HP 1910 Switch Series

User Guide

Part number: 5998-2269

Software version: Release 1511

Document version: 6W100-20120528

Contents

Overview

The HP 1910 Switch Series 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 1910 Switch 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.

Configuration through the Web interface

The device provides web-based configuration interfaces for visual device management and maintenance.

Figure 1 Web-based network management operating environment

Logging in to the Web interface

You can use the following default settings to log in to the web interface through HTTP:

- **Username**—admin
- **Password**—None
- **IP address of VLAN-interface 1 on the device**—Default IP address of the device, depending on the status of the network 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 device, as shown in Figure 2. The default subnet mask is 255.255.0.0.

Figure 2 Default IP address of the device

Default IP Address: 169.254.52.86

-
    - 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 about 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>
```

Assuming that the default IP address of the device is 169.254.52.86, to log in to the Web interface of the device from a PC:

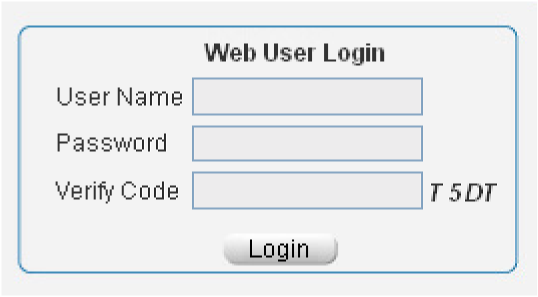
1. Connect the GigabitEthernet interface of the device to a PC by using a crossover Ethernet cable. By default, all interfaces belong to VLAN 1.
2. Configure an IP address for the PC and make sure that the PC and device can reach each other.

For example, assign the PC an IP address (for example, 169.254.52.1) within 169.254.0.0/16 (except for the default IP address of the device).

3. Open the browser, and input the login information.
    a. Type the IP address http:// 169.254.52.86 in the address bar and press **Enter**.

       The login page of the web interface (see Figure 3) appears.
    b. Enter the username **admin** and the verification code, leave the password blank, and click **Login**.

Figure 3 Login page of the Web interface



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 more information, see the corresponding configuration guides 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

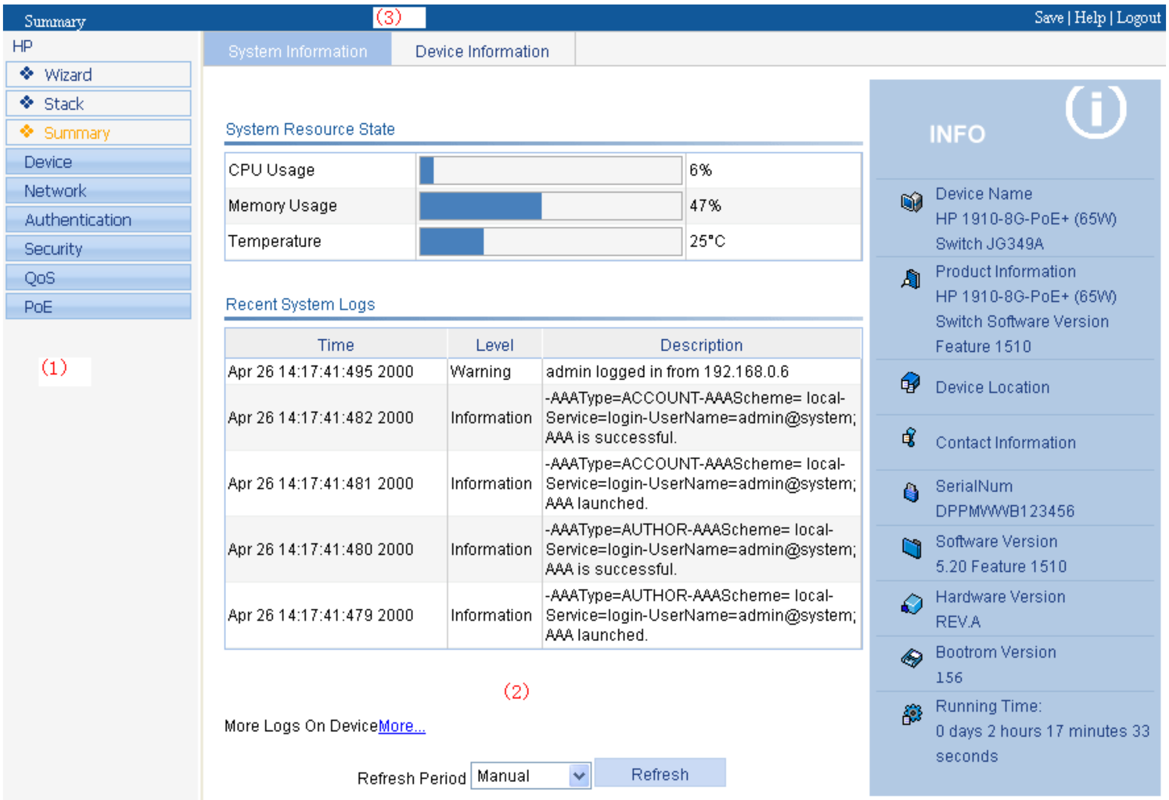
Click **Logout** in the upper-right corner of the Web interface, as shown in Figure 4 to quit the Web console.

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 4.

Figure 4 Web-based configuration interface



(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**—On the left, displays the path of the current configuration interface in the navigation area; on the right, provides the **Save** button to quickly save the current configuration, the **Help** button to display the Web-related help information, and the **Logout** button to log out of the Web interface.

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 backup/restore configuration files.
- **Management**—Users of this level can perform any operations to the device.

Introduction to the Web-based NM functions

User level in Table 1 indicates that users of this level or users of a higher level can perform the corresponding operations.

Table 1 Web-based NM function description

Function menu			Description	User level
Wizard		IP Setup	Perform quick configuration of the device.	Management
Stack		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 about 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	Upload upgrade file from local host, and upgrade the system software.	Management
		Reboot	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
		Net Time	Display the synchronization status of the system clock and configure the network time.	Monitor
	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 refreshing 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
		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

Function menu		Description	User level
Port Management	Summary	Display port information by features.	Monitor
	Detail	Display 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 about 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 about 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	Display, create, modify, and clear alarm entries.	Configure
	Event	Display, 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

Function menu			Description	User level
	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; 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 about 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	Display the member port information about 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
		OUI Summary	Display the addresses of the OUIs that can be identified by voice VLAN.	Monitor

Function menu		Description	User level
	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	Display the MSTP information about 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 about 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	Display global LLDP neighbor information.	Monitor
IGMP Snooping	Basic	Display global IGMP snooping configuration information or the IGMP snooping configuration information in a VLAN, and 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

Function menu		Description	User level
MLD Snooping	Basic	Display global MLD snooping configuration information or the MLD snooping configuration information in a VLAN, and the MLD snooping multicast entry information.	Monitor
		Configure MLD snooping globally or in a VLAN.	Configure
	Advanced	Display the MLD snooping configuration information on a port.	Monitor
		Configure MLD snooping on a port.	Configure
IPv4 Routing	Summary	Display the IPv4 active route table.	Monitor
	Create	Create an IPv4 static route.	Configure
	Remove	Delete the selected IPv4 static routes.	Configure
IPv6 Routing	Summary	Display the IPv6 active route table.	Monitor
	Create	Create an IPv6 static route.	Configure
	Remove	Delete the selected IPv6 static routes.	Configure
DHCP	DHCP Relay	Display information about the DHCP status, advanced configuration information about 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 about DHCP snooping.	Monitor
		Enable/disable DHCP snooping, and configure DHCP snooping trusted and untrusted ports.	Configure
Service	Service	Display the states of services: enabled or disabled.	Configure
		Enable/disable services, and set related parameters.	Management
Diagnostic Tools	IPv4 Ping	Ping an IPv4 address.	Visitor
	IPv6 Ping	Ping an IPv6 address.	Visitor
	IPv4 Traceroute	Perform IPv4 trace route operations.	Visitor
	IPv6 Traceroute	Perform IPv6 trace route operations.	Visitor
ARP Management	ARP Table	Display ARP table information.	Monitor
		Add, modify, and remove ARP entries.	Configure
	Gratuitous ARP	Display the configuration information about gratuitous ARP.	Monitor

Function menu			Description	User level
			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
	Portal	Portal Server	Display configuration information about the portal server and advanced parameters for portal authentication.	Monitor
			Add and delete a portal server, and modify advanced parameters for portal authentication.	Configure
		Free Rule	Display the portal-free rule configuration information.	Monitor
			Add and delete a portal-free rule.	Configure
	AAA	Domain Setup	Display ISP domain configuration information.	Monitor
			Add and remove ISP domains.	Management
		Authentication	Display the authentication configuration information about an ISP domain.	Monitor
			Specify authentication methods for an ISP domain.	Management
		Authorization	Display the authorization method configuration information about an ISP domain.	Monitor
			Specify authorization methods for an ISP domain.	Management
		Accounting	Display the accounting method configuration information about an ISP domain.	Monitor
			Specify accounting methods for an ISP domain.	Management
	RADIUS	RADIUS Server	Display and configure RADIUS server information.	Management
		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 about PKI domains and the contents of a certificate.	Monitor

Function menu			Description	User level
			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
Secu rity	Port Isolate Group	Summary	Display port isolation group information.	Monitor
		Port Setup	Configure the ports in an isolation group.	Configure
	Authorized 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
	ACL IPv6	Summary	Display IPv6 ACL configuration information.	Monitor
		Create	Create an IPv6 ACL.	Configure
		Basic Setup	Configure a rule for a basic IPv6 ACL.	Configure
		Advanced Setup	Configure a rule for an advanced IPv6 ACL.	Configure
		Remove	Delete an IPv6 ACL or its rules.	Configure
	Queue	Summary	Display the queue information about 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
	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

Function menu			Description	User level
		Port Setup	Configure 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
		PSE Setup	Configure a PoE interface.	Configure
		Port Setup	Configure a port.	Configure

Introduction to the common items on the Web pages

Buttons and icons

Table 2 Commonly used buttons and icons

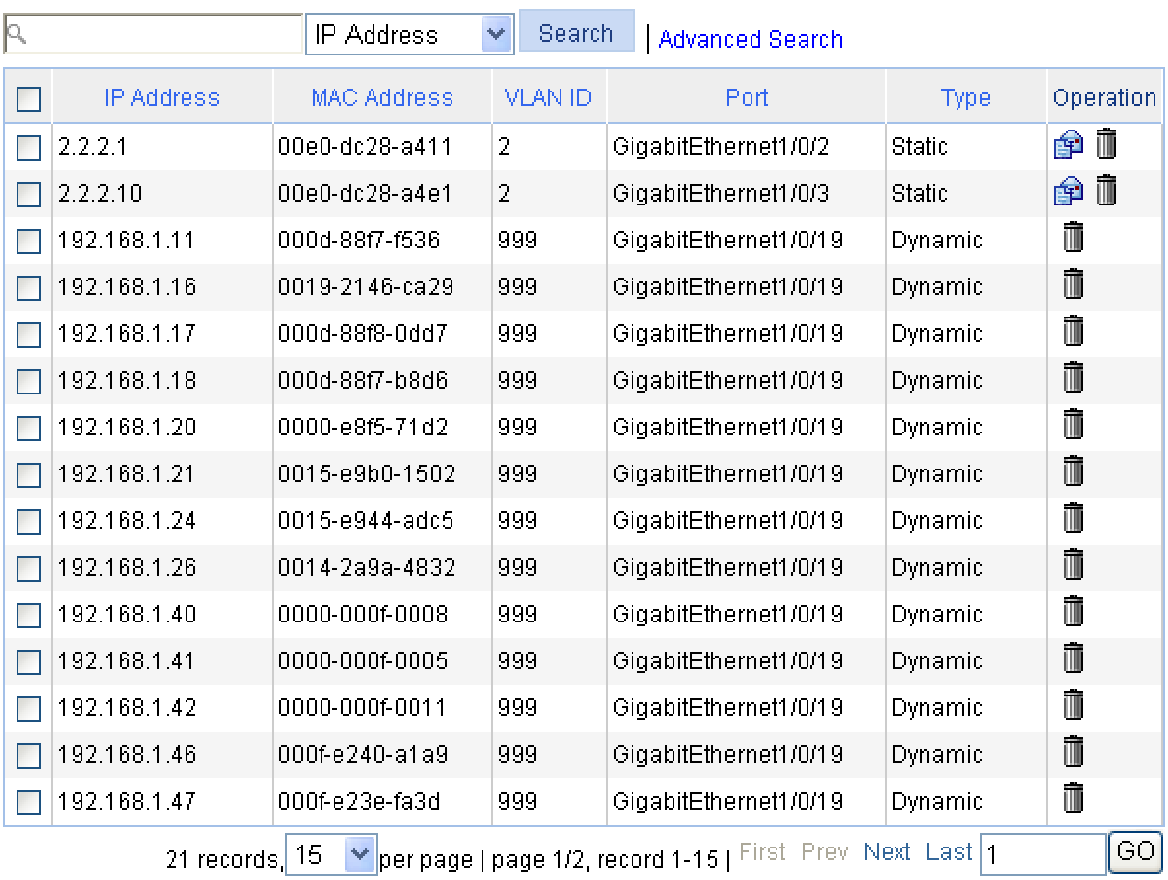
Button and icon	Function
Apply	Used to apply the configuration on the current page.
Cancel	Used to cancel the configuration on the current page, and return to the corresponding list page or the **Device Info** page.
Refresh	Used to refresh the information on the current page.
Clear	Used to clear all the information on a list or all statistics.
Add	Used to enter a page for adding an item.
Remove, Del Selected	Used to remove the selected items.

Button and icon	Function
Select All	Used to select all the entries on a list, or all the ports on the device panel.
Select None	Used to deselect all the entries on a list, or all the ports on the device panel.
Next>	Generally present on the configuration wizard; used to buffer but not apply the configuration of the current step and enter the next configuration step.
<Back	Generally present on the configuration wizard; used to buffer but not apply the configuration of the current step and return to the previous configuration step.
Finish	Generally present on the configuration wizard; used to apply the configurations of all configuration steps.
	Generally present on the "Operation" column on a list; used to enter the modification page of an item so that you can modify the configurations of the item.
	Generally present on the "Operation" column on a list; used to delete the item corresponding to this icon.

Page display

The Web interface can display a long list by pages, as shown in Figure 5. You can set the number of entries displayed per page, and use the **First**, **Prev**, **Next**, and **Last** links to view the contents on the first, previous, next, and last pages, or go to any page that you want to view.

Figure 5 Content display by pages



	IP Address	MAC Address	VLAN ID	Port	Type	Operation
	2.2.2.1	00e0-dc28-a411	2	GigabitEthernet1/0/2	Static	
	2.2.2.10	00e0-dc28-a4e1	2	GigabitEthernet1/0/3	Static	
	192.168.1.11	000d-88f7-f536	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.16	0019-2146-ca29	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.17	000d-88f8-0dd7	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.18	000d-88f7-b8d6	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.20	0000-e8f5-71d2	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.21	0015-e9b0-1502	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.24	0015-e944-adc5	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.26	0014-2a9a-4832	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.40	0000-000f-0008	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.41	0000-000f-0005	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.42	0000-000f-0011	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.46	000f-e240-a1a9	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.47	000f-e23e-fa3d	999	GigabitEthernet1/0/19	Dynamic	

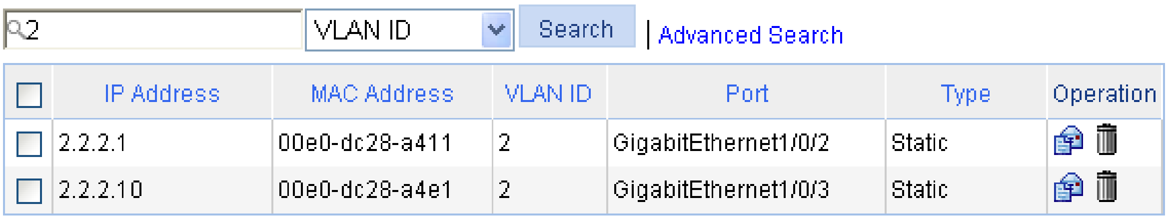
21 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Search function

On some list pages, the web interface provides basic and advanced search functions. You can use the search function to display those entries matching certain search criteria.

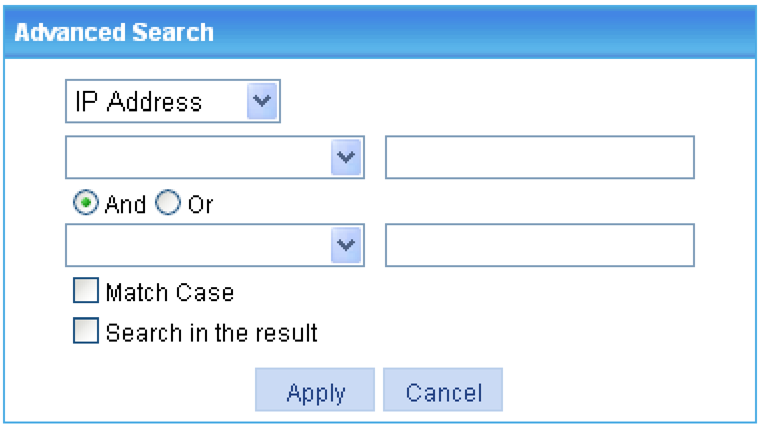
- **Basic search function**—As shown in Figure 5, input the keyword in the text box above the list, select a search item from the drop-down list and click the **Search** button to display the entries that match the criteria. Figure 6 shows an example of searching for entries with VLAN ID 2.

Figure 6 Basic search function example



- **Advanced search function**—As shown in Figure 5, you can click the **Advanced Search** link to open the advanced search page, as shown in Figure 7. Specify the search criteria, and click **Apply** to display the entries that match the criteria.

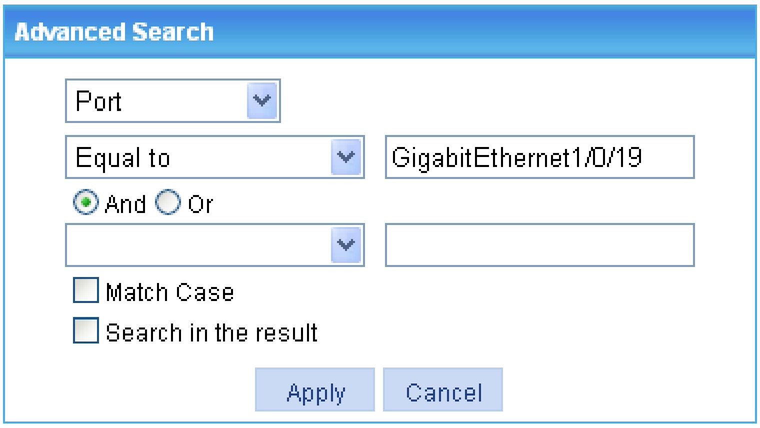
Figure 7 Advanced search



Take the ARP table shown in Figure 5 as an example. If you want to search for the ARP entries with interface being GigabitEthernet1/0/19, and IP address range being 192.168.1.50 to 192.168.1.59, follow these steps:

1. Click the **Advanced Search** link, specify the search criteria on the advanced search page as shown in Figure 8, and click **Apply**. The ARP entries with interface being GigabitEthernet1/0/19 are displayed.

Figure 8 Advanced search function example (I)



2. Click the **Advanced Search** link, specify the search criteria on the advanced search page as shown in Figure 9, and click **Apply**. The ARP entries with interface being GigabitEthernet1/0/19 and IP address range being 192.168.1.50 to 192.168.1.59 are displayed as shown in Figure 10.

Figure 9 Advanced search function example (II)

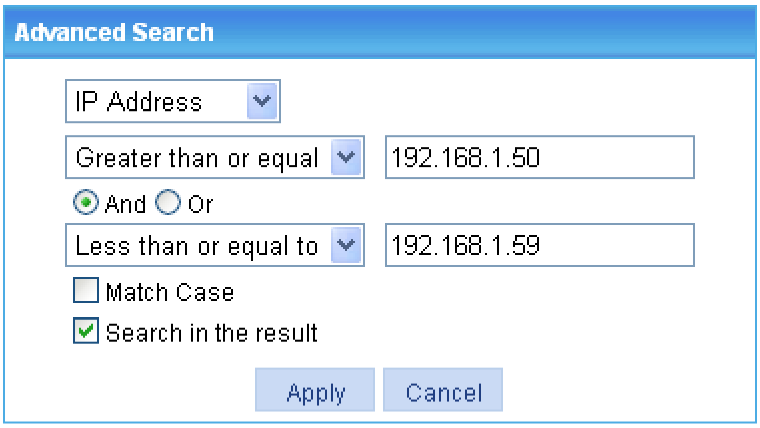
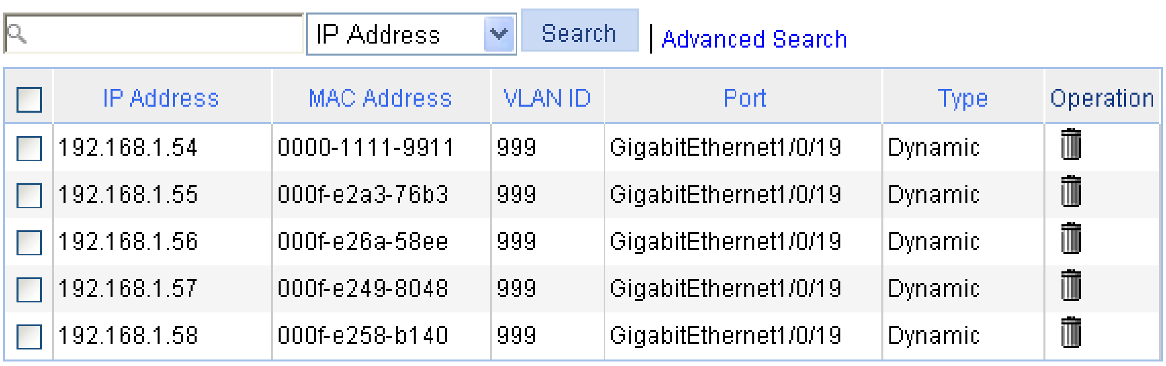


Figure 10 Advanced search function example (III)



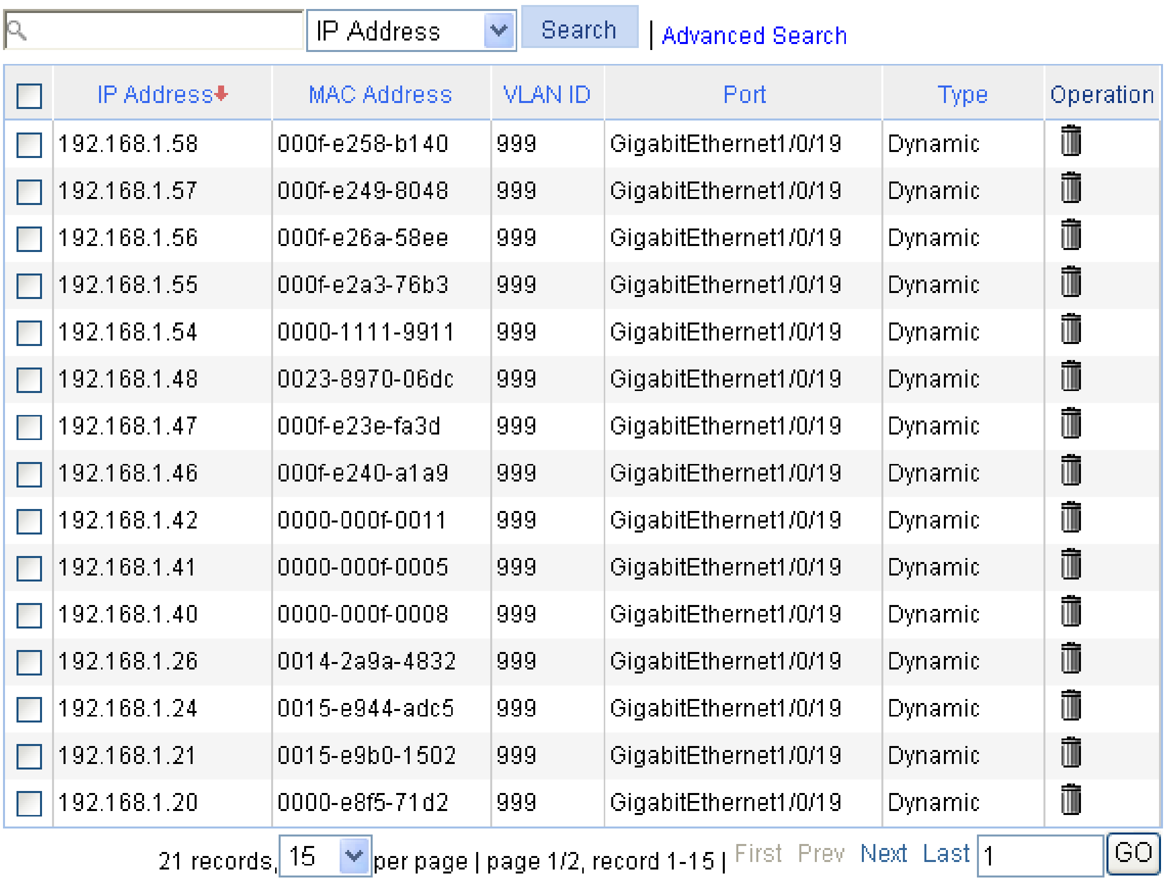
	IP Address	MAC Address	VLAN ID	Port	Type	Operation
	192.168.1.54	0000-1111-9911	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.55	000f-e2a3-76b3	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.56	000f-e26a-58ee	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.57	000f-e249-8048	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.58	000f-e258-b140	999	GigabitEthernet1/0/19	Dynamic	

Sorting function

On some list pages, the Web interface provides the sorting function to display the entries in a certain order.

As shown in Figure 11, you can click the blue heading item of each column to sort the entries based on the heading item you selected. Then, the heading item is displayed with an arrow beside it. The upward arrow indicates the ascending order, and the downward arrow indicates the descending order.

Figure 11 Sort display (based on MAC address in the ascending order)



	IP Address	MAC Address	VLAN ID	Port	Type	Operation
	192.168.1.58	000f-e258-b140	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.57	000f-e249-8048	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.56	000f-e26a-58ee	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.55	000f-e2a3-76b3	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.54	0000-1111-9911	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.48	0023-8970-06dc	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.47	000f-e23e-fa3d	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.46	000f-e240-a1a9	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.42	0000-000f-0011	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.41	0000-000f-0005	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.40	0000-000f-0008	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.26	0014-2a9a-4832	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.24	0015-e944-adc5	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.21	0015-e9b0-1502	999	GigabitEthernet1/0/19	Dynamic	
	192.168.1.20	0000-e8f5-71d2	999	GigabitEthernet1/0/19	Dynamic	

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

Configuration guidelines

- The Web console supports Windows XP, Windows 2000, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Vista, Linux and MAC OS operating systems.
- The Web console supports Microsoft Internet Explorer 6.0 SP2 and higher, Mozilla Firefox 3.0 and higher, Google Chrome 2.0.174.0 and higher.
- The Web console does not support the **Back**, **Next**, **Refresh** buttons provided by the browser. Using these buttons may result in abnormal display of Web pages.
- The Windows firewall limits the number of TCP connections, so 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, 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, delete the temporary Internet files of IE; otherwise, the Web page content may not be displayed correctly.
- A list can contain a maximum of 20000 entries if displayed in pages.

Troubleshooting web console

Unable to access devices through the web console

Symptom

You can ping and Telnet to a device, on which the HTTP service is running and the versions of the used operating system and IE browser comply with the requirements of the web console. However, you are unable to access the web console of the device.

Analysis

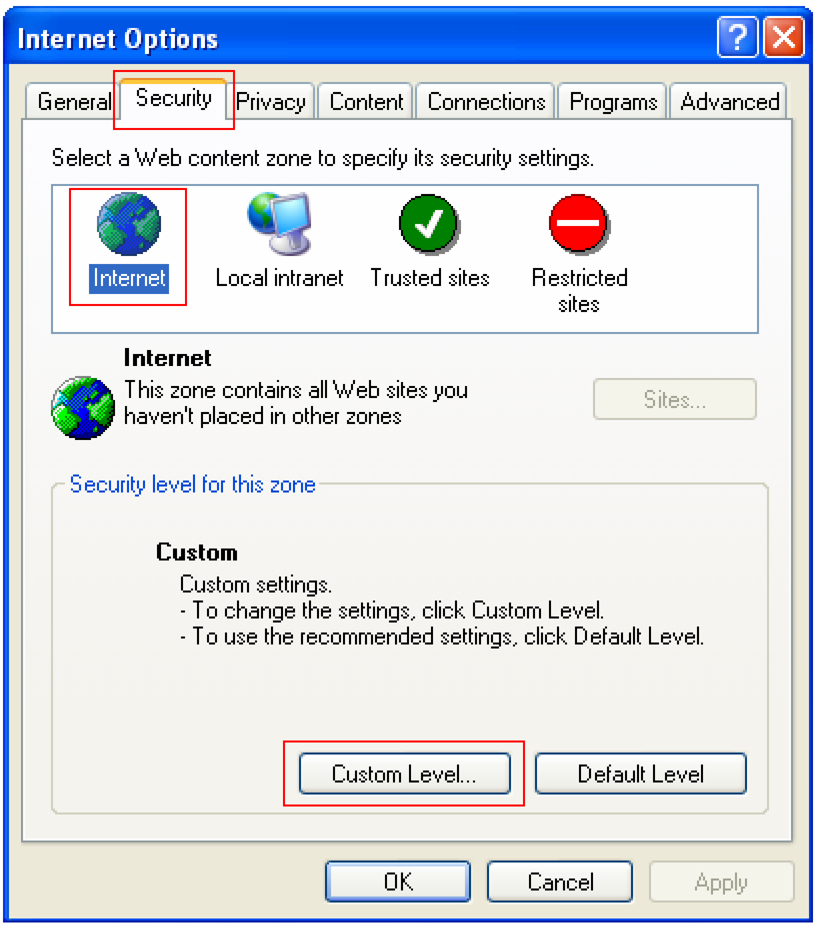
To access the web console:

- When using the Microsoft Internet Explorer browser, you must enable the security settings, including **Run ActiveX controls and plug-ins**, **Script ActiveX controls marked safe for scripting**, and **Active scripting**.
- When using the Mozilla Firefox browser, you must enable JavaScript.

For IE Browser

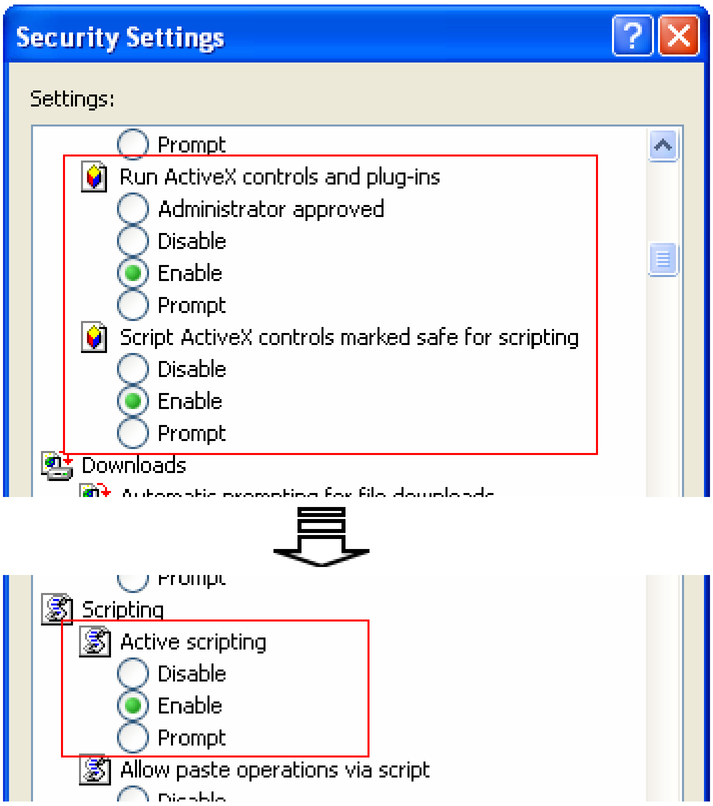
1. Launch the Internet Explorer, and select **Tools** > **Internet Options** from the main menu.
2. Select the **Security** tab, and select the content zone where the target website resides, as shown in Figure 12.

Figure 12 Internet Explorer settings (I)



3. Click **Custom Level**. The Security Settings dialog box appears, as shown in Figure 13.
4. Enable Run ActiveX controls and plug-ins, Script ActiveX controls marked safe for scripting, and Active scripting.

Figure 13 Internet Explorer settings (II)

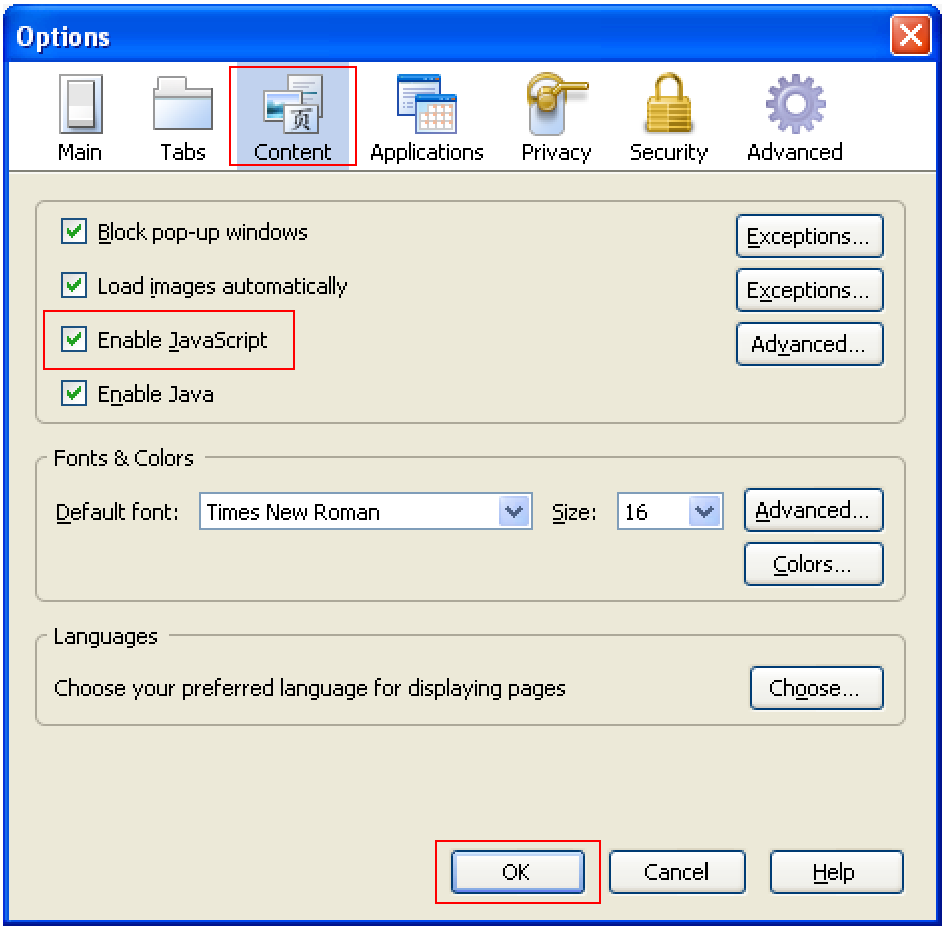


5. Click **OK** to save your settings.

For Firefox Browser

1. Launch the Firefox browser, and select **Tools** > **Options**. The **Options** dialog box appears, as shown in Figure 14.
2. Click **Content**, and select the **Enable JavaScript** check box.

Figure 14 Firefox browser settings



3. Click **OK** to save your settings.

Configuration at the CLI

The HP 1910 Switch Series can be configured through the CLI, Web interface, and SNMP/MIB, among which the Web interface supports all 1910 Switch 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 CLI

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 at the CLI.

This section describes using the CLI to manage the device.

Setting up the configuration environment

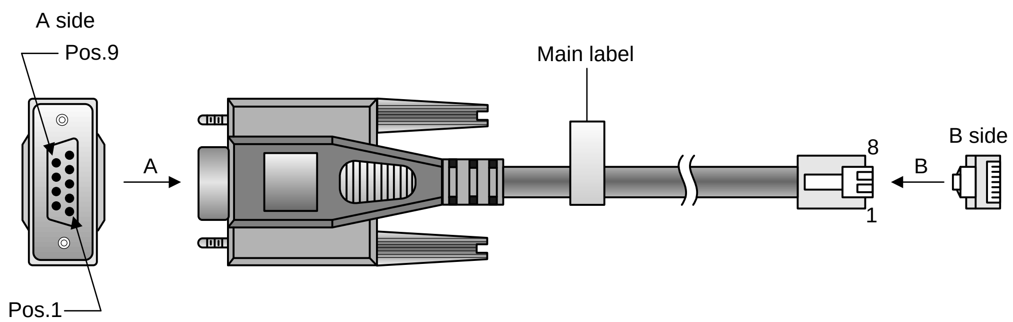
CAUTION:

Identify the mark on the console port to make sure that you are connecting to the correct port.

To set up the configuration environment, connect a terminal (a PC in this example) to the console port on the switch with a console cable.

A console cable is an 8-core shielded cable, with a crimped RJ-45 connector at one end for connecting to the console port of the switch, and a DB-9 female connector at the other end for connecting to the serial port on the console terminal.

Figure 15 Console cable



Use a console cable to connect a terminal device to the switch, as follows:

1. Plug the DB-9 female connector to the serial port of the console terminal or PC.
2. Connect the RJ-45 connector to the console port of the switch.

NOTE:

- The serial port on a PC does not support hot swapping. When you connect a PC to a powered-on switch, connect the DB-9 connector of the console cable to the PC before connecting the RJ-45 connector to the switch.
- When you disconnect a PC from a powered-on switch, disconnect the DB-9 connector of the console cable from the PC after disconnecting the RJ-45 connector from the switch.

Setting terminal parameters

To configure and manage the switch, you must run a terminal emulator program on the console terminal.

The following are the required terminal settings:

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

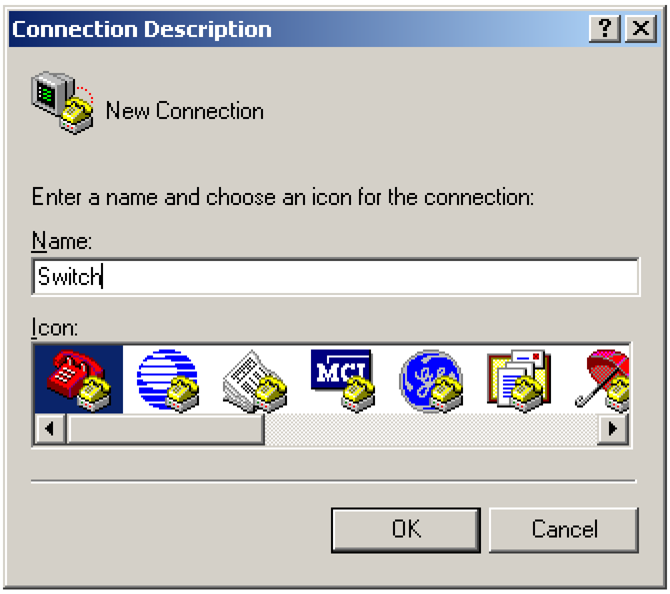
To set terminal parameters, for example, on a Windows XP HyperTerminal:

1. Select **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal**.

   The **Connection Description** dialog box appears.

2. Enter the name of the new connection in the **Name** field and click **OK**.

Figure 16 Connection description

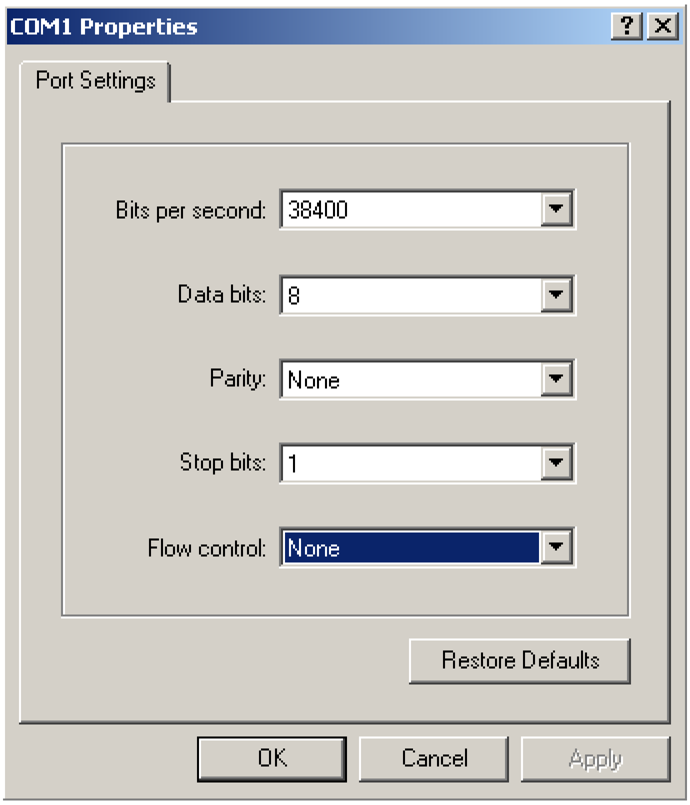


3. Select the serial port to be used from the **Connect using** list, and click **OK**.

Figure 17 Setting the serial port used by the HyperTerminal connection

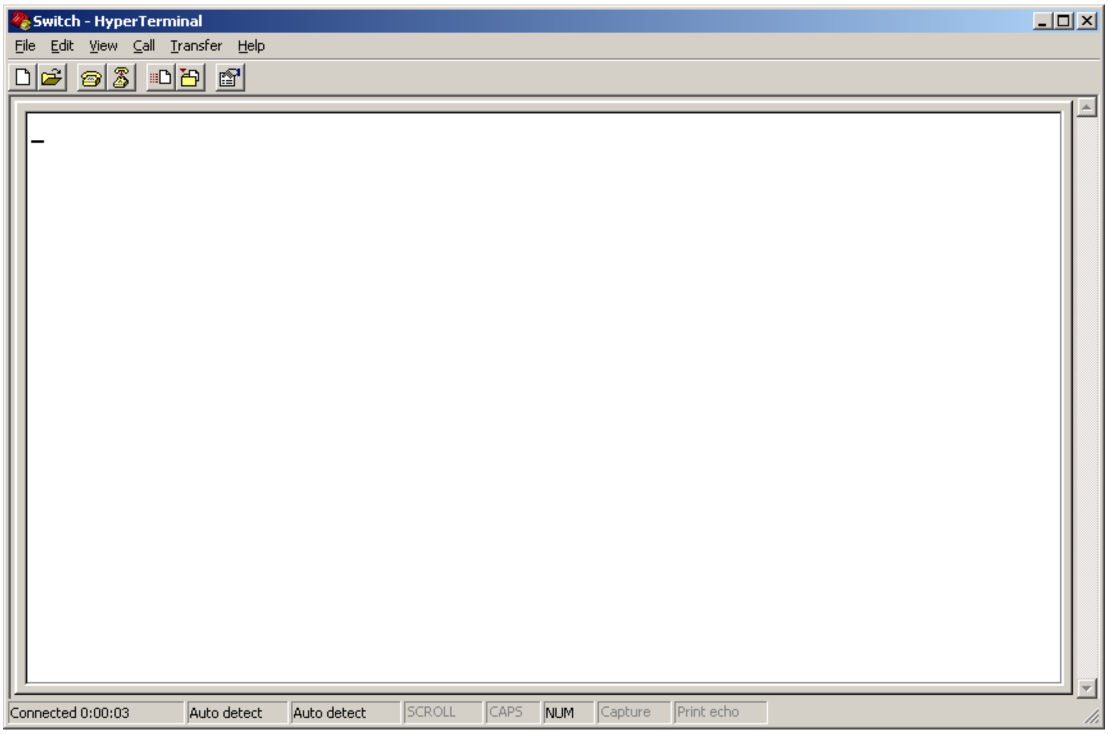
4. Set **Bits per second** to **38400**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 18 Setting the serial port parameters



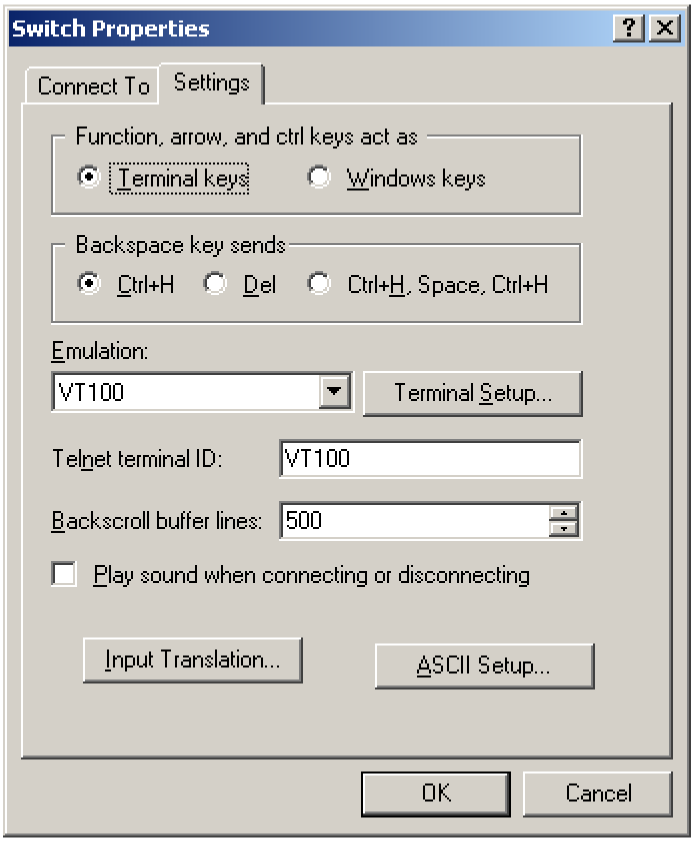
5. Select **File** > **Properties** in the HyperTerminal window.

Figure 19 HyperTerminal window



6. Click the **Settings** tab, set the emulation to **VT100**, and click **OK** in the **Switch Properties** dialog box.

Figure 20 Setting terminal emulation in Switch Properties dialog box



Logging in to the CLI

The login process requires a username and password. The default username for first time configuration is **admin**, no password is required. Usernames and passwords are case sensitive.

To log in to the CLI:

1. Press **Enter**. The **Username** prompt displays:
   ```
   Login authentication

   Username:
   ```
2. Enter your username at the **Username** prompt.
   ```
   Username:admin
   ```
3. Press **Enter**. The **Password** prompt appears.
   ```
   Password:
   ```
   The login information is verified, and the following CLI menu appears:
   ```
   <HP 1910 Switch>
   ```
   If the password is invalid, the following message appears and process restarts.
   ```
   % Login failed!
   ```

CLI commands

This section contains the following commands:

Task	Command
Display a list of CLI commands on the device.	**?**
Reboot the device and run the default configuration.	**initialize**
Configure VLAN-interface 1 to obtain an IPv4 address through DHCP or manual configuration.	**ipsetup** { **dhcp** | **ip-address** *ip-address* { *mask* | *mask-length* } [**default-gateway** *ip-address*] }
Configure VLAN-interface 1 to obtain an IPv6 address through the autoconfiguration function or manual configuration.	**ipsetup ipv6** { **auto** | **address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } [**default-gateway** *ipv6-address*] }
Modify the login password.	**password**
Log out of the system.	**quit**
Download the Boot ROM image or system software image file from the TFTP server and specify it as the startup configuration file.	**upgrade** [**ipv6**] *server-address source-filename* { **bootrom** | **runtime** }
Reboot the device and run the main configuration file.	**reboot**
View the summary information about the device.	**summary**
Ping a specified destination.	**ping** [**ipv6**] *host*
Tear down the current connection and quit the system.	**quit**

initialize

Syntax

initialize

Parameters

None

Description

Use **initialize** 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: Enables VLAN-interface 1 to obtain an IPv4 address through DHCP.

ip-address *ip-address*: Specifies an IPv4 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 IPv4 address of the default gateway. With this argument and keyword combination configured, the command not only assigns an IPv4 address to the interface, but also specifies a default route for the device.

Description

Use **ipsetup dhcp** to specify VLAN-interface 1 to obtain an IPv4 address through DHCP.

Use **ipsetup ip address** *ip-address* { *mask* | *mask-length* } to assign an IPv4 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. For more information, see Figure 2.

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 IPv4 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
```

ipsetup ipv6

Syntax

ipsetup ipv6 { **auto** | **address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } [**default-gateway** *ipv6-address*] }

Parameters

auto: Enables the stateless address autoconfiguration function. With this function enabled, VLAN-interface 1 can automatically generate a global unicast address and link local address.

address: Enables manual configuration of a global unicast IPv6 address for VLAN-interface 1.

ipv6-address: Specifies an IPv6 address.

prefix-length: Prefix length, in the range of 1 to 128.

default-gateway *ipv6-address*: Specifies the IPv6 address of the default gateway. With this argument and keyword combination configured, the command not only assigns an IPv6 address to the interface, but also specifies a default route for the device.

Description

Use **ipsetup ipv6 auto** to enable the stateless address autoconfiguration function so a global unicast address and link local address can be automatically generated.

Use **ipsetup ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } [**default-gateway** *ipv6-address*] to manually assign an IPv6 address to VLAN-interface 1.

Examples

Create VLAN-interface 1 and enable VLAN-interface 1 to automatically generate a global unicast IPv6 address and link local address.

```
<Sysname> ipsetup ipv6 auto
```

Create VLAN-interface 1 and assign 2001::2 to the interface, with the prefix length 64, and specify 2001::1 as the default gateway.

```
<Sysname> ipsetup ipv6 address 2001::2 64 default-gateway 2001::1
```

password

Syntax

password

Parameters

None

Description

Use **password** 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 IPv4 address (in dotted decimal notation) or host name (a string of 1 to 255 characters).

Description

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

To terminate a ping operation, press **Ctrl**+**C**.

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 output 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.

ping ipv6

Syntax

ping ipv6 *host*

Parameters

host: Destination IPv6 address or host name (a string of 1 to 255 characters).

Description

Use **ping ipv6** to ping a specified destination.

To terminate a ping operation, press **Ctrl**+**C**.

Examples

Ping IPv6 address 2001::4.

```
<Sysname> ping ipv6 2001::4
  PING 2001::4 : 56  data bytes, press CTRL_C to break
    Reply from 2001::4
    bytes=56 Sequence=1 hop limit=64  time = 15 ms
    Reply from 2001::4
    bytes=56 Sequence=2 hop limit=64  time = 2 ms
    Reply from 2001::4
    bytes=56 Sequence=3 hop limit=64  time = 11 ms
    Reply from 2001::4
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 2001::4
    bytes=56 Sequence=5 hop limit=64  time = 12 ms

  --- 2001::4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/8/15 ms
```

The output shows that IPv6 address 2001::4 is reachable and the echo replies are all returned from the destination. The minimum, average, and maximum roundtrip intervals are 2 milliseconds, 8 milliseconds, and 15 milliseconds respectively.

quit

Syntax

quit

Parameters

None

Description

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

Examples

Log out of the system.

```
<Sysname> quit
******************************************************************************
* Copyright (c) 2004-2012 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<Sysname>
```

reboot

Syntax

reboot

Parameters

None

Description

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

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

Examples

Display summary information about the device.

```
<sysname>summary
Select menu option:             Summary
```

```
IP Method:                      Manual
IP address:                     10.153.96.86
Subnet mask:                    255.255.255.0
Default gateway:

IPv6 Method:                    Manual
IPv6 link-local address:        FE80::2E0:FCFF:FE00:3621
IPv6 subnet mask length:        10
IPv6 global address:            2001::1
IPv6 subnet mask length:        64
IPv6 default gateway:           2001::2

Current boot app is: flash:/1910-cmw520-f1510.bin
Next main boot app is: flash:/1910-cmw520-f1510.bin
Next backup boot app is: NULL

HP Comware Platform Software
Comware Software, Version 5.20,
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP 1910-8G-PoE+ (65W) Switch uptime is 0 week, 0 day, 2 hours, 1 minute

HP 1910-8G-PoE+ (65W) Switch
128M    bytes DRAM
128M    bytes Nand Flash Memory
Config Register points to Nand Flash

Hardware Version is REV.A
CPLD Version is 001
Bootrom Version is 156
[SubSlot 0] 8GE+1SFP+POE Hardware Version is REV.A
```

upgrade

Syntax

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

Parameters

server-address: IPv4 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 image in the software package file as the startup configuration file.

runtime: Specifies the system software image file in the software package file as the startup configuration file.

Description

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

Use **upgrade** *server-address source-filename* **runtime** to upgrade the system software image file. If the system software image file in the downloaded software package file is not applicable, the original system software image file is still used as the startup configuration file.

To validate the downloaded software package file, reboot the device.

NOTE:

The HP 1910 Switch Series does not provide an independent Boot ROM image. Instead, it integrates the Boot ROM image with the system software image file together in a software package file with the extension name of **.bin**.

Examples

Download software package file **main.bin** from the TFTP server and use the Boot ROM image in the package as the startup configuration file.

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

Download software package file **main.bin** from the TFTP server and use the system software image file in the package as the startup configuration file.

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

upgrade ipv6

Syntax

upgrade ipv6 *server-address source-filename* { **bootrom** | **runtime** }

Parameters

server-address: IPv6 address of a TFTP server.

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

bootrom: Specifies the Boot ROM image in the software package file as the startup configuration file.

runtime: Specifies the system software image file in the software package file as the startup configuration file.

Description

Use **upgrade ipv6** *server-address source-filename* **bootrom** to upgrade the Boot ROM image. If the Boot ROM image in the downloaded software package file is not applicable, the original Boot ROM image is still used as the startup configuration file.

Use **upgrade ipv6** *server-address source-filename* **runtime** to upgrade the system software image file. If the system software image file in the downloaded software package file is not applicable, the original system software image file is still used as the startup configuration file.

To validate the downloaded software package file, reboot the device.

NOTE:

The HP 1910 Switch Series does not provide an independent Boot ROM image; instead, it integrates the Boot ROM image with the system software image file together in a software package file with the extension name of **.bin**.

Examples

Download software package file **main.bin** from the TFTP server and use the Boot ROM image in the package as the startup configuration file.

```
<Sysname> upgrade ipv6 2001::2 main.bin bootrom
```

Download software package file **main.bin** from the TFTP server and use the system software image file in the package as the startup configuration file.

```
<Sysname> upgrade ipv6 2001::2 main.bin runtime
```

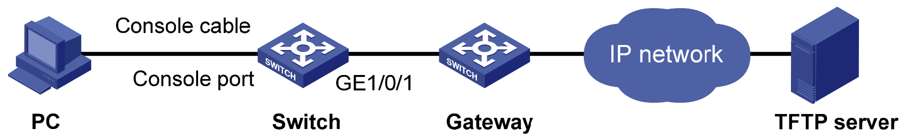
Configuration example for upgrading the system software image at the CLI

Network requirements

As shown in Figure 21, a 1910 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 system software image (suppose its name is **Switch1910.bin**) is located is 192.168.10.1/24. The gateway and the switch can reach each other.

The administrator upgrades the Boot ROM image and the system software image file of the 1910 switch through the PC and sets the IP address of the switch to 192.168.1.2/24.

Figure 21 Network diagram



Configuration procedure

1. Run the TFTP server program on the TFTP server, and specify the path of the file to be loaded. (Omitted)
2. Configure 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 software package file **Switch1910.bin** on the TFTP server to the switch, and upgrade the system software image in the package.

   ```
   <Switch> upgrade 192.168.10.1 Switch1910.bin runtime
     File will be transferred in binary mode
     Downloading file from remote TFTP server, please wait.../
     TFTP: 10262144 bytes received in 71 second(s)
     File downloaded successfully.
   ```

   # Download the software package file **Switch1910.bin** on the TFTP server to the switch, and upgrade the Boot ROM image.

   ```
   <Switch> upgrade 192.168.10.1 Switch1910.bin bootrom
   The file flash:/Switch1910.bin exists. Overwrite it? [Y/N]:y
     Verifying server file...
     Deleting the old file, please wait...
     File will be transferred in binary mode
     Downloading file from remote TFTP server, please wait.../
     TFTP: 10262144 bytes received in 61 second(s)
   ```

```
  File downloaded successfully.
  BootRom file updating finished!
```

Reboot the switch.

```
<Switch> reboot
```

After getting the new image file, reboot the switch to validate the upgraded image.

Configuration wizard

Overview

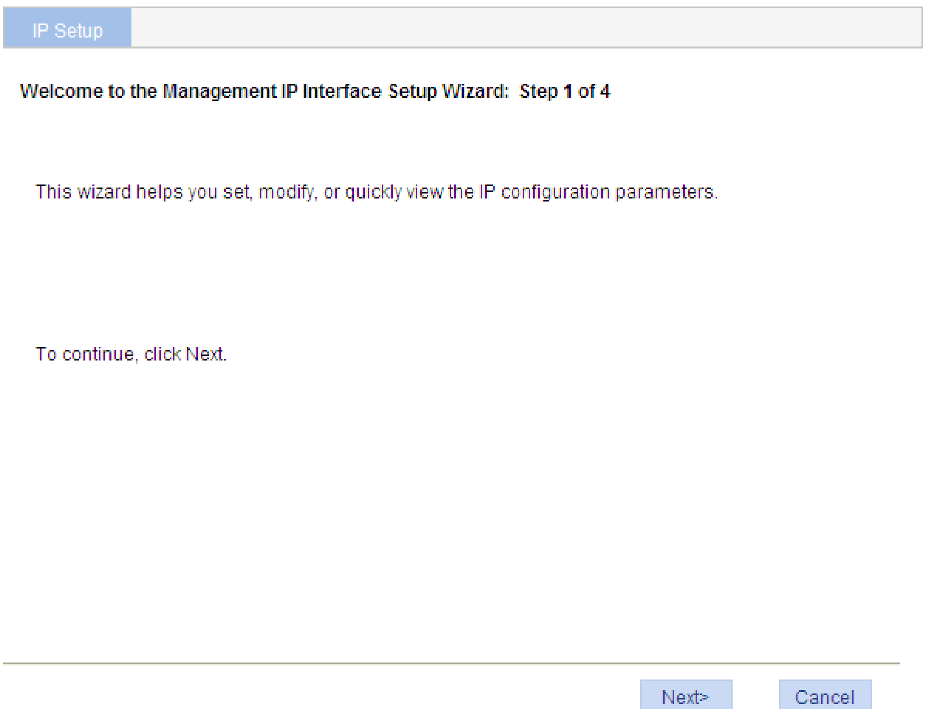
The configuration wizard guides you through configuring the basic service parameters, including the system name, the system location, the contact information, and the management IP address.

Basic service setup

Entering the configuration wizard homepage

Select **Wizard** from the navigation tree.

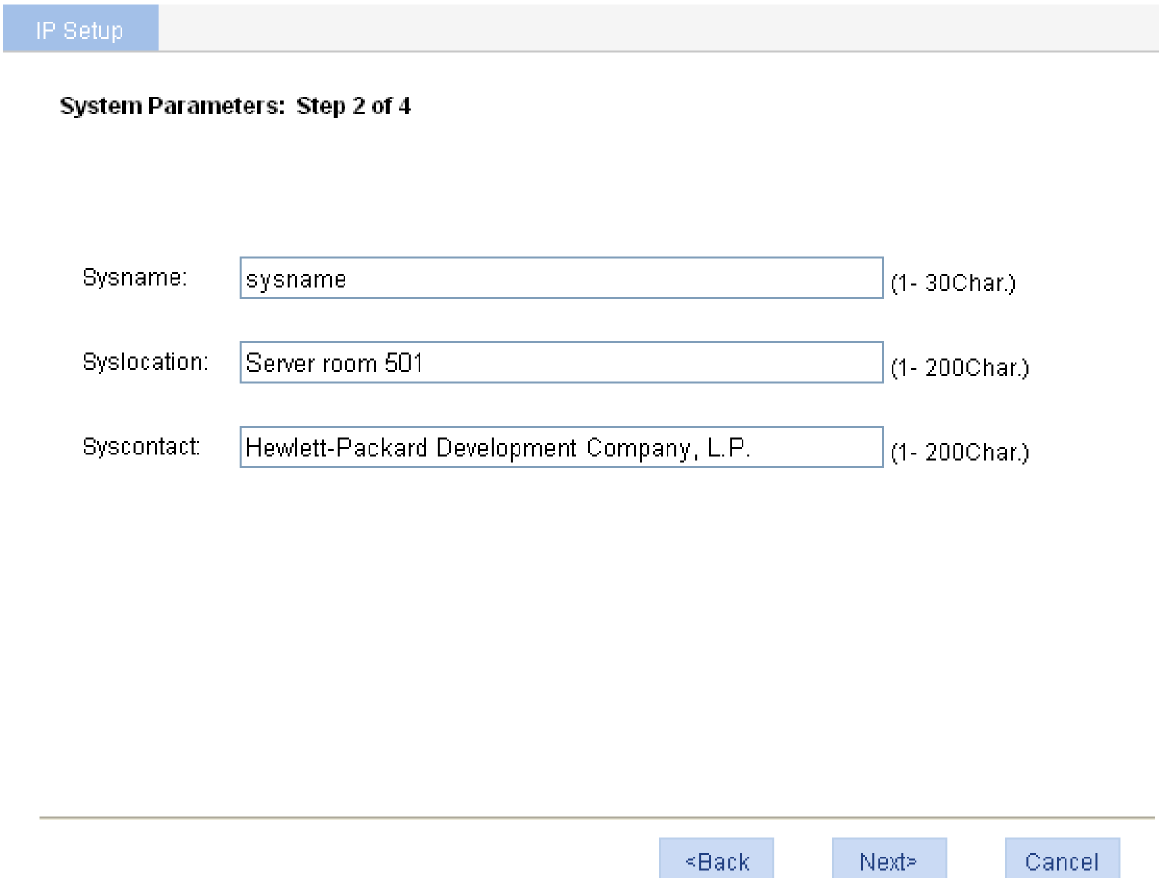
Figure 22 Configuration wizard homepage



Configuring system parameters

1. On the wizard homepage, click **Next**.

Figure 23 System parameter configuration page



2. Configure the parameters as described in Table 3.

Table 3 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 more information, see "Configuring basic device settings."
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 more information, see "Configuring SNMP."
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 more information, see "Configuring SNMP."

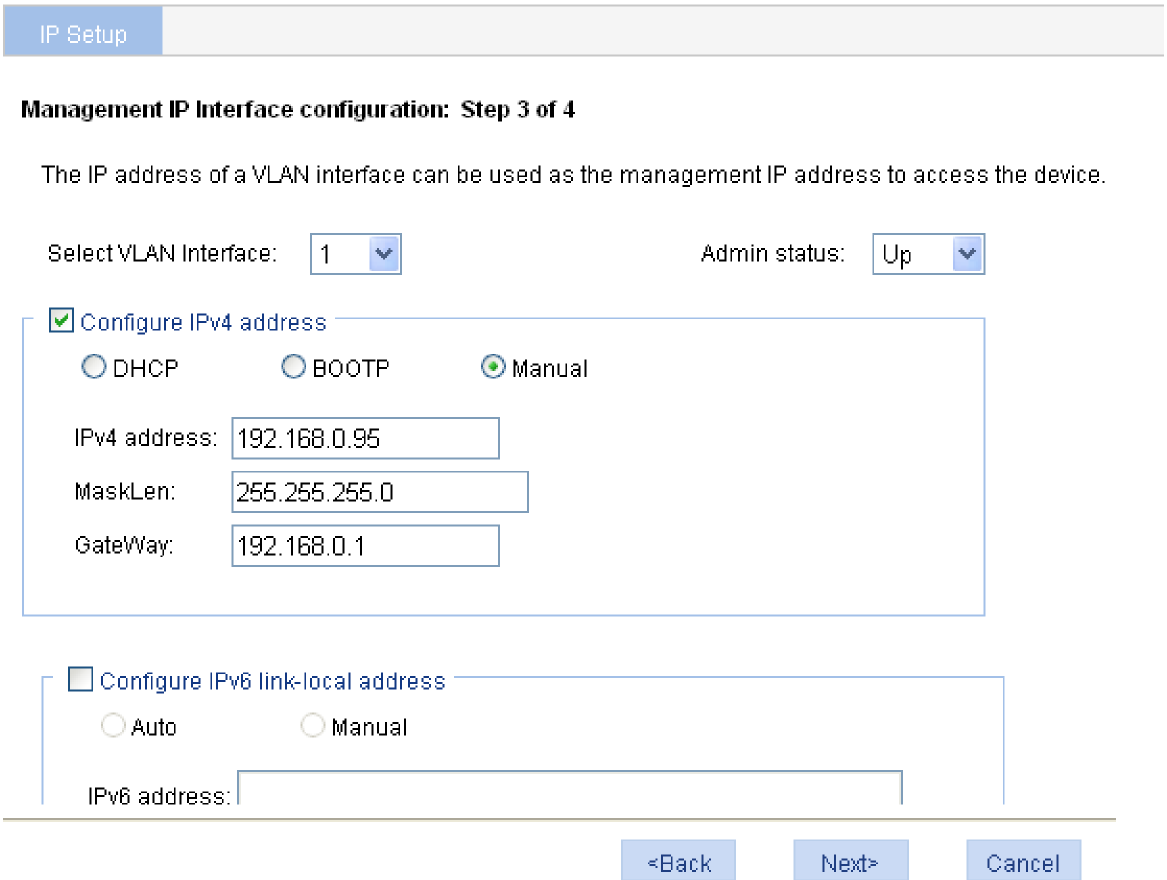
Configuring management IP address

CAUTION:

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

1. On the system parameter configuration page, click **Next**.

Figure 24 Management IP address configuration page



2. Configure the parameters as described in Table 4.

Table 4 Configuration items

Item	Description
Select VLAN Interface	Select a VLAN interface. Available VLAN interfaces are those configured in the page that you enter by selecting **Network** > **VLAN Interface** and selecting the **Create** tab. The IP address of a VLAN interface can be used as the management IP address to access the device. You can configure a VLAN interface and its IP address in the page that you enter by selecting **Network** > **VLAN Interface**. For more information, see "Configuring VLAN interfaces."
Admin status	Enable or disable the VLAN interface. When errors occurred in 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. IMPORTANT: 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.

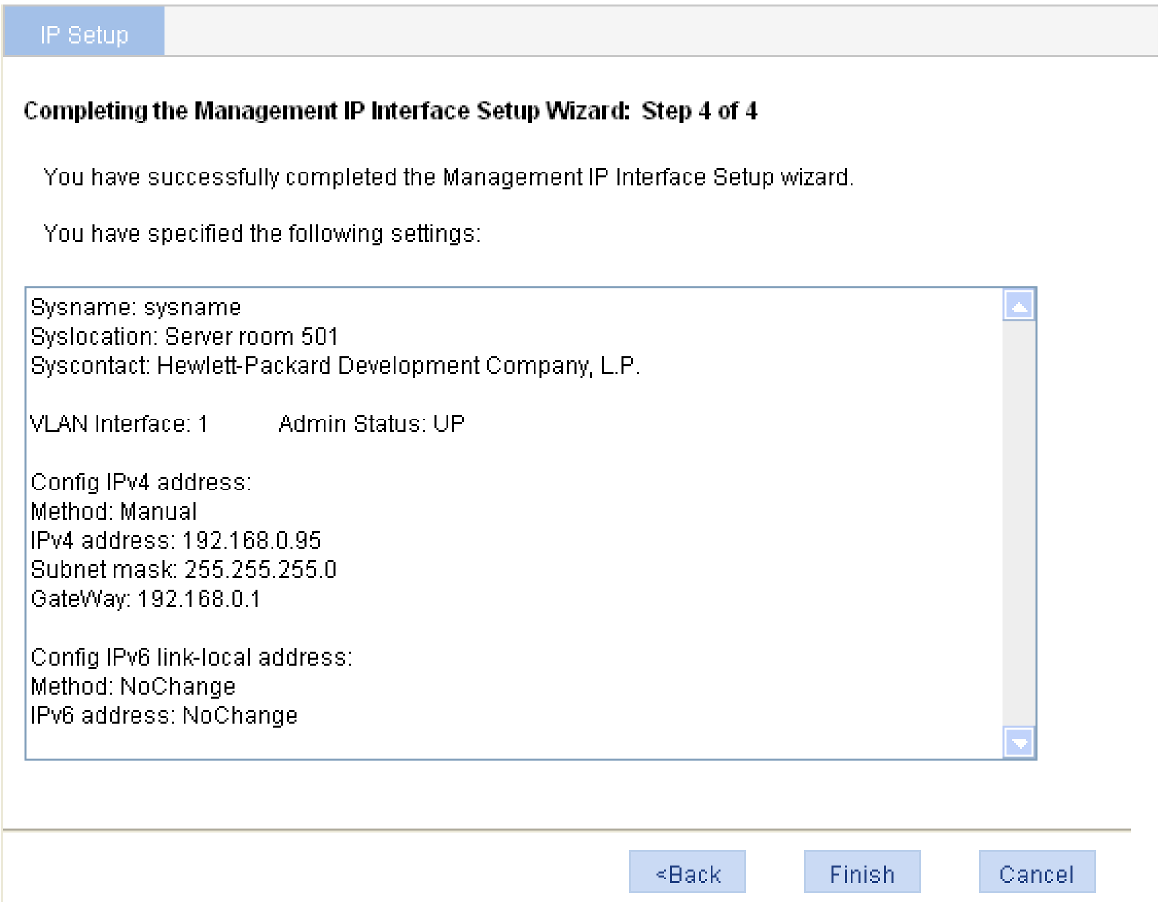
Item	Description	
Configure IPv4 address	DHCP BOOTP Manual	Configure how the VLAN interface obtains an IPv4 address. • **DHCP**—Specifies the VLAN interface to obtain an IPv4 address by DHCP. • **BOOTP**—Specifies the VLAN interface to obtain an IPv4 address through BOOTP. • **Manual**—Allows you to specify an IPv4 address and a mask length.
	IPv4 address MaskLen	Specify an IPv4 address and the mask length for the VLAN interface. Dotted decimal notation is also allowed for the mask length field. These two fields are configurable if **Manual** is selected.
	Gateway	Specify the gateway IP address. By default, the gateway IP address is not specified. Specify the gateway IP address if the device needs to connect to the Internet.
Configure IPv6 link-local address	Auto Manual	Configure how the VLAN interface obtains an IPv6 link-local address. • **Auto**—Specifies the device to automatically generate an link-local address based on the link-local address prefix (FE80::/64) and the link layer address of the interface. • **Manual**—Allows you to specify an IPv6 address.
	IPv6 address	Specify an IPv6 link-local address for the VLAN interface. This field is configurable if **Manual** is selected. The address prefix must be FE80::/64.

Finishing configuration wizard

After finishing the management IP address configuration, click **Next**.

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.

Figure 25 Configuration finishes

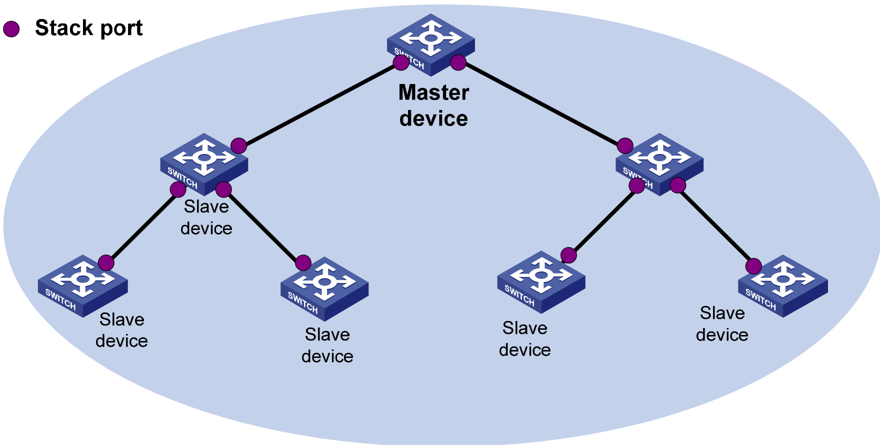


Configuring stack

Overview

The stack management feature enables you to configure and monitor a group of connected switches by logging in to one switch in the stack, as shown in Figure 26.

Figure 26 Network diagram



To set up a stack for a group of connected switches, you must log in to one switch to create the stack. This switch is the master switch for the stack, and you configure and monitor all other member switches on the master switch. The ports that connect the stack member switches are called stack ports.

Configuration task list

Task	Remarks
Configuring the master device of a stack:	
Configuring global stack parameters	Required. Configure a private IP address pool and set up the stack. By default, no IP address pool is configured for a stack and no stack is set up.
Configuring stack ports	Required. Configure the ports connected to member devices as stack ports. By default, no ports are configured as stack ports.
Configuring stack member devices: Configuring stack ports	Required. Configure ports connected to the master device or other stack member devices as stack ports. By default, no ports are configured as stack ports.

Task	Remarks
Displaying topology summary of a stack	Optional. Display stack member information.
Displaying device summary of a stack	Optional. Display the control panels of stack members. IMPORTANT: To successfully display control panel information, make sure that the user account you are logged in with to the master has also been created on each member device. You can configure the user account by selecting **Device** and then clicking **Users** from the navigation tree.
Logging in to a member device from the master	Optional. Log in to the web network management interface of a member device from the master device. IMPORTANT: To successfully log in to a member device from the master device, make sure that the user account you are logged in with to the master has also been created on the member device. You can configure the user account by selecting **Device** and then clicking **Users** from the navigation tree.

Configuring global stack parameters

1. Log in to the Web interface of the master device.
2. Select **Stack** from the navigation tree to enter the page shown in Figure 27.
3. Configure global stack parameters in the **Global Settings** area.

Figure 27 Setting up a fabric

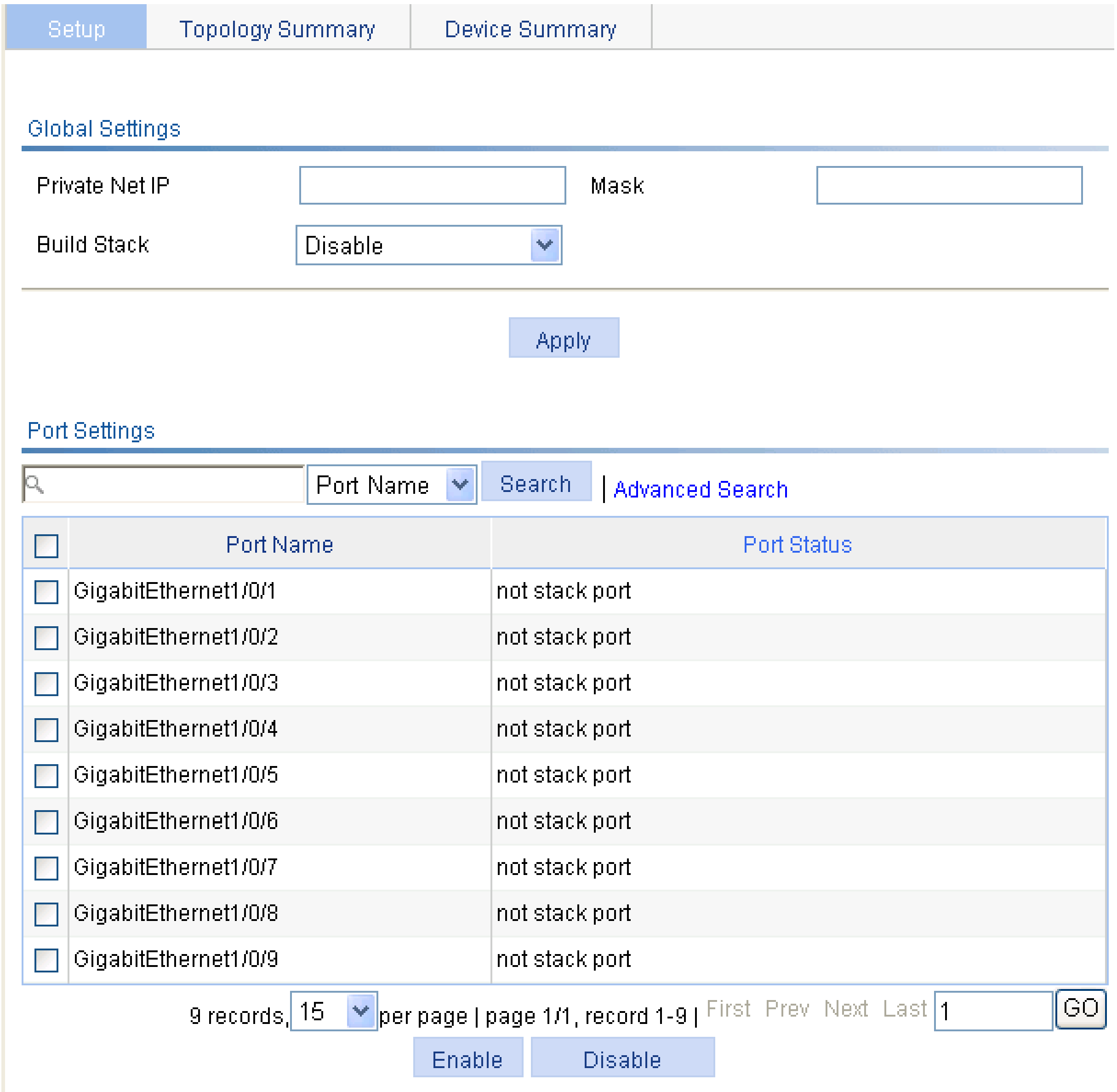


Table 5 Configuration items

Item	Description
Private Net IP Mask	Configure a private IP address pool for the stack. The master device automatically picks an IP address from this pool for each member device for intra-stack communication. IMPORTANT: Make sure the number of IP addresses in the address pool is equal to or greater than the number of devices to be added to the stack. If not, some devices cannot automatically join the stack for lack of private IP addresses.

Item	Description
Build Stack	Create the stack. As the result, the device becomes the master device of the stack and automatically adds the devices connected to its stack ports to the stack. IMPORTANT: You can delete the stack only on the master device. The **Global Settings** area is grayed out for stack member devices.

Configuring stack ports

1. Log in to the master device and each member device to perform this task.
2. Select **Stack** from the navigation tree to enter the page shown in Figure 27.
3. Configure stack ports in the **Port Settings** area, as follows:
   - Select the box before a port name, and click **Enable** to configure the port as a stack port.
   - Select the box before a port name, and click **Disable** to configure the port as a non-stack port.

Displaying topology summary of a stack

Select **Stack** from the navigation tree and click the **Topology Summary** tab to enter the page shown in Figure 28.

Figure 28 Topology Summary tab

Table 6 describes the fields of topology summary.

Table 6 Field description

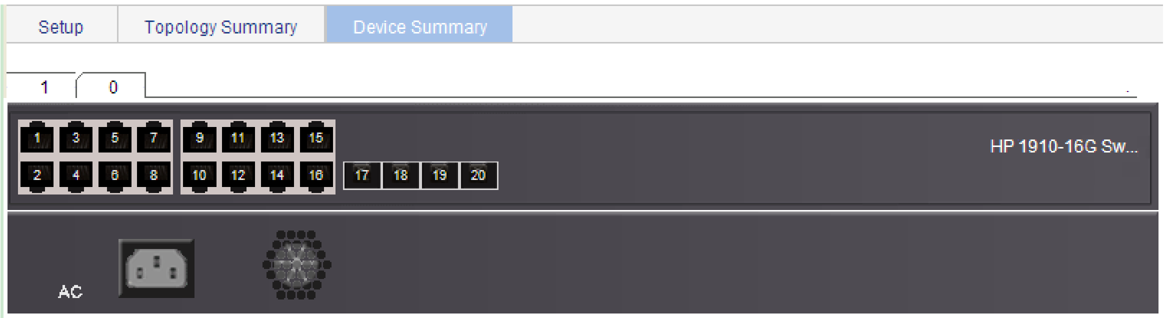
Fields	Description
Device ID	Member ID of the device in the stack: • **0**—The device is the master device. • **Any other value**—The device is a member device and the value is the member ID of the member device in the stack.
Device Role	Role of the device in the stack: master or member.

Displaying device summary of a stack

Select **Stack** from the navigation tree and click the **Device Summary** tab to enter the page shown in Figure 29.

View interfaces and power socket layout on the panel of each stack member by clicking their respective tabs.

Figure 29 Device Summary tab (on the master device)



Return to Configuration task list.

Logging in to a member device from the master

1. Select **Stack** from the navigation tree.
2. Click the **Device Summary** tab.
3. Click a member device ID tab.
4. On the page in Figure 30, click the **Configuring the Device** link.

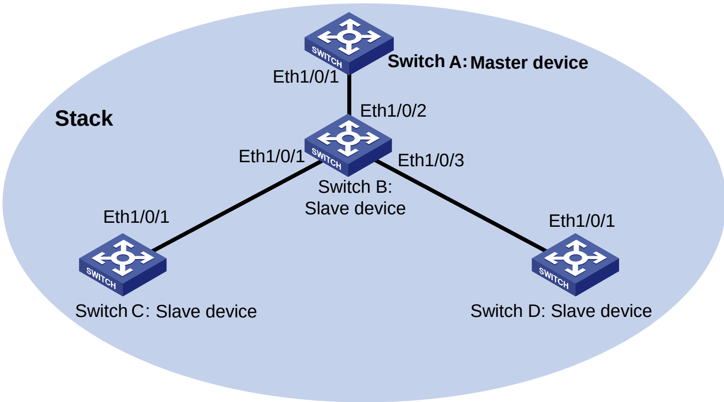
Figure 30 Device Summary tab (on a member device)

Stack configuration example

Network requirements

As shown in Figure 31, create a stack that comprises Switch A, Switch B, Switch C, and Switch D. Use Switch A as the master device so an administrator can log in to any other stack member device through Switch A for remote configuration and management.

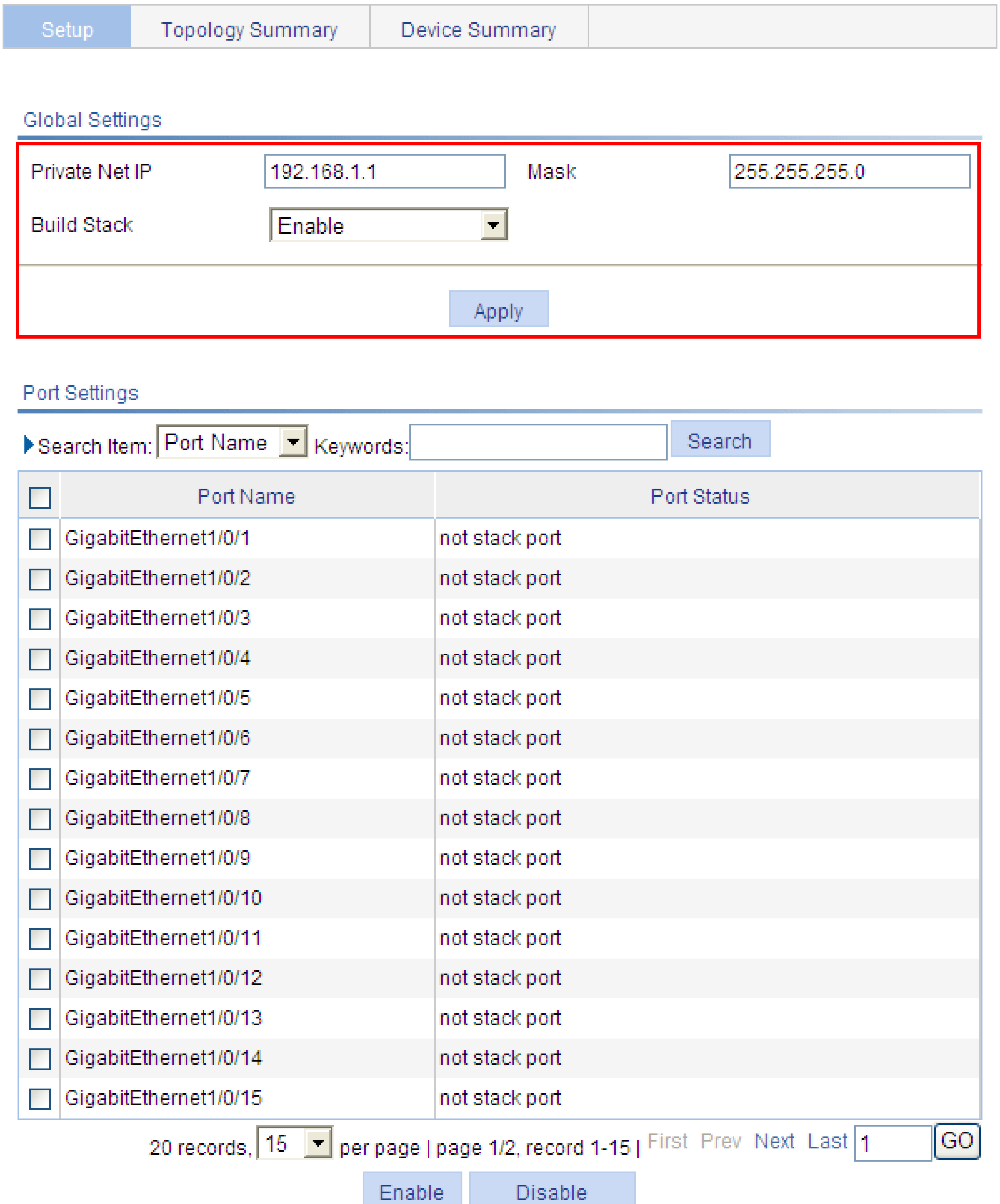
Figure 31 Network diagram



Configuration procedure

1. Configure global stack parameters on Switch A:
   a. Select **Stack** 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 32.

Figure 32 Configuring global stack parameters on Switch A



b. Type **192.168.1.1** in the field of **Private Net IP**.
c. Type **255.255.255.0** in the field of **Mask**.
d. Select **Enable** from the **Build Stack** list.
e. Click **Apply**.

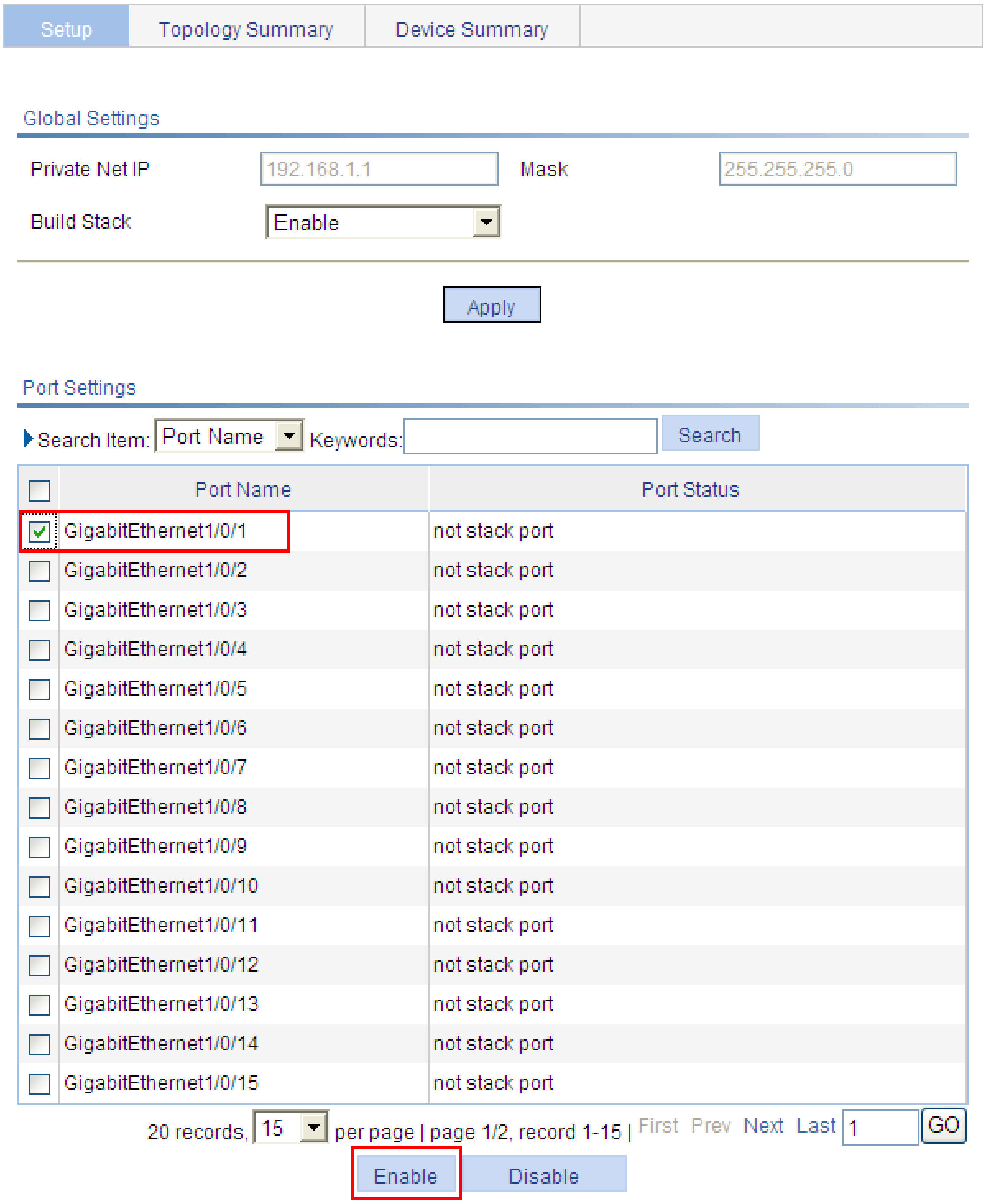
Now, switch A becomes the master device.

2. Configure the stack port on Switch A:

a. On the **Setup** tab, select the box before **Ethernet1/0/1** in the **Port Settings** area.

b. Click **Enable**.

Figure 33 Configuring a stack port on Switch A



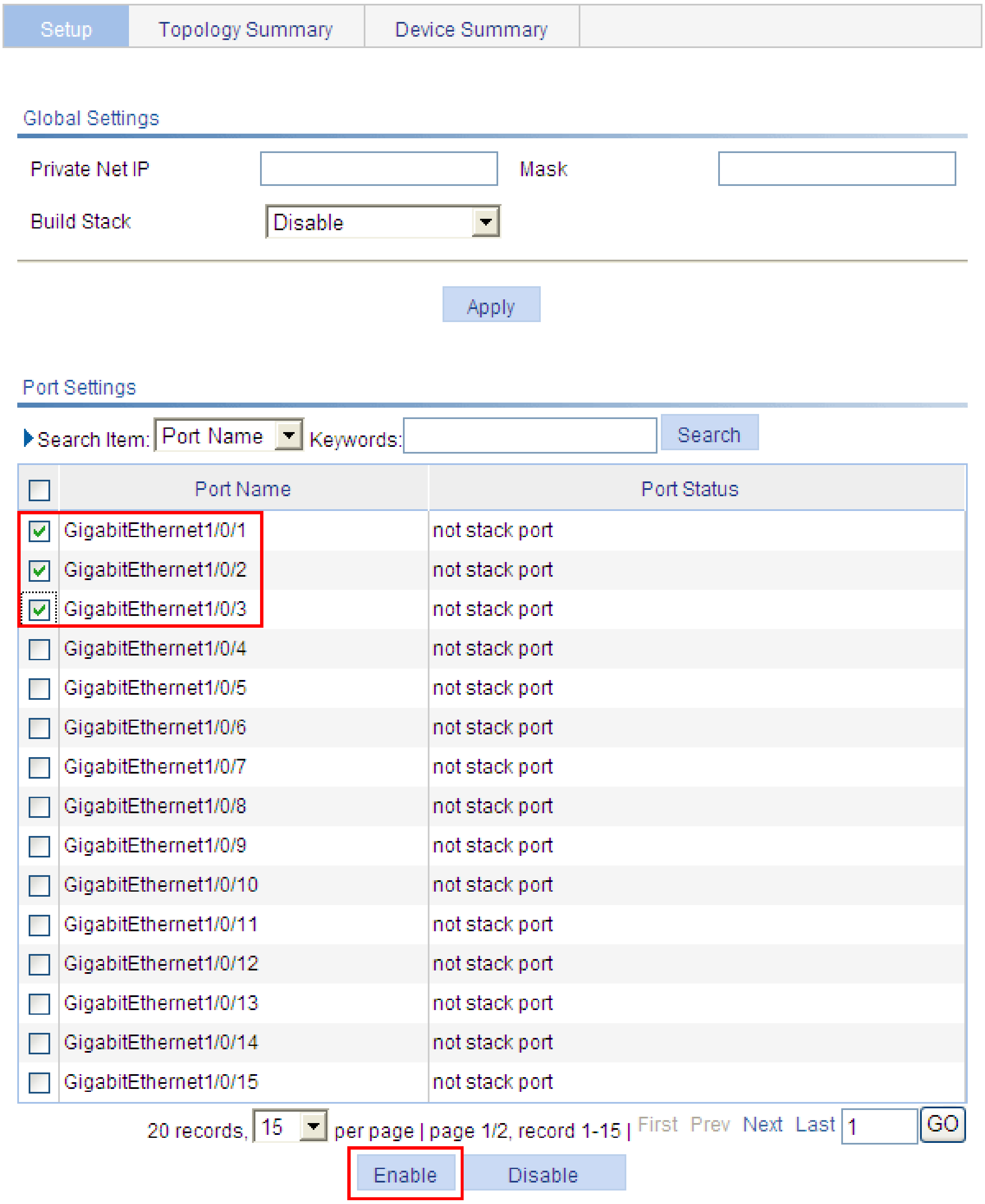
3. On Switch B, configure ports Ethernet 1/0/2, Ethernet 1/0/1, and Ethernet 1/0/3 as stack ports.

   a. Select **Stack** from the navigation tree of Switch B.

   b. On the **Setup** tab, select the boxes before **Ethernet1/0/1**, **Ethernet1/0/2**, and **Ethernet1/0/3** in the **Port Settings** area.

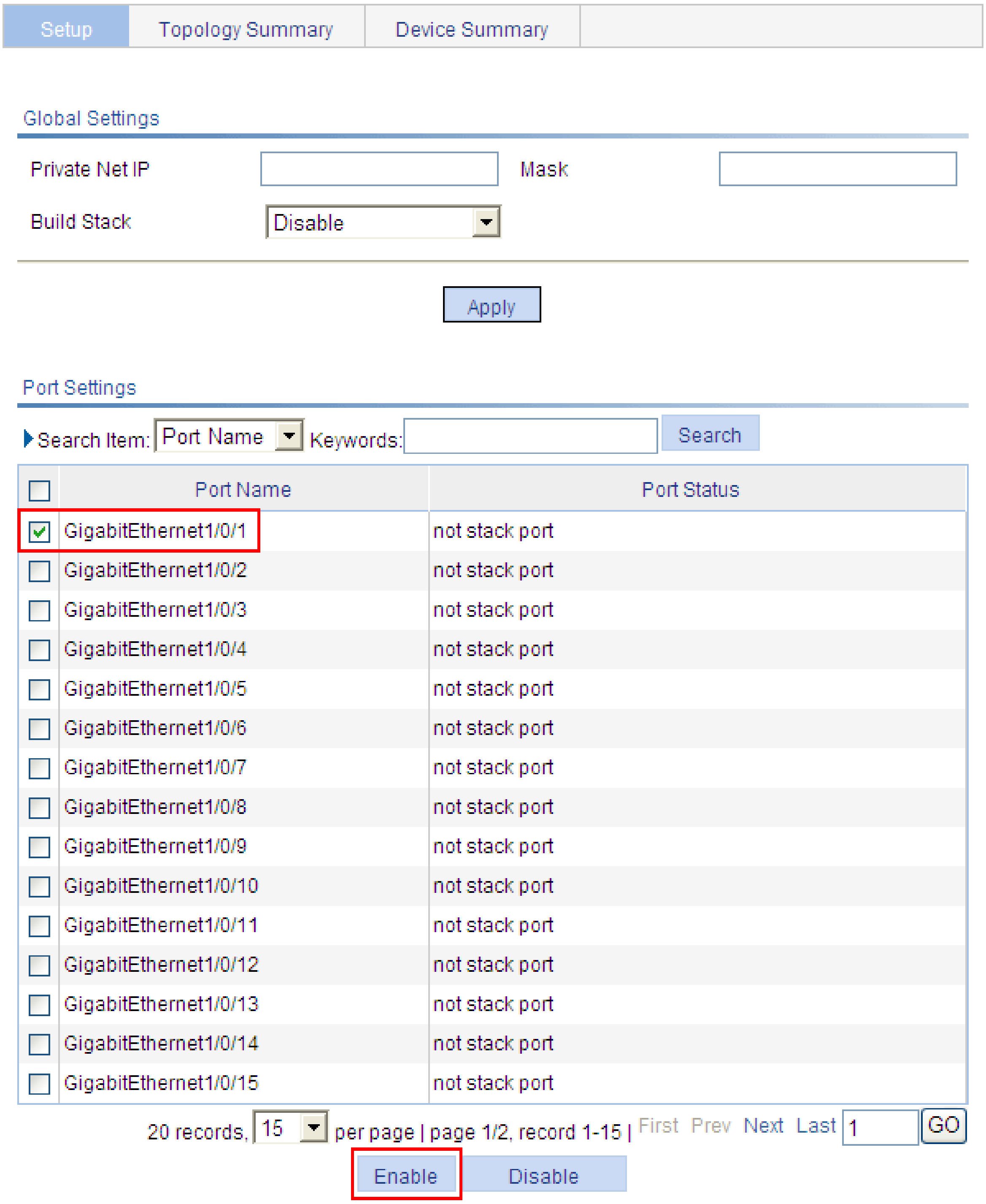
c. Click **Enable**.

Figure 34 Configuring stack ports on Switch B



4. On Switch C, configure port Ethernet 1/0/1 as a stack port.
   a. Select **Stack** from the navigation tree of Switch C.
   b. On the **Setup** tab, select the box before **Ethernet1/0/1** in the **Port Settings** area.
   c. Click **Enable**.

Figure 35 Configuring a stack port on Switch C

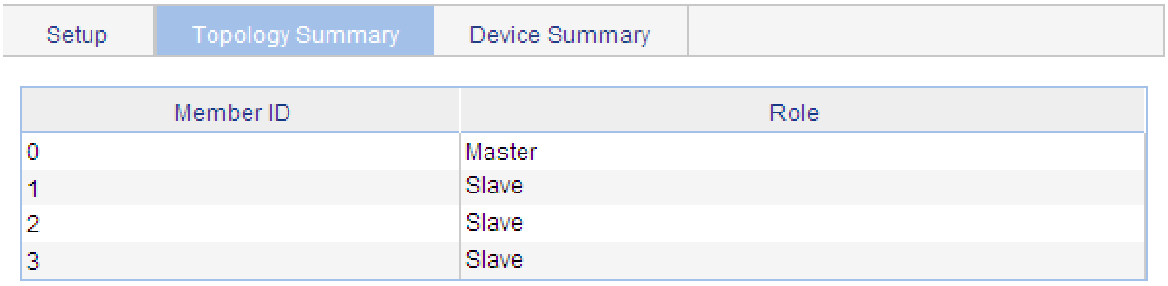


5. On Switch D, configure port Ethernet 1/0/1 as a stack port.
   a. Select **Stack** from the navigation tree of Switch D.
   b. On the **Setup** tab, select the box before **Ethernet1/0/1** in the **Port Settings** area.
   c. Click **Enable**.

Verifying the configuration

Select **Stack** from the navigation tree and click the **Topology Summary** tab to display the stack topology on Switch A.

Figure 36 Verifying the configuration



Member ID	Role
0	Master
1	Slave
2	Slave
3	Slave

Configuration guidelines

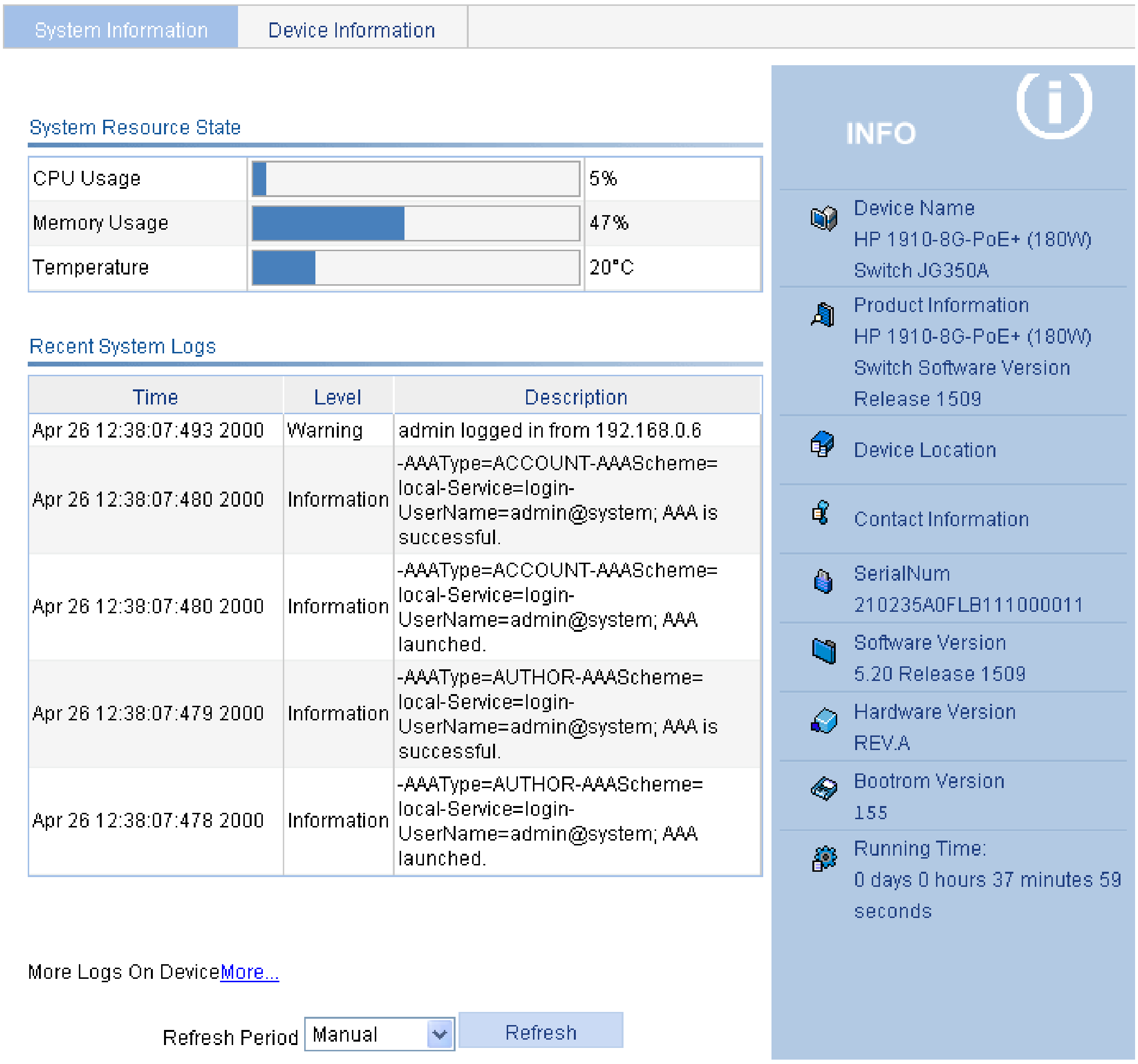
- If a device is already configured as a stack master device, you cannot modify the private IP address pool on the device.
- If a device is already configured as a stack member device, the **Global Settings** area on the member device is grayed out.

Displaying system and device information

Displaying system information

Select Summary from the navigation tree to enter the **System Information** tab to view the basic system information, system resource state, and recent system logs.

Figure 37 System information



Displaying basic system information

Table 7 Field description

Item	Description
Device Name	Display the device name.

Item	Description
Product Information	Display the description about the device.
Device Location	Display the device location, which you can configure on the page you enter by selecting **Device** > **SNMP** > **Setup**.
Contact Information	Display the contact information, which you can configure on the page you enter by selecting **Device** > **SNMP** > **Setup**.
SerialNum	Display the serial number of the device.
Software Version	Display the software version of the device.
Hardware Version	Display the hardware version of the device.
Bootrom Version	Display the Boot ROM version of the device.
Running Time	Display the system up time.

Displaying the system resource state

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

Displaying recent system logs

Table 8 Field description

Field	Description
Time	Display the time when the system logs were generated.
Level	Display the severity of the system logs.
Description	Display the description of the system logs.

NOTE:

- The **System Information** page displays up to five the most recent system logs about the login and logout events.
- For more system logs, you can click **More** to enter the **Log List** page. You can also enter this page by selecting **Device** > **Syslog**. For more information, see "Configuring syslogs."

Displaying the refresh period

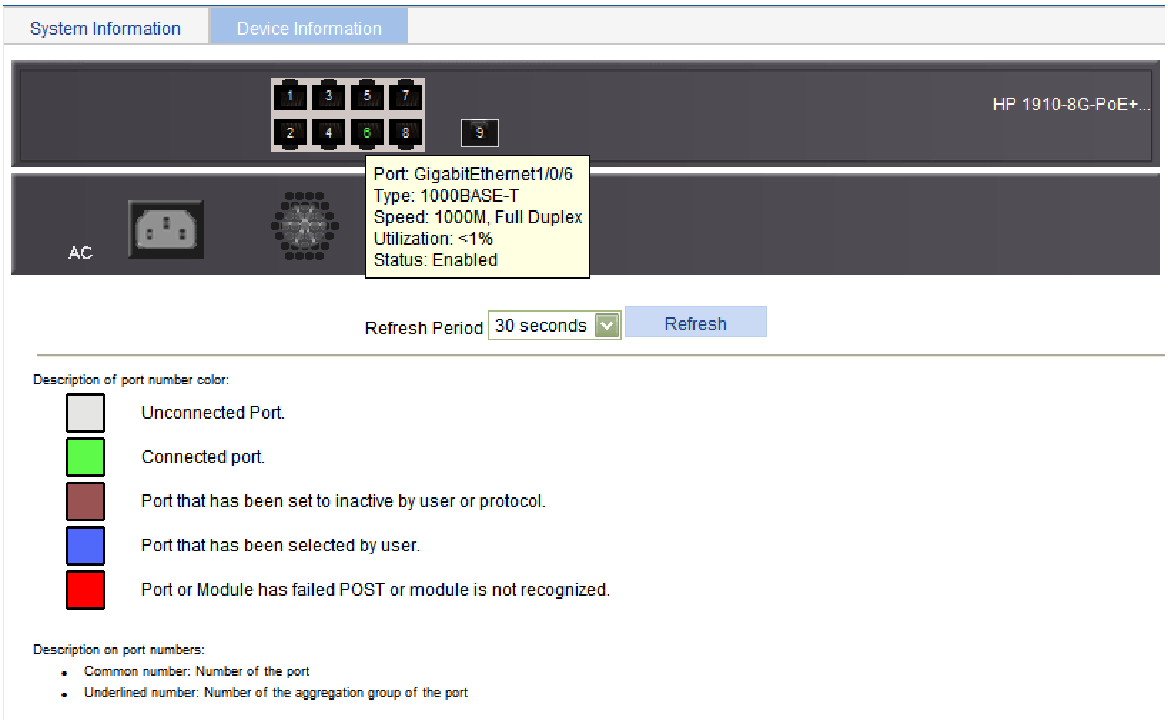
Select from the **Refresh Period** list:

- 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.

Displaying device information

Select **Summary** from the navigation tree, and click the **Device Information** tab to enter the page displaying the device ports, power supplies, and fans. Hover the cursor over a port and the port details appears, including the port name, type, speed, usage, status, and aggregation group number, as shown in Figure 38. For the description about the port number and its color, see Figure 38. Similarly, you can also view the power type and operating status and the fan operating status.

Figure 38 Device information



Select from the **Refresh Period** 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.

Configuring basic device settings

Overview

The device basic information feature provides the following functions:

- Set the system name of the device. The configured system name is displayed on the top of the navigation bar.
- Set the idle timeout period for logged-in users. The system logs an idle user off the web for security purpose after the configured period.

Configuring system name

1. Select **Device** > **Basic** from the navigation tree.

   The system name configuration page appears.

Figure 39 Configure system name

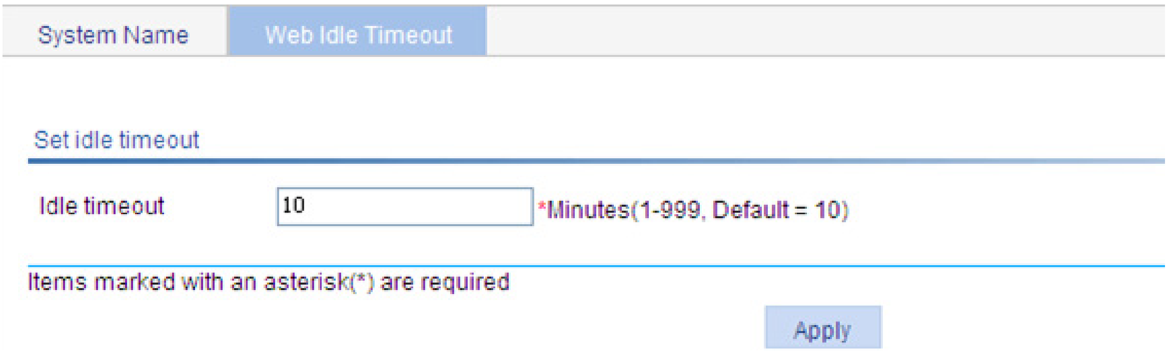
2. Enter the system name.
3. Click **Apply**.

Configuring idle timeout period

1. Select **Device** > **Basic** from the navigation tree.
2. Click the **Web Idle Timeout** tab.

   The page for configuring idle timeout period appears.

Figure 40 Configuring idle timeout period



3. Set the idle timeout period for logged-in users.
4. Click **Apply**.

Maintaining devices

Software upgrade

A boot file, also known as the system software or device software, is an application file used to boot the device. Software upgrade allows you to obtain a target application file from the local host and set the file as the boot file with the original file name to be used at the next reboot. In addition, you can select whether to reboot the device to bring the upgrade software into effect.

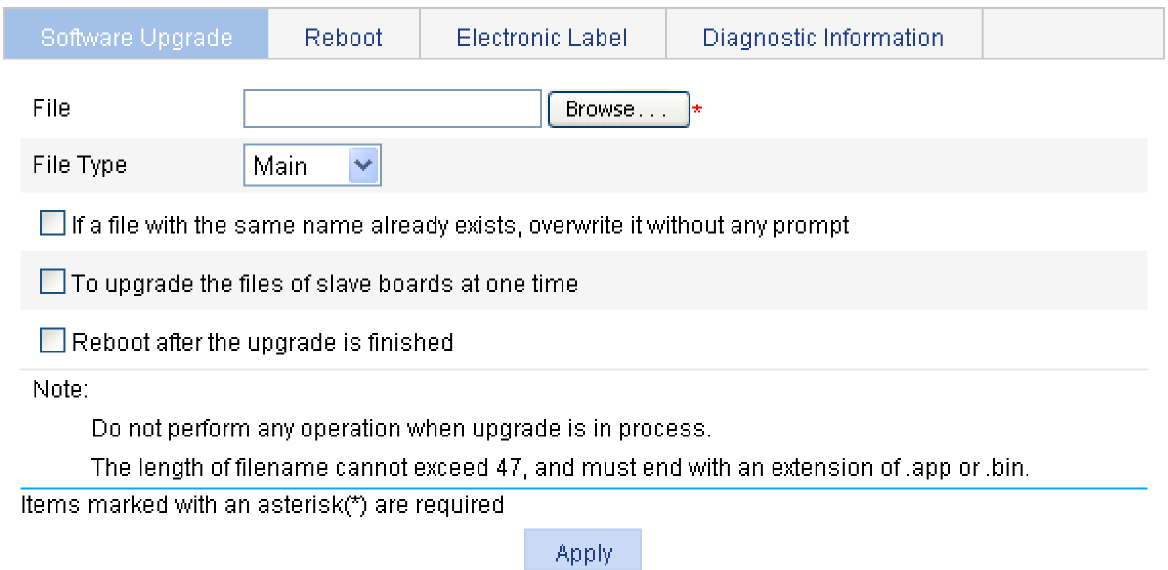
IMPORTANT:

Software upgrade takes a period of time. To avoid interrupting the upgrade operation, do not perform any operation on the Web interface during the upgrading procedure.

To upgrade software:

1. Select **Device** > **Device Maintenance** from the navigation tree to enter the **Software Upgrade** tab.

Figure 41 Software upgrade configuration page



2. Configure software upgrade parameters as described in Table 9.
3. Click **Apply**.

Table 9 Configuration items

Item	Description
File	Specify the path and filename of the local application file, which must be suffixed with the .app or .bin extension.
File Type	Specify the type of the boot file for the next reboot: • **Main**—Boots the device. • **Backup**—Boots the device when the main boot file is unavailable.

Item	Description
If a file with the same name already exists, overwrite it without any prompt	Specify 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 cannot continue the upgrade.
To upgrade the files of slave boards at one time	Specify whether to upgrade the boot file on the standby MPU (not available currently).
Reboot after the upgrade finished	Specify whether to reboot the device to make the upgraded software take effect after the application file is uploaded.

Device reboot

CAUTION:

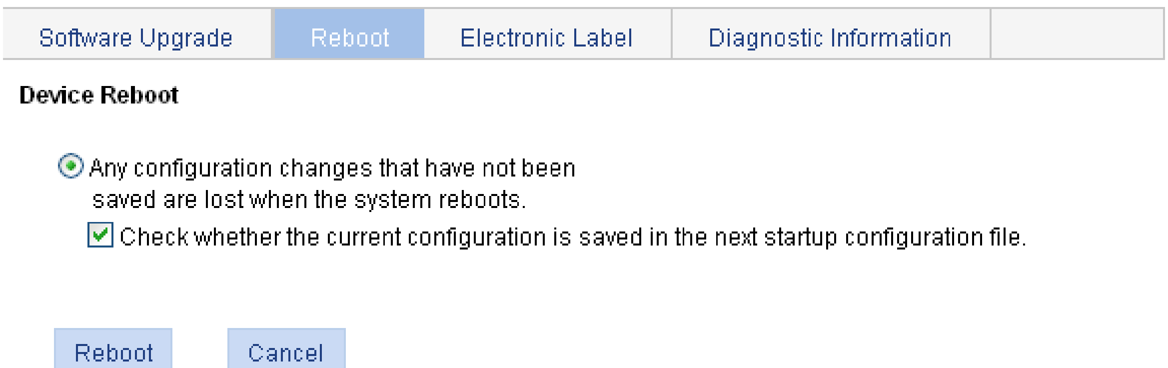
To avoid loss of unsaved configuration after the reboot, save the configuration before rebooting the device.

To reboot the device:

1. Select **Device** > **Device Maintenance** from the navigation tree.
2. Click the **Reboot** tab.

   The device reboot page appears.

Figure 42 Device reboot page



3. Clear the box before "Check whether the current configuration is saved in the next startup configuration file" or keep it selected.
   - If you select the box, 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 box, the system will reboot the device directly.
4. Click **Reboot**

   A confirmation dialog box appears.
5. Click **OK**.

After the device reboots, you need to re-log in to the device.

Electronic label

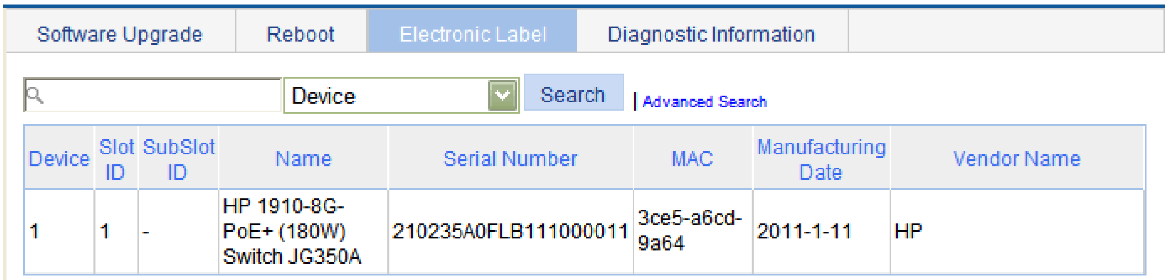
You can view information about the device electronic label, which is also known as the permanent configuration data or archive information. The information is written into the storage medium of a device or a card during the debugging and testing processes, and includes card name, product bar code, MAC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

To view information about the electronic label:

1. Select **Device** > **Device Maintenance** from the navigation tree.
2. Click the **Electronic Label** tab.

   The page for electronic label information appears.

Figure 43 Electronic label



Diagnostic information

Each functional module has its own running information, and generally, you can 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**, through which you can locate problems faster.

IMPORTANT:

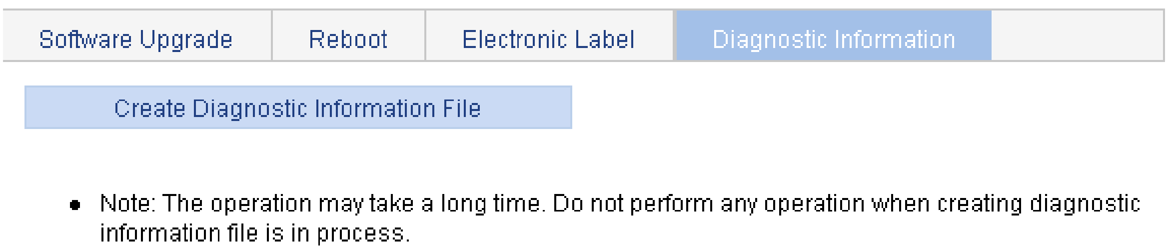
The generation of the diagnostic file takes a period of time. During this process, do not perform any operation on the Web page.

To open or save a diagnostic information file:

1. Select **Device** > **Device Maintenance** from the navigation tree.
2. Click the **Diagnostic Information** tab.

   The diagnostic information page appears.

Figure 44 Diagnostic information

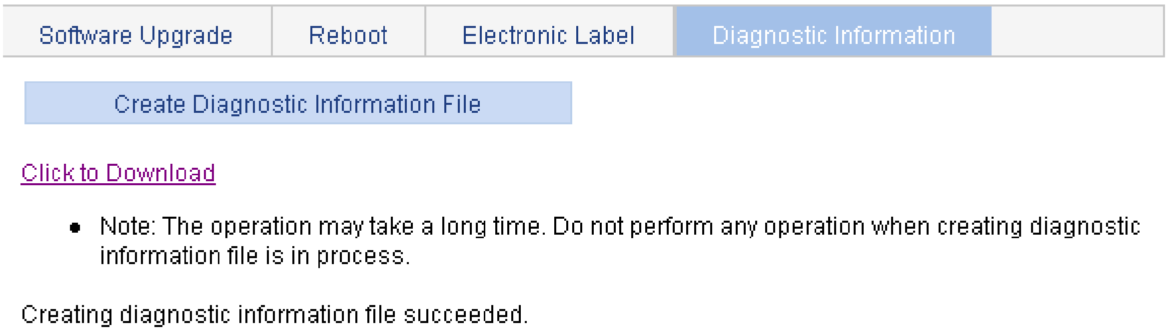


3. Click **Create Diagnostic Information File**.

   The system begins to generate a diagnostic information file.
4. Click **Click to Download**.

   The **File Download** dialog box appears.
5. Open this file or save it to the local host.

Figure 45 Finishing creating the diagnostic information file



After the diagnostic file is successfully generated, you can view this file, or download it to the local host on the page you enter by selecting **Device** > **File Management**. For more information, see "Managing files."

Configuring system time

System time overview

You must configure a correct system time so that the device can work with other devices properly. System time allows you to display and set the device system time and system zone on the web interface.

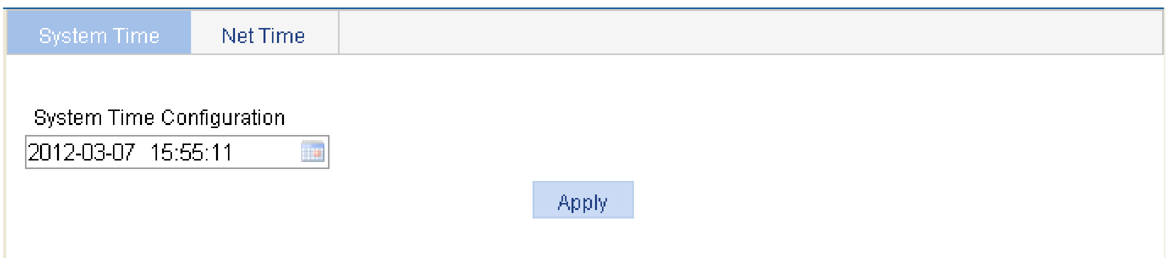
The device supports setting system time through manual configuration and automatic synchronization of NTP server time.

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP can keep consistent timekeeping among all clock-dependent devices within the network and ensure a high clock precision so that the devices can provide diverse applications based on consistent time.

Displaying the current system date and time

To view the current system date and time, select **Device** > **System Time** from the navigation tree to enter the **System Time** tab.

Figure 46 System time configuration page



Manually configuring the system date and time

1. Select **Device** > **System Time** from the navigation tree to enter the **System Time** tab.
2. Click the **System Time Configuration** text to open a calendar.

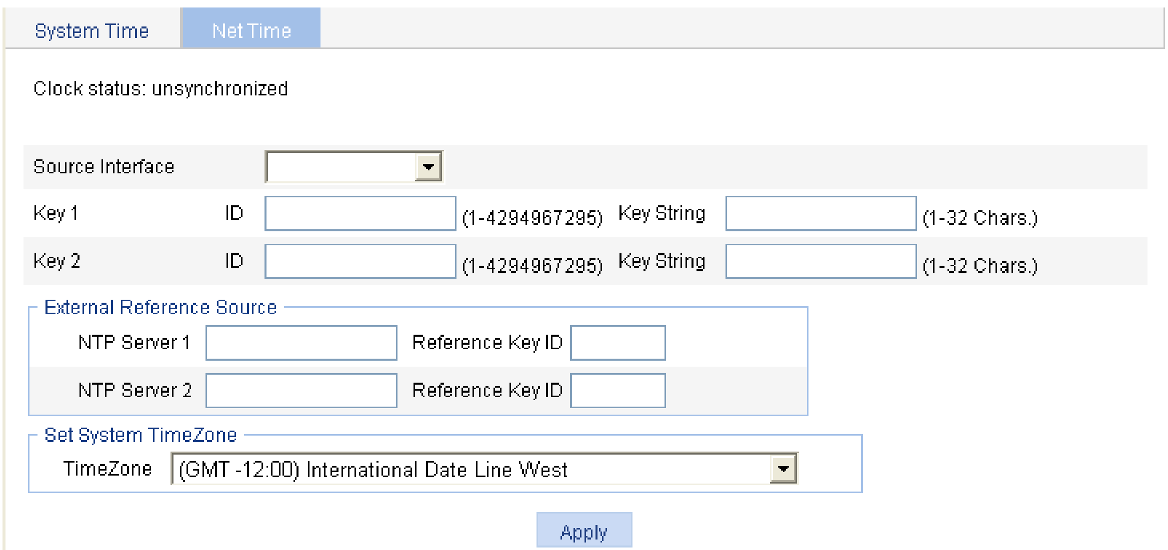
Figure 47 Calendar page

3. Enter the system date and time in the field, or select the date and time in the calendar, where you can:
    - Click **Today**. The date setting in the calendar is synchronized to the current local date configuration, and the time setting does not change.
    - Select the year, month, date, and time, and then click **OK**.
4. Click **Apply** on the system time configuration page to save your configuration.

Configuring network time

1. Select **Device** > **System Time** from the navigation tree.
2. Click the **Network Time Protocol** tab to enter the network time configuration page.

Figure 48 Network time configuration page



3. Configure the network time as described in Table 10.
4. Click **Apply**.

Table 10 Configuration items

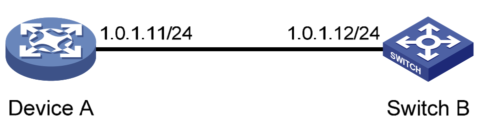
<table>
<tr><th colspan="2">Item</th><th>Description</th></tr>
<tr><td colspan="2">Clock status</td><td>Display the synchronization status of the system clock.</td></tr>
<tr><td colspan="2">Source Interface</td><td>Set the source interface for an NTP message.
If you do not want the IP address of a certain 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 IP address of this interface. If the specified source interface is down, the source IP address is the IP address of the egress interface.</td></tr>
<tr><td colspan="2">Key 1</td><td rowspan="2">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—ID of a key.
• Key string—A character string for MD5 authentication key.</td></tr>
<tr><td colspan="2">Key 2</td></tr>
<tr><td rowspan="2">External Reference Source</td><td>NTP Server 1/Reference Key ID</td><td rowspan="2">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.
IMPORTANT:
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.</td></tr>
<tr><td>NTP Server 2/Reference Key ID</td></tr>
<tr><td colspan="2">TimeZone</td><td>Set the time zone for the system.</td></tr>
</table>

Date and time configuration example

Network requirements

As shown in Figure 49, the local clock of Device A is set as the reference clock. Switch B operates in the client mode, and uses Device A as the NTP server. Configure NTP authentication on Device A and Switch B.

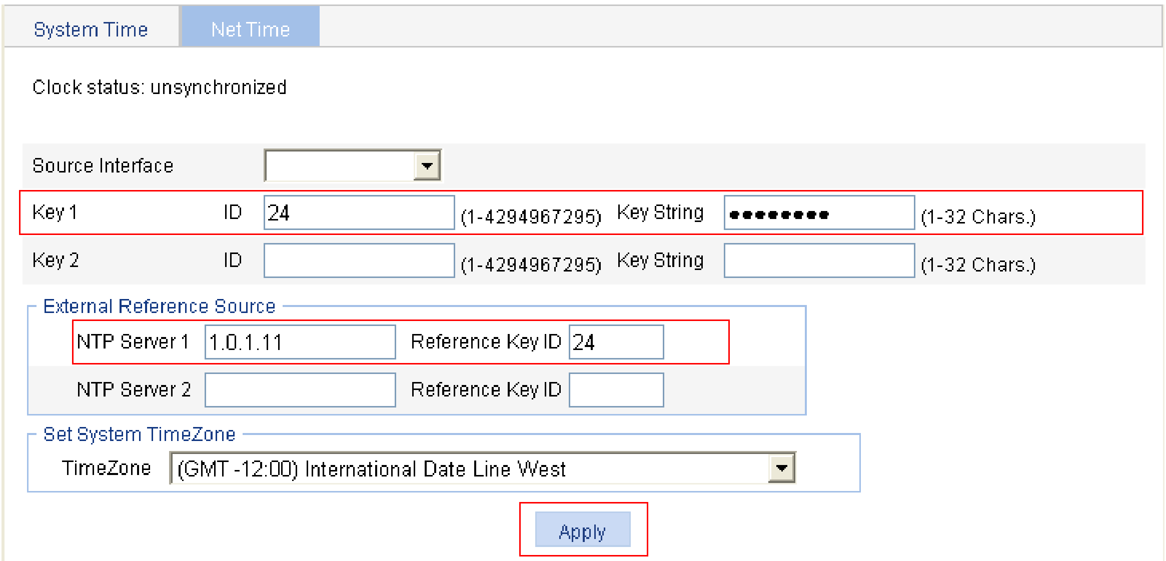
Figure 49 Network diagram



Configuring date and time

1. 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. (Details not shown.)
2. On Switch B, configure Device A as the NTP server.
   a. Select **Device** > **System Time** from the navigation tree.
   b. Click the **Network Time Protocol** tab.
   c. Enter **24** in the **ID** field and enter **aNiceKey** in the **Key String** field for key 1, enter **1.0.1.11** in the **NTP Server 1** field and enter **24** in the **Reference Key ID** field.
   d. Click **Apply**.

Figure 50 Configuring Device A as the NTP server of Switch B



Verifying the configuration

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

Configuration guidelines

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 refresh the page to view the clock status and system time later on.

If the system time of the NTP server is ahead of the system time of the device, and the difference between them exceeds the web idle time specified on the device, all online web users are logged out because of timeout. In this case, you can log in to the device again.

Configuring syslogs

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 running status. With system logs, administrators can take corresponding actions against network problems and security problems.

The system can send system logs to various destinations such as a log host or the web interface.

Displaying syslogs

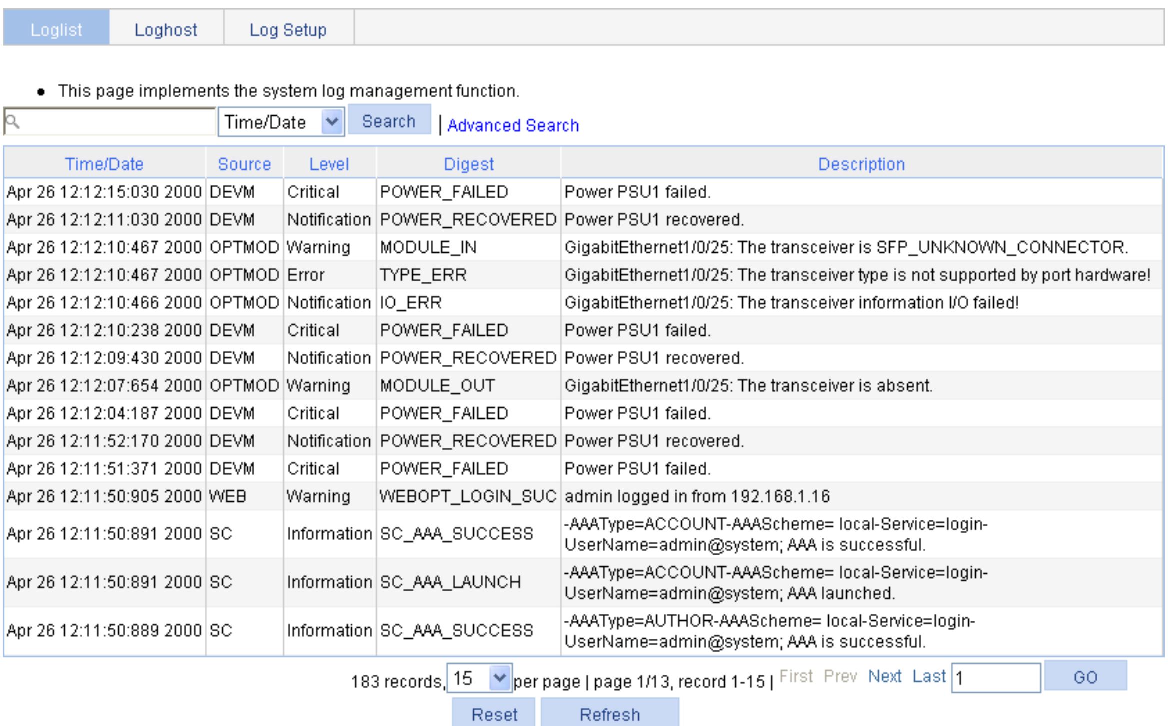
The web interface provides abundant search and sorting functions. You can view syslogs through the web interface conveniently.

To display syslogs:

1. Select **Device** > **Syslog** from the navigation tree.

   The page for displaying syslogs appears.

Figure 51 Displaying syslog



Time/Date	Source	Level	Digest	Description
Apr 26 12:12:15:030 2000	DEVM	Critical	POWER_FAILED	Power PSU1 failed.
Apr 26 12:12:11:030 2000	DEVM	Notification	POWER_RECOVERED	Power PSU1 recovered.
Apr 26 12:12:10:467 2000	OPTMOD	Warning	MODULE_IN	GigabitEthernet1/0/25: The transceiver is SFP_UNKNOWN_CONNECTOR.
Apr 26 12:12:10:467 2000	OPTMOD	Error	TYPE_ERR	GigabitEthernet1/0/25: The transceiver type is not supported by port hardware!
Apr 26 12:12:10:466 2000	OPTMOD	Notification	IO_ERR	GigabitEthernet1/0/25: The transceiver information I/O failed!
Apr 26 12:12:10:238 2000	DEVM	Critical	POWER_FAILED	Power PSU1 failed.
Apr 26 12:12:09:430 2000	DEVM	Notification	POWER_RECOVERED	Power PSU1 recovered.
Apr 26 12:12:07:654 2000	OPTMOD	Warning	MODULE_OUT	GigabitEthernet1/0/25: The transceiver is absent.
Apr 26 12:12:04:187 2000	DEVM	Critical	POWER_FAILED	Power PSU1 failed.
Apr 26 12:11:52:170 2000	DEVM	Notification	POWER_RECOVERED	Power PSU1 recovered.
Apr 26 12:11:51:371 2000	DEVM	Critical	POWER_FAILED	Power PSU1 failed.
Apr 26 12:11:50:905 2000	WEB	Warning	WEBOPT_LOGIN_SUC	admin logged in from 192.168.1.16
Apr 26 12:11:50:891 2000	SC	Information	SC_AAA_SUCCESS	-AAAType=ACCOUNT-AAAScheme= local-Service=login-UserName=admin@system; AAA is successful.
Apr 26 12:11:50:891 2000	SC	Information	SC_AAA_LAUNCH	-AAAType=ACCOUNT-AAAScheme= local-Service=login-UserName=admin@system; AAA launched.
Apr 26 12:11:50:889 2000	SC	Information	SC_AAA_SUCCESS	-AAAType=AUTHOR-AAAScheme= local-Service=login-UserName=admin@system; AAA is successful.

TIP:

- You can click **Reset** to clear all system logs saved in the log buffer on the web interface.
- You can click **Refresh** to manually refresh the page, or you can set the refresh interval on the **Log Setup** page to enable the system to automatically refresh the page periodically. For more information, see "Setting buffer capacity and refresh interval."

2. View system logs.

Table 11 Field description

Field	Description
Time/Date	Displays the time/date when system logs are generated.
Source	Displays the module that generates system logs.
Level	Displays the system information levels. The information is classified into eight levels by severity: • **Emergency**—The system is unavailable. • **Alert**—Action must be taken immediately. • **Critical**—Critical conditions. • **Error**—Error conditions. • **Warning**—Warning conditions. • **Notification**—Normal but significant condition. • **Information**—Informational messages. • **Debug**—Debug-level messages.
Digest	Displays the brief description of system logs.
Description	Displays the contents of system logs.

Setting the log host

You can set the loghost on the web interface to enable the system to output syslogs to the log host. You can specify at most four different log hosts.

To set the log host:

1. Select **Device** > **Syslog** from the navigation tree.
2. Click the **Loghost** tab.

   The loghost configuration page appears.

Figure 52 Setting loghost

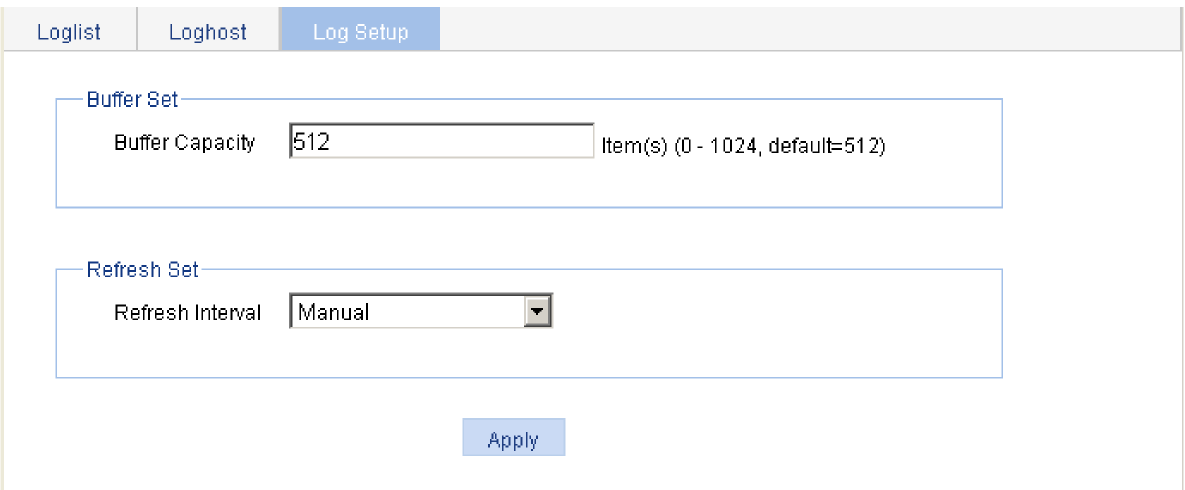
3. Configure the IPv4 address of the log host.
4. Click **Apply**.

Setting buffer capacity and refresh interval

1. Select **Device** > **Syslog** from the navigation tree.
2. Click the **Log Setup** tab.

   The syslog configuration page appears.

Figure 53 Syslog configuration page



3. Configure buffer capacity and refresh interval as described in Table 12.

4. Click **Apply**.

Table 12 Configuration items

Item	Description
Buffer Capacity	Set the number of logs that can be stored in the log buffer of the web interface.
Refresh Interval	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.

Managing the configuration

You can backup, restore, save, and reset the configuration of the device.

Backing up configuration

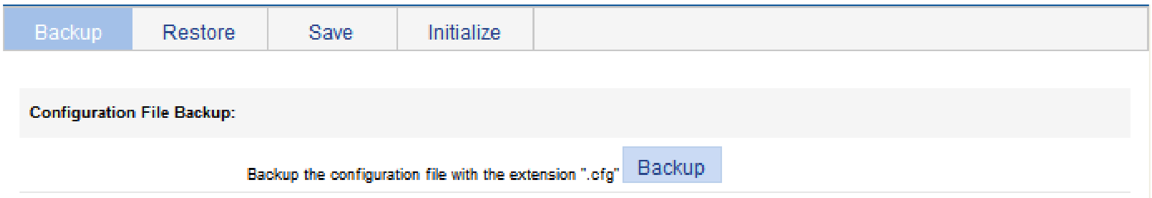
With the configuration backup function, you can perform the following tasks:

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

To backup up the configuration:

1. Select **Device** > **Configuration** from the navigation tree to enter the **Backup** tab.

Figure 54 Backing up the configuration



2. Click the upper **Backup** button.
   The file download dialog box appears.
3. View the **.cfg** file or to save the file locally.

Restoring configuration

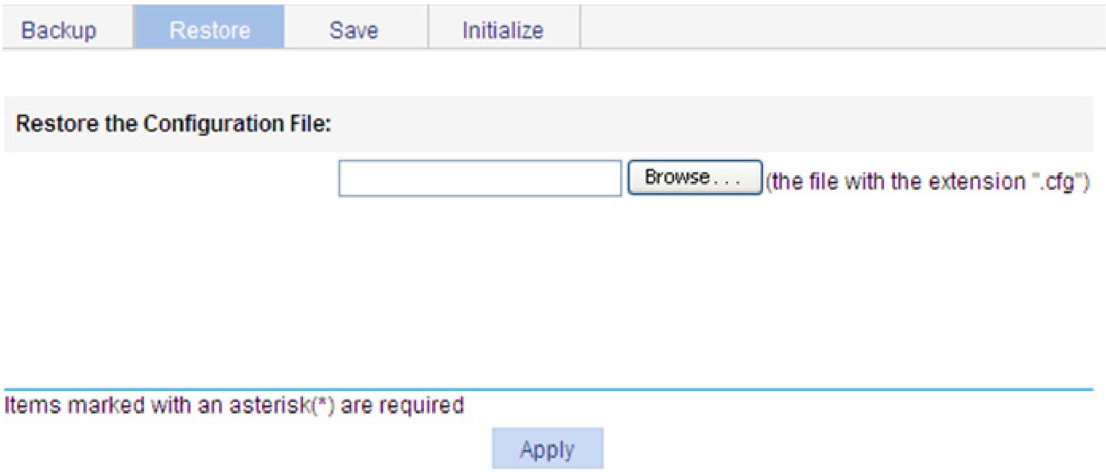
> **CAUTION:**
> The restored configuration takes effect at the next boot of the device.

The configuration restore function uploads the **.cfg** file on the host of the current user to the device for the next startup.

To restore the configuration:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Restore** tab to enter the configuration restore page.

Figure 55 Restoring the configuration



3. Click the upper **Browse** button.

   The file upload dialog box appears.
4. Select the **.cfg** file to be uploaded, and click **Apply**.

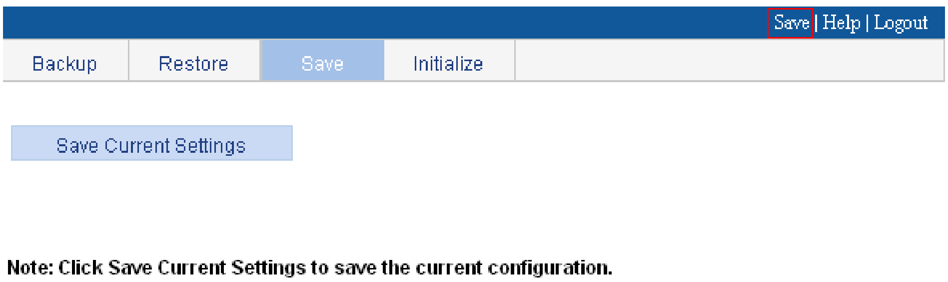
Saving configuration

The save configuration module provides the function to save the current configuration to the configuration file (**.cfg** file) to be used at the next startup.

You can save the configuration in the fast way or common way.

To save the configuration in the fast way, click the **Save** button at the upper right of the auxiliary area.

Figure 56 Saving the configuration



To save the configuration in the common way:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Save** tab to enter the save configuration confirmation page.
3. Click **Save Current Settings**.

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.

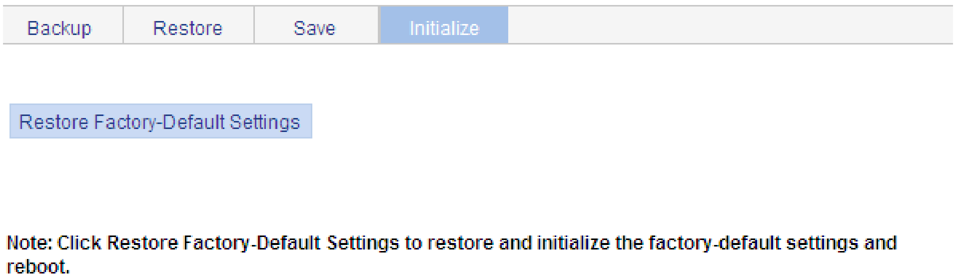
Resetting configuration

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

To reset the configuration:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Initialize** tab to enter the initialize confirmation page.
3. Click the **Restore Factory-D** button to restore the system to factory defaults.

Figure 57 Resetting the configuration



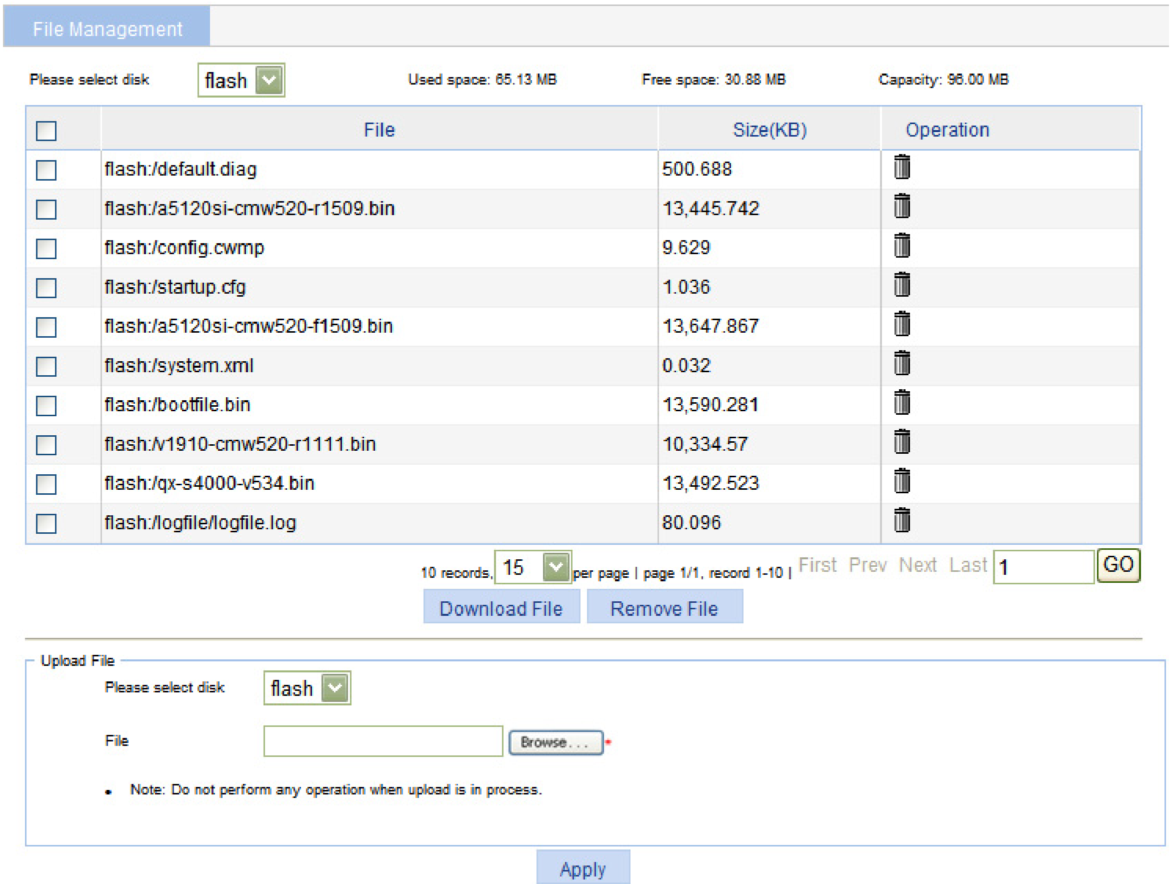
Managing files

The device saves files such as the host software file and configuration file on its storage media. The file management function allows you to manage the files on the storage media.

Displaying files

1. Select **Device** > **File Management** from the navigation tree.

Figure 58 File management page



2. Select a medium from the **Please select disk** list.

   Two categories of information is displayed:

   - Medium Information, including the used space, free space, and the capacity of the medium.
   - File information, including all files on the medium and the file sizes.

Downloading a file

1. Select **Device** > **File Management** from the navigation tree to enter the file management page. See Figure 58.
2. From the **Please select disk** list, select the medium where the file to be downloaded resides.

3. Select the file from the list.

   Only one file can be downloaded at a time.
4. Click **Download File**.

   The **File Download** dialog box appears.
5. Open the file or save the file to a specified path.

Uploading a file

NOTE:

Uploading a file may take some time. HP does not recommend performing any operation on the web interface during the upgrade.

1. Select **Device** > **File Management** from the navigation tree to enter the file management page. See Figure 58.
2. In the **Upload File** area, select the medium for saving the file from the **Please select disk** list.
3. Click **Browse** to navigate to the file to be uploaded.
4. Click **Apply**.

Removing a file

1. Select **Device** > **File Management** from the navigation tree to enter the file management page. See Figure 58.
2. Click the icon of a file to remove the file, or select from the file list and click **Remove File**.

NOTE:

To remove multiple files, repeat step 2, or select the files from the file list and click **Remove File**.

Managing ports

Overview

You can use the port management feature to set and view the operation parameters of a Layer 2 Ethernet port and an aggregate interface.

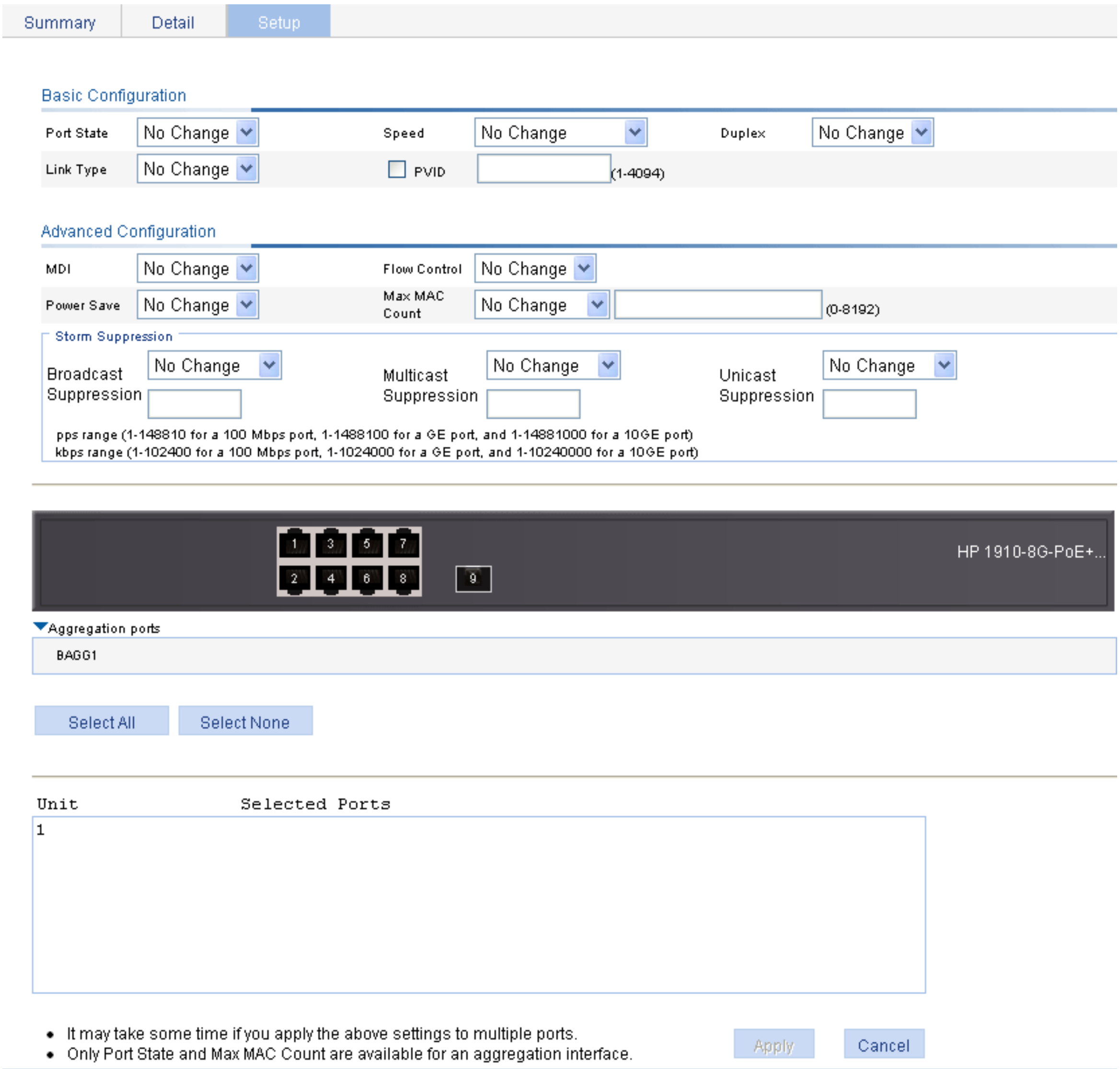
- For a Layer 2 Ethernet port, these operation parameters include its state, rate, duplex mode, link type, PVID, MDI mode, flow control settings, MAC learning limit, and storm suppression ratios.
- For an aggregate interface, these operation parameters include its state and MAC learning limit.

Configuring a port

Setting operation parameters for a port

1. Select **Device** > **Port Management** from the navigation tree.
2. Click the **Setup** tab to enter the page shown in Figure 59.

Figure 59 The Setup tab



3. Set the operation parameters for the port as described in Table 13.
4. Click **Apply**.

Table 13 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.

Item	Description
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.
Duplex	Set the duplex mode of the port. • **Auto**—Auto-negotiation. • **Full**—Full duplex. • **Half**—Half duplex.
Link Type	Set the link type of the current port, which can be access, hybrid, or trunk. For more information, see "Configuring VLANs." IMPORTANT: 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 more information about setting the PVID, see "Configuring VLANs." IMPORTANT: 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.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>MDI</td><td>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.</td></tr>
<tr><td>Flow Control</td><td>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.

IMPORTANT:

Flow control works only after it is enabled on both the ingress and egress ports.</td></tr>
<tr><td>Power Save</td><td>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.

IMPORTANT:

Support for this configuration item varies with device models.</td></tr>
<tr><td>Max MAC Count</td><td>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.</td></tr>
</table>

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 kilobits of broadcast traffic 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. IMPORTANT: 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 kilobits of multicast traffic 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. IMPORTANT: 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 kilobits of unicast traffic 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. IMPORTANT: 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**.

Item	Description
Selected Ports	Interface or interfaces that you have selected from the chassis front panel and the aggregate interface list below, for which you have set operation parameters. IMPORTANT: You can set only the state and MAC learning limit for an aggregate interface.

NOTE:

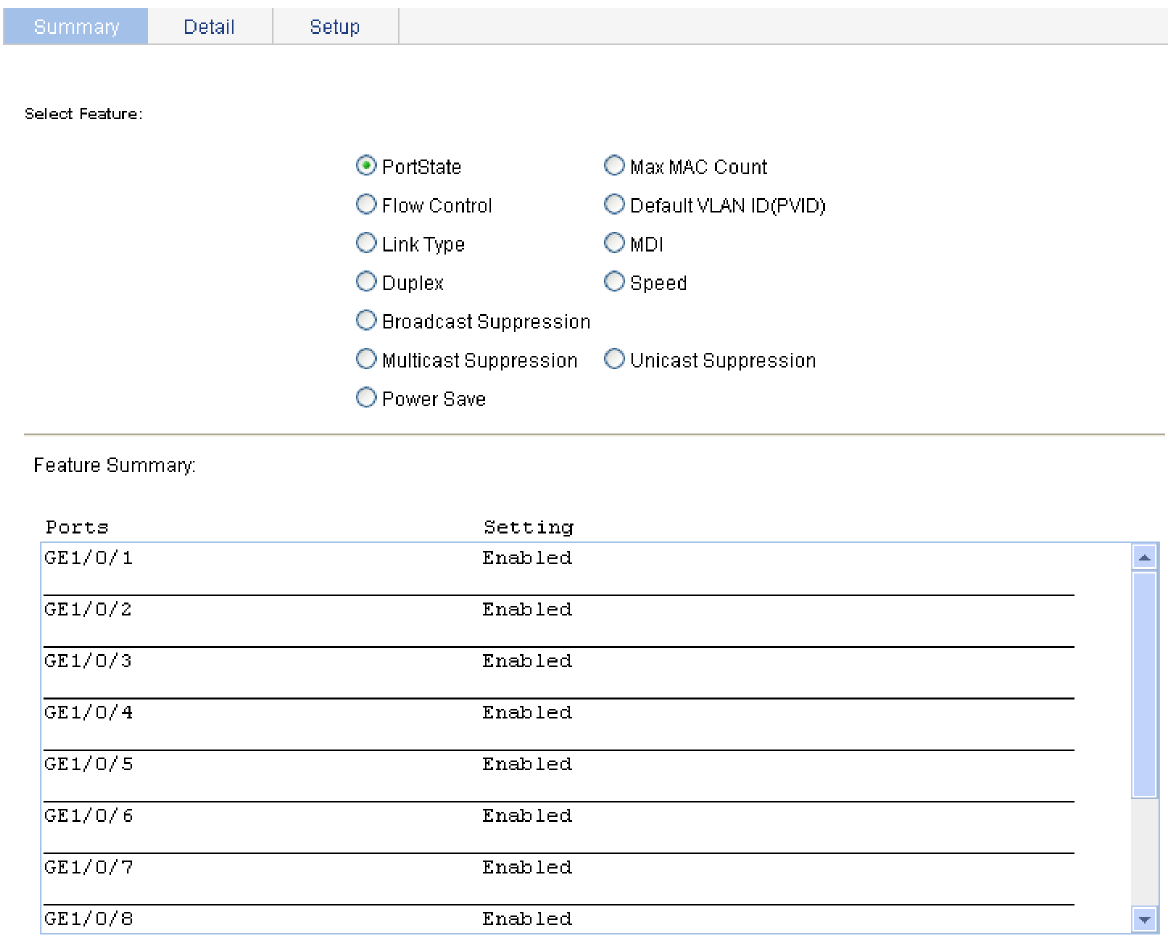
If you set operation parameters that a port does not support, you are notified of invalid settings and may fail to set the supported operation parameters for the port or other ports.

Displaying port operation parameters

Displaying a specified operation parameter for all ports

1. Select **Device** > **Port Management** from the navigation tree to enter the **Summary** page by default.
2. Click the button of a parameter you want to view and the parameter information for all the ports is displayed in the lower part of the page, as shown in Figure 60.

Figure 60 The Summary tab

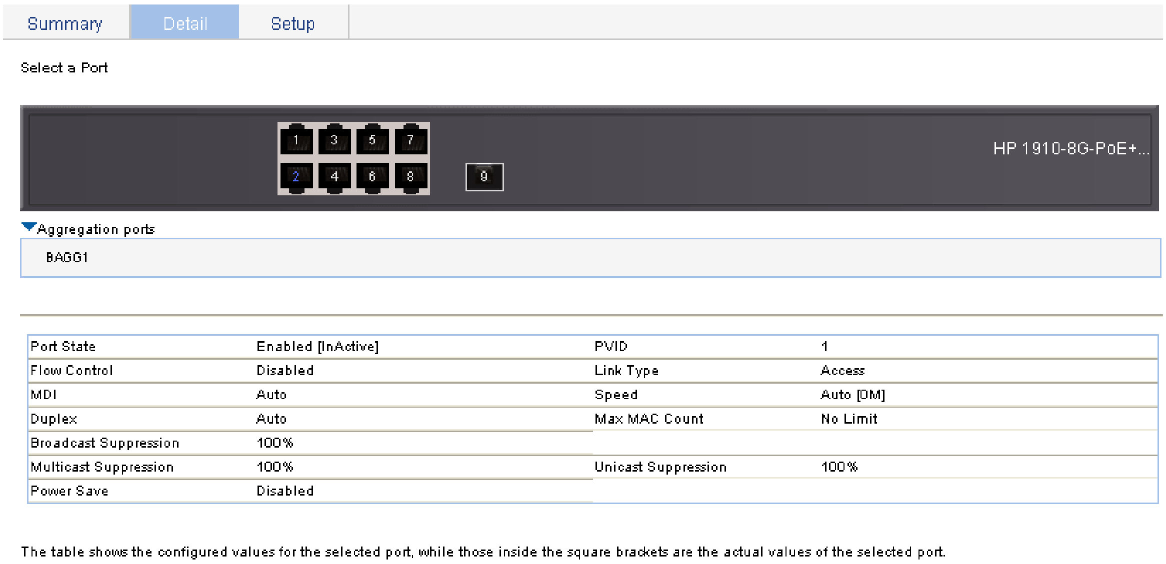


Displaying all the operation parameters for a port

1. Select **Device** > **Port Management** from the navigation tree

2. Click the **Detail** tab.
3. Select a port whose operation parameters you want to view in the chassis front panel, as shown in Figure 61. The operation parameter settings of the selected port are displayed on the lower part of the page. Whether the parameter takes effect is displayed in the square brackets.

Figure 61 The Detail tab



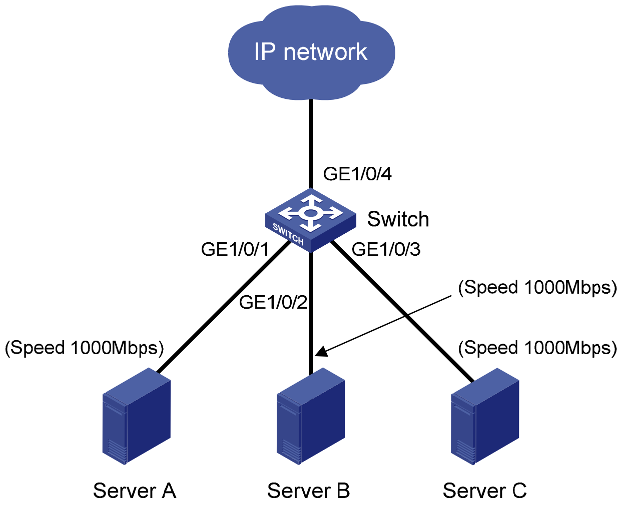
Port management configuration example

Network requirements

As shown in Figure 62:

- Server A, Server B, and Server C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on 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.

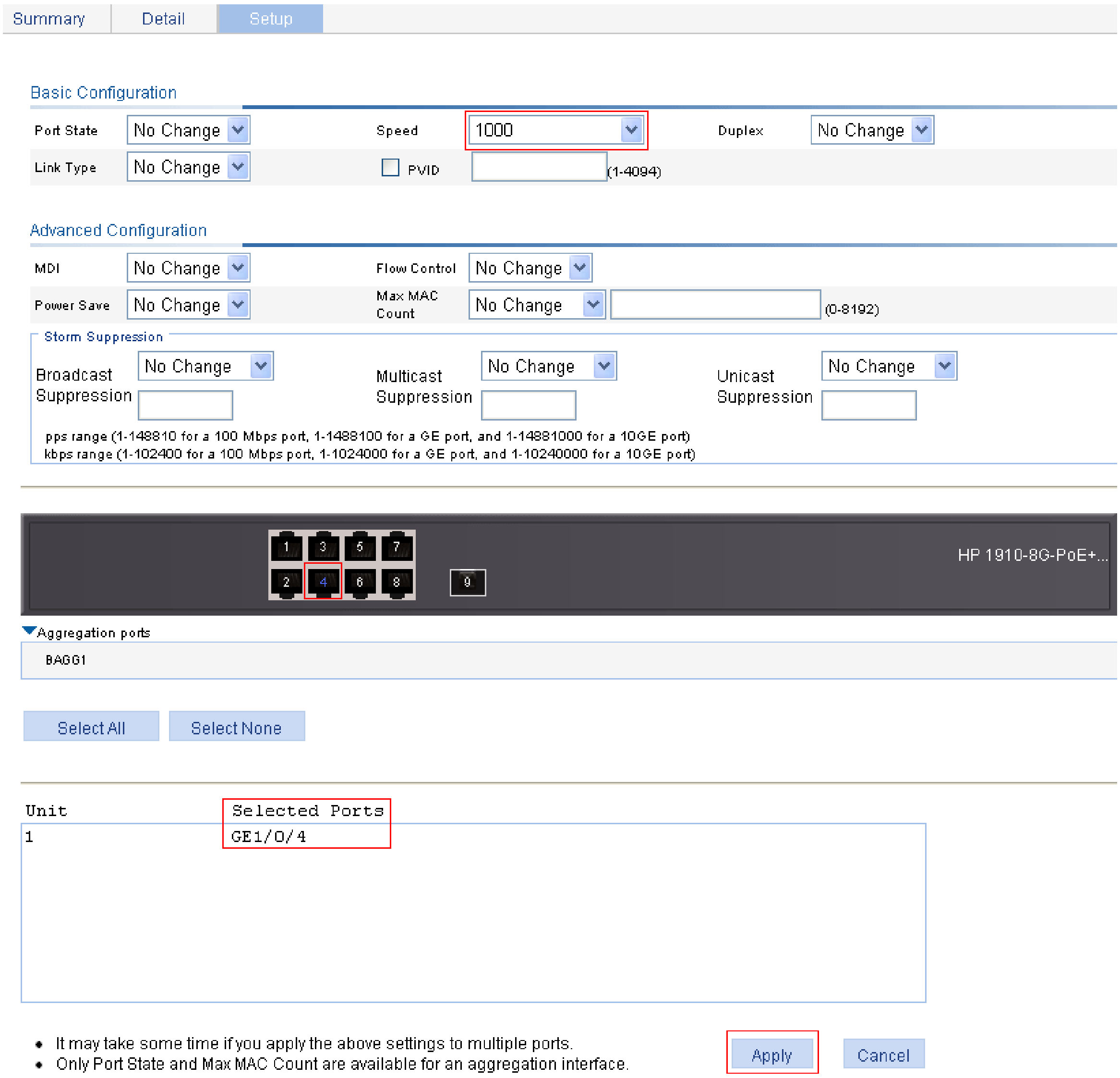
Figure 62 Network diagram



Configuring the switch

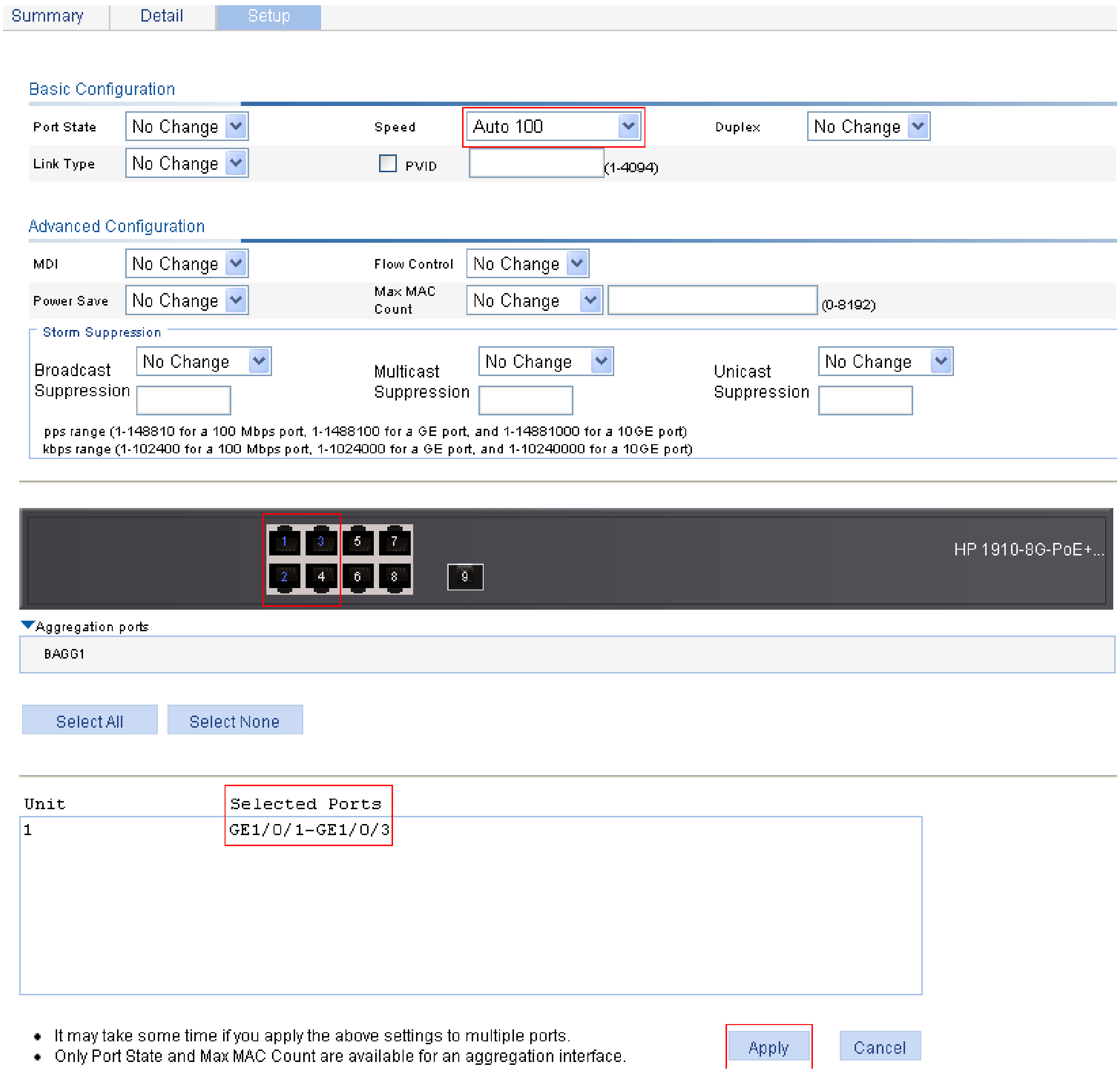
1. Set the rate of GigabitEthernet 1/0/4 to 1000 Mbps.
   a. Select **Device** > **Port Management** from the navigation tree
   b. Click the **Setup** tab to enter the page shown in Figure 63.
   c. Select **1000** from the **Speed** list.
   d. Select **4** on the chassis front panel. **4** represents port GigabitEthernet 1/0/4.
   e. Click **Apply**.

Figure 63 Configure the rate of GigabitEthernet 1/0/4



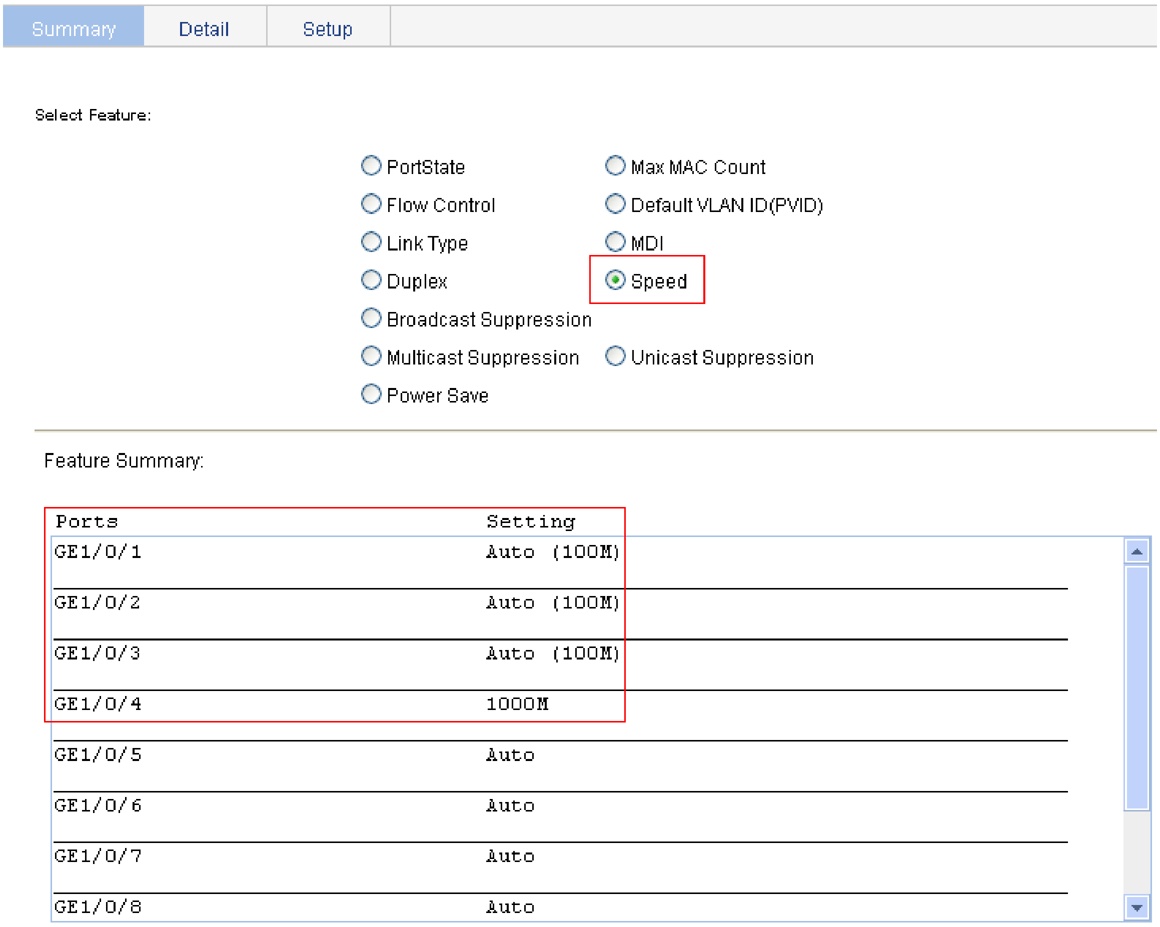
2. Batch configure the auto-negotiation rate range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.
   a. On the **Setup** tab, select **Auto 100** from the **Speed** list, as shown in Figure 64.
   b. Select **1**, **2**, and **3** on the chassis front panel. **1**, **2**, and **3** represent ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.
   c. Click **Apply**.

Figure 64 Batch configure port rate



3. Display the rate settings of ports.
   a. Click the **Summary** tab.
   b. Click the **Speed** button to display the rate information of all ports on the lower part of the page, as shown in Figure 65.

Figure 65 Display the rate settings of ports



Configuring port mirroring

Port mirroring refers to the process of copying the packets passing through a port/VLAN/CPU to the monitor port connecting to a monitoring device for packet analysis.

Terminologies of port mirroring

Mirroring source

The mirroring source can be one or more monitored ports, called source ports. The device where the ports reside is called a "source device." Packets (called "mirrored packets") passing through them are copied to a port connecting to a monitoring device for packet analysis.

Mirroring destination

The mirroring destination is the destination port (also known as the monitor port) of mirrored packets and connects to the data monitoring device. The device where the monitor port resides is called the "destination device". The monitor port forwards mirrored packets to its connected monitoring device.

NOTE:

A monitor port may receive multiple duplicates of a packet in some cases because it can monitor multiple mirroring sources. For example, assume that Port 1 is monitoring bidirectional traffic on Port 2 and Port 3 on the same device. If a packet travels from Port 2 to Port 3, two duplicates of the packet will be received on Port 1.

Mirroring direction

The mirroring direction indicates that the inbound, outbound, or bidirectional traffic can be copied on a mirroring source.

- Inbound: Copies packets received on a mirroring source.
- Outbound: Copies packets sent out of a mirroring source.
- Bidirectional: Copies packets both received and sent on a mirroring source.

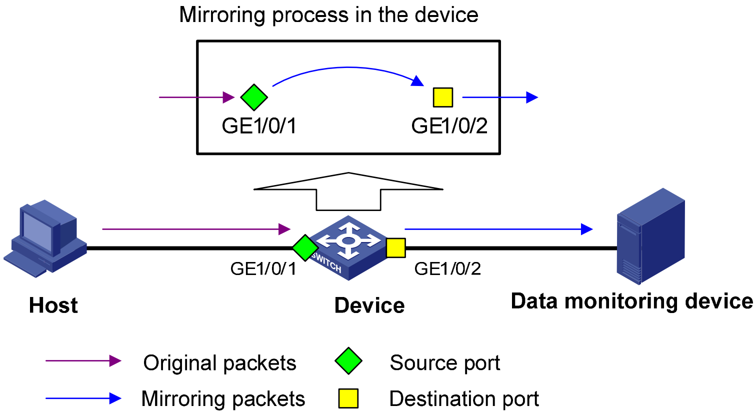
Mirroring group

Port mirroring is implemented through mirroring groups. The mirroring source and mirroring destination must belong to a mirroring group.

Port mirroring implementation

HP 1910 switch series supports local port mirroring, in which case the mirroring source and the mirroring destination are on the same device. A mirroring group that contains the mirroring source and the mirroring destination on the same device is called a "local mirroring group."

Figure 66 Local port mirroring implementation



As shown in Figure 66, the source port GigabitEthernet 1/0/1 and monitor port GigabitEthernet 1/0/2 reside on the same device. Packets of GigabitEthernet 1/0/1 are copied to GigabitEthernet 1/0/2, which then forwards the packets to the data monitoring device for analysis.

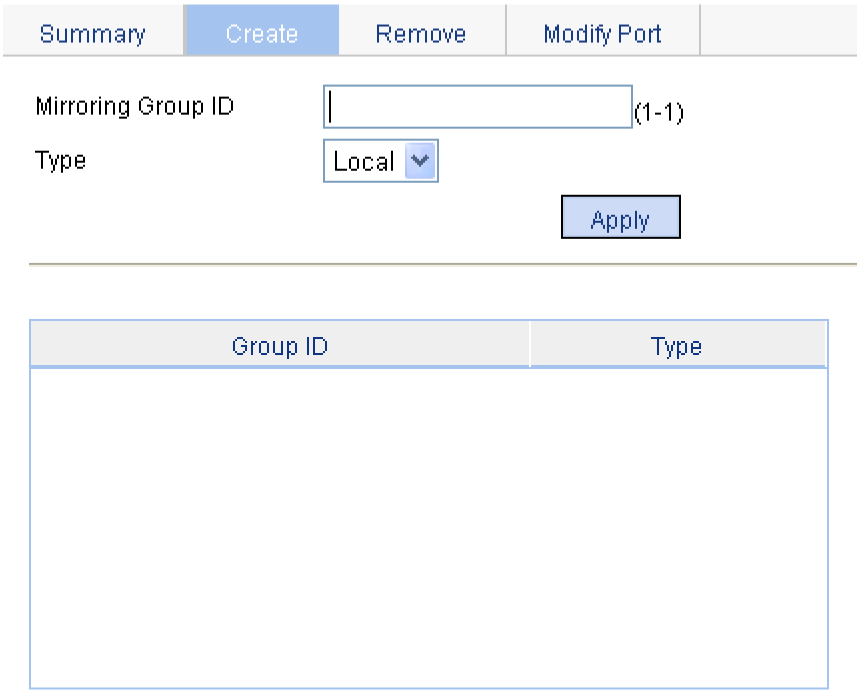
Recommended configuration procedures

Step	Remarks
1. Configure a local mirroring group	Required. For more information, see "Configuring a mirroring group." Select the mirroring group type **local** in the **Type** list.
2. Configure mirroring ports for the mirroring group	Required. For more information, see "Configuring ports for a mirroring group." Select the port type **Mirror Port**.
3. Configure the monitor port for the mirroring group	Required. For more information, see "Configuring ports for a mirroring group." Select the port type **Monitor Port**.

Configuring a mirroring group

1. Select **Device** > **Port Mirroring** from the navigation tree.
2. Click the **Add** tab to enter the page for adding a mirroring group.

Figure 67 Adding a mirroring group



3. Configure the mirroring group as described in Table 14.
4. Click **Apply**.

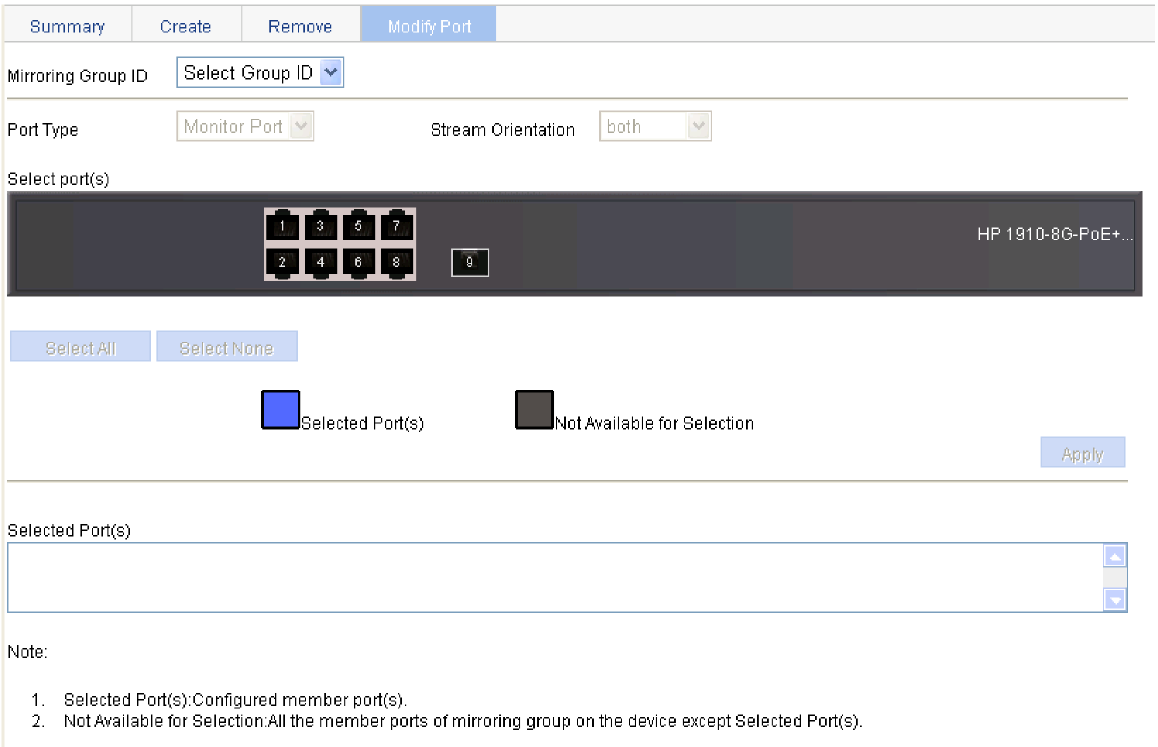
Table 14 Configuration items

Item	Description
Mirroring Group ID	ID of the mirroring group to be added. The range of the mirroring group ID varies with devices.
Type	Specify the type of the mirroring group to be added: **Local**—Adds a local mirroring group.

Configuring ports for a mirroring group

1. Select **Device** > **Port Mirroring** from the navigation tree.
2. Click the **Modify Port** tab to enter the page for configuring ports for a mirroring group, as shown in Figure 68.

Figure 68 The Modify Port tab



3. Configure ports for the mirroring group as described in Table 15.
4. Click **Apply**.

   A progress dialog box appears.
5. After the success notification appears, click **Close**.

Table 15 Configuration items

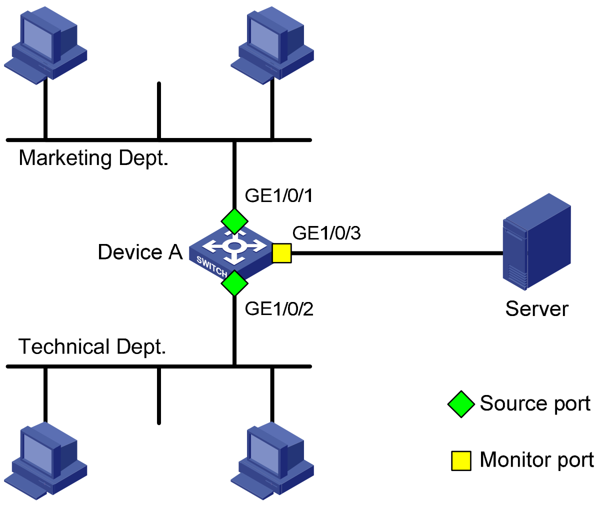
Item	Description
Mirroring Group ID	ID of the mirroring group to be configured. The available groups were added previously. Select a **Local** mirroring group ID to configure ports for the local mirroring group.
Port Type	**Monitor Port**—Configures the monitor ports for the local mirroring group. **Mirror Port**—Configures mirroring ports for the local mirroring group.
Stream Orientation	When you select **Mirror Port** for **Port Type**, set the direction of the traffic monitored by the monitor port of the mirroring group. • **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.

Local port mirroring configuration example

Network requirements

As shown in Figure 69, configure local port mirroring on Switch A to monitor the packets received and sent by the Marketing department and Technical department.

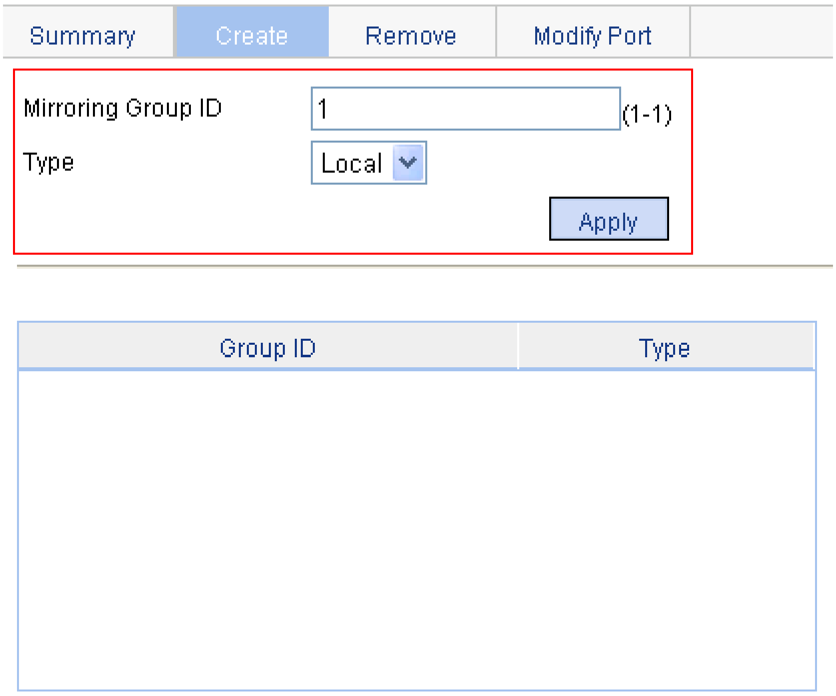
Figure 69 Network diagram



Adding a local mirroring group

1. Select **Device** > **Port Mirroring** from the navigation tree.
2. Click the **Add** tab to enter the page for add mirroring groups, as shown in Figure 70.
3. Enter **1** for **Mirroring Group ID** and select **Local** from the **Type** list.
4. Click **Apply**.

Figure 70 Adding a local mirroring group

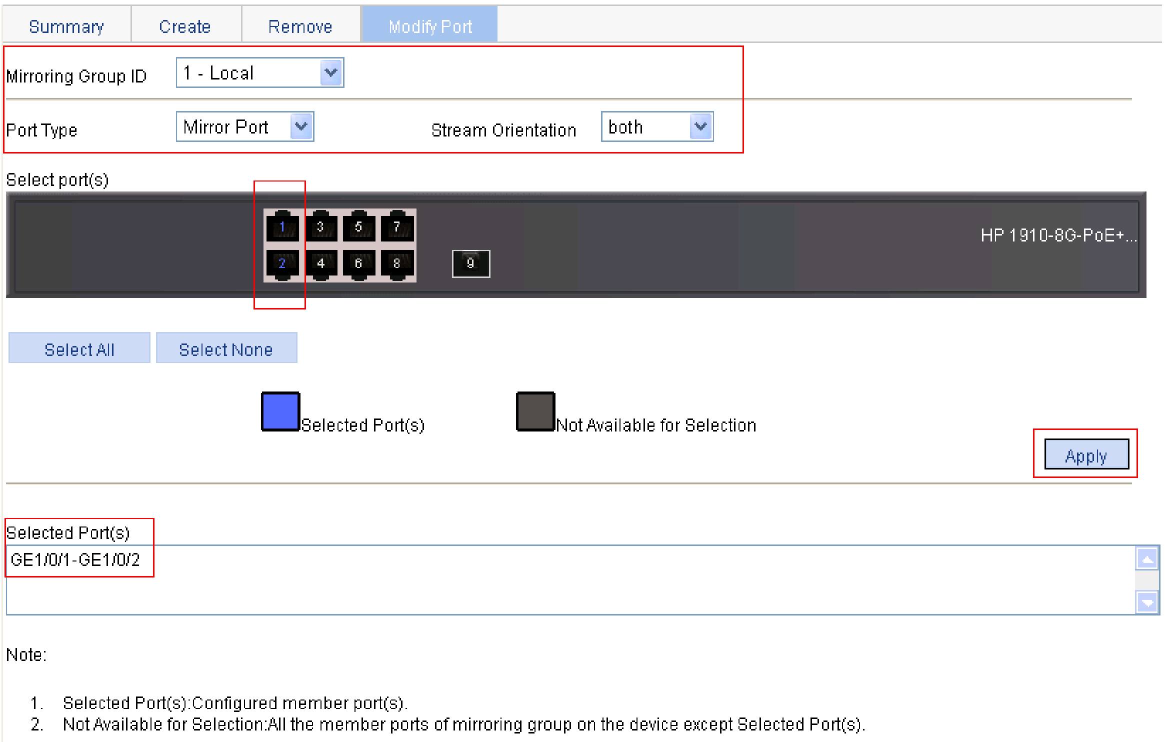


Configuring the mirroring ports as GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2

1. Click the **Modify Port** tab to enter the page, as shown in Figure 71.
2. Select **1 – Local** from the **Mirroring Group ID** list, select **Mirror Port** from the **Port Type** list, select **both** from the **Stream Orientation** list, and select **1** (GigabitEthernet 1/0/1) and **2** (GigabitEthernet 1/0/2) on the chassis front panel.
3. Click **Apply**.

   A configuration progress dialog box appears.
4. After the success notification appears, click **Close**.

Figure 71 Configuring the mirroring ports

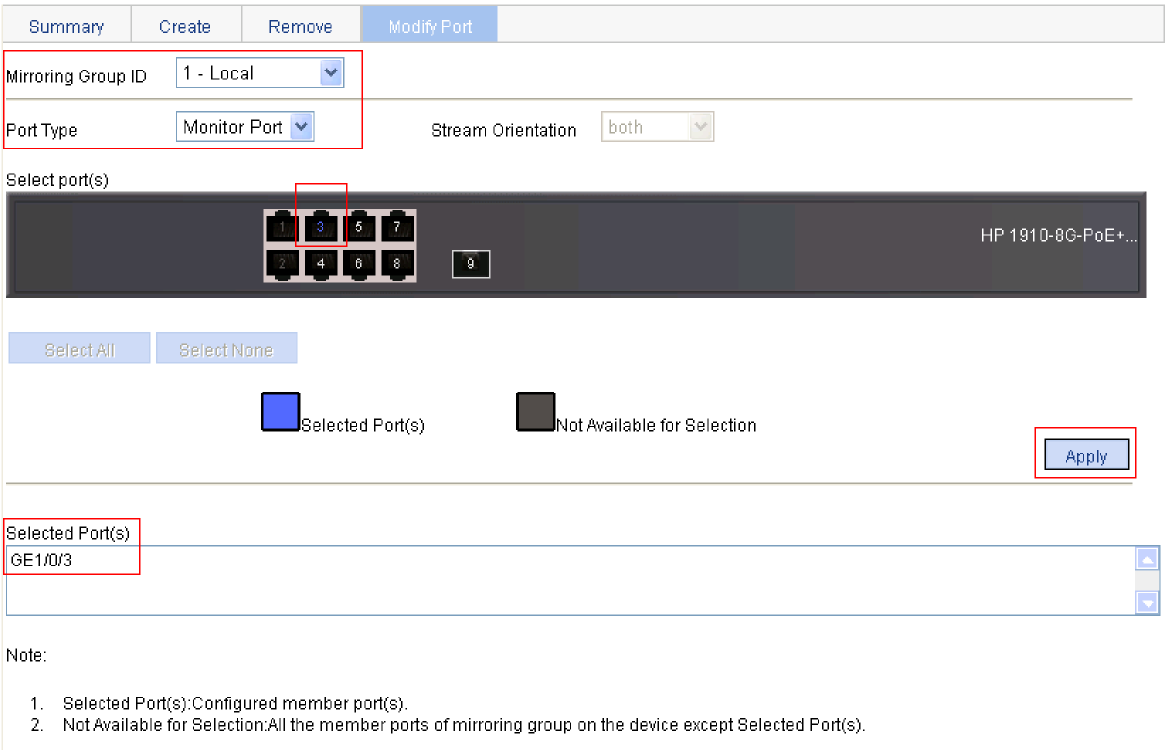


Configuring the monitor port as GigabitEthernet 1/0/3

1. Click the **Modify Port** tab to enter the page, as shown in Figure 72.
2. Select **1 – Local** from the **Mirroring Group ID** list, select **Monitor Port** from the **Port Type** list, and select **3** (GigabitEthernet 1/0/3) on the chassis front panel.
3. Click **Apply**.

   A configuration progress dialog box appears.
4. After the success notification appears, click **Close**.

Figure 72 Configuring the monitor port



Configuration guidelines

Follow these guidelines when you configure port mirroring:

1. You can configure multiple source ports but only one monitor port for a local mirroring group.
2. To ensure normal operation of mirroring, do not enable the spanning tree feature on the monitor port.
3. Use a monitor port for port mirroring only. This is to make sure that the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and normally forwarded traffic.

Managing users

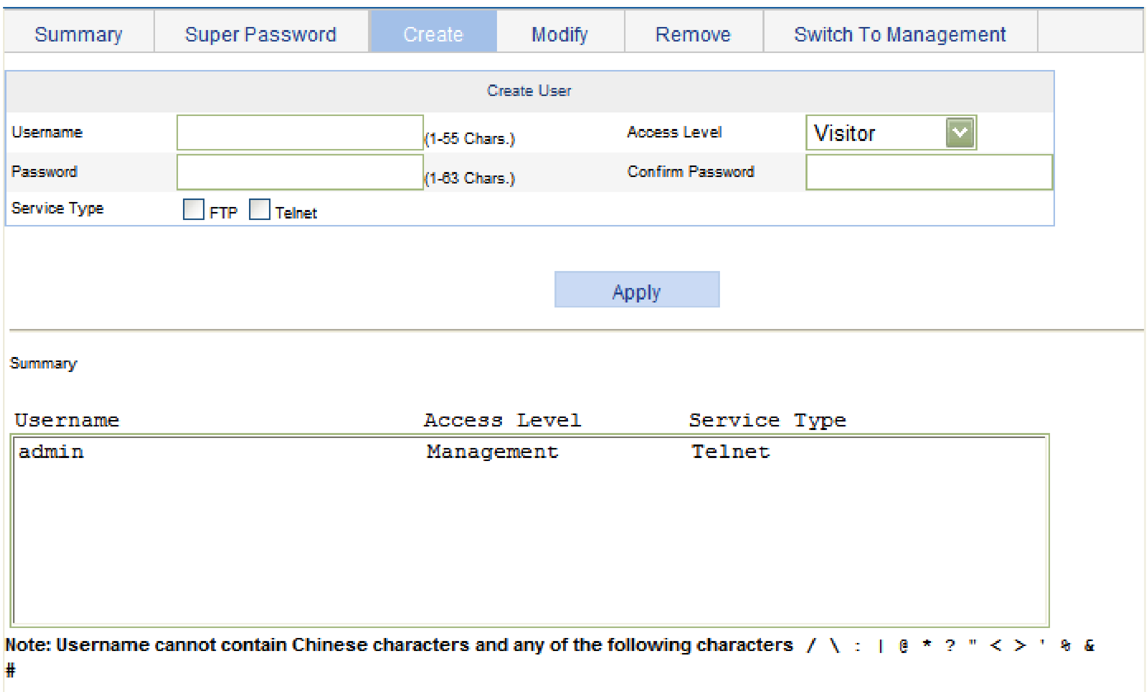
The device provides the following user management functions:

- Add a local user, and specify the password, access level, and service types for the user.
- Set the super password for non-management level users to switch to the management level.
- Switch to the management level from a lower level.

Adding a local user

1. Select **Device** > **Users** from the navigation tree.
2. Click the **Create** tab.

Figure 73 Creating a user



3. Configure a local user as described in Table 16.
4. Click **Apply**.

Table 16 Configuration items

Item	Description
Username	Set a username for the user.
Access Level	Select an access level for the user. Users of different levels can perform different operations. User levels, in order from low to high, are as follows: • **Visitor**—Users of this level can only perform ping and traceroute operations. They can neither access the data on the device nor configure the device. • **Monitor**—Users of this level can perform ping and traceroute operations and access the data on the device but cannot configure the device. • **Configure**—Users of this level can perform ping and traceroute operations, 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 configuration file. • **Management**—Users of this level can perform any operations on the device.
Password	Set the password for the user.
Confirm Password	Enter the same password again. Otherwise, the system will prompt that the two passwords are not consistent when you apply the configuration.
Service Type	Select the service types for the user to use, including FTP and Telnet. The terminal service allows users to log in from the console port. You must select at least one service type.

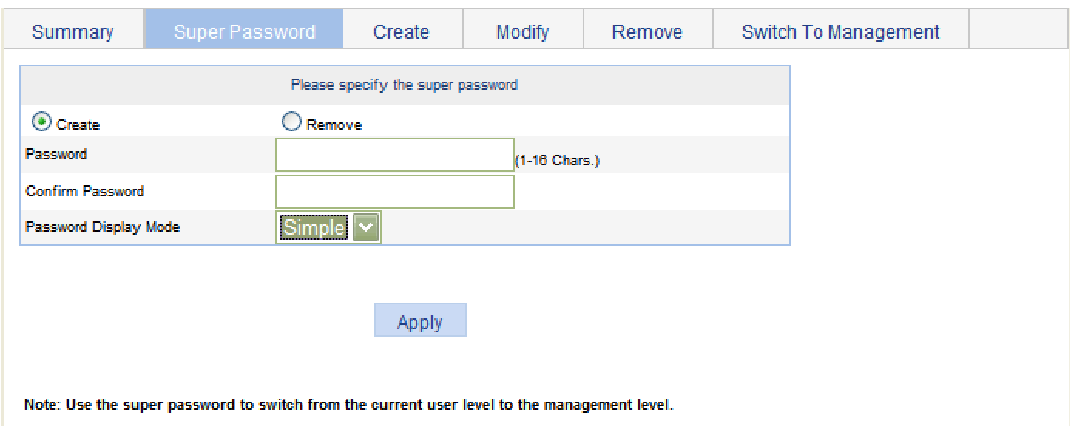
Setting the super password

A management level user can set the password for non-management level users to switch to the management level. If no such password is configured, no switchover can occur.

To set the super password:

1. Select **Device** > **Users** from the navigation tree.
2. Click the **Super Password** tab.

Figure 74 Super password



3. Configure a super password as described in Table 17.
4. Click **Apply**.

Table 17 Configuration items

Item	Description
Create/Remove	Select the operation type: • **Create**—Configure or modify the super password. • **Remove**—Remove the current super password.
Password	Set the password for non-management level users to switch to the management level.
Confirm Password	Enter the same password again. Otherwise, the system will prompt that the two passwords entered are not consistent when you apply the configuration.
Password Display Mode	Set the password display mode. Available options include **Simple** and **Cipher**. But whichever you select, the password is always saved in cipher text to the configuration file and displayed in cipher text.

Switching to the management level

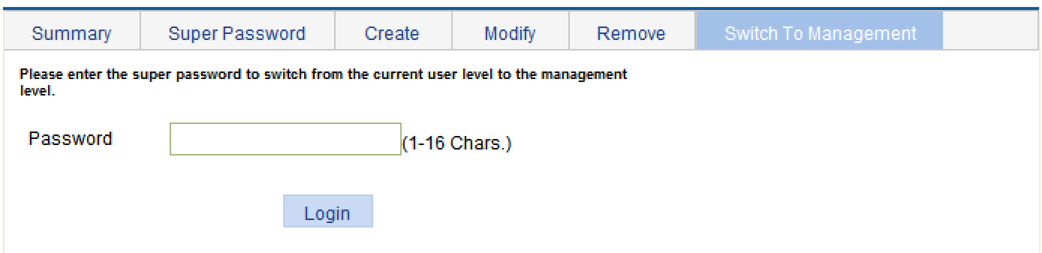
This function allows a user to switch from the current user level to the management level. To switch to the management level, a user must provide the correct super password.

The access level switchover of a user is valid for the current login only; it does not change the access level configured for the user. When the user re-logs in to the Web interface, the access level of the user is still the original level.

To switch to the management level:

1. Select **Device** > **Users** from the navigation tree.
2. Click the **Switch To Management** tab.
3. Enter the correct super password.
4. Click **Login**.

Figure 75 Switching to the management level



Configuring a loopback test

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.

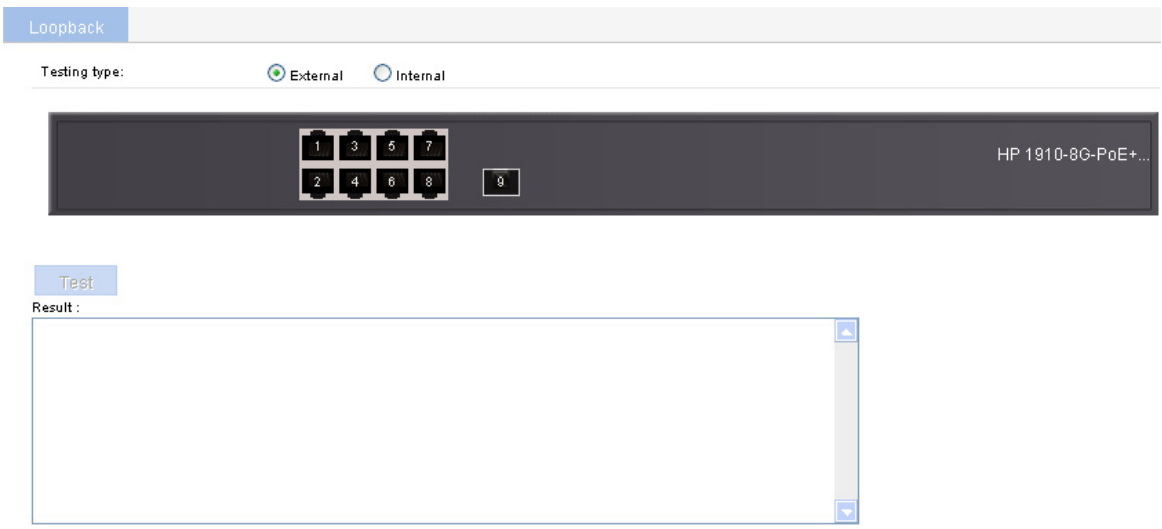
Ethernet port loopback test can be an internal loopback test or an external loopback test.

- 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.

Configuring a loopback test

1. Select **Device** > **Loopback** from the navigation tree to enter the loopback test configuration page, as shown in Figure 76.

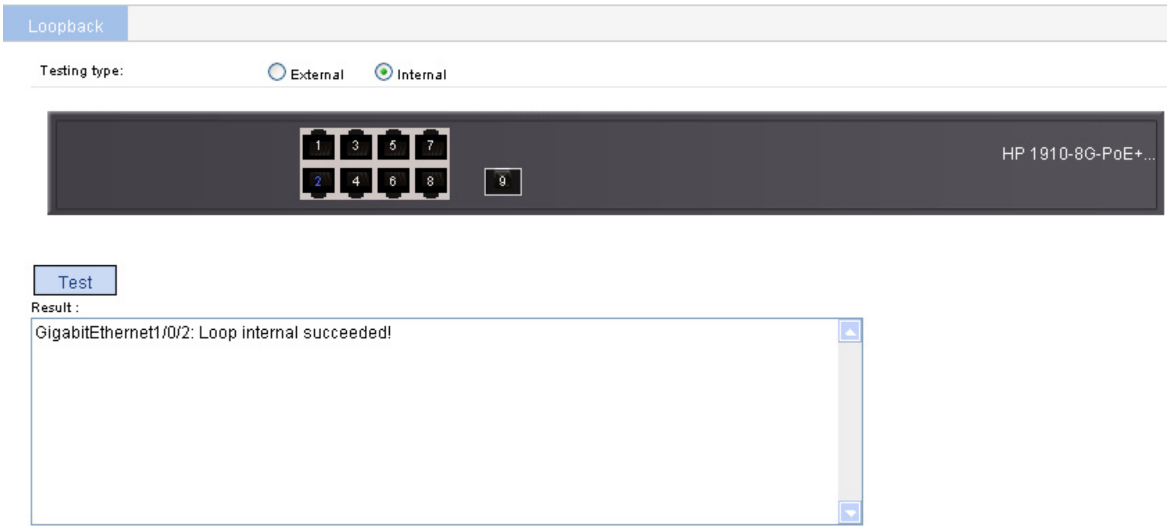
Figure 76 Loopback test page



2. Select **External** or **Internal** for loopback test type.
3. Select an Ethernet interface from the chassis front panel.
4. Click **Test**.

   After the test is complete, display the loopback test result, as shown in Figure 77.

Figure 77 Loopback test result



Configuration guidelines

Follow these guidelines when you configure 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 operates in full duplex mode when the loopback test is performed, and restores its original duplex mode after the loopback test.

Configuring VCT

Overview

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.

NOTE:

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.

Testing cable status

1. Select **Device** > **VCT** from the navigation tree to enter the page for testing cable status.
2. Select the port you want to test on the chassis front panel.
3. Click **Test**.

   The test result is returned within five seconds and displayed in the **Result** field.

Figure 78 Testing the status of the cable connected to an Ethernet port

The result displays the cable status and length:

- The cable status 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 abnormal, the cable length displayed is the length between the current port and the location where fault occurs.
- The cable length detected can have an error of up to 5 meters.

Configuring the flow interval

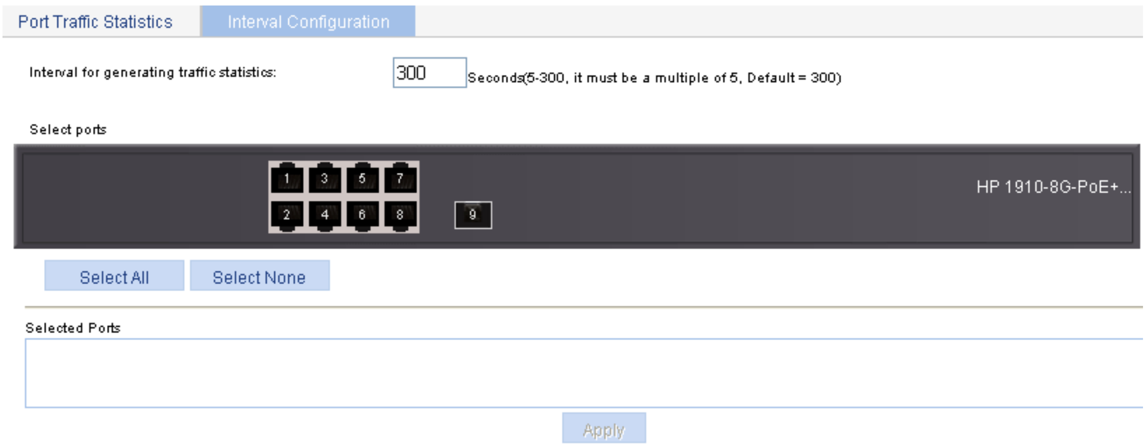
Overview

With the flow interval module, you can view the number of packets and bytes sent/received by a port and the bandwidth utilization of the port over the specified interval.

Setting the traffic statistics generating interval

1. Select **Device** > **Flow interval** from the navigation tree.
2. Click the **Interval Configuration** tab.

Figure 79 Setting the traffic statistics generating interval



3. Set the traffic statistics generating interval as described in Table 18.
4. Click **Apply**.

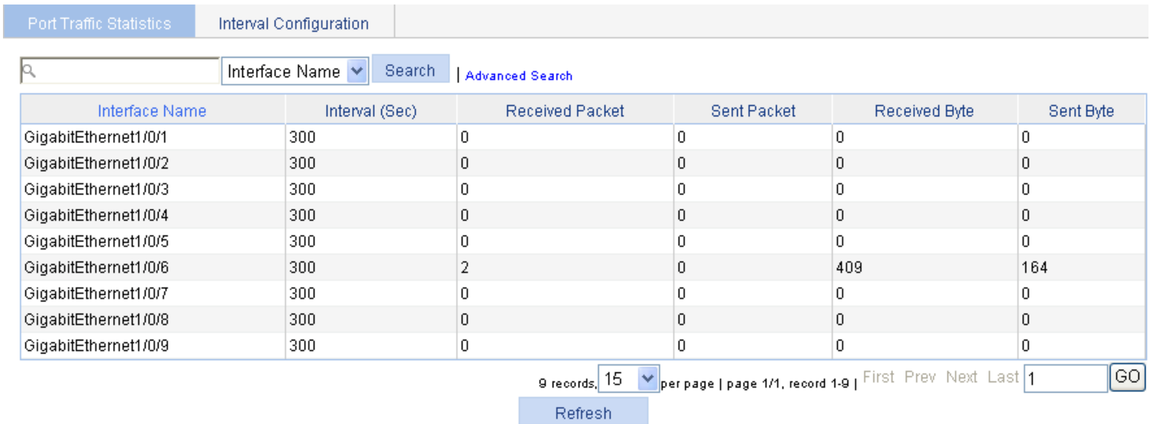
Table 18 Configuration items

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

1. Select **Device** > **Flow interval** from the navigation tree.
   By default, the **Port Traffic Statistics** tab is displayed.
2. View the number of packets and bytes sent/received by each port and the bandwidth utilization of each port over the last interval.

Figure 80 Port traffic statistics



Interface Name	Interval (Sec)	Received Packet	Sent Packet	Received Byte	Sent Byte
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	2	0	409	164
GigabitEthernet1/0/7	300	0	0	0	0
GigabitEthernet1/0/8	300	0	0	0	0
GigabitEthernet1/0/9	300	0	0	0	0

NOTE:

When the bandwidth utilization is lower than 1%, 1% is displayed.

Configuring storm constrain

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 unknown 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.

Alternatively, you can configure the storm suppression function to control a specific type of traffic. For more information about the storm suppression function, see "Managing ports." Because 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 unknown unicast storm suppression enabled on a port, do not enable storm constrain for unknown unicast traffic on the port.

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 unknown unicast) exceeds the upper threshold:

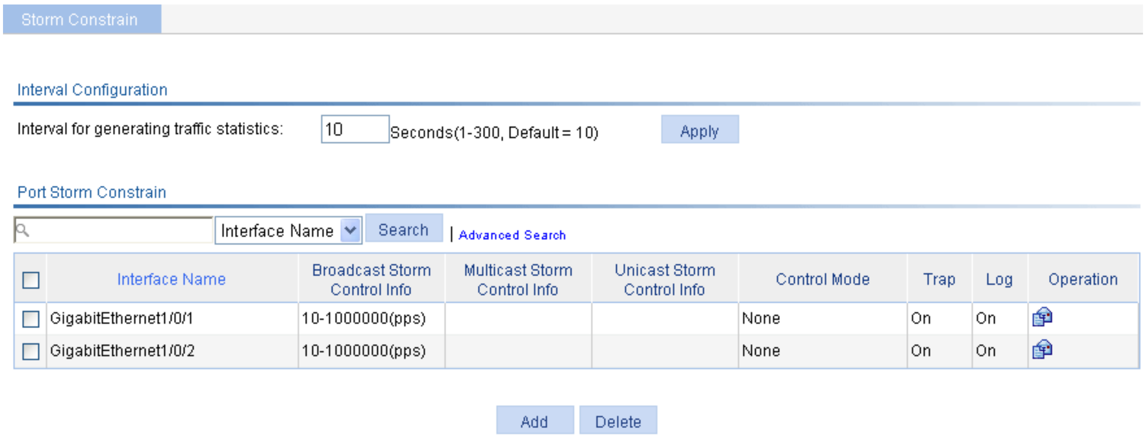
- **Block**—Blocks the port. The port is blocked and stops forwarding the traffic of this type until the type of traffic drops down below the lower threshold. A port blocked by the storm constrain function can still forward other types of traffic and collect statistics for the blocked traffic.
- **Shutdown**—Shuts down the port. The port is shut down and stops forwarding all types of traffic, and cannot automatically restore even when the type of traffic drops down below the lower threshold. To bring up the port, select **Device** > **Port Management** to configure the port (see "Managing ports"), or cancel the storm constrain setting on the port.

Setting the traffic statistics generating interval

To set the traffic statistics generating interval:

1. Select **Device** > **Storm Constrain** from the navigation tree to enter the storm constrain configuration page.
2. In the **Interval for generating traffic statistics** field, enter the traffic statistics generating interval for storm constrain.
3. Click **Apply**.

Figure 81 The storm constrain tab



NOTE:

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

1. Select **Device** > **Storm Constrain** from the navigation tree to enter the storm constrain configuration page.
2. In the **Port Storm Constrain** area, click **Add** to enter the page for adding port storm constrain configuration.

Figure 82 Adding storm constrain settings for ports

3. Set the storm constraint function.
4. Click **Apply**.

Table 19 Configuration items

<table>
<tr><th>Item</th><th>Remarks</th></tr>
<tr><td>Control Mode</td><td>Specify the action to be performed when a type of traffic exceeds the upper threshold. Available options include:
• None—Performs no action.
• Block—Blocks the traffic of this type on a port when the type of traffic exceeds the upper threshold.
• Shutdown—Shuts down the port when a type of traffic exceeds the traffic threshold. The port stops forwarding traffic as a result.
NOTE:
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. 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 when the packet storm is present. Nevertheless, the action will be taken within two intervals.</td></tr>
<tr><td>Broadcast Threshold</td><td rowspan="3">Set the broadcast, multicast, and unknown unicast thresholds.
• None—Performs no storm constrain for the selected port or ports.
• pps—Specifies the storm constrain upper threshold and lower threshold in packets per second (pps).
• ratio—Specifies the storm constrain upper threshold and lower threshold in percentage of received packets to the transmission capability of each selected port.
• kbps—Specifies the storm constrain upper threshold and lower threshold in kilobits per second (kbps).
NOTE:
• On a port, you can set the thresholds for broadcast, multicast, and unknown 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.</td></tr>
<tr><td>Multicast Threshold</td></tr>
<tr><td>Unicast Threshold</td></tr>
<tr><td>Trap</td><td>Select or clear the box to enable or disable the system to send trap messages both when an upper threshold is crossed and when the lower threshold is crossed after that.</td></tr>
<tr><td>Log</td><td>Select or clear the box to enable or disable the system to output logs both when an upper threshold is crossed and when the lower threshold is crossed after that.</td></tr>
<tr><td>Select ports</td><td>Select ports from the chassis front panel to apply the storm constrain settings to them.</td></tr>
</table>

Configuring RMON

Overview

Remote Monitoring (RMON) is an enhancement to SNMP for remote device management and traffic monitoring. An RMON monitor, typically the RMON agent embedded in a network device, periodically or continuously collects traffic statistics for the network attached to a port, and when a statistic crosses a threshold, logs the crossing event and sends a trap to the management station.

RMON uses SNMP traps to notify NMSs of exceptional conditions. RMON SNMP traps report various events, including traffic events such as broadcast traffic threshold exceeded. In contrast, SNMP standard traps report device operating status changes such as link up, link down, and module failure.

RMON enables proactive monitoring and management of remote network devices and subnets. The managed device can automatically send a trap when a statistic crosses an alarm threshold, and the NMS does not need to constantly poll MIB variables and compare the results. As a result, network traffic is reduced.

Working mechanism

RMON monitors typically take one of the following forms:

- **Dedicated RMON probes**. NMSs can obtain management information from RMON probes directly and control network resources. In this approach, NMSs can obtain all RMON MIB information.
- **RMON agents embedded in network devices**. NMSs exchange data with RMON agents by using basic SNMP operations to gather network management information. This approach consumes the resources of managed network devices, and most RMON agent implementations only provide four groups of MIB information, alarm, event, history, and statistics.

HP devices provide the embedded RMON agent function. You can configure your device to collect and report traffic statistics, error statistics, and performance statistics.

RMON groups

Among the RFC 2819 defined RMON groups, HP implements the statistics group, history group, event group, and alarm group supported by the public MIB.

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 (etherStatsTable) 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 (etherHistoryTable) 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).

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. The events can be handled in one of the following ways:

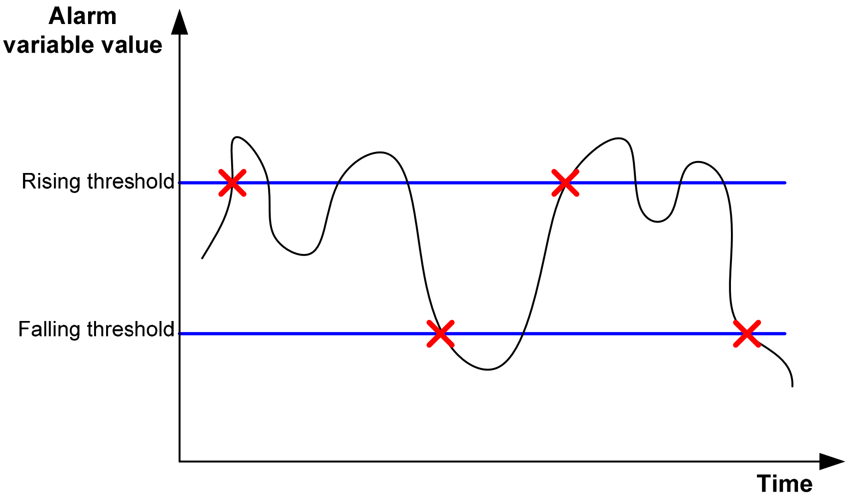
- **Log**—Logs event related information (the time of the event occurred, contents of the event, and so on) in the event log table of the RMON MIB of the device, and thus the management device can check the logs through the SNMP GET operation.
- **Trap**—Sends a trap to notify the occurrence of this event to the network management station (NMS).
- **Log-Trap**—Logs event information in the event log table and sending a trap to the NMS.
- **None**—No action.

Alarm group

The RMON alarm group monitors alarm variables, such as the count of incoming 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 rising threshold, a rising event is triggered. When the value of the monitored variable is smaller than or equal to the falling threshold, a falling event is triggered. The event is then handled as defined in the event group.

If an alarm entry crosses a threshold multiple times in succession, the RMON agent generates an alarm event only for the first crossing. For example, if the value of a sampled alarm variable crosses the rising threshold multiple times before it crosses the falling threshold, only the first crossing triggers a rising alarm event, as shown in Figure 83.

Figure 83 Rising and falling alarm events



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 20 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 21 to configure RMON history statistics function.

Table 20 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 various traffic statistics on the interface, including network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received. The statistics are cleared at a reboot. IMPORTANT: Only one statistics entry can be created for one interface.

Table 21 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. IMPORTANT: 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.

Perform the tasks in Table 22 to configure RMON alarm function.

Table 22 RMON alarm configuration task list

Task	Remarks
Configuring a statistics entry	Required. You can create up to 100 statistics entries in a statistics table. As the alarm variables that can be configured through the web interface 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. After a statistics entry is created on an interface, the system collects various traffic statistics on the interface, including network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received. The statistics are cleared at a reboot. IMPORTANT: Only one statistics entry can be created for one interface.
Configuring an event entry	Required. 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. IMPORTANT: 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. IMPORTANT: 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 23.

Table 23 Displaying RMON running status

Task	Remarks
Displaying RMON statistics	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.

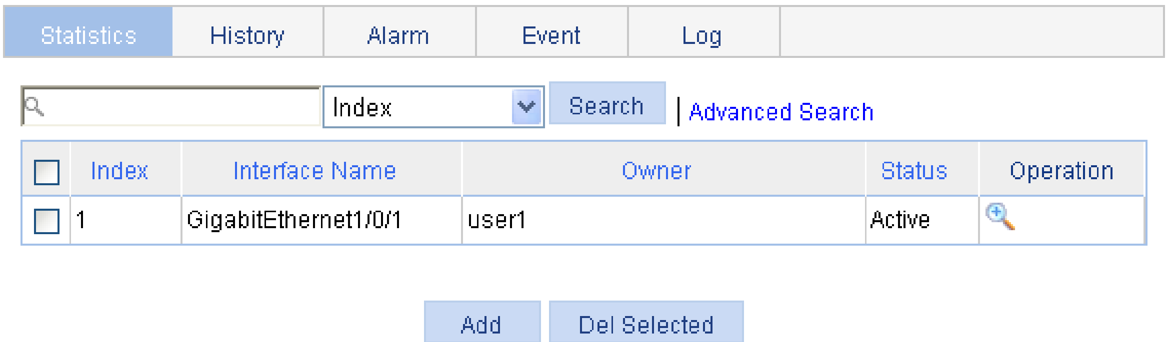
Task	Remarks
Displaying RMON event logs	If you have configured the system to log an event after the event is triggered when you configure the event group, the event is recorded into the RMON log. You can perform this task to display the details of the log table.

Configuring a statistics entry

1. Select **Device** > **RMON** from the navigation tree.

   The **Statistics** tab page appears.

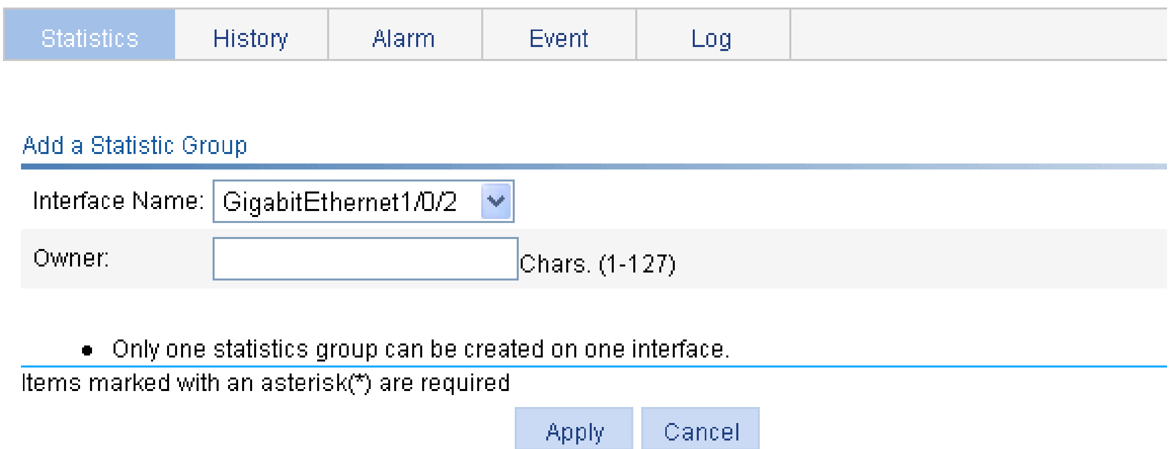
Figure 84 Statistics tab



2. Click **Add**.

   The page for adding a statistics entry appears.

Figure 85 Adding a statistics entry



3. Configure a statistic entry as described in Table 24.
4. Click **Apply**.

Table 24 Configuration items

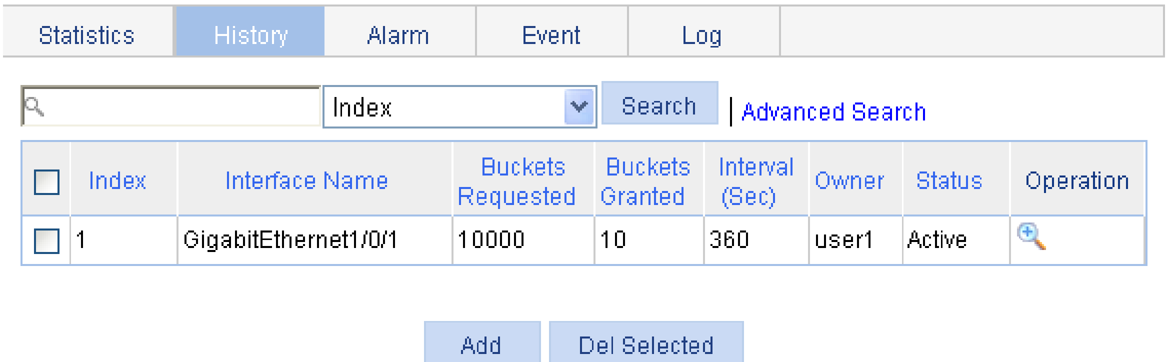
Item	Description
Interface Name	Select the name of the interface on which the statistics entry is created. Only one statistics entry can be created on one interface.

Item	Description
Owner	Set the owner of the statistics entry.

Configuring a history entry

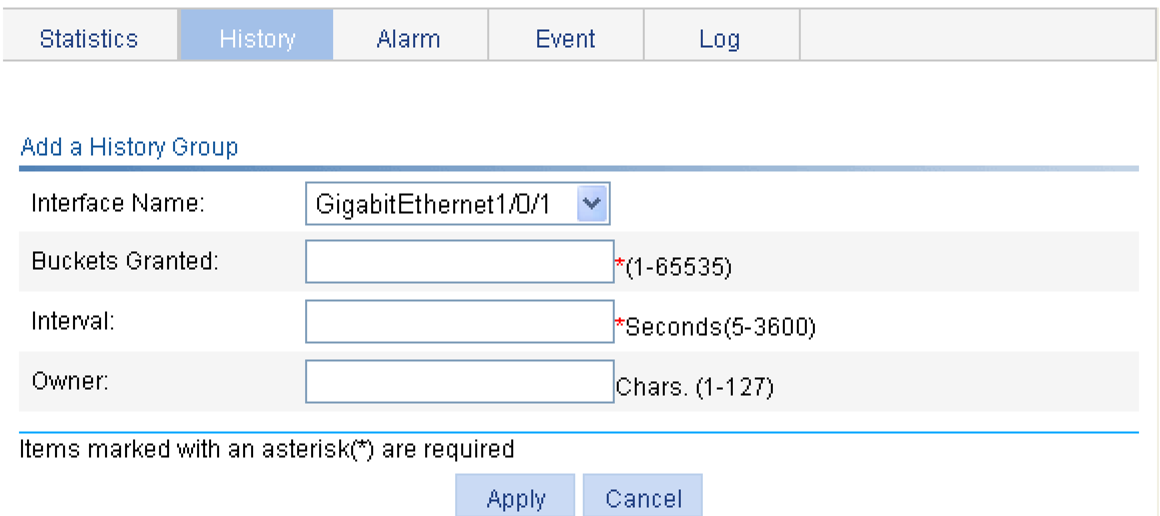
1. Select **Device** > **RMON** from the navigation tree.
2. Click the **History** tab.
   The **History** tab page appears.

Figure 86 History tab



3. Click **Add**.
   The page for adding a history entry appears.

Figure 87 Adding a history entry



4. Configure a history entry as described in Table 25.
5. Click **Apply**.

Table 25 Configuration items

Item	Description
Interface Name	Select the name of the interface on which the history entry is created.

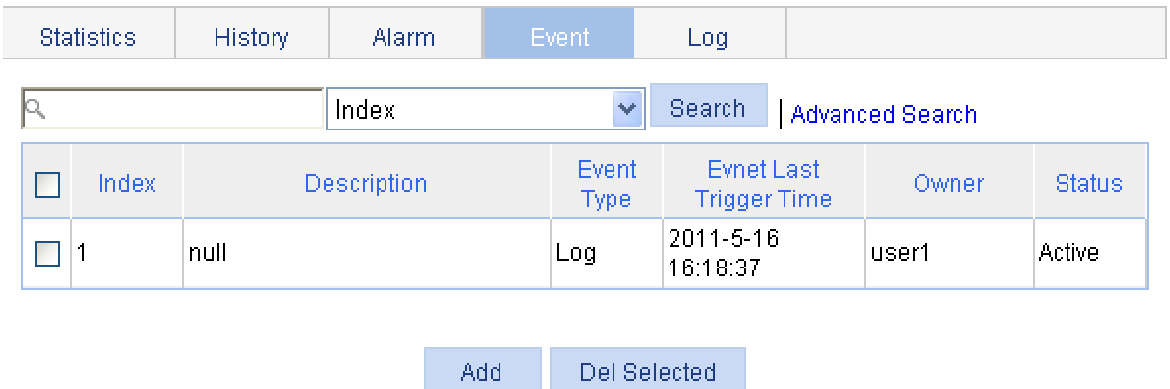
Item	Description
Buckets Granted	Set the capacity of the history record list corresponding to this history entry, namely, the maximum number of records that can be saved in the history record list. If the current number of the entries in the table has reached the maximum number, the system will delete 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.

Configuring an event entry

1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Event** tab.

   The **Event** tab page appears.

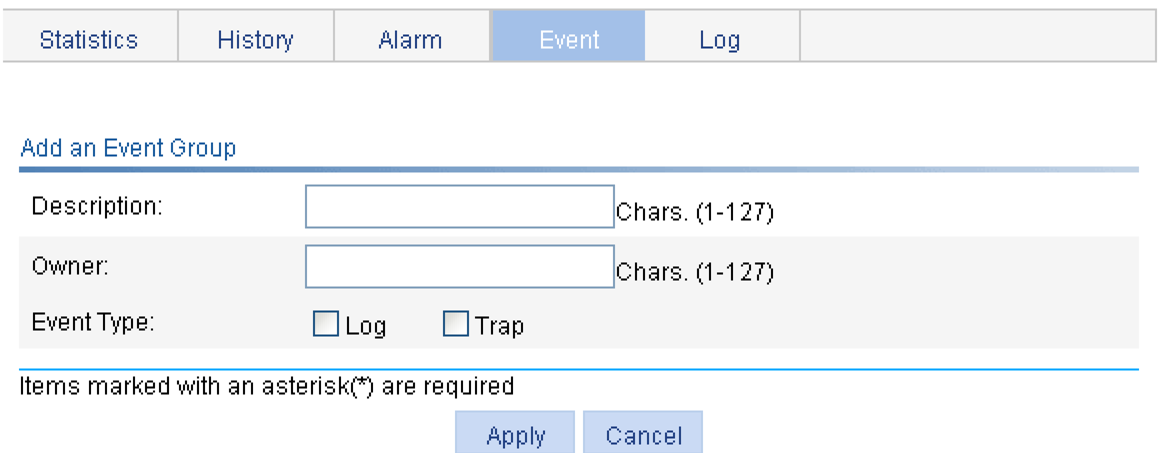
Figure 88 Event tab



3. Click **Add**.

   The page for adding an event entry appears.

Figure 89 Adding an event entry



4. Configure an event entry as described in Table 26.

5. Click **Apply**.

Table 26 Configuration items

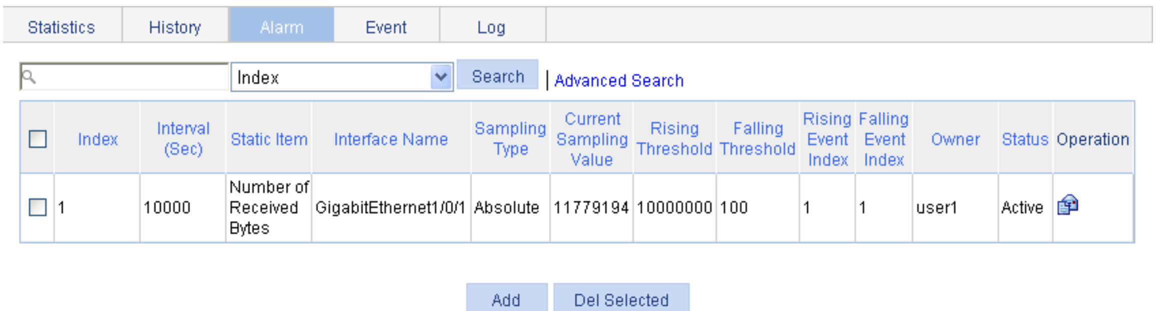
Item	Description
Description	Set the description for the event.
Owner	Set the owner of the entry.
Event Type	Set the actions that the system will take when the event is triggered: • **Log**—The system will log the event. • **Trap**—The system will send a trap in the community name of **null**. If both **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.

Configuring an alarm entry

1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Alarm** tab.

   The **Alarm** tab page appears.

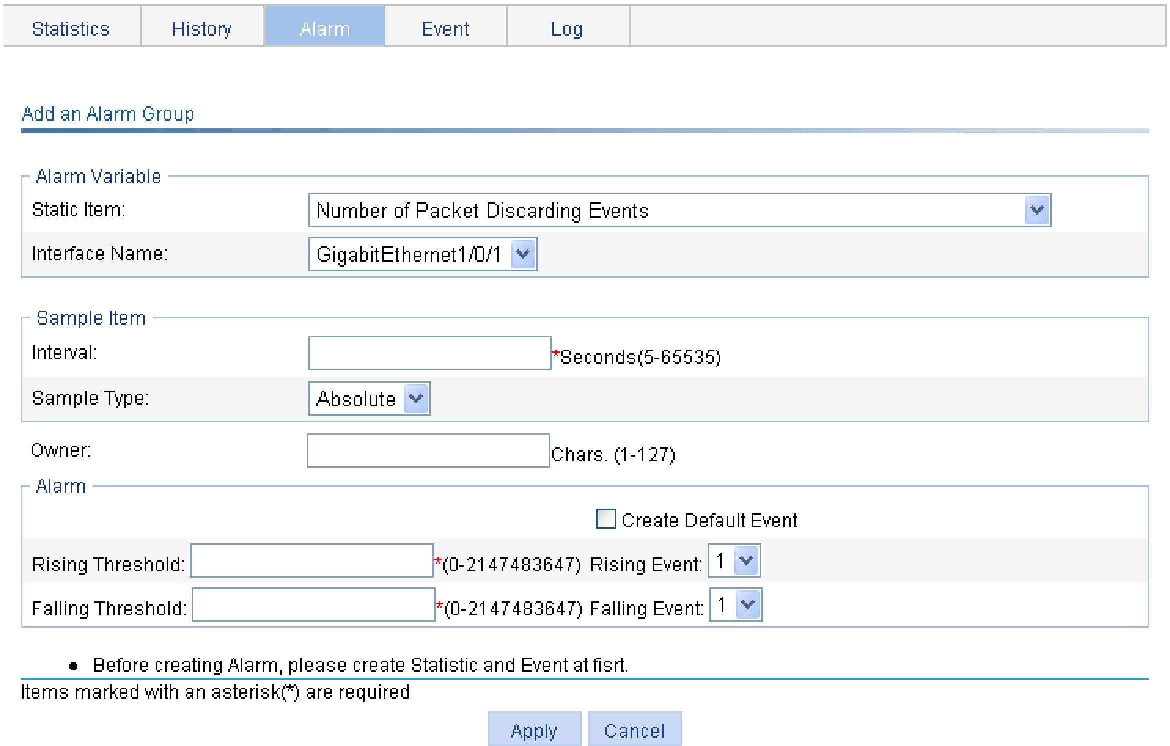
Figure 90 Alarm tab



3. Click **Add**.

   The page for adding an alarm entry appears.

Figure 91 Adding an alarm entry



4. Configure an alarm entry as described in Table 27.
5. Click **Apply**.

Table 27 Configuration items

Item	Description
Alarm variable:	
Static Item	Set the traffic statistics that will be collected and monitored, see Table 28 for details.
Interface Name	Set the name of the interface whose traffic statistics will be collected and monitored.
Sample Item:	
Interval	Set the sampling interval.
Sample Type	Set the sampling type: • **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:	

Item	Description
Create Default Event	Select whether to create a default event. 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** 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** box is selected, this option is not configurable.

Displaying RMON statistics

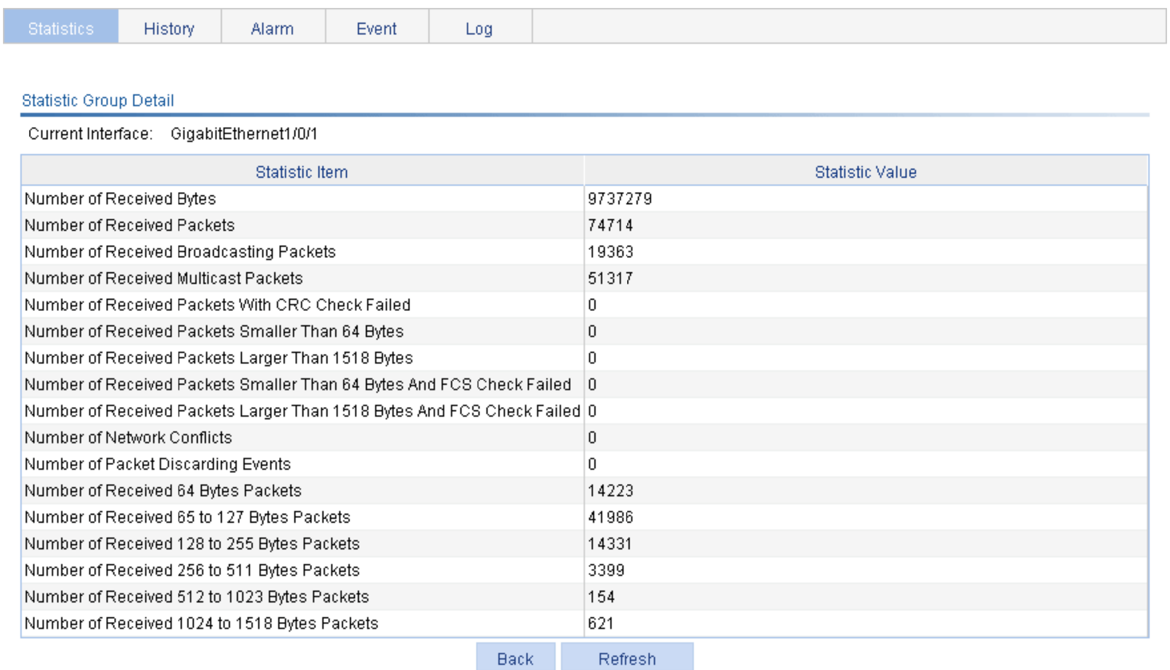
1. Select **Device** > **RMON** from the navigation tree.

   The page in Figure 84 appears.

2. Click the  icon of the statistics entry of an interface.

   The page displaying RMON statistics appears.

Figure 92 Statistics tab



3. View statistics items on the current interface.

Table 28 Field description

Field	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.
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.

Field	Description
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.

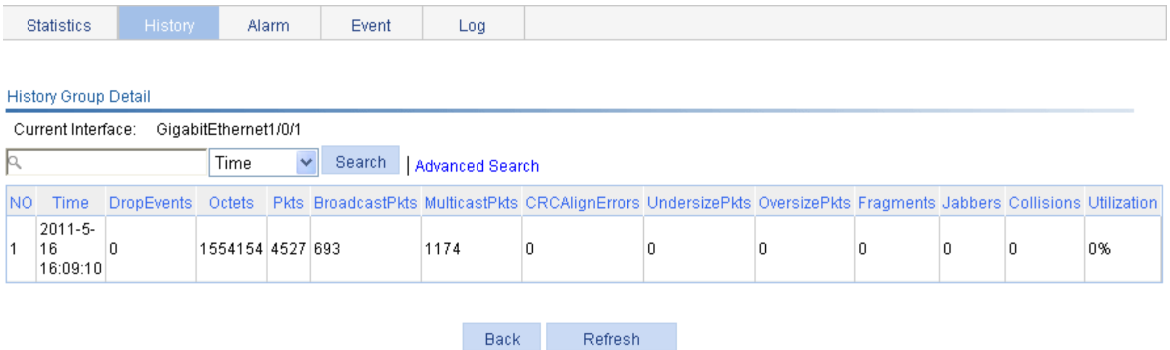
Displaying RMON history sampling information

1. Select **Device** > **RMON** from the navigation tree.
2. Click the **History** tab.

   The page in Figure 86 appears.
3. Click the icon of a history entry.

   The page displaying RMON history sampling information appears.

Figure 93 History tab



4. View history sampling information on the current interface.

Table 29 Field description

Field	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.

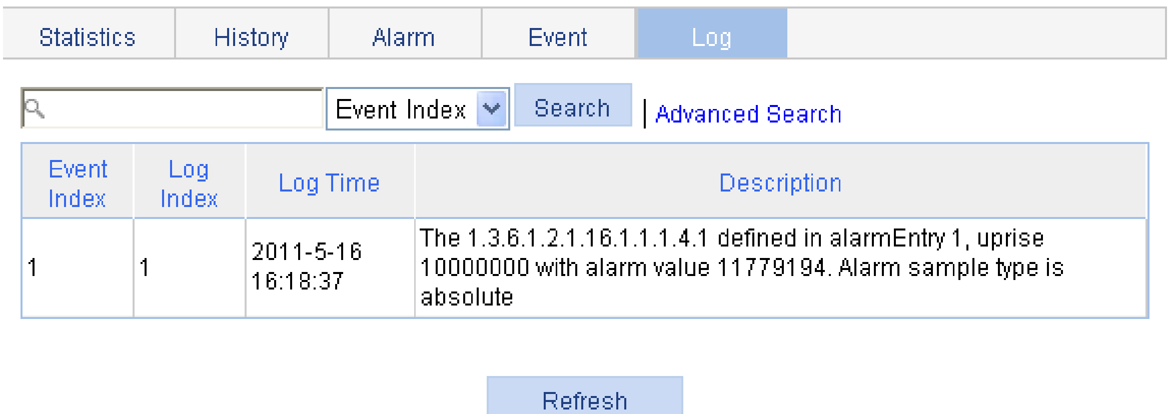
Field	Description
UndersizePkts	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
OversizePkts	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
Fragments	Number 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.

Displaying RMON event logs

1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Log** tab.

   The page displaying log information appears.

Figure 94 Log tab



3. View log information for all event entries.

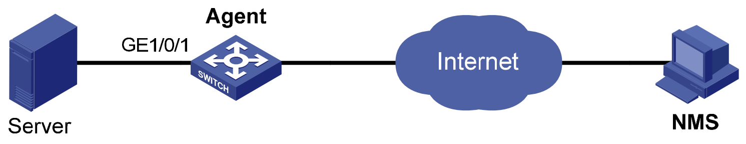
   In this example, event 1 has generated one log, which is triggered because the alarm value (11779194) exceeds the rising threshold (10000000). The sampling type is absolute.

RMON configuration example

Network requirements

As shown in Figure 95, Agent is connected to a remote NMS across the Internet. Create an entry in the RMON Ethernet statistics table to gather statistics on GigabitEthernet 1/0/1 with the sampling interval being ten seconds, and perform corresponding configurations so that the system will log the event when the number of bytes received on the interface more than 1000 or less than 100.

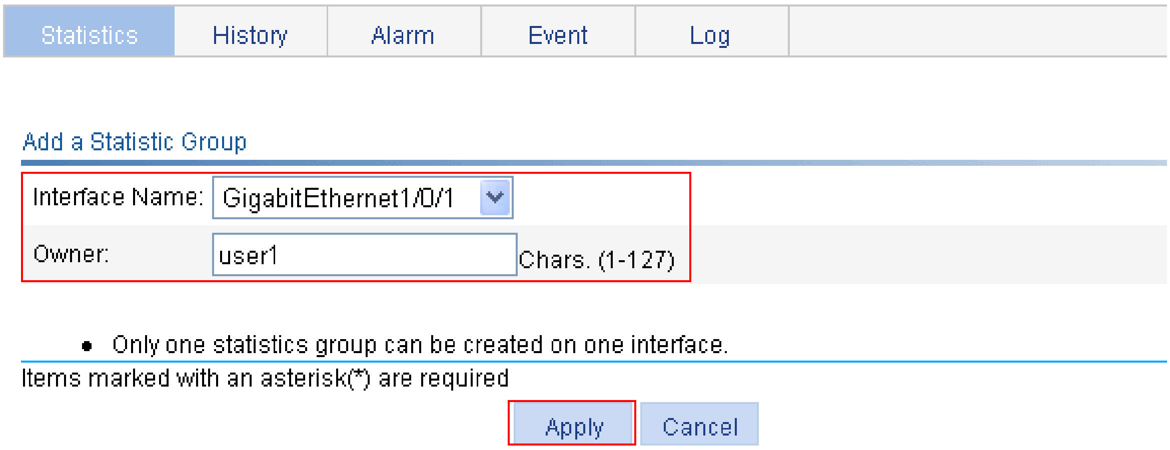
Figure 95 Network diagram



Configuration procedure

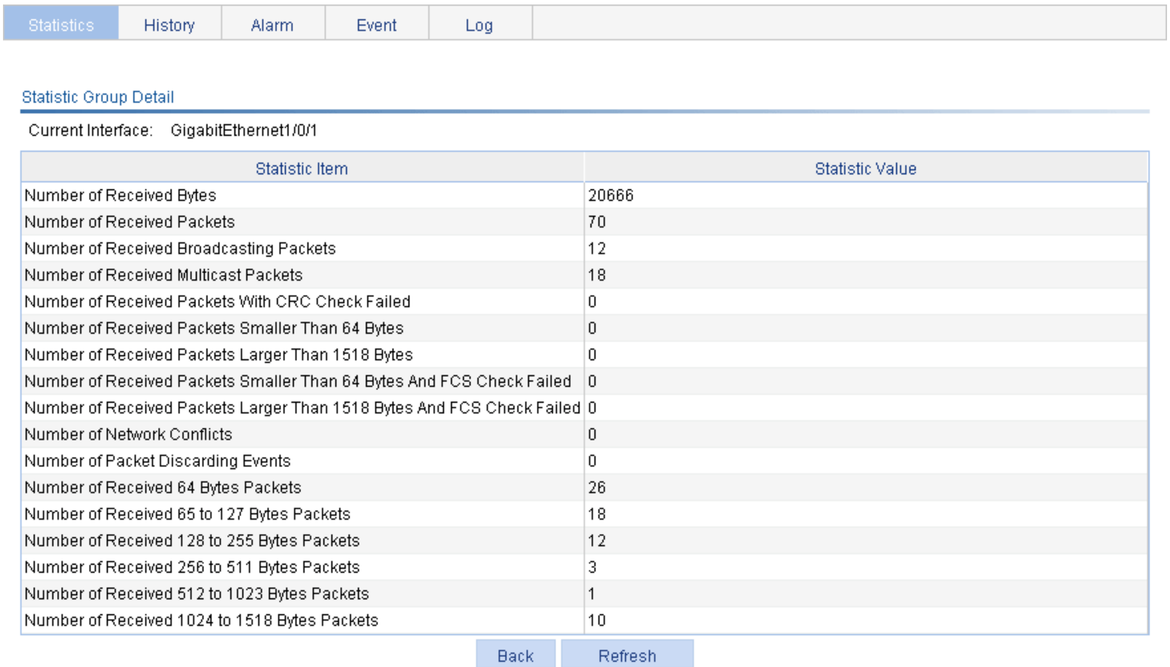
1. Configure RMON to gather statistics for interface GigabitEthernet 1/0/1:
    a. Select **Device** > **RMON** from the navigation tree.
    The **Statistics** tab page appears.
    b. Click **Add**.
    The page in Figure 96 appears.
    c. Select **GigabitEthernet1/0/1** from the **Interface Name** list, type **user1** in the **Owner** field, and click **Apply**.

Figure 96 Adding a statistics entry



2. Display RMON statistics for interface GigabitEthernet 1/0/1:
    a. Click the icon corresponding to GigabitEthernet 1/0/1.
    b. View the information as shown in Figure 97.

Figure 97 Displaying RMON statistics



Statistic Item	Statistic Value
Number of Received Bytes	20666
Number of Received Packets	70
Number of Received Broadcasting Packets	12
Number of Received Multicast Packets	18
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	26
Number of Received 65 to 127 Bytes Packets	18
Number of Received 128 to 255 Bytes Packets	12
Number of Received 256 to 511 Bytes Packets	3
Number of Received 512 to 1023 Bytes Packets	1
Number of Received 1024 to 1518 Bytes Packets	10

3. Create an event to start logging after the event is triggered:
   a. Click the **Event** tab.
   b. Click **Add**.
      The page in Figure 98 appears.
   c. Type **user1-rmon** in the **Owner** field, select the box before **Log**, and click **Apply**.
   d. The page displays the event entry, and you can see that the entry index of the new event is **1**, as shown in Figure 99.

Figure 98 Configuring an event group

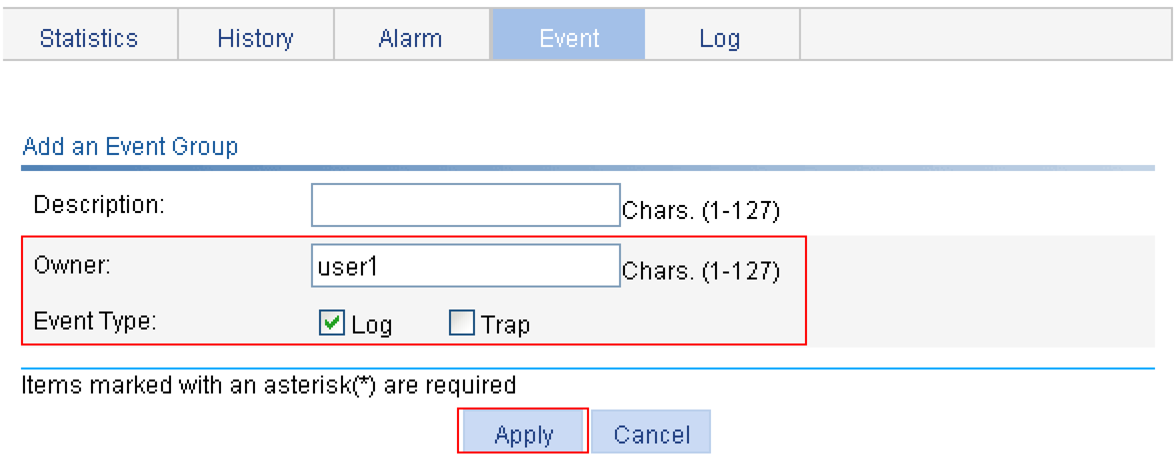
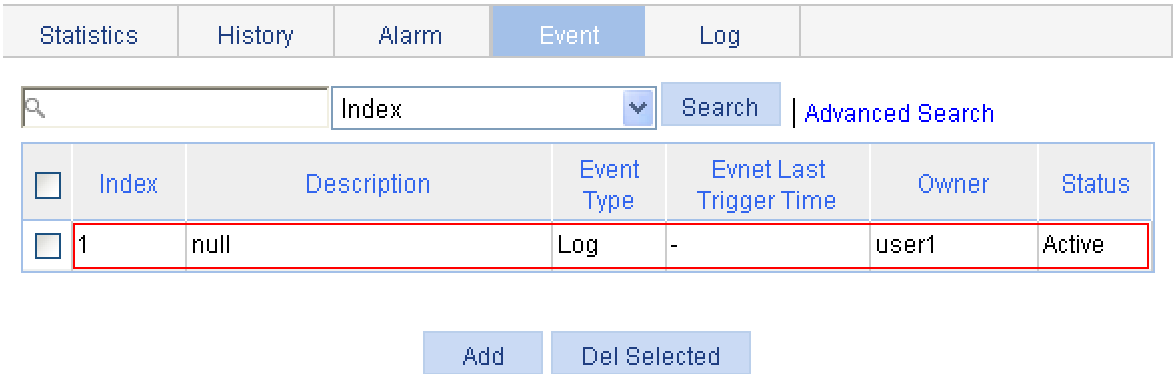


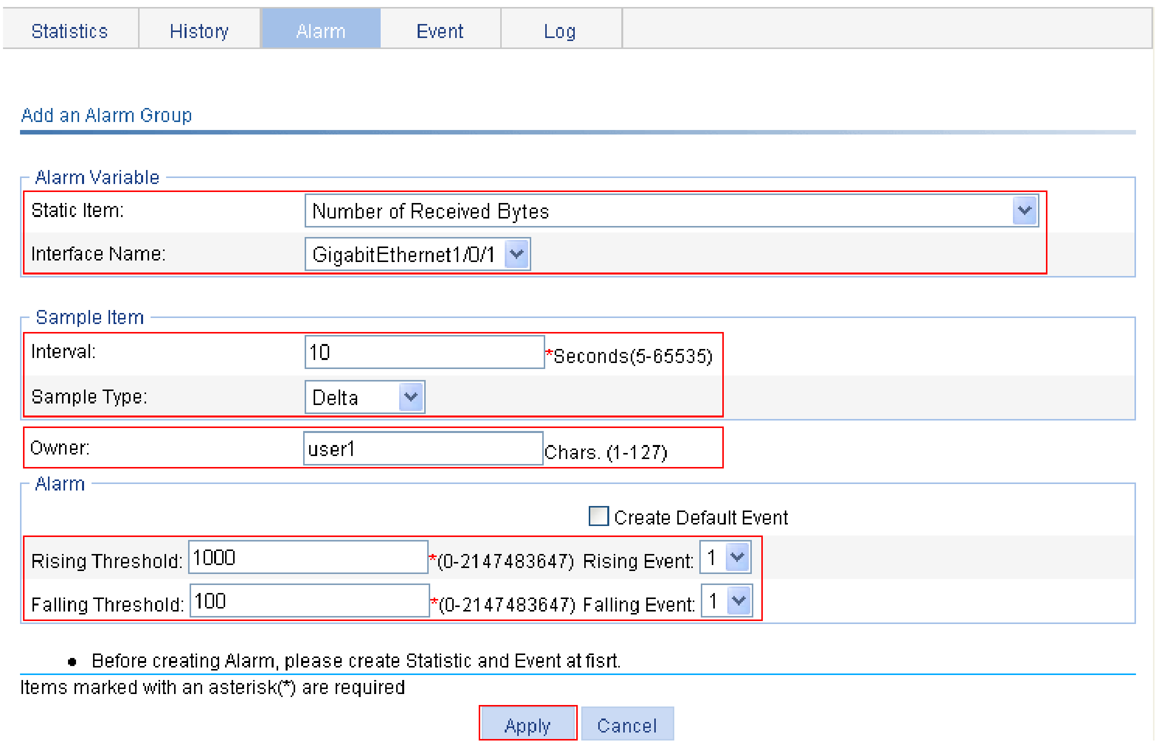
Figure 99 Displaying the index of a event entry



4. Configure an alarm group to sample received bytes on GigabitEthernet 1/0/1. When the received bytes exceed the rising or falling threshold, logging is enabled:
   a. Click the **Alarm** tab.
   b. Click **Add**.

      The page in Figure 100 appears.
   c. Select **Number of Received Bytes** from the **Static Item** list, select **GigabitEthernet1/0/1** from the **Interface Name** list, enter **10** in the **Interval** field, select **Delta** from the **Simple Type** list, enter **user1** in the **Owner** field, enter **1000** in the **Rising Threshold** field, select **1** from the **Rising Event** list, enter **100** in the **Falling Threshold** field, select **1** from the **Falling Event** list, and click **Apply**.

Figure 100 Configuring an alarm group



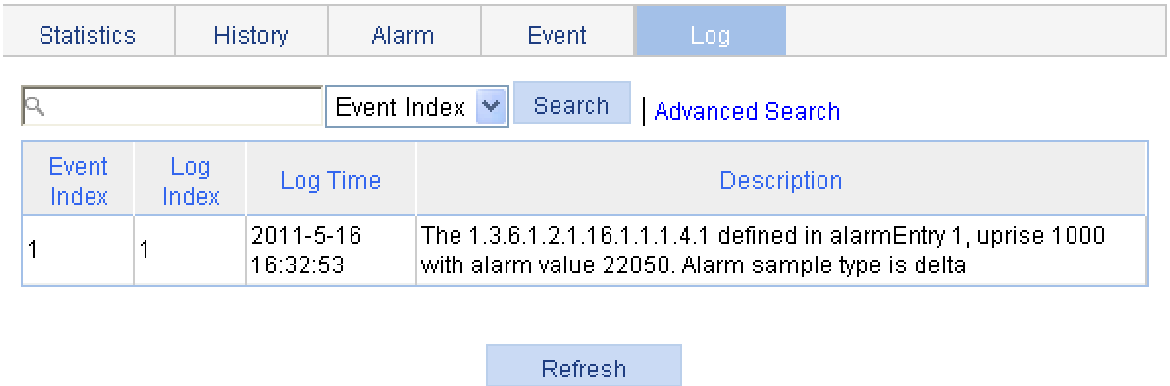
Verifying the configuration

After the above configuration, when the alarm event is triggered, you can view the log information about event 1 on the web interface.

1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Log** tab.

   The page displaying log information appears. The displayed information indicates that event 1 has generated one log, which is triggered because the alarm value (22050) exceeds the rising threshold (1000). The sampling type is absolute.

Figure 101 Log tab



Configuring energy saving

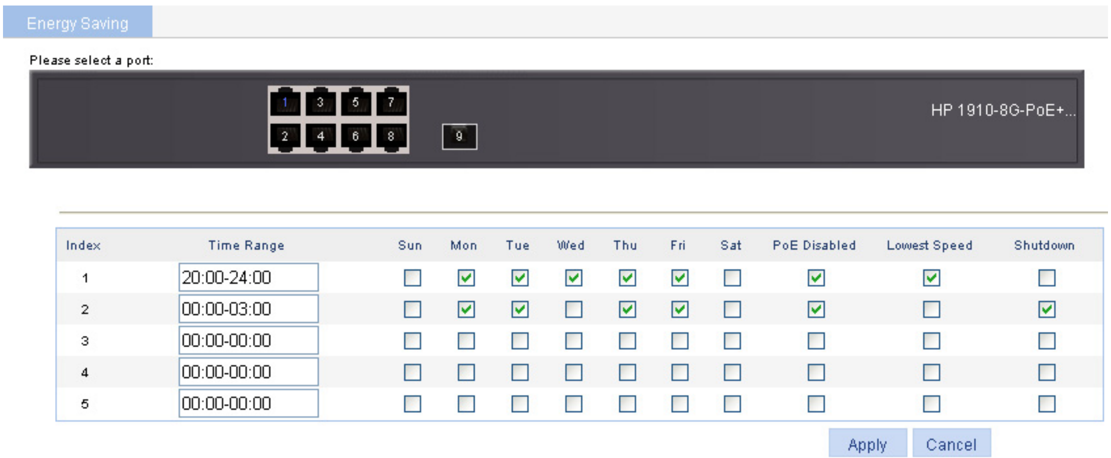
Energy saving overview

Energy saving enables a port to work at the lowest transmission speed, disable PoE, or go down during a specific 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

1. Select **Device** > **Energy Saving** from the navigation tree to enter the energy saving configuration page.
2. Click a port.

Figure 102 Energy saving configuration page



3. Configure an energy saving policy for the port as described in Table 30.
4. Click **Apply**.

Table 30 Configuration items

Item	Description
Time Range	Set the time period when the port is in the state of energy saving. IMPORTANT: • 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 is postponed and the end time is brought forward so that they meet the requirements. For example, if you set the time range to 08:08 to 10:12, the effective time range is 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. IMPORTANT: 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. IMPORTANT: An energy saving policy can have all the three energy saving schemes configured, of which the shutdown scheme takes the highest priority.

Configuring SNMP

Overview

Simple Network Management Protocol (SNMP) is an Internet standard protocol widely used for a management station to access and operate the devices on a network, regardless of their vendors, physical characteristics and interconnect technologies.

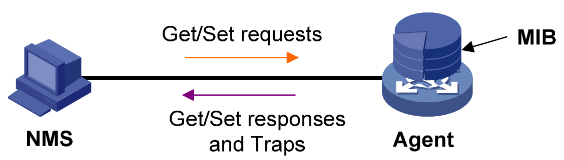
SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

SNMP mechanism

The SNMP framework comprises the following elements:

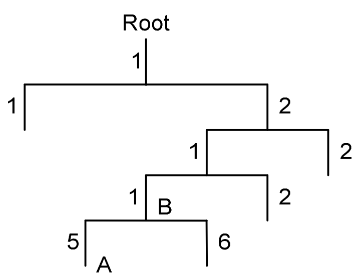
- **SNMP manager**—Works on an NMS to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and send traps to the NMS when some events, such as interface state change, occur.
- **Management Information Base (MIB)**—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

Figure 103 Relationship between an NMS, agent and MIB



A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a string of numbers that describes the path from the root node to a leaf node. For example, object B in Figure 104 is uniquely identified by the OID {1.2.1.1}.

Figure 104 MIB tree



SNMP provides the following basic operations:

- **Get**—The NMS retrieves SNMP object nodes in an agent MIB.
- **Set**—The NMS modifies the value of an object node in an agent MIB.

- **Notifications**—Includes traps and informs. SNMP agent sends traps or informs to report events to the NMS. The difference between these two types of notification is that informs require acknowledgement but traps do not. The device supports only traps.

SNMP protocol versions

HP supports SNMPv1, SNMPv2c, and SNMPv3. An NMS and an SNMP agent must use the same SNMP version to communicate with each other.

- **SNMPv1**—Uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as set on the SNMP agent. If the community name used by the NMS is different from the community name set on the agent, the NMS cannot establish an SNMP session to access the agent or receive traps and notifications from the agent.
- **SNMPv2c**—Uses community names for authentication. SNMPv2c is compatible with SNMPv1, but supports more operation modes, data types, and error codes.
- **SNMPv3**—Uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate and encrypt SNMP packets for integrity, authenticity, and confidentiality.

Recommended configuration procedure

SNMPv3 differs from SNMPv1 and SNMPv2c in many aspects. Their configuration procedures are described in separate sections.

Table 31 SNMPv1 or SNMPv2c configuration task list

Task	Remarks
1. Enabling SNMP agent	Required. By default, the SNMP agent function is disabled. IMPORTANT: If SNMP agent is disabled, all SNMP agent-related configurations will be removed.
2. 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.
3. Configuring an SNMP community	Required.
4. Configuring the 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 (usually the NMS) of the SNMP traps. The SNMP agent sends traps to inform the NMS of important events, such as a reboot. By default, an agent is allowed to send SNMP traps to the NMS.
5. Displaying SNMP packet statistics	Optional.

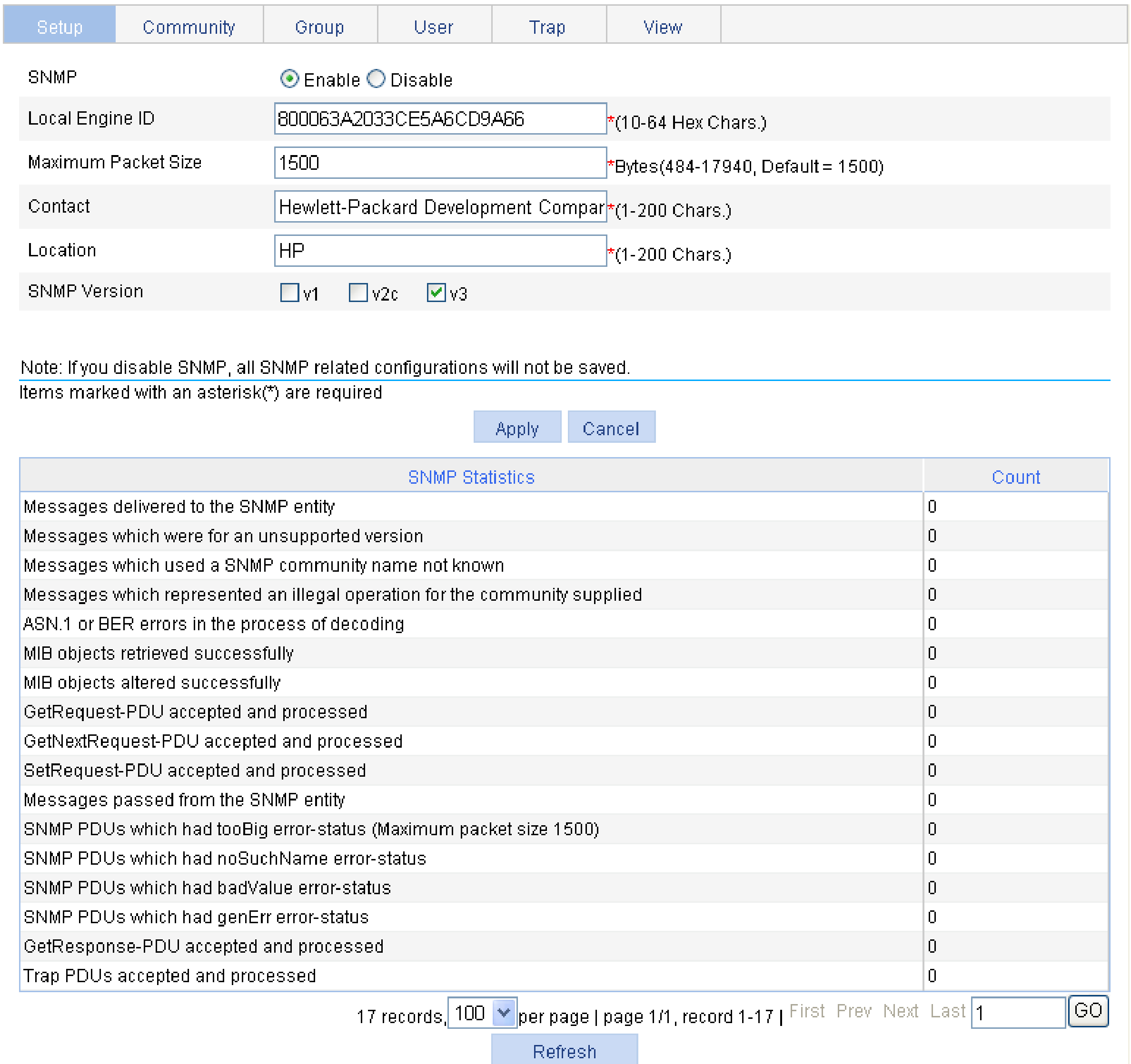
Table 32 SNMPv3 configuration task list

Task	Remarks
1. Enabling SNMP agent	Required. By default, the SNMP agent function is disabled. IMPORTANT: If SNMP agent is disabled, all SNMP agent-related configurations will be removed.
2. 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.
3. 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.
4. Configuring an SNMP user	Required. Before creating an SNMP user, you need to create the SNMP group to which the user belongs. IMPORTANT: After you change the local engine ID, the existing SNMPv3 users become invalid, and you must re-create the SNMPv3 users. For more information about engine ID, see "Enabling SNMP agent".
5. Configuring the 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 (usually the NMS) of the SNMP traps. The SNMP agent sends traps to inform the NMS of important events, such as a reboot. By default, an agent is allowed to send SNMP traps to the NMS.
6. Displaying SNMP packet statistics	Optional.

Enabling SNMP agent

1. Select **Device** > **SNMP** from the navigation tree.
   The SNMP configuration page appears.

Figure 105 Setup tab



2. Configure SNMP settings on the upper part of the page as described in Table 33.
3. Click **Apply**.

Table 33 Configuration items

Item	Description
SNMP	Specify to enable or disable SNMP agent.
Local Engine ID	Configure the local engine ID. Validity of a user 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.

Item	Description
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.

Configuring an SNMP view

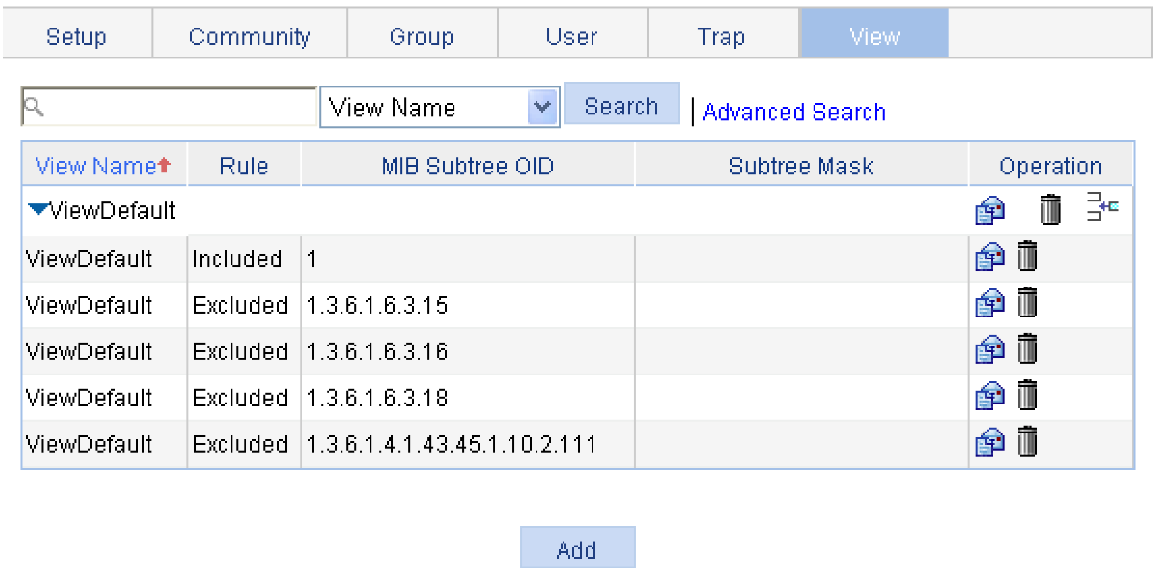
Perform the tasks in this section to configure an SNMP view.

Creating an SNMP view

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **View** tab.

   The **View** tab appears.

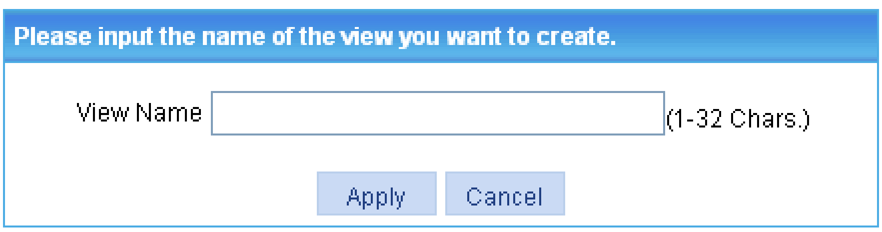
Figure 106 View tab



3. Click **Add**.

   The **Add View** window appears.

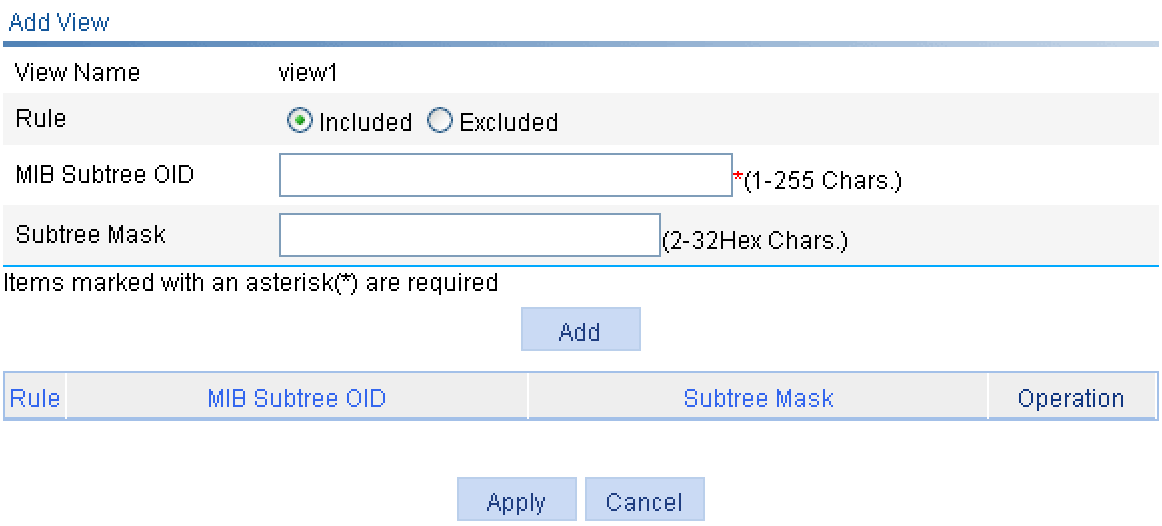
Figure 107 Creating an SNMP view (1)



4. Type the view name.
5. Click **Apply**.

   The page in Figure 108 appears.

Figure 108 Creating an SNMP view (2)



6. Configure the parameters as described in Table 34.
7. Click **Add** to add the rule into the list box at the lower part of the page.
8. Repeat steps 6 and 7 to add more rules for the SNMP view.
9. Click **Apply**.

   To cancel the view, click **Cancel**.

Table 34 Configuration items

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, a hexadecimal string. Its length must be an even number in the range of 2 to 32. If no subtree mask is specified, the default subtree mask (all Fs) will be used for mask-OID matching.

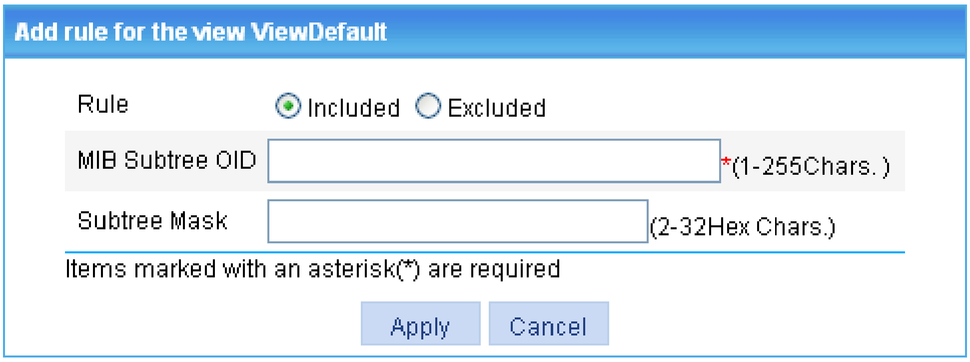
Adding rules to an SNMP view

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **View** tab.

   The page in Figure 106 appears.
3. Click the  icon of the target view.

The **Add rule for the view ViewDefault** window appears.

Figure 109 Adding rules to an SNMP view



4. Configure the parameters as described in Table 34.
5. Click **Apply**.

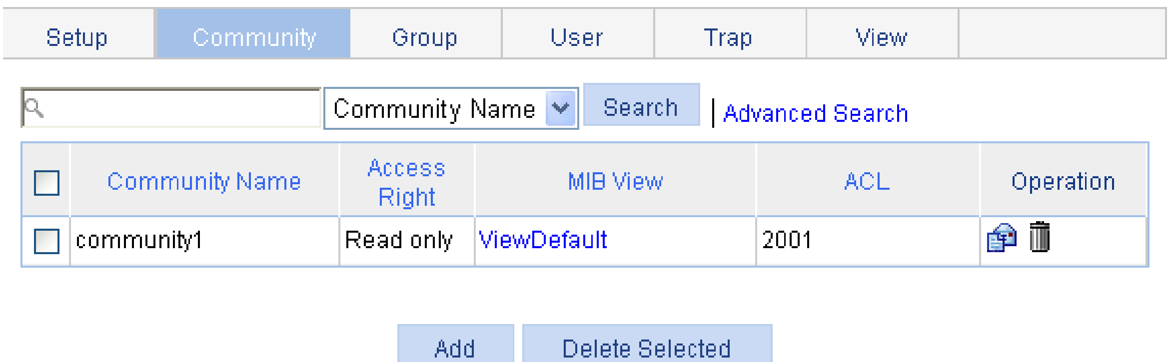
To modify a view, click the icon for the view on the **View** tab (see Figure 106).

Configuring an SNMP community

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **Community** tab.

   The **Community** tab appears.

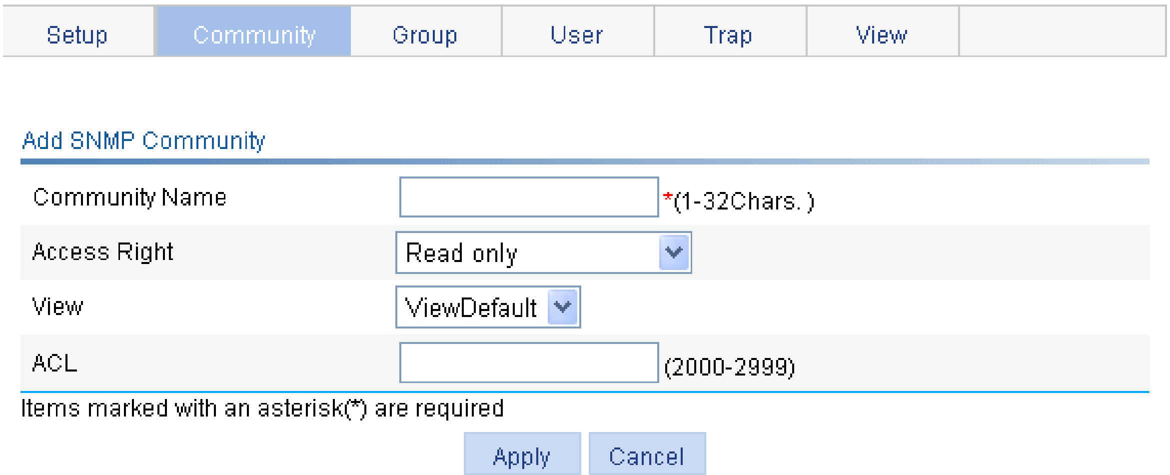
Figure 110 Configuring an SNMP community



3. Click **Add**.

   The **Add SNMP Community** page appears.

Figure 111 Creating an SNMP Community



4. Configure the SNMP community as described in Table 35.
5. Click **Apply**.

Table 35 Configuration items

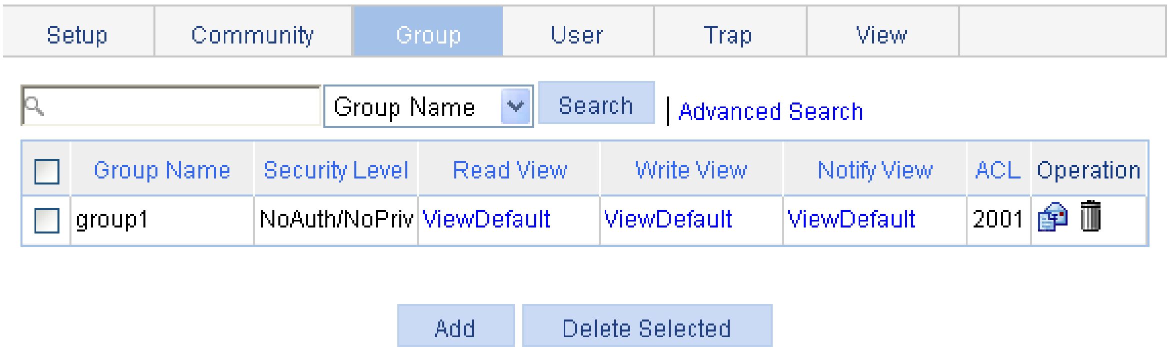
Item	Description
Community Name	Set the SNMP community name.
Access Right	Configure SNMP NMS access right: • **Read only**—The NMS can perform read-only operations to the MIB objects when it uses this community name to access the agent. • **Read and write**—The NMS can perform both read and write operations 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.

Configuring an SNMP group

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **Group** tab.

   The **Group** tab appears.

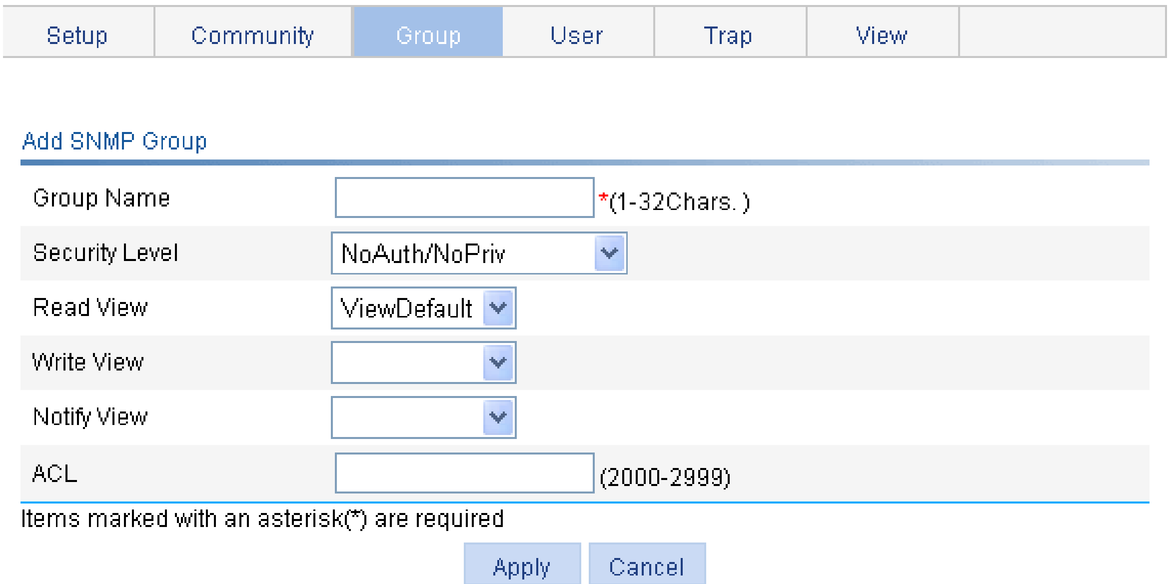
Figure 112 Group tab



3. Click **Add**.

   The **Add SNMP Group** page appears.

Figure 113 Creating an SNMP group



4. Configure SNMP group as described in Table 36.
5. Click **Apply**.

Table 36 Configuration items

Item	Description
Group Name	Set the SNMP group name.
Security Level	Select the security level for the SNMP group: • **NoAuth/NoPriv**—No authentication no privacy. • **Auth/NoPriv**—Authentication without privacy. • **Auth/Priv**—Authentication and privacy. IMPORTANT: For an existing SNMP group, its security level cannot be modified.
Read View	Select the read view of the SNMP group.

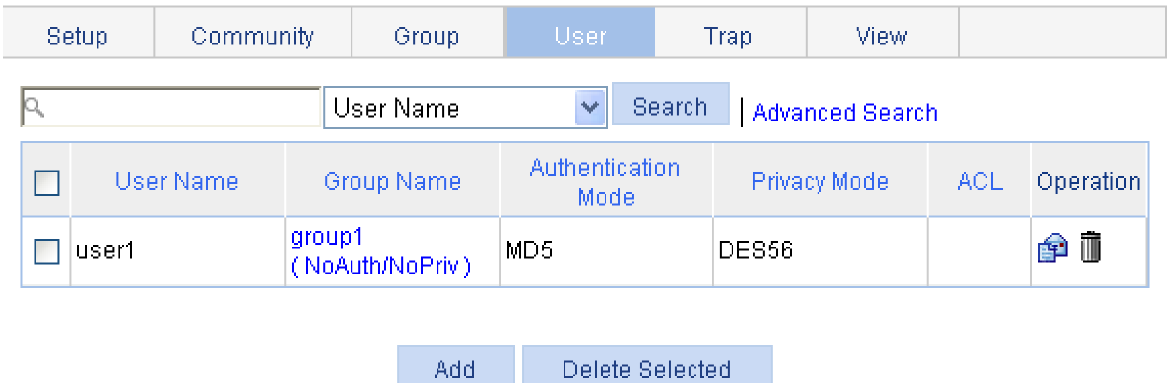
Item	Description
Write View	Select the write view of the SNMP group. If no write view is configured, the NMS cannot perform the write operations to all MIB objects on the device.
Notify View	Select the notify view of the SNMP group, that is, the view that can send trap messages. If no notify view is configured, the agent does not send traps to the NMS.
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.

Configuring an SNMP user

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **User** tab.

   The **User** tab appears.

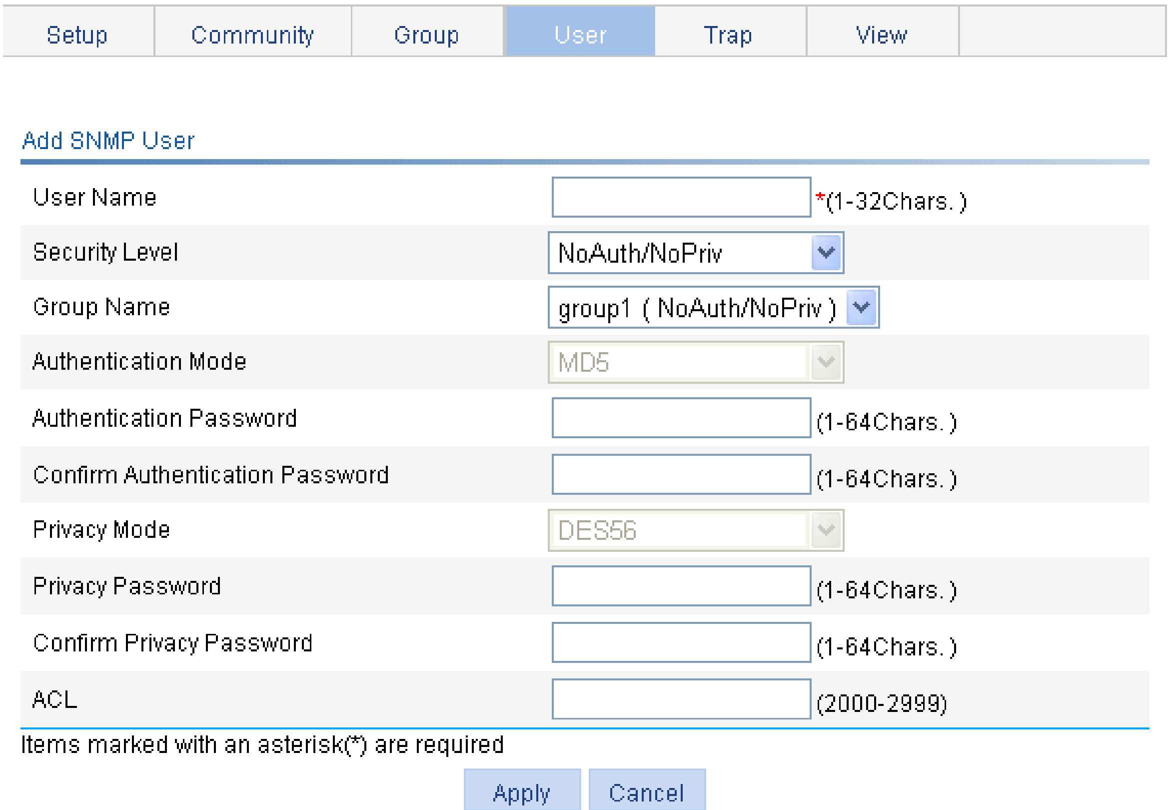
Figure 114 User tab



3. Click **Add**.

   The **Add SNMP User** page appears.

Figure 115 Creating an SNMP user



4. Configure the SNMP user as described in Table 37.
5. Click **Apply**.

Table 37 Configuration items

Item	Description
User Name	Set the SNMP user name.
Security Level	Select the security level for the SNMP group. 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

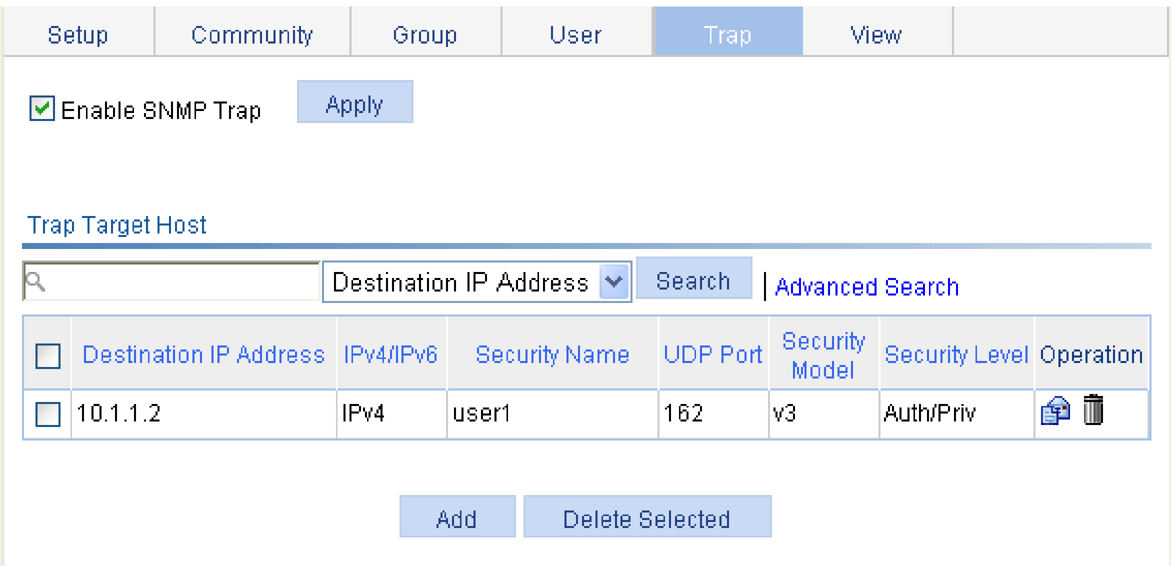
Item	Description
	Auth/Priv.
Confirm Authentication Password	Confirm authentication password must be the same with the authentication password.
Privacy Mode	Select a privacy mode (including DES56, AES128, and 3DES) when the security level is Auth/Priv.
Privacy Password	Set the privacy password when the security level is Auth/Priv.
Confirm Privacy Password	Confirm privacy password must be the same with the 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.

Configuring the SNMP trap function

1. Select **Device** > **SNMP** from the navigation tree.
2. Click the **Trap** tab.

   The **Trap** tab appears.

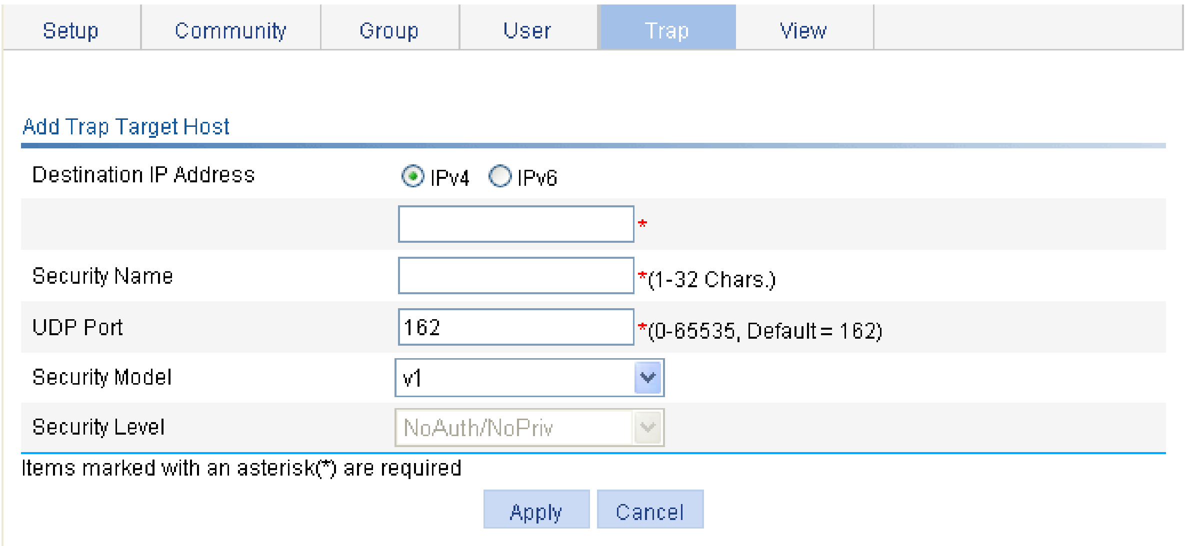
Figure 116 Trap tab



3. Select **Enable SNMP Trap**.
4. Click **Apply** to enable the SNMP trap function.
5. Click **Add**.

   The page for adding a target host of SNMP traps appears.

Figure 117 Adding a target host of SNMP traps



6. Configure the settings for the target host as described in Table 38.
7. Click **Apply**.

Table 38 Configuration items

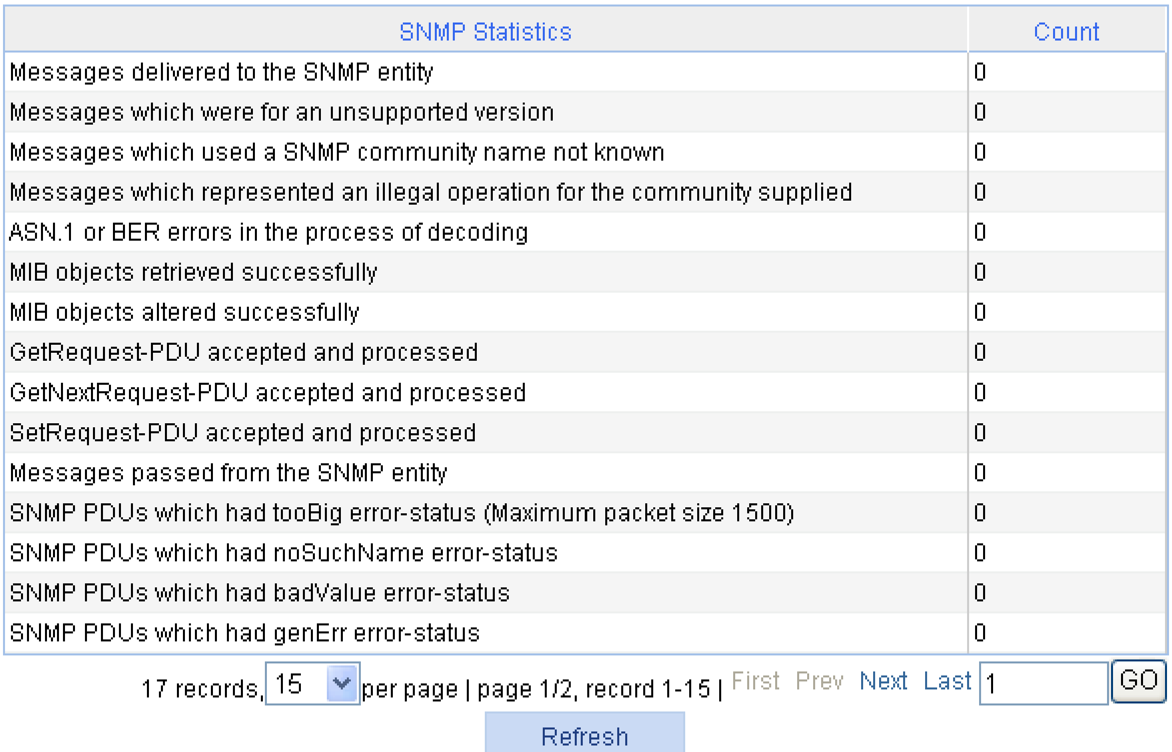
Item	Description
Destination IP Address	Select the **IPv4** or **IPv6** option, and enter the specific type of destination IP address.
Security Name	Set the security name, which can be an SNMPv1 community name, an SNMPv2c community name, or an SNMPv3 user name.
UDP Port	Set UDP port number. IMPORTANT: Default port number is 162, which is the SNMP-specified port used for receiving traps on the NMS. Generally (such as using iMC or MIB Browser as the NMS), you can use the default port number. To change this parameter to another value, you need to make sure that the configuration is the same with that on the NMS.
Security Model	Select the security model, that is, the SNMP version. Make sure 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.

Displaying SNMP packet statistics

Select **Device** > **SNMP** from the navigation tree.

The page for displaying SNMP packet statistics appears.

Figure 118 SNMP Statistics



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

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

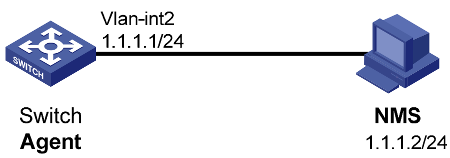
Refresh

SNMPv1/v2c configuration example

Network requirements

As shown in Figure 119, the NMS at 1.1.1.2/24 uses SNMPv1 or SNMPv2c to manage the switch (agent) at 1.1.1.1/24, and the switch automatically sends traps to report events to the NMS.

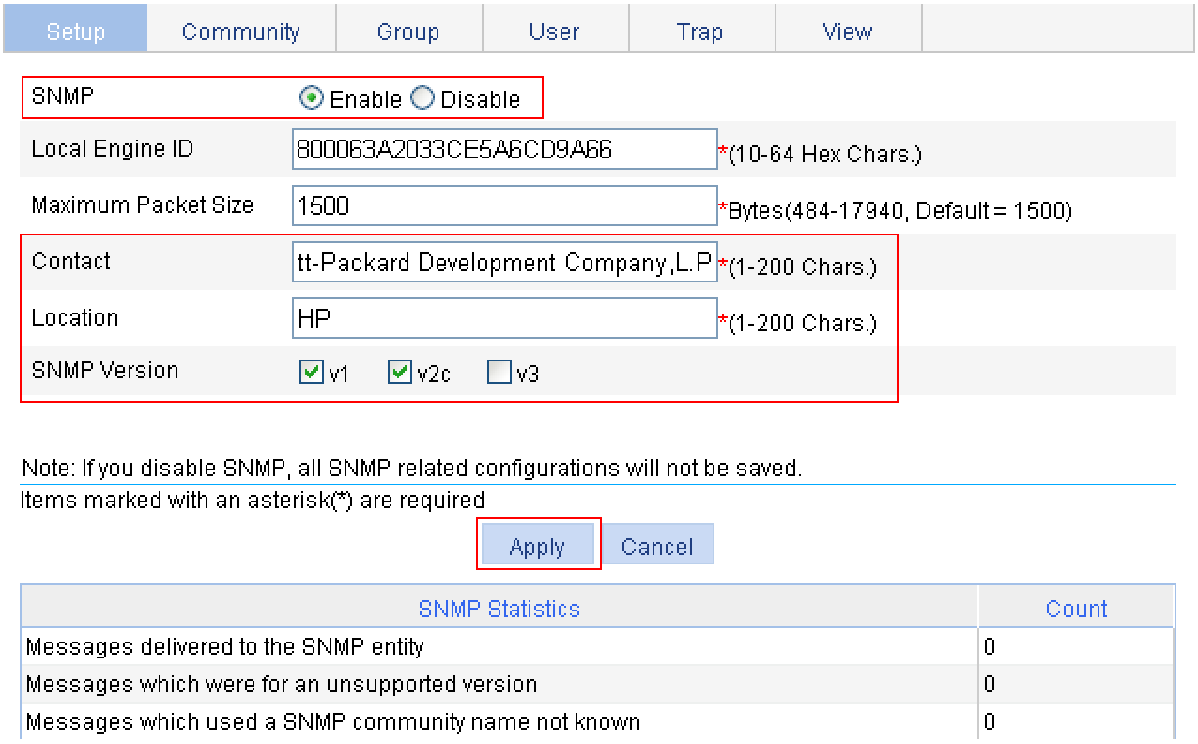
Figure 119 Network diagram



Configuring the agent

1. Enable SNMP:
    a. Select **Device** > **SNMP** from the navigation tree.
       The SNMP configuration page appears.

Figure 120 Configuring the SNMP agent



b. Select the **Enable** option, and select the **v1** and **v2** options.

c. Set **Hewlett-Packard Development Company,L.P.** as the contact person, and **HP** as the physical location.

d. Click **Apply**.

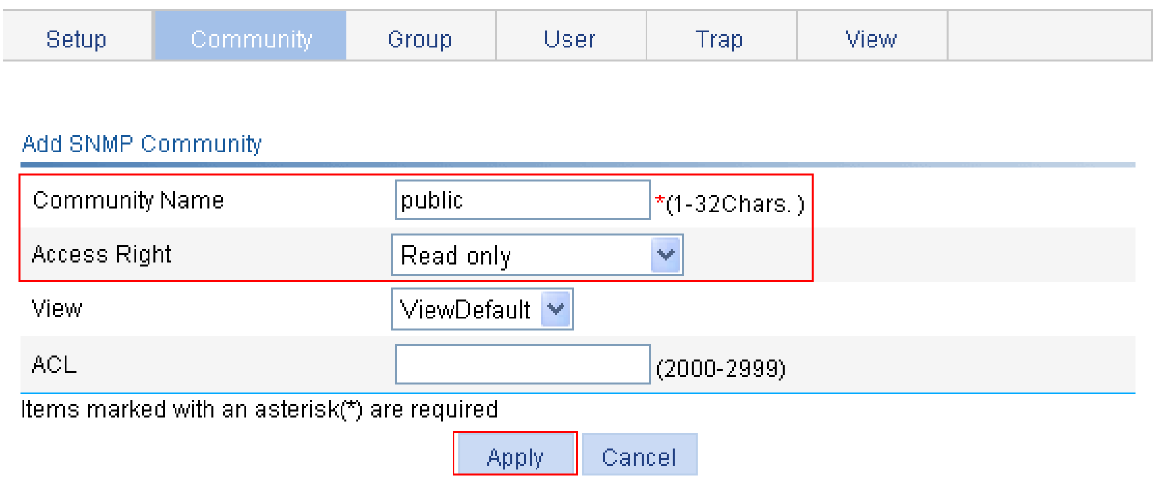
2. Configure a read-only community:

   a. Click the **Community** tab.

   b. Click **Add**.

   The **Add SNMP Community** page appears.

Figure 121 Configuring an SNMP read-only community

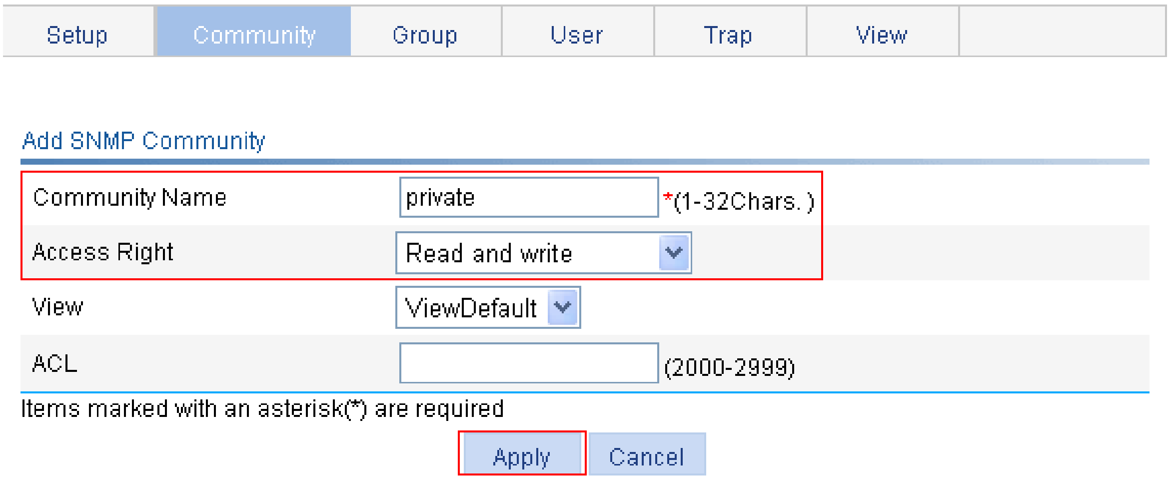


c. Enter **public** in the **Community Name** field, and select **Read only** from the **Access Right** list.

d. Click **Apply**.

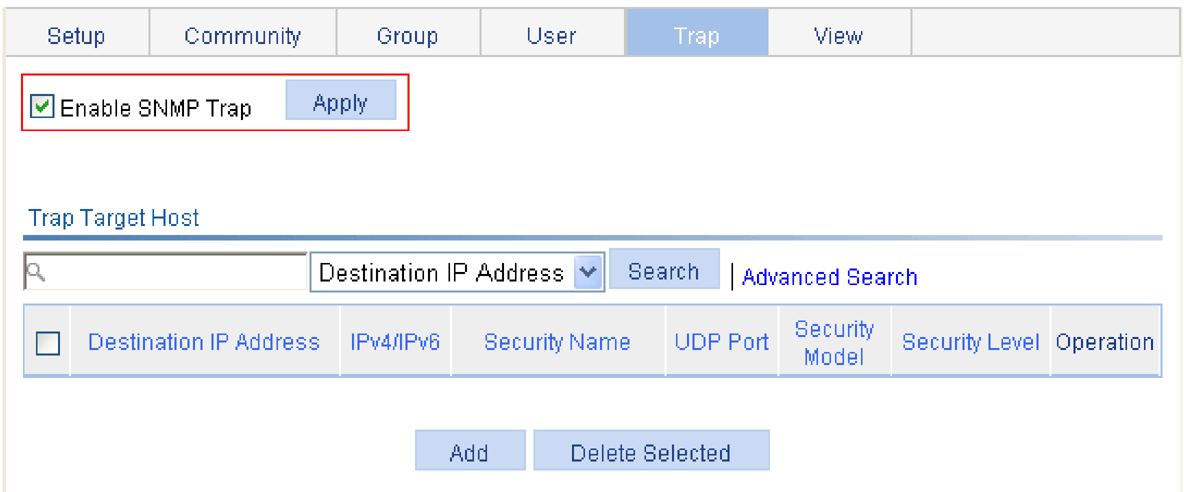
3. Configure a read and write community:
   a. Click **Add** on the **Community** tab page.
      The **Add SNMP Community** page appears.

Figure 122 Configuring an SNMP read and write community



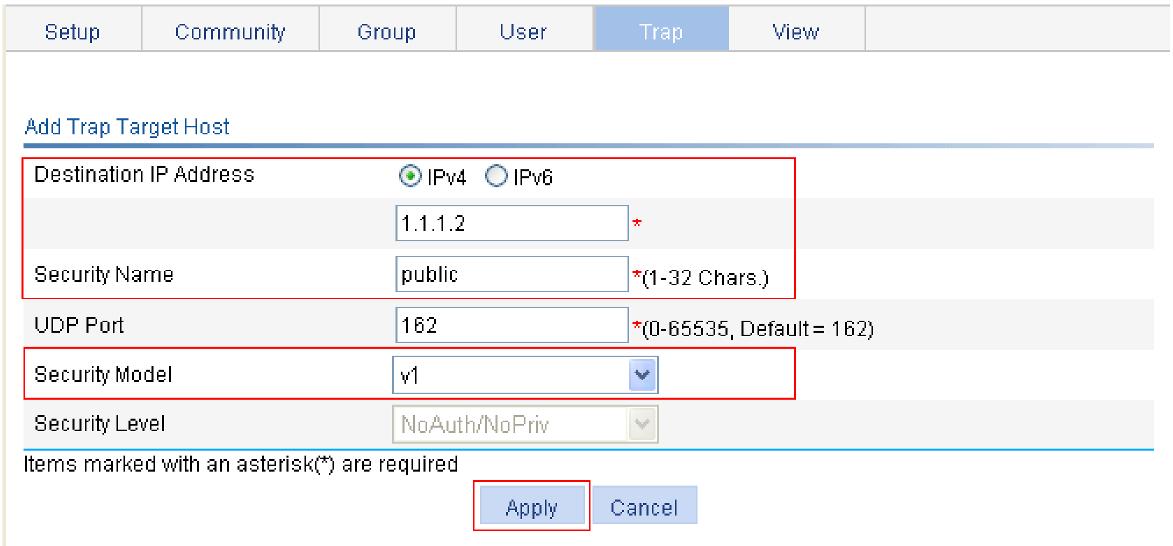
   b. Enter **private** in the **Community Name** field, and select **Read and write** from the **Access Right** list.
   c. Click **Apply**.
4. Enable SNMP traps:
   a. Click the **Trap** tab.
      The **Trap** tab page appears.

Figure 123 Enabling SNMP traps



   b. Select the box of **Enable SNMP Trap**.
   c. Click **Apply**.
5. Configure a target host SNMP traps:
   a. Click **Add** on the **Trap** tab page.
      The page for adding a target host of SNMP traps appears.

Figure 124 Adding a trap target host



b. Type **1.1.1.2** in the following field, type **public** in the **Security Name** field, and select **v1** from the **Security Model** list.
c. Click **Apply**.

Configuring the NMS

To avoid communication failures, make sure the NMS use the same SNMP settings as the agent.

1. Configure the SNMP version for the NMS as v1 or v2c.
2. Create a read-only community and name it **public**.
3. Create a read and write community and name it **private**.

For how to configure the NMS, see the NMS manual.

Verifying the configuration

- After the above configuration, an SNMP connection is established between the NMS and the agent. The NMS can get and configure the values of some parameters on the agent through MIB nodes.
- Disable or enable an idle interface on the agent, and you can see the interface state change traps on the NMS.

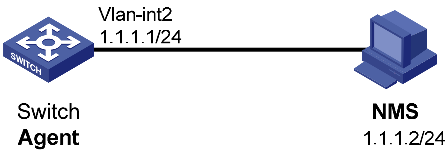
SNMPv3 configuration example

Network requirements

As shown in Figure 125, the NMS (1.1.1.2/24) uses SNMPv3 to monitor and manage the interface status of the AP (the agent) at 1.1.1.1/24, and the AP automatically sends traps to report events to the NMS.

The NMS and the agent perform authentication when they set up an SNMP session. The authentication algorithm is MD5 and the authentication key is **authkey**. The NMS and the AP also encrypt the SNMP packets between them by using the DES56 algorithm and the privacy key **prikey**.

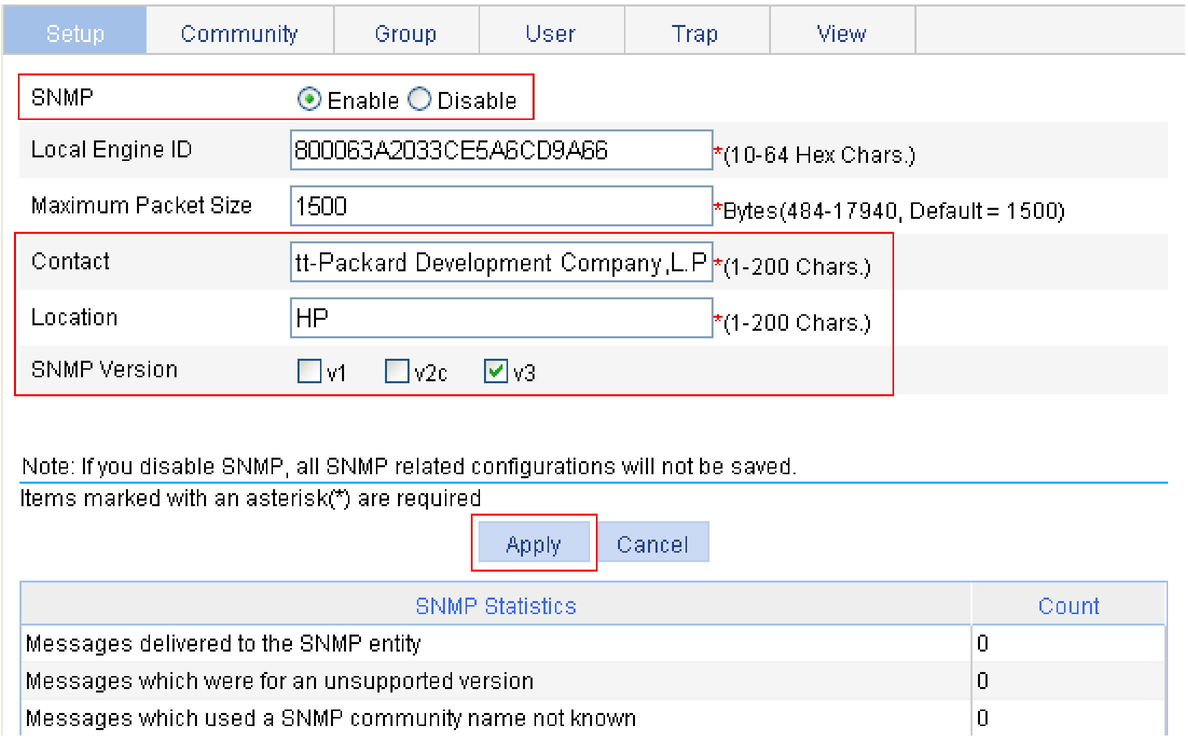
Figure 125 Network diagram



Configuring the agent

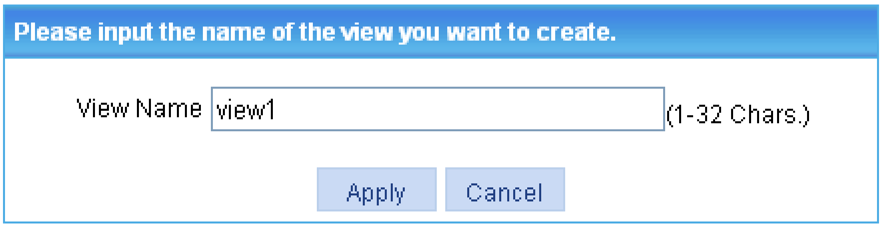
1. Enable SNMP agent:
   a. Select **Device** > **SNMP** from the navigation tree.
      The SNMP configuration page appears.

Figure 126 Configuring the SNMP agent



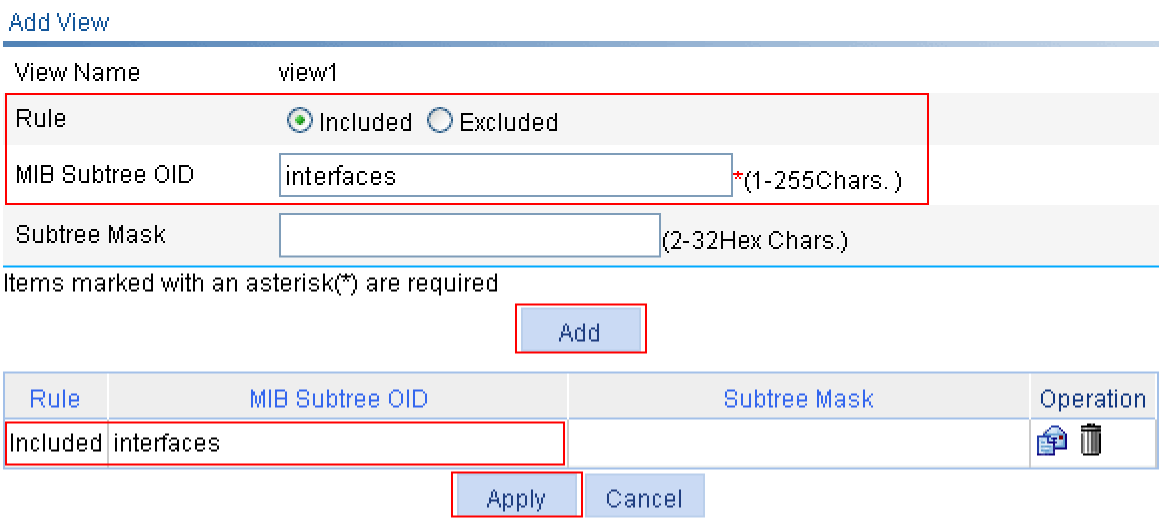
   b. Select the **Enable** option, and select the **v3** option.
   c. Set **Hewlett-Packard Development Company,L.P.** as the contact person, and **HP** as the physical location.
   d. Click **Apply**.
2. Configure an SNMP view:
   a. Click the **View** tab.
   b. Click **Add**.
      The page for creating an SNMP view appears.

Figure 127 Creating an SNMP view (1)



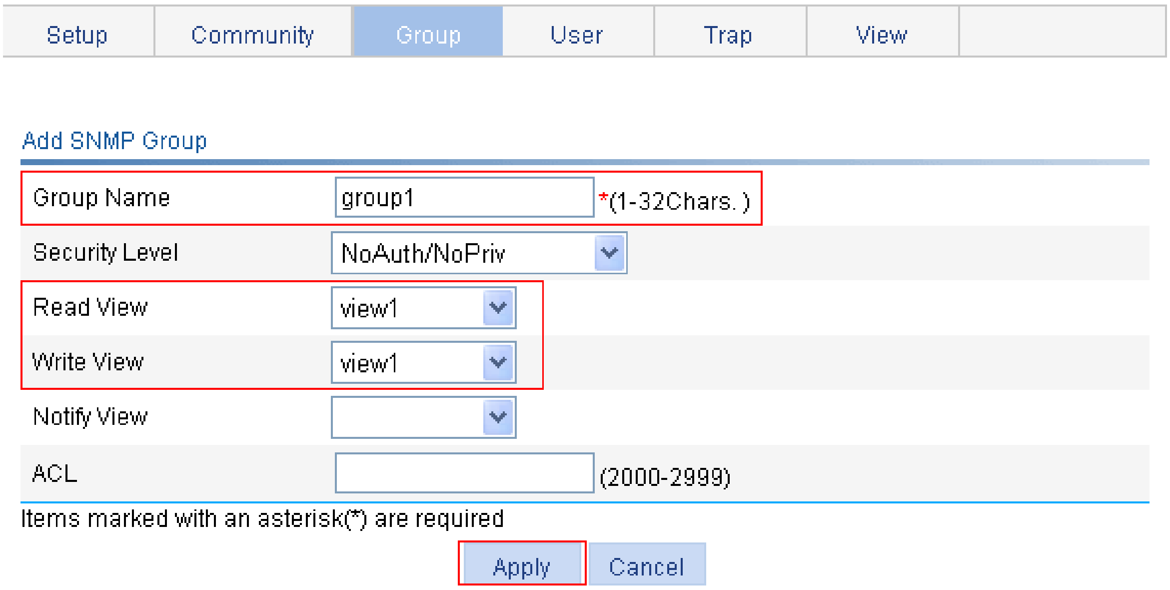
c. Type **view1** in the **View Name** field.
d. Click **Apply**.
   The page in Figure 128 appears.
e. Select the **Included** option, type the MIB subtree OID **interfaces**, and click **Add**.
f. Click **Apply**.
   A configuration progress dialog box appears.
g. Click **Close** after the configuration process is complete.

Figure 128 Creating an SNMP view (2)



3. Configure an SNMP group:
   a. Click the **Group** tab.
   b. Click **Add**.
      The page in Figure 129 appears.
   c. Type **group1** in the **Group Name** field, select **view1** from the **Read View** list, select **view1** from the **Write View** list.
   d. Click **Apply**.

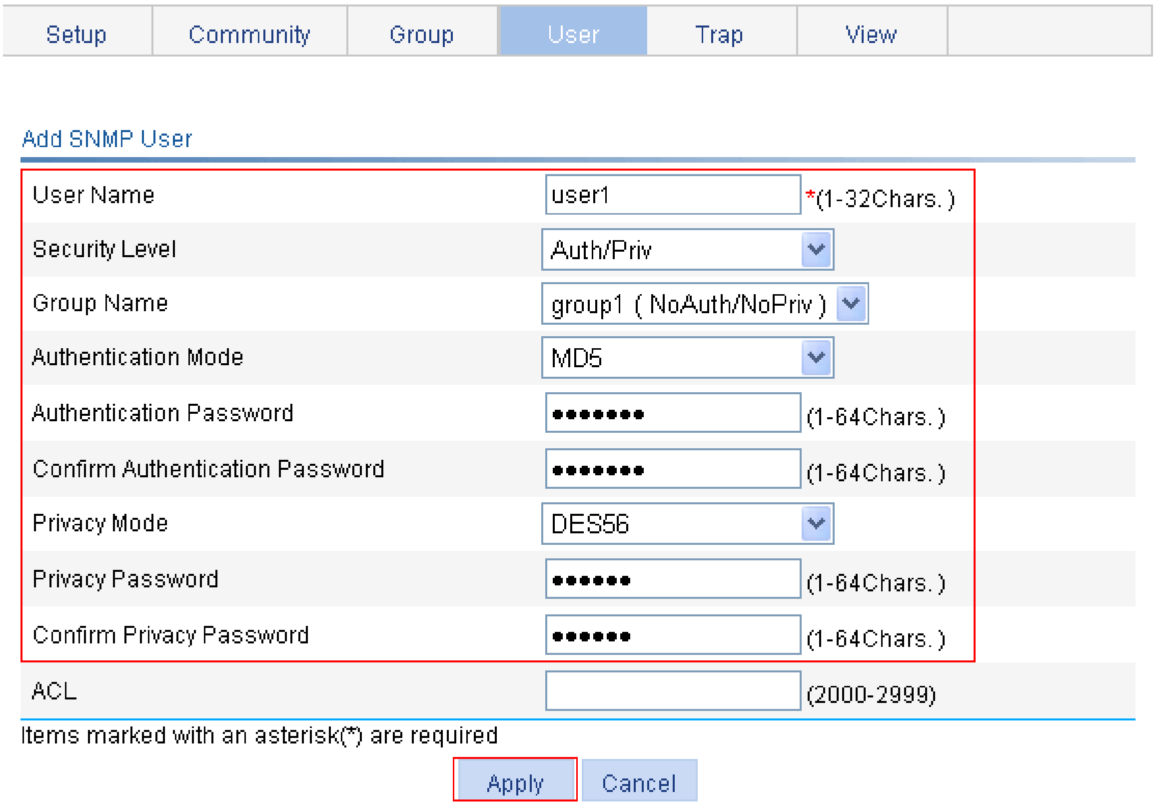
Figure 129 Creating an SNMP group



4. Configure an SNMP user:
   a. Click the **User** tab.
   b. Click **Add**.

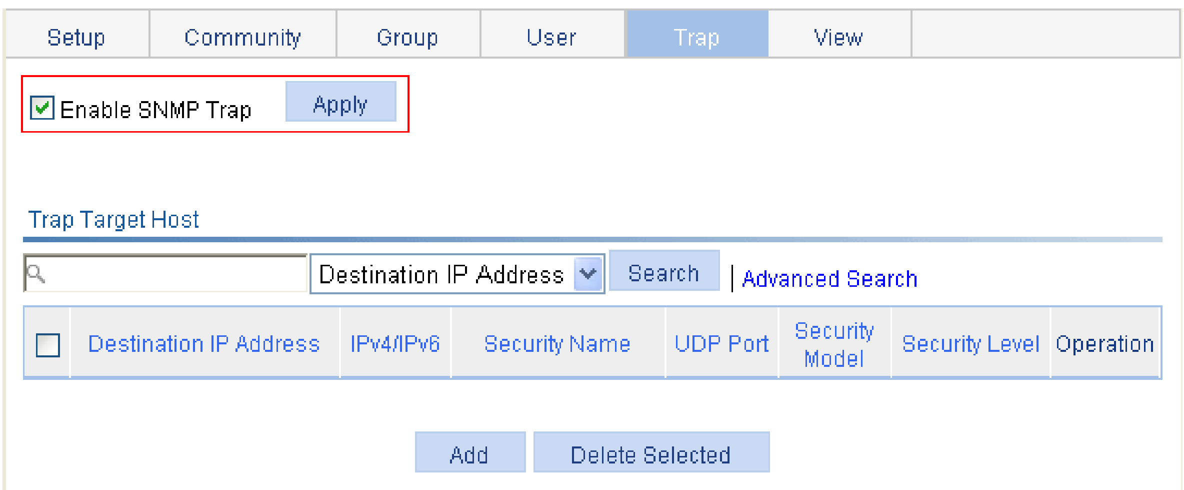
      The page in Figure 130 appears.
   c. Type **user1** in the **User Name** field, select **Auth/Priv** from the **Security Level** list, select **group1** from the **Group Name** list, select **MD5** from the **Authentication Mode** list, type **authkey** in the **Authentication Password** and **Confirm Authentication Password** fields, select **DES56** from the **Privacy Mode** list, and type **prikey** in the **Privacy Password** and **Confirm Privacy Password** fields.
   d. Click **Apply**.

Figure 130 Creating an SNMP user



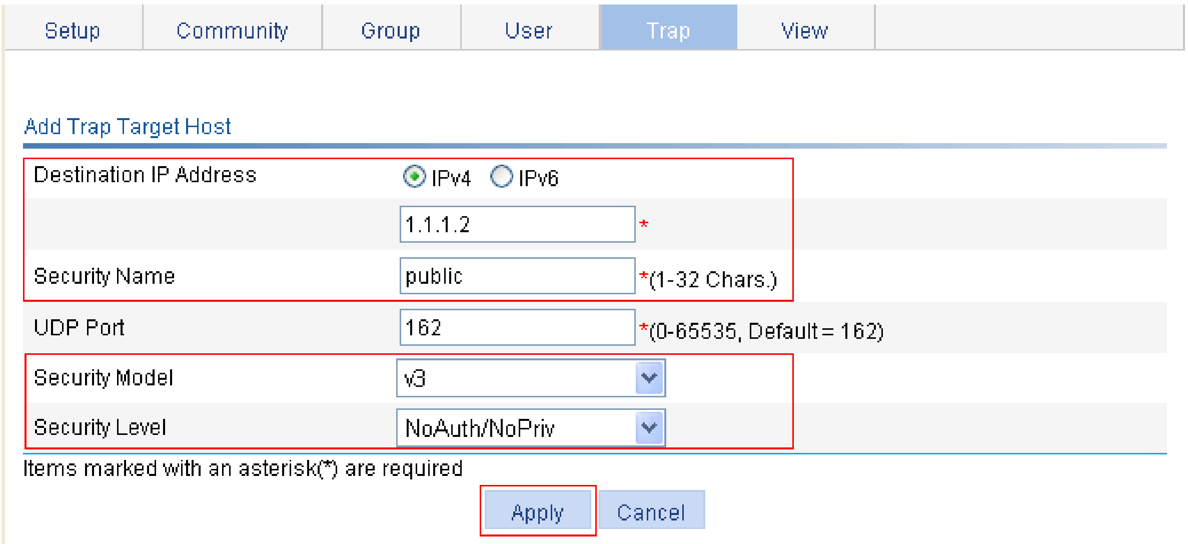
5. Enable SNMP traps:
   a. Click the **Trap** tab.
      The **Trap** tab page appears.

Figure 131 Enabling SNMP traps



   b. Select the box of **Enable SNMP Trap**.
   c. Click **Apply**.
6. Configure a target host SNMP traps:
   a. Click **Add** on the **Trap** tab page.
      The page for adding a target host of SNMP traps appears.

Figure 132 Adding a trap target host



b. Type **1.1.1.2** in the following field, type **user1** in the **Security Name** field, select **v3** from the **Security Model** list, and select **Auth/Priv** from the **Security Level** list.

c. Click **Apply**.

Configuring the NMS

To avoid communication failures, make sure the NMS use the same SNMP settings as the agent.

1. Specify the SNMP version for the NMS as v3.
2. Create an SNMP user **user1**.
3. Enable both authentication and privacy functions
4. Use MD5 for authentication and DES56 for encryption.
5. Set the authentication key to **authkey** and the privacy key to **prikey**.

For information about configuring the NMS, see the NMS manual.

Verifying the configuration

- 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.
- Disable or enable an idle interface on the agent, and you can see the interface state change traps on the NMS.

Displaying interface statistics

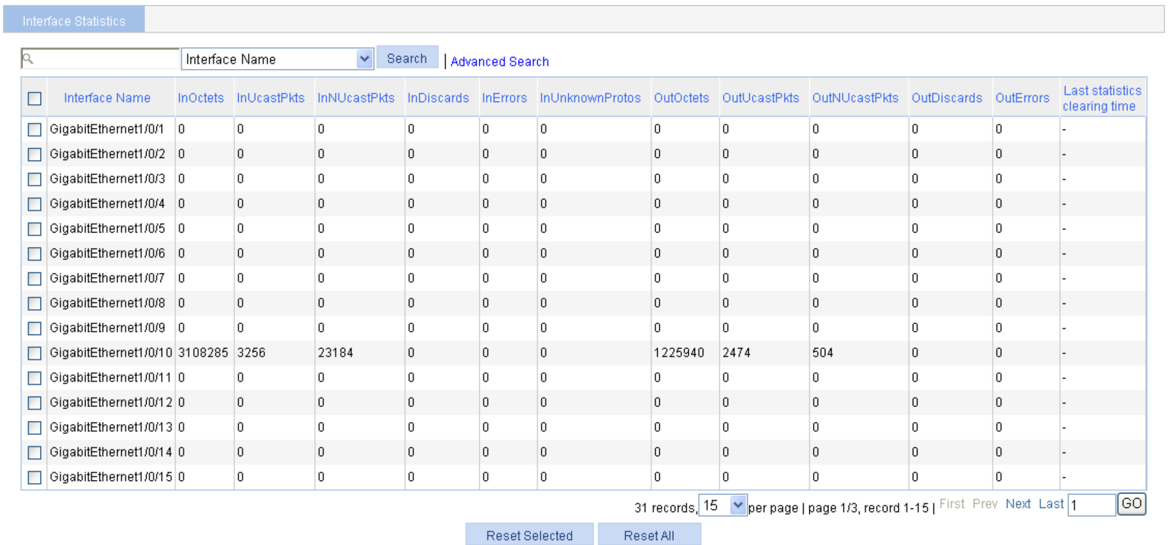
Overview

The interface statistics module displays statistics 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 133.

Figure 133 Interface statistics display page


Interface Statistics

Interface Name | Search | Advanced Search

	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	3108285	3256	23184	0	0	0	1225940	2474	504	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	0	0	0	0	0	0	0	0	0	0	0	-

31 records, 15 per page | page 1/3, record 1-15 | First Prev Next Last 1 GO

Reset Selected Reset All

Table 39 Details about the interface statistics

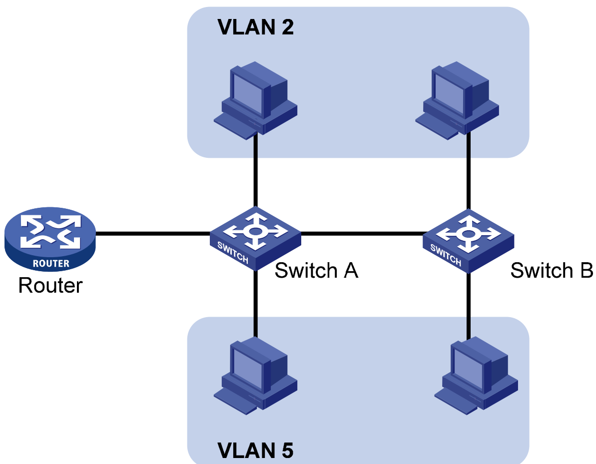
Field	Description
InOctets	Total octets of all packets received on the interface
InUcastPkts	Number of received unicast packets
InNUcastPkts	Number of received non-unicast packets
InDiscards	Number of valid packets discarded in the inbound direction
InErrors	Number of received invalid packets
InUnknownProtos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

Configuring VLANs

VLAN overview

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 to break a LAN down into separate VLANs. 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 134.

Figure 134 A VLAN diagram



A VLAN is 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 assigned to the same VLAN, regardless of their physical locations.

VLAN technology delivers the following benefits:

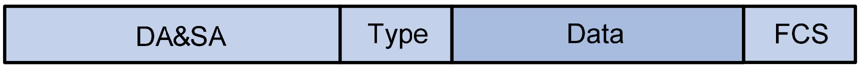
- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
- 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.

VLAN fundamentals

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 Institute of Electrical and Electronics Engineers (IEEE) 802.1Q-1999.

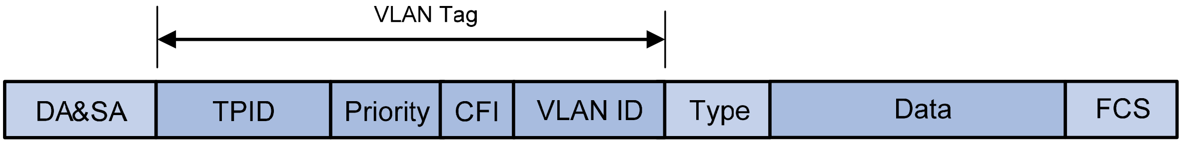
In the header of a traditional Ethernet data frame, the field after the destination MAC address and the source MAC address is the Type field indicating the upper layer protocol type, as shown in Figure 135.

Figure 135 Traditional Ethernet frame format



IEEE 802.1Q inserts a four-byte VLAN tag after the DA&SA field, as shown in Figure 136.

Figure 136 Position and format of VLAN tag



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

- The 16-bit TPID field indicates whether the frame is VLAN-tagged and is 0x8100 by default.
- 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 standard format when packets are transmitted across different media. A value of 0 indicates that MAC addresses are encapsulated in the standard format. The value of 1 indicates that MAC addresses are encapsulated in a non-standard format. The value of the field is 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, a VLAN ID actually ranges from 1 to 4094.

A network device handles an incoming frame depending on whether the frame is VLAN tagged and the value of the VLAN tag, if any.

NOTE:

- The Ethernet II encapsulation format is used in this section. In addition to the Ethernet II encapsulation format, Ethernet also supports other encapsulation formats, including 802.2 LLC, 802.2 SNAP, and 802.3 raw. The VLAN tag fields are added to frames encapsulated in these formats for VLAN identification.
- When a frame carrying multiple VLAN tags passes through, the device processes the frame according to its outer VLAN tag, and transmits the inner tags as payload.

VLAN types

You can implement VLANs based on the following criteria:

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

The web interface is available only for port-based VLANs, and this chapter introduces only port-based VLANs.

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

You can configure the link type of a port as access, trunk, or hybrid. The link types use the following VLAN tag handling methods:

- An access port belongs to only one VLAN and sends traffic untagged. It is usually used to connect a terminal device unable to identify VLAN tagged-packets or when separating different VLAN members is unnecessary.
- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic from the port VLAN ID (PVID), traffic sent through a trunk port will be VLAN tagged. Usually, ports that connect network devices are configured as trunk ports.
- A hybrid port allows traffic of some VLANs to pass through untagged and traffic of some other VLANs to pass through tagged. Hybrid ports can interconnect network devices or connect to terminals.

PVID

By default, VLAN 1 is the PVID for all ports. You can change the PVID for a port as required.

Use the following guidelines when you configure the PVID on a port:

- An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port.
- A trunk or hybrid port can join multiple VLANs, and you can configure a PVID for the port.
- You can use a nonexistent VLAN as the PVID for a hybrid or trunk port but not for an access port. After you delete the VLAN that an access port resides in, the PVID of the port changes to VLAN 1. Deleting the VLAN specified as the PVID of a trunk or hybrid port, however, does not affect the PVID setting on the port.

NOTE:

- Do not set the voice VLAN as the PVID of a port in automatic voice VLAN assignment mode. For information about voice VLAN, see "Configuring a voice VLAN."
- HP recommends that you set the same PVID for local and remote ports.
- Make sure that a port permits its PVID. Otherwise, when the port receives frames tagged with the PVID or untagged frames, the port drops these frames.

Frame handling methods

The following table shows how ports of different link types handle frames:

Actions	Access	Trunk	Hybrid
In the inbound direction for an untagged frame	Tags the frame with the PVID tag.	Checks whether the PVID is permitted on the port: • If yes, tags the frame with the PVID tag. • If not, drops the frame.	

Actions	Access	Trunk	Hybrid
In the inbound direction for a tagged frame	• Receives the frame if its VLAN ID is the same as the PVID. • Drops the frame if its VLAN ID is different from the PVID.	• Receives the frame if its VLAN is permitted on the port. • Drops the frame if its VLAN is not permitted on the port.	
In the outbound direction	Removes the VLAN tag and sends the frame.	• Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID. • Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.	Sends the frame if its VLAN is permitted on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration with the **port hybrid vlan** command. This is true of the PVID.

Recommended VLAN configuration procedures

Assigning an access port to a VLAN

Step	Remarks	
1. Creating VLANs	(Required.) Create one or multiple VLANs.	
2. Configuring the link type of a port	(Optional.) Configure the link type of the port as access. By default, the link type of a port is access.	
3. Setting the PVID for a port	Configure the PVID of the access port.	(Required.) An access port has only one untagged VLAN and the untagged VLAN is its PVID. The three operations produce the same result, and the latest operation takes effect. By default, an access port is an untagged member of VLAN 1.
4. Configuring the access ports as untagged members of a VLAN a. Selecting VLANs Specify the range of VLANs available for selection during related operations. Configure a subset of all existing VLANs. This step is required before you perform operations on the **Detail**, Modify VLAN, and **Modify Port** tabs. b. Modifying a VLAN Configure the access ports as untagged members of the specified VLAN.	N/A	
5. Modifying ports	Configure the untagged VLAN of the port.	

Assigning a trunk port to a VLAN

<table>
<tr><th>Step</th><th colspan="2">Remarks</th></tr>
<tr><td>1. Creating VLANs</td><td colspan="2">(Required.)
Create one or multiple VLANs.</td></tr>
<tr><td>2. Configuring the link type of a port</td><td colspan="2">(Optional.)
Configure the link type of the port as trunk.
By default, the link type of a port is access.</td></tr>
<tr><td>3. Setting the PVID for a port</td><td>Configure the PVID of the trunk port.</td><td rowspan="3">(Required.)
A trunk port has only one untagged VLAN and the untagged VLAN is its PVID. The three operations produce the same result, and the latest operation takes effect.
By default, the untagged VLAN of a trunk port is VLAN 1.
NOTE::
When you change the untagged VLAN (PVID) of a trunk port, the former untagged VLAN automatically becomes a tagged VLAN of the trunk port.</td></tr>
<tr><td>4. Configure the trunk port as an untagged member of the specified VLANs
a. Selecting VLANs
Specify the range of VLANs available for selection during related operations. Configure a subset of all existing VLANs. This step is required before you perform operations on the Detail, Modify VLAN, and Modify Port tabs.
b. Modifying a VLAN
Configure the trunk port as an untagged member of the specified VLANs.</td><td>N/A</td></tr>
<tr><td>5. Modifying ports</td><td>Configure the untagged VLAN of the trunk port.</td></tr>
<tr><td>6. Configure the trunk port as a tagged member of the specified VLANs
a. Selecting VLANs
Specify the range of VLANs available for selection during related operations. Configure a subset of all existing VLANs. This step is required before you perform operations on the Detail, Modify VLAN, and Modify Port tabs.
b. Modifying a VLAN
Configure the trunk port as a tagged member of the specified VLANs.</td><td>N/A</td><td rowspan="2">(Required.)
A trunk port can have multiple tagged VLANs. You can repeat these steps to configure multiple tagged VLANs for the trunk port.</td></tr>
<tr><td>7. Modifying ports</td><td>Configure the tagged VLAN of the trunk port.</td></tr>
</table>

Assigning a hybrid port to a VLAN

Step	Remarks
1. Creating VLANs	(Required.) Create one or multiple VLANs.

<table>
<tr><th>Step</th><th colspan="2">Remarks</th></tr>
<tr><td>2. Configuring the link type of a port</td><td colspan="2">(Optional.)
Configure the link type of the port as hybrid.
If you configure multiple untagged VLANs for a trunk port at the same time, the trunk port automatically becomes a hybrid port.
By default, the link type of a port is access.</td></tr>
<tr><td>3. Setting the PVID for a port</td><td colspan="2">(Optional.)
Configure the PVID of the hybrid port.
By default, the PVID of a hybrid port is VLAN 1.</td></tr>
<tr><td>4. Configure the hybrid port as an untagged member of the specified VLANs
a. Selecting VLANs
Specify the range of VLANs available for selection during related operations. Configure a subset of all existing VLANs. This step is required before you perform operations on the Detail, Modify VLAN, and Modify Port tabs.
b. Modifying a VLAN
Configure the hybrid port as an untagged member of the specified VLAN.</td><td>N/A</td><td rowspan="2">(Required.)
A hybrid port can have multiple untagged VLANs. Repeat these steps to configure multiple untagged VLANs for a hybrid port.
By default, the untagged VLAN of a hybrid port is VLAN 1.</td></tr>
<tr><td>5. Modifying ports</td><td>Configure the untagged VLAN of the hybrid port.</td></tr>
<tr><td>6. Configure the hybrid port as a tagged member of the specified VLAN
a. Selecting VLANs
Specify the range of VLANs available for selection during related operations. Configure a subset of all existing VLANs. This step is required before you perform operations on the Detail, Modify VLAN, and Modify Port tabs.
b. Modifying a VLAN
Configure the hybrid port as a tagged member of the specified VLAN.</td><td>N/A</td><td rowspan="2">(Required.)
A hybrid port can have multiple tagged VLANs. You can repeat these steps to configure multiple tagged VLANs for the hybrid port.</td></tr>
<tr><td>7. Modifying ports</td><td>Configure the tagged VLAN of the hybrid port.</td></tr>
</table>

Creating VLANs

1. Select **Network** > **VLAN** from the navigation tree.
2. Click **Create** to enter the page for creating VLANs.
3. Enter the VLAN IDs, a VLAN ID range, or both.
4. Click **Create**.

Figure 137 Creating VLANs

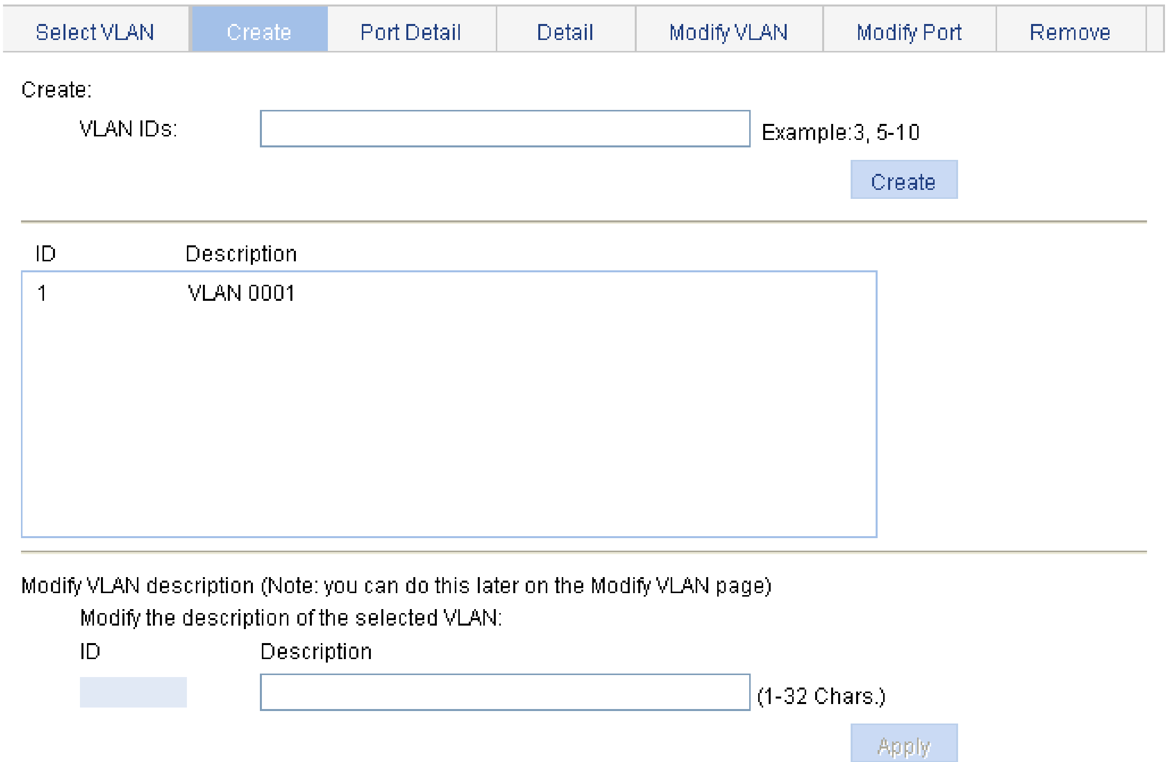


Table 40 Configuration items

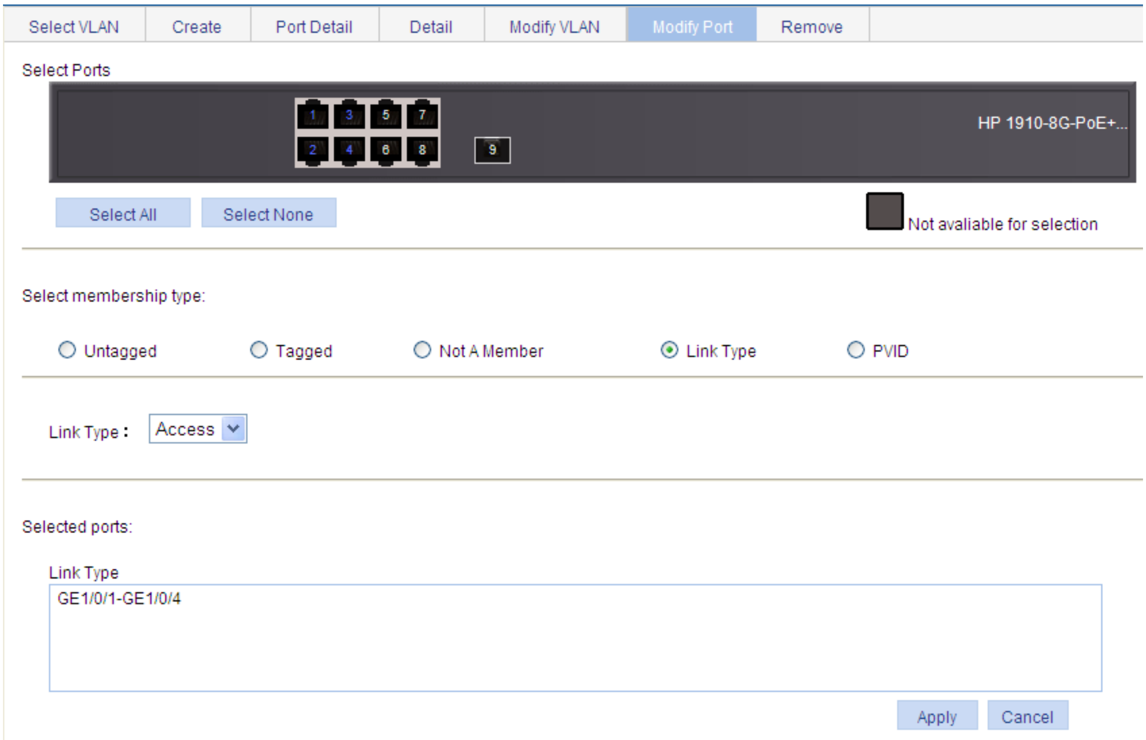
Item	Description
VLAN IDs	IDs of the VLANs to be created
Modify the description of the selected VLAN	• ID Select the ID of the VLAN whose description string is to be modified. Click the ID of the VLAN to be modified in the list in the middle of the page. • Description Set the description string of the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

Configuring the link type of a port

1. Select **Network** > **VLAN** from the navigation tree.
2. Click the **Modify Port** tab.
3. Select the port that you want to configure on the chassis front panel.
4. Select the **Link Type** option.
5. Set the link type, which can be access, hybrid, or trunk.
6. Click **Apply**.

   A progress dialog box appears.
7. Click **Close** on the progress dialog box when the dialog box prompts that the configuration succeeds.

Figure 138 Modifying ports



NOTE:

You can also configure the link type of a port on the **Setup** tab of **Device** > **Port Management**. For more information, see "Managing ports."

Setting the PVID for a port

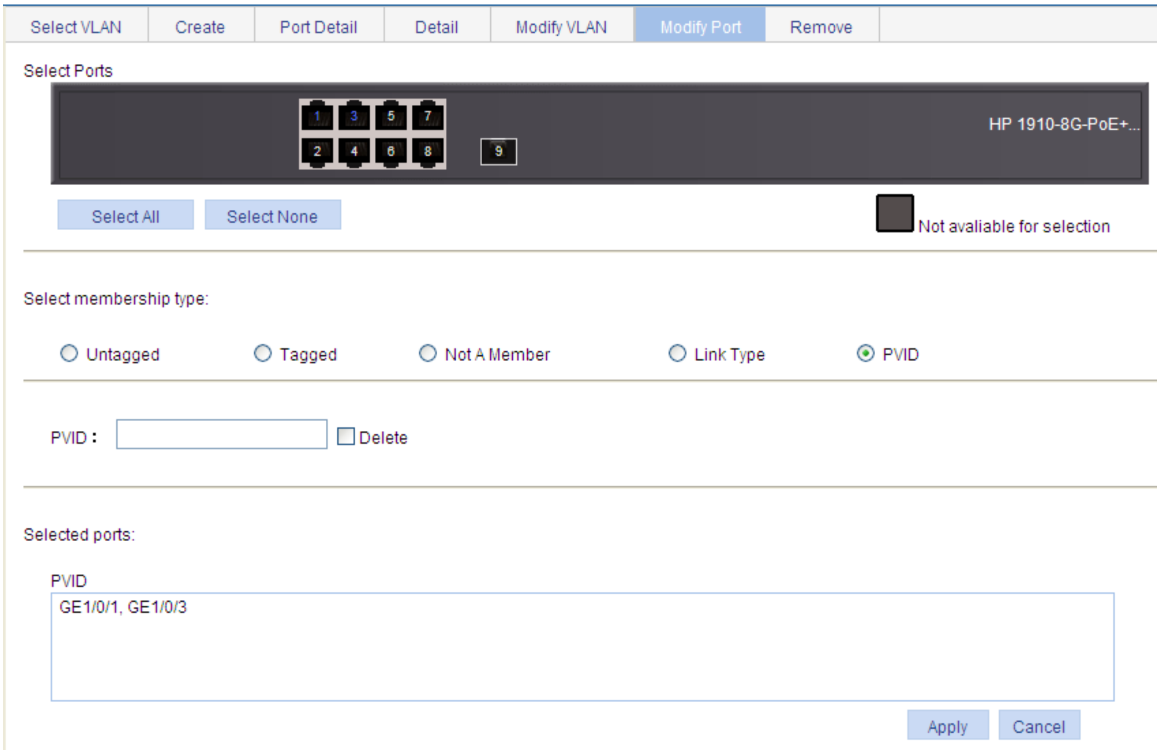
1. Select **Network** > **VLAN** from the navigation tree.
2. Click the **Modify Port** tab.
3. Select the port that you want to configure on the chassis front panel.
4. Select the **PVID** option.

   The option allows you to modify the PVID of the port.
5. Set a PVID for the port. By selecting the **Delete** box, you can restore the PVID of the port to the default, which is VLAN 1.

   The PVID of an access port must be an existing VLAN.
6. Click **Apply**.

   A progress dialog box appears.
7. Click **Close** on the progress dialog box when the dialog box prompts that the configuration succeeds.

Figure 139 Modifying the PVID for a port



NOTE:

You can also configure the PVID of a port on the **Setup** tab of **Device** > **Port Management**. For more information, see "Managing ports."

Selecting VLANs

1. Select **Network** > **VLAN** from the navigation tree.

   The **Select VLAN** tab is displayed by default for you to select VLANs.

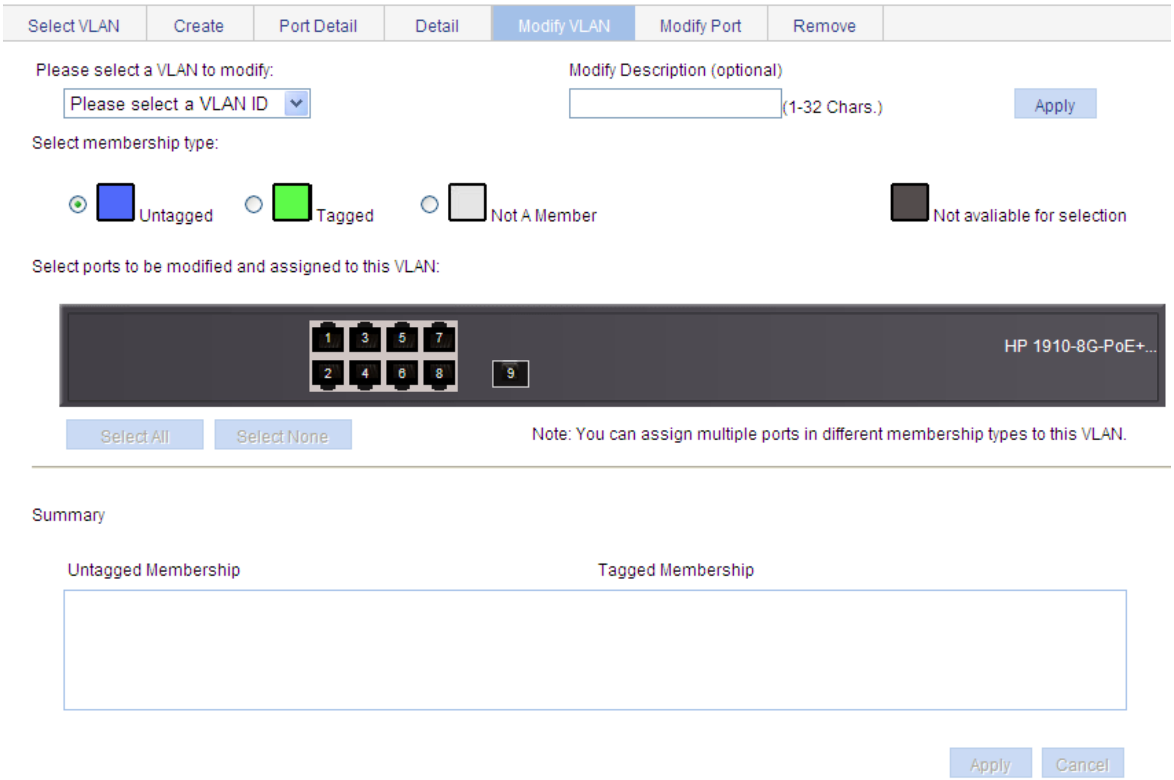
Figure 140 Selecting VLANs

2. Select the **Display all VLANs** option to display all VLANs or select the **Display a subnet of all configured VLANs** option to enter the VLAN IDs to be displayed.
3. Click **Select**.

Modifying a VLAN

1. Select **Network** > **VLAN** from the navigation tree.
2. Click **Modify VLAN** to enter the page for modifying a VLAN.

Figure 141 Modifying a VLAN



3. Modify the member ports of a VLAN as described in Table 41.
4. Click **Apply**.

   A progress dialog box appears.
5. Click **Close** on the progress dialog box when the dialog box prompts that the configuration succeeds.

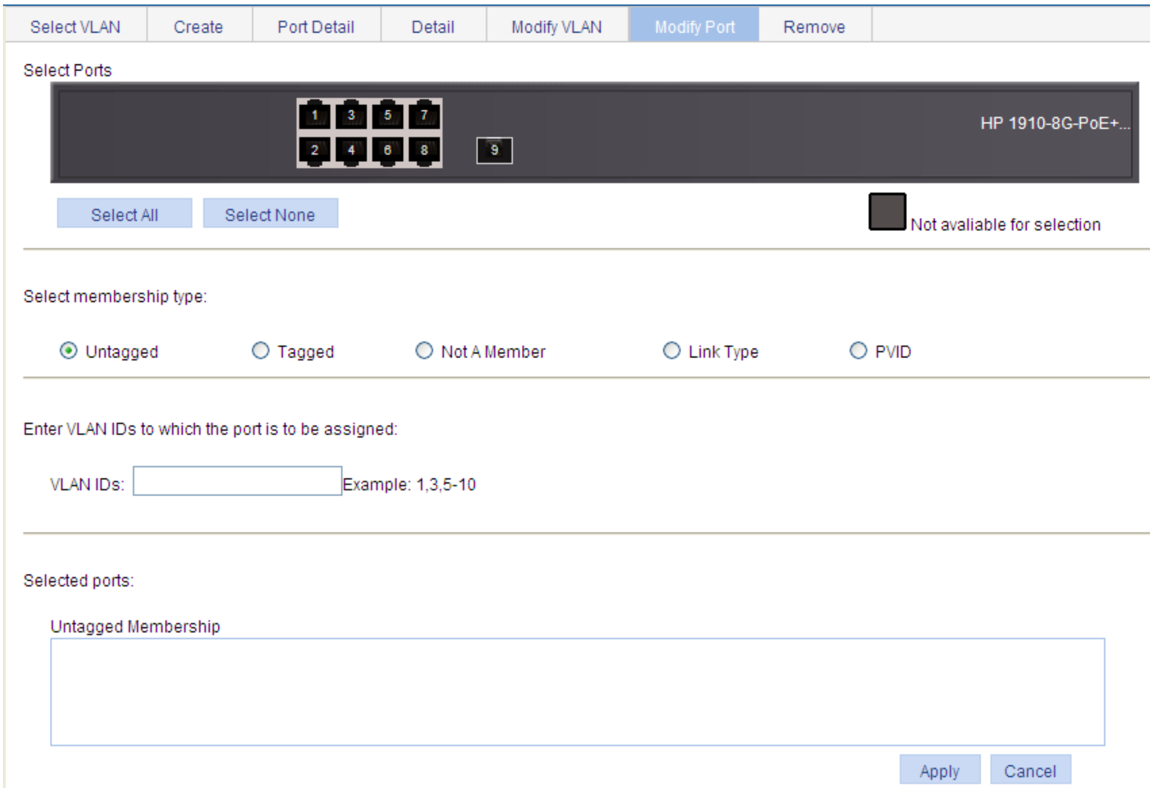
Table 41 Configuration items

Item	Description
Please select a VLAN to modify	Select the VLAN to be modified. The VLANs available for selection are existing VLANs 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	Set the member type of the port to be modified in the VLAN: • **Untagged**—Configure the port to send the traffic of the VLAN after removing the VLAN tag. • **Tagged**—Configure the port to send the traffic of the VLAN without removing the VLAN tag. • **Not a Member**—Remove the port from the VLAN.
Select ports to be modified and assigned to this VLAN	Select the ports to be modified in the selected VLAN. NOTE: When you configure an access port as a tagged member of a VLAN, the link type of the port is automatically changed into hybrid.

Modifying ports

1. Select **Network** > **VLAN** from the navigation tree.
2. Click **Modify Port** to enter the page for modifying ports.

Figure 142 Modifying ports



3. Modify the VLANs of a port as described in Table 42.
4. Click **Apply**.

   A progress dialog box appears.
5. Click **Close** on the progress dialog box when the dialog box prompts that the configuration succeeds.

Table 42 Configuration items

Item	Description
Select Ports	Select the ports to be modified.
Select membership type	Set the member types of the selected ports to be modified in the specified VLANs: • **Untagged**—Configure the ports to send the traffic of the VLANs after removing the VLAN tags. • **Tagged**—Configure the ports to send the traffic of the VLANs without removing the VLAN tags. • **Not a Member**—Remove the ports from the VLANs.

Item	Description
VLAN IDs	Set the IDs of the VLANs to/from which the selected ports are to be assigned/removed. NOTE: • You cannot configure an access port as an untagged member of a nonexistent VLAN. • When you configure an access port as a tagged member of a VLAN, or configure a trunk port as an untagged member of multiple VLANs in bulk, the link type of the port is automatically changed into hybrid. • You can configure a hybrid port as a tagged or untagged member of a VLAN only if the VLAN is an existing, static VLAN.

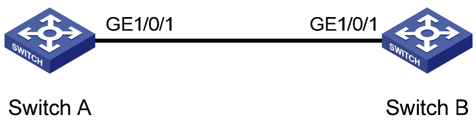
VLAN configuration example

Network requirements

As shown in Figure 143, trunk port GigabitEthernet 1/0/1 of Switch A is connected to trunk port GigabitEthernet 1/0/1 of Switch B.

Configure the PVID of GigabitEthernet 1/0/1 as VLAN 100, and configure GigabitEthernet 1/0/1 to permit packets of VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

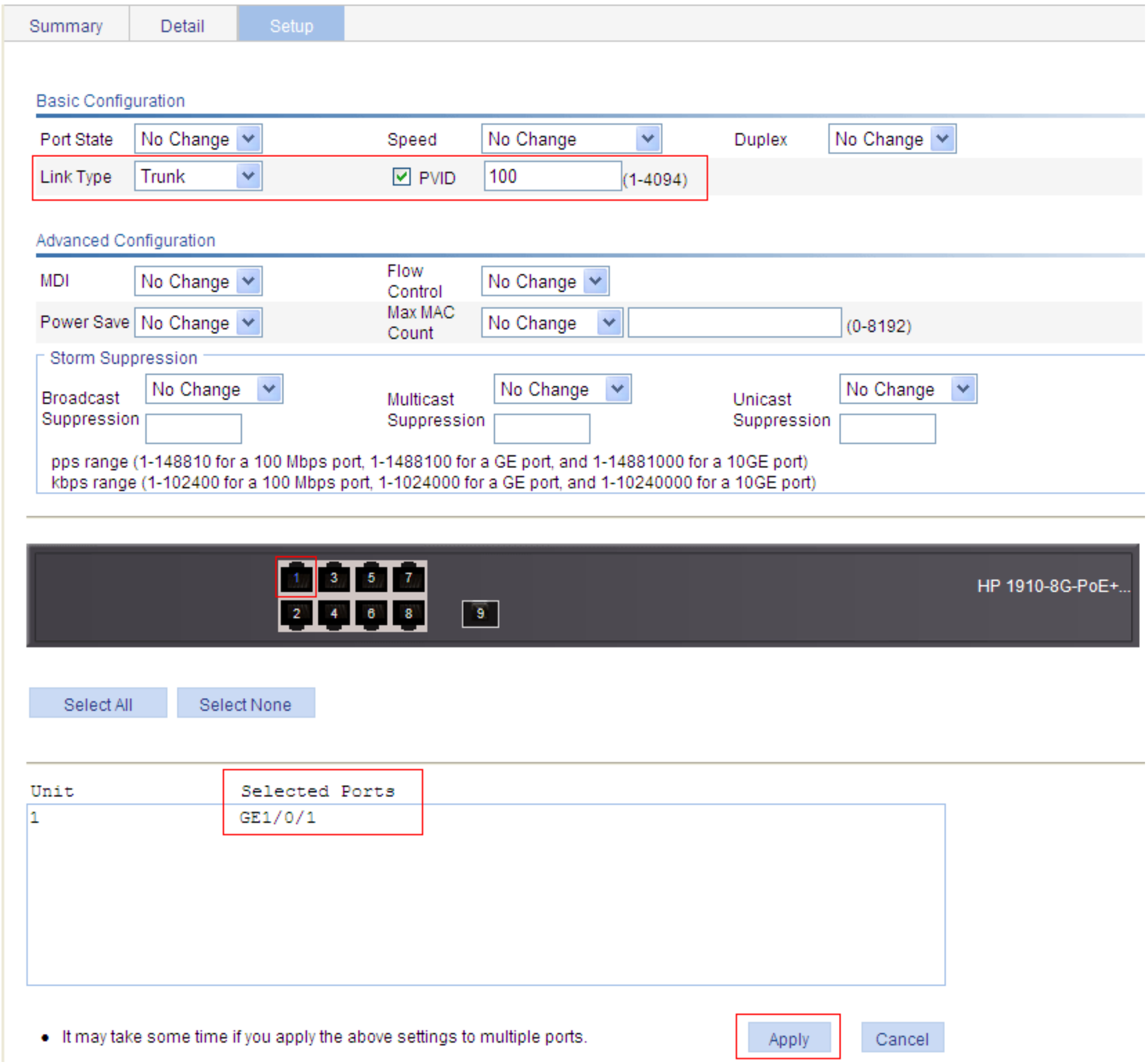
Figure 143 Network diagram



Configuring Switch A

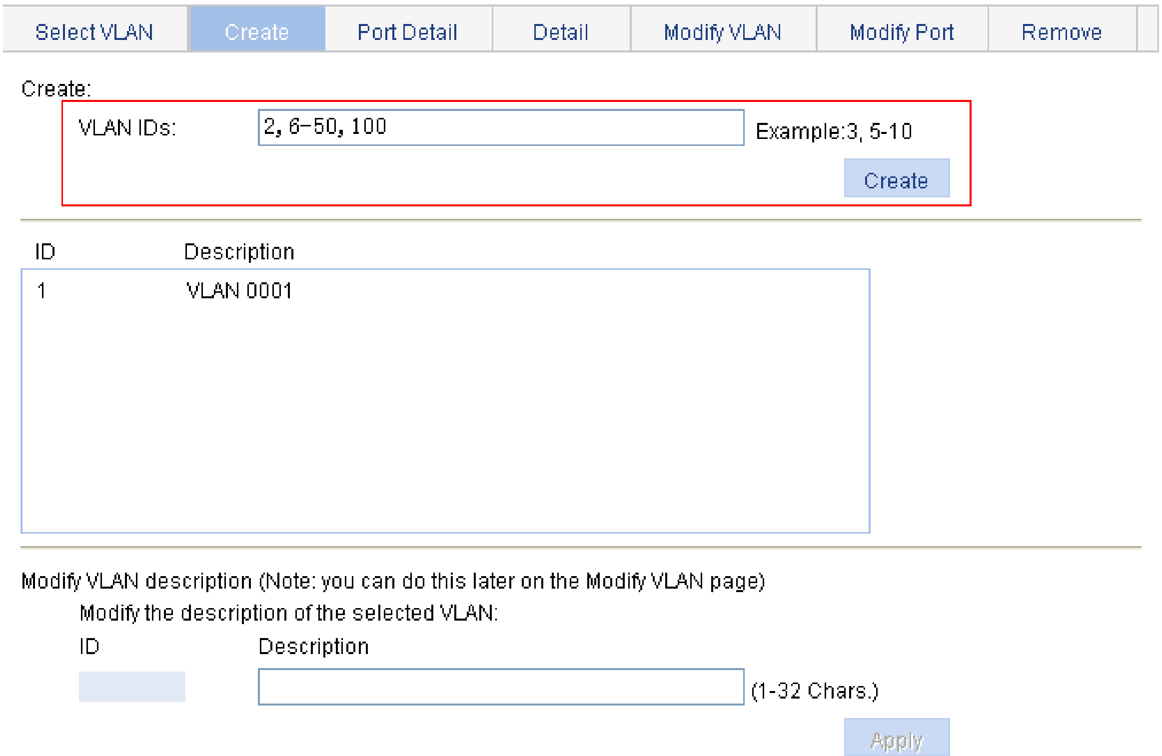
1. Configure GigabitEthernet 1/0/1 as a trunk port and configure VLAN 100 as the PVID:
   a. Select **Device** > **Port Management** from the navigation tree.
   b. Click **Setup** to enter the page for setting ports.
   c. Select **Trunk** in the **Link Type** list, select the **PVID** box, and then enter PVID 100.
   d. Select GigabitEthernet 1/0/1 on the chassis front device panel.
   e. Click **Apply**.

Figure 144 Configuring GigabitEthernet 1/0/1 as a trunk port and its PVID as 100



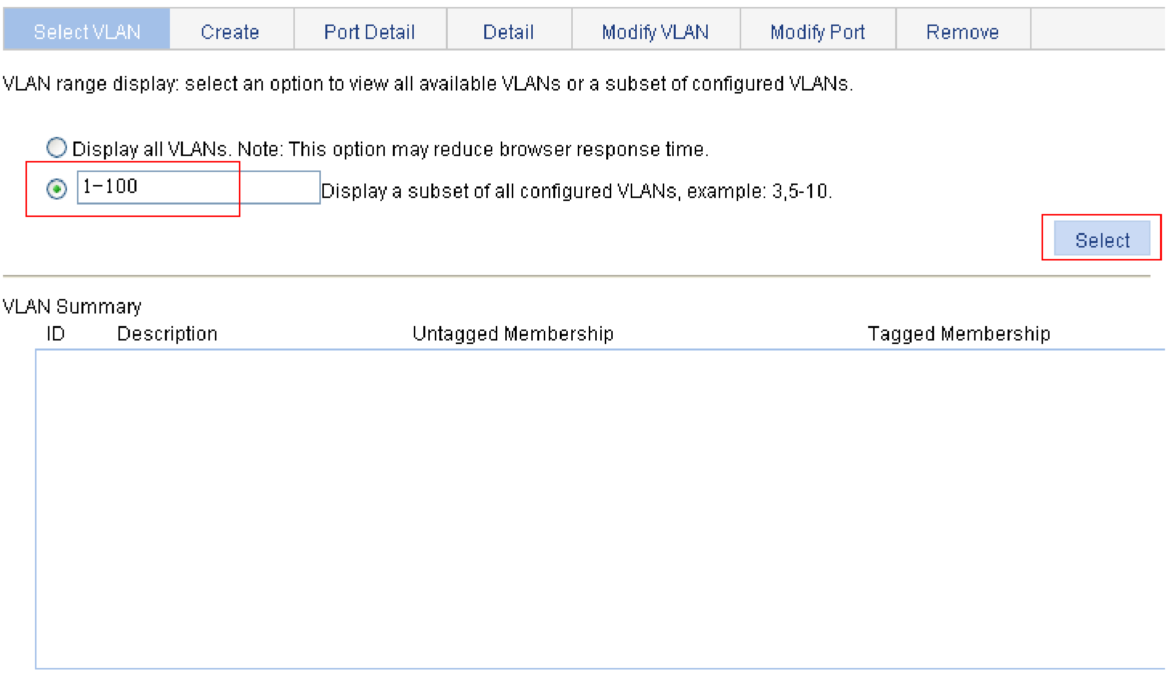
2. Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click **Create** to enter the page for creating VLANs.
   c. Enter VLAN IDs 2, 6-50, 100.
   d. Click **Apply**.

Figure 145 Creating VLAN 2, VLAN 6 through VLAN 50, and VLAN 100



3. Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member:
   a. Click **Select VLAN** to enter the page for selecting VLANs.
   b. Select the option before **Display a subnet of all configured VLANs** and enter 1-100 in the field.
   c. Click **Select**.

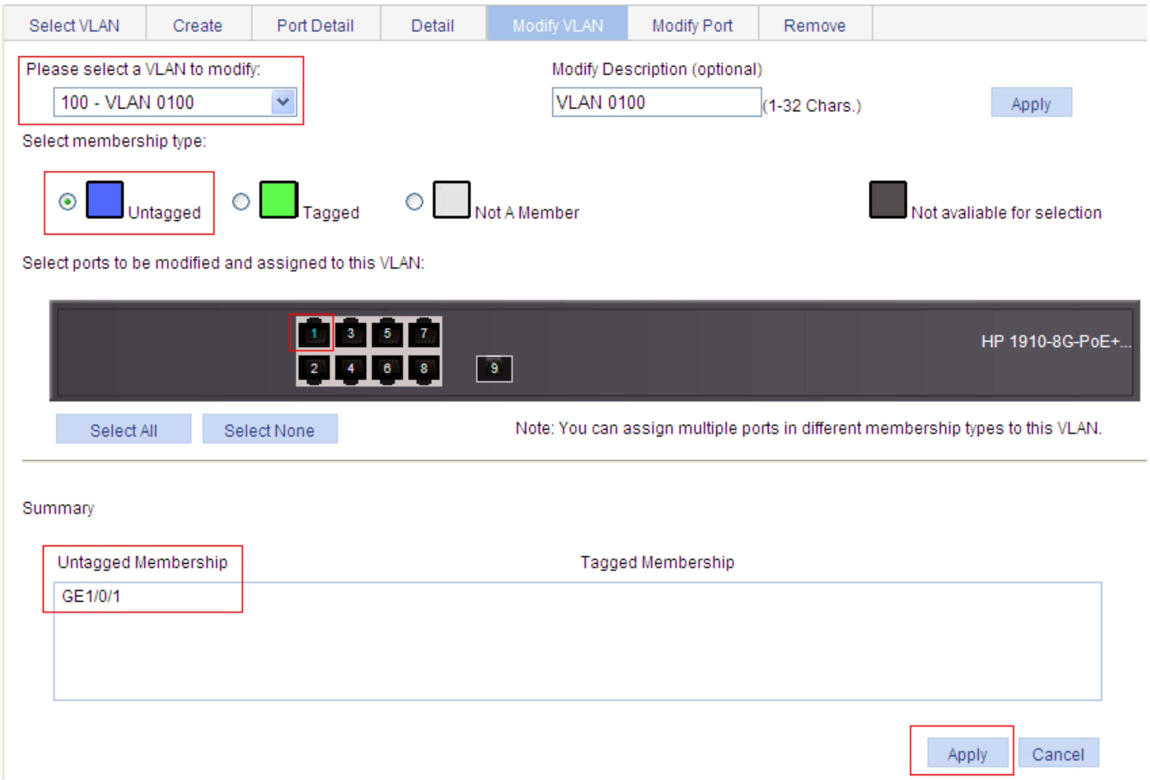
Figure 146 Setting a VLAN range



d. Click **Modify VLAN** to enter the page for modifying the ports in a VLAN.
e. Select **100 – VLAN 0100** in the **Please select a VLAN to modify:** list, select the **Untagged** option, and select GigabitEthernet 1/0/1 on the chassis front device panel.
f. Click **Apply**.

   A configuration progress dialog box appears.
g. After the configuration process is complete, click **Close**.

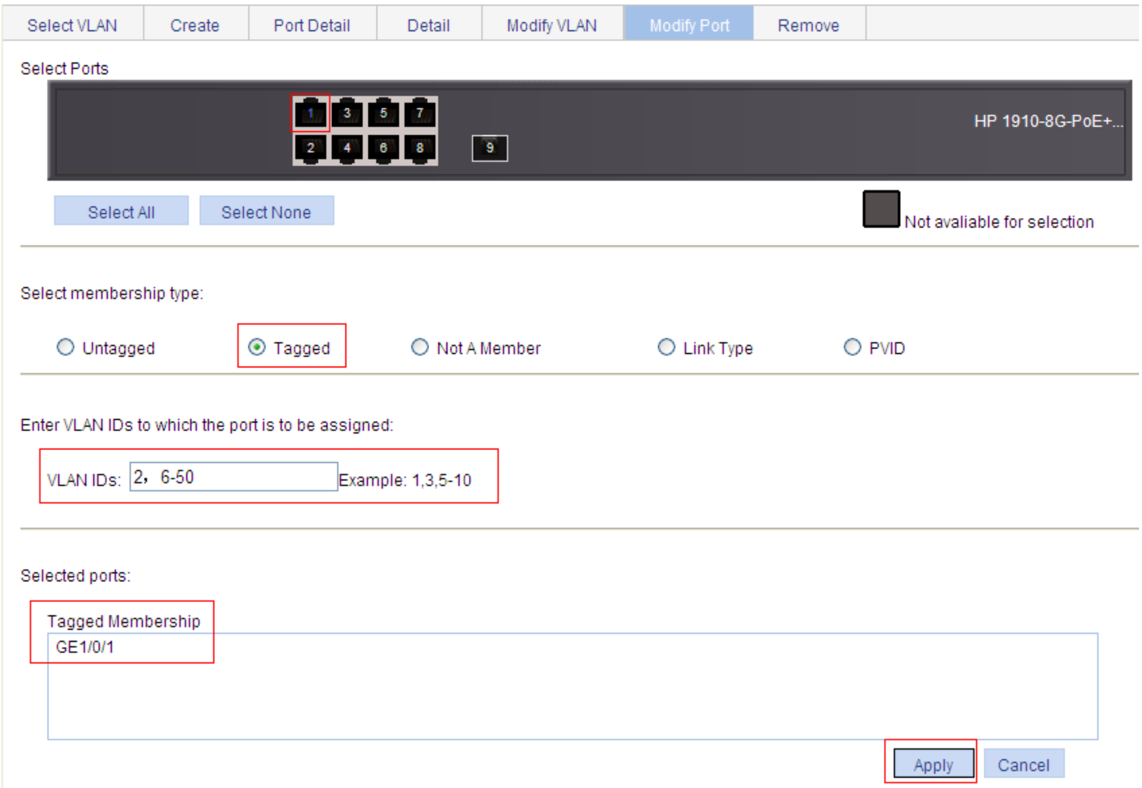
Figure 147 Assigning GigabitEthernet 1/0/1 to VLAN 100 as an untagged member



4. Assign GigabitEthernet 1/0/1 to VLAN2, and VLAN 6 through VLAN 50 as a tagged member:
   a. Click **Modify Port** to enter the page for modifying the VLANs to which a port belongs.
   b. Select GigabitEthernet 1/0/1 on the chassis front device panel, select the **Tagged** option, and enter VLAN IDs 2, 6-50.
   c. Click **Apply**.

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

Figure 148 Assigning GigabitEthernet 1/0/1 to VLAN 2 and to VLANs 6 through 50 as a tagged member



Configuring Switch B

Configure Switch B as you configure Switch A.

Configuration guidelines

Follow these guidelines when you configure VLANs:

- As the default VLAN, VLAN 1 can be neither created nor removed manually.
- You cannot manually create or remove VLANs reserved for special purposes.
- Dynamic VLANs cannot be removed on the page for removing VLANs.

Configuring VLAN interfaces

Overview

For hosts of different VLANs to communicate at Layer 3, you can use VLAN interfaces. 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 the IP address as the gateway address for the devices in the VLAN, so that traffic can be routed to other IP subnets.

Creating a VLAN interface

IMPORTANT:

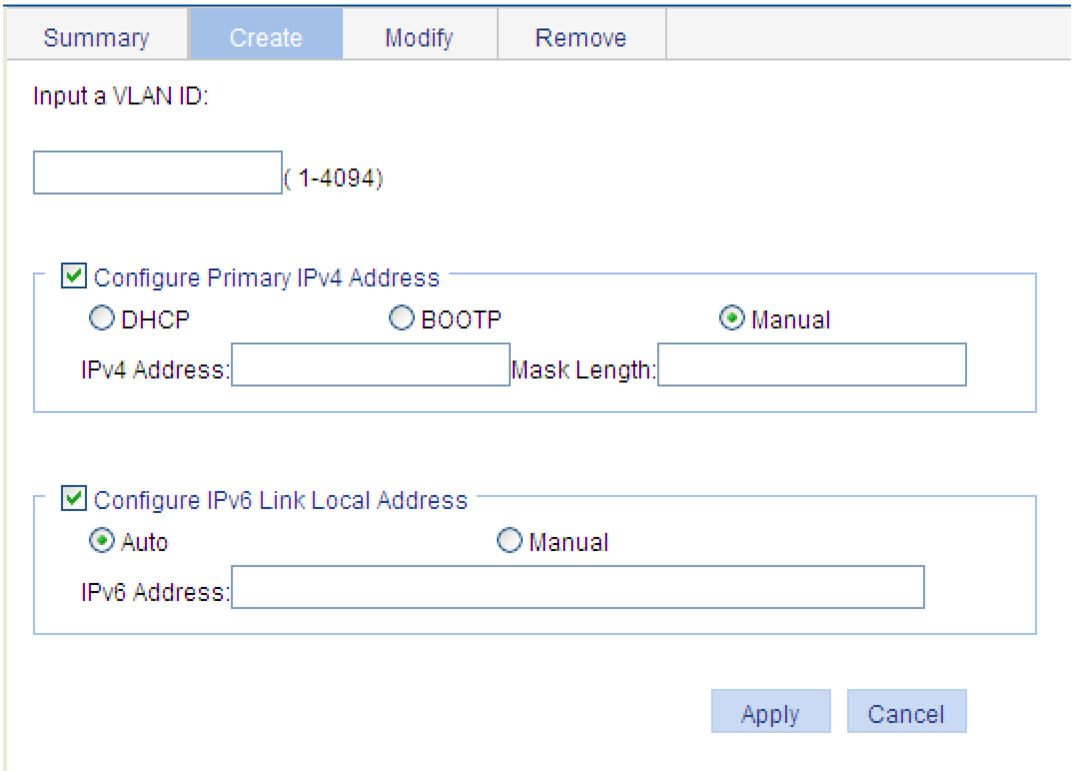
Before creating a VLAN interface, you must create the corresponding VLAN in **Network** > **VLAN**. For more information, see "Configuring VLANs."

When creating a VLAN interface, you can select to assign an IPv4 address and an IPv6 link-local address to the VLAN interface in this step or in a separate step. If you do not select to configure an IP address, you can create the VLAN interface, and configure an IP address for the VLAN interface by modifying it.

To create a VLAN interface:

1. Select **Network** > **VLAN Interface** from the navigation tree.
2. Click **Create** to enter the page for creating a VLAN interface.

Figure 149 Creating a VLAN interface



3. Configure the VLAN interface as described in Table 43.
4. Click **Apply**.

Table 43 Configuration items

Item		Description	
Input a VLAN ID:		Enter 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 BOOTP Manual	Configure the way in which the VLAN interface gets an IPv4 address. Allow the VLAN interface to obtain an IP address automatically 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** box.
	IPv4 Address	Configure an IPv4 address for the VLAN interface. This field is available after you select the **Manual** option.	
	Mask Length	Set the subnet mask length (or enter a mask in dotted decimal notation format). This field is available after you select the **Manual** option.	
Configure IPv6 Link Local Address	Auto Manual	Configure the way in which the VLAN interface obtains an IPv6 link-local address. Select the **Auto** or **Manual** option: • **Auto**—The device automatically assigns a link-local address for the VLAN interface based on the link-local address prefix (**FE80::/64**) and the link-layer address of the VLAN interface. • **Manual**—Requires manual assignment.	These items are available after you select the **Configure IPv6 Link Local**

Item	Description
IPv6 Address	**Address** box. Configure an IPv6 link-local address for the VLAN interface. This field is available after you select the **Manual** option. The prefix of the IPv6 link-local address you enter must be FE80::/64.

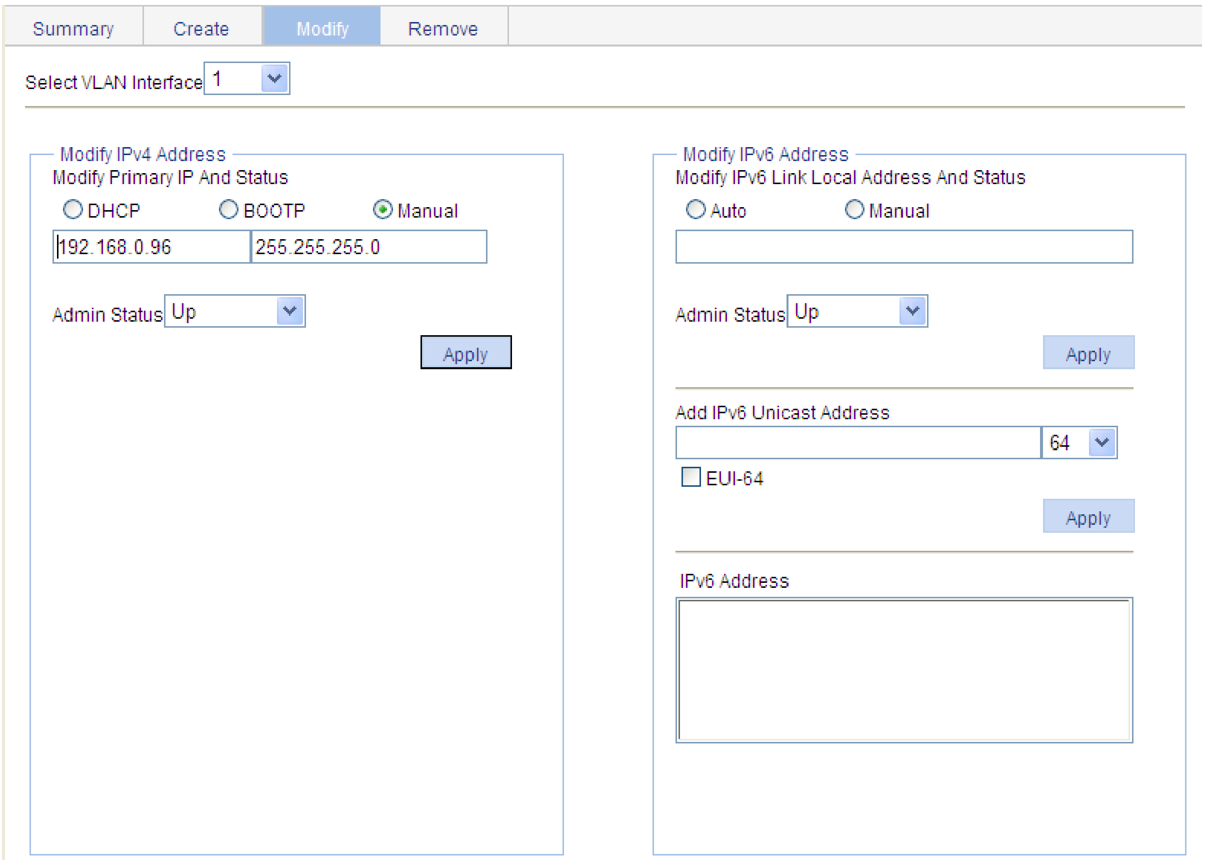
Modifying a VLAN interface

By modifying a VLAN interface, you can assign an IPv4 address, an IPv6 link-local address, and an IPv6 site-local address, or global unicast address to the VLAN interface, and shut down or bring up the VLAN interface.

To modify a VLAN interface:

1. Select **Network** > **VLAN Interface** from the navigation tree.
2. Click the **Modify** tab to enter the page for modifying a VLAN interface.

Figure 150 Modifying a VLAN interface



3. Modify a VLAN interface as described in Table 44.
4. Click **Apply**.

Table 44 Configuration items

<table>
<tr><th colspan="2">Item</th><th>Description</th></tr>
<tr><td colspan="2">Select VLAN Interface</td><td>Select the VLAN interface to be configured.
The VLAN interfaces available for selection in the list are those created on the page for creating VLAN interfaces.</td></tr>
<tr><td rowspan="4">Modify IPv4 Address</td><td>DHCP</td><td rowspan="3">Configure the way in which the VLAN interface gets an IPv4 address.
Allow the VLAN interface to obtain an IP address automatically by selecting the DHCP or BOOTP option, or manually assign the VLAN interface an IP address by selecting the Manual option. In the latter case, you need to set the mask length or enter a mask in dotted decimal notation format.</td></tr>
<tr><td>BOOTP</td></tr>
<tr><td>Manual</td></tr>
<tr><td>Admin Status</td><td>Select Up or Down in the Admin Status 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.
NOTE:
• The current VLAN interface state in the Modify IPv4 Address and Modify IPv6 Address frames changes as the VLAN interface state is modified in the Admin Status list.
• The state of each port in the VLAN is independent of the VLAN interface state.</td></tr>
</table>

<table>
<tr><th colspan="2">Item</th><th>Description</th></tr>
<tr><td rowspan="5">Modify IPv6 Address</td><td>Auto</td><td rowspan="2">Configure the way in which the VLAN interface obtains an IPv6 link-local address.
Select the Auto or Manual option:
• Auto—Indicates that the device automatically assigns a link-local address for the VLAN interface according to the link-local address prefix (FE80::/64) and the link-layer address of the VLAN interface.
• Manual—Configures an IPv6 link-local address for the VLAN interface manually.</td></tr>
<tr><td>Manual</td></tr>
<tr><td>Admin Status</td><td>Select Up or Down in the Admin Status list to bring up or shut down the selected VLAN interface.
When the VLAN interface fails, you can shut down and then enable 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.
NOTE:
• The current VLAN interface state in the Modify IPv4 Address and Modify IPv6 Address frames changes as the VLAN interface state is modified in the Admin Status list.
• The state of each port in the VLAN is independent of the VLAN interface state.</td></tr>
<tr><td>Add IPv6 Unicast Address</td><td>Assign an IPv6 site-local address or global unicast address to the VLAN interface.
Enter an IPv6 address in the field and select a prefix length in the list next to it.
The prefix of the IPv6 address you entered cannot be FE80::/10, the prefix of the link-local address.
The prefix of the IPv6 site-local address you enter must be FEC0::/10.</td></tr>
<tr><td>EUI-64</td><td>Specify to generate IPv6 site-local addresses or global unicast addresses in the EUI-64 format.
If the EUI-64 box is not specified, manually configured IPv6 site-local addresses or global unicast addresses are used.</td></tr>
</table>

NOTE:

- After you modify the IPv4 address and status or the IPv6 address and status, or add an IPv6 unicast 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.

Configuration guidelines

When you configure VLAN interfaces, follow these guidelines:

- A link-local address is automatically generated for an IPv6 VLAN interface after an IPv6 site-local address or global unicast address is configured for the VLAN interface. This generated link-local address is the same as the one generated in the **Auto** mode. If a manually assigned link-local address is available, the manually assigned one takes effect. After the manually assigned link-local address is removed, the automatically generated one takes effect.
- For an IPv6 VLAN interface whose IPv6 link-local address is generated automatically after you assign an IPv6 site-local address or global unicast address, removing the IPv6 site-local address or global unicast address also removes the generated IPv6 link-local address.

- For IPv6 link-local address configuration, manual assignment takes precedence over automatic generation. If you first adopt the manual assignment and then the automatic generation, the automatically generated link-local address will not take effect and the link-local address of the interface is still the manually assigned one. But if you remove the manually assigned one, the one automatically generated takes effect.

Configuring a voice VLAN

Overview

The voice technology is developing quickly, and more and more voice devices are in use. In broadband communities, data traffic and voice traffic are usually transmitted in the network at the same time. Usually, voice traffic needs higher priority than data traffic to reduce the transmission delay and packet loss ratio.

A voice VLAN is configured for voice traffic. After assigning the ports that connect to voice devices to a voice VLAN, the system automatically modifies quality of service (QoS) parameters for voice traffic, to improve the transmission priority of voice traffic and ensure voice quality.

NOTE:

Common voice devices include IP phones and integrated access devices (IADs). Only IP phones are used in the voice VLAN configuration examples in this document.

OUI addresses

A device determines whether an incoming 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 45 for voice traffic identification.

Table 45 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:

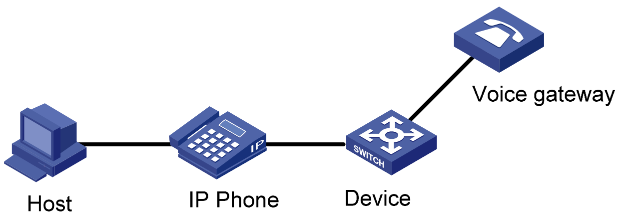
- An OUI address is usually the first 24 bits of a MAC address (in binary format). It is a globally unique identifier assigned to a vendor by the IEEE. In this document, however, OUI addresses are used by the system to determine whether received packets are voice packets and they are the results of the AND operation of a MAC address and a mask. For more information, 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 the following modes:

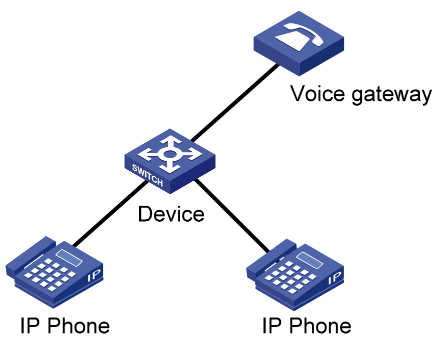
- **Automatic mode**—The system matches the source MAC addresses in the protocol packets (untagged packets) sent by the IP phone upon its power-on against the OUI list. If a match is found, the system automatically assigns the receiving port to a voice VLAN, issues ACL rules and configures the packet 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. The system automatically assigns ports to, or removes ports from, a voice VLAN. Automatic mode is suitable for scenarios where PCs and IP phones connected in series access the network through the device and ports on the device simultaneously transmit both voice traffic and data traffic, as shown in Figure 151. When the voice VLAN works normally, if the system reboots, the system reassigns ports in automatic voice VLAN assignment mode to the voice VLAN after the reboot, ensuring that existing voice connections can work normally. In this case, voice traffic streams do not trigger port assignment to the voice VLAN.

Figure 151 PCs and IP phones connected in series access the network



- **Manual mode**—You must 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, you must manually assign ports to, or remove ports from, a voice VLAN. Manual mode is suitable for scenarios where only IP phones access the network through the device, and ports on the device transmit only voice traffic, as shown in Figure 152. In this mode, ports assigned to a voice VLAN transmit voice traffic exclusively, which prevents the impact of data traffic on the transmission of voice traffic.

Figure 152 Only IP phones access the network



Both modes forward tagged packets according to their tags.

Table 46 and Table 47 list the configurations required for ports of different link types to support tagged or untagged voice traffic sent from IP phones when different voice VLAN assignment modes are configured.

- IP phones send tagged voice traffic

Table 46 Required configurations on ports of different link types for them to support tagged voice traffic

Port link type	Voice VLAN assignment mode supported for tagged voice traffic	Configuration requirements
Access	N/A	N/A
Trunk	Automatic and manual	In automatic mode, the PVID of the port cannot be the voice VLAN. In manual mode, the PVID of the port cannot be the voice VLAN. Configure the port to permit packets of the voice VLAN to pass through.
Hybrid	Automatic and manual	In automatic mode, the PVID of the port cannot be the voice VLAN. In manual mode, the PVID of the port cannot be the voice VLAN. Configure the port to permit packets of the voice VLAN to pass through tagged.

- IP phones send untagged voice traffic

  When IP phones send untagged voice traffic, you can only configure the voice traffic receiving ports on the device to operate in manual voice VLAN assignment mode.

Table 47 Required configurations on ports of different link types for them to support tagged voice traffic

Port link type	Voice VLAN assignment mode supported for untagged voice traffic	Configuration requirements
Access	Manual	Configure the PVID of the port as the voice VLAN.
Trunk	Manual	Configure the PVID of the port as the voice VLAN and assign the port to the voice VLAN.
Hybrid	Manual	Configure the PVID of the port as the voice VLAN and configure the port to permit packets 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 PVID 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 PVID of the access port as the voice VLAN. As a result, 802.1X authentication does not take effect.

Security mode and normal mode of voice VLANs

Depending on their inbound packet filtering mechanisms, voice VLAN-enabled ports operate in one of the following modes:

- **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 PVID of the port is the voice VLAN and the port operates 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 untagged 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, but all other packets are dropped.

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

HP does not recommend you transmit both voice packets and non-voice packets in a voice VLAN. If you have to, first make sure that the voice VLAN security mode is disabled.

Table 48 How a voice VLAN-enable port processes packets in security/normal mode

Voice VLAN operating 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
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

Recommended voice VLAN configuration procedure

Before configuring the voice VLAN, you must create the VLAN and configure the link type of each port to be assigned to the VLAN. Because 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, see "Managing ports."

Recommended configuration procedure for a port in automatic voice VLAN assignment mode

Step	Remarks
1. Configuring voice VLAN globally	(Optional.) Configure the voice VLAN to operate in security mode and configure the aging timer

Step	Remarks
2. Configuring voice VLAN on ports	(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.
3. Adding OUI addresses to the OUI list	(Optional.) The system supports up to 128 OUI addresses. By default, the system is configured with seven OUI addresses, as shown in Table 45.

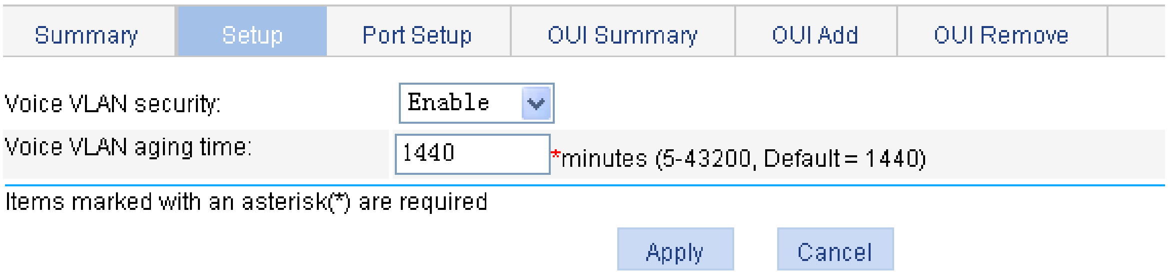
Recommended configuration procedure for a port in manual voice VLAN assignment mode

Step	Remarks
1. Configuring voice VLAN globally	(Optional.) Configure the voice VLAN to operate in security mode and configure the aging timer.
2. Assigning the port to the voice VLAN	(Required.) After an access port is assigned to the voice VLAN, the voice VLAN automatically becomes the PVID of the access port. For more information, see "Configuring VLANs."
3. Configuring the voice VLAN as the PVID 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 more information, see "Managing ports."
4. Configuring voice VLAN on ports	(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.
5. Adding OUI addresses to the OUI list	(Optional.) You can configure up to 128 OUI addresses. By default, the system is configured with the seven OUI addresses shown in Table 45.

Configuring voice VLAN globally

1. Select **Network** > **Voice VLAN** from the navigation tree.
2. Click the **Setup** tab.

Figure 153 Configuring voice VLAN



3. Configure the global voice VLAN settings as described in Table 49.
4. Click **Apply**.

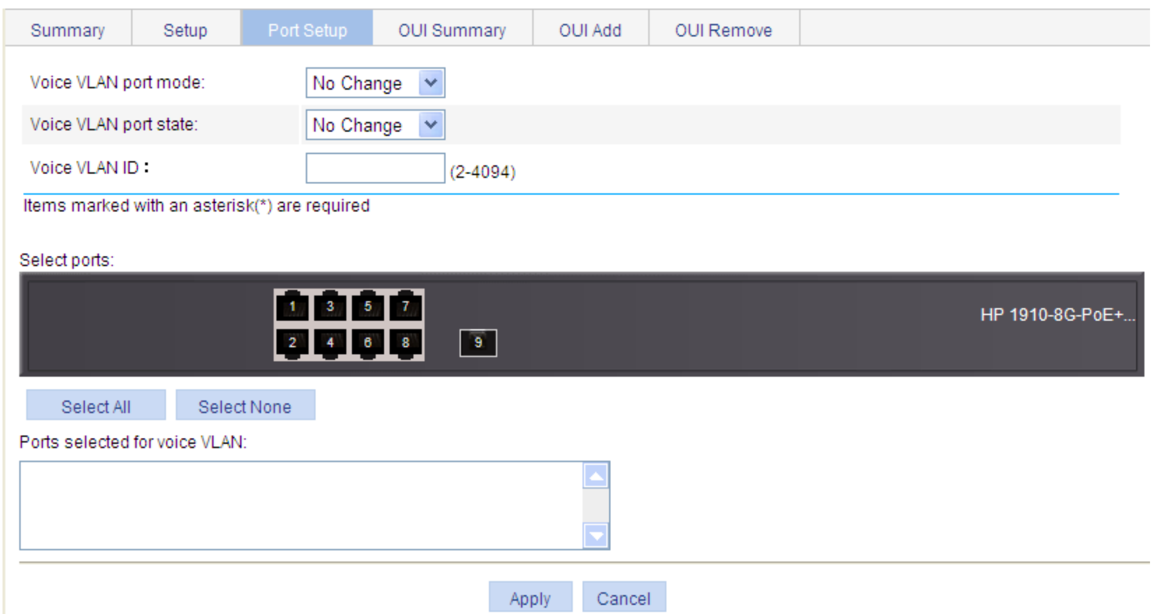
Table 49 Configuration items

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

Configuring voice VLAN on ports

1. Select **Network** > **Voice VLAN** from the navigation tree.
2. Click the **Port Setup** tab.

Figure 154 Configuring voice VLAN on ports



3. Configure the voice VLAN function for ports as described in Table 50.
4. Click **Apply**.

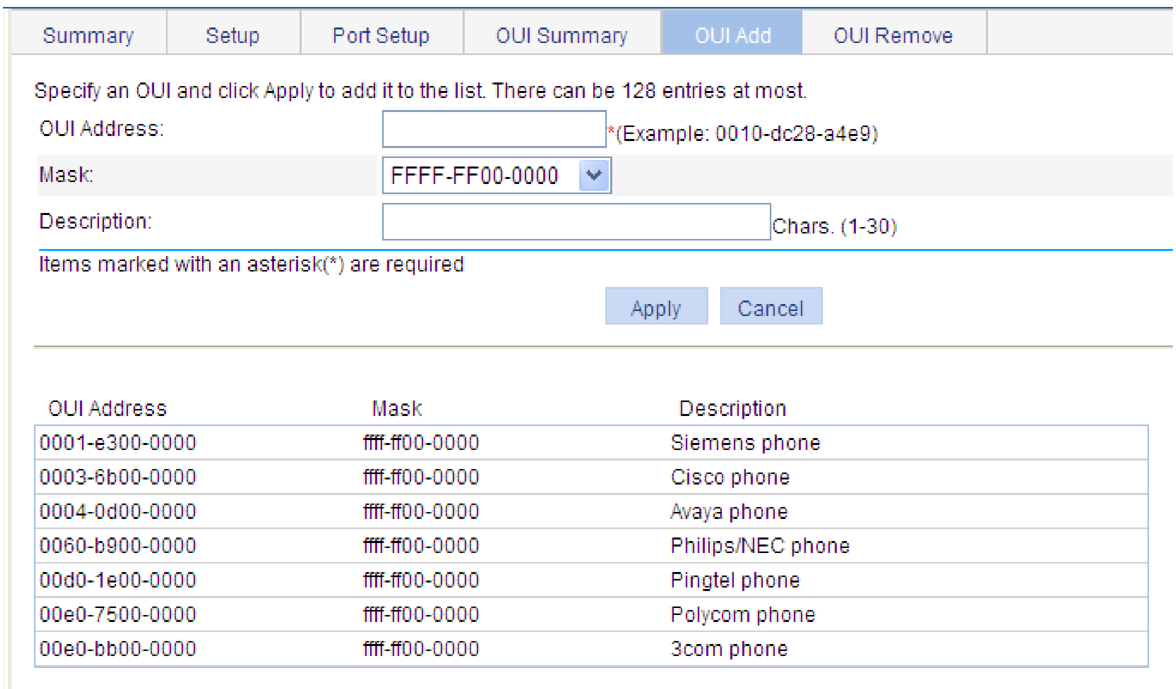
Table 50 Configuration items

Item	Description
Voice VLAN port mode	Set the voice VLAN assignment mode of a port to: • **Auto**—Automatic voice VLAN assignment mode • **Manual**—Manual voice VLAN assignment mode
Voice VLAN port state	Select **Enable** or **Disable** in the list to enable or disable the voice VLAN function on the port.
Voice VLAN ID	Set the voice VLAN ID of a port when the voice VLAN port state is set to **Enable**.
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** field. NOTE: To set the voice VLAN assignment mode of a port to automatic, you must make sure that the link type of the port is trunk or hybrid, and that the port does not belong to the voice VLAN.

Adding OUI addresses to the OUI list

1. Select **Network** > **Voice VLAN** from the navigation tree.
2. Click the **OUI Add** tab.

Figure 155 Adding OUI addresses to the OUI list



3. Add an OUI address to the list as described in Table 51.
4. Click **Apply**.

Table 51 Configuration items

Item	Description
OUI Address	Set the source MAC address of voice traffic.
Mask	Set the mask length of the source MAC address.
Description	Set the description of the OUI address entry.

Voice VLAN configuration examples

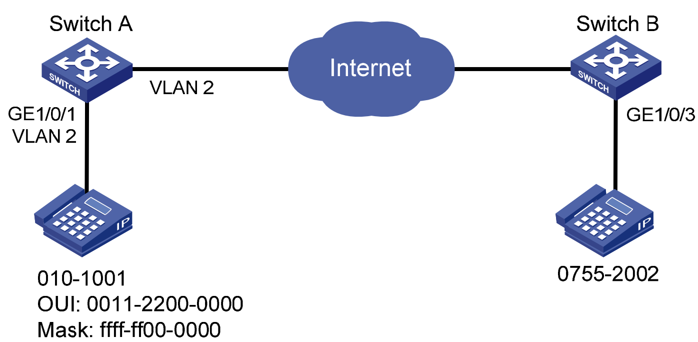
Configuring voice VLAN on a port in automatic voice VLAN assignment mode

Network requirements

As shown in Figure 156:

- 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**.

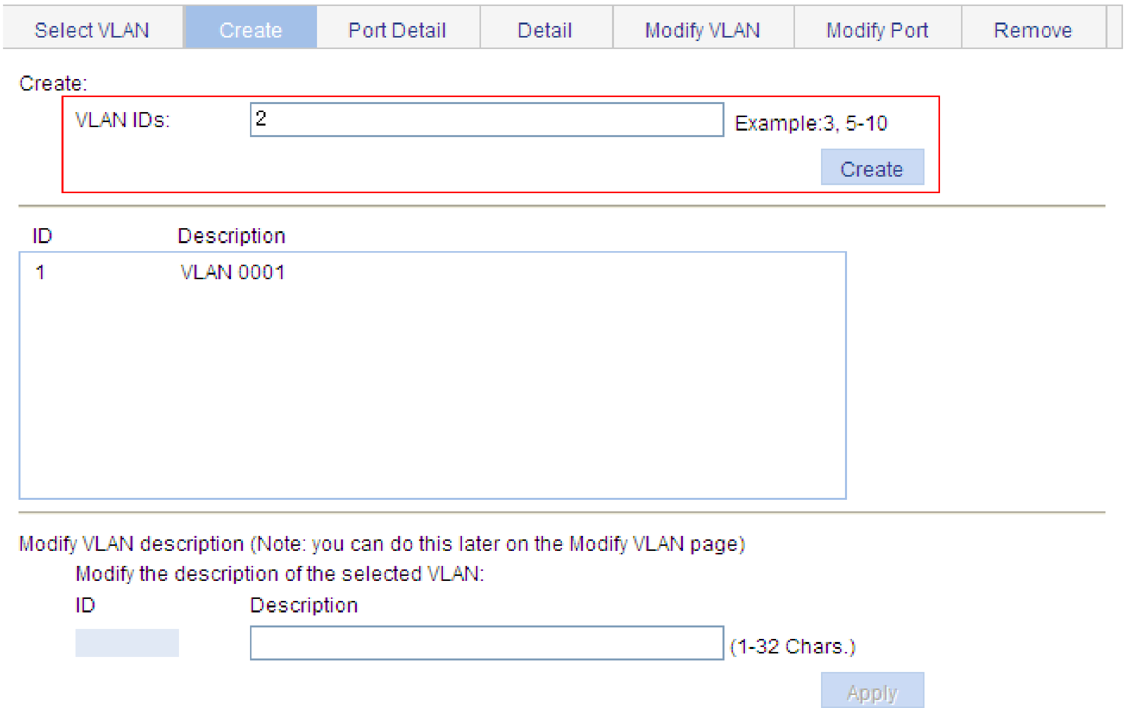
Figure 156 Network diagram



Configuring Switch A

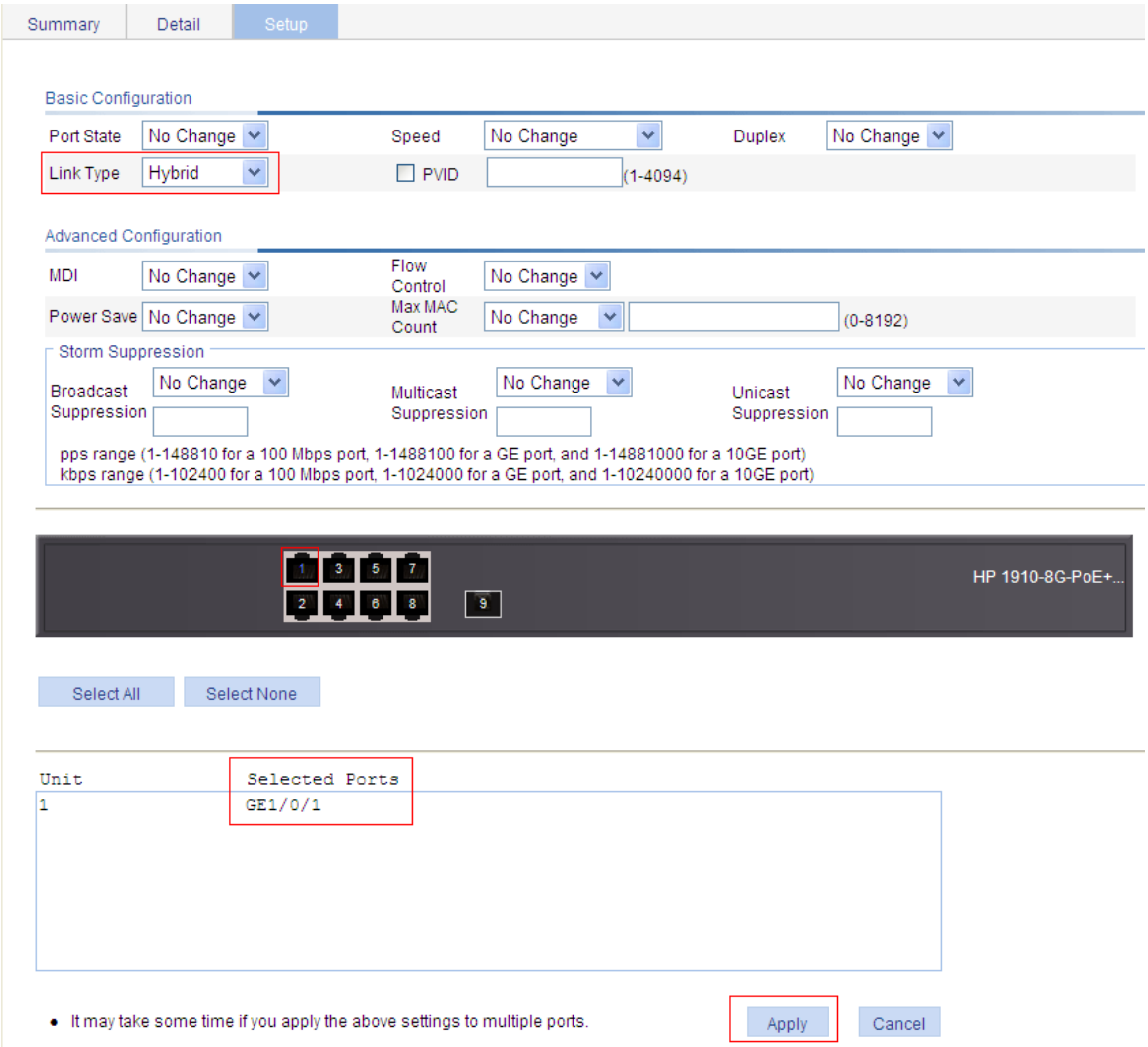
1. Create VLAN 2:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter VLAN ID 2.
   d. Click **Create**.

Figure 157 Creating VLAN 2



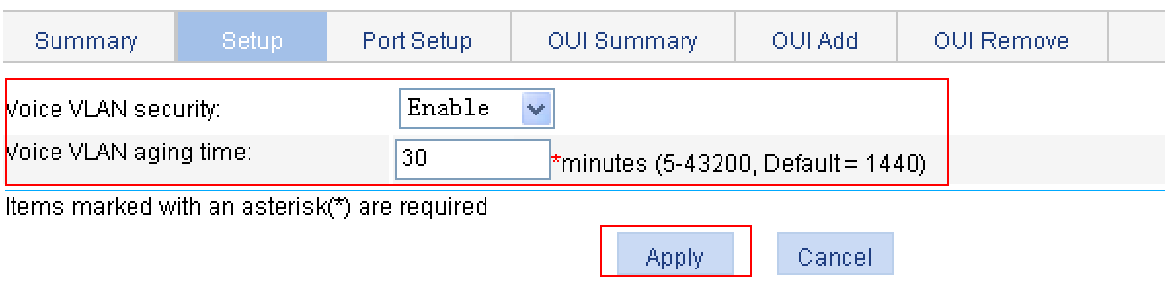
2. Configure GigabitEthernet 1/0/1 as a hybrid port:
    a. Select **Device** > **Port Management** from the navigation tree.
    b. Click the **Setup** tab.
    c. Select **Hybrid** from the **Link Type** list.
    d. Select GigabitEthernet 1/0/1 from the chassis front panel.
    e. Click **Apply**.

Figure 158 Configuring GigabitEthernet 1/0/1 as a hybrid port



3. Configure the voice VLAN function globally:
   a. Select **Network** > **Voice VLAN** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **Enable** in the **Voice VLAN security** list.
   d. Set the voice VLAN aging timer to 30 minutes.
   e. Click **Apply**.

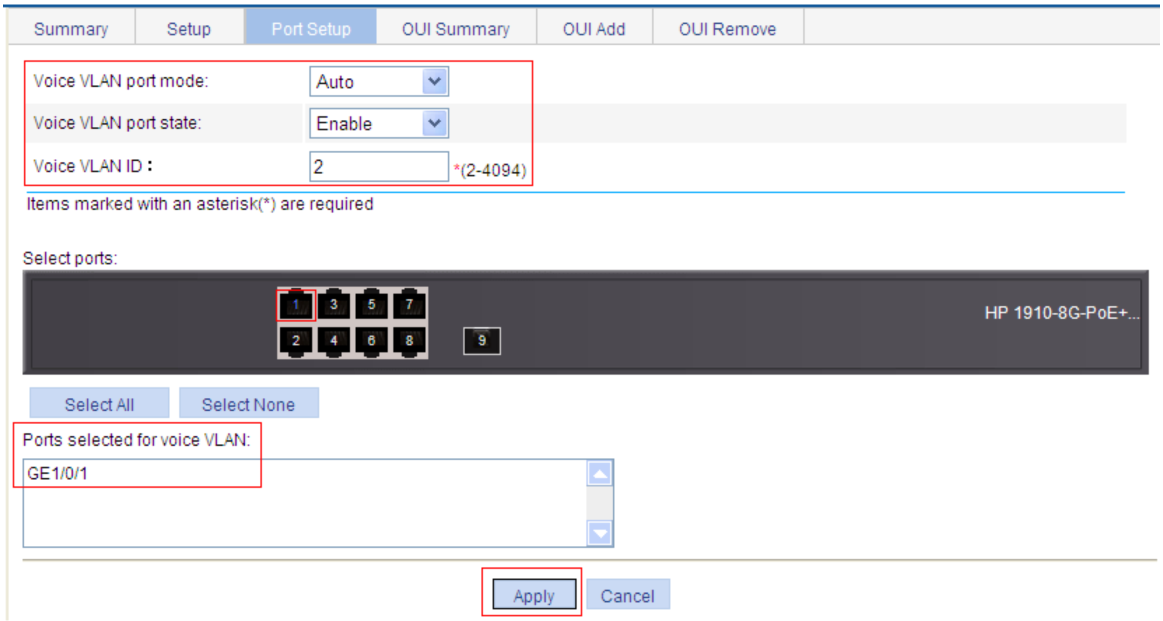
Figure 159 Configuring the voice VLAN function globally



4. Configure voice VLAN on GigabitEthernet 1/0/1:

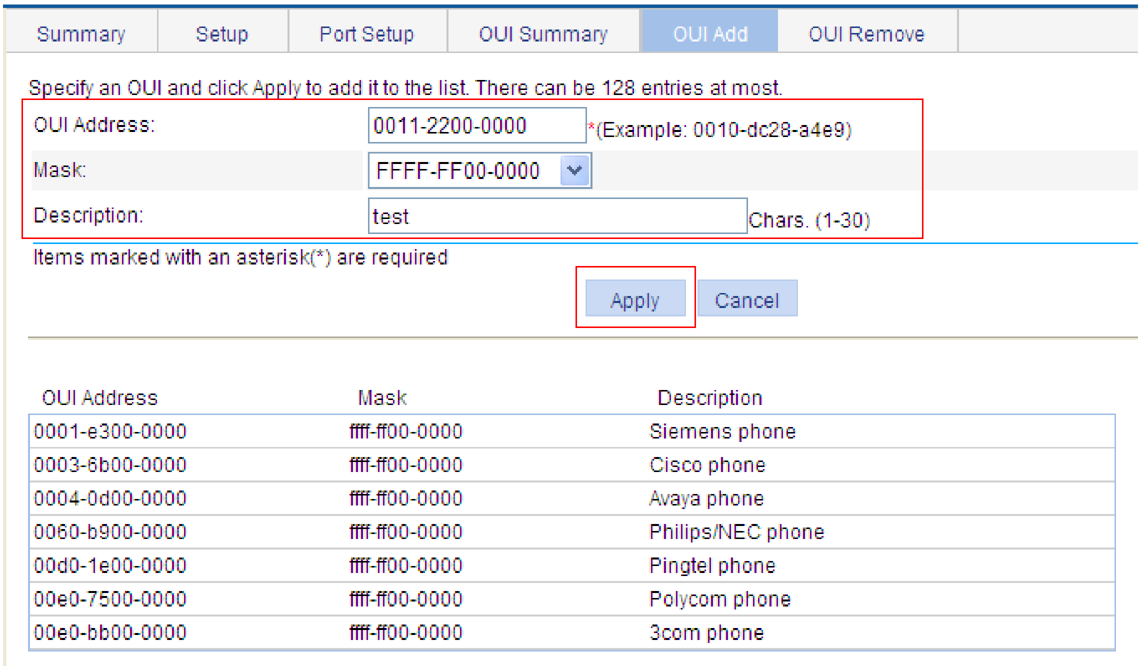
a. Click the **Port Setup** tab.
b. Select **Auto** in the **Voice VLAN port mode** list.
c. Select **Enable** in the **Voice VLAN port state** list.
d. Enter voice VLAN ID 2.
e. Select GigabitEthernet 1/0/1 on the chassis front panel.
f. Click **Apply**.

Figure 160 Configuring voice VLAN on GigabitEthernet 1/0/1



5. Add OUI addresses to the OUI list:
   a. Click the **OUI Add** tab.
   b. Enter OUI address **0011-2200-0000**.
   c. Select **FFFF-FF00-0000** in the **Mask** list.
   d. Enter description string **test**.
   e. Click **Apply**.

Figure 161 Adding OUI addresses to the OUI list

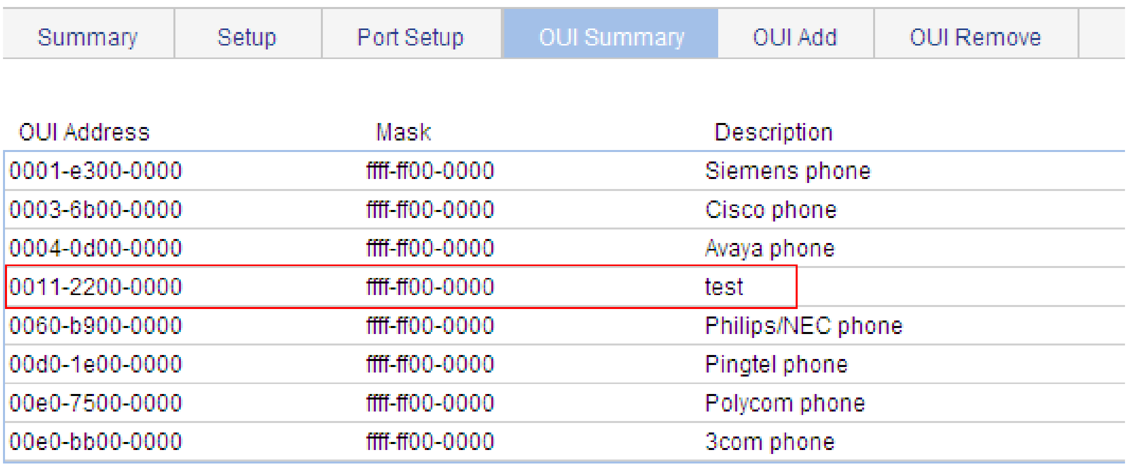


OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

Verifying the configuration

1. When the preceding configurations are completed, the **OUI Summary** tab is displayed by default, as shown in Figure 162. You can view the information about the newly-added OUI address.

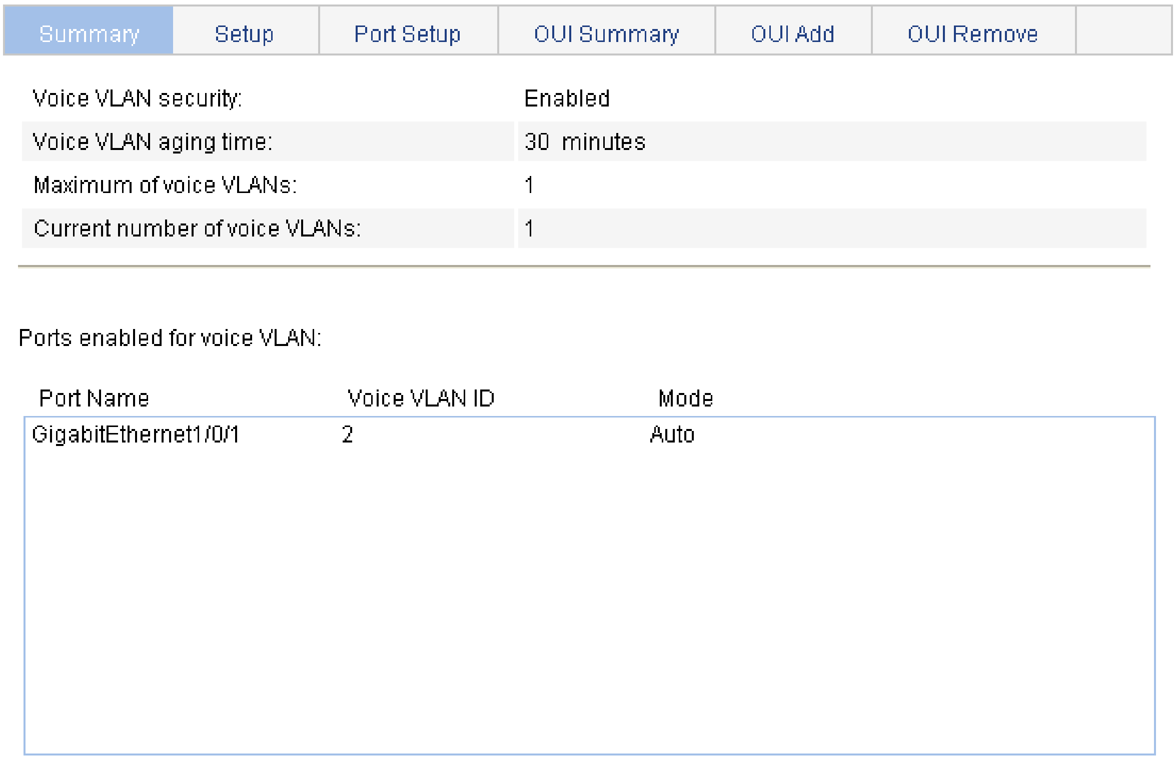
Figure 162 Displaying the current OUI list of the device



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

2. Click the **Summary** tab, where you can view the current voice VLAN information.

Figure 163 Displaying voice VLAN information



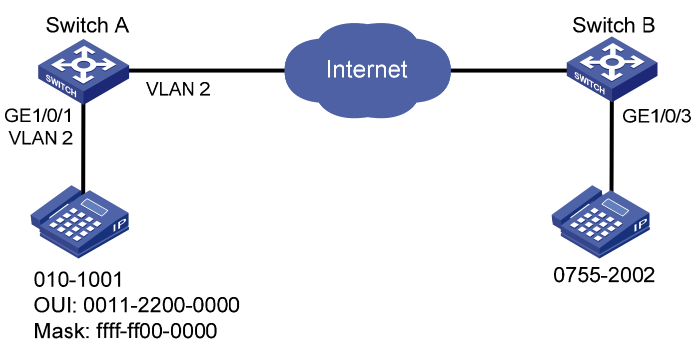
Configuring a voice VLAN on a port in manual voice VLAN assignment mode

Network requirements

As shown in Figure 164:

- 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**.

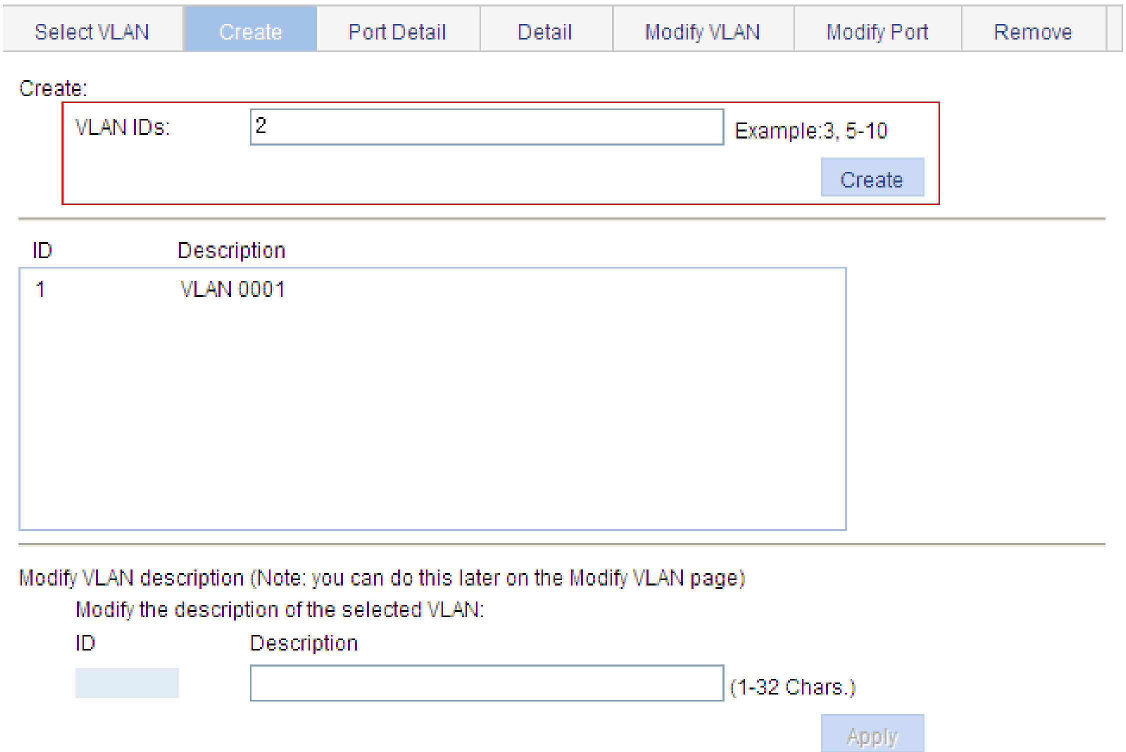
Figure 164 Network diagram



Configuring Switch A

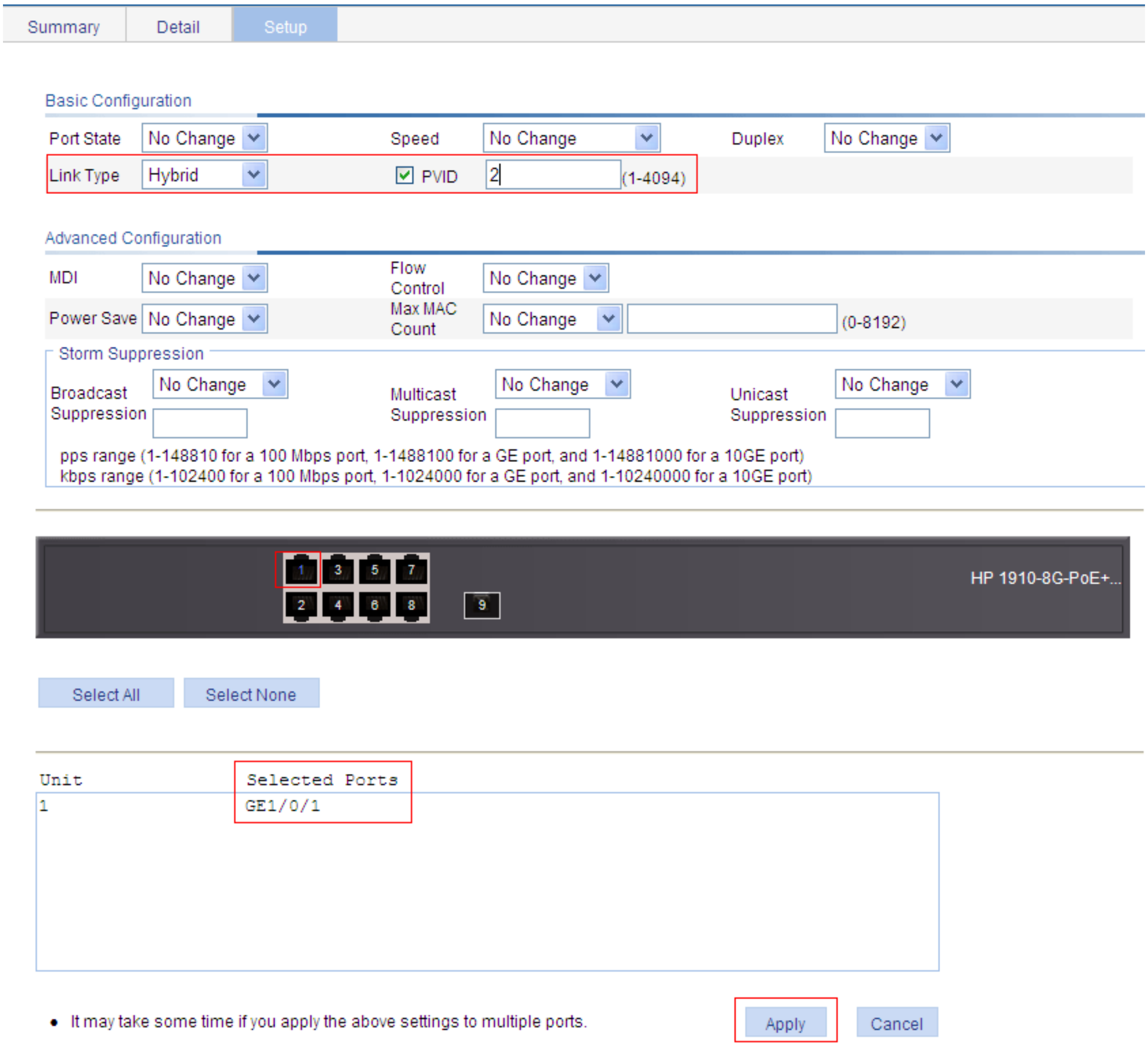
1. Create VLAN 2:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter VLAN ID 2.
   d. Click **Create**.

Figure 165 Creating VLAN 2



2. Configure GigabitEthernet 1/0/1 as a hybrid port and configure its PVID as VLAN 2:
   a. Select **Device** > **Port Management** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **Hybrid** from the **Link Type** list.
   d. Select the **PVID** box and enter 2 in the field.
   e. Select GigabitEthernet 1/0/1 from the chassis front panel.
   f. Click **Apply**.

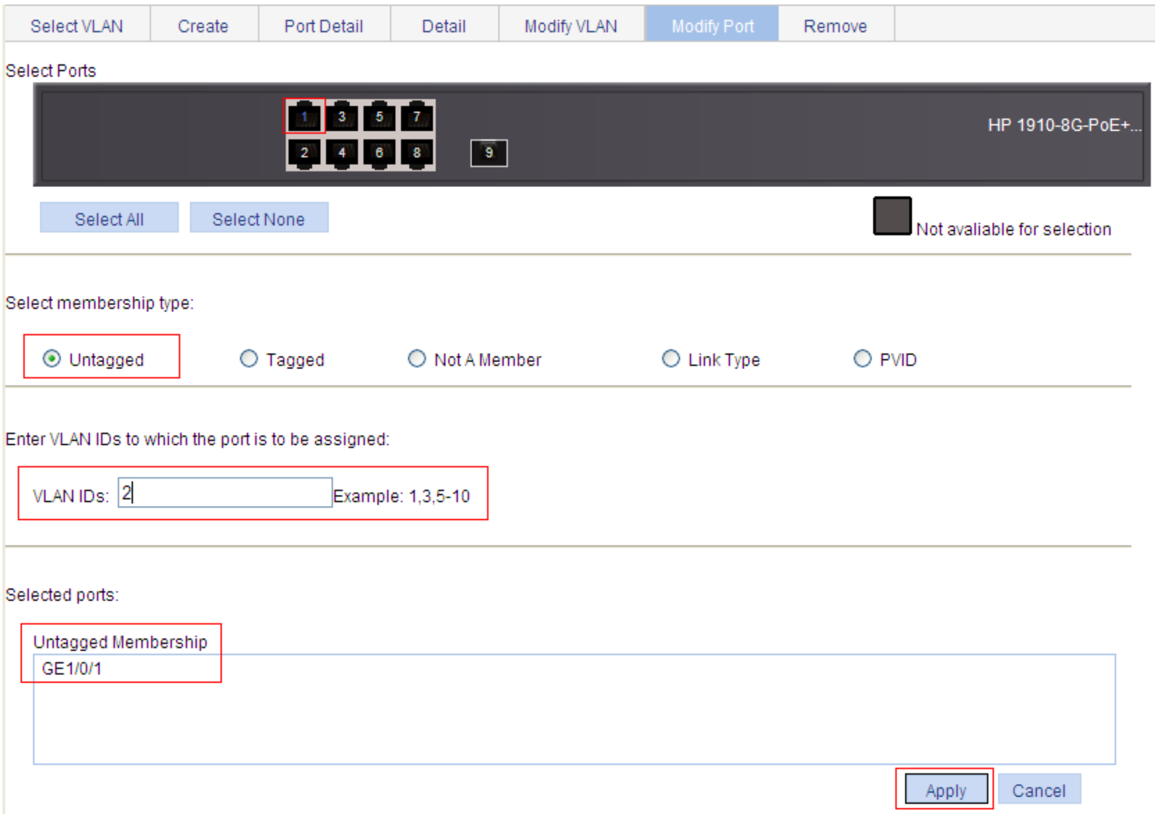
Figure 166 Configuring GigabitEthernet 1/0/1 as a hybrid port



3. Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Modify Port** tab.
   c. Select GigabitEthernet 1/0/1 from the chassis front panel.
   d. Select the **Untagged** option.
   e. Enter VLAN ID 2.
   f. Click **Apply**.

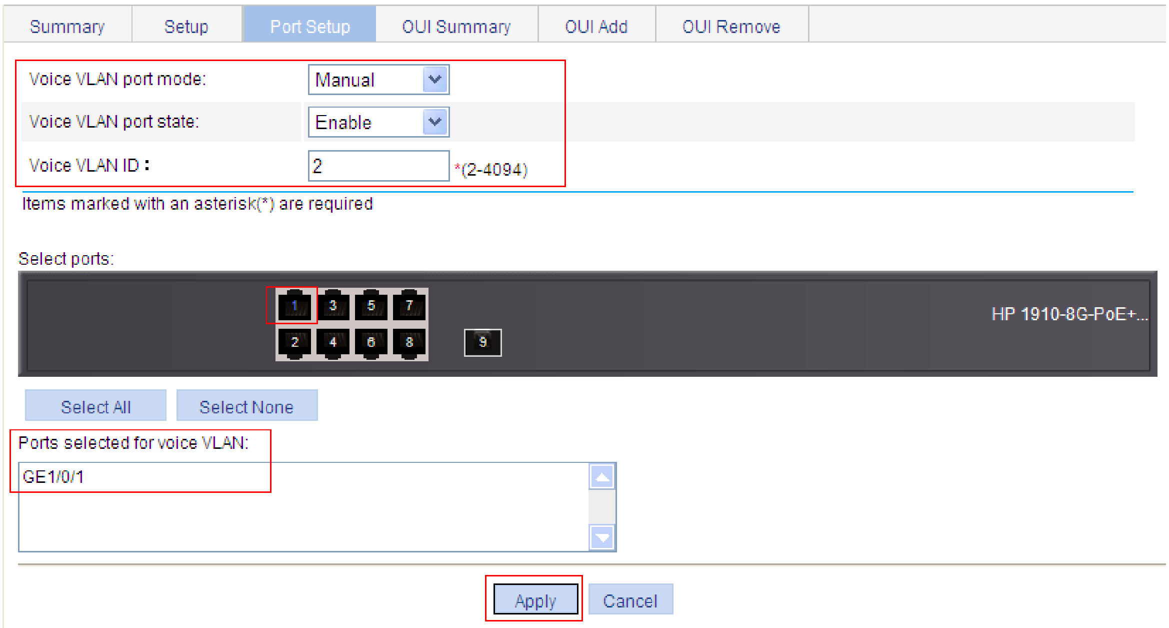
      A configuration progress dialog box appears.
   g. After the configuration process is complete, click **Close**.

Figure 167 Assigning GigabitEthernet 1/0/1 to VLAN 2 as an untagged member



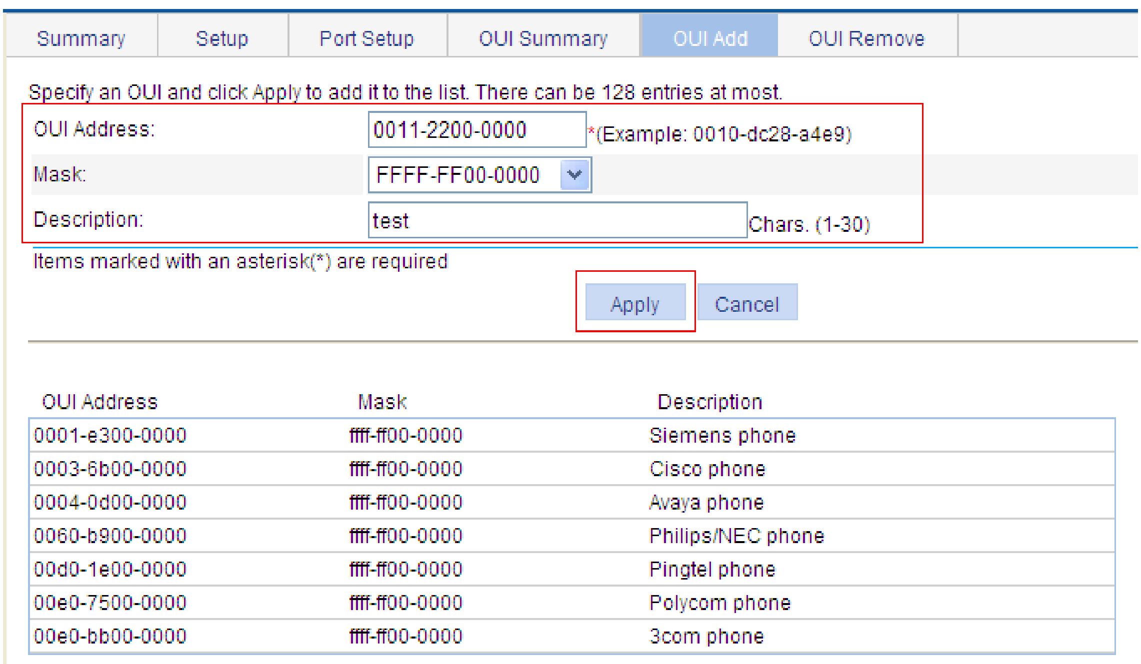
4. Configure voice VLAN on GigabitEthernet 1/0/1:
   a. Select **Network** > **Voice VLAN** from the navigation tree.
   b. Click the **Port Setup** tab.
   c. Select **Manual** in the **Voice VLAN port mode** list.
   d. Select **Enable** in the **Voice VLAN port state** list.
   e. Enter 2 in the **VLAN IDs** field.
   f. Select GigabitEthernet 1/0/1 on the chassis front panel.
   g. Click **Apply**.

Figure 168 Configuring voice VLAN on GigabitEthernet 1/0/1



5. Add OUI addresses to the OUI list:
   a. Click the **OUI Add** tab.
   b. Enter OUI address **0011-2200-0000**.
   c. Select **FFFF-FF00-0000** as the mask.
   d. Enter description string **test**.
   e. Click **Apply**.

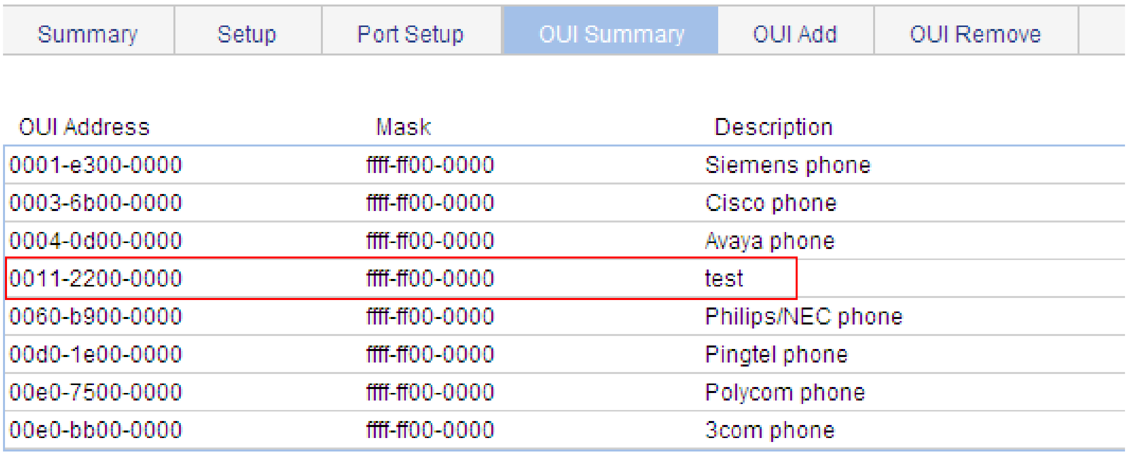
Figure 169 Adding OUI addresses to the OUI list



Verifying the configuration

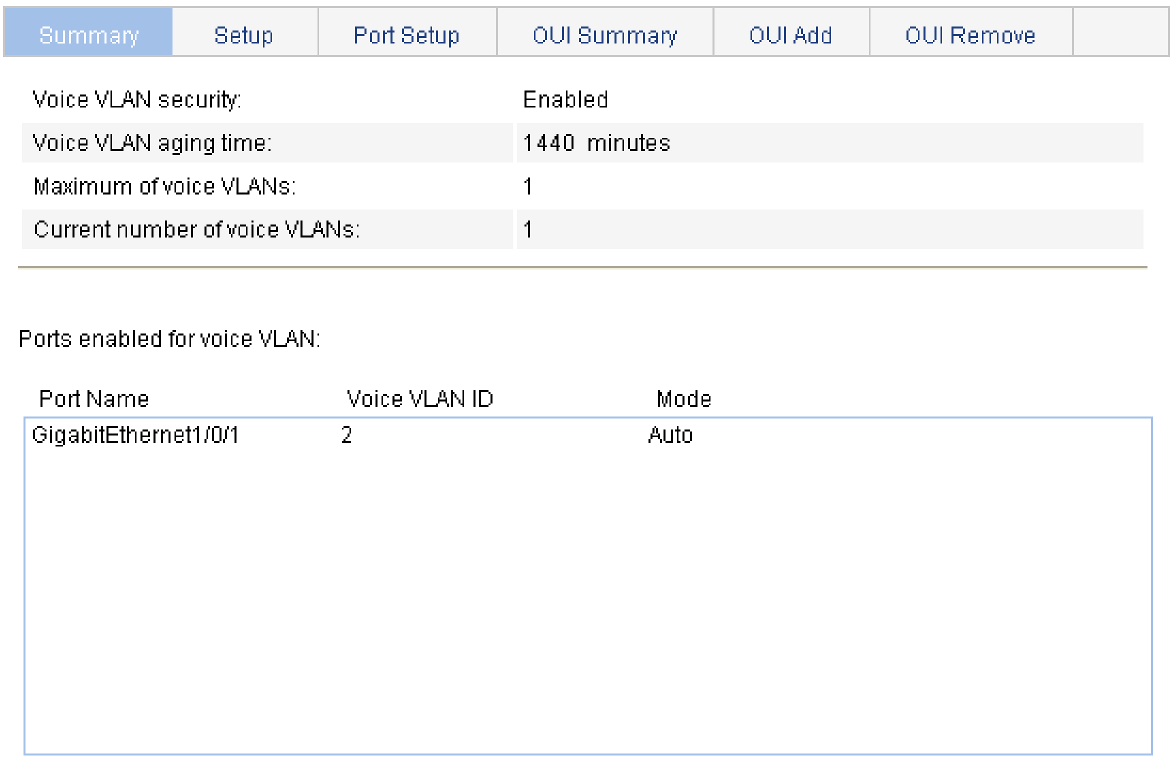
1. When the preceding configurations are complete, the **OUI Summary** tab is displayed by default, as shown in Figure 170. You can view the information about the newly-added OUI address.

Figure 170 Displaying the current OUI list of the device



2. Click the **Summary** tab, where you can view the current voice VLAN information.

Figure 171 Displaying the current voice VLAN information



Configuration guidelines

When you configure the voice VLAN function, follow these guidelines:

- To remove a VLAN functioning as a voice VLAN, disable its voice VLAN function first.

- Only one VLAN is supported and only an existing static VLAN can be configured as the voice VLAN.
- Do not enable the voice VLAN function on a link aggregation group member port.
- After you assign a port operating in manual voice VLAN assignment mode to the voice VLAN, the voice VLAN takes effect.

Configuring MAC address tables

NOTE:

- MAC address configurations related to interfaces apply only to Layer 2 Ethernet interfaces.
- This document covers only the management of static, dynamic, and blackhole MAC address entries, not multicast MAC address entries.

Overview

To reduce single-destination packet floodings in a switched LAN, an Ethernet device uses a MAC address table for forwarding frames. This table describes from which port a MAC address (or host) can be reached. When forwarding a single-destination frame, the device first looks up the destination MAC address of the frame in the MAC address table for a match. If the device finds an entry, it forwards the frame out of the outgoing port in the entry. If the device does not find an entry, it floods the frame out of all but the incoming port.

How a MAC address table entry is created

The device automatically learns entries in the MAC address table, or you can add them manually.

MAC address learning

The device can automatically populate its MAC address table by learning the source MAC addresses of incoming frames on each port.

When a frame arrives at a port, Port A, for example, the device performs the following tasks:

1. Verifies the source MAC address (for example, MAC-SOURCE) of the frame.
2. Looks up the source MAC address in the MAC address table.
3. Updates an entry if it finds one. If the device does not find an entry, it adds an entry for MAC-SOURCE and Port A.

The device performs this learning process each time it receives a frame from an unknown source MAC address, until the MAC address table is fully populated.

After learning a source MAC address, when the device receives a frame destined for MAC-SOURCE, the device finds the MAC-SOURCE entry in the MAC address table and forwards the frame out Port A.

Manually configuring MAC address entries

With dynamic MAC address learning, a device does not distinguish between illegitimate and legitimate frames. For example, when a hacker sends frames with a forged source MAC address to a port different from the one to which the real MAC address is connected, the device creates an entry for the forged MAC address, and forwards frames destined for the legal user to the hacker instead.

To improve port security, you can bind specific user devices to the port by manually adding MAC address entries to the MAC address table of the device.

Types of MAC address table entries

A MAC address table can contain the following types of entries:

- **Static entries**—Manually added and never age out.
- **Dynamic entries**—Manually added or dynamically learned, and might age out.
- **Blackhole entries**—Manually configured and never age out. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses. For example, to block all packets destined for a specific user for security concerns, you can configure the MAC address of this user as a blackhole MAC address entry.

A static or blackhole MAC address entry can overwrite a dynamic MAC address entry, but not vice versa.

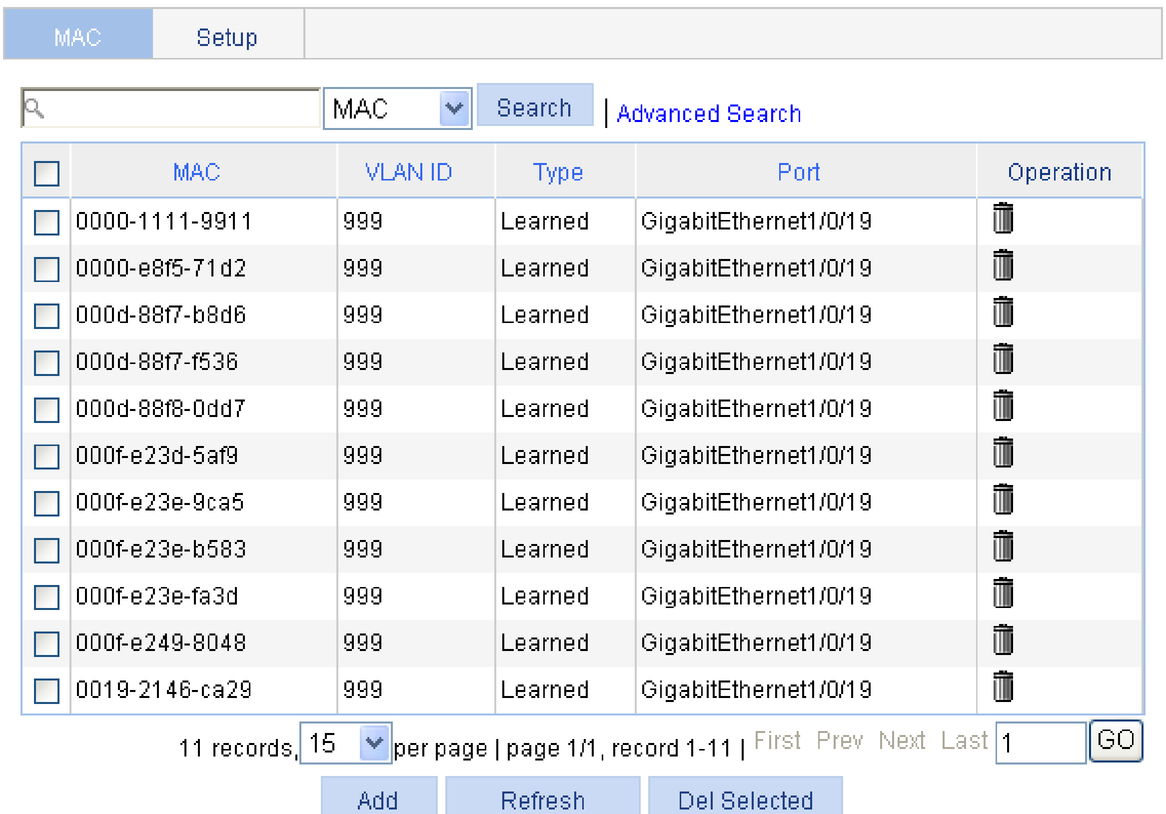
To adapt to network changes and prevent inactive entries from occupying table space, an aging mechanism is adopted for dynamic MAC address entries. Each time a dynamic MAC address entry is learned or created, an aging timer starts. If the entry has not updated when the aging timer expires, the device deletes the entry. If the entry has updated before the aging timer expires, the aging timer restarts.

Displaying and configuring MAC address entries

1. Select **Network** > **MAC** from the navigation tree.

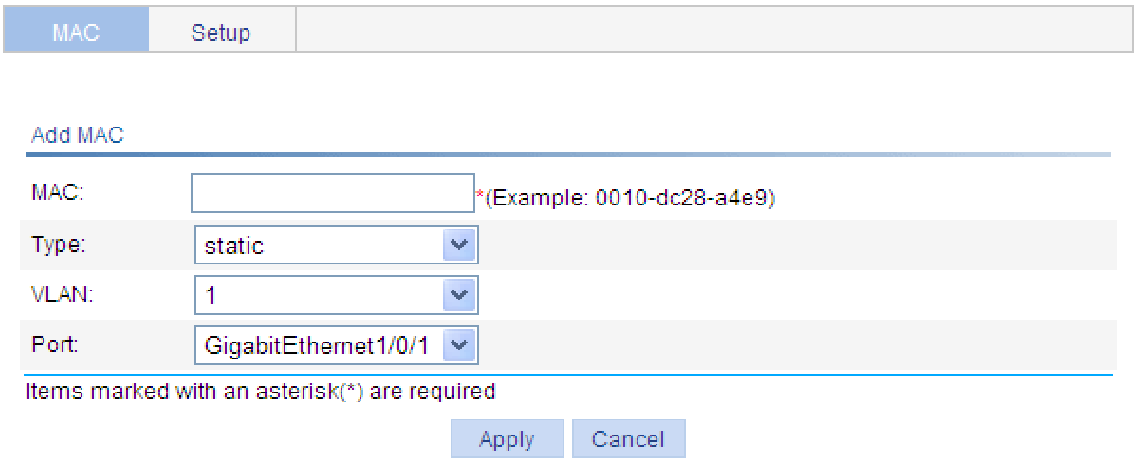
   The system automatically displays the **MAC** tab, which shows all the MAC address entries on the device, as shown in Figure 172.

Figure 172 The MAC tab



2. Click **Add** in the bottom to enter the page for creating MAC address entries, as shown in Figure 173.

Figure 173 Create a MAC address entry



3. Configure a MAC address entry.
4. Click **Apply**.

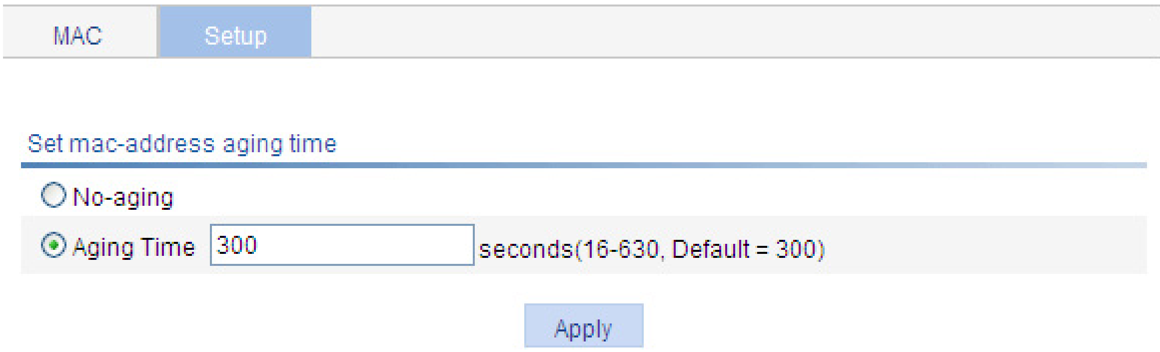
Table 52 Configuration items

Item	Description
MAC	Set the MAC address to be added.
Type	Set the type of the MAC address entry: • **Static**—Static MAC address entries that never age out. • **Dynamic**—Dynamic MAC address entries that will age out. • **Blackhole**—Blackhole MAC address entries that never age out. IMPORTANT: The tab displays the following types of MAC address entries: • **Config static**—Static MAC address entries manually configured by the users. • **Config dynamic**—Dynamic MAC address entries manually configured by the users. • **Blackhole**—Blackhole MAC address entries. • **Learned**—Dynamic MAC address entries learned by the device. • **Other**—Other types of MAC address entries.
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

1. Select **Network** > **MAC** from the navigation tree.
2. Click the **Setup** tab to enter the page for setting the MAC address entry aging time, as shown in Figure 174.

Figure 174 Set the aging time for MAC address entries



3. Configure the aging time for MAC address entries.
4. Click **Apply**.

Table 53 Configuration items

Item	Description
No-aging	Specify that the MAC address entry never ages out.
Aging time	Set the aging time for the MAC address entry

MAC address configuration example

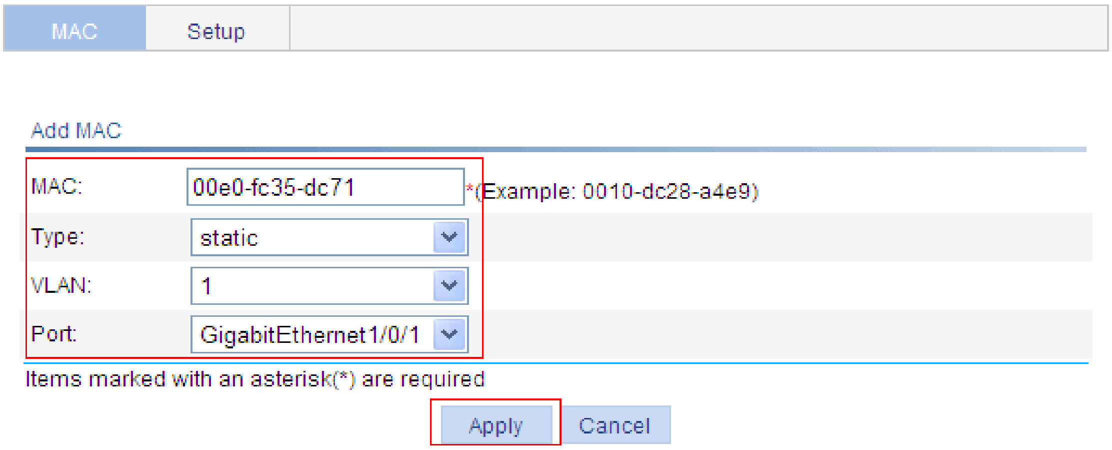
Network requirements

Use the Web-based NMS to configure the MAC address table of the device. Add a static MAC address 00e0-fc35-dc71 under GigabitEthernet 1/0/1 in VLAN 1.

Creating a static MAC address entry

1. Select **Network** > **MAC** from the navigation tree.
   By default, the **MAC** tab is displayed.
2. Click **Add**.
   The page shown in Figure 175 appears.
3. Configure a MAC address entry:
   a. Enter MAC address **00e0-fc35-dc71**.
   b. Select **static** in the **Type** list.
   c. Select **1** in the **VLAN** list.
   d. Select **GigabitEthernet1/0/1** in the **Port** list.
4. Click **Apply**.

Figure 175 Create a static MAC address entry



Configuring MSTP

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.

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.

STP protocol packets

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 have the following 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 bridge. There is only one root bridge in the entire network. The root bridge is not fixed, but can change along with changes of the network topology.

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 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

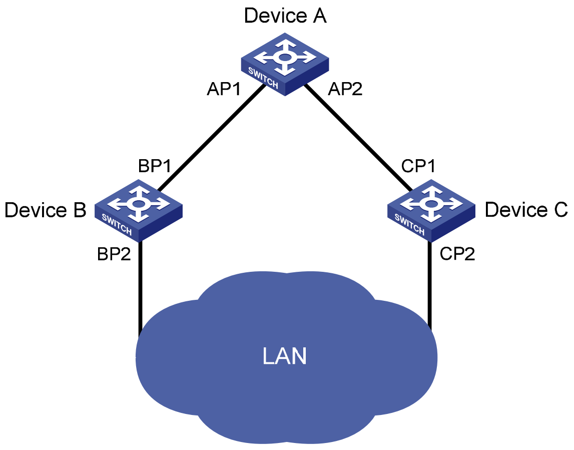
Table 54 Description of designated bridges and designated ports:

Classification	Designated bridge	Designated port
For a device	A device directly connected to 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 176, 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.
- Device B and Device C are connected to the LAN. 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 176 Designated bridges and designated ports



NOTE:

All the ports on the root bridge are 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.

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. A configuration BPDU includes the following important fields:

- **Root bridge ID**—Consisting of the priority and MAC address of the root bridge.
- **Root path cost**—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**—Delay used by STP bridges to transit the state of the root and designated ports to forwarding.

NOTE:

For simplicity, the descriptions and examples in this document involve only the following 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.

Table 55 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:

Configuration BPDU comparison uses the following principles:

- 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. For example, 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

Table 56 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.
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.

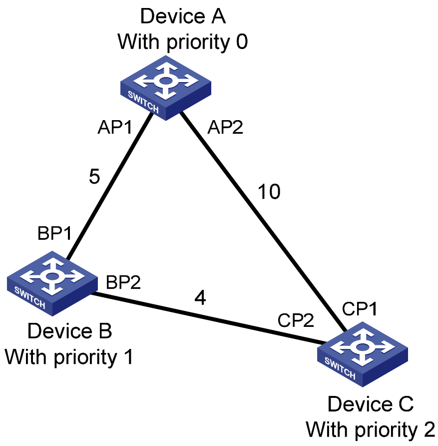
NOTE:

When the network topology is stable, only the root port and designated ports forward traffic, and other ports are all in the blocked state and 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 177, 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 177 STP network



- Initial state of each device

Table 57 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 C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

Table 58 Comparison process and result on each device

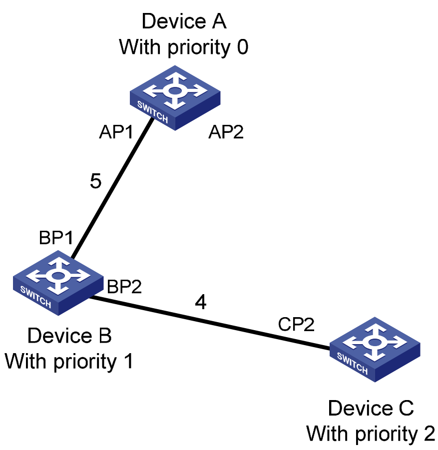
Device	Comparison process	BPDU of port after comparison
Device A	• Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the received configuration BPDU, and discards the received configuration BPDU. • 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 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. 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}

<table>
<tr><th>Device</th><th>Comparison process</th><th>BPDU of port after comparison</th></tr>
<tr><td rowspan="2">Device B</td><td>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 discards the received configuration BPDU.</td><td>BP1: {0, 0, 0, AP1}
BP2: {1, 0, 1, BP2}</td></tr>
<tr><td>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.</td><td>Root port BP1:
{0, 0, 0, AP1}
Designated port BP2:
{0, 5, 1, BP2}</td></tr>
<tr><td rowspan="3">Device C</td><td>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 updates the configuration BPDU of CP2.</td><td>CP1: {0, 0, 0, AP2}
CP2: {1, 0, 1, BP2}</td></tr>
<tr><td>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.</td><td>Root port CP1:
{0, 0, 0, AP2}
Designated port CP2:
{0, 10, 2, CP2}</td></tr>
<tr><td>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.</td><td>CP1: {0, 0, 0, AP2}
CP2: {0, 5, 1, BP2}</td></tr>
</table>

Device	Comparison process	BPDU of port after comparison
	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 Table 58, a spanning tree with Device A as the root bridge is established as shown in Figure 178.

Figure 178 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

The BPDUs are forwarded following these guidelines:

- 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. 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 the following timers: 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 make sure 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 make sure 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.

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.

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 to 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 to 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.

MSTP

Why MSTP

STP and RSTP limitations

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—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 IEEE 802.1s, MSTP overcomes the limitations 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, providing a better load sharing mechanism for redundant links.

MSTP delivers the following features:

- 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, avoiding proliferation and endless cycling of packets in a loop network. In addition, it provides multiple redundant paths for data forwarding, supporting load balancing of VLAN data.
- MSTP is compatible with STP and RSTP.

Basic concepts in MSTP

Figure 179 shows a switched network that comprises four MST regions, each MST region comprising four MSTP devices. Figure 180 shows the networking topology of MST region 3.

Figure 179 Basic concepts in MSTP

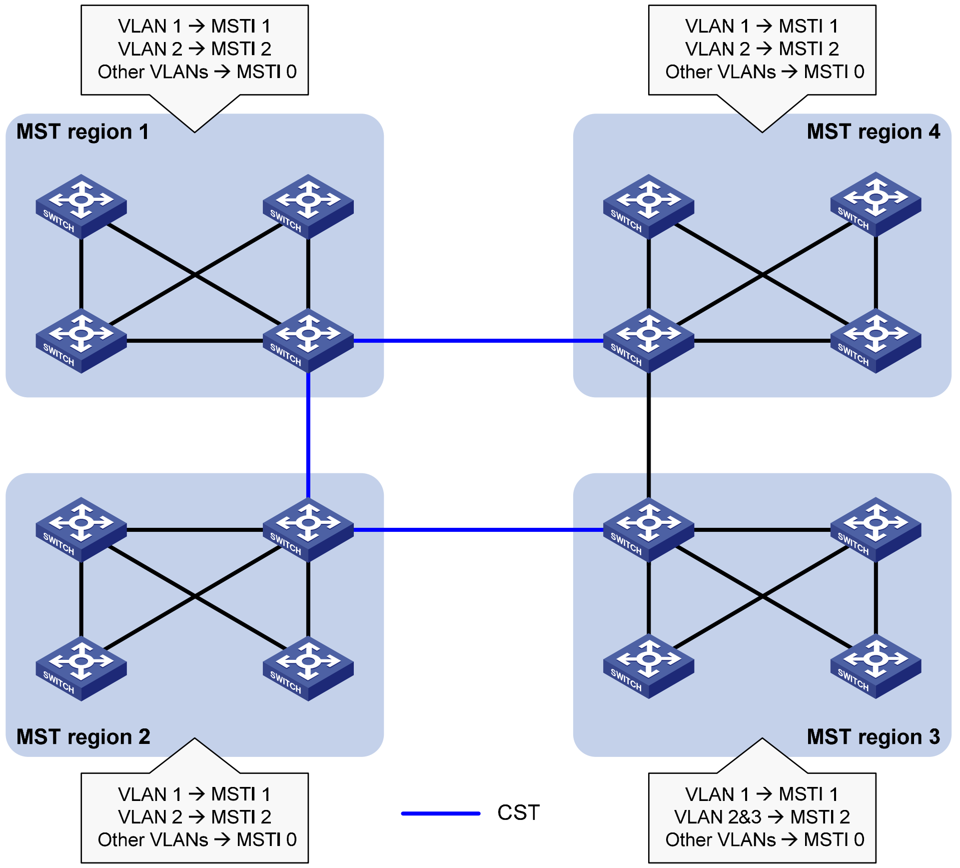
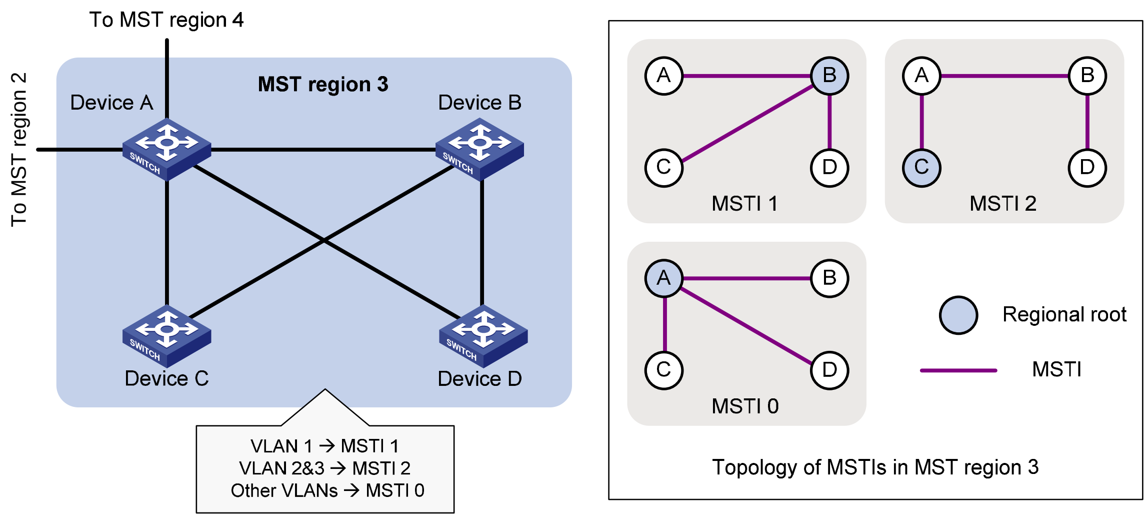


Figure 180 Network diagram and topology of MST region 3



MST region

A multiple spanning tree region (MST region) consists of multiple devices in a switched network and the network segments among them. All these devices have the following characteristics:

- A spanning tree protocol enabled
- Same region name

- Same VLAN-to-instance mapping configuration
- Same MSTP revision level
- Physically linked together

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region. In Figure 179, the switched network comprises four MST regions, MST region 1 through MST region 4, and all devices in each MST region have the same MST region configuration.

MSTI

MSTP can generate multiple independent spanning trees in an MST region, and each spanning tree is mapped to the specific VLANs. Each spanning tree is referred to as a "multiple spanning tree instance (MSTI)".

In Figure 180, MST region 3 comprises three MSTIs, MSTI 1, MSTI 2, and MSTI 0.

VLAN-to-instance mapping table

As an attribute of an MST region, the VLAN-to-instance mapping table describes the mapping relationships between VLANs and MSTIs.

In Figure 180, the VLAN-to-instance mapping table of MST region 3 is: VLAN 1 to MSTI 1, VLAN 2 and VLAN 3 to MSTI 2, and other VLANs to MSTI 0. MSTP achieves load balancing by means of the VLAN-to-instance mapping table.

CST

The common spanning tree (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.

The blue lines in Figure 179 represent the CST.

IST

An internal spanning tree (IST) is a spanning tree that runs in an MST region. It is also called MSTI 0, a special MSTI to which all VLANs are mapped by default.

In Figure 179, MSTI 0 is the IST in MST region 3.

CIST

The common and internal spanning tree (CIST) is a single spanning tree that connects all devices in a switched network. It consists of the ISTs in all MST regions and the CST.

In Figure 179, the ISTs (MSTI 0) in all MST regions plus the inter-region CST constitute the CIST of the entire network.

Regional root

The root bridge of the IST or an MSTI within an MST region is the regional root of the IST or MSTI. Based on the topology, different spanning trees in an MST region might have different regional roots.

In MST region 3 in Figure 180, the regional root of MSTI 1 is Device B, the regional root of MSTI 2 is Device C, and the regional root of MSTI 0 (also known as the IST) is Device A.

Common root bridge

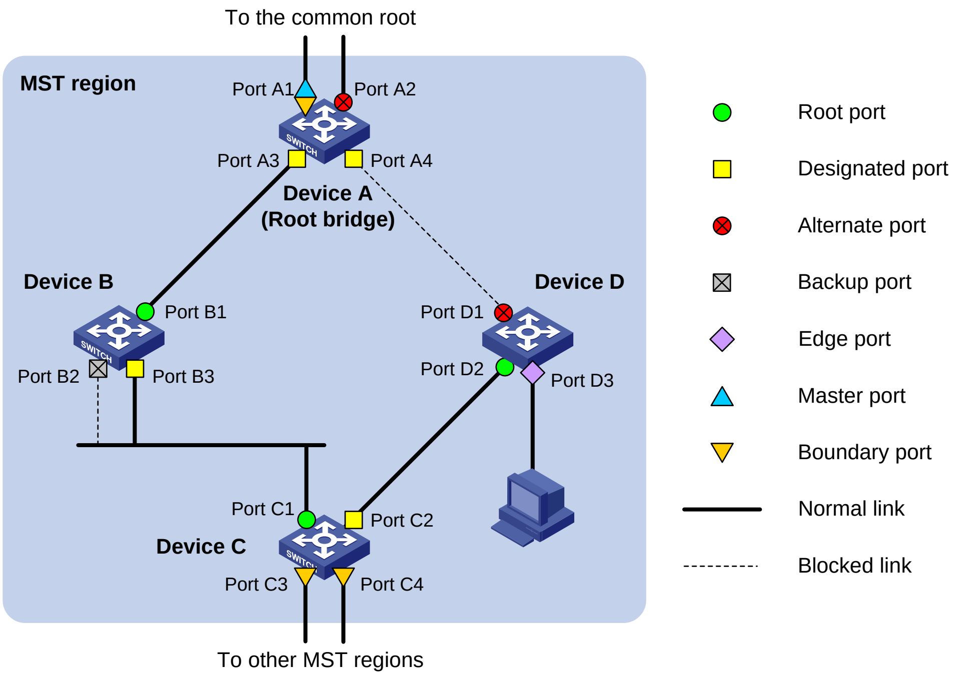
The common root bridge is the root bridge of the CIST.

In Figure 179, the common root bridge is a device in MST region 1.

Port roles

A port can play different roles in different MSTIs. As shown in Figure 181, an MST region comprises Device A, Device B, Device C, and Device D. Port A1 and port A2 of Device A connect to the common root bridge. Port B2 and Port B3 of Device B form a loop. Port C3 and Port C4 of Device C connect to other MST regions. Port D3 of Device D directly connects to a host.

Figure 181 Port roles



MSTP calculation involves the following port roles:

- **Root port**—Forwards data for a non-root bridge to the root bridge. The root bridge does not have any root port.
- **Designated port**—Forwards data to the downstream network segment or device.
- **Alternate port**—The backup port for a root port or master port. When the root port or master port is blocked, the alternate port takes over.
- **Backup port**—The backup port of a designated port. When the designated port is invalid, the backup port becomes the new designated port. A loop occurs when two ports of the same spanning tree device are interconnected, so the device blocks one of the ports. The blocked port acts as the backup.
- **Edge port**—An edge port does not connect to any network device or network segment, but directly connects to a user host.
- **Master port**—A port on the shortest path from the local MST region to the common root bridge. The master port is not always located on the regional root. It is a root port on the IST or CIST and still a master port on the other MSTIs.
- **Boundary port**—Connects an MST region to another MST region or to an STP/RSTP-running device. In MSTP calculation, a boundary port's role on an MSTI is consistent with its role on the CIST. But that is not true with master ports. A master port on MSTIs is a root port on the CIST.

Port states

In MSTP, a port can be in one of the following states:

- **Forwarding**—The port receives and sends BPDUs, learns MAC addresses, and forwards user traffic.
- **Learning**—The port receives and sends BPDUs, learns MAC addresses, but does not forward user traffic. Learning is an intermediate port state.
- **Discarding**—The port receives and sends BPDUs, but does not learn MAC addresses or forward user traffic.

NOTE:

When in different MSTIs, a port can be in different states.

A port state is not exclusively associated with a port role. Table 59 lists the port states that each port role supports. (A check mark [√] indicates that the port supports this state, while a dash [—] indicates that the port does not support this state.)

Table 59 Port states that different port roles support

Port role (right) Port state (below)	Root port/master port	Designated 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 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 more information, see "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

- IEEE 802.1d, *Spanning Tree Protocol*
- IEEE 802.1w, *Rapid Spanning Tree Protocol*
- IEEE 802.1s, *Multiple Spanning Tree Protocol*

Recommended MSTP configuration procedure

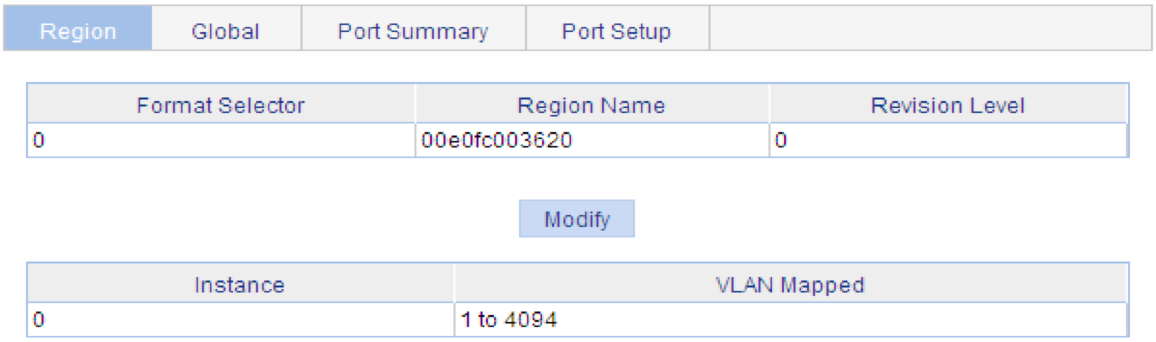
Step	Remarks
1. Configuring an MST region	(Optional.) Configure the MST region-related parameters and VLAN-to-MSTI mappings. By default, the MST region-related parameters adopt the default values, and all VLANs in an MST region are mapped to MSTI 0.
2. Configuring MSTP globally	(Required.) Enable STP globally and configure MSTP parameters. Whether STP is enabled globally depends on the device model; all MSTP parameters have default values.
3. 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.
4. 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

1. Select **Network** > **MSTP** from the navigation tree.

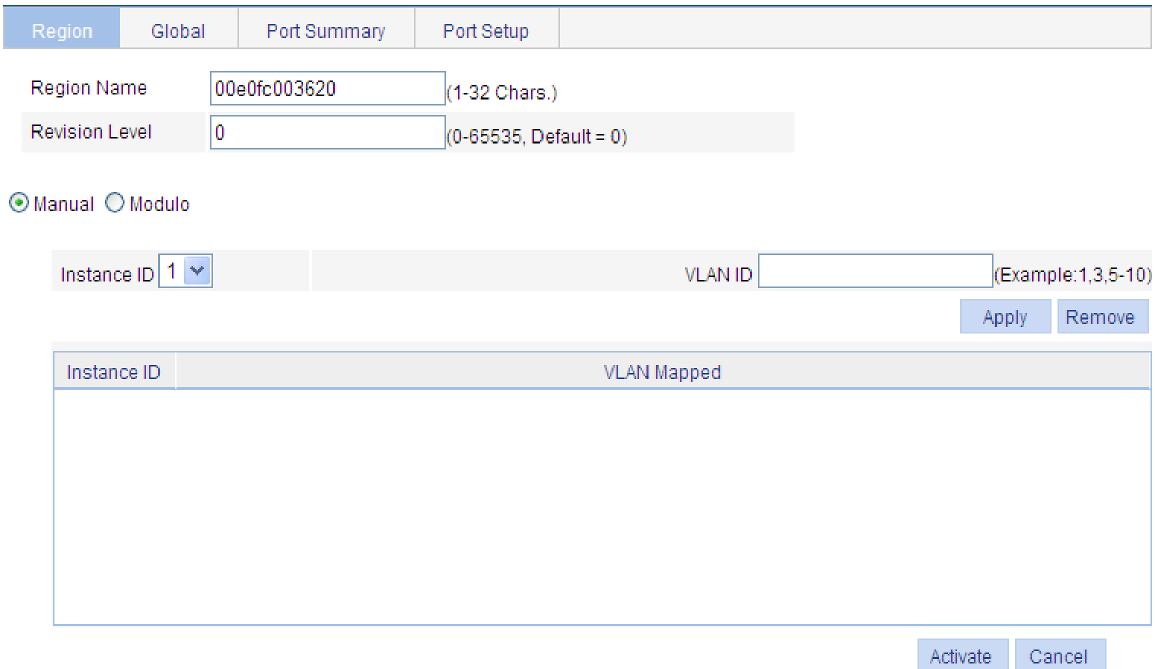
   By default, the **Region** tab is displayed.

Figure 182 MST region



2. Click **Modify** to enter the page for configuring MST regions.

Figure 183 Configuring an MST region



3. Configure the MST region information as described in Table 60, and click **Apply**.
4. Click **Activate**.

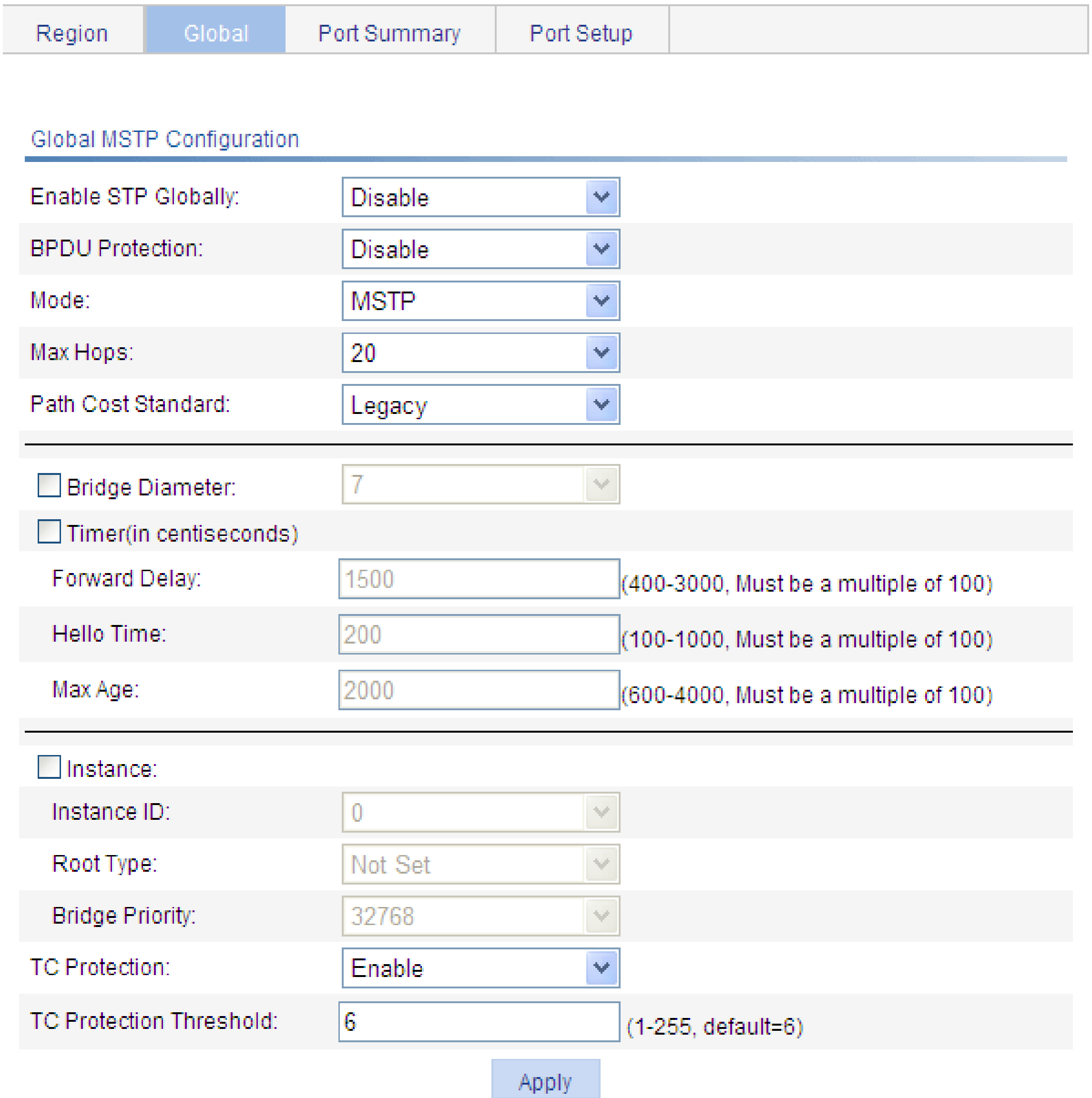
Table 60 Configuration items

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 and VLAN ID)	Manually add VLAN-to-MSTI mappings. Click **Apply** to add the VLAN-to-MSTI mapping entries to the list.
Modulo	The device automatically maps 4094 VLANs to the corresponding MSTIs based on the modulo value.

Configuring MSTP globally

1. Select **Network** > **MSTP** from the navigation tree.
2. Click the **Global** tab to enter the page for configuring MSTP globally.

Figure 184 Configuring MSTP globally



3. Configure the global MSTP configuration as described in Table 61.
4. Click **Apply**.

Table 61 Configuration items

Item	Description
Enable STP Globally	Select whether to enable STP globally. Other MSTP configurations take effect only after you enable STP globally.

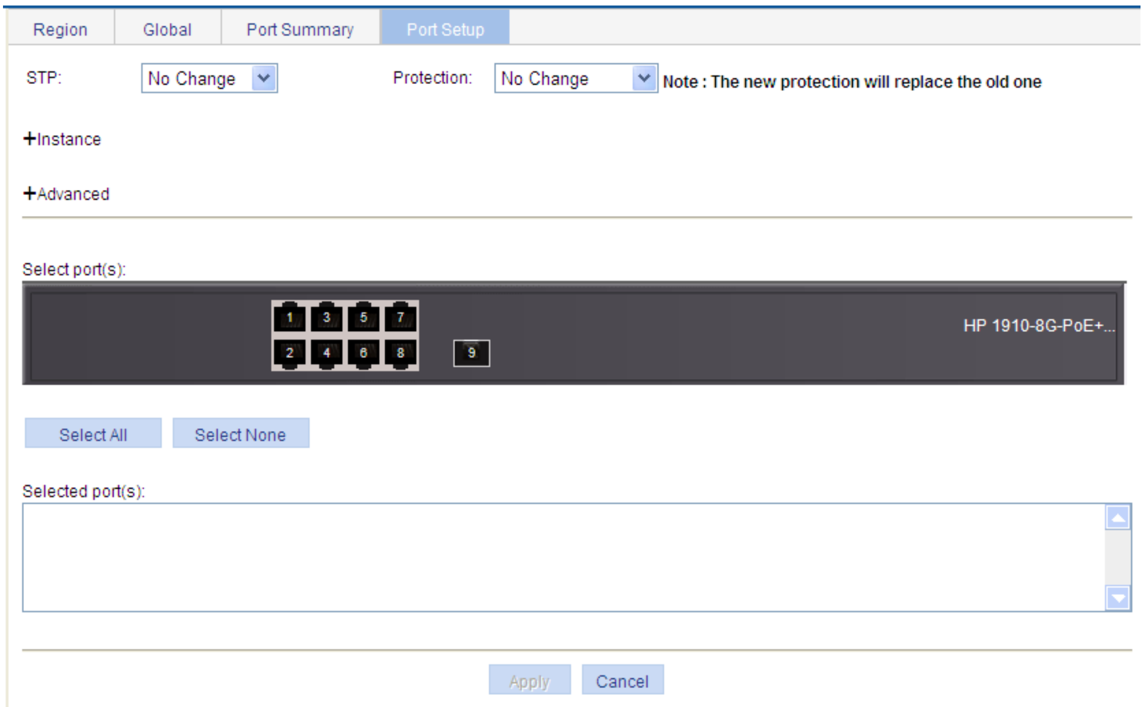
<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>BPDU Guard</td><td>Select whether to enable BPDU guard.
BPDU guard can protect the device from malicious BPDU attacks, making the network topology stable.</td></tr>
<tr><td>Mode</td><td>Set the operating mode of STP:
STP—Each port on a device 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.</td></tr>
<tr><td>Max Hops</td><td>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.</td></tr>
<tr><td>Path Cost Standard</td><td>Specify the standard for path cost calculation. It can be Legacy, IEEE 802.1D-1998, or IEEE 802.1T.</td></tr>
<tr><td>Bridge Diameter</td><td>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.
IMPORTANT:
The configured network diameter is effective for CIST only, not for MSTIs.
The bridge diameter cannot be configured together with the timers.</td></tr>
<tr><td>Timers</td><td>Forward Delay
Set the delay for the root and designated ports to transit to the forwarding state.
Hello Time
Set the interval at which the device sends hello packets to the surrounding devices to make sure that the paths are fault-free.
Max Age
Set the maximum length of time a configuration BPDU can be held by the device.
IMPORTANT:
The settings of hello time, forward delay and max age must meet a certain formula. Otherwise, the network topology will not be stable. HP recommends you 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.</td></tr>
<tr><td>Instance (Instance ID, Root Type, and Bridge Priority)</td><td>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).</td></tr>
</table>

Item	Description
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. NOTE: HP does not recommend you 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.

Configuring MSTP on a port

1. Select **Network** > **MSTP** from the navigation tree.
2. Click the **Port Setup** tab to enter the page for configuring MSTP on ports.

Figure 185 MSTP configuration on a port



3. Configure MSTP for ports as described in Table 62.
4. Click **Apply**.

Table 62 Configuration items

Item	Description
STP	Select whether to enable STP on the port.

Item	Description
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**—For more information, see Table 63.
Instance (Instance ID, Port Priority, Auto Path Cost, and Manual Path Cost)	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, 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, achieving VLAN-based load balancing. The device can automatically calculate the default path cost; alternatively, you can also manually configure path cost for ports.
Advanced	• Point to Point Specify whether the port is connected to a point-to-point link: ○ **Auto**—Configure the device to automatically detect whether or not the link type of the port is point-to-point. ○ **Force False**—The link type for the port is not point-to-point link. ○ **Force True**—The link type for the port is point-to-point link. IMPORTANT: 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. HP recommends that you 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 operating 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 63 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. HP recommends that you 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. 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.

Displaying MSTP information of a port

1. Select **Network** > **MSTP** from the navigation tree.
2. Click the **Port Summary** tab.
3. 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.

Figure 186 The port summary tab

Table 64 Field description

Field	Description
[FORWARDING]	The port is in forwarding state, so the port learns MAC addresses and forwards user traffic.
[LEARNING]	The port is in learning state, so the port learns MAC addresses but does not forward user traffic.
[DISCARDING]	The port is in discarding state, so 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.

Field	Description
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,: • **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.
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.

MSTP configuration example

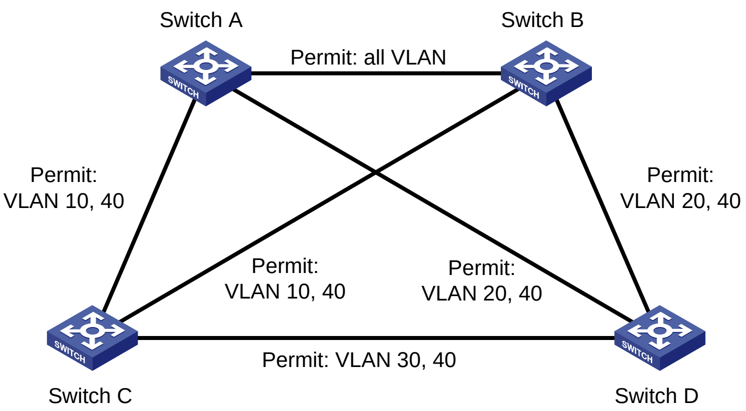
Network requirements

As shown in Figure 187, configure MSTP so that:

- 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, and the root bridge of MSTI 3 is Switch C.

Figure 187 Network diagram



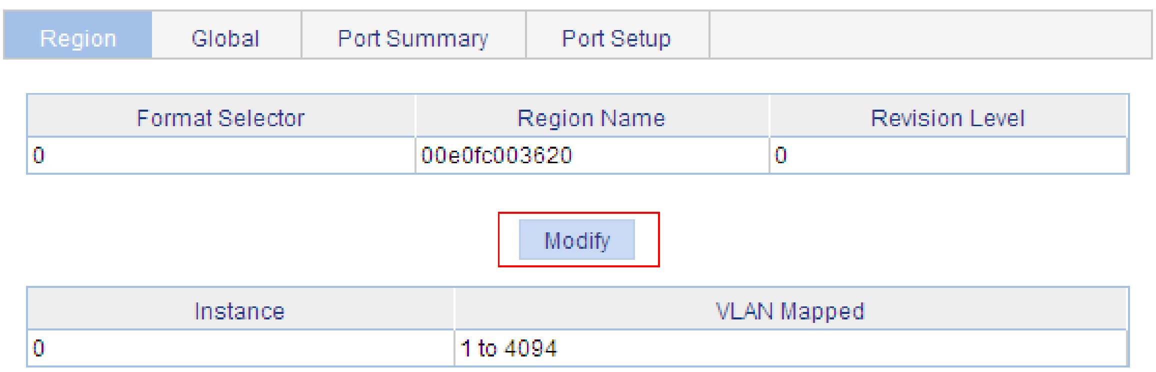
NOTE:

"Permit:" next to a link in the figure is followed by the VLANs the packets of which are permitted to pass this link.

Configuring Switch A

1. Configure an MST region:
   a. Select **Network** > **MSTP** from the navigation tree.
      By default, the **Region** tab is displayed.
   b. Click the **Modify** button to enter the page for configuring MST regions.

Figure 188 The region tab



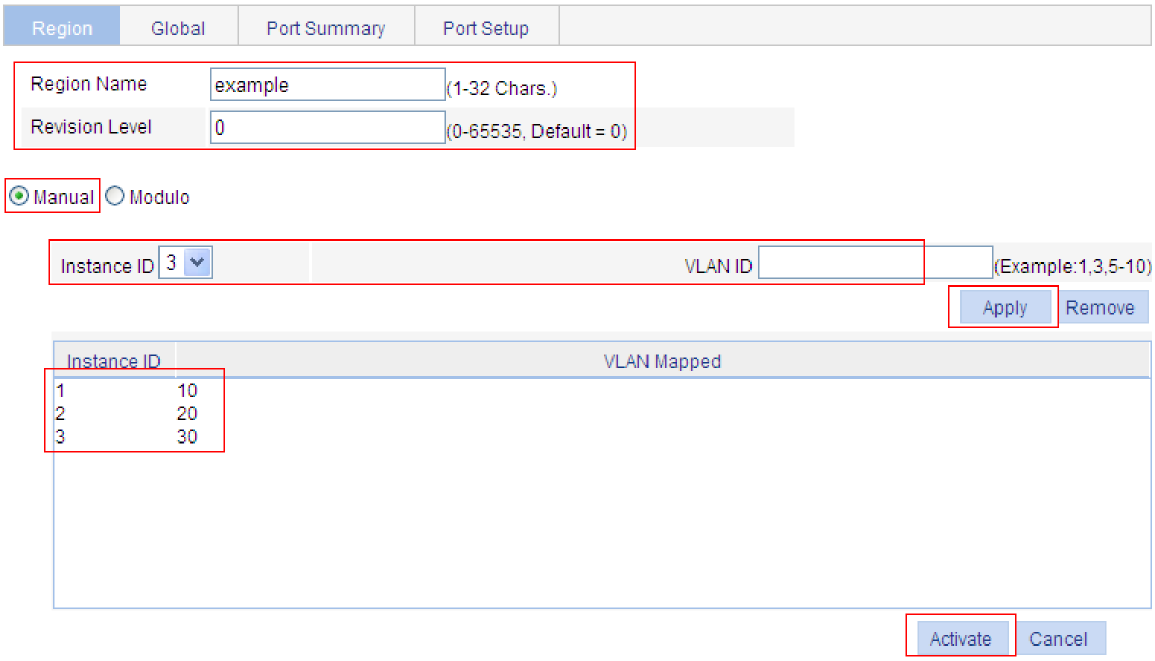
   c. Set the region name to **example**.
   d. Set the revision level to 0.
   e. Select the **Manual** option.
   f. Select 1 in the **Instance ID** list.
   g. Set the VLAN ID to 10.

h. Click **Apply** to map VLAN 10 to MSTI 1 and add the VLAN-to-MSTI mapping entry to the VLAN-to-MSTI mapping list.

i. Repeat the preceding three steps 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.

j. Click **Activate**.

Figure 189 Configuring an MST region



2. Configure MSTP globally:

a. Select **Network** > **MSTP** from the navigation tree.

b. Click the **Global** tab to enter the page for configuring MSTP globally.

c. Select **Enable** in the **Enable STP Globally** list.

d. Select **MSTP** in the **Mode** list.

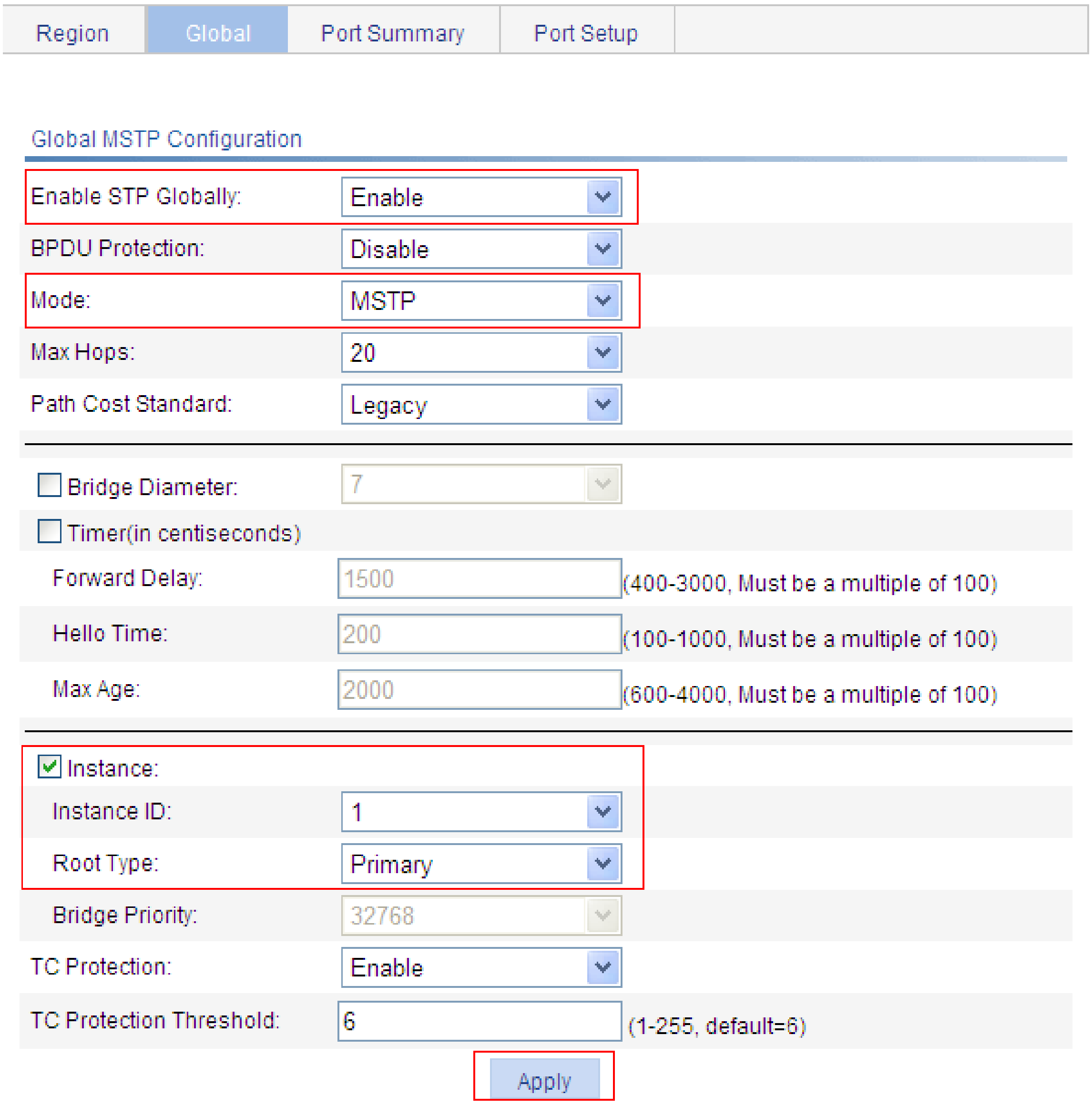
e. Select the box before **Instance**.

f. Set the **Instance ID** field to 1.

g. Set the **Root Type** field to **Primary**.

h. Click **Apply**.

Figure 190 Configuring MSTP globally (on Switch A)



Configuring Switch B

1. Configure an MST region. (The procedure here is the same as that of configuring an MST region on Switch A.)
2. Configure MSTP globally:
   a. Select **Network** > **MSTP** from the navigation tree.
   b. Click the **Global** tab to enter the page for configuring MSTP globally.
   c. Select **Enable** in the **Enable STP Globally** list.
   d. Select **MSTP** in the **Mode** list.
   e. Select the box before **Instance**.
   f. Set the **Instance ID** field to 2.
   g. Set the **Root Type** field to **Primary**.
   h. Click **Apply**.

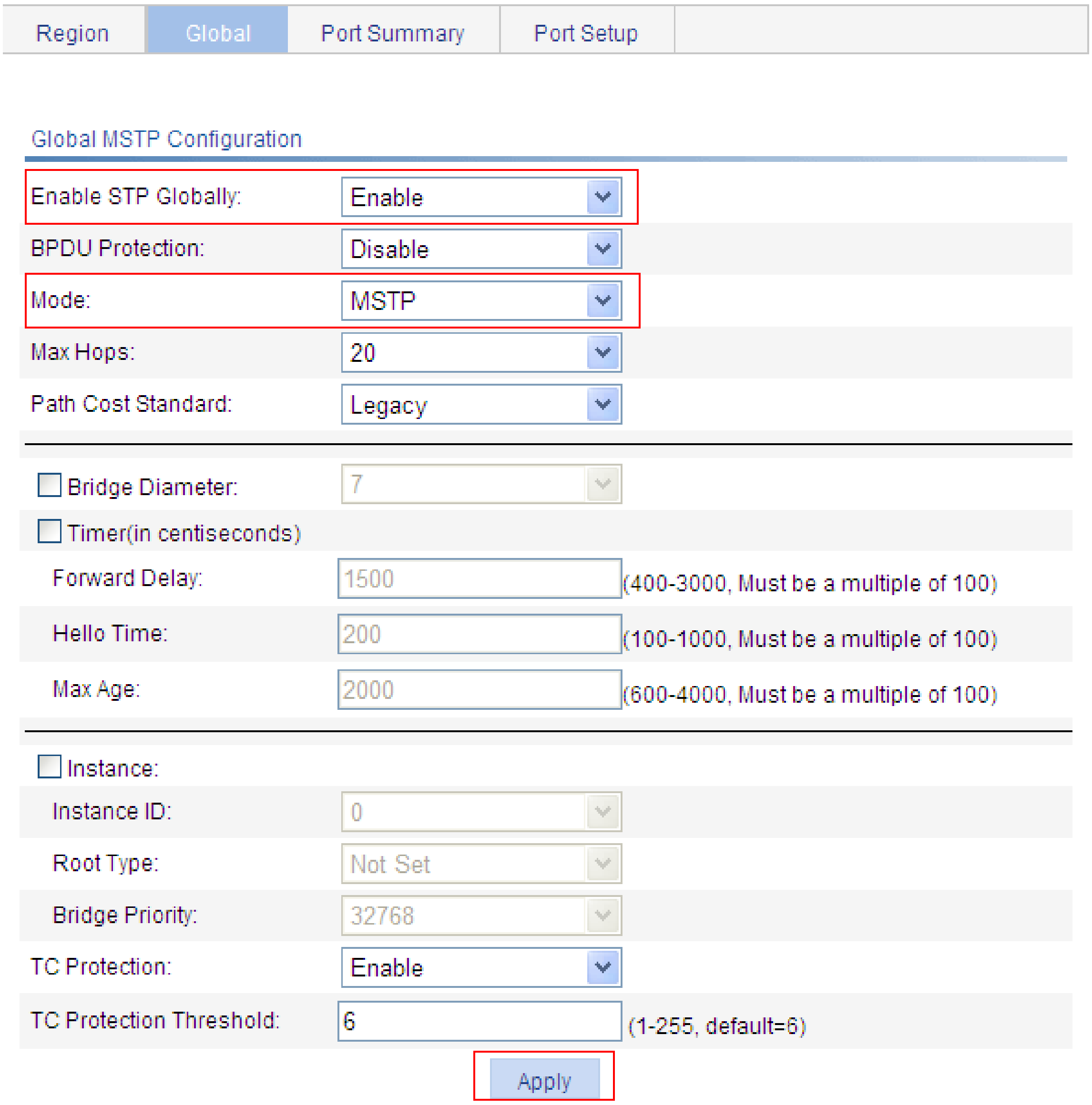
Configuring Switch C

1. Configure an MST region. (The procedure here is the same as that of configuring an MST region on Switch A.)
2. Configure MSTP globally:
   a. Select **Network** > **MSTP** from the navigation tree.
   b. Click **Global** to enter the page for configuring MSTP globally.
   c. Select **Enable** in the **Enable STP Globally** list.
   d. Select **MSTP** in the **Mode** list.
   e. Select the box before **Instance**.
   f. Set the **Instance ID** field to 3.
   g. Set the **Root Type** field to **Primary**.
   h. Click **Apply**.

Configuring Switch D

1. Configure an MST region. The procedure is the same as that of configuring an MST region on Switch A.
2. Configure MSTP globally:
   a. Select **Network** > **MSTP** from the navigation tree.
   b. Click **Global** to enter the page for configuring MSTP globally.
   c. Select **Enable** in the **Enable STP Globally** list.
   d. Select **MSTP** in the **Mode** list.
   e. Click **Apply**.

Figure 191 Configuring MSTP globally (on Switch D)



Configuration guidelines

Follow these guidelines when you configure 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 an edge port receives a BPDU from another port, it transits into a non-edge port. To restore its port role as an edge port, you need to restart the port.
- Configure ports that are directly connected to terminals as edge 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.

Configuring link aggregation and LACP

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

Aggregation group, member port, and aggregate interface

Link aggregation is implemented through link aggregation groups. An aggregation group is a group of Ethernet interfaces combined together, which are called "member ports" of the aggregation group. For each aggregation group, a logical interface, called an "aggregate interface", is created.

States of the member ports in an aggregation group

A member port in an aggregation group can be in one of the following 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. All selected member ports use the same duplex mode.

For how the state of a member port is determined, see "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, see "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 65. In an aggregation group, a member port different from the aggregate interface in the class-two configurations cannot be a Selected port.

Table 65 Class-two configurations

Type	Considerations
Port isolation	Whether a port has joined an isolation group, and the isolation group that the port belongs to
VLAN	Permitted VLAN IDs, default VLAN, link type (trunk, hybrid, or access), IP subnet-based VLAN configuration, protocol-based VLAN configuration, tag mode
MAC address learning	MAC address learning capability, MAC address learning limit, forwarding of frames with unknown destination MAC addresses after the upper limit of the MAC address table is reached

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.
- The change of a class-two configuration setting may affect the select state of link aggregation member ports and 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.

Link aggregation modes

Depending on the link aggregation procedure, link aggregation operates in one of the following 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.
- 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 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 Selected state and those with greater port numbers in 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, for example, as a result of the inter-board aggregation restriction.

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 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 negotiation procedure applies:
   - 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. If they are the same, compare the system MAC addresses. The system with the smaller MAC address wins.
   - 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. If two ports are with the same LACP priority, compare their port numbers. The port with the 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, also changes the state of its ports.
2. Set the ports that cannot aggregate with the reference port to the Unselected state, for example, as the result of the inter-board aggregation restriction.

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.
- 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 affect services. HP recommends that you do that with caution.

Recommended link aggregation and LACP configuration procedures

Recommended static aggregation group configuration procedure

Step	Remarks
1. 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.
2. Displaying information of an aggregate interface	Optional. Perform this task to view detailed information of an existing aggregation group.

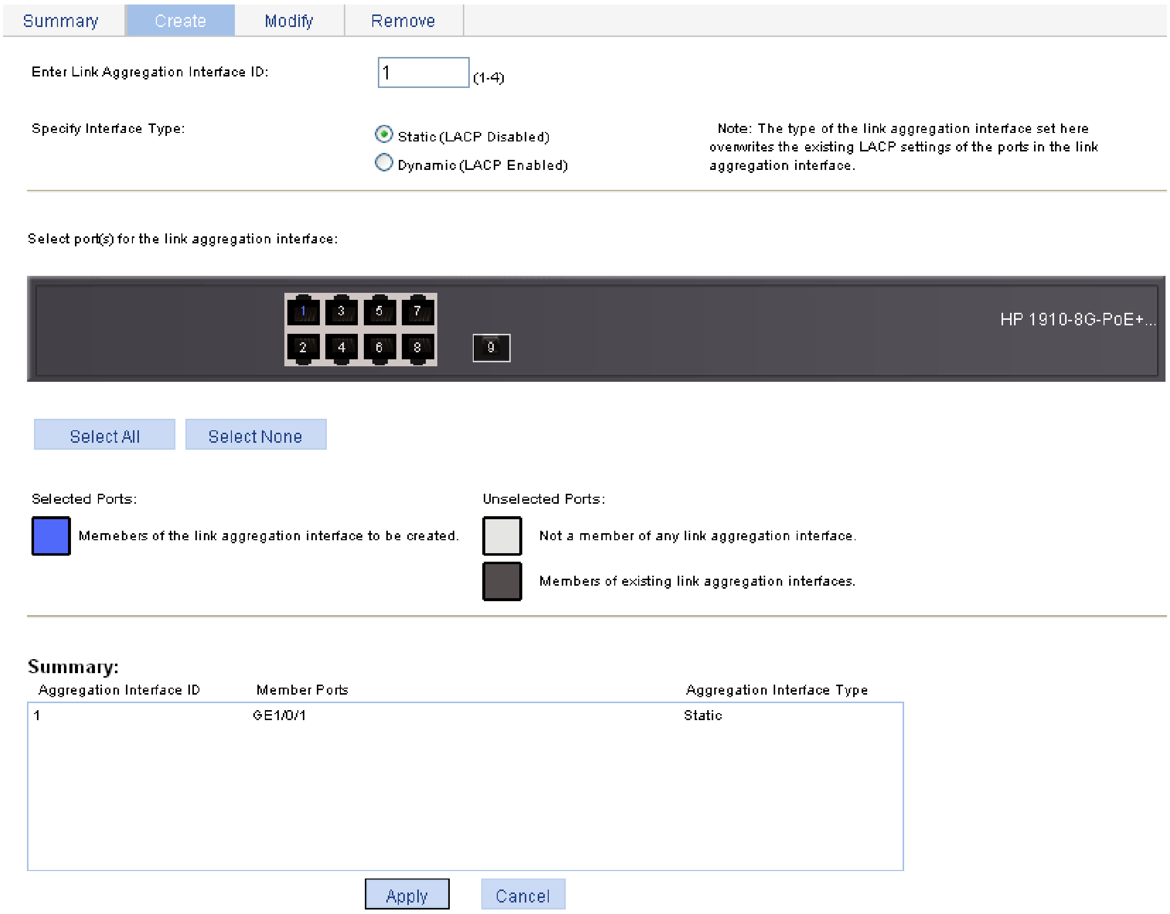
Recommended dynamic aggregation group configuration procedure

Step	Remarks
1. 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.
2. Displaying information of an aggregate interface	Optional. Perform this task to view detailed information of an existing aggregation group.
3. 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.
4. 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

1. Select **Network** > **Link Aggregation** from the navigation tree.
2. Click **Create** to enter the page as shown in Figure 192.

Figure 192 Create a link aggregation group



3. Configure a link aggregation group.
4. Click **Apply**.

Table 66 Configuration items

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** area 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** area at the bottom of the page.

Displaying information of an aggregate interface

1. Select **Network** > **Link Aggregation** from the navigation tree.

   The **Summary** tab is displayed by default, as shown in Figure 193. The list on the upper part of the page displays information about all the aggregate interfaces.
2. Select an aggregate interface from the list.

The list on the lower part of the page displays the detailed information about the member ports of the corresponding link aggregation group.

Figure 193 Displaying information of an aggregate interface

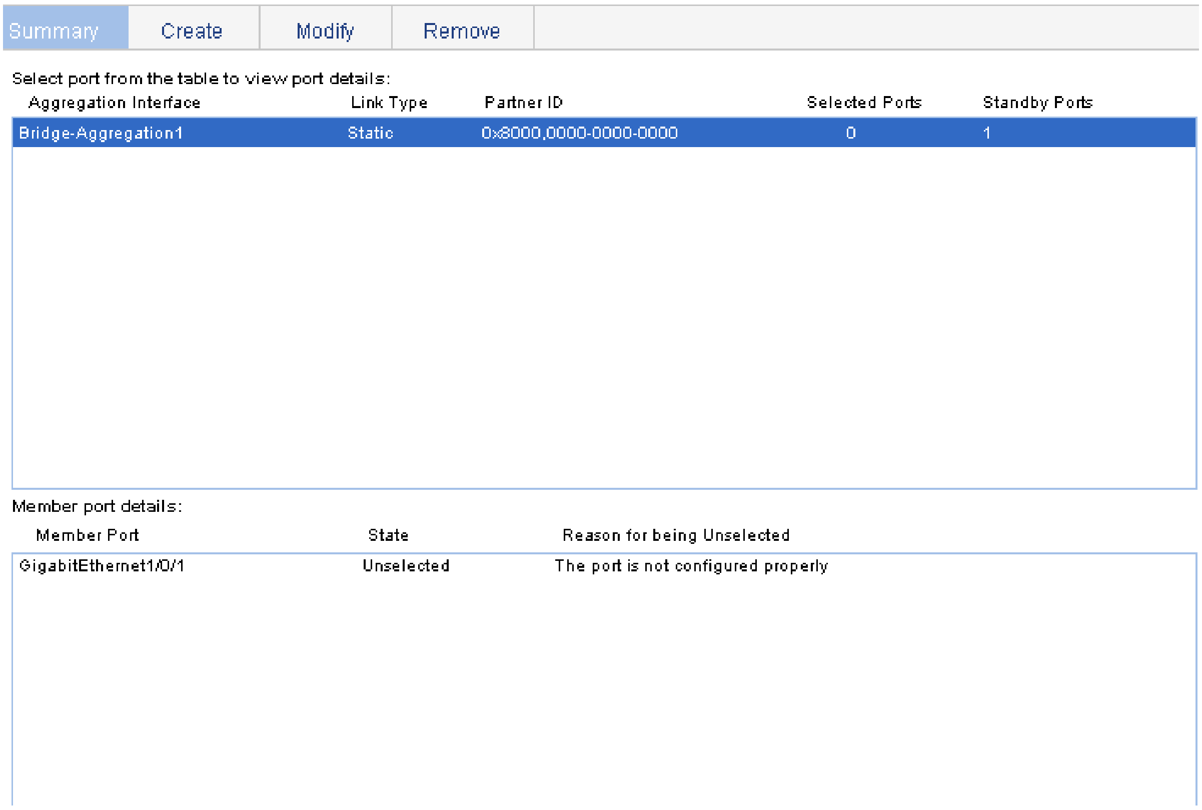


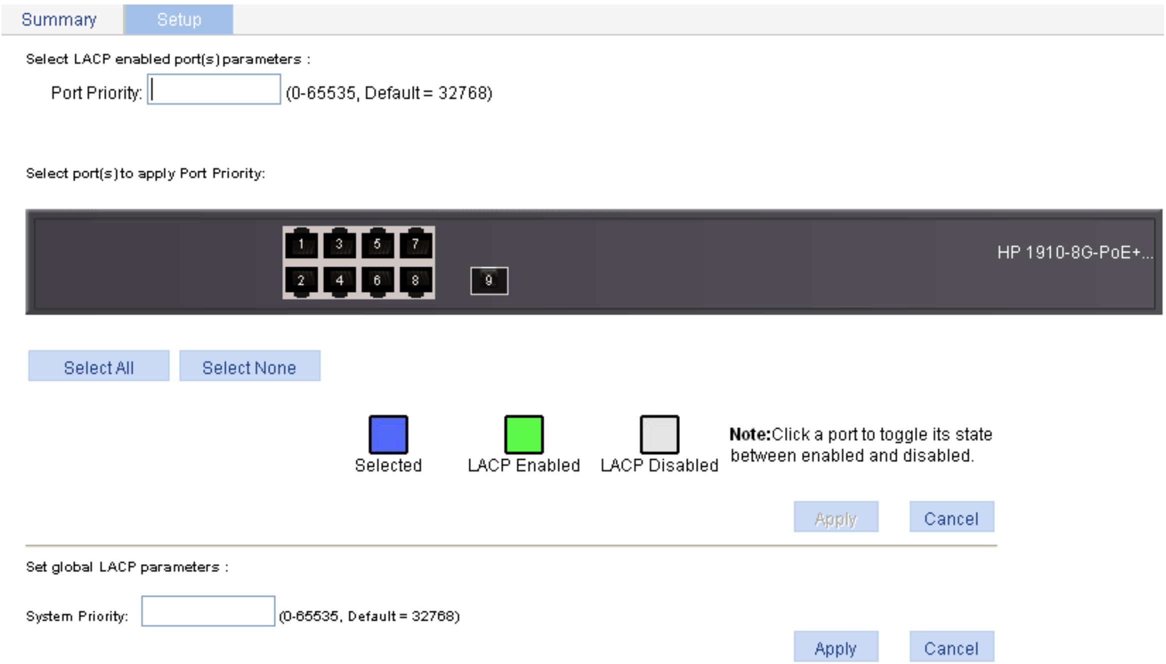
Table 67 Field description

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).
Member Port	A member port of the link aggregation group corresponding to the selected aggregate interface.
State	Select state of a member port, Selected or Unselected.
Reason for being Unselected	Reason why the state of a member port is Unselected. For a selected member port, two hyphens (--) are displayed.

Setting LACP priority

1. Select **Network** > **LACP** from the navigation tree.
2. Click **Setup** to enter the page shown in Figure 194.

Figure 194 The Setup tab



3. In the **Set LACP enabled port(s) parameters** area, set the port priority, and select the ports in the chassis front panel.
4. Click **Apply** in the area.

Table 68 Configuration items

Item	Description
Port Priority	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.)

5. In the **Set global LACP parameters** area, set the system priority.
6. Click **Apply** in the area.

Displaying information of LACP-enabled ports

1. Select **Network** > **LACP** from the navigation tree.

   The **Summary** tab is displayed by default, as shown in Figure 195. The upper part of the page displays a list of all LACP-enabled ports on the device and information about them. Table 69 describes the fields.
2. Select a port on the port list.

3. Click **View Details**.

   Detailed information about the peer port will be displayed on the lower part of the page. Table 70 describes the fields.

Figure 195 Displaying the information of LACP-enabled ports

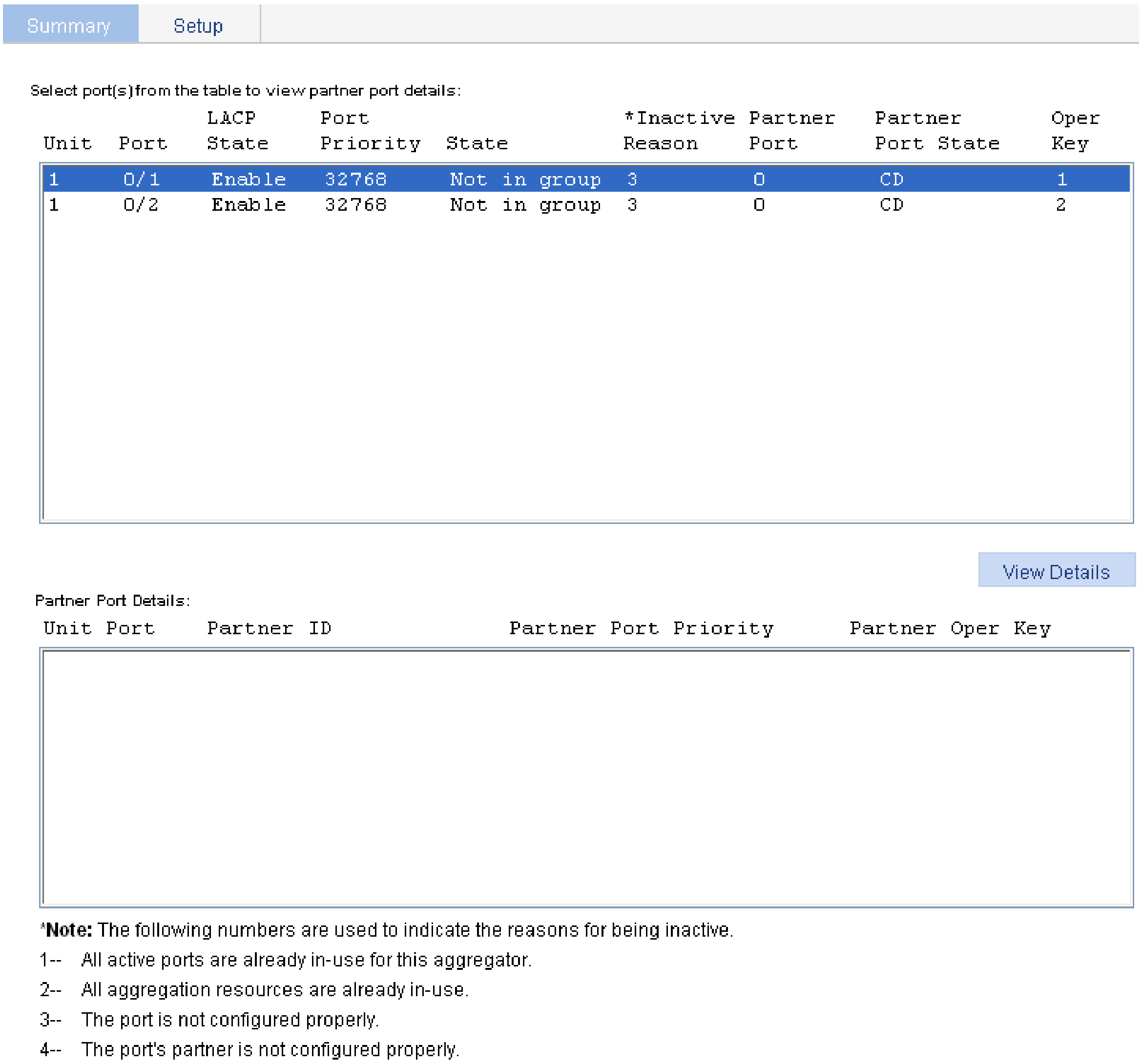


Table 69 Field description

Field	Description
Unit	ID of a device in an IRF.
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.
Inactive Reason	Reason code indicating why a port is inactive (or Unselected) for receiving/transmitting user data. For the meanings of the reason codes, see the bottom of the page shown in Figure 195.

Field	Description
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 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 expired state.
Oper Key	Operational key of the local port.

Table 70 Field description

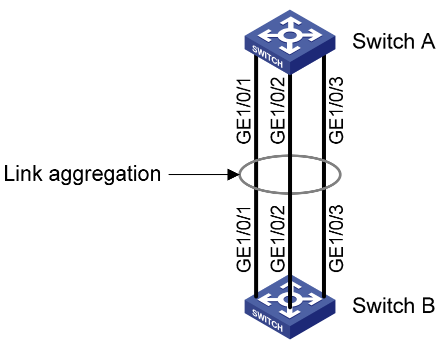
Field	Description
Unit	Number of the remote system
Port	Name of the remote port
Partner ID	LACP priority and MAC address of the remote system
Partner Port Priority	LACP priority of the remote port
Partner Oper Key	Operational key of the remote port

Link aggregation and LACP configuration example

Network requirements

As shown in Figure 196, aggregate the ports on each device to form a link aggregation group, balancing incoming/outgoing traffic across the member ports.

Figure 196 Network diagram

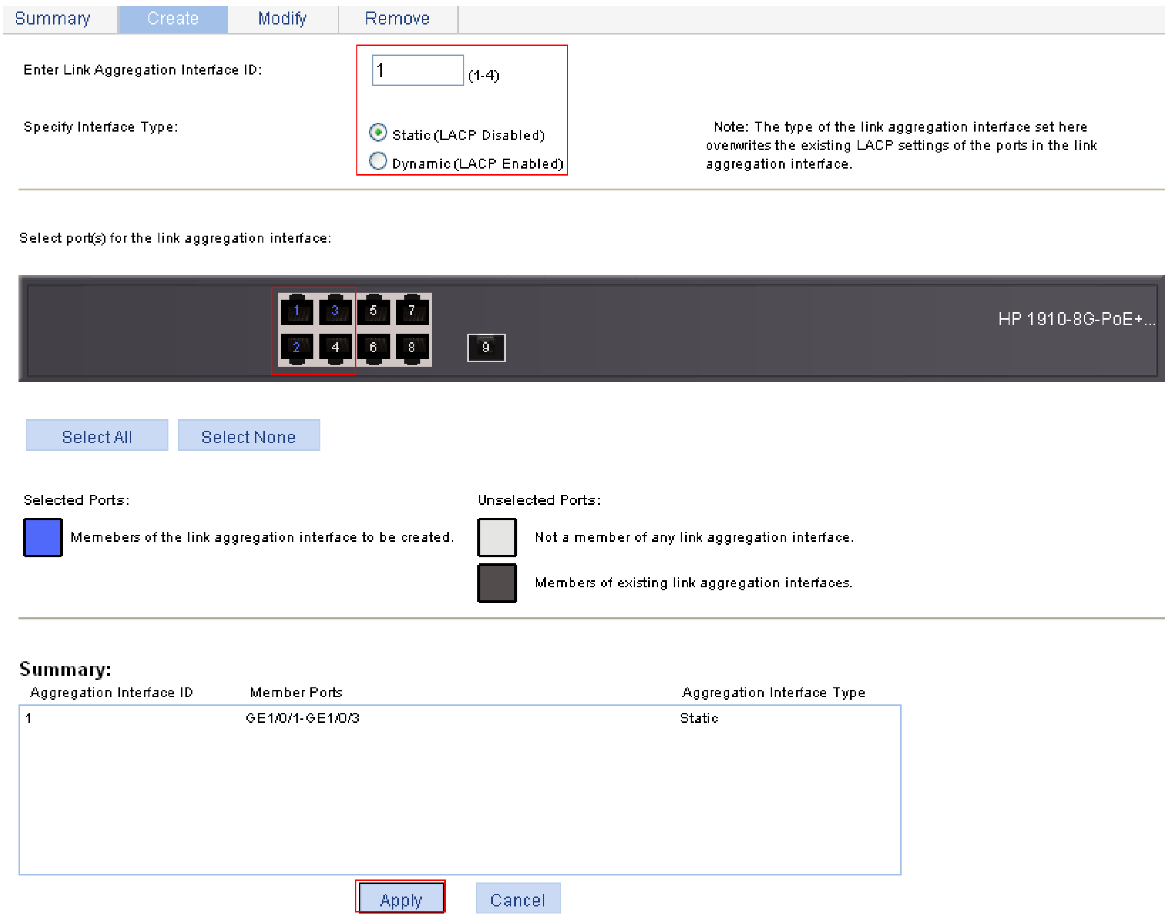


You can create a static or dynamic link aggregation group to achieve load balancing.

Approach 1: Create static link aggregation group 1

1. Select **Network** > **Link Aggregation** from the navigation tree.
2. Click **Create** to enter the page as shown in Figure 197.
3. Configure static link aggregation group 1:
   a. Enter link aggregation interface ID **1**.
   b. Select the **Static (LACP Disabled)** option for the aggregate interface type.
   c. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
4. Click **Apply**.

Figure 197 Creating static link aggregation group 1



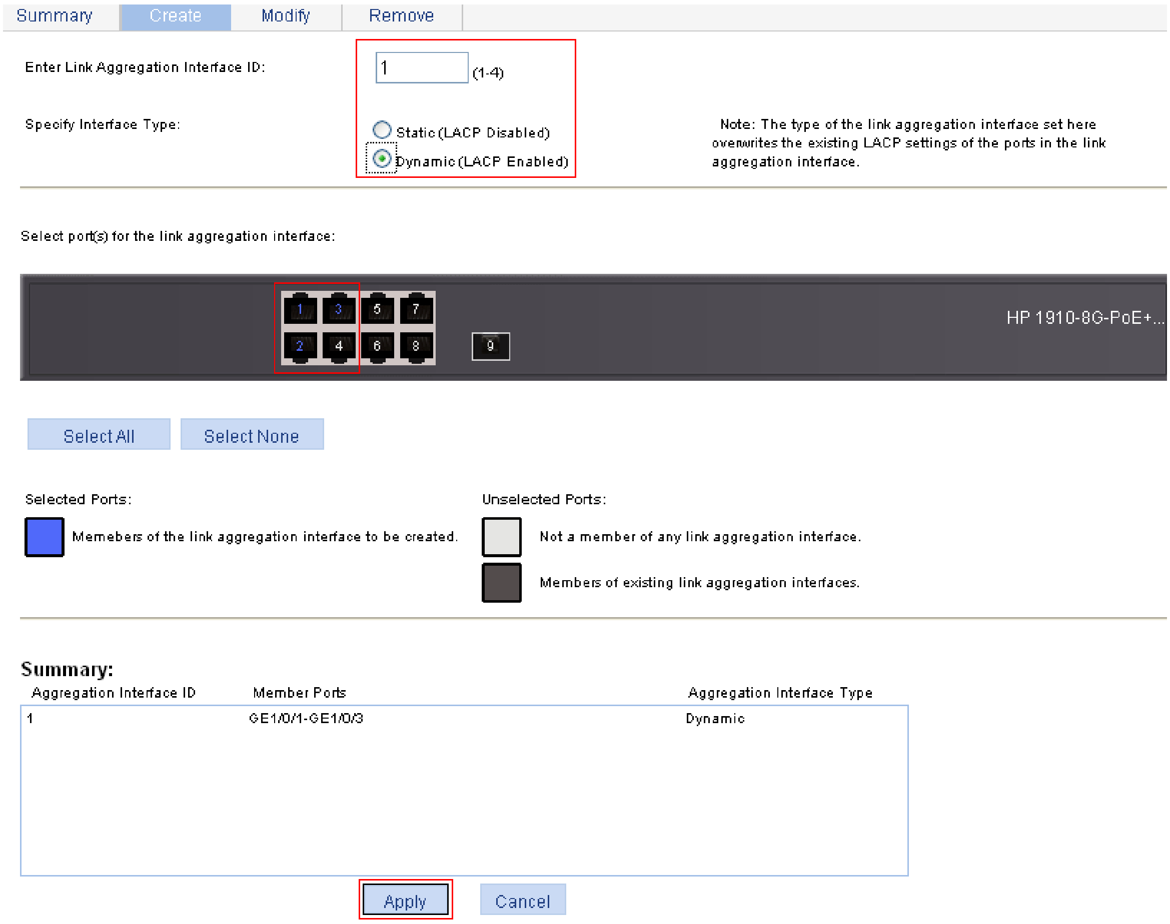
Approach 2: Create dynamic link aggregation group 1

1. Select **Network** > **Link Aggregation** from the navigation tree.
2. Click **Create** to enter the page as shown in Figure 198.
3. Configure dynamic aggregation group 1:
   a. Enter link aggregation interface ID **1**.
   b. Select the **Dynamic (LACP Enabled)** option for aggregate interface type.

c. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.

4. Click **Apply**.

Figure 198 Creating dynamic link aggregation group 1



Configuration guidelines

Follow these guidelines when you configure 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 is performed in the following order: 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.
- Port attribute configuration includes the configuration of the port rate, duplex mode, and link state. For more information about class-two configurations, see "Class-two configurations."
- To guarantee a successful static aggregation, make sure that the ports at the two ends of each link to be aggregated are consistent in Selected/Unselected state. To guarantee a successful dynamic

aggregation, make sure 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.

Configuring LLDP

Overview

Background

In a heterogeneous network, a standard configuration exchange platform ensures that different types of network devices from different vendors can discover one another and exchange configuration for the sake of interoperability and management.

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 (including its major functions, management IP address, device ID, and port ID) as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices. At the same time, the device stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). For more information about MIBs, see "Configuring SNMP." LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

Basic concepts

LLDPDU formats

LLDP sends device information in LLDP data units (LLDPDUs). LLDPDUs are encapsulated in Ethernet II or Subnetwork Access Protocol (SNAP) frames.

1. LLDPDUs encapsulated in Ethernet II

Figure 199 LLDPDU encapsulated in Ethernet II

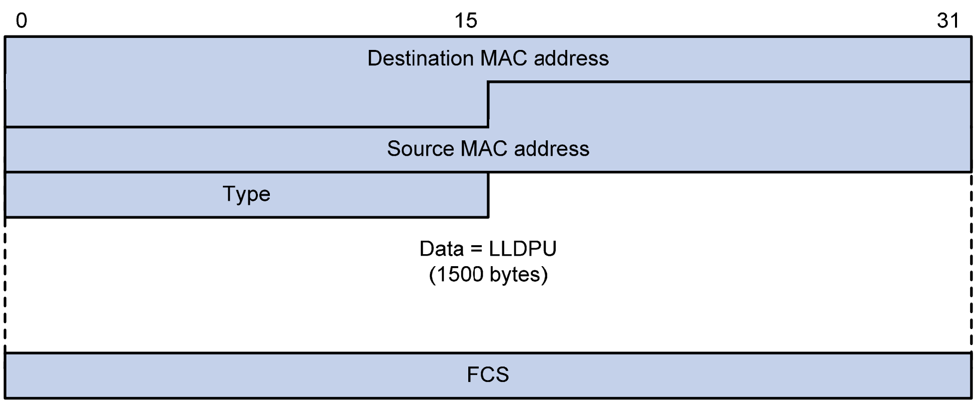


Table 71 Description of the fields in an Ethernet II encapsulated LLDPDU

Field	Description
Destination MAC address	MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	MAC address of the sending port.

Field	Description
Type	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 200 LLDPDU encapsulated in SNAP

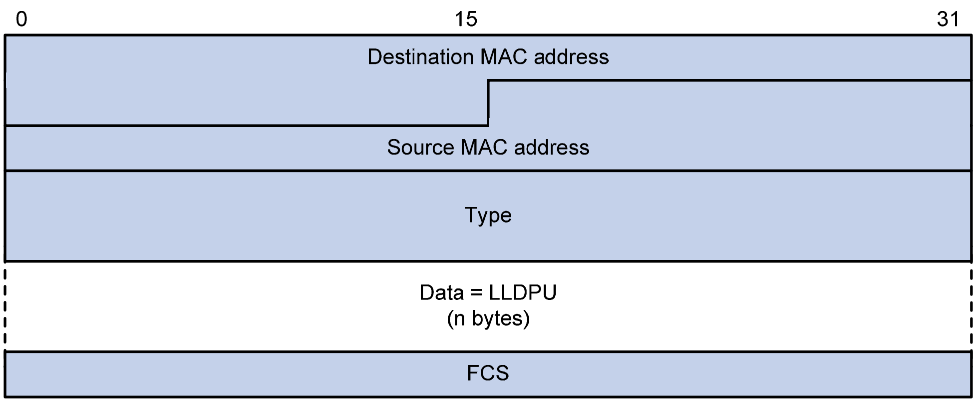


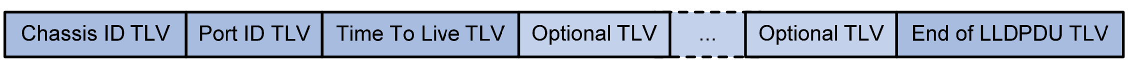
Table 72 Description of the fields in a SNAP-encapsulated LLDPDU

Field	Description
Destination MAC address	MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	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	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 201.

Figure 201 LLDPDU encapsulation format



An LLDPDU can carry up 28 types of TLVs, of which the chassis ID TLV, port ID TLV, Time to Live (TTL) TLV, and end of LLDPDU TLV 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 the following 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 are optional to LLDPDUs.

1. Basic management TLVs

   Table 73 lists the basic management TLV types in use. Some of them must be included in every LLDPDU.

Table 73 Basic LLDP TLVs

Type	Description	Remarks
Chassis ID	Specifies the bridge MAC address of the sending device.	Mandatory
Port ID	Specifies the ID of the sending port. If LLDP-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 LLDP-MED TLVs are included, the port ID TLV carries the port name.	
Time to Live	Specifies the life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	
Port Description	Specifies the port description of the sending port.	Optional
System Name	Specifies the assigned name of the sending device.	
System Description	Specifies the 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	Specifies the 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 74 IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID	Specifies the port's VLAN identifier (PVID). An LLDPDU carries only one TLV of this type.
Port And Protocol VLAN ID	Indicates whether the device supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with. An LLDPDU can carry multiple different TLVs of this type.

Type	Description
VLAN Name	Specifies the textual name of any VLAN to which the port belongs. An LLDPDU can carry multiple different TLVs of this type.
Protocol Identity	Indicates protocols supported on the port. An LLDPDU can carry multiple different TLVs of this type.
DCBX	Data center bridging exchange protocol.

NOTE:

- HP devices only support receiving protocol identity TLVs.
- Layer 3 Ethernet interfaces do not support IEEE 802.1 organizationally specific TLVs.

3. IEEE 802.3 organizationally specific TLVs

Table 75 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 the power supply capability of the port, including the Power over Ethernet (PoE) type, which can be Power Sourcing Equipment (PSE) or Powered Device (PD), PoE mode, whether PSE power supply is supported, whether PSE power supply is enabled, and whether the PoE mode is controllable.
Link Aggregation	Indicates the support of the port for link aggregation, the aggregation capability of the port, and the aggregation status (or whether the link is in an aggregation).
Maximum Frame Size	Indicates the supported maximum frame size. It is now the Maximum Transmission Unit (MTU) of the port.
Power Stateful Control	Indicates the power state control configured on the sending port, including the power type of the PSE/PD, PoE sourcing/receiving priority, and PoE sourcing/receiving power.

NOTE:

The Power Stateful Control TLV is defined in IEEE P802.3at D1.0. The later versions no longer support this TLV. HP devices send this type of TLVs only after receiving them.

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 76.

Table 76 LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a network device to advertise the LLDP-MED TLVs that it supports.
Network Policy	Allows a network device or terminal device to advertise the VLAN ID of the specific port, the VLAN type, and the Layer 2 and Layer 3 priorities for specific applications.

Type	Description
Extended Power-via-MDI	Allows a network device or terminal device to advertise power supply capability. This TLV is an extension of the Power Via MDI TLV.
Hardware Revision	Allows a terminal device to advertise its hardware version.
Firmware Revision	Allows a terminal device to advertise its firmware version.
Software Revision	Allows a terminal device to advertise its software version.
Serial Number	Allows a terminal device to advertise its serial number.
Manufacturer Name	Allows a terminal device to advertise its vendor name.
Model Name	Allows a terminal device to advertise its model name.
Asset ID	Allows a terminal device 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 a terminal device to use in the context of location-based applications.

NOTE:

For more information about LLDPDU TLVs, see the IEEE standard (LLDP) 802.1AB-2005 and the LLDP-MED standard (ANSI/TIA-1057).

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 cases:

- A new neighbor is discovered. 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. 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**—CDP packets can be transmitted and received.
- **Disable**—CDP packets can neither be transmitted nor be received.

Protocols and standards

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*

Recommended LLDP configuration procedure

Step	Remarks
1. 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.

Step	Remarks
2. Configuring LLDP settings on ports	(Optional.) LLDP settings include LLDP operating mode, packet encapsulation, CDP compatibility, device information polling, trapping, and advertisable TLVs. The default settings are as follows: • 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.
3. 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.
4. 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.
5. Displaying global LLDP information	(Optional.) You can display the local global LLDP information and statistics.
6. Displaying LLDP information received from LLDP neighbors	(Optional.) You can display the LLDP information received from LLDP neighbors.

Enabling LLDP on ports

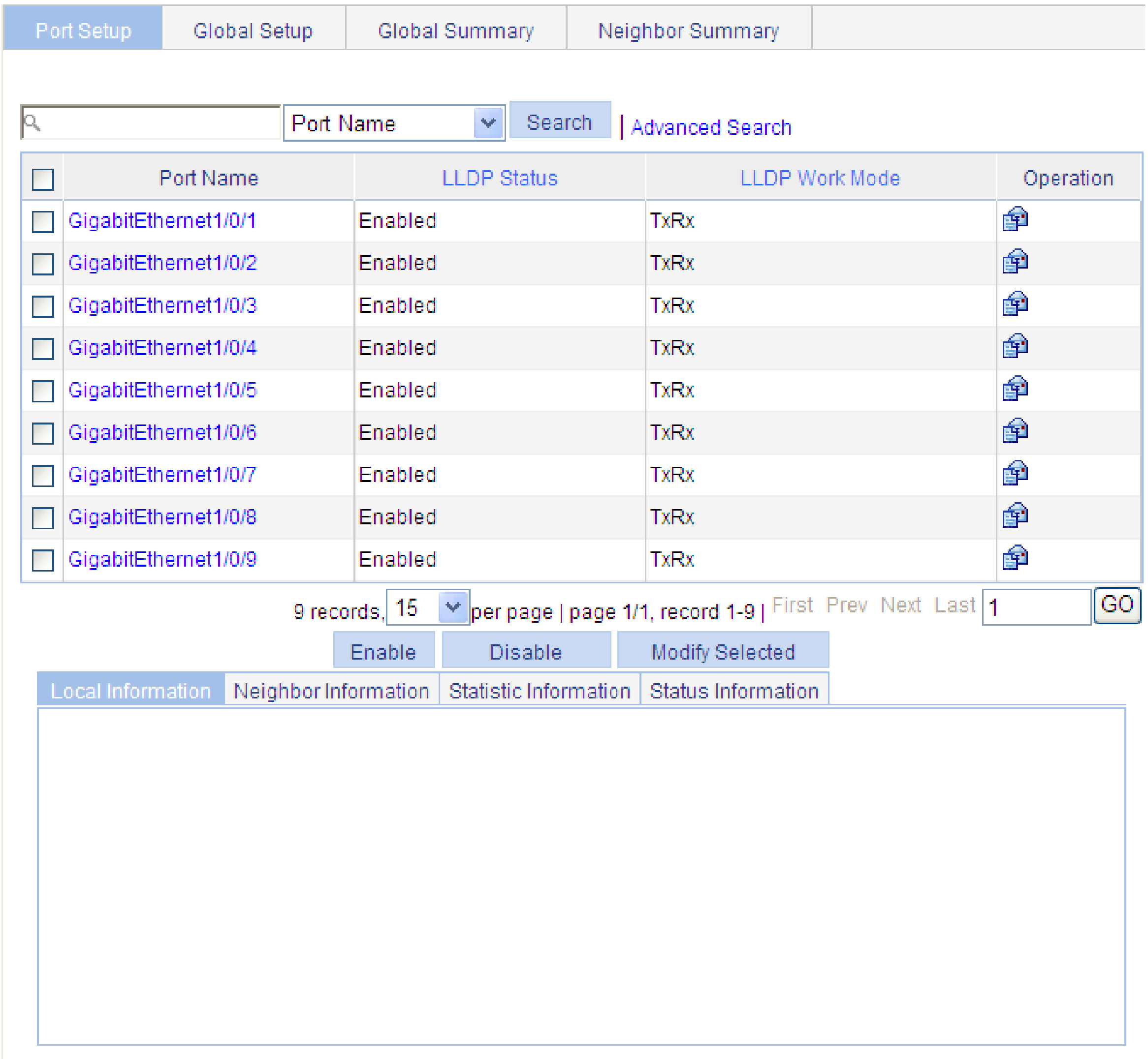
1. Select **Network** > **LLDP** from the navigation tree.

   By default, the **Port Setup** tab is displayed, as shown in Figure 202. This tab displays the enabling status and operating mode of LLDP on a port.

2. 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 202 The Port Setup tab



Configuring LLDP settings on ports

The web interface allows you to set LLDP parameters for a single port and set LLDP parameters for multiple ports in batch.

Setting LLDP parameters for a single port

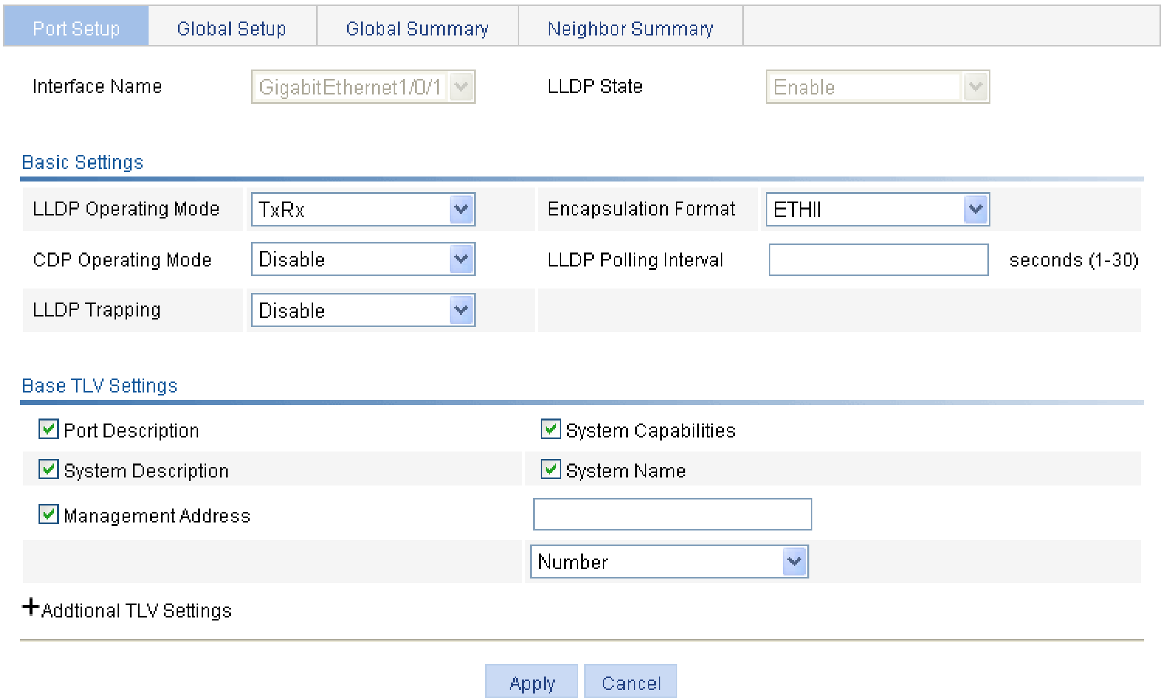
1. Select **Network** > **LLDP** from the navigation tree.

   By default, the **Port Setup** tab is displayed.

2. Click the  icon for the port you are configuring.

   On the page as shown in Figure 203, the LLDP settings of the port are displayed.

Figure 203 Modifying LLDP settings on a port



3. Modify the LLDP parameters for the port as described in Table 77.
4. Click **Apply**.

   A progress dialog box appears.
5. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Table 77 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.

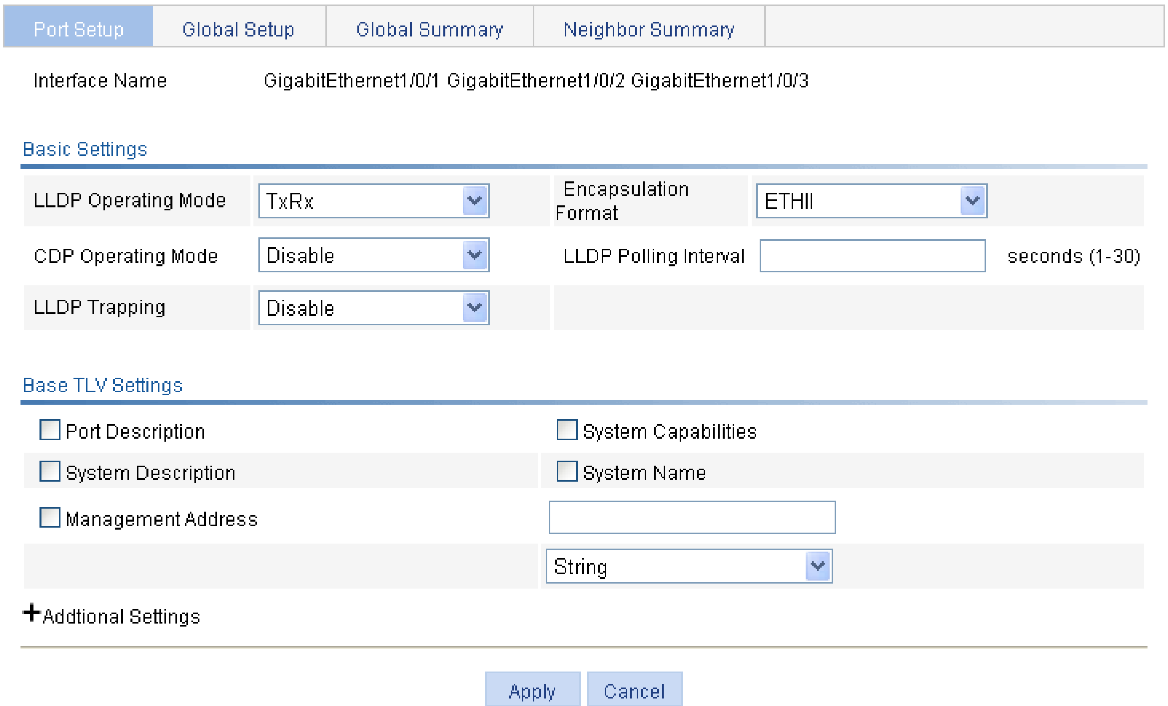
Item		Description
Basic Settings	LLDP Operating Mode	Set the LLDP operating mode on the port or ports you are configuring. Available options include: • **TxRx**—Sends and receives LLDPDUs. • **Tx**—Sends but not receives LLDPDUs. • **Rx**—Receives but not sends LLDPDUs. • **Disable**—Neither sends nor 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. NOTE: LLDP-CDP PDUs use only SNAP encapsulation.
	CDP Operating Mode	Set the CDP compatibility of LLDP. Available options include: • **Disable**—Neither sends nor receives CDPDUs. • **TxRx**—Sends and receives CDPDUs IMPORTANT: 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. NOTE: 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.

Item		Description
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.
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 and power stateful control 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 Network Device 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 you configure the network device address, select the address information type from the list, type the address information in the field below and click **Add** next to the field 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.

Configuring LLDP settings for ports in batch

1. Select **Network** > **LLDP** from the navigation tree.
   By default, the **Port Setup** tab is displayed.
2. Select one or multiple ports on the port list.
3. Click **Modify Selected** to enter the page for modifying these ports in batch.

Figure 204 Modifying LLDP settings on ports in batch



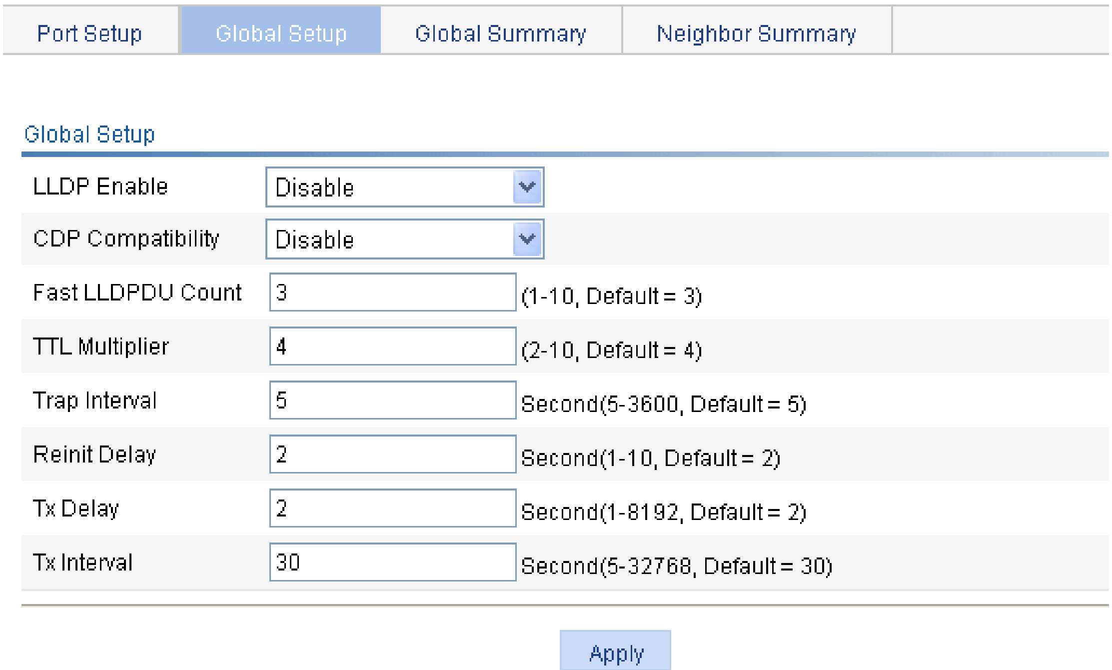
4. Set the LLDP settings for these ports as described in Table 77.
5. Click **Apply**.

   A progress dialog box appears.
6. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Configuring global LLDP setup

1. Select **Network** > **LLDP** from the navigation tree.
2. Click the **Global Setup** tab.

Figure 205 The Global Setup tab



3. Set the global LLDP setup as described in Table 78.
4. Click **Apply**.

   A progress dialog box appears.
5. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Table 78 Configuration items

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>LLDP Enable</td><td>Select from the list to enable or disable global LLDP.</td></tr>
<tr><td>CDP Compatibility</td><td>Select from the list to enable or disable CDP compatibility of LLDP.
IMPORTANT:
• To enable LLDP to be compatible with CDP on a port, you must set the CDP operating mode on the port to TxRx in addition to enabling CDP compatibility on the Global Setup tab.
• Because the maximum TTL allowed by CDP is 255 seconds, you must make sure 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.</td></tr>
<tr><td>Fast LLDPDU Count</td><td>Set the number of LLDPDUs sent each time fast LLDPDU transmission is triggered.</td></tr>
</table>

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*. NOTE: • 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. • Because the maximum TTL allowed by CDP is 255 seconds, you must make sure 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 of the port to advertise the topology changes detected over the trap 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. After sending an LLDPDU, the port must wait for the specified interval before it can send another one. IMPORTANT: LLDPDU transmit delay must be less than the TTL to make sure 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. NOTE: 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. 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.

Displaying LLDP information for a port

1. Select **Network** > **LLDP** from the navigation tree.
   By default, the **Port Setup** tab is displayed.
2. On the port list, click a port name to display its LLDP information at the lower half of the page.

By default, the Local Information tab is displayed, as shown in Figure 206. Table 79 describes the fields.

Figure 206 The Local Information tab

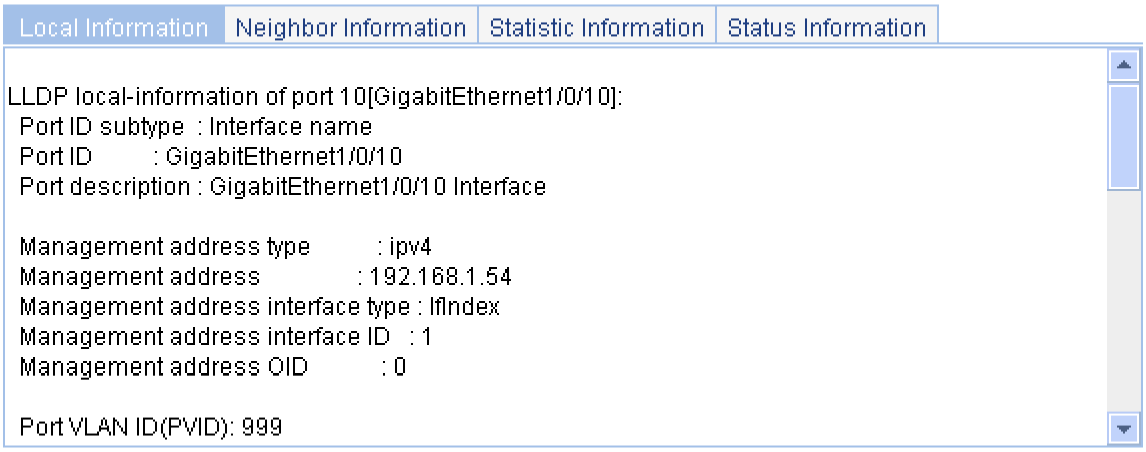


Table 79 Field description

Field	Description
Port ID subtype	Port ID type: • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned, or the local configuration
Power port class	The power over Ethernet port class: • **PSE**—Power supply device • **PD**—Powered device
Port power classification	Port power classification of the PD: • Unknown • Class0 • Class1 • Class2 • Class3 • Class4
Power type	The PoE type is **Type 2 PSE**, which supplies power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.
Power source	**Power supply type for a PSE:** • **Unknown**—Unknown power supply • **Primary**—Primary power supply • **Backup**—Backup power supply

Field	Description
Power priority	Power supply priority on a PSE: • **Unknown**—Unknown priority • **Critical**—Priority 1 • **High**—Priority 2 • **Low**—Priority 3
Media policy type	Media policy type: • 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: • Primary • Backup
Port PSE priority	PSE priority of the port: • **Unknown**—Unknown priority • **Critical**—Priority level 1. • **High**—Priority level 2 • **Low**—Priority level 3

3. Click the **Neighbor Information** tab to display the LLDP neighbor information. Table 80 describes the fields.

Figure 207 The Neighbor Information tab

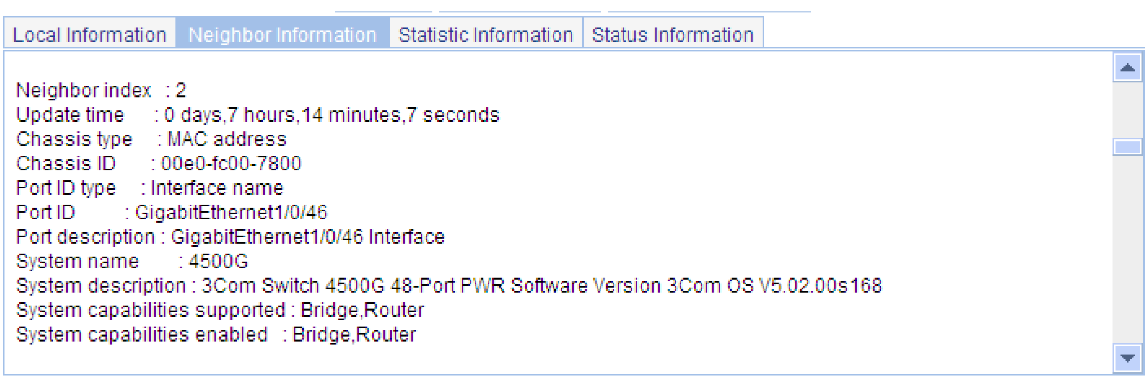


Table 80 Field description

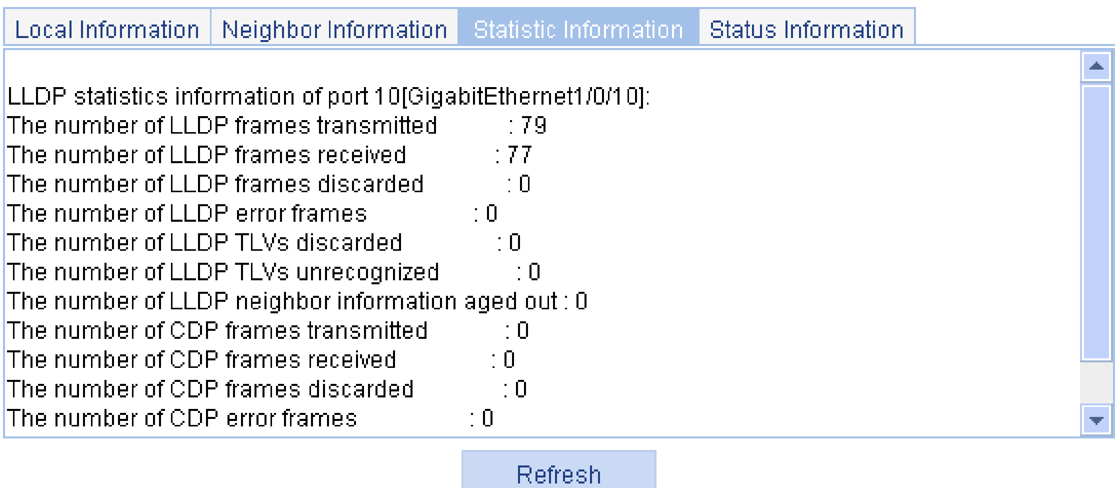
Field	Description
Chassis type	Chassis ID type: • Chassis component • Interface alias • Port component • MAC address • Network address • Interface name • Locally assigned, or the local configuration
Chassis ID	Chassis ID depending on the chassis type, which can be a MAC address of the device
Port ID type	Port ID type: • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned, or the local configuration
Port ID	The port ID value.
System capabilities supported	The primary network function of the system: • Repeater • Bridge • Router
System capabilities enabled	The network function enabled on the system: • 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
Power type	Power type: • **Type 1 PD**—This type requires power from 0 to 15.4 W, a voltage from 44 to 57 V, and a maximum current of 350 mA. • **Type 2 PD**—This type requires power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.
Power source	Power supply type for a PD: • **Unknown**—Unknown power supply. • **PSE**—PSE power supply. • **Local**—Local power supply. • **PSE and local**—PSE and local power supply.

Field	Description
Power priority	Power supply priority on a PD: • **Unknown**—Unknown priority. • **Critical**—Priority 1. • **High**—Priority 2. • **Low**—Priority 3.
PD requested power value	Power (in watts) required by the PD that connects to the port.
PSE allocated power value	Power (in watts) supplied by the PSE to the connecting port.
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: • **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	Media policy type: • 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.

Field	Description
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.
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	Type of PSE power source advertised by the neighbor: • Primary • Backup
Port PSE priority	PSE priority of the port: • **Unknown**—The PSE priority of the port is unknown. • **Critical**—Priority level 1. • **High**—Priority level 2. • **Low**—Priority level 3.

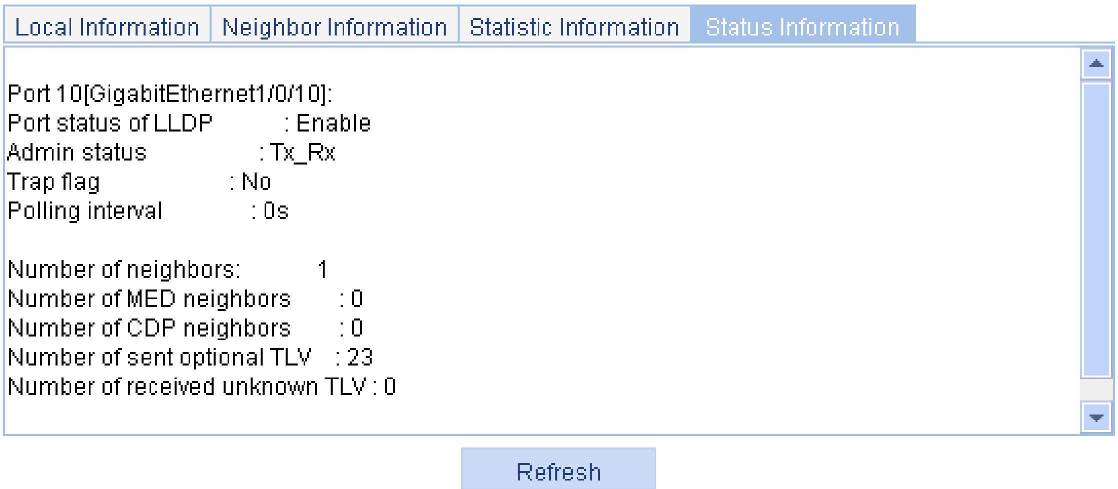
4. Click the **Statistics Information** tab to display the LLDP statistics.

Figure 208 The Statistic Information tab



5. Click the **Status Information** tab to display the LLDP status information.

Figure 209 The Status Information tab



Displaying global LLDP information

1. Select **Network** > **LLDP** from the navigation tree.
2. Click the **Global Summary** tab to display global local LLDP information and statistics, as shown in Figure 210.

   Table 81 describes the fields.

Figure 210 The Global Summary tab

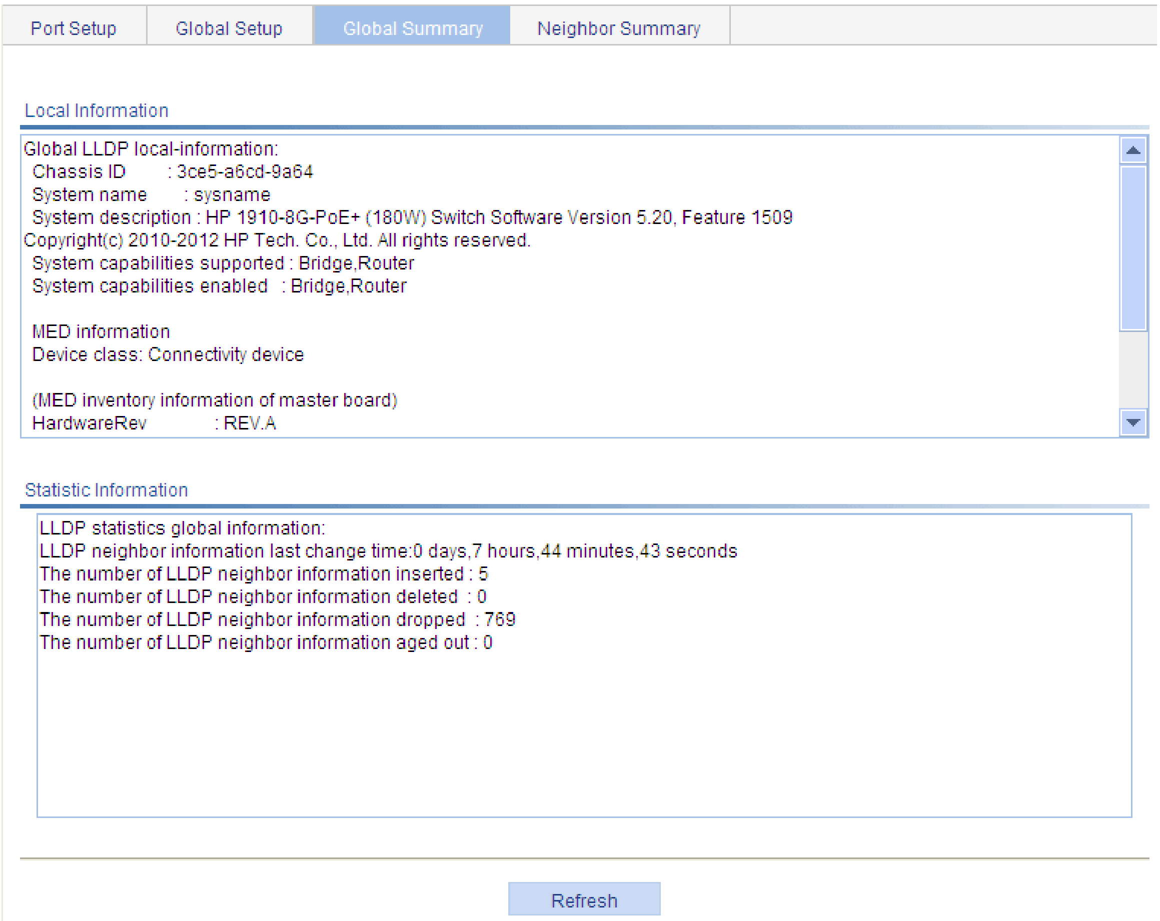


Table 81 Field description

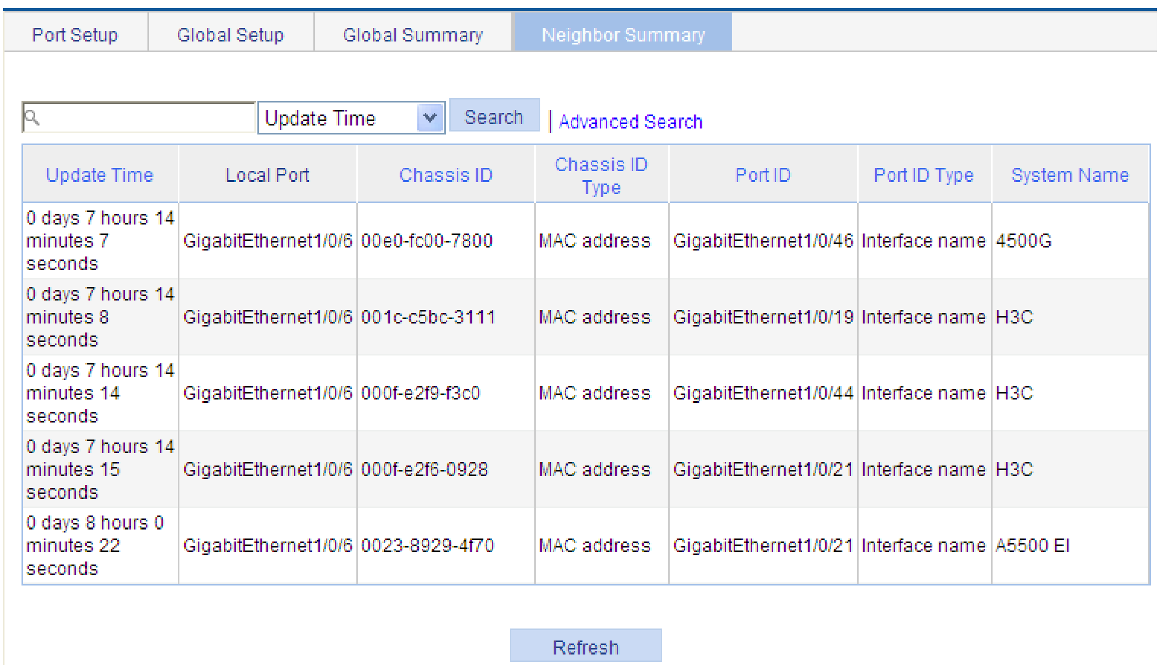
Field	Description
Chassis ID	The local chassis ID depending on the chassis type defined.
System capabilities supported	The primary network function advertised by the local device: • Repeater • Bridge • Router
System capabilities enabled	The enabled network function advertised by the local device: • Repeater • Bridge • Router

Field	Description
Device class	The device class advertised by the local device: • **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.

Displaying LLDP information received from LLDP neighbors

1. Select **Network** > **LLDP** from the navigation tree.
2. Click the **Neighbor Summary** tab to display the global LLDP neighbor information, as shown in Figure 211.

Figure 211 The Neighbor Summary tab



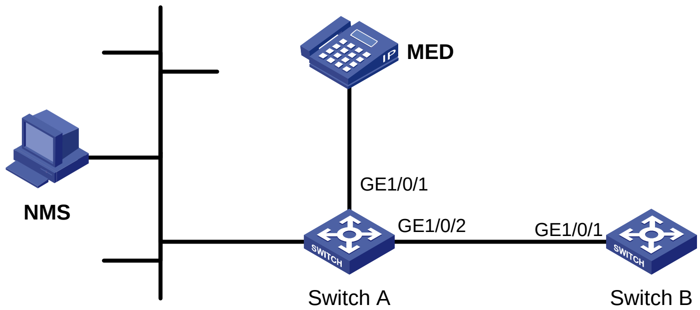
LLDP configuration examples

LLDP basic settings configuration example

Network requirements

As shown in Figure 212, configure LLDP on Switch A and Switch B so that the network management station (NMS) can determine the status of the link between Switch A and MED and the link between Switch A and Switch B.

Figure 212 Network diagram



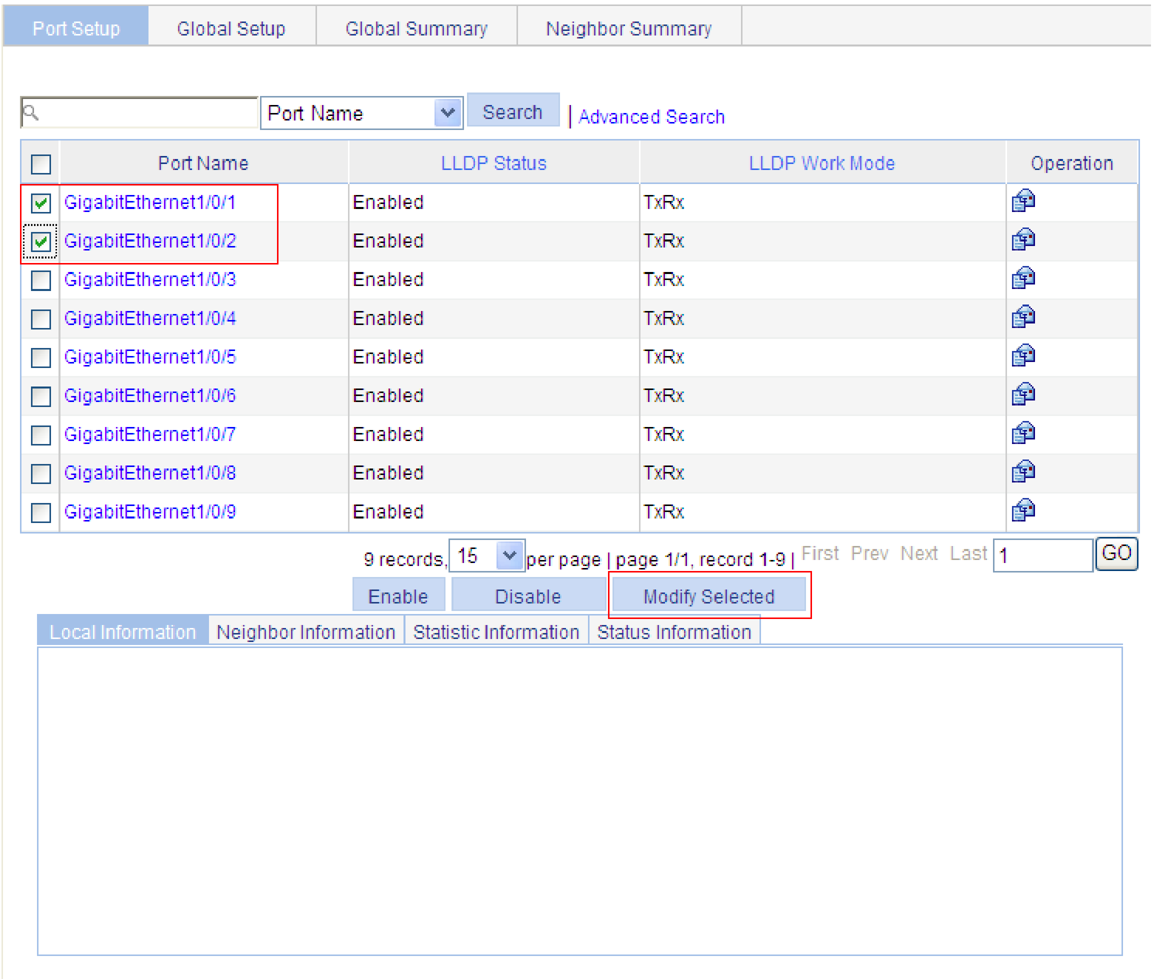
Configuring Switch A

1. Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. (Optional. By default, LLDP is enabled on Ethernet ports.)
2. Set the LLDP operating mode to Rx on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:
   a. Select **Network** > **LLDP** from the navigation tree.

      By default, the **Port Setup** tab is displayed.
   b. Select port GigabitEthernet1/0/1 and GigabitEthernet1/0/2.
   c. Click **Modify Selected**.

      The page shown in Figure 214 appears.

Figure 213 The Port Setup tab



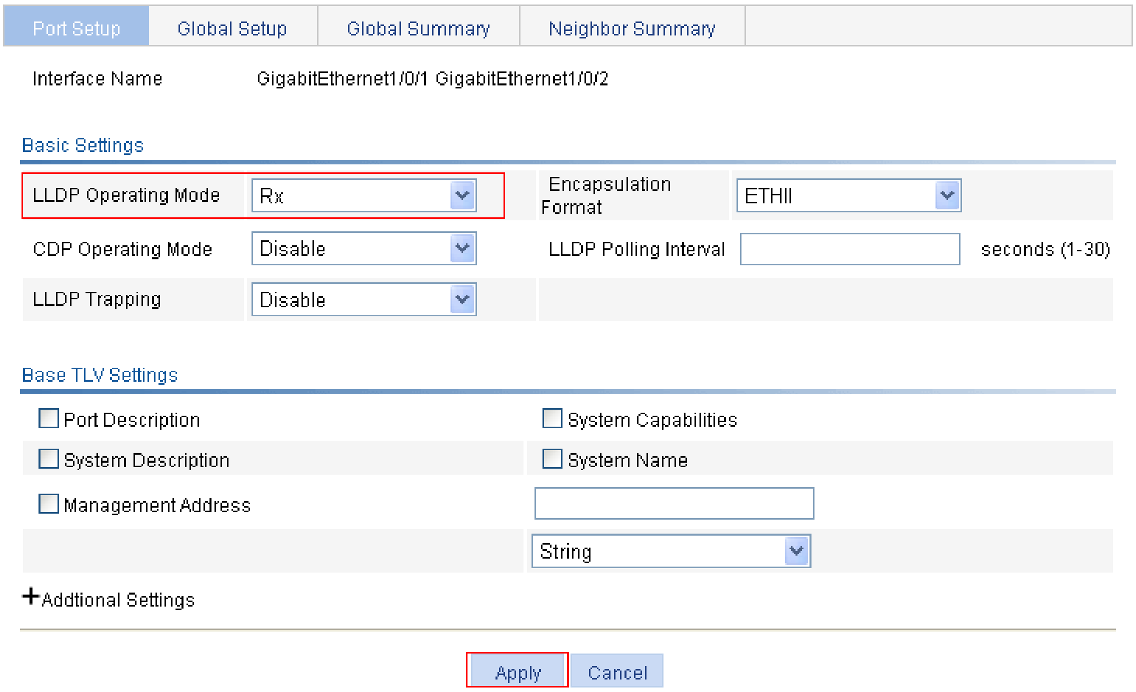
d. Select **Rx** from the **LLDP Operating Mode** list.

3. Click **Apply**.

   A progress dialog box appears.

4. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

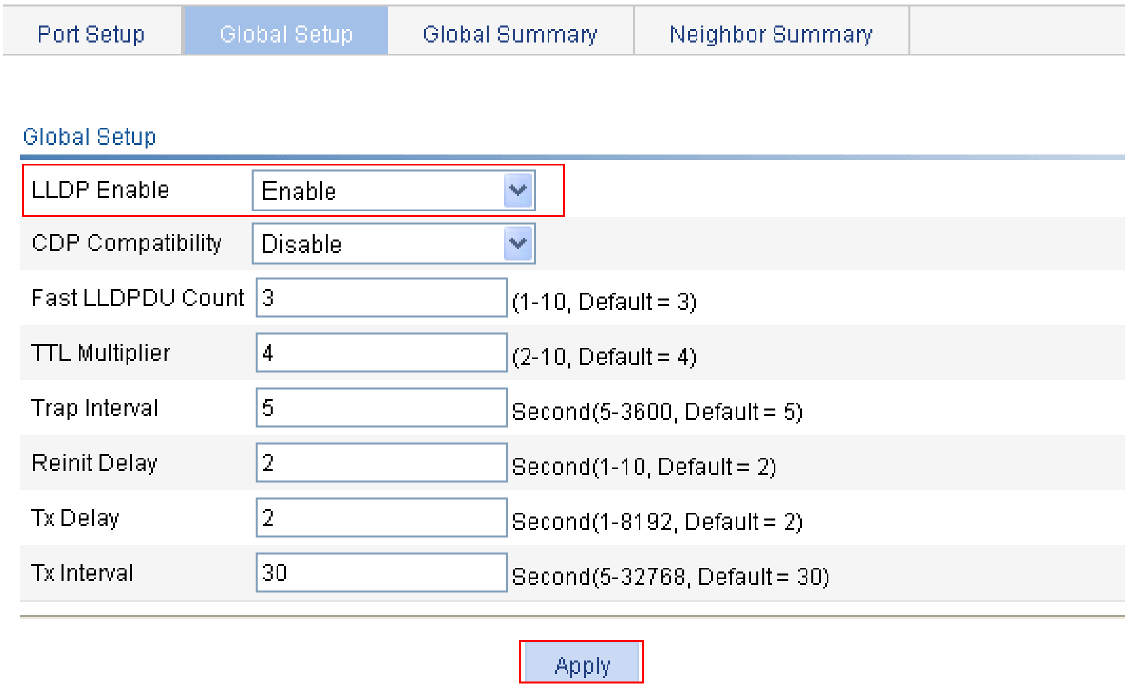
Figure 214 Setting LLDP on multiple ports



5. Enable global LLDP:
    a. Click the **Global Setup** tab.
    b. Select **Enable** from the **LLDP Enable** list.
6. Click **Apply**.

    A progress dialog box appears.
7. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

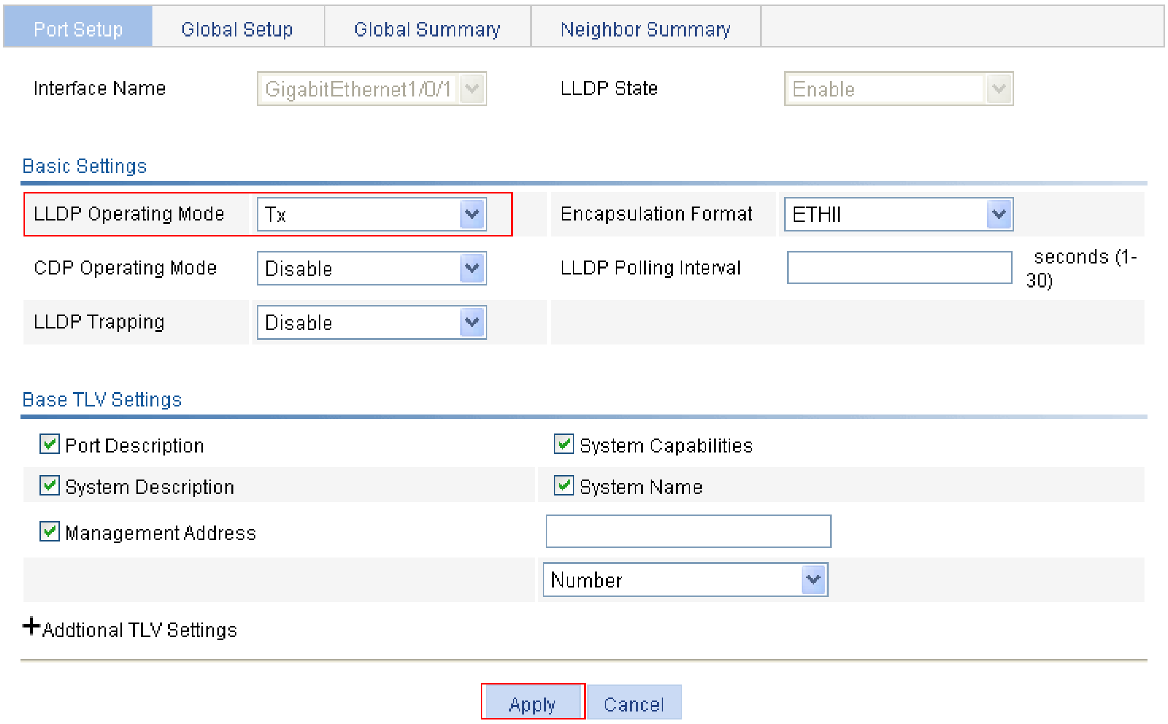
Figure 215 Enabling global LLDP



Configuring Switch B

1. Enable LLDP on port GigabitEthernet 1/0/1. (Optional. By default, LLDP is enabled on Ethernet ports.)
2. Set the LLDP operating mode to Tx on GigabitEthernet 1/0/1:
   a. Select **Network** > **LLDP** from the navigation tree.
      By default, the **Port Setup** tab is displayed.
   b. Click the icon for port GigabitEthernet1/0/1.
      The page shown in Figure 216 is displayed.
   c. Select **Tx** from the **LLDP Operating Mode** list.
3. Click **Apply**.
   A progress dialog box appears.
4. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Figure 216 Setting the LLDP operating mode to Tx



5. Enable global LLDP:
   a. Click the **Global Setup** tab.
   b. Select **Enable** from the **LLDP Enable** list.
6. Click **Apply**.

   A progress dialog box appears.
7. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

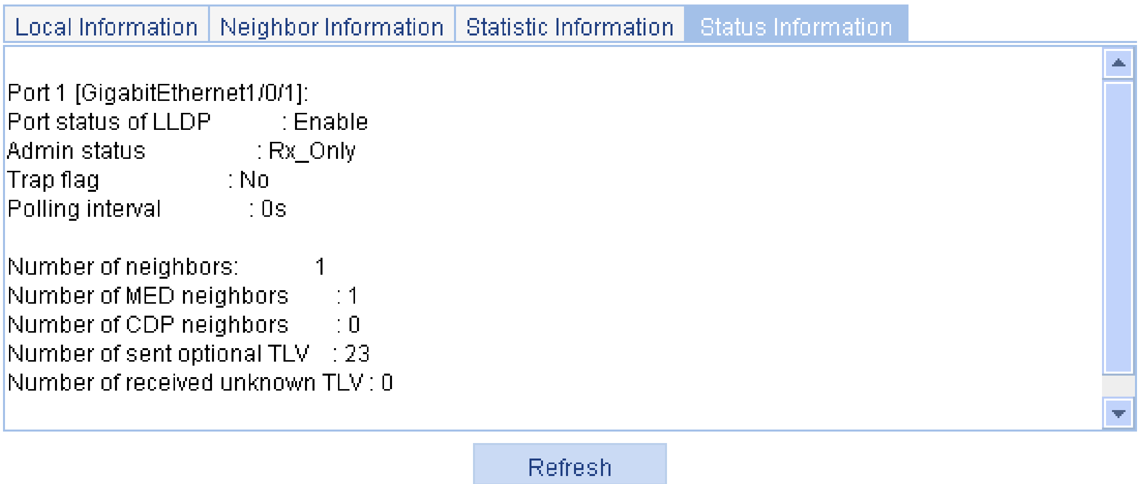
Verifying the configuration

1. Display the status information of port GigabitEthernet1/0/1 on Switch A:
   a. Select **Network** > **LLDP** from the navigation tree.

      By default, the **Port Setup** tab is displayed.
   b. Click the **GigabitEthernet1/0/1** port name in the port list.
   c. Click the **Status Information** tab at the lower half of the page.

      The output shows that port GigabitEthernet 1/0/1 is connected to an MED neighbor device.

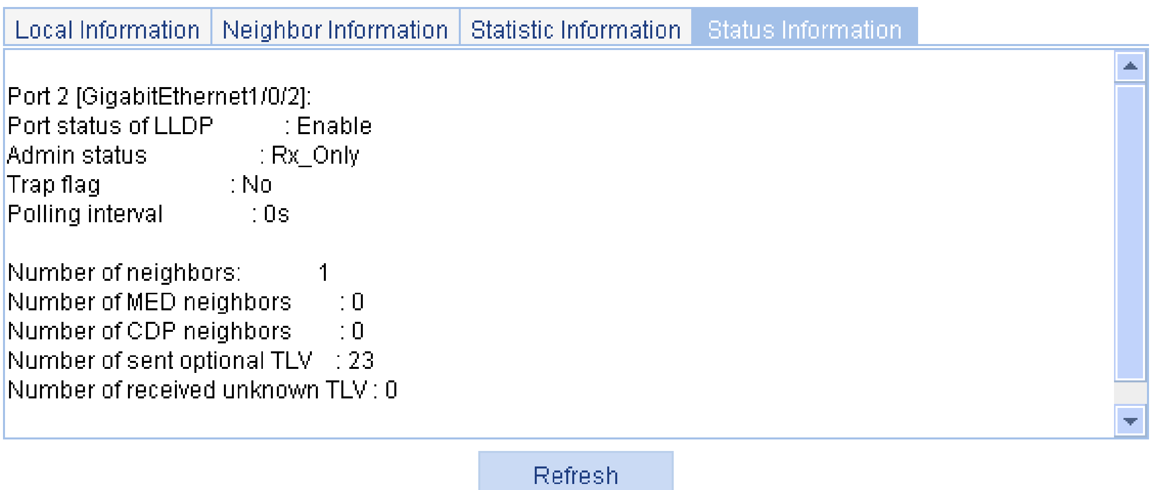
Figure 217 Viewing the status of port GigabitEthernet 1/0/1



2. Display the status information of port GigabitEthernet1/0/2 on Switch A:
    a. Click the **GigabitEthernet1/0/2** port name in the port list.
    b. 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 (Switch B).

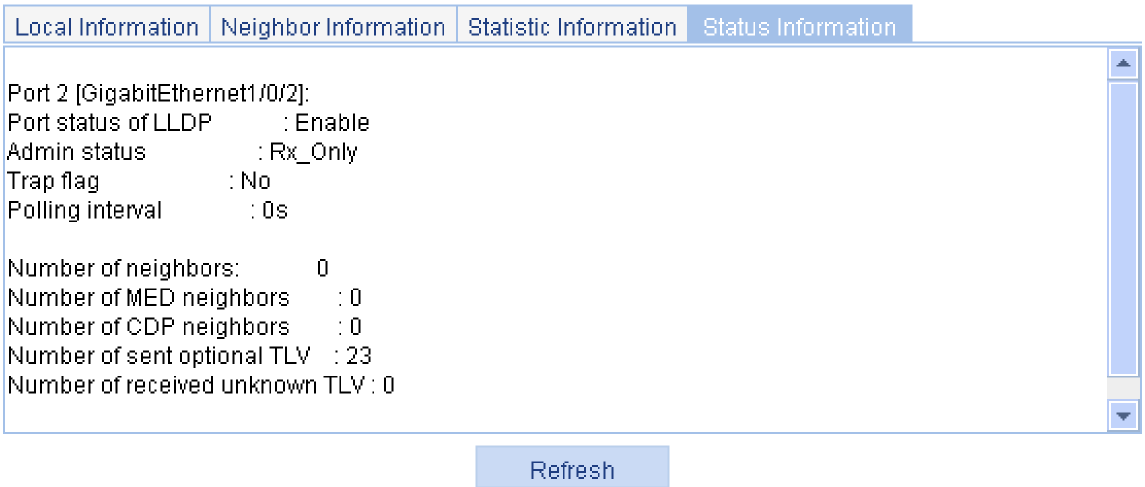
Figure 218 Viewing the status of port GigabitEthernet 1/0/2



3. Tear down the link between Switch A and Switch B.
4. Click **Refresh** to display the status information of port GigabitEthernet1/0/2 on Switch A.

    The updated status information of port GigabitEthernet 1/0/2 shows that no neighbor device is connected to the port.

Figure 219 Viewing the updated port status information

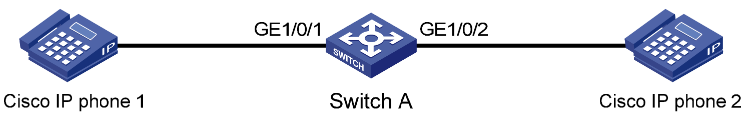


CDP-compatible LLDP configuration example

Network requirements

As shown in Figure 220, 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, confining their voice traffic within the voice VLAN to be separate from other types of traffic.

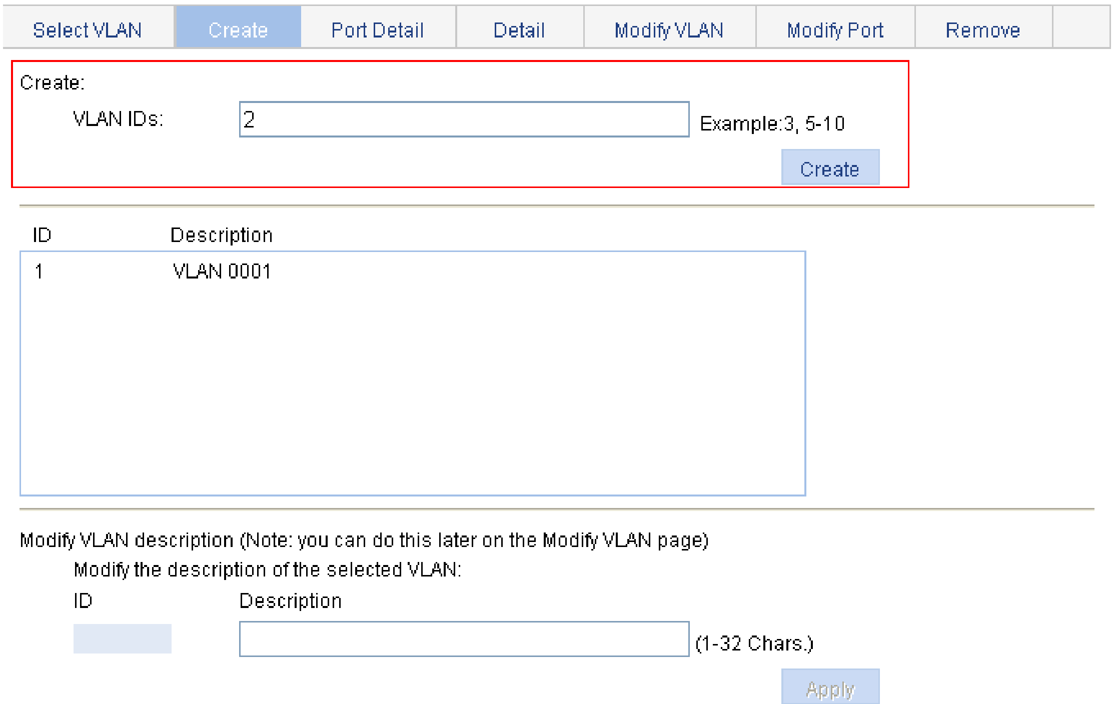
Figure 220 Network diagram



Configuring Switch A

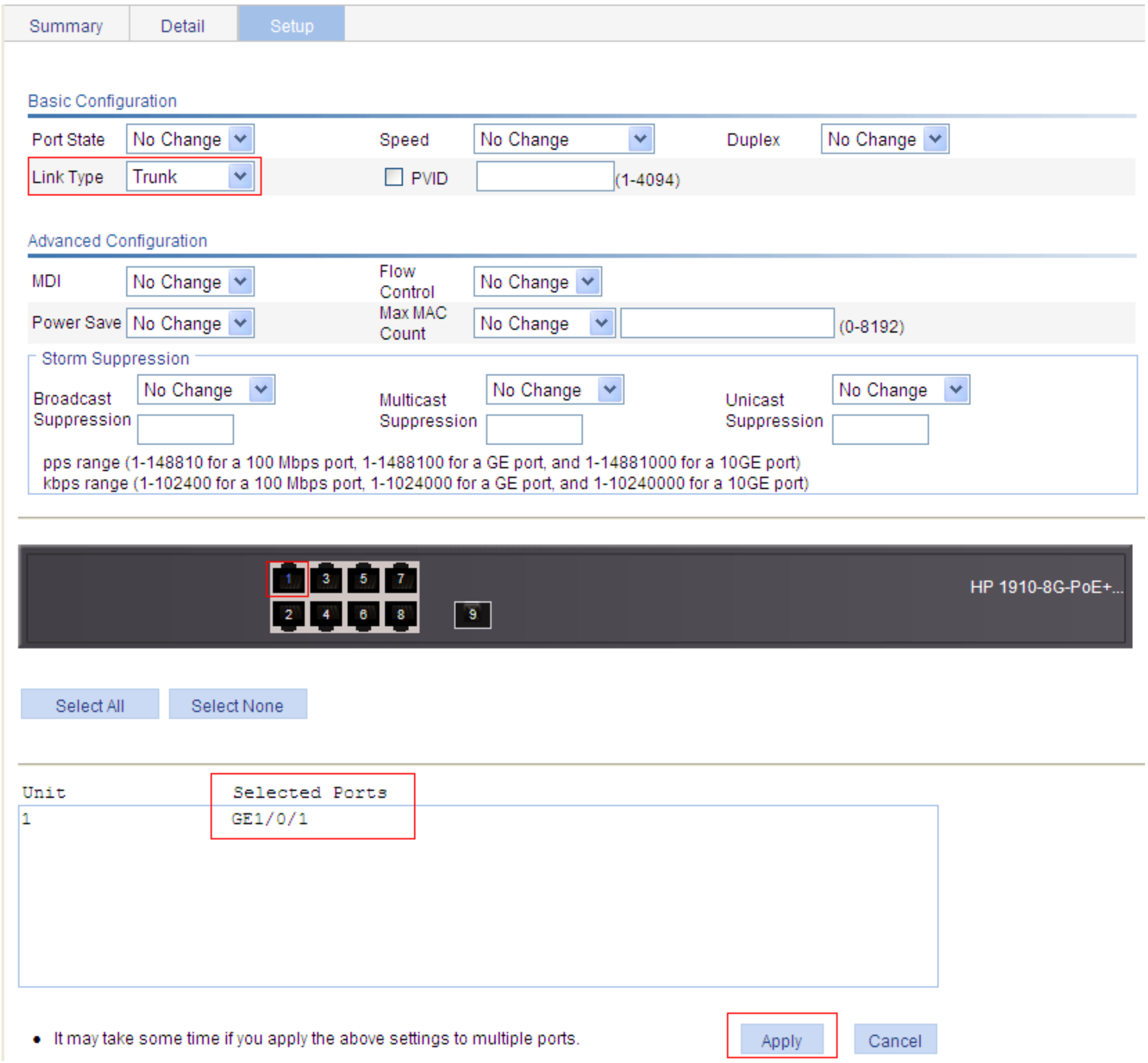
1. Create VLAN 2:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click **Create** to enter the page for creating VLANs.
   c. Enter **2** in the **VLAN IDs** field.
   d. Click **Create**.

Figure 221 Creating VLANs



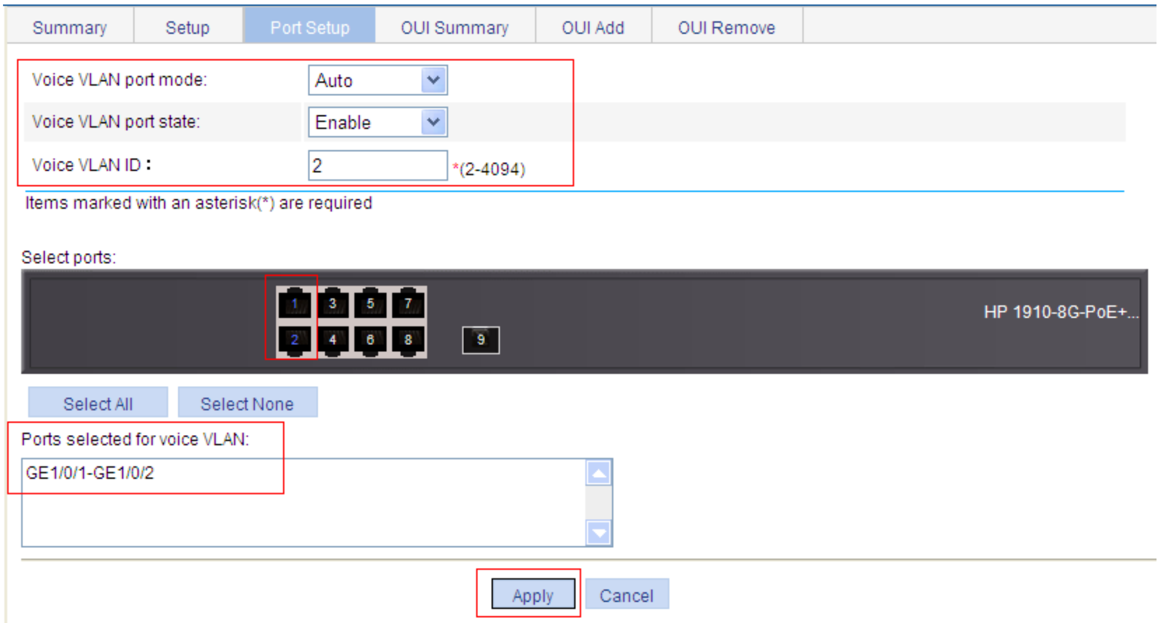
2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports:
   a. Select **Device** > **Port Management** from the navigation tree.
   b. Click the **Setup** tab to enter the page for configuring ports.
   c. Select **Trunk** in the **Link Type** list.
   d. Select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
   e. Click **Apply**.

Figure 222 Configuring ports



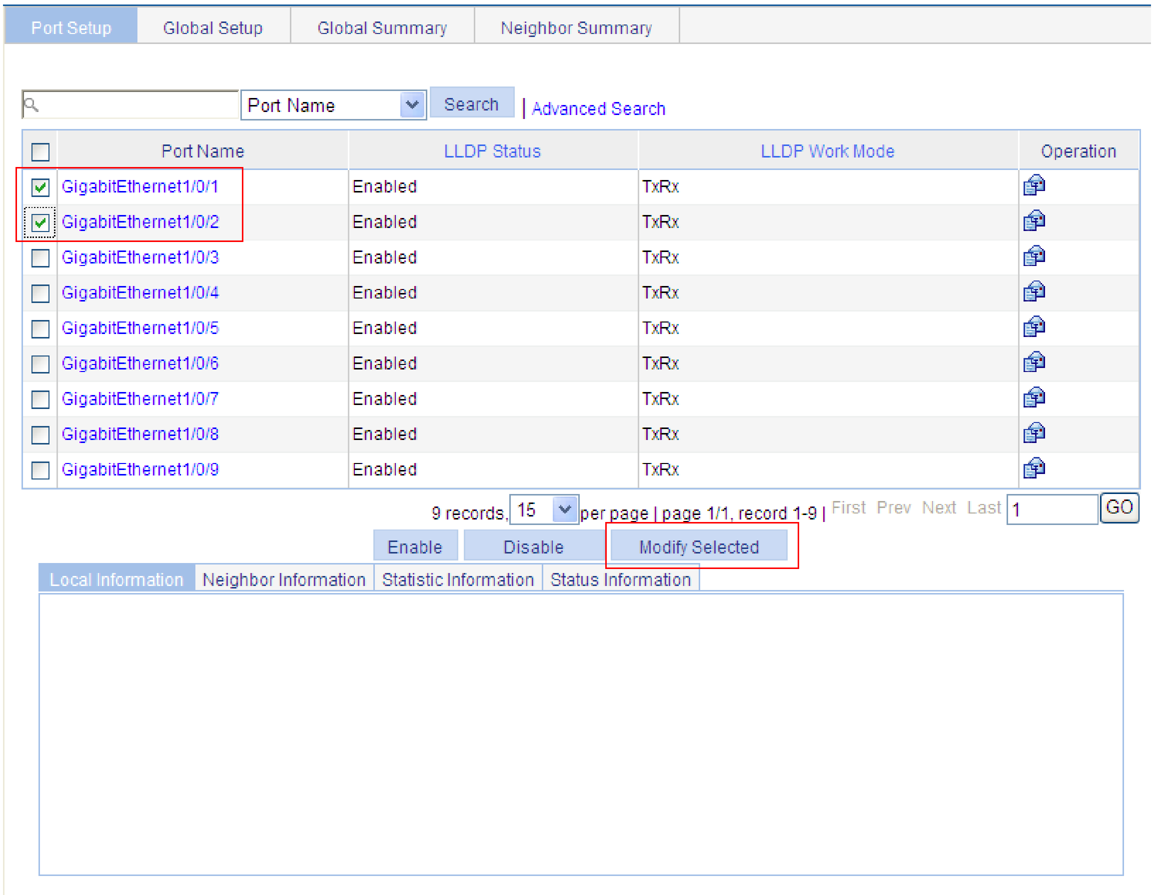
3. Configure the voice VLAN function on the two ports:
   a. Select **Network** > **Voice VLAN** from the navigation tree.
   b. Click the **Port Setup** tab to enter the page for configuring the voice VLAN function on ports.
   c. Select **Auto** in the **Voice VLAN port mode** list, select **Enable** in the **Voice VLAN port state** list, enter the voice VLAN ID **2,** and select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
   d. Click **Apply**.

Figure 223 Configuring the voice VLAN function on ports



4. Enable LLDP on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. Skip this step if LLDP is enabled (the default).
5. Set both the LLDP operating mode and the CDP operating mode to TxRx on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:
   a. Select **Network** > **LLDP** from the navigation tree.
      By default, the **Port Setup** tab is displayed.
   b. Select port GigabitEthernet1/0/1 and GigabitEthernet1/0/2.
   c. Click **Modify Selected**.
      The page shown in Figure 225 is displayed.

Figure 224 Selecting ports



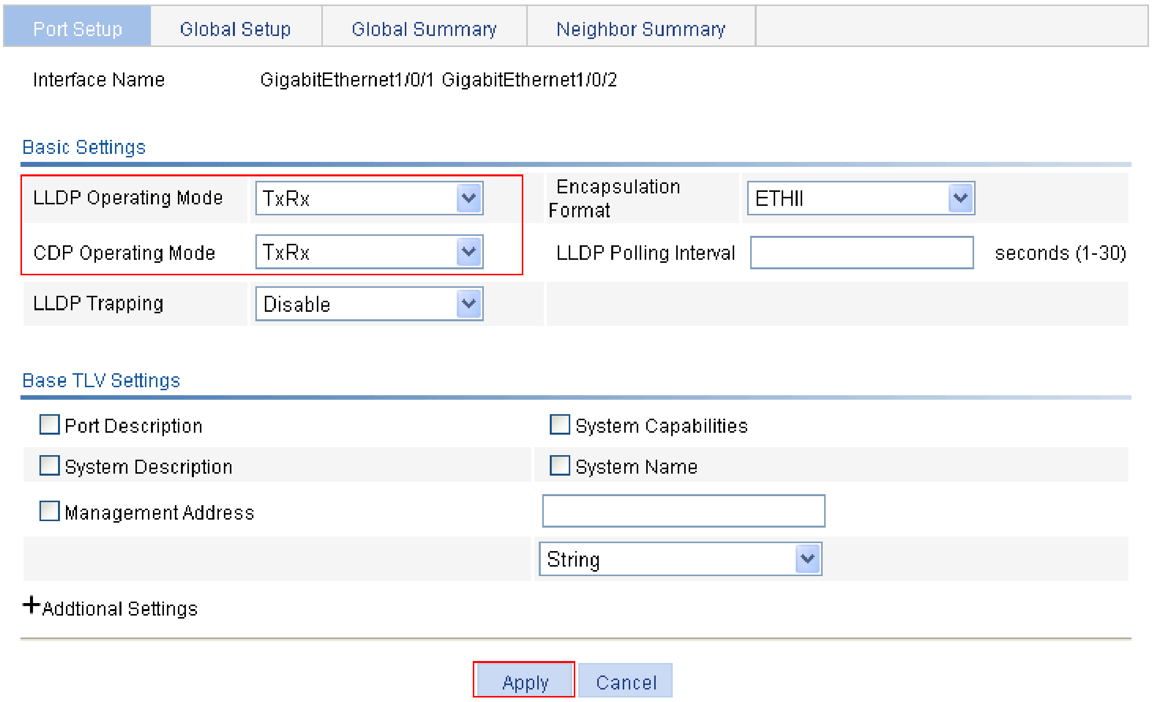
d. Select **TxRx** from the **LLDP Operating Mode** list, and select **TxRx** from the **CDP Operating Mode** list.

e. Click **Apply**.

   A progress dialog box appears.

f. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

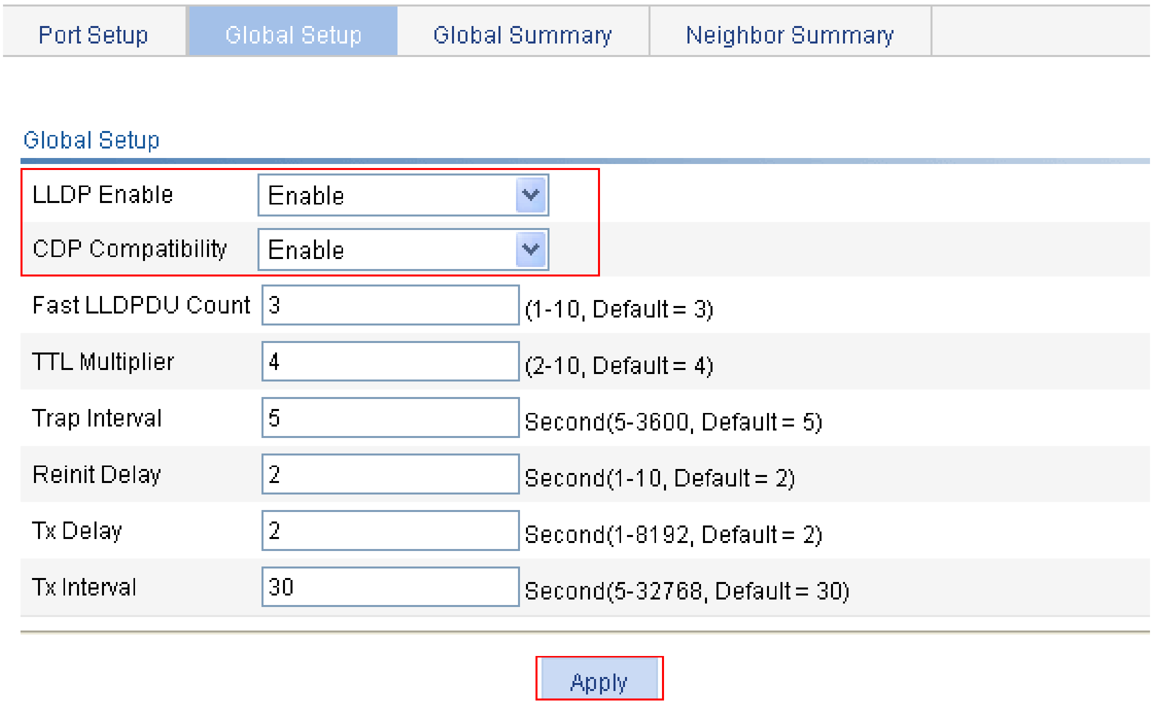
Figure 225 Modifying LLDP settings on ports



6. Enable global LLDP and CDP compatibility of LLDP:
   a. Click the **Global Setup** tab.
   b. Select **Enable** from the **LLDP Enable** list.
   c. Select **Enable** from the **CDP Compatibility** list.
   d. Click **Apply**.

      A progress dialog box appears.
   e. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Figure 226 Enabling global LLDP and CDP compatibility



Verifying the configuration

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 you configure LLDP, follow these guidelines:

- To make LLDP take effect, you must enable it both globally and at port level.
- To advertise LLDP-MED TLVs other than the LLDP-MED capabilities TLV, you must include the LLDP-MED capabilities TLV.
- To remove the LLDP-MED capabilities TLV, you must remove all other LLDP-MED TLVs.
- To remove the MAC/PHY configuration TLV, remove the LLDP-MED capabilities set TLV first.
- When the advertising of LLDP-MED capabilities TLV and MAC/PHY configuration/status TLV is disabled, if the LLDP-MED capabilities set TLV is included, the MAC/PHY configuration/status TLV is included automatically.
- When you configure LLDP settings for ports in batch, if you do not set the TLVs, each port uses its own TLV settings.

Configuring ARP

This chapter describes how to configure the Address Resolution Protocol (ARP).

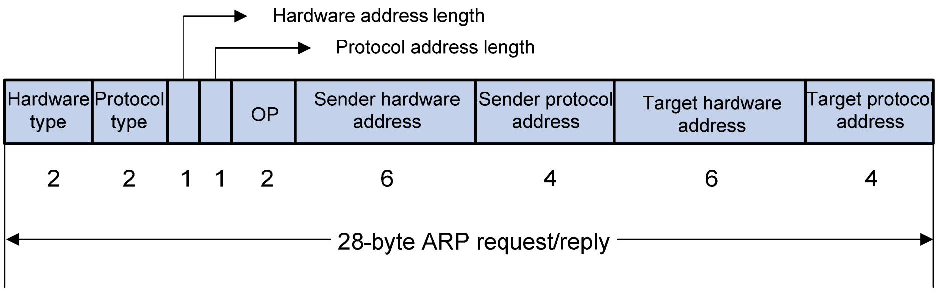
Overview

ARP resolves IP addresses into MAC addresses on Ethernet networks.

ARP message format

ARP messages are classified into ARP requests and ARP replies. Figure 227 shows the format of the ARP request/reply. Numbers in the figure refer to field lengths.

Figure 227 ARP message format



The following describe the fields in Figure 227:

- **Hardware type**—The hardware address type. The value 1 represents Ethernet.
- **Protocol type**—The type of the protocol address to be mapped. The hexadecimal value 0x0800 represents IP.
- **Hardware address length and protocol address length**—Length, in bytes, 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 IPv4 address, the value of the protocol address length field is 4.
- **OP**—Operation code. The type of the ARP message. The value 1 represents an ARP request and 2 represents an ARP reply.
- **Sender hardware address**—Hardware address of the device sending the message.
- **Sender protocol address**—Protocol address of the device sending the message.
- **Target hardware address**—Hardware address of the device the message is being sent to.
- **Target protocol address**—Protocol address of the device the message is being sent to.

ARP operation

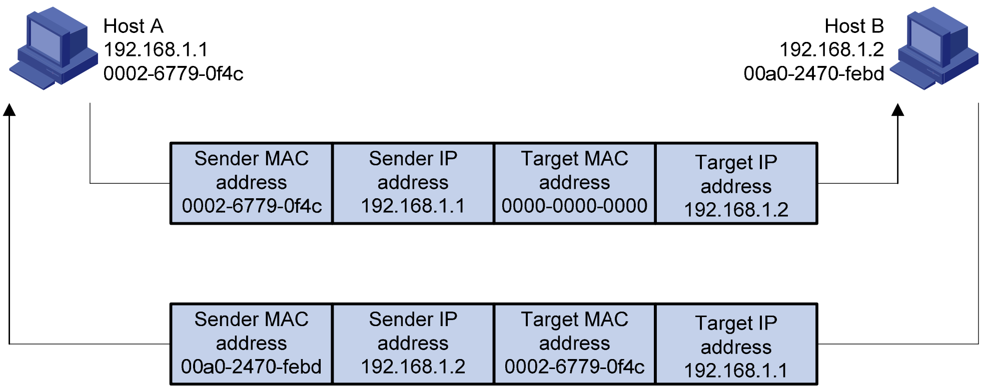
As shown in Figure 228, Host A and Host B are on the same subnet. Host A sends a packet to Host B as follows:

1. Host A looks in 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.

2. If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request using the following information:
   - **Source IP address and source MAC address**—Host A's own IP address and the MAC address
   - **Target IP address**—Host B's IP address
   - **Target MAC address**—An all-zero MAC address

   Because the ARP request is a broadcast, all hosts on this subnet can receive the request, but only the requested host (Host B) will process the request.
3. Host B compares its own IP address with the target IP address in the ARP request. If they are the same, Host B:
   a. Adds the sender IP address and sender MAC address to its ARP table.
   b. Encapsulates its MAC address into an ARP reply.
   c. Unicasts the ARP reply to Host A.
4. After receiving the ARP reply, Host A:
   a. Adds the MAC address of Host B to its ARP table.
   b. Encapsulates the MAC address in the IP packet and sends it to Host B.

Figure 228 ARP address resolution process



If Host A and Host B are not on the same subnet:

5. Host A sends an ARP request to the gateway. The target IP address in the ARP request is the IP address of the gateway.
6. After obtaining the MAC address of the gateway from an ARP reply, Host A sends the packet to the gateway.
7. 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.
8. After obtaining the MAC address of Host B, the gateway sends the packet to Host B.

ARP table

An ARP table contains dynamic and static ARP entries.

Dynamic ARP entry

ARP automatically creates and updates dynamic entries. A dynamic ARP entry is removed when its aging timer expires or the output interface goes down. In addition, a dynamic ARP entry can be overwritten by a static ARP entry.

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.

NOTE:

Usually ARP dynamically resolves IP addresses to MAC addresses, without manual intervention.

Introduction to gratuitous ARP

Gratuitous ARP packets

In a gratuitous ARP packet, the sender IP address and the target IP address are the IP address of the sending device.

A device sends a gratuitous ARP packet for either of the following purposes:

- Determine whether its IP address is already used by another device. If the IP address is already used, the device will be informed of the conflict by an ARP reply.
- Inform other devices of the change of its MAC address.

Enabling learning of gratuitous ARP packets

With this feature enabled, a device, upon receiving a gratuitous ARP packet, adds an ARP entry that contains the sender IP and MAC addresses in the packet to its ARP table. If the corresponding ARP entry exists, the device updates the ARP entry.

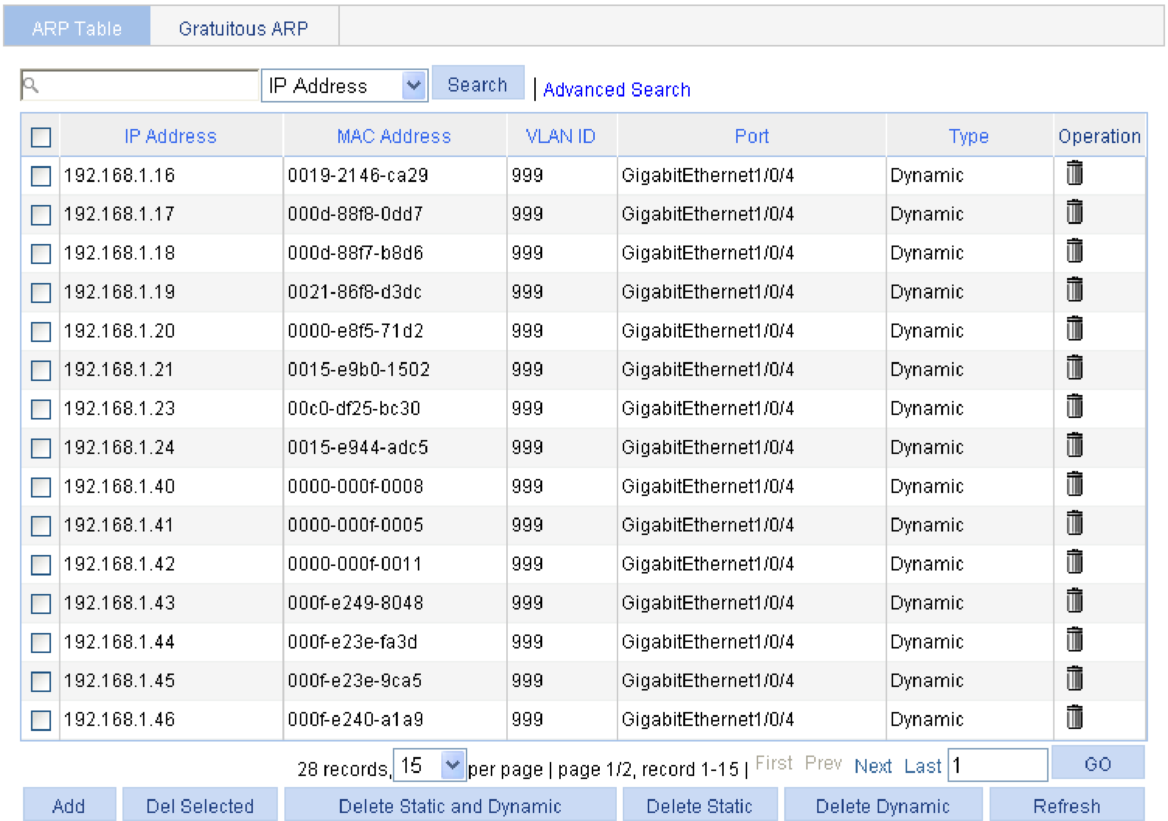
With this feature disabled, the device uses the received gratuitous ARP packets to update existing ARP entries, but not to create new ARP entries.

Configuring ARP entries

Displaying ARP entries

Select **Network** > **ARP Management** from the navigation tree to enter the **ARP Table** page shown in Figure 229. All ARP entries are displayed on the page.

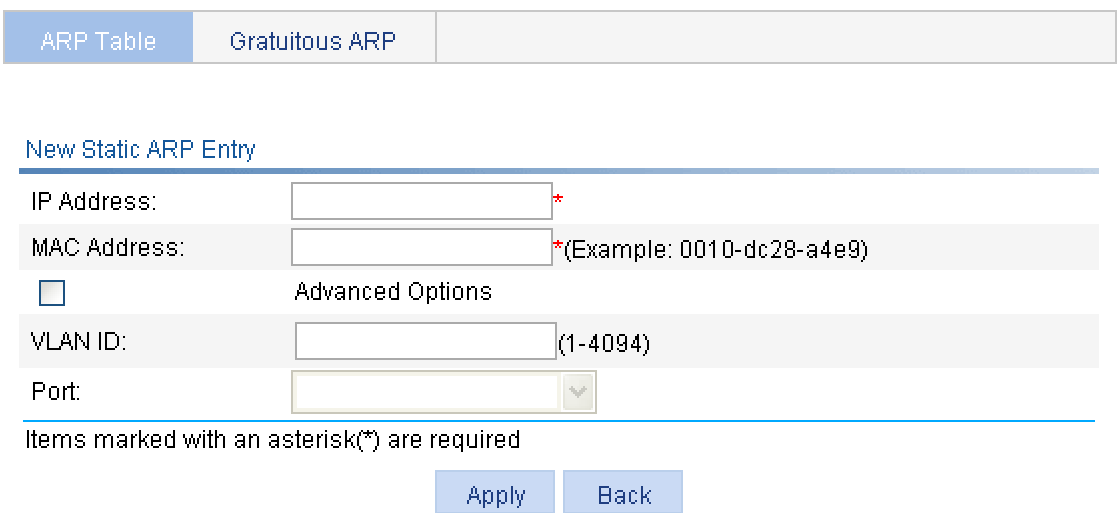
Figure 229 ARP table configuration page



Creating a static ARP entry

1. Select **Network** > **ARP Management** from the navigation tree to enter the **ARP Table** page shown in Figure 229.
2. Click **Add** to enter the **New Static ARP Entry** page.

Figure 230 Adding a static ARP entry



3. Configure the static ARP entry as described in Table 82.
4. Click **Apply**.

Table 82 Configuration items

Item		Description
IP Address		Enter an IP address for the static ARP entry.
MAC Address		Enter a MAC address for the static ARP entry.
Advanced Options	VLAN ID	Enter a VLAN ID and specify a port for the static ARP entry. IMPORTANT: 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	

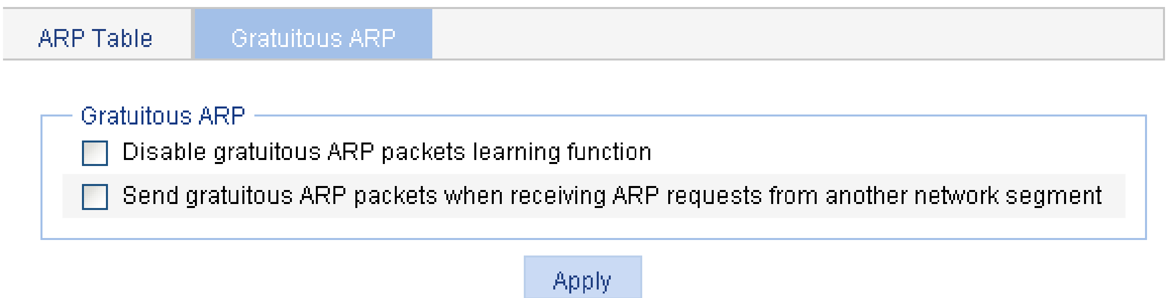
Removing ARP entries

1. Select **Network** > **ARP Management** from the navigation tree to enter the **ARP Table** page shown in Figure 229.
2. Remove ARP entries:
   - To remove specific ARP entries, select the boxes of target ARP entries, and click **Del Selected**.
   - To remove all static and dynamic ARP entries, click **Delete Static and Dynamic**.
   - To remove all static ARP entries, click **Delete Static**.
   - To remove all dynamic ARP entries, click **Delete Dynamic**.

Configuring gratuitous ARP

1. Select **Network** > **ARP Management** from the navigation tree.
2. Click the **Gratuitous ARP** tab.

Figure 231 Gratuitous ARP configuration page



3. Configure gratuitous ARP as described in Table 83.

Table 83 Configuration items

Item	Description
Disable gratuitous ARP packets learning function	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.

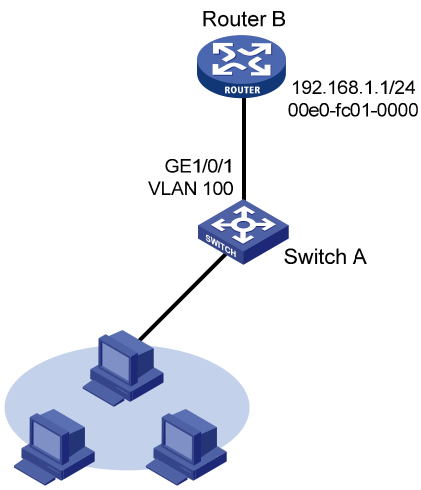
Static ARP configuration example

Network Requirements

As shown in Figure 232, hosts are connected to Switch A, which is connected to Router B through interface GigabitEthernet 1/0/1 belonging to VLAN 100.

Configure static ARP entries on Switch A to enhance communication security between Switch A and Router B.

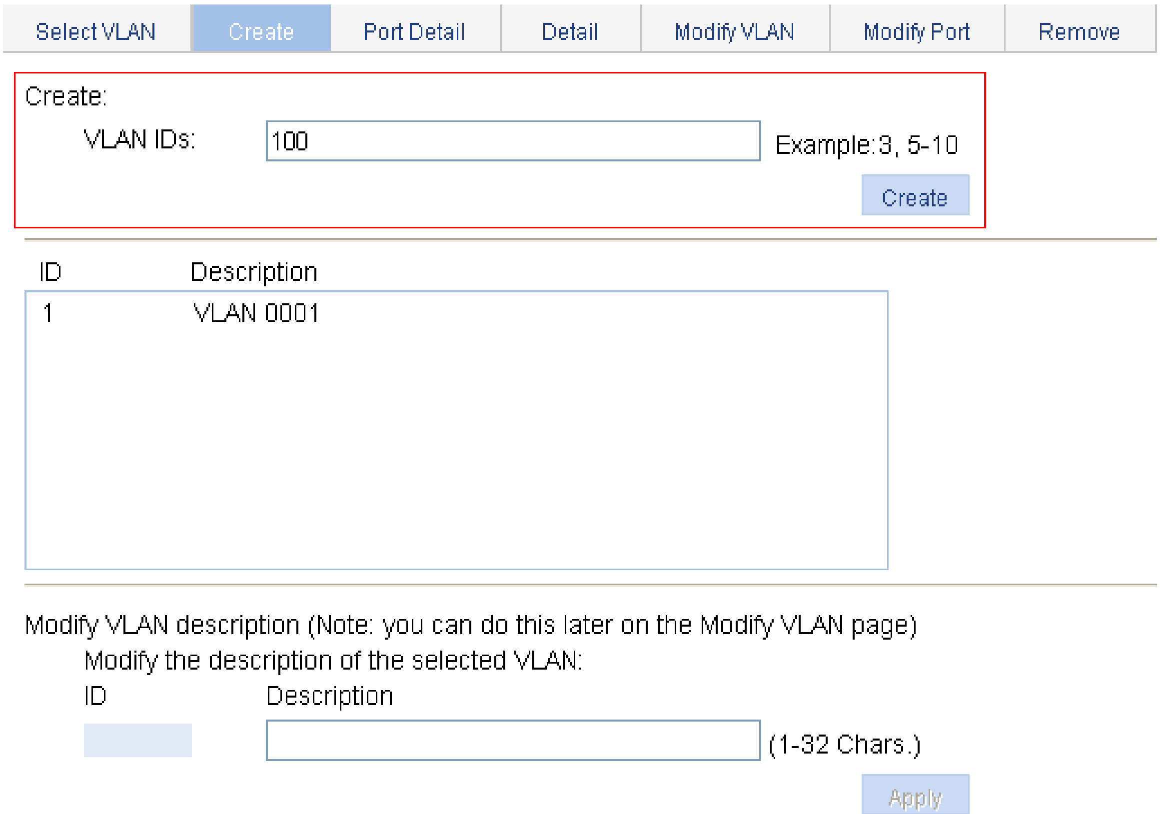
Figure 232 Network diagram



Configuring Switch A

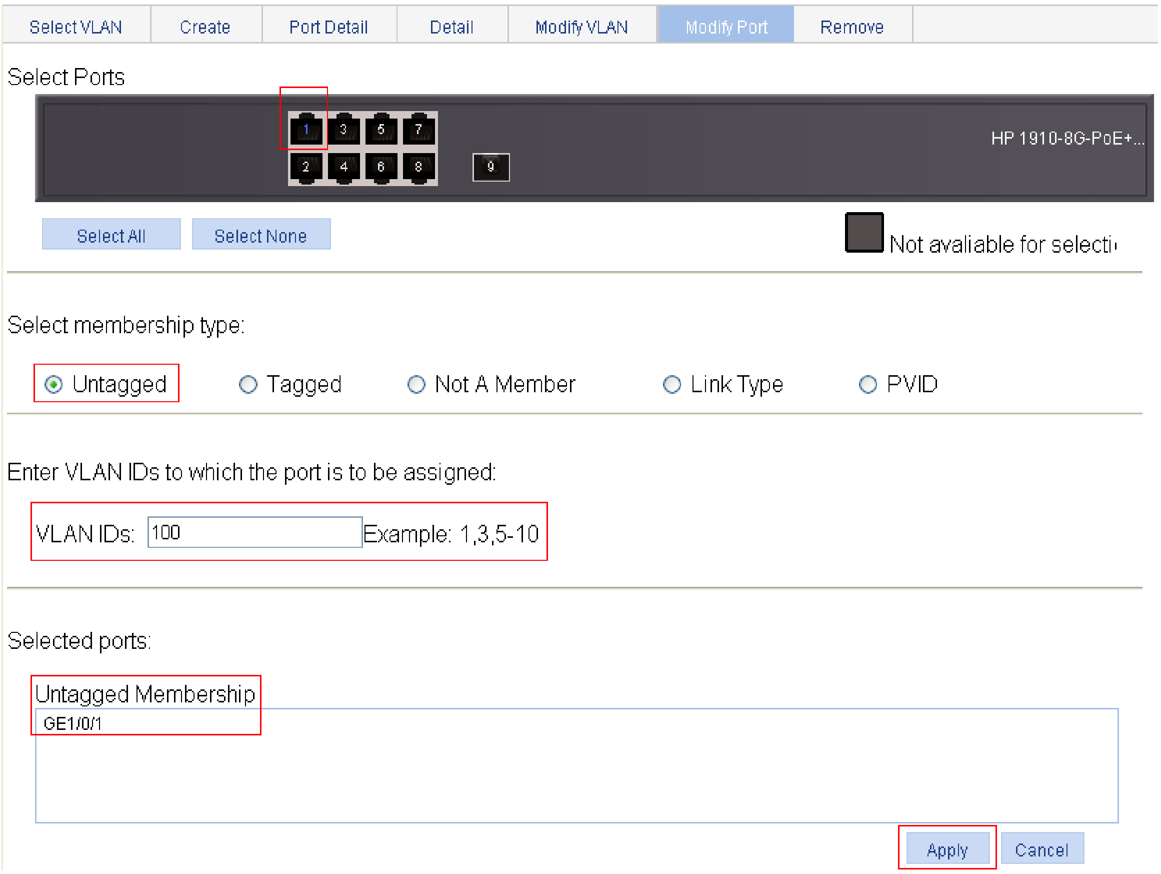
1. Create VLAN 100:
    a. Select **Network** > **VLAN** from the navigation tree.
    b. Click the **Add** tab.
    c. Enter **100** for **VLAN ID** and click **Create**.

Figure 233 Creating VLAN 100



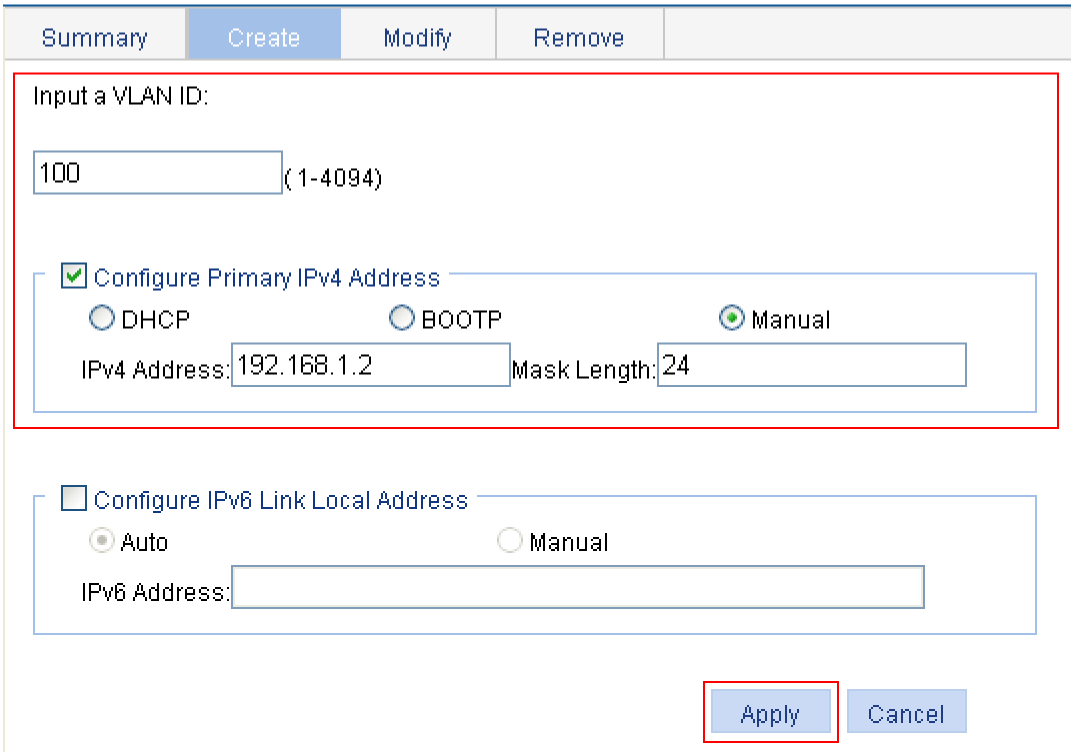
2. Add GigabitEthernet 1/0/1 to VLAN 100:
   a. Click the **Modify Port** tab
   b. Select interface GigabitEthernet 1/0/1 in the **Select Ports** area, select the **Untagged** option in the **Select membership type** area, enter **100** for **VLAN Ids,** and, click **Apply**.
   c. After the configuration process is complete, click **Close**.

Figure 234 Adding GigabitEthernet 1/0/1 to VLAN 100



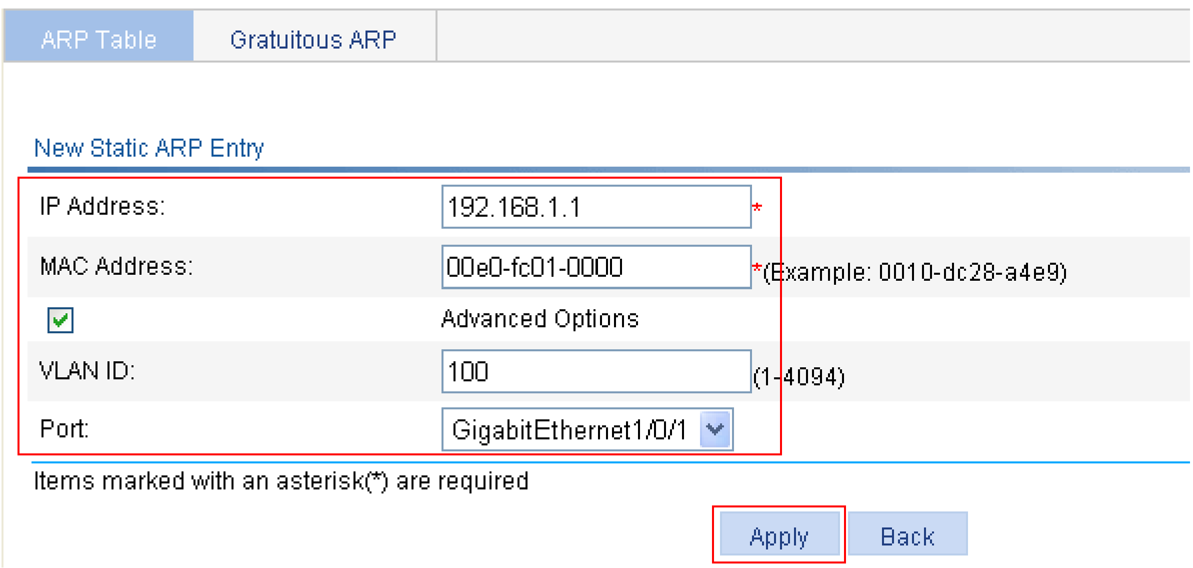
3. Create VLAN-interface 100:
   a. Select **Network** > **VLAN Interface** from the navigation tree.
   b. Click the **Create** tab.
   c. On the page that appears, enter **100** for **VLAN ID**, select the **Configure Primary IPv4 Address** box, select the **Manual** option, enter **192.168.1.2** for **IPv4 Address**, and enter **24** or **255.255.255.0** for **Mask Length**.
   d. Click **Apply**.

Figure 235 Creating VLAN-interface 100



4. Create a static ARP entry:
   a. Select **Network** > **ARP Management** from the navigation tree to enter the **ARP Table** page. Click **Add**.
   b. On the page that appears, enter **192.168.1.1** for **IP Address**, enter **00e0-fc01-0000** for **MAC Address**, select the **Advanced Options** box, enter **100** for **VLAN ID**, and select **GigabitEthernet1/0/1** for **Port**.
   c. Click **Apply**.

Figure 236 Creating a static ARP entry



Configuring ARP attack defense

Overview

Although ARP is easy to implement, it provides no security mechanism and thus is prone to network attacks. The ARP detection feature enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks.

ARP detection provides the following functions: user validity check and ARP packet validity check.

User validity check

This feature does not check ARP packets received from an ARP trusted port. It checks an ARP packet received from an ARP untrusted port as follows.

1. It compares the sender IP and MAC addresses of the ARP packet against the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses.
2. If a match is found in any of the entries, the ARP packet is considered valid and is forwarded. If the sender MAC address of the received ARP packet is an OUI MAC address, the packet is considered valid.
3. If no match is found, the ARP packet is considered invalid and is discarded.

ARP packet validity check

This feature does not check ARP packets received from an ARP trusted port. It checks ARP packets received from ARP untrusted ports based on the following objects:

- **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.

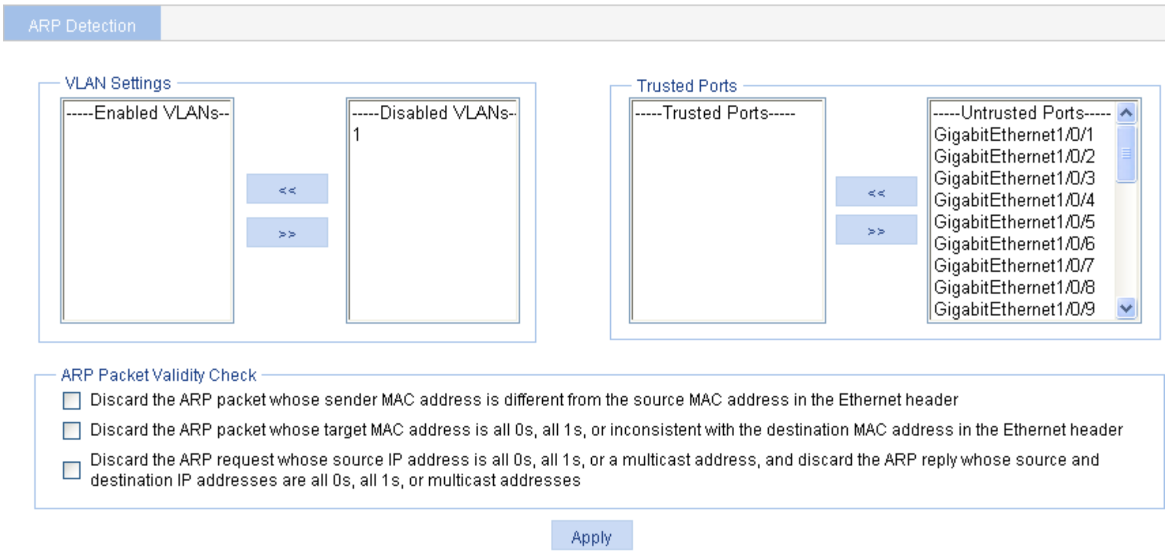
Configuring ARP detection

NOTE:

To check user validity, at least the DHCP snooping entries or 802.1X security entries must be available. Otherwise, all ARP packets received from an ARP untrusted port will be discarded, except for the ARP packets with an OUI MAC address as the sender MAC address when voice VLAN is enabled.

1. Select **Network** > **ARP Anti-Attack** from the navigation tree to enter the ARP detection configuration page.

Figure 237 ARP detection configuration page



2. Configure ARP detection as described in Table 84.
3. Click **Apply**.

Table 84 Configuration items

Item	Description
VLAN Settings	Select VLANs on which ARP detection is to be enabled. To add VLANs to the **Enabled VLANs** list box, select one or multiple VLANs from the **Disabled VLANs** list box and click the **<<** button. To remove VLANs from the **Enabled VLANs** list box, select one or multiple VLANs from the list box and click the **>>** button.
Trusted Ports	Select trusted ports and untrusted 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.
ARP Packet Validity Check	Select ARP packet validity check modes: • Discard the ARP packet whose sender MAC address is different from the source MAC address in the Ethernet header. • Discard the ARP packet whose target MAC address is all 0s, all 1s, or inconsistent with the destination MAC address in the Ethernet header. • Discard the ARP request whose source IP address is all 0s, all 1s, or a multicast address, and discard the ARP reply whose source and destination IP addresses are all 0s, all 1s, or multicast addresses. If none of the above is selected, the system does not check the validity of ARP packets. If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

Configuring IGMP snooping

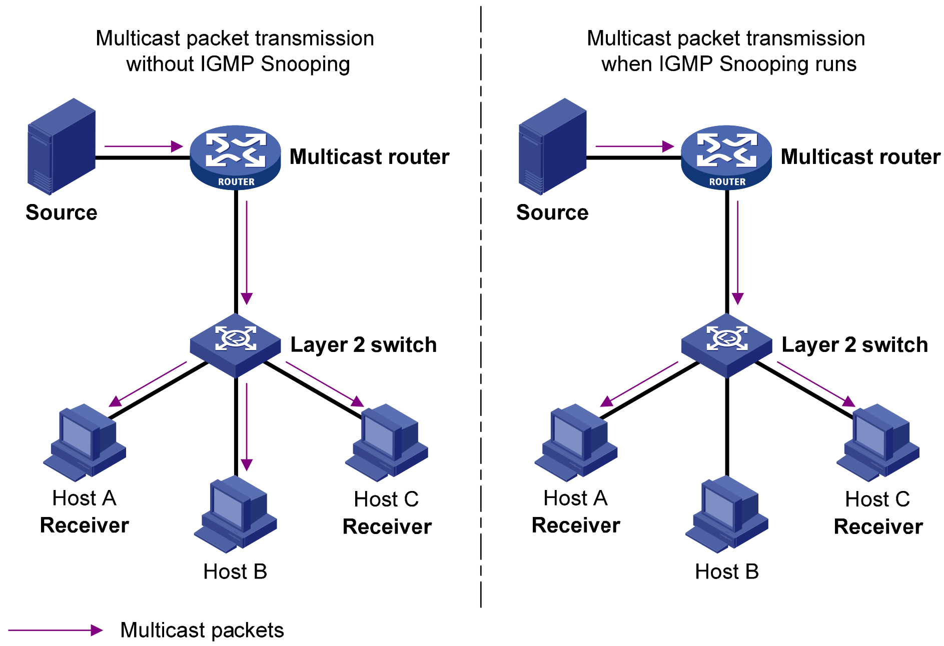
Overview

Internet Group Management Protocol (IGMP) snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

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 238, when IGMP snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. When IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than flooded to all hosts at Layer 2.

Figure 238 Multicast forwarding before and after IGMP snooping runs



IGMP snooping enables the Layer 2 switch to forward multicast data only to the receivers that require the data at Layer 2. It has the following advantages:

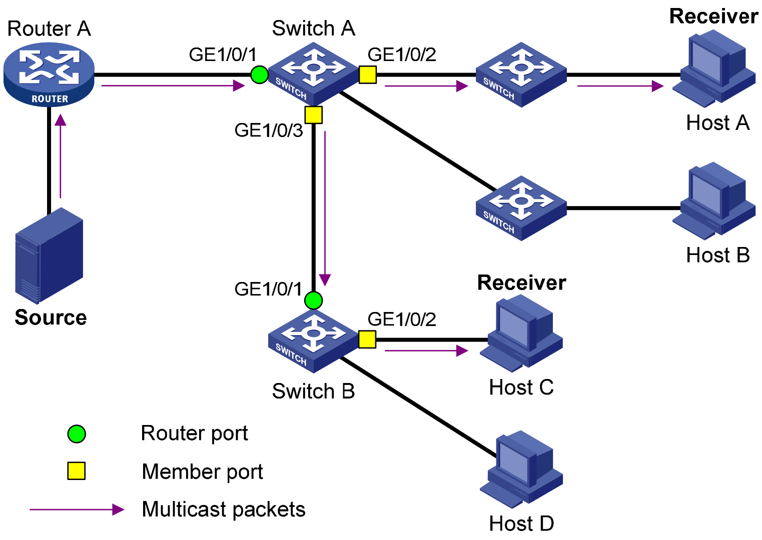
- Reducing Layer 2 broadcast packets and saving network bandwidth
- Enhancing the security of multicast traffic
- Facilitating the implementation of per-host accounting

Basic concepts in IGMP snooping

IGMP snooping related ports

As shown in Figure 239, Router A connects to the multicast source, IGMP snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (multicast group members).

Figure 239 IGMP snooping related ports



IGMP snooping related ports include the following types:

- **Router port**—Port on an Ethernet switch that leads the switch toward a Layer 3 multicast device (designated router or IGMP querier). In Figure 239, GigabitEthernet 1/0/1 of Switch A and Ethernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.

  In this document, a router port is a port on the switch that leads the switch toward a Layer 3 multicast device, rather than a port on a router.
- **Member port**—Port on an Ethernet switch that leads the switch toward multicast group members. In Figure 239, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet1/0/2 of Switch B are member ports. A switch registers all local member ports in the IGMP snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document consist of dynamic and static ports.

NOTE:

An IGMP snooping enabled switch deems that all its ports that receive IGMP general queries with the source address other than 0.0.0.0 or that receive PIM hello messages are dynamic router ports.

Aging timers for dynamic ports in IGMP snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Dynamic router port aging timer	For each dynamic router port, the switch sets an aging timer. When the timer expires, the dynamic router port ages out.	IGMP general query of which the source address is not 0.0.0.0 or PIM hello	The switch removes this port from its router port list.

Timer	Description	Message before expiry	Action after expiry
Dynamic member port aging timer	When a port dynamically joins a multicast group, the switch sets an aging timer for the port. When the timer expires, the dynamic member port ages out.	IGMP membership report	The switch removes this port from the IGMP snooping forwarding table.

NOTE:

In IGMP snooping, only dynamic ports age out. Static ports never age out.

How IGMP snooping operates

In this section, the ports involved are dynamic ports.

An IGMP snooping–enabled switch performs different actions when it receives different IGMP messages.

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 check whether any active multicast group members exist on the subnet.

After receiving an IGMP general query, the switch forwards it through all ports in the VLAN (except the port that received the query). The switch performs the following judgment:

- If the port that received the query is a dynamic router port in the router port list of the switch, the switch restarts the aging timer for the port.
- If the port that received the query is not in the router port list of the switch, the switch adds it into the router port list as a dynamic router port and starts an 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:

- After receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When the host wants to join a multicast group, it sends an IGMP report to the querier to announce its interest in the multicast information addressed to that group.

After receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group. The switch also performs the following judgment:

- If no forwarding entry matches the group address, the switch creates a forwarding entry for the group, adds the port that received the IGMP report as a dynamic member port to the forwarding entry, and starts an aging timer for that port.
- If a forwarding entry matches the group address, but the port that received the IGMP report is not in the forwarding entry for the group, the switch adds the port as a dynamic member port to the forwarding entry, and starts an aging timer for that port.
- If a forwarding entry matches the group address and the port that received the IGMP report is in the forwarding entry for the group, the switch resets an aging timer for that port.

A switch does not forward an IGMP report through a non-router port. The reason is that if the switch forwards a report through a member port, all the attached hosts that monitor the reported multicast group address, according to the IGMP report suppression mechanism, suppress their own reports after receiving this report. This makes the switch unable to know whether the reported multicast group still has active members attached to that port.

When receiving a leave group message

When an IGMPv1 host leaves a 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, because the host stops sending IGMP membership reports as soon as it leaves a multicast group, the switch removes the dynamic member port that connects to the host from the forwarding entry for the multicast group when the aging timer for the port expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router. When the switch receives an IGMP leave group message on a member port, it first checks whether a forwarding entry matches the group address in the message, and, if a match is found, whether the forwarding entry for the group contains the dynamic member port.

- If no forwarding entry matches the group address, or if the forwarding entry does not contain the port, the switch directly discards the IGMP leave group message.
- If a forwarding entry matches the group address and the forwarding entry contains the port, the switch forwards the IGMP leave group message to all router ports in the VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that group address, the switch does not immediately remove the port from the forwarding entry for that group. Instead, the switch resets the aging timer for that port.

After receiving the IGMP leave message, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to that multicast group through the port that received the leave message. After receiving 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. The switch also performs the following judgment on the port that received the IGMP leave message:

- If the port (assuming that it is a dynamic member port) receives any IGMP report in response to the group-specific query before its aging timer expires, it indicates 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 port.
- If the port receives no IGMP report in response to the group-specific query before its aging timer expires, it indicates that no hosts attached to the port are still listening to that group address. The switch removes the port from the forwarding entry for the multicast group when the aging timer expires.

Protocols and standards

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

Recommended configuration procedure

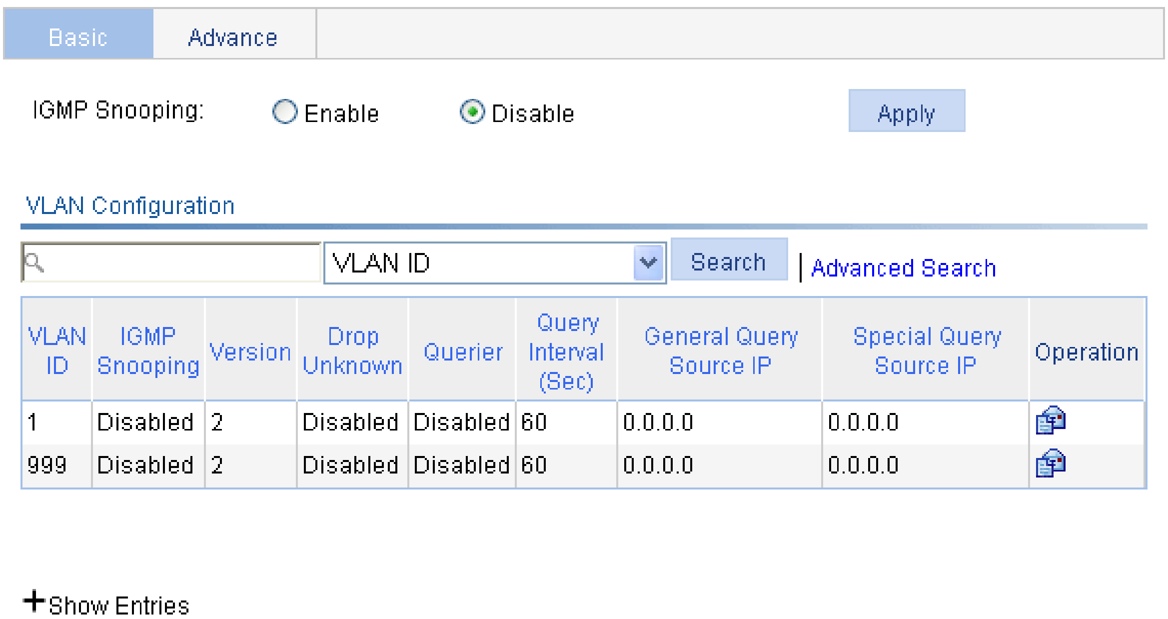
Step	Remarks
1. Enabling IGMP snooping globally	(Required.) Disabled by default.

Step	Remarks
2. Configuring IGMP snooping in a VLAN	(Required.) Enable IGMP snooping for the VLAN and configure the IGMP snooping version and querier. By default, IGMP snooping is disabled in a VLAN. IMPORTANT: • IGMP snooping must be enabled globally before you enable it for a VLAN. • When you enable IGMP snooping for a VLAN, this function takes effect for the ports only in this VLAN.
3. Configuring IGMP snooping on a port	(Optional.) Configure the maximum number of multicast groups allowed and the fast-leave function for ports in the specified VLAN. IMPORTANT: • IGMP snooping must be enabled globally before you enable it for a port. • IGMP snooping configured on a port takes effect only after IGMP snooping is enabled for the VLAN.
4. Displaying IGMP snooping multicast table entries	(Optional.)

Enabling IGMP snooping globally

1. Select **Network** > **IGMP snooping** from the navigation tree.
2. Click **Enable** for IGMP snooping.
3. Click **Apply**.

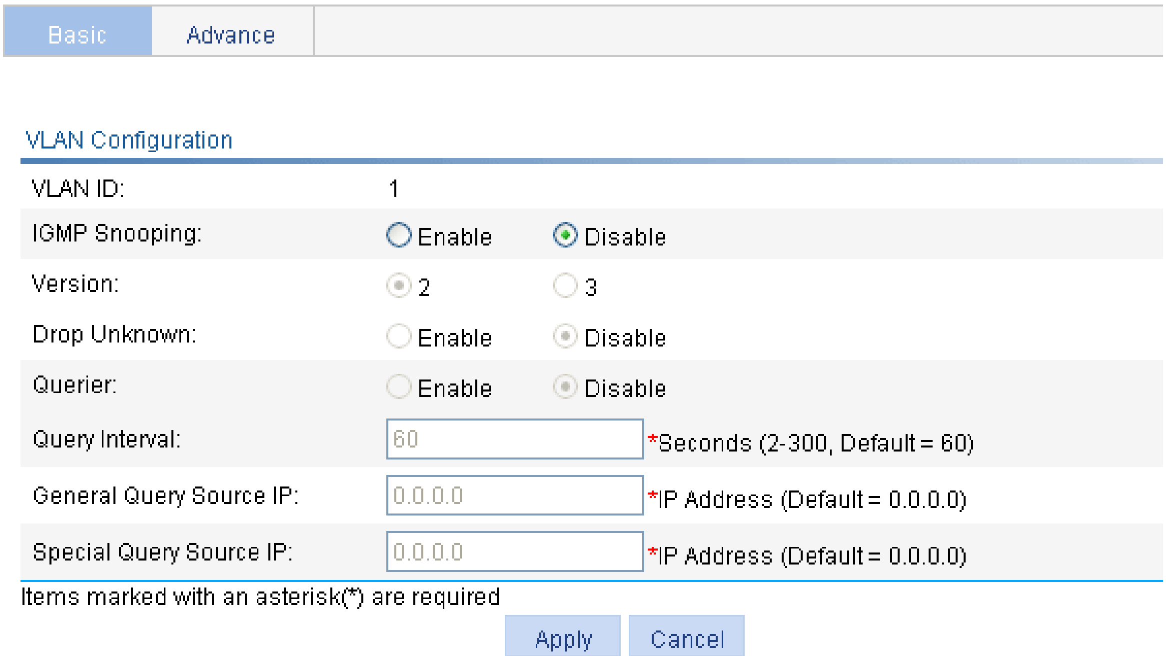
Figure 240 Basic IGMP snooping configurations



Configuring IGMP snooping in a VLAN

1. Select **Network** > **IGMP snooping** from the navigation tree.
2. Click the icon corresponding to the VLAN.

Figure 241 VLAN configuration



3. Configure the parameters as described in Table 85.
4. Click **Apply**.

Table 85 Configuration items

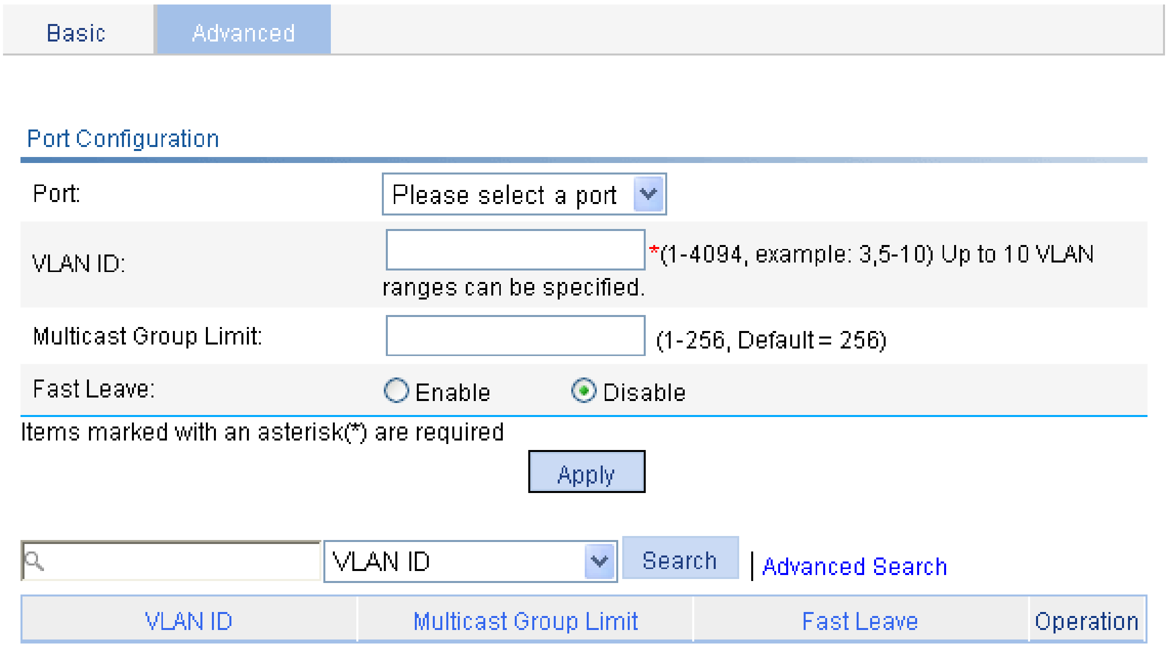
Item	Description
IGMP snooping	Enable or disable IGMP snooping in the VLAN. You can proceed with the subsequent configurations only if **Enable** is selected here.
Version	By configuring an IGMP snooping version, you actually configure the versions of IGMP messages that IGMP snooping can process. • IGMPv2 snooping can process IGMPv1 and IGMPv2 messages, but cannot process IGMPv3 messages, which will be flooded in the VLAN. • IGMPv3 snooping can process IGMPv1, IGMPv2 and IGMPv3 messages. ⚠ IMPORTANT: If you change the IGMPv3 snooping to IGMPv2 snooping, the system clears all IGMP snooping forwarding entries that are dynamically added.

Item	Description
Drop Unknown	Enable or disable the function of dropping unknown multicast packets. Unknown multicast data refers to multicast data for which no entries exist in the IGMP snooping forwarding table. • If the function of dropping unknown multicast data is enabled, the switch forwards the unknown multicast packets to the router ports instead of flooding them in the VLAN. If the switch does not have a router port, it drops the unknown multicast packets. • If the function of dropping unknown multicast data is disabled, the switch floods the unknown multicast data in the VLAN to which the unknown multicast data belong.
Querier	Enable or disable the IGMP snooping querier function. In an IP multicast network that runs IGMP, a Layer 3 device is elected as the IGMP querier to send IGMP queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries for correct multicast traffic forwarding at the network layer. 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 for correct multicast traffic forwarding at data link layer.
Query interval	Configure the IGMP general query interval.
General Query Source IP	Specify the source IP address of general queries
Special Query Source IP	Specify the source IP address of group-specific queries

Configuring IGMP snooping on a port

1. Select **Network** > **IGMP snooping** from the navigation tree.
2. Click the **Advanced** tab.

Figure 242 Advanced configuration



3. Configure the parameters as described in Table 86.
4. Click **Apply**.

Table 86 Configuration items

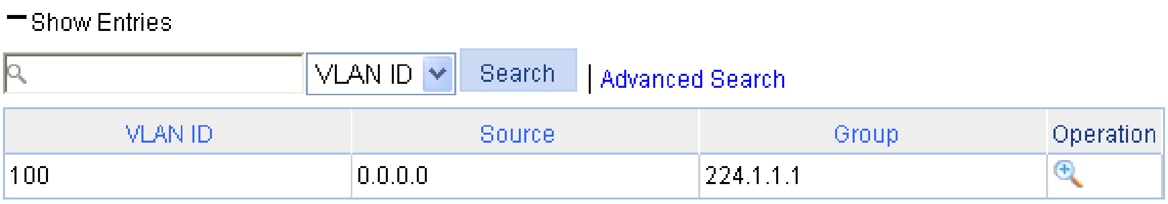
Item	Description
Port	Select the port on which advanced IGMP snooping features will be configured. The port can be an Ethernet port or Layer-2 aggregate port. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. TIP: Advanced IGMP snooping 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. IMPORTANT: 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.

Item	Description
Fast Leave	Enable or disable the fast-leave function for the port. With the fast-leave function enabled on a port, when the switch receives an IGMP leave message on the port, it immediately deletes that port from the outgoing port list of the corresponding forwarding table entry. Then, when the switch receives IGMP group-specific queries for that multicast group, it does not forward them to that port. On a port that has only one host attached, you can enable fast-leave processing to save bandwidth and resources. However, on a port that has multiple hosts attached, do not enable fast-leave processing if you have enabled dropping unknown multicast data for the VLAN which the port belongs to. Otherwise, if a host on the port leaves a multicast group, the other hosts attached to the port in the same multicast group cannot receive the multicast data for the group.

Displaying IGMP snooping multicast table entries

1. Select **Network** > **IGMP snooping** from the navigation tree.
2. Click **Show Entries** to display information about IGMP snooping multicast table entries.

Figure 243 Displaying entry information



3. To view detailed information about an entry, click the icon corresponding to the entry.

Figure 244 Detailed information about an IGMP snooping multicast entry

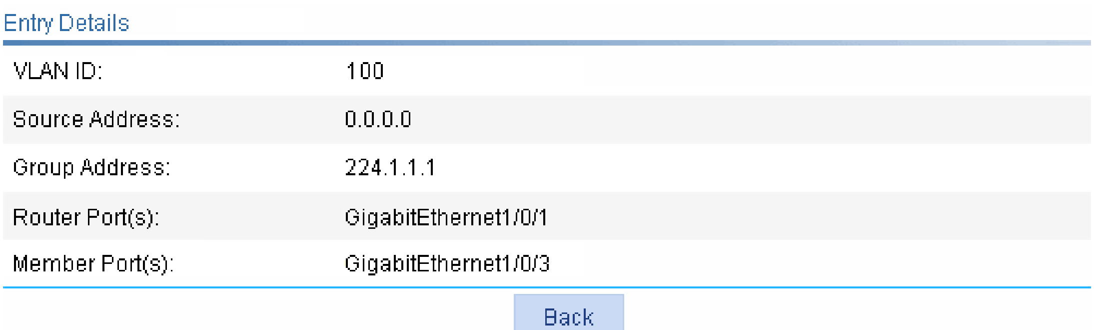


Table 87 Field description

Field	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.

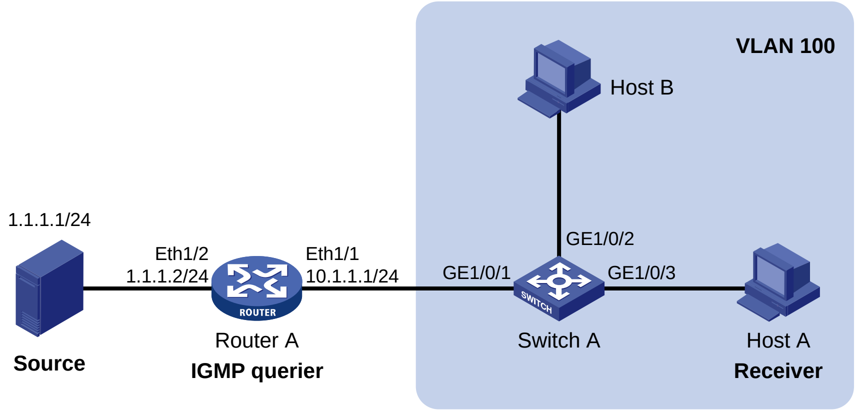
IGMP snooping configuration example

Network requirements

As shown in Figure 245, IGMPv2 runs on Router A and IGMPv2 snooping runs on Switch A. Router A acts as the IGMP querier.

Perform the configuration so that Host A can receive the multicast data destined for the multicast group (224.1.1.1), and Switch A drops the unknown multicast data rather than flooding it in the VLAN.

Figure 245 Network diagram



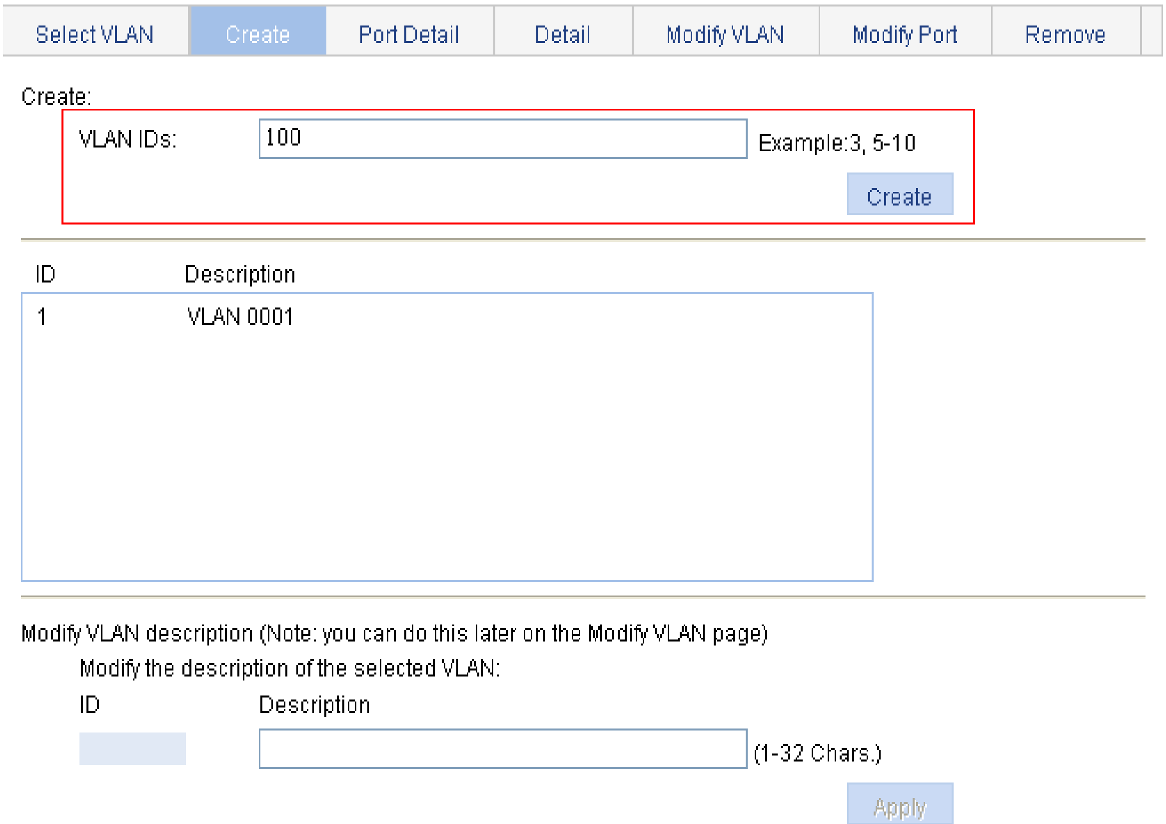
Configuring Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/1. (Details not shown.)

Configuring Switch A

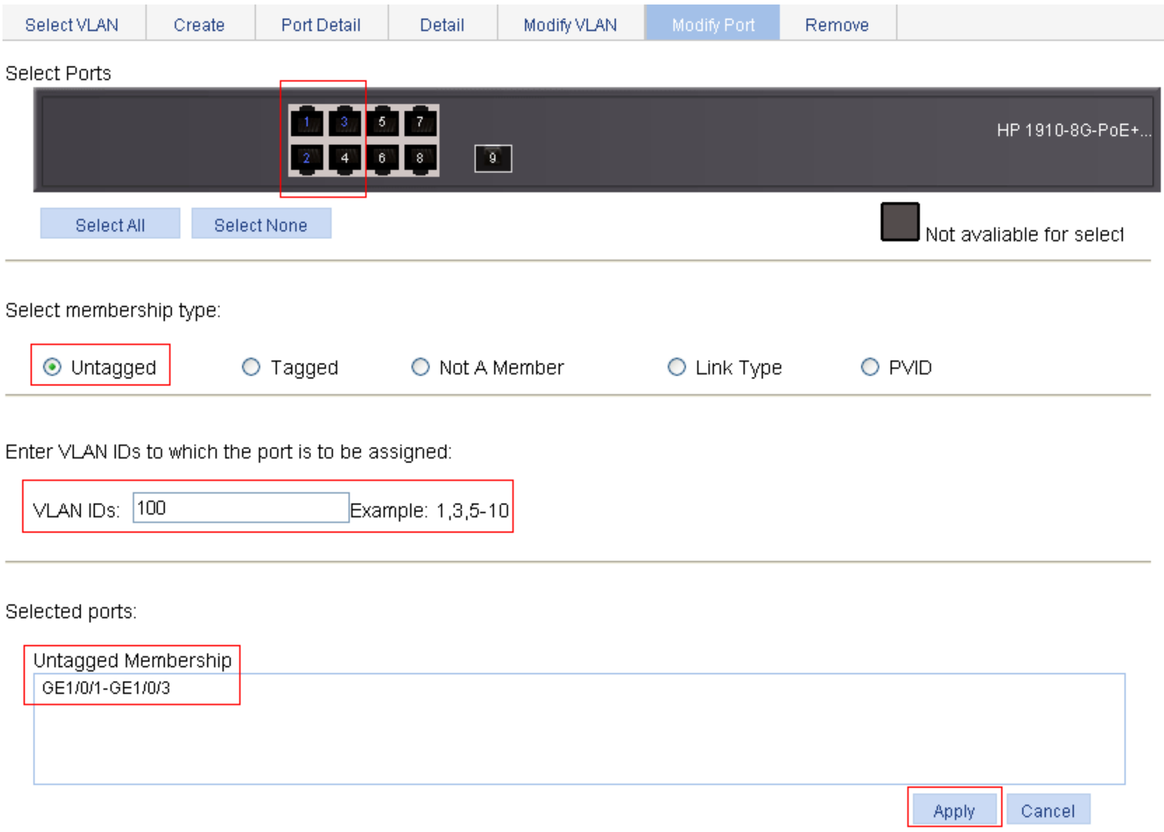
1. Create VLAN 100:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter 100 as the VLAN ID.
   d. Click **Apply**.

Figure 246 Creating VLAN 100



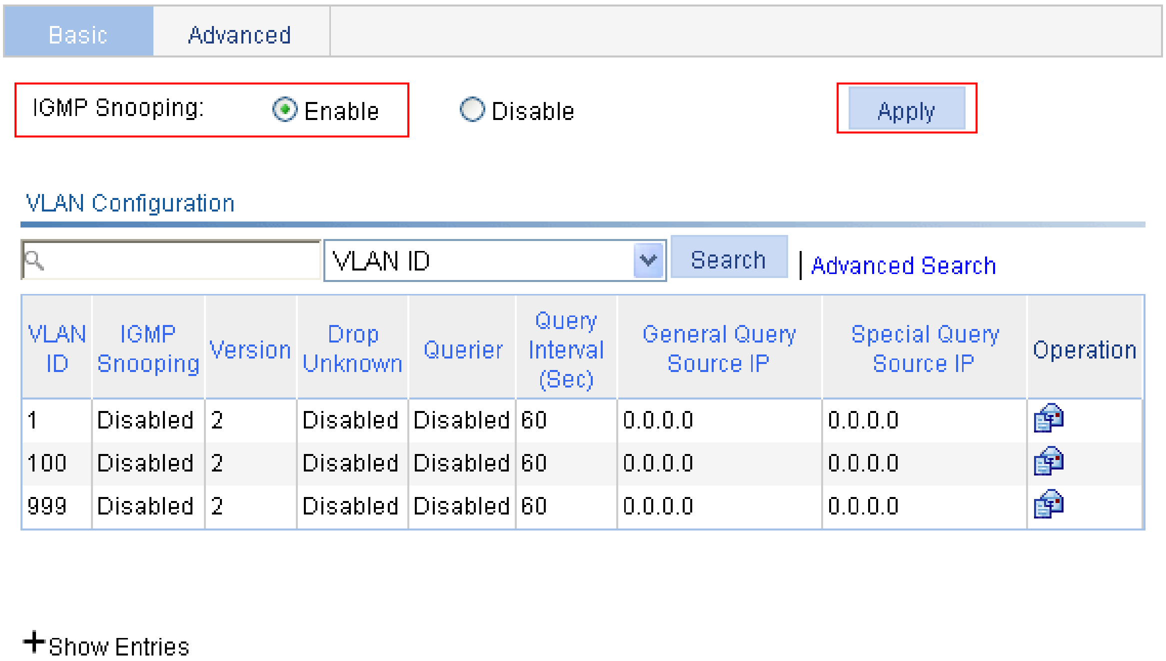
2. Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100:
   a. Click the **Modify Port** tab.
   b. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** field.
   c. Select the **Untagged** option for **Select membership type**.
   d. Enter 100 as the VLAN ID.
   e. Click **Apply**.

Figure 247 Assigning a port to the VLAN



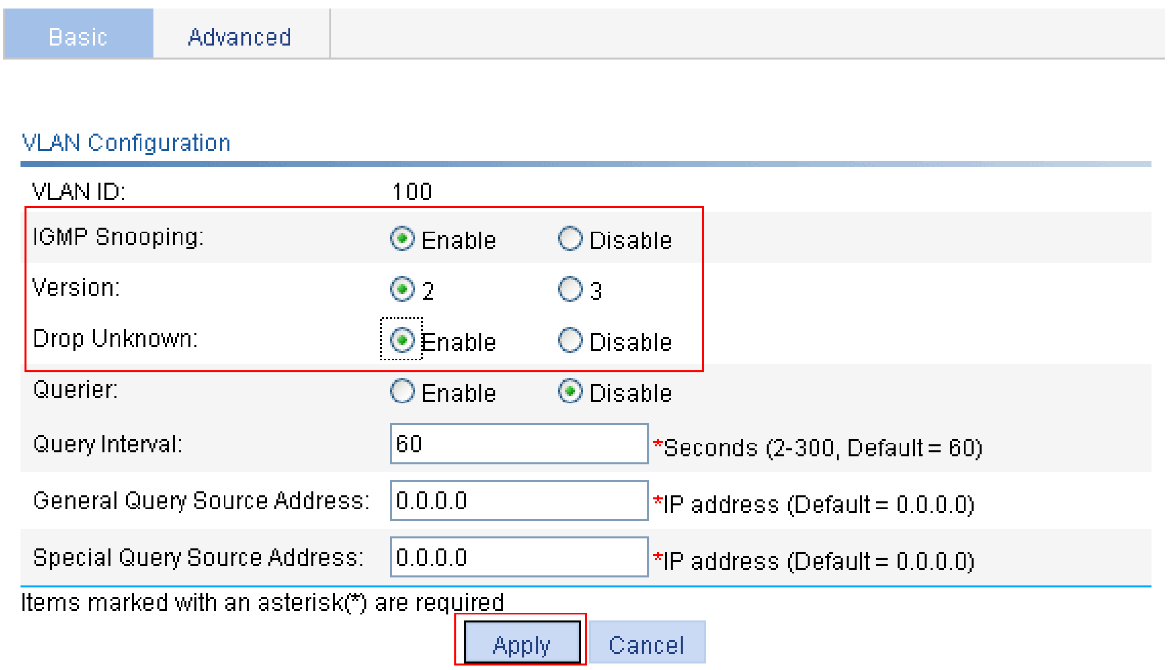
3. Enable IGMP snooping globally:
   a. Select **Network** > **IGMP snooping** from the navigation tree.
   b. Select the **Enable option.**
   c. Click **Apply**.

Figure 248 Enabling IGMP snooping globally



4. Enable IGMP snooping and the function of dropping unknown multicast data for VLAN 100:
   a. Click the icon corresponding to VLAN 100.
   b. Select the **Enable** option for **IGMP snooping**.
   c. Select the **2** option for **Version**.
   d. Select the **Enable** option for **Drop Unknown**.
   e. Click **Apply**.

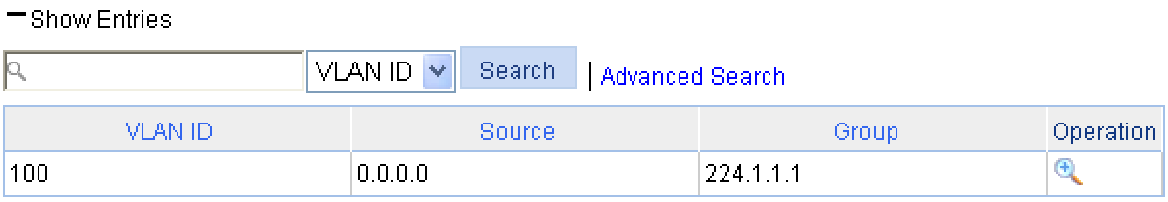
Figure 249 Enabling IGMP snooping in the VLAN



Verifying the configuration

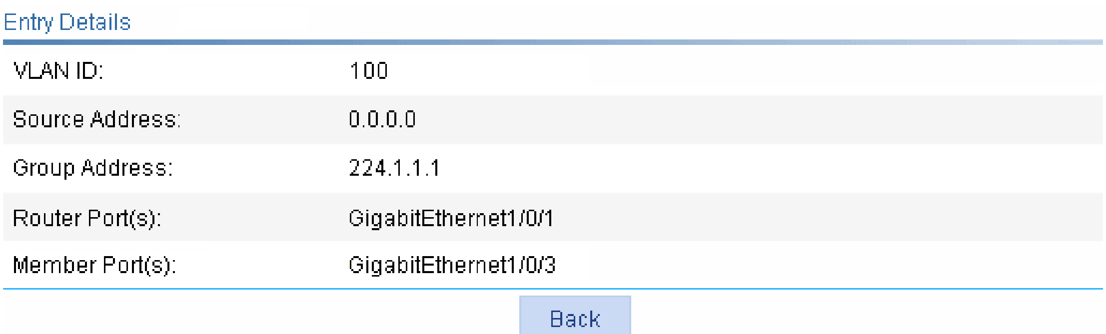
1. Select **Network** > **IGMP snooping** from the navigation tree.
2. Click **Show Entries** in the basic VLAN configuration page to display information about IGMP snooping multicast entries.

Figure 250 IGMP snooping multicast entry information displaying page



3. Click the icon corresponding to the multicast entry (0.0.0.0, 224.1.1.1) to view information about this entry.

Figure 251 IGMP snooping multicast entry information



The output shows that GigabitEthernet 1/0/3 of Switch A is listening to multicast streams destined for multicast group 224.1.1.1.

Configuring MLD snooping

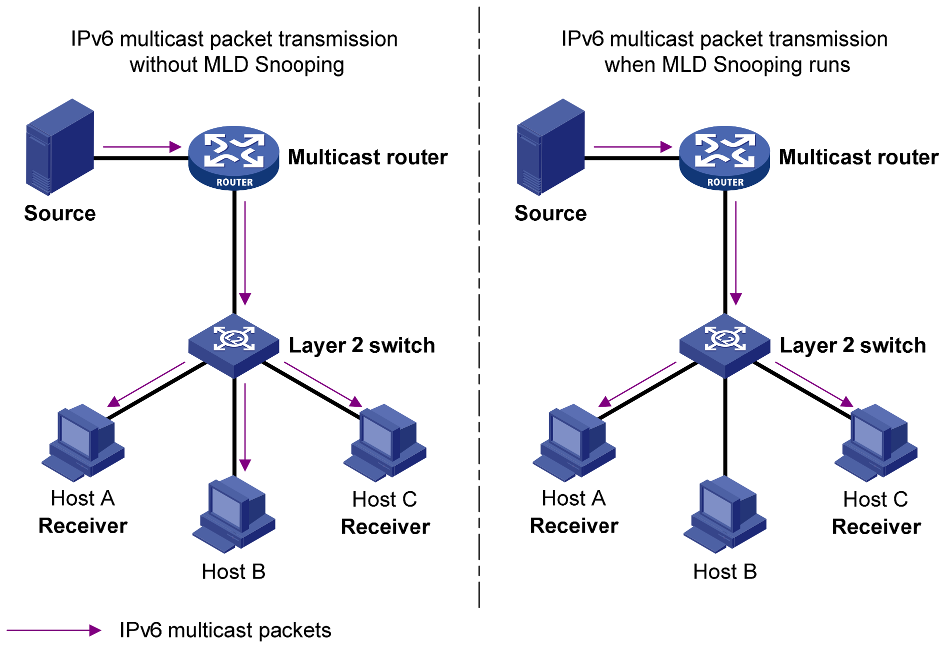
Overview

Multicast Listener Discovery (MLD) snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups.

By analyzing received MLD messages, a Layer 2 device running MLD snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

As shown in Figure 252, when MLD snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. When MLD snooping is running on the switch, IPv6 multicast packets for known multicast groups are multicast to the receivers, rather than flooded to all hosts at Layer 2.

Figure 252 IPv6 multicast forwarding before and after MLD snooping runs



MLD snooping enables the Layer 2 switch to forward IPv6 multicast data only to the receivers that require the data at Layer 2. It has the following advantages:

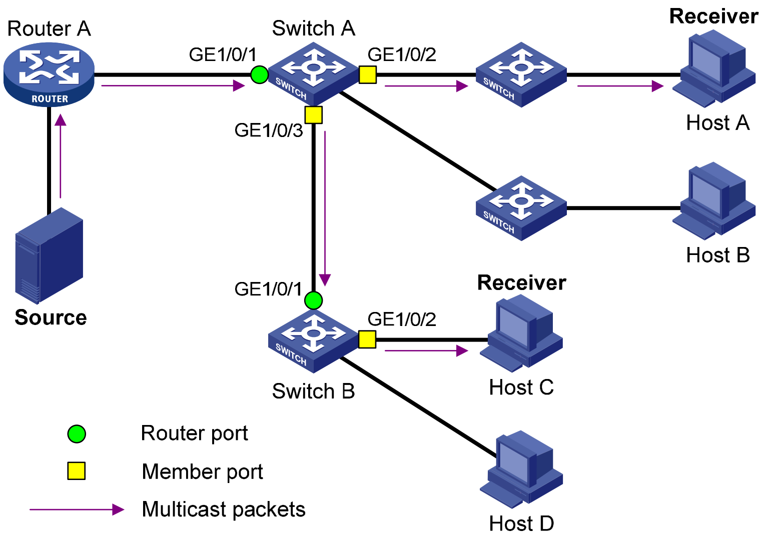
- Reducing Layer 2 broadcast packets and saving network bandwidth
- Enhancing the security of IPv6 multicast traffic
- Facilitating the implementation of per-host accounting

Basic concepts in MLD snooping

MLD snooping related ports

As shown in Figure 253, Router A connects to the multicast source, MLD snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (IPv6 multicast group members).

Figure 253 MLD snooping related ports



MLD snooping related ports include the following types:

- **Router port**—Port on an Ethernet switch that leads the switch toward a Layer 3 multicast device (designated router or MLD querier). As shown in Figure 253, GigabitEthernet 1/0/1 of Switch A and Ethernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.

  In this document, a router port is a port on the switch that leads the switch toward a Layer 3 multicast device, rather than a port on a router.
- **Member port**—Port on an Ethernet switch that leads the switch toward IPv6 multicast group members. As shown in Figure 253, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet1/0/2 of Switch B are member ports. A switch registers all local member ports in the MLD snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document consist of dynamic and static ports.

NOTE:

An MLD snooping enabled switch deems that all its ports that receive MLD general queries with the source address other than 0::0 or that receive IPv6 PIM hello messages are dynamic router ports.

Aging timers for dynamic ports in MLD snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Dynamic router port aging timer	For each dynamic router port, the switch sets an aging timer. When the timer expires, the dynamic router port ages out.	MLD general query of which the source address is not 0::0 or IPv6 PIM hello	The switch removes this port from its router port list.

Timer	Description	Message before expiry	Action after expiry
Dynamic member port aging timer	When a port dynamically joins an IPv6 multicast group, the switch sets an aging timer for the port. When the timer expires, the dynamic member port ages out.	MLD membership report	The switch removes this port from the MLD snooping forwarding table.

NOTE:

In MLD snooping, only dynamic ports age out. Static ports never age out.

How MLD snooping operates

In this section, the ports involved are dynamic ports.

An MLD snooping–enabled switch performs different actions when it receives different MLD messages.

When receiving a general query

The MLD querier periodically sends MLD general queries to all hosts and routers (FF02::1) on the local subnet to check whether any active IPv6 multicast group members exist on the subnet.

After receiving an MLD general query, the switch forwards it through all ports in the VLAN (except the port that received the query). The switch performs the following judgment:

- If the port that received the query is a dynamic router port in the router port list of the switch, the switch restarts the aging timer for the port.
- If the port that received the query is not in the router port list of the switch, the switch adds it into the router port list as a dynamic router port and starts an aging timer for the port.

When receiving a membership report

A host sends an MLD membership report to the MLD querier in the following circumstances:

- After receiving an MLD query, an IPv6 multicast group member host responds with an MLD report.
- When the host wants to join an IPv6 multicast group, it sends an MLD report to the querier to announce its interest in the multicast information addressed to that group.

After receiving an MLD report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported IPv6 multicast group. The switch also performs the following judgment:

- If no forwarding entry matches the IPv6 group address, the switch creates a forwarding entry for the group, adds the port that received the MLD report as a dynamic member port to the forwarding entry, and starts an aging timer for that port.
- If a forwarding entry matches the IPv6 group address, but the port that received the MLD report is not in the forwarding entry for the group, the switch adds the port as a dynamic member port to the forwarding entry, and starts an aging timer for that port.
- If a forwarding entry matches the IPv6 group address and the port that received the MLD report is in the forwarding entry for the group, the switch resets an aging timer for that port.

A switch does not forward an MLD report through a non-router port. The reason is that if the switch forwards a report through a member port, all the attached hosts that monitor the reported IPv6 multicast group address, according to the MLD report suppression mechanism, suppress their own reports after receiving this report. This makes the switch unable to know whether the reported IPv6 multicast group still has active members attached to that port.

When receiving a done message

When a host leaves an IPv6 multicast group, the host sends an MLD done message to the multicast router. When the switch receives an MLD done message on a member port, it first checks whether a forwarding entry matches the IPv6 group address in the message, and, if a match is found, whether the forwarding entry contains the dynamic member port.

- If no forwarding entry matches the IPv6 multicast group address, or if the forwarding entry does not contain the port, the switch directly discards the MLD done message.
- If a forwarding entry matches the IPv6 multicast group address and contains the port, the switch forwards the MLD done message to all router ports in the VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that IPv6 multicast group address, the switch does not immediately remove the port from the forwarding entry for that group. Instead, the switch resets the aging timer for that port.

After receiving the MLD done message, the MLD querier resolves the IPv6 multicast group address in the message and sends an MLD multicast-address-specific query to that IPv6 multicast group through the port that received the MLD done message. After receiving the MLD multicast-address-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that IPv6 multicast group. The switch also performs the following judgment on the port that received the MLD done message:

- If the port (assuming that it is a dynamic member port) receives any MLD report in response to the MLD multicast-address-specific query before its aging timer expires, it indicates that some host attached to the port is receiving or expecting to receive IPv6 multicast data for that IPv6 multicast group. The switch resets the aging timer for the port.
- If the port receives no MLD report in response to the MLD multicast-address-specific query before its aging timer expires, it indicates that no hosts attached to the port are still monitoring that IPv6 multicast group address.. The switch removes the port from the forwarding entry for the IPv6 multicast group when the aging timer expires.

Protocols and standards

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

Recommended configuration procedure

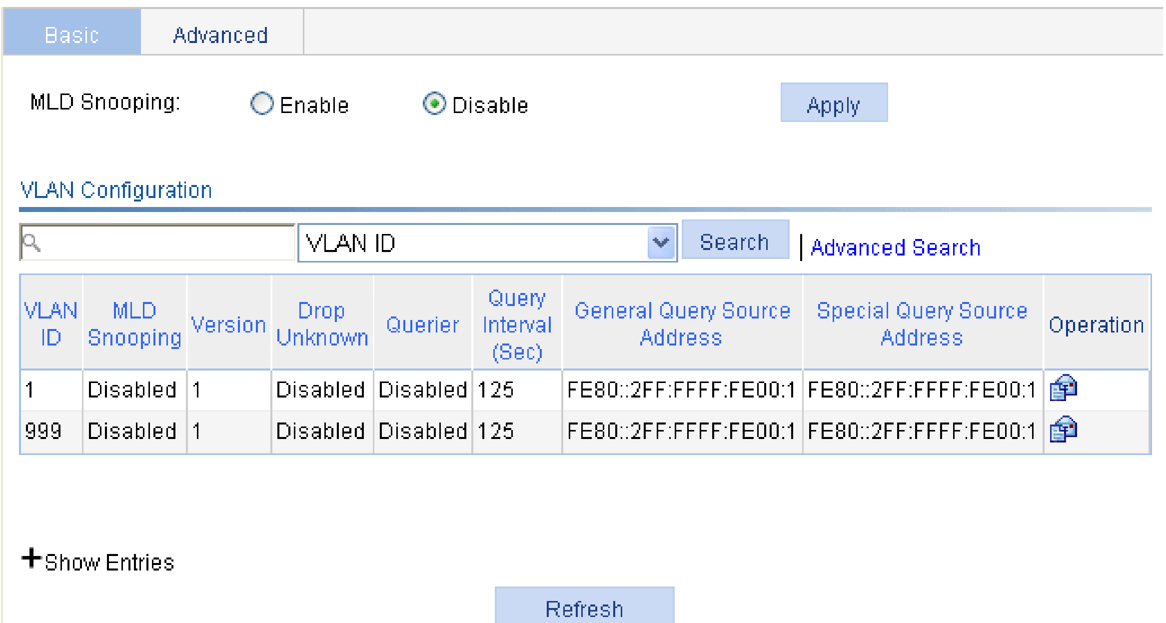
Step	Remarks
1. Enabling MLD snooping globally	(Required.) Disabled by default.

Step	Remarks
2. Configuring MLD snooping in a VLAN	(Required.) Enable MLD snooping for the VLAN and configure the MLD snooping version and querier. By default, MLD snooping is disabled in a VLAN. IMPORTANT: • MLD snooping must be enabled globally before you enable it for a VLAN. • When you enable MLD snooping for a VLAN, this function takes effect for the ports only in this VLAN.
3. Configuring MLD snooping on a port	(Optional.) Configure the maximum number of IPv6 multicast groups allowed and the fast-leave function for ports in the specified VLAN. IMPORTANT: • MLD snooping must be enabled globally before you enable it for a port. • MLD snooping configured on a port takes effect only after MLD snooping is enabled for the VLAN.
4. Displaying MLD snooping multicast table entries	(Optional.)

Enabling MLD snooping globally

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Enable** for MLD snooping.
3. Click **Apply**.

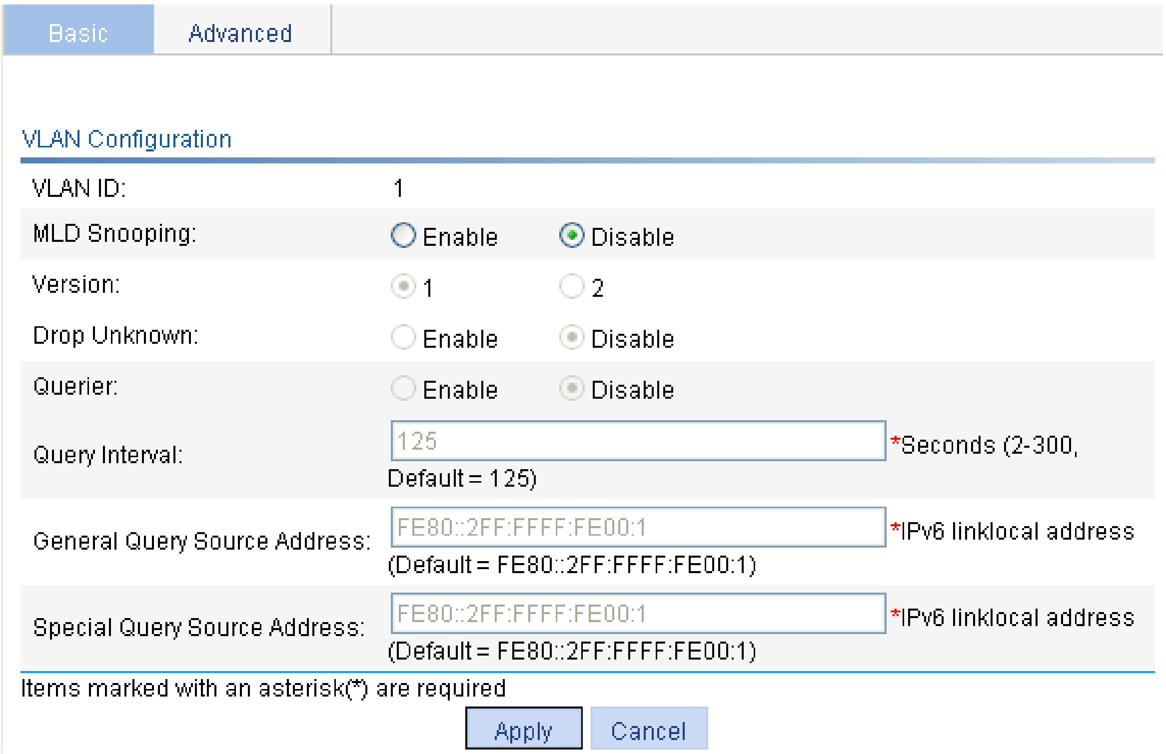
Figure 254 Basic MLD snooping configurations



Configuring MLD snooping in a VLAN

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click the icon corresponding to the VLAN.

Figure 255 VLAN configuration



3. Configure the parameters as described in Table 88.
4. Click **Apply**.

Table 88 Configuration items

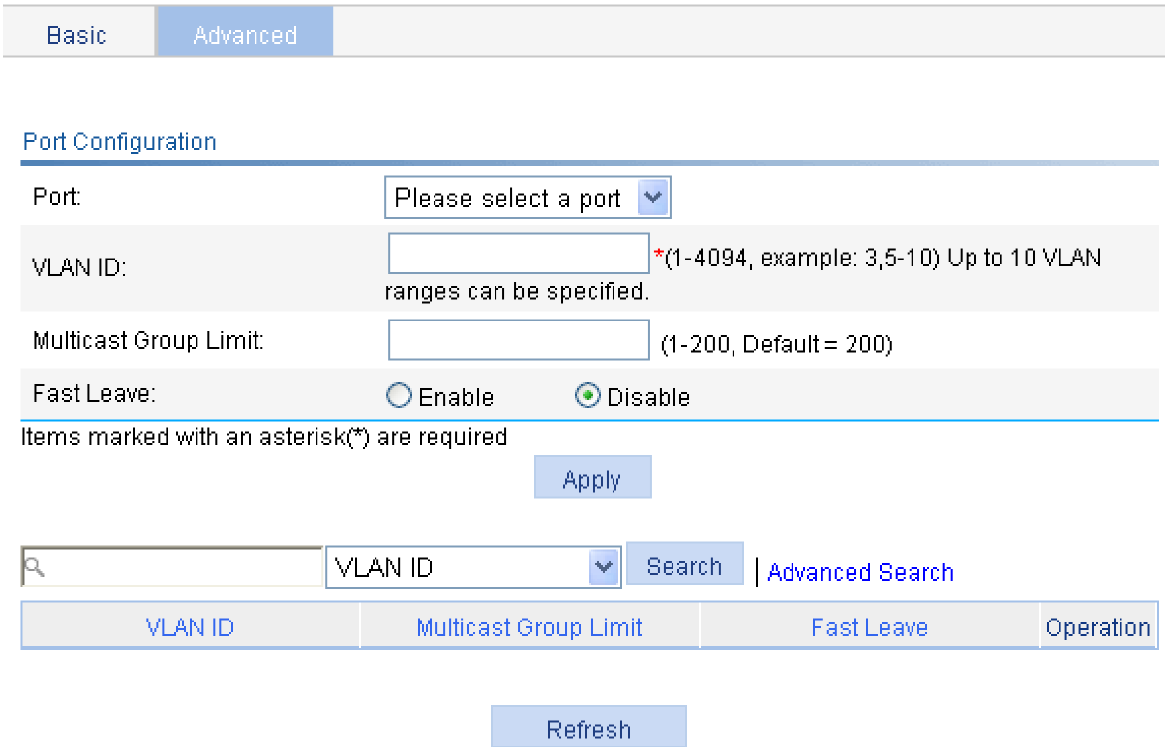
Item	Description
MLD snooping	Enable or disable MLD snooping in the VLAN. You can proceed with the subsequent configurations only if **Enable** is selected here.
Version	By configuring an MLD snooping version, you actually configure the versions of MLD messages that MLD snooping can process. • MLDv1 snooping can process MLDv1 messages, but floods MLDv2 messages in the VLAN instead of processing them. • MLDv2 snooping can process MLDv1 and MLDv2 messages. ⚠ IMPORTANT: If you change the MLDv2 snooping to MLDv1 snooping, the system clears all MLD snooping forwarding entries that are dynamically added.

Item	Description
Drop Unknown	Enable or disable the function of dropping unknown IPv6 multicast packets. Unknown IPv6 multicast data refers to IPv6 multicast data for which no entries exist in the MLD snooping forwarding table. • If the function of dropping unknown IPv6 multicast data is enabled, the switch forwards the unknown IPv6 multicast packets to the router ports instead of flooding them in the VLAN. If the switch does not have a router port, it drops the unknown IPv6 multicast packets. • If the function of dropping unknown IPv6 multicast data is disabled, the switch floods the unknown IPv6 multicast data in the VLAN to which the unknown IPv6 multicast data belong.
Querier	Enable or disable the MLD snooping querier function. In an IPv6 multicast network that runs MLD, a Layer 3 device is elected as the MLD querier to send MLD queries, so that all Layer 3 multicast devices can establish and maintain IPv6 multicast forwarding entries for correct IPv6 multicast traffic forwarding at the network layer. On an IPv6 network without Layer 3 multicast devices, no MLD querier-related function can be implemented because a Layer 2 device does not support MLD. To address this issue, you can enable MLD snooping querier on a Layer 2 device so that the device can generate and maintain IPv6 multicast forwarding entries at data link layer for correct IPv6 multicast traffic forwarding at data link layer.
Query interval	Configure the MLD general query interval.
General Query Source Address	Specify the source IPv6 address of MLD general queries
Special Query Source Address	Specify the source IPv6 address of MLD multicast-address-specific queries

Configuring MLD snooping on a port

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click the **Advanced** tab.

Figure 256 Advanced configuration



3. Configure the parameters as described in Table 89.
4. Click **Apply**.

Table 89 Configuration items

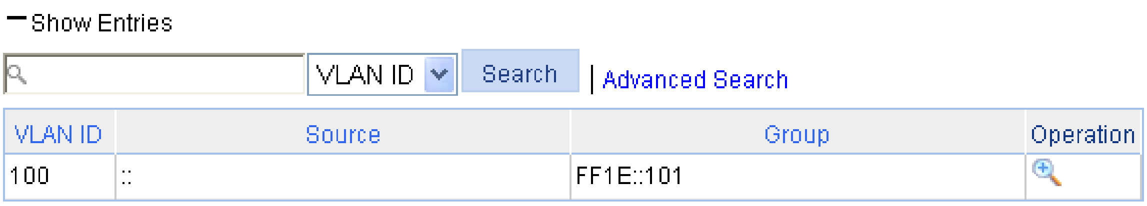
Item	Description
Port	Select the port on which advanced MLD snooping features will be configured. The port can be an Ethernet port or Layer-2 aggregate port. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. TIP: Advanced MLD snooping features 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 IPv6 multicast groups allowed on the port. Configurations made in a VLAN take effect for the ports in this VLAN only.
Multicast Group Limit	Configure the maximum number of IPv6 multicast groups that the port can join. With this feature, you can regulate IPv6 multicast traffic on the port. IMPORTANT: When the number of IPv6 multicast groups a port has joined reaches the configured threshold, the system deletes all the IPv6 forwarding entries persistent on that port from the MLD snooping forwarding table, and the hosts on this port need to join the IPv6 multicast groups again before the number of IPv6 multicast groups on this port reaches the threshold.

Item	Description
Fast Leave	Enable or disable the fast-leave function for the port. With the fast-leave function enabled on a port, when the switch receives an MLD done message on the port, it immediately deletes that port from the outgoing port list of the corresponding IPv6 forwarding table entry. Then, when the switch receives MLD multicast-address-specific queries for that multicast group, it does not forward them to that port. On a port that has only one host attached, you can enable fast-leave processing to save bandwidth and resources. However, on a port that has multiple hosts attached, do not enable fast-leave processing if you have enabled dropping unknown IPv6 multicast data for the VLAN which the port or the switch belongs to. Otherwise, if a host on the port leaves an IPv6 multicast group, the other hosts attached to the port in the same IPv6 multicast group cannot receive the IPv6 multicast data for the group.

Displaying MLD snooping multicast table entries

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Show Entries** to display information about MLD snooping multicast table entries.

Figure 257 Displaying entry information



3. To view detailed information about an entry, click the  icon corresponding to the entry.

Figure 258 Detailed information about an MLD snooping multicast entry

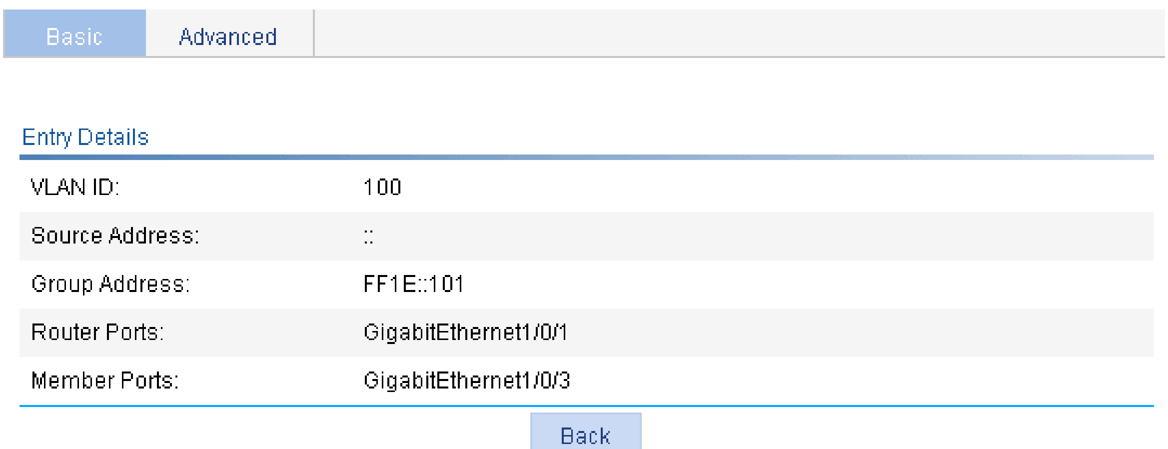


Table 90 Field description

Field	Description
VLAN ID	ID of the VLAN to which the entry belongs.
Source Address	Multicast source address, where :: indicates all multicast sources.

Field	Description
Group Address	Multicast group address.
Router Ports	All router ports.
Member Ports	All member ports.

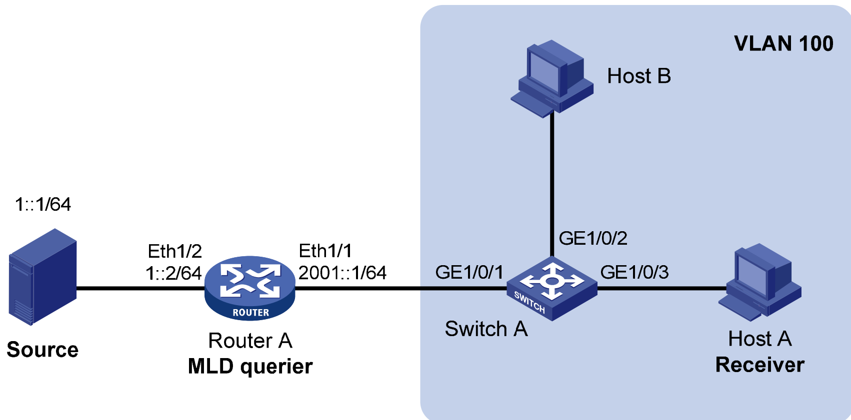
MLD snooping configuration example

Network requirements

As shown in Figure 259, MLDv1 runs on Router A and MLDv1 snooping runs on Switch A. Router A acts as the MLD querier.

Perform the configuration so that Host A can receive the IPv6 multicast packets destined for the IPv6 multicast group (FF1E::101), and Switch A drops the unknown IPv6 multicast packets rather than flooding them in the VLAN.

Figure 259 Network diagram



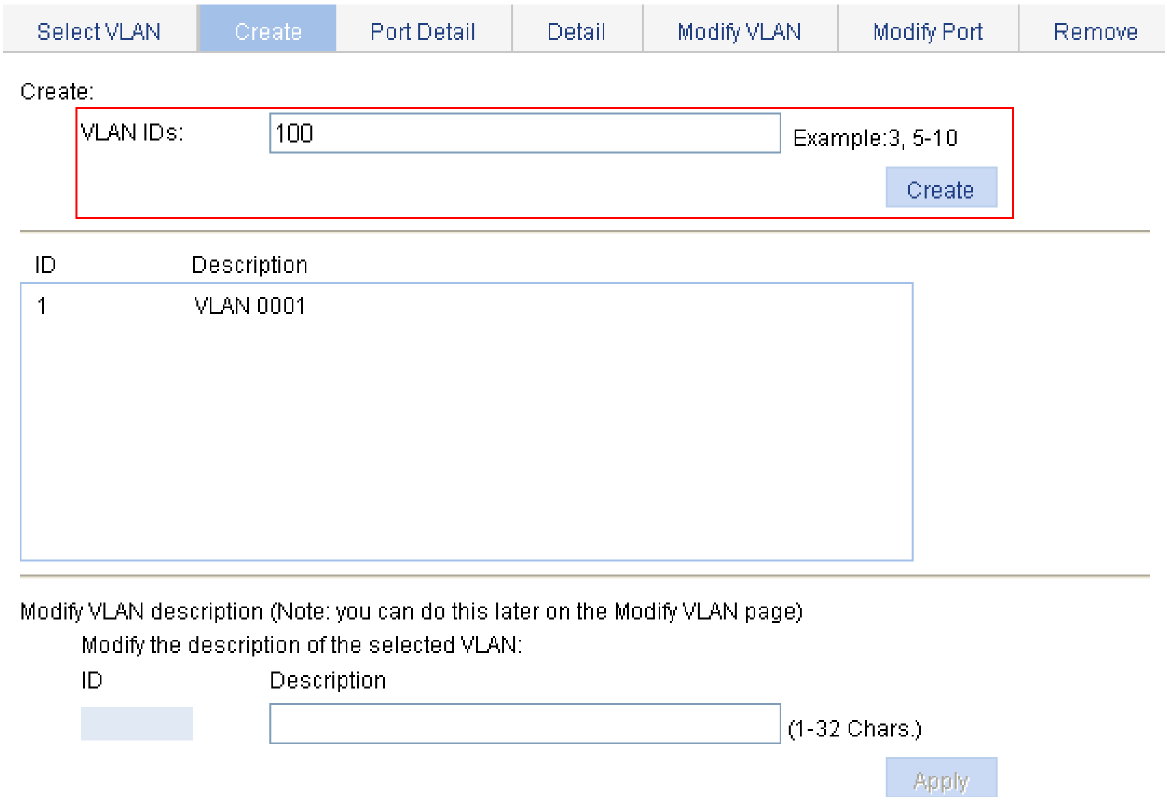
Configuring Router A

Enable IPv6 multicast routing, assign IPv6 address to each interface, enable IPv6 PIM-DM on each interface, and enable MLD on Ethernet 1/1. (Details not shown.)

Configuring Switch A

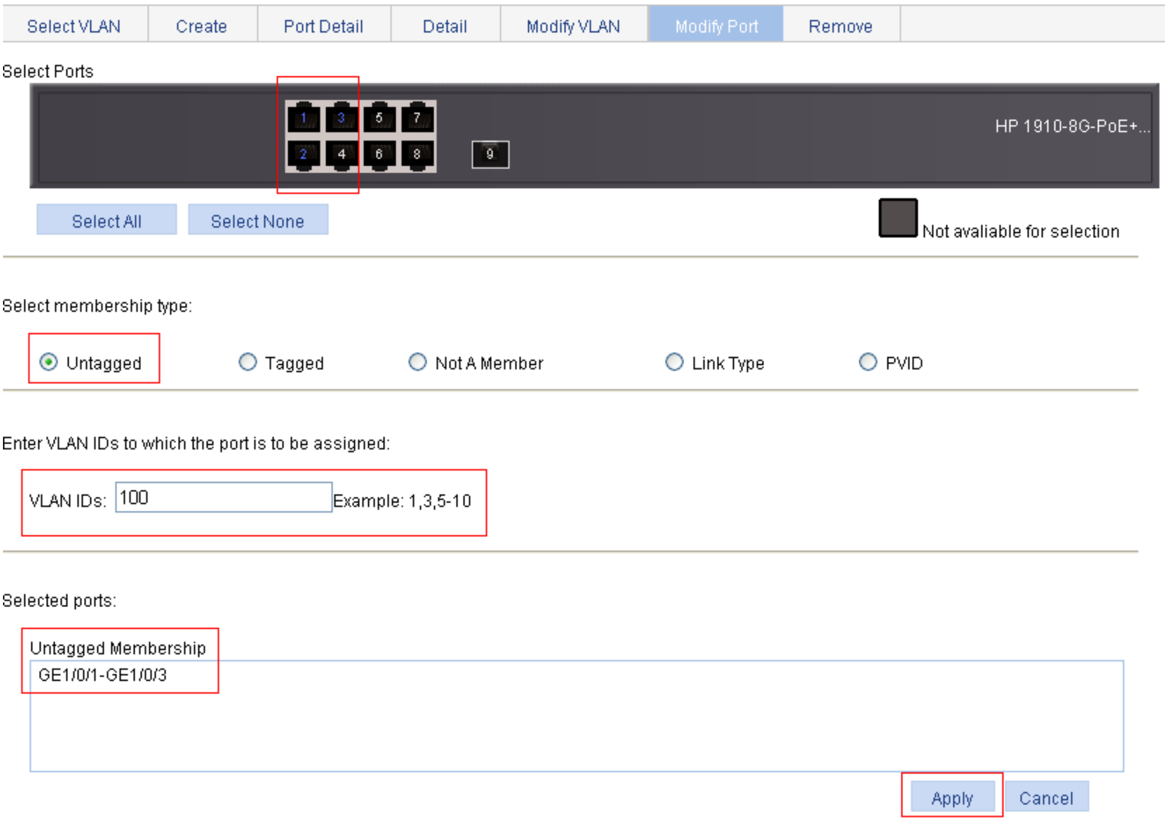
1. Create VLAN 100:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter 100 as the VLAN ID.
   d. Click **Apply**.

Figure 260 Creating VLAN 100



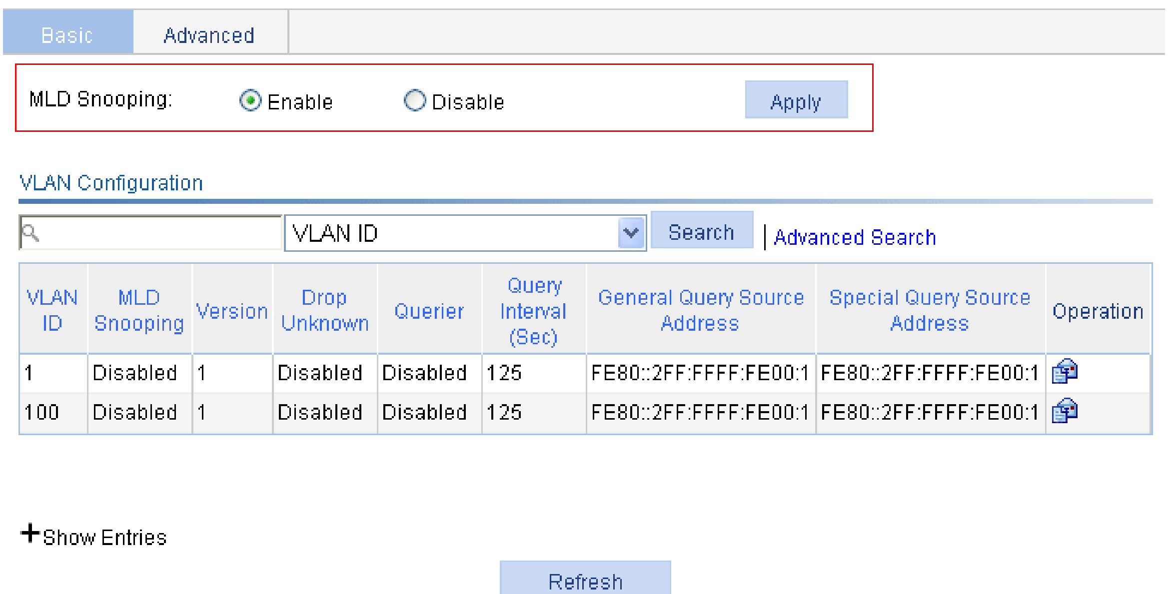
2. Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100:
   a. Click the **Modify Port** tab.
   b. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** field.
   c. Select the **Untagged** option for **Select membership type**.
   d. Enter 100 as the VLAN ID.
   e. Click **Apply**.

Figure 261 Assigning a port to the VLAN



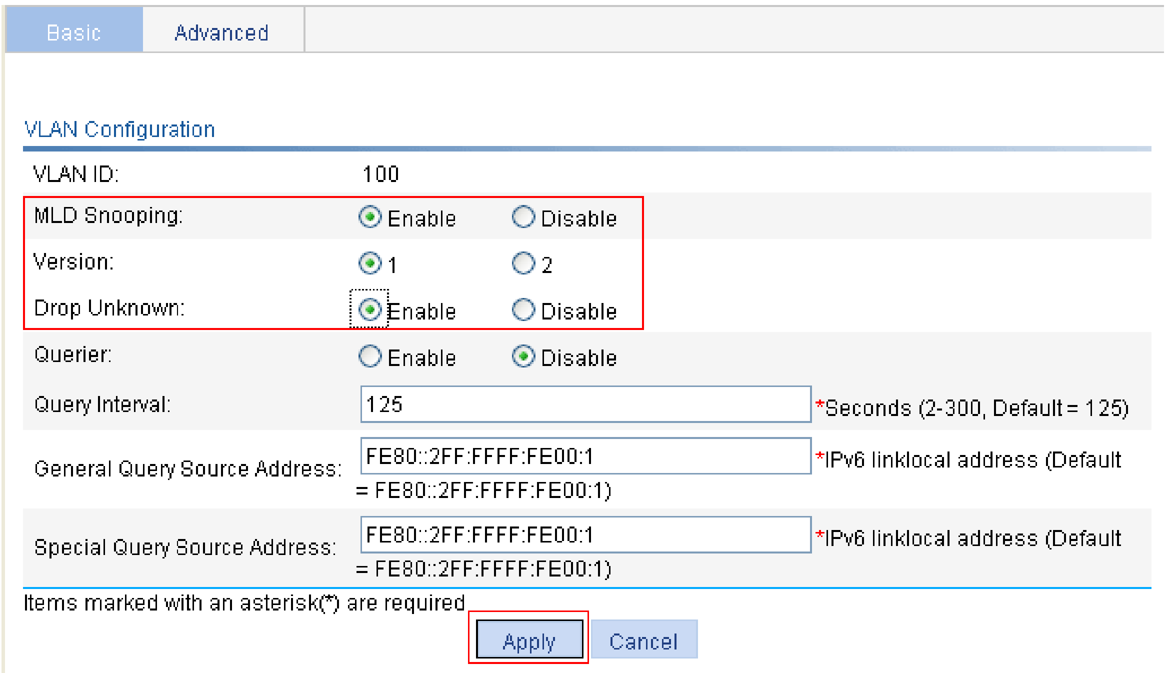
3. Enable MLD snooping globally:
   a. Select **Network** > **MLD snooping** from the navigation tree.
   b. Select the **Enable option.**
   c. Click **Apply**.

Figure 262 Enabling MLD snooping globally



4. Enable MLD snooping and the function of dropping unknown IPv6 multicast data for VLAN 100:
   a. Click the icon corresponding to VLAN 100.
   b. Select the **Enable** option for **MLD snooping**.
   c. Select the **1** option for **Version**.
   d. Select the **Enable** option for **Drop Unknown**.
   e. Click **Apply**.

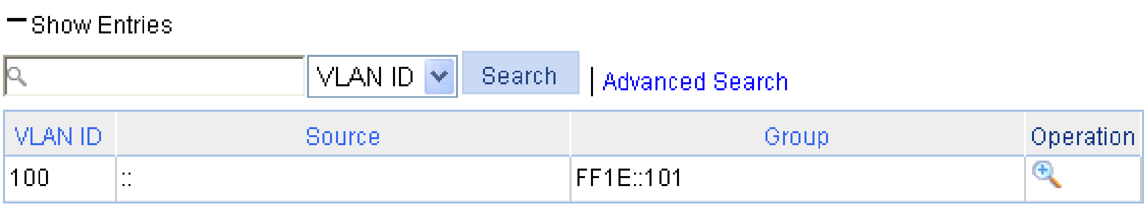
Figure 263 Enabling MLD snooping in the VLAN



Verifying the configuration

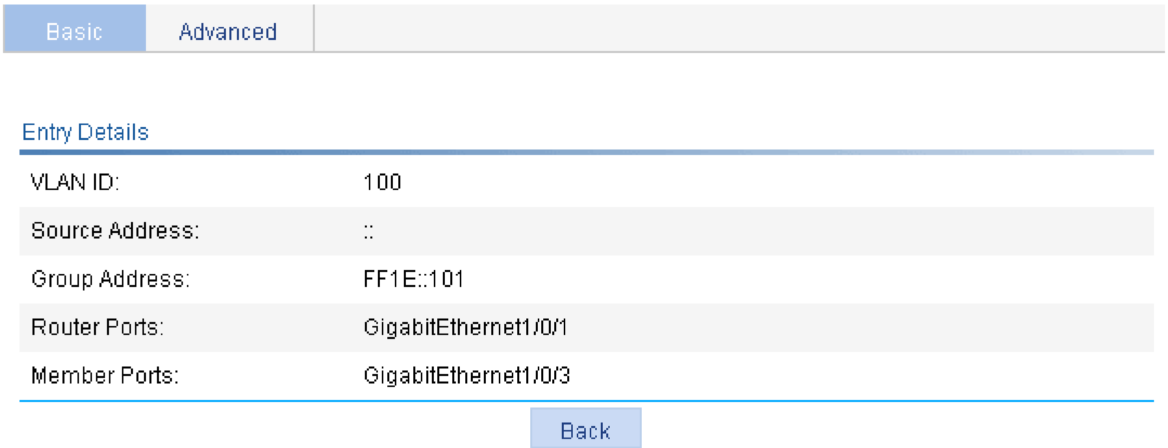
1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Show Entries** in the basic VLAN configuration page to display information about MLD snooping multicast entries.

Figure 264 MLD snooping multicast entry information page



3. Click the icon corresponding to the multicast entry (::, FF1E::101) to view information about this entry.

Figure 265 MLD snooping multicast entry information



The output shows that GigabitEthernet 1/0/3 of Switch A is listening to multicast streams destined for IPv6 multicast group (FF1E::101).

Configuring IPv4 and IPv6 routing

NOTE:

The term *router* in this document refers to both routers and Layer 3 switches.

Overview

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 provides the path information that guides the forwarding of packets.

Routing table

A router selects optimal routes from the routing table, and sends them to the forwarding information base (FIB) table to guide packet forwarding. Each router maintains a routing table and a FIB table.

Routes discovered by different routing protocols are available in a routing table and they can be divided into the following categories by origin:

- **Direct routes**—Routes discovered by data link protocols, also known as "interface routes."
- **Static routes**—Manually configured routes. Static routes are easy to configure and require fewer system resources. They work well in small and stable networks, but cannot adjust to network changes, so you must manually configure the routes again whenever the network topology changes.
- **Dynamic routes**—Routes that are discovered dynamically by routing protocols.

Each entry in the FIB table specifies a physical interface that packets destined for a certain address should go out to reach the next hop—the next router—or the directly connected destination.

A route entry has the following items:

- **Destination IP address**—Destination IP address or destination network.
- **Mask (IPv4)/prefix length (IPv6)**—Specifies, together with the destination address, the address of the destination network. A logical AND operation between the destination address and the network mask/prefix length yields the address of the destination network.
- **Preference**—Routes to the same destination may be discovered by various routing protocols or manually configured, and routing protocols and static routes have different preferences configured. The route with the highest preference (the smallest value) is optimal.
- **Outbound interface**—Specifies the interface through which a matching IP packet is to be forwarded.
- **Next hop**—Specifies the address of the next hop router on the path.

Static route

Static routes are manually configured. If a network's topology is simple, you only need to configure static routes for the network to work properly.

Static routes cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the network administrator must modify the static routes manually.

Default route

A default route is used to forward packets that match no entry in the routing table.

Without a default route, a packet that does not match any routing entries is discarded and an Internet Control Message Protocol (ICMP) destination-unreachable packet is sent to the source.

You can configure default routes in the web interface in the following ways:

- Configure an IPv4 static default route and specify both its destination IP address and mask as 0.0.0.0.
- Configure an IPv6 static default route and specify both its destination IP address and prefix as ::/0.

Displaying the IPv4 active route table

Select **Network** > **IPv4 Routing** from the navigation tree to enter the page.

Figure 266 IPv4 active route table

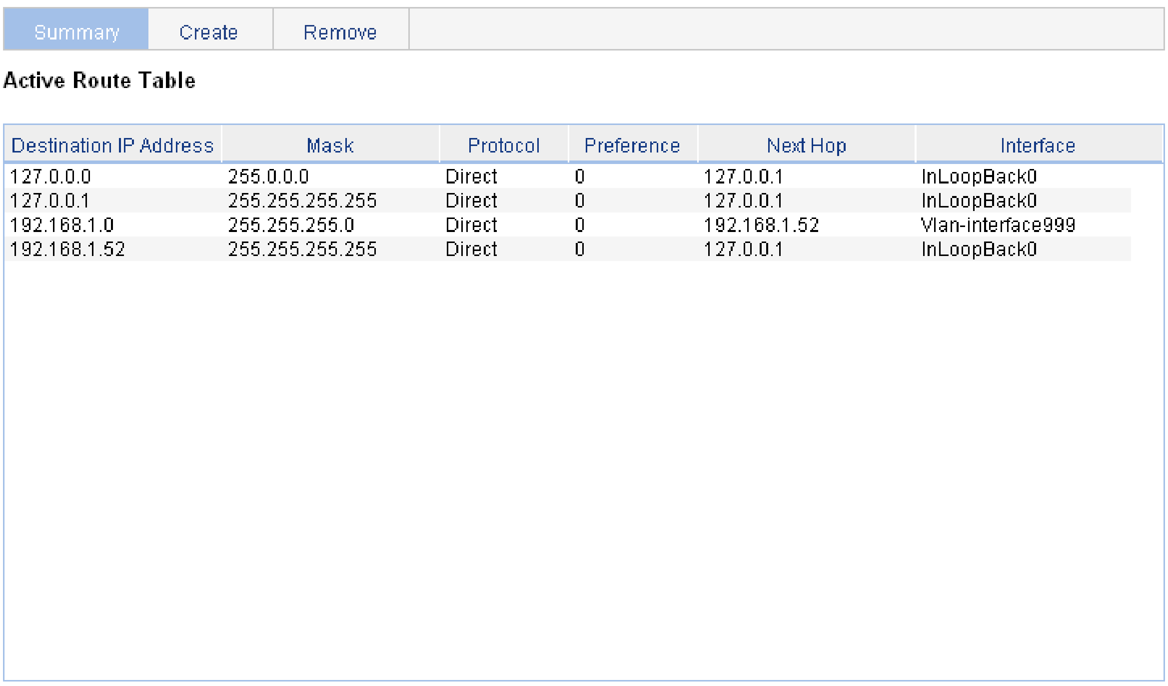


Table 91 Field **description**

Field	Description
Destination IP Address	Destination IP address.
Mask	Subnet mask of the IPv4 route.
Protocol	Protocol that discovered the IPv4 route.
Preference	Preference value for the IPv4 route. The smaller the number, the higher the preference.

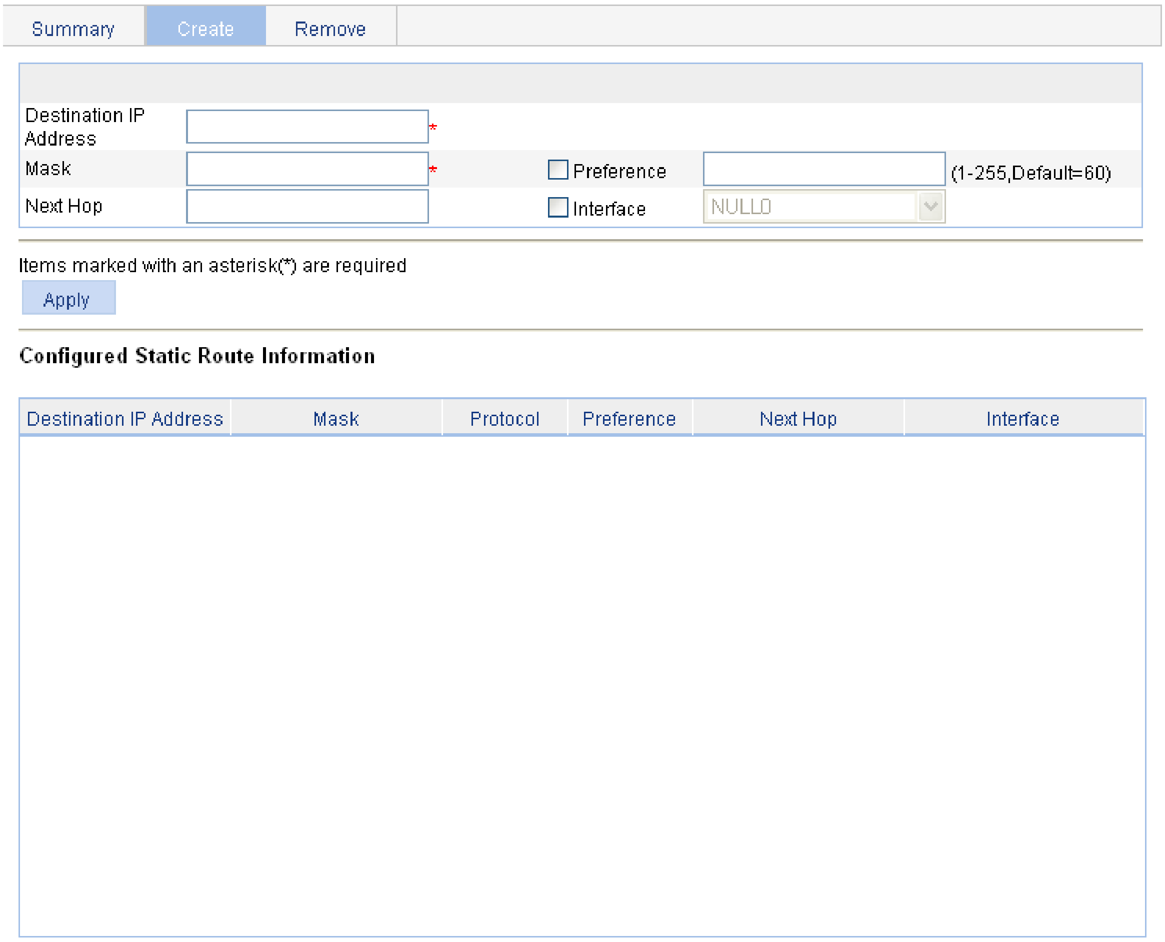
Field	Description
Next Hop	Next hop IP address of the IPv4 route.
Interface	Outgoing interface of the IPv4 route. Packets destined for the specified network segment will be sent out of the interface.

Creating an IPv4 static route

1. Select **Network** > **IPv4 Routing** from the navigation tree.
2. Click the **Create** tab.

   The page for configuring IPv4 static route appears.

Figure 267 Creating an IPv4 static route



3. Create an IPv4 static route as described in Table 92.
4. Click **Apply**.

Table 92 Configuration items

Item	Description
Destination IP Address	Enter the destination host or network IP address, in dotted decimal notation.

Item	Description
Mask	Enter the mask of the destination IP address. You can enter a mask length or a mask in dotted decimal notation.
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	Enter the next hop IP address, in dotted decimal notation.
Interface	Select the outgoing interface. You can select any available Layer 3 interface, for example, a virtual interface, of the device. If you select NULL 0, the destination IP address is unreachable.

Displaying the IPv6 active route table

Select **Network** > **IPv6 Routing** from the navigation tree to enter the page.

Figure 268 IPv6 active route table

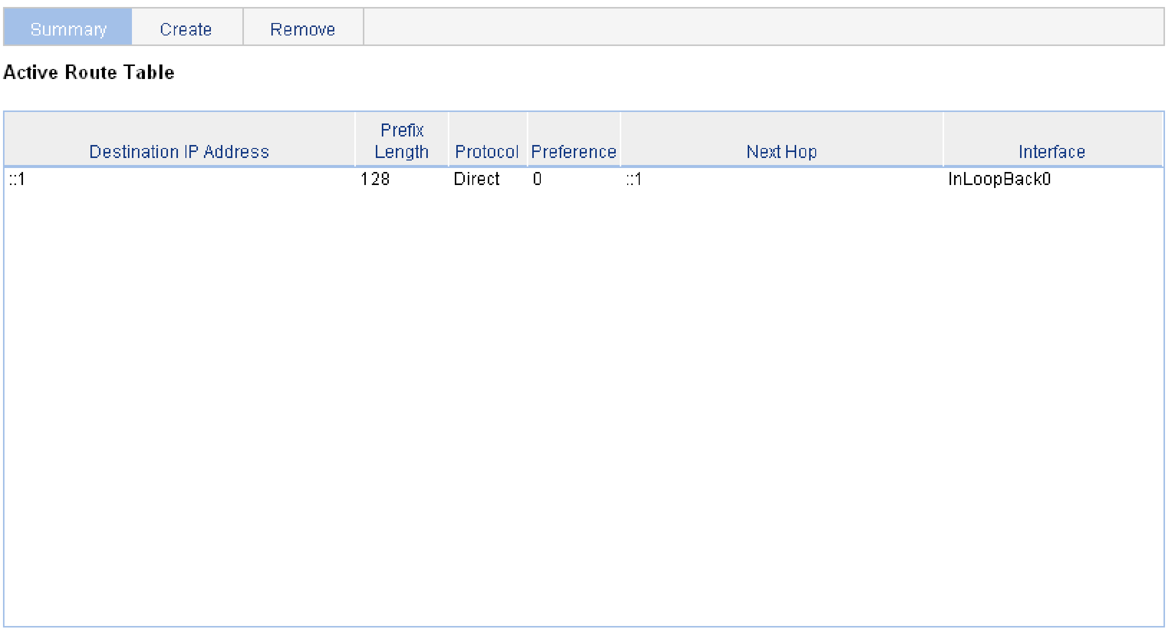


Table 93 Field description

Field	Description
Destination IP Address	Destination IP address and prefix length of the IPv6 route
Prefix Length	
Protocol	Protocol that discovered the IPv6 route
Preference	Preference value for the IPv6 route The smaller the number, the higher the preference.

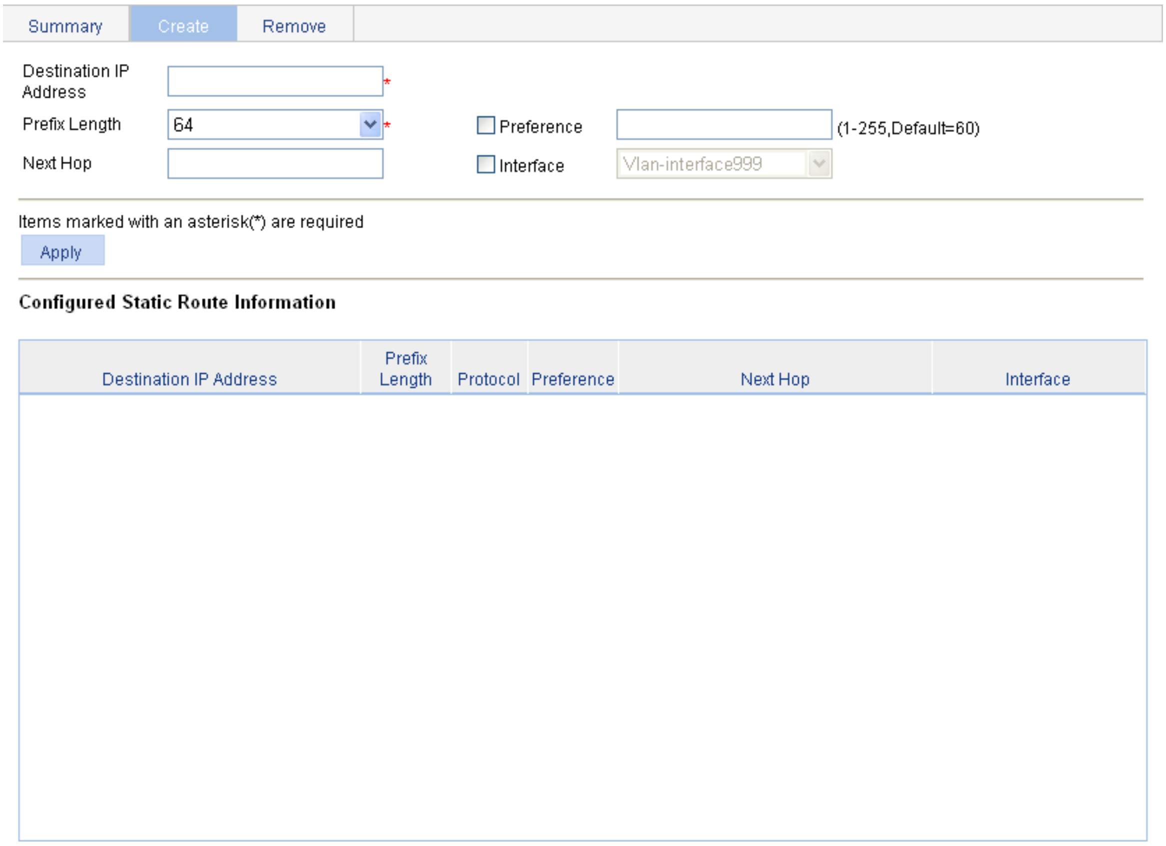
Field	Description
Next Hop	Next hop IP address of the IPv6 route
Interface	Outgoing interface of the IPv6 route. Packets destined for the specified network segment will be sent out of the interface.

Creating an IPv6 static route

1. Select **Network** > **IPv6 Routing** from the navigation tree.
2. Click the **Create** tab.

   The page for configuring IPv6 static route appears.

Figure 269 Creating an IPv6 static route



3. Create an IPv6 static route as described in Table 94.
4. Click **Apply**.

Table 94 Configuration items

Item	Description
Destination IP Address	Enter the destination host or network IP address, in the X:X::X:X format. The 128-bit destination IPv6 address is a hexadecimal address with eight parts separated by colons (:). Each part is represented by a 4-digit hexadecimal integer.
Prefix Length	Enter or select the prefix length of the destination IPv6 address.

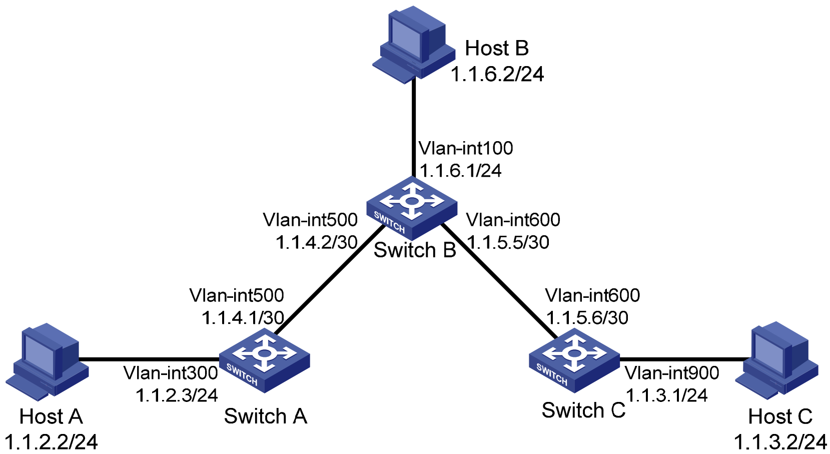
Item	Description
Preference	Set a preference value for the static route. The smaller the number, the higher the preference. For example, specifying the same preference for multiple static routes to the same destination enables load sharing on the routes, while specifying different priorities for them enables route backup.
Next Hop	Enter the next hop address, in the same format as the destination IP address.
Interface	Select the outgoing interface. You can select any available Layer 3 interface, for example, a virtual interface, of the device. If you select NULL 0, the destination IPv6 address is unreachable.

IPv4 Static route configuration example

Network requirements

The IP addresses of devices are shown in Figure 270. Configure IPv4 static routes on Switch A, Switch B and Switch C for any two hosts to communicate with each other.

Figure 270 Network diagram



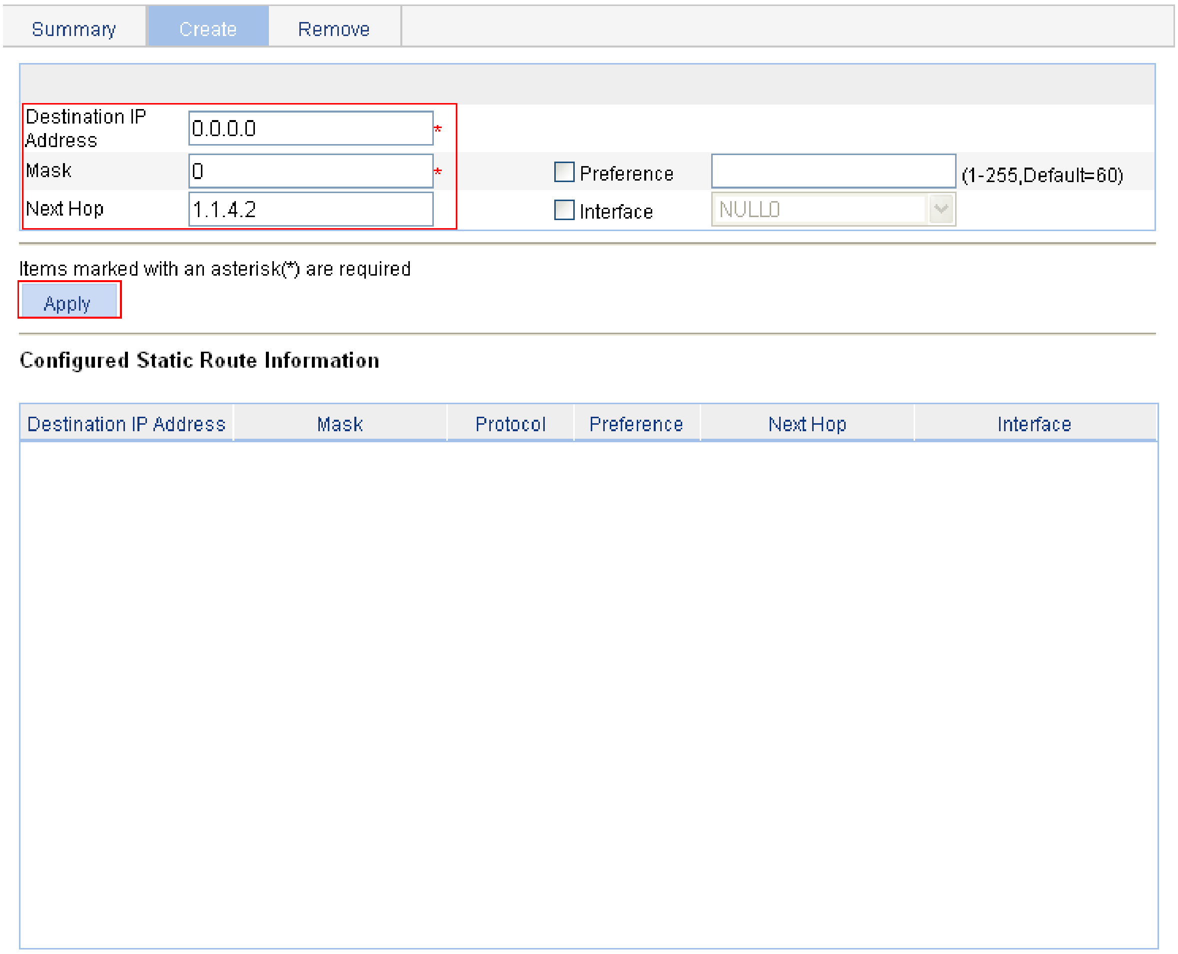
Configuration considerations

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

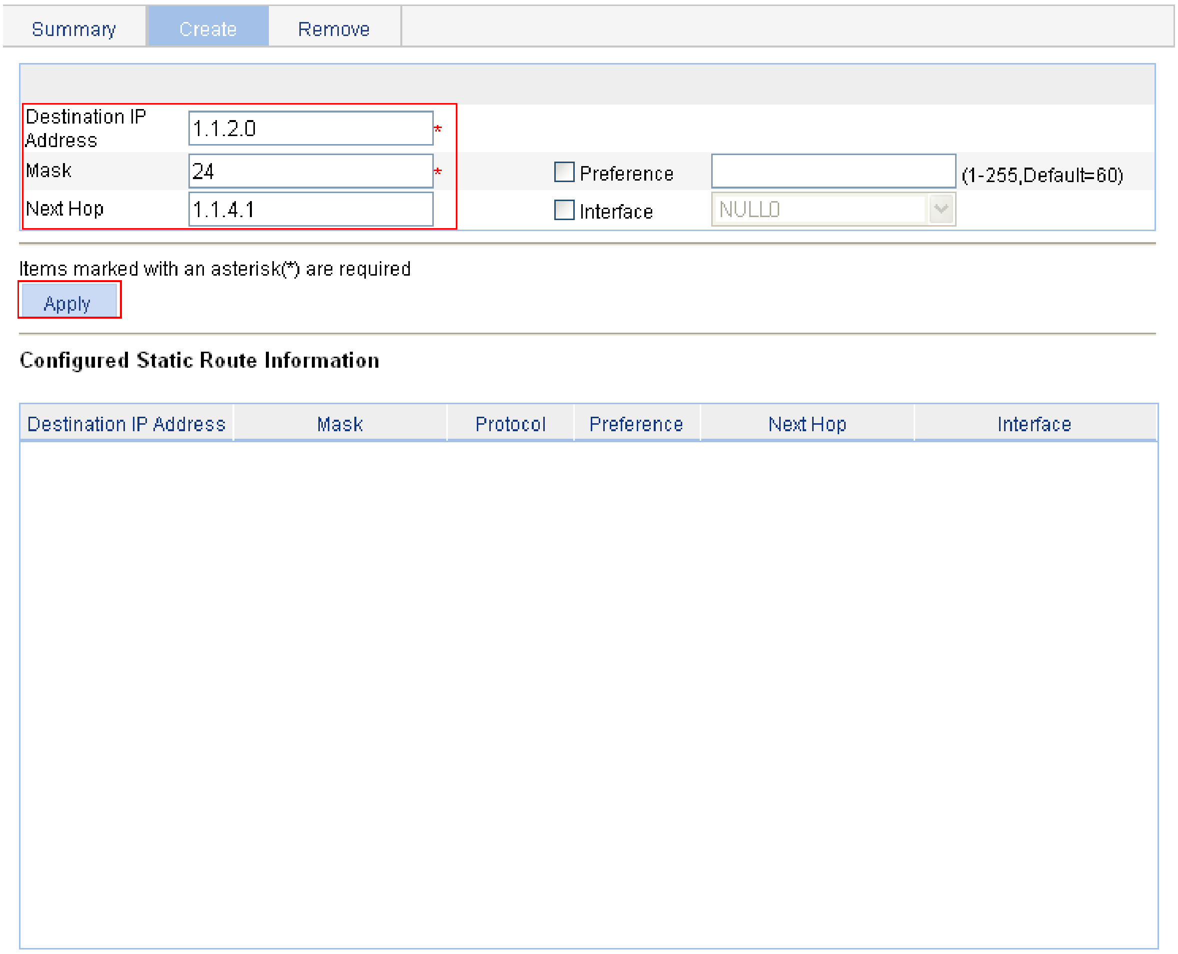
1. Configure a default route to Switch B on Switch A:
   a. Select **Network** > **IPv4 Routing** from the navigation tree of Switch A.
   b. Click the **Create** tab.
   c. Enter **0.0.0.0** for **Destination IP Address**, **0** for **Mask**, and **1.1.4.2** for **Next Hop**.
   d. Click **Apply**.

Figure 271 Configuring a default route



2. Configure a static route to Switch A and Switch C on Switch B:
    a. Select **Network** > **IPv4 Routing** from the navigation tree of Switch B.
    b. Click the **Create** tab.
       The page for configuring a static route appears.
    c. Enter **1.1.2.0** for **Destination IP Address**, **24** for **Mask**, and **1.1.4.1** for **Next Hop**.
    d. Click **Apply**.

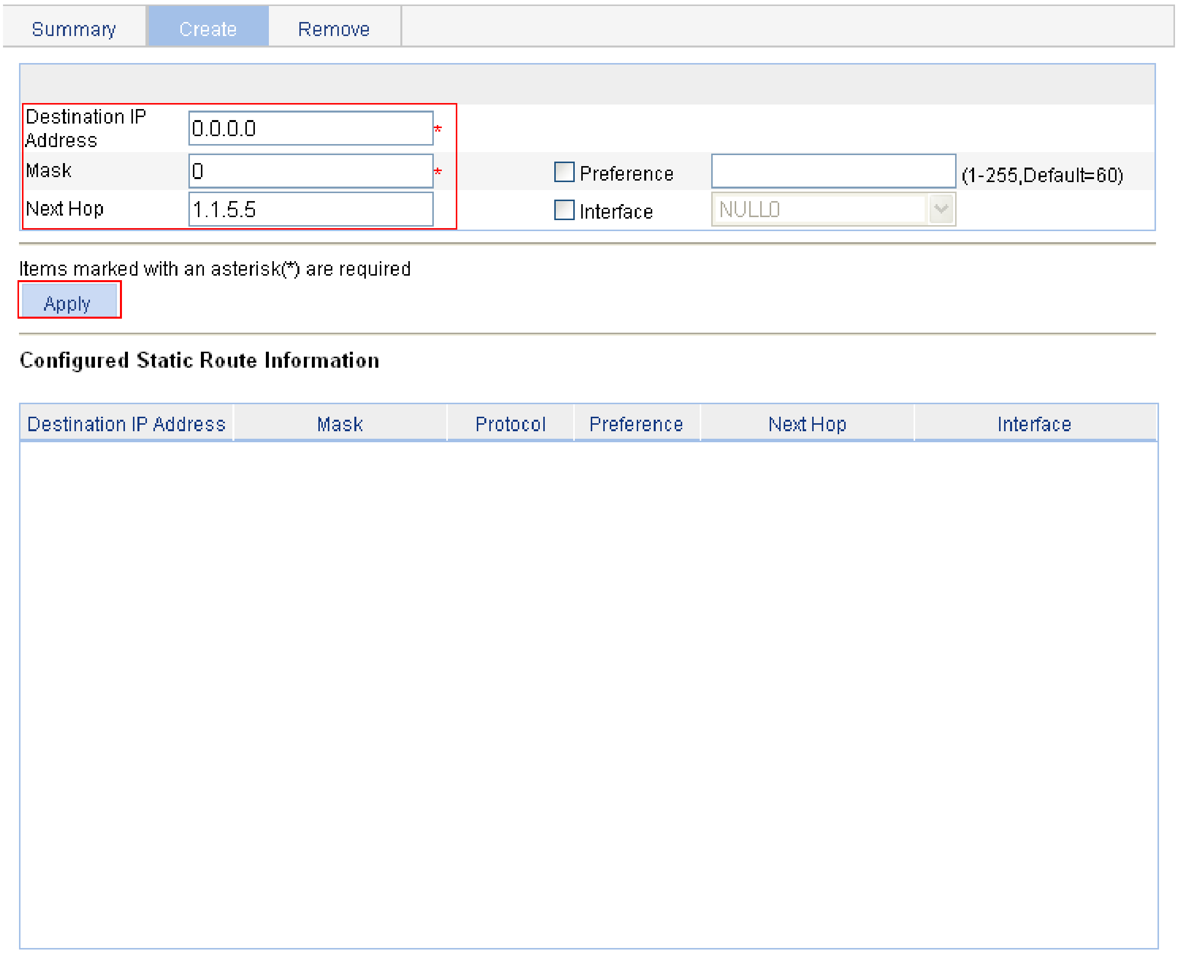
Figure 272 Configuring a static route



e. Enter **1.1.3.0** for **Destination IP Address**, enter **24** for **Mask**, and enter **1.1.5.6** for **Next Hop**.
f. Click **Apply**.

3. Configure a default route to Switch B on Switch C:
   a. Select **Network** > **IPv4 Routing** from the navigation tree of Switch C.
   b. Click the **Create** tab.
   c. Enter **0.0.0.0** for **Destination IP Address**, **0** for **Mask**, and **1.1.5.5** for **Next Hop**.
   d. Click **Apply**.

Figure 273 Configuring a default route



Verifying the configuration

1. Display the routing table:

   Enter the IPv4 route page of Switch A, Switch B, and Switch C to verify that the newly configured static routes are displayed as active routes on the page.

2. Ping Host C from Host A (assuming both hosts run Windows XP):

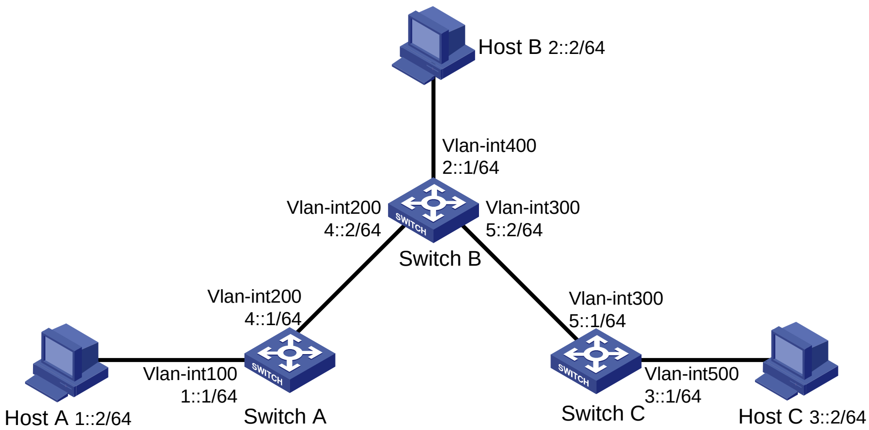
```
C:\Documents and Settings\Administrator>ping 1.1.3.2

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
```

IPv6 static route configuration example

Network requirements

The IP addresses of devices are shown in Figure 274. Configure IPv6 static routes on Switch A, Switch B and Switch C for any two hosts to communicate with each other.

Figure 274 Network diagram



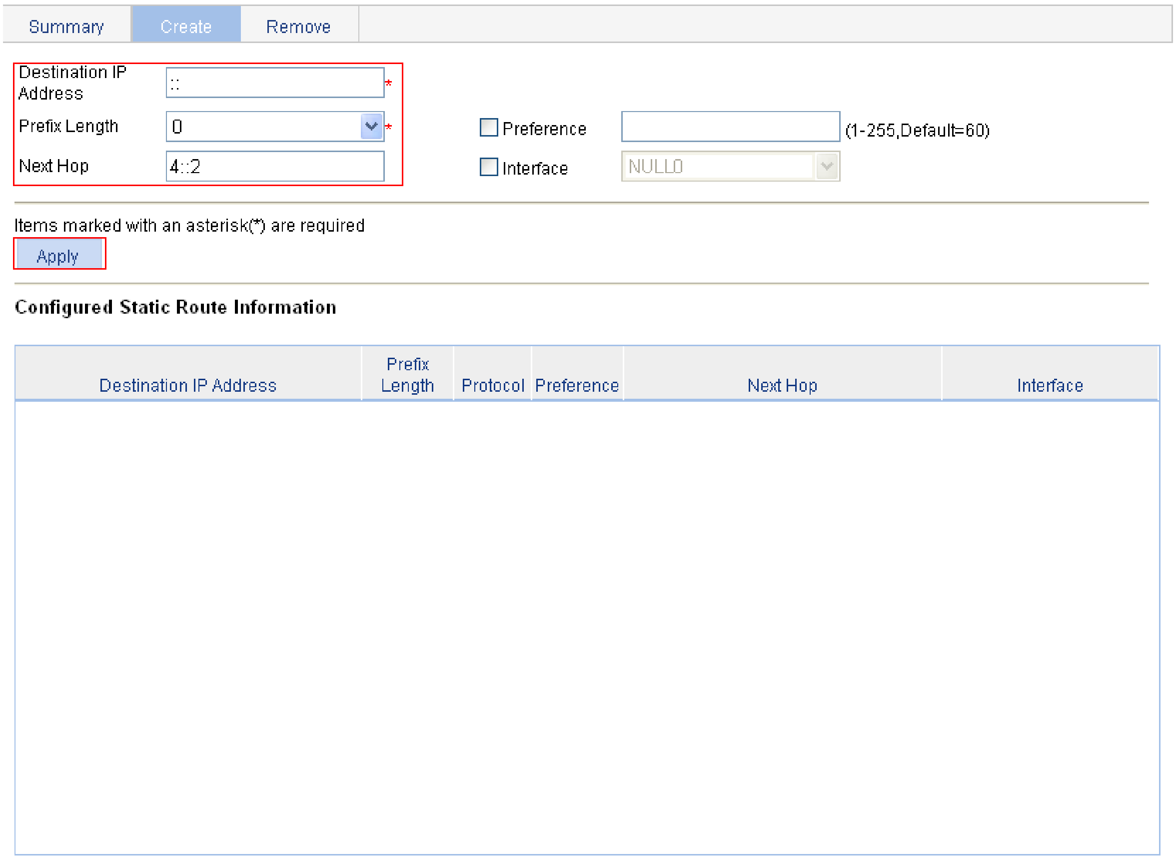
Configuration considerations

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

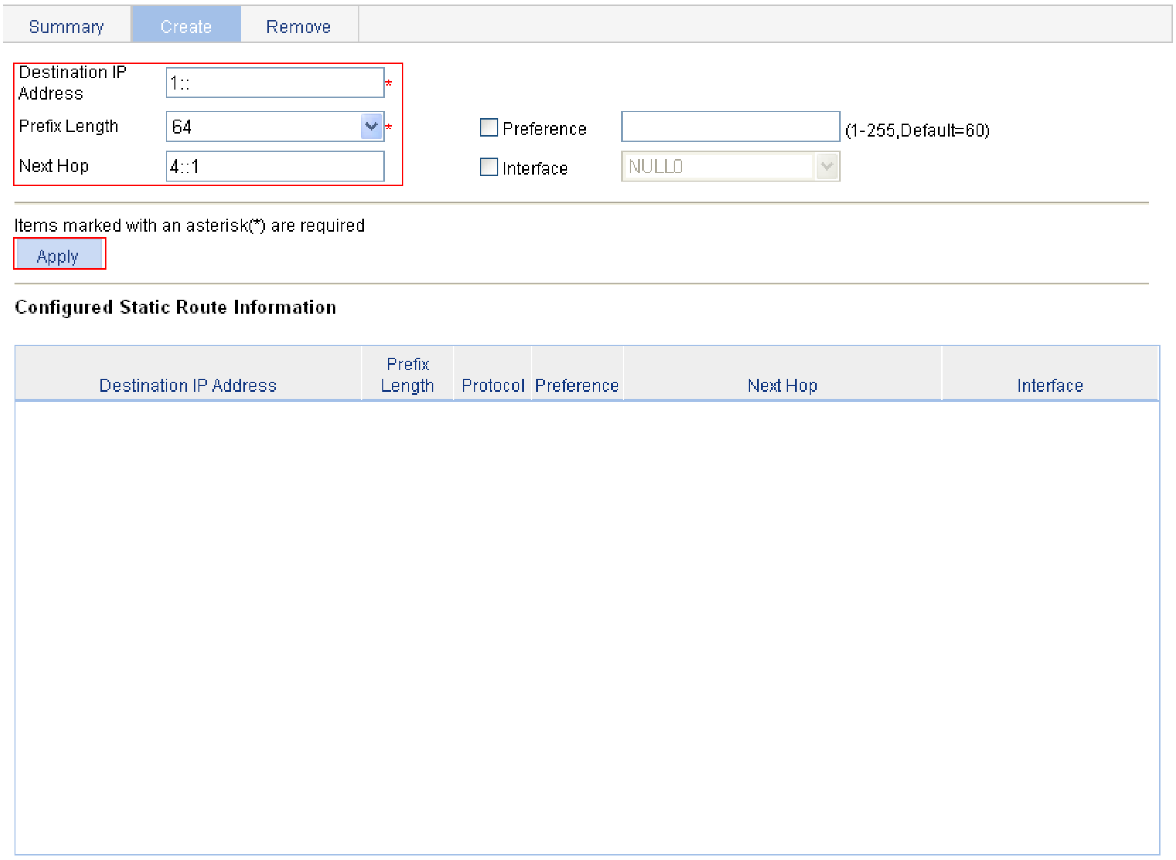
1. Configure a default route to Switch B on Switch A:
   a. Select **Network** > **IPv6 Routing** from the navigation tree of Switch A.
   b. Click the **Create** tab.
   c. Enter **::** for **Destination IP Address**, select **0** from the **Prefix Length** list, and enter **4::2** for **Next Hop**.
   d. Click **Apply**.

Figure 275 Configuring a default route



2. Configure a static route to Switch A and Switch C on Switch B:
   a. Select **Network** > **IPv6 Routing** from the navigation tree of Switch B.
   b. Click the **Create** tab.
      The page for configuring a static route appears.
   c. Enter **1::** for **Destination IP Address**, select **64** from the **Prefix Length** list, and enter **4::1** for **Next Hop**.
   d. Click **Apply**.

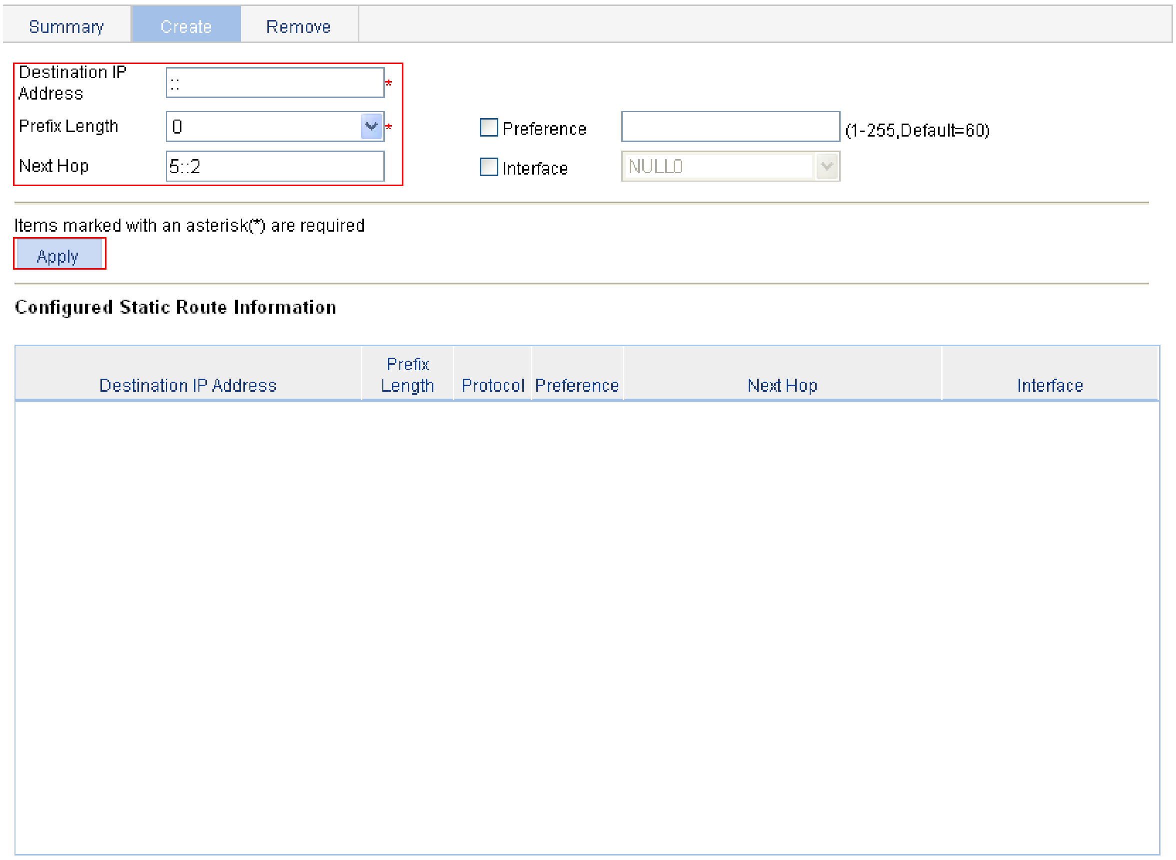
Figure 276 Configuring a static route



e. Enter **3::** for **Destination IP Address**, select **64** from the **Prefix Length** list, and enter **5::1** for **Next Hop**.
f. Click **Apply**.

3. Configure a default route to Switch B on Switch C:
   a. Select **Network** > **IPv6 Routing** from the navigation tree of Switch C.
   b. Click the **Create** tab.
   c. Enter **::** for **Destination IP Address**, select **0** from the **Prefix Length** list, and enter **5::2** for **Next Hop**.
   d. Click **Apply**.

Figure 277 Configuring a default route



Verifying the configuration

1. Display the routing table:

   Enter the IPv6 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.

2. Ping Host C from Switch A:

```
<SwitchA> system-view
[SwitchA] ping ipv6 3::2
  PING 3::2 : 56  data bytes, press CTRL_C to break
    Reply from 3::2
    bytes=56 Sequence=1 hop limit=254  time = 63 ms
    Reply from 3::2
    bytes=56 Sequence=2 hop limit=254  time = 62 ms
    Reply from 3::2
    bytes=56 Sequence=3 hop limit=254  time = 62 ms
    Reply from 3::2
    bytes=56 Sequence=4 hop limit=254  time = 63 ms
    Reply from 3::2
    bytes=56 Sequence=5 hop limit=254  time = 63 ms

  --- 3::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 62/62/63 ms
```

Configuration guidelines

When you configure a static route, follow these guidelines:

- If you do not specify the preference, 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.
- 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, the static route does not take effect.
- When you specify the outgoing interface, note the following:
  - If NULL 0 is specified as the outgoing 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 outgoing interface, which may have multiple next hops, you must specify the next hop at the same time.
- You can delete only IPv4/IPv6 static routes on the **Remove** tab.

DHCP overview

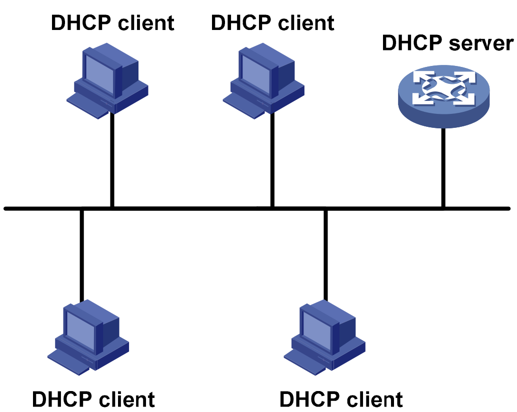
NOTE:

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 more information about the DHCP client configuration, see "Configuring VLAN interfaces" and "Managing ports."

Introduction to DHCP

The Dynamic Host Configuration Protocol (DHCP) provides a framework to assign configuration parameters to network devices.

Figure 278 A typical DHCP application



A DHCP client can obtain an IP address and other configuration parameters from a DHCP server on another subnet via a DHCP relay agent. For more information about the DHCP relay agent, see "Configuring DHCP relay agent"

DHCP address allocation

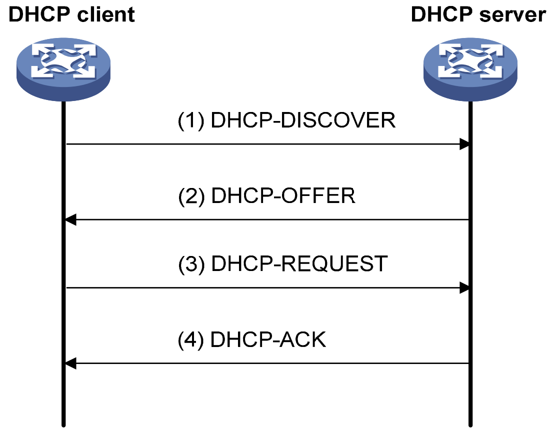
Allocation mechanisms

DHCP supports the following mechanisms for IP address allocation:

- **Static 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 279 Dynamic IP address allocation process



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. For more information about the DHCP message format, see "DHCP message format."
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 broadcasts a gratuitous ARP packet to verify whether the IP address assigned by the server is in use. If the client receives no response within the specified time, the client uses 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. To continue using the IP address, the client must extend the lease duration.

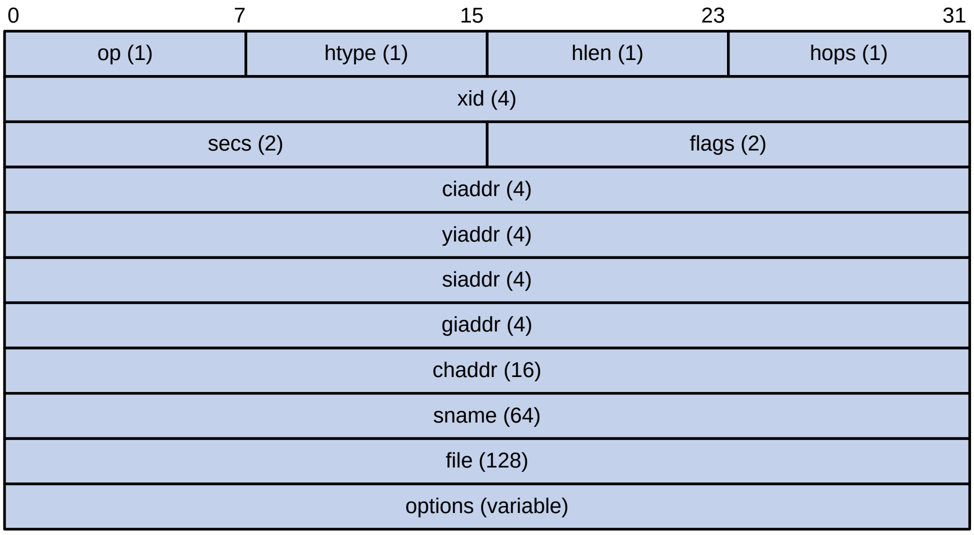
After half the lease duration, the DHCP client sends a DHCP-REQUEST unicast to the DHCP server to extend the lease. Depending on availability of the IP address, the DHCP server returns a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

If the client receives no reply, it will broadcast another DHCP-REQUEST message for lease extension after 7/8 lease duration elapses.

DHCP message format

Figure 280 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 280 DHCP message format



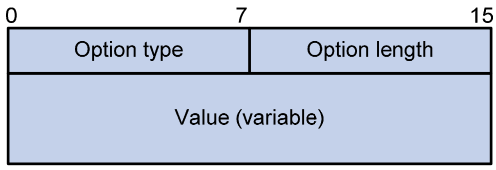
- **op**—Message type defined in option field. 1 = REQUEST, 2 = REPLY
- **htype**, **hlen**—Hardware address type and length of a DHCP client.
- **hops**—Number of relay agents a request message traveled.
- **xid**—Transaction ID, a random number chosen by the client to identify an IP address allocation.
- **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

DHCP uses the same message format as BOOTP, but DHCP uses the Option field to carry information for dynamic address allocation and to provide additional configuration information to clients.

Figure 281 DHCP option format



Introduction to DHCP options

Common DHCP options:

- **Option 3**—Router option. It specifies the gateway IP address to be assigned to the client.
- **Option 6**—DNS server option. It specifies the DNS server IP address to be assigned to the client.
- **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 both Option 33 and Option 121 exist, Option 33 is ignored.
- **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 60**—Vendor class identifier option. A client uses this option to identify the vendor to which it belongs. With this option, the DHCP server can determine the vendor a client belongs to and assign an IP address within a specific range.
- **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 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. If both Option 33 and Option 121 exist, Option 33 is ignored.
- **Option 150**—TFTP server IP address option. It specifies the TFTP server IP address to be assigned to the client.

For more information about DHCP options, see RFC 2132 and RFC 3442.

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.

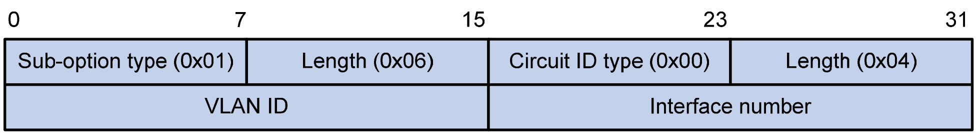
Option 82 involves at most 255 sub-options. At least one sub-option is defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

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:

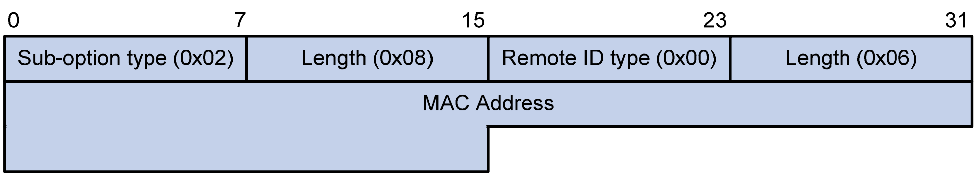
- **Sub-option 1**—Contains the VLAN ID and interface number of the interface that received the client's request. The following figure gives its format. The value of the sub-option type is 1, and that of the circuit ID type is 0.

Figure 282 Sub-option 1 in normal padding format



- **Sub-option 2**—Contains 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 283 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*
- RFC 3442, *The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4.*

Configuring DHCP relay agent

Introduction to DHCP relay agent

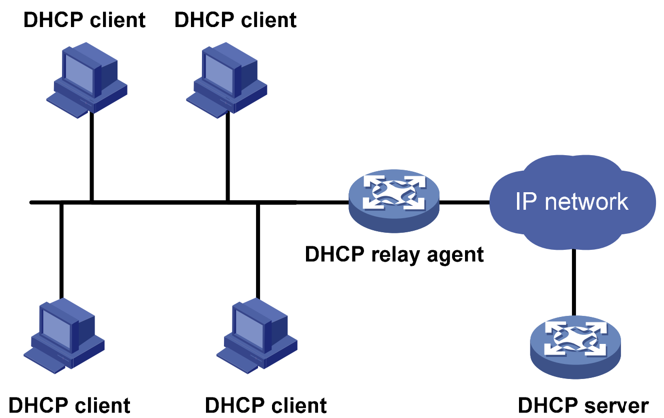
Application environment

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.

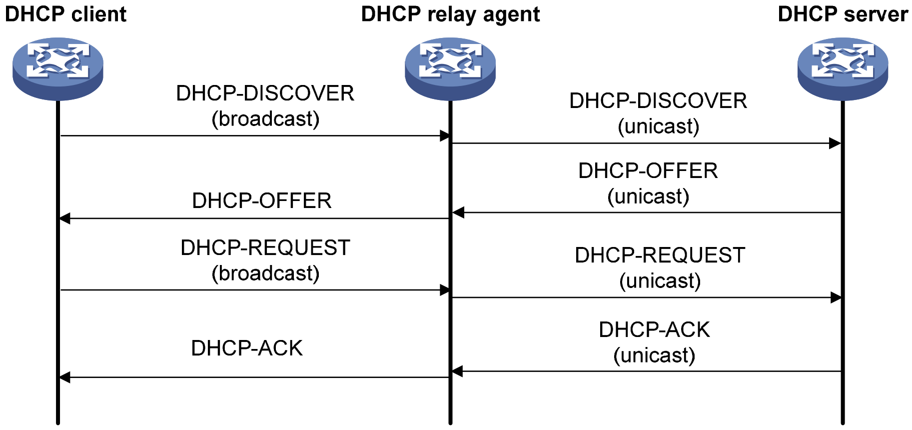
Fundamentals

Figure 284 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 "DHCP overview"). The following describes the forwarding process on the DHCP relay agent. For more information about DHCP packet exchange, see "Dynamic IP address allocation process."

Figure 285 DHCP relay agent work process



As shown in Figure 285, 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.

Recommended configuration procedure

Step	Remarks
1. 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.
2. 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.
3. 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 operate in the DHCP server mode by default. IMPORTANT: The DHCP relay agent works on interfaces with IP addresses manually configured only.

Step	Remarks
4. 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

1. Select **Network** > **DHCP** from the navigation tree to enter the **DHCP Relay** page.
2. Click **Display Advanced Configuration** to expand the advanced DHCP relay agent configuration area.

Figure 286 DHCP relay agent configuration page

3. Enable DHCP service and configure advanced parameters for DHCP relay agent as described in Table 95.
4. Click **Apply**.

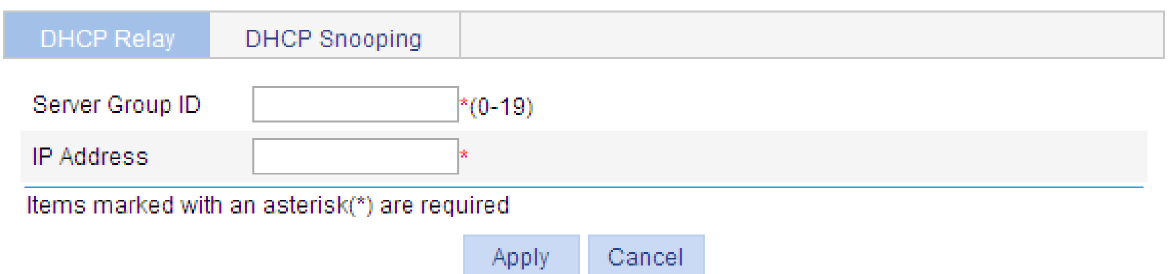
Table 95 Configuration items

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.
Track Timer Interval	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** option is selected, the refresh interval is calculated by the relay agent according to the number of client entries.

Creating a DHCP server group

1. Select **Network** > **DHCP** from the navigation tree to enter the **DHCP Relay** page shown in Figure 286.
2. In the **Server Group** area, click **Add** to enter the server group configuration page.

Figure 287 Creating a server group



3. Configure the DHCP server group as described in Table 96.

4. Click **Apply**.

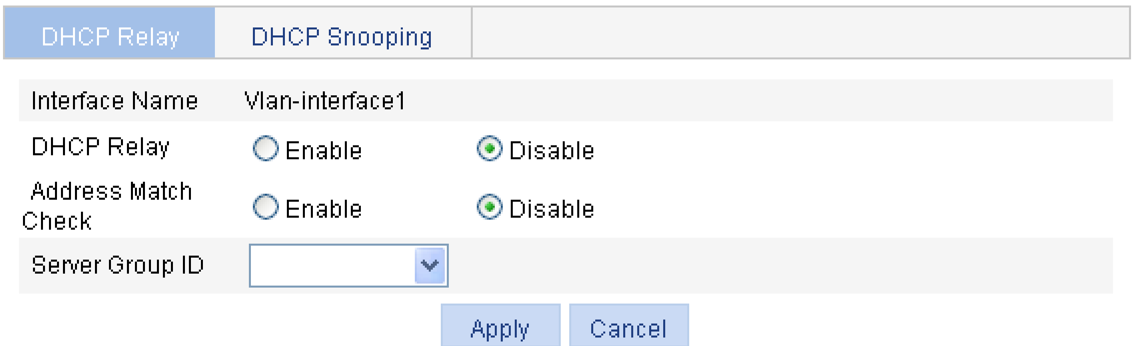
Table 96 Configuration items

Item	Description
Server Group ID	Enter the ID of a DHCP server group. You can create up to 20 DHCP server groups.
IP Address	Enter 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.

Enabling the DHCP relay agent on an interface

1. Select **Network** > **DHCP** from the navigation tree to enter the **DHCP Relay** page shown in Figure 286.
2. In the **Interface Config** area, click the  icon for a specific interface.

Figure 288 Configuring a DHCP relay agent interface



3. Configure the DHCP relay agent on the interface as shown in Table 97.
4. Click **Apply**.

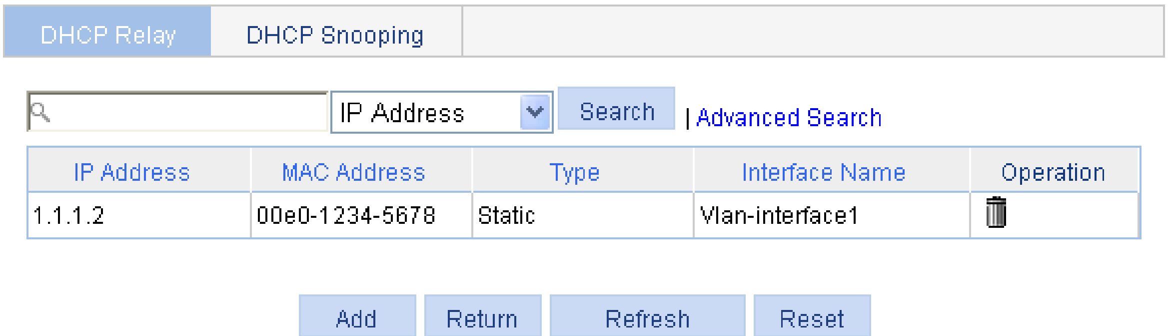
Table 97 Configuration items

Item	Description
Interface Name	Displays the name of a specific interface.
DHCP Relay	Enable or disable the DHCP relay agent on the interface. If the DHCP relay agent is disabled, the DHCP server is enabled 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.

Configuring and displaying clients' IP-to-MAC bindings

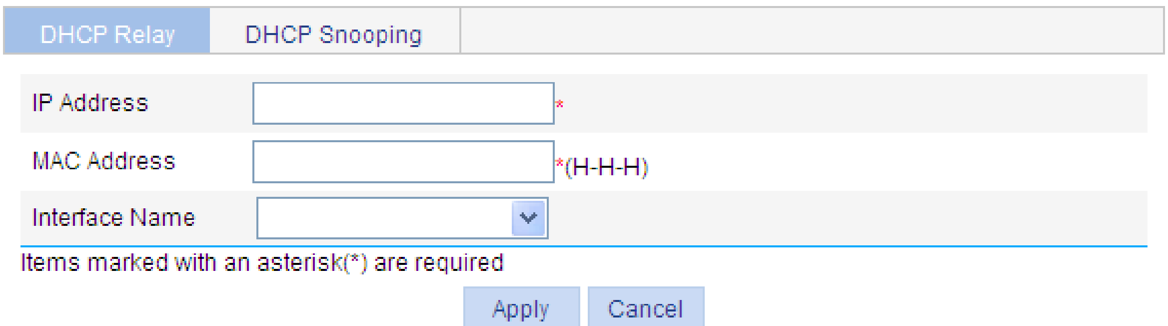
1. Select **Network** > **DHCP** from the navigation tree to enter the **DHCP Relay** page shown in Figure 286.
2. In the **User Information** area, click **User Information** to view static and dynamic bindings.

Figure 289 Displaying clients' IP-to-MAC bindings



3. Click **Add** to enter the page for creating a static IP-to-MAC binding.

Figure 290 Creating a static IP-to-MAC binding



4. Configure the static IP-to-MAC binding as described in Table 98.
5. Click **Apply**.

Table 98 Configuration items

Item	Description
IP Address	Enter the IP address of a DHCP client.
MAC Address	Enter the MAC address of the DHCP client.
Interface Name	Select the Layer 3 interface connected with the DHCP client. IMPORTANT: The interface of a static binding entry must be configured as a DHCP relay agent; otherwise, address entry conflicts may occur.

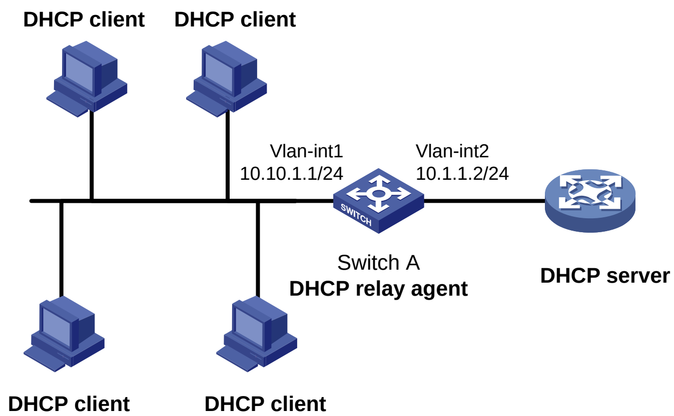
DHCP relay agent configuration example

Network requirements

As shown in Figure 291, VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. 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.

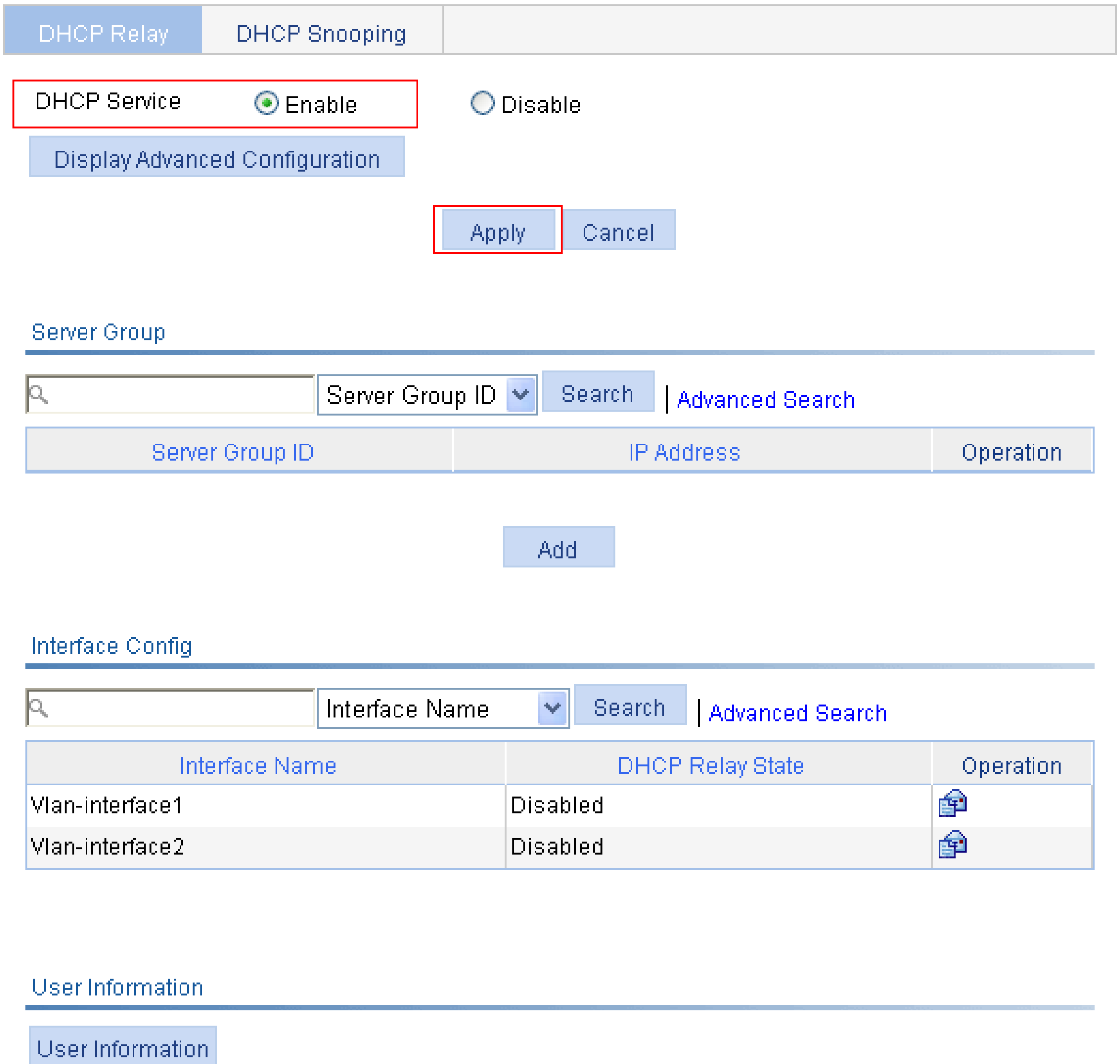
Figure 291 Network diagram



Configuring Switch A

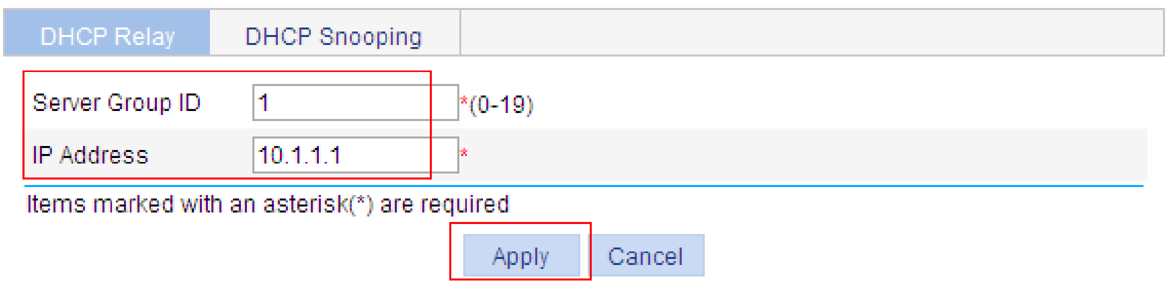
1. Enable DHCP:
   a. Select **Network** > **DHCP** from the navigation tree to enter the **DHCP Relay** page.
   b. Select the **Enable** option next to **DHCP Service**.
   c. Click **Apply**.

Figure 292 Enabling DHCP



2. Configure a DHCP server group:
   a. In the **Server Group** area, click **Add**.
   b. On the page that appears, enter **1** for **Server Group ID**, and enter **10.1.1.1** for **IP Address**.
   c. Click **Apply**.

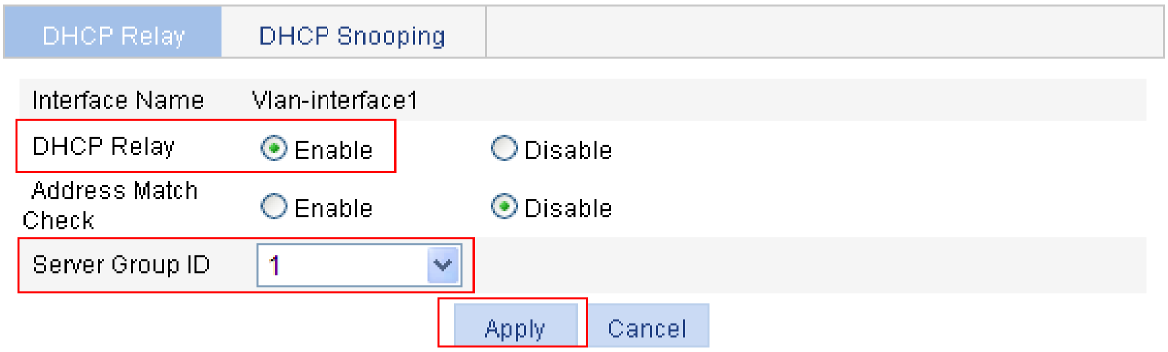
Figure 293 Adding a DHCP server group



3. Enable the DHCP relay agent on VLAN-interface 1:

a. In the **Interface Config** field, click the icon for VLAN-interface 1.
b. On that page that appears, select the **Enable** option next to **DHCP Relay** and select **1** for **Server Group ID**.
c. Click **Apply**.

Figure 294 Enabling the DHCP relay agent on an interface and correlate it with a server group



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.

Configuring DHCP snooping

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.

Overview

DHCP snooping functions

As a DHCP security feature, DHCP snooping can provide the following functions:

1. Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers.
2. Recording the IP-to-MAC mappings of DHCP clients.

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 communicate with other network devices. DHCP snooping ensures the clients to obtain IP addresses from authorized DHCP servers through trusted or untrusted port configuration.

- **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.

Configure the ports connected to DHCP servers and other DHCP snooping devices as trusted ports and configure other ports as untrusted ports.

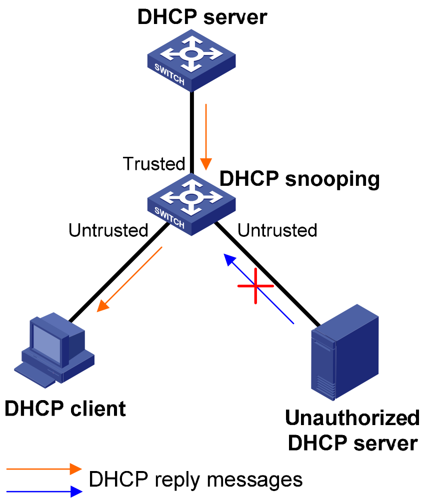
Recording IP-to-MAC mappings of DHCP clients

DHCP snooping reads DHCP-REQUEST and DHCP-ACK messages received from trusted ports to create DHCP snooping entries that each include the MAC address of a client, IP address obtained by the client, port connected to the DHCP client, and VLAN to which the port belongs. The DHCP snooping entries can be used by ARP detection to prevent ARP attacks.

Application of trusted ports

Configuring a trusted port connected to a DHCP server

Figure 295 Configuring trusted and untrusted ports



As shown in Figure 295, 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, 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 296 Configuring trusted ports in a cascaded network

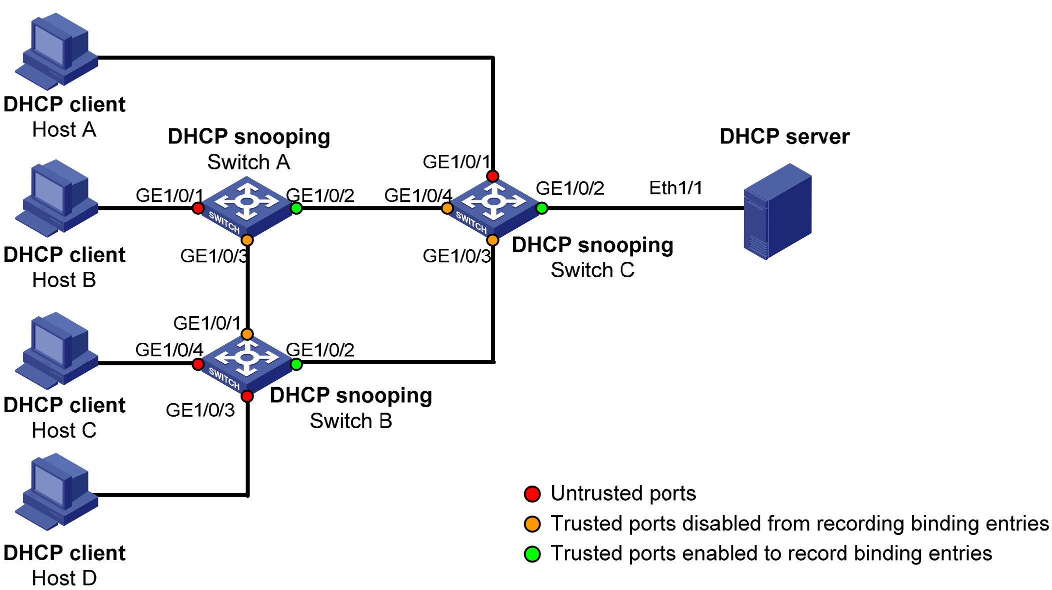


Table 99 describes roles of the ports shown in Figure 296.

Table 99 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, see "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.

Table 100 Handling strategy of DHCP snooping support for Option 82

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	N/A	Forward the message after adding the Option 82 padded in normal format.

Recommended configuration procedure

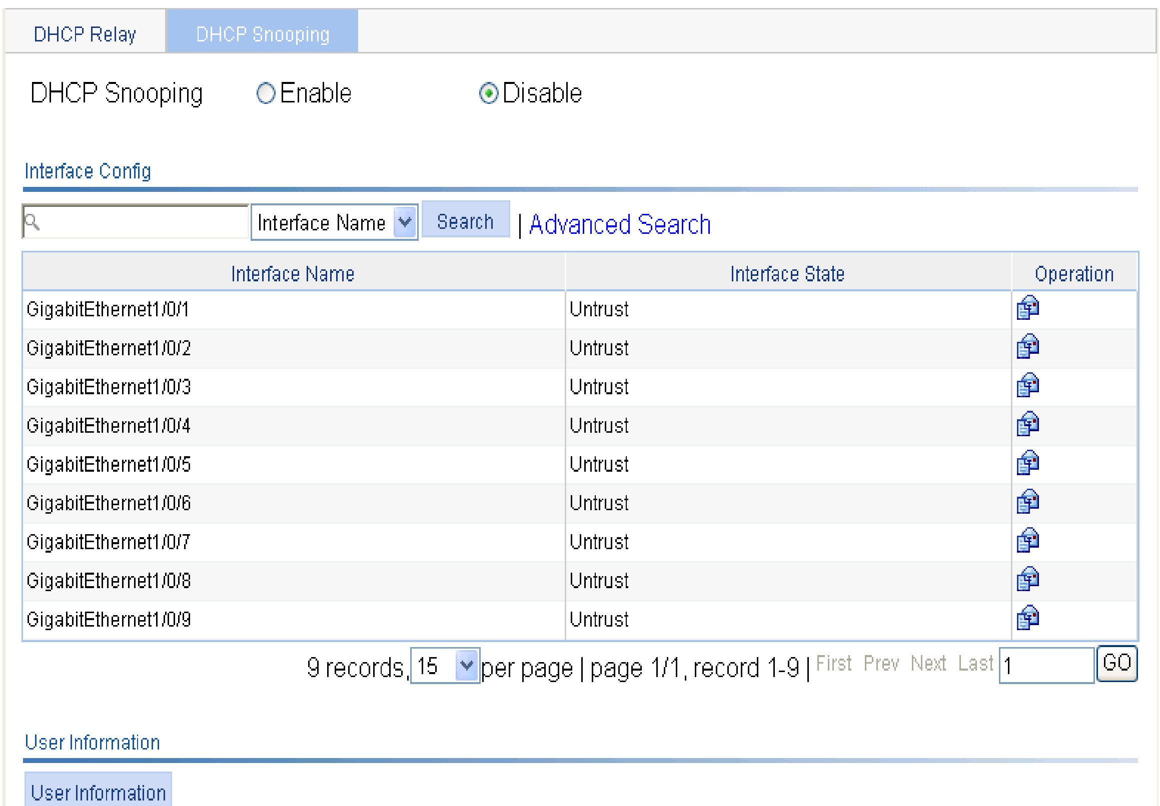
Step	Remarks
1. Enabling DHCP snooping	(Required) By default, DHCP snooping is disabled.

Step	Remarks
2. 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. IMPORTANT: You need to specify the ports connected to the authorized DHCP servers as trusted to make sure 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.
3. Displaying clients' IP-to-MAC bindings	(Optional) Display clients' IP-to-MAC bindings recorded by DHCP snooping.

Enabling DHCP snooping

1. Select **Network** > **DHCP** from the navigation tree.
2. Click the **DHCP Snooping** tab to enter the DHCP snooping configuration page.
3. Select the **Enable** option next to **DHCP Snooping** to enable DHCP Snooping.

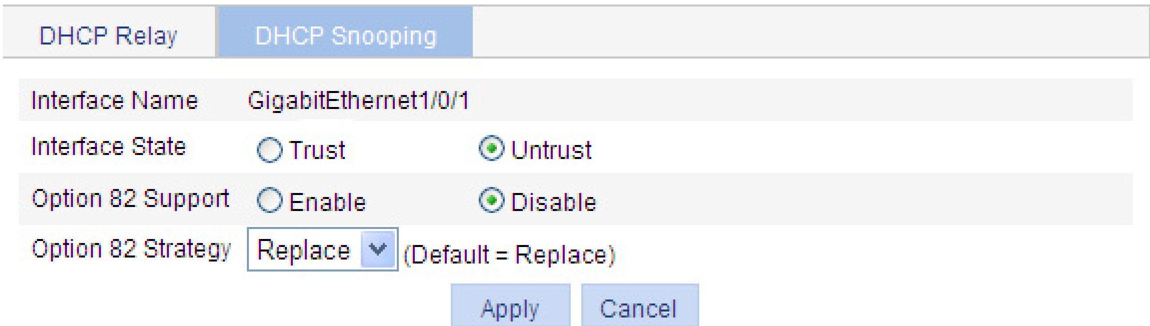
Figure 297 DHCP snooping configuration page



Configuring DHCP snooping functions on an interface

1. Select **Network** > **DHCP** from the navigation tree.
2. Click the **DHCP Snooping** tab to enter the page shown in Figure 297.
3. Click the icon for a specific interface in the **Interface Config** area.

Figure 298 DHCP snooping interface configuration page



4. Configure DHCP snooping on the interface as described in Table 101.
5. Click **Apply**.

Table 101 Configuration items

Item	Description
Interface Name	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.

Displaying clients' IP-to-MAC bindings

1. Select **Network** > **DHCP** from the navigation tree.
2. Click the **DHCP Snooping** tab to enter the page shown in Figure 297.
3. Click **User Information** to enter the DHCP snooping user information page.
   Table 102 describes the fields of DHCP snooping entries.

Figure 299 DHCP snooping user information

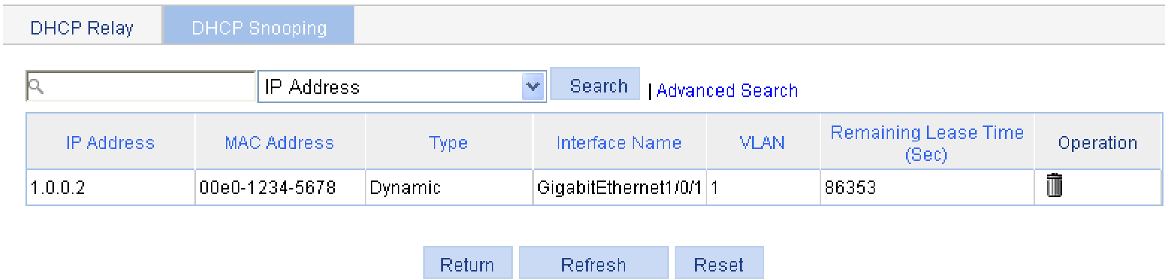


Table 102 Field description

Field	Description
IP Address	Displays the IP address assigned by the DHCP server to the client.
MAC Address	Displays the MAC address of the client.
Type	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	Displays the device interface to which the client is connected.
VLAN	Displays the VLAN to which the device belongs.
Remaining Lease Time	Displays the remaining lease time of the IP address.

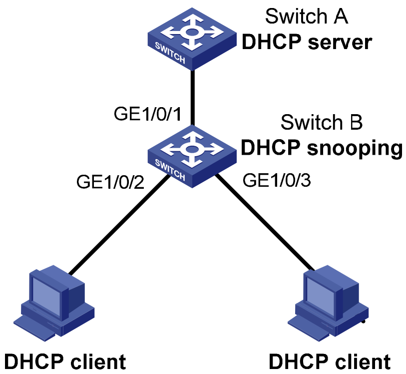
DHCP snooping configuration example

Network requirements

As shown in Figure 300, 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.

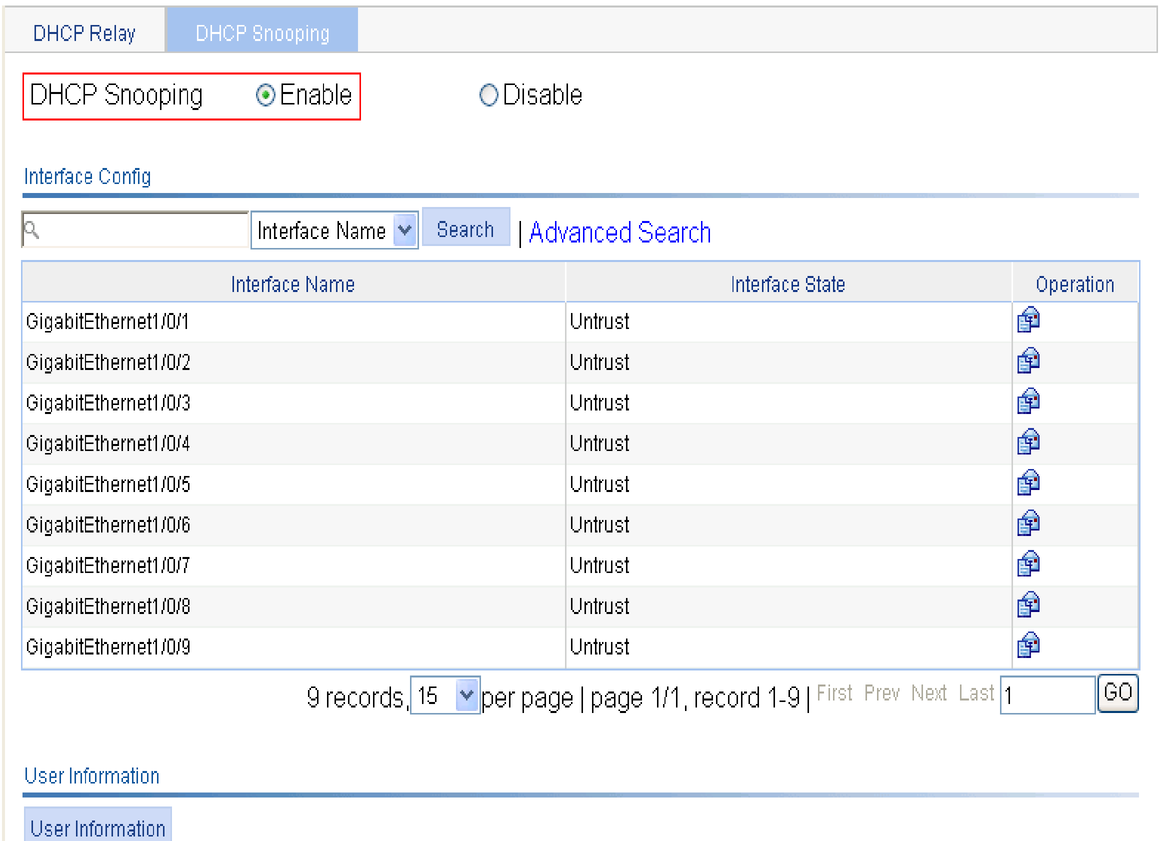
Figure 300 Network diagram



Configuring Switch B

1. Enable DHCP snooping:
   a. Select **Network** > **DHCP** from the navigation tree.
   b. Click the **DHCP Snooping** tab.
   c. Select the **Enable** option next to **DHCP Snooping** to enable DHCP snooping.

Figure 301 Enabling DHCP snooping

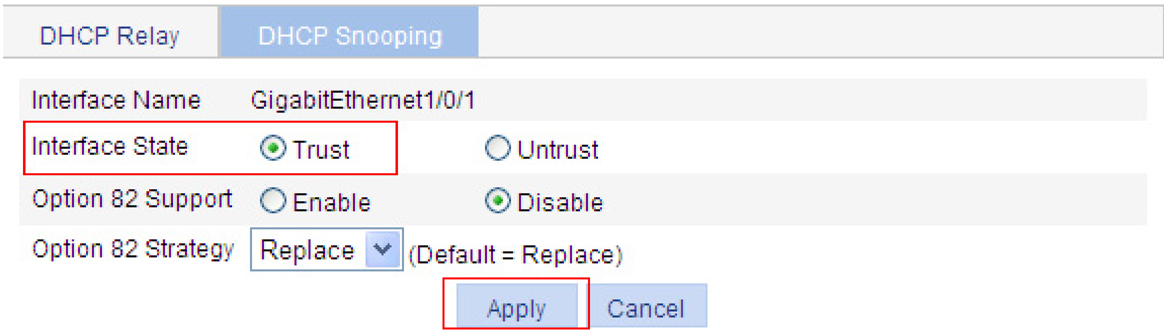


2. Configure DHCP snooping functions on GigabitEthernet 1/0/1:
   a. Click the icon for **GigabitEthernet 1/0/1** on the interface list.

b. Select the **Trust** option next to **Interface State**.

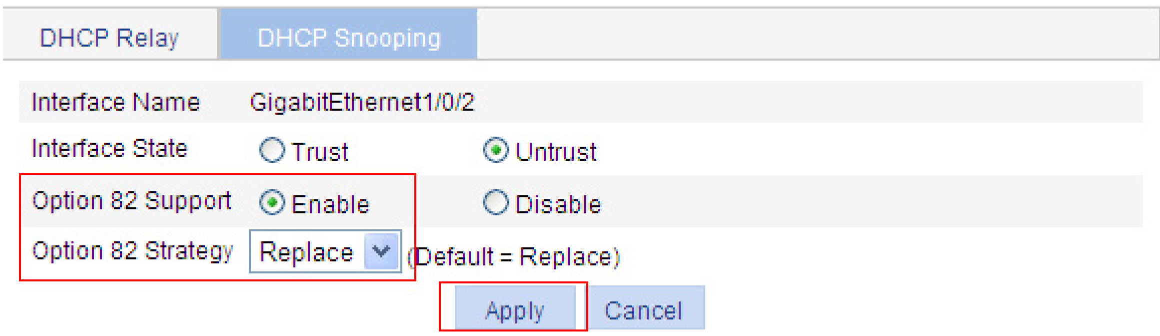
c. Click **Apply**.

Figure 302 Configuring DHCP snooping functions on GigabitEthernet 1/0/1



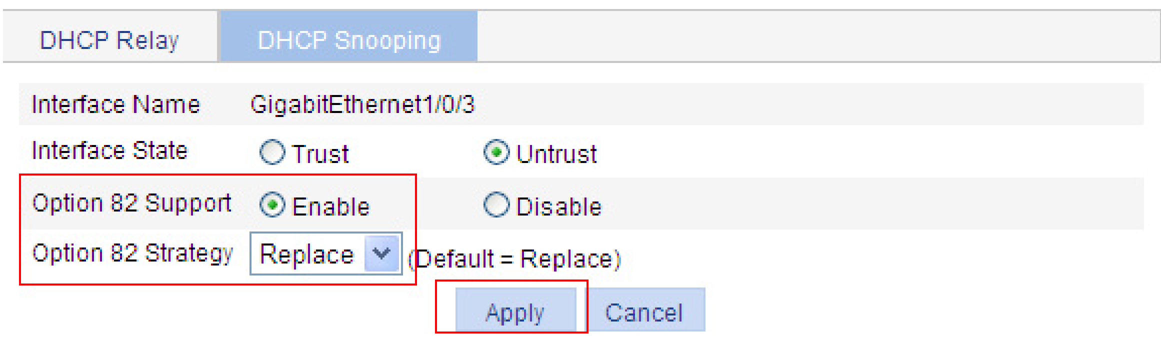
3. Configure DHCP snooping functions on GigabitEthernet 1/0/2:
   a. Click the icon for **GigabitEthernet 1/0/2** on the interface list.
   b. Select the **Untrust** option for **Interface State**, select the **Enable** option next to **Option 82 Support**, and select **Replace** for **Option 82 Strategy**.
   c. Click **Apply**.

Figure 303 Configuring DHCP snooping functions on GigabitEthernet 1/0/2



4. Configure DHCP snooping functions on GigabitEthernet 1/0/3:
   a. Click the icon for **GigabitEthernet 1/0/3** on the interface list.
   b. Select the **Untrust** option for **Interface State**, select the **Enable** option next to **Option 82 Support**, and select **Replace** for **Option 82 Strategy**.
   c. Click **Apply**.

Figure 304 Configuring DHCP snooping functions on GigabitEthernet 1/0/3



Managing services

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 Hypertext Transfer Protocol Secure (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.

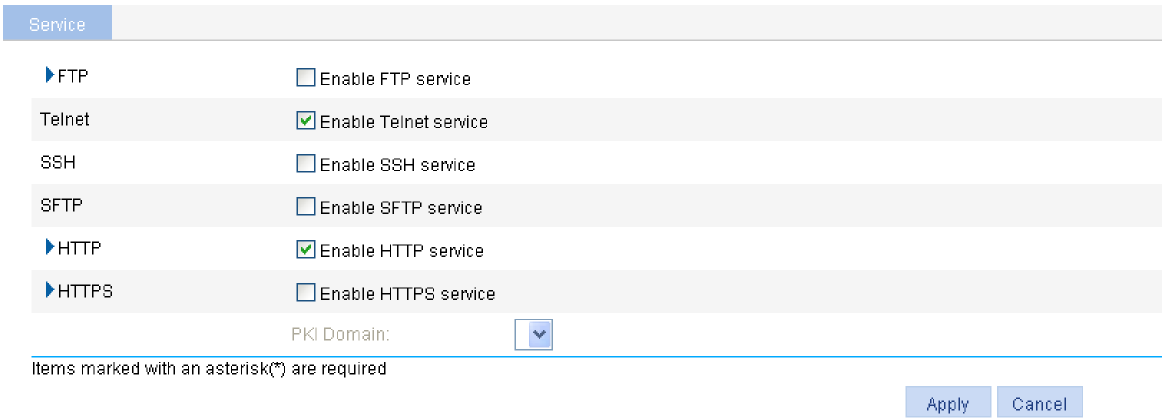
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.

Managing services

1. Select **Network** > **Service** from the navigation tree.

   The service management configuration page appears.

Figure 305 Service management



2. Manage services as described in Table 103.
3. Click **Apply**.

Table 103 Configuration items

Item		Description
FTP	Enable FTP service	Enable or disable the FTP service. The FTP service is disabled by default.
	ACL	Associate 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	Enable or disable the Telnet service. The Telnet service is disabled by default.
SSH	Enable SSH service	Enable or disable the SSH service. The SSH service is disabled by default.
SFTP	Enable SFTP service	Enable or disable the SFTP service. The SFTP service is disabled by default. IMPORTANT: When you enable the SFTP service, the SSH service must be enabled.

Item		Description
HTTP	Enable HTTP service	Enable or disable the HTTP service. The HTTP service is enabled by default.
	Port Number	Set the port number for HTTP service. You can view this configuration item by clicking the expanding button in front of **HTTP**. IMPORTANT: When you modify a port, make sure that the port is not used by any other service.
	ACL	Associate 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	Enable or disable the HTTPS service. The HTTPS service is disabled by default.
	Port Number	Set the port number for the HTTPS service. You can view this configuration item by clicking the expanding button in front of **HTTPS**. IMPORTANT: When you modify a port, make sure that the port is not used by any other service.
	ACL	Associate 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	Select a PKI domain for the HTTPS service from the **PKI Domain** dropdown list. You can configure the PKI domains available in the dropdown list in **Authentication** > **PKI**. For more information, see "Configuring PKI."

Using diagnostic tools

Overview

Ping

Use ping to test connectivity to a specified address.

Ping operates as follows:

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:

- You can ping the IP address or the host name of a destination device. If the target host name cannot be resolved, the source device outputs related information.
- If the source device does not receive an ICMP echo reply within the timeout time, it displays prompt information and ping statistics. If the source device receives an ICMP echo reply within the timeout time, it displays the number of bytes the echo reply has, message sequence number, Time to Live (TTL), response time, and ping statistics.

Ping statistics include the number of packets sent, number of echo reply messages received, percentage of messages not received, and the minimum, average, and maximum response time.

Traceroute

By using the **traceroute** command, you can view 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.

You can trace route the IP address or the host name of a destination device. If the target host name cannot be resolved, the source device outputs related information.

Traceroute operates as follows:

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) sends a TTL-expired ICMP message to the source. The source device can get the address of the first Layer 3 device from the ICMP message.
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 packet reaches the destination device. The destination device responds with a port-unreachable ICMP message to the source so the source device can get the IP address of the last device on the path.

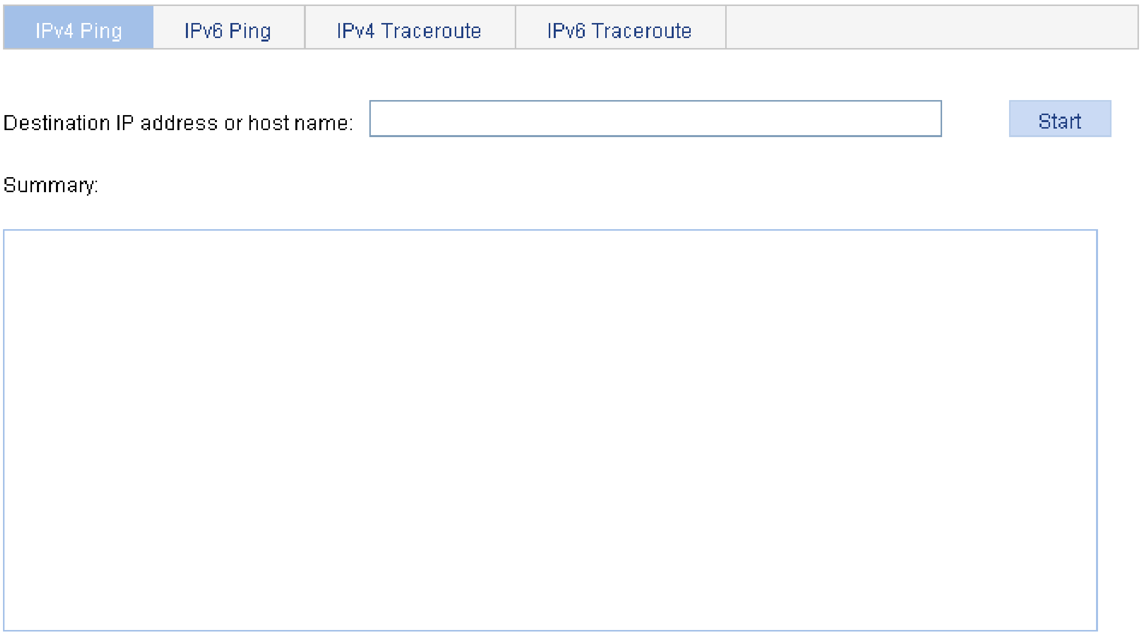
Ping operation

IPv4 ping operation

1. Select **Network** > **Diagnostic Tools** from the navigation tree.

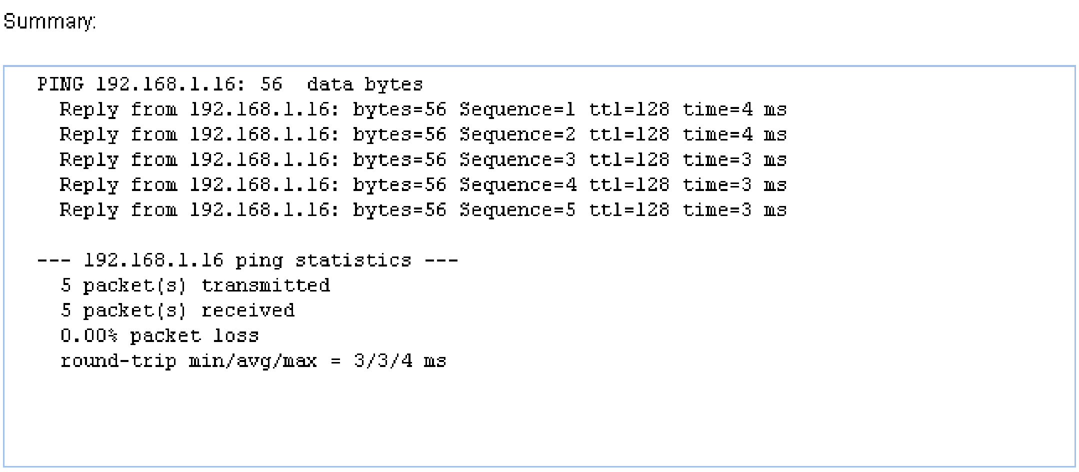
   The IPv4 ping configuration page appears.

Figure 306 IPv4 ping configuration page



2. Type the IPv4 address or the host name of the destination device in the **Destination IP address or host name** field.
3. Click **Start** to execute the **ping** command.
4. View the operation result in the **Summary** area.

Figure 307 IPv4 ping operation result




```
PING 192.168.1.16: 56  data bytes
  Reply from 192.168.1.16: bytes=56 Sequence=1 ttl=128 time=4 ms
  Reply from 192.168.1.16: bytes=56 Sequence=2 ttl=128 time=4 ms
  Reply from 192.168.1.16: bytes=56 Sequence=3 ttl=128 time=3 ms
  Reply from 192.168.1.16: bytes=56 Sequence=4 ttl=128 time=3 ms
  Reply from 192.168.1.16: bytes=56 Sequence=5 ttl=128 time=3 ms

--- 192.168.1.16 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/4 ms
```

IPv6 ping operation

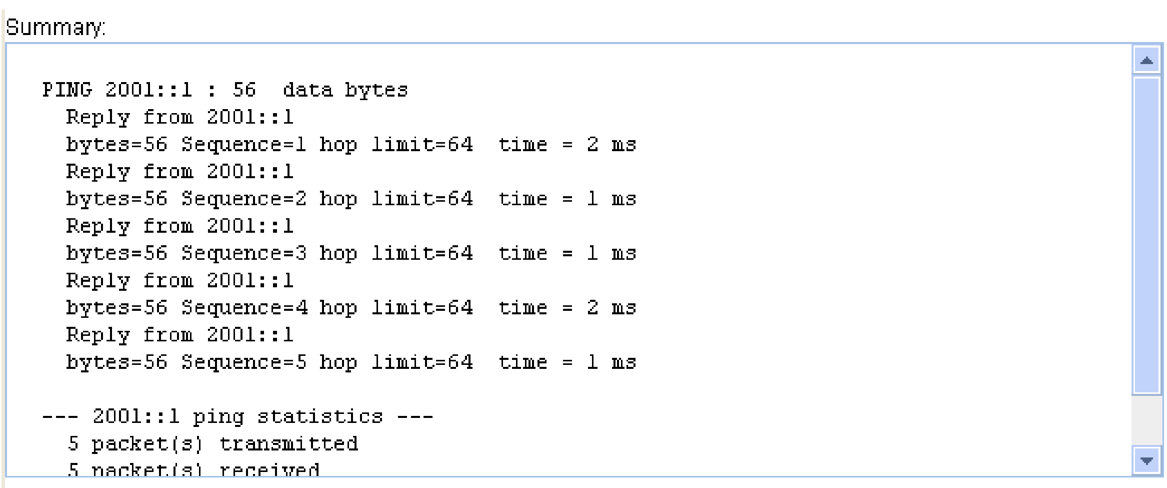
1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv6 Ping** tab.

   The IPv6 ping configuration page appears.

Figure 308 IPv6 ping configuration page

3. Type the IPv6 address or the host name of the destination device in the **Destination IPv6 address or host name** field.
4. Click **Start** to execute the **ping** command.
5. View the operation result in the **Summary** area.

Figure 309 IPv6 ping operation result



Traceroute operation

NOTE:

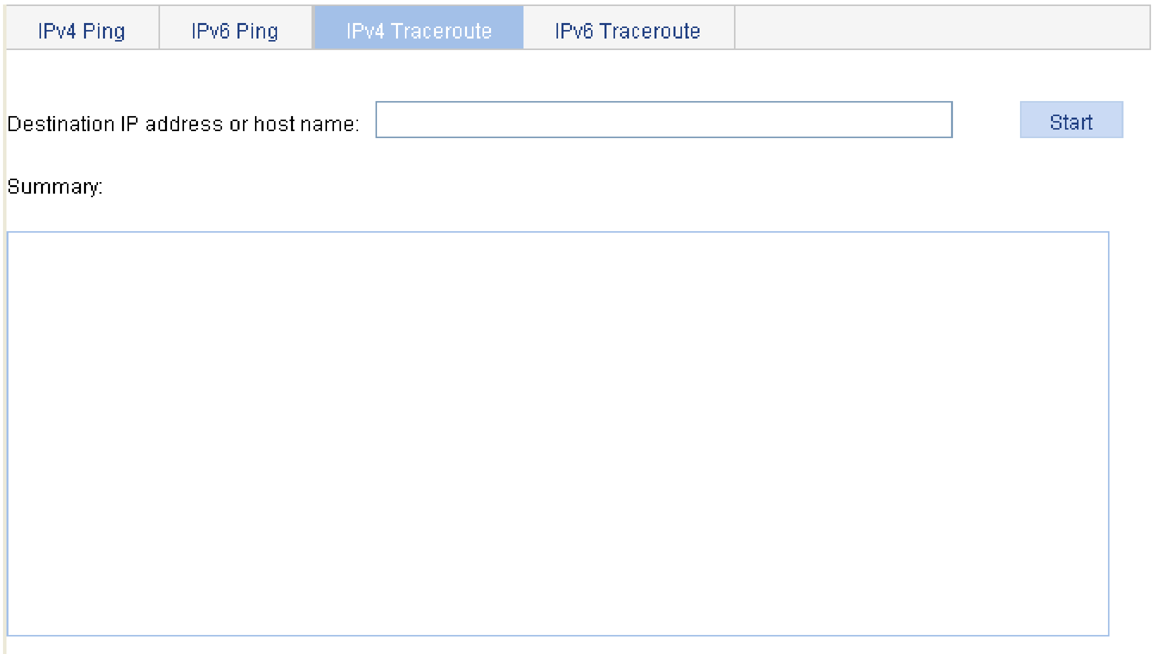
Before performing the traceroute operation, execute the **ip ttl-expires enable** command on intermediate devices to enable the sending of ICMP timeout packets, and execute the **ip unreachables enable** command on the destination device to enable the sending of ICMP destination unreachable packets.

IPv4 traceroute operation

1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv4 Traceroute** tab.

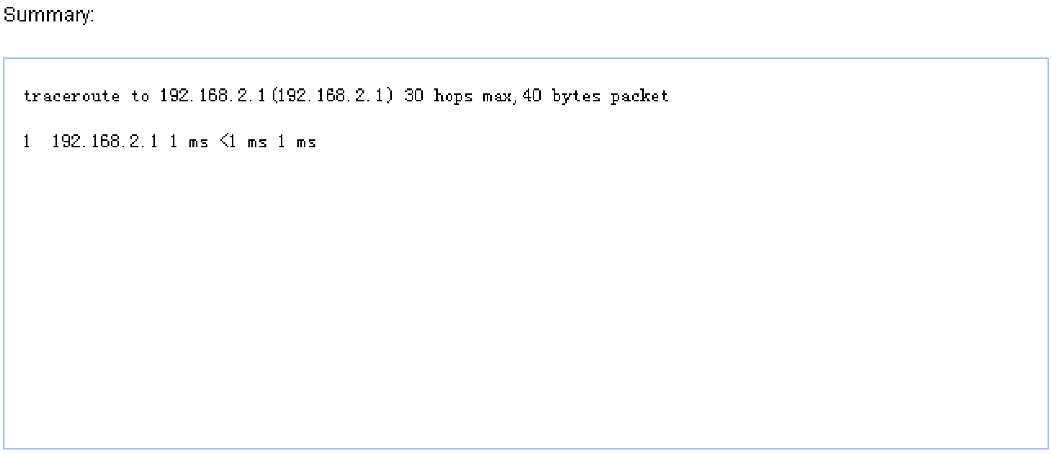
   The IPv4 traceroute configuration page appears.

Figure 310 IPv4 traceroute configuration page



3. Type the IPv4 address or host name of the destination device in the **Destination IP address or host name** field.
4. Click **Start** to execute the **traceroute** command.
5. View the operation result in the **Summary** area.

Figure 311 IPv4 traceroute operation result



IPv6 traceroute operation

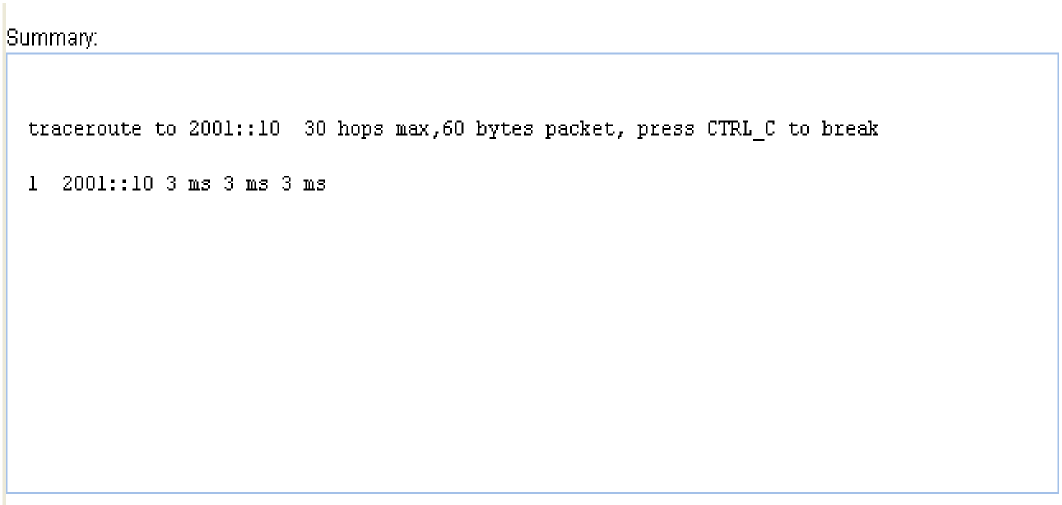
1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv6 Traceroute** tab.

   The IPv6 traceroute configuration page appears.

Figure 312 IPv6 traceroute configuration page

3. Type the IPv6 address or host name of the destination device in the **Destination IPv6 address or host name** field.
4. Click **Start** to execute the **traceroute** command.
5. View the operation result in the **Summary** area.

Figure 313 IPv6 traceroute operation result



Configuring 802.1X

Overview

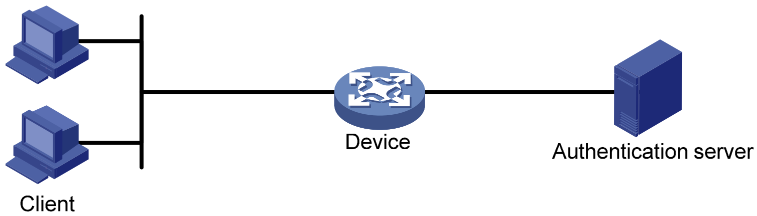
802.1X is a port-based network access control protocol initially proposed by the IEEE 802 LAN/WAN committee for the security of wireless LANs (WLANs). It has been widely used on Ethernet for access control.

802.1X controls network access by authenticating devices connected to the 802.1X-enabled LAN ports.

802.1X architecture

802.1X operates in the client/server model. It comprises three entities: the client (the supplicant), the network access device (the authenticator), and the authentication server.

Figure 314 Architecture of 802.1X



- The client is a user terminal seeking access to the LAN. It must have 802.1X software to authenticate to the network access device.
- The network access device authenticates the client to control access to the LAN. In a typical 802.1X environment, the network access device uses an authentication server to perform authentication.
- The authentication server is the entity that provides authentication services for the network access device. It authenticates 802.1X clients by using the data sent from the network access device, and returns the authentication results for the network access device to make access decisions. The authentication server is typically a Remote Authentication Dial-in User Service (RADIUS) server. In a small LAN, you can also use the network access device as the authentication server.

Access control methods

HP implements port-based access control as defined in the 802.1X protocol, and extends the protocol to support MAC-based access control.

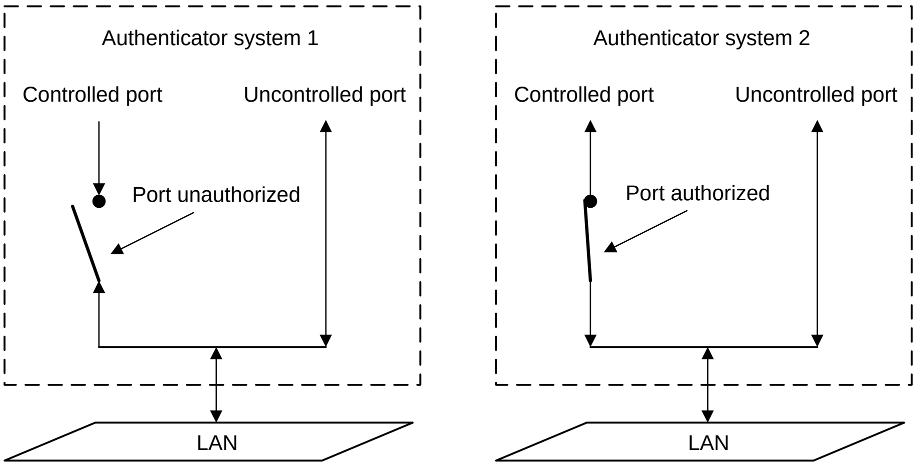
- **Port-based access control**—once an 802.1X user passes authentication on a port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.
- **MAC-based access control**—Each user is separately authenticated on a port. When a user logs off, no other online users are affected.

Controlled/uncontrolled port and port authorization status

802.1X defines two logical ports for the network access port: controlled port and uncontrolled port. Any packet arriving at the network access port is visible to both logical ports.

- The controlled port allows incoming and outgoing traffic to pass through when it is in the authorized state, and denies incoming and outgoing traffic when it is in the unauthorized state, as shown in Figure 315. The controlled port is set in the authorized state if the client has passed authentication, and in the unauthorized state, if the client has failed authentication.
- The uncontrolled port is always open to receive and transmit EAPOL frames.

Figure 315 Authorization state of a controlled port



In the unauthorized state, a controlled port controls traffic in one of the following ways:

- Performs bidirectional traffic control to deny traffic to and from the client.
- Performs unidirectional traffic control to deny traffic from the client.

The device supports only unidirectional traffic control.

802.1X-related protocols

802.1X uses the Extensible Authentication Protocol (EAP) to transport authentication information for the client, the network access device, and the authentication server. EAP is an authentication framework that uses the client/server model. It supports a variety of authentication methods, including MD5-Challenge, EAP-Transport Layer Security (EAP-TLS), and Protected EAP (PEAP).

802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the network access device over a wired or wireless LAN. Between the network access device and the authentication server, 802.1X delivers authentication information in one of the following methods:

- Encapsulates EAP packets in RADIUS by using EAP over RADIUS (EAPOR), as described in "EAP relay ."

Extracts authentication information from the EAP packets and encapsulates the information in standard RADIUS packets, as described in "EAP termination

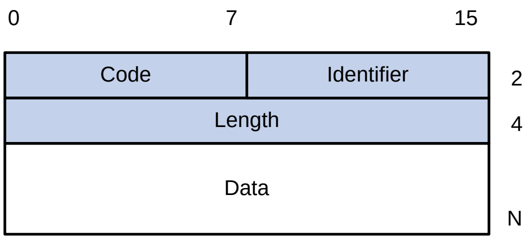
- ."

Packet formats

EAP packet format

Figure 316 shows the EAP packet format.

Figure 316 EAP packet format

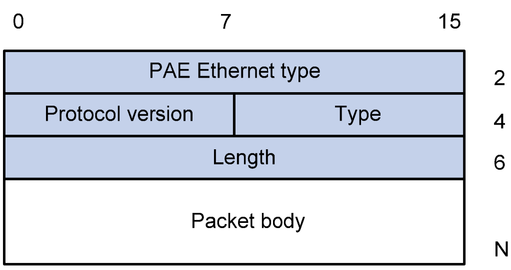


- **Code**—Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- **Identifier**—Used for matching Responses with Requests.
- **Length**—Length (in bytes) of the EAP packet, which is the sum of the Code, Identifier, Length, and Data fields.
- **Data**—Content of the EAP packet. This field appears only in a Request or Response EAP packet. The field comprises the request type (or the response type) and the type data. Type 1 (Identify) and type 4 (MD5-challenge) are two examples for the type field.

EAPOL packet format

Figure 317 shows the EAPOL packet format.

Figure 317 EAPOL packet format



- PAE Ethernet type—Protocol type. It takes the value 0x888E for EAPOL.
- **Protocol version**—The EAPOL protocol version used by the EAPOL packet sender.
- **Type**—Type of the EAPOL packet. Table 104 lists the types of EAPOL packets that the HP implementation of 802.1X supports.

Table 104 Types of EAPOL packets

Value	Type	Description
0x00	EAP-Packet	The client and the network access device uses EAP-Packets to transport authentication information.
0x01	EAPOL-Start	The client sends an EAPOL-Start message to initiate 802.1X authentication to the network access device.

Value	Type	Description
0x02	EAPOL-Logoff	The client sends an EAPOL-Logoff message to tell the network access device that it is logging off.

- **Length**—Data length in bytes, or length of the Packet body. If packet type is EAPOL-Start or EAPOL-Logoff, this field is set to 0, and no Packet body field follows.
- **Packet body**—Content of the packet. When the EAPOL packet type is EAP-Packet, the Packet body field contains an EAP packet.

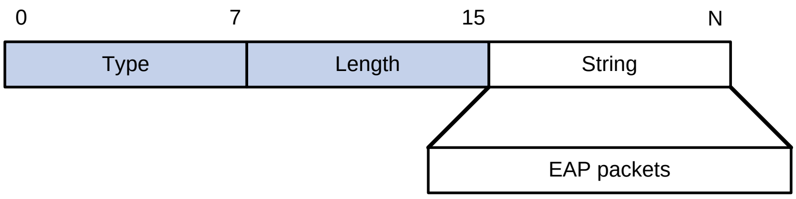
EAP over RADIUS

RADIUS adds two attributes, EAP-Message and Message-Authenticator, for supporting EAP authentication. For the RADIUS packet format, see "Configuring RADIUS."

EAP-Message

RADIUS encapsulates EAP packets in the EAP-Message attribute, as shown in Figure 318. The Type field takes 79, and the Value field can be up to 253 bytes. If an EAP packet is longer than 253 bytes, RADIUS encapsulates it in multiple EAP-Message attributes.

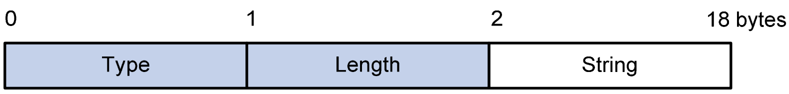
Figure 318 EAP-Message attribute format



Message-Authenticator

RADIUS includes the Message-Authenticator attribute in all packets that have an EAP-Message attribute to check their integrity. The packet receiver drops the packet if the calculated packet integrity checksum is different than the Message-Authenticator attribute value. The Message-Authenticator prevents EAP authentication packets from being tampered with during EAP authentication.

Figure 319 Message-Authenticator attribute format



Initiating 802.1X authentication

Both the 802.1X client and the access device can initiate 802.1X authentication.

802.1X client as the initiator

The client sends an EAPOL-Start packet to the access device to initiate 802.1X authentication. The destination MAC address of the packet is the IEEE 802.1X specified multicast address 01-80-C2-00-00-03 or the broadcast MAC address. If any intermediate device between the client and the authentication server does not support the multicast address, you must use an 802.1X client, the HP iNode 802.1X client for example, that can send broadcast EAPOL-Start packets.

Access device as the initiator

The access device initiates authentication, if a client, the 802.1X client available with Windows XP for example, cannot send EAPOL-Start packets.

The access device supports the following modes:

- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets periodically (every 30 seconds by default) to initiate 802.1X authentication.
- **Unicast trigger mode**—Upon receiving a frame with the source MAC address not in the MAC address table, the access device sends an Identity EAP-Request packet out of the receiving port to the unknown MAC address. It retransmits the packet if no response has been received within a certain time interval.

802.1X authentication procedures

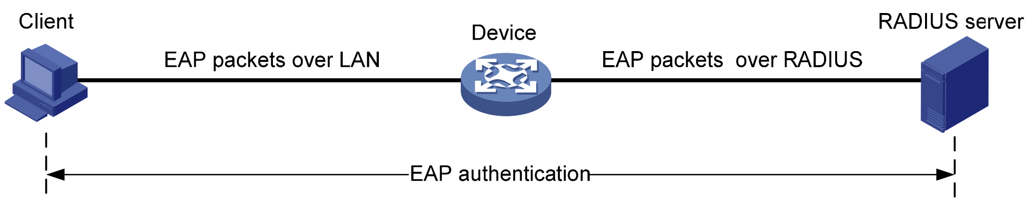
802.1X authentication has two approaches: EAP relay and EAP termination. You choose either mode depending on the support of the RADIUS server for EAP packets and EAP authentication methods.

- EAP relay mode

  EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAPoR packets to send authentication information to the RADIUS server, as shown in Figure 320.

  In EAP relay mode, the client must use the same authentication method as the RADIUS server. On the network access device, you only need to enable EAP relay.

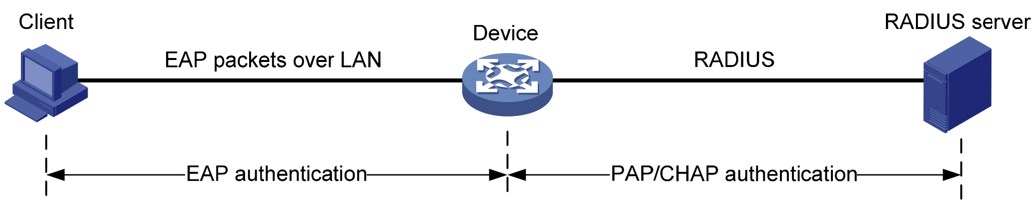
Figure 320 EAP relay



- EAP termination mode

  In EAP termination mode, the network access device terminates the EAP packets received from the client, encapsulates the client authentication information in standard RADIUS packets, and uses (Password Authentication Protocol) PAP or (Password Authentication Protocol) CHAP to authenticate to the RADIUS server, as shown in Figure 321.

Figure 321 EAP termination



A comparison of EAP relay and EAP termination

When configuring EAP relay or EAP termination, consider the following factors:

- The support of the RADIUS server for EAP packets.
- The authentication methods supported by the 802.1X client and the RADIUS server.

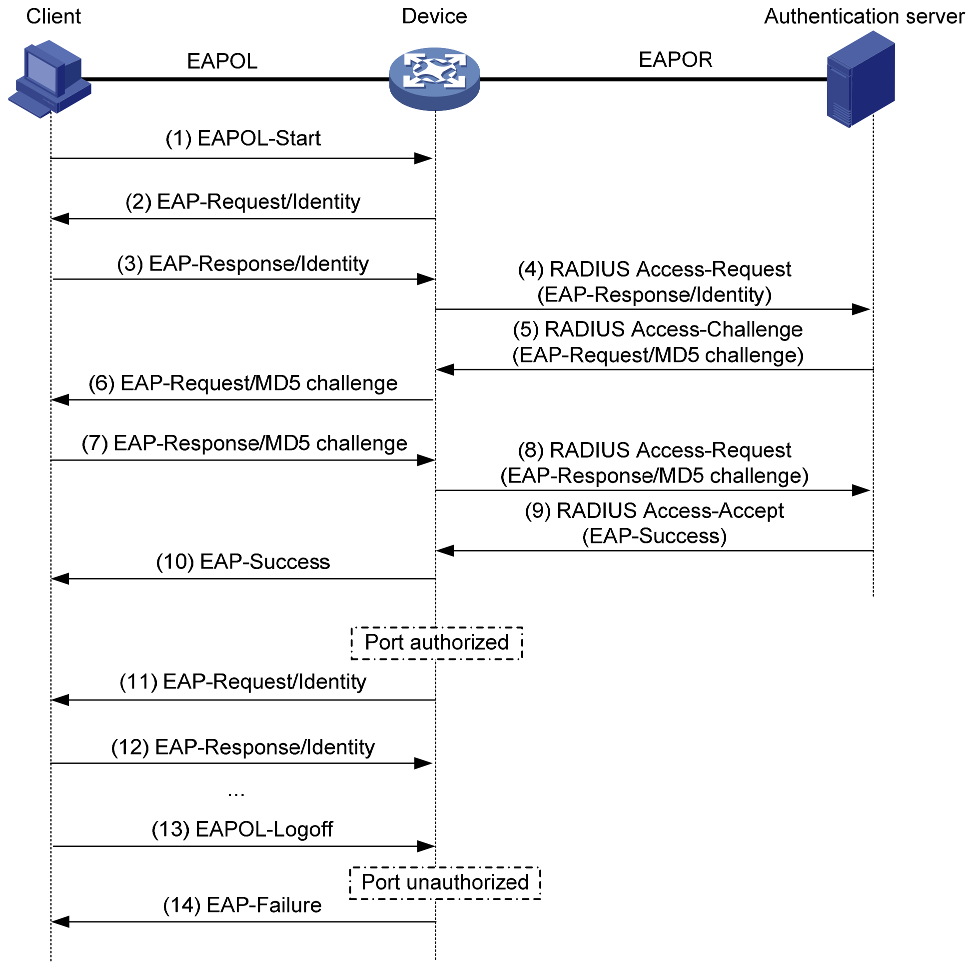
- If the client is using only MD5-Challenge EAP authentication or the "username + password" EAP authentication initiated by an HP iNode 802.1X client, you can use both EAP termination and EAP relay. To use EAP-TL, PEAP, or any other EAP authentication methods, you must use EAP relay.

Packet exchange method	Benefits	Limitations
EAP relay	• Supports various EAP authentication methods. • The configuration and processing is simple on the network access device.	The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client.
EAP termination	Works with any RADIUS server that supports PAP or CHAP authentication.	• Supports only MD5-Challenge EAP authentication and the "username + password" EAP authentication initiated by an HP iNode 802.1X client. • The processing is complex on the network access device.

EAP relay

Figure 322 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

Figure 322 802.1X authentication procedure in EAP relay mode



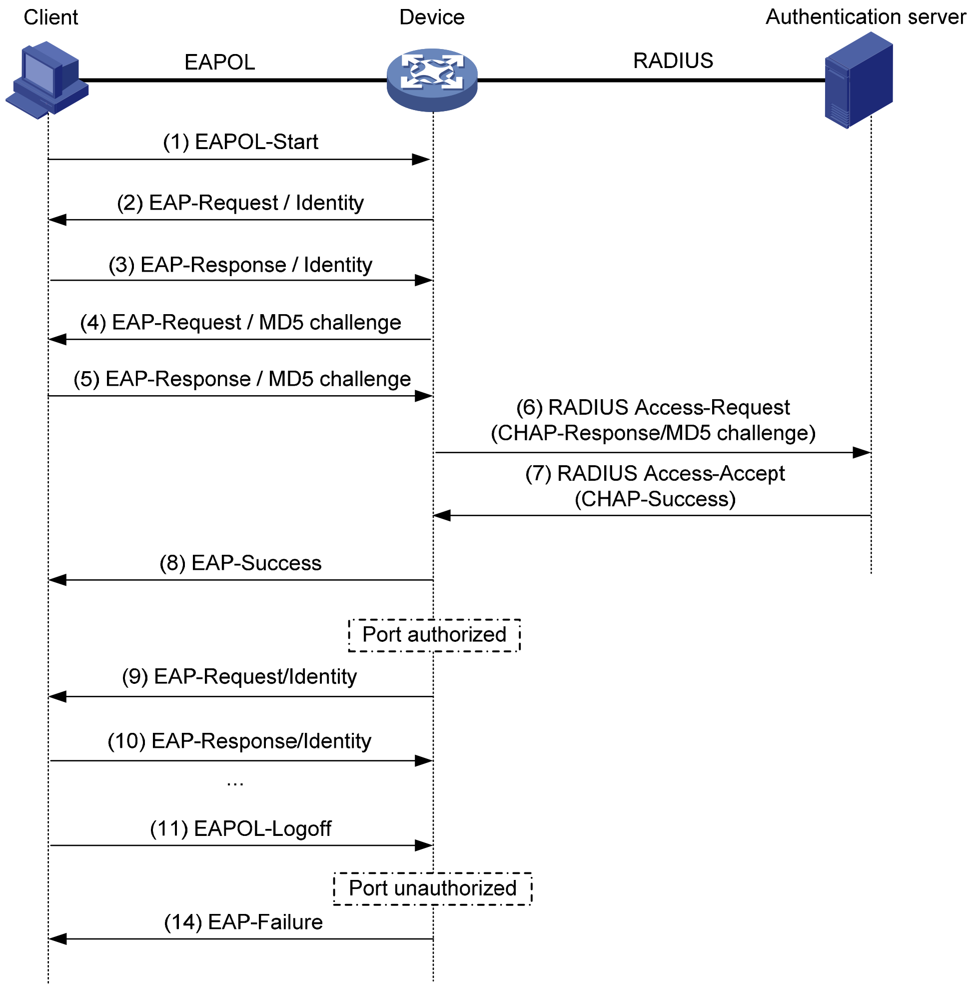
1. When a user launches the 802.1X client software and enters a registered username and password, the 802.1X client software sends an EAPOL-Start packet to the network access device.
2. The network access device responds with an Identity EAP-Request packet to ask for the client username.
3. In response to the Identity EAP-Request packet, the client sends the username in an Identity EAP-Response packet to the network access device.
4. The network access device relays the Identity EAP-Response packet in a RADIUS Access-Request packet to the authentication server.
5. The authentication server uses the identity information in the RADIUS Access-Request to search its user database. If a matching entry is found, the server uses a randomly generated challenge (EAP-Request/MD5 challenge) to encrypt the password in the entry, and sends the challenge in a RADIUS Access-Challenge packet to the network access device.
6. The network access device relays the EAP-Request/MD5 Challenge packet in a RADIUS Access-Request packet to the client.
7. The client uses the received challenge to encrypt the password, and sends the encrypted password in an EAP-Response/MD5 Challenge packet to the network access device.
8. The network access device relays the EAP-Response/MD5 Challenge packet in a RADIUS Access-Request packet to the authentication server.

9. The authentication server compares the received encrypted password with the one it generated at step 5. If the two are identical, the authentication server considers the client valid and sends a RADIUS Access-Accept packet to the network access device.
10. Upon receiving the RADIUS Access-Accept packet, the network access device sends an EAP-Success packet to the client, and sets the controlled port in the authorized state so the client can access the network.
11. After the client comes online, the network access device periodically sends handshake requests to check whether the client is still online. By default, if two consecutive handshake attempts fail, the device logs off the client.
12. Upon receiving a handshake request, the client returns a response. If the client fails to return a response after a certain number of consecutive handshake attempts (two by default), the network access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users that have abnormally gone offline.
13. The client can also send an EAPOL-Logoff packet to ask the network access device for a logoff.
14. In response to the EAPOL-Logoff packet, the network access device changes the status of the controlled port from authorized to unauthorized and sends an EAP-Failure packet to the client.

EAP termination

Figure 323 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 323 802.1X authentication procedure in EAP termination mode



In EAP termination mode, it is the network access device rather than the authentication server generates an MD5 challenge for password encryption (see Step 4). The network access device then sends the MD5 challenge together with the username and encrypted password in a standard RADIUS packet to the RADIUS server.

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 properly.

- **Username request timeout timer**—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device receives no response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.
- **Client timeout timer**—Starts when the access device sends an EAP-Request/MD5 Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Server timeout timer**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.

- **Handshake timer**—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device receives no response after sending the maximum number of handshake requests, it considers that the client has logged off.
- **Quiet timer**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.
- **Periodic online user re-authentication timer**—Sets the interval at which the network device periodically re-authenticates online 802.1X users. The change to the periodic re-authentication timer applies to the users that have been online only after the old timer expires.

Using 802.1X authentication with other features

VLAN assignment

You can configure the authentication server to assign a VLAN for an 802.1X user that has passed authentication. The way that the network access device handles VLANs on an 802.1X-enabled port differs by 802.1X access control mode.

Access control	VLAN manipulation
Port-based	Assigns the VLAN to the port as the port VLAN (PVID). The authenticated 802.1X user and all subsequent 802.1X users can access the VLAN without authentication. When the user logs off, the previous PVID restores, and all other online users are logged off.
MAC-based	If the port is an access, trunk, or hybrid port, assigns the first authenticated user's VLAN to the port as the PVID. If a different VLAN is assigned to a subsequent user, the user cannot pass the authentication. To avoid the authentication failure of subsequent users, be sure to assign the same VLAN to all 802.1X users on these ports.

NOTE:

With 802.1X authentication, a hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not re-configure the port as a tagged member in the VLAN.

Guest VLAN

You can configure a guest VLAN on a port to accommodate users that have not performed 802.1X authentication, so they can access a limited set of network resources, such as a software server, to download anti-virus software and system patches. After a user in the guest VLAN passes 802.1X authentication, it is removed from the guest VLAN and can access authorized network resources.

The network device supports guest VLAN only on the port that performs port-based access control. The Following describes the way how the network access device handles VLANs on such port

Authentication status	VLAN manipulation
No 802.1X user has performed authentication within 90 seconds after 802.1X is enabled	Assigns the 802.1X guest VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the guest VLAN. If no 802.1X guest VLAN is configured, the access device does not perform any VLAN operation.
A user in the 802.1X guest VLAN fails 802.1X authentication	If an 802.1X Auth-Fail VLAN (see "Auth-Fail VLAN") is available, assigns the Auth-Fail VLAN to the port as the PVID. All users on this port can access only resources in the Auth-Fail VLAN. If no Auth-Fail VLAN is configured, the PVID on the port is still the 802.1X guest VLAN. All users on the port are in the guest VLAN.
A user in the 802.1X guest VLAN passes 802.1X authentication	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the 802.1X guest VLAN. After the user logs off, the user configured PVID restores. • If the authentication server assigns no VLAN, the user-configured PVID applies. The user and all subsequent 802.1X users are assigned to the user-configured port VLAN. After the user logs off, the port VLAN remains unchanged.

NOTE:

The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member.

Auth-Fail VLAN

You can configure an Auth-Fail VLAN to accommodate users that have failed 802.1X authentication because of the failure to comply with the organization security strategy, such as using a wrong password. Users in the Auth-Fail VLAN can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

The Auth-Fail VLAN does not accommodate 802.1X users that have failed authentication for authentication timeouts or network connection problems.

The network device supports Auth-Fail VLAN only on the port that performs port-based access control. The Following describes the way how the network access device handles VLANs on such port.

Authentication status	VLAN manipulation
A user fails 802.1X authentication	Assigns the Auth-Fail VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the Auth-Fail VLAN.
A user in the Auth-Fail VLAN fails 802.1X re-authentication	The Auth-Fail VLAN is still the PVID on the port, and all 802.1X users on this port are in this VLAN.
A user passes 802.1X authentication	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the Auth-Fail VLAN. After the user logs off, the user-configured PVID restores. • If the authentication server assigns no VLAN, the initial PVID applies. The user and all subsequent 802.1X users are assigned to the user-configured PVID. After the user logs off, the PVID remains unchanged.

NOTE:

The network device assigns a hybrid port to an 802.1X Auth-Fail VLAN as an untagged member.

ACL assignment

You can specify an ACL for an 802.1X user to control its access to network resources. After the user passes 802.1X authentication, the authentication server, either the local access device or a RADIUS server, assigns the ACL to the port to filter the traffic from this user. In either case, you must configure the ACL on the access device. You can change ACL rules while the user is online.

Configuration prerequisites

- Configure an ISP domain and AAA scheme (local or RADIUS authentication) for 802.1X users. For more information, see "Configuring AAA" and "Configuring RADIUS."
- If RADIUS authentication is used, create user accounts on the RADIUS server.
- If local authentication is used, create local user accounts on the access device and specify the LAN access service for the user accounts. For more information, see "Configuring users and user groups."

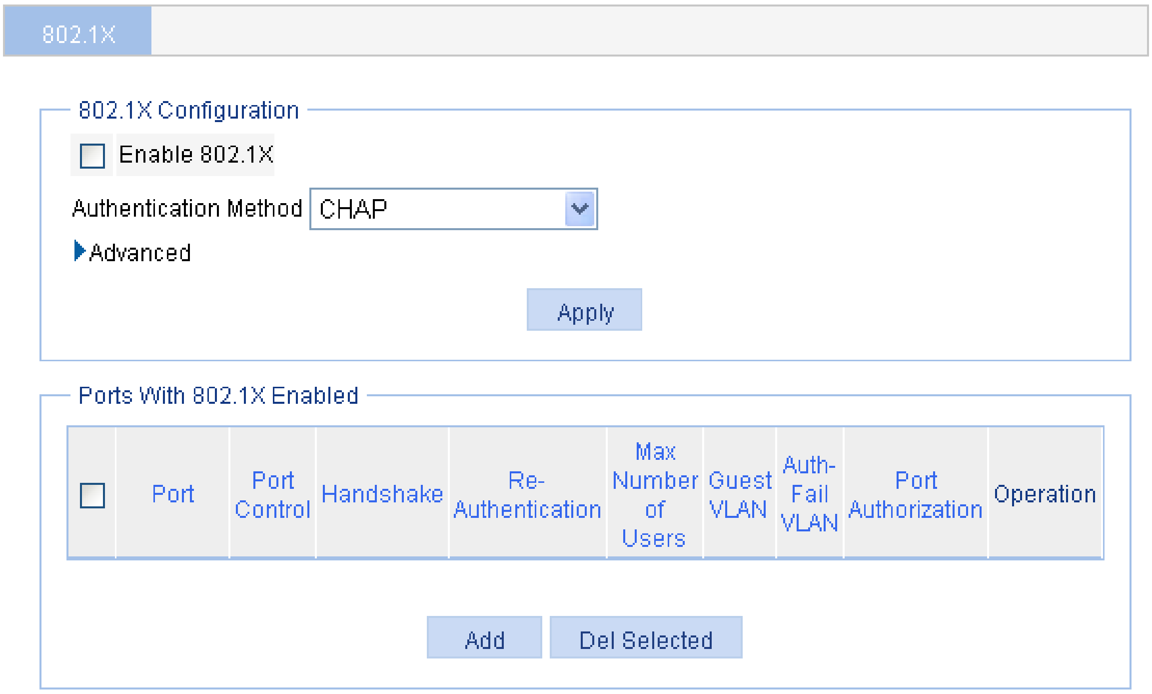
Recommended configuration procedure

Step	Description
1. 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.
2. Configuring 802.1X on a port	Required. Enable 802.1X authentication on the specified port and configure 802.1X parameters for the port. By default, 802.1X authentication is disabled on a port.

Configuring 802.1X globally

1. From the navigation tree, select **Authentication** > **802.1X**.

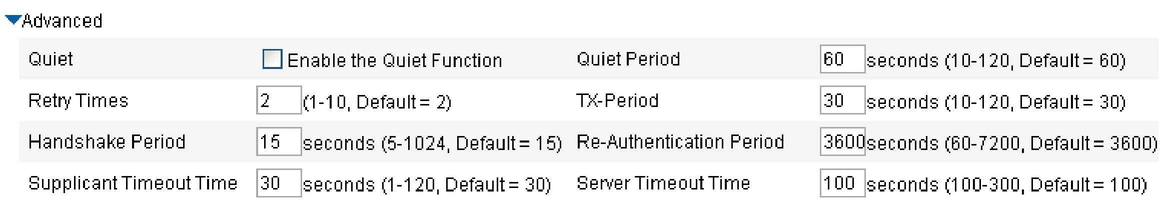
Figure 324 802.1X global configuration



2. In the **802.1X Configuration** area, select the **Enable 802.1X** box.
3. Select an authentication method. Options include CHAP, PAP, and EAP. For more information about EAP relay and EAP termination, see "A comparison of EAP relay and EAP termination."
    - **CHAP**—Sets the access device to perform EAP termination and use the CHAP to communicate with the RADIUS server.
    - **PAP**—Sets the access device to perform EAP termination and use the PAP to communicate with the RADIUS server.
    - **EAP**—Sets the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.
4. Click **Advanced**.

   The advanced 802.1X configuration area is expanded, as shown in Figure 325.

Figure 325 802.1X configuration page



5. Configure advanced 802.1X settings as described in Table 105. For more information about 802.1X timers, see "802.1X timers."
6. Click **Apply**.

Table 105 Configuration items

Item	Description
Quiet	Specify whether to enable the quiet timer. The quiet timer enables the network access device to wait a period of time defined by the **Quiet Period** option before it can process any authentication request from a client that has failed an 802.1X authentication.
Quiet Period	Set the value of the quiet timer.
Retry Times	Set the maximum number of authentication request attempts. The network access device retransmits an authentication request if it receives no response to the request it has sent to the client within a period of time (specified by using the **TX Period** option or the **Supplicant Timeout Time** option). The network access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.
TX-Period	Set the username request timeout timer.
Handshake Period	Set the handshake timer. For information about how to enable the online user handshake function, see "Configuring 802.1X on a port."
Re-Authentication Period	Set the periodic online user re-authentication timer. For information about how to enable periodic online user re-authentication on a port, see "Configuring 802.1X on a port."
Supplicant Timeout Time	Set the client timeout timer.
Server Timeout Time	Set the server timeout timer.

NOTE:

You can set the client timeout timer to a high value in a low-performance network, and adjust the server timeout timer to adapt to the performance of different authentication servers. In most cases, the default settings are sufficient.

Configuring 802.1X on a port

Configuration guidelines

- 802.1X configuration on a specific port can take effect only after global 802.1X and port-specific 802.1X are enabled.
- If the PVID of a port is a voice VLAN, the 802.1X function cannot take effect on the port.
- 802.1X is mutually exclusive with link aggregation and service loopback group configuration on a port.

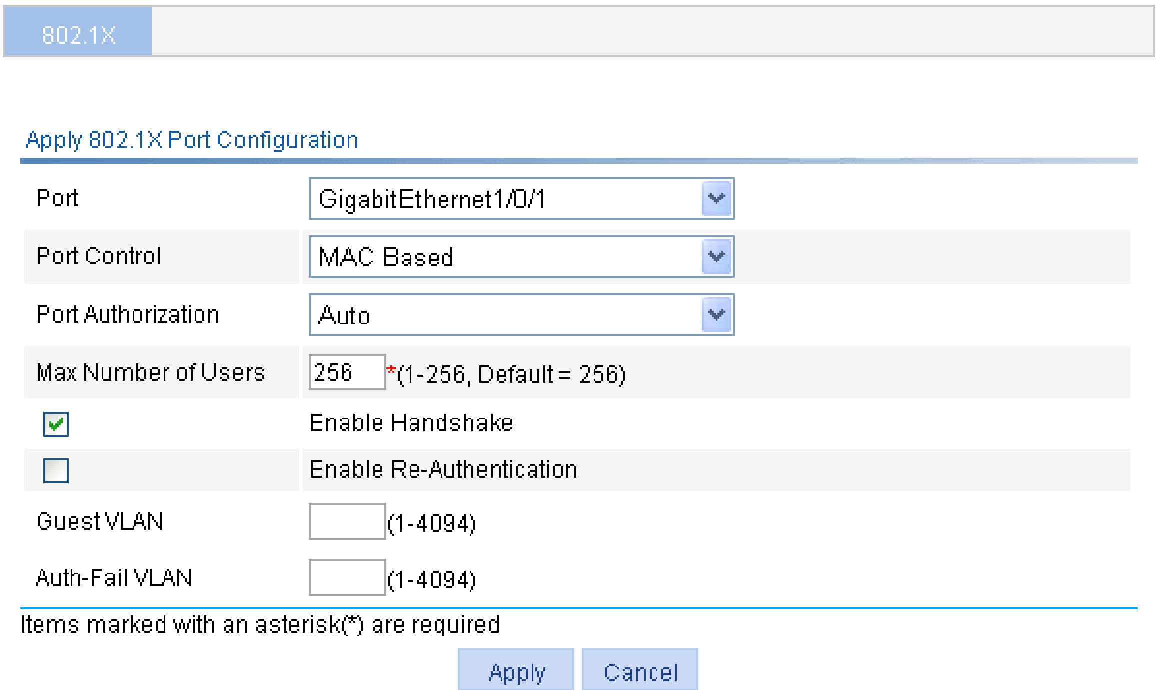
Configuration procedure

1. From the navigation tree, select **Authentication** > **802.1X** to enter the 802.1X configuration page, as shown in Figure 324.

   The **Ports With 802.1X Enabled** area displays the port-specific 802.1X configuration.

2. In the **Ports With 802.1X Enabled** area, click **Add**.

Figure 326 802.1X configuration on a port



3. Configure the 802.1X feature on a port as described in Table 106.
4. Click **Apply**.

Table 106 Configuration items

Item	Description
Port	Select a port where you want to enable 802.1X. Only 802.1X-disabled ports are available.
Port Control	Select an access control method for the port, which can be **MAC Based** or **Port Based**.
Port Authorization	Select the 802.1X authorization mode for the port. Options include: • **Auto**—Places the specified or all ports initially in the unauthorized state to allow only EAPOL packets to pass, and after a user passes authentication, sets the port in the authorized state to allow access to the network. You can use this option in most scenarios. • **Force-Authorized**—Places the specified or all ports in the authorized state, enabling users on the ports to access the network without authentication. • **Force-Unauthorized**—Places the specified or all ports in the unauthorized state, denying any access requests from users on the ports.
Max Number of Users	Set the maximum number of concurrent 802.1X users on the port.

Item	Description
Enable Handshake	Select the box to enable the online user handshake function. The online user handshake function checks the connectivity status of online 802.1X users. The network access device sends handshake messages to online users at the interval specified by the **Handshake Period** option. If no response is received from an online user after the maximum number of handshake attempts (set by the **Retry Times** option) has been made, the network access device sets the user in the offline state. For information about the timers, see Table 105.
Enable Re-Authentication	Select the box to enable periodic online user re-authentication on the port. Periodic online user re-authentication tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL, and VLAN. The re-authentication interval is specified by the **Re-Authentication Period** option in Table 105.
Guest VLAN	Specify an existing VLAN as the guest VLAN. For more information, see "Configuring an 802.1X guest VLAN."
Auth-Fail VLAN	Specify an existing VLAN as the Auth-Fail VLAN to accommodate users that have failed 802.1X authentication. For more information, see "Configuring an Auth-Fail VLAN."

Configuring an 802.1X guest VLAN

Configuration prerequisites

- Create the VLAN to be specified as the 802.1X guest VLAN.
- On the 802.1X-enabled port that performs port-based access control, enable 802.1X multicast trigger at the command line interface. (802.1X multicast trigger is enabled by default.)

Configuration guidelines

- You can configure only one 802.1X guest VLAN on a port. The 802.1X guest VLANs on different ports can be different.
- Assign different IDs to the voice VLAN, the PVID, and the 802.1X guest VLAN on a port, so the port can correctly process incoming VLAN tagged traffic.
- With 802.1X authentication, a hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not re-configure the port as a tagged member in the VLAN.

Configuring an Auth-Fail VLAN

Configuration prerequisites

- Create the VLAN to be specified as the 802.1X Auth-Fail VLAN.
- On the 802.1X-enabled port that performs port-based access control, enable 802.1X multicast trigger. (802.1X multicast trigger is enabled by default.)

Configuration guidelines

Assign different IDs to the voice VLAN, PVID and the 802.1X Auth-Fail VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.

Configuration examples

802.1X configuration example

Network requirements

As shown in Figure 327, the access device performs 802.1X authentication for users that connect to port GigabitEthernet 1/0/1. Implement MAC-based access control on the port, so the logoff of one user does not affect other online 802.1X users. Enable periodic re-authentication of online users on the port, so that the server can periodically update the authorization information of the users.

Use RADIUS servers to perform authentication, authorization, and accounting for the 802.1X users. If RADIUS accounting fails, the access device logs the user off. The RADIUS servers run CAMS or IMC.

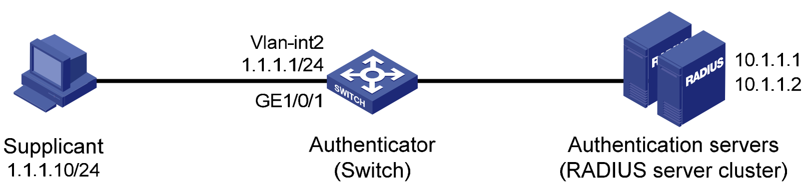
Configure the host at 10.1.1.1 as the primary authentication and secondary accounting servers, and the host at 10.1.1.2 as the secondary authentication and primary accounting servers. Assign all users to the ISP domain **test**.

Configure the shared key as **name** for packets between the access device and the authentication server, and the shared key as **money** for packets between the access device and the accounting server.

Exclude the ISP domain name from the username sent to the RADIUS servers.

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.

Figure 327 Network diagram



The following configuration procedure covers RADIUS client configuration on the switch, and configurations on the RADIUS servers are not shown. For more information about RADIUS configuration, see "Configuring RADIUS."

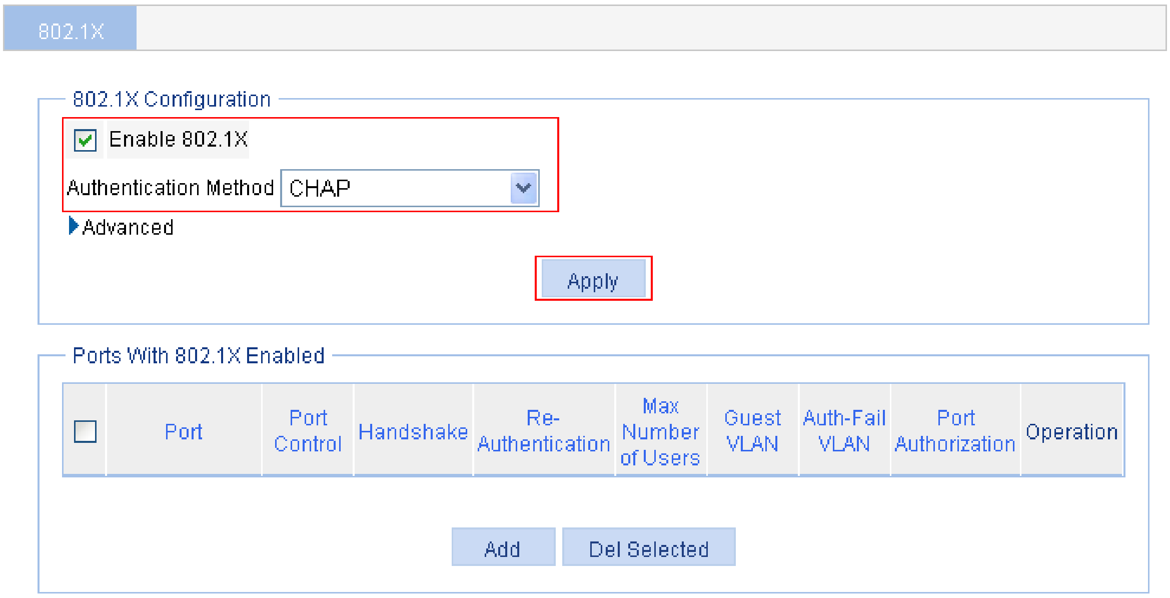
Configuring the IP addresses of the interfaces

Details not shown.

Configuring 802.1X

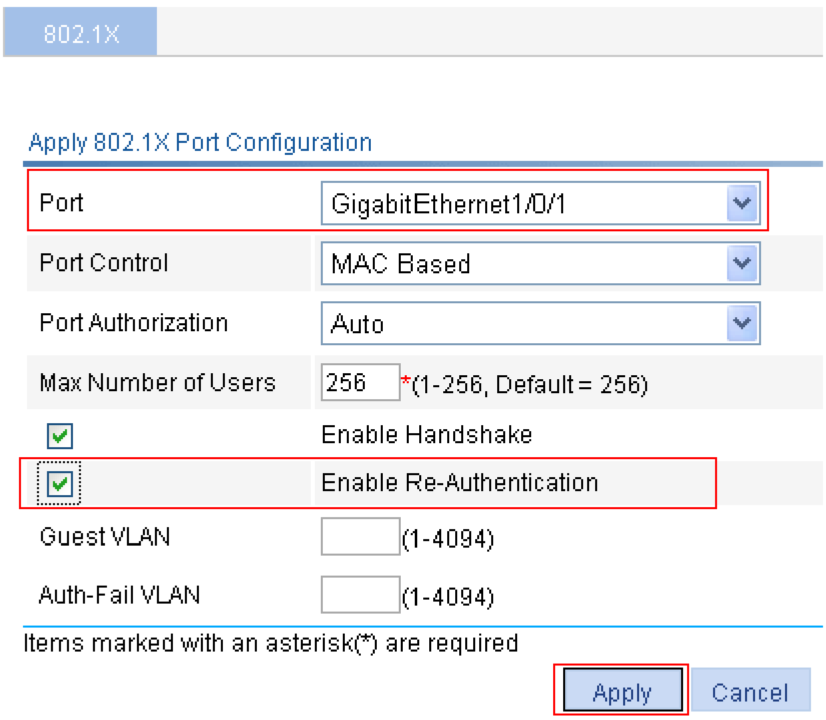
1. From the navigation tree, select **Authentication** > **802.1X**.
2. Select the **Enable 802.1X** box, select the authentication method as **CHAP**, and click **Apply**.

Figure 328 Global 802.1X configuration



3. In the **Ports With 802.1X Enabled** area, click **Add**.
4. Select **GigabitEthernet1/0/1** from the **Port** list.
5. Select the **Enable Re-Authentication** box, and click **Apply**.

Figure 329 802.1X configuration of GigabitEthernet 1/0/1



Configuring a RADIUS scheme

1. From the navigation tree, select **Authentication** > **RADIUS.**
   The RADIUS server configuration page appears.
2. Configure the RADIUS primary and secondary authentication servers:

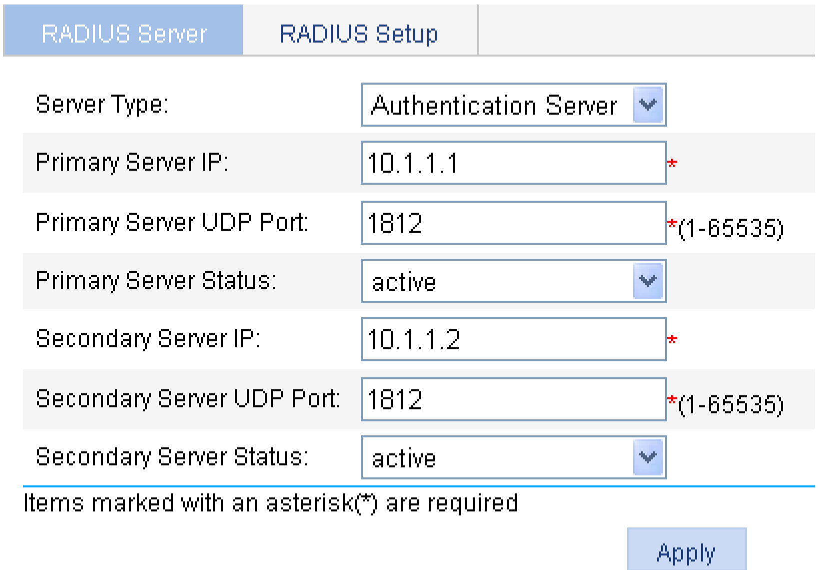
a. Select the server type **Authentication Server**.

b. Enter the IP address **10.1.1.1**, enter the port number **1812**, and select the primary server status **active**.

c. Enter the IP address **10.1.1.2**, enter the port number **1813**, and select the secondary server status **active**.

d. Click **Apply**.

Figure 330 Configuring the RADIUS authentication servers



3. Click the **RADIUS Setup** tab.
4. Configure a RADIUS scheme:

a. Select the server type **extended**.

b. Select the **Authentication Server Shared Key** box, enter **name** in the field next to the box and the **Confirm Authentication Shared Key** field.

c. Select the **Accounting Server Shared Key** box, enter **name** in the field next to the box and the **Confirm Accounting Shared Key** field.

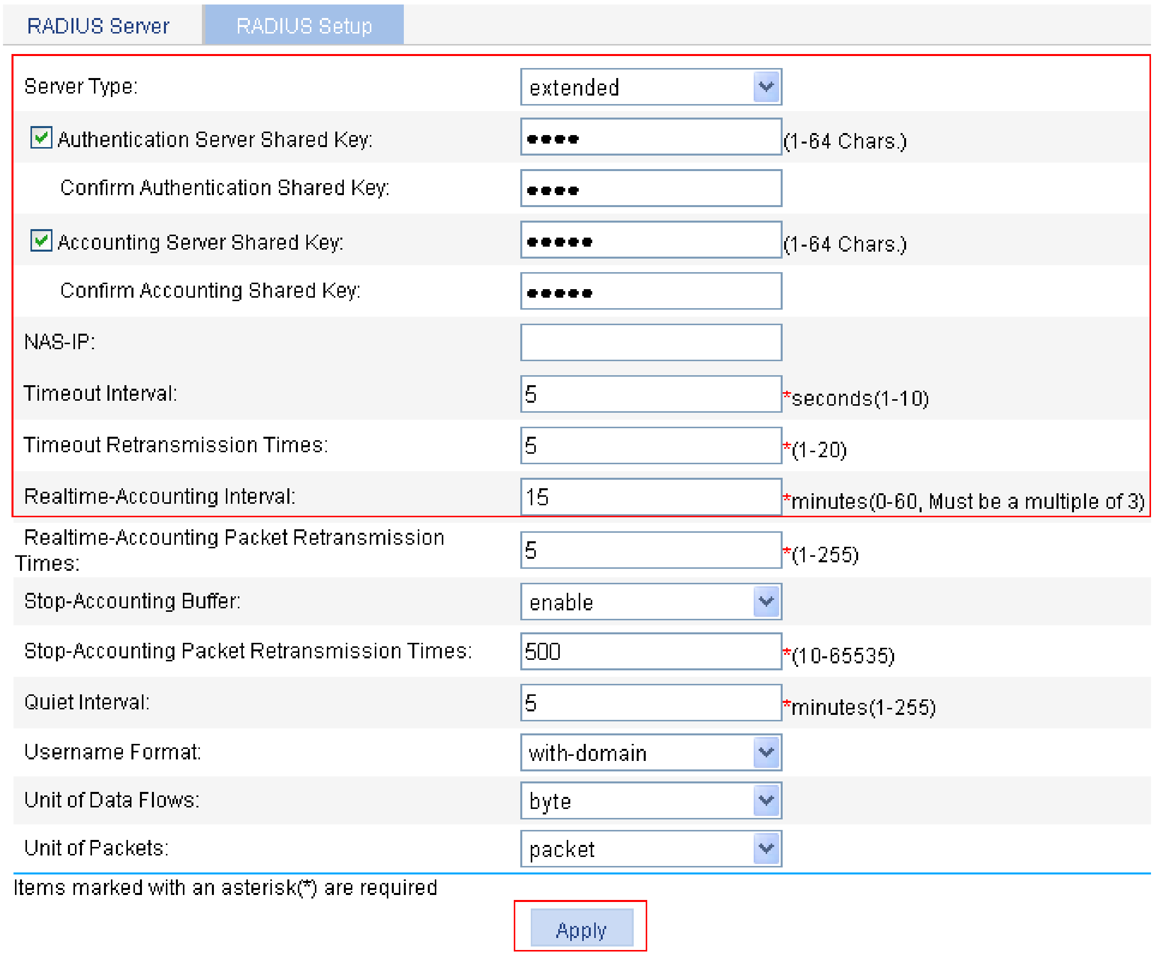
d. Enter **5** as the server timeout timer.

e. Enter **5** as the maximum number of request transmission attempts.

f. Enter **15** as the realtime accounting interval.

g. Click **Apply**.

Figure 331 Configuring a RADIUS scheme



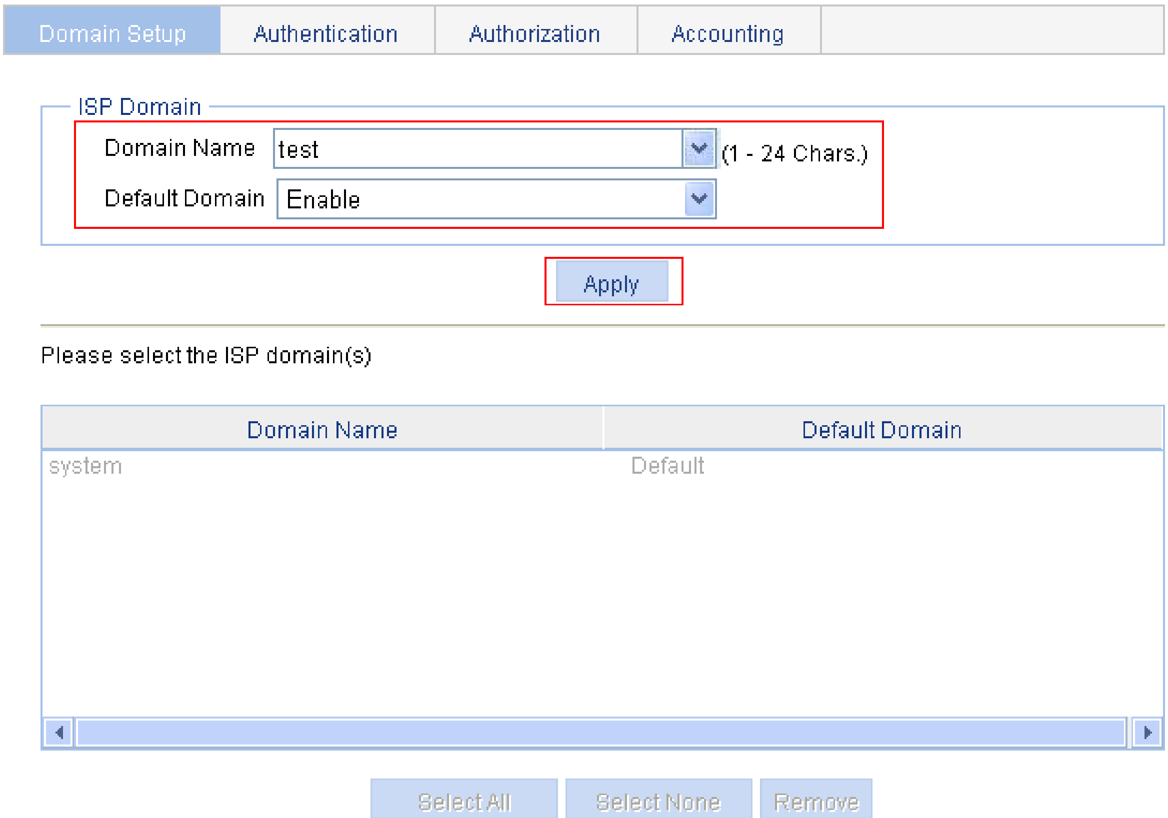
Configuring AAA

1. From the navigation tree, select **Authentication** > **AAA**.

   The domain setup page appears.

2. Enter **test** in the **Domain Name** field, and select **Enable** from the **Default Domain** list.
3. Click **Apply**.

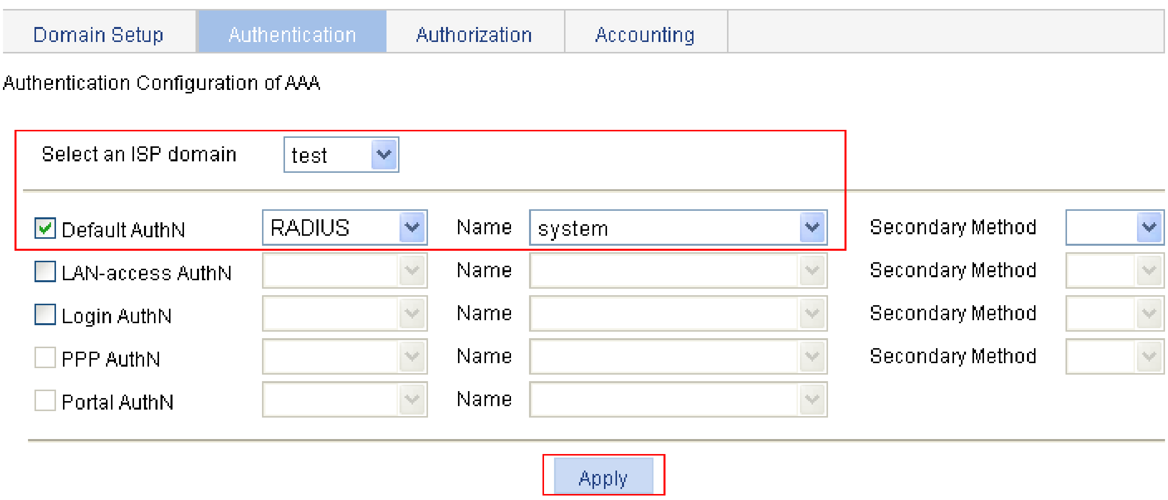
Figure 332 Creating an ISP domain



4. On the **Authentication** tab, select the ISP domain **test**, select the **Default AuthN** box, select the authentication method **RADIUS**, select the authentication scheme **system** from the **Name** list, and click **Apply**.

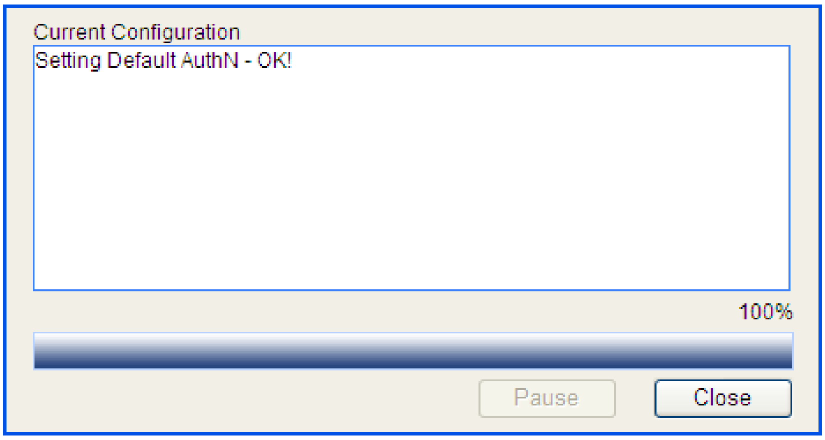
   A configuration progress dialog box appears, as shown in Figure 334.

Figure 333 Configuring the AAA authentication method for the ISP domain



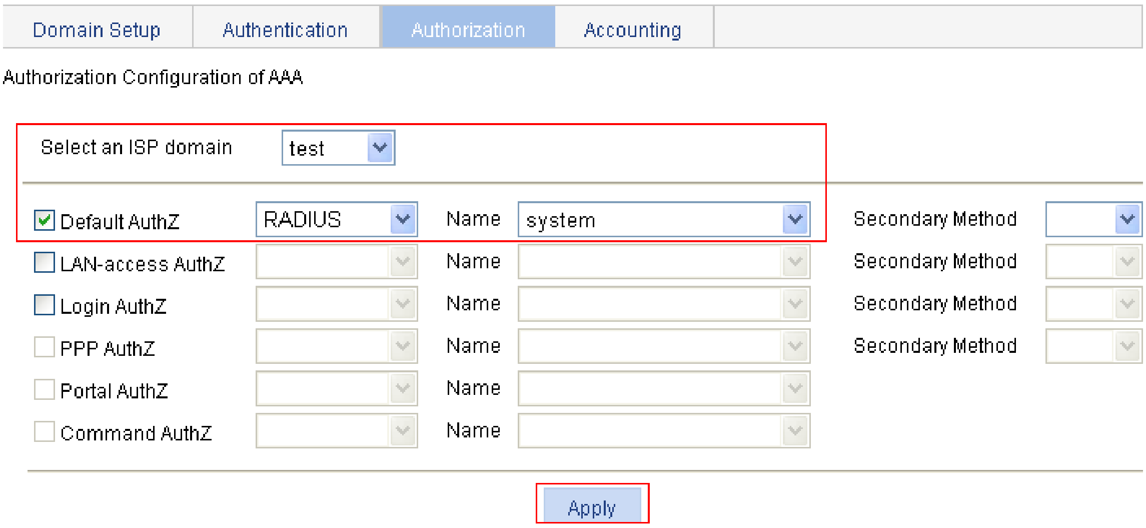
5. After the configuration process is complete, click **Close**.

Figure 334 Configuration progress dialog box



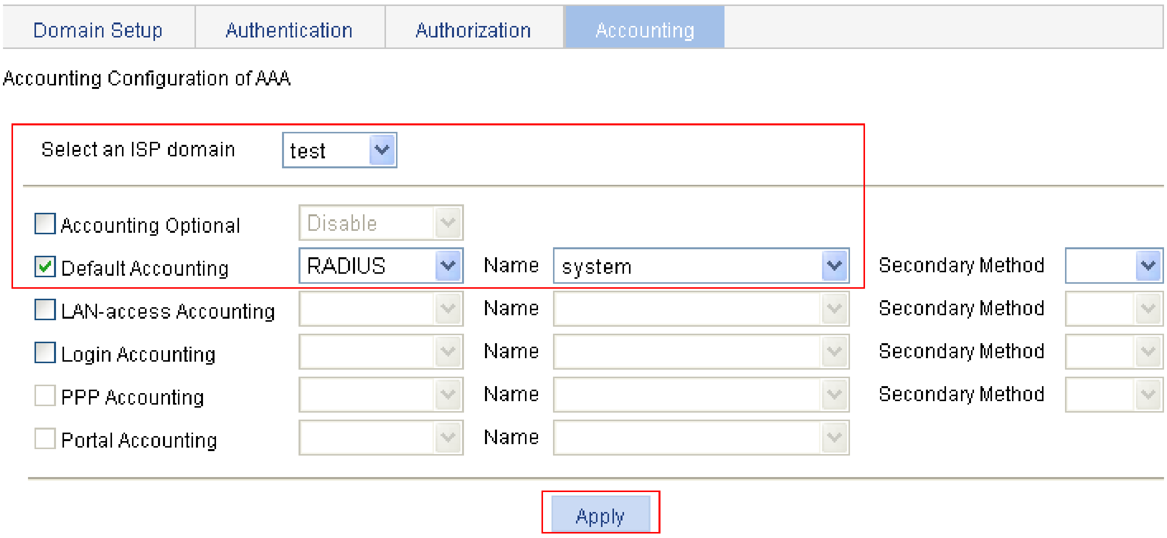
6. On the **Authorization** tab, select the ISP domain **test**, select the **Default AuthZ** box, select the authorization method **RADIUS**, select the authorization scheme **system** from the **Name** list, and click **Apply**.
7. After the configuration process is complete, click **Close**.

Figure 335 Configuring the AAA authorization method for the ISP domain



8. On the **Accounting** tab, select the domain name **test**, select the **Default Accounting** box, select the accounting method **RADIUS**, select the accounting scheme **system** from the **Name** list, and click **Apply**.
9. After the configuration process is complete, click **Close**.

Figure 336 Configuring the AAA accounting method for the ISP domain



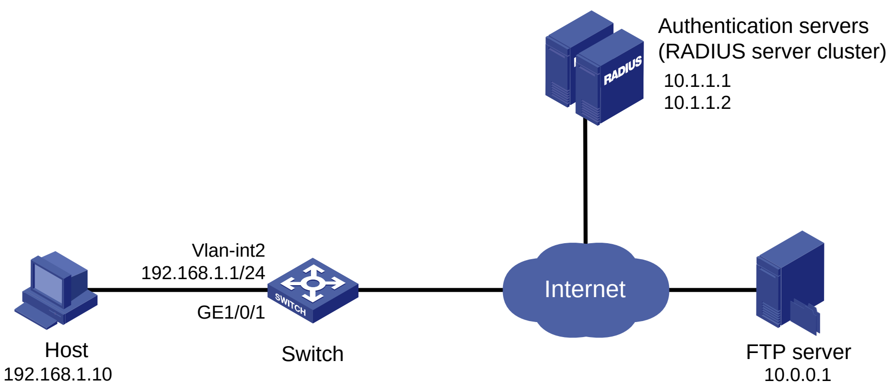
ACL assignment configuration example

Network requirements

As shown in Figure 337, the host at 192.168.1.10 connects to port GigabitEthernet 1/0/1 of the network access device.

Perform 802.1X authentication on the port. Use the RADIUS server at 10.1.1.1 as the authentication and authorization server and the RADIUS server at 10.1.1.2 as the accounting server. Assign an ACL to GigabitEthernet 1/0/1 to deny the access of 802.1X users to the FTP server at 10.0.0.1/24.

Figure 337 Network diagram



Configuring the IP addresses of the interfaces

Details are not shown.

Configuring a RADIUS scheme

1. From the navigation tree, select **Authentication** > **RADIUS**.

   The RADIUS server configuration page appears.

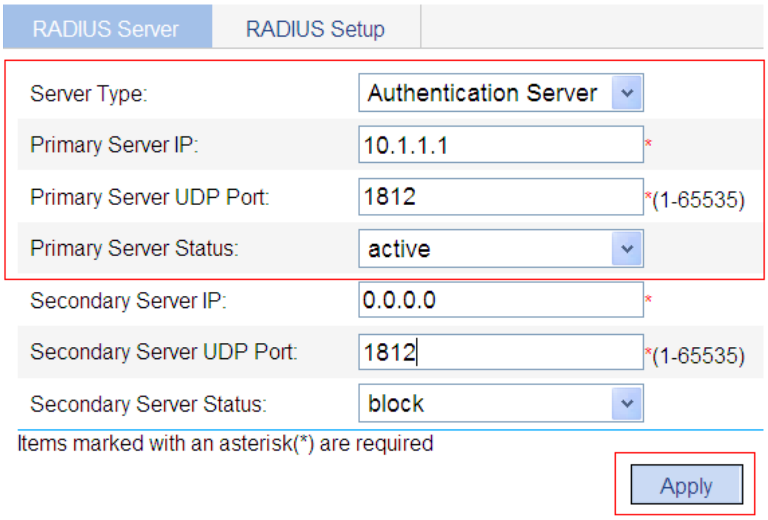
2. Configure the RADIUS primary authentication server:

   a. Select the server type **Authentication Server**.

b. Enter the IP address **10.1.1.1**, enter the port number **1812**, and select the primary server status **active**.

c. Click **Apply**.

Figure 338 Configuring the RADIUS primary authentication server



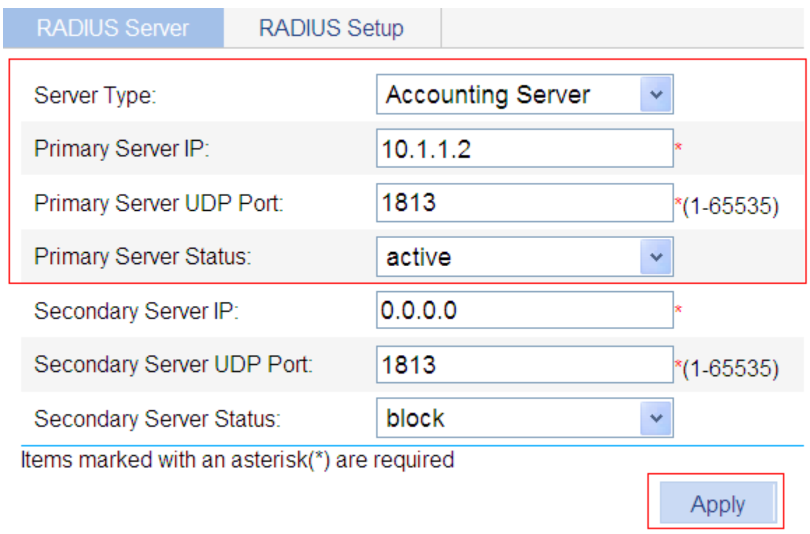
3. Configure the RADIUS primary accounting server:

   a. Select the server type **Accounting Server**.

   b. Enter the IP address **10.1.1.2**, enter the port number **1813**, and select the primary server status **active**.

   c. Click **Apply**.

Figure 339 Configuring the RADIUS primary accounting server



4. Click the **RADIUS Setup** tab.

5. Configure a RADIUS scheme:

   a. Select the server type **extended**.

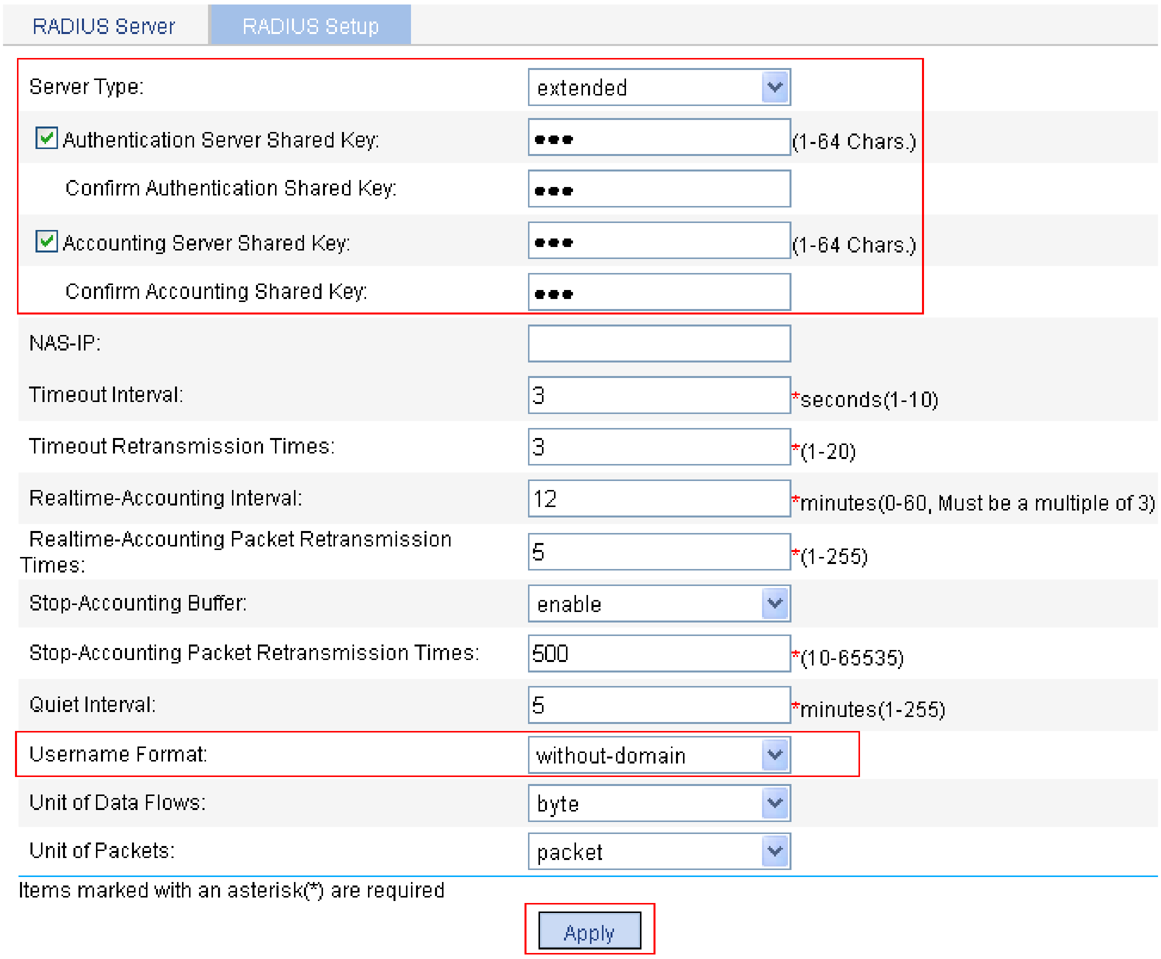
   b. Select the **Authentication Server Shared Key** box, enter **abc** in the field next to the box and the **Confirm Authentication Shared Key** field.

c. Select the **Accounting Server Shared Key** box, enter **abc** in the field next to the box and the **Confirm Accounting Shared Key** field.

d. Select **with-domain** from the **Username Format** list.

e. Click **Apply**.

Figure 340 Configuring a RADIUS scheme



Configuring AAA

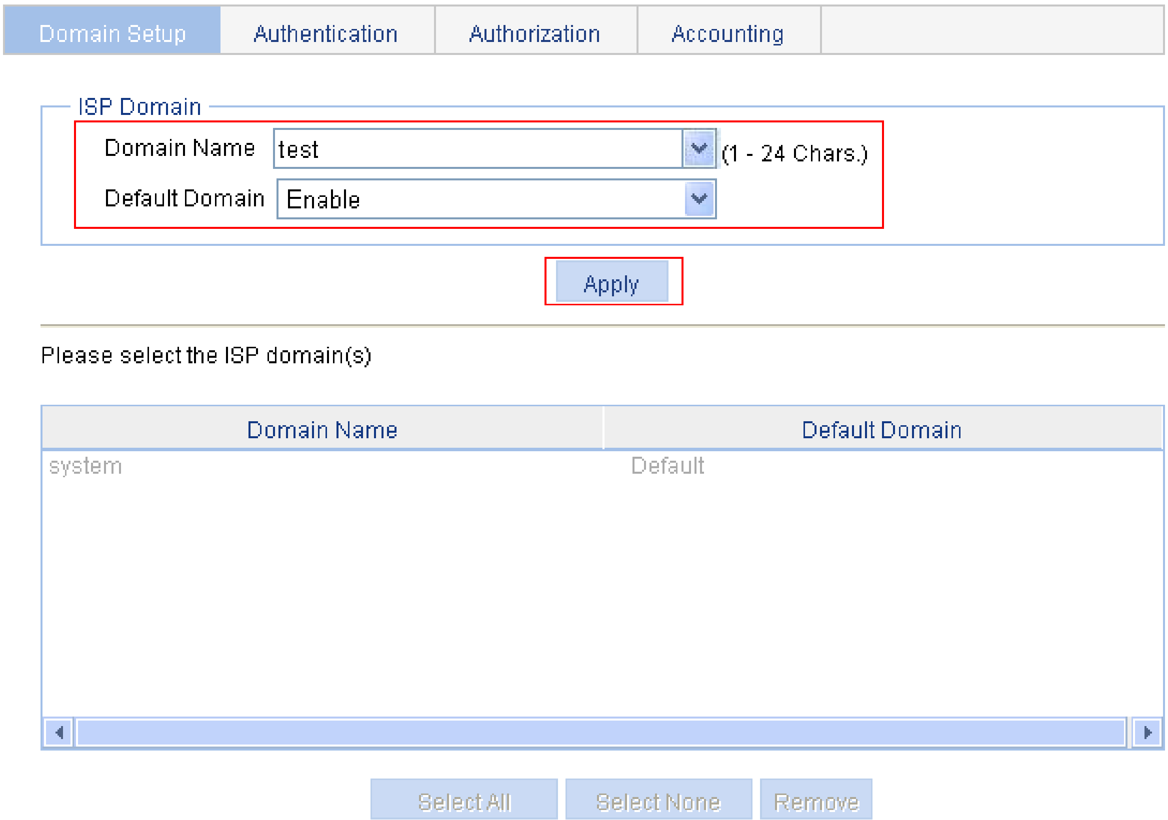
1. From the navigation tree, select **Authentication** > **AAA**.

   The domain setup page appears.

2. Enter **test** in the **Domain Name** field, and select **Enable** from use **Default Domain** list.

3. Click **Apply**.

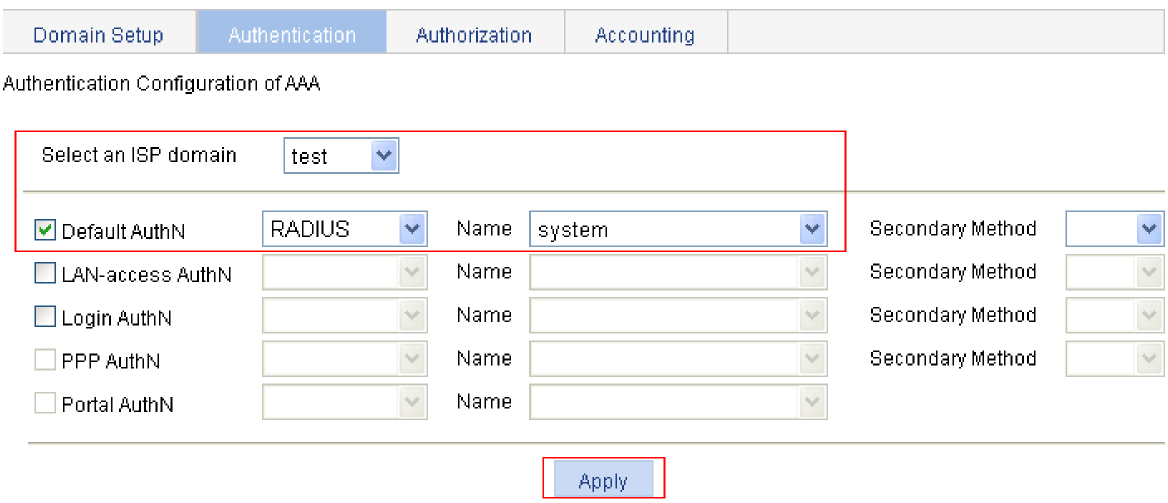
Figure 341 Creating an ISP domain



4. On the **Authentication** tab, select the ISP domain **test**, select the **Default AuthN** box, select the authentication method **RADIUS** as mode, select the authentication scheme **system** from the **Name** list, and click **Apply**.

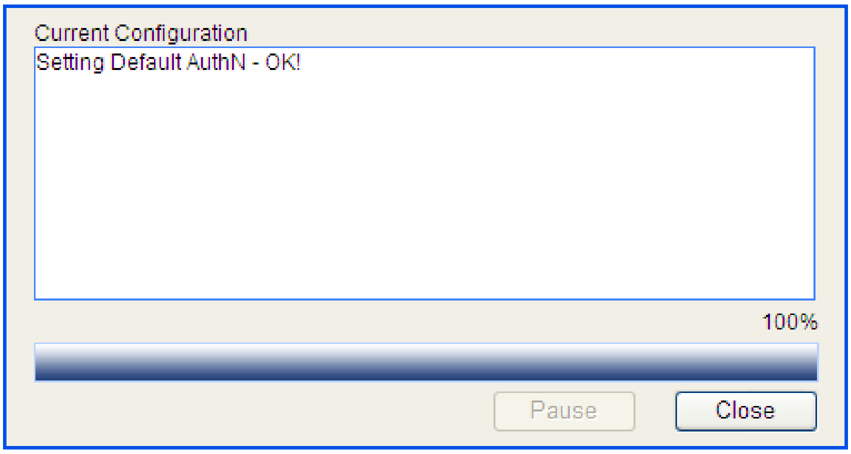
   A configuration progress dialog box appears, as shown in Figure 343.

Figure 342 Configuring the AAA authentication method for the ISP domain



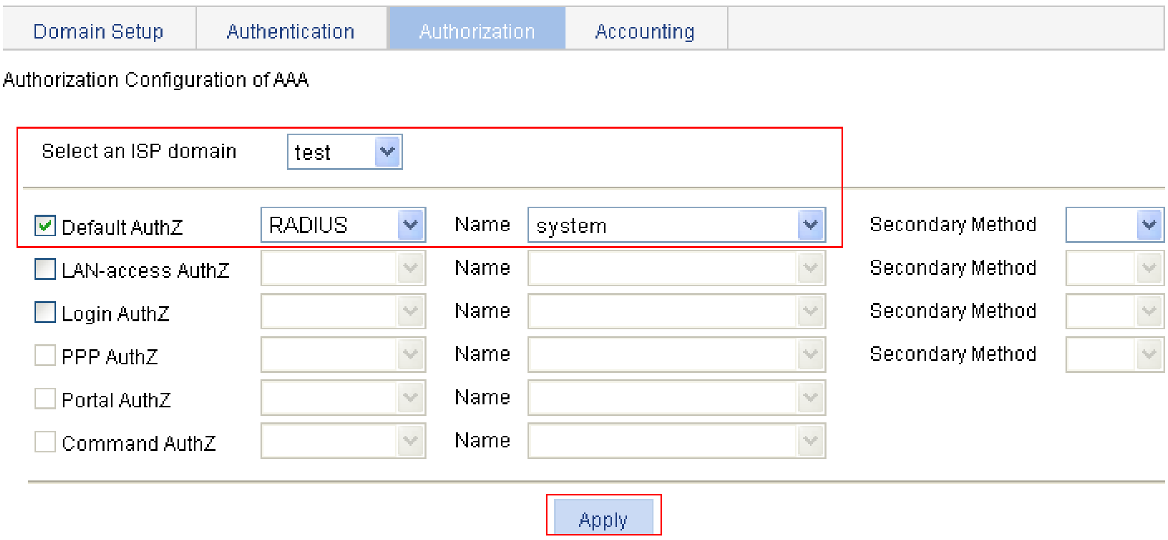
5. After the configuration process is complete, click **Close**.

Figure 343 Configuration progress dialog box



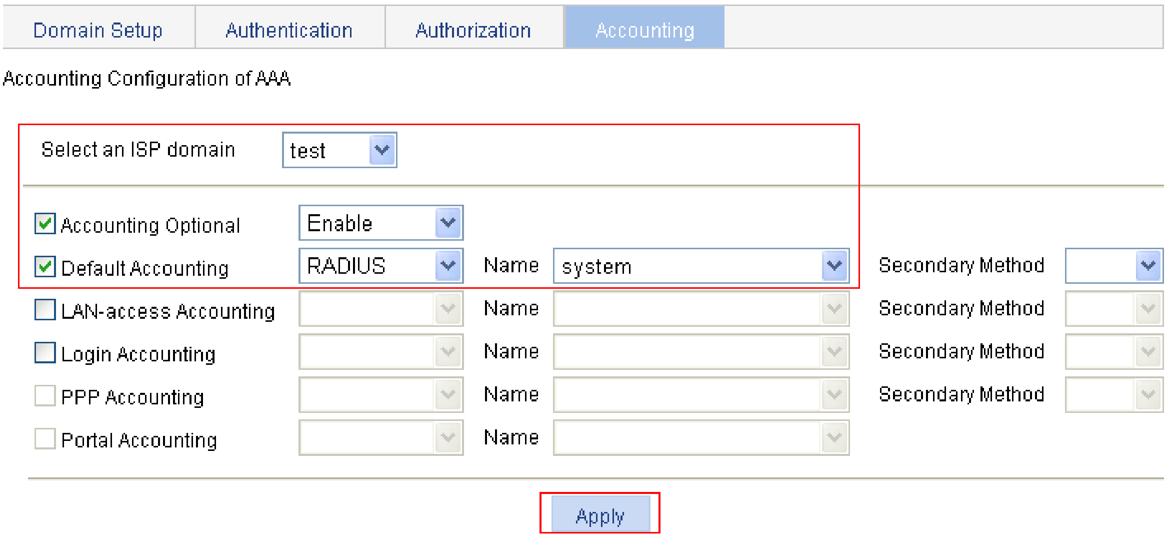
6. On the **Authorization** tab, select the ISP domain **test**, Select the **Default AuthZ** box, select the authorization method **RADIUS**, select the authorization scheme **system** from the **Name** list, and click **Apply**.
7. After the configuration process is complete, click **Close**.

Figure 344 Configuring the AAA authorization method for the ISP domain



8. On the **Accounting** tab, select the domain name **test**, select the **Accounting Optional** box, select **Enable** from the list, select the **Default Accounting** box, select the accounting method **RADIUS**, select the accounting scheme **system** from the **Name** list, and click **Apply**.
9. After the configuration process is complete, click **Close**.

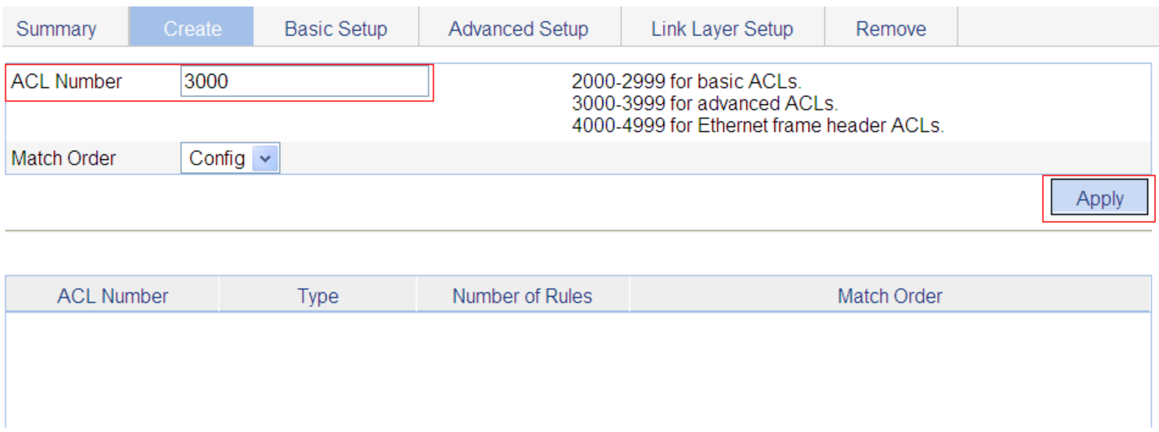
Figure 345 Configuring the AAA accounting method for the ISP domain



Configuring an ACL

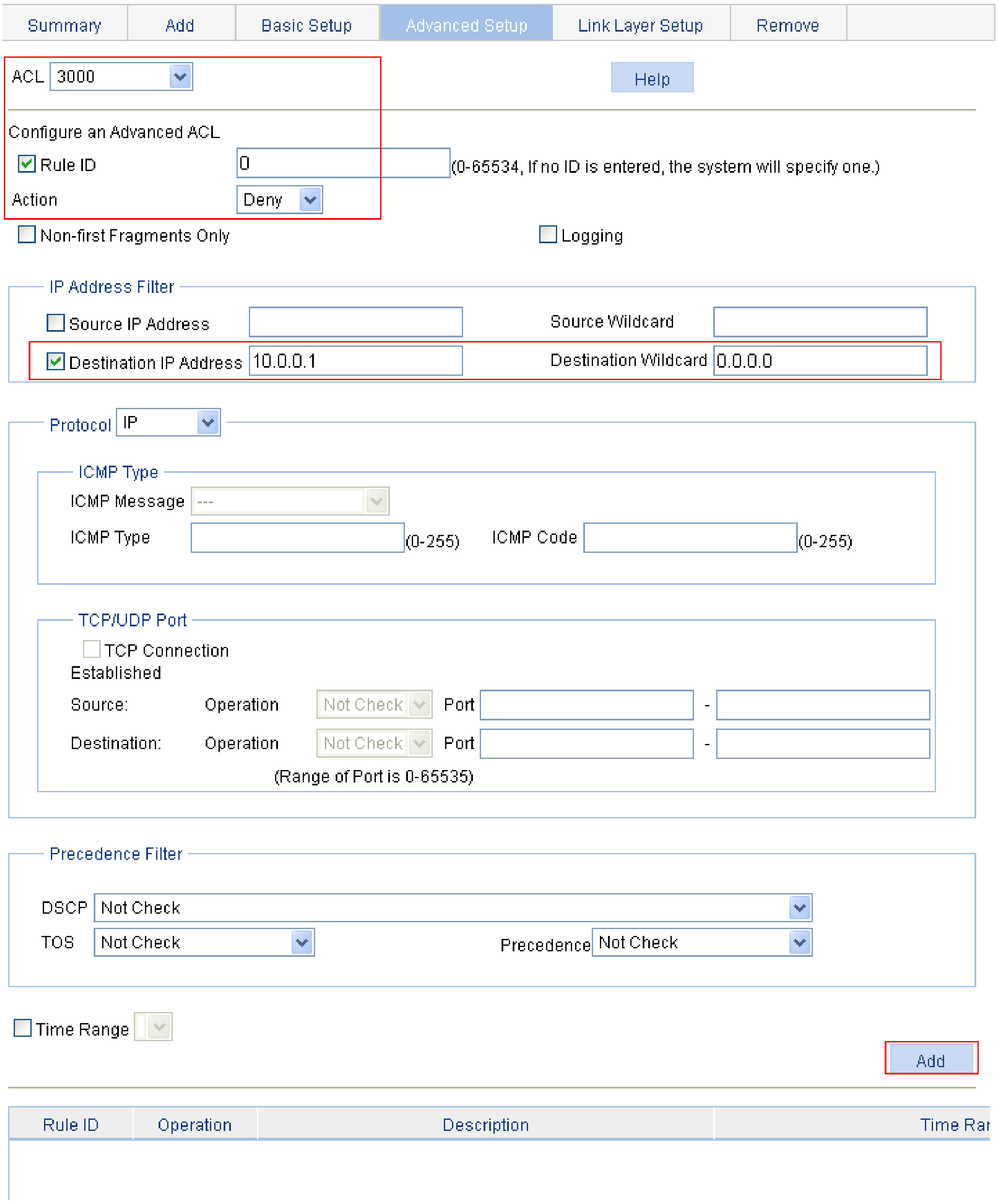
1. From the navigation tree, select **QoS** > **ACL IPv4**.
2. On the **Add** tab, enter the ACL number **3000**, and click **Apply**.

Figure 346 Creating ACL 3000



3. On the **Advanced Setup** tab, configure an ACL rule:
   a. Select **3000** from the **ACL** list.
   b. Select the **Rule ID** box, enter the rule ID **0**, and select the action **Deny**.
   c. In the **IP Address Filter** area, select the **Destination IP Address** box, enter **10.0.0.1** in the field, and enter **0.0.0.0** in the **Destination Wildcard** field.
   d. Click **Add**.

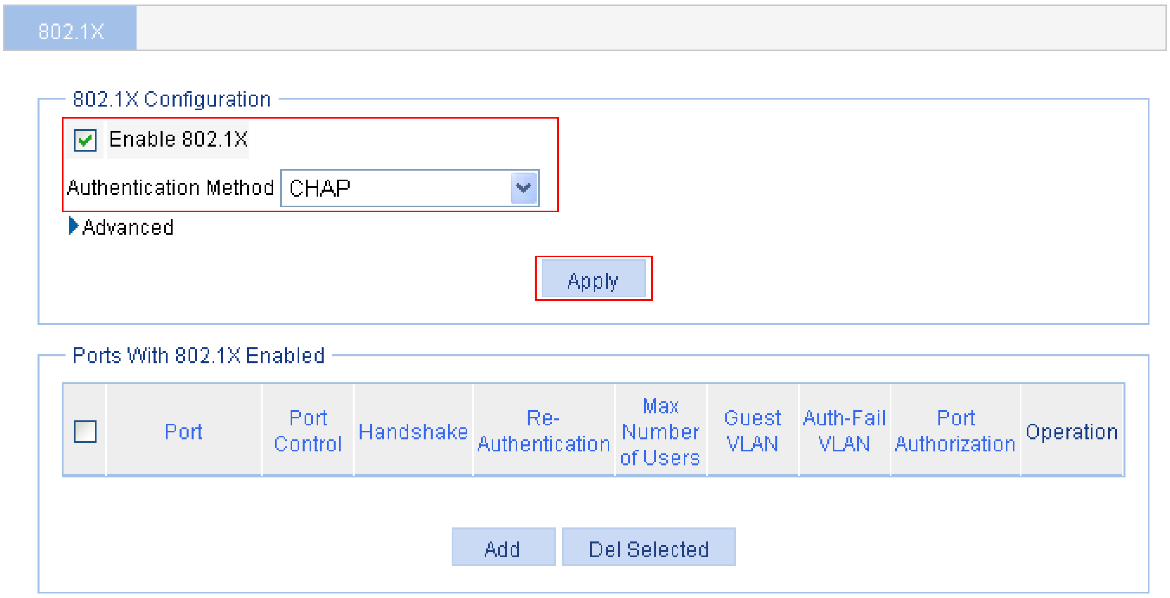
Figure 347 ACL rule configuration



Configuring the 802.1X feature

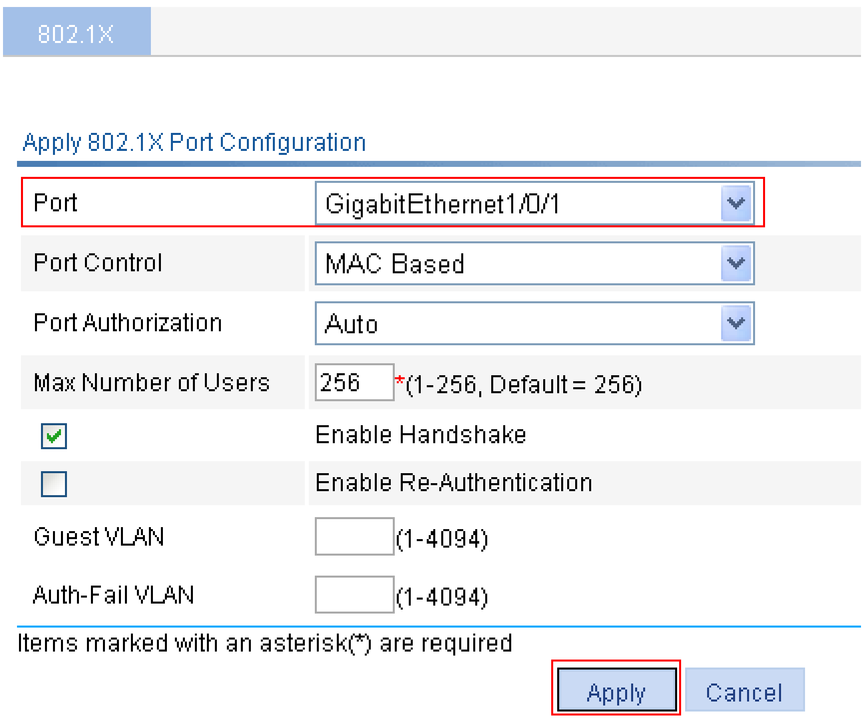
1. From the navigation tree, select **Authentication** > **802.1X**.
2. Select the **Enable 802.1X** box.
3. Select the authentication method **CHAP**.
4. Click **Apply**.

Figure 348 Global 802.1X globally



5. In the **Ports With 802.1X Enabled** area, click **Add**.
6. Select **GigabitEthernet1/0/1** from the **Port** list.
7. Click **Apply**.

Figure 349 802.1X configuration of GigabitEthernet 1/0/1



Verifying the configuration

After the user passes authentication and gets online, use the **ping** command to test whether ACL 3000 takes effect.

1. From the navigation tree, select **Network** > **Diagnostic Tools**.

The ping page appears.

2. Enter the destination IP address **10.0.0.1**.
3. Click **Start** to start the ping operation.

   Figure 350 shows the ping operation summary.

Figure 350 Ping operation summary

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
```

Configuring AAA

AAA overview

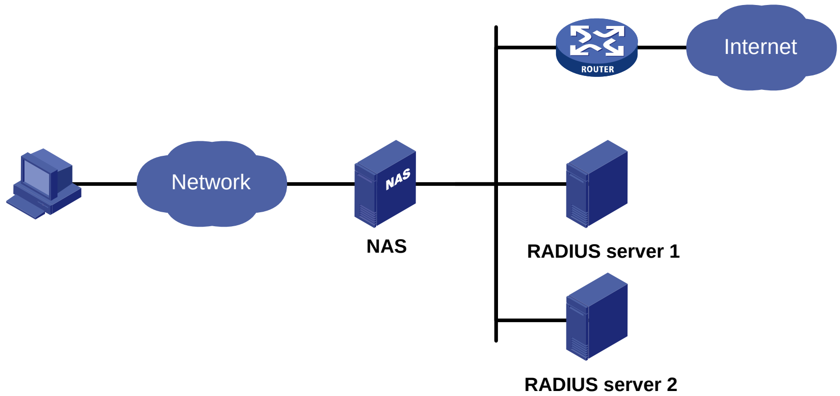
Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. It provides the following security functions:

- **Authentication**—Identifies users and determines whether a user is valid.
- **Authorization**—Grants different users different rights and controls their access to resources and services. For example, a user who has successfully logged in to the switch can be granted read and print permissions to the files on the switch.
- **Accounting**—Records all network service usage information of users, including the service type, start time, and traffic. The accounting function not only provides the information required for charging, but also allows for network security surveillance.

AAA can be implemented through multiple protocols. The switch series supports RADIUS, the most commonly used protocol in practice. For more information about RADIUS, see "Configuring RADIUS."

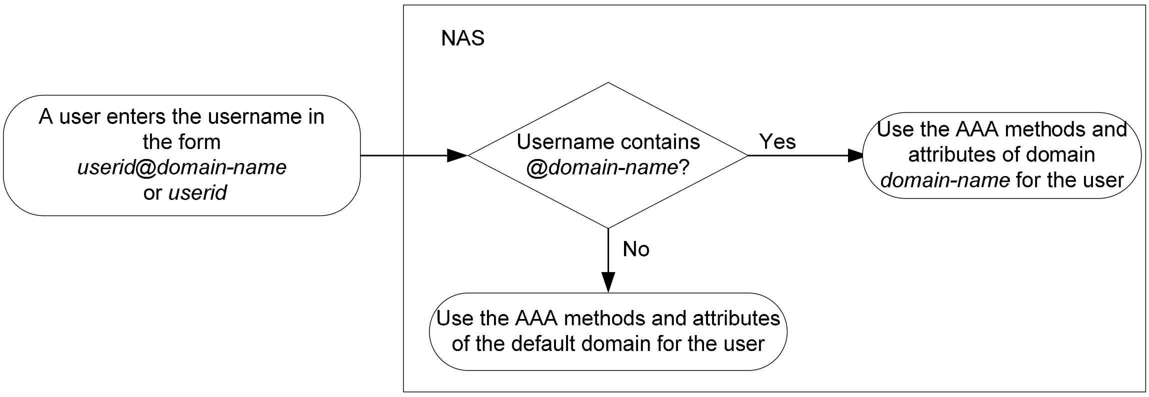
AAA usually uses a client/server model. The client runs on the network access server (NAS) and the server maintains user information centrally. In an AAA network, a NAS is a server for users but a client for the AAA servers, as shown in Figure 351.

Figure 351 Network diagram for AAA



The NAS manages users based on Internet service provider (ISP) domains. On the NAS, each user belongs to one ISP domain. The NAS determines the ISP domain for a user by the username entered by the user at login, as shown in Figure 352.

Figure 352 Determining the ISP domain of a user by the username



The authentication, authorization, and accounting of a user depends on the AAA methods configured for the domain that the user belongs to. If no specific AAA methods are configured for the domain, the default methods are used. By default, a domain uses local authentication, local authorization, and local accounting.

AAA allows you to manage users based on their access types:

- **LAN-access users**—Users on a LAN who must pass, for example, 802.1X or MAC address authentication to access the network.
- **Login users**—Users who want to log in to the switch, including SSH users, Telnet users, web users, FTP users, and terminal users.

In addition, AAA provides command authorization for login users to enhance security. With this function configured, the NAS has every single command entered by a login user verified by the authorization server to restrict the user to execute only authorized commands.

Recommended AAA configuration procedure

Before configuring AAA, complete the following tasks:

- To implement local authentication, configure local users on the access device as described in "Configuring users and user groups."
- To implement RADIUS authentication, create the RADIUS schemes to be used as described in "Configuring RADIUS."

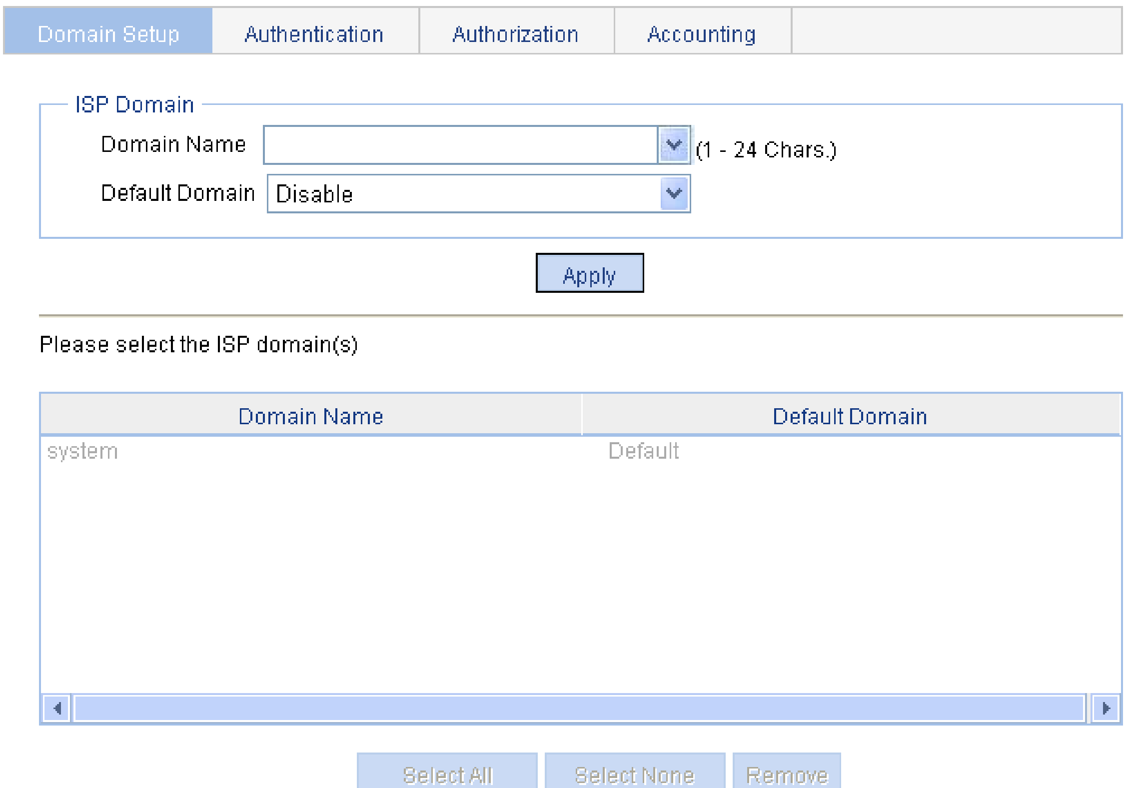
Step	Remarks
1. Configuring an ISP domain	(Optional.) Create ISP domains and specify one of them as the default ISP domain. By default, there is an ISP domain named **system**, which is the default ISP domain.
2. Configuring authentication methods for the ISP domain	(Optional.) Configure authentication methods for various types of users. By default, all types of users use local authentication.

Step	Remarks
3. 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.
4. Configuring accounting methods for the ISP domain	(Optional.) Specify the accounting methods for various types of users. By default, all types of users use local accounting.

Configuring an ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
   The **Domain Setup** page appears.

Figure 353 Domain Setup page



2. Create an ISP domain as described in Table 107.
3. Click **Apply**.

Table 107 Configuration items

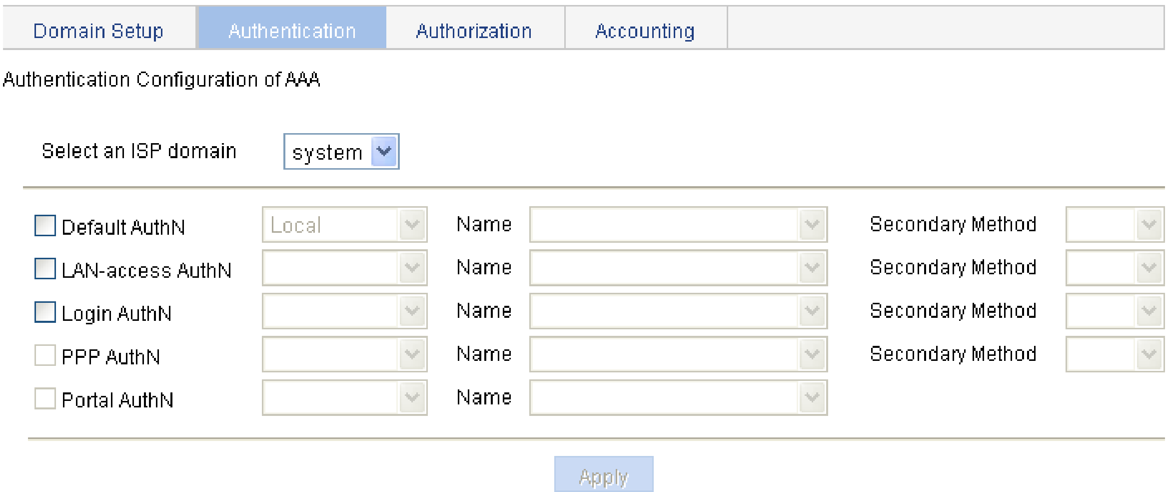
Item	Description
Domain Name	Enter the ISP domain name, which is for identifying the domain. You can enter a new domain name to create a domain, or specify an existing domain to change its status (whether it is the default domain).

Item	Description
Default Domain	Specify whether to use the ISP domain as the default domain. Options include: • **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 becomes a non-default domain.

Configuring authentication methods for the ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
2. Click the **Authentication** tab.

Figure 354 Authentication method configuration page



3. Select the ISP domain and specify authentication methods for the domain as described in Table 108.
4. Click **Apply**.
5. Click **Close** in the success message dialog box that appears.

Table 108 Configuration items

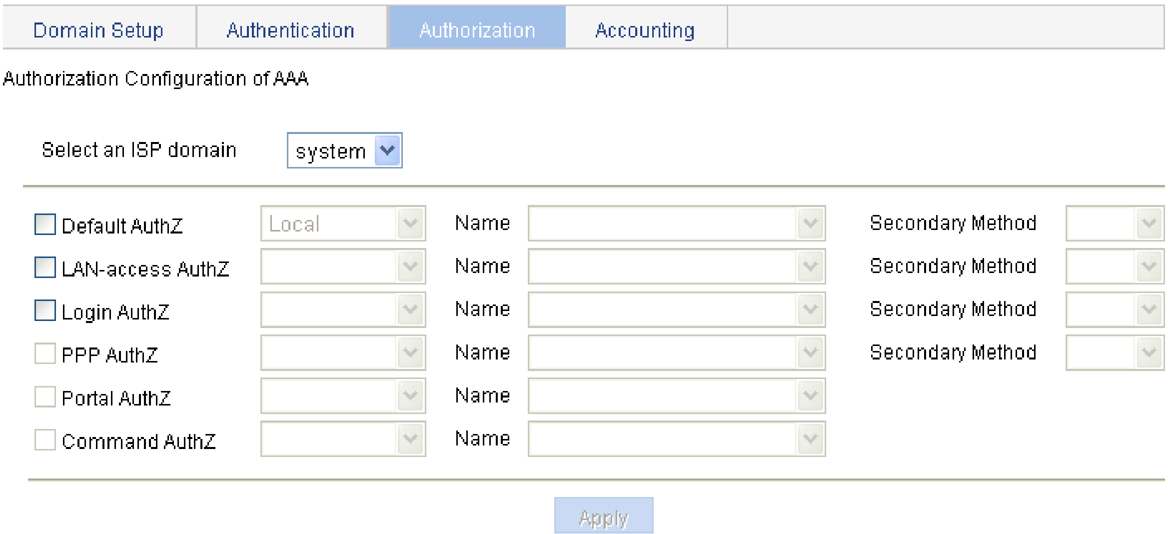
Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.

Item	Description
Default AuthN Name Secondary Method	Configure the default authentication method and secondary authentication method for all types of users. Options include: • **HWTACACS**—Performs HWTACACS authentication based on an HWTACACS scheme. The switch series does not support this option. • **Local**—Performs local authentication. • **None**—All users are trusted and no authentication is performed. Generally, do not use this mode. • **RADIUS**—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—Restores the default local authentication.
LAN-access AuthN Name Secondary Method	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, do not use this mode. • **RADIUS**—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—Uses the default authentication methods.
Login AuthN Name Secondary Method	Configure the authentication method and secondary authentication method for login users. Options include: • **HWTACACS**—Performs HWTACACS authentication based on an HWTACACS scheme. The switch series does not support this option. • **Local**—Performs local authentication. • **None**—All users are trusted and no authentication is performed. Generally, do not use this mode. • **RADIUS**—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—Uses the default authentication methods.

Configuring authorization methods for the ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
2. Click the **Authorization** tab.

Figure 355 Authorization method configuration page



3. Select the ISP domain and specify authorization methods for the ISP domain as described in Table 109.
4. Click **Apply**.
5. Click **Close** in the success message dialog box that appears.

Table 109 Configuration items

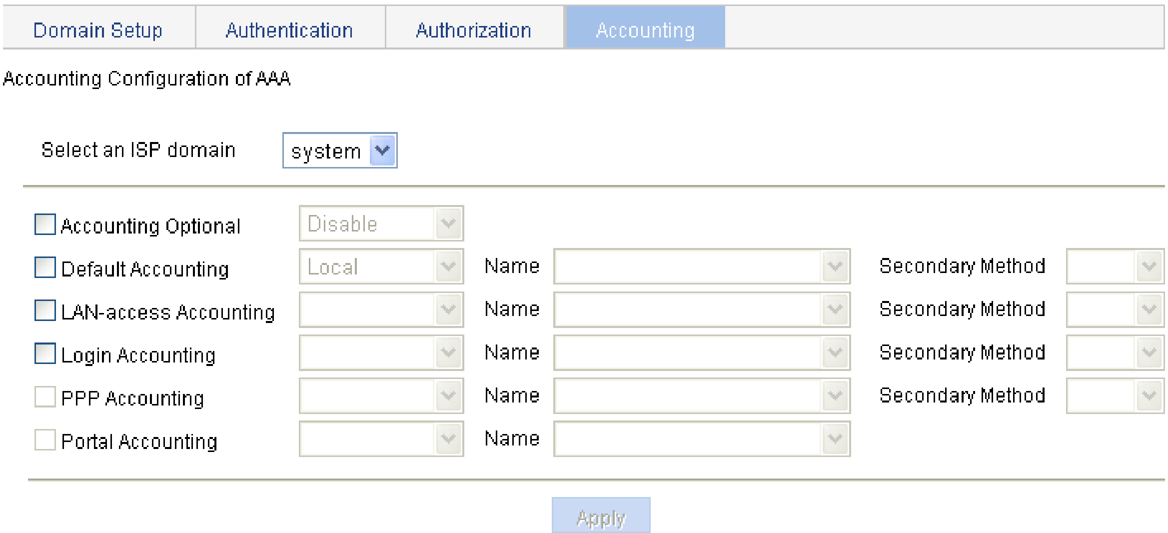
Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthZ Name Secondary Method	Configure the default authorization method and secondary authorization method for all types of users. Options include: • **HWTACACS**—Performs authorization based on an HWTACACS scheme. The switch series does not support this option. • **Local**—Performs local authorization. • **None**—All users are trusted and authorized. A user gets the default rights of the system. • **RADIUS**—Performs RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—Restores the default local authorization.
LAN-access AuthZ Name Secondary Method	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 default rights of the system. • **RADIUS**—Performs RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—Uses the default authorization methods.

Item	Description
Login AuthZ Name Secondary Method	Configure the authorization method and secondary authorization method for login users. Options include: • **HWTACACS**—Performs authorization based on an HWTACACS scheme. The switch series does not support this option. • **Local**—Performs local authorization. • **None**—All users are trusted and authorized. A user gets the default rights of the system. • **RADIUS**—Performs RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—Uses the default authorization methods.

Configuring accounting methods for the ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
2. Click the **Accounting** tab.

Figure 356 Accounting method configuration page



3. Select the ISP domain and specify accounting methods for the ISP domain as described in Table 110.
4. Click **Apply**.
5. Click **Close** in the success message dialog box that appears.

Table 110 Configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.

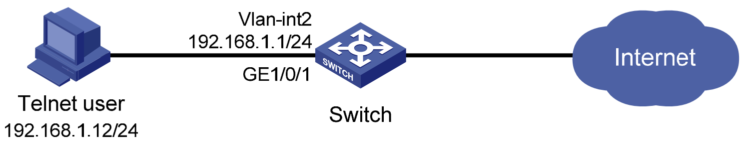
Item	Description
Accounting Optional	Specify whether to enable the accounting optional feature. With the feature enabled, a user who would otherwise be disconnected can use the network resources even when there is no accounting server available or when communication with the current accounting server fails. If accounting for such a user fails, the switch no longer sends real-time accounting updates for the user.
Default Accounting Name Secondary Method	Configure the default accounting method and secondary accounting method for all types of users. Options include: • **HWTACACS**—Performs accounting based on an HWTACACS scheme. The switch series does not support this option • **Local**—Performs local accounting. • **None**—Performs no accounting. • **RADIUS**—Performs RADIUS accounting. You must specify the RADIUS scheme to be used. • **Not Set**—Restores the default local accounting.
LAN-access Accounting Name Secondary Method	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 must specify the RADIUS scheme to be used. • **Not Set**—Uses the default accounting methods.
Login Accounting Name Secondary Method	Configure the accounting method and secondary accounting method for login users. Options include: • **HWTACACS**—Performs accounting based on an HWTACACS scheme. The switch series does not support this option • **Local**—Performs local accounting. • **None**—Performs no accounting. • **RADIUS**—Performs RADIUS accounting. You must specify the RADIUS scheme to be used. • **Not Set**—Uses the default accounting methods.

AAA configuration example

Network requirements

As shown in Figure 357, configure the switch to perform local authentication, authorization, and accounting for Telnet users.

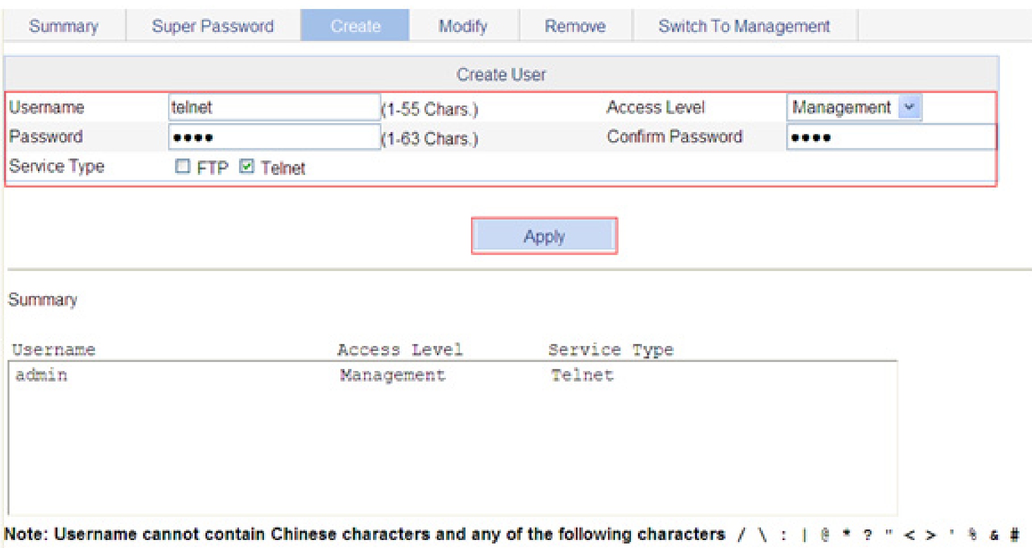
Figure 357 Network diagram



Configuration procedure

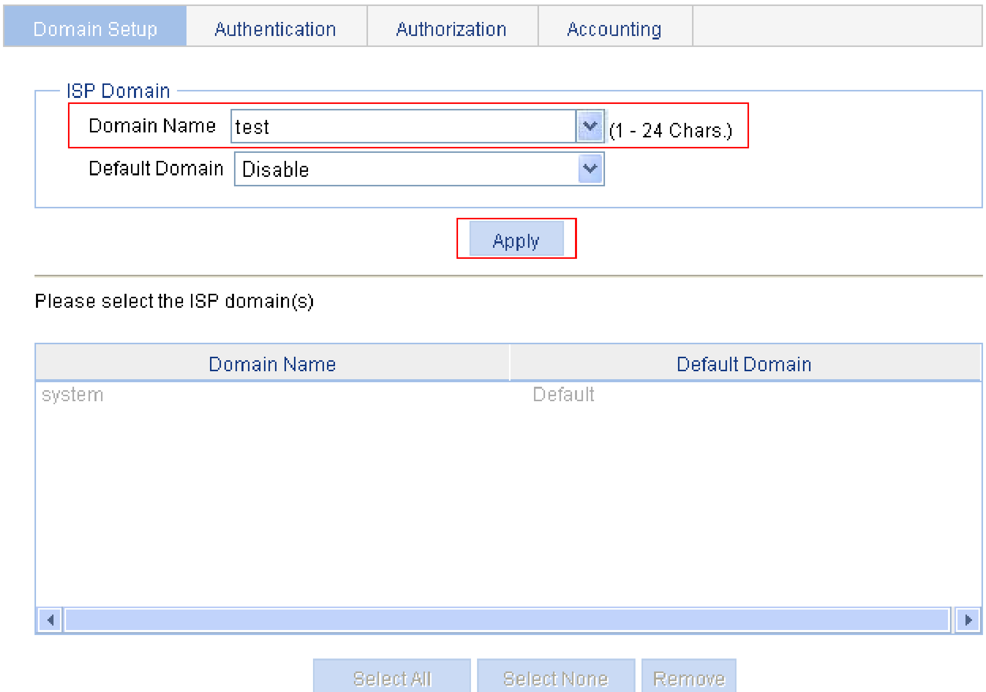
1. Enable the Telnet server function, and configure the switch to use AAA for Telnet users. (Details not shown.)
2. Configure IP addresses for the interfaces. (Details not shown.)
3. Configure a local user:
    a. Select **Device** > **Users** from the navigation tree.
    b. Click the **Create** tab.
    c. Enter the username **telnet**.
    d. Select the access level **Management**.
    e. Enter the password **abcd** and confirm the password.
    f. Select the service type **Telnet**.
    g. Click **Apply**.

Figure 358 Configuring a local user



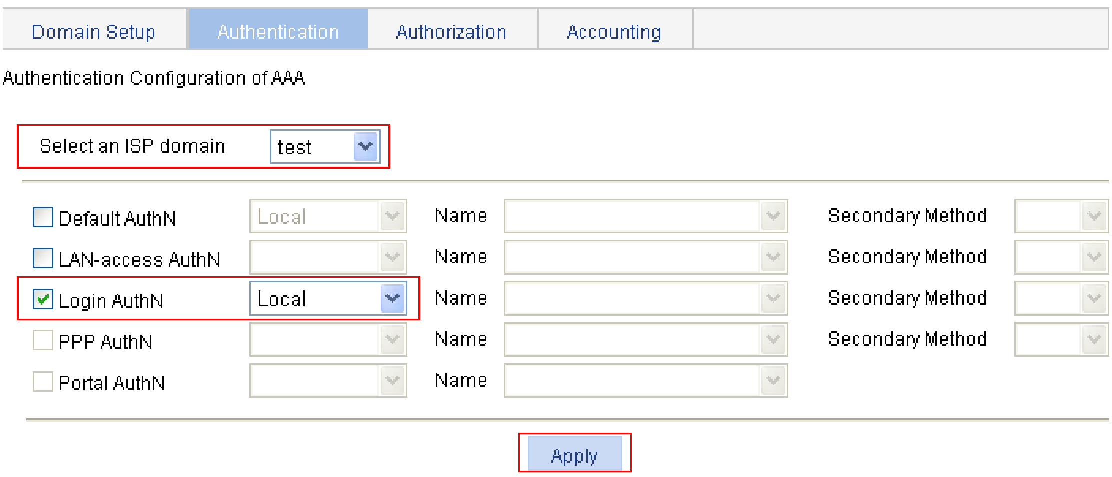
4. Configure ISP domain **test**:
    a. Select **Authentication** > **AAA** from the navigation tree.
       The domain configuration page appears.
    b. Enter the domain name **test**.
    c. Click **Apply**.

Figure 359 Configuring an ISP domain



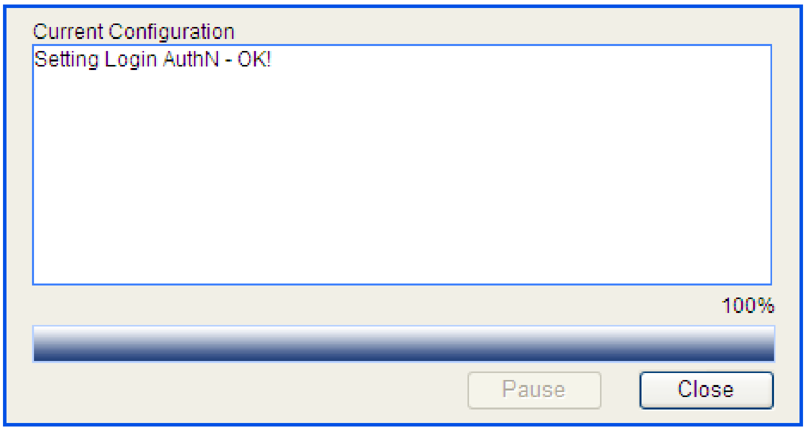
5. Configure the ISP domain to use local authentication:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. Click the **Authentication** tab.
   c. Select the domain **test**.
   d. Select **Login AuthN** and select the authentication method **Local**.

Figure 360 Configuring the ISP domain to use local authentication



   e. Click **Apply**.
      A configuration progress dialog box appears, as shown in Figure 361.
   f. After the configuration process is complete, click **Close**.

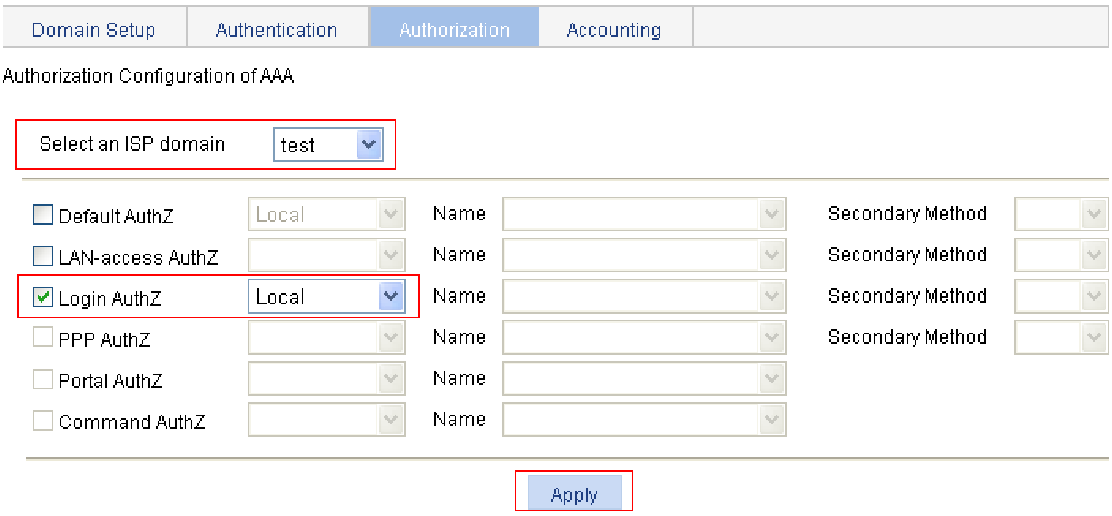
Figure 361 Configuration progress dialog box



6. Configure the ISP domain to use local authorization:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. Click the **Authorization** tab.
   c. Select the domain **test**.
   d. Select **Login AuthZ** and select the authorization method **Local**.
   e. Click **Apply**.

      A configuration progress dialog box appears.
   f. After the configuration progress is complete, click **Close**.

Figure 362 Configuring the ISP domain to use local authorization

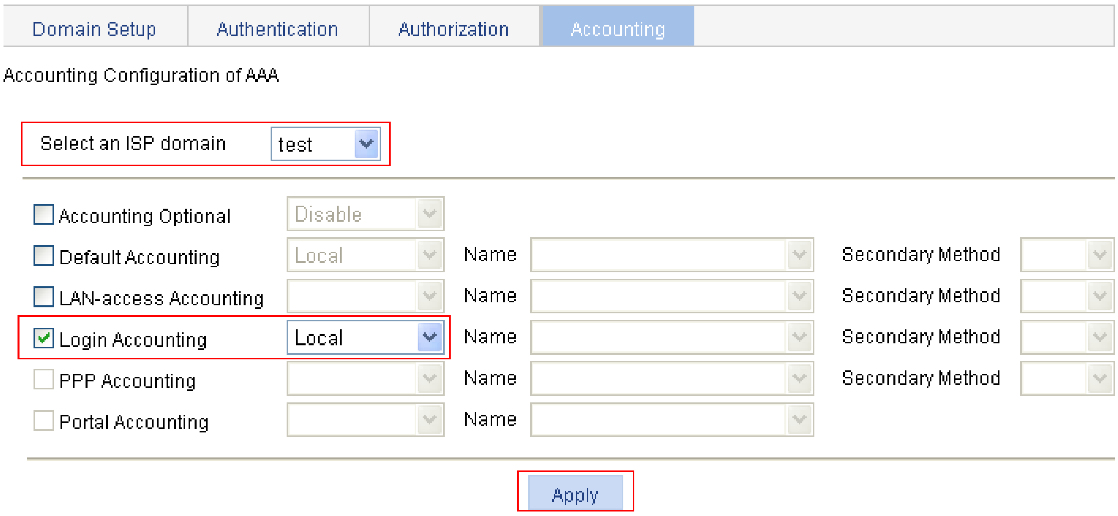


7. Configure the ISP domain to use local accounting:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. Click the **Accounting** tab.
   c. Select the domain **test**.
   d. Select **Login Accounting** and select the accounting method **Local**.
   e. Click **Apply**.

      A configuration progress dialog box appears.

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

Figure 363 Configuring the ISP domain to use local accounting



Verifying the configuration

Telnet to the switch and enter the username **telnet@test** and password **abcd**. You should be serviced as a user in domain **test**.

Configuring portal authentication

Overview

Portal authentication helps control access to the Internet. It is also called "web authentication." A website implementing portal authentication is called a "portal website."

With portal authentication, an access device redirects all users to the portal authentication page. All users can access the free services provided on the portal website. To access the Internet, however, a user must pass portal authentication.

A user can access a known portal website and enter a username and password for authentication. This authentication mode is called active authentication. There is another authentication mode, forced authentication, in which the access device forces a user who is trying to access the Internet through HTTP to log on to a portal website for authentication.

The portal feature provides the flexibility for Internet service providers (ISPs) to manage services. A portal website can, for example, present advertisements and deliver community and personalized services. In this way, broadband network providers, equipment vendors, and content service providers form an industrial ecological system.

Extended portal functions

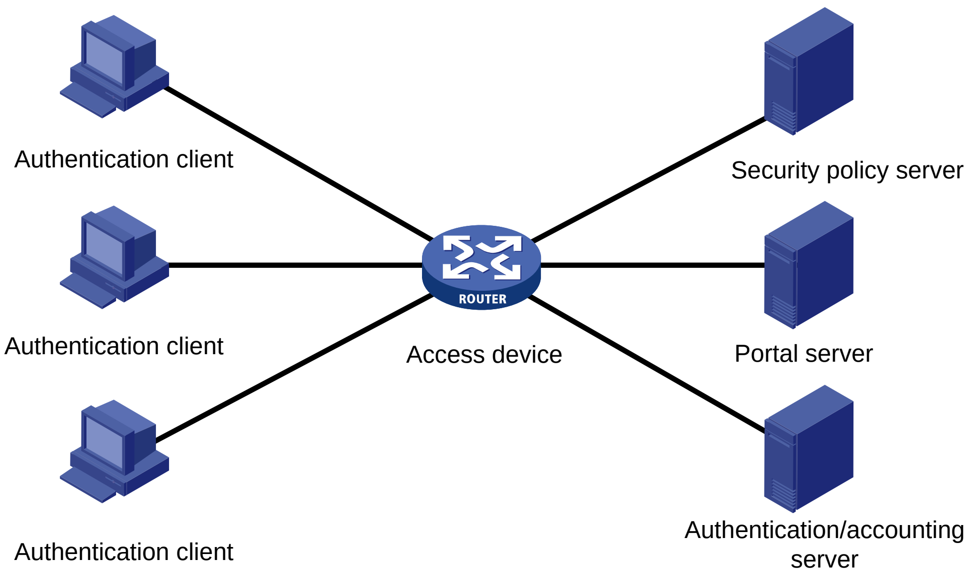
By forcing patching and anti-virus policies, extended portal functions help users to defend against viruses. Portal authentication supports the following extended functions:

- **Security check**—Works after identity authentication succeeds to check whether the required anti-virus software, virus definition file, and operating system (OS) patches are installed, and whether there is any unauthorized software installed on the user host.
- **Resource access restriction**—Allows a user passing identity authentication to access only network resources in the quarantined area, such as the anti-virus server and the patch server. Only users passing both identity authentication and security check can access restricted network resources.

Portal system components

A typical portal system comprises these basic components: authentication client, access device, portal server, authentication/accounting server, and security policy server.

Figure 364 Portal system components



Authentication client

An authentication client is an entity seeking access to network resources. It is typically an end-user terminal, such as a PC. The client can use a browser or a portal client software for portal authentication. Client security check is implemented through communications between the client and the security policy server.

Access device

An access device controls user access. It can be a switch or a router that provides the following functions:

- Redirecting all HTTP requests from unauthenticated users in authentication subnets to the portal server.
- Interacting with the portal server, the security policy server, and the authentication/accounting server for identity authentication, security check, and accounting.
- Allowing users who have passed identity authentication and security check to access granted Internet resources.

Portal server

A portal server listens to authentication requests from authentication clients and exchanges client authentication information with the access device. It provides free portal services and pushes web authentication pages to users.

A portal server can be an entity independent of the access device or an entity embedded in the access device. In this document, the term "portal server" refers to an independent portal server, and the term "local portal server" refers to an embedded portal server.

Authentication/accounting server

An authentication/accounting server implements user authentication and accounting through interaction with the access device.

Only a RADIUS server can serve as the remote authentication/accounting server in a portal system.

Security policy server

A security policy server interacts with authentication clients and access devices for security check and resource authorization.

The components of a portal system interact in the following procedure:

1. When an unauthenticated user enters a website address in the address bar of the browser to access the Internet, an HTTP request is created and sent to the access device, which redirects the HTTP request to the web authentication homepage of the portal server. For extended portal functions, authentication clients must run the portal client software.
2. On the authentication homepage/authentication dialog box, the user enters and submits the authentication information, which the portal server then transfers to the access device.
3. Upon receipt of the authentication information, the access device communicates with the authentication/accounting server for authentication and accounting.
4. After successful authentication, the access device checks whether there is a corresponding security policy for the user. If not, it allows the user to access the Internet. Otherwise, the client communicates with the access device and the security policy server for security check. If the client passes security check, the security policy server authorizes the user to access the Internet resources.

NOTE:

To implement security check, the client must be the HP iNode client.

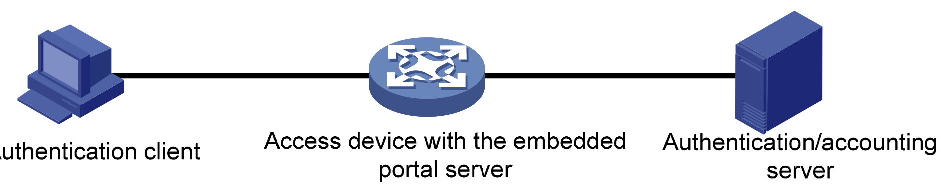
Portal authentication supports NAT traversal whether it is initiated by a web client or an HP iNode client. When the portal authentication client is on a private network, but the portal server is on a public network and the access device is enabled with NAT, network address translations performed on the access device do not affect portal authentication.

Portal system using the local portal server

System components

In addition to use a separate device as the portal server, a portal system can also use the local portal server function of the access device to authenticate web users directly. A portal system using the local portal server does not support extended portal functions. No security policy server is needed for local portal service. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server.

Figure 365 Portal system using the local portal server



NOTE:

The local portal server function of the access device only implements some simple portal server functions, allowing users to log in and log out through the web interface. It cannot take the place of an independent portal server.

Protocols used for interaction between the client and local portal server

HTTP and HTTPS can be used for communication between an authentication client and an access device providing the local portal server function. If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text. If HTTPS is used, secure data transmission is ensured because HTTPS packets are transferred in cipher text based on SSL.

Portal authentication modes

Portal authentication may work at Layer 2 or Layer 3 of the OSI model.

Layer 2 portal authentication

You can enable Layer 2 portal authentication on an access device's Layer 2 ports that connect authentication clients, so that only clients whose MAC addresses pass authentication can access the external network. Only the local portal server provided by the access device supports Layer 2 portal authentication.

Layer 2 portal authentication allows the authentication server to assign different VLANs according to user authentication results so that access devices can thereby control user access to resources. After a client passes authentication, the authentication server can assign an authorized VLAN to allow the user to access the resources in the VLAN. If a client fails authentication, the authentication server can assign an Auth-Fail VLAN. Layer 3 portal authentication does not support VLAN assignment.

Layer 3 portal authentication

In Layer 3 authentication mode, portal authentication is enabled on an access device's Layer 3 interfaces that connect authentication clients. Portal authentication performed on a Layer 3 interface can be direct authentication or cross-subnet authentication. In direct authentication, no Layer 3 forwarding devices exist between the authentication client and the access device. In cross-subnet authentication, Layer 3 forwarding devices may exist between the authentication client and the access device.

- Direct authentication

  Before authentication, a user manually configures a public IP address or directly obtains a public IP address through DHCP, and can access only the portal server and predefined free websites. After passing authentication, the user can access the network resources.

- Cross-subnet authentication

  Cross-subnet authentication is similar to direct authentication, but it allows Layer 3 forwarding devices to be present between the authentication client and the access device.

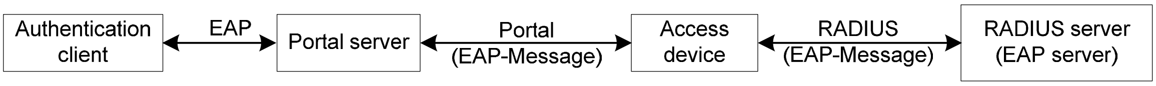
  In direct authentication and cross-subnet authentication, the IP address of a client is used for identification of the client. After a client passes authentication, the access device generates an access control list (ACL) for the client based on the client's IP address to permit packets from the client to go through the access port. Because no Layer 3 devices are present between the authentication clients and the access device in direct authentication, the access device can directly learn the MAC addresses of the clients, and thus can control the forwarding of packets from clients in a more granular way by also using the learnt MAC addresses.

Portal support for EAP

Authentication by using the username and password is less secure. Digital certificate authentication is usually used to ensure higher security.

The Extensible Authentication Protocol (EAP) supports several digital certificate-based authentication methods, for example, EAP-TLS. Working together with EAP, portal authentication can implement digital certificate-based user authentication.

Figure 366 Portal support for EAP working flow diagram



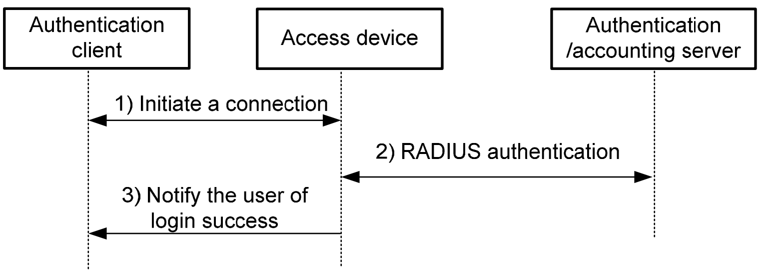
As shown in Figure 366, the authentication client and the portal server exchange EAP authentication packets. The portal server and the access device exchange portal authentication packets that carry the EAP-Message attributes. The access device and the RADIUS server exchange RADIUS packets that carry the EAP-Message attributes. The RADIUS server that supports the EAP server function processes the EAP packets encapsulated in the EAP-Message attributes, and provides the EAP authentication result. During the whole EAP authentication process, the access device does not process the packets that carry the EAP-Message attributes but only transports them between the portal server and the RADIUS server. Therefore, no additional configuration is needed on the access device.

NOTE:

- This function requires the cooperation of the HP IMC portal server and HP iNode portal client.
- Only Layer 3 portal authentication that uses a remote portal server supports EAP authentication.

Layer 2 portal authentication process

Figure 367 Local Layer-2 portal authentication process



The process of local Layer-2 portal authentication is as follows:

1. The portal authentication client sends an HTTP or HTTPS request. Upon receiving the HTTP request, the access device redirects it to the listening IP address of the local portal server, which then pushes a web authentication page to the authentication client. The user types the username and password on the web authentication page. The listening IP address of the local portal server is the IP address of a Layer 3 interface on the access device that can communicate with the portal client. Usually, it is a loopback interface's IP address.
2. The access device and the RADIUS server exchange RADIUS packets to authenticate the user.
3. If the user passes RADIUS authentication, the local portal server pushes a logon success page to the authentication client.

Assignment of authorized ACLs

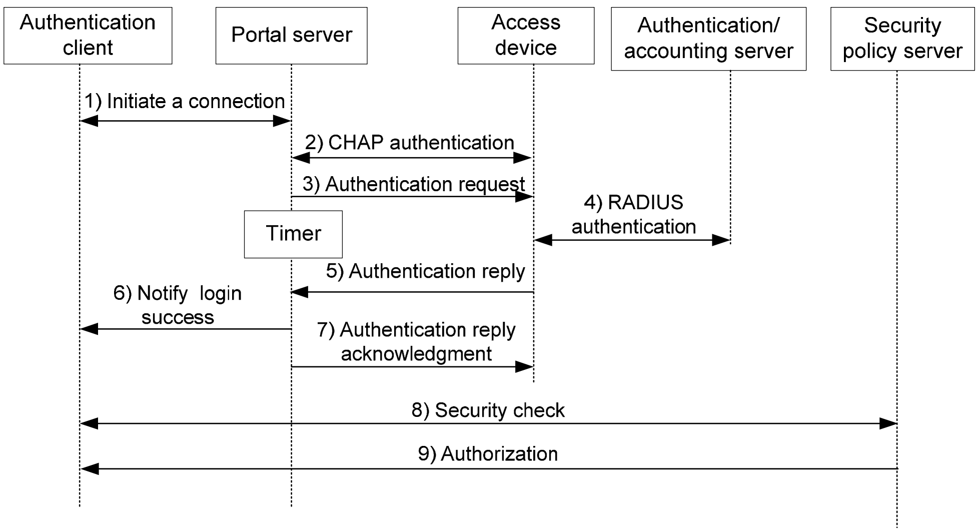
The device can use ACLs to control user access to network resources and limit user access rights. With authorized ACLs specified on the authentication server, when a user passes authentication, the authentication server assigns an authorized ACL for the user, and the device filters traffic from the user on the access port according to the authorized ACL. You must configure the authorized ACLs on the access device if you specify authorized ACLs on the authentication server. To change the access right of a user, you can specify a different authorized ACL on the authentication server or change the rules of the corresponding authorized ACL on the device.

Layer 3 portal authentication process

Direct authentication and cross-subnet authentication share the same authentication process.

Direct authentication/cross-subnet authentication process (with CHAP/PAP authentication)

Figure 368 Direct authentication/cross-subnet authentication process



The direct authentication/cross-subnet authentication process is as follows:

1. A portal user initiates an authentication request through HTTP. When the HTTP packet arrives at the access device, the access device allows it to pass if it is destined for the portal server or a predefined free website, or redirects it to the portal server if it is destined for other websites. The portal server provides a web page for the user to enter the username and password.
2. The portal server and the access device exchange Challenge Handshake Authentication Protocol (CHAP) messages. For Password Authentication Protocol (PAP) authentication, this step is skipped.
3. The portal server assembles the username and password into an authentication request message and sends it to the access device. Meanwhile, the portal server starts a timer to wait for an authentication acknowledgment message.
4. The access device and the RADIUS server exchange RADIUS packets to authenticate the user.
5. The access device sends an authentication reply to the portal server.
6. The portal server sends an authentication success message to the authentication client to notify it of logon success.
7. The portal server sends an authentication reply acknowledgment to the access device.

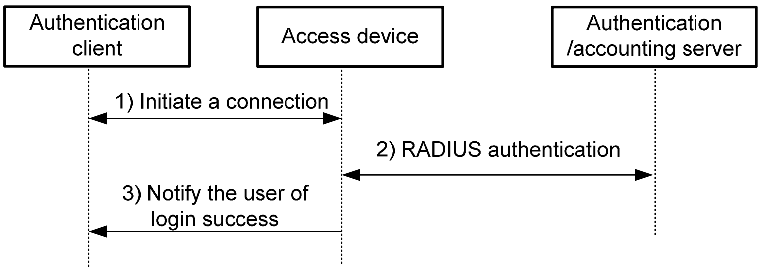
With extended portal functions, the process includes additional steps:

8. The security policy server exchanges security check information with the authentication client to check whether the authentication client meets the security requirements.

9. Based on the security check result, the security policy server authorizes the user to access certain resources, and sends the authorization information to the access device. The access device then controls access of the user based on the authorization information.

Authentication process with the local portal server

Figure 369 Authentication process with local portal server

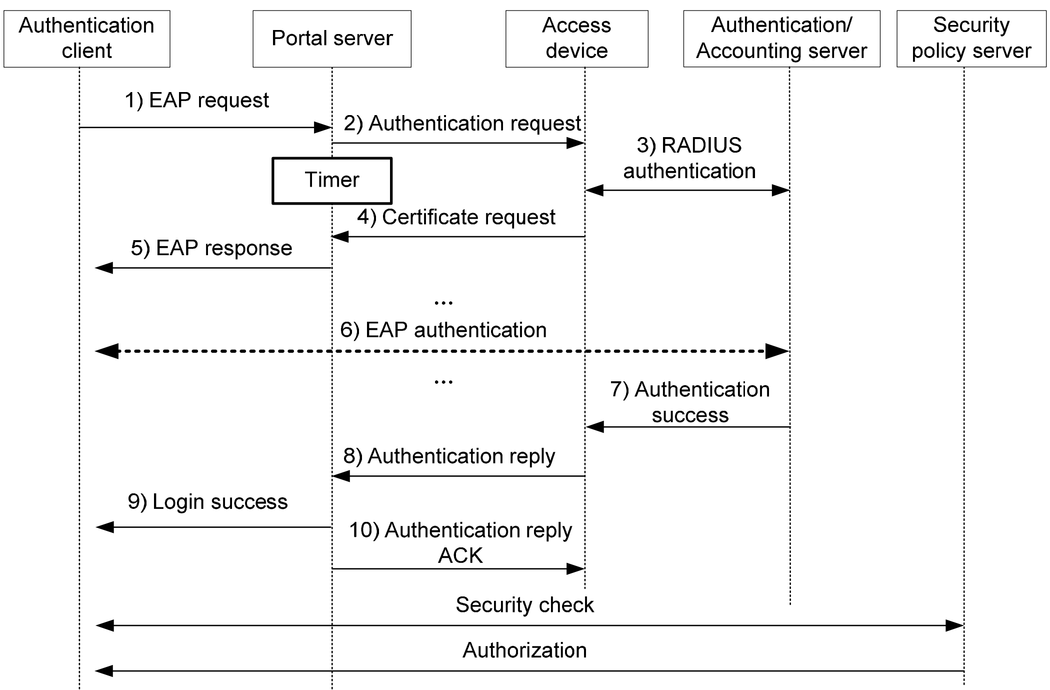


With local portal server, the direct/cross-subnet authentication process is as follows:

1. A portal client initiates authentication by sending an HTTP or HTTPS request. When the HTTP packet arrives at an access device using the local portal server, it is redirected to the local portal server, which then pushes a web authentication page for the user to enter the username and password. The listening IP address of the local portal server is the IP address of a Layer 3 interface on the access device that can communicate with the portal authentication client.
2. The access device and the RADIUS server exchange RADIUS packets to authenticate the user.
3. If the user passes authentication, the local portal server pushes a logon success page to the authentication client, informing the user of the authentication (logon) success.

Portal support for EAP authentication process

Figure 370 Portal support for EAP authentication process



All portal authentication modes share the same EAP authentication steps. The following takes the direct portal authentication as an example to show the EAP authentication process:

1. The authentication client sends an EAP Request/Identity message to the portal server to initiate an EAP authentication process.
2. The portal server sends a portal authentication request to the access device, and starts a timer to wait for the portal authentication reply. The portal authentication request contains several EAP-Message attributes, which are used to encapsulate the EAP packet sent from the authentication client and carry the certificate information of the client.
3. After the access device receives the portal authentication request, it constructs a RADIUS authentication request and sends it to the RADIUS server. The EAP-Message attributes in the RADIUS authentication request are those carried in the received portal authentication request.
4. The access device sends a certificate request to the portal server according to the reply received from the RADIUS server. The certificate request also contains several EAP-Message attributes, which are used to transfer the certificate information of the RADIUS server. The EAP-Message attributes in the certificate request are those carried in the RADIUS authentication reply.
5. After receiving the certificate request, the portal server sends an EAP authentication reply to the authentication client, carrying the EAP-Message attribute values.
6. The authentication client sends another EAP request to continue the EAP authentication with the RADIUS server, during which there may be several portal authentication requests. The subsequent authentication processes are the same as that initiated by the first EAP request, except that the EAP request types vary with the EAP authentication phases.
7. After the authentication client passes the EAP authentication, the RADIUS server sends an authentication reply to the access device. This reply carries the EAP-Success message in the EAP-Message attribute.
8. The access device sends an authentication reply to the portal server. This reply carries the EAP-Success message in the EAP-Message attribute.
9. The portal server notifies the authentication client of the authentication success.
10. The portal server sends an authentication replay acknowledgment to the access device.

The remaining steps are for extended portal authentication. For more information about the steps, see the portal authentication process with CHAP/PAP authentication.

Configuring portal authentication

Configuration prerequisites

The portal feature provides a solution for user identity authentication and security check. However, the portal feature cannot implement this solution by itself. RADIUS authentication needs to be configured on the access device to cooperate with the portal feature to complete user authentication.

The prerequisites for portal authentication configuration are as follows:

- The portal-enabled interfaces of the access device are configured with valid IP addresses or have obtained valid IP addresses through DHCP.
- The portal server and the RADIUS server have been installed and configured properly. Local portal authentication requires no independent portal server.
- The portal client, access device, and servers can reach each other.
- With RADIUS authentication, usernames and passwords of the users are configured on the RADIUS server, and the RADIUS client configuration is performed on the access device. For information about RADIUS client configuration, see "Configuring RADIUS."

- To implement extended portal functions, install and configure IMC EAD, and make sure the ACLs configured on the access device correspond to those specified for the resources in the quarantined area and for the restricted resources on the security policy server. On the access device, the security policy server address is the same as the authentication server address. For more information about security policy server configuration on the access device, see "Configuring RADIUS."

Configuration task list

Recommended configuration procedure for Layer 2 portal authentication

Step	Remarks
1. Configuring the Layer 2 portal service	Required. Configure a local portal server, apply the portal server to a Layer 2 interface, and configure the Layer 2 portal authentication parameters. By default, no local portal server is configured. IMPORTANT: To ensure normal operation of portal authentication on a Layer 2 interface, do not configure port security or guest VLAN of 802.1X on the interface.
2. Configuring advanced parameters for portal authentication	Optional. Configure web proxy server ports, an auto redirection URL, the time that the device must wait before redirecting an authenticated user to the auto redirection URL, and the portal user moving function.
3. Configuring a portal-free rule	Optional. Configure a portal-free rule, specifying the source and destination information for packet filtering A portal-free rule allows specified users to access specified external websites without portal authentication. Packets matching a portal-free rule do not trigger portal authentication and the users can directly access the specified external websites. By default, no portal-free policy is configured.

Recommended configuration procedure for Layer 3 portal authentication

Step	Remarks
1. Configuring the Layer 3 portal service	Required. Configure a portal server, apply the portal server to a Layer 3 interface, and configure the portal authentication parameters. By default, no portal server is configured.
2. Configuring advanced parameters for portal authentication	Optional. Configure an auto redirection URL, the time that the device must wait before redirecting an authenticated user to the auto redirection URL, and the portal user moving function.

Step	Remarks
3. Configuring a portal-free rule	Optional. Configure a portal-free rule, specifying the source and destination information for packet filtering A portal-free rule allows specified users to access specified external websites without portal authentication. Packets matching a portal-free rule will not trigger portal authentication and the users can directly access the specified external websites. By default, no portal-free policy is configured.

Configuring the Layer 2 portal service

1. Select **Authentication** > **Portal** from the navigation tree.

   The portal server configuration page appears.

Figure 371 Portal server configuration

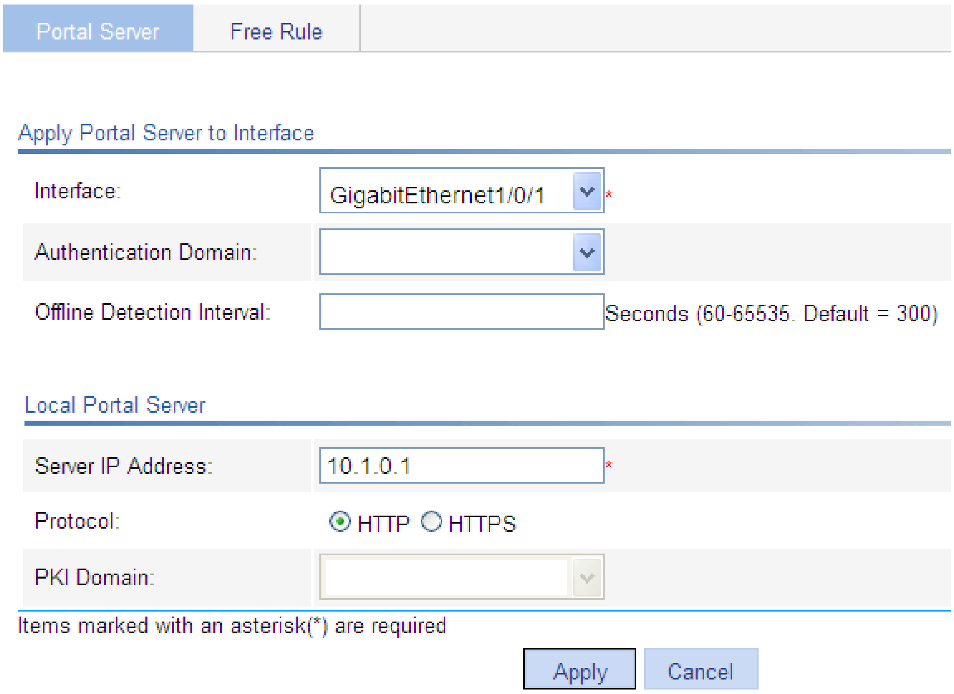
TIP:

The portal service applied on an interface may be in the following states:

- **Running**—Indicates that portal authentication has taken effect on the interface.
- **Enabled**—Indicates that portal authentication has been enabled on the interface but has not taken effect.

2. In the **Portal Application: Layer 2 Interfaces** area, click **Add** to enter the portal server application page.

Figure 372 Applying a portal server to a Layer 2 interface



3. Configure Layer 2 portal authentication as described in Table 111.
4. Click **Apply**.

Table 111 Configuration items

Item	Description
Interface	Select the Layer 2 interface to be enabled with portal authentication.
Authentication Domain	Specify the authentication domain for Layer 2 portal users. After you specify an authentication domain on a Layer 2 interface, the device uses the authentication domain for authentication, authorization, and accounting (AAA) of the portal users on the interface, ignoring the domain names carried in the usernames. You can specify different authentication domains for different interfaces as needed. The available authentication domains are those specified on the page you enter by selecting **Authentication** > **AAA** from the navigation tree. For more information, see "Configuring AAA."

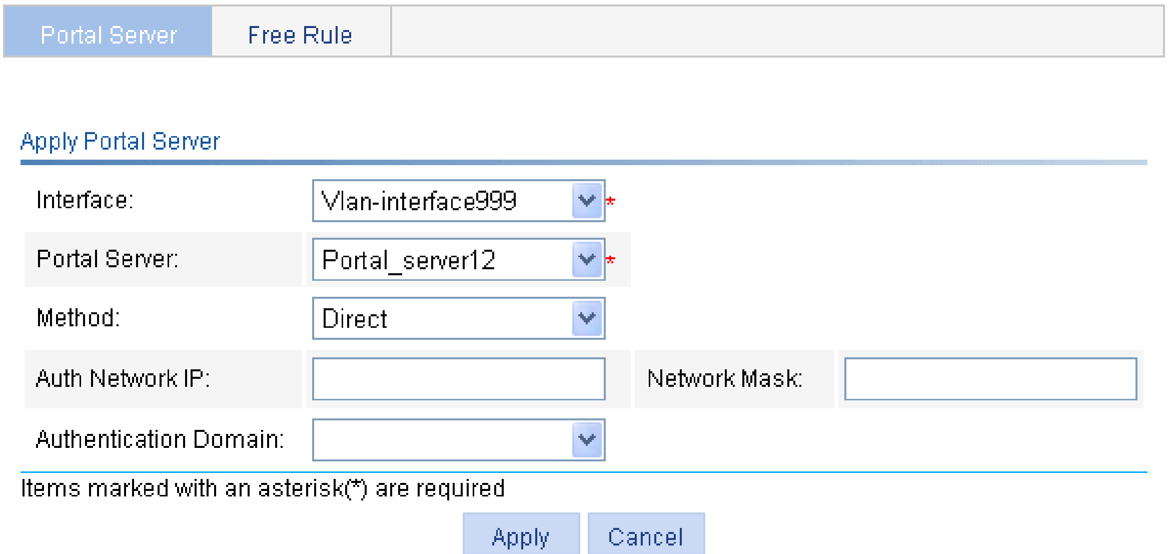
Item	Description
Online Detection Interval	Set the Layer 2 portal user detection interval. After a Layer 2 portal user gets online, the device starts a detection timer for the user, and checks whether the user's MAC address entry has been aged out or the user's MAC address entry has been matched (a match means a packet has been received from the user) at the interval. If the device finds no MAC address entry for the user or receives no packets from the user during two successive detection intervals, the device considers that the user has gone offline and clears the authentication information of the user.
Server IP Address	Specify a listening IP address for the local portal server. IMPORTANT: After you specify a listening IP address, the device automatically assigns the IP address to the Loopback interface on the device, because: • The status of a loopback interface is stable. There will be no authentication page access failures caused by interface failures. • A loopback interface does not forward received packets to any network, avoiding impact on system performance when there are many network access requests.
Protocol	Select the protocol to be used for communication between the portal client and local portal server. Available protocols are HTTP and HTTPS.
PKI Domain	Specify the PKI domain for HTTPS. This field is configurable when you select HTTPS. The available PKI domains are those specified on the page you enter by selecting **Authentication** > **PKI** from the navigation tree. For more information, see "Configuring PKI." IMPORTANT: The service management and portal authentication modules always reference the same PKI domain. Changing the referenced PKI domain in either module also changes that referenced in the other module.

Configuring the Layer 3 portal service

1. Select **Authentication** > **Portal** from the navigation tree.

   The portal server configuration page appears, as shown in Figure 371.
2. In the **Portal Application: Layer 3 Interfaces** area, click **Add** to enter the portal server application page.

Figure 373 Applying a portal server to a Layer 3 interface



3. Configure Layer 3 portal authentication as described in Table 112.
4. Click **Apply**.

Table 112 Configuration items

Item	Description
Interface	Select the Layer 3 interface to be enabled with portal authentication.
Portal Server	Select the portal server to be applied on the selected interface. Options include: • **Select Server**—Select an existing portal server from the portal server drop-down list. • **New Server**—If you select this option from the drop-down list, the portal server configuration area (see Figure 374) will be displayed at the lower part of the page. You can add a remote portal server and apply the portal server to the Layer 3 interface. For configuration details, see Table 113. • **Enable Local Server**—If you select this option from the drop-down list, the local portal service configuration area (see Figure 375) will be displayed at the lower part of the page. You can configure the parameters for the Layer 3 local portal service. For configuration details, see Table 114.
Method	Specify the portal authentication mode, which can be: • **Direct**—Direct portal authentication. • **Layer3**—Cross-subnet portal authentication. IMPORTANT: Cross-subnet portal authentication mode does not require Layer 3 forwarding devices to be present between the authentication client and the access device. However, if there are Layer 3 forwarding devices between the authentication client and the access device, you must select the cross-subnet portal authentication mode.

Item	Description
Auth Network IP	Enter the IP address and mask of the authentication subnet. This field is configurable when you select the **Layer3** mode (cross-subnet portal authentication).
Network Mask	By configuring an authentication subnet, you specify that only HTTP packets from users on the authentication subnet can trigger portal authentication. If an unauthenticated user is not on any authentication subnet, the access device discards all the user's HTTP packets that do not match any portal-free rule. IMPORTANT: The authentication subnet in direct mode is any source IP address.
Authentication Domain	Specify an authentication domain for Layer 3 portal users. After you specify an authentication domain on a Layer 3 interface, the device uses the authentication domain for authentication, authorization, and accounting (AAA) of the portal users on the interface, ignoring the domain names carried in the usernames. You can specify different authentication domains for different interfaces as needed. The available authentication domains are those specified on the page you enter by selecting **Authentication** > **AAA** from the navigation tree. For more information, see "Configuring AAA."

Figure 374 Adding a portal server

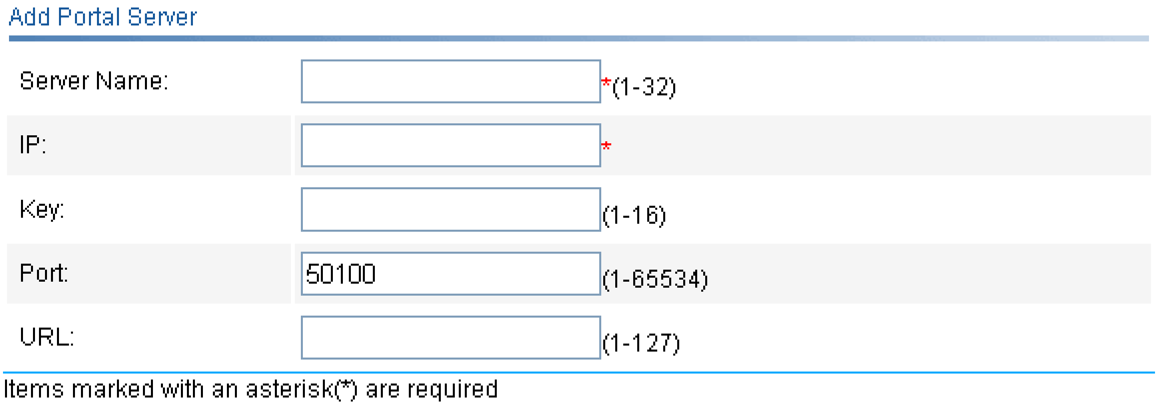


Table 113 Configuration items

Item	Description
Server Name	Type a name for the remote portal server.
IP	Type the IP address of the remote portal server.
Key	Type the shared key to be used for communication between the device and the remote portal server.
Port	Type the port number of the remote portal server.
URL	Specify the URL for HTTP packets redirection. IMPORTANT: Redirection URL supports domain name resolution, however, you need to configure a portal-free rule and add the DNS server address into the portal-free address range.

Figure 375 Configuring the local portal server

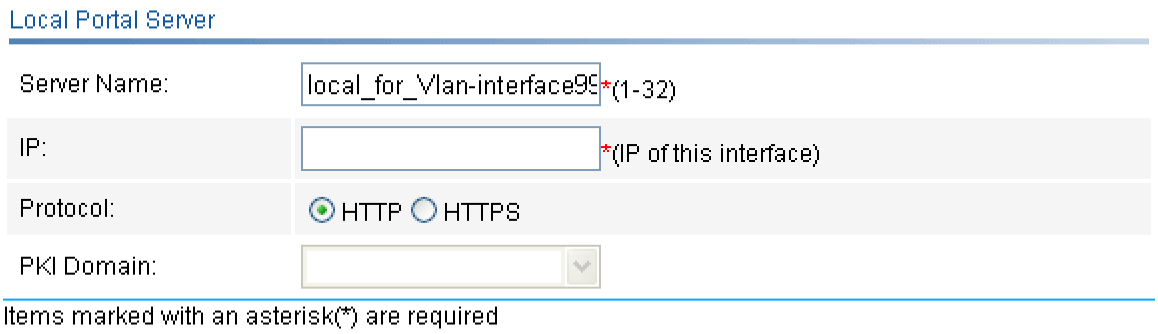


Table 114 Configuration items

Item	Description
Server Name	Type a name for the local portal server.
IP	Type the IP address of the local portal server. You need to specify the IP address of the interface where the local portal server is applied.
Protocol	Specify the protocol to be used for authentication information exchange between the local portal server and the client. It can be HTTP or HTTPS. If you select HTTPS, you also need to specify the PKI domain.
PKI Domain	Type the PKI domain for HTTPS. This field is configurable when you select HTTPS. The available PKI domains are those specified on the page you enter by selecting **Authentication** > **PKI** from the navigation tree. For more information, see "Configuring PKI." IMPORTANT: The service management and portal authentication modules always reference the same PKI domain. Changing the referenced PKI domain in either module also changes that referenced in the other module.

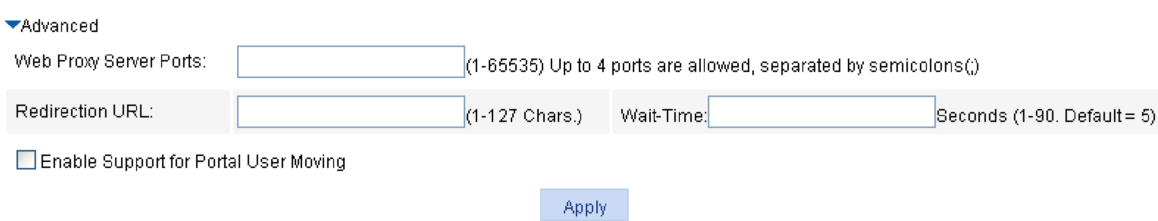
Configuring advanced parameters for portal authentication

1. Select **Authentication** > **Portal** from the navigation tree.

   The portal server configuration page appears, as shown in Figure 371.

2. Expand the **Advanced** area to show the advanced parameters for portal authentication.

Figure 376 Advanced configuration



3. Configure the advanced parameters as described in Table 115.
4. Click **Apply**.

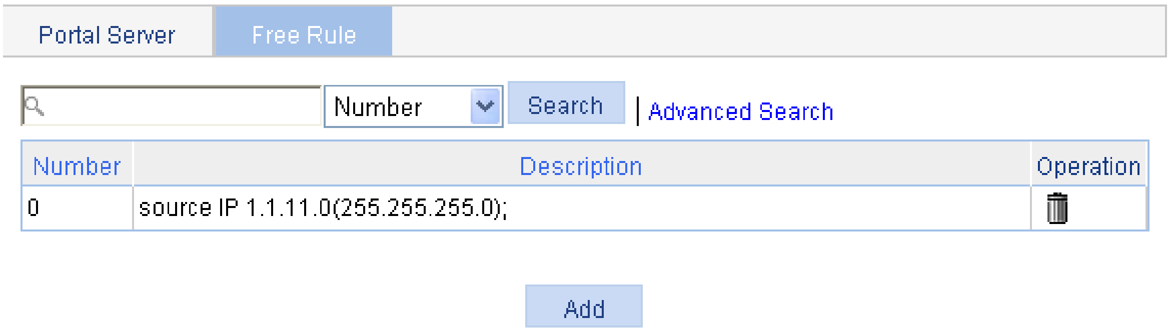
Table 115 Configuration items

Item	Description
Web Proxy Server Ports	Configure the web proxy server ports to allow HTTP requests proxied by the specified proxy servers to trigger portal authentication. By default, only HTTP requests that are not proxied can trigger portal authentication. To make sure that a user using a web proxy server can trigger portal authentication, you need to add the port number of the proxy server on the device and the user needs to specify the listening IP address of the local portal server as a proxy exception in the browser. Thus, HTTP packets that the portal user sends to the local portal server are not sent to the proxy server. IMPORTANT: • Only Layer 2 portal authentication supports this feature. • If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover web proxy servers, add the port numbers of the web proxy servers on the device, and configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.
Redirection URL	Specify the auto redirection URL to which users will be automatically redirected after they pass portal authentication. To access the network, an unauthenticated user either goes to or is automatically forced to the portal authentication page for authentication. If the user passes portal authentication and the access device is configured with an auto redirection URL, the access device redirects the user to the URL after a specific period of time.
Wait-Time	Set the time that the device must wait before redirecting an authenticated portal user to the auto redirection URL.
Enable Support for Portal User Moving	Specify whether to enable support for portal user moving. In scenarios where there are hubs, Layer 2 switches, or APs between users and the access devices, if an authenticated user moves from an access port to another Layer 2-portal-authentication-enabled port of the device without logging off, the user cannot get online when the original port is still up. The reason is that the original port is still maintaining the authentication information of the user and the device does not permit such a user to get online from another port by default. To solve the problem described above, enable support for portal user moving on the device. Then, when a user moves from a port of the device to another, the device provides services in either of the following two ways: • If the original port is still up and the two ports belong to the same VLAN, the device allows the user to continue to access the network without re-authentication, and uses the new port information for accounting of the user. • If the original port is down or the two ports belong to different VLANs, the device removes the authentication information of the user from the original port and authenticates the user on the new port. IMPORTANT: For a user with authorization information (such as authorized VLAN) configured, after the user moves from a port to another, the device tries to assign the authorization information to the new port. If the operation fails, the device deletes the user's information from the original port and re-authenticates the user on the new port.

Configuring a portal-free rule

1. Select **Authentication** > **Portal** from the navigation tree
2. Click the **Free Rule** tab to enter the portal-free rule list page.

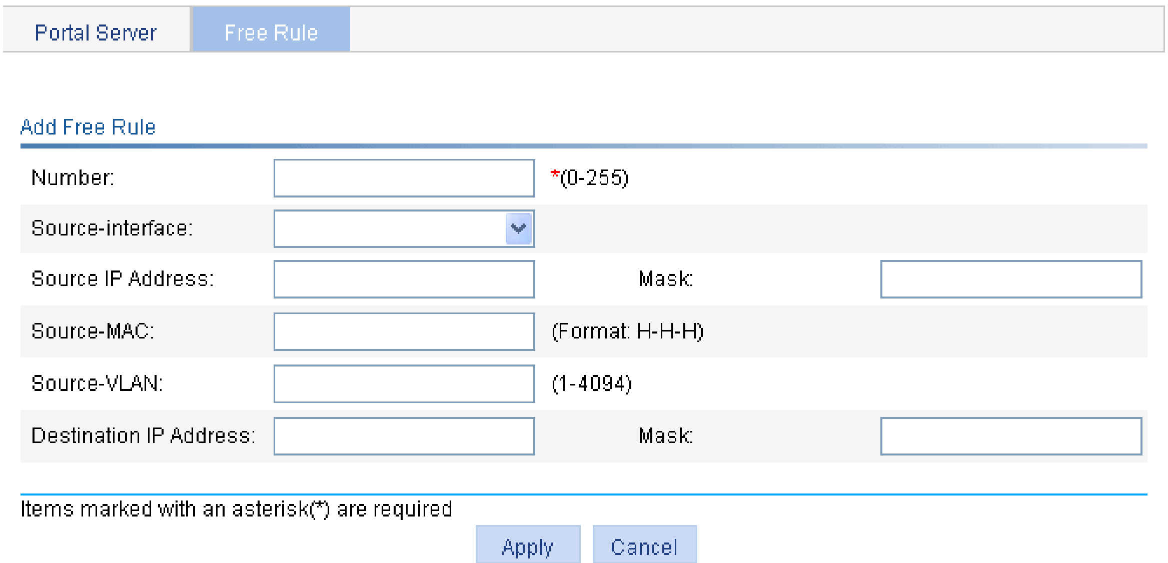
Figure 377 Portal-free rule list



3. Click **Add**.

   The page for adding a new portal-free rule appears.

Figure 378 Adding a portal-free rule



4. Configure a portal-free rule as described in Table 116.
5. Click **Apply**.

Table 116 Configuration items

Item	Description
Number	Specify a sequence number for the portal-free rule.
Source-interface	Specify a source interface for the portal-free rule.
Source IP address	Specify a source IP address and mask for the portal-free rule.
Mask	

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Source MAC</td><td>Specify a source MAC address for the portal-free rule.
IMPORTANT:
If you configure both the source IP address and the source MAC address, make sure that the mask of the specified source IP address is 255.255.255.255. Otherwise, the specified source MAC address will not take effect.</td></tr>
<tr><td>Source-VLAN</td><td>Specify a source VLAN for the portal-free rule.
IMPORTANT:
If you configure both a source interface and a source VLAN for a portal-free rule, make sure that the source interface is in the source VLAN. Otherwise, the portal-free rule will not take effect.</td></tr>
<tr><td>Destination IP Address</td><td rowspan="2">Specify the destination IP address and mask of the portal-free rule.</td></tr>
<tr><td>Mask</td></tr>
</table>

Portal authentication configuration examples

Configuring direct portal authentication

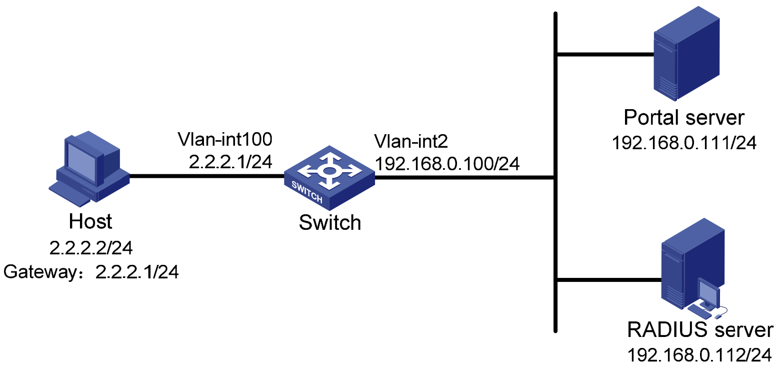
Network requirements

As shown in Figure 379, the host is assigned a public network IP address either manually or through DHCP.

Configure the switch to perform direct portal authentication for users on the host. Before passing portal authentication, users can access only the portal server. After passing portal authentication, they can access Internet resources.

Use the IMC server as the RADIUS server for user authentication, authorization and accounting.

Figure 379 Network diagram



Configuration procedure

Make sure that the IP address of the access device added on the portal server is the IP address of the interface connected to the host (2.2.2.1 in this example), and the IP address group associated with the access device is the subnet where the host resides (2.2.2.0/24 in this example).

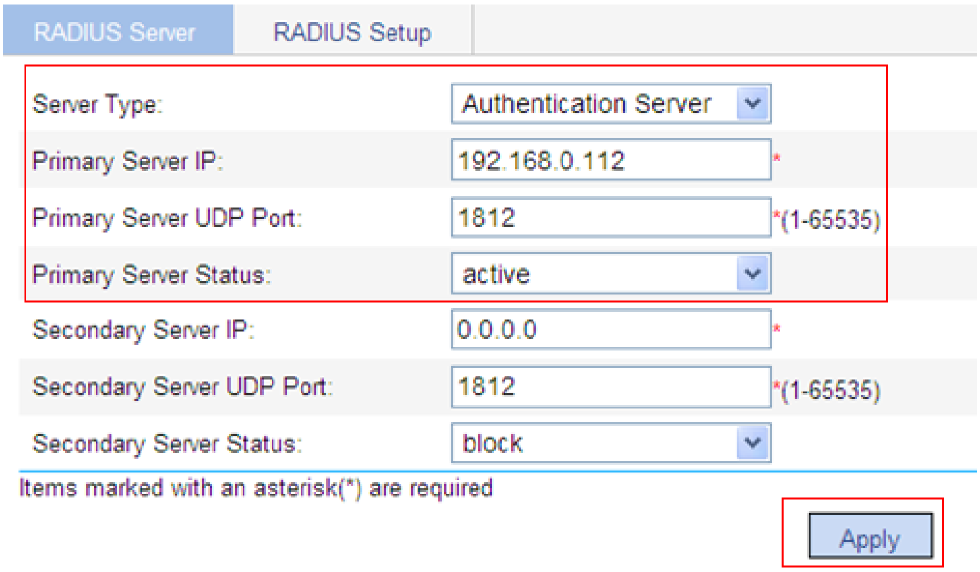
Configure IP addresses for the host, switch, and servers as shown in Figure 379 and make sure that they can reach each other.

Configure the RADIUS server properly to provide authentication and accounting functions for users.

Perform the following configuration on the switch to implement direct portal authentication:

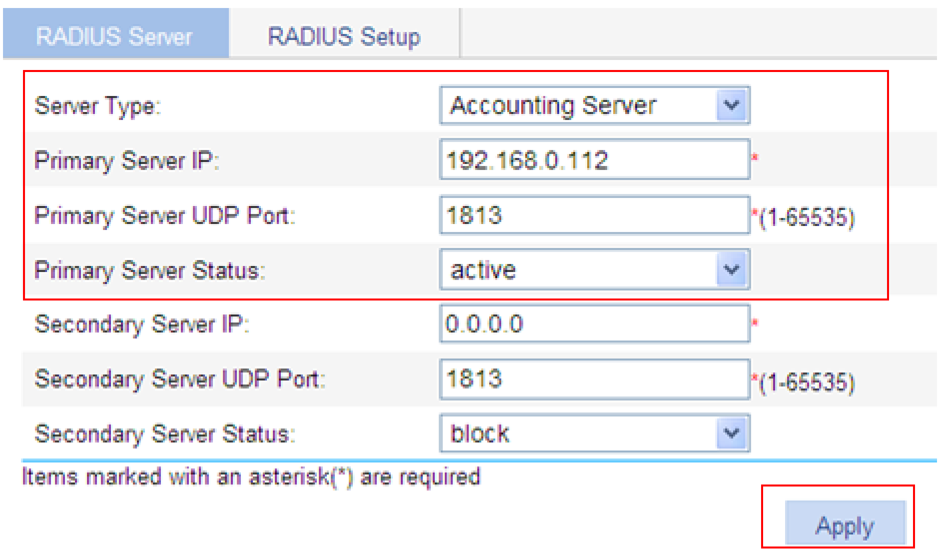
1. Configure the RADIUS authentication server:
   a. Select **Authentication** > **RADIUS** from the navigation tree.
      The RADIUS server configuration page appears, as shown in Figure 380.
   b. Select **Authentication Server** as the server type, enter the IP address **192.168.0.112** and port number **1812**, select **active** from the **Primary Server Status** list, and click **Apply**.

Figure 380 Configuring the RADIUS authentication server



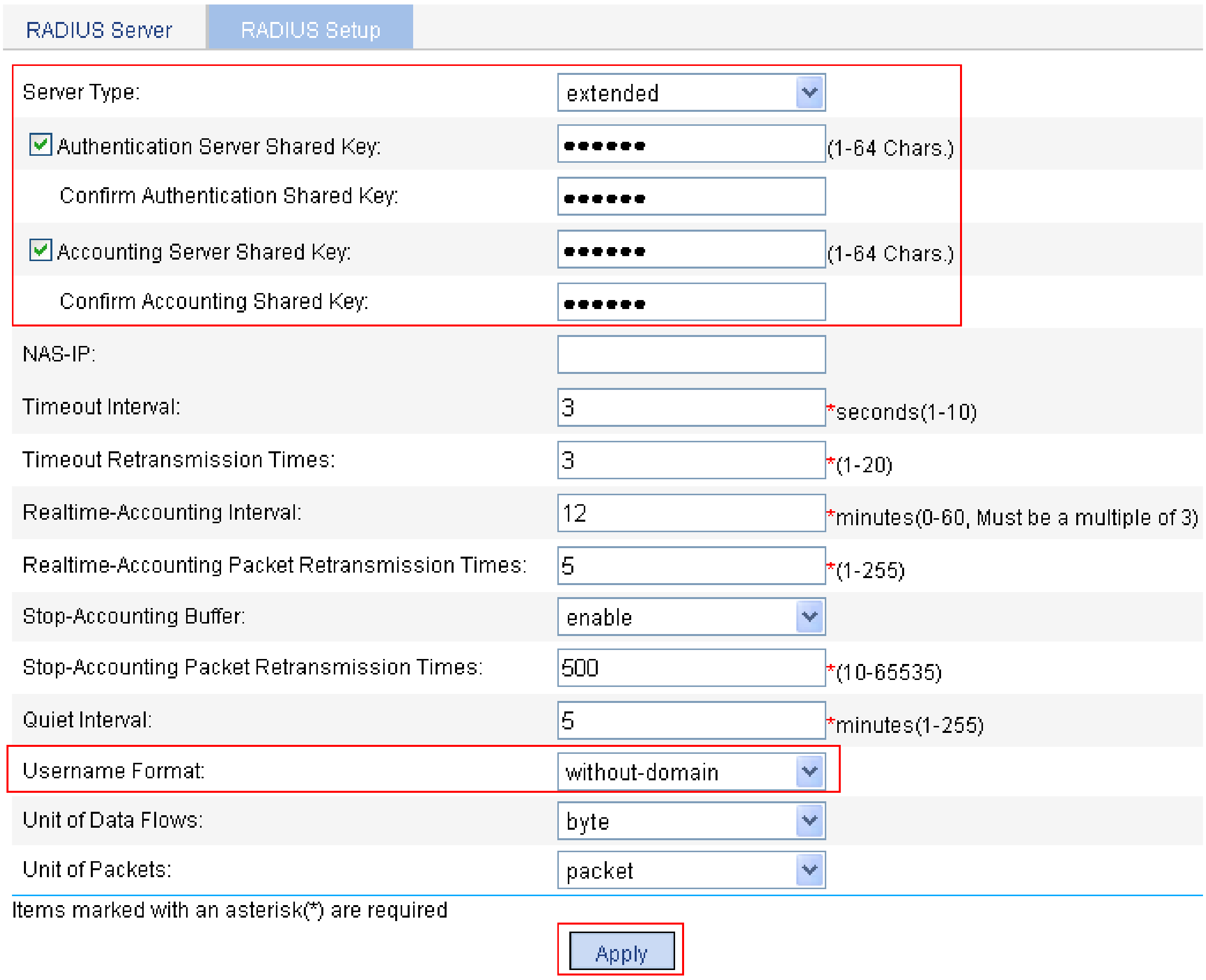
2. Configure a RADIUS accounting server:
   On the RADIUS server configuration page, select **Accounting Server** as the server type, and enter the IP address **192.168.0.112** and port number **1813**, select **active** from the **Primary Server Status** list, and click **Apply**.

Figure 381 Configuring a RADIUS accounting server



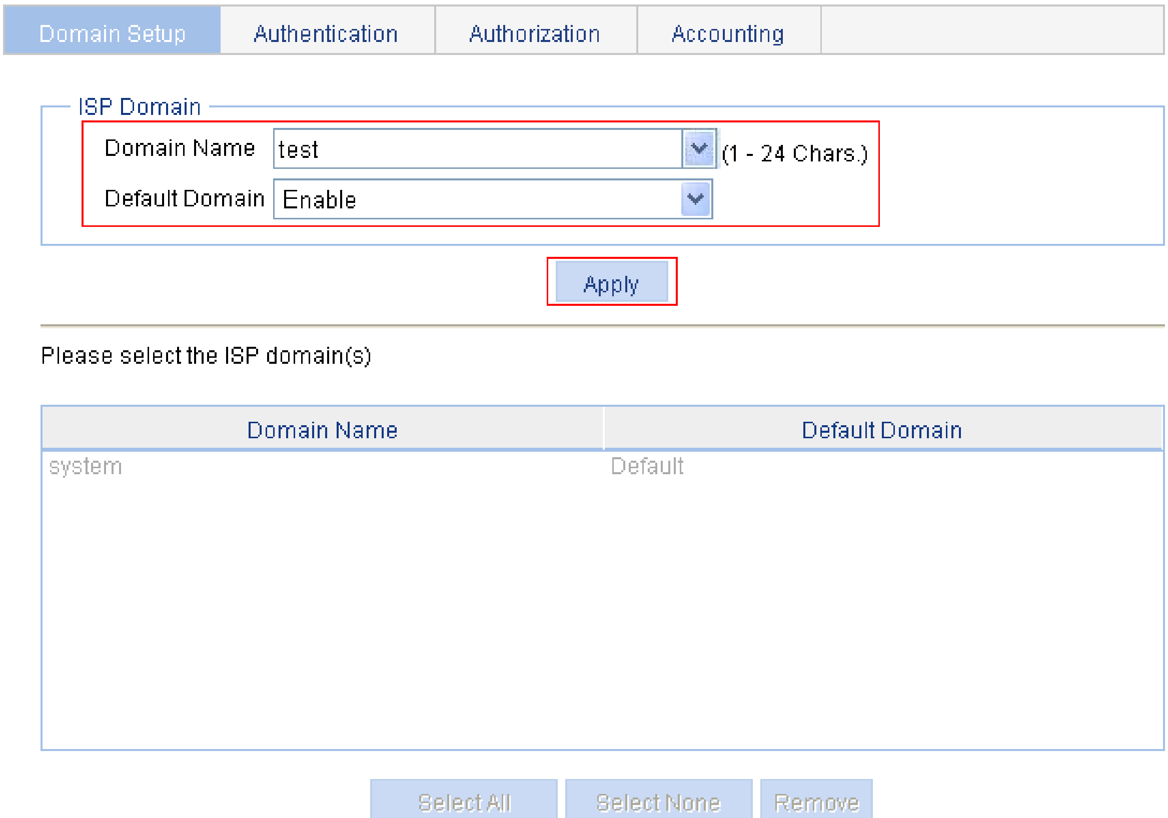
3. Configure RADIUS scheme **system** for exchanges between the device and the RADIUS servers:
   a. Click the **RADIUS Setup** tab.
   b. Select **extended** as the server type.
   c. Select the **Authentication Server Shared Key** box, enter the key **expert**, and then enter the key again in the **Confirm Authentication Shared Key** field.
   d. Select the **Accounting Server Shared Key** box, enter the key **expert**, and then enter the key again in the **Confirm Accounting Shared Key** field.
   e. Select **without-domain** as the username format.
   f. Click **Apply**.

Figure 382 Configuring the RADIUS scheme



4. Configure AAA:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. On the **Domain Setup** tab, enter the domain name **test**, select **Enable** for the **Default Domain** field, and click **Apply**.

Figure 383 Creating an ISP domain

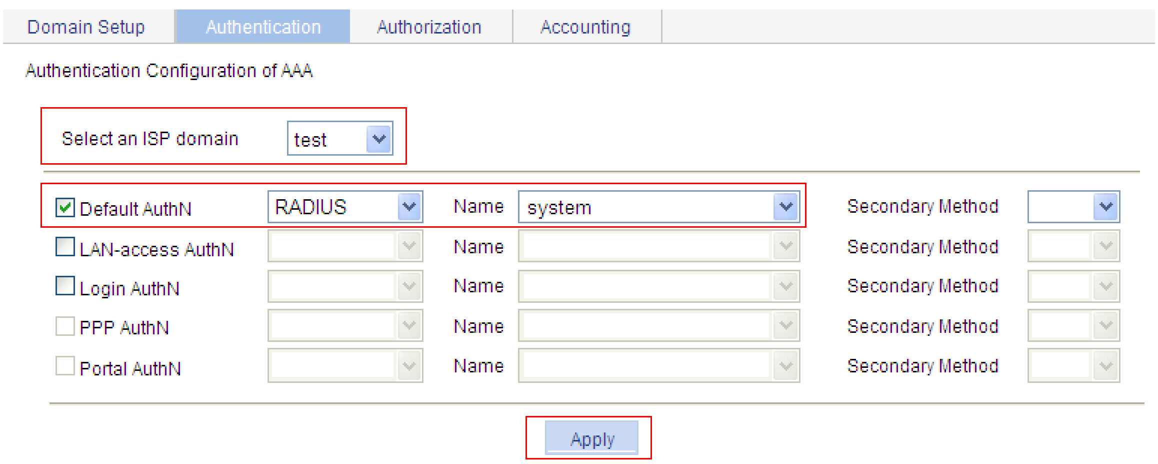


c. On the **Authentication** tab, select the ISP domain **test**, select the **Default AuthN** box, select **RADIUS** from the **Default AuthN** list, select **system** from the **Name** list to use it as the authentication scheme, and click **Apply**.

   A configuration progress dialog box appears.

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

Figure 384 Configuring the authentication method for the ISP domain

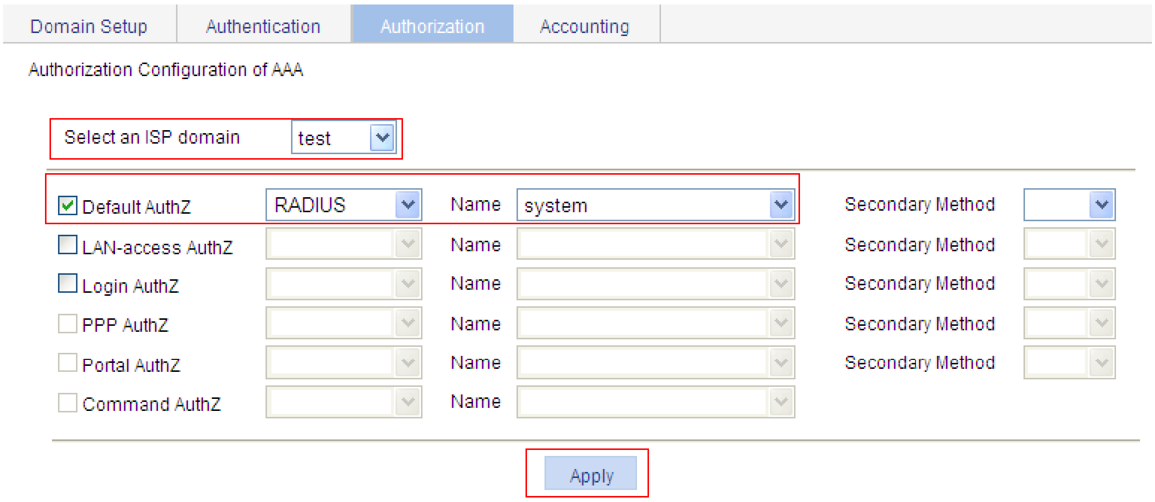


e. On the **Authorization** tab, select the ISP domain **test**, select the **Default AuthZ** box, select **RADIUS** from the **Default AuthZ** list, select **system** from the **Name** list to use it as the authorization scheme, and click **Apply**.

A configuration progress dialog box appears.

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

Figure 385 Configuring the authorization method for the ISP domain

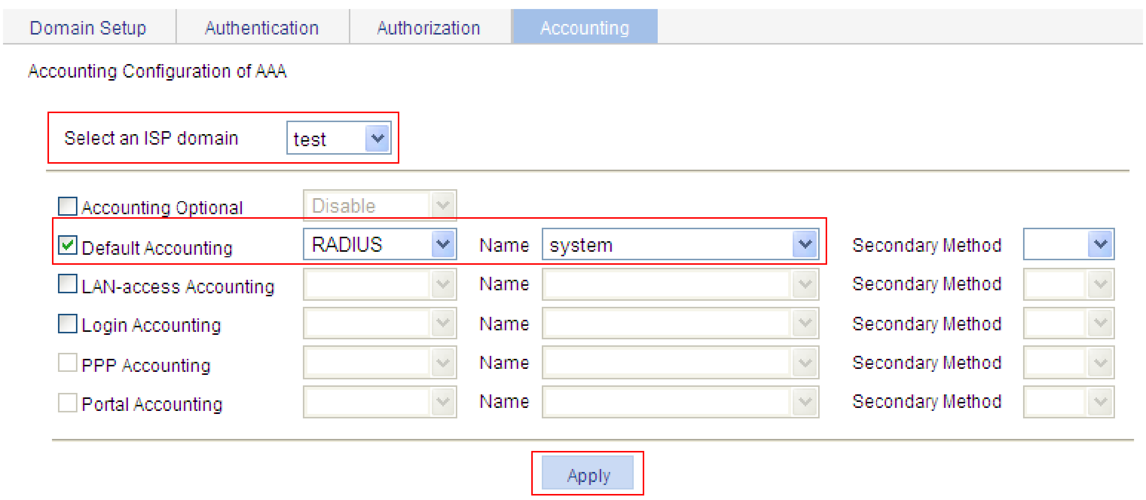


g. On the **Accounting** tab, select the ISP domain **test**, select the **Default Accounting** box, select **RADIUS** from **Default Accounting** list, select **system** from the **Name** list to use it as the accounting scheme, and click **Apply**.

   The configuration progress dialog box appears.

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

Figure 386 Configuring the accounting method for the ISP domain



5. Configure Layer 3 portal authentication:

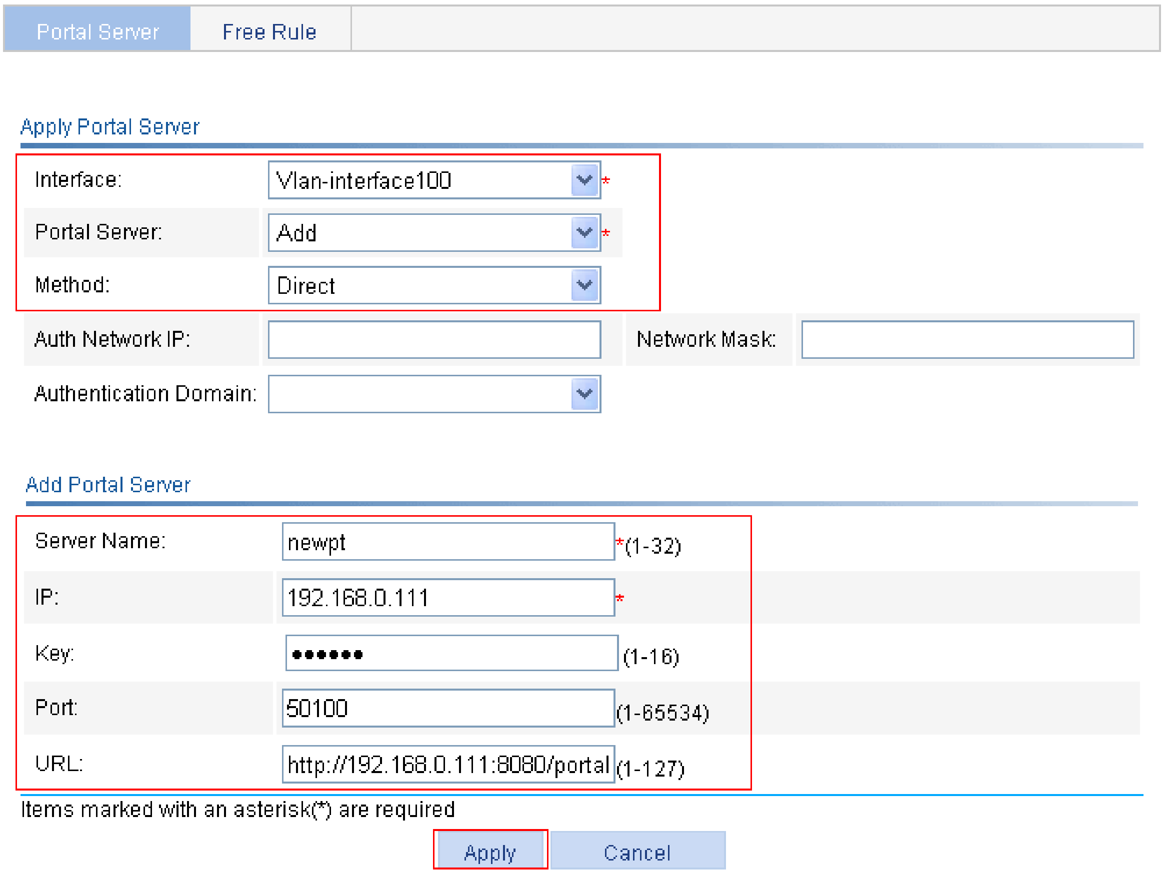
   a. From the navigation tree select **Authentication** > **Portal**.

      The portal server configuration page appears.

   b. In the **Portal Application: Layer 3 Interfaces** area, click **Add**.

   c. On the page that appears, select the interface **Vlan-interface100**, select **Add** for **Portal Server** to add a portal server, select the **Direct** portal authentication mode, enter the portal server name **newpt**, the portal server IP address **192.168.0.111**, the shared key **portal**, the port number **50100**, and the redirection URL **http://192.168.0.111:8080/portal** for portal authentication, and click **Apply**.

Figure 387 Applying the portal server to a Layer 3 interface

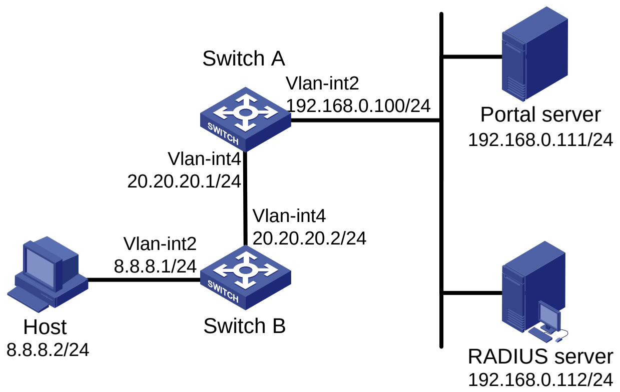


Configuring cross-subnet portal authentication

Network requirements

As shown in Figure 388, configure Switch A to perform cross-subnet portal authentication for users. Before passing portal authentication, the host can access only the portal server. After passing portal authentication, the host can access Internet resources. Use the IMC server as the RADIUS server for user authentication, authorization, and accounting.

Figure 388 Network diagram



Configuration procedure

Make sure that the IP address of the access device added on the portal server is the IP address of the interface connected to the host (20.20.20.1 in this example), and the IP address group associated with the access device is the subnet where the host resides (8.8.8.0/24 in this example).

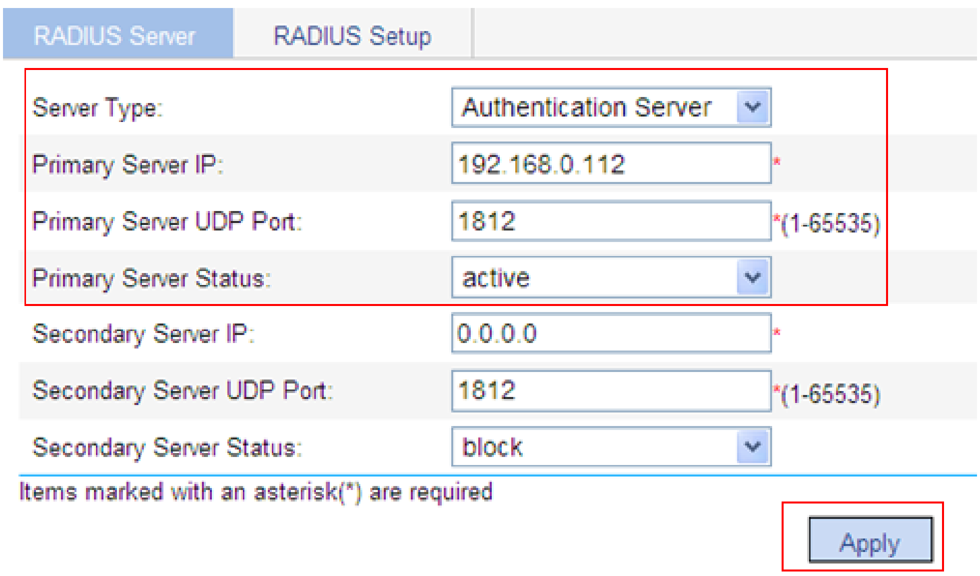
Assign IP addresses to the host, switches, and servers as shown in Figure 388 and make sure that they can reach each other.

Configure the RADIUS server properly to provide authentication and accounting functions for users.

Perform the following configuration on Switch A to implement cross-subnet portal authentication:

1. Configure the RADIUS authentication server:
   a. Select **Authentication** > **RADIUS** from the navigation tree.
      The RADIUS server configuration page appears, as shown in Figure 389.
   b. Select **Authentication Server** as the server type, enter the IP address **192.168.0.112** and port number **1812**, select **active** from the **Primary Server Status** list, and click **Apply**.

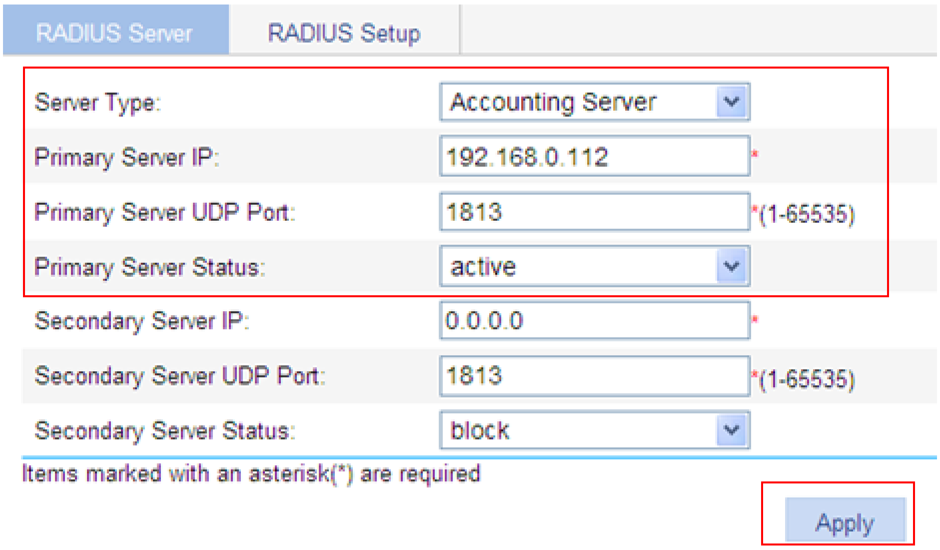
Figure 389 Configuring the RADIUS authentication server



2. Configure a RADIUS accounting server:

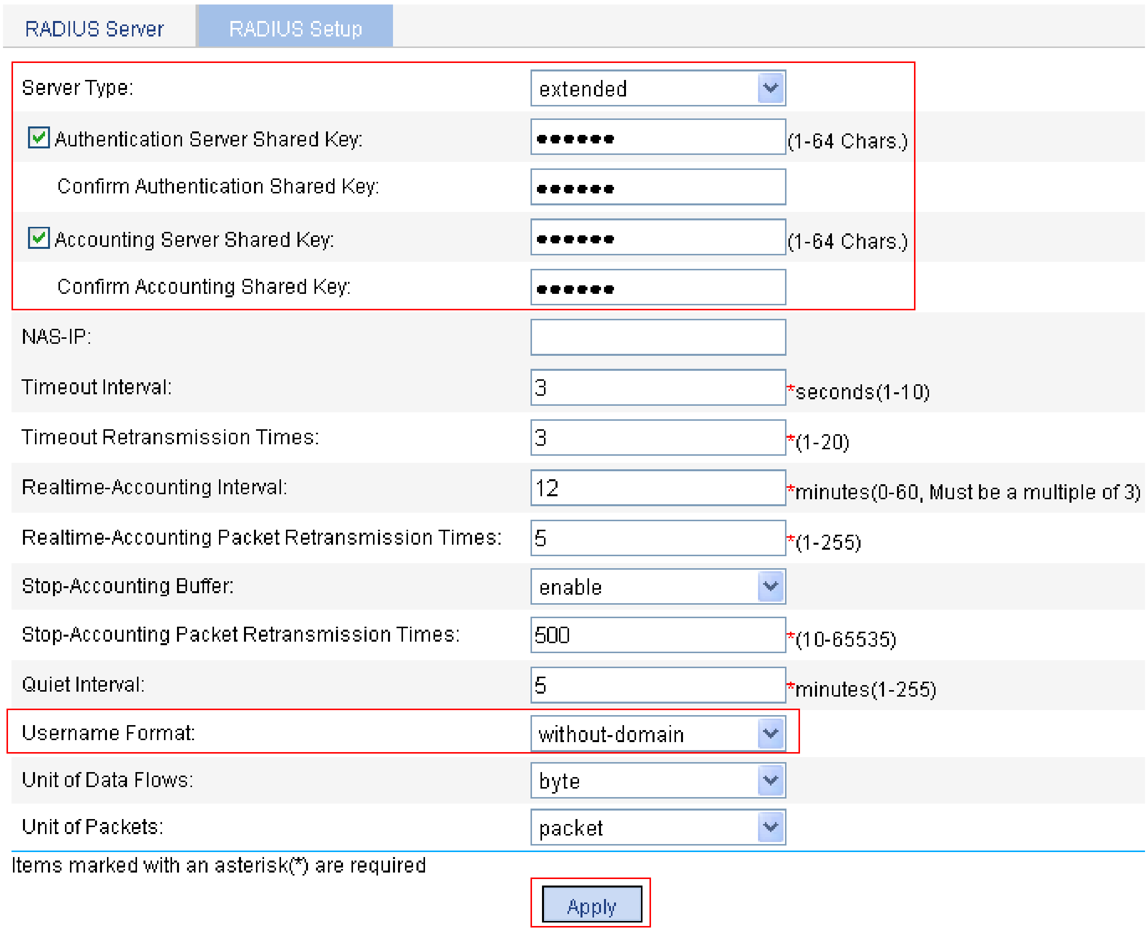
On the RADIUS server configuration page, select **Accounting Server** as the server type, and enter the IP address **192.168.0.112** and port number **1813**, select **active** from the **Primary Server Status** list, and click **Apply**.

Figure 390 Configuring a RADIUS accounting server



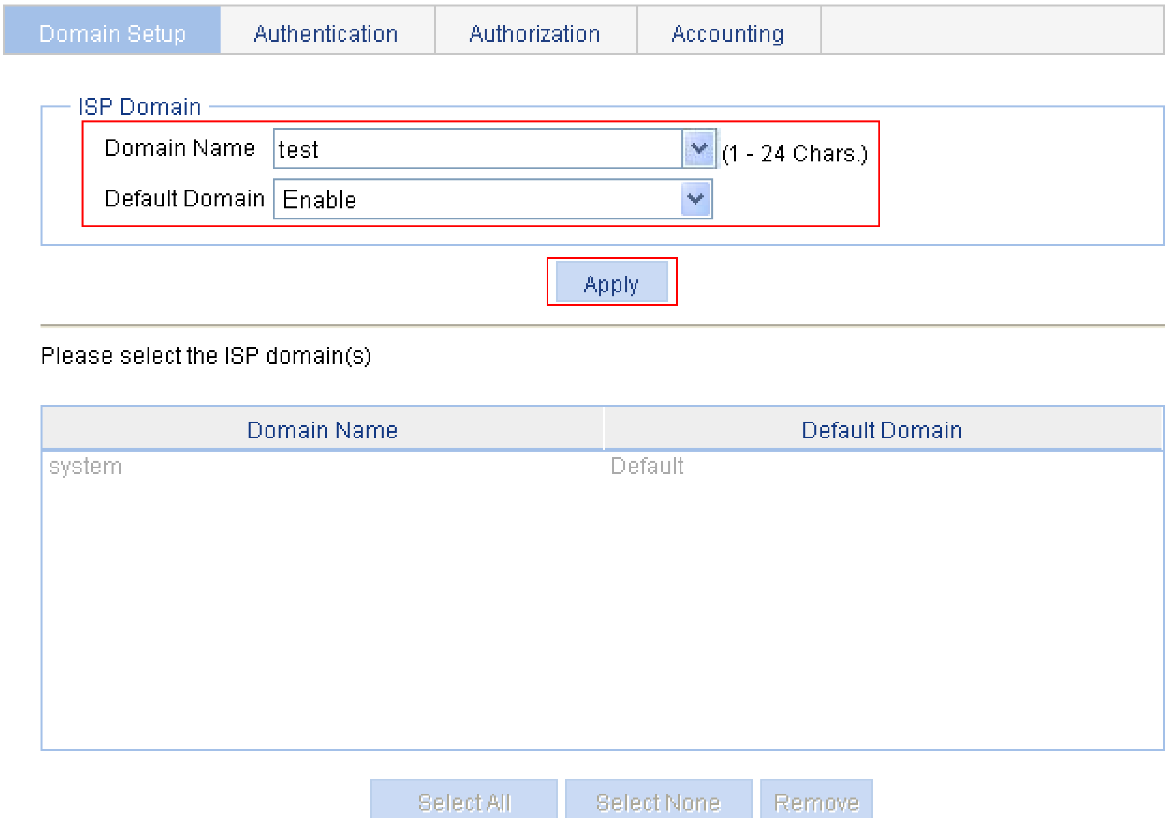
3. Configure RADIUS scheme **system** for exchanges between the device and the RADIUS servers:
   a. Click the **RADIUS Setup** tab.
   b. Select **extended** as the server type.
   c. Select the **Authentication Server Shared Key** box, enter the key **expert**, and then enter the key again in the **Confirm Authentication Shared Key** field.
   d. Select the **Accounting Server Shared Key** box, enter the key **expert**, and then enter the key again in the **Confirm Accounting Shared Key** field.
   e. Select **without-domain** as the username format.
   f. Click **Apply**.

Figure 391 Configuring the RADIUS scheme



4. Configure AAA:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. On the **Domain Setup** tab, enter the domain name **test**, select **Enable** for the **Default Domain** field, and click **Apply**.

Figure 392 Creating an ISP domain

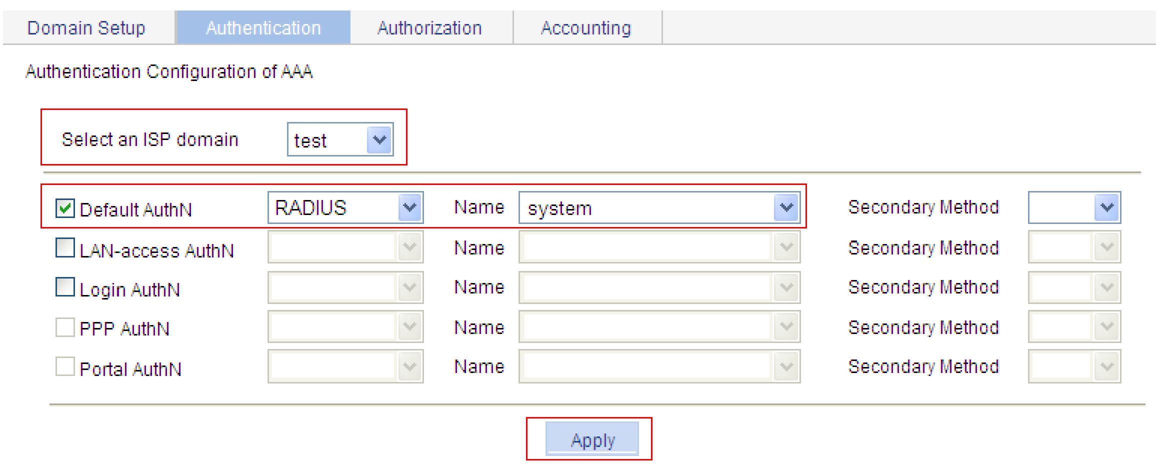


c. On the **Authentication** tab, select the ISP domain **test**, select the **Default AuthN** box, select **RADIUS** from the **Default AuthN** list, select **system** from the **Name** list to use it as the authentication scheme, and click **Apply**.

A configuration progress dialog box appears.

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

Figure 393 Configuring the authentication method for the ISP domain

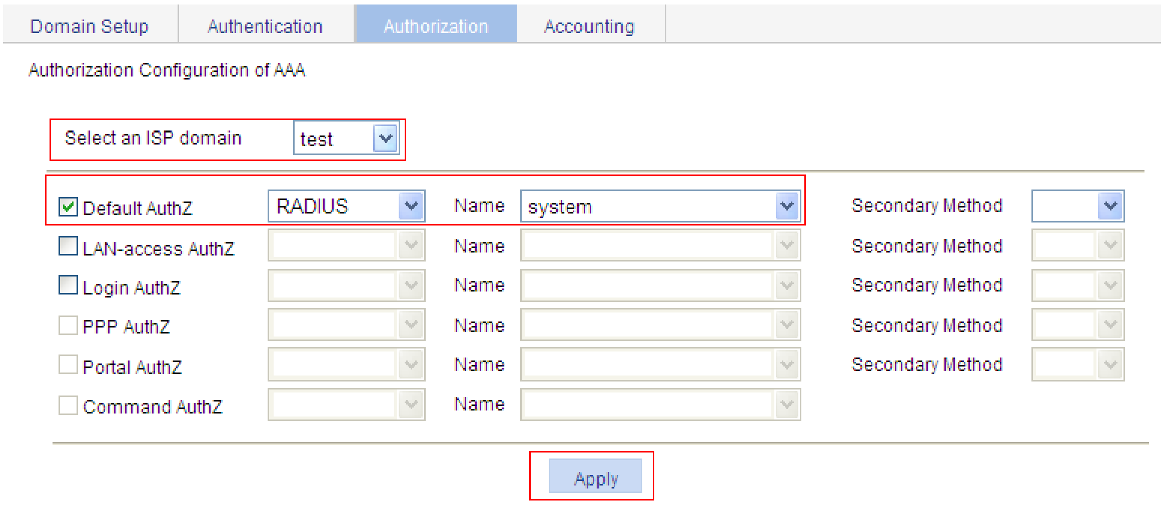


e. On the **Authorization** tab, select the ISP domain **test**, select the **Default AuthZ** box, select **RADIUS** from the **Default AuthZ** list, select **system** from the **Name** list to use it as the authorization scheme, and click **Apply**.

A configuration progress dialog box appears.

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

Figure 394 Configuring the authorization method for the ISP domain

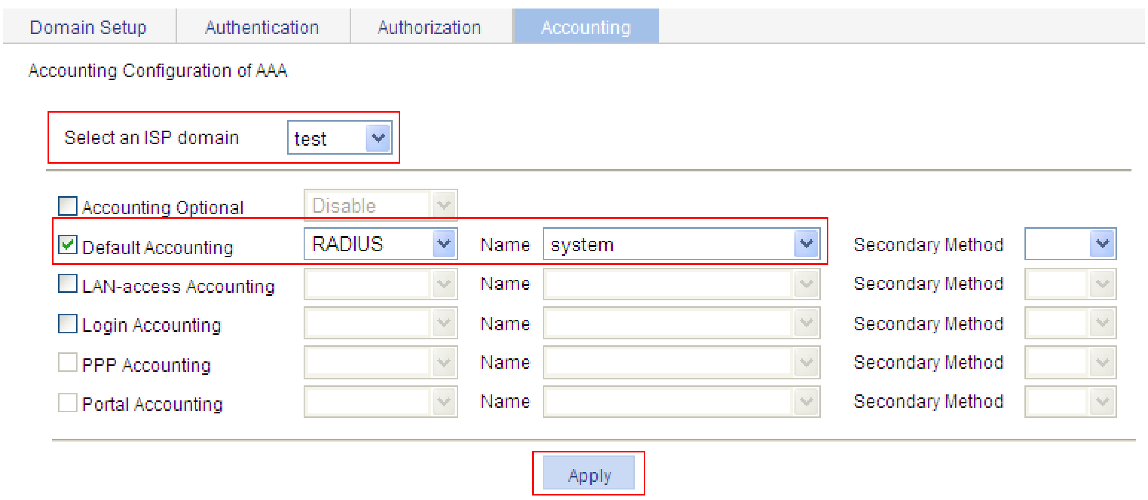


g. On the **Accounting** tab, select the ISP domain **test**, select the **Default Accounting** box, select **RADIUS** from **Default Accounting** list, select **system** from the **Name** list to use it as the accounting scheme, and click **Apply**.

The configuration progress dialog box appears.

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

Figure 395 Configuring the accounting method for the ISP domain



5. Configure Layer 3 portal authentication:

a. Select **Authentication** > **Portal** from the navigation tree.

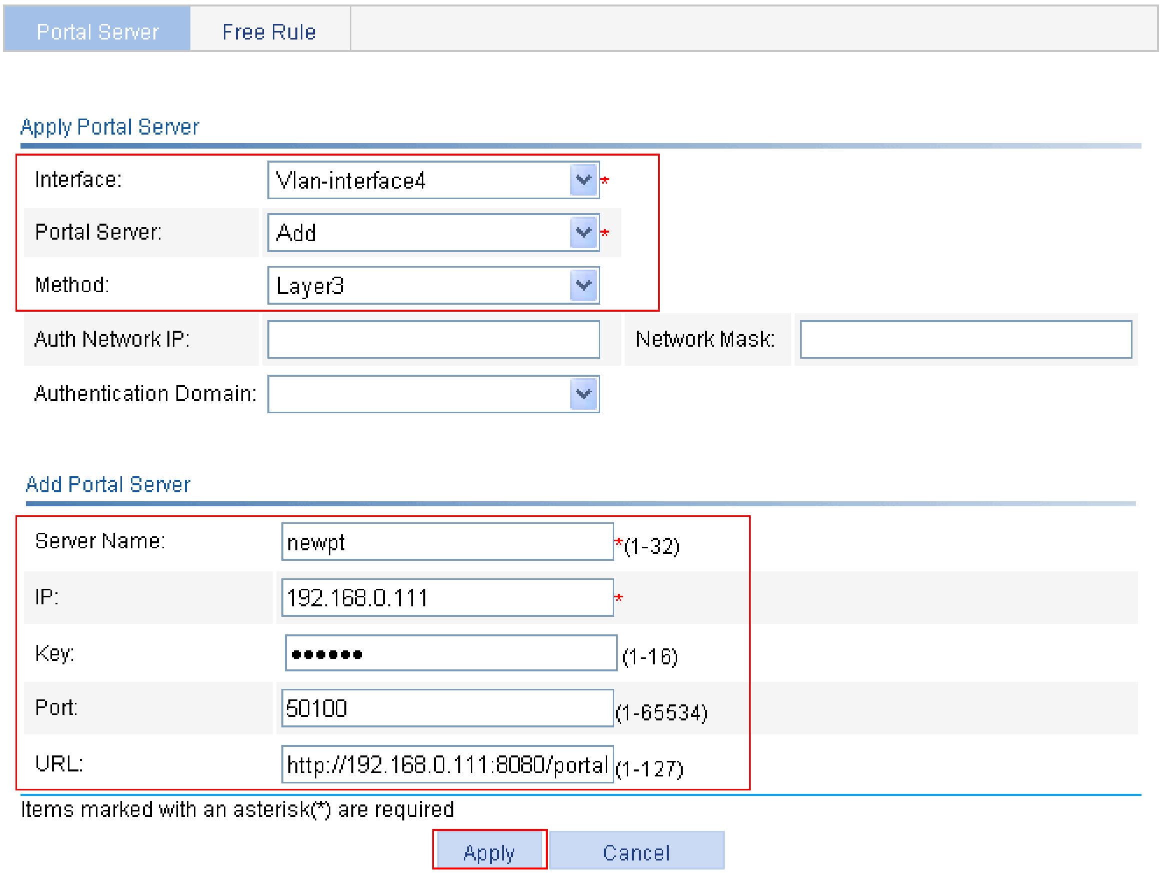
The portal server configuration page appears.

b. In the **Portal Application: Layer 3 Interfaces** area, click **Add**.

c. On the page that appears, select the interface **Vlan-interface4**, select **Add** for **Portal Server** to add a portal server, select the **Layer3** portal authentication mode, enter the portal server name **newpt**, the portal server IP address **192.168.0.111**, the shared key **portal**, the port number

50100, and the redirection URL **http://192.168.0.111:8080/portal** for portal authentication, and click **Apply**.

Figure 396 Applying the portal server to a Layer 3 interface



On Switch B, you must configure a default route to subnet 192.168.0.0/24 with the next hop as 20.20.20.1. (Details not shown.)

Configuring RADIUS

RADIUS is a protocol for implementing Authentication, Authorization, and Accounting (AAA). For more information about AAA, see "Configuring AAA."

Overview

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model. It can protect networks against unauthorized access and is often used in network environments with requirements for both high security and remote user access.

RADIUS uses UDP as the transport protocol. It uses UDP port 1812 for authentication and UDP port 1813 for accounting.

RADIUS was originally designed for dial-in user access. With the addition of new access methods, RADIUS has been extended to support additional access methods, such as Ethernet and ADSL. RADIUS provides access authentication and authorization services, and its accounting function collects and records network resource usage information.

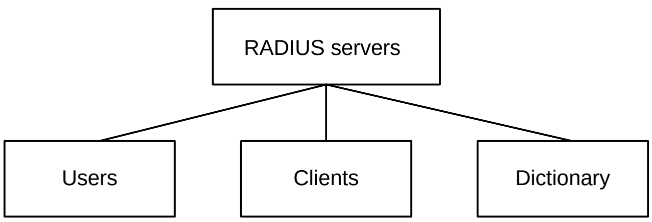
Client/Server model

The RADIUS client runs on the NASs located throughout the network. It passes user information to RADIUS servers and acts on the responses to, for example, reject or accept user access requests.

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 user access control information (for example, rejecting or accepting the user access request) to the clients.

In general, the RADIUS server maintains the following databases: Users, Clients, and Dictionary.

Figure 397 RADIUS server databases



- **Users**—Stores user information, such as the usernames, passwords, applied protocols, and IP addresses.
- **Clients**—Stores information about RADIUS clients, such as shared keys and IP addresses.
- **Dictionary**—Stores RADIUS protocol attributes and their values.

Security and authentication mechanisms

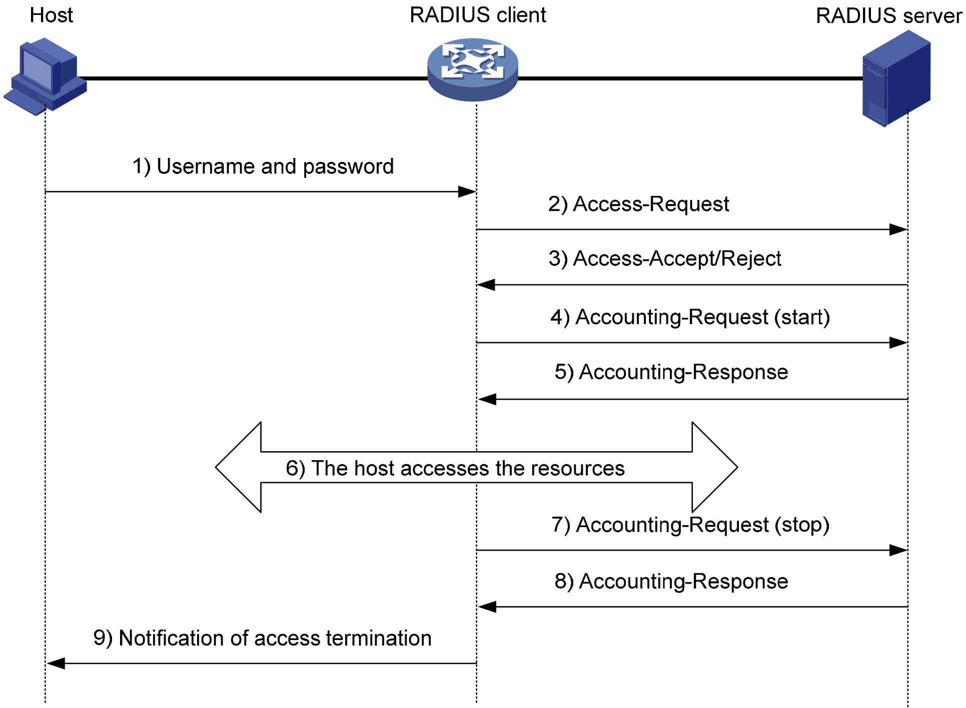
A RADIUS client and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords that are exchanged between them. The keys are never transmitted over the network. This security mechanism improves the security of RADIUS communication and prevents user passwords from being intercepted on insecure networks.

A RADIUS server supports multiple user authentication methods. A RADIUS server can also act as the client of another AAA server to provide authentication proxy services.

Basic RADIUS message exchange process

Figure 398 illustrates the interactions between the host, the RADIUS client, and the RADIUS server.

Figure 398 Basic RADIUS message exchange process



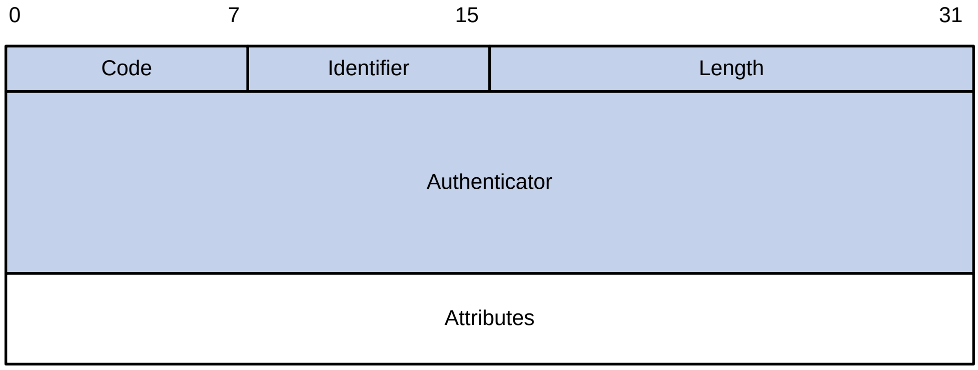
RADIUS operates in the following manner:

1. The host initiates a connection request that carries the user's 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, the server sends back an Access-Accept message containing the user's authorization information. If the authentication fails, the server 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 an acknowledgement (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 an acknowledgement (Accounting-Response) and stops accounting for the user.

RADIUS packet format

RADIUS uses UDP to transmit messages. To ensure smooth message exchange between the RADIUS server and the client, RADIUS uses a series of mechanisms, including the timer management mechanism, the retransmission mechanism, and the backup server mechanism. Figure 399 shows the RADIUS packet format.

Figure 399 RADIUS packet format



Descriptions of the fields are as follows:

- The Code field (1 byte long) indicates the type of the RADIUS packet. Table 117 gives the main values and their meanings.

Table 117 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, the authentication succeeds, and 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 authentication fails, and the server 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 or stop accounting for the user. The Acct-Status-Type attribute in the packet indicates whether to start or stop accounting.
5	Accounting-Response	From the server to the client. The server sends a packet of this type to notify the client that it has received the Accounting-Request and has successfully recorded the accounting information.

- The Identifier field (1 byte long) is used to match request packets and response packets and to detect duplicate request packets. Request and response packets of the same type have the same identifier.
- The Length field (2 bytes long) indicates the length of the entire packet, including the Code, Identifier, Length, Authenticator, and Attributes fields. Bytes beyond this length are considered padding and are ignored at the receiver. If the length of a received packet is less than this length, the packet is dropped. The value of this field is in the range 20 to 4096.

- The Authenticator field (16 bytes long) is used to authenticate responses from the RADIUS server and to encrypt user passwords. There are two types of authenticators: request authenticator and response authenticator.
- The Attributes field (variable in length) carries the specific authentication, authorization, and accounting information that defines the configuration details of the request or response. This field may contain multiple attributes, each with three sub-fields:
  - **Type**—(1 byte long) Type of the attribute. It is in the range of 1 to 255. Commonly used RADIUS attributes are defined in RFC 2865, RFC 2866, RFC 2867, and RFC 2868. Table 118 shows a list of the attributes.
  - **Length**—(1 byte long) Length of the attribute in bytes, including the Type, Length, and Value sub-fields.
  - Value—(Up to 253 bytes) Value of the attribute. Its format and content depend on the Type and Length sub-fields.

Table 118 Commonly used 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
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features

No.	Attribute	No.	Attribute
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

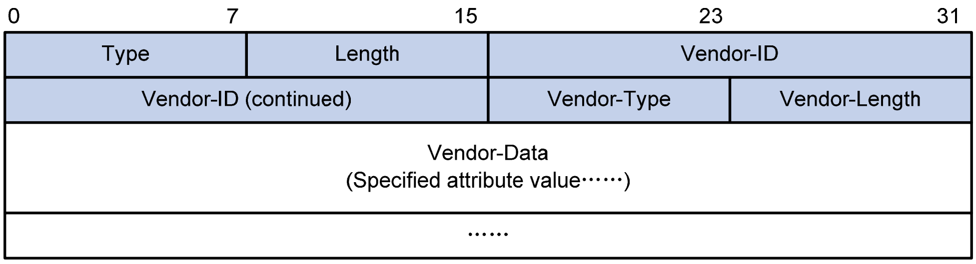
Extended RADIUS attributes

The RADIUS protocol features excellent extensibility. Attribute 26 (Vendor-Specific), an attribute defined in RFC 2865, allows a vendor to define extended attributes to implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple sub-attributes in the type-length-value (TLV) format in attribute 26 to provide extended functions. As shown in Figure 400, a sub-attribute encapsulated in attribute 26 consists of the following parts:

- **Vendor-ID**—Indicates the ID of the vendor. Its most significant byte is 0, and the other three bytes contains a code that is compliant to 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 400 Format of attribute 26



Protocols and standards

- 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*

Recommended RADIUS configuration procedure

The RADIUS scheme configured through the web interface is named **system**.

If the switch does not contain a RADIUS scheme named **system**, it automatically creates the scheme when you select **Authentication** > **RADIUS** to enter the RADIUS module.

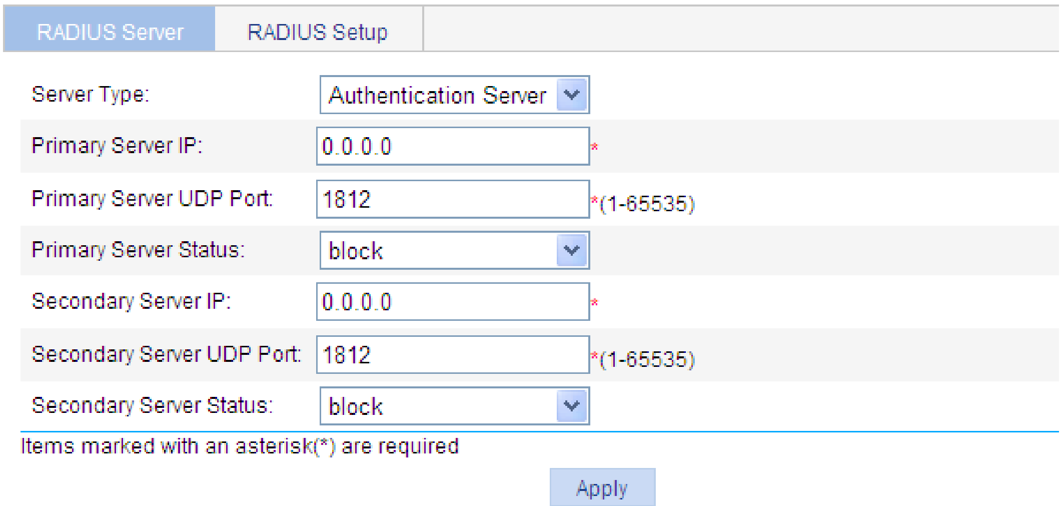
Step	Remarks
1. Configuring RADIUS authentication servers	(Required.) Configure the primary and secondary RADIUS authentication servers. By default, no RADIUS authentication server is configured. For more information about the configuration procedure, see "Configuring RADIUS servers."
2. Configuring RADIUS accounting servers	(Optional.) Configure the primary and secondary RADIUS accounting servers. By default, no RADIUS accounting server is configured. For more information about the configuration procedure, see "Configuring RADIUS servers."
3. Configuring RADIUS communication parameters	(Required.) Configure the parameters used for information exchange between the switch and RADIUS servers.

Configuring RADIUS servers

1. Select **Authentication** > **RADIUS** from the navigation tree.

   The RADIUS server configuration page appears.

Figure 401 RADIUS Server page



2. Configure the RADIUS server parameters as described in Table 119.
3. Click **Apply**.

Table 119 Configuration items

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 field displays **0.0.0.0**. To remove the previously configured primary server, enter **0.0.0.0**. 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 field displays **0.0.0.0**. To remove the previously configured secondary server, enter **0.0.0.0**. 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.

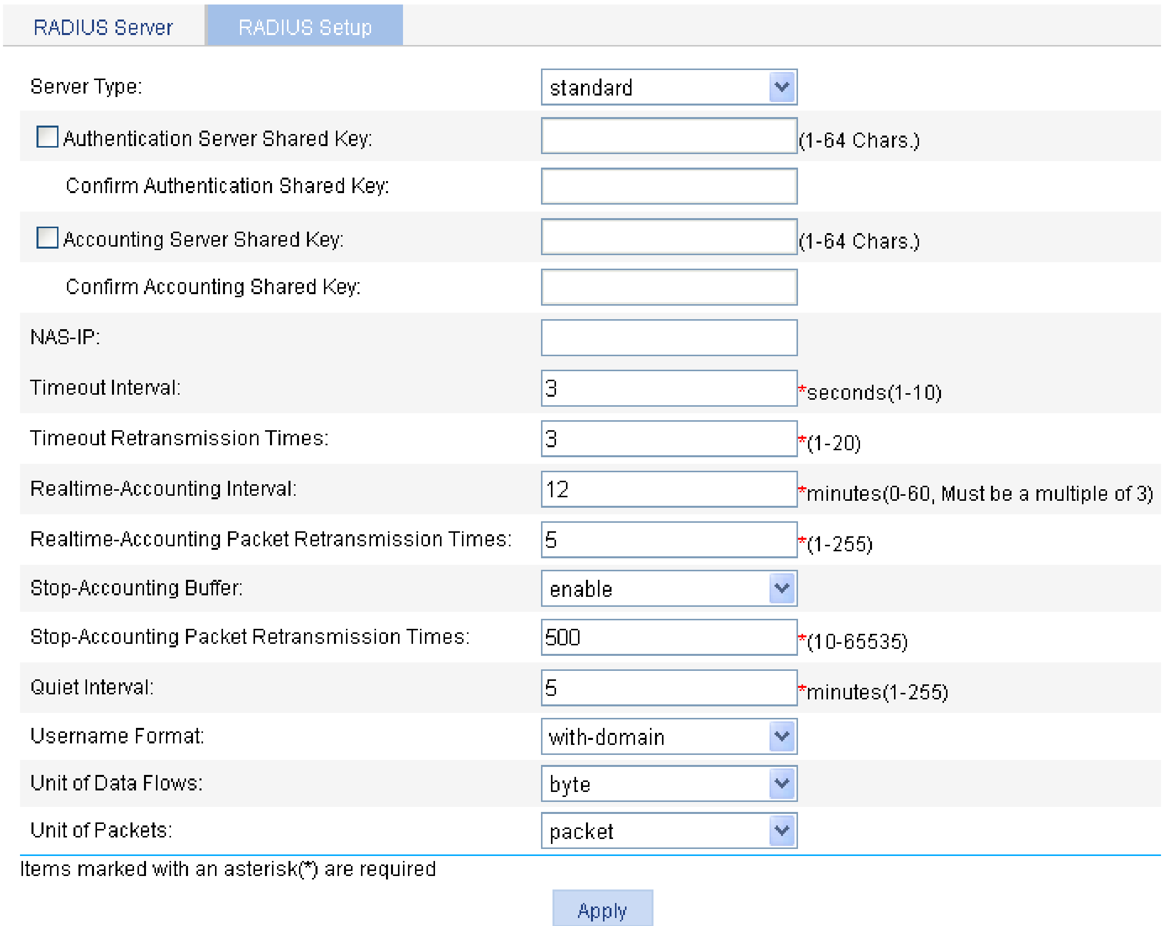
Item	Description
Secondary Server Status	Status of the secondary server, including: • **Active**—The server is working normally. • **Blocked**—The server is down. If the IP address of the secondary server is not specified or the specified IP address is to be removed, the status is **Blocked**.

Configuring RADIUS communication parameters

1. Select **Authentication** > **RADIUS** from the navigation tree, and then click the **RADIUS Setup** tab.

   The RADIUS parameter configuration page appears.

Figure 402 RADIUS Setup page



2. Configure the RADIUS communication parameters as described in Table 120.
3. Click **Apply**.

Table 120 Configuration items

Item	Description
Server Type	Specify the type of the RADIUS server supported by the switch, including: • **Extended**—Specifies an extended RADIUS server (offered by IMC). The RADIUS client and RADIUS server communicate using the proprietary RADIUS protocol and packet format. • **Standard**—Specifies a standard RADIUS server. The RADIUS client and RADIUS server communicate using the standard RADIUS protocol and packet format defined in RFC 2138/2139 or later.
Authentication Server Shared Key Confirm Authentication Shared Key	Specify and confirm the shared key for the authentication server. These two parameters must have the same values.
Accounting Server Shared Key Confirm Accounting Shared Key	Specify and confirm the shared key for the accounting server. These two parameters must have the same values.
NAS-IP	Specify the source IP address for the switch 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 switch.
Timeout Interval	Set the RADIUS server response timeout.
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 switch 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 121 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 switch.
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 RADIUS servers have to wait before being active

Item	Description
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 switch 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 switch to remove the domain name of a username before sending it to the RADIUS server. • **Without-domain**—Remove the domain name of a username that is to be sent to the RADIUS server. • **With-domain**—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 121 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

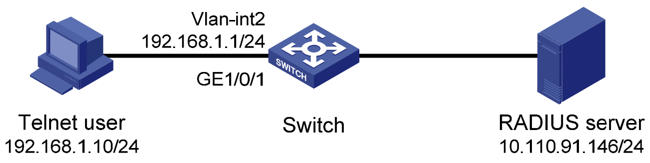
RADIUS configuration example

Network requirements

As shown in Figure 403, the RADIUS server runs on IMC. It contains the telnet usernames and passwords, and uses the default authentication port, default accounting port, and the shared key **expert** for packet exchange with the switch.

Configure the switch to implements RADIUS authentication and online time accounting for Telnet users, and to remove the domain name of a username before sending it to the RADIUS server.

Figure 403 Network diagram



Configuration procedure

1. Enable the Telnet server function, and configure the switch to use AAA for Telnet users. (Details not shown.)
2. Configure IP addresses for the interfaces. (Details not shown.)
3. Configure RADIUS scheme **system**:

   # Configure the RADIUS authentication server.

   a. Select **Authentication** > **RADIUS** from the navigation tree.

      The RADIUS server configuration page appears.

   b. Configure the following parameters, as shown in Figure 404.

      Select **Authentication Server** as the server type.

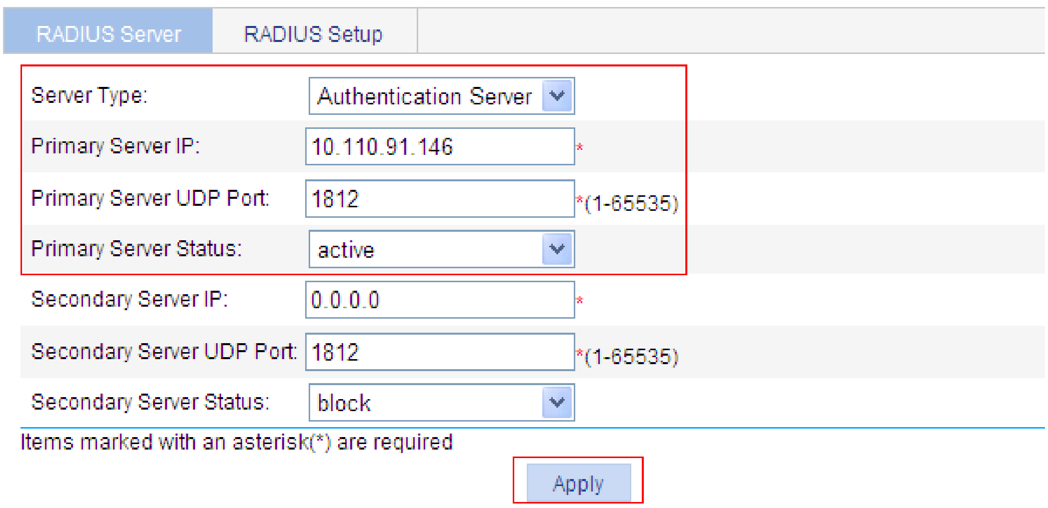
      Enter **10.110.91.146** as the IP address of the primary authentication server

      Enter **1812** as the UDP port of the primary authentication server.

      Select **active** as the primary server status.

   c. Click **Apply**.

Figure 404 Configuring the RADIUS authentication server



   # Configure the RADIUS accounting server.

   a. Select **Authentication** > **RADIUS** from the navigation tree.

      The RADIUS server configuration page appears.

   b. Configure the following parameters, as shown in Figure 405.

      Select **Accounting Server** as the server type.

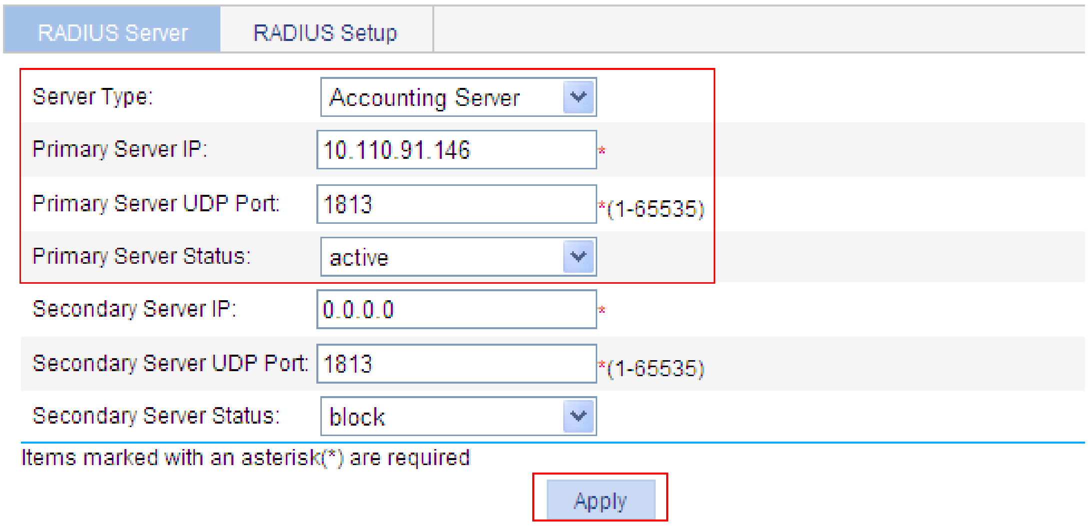
      Enter **10.110.91.146** as the IP address of the primary accounting server.

      Enter **1813** as the UDP port of the primary accounting server.

Select **active** as the primary server status.

c. Click **Apply**.

Figure 405 Configuring the RADIUS accounting server



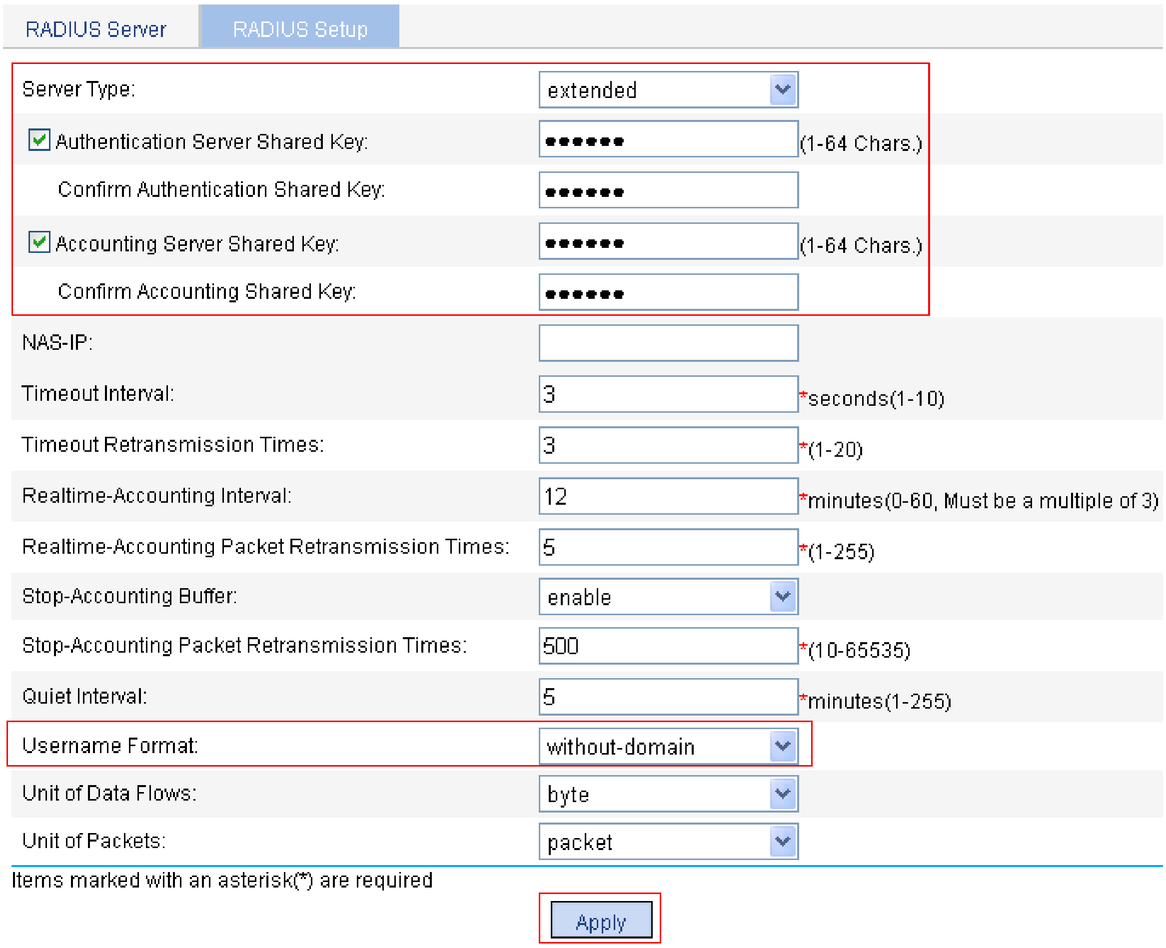
Configure the RADIUS communication parameters.

a. Select **Authentication** > **RADIUS** from the navigation tree and then click the **RADIUS Setup** tab.
   The RADIUS parameter configuration page appears.

b. Configure the following parameters, as shown in Figure 406.
   Select **extended** as the server type.
   Select the **Authentication Server Shared Key** box and enter **expert**.
   Enter **expert** in the **Confirm Authentication Shared Key** field.
   Select the **Accounting Server Shared Key** box and enter **expert**.
   Enter **expert** in the **Confirm Accounting Shared Key** field.
   Select **without-domain** for **Username Format**.

c. Click **Apply**.

Figure 406 Configuring RADIUS communication parameters



4. Configure AAA:

   # Create an ISP domain.

   a. Select **Authentication** > **AAA** from the navigation tree.

      The domain setup page appears.

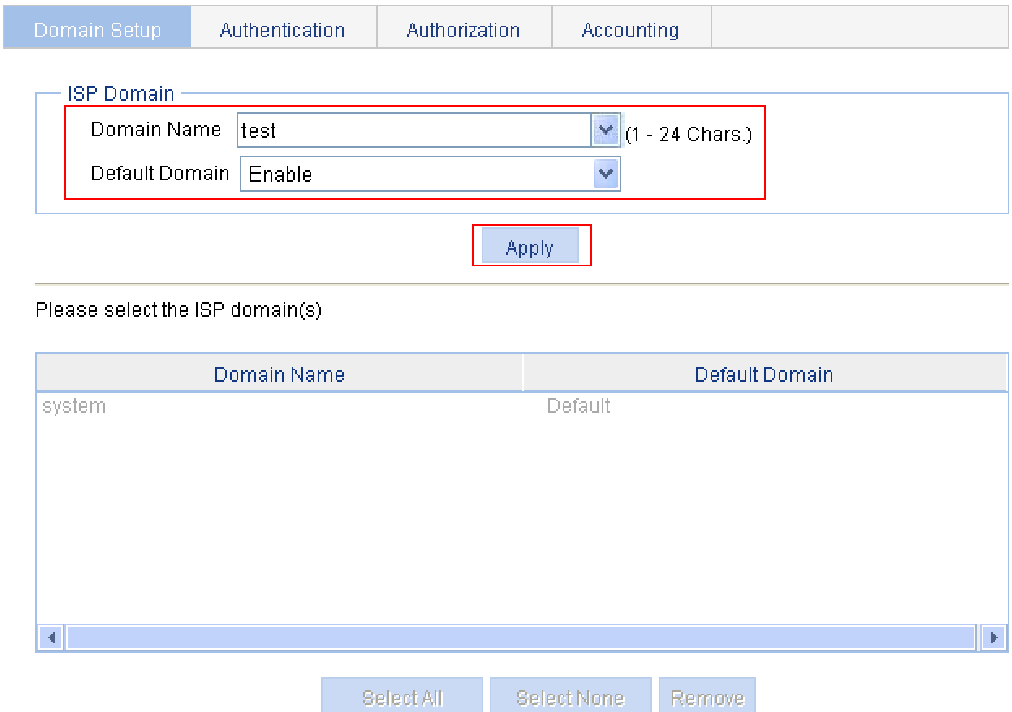
   b. Configure the following parameters, as shown in Figure 407.

      Enter **test** in the **Domain Name** field.

      Select **Enable** to use the domain as the default domain.

   c. Click **Apply**.

Figure 407 Adding an ISP domain



Configure the authentication method for the ISP domain.

a. Select **Authentication** > **AAA** from the navigation tree, and then click the **Authentication** tab.
b. Configure the following parameters, as shown in Figure 408.
   Select the domain name **test**.
   Select the **Default AuthN** box and then select **RADIUS** as the authentication mode.
   Select **system** from the **Name** list to use it as the authentication scheme.
c. Click **Apply**.
   A configuration progress dialog box appears, as shown in Figure 409.
d. After the configuration process is complete, click **Close**.

Figure 408 Configuring the authentication method for the ISP domain

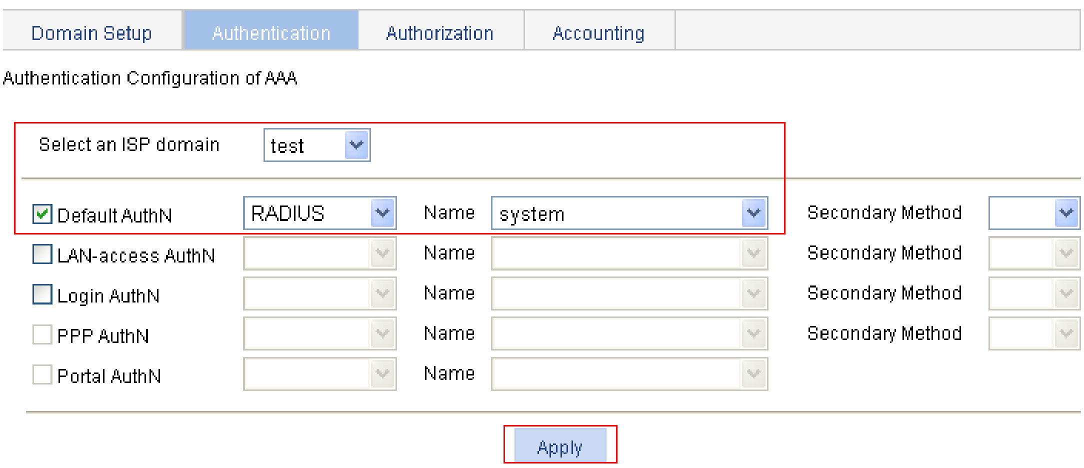
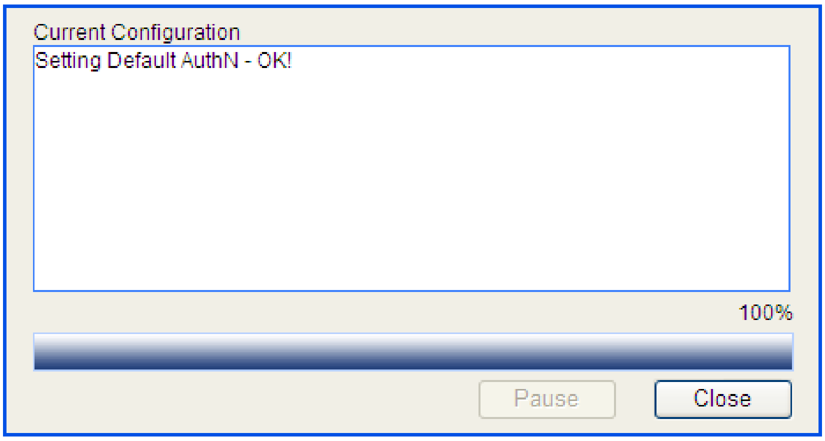


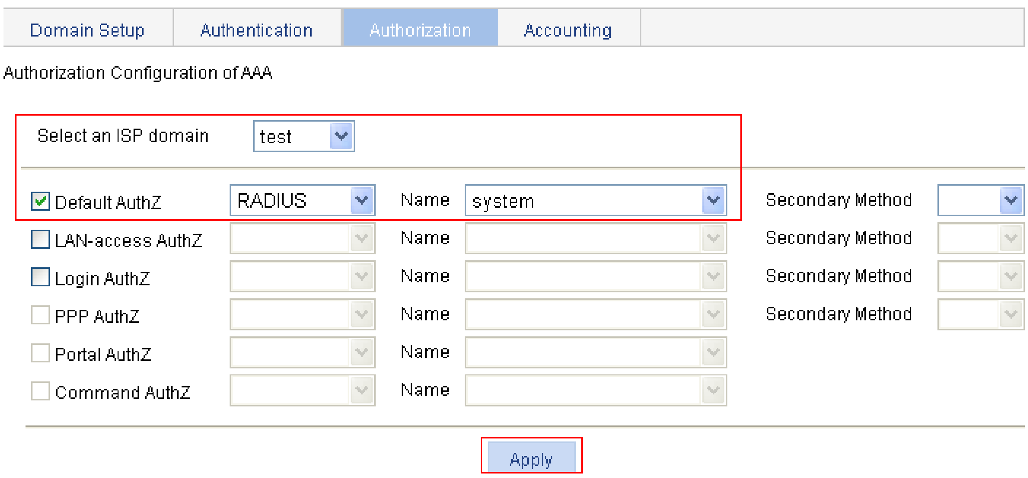
Figure 409 Configuration progress dialog box



Configure the authorization method for the ISP domain.

a. Select **Authentication** > **AAA** from the navigation tree, and then click the **Authorization** tab.
b. Configure the following parameters, as shown in Figure 410.
   Select the domain name **test**.
   Select the **Default AuthZ** box and then select **RADIUS** as the authorization mode.
   Select **system** from the **Name** list to use it as the authorization scheme.
c. Click **Apply**.
   A configuration progress dialog box appears.
d. After the configuration process is complete, click **Close**.

Figure 410 Configuring the authorization method for the ISP domain



Configure the accounting method for the ISP domain.

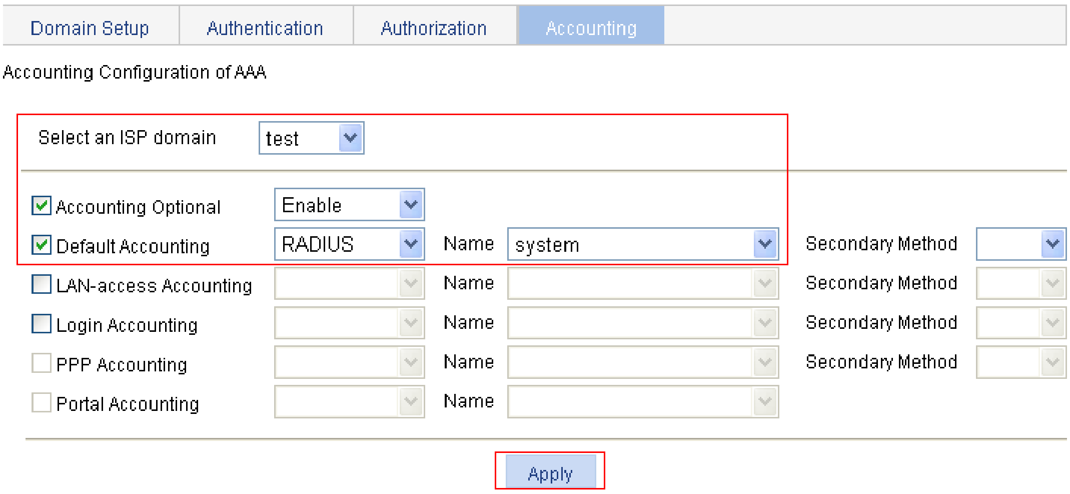
a. Select **Authentication** > **AAA** from the navigation tree, and then click the **Accounting** tab.
b. Configure the following parameters, as shown in Figure 411.
   Select the domain name **test**.
   Select the **Accounting Optional** box and then select **Enable**.
   Select the **Default Accounting** box and then select **RADIUS** as the accounting mode.
   Select **system** from the **Name** list to use it as the accounting scheme.

c. Click **Apply**.

A configuration progress dialog box appears.

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

Figure 411 Configuring the accounting method for the ISP domain



Configuration guidelines

When you configure the RADIUS client, follow these guidelines:

- The specified server status is dynamic information, which cannot be saved in the configuration file. After the switch reboots, the status of servers becomes **active**.
- Accounting for FTP users is not supported.
- If you remove the accounting server used for online users, the switch cannot send real-time accounting requests and stop-accounting messages of the users to the server, and the stop-accounting messages are not buffered locally.
- For the primary and secondary servers (assume only one secondary server exists) in a RADIUS scheme, the switch follows these rules to exchange packets with the servers:
  - If the primary server and secondary server are in the same state, the switch communicates with the primary server.
  - If both the primary server and secondary server are in **active** state, the switch communicates with the primary server. When the primary server becomes unreachable, the switch sets the server's status to **block** and turns to the secondary server for communication. When the quiet timer expires, the switch changes the status of the primary server to **active** while keeping the status of the secondary server unchanged. For authentication and authorization, the switch resumes the communication with the primary server if the primary server has come back into operation; in the case of accounting, however, the switch keeps communicating with the secondary server no matter whether the primary server recovers or not.
  - If one server is in **active** state and the other is in **block** state, the switch only tries to communicate with the server in **active** state, even if the server is unreachable.
  - If both the primary server and secondary server are in **block** state, the switch only communicates with the primary server. In this case, if the primary server is reachable, the switch changes the primary server's status to **active**. To use the secondary server for

communication, you need to manually change the status of the secondary server to **active**; otherwise, no primary/secondary server switchover will take place.

Configuring users and user groups

Overview

You can configure local users and user groups on the switch series.

A local user represents a set of user attributes configured on a switch (such as the user password, use type, 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 switch. For more information about local authentication, see "Configuring AAA."

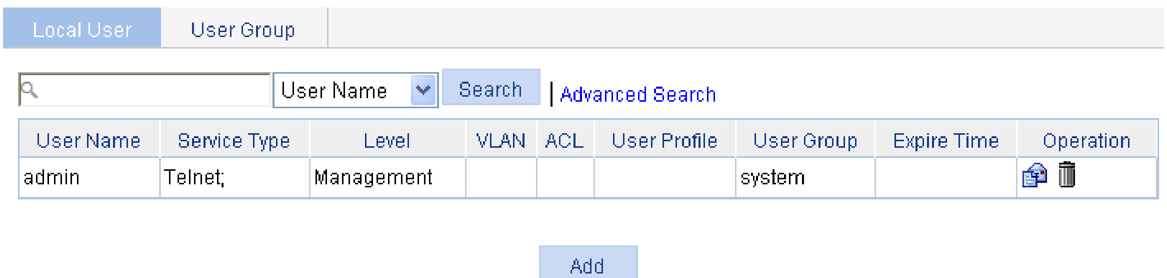
A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. All local users in a user group inherit the user attributes of the 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 a local user

1. Select **Authentication** > **Users** from the navigation tree to enter the **Local User** tab, which displays all local users.

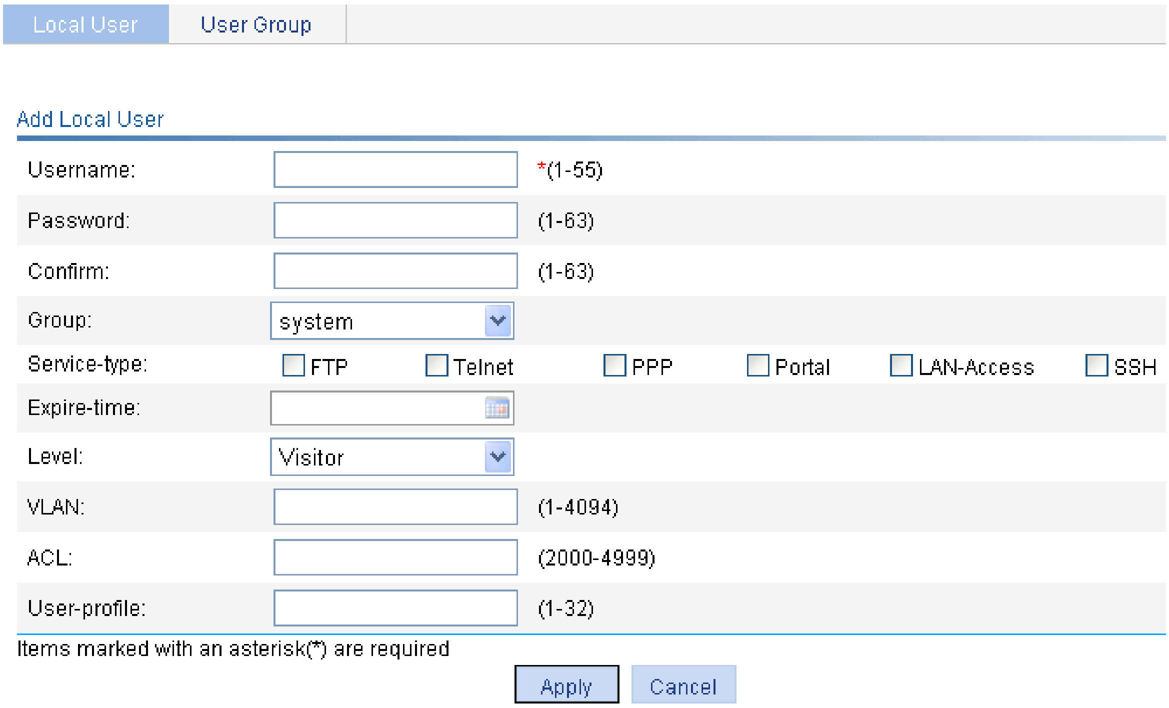
Figure 412 Local user list



2. Click **Add**.

   The page for adding a local user appears.

Figure 413 Local user configuration page



3. Configure the local user as described in Table 122.
4. Click **Apply**.

Table 122 Configuration items

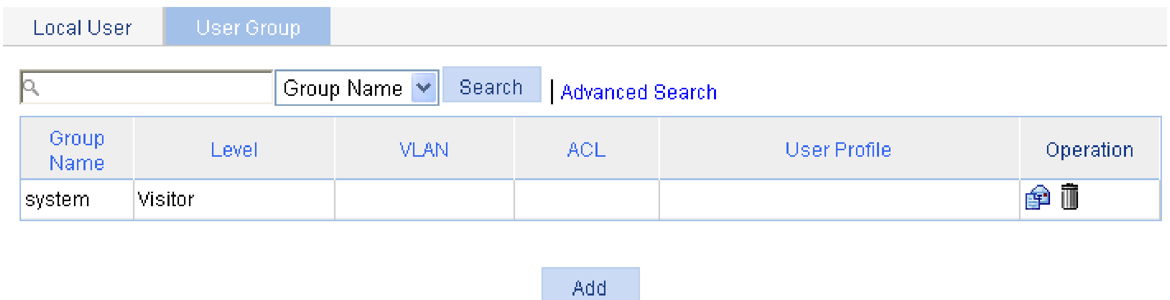
Item	Description
Username	Specify a name for the local user.
Password Confirm	Specify and confirm the password of the local user. The settings of these two fields must be the same. IMPORTANT: HP recommends that you do not specify a password starting with spaces because spaces at the beginning of the password string will be ignored, but they count at the user login page.
Group	Select a user group for the local user. For information about user group configuration, see "Configuring a user group."
Service-type	Select the service types for the local user to use, including FTP, Telnet, portal, LAN-access, and SSH. LAN-access primarily represents Ethernet users, such as 802.1X users. The switch series does not support PPP. IMPORTANT: 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 HH:MM:SS-YYYY/MM/DD format. When the NAS authenticates a local user with the expiration time argument configured, it checks whether the expiration time has elapsed. If not, the NAS 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. This option is effective only for FTP, Telnet, and SSH users.
VLAN	Specify the VLAN to be authorized to the local user after the user passes authentication. This option is effective only for LAN-access and portal users.
ACL	Specify the ACL to be used by the NAS to restrict the access of the local user after the user passes authentication. This option is effective only for LAN-access and portal users.
User-profile	User profile for the local user. The switch series does not support this option.

Configuring a user group

1. Select **Authentication** > **Users** from the navigation tree.
2. Click the **User Group** tab to display the existing user groups.

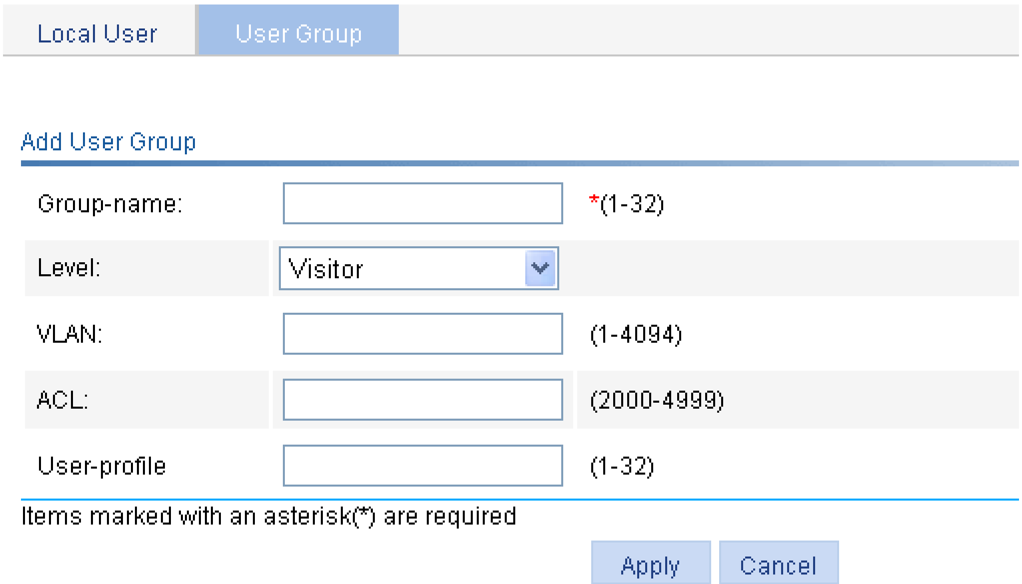
Figure 414 User group list



3. Click **Add**.

   The page for configuring a user group appears.

Figure 415 User group configuration page



4. Configure the user group as described in Table 123.
5. Click **Apply**.

Table 123 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 NAS to control the access of users of the user group after the users pass authentication.
User-profile	User profile for the user group. The switch series does not support this option.

Configuring PKI

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 document involves local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity. A CA certificate, also known as a "root certificate", is signed by the CA for itself.

CRL

An existing certificate might need to be revoked when, for example, the user name changes, the private key leaks, or the user stops the business. Revoking a certificate will 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 might publish multiple CRLs when the number of revoked certificates is so large that publishing them in a single CRL might degrade network performance.

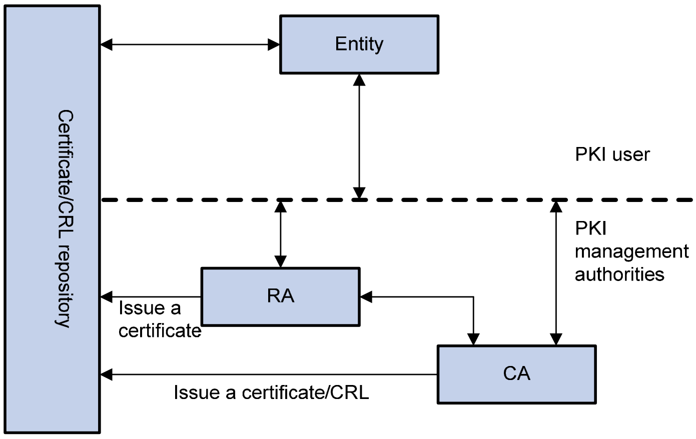
CA policy

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 email. As different CAs might 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.

PKI architecture

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository.

Figure 416 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 no independent RA exists. 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, and it provides 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.

PKI applications

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 email

Emails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure email protocol that is 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.

How PKI operates

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 operates:

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. The CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

Configuring PKI

The device supports the following 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.

Recommended configuration procedure for manual request

Step	Remarks
1. Creating a PKI entity	(Required.) Create a PKI entity and configure the identity information. A certificate is the binding of a public key and the identity information of an entity, where the identity information is identified by an entity distinguished name (DN). A CA identifies a certificate applicant uniquely by an entity DN. IMPORTANT: The DN settings of an entity must be compliant to the CA certificate issue policy for confirming which entity parameters are mandatory or optional. Otherwise, the certificate request might be rejected.
2. 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, and has only local significance.
3. 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, and the public key is transferred to the CA along with some other information. IMPORTANT: If a local certificate already exists, you must remove the certificate before generating a new key pair, so as to keep the consistency between the key pair and the local certificate.
4. Retrieving the CA certificate	(Required.) Certificate retrieval serves the following purposes: • Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count, • Prepare for certificate verification. IMPORTANT: If a local CA certificate already exists, you cannot perform the CA certificate retrieval operation. This will 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.

Step	Remarks
5. 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 online mode or offline mode. • 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. IMPORTANT: If a local certificate already exists, you cannot perform the local certificate retrieval operation. This will 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.
6. 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.
7. Retrieving and displaying a certificate	(Optional.) Retrieve an existing certificate.
8. Retrieving and displaying a CRL	(Optional.) Retrieve a CRL and display its contents.

Recommended configuration procedure for automatic request

Task	Remarks
1. 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 might be rejected.
2. 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, and has only local significance.

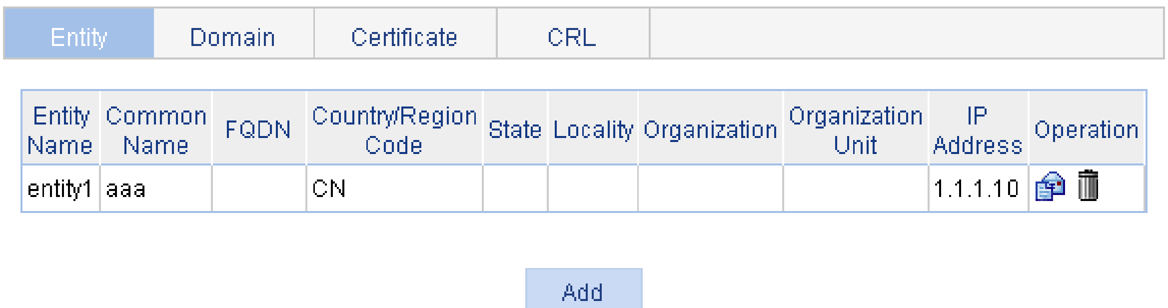
Task	Remarks
3. Destroying the RSA key pair	(Optional.) Destroy the existing RSA key pair and the corresponding local certificate. If the certificate to be retrieved contains an RSA key pair, you need to destroy the existing key pair. Otherwise, the retrieving operation will fail.
4. Retrieving and displaying a certificate	(Optional.) Retrieve an existing certificate.
5. Retrieving and displaying a CRL	(Optional.) Retrieve a CRL and display its contents.

Creating a PKI entity

1. Select **Authentication** > **PKI** from the navigation tree.

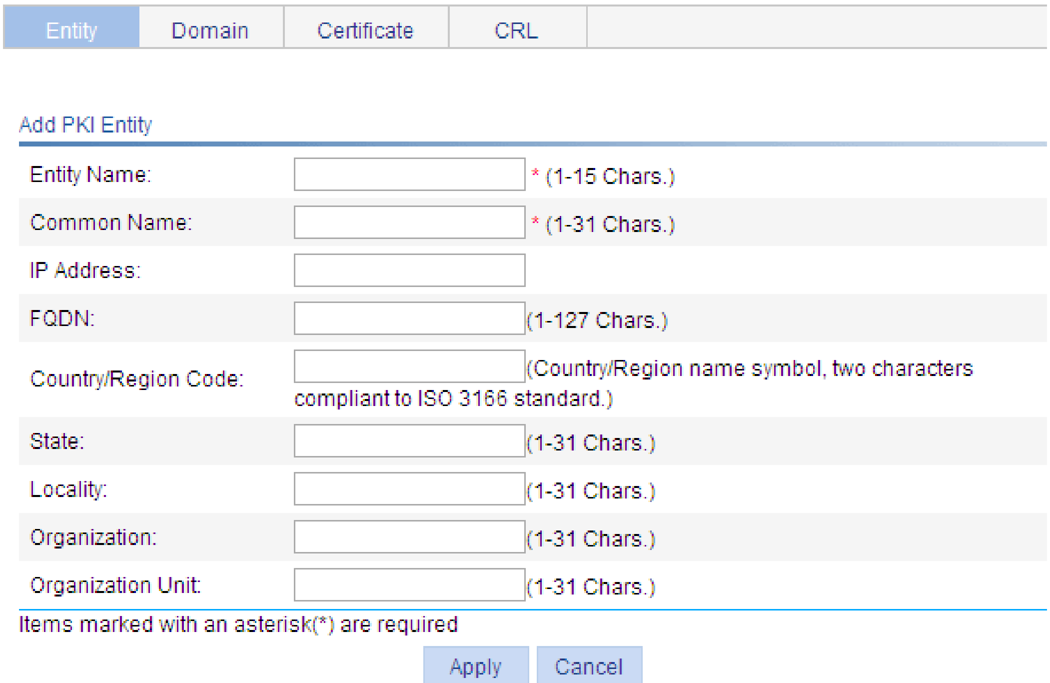
   The PKI entity list page is displayed by default.

Figure 417 PKI entity list



2. Click **Add**.

Figure 418 PKI entity configuration page



3. Configure the parameters as described in Table 124.
4. Click **Apply**.

Table 124 Configuration items

Item	Description
Entity Name	Enter the name for the PKI entity.
Common Name	Enter the common name for the entity.
IP Address	Enter the IP address of the entity.
FQDN	Enter 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	Enter the country or region code for the entity.
State	Enter the state or province for the entity.
Locality	Enter the locality for the entity.
Organization	Enter the organization name for the entity.
Organization Unit	Enter the unit name for the entity.

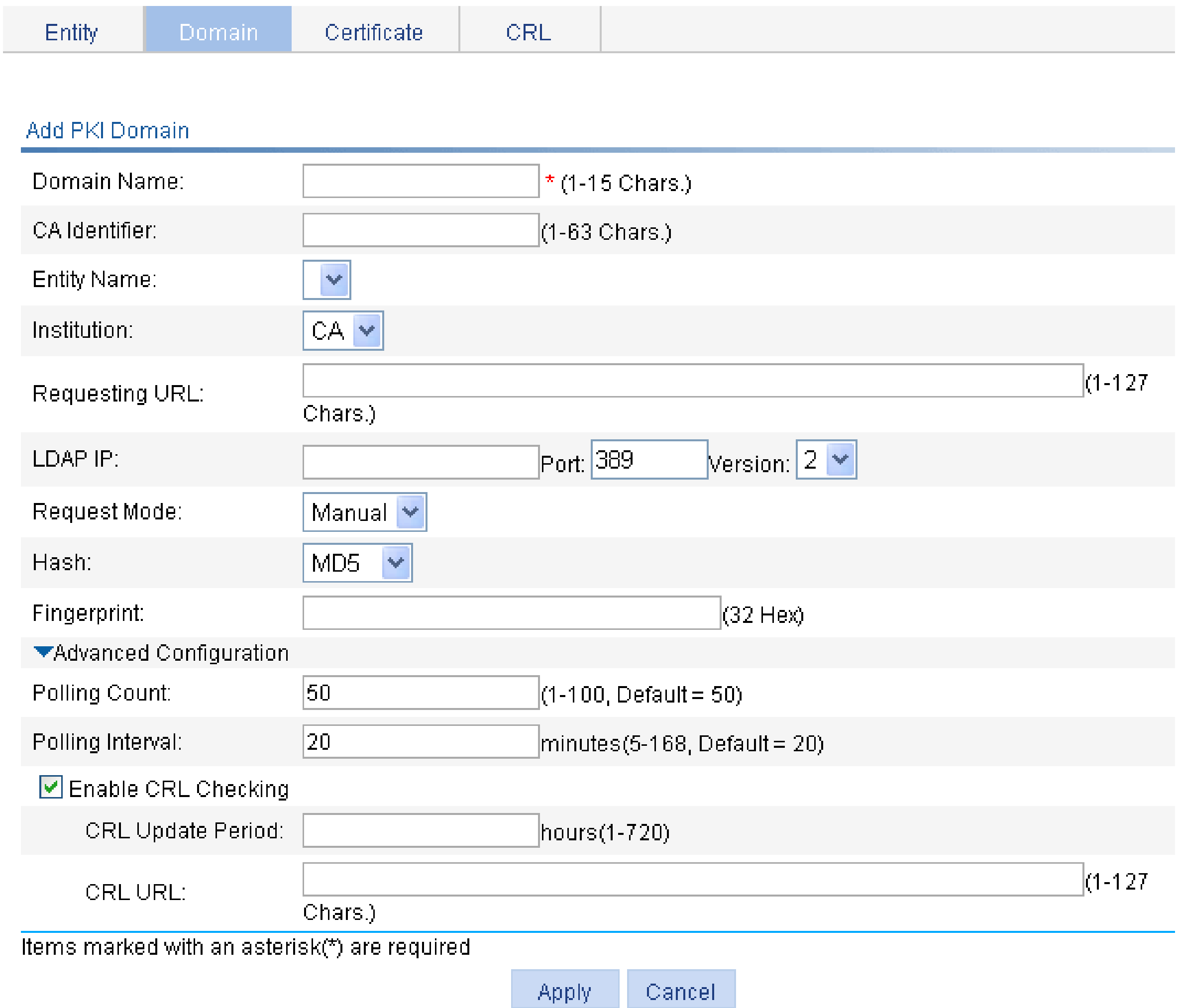
Creating a PKI domain

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **Domain** tab.

Figure 419 PKI domain list

3. Click **Add**.
4. Click **Advanced Configuration** to display the advanced configuration items.

Figure 420 PKI domain configuration page



5. Configure the parameters as described in Table 125.
6. Click **Apply**.

Table 125 Configuration items

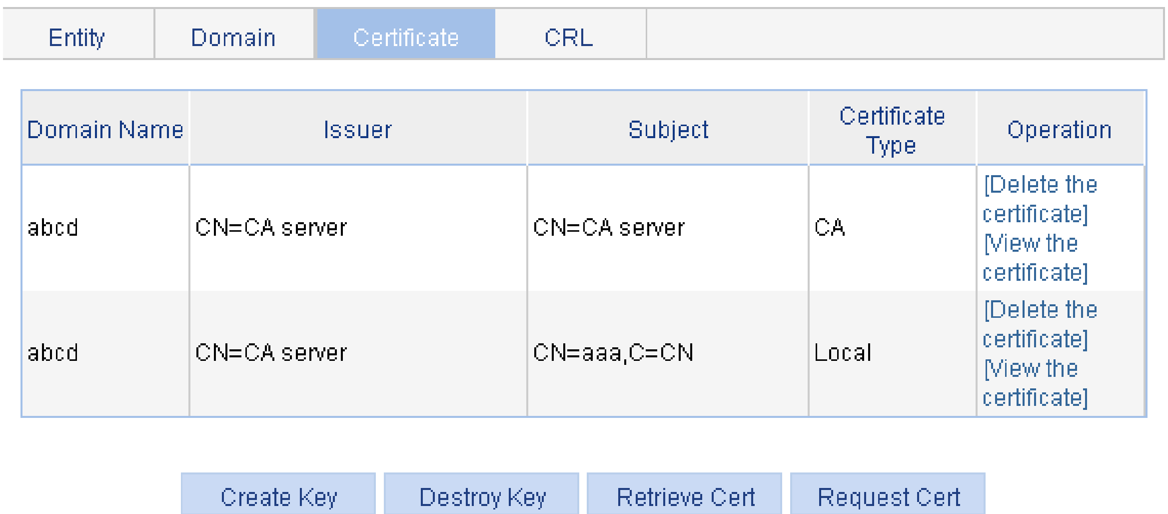
<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Domain Name</td><td>Enter the name for the PKI domain.</td></tr>
<tr><td>CA Identifier</td><td>Enter the identifier of the trusted CA.
An entity requests a certificate from a trusted CA. The trusted CA takes the responsibility of certificate registration, distribution, and revocation, and query.
In offline mode, this item is optional. In other modes, this item is required.</td></tr>
<tr><td>Entity Name</td><td>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.</td></tr>
<tr><td>Institution</td><td>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.</td></tr>
<tr><td>Requesting URL</td><td>Enter 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. In other modes, this item is required.
IMPORTANT:
This item does not support domain name resolution.</td></tr>
<tr><td>LDAP IP</td><td rowspan="3">Enter 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.</td></tr>
<tr><td>Port</td></tr>
<tr><td>Version</td></tr>
<tr><td>Request Mode</td><td>Select the online certificate request mode, which can be auto or manual.</td></tr>
<tr><td>Password</td><td rowspan="2">Set a password for certificate revocation and re-enter it for confirmation.
The two boxes are available only when the certificate request mode is set to Auto.</td></tr>
<tr><td>Confirm Password</td></tr>
<tr><td>Fingerprint Hash</td><td rowspan="2">Specify the fingerprint used for verifying the CA root certificate.
After 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.
• If you specify MD5 as the hash algorithm, enter an MD5 fingerprint. The fingerprint must a string of 32 characters in hexadecimal notation.
• If you specify SHA1 as the hash algorithm, enter an SHA1 fingerprint. The fingerprint must a string of 40 characters in hexadecimal notation.
IMPORTANT:
The fingerprint must be configured if you specify the certificate request mode as Auto. If you specify the certificate request mode as Manual, you can leave the fingerprint settings null. If you do not configure the fingerprint, the entity will not verify the CA root certificate and you yourself must make sure that the CA server is trusted.</td></tr>
<tr><td>Fingerprint</td></tr>
<tr><td>Polling Count</td><td>Set the polling interval and attempt limit for querying the certificate request status.</td></tr>
</table>

Item	Description
Polling Interval	After an entity makes a certificate request, the CA might 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.
Enable CRL Checking	Select this box to specify that CRL checking is required during certificate verification.
CRL Update Period	Enter the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs. This item is available after you click the **Enable CRL Checking** box. By default, the CRL update period depends on the next update field in the CRL file.
CRL URL	Enter the URL of the CRL distribution point. 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.

Generating an RSA key pair

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **Certificate** tab.

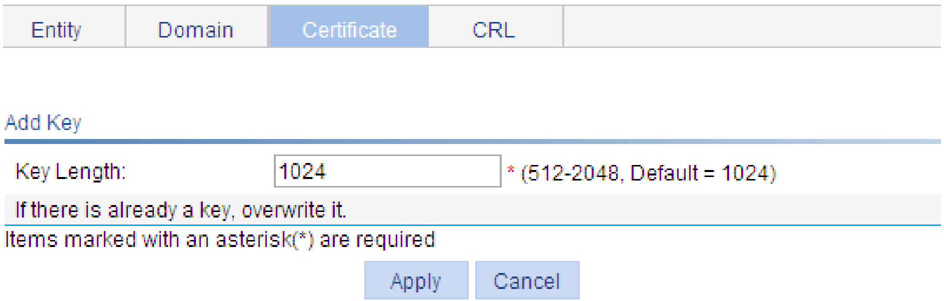
Figure 421 Certificate configuration page



- 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.

3. Click **Create Key**.
4. Set the key length.
5. Click **Apply**.

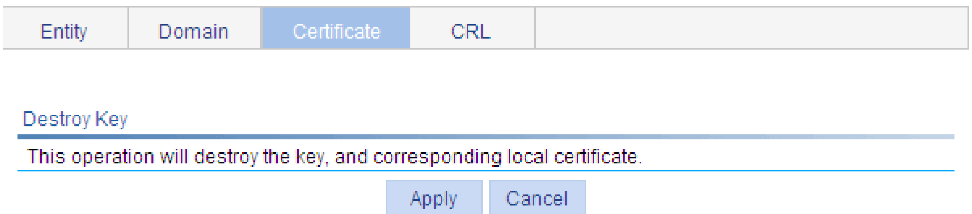
Figure 422 Key pair parameter configuration page



Destroying the RSA key pair

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **Certificate** tab.
3. Click **Destroy Key**.
4. Click **Apply** to destroy the existing RSA key pair and the corresponding local certificate.

Figure 423 Key pair destruction page



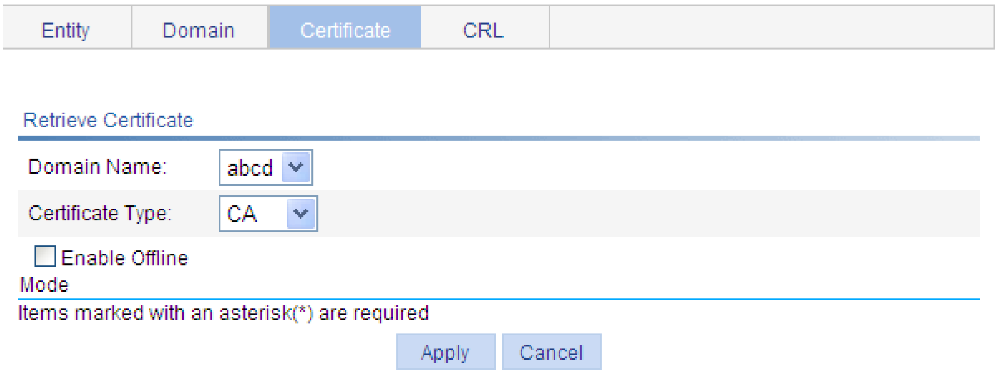
Retrieving and displaying a certificate

You can retrieve an existing CA certificate or local certificate from the CA server and save it locally. To do so, you can use offline mode or online. In offline mode, you must retrieve a certificate by an out-of-band means like FTP, disk, email and then import it into the local PKI system. By default, the retrieved certificate is saved in a file under the root directory of the device, and the filename is *domain-name*_ca.cer for the CA certificate, or *domain-name_local.cer* for the local certificate.

To retrieve a certificate:

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **Certificate** tab.
3. Click **Retrieve Cert**.

Figure 424 PKI certificate retrieval page



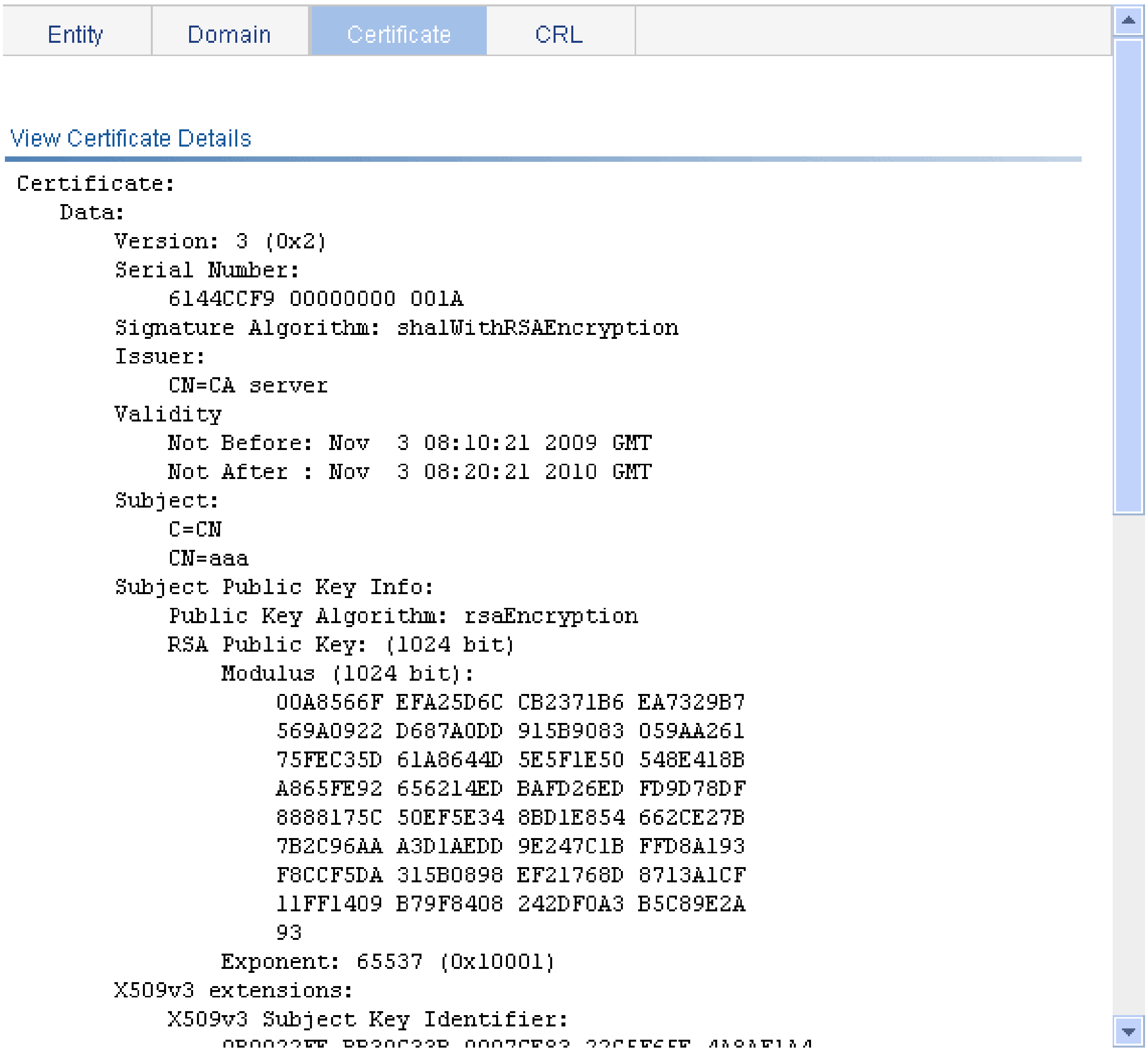
4. Configure the parameters as described in Table 126.
5. Click **Apply**.

Table 126 Configuration items

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	Click this box to retrieve a certificate in offline mode (that is, by an out-of-band means like FTP, disk, or email) and then import the certificate into the local PKI system. The following configuration items are displayed if this box is selected.
Get File From Device	Specify the path and name of the certificate file to import: • If the certificate file is saved on the device, select **Get File From Device** and then specify the path and name of the file on the device. If no file is specified, the system, by default, gets the file *domain-name*_ca.cer (for the CA certificate) or *domain-name_local.cer* (for the local certificate) under the root directory of the device.
Get File From PC	• If the certificate file is saved on a local PC, select **Get File From PC** and. then specify the path and name of the file and specify the partition that saves the file.
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.

Figure 425 Certificate information



Requesting a local certificate

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **Certificate** tab.
3. Click **Request Cert**.

Figure 426 Local certificate request page

4. Configure the parameters as described in Table 127.

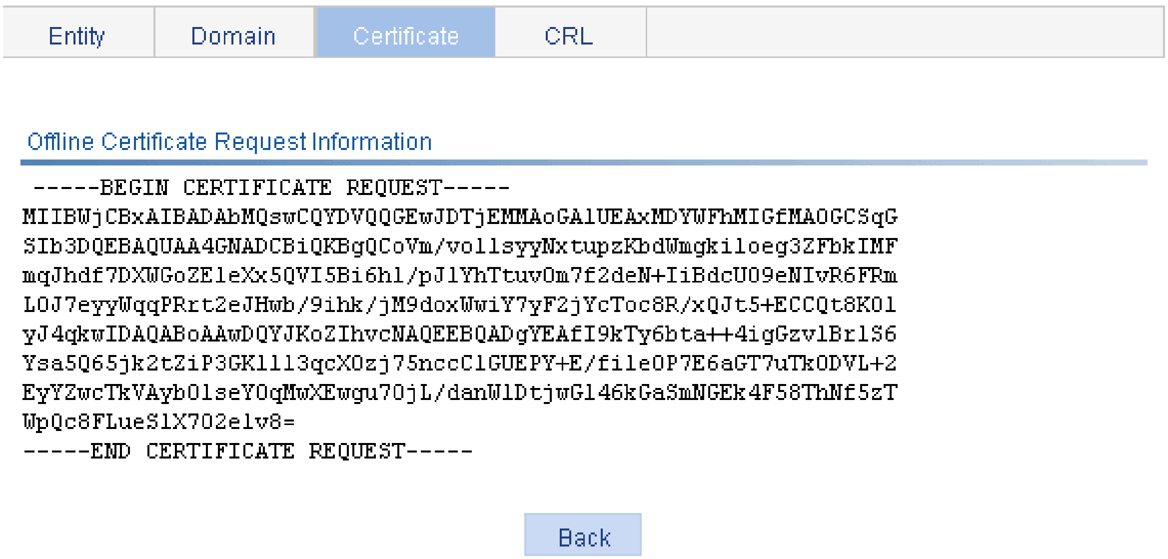
Table 127 Configuration items

Item	Description
Domain Name	Select the PKI domain for the certificate.
Password	Enter the password for certificate revocation.
Enable Offline Mode	Select this box to request a certificate in offline mode, that is, by an out-of-band means like FTP, disk, or email.

5. Click **Apply**.

   If you select the online mode, the system gives a prompt that certificate request has been submitted. In this case, click **OK** to finish the operation. If you select the offline mode, the offline certificate request information page appears In this case, you must submit the information by an out-of-band way to the CA to request a local certificate.

Figure 427 Offline certificate request information page



Retrieving and displaying a CRL

1. Select **Authentication** > **PKI** from the navigation tree.
2. Click the **CRL** tab.

Figure 428 CRL page

3. Click **Retrieve CRL** to retrieve the CRL of a domain.
4. Click **View CRL** for the domain to display the contents of the CRL.

Figure 429 CRL information

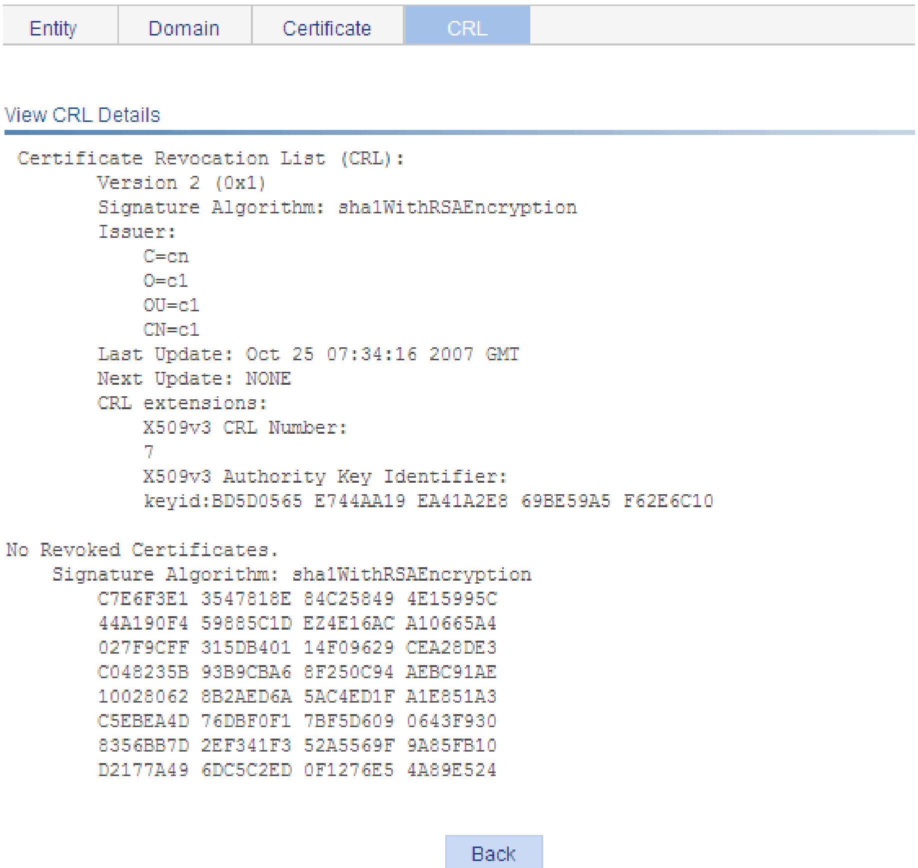


Table 128 Field description

Field	Description
Version	CRL version number
Signature Algorithm	Signature algorithm that the CRL uses
Issuer	CA that issued the CRL
Last Update	Last update time
Next Update	Next update time
X509v3 Authority Key Identifier	Identifier of the CA that issued the certificate and the certificate version (X509v3).
keyid	Pubic key identifier A CA might have multiple key pairs, and this field identifies which key pair is used for the CRL signature.
No Revoked Certificates.	No certificates are revoked.
Revoked Certificates	Information about the revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Certificate revocation date

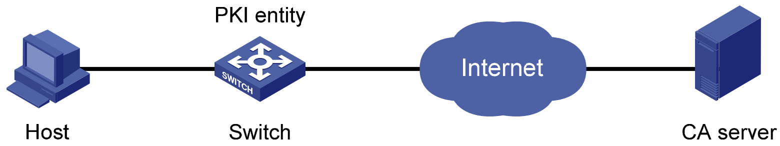
PKI configuration example

Network requirements

As shown in Figure 430, configure the switch that acts 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 retrieves CRLs for certificate verification.

Figure 430 Network diagram



Configuring the CA server

1. Create a CA server named **myca**:

   In this example, you must first configure the basic attributes of **Nickname** and **Subject DN** on the CA server: the nickname is the name of the trusted CA, and the subject DN is the DN attributes of the CA, including the common name (CN), organization unit (OU), organization (O), and country (C). Leave the default values of the other attributes.
2. 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.
3. Configure the CRL publishing behavior:

   After completing the 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.

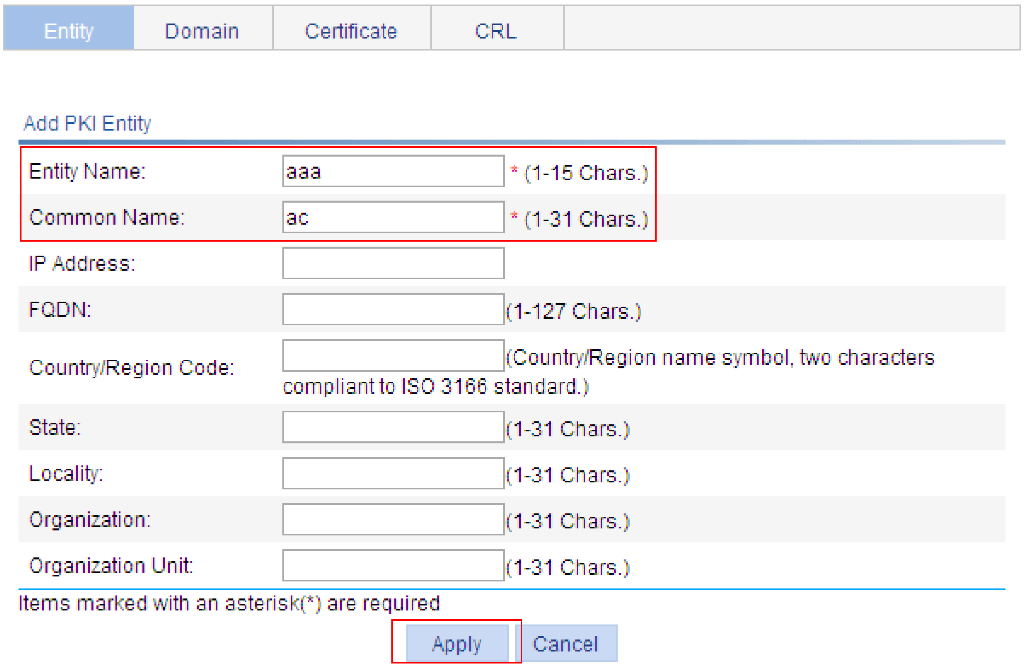
   After the configuration, make sure that the system clock of the switch is synchronous to that of the CA, so that the switch can request certificates and retrieve CRLs properly.

Configuring the switch

1. Create a PKI entity:
   a. Select **Authentication** > **PKI** from the navigation tree.

      The PKI entity list page is displayed by default.
   b. Click **Add**.
   c. Enter **aaa** as the PKI entity name, enter **ac** as the common name, and click **Apply**.

Figure 431 Creating a PKI entity

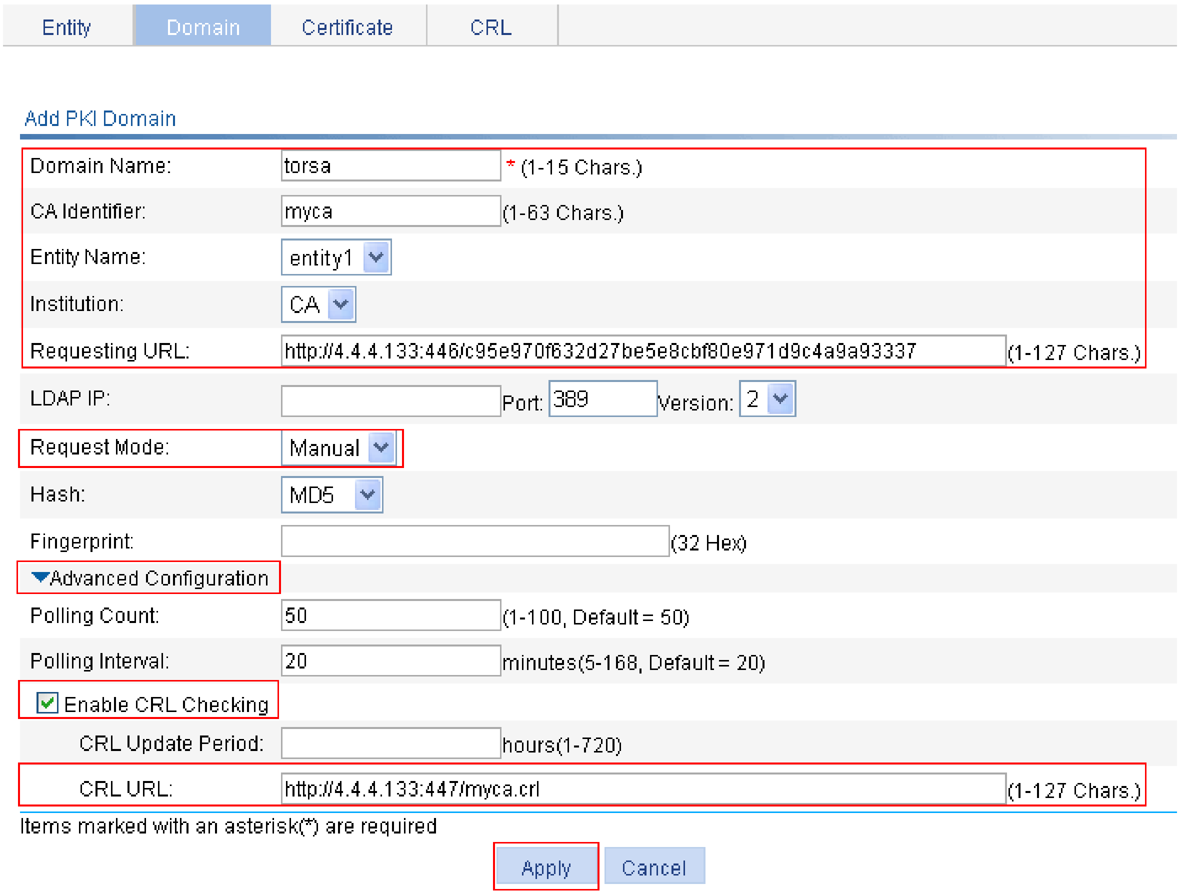


2. Create a PKI domain:
   a. Click the **Domain** tab.
   b. Click **Add**.

      The page in Figure 432 appears.
   c. Enter **torsa** as the PKI domain name, enter **myca** as the CA identifier, select **aaa** as the local entity, select **CA** as the authority for certificate request, enter **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), and select **Manual** as the certificate request mode.
   d. Click the collapse button before **Advanced Configuration**.
   e. In the advanced configuration area, click the **Enable CRL Checking** box, and enter **http://4.4.4.133:447/myca.crl** as the CRL URL.
   f. Click **Apply**.

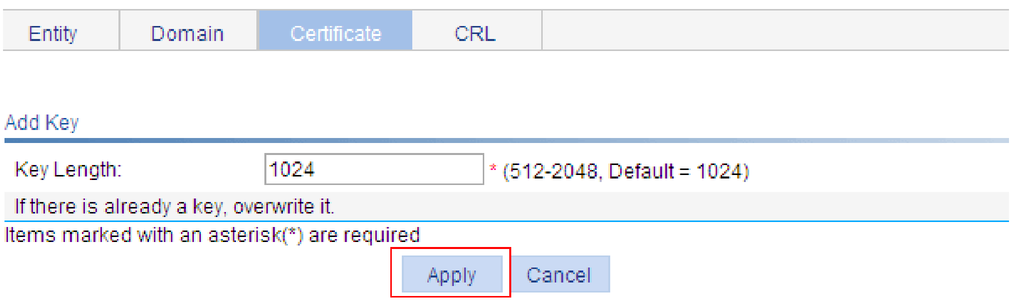
      A dialog box appears, asking "Fingerprint of the root certificate not specified. No root certificate validation will occur. Continue?"
   g. Click **OK**.

Figure 432 Creating a PKI domain



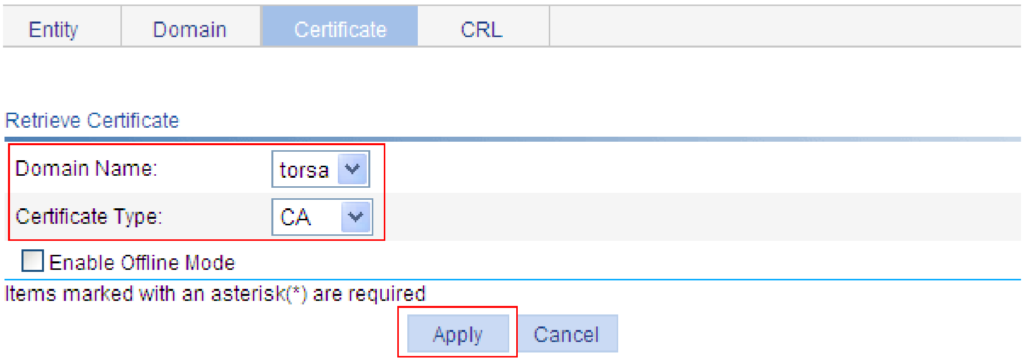
3. Generate an RSA key pair:
   a. Click the **Certificate** tab.
   b. Click **Create Key**.
   c. Enter **1024** as the key length, and click **Apply** to generate an RSA key pair.

Figure 433 Generating an RSA key pair



4. Retrieve the CA certificate:
   a. Click the **Certificate** tab.
   b. Click **Retrieve Cert**.
   c. Select **torsa** as the PKI domain, select **CA** as the certificate type, and click **Apply**.

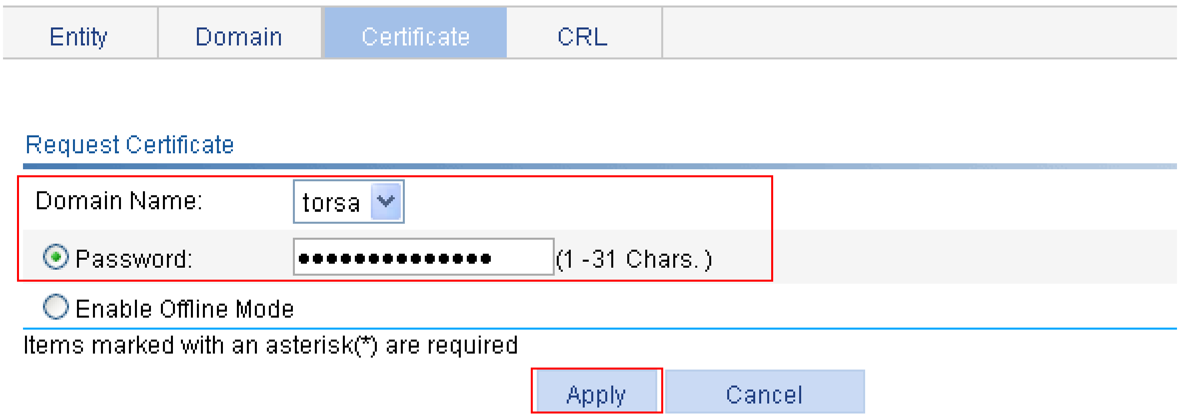
Figure 434 Retrieving the CA certificate



5. Request a local certificate:
   a. Click the **Certificate** tab.
   b. Click **Request Cert**.
   c. Select **torsa** as the PKI domain, select **Password** , and enter **challenge-word** as the password.
   d. Click **Apply**.

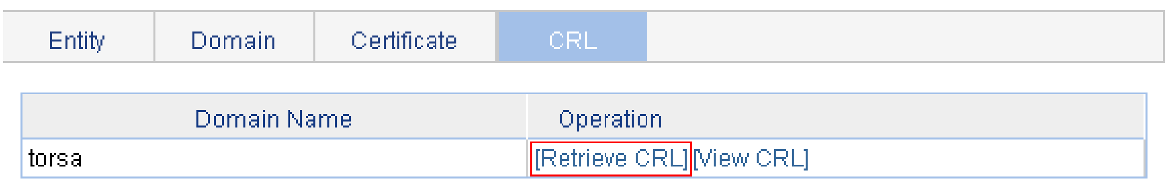
      The system displays "Certificate request has been submitted."
   e. Click **OK** to finish the operation.

Figure 435 Requesting a local certificate



6. Retrieve the CRL:
   a. Click the **CRL** tab.
   b. Click **Retrieve CRL** of the PKI domain of **torsa**.

Figure 436 Retrieving the CRL



Verifying the configuration

After the configuration, select **Authentication** > **PKI** > **Certificate** from the navigation tree to view detailed information about the retrieved CA certificate and local certificate, or select **Authentication** > **PKI** > **CRL** from the navigation tree to view detailed information about the retrieved CRL.

Configuration guidelines

When you configure PKI, follow these guidelines:

- Make sure the clocks of entities and the CA are synchronous. Otherwise, the validity period of certificates will be abnormal.
- 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.
- 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 you configure the PKI domain.
- 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 you configure the PKI domain.

Configuring authorized IP

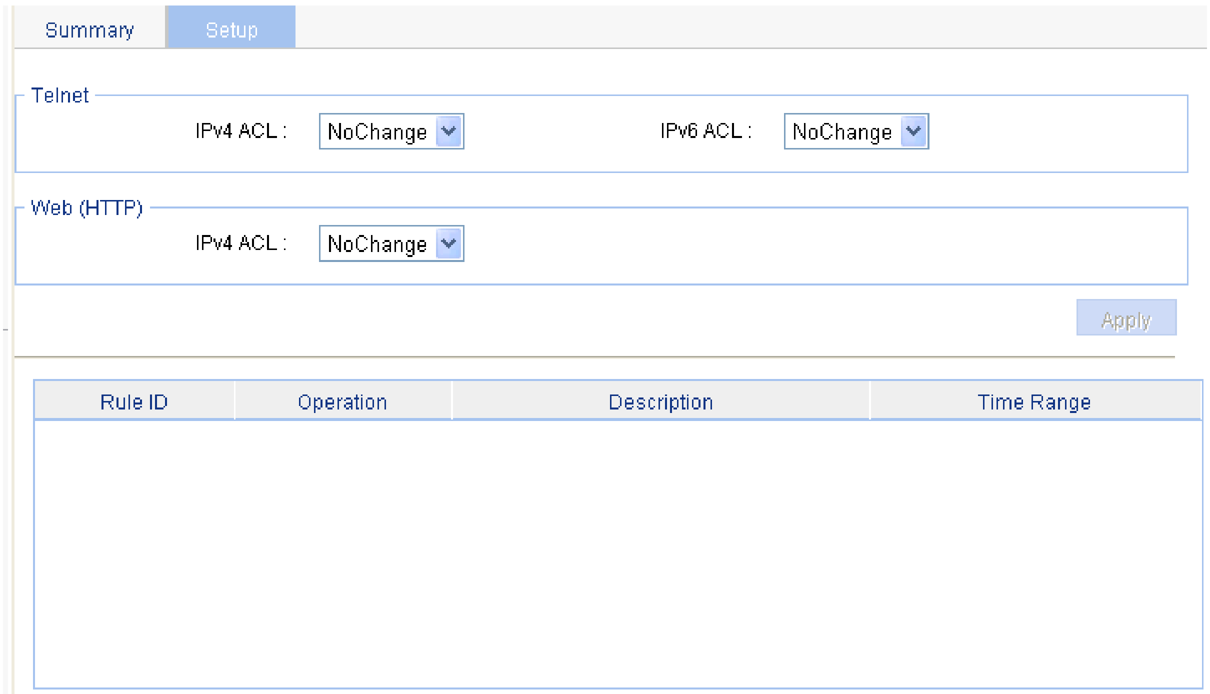
Overview

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

1. Select **Security** > **Authorized IP** from the navigation tree.
2. Click the **Setup** tab to enter the authorized IP configuration page.

Figure 437 Authorized IP configuration page



3. Configure authorized IP as described in Table 129.
4. Click **Apply**.

Table 129 Configuration items

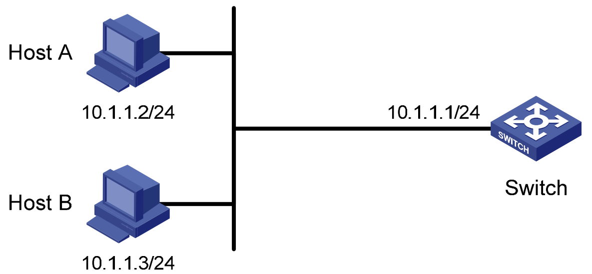
Item		Description
Telnet	IPv4 ACL	Associate the Telnet service with an IPv4 ACL. You can configure the IPv4 ACL to be selected by selecting **QoS** > **ACL IPv4**.
	IPv6 ACL	Associate the Telnet service with an IPv6 ACL. You can configure the IPv6 ACL to be selected by selecting **QoS** > **ACL IPv6**.
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

Network requirements

In Figure 438, configure Switch to deny Telnet and HTTP requests from Host A, and permit Telnet and HTTP requests from Host B.

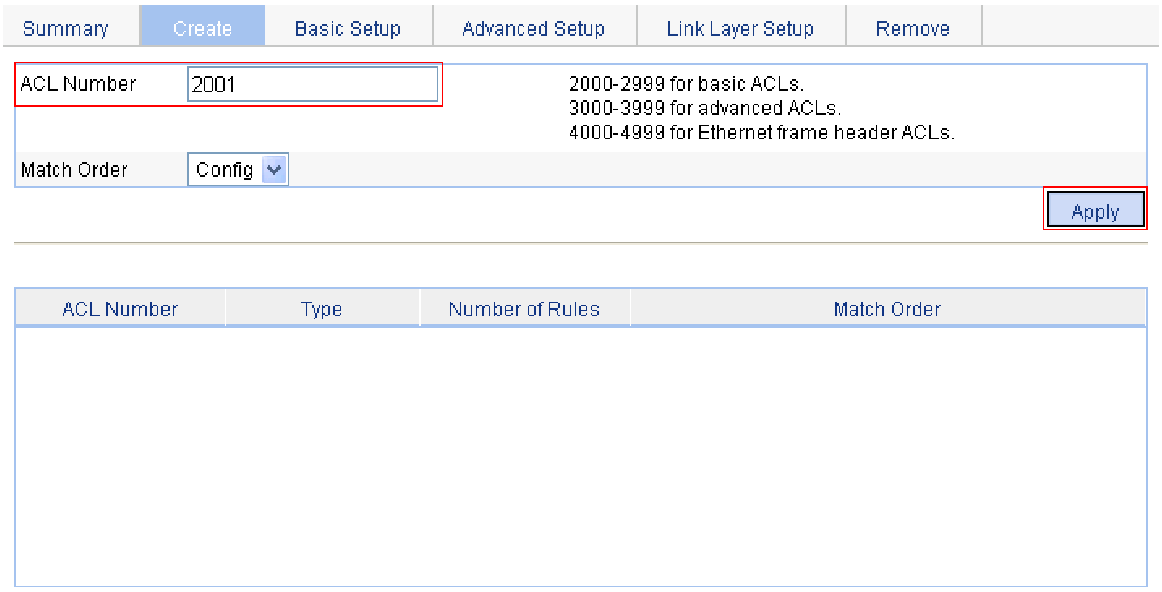
Figure 438 Network diagram



Configuration procedure

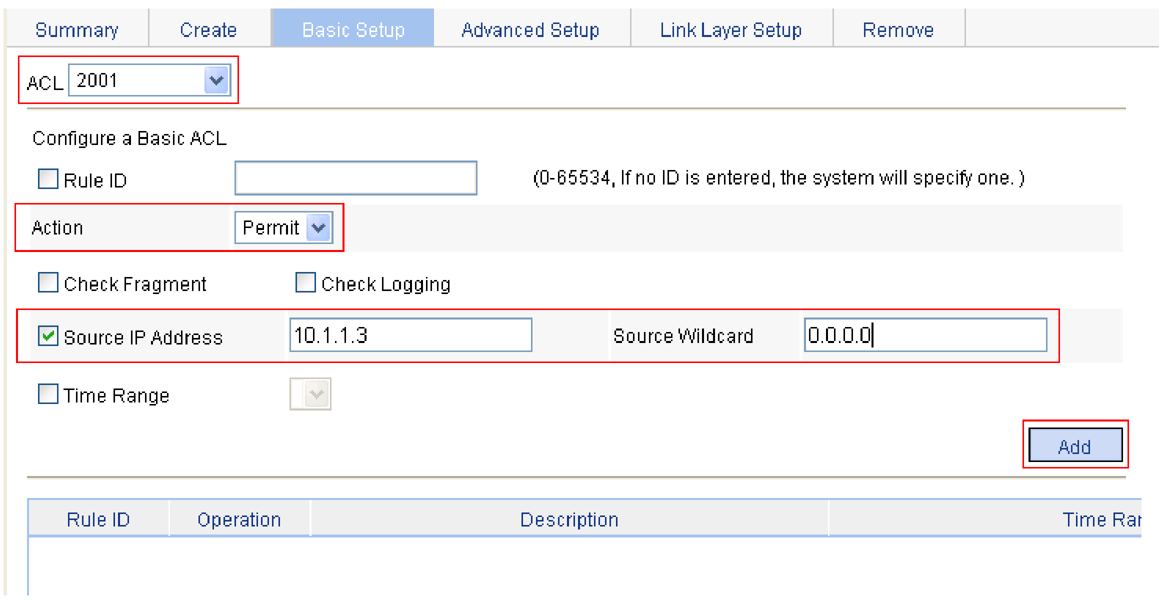
1. Create an ACL:
    a. Select **QoS** > **ACL IPv4** from the navigation tree.
    b. Click the **Create** tab.
    c. Enter **2001** for **ACL Number**.
    d. Click **Apply**.

Figure 439 Creating an ACL



2. Configure an ACL rule to permit Host B:
   a. Click the **Basic Setup** tab
      The page for configuring an ACL rule appears.
   b. Select 2001 from the **ACL** list, select **Permit** from the **Action** list, select the **Source IP Address** box and then enter **10.1.1.3**, and enter **0.0.0.0** in the **Source Wildcard** field.
   c. Click **Add**.

Figure 440 Configuring an ACL rule to permit Host B

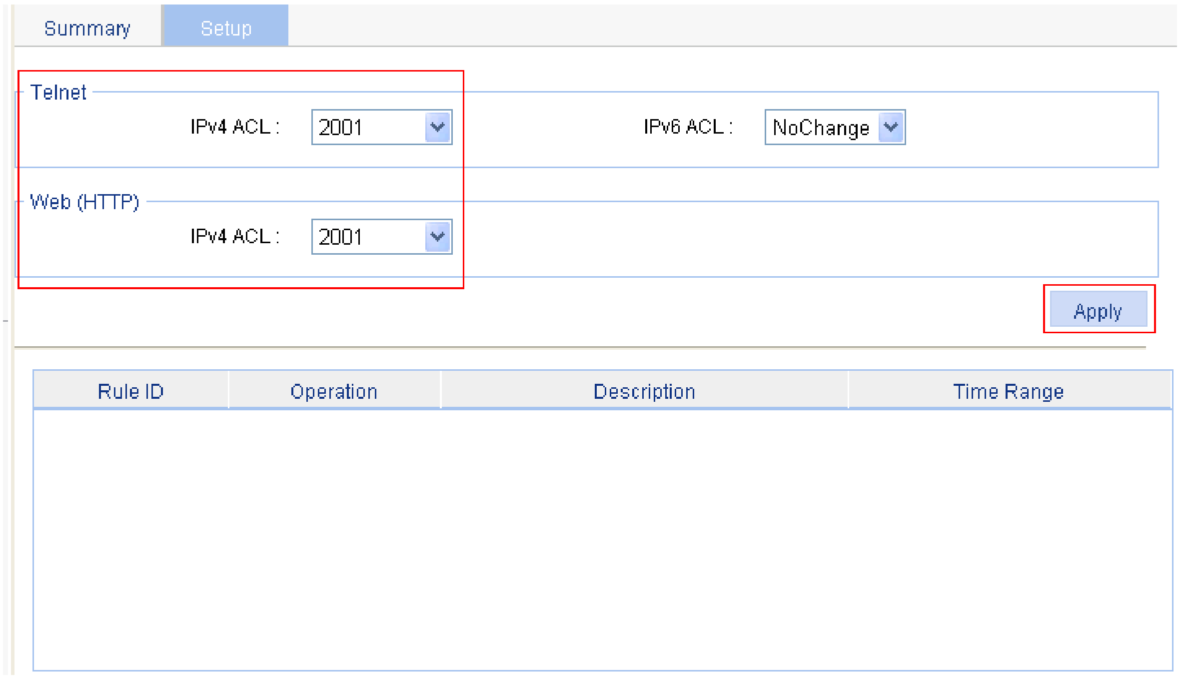


3. Configure authorized IP:
   a. Select **Security** > **Authorized IP** from the navigation tree.
   b. Click the **Setup** tab.
      The authorized IP configuration page appears.

c. Select **2001** for **IPv4 ACL** in the **Telnet** field, and select **2001** for **IPv4 ACL** in the **Web (HTTP)** field.

d. Click **Apply**.

Figure 441 Configuring authorized IP



Configuring port isolation

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.

The switch series supports 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 the switches.

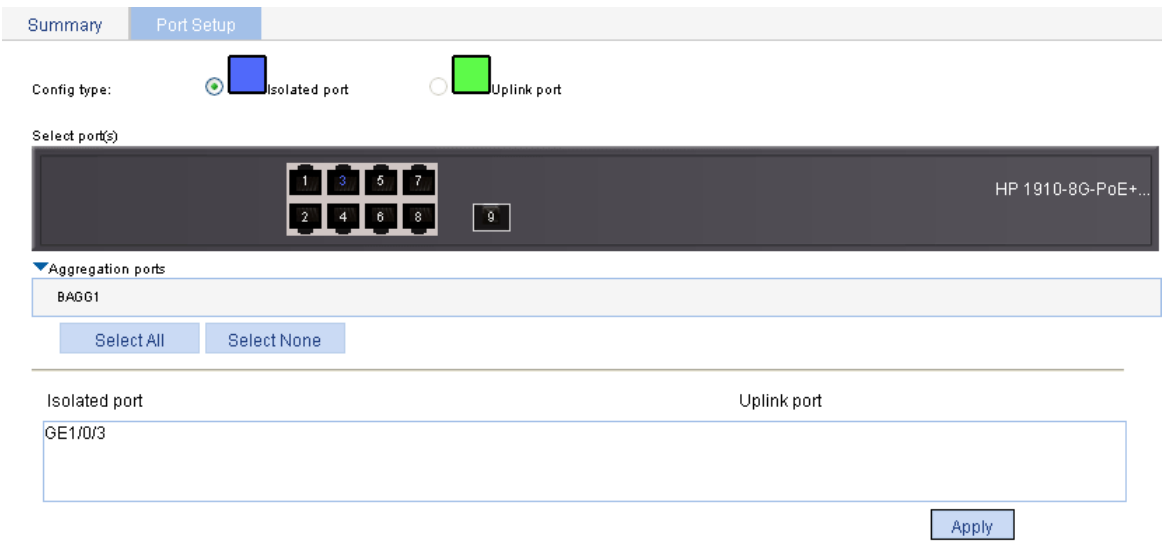
There is no restriction on the number of ports assigned to the isolation group.

Layer 2 traffic is isolated between ports from different VLANs. Within the same VLAN, Layer 2 data transmission between ports within and outside the isolation group is supported.

Configuring the isolation group

1. Select **Security** > **Port Isolate Group** from the navigation tree.
2. Click the **Port Setup** tab to enter the page shown in Figure 442.

Figure 442 Configure a port isolation group



3. Configure the port isolation group as described in Table 130.
4. Click **Apply**.

Table 130 Configuration items

Item	Description
Config type	Specify the role of the port or ports in the isolation group. • **Isolated 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. This option is not available for the switch series.
Select port(s)	Select the ports you want to assign to the isolation group. You can click ports on the chassis front panel for selection. If aggregate interfaces are configured, they will appear under the chassis panel for selection.

Port isolation configuration example

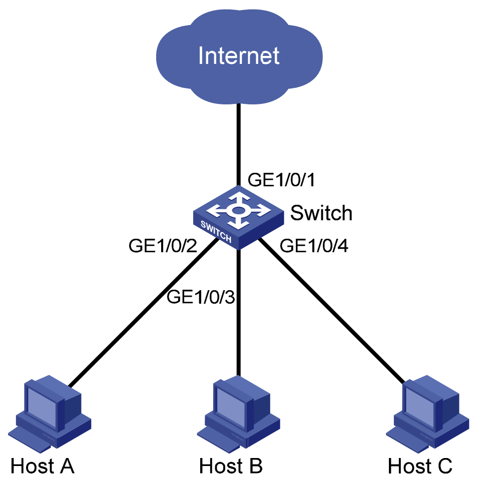
Network requirements

As shown in Figure 443:

- 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 external network 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.

Configure Host A, Host B, and Host C to access the external network but to be isolated from one another on Layer 2.

Figure 443 Networking diagram

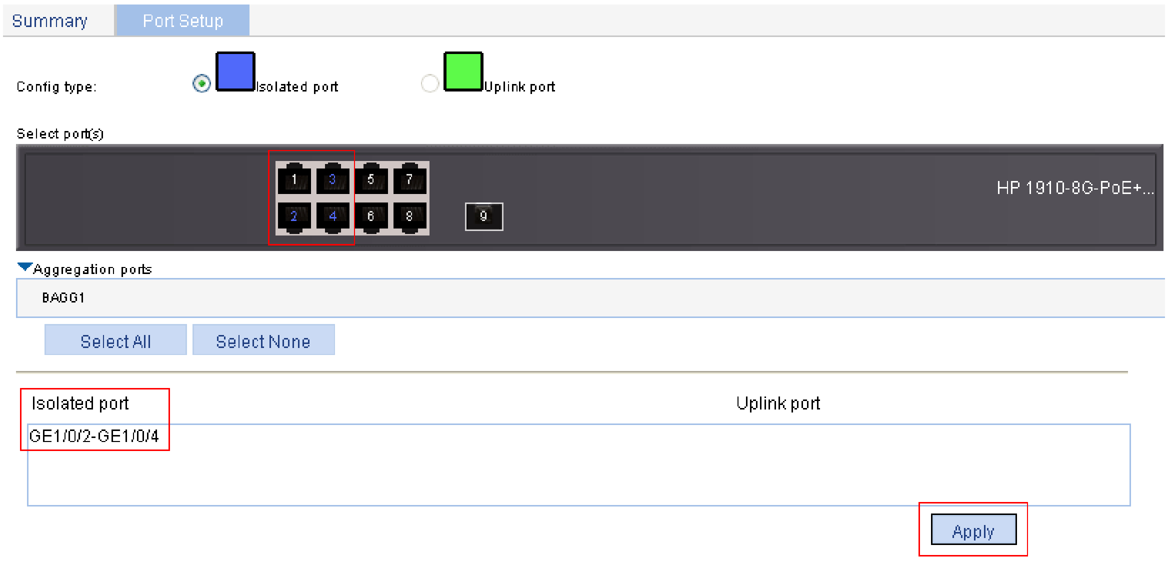


Configuring the switch

1. Assign GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the isolation group:
   a. Select **Security** > **Port Isolate Group** from the navigation tree.
   b. Click the **Port Setup** tab to enter the page shown in Figure 444.
   c. Select **Isolated port** for **Config Type**.

d. Select **2**, **3**, and **4** on the chassis front panel. The numbers represent ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 respectively.

Figure 444 Configure isolated ports for the isolation group



a. Click **Apply**.

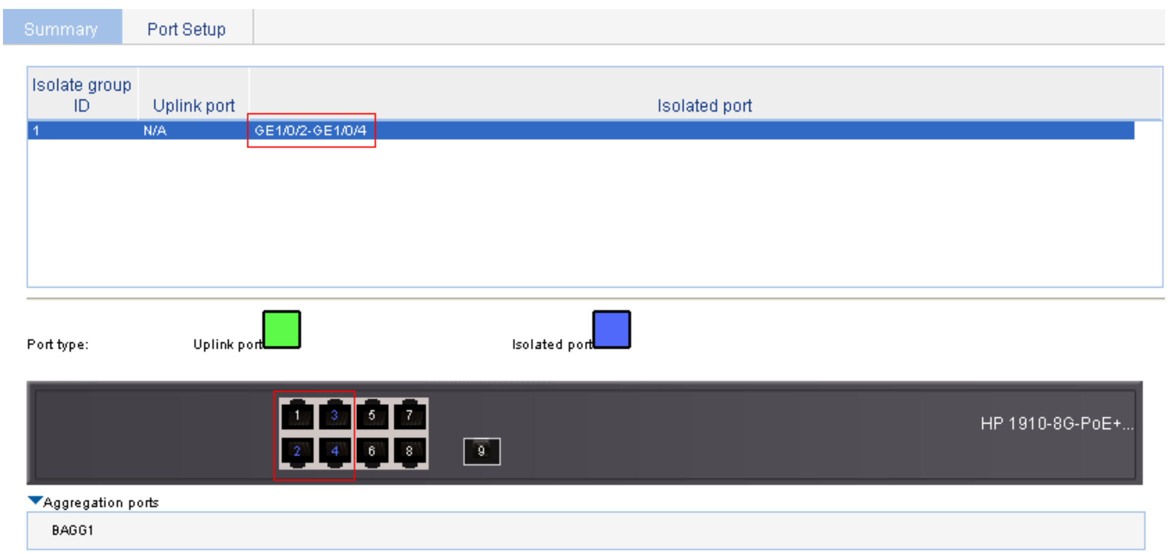
   A configuration progress dialog box appears.

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

Viewing information about the isolation group

1. Click **Summary**. The page shown in Figure 445 appears.
2. Display port isolation group 1, which contains isolated ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.

Figure 445 Information about port isolation group 1



Configuring ACLs

NOTE:

Unless otherwise stated, ACLs refer to both IPv4 and IPv6 ACLs throughout this document.

ACL overview

An access control list (ACL) is a set of rules (or permit or deny statements) for identifying traffic based on criteria such as source IP address, destination IP address, and port number.

ACLs are essentially used for packet filtering. A packet filter drops packets that match a deny rule and permits packets that match a permit rule. ACLs are also widely used by many modules, for example, QoS and IP routing, for traffic identification.

ACL categories

Table 131 ACL categories

Category	ACL number	IP version	Match criteria
Basic ACLs	2000 to 2999	IPv4	Source IPv4 address
		IPv6	Source IPv6 address
Advanced ACLs	3000 to 3999	IPv4	Source/destination IPv4 address, protocols over IPv4, and other Layer 3 and Layer 4 header fields
		IPv6	Source/destination IPv6 address, protocols over IPv6, and other Layer 3 and Layer 4 header fields
Ethernet frame header ACLs	4000 to 4999	IPv4 and IPv6	Layer 2 header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type

Match order

The rules in an ACL are sorted in certain order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule. If an ACL contains overlapping or conflicting rules, the matching result and action to take depend on the rule order.

The following ACL match orders are available:

- **Config**—Sorts ACL rules in ascending order of rule ID. A rule with a lower ID is matched before a rule with a higher ID. If you use this approach, check the rule content and order carefully.
- **Auto**—Sorts ACL rules in depth-first order. Depth-first ordering ensures that any subset of a rule is always matched before the rule. Table 132 lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

Table 132 Depth-first match for ACLs

ACL category	Sequence of tie breakers
IPv4 basic ACL	6. More 0s in the source IP address wildcard (more 0s means a narrower IP address range) 7. Smaller rule ID
IPv4 advanced ACL	8. Specific protocol type rather than IP (IP represents any protocol over IP) 9. More 0s in the source IP address wildcard mask 10. More 0s in the destination IP address wildcard 11. Narrower TCP/UDP service port number range 12. Smaller ID
IPv6 basic ACL	13. Longer prefix for the source IP address (a longer prefix means a narrower IP address range) 14. Smaller ID
IPv6 advanced ACL	15. Specific protocol type rather than IP (IP represents any protocol over IPv6) 16. Longer prefix for the source IPv6 address 17. Longer prefix for the destination IPv6 address 18. Narrower TCP/UDP service port number range 19. Smaller ID
Ethernet frame header ACL	20. More 1s in the source MAC address mask (more 1s means a smaller MAC address) 21. More 1s in the destination MAC address mask 22. Smaller ID

NOTE:

A wildcard mask, also called an "inverse mask", is a 32-bit binary and represented in dotted decimal notation. In contrast to a network mask, the 0 bits in a wildcard mask represent 'do care' bits, while the 1 bits represent 'don't care bits'. If the 'do care' bits in an IP address identical to the 'do care' bits in an IP address criterion, the IP address matches the criterion. All 'don't care' bits are ignored. The 0s and 1s in a wildcard mask can be noncontiguous. For example, 0.255.0.255 is a valid wildcard mask.

ACL rule numbering

What is the ACL rule numbering step

If you do not assign an ID for the rule you are adding, the system automatically assigns it a rule ID. The rule numbering step sets the increment by which the system automatically numbers rules. For example, the default ACL rule numbering step is 5. If you do not assign IDs to rules you are adding, they are numbered 0, 5, 10, 15, and so on. The wider the numbering step, the more rules you can insert between two rules.

By introducing a gap between rules rather than contiguously numbering rules, you have the flexibility of inserting rules in an ACL. This feature is important for a config order ACL, where ACL rules are matched in ascending order of rule ID.

Automatic rule numbering and re-numbering

The ID automatically assigned to an ACL rule takes the nearest higher multiple of the numbering step to the current highest rule ID, starting with 0.

For example, if the numbering step is 5 (the default), and five ACL rules numbered 0, 5, 9, 10, and 12 exist, the newly defined rule will be numbered 15. If the ACL does not contain any rule, the first rule will be numbered 0.

Whenever the step changes, the rules are renumbered, starting from 0. For example, if five rules numbered 5, 10, 13, 15, and 20 exist, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6 and 8.

Implementing time-based ACL rules

You can implement ACL rules based on the time of day by applying a time range to them. A time-based ACL rule takes effect only in any time periods specified by the time range.

The following basic types of time range are available:

- **Periodic time range**—Recurs periodically on a day or days of the week.
- **Absolute time range**—Represents only a period of time and does not recur.

IPv4 fragments filtering with ACLs

Traditional packet filtering matches only first fragments of IPv4 packets, and allows all subsequent non-first fragments to pass through. Attackers can fabricate non-first fragments to attack networks.

To avoid the risks, the HP ACL implementation filters unfragmented packets and all fragments (including non-first fragments) by default. To improve the match efficiency, you can change the default packet matching policy. For example, you can configure ACL to match only the non-first fragments.

Recommend ACL configuration procedures

Recommended IPv4 ACL configuration procedure

Step	Remarks
1. Configuring a time range	(Optional) Add a time range. A rule referencing a time range takes effect only during the specified time range.
2. Adding an IPv4 ACL	(Required) Add an IPv4 ACL. The category of the added ACL depends on the ACL number that you specify.
3. Configuring a rule for a basic IPv4 ACL	(Required) Complete one of the following tasks according to the ACL category.
4. Configuring a rule for an advanced IPv4 ACL	
5. Configuring a rule for an Ethernet frame header ACL	

Recommended IPv6 ACL configuration procedure

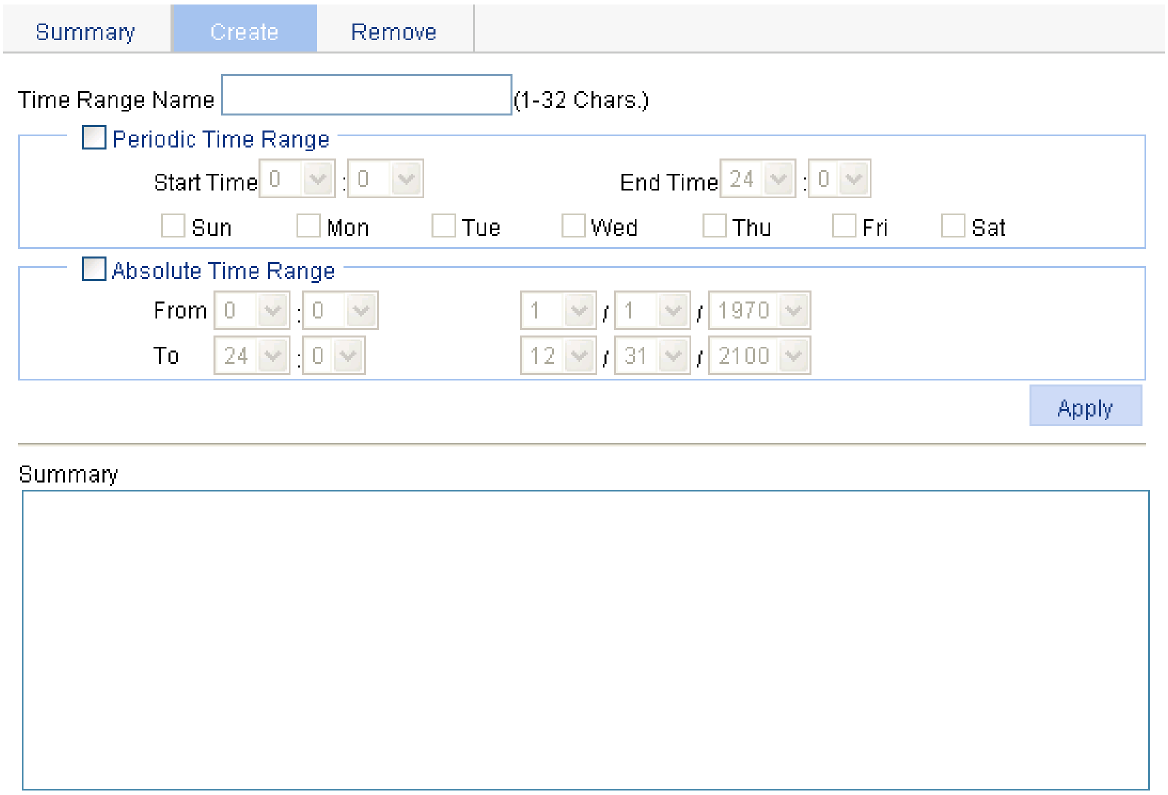
Step	Remarks
1. Configuring a time range	Optional Add a time range. A rule referencing a time range takes effect only during the specified time range.

Step	Remarks
2. Adding an IPv6 ACL	Required Add an IPv6 ACL. The category of the added IPv6 ACL depends on the ACL number that you specify.
3. Configuring a rule for a basic IPv6 ACL	Required Complete one of the tasks according to the ACL category.
4. Configuring a rule for an advanced IPv6 ACL	

Configuring a time range

1. Select **QoS** > **Time Range** from the navigation tree.
2. Click the **Create** tab to enter the time range configuration page.

Figure 446 Adding a time range



3. Configure a time range as described in Table 133.
4. Click **Apply**.

Table 133 Configuration items

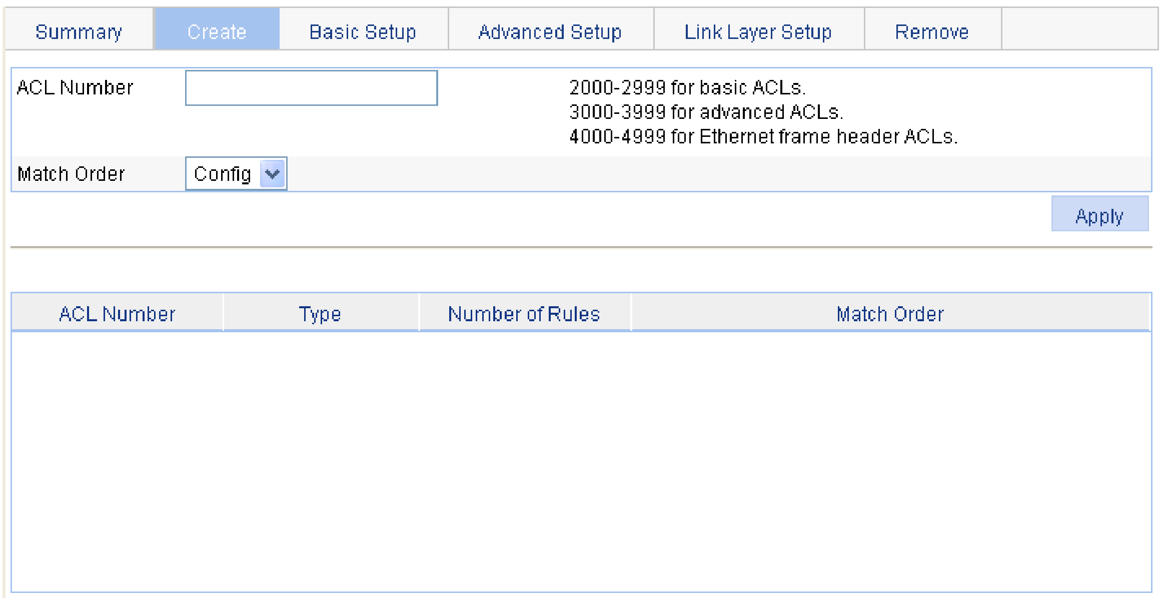
Item	Description
Time Range Name	Set the name for the time range.

Item		Description	
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 add 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.	

Adding an IPv4 ACL

1. Select **QoS** > **ACL IPv4** from the navigation tree.
2. Click the **Create** tab to enter the IPv4 ACL configuration page.

Figure 447 Adding an IPv4 ACL



3. Add an IPv4 ACL as described in Table 134.
4. Click **Apply**.

Table 134 Configuration items

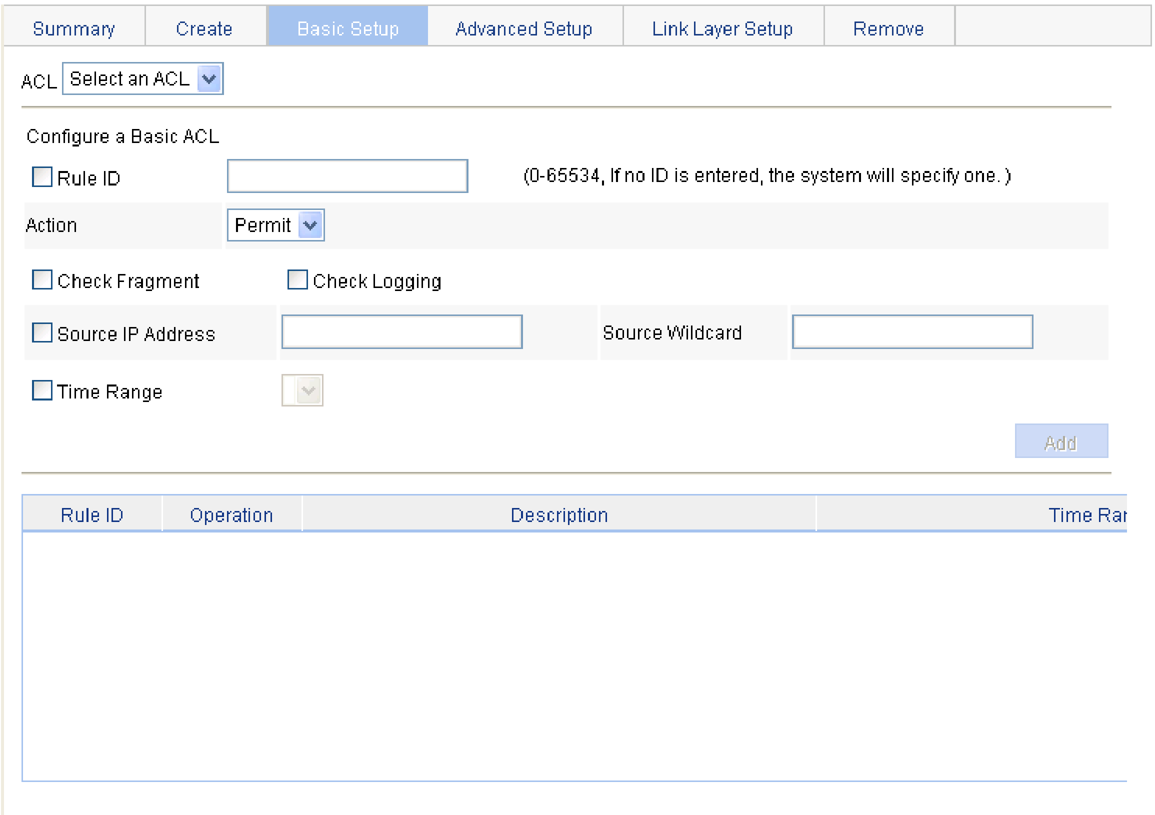
Item	Description
ACL Number	Set the number of the IPv4 ACL.

Item	Description
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.

Configuring a rule for a basic IPv4 ACL

1. Select **QoS** > **ACL IPv4** from the navigation tree.
2. Click the **Basic Setup** tab to enter the rule configuration page for a basic IPv4 ACL.

Figure 448 Configuring an basic IPv4 ACL



3. Configure a rule for a basic IPv4 ACL as described in Table 135.
4. Click **Add**.

Table 135 Configuration items

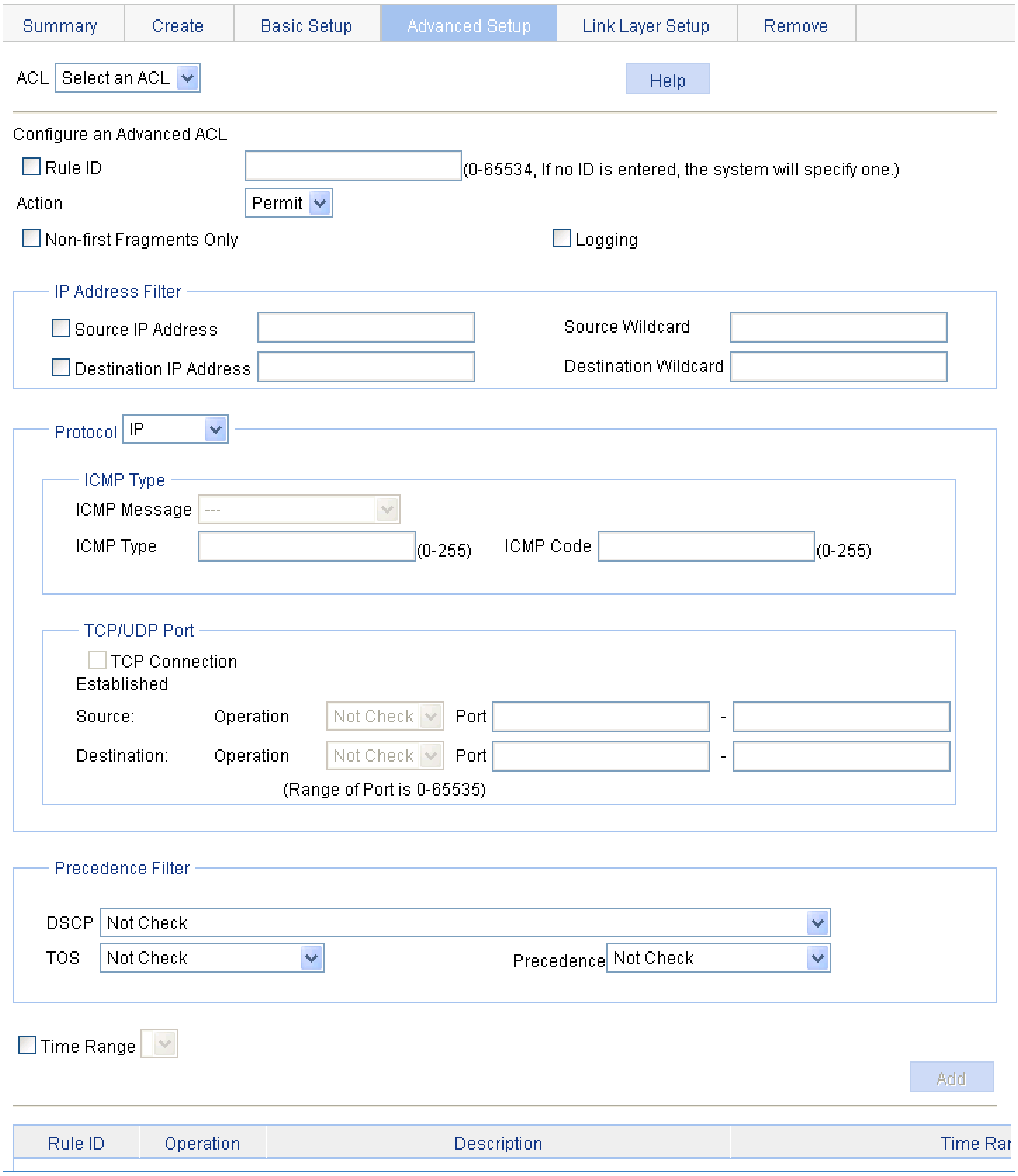
Item	Description
ACL	Select the basic IPv4 ACL for which you want to configure rules. Available ACLs are basic IPv4 ACLs.

Item	Description
Rule ID	Select the **Rule ID** box and enter a number for the rule. If you do not specify the rule number, the system will assign one automatically. NOTE: If the rule number you specify already exists, the following operations modify the configuration of the rule.
Action	Select the action to be performed for IPv4 packets matching the rule. • **Permit**—Allows matched packets to pass. • **Deny**—Drops matched packets.
Check Fragment	Select this box to apply the rule to only non-first fragments. If you do no select this box, the rule applies to all fragments and non-fragments.
Check Logging	Select this box 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** box and enter a source IPv4 address and a wildcard mask, in dotted decimal notation.
Source Wildcard	
Time Range	Select the time range during which the rule takes effect.

Configuring a rule for an advanced IPv4 ACL

1. Select **QoS** > **ACL IPv4** from the navigation tree.
2. Click the **Advance Setup** tab to enter the rule configuration page for an advanced IPv4 ACL.

Figure 449 Configuring an advanced IPv4 ACL



3. Configure a rule for an advanced IPv4 ACL as described in Table 136.
4. Click **Add**.

Table 136 Configuration items

Item	Description
ACL	Select the advanced IPv4 ACL for which you want to configure rules. Available ACLs are advanced IPv4 ACLs.

<table>
<tr><th colspan="3">Item</th><th>Description</th></tr>
<tr><td colspan="3">Rule ID</td><td>Select the Rule ID box and enter a number for the rule.
If you do not specify the rule number, the system will assign one automatically.
NOTE:
If the rule number you specify already exists, the following operations modify the configuration of the rule.</td></tr>
<tr><td colspan="3">Action</td><td>Select the action to be performed for packets matching the rule.
• Permit—Allows matched packets to pass.
• Deny—Drops matched packets.</td></tr>
<tr><td colspan="3">Non-First Fragments Only</td><td>Select this box to apply the rule to only non-first fragments.
If you do no select this box, the rule applies to all fragments and non-fragments.</td></tr>
<tr><td colspan="3">Logging</td><td>Select this box 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.</td></tr>
<tr><td rowspan="4">IP Address Filter</td><td colspan="2">Source IP Address</td><td rowspan="2">Select the Source IP Address box and enter a source IPv4 address and a source wildcard mask, in dotted decimal notation.</td></tr>
<tr><td colspan="2">Source Wildcard</td></tr>
<tr><td colspan="2">Destination IP Address</td><td rowspan="2">Select the Source IP Address box and enter a source IP address and a source wildcard mask, in dotted decimal notation.</td></tr>
<tr><td colspan="2">Destination Wildcard</td></tr>
<tr><td colspan="3">Protocol</td><td>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.</td></tr>
<tr><td rowspan="3">ICMP Type</td><td colspan="2">ICMP Message</td><td rowspan="3">Specify the ICMP message type and code.
These items are available only when you select 1 ICMP from the Protocol list.
If you select Other from the ICMP Message list, 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.</td></tr>
<tr><td colspan="2">ICMP Type</td></tr>
<tr><td colspan="2">ICMP Code</td></tr>
<tr><td rowspan="6">TCP/UDP Port</td><td colspan="2">TCP Connection Established</td><td>Select this box 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 list.</td></tr>
<tr><td rowspan="3">Source</td><td>Operator</td><td rowspan="5">Select the operators and enter 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 list.
Different operators have different configuration requirements for the port number fields:</td></tr>
<tr><td>Port</td></tr>
<tr><td>-</td></tr>
<tr><td rowspan="2">Destination</td><td>Operator</td></tr>
<tr><td>Port</td></tr>
</table>

<table>
<tr><th colspan="2">Item</th><th colspan="2">Description</th></tr>
<tr><td></td><td>-</td><td colspan="2">

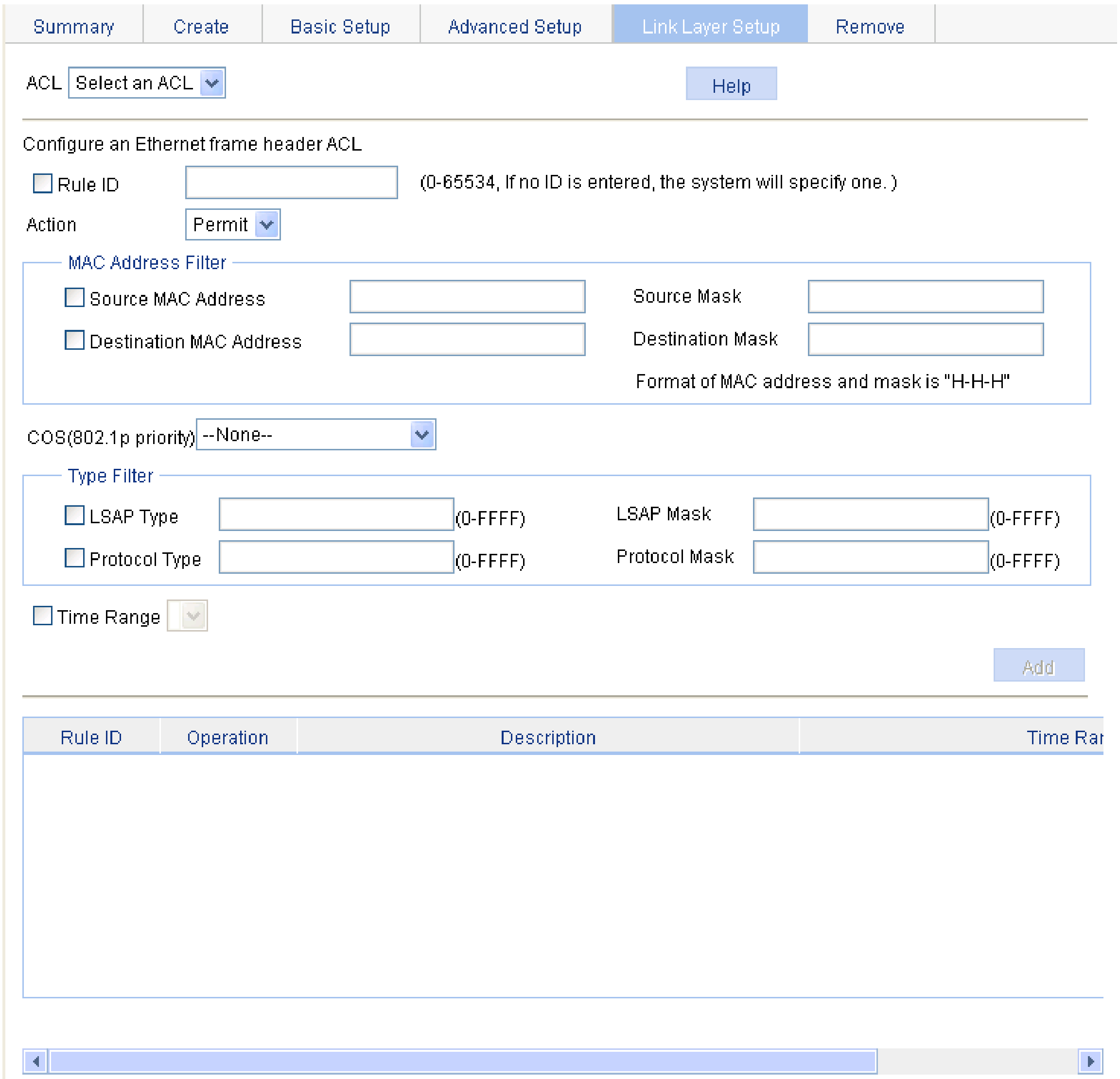
- **Not Check**—The following port number fields cannot be configured.
- **Range**—The following port number fields must be configured to define a port range.
- **Other values**—The first port number field must be configured and the second must not.

</td></tr>
<tr><td rowspan="3">Precedence Filter</td><td>DSCP</td><td>Specify the DSCP value.</td><td rowspan="3">IMPORTANT:
If you specify the ToS precedence or IP precedence when you specify the DSCP value, the specified TOS or IP precedence does not take effect.</td></tr>
<tr><td>TOS</td><td>Specify the ToS preference.</td></tr>
<tr><td>Precedence</td><td>Specify the IP precedence.</td></tr>
<tr><td colspan="2">Time Range</td><td colspan="2">Select the time range during which the rule takes effect.</td></tr>
</table>

Configuring a rule for an Ethernet frame header ACL

1. Select **QoS** > **ACL IPv4** from the navigation tree.
2. Click the **Link Layer Setup** tab to enter the rule configuration page for an Ethernet frame header IPv4 ACL.

Figure 450 Configuring a rule for an Ethernet frame header ACL



3. Configure a rule for an Ethernet frame header IPv4 ACL as described in Table 137.
4. Click **Add**.

Table 137 Configuration items

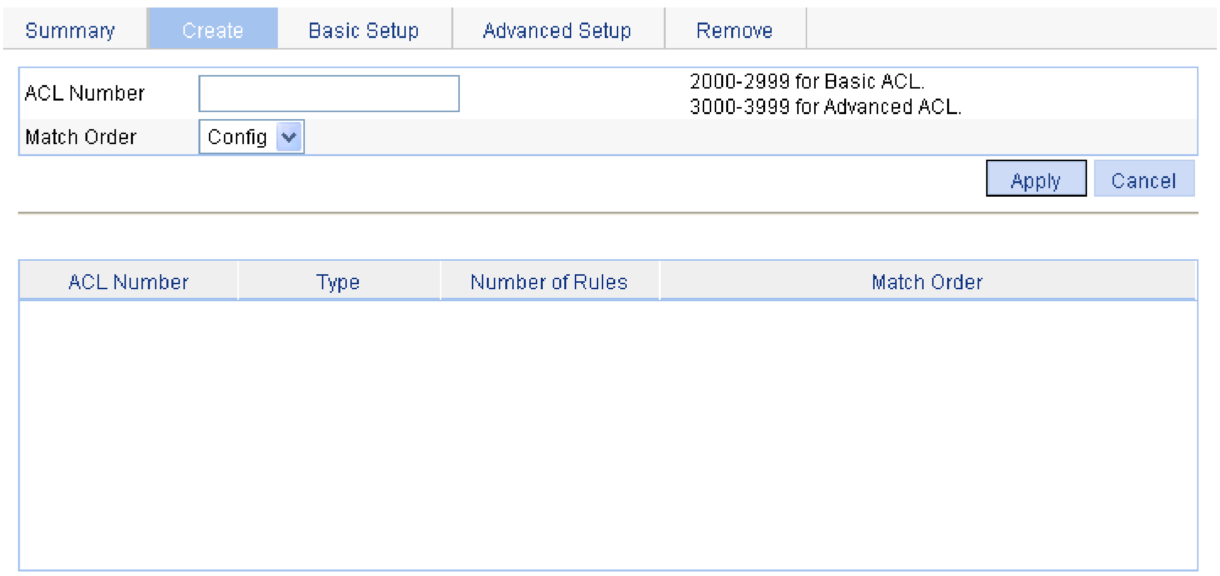
Item	Description
ACL	Select the Ethernet frame header IPv4 ACL for which you want to configure rules. Available ACLs are Ethernet frame header IPv4 ACLs.
Rule ID	Select the **Rule ID** box and enter a number for the rule. If you do not specify the rule number, the system will assign one automatically. NOTE: If the rule number you specify already exists, the following operations modify the configuration of the rule.

Item		Description
Action		Select the action 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** box and enter a source MAC address and a mask.
	Source Mask	
	Destination MAC Address	Select the **Destination MAC Address** box and enter a destination MAC address and a mask.
	Destination Mask	
COS(802.1p priority)		Specify the 802.1p priority for the rule.
Type Filter	LSAP Type	Select the **LSAP Type** box and specify the DSAP and SSAP fields in the LLC encapsulation by configuring the following items: • **LSAP Type**—Indicates the frame encapsulation format. • **LSAP Mask**—Indicates the LSAP mask.
	LSAP Mask	
	Protocol Type	Select the **Protocol Type** box and specify the link layer protocol type by configuring the following 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.

Adding an IPv6 ACL

1. Select **QoS** > **ACL IPv6** from the navigation tree.
2. Click the **Create** tab to enter the IPv6 ACL configuration page, as shown in Figure 451.

Figure 451 Adding an IPv6 ACL



3. Add an IPv6 ACL.

4. Click **Apply**.

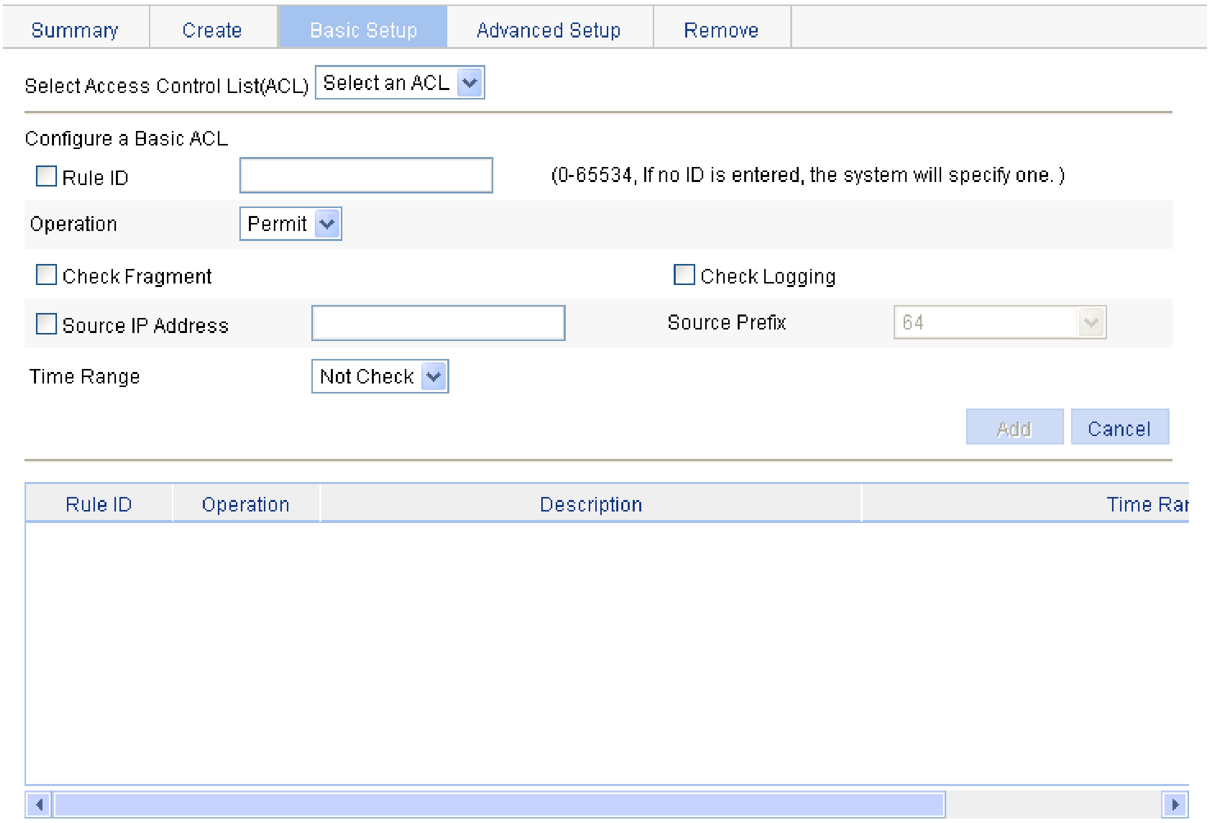
Table 138 Configuration items

Item	Description
ACL Number	Enter a number for the IPv6 ACL.
Match Order	Select a match order for the ACL. Available values are: • **Config**—Packets are compared against ACL rules in the order the rules are configured. • **Auto**—Packets are compared against ACL rules in the depth-first match order.

Configuring a rule for a basic IPv6 ACL

1. Select **QoS** > **ACL IPv6** from the navigation tree.
2. Click the **Basic Setup** tab to enter the rule configuration page for a basic IPv6 ACL, as shown in Figure 452.

Figure 452 Configuring a rule for a basic IPv6 ACL



3. Add a rule for a basic IPv6 ACL.
4. Click **Add**.

Table 139 Configuration items

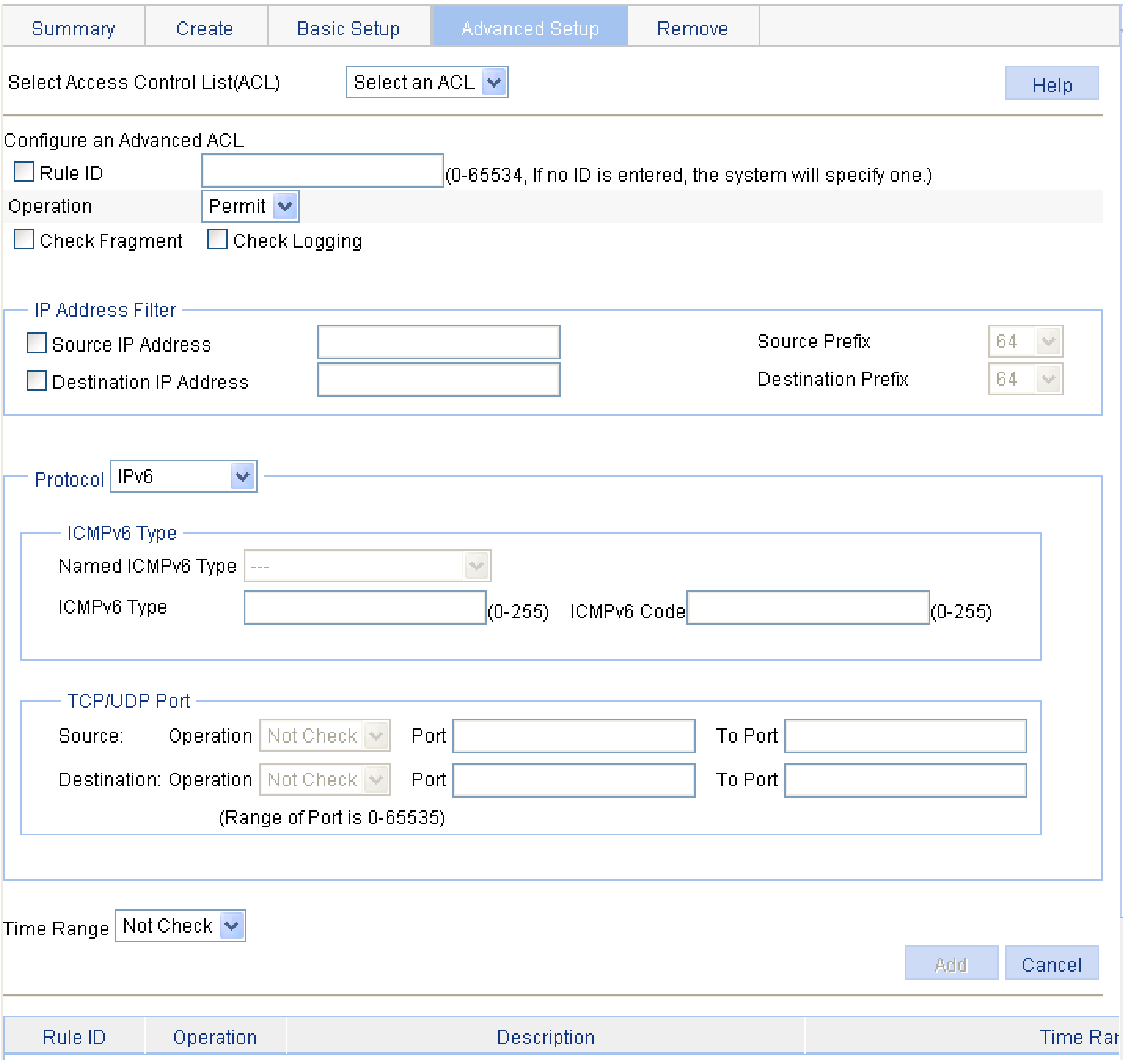
Item	Description
Select Access Control List (ACL)	Select the basic IPv6 ACL for which you want to configure rules.

Item	Description
Rule ID	Select the **Rule ID** box and enter a number for the rule. If you do not specify the rule number, the system will assign one automatically. IMPORTANT: If the rule number you specify already exists, the following operations modify the configuration of the rule.
Operation	Select the operation to be performed for IPv6 packets matching the rule. • **Permit**—Allows matched packets to pass. • **Deny**—Drops matched packets.
Check Fragment	Select this box to apply the rule to only non-first fragments. If you do no select this box, the rule applies to all fragments and non-fragments.
Check Logging	Select this box to keep a log of matched IPv6 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** box and enter a source IPv6 address and prefix length. The IPv6 address must be in a format like X:X::X:X. An IPv6 address consists of eight 16-bit long fields, each of which is expressed with two hexadecimal numbers and separated from its neighboring fields by colon (:).
Source Prefix	
Time Range	Select the time range during which the rule takes effect.

Configuring a rule for an advanced IPv6 ACL

1. Select **QoS** > **ACL IPv6** from the navigation tree.
2. Click the **Advance Setup** tab to enter the rule configuration page for an advanced IPv6 ACL, as shown in Figure 453.

Figure 453 Configuring a rule for an advanced IPv6 ACL



3. Add a rule for an advanced IPv6 ACL.
4. Click **Add**.

Table 140 Configuration items

Item	Description
Select Access Control List (ACL)	Select the advanced IPv6 ACL for which you want to configure rules.
Rule ID	Select the **Rule ID** box and enter a number for the rule. If you do not specify the rule number, the system will assign one automatically. IMPORTANT: If the rule number you specify already exists, the following operations modify the configuration of the rule.

<table>
<tr><th colspan="3">Item</th><th>Description</th></tr>
<tr><td colspan="3">Operation</td><td>Select the operation to be performed for IPv6 packets matching the rule.
• Permit—Allows matched packets to pass.
• Deny—Drops matched packets.</td></tr>
<tr><td colspan="3">Check Fragment</td><td>Select this box to apply the rule to only non-first fragments.
If you do no select this box, the rule applies to all fragments and non-fragments.</td></tr>
<tr><td colspan="3">Check Logging</td><td>Select this box to keep a log of matched IPv6 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.</td></tr>
<tr><td rowspan="4">IP Address Filter</td><td colspan="2">Source IP Address</td><td rowspan="2">Select the Source IP Address box and enter a source IPv6 address and prefix length.
The IPv6 address must be in a format like X:X::X:X. An IPv6 address consists of eight 16-bit long fields, each of which is expressed with two hexadecimal numbers and separated from its neighboring fields by colon (:).</td></tr>
<tr><td colspan="2">Source Prefix</td></tr>
<tr><td colspan="2">Destination IP Address</td><td rowspan="2">Select the Destination IP Address box and enter a destination IPv6 address and prefix length.
The IPv6 address must be in a format like X:X::X:X. An IPv6 address consists of eight 16-bit long fields, each of which is expressed with two hexadecimal numbers and separated from its neighboring fields by colon (:).</td></tr>
<tr><td colspan="2">Destination Prefix</td></tr>
<tr><td colspan="3">Protocol</td><td>Select the protocol to be carried by IP.
If you select 58 ICMPv6, you can configure the ICMP message type and code; if you select 6 TCP or 17 UDP, you can configure the TCP or UDP specific items.</td></tr>
<tr><td rowspan="3">ICMPv6 Type</td><td colspan="2">Named ICMPv6 Type</td><td rowspan="3">Specify the ICMPv6 message type and code.
These items are available only when you select 58 ICMPv6 from the Protocol list.
If you select Other from the Named ICMPv6 Type list, you need to enter values in the ICMPv6 Type and ICMPv6 Code fields. Otherwise, the two fields will take the default values, which cannot be changed.</td></tr>
<tr><td colspan="2">ICMPv6 Type</td></tr>
<tr><td colspan="2">ICMPv6 Code</td></tr>
<tr><td rowspan="6">TCP/UDP Port</td><td rowspan="3">Source</td><td>Operator</td><td rowspan="6">Select the operators and enter 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 list.
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.</td></tr>
<tr><td>Port</td></tr>
<tr><td>To Port</td></tr>
<tr><td rowspan="3">Destination</td><td>Operator</td></tr>
<tr><td>Port</td></tr>
<tr><td>Port</td></tr>
<tr><td colspan="3">Time Range</td><td>Select the time range during which the rule takes effect.</td></tr>
</table>

Configuration guidelines

When you configure an ACL, follow these guidelines:

- You cannot add a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
- 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.

Configuring QoS

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 email.

QoS requirements of new applications

The Internet has been growing along with the fast development of networking technologies.

Besides traditional applications such as WWW, email 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 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.

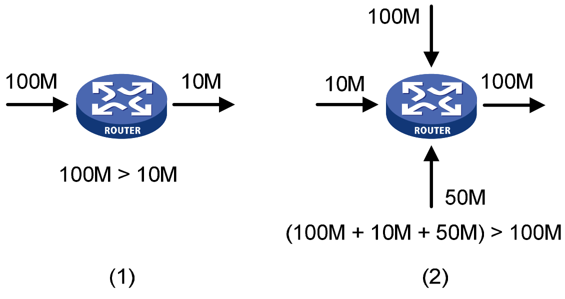
Congestion: causes, impacts, and countermeasures

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. Figure 454 shows two common cases:

Figure 454 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 of 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 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.

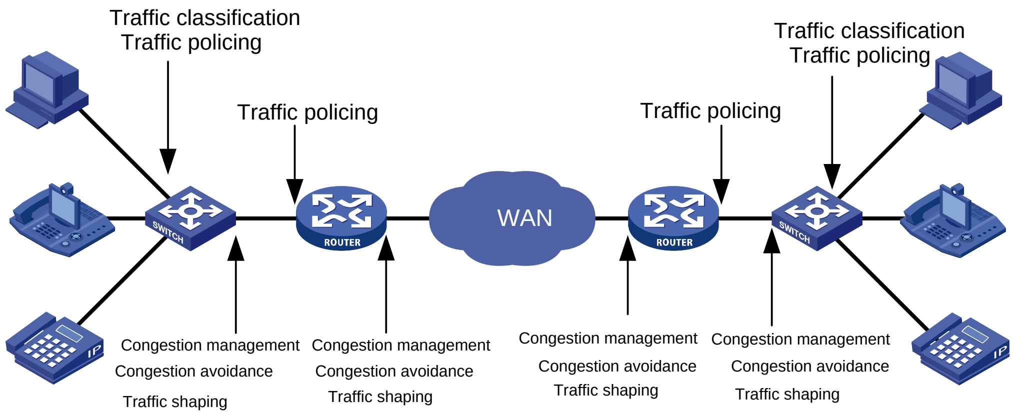
Countermeasures

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 455 End-to-end QoS model



As shown in Figure 455, 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.

This section is focused on traffic classification, and the subsequent sections will introduce the other technologies in details.

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.

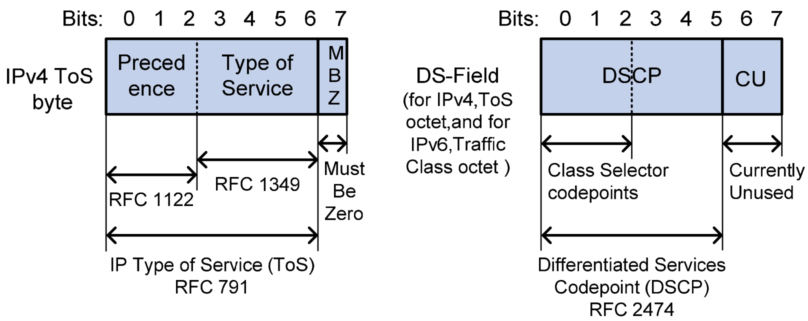
When packets are classified on the network boundary, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be directly used to classify the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream network can either use 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 use depends on the current phase and the resources of the network. For example, CAR polices 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

IP precedence and DSCP values

Figure 456 ToS field and DS field



As shown in Figure 456, 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 differentiated services code point (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 141 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

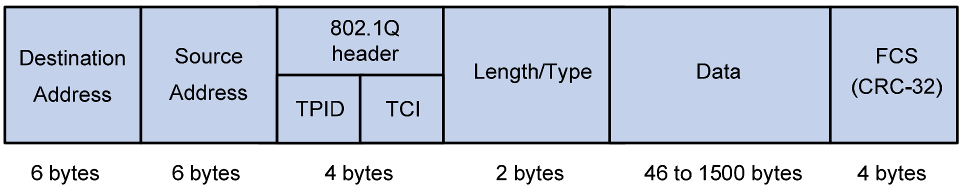
Table 142 Description on DSCP values

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)

802.1p priority

802.1p priority lies in Layer 2 packet headers and applies to occasions where Layer 3 header analysis is not needed and QoS must be assured at Layer 2.

Figure 457 An Ethernet frame with an 802.1Q tag header



As shown in Figure 457, 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 458 presents the format of the 802.1Q tag header. The priority in the 802.1Q tag header is called "802.1p priority", because its use is defined in IEEE 802.1p. Table 143 presents the values for 802.1p priority.

Figure 458 802.1Q tag header

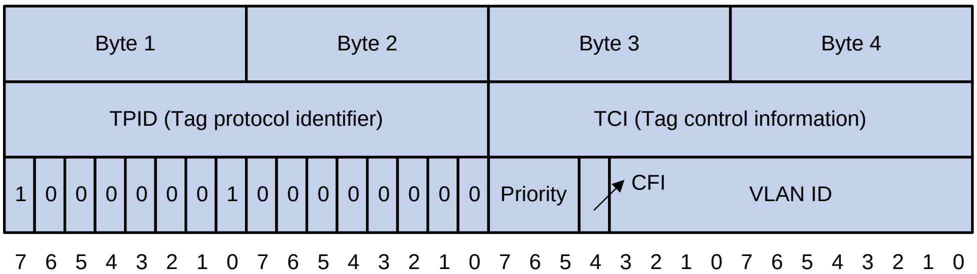


Table 143 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (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

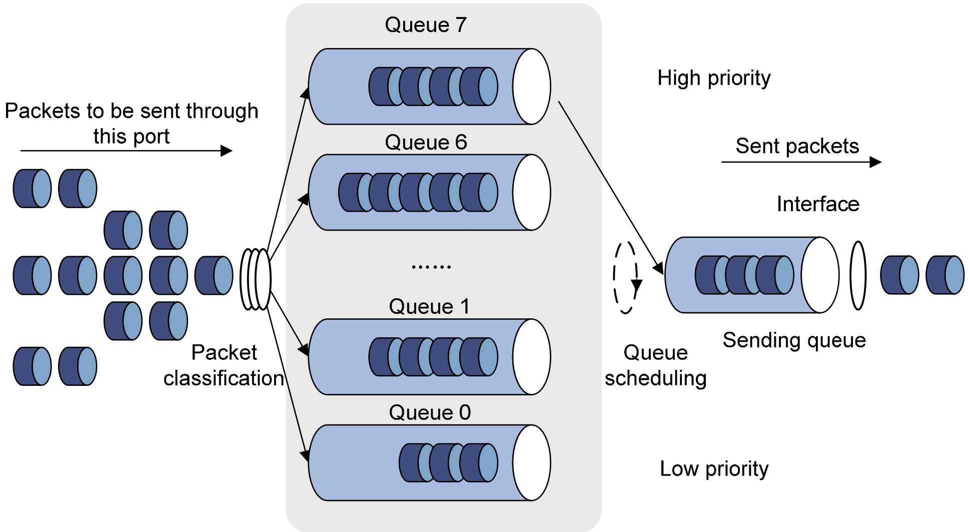
In general, congestion management uses queuing technology. The system uses a certain queuing algorithm for traffic classification, and then uses a certain precedence algorithm to send the traffic. Each queuing algorithm handles a particular network traffic problem and has significant impacts on bandwidth 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 designed for mission-critical applications, which require preferential service to reduce response delay when congestion occurs.

Figure 459 SP queuing



A typical switch provides eight queues per port. As shown in Figure 459, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

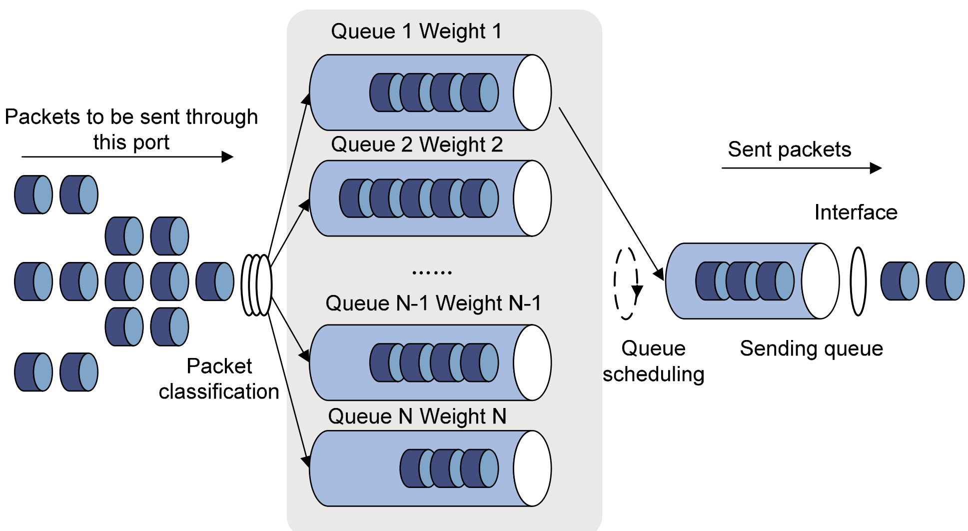
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. You can assign mission-critical packets to the high priority queue to make sure 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 the higher priority queues have packets. This may cause lower priority traffic to starve to death.

WRR queuing

WRR queuing schedules all the queues in turn to make sure that every queue can be served for a certain time, as shown in Figure 460.

Figure 460 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, and the disadvantage of SP queuing (that packets in low-priority queues may fail to be served for a long time) is avoided.

Another advantage of WRR queuing is that while the queues are scheduled in turn, the service time for each queue is not fixed. If a queue is empty, the next queue will be scheduled immediately. This improves bandwidth resource use efficiency.

All the queues are scheduled by WRR. 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.

You can implement SP+WRR queue scheduling on a port by assigning some queues on the port to the SP scheduling group when you configure 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.

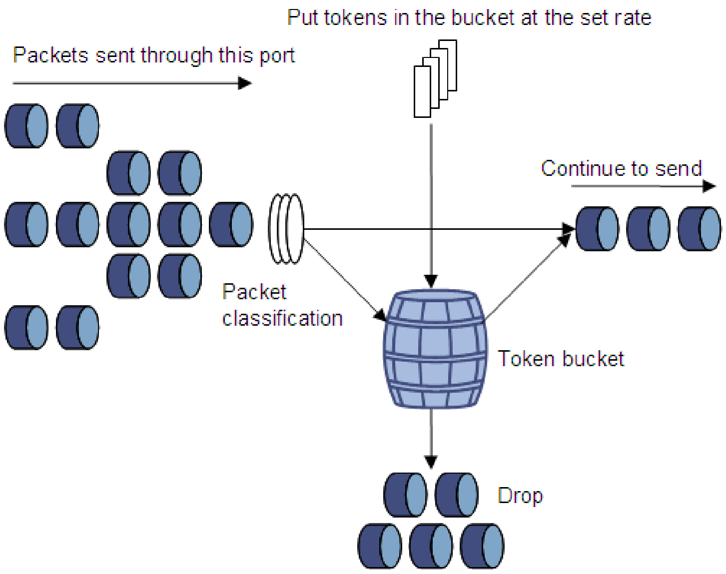
Line rate

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 incoming or outgoing packets of 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 461 Evaluate traffic with the token bucket



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 (usually, 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:

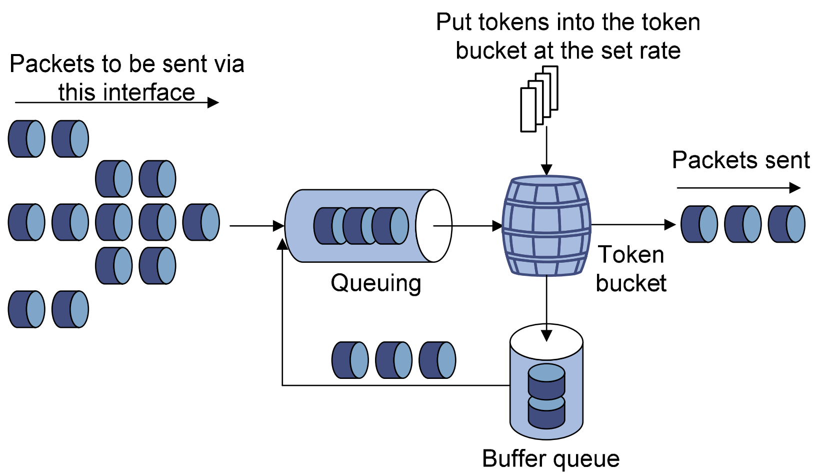
- **Mean rate**—Rate at which tokens are put into the bucket, or the permitted average rate of traffic. It is usually set to the committed information rate (CIR).
- **Burst size**—The capacity of the token bucket, or the maximum traffic size permitted in each burst. It is usually set to the committed 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 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

This section uses the outgoing packets for example. With line rate configured on an interface, all packets to be sent out of the interface are firstly handled by the token bucket of line rate. If the token bucket has enough tokens, 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 462 Line rate implementation



With a token bucket used for traffic control, when the token bucket has tokens, 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, the traffic rate is limited, and bursty traffic is allowed.

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 priority, DSCP values, IP precedence, and local precedence).

- For more information about 802.1p priority, DSCP values, and IP precedence, see "Packet precedences."

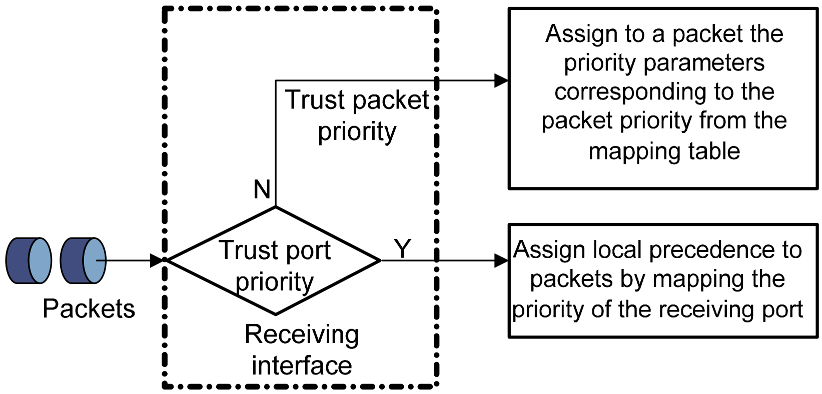
- Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to an output queue. Packets with the highest local precedence are processed preferentially.

The device provides the following 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 463 shows the process of priority mapping on a device.

Figure 463 Priority mapping process



Introduction to priority mapping tables

The device provides the following types of priority mapping tables:

- **CoS to DSCP**—802.1p-to-DSCP mapping table.
- **CoS to Queue**—802.1p-to-local mapping table.
- **DSCP to CoS**—DSCP-to-802.1p mapping table, which applies to only IP packets.
- **DSCP to DSCP**—DSCP-to-DSCP mapping table, which applies to only IP packets.
- **DSCP to Queue**—DSCP-to-local mapping table, which applies to only IP packets.

Table 144 through Table 145 list the default priority mapping tables.

Table 144 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

Input CoS value	Local precedence (Queue)	DSCP
7	7	56

Table 145 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
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.

Recommended QoS configuration procedures

Recommended QoS policy configuration procedure

A QoS policy involves the following components: class, traffic behavior, and policy. You can associate a class with a traffic behavior using a QoS policy.

1. Class

Classes 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 to regulate the inbound or outbound traffic of the port. A QoS policy can be applied to multiple ports. Only one policy can be applied in the inbound direction of a port.

Perform the tasks in Table 146 to configure a QoS policy:

Table 146 Recommended QoS policy configuration procedure

Step	Remarks
1. Adding a class	(Required) Add a class and specify the logical relationship between the match criteria in the class.
2. Configuring classification rules	(Required) Configure match criteria for the class.
3. Adding a traffic behavior	(Required) Add a traffic behavior.
4. Configure actions for the behavior: • Configuring traffic redirecting for a traffic behavior • Configuring other actions for a traffic behavior	(Required) Use either approach Configure various actions for the traffic behavior.
5. Adding a policy	(Required) Add a policy.
6. 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. Associating a class already associated with a traffic behavior will overwrite the old association.
7. Applying a policy to a port	(Required) Apply the QoS policy to a port.

Recommended queue scheduling configuration procedure

Step	Remarks
1. Configuring queue scheduling on a port	(Optional) Configure the queue scheduling mode for a port.

Recommended line rate configuration procedure

Step	Remarks
1. Configuring line rate on a port	(Required) Limit the rate of incoming packets or outgoing packets of a physical port.

Recommended priority mapping table configuration procedure

Step	Remarks
1. Configuring priority mapping tables	(Optional) Set priority mapping tables.

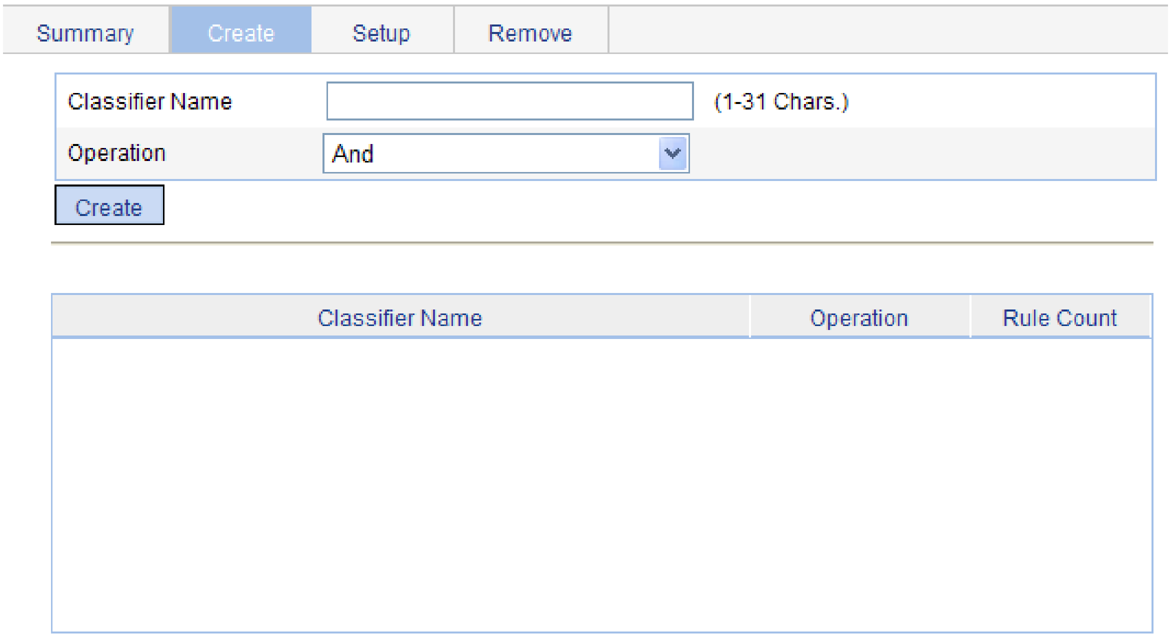
Recommended priority trust mode configuration procedure

Step	Remarks
1. Configuring priority trust mode on a port	(Required) Set the priority trust mode of a port.

Adding a class

1. Select **QoS** > **Classifier** from the navigation tree.
2. Click the **Create** tab to enter the page for adding a class.

Figure 464 Adding a class



3. Add a class as described in Table 147.
4. Click **Create**.

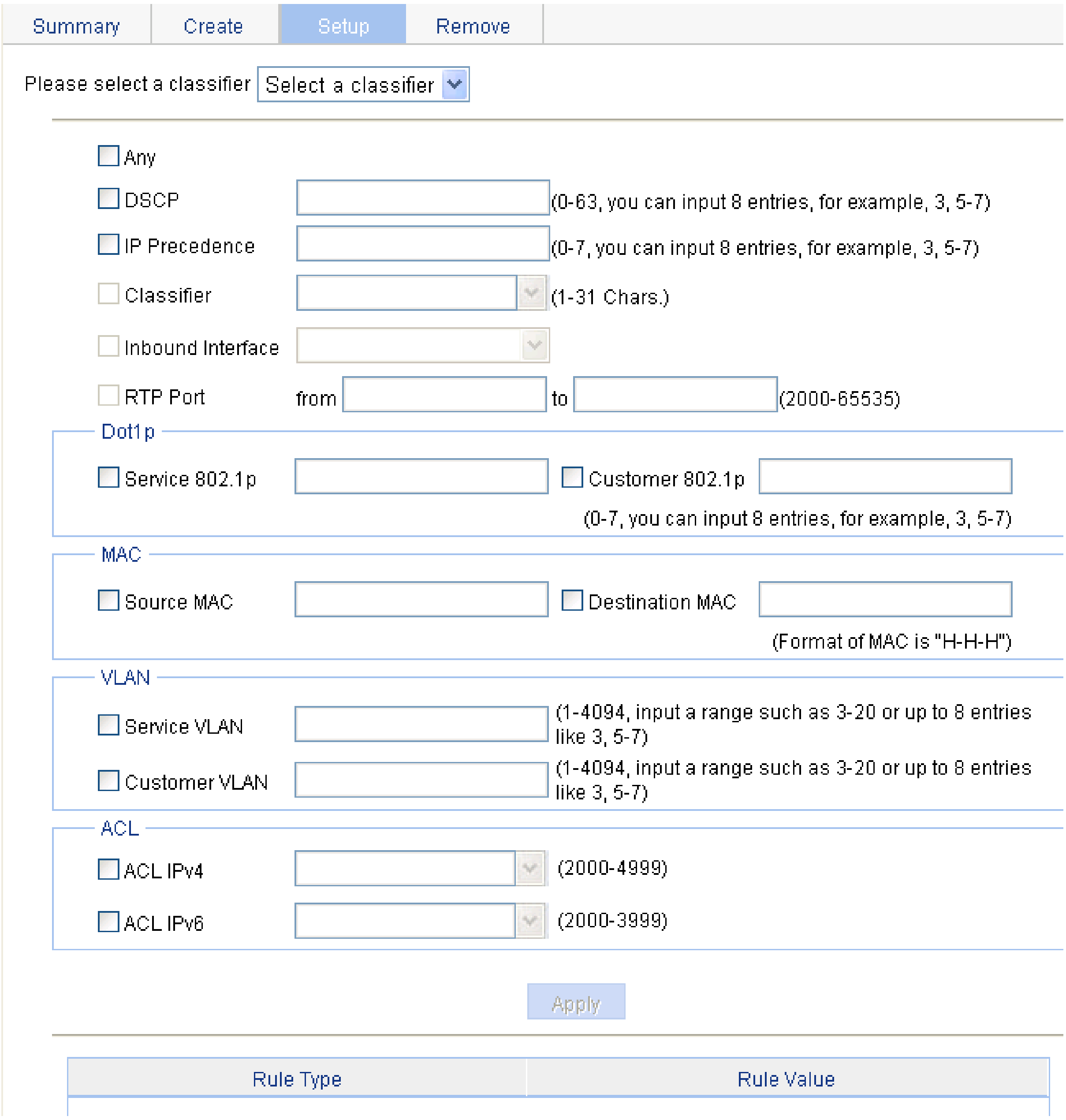
Table 147 Configuration items

Item	Description
Classifier Name	Specify a name for the classifier to be added.
Operator	Specify the logical relationship between rules of the classifier. • **and**—Specifies the relationship between the rules in a class as logic AND. 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. The device considers a packet belongs to a class as long as the packet matches one of the rules in the class.

Configuring classification rules

1. Select **QoS** > **Classifier** from the navigation tree.
2. Click **Setup** to enter the page for setting a class.

Figure 465 Configuring classification rules



3. Configure classification rules for a class as described in Table 148.
4. Click **Apply**.

Table 148 Configuration items

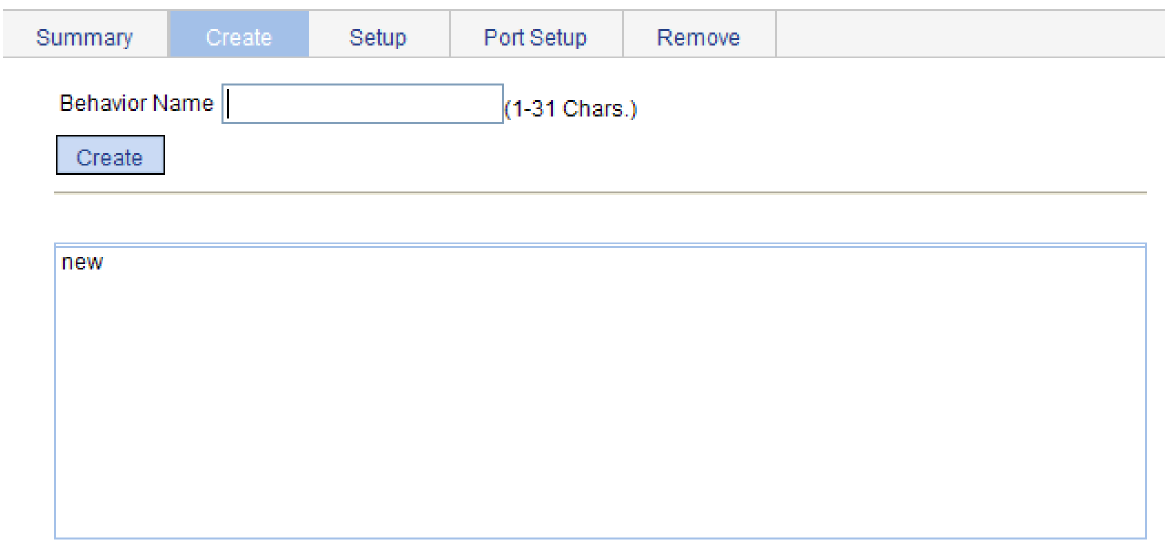
Item		Description
Please select a classifier		Select an existing classifier from the list.
Any		Define a rule to match all packets. Select the box to match all packets.
DSCP		Define a rule to match DSCP values. If multiple such rules are configured for a class, the new configuration does not overwrite 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.
Dot1p	Service 802.1p	Define a rule to match the service 802.1p priority 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 priority values each time. If multiple identical 802.1p priority values are specified, the system considers them as one. The relationship between different 802.1p priority values is **OR**. After such configurations, all the 802.1p priority values are arranged in ascending order automatically.
	Customer 802.1p	Define a rule to match the customer 802.1p priority 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 priority values each time. If multiple identical 802.1p priority values are specified, the system considers them as one. The relationship between different 802.1p priority values is **OR**. After such configurations, all the 802.1p priority 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 either of the following 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 either of the following 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	ACL IPv4	Define an IPv4 ACL-based rule.
	ACL IPv6	Define an IPv6 ACL-based rule.

Adding a traffic behavior

1. Select **QoS** > **Behavior** from the navigation tree.
2. Click the **Create** tab to enter the page for adding a traffic behavior.

Figure 466 Adding a traffic behavior



3. Add a traffic behavior as described in Table 149.
4. Click **Create**.

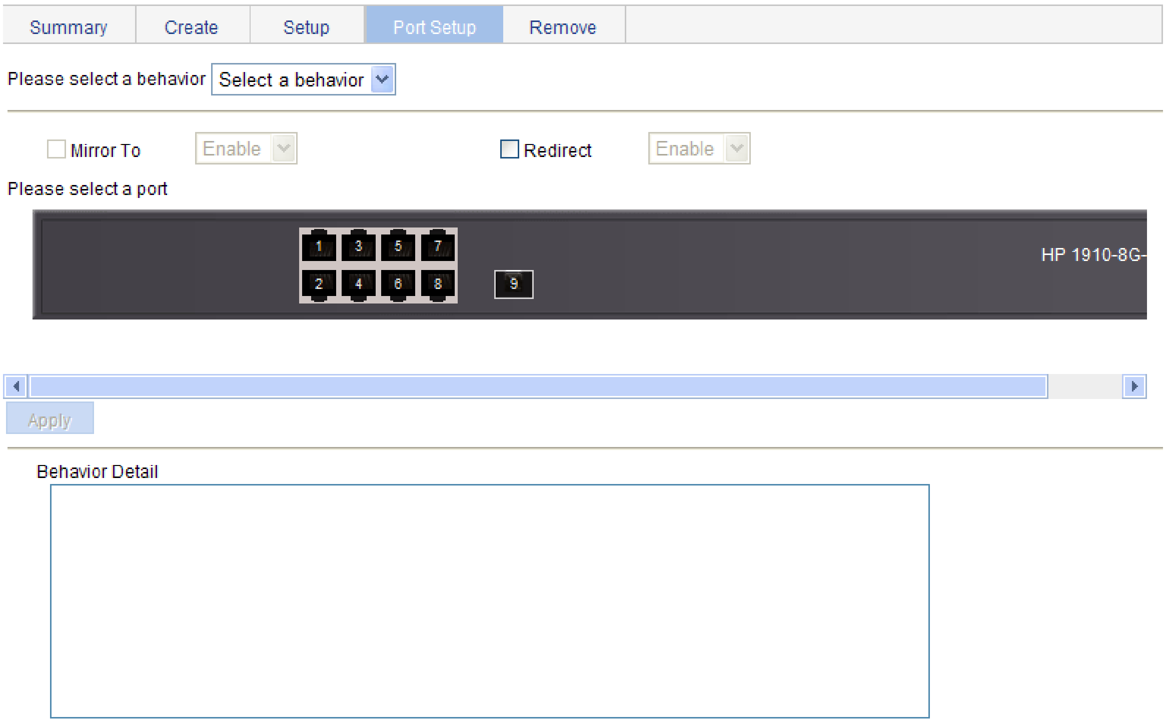
Table 149 Configuration items

Item	Description
Behavior name	Specify a name for the behavior to be added.

Configuring traffic redirecting for a traffic behavior

1. Select **QoS** > **Behavior** from the navigation tree.
2. Click **Port Setup** to enter the port setup page for a traffic behavior.

Figure 467 Port setup page for a traffic behavior



3. Configure traffic redirecting as described in Table 150.
4. Click **Apply**.

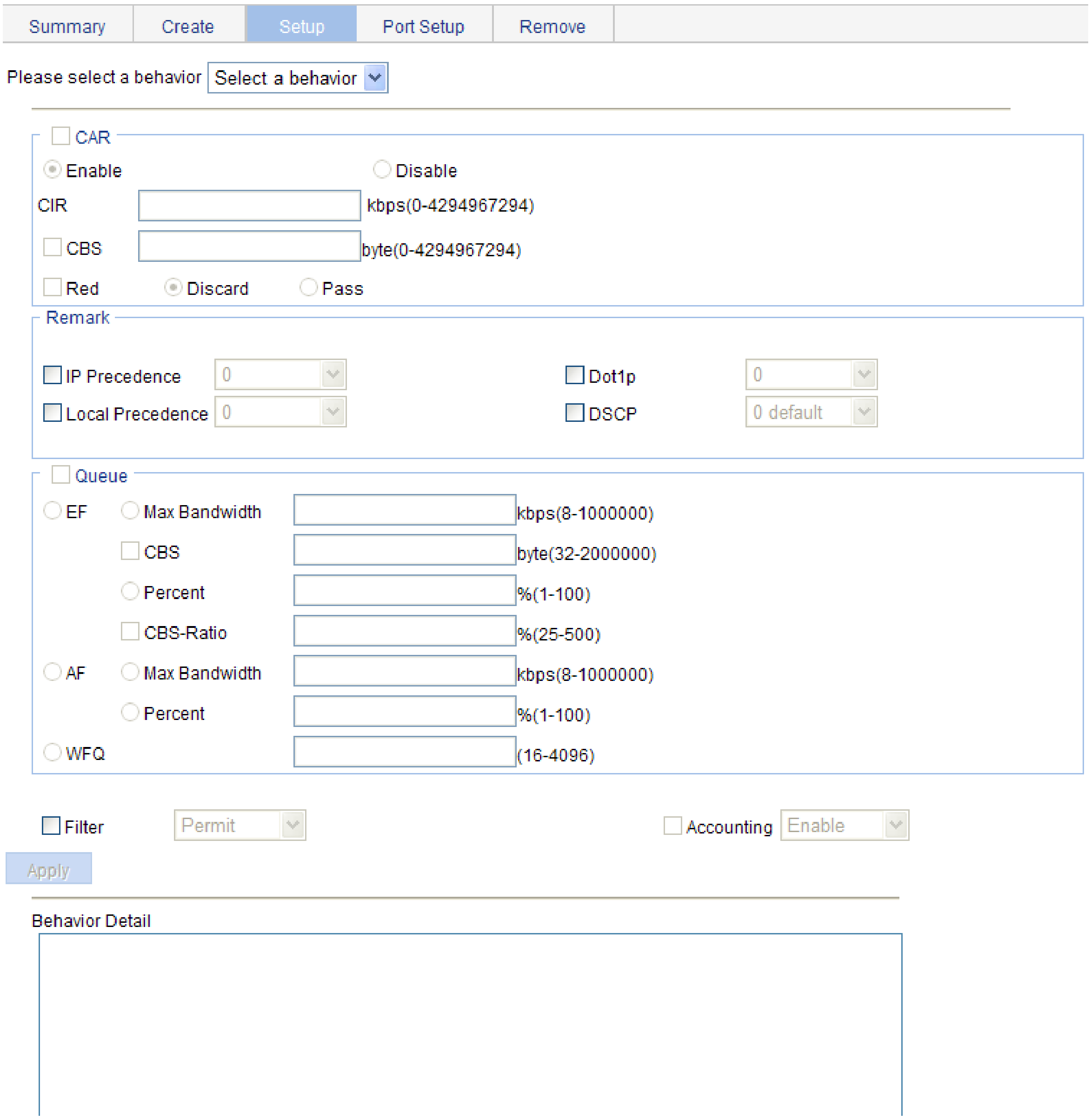
Table 150 Configuration items

Item	Description
Please select a behavior	Select an existing behavior in the 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.

Configuring other actions for a traffic behavior

1. Select **QoS** > **Behavior** from the navigation tree.
2. Click **Setup** to enter the page for setting a traffic behavior.

Figure 468 Setting a traffic behavior



3. Configure other actions for a traffic behavior as described in Table 151.
4. Click **Apply**.

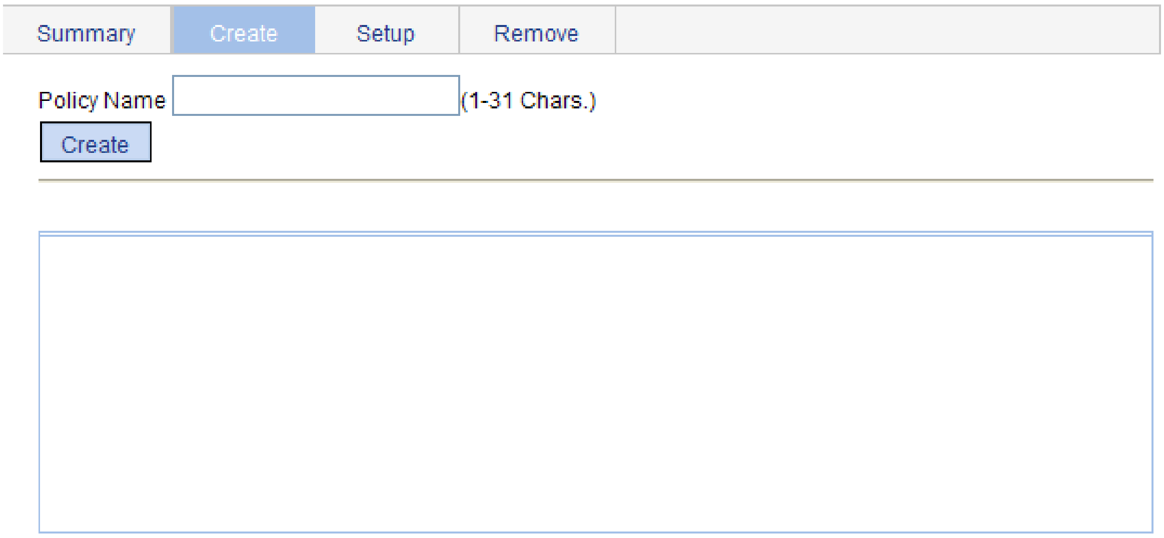
Table 151 Configuration items

<table>
<tr><th colspan="2">Item</th><th>Description</th></tr>
<tr><td colspan="2">Please select a behavior</td><td>Select an existing behavior in the list.</td></tr>
<tr><td rowspan="4">Remark</td><td>IP Precedence</td><td>Configure the action of marking IP precedence for packets.
Select the IP Precedence box and then select the IP precedence value to be marked for packets in the following list. Select Not Set to cancel the action of marking IP precedence.</td></tr>
<tr><td>Dot1p</td><td>Configure the action of marking 802.1p priority for packets.
Select the Dot1p box and then select the 802.1p priority value to be marked for packets in the following list. Select Not Set to cancel the action of marking 802.1p priority.</td></tr>
<tr><td>Local Precedence</td><td>Configure the action of marking local precedence for packets.
Select the Local Precedence box and then select the local precedence value to be marked for packets in the following list. Select Not Set to cancel the action of marking local precedence.</td></tr>
<tr><td>DSCP</td><td>Configure the action of marking DSCP value for packets.
Select the DSCP box and then select the DSCP value to be marked for packets in the following list. Select Not Set to cancel the action of marking DSCP value.</td></tr>
<tr><td colspan="2">Filter</td><td>Configure the packet filtering action.
After selecting the Filter box, select one item in the following list:
• Permit—Forwards the packet.
• Deny—Drops the packet.
• Not Set—Cancels the packet filtering action.</td></tr>
</table>

Adding a policy

1. Select **QoS** > **QoS Policy** from the navigation tree.
2. Click the **Add** tab to enter the page for adding a policy, as shown in Figure 469.

Figure 469 Adding a policy



3. Add a policy as described in Table 152.
4. Click **Create**.

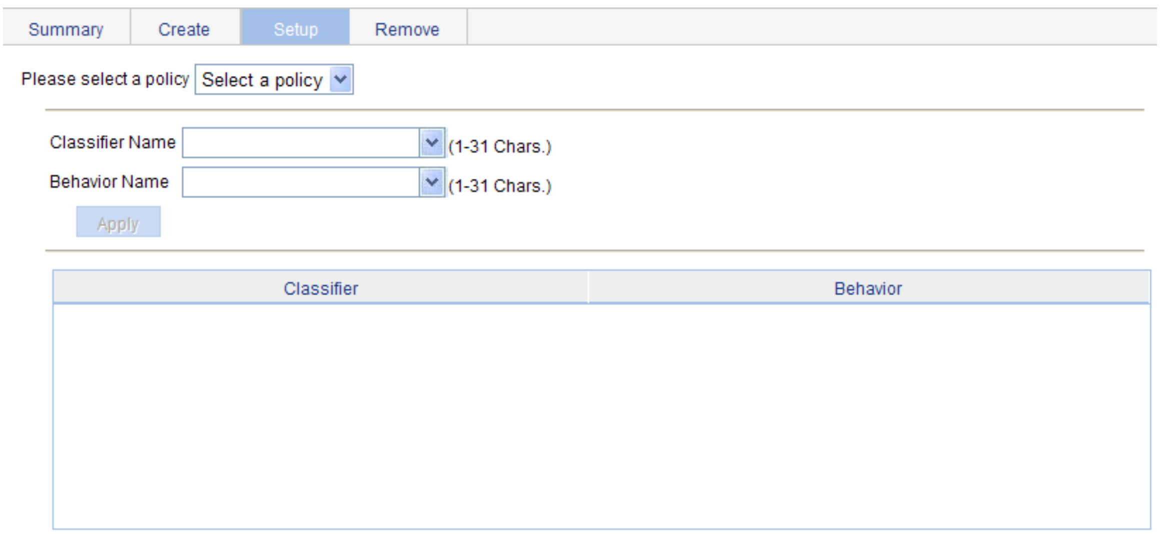
Table 152 Configuration items

Item	Description
Policy Name	Specify a name for the policy to be added.

Configuring classifier-behavior associations for the policy

1. Select **QoS** > **QoS Policy** from the navigation tree.
2. Click **Setup** to enter the page for setting a policy.

Figure 470 Setting a policy



3. Configure a classifier-behavior association for a policy as described in Table 153.
4. Click **Apply**.

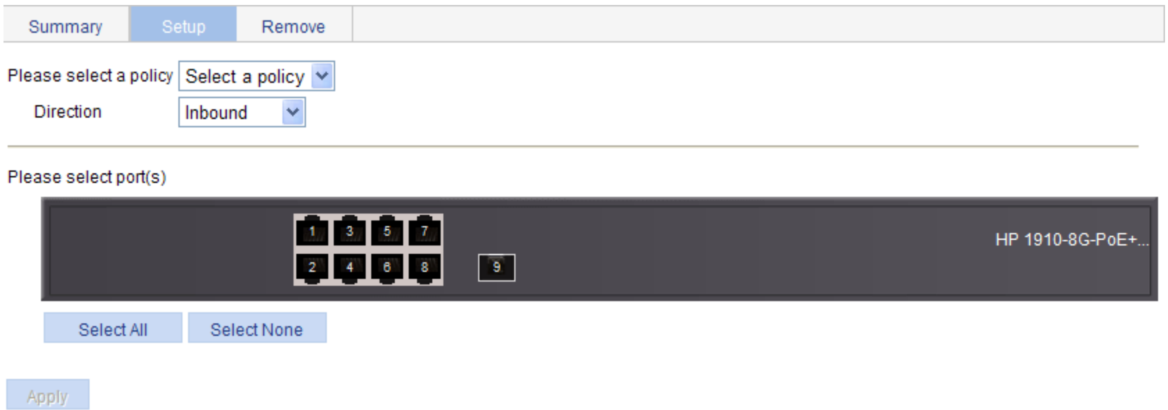
Table 153 Configuration items

Item	Description
Please select a policy	Select an existing policy in the list.
Classifier Name	Select an existing classifier in the list.
Behavior Name	Select an existing behavior in the list.

Applying a policy to a port

1. Select **QoS** > **Port Policy** from the navigation tree.
2. Click **Setup** to enter the page for applying a policy to a port.

Figure 471 Applying a policy to a port



3. Apply a policy to a port as described in Table 154.
4. Click **Apply**.

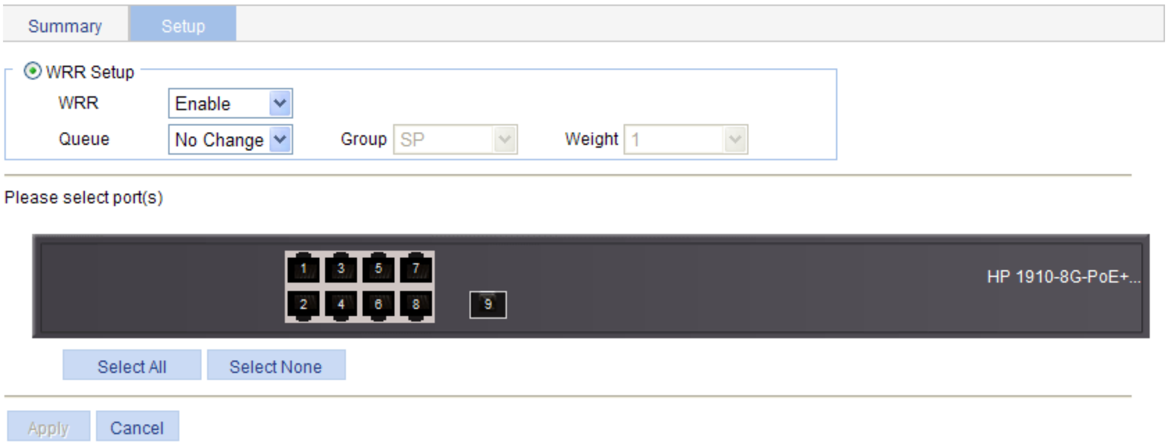
Table 154 Configuration items

Item	Description
Please select a policy	Select an existing policy in the list.
Direction	Set the direction in which the policy is to be applied. **Inbound** means to apply 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.

Configuring queue scheduling on a port

1. Select **QoS** > **Queue** from the navigation tree.
2. Click **Setup** to enter the queue scheduling configuration page.

Figure 472 Configuring queue scheduling



3. Configure queue scheduling on a port as described in Table 155.
4. Click **Apply**.

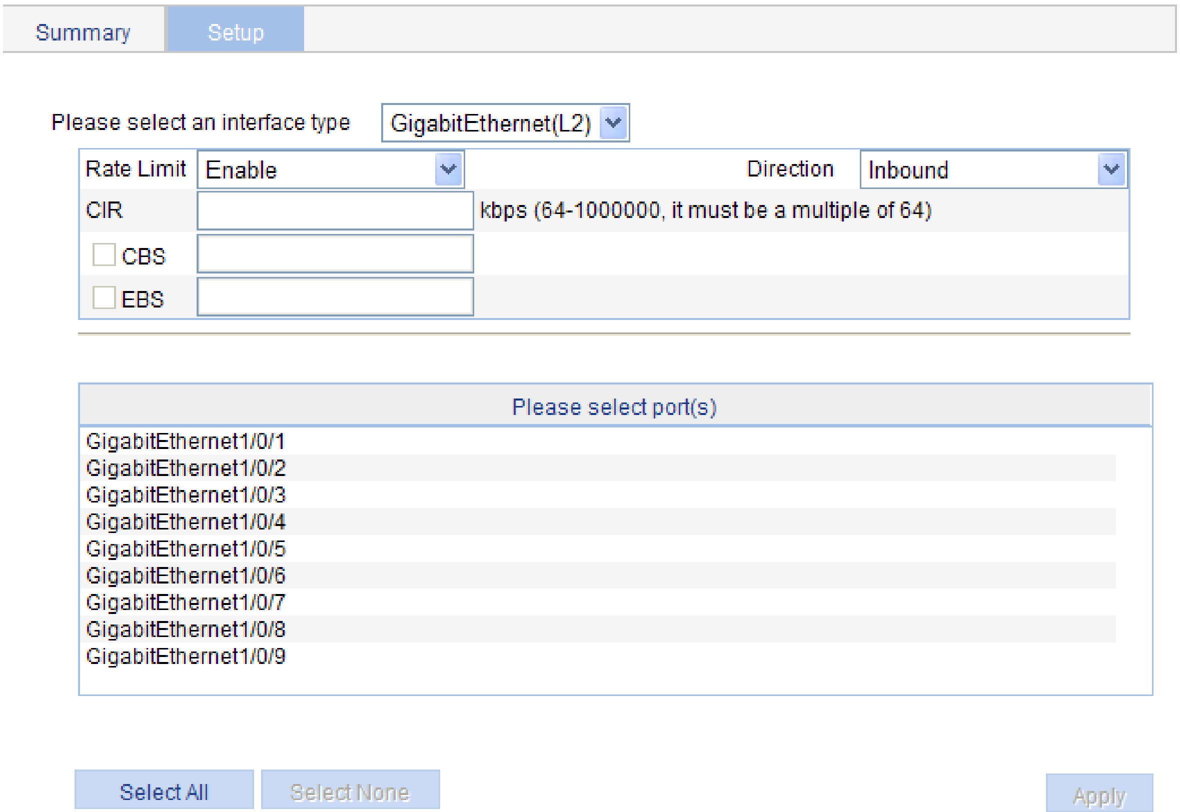
Table 155 Configuration items

Item		Description
WRR Setup	WRR	Enable or disable the WRR queue scheduling mechanism on selected ports. The following 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. A queue ID ranges from 0 to 7.
	Group	Specify the group the current queue is to be assigned to. This 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 list 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.

Configuring line rate on a port

1. Select **QoS** > **Line rate** from the navigation tree.
2. Click the **Setup** tab to enter the line rate configuration page.

Figure 473 Configuring line rate on a port



3. Configure line rate on a port as described in Table 156.
4. Click **Apply**.

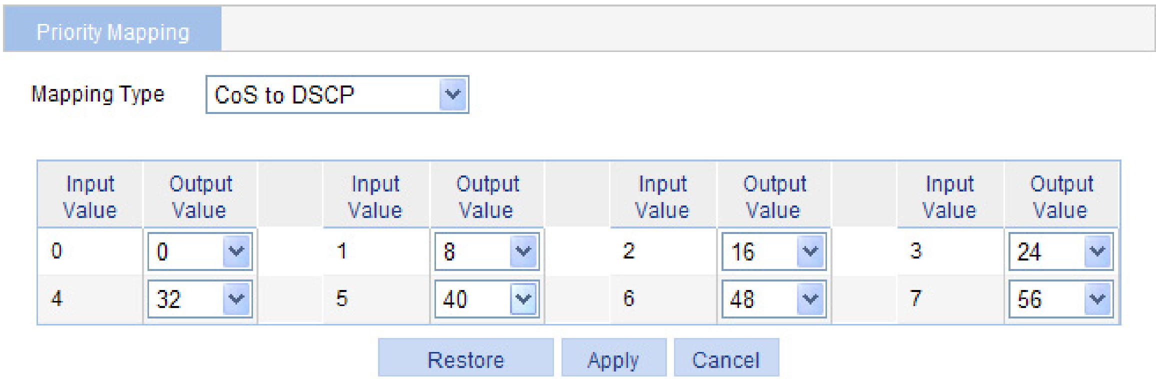
Table 156 Configuration items

Item	Description
Please select an interface type	Select the types of interfaces to be configured with line rate.
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.
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.

Configuring priority mapping tables

1. Select **QoS** > **Priority Mapping** from the navigation tree to enter the priority mapping configuration page.

Figure 474 Configuring priority mapping tables



2. Configure a priority mapping table as described in Table 157.
3. Click **Apply**.

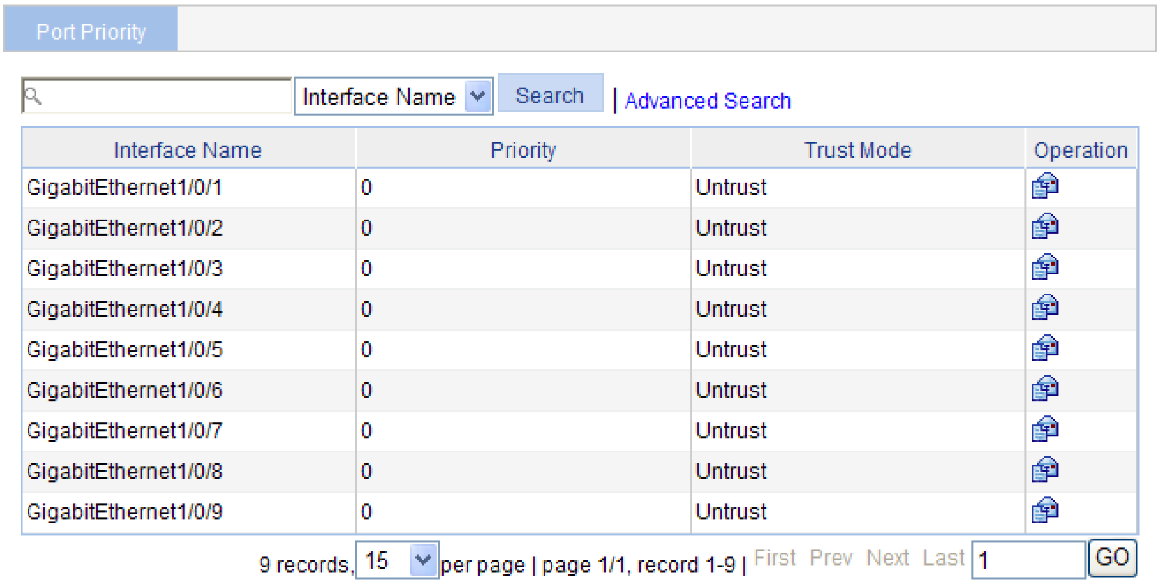
Table 157 Configuration items

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.
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**.

Configuring priority trust mode on a port

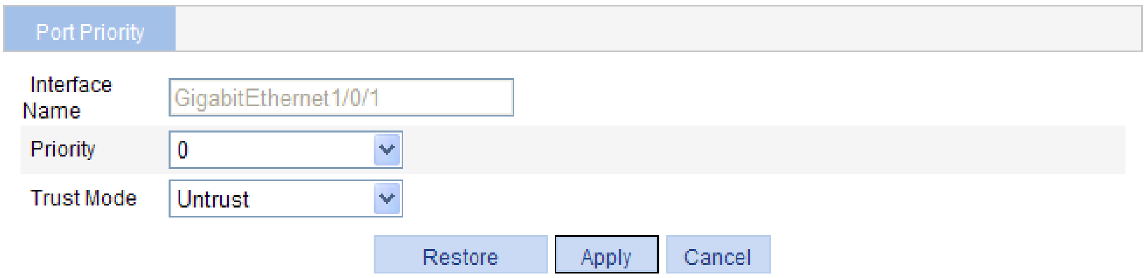
1. Select **QoS** > **Port Priority** from the navigation tree to enter the port priority configuration page.

Figure 475 Configuring port priority



2. Click the icon for a port to enter the page for modifying port priority.

Figure 476 The page for modifying port priority



3. Configure the port priority for a port as described in Table 158.
4. Click **Apply**.

Table 158 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**—Packet priority is not trusted. • **CoS**—802.1p priority of the incoming packets is trusted and used for priority mapping. • **DSCP**—DSCP value of the incoming packets is trusted and used for priority mapping.

Configuration guidelines

If an ACL is referenced by a QoS policy for defining traffic classification rules, packets matching the referenced ACL rule are organized as a class and the behavior defined in the QoS policy applies to the class regardless of whether the referenced ACL rule is a **deny** or **permit** clause.

ACL and QoS configuration example

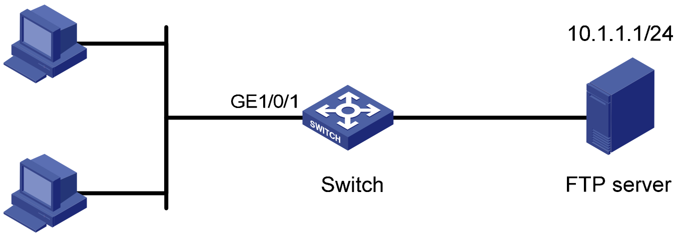
Network requirements

As shown in Figure 477, the FTP server (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. Add 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.

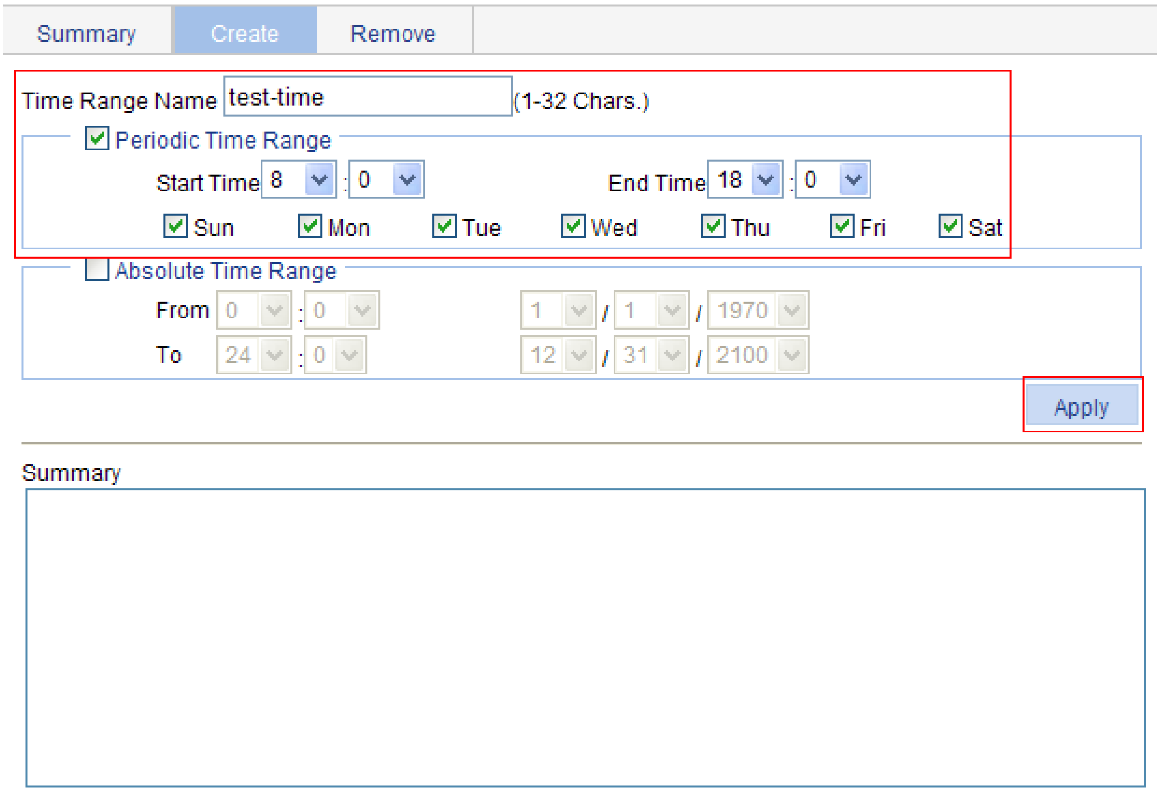
Figure 477 Network diagram



Configuring Switch

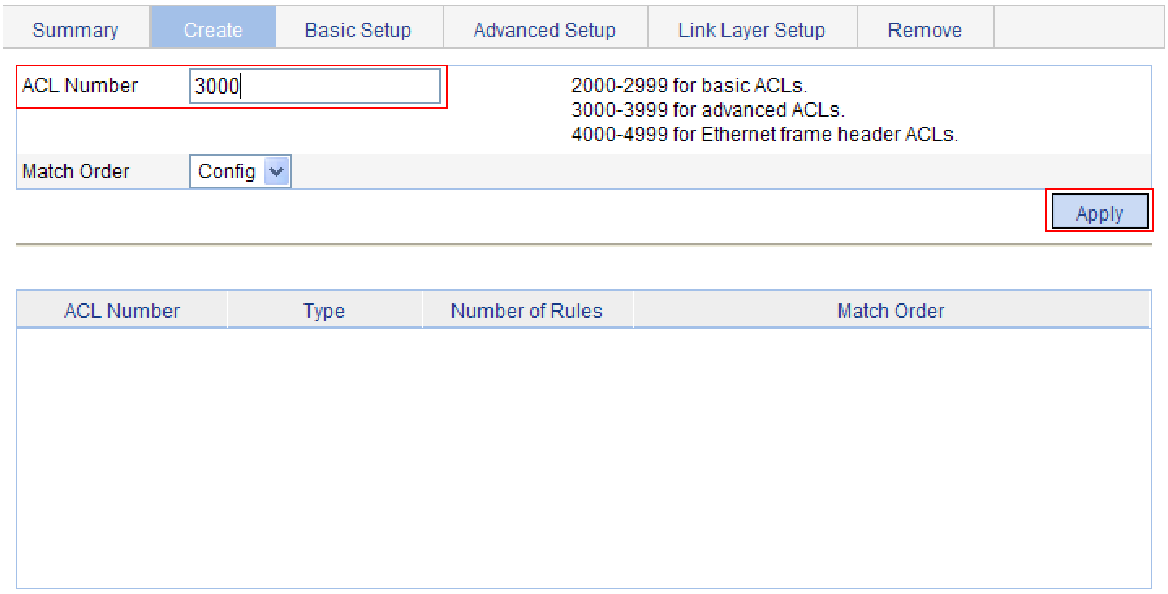
1. Define a time range to cover the time range from 8:00 to 18:00 every day:
   a. Select **QoS** > **Time Range** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter the time range name **test-time**.
   d. Select the **Periodic Time Range** box.
   e. Set the **Start Time** to 8:00 and the **End Time** to 18:00.
   f. Select the options **Sun** through **Sat**.
   g. Click **Apply**.

Figure 478 Defining a time range covering 8:00 to 18:00 every day



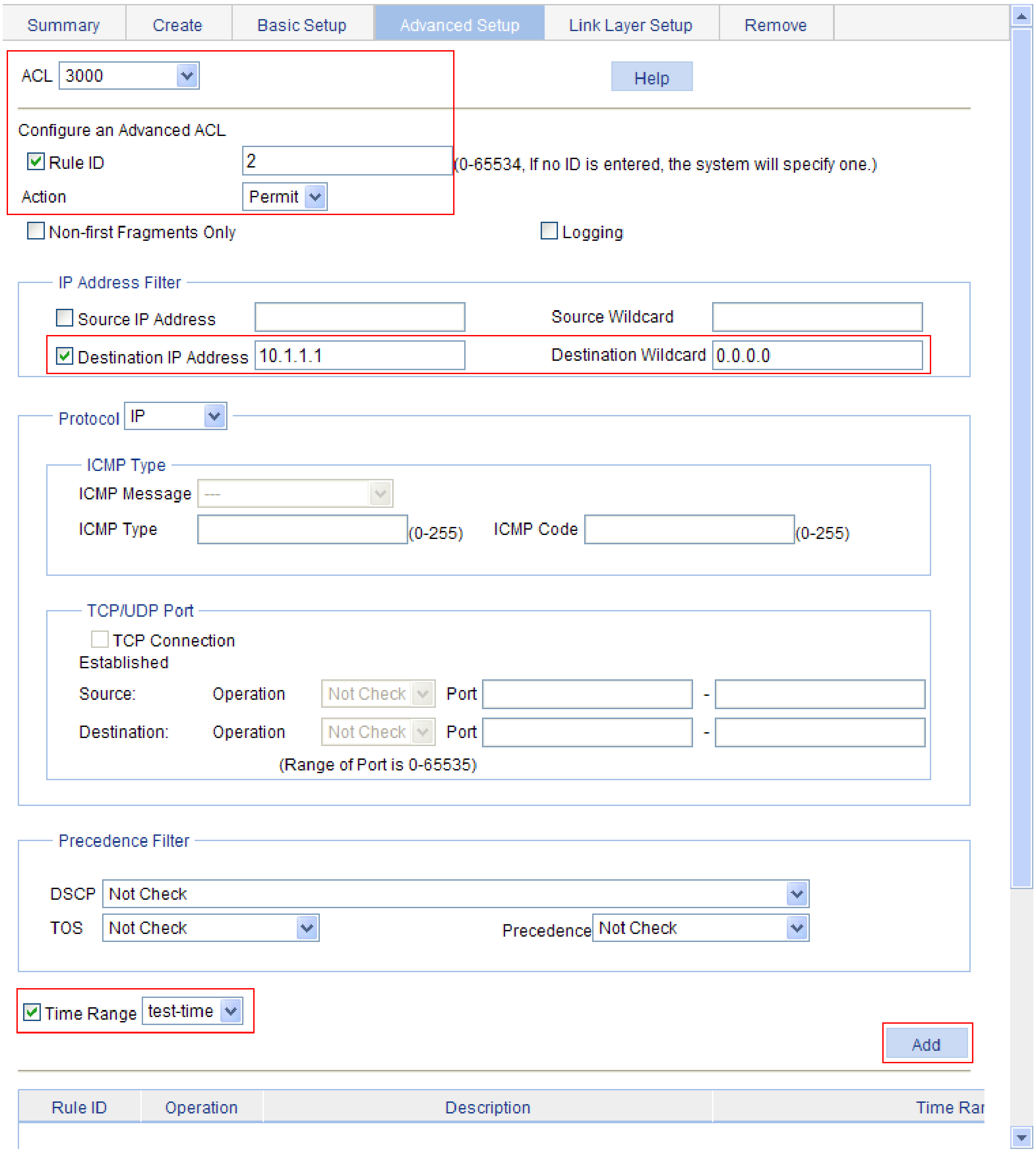
2. Add an advanced IPv4 ACL:
   a. Select **QoS** > **ACL IPv4** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter the ACL number 3000.
   d. Click **Apply**.

Figure 479 Adding an advanced IPv4 ACL



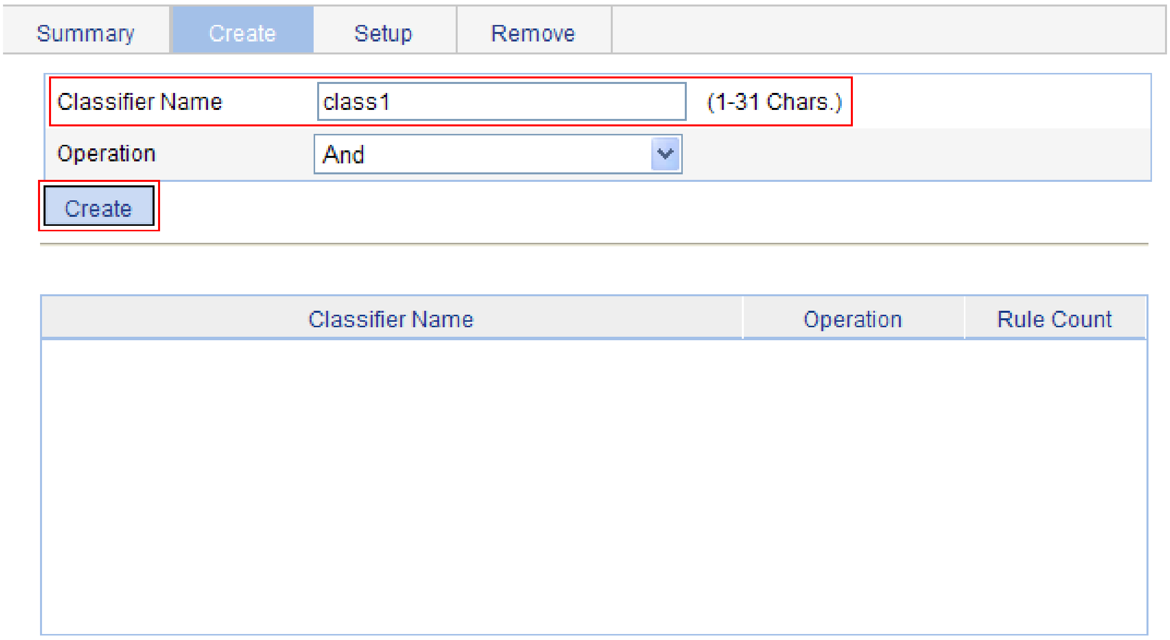
3. Define an ACL rule for traffic to the FTP server:
    a. Click the **Advanced Setup** tab.
    b. Select **3000** from the **ACL** list.
    c. Select the **Rule ID** box, and enter rule ID **2**.
    d. Select **Permit** from the **Action** list.
    e. Select the **Destination IP Address** box, and enter IP address **10.1.1.1** and destination wildcard **0.0.0.0**.
    f. Select **test-time** from the **Time Range** list.
    g. Click **Add**.

Figure 480 Defining an ACL rule for traffic to the FTP server



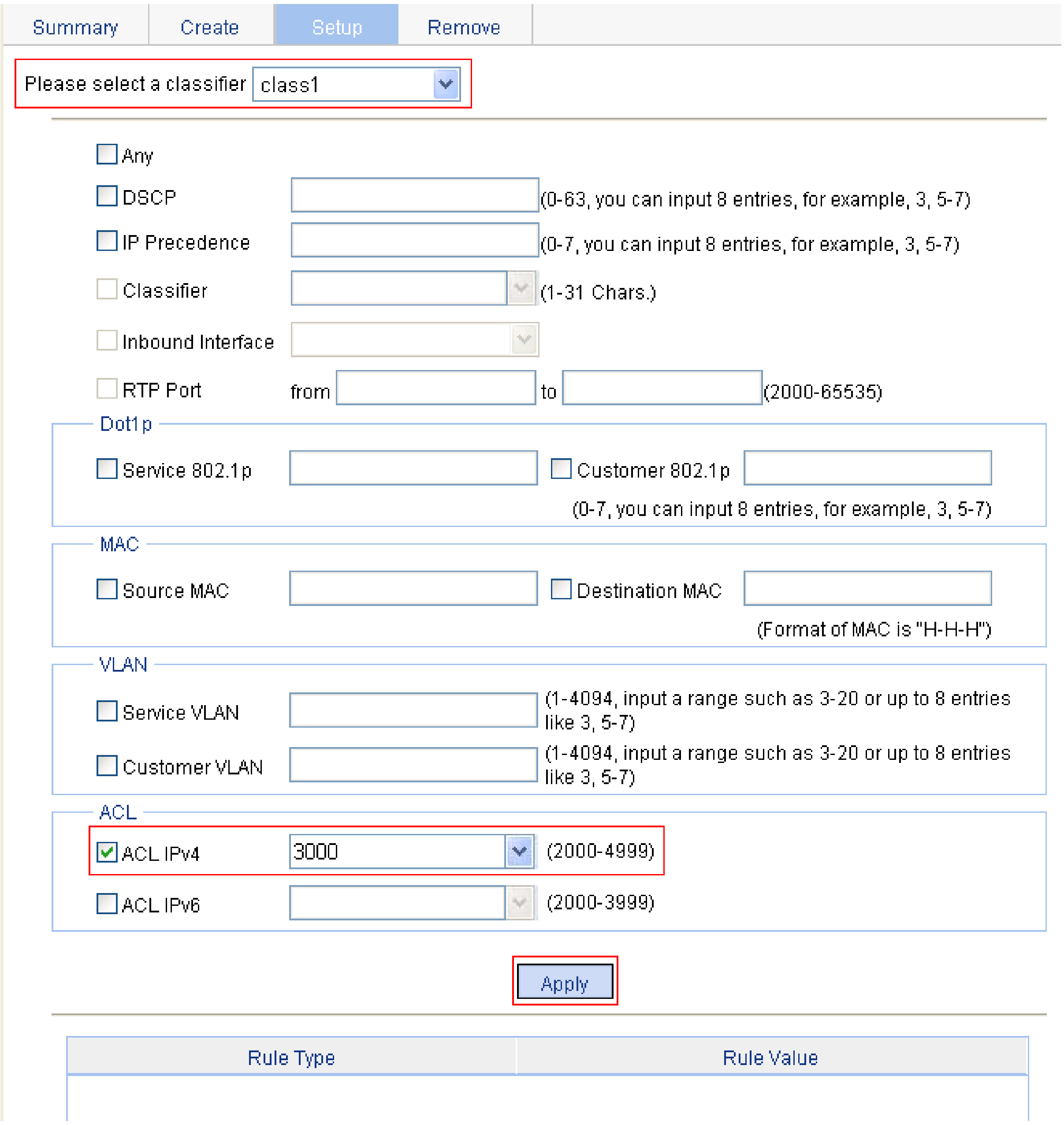
4. Add a class:
   a. Select **QoS** > **Classifier** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter the class name **class1**.
   d. Click **Add**.

Figure 481 Adding a class



5. Define classification rules:
   a. Click the **Setup** tab.
   b. Select the class name **class1** from the list.
   c. Select the **ACL IPv4** box, and select ACL **3000** from the following list.

Figure 482 Defining classification rules

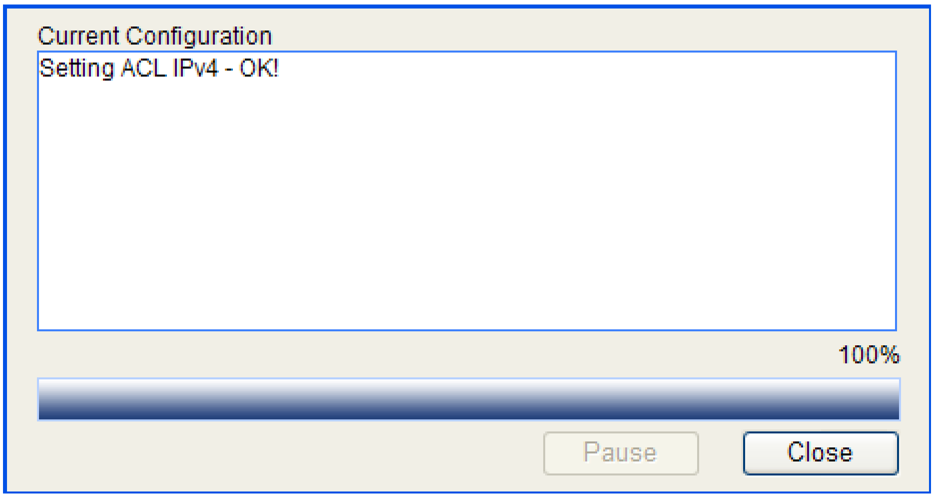


d. Click **Apply**.

   A progress dialog box appears, as shown in Figure 483.

e. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Figure 483 Configuration progress dialog box



6. Add a traffic behavior:
   a. Select **QoS** > **Behavior** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter the behavior name **behavior1**.
   d. Click **Create**.

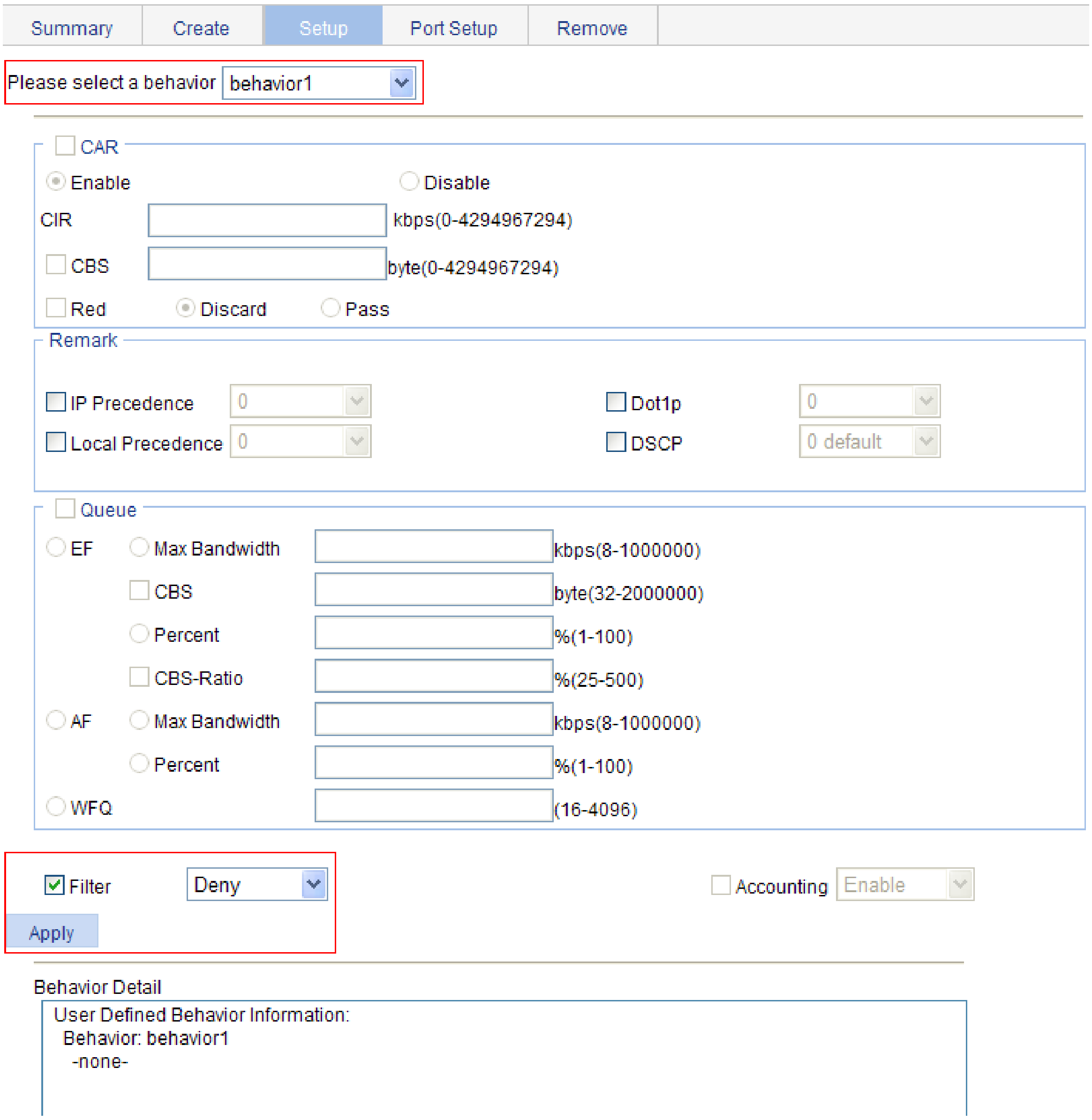
Figure 484 Adding a traffic behavior

7. Configure actions for the traffic behavior:
   a. Click the **Setup** tab.
   b. Select **behavior1** from the list.
   c. Select the **Filter** box, and then select **Deny** from the following list.
   d. Click **Apply**.

      A progress dialog box appears.

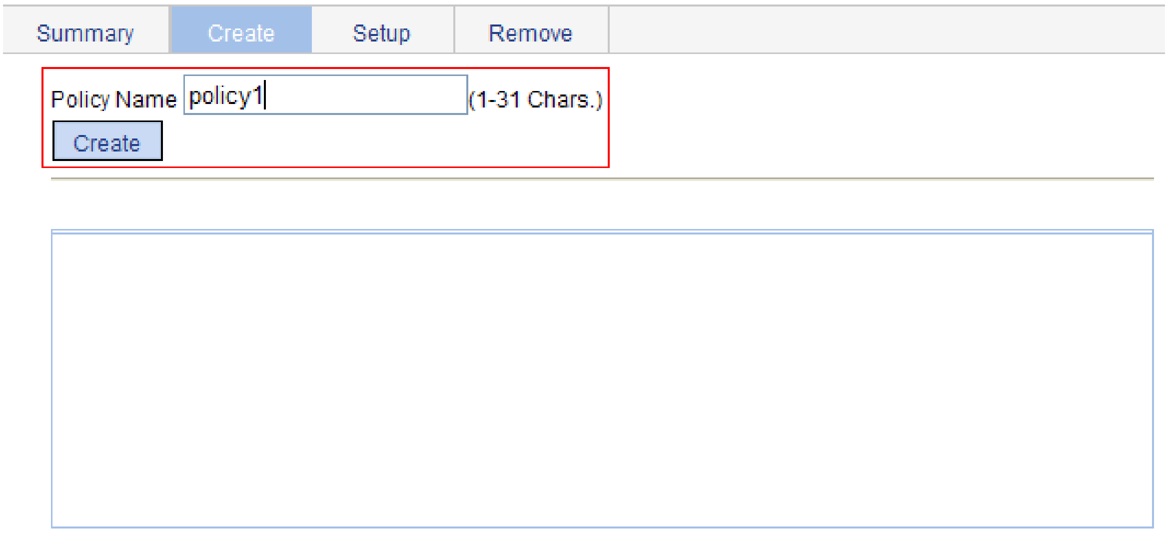
e. Click **Close** when the progress dialog box prompts that the configuration succeeds.

Figure 485 Configuring actions for the behavior



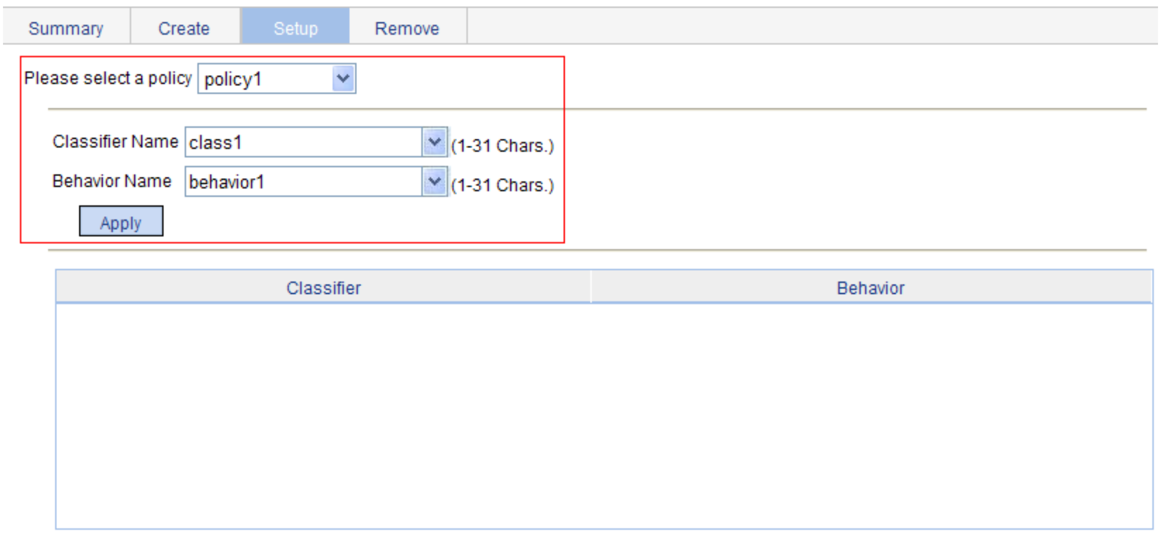
8. Add a policy:
   a. Select **QoS** > **QoS Policy** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the policy name **policy1**.
   d. Click **Add**.

Figure 486 Adding a policy



9. Configure classifier-behavior associations for the policy:
   a. Click the **Setup** tab.
   b. Select **policy1**.
   c. Select **class1** from the **Classifier Name** list.
   d. Select **behavior1** from the **Behavior Name** list.
   e. Click **Apply**.

Figure 487 Configuring classifier-behavior associations for the policy



10. Apply the QoS policy in the inbound direction of interface GigabitEthernet 1/0/1:
   a. Select **QoS** > **Port Policy** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **policy1** from the **Please select a policy** list.
   d. Select **Inbound** from the **Direction** list.

e. Select port GigabitEthernet 1/0/1.
f. Click **Apply**.

   A configuration progress dialog box appears.
g. Click **Close** when the progress dialog box prompts that the configuration succeeds.

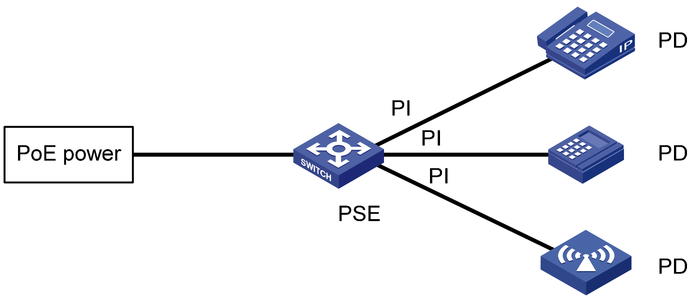
Figure 488 Applying the QoS policy in the inbound direction of GigabitEthernet 1/0/1

Configuring PoE

IEEE 802.3af-compliant power over Ethernet (PoE) enables a power sourcing equipment (PSE) to supply power to powered devices (PDs) through Ethernet interfaces over twisted pair cables. Examples of PDs include IP telephones, wireless APs, portable chargers, card readers, web cameras, and data collectors. A PD can also use a different power source from the PSE at the same time for power redundancy.

A 1910 switch has a build-in PSE to supply DC power to PDs over the data pairs (pins 1, 2 and 3, 6) of category 3/5 twisted pair cable, as shown in Figure 489. In this figure, PI represents PoE Ethernet interfaces.

Figure 489 PoE system



If a PD does not accept power over data pairs, the switch cannot supply power to it.

Restrictions and prerequisites

PoE is available only for PoE switches. For non-PoE switches, PoE related fields and tabs are not available or configurable.

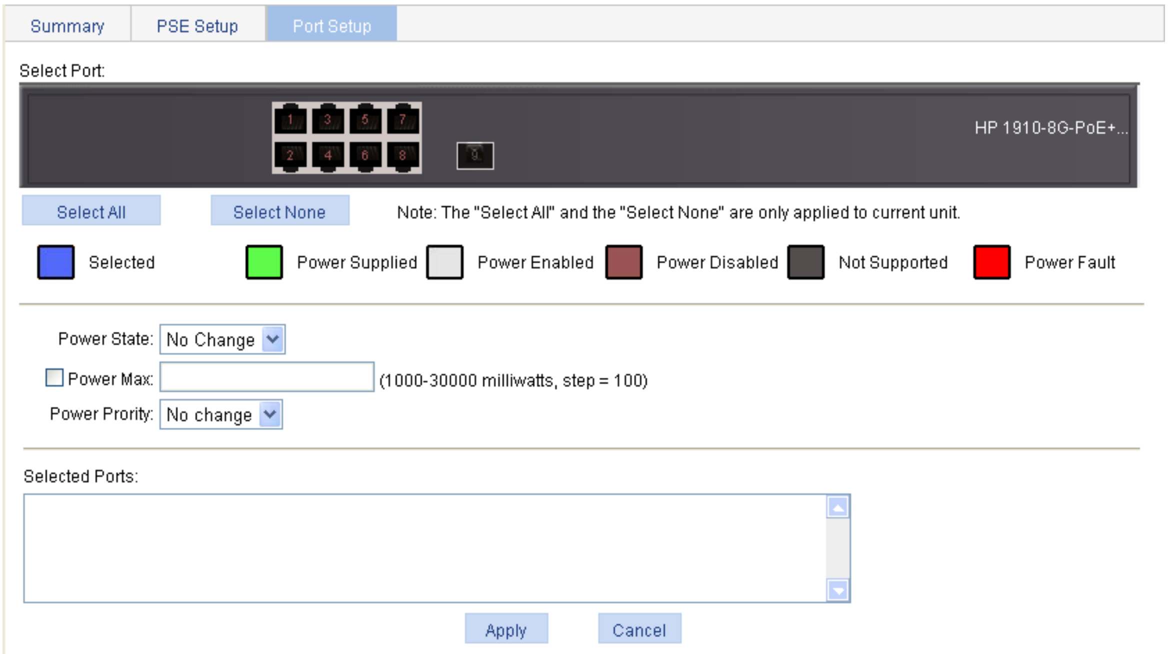
To configure PoE and make the PoE setting take effect, make sure the PoE power supply and the PSE are operating properly.

Make sure PDs accept power supplied over data pairs of category 3/5 twisted pair cable. If a PD does not support this power supplying mode, change the order of the lines in the cable.

Configuring PoE ports

1. Select **PoE** > **PoE** from the navigation tree.
2. Click the **Port Setup** tab.

Figure 490 Port Setup tab



3. Configure the PoE ports as described in Table 159.
4. Click **Apply**.

Table 159 Configuration items

Item	Description
Select Port	Select ports to be configured. They will be displayed in the **Selected Ports** area.
Power State	Enable or disable PoE on the selected ports. • 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. IMPORTANT: **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. 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, a PoE port can supply a maximum power of 30,000 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**. IMPORTANT: • 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.

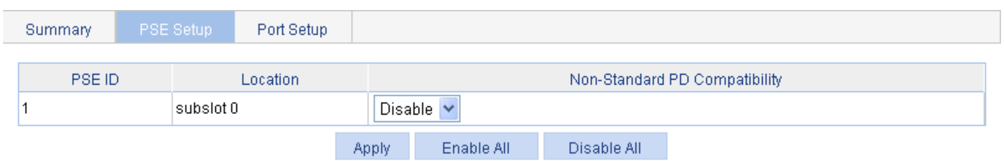
Configuring non-standard PD detection

There are standard PDs and nonstandard PDs. Standard PDs are those conforming to the IEEE 802.3af standard. Usually, the PSE can detect only standard PDs and supply power to them. The PSE can detect nonstandard PDs and supply power to them only after the PSE is enabled to detect nonstandard PDs.

1. Select **PoE** > **PoE** from the navigation tree.
2. Click the **PSE Setup** tab.

   The page displays the location of the PSE, and the status of the non-standard PD detection function.

Figure 491 PSE Setup tab



Enabling the non-standard PD detection function

Perform one of the following tasks on the **PSE Setup** tab to enable the non-standard PD detection function:

- Select **Enable** in the **Non-Standard PD Compatibility** column, and click **Apply**.
- Click **Enable All**.

Disabling the non-standard PD detection function for a PSE

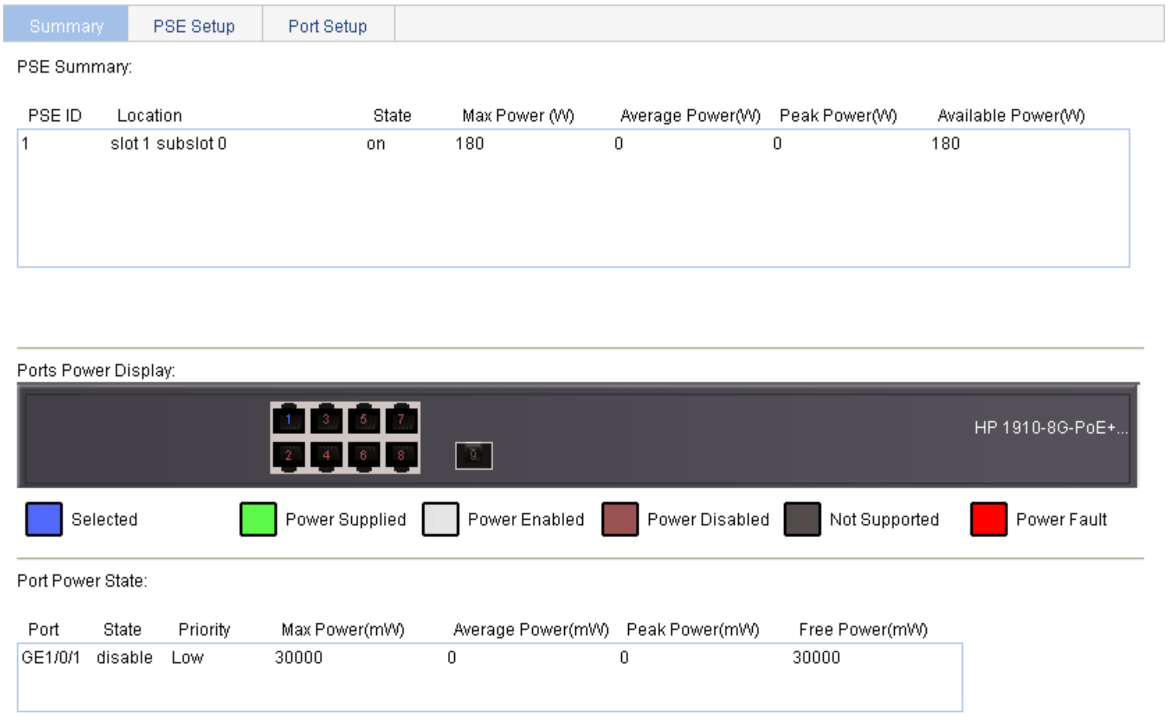
Perform one of the following tasks on the **PSE Setup** tab to disable the non-standard PD detection function:

- Select **Disable** in the **Non-Standard PD Compatibility** column, and click **Apply**.
- Click **Disable All**.

Displaying information about PSE and PoE ports

1. Select **PoE** > **PoE** from the navigation tree to enter the **Summary** tab.
   The upper part of the page displays the PSE summary.
2. To view the configuration and power information, click a port on the chassis front panel.

Figure 492 Summary tab (with GigabitEthernet 1/0/1 selected)



PoE configuration example

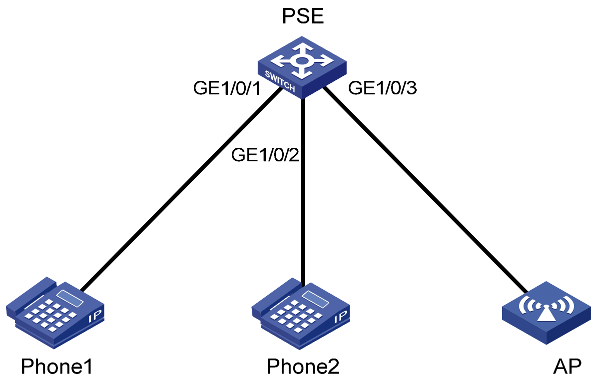
Network requirements

As shown in Figure 493, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are connected to IP telephones.

GigabitEthernet 1/0/3 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.

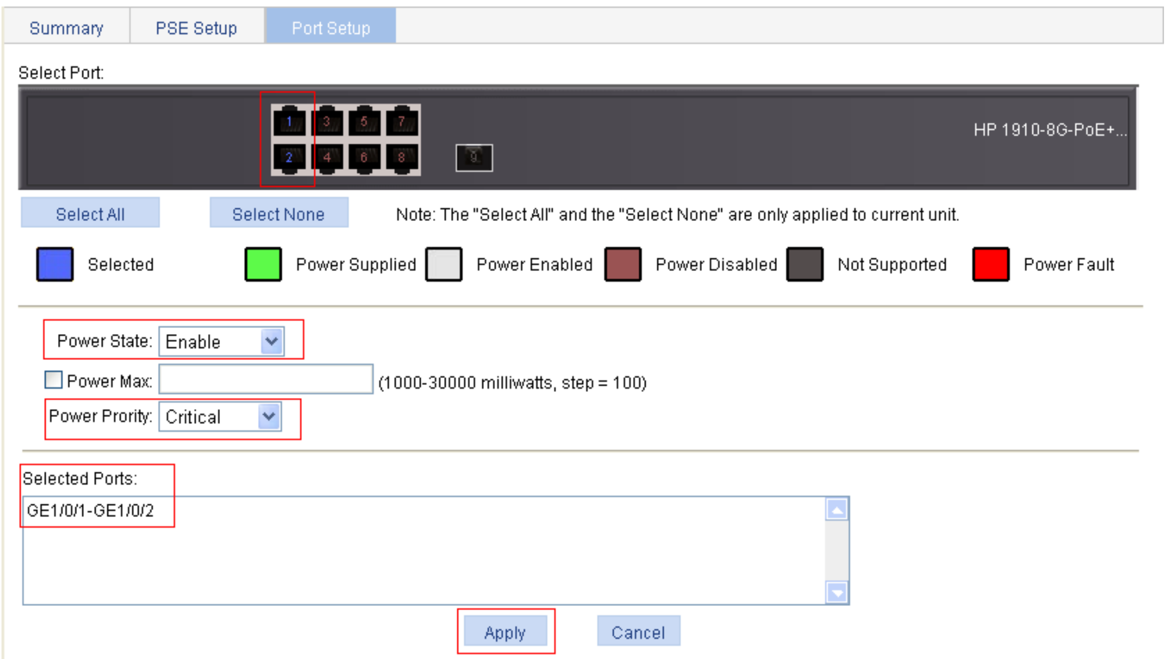
Figure 493 Network diagram



Configuration procedure

1. Enable PoE on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, and set their power supply priority to **critical**:
   a. Select **PoE** > **PoE** from the navigation tree.
   b. Click the **Setup** tab.
   c. On the tab, click to select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel, select **Enable** from the **Power State** list, and select **Critical** from the **Power Priority** list.
   d. Click **Apply**.

Figure 494 Configuring the PoE ports supplying power to the IP telephones

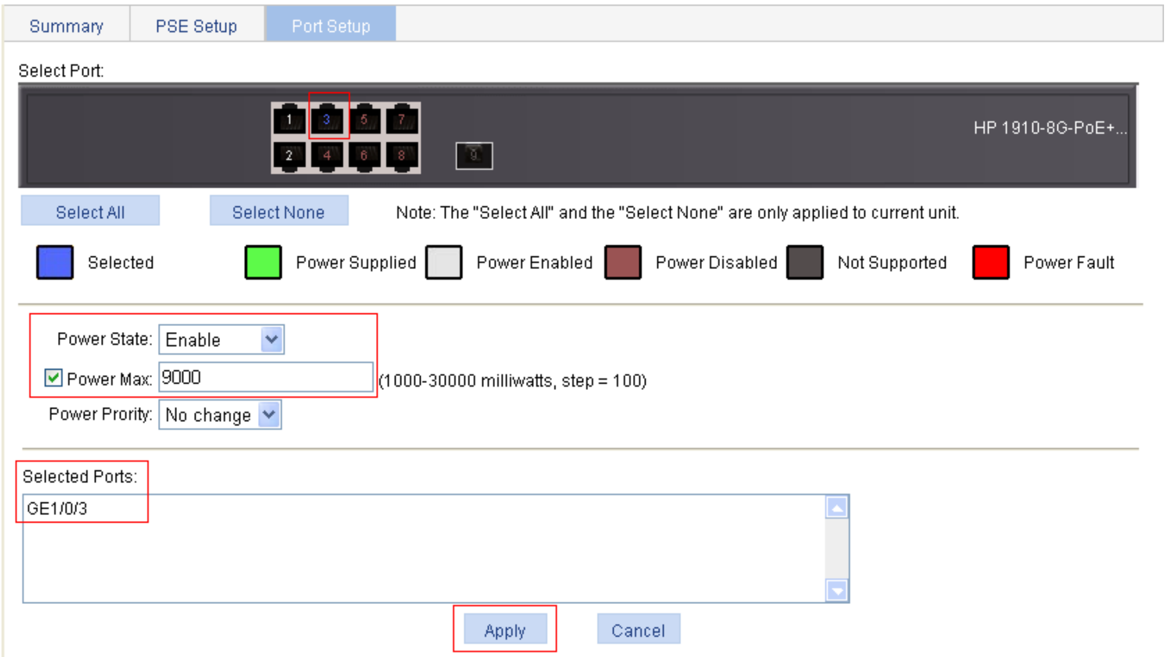


2. Enable PoE on GigabitEthernet 1/0/3 and set the maximum power of the port to 9000 milliwatts:
   a. Click the **Setup** tab.

b. On the tab, click to select port GigabitEthernet 1/0/3 from the chassis front panel, select **Enable** from the **Power State** list, and select the box before **Power Max** and enter **9000**.

c. Click **Apply**.

Figure 495 Configuring the PoE port supplying power to AP



After the configuration takes effect, the IP telephones and the AP are powered and can work properly.

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP A-Series Acronyms.*

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

<table>
<tr><th>Convention</th><th>Description</th></tr>
<tr><td>Boldface</td><td>Bold text represents commands and keywords that you enter literally as shown.</td></tr>
<tr><td>Italic</td><td>Italic text represents arguments that you replace with actual values.</td></tr>
<tr><td>[ ]</td><td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td></tr>
<tr><td>{ x | y | ... }</td><td>Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.</td></tr>
<tr><td>[x | y | ...]</td><td>Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.</td></tr>
<tr><td>{ x | y | ... } *</td><td>Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.</td></tr>
<tr><td>[x | y | ...] *</td><td>Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.</td></tr>
<tr><td>&<1-n></td><td>The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.</td></tr>
<tr><td>#</td><td>A line that starts with a pound (#) sign is comments.</td></tr>
</table>

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index