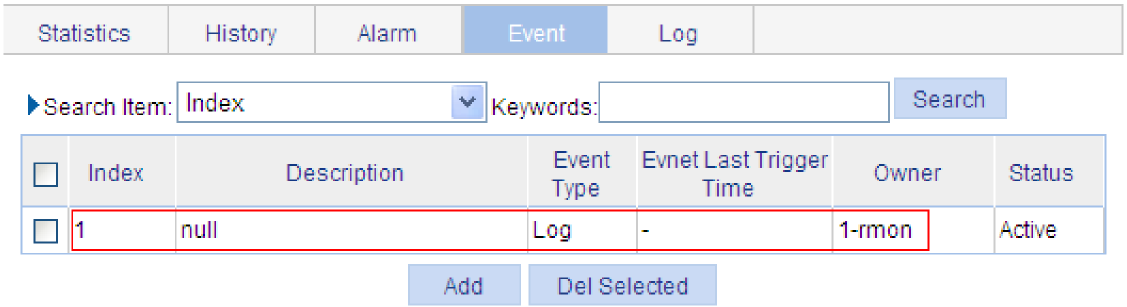
Owner: 1-rmon Chars.(1-127)

Event Type: ☑ Log ☐ Trap

Items marked with an asterisk(*) are required

- Type **1-rmon** in the text box of **Owner**.
- Select the check box before **Log**.
- Click **Apply**.
- The page goes to the page displaying the event entry, and you can see that the entry index of the new event is **1**, as shown in Figure 1-16.

Figure 1-16 Display the index of a event entry



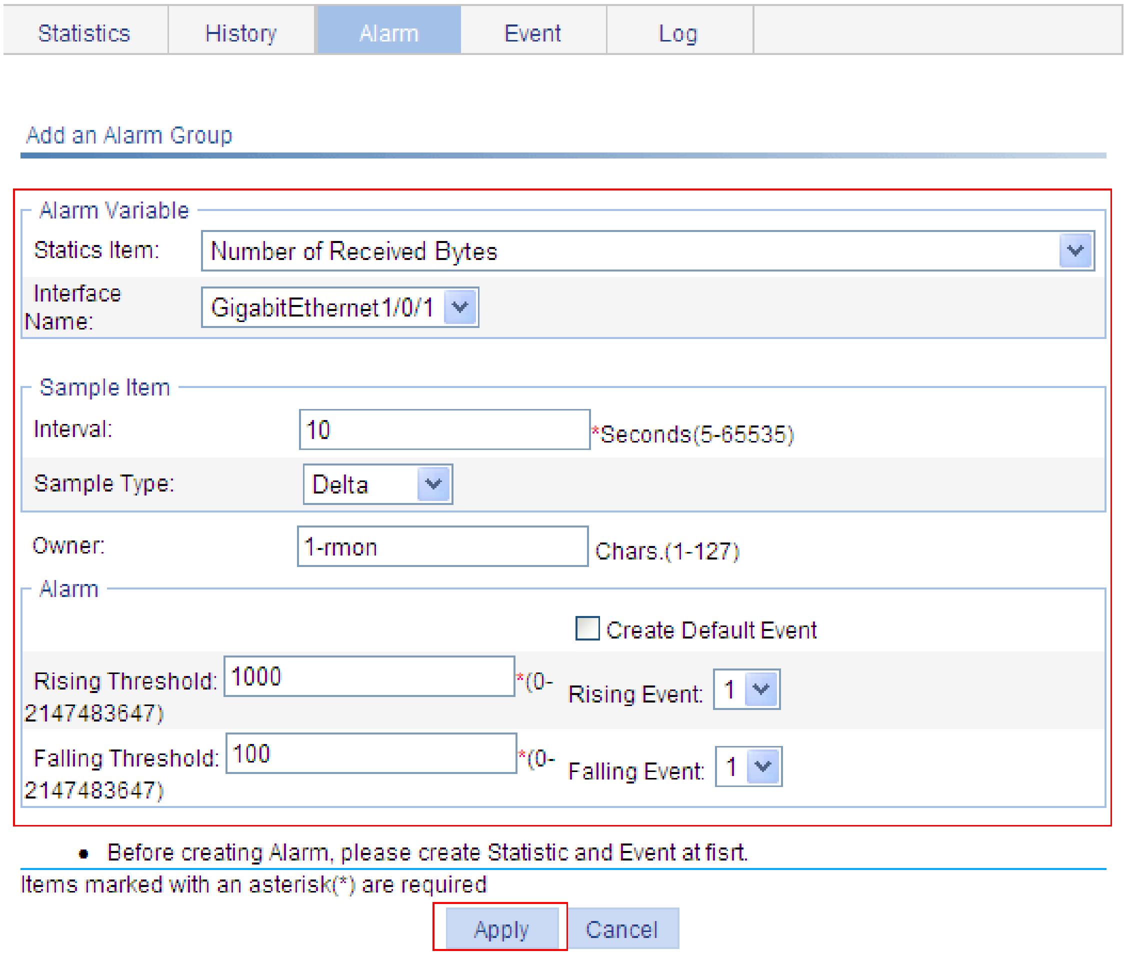
Search Item: Index Keywords:

□	Index	Description	Event Type	Evnet Last Trigger Time	Owner	Status
□	1	null	Log	-	1-rmon	Active

# Configure an alarm group to sample received bytes on Ethernet 1/0/1. When the received bytes exceed the rising or falling threshold, logging is enabled.

- Click the **Alarm** tab, click **Add**, and then perform the following configurations, as shown in Figure 1-17.

Figure 1-17 Configure an alarm group



Add an Alarm Group

Alarm Variable

Statics Item: Number of Received Bytes

Interface Name: GigabitEthernet1/0/1

Sample Item

Interval: 10 *Seconds(5-65535)

Sample Type: Delta

Owner: 1-rmon Chars.(1-127)

Alarm

□ Create Default Event

Rising Threshold: 1000 *(0-2147483647) Rising Event: 1

Falling Threshold: 100 *(0-2147483647) Falling Event: 1

- Before creating Alarm, please create Statistic and Event at first.

Items marked with an asterisk(*) are required

- Select **Number of Received Bytes** from the **Statics Item** drop-down box.
- Select **GigabitEthernet1/0/1** from the **Interface Name** drop-down box.
- Type **10** in the text box of **Interval**.
- Select **Delta** from the **Simple Type** drop-down box.
- Type **1-rmon** in the text box of **Owner**.
- Type **1000** in the text box of **Rising Threshold**.
- Select **1** from the **Rising Event** drop-down box.
- Type **100** in the text box of **Falling Threshold**.
- Select **1** from the **Falling Event** drop-down box.
- Click **Apply**.

Table of Contents

1 Energy Saving Configuration

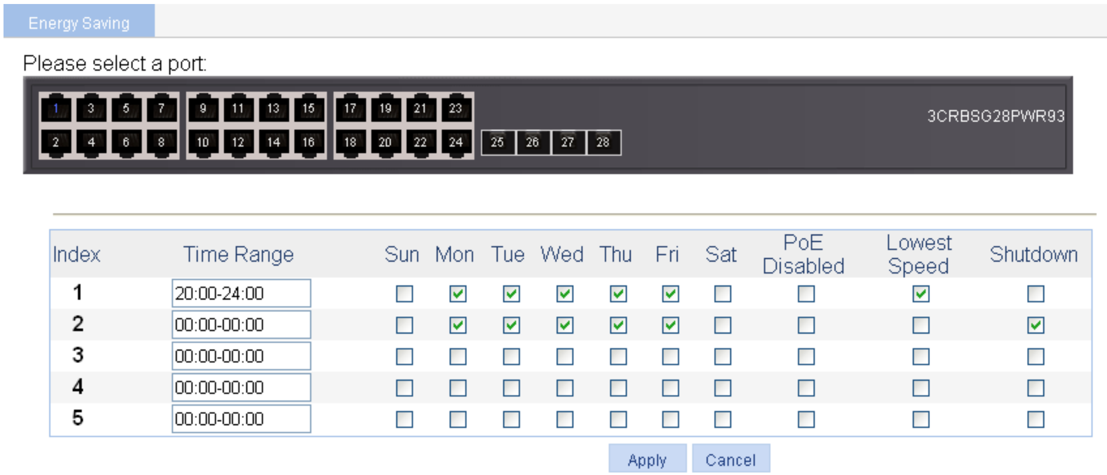
Overview

Energy saving allows you to configure a port to work at the lowest transmission speed, disable PoE, or go down during a specified time range on certain days of a week. The port resumes working normally when the effective time period ends.

Configuring Energy Saving on a Port

Select **Device** > **Energy Saving** from the navigation tree to enter the energy saving configuration page, as shown in Figure 1-1. You can select a port and configure an energy saving policy for the port.

Figure 1-1 Energy saving configuration page



Index	Time Range	Sun	Mon	Tue	Wed	Thu	Fri	Sat	PoE Disabled	Lowest Speed	Shutdown
1	20:00-24:00	□	☑	☑	☑	☑	☑	□	□	☑	□
2	00:00-00:00	□	☑	☑	☑	☑	☑	□	□	□	☑
3	00:00-00:00	□	□	□	□	□	□	□	□	□	□
4	00:00-00:00	□	□	□	□	□	□	□	□	□	□
5	00:00-00:00	□	□	□	□	□	□	□	□	□	□

Table 1-1 describes the configuration items for configuring energy saving on a port.

Table 1-1 Configuration items for configuring energy saving on a port

Item	Description
Time Range	Set the time period when the port is in the state of energy saving. **Highlight** • *Up to five energy saving policies with different time ranges can be configured on a port.* • *Specify the start time and end time in units of 5 minutes, such as 08:05 to 10:15. Otherwise, the start time will be postponed and the end time will be brought forward so that they meet the requirements. For example, if you set the time range to 08:08 to 10:12, however, the effective time range is actually 08:10 to 10:10.*
Sun through Sat	
PoE Disabled	*Disable PoE on the port.*

Item	Description
Lowest Speed	Set the port to transmit data at the lowest speed. 💡 **Highlight** *If you configure the lowest speed limit on a port that does not support 10 Mbps, the configuration cannot take effect.*
Shutdown	Shut down the port. 💡 **Highlight** *An energy saving policy can have all the three energy saving schemes configured, of which the shutdown scheme takes the highest priority.*

Table of Contents

1 SNMP

SNMP Overview

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

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

SNMP Mechanism

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

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

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

SNMP provides the following four basic operations:

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

SNMP Protocol Version

Currently, SNMP agents support SNMPv3 and are compatible with SNMPv1 and SNMPv2c.

- SNMPv1 uses community name for authentication. Community name defines the relationship between an SNMP NMS and an SNMP agent. SNMP packets with community names that do not pass the authentication on the device are simply discarded. A community name plays a similar role as a key word and can be used to control access from NMS to the agent.
- SNMPv2c uses community name for authentication. Compatible with SNMPv1, it extends the functions of SNMPv1. SNMPv2c provides more operation modes such as GetBulk and

InformRequest; it supports more data types such as Counter64; and it provides various error codes, thus being able to distinguish errors in more detail.

- SNMPv3 offers an authentication that is implemented with a User-Based Security Model (USM). You can set the authentication and privacy functions. The former is used to authenticate the validity of the sending end of the authentication packets, preventing access of illegal users; the latter is used to encrypt packets between the NMS and agents, preventing the packets from being intercepted. USM ensures a more secure communication between SNMP NMS and SNMP agent by authentication with privacy.

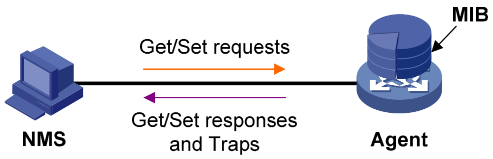
Successful interaction between NMS and agents requires consistency of SNMP versions configured on them. You can configure multiple SNMP versions for an agent to interact with different NMSs.

MIB Overview

MIB

Any managed resource can be identified as an object, which is known as the managed object. Management Information Base (MIB) is a collection of all the managed objects. It defines the hierarchy of the objects and a set of characteristics associated with the managed objects, such as the object identifier (OID), access right and data type. Each agent has its own MIB. NMS can read or write the managed objects in the MIB. TheFigure 1-1Figure 1-1Figure 1-1 relationship between an NMS, agent and MIB is shown in Figure 1-1.

Figure 1-1 Relationship between NMS, agent and MIB

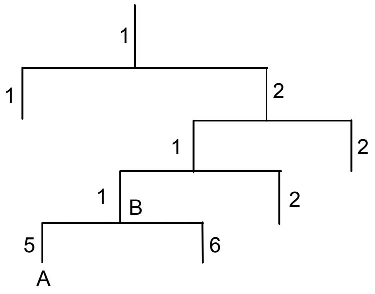


Subtree OID

MIB stores data using a tree structure. A node of the tree is a managed object and can be uniquely identified by a path starting from the root node. As illustrated in Figure 1-2, the managed object A can be uniquely identified by a string of numbers {1.2.1.1.5}. This string of numbers is the OID of the managed object A.

A subtree can be identified by the OID of the root node of the subtree. For example, the OID of the subtree with the root node being B is the OID of node B — {1.2.1.1}.

Figure 1-2 MIB tree



Subtree mask

A subtree OID used with a subtree mask defines a view subtree. A subtree mask is in hexadecimal format. After it is converted to binary bits, each bit corresponds to a node of the OID.

- 1 means precise matching, that is, the OID of the MIB object to be accessed must be identical with the subtree OID.
- 0 means wildcard matching, that is, the OID of the MIB object to be accessed can be different from the subtree OID.

For example, provided the subtree mask 0xDB (11011011 in binary) and the subtree OID 1.3.6.1.6.1.2.1, their relationship is as shown in Figure 1-3. The view determined by them includes all the nodes under the subtree whose OID is 1.3.*.1.6.*.2.1, where * represents any number.

Figure 1-3 Subtree OID and subtree mask

Subtree OID	1	3	6	1	6	1	2	1
Subtree mask	1	1	0	1	1	0	1	1

Note

- If the number of bits in the subtree mask is greater than the number of nodes of the OID, the excessive bits of the subtree mask will be ignored during subtree mask-OID matching.
- If the number of bits in the subtree mask is smaller than the number of nodes of the OID, the short bits of the subtree mask will be set to 1 during subtree mask-OID matching.
- If no subtree mask is specified, the default subtree mask (all Fs) will be used for mask-OID matching.

SNMP Configuration

Configuration Task List

As configurations for SNMPv3 differ substantially from those for SNMPv1 and SNMPv2c, their configuration tasks are introduced separately as follows.

Configuring SNMPv1 or SNMPv2c

Perform the tasks in Table 1-1 to configure SNMPv1 or SNMPv2c:

Table 1-1 SNMPv1 or SNMPv2c configuration task list

Task	Remarks
Enabling SNMP	Required The SNMP agent function is disabled by default.
Configuring an SNMP View	Optional After creating SNMP views, you can specify an SNMP view for an SNMP community to limit the MIB objects that can be accessed by the SNMP community.

Task	Remarks
Configuring an SNMP Community	Required
Configuring SNMP Trap Function	Optional Allows you to configure that the agent can send SNMP traps to the NMS, and configure information about the target host of the SNMP traps. By default, an agent is allowed to send SNMP traps to the NMS.

Configuring SNMPv3

Perform the tasks in Table 1-2 to configure SNMPv3:

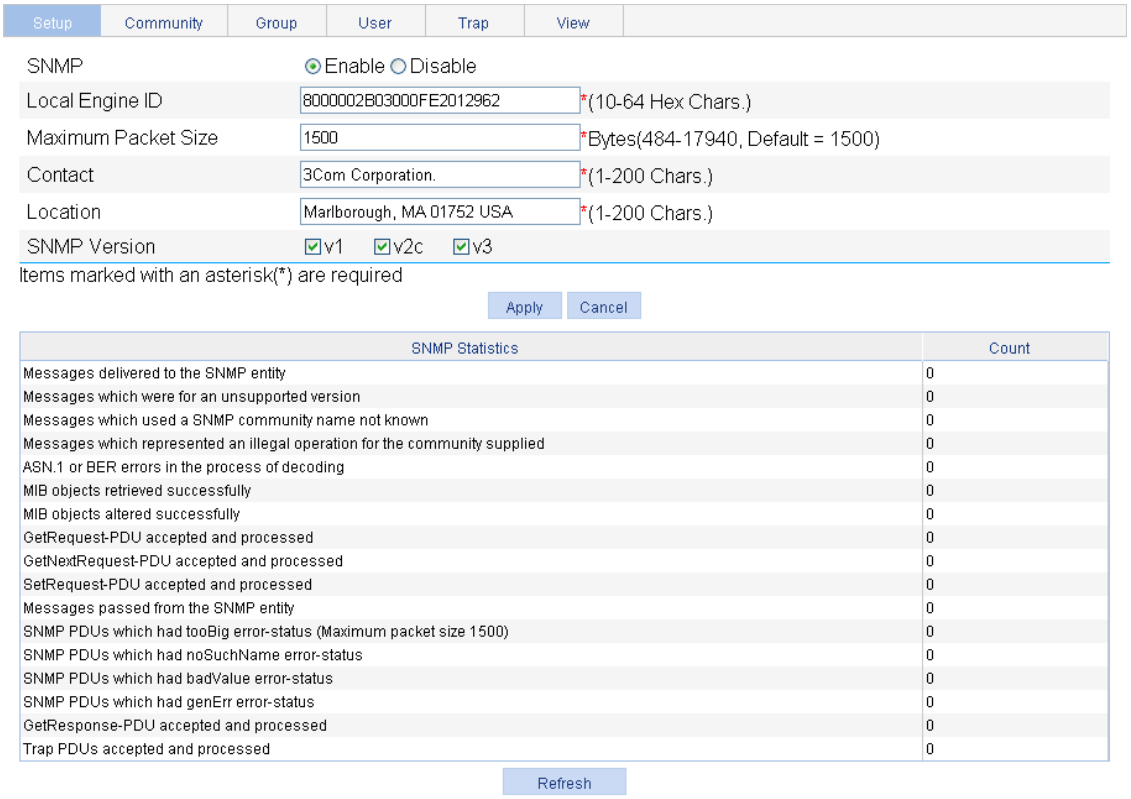
Table 1-2 SNMPv3 configuration task list

Task	Remarks
Enabling SNMP	Required The SNMP agent function is disabled by default.
Configuring an SNMP View	Optional After creating SNMP views, you can specify an SNMP view for an SNMP group to limit the MIB objects that can be accessed by the SNMP group.
Configuring an SNMP Group	Required After creating an SNMP group, you can add SNMP users to the group when creating the users. Therefore, you can realize centralized management of users in the group through the management of the group.
Configuring an SNMP User	Required Before creating an SNMP user, you need to create the SNMP group to which the user belongs.
Configuring SNMP Trap Function	Optional Allows you to configure that the agent can send SNMP traps to the NMS, and configure information about the target host of the SNMP traps By default, an agent is allowed to send SNMP traps to the NMS.

Enabling SNMP

Select **Device** > **SNMP** from the navigation tree to enter the SNMP configuration page, as shown in Figure 1-4. On the upper part of the page, you can select to enable or disable SNMP and configure parameters such as SNMP version; on the lower part of the page, you can view the SNMP statistics, which helps you understand the running status of the SNMP after your configuration.

Figure 1-4 Set up



SNMP ● Enable ○ Disable

Local Engine ID 8000002B03000FE2012962 *(10-64 Hex Chars.)

Maximum Packet Size 1500 *Bytes(484-17940, Default = 1500)

Contact 3Com Corporation. *(1-200 Chars.)

Location Marlborough, MA 01752 USA *(1-200 Chars.)

SNMP Version ☑ v1 ☑ v2c ☑ v3

Items marked with an asterisk(*) are required

SNMP Statistics	Count
Messages delivered to the SNMP entity	0
Messages which were for an unsupported version	0
Messages which used a SNMP community name not known	0
Messages which represented an illegal operation for the community supplied	0
ASN.1 or BER errors in the process of decoding	0
MIB objects retrieved successfully	0
MIB objects altered successfully	0
GetRequest-PDU accepted and processed	0
GetNextRequest-PDU accepted and processed	0
SetRequest-PDU accepted and processed	0
Messages passed from the SNMP entity	0
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	0
SNMP PDUs which had noSuchName error-status	0
SNMP PDUs which had badValue error-status	0
SNMP PDUs which had genErr error-status	0
GetResponse-PDU accepted and processed	0
Trap PDUs accepted and processed	0

Table 1-3 describes the configuration items for enabling SNMP.

Table 1-3 Configuration items for enabling SNMP

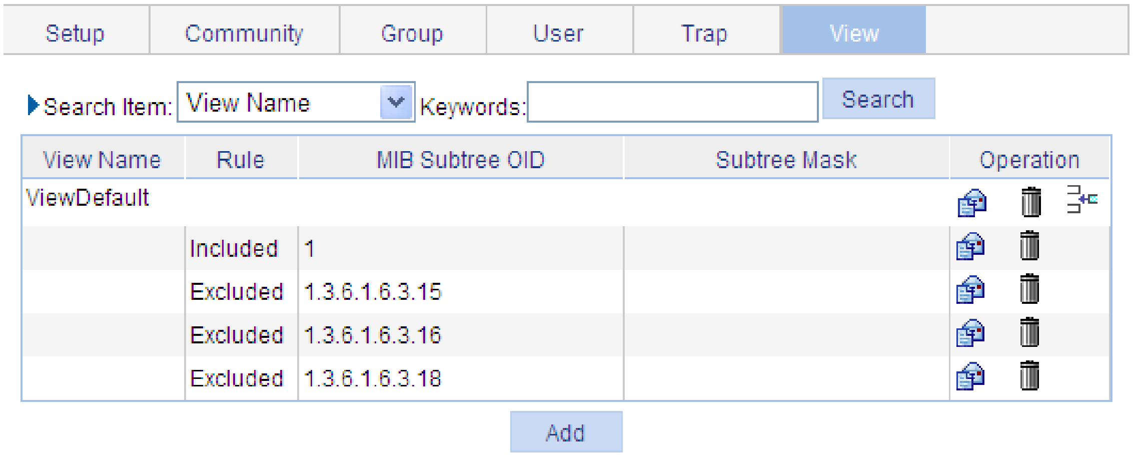
Item	Description
SNMP	Specify to enable or disable SNMP.
Local Engine ID	Configure the local engine ID. The validity of a user after it is created depends on the engine ID of the SNMP agent. If the engine ID when the user is created is not identical to the current engine ID, the user is invalid.
Maximum Packet Size	Configure the maximum size of an SNMP packet that the agent can receive/send.
Contact	Set a character string to describe the contact information for system maintenance. If the device is faulty, the maintainer can contact the manufacture factory according to the contact information of the device.
Location	Set a character string to describe the physical location of the device.
SNMP Version	Set the SNMP version run by the system

Return to SNMPv1 or SNMPv2c configuration task list or SNMPv3 configuration task list.

Configuring an SNMP View

Select **Device** > **SNMP** from the navigation tree, and then click the **View** tab to enter the page as shown in Figure 1-5.

Figure 1-5 View page



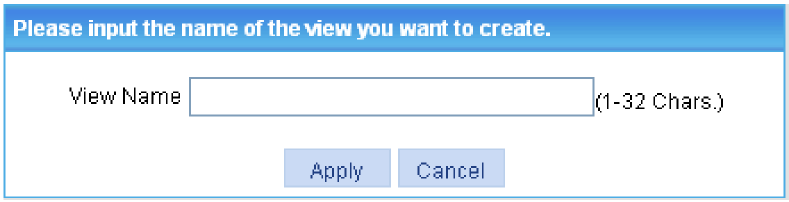
Search Item: View Name Keywords:

View Name	Rule	MIB Subtree OID	Subtree Mask	Operation
ViewDefault				
	Included	1		
	Excluded	1.3.6.1.6.3.15		
	Excluded	1.3.6.1.6.3.16		
	Excluded	1.3.6.1.6.3.18		

Creating an SNMP view

Click **Add**, the window appears as shown in Figure 1-6. Type the view name and click **Apply**, and then you enter the page as shown in Figure 1-7.

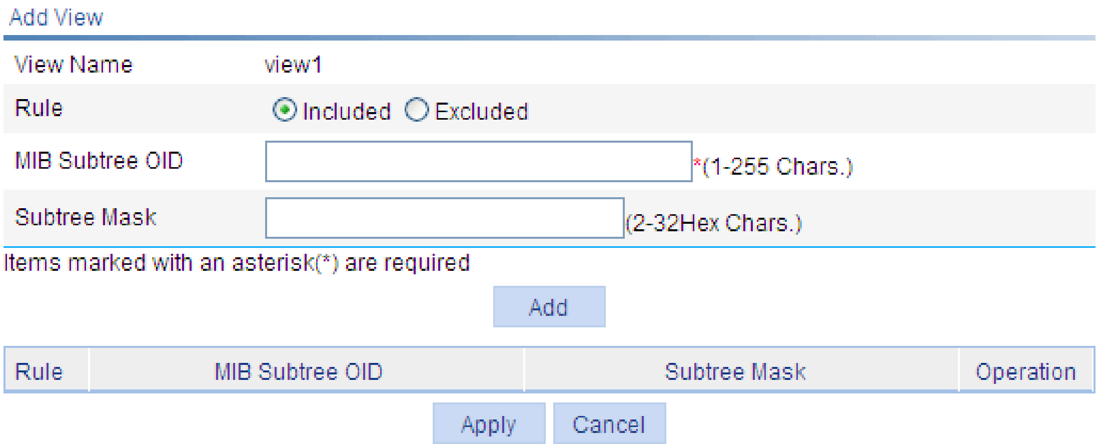
Figure 1-6 Create an SNMP view (1)



Please input the name of the view you want to create.

View Name (1-32 Chars.)

Figure 1-7 Create an SNMP view (2)



Add View

View Name	view1
Rule	● Included ○ Excluded
MIB Subtree OID	*(1-255 Chars.)
Subtree Mask	(2-32Hex Chars.)

Items marked with an asterisk(*) are required

Rule	MIB Subtree OID	Subtree Mask	Operation

Table 1-4 describes the configuration items for creating an SNMP view. After configuring the parameters of a rule, click **Add** to add the rule into the list box at the lower part of the page. After configuring all rules, click **Apply** to crate an SNMP view. Note that the view will not be created if you click **Cancel**.

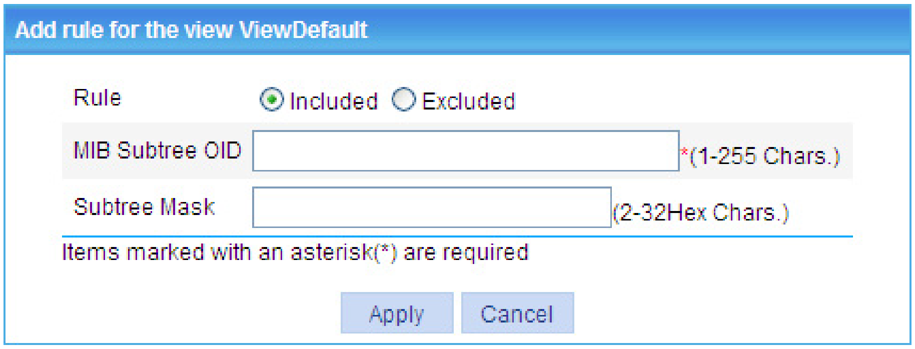
Table 1-4 Configuration items for creating an SNMP view

Item	Description
View Name	Set the SNMP view name.
Rule	Select to exclude or include the objects in the view range determined by the MIB subtree OID and subtree mask.
MIB Subtree OID	Set the MIB subtree OID (such as 1.4.5.3.1) or name (such as system). MIB subtree OID identifies the position of a node in the MIB tree, and it can uniquely identify a MIB subtree.
Subtree Mask	Set the subtree mask. If no subtree mask is specified, the default subtree mask (all Fs) will be used for mask-OID matching.

Adding rules to an SNMP view

Click the icon corresponding to the specified view on the page as shown in Figure 1-5, the **Add rule for the view ViewDefault** window appears as shown in Figure 1-8. After configuring the parameters, click **Apply** to add the rule for the view. Table 1-4 describes the configuration items for creating an SNMP view.

Figure 1-8 Add rules to an SNMP view



Add rule for the view ViewDefault

Rule ● Included ○ Excluded

MIB Subtree OID *(1-255 Chars.)

Subtree Mask (2-32Hex Chars.)

Items marked with an asterisk(*) are required

Note

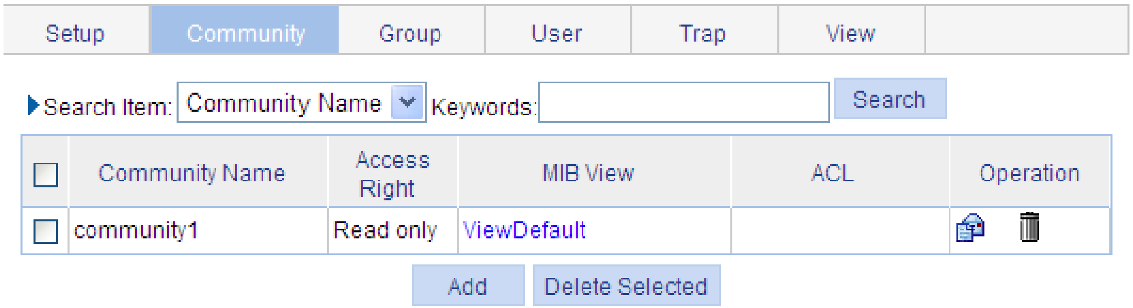
You can also click the icon corresponding to the specified view on the page as shown in Figure 1-5, and then you can enter the page to modify the view.

Return to SNMPv1 or SNMPv2c configuration task list or SNMPv3 configuration task list.

Configuring an SNMP Community

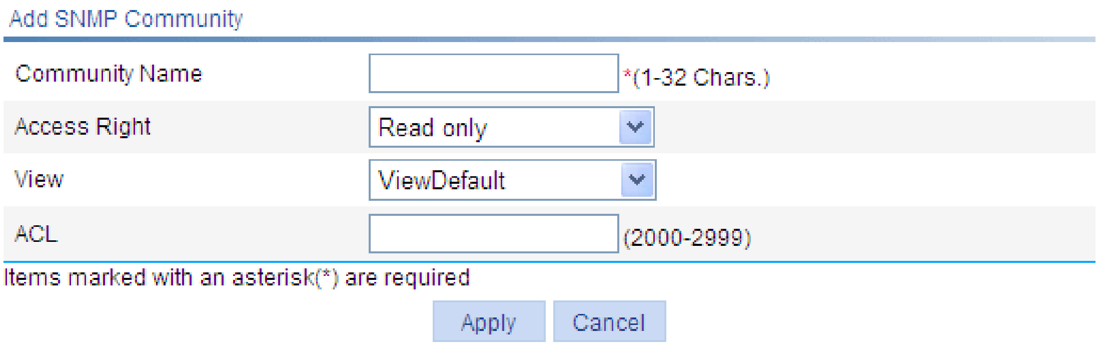
Select **Device** > **SNMP** from the navigation tree, then click the **Community** tab to enter the page as shown in Figure 1-9. Click **Add** to enter the **Add SNMP Community** page as shown in Figure 1-10.

Figure 1-9 Configure an SNMP community



□	Community Name	Access Right	MIB View	ACL	Operation
□	community1	Read only	ViewDefault		

Figure 1-10 Create an SNMP Community



Community Name	*(1-32 Chars.)
Access Right	Read only
View	ViewDefault
ACL	(2000-2999)

Items marked with an asterisk(*) are required

Table 1-5 describes the configuration items for configuring an SNMP community.

Table 1-5 Configuration items for configuring an SNMP community

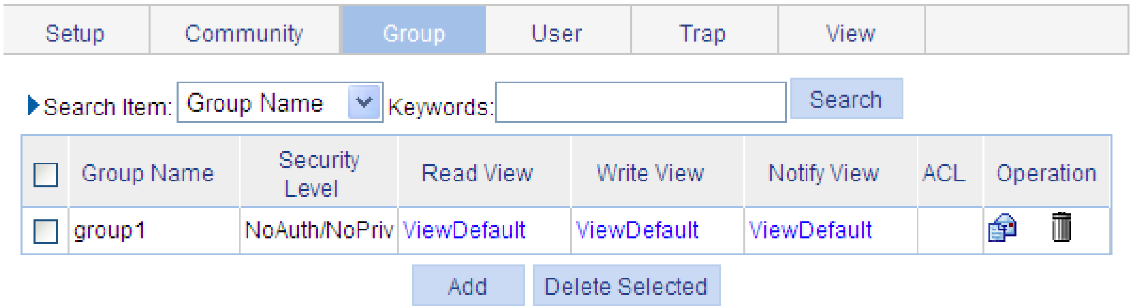
Item	Description
Community Name	Set the SNMP community name.
Access Right	Configure SNMP NMS access right • Read only: The NMS can perform read-only operations to the MIB objects when it uses this community name to access the agent, • Read and write: The NMS can perform both read and write operations to the MIB objects when it uses this community name to access the agent.
View	Specify the view associated with the community to limit the MIB objects that can be accessed by the NMS.
ACL	Associate the community with a basic ACL to allow or prohibit the access to the agent from the NMS with the specified source IP address.

Return to SNMPv1 or SNMPv2c configuration task list.

Configuring an SNMP Group

Select **Device** > **SNMP** from the navigation tree, then click the **Group** tab to enter the page as shown in Figure 1-11. Click **Add** to enter the **Add SNMP Group** page as shown in Figure 1-12.

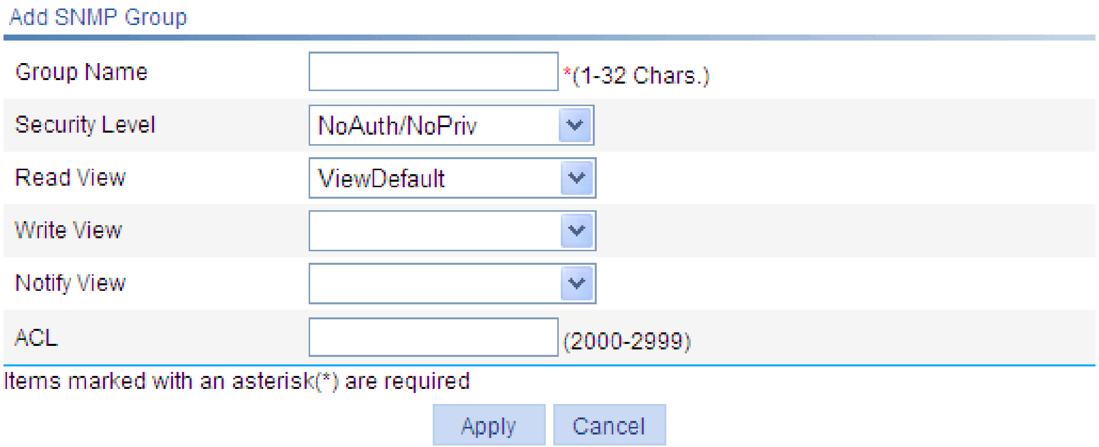
Figure 1-11 SNMP group



Search Item: Group Name

□	Group Name	Security Level	Read View	Write View	Notify View	ACL	Operation
□	group1	NoAuth/NoPriv	ViewDefault	ViewDefault	ViewDefault		

Figure 1-12 Create an SNMP group



Group Name	*(1-32 Chars.)
Security Level	NoAuth/NoPriv
Read View	ViewDefault
Write View	
Notify View	
ACL	(2000-2999)

Items marked with an asterisk(*) are required

Table 1-6 describes the configuration items for creating an SNMP group.

Table 1-6 Configuration items for creating an SNMP group

Item	Description
Group Name	Set the SNMP group name.
Security Level	Select the security level for the SNMP group. The available security levels are: • NoAuth/NoPriv: No authentication no privacy. • Auth/NoPriv: Authentication without privacy. • Auth/Priv: Authentication and privacy. **Highlight** *For an existing SNMP group, its security level cannot be modified.*
Read View	Select the read view of the SNMP group.
Write View	Select the write view of the SNMP group. If no write view is configured, the NMS cannot perform the write operations to all MIB objects on the device.
Notify View	Select the notify view of the SNMP group, that is, the view that can send trap messages. If no notify view is configured, the agent does not send traps to the NMS.

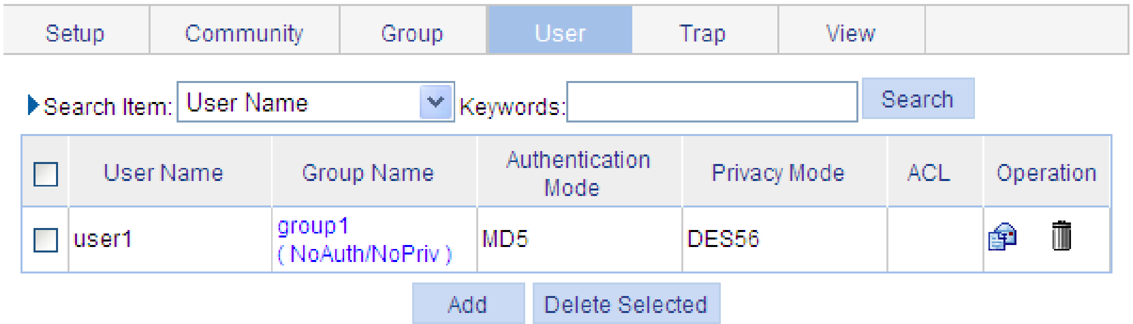
Item	Description
ACL	Associate a basic ACL with the group to restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to restrict the intercommunication between the NMS and the agent.

Return to SNMPv3 configuration task list.

Configuring an SNMP User

Select **Device** > **SNMP** from the navigation tree, then click the **User** tab to enter the page as shown in Figure 1-13. Click **Add** to enter the **Add SNMP User** page, as shown in Figure 1-14.

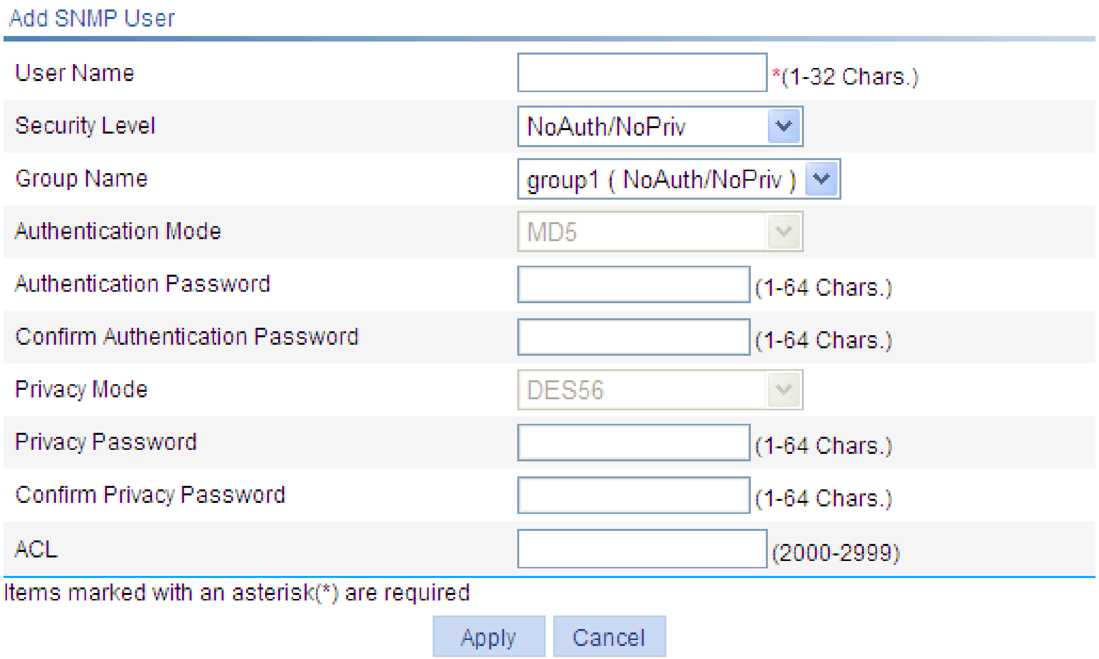
Figure 1-13 SNMP user



Search Item: User Name Keywords:

□	User Name	Group Name	Authentication Mode	Privacy Mode	ACL	Operation
□	user1	group1 (NoAuth/NoPriv)	MD5	DES56		

Figure 1-14 Create an SNMP user



Add SNMP User

User Name		*(1-32 Chars.)
Security Level	NoAuth/NoPriv	
Group Name	group1 (NoAuth/NoPriv)	
Authentication Mode	MD5	
Authentication Password		(1-64 Chars.)
Confirm Authentication Password		(1-64 Chars.)
Privacy Mode	DES56	
Privacy Password		(1-64 Chars.)
Confirm Privacy Password		(1-64 Chars.)
ACL		(2000-2999)

Items marked with an asterisk(*) are required

Table 1-7 describes the configuration items for creating an SNMP user.

Table 1-7 Configuration items for creating an SNMP user

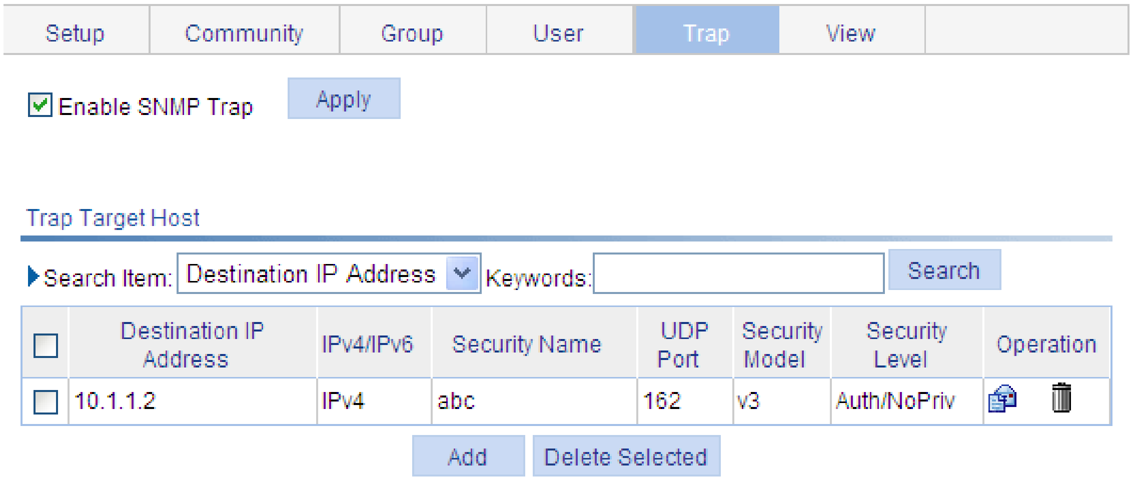
Item	Description
User Name	Set the SNMP user name.
Security Level	Select the security level for the SNMP group. The available security levels are: • NoAuth/NoPriv: No authentication no privacy. • Auth/NoPriv: Authentication without privacy. • Auth/Priv: Authentication and privacy.
Group Name	Select an SNMP group to which the user belongs. • When the security level is NoAuth/NoPriv, you can select an SNMP group with no authentication no privacy. • When the security level is Auth/NoPriv, you can select an SNMP group with no authentication no privacy or authentication without privacy. • When the security level is Auth/Priv, you can select an SNMP group of any security level.
Authentication Mode	Select an authentication mode (including MD5 and SHA) when the security level is Auth/NoPriv or Auth/Priv.
Authentication Password	Set the authentication password when the security level is Auth/NoPriv or Auth/Priv. The confirm authentication password must be the same with the authentication password.
Confirm Authentication Password	
Privacy Mode	Select a privacy mode (including DES56, AES128, and 3DES) when the security level is Auth/Priv.
Privacy Password	Set the privacy password when the security level is Auth/Priv. The confirm privacy password must be the same with the privacy password.
Confirm Privacy Password	
ACL	Associate a basic ACL with the user to restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

Return to SNMPv3 configuration task list.

Configuring SNMP Trap Function

Select **Device** > **SNMP** from the navigation tree, and click the **Trap** tab to enter the page as shown in Figure 1-15. On the upper part of the page, you can select to enable the SNMP trap function; on the lower part of the page, you can configure target hosts of the SNMP traps. Click **Add** to enter the **Add Trap Target Host** page, as shown in Figure 1-16.

Figure 1-15 Traps configuration



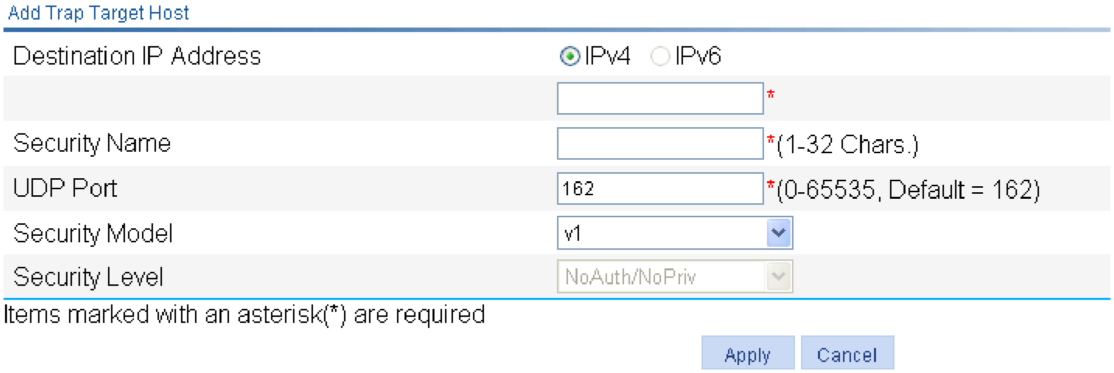
☑ Enable SNMP Trap

Trap Target Host

Search Item: Destination IP Address Keywords:

□	Destination IP Address	IPv4/IPv6	Security Name	UDP Port	Security Model	Security Level	Operation
□	10.1.1.2	IPv4	abc	162	v3	Auth/NoPriv	

Figure 1-16 Add a target host of SNMP traps



Add Trap Target Host

Destination IP Address	● IPv4 ○ IPv6
	*
Security Name	*(1-32 Chars.)
UDP Port	162 *(0-65535, Default = 162)
Security Model	v1
Security Level	NoAuth/NoPriv

Items marked with an asterisk(*) are required

Table 1-8 describes the configuration items for adding a target host of SNMP traps.

Table 1-8 Configuration items for adding a target host

Item	Description
Destination IP Address	Set the destination IP address. Select the IP address type: IPv4 or IPv6, and then type the corresponding IP address in the text box according to the IP address type.
Security Name	Set the security name, which can be an SNMPv1 community name, an SNMPv2c community name, or an SNMPv3 user name.
UDP Port	Set UDP port number.
Security Model	Select the security model, that is, the SNMP version. Ensure that the SNMP version is the same with that on the NMS; otherwise, the NMS cannot receive any trap.
Security Level	Set the authentication and privacy mode for SNMP traps when the security model is selected as **v3.** The available security levels are: no authentication no privacy, authentication but no privacy, and authentication and privacy. When the security model is selected as **v1** or **v2c**, the security level is no authentication no privacy, and cannot be modified.

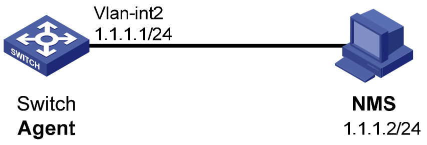
Return to SNMPv1 or SNMPv2c configuration task list or SNMPv3 configuration task list.

SNMP Configuration Example

Network requirements

- As shown in Figure 1-17, the NMS connects to the agent, Switch, through an Ethernet.
- The IP address of the NMS is 1.1.1.2/24.
- The IP address of the VLAN interface on Switch is 1.1.1.1/24.
- The NMS monitors the agent using SNMPv3. The agent reports errors or faults to the NMS. The NMS uses port 5000 to receive traps.

Figure 1-17 Network diagram for SNMP configuration



Configuration procedure

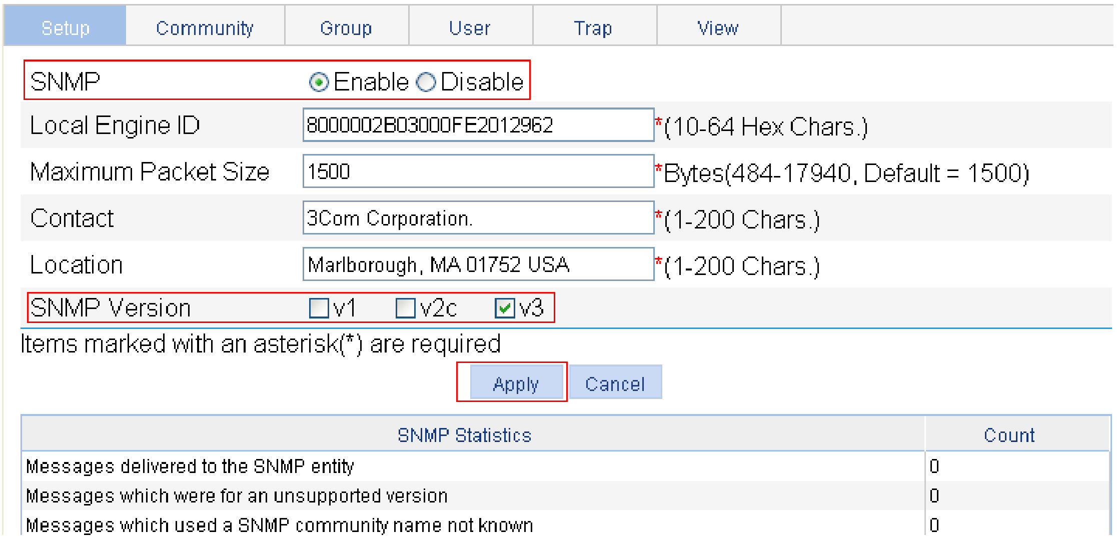
1) Configure Agent

# Configuration IP addresses for the interfaces. (Omitted)

# Enable SNMP.

Select **Device** > **SNMP** from the navigation tree, and you will enter the **Setup** page as shown in Figure 1-18.

Figure 1-18 Enable SNMP



SNMP	● Enable ○ Disable	
Local Engine ID	8000002B03000FE2012962	*(10-64 Hex Chars.)
Maximum Packet Size	1500	*Bytes(484-17940, Default = 1500)
Contact	3Com Corporation.	*(1-200 Chars.)
Location	Marlborough, MA 01752 USA	*(1-200 Chars.)
SNMP Version	□ v1 □ v2c ☑ v3	

Items marked with an asterisk(*) are required

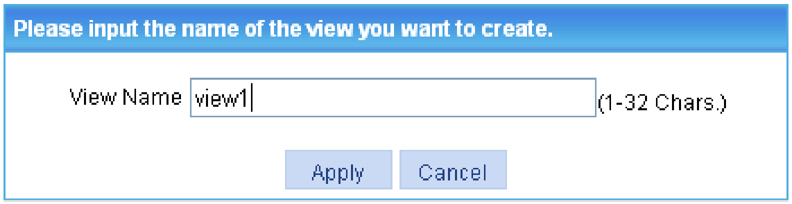
SNMP Statistics	Count
Messages delivered to the SNMP entity	0
Messages which were for an unsupported version	0
Messages which used a SNMP community name not known	0

- Select the **Enable** radio box.
- Select the **v3** radio box.
- Click **Apply**.

# Configure an SNMP view.

- Click the **View** tab and then click **Add** to enter the page as shown in Figure 1-19.

Figure 1-19 Create an SNMP view (1)

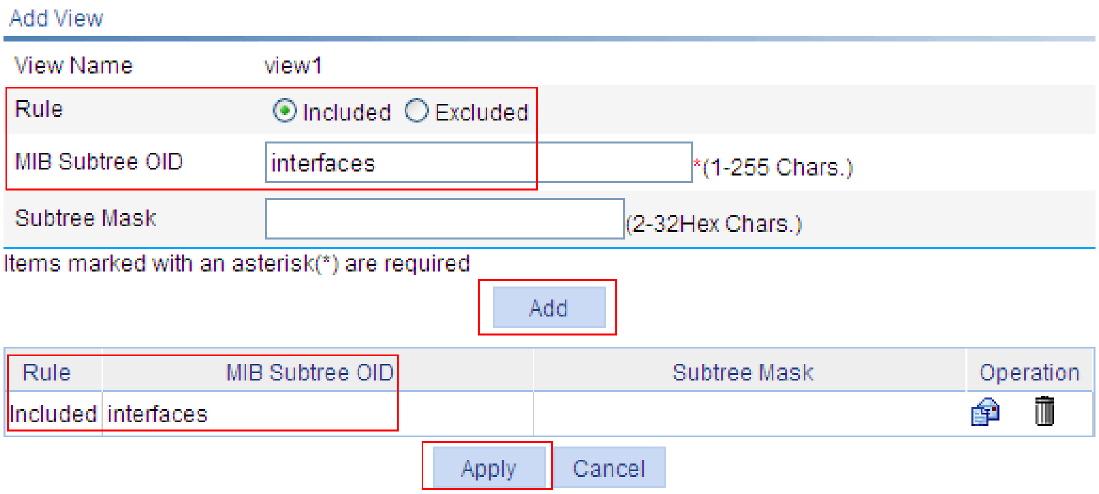


Please input the name of the view you want to create.

View Name: view1 (1-32 Chars.)

- Type **view1** in the text box.
- Click **Apply** to enter the SNMP rule configuration page, as shown in Figure 1-20.

Figure 1-20 Create an SNMP view (2)



Add View

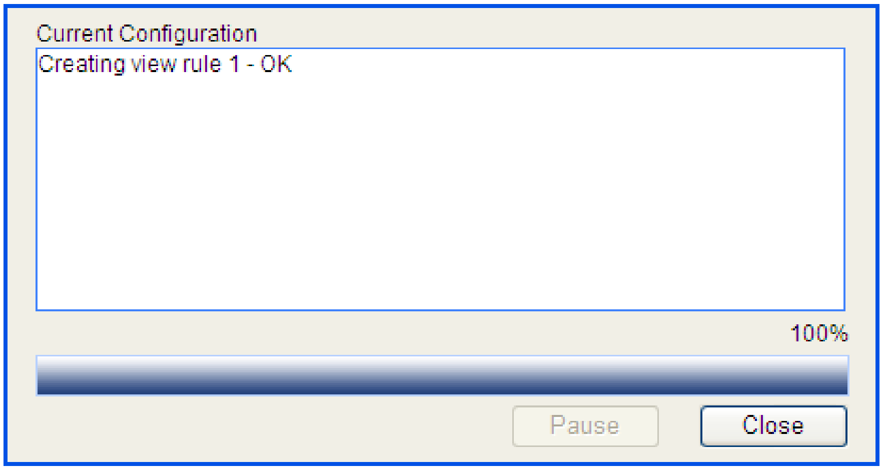
View Name	view1
Rule	● Included ○ Excluded
MIB Subtree OID	interfaces *(1-255 Chars.)
Subtree Mask	(2-32Hex Chars.)

Items marked with an asterisk(*) are required

Rule	MIB Subtree OID	Subtree Mask	Operation
Included	interfaces		

- Select the **Included** radio box.
- Type the MIB subtree OID **interfaces.**
- Click **Add.**
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-21.

Figure 1-21 Configuration progress dialog box



Current Configuration

```
Creating view rule 1 - OK
```

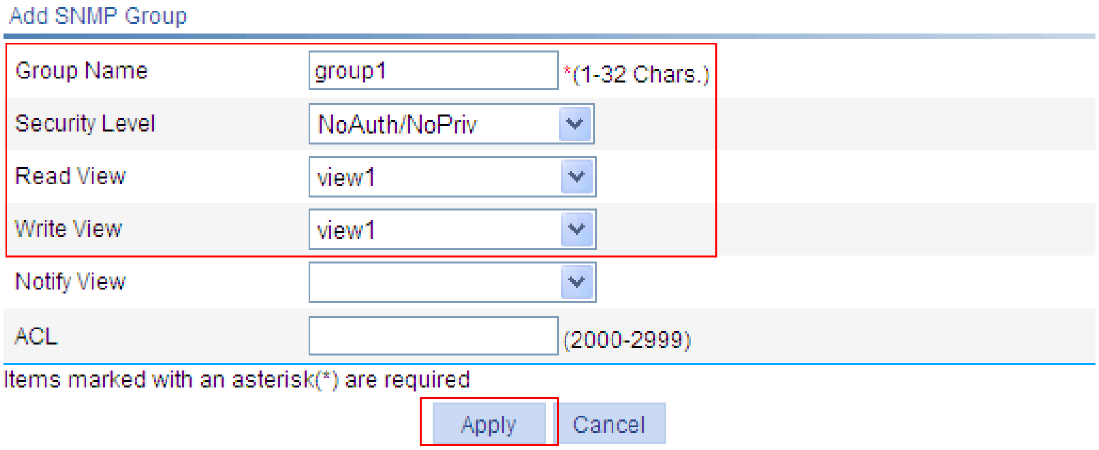
100%

- After the configuration process is complete, click **Close**.

# Configure an SNMP group.

- Click the **Group** tab and then click **Add** to enter the page as shown in Figure 1-22.

Figure 1-22 Create an SNMP group



Add SNMP Group

Group Name	group1	*(1-32 Chars.)
Security Level	NoAuth/NoPriv	
Read View	view1	
Write View	view1	
Notify View		
ACL		(2000-2999)

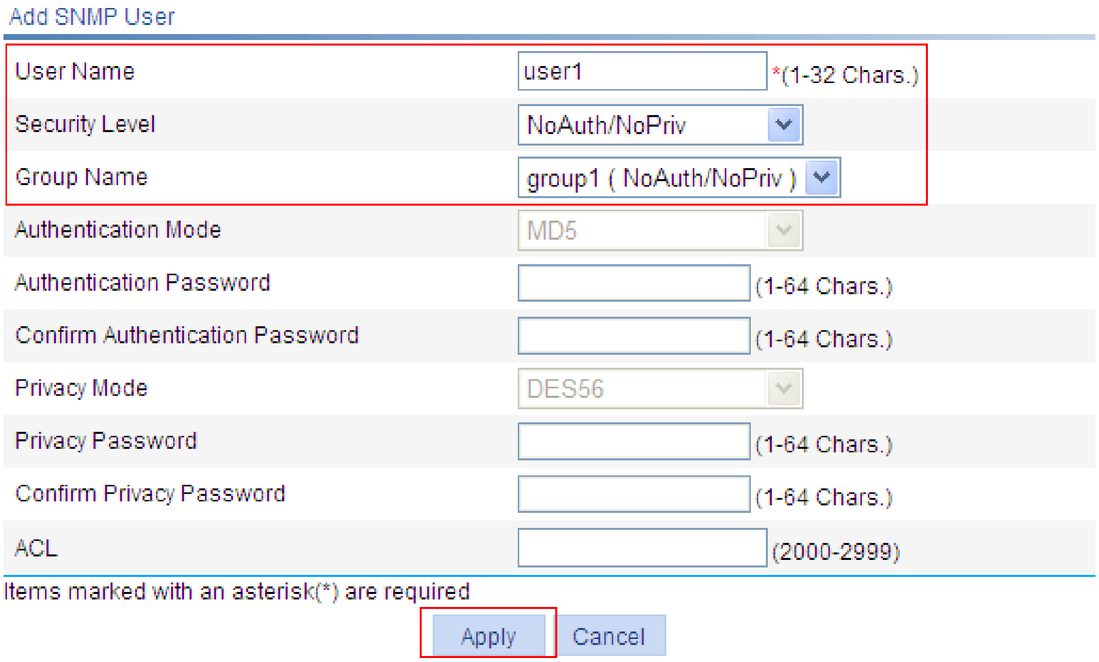
Items marked with an asterisk(*) are required

- Type **group1** in the text box of **Group Name**.
- Select **view1** from the **Read View** drop-down box.
- Select **view1** from the **Write View** drop-down box.
- Click **Apply**.

# Configure an SNMP user

- Click the **User** tab and then click **Add** to enter the page as shown in Figure 1-23.

Figure 1-23 Create an SNMP user



Add SNMP User

User Name	user1	*(1-32 Chars.)
Security Level	NoAuth/NoPriv	
Group Name	group1 (NoAuth/NoPriv)	
Authentication Mode	MD5	
Authentication Password		(1-64 Chars.)
Confirm Authentication Password		(1-64 Chars.)
Privacy Mode	DES56	
Privacy Password		(1-64 Chars.)
Confirm Privacy Password		(1-64 Chars.)
ACL		(2000-2999)

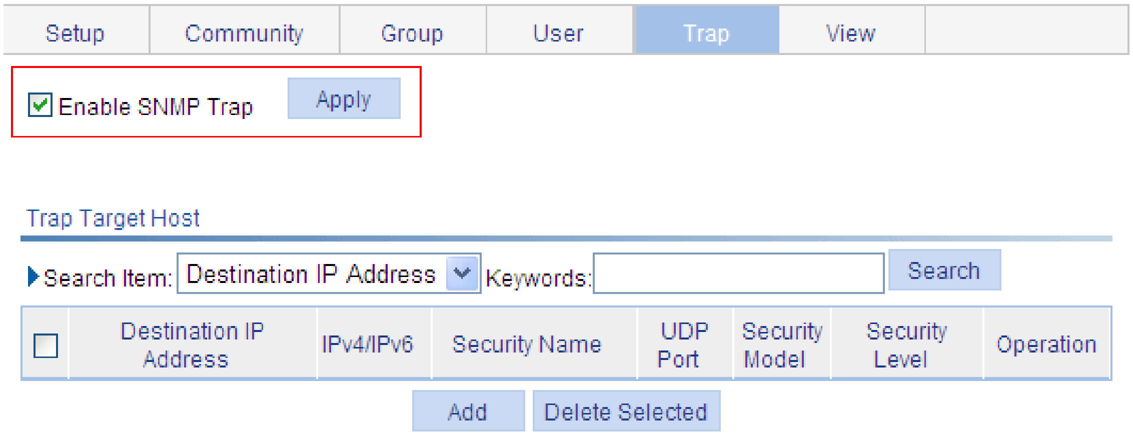
Items marked with an asterisk(*) are required

- Type **user1** in the text box of **User Name**.
- Select **group1** from the **Group Name** drop-down box.
- Click **Apply**.

# Enable the agent to send SNMP traps.

- Click the **Trap** tab and enter the page as shown in Figure 1-24.

Figure 1-24 Enable the agent to send SNMP traps



☑ Enable SNMP Trap

Search Item: Destination IP Address Keywords:

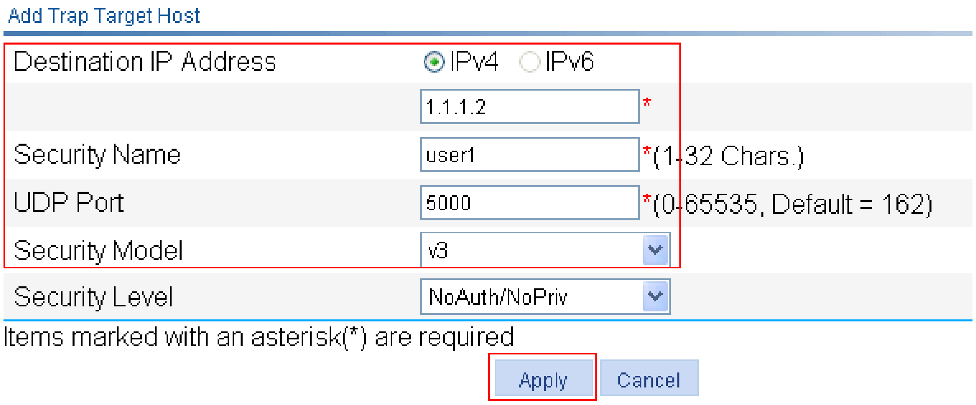
□	Destination IP Address	IPv4/IPv6	Security Name	UDP Port	Security Model	Security Level	Operation

- Select the **Enable SNMP Trap** check-box.
- Click **Apply**.

# Add target hosts of SNMP traps.

- Click **Add** to enter the page as shown in Figure 1-25.

Figure 1-25 Add target hosts of SNMP traps



Destination IP Address	● IPv4 ○ IPv6
	1.1.1.2 *
Security Name	user1 *(1-32 Chars.)
UDP Port	5000 *(0-65535, Default = 162)
Security Model	v3
Security Level	NoAuth/NoPriv

Items marked with an asterisk(*) are required

- Select the destination IP address type as **IPv4**.
- Type the destination address **1.1.1.2**.
- Type the user name **user1**.
- Type the UDP port **5000**.
- Select **v3** from the **Security Model** drop-down box.
- Click **Apply**.

2) Configure NMS.

⚠ **Caution**

The configuration on NMS must be consistent with that on the agent. Otherwise, you cannot perform corresponding operations.

SNMPv3 adopts a security mechanism of authentication and privacy. You need to configure username and security level. According to the configured security level, you need to configure the related authentication mode, authentication password, privacy mode, privacy password, and so on.

Besides, you need to configure the aging time and retry times. After the above configurations, you can configure the device as needed through the NMS. For related configurations, refer to the manual provided for NMS.

Configuration verification

- After the above configuration, the NMS can establish an SNMP connection with the agent and query and reconfigure values of objects in the agent MIB.
- If an idle interface on the agent is shut down or brought up, the NMS will receive a trap information sent by the agent.

Table of Contents

1 Interface Statistics

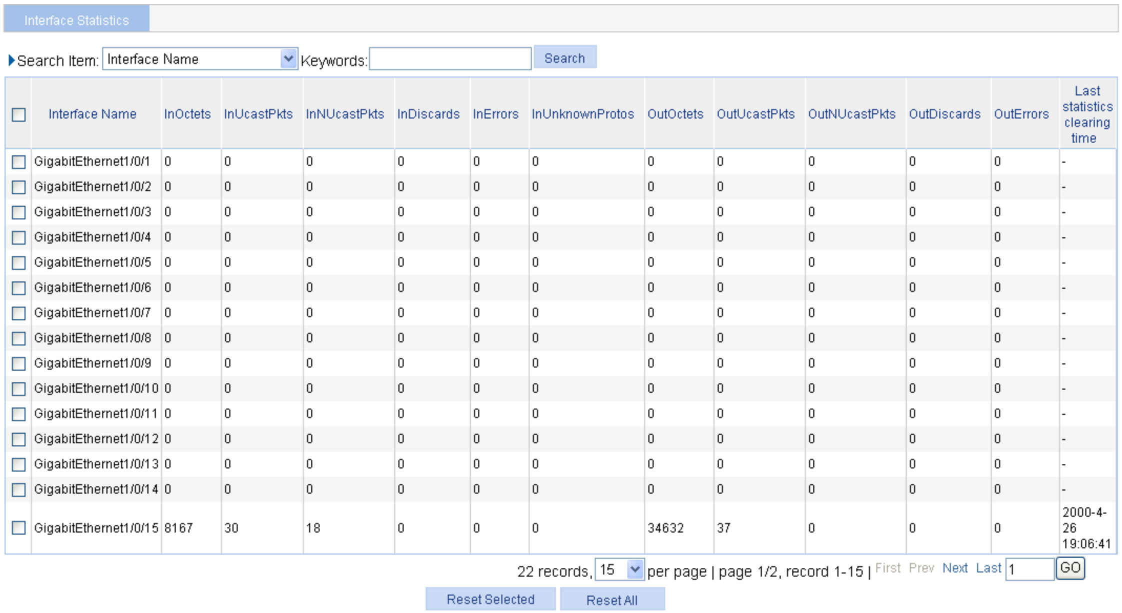
Overview

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

Displaying Interface Statistics

Select **Device** > **Interface Statistics** from the navigation tree to enter the interface statistics display page, as shown in Figure 1-1.

Figure 1-1 Interface statistics display page



□	Interface Name	InOctets	InUcastPkts	InNUcastPkts	InDiscards	InErrors	InUnknownProtos	OutOctets	OutUcastPkts	OutNUcastPkts	OutDiscards	OutErrors	Last statistics clearing time
□	GigabitEthernet1/0/1	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/2	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/3	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/4	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/5	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/6	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/7	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/8	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/9	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/10	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/11	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/12	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/13	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/14	0	0	0	0	0	0	0	0	0	0	0	-
□	GigabitEthernet1/0/15	8167	30	18	0	0	0	34632	37	0	0	0	2000-4-26 19:06:41

22 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Table 1-1 describes the details about the interface statistics.

Table 1-1 Details about the interface statistics

Field	Description
InOctets	Total octets of all packets received on the interface.
InUcastPkts	Number of received unicast packets.
InNUcastPkts	Number of received non-unicast packets.
InDiscards	Number of valid packets discarded in the inbound direction.
InErrors	Number of received invalid packets.
InUnknownProtos	Number of received unknown protocol packets.
OutOctets	Total octets of all packets sent through the interface.

Field	Description
OutUcastPkts	Number of unicast packets sent through the interface.
OutNUcastPkts	Number of non-unicast packets sent through the interface.
OutDiscards	Number of valid packets discarded in the outbound direction.
OutErrors	Number of invalid packets sent through the interface.

Table of Contents

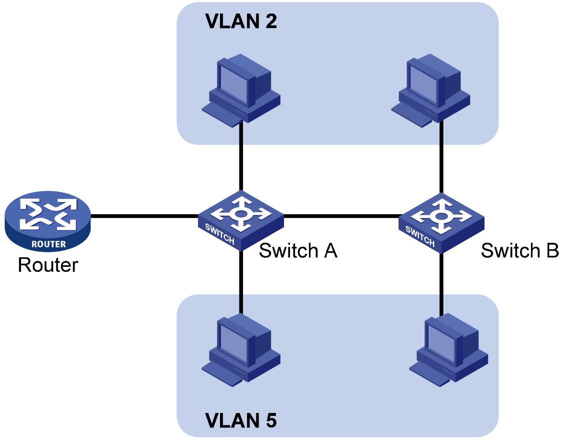
1 VLAN Configuration

Overview

Introduction to VLAN

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

Figure 1-1 A VLAN diagram



VLANs are logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same LAN, regardless of their physical locations.

VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. For hosts in different VLANs to communicate, routers or Layer 3 switches are required.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

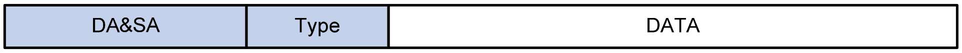
How VLAN Works

To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

The format of VLAN-tagged frames is defined in IEEE 802.1Q-1999.

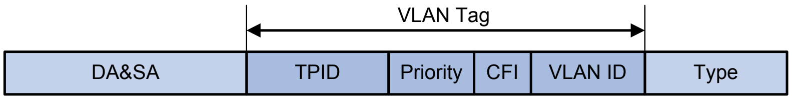
In the header of a traditional Ethernet data frame as shown in Figure 1-2, the field after the destination MAC address and the source MAC address fields (DA&SA in the figure) is the Type field indicating the upper layer protocol type.

Figure 1-2 The format of a traditional Ethernet frame



IEEE 802.1Q inserts a four-byte VLAN tag before the Type field, as shown in Figure 1-3.

Figure 1-3 The position and format of VLAN tag



A VLAN tag comprises four fields: tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN tagged.
- The 3-bit priority field indicates the 802.1p priority of the frame.
- The 1-bit CFI field specifies whether the MAC addresses are encapsulated in the canonical format for the receiving device to correctly interpret the MAC addresses. Value 0 indicates that the MAC addresses are encapsulated in canonical format; value 1 indicates that the MAC addresses are encapsulated in non-canonical format. The field is set to 0 by default.
- The 12-bit VLAN ID field identifies the VLAN the frame belongs to. The VLAN ID range is 0 to 4095. As 0 and 4095 are reserved by the protocol, the VLAN ID range available for assignment is 1 to 4094.

When receiving a frame, a network device looks at its VLAN tag to decide how to handle the frame.

Note

The Ethernet II encapsulation format is used in this section. Besides this format, other encapsulation formats, including 802.2 LLC, 802.2 SNAP, and 802.3 raw, are also supported by Ethernet. The VLAN tag fields are also used in these encapsulations for VLAN identification.

VLAN Types

You can create VLANs based on:

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

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

Introduction to Port-Based VLAN

Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

Port link type

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

- Access. An access port belongs to only one VLAN and usually connects to a user device.
- Trunk. A trunk port can join multiple VLANs to receive and send traffic for them. It usually connects to a network device.
- Hybrid. A hybrid port can join multiple VLANs to receive and send traffic for them. It can connect either a user device or a network device.

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

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

Default VLAN (PVID)

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

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

A port configured with a default VLAN handles a frame as follows:

Port type	Actions (in the inbound direction)		Actions (in the outbound direction)
	Untagged frame	Tagged frame	
Access	Tag the frame with the default VLAN tag.	• Receive the frame if its VLAN ID is the same as the default VLAN ID. • Drop the frame if its VLAN ID is different from the default VLAN ID.	Remove the default VLAN tag and send the frame.
Trunk	Check whether the default VLAN is carried on the port: • If yes, tag the frame with the default VLAN tag. • If not, drop the frame.	• Receive the frame if its VLAN is carried on the port. • Drop the frame if its VLAN is not carried on the port.	• Remove the tag and send the frame if the frame carries the default VLAN tag and the port belongs to the default VLAN. • Send the frame without removing the tag if its VLAN is carried on the port but is different from the default one.
Hybrid			Send the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration.

Configuring a VLAN

Configuration Task List

Use one of the following two approaches or combine the following two approaches to configure a VLAN:

- Approach I: modify a VLAN, as shown in Table 1-1.
- Approach II: modify a port, as shown in Table 1-2.

Table 1-1 VLAN configuration task list (approach I)

Task	Remarks
Creating VLANs	Required Create one or multiple VLANs
Selecting VLANs	Required Reduce the range of VLANs available for selection during related operations, that is, configure a subset of all existing VLANs. This step is required before displaying, modifying, or removing a VLAN.
Modifying a VLAN	Required Configure the untagged member ports and tagged member ports of the VLAN, or remove the specified ports from the VLAN.

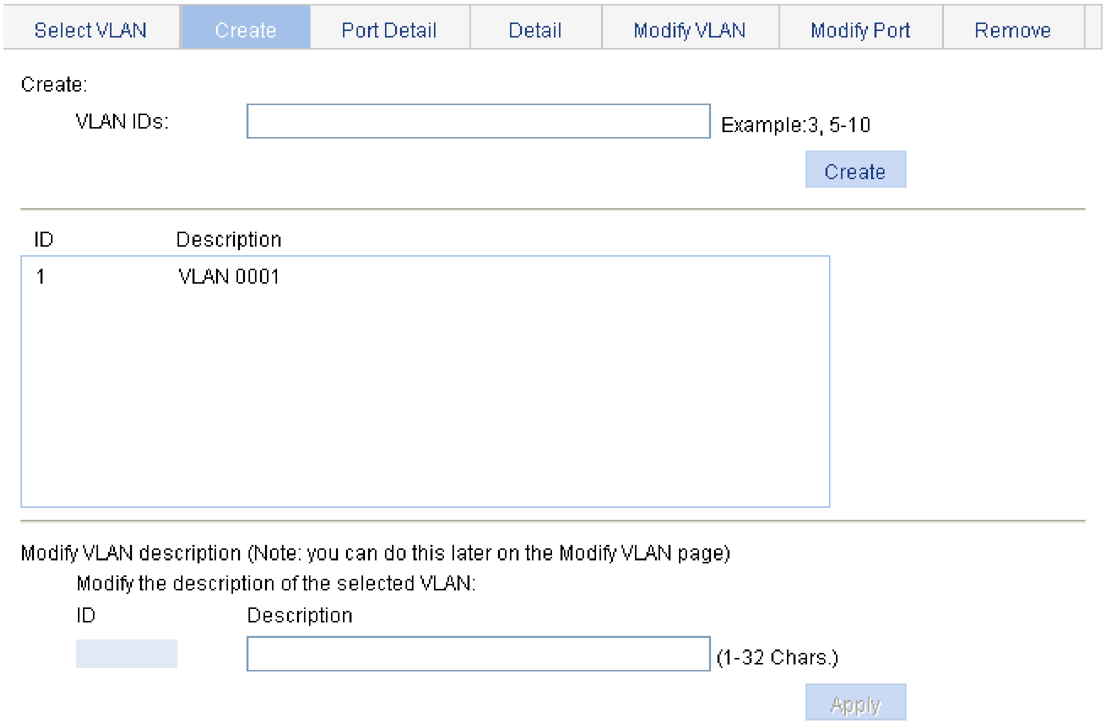
Table 1-2 VLAN configuration task list (approach II)

Task	Remarks
Creating VLANs	Required Create one or multiple VLANs
Modifying Ports	Required Configure ports as the untagged members or tagged members of VLANs, or remove ports from VLANs; configure the link type and PVID of the ports.

Creating VLANs

Select **Network** > **VLAN** from the navigation tree and click **Create** to enter the page for creating VLANs, as shown in Figure 1-4.

Figure 1-4 The **Create** tab



Create:

VLAN IDs: Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID Description (1-32 Chars.)

Table 1-3 describes the configuration items of creating a VLAN.

Table 1-3 Configuration items of creating VLANs

Item		Description
VLAN IDs		IDs of the VLANs to be created
Modify the description of the selected VLAN	ID	Select the ID of the VLAN whose description string is to be modified. Click the ID of the VLAN to be modified in the list in the middle of the page.
	Description	Set the description string of the selected VLAN. By default, the description string of a VLAN is its VLAN ID, such as **VLAN 0001**.

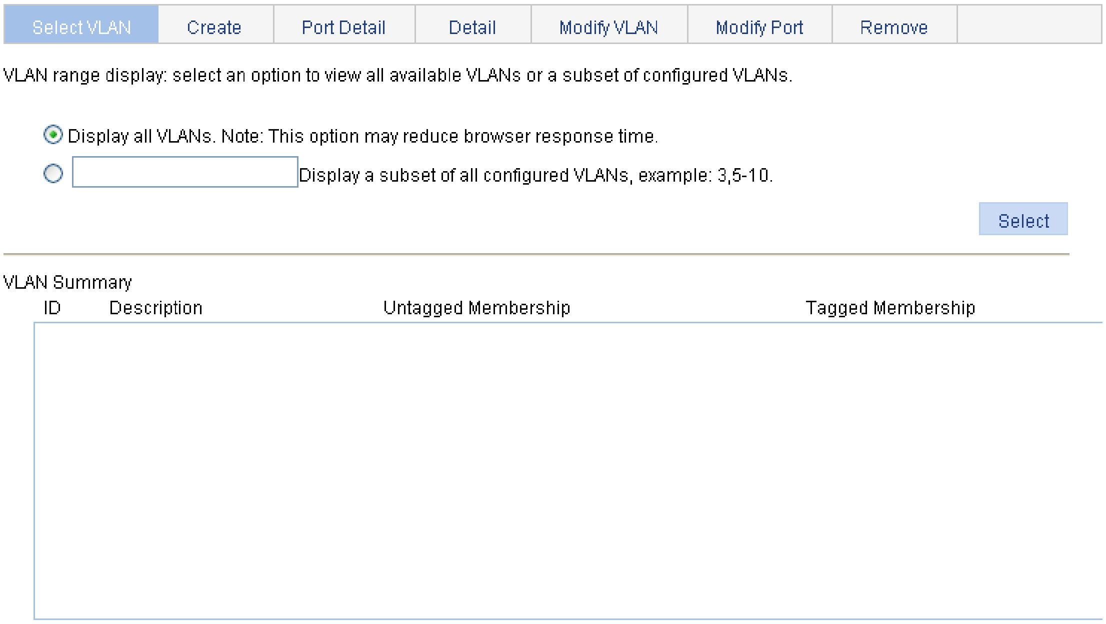
Return to VLAN configuration task list (approach I).

Return to VLAN configuration task list (approach II).

Selecting VLANs

Select **Network** > **VLAN** from the navigation tree. The **Select VLAN** tab is displayed by default for you to select VLANs, as shown in Figure 1-5.

Figure 1-5 The Select VLAN tab



VLAN range display: select an option to view all available VLANs or a subset of configured VLANs.

● Display all VLANs. Note: This option may reduce browser response time.

○ Display a subset of all configured VLANs, example: 3,5-10.

VLAN Summary

ID	Description	Untagged Membership	Tagged Membership

[Table 1-4](#) describes the configuration items of selecting VLANs.

Table 1-4 Configuration items of selecting VLANs

Item	Description
Display all VLANs	Select one of the two radio buttons: • Display all VLANs: displays all configured VLANs. • Display a subnet of all configured VLANs: type the VLAN ID(s) to be displayed.
Display a subnet of all configured VLANs	

Return to [VLAN configuration task list (approach I)](#).

Modifying a VLAN

Select **Network** > **VLAN** from the navigation tree and click **Modify VLAN** to enter the page for modifying a VLAN, as shown in [Figure 1-6](#).

Figure 1-6 The Modify VLAN tab

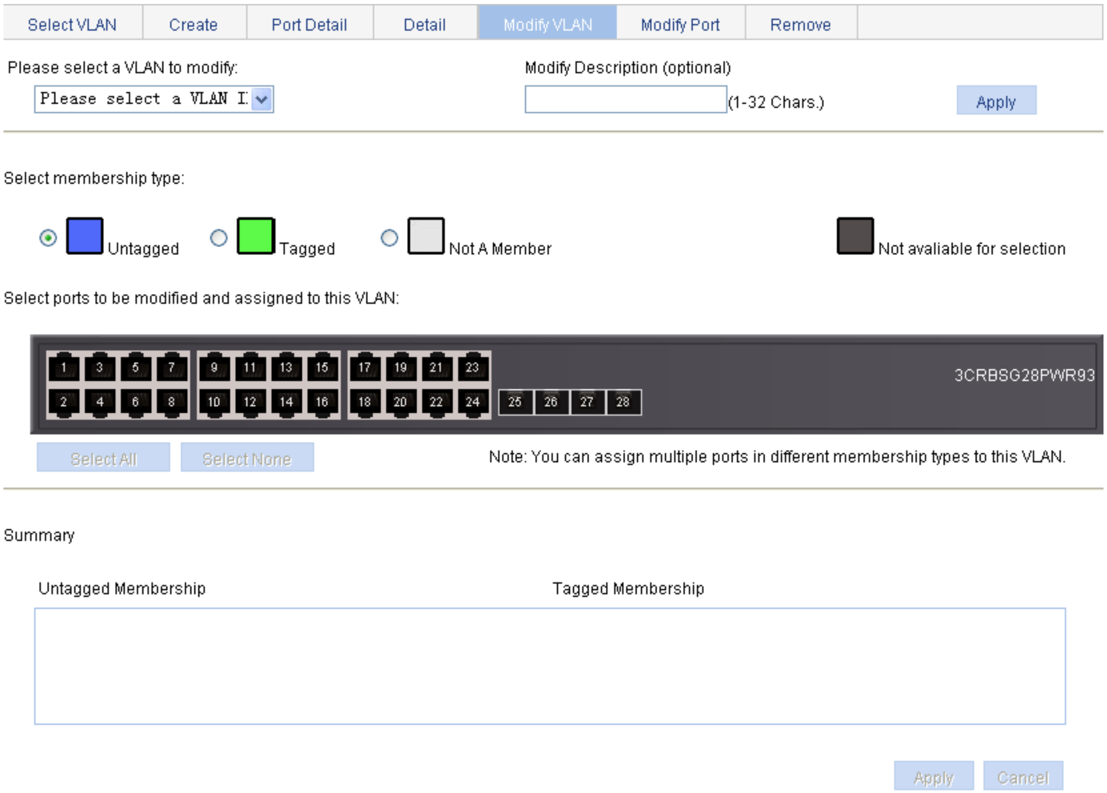


Table 1-5 describes the configuration items of modifying a VLAN.

Table 1-5 Configuration items of modifying a VLAN

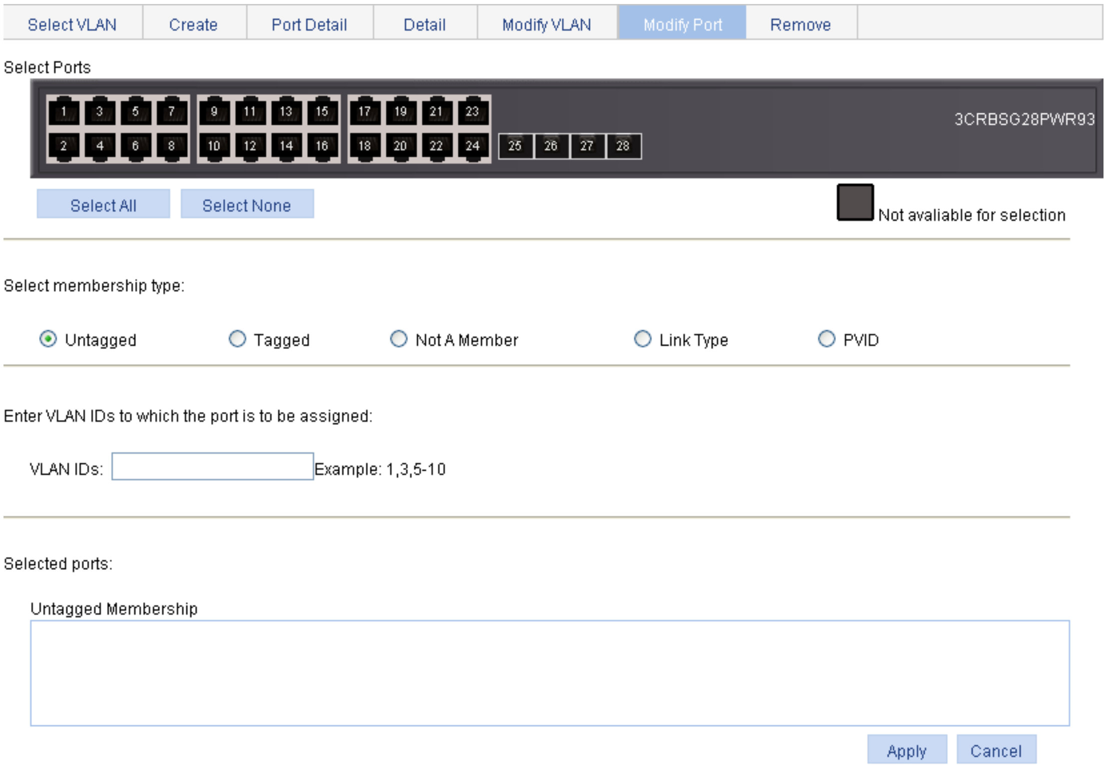
Item		Description
Please select a VLAN to modify		Select the VLAN to be modified. Select a VLAN in the drop-down list. The VLANs available for selection are created first and then selected on the page for selecting VLANs.
Modify Description		Modify the description string of the selected VLAN. By default, the description string of a VLAN is its VLAN ID, such as **VLAN 0001**.
Select membership type	Untagged	Set the member type of the port to be modified in the VLAN Select the **Untagged**, **Tagged**, or **Not A Member** radio button: • Untagged: Indicates that the port sends the traffic of the VLAN with the VLAN tag removed. • Untagged: Indicates that the port sends the traffic of the VLAN without removing the VLAN tag. • Not a Member: Removes the port from the VLAN.
	Tagged	
	Not A Member	
Select ports to be modified and assigned to this VLAN		Select the ports to be modified in the selected VLAN. Click the ports to be modified on the chassis front panel. You can select one or more ports. If aggregation groups are configured on the device, the page displays a list of aggregated ports below the chassis front panel. You can select ports from this list.

Return to VLAN configuration task list (approach I).

Modifying Ports

Select **Network** > **VLAN** from the navigation tree and click **Modify Port** to enter the page for modifying ports, as shown in Figure 1-7.

Figure 1-7 The Modify Port tab



Select Ports

■ Not avaliable for selection

Select membership type:

● Untagged ○ Tagged ○ Not A Member ○ Link Type ○ PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: Example: 1,3,5-10

Selected ports:

Untagged Membership

Table 1-6 describes the configuration items of modifying ports.

Table 1-6 Configuration items of modifying ports

Item		Description
Select Ports		Select the ports to be modified. Click the ports to be modified on the chassis front panel. You can select one or more ports. If aggregation groups are configured on the device, the page displays a list of aggregated ports below the chassis front panel. You can select ports from this list.
Select membership type	Untagged	Set the member type of the ports to be modified in the specified VLANs. Select the **Untagged**, **Tagged**, or **Not A Member** radio button: • Untagged: Assigns the selected prots to the specified VLANs as untagged members. After that, the ports send the traffic of those VLANs with the VLAN tags removed. • Tagged: Assigns the selected prots to the specified VLANs as tagged members. After that, the ports send the traffic of those VLANs without removing the VLAN tags. • Not A Member: Removes the selected ports from the specified VLANs.
	Tagged	
	Not A Member	
VLAN IDs		Set the IDs of the VLANs to/from which the selected ports are to be assigned/removed. This item is available when the **Untagged**, **Tagged**, or **Not A Member** option is selected in the **Select membership type** area.

Item	Description
Link Type	Set the link type of the selected ports, which can be access, hybrid, or trunk. This item is available when the **Link Type** option is selected in the **Select membership type** area.
PVID	Set the PVID of the select ports; selecting **Delete** is to restore the default VLAN, VLAN 1, of the ports. This item is available when the **PVID** option is selected in the **Select membership type** area.
Delete	

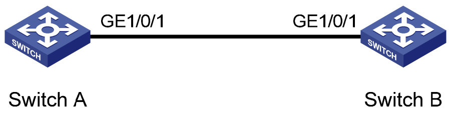
Return to VLAN configuration task list (approach II).

VLAN Configuration Example

Network requirements

- Trunk port GigabitEthernet 1/0/1 of Switch A is connected to trunk port GigabitEthernet 1/0/1 of Switch B.
- The default VLAN of GigabitEthernet 1/0/1 is VLAN 100.
- GigabitEthernet 1/0/1 permits packets of VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

Figure 1-8 Network diagram for VLAN configuration



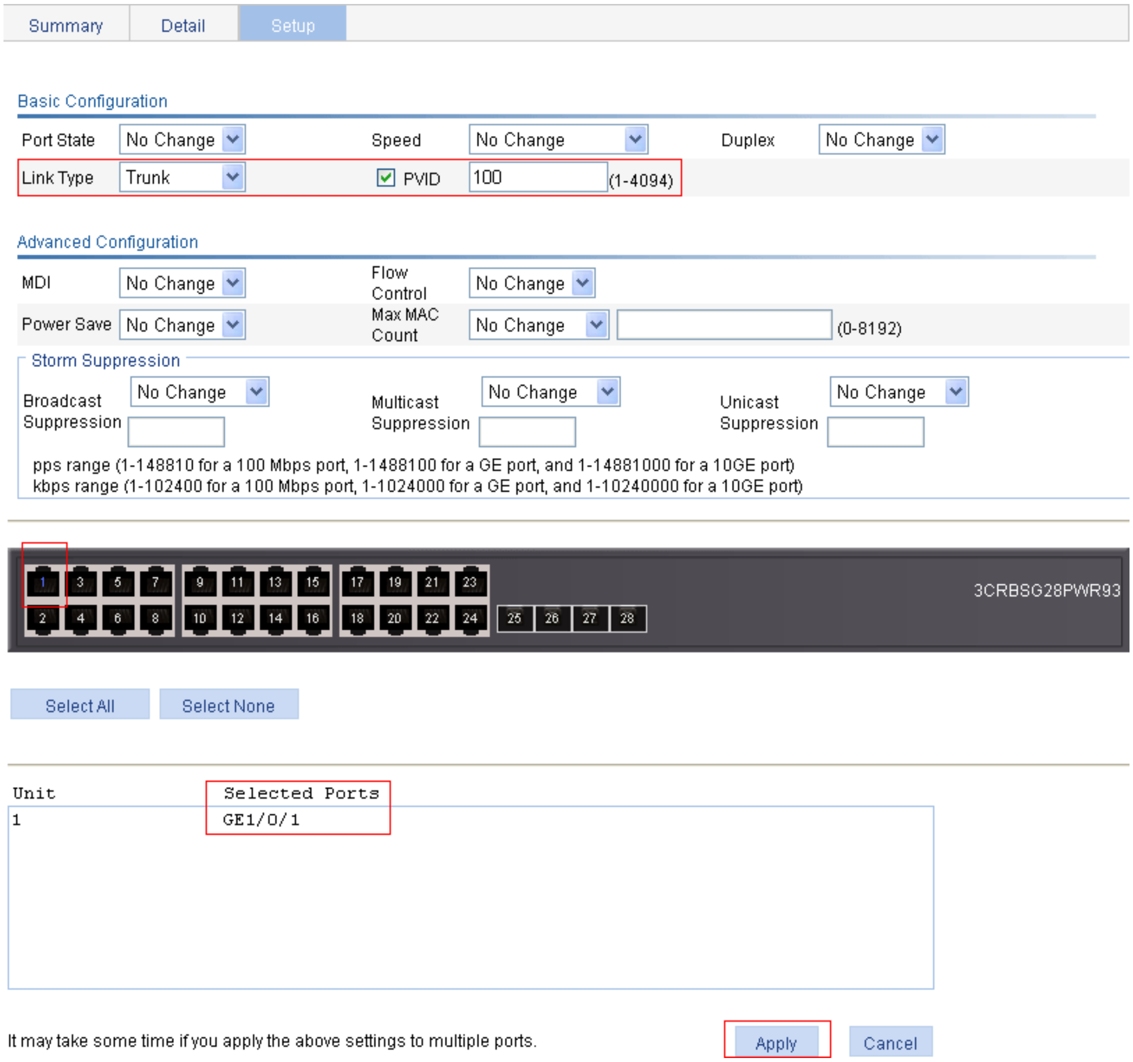
Configuration procedure

1) Configure Switch A

# Configure GigabitEthernet 1/0/1 as a trunk port and configure VLAN 100 as its default VLAN.

Select **Device** > **Port Management** from the navigation tree and click **Setup** to enter the page for setting ports, as shown in Figure 1-9.

Figure 1-9 Configure GigabitEthernet 1/0/1 as a trunk port and its PVID as 100



Basic Configuration

Port State	No Change	Speed	No Change	Duplex	No Change
Link Type	Trunk	☑ PVID	100 (1-4094)		

Advanced Configuration

MDI	No Change	Flow Control	No Change
Power Save	No Change	Max MAC Count	No Change (0-8192)

Storm Suppression

Broadcast Suppression	No Change	Multicast Suppression	No Change	Unicast Suppression	No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Unit	Selected Ports
1	GE1/0/1

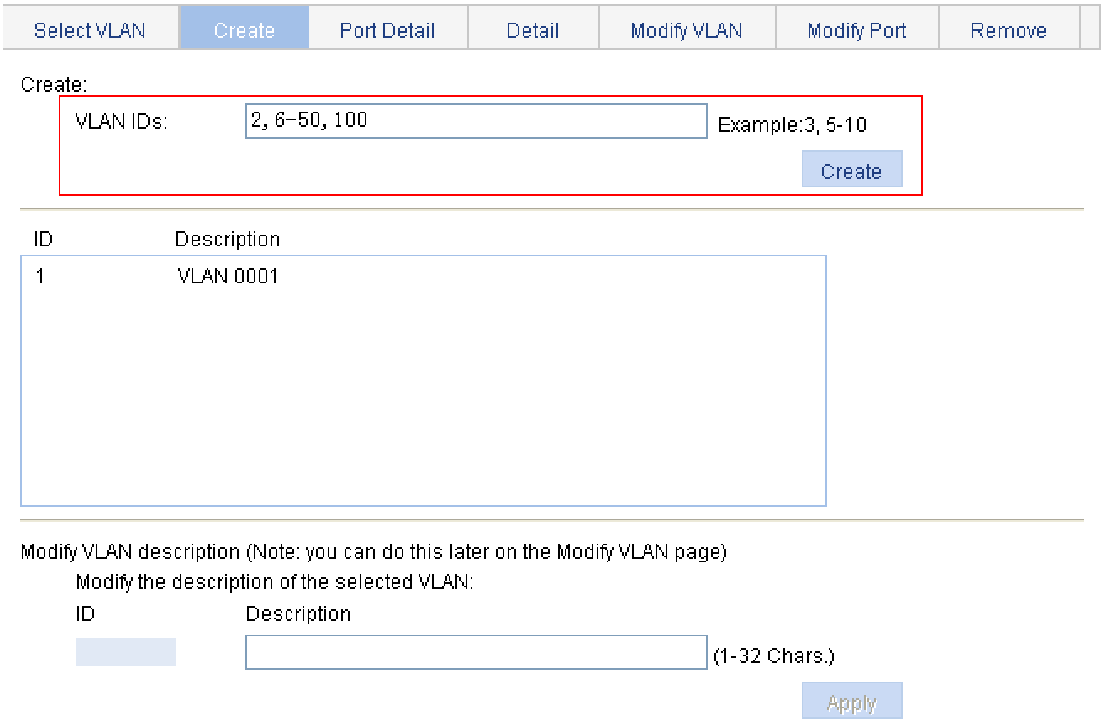
It may take some time if you apply the above settings to multiple ports.

- Select **Trunk** in the **Link Type** drop-down list.
- Select the **PVID** check box, and then type in PVID 100.
- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Click **Apply**.

# Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100.

Select **Network** > **VLAN** from the navigation tree and click **Create** to enter the page for creating VLANs, as shown in Figure 1-10.

Figure 1-10 Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100



Create:

VLAN IDs: 2, 6-50, 100 Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

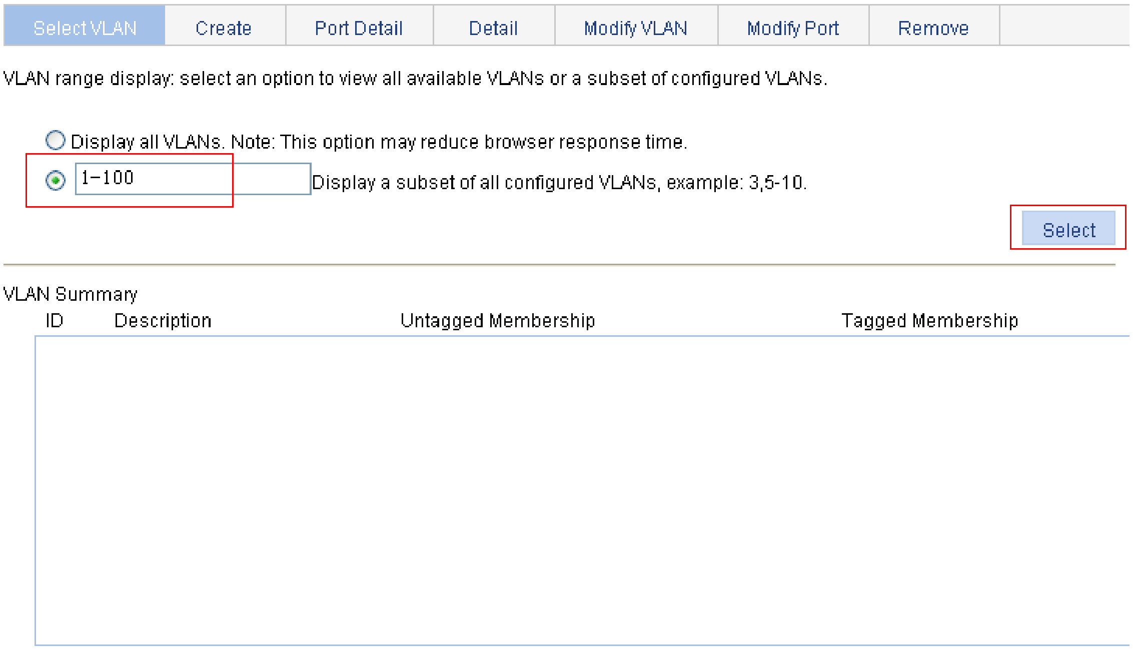
ID Description (1-32 Chars.)

- Type in VLAN IDs 2, 6-50, 100.
- Click **Apply**.

# Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member.

Click **Select VLAN** to enter the page for selecting VLANs, as shown in Figure 1-11.

Figure 1-11 Set a VLAN range



VLAN range display: select an option to view all available VLANs or a subset of configured VLANs.

○ Display all VLANs. Note: This option may reduce browser response time.

● 1-100 Display a subset of all configured VLANs, example: 3,5-10.

VLAN Summary

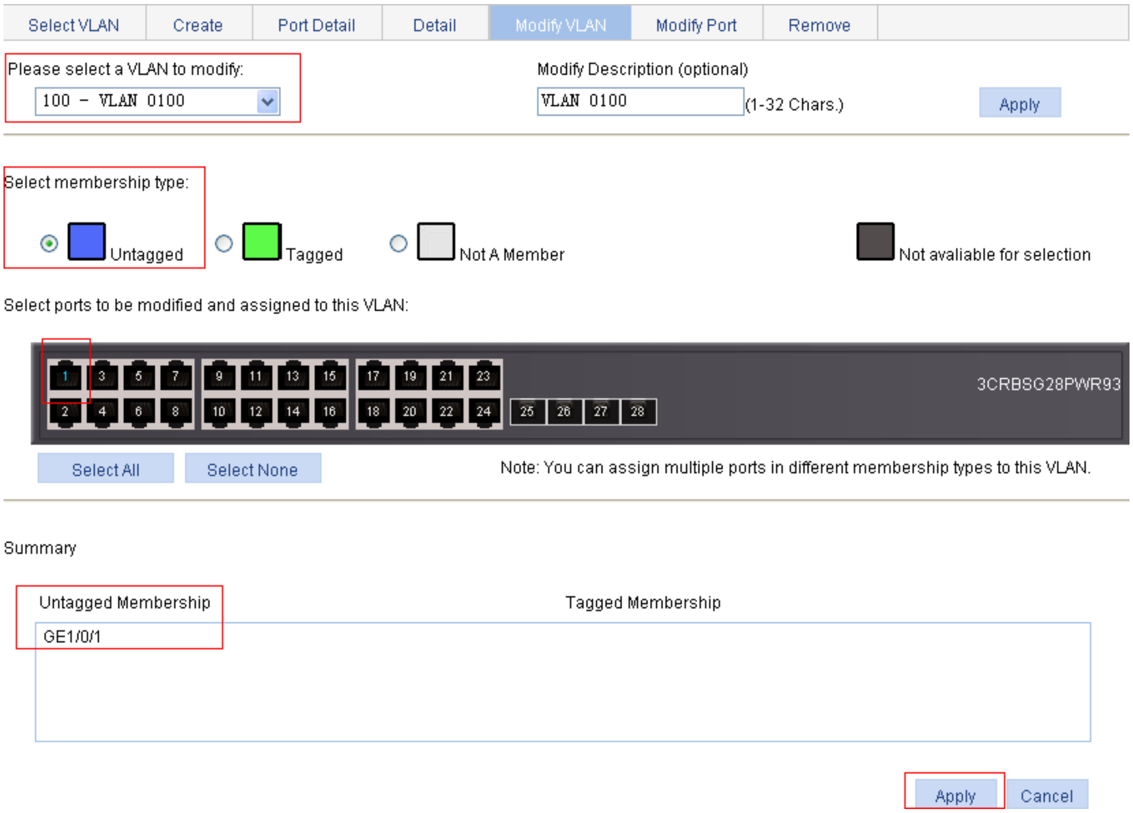
ID	Description	Untagged Membership	Tagged Membership

- Select the radio button before **Display a subnet of all configured VLANs** and type 1-100 in the text box.

- Click **Select**.

Click **Modify VLAN** to enter the page for modifying the ports in a VLAN, as shown in Figure 1-12.

Figure 1-12 Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member



Please select a VLAN to modify: 100 – VLAN 0100

Modify Description (optional) VLAN 0100 (1-32 Chars.)

● Untagged ○ Tagged ○ Not A Member

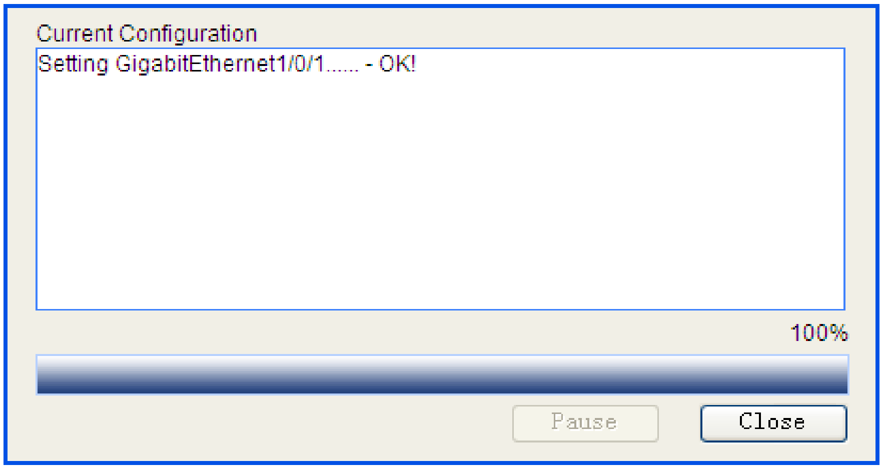
Note: You can assign multiple ports in different membership types to this VLAN.

Summary

Untagged Membership	Tagged Membership
GE1/0/1	

- Select **100 – VLAN 0100** in the **Please select a VLAN to modify:** drop-down list.
- Select the **Untagged** radio button.
- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-13.

Figure 1-13 Configuration progress dialog box



Current Configuration

```
Setting GigabitEthernet1/0/1...... - OK!
```

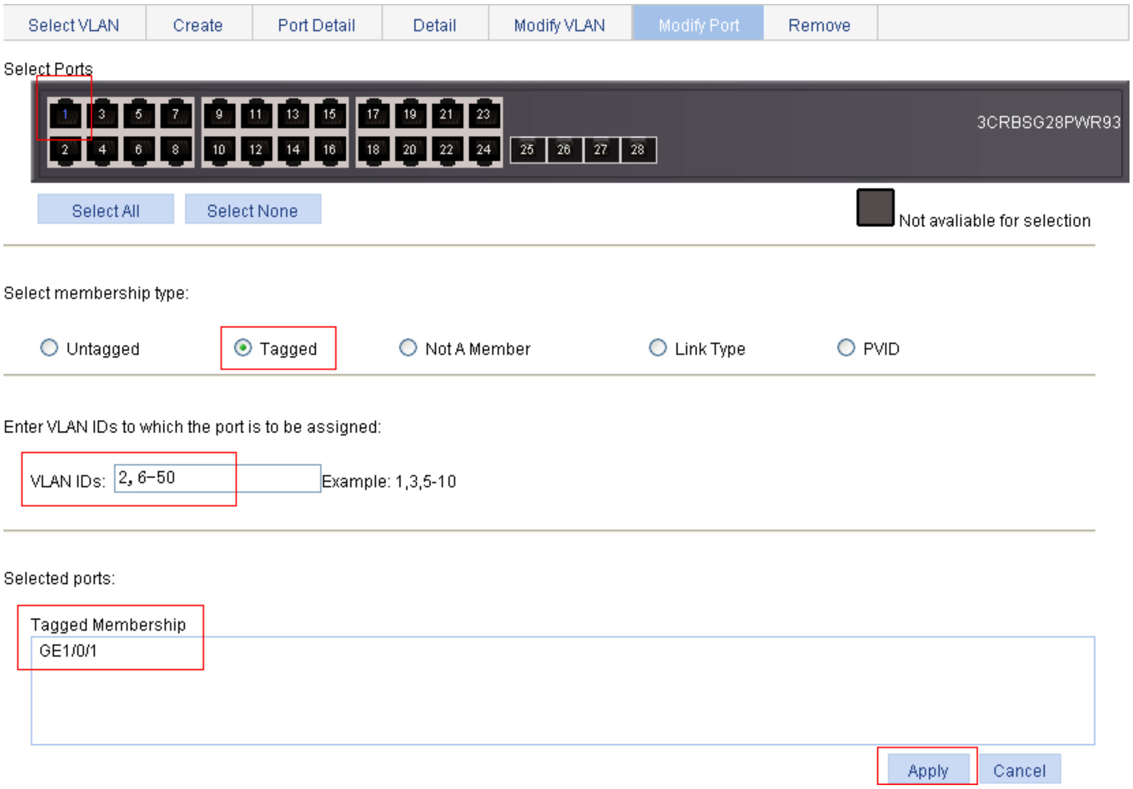
100%

- After the configuration process is complete, click **Close**.

# Assign GigabitEthernet 1/0/1 to VLAN2, and VLAN 6 through VLAN 50 as a tagged member.

Click **Modify Port** to enter the page for modifying the VLANs to which a port belongs, as shown in Figure 1-14.

Figure 1-14 Assign GigabitEthernet 1/0/1 to VLAN 2, and VLAN 6 through VLAN 50 as a tagged member



Select membership type:

○ Untagged ● Tagged ○ Not A Member ○ Link Type ○ PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: 2, 6–50 Example: 1,3,5-10

Selected ports:

Tagged Membership
GE1/0/1

- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Select the **Tagged** radio button.
- Type in VLAN IDs 2, 6-50.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

2) Configure Switch B

Configure Switch B as you configure Switch A.

Configuration Guidelines

When configuring VLAN, note that:

1) VLAN 1 is the default VLAN, which can be neither created nor removed manually.
2) Some VLANs are reserved for some special purposes. You can neither create nor remove them manually.
3) Dynamic VLANs cannot be removed on the page for removing VLANs.
4) You cannot remove a VLAN that has referenced a QoS policy.
5) You cannot directly remove a VLAN configured as a remote probe VLAN. To remove the VLAN, you must remove the remote probe VLAN configuration first.

Table of Contents

1 VLAN Interface Configuration

Overview

Note

For details about VLAN, refer to *VLAN Configuration*.

For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, VLAN interfaces are used.

VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface. You can assign the VLAN interface an IP address and specify it as the gateway of the VLAN to forward the traffic destined for an IP network segment different from that of the VLAN.

Configuring VLAN Interfaces

Configuration Task List

Perform the tasks in Table 1-1 to configure a VLAN interface:

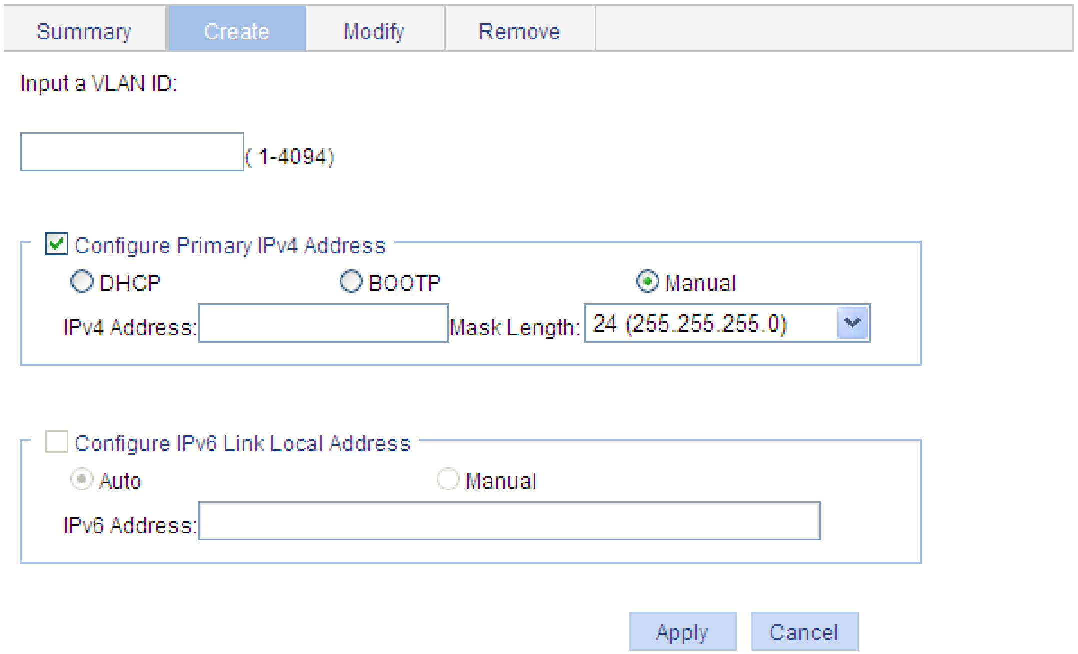
Table 1-1 VLAN interface configuration task list

Task	Remarks
Creating a VLAN Interface	Required Create a VLAN interface. You can select to assign an IPv4 address to the VLAN interface in this step or in a separate step. Before creating a VLAN interface for a VLAN, create the VLAN first (select **Network** > **VLAN**). For detailed configuration, refer to *VLAN Configuration*.
Modifying a VLAN Interface	Optional Assign an IPv4 address to the VLAN interface; shut down or bring up the VLAN interface.

Creating a VLAN Interface

Select **Network** > **VLAN Interface** from the navigation tree and click **Create** to enter the page for creating a VLAN interface, as shown in Figure 1-1.

Figure 1-1 The **Create** tab



Input a VLAN ID:

(1-4094)

☑ Configure Primary IPv4 Address

○ DHCP ○ BOOTP ● Manual

IPv4 Address: Mask Length: 24 (255.255.255.0)

□ Configure IPv6 Link Local Address

● Auto ○ Manual

IPv6 Address:

Table 1-2 describes the configuration items of creating a VLAN interface.

Table 1-2 Configuration items of creating a VLAN interface

Item		Description	
Input a VLAN ID:		Input the ID of the VLAN interface to be created. Before creating a VLAN interface, make sure that the corresponding VLAN exists.	
Configure Primary IPv4 Address	DHCP	Configure the way in which the VLAN interface gets an IPv4 address. Allow the VLAN interface to automatically obtain an IP address by selecting the **DHCP** or **BOOTP** option, or manually assign the VLAN interface an IP address by selecting the **Manual** option.	These items are available after you select the **Configure Primary IPv4 Address** check box.
	BOOTP		
	Manual		
	IPv4 Address	Configure an IPv4 address for the VLAN interface. This option is available after you select the **Manual** option.	
	Mask Length	Select the subnet mask length. This option is available after you select the **Manual** option.	

Return to VLAN interface configuration task list.

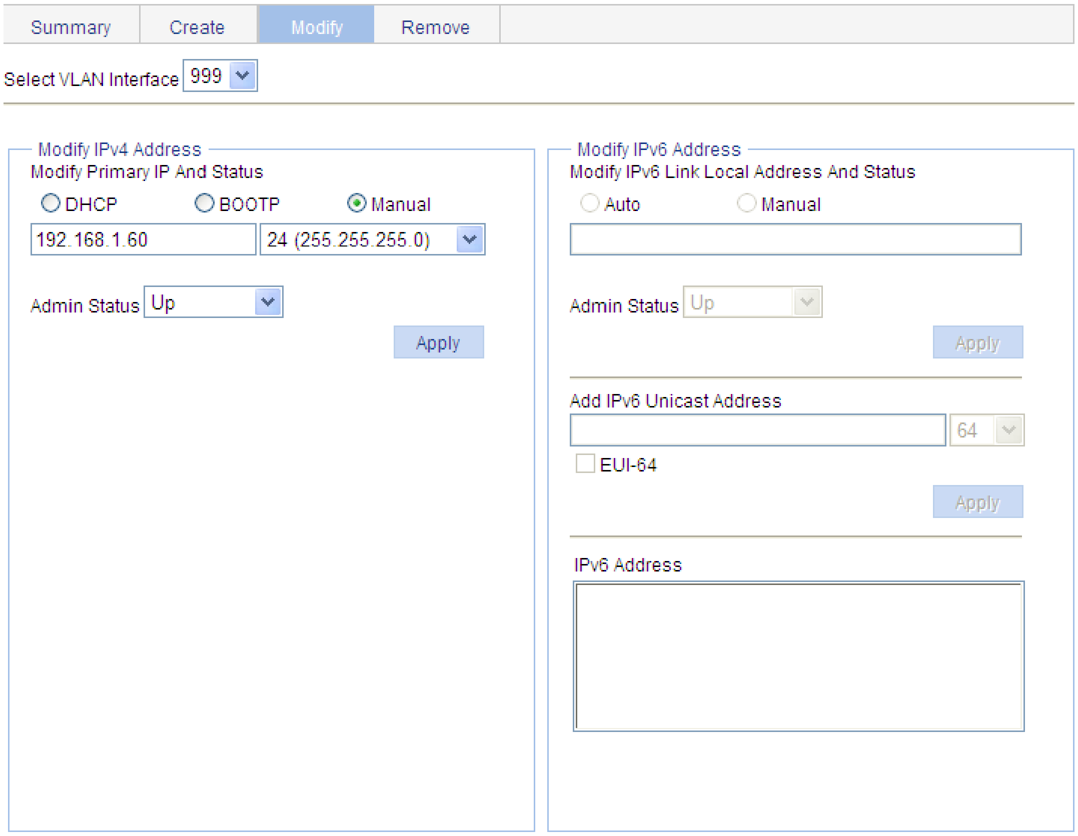
Modifying a VLAN Interface

Note

- After you modify the IPv4 address for a selected VLAN interface on the page for modifying VLAN interfaces, you need to click the correct **Apply** button to submit the modification.
- After you change the IP address of the VLAN interface you are using to log in to the device, you will be disconnected from the device. You can use the changed IP address to re-log in.

Select **Network** > **VLAN Interface** from the navigation tree and click **Modify** to enter the page for modifying a VLAN interface, as shown in Figure 1-2.

Figure 1-2 The **Modify** tab



Select VLAN Interface: 999

○ DHCP ○ BOOTP ● Manual

192.168.1.60 | 24 (255.255.255.0)

Admin Status: Up

○ Auto ○ Manual

Admin Status: Up

64

□ EUI-64

Table 1-3 describes the configuration items of modifying a VLAN interface.

Table 1-3 Configuration items of modifying a VLAN interface

Item	Description
Select VLAN Interface	Select the VLAN interface to be configured. The VLAN interfaces available for selection in the drop-down list are those created on the page for creating VLAN interfaces.

Item		Description
Modify IPv4 Address	DHCP	Configure the way in which the VLAN interface gets an IPv4 address. Allow the VLAN interface to automatically obtain an IP address by selecting the **DHCP** or **BOOTP** option, or manually assign the VLAN interface an IP address by selecting the **Manual** option.
	BOOTP	
	Manual	
	Admin Status	Select **Up** or **Down** in the **Admin Status** drop-down list to bring up or shut down the selected VLAN interface. When the VLAN interface fails, you can shut down and then bring up the VLAN interface, which may restore it. By default, a VLAN interface is down if all Ethernet ports in the VLAN are down; otherwise, the VLAN interface is up. **Highlight** • *The current VLAN interface state in the* ***Modify IPv4 Address*** *frames changes as the VLAN interface state is modified in the* ***Admin Status*** *drop-down list.* • *The state of each port in the VLAN is independent of the VLAN interface state.*

Return to VLAN interface configuration task list.

Table of Contents

1 Voice VLAN Configuration

Overview

A voice VLAN is dedicated to voice traffic. After assigning the ports connecting to voice devices to a voice VLAN, you can configure quality of service (QoS) parameters for the voice traffic, thus improving transmission priority and ensuring voice quality.

A device determines whether a received packet is a voice packet by checking its source MAC address. If the source MAC address of a received packet matches an organizationally unique identifier (OUI) in the voice device OUI list (referred to as the OUI list in this document) maintained by the switch, the packet is regarded as a voice packet.

You can add OUI addresses to the OUI list maintained by the device or use the default OUI list shown in Table 1-1 for voice traffic identification.

Table 1-1 The default OUI list

Number	OUI Address	Vendor
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Note

- Generally, an OUI is the first 24 bits of a MAC address (in binary format). It is a globally unique identifier assigned to a vendor by the IEEE. In this document, however, OUI addresses are used by the system to determine whether received packets are voice packets and they are the results of the AND operation of a MAC address and a mask. For details, see Adding OUI Addresses to the OUI List.
- You can remove default OUI addresses and if needed, add them to the OUI list after their removal.

Voice VLAN Assignment Modes

A port connected to a voice device, an IP phone for example, can be assigned to a voice VLAN in one of these two modes: Automatic mode and manual mode. Ports on a same device can be assigned to VLANs in different modes.

When untagged packets are received from an IP phone:

- In automatic mode, the system matches the source MAC addresses in the untagged packets sent by the IP phone upon its power-on against the OUI list. If a match is found, the system automatically assigns the receiving port to a voice VLAN, issues ACL rules and configures the packet precedence. You can configure an aging timer for the voice VLAN. The system will remove the port from the voice VLAN when the aging timer expires if no voice packet is received on the port during the aging timer. Assigning ports to and removing ports from a voice VLAN are automatically performed.
- In manual mode, you need to assign the port to a voice VLAN manually. Then, the system matches the source MAC addresses in the packets against the OUI addresses. If a match is found, the system issues ACL rules and configures the packet precedence. In this mode, assigning ports to and removing ports from a voice VLAN are performed manually.

In both modes, tagged packets are forwarded according to their tags.

The following table lists the relationships between the voice assignment VLAN mode, the voice traffic type of an IP phone, and the port link type.

Table 1-2 Co-relation

Voice VLAN assignment mode	Voice traffic type	Port link type		
		Access	Trunk	Hybrid
Automatic mode	Tagged voice traffic	Not supported	Supported, but you must ensure that the default VLAN of the port has been created and is not the voice VLAN and the traffic of the default VLAN can pass through the port.	Supported, but you must ensure that the default VLAN of the port has been created and is not the voice VLAN and the traffic of the default VLAN can pass through the port tagged.
	Untagged voice traffic	Not supported	Not supported	Not supported
Manual mode	Tagged voice traffic	Not supported	Supported, but you must ensure that the default VLAN of the port has been created and is not the voice VLAN and the traffic of the default VLAN can pass through the port.	Supported, but you must ensure that the default VLAN of the port has been created and is not the voice VLAN and the traffic of the voice VLAN can pass through the port tagged.
	Untagged voice traffic	Supported, but you must configure the default VLAN of the port as the voice VLAN.	Supported, but you must configure the default VLAN of the port as the voice VLAN and configure the port to allow the traffic of the voice VLAN to pass through.	Supported, but you must configure the default VLAN of the port as the voice VLAN and configure the port to allow the traffic of the voice VLAN to pass through untagged.

Note

- If an IP phone sends tagged voice traffic and its access port is configured with 802.1X authentication and guest VLAN, you must assign different VLAN IDs for the voice VLAN, the default VLAN of the access port, and the 802.1X guest VLAN for the functions to operate normally.
- If an IP phone sends untagged voice traffic, to deliver the voice VLAN function, you must configure the default VLAN of the access port as the voice VLAN. In this case, 802.1X authentication function cannot take effect.

Security Mode and Normal Mode of Voice VLANs

A voice VLAN-enabled port can operate in security mode or normal mode depending on its inbound packet filtering mechanism.

- Normal mode: In this mode, both voice packets and non-voice packets are allowed to pass through a voice VLAN-enabled inbound port. When receiving a voice packet, the port forwards it without checking its source MAC address against the OUI addresses configured for the device. If the default VLAN of the port is the voice VLAN and the port works in manual VLAN assignment mode, the port forwards all received untagged packets in the voice VLAN. In normal mode, the voice VLANs are vulnerable to traffic attacks. Vicious users can forge a large amount of voice packets and send them to voice VLAN-enabled ports to consume the voice VLAN bandwidth, affecting normal voice communication.
- Security mode: In this mode, only voice packets whose source MAC addresses comply with the recognizable OUI addresses can pass through the voice VLAN-enabled inbound port, while all other packets are dropped.

In a safe network, you can configure the voice VLANs to operate in normal mode, thus reducing the consumption of system resources due to source MAC addresses checking.

It is recommended not to transmit both voice packets and non-voice packets in a voice VLAN. If you have to, first ensure that the voice VLAN security mode is disabled.

Table 1-3 How a voice VLAN-enable port processes packets in security/normal mode

Voice VLAN working mode	Packet type	Packet processing mode
Security mode	Untagged packets	If the source MAC address of a packet matches an OUI address configured for the device, it is forwarded in the voice VLAN; otherwise, it is dropped.
	Packets carrying the voice VLAN tag	
	Packets carrying other tags	Forwarded or dropped depending on whether the port allows packets of these VLANs to pass through

Voice VLAN working mode	Packet type	Packet processing mode
Normal mode	Untagged packets	The port does not check the source MAC addresses of inbound packets. All types of packets can be transmitted in the voice VLAN.
	Packets carrying the voice VLAN tag	
	Packets carrying other tags	Forwarded or dropped depending on whether the port allows packets of these VLANs to pass through

Configuring the Voice VLAN

Configuration Task List

Before configuring the voice VLAN, you must create the corresponding VLAN and configure the link type of each port to be assigned to the VLAN. As VLAN 1 is the system-default VLAN, you do not need to create it; however, you cannot configure it as the voice VLAN. For information about port link types, refer to *Port Management Configuration*.

Configuring voice VLAN on a port in automatic voice VLAN assignment mode

Perform the tasks described in Table 1-4 to configure the voice VLAN function on a port working in automatic voice VLAN assignment mode.

Table 1-4 Voice VLAN configuration task list for a port in automatic voice VLAN assignment mode

Task	Remarks
Configuring Voice VLAN Globally	Optional Configure the voice VLAN to operate in security mode and configure the aging timer
Configuring Voice VLAN on a Port	Required Configure the voice VLAN assignment mode of a port as automatic and enable the voice VLAN function on the port. By default, the voice VLAN assignment mode of a port is automatic, and the voice VLAN function is disabled on a port.
Adding OUI Addresses to the OUI List	Optional The system supports up to 16 OUI addresses. By default, the system is configured with seven OUI addresses, as shown in Table 1-1.

Configuring voice VLAN on a port working in manual voice VLAN assignment mode

Perform the tasks described in Table 1-5 to configure the voice VLAN function on a port working in manual voice VLAN assignment mode.

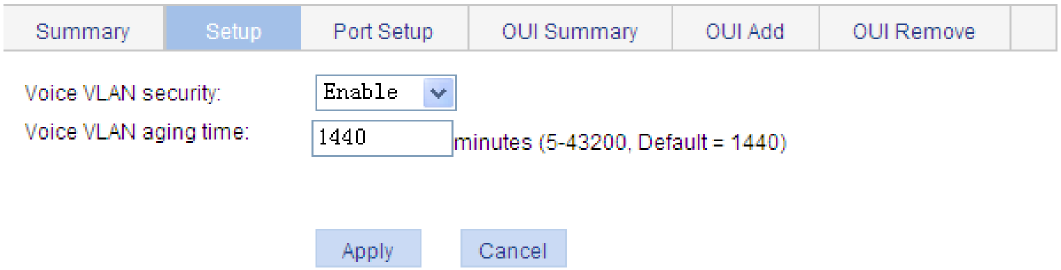
Table 1-5 Configuration task list for a port in manual voice VLAN assignment mode

Task	Remarks
Configuring Voice VLAN Globally	Optional Configure the voice VLAN to operate in security mode and configure the aging timer.
Assigning the port to the voice VLAN	Required Note that after an access port is assigned to the voice VLAN, the voice VLAN automatically becomes the default VLAN of the access port. For details, refer to *VLAN Configuration*.
Configuring the Voice VLAN as the Default VLAN of a Hybrid or Trunk Port	Optional This task is required if the incoming voice traffic is untagged and the link type of the receiving port is trunk or hybrid. If the incoming voice traffic is tagged, do not perform this task. For details, refer to *Port Management Configuration*.
Configuring Voice VLAN on a Port	Required Configure the voice VLAN assignment mode of a port as manual and enable voice VLAN on the port. By default, the voice VLAN assignment mode of a port is automatic, and voice VLAN is disabled on a port.
Adding OUI Addresses to the OUI List	Optional You can configure up to 16 OUI addresses. By default, the system is configured with the seven OUI addresses shown in Table 1-1.

Configuring Voice VLAN Globally

Select **Network** > **Voice VLAN** from the navigation tree, and click the **Setup** tab on the displayed page to enter the page shown in Figure 1-1.

Figure 1-1 Configure voice VLAN



Voice VLAN security: Enable

Voice VLAN aging time: 1440 minutes (5-43200, Default = 1440)

Table 1-6 describes the global voice VLAN configuration items.

Table 1-6 Global voice VLAN configuration items

Item	Description
Voice VLAN security	Select **Enable** or **Disable** in the drop-down list to enable or disable the voice VLAN security mode. By default, the voice VLANs operate in security mode.

Item	Description
Voice VLAN aging time	Set the voice VLAN aging timer. The voice VLAN aging timer setting only applies to a port in automatic voice VLAN assignment mode. The voice VLAN aging timer starts as soon as the port is assigned to the voice VLAN. If no voice packet has been received before the timer expires, the port is removed from the voice VLAN.

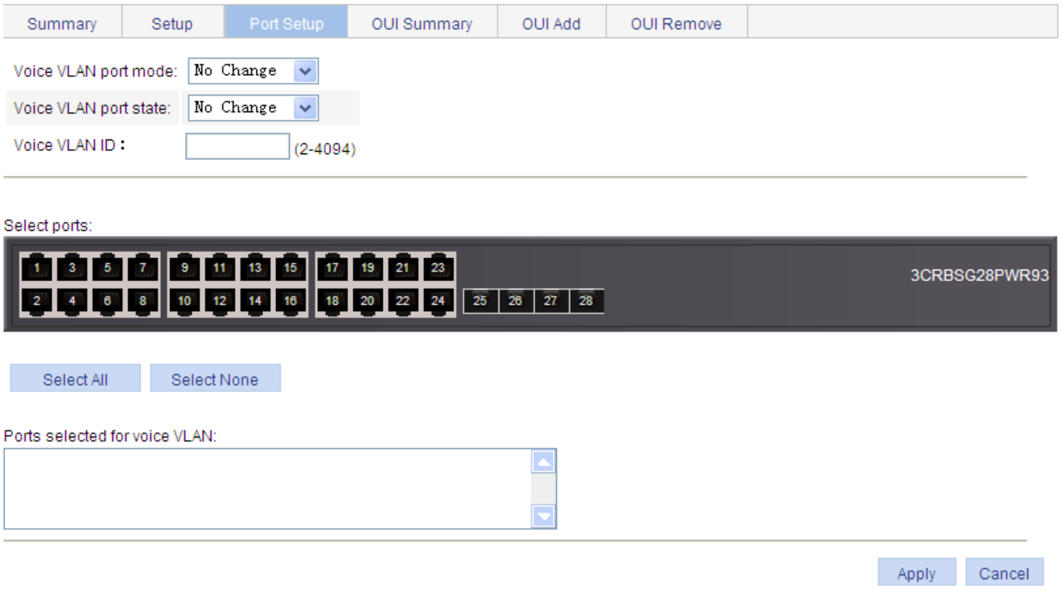
Return to Configuring voice VLAN on a port in automatic voice VLAN assignment mode.

Return to Configuring voice VLAN on a port working in manual voice VLAN assignment mode.

Configuring Voice VLAN on a Port

Select **Network** > **Voice VLAN** from the navigation tree, and click the **Port Setup** tab on the displayed page to enter the page shown in Figure 1-2.

Figure 1-2 Configure voice VLAN on a port



Voice VLAN port mode: No Change

Voice VLAN port state: No Change

Voice VLAN ID : (2-4094)

Select ports:

Ports selected for voice VLAN:

Table 1-7 describes the configuration items of configuring voice VLAN for a port.

Table 1-7 Configuration items of configuring Voice VLAN for a port

Item	Description
Voice VLAN port mode	Set the voice VLAN assignment mode of a port to: • Auto, that is, automatic voice VLAN assignment mode • Manual, that is, manual voice VLAN assignment mode
Voice VLAN port state	Select **Enable** or **Disable** in the drop-down list to enable or disable the voice VLAN function on the port.
Voice VLAN ID	Set the voice VLAN ID. This option is available when the voice VLAN port state is set to Enable. **Highlight** *The device supports only one voice VLAN. Only an existing static VLAN can be configured as the voice VLAN.*

Item	Description
Select Ports	Select the port on the chassis front panel. You can select multiple ports to configure them in bulk. The numbers of the selected ports will be displayed in the **Ports selected for voice VLAN** text box. **Highlight** *To set the voice VLAN assignment mode of a port to automatic, you must ensure that the link type of the port is trunk or hybrid, and that the port does not belong to the voice VLAN.*

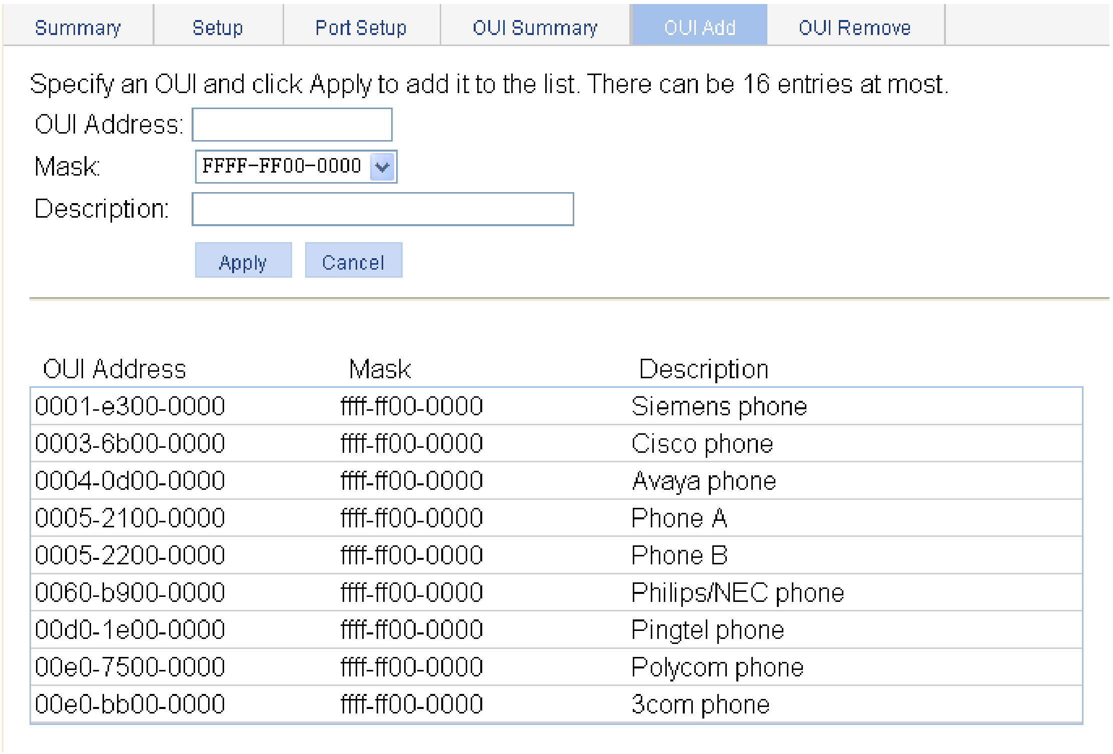
Return to Configuring voice VLAN on a port in automatic voice VLAN assignment mode.

Return to Configuring voice VLAN on a port working in manual voice VLAN assignment mode.

Adding OUI Addresses to the OUI List

Select **Network** > **Voice VLAN** from the navigation tree and click the **OUI Add** tab on the displayed page to enter the page shown in Figure 1-3.

Figure 1-3 Add OUI addresses to the OUI list



Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address:

Mask: FFFF-FF00-0000

Description:

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0005-2100-0000	ffff-ff00-0000	Phone A
0005-2200-0000	ffff-ff00-0000	Phone B
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

Table 1-8 describes the OUI list configuration items.

Table 1-8 OUI list configuration items

Item	Description
OUI Address	Set the source MAC address of voice traffic.
Mask	Set the mask length of the source MAC address.

Item	Description
Description	Set the description of the OUI address entry.

Return to Configuring voice VLAN on a port in automatic voice VLAN assignment mode.

Return to Configuring voice VLAN on a port working in manual voice VLAN assignment mode.

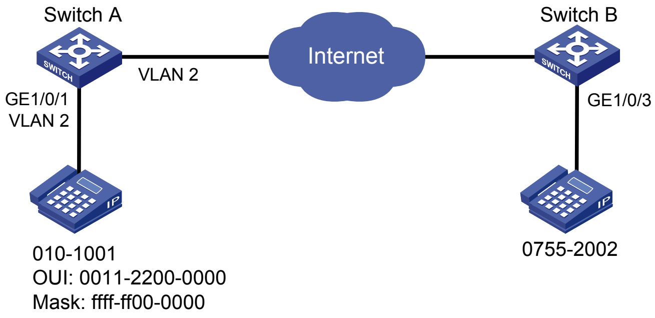
Voice VLAN Configuration Examples

Configuring Voice VLAN on a Port in Automatic Voice VLAN Assignment Mode

Network requirements

- Configure VLAN 2 as the voice VLAN allowing only voice traffic to pass through.
- The IP phone connected to hybrid port GigabitEthernet 1/0/1 sends untagged voice traffic.
- GigabitEthernet 1/0/1 operates in automatic VLAN assignment mode. Set the voice VLAN aging timer to 30 minutes.
- Configure GigabitEthernet 1/0/1 to allow voice packets whose source MAC addresses match the OUI addresses specified by OUI address 0011-2200-0000 and mask ffff-ff00-0000. The description of the OUI address entry is **test**.

Figure 1-4 Network diagram for configuring voice VLAN on a port working in automatic voice VLAN assignment mode

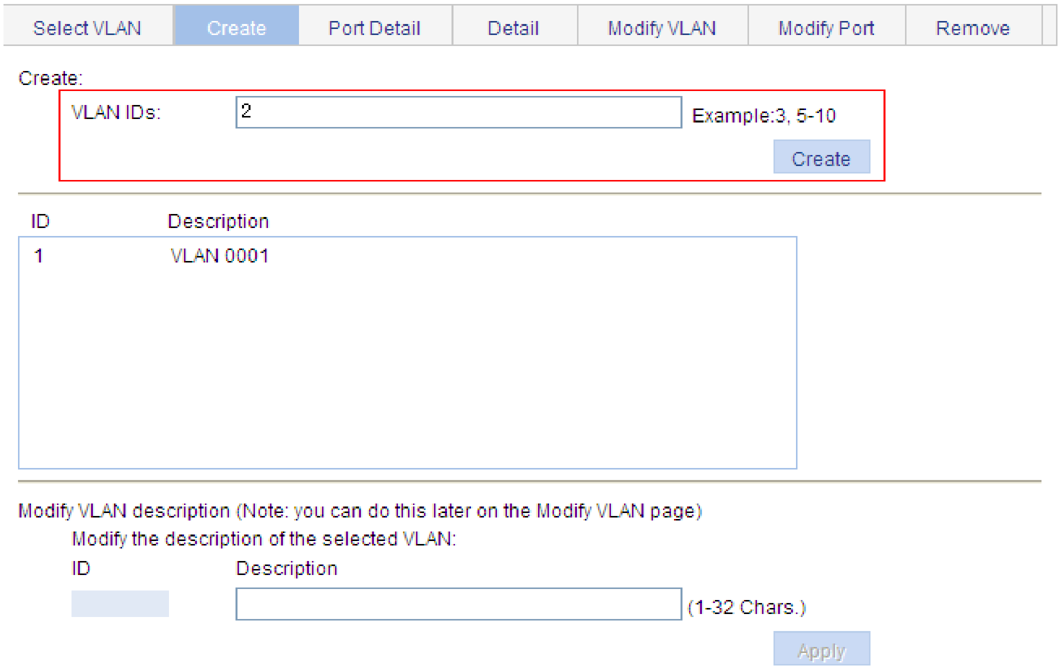


Configuration procedure

# Create VLAN 2.

- Select **Network** > **VLAN** from the navigation tree, and click **Create** on the displayed page to enter the page shown in Figure 1-5.

Figure 1-5 Create VLAN 2



Create:

VLAN IDs: 2 Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID Description

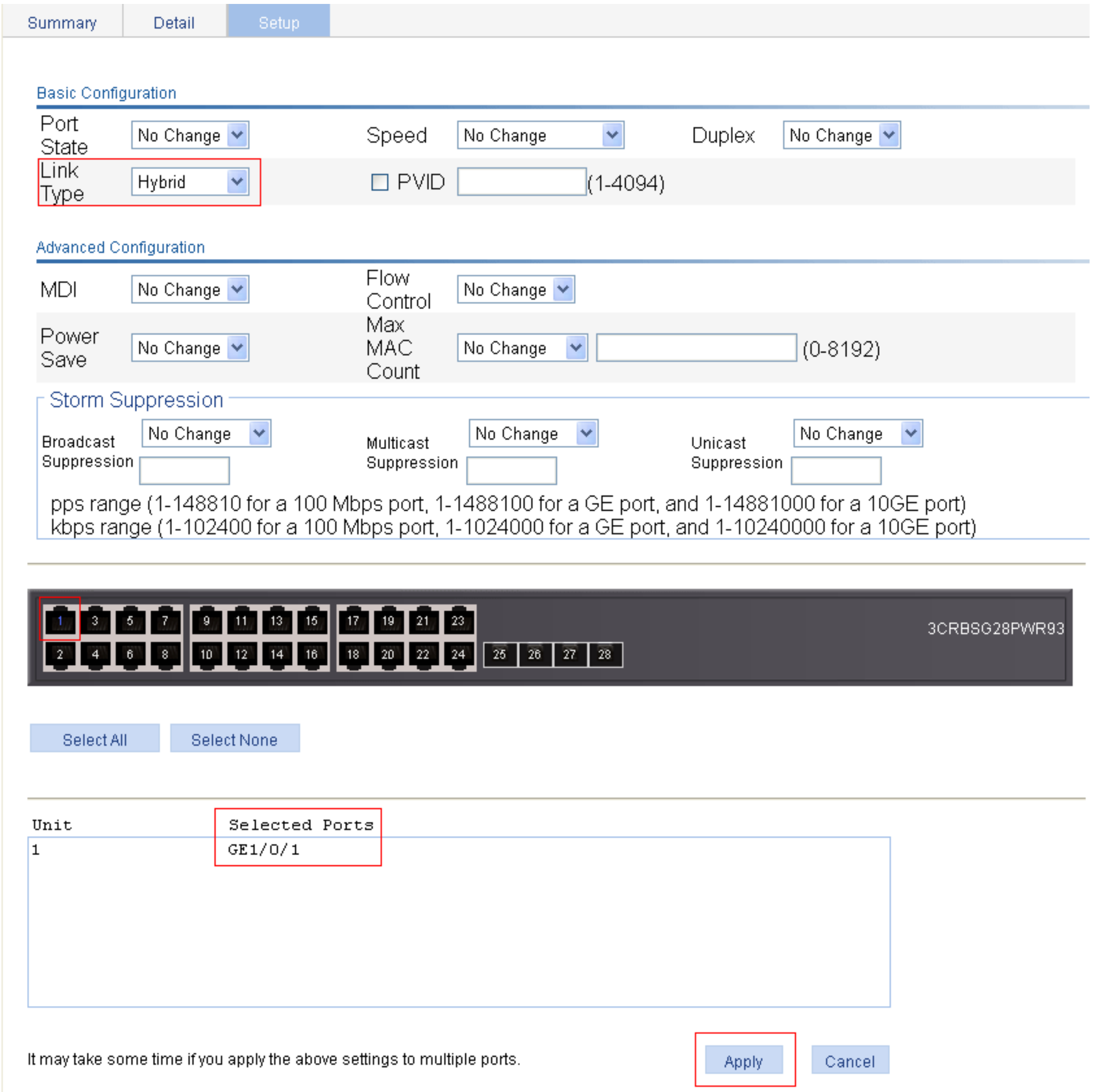
(1-32 Chars.)

- Type in VLAN ID 2.
- Click **Create**.

# Configure GigabitEthernet 1/0/1 as a hybrid port.

- Select **Device** > **Port Management** from the navigation tree, and click **Setup** on the displayed page to enter the page shown in Figure 1-6.

Figure 1-6 Configure GigabitEthernet 1/0/1 as a hybrid port



Basic Configuration

Port State: No Change
Speed: No Change
Duplex: No Change
Link Type: Hybrid
□ PVID (1-4094)

Advanced Configuration

MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)

Storm Suppression

Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Unit	Selected Ports
1	GE1/0/1

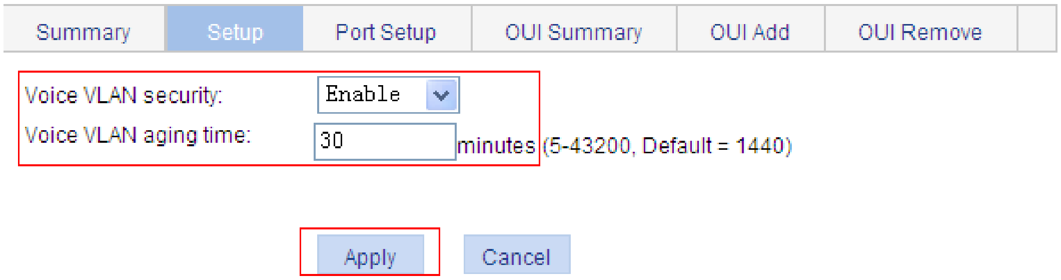
It may take some time if you apply the above settings to multiple ports.

- Select **Hybrid** from the **Link Type** dropdown list.
- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Click **Apply**.

# Configure the voice VLAN function globally.

- Select **Network** > **Voice VLAN** from the navigation tree and click the **Setup** tab on the displayed page to enter the page shown in Figure 1-7.

Figure 1-7 Configure the voice VLAN function globally



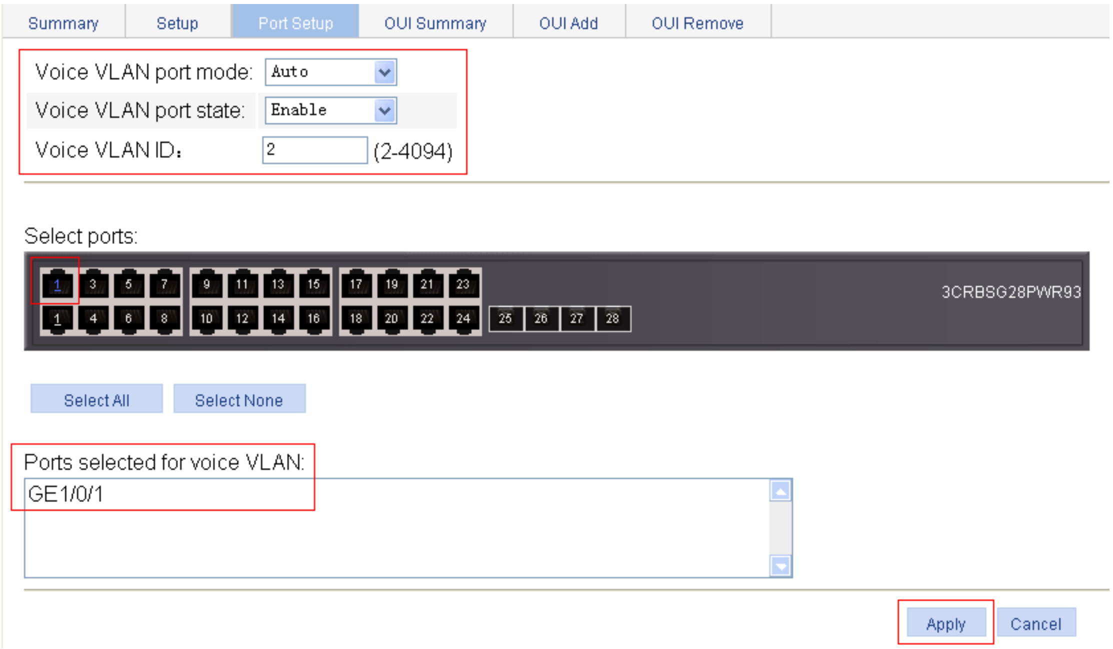
Voice VLAN security: Enable
Voice VLAN aging time: 30 minutes (5-43200, Default = 1440)

- Select **Enable** in the **Voice VLAN security** drop-down list. (You can skip this step, because the voice VLAN security mode is enabled by default)
- Set the voice VLAN aging timer to 30 minutes.
- Click **Apply**.

# Configure voice VLAN on GigabitEthernet 1/0/1.

- Click the **Port Setup** tab to enter the page shown in Figure 1-8.

Figure 1-8 Configure voice VLAN on GigabitEthernet 1/0/1



Voice VLAN port mode: Auto

Voice VLAN port state: Enable

Voice VLAN ID: 2 (2-4094)

Select ports:

Ports selected for voice VLAN:

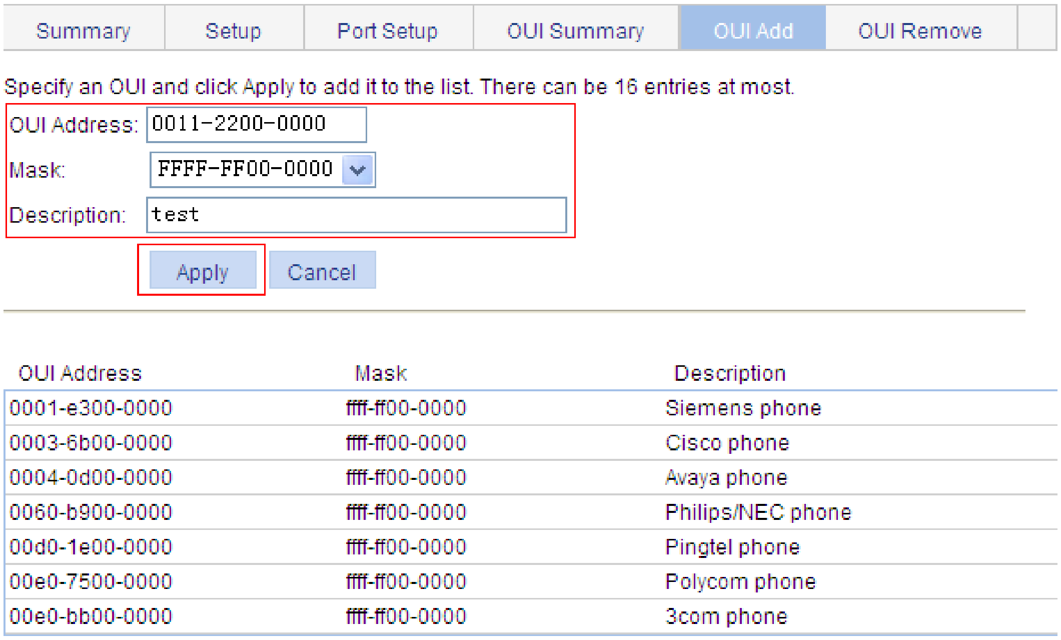
GE1/0/1

- Select **Auto** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type in voice VLAN ID 2.
- Select GigabitEthernet 1/0/1 on the chassis front panel.
- Click **Apply**.

# Add OUI addresses to the OUI list.

- Click the **OUI Add** tab to enter the page shown in Figure 1-9.

Figure 1-9 Add OUI addresses to the OUI list



Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address: 0011-2200-0000

Mask: FFFF-FF00-0000

Description: test

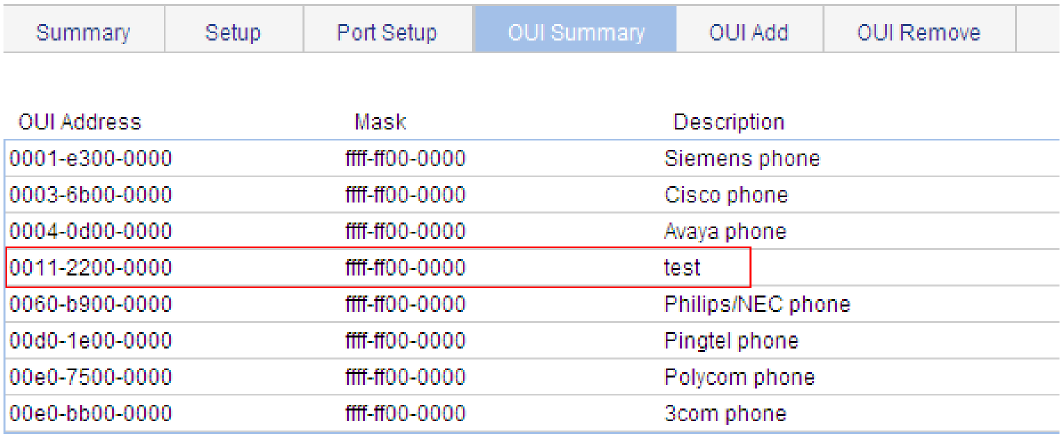
OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Type in OUI address **0011-2200-0000**.
- Select **FFFF-FF00-0000** in the **Mask** drop-down list.
- Type in description string **test**.
- Click **Apply**.

Verify the configuration

- When the configurations described above are completed, the **OUI Summary** tab is displayed by default, as shown in Figure 1-10. You can view the information about the newly-added OUI address.

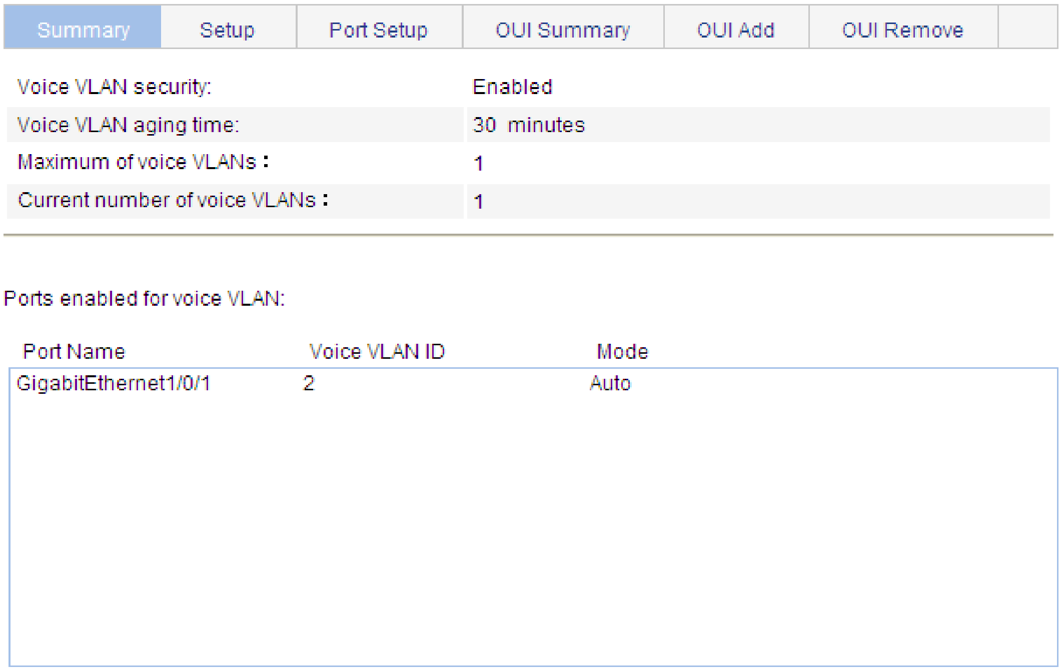
Figure 1-10 Current OUI list of the device



OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0011-2200-0000	ffff-ff00-0000	test
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Click the **Summary** tab to enter the page shown in Figure 1-11, where you can view the current voice VLAN information.

Figure 1-11 Current voice VLAN information



Voice VLAN security:	Enabled
Voice VLAN aging time:	30 minutes
Maximum of voice VLANs :	1
Current number of voice VLANs :	1

Ports enabled for voice VLAN:

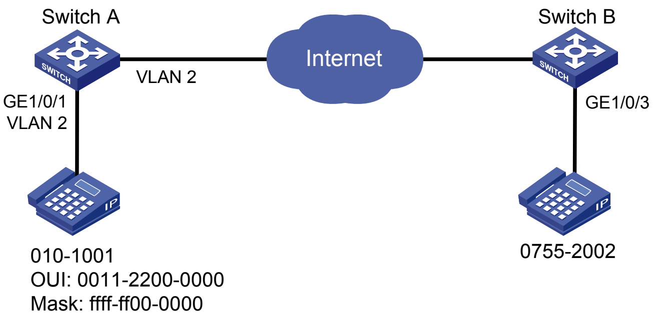
Port Name	Voice VLAN ID	Mode
GigabitEthernet1/0/1	2	Auto

Configuring a Voice VLAN on a Port in Manual Voice VLAN Assignment Mode

Network requirements

- Configure VLAN 2 as a voice VLAN that carries only voice traffic.
- The IP phone connected to hybrid port GigabitEthernet 1/0/1 sends untagged voice traffic.
- GigabitEthernet 1/0/1 operates in manual voice VLAN assignment mode and allows voice packets whose source MAC addresses match the OUI addresses specified by OUI address 0011-2200-0000 and mask ffff-ff00-0000 to pass through. The description of the OUI address entry is **test**.

Figure 1-12 Network diagram for voice VLAN configuration on a port in manual voice VLAN assignment mode

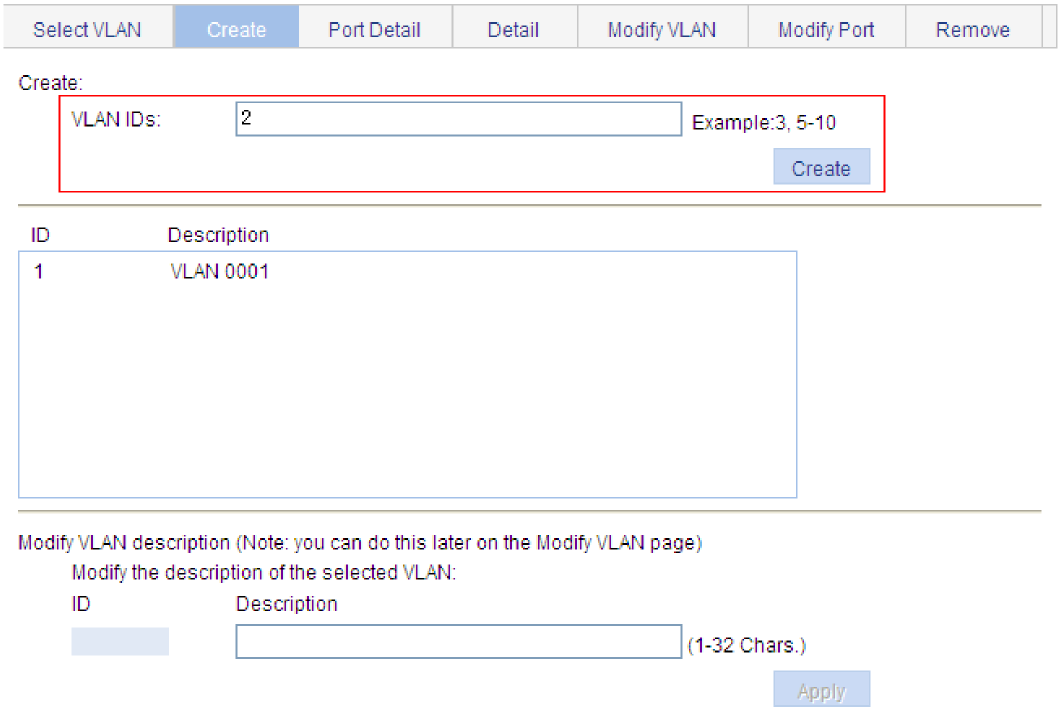


Configuration procedure

# Create VLAN 2.

- Select **Network** > **VLAN** from the navigation tree, and click **Create** on the displayed page to enter the page shown in Figure 1-13.

Figure 1-13 Create VLAN 2



Create:

VLAN IDs: 2 Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

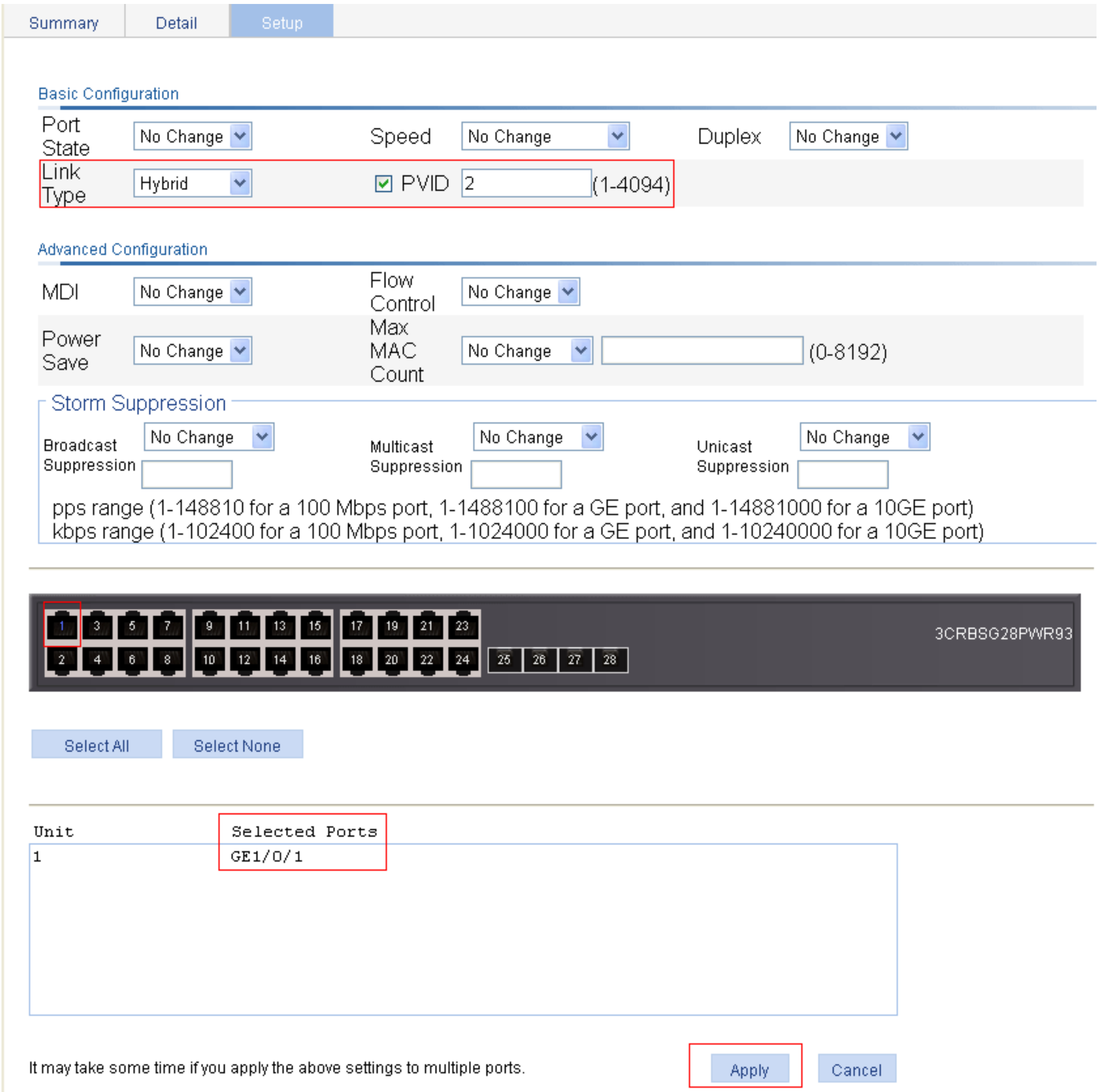
ID Description (1-32 Chars.)

- Type in VLAN ID 2.
- Click **Create**.

# Configure GigabitEthernet 1/0/1 as a hybrid port and configure its default VLAN as VLAN 2.

- Select **Device** > **Port Management** from the navigation tree, and click **Setup** on the displayed page to enter the page shown in Figure 1-14.

Figure 1-14 Configure GigabitEthernet 1/0/1 as a hybrid port



Port State: No Change
Speed: No Change
Duplex: No Change
Link Type: Hybrid
☑ PVID: 2 (1-4094)

MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)

Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Unit	Selected Ports
1	GE1/0/1

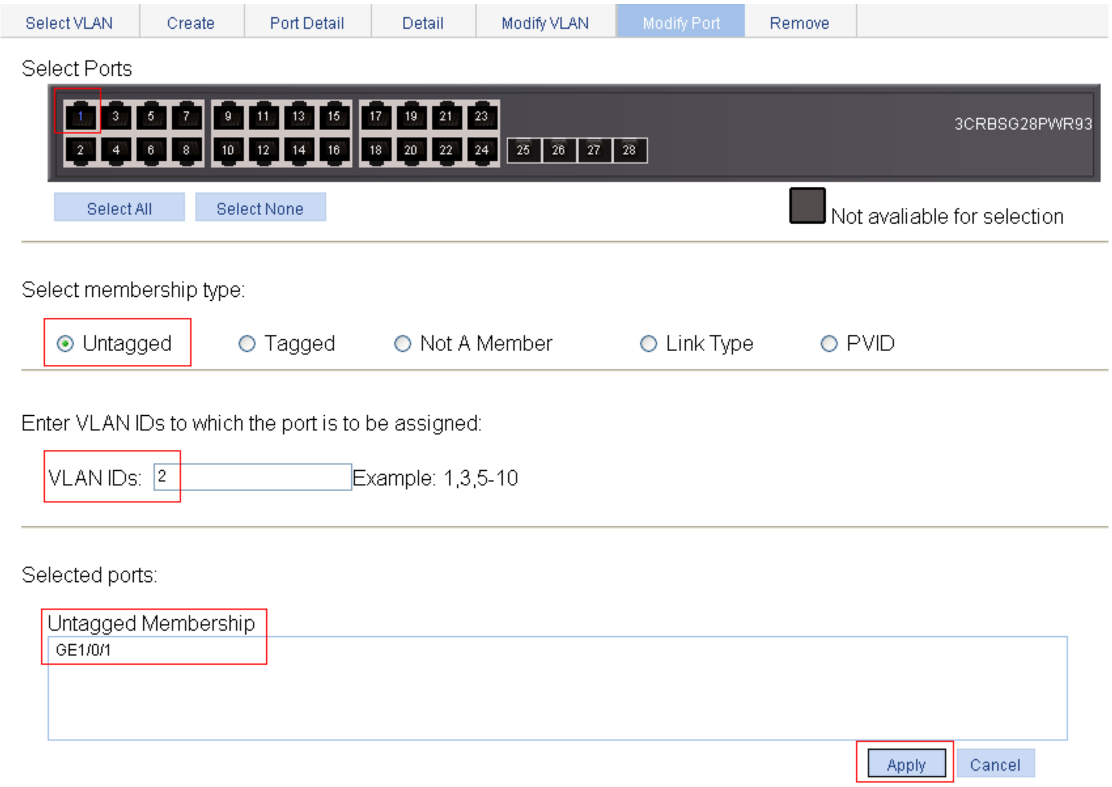
It may take some time if you apply the above settings to multiple ports.

- Select **Hybrid** from the **Link Type** dropdown list.
- Select the **PVID** option and type 2 in the text box.
- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Click **Apply**.

# Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member.

- Select **Network** > **VLAN** from the navigation tree, and click **Modify Port** on the displayed page to enter the page shown in Figure 1-15.

Figure 1-15 Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member



Select Ports

■ Not avaliable for selection

Select membership type:

● Untagged ○ Tagged ○ Not A Member ○ Link Type ○ PVID

Enter VLAN IDs to which the port is to be assigned:

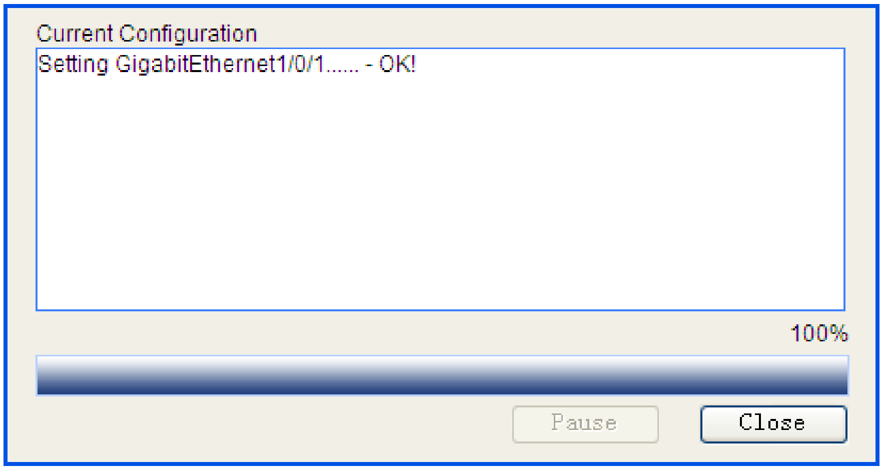
VLAN IDs: 2 Example: 1,3,5-10

Selected ports:

Untagged Membership
GE1/0/1

- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Select the **Untagged** option.
- Type in VLAN ID 2.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-16.

Figure 1-16 Configuration progress dialog box



Current Configuration

Setting GigabitEthernet1/0/1...... - OK!

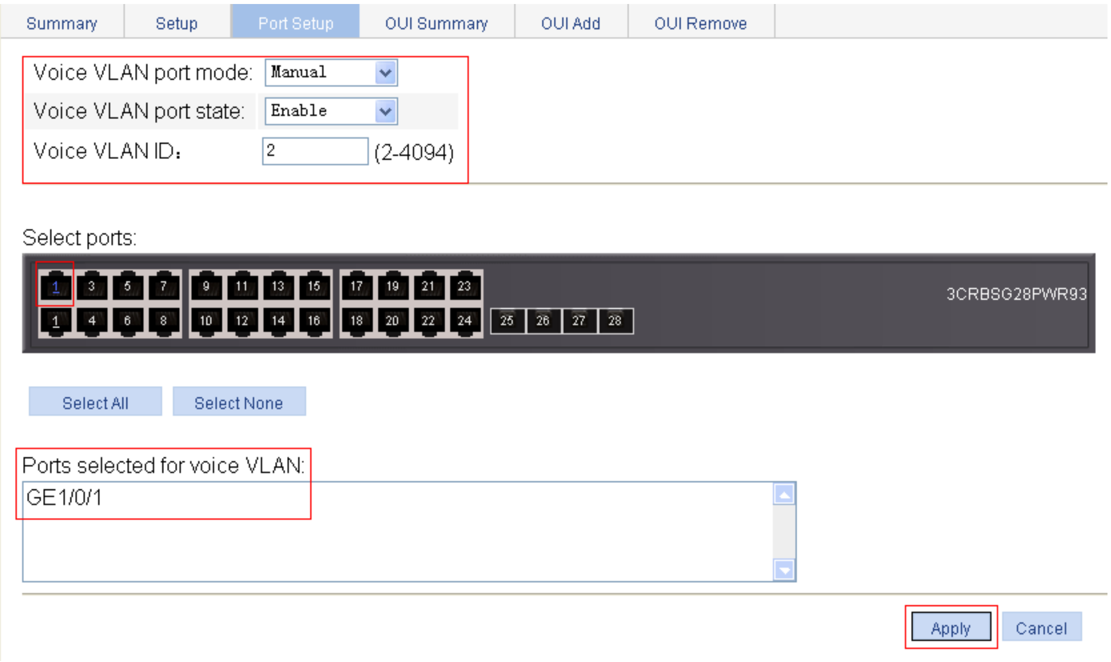
100%

- After the configuration process is complete, click **Close**.

# Configure voice VLAN on GigabitEthernet 1/0/1.

- Select **Network** > **Voice VLAN** from the navigation tree, and click **Port Setup** on the displayed page to enter the page shown in Figure 1-17.

Figure 1-17 Configure voice VLAN on GigabitEthernet 1/0/1



Voice VLAN port mode: Manual

Voice VLAN port state: Enable

Voice VLAN ID: 2 (2-4094)

Select ports:

Ports selected for voice VLAN:

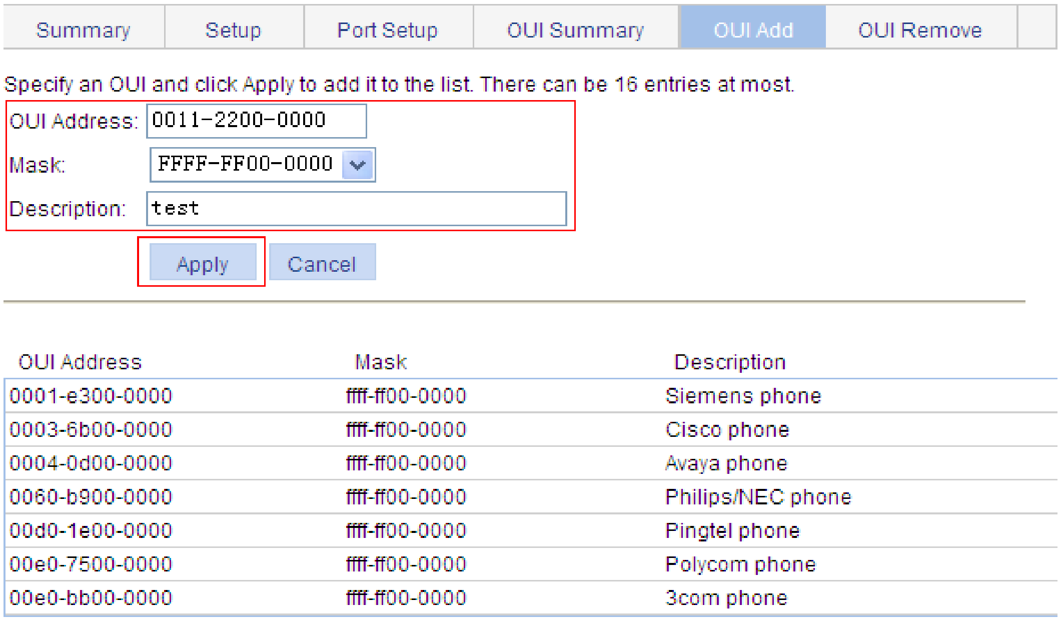
GE1/0/1

- Select **Manual** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type in voice VLAN ID 2.
- Select GigabitEthernet 1/0/1 on the chassis front panel.
- Click **Apply**.

# Add OUI addresses to the OUI list.

- Click the **OUI Add** tab to enter the page shown in Figure 1-18.

Figure 1-18 Add OUI addresses to the OUI list



Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address: 0011-2200-0000

Mask: FFFF-FF00-0000

Description: test

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

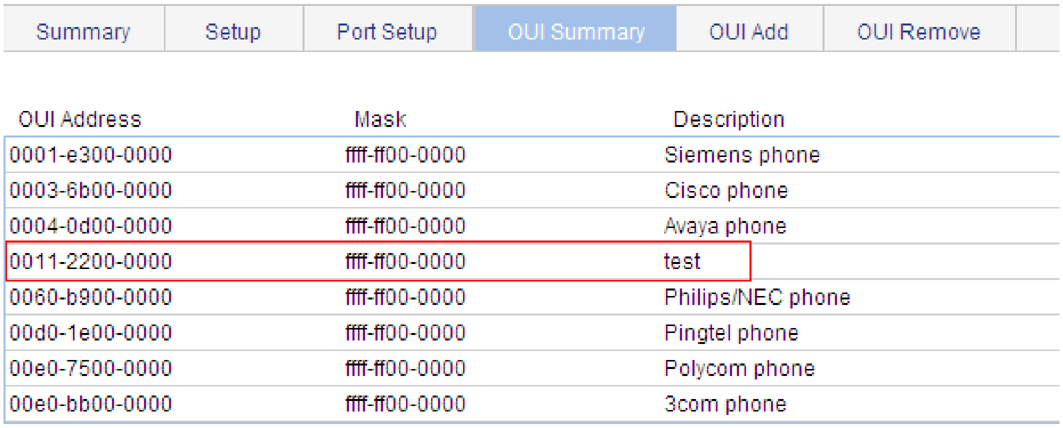
- Type in OUI address **0011-2200-0000**.
- Select **FFFF-FF00-0000** as the mask.

- Type in description string **test**.
- Click **Apply**.

Verify the configuration

- When the configurations described above are completed, the **OUI Summary** tab is displayed by default, as shown in Figure 1-19. You can view the information about the newly-added OUI address.

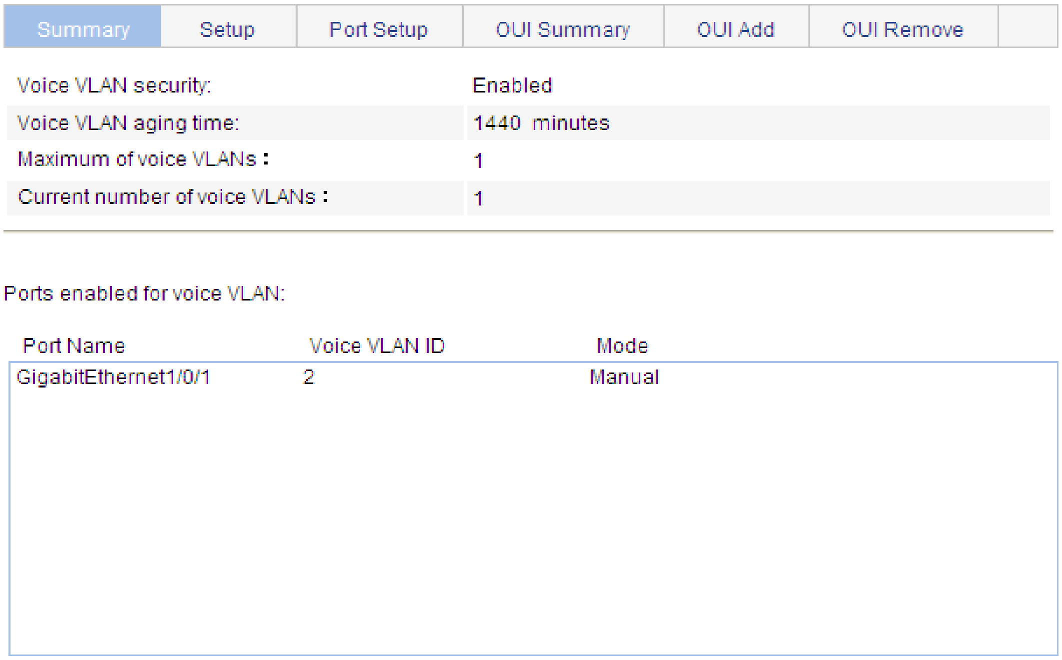
Figure 1-19 Current OUI list of the device



OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0011-2200-0000	ffff-ff00-0000	test
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Click the **Summary** tab to enter the page shown in Figure 1-20, where you can view the current voice VLAN information.

Figure 1-20 Current voice VLAN information



Voice VLAN security:	Enabled
Voice VLAN aging time:	1440 minutes
Maximum of voice VLANs :	1
Current number of voice VLANs :	1

Ports enabled for voice VLAN:

Port Name	Voice VLAN ID	Mode
GigabitEthernet1/0/1	2	Manual

Configuration Guidelines

When configuring the voice VLAN function, follow these guidelines:

- To remove a VLAN functioning as a voice VLAN, disable its voice VLAN function first.

- In automatic voice VLAN assignment mode, a hybrid port can process only tagged voice traffic. However, the protocol-based VLAN function requires hybrid ports to process untagged traffic. Therefore, if a VLAN is configured as the voice VLAN and a protocol-based VLAN at the same time, the protocol-based VLAN cannot be associated with the port.
- At present, only one VLAN is supported and only an existing static VLAN can be configured as the voice VLAN.
- If Link Aggregation Control Protocol (LACP) is enabled on a port, the voice VLAN function cannot be enabled on it.
- After you assign a port working in manual voice VLAN assignment mode to the voice VLAN, the voice VLAN takes effect.

Table of Contents

1 MAC Address Configuration

Note

- Currently, MAC address configurations related to interfaces only apply to Layer 2 Ethernet interfaces.
- This manual covers only the management of static and dynamic MAC address entries, not multicast MAC address entries.

Overview

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

The following is how your device learns a MAC address after it receives a frame from a port, port A for example:

1) Checks the frame for the source MAC address (MAC-SOURCE for example).
2) Looks up the MAC address table for an entry corresponding to the MAC address and do the following:

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

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

Note

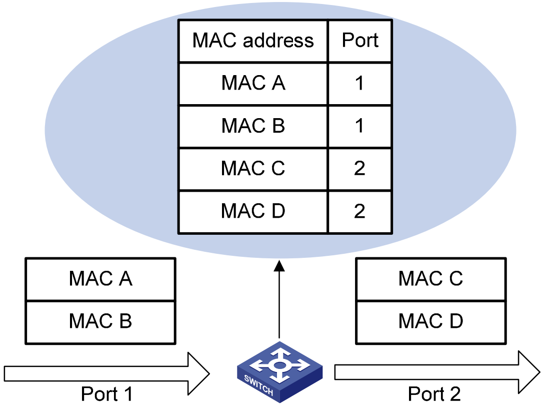
Dynamically learned MAC addresses cannot overwrite static MAC address entries, but the latter can overwrite the former.

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

- Unicast mode: If an entry matching the destination MAC address exists, the device forwards the frame directly from the sending port recorded in the entry.

- Broadcast mode: If the device receives a frame with the destination address being all Fs, or no entry matches the destination MAC address, the device broadcasts the frame to all the ports except the receiving port.

Figure 1-1 MAC address table of the device



MAC address	Port
MAC A	1
MAC B	1
MAC C	2
MAC D	2

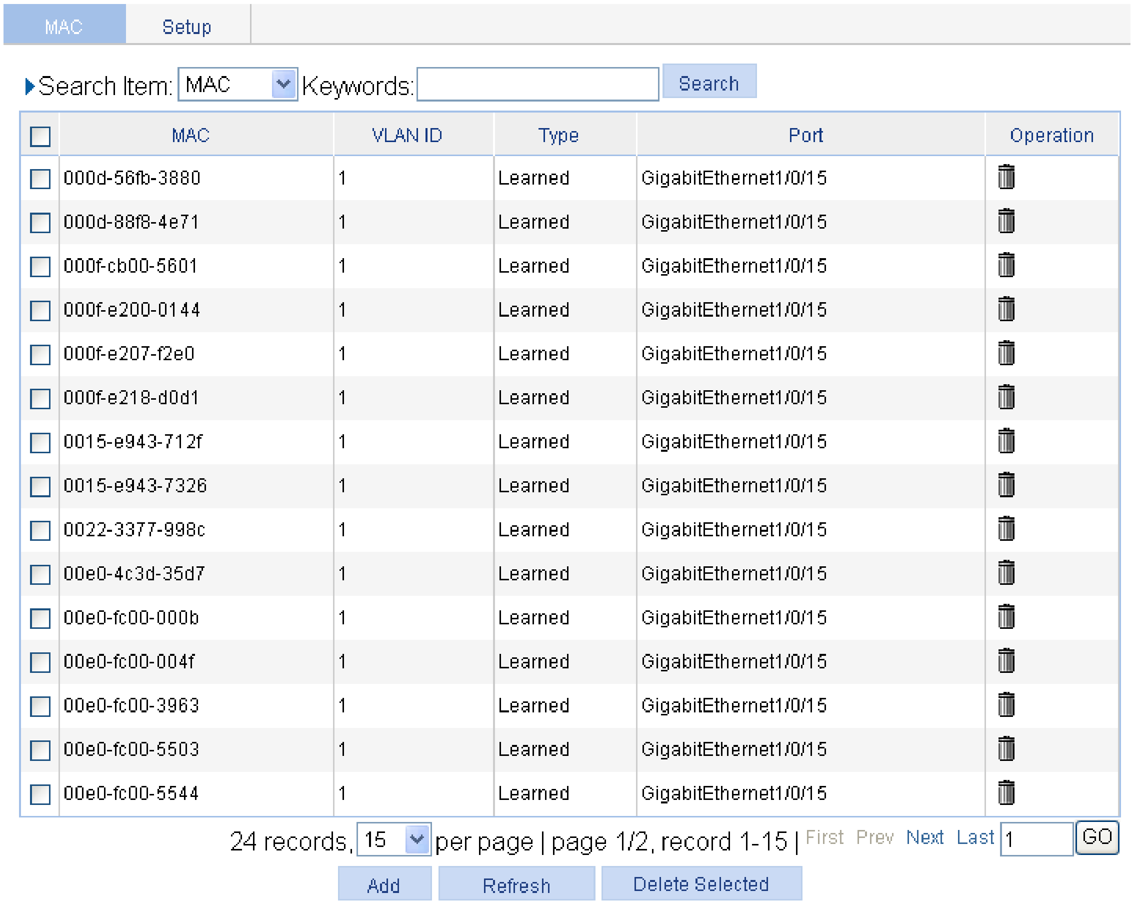
Configuring MAC Addresses

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

Configuring a MAC Address Entry

Select **Network** > **MAC** from the navigation tree. The system automatically displays the **MAC** tab, which shows all the MAC address entries on the device, as shown in Figure 1-2. Click **Add** in the bottom to enter the page for creating MAC address entries, as shown in Figure 1-3.

Figure 1-2 The **MAC** tab

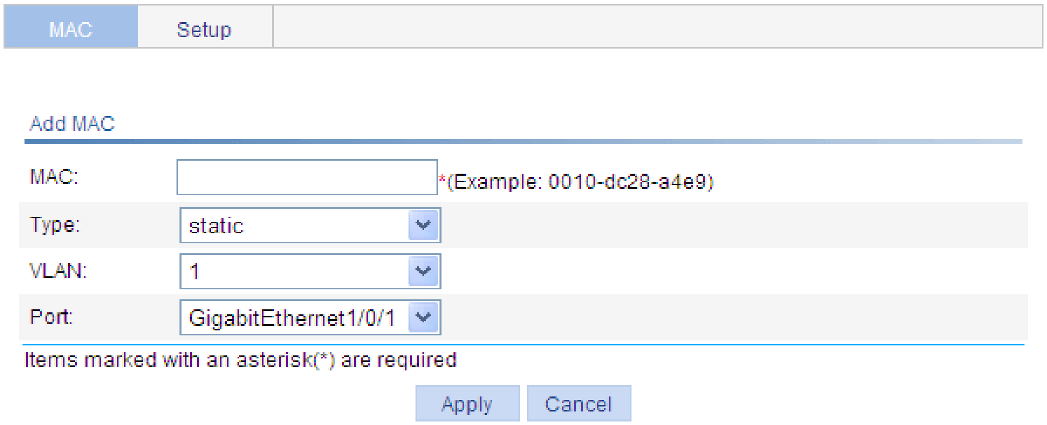


Search Item: MAC Keywords:

□	MAC	VLAN ID	Type	Port	Operation
□	000d-56fb-3880	1	Learned	GigabitEthernet1/0/15	🗑
□	000d-88f8-4e71	1	Learned	GigabitEthernet1/0/15	🗑
□	000f-cb00-5601	1	Learned	GigabitEthernet1/0/15	🗑
□	000f-e200-0144	1	Learned	GigabitEthernet1/0/15	🗑
□	000f-e207-f2e0	1	Learned	GigabitEthernet1/0/15	🗑
□	000f-e218-d0d1	1	Learned	GigabitEthernet1/0/15	🗑
□	0015-e943-712f	1	Learned	GigabitEthernet1/0/15	🗑
□	0015-e943-7326	1	Learned	GigabitEthernet1/0/15	🗑
□	0022-3377-998c	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-4c3d-35d7	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-fc00-000b	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-fc00-004f	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-fc00-3963	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-fc00-5503	1	Learned	GigabitEthernet1/0/15	🗑
□	00e0-fc00-5544	1	Learned	GigabitEthernet1/0/15	🗑

24 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Figure 1-3 Create a MAC address entry



Add MAC

MAC:	*(Example: 0010-dc28-a4e9)
Type:	static
VLAN:	1
Port:	GigabitEthernet1/0/1

Items marked with an asterisk(*) are required

Table 1-1 shows the detailed configuration of creating a MAC address entry.

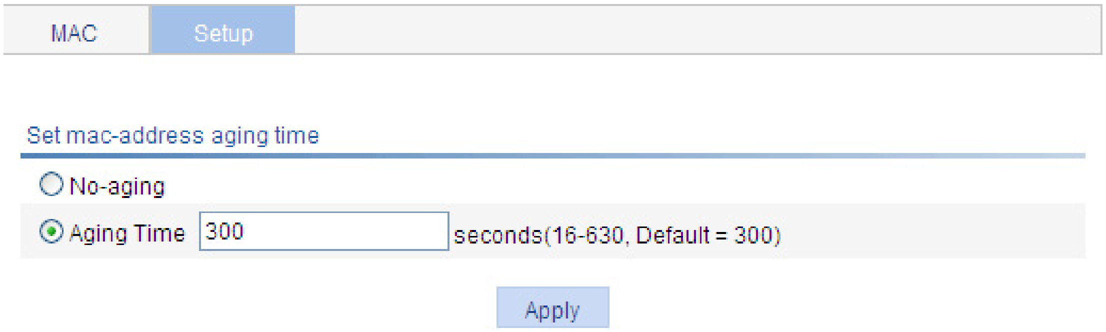
Table 1-1 Configuration items of creating a MAC address entry

Item	Description
MAC	Set the MAC address to be added
Type	Set the type of the MAC address entry, which can be: • **static**: indicates static MAC address entries that never age out • **dynamic**: indicates dynamic MAC address entries that will age out • **blackhole**: indicates blackhole MAC address entries that never age out **Highlight** *The types of the MAC address entries displayed in the tab are as follows:* • ***Config static****: indicates static MAC address entries manually configured by the users* • ***Config dynamic****: indicates dynamic MAC address entries manually configured by the users* • ***Blackhole****: indicates blackhole MAC address entries* • ***Learned****: indicates dynamic MAC address entries learned by the device* • ***Other****: indicates types other than the ones mentioned above*
VLAN	Set the ID of the VLAN to which the MAC address belongs
Port	Set the port to which the MAC address belongs

Setting the Aging Time of MAC Address Entries

Select **Network** > **MAC** from the navigation tree, and then select the **Setup** tab to enter the page for setting the MAC address entry aging time, as shown in Figure 1-4.

Figure 1-4 Set the aging time for MAC address entries



Set mac-address aging time

○ No-aging

● Aging Time 300 seconds(16-630, Default = 300)

The following table shows the detailed configuration of setting the MAC address entry aging time.

Table 1-2 Configuration items of setting the aging time for a MAC address entry

Item	Description
No-aging	Specifies that the MAC address entry never ages out.
Aging time	Sets the aging time for the MAC address entry

MAC Address Configuration Example

Network requirements

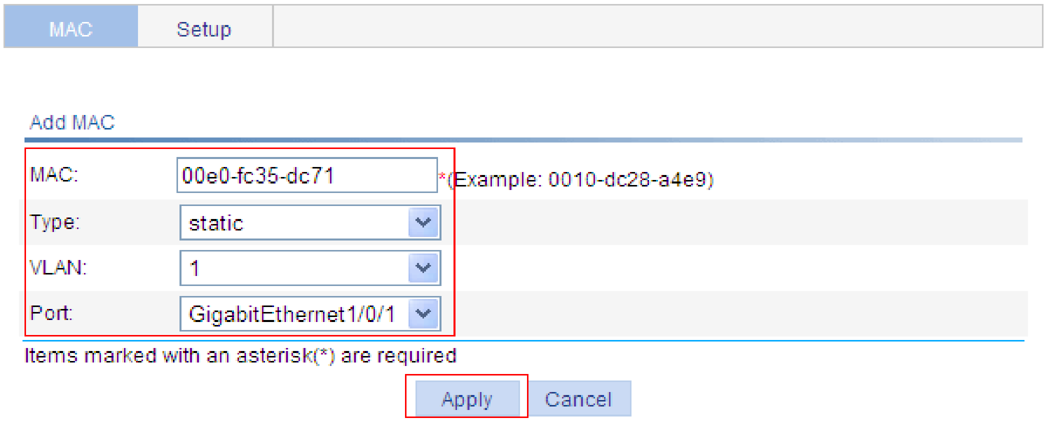
Use the MAC address table management function of the Web-based NMS. It is required to add a static MAC address 00e0-fc35-dc71 under GigabitEthernet 1/0/1 in VLAN 1.

Configuration procedure

# Create a static MAC address entry.

Select **Network** > **MAC** from the navigation tree to enter the **MAC** tab, and then click **Add**, as shown in Figure 1-2. The page shown in Figure 1-5 appears.

Figure 1-5 Create a static MAC address entry



Add MAC

MAC: 00e0-fc35-dc71 *(Example: 0010-dc28-a4e9)

Type: static

VLAN: 1

Port: GigabitEthernet1/0/1

Items marked with an asterisk(*) are required

Make the following configurations on the page shown in Figure 1-5:

- Type in MAC address **00e0-fc35-dc71**.
- Select **static** in the **Type** drop down list.
- Select **1** in the **VLAN** drop down list.
- Select **GigabitEthernet1/0/1** in the **Port** drop down list.
- Click **Apply**.

Table of Contents

1 MSTP Configuration

Overview

As a Layer 2 management protocol, the Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.

Like many other protocols, STP evolves as the network grows. The later versions of STP are Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). This chapter describes the characteristics of STP, RSTP, and MSTP and the relationship among them.

Introduction to STP

STP was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging information with one another and eliminate loops by selectively blocking certain ports to prune the loop structure into a loop-free tree structure. This avoids proliferation and infinite cycling of packets that would occur in a loop network and prevents decreased performance of network devices caused by duplicate packets received.

In the narrow sense, STP refers to the IEEE 802.1d STP; in the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP-enabled network devices exchange BPDUs to establish a spanning tree. BPDUs contain sufficient information for the network devices to complete spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used for calculating a spanning tree and maintaining the spanning tree topology.
- Topology change notification (TCN) BPDUs, used for notifying the concerned devices of network topology changes, if any.

Basic Concepts in STP

Root bridge

A tree network must have a root; hence the concept of root bridge was introduced in STP.

There is one and only one root bridge in the entire network, and the root bridge can change along with changes of the network topology. Therefore, the root bridge is not fixed.

Upon initialization of a network, each device generates and sends out BPDUs periodically with itself as the root bridge; after network convergence, only the root bridge generates and sends out configuration BPDUs at a certain interval, and the other devices just forward the BPDUs.

Root port

On a non-root bridge, the port nearest to the root bridge is called the root port. The root port is responsible for communication with the root bridge. Each non-root bridge has one and only one root port. The root bridge has no root port.

Designated bridge and designated port

The following table describes designated bridges and designated ports.

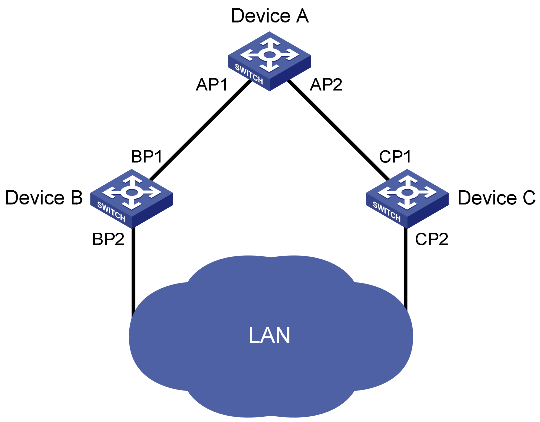
Table 1-1 Description of designated bridges and designated ports:

Classification	Designated bridge	Designated port
For a device	A device directly connected with the local device and responsible for forwarding BPDUs to the local device	The port through which the designated bridge forwards BPDUs to the local device
For a LAN	The device responsible for forwarding BPDUs to this LAN segment	The port through which the designated bridge forwards BPDUs to this LAN segment

As shown in Figure 1-1, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port of Device B is port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port for the LAN is the port BP2 on Device B.

Figure 1-1 A schematic diagram of designated bridges and designated ports



Path cost

Path cost is a reference value used for link selection in STP. By calculating path costs, STP selects relatively robust links and blocks redundant links, and finally prunes the network into a loop-free tree.

Note

All the ports on the root bridge are designated ports.

How STP Works

The devices on a network exchange BPDUs to identify the network topology. Configuration BPDUs contain sufficient information for the network devices to complete spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID: consisting of the priority and MAC address of the root bridge.
- Root path cost: the cost of the path to the root bridge.
- Designated bridge ID: consisting of the priority and MAC address of the designated bridge.
- Designated port ID: designated port priority plus port name.
- Message age: age of the configuration BPDU while it propagates in the network.
- Max age: maximum age of the configuration BPDU can be maintained on a device.
- Hello time: configuration BPDU interval.
- Forward delay: the delay used by STP bridges to transit the state of the root and designated ports to forwarding.

Note

For simplicity, the descriptions and examples below involve only four fields in the configuration BPDUs:

- Root bridge ID (represented by device priority)
- Root path cost
- Designated bridge ID (represented by device priority)
- Designated port ID (represented by port name)

Calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each port generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Table 1-2 Selection of the optimum configuration BPDU

Step	Actions
1	Upon receiving a configuration BPDU on a port, the device performs the following: • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device discards the received configuration BPDU and does not process the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device replaces the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

Note

The following are the principles of configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all the configuration BPDUs have the same root bridge ID, their root path costs are compared. Assume that the root path cost in a configuration BPDU plus the path cost of a receiving port is S. The configuration BPDU with the smallest S value has the highest priority.
- If all configuration BPDUs have the same S value, their designated bridge IDs, designated port IDs, and the IDs of the receiving ports are compared in sequence. The configuration BPDU containing a smaller ID wins out.

- Selection of the root bridge

Initially, each STP-enabled device on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the devices compare their root bridge IDs to elect the device with the smallest root bridge ID as the root bridge.

- Selection of the root port and designated ports on a non-root device

The process of selecting the root port and designated ports is as follows:

Table 1-3 Selection of the root port and designated ports

Step	Description
1	A non-root device regards the port on which it received the optimum configuration BPDU as the root port.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost of the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.

Step	Description
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port of which the port role is to be defined, and acts depending on the comparison result: • If the calculated configuration BPDU is superior, the device considers this port as the designated port, and replaces the configuration BPDU on the port with the calculated configuration BPDU, which will be sent out periodically. • If the configuration BPDU on the port is superior, the device blocks this port without updating its configuration BPDU. The blocked port can receive BPDUs but cannot send BPDUs or forward data.

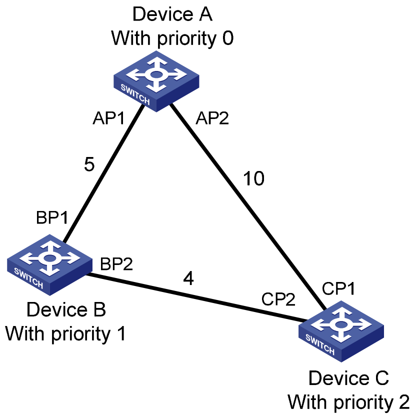
Note

When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state – they receive BPDUs but do not forward BPDUs or user traffic.

A tree-shape topology forms upon successful election of the root bridge, the root port on each non-root bridge and the designated ports.

The following is an example of how the STP algorithm works. As shown in Figure 1-2, assume that the priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

Figure 1-2 Network diagram for the STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 1-4 Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}

Device	Port name	BPDU of port
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

Table 1-5 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison

Device A	• Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU.
	• Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU.
	• Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically.
		AP1: {0, 0, 0, AP1}
		AP2: {0, 0, 0, AP2}

Device B	• Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1.
	• Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU.
		BP1: {0, 0, 0, AP1}
		BP2: {1, 0, 1, BP2}

	• Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed.
	• Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}.
	• Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically.
		Root port BP1:
		{0, 0, 0, AP1}
		Designated port BP2:
		{0, 5, 1, BP2}

Device	Comparison process	BPDU of port after comparison

Device C	• Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1.
	• Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the configuration BPDU is updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and therefore updates the configuration BPDU of CP2.
		CP1: {0, 0, 0, AP2}
		CP2: {1, 0, 1, BP2}

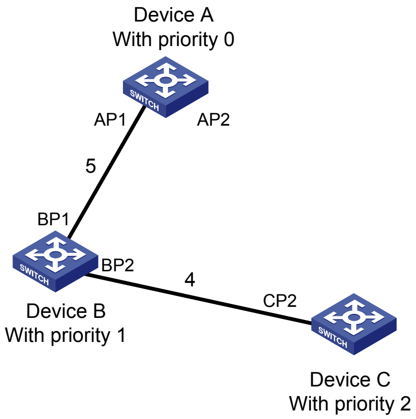
	After comparison:
	• The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed.
	• Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU.
		Root port CP1:
		{0, 0, 0, AP2}
		Designated port CP2:
		{0, 10, 2, CP2}

	• Then, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its own configuration BPDU, Device C launches a BPDU update process.
	• At the same time, port CP1 receives periodic configuration BPDUs from Device A. Device C does not launch an update process after comparison.
		CP1: {0, 0, 0, AP2}
		CP2: {0, 5, 1, BP2}

	After comparison:
	• Because the root path cost of CP2 (9) (root path cost of the BPDU (5) plus path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed.
	• After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new event, for example, the link from Device B to Device C going down.
		Blocked port CP2:
		{0, 0, 0, AP2}
		Root port CP2:
		{0, 5, 1, BP2}

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is established as shown in Figure 1-3.

Figure 1-3 The final calculated spanning tree



Note

The spanning tree calculation process in this example is only a simplified process.

The BPDU forwarding mechanism in STP

- Upon network initiation, every device regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular hello interval.
- If it is the root port that received a configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device increases the message age carried in the configuration BPDU following a certain rule and starts a timer to time the configuration BPDU while sending out this configuration BPDU through the designated port.
- If the configuration BPDU received on a designated port has a lower priority than the configuration BPDU of the local port, the port immediately sends out its own configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device will generate configuration BPDUs with itself as the root. This triggers a new spanning tree calculation process to establish a new path to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root ports and designated ports begin to forward data as soon as they are elected, a temporary loop may occur.

STP timers

STP calculation involves three important timing parameters: forward delay, hello time, and max age.

- Forward delay is the delay time for device state transition.

A path failure can cause spanning tree re-calculation to adapt the spanning tree structure to the change. However, the resulting new configuration BPDU cannot propagate throughout the network immediately. If the newly elected root ports and designated ports start to forward data right away, a temporary loop is likely to occur.

For this reason, as a mechanism for state transition in STP, the newly elected root ports or designated ports require twice the forward delay time before transiting to the forwarding state to ensure that the new configuration BPDU has propagated throughout the network.

- Hello time is the time interval at which a device sends hello packets to the surrounding devices to ensure that the paths are fault-free.
- Max age is a parameter used to determine whether a configuration BPDU held by the device has expired. A configuration BPDU beyond the max age will be discarded.

Introduction to RSTP

Developed based on the 802.1w standard of IEEE, RSTP is an optimized version of STP. It achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP.

Note

- In RSTP, a newly elected root port can enter the forwarding state rapidly if this condition is met: The old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.
- In RSTP, a newly elected designated port can enter the forwarding state rapidly if this condition is met: The designated port is an edge port or a port connected with a point-to-point link. If the designated port is an edge port, it can enter the forwarding state directly; if the designated port is connected with a point-to-point link, it can enter the forwarding state immediately after the device undergoes handshake with the downstream device and gets a response.

Introduction to MSTP

Why MSTP

Weaknesses of STP and RSTP

STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or an edge port, which directly connects to a user terminal rather than to another device or a shared LAN segment.

Although RSTP supports rapid network convergence, it has the same drawback as STP does: All bridges within a LAN share the same spanning tree, so redundant links cannot be blocked based on VLAN, and the packets of all VLANs are forwarded along the same spanning tree.

Features of MSTP

Developed based on the 802.1s standard of IEEE, MSTP overcomes the shortcomings of STP and RSTP. In addition to the support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along separate paths, thus providing a better load sharing mechanism for redundant links.

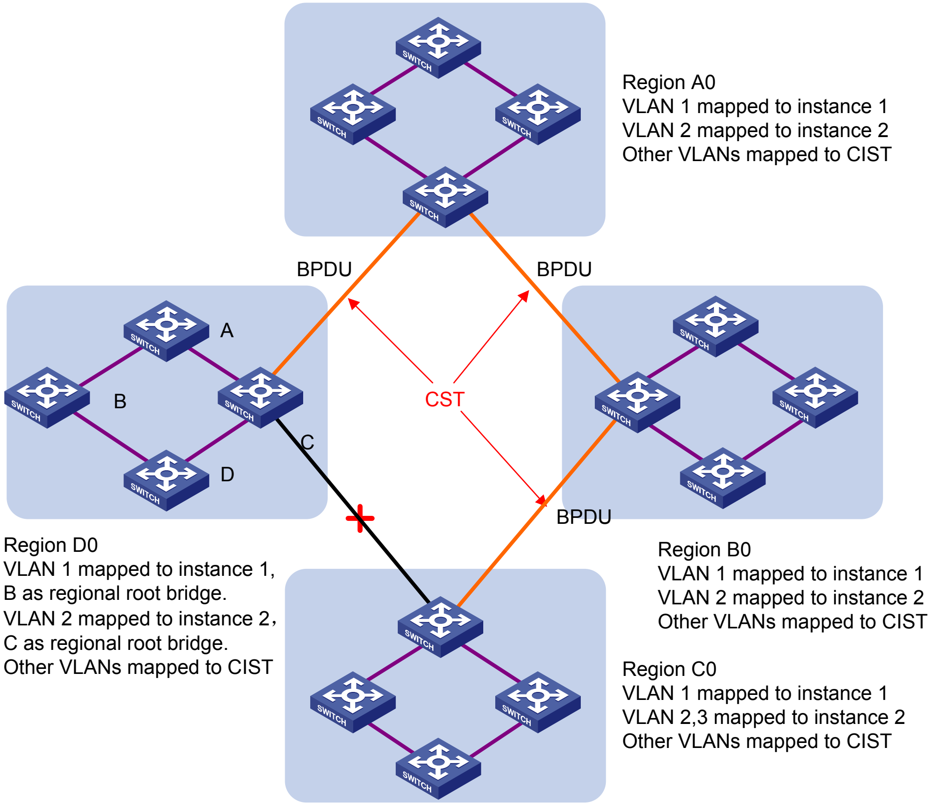
MSTP features the following:

- MSTP supports mapping VLANs to MST instances (MSTIs) by means of a VLAN-to-MSTI mapping table. MSTP can reduce communication overheads and resource usage by mapping multiple VLANs to one MSTI.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a loop network into a loop-free tree, thus avoiding proliferation and endless cycling of packets in a loop network. In addition, it provides multiple redundant paths for data forwarding, thus supporting load balancing of VLAN data.
- MSTP is compatible with STP and RSTP.

Basic Concepts in MSTP

Assume that all the four devices in Figure 1-4 are running MSTP. This section explains some basic concepts of MSTP based on the figure.

Figure 1-4 Basic concepts in MSTP


Region A0
VLAN 1 mapped to instance 1
VLAN 2 mapped to instance 2
Other VLANs mapped to CIST
BPDU
BPDU
A
B
C
D
CST
BPDU
Region D0
VLAN 1 mapped to instance 1,
B as regional root bridge.
VLAN 2 mapped to instance 2,
C as regional root bridge.
Other VLANs mapped to CIST
Region B0
VLAN 1 mapped to instance 1
VLAN 2 mapped to instance 2
Other VLANs mapped to CIST
Region C0
VLAN 1 mapped to instance 1
VLAN 2,3 mapped to instance 2
Other VLANs mapped to CIST
SWITCH

MST region

A multiple spanning tree region (MST region) consists of multiple devices in a switched network and the network segments among them. These devices have the following characteristics:

- All are MSTP-enabled,
- They have the same region name,
- They have the same VLAN-to-MSTI mapping configuration,
- They have the same MSTP revision level configuration, and
- They are physically linked with one another.

For example, all the devices in region A0 in Figure 1-4 have the same MST region configuration as follows:

- The same region name,
- The same VLAN-to-MSTI mapping configuration (VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to the common and internal spanning tree (CIST, that is, MSTI 0), and
- The same MSTP revision level (not shown in the figure).

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region.

VLAN-to-MSTI mapping table

As an attribute of an MST region, the VLAN-to-MSTI mapping table describes the mapping relationships between VLANs and MSTIs. In Figure 1-4, for example, the VLAN-to-MSTI mapping table of region A0 is: VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to CIST. MSTP achieves load balancing by means of the VLAN-to-MSTI mapping table.

IST

An internal spanning tree (IST) is a spanning tree that runs in an MST region.

ISTs in all MST regions and the common spanning tree (CST) jointly constitute the common and internal spanning tree (CIST) of the entire network. An IST is a section of the CIST. An IST is a special MSTI.

In Figure 1-4, for example, the CIST has a section in each MST region, and this section is the IST in the respective MST region.

CST

The CST is a single spanning tree that connects all MST regions in a switched network. If you regard each MST region as a “device”, the CST is a spanning tree calculated by these devices through STP or RSTP. CSTs are indicated by red lines in Figure 1-4.

CIST

Jointly constituted by ISTs and the CST, the CIST is a single spanning tree that connects all devices in a switched network.

In Figure 1-4, for example, the ISTs in all MST regions plus the inter-region CST constitute the CIST of the entire network.

MSTI

Multiple spanning trees can be generated in an MST region through MSTP, one spanning tree being independent of another. Each spanning tree is referred to as a multiple spanning tree instance (MSTI).

In Figure 1-4, for example, multiple MSTIs can exist in each MST region, each MSTI corresponding to the specified VLANs.

Regional root bridge

The root bridge of the IST or an MSTI within an MST region is the regional root bridge of the IST or the MSTI. Based on the topology, different spanning trees in an MST region may have different regional roots.

For example, in region D0 in Figure 1-4, the regional root of MSTI 1 is device B, while that of MSTI 2 is device C.

Common root bridge

The common root bridge is the root bridge of the CIST.

In Figure 1-4, for example, the common root bridge is a device in region A0.

Boundary port

A boundary port is a port that connects an MST region to another MST region, or to a single spanning-tree region running STP, or to a single spanning-tree region running RSTP. It is at the boundary of an MST region.

During MSTP calculation, the role of a boundary port in an MSTI must be consistent with its role in the CIST. But this is not true with master ports. A master port on MSTIs is a root port on the CIST. For example, in Figure 1-4, if a device in region A0 is interconnected with the first port of a device in region D0 and the common root bridge of the entire switched network is located in region A0, the first port of that device in region D0 is the boundary port of region D0.

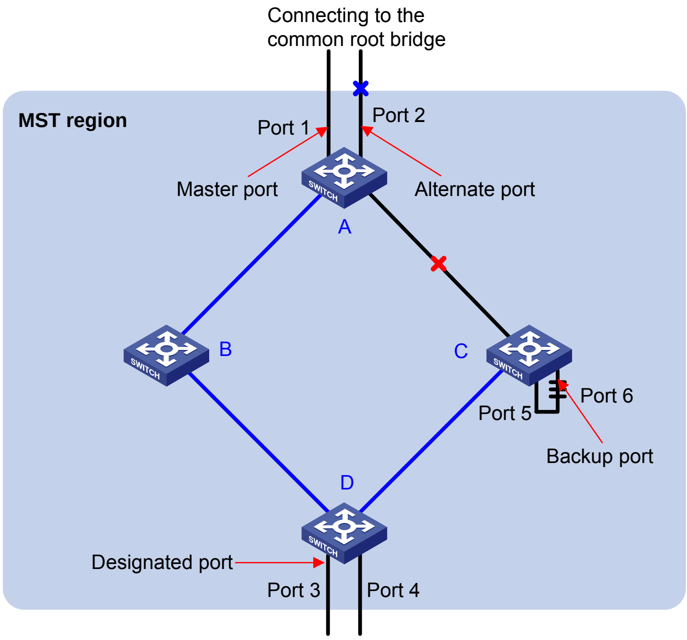
Roles of ports

MSTP calculation involves these port roles: root port, designated port, master port, boundary port, alternate port, backup port, and so on.

- Root port: a port responsible for forwarding data to the root bridge.
- Designated port: a port responsible for forwarding data to the downstream network segment or device.
- Master port: a port on the shortest path from the current region to the common root bridge, connecting the MST region to the common root bridge. If the region is seen as a node, the master port is the root port of the region on the CST. The master port is a root port on IST/CIST and still a master port on the other MSTIs.
- Alternate port: the standby port for the root port and the master port. When the root port or master port is blocked, the alternate port becomes the new root port or master port.
- Backup port: the backup port of a designated port. When the designated port is blocked, the backup port becomes a new designated port and starts forwarding data without delay. A loop occurs when two ports of the same MSTP device are interconnected. Therefore, the device will block either of the two ports, and the backup port is the port to be blocked.

A port can play different roles in different MSTIs.

Figure 1-5 Port roles



In Figure 1-5, devices A, B, C, and D constitute an MST region. Port 1 and port 2 of device A are connected to the common root bridge, port 5 and port 6 of device C form a loop, port 3 and port 4 of Device D are connected downstream to the other MST regions.

Port states

In MSTP, port states fall into the following three:

- Forwarding: the port learns MAC addresses and forwards user traffic;
- Learning: the port learns MAC addresses but does not forward user traffic;
- Discarding: the port does not learn MAC addresses or forwards user traffic.

Note

A port can have different port states in different MSTIs.

A port state is not exclusively associated with a port role. Table 1-6 lists the port state(s) supported by each port role. ("√" indicates that the port state is available for the corresponding port role; "—" indicates that the port state is not available for the corresponding port role.)

Table 1-6 Ports states supported by different port roles

Port state	Port role				
	Root port/master port	Designated port	Boundary port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

How MSTP Works

MSTP divides an entire Layer 2 network into multiple MST regions, which are interconnected by a calculated CST. Inside an MST region, multiple spanning trees are calculated, each being called an MSTI (Among these MSTIs, MSTI 0 is called the CIST). Similar to RSTP, MSTP uses configuration BPDUs to calculate spanning trees. The only difference between the two protocols is that an MSTP BPDU carries the MSTP configuration on the device from which this BPDU is sent.

CIST calculation

The calculation of a CIST tree is also the process of configuration BPDU comparison. During this process, the device with the highest priority is elected as the root bridge of the CIST. MSTP generates an IST within each MST region through calculation, and, at the same time, MSTP regards each MST region as a single device and generates a CST among these MST regions through calculation. The CST and ISTs constitute the CIST of the entire network.

MSTI calculation

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-MSTI mappings. MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP/RSTP, for each spanning tree. For details, refer to How STP Works.

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

Implementation of MSTP on Devices

MSTP is compatible with STP and RSTP. STP and RSTP protocol packets can be recognized by devices running MSTP and used for spanning tree calculation.

In addition to basic MSTP functions, the device provides the following functions for ease of management:

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU (a message that notifies the device of topology changes) guard

Protocols and Standards

MSTP is documented in:

- IEEE 802.1d: Spanning Tree Protocol
- IEEE 802.1w: Rapid Spanning Tree Protocol
- IEEE 802.1s: Multiple Spanning Tree Protocol

Configuring MSTP

Configuration Task List

Perform the tasks described in Table 1-7 to configure MSTP.

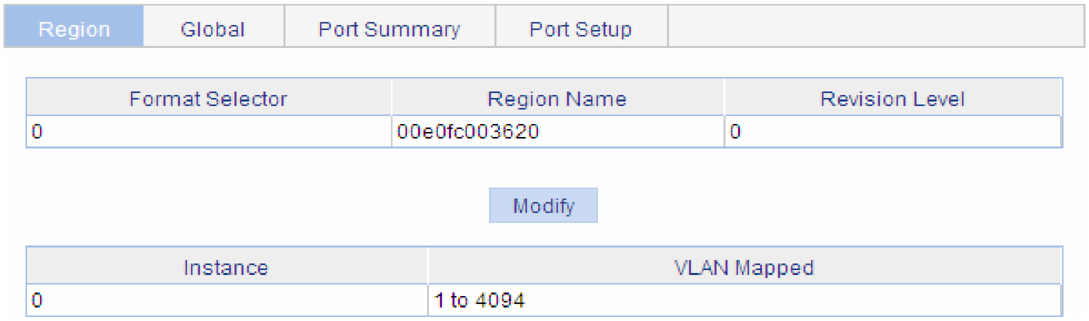
Table 1-7 MSTP configuration task list

Task	Remarks
Configuring an MST Region	Optional Configure the MST region-related parameters and VLAN-to-MSTI mappings. By default, the MST region-related parameters adopt the default values, and all VLANs in an MST region are mapped to MSTI 0.
Configuring MSTP Globally	Required Enable MSTP globally and configure MSTP parameters. By default, MSTP is enabled globally; and all MSTP parameters have default values.
Configuring MSTP on a Port	Optional Enable MSTP on a port and configure MSTP parameters. By default, MSTP is enabled on a port, and all MSTP parameters adopt the default values.
Displaying MSTP Information of a Port	Optional Display MSTP information of a port in MSTI 0, the MSTI to which the port belongs, and the path cost and priority of the port.

Configuring an MST Region

Select **Network** > **MSTP** from the navigation tree to enter the page as shown in Figure 1-6.

Figure 1-6 MST region

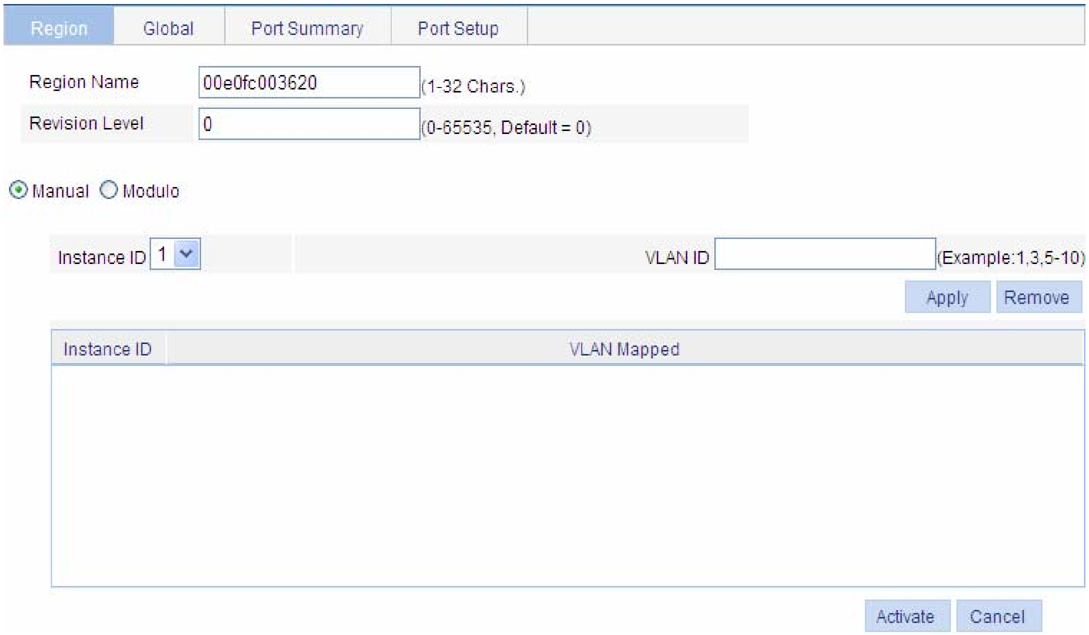


Format Selector	Region Name	Revision Level
0	00e0fc003620	0

Instance	VLAN Mapped
0	1 to 4094

Click **Modify** to enter the page for configuring MST regions, as shown in Figure 1-7.

Figure 1-7 Configure an MST region



Region Name 00e0fc003620 (1-32 Chars.)

Revision Level 0 (0-65535, Default = 0)

● Manual ○ Modulo

Instance ID 1 VLAN ID (Example:1,3,5-10)

Instance ID	VLAN Mapped

Table 1-8 describes the configuration items of configuring an MST region.

Table 1-8 Configuration items of configuring an MST region

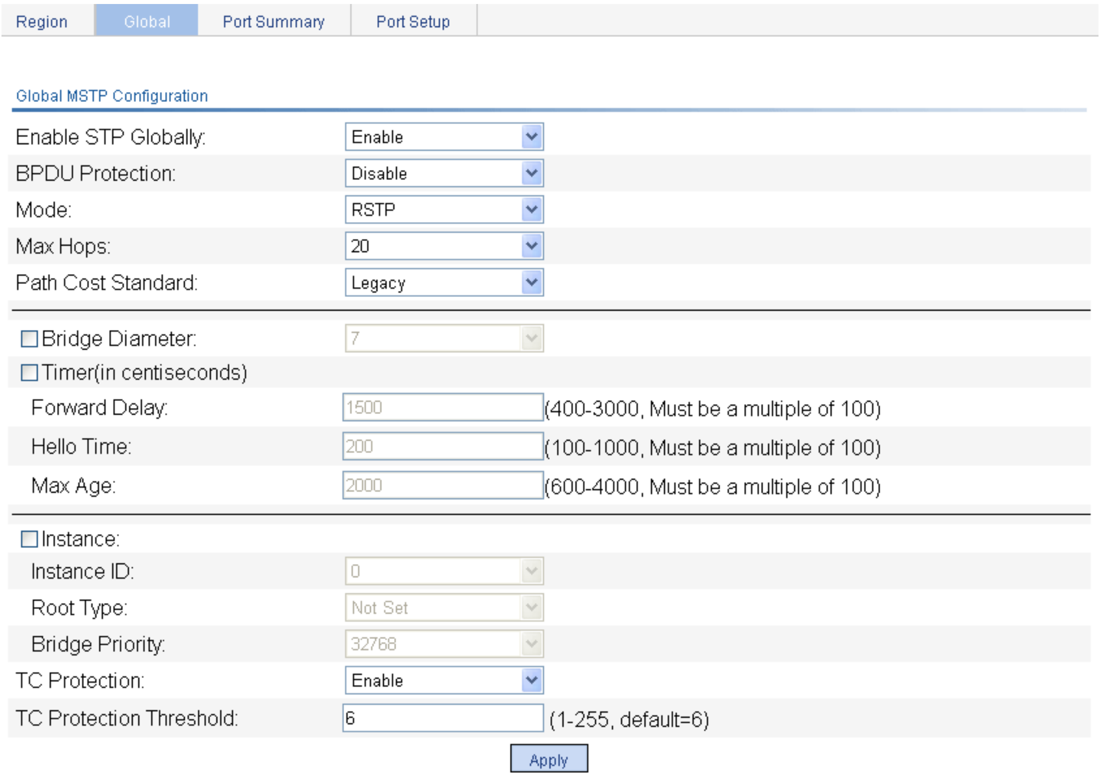
Item		Description
Region Name		MST region name The MST region name is the bridge MAC address of the device by default.
Revision Level		Revision level of the MST region
Manual	Instance ID	Manually add VLAN-to-MSTI mappings. Click **Apply** to add the VLAN-to-MSTI mapping entries to the list below.
	VLAN ID	
Modulo	Modulo Value	The device automatically maps 4094 VLANs to the corresponding MSTIs based on the modulo value.

Return to MSTP configuration task list.

Configuring MSTP Globally

Select **Network** > **MSTP** from the navigation tree, and then click **Global** to enter the page for configuring MSTP globally, as shown in Figure 1-8.

Figure 1-8 Configure MSTP globally



Global MSTP Configuration

Enable STP Globally: Enable

BPDU Protection: Disable

Mode: RSTP

Max Hops: 20

Path Cost Standard: Legacy

□ Bridge Diameter: 7

□ Timer(in centiseconds)

Forward Delay: 1500 (400-3000, Must be a multiple of 100)

Hello Time: 200 (100-1000, Must be a multiple of 100)

Max Age: 2000 (600-4000, Must be a multiple of 100)

□ Instance:

Instance ID: 0

Root Type: Not Set

Bridge Priority: 32768

TC Protection: Enable

TC Protection Threshold: 6 (1-255, default=6)

Table 1-9 describes the configuration items of configuring MSTP globally.

Table 1-9 Configuration items of configuring MSTP globally

Item	Description
Enable STP Globally	Select whether to enable STP globally. Other MSTP configurations take effect only after you enable STP globally.
BPDU Guard	Select whether to enable BPDU guard BPDU guard can protect the device from malicious BPDU attacks, thus making the network topology stable.
Mode	Set the working mode of STP, which can be STP, RSTP, or MSTP. • STP: Each port on a device sends out STP BPDUs. • RSTP: Each port on a device sends out RSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP. • MSTP: Each port on a device sends out MSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP. The working mode is RSTP by default.
Max Hops	Set the maximum number of hops in an MST region to restrict the region size. The setting can take effect only when it is configured on the regional root bridge.
Path Cost Standard	Specify the standard for path cost calculation. It can be Legacy, IEEE 802.1D-1998, or IEEE 802.1T.

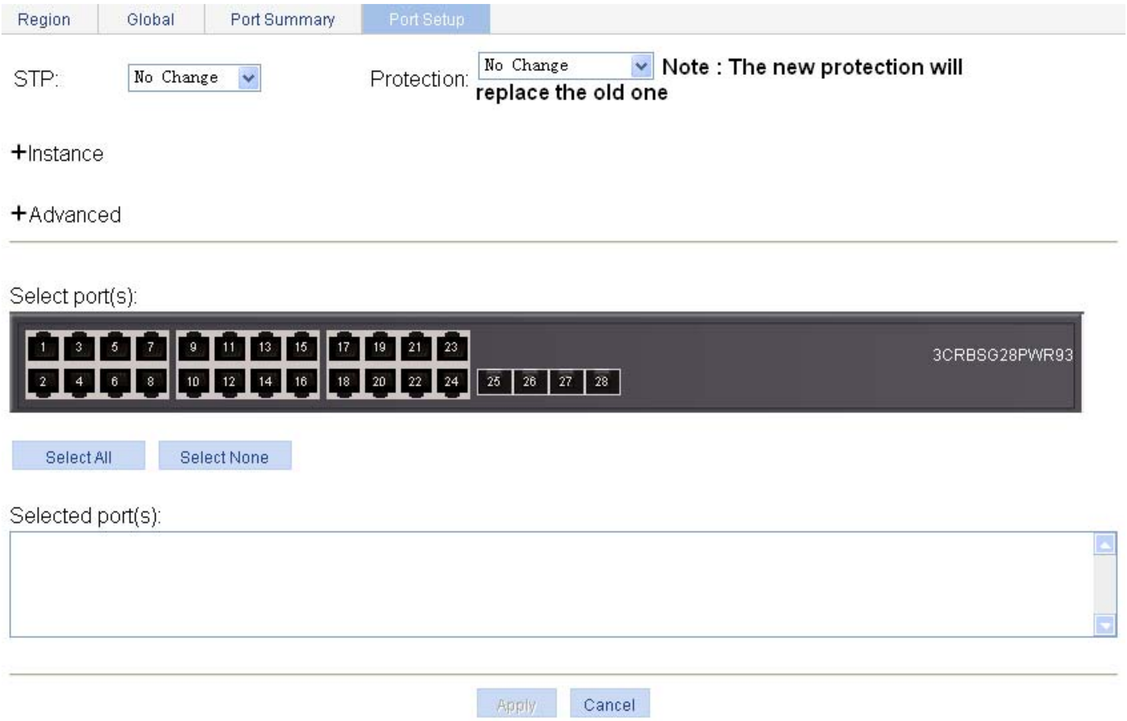
Item		Description	
Bridge Diameter		Any two stations in a switched network are interconnected through a specific path composed of a series of devices. The bridge diameter (or the network diameter) is the number of devices on the path composed of the most devices. After you set the network diameter, you cannot set the timers. Instead, the device automatically calculates the forward delay, hello time, and max age. **Highlight** • *The configured network diameter is effective for CIST only, not for MSTIs.* • *The bridge diameter cannot be configured together with the timers.*	
Timers	Forward Delay	Set the delay for the root and designated ports to transit to the forwarding state.	**Highlight** • *The settings of hello time, forward delay and max age must meet a certain formula. Otherwise, the network topology will not be stable. You are recommended to set the network diameter and then have the device automatically calculate the forward delay, hello time, and max age.* • *The bridge diameter cannot be configured together with the timers.*
	Hello Time	Set the interval at which the device sends hello packets to the surrounding devices to ensure that the paths are fault-free.	
	Max Age	Set the maximum length of time a configuration BPDU can be held by the device.	
Instance	Instance ID	Set the role of the device in the MSTI or the bridge priority of the device, which is one of the factors deciding whether the device can be elected as the root bridge. Role of the device in the MSTI: • Not Set: Not set (you can set the bridge priority of the device when selecting this role) • Primary: Configure the device as the root bridge (you cannot set the bridge priority of the device when selecting this role) • Secondary: Configure the device as a secondary root bridge (you cannot set the bridge priority of the device when selecting this role).	
	Root Type		
	Bridge Priority		
tc-protection		Select whether to enable TC-BPDU guard. When receiving topology change (TC) BPDUs, the device flushes its forwarding address entries. If someone forges TC-BPDUs to attack the device, the device will receive a large number of TC-BPDUs within a short time and frequently flushes its forwarding address entries. This affects network stability. With the TC-BPDU guard function, you can prevent frequent flushing of forwarding address entries. **Highlight** *You are recommended not to disable this function.*	
tc-protection threshold		Set the maximum number of immediate forwarding address entry flushes the device can perform within a certain period of time after receiving the first TC-BPDU.	

Return to MSTP configuration task list.

Configuring MSTP on a Port

Select **Network > MSTP** from the navigation tree, and then click **Port Setup** to enter the page for configuring MSTP on ports, as shown in Figure 1-9.

Figure 1-9 MSTP configuration on a port



STP: No Change

Protection: No Change

Note : The new protection will replace the old one

Table 1-10 describes the configuration items of configuring MSTP on a port.

Table 1-10 Configuration items of configuring MSTP on a port

Item	Description
STP	Select whether to enable STP on the port
Protection	Set the type of protection to be enabled on the port: ● Not Set: No protection is enabled on the port. ● Edged Port, Root Protection, Loop Protection: Refer to Table 1-11.

Item		Description
Instance	Instance ID	Set the priority and path cost of the port in the current MSTI. • The priority of a port is an important factor in determining whether the port can be elected as the root port of a device. If all other conditions are the same, the port with the highest priority will be elected as the root port. On an MSTP-enabled device, a port can have different priorities in different MSTIs, and the same port can play different roles in different MSTIs, so that data of different VLANs can be propagated along different physical paths, thus implementing per-VLAN load balancing. You can set port priority values based on the actual networking requirements. • Path cost is a parameter related to the rate of a port. On an MSTP-enabled device, a port can have different path costs in different MSTIs. Setting appropriate path costs allows VLAN traffic flows to be forwarded along different physical links, thus achieving VLAN-based load balancing. The device can automatically calculate the default path cost; alternatively, you can also manually configure path cost for ports.
	Port Priority	
	Auto Path Cost	
	Manual Path Cost	
Advanced	Point to Point	Specify whether the port is connected to a point-to-point link. • Auto: Automatically detects whether the link type of the port is point-to-point. • Force False: Specifies that the link type for the port is not point-to-point link. • Force True: Specifies that the link type for the port is point-to-point link. **Highlight** *If a port is configured as connecting to a point-to-point link, the setting takes effect for the port in all MSTIs. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, the configuration may incur a temporary loop.*
	Transmit Limit	Configure the maximum number of MSTP packets that can be sent during each Hello interval. The larger the transmit limit is, the more network resources will be occupied. Therefore, you are recommended to use the default value.
	MSTP Mode	Set whether the port migrates to the MSTP mode. In a switched network, if a port on an MSTP (or RSTP) device connects to a device running STP, this port will automatically migrate to the STP-compatible mode. After the device running STP is removed, the port on the MSTP (or RSTP) device may not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. You can set this option to enable the port to automatically migrate to the MSTP (or RSTP) mode.
Select port(s)		Select one or multiple ports on which you want to configure MSTP on the chassis front panel. If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel. You can select aggregate interfaces from this list.

Table 1-11 Protection types

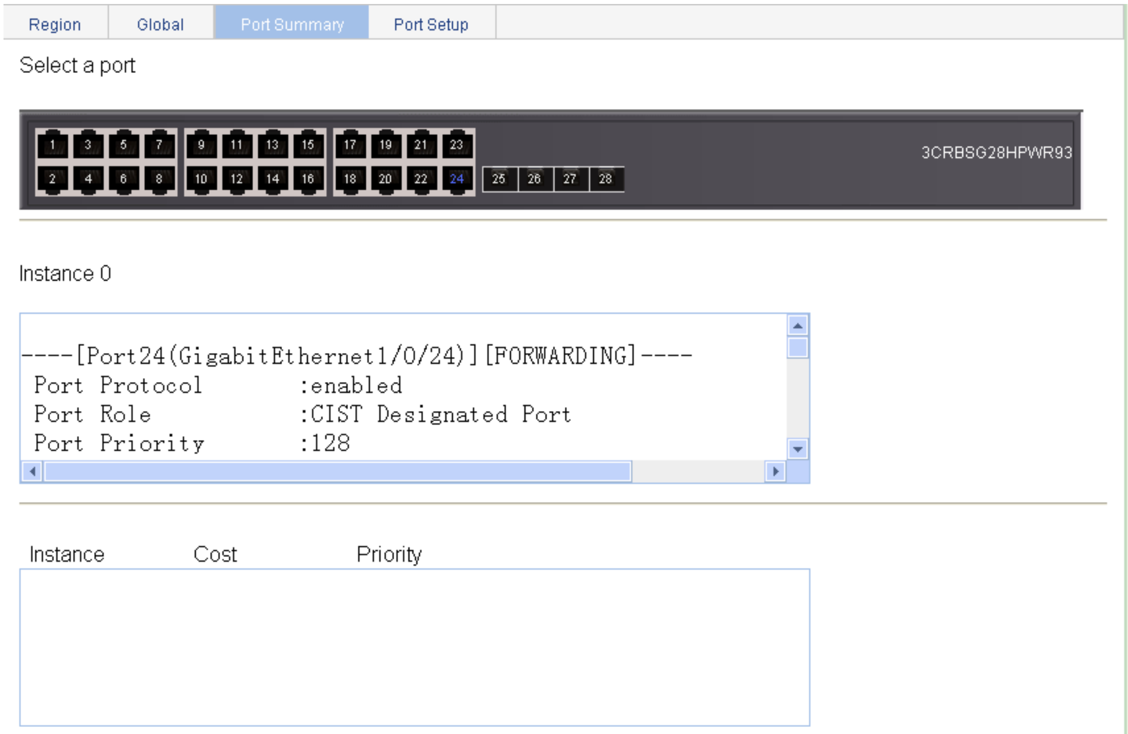
Protection type	Description
Edged Port	Set the port as an edge port. Some ports of access layer devices are directly connected to PCs or file servers, which cannot generate BPDUs. You can set these ports as edge ports to achieve fast transition for these ports. You are recommended to enable the BPDU guard function in conjunction with the edged port function to avoid network topology changes when the edge ports receive configuration BPDUs.
Root Protection	Enable the root guard function. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology change to occur. The root guard function is used to address such a problem.
Loop Protection	Enable the loop guard function. By keeping receiving BPDUs from the upstream device, a device can maintain the state of the root port and other blocked ports. These BPDUs may get lost because of network congestion or unidirectional link failures. In this case, the device will re-elect a root port, and blocked ports may transit to the forwarding state, causing loops in the network. The loop guard function is used to address such a problem.

Return to MSTP configuration task list.

Displaying MSTP Information of a Port

Select **Network > MSTP** from the navigation tree, and then click **Port Summary** to enter the page shown in Figure 1-10.

Figure 1-10 The Port Summary tab



```
----[Port24(GigabitEthernet1/0/24)][FORWARDING]----
 Port Protocol        :enabled
 Port Role            :CIST Designated Port
 Port Priority        :128
```

Select a port (GigabitEthernet 1/0/16 for example) on the chassis front panel (If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel. You can select aggregate interfaces from this list). The lower part of the page displays the MSTP information of the port in MSTI 0 (when STP is enabled globally) or the STP status and statistics (when STP is not enabled globally), the MSTI to which the port belongs, and the path cost and priority of the port in the MSTI.

Table 1-12 describes fields in the displayed MSTP information of GigabitEthernet 1/0/16 in MSTI 0.

Table 1-12 Fields in the displayed MSTP information of GigabitEthernet 1/0/16 in MSTI 0

Field	Description
[FORWARDING]	The port is in forwarding state: The port learns MAC addresses and forwards user traffic
[LEARNING]	The port is in learning state: The port learns MAC addresses but does not forward user traffic
[DISCARDING]	The port is in discarding state: The port does not learn MAC addresses or forward user traffic
[DOWN]	The port is down
Port Protocol	Whether STP is enabled on the port
Port Role	The role of the port, which can be Alternate, Backup, Root, Designated, Master, or Disabled
Port Priority	The priority of the port
Port Cost(Legacy)	Path cost of the port. The field in the bracket indicates the standard used for port path cost calculation, which can be **legacy**, **dot1d-1998**, or **dot1t**. **Config** indicates the configured value, and **Active** indicates the actual value.
Desg. Bridge/Port	Designated bridge ID and port ID of the port The port ID displayed is insignificant for a port that does not support port priority.
Port Edged	Whether the port is an edge port: • **Config** indicates the configured value • **Active** indicates the actual value.
Point-to-point	Whether the port is connected to a point-to-point link: • **Config** indicates the configured value • **Active** indicates the actual value.
Transmit Limit	The maximum number of packets sent within each Hello time
Protection Type	Protection type on the port, which can be one of the following: • Root: Root guard • Loop: Loop guard • BPDU: BPDU guard • None: No protection
MST BPDU Format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s. **Config** indicates the configured value, and **Active** indicates the actual value.
Port Config-Digest-Snooping	Whether digest snooping is enabled on the port
Rapid transition	Whether the current port rapidly transitions to the forwarding state

Field	Description
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI
PortTimes	Major parameters for the port: • Hello: Hello timer • MaxAge: Max Age timer • FWDly: Forward delay timer • MsgAge: Message Age timer • Remain Hop: Remaining hops
BPDU Sent	Statistics on sent BPDUs
BPDU Received	Statistics on received BPDUs
Protocol Status	Whether MSTP is enabled
Protocol Std.	MSTP standard
Version	MSTP version
CIST Bridge-Prio.	Priority of the current device in the CIST
MAC address	MAC address of the current device
Max age(s)	Maximum age of a configuration BPDU
Forward delay(s)	Port state transition delay, in seconds
Hello time(s)	Configuration BPDU transmission interval, in seconds
Max hops	Maximum hops of the current MST region

Return to MSTP configuration task list.

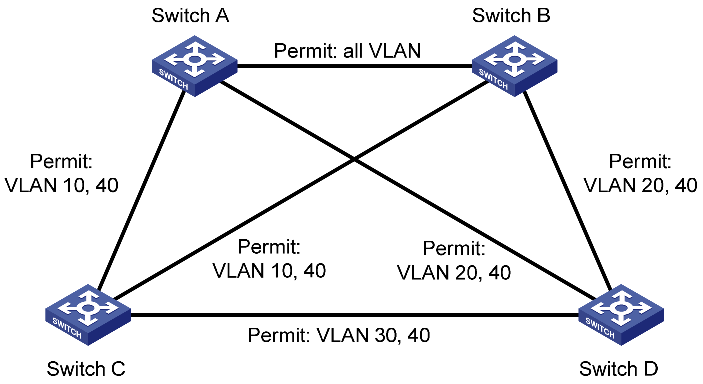
MSTP Configuration Example

Network requirements

Configure MSTP in the network shown in Figure 1-11 to enable packets of different VLANs to be forwarded along different MSTIs. The detailed configurations are as follows:

- All devices on the network are in the same MST region.
- Packets of VLAN 10, VLAN 20, VLAN 30, and VLAN 40 are forwarded along MSTI 1, MSTI 2, MSTI 3, and MSTI 0 respectively.
- Switch A and Switch B operate at the distribution layer; Switch C and Switch D operate at the access layer. VLAN 10 and VLAN 20 are terminated on the distribution layer devices, and VLAN 30 is terminated on the access layer devices, so the root bridges of MSTI 1 and MSTI 2 are Switch A and Switch B respectively, while the root bridge of MSTI 3 is Switch C.

Figure 1-11 Network diagram for MSTP configuration



Note

"Permit:" next to a link in the figure is followed by the VLANs the packets of which are permitted to pass this link.

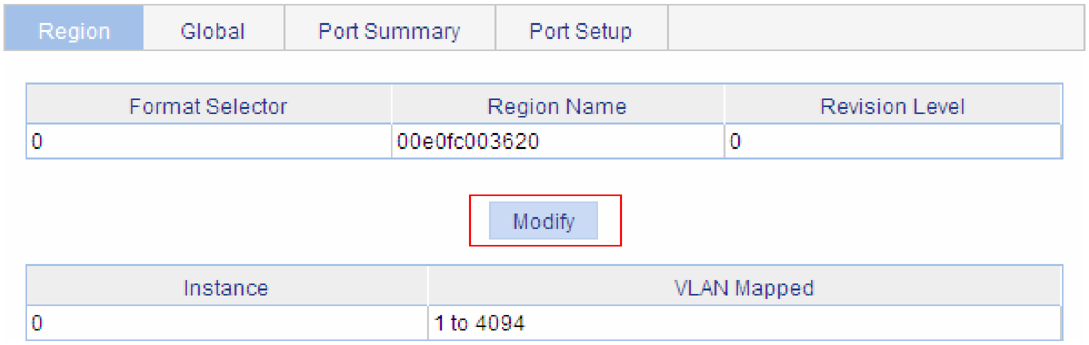
Configuration procedure

1) Configure Switch A.

# Configure an MST region.

- Select **Network > MSTP** from the navigation tree to enter the page shown in Figure 1-12.

Figure 1-12 The **Region** tab

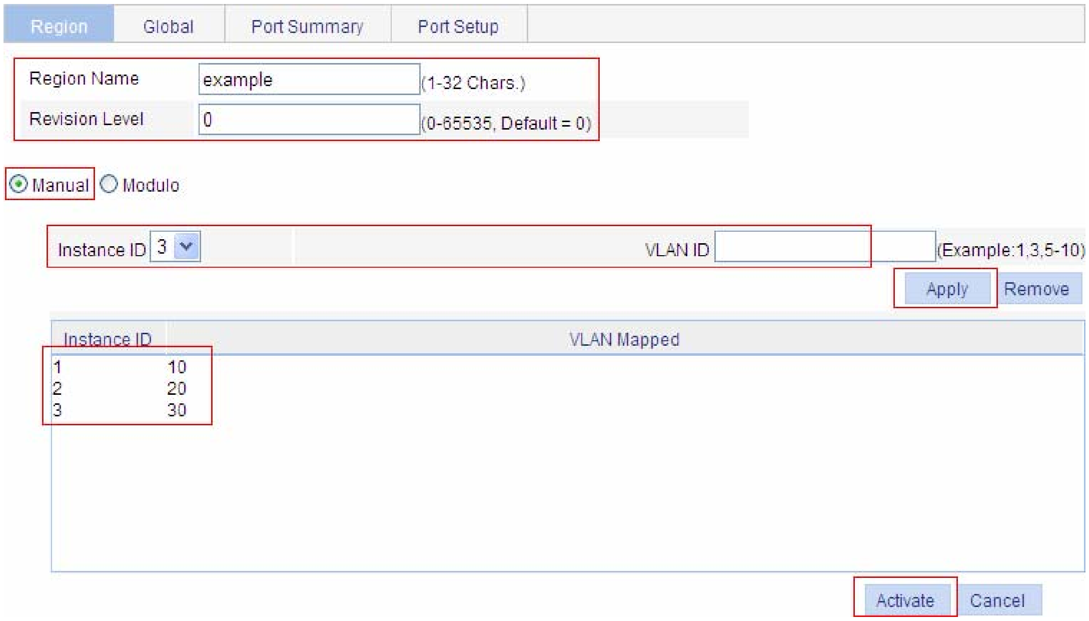


Format Selector	Region Name	Revision Level
0	00e0fc003620	0

Instance	VLAN Mapped
0	1 to 4094

- Click **Modify** to enter the page for configuring MST regions, as shown in Figure 1-13.

Figure 1-13 Configure an MST region



Region Name: example (1-32 Chars.)

Revision Level: 0 (0-65535, Default = 0)

● Manual ○ Modulo

Instance ID: 3

VLAN ID: (Example:1,3,5-10)

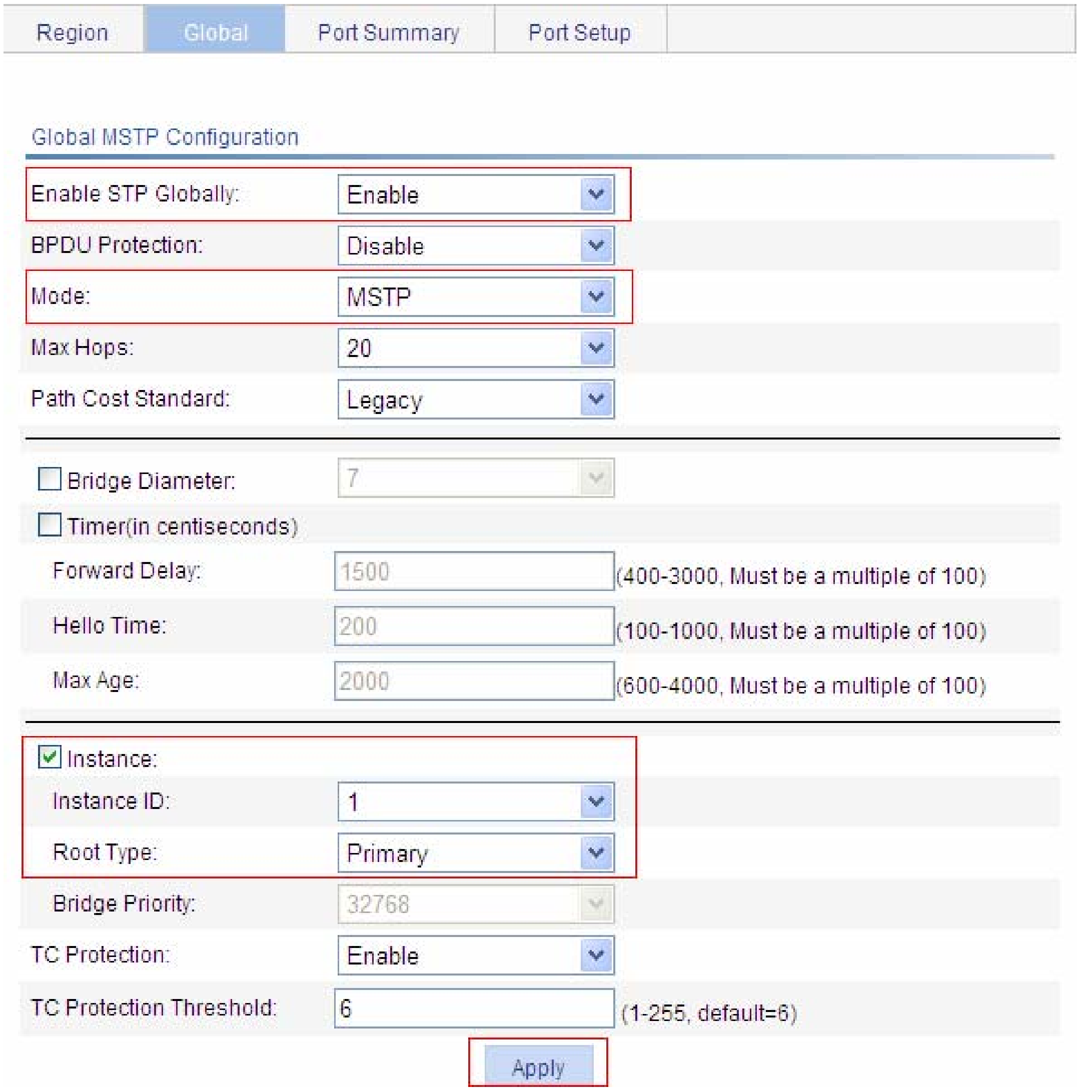
Instance ID	VLAN Mapped
1	10
2	20
3	30

- Set the region name to **example**.
- Set the revision level to 0.
- Select the **Manual** radio button.
- Select 1 in the **Instance ID** drop-down list.
- Set the VLAN ID to 10.
- Click **Apply** to map VLAN 10 to MSTI 1 and add the VLAN-to-MSTI mapping entry to the VLAN-to-MSTI mapping list.
- Repeat the steps above to map VLAN 20 to MSTI 2 and VLAN 30 to MSTI 3 and add the VLAN-to-MSTI mapping entries to the VLAN-to-MSTI mapping list.
- Click **Activate**.

# Configure MSTP globally.

- Select **Network > MSTP** from the navigation tree, and then click **Global** to enter the page for configuring MSTP globally, as shown in Figure 1-14.

Figure 1-14 Configure MSTP globally (on Switch A)



Global MSTP Configuration

Enable STP Globally:	Enable	
BPDU Protection:	Disable	
Mode:	MSTP	
Max Hops:	20	
Path Cost Standard:	Legacy	
□ Bridge Diameter:	7	
□ Timer(in centiseconds)		
Forward Delay:	1500	(400-3000, Must be a multiple of 100)
Hello Time:	200	(100-1000, Must be a multiple of 100)
Max Age:	2000	(600-4000, Must be a multiple of 100)
☑ Instance:		
Instance ID:	1	
Root Type:	Primary	
Bridge Priority:	32768	
TC Protection:	Enable	
TC Protection Threshold:	6	(1-255, default=6)

- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the check box before **Instance**.
- Set the **Instance ID** field to 1.
- Set the **Root Type** field to **Primary**.
- Click **Apply**.

2) Configure Switch B.

# Configure an MST region. (The procedure here is the same as that of configuring an MST region on Switch A.)

# Configure MSTP globally.

- Select **Network > MSTP** from the navigation tree, and then click **Global** to enter the page for configuring MSTP globally. See Figure 1-14.
- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the check box before **Instance**.
- Set the **Instance ID** field to 2.

- Set the **Root Type** field to **Primary**.
- Click **Apply**.

3) Configure Switch C.

# Configure an MST region. (The procedure here is the same as that of configuring an MST region on Switch A.)

# Configure MSTP globally.

- Select **Network > MSTP** from the navigation tree, and then click **Global** to enter the page for configuring MSTP globally. See Figure 1-14.
- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the check box before **Instance**.
- Set the **Instance ID** field to 3.
- Set the **Root Type** field to **Primary**.
- Click **Apply**.

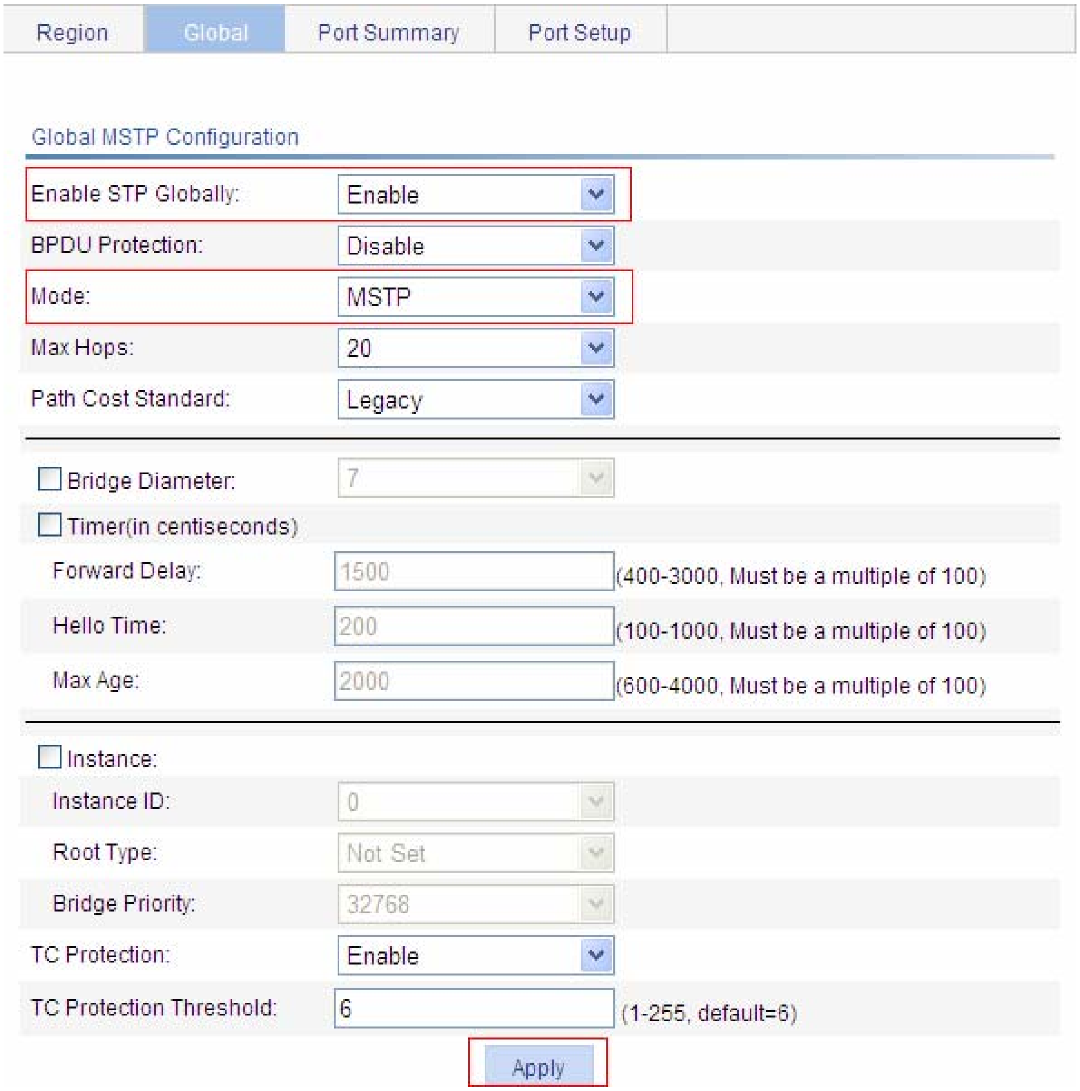
4) Configure Switch D.

# Configure an MST region. (The procedure here is the same as that of configuring an MST region on Switch A.)

# Configure MSTP globally.

- Select **Network > MSTP** from the navigation tree, and then click **Global** to enter the page for configuring MSTP globally, as shown in Figure 1-15.

Figure 1-15 Configure MSTP globally (on Switch D)



Global MSTP Configuration

Enable STP Globally: Enable

BPDU Protection: Disable

Mode: MSTP

Max Hops: 20

Path Cost Standard: Legacy

□ Bridge Diameter: 7

□ Timer(in centiseconds)

Forward Delay: 1500 (400-3000, Must be a multiple of 100)

Hello Time: 200 (100-1000, Must be a multiple of 100)

Max Age: 2000 (600-4000, Must be a multiple of 100)

□ Instance:

Instance ID: 0

Root Type: Not Set

Bridge Priority: 32768

TC Protection: Enable

TC Protection Threshold: 6 (1-255, default=6)

- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Click **Apply**.

Guidelines

Follow these guidelines when configuring MSTP:

- Two devices belong to the same MST region only if they are interconnected through physical links, and share the same region name, the same MSTP revision level, and the same VLAN-to-MSTI mappings.
- If two or more devices have been designated to be root bridges of the same spanning tree instance, MSTP will select the device with the lowest MAC address as the root bridge.
- If the device is not enabled with BPDU guard, when a boundary port receives a BPDU from another port, it transits into a non-boundary port. To restore its port role as a boundary port, you need to restart the port.

- Configure ports that are directly connected to terminals as boundary ports and enable BPDU guard for them. In this way, these ports can rapidly transit to the forwarding state, and the network security can be ensured.

Table of Contents

1 Link Aggregation and LACP Configuration

Overview

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group.

It allows you to increase bandwidth by distributing traffic across the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

Basic Concepts of Link Aggregation

Aggregate interface

An aggregate interface is a logical Layer 2 or Layer 3 aggregate interface.

Note

The current device only supports Layer 2 aggregation interface.

Aggregation group

An aggregation group is a collection of Ethernet interfaces. When you create an aggregate interface, an aggregation group numbered the same is created automatically depending on the type of the aggregate interface:

- If the aggregate interface is a Layer 2 interface, a Layer 2 aggregation group is created. You can assign only Layer 2 Ethernet interfaces to the group.
- If the aggregate interface is a Layer 3 interface, a Layer 3 aggregation group is created. You can assign only Layer 3 Ethernet interfaces to the group.

Note

The current device only supports Layer 2 aggregation group

States of the member ports in an aggregation group

A member port in an aggregation group can be in one of the following two states:

- Selected: a selected port can forward user traffic.
- Unselected: an unselected port cannot forward user traffic.

The rate of an aggregate interface is the sum of the selected member ports' rates. The duplex mode of an aggregate interface is consistent with that of the selected member ports. Note that all selected member ports use the same duplex mode.

For how the state of a member port is determined, refer to Static aggregation mode and Dynamic aggregation mode.

LACP protocol

The Link Aggregation Control Protocol (LACP) is defined in IEEE 802.3ad. It uses link aggregation control protocol data units (LACPDUs) for information exchange between LACP-enabled devices.

LACP is automatically enabled on interfaces in a dynamic aggregation group. For information about dynamic aggregation groups, refer to Dynamic aggregation mode. An LACP-enabled interface sends LACPDUs to notify the remote system (the partner) of its system LACP priority, system MAC address, LACP port priority, port number, and operational key. Upon receiving an LACPDU, the partner compares the received information with the information received on other interfaces to determine the interfaces that can operate as selected interfaces. This allows the two systems to reach an agreement on which link aggregation member ports should be placed in selected state.

Operational key

When aggregating ports, link aggregation control automatically assigns each port an operational key based on port attributes, including the port rate, duplex mode and link state configuration.

In an aggregation group, all selected ports are assigned the same operational key.

Class-two configurations

The contents of class-two configurations are listed in Table 1-1. In an aggregation group, a member port different from the aggregate interface in the class-two configurations cannot be a selected port.

Table 1-1 Class-two configurations

Type	Considerations
Port isolation	Whether a port has joined an isolation group
VLAN	Permitted VLAN IDs, default VLAN, link type (trunk, hybrid, or access), ,tag mode

Note

- Some configurations are called class-one configurations. Such configurations, for example, MSTP, can be configured on aggregate interfaces and member ports but are not considered during operational key calculation. For details of MSTP configuration on member ports of link aggregation groups or aggregate interfaces, see related sections in *MSTP Configuration.*
- The change of a class-two configuration setting may affect the select state of link aggregation member ports and thus the ongoing service. To prevent unconsidered change, a message warning of the hazard will be displayed when you attempt to change a class-two setting, upon which you can decide whether to continue your change operation. For details of port isolation configuration and VLAN configuration on member ports of link aggregation groups or aggregate interfaces, see related sections in *Port Isolation Configuration* and *VLAN Configuration*.

Link Aggregation Modes

Depending on the link aggregation procedure, link aggregation operates in one of the following two modes:

- Static aggregation mode
- Dynamic aggregation mode

Static aggregation mode

LACP is disabled on the member ports in a static aggregation group. In a static aggregation group, the system sets a port to selected or unselected state by the following rules:

- Select a port as the reference port from the ports that are in up state and with the same class-two configurations as the corresponding aggregate interface. These ports are selected in the order of full duplex/high speed, full duplex/low speed, half duplex/high speed, and half duplex/low speed, with full duplex/high speed being the most preferred. If two ports with the same duplex mode/speed pair are present, the one with the lower port number wins out.
- Consider the ports in up state with the same port attributes and class-two configurations as the reference port as candidate selected ports, and set all others in the unselected state.
- Static aggregation limits the number of selected ports in an aggregation group. When the number of the candidate selected ports is under the limit, all the candidate selected ports become selected ports. When the limit is exceeded, set the candidate selected ports with smaller port numbers in the selected state and those with greater port numbers in the unselected state.
- If all the member ports are down, set their states to unselected.
- Set the ports that cannot aggregate with the reference port to the unselected state.

⚠ **Caution**

A port that joins the aggregation group after the limit on the number of selected ports has been reached will not be placed in the selected state even if it should be in normal cases. This can prevent the ongoing traffic on the current selected ports from being interrupted. You should avoid the situation however, as this may cause the selected/unselected state of a port to change after a reboot.

Dynamic aggregation mode

LACP is enabled on member ports in a dynamic aggregation group.

In a dynamic aggregation group,

- A selected port can receive and transmit LACPDUs.
- An unselected port can receive and send LACPDUs only if it is up and with the same configurations as those on the aggregate interface.

In a dynamic aggregation group, the system sets the ports to selected or unselected state in the following steps:

1) The local system (the actor) negotiates with the remote system (the partner) to determine port state based on the port IDs on the end with the preferred system ID. The following is the detailed negotiation procedure:

- Compare the system ID (comprising the system LACP priority and the system MAC address) of the actor with that of the partner. The system with the lower LACP priority wins out. If they are the same, compare the system MAC addresses. The system with the smaller MAC address wins out.
- Compare the port IDs of the ports on the system with the smaller system ID. A port ID comprises a port LACP priority and a port number. First compare the port LACP priorities. The port with the lower LACP priority wins out. If two ports are with the same LACP priority, compare their port numbers. The port with the smaller port ID, that is, the port with smaller port number, is selected as the reference port.
- If a port (in up state) is with the same port attributes and class-two configuration as the reference port, and the peer port of the port is with the same port attributes and class-two configurations as the peer port of the reference port, consider the port as a candidate selected port; otherwise set the port to the unselected state.
- The number of selected ports that an aggregation group can contain is limited. When the number of candidate selected ports is under the limit, all the candidate selected ports are set to selected state. When the limit is exceeded, the system selects the candidate selected ports with smaller port IDs as the selected ports, and set other candidate selected ports to unselected state. At the same time, the peer device, being aware of the changes, changes the state of its ports accordingly.

2) Set the ports that cannot aggregate with the reference port to the unselected state.

Note

For static and dynamic aggregation modes:

- In an aggregation group, the port to be a selected port must be the same as the reference port in port attributes, and class-two configurations. To keep these configurations consistent, you should configure the port manually.
- Because changing a port attribute or class-two configuration setting of a port may cause the select state of the port and other member ports to change and thus affects services, you are recommended to do that with caution.

Load Sharing Mode of an Aggregation Group

Every link aggregation group created on 3Com Switch 2900 operates in load sharing mode all the time, that is, even when it contains only one member port.

Configuring Link Aggregation and LACP

Configuration Task List

Configuring a static aggregation group

Perform the tasks in Table 1-2 to configure a static aggregation group.

Table 1-2 Static aggregation group configuration task list

Task	Remarks
Creating a Link Aggregation Group	Required Create a static aggregate interface and configure member ports for the static aggregation group automatically created by the system when you create the aggregate interface. By default, no link aggregation group exists.
Displaying Information of an Aggregate Interface	Optional Perform this task to view detailed information of an existing aggregation group.

Configuring a dynamic aggregation group

Perform the tasks in Table 1-3 to configure a dynamic aggregation group.

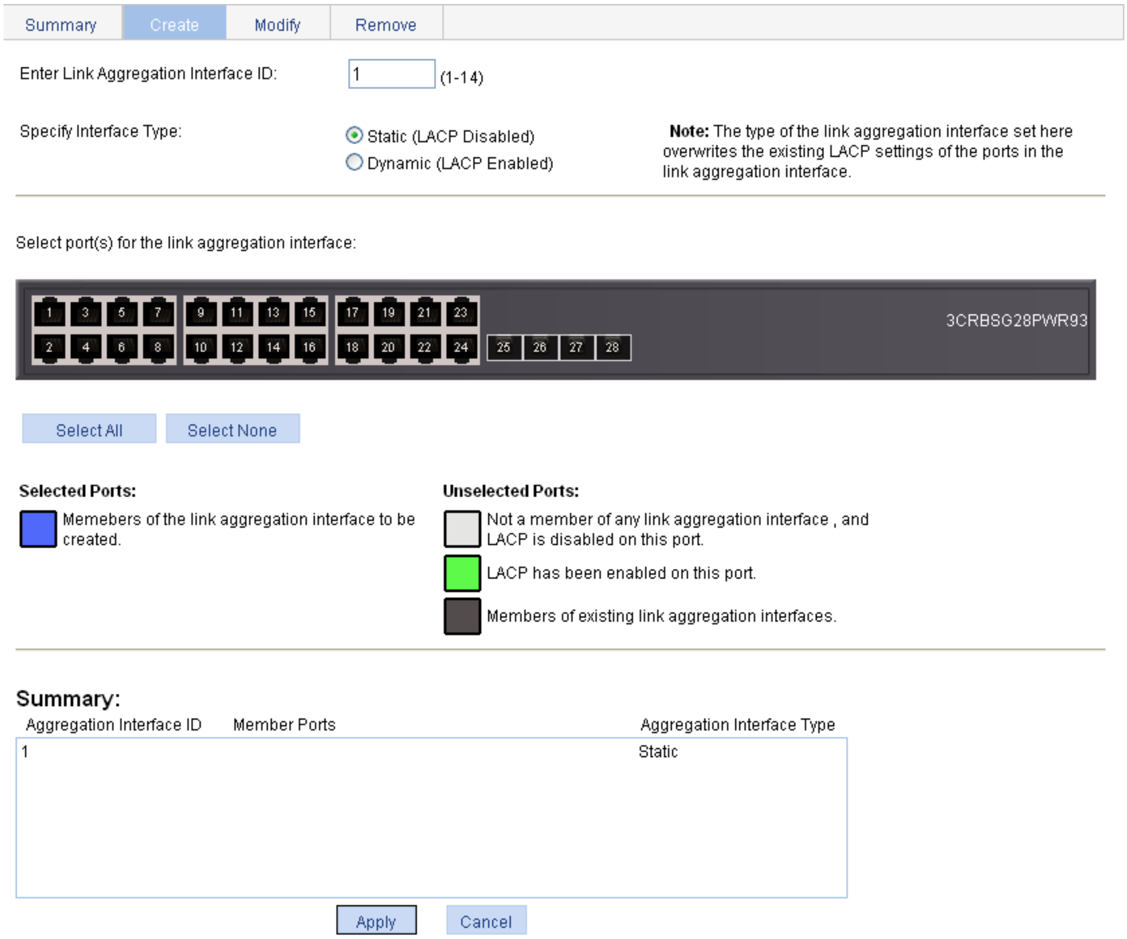
Table 1-3 Dynamic aggregation group configuration task list

Task	Remarks
Creating a Link Aggregation Group	Required Create a dynamic aggregate interface and configure member ports for the dynamic aggregation group automatically created by the system when you create the aggregate interface. LACP is enabled automatically on all the member ports. By default, no link aggregation group exists.
Displaying Information of an Aggregate Interface	Optional Perform this task to view detailed information of an existing aggregation group.
Setting LACP Priority	Optional Perform the task to set LACP priority for the local system and link aggregation member ports. Changes of LACP priorities affect the selected/unselected state of link aggregation member ports. The default port LACP priority and system LACP priority are both 32768.
Displaying Information of LACP-Enabled Ports	Optional Perform the task to view detailed information of LACP-enabled ports and the corresponding remote (partner) ports.

Creating a Link Aggregation Group

Select **Network** > **Link Aggregation** from the navigation tree, and then click **Create** to enter the page as shown in Figure 1-1.

Figure 1-1 Create a link aggregation group



Enter Link Aggregation Interface ID: 1 (1-14)

Specify Interface Type: ● Static (LACP Disabled) ○ Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

Selected Ports:

🟦 Memebers of the link aggregation interface to be created.

Unselected Ports:

⬜ Not a member of any link aggregation interface , and LACP is disabled on this port.

🟩 LACP has been enabled on this port.

⬛ Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1		Static

Table 1-4 describes the configuration items of creating a link aggregation group.

Table 1-4 Configuration items of creating a link aggregation group

Item	Description
Enter Link Aggregation Interface ID	Assign an ID to the link aggregation group to be created. You can view the result in the **Summary** list box at the bottom of the page.
Specify Interface Type	Set the type of the link aggregation interface to be created: • Static (LACP Disabled) • Dynamic (LACP Enabled)
Select port(s) for the link aggregation interface	Select one or multiple ports to be assigned to the link aggregation group from the chassis front panel. You can view the result in the **Summary** list box at the bottom of the page.

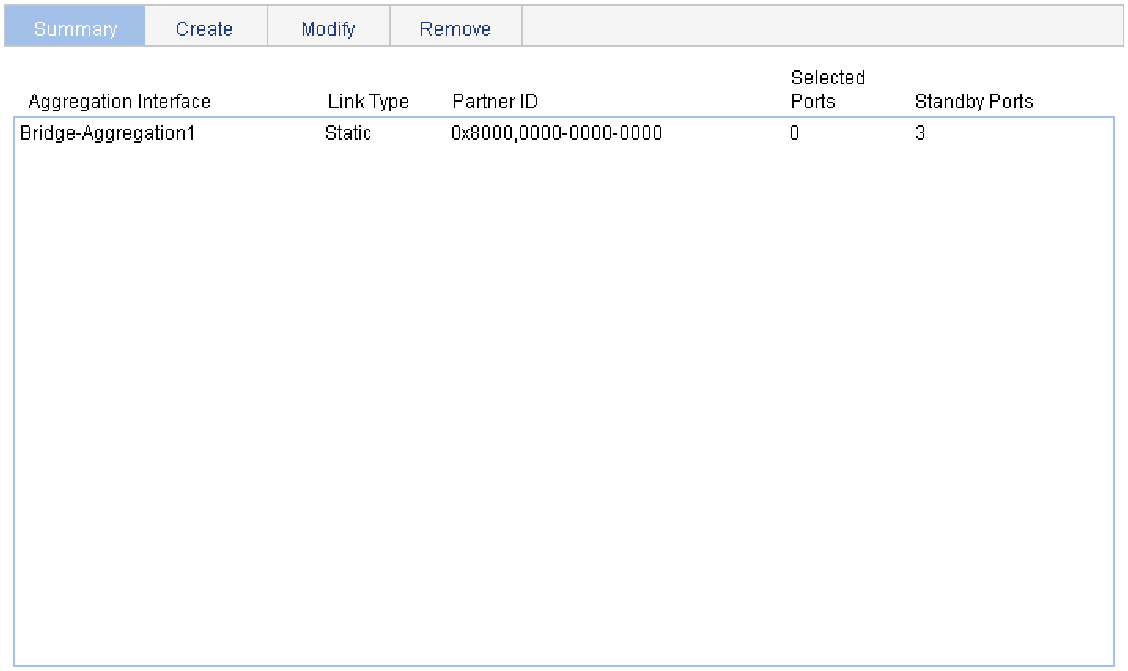
Return to Static aggregation group configuration task list.

Return to Dynamic aggregation group configuration task list.

Displaying Information of an Aggregate Interface

Select **Network** > **Link Aggregation** from the navigation tree. The **Summary** tab is displayed by default, as shown in Figure 1-2.

Figure 1-2 Display information of an aggregate interface



Aggregation Interface	Link Type	Partner ID	Selected Ports	Standby Ports
Bridge-Aggregation1	Static	0x8000,0000-0000-0000	0	3

Table 1-5 describes the fields on the **Summary** tab.

Table 1-5 Fields on the Summary tab

Field	Description
Aggregation interface	Type and ID of the aggregate interface **Bridge-Aggregation** indicates a Layer 2 aggregate interface
Link Type	Type of the aggregate interface, which can be static or dynamic
Partner ID	ID of the remote device, including its LACP priority and MAC address
Selected Ports	Number of selected ports in each link aggregation group (Only selected ports can transmit and receive user data)
Standby Ports	Number of unselected ports in each link aggregation group (Unselected ports cannot transmit or receive user data)

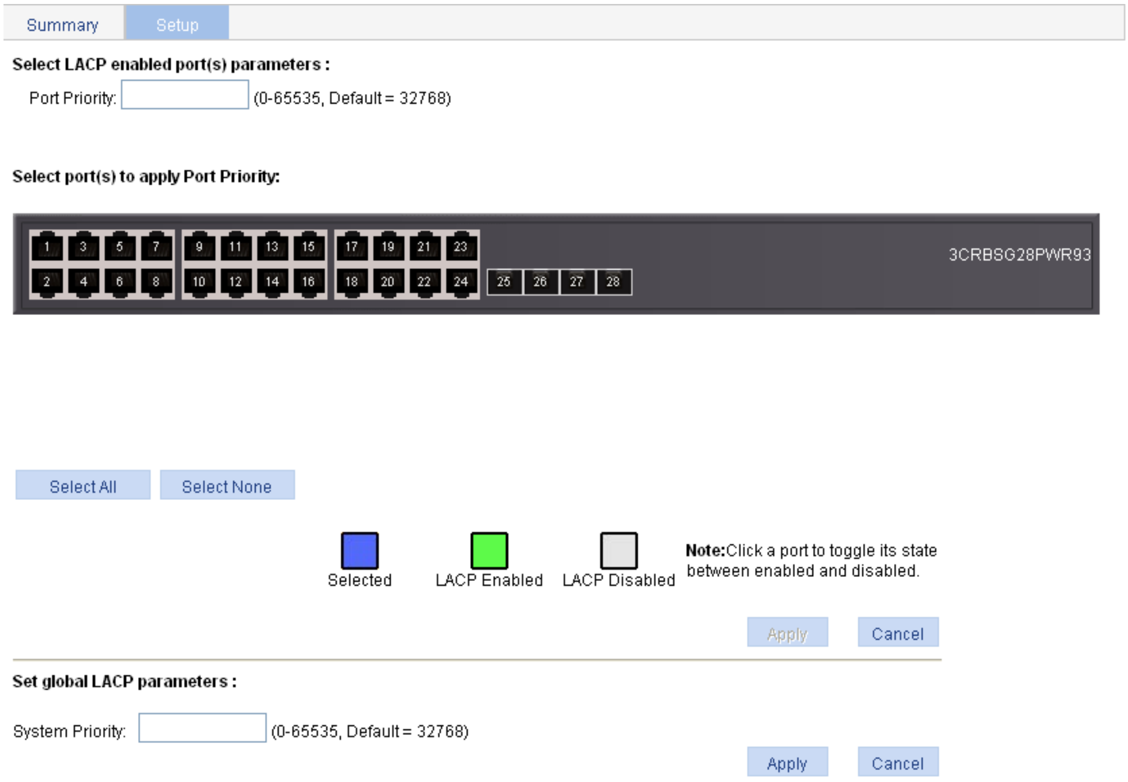
Return to Static aggregation group configuration task list.

Return to Dynamic aggregation group configuration task list.

Setting LACP Priority

Select **Network** > **LACP** from the navigation tree, and then click **Setup** to enter the page shown in Figure 1-3.

Figure 1-3 The **Setup** tab



Select LACP enabled port(s) parameters :

Port Priority: (0-65535, Default = 32768)

Select port(s) to apply Port Priority:

Note: Click a port to toggle its state between enabled and disabled.

Set global LACP parameters :

System Priority: (0-65535, Default = 32768)

After finishing each configuration item, click the right **Apply** button to submit the configuration.

Table 1-6 describes the configuration items.

Table 1-6 LACP priority configuration items

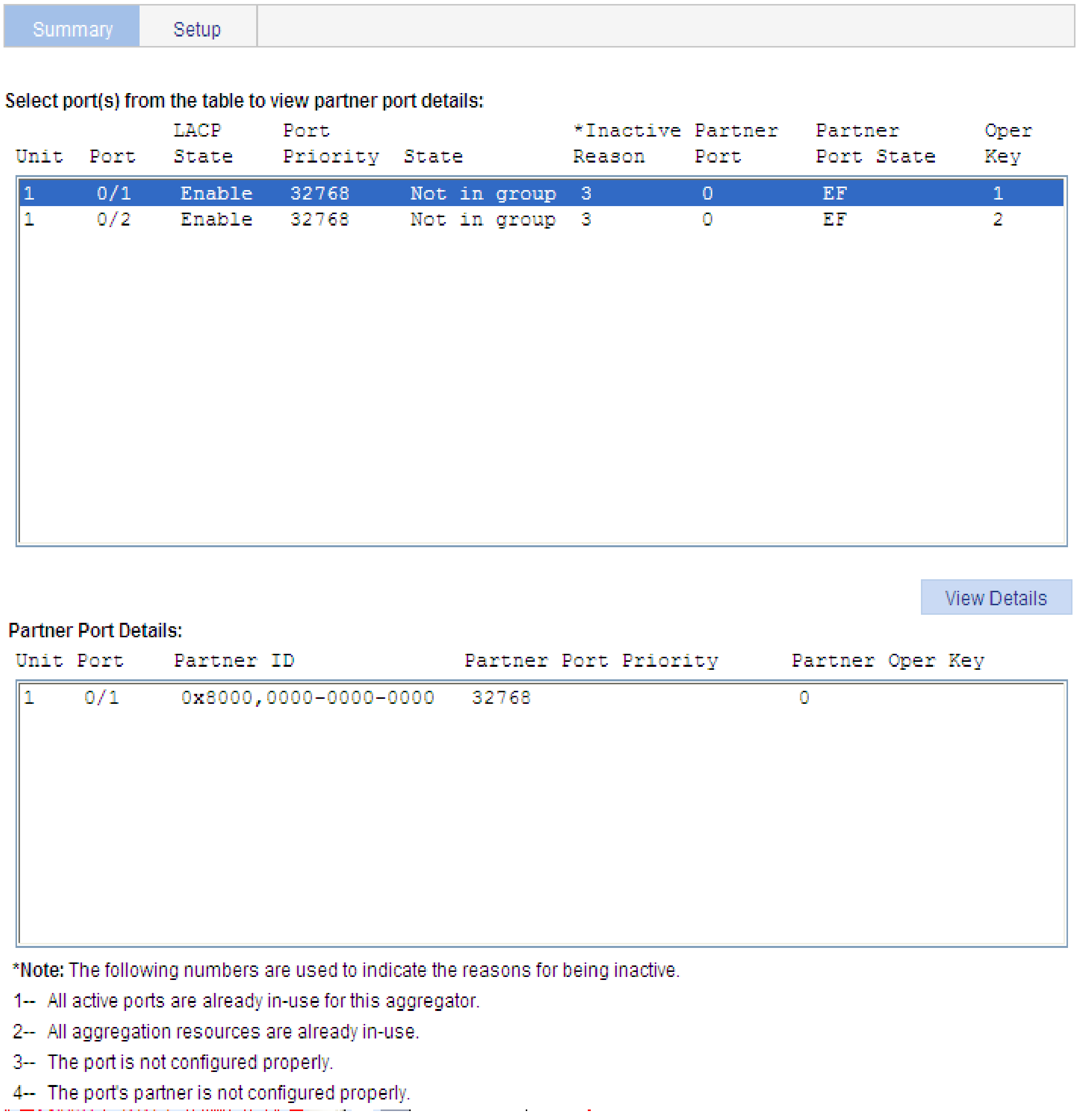
Item	Description
Select LACP enabled port(s) parameters	Set a port LACP priority.
Select port(s) to apply Port Priority	Select the ports where the port LACP priority you set will apply on the chassis front panel. (You can set LACP priority not only on LACP-enabled ports but also on LACP-disabled ports.)
System Priority	Set the LACP priority of the local system

Return to Dynamic aggregation group configuration task list.

Displaying Information of LACP-Enabled Ports

Select **Network** > **LACP** from the navigation tree. The **Summary** tab is displayed by default, as shown in Figure 1-4.

Figure 1-4 Display the information of LACP-enabled ports



Select port(s) from the table to view partner port details:

Unit	Port	LACP State	Port Priority	State	*Inactive Reason	Partner Port	Partner Port State	Oper Key
1	0/1	Enable	32768	Not in group	3	0	EF	1
1	0/2	Enable	32768	Not in group	3	0	EF	2

Partner Port Details:

Unit	Port	Partner ID	Partner Port Priority	Partner Oper Key
1	0/1	0x8000,0000-0000-0000	32768	0

***Note:** The following numbers are used to indicate the reasons for being inactive.

1-- All active ports are already in-use for this aggregator.

2-- All aggregation resources are already in-use.

3-- The port is not configured properly.

4-- The port's partner is not configured properly.

The upper part of the page displays a list of all LACP-enabled ports on the device and information about them. To view information about the partner port of a LACP-enabled port, select it in the port list, and then click **View Details**. Detailed information about the peer port will be displayed on the lower part of the page.

Table 1-7 describes the fields on the **Summary** tab.

Table 1-7 Fields in the LACP-enabled port summary table

Field/button	Description
Unit	The ID of a device in a stack
Port	Port where LACP is enabled
LACP State	State of LACP on the port
Port Priority	LACP priority of the port
State	Active state of the port. If a port is selected, its state is active and the ID of the aggregation group it belongs to will be displayed.

Field/button	Description
Inactive Reason	Reason code indicating why a port is inactive (that is, unselected) for receiving/transmitting user data. For the meanings of the reason codes, see the bottom of the page shown in Figure 1-4.
Partner Port	Name of the peer port
Partner Port State	State information of the peer port, represented by letters A through H. • A indicates that LACP is enabled. • B indicates that LACP short timeout has occurred. If B does not appear, it indicates that LACP long timeout has occurred. • C indicates that the link is considered as aggregatable by the sending system. • D indicates that the link is considered as synchronized by the sending system. • E indicates that the sending system considers that collection of incoming frames is enabled on the link. • F indicates that the sending system considers that distribution of outgoing frames is enabled on the link. • G indicates that the receive state machine of the sending system is using the default operational partner information. • H indicates that the receive state machine of the sending system is in the expired state.
Oper Key	Operational key of the local port

Table 1-8 describes the fields in the **Partner Port Details** table

Table 1-8 Fields in the Partner Port Details table

Field	Description
Unit	Number of the remote system
Port	Name of the remote port
Partner ID	LACP priority and MAC address of the remote system
Partner Port Priority	LACP priority of the remote port
Partner Oper Key	Operational key of the remote port

Return to Dynamic aggregation group configuration task list.

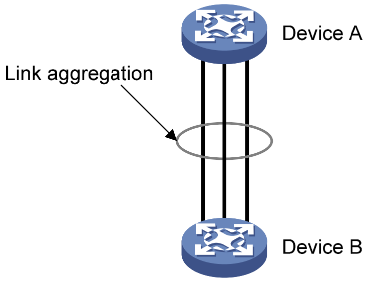
Link Aggregation and LACP Configuration Example

Network requirements

As shown in Figure 1-5, Switch A and Switch B are connected to each other through their Layer 2 Ethernet ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

Aggregate the ports on each device to form a link aggregation group, thus balancing incoming/outgoing traffic across the member ports.

Figure 1-5 Network diagram for static link aggregation configuration



Configuration procedure

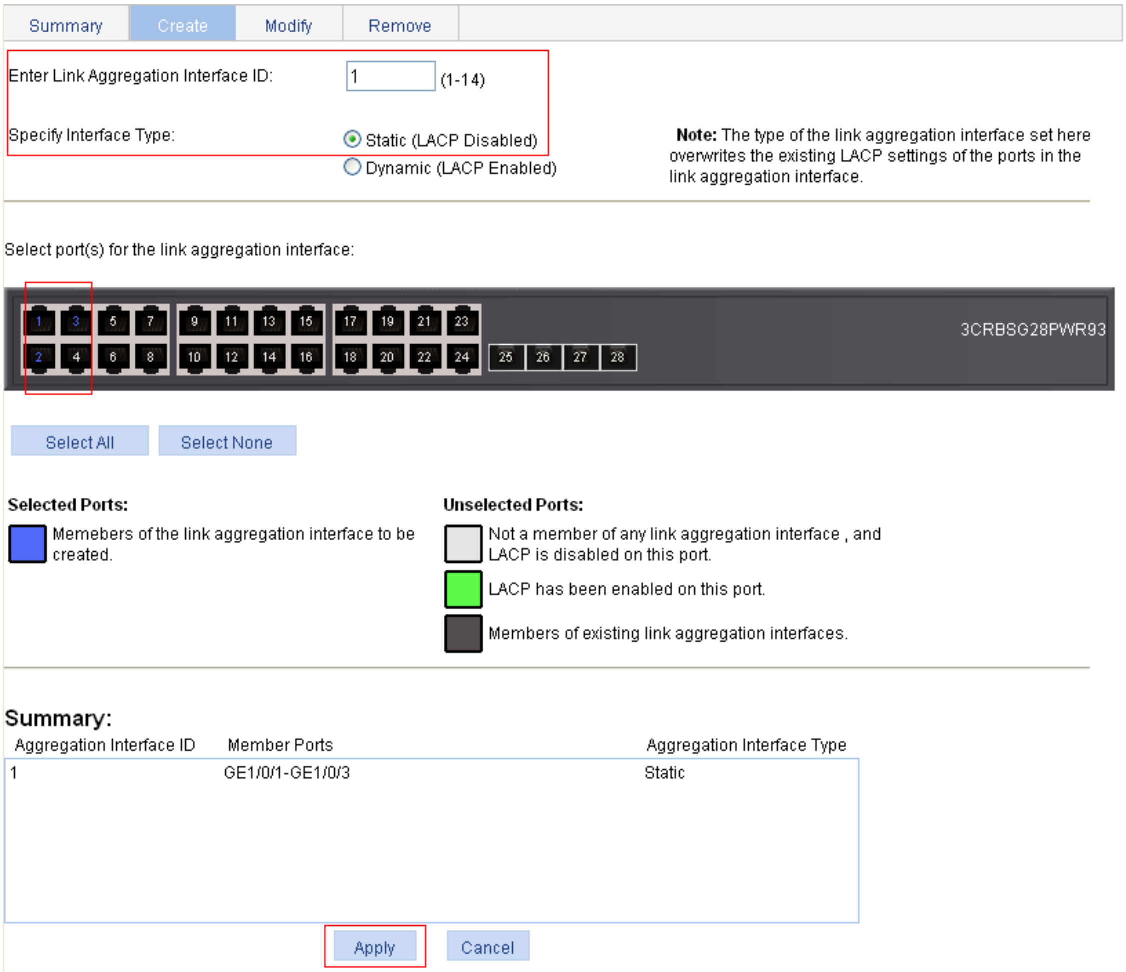
You can create a static or dynamic link aggregation group to achieve load balancing.

1) Approach 1: Create a static link aggregation group

# Create static link aggregation group 1.

Select **Network** > **Link Aggregation** from the navigation tree, and then click **Create** to enter the page as shown in Figure 1-6.

Figure 1-6 Create static link aggregation group 1



Enter Link Aggregation Interface ID: 1 (1-14)

Specify Interface Type: ● Static (LACP Disabled) ○ Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

Selected Ports:

■ Memebers of the link aggregation interface to be created.

Unselected Ports:

□ Not a member of any link aggregation interface , and LACP is disabled on this port.

🟩 LACP has been enabled on this port.

■ Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1	GE1/0/1-GE1/0/3	Static

- Set the link aggregation interface ID to **1.**
- Select the **Static (LACP Disabled)** option for the aggregate interface type.

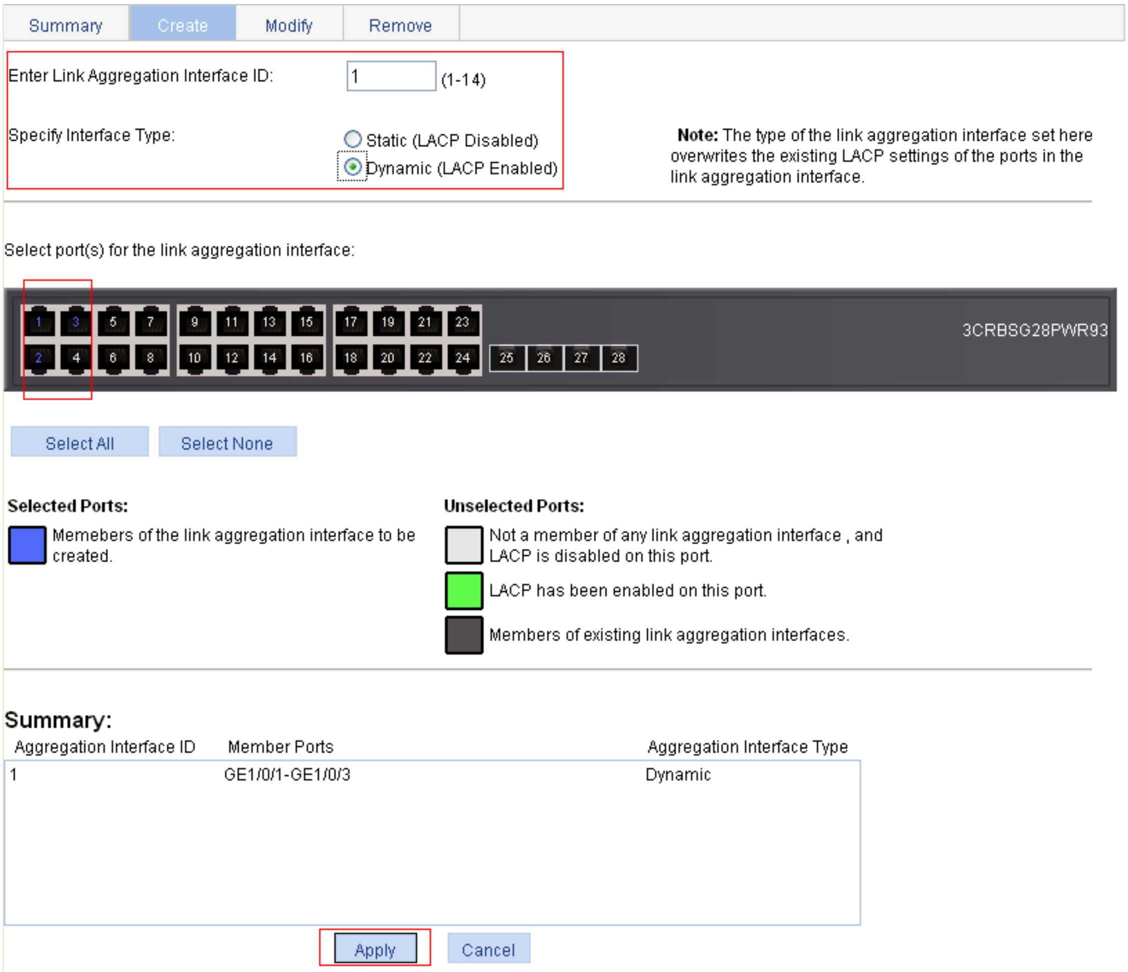
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**.

2) Approach 2: Create a dynamic link aggregation group

# Create dynamic link aggregation group 1.

Select **Network** > **Link Aggregation** from the navigation tree, and then click **Create** to enter the page as shown in Figure 1-7.

Figure 1-7 Create dynamic link aggregation group 1



Enter Link Aggregation Interface ID: 1 (1-14)

Specify Interface Type: ○ Static (LACP Disabled) ● Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

Selected Ports:

🟦 Memebers of the link aggregation interface to be created.

Unselected Ports:

□ Not a member of any link aggregation interface , and LACP is disabled on this port.

🟩 LACP has been enabled on this port.

■ Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1	GE1/0/1-GE1/0/3	Dynamic

- Set the link aggregation interface ID to **1**.
- Select the **Dynamic (LACP Enabled)** option for aggregate interface type.
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**.

Configuration Guidelines

Follow these guidelines when configuring a link aggregation group:

- In an aggregation group, the port to be a selected port must be the same as the reference port in port attributes, and class-two configurations. To keep these configurations consistent, you should configure the port manually.

- Reference port: Select a port as the reference port from the ports that are in up state and with the same class-two configurations as the corresponding aggregate interface. The selection order is as follows: full duplex/high speed, full duplex/low speed, half duplex/high speed, and half duplex/low speed, with full duplex/high speed being the most preferred. If two ports with the same duplex mode/speed pair are present, the one with the lower port number wins out.
- Port attribute configuration includes the configuration of the port rate, duplex mode, and link state.
- For details about class-two configurations, see section Class-two configurations.
- To guarantee a successful static aggregation, ensure that the ports at the two ends of each link to be aggregated are consistent in the selected/unselected state; to guarantee a successful dynamic aggregation, ensure that the peer ports of the ports aggregated at one end are also aggregated. The two ends can automatically negotiate the selected state of the ports.
- Removing a Layer 2 aggregate interface also removes the corresponding aggregation group. Meanwhile, the member ports of the aggregation group, if any, leave the aggregation group.

Table of Contents

1 LLDP

Overview

Background

In a heterogeneous network, it is important that different types of network devices from different vendors can discover one other and exchange configuration for interoperability and management sake. This calls for a standard configuration exchange platform.

To address the needs, the IETF drafted the Link Layer Discovery Protocol (LLDP) in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDPDUs to the directly connected devices, and at the same time, stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). It allows a network management system to fast detect Layer-2 network topology change and identify what the change is.

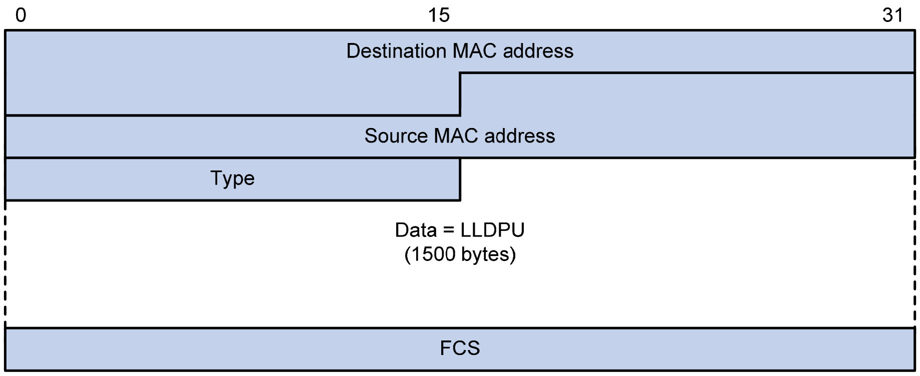
Basic Concepts

LLDPDUs

LLDP sends device information in LLDP data units (LLDPDUs). LLDPDUs are encapsulated in Ethernet II or SNAP frames.

1) LLDPDUs encapsulated in Ethernet II

Figure 1-1 LLDPDU encapsulated in Ethernet II



The fields in the frame are described in Table 1-1:

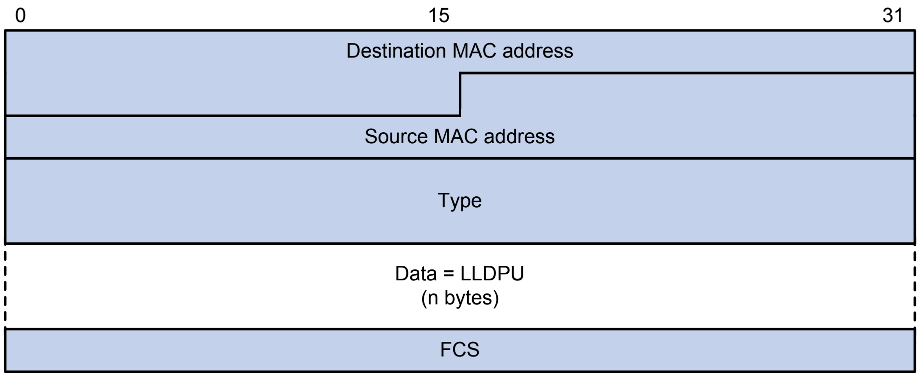
Table 1-1 Description of the fields in an Ethernet II encapsulated LLDPDU

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.

Field	Description
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The Ethernet type for the upper layer protocol. It is 0x88CC for LLDP.
Data	LLDP data.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

2) LLDPDUs encapsulated in SNAP

Figure 1-2 LLDPDU encapsulated in SNAP



The fields in the frame are described in Table 1-2:

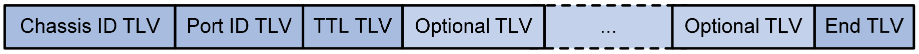
Table 1-2 Description of the fields in a SNAP encapsulated LLDPDU

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The SNAP-encoded LLDP Ethernet type for the upper layer protocol. It is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDP data unit.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDPDUs

LLDP uses LLDPDUs to exchange information. An LLDPDU comprises multiple type, length, and value (TLV) sequences, each carrying a type of device information, as shown in Figure 1-3.

Figure 1-3 An LLDPDU



An LLDPDU can carry up 28 types of TLVs, of which the chassis ID TLV, port ID TLV, TTL TLV, and end of LLDPDU TLV (end TLV in the figure) are mandatory TLVs that must be carried and other TLVs are optional.

TLVs

TLVs are type, length, and value sequences that carry information elements, where the type field identifies the type of information, the length field indicates the length of the information field in octets, and the value field contains the information itself.

LLDPDU TLVs fall into these categories: basic management TLVs, organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs, and LLDP-MED (media endpoint discovery) TLVs. Basic management TLVs are essential to device management. Organizationally specific TLVs and LLDP-MED TLVs are used for enhanced device management; they are defined by standardization or other organizations and thus are optional to LLDPDUs.

1) Basic management TLVs

Table 1-3 lists the basic management TLV types currently in use. Some of them are mandatory to LLDPDUs, that is, must be included in every LLDPDU.

Table 1-3 Basic LLDP TLVs

Type	Description	Remarks
Chassis ID	Bridge MAC address of the sending device.	Mandatory
Port ID	ID of the sending port. If MED TLVs are included in the LLDPDU, the port ID TLV carries the MAC address of the sending port or the bridge MAC in case the port does not have a MAC address. If no MED TLVs are included, the port ID TLV carries the port name.	
Time To Live	Life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	
Port Description	Port description of the sending port.	Optional
System Name	Assigned name of the sending device.	
System Description	Description of the sending device.	
System Capabilities	Identifies the primary functions of the sending device and the primary functions that have been enabled.	
Management Address	Management address used to reach higher level entities to assist discovery by network management, and the interface number and OID (object identifier) associated with the address.	

2) IEEE 802.1 organizationally specific TLVs

Table 1-4 IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID	PVID of the sending port
Port And Protocol VLAN ID	Port and protocol VLAN IDs

Type	Description
VLAN Name	A specific VLAN name on the port
Protocol Identity	Protocols supported on the port

Note

Currently, 3Com Switch 2900 supports receiving but not sending protocol identity TLVs.

3) IEEE 802.3 organizationally specific TLVs

Table 1-5 IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the rate and duplex capabilities of the sending port, support for auto negotiation, enabling status of auto negotiation, and the current rate and duplex mode.
Power Via MDI	Contains Power supply capability of the port.
Link Aggregation	Indicates the support of the port for link aggregation, the aggregation capability of the port, and the aggregation status (that is, whether the link is in an aggregation).
Maximum Frame Size	Indicates the supported maximum frame size. It is now the MTU of the port.

LLDP-MED TLVs

LLDP-MED TLVs provide multiple advanced applications for voice over IP (VoIP), such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs satisfy the voice device vendors' requirements for cost effectiveness, ease of deployment, and ease of management. In addition, LLDP-MED TLVs make deploying voice devices in Ethernet easier. LLDP-MED TLVs are shown in Table 1-6:

Table 1-6 LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a MED endpoint to advertise the supported LLDP-MED TLVs and its device type.
Network Policy	Allows a network device or MED endpoint to advertise LAN type and VLAN ID of the specific port, and the Layer 2 and Layer 3 priorities for a specific set of applications.
Extended Power-via-MDI	Allows a network device or MED endpoint to advertise power-related information (according to IEEE 802.3AF).
Hardware Revision	Allows a MED endpoint device to advertise its hardware version.
Firmware Revision	Allows a MED endpoint to advertise its firmware version.
Software Revision	Allows a MED endpoint to advertise its software version.
Serial Number	Allows an LLDP-MED endpoint device to advertise its serial number.

Type	Description
Manufacturer Name	Allows a MED endpoint to advertise its vendor name.
Model Name	Allows a MED endpoint to advertise its model name.
Asset ID	Allows a MED endpoint to advertise its asset ID. The typical case is that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.
Location Identification	Allows a network device to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications.

Note

See the IEEE standard (LLDP) 802.1AB-2005 and the LLDP-MED standard (ANSI/TIA-1057) for more information about LLDPDU TLVs.

Management address

The management address of a device is used by the network management system to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

Operating Modes of LLDP

LLDP can operate in one of the following modes:

- TxRx mode. A port in this mode sends and receives LLDPDUs.
- Tx mode. A port in this mode only sends LLDPDUs.
- Rx mode. A port in this mode only receives LLDPDUs.
- Disable mode. A port in this mode does not send or receive LLDPDUs.

Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. To prevent LLDP from being initialized too frequently at times of frequent operating mode change, an initialization delay, which is user configurable, is introduced. With this delay mechanism, a port must wait for the specified interval before it can initialize LLDP after the LLDP operating mode changes.

How LLDP Works

Transmitting LLDPDUs

An LLDP-enabled port operating in TxRx mode or Tx mode sends LLDPDUs to its directly connected devices both periodically and when the local configuration changes. To prevent the network from being overwhelmed by LLDPDUs at times of frequent local device information change, an interval is introduced between two successive LLDPDUs.

This interval is shortened to 1 second in either of the following two cases:

- A new neighbor is discovered, that is, a new LLDPDU is received carrying device information new to the local device.
- The LLDP operating mode of the port changes from Disable/Rx to TxRx or Tx.

This is the fast sending mechanism of LLDP. With this mechanism, a specific number of LLDPDUs are sent successively at the 1-second interval to help LLDP neighbors discover the local device as soon as possible. Then, the normal LLDPDU transit interval resumes.

Receiving LLDPDUs

An LLDP-enabled port operating in TxRx mode or Rx mode checks the TLVs carried in every LLDPDU it receives for validity violation. If valid, the information is saved and an aging timer is set for it based on the time to live (TTL) TLV carried in the LLDPDU. If the TTL TLV is zero, the information is aged out immediately.

Compatibility of LLDP with CDP

You need to enable CDP compatibility for your device to work with Cisco IP phones.

As your LLDP-enabled device cannot recognize Cisco Discovery Protocol (CDP) packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. This can cause a requesting Cisco IP phone to send voice traffic untagged to your device, disabling your device to differentiate voice traffic from other types of traffic.

By configuring CDP compatibility, you can enable LLDP on your device to receive and recognize CDP packets from Cisco IP phones and respond with CDP packets carrying the voice VLAN configuration TLV for the IP phones to configure the voice VLAN automatically. Thus, the voice traffic is confined in the configured voice VLAN to be differentiated from other types of traffic.

CDP-compatible LLDP operates in one of the follows two modes:

- TxRx, where CDP packets can be transmitted and received.
- Disable, where CDP packets can neither be transmitted nor be received.

Protocols and Standards

The protocols and standards related to LLDP include:

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*

Configuring LLDP

LLDP Configuration Task List

Perform the tasks in Table 1-1 to configure LLDP:

Table 1-7 LLDP configuration task list

Task	Remarks
Enabling LLDP on Ports	Optional By default, LLDP is enabled on ports. Make sure that LLDP is also enabled globally, because LLDP can work on a port only when it is enabled both globally and on the port.

Task	Remarks
Configuring LLDP Settings on Ports	Optional LLDP settings include LLDP operating mode, packet encapsulation, CDP compatibility, device information polling, trapping, and advertised TLVs. By default, • The LLDP operating mode is TxRx. • The encapsulation format is Ethernet II. • CDP compatibility is disabled. • Device information polling and trapping are disabled. • All TLVs except the Location Identification TLV are advertised.
Configuring Global LLDP Setup	Required By default, global LLDP is disabled. To enable LLDP to work on a port, enable LLDP both globally and on the port.
Displaying LLDP Information for a Port	Optional You can display the local LLDP information, neighbor information, statistics, and status information of a port, where • The local LLDP information refers to the TLVs to be advertised by the local device to neighbors. • The neighbor information refers to the TLVs received from neighbors.
Displaying Global LLDP Information	Optional You can display the local global LLDP information and statistics.
Displaying LLDP Information Received from LLDP Neighbors	Optional You can display the LLDP information received from LLDP neighbors.

Note

LLDP-related configurations made in Ethernet interface view takes effect only on the current port, and those made in port group view takes effect on all ports in the current port group.

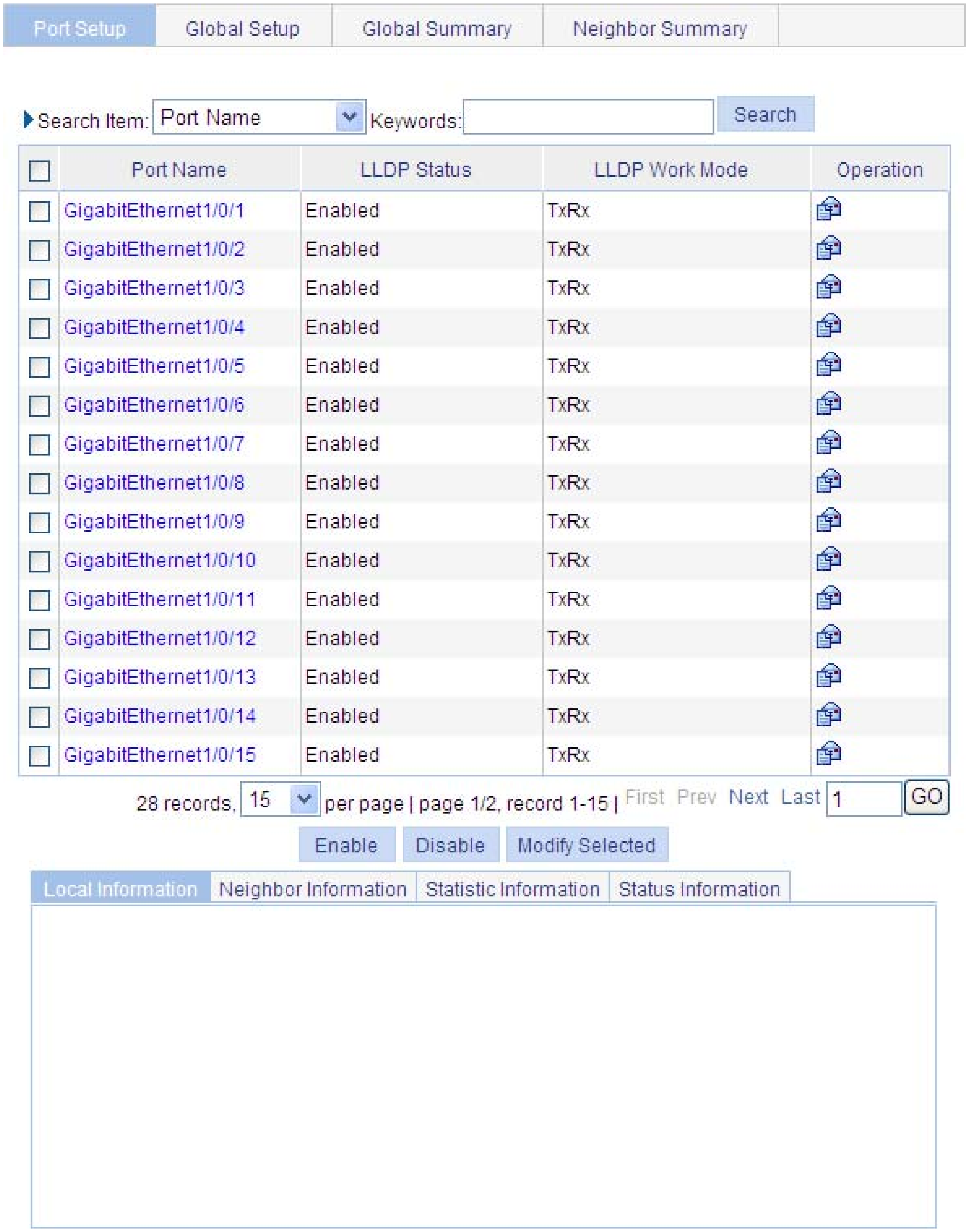
Enabling LLDP on Ports

Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in Figure 1-4.

This tab displays the enabling status and operating mode of LLDP on a port. Select one or more ports and click **Enable** beneath the port list to enable LLDP on them.

To disable LLDP on a port, select the port and click **Disable**.

Figure 1-4 The Port Setup tab



□	Port Name	LLDP Status	LLDP Work Mode	Operation
□	GigabitEthernet1/0/1	Enabled	TxRx	✎
□	GigabitEthernet1/0/2	Enabled	TxRx	✎
□	GigabitEthernet1/0/3	Enabled	TxRx	✎
□	GigabitEthernet1/0/4	Enabled	TxRx	✎
□	GigabitEthernet1/0/5	Enabled	TxRx	✎
□	GigabitEthernet1/0/6	Enabled	TxRx	✎
□	GigabitEthernet1/0/7	Enabled	TxRx	✎
□	GigabitEthernet1/0/8	Enabled	TxRx	✎
□	GigabitEthernet1/0/9	Enabled	TxRx	✎
□	GigabitEthernet1/0/10	Enabled	TxRx	✎
□	GigabitEthernet1/0/11	Enabled	TxRx	✎
□	GigabitEthernet1/0/12	Enabled	TxRx	✎
□	GigabitEthernet1/0/13	Enabled	TxRx	✎
□	GigabitEthernet1/0/14	Enabled	TxRx	✎
□	GigabitEthernet1/0/15	Enabled	TxRx	✎

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Return to LLDP Configuration Task List.

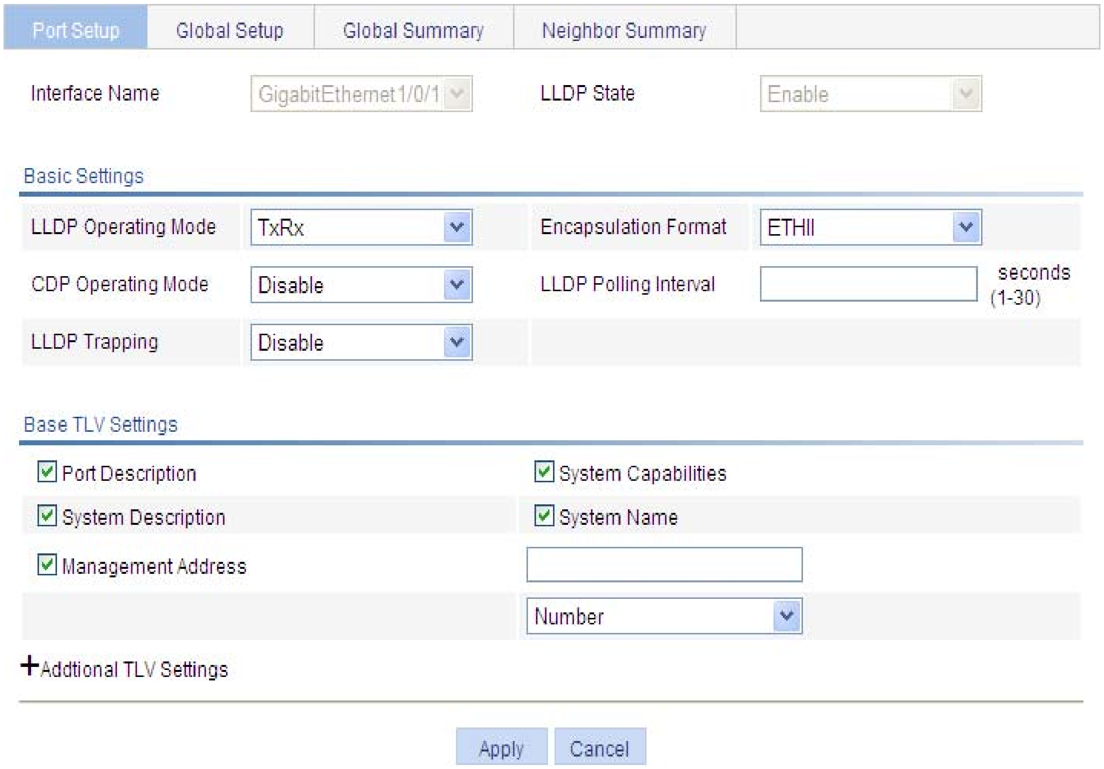
Configuring LLDP Settings on Ports

Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in Figure 1-4.

You can configure LLDP settings on ports individually or in batch.

- To configure LLDP settings on ports individually, click the icon for the port you are configuring. On the page displayed as shown in Figure 1-5, you can modify or view the LLDP settings of the port.

Figure 1-5 The page for modifying LLDP settings on a port



Interface Name	GigabitEthernet1/0/1	LLDP State	Enable

Basic Settings

LLDP Operating Mode	TxRx	Encapsulation Format	ETHII
CDP Operating Mode	Disable	LLDP Polling Interval	seconds (1-30)
LLDP Trapping	Disable		

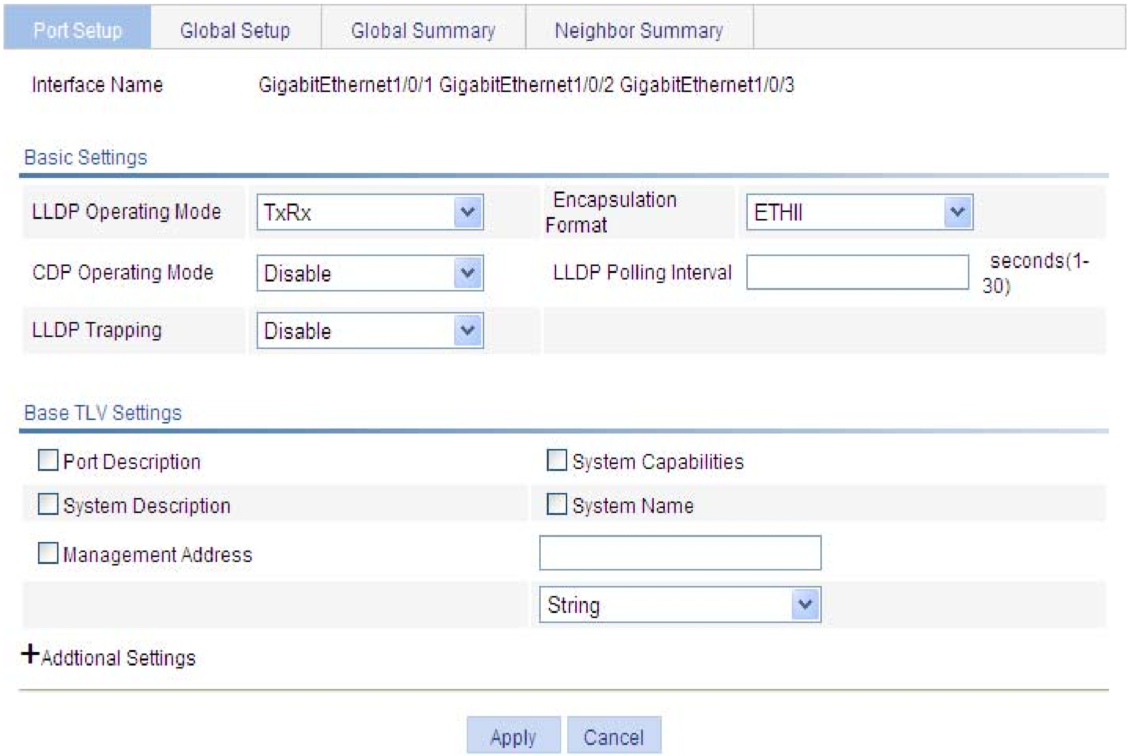
Base TLV Settings

☑ Port Description	☑ System Capabilities
☑ System Description	☑ System Name
☑ Management Address	
	Number

+Addtional TLV Settings

- To configure LLDP settings on ports in batch, select one or more ports and click **Modify Selected**. The page shown in Figure 1-6 appears.

Figure 1-6 The page for modifying LLDP settings on ports in batch



Interface Name GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3

Basic Settings

LLDP Operating Mode	TxRx	Encapsulation Format	ETHII
CDP Operating Mode	Disable	LLDP Polling Interval	seconds(1-30)
LLDP Trapping	Disable		

Base TLV Settings

□ Port Description □ System Capabilities

□ System Description □ System Name

□ Management Address

String

+Addtional Settings

Table 1-8 describes the port LLDP configuration items.

Table 1-8 Port LLDP configuration items

Item		Description
Interface Name		Displays the name of the port or ports you are configuring.
DLDP State		Displays the LLDP enabling status on the port you are configuring. This field is not available when you batch-configure ports.
Basic Settings	LLDP Operating Mode	Set the LLDP operating mode on the port or ports you are configuring. Available options include: • TxRx: Sends and receives LLDPDUs. • Tx: Sends but not receives LLDPDUs. • Rx: Receives but not sends LLDPDUs. • Disable: Neither sends nor receives LLDPDUs.
	Encapsulation Format	Set the encapsulation for LLDPDUs. Available options include: • ETHII: Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. • SNAP: Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. **Highlight** *LLDP-CDP PDUs use only SNAP encapsulation.*

Item		Description
	CDP Operating Mode	Set the CDP compatibility of LLDP. Available options include: • Disable: Neither sends nor receives CDPDUs. • TxRx: Sends and receives CDPDUs **Highlight** *To enable LLDP to be compatible with CDP on the port, you must enable CDP compatibility on the* ***Global Setup*** *tab and set the CDP operating mode on the port to TxRx.*
	LLDP Polling Interval	Enable LLDP polling and set the polling interval. If no polling interval is set, LLDP polling is disabled. With the polling mechanism, LLDP periodically detects local configuration changes. If a configuration change is detected, an LLDPDU is sent to inform the LLDP neighbors of the change.
	LLDP Trapping	Set the enable status of the LLDP trapping function on the port or ports. LLDP trapping is used to report to the network management station critical events such as new neighbor devices detected and link failures. **Highlight** *To avoid excessive traps from being sent when topology is instable, you can tune the minimum trap transit interval on the* ***Global Setup*** *tab.*
Base TLV Settings	Port Description	Select to include the port description TLV in transmitted LLDPDUs.
	System Capabilities	Select to include the system capabilities TLV in transmitted LLDPDUs.
	System Description	Select to include the system description TLV in transmitted LLDPDUs.
	System Name	Select to include the system name TLV in transmitted LLDPDUs.
	Management Address	Select to include the management address TLV in transmitted LLDPDUs and in addition, set the management address and its format (a numeric or character string in the TLV). If no management address is specified, the main IP address of the lowest VLAN carried on the port is used. If no main IP address is assigned to the VLAN, 127.0.0.1 is used.
DOT1 TLV Setting	Port VLAN ID	Select to include the PVID TLV in transmitted LLDPDUs.
	Protocol VLAN ID	Select to include port and protocol VLAN ID TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised. If no VLAN is specified, the lowest protocol VLAN ID is transmitted.
	VLAN Name	Select to include VLAN name TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised. If no VLAN is specified, the lowest VLAN carried on the port is advertised.

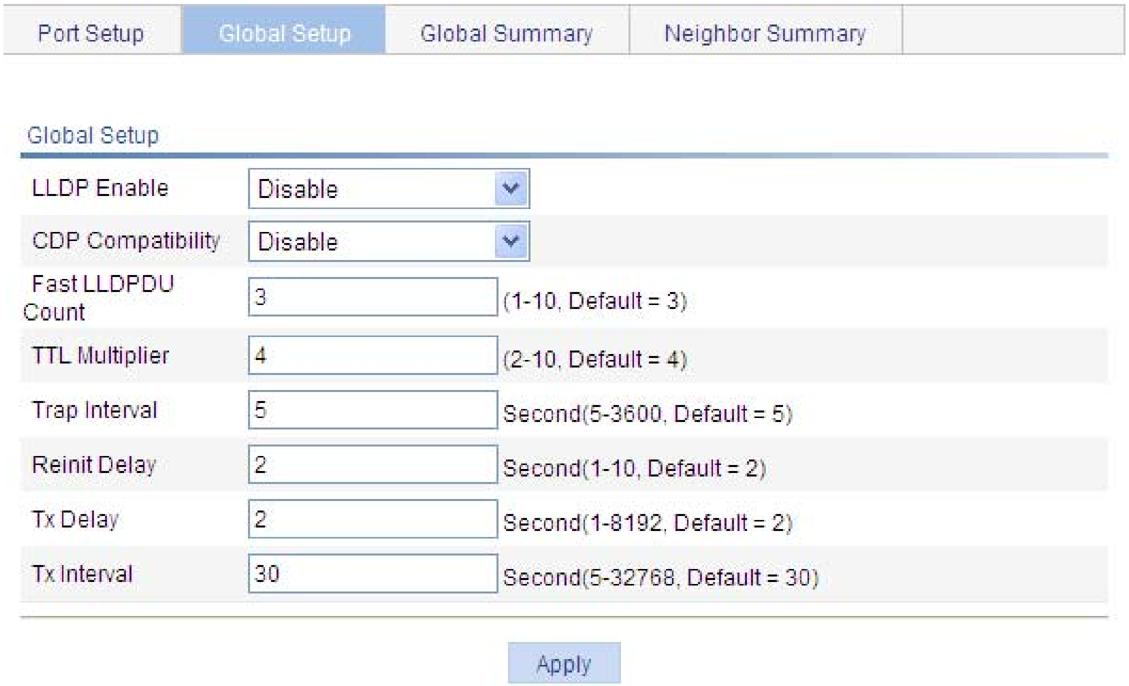
Item		Description
DOT3 TLV Setting	Link Aggregation	Select to include the link aggregation TLV in transmitted LLDPDUs.
	MAC/PHY Configuration/Status	Select to include the MAC/PHY configuration/status TLV in transmitted LLDPDUs.
	Maximum Frame Size	Select to include the maximum frame size TLV in transmitted LLDPDUs.
	Power via MDI	Select to include the power via MDI TLV in transmitted LLDPDUs.
MED TLV Setting	LLDP-MED Capabilities	Select to include the LLDP-MED capabilities TLV in transmitted LLDPDUs.
	Inventory	Select to include the hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV and asset ID TLV in transmitted LLDPDUs.
	Network Policy	Select to include the network policy TLV in transmitted LLDPDUs.
	Extended Power-via-MDI Capability	Select to include the extended power-via-MDI TLV in transmitted LLDPDUs.
	Emergency Number	Select to encode the emergency call number in the location identification TLV in transmitted LLDPDUs and set the emergency call number.
	Address	Select **Address** to encode the civic address information of the network connectivity device in the location identification TLV in transmitted LLDPDUs. In addition, set the device type, which can be a DHCP server, switch or LLDP-MED endpoint, country code, and network device address. When configuring the network device address, select the address information type from the dropdown list, type the address information in the text box below and click **Add** next to the text box to add the information to the address information list below. To remove an address information entry, select the entry from the list, and click **Delete**. The civic address information can include language, province/state, country, city, street, house number, name, postal/zip code, room number, post office box, and if necessary, additional information.
	Network Device Address	

Return to LLDP Configuration Task List.

Configuring Global LLDP Setup

Select **Network** > **LLDP** from the navigation tree and click **Global Setup** tab to enter the page shown in Figure 1-7.

Figure 1-7 The Global Setup tab



Global Setup

LLDP Enable	Disable	
CDP Compatibility	Disable	
Fast LLDPDU Count	3	(1-10, Default = 3)
TTL Multiplier	4	(2-10, Default = 4)
Trap Interval	5	Second(5-3600, Default = 5)
Reinit Delay	2	Second(1-10, Default = 2)
Tx Delay	2	Second(1-8192, Default = 2)
Tx Interval	30	Second(5-32768, Default = 30)

Table 1-9 describes the global LLDP setup configuration items.

Table 1-9 Global LLDP setup configuration items

Item	Description
LLDP Enable	Select from the dropdown list to enable or disable global LLDP.
CDP Compatibility	Select from the dropdown list to enable or disable CDP compatibility of LLDP. **Highlight** • *To enable LLDP to be compatible with CDP on a port, you must set the CDP work mode (or the CDP operating mode) on the port to TxRx in addition to enabling CDP compatibility on the **Global Setup** tab.* • *As the maximum TTL allowed by CDP is 255 seconds, you must ensure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.*
Fast LLDPDU Count	Set the number of LLDPDUs sent each time fast LLDPDU transmission is triggered.

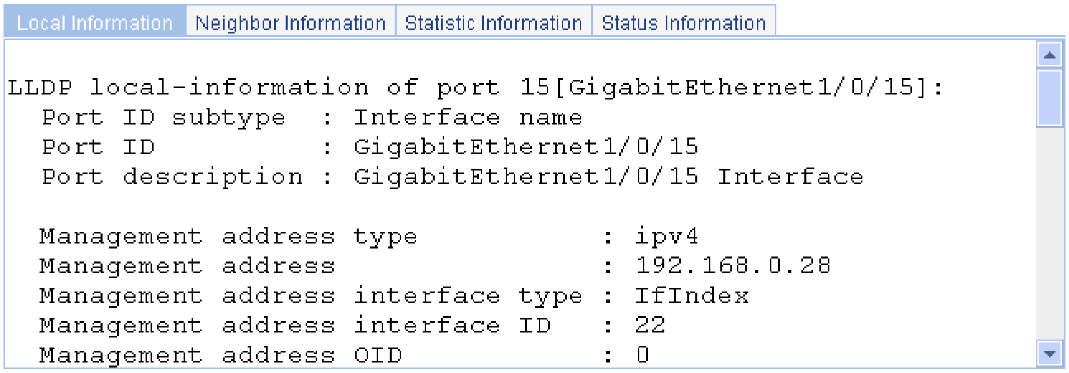
Item	Description
TTL Multiplier	Set the TTL multiplier. The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device. You can configure the TTL of locally sent LLDPDUs to determine how long information about the local device can be saved on a neighbor device by setting the TTL multiplier. The TTL is expressed as *TTL multiplier* × *LLDPDU transit interval*. **Highlight** • *If the product of the TTL multiplier and the LLDPDU transmit interval is greater than 65535, the TTL carried in transmitted LLDPDUs takes 65535 seconds.* • *As the maximum TTL allowed by CDP is 255 seconds, you must ensure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.*
Trap Interval	Set the minimum interval for sending traps. With the LLDP trapping function enabled on a port, traps are sent out the port to advertise the topology changes detected over the interval to neighbors. By tuning this interval, you can prevent excessive traps from being sent when topology is instable.
Reinit Delay	Set initialization delay for LLDP-enabled ports. Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. To prevent LLDP from being initialized too frequently at times of frequent operating mode change, initialization delay is introduced. With this delay mechanism, a port must wait for the specified interval before it can initialize LLDP after the LLDP operating mode changes.
Tx Delay	Set LLDPDU transmit delay. With LLDP enabled, a port advertises LLDPDUs to its neighbors both periodically and when the local configuration changes. To avoid excessive number of LLDPDUs caused by frequent local configuration changes, an LLDPDU transmit delay is introduced. Thus, after sending an LLDPDU, the port must wait for the specified interval before it can send another one. **Highlight** *LLDPDU transmit delay must be less than the TTL to ensure that the LLDP neighbors can receive LLDPDUs to update information about the device you are configuring before it is aged out.*
Tx Interval	Set the LLDPDU transmit interval. **Highlight** *If the product of the TTL multiplier and the LLDPDU transmit interval is greater than 65535, the TTL carried in transmitted LLDPDUs takes 65535 seconds. In this case, the likelihood exists that the LLDPDU transmit interval is greater than TTL. You should avoid the situation, because the LLDP neighbors will fail to receive LLDPDUs to update information about the device you are configuring before it is aged out.*

Return to LLDP Configuration Task List.

Displaying LLDP Information for a Port

Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in Figure 1-4. In the port list click a port name to display its LLDP information at the lower half of the page. The LLDP information is organized by type and displayed in tabs as shown in Figure 1-8. You can click these tabs to display data you are interested in.

Figure 1-8 The Local Information tab



```
LLDP local-information of port 15[GigabitEthernet1/0/15]:
  Port ID subtype  : Interface name
  Port ID          : GigabitEthernet1/0/15
  Port description : GigabitEthernet1/0/15 Interface

  Management address type           : ipv4
  Management address                : 192.168.0.28
  Management address interface type : IfIndex
  Management address interface ID   : 22
  Management address OID            : 0
```

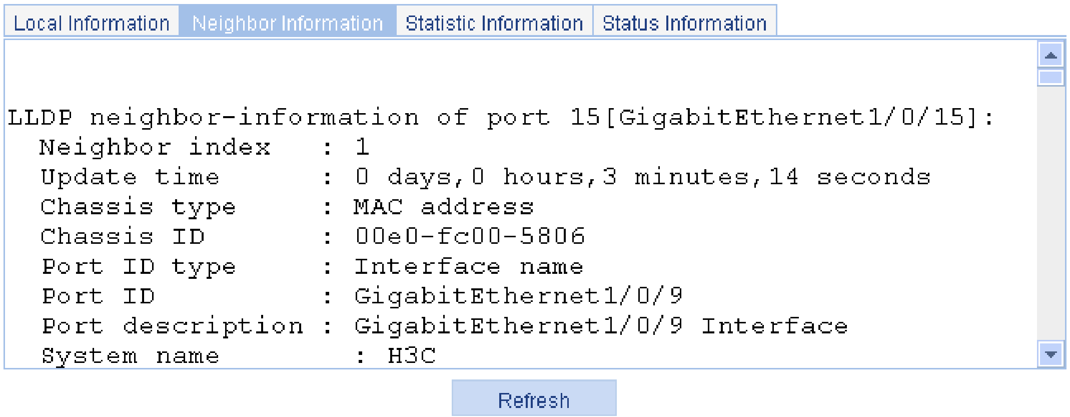
Table 1-10 describes the local LLDP information of a port.

Table 1-10 Local information of an LLDP-enabled port

Field	Description
Port ID subtype	Port ID type, which can be • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned, namely, the local configuration
Power port class	The power over Ethernet port class: • PSE, indicating a power supply device • PD: indicating a powered device
Port power classification	Port power classification of the PD, which can be • Unknown • Class0 • Class1 • Class2 • Class3 • Class4
Media policy type	Available options include: • Unknown • Voice • Voice signaling • Guest voice • Guest voice signaling • Soft phone voice • Videoconferencing • Streaming video • Video signaling
PoE PSE power source	The type of PSE power source advertised by the local device, which can be • Primary • Backup

Field	Description
Port PSE priority	Available options include: • Unknown, which indicates that PSE priority of the port is unknown. • Critical, which is priority level 1. • High, which is priority level 2 • Low: which is priority level 3

Figure 1-9 The Neighbor Information tab



```
LLDP neighbor-information of port 15[GigabitEthernet1/0/15]:
  Neighbor index   : 1
  Update time      : 0 days,0 hours,3 minutes,14 seconds
  Chassis type     : MAC address
  Chassis ID       : 00e0-fc00-5806
  Port ID type     : Interface name
  Port ID          : GigabitEthernet1/0/9
  Port description : GigabitEthernet1/0/9 Interface
  System name        : H3C
```

Table 1-11 describes the LLDP neighbor information of a port.

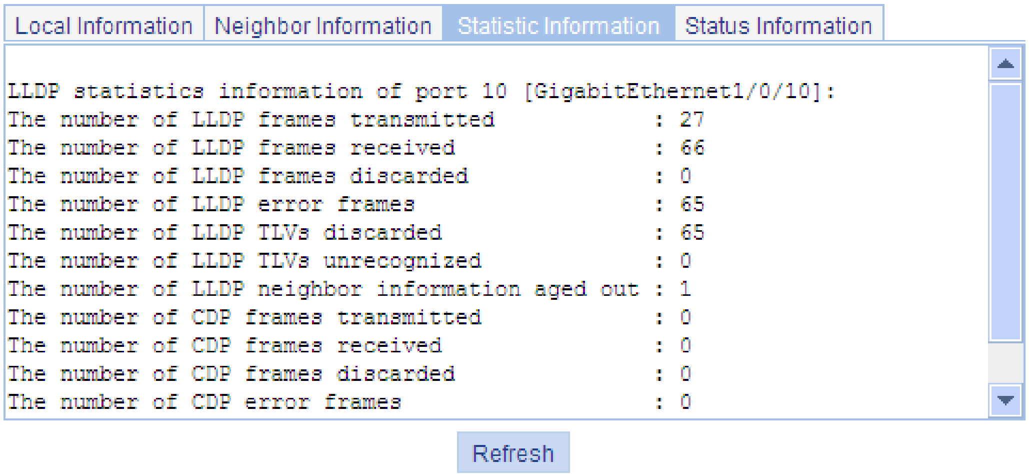
Table 1-11 LLDP neighbor information of an LLDP-enabled port

Field	Description
Chassis type	Chassis ID type. Available options include: • Chassis component • Interface alias • Port component • MAC address • Network address • Interface name • Locally assigned, namely, local configuration
Chassis ID	Chassis ID depending on the chassis type, which can be a MAC address of the device
Port ID type	Port ID type, which can be • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned, namely, the local configuration
Port ID	The port ID value.
System capabilities supported	The primary network function of the system, which can be • Repeater • Bridge • Router

Field	Description
System capabilities enabled	The network function enabled on the system, which an be • Repeater • Bridge • Router
Auto-negotiation supported	The support of the neighbor for auto negotiation
Auto-negotiation enabled	The enable status of auto negotiation on the neighbor.
OperMau	Current speed and duplex mode of the neighbor
Link aggregation supported	The support of the neighbor for link aggregation
Link aggregation enabled	The enable status of link aggregation on the neighbor
Aggregation port ID	Link aggregation group ID. It is 0 if the neighbor port is not assigned to any link aggregation group.
Maximum frame Size	The maximum frame size supported on the neighbor port.
Device class	MED device type, which can be • Connectivity device: An intermediate device that provide network connectivity. • Class I: a generic endpoint device. All endpoints that require the discovery service of LLDP belong to this category. • Class II: A media endpoint device. The class II endpoint devices support the media stream capabilities in addition to the capabilities of generic endpoint devices. • Class III: A communication endpoint device. The class III endpoint devices directly support end users of the IP communication system. Providing all capabilities of generic and media endpoint devices, Class III endpoint devices are used directly by end users.
Media policy type	Available options include: • Unknown • Voice • Voice signaling • Guest voice • Guest voice signaling • Soft phone voice • Videoconferencing • Streaming video • Video signaling
Unknown Policy	Indicates whether the media policy type is unknown.
VLAN tagged	Indicates whether packets of the media VLAN are tagged.
Media policy VlanID	ID of the media VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP precedence.
HardwareRev	Hardware version of the neighbor.
FirmwareRev	Firmware version of the neighbor.
SoftwareRev	Software version of the neighbor.
SerialNum	The serial number advertised by the neighbor.
Manufacturer name	The manufacturer name advertised by the neighbor.
Model name	The model name advertised by the neighbor.

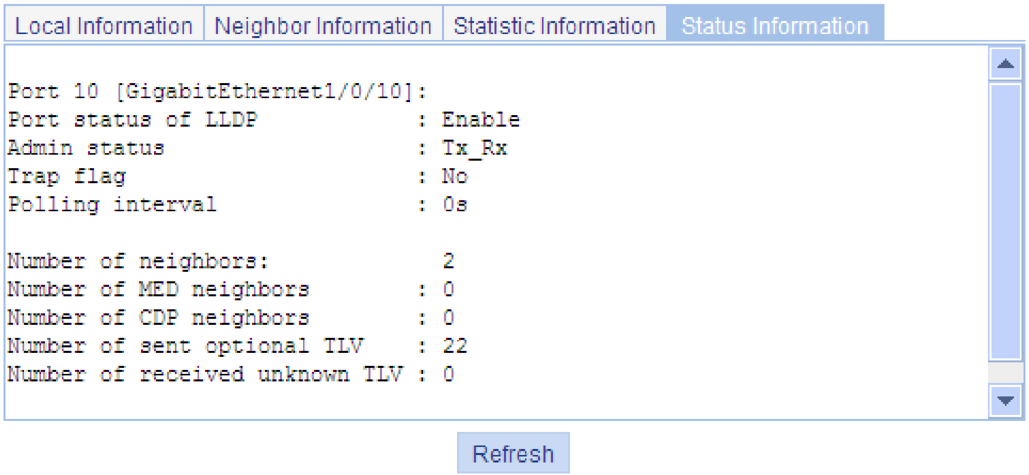
Field	Description
Asset tracking identifier	Asset ID advertised by the neighbor. This ID is used for the purpose of inventory management and asset tracking.
PoE PSE power source	The type of PSE power source advertised by the neighbor, which can be: • Primary • Backup
Port PSE priority	Available options include: • Unknown, which indicates that PSE priority of the port is unknown. • Critical, which is priority level 1. • High, which is priority level 2. • Low, which is priority level 3.

Figure 1-10 The Statistic Information tab



```
LLDP statistics information of port 10 [GigabitEthernet1/0/10]:
The number of LLDP frames transmitted            : 27
The number of LLDP frames received               : 66
The number of LLDP frames discarded              : 0
The number of LLDP error frames                  : 65
The number of LLDP TLVs discarded                : 65
The number of LLDP TLVs unrecognized             : 0
The number of LLDP neighbor information aged out : 1
The number of CDP frames transmitted             : 0
The number of CDP frames received                : 0
The number of CDP frames discarded               : 0
The number of CDP error frames                   : 0
```

Figure 1-11 The Status Information tab



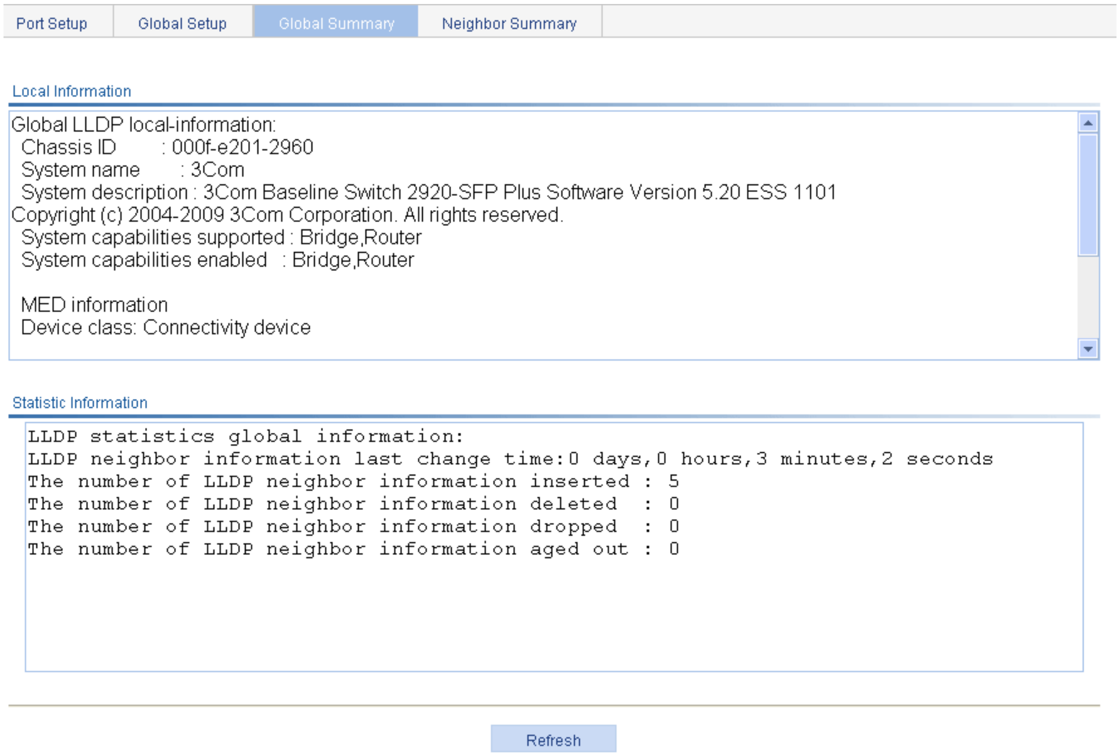
```
Port 10 [GigabitEthernet1/0/10]:
Port status of LLDP            : Enable
Admin status                   : Tx_Rx
Trap flag                      : No
Polling interval               : 0s

Number of neighbors:             2
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 22
Number of received unknown TLV : 0
```

Return to LLDP Configuration Task List.

Displaying Global LLDP Information

Select **Network** > **LLDP** from the navigation tree, and click the **Global Summary** tab to display global local LLDP information and statistics, as shown in Figure 1-12.

Figure 1-12 The Global Summary tab



```
Global LLDP local-information:
 Chassis ID        : 000f-e201-2960
 System name       : 3Com
 System description : 3Com Baseline Switch 2920-SFP Plus Software Version 5.20 ESS 1101
Copyright (c) 2004-2009 3Com Corporation. All rights reserved.
 System capabilities supported : Bridge,Router
 System capabilities enabled   : Bridge,Router

 MED information
 Device class: Connectivity device
```

```
LLDP statistics global information:
LLDP neighbor information last change time:0 days,0 hours,3 minutes,2 seconds
The number of LLDP neighbor information inserted : 5
The number of LLDP neighbor information deleted  : 0
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 0
```

Table 1-12 describes the global LLDP information.

Table 1-12 Global LLDP information

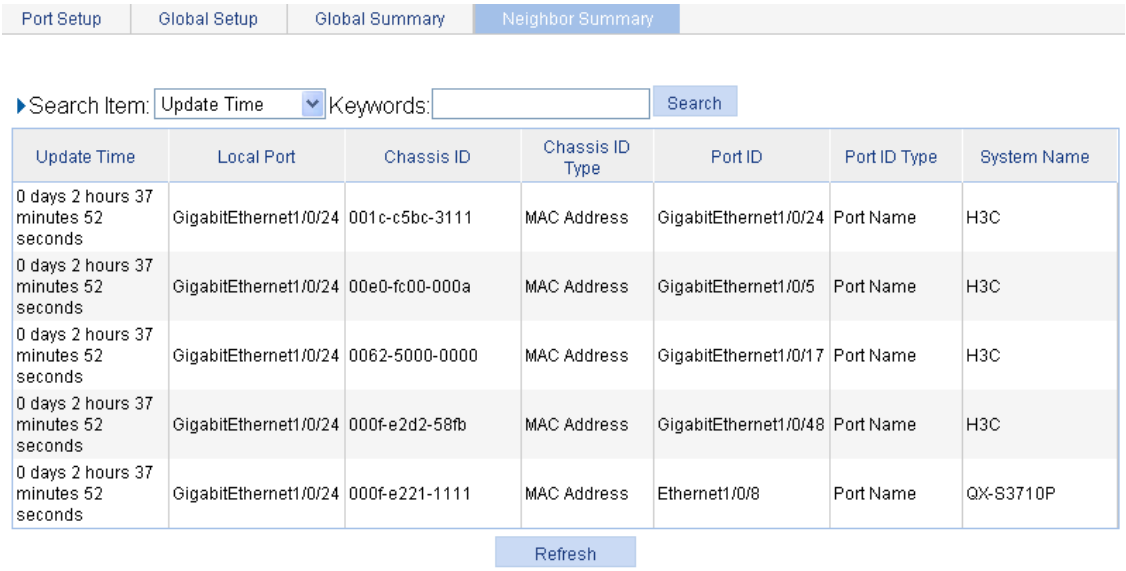
Field	Description
Chassis ID	The local chassis ID depending on the chassis type defined.
System capabilities supported	The primary network function advertised by the local device, which can be • Bridge • Router
System capabilities enabled	The enabled network function advertised by the local device, which can be • Bridge • Router
Device class	The device class advertised by the local device, which can be • Connectivity device: An intermediate device that provide network connectivity. • Class I: a generic endpoint device. All endpoints that require the discovery service of LLDP belong to this category. • Class II: A media endpoint device. The class II endpoint devices support the media stream capabilities in addition to the capabilities of generic endpoint devices. • Class III: A communication endpoint device. The class III endpoint devices directly support end users of the IP communication system. Providing all capabilities of generic and media endpoint devices, Class III endpoint devices are used directly by end users.

Return to LLDP Configuration Task List.

Displaying LLDP Information Received from LLDP Neighbors

Select **Network** > **LLDP** from the navigation tree and click the **Neighbor Summary** tab to display the global LLDP neighbor information, as shown in Figure 1-13.

Figure 1-13 The Neighbor Summary tab



Search Item: Update Time Keywords:

Update Time	Local Port	Chassis ID	Chassis ID Type	Port ID	Port ID Type	System Name
0 days 2 hours 37 minutes 52 seconds	GigabitEthernet1/0/24	001c-c5bc-3111	MAC Address	GigabitEthernet1/0/24	Port Name	H3C
0 days 2 hours 37 minutes 52 seconds	GigabitEthernet1/0/24	00e0-fc00-000a	MAC Address	GigabitEthernet1/0/5	Port Name	H3C
0 days 2 hours 37 minutes 52 seconds	GigabitEthernet1/0/24	0062-5000-0000	MAC Address	GigabitEthernet1/0/17	Port Name	H3C
0 days 2 hours 37 minutes 52 seconds	GigabitEthernet1/0/24	000f-e2d2-58fb	MAC Address	GigabitEthernet1/0/48	Port Name	H3C
0 days 2 hours 37 minutes 52 seconds	GigabitEthernet1/0/24	000f-e221-1111	MAC Address	Ethernet1/0/8	Port Name	QX-S3710P

Return to LLDP Configuration Task List.

LLDP Configuration Examples

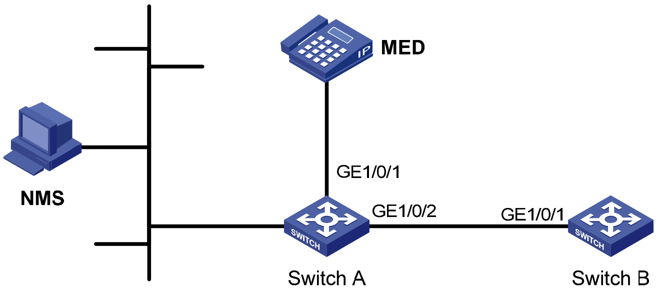
LLDP Basic Settings Configuration Example

Network requirements

As shown in Figure 1-14, a network management station is connected to Switch A over Ethernet and Switch A is connected to a MED device and Switch B through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively.

Configure LLDP on Switch A and Switch B so that the network management station can determine the link status of Switch A.

Figure 1-14 Network diagram for basic LLDP settings configuration



Configuration procedure

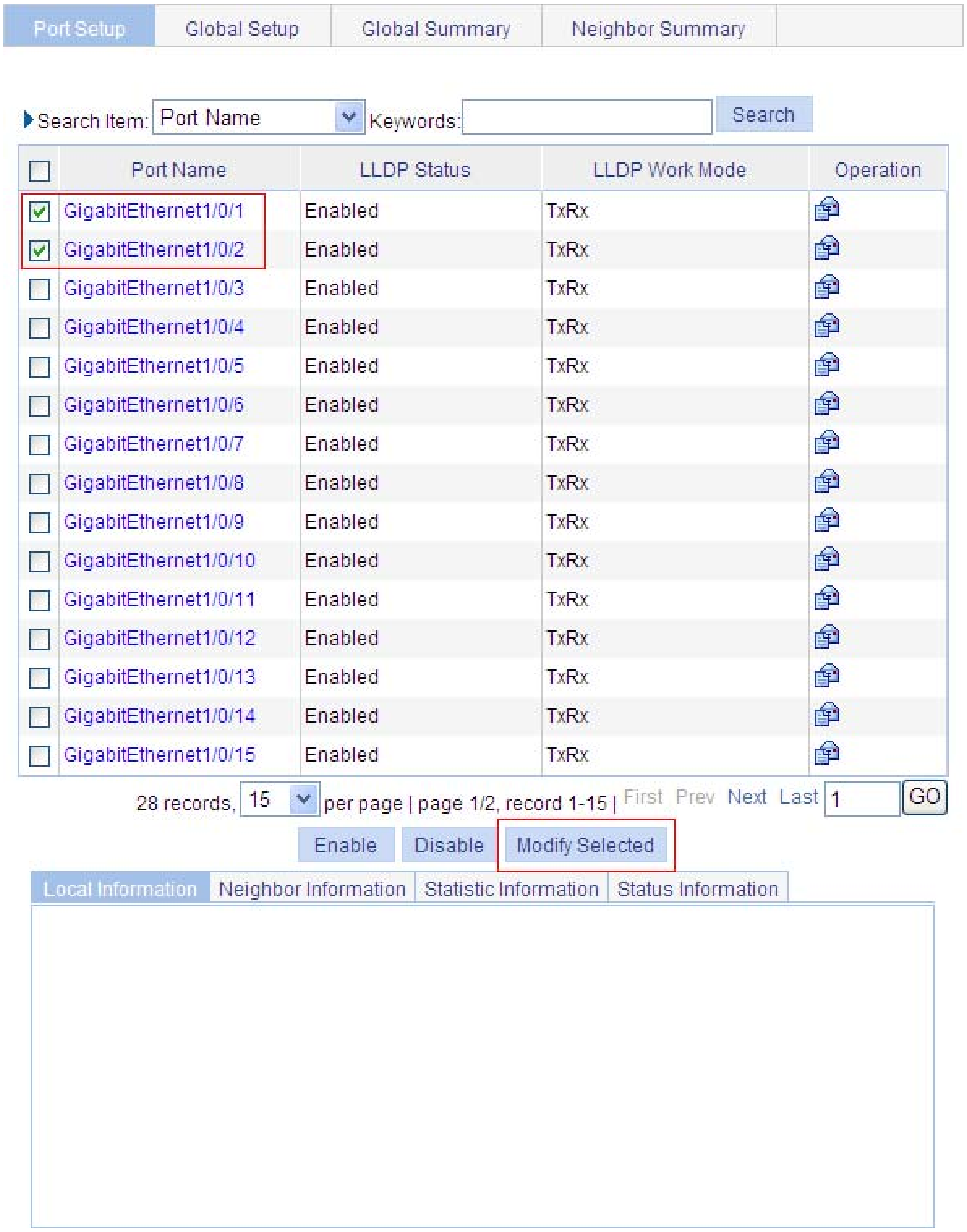
1) Configure Switch A

# Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. (Optional. By default, LLDP is enabled on Ethernet ports.)

# Set the LLDP operating mode to Rx on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

- Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in Figure 1-15. Select port GigabitEthernet1/0/1 and GigabitEthernet1/0/2 and click **Modify Selected.** The page shown in Figure 1-16 appears.

Figure 1-15 The Port Setup tab

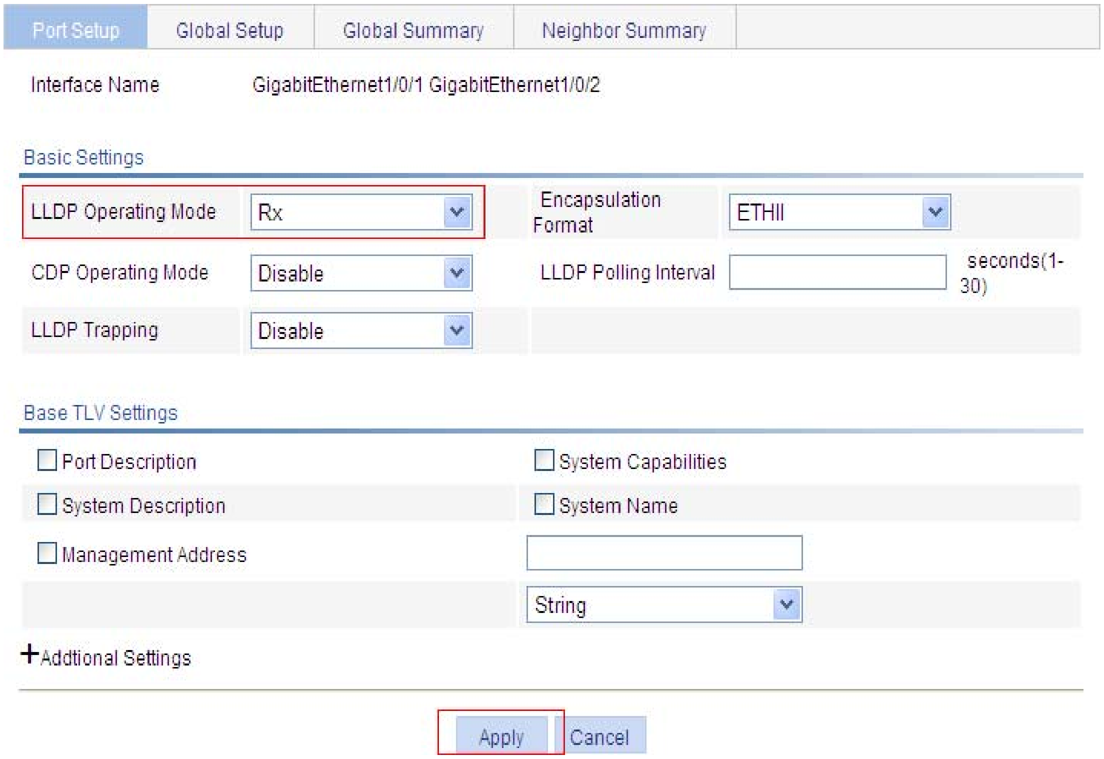


Search Item: Port Name Keywords: Search

□	Port Name	LLDP Status	LLDP Work Mode	Operation
☑	GigabitEthernet1/0/1	Enabled	TxRx	📝
☑	GigabitEthernet1/0/2	Enabled	TxRx	📝
□	GigabitEthernet1/0/3	Enabled	TxRx	📝
□	GigabitEthernet1/0/4	Enabled	TxRx	📝
□	GigabitEthernet1/0/5	Enabled	TxRx	📝
□	GigabitEthernet1/0/6	Enabled	TxRx	📝
□	GigabitEthernet1/0/7	Enabled	TxRx	📝
□	GigabitEthernet1/0/8	Enabled	TxRx	📝
□	GigabitEthernet1/0/9	Enabled	TxRx	📝
□	GigabitEthernet1/0/10	Enabled	TxRx	📝
□	GigabitEthernet1/0/11	Enabled	TxRx	📝
□	GigabitEthernet1/0/12	Enabled	TxRx	📝
□	GigabitEthernet1/0/13	Enabled	TxRx	📝
□	GigabitEthernet1/0/14	Enabled	TxRx	📝
□	GigabitEthernet1/0/15	Enabled	TxRx	📝

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Figure 1-16 The page for setting LLDP on multiple ports



Interface Name GigabitEthernet1/0/1 GigabitEthernet1/0/2

Basic Settings

LLDP Operating Mode	Rx	Encapsulation Format	ETHII
CDP Operating Mode	Disable	LLDP Polling Interval	seconds(1-30)
LLDP Trapping	Disable		

Base TLV Settings

□ Port Description □ System Capabilities

□ System Description □ System Name

□ Management Address

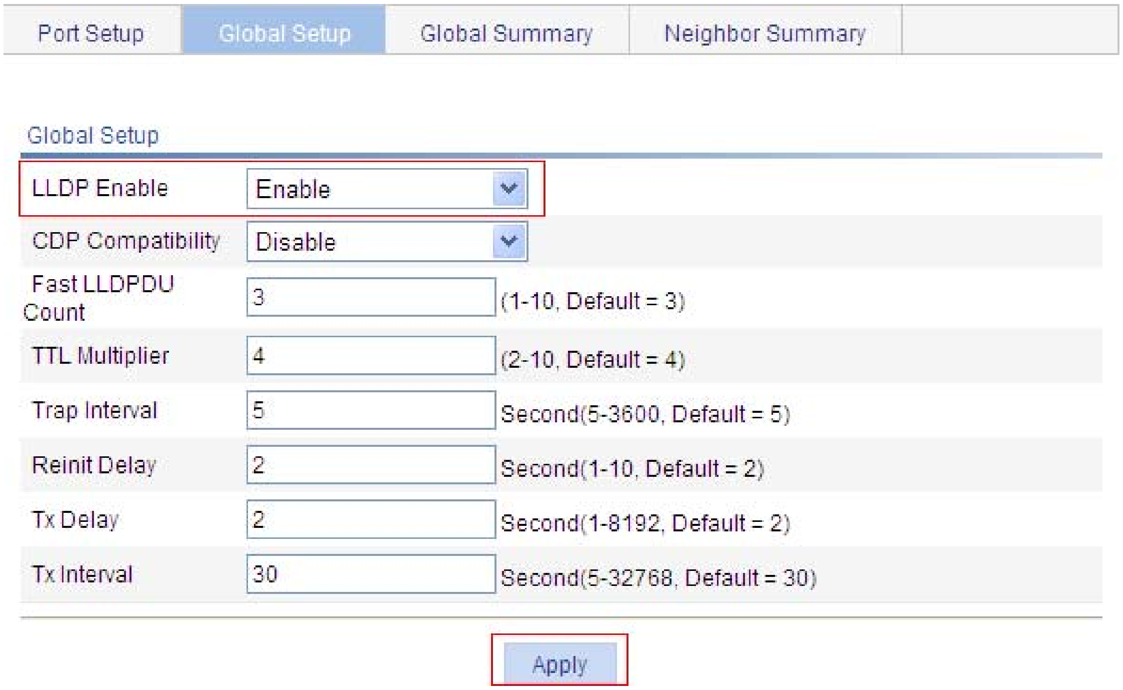
String

- Select **Rx** from the **LLDP Operating Mode** dropdown list.
- Click **Apply**.

# Enable global LLDP.

- Click the **Global Setup** tab, as shown in Figure 1-17.

Figure 1-17 The Global Setup tab



Global Setup

LLDP Enable	Enable	
CDP Compatibility	Disable	
Fast LLDPDU Count	3	(1-10, Default = 3)
TTL Multiplier	4	(2-10, Default = 4)
Trap Interval	5	Second(5-3600, Default = 5)
Reinit Delay	2	Second(1-10, Default = 2)
Tx Delay	2	Second(1-8192, Default = 2)
Tx Interval	30	Second(5-32768, Default = 30)

- Select **Enable** from the **LLDP Enable** dropdown list.
- Click **Apply**.

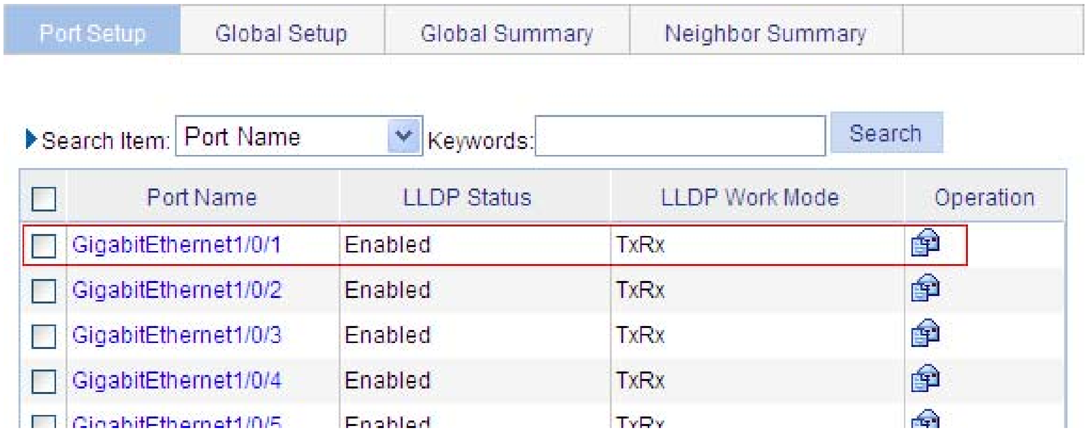
2) Configure Switch B

# Enable LLDP on port GigabitEthernet 1/0/1. (Optional. By default, LLDP is enabled on Ethernet ports.)

# Set the LLDP operating mode to Rx on GigabitEthernet 1/0/1.

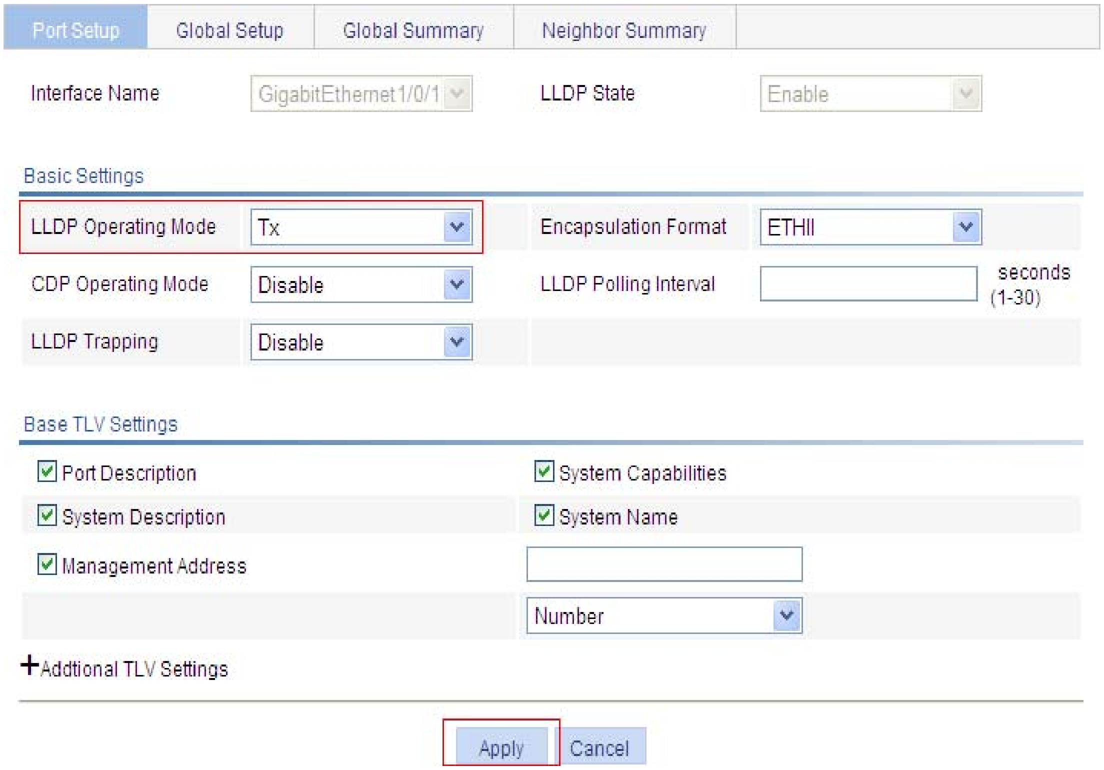
- Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in Figure 1-18. Click the 📋 icon for port GigabitEthernet1/0/1. The page shown in Figure 1-19 is displayed.

Figure 1-18 The Port Setup tab



□	Port Name	LLDP Status	LLDP Work Mode	Operation
□	GigabitEthernet1/0/1	Enabled	TxRx	📋
□	GigabitEthernet1/0/2	Enabled	TxRx	📋
□	GigabitEthernet1/0/3	Enabled	TxRx	📋
□	GigabitEthernet1/0/4	Enabled	TxRx	📋
□	GigabitEthernet1/0/5	Enabled	TxRx	📋

Figure 1-19 The page for configuring LLDP on the selected port



Interface Name	GigabitEthernet1/0/1	LLDP State	Enable

Basic Settings

LLDP Operating Mode	Tx	Encapsulation Format	ETHII
CDP Operating Mode	Disable	LLDP Polling Interval	seconds (1-30)
LLDP Trapping	Disable		

Base TLV Settings

☑ Port Description	☑ System Capabilities
☑ System Description	☑ System Name
☑ Management Address	
	Number

+Addtional TLV Settings

- Select **Tx** from the **LLDP Operating Mode** dropdown list.
- Click **Apply**.

# Enable global LLDP and configure the global LLDP setup as needed (see).

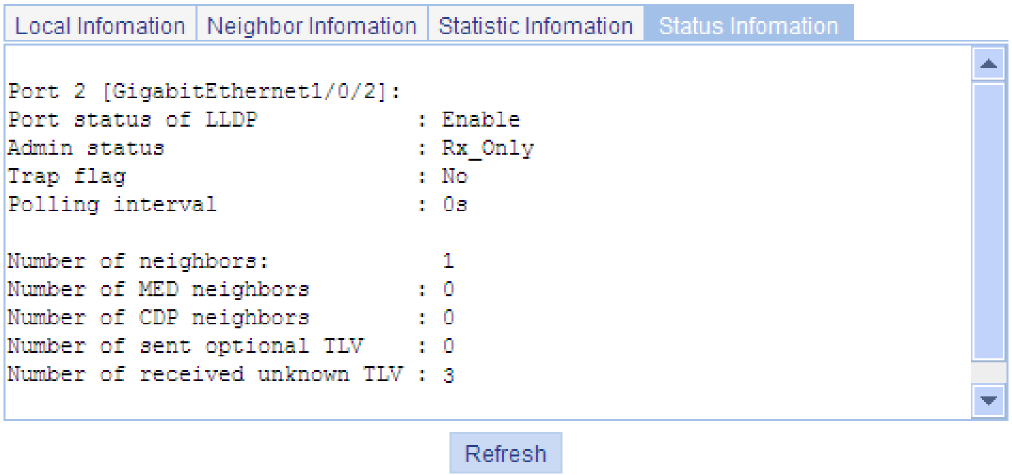
- Click the **Global Setup** tab.
- Select **Enable** from the **LLDP Enable** dropdown list.
- Click **Apply**.

Configuration verification

# Display the status information of port GigabitEthernet1/0/2 on Switch A.

- Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab.
- Click the **GigabitEthernet1/0/2** port name in the port list.
- Click the **Status Information** tab at the lower half of the page. The output shows that port GigabitEthernet 1/0/2 is connected to a non-MED neighbor device, that is, Switch B, as shown in Figure 1-20.

Figure 1-20 The Status Information tab



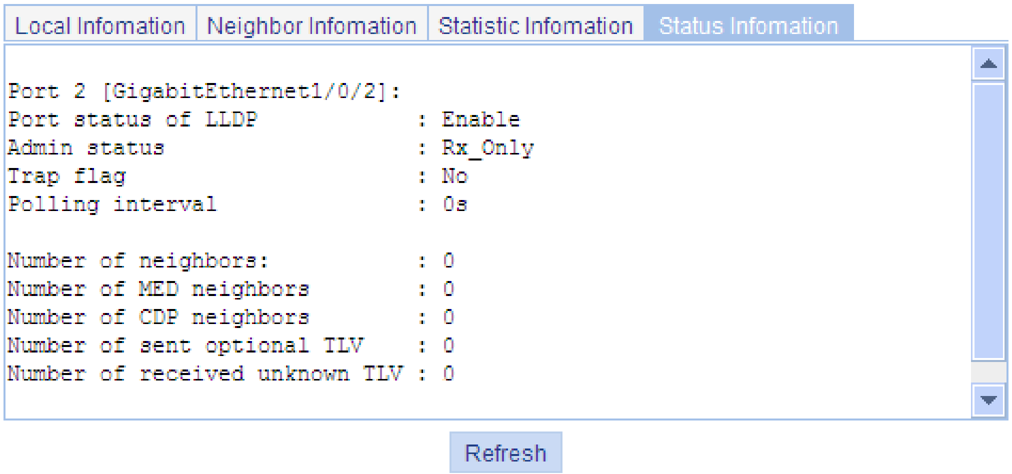
```
Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

Number of neighbors:             1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 3
```

# Tear down the link between Switch A and Switch B.

# Display the status information of port GigabitEthernet1/0/2 on Switch A.

- Click **Refresh**. The updated status information of port GigabitEthernet 1/0/2 shows that no neighbor device is connected to the port, as shown in Figure 1-21.

Figure 1-21 The **Status Information** tab displaying the updated port status information



```
Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Polling interval               : 0s

Number of neighbors:           : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 0
```

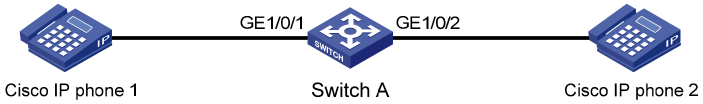
CDP-Compatible LLDP Configuration Example

Network requirements

As shown in Figure 1-22, port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone.

On Switch A configure VLAN 2 as a voice VLAN and configure CDP-compatible LLDP to enable the Cisco IP phones to automatically configure the voice VLAN, thus confining their voice traffic within the voice VLAN to be separate from other types of traffic.

Figure 1-22 Network diagram for CDP-compatible LLDP configuration

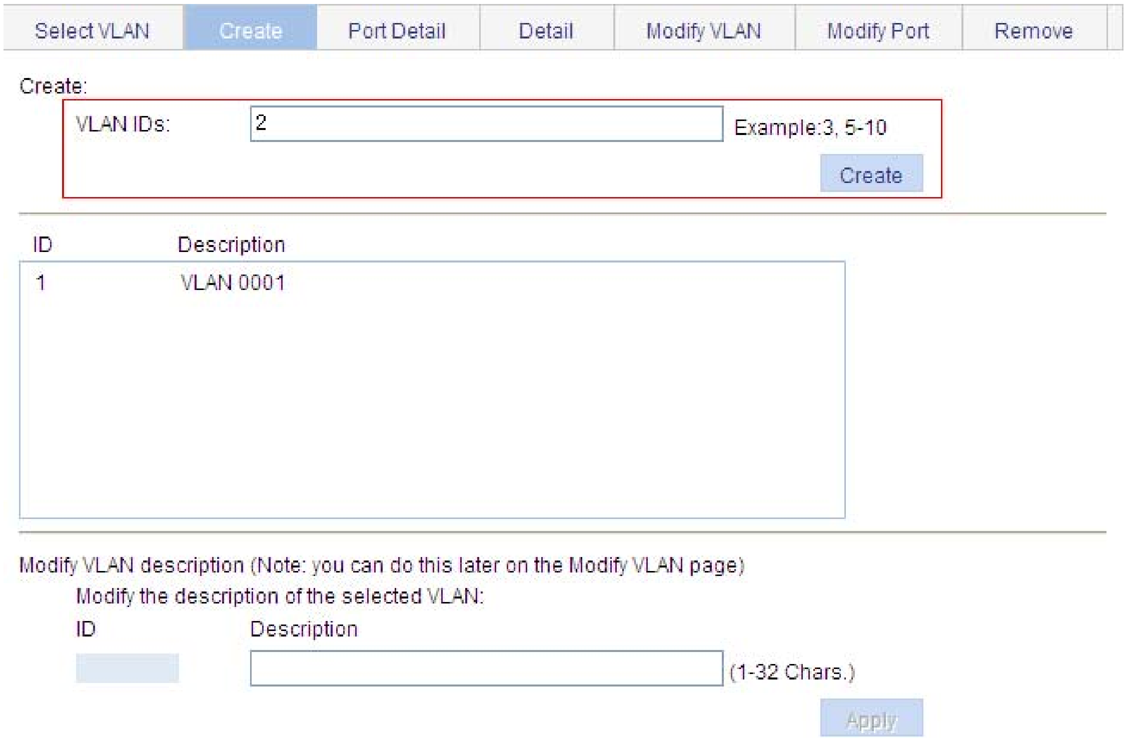


Configuration procedure

# Create VLAN 2.

- Select **Network** > **VLAN** from the navigation bar and click **Create** to enter the page for creating VLANs shown in Figure 1-23.

Figure 1-23 The page for creating VLANs



Create:

VLAN IDs: 2 Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

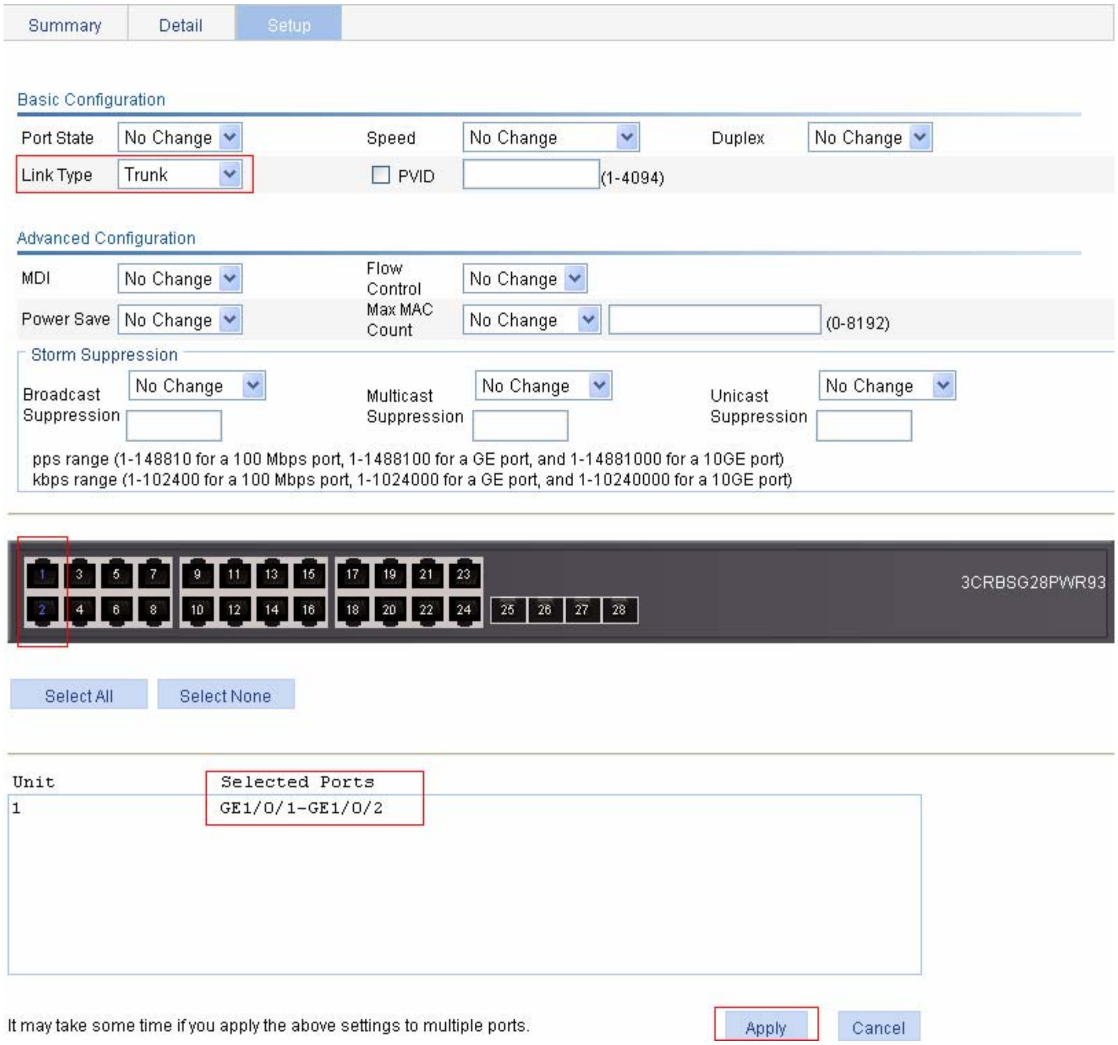
ID Description (1-32 Chars.)

- Type **2** in the **VLAN IDs** field.
- Click **Create**.

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports.

- Select **Device** > **Port Management** from the navigation bar and click the **Setup** tab to enter the page for configuring ports as shown in Figure 1-24.

Figure 1-24 The page for configuring ports



Port State: No Change
Speed: No Change
Duplex: No Change
Link Type: Trunk
□ PVID (1-4094)
MDI: No Change
Flow Control: No Change
Power Save: No Change
Max MAC Count: No Change (0-8192)
Broadcast Suppression: No Change
Multicast Suppression: No Change
Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kbps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

Unit	Selected Ports
1	GE1/0/1-GE1/0/2

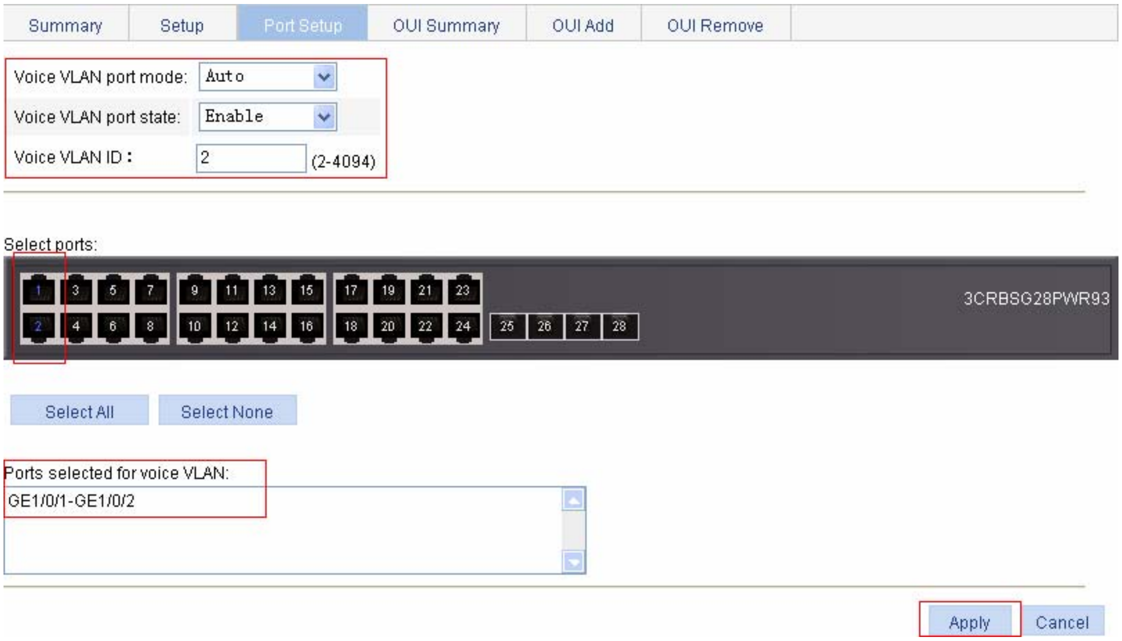
It may take some time if you apply the above settings to multiple ports.

- Select **Trunk** in the **Link Type** drop-down list.
- Click to select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
- Click **Apply**.

# Configure the voice VLAN function on the two ports.

- Select **Network** > **Voice VLAN** from the navigation bar and click the **Port Setup** tab to enter the page for configuring the voice VLAN function on ports, as shown in Figure 1-25.

Figure 1-25 The page for configuring the voice VLAN function on ports



Voice VLAN port mode: Auto

Voice VLAN port state: Enable

Voice VLAN ID : 2 (2-4094)

Select ports:

Ports selected for voice VLAN:
GE1/0/1-GE1/0/2

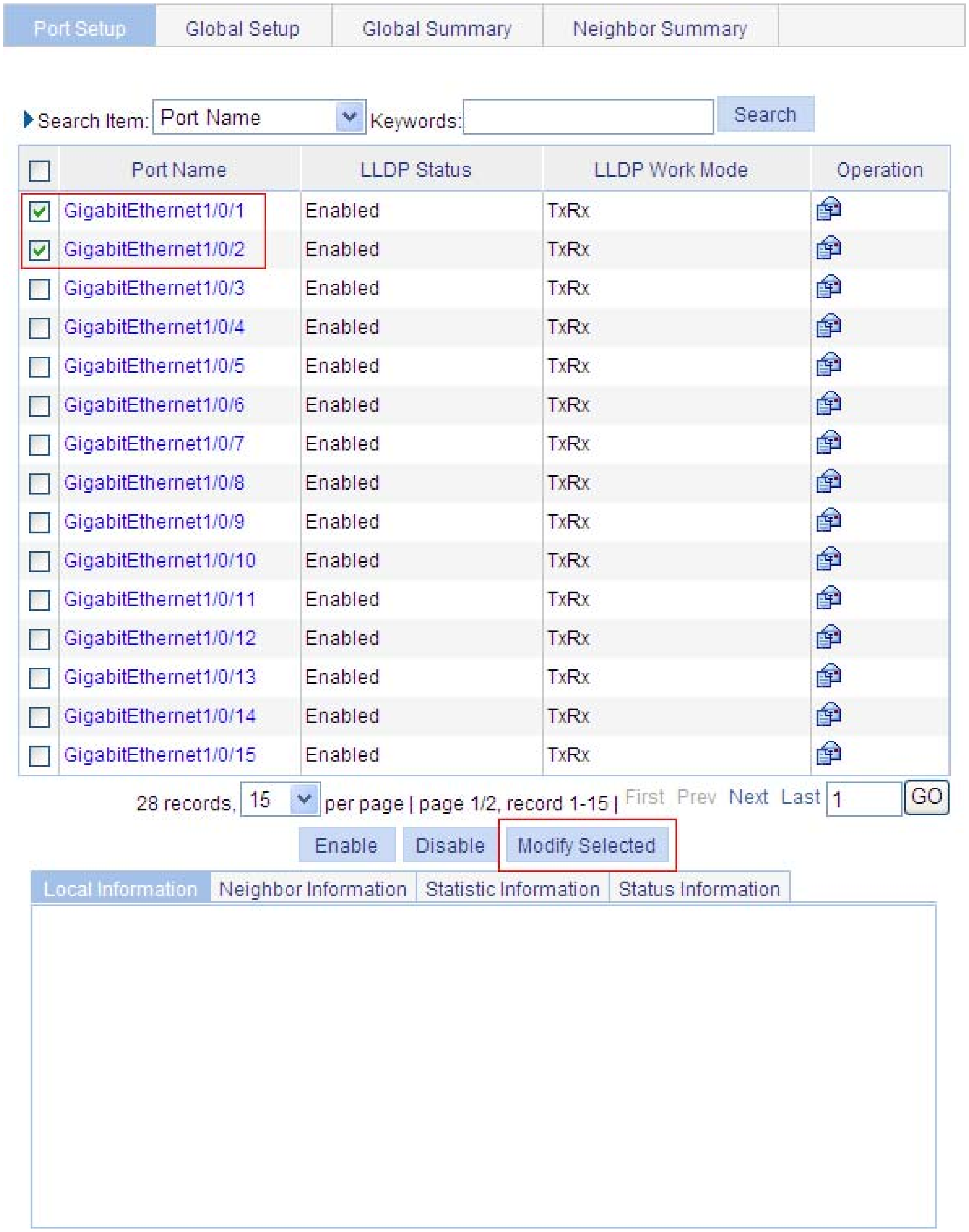
- Select **Auto** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type the voice VLAN ID **2**.
- Click to select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
- Click **Apply**.

# Enable LLDP on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. If LLDP is enabled (the default), skip this step.

# Set both the LLDP operating mode and the CDP operating mode to TxRx on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

- Select **Network** > **LLDP** from the navigation tree to enter the **Port Setup** tab. Select port GigabitEthernet1/0/1 and GigabitEthernet1/0/2 and click **Modify Selected**, as shown in Figure 1-26. The page shown in Figure 1-27 is displayed.

Figure 1-26 The Port Setup tab

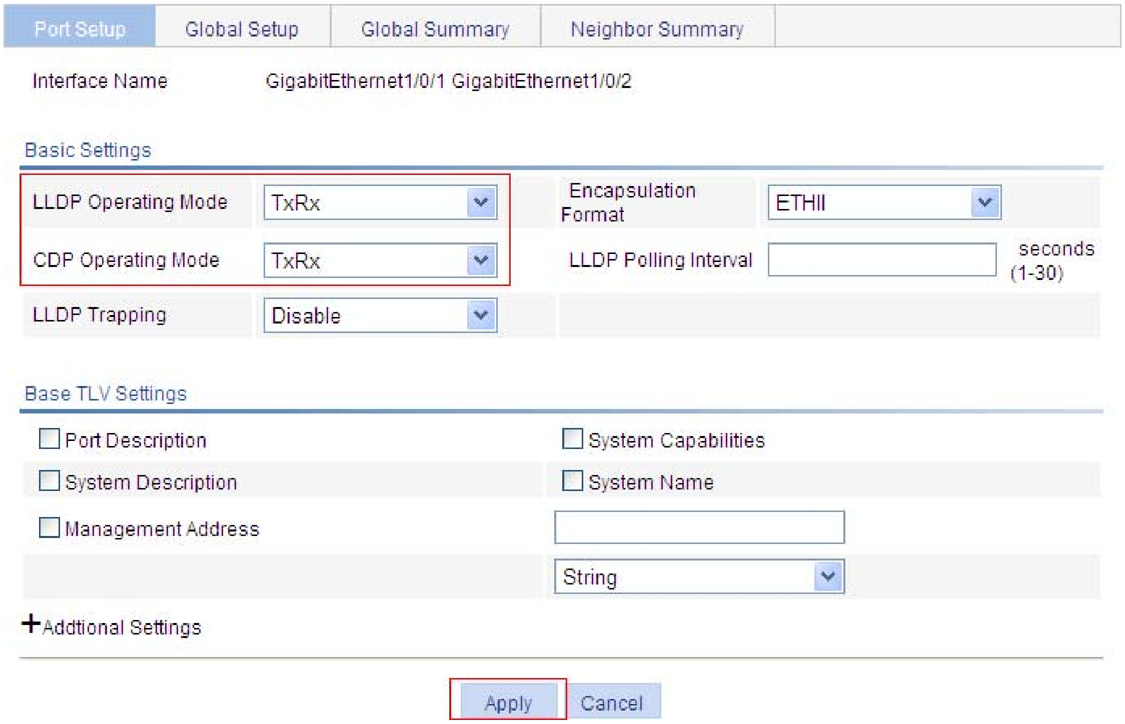


Search Item: Port Name Keywords:

□	Port Name	LLDP Status	LLDP Work Mode	Operation
☑	GigabitEthernet1/0/1	Enabled	TxRx	📋
☑	GigabitEthernet1/0/2	Enabled	TxRx	📋
□	GigabitEthernet1/0/3	Enabled	TxRx	📋
□	GigabitEthernet1/0/4	Enabled	TxRx	📋
□	GigabitEthernet1/0/5	Enabled	TxRx	📋
□	GigabitEthernet1/0/6	Enabled	TxRx	📋
□	GigabitEthernet1/0/7	Enabled	TxRx	📋
□	GigabitEthernet1/0/8	Enabled	TxRx	📋
□	GigabitEthernet1/0/9	Enabled	TxRx	📋
□	GigabitEthernet1/0/10	Enabled	TxRx	📋
□	GigabitEthernet1/0/11	Enabled	TxRx	📋
□	GigabitEthernet1/0/12	Enabled	TxRx	📋
□	GigabitEthernet1/0/13	Enabled	TxRx	📋
□	GigabitEthernet1/0/14	Enabled	TxRx	📋
□	GigabitEthernet1/0/15	Enabled	TxRx	📋

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1

Figure 1-27 The page for modifying LLDP settings on ports



Interface Name GigabitEthernet1/0/1 GigabitEthernet1/0/2

Basic Settings

LLDP Operating Mode	TxRx	Encapsulation Format	ETHII
CDP Operating Mode	TxRx	LLDP Polling Interval	seconds (1-30)
LLDP Trapping	Disable		

Base TLV Settings

□ Port Description
□ System Capabilities
□ System Description
□ System Name
□ Management Address

String

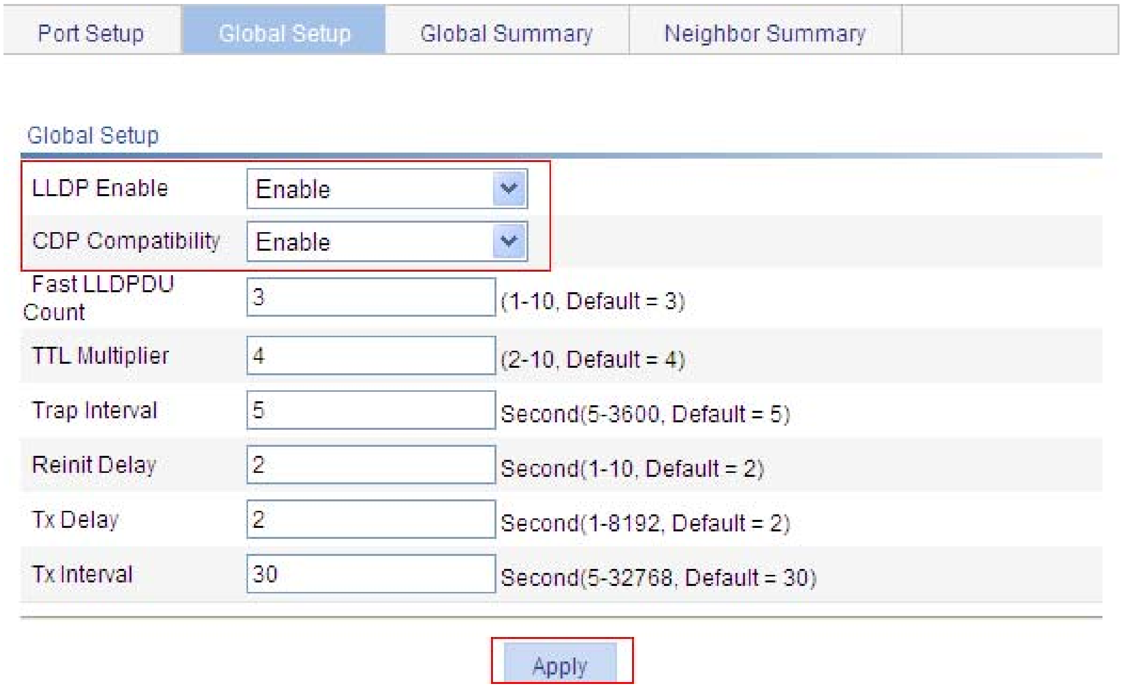
+Addtional Settings

- Select **TxRx** from the **LLDP Operating Mode** dropdown list.
- Select **TxRx** from the **CDP Operating Mode** dropdown list.
- Click **Apply**.

# Enable global LLDP and CDP compatibility of LLDP.

- Click the **Global Setup** tab, as shown in Figure 1-28.

Figure 1-28 The Global Setup tab



Global Setup

LLDP Enable	Enable	
CDP Compatibility	Enable	
Fast LLDPDU Count	3	(1-10, Default = 3)
TTL Multiplier	4	(2-10, Default = 4)
Trap Interval	5	Second(5-3600, Default = 5)
Reinit Delay	2	Second(1-10, Default = 2)
Tx Delay	2	Second(1-8192, Default = 2)
Tx Interval	30	Second(5-32768, Default = 30)

- Select **Enable** from the **LLDP Enable** dropdown list.
- Select **Enable** from the **CDP Compatibility** dropdown list.
- Click **Apply**.

Configuration verification

# Display information about LLDP neighbors on Switch A.

Display information about LLDP neighbors on Switch A after completing the configuration. You can see that Switch A has discovered the Cisco IP phones attached to ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2 and obtained their device information.

LLDP Configuration Guidelines

When configuring LLDP, follow these guidelines:

1) To make LLDP take effect, you must enable it both globally and at port level.
2) When selecting TLVs to send in LLDPDUs, note that:

- To advertise LLDP-MED TLVs, you must include the LLDP-MED capabilities set TLV.
- To remove the LLDP-MED capabilities set TLV, you must remove all other LLDP-MED TLVs.
- To remove the MAC/PHY configuration TLV, remove the LLDP-MED capabilities set TLV first.
- If the LLDP-MED capabilities set TLV is included, the MAC/PHY configuration/status TLV is included automatically.

Table of Contents

1 IGMP snooping

Overview

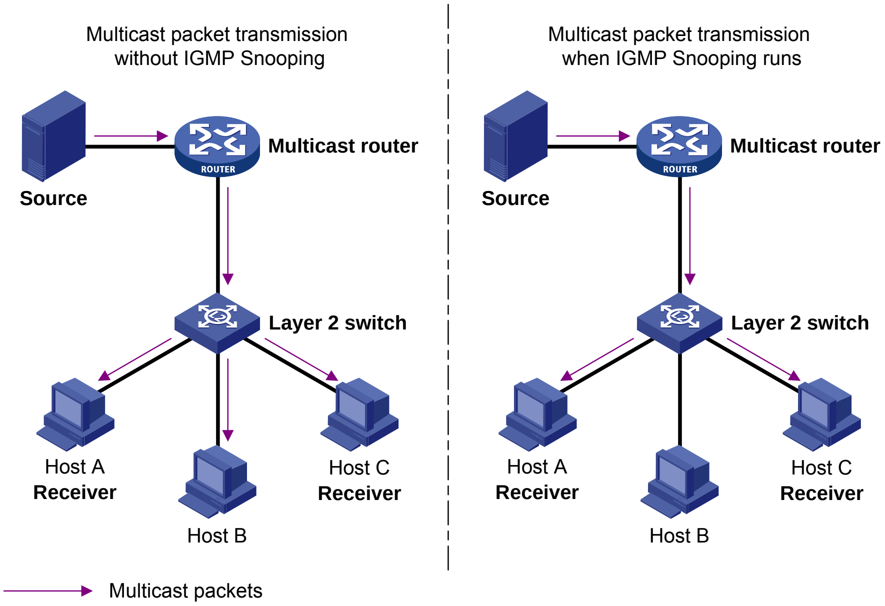
Internet Group Management Protocol Snooping (IGMP snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in Figure 1-1, when IGMP snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. However, when IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

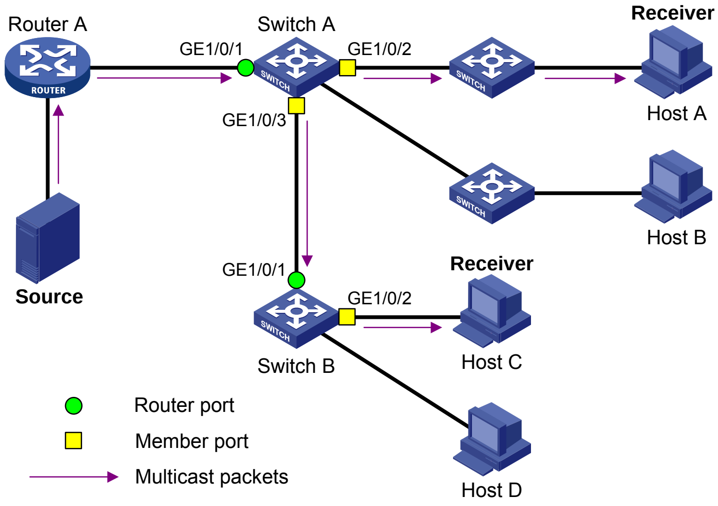
Figure 1-1 Multicast forwarding before and after IGMP snooping runs



IGMP Snooping Related Ports

As shown in Figure 1-2, Router A connects to the multicast source, IGMP snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

Figure 1-2 IGMP snooping related ports



IGMP snooping related ports include:

- Router port: A router port is a port on an Ethernet switch that leads the switch towards the Layer 3 multicast device (DR or IGMP querier). In the figure, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.
- Member port: On an Ethernet switch, a member port (also known as multicast group member port) connects the switch to a multicast group member. In the figure, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. A switch registers all its member ports in the IGMP snooping forwarding table.

Note

- Whenever mentioned in this document, a router port is a port on the switch that leads the switch to a Layer 3 multicast device, rather than a port on a router.
- Unless otherwise specified, router ports and member ports mentioned in this document consist of dynamic and static ports.
- An IGMP-Snooping-enabled switch deems that all its ports on which IGMP general queries with the source address other than 0.0.0.0 or PIM hello messages are received to be router ports.

Work Mechanism of IGMP Snooping

A switch running IGMP snooping performs different actions when it receives different IGMP messages, as follows:

Caution

You can add or delete only dynamic ports rather than static ports.

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether any active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- The switch resets the aging timer for the receiving port if the port is in the router port list;
- The switch adds the receiving port to the router port list if it is not in the list and starts the aging timer for the port.

When receiving a membership report

A host sends an IGMP membership report to the IGMP querier in the following circumstances:

- Upon receiving an IGMP query, a multicast group member host responds with an IGMP report;
- When intended to join a multicast group, a host sends an IGMP report to the querier to announce its interest in the multicast information addressed to that group.

Upon receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group, and performs the following:

- If no forwarding table entry exists for the reported group, the switch creates an entry, adds the port as a member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported group, but the port is not included in the outgoing port list, the switch adds the port as a member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported group and the port is not included in the outgoing port list, the switch resets the member port aging timer for that port.

Note

A switch does not forward an IGMP report through a non-router port. This is because if the switch forwards a report message through a member port, all the attached hosts listening to the reported multicast address will suppress their own reports upon hearing this report according to the IGMP report suppression mechanism on them, and this will prevent the switch from knowing whether any hosts attached to that port are still active members of the reported multicast group.

When receiving a leave group message

When an IGMPv1 host leaves an multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP membership reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router to announce that it has left the multicast group. When the switch receives a group-specific IGMP leave group message on a member port, it first checks whether a forwarding table entry for that group exists, and, if one exists, whether its outgoing port list contains that port.

- If the forwarding table entry does not exist or if its outgoing port list does not contain the port, the switch discards the IGMP leave group message instead of forwarding it to any port.
- If the forwarding table entry exists and its outgoing port list contains the port, the switch forwards the IGMP leave group message to the router ports in the VLAN. Because the switch does not know whether any other member hosts for that group still exist under the port to which the leave message arrived, the switch does not immediately remove the port from the outgoing port list; instead, the switch resets the member port aging timer for that port.

Upon receiving the IGMP leave group message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave group message. Upon hearing the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that multicast group, and performs the following to the port (in case it is a dynamic member port) before the member port aging timer of the port expires:

- If any IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that some host attached to the port is receiving or expecting to receive multicast data for that multicast group. The switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that no hosts attached to the port are still listening to that group address. The switch removes the port from the outgoing port list of the forwarding table entry for that multicast group when the aging timer expires.

Protocols and Standards

IGMP snooping is documented in:

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

Configuring IGMP Snooping

Configuration Task List

Perform the tasks in Table 1-1 to configure IGMP snooping.

Table 1-1 IGMP snooping configuration task list

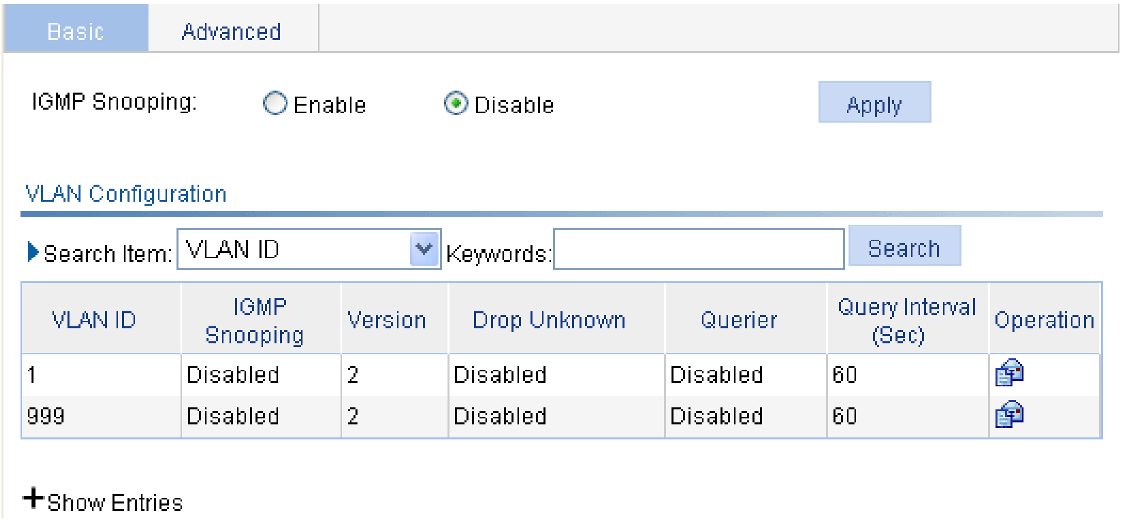
Task	Remarks
Enabling IGMP snooping Globally	Required Disabled by default.

Task	Remarks
Configuring IGMP Snooping in a VLAN	Required Enable IGMP snooping in the VLAN and configure the IGMP snooping version and querier feature. By default, IGMP snooping is disabled in a VLAN. **Highlight** • *IGMP snooping must be enabled globally before it can be enabled in a VLAN.* • *When you enable IGMP snooping in a VLAN, this function takes effect for ports in this VLAN only.*
Configuring IGMP Snooping Port Functions	Optional Configure the maximum number of multicast groups allowed and the fast leave function for ports in the specified VLAN. **Highlight** • *IGMP snooping must be enabled globally before IGMP snooping can be enabled on a port.* • *IGMP snooping configured on a port takes effect only after IGMP snooping is enabled in the VLAN.*
Display IGMP Snooping Multicast Entry Information	Optional

Enabling IGMP snooping Globally

Select **Network** > **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in Figure 1-3.

Figure 1-3 Basic IGMP snooping configurations



IGMP Snooping: ○ Enable ● Disable

VLAN Configuration

Search Item: VLAN ID Keywords:

VLAN ID	IGMP Snooping	Version	Drop Unknown	Querier	Query Interval (Sec)	Operation
1	Disabled	2	Disabled	Disabled	60	
999	Disabled	2	Disabled	Disabled	60	

Table 1-2 describes the IGMP snooping configuration items.

Table 1-2 IGMP snooping configuration items

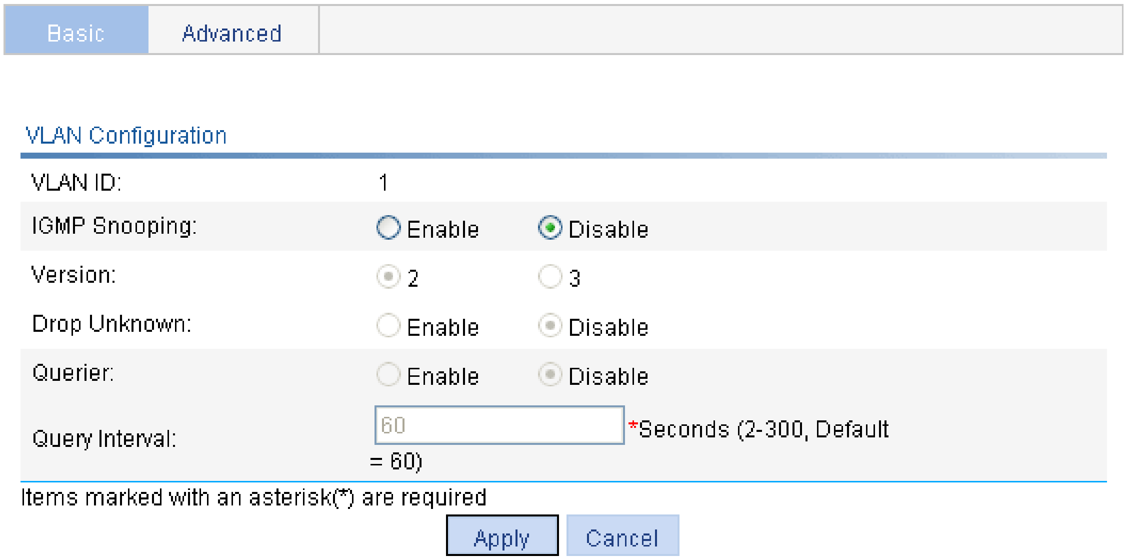
Item	Description
IGMP snooping	Globally enable or disable IGMP snooping.

Return to IGMP snooping configuration task list.

Configuring IGMP Snooping in a VLAN

Select **Network** > **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in Figure 1-3. Click the icon corresponding to the VLAN to enter the page you can configure IGMP snooping in the VLAN, as shown in Figure 1-4.

Figure 1-4 VLAN configuration



VLAN Configuration

VLAN ID:	1	
IGMP Snooping:	○ Enable	● Disable
Version:	● 2	○ 3
Drop Unknown:	○ Enable	● Disable
Querier:	○ Enable	● Disable
Query Interval:	60 *Seconds (2-300, Default = 60)	

Items marked with an asterisk(*) are required

Table 1-3 describes the items for configuring IGMP snooping in a VLAN.

Table 1-3 Items for configuring IGMP snooping in a VLAN

Item	Description
VLAN ID	This field displays the ID of the VLAN to be configured.
IGMP Snooping	Enable or disable IGMP snooping in the VLAN. You can proceed with the subsequent configurations only if **Enable** is selected here.
Version	By configuring an IGMP snooping version, you actually configure the versions of IGMP messages that IGMP snooping can process. • IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN. • IGMP snooping version 3 can process IGMPv1, IGMPv2, and IGMPv3 messages.

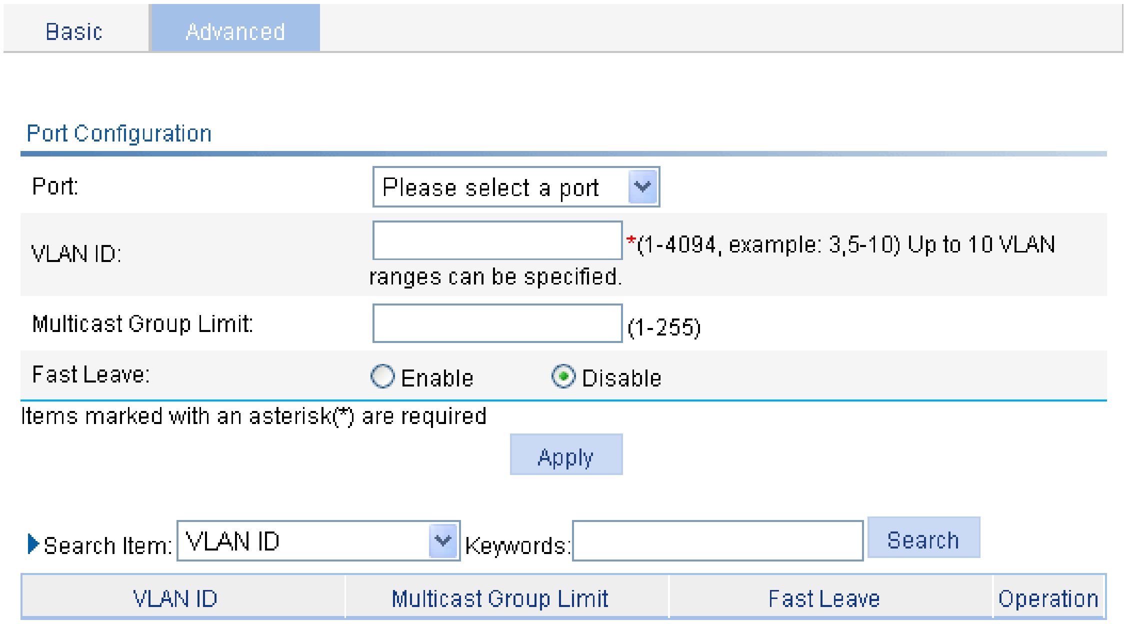
Item	Description
Drop Unknown	Enable or disable the function of dropping unknown multicast packets. Unknown multicast data refer to multicast data for which no entries exist in the IGMP snooping forwarding table. • With the function of dropping unknown multicast data enabled, the switch drops all the unknown multicast data received. • With the function of dropping unknown multicast data disabled, the switch floods unknown multicast data in the VLAN to which the unknown multicast data belong.
Querier	Enable or disable the IGMP snooping querier function. On a network without Layer 3 multicast devices, no IGMP querier-related function can be implemented because a Layer 2 device does not support IGMP. To address this issue, you can enable IGMP snooping querier on a Layer 2 device so that the device can generate and maintain multicast forwarding entries at data link layer, thereby implementing IGMP querier-related functions.
Query interval	Configure the IGMP query interval.

Return to IGMP snooping configuration task list.

Configuring IGMP Snooping Port Functions

Select **Network** > **IGMP Snooping** in the navigation tree to enter the basic configuration page and then click the **Advanced** tab to enter the page shown in Figure 1-5.

Figure 1-5 Advanced configuration



Port Configuration

Port:	Please select a port
VLAN ID:	*(1-4094, example: 3,5-10) Up to 10 VLAN ranges can be specified.
Multicast Group Limit:	(1-255)
Fast Leave:	○ Enable ● Disable

Items marked with an asterisk(*) are required

Search Item: VLAN ID Keywords:

VLAN ID	Multicast Group Limit	Fast Leave	Operation

Table 1-4 describes items for configuring advanced IGMP snooping features.

Table 1-4 Configuration items for advanced IGMP snooping features

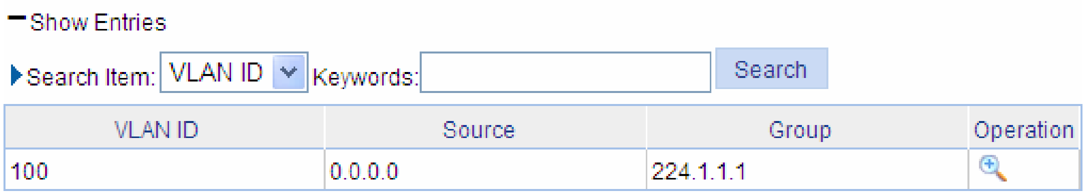
Item	Description
Port	Select the port on which advanced IGMP snooping features are to be configured. The port can be an Ethernet port or Layer-2 aggregate port. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. **Tip** *Advanced IGMP snooping features configured on a Layer 2 aggregate port do not interfere with features configured on its member ports, nor do they take part in aggregation calculations; features configured on a member port of the aggregate group will not take effect until it leaves the aggregate group*
VLAN ID	Specify a VLAN in which you can configure the fast leave function for the port or the maximum number of multicast groups allowed on the port. Configurations made in a VLAN take effect for the ports in this VLAN only.
Group Limit	Configure the maximum number of multicast groups that the port can join. With this feature, you can regulate multicast traffic on the port. **Highlight** *When the number of multicast groups a port has joined reaches the configured threshold, the system deletes all the forwarding entries persistent on that port from the IGMP snooping forwarding table, and the hosts on this port need to join the multicast groups again.*
Fast Leave	Enable or disable the fast leave function for the port. With the fast leave function enabled on a port, the switch, when receiving an IGMP leave message on the port, immediately deletes that port from the outgoing port list of the corresponding forwarding table entry. Then, when receiving IGMP group-specific queries for that multicast group, the switch will not forward them to that port. In VLANs where only one host is attached to each port, the fast leave function helps improve bandwidth and resource usage. **Highlight** *If fast leave is enabled for a port to which more than one host is attached, when one host leaves a multicast group, the other hosts listening to the same multicast group will fail to receive multicast data.*

Return to IGMP snooping configuration task list.

Display IGMP Snooping Multicast Entry Information

Select **Network** > **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in Figure 1-3. Click the plus sign (+) in front of **Show Entries** to display information about IGMP snooping multicast entries, as shown in Figure 1-6. You can view the detailed information of an entry by click the 🔍 icon corresponding to the entry.

Figure 1-6 Display entry information

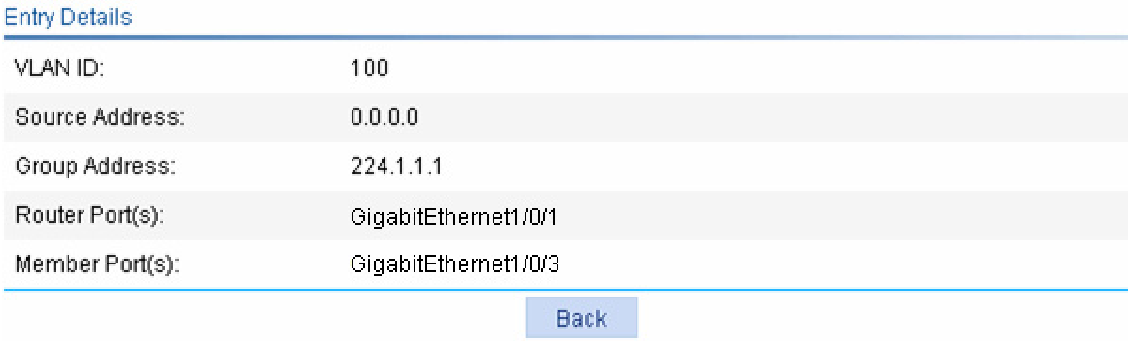


− Show Entries

Search Item: VLAN ID Keywords: Search

VLAN ID	Source	Group	Operation
100	0.0.0.0	224.1.1.1	🔍

Figure 1-7 Details about an IGMP snooping multicast entry



Entry Details

VLAN ID:	100
Source Address:	0.0.0.0
Group Address:	224.1.1.1
Router Port(s):	GigabitEthernet1/0/1
Member Port(s):	GigabitEthernet1/0/3

Table 1-5Table 1-5Table 1-5 describes the IGMP snooping multicast entry information.

Table 1-5 Description of IGMP snooping multicast entries

Item	Description
VLAN ID	ID of the VLAN to which the entry belongs
Source Address	Multicast source address, where 0.0.0.0 indicates all multicast sources.
Group Address	Multicast group address
Router Port(s)	All router ports
Member Port(s)	All member ports

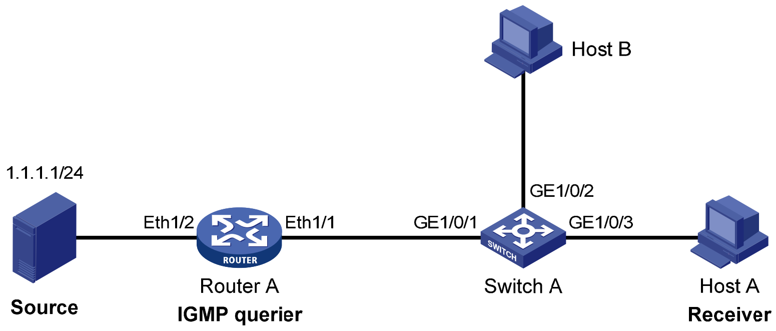
Return to IGMP snooping configuration task list.

IGMP Snooping Configuration Examples

Network requirements

- As shown in Figure 1-8, Router A connects to a multicast source (Source) through Ethernet 1/2, and to Switch A through Ethernet 1/1.
- The multicast source sends multicast data to group 224.1.1.1. Host A is a receiver of the multicast group.
- IGMPv2 runs on Router A and IGMP snooping version 2 runs on Switch A.
- The function of dropping unknown multicast packets is enabled on Switch A to prevent Switch A from flooding multicast packets in the VLAN if no corresponding Layer 2 forwarding entry exists.
- The fast leave function is enabled for GigabitEthernet 1/0/3 on Switch A to improve bandwidth and resource usage.

Figure 1-8 Network diagram for IGMP snooping configuration



Configuration procedure

1) Configure IP addresses

Configure the IP address for each interface as per Figure 1-8. The detailed configuration steps are omitted.

2) Configure Router A

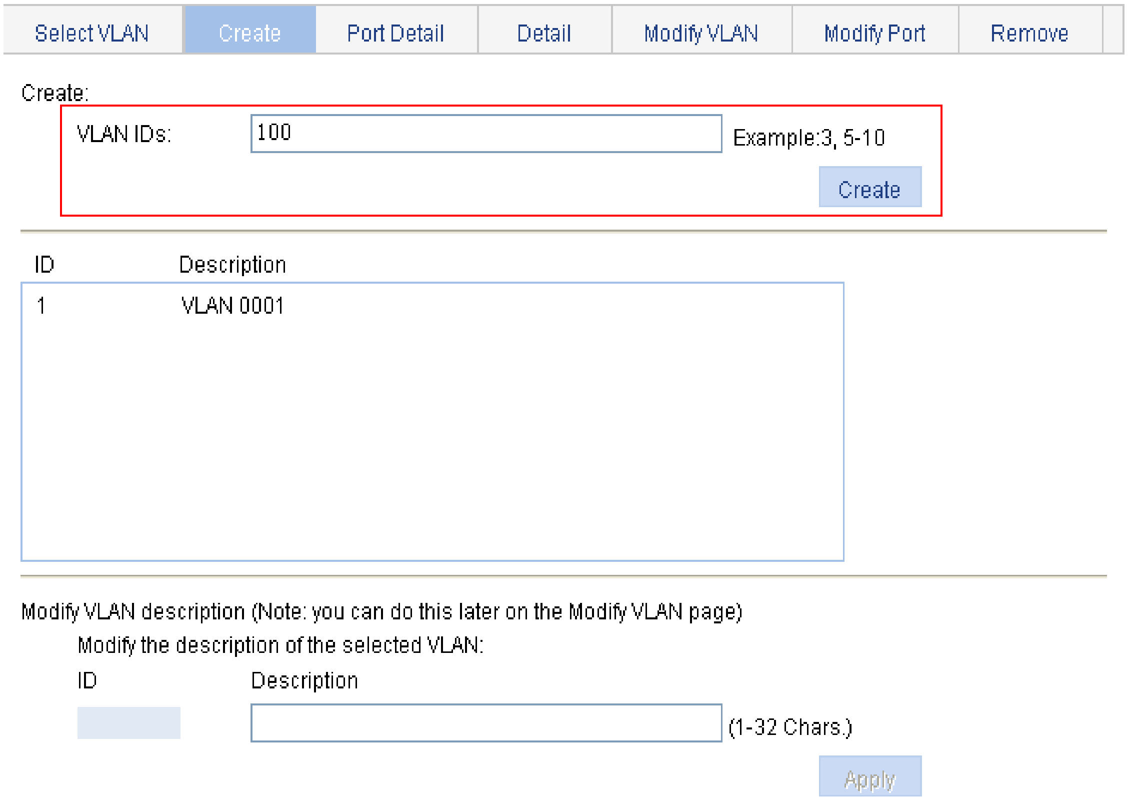
Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/1. The detailed configuration steps are omitted.

3) Configure Switch A

# Create VLAN 100 and add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100.

- Select **Network** > **VLAN** in the navigation tree and click the **Create** tab to enter the configuration page shown in Figure 1-9.

Figure 1-9 Create VLAN 100



Create:

VLAN IDs: 100 Example:3, 5-10

ID	Description
1	VLAN 0001

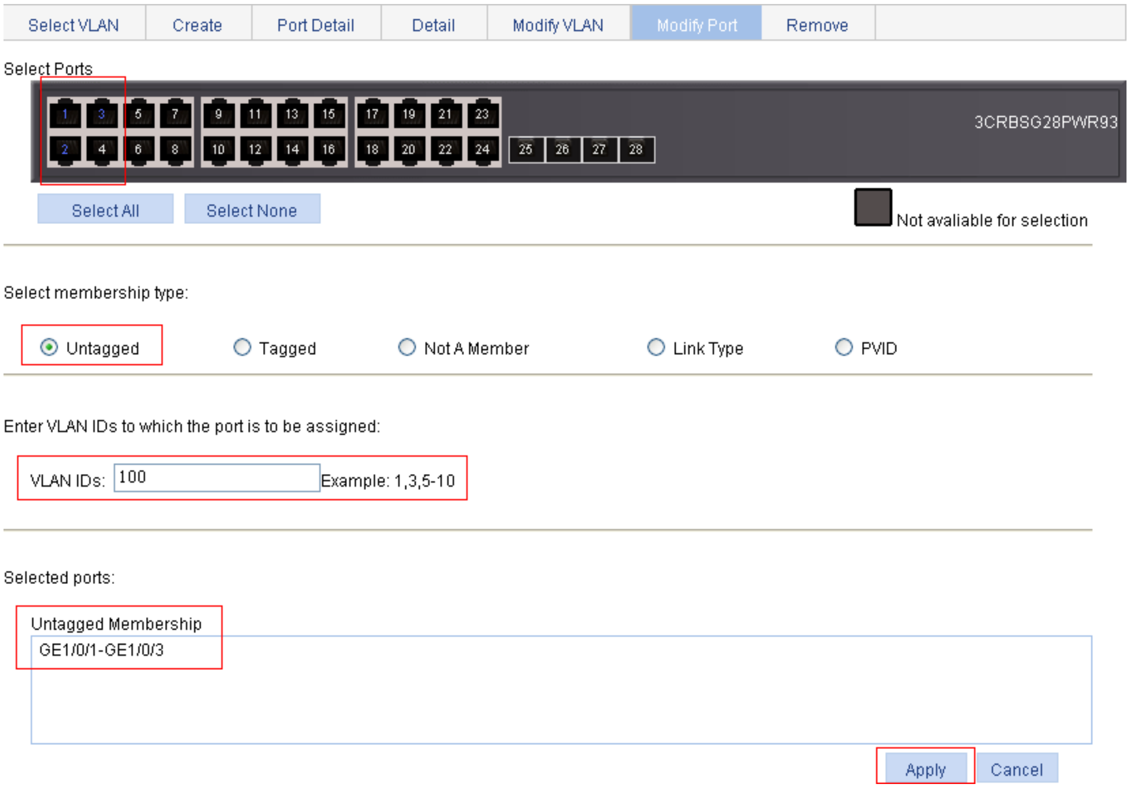
Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID Description (1-32 Chars.)

- Type the VLAN ID 100.
- Click **Apply** to complete the operation.
- Click the **Modify Port** tab to enter the configuration page shown in Figure 1-10.

Figure 1-10 Add a port to the VLAN



Select membership type:

● Untagged ○ Tagged ○ Not A Member ○ Link Type ○ PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: 100 Example: 1,3,5-10

Selected ports:

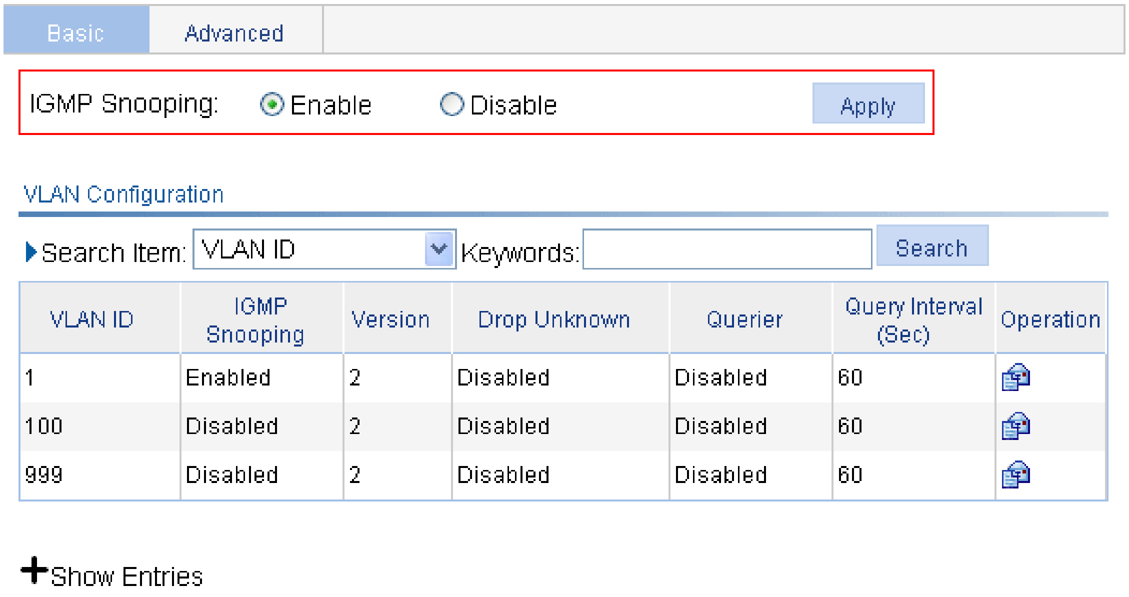
Untagged Membership
GE1/0/1-GE1/0/3

- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** field.
- Select the **Untagged** radio button for **Select membership type**.
- Type the VLAN ID 100.
- Click **Apply** to complete the operation.

# Enable IGMP snooping globally.

- Select **Network** > **IGMP snooping** in the navigation tree to enter the basic configuration page and perform the following as shown in Figure 1-11.

Figure 1-11 Enable IGMP snooping globally



IGMP Snooping: ● Enable ○ Disable Apply

VLAN Configuration

Search Item: VLAN ID Keywords: Search

VLAN ID	IGMP Snooping	Version	Drop Unknown	Querier	Query Interval (Sec)	Operation
1	Enabled	2	Disabled	Disabled	60	📝
100	Disabled	2	Disabled	Disabled	60	📝
999	Disabled	2	Disabled	Disabled	60	📝

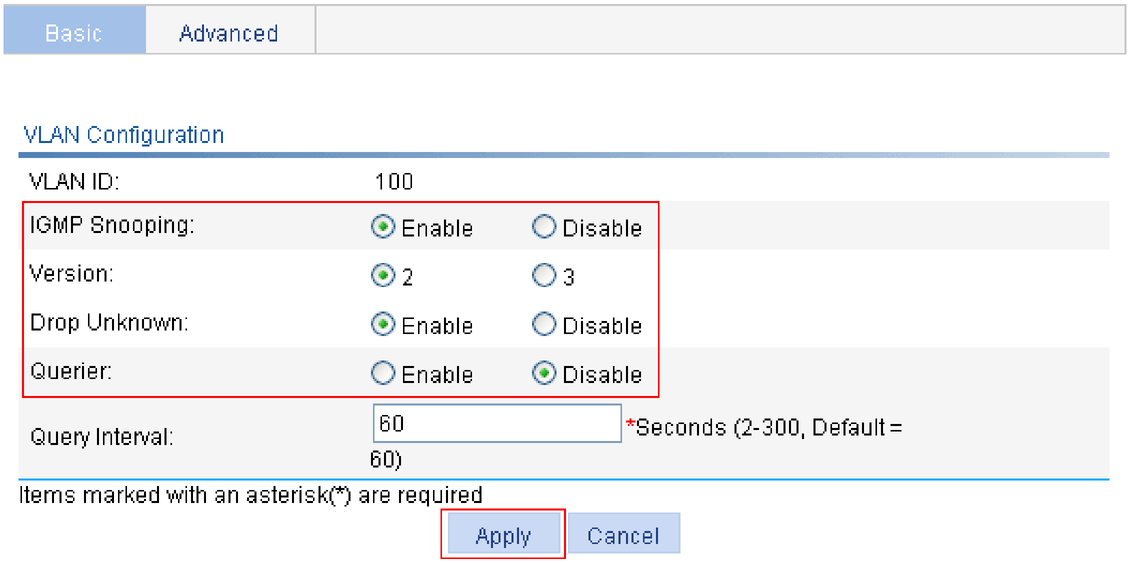
+Show Entries

- Select **Enable** and click **Apply** to globally enable IGMP snooping.

# In VLAN 100, enable IGMP snooping and the function of dropping unknown multicast data.

- Click the 📝 icon corresponding to VLAN 100 to enter its configuration page and perform the following configurations, as shown in Figure 1-12.

Figure 1-12 Configure IGMP snooping in the VLAN



VLAN Configuration

VLAN ID:	100	
IGMP Snooping:	● Enable	○ Disable
Version:	● 2	○ 3
Drop Unknown:	● Enable	○ Disable
Querier:	○ Enable	● Disable
Query Interval:	60 *Seconds (2-300, Default = 60)	

Items marked with an asterisk(*) are required

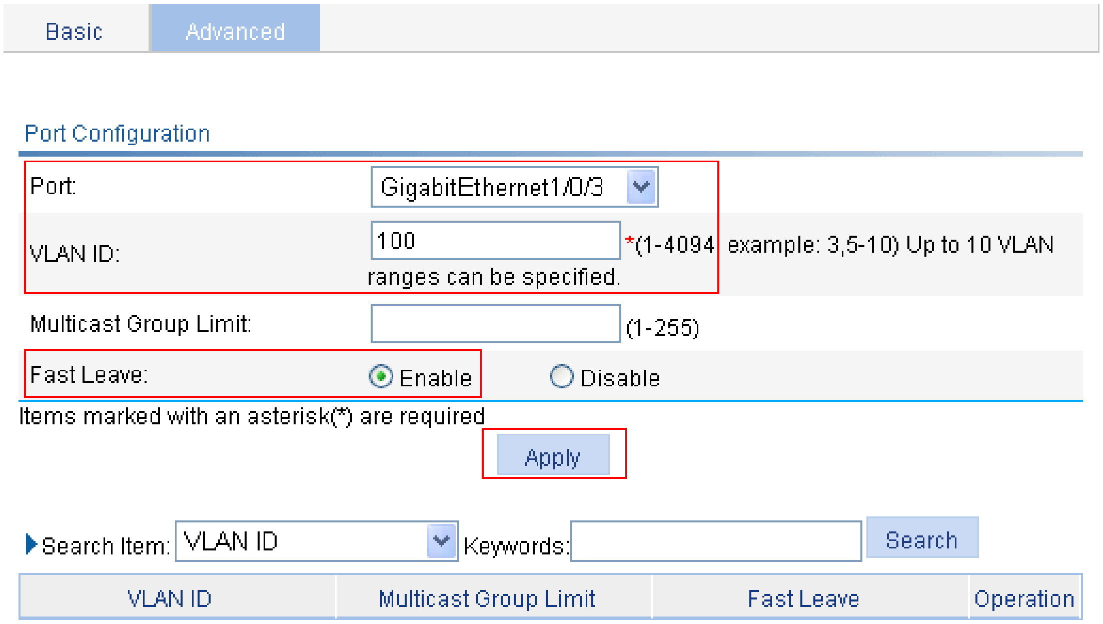
Apply Cancel

- Select the **Enable** radio buttion for **IGMP snooping** and **2** for **Version**.
- Select the **Enable** radio buttion for **Drop Unknown**.
- Select the **Disable** radio button for **Querier**.
- Click **Apply** to complete the operation.

# Enable the fast leave function for GigabitEthernet 1/0/3.

- Click the **Advanced** tab and perform the following configurations as shown in Figure 1-13.

Figure 1-13 Configure IGMP snooping on GigabitEthernet 1/0/3.



Port: GigabitEthernet1/0/3

VLAN ID: 100 *(1-4094 example: 3,5-10) Up to 10 VLAN ranges can be specified.

Multicast Group Limit: (1-255)

Fast Leave: ● Enable ○ Disable

Items marked with an asterisk(*) are required

Search Item: VLAN ID Keywords:

VLAN ID	Multicast Group Limit	Fast Leave	Operation

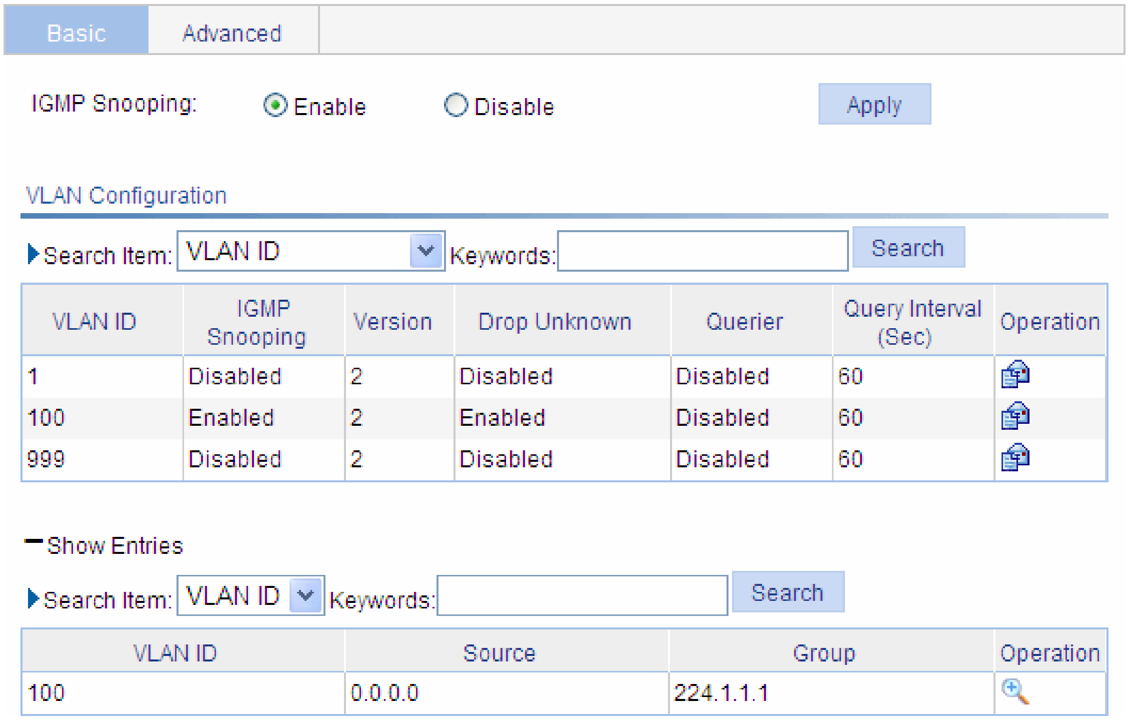
- Select GigabitEthernet 1/0/3 from the **Port** drop-down list.
- Type the VLAN ID 100.
- Select the **Enable** radio buttion for **Fast Leave**.
- Click **Apply** to complete the operation.

Configuration verification

# Display the IGMP snooping multicast entry information on Switch A.

- Select **Network** > **IGMP Snooping** in the navigation tree to enter the basic configuration page.
- Click the plus sign (+) in front of **Show Entries** in the basic VLAN configuration page to display information about IGMP snooping multicast entries, as shown in Figure 1-14.

Figure 1-14 IGMP snooping multicast entry information displaying page



IGMP Snooping: ● Enable ○ Disable

VLAN Configuration

Search Item: VLAN ID Keywords:

VLAN ID	IGMP Snooping	Version	Drop Unknown	Querier	Query Interval (Sec)	Operation
1	Disabled	2	Disabled	Disabled	60	
100	Enabled	2	Enabled	Disabled	60	
999	Disabled	2	Disabled	Disabled	60	

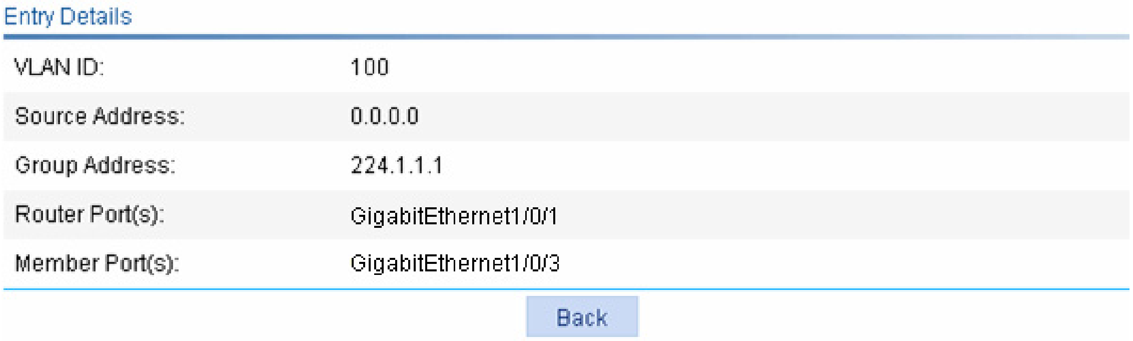
Show Entries

Search Item: VLAN ID Keywords:

VLAN ID	Source	Group	Operation
100	0.0.0.0	224.1.1.1	🔍

- Click the 🔍 icon corresponding to the multicast entry (0.0.0.0, 224.1.1.1) to view details about this entry, as shown in Figure 1-15.

Figure 1-15 Details about an IGMP snooping multicast entry



Entry Details

VLAN ID:	100
Source Address:	0.0.0.0
Group Address:	224.1.1.1
Router Port(s):	GigabitEthernet1/0/1
Member Port(s):	GigabitEthernet1/0/3

As shown above, GigabitEthernet 1/0/3 of Switch A is listening to multicast streams destined for multicast group 224.1.1.1.

Table of Contents

1 Routing Configuration

Note

The term “router” in this document refers to a switch supporting routing function.

Overview

Routers are responsible for routing packets on the Internet. A router selects an appropriate route according to the destination address of a received packet and forwards the packet to the next router. The last router on the path is responsible for sending the packet to the destination host.

Routing Table

Routers forward packets through a routing table. Each entry in the table specifies which physical interface a packet should go out to reach the next hop (the next router) or the directly connected destination.

Routes in a routing table fall into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

A route entry has the following items:

- Destination IP address: Destination IP address or destination network.
- Mask: Specifies, together with the destination address, the address of the destination network.
- Outbound interface: Specifies the interface through which a matching IP packet is to be forwarded.
- Nexthop: Specifies the address of the next hop router on the path.
- Preference for the route: Routes to the same destination may be found by various routing protocols or manually configured, and routing protocols and static routes have different priorities configured. The route with the highest priority (the smallest value) will be selected as the optimal route.

Static Route

A static route is manually configured. If a network’s topology is simple, you only need to configure static routes for the network to work normally. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, some routes will be unreachable. In this case, the network administrator has to modify the static routes manually.

While configuring a static route, you can specify either the output interface or the next hop address as needed. The nexthop address cannot be a local interface's IP address; otherwise, the route configuration will not take effect.

Actually, it is necessary to identify next hop addresses for all route entries because the router needs to use the next hop address of a matching entry to resolve the corresponding link layer address.

Default Route

A router selects the default route when it cannot find any matching entry in the routing table for a packet. If there is no default route, the packet will be discarded and an ICMP packet will be sent to the source to report that the destination is unreachable.

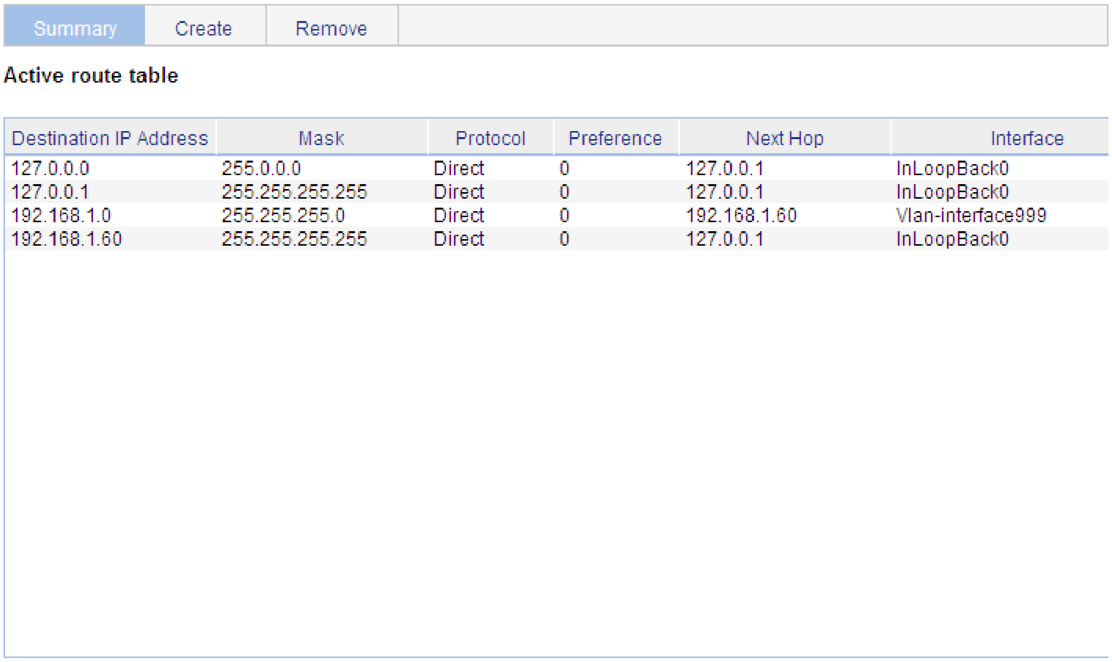
You can configure the default route, an IPv4 static default route has both its destination IP address and mask configured as 0.0.0.0.

Configuring IPv4 Routing

Displaying the IPv4 Active Route Table

Select **Network** > **IPv4 Routing** from the navigation tree to enter the page shown in Figure 1-1.

Figure 1-1 IPv4 active route table



Active route table

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
127.0.0.0	255.0.0.0	Direct	0	127.0.0.1	InLoopBack0
127.0.0.1	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
192.168.1.0	255.255.255.0	Direct	0	192.168.1.60	Vlan-interface999
192.168.1.60	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0

Table 1-1 describes the fields of the IPv4 active route table:

Table 1-1 Description of the fields of the IPv4 active route table

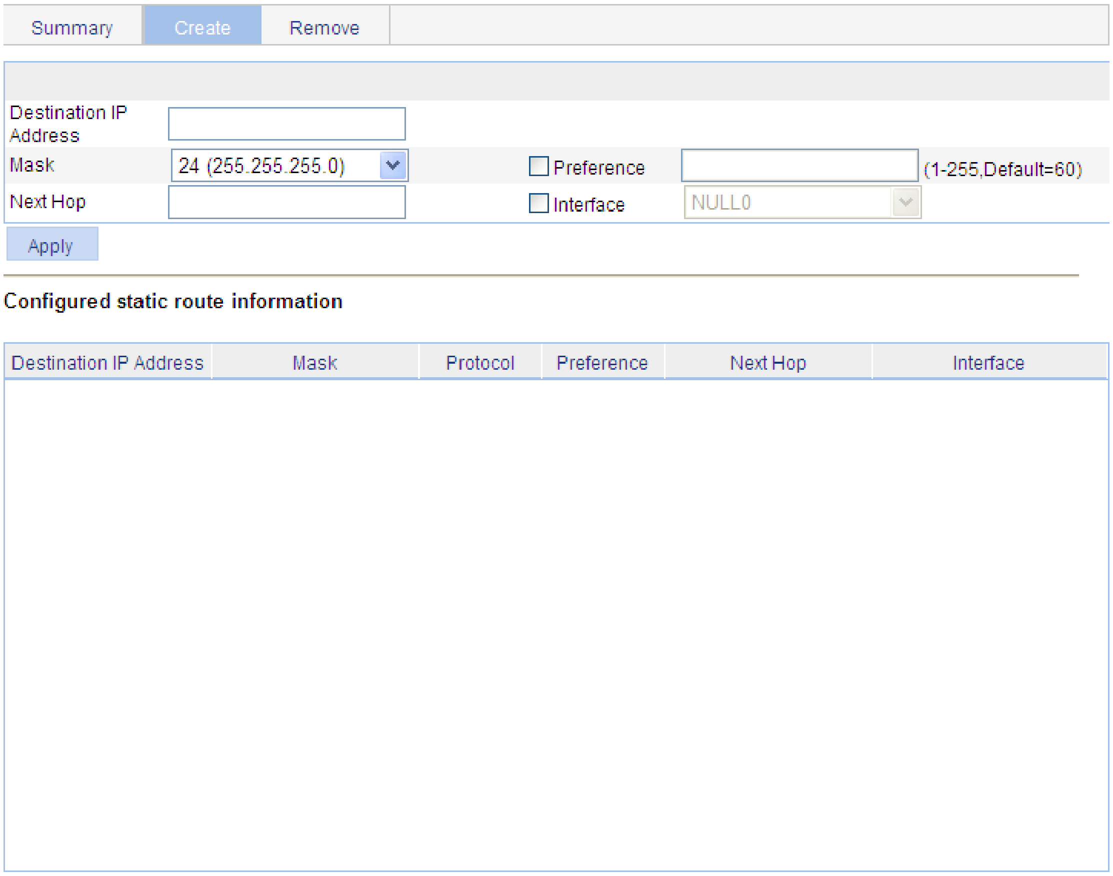
Field	Description
Destination IP Address	Destination IP address and subnet mask of the IPv4 route
Mask	
Protocol	Protocol that discovered the IPv4 route

Field	Description
Preference	Preference value for the IPv4 route The smaller the number, the higher the preference.
Next Hop	Nexthop IP address of the IPv4 route
Interface	Outgoing interface of the IPv4 route. Packets destined for the specified network segment will be sent out the interface.

Creating an IPv4 Static Route

Select **Network** > **IPv4 Routing** from the navigation tree and click the **Create** tab to enter the IPv4 static route configuration page, as shown in Figure 1-2.

Figure 1-2 Create an IPv4 static route



Destination IP Address				
Mask	24 (255.255.255.0)	□ Preference		(1-255,Default=60)
Next Hop		□ Interface	NULL0	

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface

Table 1-2 describes the IPv4 static route configuration items:

Table 1-2 IPv4 static route configuration items

Item	Description
Destination IP Address	Type the destination host or network IP address, in dotted decimal notation.
Mask	Type the mask of the destination IP address. Select a mask length (number of consecutive 1s in the mask) or a mask in dotted decimal notation from the drop-down list.

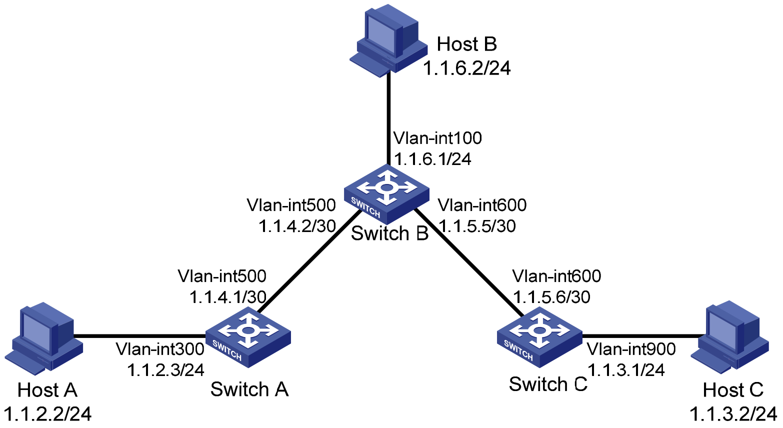
Item	Description
Preference	Set a preference value for the static route. The smaller the number, the higher the preference. For example, specifying the same preference for multiple static routes to the same destination enables load sharing on the routes, while specifying different preferences enables route backup.
Next Hop	Type the nexthop IP address, in dotted decimal notation.
Interface	Select the outgoing interface. You can select any available interface, for example, a virtual interface, of the device. If you select NULL 0, the destination IP address is unreachable.

Static Route Configuration Examples

Network requirements

The IP addresses of devices are shown in Figure 1-3. IPv4 static routes need to be configured on Switch A, Switch B and Switch C for any two hosts to communicate with each other.

Figure 1-3 Network diagram for IPv4 static route configuration



Configuration outlines

1) On Switch A, configure a default route with Switch B as the next hop.
2) On Switch B, configure one static route with Switch A as the next hop and the other with Switch C as the next hop.
3) On Switch C, configure a default route with Switch B as the next hop.

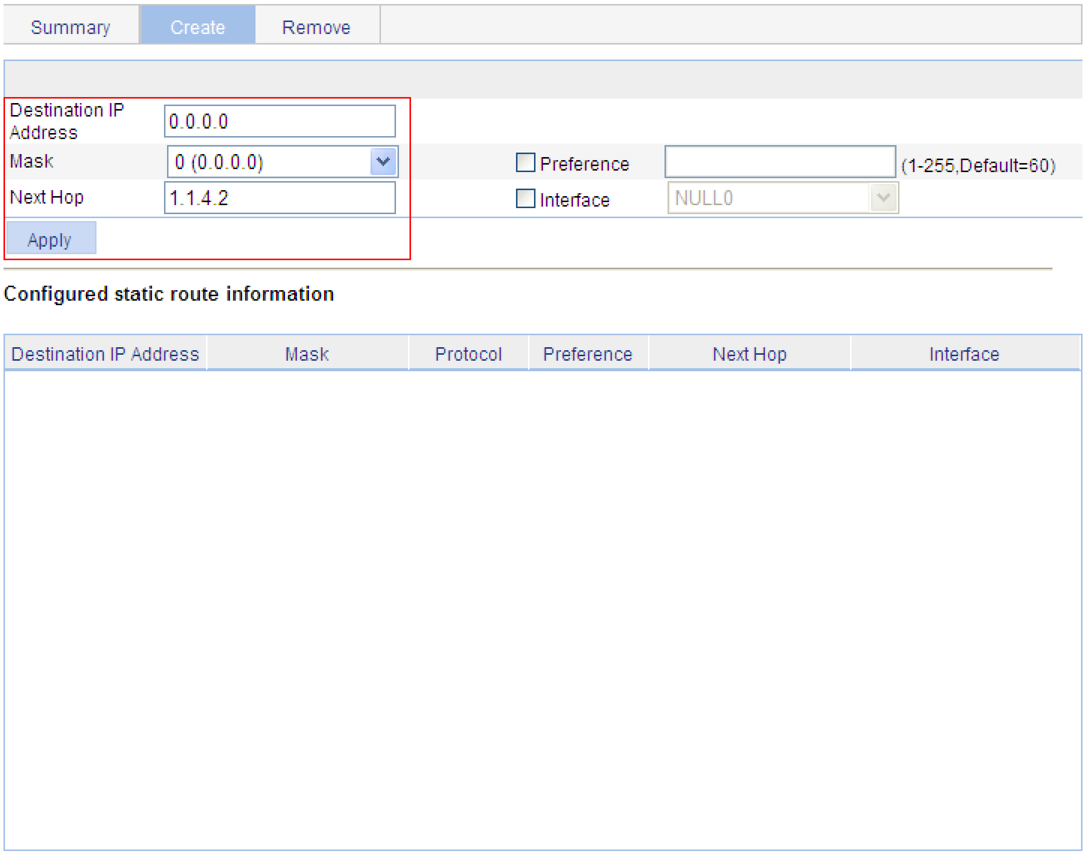
Configuration procedure

1) Configure the IP addresses of the interfaces (omitted)
2) Configure IPv4 static routes

# Configure a default route to Switch B on Switch A.

- After you log in to the web interface of Switch A, select **Network** > **IPv4 Routing** from the navigation tree and then click the **Create** tab to enter the page shown in Figure 1-4.

Figure 1-4 Configure a default route



Destination IP Address	0.0.0.0			
Mask	0 (0.0.0.0)	□ Preference		(1-255,Default=60)
Next Hop	1.1.4.2	□ Interface	NULL0	

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface

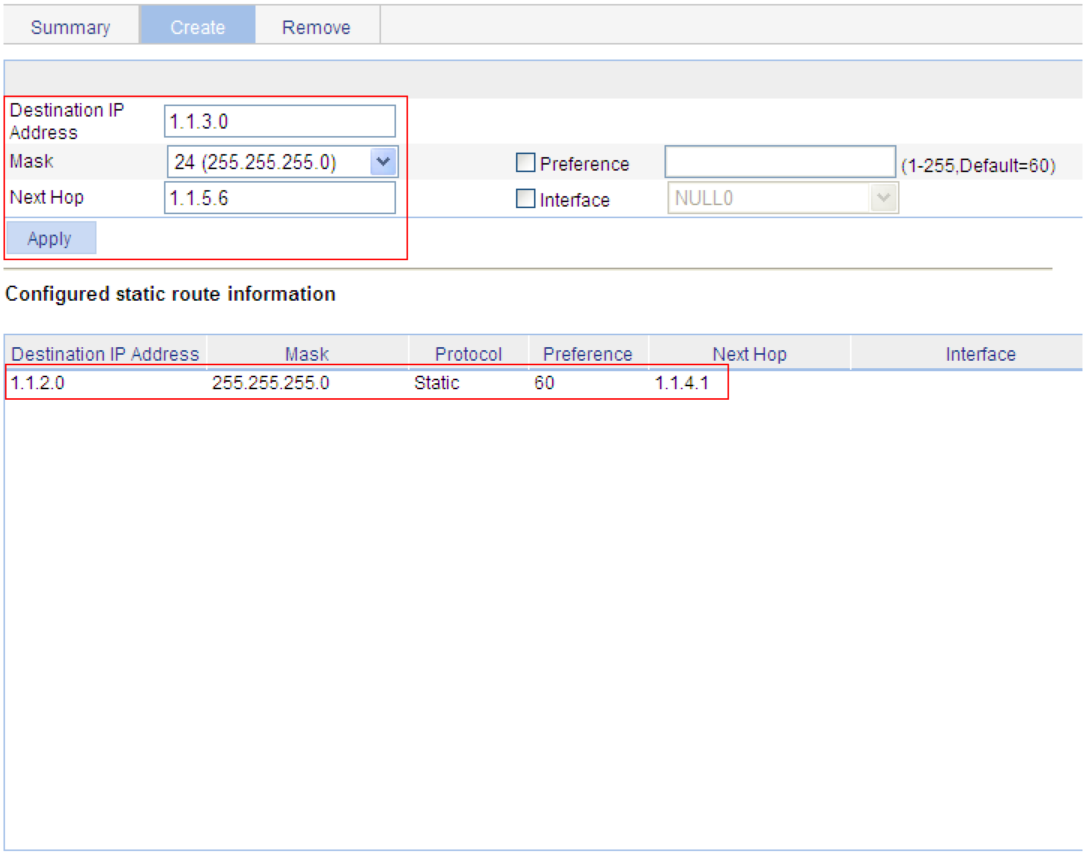
Make the following configurations on the page:

- Type **0.0.0.0** for **Destination IP Address.**
- Select **0 (0.0.0.0)** from the **Mask** drop-down list.
- Type **1.1.4.2** for **Next Hop**.
- Click **Apply**.

# Configure a static route to Switch A and Switch C respectively on Switch B.

- After you log in to the Web interface of Switch B, select **Network** > **IPv4 Routing** from the navigation tree and then click the **Create** tab to enter the page shown in Figure 1-5.

Figure 1-5 Configure a static route



Destination IP Address	1.1.3.0		
Mask	24 (255.255.255.0)	□ Preference	(1-255,Default=60)
Next Hop	1.1.5.6	□ Interface	NULL0

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
1.1.2.0	255.255.255.0	Static	60	1.1.4.1	

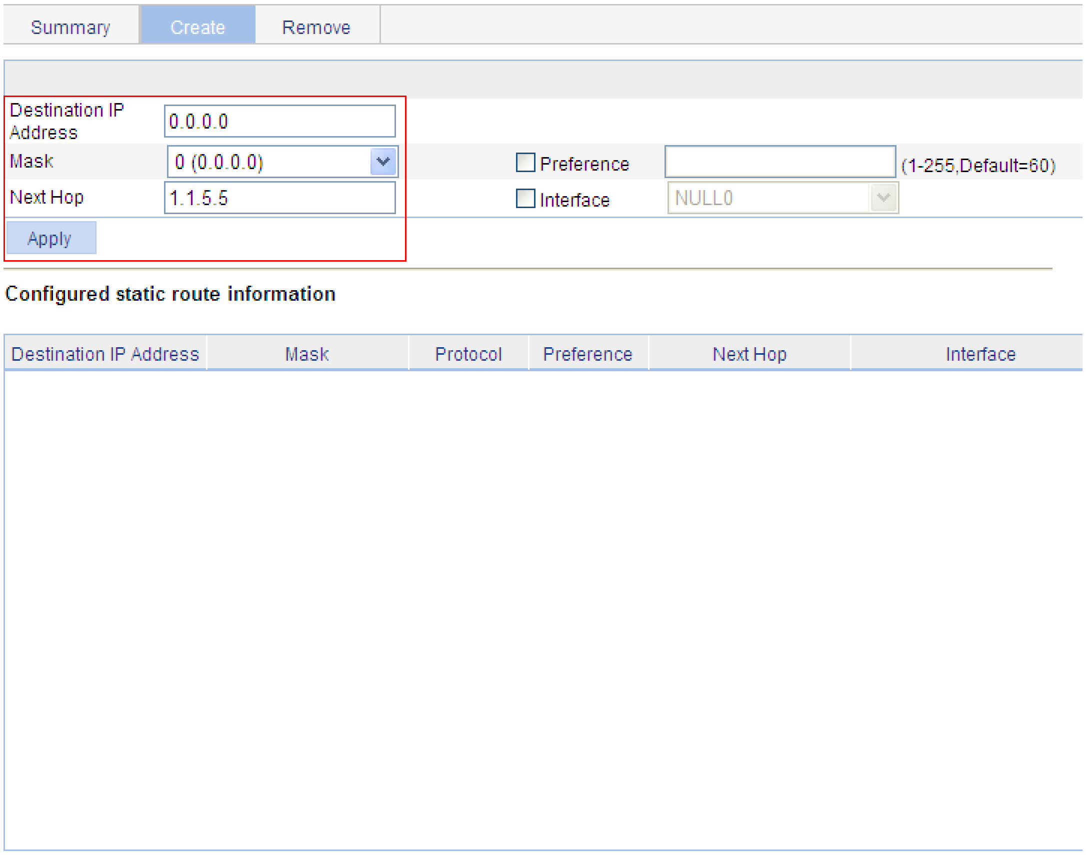
Make the following configurations on the page:

- Type **1.1.2.0** for **Destination IP Address.**
- Select **24 (255.255.255.0)** from the **Mask** drop-down list.
- Type **1.1.4.1** for **Next Hop.**
- Click **Apply.**
- Type **1.1.3.0** for **Destination IP Address.**
- Select **24 (255.255.255.0)** from the **Mask** drop-down list.
- Type **1.1.5.6** for **Next Hop.**
- Click **Apply.**

# Configure a default route to Switch B on Switch C.

- After you log in to the Web interface of Switch C, select **Network** > **IPv4 Routing** from the navigation tree and then click the **Create** tab to enter the page as shown in Figure 1-6.

Figure 1-6 Configure a default route



Destination IP Address	0.0.0.0			
Mask	0 (0.0.0.0)	□ Preference		(1-255,Default=60)
Next Hop	1.1.5.5	□ Interface	NULL0	

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface

- Type **0.0.0.0** for **Destination IP Address**.
- Select **0 (0.0.0.0)** from the **Mask** drop-down list.
- Type **1.1.5.5** for **Next Hop**.
- Click **Apply**.

Verify the configuration

# Display the route table.

Enter the IPv4 route page of Switch A, Switch B, and Switch C respectively to verify that the newly configured static routes are displayed as active routes on the page.

# Use the **ping** command for verification.

Ping Host B from Host A (assuming both hosts run Windows XP).

```
C:\Documents and Settings\Administrator>ping 1.1.3.2

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128

Ping statistics for 1.1.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Precautions

When configuring a static route, note the following:

1) If you do not specify the preference when configuring a static route, the default preference will be used. Reconfiguration of the default preference applies only to newly created static routes. Currently, the Web interface does not support configuration of the default preference.
2) When configuring a static route, the static route does not take effect if you specify the next hop address first and then configure it as the IP address of a local interface, such as a VLAN interface.
3) When specifying the output interface, note that:

- If NULL 0 interface is specified as the output interface, there is no need to configure the next hop address.
- If you want to specify a broadcast interface (such as a VLAN interface) as the output interface, which may have multiple next hops, you need to specify the next hop at the same time.

4) You can delete only static routes on the **Remove** tab.

Table of Contents

1 DHCP Overview

Note

After the DHCP client is enabled on an interface, the interface can dynamically obtain an IP address and other configuration parameters from the DHCP server. This facilitates configuration and centralized management. For details about the DHCP client configuration, refer to *VLAN Interface Configuration*.

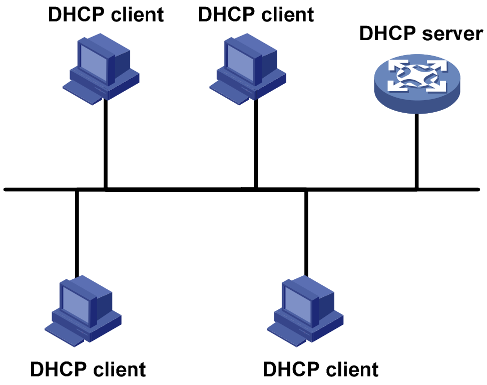
Introduction to DHCP

The fast expansion and growing complexity of networks result in scarce IP addresses assignable to hosts. Meanwhile, as many people need to take their laptops across networks, the IP addresses need to be changed accordingly. Therefore, related configurations on hosts become more complex. The Dynamic Host Configuration Protocol (DHCP) was introduced to solve these problems.

DHCP is built on a client-server model, in which a client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client.

A typical DHCP application, as shown in Figure 1-1, includes a DHCP server and multiple clients (PCs and laptops).

Figure 1-1 A typical DHCP application



A DHCP client can get an IP address and other configuration parameters from a DHCP server on another subnet via a DHCP relay agent. For details about the DHCP relay agent configuration, refer to DHCP Relay Agent Configuration.

DHCP Address Allocation

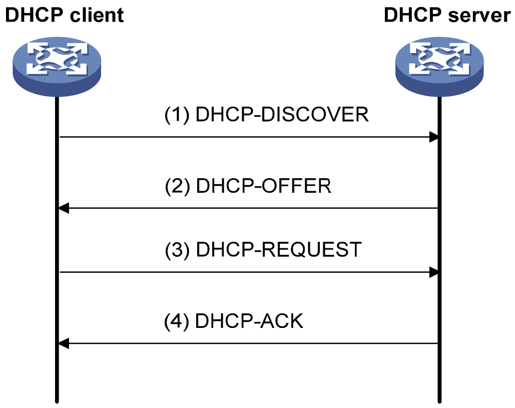
Allocation Mechanisms

DHCP supports three mechanisms for IP address allocation.

- Manual allocation: The network administrator assigns an IP address to a client like a WWW server, and DHCP conveys the assigned address to the client.
- Automatic allocation: DHCP assigns a permanent IP address to a client.
- Dynamic allocation: DHCP assigns an IP address to a client for a limited period of time, which is called a lease. Most DHCP clients obtain their addresses in this way.

Dynamic IP Address Allocation Process

Figure 1-2 Dynamic IP address allocation process



As shown in Figure 1-2, a DHCP client obtains an IP address from a DHCP server via four steps:

1) The client broadcasts a DHCP-DISCOVER message to locate a DHCP server.
2) A DHCP server offers configuration parameters such as an IP address to the client in a DHCP-OFFER message. The sending mode of the DHCP-OFFER is determined by the flag field in the DHCP-DISCOVER message.
3) If several DHCP servers send offers to the client, the client accepts the first received offer, and broadcasts it in a DHCP-REQUEST message to request the IP address formally.
4) All DHCP servers receive the DHCP-REQUEST message, but only the server from which the client accepts the offered IP address returns a DHCP-ACK message to the client, confirming that the IP address has been allocated to the client, or a DHCP-NAK unicast message, denying the IP address allocation.

Note

- After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within the specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.
- IP addresses offered by other DHCP servers are still assignable to other clients.

IP Address Lease Extension

The IP address dynamically allocated by a DHCP server to a client has a lease. When the lease expires, the DHCP server will reclaim the IP address. If the client wants to use the IP address longer, it has to extend the lease duration.

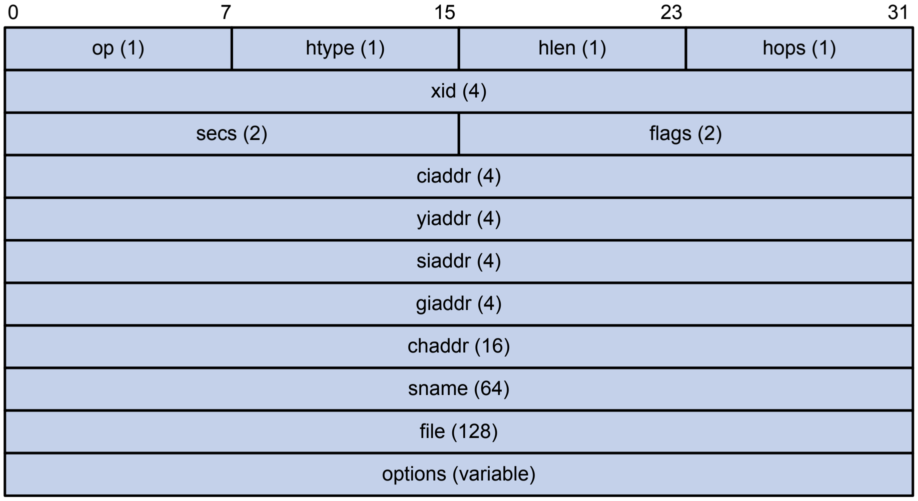
When the half lease duration elapses, the DHCP client sends to the DHCP server a DHCP-REQUEST unicast to extend the lease duration. Upon availability of the IP address, the DHCP server returns a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

If the client receives no reply, it will broadcast another DHCP-REQUEST message for lease extension after 7/8 lease duration elapses. The DHCP server will handle the request as above mentioned.

DHCP Message Format

Figure 1-3 gives the DHCP message format, which is based on the BOOTP message format and involves eight types. These types of messages have the same format except that some fields have different values. The numbers in parentheses indicate the size of each field in bytes.

Figure 1-3 DHCP message format



- op: Message type defined in option field. 1 = REQUEST, 2 = REPLY
- htype, hlen: Hardware address type and length of a DHCP client.
- hops: Number of relay agents a request message traveled.
- xid: Transaction ID, a random number chosen by the client to identify an IP address allocation.
- secs: Filled in by the client, the number of seconds elapsed since the client began address acquisition or renewal process. Currently this field is reserved and set to 0.
- flags: The leftmost bit is defined as the BROADCAST (B) flag. If this flag is set to 0, the DHCP server sent a reply back by unicast; if this flag is set to 1, the DHCP server sent a reply back by broadcast. The remaining bits of the flags field are reserved for future use.
- ciaddr: Client IP address.
- yiaddr: 'your' (client) IP address, assigned by the server.
- siaddr: Server IP address, from which the clients obtained configuration parameters.
- giaddr: IP address of the first relay agent a request message traveled.
- chaddr: Client hardware address.
- sname: Server host name, from which the client obtained configuration parameters.

- file: Bootfile name and path information, defined by the server to the client.
- options: Optional parameters field that is variable in length, which includes the message type, lease, domain name server IP address, and WINS IP address.

DHCP Options

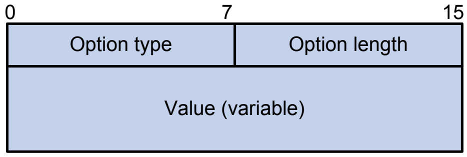
DHCP Options Overview

The DHCP message adopts the same format as the Bootstrap Protocol (BOOTP) message for compatibility, but differs from it in the option field, which identifies new features for DHCP.

DHCP uses the option field in DHCP messages to carry control information and network configuration parameters, implementing dynamic address allocation and providing more network configuration information for clients.

Figure 1-4 shows the DHCP option format.

Figure 1-4 DHCP option format



Introduction to DHCP Options

The common DHCP options are as follows:

- Option 6: DNS server option. It specifies the DNS server IP address to be assigned to the client.
- Option 51: IP address lease option.
- Option 53: DHCP message type option. It identifies the type of the DHCP message.
- Option 55: Parameter request list option. It is used by a DHCP client to request specified configuration parameters. The option contains values that correspond to the parameters requested by the client.
- Option 66: TFTP server name option. It specifies a TFTP server to be assigned to the client.
- Option 67: Bootfile name option. It specifies the bootfile name to be assigned to the client.
- Option 150: TFTP server IP address option. It specifies the TFTP server IP address to be assigned to the client.
- Option 121: Classless route option. It specifies a list of classless static routes (the destination addresses in these static routes are classless) that the requesting client should add to its routing table.
- Option 33: Static route option. It specifies a list of classful static routes (the destination addresses in these static routes are classful) that a client should add to its routing table. If Option 121 exists, Option 33 is ignored.

For more information about DHCP options, refer to RFC 2132.

Introduction to Option 82

Some options, such as Option 82, have no unified definitions in RFC 2132.

Option 82 is the relay agent option in the option field of the DHCP message. It records the location information of the DHCP client. When a DHCP relay agent or DHCP snooping device receives a client's request, it adds Option 82 to the request message before forwarding the message to the server.

The administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

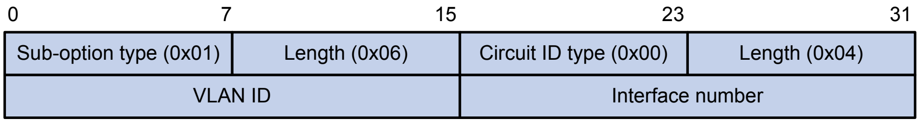
Option 82 involves at most 255 sub-options. At least one sub-option is defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

Option 82 has no unified definition. Its padding formats vary with vendors.

By default, the normal padding format is used on the device. You can specify the code type for the sub-options as ASCII or HEX. The padding contents for sub-options in the normal padding format are as follows:

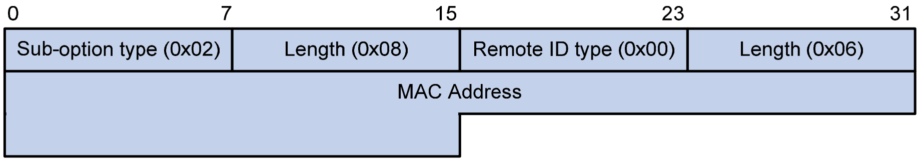
- Sub-option 1: Padded with the VLAN ID and interface number of the interface that received the client's request. The following figure gives its format. The value of the sub-option type is 1, and that of the circuit ID type is 0.

Figure 1-5 Sub-option 1 in normal padding format



- Sub-option 2: Padded with the MAC address of the DHCP relay agent interface or the MAC address of the DHCP snooping device that received the client's request. The following figure gives its format. The value of the sub-option type is 2, and that of the remote ID type is 0.

Figure 1-6 Sub-option 2 in normal padding format



Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 3046: DHCP Relay Agent Information Option

2 DHCP Relay Agent Configuration

Introduction to DHCP Relay Agent

Application Environment

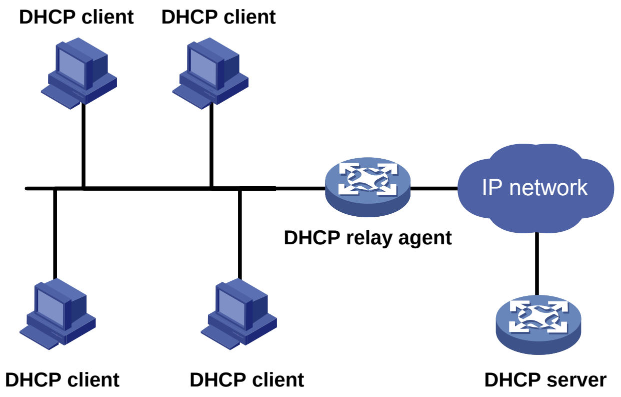
Since DHCP clients request IP addresses via broadcast messages, the DHCP server and clients must be on the same subnet. Therefore, a DHCP server must be available on each subnet, which is not practical.

DHCP relay agent solves the problem. Via a relay agent, DHCP clients communicate with a DHCP server on another subnet to obtain configuration parameters. Thus, DHCP clients on different subnets can contact the same DHCP server, and centralized management and cost reduction are achieved.

Fundamentals

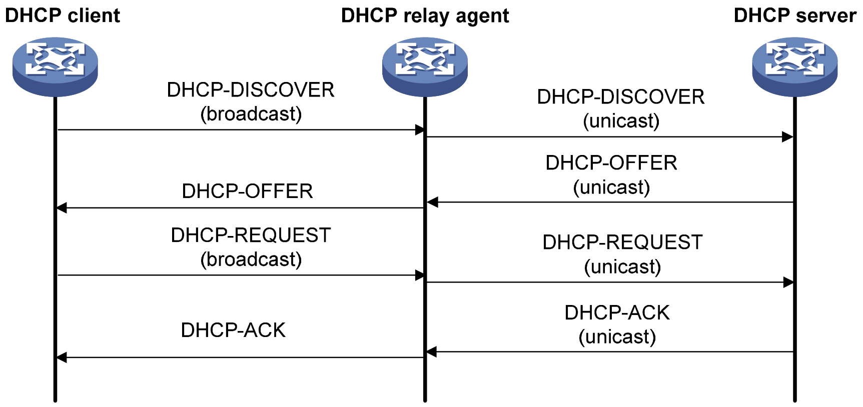
Figure 2-1 shows a typical application of the DHCP relay agent.

Figure 2-1 DHCP relay agent application



No matter whether a relay agent exists or not, the DHCP server and client interact with each other in a similar way (see section Dynamic IP Address Allocation Process). The following describes the forwarding process on the DHCP relay agent.

Figure 2-2 DHCP relay agent work process



As shown in Figure 2-2, the DHCP relay agent works as follows:

1) After receiving a DHCP-DISCOVER or DHCP-REQUEST broadcast message from a DHCP client, the DHCP relay agent fills the giaddr field of the message with its IP address and forwards the message to the designated DHCP server in unicast mode.
2) Based on the giaddr field, the DHCP server returns an IP address and other configuration parameters to the relay agent, which conveys them to the client.

DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

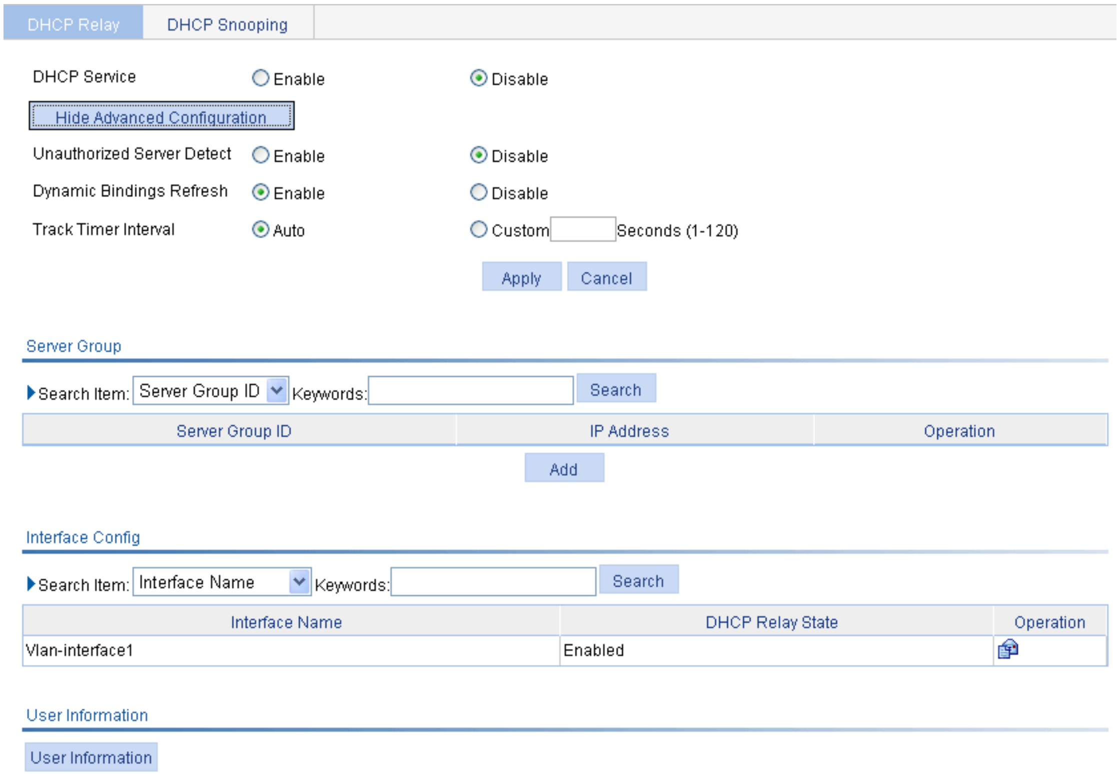
Task	Remarks
Enabling DHCP and Configuring Advanced Parameters for the DHCP Relay Agent	Required Enable DHCP globally and configure advanced DHCP parameters. By default, global DHCP is disabled.
Creating a DHCP Server Group	Required To improve reliability, you can specify several DHCP servers as a group on the DHCP relay agent and correlate a relay agent interface with the server group. When the interface receives requesting messages from clients, the relay agent will forward them to all the DHCP servers of the group.
Enabling the DHCP Relay Agent on an Interface	Required Enable the DHCP relay agent on an interface, and correlate the interface with a DHCP server group. With DHCP enabled, interfaces work in the DHCP server mode by default. **Highlight** • *You can enable either the DHCP server or the DHCP relay agent on an interface. The latest configuration takes effect.* • *The DHCP relay agent works on interfaces with IP addresses manually configured only.*

Task	Remarks
Configuring and Displaying Clients' IP-to-MAC Bindings	Optional Create a static IP-to-MAC binding, and view static and dynamic bindings. The DHCP relay agent can dynamically record clients' IP-to-MAC bindings after clients get IP addresses. It also supports static bindings, that is, you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses. By default, no static binding is created.

Enabling DHCP and Configuring Advanced Parameters for the DHCP Relay Agent

Select **Network** > **DHCP** from the navigation tree to enter the default **DHCP Relay** page. Enable or disable DHCP in the **DHCP Service** field. Click **Display Advanced Configuration** to expand the advanced DHCP relay agent configuration field, as shown in Figure 2-3.

Figure 2-3 DHCP relay agent configuration page



DHCP Service ○ Enable ● Disable

Unauthorized Server Detect ○ Enable ● Disable

Dynamic Bindings Refresh ● Enable ○ Disable

Track Timer Interval ● Auto ○ Custom Seconds (1-120)

Server Group

Search Item: Server Group ID Keywords:

Server Group ID	IP Address	Operation

Interface Config

Search Item: Interface Name Keywords:

Interface Name	DHCP Relay State	Operation
Vlan-interface1	Enabled	

User Information

Table 2-1 describes the DHCP service and advanced DHCP relay agent configuration items.

Table 2-1 DHCP service and advanced DHCP relay agent configuration items

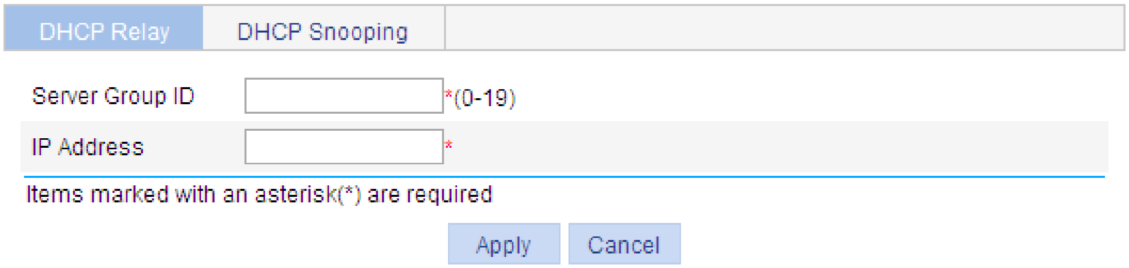
Item	Description
DHCP Service	Enable or disable global DHCP.
Unauthorized Server Detect	Enable or disable unauthorized DHCP server detection. There are unauthorized DHCP servers on networks, which reply DHCP clients with wrong IP addresses. With this feature enabled, upon receiving a DHCP request, the DHCP relay agent will record the IP address of any DHCP server that assigned an IP address to the DHCP client and the receiving interface. The administrator can use this information to check out DHCP unauthorized servers. The device puts a record once for each DHCP server. The administrator needs to find unauthorized DHCP servers from the log information. After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.
Dynamic Bindings Refresh	Enable or disable periodic refresh of dynamic client entries, and set the refresh interval. Via the DHCP relay agent, a DHCP client sends a DHCP-RELEASE unicast message to the DHCP server to relinquish its IP address. In this case the DHCP relay agent simply conveys the message to the DHCP server, thus it does not remove the IP address from dynamic client entries. To solve this problem, the periodic refresh of dynamic client entries feature is introduced. With this feature, the DHCP relay agent uses the IP address of a client and the MAC address of the DHCP relay agent interface to periodically send a DHCP-REQUEST message to the DHCP server. • If the server returns a DHCP-ACK message or does not return any message within a specified interval, which means that the IP address is assignable now, the DHCP relay agent will age out the client entry. • If the server returns a DHCP-NAK message, which means the IP address is still in use, the relay agent will not age it out. Note that if the **Auto** radio button is clicked on, the refresh interval is calculated by the relay agent according to the number of client entries.
Track Timer Interval	

Return to DHCP Relay Agent Configuration Task List.

Creating a DHCP Server Group

Select **Network** > **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in Figure 2-3. In the **Server Group** field, click **Add** to enter the page shown in Figure 2-4.

Figure 2-4 Create a server group



Server Group ID *(0-19)

IP Address *

Items marked with an asterisk(*) are required

Table 2-2 describes the DHCP server group configuration items.

Table 2-2 DHCP server group configuration items

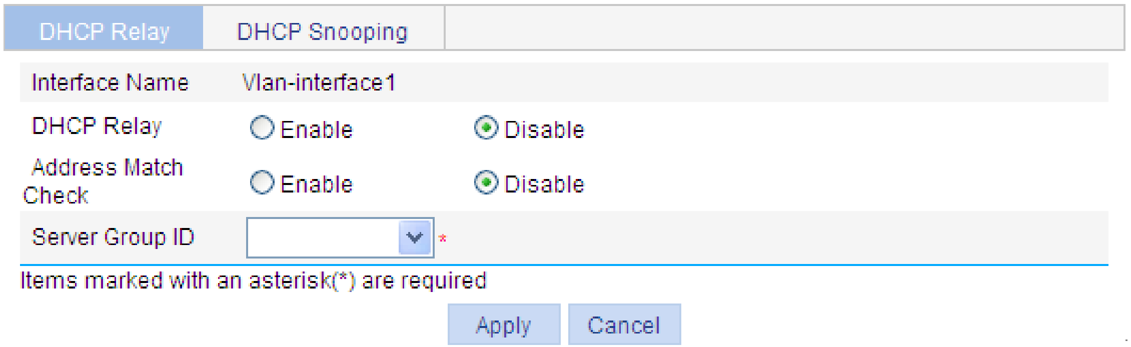
Item	Description
Server Group ID	Type the ID of a DHCP server group. You can create up to 20 DHCP server groups.
IP Address	Type the IP address of a server in the DHCP server group. The server IP address cannot be on the same subnet as the IP address of the DHCP relay agent; otherwise, the client cannot obtain an IP address.

Return to DHCP Relay Agent Configuration Task List.

Enabling the DHCP Relay Agent on an Interface

Select **Network** > **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in Figure 2-3. In the **Interface Config** field, the DHCP relay agent state of interfaces is displayed. Click the 📋 icon of a specific interface to enter the page shown in Figure 2-5.

Figure 2-5 Configure a DHCP relay agent interface



Interface Name Vlan-interface1

DHCP Relay ○ Enable ● Disable

Address Match Check ○ Enable ● Disable

Server Group ID *

Items marked with an asterisk(*) are required

Table 2-3 describes the DHCP relay agent interface configuration items.

Table 2-3 DHCP relay agent interface configuration items

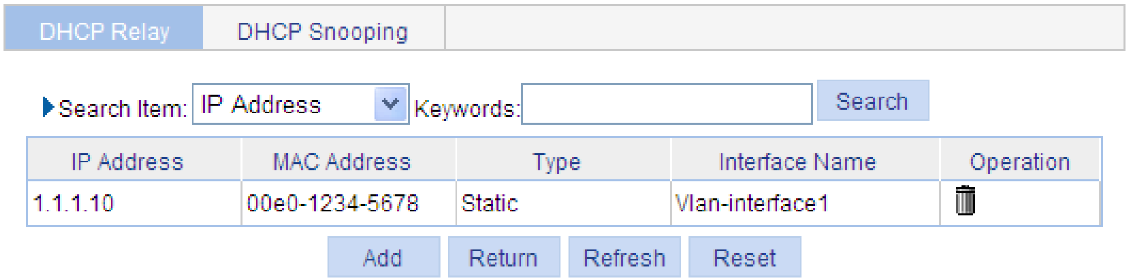
Item	Description
Interface Name	This field displays the name of a specific interface.
DHCP Relay	Enable or disable the DHCP relay agent on the interface.
Address Match Check	Enable or disable IP address check. With this function enabled, the DHCP relay agent checks whether a requesting client's IP and MAC addresses match a binding (dynamic or static) on the DHCP relay agent. If not, the client cannot access outside networks via the DHCP relay agent. This prevents invalid IP address configuration.
Server Group ID	Correlate the interface with a DHCP server group. A DHCP server group can be correlated with multiple interfaces.

Return to DHCP Relay Agent Configuration Task List.

Configuring and Displaying Clients' IP-to-MAC Bindings

Select **Network** > **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in Figure 2-3. In the **User Information** field, click the **User Information** button to view static and dynamic bindings, as shown in Figure 2-6. Click **Add** to enter the page shown in Figure 2-7.

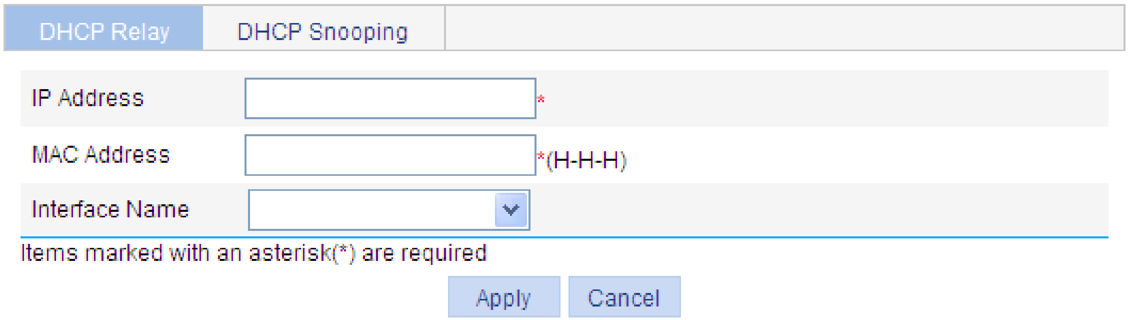
Figure 2-6 Display clients' IP-to-MAC bindings



Search Item: IP Address Keywords:

IP Address	MAC Address	Type	Interface Name	Operation
1.1.1.10	00e0-1234-5678	Static	Vlan-interface1	🗑

Figure 2-7 Create a static IP-to-MAC binding



IP Address *

MAC Address *(H-H-H)

Interface Name

Items marked with an asterisk(*) are required

Table 2-4 describes static IP-to-MAC binding configuration items.

Table 2-4 Static IP-to-MAC binding configuration items

Item	Description
IP Address	Type the IP address of a DHCP client.
MAC Address	Type the MAC address of the DHCP client.
Interface Name	Select the Layer 3 interface connected with the DHCP client. **Highlight** *The interface of a static binding entry must be configured as a DHCP relay agent; otherwise, address entry conflicts may occur.*

Return to DHCP Relay Agent Configuration Task List.

DHCP Relay Agent Configuration Example

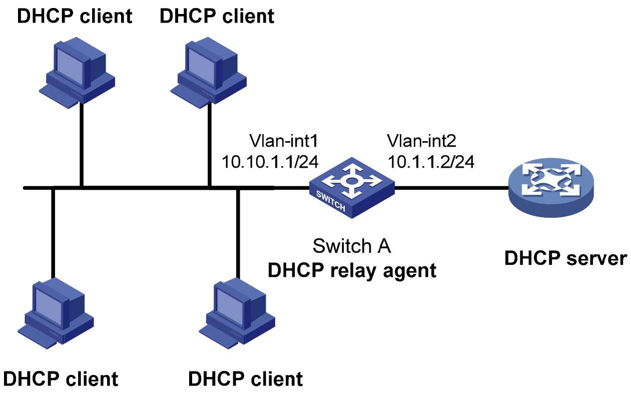
Network requirements

As shown in Figure 2-8, VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and the IP address of

VLAN-interface 2 is 10.1.1.1/24. VLAN-interface 2 is connected to the DHCP server whose IP address is 10.1.1.1/24.

The switch forwards messages between DHCP clients and the DHCP server.

Figure 2-8 Network diagram for DHCP relay agent configuration



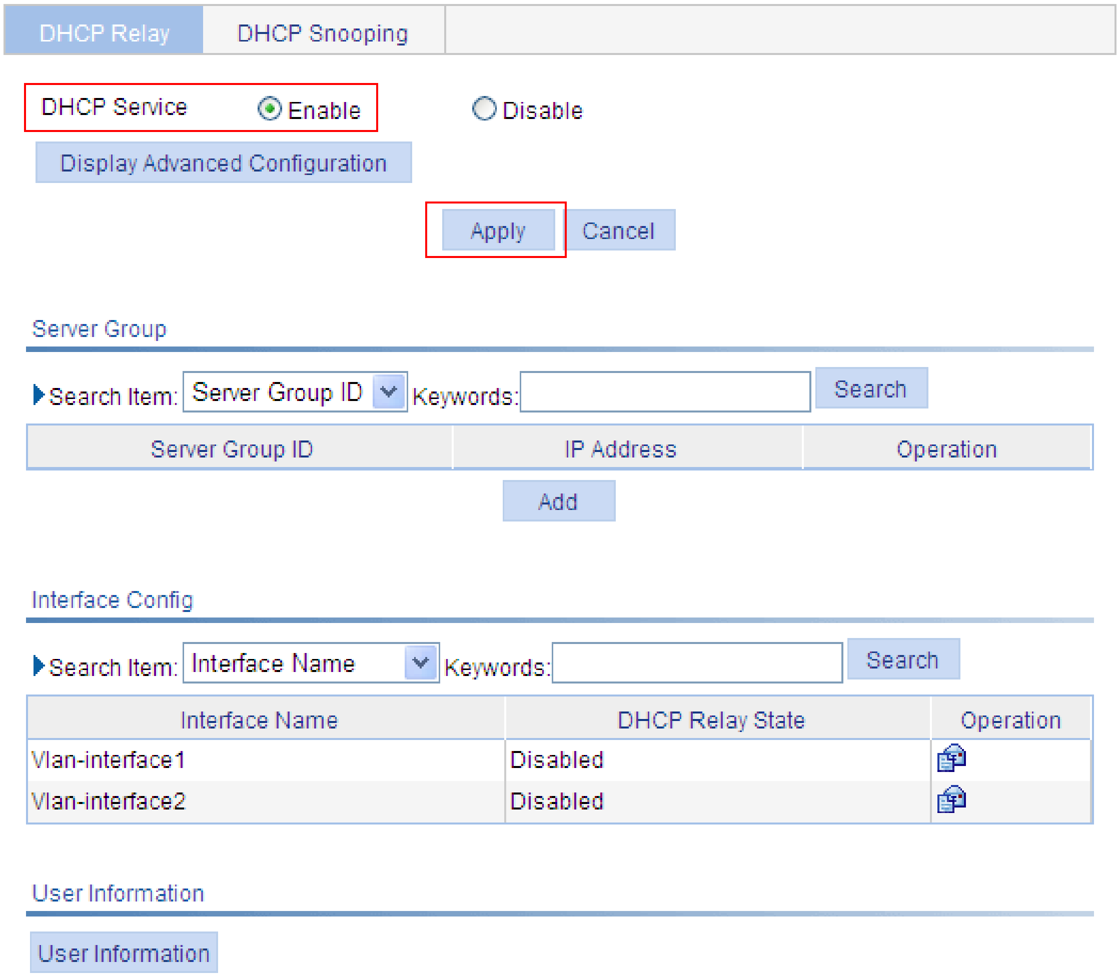
Configuration procedure

1) Specify IP addresses for interfaces (omitted)
2) Configure the DHCP relay agent

# Enable DHCP.

- Select **Network** > **DHCP** from the navigation tree to enter the default **DHCP Relay** page. Perform the following operations, as shown in Figure 2-9.

Figure 2-9 Enable DHCP



DHCP Service ● Enable ○ Disable

Server Group ID	IP Address	Operation

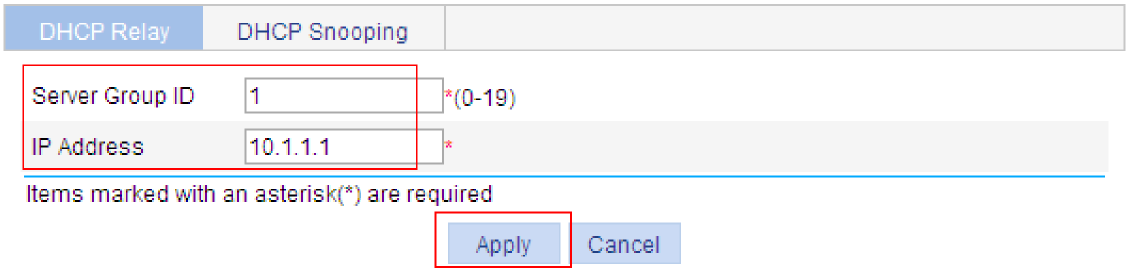
Interface Name	DHCP Relay State	Operation
Vlan-interface1	Disabled	
Vlan-interface2	Disabled	

- Click on the **Enable** radio button next to **DHCP Service**.
- Click **Apply**.

# Configure a DHCP server group.

- In the **Server Group** field, click **Add** and then perform the following operations, as shown in Figure 2-10.

Figure 2-10 Add a DHCP server group



Server Group ID: 1 *(0-19)

IP Address: 10.1.1.1 *

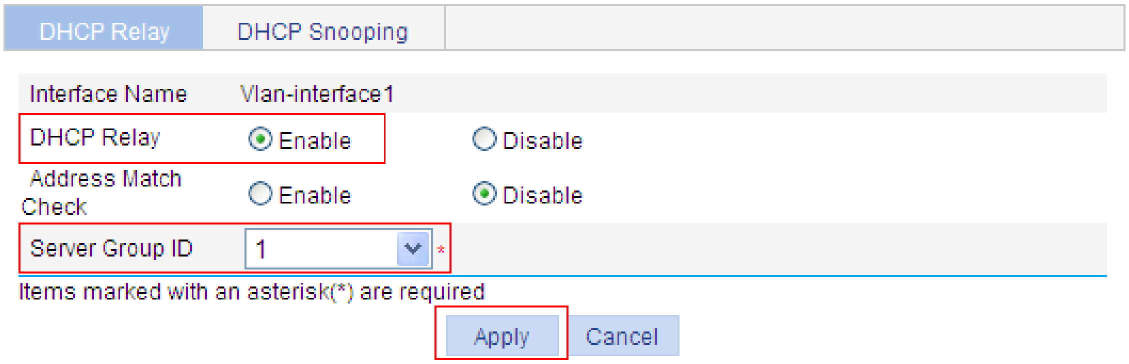
Items marked with an asterisk(*) are required

- Type **1** for **Server Group ID**.
- Type **10.1.1.1** for **IP Address**.
- Click **Apply**.

# Enable the DHCP relay agent on VLAN-interface 1.

- In the **Interface Config** field, click the icon of VLAN-interface 1, and then perform the following operations, as shown in Figure 2-11.

Figure 2-11 Enable the DHCP relay agent on an interface and correlate it with a server group



Interface Name Vlan-interface1

DHCP Relay ● Enable ○ Disable

Address Match Check ○ Enable ● Disable

Server Group ID 1 *

Items marked with an asterisk(*) are required

- Click on the **Enable** radio button next to **DHCP Relay**.
- Select **1** for **Server Group ID**.
- Click **Apply**.

Note

Because the DHCP relay agent and server are on different subnets, you need to configure a static route or dynamic routing protocol to make them reachable to each other.

3 DHCP Snooping Configuration

Note

- A DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.
- You are not recommended to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.

DHCP Snooping Overview

Functions of DHCP Snooping

As a DHCP security feature, DHCP snooping can implement the following:

1) Recording IP-to-MAC mappings of DHCP clients
2) Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers

Recording IP-to-MAC mappings of DHCP clients

DHCP snooping reads DHCP-REQUEST messages and DHCP-ACK messages from trusted ports to record DHCP snooping entries, including MAC addresses of clients, IP addresses obtained by the clients, ports that connect to DHCP clients, and VLANs to which the ports belong.

Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers

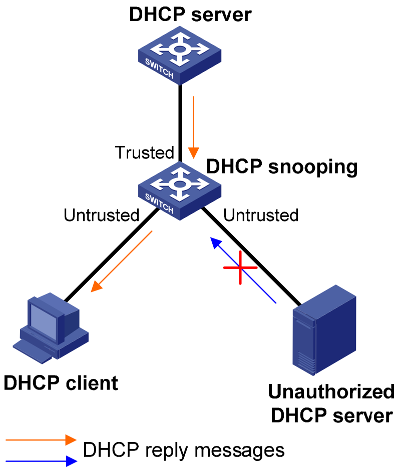
If there is an unauthorized DHCP server on a network, DHCP clients may obtain invalid IP addresses and network configuration parameters, and cannot normally communicate with other network devices. With DHCP snooping, the ports of a device can be configured as trusted or untrusted, ensuring the clients to obtain IP addresses from authorized DHCP servers.

- Trusted: A trusted port forwards DHCP messages normally.
- Untrusted: An untrusted port discards the DHCP-ACK or DHCP-OFFER messages received from any DHCP server.

Application Environment of Trusted Ports

Configuring a trusted port connected to a DHCP server

Figure 3-1 Configure trusted and untrusted ports



As shown in Figure 3-1, a DHCP snooping device's port that is connected to an authorized DHCP server should be configured as a trusted port to forward reply messages from the DHCP server, so that the DHCP client can obtain an IP address from the authorized DHCP server.

Configuring trusted ports in a cascaded network

In a cascaded network involving multiple DHCP snooping devices, the ports connected to other DHCP snooping devices should be configured as trusted ports.

To save system resources, you can disable the trusted ports, which are indirectly connected to DHCP clients, from recording clients' IP-to-MAC bindings upon receiving DHCP requests.

Figure 3-2 Configure trusted ports in a cascaded network

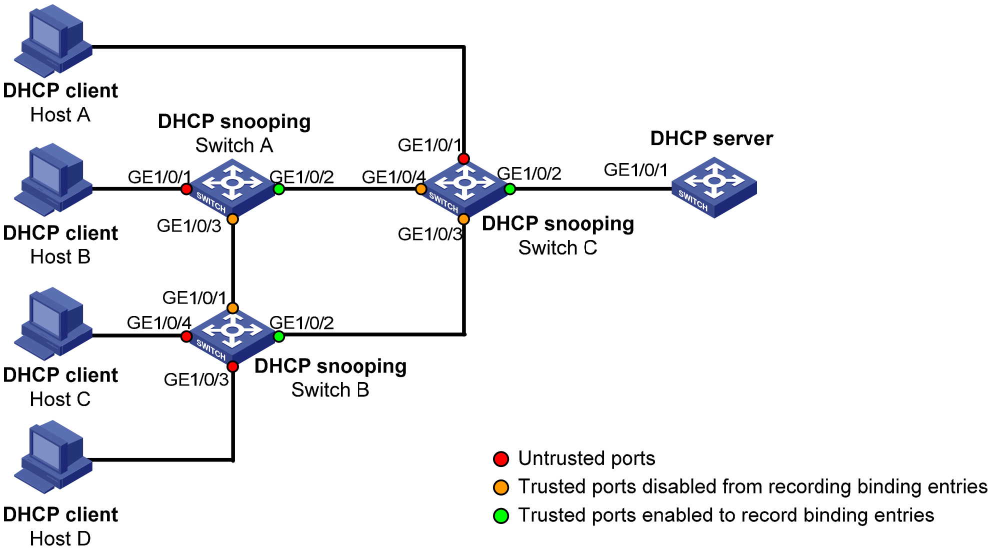


Table 3-1 describes roles of the ports shown in Figure 3-2.

Table 3-1 Roles of ports

Device	Untrusted port	Trusted port disabled from recording binding entries	Trusted port enabled to record binding entries
Switch A	GigabitEthernet 1/0/1	GigabitEthernet 1/0/3	GigabitEthernet 1/0/2
Switch B	GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4	GigabitEthernet 1/0/1	GigabitEthernet 1/0/2
Switch C	GigabitEthernet 1/0/1	GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4	GigabitEthernet 1/0/2

DHCP Snooping Support for Option 82

Option 82 records the location information of the DHCP client. The administrator can locate the DHCP client to further implement security control and accounting. For more information, refer to Introduction to Option 82.

If DHCP snooping supports Option 82, it will handle a client's request according to the contents defined in Option 82, if any. The handling strategies are described in the table below.

If a reply returned by the DHCP server contains Option 82, the DHCP snooping device will remove the Option 82 before forwarding the reply to the client. If the reply contains no Option 82, the DHCP snooping device forwards it directly.

If a client's requesting message has…	Handling strategy	The DHCP snooping device will…
Option 82	Drop	Drop the message.
	Keep	Forward the message without changing Option 82.
	Replace	Forward the message after replacing the original Option 82 with the Option 82 padded in normal format.
no Option 82	—	Forward the message after adding the Option 82 padded in normal format.

DHCP Snooping Configuration Task List

Complete the following tasks to configure DHCP snooping:

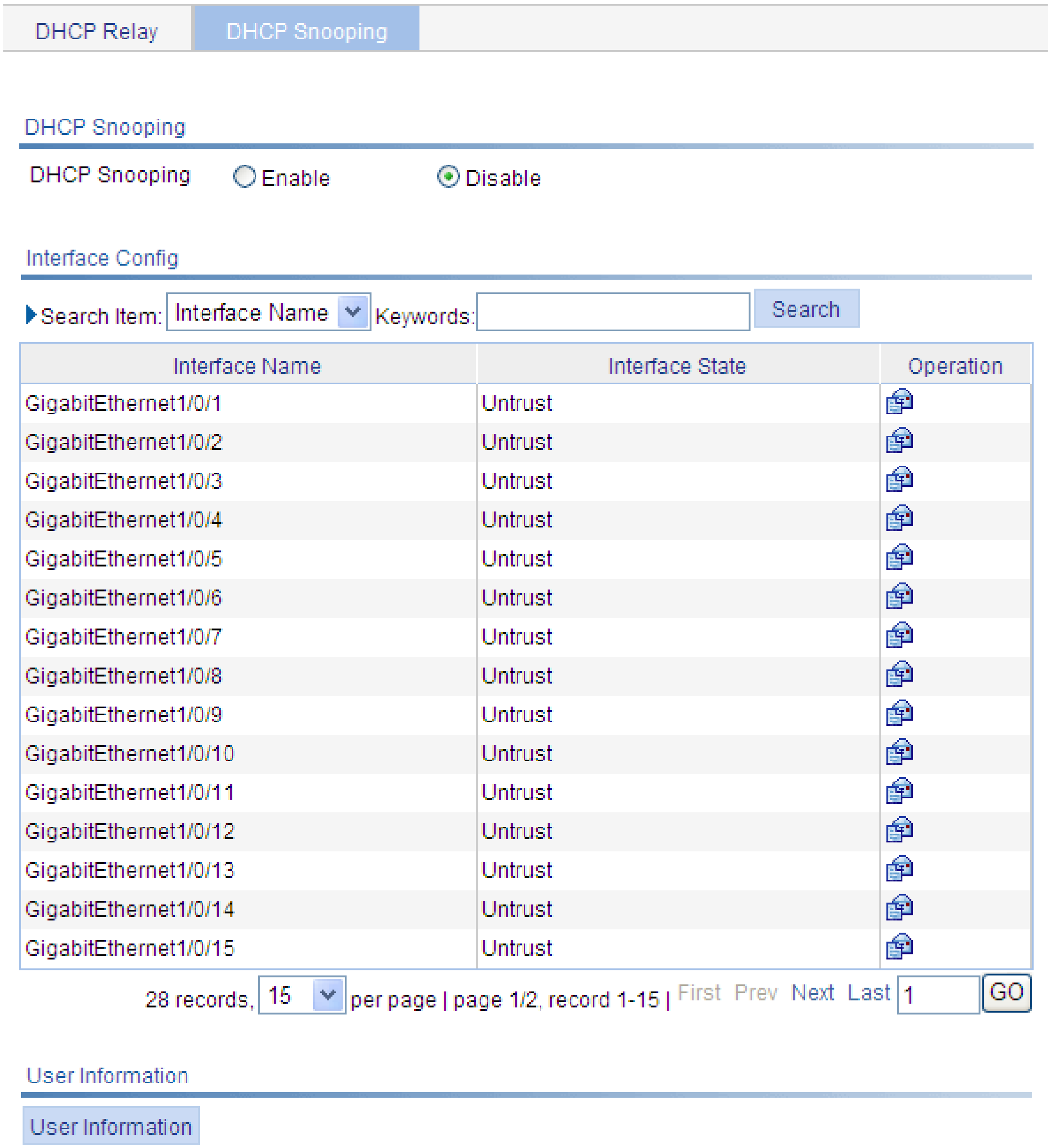
Task	Remarks
Enabling DHCP Snooping	Required By default, DHCP snooping is disabled.
Configuring DHCP Snooping Functions on an Interface	Required Specify an interface as trusted and configure DHCP snooping to support Option 82. By default, an interface is untrusted and DHCP snooping does not support Option 82. **Highlight** *You need to specify the ports connected to the authorized DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.*

Task	Remarks
Displaying Clients' IP-to-MAC Bindings	Optional Display clients' IP-to-MAC bindings recorded by DHCP snooping.

Enabling DHCP Snooping

Select **Network** > **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in Figure 3-3. You can enable or disable DHCP snooping in the **DHCP Snooping** field.

Figure 3-3 DHCP snooping configuration page



DHCP Snooping

DHCP Snooping ○ Enable ● Disable

Interface Config

Search Item: Interface Name Keywords: Search

Interface Name	Interface State	Operation
GigabitEthernet1/0/1	Untrust	✎
GigabitEthernet1/0/2	Untrust	✎
GigabitEthernet1/0/3	Untrust	✎
GigabitEthernet1/0/4	Untrust	✎
GigabitEthernet1/0/5	Untrust	✎
GigabitEthernet1/0/6	Untrust	✎
GigabitEthernet1/0/7	Untrust	✎
GigabitEthernet1/0/8	Untrust	✎
GigabitEthernet1/0/9	Untrust	✎
GigabitEthernet1/0/10	Untrust	✎
GigabitEthernet1/0/11	Untrust	✎
GigabitEthernet1/0/12	Untrust	✎
GigabitEthernet1/0/13	Untrust	✎
GigabitEthernet1/0/14	Untrust	✎
GigabitEthernet1/0/15	Untrust	✎

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

User Information

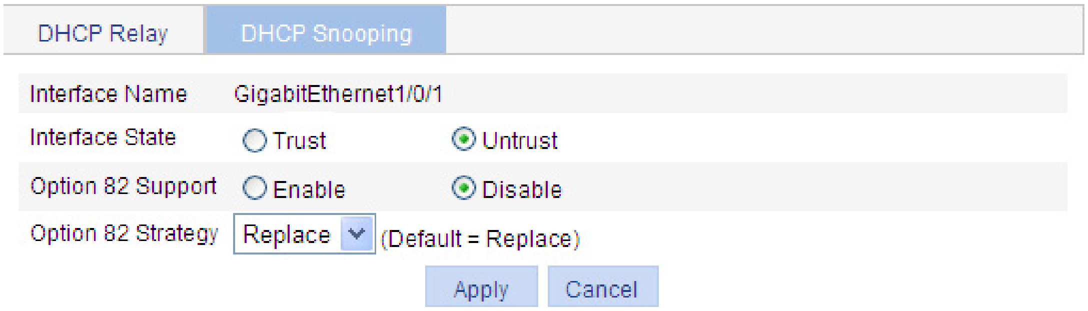
- To enable DHCP snooping, click on the **Enable** radio button in the **DHCP Snooping** field.
- To disable DHCP snooping, click on the **Disable** radio button in the **DHCP Snooping** field.

Return to DHCP Snooping Configuration Task List.

Configuring DHCP Snooping Functions on an Interface

Select **Network** > **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in Figure 3-3. You can view trusted and untrusted ports in the **Interface Config** field. Click the icon of a specific interface to enter the page shown in Figure 3-4.

Figure 3-4 DHCP snooping interface configuration page



Interface Name GigabitEthernet1/0/1

Interface State ○ Trust ● Untrust

Option 82 Support ○ Enable ● Disable

Option 82 Strategy Replace (Default = Replace)

Table 3-2 describes DHCP snooping interface configuration items.

Table 3-2 DHCP snooping interface configuration items

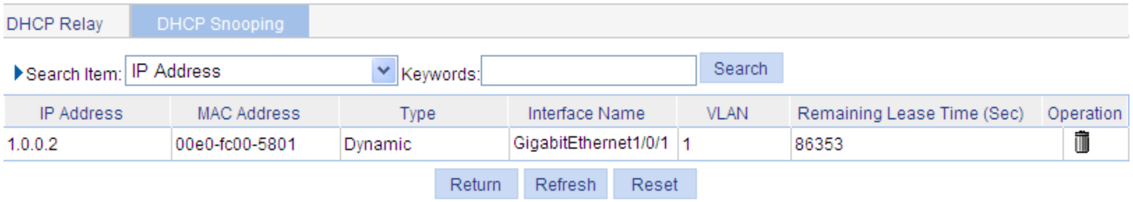
Item	Description
Interface Name	This field displays the name of a specific interface.
Interface State	Configure the interface as trusted or untrusted.
Option 82 Support	Configure DHCP snooping to support Option 82 or not.
Option 82 Strategy	Select the handling strategy for DHCP requests containing Option 82. The strategies include: • Drop: The message is discarded if it contains Option 82. • Keep: The message is forwarded without its Option 82 being changed. • Replace: The message is forwarded after its original Option 82 is replaced with the Option 82 padded in normal format.

Return to DHCP Snooping Configuration Task List.

Displaying Clients' IP-to-MAC Bindings

Select **Network** > **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in Figure 3-3. Click the **User Information** button to view clients' IP-to-MAC bindings recorded by DHCP snooping, as shown in Figure 3-5.

Figure 3-5 DHCP snooping user information



Search Item: IP Address Keywords:

IP Address	MAC Address	Type	Interface Name	VLAN	Remaining Lease Time (Sec)	Operation
1.0.0.2	00e0-fc00-5801	Dynamic	GigabitEthernet1/0/1	1	86353	🗑

Table 3-3 describes DHCP snooping user information configuration items.

Table 3-3 DHCP snooping user information configuration items

Item	Description
IP Address	This field displays the IP address assigned by the DHCP server to the client.
MAC Address	This field displays the MAC address of the client.
Type	This field displays the client type, which can be: • Dynamic: The IP-to-MAC binding is generated dynamically. • Static: The IP-to-MAC binding is configured manually. Currently, static bindings are not supported.
Interface Name	This field displays the device interface to which the client is connected.
VLAN	This field displays the VLAN to which the device belongs.
Remaining Lease Time	This field displays the remaining lease time of the IP address.

Return to DHCP Snooping Configuration Task List.

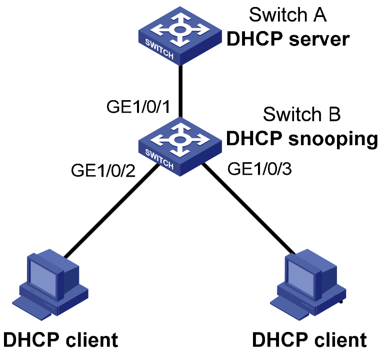
DHCP Snooping Configuration Example

Network requirements

As shown in Figure 3-6, a DHCP snooping device (Switch B) is connected to a DHCP server through GigabitEthernet 1/0/1, and to DHCP clients through GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

- Enable DHCP snooping on Switch B and configure DHCP snooping to support Option 82. Configure the handling strategy for DHCP requests containing Option 82 as **replace**.
- Enable GigabitEthernet 1/0/1 to forward DHCP server responses; disable GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 from forwarding DHCP server responses.
- Configure Switch B to record clients' IP-to-MAC address bindings in DHCP-REQUEST messages and DHCP-ACK messages received from a trusted port.

Figure 3-6 Network diagram for DHCP snooping configuration

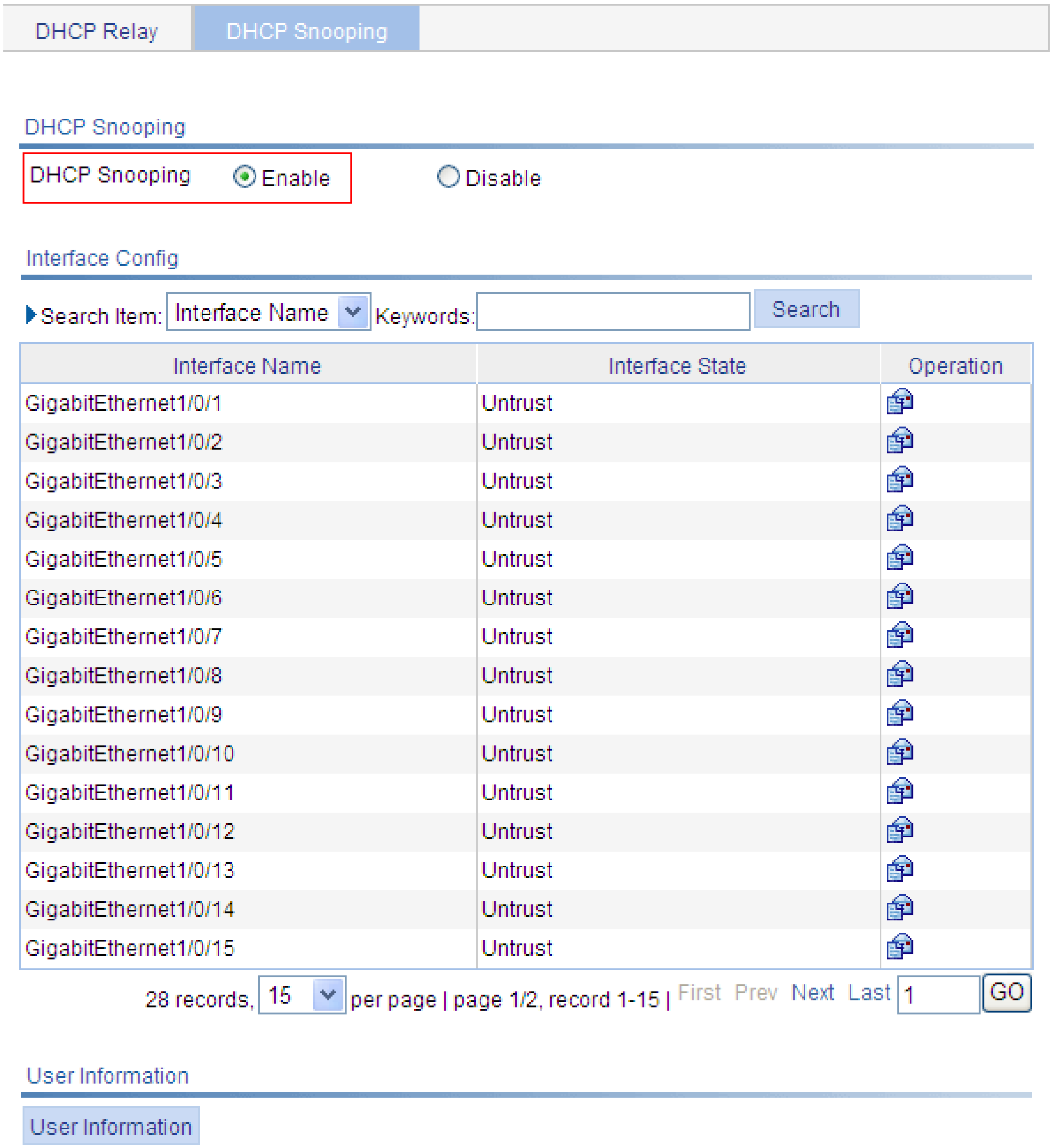


Configuration procedure

# Enable DHCP snooping.

- Select **Network** > **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab. Perform the following operation, as shown in Figure 3-7.

Figure 3-7 Enable DHCP snooping



DHCP Snooping

DHCP Snooping ● Enable ○ Disable

Interface Config

Search Item: Interface Name Keywords: [ ] Search

Interface Name	Interface State	Operation
GigabitEthernet1/0/1	Untrust	✎
GigabitEthernet1/0/2	Untrust	✎
GigabitEthernet1/0/3	Untrust	✎
GigabitEthernet1/0/4	Untrust	✎
GigabitEthernet1/0/5	Untrust	✎
GigabitEthernet1/0/6	Untrust	✎
GigabitEthernet1/0/7	Untrust	✎
GigabitEthernet1/0/8	Untrust	✎
GigabitEthernet1/0/9	Untrust	✎
GigabitEthernet1/0/10	Untrust	✎
GigabitEthernet1/0/11	Untrust	✎
GigabitEthernet1/0/12	Untrust	✎
GigabitEthernet1/0/13	Untrust	✎
GigabitEthernet1/0/14	Untrust	✎
GigabitEthernet1/0/15	Untrust	✎

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

User Information

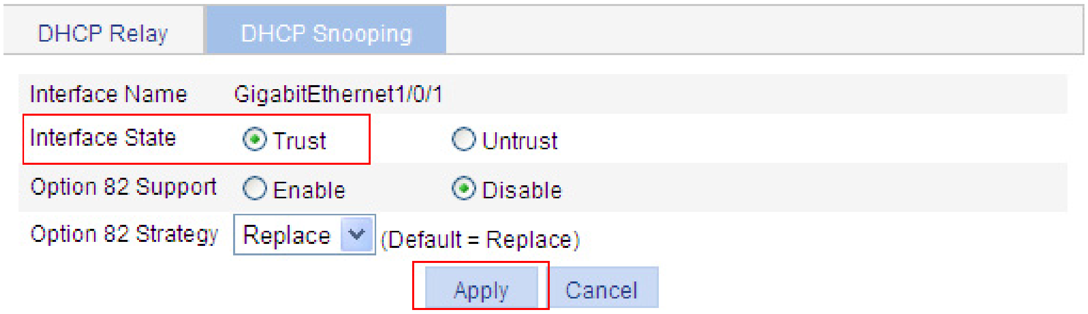
User Information

- Click on the **Enable** radio button next to **DHCP Snooping**.

# Configure DHCP snooping functions on GigabitEthernet 1/0/1.

- Click the ✎ icon of GigabitEthernet 1/0/1 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in Figure 3-8.

Figure 3-8 Configure DHCP snooping functions on GigabitEthernet 1/0/1



Interface Name GigabitEthernet1/0/1

Interface State ● Trust ○ Untrust

Option 82 Support ○ Enable ● Disable

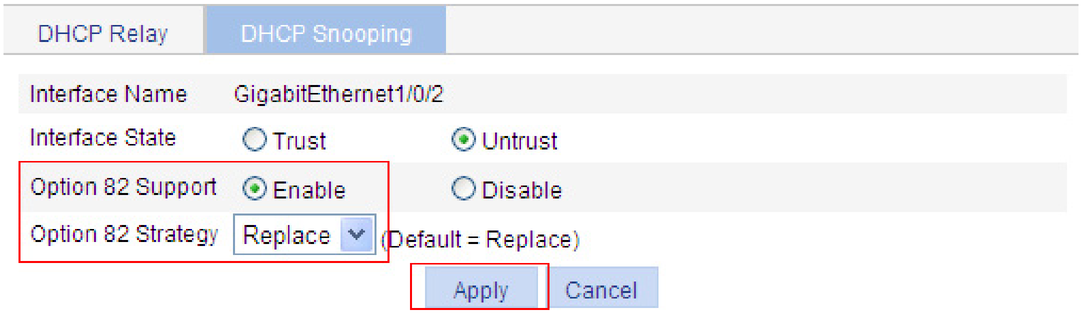
Option 82 Strategy Replace (Default = Replace)

- Click on the **Trust** radio button next to **Interface State**.
- Click **Apply**.

# Configure DHCP snooping functions on GigabitEthernet 1/0/2.

- Click the 📝 icon of GigabitEthernet 1/0/2 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in Figure 3-9.

Figure 3-9 Configure DHCP snooping functions on GigabitEthernet 1/0/2



Interface Name GigabitEthernet1/0/2

Interface State ○ Trust ● Untrust

Option 82 Support ● Enable ○ Disable

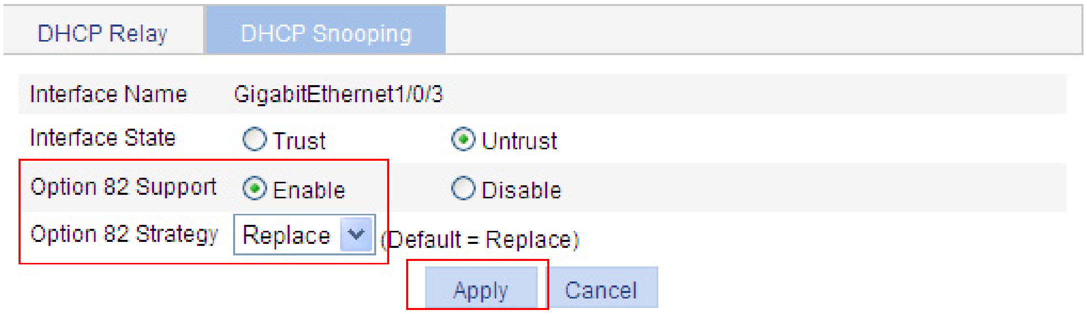
Option 82 Strategy Replace (Default = Replace)

- Click on the **Untrust** radio button for **Interface State**.
- Click on the **Enable** radio button next to **Option 82 Support**.
- Select **Replace** for **Option 82 Strategy**.
- Click **Apply**.

# Configure DHCP snooping functions on GigabitEthernet 1/0/3.

- Click the 📝 icon of GigabitEthernet 1/0/3 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in Figure 3-10.

Figure 3-10 Configure DHCP snooping functions on GigabitEthernet 1/0/3



Interface Name GigabitEthernet1/0/3

Interface State ○ Trust ● Untrust

Option 82 Support ● Enable ○ Disable

Option 82 Strategy Replace (Default = Replace)

- Click on the **Untrust** radio button for **Interface State**.
- Click on the **Enable** radio button next to **Option 82 Support**.
- Select **Replace** for **Option 82 Strategy**.
- Click **Apply**.

Table of Contents

1 Service Management

Overview

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

The service management module also provides the function to modify HTTP and HTTPS port numbers, and the function to associate the FTP, HTTP, or HTTPS service with an ACL, thus reducing attacks of illegal users on these services.

FTP service

The File Transfer Protocol (FTP) is an application layer protocol for sharing files between server and client over a TCP/IP network.

Telnet service

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

SSH service

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

SFTP service

The secure file transfer protocol (SFTP) is a new feature in SSH2.0. SFTP uses the SSH connection to provide secure data transfer. The device can serve as the SFTP server, allowing a remote user to log in to the SFTP server for secure file management and transfer. The device can also serve as an SFTP client, enabling a user to login from the device to a remote device for secure file transfer.

HTTP service

The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite.

You can log in to the device using the HTTP protocol with HTTP service enabled, accessing and controlling the device with Web-based network management.

HTTPS service

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol.

The SSL protocol of HTTPS enhances the security of the device in the following ways:

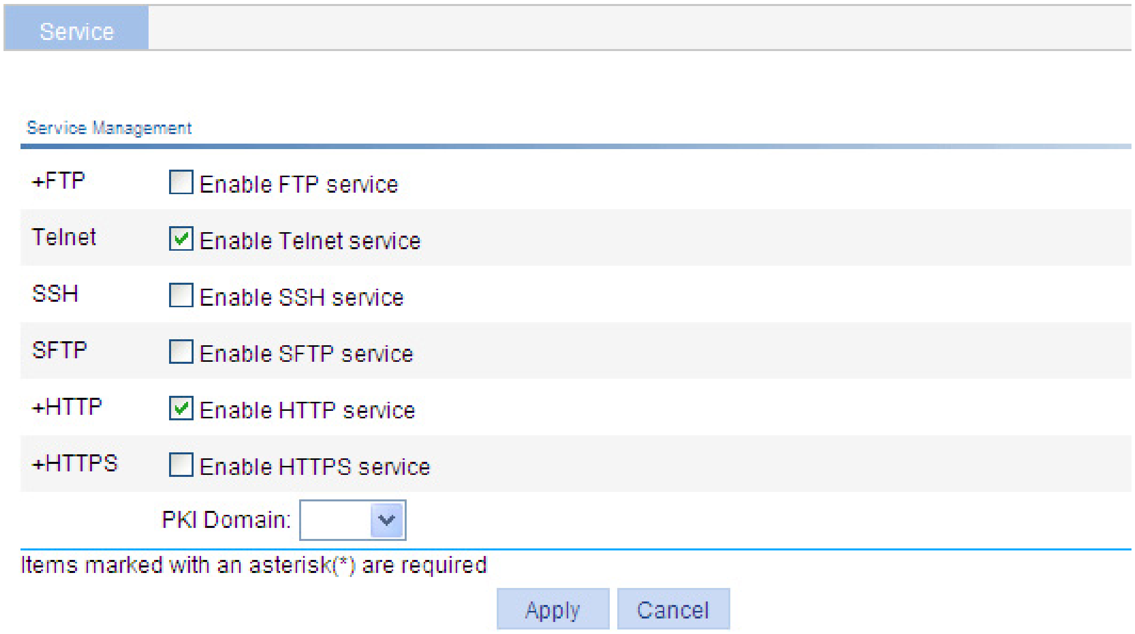
- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;

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

Configuring Service Management

Select **Network** > **Service** from the navigation tree to enter the service management configuration page, as shown in Figure 1-1.

Figure 1-1 Service management



Service

Service Management

+FTP ☐ Enable FTP service

Telnet ☑ Enable Telnet service

SSH ☐ Enable SSH service

SFTP ☐ Enable SFTP service

+HTTP ☑ Enable HTTP service

+HTTPS ☐ Enable HTTPS service

PKI Domain:

Items marked with an asterisk(*) are required

Table 1-1 shows the detailed configuration for service management.

Table 1-1 Service management configuration items

Item		Description
FTP	Enable FTP service	Specifies whether to enable the FTP service. The FTP service is disabled by default.
	ACL	Associates the FTP service with an ACL. Only the clients that pass the ACL filtering are permitted to use the FTP service. You can view this configuration item by clicking the expanding button in front of **FTP**.
Telnet	Enable Telnet service	Specifies whether to enable the Telnet service. The Telnet service is disabled by default.
SSH	Enable SSH service	Specifies whether to enable the SSH service. The SSH service is disabled by default.

Item		Description
SFTP	Enable SFTP service	Specifies whether to enable the SFTP service. The SFTP service is disabled by default. **Highlight** *When you enable the SFTP service, the SSH service must be enabled.*
HTTP	Enable HTTP service	Specifies whether to enable the HTTP service. The HTTP service is enabled by default.
	Port Number	Sets the port number for HTTP service. You can view this configuration item by clicking the expanding button in front of **HTTP**. **Highlight** *When you modify a port, ensure that the port is not used by other service.*
	ACL	Associates the HTTP service with an ACL. Only the clients that pass the ACL filtering are permitted to use the HTTP service. You can view this configuration item by clicking the expanding button in front of **HTTP**.
HTTPS	Enable HTTPS service	Specifies whether to enable the HTTPS service. The HTTPS service is disabled by default.
	Port Number	Sets the port number for HTTPS service. You can view this configuration item by clicking the expanding button in front of **HTTPS**. **Highlight** *When you modify a port, ensure that the port is not used by other service.*
	ACL	Associates the HTTPS service with an ACL. Only the clients that pass the ACL filtering are permitted to use the HTTPS service. You can view this configuration item by clicking the expanding button in front of **HTTPS**.
	PKI Domain	Sets the PKI domain for the HTTPS service. You can configure the available PKI domains by selecting **Authentication** > **PKI** from the navigation tree at the left side of the interface. For more information, refer to *PKI Configuration* of this manual.

Table of Contents

1 Diagnostic Tools

Overview

Ping

You can use the ping function to check whether a device with a specified address is reachable, and to examine network connectivity.

A successful execution of the **ping** command involves the following steps:

1) The source device sends an ICMP echo request (ECHO-REQUEST) to the destination device.
2) The destination device responds by sending an ICMP echo reply (ECHO-REPLY) to the source device after receiving the ICMP echo request.
3) The source device displays related statistics after receiving the reply.

Output of the **ping** command falls into the following:

- If the source device does not receive an ICMP echo reply within the timeout time, it displays the prompt information and the statistics during the ping operation.
- If the source device receives an ICMP echo reply within the timeout time, it displays the number of bytes of the echo reply, the message sequence number, Time to Live (TTL), the response time, and the statistics during the ping operation. Statistics during the ping operation include number of packets sent, number of echo reply messages received, percentage of messages not received, and the minimum, average, and maximum response time.

Trace Route

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

The **trace route** command involves the following steps in its execution:

1) The source device sends a packet with a TTL value of 1 to the destination device.
2) The first hop (the Layer 3 device that first receives the packet) responds by sending a TTL-expired ICMP message to the source, with its IP address encapsulated. In this way, the source device can get the address of the first Layer 3 device.
3) The source device sends a packet with a TTL value of 2 to the destination device.
4) The second hop responds with a TTL-expired ICMP message, which gives the source device the address of the second Layer 3 device.
5) The above process continues until the ultimate destination device is reached. In this way, the source device can trace the addresses of all the Layer 3 devices involved to get to the destination device.

Diagnostic Tool Operations

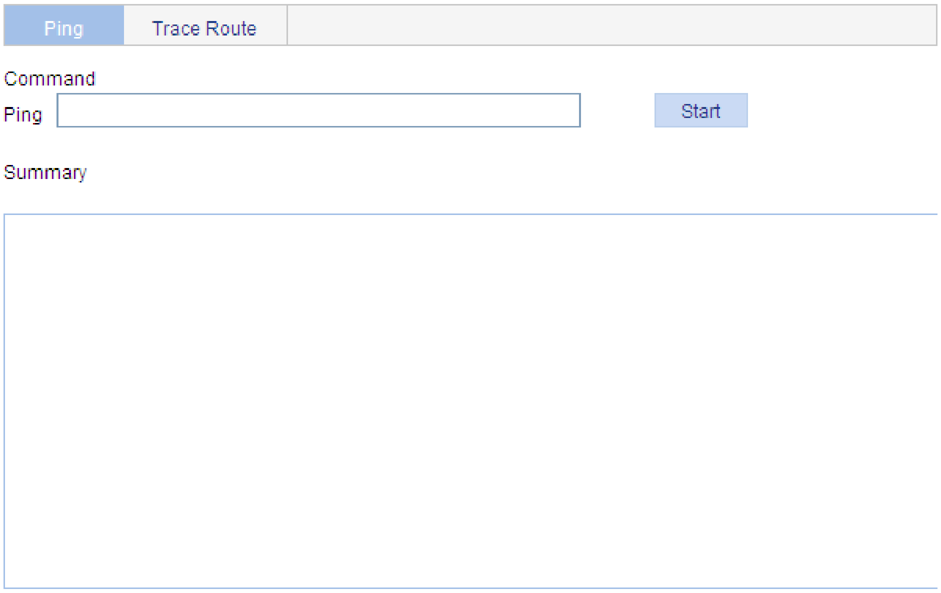
Ping Operation

Note

The Web interface supports the IPv4 ping operations only.

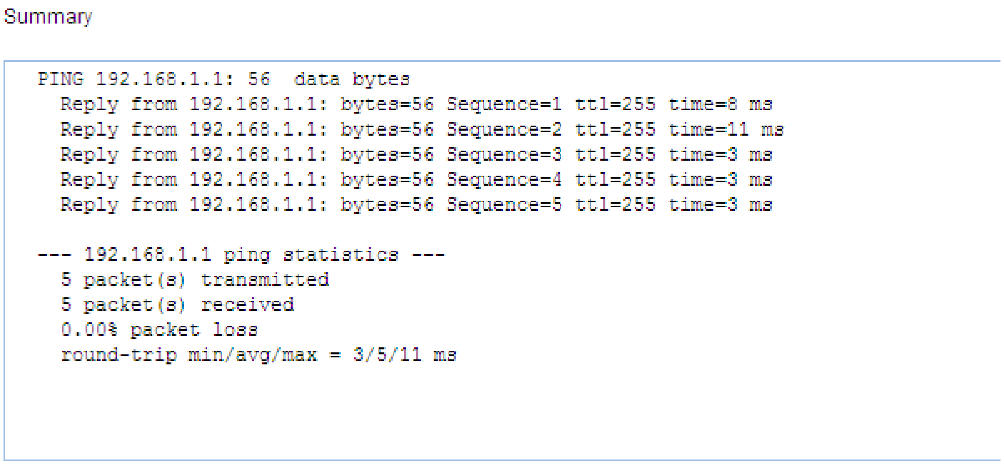
Select **Network** > **Diagnostic Tools** from the navigation tree to enter the ping configuration page, as shown in Figure 1-1.

Figure 1-1 Ping configuration page



Type the IPv4 address of the destination device in the **Ping** text box, and click **Start** to execute the **ping** command. You will see the result in the **Summary** area.

Figure 1-2 Ping operation result



```
PING 192.168.1.1: 56  data bytes
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=8 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=11 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=255 time=3 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/5/11 ms
```

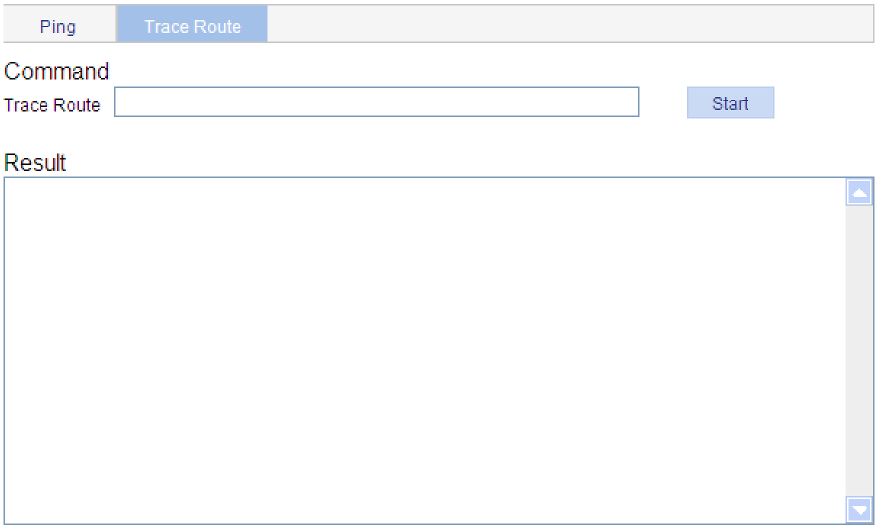
Trace Route Operation

Note

- The Web interface supports trace route on IPv4 addresses only.
- Before performing the trace route operation on the Web interface, on the device execute the commands of **ip ttl-expires enable** and **ip unreachables enable** to enable the sending of ICMP timeout and destination unreachable packets.

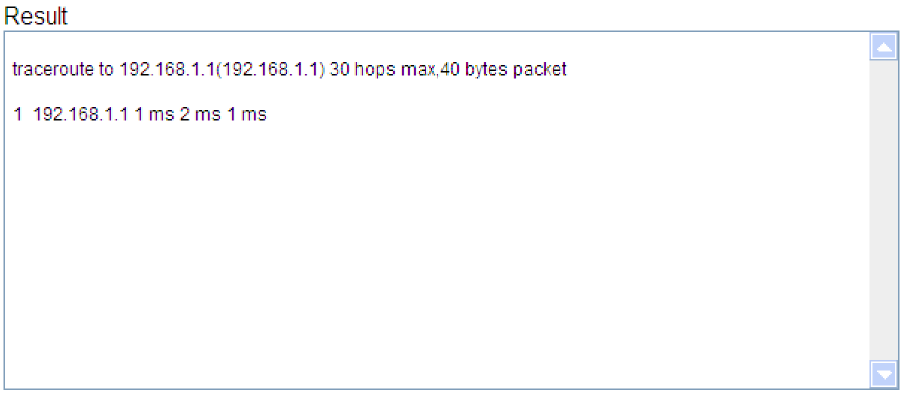
Select **Network** > **Diagnostic Tools** from the navigation tree and then select the **Trace Route** to enter the Trace Route configuration page, as shown in Figure 1-3.

Figure 1-3 Trace Route configuration page



Type the destination IP address in the **Trace Route** text box, and click **Start** to execute the **trace route** command. You will see the result in the **Result** area, as shown in Figure 1-4.

Figure 1-4 Trace route operation result



```
traceroute to 192.168.1.1(192.168.1.1) 30 hops max,40 bytes packet

1  192.168.1.1 1 ms 2 ms 1 ms
```

Table of Contents

1 ARP Management

ARP Overview

ARP Function

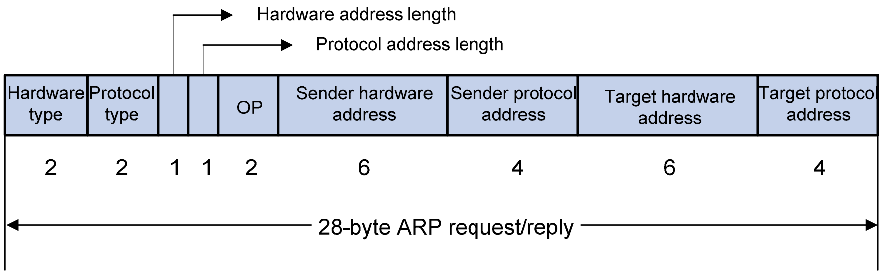
The Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address (or physical address).

In an Ethernet LAN, when a device sends data to another device, it uses ARP to translate the IP address of the destination device to the corresponding MAC address.

ARP Message Format

ARP messages are classified into ARP requests and ARP replies. Figure 1-1 shows the format of the ARP request/reply.

Figure 1-1 ARP message format



Hardware type	Protocol type			OP	Sender hardware address	Sender protocol address	Target hardware address	Target protocol address
2	2	1	1	2	6	4	6	4

The following describe the fields in Figure 1-1.

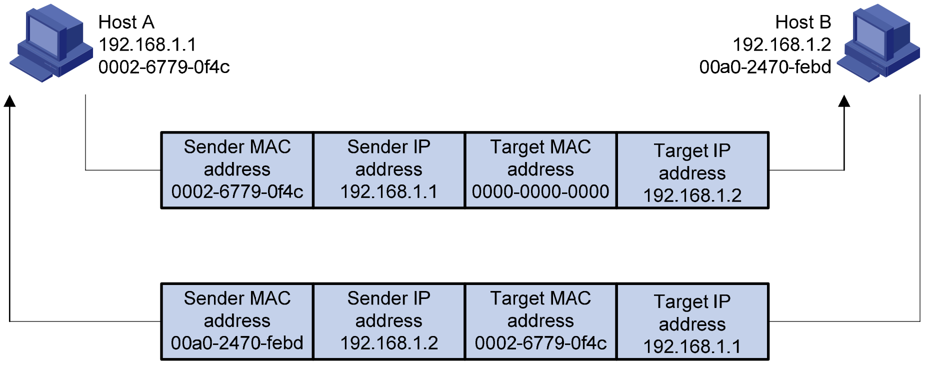
- Hardware type: This field specifies the hardware address type. The value “1” represents Ethernet.
- Protocol type: This field specifies the type of the protocol address to be mapped. The hexadecimal value “0x0800” represents IP.
- Hardware address length and protocol address length: They respectively specify the length of a hardware address and a protocol address, in bytes. For an Ethernet address, the value of the hardware address length field is "6”. For an IP(v4) address, the value of the protocol address length field is “4”.
- OP: Operation code. This field specifies the type of the ARP message. The value “1” represents an ARP request and “2” represents an ARP reply.
- Sender hardware address: This field specifies the hardware address of the device sending the message.
- Sender protocol address: This field specifies the protocol address of the device sending the message.
- Target hardware address: This field specifies the hardware address of the device the message is being sent to.
- Target protocol address: This field specifies the protocol address of the device the message is being sent to.

ARP Operation

Suppose that Host A and Host B are on the same subnet and Host A sends a packet to Host B, as shown in Figure 1-2. The resolution process is as follows:

- Host A looks into its ARP table to see whether there is an ARP entry for Host B. If yes, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
- If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the sender IP address and the sender MAC address are the IP address and the MAC address of Host A respectively, and the target IP address and the target MAC address are the IP address of Host B and an all-zero MAC address respectively. Because the ARP request is a broadcast, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will respond to the request.
- Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address in its ARP table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
- After receiving the ARP reply, Host A adds the MAC address of Host B to its ARP table. Meanwhile, Host A encapsulates the IP packet and sends it out.

Figure 1-2 ARP address resolution process



Sender MAC address	Sender IP address	Target MAC address	Target IP address
0002-6779-0f4c	192.168.1.1	0000-0000-0000	192.168.1.2

Sender MAC address	Sender IP address	Target MAC address	Target IP address
00a0-2470-febd	192.168.1.2	0002-6779-0f4c	192.168.1.1

If Host A is not on the same subnet with Host B, Host A first sends an ARP request to the gateway. The target IP address in the ARP request is the IP address of the gateway. After obtaining the MAC address of the gateway from an ARP reply, Host A sends the packet to the gateway. If the gateway maintains the ARP entry of Host B, it forwards the packet to Host B directly; if not, it broadcasts an ARP request, in which the target IP address is the IP address of Host B. After obtaining the MAC address of Host B, the gateway sends the packet to Host B.

ARP Table

After obtaining the MAC address for the destination host, the device puts the IP-to-MAC mapping into its own ARP table. This mapping is used for forwarding packets with the same destination in future.

An ARP table contains ARP entries, which fall into one of two categories: dynamic or static.

Dynamic ARP entry

A dynamic entry is automatically created and maintained by ARP. It can get aged, be updated by a new ARP packet, or be overwritten by a static ARP entry. When the aging timer expires or the interface goes down, the corresponding dynamic ARP entry will be removed.

Static ARP entry

A static ARP entry is manually configured and maintained. It cannot get aged or be overwritten by a dynamic ARP entry.

Using static ARP entries enhances communication security. After a static ARP entry is specified, only a specific MAC address is associated with the specified IP address. Attack packets cannot modify the IP-to-MAC mapping. Thus, communications between devices are protected.

Static ARP entries can be classified into permanent or non-permanent.

- A permanent static ARP entry can be directly used to forward packets. When configuring a permanent static ARP entry, you must configure a VLAN and an outbound interface for the entry besides the IP address and the MAC address.
- A non-permanent static ARP entry has only an IP address and a MAC address configured. It cannot be directly used for forwarding data. If a non-permanent static ARP entry matches an IP packet to be forwarded, the device sends an ARP request first. If the sender IP and MAC addresses in the received ARP reply are the same as those in the non-permanent static ARP entry, the device adds the interface receiving the ARP reply to the non-permanent static ARP entry. Then the entry can be used for forwarding IP packets.

Note

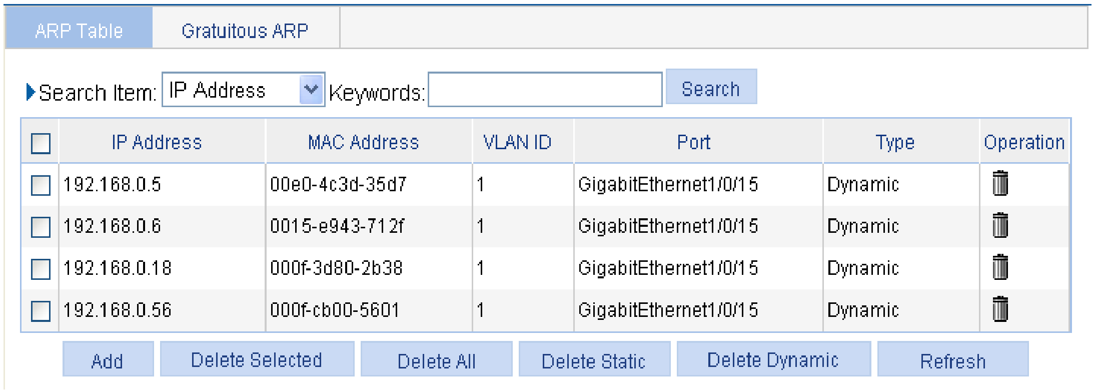
Usually ARP dynamically resolves IP addresses to MAC addresses, without manual intervention.

Managing ARP Entries

Displaying ARP Entries

Select **Network** > **ARP Management** from the navigation tree to enter the default **ARP Table** page shown in Figure 1-3. All ARP entries are displayed on the page.

Figure 1-3 ARP Table configuration page



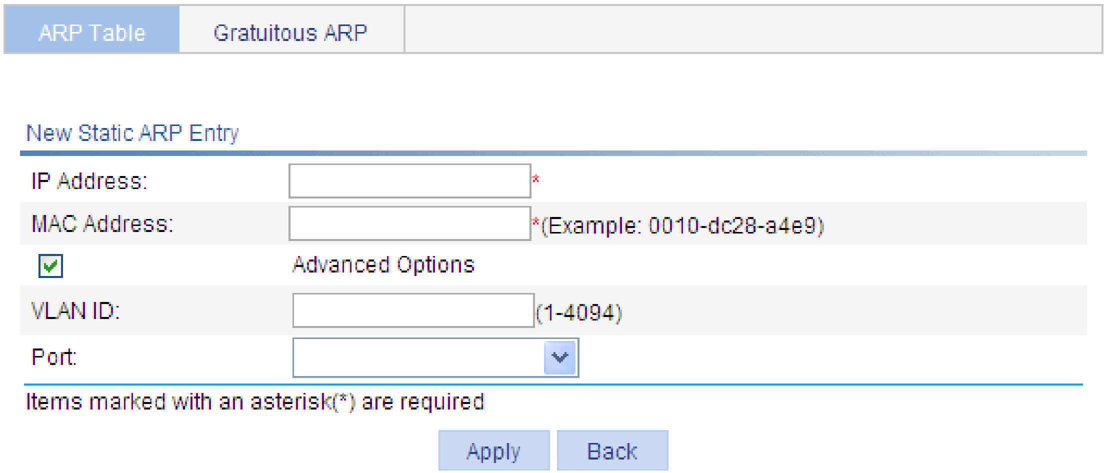
Search Item: IP Address Keywords:

□	IP Address	MAC Address	VLAN ID	Port	Type	Operation
□	192.168.0.5	00e0-4c3d-35d7	1	GigabitEthernet1/0/15	Dynamic	🗑
□	192.168.0.6	0015-e943-712f	1	GigabitEthernet1/0/15	Dynamic	🗑
□	192.168.0.18	000f-3d80-2b38	1	GigabitEthernet1/0/15	Dynamic	🗑
□	192.168.0.56	000f-cb00-5601	1	GigabitEthernet1/0/15	Dynamic	🗑

Creating a Static ARP Entry

Select **Network** > **ARP Management** from the navigation tree to enter the default **ARP Table** page shown in Figure 1-3. Click **Add** to enter the **New Static ARP Entry** page. Select the **Advanced Options** checkbox to expand advanced configuration items, as shown in Figure 1-4.

Figure 1-4 Add a static ARP entry



New Static ARP Entry

IP Address:	*
MAC Address:	*(Example: 0010-dc28-a4e9)
☑	Advanced Options
VLAN ID:	(1-4094)
Port:	

Items marked with an asterisk(*) are required

Table 1-1 describes the static ARP entry configuration items.

Table 1-1 Static ARP entry configuration items

Item		Description
IP Address		Type an IP address for the static ARP entry.
MAC Address		Type a MAC address for the static ARP entry.
Advanced Options	VLAN ID	Type a VLAN ID and specify a port for the static ARP entry. **Highlight** *The VLAN ID must be the ID of the VLAN that has already been created, and the port must belong to the VLAN. The corresponding VLAN interface must have been created.*
	Port	

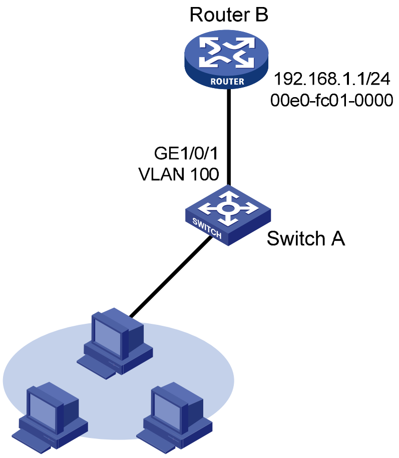
Static ARP Configuration Example

Network Requirements

As shown in Figure 1-5, hosts are connected to Switch A, which is connected to Router B through interface GigabitEthernet 1/0/1 belonging to VLAN 100. The IP address of Router B is 192.168.1.1/24. The MAC address of Router B is 00e0-fc01-0000.

To enhance communication security between Switch A and Router B, static ARP entries need to be configured on Switch A.

Figure 1-5 Network diagram for configuring static ARP entries

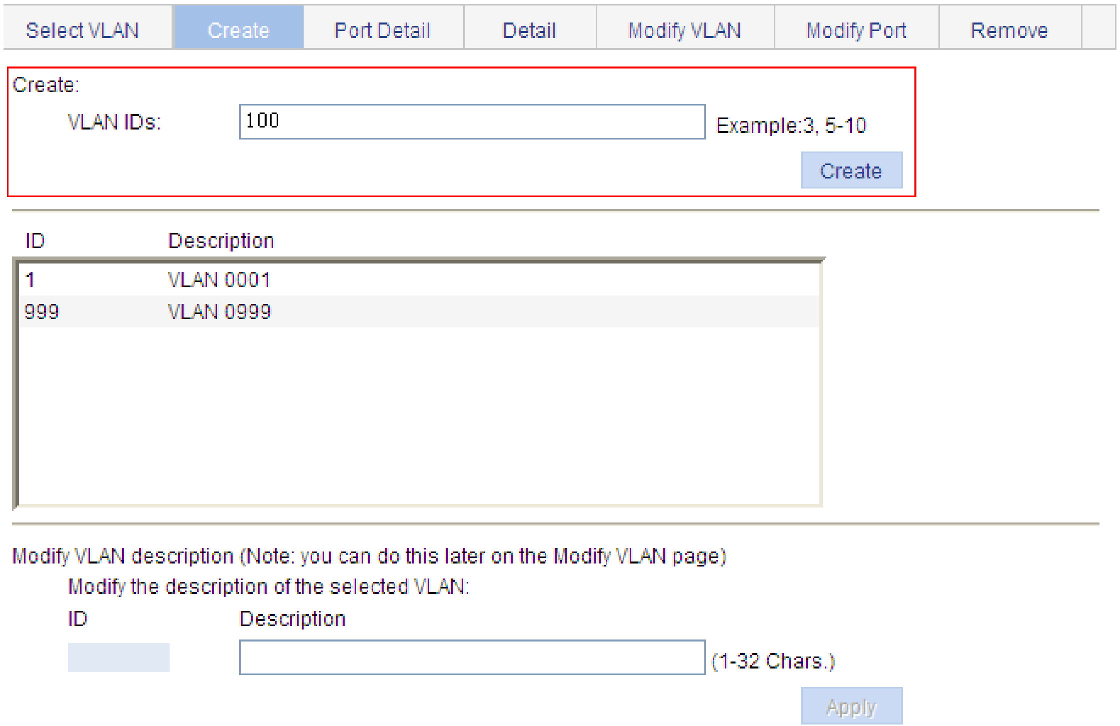


Configuration procedure

# Create VLAN 100.

- Select **Network** > **VLAN** from the navigation tree, click the **Add** tab, and then perform the following operations, as shown in Figure 1-6.

Figure 1-6 Create VLAN 100



Create:

VLAN IDs: 100 Example:3, 5-10

ID	Description
1	VLAN 0001
999	VLAN 0999

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID Description

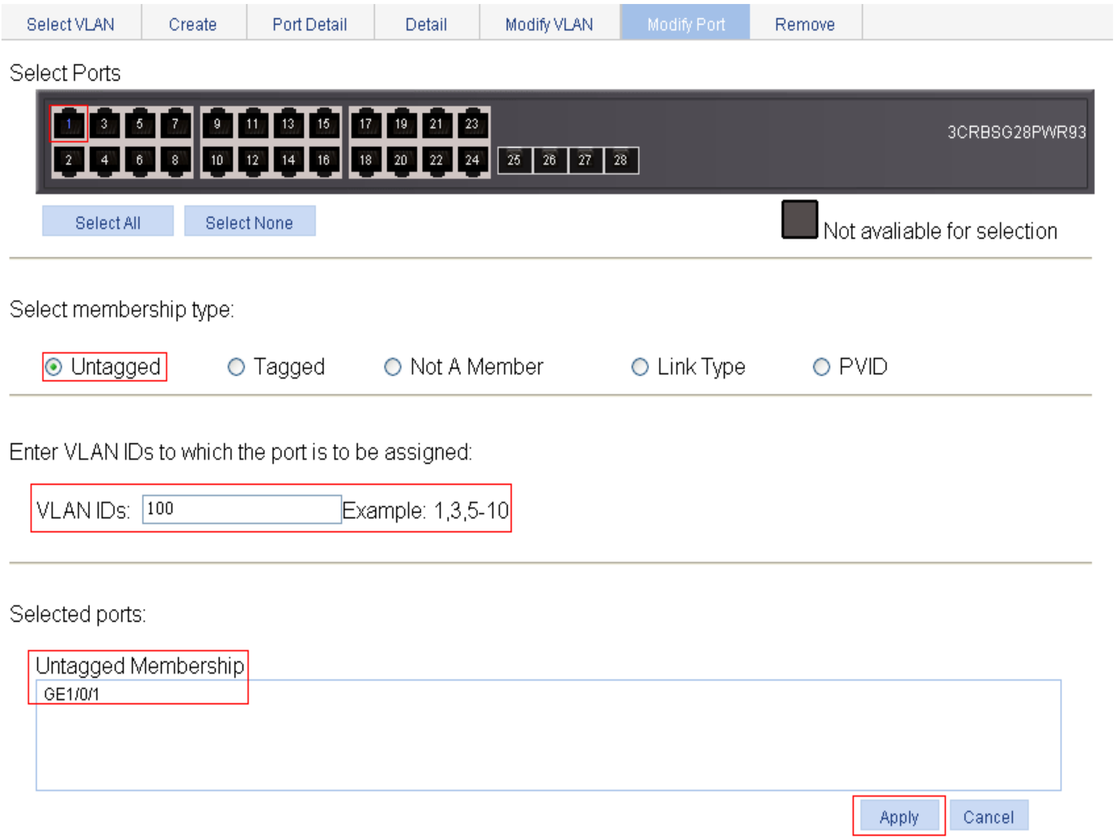
(1-32 Chars.)

- Type **100** for **VLAN ID**.
- Click **Create** to complete the configuration.

# Add GigabitEthernet 1/0/1 to VLAN 100.

- Click the **Modify Port** tab and then perform the following operations, as shown in Figure 1-7.

Figure 1-7 Add GigabitEthernet 1/0/1 to VLAN 100



Select Ports

Select membership type:

● Untagged ○ Tagged ○ Not A Member ○ Link Type ○ PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: 100 Example: 1,3,5-10

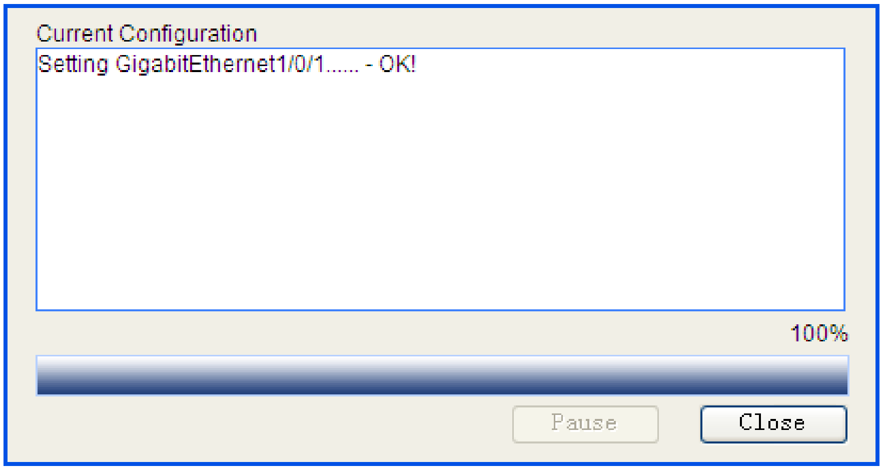
Selected ports:

Untagged Membership

GE1/0/1

- Select interface GigabitEthernet 1/0/1 in the **Select Ports** field.
- Click on the **Untagged** radio button in the **Select membership type** field.
- Type **100** for **VLAN IDs**.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-8.

Figure 1-8 Configuration progress dialog box



Current Configuration

Setting GigabitEthernet1/0/1...... - OK!

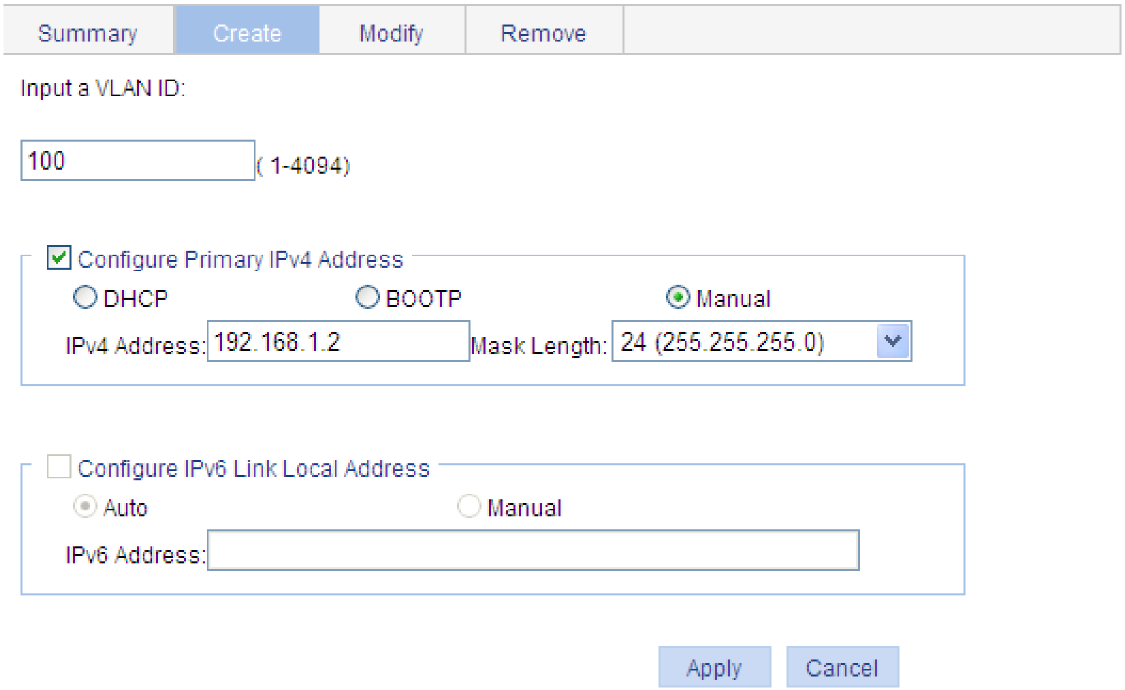
100%

- After the configuration process is complete, click **Close**.

# Create VLAN-interface 100.

- Select **Network** > **VLAN Interface** from the navigation tree, click the **Create** tab, and then perform the following operations, as shown in Figure 1-9.

Figure 1-9 Create VLAN-interface 100



Input a VLAN ID:

100 (1-4094)

☑ Configure Primary IPv4 Address

○ DHCP ○ BOOTP ● Manual

IPv4 Address: 192.168.1.2 Mask Length: 24 (255.255.255.0)

□ Configure IPv6 Link Local Address

● Auto ○ Manual

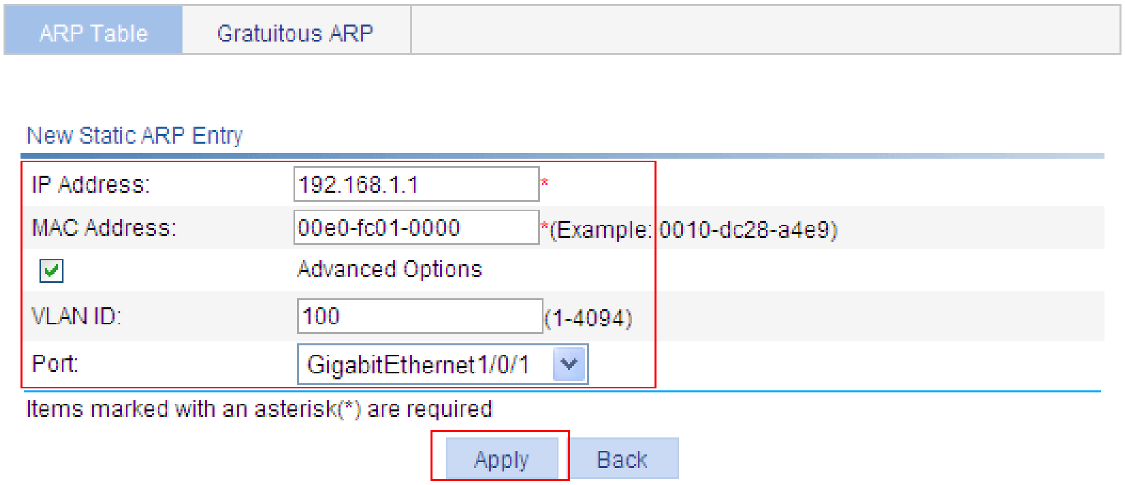
IPv6 Address:

- Type **100** for **VLAN ID**.
- Select the **Configure Primary IPv4 Address** checkbox.
- Click on the **Manual** radio botton.
- Type **192.168.1.2** for **IPv4 Address**.
- Select **24 (255.255.255.0)** for **Mask Length**.
- Click **Apply** to complete the configuration.

# Create a static ARP entry.

- Select **Network** > **ARP Management** from the navigation tree to enter the default **ARP Table** page. Click **Add** Perform the following operations, as shown in Figure 1-10.

Figure 1-10 Create a static ARP entry



New Static ARP Entry

IP Address:	192.168.1.1 *
MAC Address:	00e0-fc01-0000 *(Example: 0010-dc28-a4e9)
☑	Advanced Options
VLAN ID:	100 (1-4094)
Port:	GigabitEthernet1/0/1

Items marked with an asterisk(*) are required

- Type **192.168.1.1** for **IP Address**.
- Type **00e0-fc01-0000** for **MAC Address**.

- Select the **Advanced Options** checkbox.
- Type **100** for **VLAN ID**.
- Select **GigabitEthernet1/0/1** for **Port**.
- Click **Apply** to complete the configuration.

Gratuitous ARP

Introduction to Gratuitous ARP

In a gratuitous ARP packet, the sender IP address and the target IP address are both the IP address of the device issuing the packet, the sender MAC address is the MAC address of the device, and the target MAC address is the broadcast address ff:ff:ff:ff:ff:ff.

A device implements the following functions by sending gratuitous ARP packets:

- Determining whether its IP address is already used by another device.
- Informing other devices about the change of its MAC address so that they can update their ARP entries.

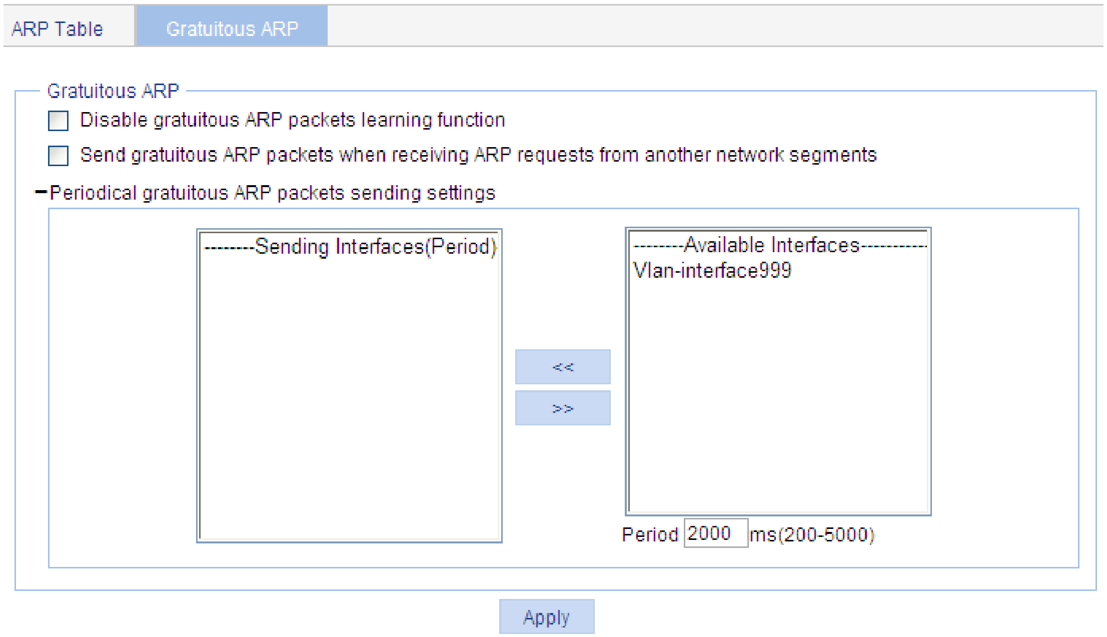
A device receiving a gratuitous ARP packet adds the information carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry exists in the cache.

An attacker sends spoofed gratuitous ARP packets to hosts on a network. As a result, traffic that the hosts want to send to the gateway is sent to the attacker instead, and the hosts cannot access external networks. To prevent such gateway spoofing attacks, you can enable the gateway to send gratuitous ARP packets periodically. In this way, each host can learn correct gateway address information.

Configuring Gratuitous ARP

Select **Network** > **ARP Management** from the navigation tree, and click the **Gratuitous ARP** tab to enter the page shown in Figure 1-11.

Figure 1-11 Gratuitous ARP configuration page



Gratuitous ARP

□ Disable gratuitous ARP packets learning function

□ Send gratuitous ARP packets when receiving ARP requests from another network segments

−Periodical gratuitous ARP packets sending settings

--------Sending Interfaces(Period)

--------Available Interfaces----------
Vlan-interface999

Period 2000 ms(200-5000)

Table 1-2 describes the gratuitous ARP configuration items.

Table 1-2 Gratuitous ARP configuration items

Item	Description
Disable gratuitous ARP packets learning function	Enable or disable learning of ARP entries according to gratuitous ARP packets. Enabled by default.
Send gratuitous ARP packets when receiving ARP requests from another network segment	Enable the device to send gratuitous ARP packets upon receiving ARP requests from another network segment. Disabled by default.
Periodical gratuitous ARP packets sending settings	Select interfaces for sending gratuitous ARP packets and type the sending period. To add an interface to the **Sending Interfaces(Period)** list box, select the interface from the **Available Interfaces** list box, type the sending period, and click the **<<** button. To remove an interface from the **Sending Interfaces(Period)** list box, select the interface from the list box and click the **>>** button. **Highlight** • *This function takes effect only when the link of the interface goes up and an IP address has been assigned to the interface.* • *If you change the period for sending ARP packets, the configuration is effective at the next sending period.*

2 ARP Attack Defense Configuration

Although ARP is easy to implement, it provides no security mechanism and thus is prone to network attacks. Currently, ARP attacks and viruses are threatening LAN security. The device can provide multiple features to detect and prevent such attacks. This chapter mainly introduces these features.

ARP Detection

Introduction to ARP Detection

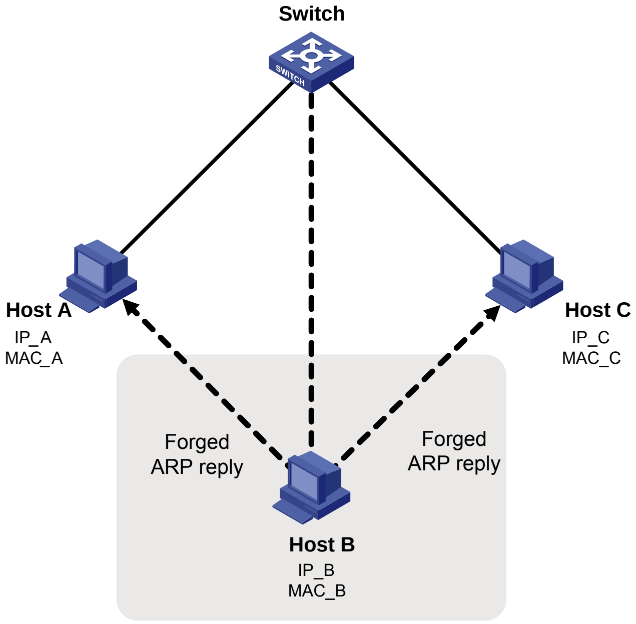
The ARP detection feature allows only the ARP packets of authorized clients to be forwarded, hence preventing man-in-the-middle attacks.

Man-in-the-middle attack

According to the ARP design, after receiving an ARP reply, a host adds the IP-to-MAC mapping of the sender to its ARP mapping table. This design reduces the ARP traffic on the network, but also makes ARP spoofing possible.

As shown in Figure 2-1, Host A communicates with Host C through a switch. After intercepting the traffic between Host A and Host C, a hacker (Host B) forwards forged ARP replies to Host A and Host C respectively. Upon receiving the ARP replies, the two hosts update the MAC address corresponding to the peer IP address in their ARP tables with the MAC address of Host B (MAC_B). After that, Host B establishes independent connections with Host A and Host C and relays messages between them, deceiving them into believing that they are talking directly to each other over a private connection, while the entire conversation is actually controlled by Host B. Host B may intercept and modify the communication data. Such an attack is called a man-in-the-middle attack.

Figure 2-1 Man-in-the-middle attack



ARP detection mechanism

With ARP detection enabled for a specific VLAN, ARP messages arrived on any interface in the VLAN are redirected to the CPU to have their MAC and IP addresses checked. ARP messages that pass the check are forwarded, and other ARP messages are discarded.

1) ARP detection based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings

With this feature enabled, the device compares the source IP and MAC addresses of an ARP packet received from the VLAN against the DHCP snooping entries, 802.1X security entries, or static IP-to-MAC binding entries. You can specify a detection type or types as needed.

After you enable ARP detection based on DHCP snooping entries for a VLAN,

- Upon receiving an ARP packet from an ARP untrusted port, the device compares the ARP packet against the DHCP snooping entries. If a match is found, that is, the parameters (such as IP address, MAC addresses, port index, and VLAN ID) are consistent, the ARP packet passes the check; if not, the ARP packet cannot pass the check.
- Upon receiving an ARP packet from an ARP trusted port, the device does not check the ARP packet.
- If ARP detection is not enabled for the VLAN, the ARP packet is not checked even if it is received from an ARP untrusted port.

After you enable ARP detection based on 802.1X security entries, the device, upon receiving an ARP packet from an ARP untrusted port, compares the ARP packet against the 802.1X security entries.

- If an entry with identical source IP and MAC addresses, port index, and VLAN ID is found, the ARP packet is considered valid.
- If an entry with no matching IP address but with a matching OUI MAC address is found, the ARP packet is considered valid.

Otherwise, the packet is considered invalid and discarded.

After you enable ARP detection based on static IP-to-MAC bindings, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings.

- If an entry with a matching IP address but a different MAC address is found, the ARP packet is considered invalid and discarded.
- If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.
- If no match is found, the ARP packet is considered valid and can pass the detection.

If all the detection types are specified, the system uses static IP-to-MAC binding entries first, then DHCP snooping entries, and then 802.1X security entries. To prevent gateway spoofing, ARP detection based on IP-to-MAC binding entries is required. After passing this type of ARP detection, users that can pass ARP detection based on DHCP snooping entries or 802.1X security entries are considered to be valid. The last two detection types are used to prevent user spoofing. You can select detection types according to the networking environment.

- If all access clients acquire IP addresses through DHCP, it is recommended that you enable DHCP snooping and ARP detection based on DHCP snooping entries on your access device.
- If access clients are 802.1X clients and large in number, and most of them use static IP addresses, it is recommended that you enable 802.1X authentication, upload of client IP addresses, and ARP detection based on 802.1X security entries on your access device. After that, the access device uses mappings between IP addresses, MAC addresses, VLAN IDs, and ports of 802.1X authentication clients for ARP detection.

If all the detection types are specified, the system uses IP-to-MAC bindings first, then DHCP snooping entries, and then 802.1X security entries. If an ARP packet fails to pass ARP detection based on static IP-to-MAC bindings, it is discarded. If the packet passes this detection, it will be checked against DHCP snooping entries. If a match is found, the packet is considered to be valid and will not be checked against 802.1X security entries; otherwise, the packet is checked against 802.1X security entries. If a match is found, the packet is considered to be valid; otherwise, the packet is discarded.

2) ARP detection based on specified objects

You can also specify objects in ARP packets to be detected. The objects involve:

- src-mac: Checks whether the sender MAC address of an ARP packet is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded; otherwise, the packet is discarded.
- dst-mac: Checks the target MAC address of ARP replies. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.
- ip: Checks both the source and destination IP addresses in an ARP packet. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this object specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests are checked.

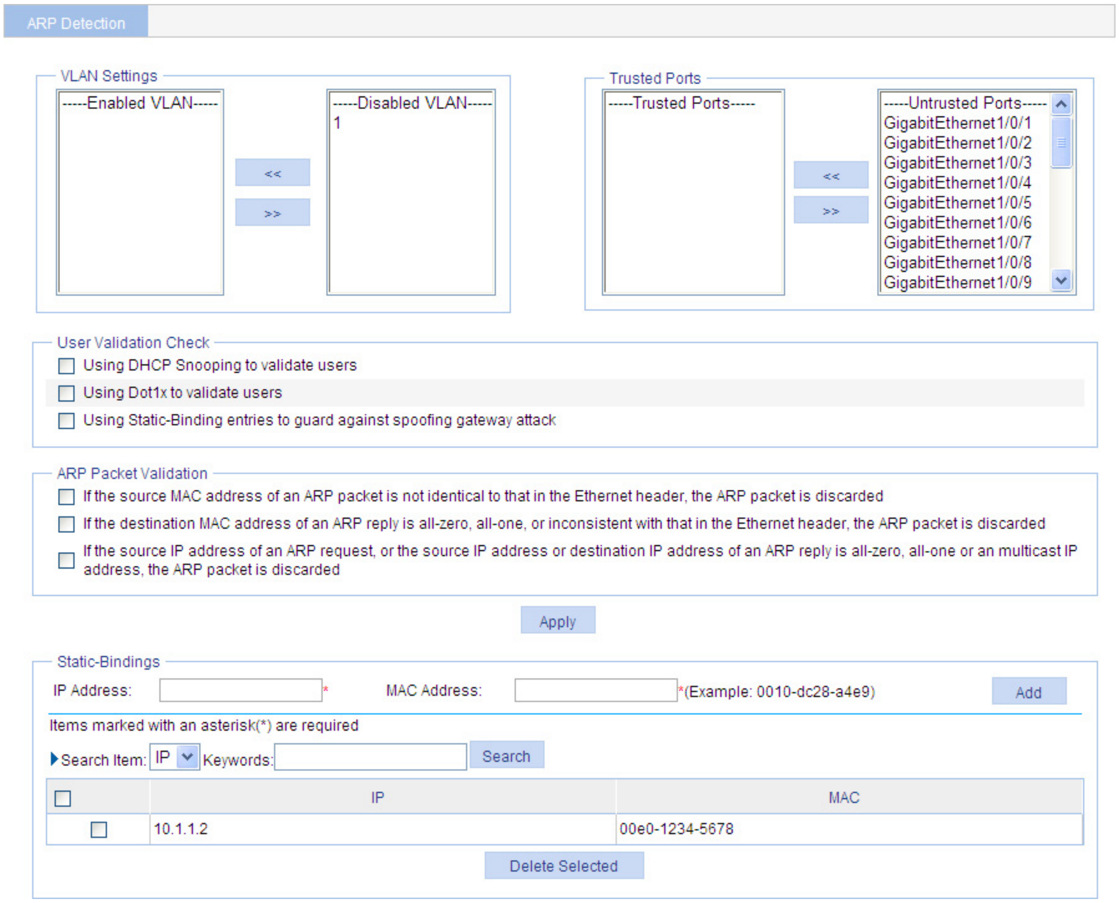
Configuring ARP Detection

Note

If both the ARP detection based on specified objects and the ARP detection based on static IP-to-MAC bindings/DHCP snooping entries/802.1X security entries are enabled, the former one applies first, and then the latter applies.

Select **Network** > **ARP Anti-Attack** from the navigation tree to enter the default **ARP Detection** page shown in Figure 2-2.

Figure 2-2 ARP Detection configuration page



User Validation Check

- □ Using DHCP Snooping to validate users
- □ Using Dot1x to validate users
- □ Using Static-Binding entries to guard against spoofing gateway attack

ARP Packet Validation

- □ If the source MAC address of an ARP packet is not identical to that in the Ethernet header, the ARP packet is discarded
- □ If the destination MAC address of an ARP reply is all-zero, all-one, or inconsistent with that in the Ethernet header, the ARP packet is discarded
- □ If the source IP address of an ARP request, or the source IP address or destination IP address of an ARP reply is all-zero, all-one or an multicast IP address, the ARP packet is discarded

IP Address: * MAC Address: *(Example: 0010-dc28-a4e9)

Items marked with an asterisk(*) are required

Search Item: IP Keywords:

□	IP	MAC
□	10.1.1.2	00e0-1234-5678

Table 2-1 describes the ARP Detection configuration items.

Table 2-1 ARP Detection configuration items

Item	Description
VLAN Settings	Select VLANs on which ARP detection is to be enabled. To add VLANs to the **Enabled VLAN** list box, select one or multiple VLANs from the **Disabled VLAN** list box and click the **<<** button. To remove VLANs from the **Enabled VLAN** list box, select one or multiple VLANs from the list box and click the **>>** button.

Item	Description
Trusted Ports	Select trusted ports. To add ports to the **Trusted Ports** list box, select one or multiple ports from the **Untrusted Ports** list box and click the **<<** button. To remove ports from the **Trusted Ports** list box, select one or multiple ports from the list box and click the **>>** button.
User Validation Check	Select user validity check modes, including: • Using DHCP Snooping to validate users • Using Dot1x to validate users • Using Static-Binding entries to guard against spoofing gateway attack: You can configure static IP-to-MAC bindings if you select this mode. For the detailed configuration, refer to Creating a Static Binding Entry. If all the detection types are specified, the system uses static IP-to-MAC bindings first, then DHCP snooping entries, and then 802.1X security entries. If an ARP packet fails to pass ARP detection based on static IP-to-MAC bindings, it is discarded. If the packet passes this detection, it will be checked against DHCP snooping entries. If a match is found, the packet is considered to be valid and will not be checked against 802.1X security entries; otherwise, the packet is checked against 802.1X security entries. If a match is found, the packet is considered to be valid; otherwise, the packet is discarded. If none of the above is selected, all ARP packets are considered to be invalid. **Highlight** • *Before enabling ARP detection based on DHCP snooping entries, make sure that DHCP snooping is enabled.* • *Before enabling ARP detection based on 802.1X security entries, make sure that 802.1X is enabled and the 802.1X clients are configured to upload IP addresses.*
ARP Packet Validation	Select ARP packet validity check modes, including: • If the source MAC address of an ARP packet is not identical to that in the Ethernet header, the ARP packet is discarded • If the destination MAC address of an ARP reply is all-zero, all-one, or inconsistent with that in the Ethernet header, the ARP packet is discarded • If the source IP address of an ARP request, or the source IP address or destination IP address of an ARP reply is all-zero, all-one or an multicast IP address, the ARP packet is discarded If none of the above is selected, the system does not check the validity of ARP packets.

Creating a Static Binding Entry

If you select **Using Static-Binding entries to anti fake gateway attack**, you can configure static IP-to-MAC binding entries.

To create a static binding entry, type an IP address and MAC address in the **Static Bindings** field, and then click **Add**, as shown in Figure 2-2.

Note

If an entry with a matching IP address but a different MAC address is found, the ARP packet is considered invalid and discarded. If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.

Table of Contents

1 802.1X

Overview

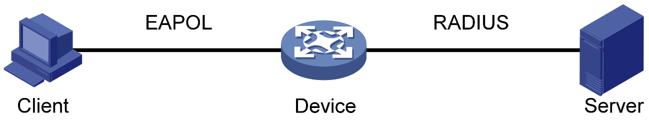
The 802.1X protocol was proposed by the IEEE 802 LAN/WAN committee for security of wireless LANs (WLAN).It has been widely used on Ethernet as a common port access control mechanism.

As a port-based access control protocol, 802.1X authenticates and controls accessing devices at the port level. A device connected to an 802.1X-enabled port of an access control device can access the resources on the LAN only after passing authentication.

Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: Client, Device, and Server, as shown in Figure 1-1.

Figure 1-1 Architecture of 802.1X



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

Authentication Modes of 802.1X

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

- Between the client and the device, EAP protocol packets are encapsulated using EAPOL to be transferred on the LAN.

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

Basic Concepts of 802.1X

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

Controlled port and uncontrolled port

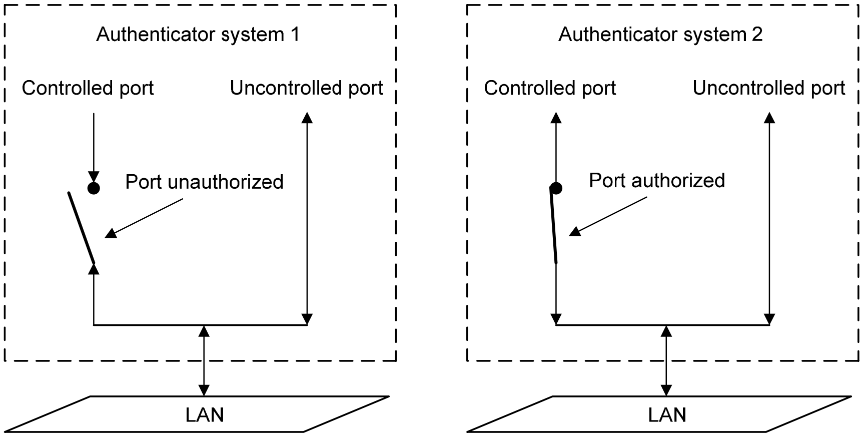
A device provides ports for clients to access the LAN. Each port can be regarded as a unity of two logical ports: a controlled port and an uncontrolled port. Any packets arriving at the port are visible to both of the logical ports.

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

Authorized state and unauthorized state

A controlled port can be in either authorized state or unauthorized state, which depends on the authentication result, as shown in Figure 1-2.

Figure 1-2 Authorized/unauthorized state of a controlled port



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

- Force-Authorized: Places the port in authorized state, allowing users of the port to access the network without authentication.
- Force-Unauthorized: Places the port in unauthorized state, denying any access requests from users of the port.
- Auto: Places the port in the unauthorized state initially to allow only EAPOL packets to pass, and turns the port into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

Control direction

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

Note

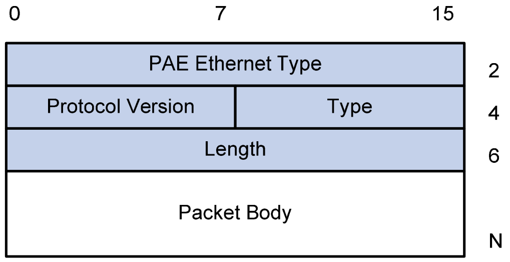
Currently, your device can only be set to deny traffic from the client.

EAP over LANs

EAPOL frame format

EAPOL, defined in 802.1X, is intended to carry EAP protocol packets between clients and devices over LANs. Figure 1-3 shows the EAPOL frame format.

Figure 1-3 EAPOL frame format



PAE Ethernet type: Protocol type. It takes the value 0x888E.

Protocol version: Version of the EAPOL protocol supported by the sender.

Type: Type of the EAPOL frame. Table 1-1 lists the types that the device currently supports.

Table 1-1 Types of EAPOL frames

Type	Description
EAP-Packet (a value of 0x00)	Packet for carrying authentication information, present between the device and the authentication server. A packet of this type is repackaged and transferred by RADIUS on the device to get through complex networks to reach the authentication server.
EAPOL-Start (a value of 0x01)	Packet for initiating authentication, present between a client and the device.
EAPOL-Logoff (a value of 0x02)	Packet for the logoff request, present between a client and the device.

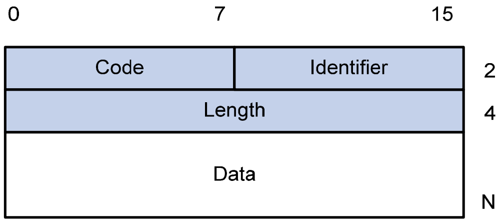
Length: Length of the data, that is, length of the Packet body field, in bytes. If the value of this field is 0, no subsequent data field is present.

Packet body: Content of the packet. The format of this field depends on the value of the Type field.

EAP packet format

An EAP-Packet-type EAPOL frame carries an EAP packet in its Packet body field. The format of the EAP packet is shown in Figure 1-4.

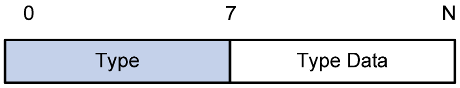
Figure 1-4 EAP packet format



Code: Type of the EAP packet, which can be Request, Response, Success, or Failure.

- An EAP success/failure packet has no Data field, and has a length of 4.
- An EAP Request/Response packet has a Data field in the format shown in Figure 1-5. The Type field indicates the EAP authentication type. A value of 1 represents Identity, indicating that the packet is for querying the identity of the client. A value of 4 represents MD5-Challenge, which are similar to the PPP CHAP protocol.

Figure 1-5 Format of the Data field in an EAP request/response packet



Identifier: Helps match responses with requests.

Length: Length of the EAP packet, including the Code, Identifier, Length, and Data fields, in bytes.

Data: Content of the EAP packet. Its format is determined by the Code field.

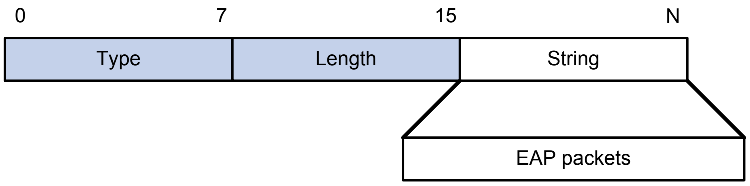
EAP over RADIUS

Two attributes of RADIUS are intended for supporting EAP authentication: EAP-Message and Message-Authenticator. For information about RADIUS packet format, refer to *RADIUS Configuration*.

EAP-Message

The EAP-Message attribute is used to encapsulate EAP packets. Figure 1-6 shows its encapsulation format. The value of the Type field is 79. The String field can be up to 253 bytes long. If the EAP packet is longer than 253 bytes, it can be fragmented and encapsulated into multiple EAP-Message attributes.

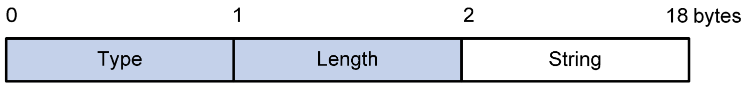
Figure 1-6 Encapsulation format of the EAP-Message attribute



Message-Authenticator

Figure 1-7 shows the encapsulation format of the Message-Authenticator attribute. The Message-Authenticator attribute is used to prevent access requests from being snooped during EAP or CHAP authentication. It must be included in any packet with the EAP-Message attribute; otherwise, the packet will be considered invalid and discarded.

Figure 1-7 Encapsulation format of the Message-Authenticator attribute



802.1X Authentication Triggering

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

Unsolicited triggering of a client

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

Some devices in the network may not support multicast packets with the above destination address, and unable to receive authentication requests of clients as a result. To solve this problem, the device also supports EAPOL-Start packets using a broadcast MAC address as the destination address. This solution requires the iNode 802.1X client.

Unsolicited triggering of the device

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

Authentication Process of 802.1X

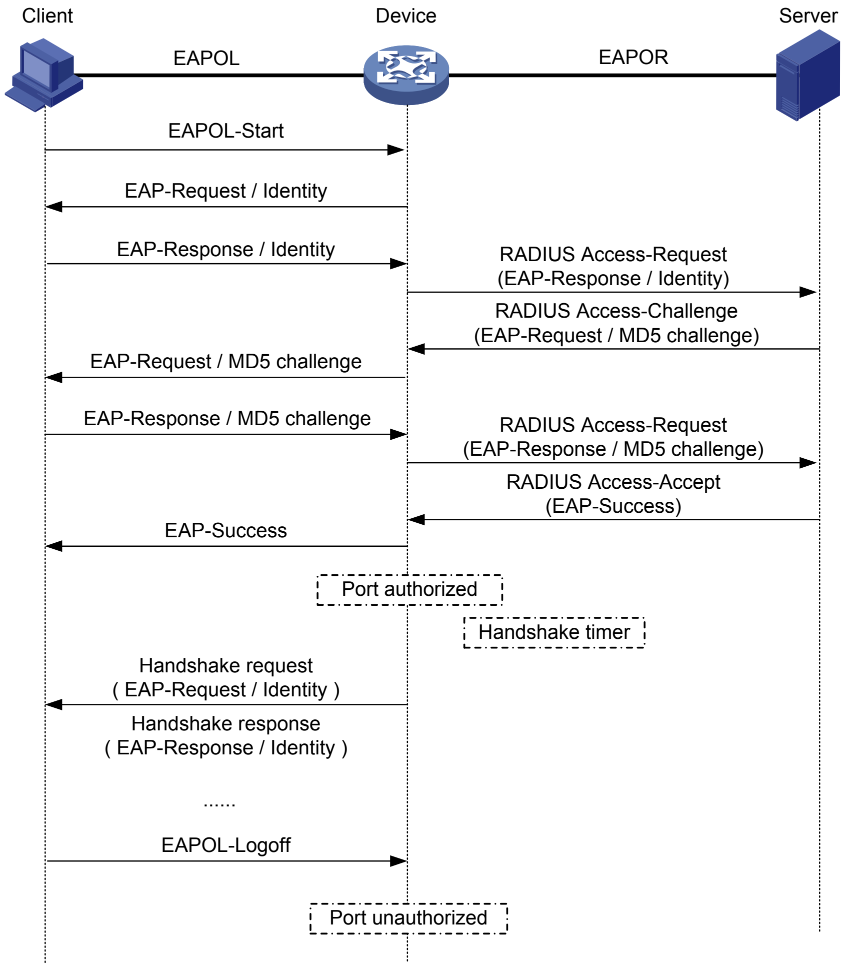
An 802.1X device communicates with a remote RADIUS server in two modes: EAP relay and EAP termination. The following describes the 802.1X authentication procedure in the two modes, which is triggered by the client in the examples.

EAP relay

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

Figure 1-8 shows the message exchange procedure with EAP-MD5.

Figure 1-8 802.1X authentication procedure in EAP relay mode



1) When a user launches the 802.1X client software and enters the registered username and password, the 802.1X client software generates an EAPOL-Start frame and sends it to the device to initiate an authentication process.
2) Upon receiving the EAPOL-Start frame, the device responds with an EAP-Request/Identity packet for the username of the client.
3) When the client receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the device.
4) Upon receiving the EAP-Response/Identity packet, the device relays the packet in a RADIUS Access-Request packet to the authentication server.
5) When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the device.
6) After receiving the RADIUS Access-Challenge packet, the device relays the contained EAP-Request/MD5 Challenge packet to the client.
7) When receiving the EAP-Request/MD5 Challenge packet, the client uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the device.
8) After receiving the EAP-Response/MD5 Challenge packet, the device relays the packet through a RADIUS Access-Request packet to the authentication server.

9) When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the device a RADIUS Access-Accept packet.
10) Upon receiving the RADIUS Access-Accept packet, the device opens the port to grant the access request of the client. After the client gets online, the device periodically sends handshake requests to the client to check whether the client is still online. By default, if two consecutive handshake attempts end up with failure, the device concludes that the client has gone offline and performs the necessary operations, guaranteeing that the device always knows when a client goes offline.
11) The client can also send an EAPOL-Logoff frame to the device to go offline unsolicitedly. In this case, the device changes the status of the port from authorized to unauthorized and sends an EAP-Failure packet to the client.

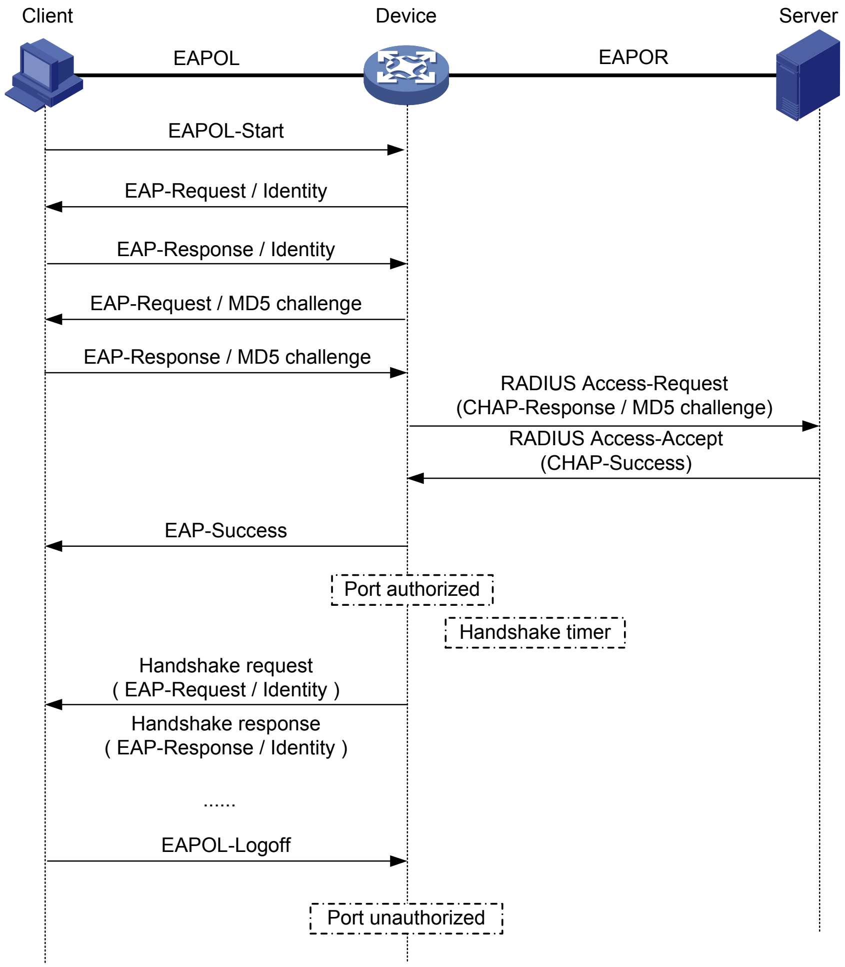
Note

In EAP relay mode, a client must use the same authentication method as that of the RADIUS server. On the device, however, you only need to enable EAP relay.

EAP termination

In EAP termination mode, EAP packets are terminated at the device and then repackaged into the PAP or CHAP attributes of RADIUS and transferred to the RADIUS server for authentication, authorization, and accounting. Figure 1-9 shows the message exchange procedure with CHAP authentication.

Figure 1-9 802.1X authentication procedure in EAP termination mode



Different from the authentication process in EAP relay mode, it is the device that generates the random challenge for encrypting the user password information in EAP termination authentication process. Consequently, the device sends the challenge together with the username and encrypted password information from the client to the RADIUS server for authentication.

802.1X Timers

This section describes the timers used on an 802.1X device to guarantee that the client, the device, and the RADIUS server can interact with each other in a reasonable manner.

- Username request timeout timer: This timer is triggered by the device in two cases. The first case is when the client requests for authentication. The device starts this timer when it sends an EAP-Request/Identity packet to a client. If it receives no response before this timer expires, the device retransmits the request. The second case is when the device authenticates the 802.1X client that cannot request for authentication actively. The device sends multicast EAP-Request/Identity packets periodically through the port enabled with 802.1X function. In this case, this timer sets the interval between sending the multicast EAP-Request/Identity packets.
- Client timeout timer: Once a device sends an EAP-Request/MD5 Challenge packet to a client, it starts this timer. If this timer expires but it receives no response from the client, it retransmits the request.

- Server timeout timer: Once a device sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Handshake timer: After a client passes authentication, the device sends to the client handshake requests at this interval to check whether the client is online. If the device receives no response after sending the allowed maximum number of handshake requests, it considers that the client is offline.
- Quiet timer (quiet-period): When a client fails the authentication, the device refuses further authentication requests from the client in this period of time.
- Periodic re-authentication timer: If periodic re-authentication is enabled on a port, the device re-authenticates online users on the port at the interval specified by this timer.

802.1X Extensions

The devices extend and optimize the mechanism that the 802.1X protocol specifies by:

- Allowing multiple users to access network services through the same physical port.
- Supporting two port access control methods: MAC-based access control and port-based access control. With the MAC-based access control method configured on a port, all users of the port must be authenticated separately, and when a user goes offline, no other users are affected. With the port-based access control method configured on a port, after a user connected to the port passes authentication, all subsequent users of the port can access network resources without authentication. However, when the authenticated user goes offline, the others are denied as well.

Features Working Together with 802.1X

VLAN assignment

After an 802.1X user passes the authentication, the server will send an authorization message to the device. If the server is configured with the VLAN assignment function, the assigned VLAN information will be included in the message. The device, depending on the link type of the port used to log in, adds the port to the assigned VLAN according to the following rules:

- If the port link type is Access, the port leaves its initial VLAN, that is, the VLAN configured for it and joins the assigned VLAN.
- If the port link type is Trunk, the assigned VLAN is allowed to pass the current trunk port. The default VLAN ID of the port is that of the assigned VLAN.
- If the port link type is Hybrid, the assigned VLAN is allowed to pass the current port without carrying the tag. The default VLAN ID of the port is that of the assigned VLAN. Note that if the Hybrid port is assigned a MAC-based VLAN, the device will dynamically create a MAC-based VLAN according to the VLAN assigned by the authentication server, and remain the default VLAN ID of the port unchanged.

The assigned VLAN neither changes nor affects the configuration of a port. However, as the assigned VLAN has higher priority than the initial VLAN of the port, it is the assigned VLAN that takes effect after a user passes authentication. After the user goes offline, the port returns to the initial VLAN of the port.

Note

- With a Hybrid port, the VLAN assignment will fail if you have configured the assigned VLAN to carry tags.
- With a Hybrid port, you cannot configure an assigned VLAN to carry tags after the VLAN has been assigned.

ACL assignment

ACLs provide a way of controlling access to network resources and defining access rights. When a user logs in through a port, and the RADIUS server is configured with authorization ACLs, the device will permit or deny data flows traversing through the port according to the authorization ACLs. Before specifying authorization ACLs on the server, you need to configure the ACL rules on the device. You can change the access rights of users by modifying authorization ACL settings on the RADIUS server or changing the corresponding ACL rules on the device.

Configuring 802.1X

Configuration Task List

802.1X provides a method for implementing user identity authentication. However, 802.1X cannot implement the authentication method solely by itself. RADIUS or local authentication must be configured to work with 802.1X. Therefore, before the 802.1X configuration, you need to configure the following:

- Configure the ISP domain to which the 802.1X user belongs and the AAA method to be used (that is, local authentication or RADIUS authentication.
- For remote RADIUS authentication, the username and password information must be configured on the RADIUS server.
- For local authentication, the username and password information must be configured on the device and the service type must be set to LAN-access.

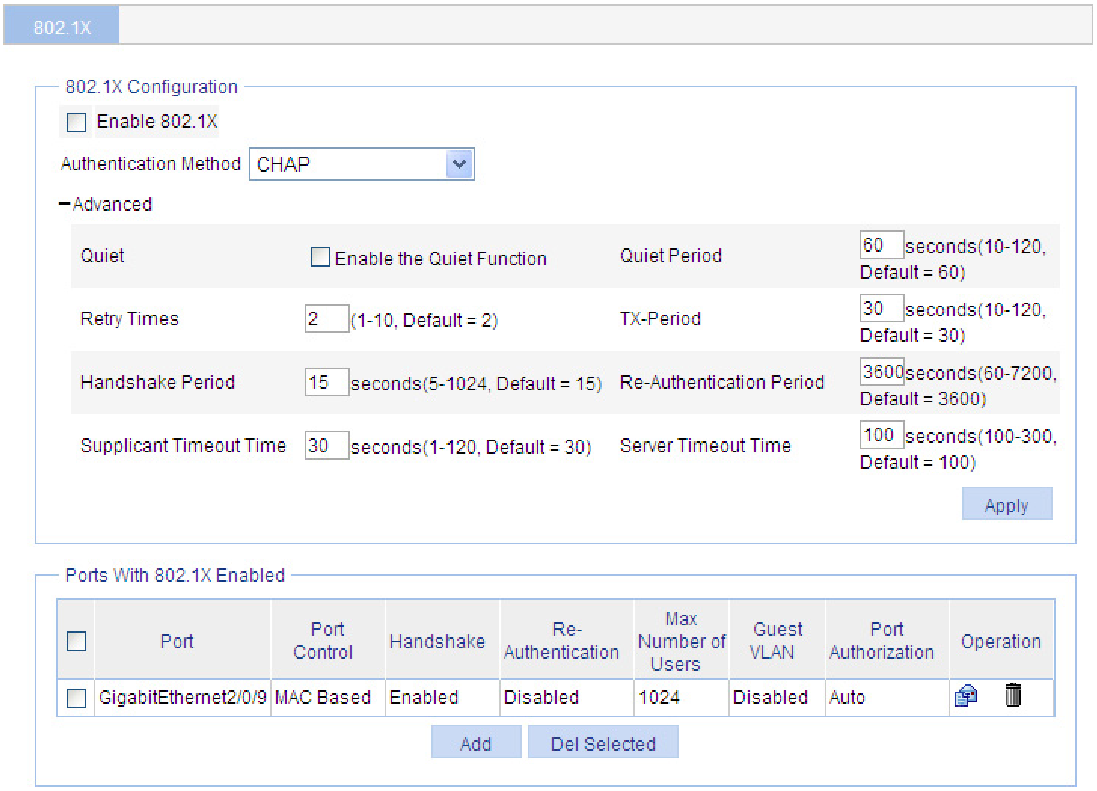
Table 1-2 lists the 802.1X configuration procedure.

Table 1-2 802.1X configuration procedure

Task	Description
Configuring 802.1X Globally	Required Enable 802.1X authentication globally and configure the authentication method and advanced parameters. By default, 802.1X authentication is disabled globally.
Configuring 802.1X on a Port	Required Enable 802.1X authentication on specified ports and configure 802.1X parameters for the ports. By default, 802.1X authentication is disabled on a port.

Configuring 802.1X Globally

From the navigation tree, select **Authentication** > **802.1X** to enter the 802.1X configuration page. Click the expansion mark **+** before **Advanced** to display the complete 802.1X configuration page, as shown in Figure 1-10. In the **802.1X Configuration** area, you can view and configure the 802.1X feature globally.



802.1X Configuration

☐ Enable 802.1X

Authentication Method: CHAP

−Advanced

Quiet	☐ Enable the Quiet Function	Quiet Period	60 seconds(10-120, Default = 60)
Retry Times	2 (1-10, Default = 2)	TX-Period	30 seconds(10-120, Default = 30)
Handshake Period	15 seconds(5-1024, Default = 15)	Re-Authentication Period	3600 seconds(60-7200, Default = 3600)
Supplicant Timeout Time	30 seconds(1-120, Default = 30)	Server Timeout Time	100 seconds(100-300, Default = 100)

Ports With 802.1X Enabled

☐	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation
☐	GigabitEthernet2/0/9	MAC Based	Enabled	Disabled	1024	Disabled	Auto	✎ 🗑

Figure 1-10 802.1X configuration page

Table 1-3 lists global 802.1X configuration items.

Table 1-3 Global 802.1X configuration items

Item	Description
Enable 802.1X	Enable or disable 802.1X authentication globally.
Authentication Method	Specify the authentication method for 802.1X users. Options include CHAP, PAP, and EAP.

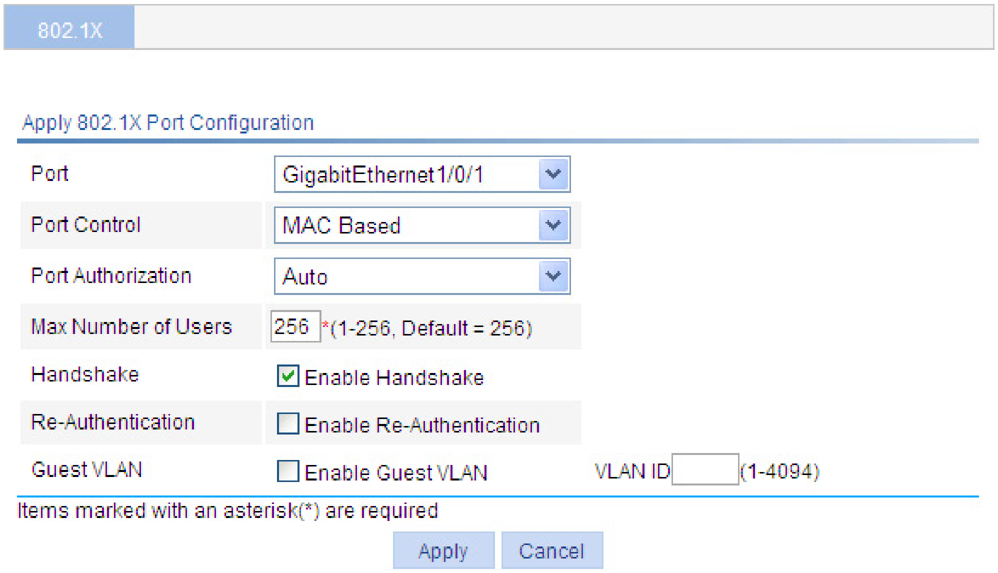
Item		Description
Advanced	Quiet	Specify whether to enable the quiet timer. After an 802.1X user fails to be authenticated, the device will keep quiet for a period of time defined by **Quiet Period**. During the quiet period, the device will not perform 802.1X authentication on the user.
	Quiet Period	Specify the value of the quiet timer.
	Retry Times	Specify the maximum number of attempts to send an authentication request to a client. Within a specified period of time (defined by the **TX Period** or **Supplicant Timeout Time** option), if the device does not receive the response from the client, the device will determine whether to send an authentication request again according to the value defined by this parameter. 1 means that the device will send an authentication request only once even if it does not receive any response from the client within the set interval. 2 means that the device will send an authentication request again if it does not receive any response from the client within the set interval, and so forth.
	TX-Period	Specify the transmission interval.
	Handshake Period	Specify the handshake interval.
	Re-Authentication Period	Specify the re-authentication interval.
	Supplicant Timeout Time	Specify the client timeout interval.
	Server Timeout Time	Specify the server timeout interval.

Return to 802.1X configuration procedure.

Configuring 802.1X on a Port

From the navigation tree, select **Authentication** > **802.1X** to enter the 802.1X configuration page, as shown in Figure 1-10. In the **Ports With 802.1X Enabled** area, the 802.1X configuration on ports are listed. Click **Add** to enter the port 802.1X configuration page, as shown in Figure 1-11.

Figure 1-11 802.1X configuration on a port



Apply 802.1X Port Configuration

Port	GigabitEthernet1/0/1
Port Control	MAC Based
Port Authorization	Auto
Max Number of Users	256 *(1-256, Default = 256)
Handshake	☑ Enable Handshake
Re-Authentication	□ Enable Re-Authentication
Guest VLAN	□ Enable Guest VLAN VLAN ID (1-4094)

Items marked with an asterisk(*) are required

Table 1-4 lists port 802.1X configuration items.

Table 1-4 Port 802.1X configuration items

Item	Description
Port	Select the port to be enabled with 802.1X authentication. Only ports not enabled with 802.1X authentication are available.
Port Control	Specify the 802.1X port access control method for the port, which can be **MAC Based** or **Port Based**.
Port Authorization	Specify the 802.1X authorization mode for the port. Options include: • Auto: The initial state on the specified port is unauthorized and becomes authorized when the authentication is successful. This mode is commonly applied. • Force-Authorized: The specified port is always in the authorized state. • Force-Unauthorized: The specified port is always in the unauthorized state.
Max Number of Users	Specify the maximum number of users allowed on the specified port.
HandShake	Specify whether to enable the online user handshake function, which is used by the device to periodically detect whether a user is still online.
Re-authentication	Specify whether to enable periodic re-authentication on the specified port.
Guest VLAN	**Note** *Currently, switch 2900 series do not support Guest VLAN function.*

Return to 802.1X configuration procedure.

Configuration Examples

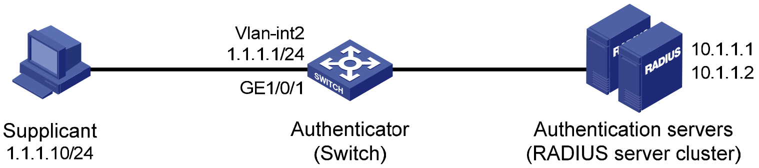
802.1X Configuration Example

Network requirements

As shown in Figure 1-12:

- It is required to perform 802.1X authentication on port GigabitEthernet 1/0/1 to control user access to the Internet, configure the access control method as MAC address based on the port, and enable periodic re-authentication of online users on the port, so that the server can periodically update the authorization information of the users.
- All users belong to default domain **test**. RADIUS authentication is performed. If RADIUS accounting fails, the switch gets the corresponding user offline. The RADIUS servers run iMC.
- A server group with two RADIUS servers is connected to the switch. The IP addresses of the servers are 10.1.1.1 and 10.1.1.2 respectively. Use the former as the primary authentication/secondary accounting server, and the latter as the secondary authentication/primary accounting server.
- Set the shared key for the device to exchange packets with the authentication server as **name**, and that for the device to exchange packets with the accounting server as **money**.
- Specify the device to try up to five times at an interval of 5 seconds in transmitting a packet to the RADIUS server until it receives a response from the server, and to send real time accounting packets to the accounting server every 15 minutes.
- Specify the device to remove the domain name from the username before passing the username to the RADIUS server.

Figure 1-12 Network diagram for 802.1X configuration



Configuration procedure

Note

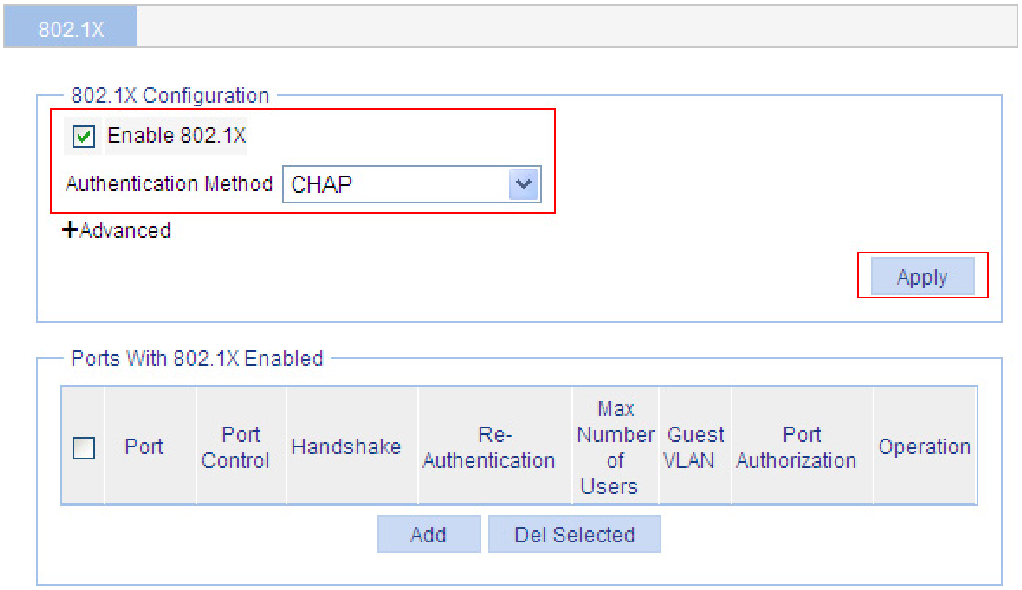
The following configuration procedure involves RADIUS client configuration for the switch, while configurations on the RADIUS servers are omitted. For information about RADIUS configuration, refer to *RADIUS Configuration*.

1) Configure the IP addresses of the interfaces. (omitted)
2) Configure 802.1X

# Enable 802.1X globally.

- From the navigation tree, select **Authentication** > **802.1X** to enter the 802.1X configuration page.

Figure 1-13 Global 802.1X configuration



802.1X

802.1X Configuration

☑ Enable 802.1X

Authentication Method: CHAP

+Advanced

Ports With 802.1X Enabled

□	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation

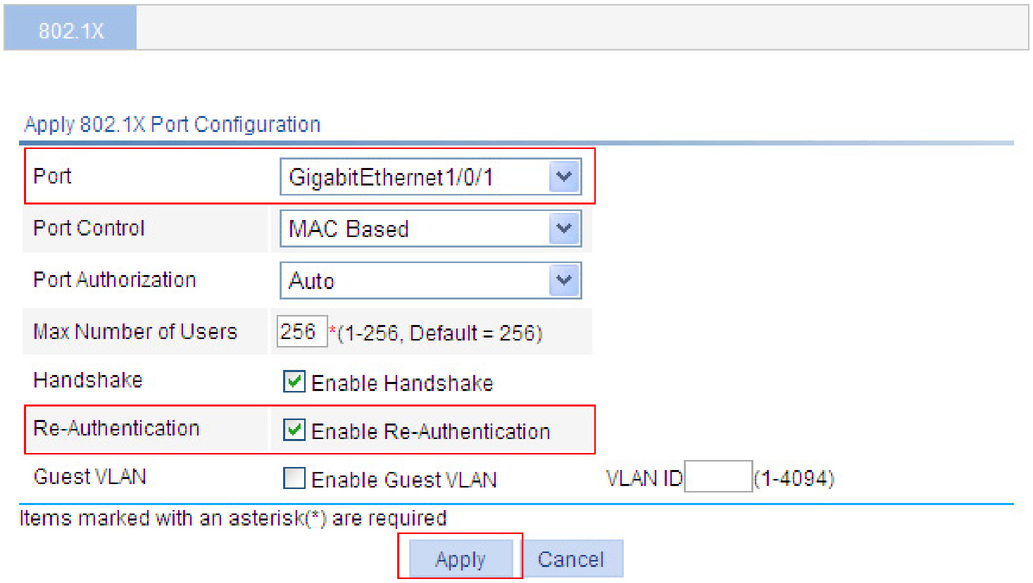
Perform the following configurations as shown in Figure 1-13.

- Select the check box before **Enable 802.1X**.
- Select the authentication method as CHAP.
- Click **Apply** to finish the operation.

# Enable and configure 802.1X on port GigabitEthernet 1/0/1.

- In the **Ports With 802.1X Enabled** area, click **Add**.

Figure 1-14 802.1X configuration of GigabitEthernet 1/0/1



802.1X

Apply 802.1X Port Configuration

Port	GigabitEthernet1/0/1
Port Control	MAC Based
Port Authorization	Auto
Max Number of Users	256 *(1-256, Default = 256)
Handshake	☑ Enable Handshake
Re-Authentication	☑ Enable Re-Authentication
Guest VLAN	□ Enable Guest VLAN VLAN ID (1-4094)

Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-14.

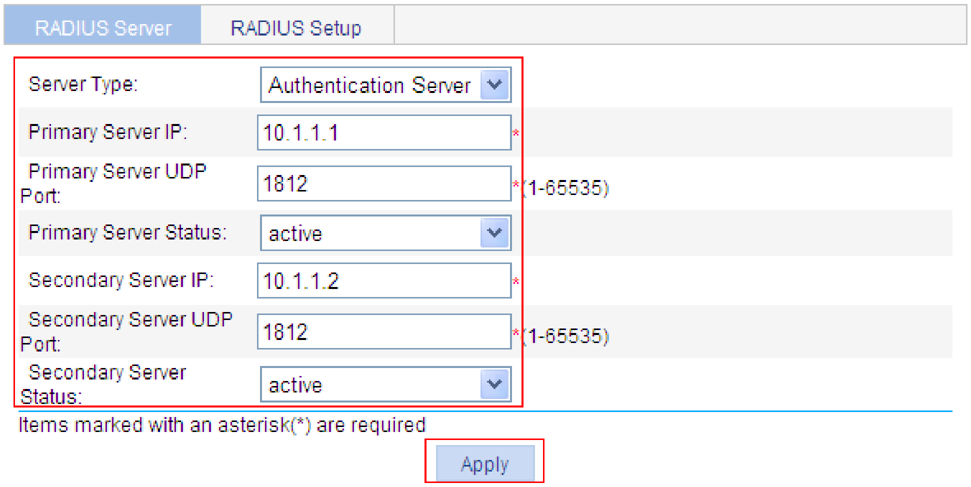
- Select port **GigabitEthernet1/0/1** from the port drop-down list.
- Select the checkbox before **Enable Re-Authentication**.
- Click **Apply** to finish the operation.

3) Configure the RADIUS scheme **system**

# Configure the RADIUS authentication servers.

- From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears.

Figure 1-15 RADIUS authentication server configuration



Server Type: Authentication Server

Primary Server IP: 10.1.1.1 *

Primary Server UDP Port: 1812 *(1-65535)

Primary Server Status: active

Secondary Server IP: 10.1.1.2 *

Secondary Server UDP Port: 1812 *(1-65535)

Secondary Server Status: active

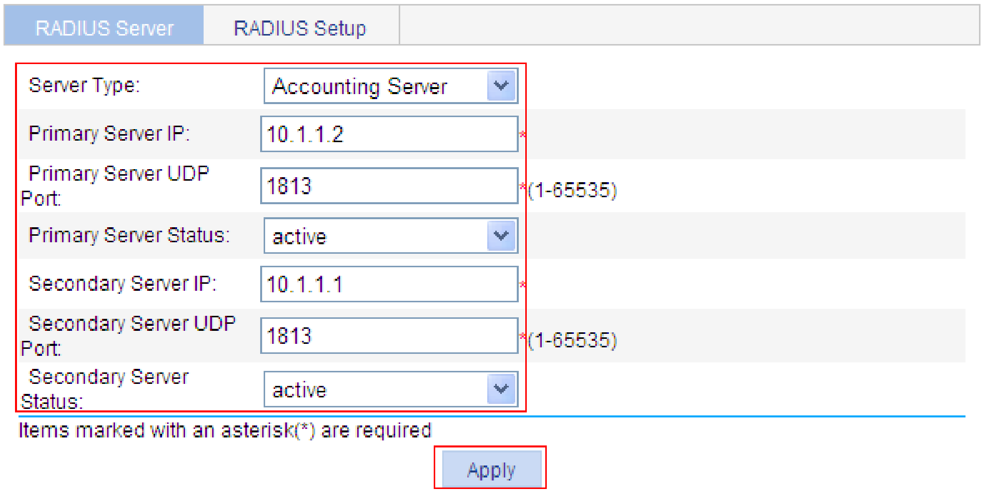
Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-15.

- Select **Authentication Server** as the server type.
- Enter the primary server IP address 10.1.1.1.
- Select **active** as the primary server's status.
- Enter the secondary server IP address 10.1.1.2.
- Select **active** as the secondary server's status.
- Click **Apply**.

# Configure the RADIUS accounting servers.

Figure 1-16 RADIUS accounting server configuration



Server Type: Accounting Server

Primary Server IP: 10.1.1.2 *

Primary Server UDP Port: 1813 *(1-65535)

Primary Server Status: active

Secondary Server IP: 10.1.1.1 *

Secondary Server UDP Port: 1813 *(1-65535)

Secondary Server Status: active

Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-16:

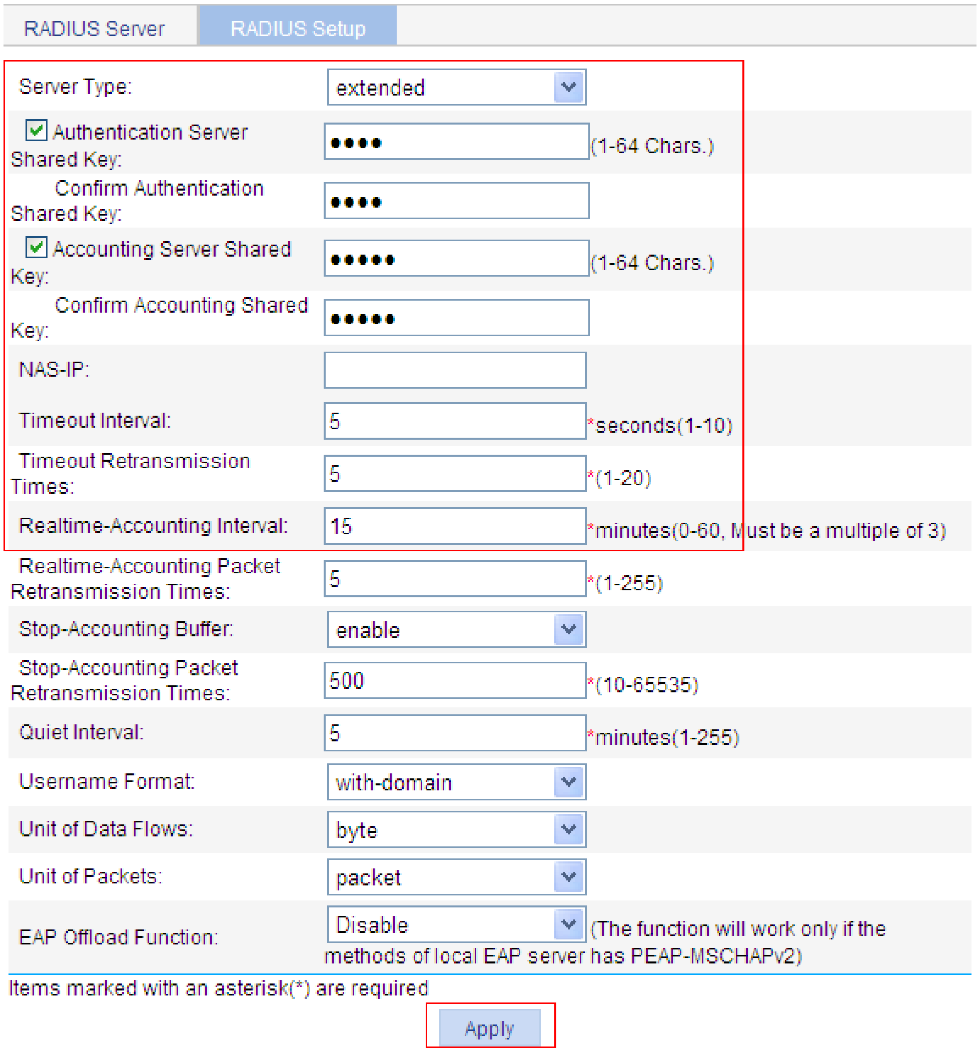
- Select **Accounting Server** as the server type.
- Enter the primary server IP address 10.1.1.2.
- Select **active** as the primary server's status.

- Enter the secondary server IP address 10.1.1.1.
- Select **active** as the secondary server's status.
- Click **Apply** to finish the operation.

# Configure the scheme used for communication between the device and the RADIUS servers.

- Select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page. Perform the following configurations as shown in Figure 1-17.

Figure 1-17 RADIUS parameter configuration



Server Type:	extended	
☑ Authentication Server Shared Key:	••••	(1-64 Chars.)
Confirm Authentication Shared Key:	••••	
☑ Accounting Server Shared Key:	•••••	(1-64 Chars.)
Confirm Accounting Shared Key:	•••••	
NAS-IP:		
Timeout Interval:	5	*seconds(1-10)
Timeout Retransmission Times:	5	*(1-20)
Realtime-Accounting Interval:	15	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	with-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	
EAP Offload Function:	Disable	(The function will work only if the methods of local EAP server has PEAP-MSCHAPv2)

Items marked with an asterisk(*) are required

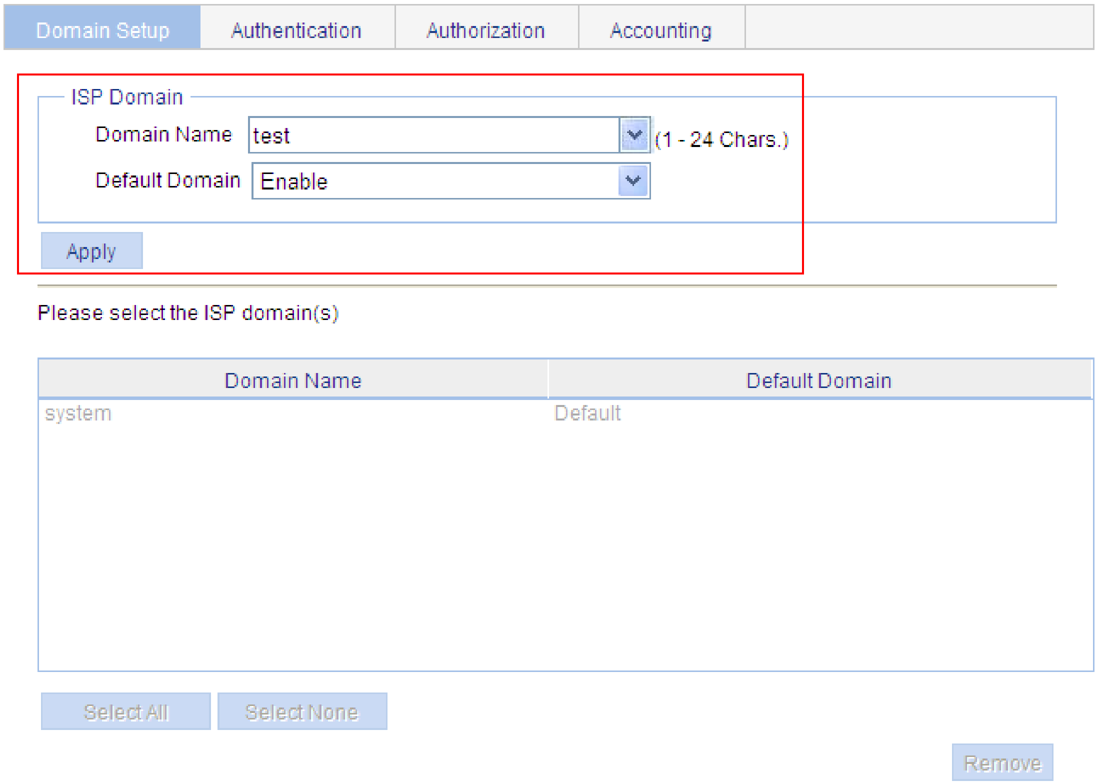
- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** checkbox, and enter **name** in the textbox.
- Enter **name** again in the **Confirm Authentication Shared Key** textbox.
- Select the **Accounting Server Shared Key** checkbox, and enter **money** in the textbox.
- Enter **money** again in the **Confirm Accounting Shared Key** textbox.
- Enter **5** in the **Timeout Interval** textbox
- Enter **5** in the **Timeout Retransmission Times** textbox.
- Enter **15** in the **Realtime-Accounting Interval** textbox.
- Click **Apply** to finish the operation.

4) Configure AAA

# Create an ISP domain.

- From the navigation tree, select **Authentication** > **AAA**. The domain setup page appears. Perform the following configurations as shown in Figure 1-18.

Figure 1-18 Create an ISP domain



ISP Domain

Domain Name: test (1 - 24 Chars.)

Default Domain: Enable

Please select the ISP domain(s)

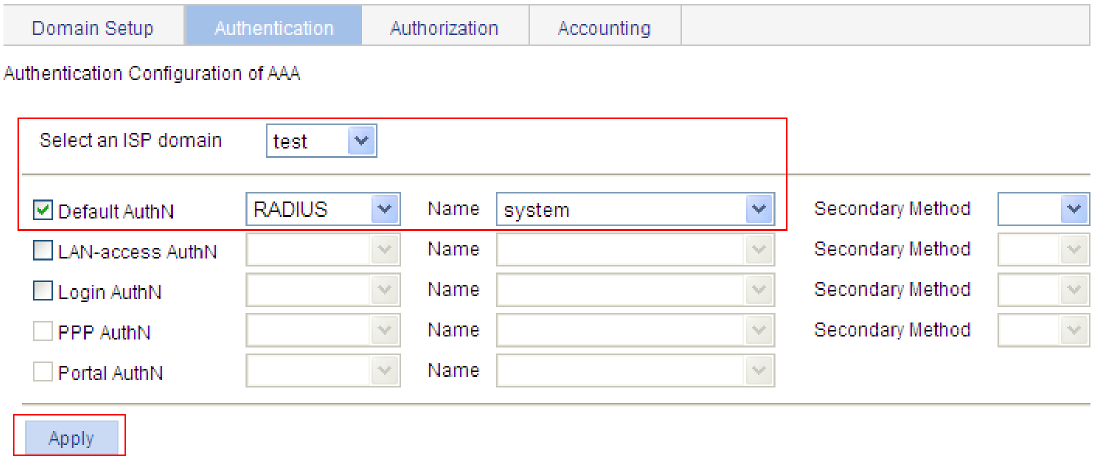
Domain Name	Default Domain
system	Default

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain as the default domain.
- Click **Apply** to finish the operation.

# Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab. Perform the following configurations as shown in Figure 1-19.

Figure 1-19 Configure the AAA authentication method for the ISP domain



Authentication Configuration of AAA

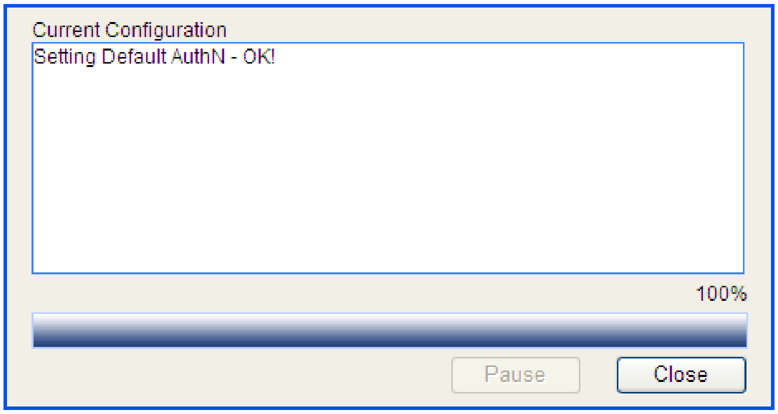
Select an ISP domain: test

☑ Default AuthN	RADIUS	Name	system	Secondary Method	
☐ LAN-access AuthN		Name		Secondary Method	
☐ Login AuthN		Name		Secondary Method	
☐ PPP AuthN		Name		Secondary Method	
☐ Portal AuthN		Name			

- Select the domain name **test**.
- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.

- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-20.

Figure 1-20 Configuration progress dialog box



Current Configuration

Setting Default AuthN - OK!

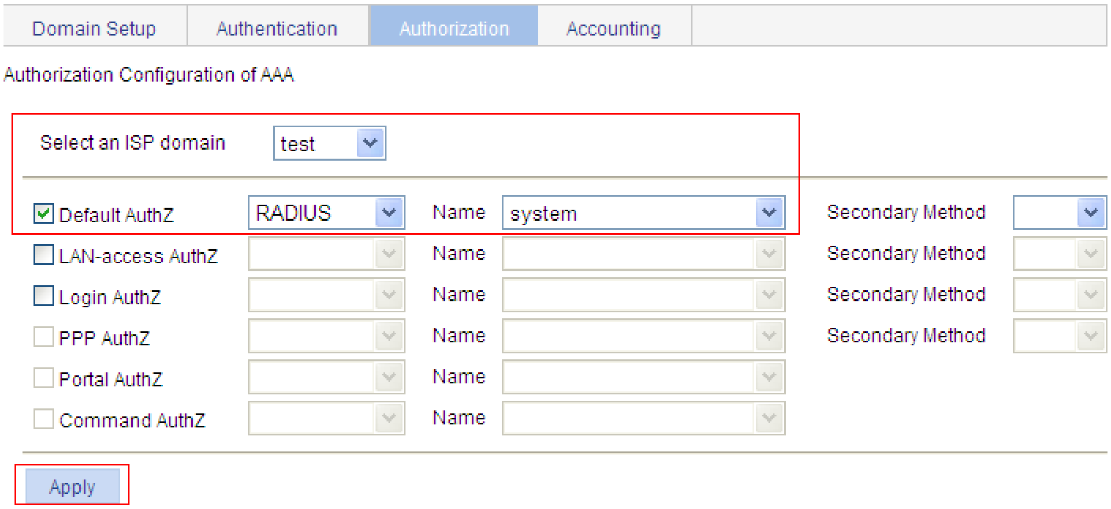
100%

- After the configuration process is complete, click **Close**.

# Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab. Perform the following configuration as shown in Figure 1-21.

Figure 1-21 Configure the AAA authorization method for the ISP domain



Authorization Configuration of AAA

Select an ISP domain: test

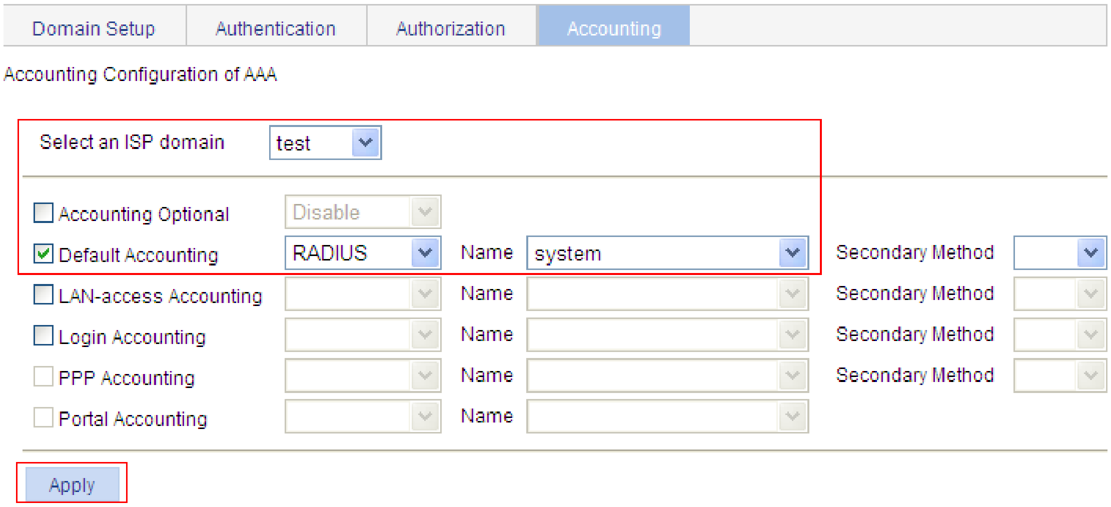
☑ Default AuthZ	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthZ		Name		Secondary Method	
□ Login AuthZ		Name		Secondary Method	
□ PPP AuthZ		Name		Secondary Method	
□ Portal AuthZ		Name			
□ Command AuthZ		Name			

- Select the domain name **test.**
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA accounting method for the ISP domain.

- Select the **Accounting** tab. Perform the following configurations, as shown in Figure 1-22.

Figure 1-22 Configure the AAA accounting method for the ISP domain



Accounting Configuration of AAA

Select an ISP domain: test

□ Accounting Optional	Disable				
☑ Default Accounting	RADIUS	Name	system	Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
□ Login Accounting		Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name			

- Select the domain name **test**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

ACL Assignment Configuration Example

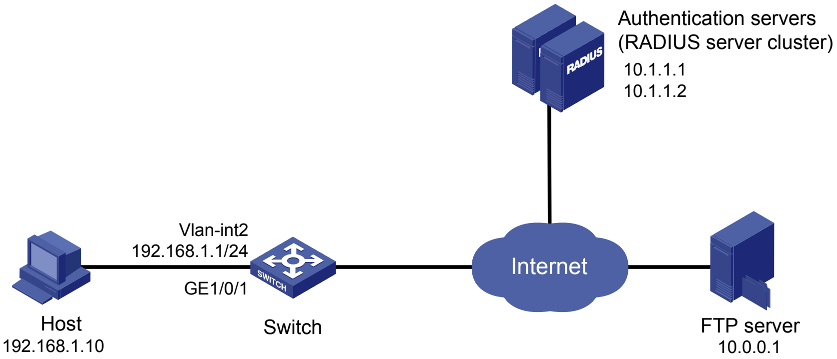
Network requirements

As shown in Figure 1-23, the switch and the RADIUS authentication servers (iMC servers) work together to authenticate the host that is to access the Internet. An FTP server is on the Internet, and its IP address is 10.0.0.1.

- Configure the authentication server to assign ACL 3000.
- Enable 802.1X for port GigabitEthernet 1/0/1 and configure ACL 3000 on the switch.

After a user passes authentication, the authentication server assigns ACL 3000. At this time, ACL 3000 takes effect on GigabitEthernet 1/0/1, allowing the host to access the Internet but not the FTP server.

Figure 1-23 Network diagram for ACL assignment



Configuration procedure

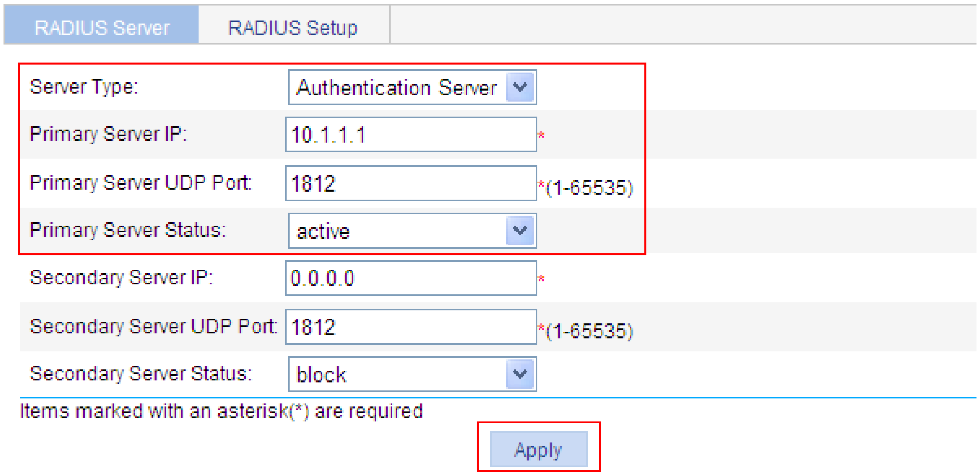
1) Configure the IP addresses of the interfaces. (Omitted)

2) Configure the RADIUS scheme **system**

# Configure the RADIUS authentication server.

- From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears.

Figure 1-24 RADIUS authentication server configuration



Server Type: Authentication Server

Primary Server IP: 10.1.1.1 *

Primary Server UDP Port: 1812 *(1-65535)

Primary Server Status: active

Secondary Server IP: 0.0.0.0 *

Secondary Server UDP Port: 1812 *(1-65535)

Secondary Server Status: block

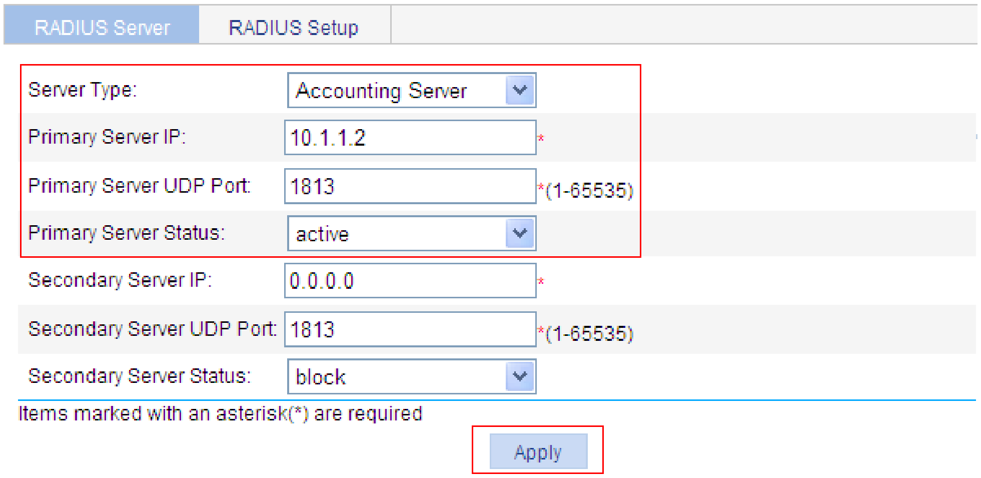
Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-24.

- Select **Authentication Server** as the server type.
- Enter the primary server IP address 10.1.1.1.
- Enter the primary server UDP port number 1812.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the RADIUS accounting server.

Figure 1-25 RADIUS accounting server configuration



Server Type: Accounting Server

Primary Server IP: 10.1.1.2 *

Primary Server UDP Port: 1813 *(1-65535)

Primary Server Status: active

Secondary Server IP: 0.0.0.0 *

Secondary Server UDP Port: 1813 *(1-65535)

Secondary Server Status: block

Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-25:

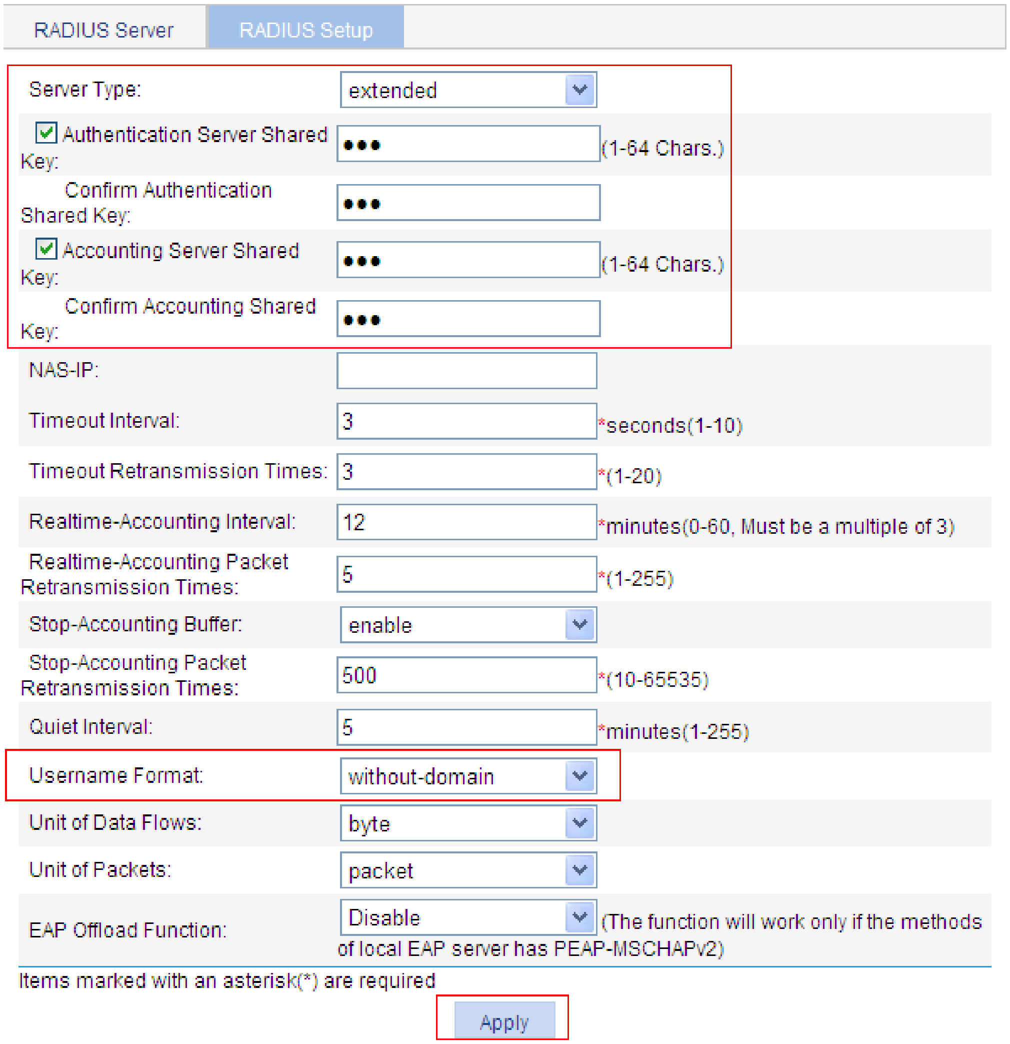
- Select **Accounting Server** as the server type.
- Enter the primary server IP address 10.1.1.2.

- Enter the primary server UDP port number 1813.
- Select **active** as the primary server status.
- Click **Apply** to finish the operation.

# Configure the scheme to be used for communication between the switch and the RADIUS servers.

- Select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page.

Figure 1-26 RADIUS parameter configuration



Server Type:	extended	
☑ Authentication Server Shared Key:	●●●	(1-64 Chars.)
Confirm Authentication Shared Key:	●●●	
☑ Accounting Server Shared Key:	●●●	(1-64 Chars.)
Confirm Accounting Shared Key:	●●●	
NAS-IP:		
Timeout Interval:	3	*seconds(1-10)
Timeout Retransmission Times:	3	*(1-20)
Realtime-Accounting Interval:	12	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	without-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	
EAP Offload Function:	Disable	(The function will work only if the methods of local EAP server has PEAP-MSCHAPv2)

Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-26.

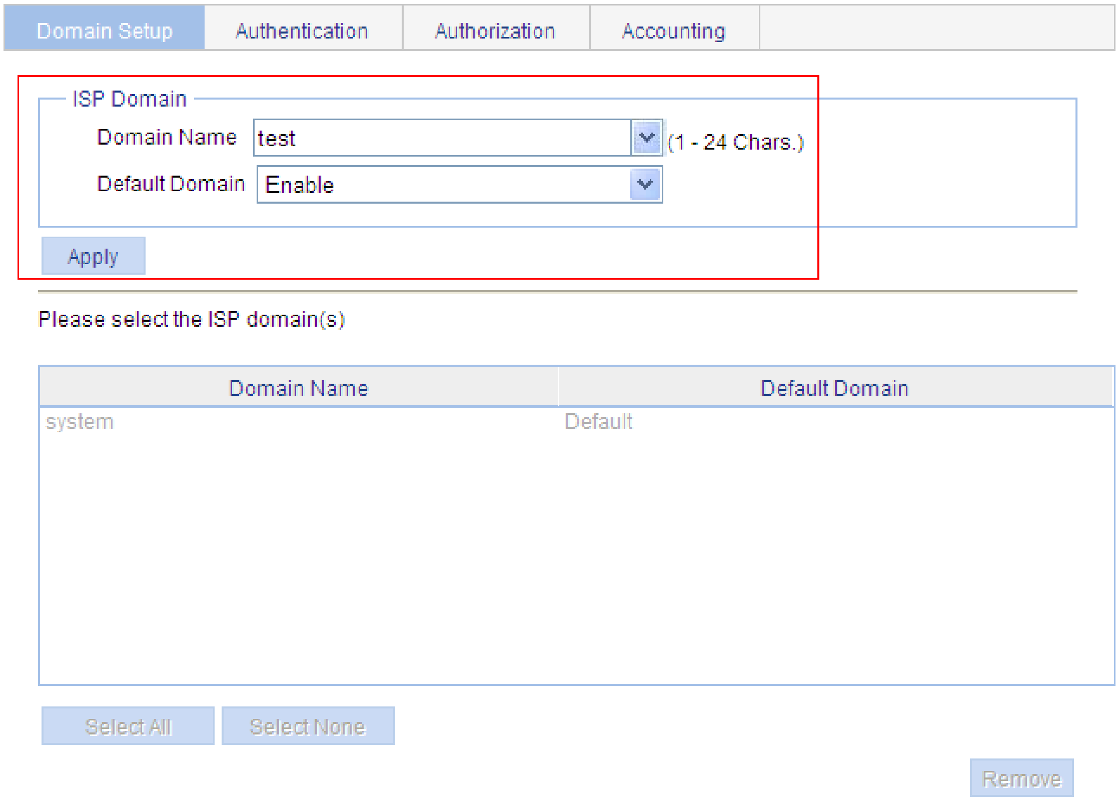
- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** checkbox, and enter **abc** in the textbox.
- Enter **abc** again in the **Confirm Authentication Shared Key** textbox.
- Select the **Accounting Server Shared Key** checkbox, and enter **abc** in the textbox.
- Enter **abc** again in the **Confirm Accounting Shared Key** textbox.
- Select **without-domain** as the username format.
- Click **Apply** to finish the operation.

3) Configure AAA

# Create an ISP domain.

- From the navigation tree, select **Authentication** > **AAA.** The domain setup page appears.

Figure 1-27 Create an ISP domain



Domain Name: test (1 - 24 Chars.)

Default Domain: Enable

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

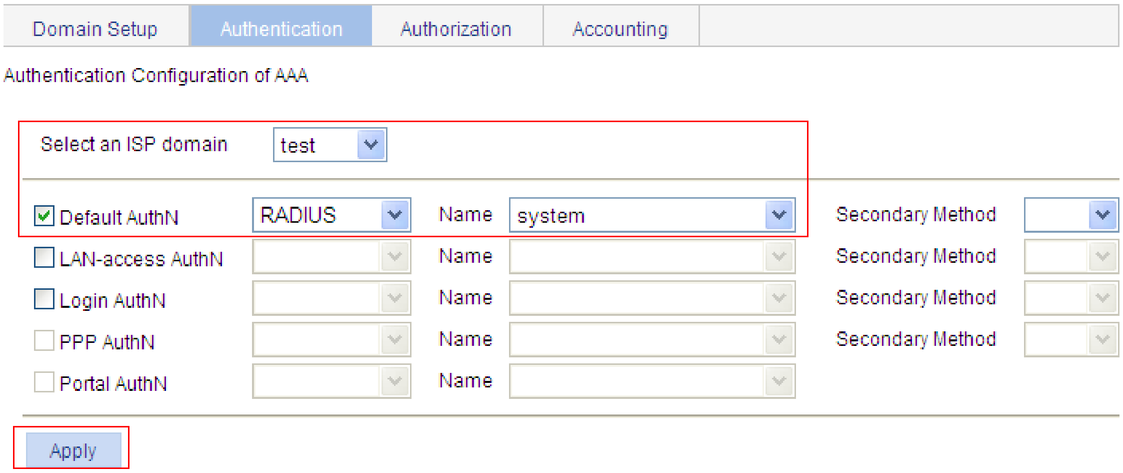
Perform the following configurations, as shown in Figure 1-27.

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain the default domain.
- Click **Apply** to finish the operation.

# Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab.

Figure 1-28 Configure the AAA authentication method for the ISP domain



Authentication Configuration of AAA

Select an ISP domain: test

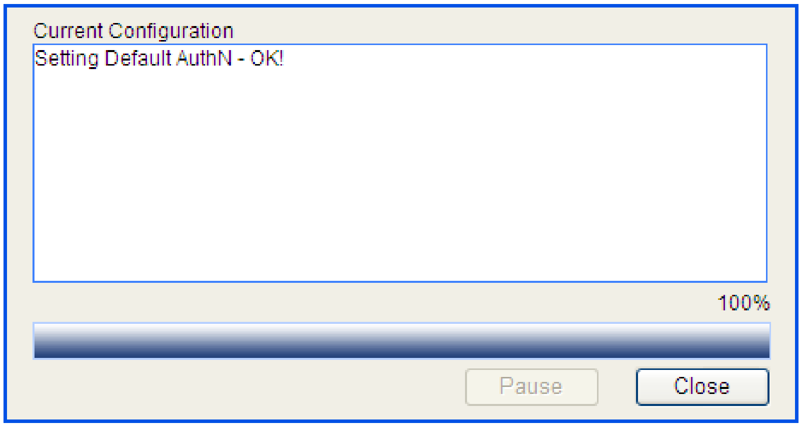
☑ Default AuthN	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthN		Name		Secondary Method	
□ Login AuthN		Name		Secondary Method	
□ PPP AuthN		Name		Secondary Method	
□ Portal AuthN		Name			

Perform the following configurations as shown in Figure 1-28.

- Select the domain name **test**.

- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. The configuration progress dialog box appears, as shown in Figure 1-29.

Figure 1-29 Configuration progress dialog box



Current Configuration

Setting Default AuthN - OK!

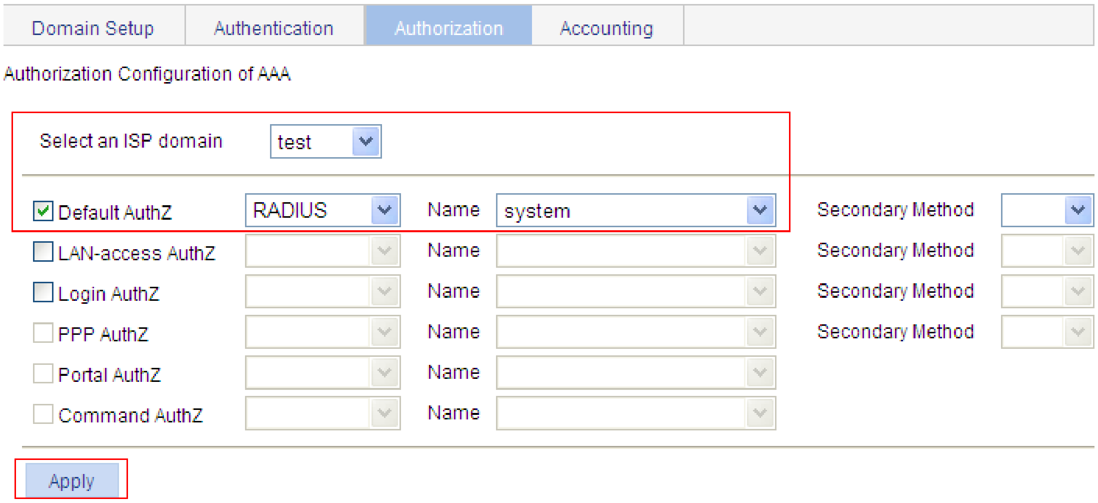
100%

- After you see the prompt of configuration success, click **Close** to finish the operation.

# Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab.

Figure 1-30 Configure the AAA authorization method for the ISP domain



Authorization Configuration of AAA

Select an ISP domain: test

☑ Default AuthZ	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthZ		Name		Secondary Method	
□ Login AuthZ		Name		Secondary Method	
□ PPP AuthZ		Name		Secondary Method	
□ Portal AuthZ		Name			
□ Command AuthZ		Name			

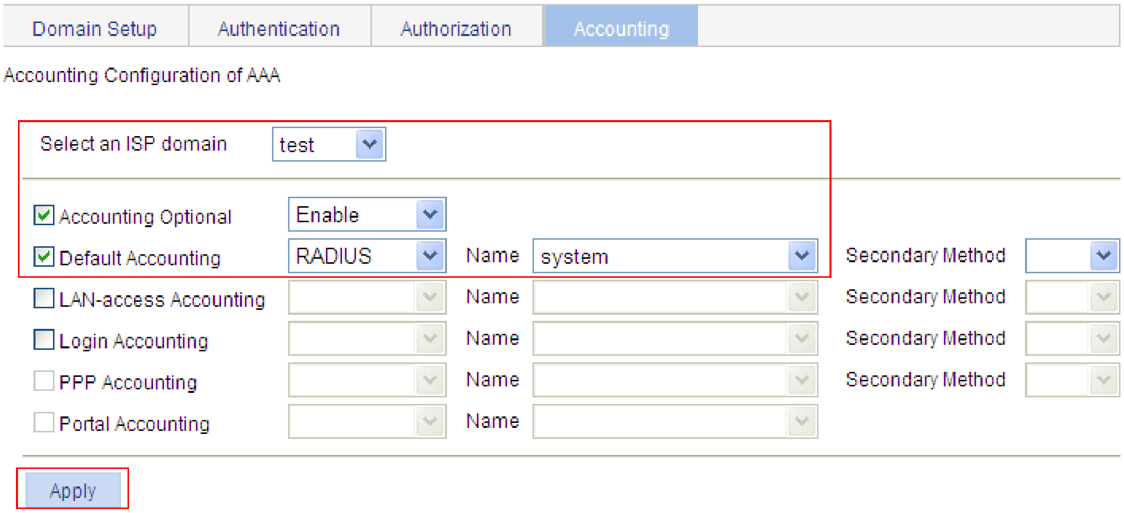
Perform the following configuration as shown in Figure 1-30.

- Select the domain name **test**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. The configuration progress dialog box appears.
- After you see the prompt of configuration success, click **Close** to finish the operation.

# Configure the AAA accounting method for the ISP domain, and enable accounting optional.

- Select the **Accounting** tab.

Figure 1-31 Configure the AAA accounting method for the ISP domain



Accounting Configuration of AAA

Select an ISP domain: test

☑ Accounting Optional	Enable				
☑ Default Accounting	RADIUS	Name	system	Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
□ Login Accounting		Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name			

Perform the following configurations, as shown in Figure 1-31.

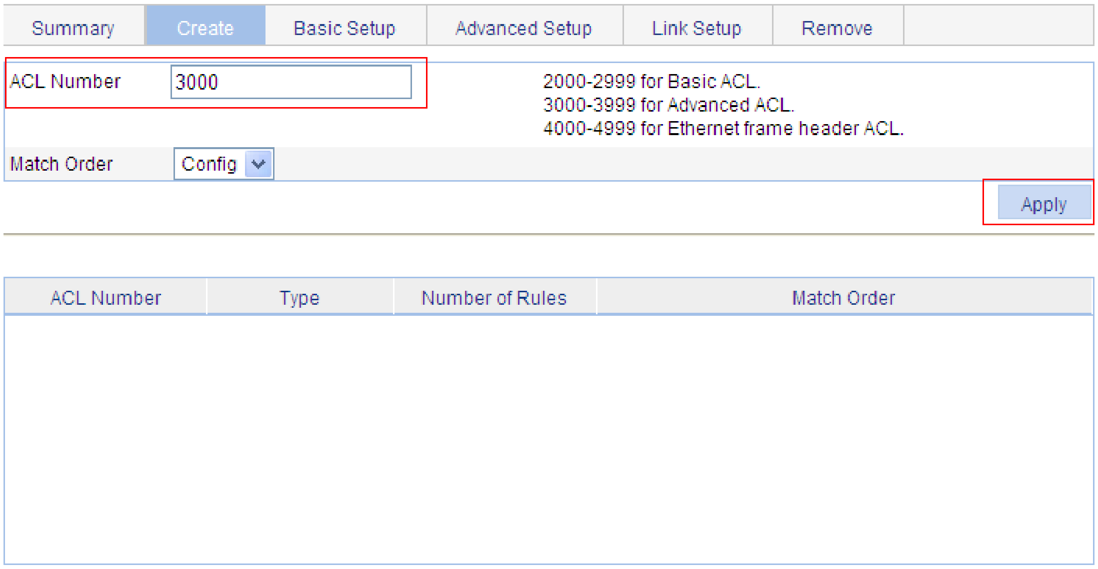
- Select the domain name **test**.
- Select the **Accounting Optional** checkbox, and then select **Enable** for this parameter.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. The configuration progress dialog box appears.
- After seeing the prompt of configuration success, click **Close** to finish the operation.

4) Configure an ACL

# Create ACL 3000 that denies packets with destination IP address 10.0.0.1.

- From the navigation tree, select **QoS** > **ACL IPv4** to enter the IPv4 ACL configuration page, and then select the **Create** tab.

Figure 1-32 Create ACL 3000



ACL Number: 3000

2000-2999 for Basic ACL.
3000-3999 for Advanced ACL.
4000-4999 for Ethernet frame header ACL.

Match Order: Config

ACL Number	Type	Number of Rules	Match Order

Perform the following configurations, as shown in Figure 1-32.

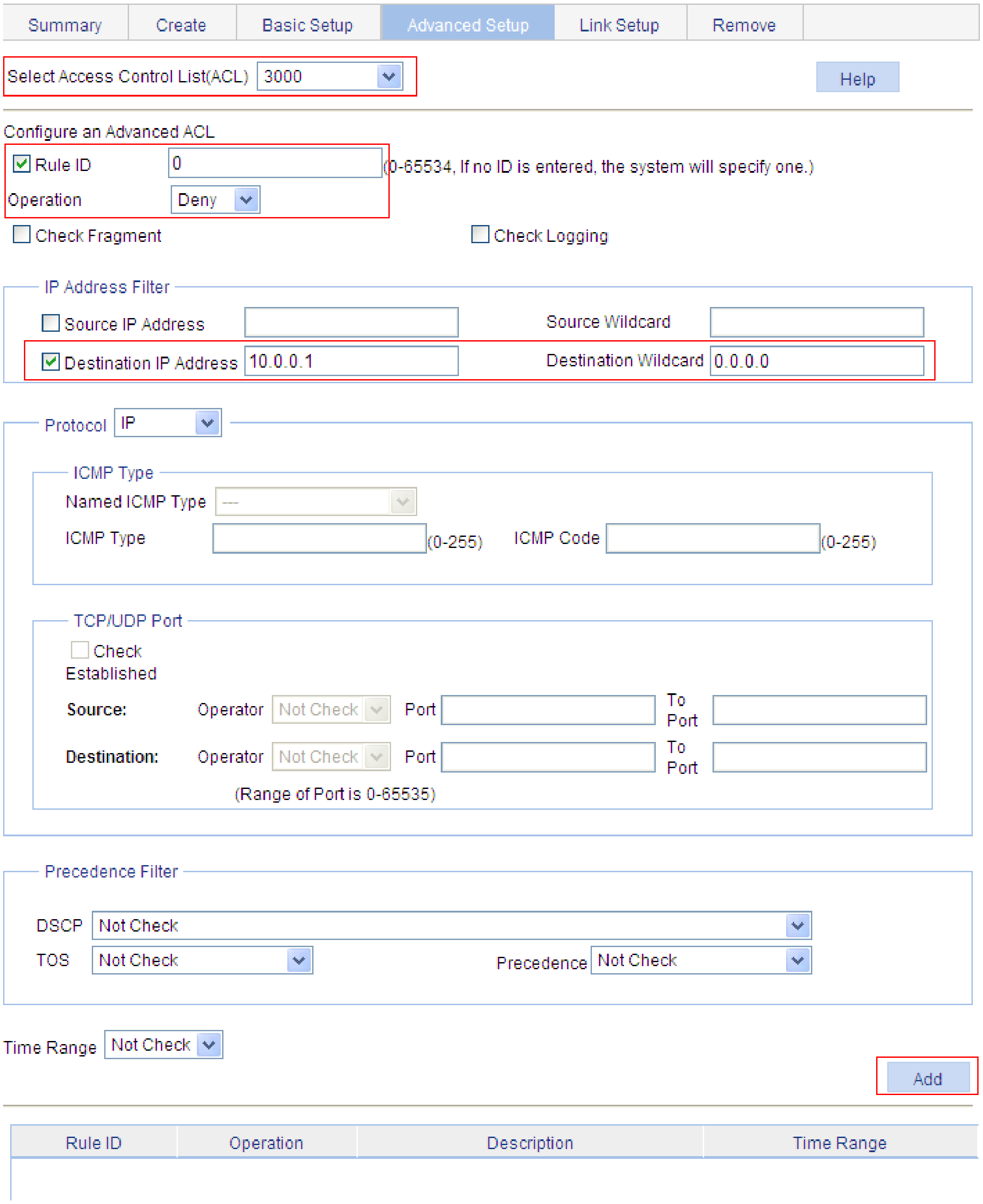
- Enter 3000 as the ACL number.

- Click **Apply** to finish the operation.

# Configure the ACL to deny packets with destination IP address 10.0.0.1.

- Select the **Advanced Setup** tab.

Figure 1-33 ACL rule configuration



Select Access Control List(ACL) 3000

Configure an Advanced ACL

☑ Rule ID 0 (0-65534, If no ID is entered, the system will specify one.)

Operation Deny

□ Check Fragment □ Check Logging

IP Address Filter

□ Source IP Address | Source Wildcard

☑ Destination IP Address 10.0.0.1 | Destination Wildcard 0.0.0.0

Protocol IP

ICMP Type

Named ICMP Type ---

ICMP Type (0-255) ICMP Code (0-255)

TCP/UDP Port

□ Check Established

Source: Operator Not Check Port To Port

Destination: Operator Not Check Port To Port

(Range of Port is 0-65535)

Precedence Filter

DSCP Not Check

TOS Not Check Precedence Not Check

Time Range Not Check

Perform the following configurations, as shown in Figure 1-33.

- Select 3000 from the **Select Access Control List(ACL)** drop-down list.
- Select the **Rule ID** check box, and enter 0 as the rule ID.
- Select **Deny** as the operation action.
- In the **IP Address Filter** area, select the **Destination IP Address** check box, and enter 10.0.0.1 in the text box.

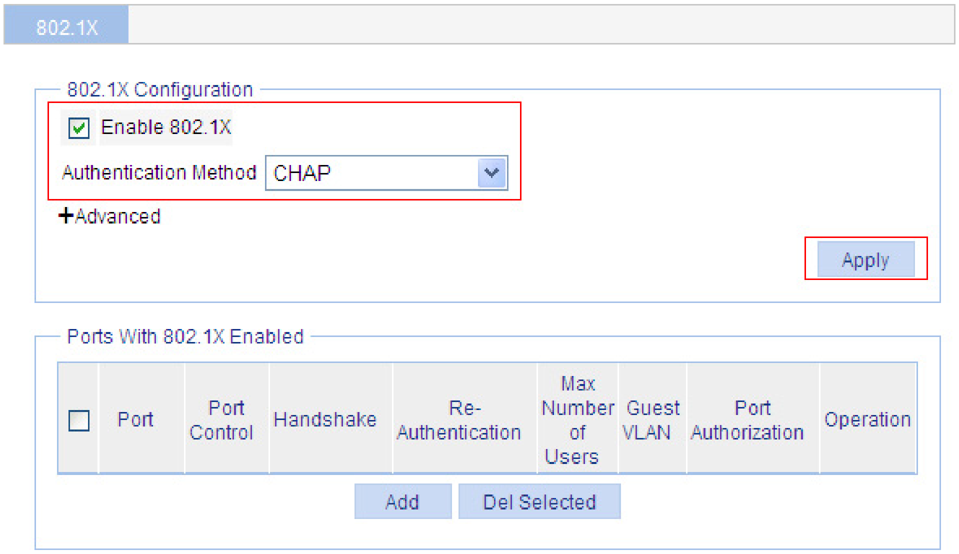
- Enter 0.0.0.0 in the **Destination Wildcard** text box.
- Click **Add** to finish the operation.

5) Configure the 802.1X feature

# Enable the 802.1X feature globally.

- From the navigation tree, select **Authentication** > **802.1X** to enter the 802.1X configuration page.

Figure 1-34 Global 802.1X globally



802.1X

802.1X Configuration

☑ Enable 802.1X

Authentication Method: CHAP

+Advanced

Ports With 802.1X Enabled

□	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation

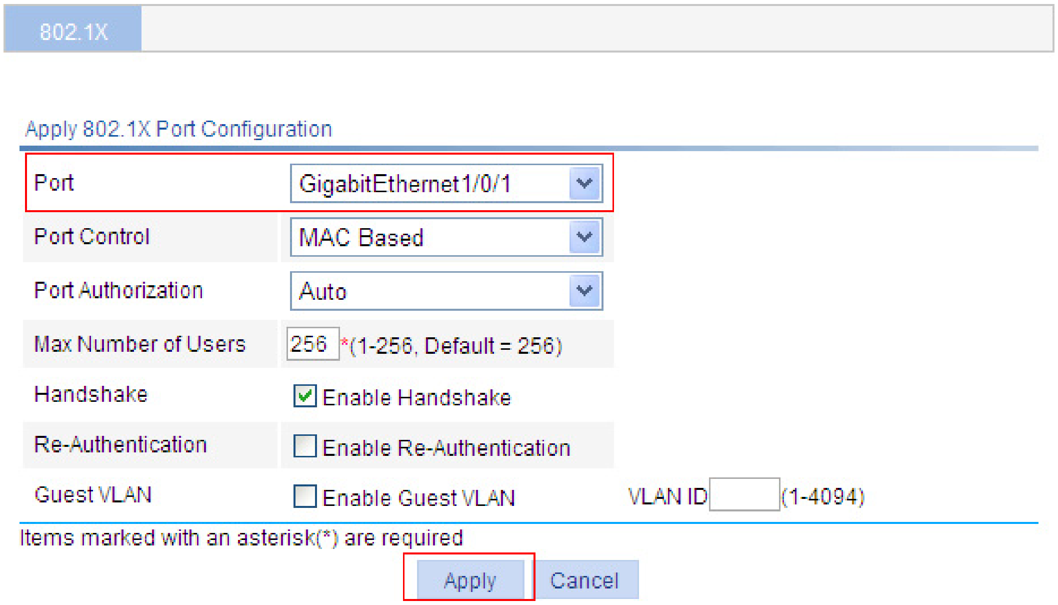
Perform the following configuration as shown in Figure 1-34.

- Select the check box before **Enable 802.1X**.
- Select the authentication method as CHAP.
- Click **Apply** to finish the operation.

# Enable 802.1X on port GigabitEthernet 1/0/1.

- In the **Ports With 802.1X Enabled** area, click **Add**.

Figure 1-35 802.1X configuration of GigabitEthernet 1/0/1



802.1X

Apply 802.1X Port Configuration

Port	GigabitEthernet1/0/1
Port Control	MAC Based
Port Authorization	Auto
Max Number of Users	256 *(1-256, Default = 256)
Handshake	☑ Enable Handshake
Re-Authentication	□ Enable Re-Authentication
Guest VLAN	□ Enable Guest VLAN VLAN ID (1-4094)

Items marked with an asterisk(*) are required

Perform the following configurations as shown in Figure 1-35.

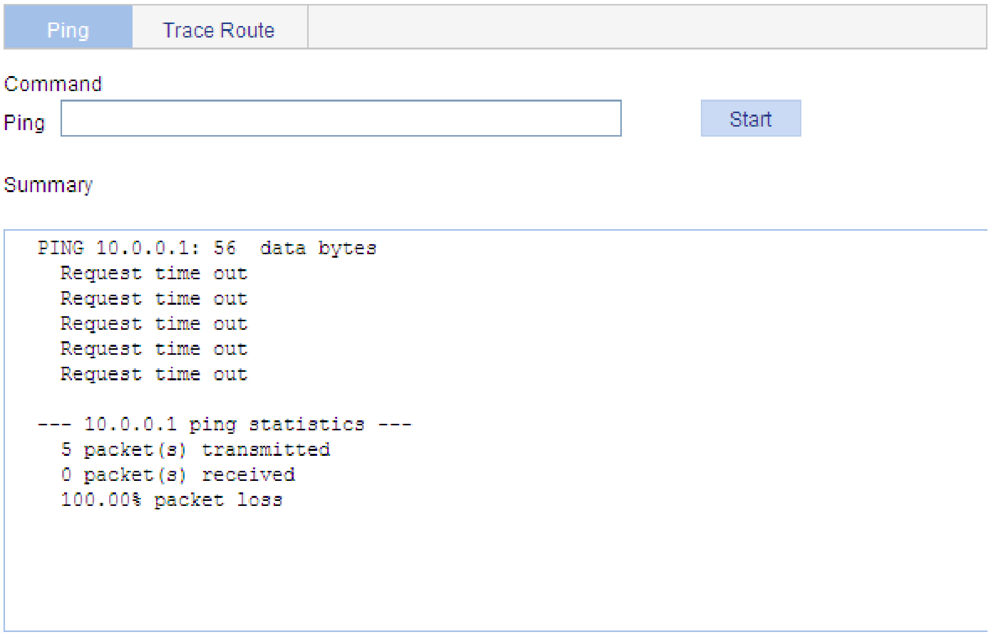
- Select **GigabitEthernet1/0/1** from the port list.
- Click **Apply** to finish the operation.

Configuration verification

# After the user passes authentication and gets online, use the **ping** command to test whether ACL 3000 takes effect.

- From the navigation tree, select **Network** > **Diagnostic Tools**. The ping page appears.
- Enter the destination IP address 10.0.0.1.
- Click **Start** to start the ping operation.
- Figure 1-36 shows the ping operation summary.

Figure 1-36 Ping operation summary



```
PING 10.0.0.1: 56  data bytes
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out

--- 10.0.0.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Configuration Guidelines

When configuring 802.1X, note that:

1) 802.1X configuration on a specific port can take effect only after both global 802.1X and 802.1X on the specific port are enabled.
2) Do not change the timer parameters of global 802.1X from their default values unless you have determined that the changes would better the interaction process in some special network environment.
3) A port enabled with 802.1X cannot be added to an aggregation group. Meanwhile, it is prohibited to enable 802.1X on a port that belongs to an aggregation group.
4) For an 802.1X client using Extensible Authentication Protocol (EAP) authentication, the device directly encapsulates contents from the client and sends them to the authentication server. In this scenario, the configuration on username format on the device does not take effect. For details about username format configuration, refer to *RADIUS Configuration.*
5) The Voice VLAN and 802.1X functions are mutually exclusive on an access port if the connected client sends untagged traffic.

Table of Contents

1 AAA Configuration

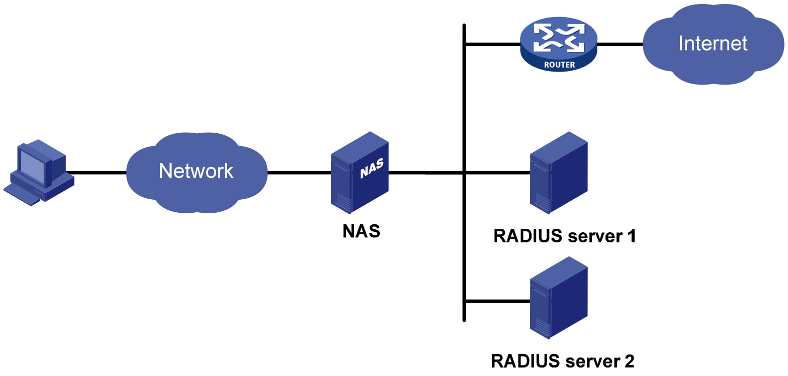
Overview

Introduction to AAA

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for configuring these three security functions to implement network security management.

AAA usually uses a client/server model, where the client runs on the network access server (NAS) and the server maintains user information centrally. In an AAA network, a NAS is a server for users but a client for the AAA servers, as shown in Figure 1-1.

Figure 1-1 AAA networking diagram



When a user tries to establish a connection to the NAS and to obtain the rights to access other networks or some network resources, the NAS authenticates the user or the corresponding connection. The NAS takes the responsibility to transparently pass the user's AAA information to the server (RADIUS server, for example). The RADIUS protocol defines how a NAS and a server exchange user information between them.

In the AAA network shown in Figure 1-1, there are two RADIUS servers. You can determine which of the authentication, authorization and accounting functions should be assumed by which servers. For example, you can use RADIUS server 1 for authentication and authorization, and RADIUS server 2 for accounting.

The three security functions are described as follows:

- Authentication: Identifies remote users and judges whether a user is legal.
- Authorization: Grants different users different rights. For example, a user logging into the server can be granted the permission to access and print the files in the server.
- Accounting: Records all network service usage information of users, including the service type, start and end time, and traffic. In this way, accounting can be used for not only charging, but also network security surveillance.

You can use AAA to provide only one or two security functions, if desired. For example, if your company only wants employees to be authenticated before they access specific resources, you only need to configure an authentication server. If network usage information is expected to be recorded, you also need to configure an accounting server.

As described above, AAA provides a uniform framework to implement network security management. It is a security mechanism that enables authenticated and authorized entities to access specific resources and records operations of the entities. As the AAA framework allows for excellent scalability and centralized user information management, it has gained wide application.

AAA can be implemented through multiple protocols. Currently, the device supports using RADIUS, which is often used in practice. For details about RADIUS, refer to *RADIUS Configuration*.

Introduction to ISP Domain

An Internet service provider (ISP) domain represents a group of users. For a username in the *userid@isp-name* format, the access device considers the *userid* part the username for authentication and the *isp-name* part the ISP domain name.

In a networking scenario with multiple ISPs, an access device may connect users of different ISPs. As users of different ISPs may have different user attributes (such as username and password structure, service type, and rights), you need to configure ISP domains to distinguish the users. In addition, you need to configure different attribute sets including AAA methods for the ISP domains.

For the NAS, each user belongs to an ISP domain. If a user does not provide the ISP domain name, the system considers that the user belongs to the default ISP domain.

Configuring AAA

Configuration Prerequisites

1) To deploy local authentication, you need to configure local users on the access device. Refer to *User Configuration* for details.
2) To deploy remote authentication, authorization, or accounting, you need to create the RADIUS schemes to be referenced. For details about RADIUS scheme configuration, refer to *RADIUS Configuration*.

Configuration Task List

Perform the tasks in Table 1-1 to configure AAA.

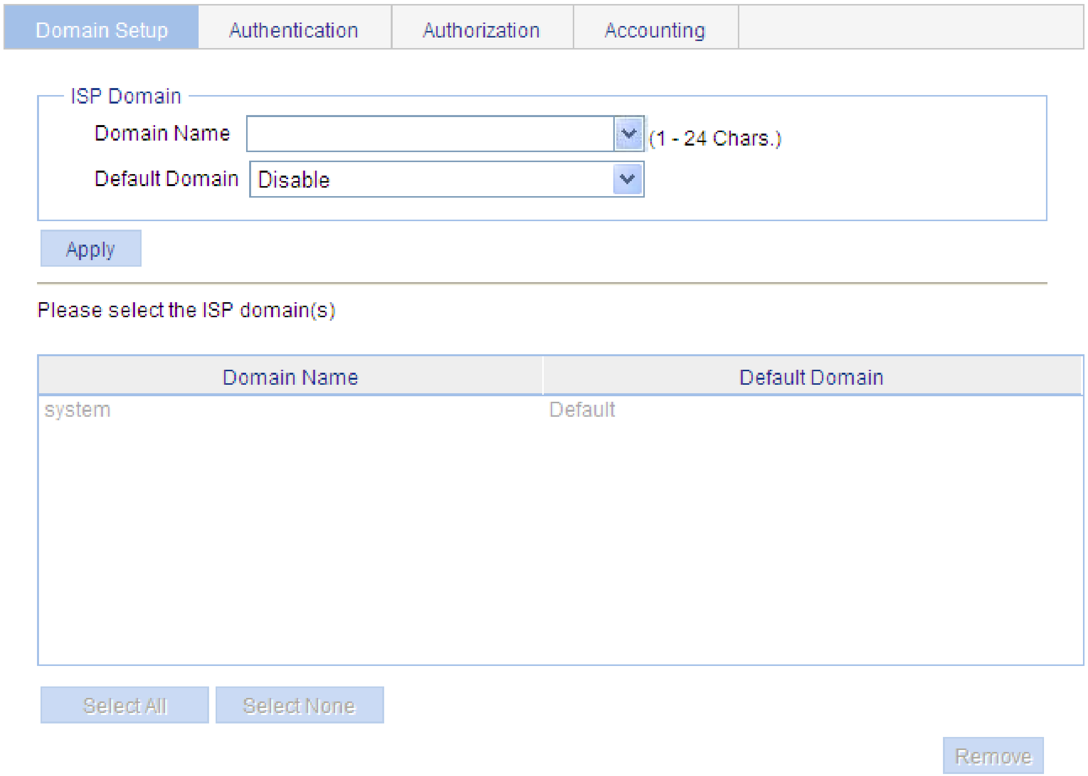
Table 1-1 AAA configuration task list

Task	Remarks	
Configuring an ISP Domain	Optional Create ISP domains and specify one of them as the default ISP domain. By default, there is an ISP domain named **system**, which is the default ISP domain.	
Configuring Authentication Methods for the ISP Domain	Optional Configure authentication methods for various types of users. By default, all types of users use local authentication.	AAA user types include LAN access users (such as 802.1X authentication users and MAC authentication users), login users (such as SSH, Telnet, FTP, terminal access users), and Command users.
Configuring Authorization Methods for the ISP Domain	Optional Specify the authorization methods for various types of users. By default, all types of users use local authorization.	
Configuring Accounting Methods for the ISP Domain	Required Specify the accounting methods for various types of users. By default, all types of users use local accounting.	

Configuring an ISP Domain

Select **Authentication** > **AAA** from the navigation tree. The **Domain Setup** page appears, as shown in Figure 1-2.

Figure 1-2 Domain Setup page



Domain Name (1 - 24 Chars.)

Default Domain: Disable

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

Table 1-2 describes the configuration items for creating an ISP domain.

Table 1-2 ISP domain configuration items

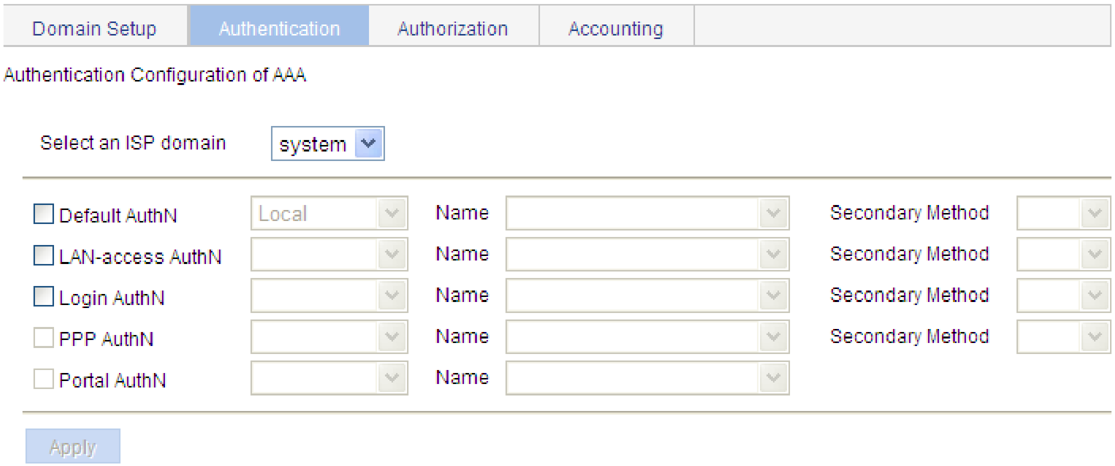
Item	Description
Domain Name	Type the ISP domain name, which is for identifying the domain. You can type a new domain name to create a domain, or specify an existing domain to change its status (whether it is the default domain).
Default Domain	Specify whether to use the ISP domain as the default domain. • Enable: Uses the domain as the default domain. • Disable: Uses the domain as a non-default domain. There can only be one default domain at a time. If you specify a second domain as the default domain, the original default domain will become a non-default domain.

Return to Configuration Task List.

Configuring Authentication Methods for the ISP Domain

Select **Authentication** > **AAA** from the navigation tree and then select the **Authentication** tab to enter the authentication method configuration page, as shown in Figure 1-3.

Figure 1-3 Authentication method configuration page



Authentication Configuration of AAA

Select an ISP domain: system

□ Default AuthN	Local	Name		Secondary Method	
□ LAN-access AuthN		Name		Secondary Method	
□ Login AuthN		Name		Secondary Method	
□ PPP AuthN		Name		Secondary Method	
□ Portal AuthN		Name			

Table 1-3 describes the configuration items for specifying the authentication methods for an ISP domain.

Table 1-3 Authentication method configuration items

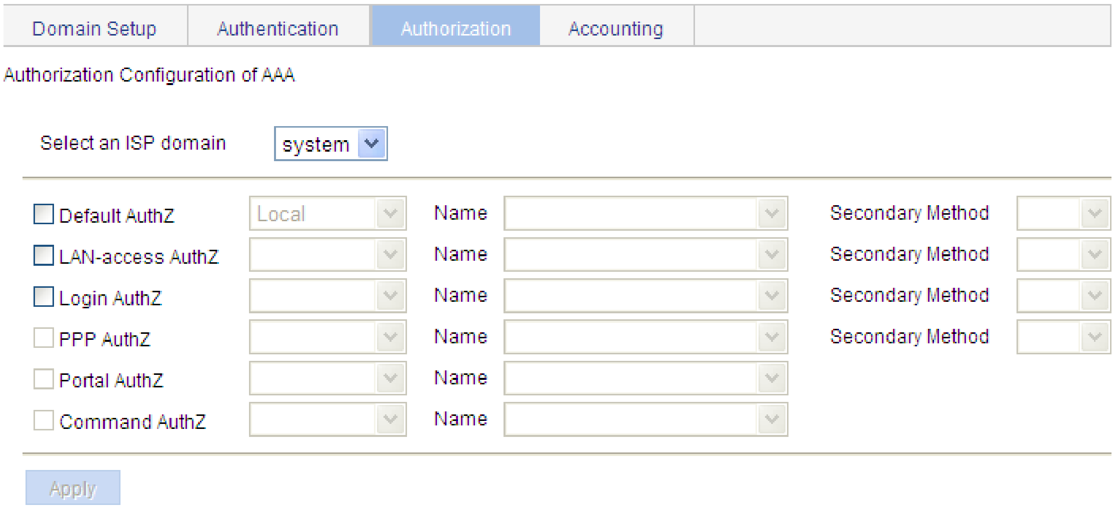
Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthN	Configure the default authentication method and secondary authentication method for all types of users. Options include: • Local: Performs local authentication. • None: All users are trusted and no authentication is performed. Generally, this mode is not recommended. • RADIUS: Performs RADIUS authentication. You need to specify the RADIUS scheme to be used. • Not Set: Restore the default, that is, local authentication.
Name	
Secondary Method	
LAN-access AuthN	Configure the authentication method and secondary authentication method for LAN access users. Options include: • Local: Performs local authentication. • None: All users are trusted and no authentication is performed. Generally, this mode is not recommended. • RADIUS: Performs RADIUS authentication. You need to specify the RADIUS scheme to be used. • Not Set: Uses the default authentication methods.
Name	
Secondary Method	
Login AuthN	Configure the authentication method and secondary authentication method for login users. Options include: • Local: Performs local authentication. • None: All users are trusted and no authentication is performed. Generally, this mode is not recommended. • RADIUS: Performs RADIUS authentication. You need to specify the RADIUS scheme to be used. • Not Set: Uses the default authentication methods.
Name	
Secondary Method	

Return to Configuration Task List.

Configuring Authorization Methods for the ISP Domain

Select **Authentication** > **AAA** from the navigation tree and then select the **Authorization** tab to enter the authorization method configuration page, as shown in Figure 1-4.

Figure 1-4 Authorization method configuration page



Domain Setup | Authentication | Authorization | Accounting

Authorization Configuration of AAA

Select an ISP domain: system

□ Default AuthZ	Local	Name		Secondary Method	
□ LAN-access AuthZ		Name		Secondary Method	
□ Login AuthZ		Name		Secondary Method	
□ PPP AuthZ		Name		Secondary Method	
□ Portal AuthZ		Name			
□ Command AuthZ		Name			

Table 1-4 describes the configuration items for configuring the authorization methods for an ISP domain.

Table 1-4 Authorization method configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthZ	Configure the default authorization method and secondary authorization method for all types of users. Options include: • Local: Performs local authorization. • None: All users are trusted and authorized. A user gets the corresponding default rights of the system. • RADIUS: Performs RADIUS authorization. You need to specify the RADIUS scheme to be used. • Not Set: Restore the default, that is, local authorization.
Name	
Secondary Method	
LAN-access AuthZ	Configure the authorization method and secondary authorization method for LAN access users. Options include: • Local: Performs local authorization. • None: All users are trusted and authorized. A user gets the corresponding default rights of the system. • RADIUS: Performs RADIUS authorization. You need to specify the RADIUS scheme to be used. • Not Set: Uses the default authorization methods.
Name	
Secondary Method	

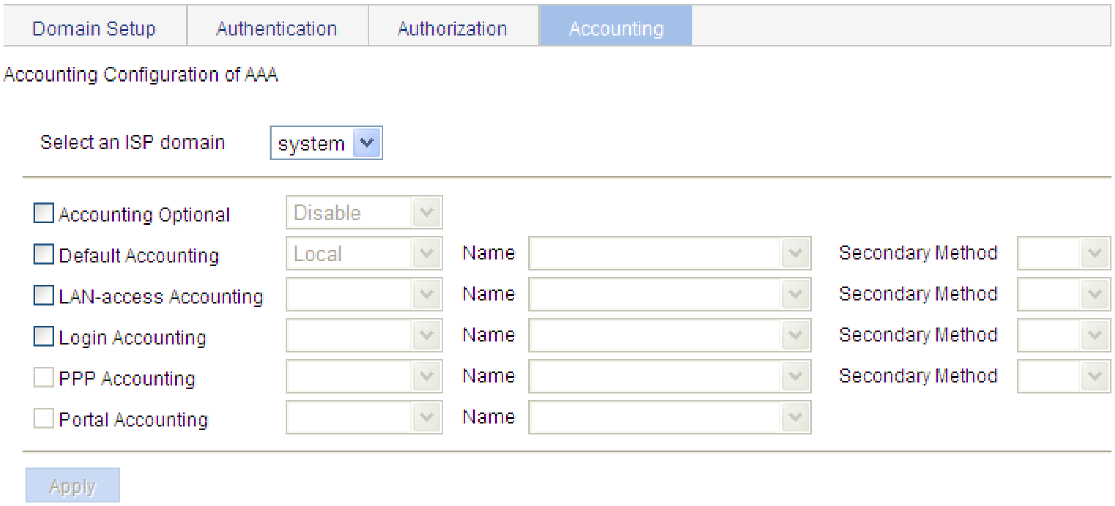
Item	Description
Login AuthZ	Configure the authorization method and secondary authorization method for login users. Options include: • Local: Performs local authorization. • None: All users are trusted and authorized. A user gets the corresponding default rights of the system. • RADIUS: Performs RADIUS authorization. You need to specify the RADIUS scheme to be used. • Not Set: Uses the default authorization methods.
Name	
Secondary Method	
Name	

Return to Configuration Task List.

Configuring Accounting Methods for the ISP Domain

Select **Authentication** > **AAA** from the navigation tree and then select the **Accounting** tab to enter the accounting method configuration page, as shown in Figure 1-5.

Figure 1-5 Accounting method configuration page



Accounting Configuration of AAA

Select an ISP domain: system

□ Accounting Optional	Disable				
□ Default Accounting	Local	Name		Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
□ Login Accounting		Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name			

Table 1-5 describes the configuration items for configuring the accounting methods for an ISP domain.

Table 1-5 Accounting method configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Accounting Optional	Specify whether to enable the accounting optional feature. • With the feature enabled, a user that will be disconnected otherwise can use the network resources even when there is no accounting server available or communication with the current accounting server fails. • If accounting for such a user fails, the device will not send real-time accounting updates for the user any more.
Default Accounting	Configure the default accounting method and secondary accounting method for all types of users. Options include: • Local: Performs local accounting.
Name	

Item	Description
Secondary Method	- None: Performs no accounting. - RADIUS: Performs RADIUS accounting. You need to specify the RADIUS scheme to be used. - Not Set: Restore the default, that is, local accounting.
LAN-access Accounting	Configure the accounting method and secondary accounting method for LAN access users. Options include: - Local: Performs local accounting. - None: Performs no accounting. - RADIUS: Performs RADIUS accounting. You need to specify the RADIUS scheme to be used. - Not Set: Uses the default accounting methods.
Name	
Secondary Method	
Login Accounting	Configure the accounting method and secondary accounting method for login users. Options include: - Local: Performs local accounting. - None: Performs no accounting. - RADIUS: Performs RADIUS accounting. You need to specify the RADIUS scheme to be used. - Not Set: Uses the default accounting methods.
Name	
Secondary Method	

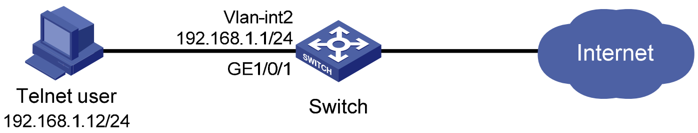
Return to Configuration Task List.

AAA Configuration Example

Network requirements

As shown in Figure 1-6, configure the switch to perform local authentication, authorization, and accounting for Telnet users.

Figure 1-6 Network diagram for AAA configuration example



Configuration procedure

Note

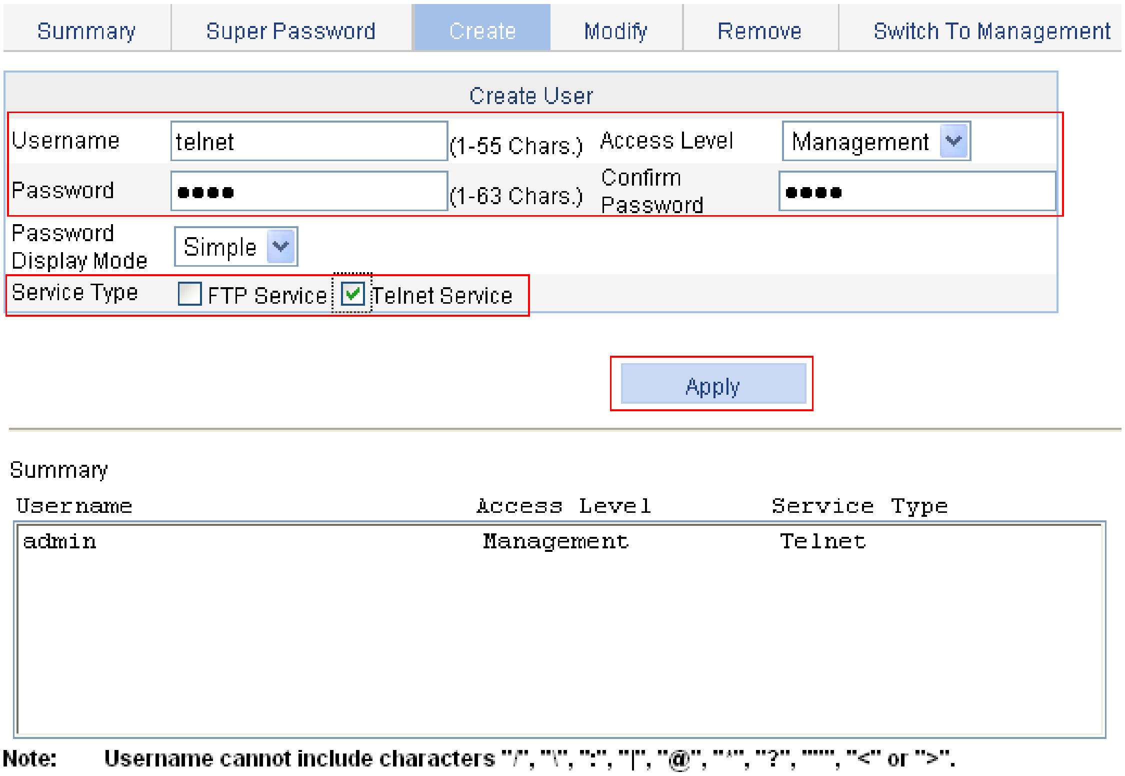
Enable the Telnet server function, and configure the switch to use AAA for Telnet users. The configuration steps are omitted.

# Configure IP addresses for the interfaces. (Omitted)

# Configure a local user.

- Select **Device** > **Users** from the navigation tree and then select the **Create** tab to configure a local user as shown in Figure 1-7.

Figure 1-7 Configure a local user



Username	telnet	(1-55 Chars.)	Access Level	Management
Password	●●●●	(1-63 Chars.)	Confirm Password	●●●●
Password Display Mode	Simple			
Service Type	□ FTP Service	☑ Telnet Service		

Summary

Username	Access Level	Service Type
admin	Management	Telnet

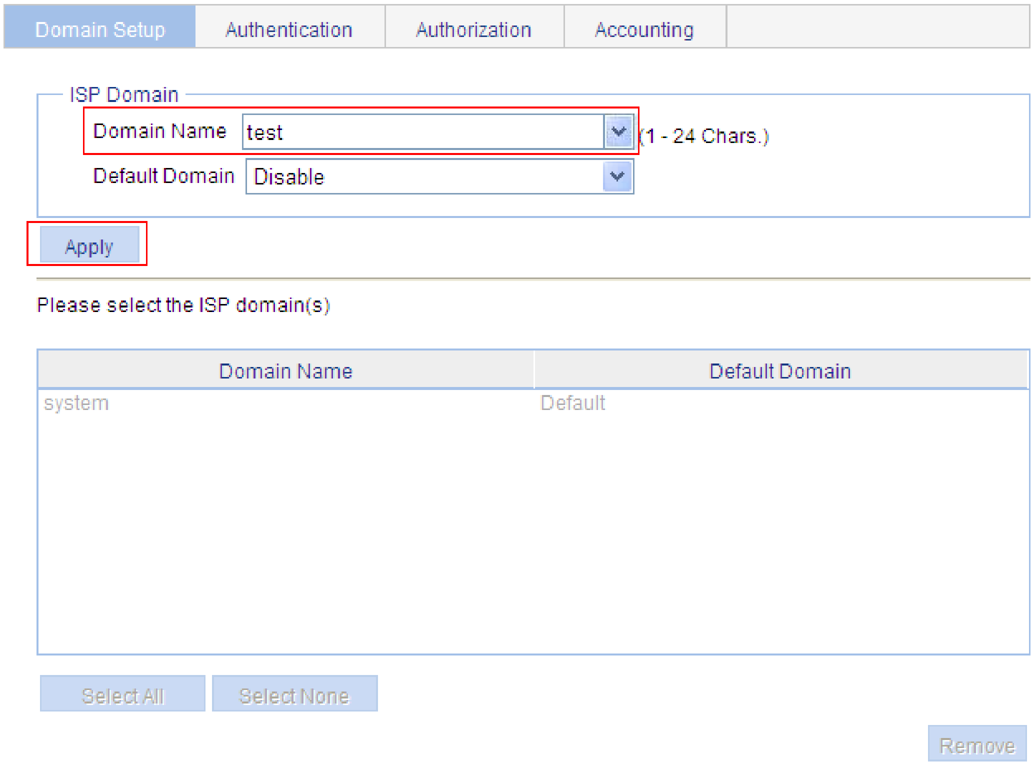
Note: Username cannot include characters "/", "\", ":", "|", "@", "*", "?", """", "<" or ">".

- Enter **telnet** as the username.
- Select **Management** as the access level.
- Enter **abcd** as the password.
- Enter **abcd** to confirm the password.
- Select **Telnet Service** as the service type.
- Click **Apply**.

# Configure ISP domain **test**.

- Select **Authentication** > **AAA** from the navigation tree. The domain configuration page appears. Perform the configurations shown in Figure 1-8.

Figure 1-8 Configure ISP domain test



ISP Domain

Domain Name: test (1 - 24 Chars.)

Default Domain: Disable

Please select the ISP domain(s)

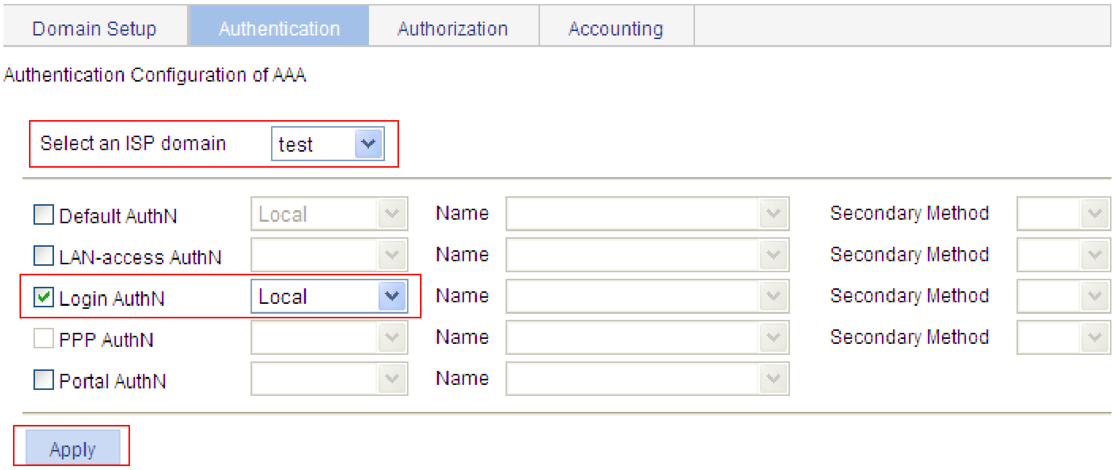
Domain Name	Default Domain
system	Default

- Enter **test** as the domain name.
- Click **Apply**.

# Configure the ISP domain to use local authentication.

- Select **Authentication** > **AAA** from the navigation tree and then select the **Authentication** tab and configure AAA authentication as shown in Figure 1-9.

Figure 1-9 Configure the ISP domain to use local authentication



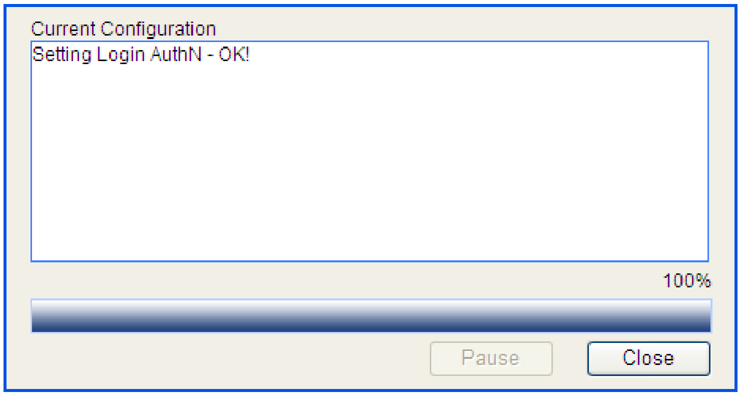
Authentication Configuration of AAA

Select an ISP domain: test

□ Default AuthN	Local	Name		Secondary Method	
□ LAN-access AuthN		Name		Secondary Method	
☑ Login AuthN	Local	Name		Secondary Method	
□ PPP AuthN		Name		Secondary Method	
□ Portal AuthN		Name			

- Select the domain **test**.
- Select the **Login AuthN** check box and select the authentication method **Local**.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-10.

Figure 1-10 Configuration progress dialog box



Current Configuration

Setting Login AuthN - OK!

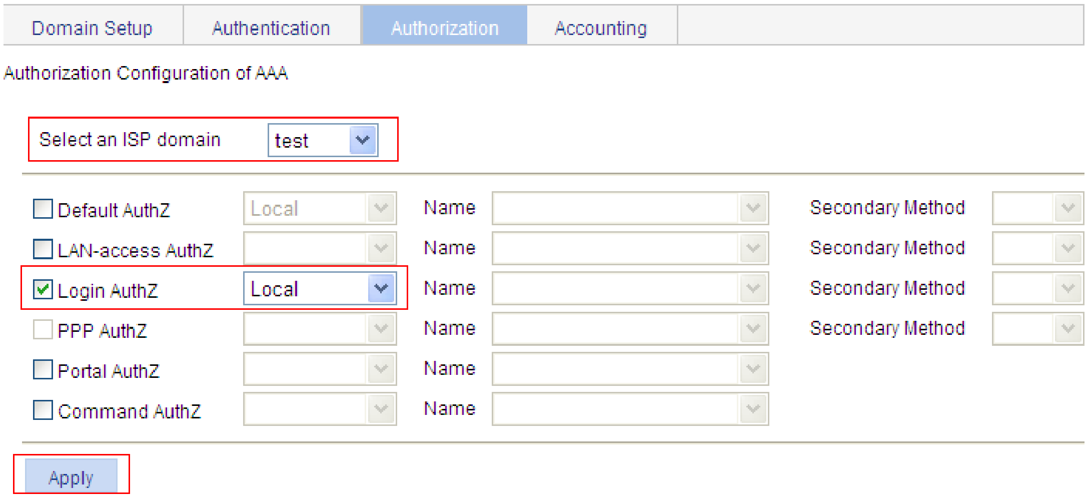
100%

- After the configuration process is complete, click **Close**.

# Configure the ISP domain to use local authorization.

- Select **Authentication** > **AAA** from the navigation tree and then select the **Authorization** tab and configure AAA authorization as shown in Figure 1-11.

Figure 1-11 Configure the ISP domain to use local authorization



Authorization Configuration of AAA

Select an ISP domain: test

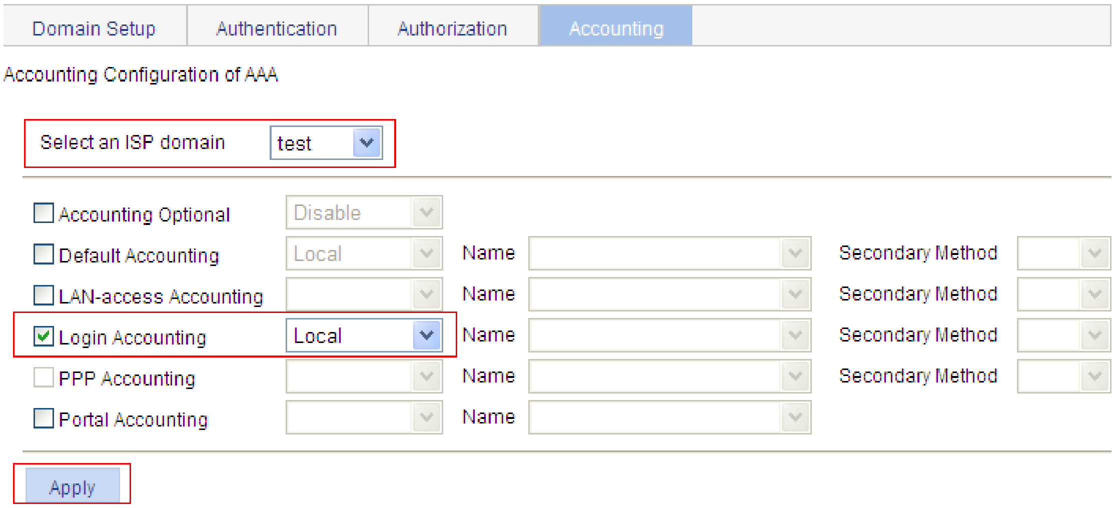
□ Default AuthZ	Local	Name		Secondary Method	
□ LAN-access AuthZ		Name		Secondary Method	
☑ Login AuthZ	Local	Name		Secondary Method	
□ PPP AuthZ		Name		Secondary Method	
□ Portal AuthZ		Name			
□ Command AuthZ		Name			

- Select the domain **test**.
- Select the **Login AuthZ** check box and select the authorization method **Local**.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration progress is complete, click **Close**.

# Configure the ISP domain to use local accounting.

- Select **Authentication** > **AAA** from the navigation tree and then select the **Accounting** tab and configure AAA accounting as shown in Figure 1-12.

Figure 1-12 Configure the ISP domain to use local accounting



Accounting Configuration of AAA

Select an ISP domain: test

□ Accounting Optional	Disable				
□ Default Accounting	Local	Name		Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
☑ Login Accounting	Local	Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name			

- Select the domain **test**.
- Select the **Login Accounting** check box and select the accounting method **Local**.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Now, if you telnet to the switch and enter username **telnet@test** and password **abcd**, you should be serviced as a user in domain **test**.

Table of Contents

1 RADIUS

Overview

Remote Authentication Dial-In User Service (RADIUS) is protocol for implementing Authentication, Authorization, and Accounting (AAA). For details about AAA, refer to *AAA Configuration*.

Introduction to RADIUS

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

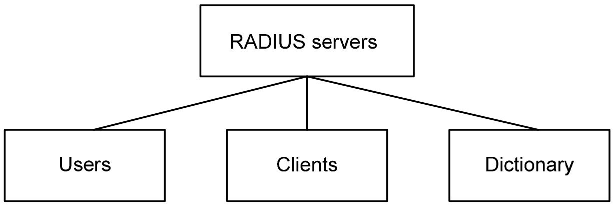
RADIUS was originally designed for dial-in user access. With the diversification of access methods, RADIUS has been extended to support more access methods, for example, Ethernet access and ADSL access. It uses authentication and authorization in providing access services and uses accounting to collect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

Client/Server Model

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

In general, the RADIUS server maintains three databases, namely, Users, Clients, and Dictionary, as shown in Figure 1-1.

Figure 1-1 RADIUS server components



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

Security and Authentication Mechanisms

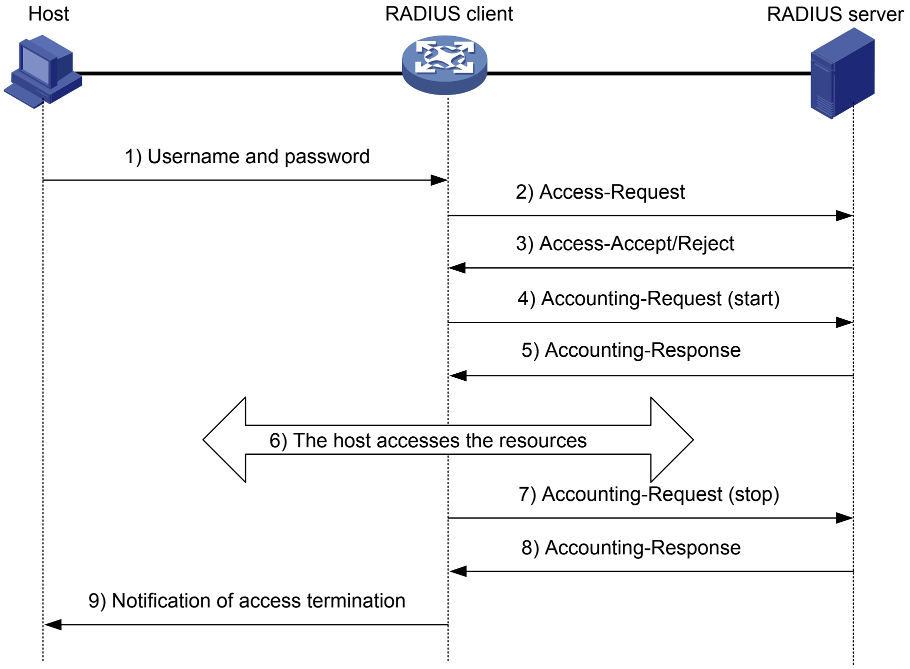
Information exchanged between a RADIUS client and the RADIUS server is authenticated with a shared key, which is never transmitted over the network. This enhances the information exchange security. In addition, to prevent user passwords from being intercepted on insecure networks, RADIUS encrypts passwords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

A RADIUS server supports multiple user authentication methods. Moreover, a RADIUS server can act as the client of another AAA server to provide authentication proxy services.

Basic Message Exchange Process of RADIUS

Figure 1-2 illustrates the interaction of the host, the RADIUS client, and the RADIUS server.

Figure 1-2 Basic message exchange process of RADIUS



The following is how RADIUS operates:

1) The host initiates a connection request carrying the username and password to the RADIUS client.
2) Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.
3) The RADIUS server authenticates the username and password. If the authentication succeeds, it sends back an Access-Accept message containing the user's authorization information. If the authentication fails, it returns an Access-Reject message.
4) The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.
5) The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.
6) The user accesses the network resources.
7) The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.

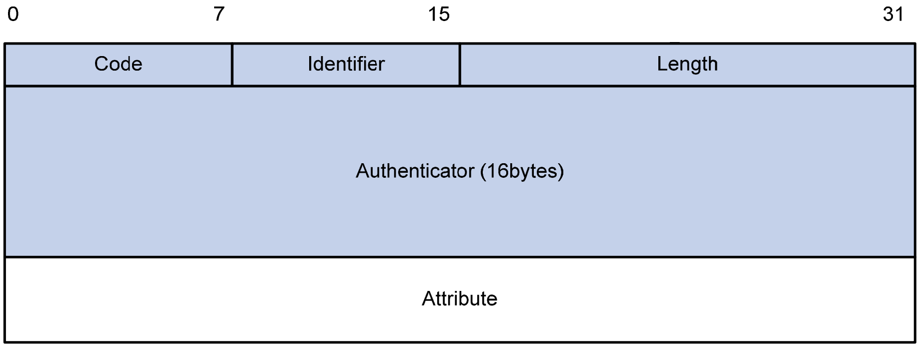
8) The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.

9) The user stops access to network resources.

RADIUS Packet Format

RADIUS uses UDP to transmit messages. It ensures the smooth message exchange between the RADIUS server and the client through a series of mechanisms, including the timer management mechanism, retransmission mechanism, and slave server mechanism. Figure 1-3 shows the RADIUS packet format.

Figure 1-3 RADIUS packet format



Descriptions of the fields are as follows:

1) The Code field (1-byte long) is for indicating the type of the RADIUS packet. Table 1-1 gives the possible values and their meanings.

Table 1-1 Main values of the Code field

Code	Packet type	Description
1	Access-Request	From the client to the server. A packet of this type carries user information for the server to authenticate the user. It must contain the User-Name attribute and can optionally contain the attributes of NAS-IP-Address, User-Password, and NAS-Port.
2	Access-Accept	From the server to the client. If all the attribute values carried in the Access-Request are acceptable, that is, the authentication succeeds, the server sends an Access-Accept response.
3	Access-Reject	From the server to the client. If any attribute value carried in the Access-Request is unacceptable, the server rejects the user and sends an Access-Reject response.
4	Accounting-Request	From the client to the server. A packet of this type carries user information for the server to start/stop accounting for the user. It contains the Acct-Status-Type attribute, which indicates whether the server is requested to start the accounting or to end the accounting.
5	Accounting-Response	From the server to the client. The server sends to the client a packet of this type to notify that it has received the Accounting-Request and has correctly started recording the accounting information.

2) The Identifier field (1-byte long) is for matching request packets and response packets and detecting retransmitted request packets. The request and response packets of the same type have the same identifier.

3) The Length field (2-byte long) indicates the length of the entire packet, including the Code, Identifier, Length, Authenticator, and Attribute fields. The value of the field is in the range 20 to 4096. Bytes beyond the length are considered the padding and are neglected upon reception. If the length of a received packet is less than that indicated by the Length field, the packet is dropped.

4) The Authenticator field (16-byte long) is used to authenticate replies from the RADIUS server, and is also used in the password hiding algorithm. There are two kinds of authenticators: request authenticator and response authenticator.

5) The Attribute field, with a variable length, carries the specific authentication, authorization, and accounting information for defining configuration details of the request or response. This field is represented in triplets of Type, Length, and Value.

- Type: One byte, in the range 1 to 255. It indicates the type of the attribute. Commonly used attributes for RADIUS authentication, authorization and accounting are listed in Table 1-2.
- Length: One byte for indicating the length of the attribute in bytes, including the Type, Length, and Value fields.
- Value: Value of the attribute, up to 253 bytes. Its format and content depend on the Type and Length fields.

Table 1-2 RADIUS attributes

No.	Attribute	No.	Attribute
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply_Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint

No.	Attribute	No.	Attribute
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

Note

The attribute types listed in Table 1-2 are defined by RFC 2865, RFC 2866, RFC 2867, and RFC 2868.

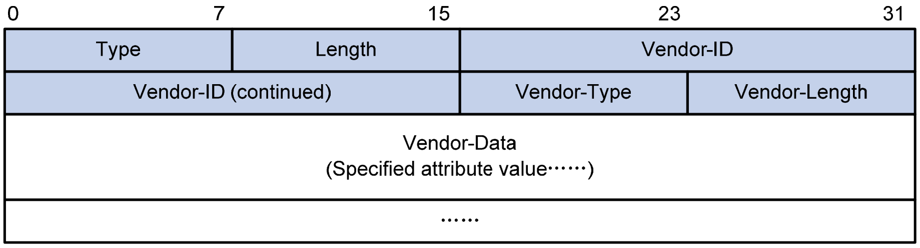
Extended RADIUS Attributes

The RADIUS protocol features excellent extensibility. Attribute 26 (Vender-Specific) defined by RFC 2865 allows a vender to define extended attributes to implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple type-length-value (TLV) sub-attributes in RADIUS packets for extension in applications. As shown in Figure 1-4, a sub-attribute that can be encapsulated in Attribute 26 consists of the following four parts:

- Vendor-ID (four bytes): Indicates the ID of the vendor. Its most significant byte is 0 and the other three bytes contain a code complying with RFC 1700.
- Vendor-Type: Indicates the type of the sub-attribute.
- Vendor-Length: Indicates the length of the sub-attribute.
- Vendor-Data: Indicates the contents of the sub-attribute.

Figure 1-4 Segment of a RADIUS packet containing an extended attribute



Protocols and Standards

The protocols and standards related to RADIUS include:

- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support
- RFC 2869: RADIUS Extensions

Configuring RADIUS

Configuration Task List

Note

- The RADIUS scheme configured through the Web interface is named **system**.
- If there is no RADIUS scheme named **system** in the system, when you select **Authentication** > **RADIUS** to enter the RADIUS module, a scheme named **system** will be created automatically.

Table 1-3 lists the RADIUS configuration steps.

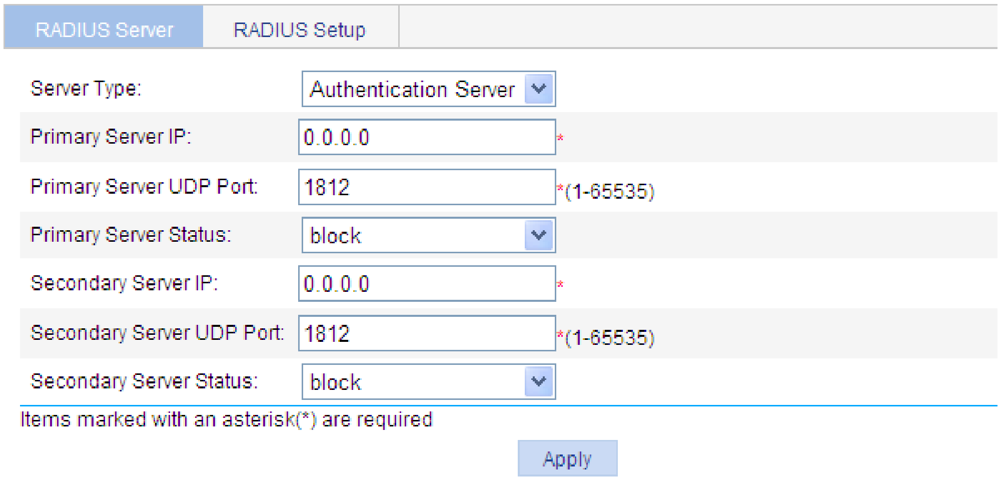
Table 1-3 RADIUS configuration task list

Task	Description	
Configuring RADIUS Authentication Servers	Required Configure the information related to the primary and secondary RADIUS authentication servers. By default, no RADIUS authentication server is configured.	For configuration details, refer to Configuring RADIUS Servers.
Configuring RADIUS Accounting Servers	Optional Configure the information related to the primary and secondary RADIUS accounting servers. By default, no RADIUS accounting server is configured.	
Configuring RADIUS Parameters	Required Configure the parameters that are necessary for information exchange between the device and RADIUS servers.	

Configuring RADIUS Servers

From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears, as shown in Figure 1-5.

Figure 1-5 RADIUS server configuration



Server Type: Authentication Server

Primary Server IP: 0.0.0.0 *

Primary Server UDP Port: 1812 *(1-65535)

Primary Server Status: block

Secondary Server IP: 0.0.0.0 *

Secondary Server UDP Port: 1812 *(1-65535)

Secondary Server Status: block

Items marked with an asterisk(*) are required

Table 1-4 lists the RADIUS server configuration items.

Table 1-4 RADIUS server configuration

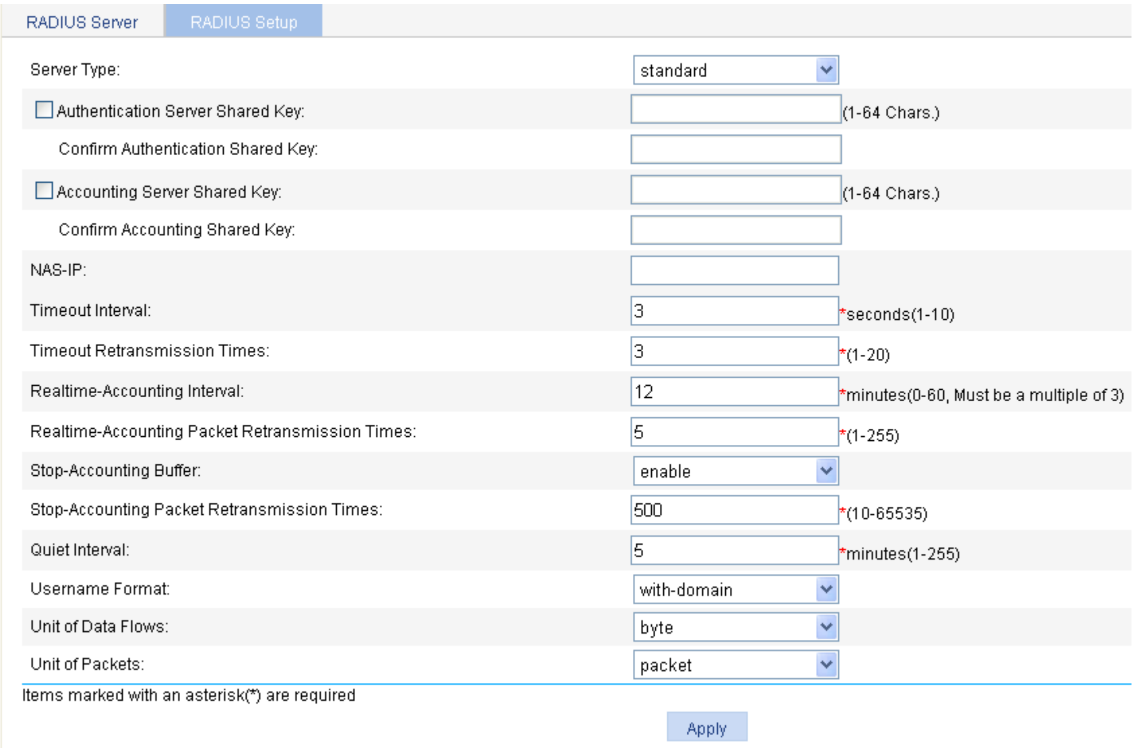
Item	Description
Server Type	Specify the type of the server to be configured, which can be Authentication Server and Accounting Sever.
Primary Server IP	Specify the IP address of the primary server. If no primary server is specified, the text box displays 0.0.0.0. To remove the previously configured primary server, enter 0.0.0.0 in the text box. The specified IP address of the primary server cannot be the same as that of the secondary server.
Primary Server UDP Port	Specify the UDP port of the primary server. If the IP address of the primary server is not specified or the specified IP address is to be removed, the port number is 1812 for authentication or 1813 for accounting.
Primary Server Status	Set the status of the primary server, including: ● active: The server is working normally. ● blocked: The server is down. If the IP address of the primary server is not specified or the specified IP address is to be removed, the status is blocked.
Secondary Server IP	Specify the IP address of the secondary server. If no secondary server is specified, the text box displays 0.0.0.0. To remove the previously configured secondary server, enter 0.0.0.0 in the text box. The specified IP address of the secondary server cannot be the same as that of the primary server.
Secondary Server UDP Port	Specify the UDP port of the secondary server. If the IP address of the secondary server is not specified or the specified IP address is to be removed, the port number is 1812 for authentication or 1813 for accounting.
Secondary Server Status	Status of the secondary server, including: ● active: The server is working normally. ● blocked: The server is down. If the IP address of the secondary server is not specified or the specified IP address is to be removed, the status is blocked.

Return to RADIUS configuration task list.

Configuring RADIUS Parameters

From the navigation tree, select **Authentication** > **RADIUS** and then select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page, as shown in Figure 1-6.

Figure 1-6 RADIUS parameter configuration



Server Type:	standard	
□ Authentication Server Shared Key:		(1-64 Chars.)
Confirm Authentication Shared Key:		
□ Accounting Server Shared Key:		(1-64 Chars.)
Confirm Accounting Shared Key:		
NAS-IP:		
Timeout Interval:	3	*seconds(1-10)
Timeout Retransmission Times:	3	*(1-20)
Realtime-Accounting Interval:	12	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	with-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	

Items marked with an asterisk(*) are required

Table 1-5 lists the RADIUS parameters.

Table 1-5 RADIUS parameters

Item	Description
Server Type	Specify the type of the RADIUS server supported by the device, including: • extended: Specifies an extended RADIUS server (usually an iMC server). That is, the RADIUS client (the device) and RADIUS server communicate using the proprietary RADIUS protocol and packet format. • standard: Specifies a standard RADIUS server. That is, the RADIUS client (the device) and RADIUS server communicate using the standard RADIUS protocol and packet format defined in RFC 2138/2139 or later.
Authentication Server Shared Key	Specify and confirm the shared key for the authentication server. These two parameters must have the same values.
Confirm Authentication Shared Key	
Accounting Server Shared Key	Specify and confirm the shared key for the accounting server. These two parameters must have the same values.
Confirm Accounting Shared Key	
NAS-IP	Specify the source IP address for the device to use in RADIUS packets to be sent to the RADIUS server. It is recommended to use a loopback interface address instead of a physical interface address as the source IP address, because if the physical interface is down, the response packets from the server cannot reach the device.
Timeout Interval	Set the RADIUS server response timeout.

Item	Description
Timeout Retransmission Times	Set the maximum number of transmission attempts. The product of the timeout value and the number of retransmission attempts cannot exceed 75.
Realtime-Accounting Interval	Set the real-time accounting interval, whose value must be n times 3 (n is an integer). To implement real-time accounting on users, it is necessary to set the real-time accounting interval. After this parameter is specified, the device will send the accounting information of online users to the RADIUS server every the specified interval. The value of the real-time accounting interval is related to the requirement on the performance of the NAS and RADIUS server. The smaller the value, the higher the requirement. It is recommended to set a large value if the number of users is equal to or larger than 1000. Table 1-6 shows the relationship between the interval value and the number of users.
Realtime-Accounting Packet Retransmission Times	Set the maximum number of real-time accounting request retransmission times.
Stop-Accounting Buffer	Enable or disable buffering stop-accounting requests without responses in the device.
Stop-Accounting Packet Retransmission Times	Set the maximum number of transmission attempts if no response is received for the stop-accounting packet.
Quiet Interval	Specify the interval the primary server has to wait before being active
Username Format	Set the format of username sent to the RADIUS server. A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. If a RADIUS server does not accept a username including an ISP domain name, you can configure the device to remove the domain name of a username before sending it to the RADIUS server. without-domain: Specifies to remove the domain name of a username that is to be sent to the RADIUS server. with-domain: Specifies to keep the domain name of a username that is to be sent to the RADIUS server.
Unit of Data Flows	Specify the unit for data flows sent to the RADIUS server, which can be: ● byte ● kilo-byte ● mega-byte ● giga-byte
Unit of Packets	Specify the unit for data packets sent to the RADIUS server, which can be: ● one-packet ● kilo-packet ● mega-packet ● giga-packet

Table 1-6 Relationship between the real-time accounting interval and the number of users

Number of users	Real-time accounting interval (in minutes)
1 to 99	3
100 to 499	6
500 to 999	12
⩾1000	⩾15

Return to RADIUS configuration task list.

RADIUS Configuration Example

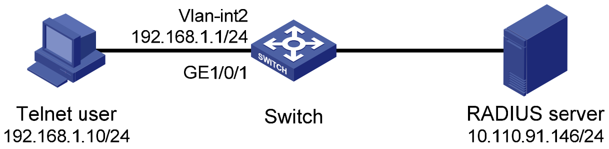
Network requirements

As shown in Figure 1-7, it is required to configure the switch to let the RADIUS server assign an IP address to the Telnet user and authenticate and keep accounts on the user (record the online duration of the Telnet user).

On the RADIUS server (an iMC server, using the default port for authentication and accounting), the Telnet user's username and password and the shared key **expert** have been configured for packet exchange with the switch.

On the switch, it is required to configure the shared key for packet exchange with the RADIUS server as **expert**, and configure the system to remove the domain name of a username before sending it to the RADIUS server.

Figure 1-7 Network diagram for RADIUS server configuration



Configuration procedure

Note

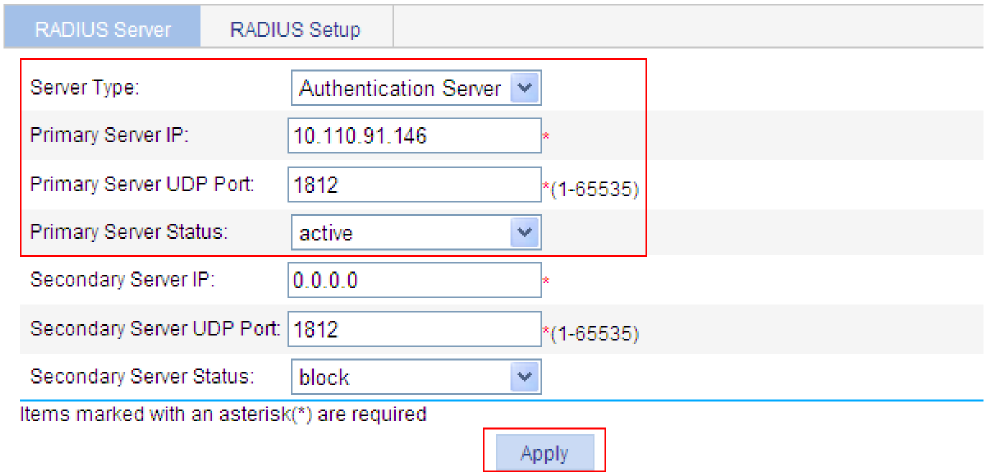
Enable the Telnet server function, and configure the switch to use AAA for authentication, authorization and accounting of Telnet users. (Omitted)

1) Configure IP addresses for the interfaces. (Omitted)
2) Configure RADIUS scheme **system**

# Configure the RADIUS authentication server.

- From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears.

Figure 1-8 Configure the RADIUS authentication server



Server Type: Authentication Server

Primary Server IP: 10.110.91.146 *

Primary Server UDP Port: 1812 *(1-65535)

Primary Server Status: active

Secondary Server IP: 0.0.0.0 *

Secondary Server UDP Port: 1812 *(1-65535)

Secondary Server Status: block

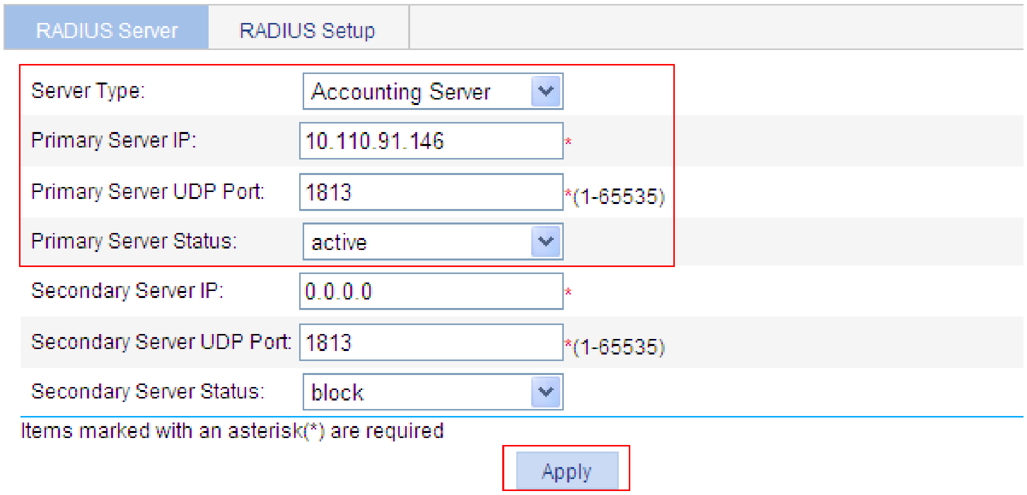
Items marked with an asterisk(*) are required

Perform the following configurations, as shown in Figure 1-8.

- Select **Authentication Server** as the server type.
- Enter **10.110.91.146** as the IP address of the primary authentication server
- Enter **1812** as the UDP port of the primary authentication server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the RADIUS accounting server.

Figure 1-9 Configure the RADIUS accounting server



Server Type: Accounting Server

Primary Server IP: 10.110.91.146 *

Primary Server UDP Port: 1813 *(1-65535)

Primary Server Status: active

Secondary Server IP: 0.0.0.0 *

Secondary Server UDP Port: 1813 *(1-65535)

Secondary Server Status: block

Items marked with an asterisk(*) are required

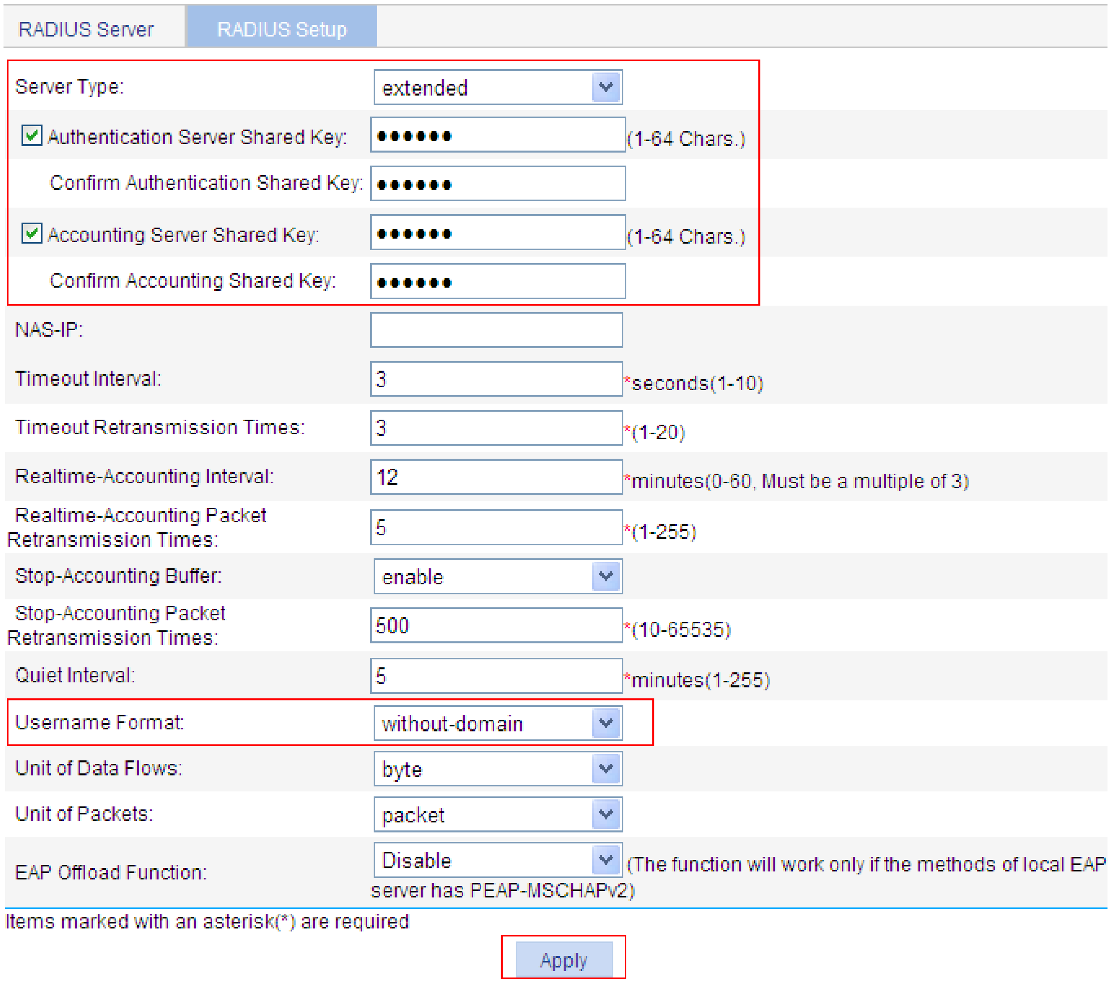
Perform the following configurations, as shown in Figure 1-9.

- Select **Accounting Server** as the server type.
- Enter **10.110.91.146** as the IP address of the primary accounting server.
- Enter **1813** as the UDP port of the primary accounting server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the parameters for communication between the switch and the RADIUS servers.

- Select the **RADIUS Setup** tab and perform the following configurations, as shown in Figure 1-10.

Figure 1-10 Configure RADIUS parameters



Server Type:	extended	
☑ Authentication Server Shared Key:	••••••	(1-64 Chars.)
Confirm Authentication Shared Key:	••••••	
☑ Accounting Server Shared Key:	••••••	(1-64 Chars.)
Confirm Accounting Shared Key:	••••••	
NAS-IP:		
Timeout Interval:	3	*seconds(1-10)
Timeout Retransmission Times:	3	*(1-20)
Realtime-Accounting Interval:	12	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	without-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	
EAP Offload Function:	Disable	(The function will work only if the methods of local EAP server has PEAP-MSCHAPv2)

Items marked with an asterisk(*) are required

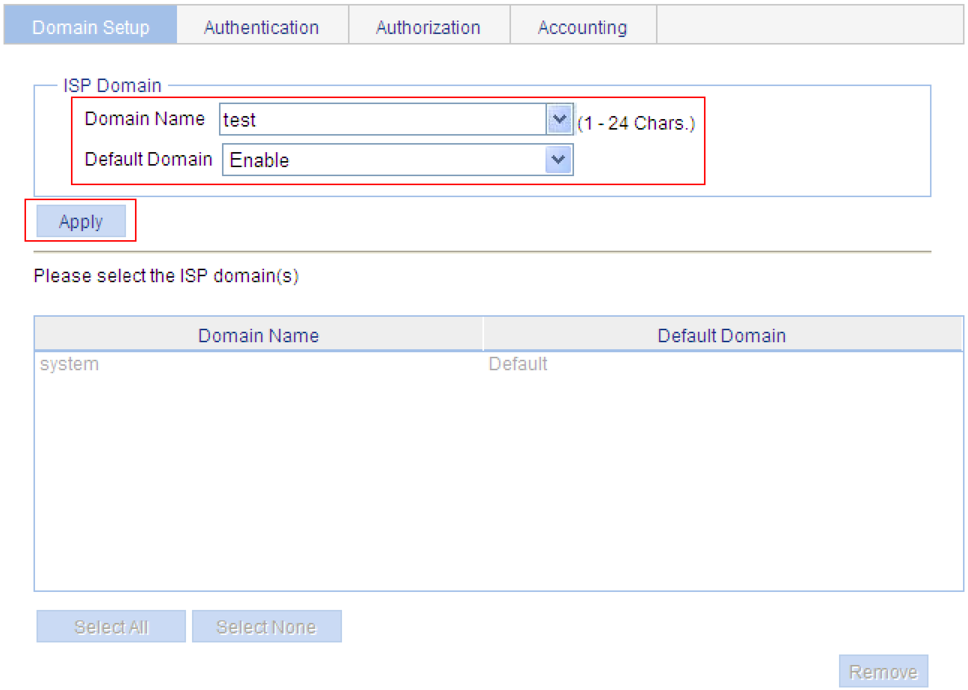
- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Authentication Shared Key** text box.
- Select the **Accounting Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Accounting Shared Key** text box.
- Select **without-domain** for **Username Format**.
- Click **Apply**

3) Configure AAA

# Create an ISP domain.

- From the navigation tree, select **Authentication** > **AAA.** The domain setup page appears.

Figure 1-11 Create an ISP domain



Domain Setup | Authentication | Authorization | Accounting

ISP Domain

Domain Name: test (1 - 24 Chars.)

Default Domain: Enable

Apply

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

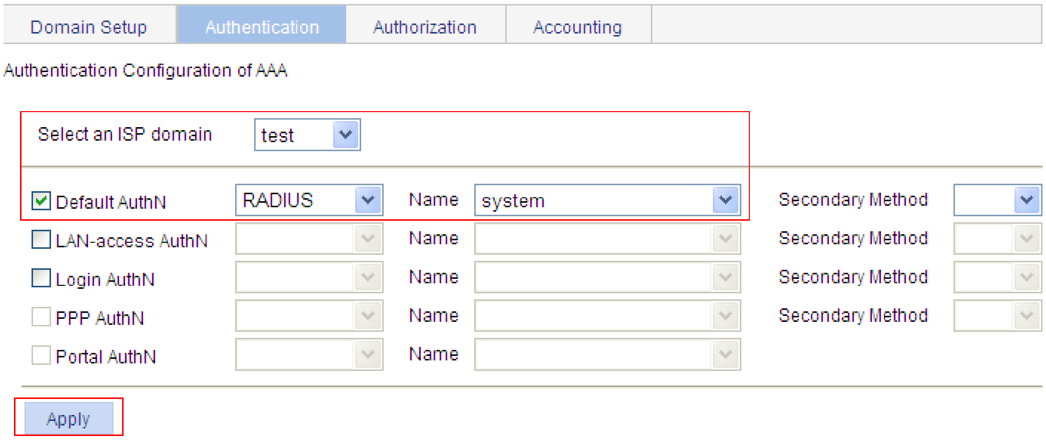
Perform the following configurations, as shown in Figure 1-11.

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain as the default domain.
- Click **Apply**.

# Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab.

Figure 1-12 Configure the AAA authentication method for the ISP domain



Domain Setup | Authentication | Authorization | Accounting

Authentication Configuration of AAA

Select an ISP domain: test

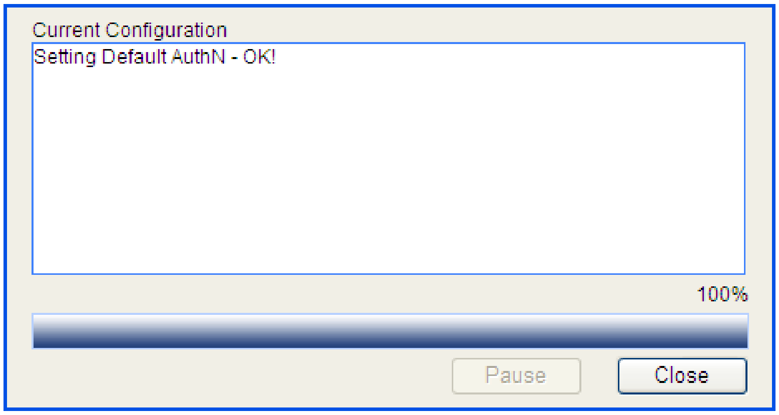
☑ Default AuthN	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthN		Name		Secondary Method	
□ Login AuthN		Name		Secondary Method	
□ PPP AuthN		Name		Secondary Method	
□ Portal AuthN		Name			

Apply

Perform the following configurations, as shown in Figure 1-12.

- Select the domain name **test**.
- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 1-13.

Figure 1-13 Configuration progress dialog box



Current Configuration

Setting Default AuthN - OK!

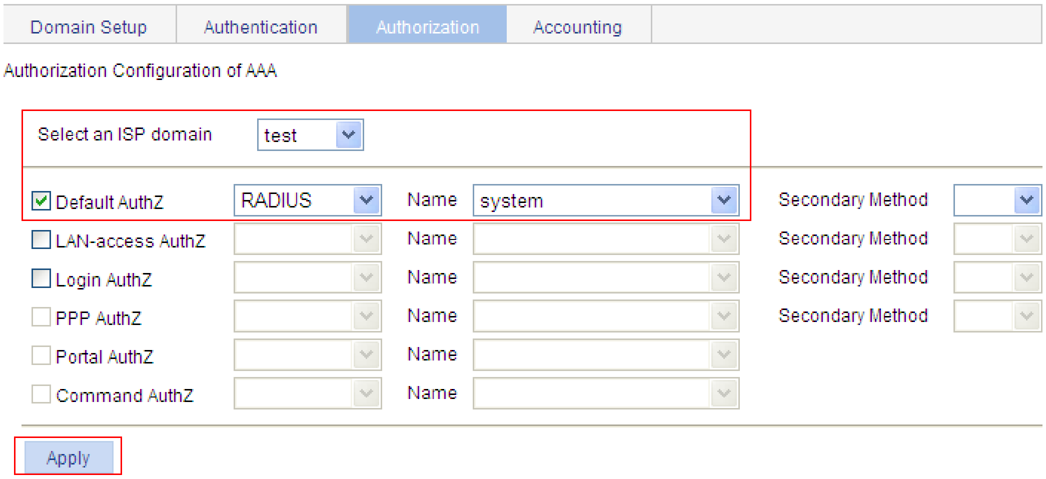
100%

- After the configuration process is complete, click **Close**.

# Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab.

Figure 1-14 Configure the AAA authorization method for the ISP domain



Authorization Configuration of AAA

Select an ISP domain: test

☑ Default AuthZ	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthZ		Name		Secondary Method	
□ Login AuthZ		Name		Secondary Method	
□ PPP AuthZ		Name		Secondary Method	
□ Portal AuthZ		Name			
□ Command AuthZ		Name			

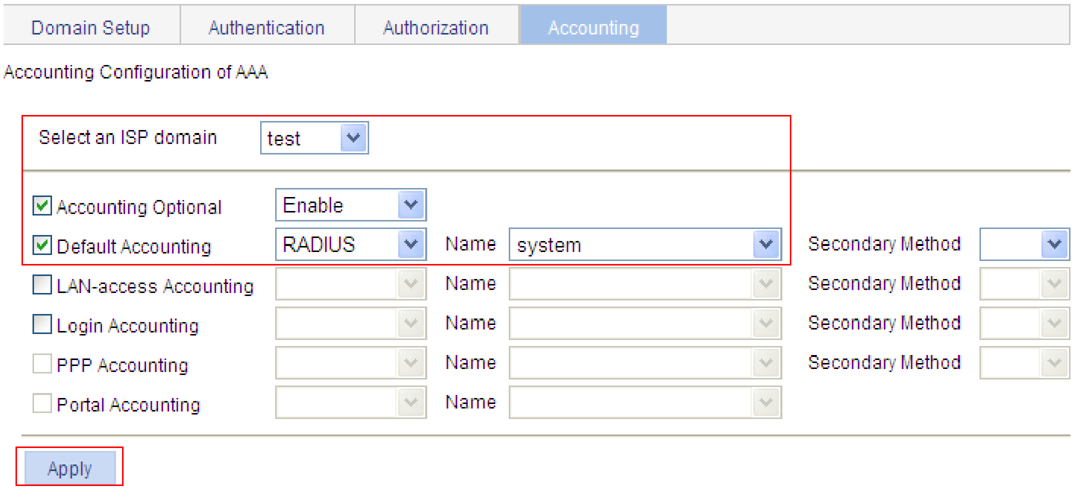
Perform the following configurations, as shown in Figure 1-14.

- Select the domain name **test**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA accounting method for the ISP domain, and enable accounting optional.

- Select the **Accounting** tab.

Figure 1-15 Configure the AAA accounting method for the ISP domain



Accounting Configuration of AAA

Select an ISP domain: test

☑ Accounting Optional	Enable				
☑ Default Accounting	RADIUS	Name	system	Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
□ Login Accounting		Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name			

Perform the following configurations, as shown in Figure 1-15.

- Select the domain name **test**.
- Select the **Accounting Optional** checkbox and then select **Enable**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Configuration Guidelines

When configuring the RADIUS client, note that:

1) When you modify the parameters of the RADIUS scheme, the system does not check whether the scheme is being used by users.
2) After accounting starts, update-accounting and stop-accounting packets will be sent to the designated server, and no primary/secondary server switchover will take place even if the designated server fails. Such a switchover can take place only during AAA session establishment.
3) If an AAA server has active TCP connections, it cannot be removed.
4) RADIUS does not support accounting for FTP users.
5) If the iMC server is used as the RADIUS server, it is necessary to configure accounting as optional for users in the ISP domain because the iMC server does not respond to accounting packets.

Table of Contents

1 Users

Overview

This module allows you to configure local users and user groups.

Local user

A local user represents a set of user attributes configured on a device (such as the user password, service type, and authorization attribute), and is uniquely identified by the username. For a user requesting a network service to pass local authentication, you must add an entry as required in the local user database of the device. For details about local authentication, refer to *AAA Configuration*.

User group

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. All local users in a user group inherit the user attributes of the group, but if you configure user attributes for a local user, the settings of the local user take precedence over the settings for the user group.

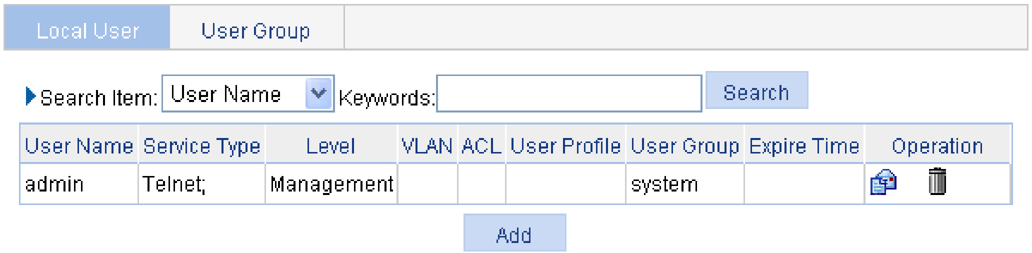
By default, every newly added local user belongs to a user group named system, which is automatically created by the system.

Configuring Users

Configuring a Local User

Select **Authentication** > **Users** from the navigation tree. The **Local User** page appears, displaying all local users, as shown in Figure 1-1. Click **Add** to enter the local user configuration page.

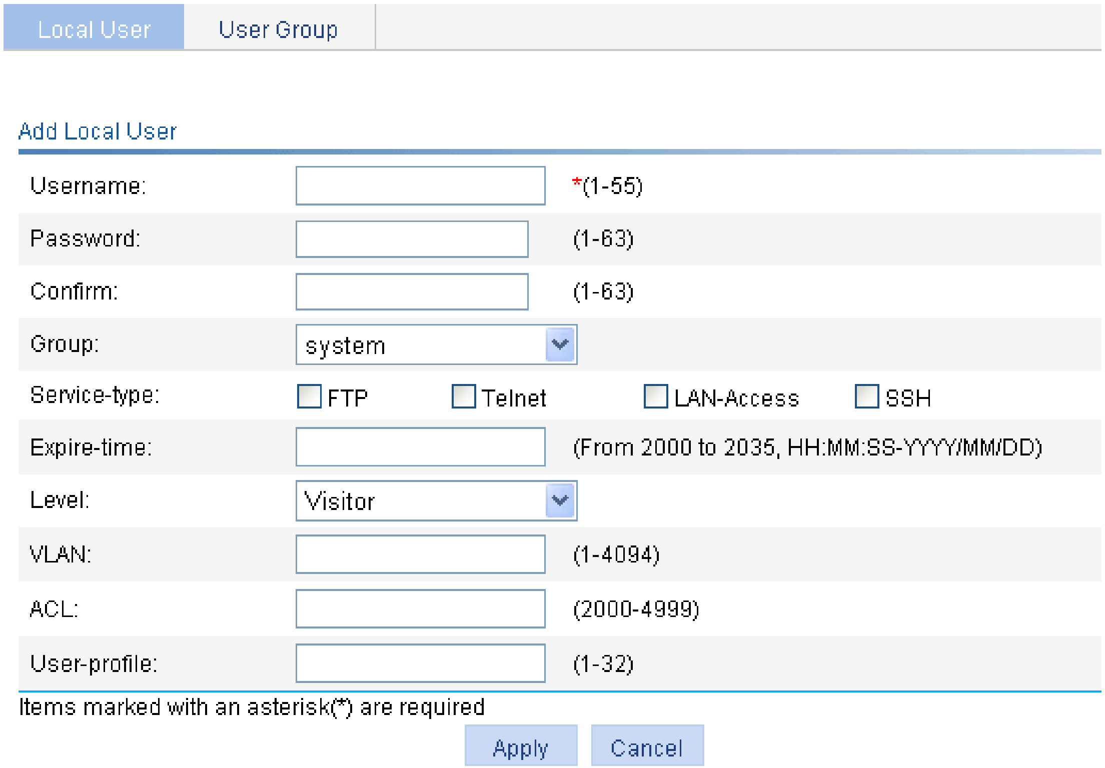
Figure 1-1 Local user list



Search Item: User Name Keywords:

User Name	Service Type	Level	VLAN	ACL	User Profile	User Group	Expire Time	Operation
admin	Telnet;	Management				system		✎ 🗑

Figure 1-2 Local user configuration page



Add Local User

Username:		*(1-55)
Password:		(1-63)
Confirm:		(1-63)
Group:	system	
Service-type:	□ FTP □ Telnet □ LAN-Access □ SSH	
Expire-time:		(From 2000 to 2035, HH:MM:SS-YYYY/MM/DD)
Level:	Visitor	
VLAN:		(1-4094)
ACL:		(2000-4999)
User-profile:		(1-32)

Items marked with an asterisk(*) are required

Table 1-1 describes the configuration items for configuring a local user.

Table 1-1 Local user configuration items

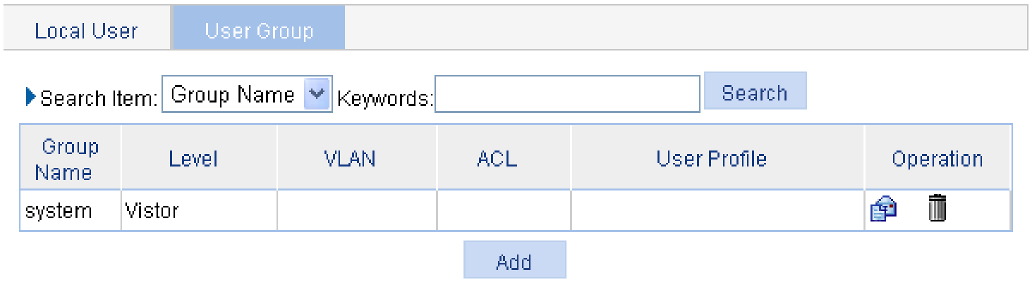
Item	Description
Username	Specify a name for the local user.
Password	Specify and confirm the password of the local user. The settings of these two fields must be the same.
Confirm	
Group	Select a user group for the local user. For information about user group configuration, refer for Configuring a User Group.
Service-type	Select the service types for the local user to use, including FTP, Telnet, LAN access (accessing through the Ethernet, such as 802.1x users), and SSH. **Highlight** *If you do not specify any service type for a local user who uses local authentication, the user cannot pass authentication and therefore cannot log in.*
Expire-time	Specify an expiration time for the local user, in the format HH:MM:SS-YYYY/MM/DD. When authenticating a local user with the expiration time argument configured, the access device checks whether the expiration time has elapsed. If not, the device permits the user to log in.

Item	Description	
Level	Select an authorization level for the local user, which can be Visitor, Monitor, Configure, or Management, in ascending order of priority.	**Highlight** *Every authorization attribute has its definite application environments and purposes. Therefore, when configuring authorization attributes for a local user, determine what attributes are needed first.*
VLAN	Specify the VLAN to be authorized to the local user after the user passes authentication.	
ACL	Specify the ACL to be used by the access device to restrict the access of the local user after the user passes authentication.	
User-profile	Specify the user profile for the local user. **Note** *Currently, switch 2900 series do not support user-profile configuration.*	

Configuring a User Group

Select **Authentication** > **Users** from the navigation tree, and then select the **User Group** tab to display the existing user groups, as shown in Figure 1-3. Then, click **Add** to enter the user group configuration page, as shown in Figure 1-4.

Figure 1-3 User group list



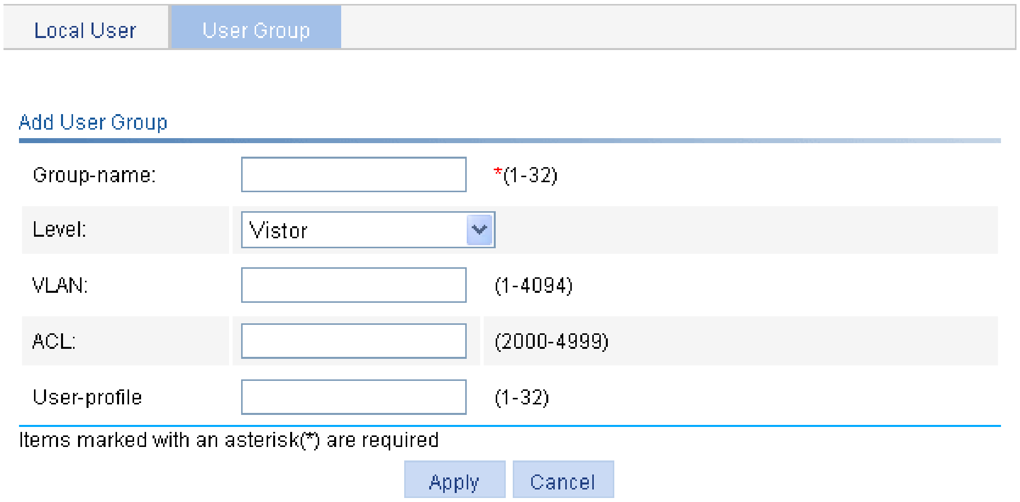
Local User | User Group

Search Item: Group Name ▾ Keywords: [ ] Search

Group Name	Level	VLAN	ACL	User Profile	Operation
system	Vistor				

Add

Figure 1-4 User group configuration page



Local User | User Group

Add User Group

Group-name:	[ ]	*(1-32)
Level:	Vistor ▾	
VLAN:	[ ]	(1-4094)
ACL:	[ ]	(2000-4999)
User-profile	[ ]	(1-32)

Items marked with an asterisk(*) are required

Apply Cancel

Table 1-2 describes the configuration items for configuring a user group.

Table 1-2 User group configuration items

Item	Description
Group-name	Specify a name for the user group.
Level	Select an authorization level for the user group, which can be Visitor, Monitor, Configure, or Management, in ascending order of priority.
VLAN	Specify the VLAN to be authorized to users of the user group after the users pass authentication.
ACL	Specify the ACL to be used by the access device to control the access of users of the user group after the users pass authentication.
User-profile	Specify the user profile for the user group. **Note** *Currently, switch 2900 series do not support user-profile configuration.*

Table of Contents

1 PKI Configuration

PKI Overview

The Public Key Infrastructure (PKI) is a hierarchical framework designed for providing information security through public key technologies and digital certificates and verifying the identities of the digital certificate owners.

PKI employs digital certificates, which are bindings of certificate owner identity information and public keys. It allows users to obtain certificates, use certificates, and revoke certificates. By leveraging digital certificates and relevant services like certificate distribution and blacklist publication, PKI supports authenticating the entities involved in communication, and thus guaranteeing the confidentiality, integrity and non-repudiation of data.

PKI Terms

Digital certificate

A digital certificate is a file signed by a certificate authority (CA) that contains a public key and the related user identity information. A simplest digital certificate contains a public key, an entity name, and a digital signature from the CA. Generally, a digital certificate also includes the validity period of the key, the name of the CA and the sequence number of the certificate. A digital certificate must comply with the international standard of ITU-T_X.509. This manual involves two types of certificates: local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity, while a CA certificate, also known as a root certificate, is signed by the CA for itself.

CRL

An existing certificate may need to be revoked when, for example, the user name changes, the private key leaks, or the user stops the business. Revoking a certificate is to remove the binding of the public key with the user identity information. In PKI, the revocation is made through certificate revocation lists (CRLs). Whenever a certificate is revoked, the CA publishes one or more CRLs to show all certificates that have been revoked. The CRLs contain the serial numbers of all revoked certificates and provide an effective way for checking the validity of certificates.

A CA may publish multiple CRLs when the number of revoked certificates is so large that publishing them in a single CRL may degrade network performance.

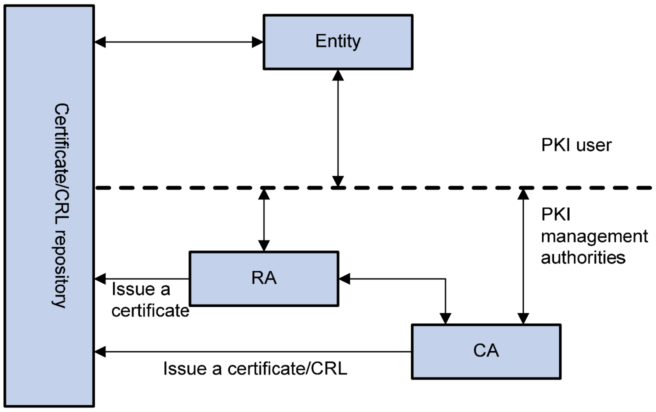
CA policy

A CA policy is a set of criteria that a CA follows in processing certificate requests, issuing and revoking certificates, and publishing CRLs. Usually, a CA advertises its policy in the form of certification practice statement (CPS). A CA policy can be acquired through out-of-band means such as phone, disk, and e-mail. As different CAs may use different methods to check the binding of a public key with an entity, make sure that you understand the CA policy before selecting a trusted CA for certificate request.

Architecture of PKI

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository, as shown in Figure 1-1.

Figure 1-1 PKI architecture



Entity

An entity is an end user of PKI products or services, such as a person, an organization, a device like a router or a switch, or a process running on a computer.

CA

A certificate authority (CA) is a trusted authority responsible for issuing and managing digital certificates. A CA issues certificates, specifies the validity periods of certificates, and revokes certificates as needed by publishing CRLs.

RA

A registration authority (RA) is an extended part of a CA or an independent authority. An RA can implement functions including identity authentication, CRL management, key pair generation and key pair backup. It only examines the qualifications of users; it does not sign certificates. Sometimes, a CA assumes the registration management responsibility and therefore there is no independent RA. The PKI standard recommends that an independent RA be used for registration management to achieve higher security of application systems.

PKI repository

A PKI repository can be a Lightweight Directory Access Protocol (LDAP) server or a common database. It stores and manages information like certificate requests, certificates, keys, CRLs and logs while providing a simple query function.

LDAP is a protocol for accessing and managing PKI information. An LDAP server stores user information and digital certificates from the RA server and provides directory navigation service. From an LDAP server, an entity can retrieve digital certificates of its own and other entities.

Applications of PKI

The PKI technology can satisfy the security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

VPN

A virtual private network (VPN) is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for instance, IPSec) in conjunction with PKI-based encryption and digital signature technologies to achieve confidentiality.

Secure E-mail

E-mails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure E-mail protocol that is currently developing rapidly is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

Web security

For Web security, two peers can establish a Secure Sockets Layer (SSL) connection first for transparent and secure communications at the application layer. With PKI, SSL enables encrypted communications between a browser and a server. Both the communication parties can verify the identity of each other through digital certificates.

Operation of PKI

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificate. The following describes how it works:

1) An entity submits a certificate request to the CA.
2) The RA verifies the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.
3) The CA verifies the digital signature, approves the application, and issues a certificate.
4) The RA receives the certificate from the CA, sends it to the LDAP server to provide directory navigation service, and notifies the entity that the certificate is successfully issued.
5) The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.
6) The entity makes a request to the CA when it needs to revoke its certificate, while the CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

Configuring PKI

Configuration Task List

There are two PKI certificate request modes:

- Manual: In manual mode, you need to retrieve a CA certificate, generate a local RSA key pair, and submit a local certificate request for an entity.
- Auto: In auto mode, an entity automatically requests a certificate through the Simple Certification Enrollment Protocol (SCEP) when it has no local certificate or the present certificate is about to expire.

You can specify the PKI certificate request mode for a PKI domain. Different PKI certificate request modes require different configurations:

Requesting a certificate manually

Perform the tasks in Table 1-1 to request a certificate manually.

Table 1-1 Configuration task list for requesting a certificate manually

Task	Remarks
Creating a PKI Entity	Required Create a PKI entity and configure the identity information. A certificate is the binding of a public key and an entity, where an entity is the collection of the identity information of a user. A CA identifies a certificate applicant by entity. **Highlight** *The identity settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request may be rejected.*
Creating a PKI Domain	Required Create a PKI domain, setting the certificate request mode to Manual. Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain. A PKI domain is intended only for convenience of reference by other applications like SSL, and has only local significance.
Generating an RSA Key Pair	Required Generate a local RSA key pair. By default, no local RSA key pair exists. Generating an RSA key pair is an important step in certificate request. The key pair includes a public key and a private key. The private key is kept by the user, while the public key is transferred to the CA along with some other information. **Highlight** *If there is already a local certificate, you need to remove the certificate before generating a new key pair, so as to keep the consistency between the key pair and the local certificate.*
Retrieving the CA certificate	Required Certificate retrieval serves two purposes: • Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count, • Prepare for certificate verification. **Highlight** *If there are already CA certificates locally, you cannot perform the CA certificate retrieval operation. This is to avoid possible mismatch between certificates and registration information resulting from relevant changes. To retrieve the CA certificate, you need to remove the CA certificate and local certificate first.*

Task	Remarks
Requesting a Local Certificate	Required When requesting a certificate, an entity introduces itself to the CA by providing its identity information and public key, which will be the major components of the certificate. A certificate request can be submitted to a CA in two ways: online and offline. • In online mode, if the request is granted, the local certificate will be retrieved to the local system automatically. • In offline mode, you need to retrieve the local certificate by an out-of-band means. **Highlight** *If there is already a local certificate, you cannot perform the local certificate retrieval operation. This is to avoid possible mismatch between the local certificate and registration information resulting from relevant changes. To retrieve a new local certificate, you need to remove the CA certificate and local certificate first.*
Destroying the RSA Key Pair	Optional Destroy the existing RSA key pair and the corresponding local certificate. If the certificate to be retrieved contains an RSA key pair, you need to destroy the existing key pair. Otherwise, the retrieving operation will fail.
Retrieving a Certificate	Optional Retrieve an existing certificate.
Retrieving and Displaying a CRL	Optional Retrieve a CRL and display its contents.

Requesting a Certificate Automatically

Perform the tasks in Table 1-2 to configure the PKI system to request a certificate automatically.

Table 1-2 Configuration task list for requesting a certificate automatically

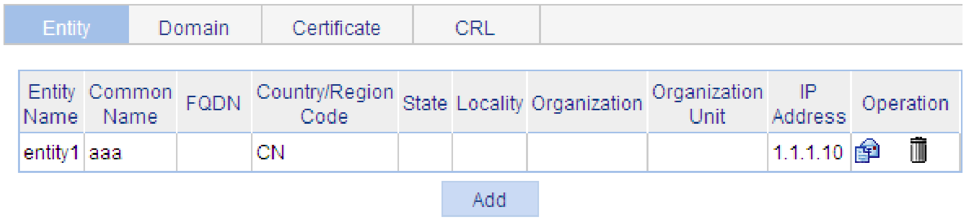
Task	Remarks
Creating a PKI Entity	Required Create a PKI entity and configure the identity information. A certificate is the binding of a public key and an entity, where an entity is the collection of the identity information of a user. A CA identifies a certificate applicant by entity. The identity settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request may be rejected.
Creating a PKI Domain	Required Create a PKI domain, setting the certificate request mode to **Auto**. Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain. A PKI domain is intended only for convenience of reference by other applications like SSL, and has only local significance.
Destroying the RSA Key Pair	Optional Destroy the existing RSA key pair and the corresponding local certificate. If the certificate to be retrieved contains an RSA key pair, you need to destroy the existing key pair. Otherwise, the retrieving operation will fail.

Task	Remarks
Retrieving a Certificate	Optional Retrieve an existing certificate.
Retrieving and Displaying a CRL	Optional Retrieve a CRL and display its contents.

Creating a PKI Entity

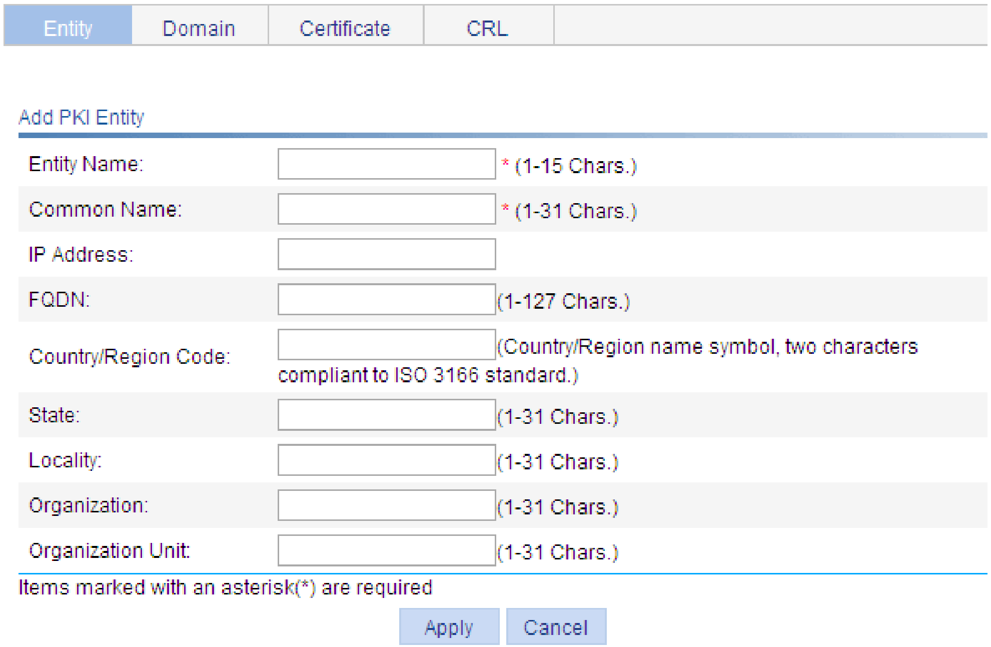
Select **Authentication** > **PKI** from the navigation tree. The PKI entity list page is displayed by default, as shown in Figure 1-2. Click **Add** on the page to enter the PKI entity configuration page, as shown in Figure 1-3.

Figure 1-2 PKI entity list



Entity Name	Common Name	FQDN	Country/Region Code	State	Locality	Organization	Organization Unit	IP Address	Operation
entity1	aaa		CN					1.1.1.10	

Figure 1-3 PKI entity configuration page



Add PKI Entity

Entity Name:		* (1-15 Chars.)
Common Name:		* (1-31 Chars.)
IP Address:		
FQDN:		(1-127 Chars.)
Country/Region Code:		(Country/Region name symbol, two characters compliant to ISO 3166 standard.)
State:		(1-31 Chars.)
Locality:		(1-31 Chars.)
Organization:		(1-31 Chars.)
Organization Unit:		(1-31 Chars.)

Items marked with an asterisk(*) are required

Table 1-3 describes the configuration items for creating a PKI entity.

Table 1-3 PKI entity configuration items

Item	Description
Entity Name	Type the name for the PKI entity.
Common Name	Type the common name for the entity.

Item	Description
IP Address	Type the IP address of the entity.
FQDN	Type the fully qualified domain name (FQDN) for the entity. An FQDN is a unique identifier of an entity on the network. It consists of a host name and a domain name and can be resolved to an IP address. For example, www.whatever.com is an FQDN, where www indicates the host name and whatever.com the domain name.
Country/Region Code	Type the country or region code for the entity.
State	Type the state or province for the entity.
Locality	Type the locality for the entity.
Organization	Type the organization name for the entity.
Organization Unit	Type the unit name for the entity.

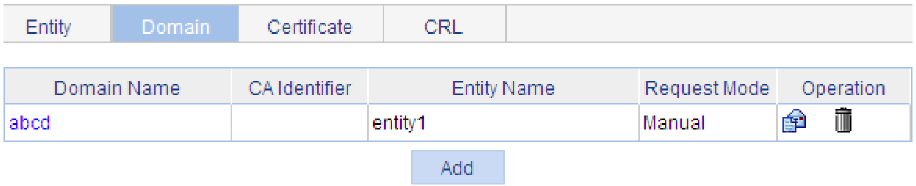
Return to Configuration task list for requesting a certificate manually.

Return to Configuration task list for requesting a certificate automatically.

Creating a PKI Domain

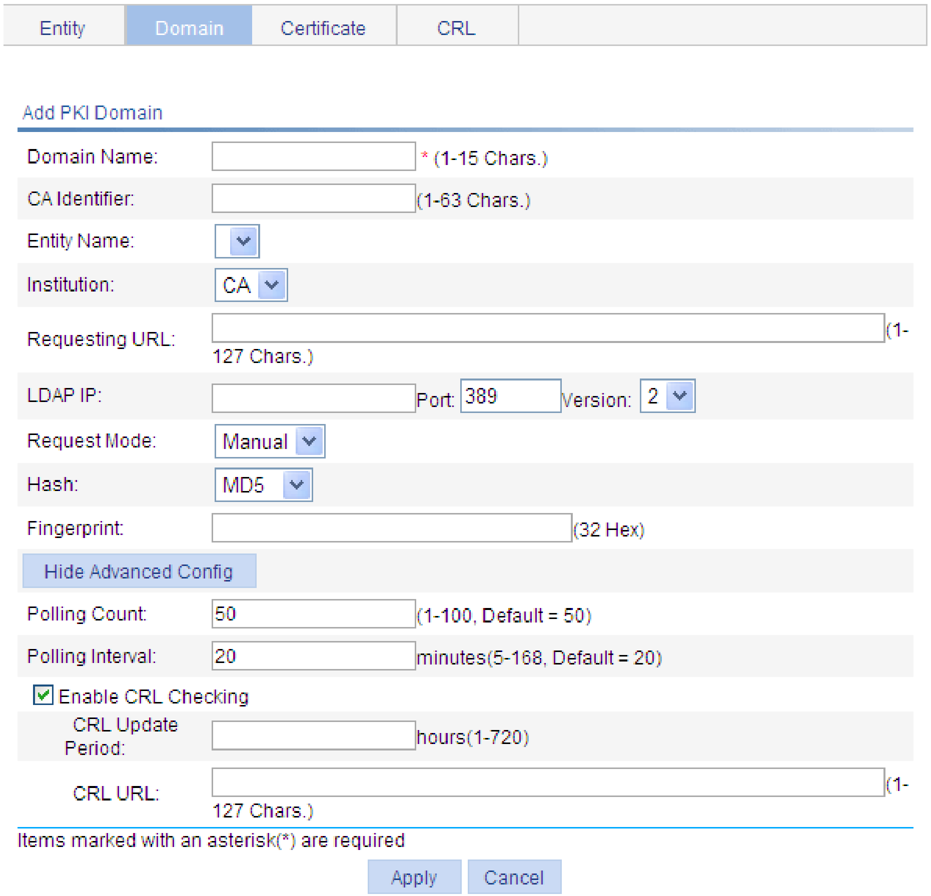
Select **Authentication** > **PKI** from the navigation tree, and then select the **Domain** tab to enter the page displaying existing PKI domains, as shown in Figure 1-4. Then, click **Add** to enter the PKI domain configuration page, and click **Display Advanced Config** to display the advanced configuration items, as shown in Figure 1-5.

Figure 1-4 PKI domain list



Domain Name	CA Identifier	Entity Name	Request Mode	Operation
abcd		entity1	Manual	📄 🗑

Figure 1-5 PKI domain configuration page



Domain Name: * (1-15 Chars.)

CA Identifier: (1-63 Chars.)

Entity Name:

Institution: CA

Requesting URL: (1-127 Chars.)

LDAP IP: Port: 389 Version: 2

Request Mode: Manual

Hash: MD5

Fingerprint: (32 Hex)

Polling Count: 50 (1-100, Default = 50)

Polling Interval: 20 minutes(5-168, Default = 20)

☑ Enable CRL Checking

CRL Update Period: hours(1-720)

CRL URL: (1-127 Chars.)

Items marked with an asterisk(*) are required

Table 1-4 describes the configuration items for creating a PKI domain.

Table 1-4 PKI domain configuration items

Item	Description
Domain Name	Type the name for the PKI domain.
CA Identifier	Type the identifier of the trusted CA. An entity requests a certificate from a trusted CA. The trusted CA takes the responsibility of certificate registration, distribution, and revocation, and query. In offline mode, this item is optional; while in other modes, this item is required.
Entity Name	Select the local PKI entity. When submitting a certificate request to a CA, an entity needs to show its identity information. Available PKI entities are those that have been configured.
Institution	Select the authority for certificate request. • **CA**: Indicates that the entity requests a certificate from a CA. • **RA**: Indicates that the entity requests a certificate from an RA. RA is recommended.

Item	Description
Requesting URL	Type the URL of the RA. The entity will submit the certificate request to the server at this URL through the SCEP protocol. The SCEP protocol is intended for communication between an entity and an authentication authority. In offline mode, this item is optional; while in other modes, this item is required. **Highlight** *Currently, this item does not support domain name resolution.*
LDAP IP	Type the IP address, port number and version of the LDAP server. In a PKI system, the storage of certificates and CRLs is a crucial problem, which is usually addressed by deploying an LDAP server.
Port	
Version	
Request Mode	Select the online certificate request mode, which can be auto or manual.
Password Encrypt	Select this check box to display the password in cipher text. This check box is available only when the certificate request mode is set to **Auto**.
Password	Type the password for certificate revocation. This item is available only when the certificate request mode is set to **Auto**.
Hash	Specify the hash algorithm and fingerprint for verification of the CA root certificate. Upon receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate, namely, the hash value of the root certificate content. This hash value is unique to every certificate. If the fingerprint of the root certificate does not match the one configured for the PKI domain, the entity will reject the root certificate. **Highlight** *The fingerprint of the CA root certificate is required when the certificate request mode is **Auto**, and can be omitted when the certificate request mode is **Manual**. When it is omitted, no CA root certificate verification occurs automatically and you need to verify the CA server by yourself.*
Fingerprint	
Polling Count	Set the polling interval and attempt limit for querying the certificate request status. After an entity makes a certificate request, the CA may need a long period of time if it verifies the certificate request in manual mode. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.
Polling Interval	
Enable CRL Checking	Select this box to specify that CRL checking is required during certificate verification.
CRL Update Period	Type the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs. This item is available when the **Enable CRL Checking** check box is selected. By default, the CRL update period depends on the next update field in the CRL file.

Item	Description
CRL URL	Type the URL of the CRL distribution point. This item is available when the **Enable CRL Checking** check box is selected. Note that when the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP. **Highlight** *Currently, this item does not support domain name resolution.*

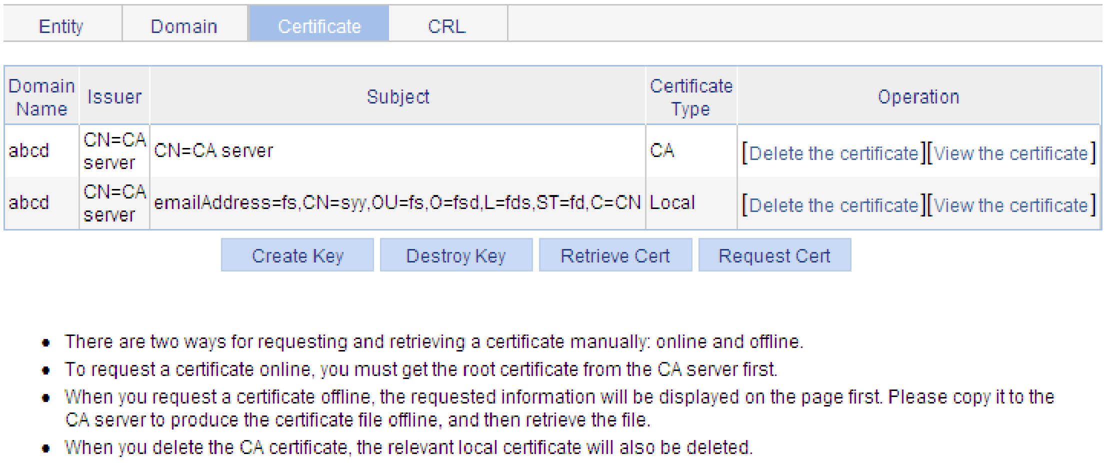
Return to Configuration task list for requesting a certificate manually.

Return to Configuration task list for requesting a certificate automatically.

Generating an RSA Key Pair

Select **Authentication** > **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in Figure 1-6. Then, click **Create Key** to enter RSA key pair parameter configuration page, as shown in Figure 1-7.

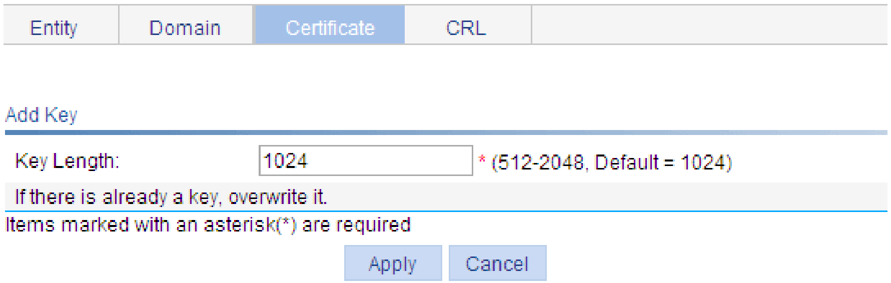
Figure 1-6 Certificate configuration page



Domain Name	Issuer	Subject	Certificate Type	Operation
abcd	CN=CA server	CN=CA server	CA	[Delete the certificate][View the certificate]
abcd	CN=CA server	emailAddress=fs,CN=syy,OU=fs,O=fsd,L=fds,ST=fd,C=CN	Local	[Delete the certificate][View the certificate]

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

Figure 1-7 Key pair parameter configuration page



Add Key

Key Length: 1024 * (512-2048, Default = 1024)

If there is already a key, overwrite it.

Items marked with an asterisk(*) are required

Table 1-5 describes the configuration item for generating an RSA key pair.

Table 1-5 Configuration item for generating an RSA key pair

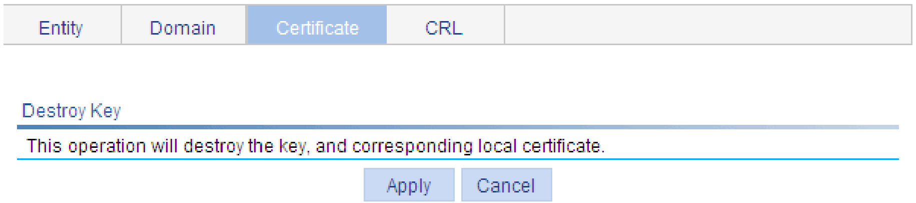
Item	Description
Key Length	Type the length of the RSA keys.

Return to Configuration task list for requesting a certificate manually.

Destroying the RSA Key Pair

Select **Authentication** > **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in Figure 1-6. Click **Destroy Key** to enter RSA key pair destruction page, as shown in Figure 1-8. Then, click **Apply** to destroy the existing RSA key pair and the corresponding local certificate.

Figure 1-8 Key pair destruction page



This operation will destroy the key, and corresponding local certificate.

Return to Configuration task list for requesting a certificate manually.

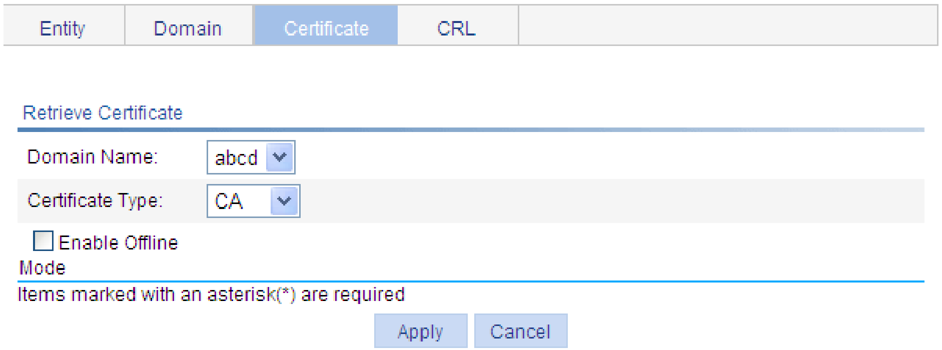
Return to Configuration task list for requesting a certificate automatically.

Retrieving a Certificate

You can download an existing CA certificate or local certificate from the CA server and save it locally. To do so, you can use two ways: online and offline. In offline mode, you need to retrieve a certificate by an out-of-band means like FTP, disk, e-mail and then import it into the local PKI system.

Select **Authentication** > **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in Figure 1-6. Click **Retrieve Cert** to enter PKI certificate retrieval page, as shown in Figure 1-9.

Figure 1-9 PKI certificate retrieval page



Domain Name: abcd

Certificate Type: CA

☐ Enable Offline Mode

Items marked with an asterisk(*) are required

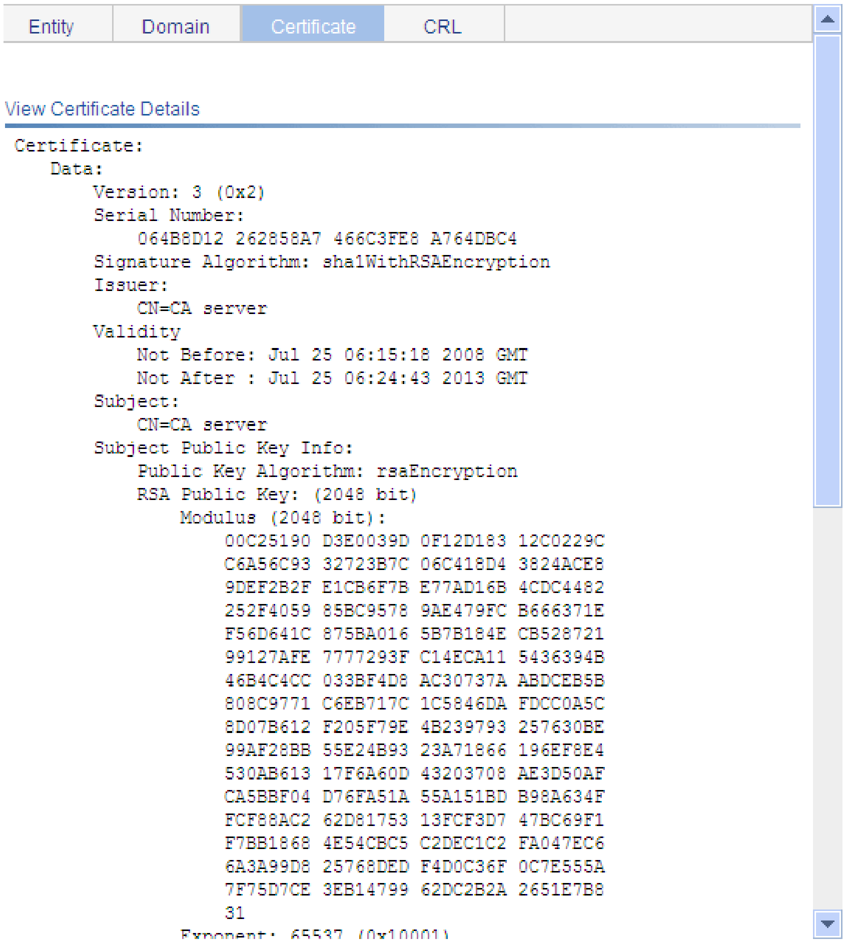
Table 1-6 describes the configuration items for retrieving a PKI certificate.

Table 1-6 Configuration items for retrieving a PKI certificate

Item	Description
Domain Name	Select the PKI domain for the certificate.
Certificate Type	Select the type of the certificate to be retrieved, which can be CA or local.
Enable Offline Mode	Select this check box to retrieve a certificate in offline mode (that is, by an out-of-band means like FTP, disk, or e-mail) and then import the certificate into the local PKI system. The following configuration items are displayed if this check box is selected.
Get File From Device	Specify the path and name of the certificate file. • If the certificate file is saved on the device, select **Get File From Device** and then specify the path of the file on the device. • If the certificate file is saved on a local PC, select **Get File From PC** and. then specify the path to the file and select the partition of the device for saving the file.
Get File From PC	
Password	Enter the password for protecting the private key, which was specified when the certificate was exported.

After retrieving a certificate, you can click **View Cert** corresponding to the certificate from the PKI certificates list to display the contents of the certificate, as shown in Figure 1-10.

Figure 1-10 Certificate details



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            064B8D12 262858A7 466C3FE8 A764DBC4
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=CA server
        Validity
            Not Before: Jul 25 06:15:18 2008 GMT
            Not After : Jul 25 06:24:43 2013 GMT
        Subject:
            CN=CA server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00C25190 D3E0039D 0F12D183 12C0229C
                    C6A56C93 32723B7C 06C418D4 3824ACE8
                    9DEF2B2F E1CB6F7B E77AD16B 4CDC4482
                    252F4059 85BC9578 9AE479FC B666371E
                    F56D641C 875BA016 5B7B184E CB528721
                    99127AFE 7777293F C14ECA11 5436394B
                    46B4C4CC 033BF4D8 AC30737A ABDCEB5B
                    808C9771 C6EB717C 1C5846DA FDCC0A5C
                    8D07B612 F205F79E 4B239793 257630BE
                    99AF28BB 55E24B93 23A71866 196EF8E4
                    530AB613 17F6A60D 43203708 AE3D50AF
                    CA5BBF04 D76FA51A 55A151BD B98A634F
                    FCF88AC2 62D81753 13FCF3D7 47BC69F1
                    F7BB1868 4E54CBC5 C2DEC1C2 FA047EC6
                    6A3A99D8 25768DED F4D0C36F 0C7E555A
                    7F75D7CE 3EB14799 62DC2B2A 2651E7B8
                    31
                Exponent: 65537 (0x10001)
```

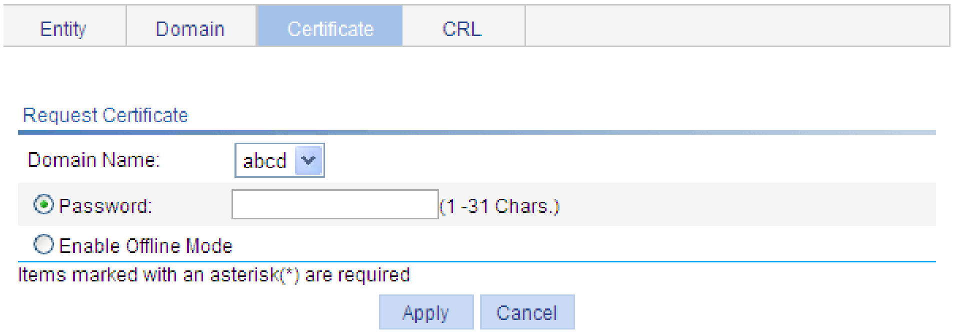
Return to Configuration task list for requesting a certificate manually.

Return to Configuration task list for requesting a certificate automatically.

Requesting a Local Certificate

Select **Authentication** > **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in Figure 1-6. Click **Request Cert** to enter the local certificate request page, as shown in Figure 1-11.

Figure 1-11 Local certificate request page



Request Certificate

Domain Name: abcd

● Password: (1 -31 Chars.)

○ Enable Offline Mode

Items marked with an asterisk(*) are required

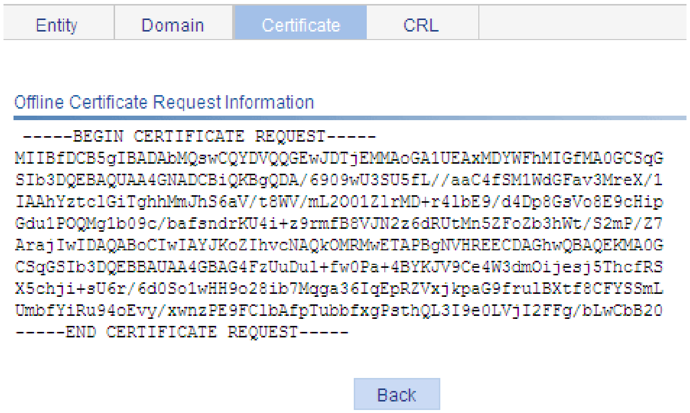
Table 1-7 describes the configuration items for requesting a local certificate.

Table 1-7 Configuration items for requesting a local certificate

Item	Description
Domain Name	Select the PKI domain for the certificate.
Password	Type the password for certificate revocation.
Enable Offline Mode	Select this check box to request a certificate in offline mode, that is, by an out-of-band means like FTP, disk, or e-mail.

If you select the offline mode and click **Apply**, the offline certificate request information page appears, as shown in Figure 1-12. Submit the information to the CA to request a local certificate.

Figure 1-12 Offline certificate request information page



Offline Certificate Request Information

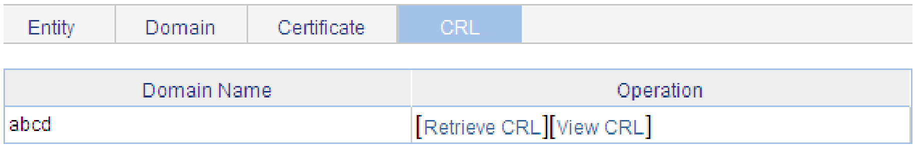
```
 -----BEGIN CERTIFICATE REQUEST-----
MIIBfDCB5gIBADAbMQswCQYDVQQGEwJDTjEMMAoGA1UEAxMDYWFhMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDA/6909wU3SU5fL//aaC4fSM1WdGFav3MreX/1
IAAhYztclGiTghhMmJhS6aV/t8WV/mL2O01ZlrMD+r4lbE9/d4Dp8GsVo8E9cHip
Gdu1POQMg1b09c/bafsndrKU4i+z9rmfB8VJN2z6dRUtMn5ZFoZb3hWt/S2mP/Z7
ArajIwIDAQABoCIwIAYJKoZIhvcNAQkOMRMwETAPBgNVHREECDAGhwQBAQEKMA0G
CSqGSIb3DQEBBAUAA4GBAG4FzUuDul+fw0Pa+4BYKJV9Ce4W3dmOijesj5ThcfRS
X5chji+sU6r/6d0So1wHH9o28ib7Mqga36IqEpRZVxjkpaG9frulBXtf8CFYSSmL
UmbfYiRu94oEvy/xwnzPE9FClbAfpTubbfxgPsthQL3I9e0LVjI2FFg/bLwCbB20
-----END CERTIFICATE REQUEST-----
```

Return to Configuration task list for requesting a certificate manually.

Retrieving and Displaying a CRL

Select **Authentication** > **PKI** from the navigation tree, and then select the **CRL** tab to enter the page displaying CRLs, as shown in Figure 1-13.

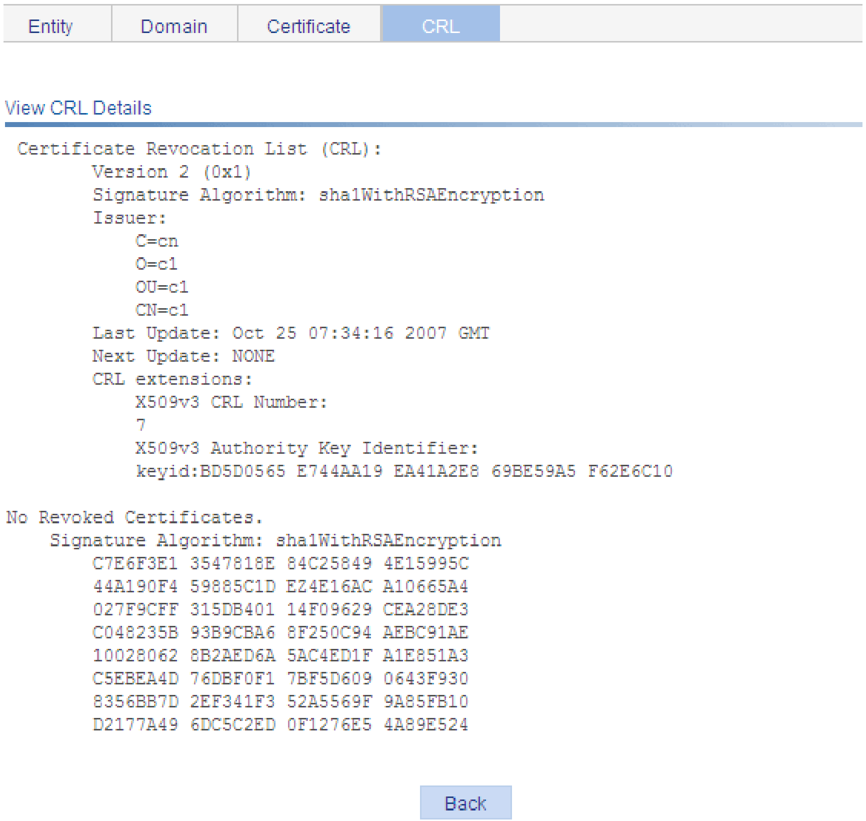
Figure 1-13 CRL page



Domain Name	Operation
abcd	[Retrieve CRL][View CRL]

- Click **Retrieve CRL** to retrieve the CRL of a domain.
- Then, click **View CRL** for the domain to display the contents of the CRL, as shown in Figure 1-14.

Figure 1-14 CRL details



```
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=cn
            O=c1
            OU=c1
            CN=c1
        Last Update: Oct 25 07:34:16 2007 GMT
        Next Update: NONE
        CRL extensions:
            X509v3 CRL Number:
            7
            X509v3 Authority Key Identifier:
            keyid:BD5D0565 E744AA19 EA41A2E8 69BE59A5 F62E6C10

No Revoked Certificates.
    Signature Algorithm: sha1WithRSAEncryption
        C7E6F3E1 3547818E 84C25849 4E15995C
        44A190F4 59885C1D EZ4E16AC A10665A4
        027F9CFF 315DB401 14F09629 CEA28DE3
        C048235B 93B9CBA6 8F250C94 AEBC91AE
        10028062 8B2AED6A 5AC4ED1F A1E851A3
        C5EBEA4D 76DBF0F1 7BF5D609 0643F930
        8356BB7D 2EF341F3 52A5569F 9A85FB10
        D2177A49 6DC5C2ED 0F1276E5 4A89E524
```

Table 1-8 describes some fields of the CRL details.

Table 1-8 Description about some fields of the CRL details

Field	Description
Version	CRL version number
Signature Algorithm	Signature algorithm that the CRL uses
Issuer	CA that issued the CRL
X509v3 Authority Key Identifier	Identifier of the CA that issued the certificate and the certificate version (X509v3).

Field	Description
keyid	Pubic key identifier A CA may have multiple key pairs, and this field identifies which key pair is used for the CRL signature.

Return to Configuration task list for requesting a certificate manually.

Return to Configuration task list for requesting a certificate automatically.

PKI Configuration Example

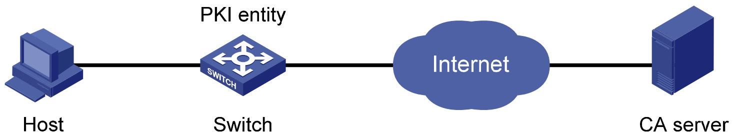
Configuring a PKI Entity to Request a Certificate from a CA

Network requirements

As shown in Figure 1-15, configure the Switch working as the PKI entity, so that:

- The Switch submits a local certificate request to the CA server, which runs the RSA Keon software.
- The Switch acquires CRLs for certificate verification.

Figure 1-15 Network diagram for configuring a PKI entity to request a certificate from a CA



Configuration procedure

1) Configure the CA server

# Create a CA server named **myca**.

In this example, you need to configure the basic attributes of **Nickname** and **Subject DN** on the CA server at first:

- Nickname: Name of the trusted CA.
- Subject DN: DN information of the CA, including the Common Name (CN),
- Organization Unit (OU),
- Organization (O), and
- Country (C).

The other attributes may use the default values.

# Configure extended attributes

After configuring the basic attributes, you need to perform configuration on the **Jurisdiction Configuration** page of the CA server. This includes selecting the proper extension profiles, enabling the SCEP autovetting function, and adding the IP address list for SCEP autovetting.

# Configure the CRL publishing behavior

After completing the above configuration, you need to perform CRL related configurations.

In this example, select the local CRL publishing mode of HTTP and set the HTTP URL to http://4.4.4.133:447/myca.crl.

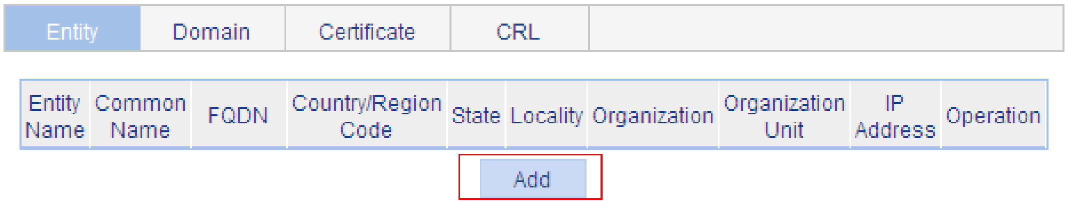
After the above configuration, make sure that the system clock of the Switch is synchronous to that of the CA, so that the Switch can request certificates and retrieve CRLs properly.

2) Configure Switch

# Create a PKI entity.

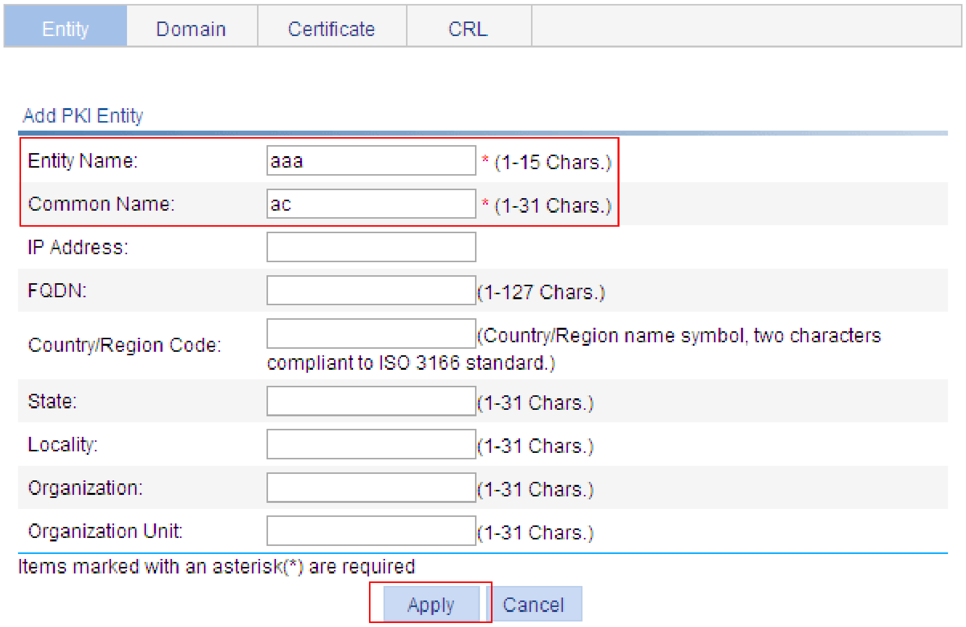
- Select **Authentication** > **PKI** from the navigation tree. The PKI entity list page is displayed by default. Click **Add** on the page, as shown in Figure 1-16, and then perform the following configurations as shown in Figure 1-17.

Figure 1-16 PKI entity list



Entity Name	Common Name	FQDN	Country/Region Code	State	Locality	Organization	Organization Unit	IP Address	Operation

Figure 1-17 Configure a PKI entity



Add PKI Entity

Entity Name:	aaa	* (1-15 Chars.)
Common Name:	ac	* (1-31 Chars.)
IP Address:		
FQDN:		(1-127 Chars.)
Country/Region Code:		(Country/Region name symbol, two characters compliant to ISO 3166 standard.)
State:		(1-31 Chars.)
Locality:		(1-31 Chars.)
Organization:		(1-31 Chars.)
Organization Unit:		(1-31 Chars.)

Items marked with an asterisk(*) are required

- Type **aaa** as the PKI entity name.
- Type **ac** as the common name.
- Click **Apply**.

# Create a PKI domain.

- Select the **Domain** tab, and then click **Add**, as shown in Figure 1-18, and then perform the following configurations as shown in Figure 1-19.

Figure 1-18 PKI domain list

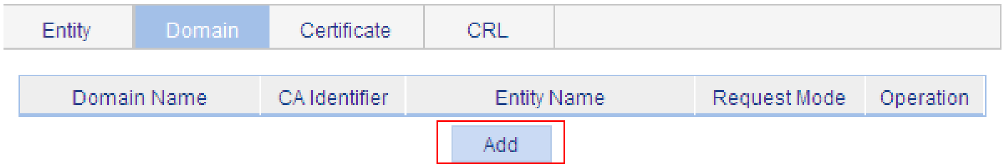
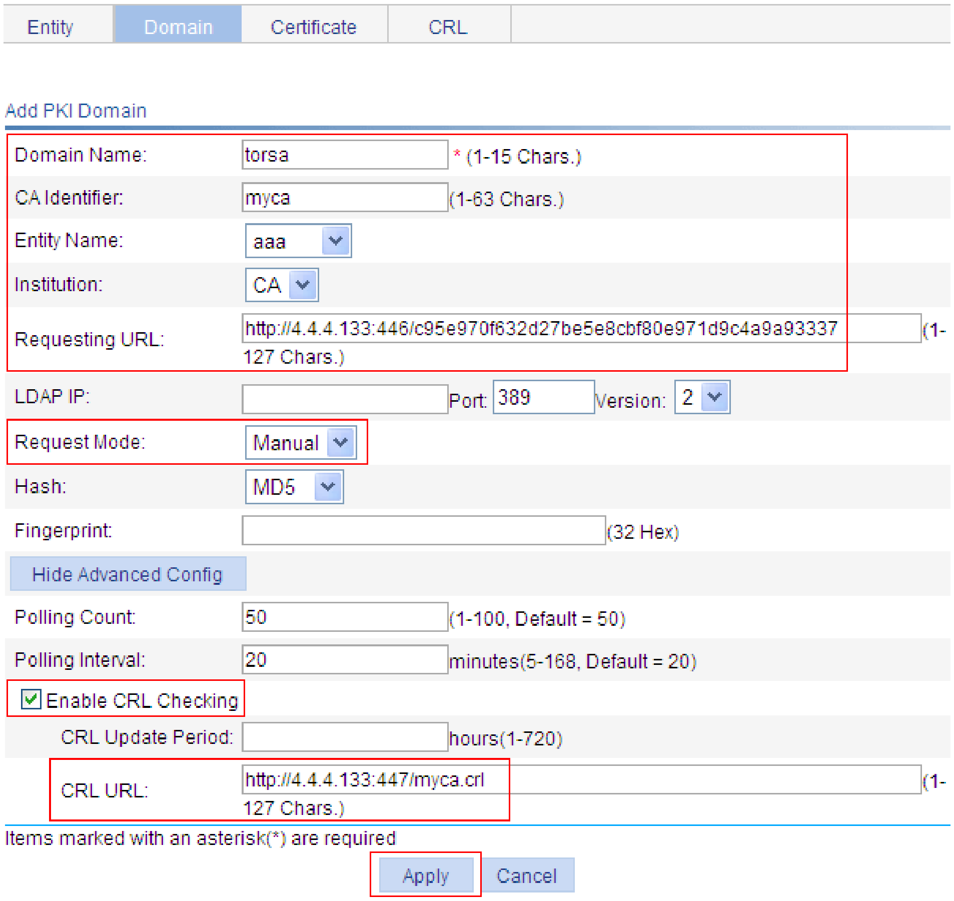


Figure 1-19 Configure a PKI domain



Domain Name: torsa * (1-15 Chars.)

CA Identifier: myca (1-63 Chars.)

Entity Name: aaa

Institution: CA

Requesting URL: http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337 (1-127 Chars.)

LDAP IP: Port: 389 Version: 2

Request Mode: Manual

Hash: MD5

Fingerprint: (32 Hex)

Polling Count: 50 (1-100, Default = 50)

Polling Interval: 20 minutes(5-168, Default = 20)

☑ Enable CRL Checking

CRL Update Period: hours(1-720)

CRL URL: http://4.4.4.133:447/myca.crl (1-127 Chars.)

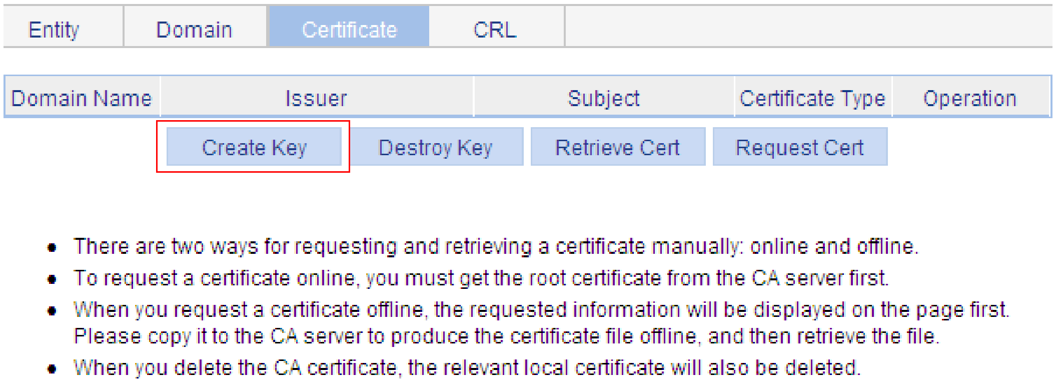
Items marked with an asterisk(*) are required

- Type **torsa** as the PKI domain name.
- Type **myca** as the CA identifier.
- Select **aaa** as the local entity.
- Select **CA** as the authority for certificate request.
- Type **http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337** as the URL for certificate request. The URL must be in the format of http://host:port/Issuing Jurisdiction ID, where Issuing Jurisdiction ID is the hexadecimal string generated on the CA.
- Select **Manual** as the certificate request mode.
- Click **Display Advanced Config** to display the advanced configuration items.
- Select the **Enable CRL Checking** check box.
- Type **http://4.4.4.133:447/myca.crl** as the CRL URL.
- Click **Apply**. A dialog box appears, asking "Fingerprint of the root certificate not specified. No root certificate validation will occur. Continue?" Click **OK**.

# Generate an RSA key pair.

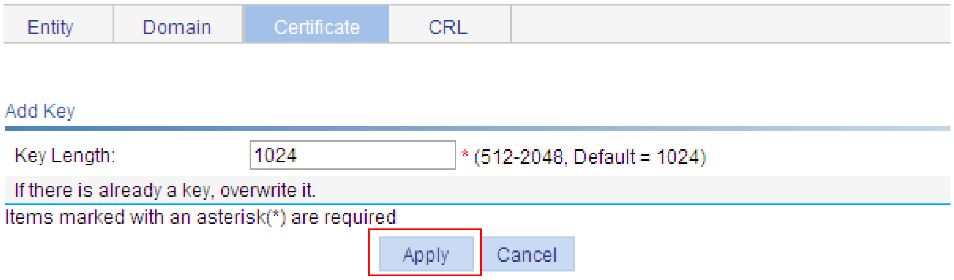
- Select the **Certificate** tab, and then click **Create Key**, as shown in Figure 1-20, and perform the configuration as shown in Figure 1-21.

Figure 1-20 Certificate list



- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

Figure 1-21 Generate an RSA key pair



Key Length: 1024 * (512-2048, Default = 1024)

If there is already a key, overwrite it.

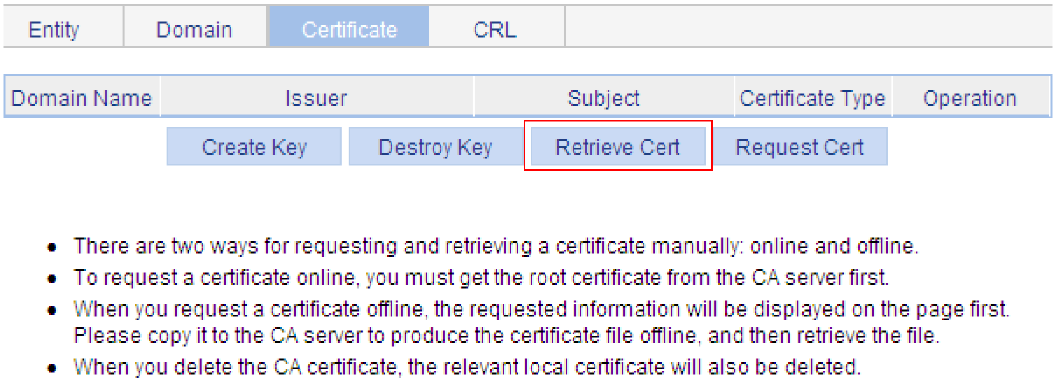
Items marked with an asterisk(*) are required

- Click **Apply** to generate an RSA key pair.

# Retrieve the CA certificate.

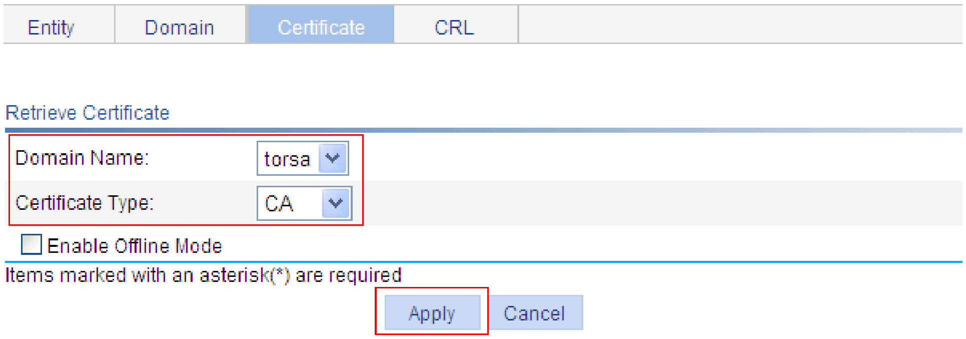
- Select the **Certificate** tab, and then click **Retrieve Cert**, as shown in Figure 1-22, and then perform the following configurations as shown in Figure 1-23.

Figure 1-22 Certificate list



- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

Figure 1-23 Retrieve the CA certificate



Retrieve Certificate

Domain Name: torsa

Certificate Type: CA

□ Enable Offline Mode

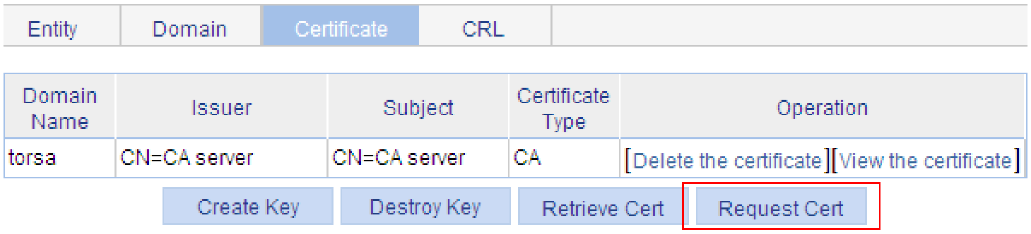
Items marked with an asterisk(*) are required

- Select **torsa** as the PKI domain.
- Select **CA** as the certificate type.
- Click **Apply**.

# Request a local certificate.

- Select the **Certificate** tab, and then click **Request Cert**, as shown in Figure 1-24, and then perform the following configurations as shown in Figure 1-25.

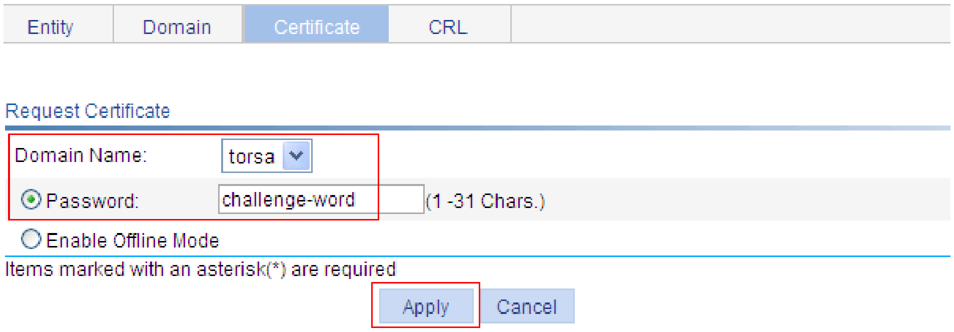
Figure 1-24 Certificate list



Domain Name	Issuer	Subject	Certificate Type	Operation
torsa	CN=CA server	CN=CA server	CA	[Delete the certificate][View the certificate]

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieval the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

Figure 1-25 Request a local certificate



Request Certificate

Domain Name: torsa

● Password: challenge-word (1 -31 Chars.)

○ Enable Offline Mode

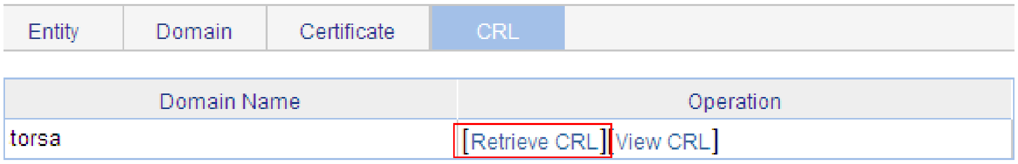
Items marked with an asterisk(*) are required

- Select **torsa** as the PKI domain.
- Select **Password** and then type challenge-word as the password.
- Click **Apply**.

Retrieve the CRL.

- After retrieving a local certificate, select the **CRL** tab.
- Click **Retrieve CRL** of the PKI domain of **torsa**, as shown in Figure 1-26.

Figure 1-26 Retrieve the CRL



Domain Name	Operation
torsa	[Retrieve CRL][View CRL]

Configuration Guidelines

When configuring PKI, note that:

1) Make sure the clocks of entities and the CA are synchronous. Otherwise, the validity period of certificates will be abnormal.
2) The Windows 2000 CA server has some restrictions on the data length of a certificate request. If the PKI entity identity information in a certificate request goes beyond a certain limit, the server will not respond to the certificate request.
3) The SCEP plug-in is required when you use the Windows Server as the CA. In this case, you need to specify **RA** as the authority for certificate request when configuring the PKI domain.
4) The SCEP plug-in is not required when you use the RSA Keon software as the CA. In this case, you need to specify **CA** as the authority for certificate request when configuring the PKI domain.

Table of Contents

1 Port Isolation Group Configuration

Overview

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

Currently:

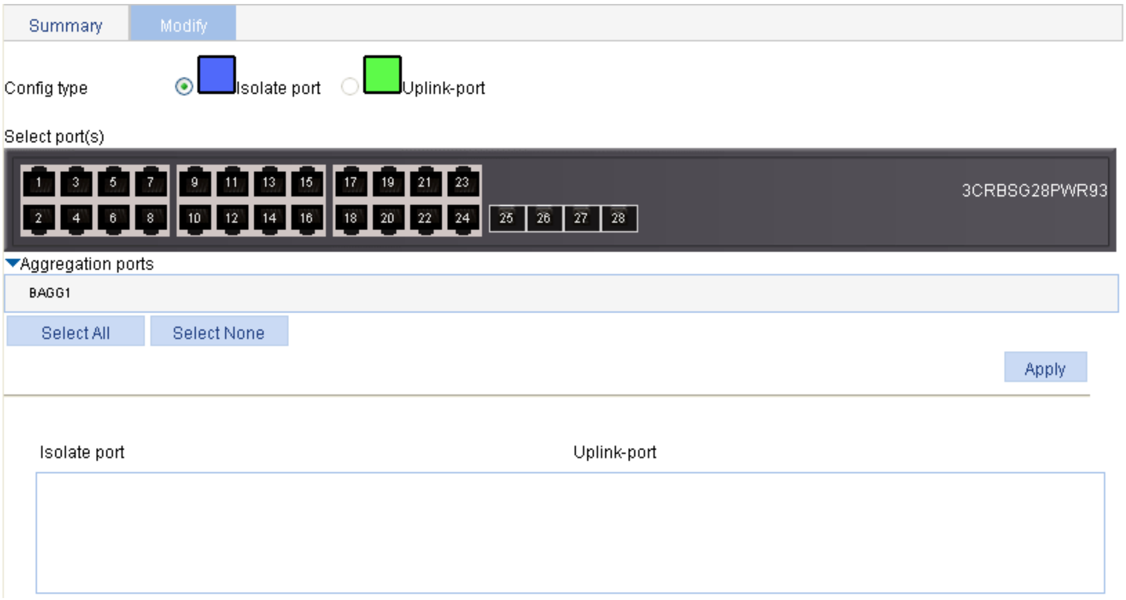
- 3Com Switch 2900 series support only one isolation group that is created automatically by the system as isolation group 1. You can neither remove the isolation group nor create other isolation groups on such devices.
- There is no restriction on the number of ports assigned to an isolation group.

Usually, Layer 2 traffic cannot be forwarded between ports in different VLANs. However, the Layer 2 data transmission between ports within and outside the isolation group is supported.

Configuring a Port Isolation Group

Select **Security** > **Port Isolate Group** from the navigation tree and in the page that appears, click the **Modify** tab to enter the page shown in Figure 1-1.

Figure 1-1 Configure a port isolation group



Config type ● 🟦Isolate port ○ 🟩Uplink-port

Table 1-1 describes the port isolation group configuration items.

Table 1-1 Port isolation group configuration items

Item	Description
Config type	Specify the role of the port or ports in the isolation group. • Isolate port: Assign the port or ports to the isolation group as an isolated port or ports. • Uplink-port: Assign the port to the isolation group as the uplink port. **Highlight** *The uplink port is not supported on 3Com Switch 2900.series*
Select port(s)	Select the port(s) you want to assign to the isolation group. You can click ports on the chassis front panel for selection; if aggregation interfaces are configured, they will be listed under the chassis panel for selection.

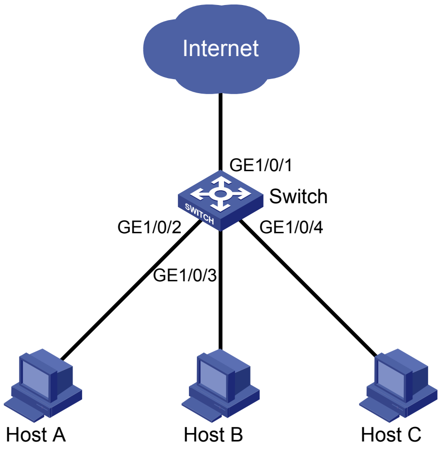
Port Isolation Group Configuration Example

Network requirements

- Campus network users Host A, Host B, and Host C are connected to GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 of Switch.
- Switch is connected to the Internet through GigabitEthernet 1/0/1.
- GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 belong to the same VLAN.

It is required that Host A, Host B, and Host C can access the Internet while being isolated from one another.

Figure 1-2 Networking diagram for port isolation group configuration

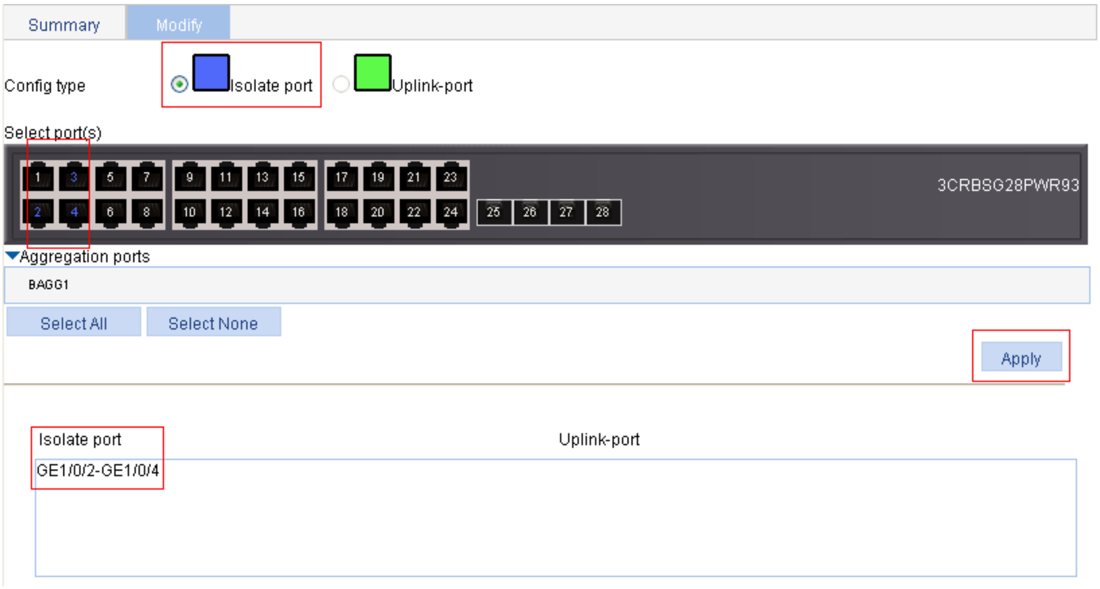


Configuration procedure

# Assign GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to an isolation group as isolated ports.

Select **Security** > **Port Isolate Group** from the navigation tree and in the page that appears, click the **Modify** tab to enter the page shown in Figure 1-3.

Figure 1-3 Configure isolated ports for an isolation group



Config type: ● 🟦 Isolate port ○ 🟩 Uplink-port

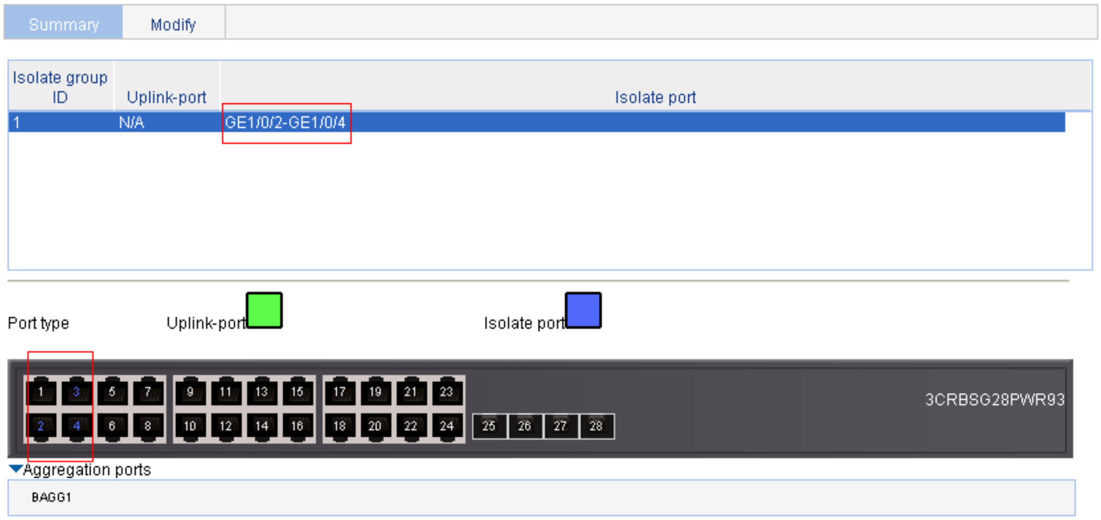
Isolate port	Uplink-port
GE1/0/2-GE1/0/4	

- Select **Isolate port** for the port type.
- Select GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 on the chassis front panel.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

# View information about the isolation group.

Click **Summary**. The page shown in Figure 1-4 appears.

Figure 1-4 Information about port isolation group 1



Isolate group ID	Uplink-port	Isolate port
1	N/A	GE1/0/2-GE1/0/4

Port type: Uplink-port 🟩 Isolate port 🟦

As shown on the page, port isolation group 1 contains these isolated ports: GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.

Table of Contents

1 Authorized IP Configuration

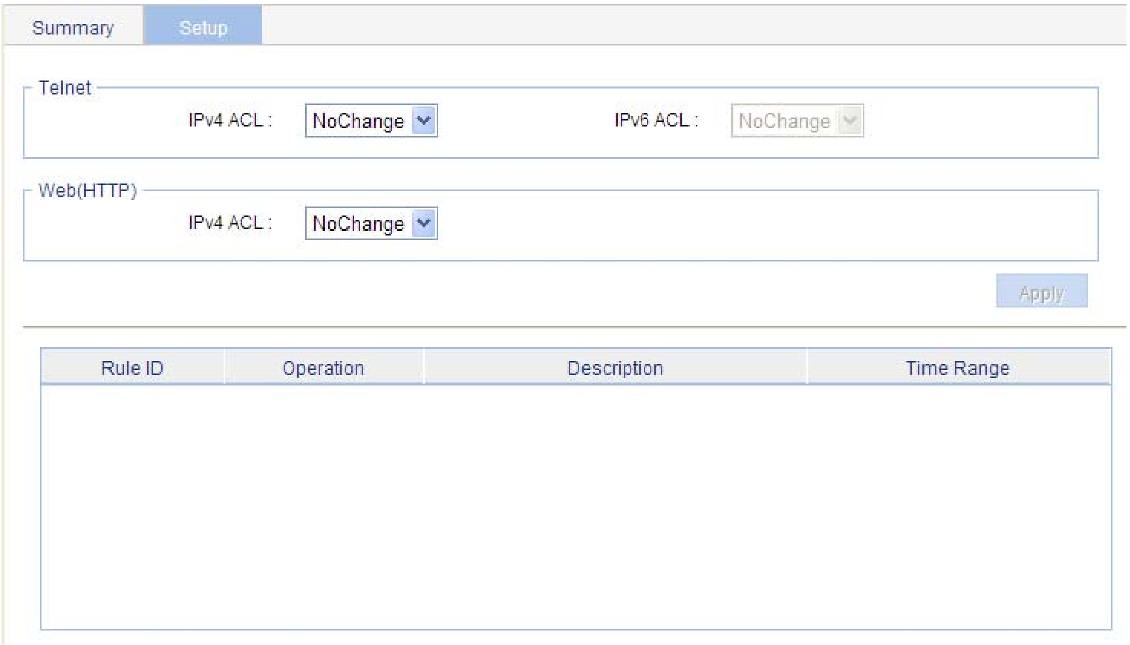
Overview

The authorized IP function is to associate the HTTP or Telnet service with an ACL to filter the requests of clients. Only the clients that pass the ACL filtering can access the device.

Configuring Authorized IP

Select **Security** > **Authorized IP** from the navigation tree, and then click the **Setup** tab to enter the authorized IP configuration page, as shown in Figure 1-1.

Figure 1-1 Authorized IP configuration page



Telnet

IPv4 ACL : NoChange

IPv6 ACL : NoChange

Web(HTTP)

IPv4 ACL : NoChange

Rule ID	Operation	Description	Time Range

Table 1-1 describes the authorized IP configuration items.

Table 1-1 Authorized IP configuration items

Item		Description
Telnet	IPv4 ACL	Associate the Telnet service with an IPv4 ACL. You can configure the IPv4 ACL to be selected by selecting **QoS** > **ACL IPv4**.
	IPv6 ACL(Not Supported)	Associate the Telnet service with an IPv6 ACL. You can configure the IPv6 ACL to be selected by selecting **QoS** > **ACL IPv6**.
Web (HTTP)	IPv4 ACL	Associate the HTTP service with an IPv4 ACL. You can configure the IPv4 ACL to be selected by selecting **QoS** > **ACL IPv4**.

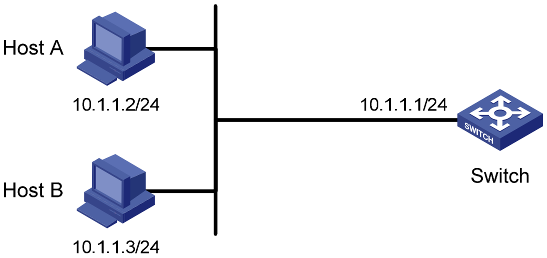
Authorized IP Configuration Example

Authorized IP Configuration Example

Network requirements

In Figure 1-2, configure Switch to deny telnet and HTTP requests from Host A , while permit telnet and HTTP requests from Host B.

Figure 1-2 Network diagram for authorized IP

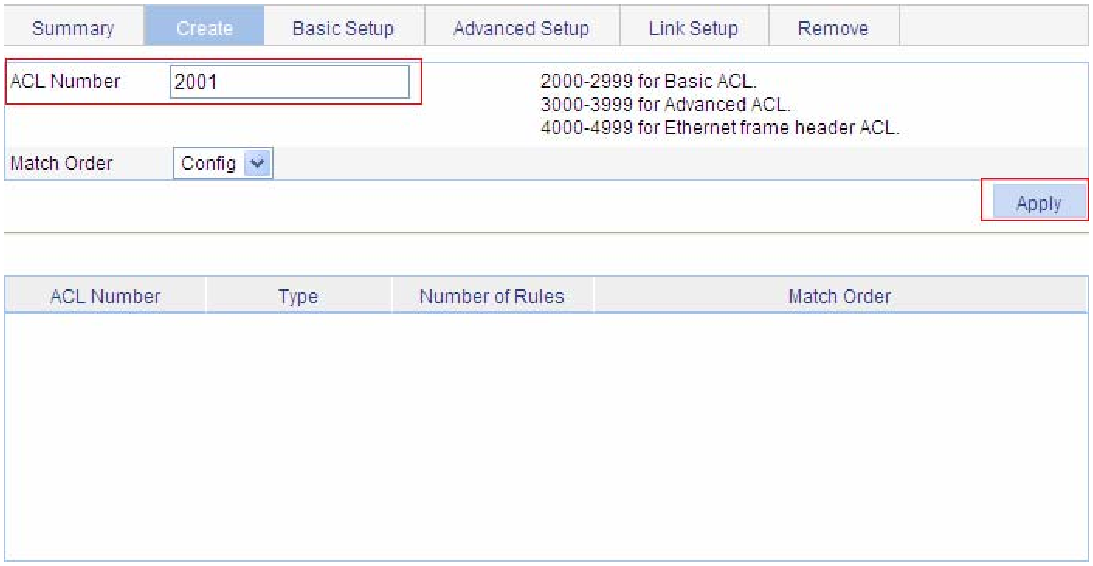


Configuration procedure

# Create an ACL.

- Select **QoS** > **ACL IPv4** from the navigation tree and then click the **Create** tab to enter the ACL configuration page shown in Figure 1-3.

Figure 1-3 Create an ACL



ACL Number: 2001

2000-2999 for Basic ACL.
3000-3999 for Advanced ACL.
4000-4999 for Ethernet frame header ACL.

Match Order: Config

ACL Number	Type	Number of Rules	Match Order

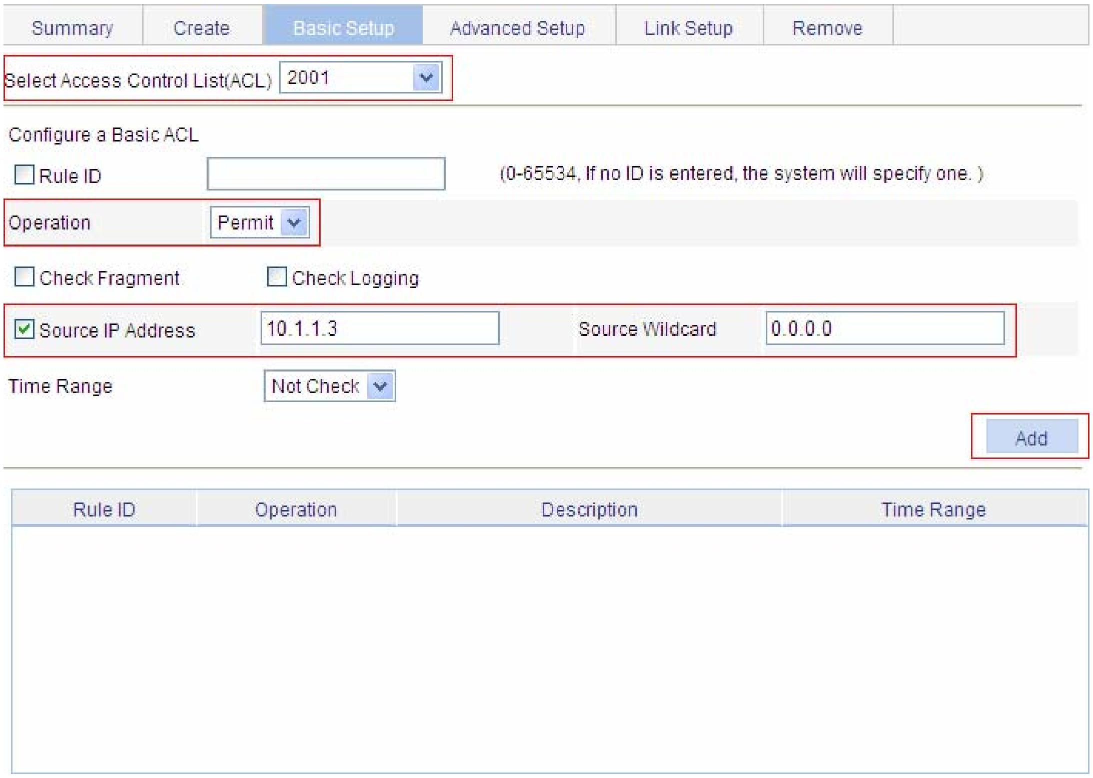
Make the following configurations on the page:

- Type **2001** for **ACL Number**.
- Click **Apply**.

# Configure an ACL rule to permit Host B.

- Click the **Basic Setup** tab to enter the page shown in Figure 1-4.

Figure 1-4 Configure an ACL rule to permit Host B



Select Access Control List(ACL) 2001

Configure a Basic ACL

□ Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit

□ Check Fragment □ Check Logging

☑ Source IP Address 10.1.1.3 Source Wildcard 0.0.0.0

Time Range Not Check

Rule ID	Operation	Description	Time Range

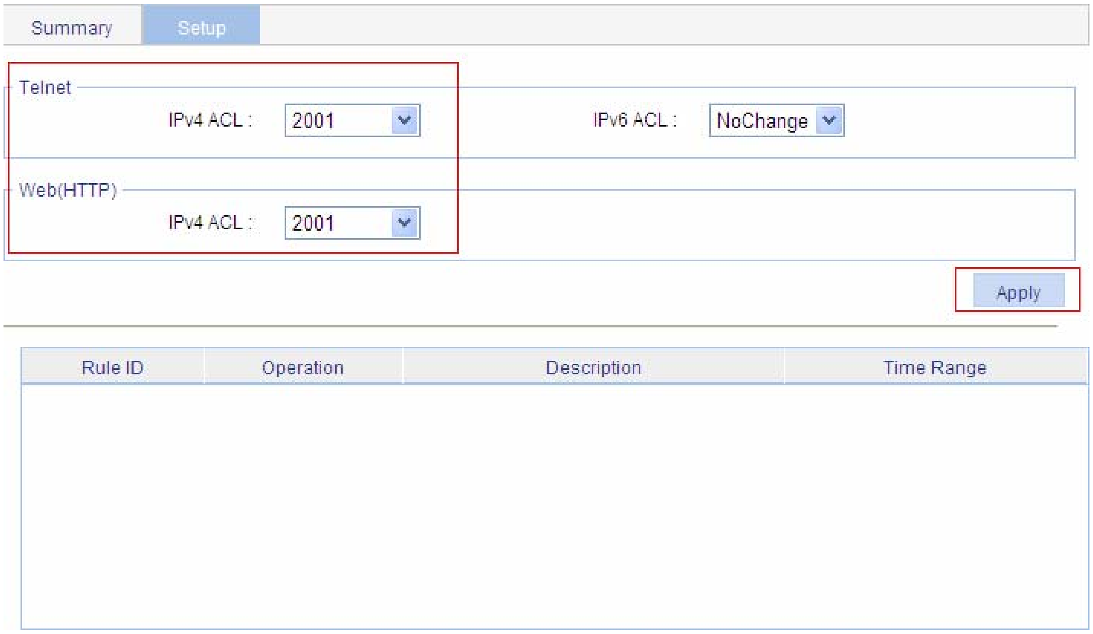
Make the following configurations on the page:

- Select 2001 from the **Select Access Control List (ACL)** drop-down list.
- Select **Permit** from the **Operation** drop-down list.
- Select the **Source IP Address** check box and then type **10.1.1.3**.
- Type **0.0.0.0** in the **Source Wildcard** text box.
- Click **Add**.

# Configure authorized IP.

- Select **Security** > **Authorized IP** from the navigation tree and then click the **Setup** tab to enter the authorized IP configuration page shown in Figure 1-5.

Figure 1-5 Configure authorized IP



Telnet

IPv4 ACL : 2001

IPv6 ACL : NoChange

Web(HTTP)

IPv4 ACL : 2001

Make the following configurations on the page:

- Select **2001** for **IPv4 ACL** in the **Telnet** field.
- Select **2001** for **IPv4 ACL** in the **Web(HTTP)** field.
- Click **Apply**.

Table of Contents

1 ACL Configuration

ACL Overview

With the growth of network scale and network traffic, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal access to networks and to control network traffic and save network resources. One way to implement packet filtering is to use access control lists (ACLs).

An ACL is a set of rules (or a set of permit or deny statements) for determining which packets can pass and which ones should be rejected based on matching criteria such as source address, destination address, and port number. ACLs are widely used with technologies such as QoS, where traffic identification is desired.

Introduction to IPv4 ACL

IPv4 ACL Classification

IPv4 ACLs, identified by ACL numbers, fall into three categories, as shown in Table 1-1.

Table 1-1 IPv4 ACL categories

Category	ACL number	Matching criteria
Basic IPv4 ACL	2000 to 2999	Source IP address
Advanced IPv4 ACL	3000 to 3999	Source IP address, destination IP address, protocol carried over IP, and other Layer 3 or Layer 4 protocol header information
Ethernet frame header ACL	4000 to 4999	Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p precedence, and link layer protocol type

IPv4 ACL Match Order

An ACL may consist of multiple rules, which specify different matching criteria. These criteria may have overlapping or conflicting parts. The match order is for determining how packets should be matched against the rules.

There are two types of IPv4 ACL match orders:

- **config**: Packets are compared against ACL rules in the order that the rules are configured.
- **auto**: Packets are compared against ACL rules in the depth-first match order.

The term depth-first match has different meanings for different types of IPv4 ACLs, as shown in Table 1-2.

Table 1-2 Depth-first match for IPv4 ACLs

IPv4 ACL category	Depth-first match procedure
Basic IPv4 ACL	1) Sort rules by source IP address wildcard mask and compare packets against the rule configured with more zeros in the source IP address wildcard mask. 2) In case of a tie, compare packets against the rule configured first.
Advanced IPv4 ACL	1) Sort rules by the protocol carried over IP. A rule with no limit to the protocol type (that is, configured with the **ip** keyword) has the lowest precedence. Rules each of which has a single specified protocol type are of the same precedence level. 2) If the protocol types have the same precedence, look at the source IP address wildcard mask. Then, compare packets against the rule configured with more zeros in the source IP address wildcard mask. 3) If the numbers of zeros in the source IP address wildcard masks are the same, look at their destination IP address wildcard masks. Then, compare packets against the rule configured with more zeros in the destination IP address wildcard mask. 4) If the numbers of zeros in the destination IP address wildcard masks are the same, look at the Layer 4 port number ranges, namely the TCP/UDP port number ranges. Then compare packets against the rule configured with the smaller port number range. 5) If the port number ranges are the same, compare packets against the rule configured first.
Ethernet frame header ACL	1) Sort rules by source MAC address mask first and compare packets against the rule configured with more ones in the source MAC address mask. 2) If two rules are present with the same number of ones in their source MAC address masks, look at the destination MAC address masks. Then, compare packets against the rule configured with more ones in the destination MAC address mask. 3) If the numbers of ones in the destination MAC address masks are the same, compare packets against the one configured first.

The comparison of a packet against ACL rules stops immediately after a match is found. The packet is then processed as per the rule.

Fragments Filtering with IPv4 ACLs

Traditional packet filtering performs match operation on only the first fragments. All non-first fragments are permitted. This results in security risks, because attackers may exploit this vulnerability to fabricate non-first fragments to attack your network.

As for the configuration of a rule of an IPv4 ACL, you can specify that the rule applies to non-first fragment packets only, and does not apply to non-fragment packets or the first fragment packets. ACL rules that do not contain this keyword is applicable to both non-fragment packets and fragment packets.

Effective Period of an ACL

You can control when a rule can take effect by referencing a time range in the rule.

A referenced time range can be one that has not been created yet. The rule, however, can take effect only after the time range is defined and becomes active.

ACL Step

Note

Currently, the Web interface does not support ACL step configuration.

Meaning of the step

The step defines the difference between two neighboring numbers that are automatically assigned to ACL rules by the device. For example, with a step of 5, rules are automatically numbered 0, 5, 10, 15, and so on. By default, the step is 5.

Whenever the step changes, the rules are renumbered, starting from 0. For example, if four rules are numbered 0, 5, 10, and 15 respectively, changing the step from 5 to 2 will cause the rules to be renumbered 0, 2, 4, and 6.

Benefits of using the step

With the step and rule numbering/renumbering mechanism, you do not need to assign numbers to rules when defining them. The system will assign a newly defined rule a number that is the smallest multiple of the step bigger than the current biggest number. For example, with a step of five, if the biggest number is currently 28, the newly defined rule will get a number of 30. If the ACL has no rule defined already, the first defined rule will get a number of 0.

Another benefit of using the step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, and 15 in an ACL with a step of five, you can insert a rule numbered 1.

Configuring an ACL

Configuration Task List

Configuring an IPv4 ACL

Table 1-3 lists the IPv4 ACL configuration tasks.

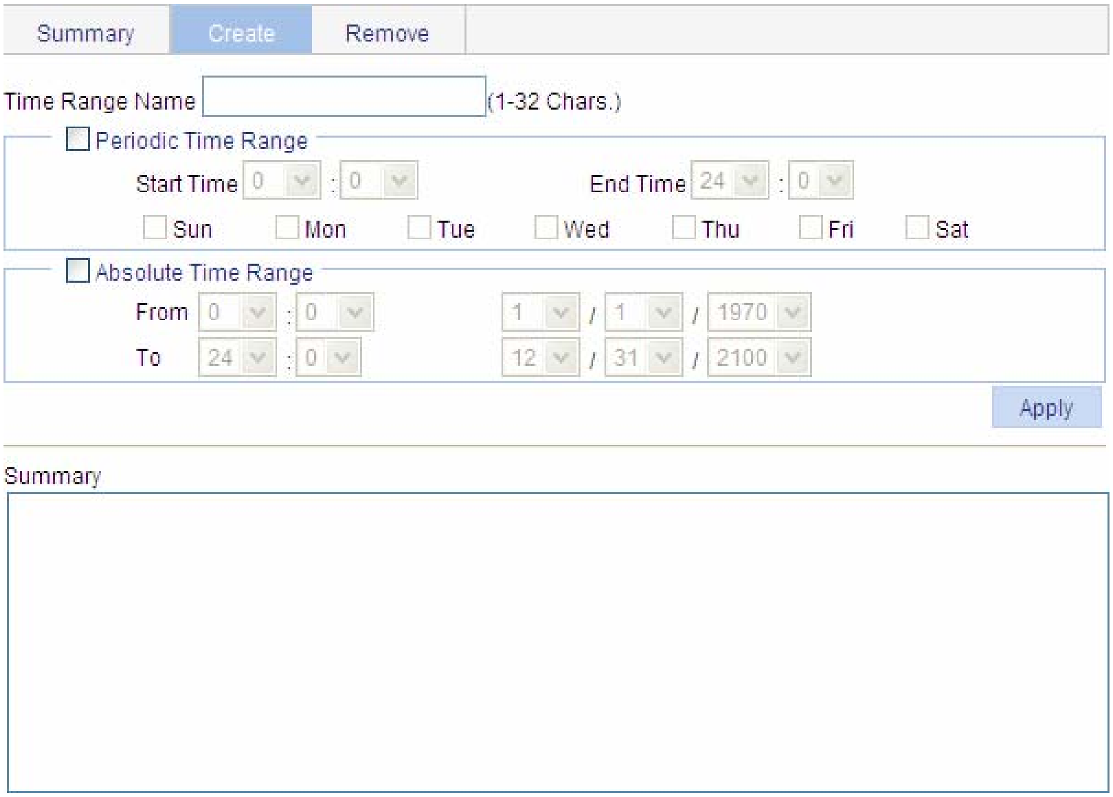
Table 1-3 IPv4 ACL configuration task list

Task	Remarks
Configuring a Time Range	Optional A rule referencing a time range takes effect only during the specified time range.
Creating an IPv4 ACL	Required The category of the created ACL depends on the ACL number that you specify.
Configuring a Rule for a Basic IPv4 ACL	Required Complete one of the three tasks according to the ACL category.
Configuring a Rule for an Advanced IPv4 ACL	
Configuring a Rule for an Ethernet Frame Header ACL	

Configuring a Time Range

Select **QoS** > **Time Range** from the navigation tree and then select the **Create** tab to enter the time range configuration page, as shown in Figure 1-1.

Figure 1-1 The page for creating a time range



Summary | Create | Remove

Time Range Name [ ] (1-32 Chars.)

□ Periodic Time Range

Start Time 0 : 0   End Time 24 : 0

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

□ Absolute Time Range

From 0 : 0   1 / 1 / 1970

To 24 : 0   12 / 31 / 2100

Apply

Summary

Table 1-4 describes the configuration items for creating a time range.

Table 1-4 Time range configuration items

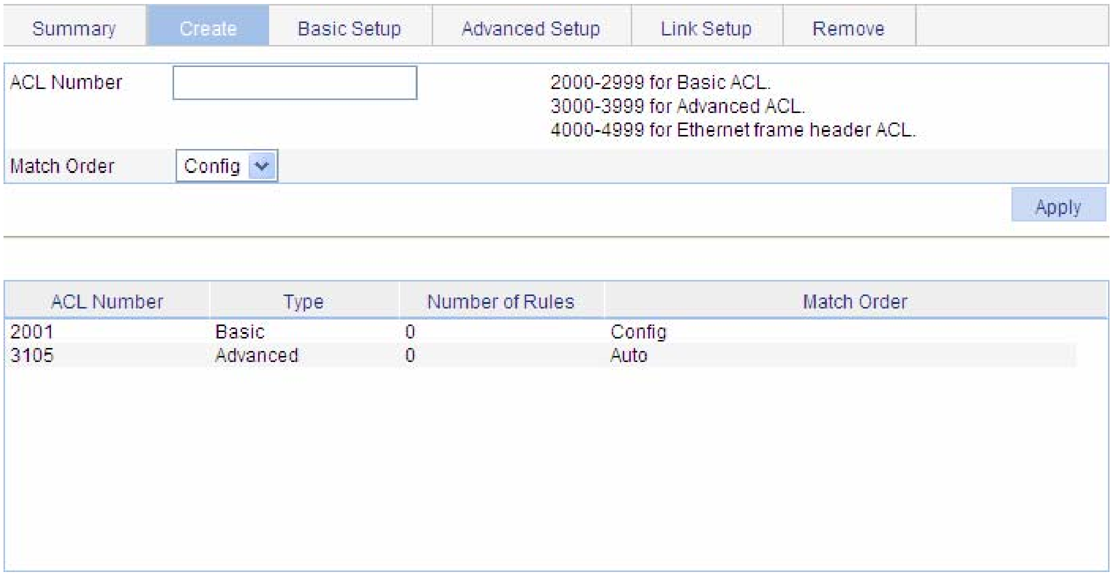
Item		Description	
Time Range Name		Set the name for the time range.	
Periodic Time Range	Start Time	Set the start time of the periodic time range.	You can define both a periodic time range and an absolute time range to create a compound time range. This compound time range recurs on the day or days of the week only within the specified period.
	End Time	Set the end time of the periodic time range. The end time must be greater than the start time.	
	Sun, Mon, Tue, Wed, Thu, Fri, and Sat.	Select the day or days of the week on which the periodic time range is valid. You can select any combination of the days of the week.	
Absolute Time Range	From	Set the start time and date of the absolute time range. The time of the day is in the *hh*:*mm* format (24-hour clock), and the date is in the *MM*/*DD*/*YYYY* format.	
	To	Set the end time and date of the absolute time range. The time of the day is in the *hh*:*mm* format (24-hour clock), and the date is in the *MM*/*DD*/*YYYY* format. The end time must be greater than the start time.	

Return to IPv4 ACL configuration task list.

Creating an IPv4 ACL

Select **QoS** > **ACL IPv4** from the navigation tree and then select the **Create** tab to enter the IPv4 ACL configuration page, as shown in Figure 1-2.

Figure 1-2 The page for creating an IPv4 ACL



ACL Number

2000-2999 for Basic ACL.
3000-3999 for Advanced ACL.
4000-4999 for Ethernet frame header ACL.

Match Order: Config

ACL Number	Type	Number of Rules	Match Order
2001	Basic	0	Config
3105	Advanced	0	Auto

Table 1-5 describes the configuration items for creating an IPv4 ACL.

Table 1-5 IPv4 ACL configuration items

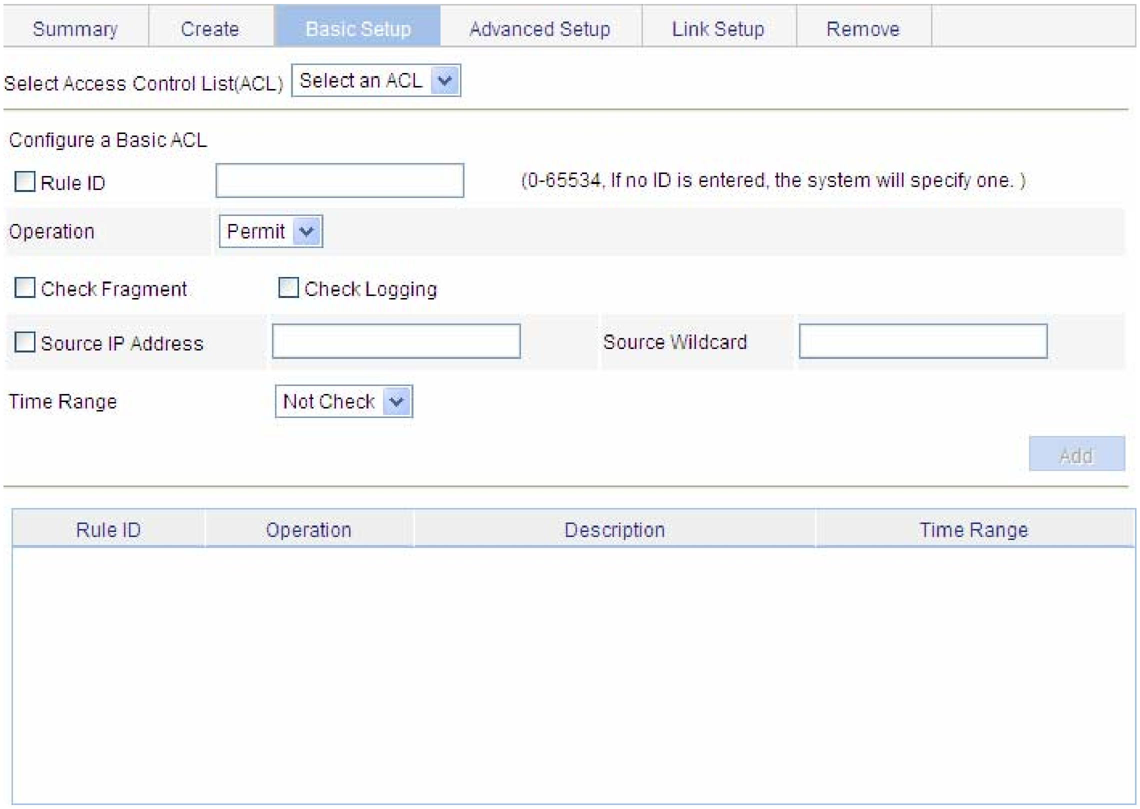
Item	Description
ACL Number	Set the number of the IPv4 ACL.
Match Order	Set the match order of the ACL. Available values are: • **Config**: Packets are compared against ACL rules in the order that the rules are configured. • **Auto**: Packets are compared against ACL rules in the depth-first match order.

Return to IPv4 ACL configuration task list.

Configuring a Rule for a Basic IPv4 ACL

Select **QoS** > **ACL IPv4** from the navigation tree and then select the **Basic Setup** tab to enter the rule configuration page for a basic IPv4 ACL, as shown in Figure 1-3.

Figure 1-3 The page for configuring an basic IPv4 ACL



Select Access Control List(ACL) Select an ACL

Configure a Basic ACL

□ Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit

□ Check Fragment □ Check Logging

□ Source IP Address Source Wildcard

Time Range Not Check

Rule ID	Operation	Description	Time Range

Table 1-6 describes the configuration items for creating a rule for a basic IPv4 ACL.

Table 1-6 Configuration items for a basic IPv4 ACL rule

Item	Description
Select Access Control List (ACL)	Select the basic IPv4 ACL for which you want to configure rules. Available ACLs are basic IPv4 ACLs that have been configured.
Rule ID	Select the **Rule ID** option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.
Operation	Select the operation to be performed for IPv4 packets matching the rule. ● **Permit**: Allows matched packets to pass. ● **Deny**: Drops matched packets.
Check Fragment	Select this option to apply the rule to only non-first fragments. If you do no select this option, the rule applies to all fragments and non-fragments.
Check Logging	Select this option to keep a log of matched IPv4 packets. A log entry contains the ACL rule number, operation for the matched packets, protocol that IP carries, source/destination address, source/destination port number, and number of matched packets.
Source IP Address	Select the **Source IP Address** option and type a source IPv4 address and a wildcard mask, in dotted decimal notation.
Source Wildcard	

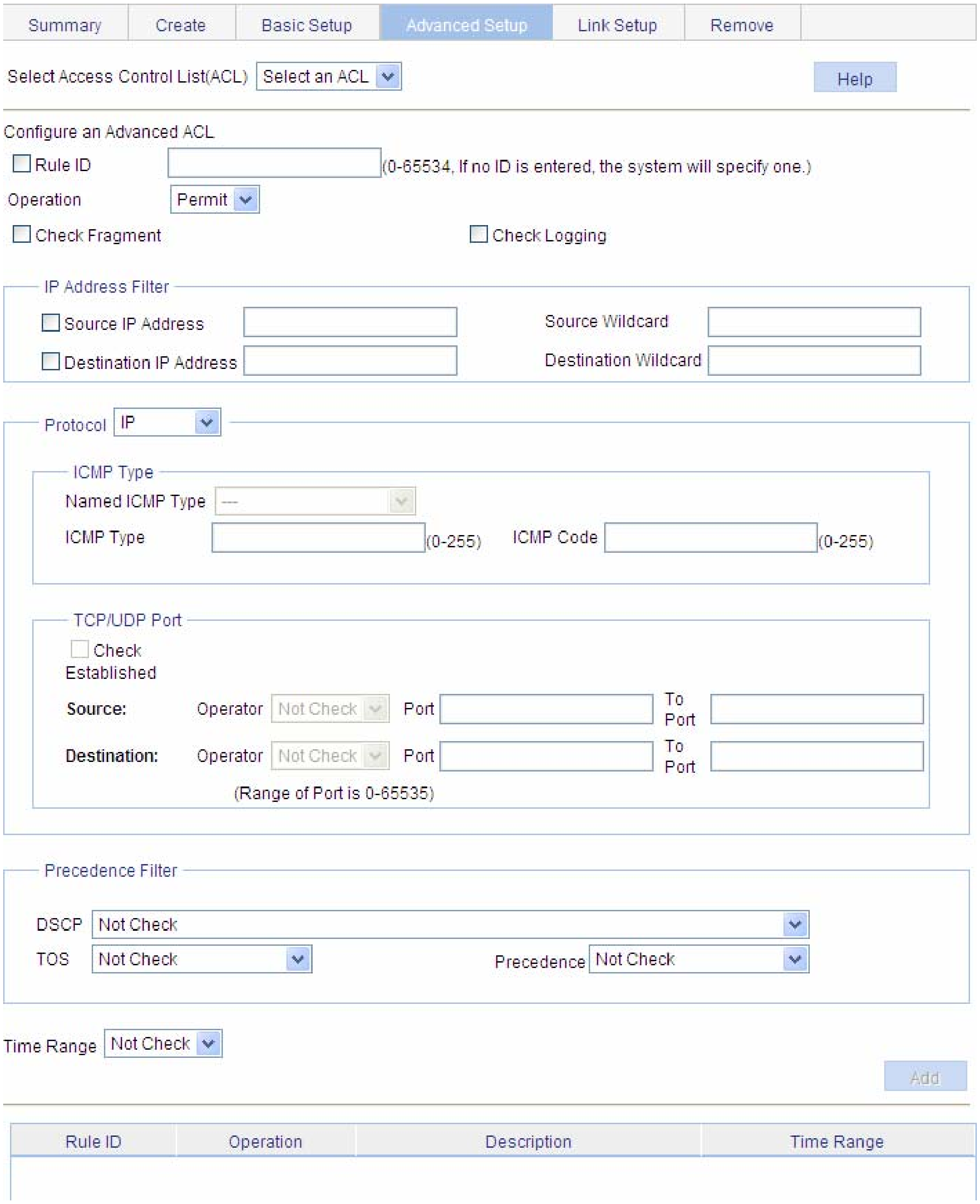
Item	Description
Time Range	Select the time range during which the rule takes effect. Available time ranges are those that have been configured.

Return to IPv4 ACL configuration task list.

Configuring a Rule for an Advanced IPv4 ACL

Select **QoS** > **ACL IPv4** from the navigation tree and then select the **Advance Setup** tab to enter the rule configuration page for an advanced IPv4 ACL, as shown in Figure 1-4.

Figure 1-4 The page for configuring an advanced IPv4 ACL



Select Access Control List(ACL) Select an ACL

Configure an Advanced ACL

□ Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit

□ Check Fragment

□ Check Logging

IP Address Filter

□ Source IP Address

Source Wildcard

□ Destination IP Address

Destination Wildcard

Protocol IP

ICMP Type

Named ICMP Type ---

ICMP Type (0-255)

ICMP Code (0-255)

TCP/UDP Port

□ Check Established

Source: Operator Not Check Port To Port

Destination: Operator Not Check Port To Port

(Range of Port is 0-65535)

Precedence Filter

DSCP Not Check

TOS Not Check

Precedence Not Check

Time Range Not Check

Rule ID	Operation	Description	Time Range

Table 1-7 describes the configuration items for creating a rule for an advanced IPv4 ACL.

Table 1-7 Configuration items for an advanced IPv4 ACL rule

Item		Description
Select Access Control List (ACL)		Select the advanced IPv4 ACL for which you want to configure rules. Available ACLs are advanced IPv4 ACLs that have been configured.
Rule ID		Select the **Rule ID** option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.
Operation		Select the operation to be performed for packets matching the rule. ● **Permit**: Allows matched packets to pass. ● **Deny**: Drops matched packets.
Check Fragment		Select this option to apply the rule to only non-first fragments. If you do no select this option, the rule applies to all fragments and non-fragments.
Check Logging		Select this option to keep a log of matched packets. A log entry contains the ACL rule number, operation for the matched packets, protocol that IP carries, source/destination address, source/destination port number, and number of matched packets.
IP Address Filter	Source IP Address	Select the **Source IP Address** option and type a source IPv4 address and a source wildcard mask, in dotted decimal notation.
	Source Wildcard	
	Destination IP Address	Select the **Source IP Address** option and type a source IP address and a source wildcard mask, in dotted decimal notation.
	Destination Wildcard	
Protocol		Select the protocol to be carried by IP. If you select **1 ICMP**, you can configure the ICMP message type and code; if you select **6 TCP** or **17 UDP**, you can configure the TCP or UDP port.
ICMP Type	Named ICMP Type	Specify the ICMP message type and code. These items are available only when you select **1 ICMP** from the **Protocol** drop-down box. If you select **Other** from the **Named ICMP Type** drop-down box, you need to type values in the **ICMP Type** and **ICMP Code** fields. Otherwise, the two fields will take the default values, which cannot be changed.
	ICMP Type	
	ICMP Code	

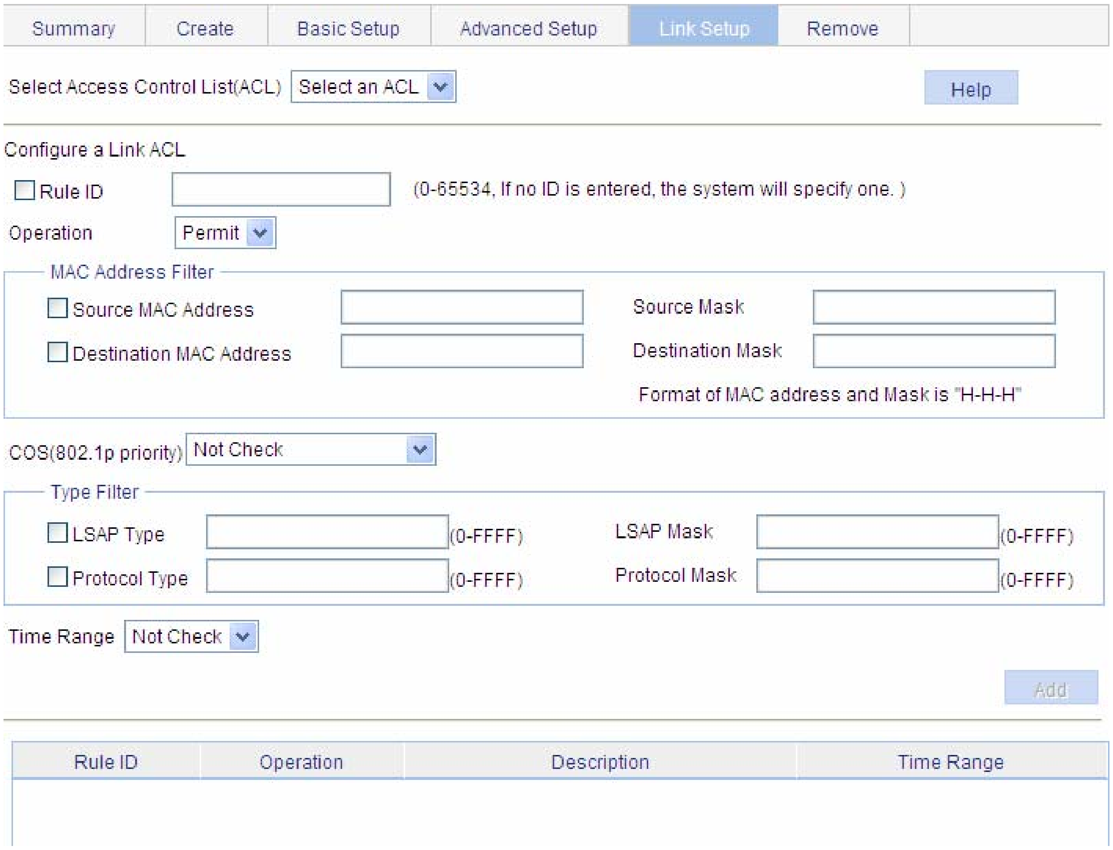
Item			Description	
TCP/UDP Port	Check Established		Select this option to make the rule match packets used for establishing and maintaining TCP connections. These items are available only when you select **6 TCP** from the **Protocol** drop-down box.	
	Source	Operator	Select the operators and type the source port numbers and destination port numbers as required. These items are available only when you select **6 TCP** or **17 UDP** from the **Protocol** drop-down box. Different operators have different configuration requirements for the port number fields: • **Not Check**: The following port number fields cannot be configured. • **Range**: The following port number fields must be configured to define a port range. • Other values: The first port number field must be configured and the second must not.	
		Port		
		To Port		
	Destination	Operator		
		Port		
		To Port		
Precedence Filter	DSCP		Specify the DSCP priority.	💡 **Highlight** *If you specify the ToS precedence or IP precedence when you specify the DSCP precednece, the specified TOS or IP precedence does not take effect.*
	TOS		Specify the ToS preference.	
	Precedence		Specify the IP precedence.	
Time Range			Select the time range during which the rule takes effect. Available time ranges are those that have been configured.	

Return to IPv4 ACL configuration task list.

Configuring a Rule for an Ethernet Frame Header ACL

Select **QoS** > **ACL IPv4** from the navigation tree and then select the **Link Setup** tab to enter the rule configuration page for an Ethernet frame header IPv4 ACL, as shown in Figure 1-5.

Figure 1-5 The page for configuring a rule for an Ethernet frame header ACL



Select Access Control List(ACL) Select an ACL

Configure a Link ACL

□ Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit

MAC Address Filter

□ Source MAC Address Source Mask

□ Destination MAC Address Destination Mask

Format of MAC address and Mask is "H-H-H"

COS(802.1p priority) Not Check

Type Filter

□ LSAP Type (0-FFFF) LSAP Mask (0-FFFF)

□ Protocol Type (0-FFFF) Protocol Mask (0-FFFF)

Time Range Not Check

Rule ID	Operation	Description	Time Range

Table 1-8 describes the configuration items for creating a rule for an Ethernet frame header IPv4 ACL.

Table 1-8 Configuration items for an Ethernet frame header IPv4 ACL rule

Item		Description
Select Access Control List (ACL)		Select the Ethernet frame header IPv4 ACL for which you want to configure rules. Available ACLs are Ethernet frame header IPv4 ACLs that have been configured.
Rule ID		Select the **Rule ID** option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.
Operation		Select the operation to be performed for packets matching the rule. ● **Permit**: Allows matched packets to pass. ● **Deny**: Drops matched packets.
MAC Address Filter	Source MAC Address	Select the **Source MAC Address** option and type a source MAC address and a mask.
	Source Mask	
	Destination MAC Address	Select the **Destination MAC Address** option and type a destination MAC address and a mask.
	Destination Mask	
COS(802.1p precedence)		Specify the 802.1p precedence for the rule.

Item		Description
Type Filter	Protocol Type	Select the **Protocol Type** option and specify the link layer protocol type by configuring the following two items: • **Protocol Type**: Indicates the frame type. It corresponds to the type-code field of Ethernet_II and Ethernet_SNAP frames. • **Protocol Mask**: Indicates the protocol mask.
	Protocol Mask	
Time Range		Select the time range during which the rule takes effect. Available time ranges are those that have been configured.

Return to IPv4 ACL configuration task list.

Configuration Guidelines

When configuring an ACL, note that:

1) When defining rules in an ACL, you do not necessarily assign them numbers; the system can do this automatically. Refer to ACL Step.
2) You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
3) You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

2 QoS Configuration

Introduction to QoS

Quality of Service (QoS) reflects the ability of a network to meet customer needs. In an internet, QoS evaluates the ability of the network to forward packets of different services.

The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

Networks Without QoS Guarantee

On traditional IP networks without QoS guarantee, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, and so on.

This service policy is only suitable for applications insensitive to bandwidth and delay, such as Word Wide Web (WWW) and E-Mail.

QoS Requirements of New Applications

The Internet has been growing along with the fast development of networking technologies.

Besides traditional applications such as WWW, E-Mail and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together with VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet.

These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For example, videoconference and VoD require high bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require high bandwidth but do require low delay and preferential service during congestion.

The emerging applications demand higher service performance of IP networks. Better network services during packets forwarding are required, such as providing dedicated bandwidth, reducing packet loss ratio, managing and avoiding congestion, and regulating network traffic. To meet these requirements, networks must provide more improved services.

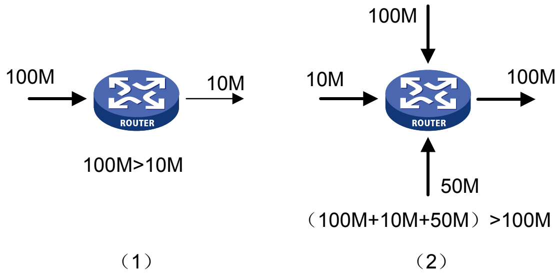
Congestion: Causes, Impacts, and Countermeasures

Network congestion is a major factor contributed to service quality degrading on a traditional network. Congestion is a situation where the forwarding rate decreases due to insufficient resources, resulting in extra delay.

Causes

Congestion easily occurs in complex packet switching circumstances in the Internet. The following figure shows two common cases:

Figure 2-1 Traffic congestion causes



- The traffic enters a device from a high speed link and is forwarded over a low speed link.
- The packet flows enter a device from several incoming interfaces and are forwarded out an outgoing interface, whose rate is smaller than the total rate of these incoming interfaces.

When traffic arrives at the line speed, a bottleneck is created at the outgoing interface causing congestion.

Besides bandwidth bottlenecks, congestion can be caused by resource shortage in various forms such as insufficient processor time, buffer, and memory, and by network resource exhaustion resulting from excessive arriving traffic in certain periods.

Impacts

Congestion may bring these negative results:

- Increased delay and jitter during packet transmission
- Decreased network throughput and resource use efficiency
- Network resource (memory in particular) exhaustion and even system breakdown

It is obvious that congestion hinders resource assignment for traffic and thus degrades service performance. Congestion is unavoidable in switched networks and multi-user application environments. To improve the service performance of your network, you must address the congestion issues.

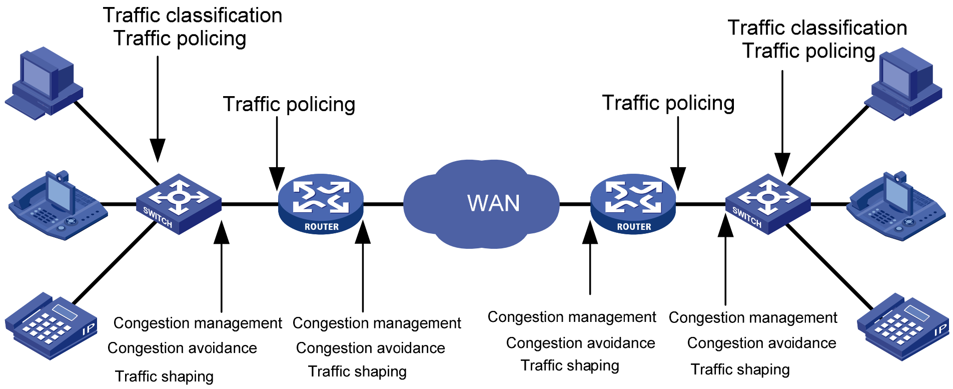
Countermeasures

A simple solution for congestion is to increase network bandwidth, however, it cannot solve all the problems that cause congestion because you cannot increase network bandwidth infinitely.

A more effective solution is to provide differentiated services for different applications through traffic control and resource allocation. In this way, resources can be used more properly. During resources allocation and traffic control, the direct or indirect factors that might cause network congestion should be controlled to reduce the probability of congestion. Once congestion occurs, resource allocation should be performed according to the characteristics and demands of applications to minimize the effects of congestion.

End-to-End QoS

Figure 2-2 End-to-end QoS model



As shown in Figure 2-2, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions:

- Traffic classification uses certain match criteria to organize packets with different characteristics into different classes. Traffic classification is usually applied in the inbound direction of a port.
- Traffic policing polices particular flows entering or leaving a device according to configured specifications and can be applied in both inbound and outbound directions of a port. When a flow exceeds the specification, some restriction or punishment measures can be taken to prevent overconsumption of network resources.
- Traffic shaping proactively adjusts the output rate of traffic to adapt traffic to the network resources of the downstream device and avoid unnecessary packet drop and congestion. Traffic shaping is usually applied in the outbound direction of a port.
- Congestion management provides a resource scheduling policy to arrange the forwarding sequence of packets when congestion occurs. Congestion management is usually applied in the outbound direction of a port.
- Congestion avoidance monitors the usage status of network resources and is usually applied in the outbound direction of a port. As congestion becomes worse, it actively reduces the amount of traffic by dropping packets.

Among these QoS technologies, traffic classification is the basis for providing differentiated services. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services.

Traffic Classification

When defining match criteria for classifying traffic, you can use IP precedence bits in the type of service (ToS) field of the IP packet header, or other header information such as IP addresses, MAC addresses, IP protocol field and port numbers. You can define a class for packets with the same quintuple (source address, source port number, protocol number, destination address and destination port number for example), or for all packets to a certain network segment.

When packets are classified on the network boundary, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be directly adopted to classify the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream network can either adopt the classification results from its upstream network or classify the packets again according to its own criteria.

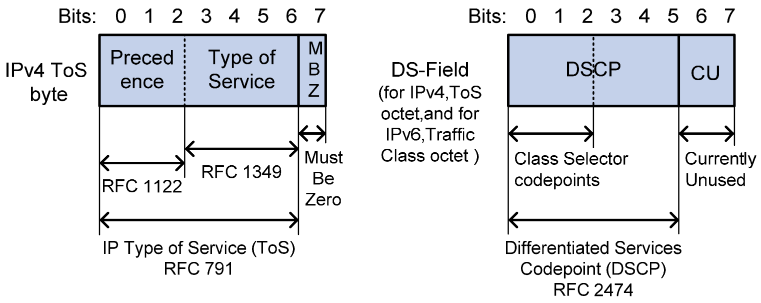
To provide differentiated services, traffic classes must be associated with certain traffic control actions or resource allocation actions. What traffic control actions to adopt depends on the current phase and the resources of the network. For example, CAR is adopted to police packets when they enter the network; GTS is performed on packets when they flow out of the node; queue scheduling is performed when congestion happens; congestion avoidance measures are taken when the congestion deteriorates.

Packet Precedences

This section introduces IP precedence, ToS precedence, differentiated services codepoint (DSCP) values, and 802.1p precedence.

1) IP precedence, ToS precedence, and DSCP values

Figure 2-3 DS field and ToS bytes


Bits: 0 1 2 3 4 5 6 7
IPv4 ToS byte
Preced ence
Type of Service
M B Z
RFC 1122
RFC 1349
Must Be Zero
IP Type of Service (ToS) RFC 791
Bits: 0 1 2 3 4 5 6 7
DS-Field (for IPv4,ToS octet,and for IPv6,Traffic Class octet)
DSCP
CU
Class Selector codepoints
Currently Unused
Differentiated Services Codepoint (DSCP) RFC 2474

As shown in Figure 2-3, the ToS field of the IP header contains eight bits: the first three bits (0 to 2) represent IP precedence from 0 to 7; the subsequent four bits (3 to 6) represent a ToS value from 0 to 15. According to RFC 2474, the ToS field of the IP header is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved.

Table 2-1 Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

In a network in the Diff-Serve model, traffic is grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets are forwarded regardless of link share of other traffic. The class is suitable for preferential services requiring low delay, low packet loss, low jitter, and high bandwidth.
- Assured forwarding (AF) class: This class is divided into four subclasses (AF 1 to AF 4), each containing three drop priorities for more granular classification. The QoS level of the AF class is lower than that of the EF class.
- Class selector (CS) class: This class is derived from the IP ToS field and includes eight subclasses;
- Best effort (BE) class: This class is a special CS class that does not provide any assurance. AF traffic exceeding the limit is degraded to the BE class. Currently, all IP network traffic belongs to this class by default.

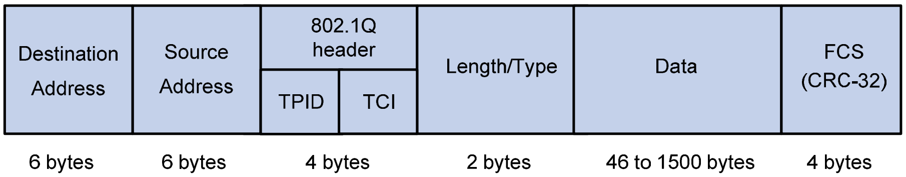
Table 2-2 Description on DSCP values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

2) 802.1p precedence

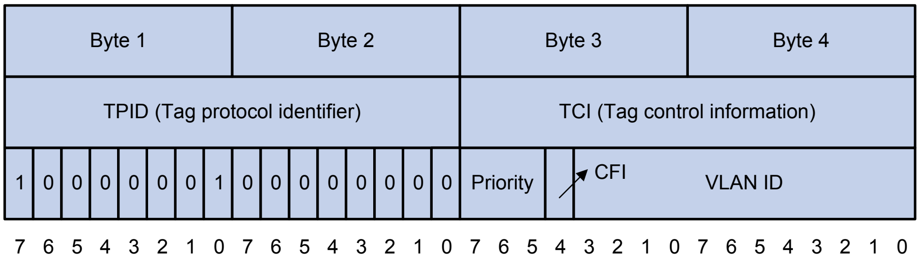
802.1p precedence lies in Layer 2 packet headers and is applicable to occasions where Layer 3 header analysis is not needed and QoS must be assured at Layer 2.

Figure 2-4 An Ethernet frame with an 802.1Q tag header



As shown in Figure 2-4, the 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). Figure 2-5 presents the format of the 802.1Q tag header.

Figure 2-5 802.1Q tag header



The priority in the 802.1Q tag header is called 802.1p precedence, because its use is defined in IEEE 802.1p. Table 2-3 presents the values for 802.1p precedence.

Table 2-3 Description on 802.1p precedence

802.1p precedence (decimal)	802.1p precedence (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

Queue Scheduling

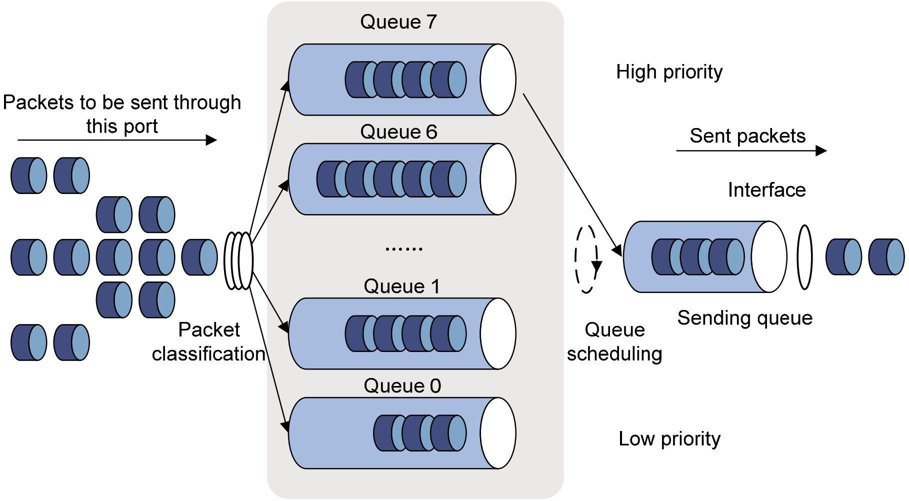
In general, congestion management adopts queuing technology. The system uses a certain queuing algorithm for traffic classification, and then uses a certain precedence algorithm to send the traffic. Each queuing algorithm is used to handle a particular network traffic problem and has significant impacts on bandwidth resource assignment, delay, and jitter.

In this section, two common hardware queue scheduling algorithms Strict Priority (SP) queuing and Weighted Round Robin (WRR) queuing are introduced.

SP queuing

SP queuing is specially designed for mission-critical applications, which require preferential service to reduce response delay when congestion occurs.

Figure 2-6 Schematic diagram for SP queuing



A typical switch provides eight queues per port. As shown in Figure 2-6, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

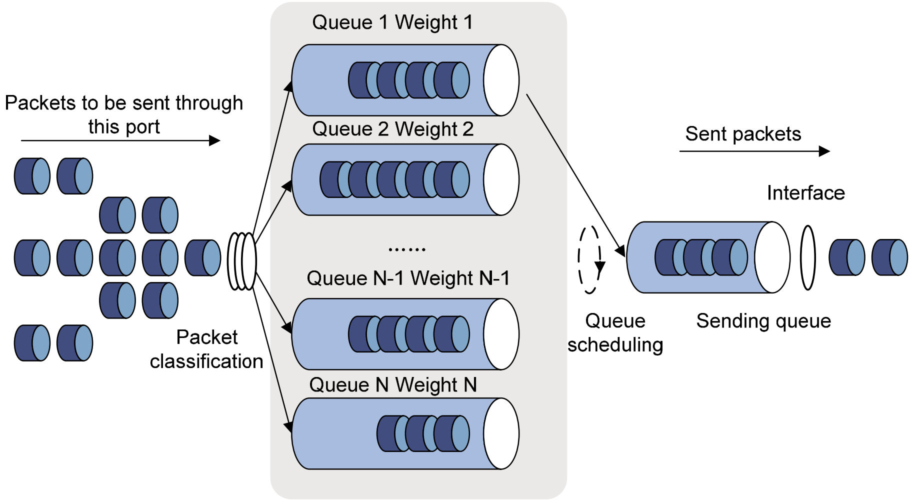
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. Thus, you can assign mission-critical packets to the high priority queue to ensure that they are always served first and common service (such as Email) packets to the low priority queues to be transmitted when the high priority queues are empty.

The disadvantage of SP queuing is that packets in the lower priority queues cannot be transmitted if there are packets in the higher priority queues. This may cause lower priority traffic to starve to death.

WRR queuing

WRR queuing schedules all the queues in turn to ensure that every queue can be served for a certain time, as shown in Figure 2-7.

Figure 2-7 Schematic diagram for WRR queuing



A typical switch provides eight output queues per port. WRR assigns each queue a weight value (represented by w7, w6, w5, w4, w3, w2, w1, or w0) to decide the proportion of resources assigned to the queue. On a 100 Mbps port, you can set the weight values of WRR queuing to 50, 30, 10, 10, 50, 30, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 respectively). In this way, the queue with the lowest priority is assured of at least 5 Mbps of bandwidth, thus avoiding the disadvantage of SP queuing that packets in low-priority queues may fail to be served for a long time.

Another advantage of WRR queuing is that while the queues are scheduled in turn, the service time for each queue is not fixed, that is, if a queue is empty, the next queue will be scheduled immediately. This improves bandwidth resource use efficiency.

You can assign the output queues to WRR priority queue group 1 and WRR priority queue group 2. Round robin queue scheduling is performed for group 1 first. If group 1 is empty, round robin queue scheduling is performed for group 2.

Note

You can implement SP+WRR queue scheduling on a port by assigning some queues on the port to the SP scheduling group when configuring WRR. Packets in the SP scheduling group are scheduled preferentially by SP. When the SP scheduling group is empty, the other queues are scheduled by WRR.

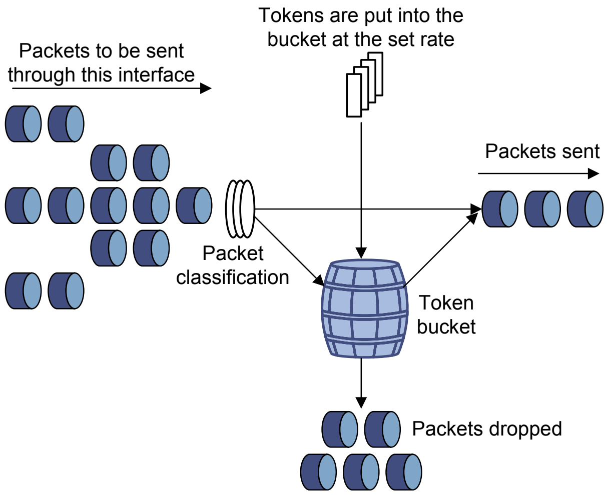
Line Rate

Line rate is a traffic control method using token buckets. The line rate of a physical interface specifies the maximum rate for forwarding packets (including critical packets). Line rate can limit all the packets passing a physical interface.

Traffic evaluation and token bucket

A token bucket can be considered as a container holding a certain number of tokens. The system puts tokens into the bucket at a set rate. When the token bucket is full, the extra tokens will overflow.

Figure 2-8 Evaluate traffic with the token bucket


Tokens are put into the bucket at the set rate
Packets to be sent through this interface
Packets sent
Packet classification
Token bucket
Packets dropped

The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets (generally, one token is associated with a 1-bit forwarding authority), the traffic conforms to the specification, and the traffic is called conforming traffic; otherwise, the traffic does not conform to the specification, and the traffic is called excess traffic.

A token bucket has the following configurable parameters:

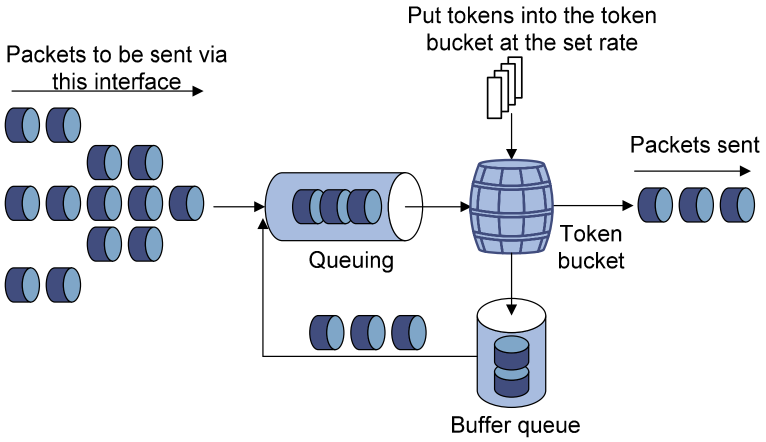
- Mean rate: At which tokens are put into the bucket, namely, the permitted average rate of traffic. It is usually set to the committed information rate (CIR).
- Burst size: the capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is usually set to the committed burst size (CBS). The set burst size must be greater than the maximum packet size.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic conforms to the specification and the corresponding tokens for forwarding the packet are taken away; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excessive.

The working mechanism of line rate

With line rate configured on an interface, all packets to be sent through the interface are firstly handled by the token bucket of line rate. If there are enough tokens in the token bucket, packets can be forwarded; otherwise, packets are put into QoS queues for congestion management. In this way, the traffic passing the physical interface is controlled.

Figure 2-9 Line rate implementation


Put tokens into the token bucket at the set rate
Packets to be sent via this interface
Packets sent
Queuing
Token bucket
Buffer queue

With a token bucket used for traffic control, when there are tokens in the token bucket, the bursty packets can be transmitted; if no tokens are available, packets cannot be transmitted until new tokens are generated in the token bucket. In this way, the traffic rate is restricted to the rate for generating tokens, thus limiting traffic rate and allowing bursty traffic.

Priority Mapping

Concepts

When a packet enters a network, it is marked with a certain priority to indicate its scheduling weight or forwarding priority. Then, the intermediate nodes in the network process the packet according to the priority.

When a packet enters a device, the device assigns to the packet a set of predefined parameters (including the 802.1p precedence, DSCP values, IP precedence, and local precedence).

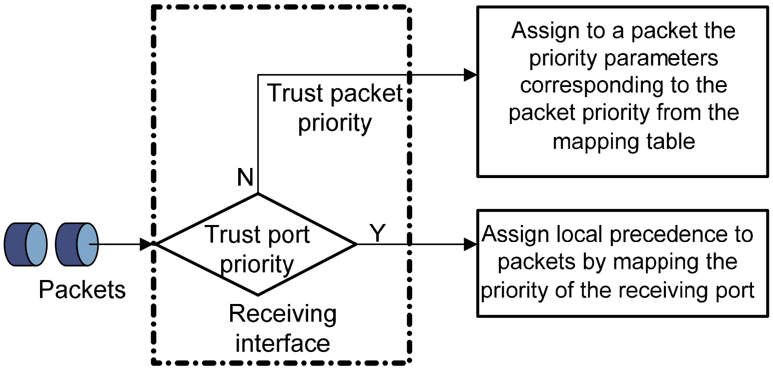
- For more information about 802.1p precedence, DSCP values, and IP precedence, refer to Packet Precedences.
- Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to an output queue. Packets with the highest local precedence are processed preferentially.

The device provides two priority trust modes on a port:

- Trust packet priority: the device assigns to the packet the priority parameters corresponding to the packet's priority from the mapping table.
- Trust port priority: the device assigns a priority to a packet by mapping the priority of the receiving port.

You can select one priority trust mode as needed. Figure 2-10 shows the process of priority mapping on a device.

Figure 2-10 Priority mapping process


Assign to a packet the priority parameters corresponding to the packet priority from the mapping table
Trust packet priority
N
Trust port priority
Y
Packets
Receiving interface
Assign local precedence to packets by mapping the priority of the receiving port

Introduction to Priority Mapping Tables

The device provides various types of priority mapping table, as listed below:

- **CoS to DSCP**: 802.1p-precedence-to-DSCP mapping table.
- **CoS to Queue**: 802.1p-precedence-to-local-precedence mapping table.
- **DSCP to CoS**: DSCP-to-802.1p-precedence mapping table, which is applicable to only IP packets.
- **DSCP to DSCP**: DSCP-to-DSCP mapping table, which is applicable to only IP packets.
- **DSCP to Queue**: DSCP-to-local-precedence mapping table, which is applicable to only IP packets.

Table 2-4 through Table 2-5 list the default priority mapping tables.

Table 2-4 The default CoS to DSCP/CoS to Queue mapping table

Input CoS value	Local precedence (Queue)	DSCP
0	2	0
1	0	8
2	1	16
3	3	24
4	4	32
5	5	40
6	6	48
7	7	56

Table 2-5 The default DSCP to CoS/DSCP to Queue mapping table

Input DSCP value	Local precedence (Queue)	CoS
0 to 7	0	0
8 to 15	1	1
16 to 23	2	2
24 to 31	3	3
32 to 39	4	4
40 to 47	5	5

Input DSCP value	Local precedence (Queue)	CoS
48 to 55	6	6
56 to 63	7	7

Note

In the default DSCP to DSCP mapping table, an input value yields a target value equal to it.

QoS Configuration

Configuration Task Lists

Configuring a QoS policy

A QoS policy involves three components: class, traffic behavior, and policy. You can associate a class with a traffic behavior using a QoS policy.

1) Class

Classes are used to identify traffic.

A class is identified by a class name and contains some match criteria.

You can define a set of match criteria to classify packets. The relationship between criteria can be **and** or **or**.

- and: The device considers a packet belongs to a class only when the packet matches all the criteria in the class.
- or: The device considers a packet belongs to a class as long as the packet matches one of the criteria in the class.

2) Traffic behavior

A traffic behavior, identified by a name, defines a set of QoS actions for packets.

3) Policy

You can apply a QoS policy to a port.

Applies a QoS policy to a port to regulate the inbound traffic of the port. A QoS policy can be applied to multiple ports. Only one policy can be applied in inbound direction of a port.

Perform the tasks in Table 2-6 to configure a QoS policy:

Table 2-6 QoS policy configuration task list

Task		Remarks
Configure a class	Creating a Class	Required Create a class and specify the logical relationship between the match criteria in the class.
	Configuring Classification Rules	Required Configure match criteria for the class.

Task			Remarks
Configure a traffic behavior	Creating a Traffic Behavior		Required Create a traffic behavior.
	Configuring actions for a behavior	Configuring Traffic Mirroring and Traffic Redirecting for a Traffic Behavior	Use either approach Configure various actions for the traffic behavior.
		Configuring Other Actions for a Traffic Behavior	
Configure a policy	Creating a Policy		Required Create a policy.
	Configuring Classifier-Behavior Associations for the Policy		Required Associate the traffic behavior with the class in the QoS policy. A class can be associated with only one traffic behavior in a QoS policy. Therefore, associating a class that is already associated with a traffic behavior will overwrite the old association.
Apply the policy	Applying a Policy to a Port		Required Apply the QoS policy to a port.

Configuring queue scheduling

Perform the task in Table 2-7 to configure queue scheduling.

Table 2-7 Queue scheduling configuration task list

Task	Remarks
Configuring Queue Scheduling on a Port	Optional Configure the queue scheduling mode for a port.

Configuring line rate

Perform the task in Table 2-8 to configure line rate.

Table 2-8 Line rate configuration task list

Task	Remarks
Configuring Line Rate on a Port	Required Limit the rate of incoming packets or outgoing packets of a physical port.

Configuring the priority mapping tables

Perform the task in Table 2-9 to configure the priority mapping tables:

Table 2-9 Priority mapping table configuration task list

Task	Remarks
Configuring Priority Mapping Tables	Required Set priority mapping tables.

Configuring priority trust mode

Perform the task in Table 2-10 to configure priority trust mode:

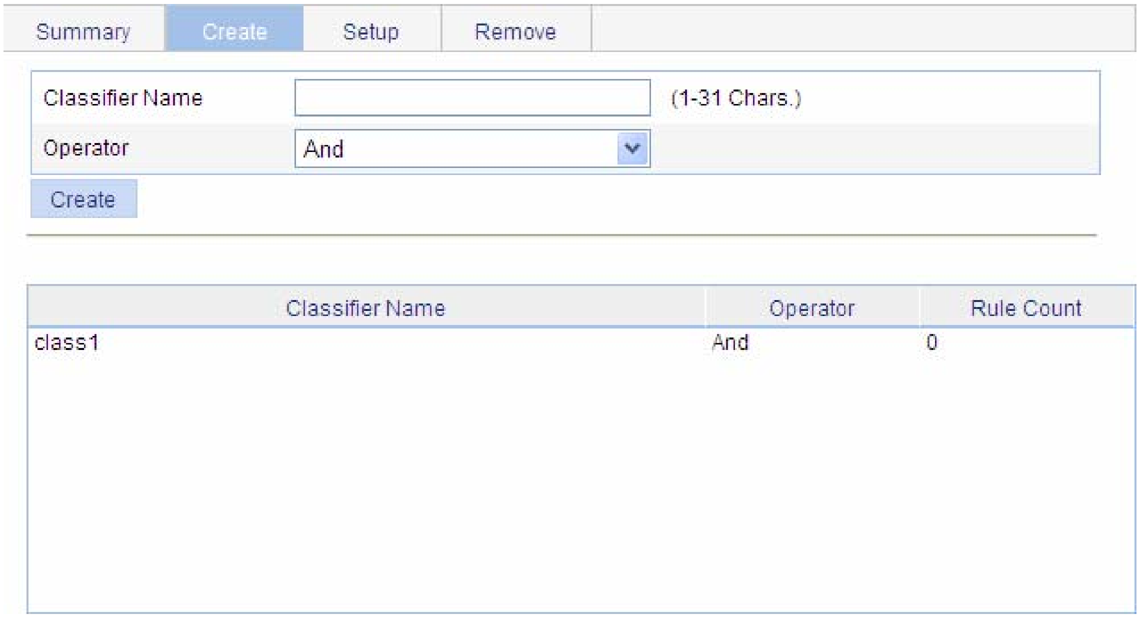
Table 2-10 Priority trust mode configuration task list

Task	Remarks
Configuring Priority Trust Mode on a Port	Required Set the priority trust mode of a port.

Creating a Class

Select **QoS** > **Classifier** from the navigation tree and click **Create** to enter the page for creating a class, as shown in Figure 2-11.

Figure 2-11 The page for creating a class



Classifier Name		(1-31 Chars.)
Operator	And	

Classifier Name	Operator	Rule Count
class1	And	0

Table 2-11 shows the configuration items of creating a class.

Table 2-11 Configuration items of creating a class

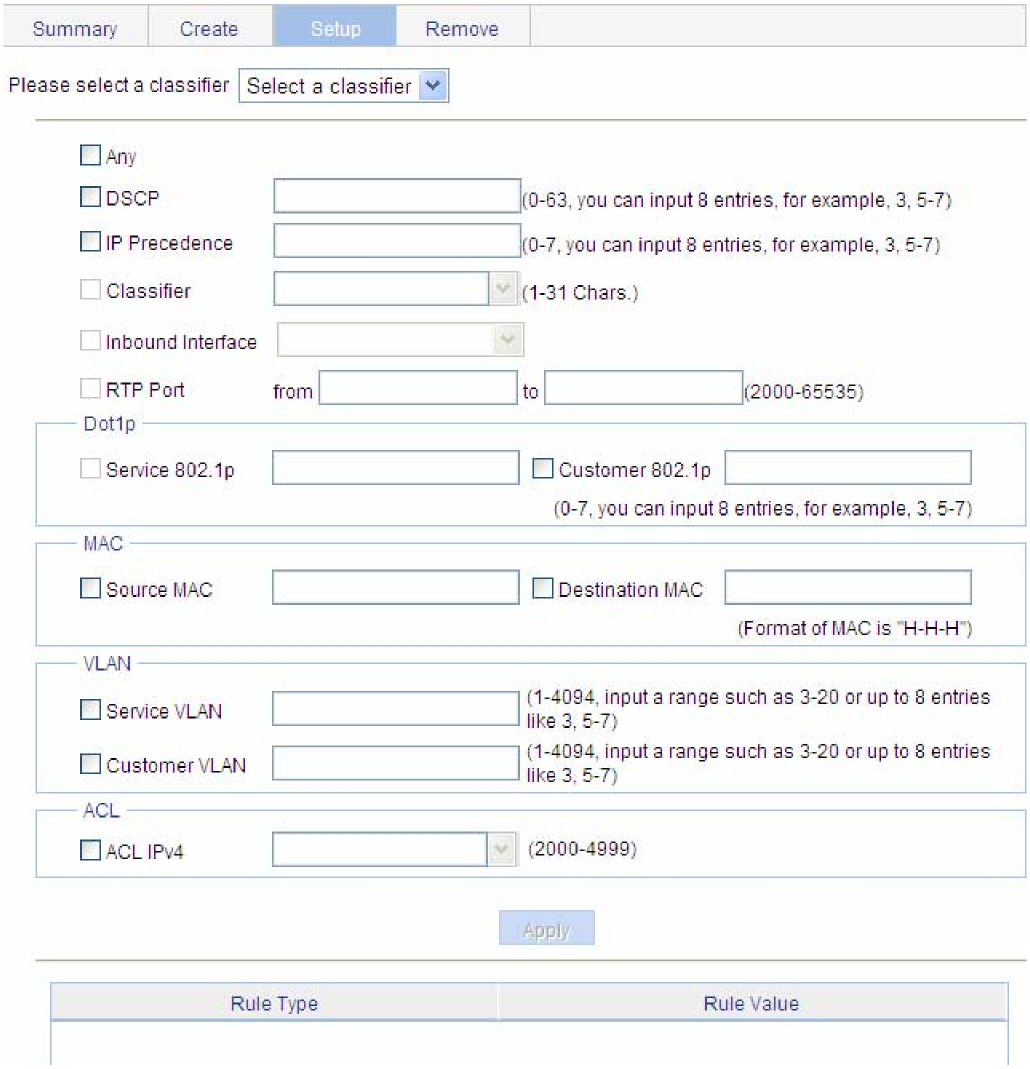
Item	Description
Classifier Name	Specify a name for the classifier to be created.
Operator	Specify the logical relationship between rules of the classifier. • **and**: Specifies the relationship between the rules in a class as logic AND. That is, the device considers a packet belongs to a class only when the packet matches all the rules in the class. • **or**: Specifies the relationship between the rules in a class as logic OR. That is, the device considers a packet belongs to a class as long as the packet matches one of the rules in the class.

Return to QoS policy configuration task list.

Configuring Classification Rules

Select **QoS** > **Classifier** from the navigation tree and click **Setup** to enter the page for setting a class, as shown in Figure 2-12.

Figure 2-12 The page for configuring classification rules



Please select a classifier: Select a classifier

□ Any

□ DSCP (0-63, you can input 8 entries, for example, 3, 5-7)

□ IP Precedence (0-7, you can input 8 entries, for example, 3, 5-7)

□ Classifier (1-31 Chars.)

□ Inbound Interface

□ RTP Port from … to … (2000-65535)

Dot1p

□ Service 802.1p □ Customer 802.1p

(0-7, you can input 8 entries, for example, 3, 5-7)

MAC

□ Source MAC □ Destination MAC

(Format of MAC is "H-H-H")

VLAN

□ Service VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

□ Customer VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

ACL

□ ACL IPv4 (2000-4999)

Rule Type	Rule Value

Table 2-12 shows the configuration items of configuring classification rules.

Table 2-12 Configuration items of configuring classification rules

Item		Description
Please select a classifier		Select an existing classifier in the drop-down list.
Any		Define a rule to match all packets. Select the option to match all packets.
DSCP		Define a rule to match DSCP values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight DSCP values each time. If multiple identical DSCP values are specified, the system considers them as one. The relationship between different DSCP values is **OR**. After such configurations, all the DSCP values are arranged in ascending order automatically.
IP Precedence		Define a rule to match IP precedence values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight IP precedence values each time. If multiple identical IP precedence values are specified, the system considers them as one. The relationship between different IP precedence values is **OR**. After such configurations, all the IP precedence values are arranged in ascending order automatically.
Customer 802.1p		Define a rule to match the customer 802.1p precedence values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight 802.1p precedence values each time. If multiple identical 802.1p precedence values are specified, the system considers them as one. The relationship between different 802.1p precedence values is **OR**. After such configurations, all the 802.1p precedence values are arranged in ascending order automatically.
MAC	Source MAC	Define a rule to match a source MAC address. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. A rule to match a source MAC address is significant only to Ethernet interfaces.
	Destination MAC	Define a rule to match a destination MAC address. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. A rule to match a destination MAC address is significant only to Ethernet interfaces.

Item		Description
VLAN	Service VLAN	Define a rule to match service VLAN IDs. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**. After such a configuration. You can specify VLAN IDs in two ways: • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. • Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.
	Customer VLAN	Define a rule to match customer VLAN IDs. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**. You can specify VLAN IDs in two ways: • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. • Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.
ACL IPv4		Define an IPv4 ACL-based rule. The ACLs available for selection are existing IPv4 ACLs.

Return to QoS policy configuration task list.

Creating a Traffic Behavior

Select **QoS** > **Behavior** from the navigation tree and click the **Create** tab to enter the page for creating a traffic behavior, as shown in Figure 2-13.

Figure 2-13 The page for creating a traffic behavior

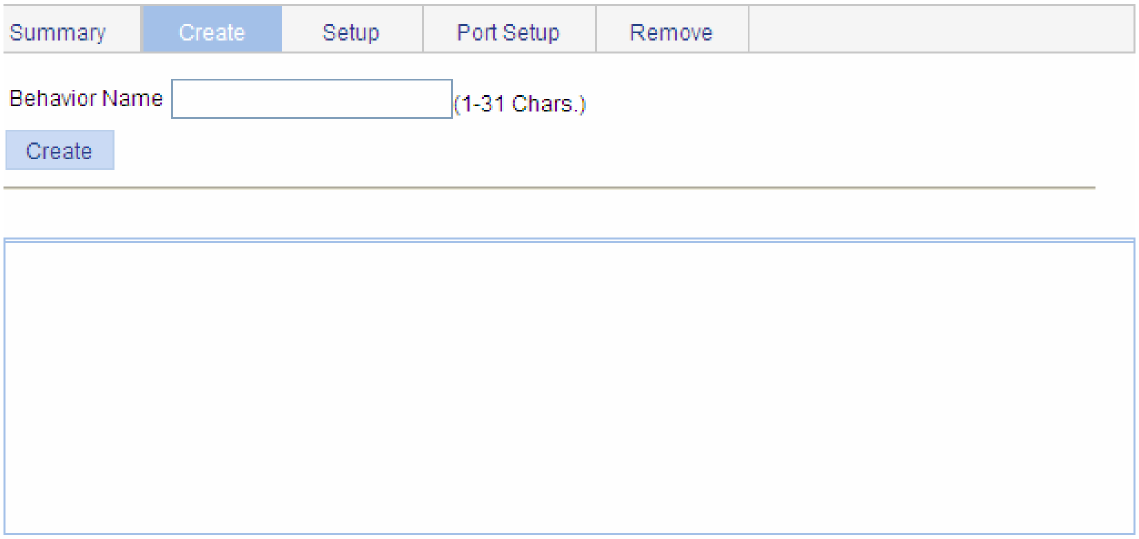


Table 2-13 describes the configuration items of creating a behavior.

Table 2-13 Configuration items of creating a behavior

Item	Description
Behavior name	Specify a name for the behavior to be created.

Return to QoS policy configuration task list.

Configuring Traffic Mirroring and Traffic Redirecting for a Traffic Behavior

Select **QoS** > **Behavior** from the navigation tree and click **Port Setup** to enter the port setup page for a traffic behavior, as shown in Figure 2-14.

Figure 2-14 Port setup page for a traffic behavior

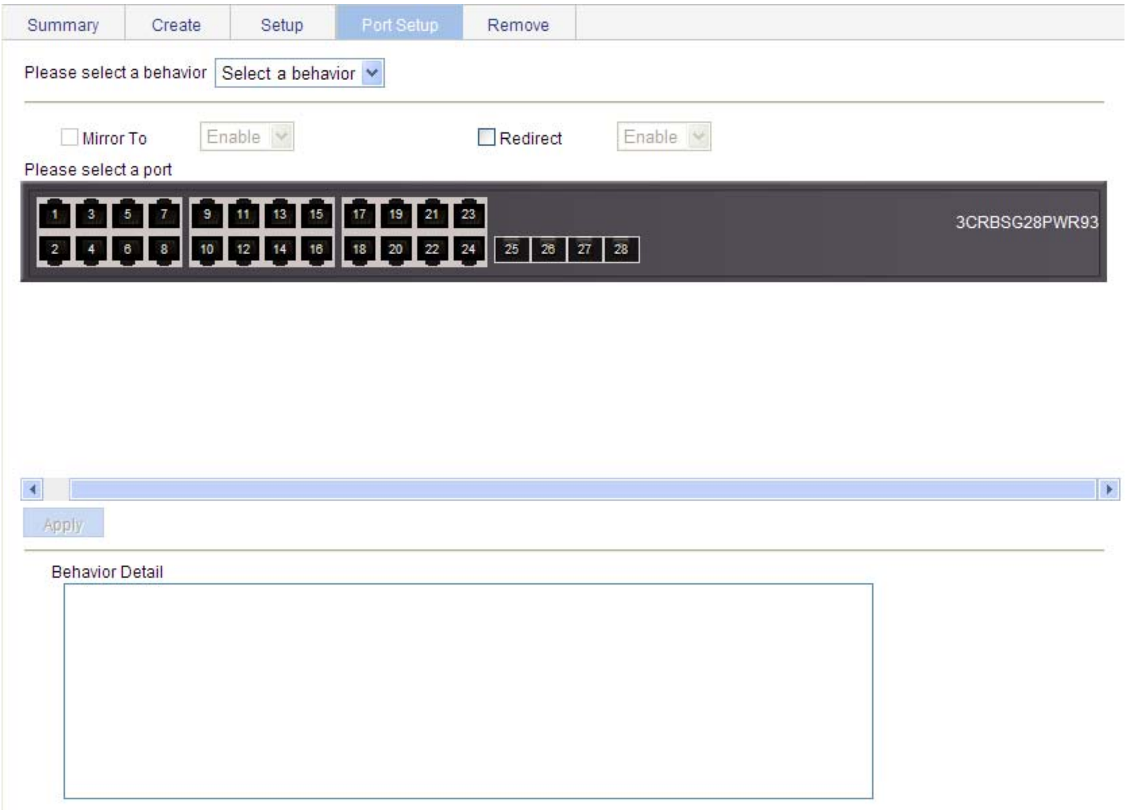


Table 2-14 describes the traffic mirroring and traffic redirecting configuration items.

Table 2-14 Traffic mirroring and traffic redirecting configuration items

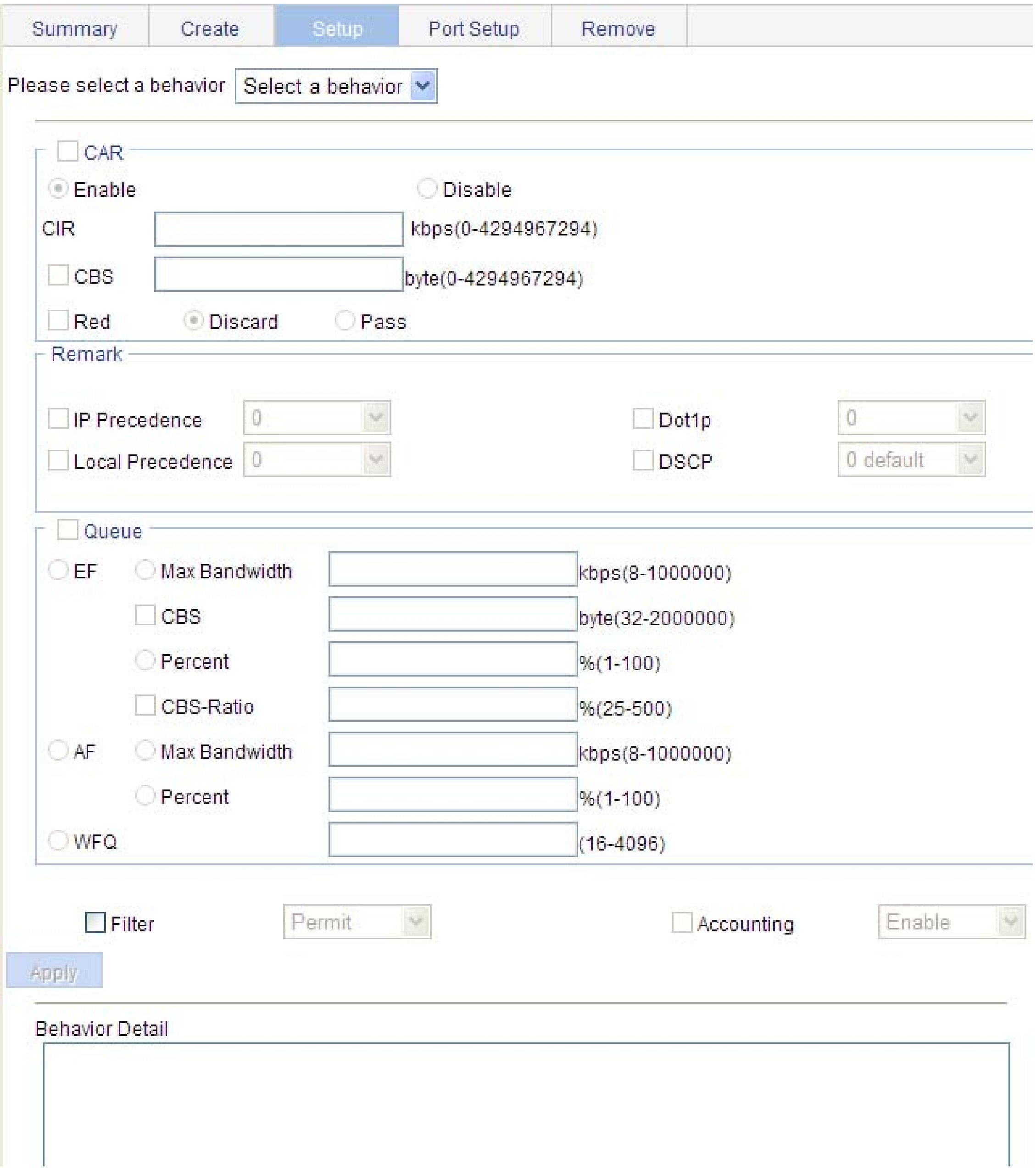
Item	Description
Please select a behavior	Select an existing behavior in the drop-down list.
Redirect	Set the action of redirecting traffic to the specified destination port.
Please select a port	Specify the port to be configured as the destination port of traffic mirroring or traffic directing on the chassis front panel.

Return to QoS policy configuration task list.

Configuring Other Actions for a Traffic Behavior

Select **QoS** > **Behavior** from the navigation tree and click **Setup** to enter the page for setting a traffic behavior, as shown in Figure 2-15.

Figure 2-15 The page for setting a traffic behavior



Please select a behavior: Select a behavior

☐ CAR

● Enable ○ Disable

CIR: kbps(0-4294967294)

☐ CBS: byte(0-4294967294)

☐ Red ● Discard ○ Pass

Remark

☐ IP Precedence: 0 ☐ Dot1p: 0

☐ Local Precedence: 0 ☐ DSCP: 0 default

☐ Queue

○ EF ○ Max Bandwidth: kbps(8-1000000)

☐ CBS: byte(32-2000000)

○ Percent: %(1-100)

☐ CBS-Ratio: %(25-500)

○ AF ○ Max Bandwidth: kbps(8-1000000)

○ Percent: %(1-100)

○ WFQ: (16-4096)

☐ Filter: Permit ☐ Accounting: Enable

Behavior Detail

Table 2-15 describes the configuration items of configuring other actions for a traffic behavior.

Table 2-15 Configuration items of configuring other actions for a traffic behavior

Item	Description
Please select a behavior	Select an existing behavior in the drop-down list.
Filter	Configure the packet filtering action. After selecting the **Filter** option, select one item in the following drop-down list: ● **Permit**: Forwards the packet. ● **Deny**: Drops the packet. ● **Not Set**: Cancels the packet filtering action.

Return to QoS policy configuration task list.

Creating a Policy

Select **QoS** > **QoS Policy** from the navigation tree and click **Create** to enter the page for creating a policy, as shown in Figure 2-16.

Figure 2-16 The page for creating a policy

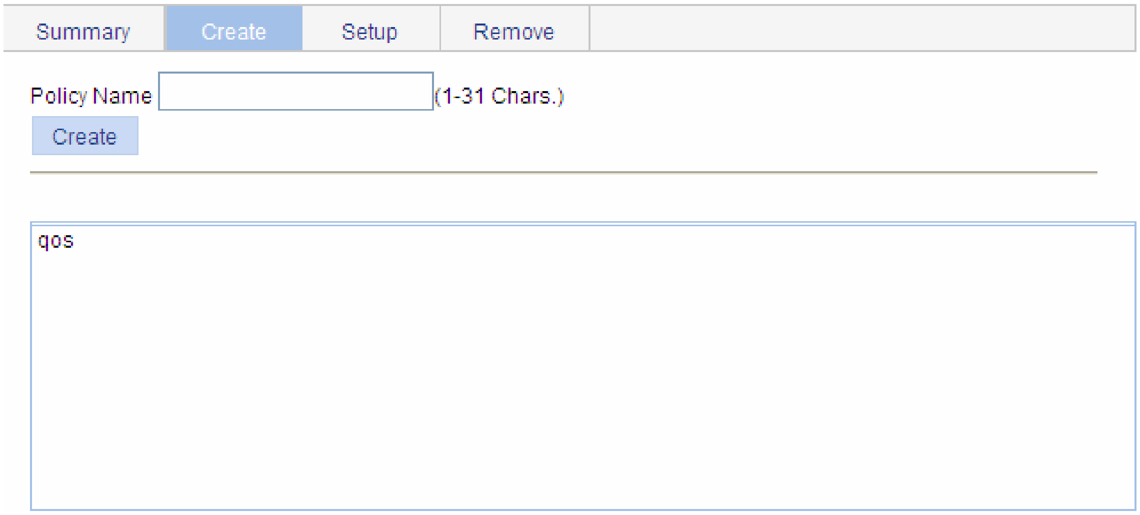


Table 2-16 describes the configuration items of creating a policy.

Table 2-16 Configuration items of creating a policy

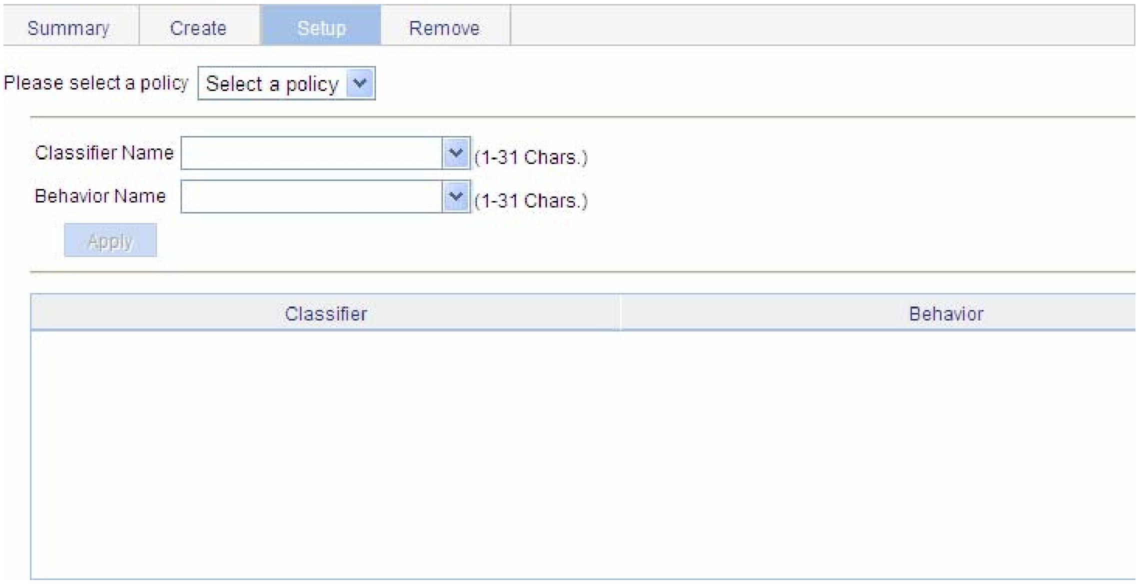
Item	Description
Policy Name	Specify a name for the policy to be created.

Return to QoS policy configuration task list.

Configuring Classifier-Behavior Associations for the Policy

Select **QoS** > **QoS Policy** from the navigation tree and click **Setup** to enter the page for setting a policy, as shown in Figure 2-17.

Figure 2-17 The page for setting a policy



Please select a policy: Select a policy

Classifier Name: (1-31 Chars.)

Behavior Name: (1-31 Chars.)

Table 2-17 describes the configuration items of configuring classifier-behavior associations for the policy.

Table 2-17 Configuration items of configuring classifier-behavior associations for the policy

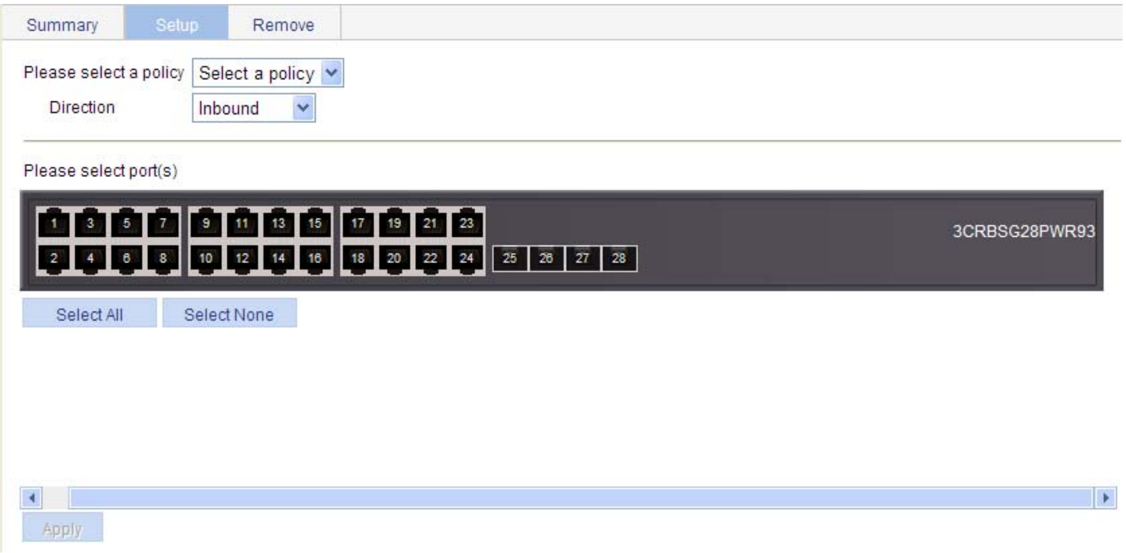
Item	Description
Please select a policy	Select a created policy in the drop-down list.
Classifier Name	Select an existing classifier in the drop-down list. The classifiers available for selection are created on the page for creating a classifier.
Behavior Name	Select an existing behavior in the drop-down list. The behaviors available for selection are created on the page for creating a behavior.

Return to QoS policy configuration task list.

Applying a Policy to a Port

Select **QoS** > **Port Policy** from the navigation tree and click **Setup** to enter the page for applying a policy to a port, as shown in Figure 2-18.

Figure 2-18 The page for applying a policy to a port



Please select a policy: Select a policy

Direction: Inbound

Please select port(s)

Table 2-18 describes the configuration items of applying a policy to a port.

Table 2-18 Configuration items of applying a policy to a port

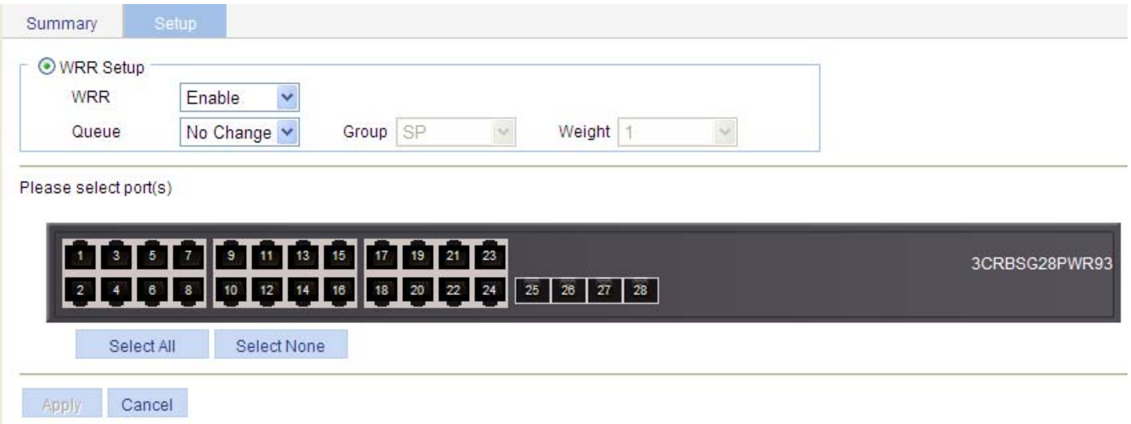
Item	Description
Please select a policy	Select a created policy in the drop-down list.
Direction	Set the direction in which the policy is to be applied. **Inbound**: Applies the policy to the incoming packets of the specified ports.
Please select port(s)	Click to select ports to which the QoS policy is to be applied on the chassis front panel.

Return to QoS policy configuration task list.

Configuring Queue Scheduling on a Port

Select **QoS** > **Queue** from the navigation tree and click **Setup** to enter the queue scheduling configuration page, as shown in Figure 2-19.

Figure 2-19 The page for configuring queue scheduling



● WRR Setup

WRR: Enable

Queue: No Change   Group: SP   Weight: 1

Please select port(s)

Table 2-19 describes the configuration items of configuring queue scheduling on a port.

Table 2-19 Configuration items of configuring queue scheduling on a port

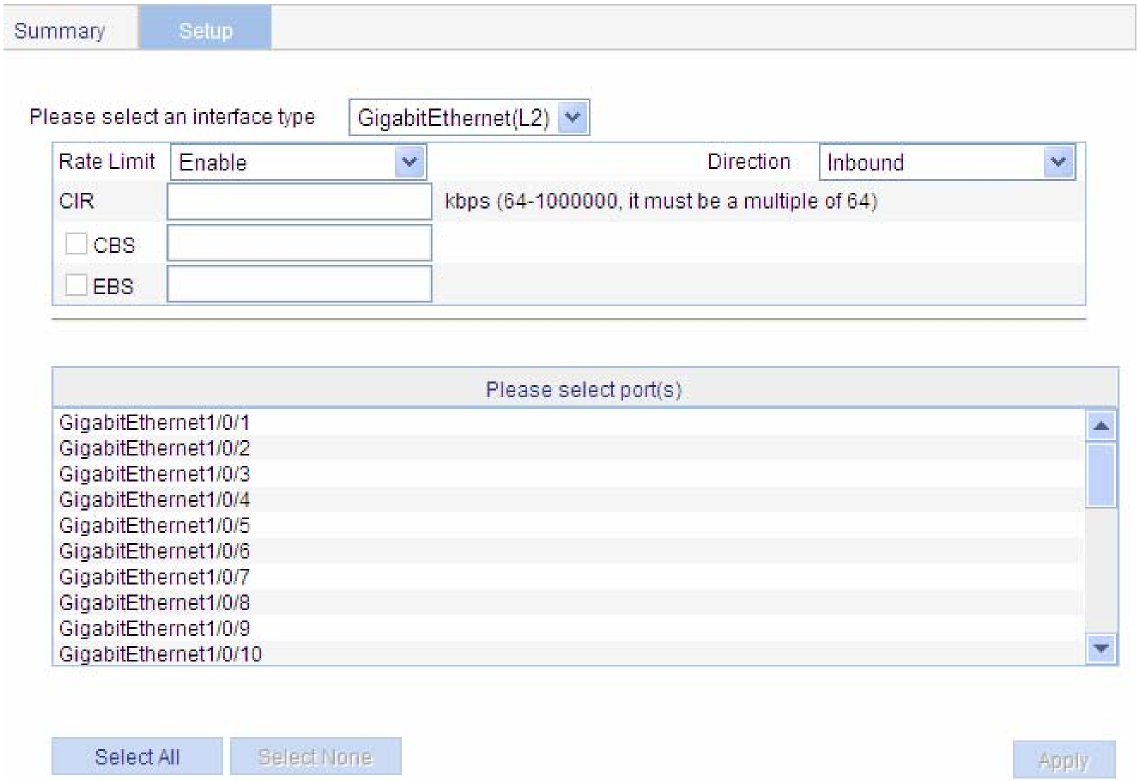
Item		Description
WRR Setup	WRR	Enable or disable the WRR queue scheduling mechanism on selected ports. Two options are available: • **Enable**: Enables WRR on selected ports. • **Not Set**: Restores the default queuing algorithm on selected ports.
	Queue	Select the queue to be configured. Its value range is 0 to 7, but only 0 to 3 is user configurable and 4 to 7 are reserved.
	Group	Specify the group the current queue is to be assigned to. This drop-down list is available after you select a queue ID. The following groups are available for selection: • SP: Assigns a queue to the SP group. • 1: Assigns a queue to WRR group 1. • 2: Assigns a queue to WRR group 2.
	Weight	Set a weight for the current queue. This option is available when group 1 or group 2 is selected.
Please select port(s)		Click to select ports to be configured with queuing on the chassis front panel.

Return to Queue scheduling configuration task list.

Configuring Line Rate on a Port

Select **QoS** > **Line rate** from the navigation tree and click the **Setup** tab to enter the line rate configuration page, as shown in Figure 2-20.

Figure 2-20 The page for configuring line rate on a port



Please select an interface type GigabitEthernet(L2)

Rate Limit	Enable	Direction	Inbound
CIR		kbps (64-1000000, it must be a multiple of 64)	
□ CBS			
□ EBS			

Please select port(s)

GigabitEthernet1/0/1
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/6
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/9
GigabitEthernet1/0/10

Table 2-20 describes the configuration items of configuring line rate on a port.

Table 2-20 Configuration items of configuring line rate on a port

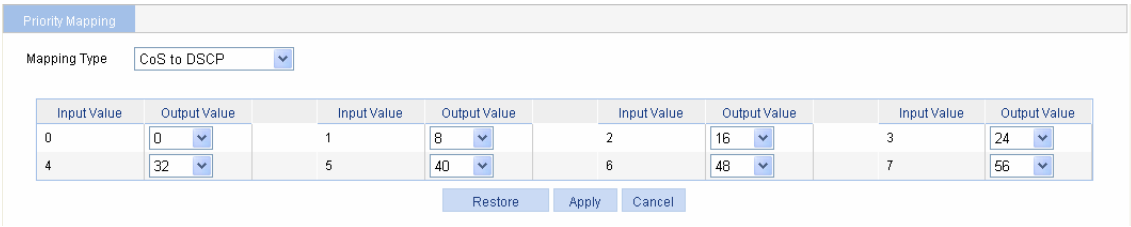
Item	Description
Please select an interface type	Select the types of interfaces to be configured with line rate. The interface types available for selection depend on your device model.
Rate Limit	Enable or disable line rate on the specified port.
Direction	Select a direction in which the line rate is to be applied. ● **Inbound**: Limits the rate of packets received on the specified port. ● **Outbound**: Limits the rate of packets sent by the specified port. ● **Both** : Limits the rate of packets received on and sent by the specified port.
CIR	Set the committed information rate (CIR), the average traffic rate.
Please select port(s)	Specify the ports to be configured with line rate Click the ports to be configured with line rate in the port list. You can select one or more ports.

Return to Line rate configuration task list.

Configuring Priority Mapping Tables

Select **QoS** > **Priority Mapping** from the navigation tree to enter the page shown in Figure 2-21.

Figure 2-21 The page for configuring priority mapping tables



Mapping Type: CoS to DSCP

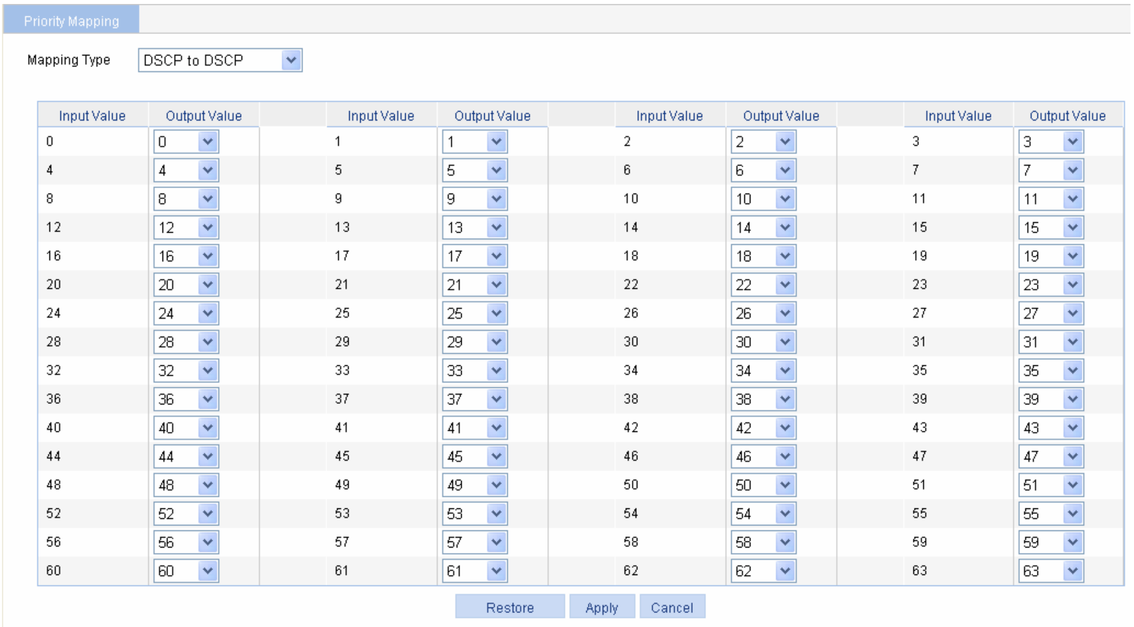
Input Value	Output Value	Input Value	Output Value	Input Value	Output Value	Input Value	Output Value
0	0	1	8	2	16	3	24
4	32	5	40	6	48	7	56

Table 2-18 describes the configuration items of configuring priority mapping tables.

Table 2-21 Configuration items of configuring priority mapping tables

Item	Description
Mapping Type	Select the priority mapping table to be configured, which can be CoS to DSCP, CoS to Queue, DSCP to CoS, DSCP to DSCP, or DSCP to Queue. For example, select DSCP to DSCP mapping type to enter the page shown in Table 2-22.
Input Priority Value	Set the output priority value for an input priority value.
Output Priority Value	
Restore	Click **Restore** to display the default settings of the current priority mapping table on the page. To restore the priority mapping table to the default, click **Apply**.

Figure 2-22 The page for configuring DSCP to DSCP mapping table



Mapping Type: DSCP to DSCP

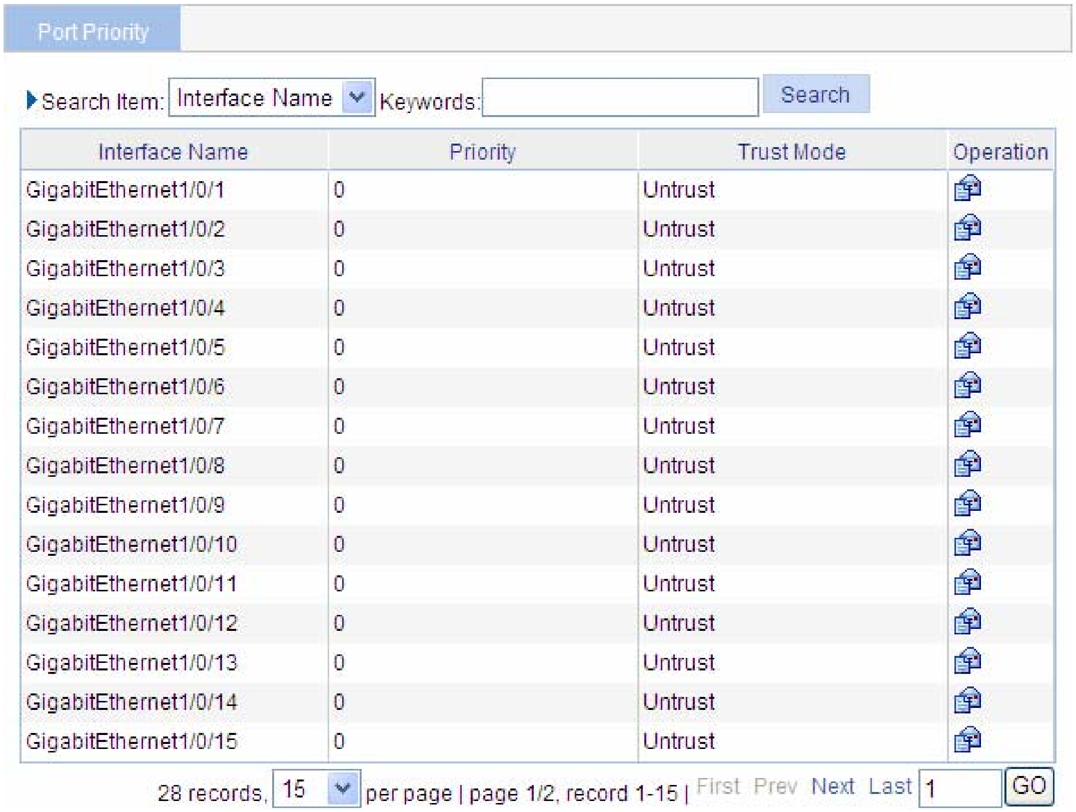
Input Value	Output Value	Input Value	Output Value	Input Value	Output Value	Input Value	Output Value
0	0	1	1	2	2	3	3
4	4	5	5	6	6	7	7
8	8	9	9	10	10	11	11
12	12	13	13	14	14	15	15
16	16	17	17	18	18	19	19
20	20	21	21	22	22	23	23
24	24	25	25	26	26	27	27
28	28	29	29	30	30	31	31
32	32	33	33	34	34	35	35
36	36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

Return to Priority mapping table configuration task list.

Configuring Priority Trust Mode on a Port

Select **QoS** > **Port Priority** from the navigation tree to enter the page shown in Figure 2-23. Click the 📝 icon corresponding to a port to enter the page shown in Figure 2-24.

Figure 2-23 The page for configuring port priority



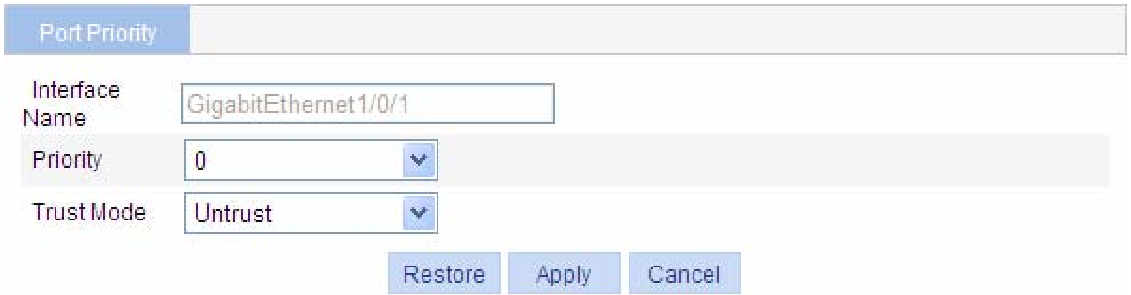
Port Priority

Search Item: Interface Name Keywords: Search

Interface Name	Priority	Trust Mode	Operation
GigabitEthernet1/0/1	0	Untrust	✎
GigabitEthernet1/0/2	0	Untrust	✎
GigabitEthernet1/0/3	0	Untrust	✎
GigabitEthernet1/0/4	0	Untrust	✎
GigabitEthernet1/0/5	0	Untrust	✎
GigabitEthernet1/0/6	0	Untrust	✎
GigabitEthernet1/0/7	0	Untrust	✎
GigabitEthernet1/0/8	0	Untrust	✎
GigabitEthernet1/0/9	0	Untrust	✎
GigabitEthernet1/0/10	0	Untrust	✎
GigabitEthernet1/0/11	0	Untrust	✎
GigabitEthernet1/0/12	0	Untrust	✎
GigabitEthernet1/0/13	0	Untrust	✎
GigabitEthernet1/0/14	0	Untrust	✎
GigabitEthernet1/0/15	0	Untrust	✎

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Figure 2-24 The page for modifying port priority



Port Priority

Interface Name	GigabitEthernet1/0/1
Priority	0
Trust Mode	Untrust

Restore Apply Cancel

Table 2-22 describes the port priority configuration items.

Table 2-22 Port priority configuration items

Item	Description
Interface	The interface to be configured.
Priority	Set a local precedence value for the port.
Trust Mode	Select a priority trust mode for the port, which can be • Untrust: where packet priority is not trusted. • CoS: where the 802.1p precedence of the incoming packets is trusted and used for priority mapping. • DSCP: where the DSCP precedence of the incoming packets is trusted and used for priority mapping.

Return to Priority trust mode configuration task list.

Configuration Guidelines

When configuring QoS, note that:

When an ACL is referenced to implement QoS, the actions defined in the ACL rules, deny or permit, do not take effect; actions to be taken on packets matching the ACL depend on the traffic behavior definition in QoS.

3 ACL/QoS Configuration Examples

ACL/QoS Configuration Example

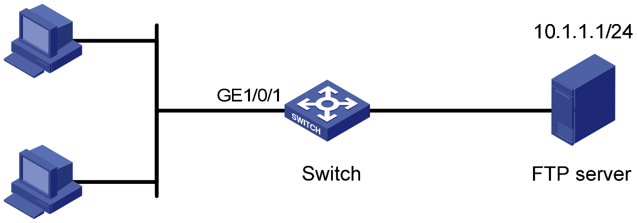
Network requirements

As shown in Figure 3-1, in the network, the FTP server at IP address 10.1.1.1/24 is connected to the Switch, and the clients access the FTP server through GigabitEthernet 1/0/1 of the Switch.

Configure an ACL and a QoS policy as follows to prevent the hosts from accessing the FTP server from 8:00 to 18:00 every day:

1) Create an ACL to prohibit the hosts from accessing the FTP server from 8:00 to 18:00 every day.
2) Configure a QoS policy to drop the packets matching the ACL.
3) Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1.

Figure 3-1 Network diagram for ACL/QoS configuration



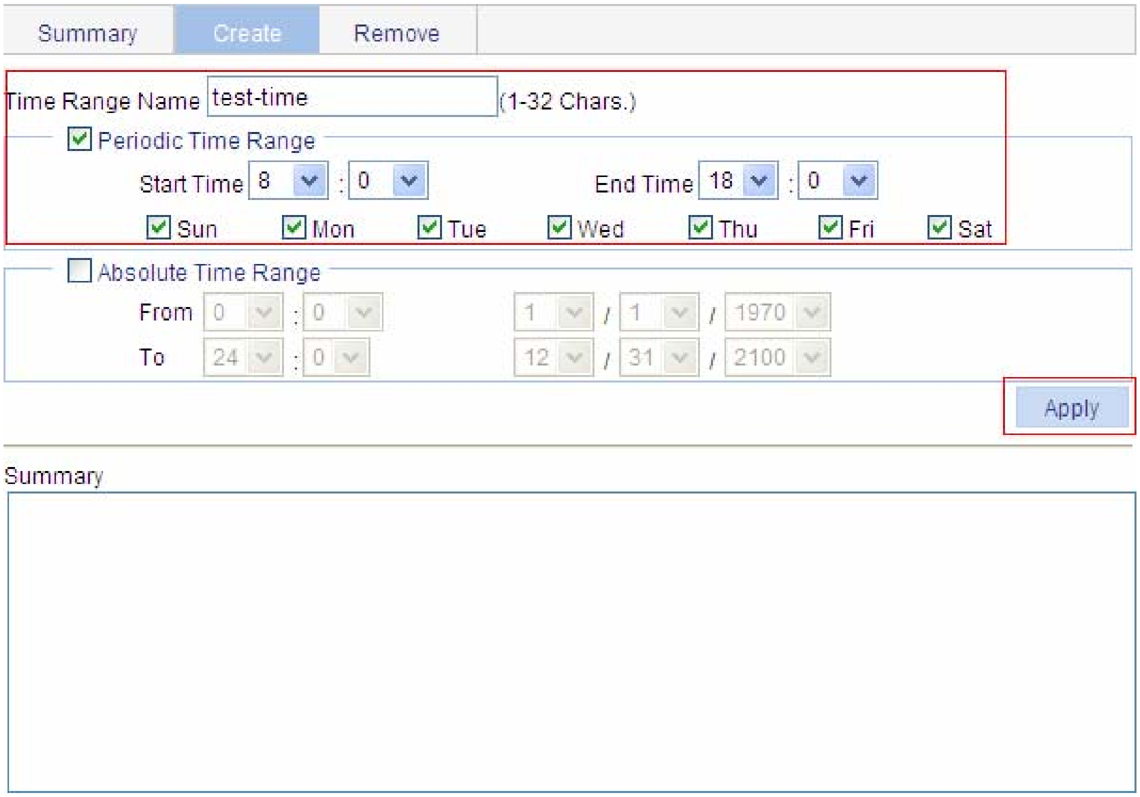
Configuration procedure

1) Configure the time range

# Define a time range covering the time range from 8:00 to 18:00 every day.

- Select **QoS** > **Time Range** from the navigation tree and click **Create**. Perform configuration as shown in Figure 3-2.

Figure 3-2 Define a time range covering 8:00 to 18:00 every day



Time Range Name: test-time (1-32 Chars.)

☑ Periodic Time Range

Start Time 8 : 0   End Time 18 : 0

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

□ Absolute Time Range

From 0 : 0   1 / 1 / 1970

To 24 : 0   12 / 31 / 2100

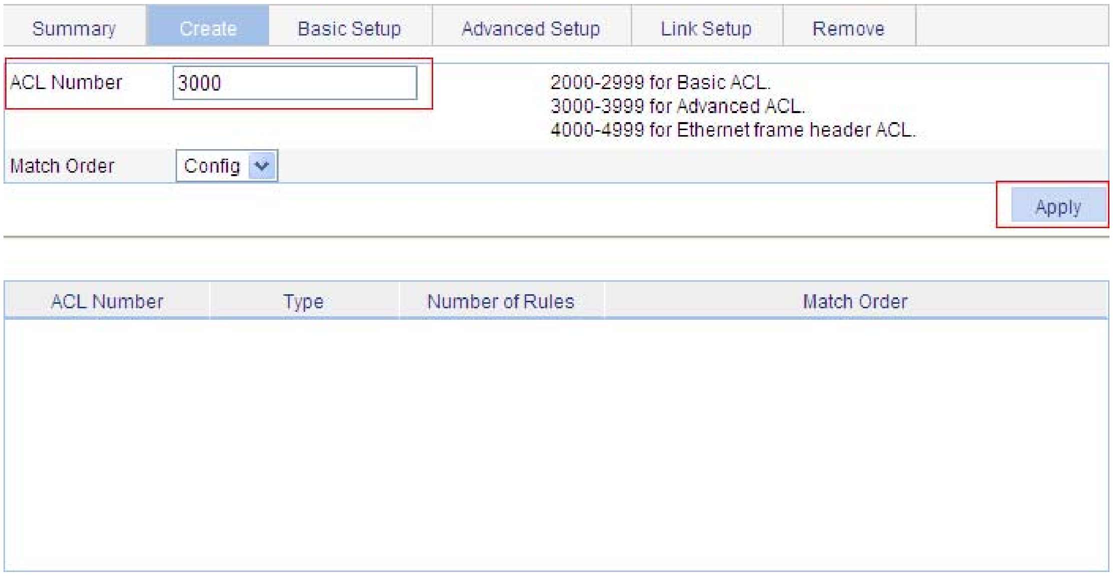
- Type the time range name **test-time**.
- Select the **Periodic Time Range** option, set the **Start Time** to 8:00 and the **End Time** to 18:00, and then select the checkboxes **Sun** through **Sat**.
- Click **Apply**.

2) Define an IPv4 ACL for traffic to the FTP server.

# Create an advanced IPv4 ACL.

- Select **QoS** > **ACL IPv4** from the navigation tree and click **Create**. Perform configuration as shown in Figure 3-3.

Figure 3-3 Create an advanced IPv4 ACL



ACL Number: 3000

2000-2999 for Basic ACL.
3000-3999 for Advanced ACL.
4000-4999 for Ethernet frame header ACL.

Match Order: Config

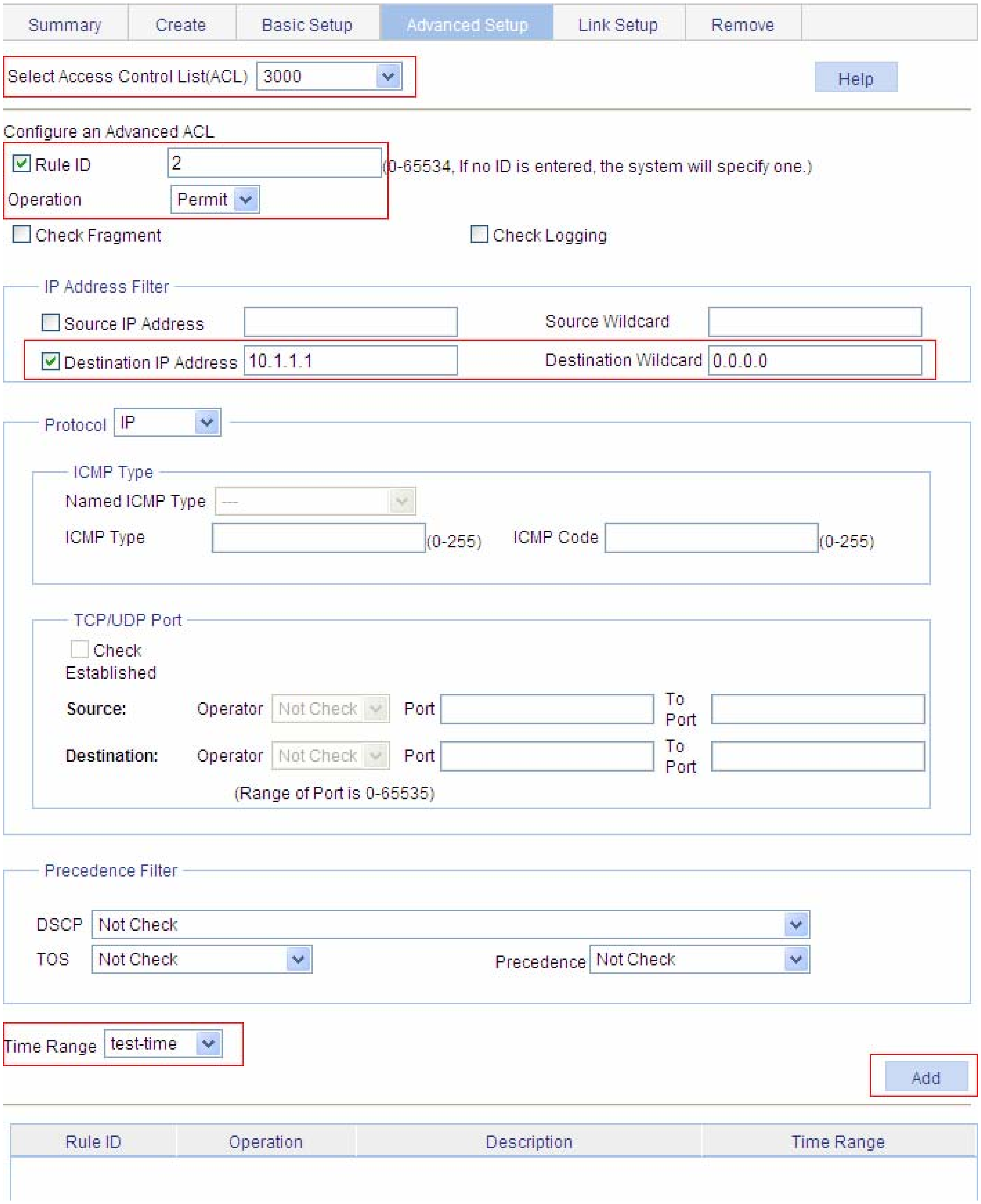
ACL Number	Type	Number of Rules	Match Order

- Type the ACL number 3000.
- Click **Apply**.

# Define an ACL rule for traffic to the FTP server.

- Click **Advance Setup**. Perform configuration as shown in Figure 3-4.

Figure 3-4 Define an ACL rule for traffic to the FTP server



Select Access Control List(ACL) 3000

Configure an Advanced ACL

☑ Rule ID 2 (0-65534, If no ID is entered, the system will specify one.)

Operation Permit

□ Check Fragment □ Check Logging

IP Address Filter

□ Source IP Address Source Wildcard

☑ Destination IP Address 10.1.1.1 Destination Wildcard 0.0.0.0

Protocol IP

ICMP Type

Named ICMP Type ---

ICMP Type (0-255) ICMP Code (0-255)

TCP/UDP Port

□ Check Established

Source: Operator Not Check Port To Port

Destination: Operator Not Check Port To Port

(Range of Port is 0-65535)

Precedence Filter

DSCP Not Check

TOS Not Check Precedence Not Check

Time Range test-time

Add

Rule ID	Operation	Description	Time Range

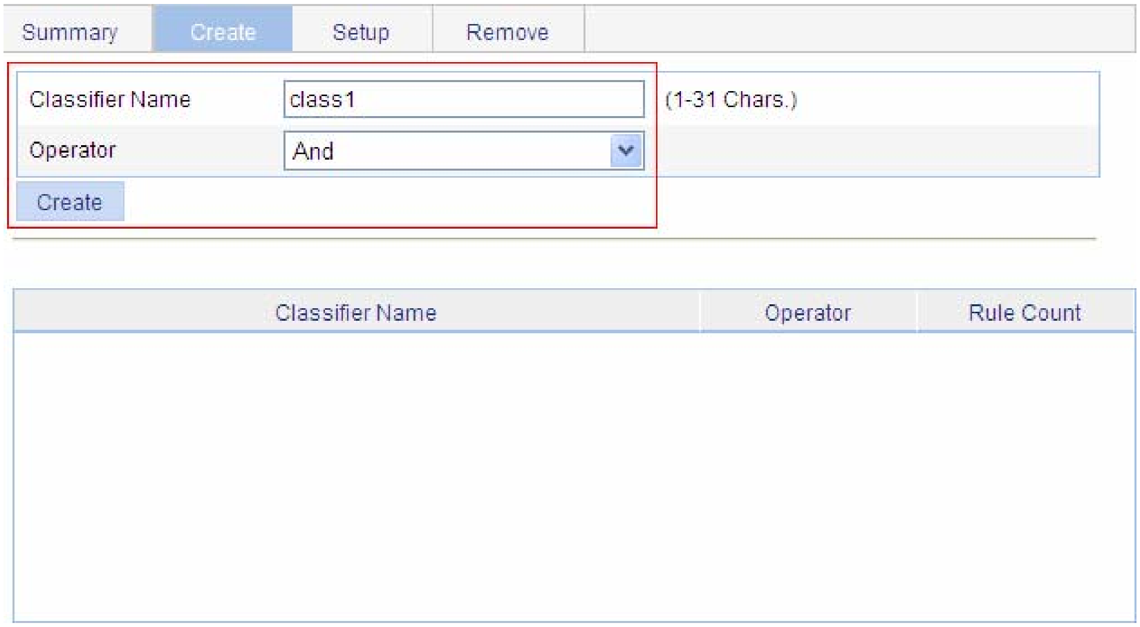
- Select ACL 3000 in the drop-down list.
- Select the **Rule ID** option, and type rule ID 2.
- Select **Permit** in the **Operation** drop-down list.
- Select the **Destination IP Address** option, and type IP address 10.1.1.1 and destination wildcard mask 0.0.0.0.
- Select **test-time** in the **Time Range** drop-down list.
- Click **Add**.

3) Configure a QoS policy

# Create a class.

- Select **QoS** > **Classifier** from the navigation tree and click **Create**. Perform configuration as shown in Figure 3-5.

Figure 3-5 Create a class



Classifier Name: class1 (1-31 Chars.)

Operator: And

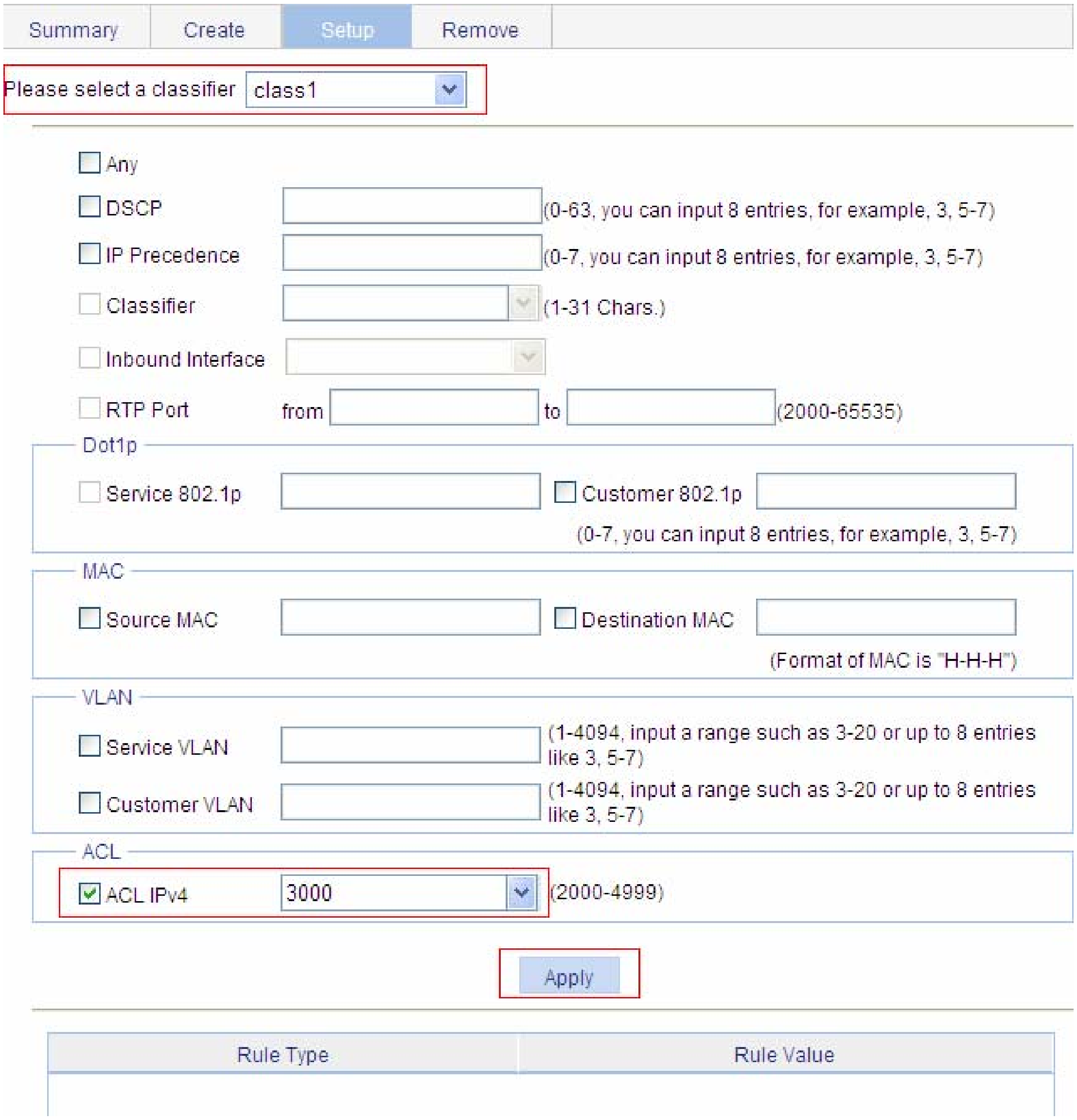
Classifier Name	Operator	Rule Count

- Type the class name **class1**.
- Click **Create**.

# Define classification rules.

- Click **Setup**. Perform configuration as shown in Figure 3-6.

Figure 3-6 Define classification rules

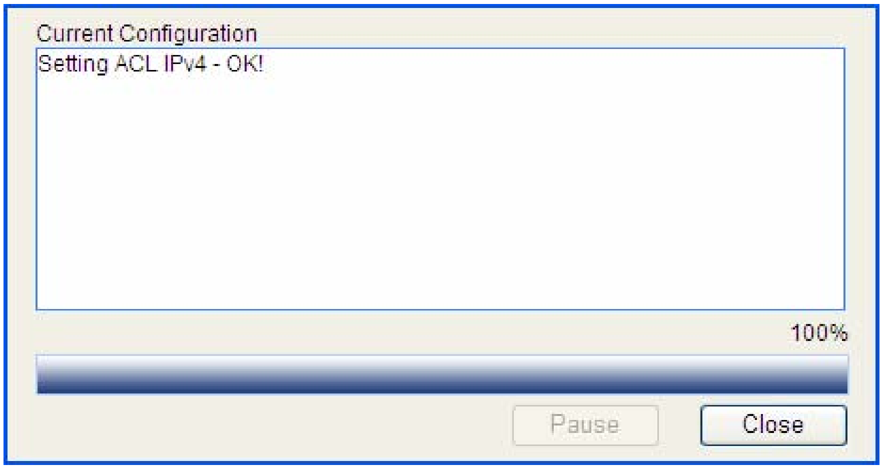

Summary
Create
Setup
Remove
Any
DSCP
(0-63, you can input 8 entries, for example, 3, 5-7)
IP Precedence
(0-7, you can input 8 entries, for example, 3, 5-7)
Classifier
(1-31 Chars.)
Inbound Interface
RTP Port
from
to
(2000-65535)
Dot1p
Service 802.1p
Customer 802.1p
(0-7, you can input 8 entries, for example, 3, 5-7)
MAC
Source MAC
Destination MAC
(Format of MAC is "H-H-H")
VLAN
Service VLAN
(1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)
Customer VLAN
(1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)
ACL
(2000-4999)
Apply
Rule Type
Rule Value

Please select a classifier: class1

☑ ACL IPv4: 3000

- Select the class name **class1** in the drop-down list.
- Select the **ACL IPv4** option, and select ACL 3000 in the following drop-down list.
- Click **Apply**. A configuration progress dialog box appears, as shown in Figure 3-7.

Figure 3-7 Configuration progress dialog box



Current Configuration

Setting ACL IPv4 - OK!

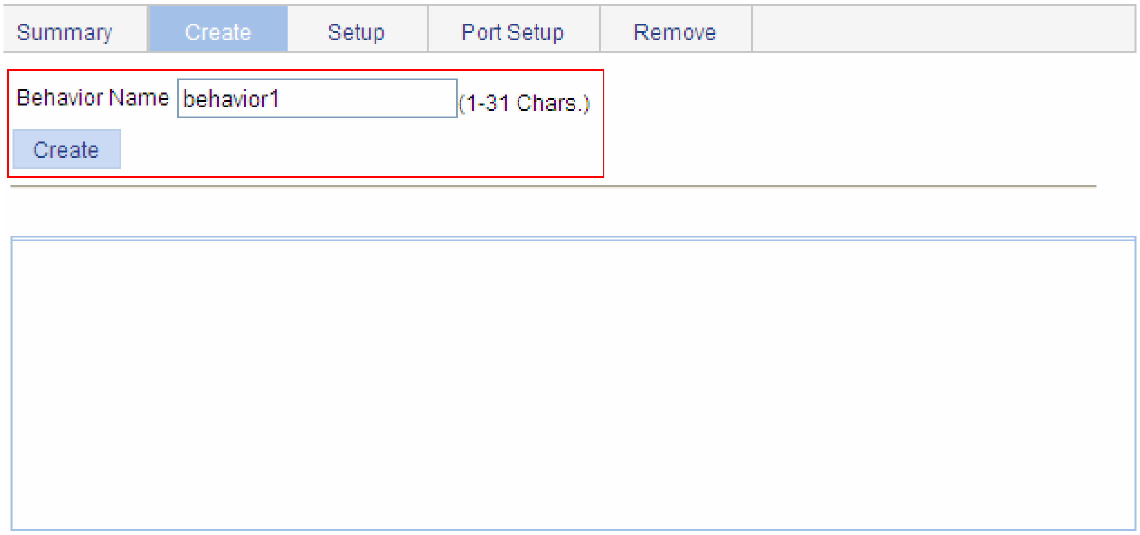
100%

- After the configuration is complete, click **Close** on the dialog box.

# Create a traffic behavior.

- Select **QoS** > **Behavior** from the navigation tree and click **Create**. Perform configuration as shown in Figure 3-8.

Figure 3-8 Create a traffic behavior



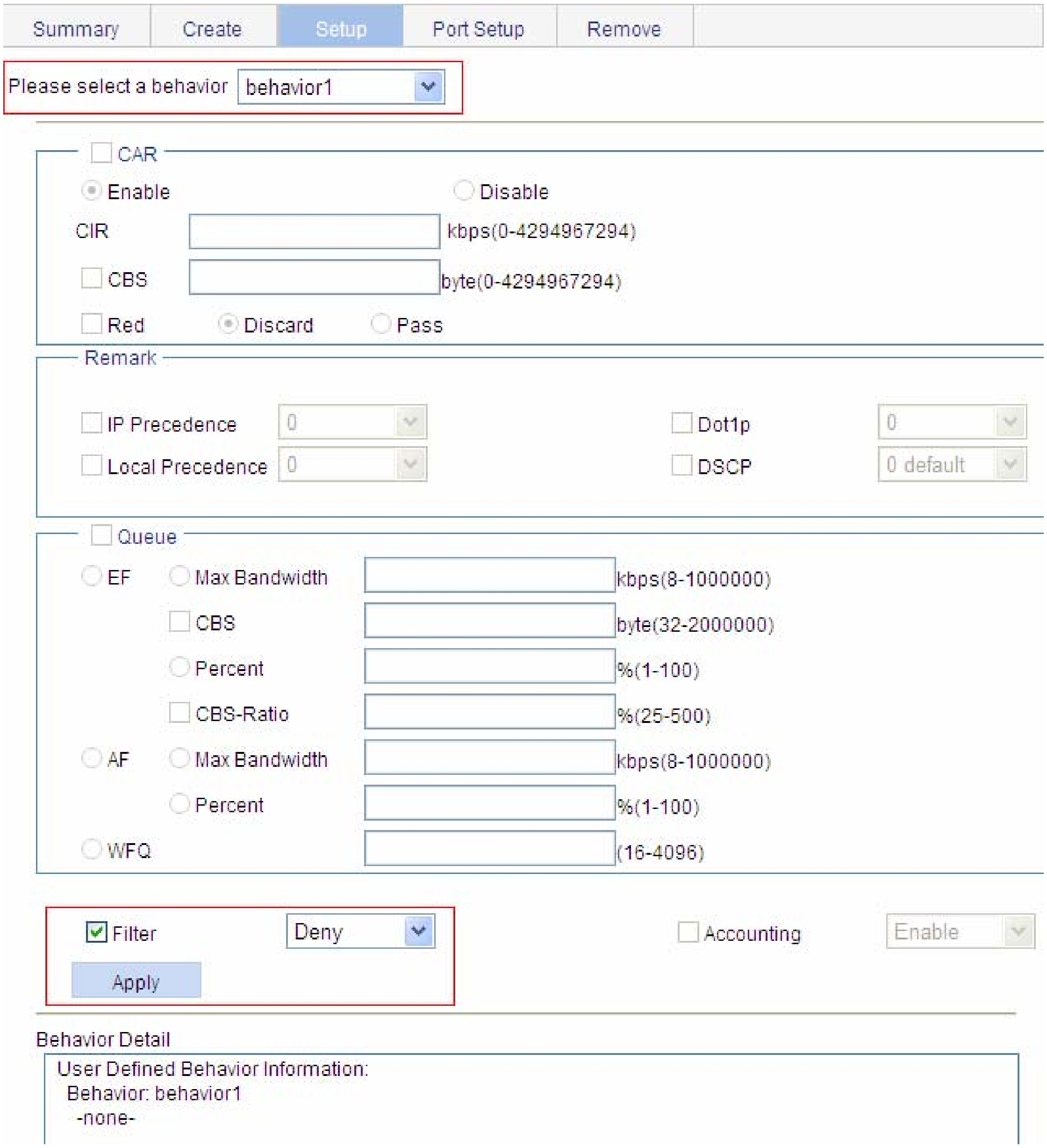
Behavior Name behavior1 (1-31 Chars.)

- Type the behavior name **behavior1**.
- Click **Create**.

# Configure actions for the traffic behavior.

- Click **Setup**. Perform configuration as shown in Figure 3-9.

Figure 3-9 Configure actions for the behavior



Please select a behavior: behavior1

□ CAR

● Enable ○ Disable

CIR kbps(0-4294967294)

□ CBS byte(0-4294967294)

□ Red ● Discard ○ Pass

Remark

□ IP Precedence 0 □ Dot1p 0

□ Local Precedence 0 □ DSCP 0 default

□ Queue

○ EF ○ Max Bandwidth kbps(8-1000000)

□ CBS byte(32-2000000)

○ Percent %(1-100)

□ CBS-Ratio %(25-500)

○ AF ○ Max Bandwidth kbps(8-1000000)

○ Percent %(1-100)

○ WFQ (16-4096)

☑ Filter Deny □ Accounting Enable

Apply

Behavior Detail

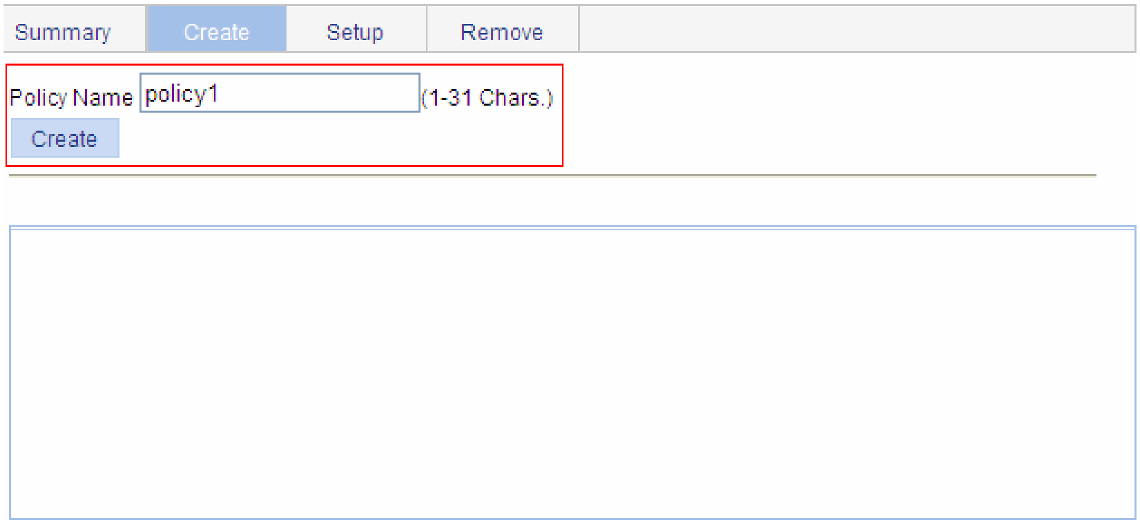
```
User Defined Behavior Information:
 Behavior: behavior1
  -none-
```

- Select **behavior1** in the drop-down list.
- Select the **Filter** option, and then select **Deny** in the following drop-down list.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration is complete, click **Close** on the dialog box.

# Create a policy.

- Select **QoS** > **QoS Policy** from the navigation tree and click the **Create** tab. Perform configuration as shown in Figure 3-10.

Figure 3-10 Create a policy



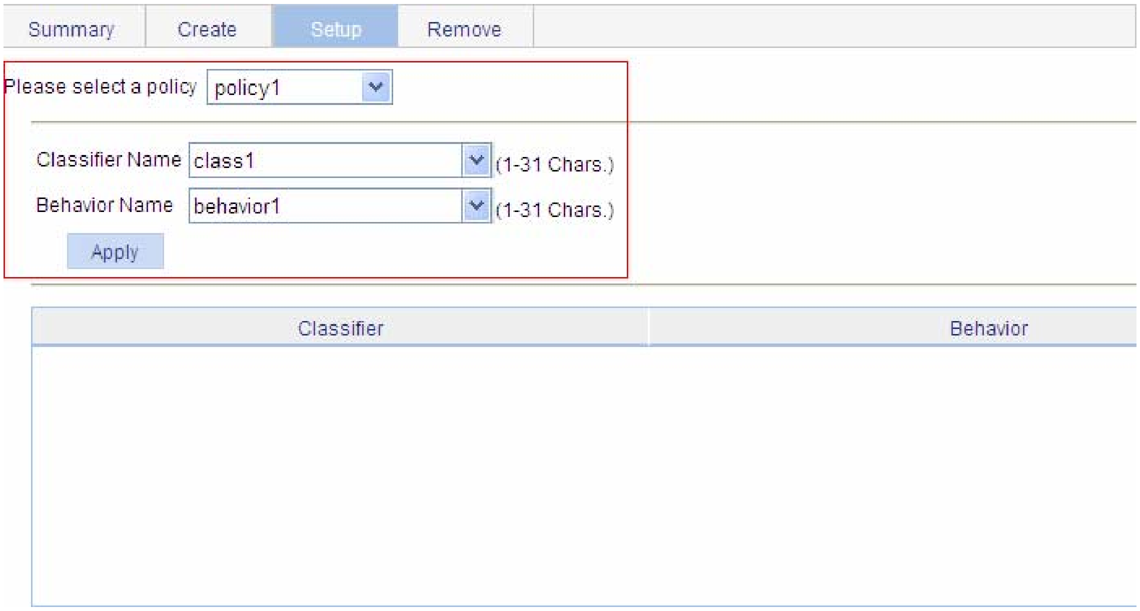
Policy Name policy1 (1-31 Chars.)

- Type the policy name **policy1**.
- Click **Create**.

# Configure classifier-behavior associations for the policy.

- Click **Setup**. Perform configuration as shown in Figure 3-11.

Figure 3-11 Configure classifier-behavior associations for the policy



Please select a policy policy1

Classifier Name class1 (1-31 Chars.)

Behavior Name behavior1 (1-31 Chars.)

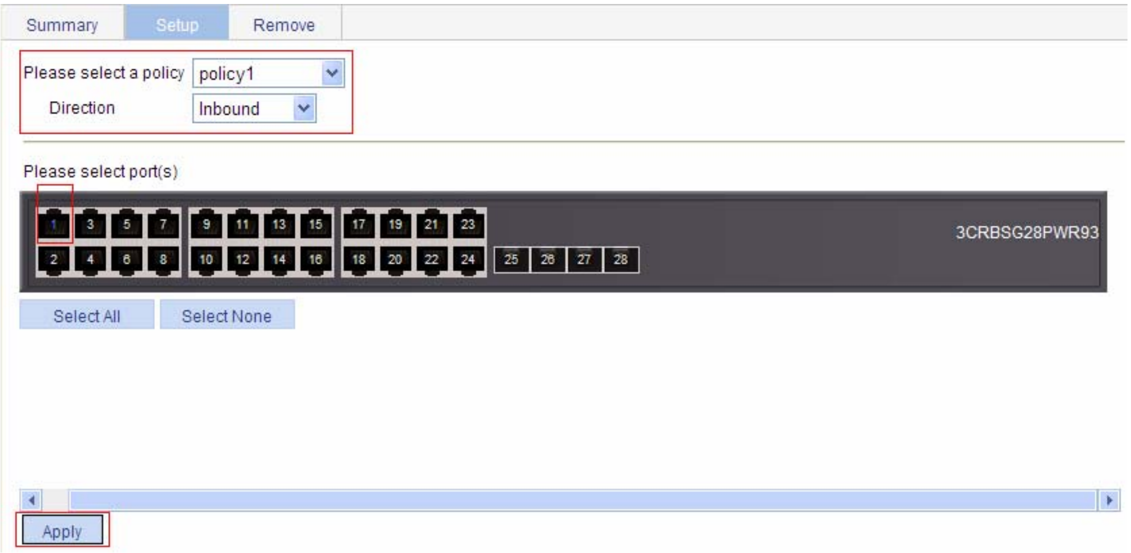
Classifier	Behavior

- Select **policy1**.
- Select **class1** in the **Classifier Name** drop-down list.
- Select **behavior1** in the **Behavior Name** drop-down list.
- Click **Apply**.

# Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1.

- Select **QoS** > **Port Policy** from the navigation tree and click the **Setup** tab. Perform configuration as shown in Figure 3-12.

Figure 3-12 Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1



Please select a policy: policy1

Direction: Inbound

- Select **policy1** in the **Please select a policy** drop-down list.
- Select **Inbound** in the **Direction** drop-down list.
- Select port GigabitEthernet 1/0/1.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration is complete, click **Close** on the dialog box.

Table of Contents

1 PoE Configuration

PoE Overview

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

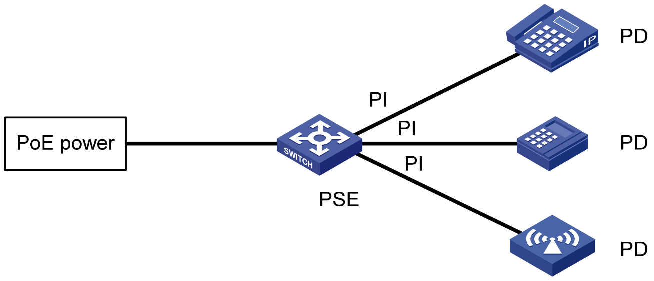
Advantages

- Reliable: Power is supplied in a centralized way so that it is very convenient to provide a backup power supply.
- Easy to connect: A network terminal requires no external power supply but only an Ethernet cable.
- Standard: In compliance with IEEE 802.3af, and a globally uniform power interface is adopted.
- Promising: It can be applied to IP telephones, wireless LAN access points (APs), portable chargers, card readers, web cameras, and data collectors.

Composition

As shown in Figure 1-1, a PoE system consists of PoE power, PSE, power interface (PI), and PD.

Figure 1-1 PoE system diagram



PoE power

The whole PoE system is powered by the PoE power.

PSE

A PSE is a device supplying power for PDs. A PSE can be built-in (Endpoint) or external (Midspan). A built-in PSE is integrated in a switch or router, and an external PSE is independent from a switch or router.

The PSEs of 3Com are built in, and can be classified into two types:

- Device with a single PSE: Only one PSE is available on the device; so the whole device is considered as a PSE.
- Device with multiple PSEs: For a device with multiple PSEs, an interface board with the PoE power supply capability is a PSE. The system uses PSE IDs to identify different PSEs.

Note

3Com Baseline Switch 2920-SFP Plus is a single PSE device, as so .this manual introduces the device with a single PSE only.

A PSE can examine the Ethernet cables connected to PoE interfaces, search for PDs, classify them, and supply power to them. When detecting that a PD is unplugged, the PSE stops supplying power to the PD.

PI

An Ethernet interface with the PoE capability is called PoE interface. Currently, a PoE interface can be an FE or GE interface.

The PSE supplies power for a PoE interface in the following two modes:

- Over signal wires: The PSE uses the pairs (1, 2, 3, 6) for transmitting data in a category 3/5 twisted pair cable to supply DC power while transmitting data to PDs.
- Over spare wires: The PSE uses the pairs (4, 5, 7, 8) not transmitting data in a category 3/5 twisted pair cable to supply DC power to PDs.

Note

3Com Baseline Switch 2920-SFP Plus only support for signal mode.

PD

A PD is a device accepting power from the PSE, including IP phones, wireless APs, chargers of portable devices, POS, and web cameras.

The PD that is being powered by the PSE can be connected to another power supply unit for redundancy power backup.

Protocol Specification

The protocol specification related to PoE is IEEE 802.3af.

Configuring PoE

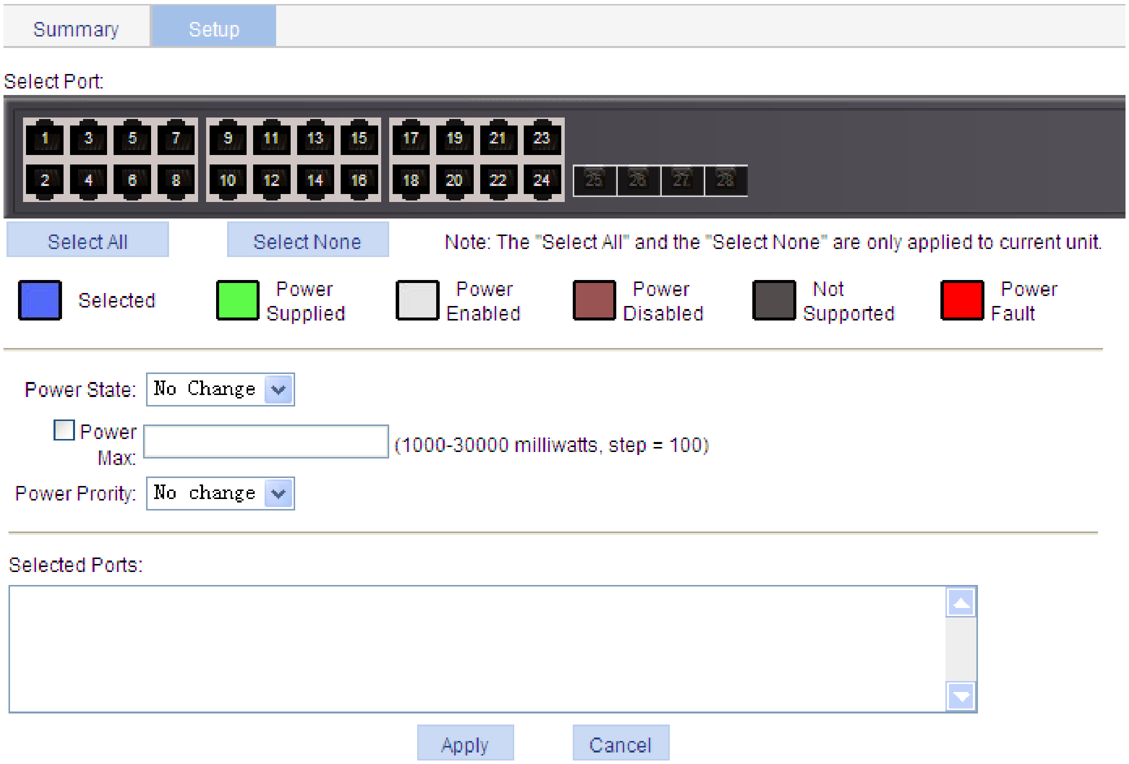
Caution

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

Configuring PoE Ports

Select **PoE** > **PoE** from the navigation tree and click the **Setup** tab, as shown in Figure 1-2.

Figure 1-2 Setup page



Select Port:

Note: The "Select All" and the "Select None" are only applied to current unit.

🟦 Selected 🟩 Power Supplied ⬜ Power Enabled 🟫 Power Disabled ⬛ Not Supported 🟥 Power Fault

Power State: No Change

□ Power Max: (1000-30000 milliwatts, step = 100)

Power Prority: No change

Selected Ports:

Table 1-1 describes the PoE port configuration items.

Table 1-1 PoE port configuration items

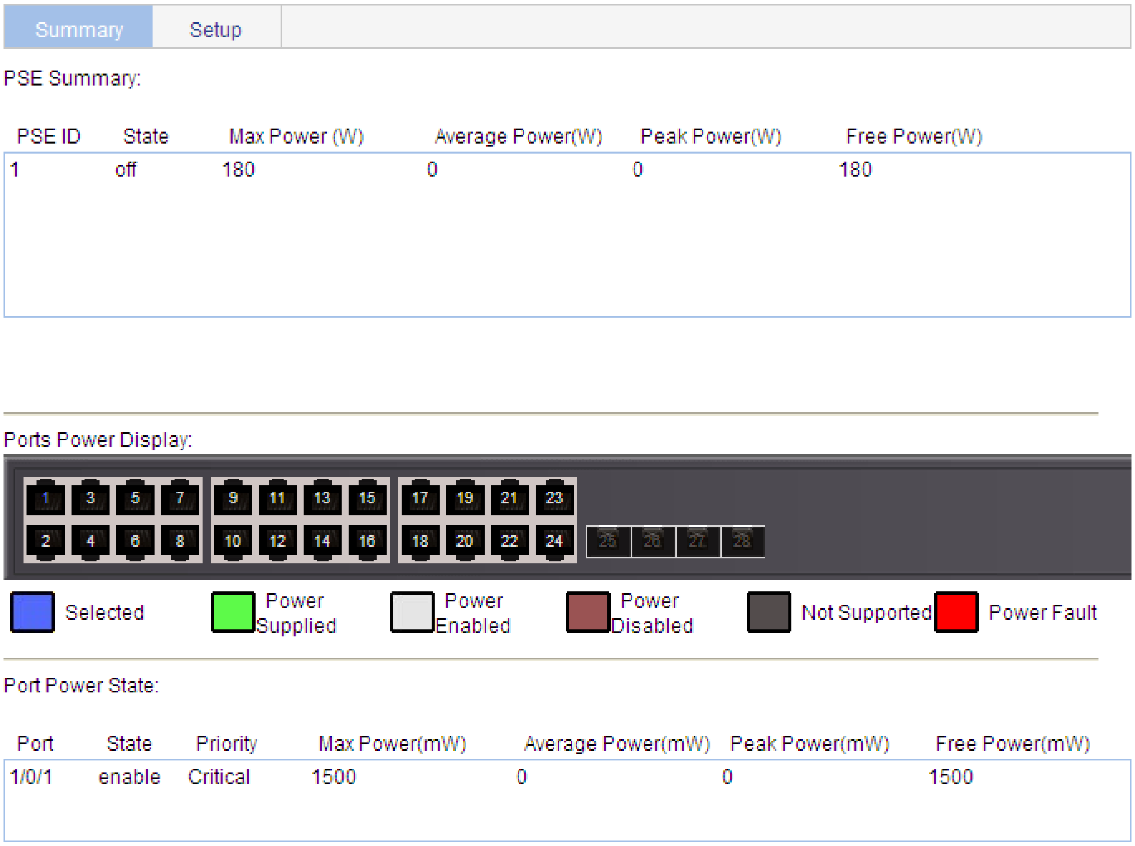
Item	Description
Select Port	Click to select ports to be configured and they will be displayed in the **Selected Ports** list box.
Power State	Enable or disable PoE on the selected ports. • The system does not supply power to or reserve power for the PD connected to a PoE port if the PoE port is not enabled with the PoE function. • You are allowed to enable PoE for a PoE port if the PoE port will not result in PoE power overload; otherwise, you are not allowed to enable PoE for the PoE port. By default, PoE is disabled on a PoE port. **Highlight** *PSE power overload: When the sum of the power consumption of all ports exceeds the maximum power of PSE, the system considers the PSE is overloaded.*
Power Max	Set the maximum power for the PoE port. The maximum PoE port power is the maximum power that the PoE port can provide to the connected PD. If the power required by the PD is larger than the maximum PoE port power, the PoE port will not supply power to the PD. By default, the maximum power of a PoE port is 30000 milliwatts.

Item	Description
Power Priority	Set the power supply priority for a PoE port. The priority levels of a PoE port include low, high, and critical in ascending order. • When the PoE power is insufficient, power is first supplied to PoE ports with a higher priority level. • When the PSE power is overloaded, the PoE port with a lower priority is first disconnected to guarantee the power supply to the PD with a higher priority. • If you set the priority of a PoE port to **critical**, the system compares the guaranteed remaining PSE power (the maximum PSE power minus the maximum power allocated to the existing critical PoE port, regardless of whether PoE is enabled for the PoE port) with the maximum power of this PoE port. If the former is greater than the latter, you can succeed in setting the priority to **critical**, and this PoE port will preempt the power of other PoE ports with a lower priority level; otherwise, you will fail to set the PoE port to **critical**. In the former case, the PoE ports whose power is preempted will be powered off, but their configurations will remain unchanged. When you change the priority of a PoE port from critical to a lower level, the PDs connecting to other PoE ports will have an opportunity of being powered. By default, the power priority of a PoE port is **low**. **Highlight** • *19 watts guard band is reserved for each PoE port on the device to prevent a PD from being powered off because of a sudden increase of the PD power. When the remaining power of the PSE is lower than 19 watts, the port with a higher priority can preempt the power of the port with a lower priority to ensure the normal working of the higher priority port.* • *If the sudden increase of the PD power results in PSE power overload, power supply to the PD on the PoE interface with a lower priority will be stopped to ensure the power supply to the PD with a higher priority.*

Displaying Information About PSE and PoE Ports

Select **PoE** > **PoE** from the navigation tree to enter the page of the **Summary** tab. The upper part of the page displays the PSE summary; Click a port on the chassis front panel, the configuration and power information will be displayed in the lower part of the page, as shown in Figure 1-3.

Figure 1-3 PoE summary



PSE Summary:

PSE ID	State	Max Power (W)	Average Power(W)	Peak Power(W)	Free Power(W)
1	off	180	0	0	180

Ports Power Display:

🟦 Selected 🟩 Power Supplied □ Power Enabled 🟫 Power Disabled ■ Not Supported 🟥 Power Fault

Port Power State:

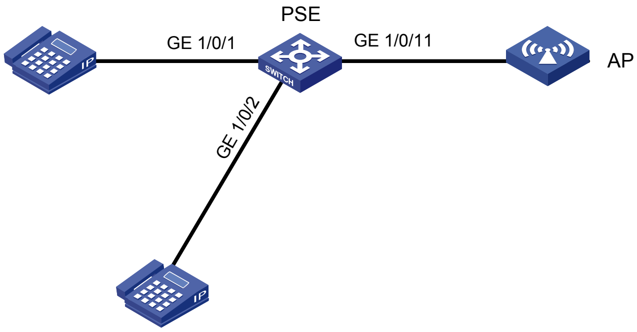
Port	State	Priority	Max Power(mW)	Average Power(mW)	Peak Power(mW)	Free Power(mW)
1/0/1	enable	Critical	1500	0	0	1500

PoE Configuration Example

Network requirements

- As shown in Figure 1-4, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are connected to IP telephones.
- GigabitEthernet 1/0/11 is connected to AP whose maximum power does not exceed 9000 milliwatts.
- The power supply priority of IP telephones is higher than that of AP; therefore, the PSE supplies power to IP telephones first when the PSE power is overloaded.

Figure 1-4 Network diagram for PoE

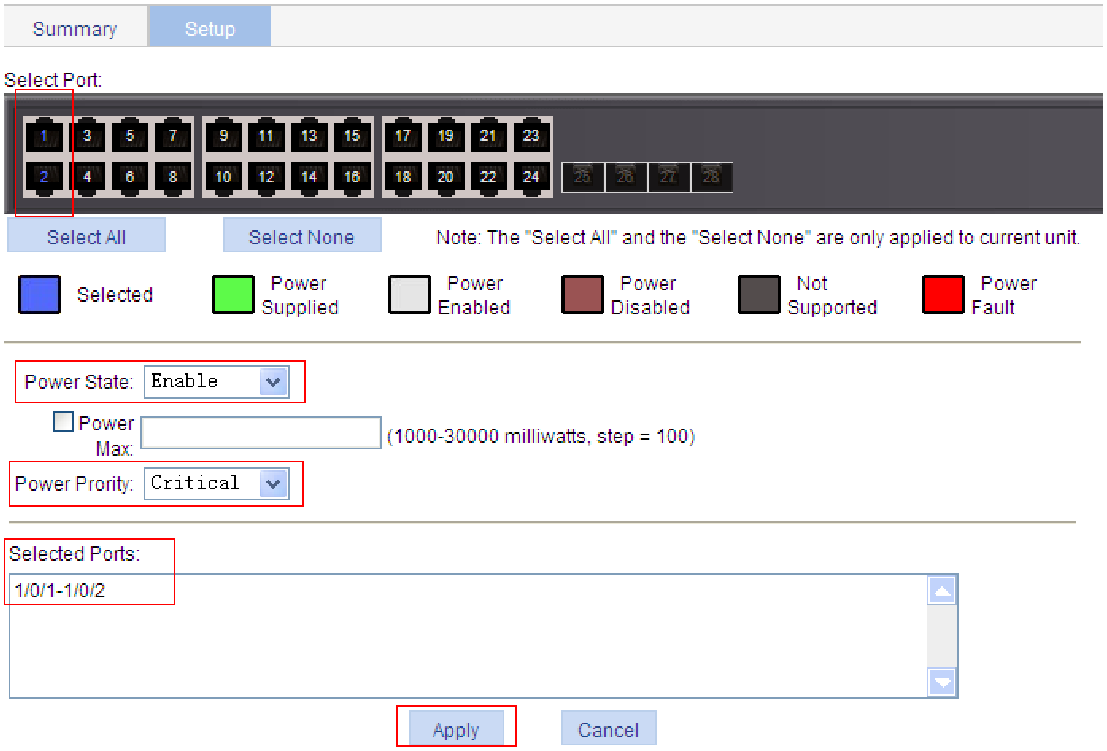


Configuration procedure

# Enable PoE on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, and configure their power supply priority to **critical**.

- Select **PoE** > **PoE** from the navigation tree and click the **Setup** tab to perform the following configurations, as shown in Figure 1-5.

Figure 1-5 Configure the PoE ports supplying power to the IP telephones



Note: The "Select All" and the "Select None" are only applied to current unit.

Power State: Enable

□ Power Max: (1000-30000 milliwatts, step = 100)

Power Prority: Critical

Selected Ports:

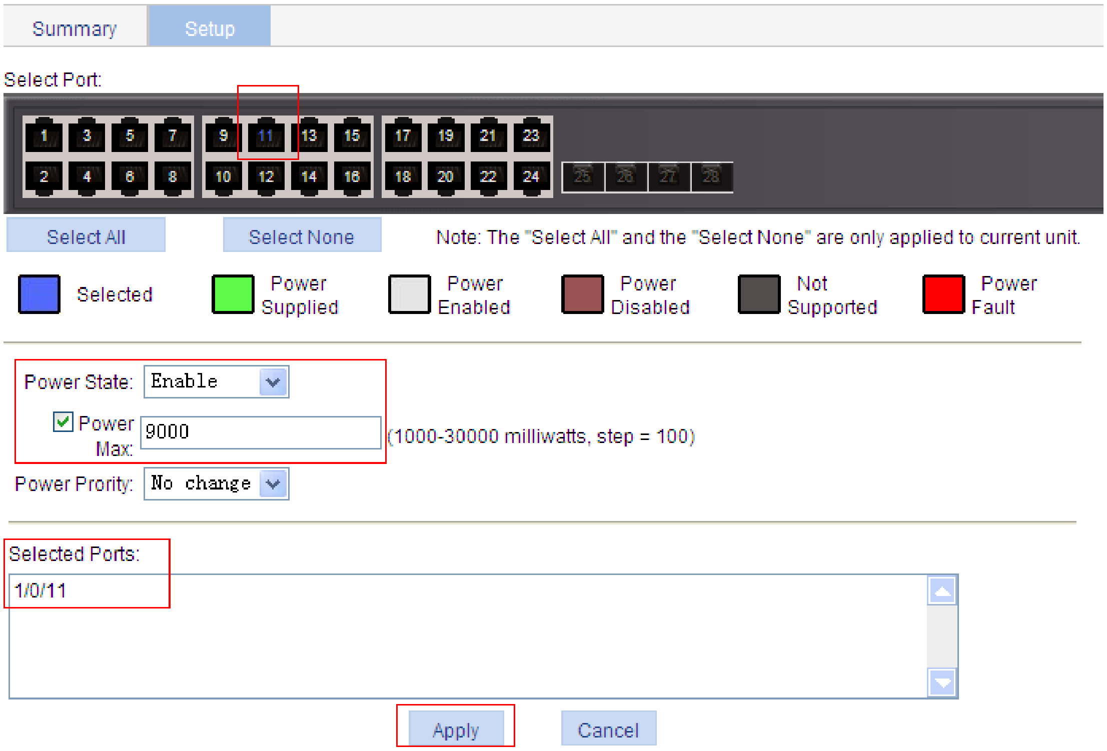
1/0/1-1/0/2

- Click to select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
- Select **Enable** from the **Power State** drop-down list.
- Select **Critical** from the **Power Priority** drop-down list.
- Click **Apply**.

# Enable PoE on GigabitEthernet 1/0/11 and configure the maximum power of the port to 9000 milliwatts.

- Click the **Setup** tab and perform the following configurations, as shown in Figure 1-6.

Figure 1-6 Configure the PoE port supplying power to AP



Note: The "Select All" and the "Select None" are only applied to current unit.

🟦 Selected 🟩 Power Supplied ⬜ Power Enabled 🟫 Power Disabled ⬛ Not Supported 🟥 Power Fault

Power State: Enable

☑ Power Max: 9000 (1000-30000 milliwatts, step = 100)

Power Prority: No change

Selected Ports:

1/0/11

- Click to select port GigabitEthernet 1/0/11 from the chassis front panel.
- Select **Enable** from the **Power State** drop-down list.
- Select the check box before **Power Max** and type **9000**.
- Click **Apply**.

After the configuration takes effect, the IP telephones and AP are powered and can work normally.