Hewlett Packard Enterprise

HPE OfficeConnect 1920 Switch Series

User Guide

Part number: 5998-5627s
Software version: Release 1117
Document version: 6W103-20170810

Acknowledgments

Contents

Overview

The HPE OfficeConnect 1920 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 1920 Switch Series configurations.
- The CLI provides configuration commands to facilitate your operation. To perform other configurations not supported by the CLI, use the Web interface.

Configuring the switch in the Web interface

Restrictions and guidelines

To ensure a successful login, verify that your operating system and Web browser meet the requirements, and follow the guidelines in this section.

Operating system requirements

- The device supports the following operating systems:
- Windows XP.
- Windows 2000.
- Windows Server 2003 Enterprise Edition.
- Windows Server 2003 Standard Edition.
- Windows Vista.
- Windows 7.
- Linux.
- MAC OS.
- If you are using a Windows operating system, turn off the Windows firewall. The Windows firewall limits the number of TCP connections. When the limit is reached, you cannot log in to the Web interface.

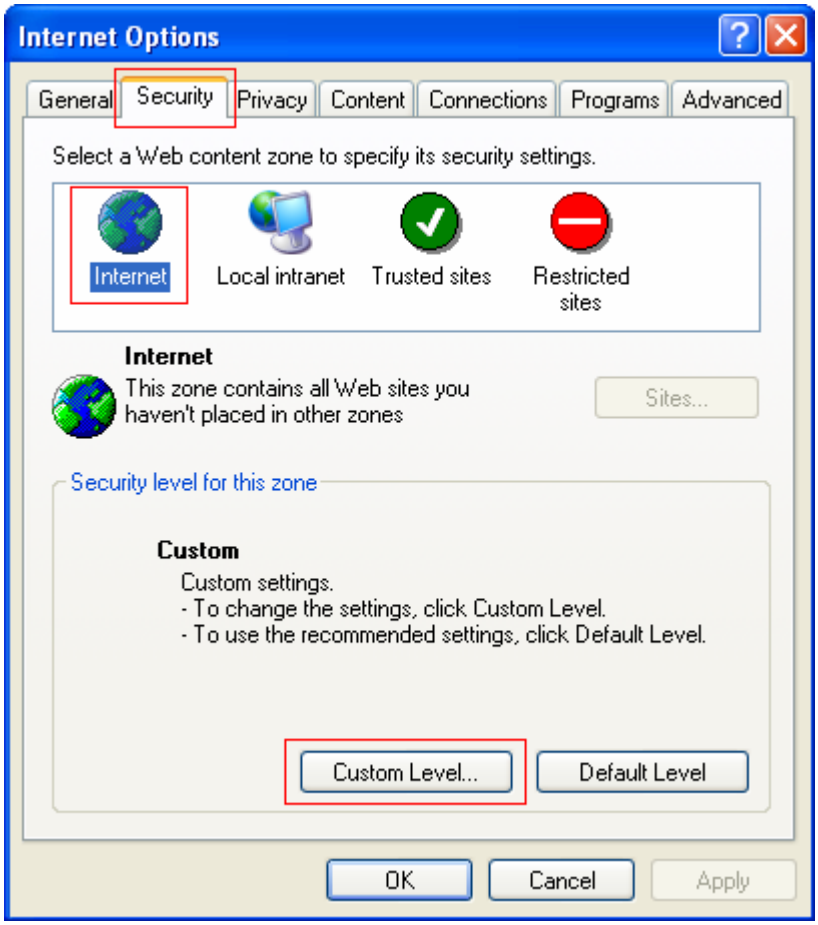
Web browser requirements

- Hewlett Packard Enterprise recommends that you use the following Web browsers:
- Internet Explorer 6 SP2 or higher.
- Mozilla Firefox 3 or higher.
- Google Chrome 2.0.174.0 or higher.
- If you are using a Microsoft Internet Explorer browser, you must enable the security settings (see "Enabling securing settings in a Microsoft Internet Explorer browser"), including **Run ActiveX controls and plug-ins**, **Script ActiveX controls marked safe for scripting**, and **Active scripting**.
- If you are using a Mozilla Firefox browser, you must enable JavaScript (see "Enabling JavaScript in a Firefox browserEnabling JavaScript in a Firefox browser").

Enabling securing settings in a Microsoft Internet Explorer browser

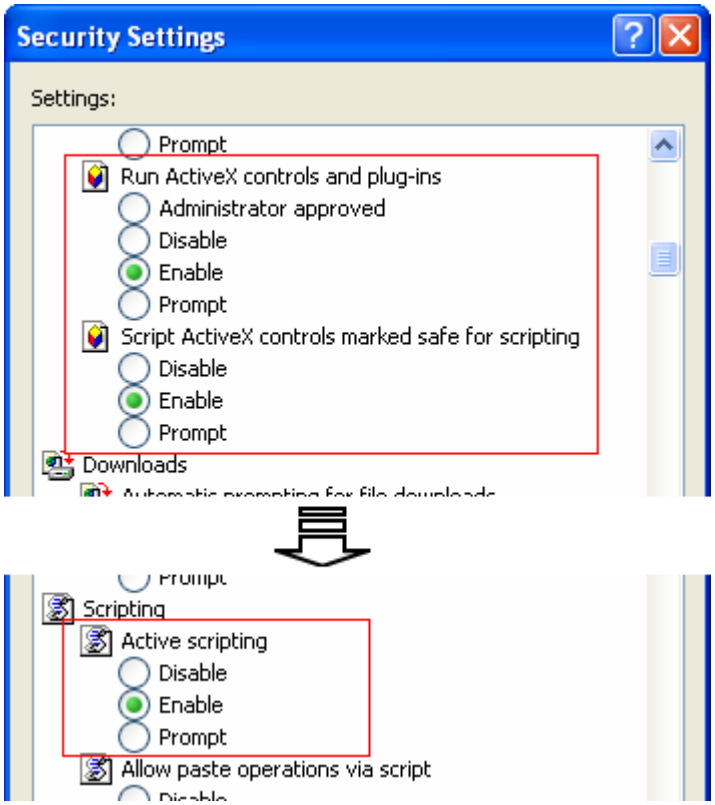
1. Launch the Internet Explorer, and select **Tools** > **Internet Options** from the main menu.
2. Select the **Security** tab, and select the content zone where the target Website resides, as shown in Figure 1.

Figure 1 Internet Explorer settings (1)



3. Click **Custom Level**.
4. In the **Security Settings** dialog box, enable **Run ActiveX controls and plug-ins**, **Script ActiveX controls marked safe for scripting**, and **Active scripting**.

Figure 2 Internet Explorer settings (2)

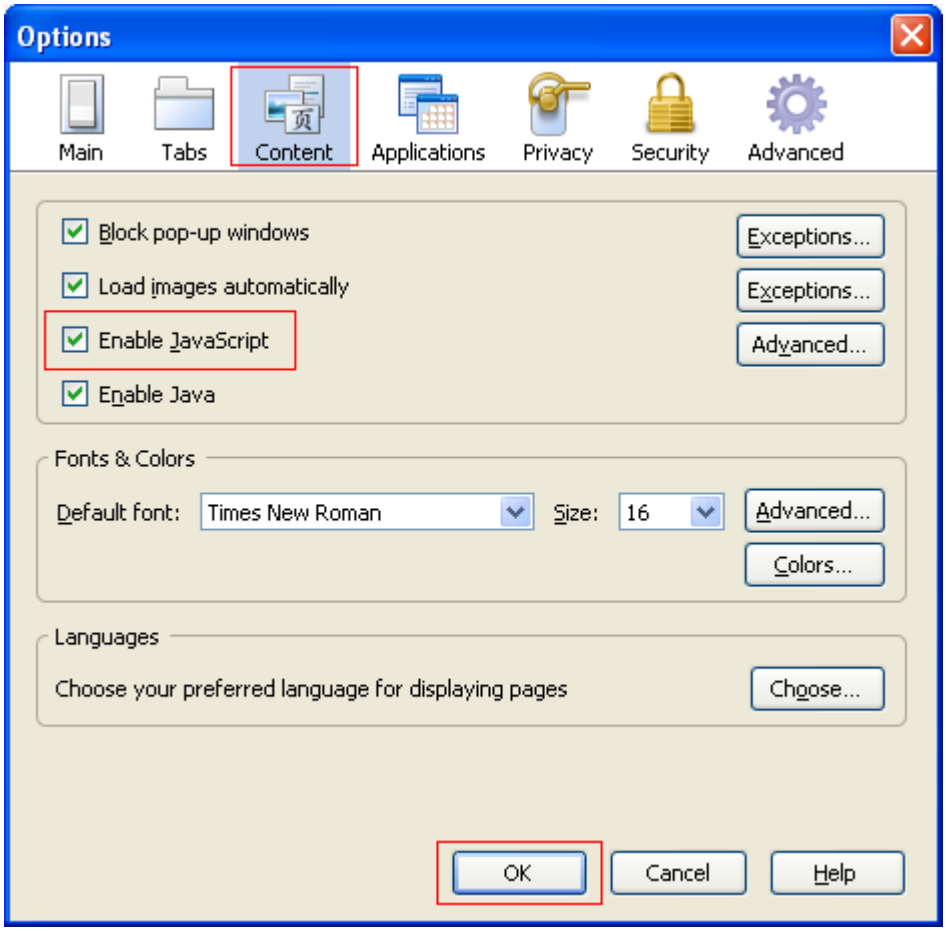


5. Click **OK** to save your settings.

Enabling JavaScript in a Firefox browser

1. Launch the Firefox browser, and select **Tools** > **Options**.
2. In the **Options** dialog box, click the **Content** icon, and select **Enable JavaScript**.

Figure 3 Firefox browser settings



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

Others

- The Web interface does not support the **Back**, **Next**, and **Refresh** buttons provided by the browser. Using these buttons might result in abnormal display of Web pages.
- To ensure correct display of Web page contents after software upgrade or downgrade, clear data cached by the browser before you log in.
- 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.
- A list can contain a maximum of 20000 entries if displayed in pages.
- 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.

Overview

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

Figure 4 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**—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 IP address of the device on the label on the device. IP address is 169.254.xxx.xxx. If the MAC address is 08004E000102, the IP address would be 169.254.1.2.
- If a DHCP server exists in the subnet where the device resides, the device will dynamically obtain its 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 IP address.

```
<Sysname> summary
Select menu option:             Summary
IP Method:                      DHCP
IP address:                     169.254.1.2
Subnet mask:                    255.255.0.0
Default gateway:                0.0.0.0
<Omitted>
```

Assuming that the IP address of the device is 169.254.1.2, to log in to the Web interface of the device from a PC:

1. Connect the Ethernet 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, 169.254.1.27) within 169.254.0.0/16 (except for the IP address of the device).
3. Open the browser, and input the login information.
   a. Type the IP address http:// 169.254.1.2 in the address bar and press **Enter**.

      The login page of the web interface (see Figure 5) appears.
   b. Enter the username **admin** and the verification code, leave the password blank, and click **Login**.

Figure 5 Login page of the Web interface

Logging out of the Web interface

CAUTION:

- You cannot log out by directly closing the browser.
- For security purposes, log out of the Web interface after you finish your operations.

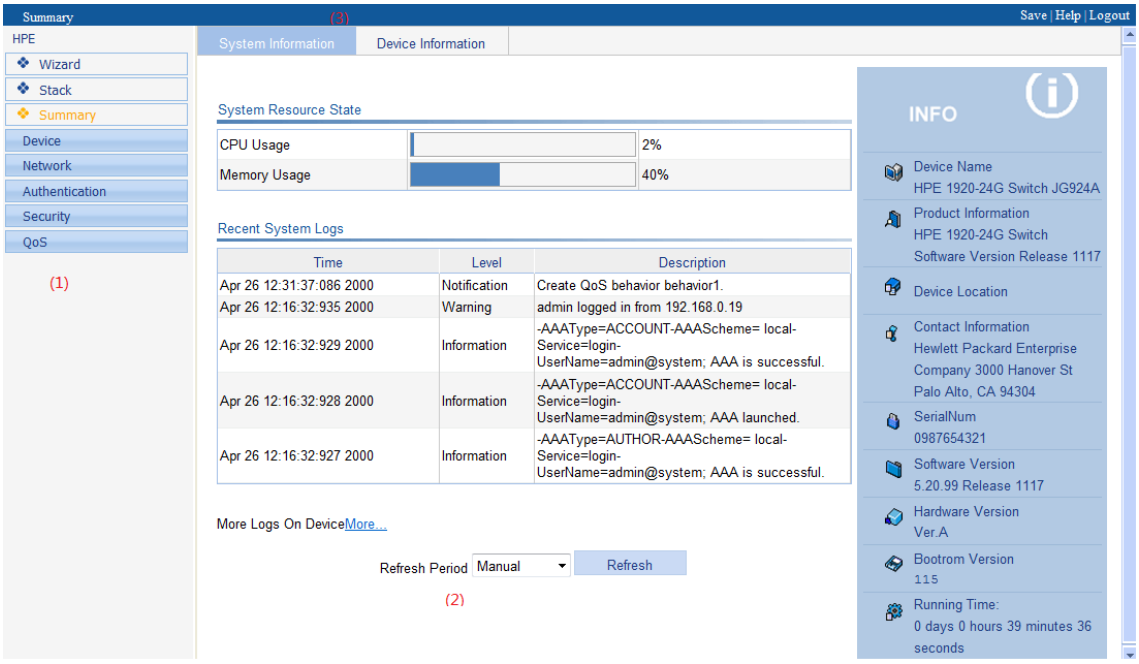
1. Save the current configuration.

   Because the system does not save the current configuration automatically, Hewlett Packard Enterprise recommends that you perform this step to avoid loss of configuration.
2. Click **Logout** in the upper-right corner of the Web interface.

Web interface

The Web interface includes three parts: navigation tree, title area, and body area, as shown in Figure 6.

Figure 6 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.

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
	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
		Add	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
	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
	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
Network	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
		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
	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
			Configure gratuitous ARP.	Configure

	ARP Anti-Attack	ARP Detection	Display ARP detection configuration information.	Monitor
			Configure ARP detection.	Configure
	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
	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
		DHCPv6 Relay	Display configuration information about the DHCPv6 relay agent	Monitor
			Configure a DHCPv6 relay agent	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
Authentication	MAC Authentication	MAC Authentication	Display MAC authentication configuration information.	Monitor
			Configure MAC authentication.	Configure
	802.1X	802.1X	Display 802.1X configuration information globally or on a port.	Monitor
			Configure 802.1X globally or on a port.	Configure
	Port Security	Port Security	Display port security configuration information.	Monitor
			Configure port security.	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
	Certificate Management	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

			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
Security	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
	Loopback Detection	Loopback Detection	Display and configure system loopback detection parameters and port loopback detection parameters.	Configure
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

		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

Common items on the Web pages

Buttons and icons

Table 2 Commonly used buttons and icons

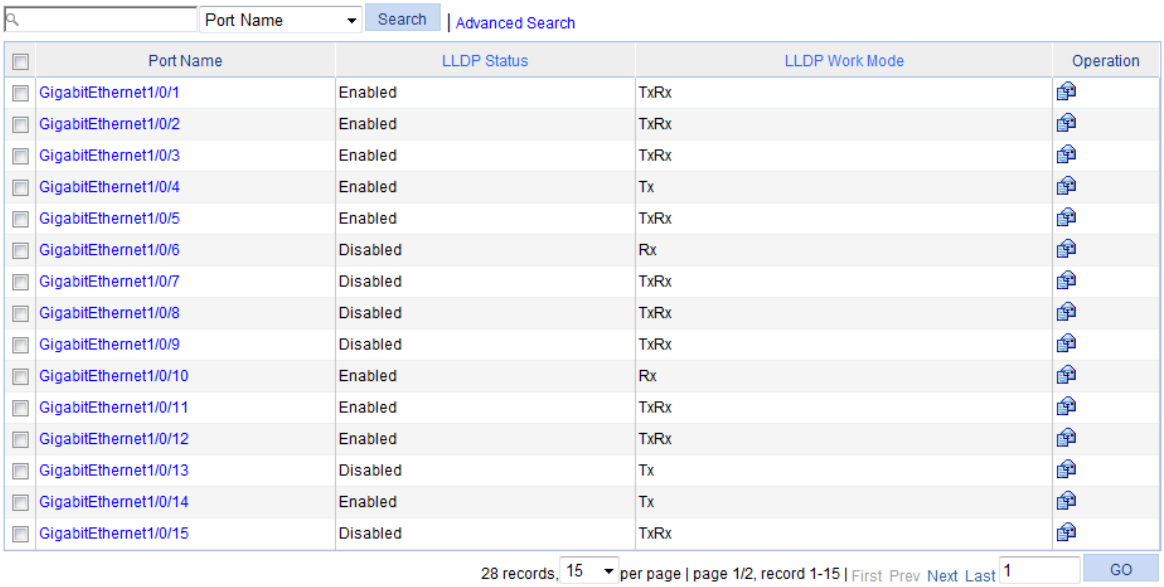
Button and icon	Function
Apply	Applies the configuration on the current page.
Cancel	Cancels the configuration on the current page.
Refresh	Refreshes the current page.
Clear	Clears all entries in a list or all statistics.
Add	Adds an item.
Remove, Del Selected	Removes the selected items.
Select All	Selects all the entries in a list.
Select None	Clears selection of all entries in a list.
Next>	Buffers but does not apply the configuration of the current step, and enters the next configuration step.

Button and icon	Function
<Back	Buffers but does not apply the configuration of the current step, and returns to the previous configuration step.
Finish	Applies the configurations of all configuration steps.
	Enters the modification page of an item so that you can modify the configurations of the item.
	Deletes the item corresponding to this icon.

Page display function

The Web interface can display contents by pages, as shown in Figure 7. You can set the number of entries displayed per page, and view the contents on the first, previous, next, and last pages, or go to any page that you want to check.

Figure 7 Content display by pages

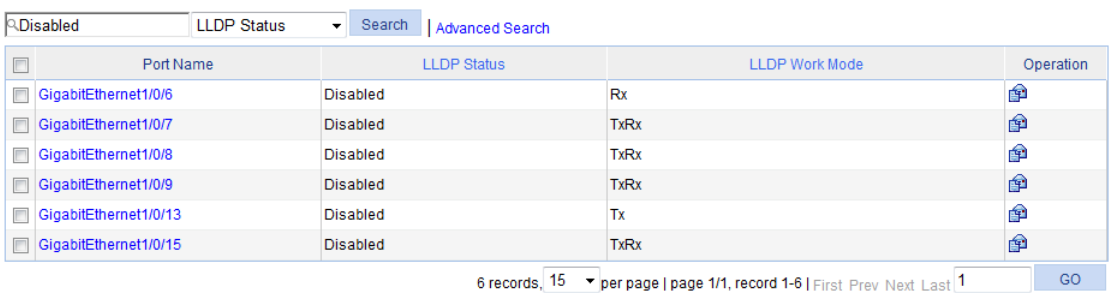


Search function

The Web interface provides you with the basic and advanced searching functions to display only the entries that match specific searching criteria.

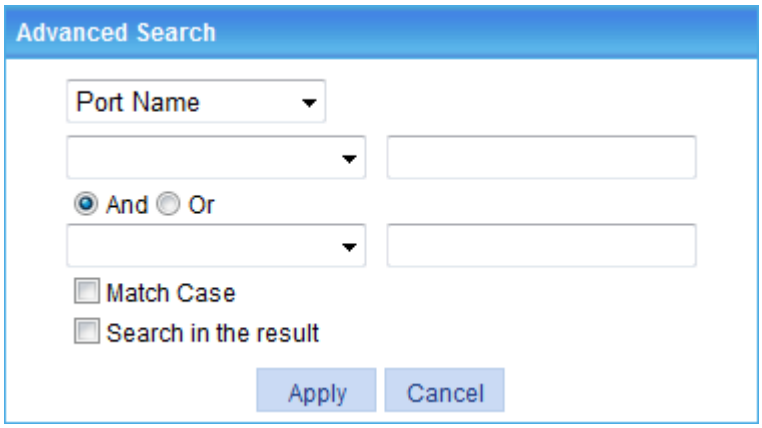
- **Basic search**—As shown in Figure 7, type the keyword in the text box above the list, select a search item from the list and click **Search** to display the entries that match the criteria. Figure 8 shows an example of searching for entries with LLDP disabled.

  Figure 8 Basic search function example



- **Advanced search**—As shown in Figure 9, you can click the **Advanced Search** link to open the advanced search area. Specify the search criteria, and click **Apply** to display the entries that match the criteria.

  Figure 9 Advanced search

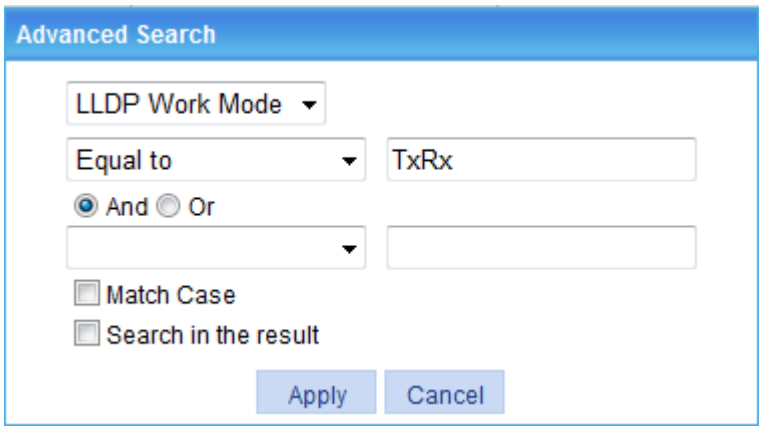
  

Take the LLDP table shown in Figure 7 as an example.

To search for the LLDP entries with LLDP Work Mode **TxRx**, and LLDP Status **Disabled**:

1. Click the **Advanced Search** link, specify the search criteria on the advanced search page as shown in Figure 10, and click **Apply**. The LLDP entries with LLDP Work Mode being TxRx are displayed.

   Figure 10 Advanced search function example (1)

2. Click the **Advanced Search** link, specify the search criteria on the advanced search page as shown in Figure 11, and click **Apply**. The LLDP entries with LLDP Work Mode being TxRx and LLDP Status being Disabled are displayed as shown in Figure 12.

Figure 11 Advanced search function example (2)

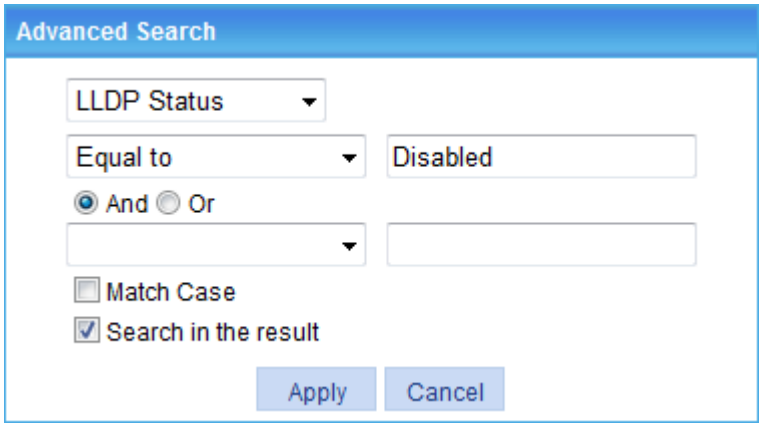
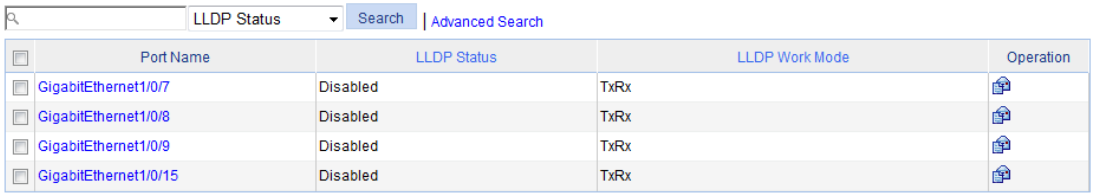


Figure 12 Advanced search function example (3)



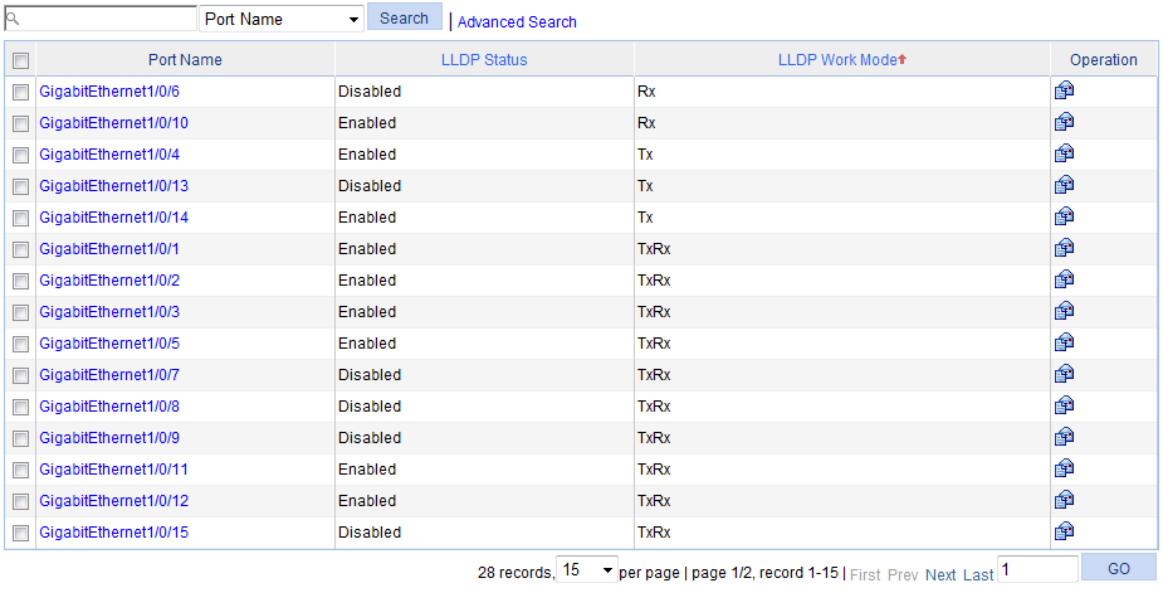
Sort function

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

The Web interface provides you with the sorting functions to display entries in certain orders.

On a list page, you can click the blue heading item of each column to sort the entries based on the heading item you selected. After your clicking, the heading item is displayed with an arrow beside it as shown in Figure 13. The upward arrow indicates the ascending order, and the downward arrow indicates the descending order.

Figure 13 Sort display



Configuring the switch at the CLI

The HPE OfficeConnect 1920 Switch Series can be configured through the CLI, Web interface, and SNMP/MIB, among which the Web interface supports all 1920 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.

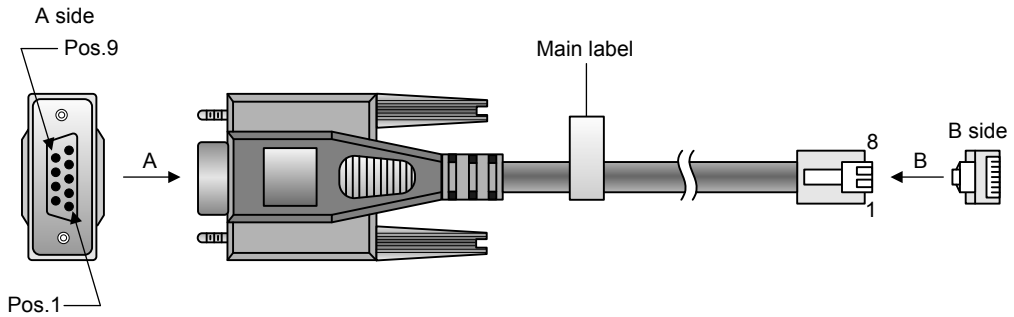
This section describes using the CLI to manage the device.

Setting up the configuration environment

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 14 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.

CAUTION:

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

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:

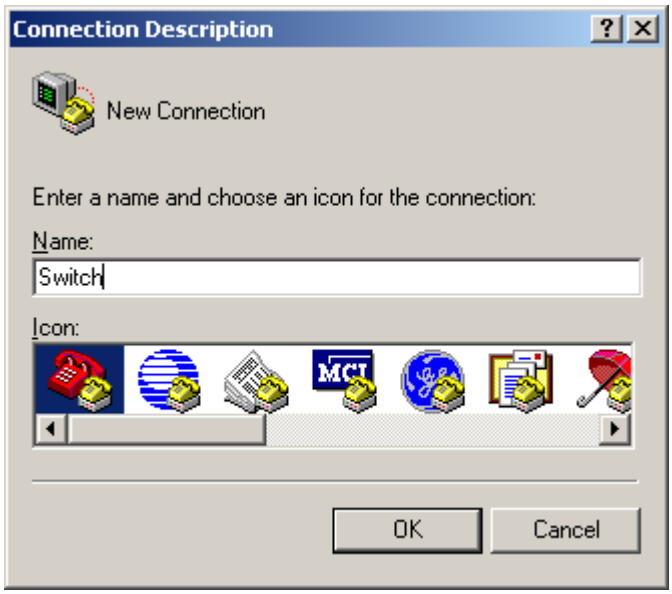
- **Bits per second**—38400.
- **Data bits**—8.
- **Parity**—None.
- **Stop bits**—1.
- **Flow control**—None.
- **Emulation**—VT100.

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 15 Connection description

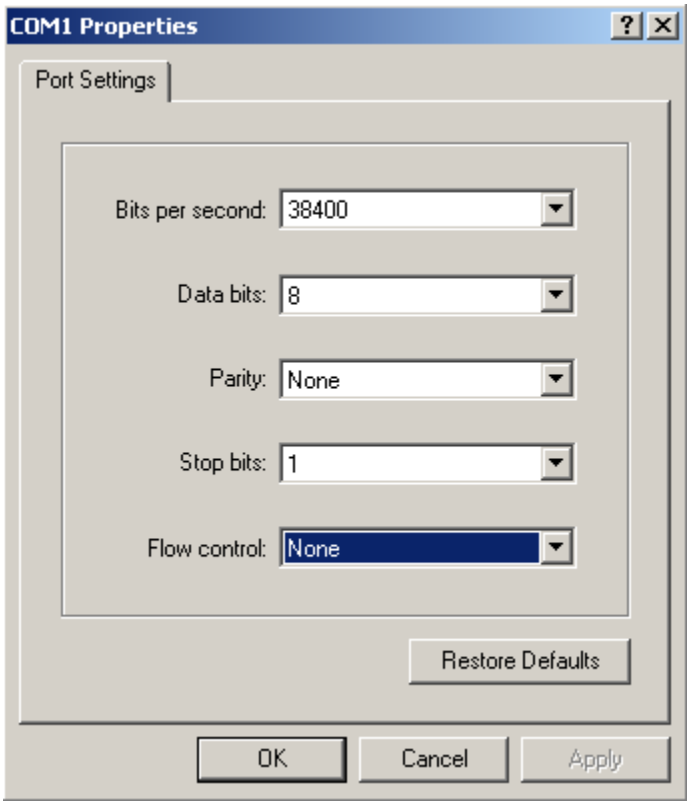


3. Select the serial port to be used from the **Connect using** list, and click **OK**.

Figure 16 Setting the serial port used by the HyperTerminal connection

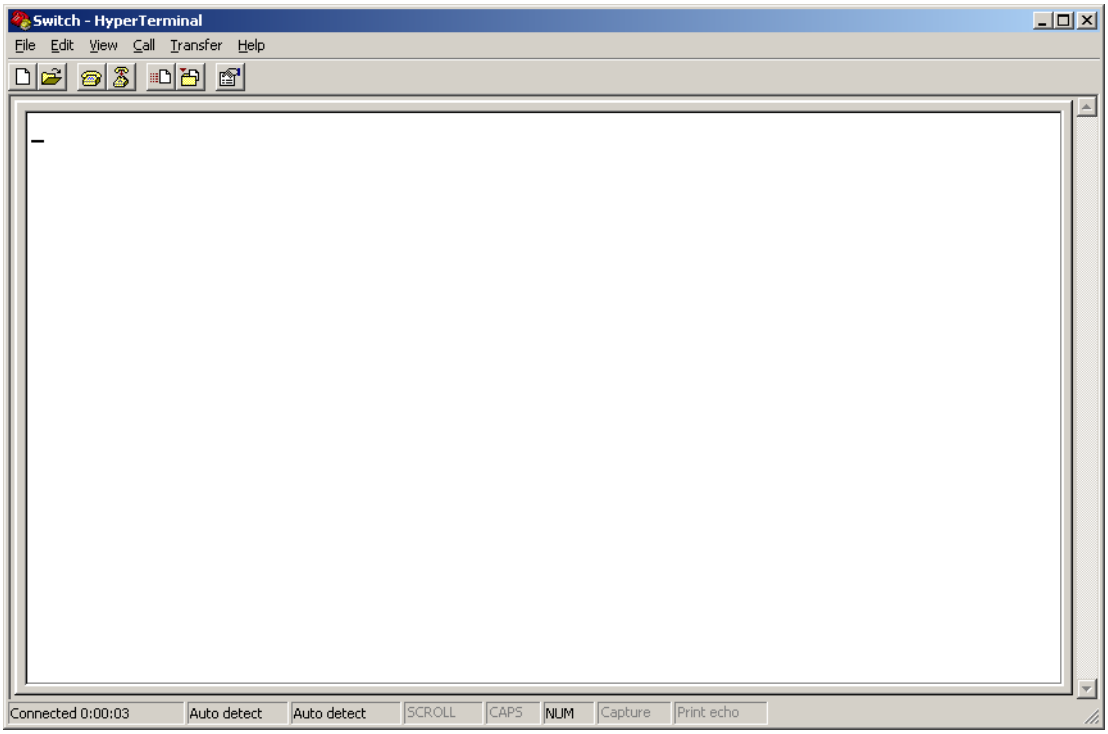
4. Set **Bits per second** to **38400**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 17 Setting the serial port parameters



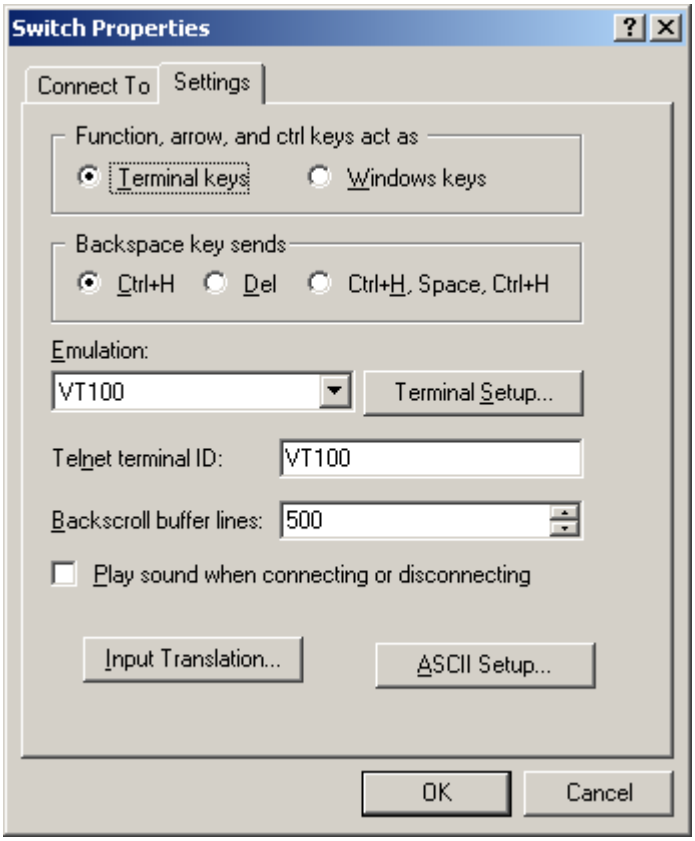
5. Select **File** > **Properties** in the HyperTerminal window.

Figure 18 HyperTerminal window



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

Figure 19 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:

   ```
   <HPE>
   ```

   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: Specifies the interface 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 IPv4 address through DHCP; if fails, it uses the assigned IP address.

If there is no VLAN-interface 1, either command creates VLAN-interface 1 first, and then specifies its IPv4 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 millisecond, 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) 2010-2017 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

User interface aux0 is available.
```

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
Vlan-interface:                 1

Select menu option:             Summary
IP Method:                      Manual
IP address:                     192.168.0.233
Subnet mask:                    255.255.255.0
Default gateway:

IPv6 Method:
IPv6 link-local address:
```

```
IPv6 subnet mask length:
IPv6 global address:
IPv6 subnet mask length:
IPv6 default gateway:

Mac address: 0002-0133-D143

Current boot app is: flash:/jg924a-cmw520-r1117.bin
Next main boot app is: flash:/jg924a-cmw520-r1117.bin
Next backup boot app is: NULL

HPE Comware Platform Software
Comware Software, Version 5.20.99, Release 1117
Copyright (c) 2010-2017 Hewlett Packard Enterprise Development LP
HPE 1920-24G Switch uptime is 0 week, 0 day, 1 hour, 20 minutes

HPE 1920-24G Switch
128M    bytes DRAM
32M     bytes Flash Memory
Config Register points to Flash

Hardware Version is Ver.A
Bootrom Version is 115
[SubSlot 0] 24GE+4SFP Hardware Version is Ver.A
```

telnet

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host, a case-insensitive string of 1 to 20 characters.

service-port: Specifies the TCP port number for the Telnet service on the remote host. It ranges from 0 to 65535 and defaults to 23.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies the source IPv4 address for outgoing Telnet packets.

Description

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

The source IPv4 address or source interface specified by this command is only applicable to the current Telnet connection.

Examples

Telnet to host 1.1.1.2, using 1.1.1.1 as the source IP address for outgoing Telnet packets.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

telnet ipv6

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*]

Parameters

remote-host: Specifies the IP address or host name of a remote host, a case-insensitive string of 1 to 46 characters.

-i *interface-type interface-number*: Specifies the outbound interface for sending Telnet packets. This option is required when the destination address is a link-local address.

port-number: Specifies the TCP port number for the Telnet service on the remote host. It ranges from 0 to 65535 and defaults to 23.

Description

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

Examples

Telnet to the host at 5000::1.

```
<Sysname> telnet ipv6 5000::1
```

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 HPE OfficeConnect 1920 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 HPE OfficeConnect 1920 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
```

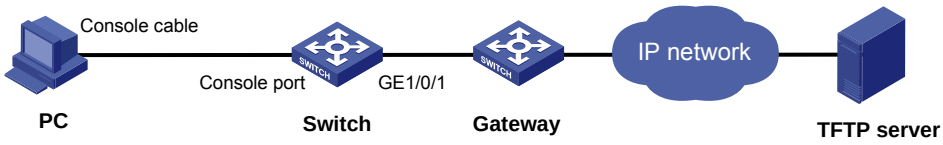
Configuration example for upgrading the system software image at the CLI

Network requirements

As shown in Figure 20, a 1920 switch is connected to the PC through the console cable, and connected to the gateway through Ethernet 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 **Switch1920.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 1920 switch through the PC and sets the IP address of the switch to 192.168.1.2/24.

Figure 20 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 **Switch1920.bin** on the TFTP server to the switch, and upgrade the system software image in the package.

   ```
   <Switch> upgrade 192.168.10.1 Switch1920.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 **Switch1920.bin** on the TFTP server to the switch, and upgrade the Boot ROM image.

   ```
   <Switch> upgrade 192.168.10.1 Switch1920.bin bootrom
   The file flash:/Switch1920.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

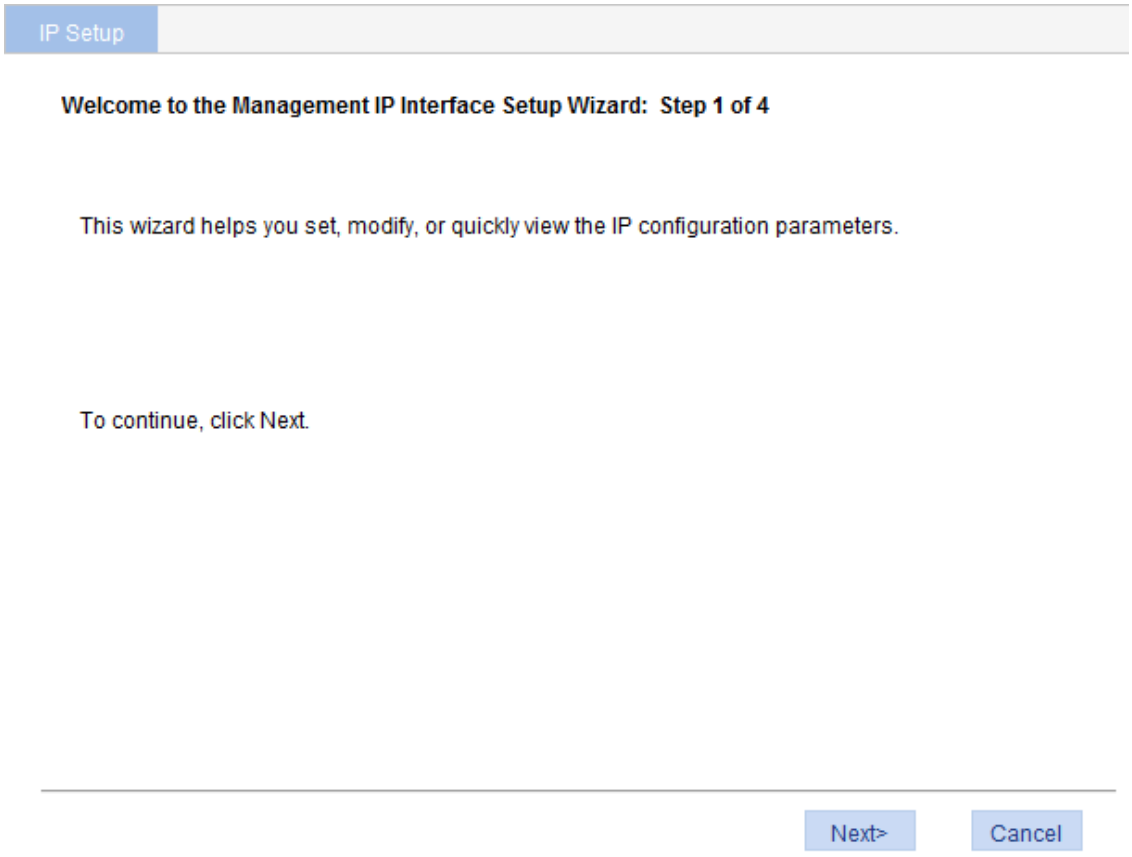
The configuration wizard guides you through configuring the basic service parameters, including the system name, system location, contact information, and management IP address.

Basic service setup

Entering the configuration wizard homepage

Select **Wizard** from the navigation tree.

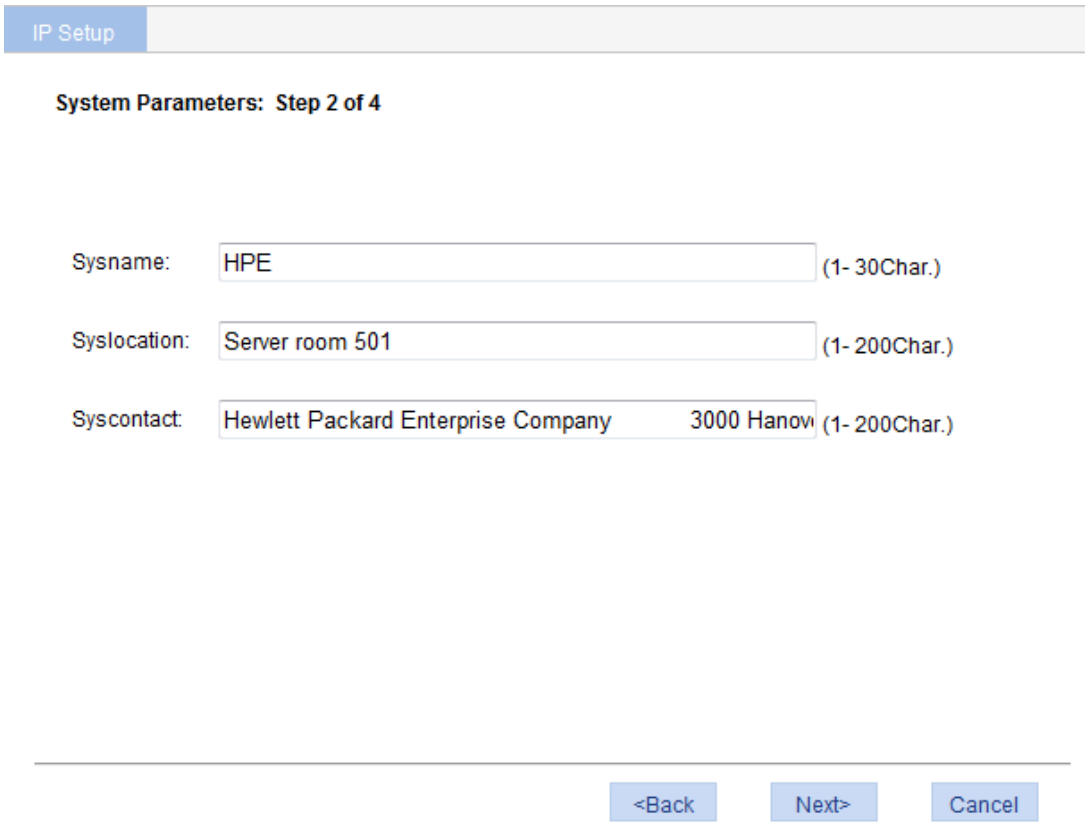
Figure 21 Configuration wizard homepage



Configuring system parameters

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

Figure 22 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."

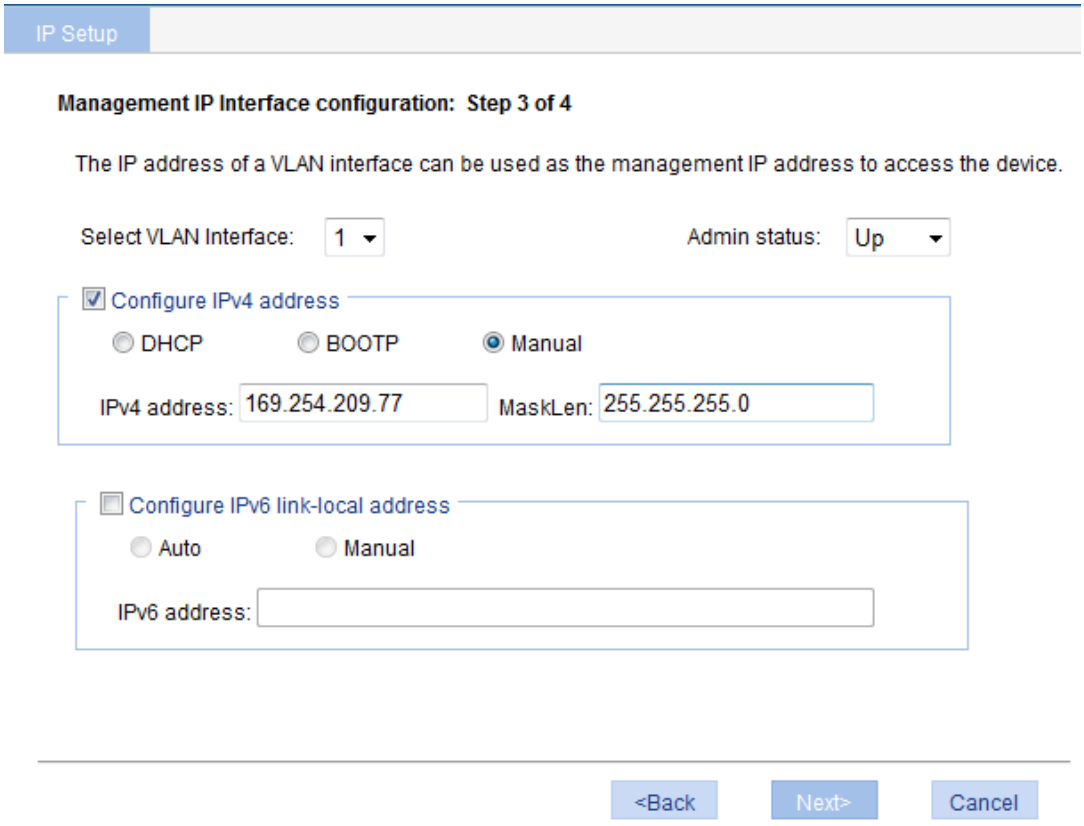
Configuring management IP address

CAUTION:

Modifying the management IP address used for the current login terminates 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 23 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. 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."

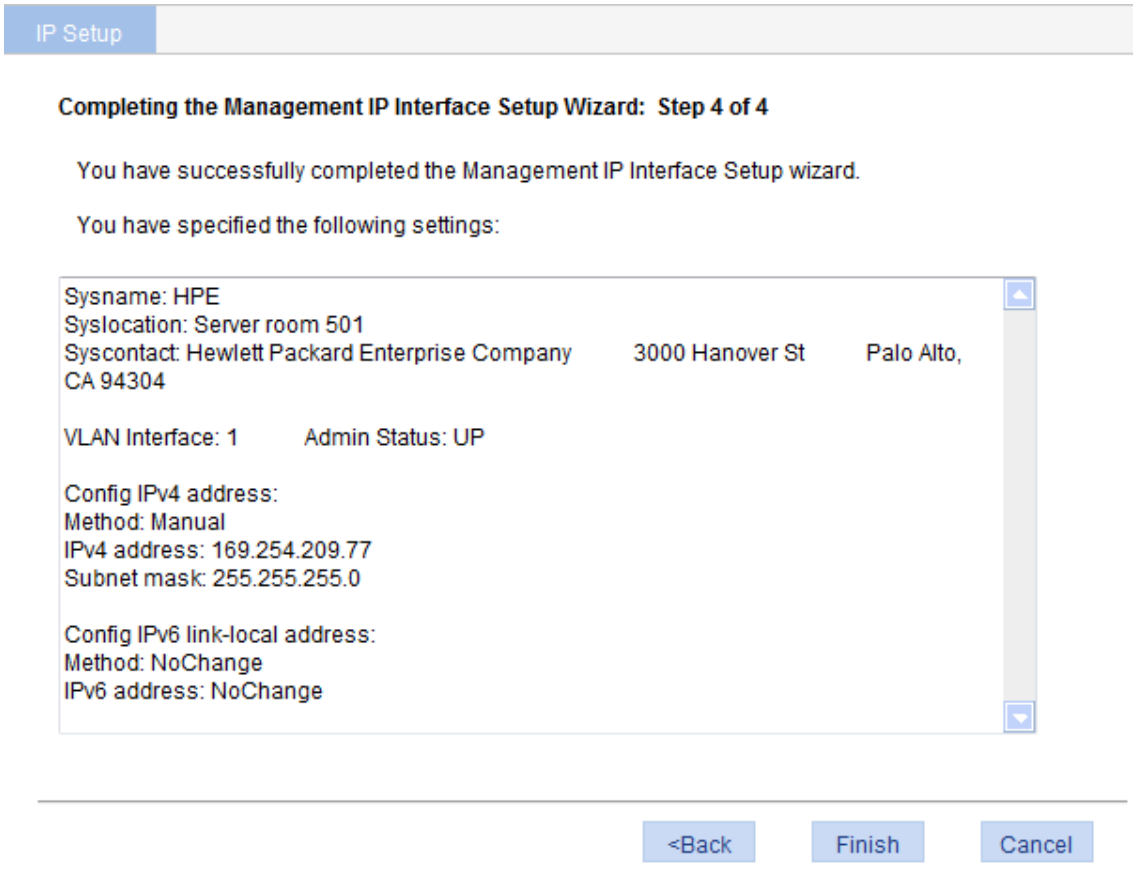
Item	Description	
Admin status	Enable or disable the VLAN interface. When errors occurred in the VLAN interface, disable the interface and then enable the port to bring the port to operate correctly. By default, the VLAN interface is down if no Ethernet ports in the VLAN is up. The VLAN is in the up 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.	
Configure IPv4 address	DHCP BOOTP Manual	Configure how the VLAN interface obtains an IPv4 address: • **DHCP**—Select the option for the VLAN interface to get an IP address through DHCP. • **BOOTP**—Select the option for the VLAN interface to get an IP address through BOOTP. • **Manual**—Select this option to manually specify an IPv4 address and the mask length for the VLAN interface.
	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.
Configure IPv6 link-local address	Auto Manual	Configure how the VLAN interface obtains an IPv6 link-local address. • **Auto**—Select this option for the device to automatically generate a link-local address based on the link-local address prefix (FE80::/64) and the link layer address of the interface. • **Manual**—Select this option to manually assign an IPv6 link-local address to the interface.
	IPv6 address	Specify an IPv6 link-local address for the VLAN interface. This field is configurable if you select **Manual**. 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 24 Configuration complete

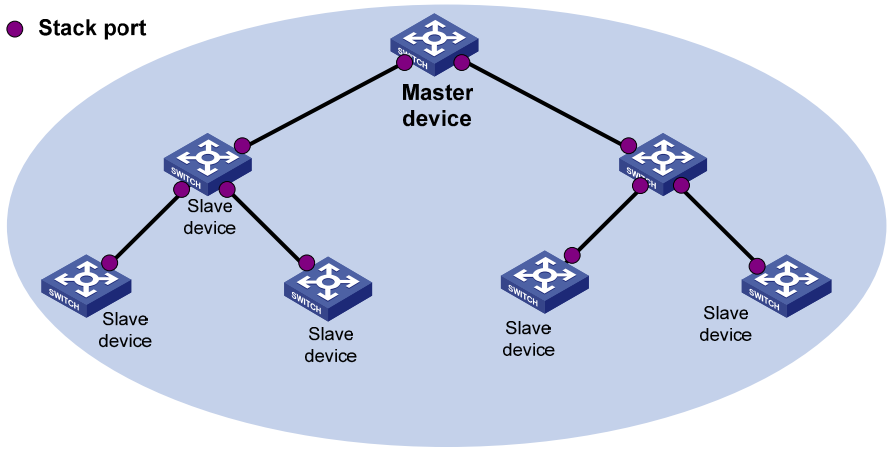


Configuring stack

Overview

The stack management feature allows you to configure and monitor a group of connected devices by logging in to one device in the stack, as shown in Figure 25.

Figure 25 Stacking devices



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

Configuration task list

Perform the tasks in Table 5 to configure a stack.

Table 5 Stack configuration task list

Task	Remarks
Configuring the master device of a stack:	
Configuring global parameters of a stack	Required. Configure a private IP address pool for a stack and establish the stack, and meantime the device becomes the master device of the stack. By default, no IP address pool is configured for a stack and no stack is established.
Configuring stack ports	Required. Configure the ports of the master device that connect to member devices as stack ports. By default, a port is not a stack port.
Configuring member devices of a stack:	

Task	Remarks
Configuring stack ports	Required. Configure a port of a member device that connects to the master device or another member device as a stack port. By default, a port is not a stack port.
Displaying topology summary of a stack	Optional. Display information about stack members.
Displaying device summary of a stack	Optional. Display the control panels of stack members. **IMPORTANT:** Before viewing the control panel of a member device, you must make sure the username, password, and access right you used to log on to the master device are the same with those configured on the member device; otherwise, the control panel of the member device cannot be displayed.
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:** Before logging in to a member device, you must make sure the username, password, and access right you used to log on to the master device are the same with those configured on the member device. Otherwise, you cannot log in to the member device. You can configure them by selecting **Device** and then clicking **Users** from the navigation tree.

Configuring global parameters of a stack

Select **Stack** from the navigation tree to enter the page shown in Figure 26. You can configure global parameters of a stack in the **Global Settings** area.

Figure 26 Setting up

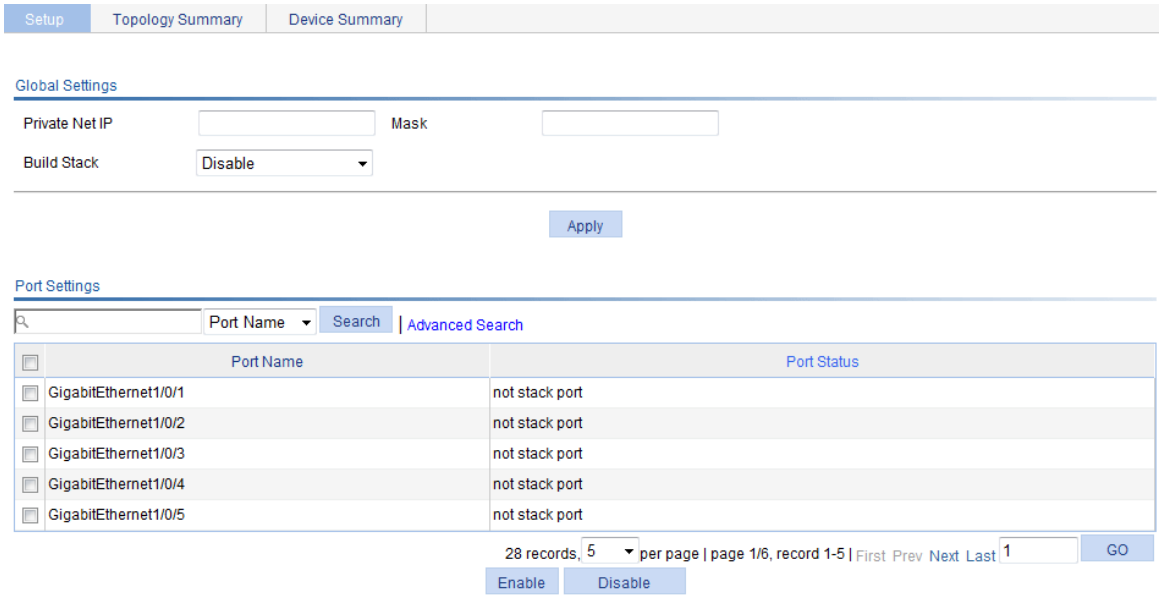


Table 6 Configuration items

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

Configuring stack ports

Select **Stack** from the navigation tree to enter the page shown in Figure 26. You can configure stack ports in the **Port Settings** area.

- 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 27.

Figure 27 Topology Summary tab

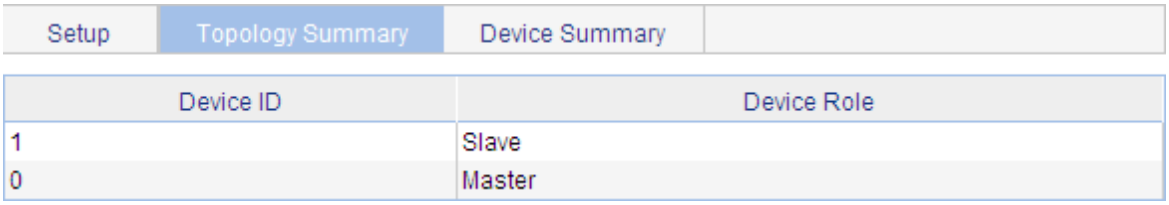


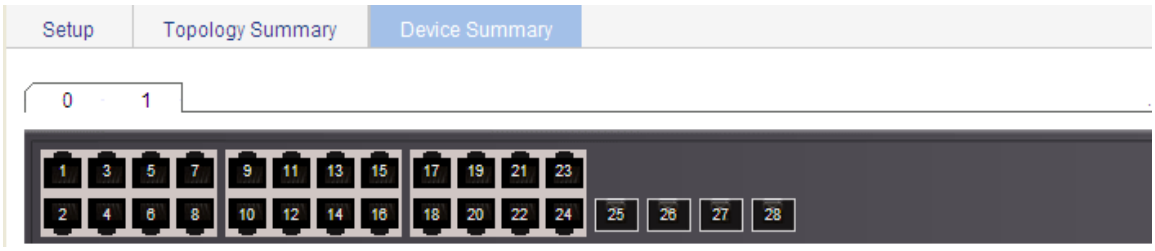
Table 7 Field description

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

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 28. On this page, you can view interfaces on the panel of each stack member by clicking the tab of the corresponding member device.

Figure 28 Device summary (the master device)

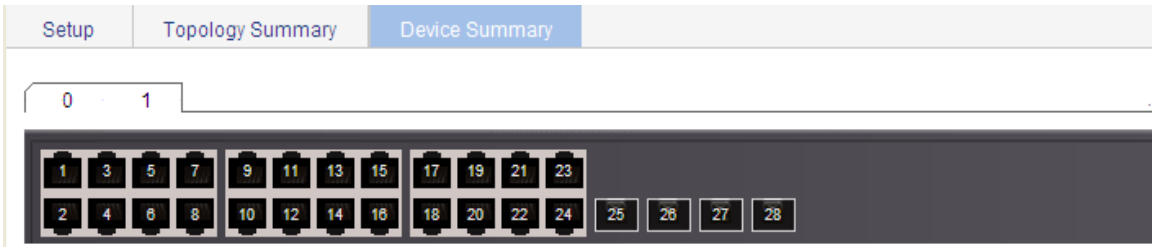


Logging in to a member device from the master

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

Click the **Configuring the Device** hyperlink, you can log in to the Web interface of the member device to manage and maintain the member device directly.

Figure 29 Device summary (a member device)



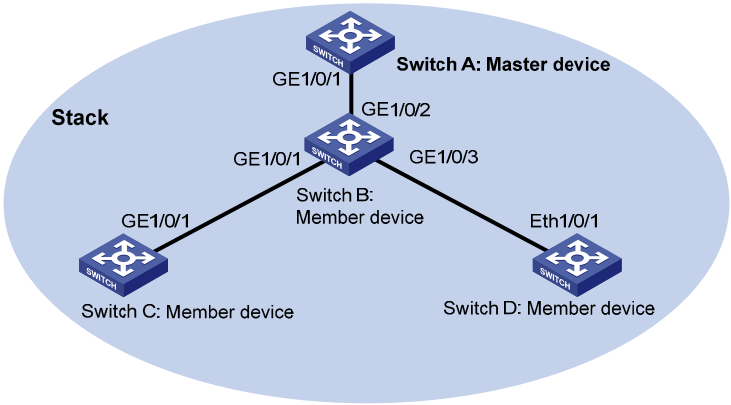
Stack configuration example

Network requirements

As shown in Figure 30, Switch A, Switch B, Switch C, and Switch D are connected to one another.

Create a stack, where Switch A is the master device, and Switch B, Switch C, and Switch D are member devices. An administrator can log in to Switch B, Switch C, and Switch D through Switch A to perform remote configurations.

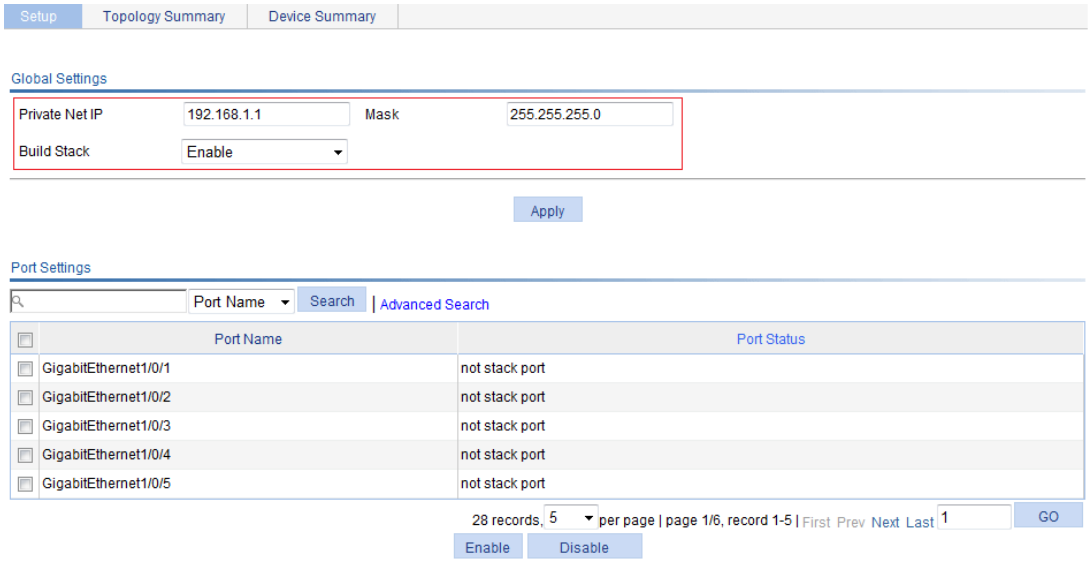
Figure 30 Network diagram



Configuration procedure

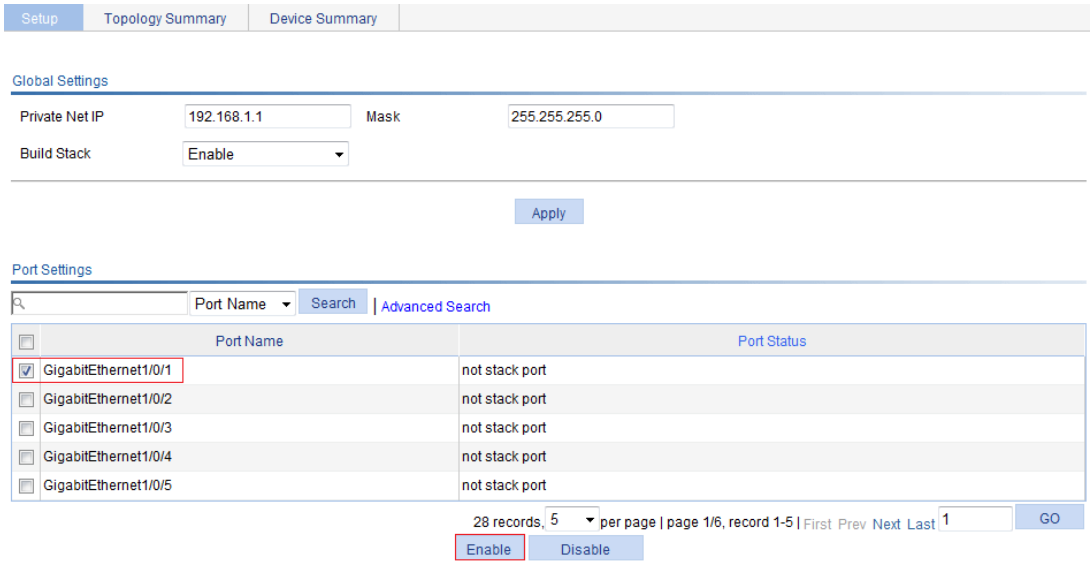
1. Configure global parameters for the stack on Switch A:
   a. Select **Stack** from the navigation tree of Switch A, and then perform the subsequent steps on the **Setup** tab, as shown in Figure 31.
   b. Type **192.168.1.1** in the field of **Private Net IP**.
   c. Type **255.255.255.0** in the field of **Mask**.
   d. Select **Enable** from the **Build Stack** list.
   e. Click **Apply**.

   Figure 31 Configuring global parameters for the stack on Switch A



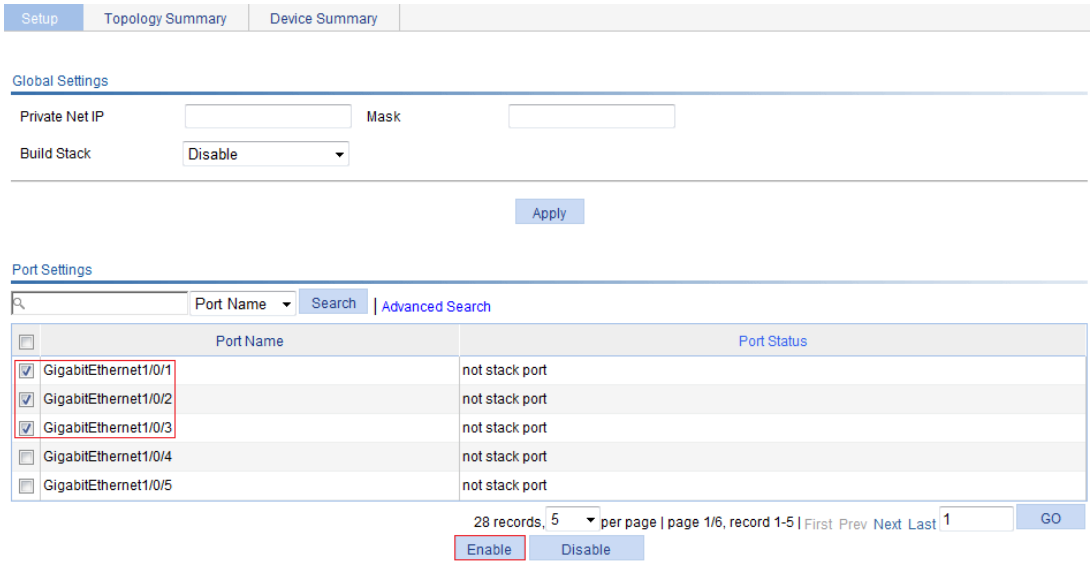
   Switch A becomes the master device.
2. Configure a stack port on Switch A:
   a. In the **Port Settings** area on the **Setup** tab, select **GigabitEthernet1/0/1**.
   b. Click **Enable**.

Figure 32 Configuring a stack port on Switch A



3. On Switch B, configure GigabitEthernet 1/0/2 (connected to Switch A), GigabitEthernet 1/0/1 (connected to Switch C), and GigabitEthernet 1/0/3 (connected to Switch D) as stack ports:
   a. Select **Stack** from the navigation tree of Switch B.
   b. In the **Port Settings** area on the **Setup** tab, select **GigabitEthernet1/0/1**, **GigabitEthernet1/0/2**, and **GigabitEthernet1/0/3**.
   c. Click **Enable**.

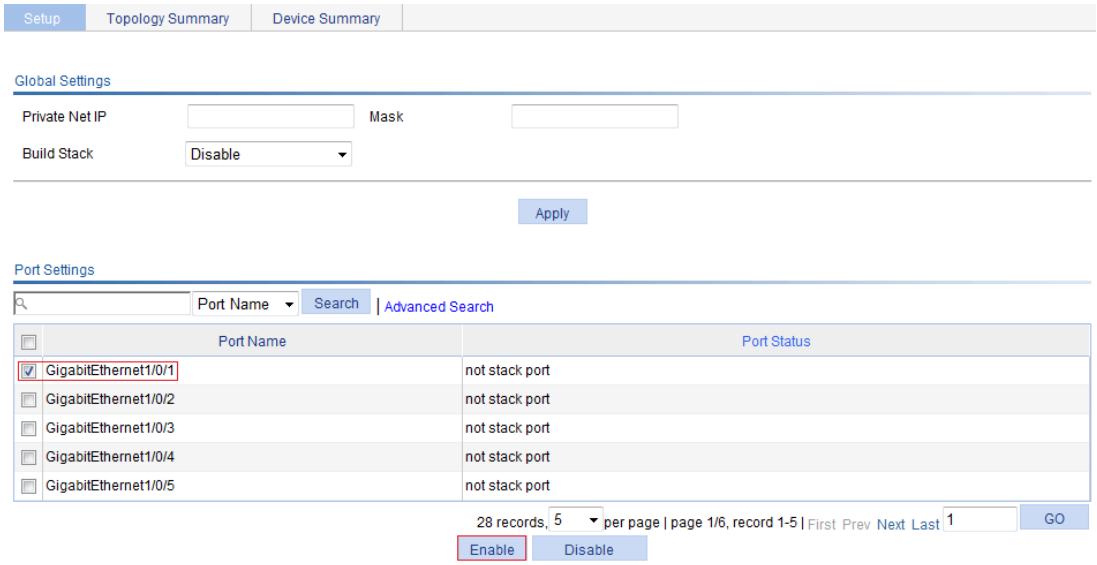
Figure 33 Configuring stack ports on Switch B



Switch B becomes a member device.

4. On Switch C, configure GigabitEthernet 1/0/1 (the port connected to Switch B) as a stack port:
   a. Select **Stack** from the navigation tree of Switch C.
   b. In the **Port Settings** area on the **Setup** tab, select **GigabitEthernet1/0/1**.
   c. Click **Enable**.

Figure 34 Configuring a stack port on Switch C



Switch C becomes a member device.

5. On Switch D, configure GigabitEthernet 1/0/1 (the port connected to Switch B) as a stack port:
   a. Select **Stack** from the navigation tree of Switch D.
   b. In the **Port Settings** area on the **Setup** tab, select **GigabitEthernet1/0/1**.
   c. Click **Enable**.

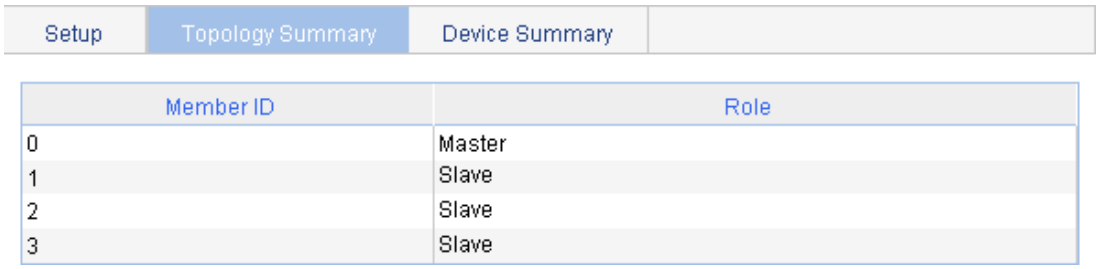
   Switch D becomes a member device.

Verifying the configuration

To verify the stack topology on Switch A:

1. Select **Stack** from the navigation tree of Switch A.
2. Click the **Topology Summary** tab.

Figure 35 Verifying the configuration



Configuration guidelines

When you configure a stack, follow these guidelines:

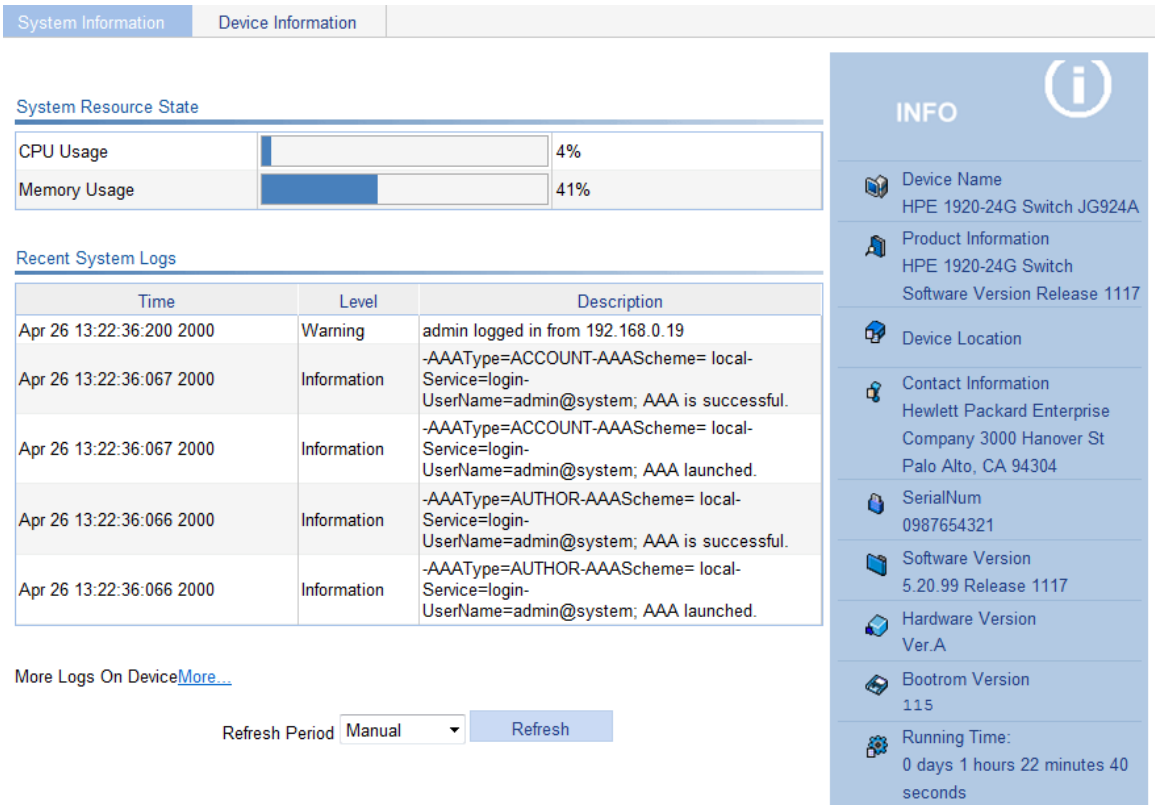
- If a device is already configured as the master device of a stack, you cannot modify the private IP address pool on the device.
- If a device is already configured as a member device of a stack, the **Global Settings** area on the member device is not available.

Displaying system and device information

Displaying system information

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

Figure 36 System information



Displaying basic system information

Table 8 Field description

Item	Description
Product Information	Description for the device.
Device Location	Device location, which you can configure on the page you enter by selecting **Device** > **SNMP** > **Setup**.
Contact Information	Contact information, which you can configure on the page you enter by selecting **Device** > **SNMP** > **Setup**.
SerialNum	Serial number of the device.
Software Version	Software version of the device.
Hardware Version	Hardware version of the device.
Bootrom Version	Boot ROM version of the device.

Item	Description
Running Time	System up time.

Displaying the system resource state

The **System Resource State** area displays the most recent CPU usage and memory usage.

Displaying recent system logs

Table 9 Field description

Field	Description
Time	Time when the system logs were generated.
Level	Severity of the system logs.
Description	Description for the system logs.

The **System Information** page displays up to five the most recent system logs.

To display more system logs, click **More** to enter the **Log List** page. You can also enter this page by selecting **Device** > **Syslog**. For more information, see "Configuring syslog."

Setting the refresh period

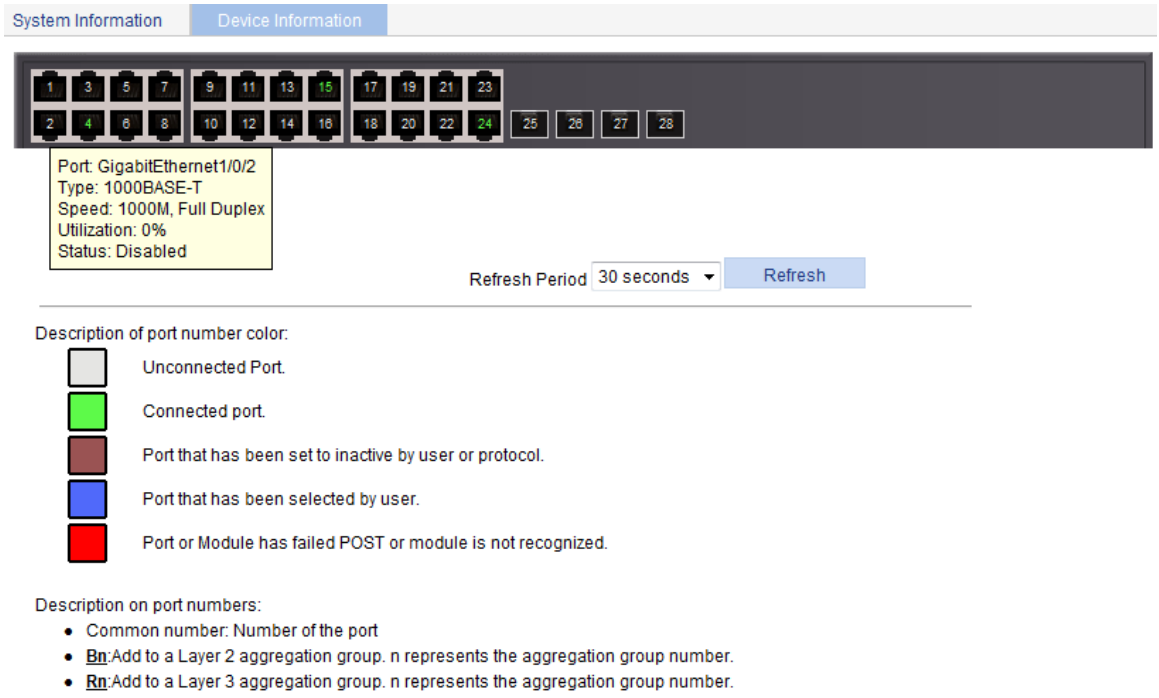
To set the interval for refreshing system information, select one of the following options from the **Refresh Period** list:

- If you select a certain period, the system refreshes system information at the specified interval.
- If you select **Manual**, the system refreshes system 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 that displays information about the device ports. Hover the cursor over a port and the port details appear, including the port name, type, speed, utilization, and status, as shown in Figure 37. The aggregation group number is also displayed if the port is added to an aggregation group. For the description about the port number and its color, see Figure 37.

Figure 37 Device information



To set the interval for refreshing device information, select one of the following options from the **Refresh Period** list:

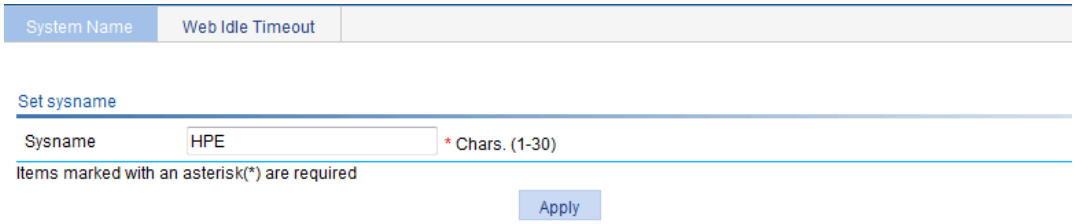
- If you select a certain period, the system refreshes device information at the specified interval.
- If you select **Manual**, the system refreshes device information only when you click the **Refresh** button.

Configuring basic device settings

The device basic information feature provides the following functions:

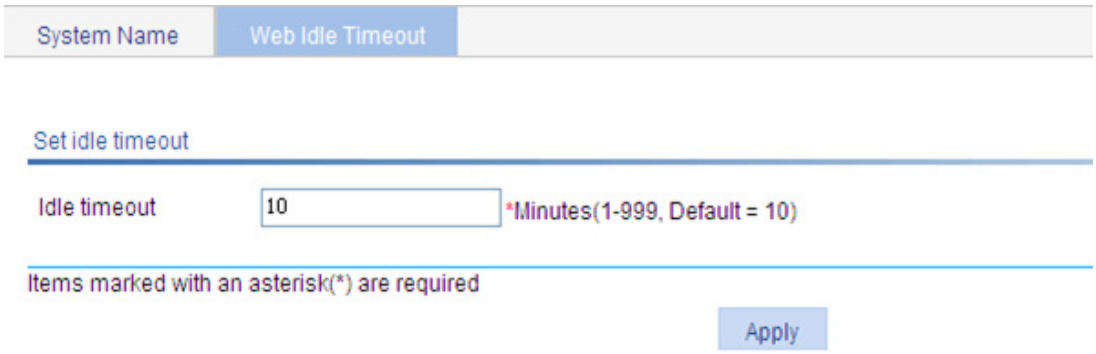
- Set the system name of the device. The configured system name is displayed on the top of the navigation bar.
- Set the idle timeout period for logged-in users. The system logs an idle user off the Web for security purpose after the configured period.

Configuring system name

1. Select **Device** > **Basic** from the navigation tree.
   The system name configuration page appears.
   Figure 38 Configuring the 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 39 Configuring the idle timeout period
   

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

Maintaining devices

Software upgrade

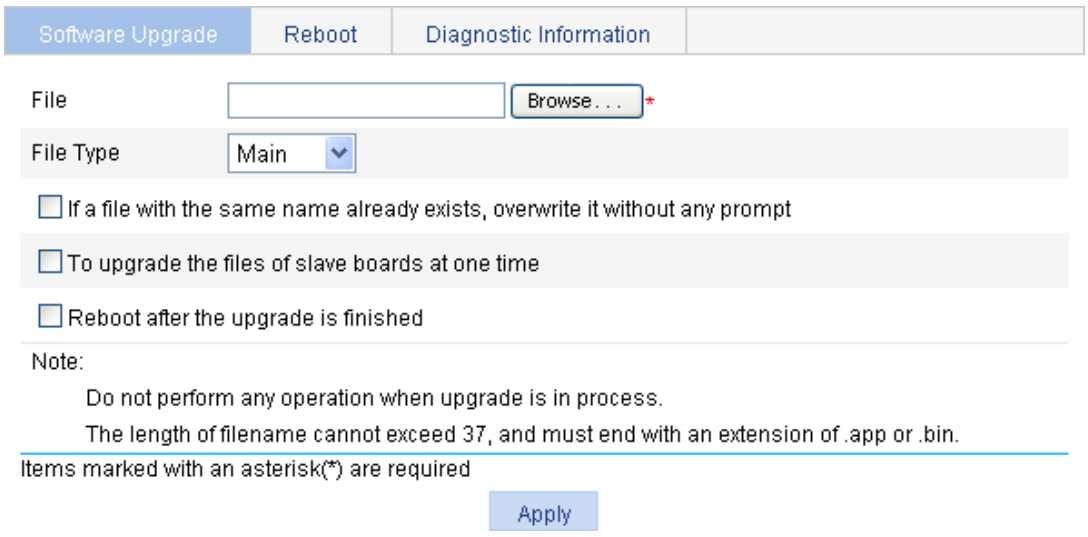
CAUTION:

Software upgrade takes some time. Avoid performing any operation on the Web interface during the upgrading procedure. Otherwise, the upgrade operation may be interrupted.

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 to be used at the next reboot. In addition, you can select whether to reboot the device to bring the upgrade software into effect.

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

Figure 40 Software upgrade configuration page



2. Configure software upgrade parameters as described in Table 10.
3. Click **Apply**.

Table 10 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 boot: • **Main**—Boots the device. • **Backup**—Boots the device when the main boot file is unavailable.
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.
Reboot after the upgrade finished	Specify whether to reboot the device to make the upgraded software take effect after the application file is uploaded.

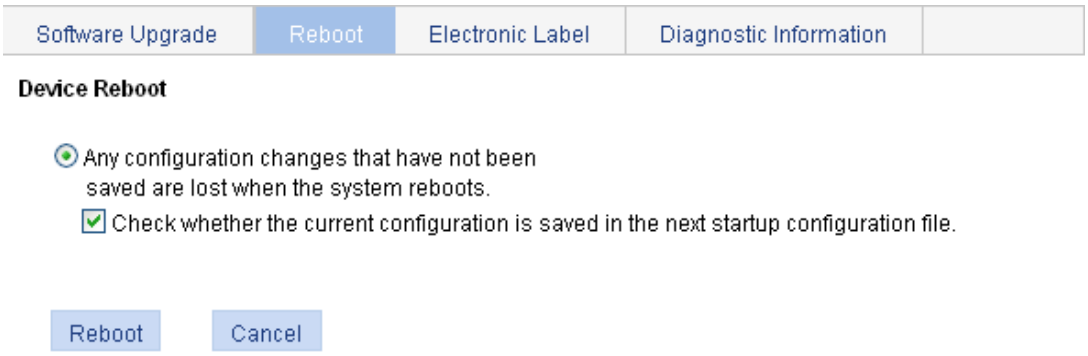
Device reboot

CAUTION:

- Before rebooting the device, save the configuration. Otherwise, all unsaved configuration will be lost after device reboot.
- When the device reboots, re-log in to the device.

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

Figure 41 Device reboot page



3. Enable or disable the "**Check whether the current configuration is saved in the next startup configuration file**" option.
4. Click **Reboot**. A confirmation dialog box appears.
5. Click **OK**.

- If you select **Check whether the current configuration is saved in the next startup configuration file**, the system will check the configuration before rebooting the device. If the check succeeds, the system reboots 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 is not rebooted. In this case, save the current configuration manually before you can reboot the device.
- If you do not select the box, the system reboots the device directly.

Electronic label

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

1. Select **Device** > **Device Maintenance** from the navigation tree.
2. Click the **Electronic Label** tab to view the electronic label information.

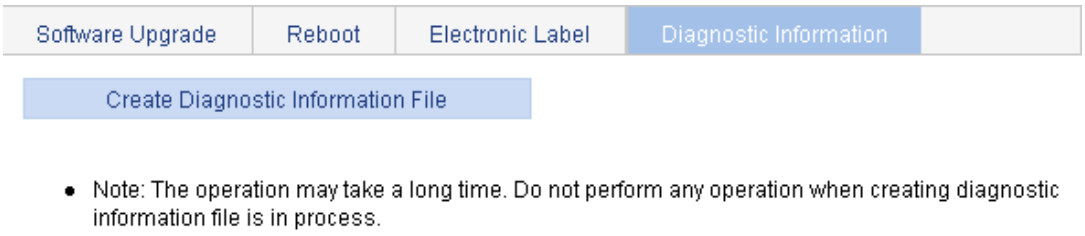
Figure 42 Electronic label

Diagnostic information

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

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

   Figure 43 Diagnostic information

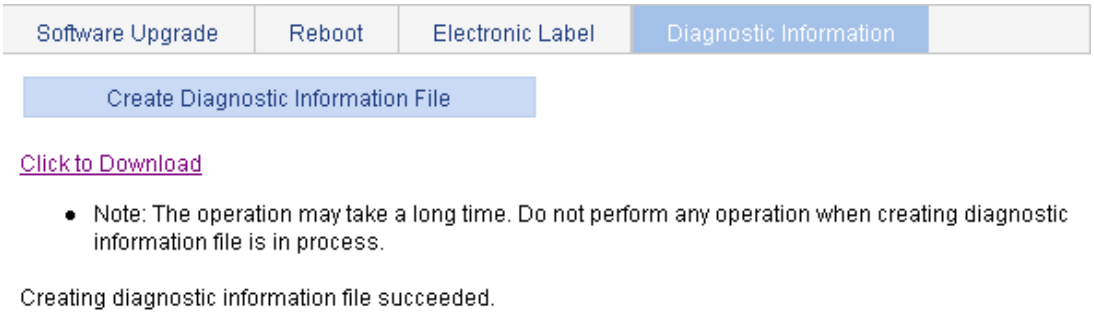
   

3. Click **Create Diagnostic Information File**.

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

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

   Figure 44 The diagnostic information file is created

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

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

Configuring system time

Overview

You must configure a correct system time so that the device can operate correctly with other devices. The system time module allows you to display and set the device system time on the Web interface.

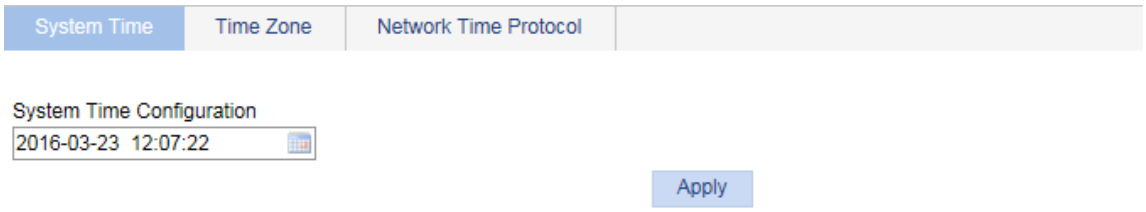
You can set the system time through manual configuration or network time protocol (NTP) automatic synchronization.

Defined in RFC 1305, the 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 time

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

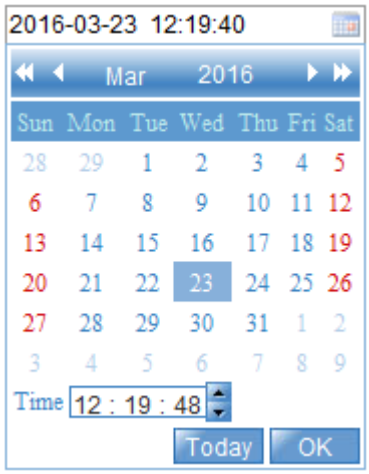
Figure 45 System time configuration page



Manually configuring the system time

1. Select **Device** > **System Time** from the navigation tree.
   The page for configuration the system time appears.
2. Click the **System Time Configuration** text to open a calendar.

   Figure 46 Calendar page



3. Enter the system date and time in the **Time** field, or select the date and time in the calendar. To set the time on the calendar page, select one of the following methods:

- 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**.

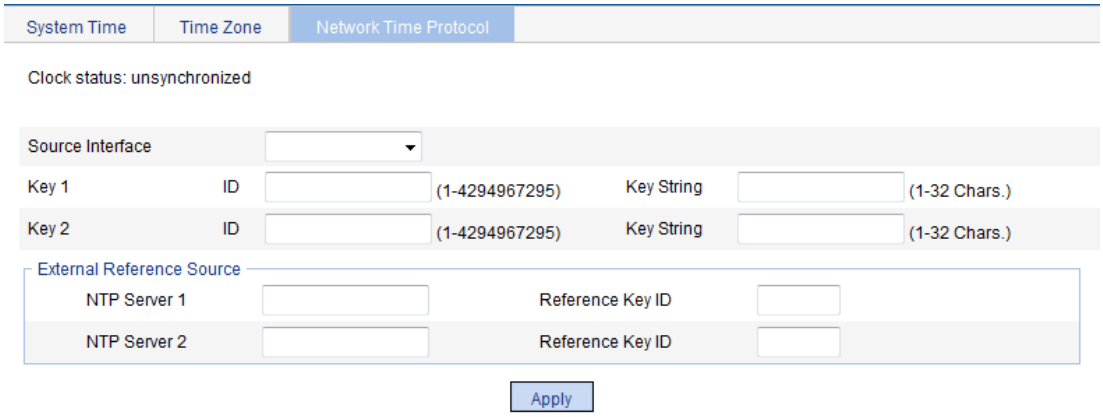
4. Click **Apply** on the system time configuration page to save your configuration.

Configuring system time by using NTP

1. Select **Device** > **System Time** from the navigation tree.
2. Click the **Network Time Protocol** tab.

   The page for configuring the system time through NTP appears.

Figure 47 NTP configuration page



3. Configure the system time as described in Table 11.
4. Click **Apply**.

Table 11 Configuration items

Item	Description
Clock status	Display the synchronization status of the system clock.
Source Interface	Set the source interface for an NTP message. This configuration makes the source IP address in the NTP messages the primary IP address of this interface. If the specified source interface is down, the source IP address is the primary IP address of the egress interface. **TIP:** If you do not want the IP address of an interface on the local device to become the destination address of response messages, specify the source interface for NTP messages.

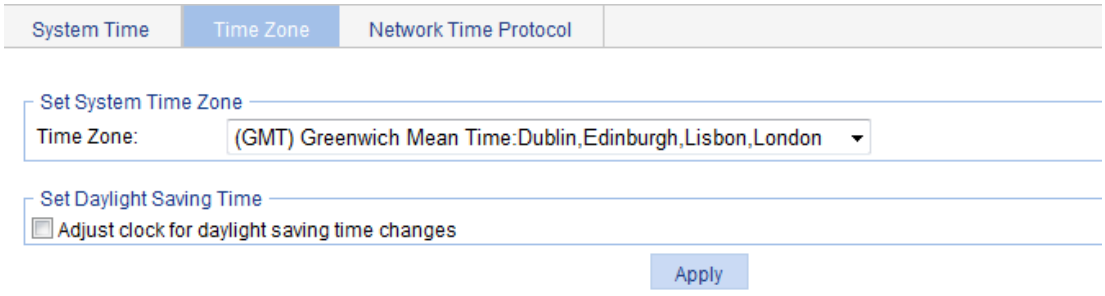
Item		Description
Key 1		Set NTP authentication key. Enable the NTP authentication feature for a system running NTP in a network that requires high security. This feature improves the network security by means of client-server key authentication, and prohibits a client from synchronizing with a device that has failed authentication. You can set two authentication keys, each of which has a key ID and a key string. • **ID**—ID of a key. • **Key string**—Character string of the MD5 authentication key.
Key 2		
External Reference Source	NTP Server 1/Reference Key ID.	Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. The device synchronizes its time to the NTP server only if the key provided by the server is the same as the specified key. You can configure two NTP servers. The clients 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.
	NTP Server 2/Reference Key ID.	

Configuring the time zone and daylight saving time

1. Select Device > System Time from the navigation tree.
2. Click the **Time Zone** tab.

   The time zone configuration page appears.

   Figure 48 Setting the time zone

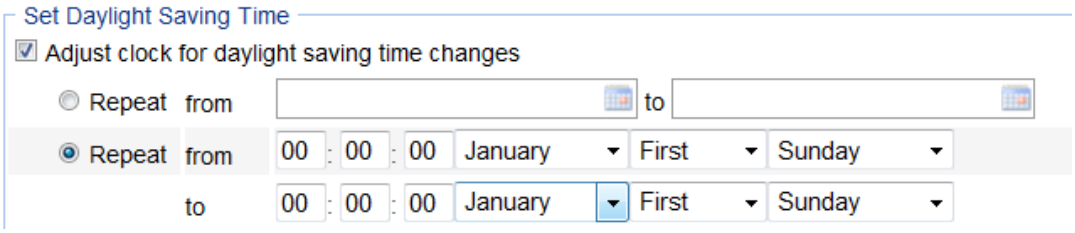


3. Configure the time zone and daylight saving time as described in Table 12.
4. Click **Apply**.

Table 12 Configuration items

Item	Description
Time Zone	Set the time zone for the system.
Adjust clock for daylight saving time changes	Adjust the system clock for daylight saving time changes, which means adding one hour to the current system time. Click **Adjust clock for daylight saving time changes** to expand the option, as shown in Figure 49. You can configure the daylight saving time changes in the following ways: • Specify that the daylight saving time starts on a specific date and ends on a specific date. The time range must be greater than one day and smaller than one year. For example, configure the daylight saving time to start on August 1st, 2006 at 06:00:00 a.m., and end on September 1st, 2006 at 06:00:00 a.m. • Specify that the daylight saving time starts and ends on the corresponding specified days every year. The time range must be greater than one day and smaller than one year. For example, configure the daylight saving time to start on the first Monday in August at 06:00:00 a.m., and end on the last Sunday in September at 06:00:00 a.m.

Figure 49 Setting the daylight saving time



System time configuration example

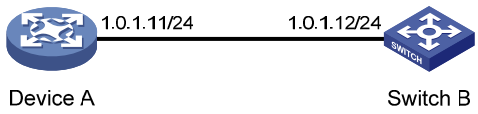
Network requirements

As shown in Figure 50:

- The local clock of Device A is set as the reference clock.
- Switch B operates in client mode, and uses Device A as the NTP server.

Configure NTP authentication on Device A and Switch B so that Switch B is to be synchronized to Device A.

Figure 50 Network diagram

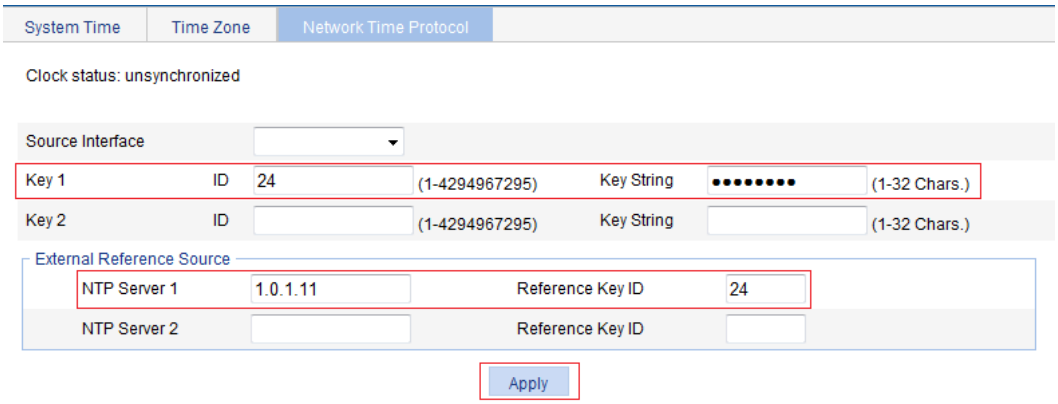


Configuring the system time

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** as 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, 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 51 Configuring Device A as the NTP server of Switch B



Verifying the configuration

After the configuration, verify that Device A and Switch B have the same system time.

Configuration guidelines

When you configure the system time, follow these 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 the level of a client's clock, the client will not synchronize its clock to the server's.
- The synchronization process takes some time. The clock status might be displayed as **unsynchronized** after your configuration. In this case, 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 time gap exceeds the Web idle time specified on the device, all online Web users are logged out because of timeout after the synchronization finishes.

Configuring syslog

System logs record network and device information, including running status and configuration changes. With system logs, administrators can take corresponding actions against network problems and security problems.

The system sends system logs to the following destinations:

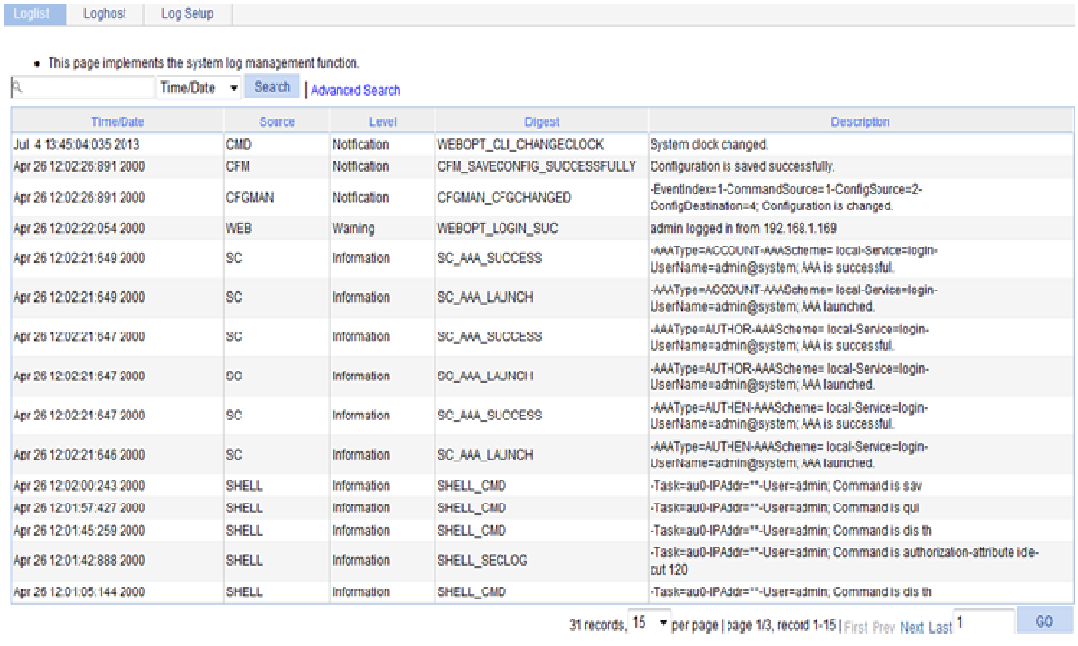
- Console.
- Monitor terminal, a terminal that has logged in to the device through the AUX or VTY user interface.
- Log buffer.
- Log host.
- Web interface.
- Log file.

Displaying syslogs

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

   The page for displaying syslogs appears. 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."

   Figure 52 Displaying syslogs



2. View system logs.

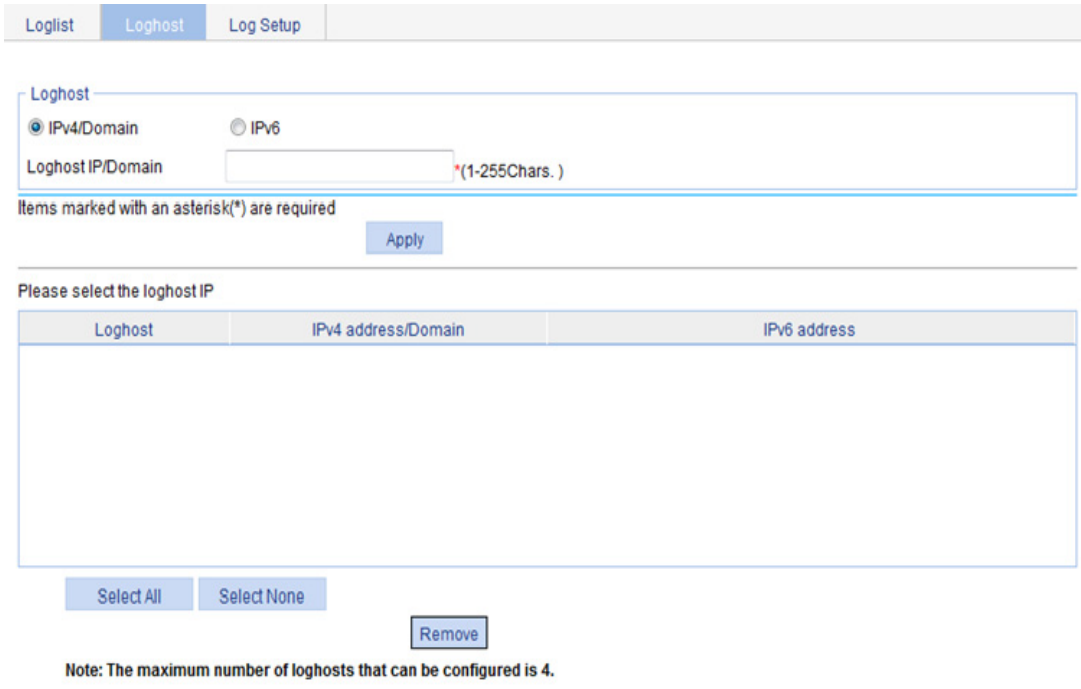
Table 13 Field description

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

Setting the log host

1. Select **Device** > **Syslog** from the navigation tree.
2. Click the **Loghost** tab.
   The log host configuration page appears.

   Figure 53 Setting the log host



3. Configure the log host as described in Table 14.
4. Click **Apply**.

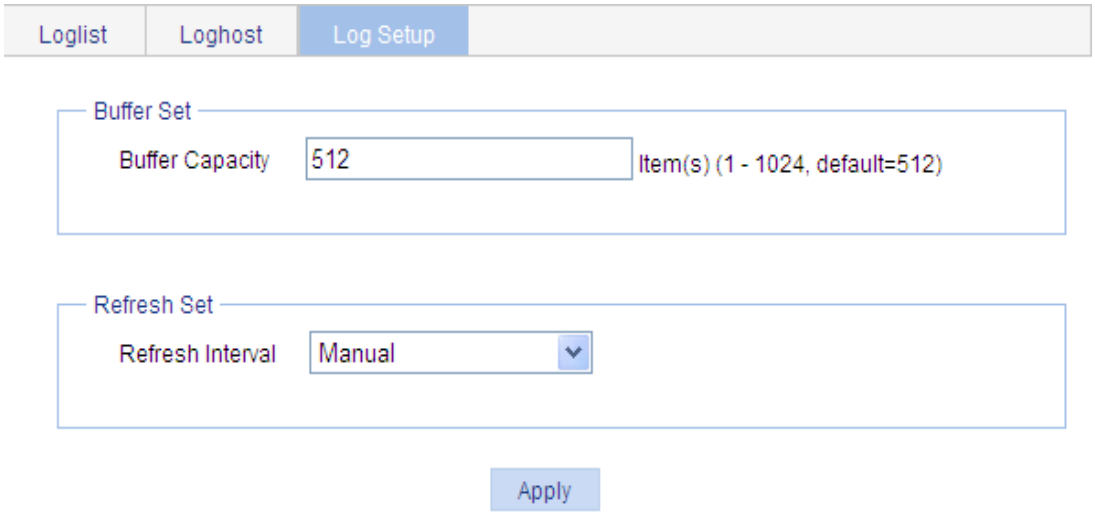
Table 14 Configuration items

Item	Description	
IPv4/Domain	Specify the IPv4 address or domain name of the log host.	**IMPORTANT:** You can specify up to four log hosts.
Loghost IP/Domain		
IPv6	Set the IPv6 address of the log host.	
Loghost IP		

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 54 Syslog configuration page



3. Configure buffer capacity and refresh interval as described in Table 15.
4. Click **Apply**.

Table 15 Configuration items

Item	Description
Buffer Capacity	Set the number of logs that can be stored in the log buffer.
Refresh Interval	Set the log refresh interval. You can select manual refresh or automatic refresh: • **Manual**—Click **Refresh** to view the latest log information. • **Automatic**—Select to refresh the Web interface every 1 minute, 5 minutes, or 10 minutes.

Managing the configuration

You can back up, restore, save, or reset the device configuration.

Backing up the configuration

Configuration backup allows you to do the following:

- Open and view the configuration files for the next startup, including the **.cfg** file and **.xml** file.
- Back up the configuration files for the next startup to your local host.

IMPORTANT:

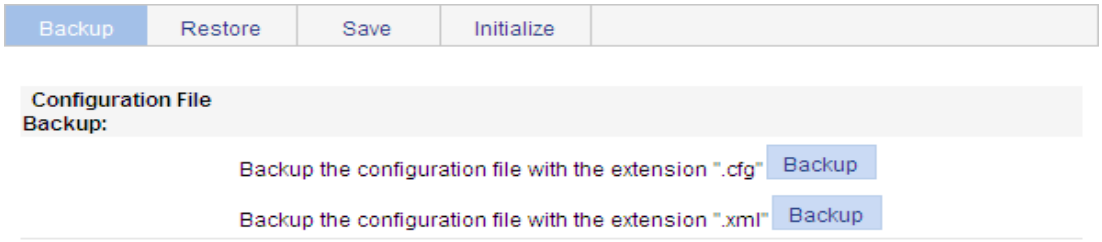
Hewlett Packard Enterprise recommends backing up both the **.cfg** and **.xml** files. If you back up only the **.cfg** file, some configuration information might not be restored when, for example, the configuration is mistakenly removed.

To back up the configuration:

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

   The **Backup** page appears.

   Figure 55 Backing up the configuration

2. Click the upper **Backup** button.

   The file download dialog box appears.
3. Choose to view the **.cfg** file or to save the file to your local host.
4. Click the lower **Backup** button.

   The file download dialog box appears.
5. Choose to view the **.xml** file or to save the file to the local host.

Restoring the configuration

Configuration restoration allows you to do the following:

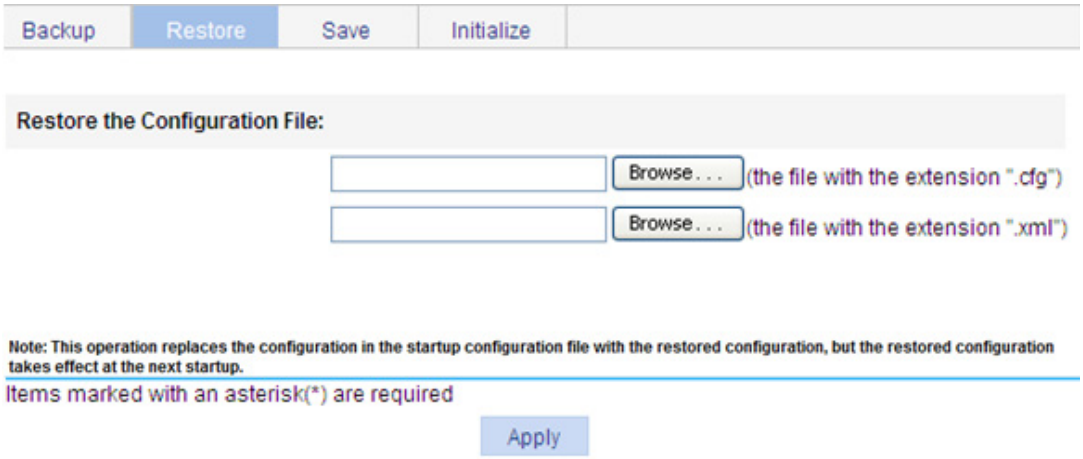
- Upload a **.cfg** file from your local host to the device.
- Upload an **.xml** file from your local host to the device, and delete the **.xml** configuration file that was used for the next startup.

The restored configuration takes effect at the next device startup.

To restore the configuration:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Restore** tab.

Figure 56 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 **OK**.
5. Click the lower **Browse** button.

   The file upload dialog box appears.
6. Select the **.xml** file to be uploaded, and click **OK**.

Saving the configuration

You save the running configuration to both the **.cfg** configuration file and **.xml** configuration file that will be used at the next startup.

Saving the configuration takes some time.

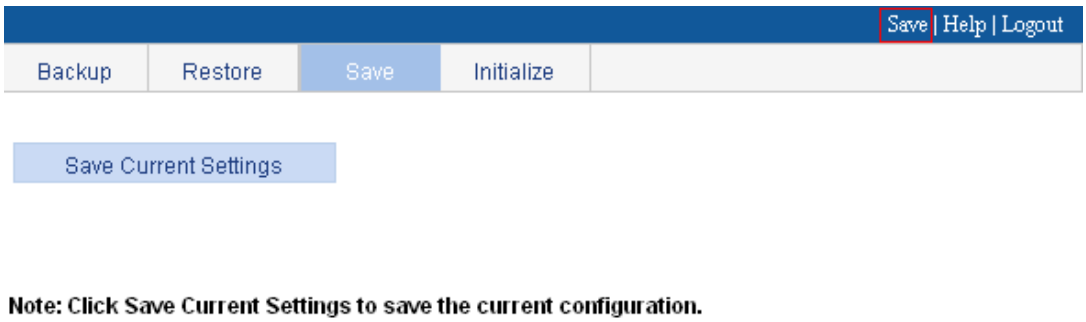
Only one administrator can save the configuration at a moment. If you save the configuration while the system is saving the configuration as required by another administrator, the system prompts you to try again later.

You can save the configuration in either of the following modes:

- Fast mode.

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

  Figure 57 Saving the configuration

- Common mode.

  To save the configuration in common mode:

  a. Select **Device** > **Configuration** from the navigation tree.

  b. Click the **Save** tab.

  c. Click **Save Current Settings**.

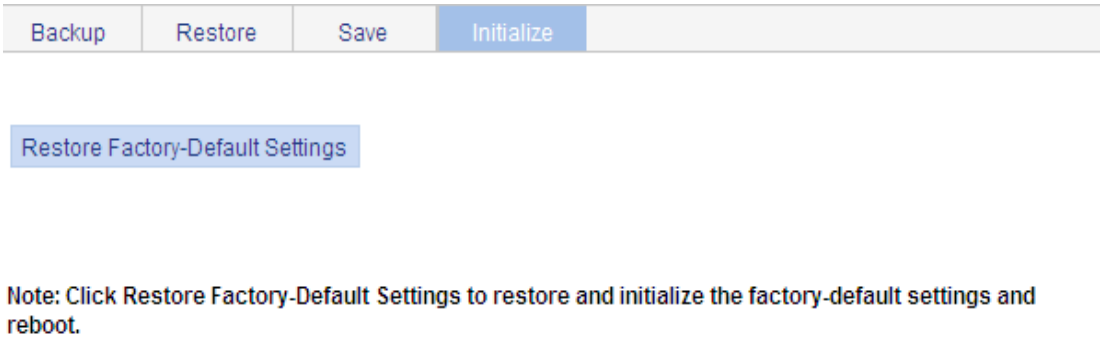
Resetting the configuration

Resetting the configuration restores the device's factory defaults, deletes the current configuration files, and reboots the device.

To reset the configuration:

1. Select **Device** > **Configuration** from the navigation tree.
2. Click the **Initialize** tab.
3. Click **Restore Factory-Default Settings**.

Figure 58 Resetting the configuration



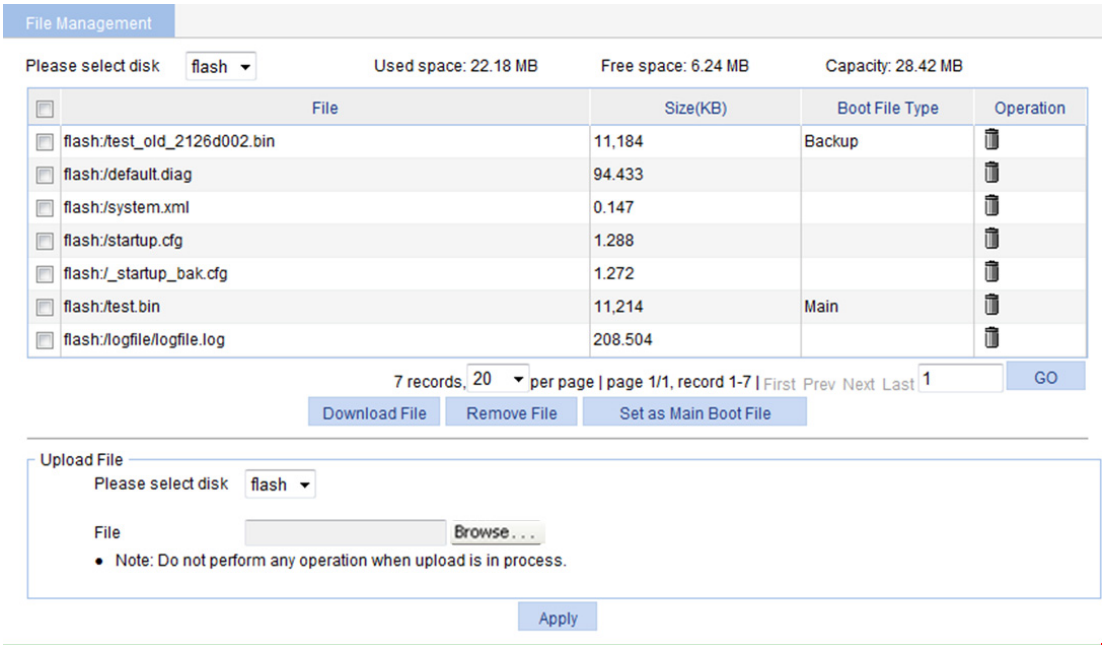
Managing files

The device requires a series of files for correct operation, including boot files and configuration files. These files are saved on the storage media. You can display files on the storage media, download, upload, or remove a file, or specify the main boot file.

Displaying files

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

   Figure 59 File management page



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

   Two categories of information are displayed:

- Medium information, including the used space, the free space, and the capacity of the medium.
- File information, including all files on the medium, the file sizes, and the boot file types (**Main** or **Backup**). The boot file type is only displayed for an application file (**.bin** or **.app** file) that will be used as the main or backup boot file.

Downloading a file

1. Select **Device** > **File Management** from the navigation tree to enter the file management page (see Figure 59).
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 path.

Uploading a file

IMPORTANT:

Uploading a file takes some time. Hewlett Packard Enterprise recommends not performing any operation on the Web interface during the upload.

1. Select **Device** > **File Management** from the navigation tree to enter the file management page (see Figure 59).
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 59).
2. Do one of the following:

- Click the  icon of a file to remove the file.
- Select a file from the file list and click **Remove File**.

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

Specifying the main boot file

1. Select **Device** > **File Manage** from the navigation tree to enter the file management page (see Figure 59).
2. From the **Please select disk** list, select the medium that holds the application file to be used as the main boot file.
3. Select the application file (**.bin** or **.app** file) from the file list.
4. Click **Set as Main Boot File**.

Managing ports

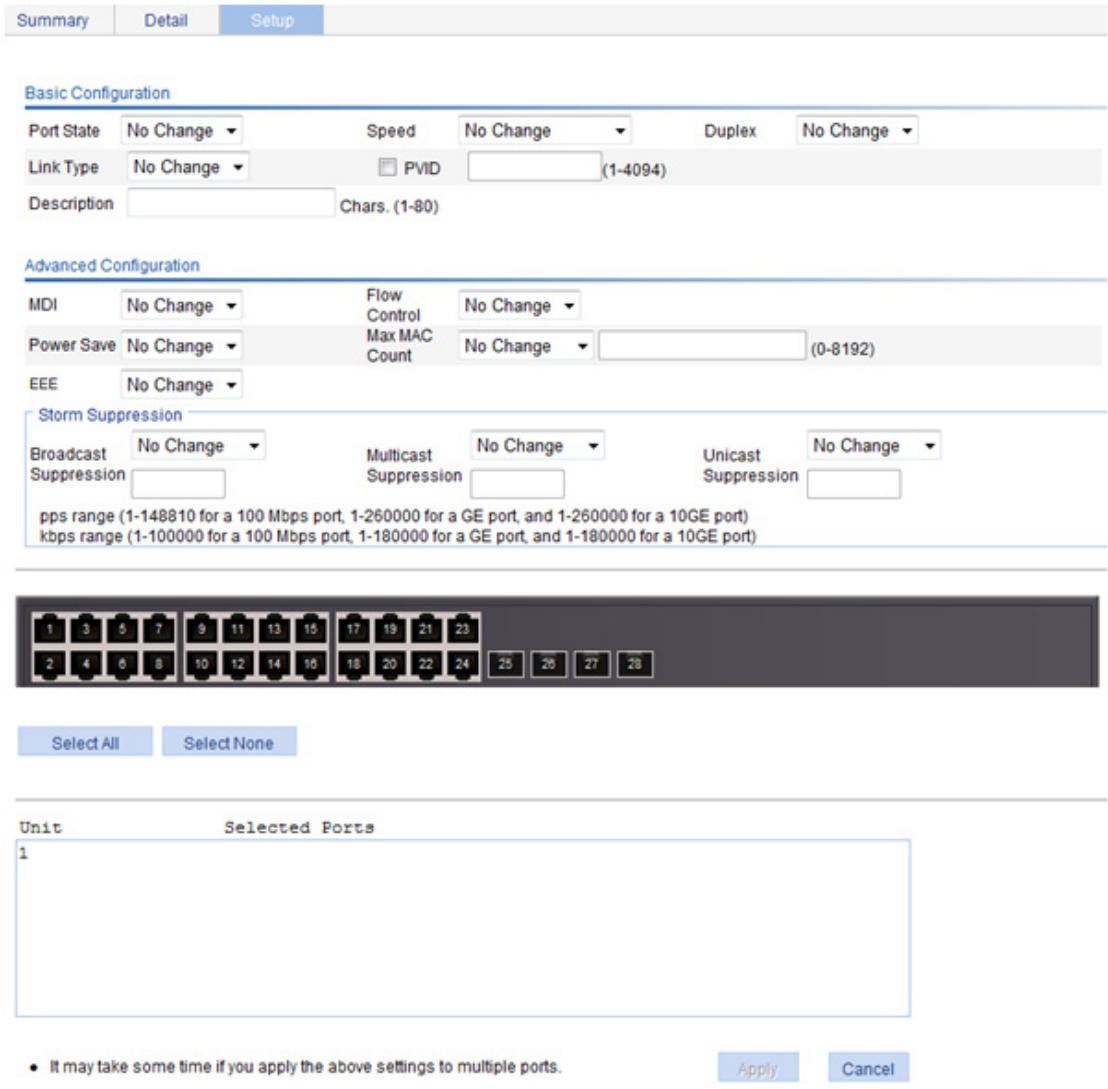
You can use the port management feature to set and view the operation parameters of a Layer 2 Ethernet port and an aggregate interface.

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

Setting operation parameters for a port

1. Select **Device** > **Port Management** from the navigation tree.
2. Click the **Setup** tab.

Figure 60 The Setup tab



3. Set the operation parameters for the port as described in Table 16.

4. Click **Apply**.

Table 16 Configuration items

Item	Description
Port State	Enable or disable the port. Sometimes, after you modify the operation parameters of a port, you must disable and then enable the port to have the modifications take effect.
Speed	Set the transmission speed of the port: • **10**—10 Mbps. • **100**—100 Mbps. • **1000**—1000 Mbps. • **Auto**—Autonegotiation. • **Auto 10**—Autonegotiated to 10 Mbps. • **Auto 100**—Autonegotiated to 100 Mbps. • **Auto 1000**—Autonegotiated to 1000 Mbps. • **Auto 10 100**—Autonegotiated to 10 or 100 Mbps. • **Auto 10 1000**—Autonegotiated to 10 or 1000 Mbps. • **Auto 100 1000**—Autonegotiated to 100 or 1000 Mbps. • **Auto 10 100 1000**—Autonegotiated to 10, 100, or 1000 Mbps.
Duplex	Set the duplex mode of the port: • **Auto**—Autonegotiation. • **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." 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 port VLAN ID (PVID) of the interface. For more information about setting the PVID, see "Configuring VLANs." To make sure a link correctly transmits packets, the trunk or hybrid ports at the two ends of the link must have the same PVID.
Description	Set the description of the port.
MDI	Set the MDI mode of the port. You can use two types of Ethernet cables 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, and 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, and 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 autonegotiation. • For an Ethernet port in normal mode, the pin roles are changed. Pin 1 and pin 2 are used for receiving signals, and 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. Configure the MDI mode depending on the cable types. When you configure the MID mode, follow these guidelines: • Typically, use the **auto** mode. 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.

Item	Description
	• 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**.
Flow Control	Enable or disable flow control on the port. With flow control enabled at both sides, when traffic congestion occurs on the ingress port, the ingress port sends 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. Flow control works only after it is enabled on both the ingress and egress ports.
Power Save	Enable or disable auto power-down on a port that is down. By default, auto power-down is disabled on an Ethernet port that is down. With auto power-down enabled on an Ethernet port that stays in the down state for a certain period, the following events occur: • The device automatically stops supplying power to the port. • The port enters the power save mode. When the Ethernet port comes up, the following events occur: • The device automatically restores power supply to the port. • The port resumes its normal state.
Max MAC Count	Set the MAC learning limit on the port: • **User Defined**—Select this option to set the limit manually. • **No Limited**—Select this option to set no limit.
EEE	Enable or disable Energy Efficient Ethernet (EEE) on a link-up port. With EEE enabled, when a link-up Ethernet port does not receive any packet for a certain period, it automatically enters low power mode. When a packet arrives later, the device restores power supply to the port and the port resumes its normal state.
Broadcast Suppression	Set broadcast suppression on the port: • **ratio**—Sets the maximum percentage of broadcast traffic to the total bandwidth of an Ethernet port. When you select this option, you must enter 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 you select this option, you must enter 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 you select this option, you must enter a number in the box below.
Multicast Suppression	Set multicast suppression on the port: • **ratio**—Sets the maximum percentage of multicast traffic to the total bandwidth of an Ethernet port. When you select this option, you must enter 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 you select this option, you must enter 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 you select this option, you must enter a number in the box below.

Item	Description
Unicast Suppression	Set unicast suppression on the port: • **ratio**—Sets the maximum percentage of unicast traffic to the total bandwidth of an Ethernet port. When you select this option, you must enter 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 you select this option, you must enter 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 you select this option, you must enter a number in the box below.
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. You can set only the state and MAC learning limit for an aggregate interface.

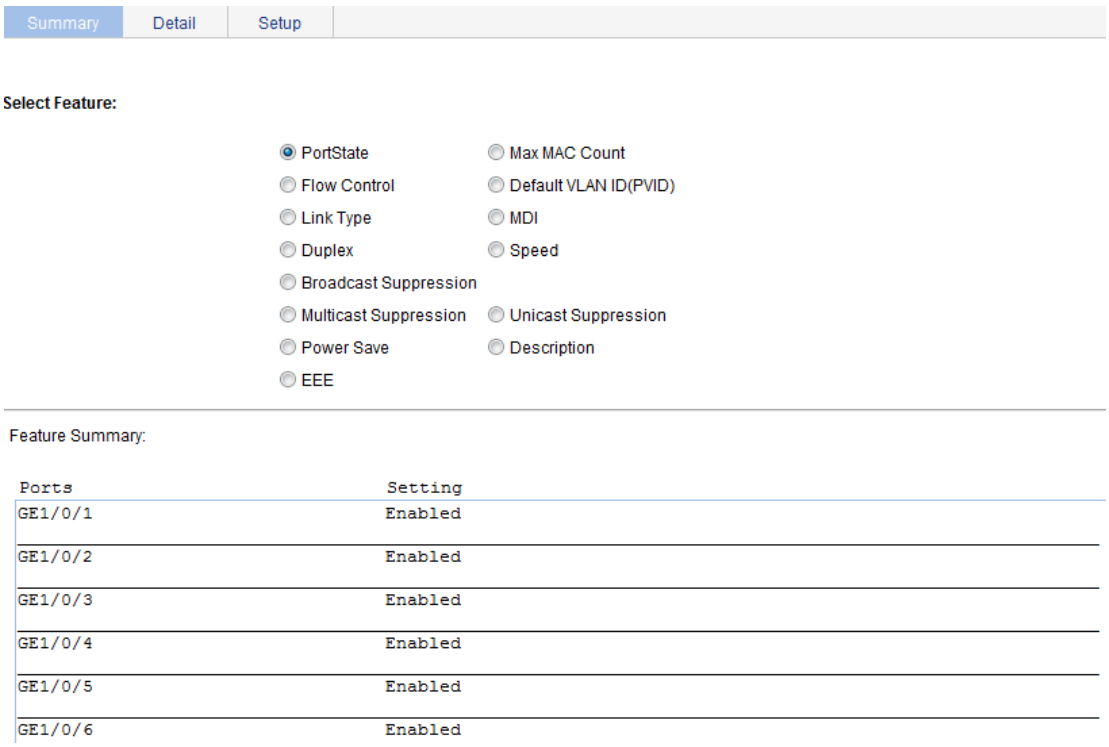
If you set operation parameters that a port does not support, you are notified of invalid settings and might fail to set the supported operation parameters for the port or other ports.

Displaying port operation parameters

Displaying a specified operation parameter for all ports

1. Select **Device** > **Port Management** from the navigation tree.
   The **Summary** page appears by default.
2. Select the option for a parameter you want to view.
   The parameter information for all the ports is displayed in the lower part of the page.

Figure 61 The Summary tab

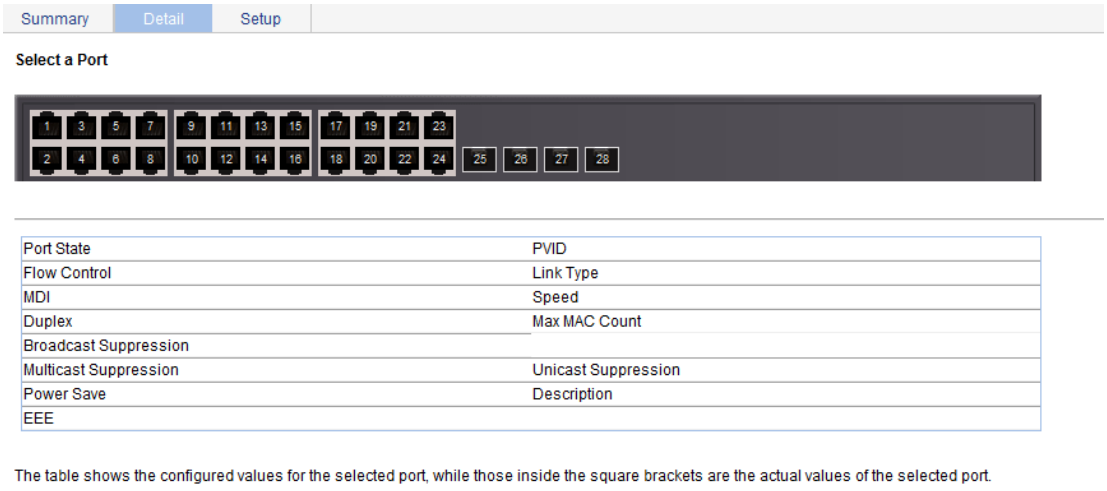


Displaying all the operation parameters for a port

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.

   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 62 The Detail tab



Port management configuration example

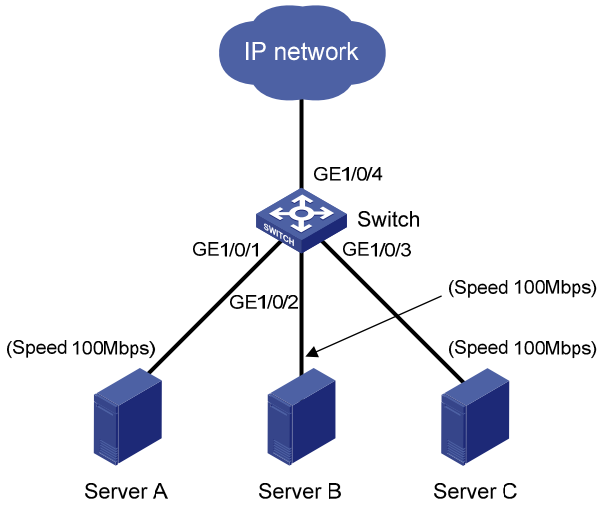
Network requirements

As shown in Figure 63:

- Server A, Server B, and Server C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of 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 speed is 1000 Mbps.

To avoid congestion at the egress port GigabitEthernet 1/0/4, configure the autonegotiation speed range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.

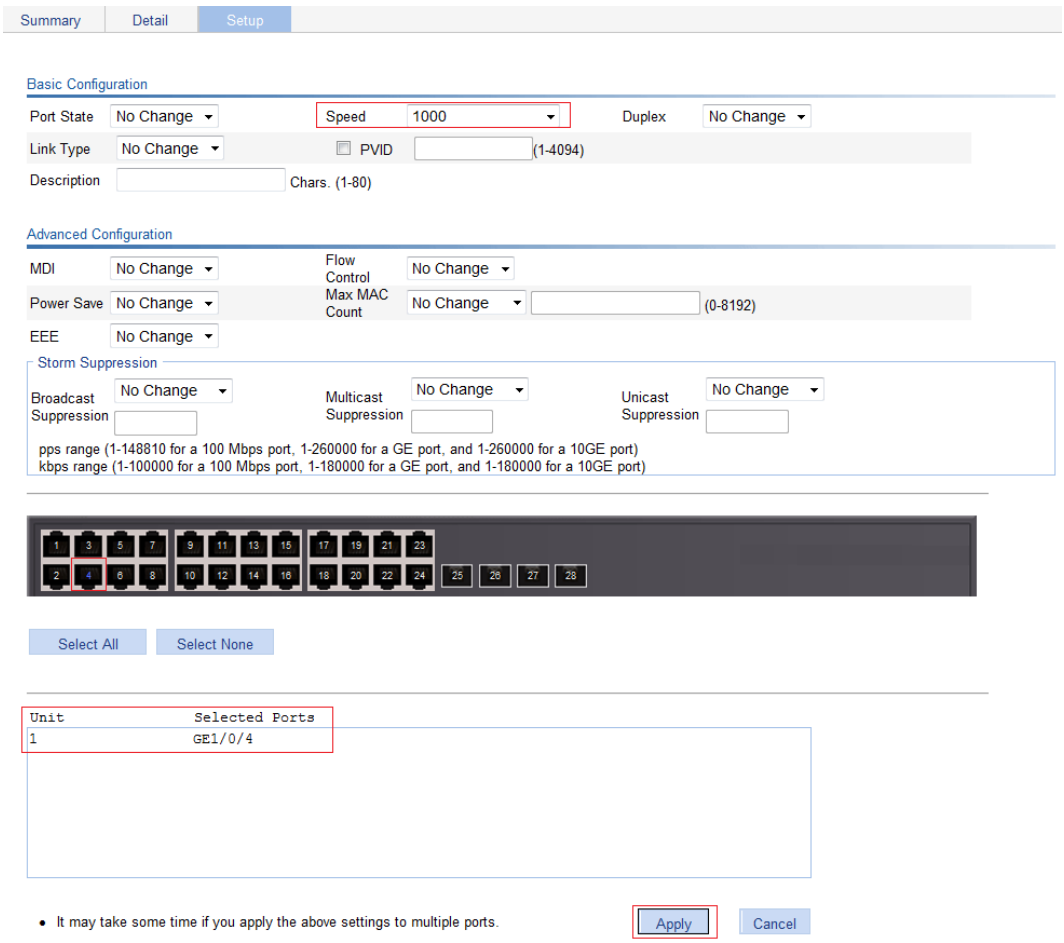
Figure 63 Network diagram



Configuring the switch

1. As shown in Figure 64, set the speed of GigabitEthernet 1/0/4 to 1000 Mbps:

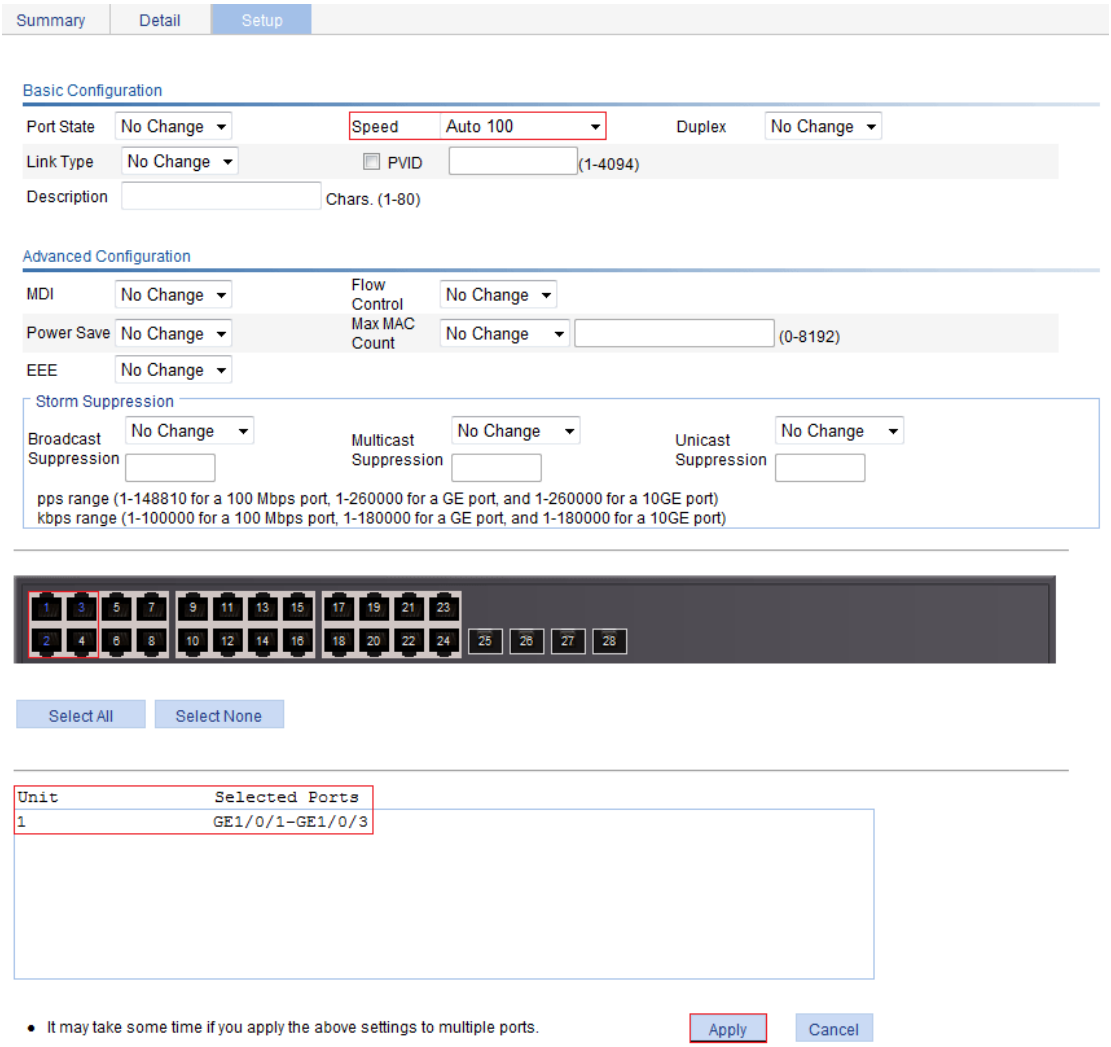
Figure 64 Configuring the speed of GigabitEthernet 1/0/4



2. Batch configure the autonegotiation speed 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.
   b. Select **1**, **2**, and **3** on the chassis front panel.

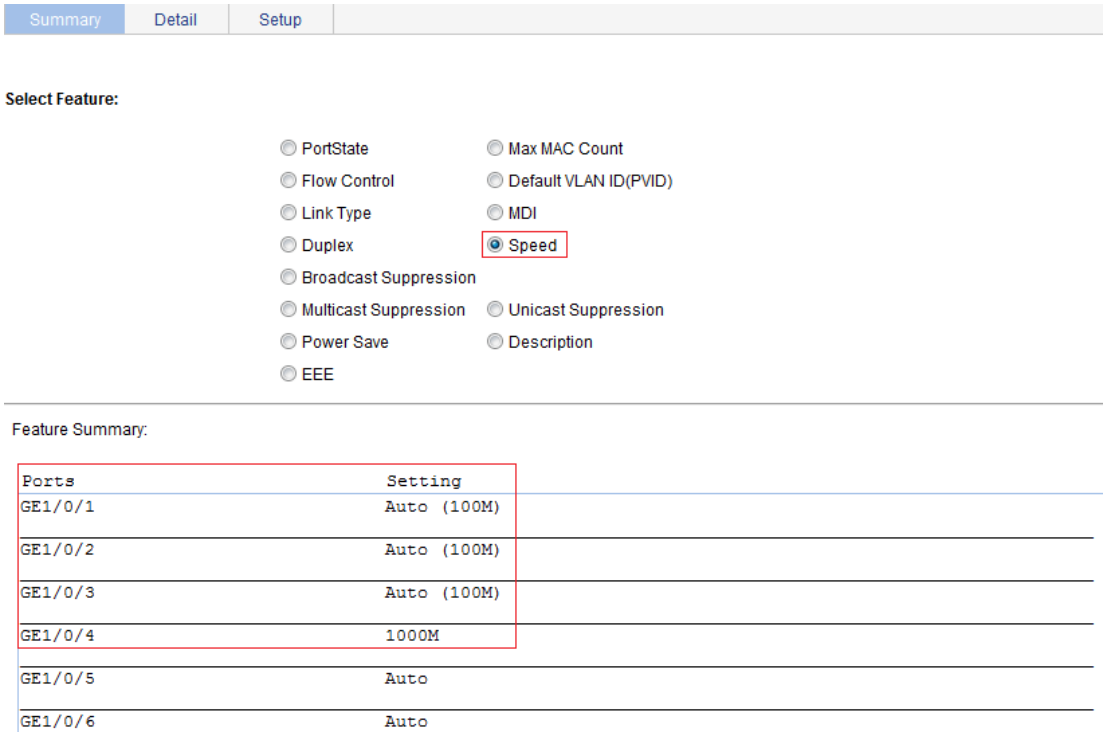
      1, **2**, and **3** represent ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.
   c. Click **Apply**.

Figure 65 Batch configuring the port speed



3. Display the speed settings of ports:
   a. Click the **Summary** tab.
   b. Click the **Speed** button to display the speed information of all ports on the lower part of the page, as shown in Figure 66.

Figure 66 Displaying the speed 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.

Terminology

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 the mirrored packets to its connecting monitoring device.

A monitor port might 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.

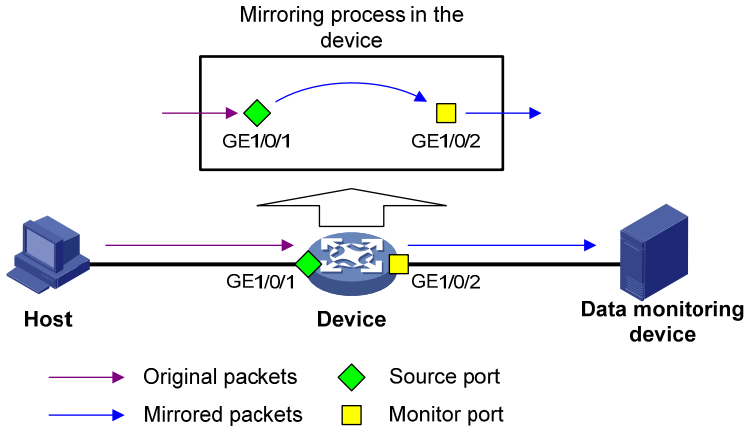
Mirroring group

Port mirroring is implemented through mirroring groups, which include local and remote mirroring groups. Only local mirroring groups are supported.

Local port mirroring

In local port mirroring, 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 device is called a "local mirroring group."

Figure 67 Local port mirroring implementation



As shown in Figure 67, 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.

Configuration restrictions and guidelines

When you configure port mirroring, follow these restrictions and guidelines:

- A local mirroring group can contain multiple source ports, but only one monitor port.
- Do not enable the spanning tree feature on the monitor port.
- Use a monitor port only for port mirroring to make sure the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and other forwarded traffic.

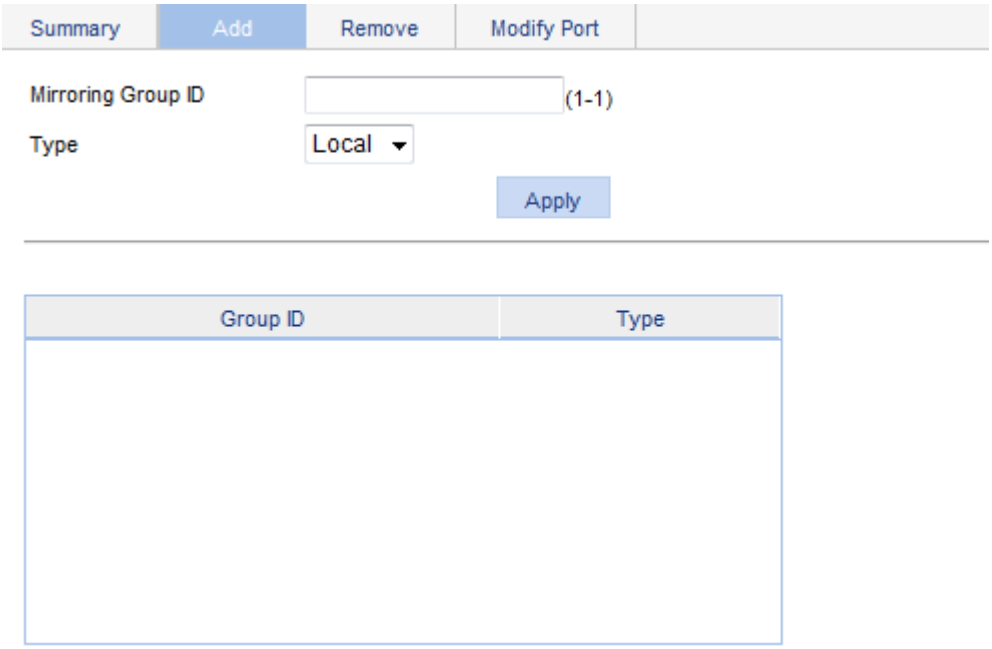
Recommended configuration procedures

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 source ports for the mirroring group.	Required. For more information, see "Configuring ports for the 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 the mirroring group." Select the port type **Monitor Port**.

Configuring a mirroring group

1. From the navigation tree, select **Device** > **Port Mirroring**.
2. Click **Add** to enter the page for adding a mirroring group.

Figure 68 Adding a mirroring group



3. Configure the mirroring group as described in Table 17.
4. Click **Apply**.

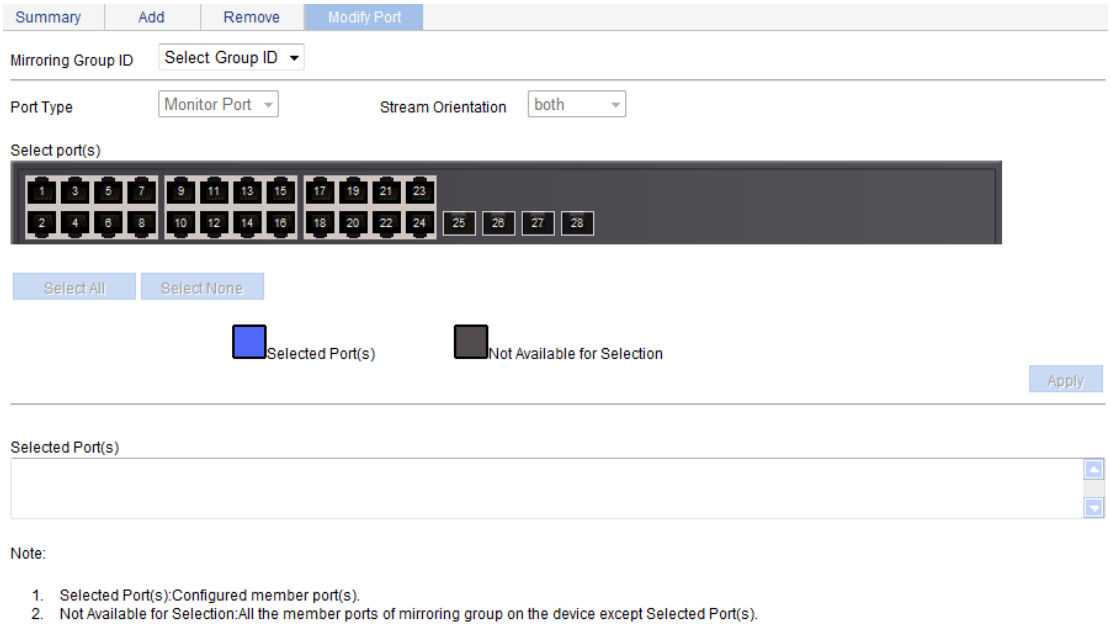
Table 17 Configuration items

Item	Description
Mirroring Group ID	ID of the mirroring group to be added.
Type	Specify the type of the mirroring group to be added as **Local**, which indicates adding a local mirroring group.

Configuring ports for the mirroring group

1. From the navigation tree, select **Device** > **Port Mirroring**.
2. Click **Modify Port** to enter the page for configuring ports for a mirroring group.

Figure 69 Modifying ports



3. Configure ports for the mirroring group as described in Table 18.
4. Click **Apply**.

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

Table 18 Configuration items

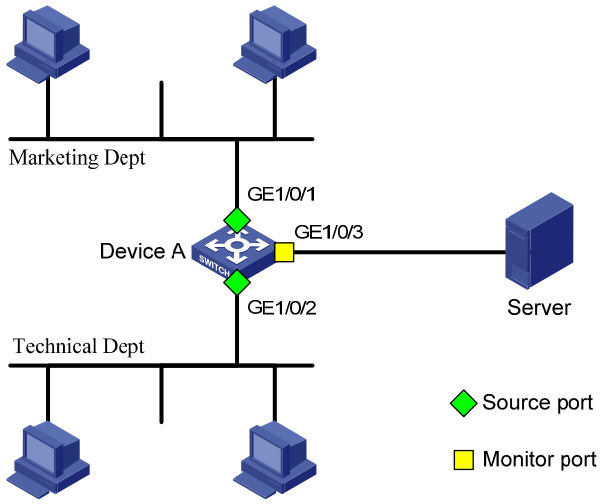
Item	Description
Mirroring Group ID	ID of the mirroring group to be configured. The available groups were added previously. Select a **Local** mirroring group ID to configure ports for the local mirroring group.
Port Type	Configure ports for a local mirroring group: • **Monitor Port**—Configures the monitor ports for the local mirroring group. • **Mirror Port**—Configures mirroring ports for the local mirroring group.
Stream Orientation	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. 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 and configure them as mirroring ports of a port mirroring group.

Local port mirroring configuration example

Network requirements

As shown in Figure 70, configure local port mirroring on Switch A so the server can monitor the packets received and sent by the Marketing department and Technical department.

Figure 70 Network diagram

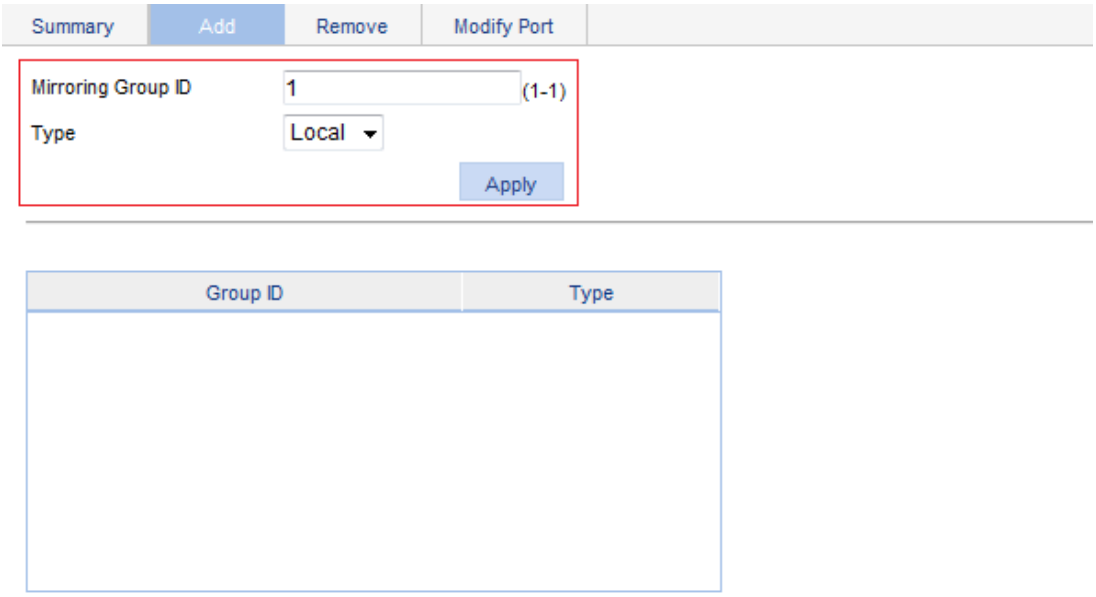


Configuration procedure

Adding a local mirroring group

1. From the navigation tree, select **Device** > **Port Mirroring**.
2. Click **Add** to enter the page for adding mirroring groups as shown in Figure 71.

   Figure 71 Adding a local mirroring group



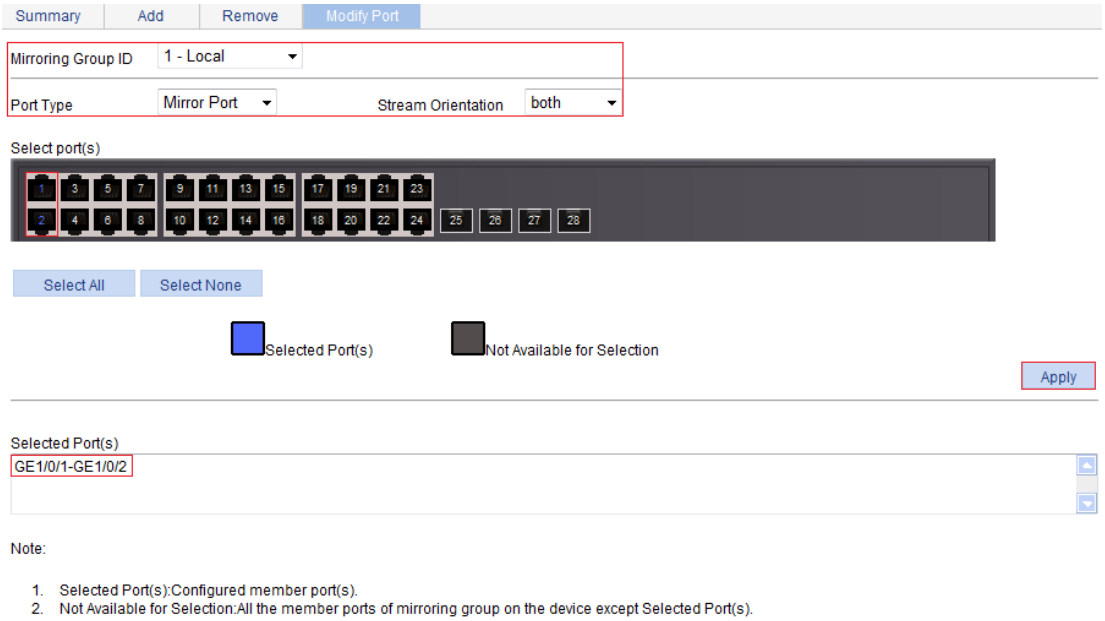
3. Enter **1** for **Mirroring Group ID**, and select **Local** from the **Type** list.
4. Click **Apply**.

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

1. Click **Modify Port**.
2. Select **1 – Local** from the **Mirroring Group ID** list.
3. Select **Mirror Port** from the **Port Type** list.
4. Select **both** from the **Stream Orientation** list.

5. Select **1** (GigabitEthernet 1/0/1) and **2** (GigabitEthernet 1/0/2) on the chassis front panel.

Figure 72 Configuring the source ports



6. Click **Apply**.

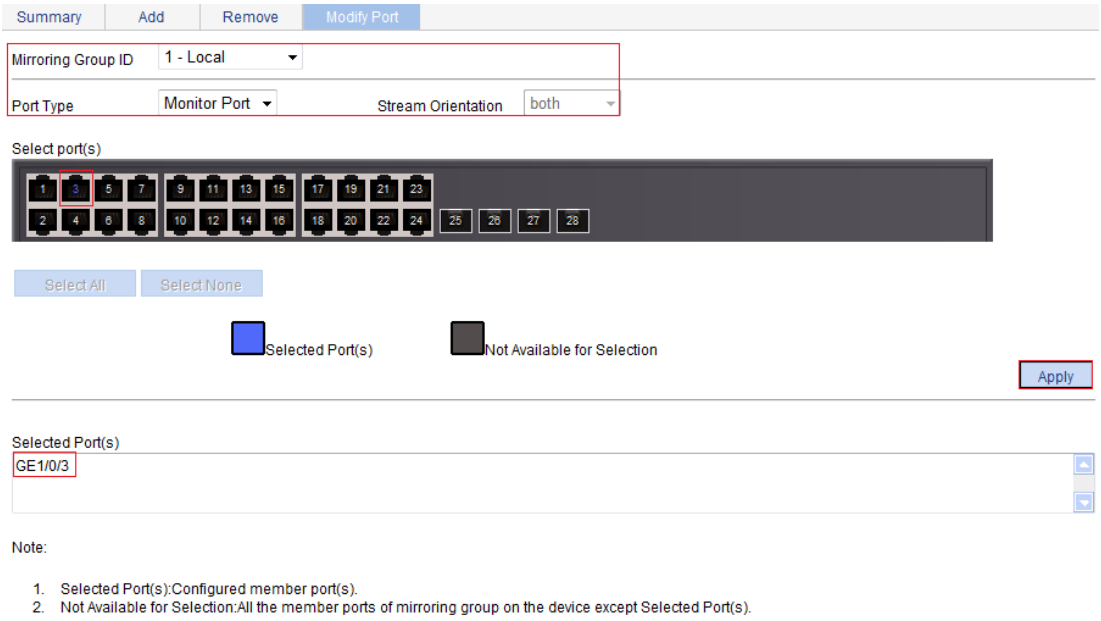
   A configuration progress dialog box appears.

7. After the success notification appears, click **Close**.

Configuring GigabitEthernet 1/0/3 as the monitor port

1. Click **Modify Port**.
2. Select **1 – Local** from the **Mirroring Group ID** list.
3. Select **Monitor Port** from the **Port Type** list.
4. Select **3** (GigabitEthernet 1/0/3) on the chassis front panel.

Figure 73 Configuring the monitor port



5. Click **Apply**.
   A configuration progress dialog box appears.
6. After the success notification appears, click Close.

Managing users

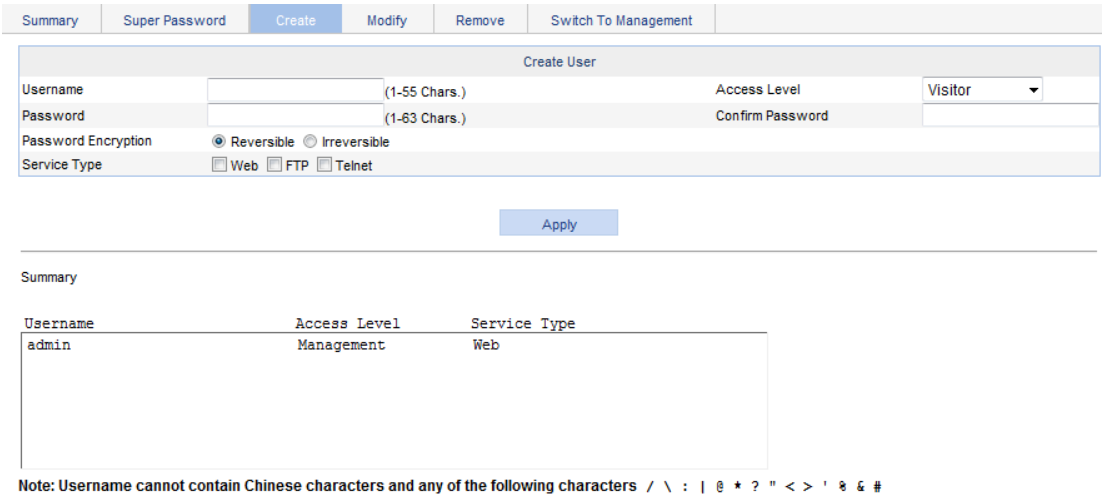
The user management function allows you to do the following:

- Adding a local user, and specifying the password, access level, and service types for the user.
- Setting the super password for non-management level users to switch to the management level.
- Switching 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 74 Adding a local user



3. Configure a local user as described in Table 19.
4. Click **Apply**.

Table 19 Configuration items

Item	Description
Username	Enter 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**—A visitor level user can perform only ping and traceroute operations. They cannot access the data on the device or configure the device. • **Monitor**—A monitor level user can perform ping and traceroute operations and access the data on the device, but they cannot configure the device. • **Configure**—A configure level user can perform ping and traceroute operations, access data on the device, and configure the device, but they cannot upgrade the software, add/delete/modify users, or back up or restore the configuration file. • **Management**—A management level user can perform any operations on the device.
Password	Set the password for the user.

Item	Description
Confirm Password	Enter the same password again.
Password Encryption	Select the password encryption type: • **Reversible**—Uses a reversible encryption algorithm. The ciphertext password can be decrypted to get the plaintext password. • **Irreversible**—Uses an irreversible encryption algorithm. The ciphertext password cannot be decrypted to get the plaintext password.
Service Type	Select the service types for the user to use, including Web, FTP, and Telnet. You must select at least one service type.

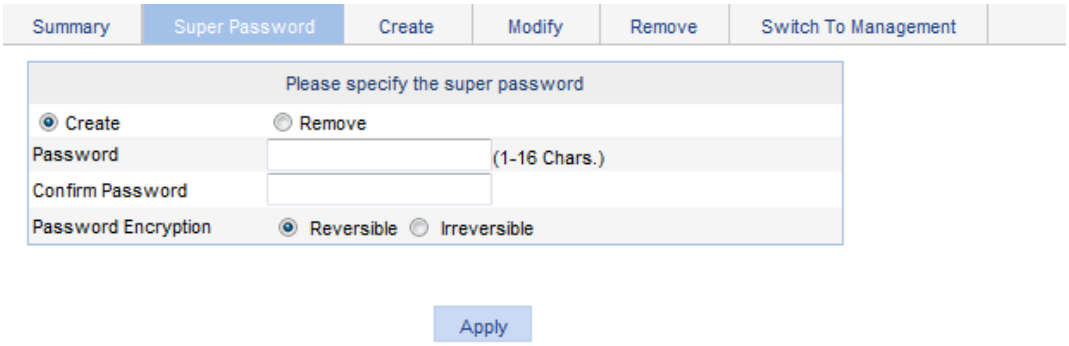
Setting the super password

A management level user can set the password for non-management level users to switch to the management level. If the password is not set, non-management level users cannot switch to the management level from a lower level.

To set the super password:

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

Figure 75 Setting the super password



3. Configure a super password as described in Table 20.
4. Click **Apply**.

Table 20 Configuration items

Item	Description
Create/Remove	Select the operation type: • **Create**—Configure or change 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.

Item	Description
Password Encryption	Select the password encryption type: • **Reversible**—Uses a reversible encryption algorithm. The ciphertext password can be decrypted to get the plaintext password. • **Irreversible**—Uses an irreversible encryption algorithm. The ciphertext password cannot be decrypted to get the plaintext password.

Switching to the management level

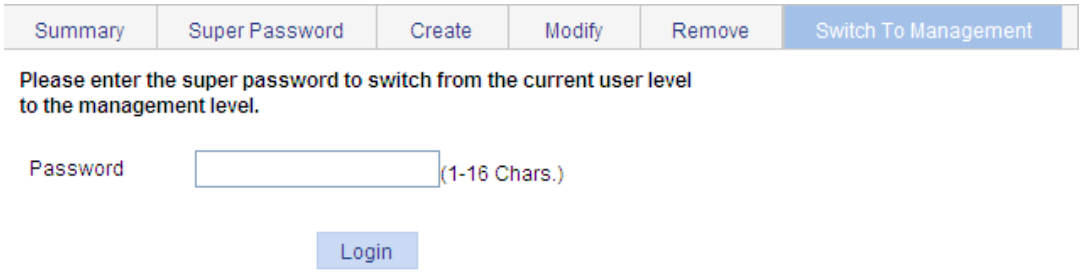
A non-management level user can switch to the management level after providing the correct super password.

The level switching operation does not change the access level setting for the user. When the user logs in to the Web interface again, the access level of the user is still the level set for the user.

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 76 Switching to the management level



Configuring a loopback test

You can check whether an Ethernet port operates correctly by performing Ethernet port loopback test. During the test time, the port cannot forward data packets correctly.

Ethernet port loopback test has the following types:

- **Internal loopback test**—Establishes self loop in the switching chip and checks whether there is a chip failure related to the functions of the port.
- **External loopback test**—Uses a loopback plug 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.

Configuration guidelines

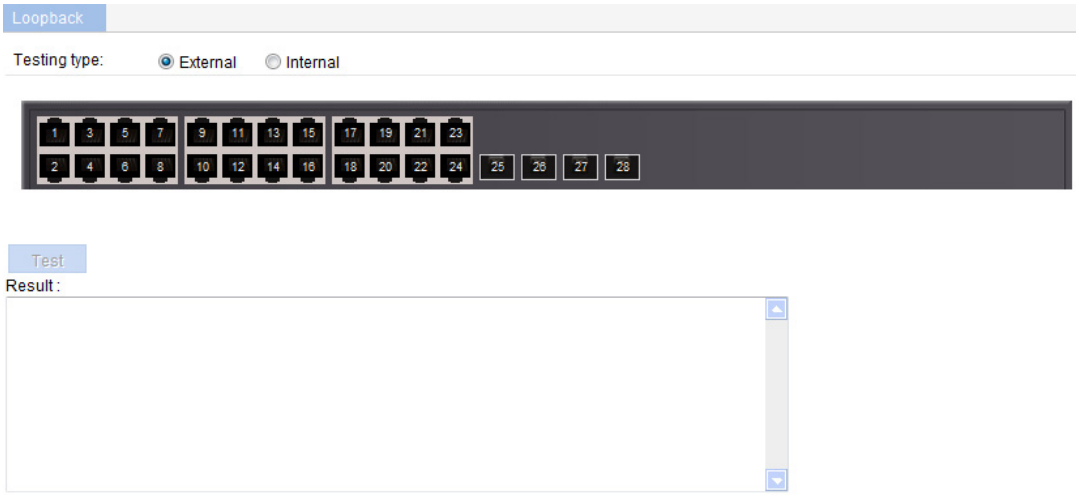
When you configure a loopback test, follow these restrictions and guidelines:

- When a port is physically down, you cannot perform an external loopback test on the port.
- After a port is shut down manually, you can perform neither internal nor external test on the port.
- When a port is under loopback test, you cannot apply **Rate**, **Duplex**, **Cable Type**, and **Port Status** configuration to the port.
- An Ethernet port operates in full duplex mode when a loopback test is performed. It restores its original duplex mode after the loopback test is finished.

Configuration procedure

1. From the navigation tree, select **Device** > **Loopback**.

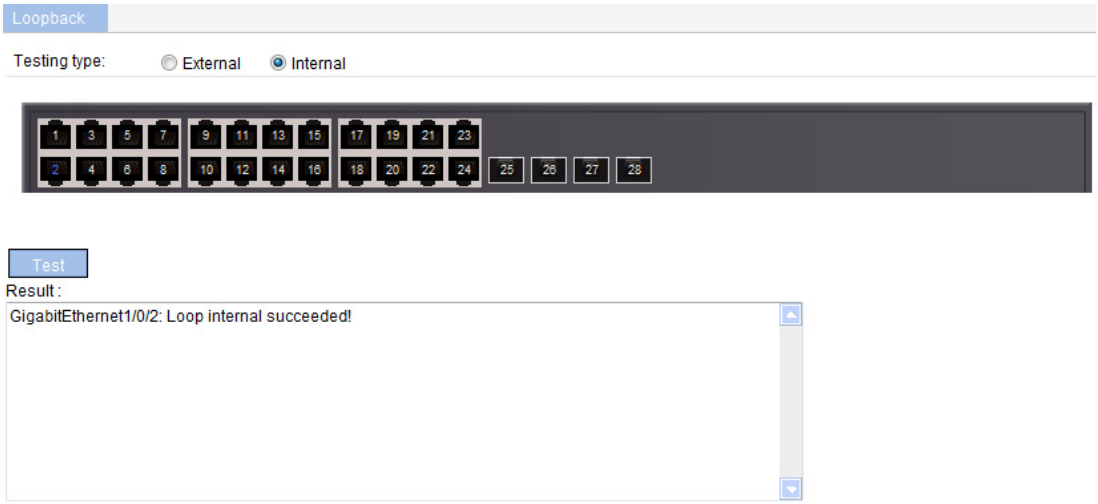
   Figure 77 Loopback test page

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, the system displays the loopback test result.

Figure 78 Loopback test result



Configuring VCT

Overview

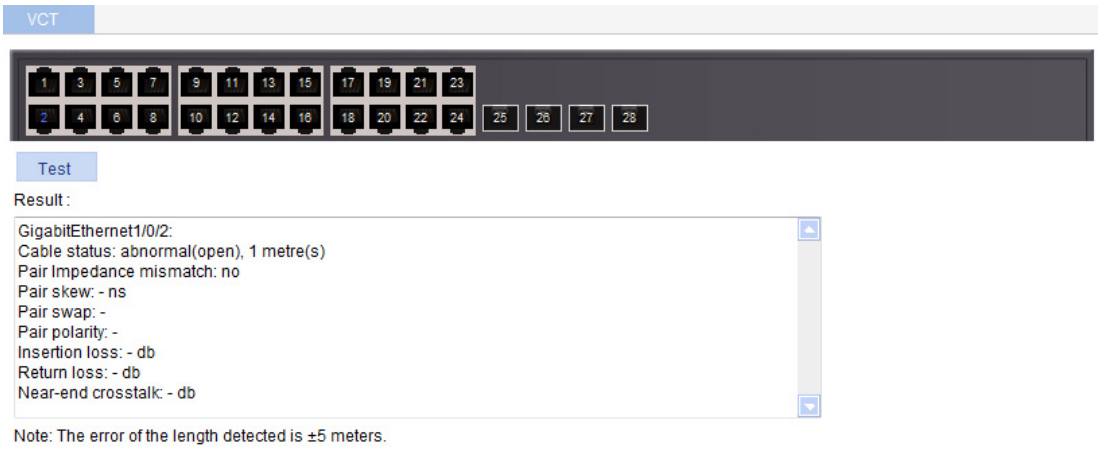
You can use the Virtual Cable Test (VCT) function to check the status of the cable connected to an Ethernet port on the device. The result is returned in less than 5 seconds. The test covers whether short circuit or open circuit occurs on the cable and the length of the faulty cable.

The fiber port does not support this feature.

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 5 seconds and displayed in the **Result** field.

Figure 79 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

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

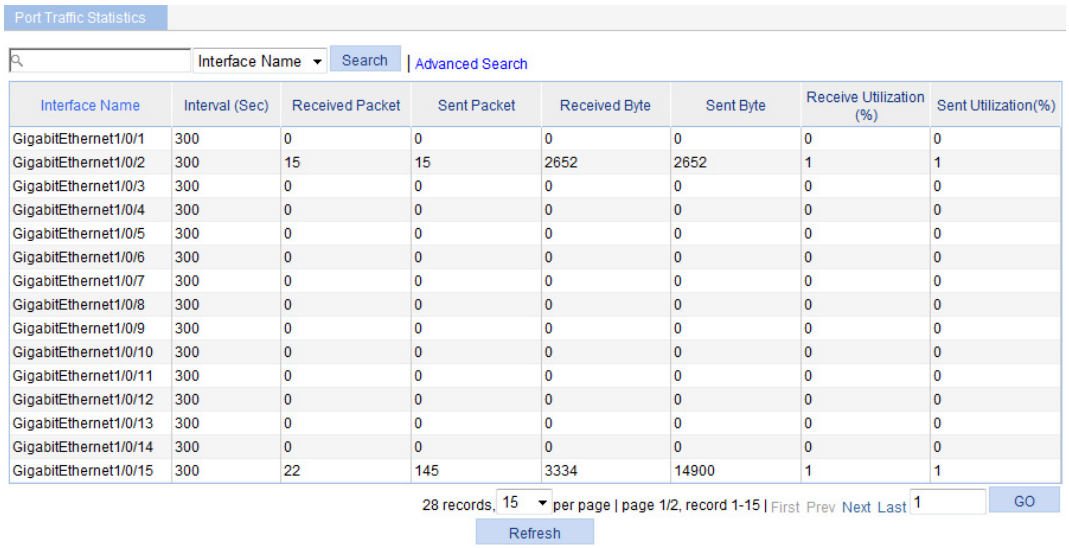
Viewing port traffic statistics

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 and received by each port, and the bandwidth use of each port over the last interval.

   Figure 80 Port traffic statistics



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

Configuring RMON

Overview

Remote Network Monitoring (RMON) is an enhancement to SNMP. It enables proactive remote monitoring and management of network devices and subnets. An RMON monitor periodically or continuously collects traffic statistics for the network attached to a port on the managed device. The managed device can automatically send a notification when a statistic crosses an alarm threshold, so the NMS does not need to constantly poll MIB variables and compare the results.

RMON uses SNMP notifications to notify NMSs of various alarm conditions such as broadcast traffic threshold exceeded. In contrast, SNMP reports function and interface operating status changes such as link up, link down, and module failure.

HPE devices provide an embedded RMON agent as the RMON monitor. An NMS can perform basic SNMP operations to access the RMON MIB.

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. NMSs can obtain all RMON MIB information by using this method.
- **RMON agents embedded in network devices**—NMSs exchange data with RMON agents by using basic SNMP operations to gather network management information. Because this method is resource intensive, most RMON agent implementations provide only four groups of MIB information: alarm, event, history, and statistics.

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, Hewlett Packard Enterprise implements the statistics group, history group, event group, and alarm group supported by the public MIB. Hewlett Packard Enterprise also implements a private alarm group, which enhances the standard alarm group.

Ethernet statistics group

The statistics group defines that the system collects various traffic statistics on an interface (only Ethernet interfaces are supported), and saves the statistics in the Ethernet statistics table (ethernetStatsTable) for future retrieval. The interface traffic statistics include network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received.

After you create a statistics entry for an interface, the statistics group starts to collect traffic statistics on the interface. The statistics in the Ethernet statistics table are cumulative sums.

History group

The history group defines that the system periodically collects traffic statistics on interfaces and saves the statistics in the history record table (ethernetHistoryTable). The statistics include bandwidth utilization, number of error packets, and total number of packets.

The history statistics table record traffic statistics collected for each sampling interval. The sampling interval is user-configurable.

Event group

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

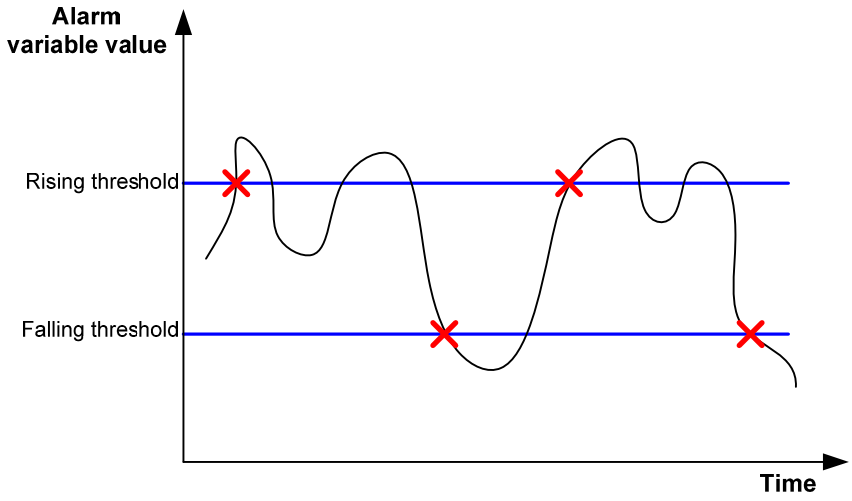
- **Log**—Logs event information (including event time and description) in the event log table so the management device can get the logs through SNMP.
- **Trap**—Sends an SNMP notification when the event occurs.
- **Log-Trap**—Logs event information in the event log table and sends an SNMP notification when the event occurs.
- **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. If the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered. If 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 81.

Figure 81 Rising and falling alarm events



RMON configuration task list

Configuring the RMON statistics function

The RMON statistics function can be implemented by either the Ethernet statistics group or the history group, but the objects of the statistics are different, as follows:

- A statistics object of the Ethernet 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 21 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 22 to configure RMON history statistics function.

Table 21 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 you create a statistics entry 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:** You can create only one statistics entry on one interface.

Table 22 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. It 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

To send traps to the NMS when an alarm is triggered, configure the SNMP agent as described in "Configuring SNMP" before configuring the RMON alarm function.

Perform the tasks in Table 23 to configure RMON alarm function.

Table 23 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, configure the RMON Ethernet statistics function or the RMON history statistics function on the monitored Ethernet interface. After you create a statistics entry 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:** You can create only one statistics entry for one interface.

Task	Remarks
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 takes, 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:** You cannot create an entry 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 is triggered when an abnormity occurs. The alarm event defines how to deal with the abnormity. **IMPORTANT:** You cannot create an entry 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 24.

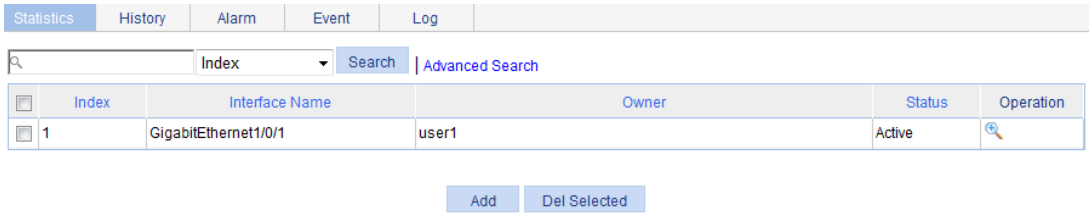
Table 24 Displaying RMON running status

Task	Remarks
Displaying RMON statistics	Display 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 create 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 display the entries in this table. When you configure the history group, the system specifies the number of history sampling records that can be displayed and the history sampling interval.
Displaying RMON event logs	If you configure the system to log an event after the event is triggered when you configure the event group, the event is recorded in the RMON log. Perform this task to display the details of the log table.

Configuring a statistics entry

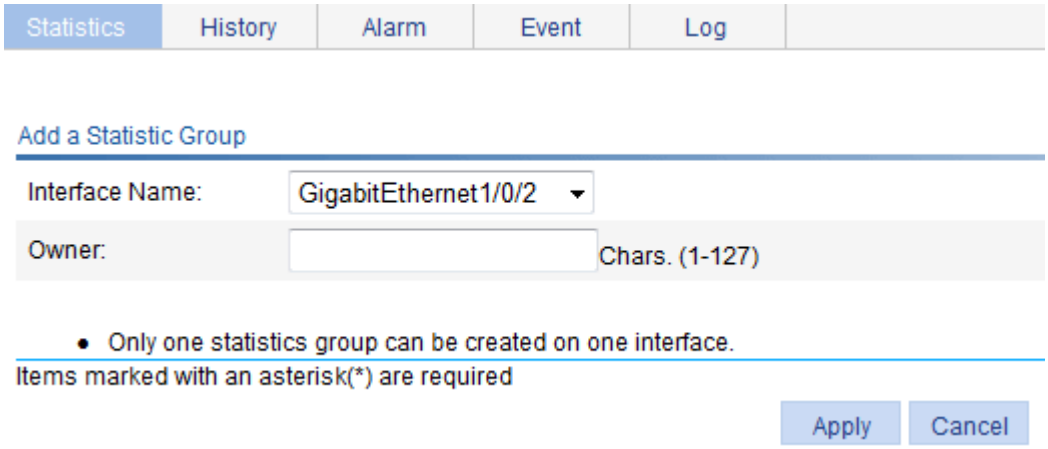
1. Select **Device** > **RMON** from the navigation tree.
   The **Statistics** tab page appears.

   Figure 82 Statistics entry



2. Click **Add**.

Figure 83 Adding a statistics entry



3. Configure a statistic entry as described in Table 25.
4. Click **Apply**.

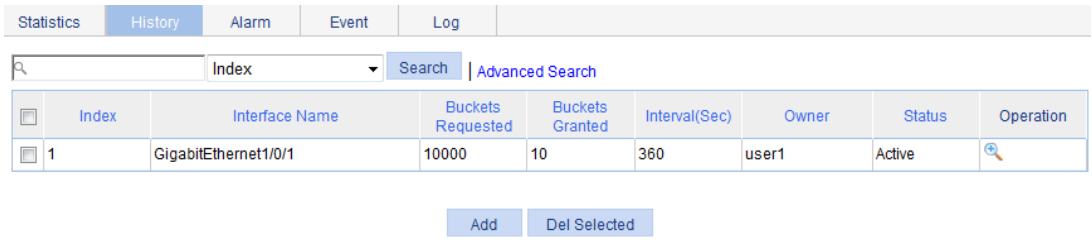
Table 25 Configuration items

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

Configuring a history entry

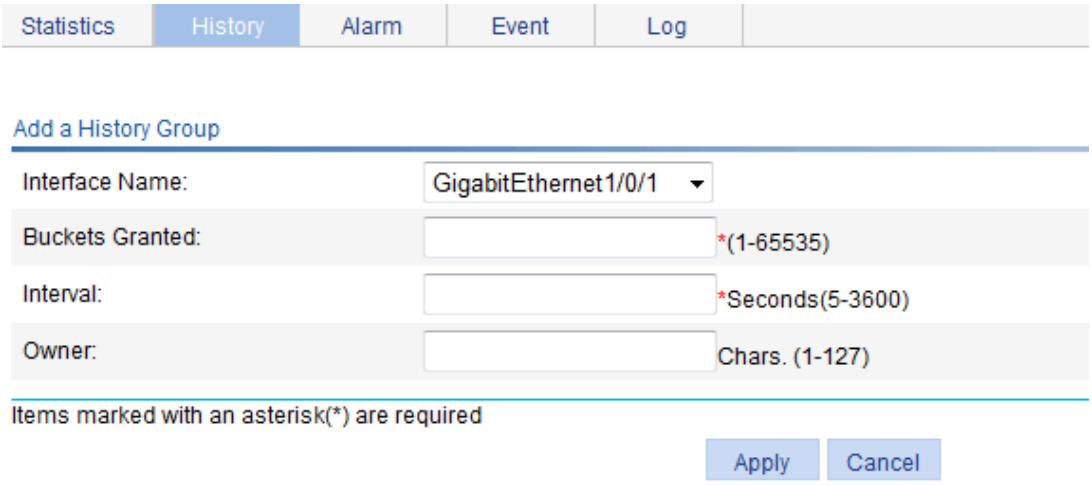
1. Select **Device** > **RMON** from the navigation tree.
2. Click the **History** tab.

Figure 84 History entry



3. Click **Add**.

Figure 85 Adding a history entry



4. Configure a history entry as described in Table 26.
5. Click **Apply**.

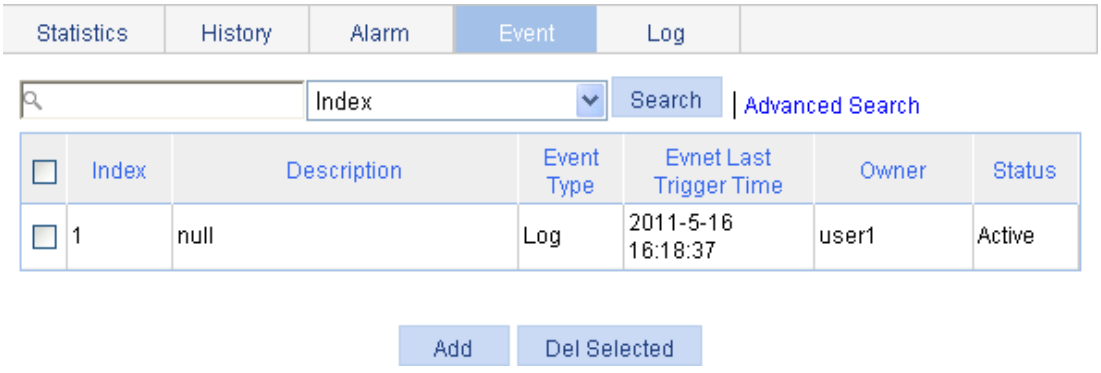
Table 26 Configuration items

Item	Description
Interface Name	Select the name of the interface on which the history entry is created.
Buckets Granted	Set the capacity of the history record list corresponding to this history entry (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 deletes 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, and total number of multicast packets in a sampling period.
Interval	Set the sampling period.
Owner	Set the owner of the entry.

Configuring an event entry

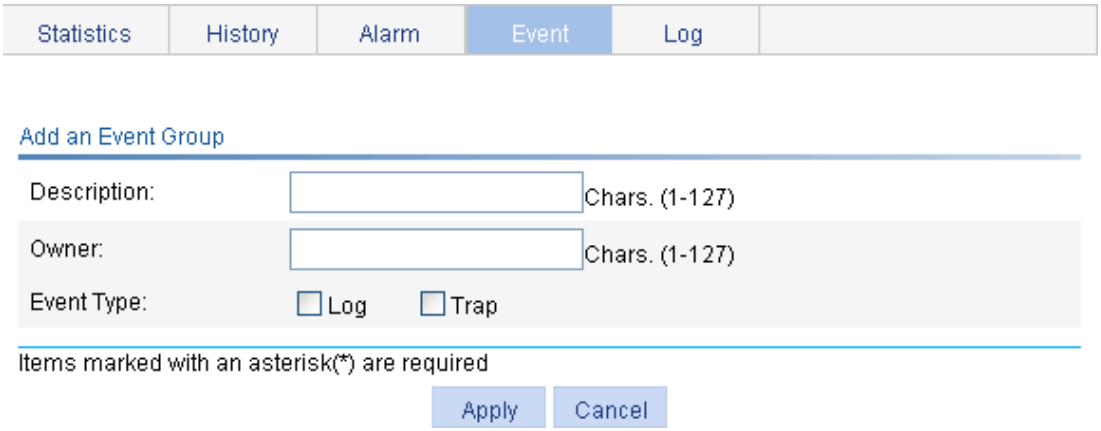
1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Event** tab.

Figure 86 Event entry



3. Click **Add**.

Figure 87 Adding an event entry



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

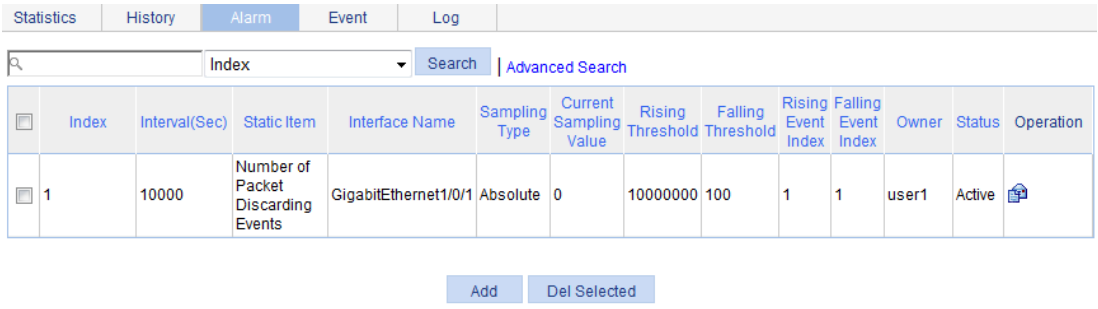
Table 27 Configuration items

Item	Description
Description	Set the description for the event.
Owner	Set the entry owner.
Event Type	Set the actions that the system takes when the event is triggered: • **Log**—The system logs the event. • **Trap**—The system sends a trap in the community name of **null**. If you select both **Log** and **Trap**, the system logs the event and sends a trap. If neither is selected, the system takes no action.

Configuring an alarm entry

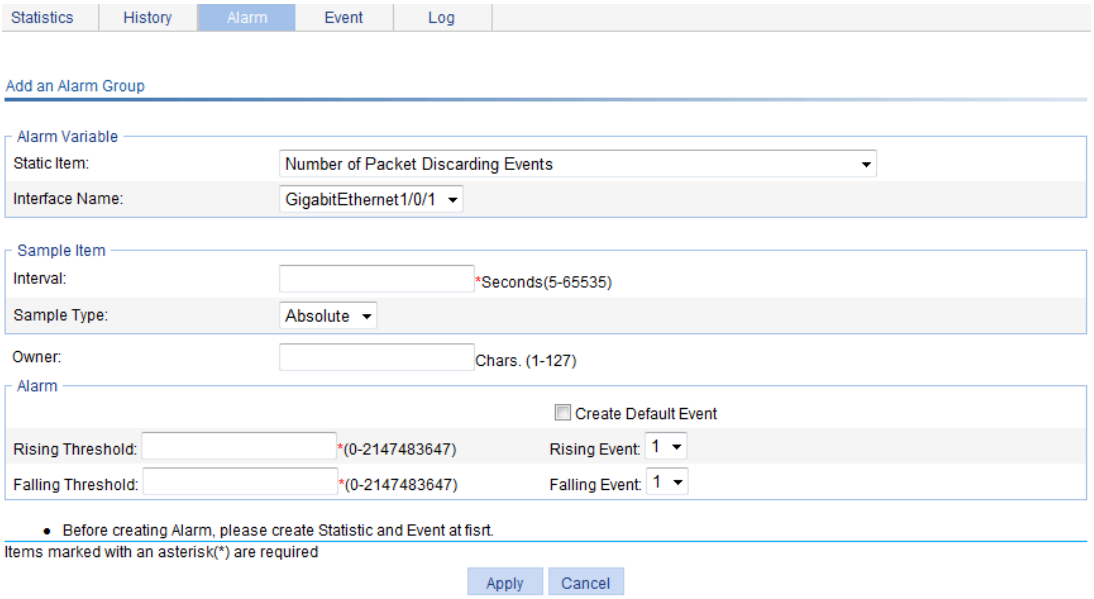
1. Select **Device** > **RMON** from the navigation tree.
2. Click the **Alarm** tab.

Figure 88 Alarm entry



3. Click **Add**.

Figure 89 Adding an alarm entry



4. Configure an alarm entry as described in Table 28.
5. Click **Apply**.

Table 28 Configuration items

Item	Description
Alarm variable:	
Static Item	Set the traffic statistics that are collected and monitored. For more information, see Table 29.
Interface Name	Set the name of the interface whose traffic statistics are collected and monitored.
Sample Item:	
Interval	Set the sampling interval.
Sample Type	Set the sampling type: • **Absolute**—Absolute sampling to obtain the value of the variable when the sampling time is reached. • **Delta**—Delta sampling to obtain the variation value of the variable during the sampling interval when the sampling time is reached.
Owner:	Set the owner of the alarm entry.
Alarm:	
Create Default Event	Select whether to create a default event. The description of the default event is **default event**, the action is **log-and-trap**, and the owner is **default owner**. If there is no event, you can 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 adopts the default action **log-and-trap**.
Rising Threshold	Set the alarm rising threshold.

Item	Description
Rising Event	Set the action that the system takes when the value of the alarm variable is higher than the alarm rising threshold. If you select the **Create Default Event** box, this option is not configurable.
Falling Threshold	Set the alarm falling threshold.
Falling Event	Set the action that the system takes when the value of the alarm variable is lower than the alarm falling threshold. If you select the **Create Default Event** box, this option is not configurable.

Displaying RMON statistics

1. Select **Device** > **RMON** from the navigation tree.
   The page in Figure 82 appears.
2. Click the icon for the statistics entry of an interface.

Figure 90 RMON statistics

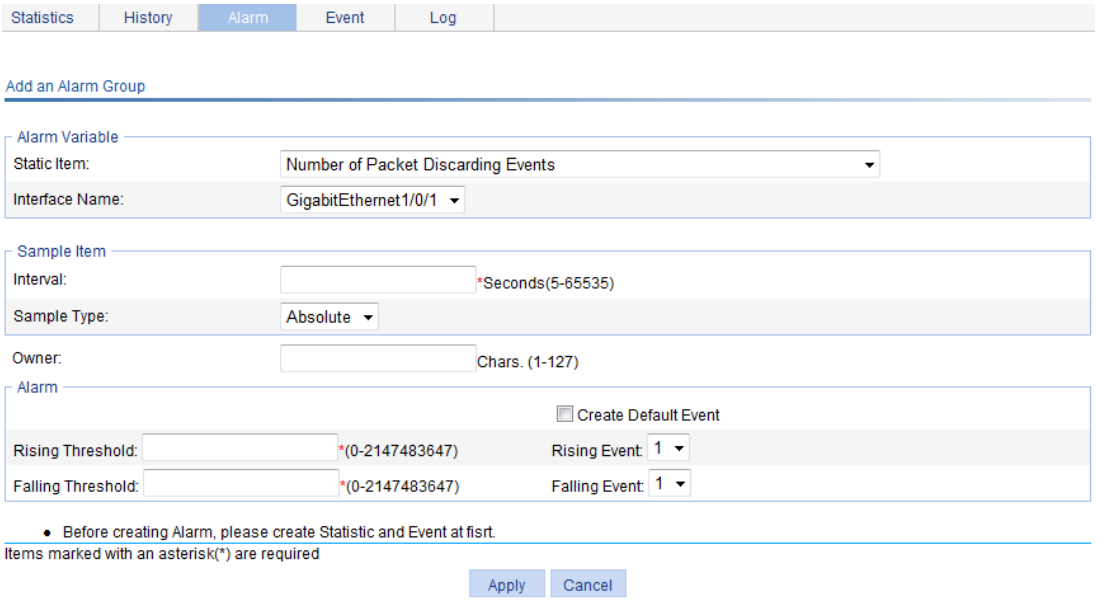


Table 29 Field description

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.

Field	Description
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.
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.
3. Click the  icon for a history entry.

Figure 91 RMON history sampling information

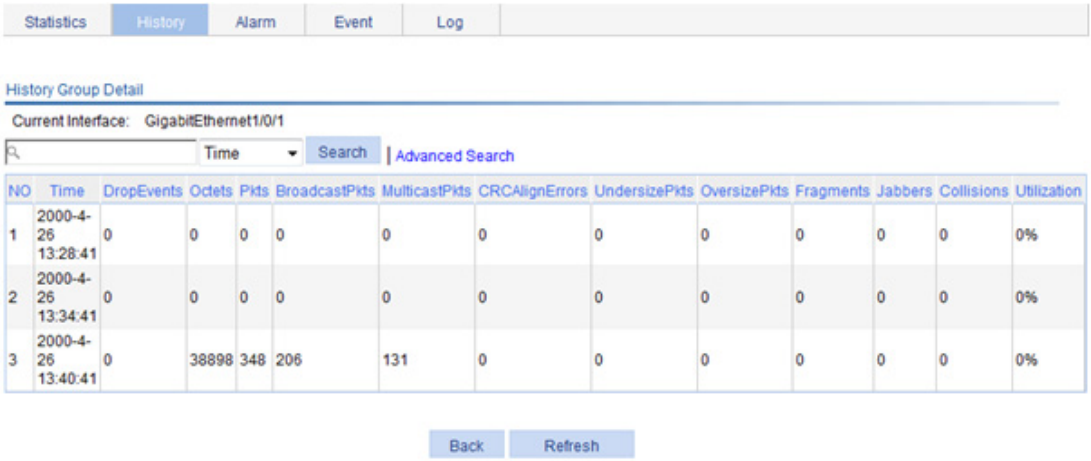


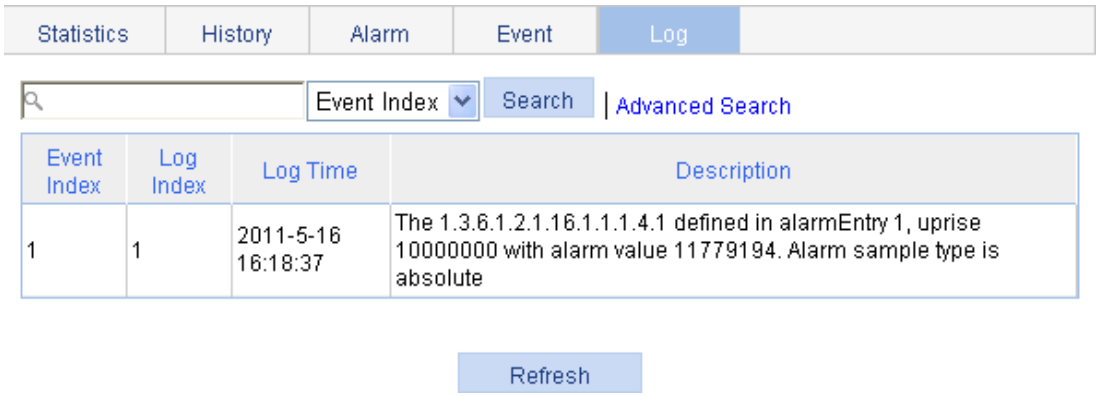
Table 30 Field description

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.
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, corresponding to the MIB node etherHistoryJabbers. Support for the field depends on the device model.
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.

Figure 92 Log tab



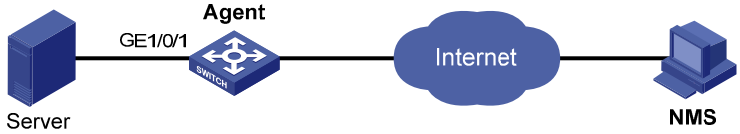
In this example, event 1 has generated one log, which is triggered because the alarm value (11779194) exceeds the rising threshold (10000000). The sampling type is absolute.

RMON configuration example

Network requirements

As shown in Figure 93, create an entry in the RMON Ethernet statistics table to gather statistics on GigabitEthernet 1/0/1 with the sampling interval being 10 seconds. Perform corresponding configurations so that the system logs the event when the number of bytes received on the interface more than 1000 or less than 100.

Figure 93 Network diagram



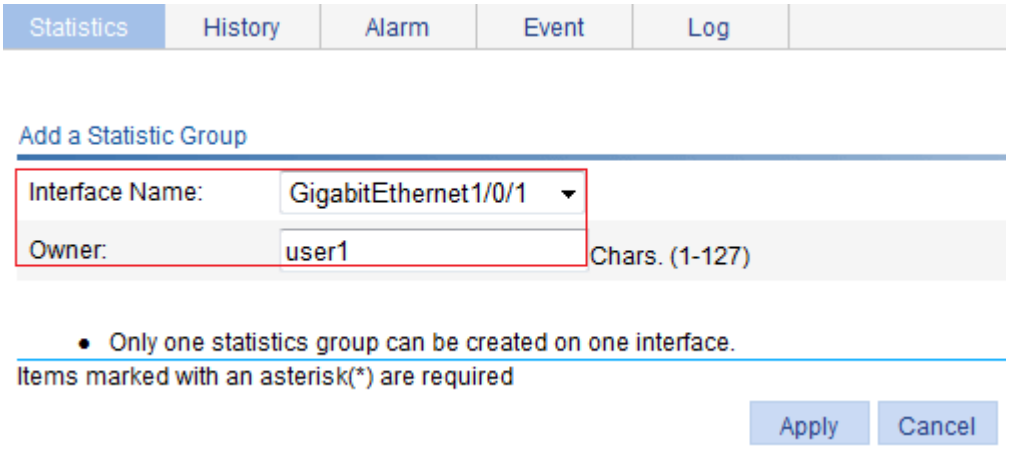
Configuration procedure

1. Configure RMON to gather statistics for GigabitEthernet 1/0/1:
   a. Select **Device** > **RMON** from the navigation tree.

      The **Statistics** tab page appears.
   b. Click **Add**.

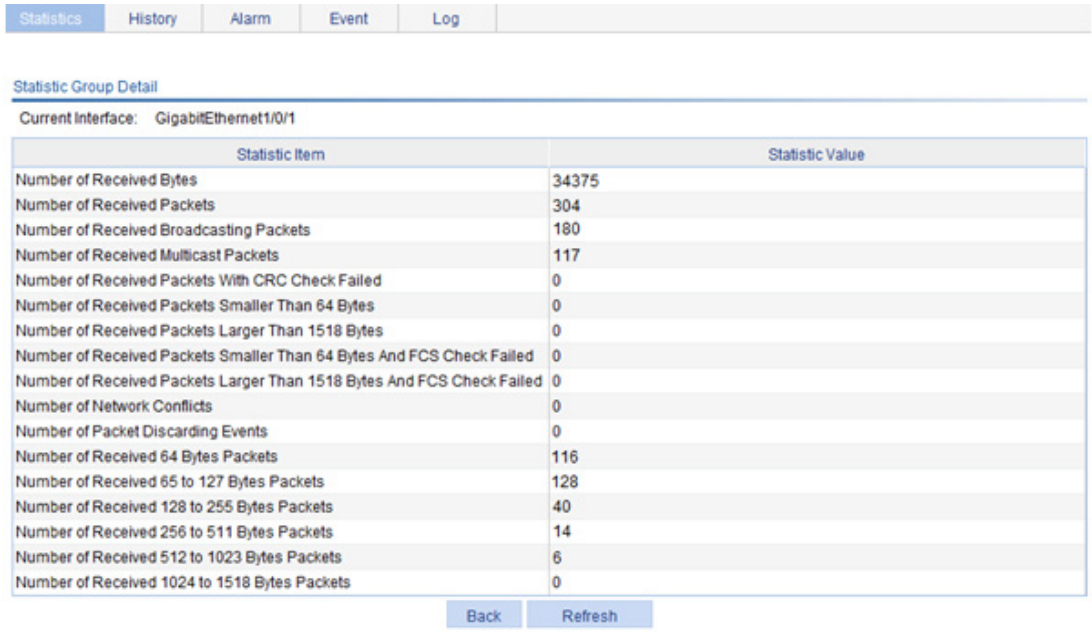
      The page in Figure 94 appears.
   c. Select **GigabitEthernet1/0/1** from the **Interface Name** list, type **user1** in the **Owner** field, and click **Apply**.

Figure 94 Adding a statistics entry



2. Display RMON statistics for GigabitEthernet 1/0/1:
   a. Click the icon corresponding to GigabitEthernet 1/0/1.
   b. Display this information as shown in Figure 95.

Figure 95 Displaying RMON statistics



3. Create an event to start logging after the event is triggered:
   a. Click the **Event** tab.
   b. Click **Add**.

      The page in Figure 96 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 97.

Figure 96 Configuring an event group

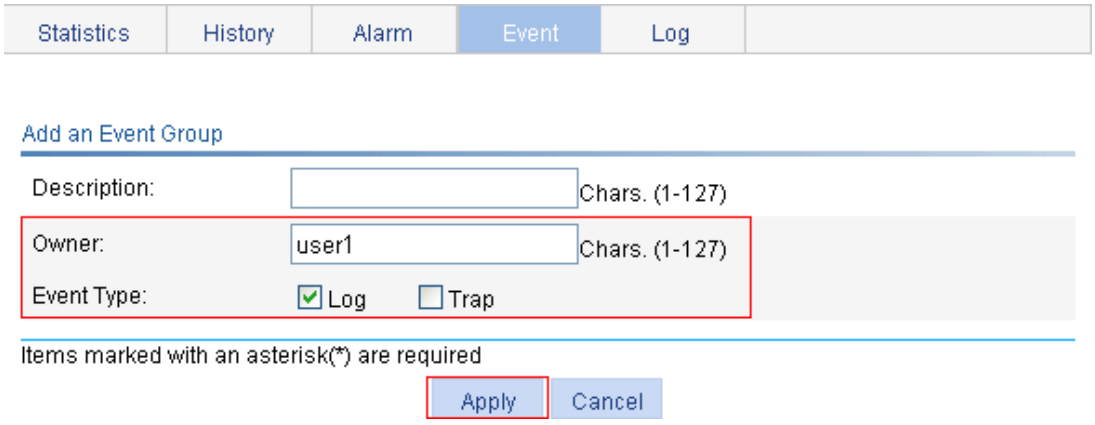
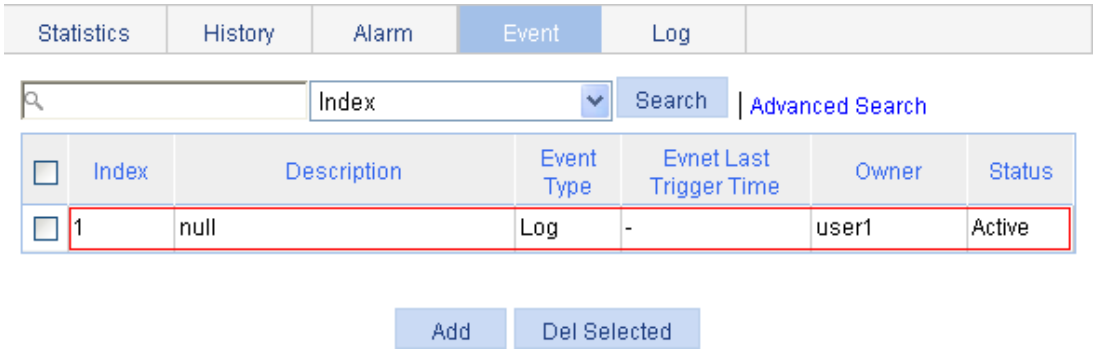


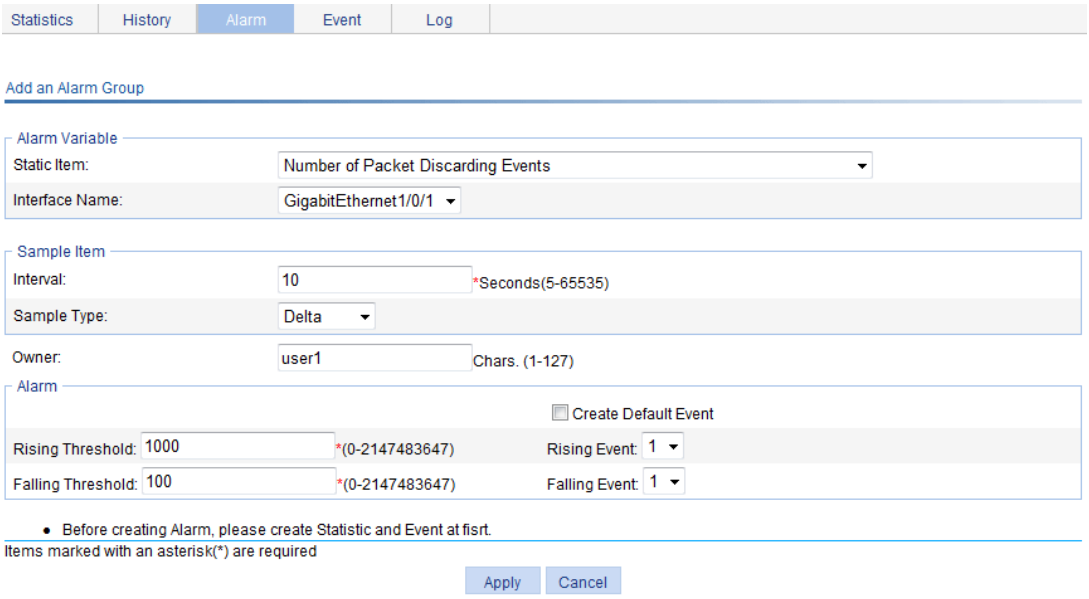
Figure 97 Displaying the index of an event entry



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 98 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 98 Configuring an alarm group



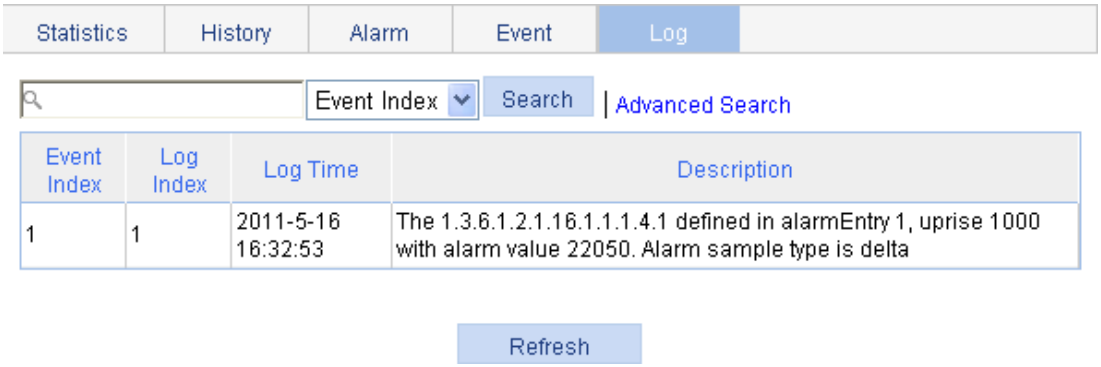
Verifying the configuration

After the above configuration, when the alarm event is triggered, you can display log information for event 1 on the Web interface.

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

   The log page appears. The log in this example indicates that event 1 generated one log, which was triggered because the alarm value (22050) exceeded the rising threshold (1000). The sampling type is absolute.

Figure 99 Log information for event 1



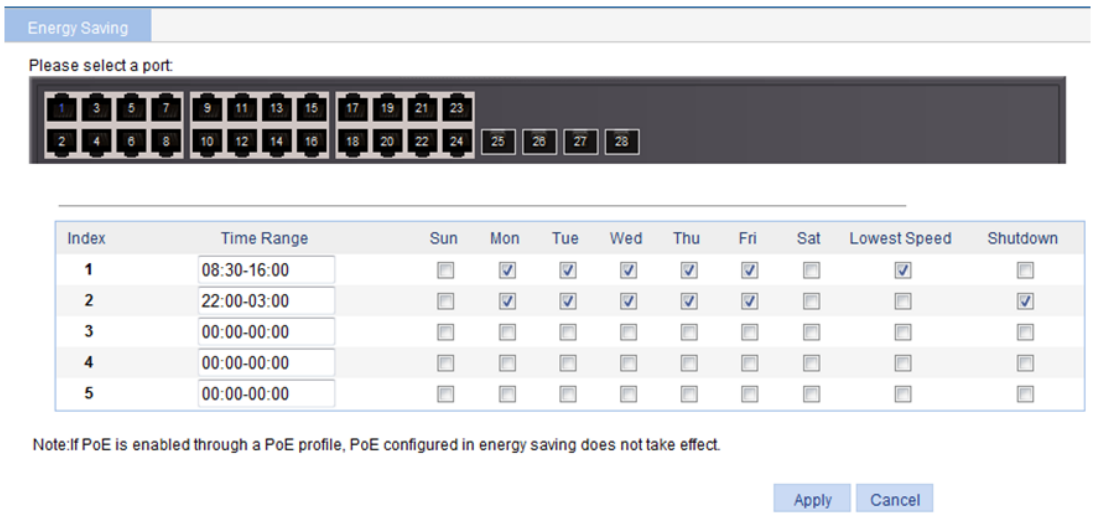
Configuring energy saving

Energy saving enables a port to operate at the lowest transmission speed, disable PoE, or go down during a specific time range on certain days of a week. The port resumes 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 100 Energy saving configuration page



3. Configure an energy saving policy for the port as described in Table 31.
4. Click **Apply**.

Table 31 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.
Lowest Speed	Set the port to transmit data at the lowest speed. 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. An energy saving policy can have all the three energy saving schemes configured, of which the shutdown scheme takes the highest priority.

Configuring SNMP

This chapter provides an overview of the Simple Network Management Protocol (SNMP) and guides you through the configuration procedure.

Overview

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.

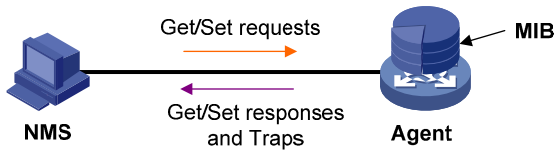
SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

SNMP mechanism

The SNMP framework comprises the following elements:

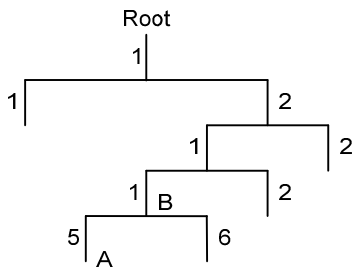
- **SNMP manager**—Works on an NMS to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and send traps to the NMS when some events, such as interface state change, occur.
- **Management Information Base (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 101 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, the object B in Figure 102 is uniquely identified by the OID {1.2.1.1}.

Figure 102 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

Hewlett Packard Enterprise 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 ways. Their configuration procedures are described in separate sections.

Table 32 SNMPv1 or SNMPv2c configuration task list

Task	Remarks
1. Enabling SNMP agent	Required. The SNMP agent function is disabled by default. **IMPORTANT:** If SNMP agent is disabled, all SNMP agent-related configurations are 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 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.

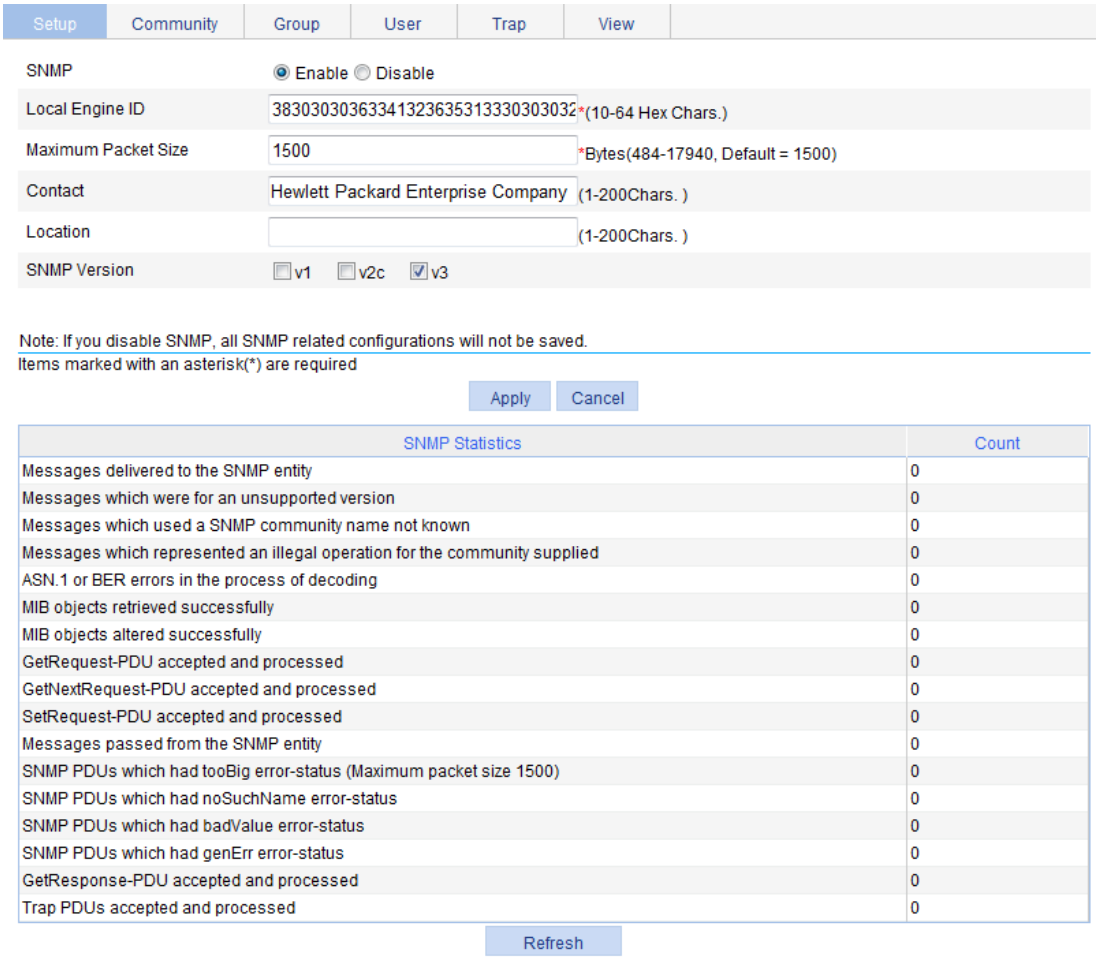
Table 33 SNMPv3 configuration task list

Task	Remarks
1. Enabling SNMP agent	Required. The SNMP agent function is disabled by default. **IMPORTANT:** If SNMP agent is disabled, all SNMP agent-related configurations are 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 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 103 Setup tab



2. Configure SNMP settings on the upper part of the page as described in Table 34.
3. Click **Apply**.

Table 34 Configuration items

Item	Description
SNMP	Specify to enable or disable SNMP agent.
Local Engine ID	Configure the local engine ID. The validity of a user after it is created depends on the engine ID of the SNMP agent. If the engine ID when the user is created is not identical to the current engine ID, the user is invalid.
Maximum Packet Size	Configure the maximum size of an SNMP packet that the agent can receive or send.
Contact	Set a character string to describe 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.

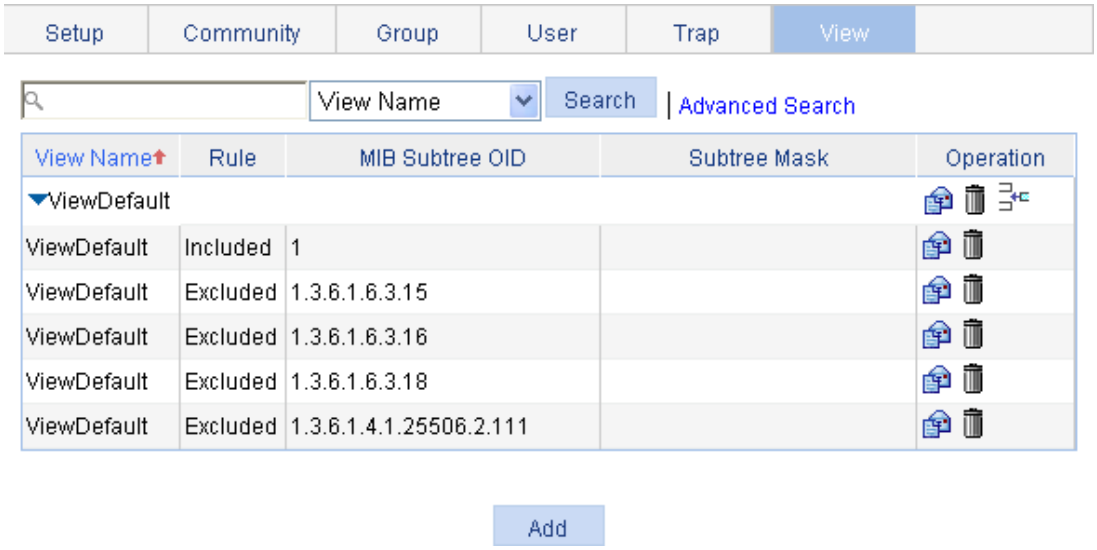
Configuring an SNMP view

Creating an SNMP view

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

   The **View** tab appears.

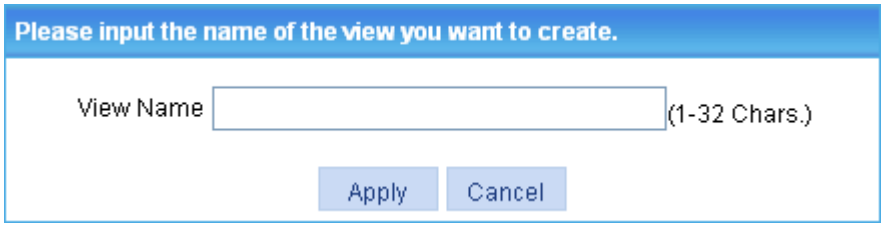
   Figure 104 View tab



3. Click **Add**.

   The **Add View** window appears.

   Figure 105 Creating an SNMP view (1)



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

   The page in Figure 106 appears.
6. Configure the parameters as described in Table 35.
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**.

Figure 106 Creating an SNMP view (2)

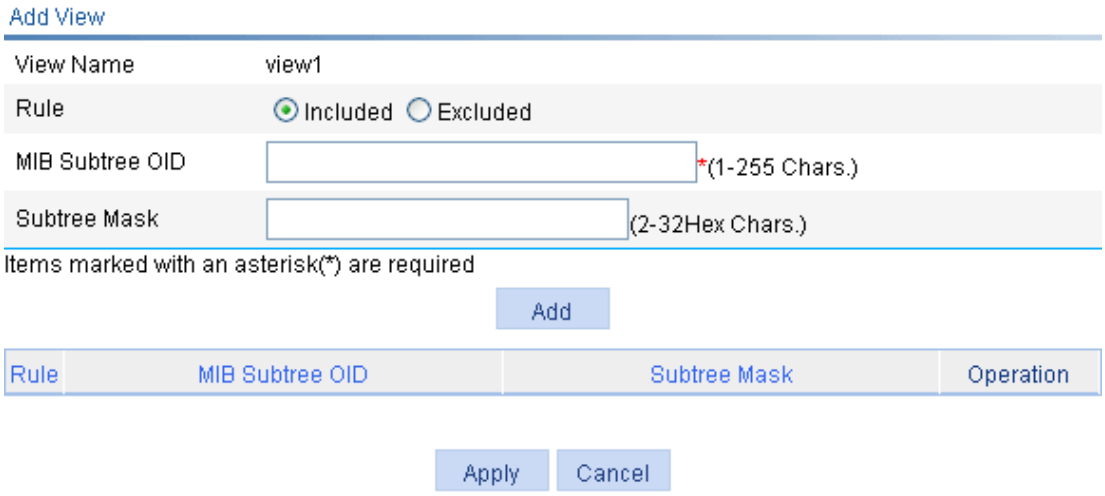


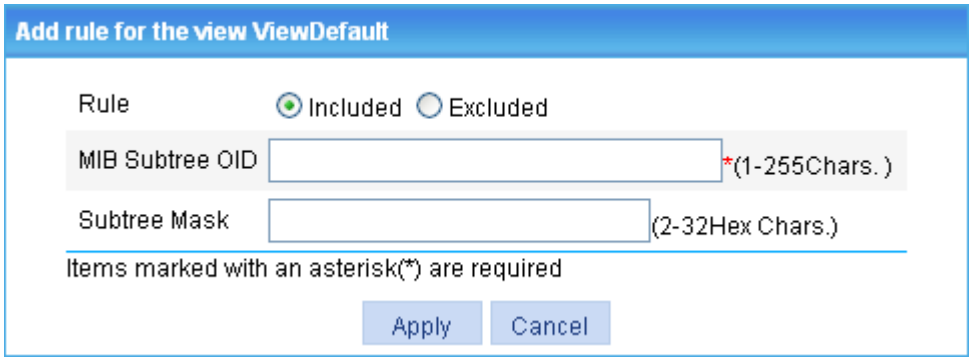
Table 35 Configuration items

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 104 appears.
3. Click the icon of the target view.
   The **Add rule for the view ViewDefault** window appears.

Figure 107 Adding rules to an SNMP view



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

NOTE:

You can also click the icon corresponding to the specified view on the page as shown in Figure 104, and then you can enter the page to modify the view.

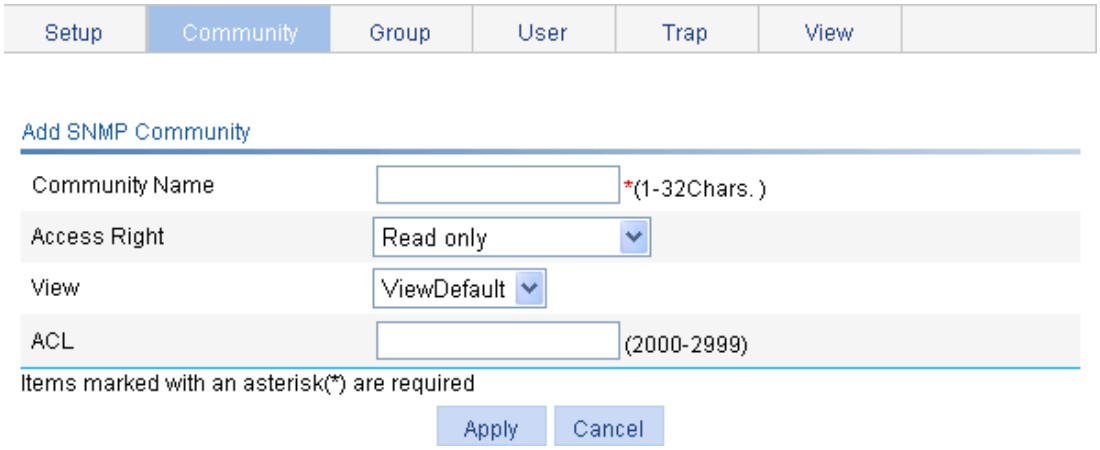
Configuring an SNMP community

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

Figure 108 Configuring an SNMP community

3. Click **Add**.
   The **Add SNMP Community** page appears.

Figure 109 Creating an SNMP Community



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

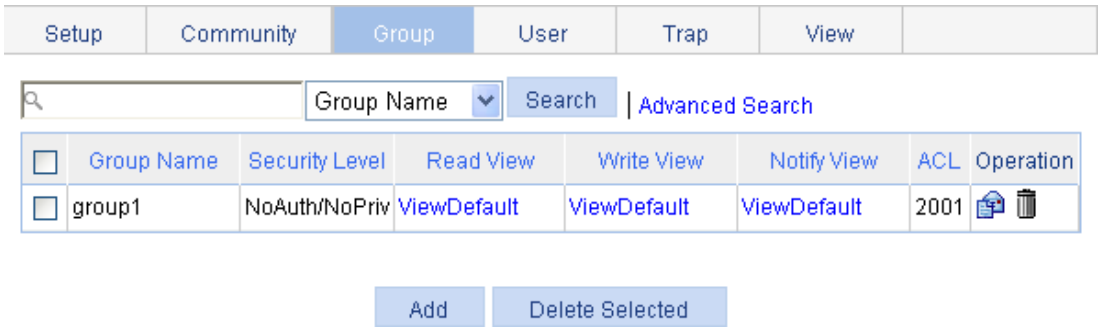
Table 36 Configuration items

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.

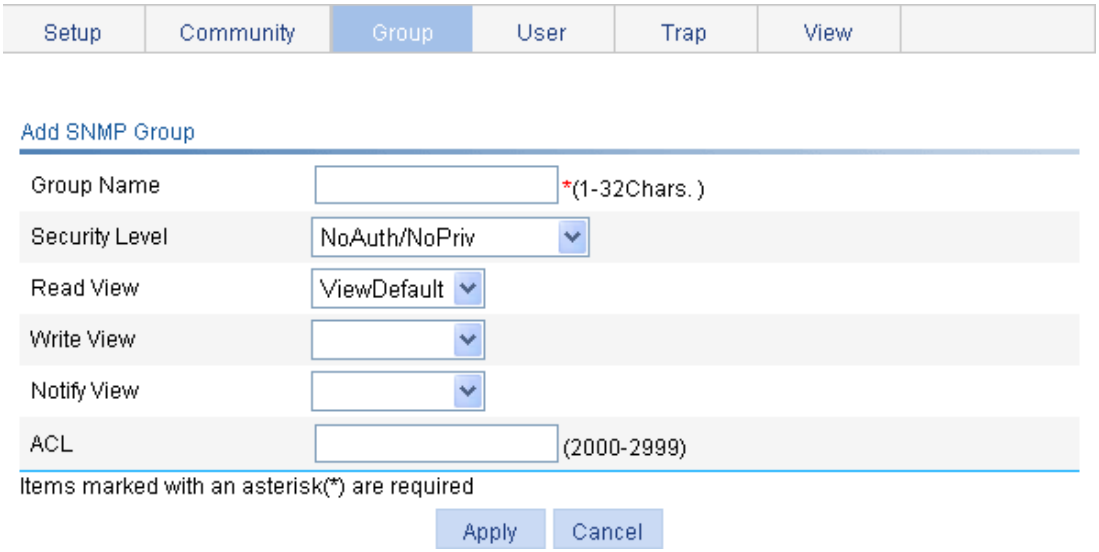
Figure 110 SNMP group



3. Click **Add**.

The **Add SNMP Group** page appears.

Figure 111 Creating an SNMP group



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

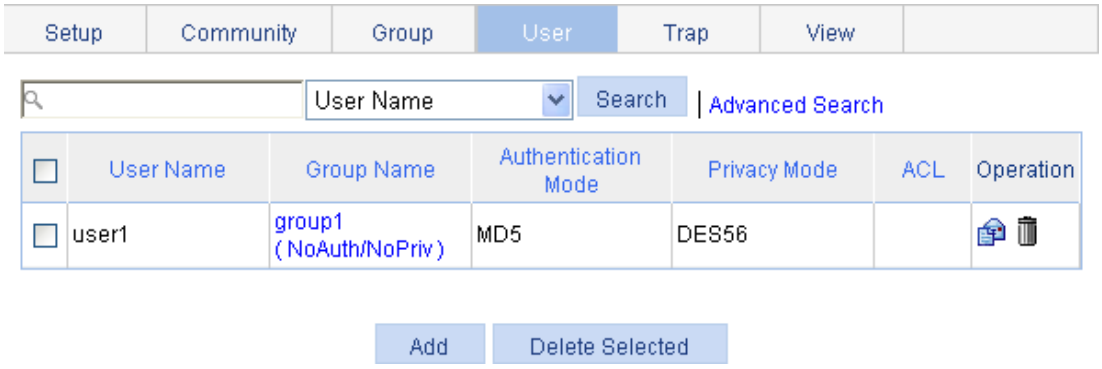
Table 37 Configuration items

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.
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 (the view that can send trap messages) of the SNMP group. 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. To restrict the intercommunication between the NMS and the agent, you can allow or prohibit SNMP packets with a specific source IP address.

Configuring an SNMP user

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

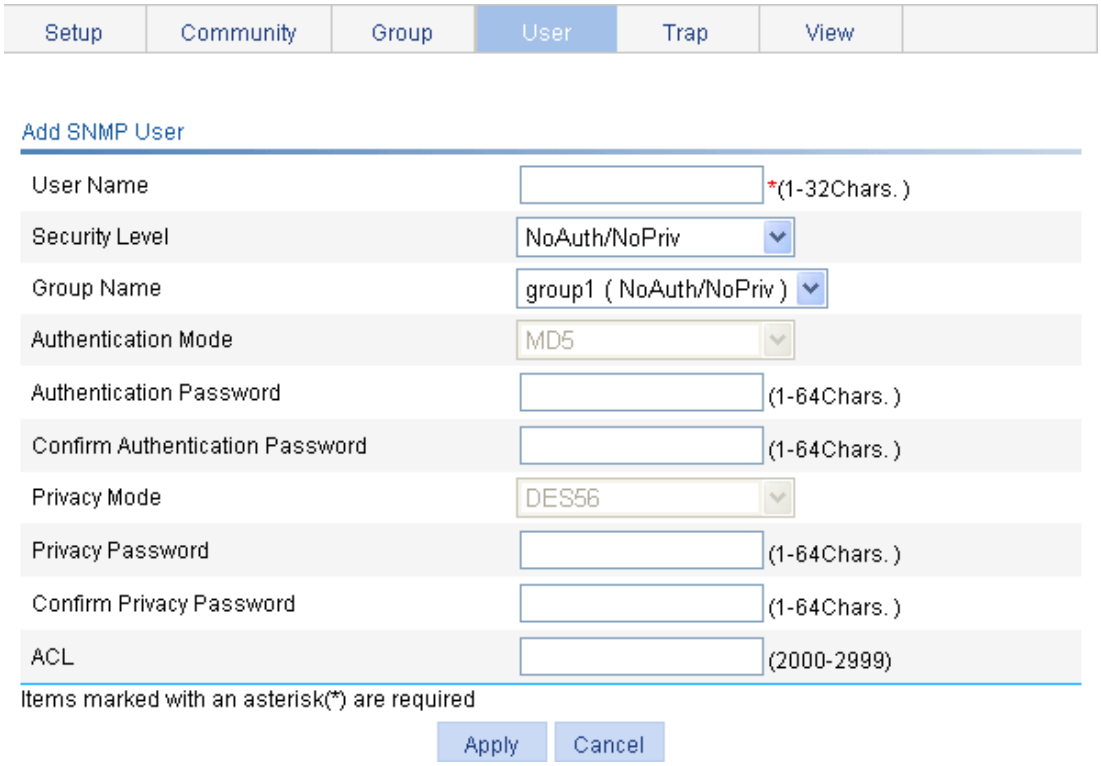
Figure 112 SNMP user



3. Click **Add**.

   The **Add SNMP User** page appears.

Figure 113 Creating an SNMP user



4. Configure the SNMP user as described in Table 38.
5. Click **Apply**.

Table 38 Configuration items

Item	Description
User Name	Set the SNMP user name.
Security Level	Select the security level for the SNMP group. The available security levels are: • **NoAuth/NoPriv**—No authentication no privacy. • **Auth/NoPriv**—Authentication without privacy. • **Auth/Priv**—Authentication and privacy.

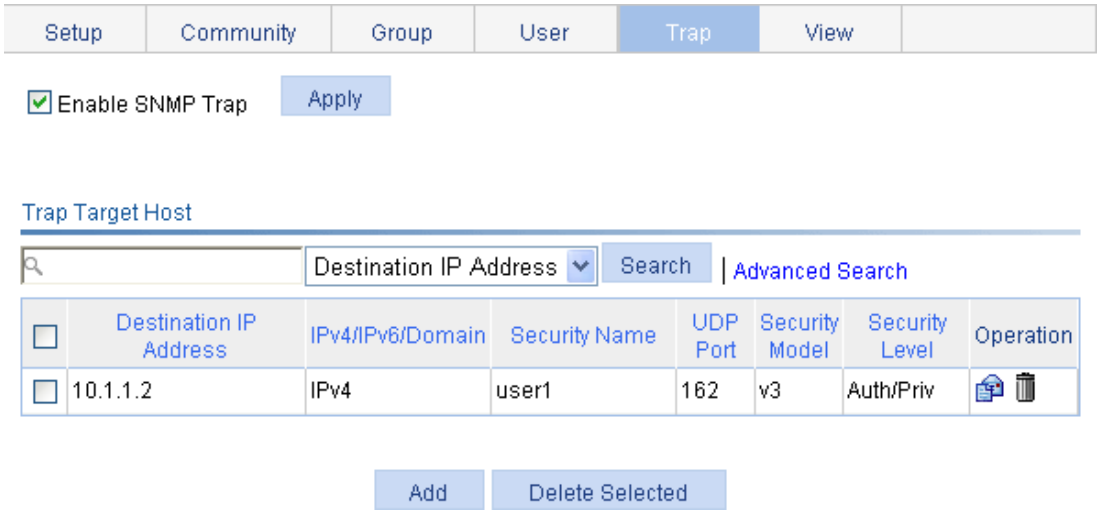
Item	Description
Group Name	Select an SNMP group to which the user belongs: • When the security level is NoAuth/NoPriv, you can select an SNMP group with no authentication no privacy. • When the security level is Auth/NoPriv, you can select an SNMP group with no authentication no privacy or authentication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

Configuring SNMP trap function

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

   The **Trap** tab appears.

   Figure 114 Traps configuration

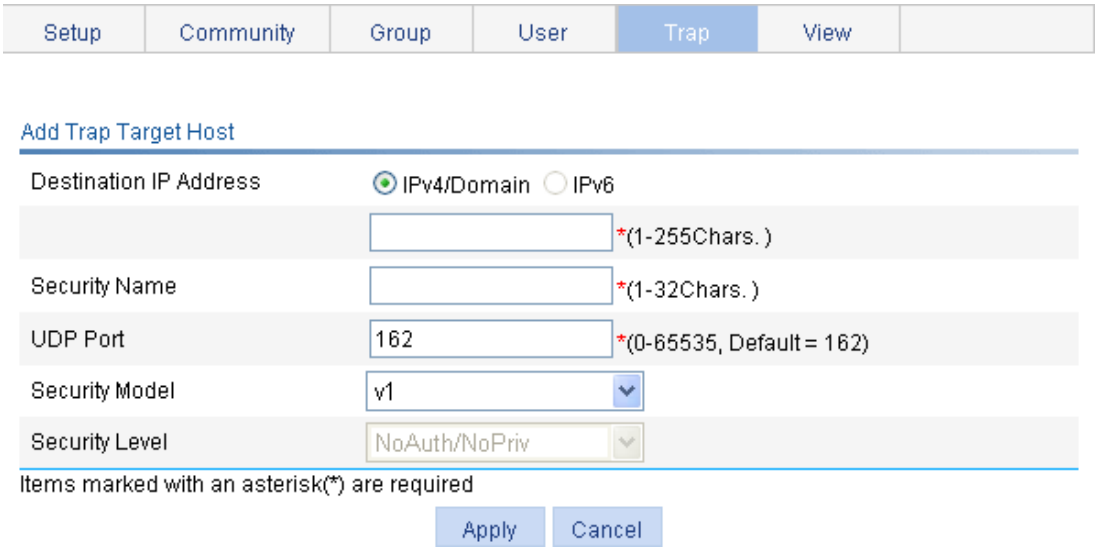


3. Select **Enable SNMP Trap**.
4. Click **Apply** to enable the SNMP trap function.

5. Click **Add**.

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

Figure 115 Adding a target host of SNMP traps



6. Configure the settings for the target host as described in Table 39.
7. Click **Apply**.

Table 39 Configuration items

Item	Description
Destination IP Address	Set the destination IP address. Select the IP address type: IPv4 or IPv6, and then type the corresponding IP address in the field according to the IP address type.
Security Name	Set the security name, which can be an SNMPv1 community name, an SNMPv2c community name, or an SNMPv3 user name.
UDP Port	Set UDP port number. **IMPORTANT:** The 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 the configuration is the same with that on the NMS.
Security Model	Select the security model, for which you must set the SNMP version. For the NMS to receive notifications, make sure the SNMP version is the same with that on the NMS.
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 116 SNMP packet 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 2000)	0
SNMP PDUs which had noSuchName error-status	0
SNMP PDUs which had badValue error-status	0
SNMP PDUs which had genErr error-status	0
GetResponse-PDU accepted and processed	0
Trap PDUs accepted and processed	0

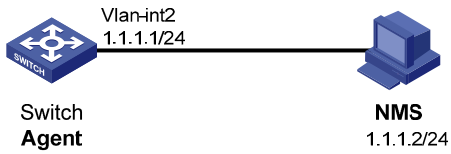
Refresh

SNMPv1/v2c configuration example

Network requirements

As shown in Figure 117, 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.

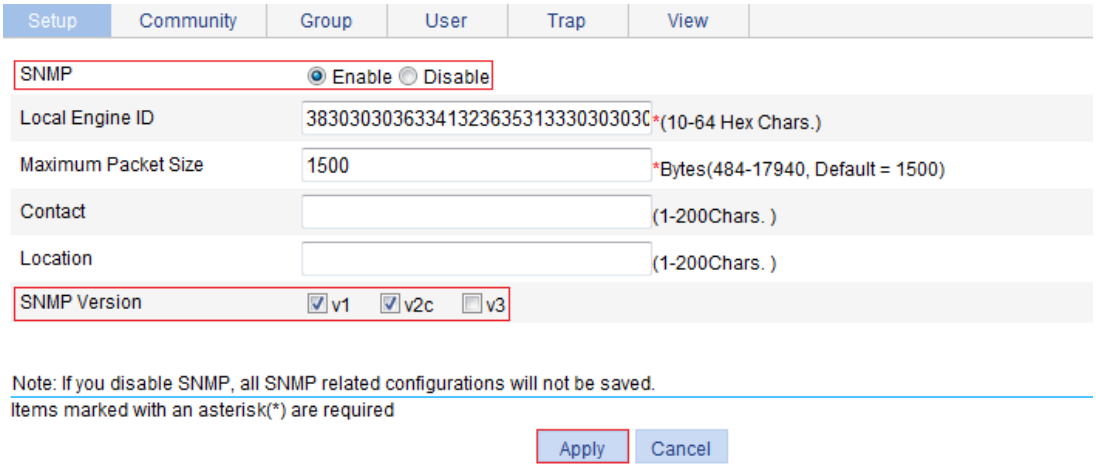
Figure 117 Network diagram



Configuring the agent

1. Enable SNMP:
   a. Select **Device** > **SNMP** from the navigation tree.
      The SNMP configuration page appears.
   b. Select the **Enable** option, and select the **v1** and **v2c** options.
   c. Click **Apply**.

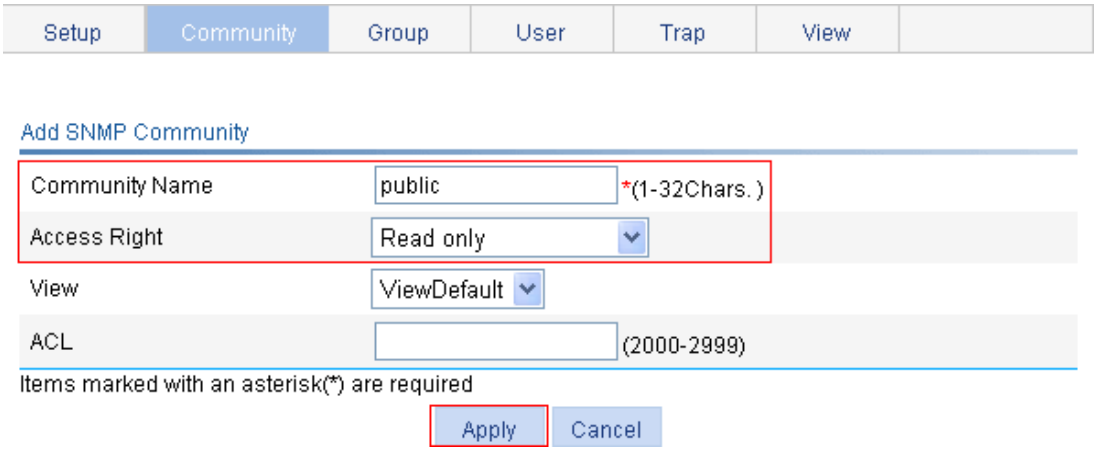
Figure 118 Configuring the SNMP agent



2. Configure a read-only community:
   a. Click the **Community** tab.
   b. Click **Add**.

      The **Add SNMP Community** page appears.
   c. Enter **public** in the **Community Name** field, and select **Read only** from the **Access Right** list.
   d. Click **Apply**.

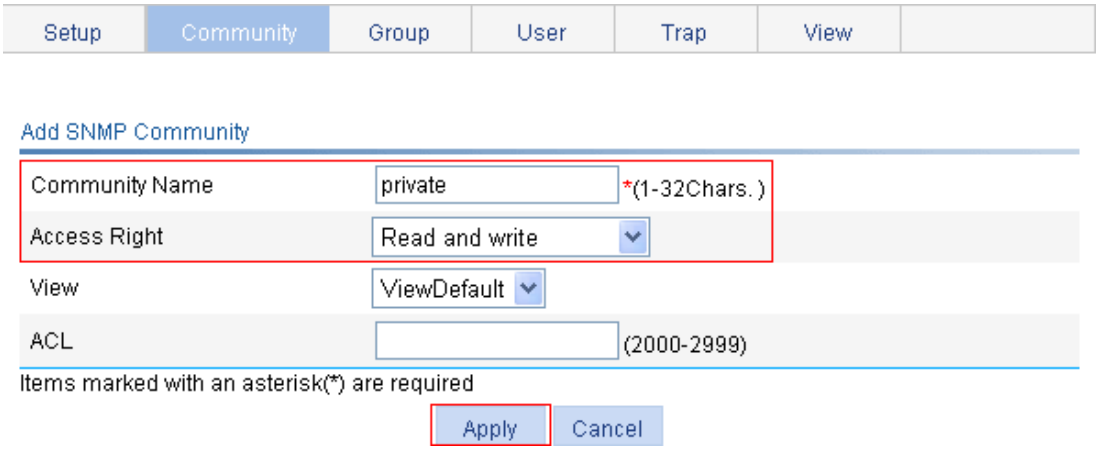
Figure 119 Configuring an SNMP read-only community



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

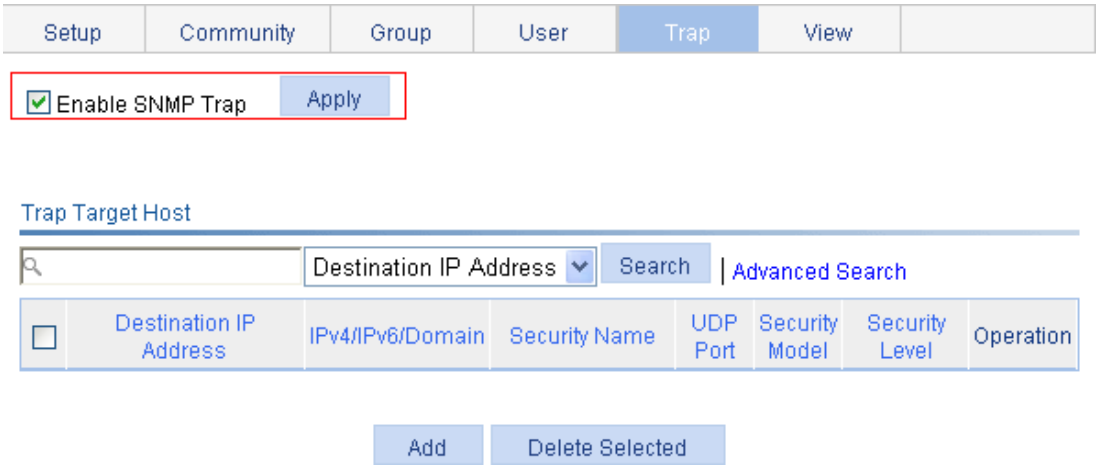
      The **Add SNMP Community** page appears.
   b. Enter **private** in the **Community Name** field, and select **Read and write** from the **Access Right** list.
   c. Click **Apply**.

Figure 120 Configuring an SNMP read and write community



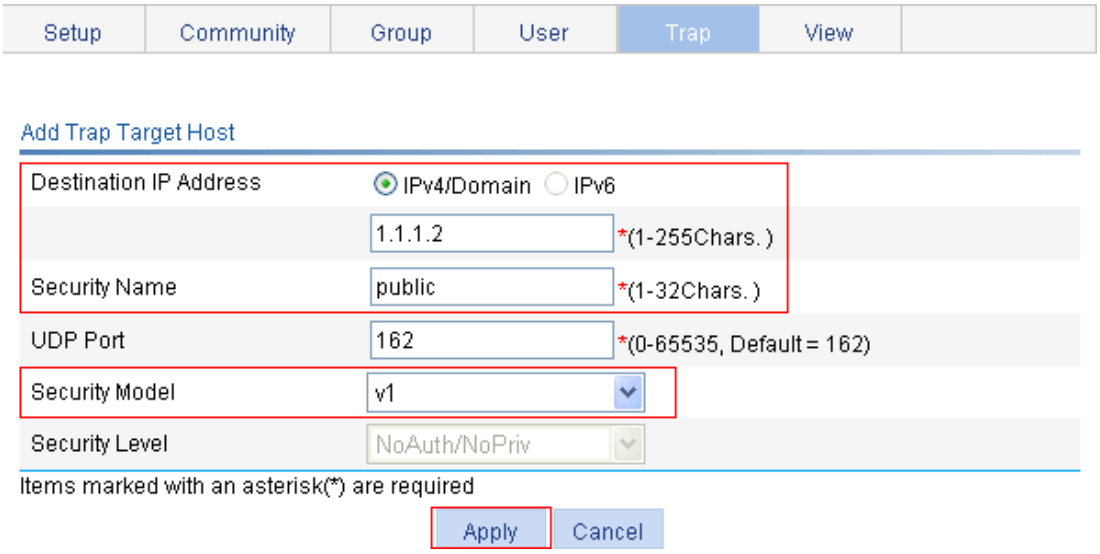
4. Enable SNMP traps:
   a. Click the **Trap** tab.
      The **Trap** tab page appears.
   b. Select **Enable SNMP Trap**.
   c. Click **Apply**.

Figure 121 Enabling SNMP traps



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.
   b. Select the **IPv4/Domain** option and 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**.

Figure 122 Adding a trap target host



Configuring the NMS

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

To configure the NMS:

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 information about 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.

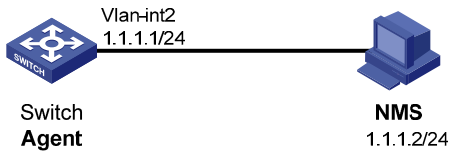
SNMPv3 configuration example

Network requirements

As shown in Figure 123, 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**.

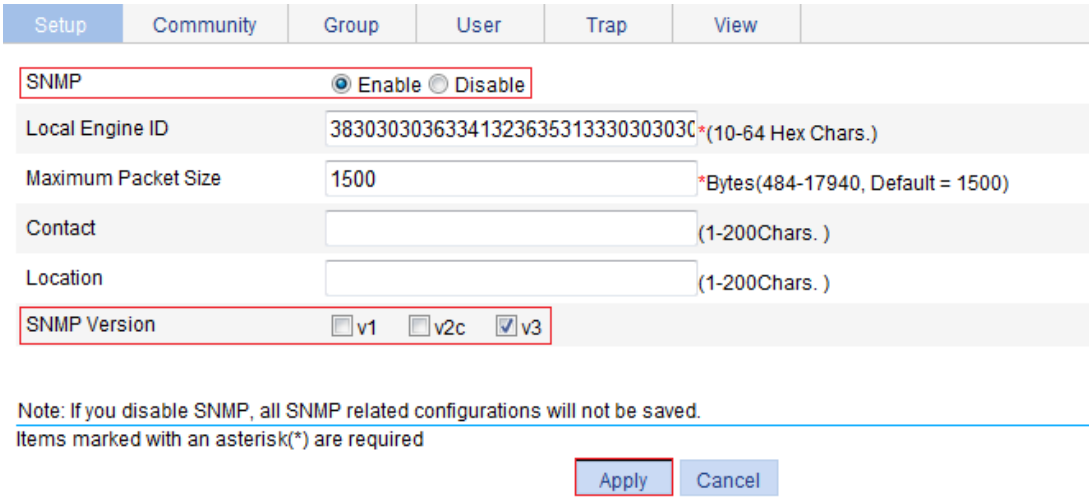
Figure 123 Network diagram



Configuring the agent

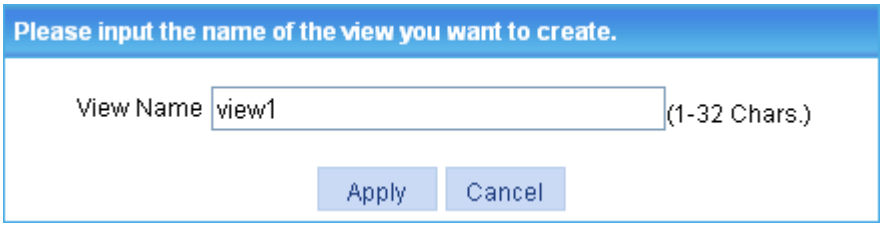
1. Enable SNMP agent:
   a. Select **Device** > **SNMP** from the navigation tree.
      The SNMP configuration page appears.
   b. Select the **Enable** option, and select the **v3** option.
   c. Click **Apply**.

Figure 124 Configuring the SNMP agent



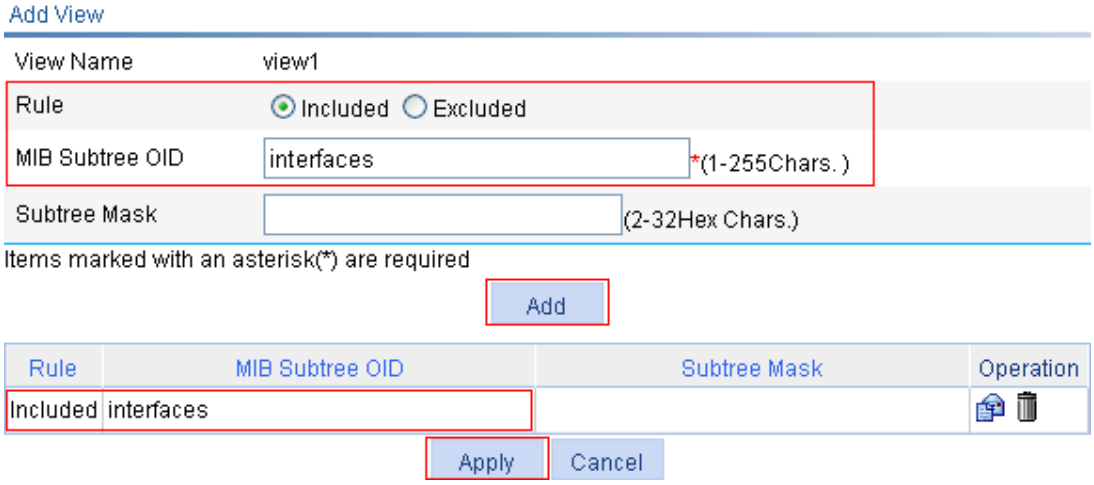
2. Configure an SNMP view:
   a. Click the **View** tab.
   b. Click **Add**.
      The page for creating an SNMP view appears.
   c. Type **view1** in the **View Name** field.
   d. Click **Apply**.

Figure 125 Creating an SNMP view (1)



   e. On the page that appears, 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.

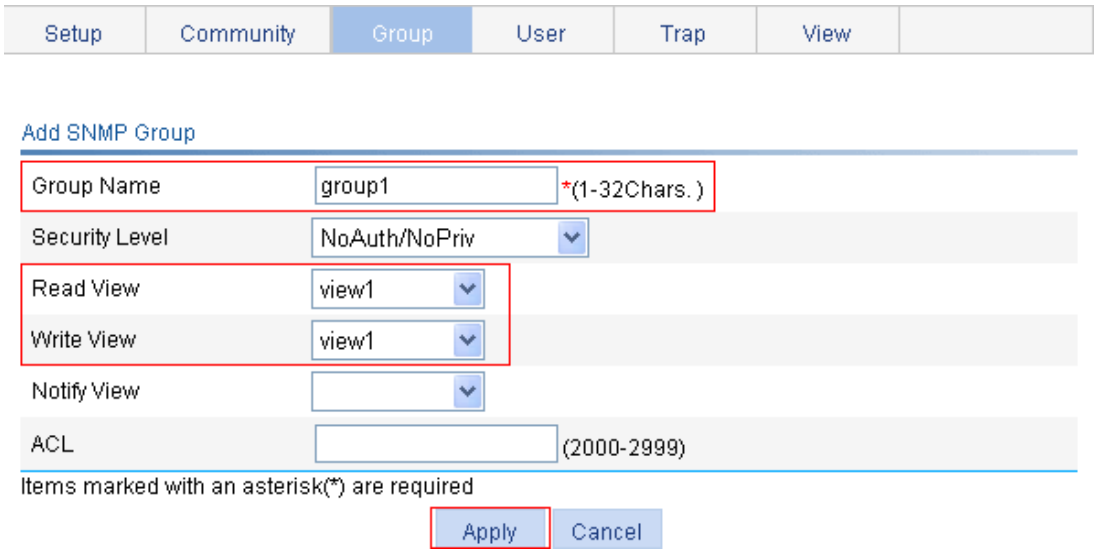
Figure 126 Creating an SNMP view (2)



3. Configure an SNMP group:
   a. Click the **Group** tab.
   b. Click **Add**.

      The page in Figure 127 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 127 Creating an SNMP group



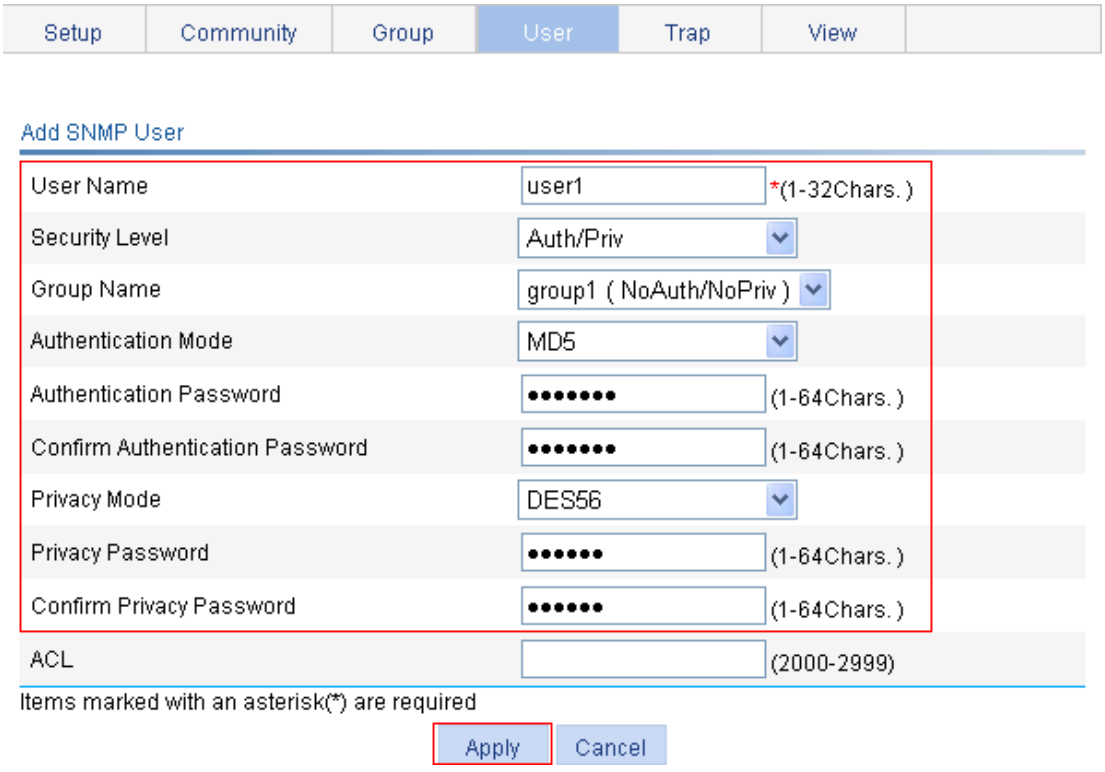
4. Configure an SNMP user:
   a. Click the **User** tab.
   b. Click **Add**.

      The page in Figure 128 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 128 Creating an SNMP user



5. Enable SNMP traps:

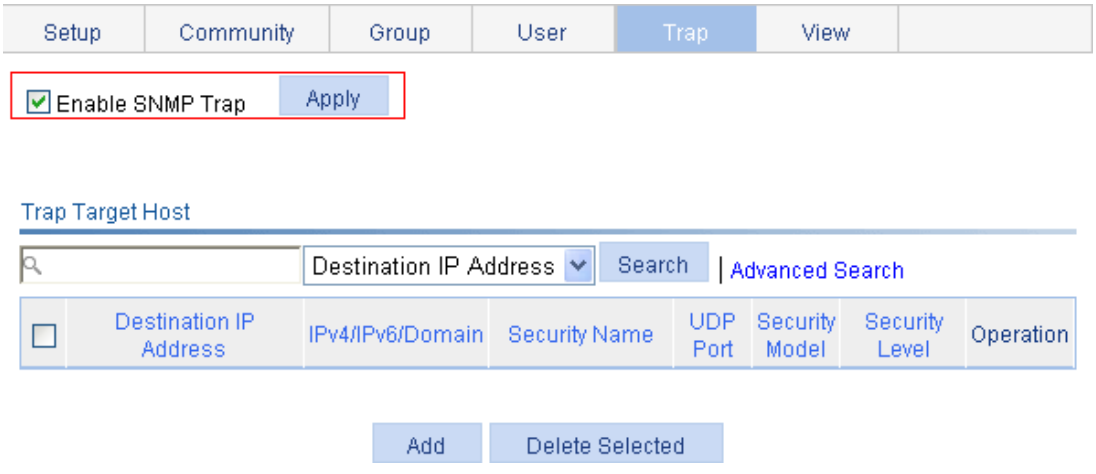
a. Click the **Trap** tab.

The **Trap** tab page appears.

b. Select **Enable SNMP Trap**.

c. Click **Apply**.

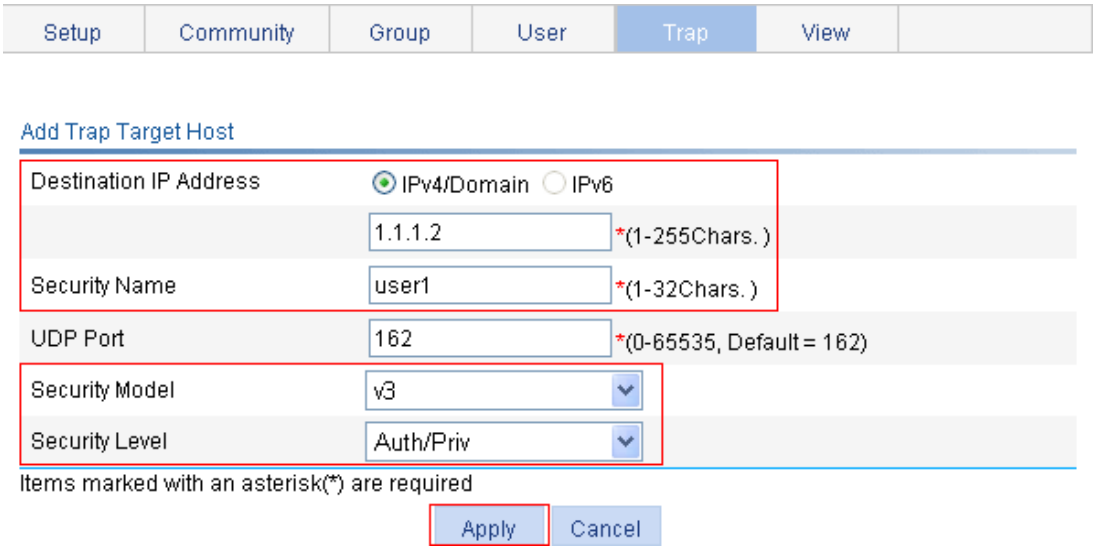
Figure 129 Enabling SNMP traps



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.
   b. Select the **IPv4/Domain** option and 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**.

Figure 130 Adding a trap target host



Configuring the NMS

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

To configure the NMS:

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

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

To display interface statistics, select **Device** > **Interface Statistics** from the navigation tree.

Figure 131 Interface statistics display page

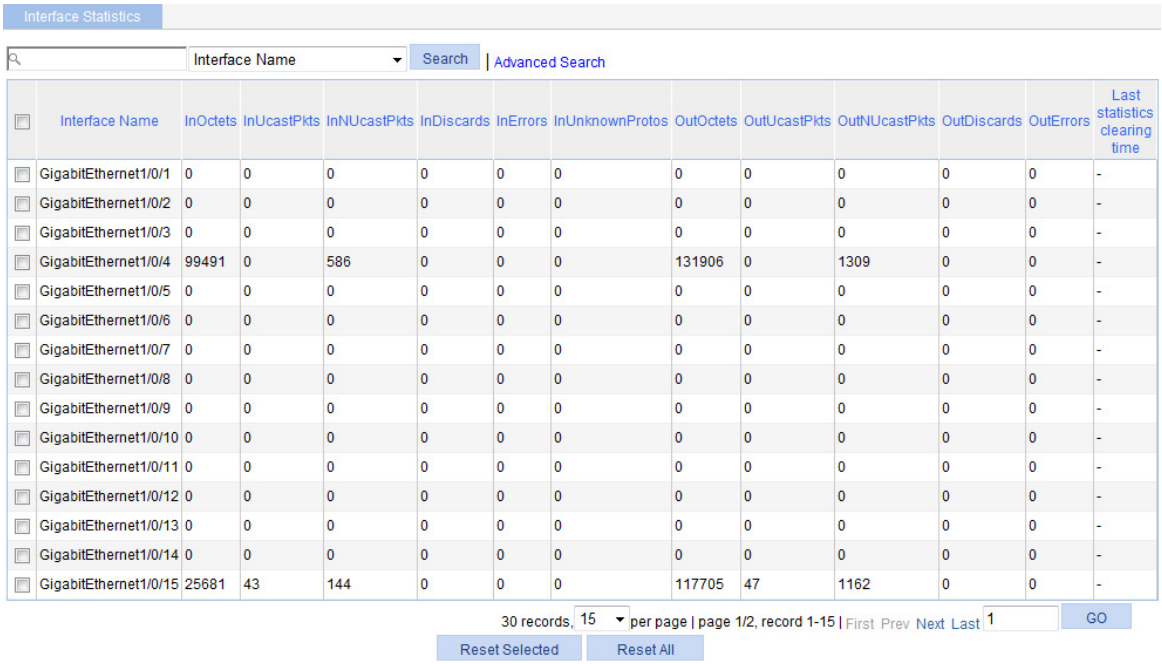


Table 40 describes the fields on the page.

Table 40 Field description

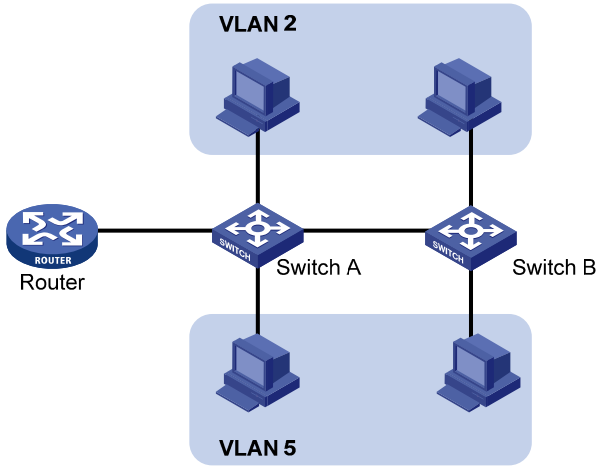
Field	Description
InOctets	Total octets of all packets received on the interface.
InUcastPkts	Number of received unicast packets.
InNUcastPkts	Number of received non-unicast packets.
InDiscards	Number of valid packets discarded in the inbound direction.
InErrors	Number of received invalid packets.
InUnknownProtos	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.
Last statistics clearing time	Last time when the statistics were cleared.

Configuring VLANs

Overview

Ethernet is a network technology based on the 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 132.

Figure 132 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

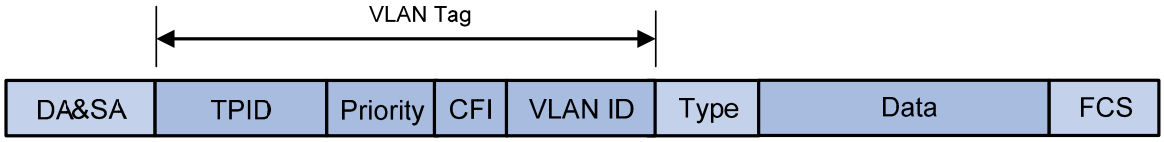
To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation. The format of VLAN-tagged frames is defined in IEEE 802.1Q-1999.

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 133.

Figure 133 Traditional Ethernet frame format

IEEE 802.1Q inserts a four-byte VLAN tag after the DA&SA field, as shown in Figure 134.

Figure 134 Position and format of VLAN tag



A VLAN tag comprises the following fields:

- **Tag protocol identifier (TPID)**—The 16-bit TPID field indicates whether the frame is VLAN-tagged and is 0x8100 by default.
- **Priority**—The 3-bit priority field indicates the 802.1p priority of the frame.
- **Canonical format indicator (CFI)**—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.
- **VLAN ID**—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.

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

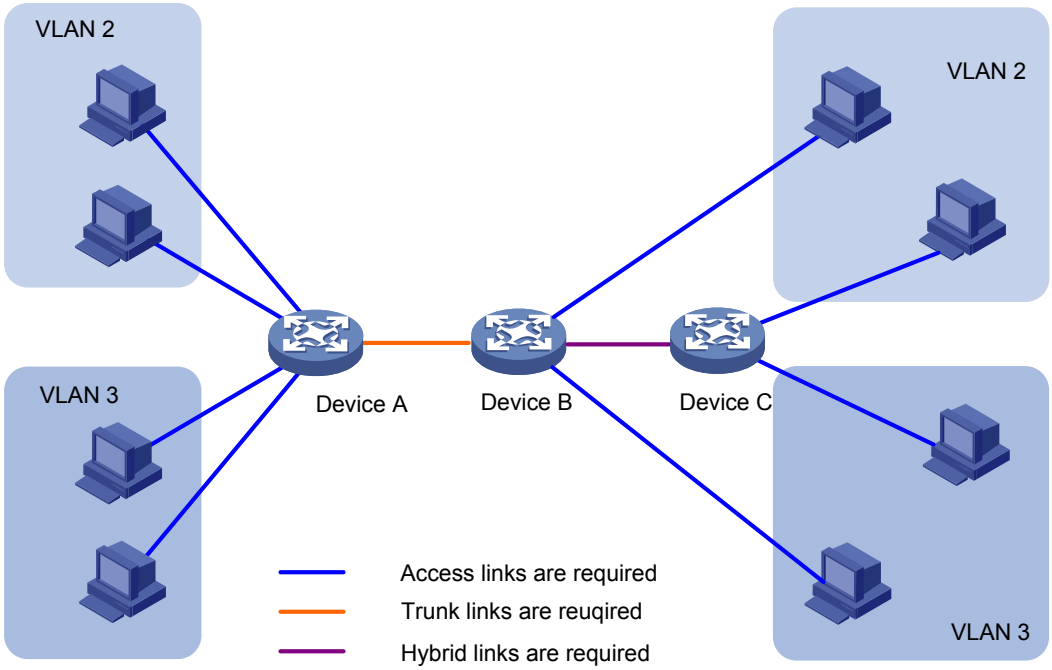
Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

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:

- **Access port**—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 it is unnecessary to separate different VLAN members. As shown in Figure 135, Device A is connected to common PCs that cannot recognize VLAN tagged-packets, and you must configure Device A's ports that connect to the PCs as access ports.
- **Trunk port**—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. As shown in Figure 135, Device A and Device B need to transmit packets of VLAN 2 and VLAN 3, and you must configure the ports interconnecting Device A and Device B as trunk ports and assign them to VLAN 2 and VLAN 3.
- **Hybrid port**—A hybrid port allows traffic of some VLANs to pass through untagged and traffic of some other VLANs to pass through tagged. Usually, hybrid ports are configured to connect devices whose support for VLAN-tagged packets are uncertain. As shown in Figure 135, Device C connects to a small-sized LAN in which some PCs belong to VLAN 2 and other PCs belong to VLAN 3, and Device B is uncertain about whether Device C supports VLAN-tagged packets. Configure on Device B the port connecting to Device C as a hybrid port to allow packets of VLAN 2 and VLAN 3 to pass through untagged.

Figure 135 Port link types



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. However, deleting the VLAN specified as the PVID of a trunk or hybrid port does not affect the PVID setting on the port.
- Hewlett Packard Enterprise recommends that you set the same PVID for local and remote ports.

- Make sure 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.	
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

Recommended configuration procedure for 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.

Step	Remarks	
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.	

Recommended configuration procedure for assigning a trunk 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 trunk. To configure a hybrid port as a trunk port, first configure it as an access port. By default, the link type of a port is access.	
3. Setting the PVID for a port.	Configure the PVID of the trunk port.	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. When you change the untagged VLAN (PVID) of a trunk port, the former untagged VLAN automatically becomes a tagged VLAN of the trunk port.
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.	N/A	
5. Modifying ports.	Configure the untagged VLAN of the trunk port.	

Step	Remarks	
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.	N/A	Required. A trunk port can have multiple tagged VLANs. You can repeat these steps to configure multiple tagged VLANs for the trunk port.
7. Modifying ports.	Configure the tagged VLAN of the trunk port.	

Recommended configuration procedure for assigning a hybrid 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 hybrid. To configure a trunk port as a hybrid port, first configure it as an access port. 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.	
3. Setting the PVID for a port.	Optional. Configure the PVID of the hybrid port. By default, the PVID of a hybrid port is VLAN 1.	
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.	N/A	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.
5. Modifying ports.	Configure the untagged VLAN of the hybrid port.	

Step		Remarks	
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.	N/A	Required. A hybrid port can have multiple tagged VLANs. You can repeat these steps to configure multiple tagged VLANs for the hybrid port.
7.	Modifying ports.	Configure the tagged VLAN of the hybrid port.	

Creating VLANs

1. From the navigation tree, select **Network** > **VLAN**.
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 136 Creating VLANs

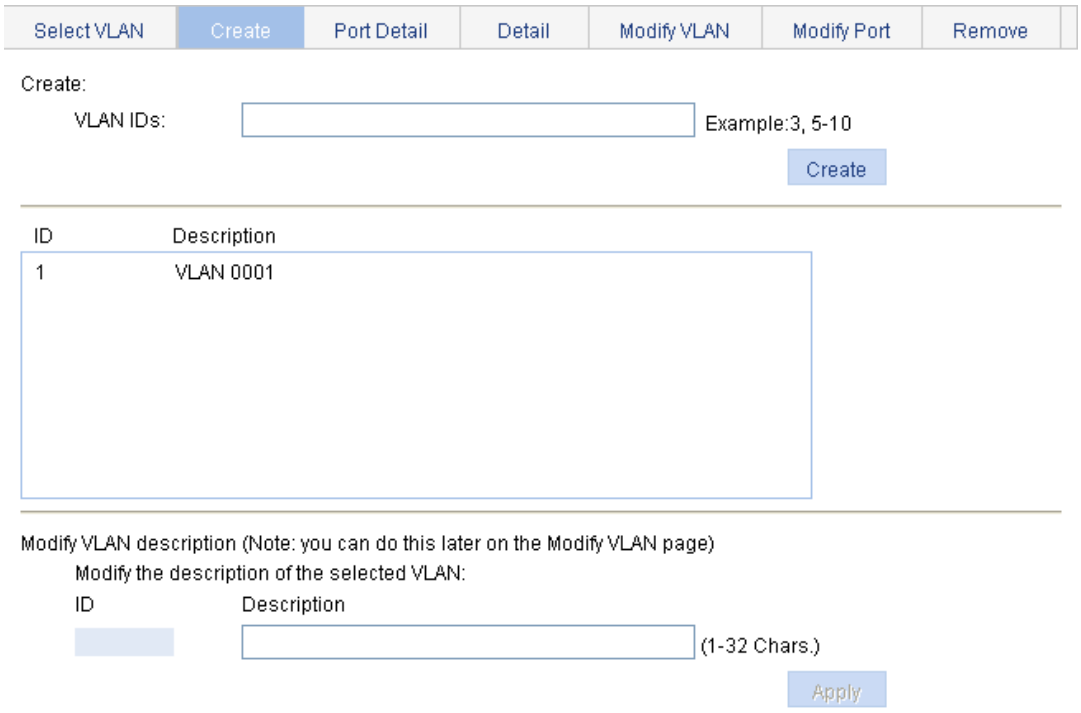


Table 41 Configuration items

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

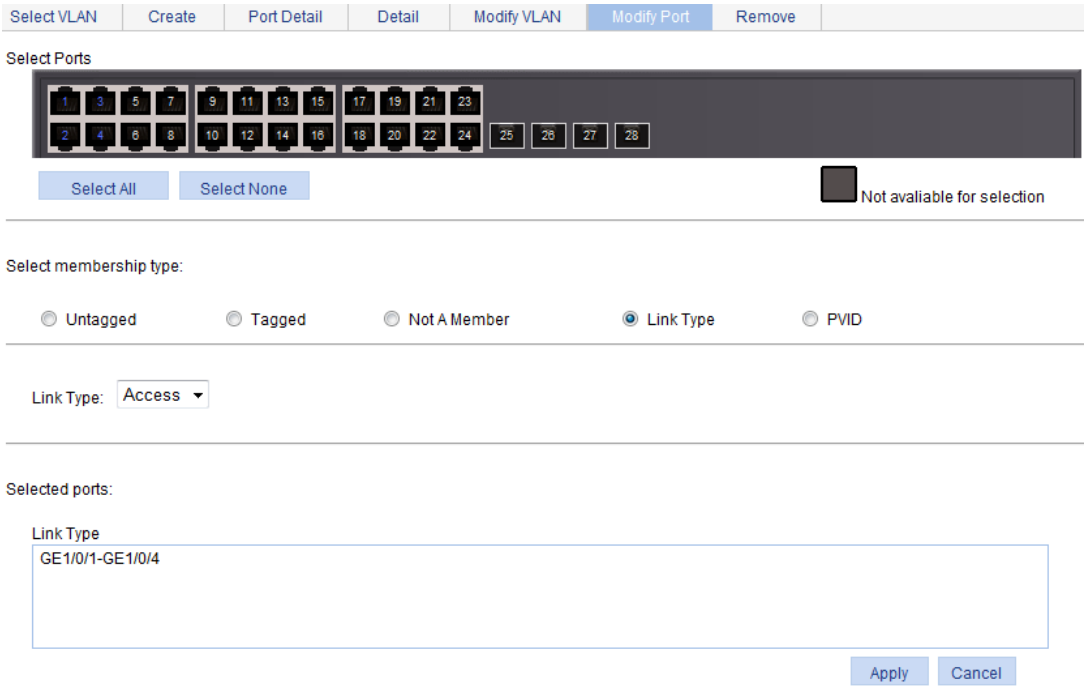
You can also configure the link type of a port on the **Setup** tab of **Device** > **Port Management**. For more information, see "Managing ports."

To configure the link type of a port:

1. From the navigation tree, select **Network** > **VLAN**.
2. Click **Modify Port**.
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 to 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 137 Modifying ports



Setting the PVID for a port

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

To set the PVID for a port:

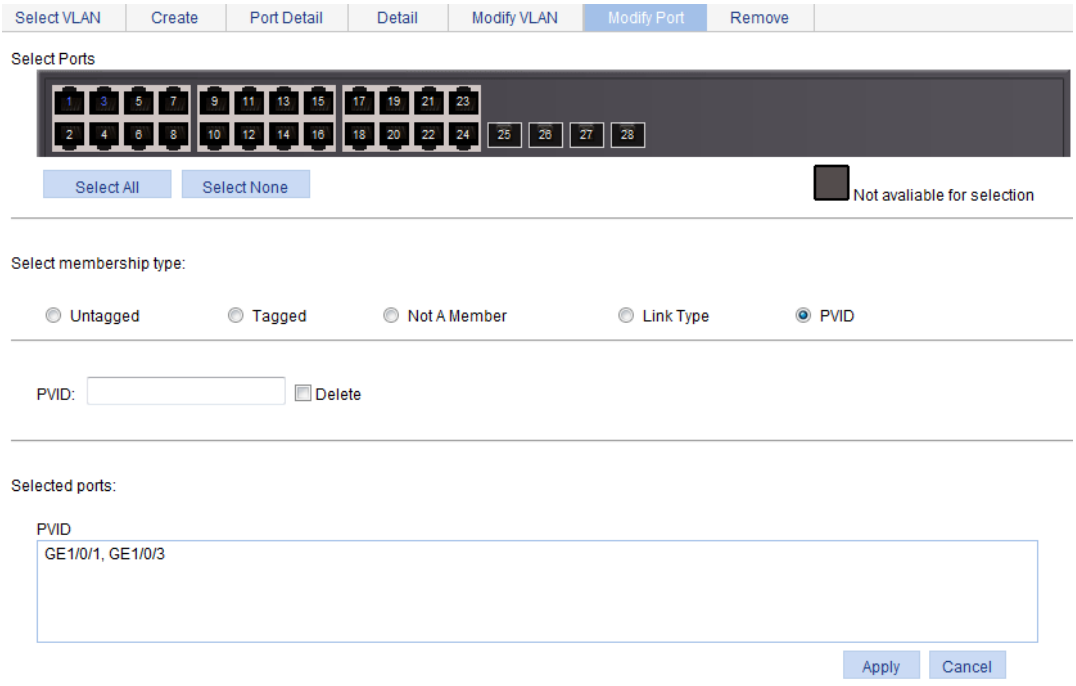
1. From the navigation tree, select **Network** > **VLAN**.
2. Click **Modify Port**.
3. Select the port that you want to configure on the chassis front panel.
4. Select the **PVID** option.

   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 138 Modifying the PVID for a port

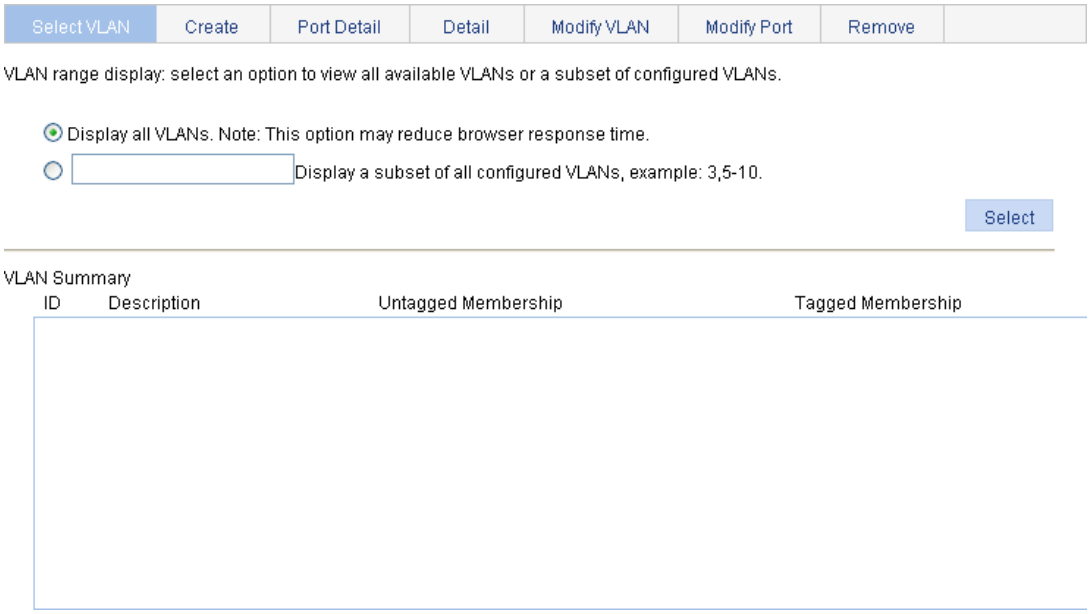


Selecting VLANs

1. From the navigation tree, select **Network** > **VLAN**.

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

Figure 139 Selecting VLANs

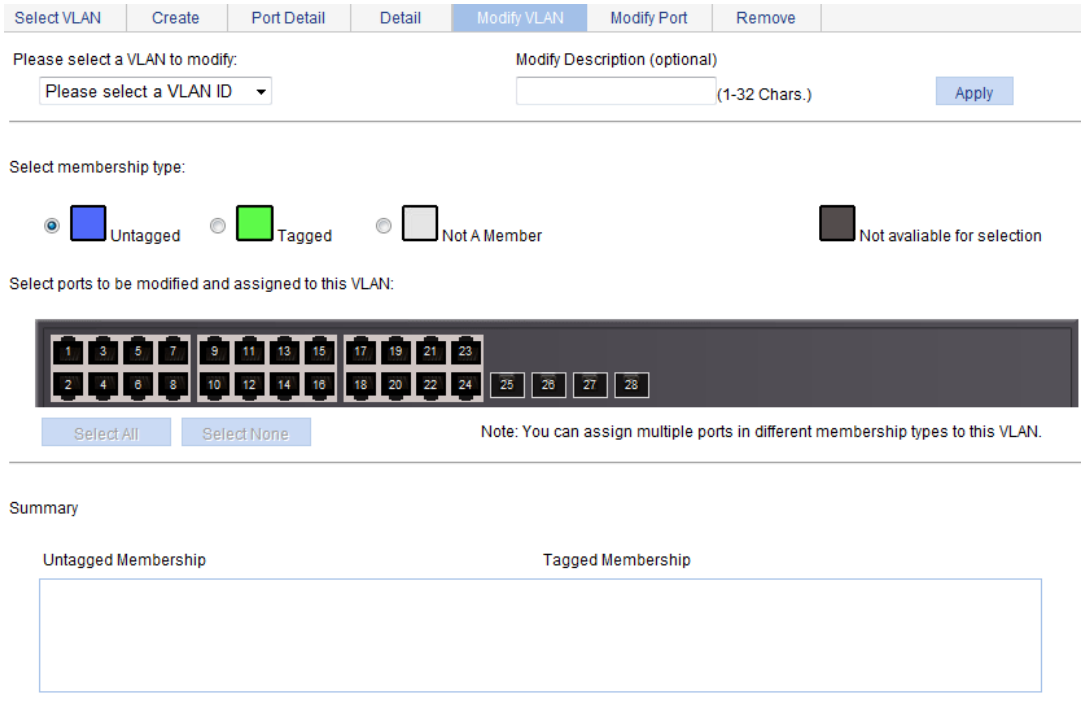


2. Select the **Display all VLANs** option to display all VLANs, or select the **Display a subnet of all configured VLANs** option to enter the VLAN IDs to be displayed.
3. Click **Select**.

Modifying a VLAN

1. From the navigation tree, select **Network** > **VLAN**.
2. Click **Modify VLAN** to enter the page for modifying a VLAN.

Figure 140 Modifying a VLAN



3. Modify the member ports of a VLAN 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.

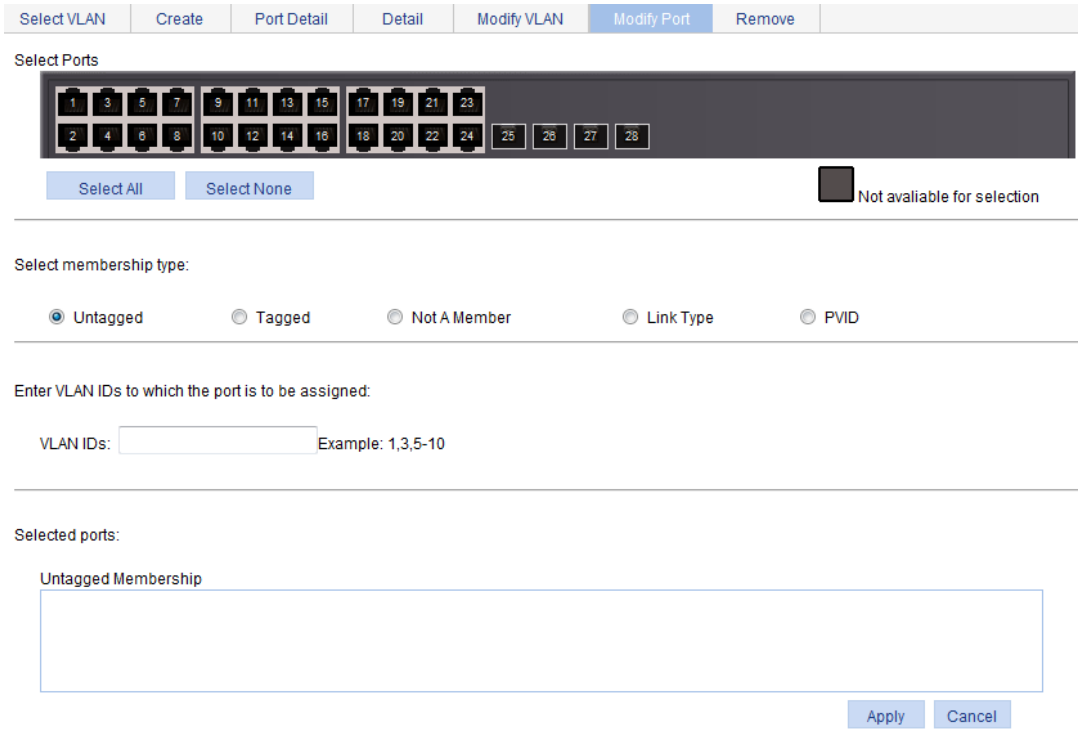
Table 42 Configuration items

Item	Description
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**—Configures the port to send the traffic of the VLAN after removing the VLAN tag. • **Tagged**—Configures the port to send the traffic of the VLAN without removing the VLAN tag. • **Not a Member**—Removes 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. 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. From the navigation tree, select **Network** > **VLAN**.
2. Click **Modify Port** to enter the page for modifying ports.

Figure 141 Modifying ports



3. Modify the VLANs of a port as described in Table 43.
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 43 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**—Configures the ports to send the traffic of the VLANs after removing the VLAN tags. • **Tagged**—Configures the ports to send the traffic of the VLANs without removing the VLAN tags. • **Not a Member**—Removes the ports from the VLANs.
VLAN IDs	Set the IDs of the VLANs to or from which the selected ports are to be assigned or removed. When you set the VLAN IDs, follow these guidelines: • 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.

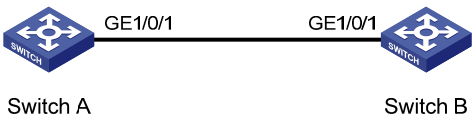
VLAN configuration example

Network requirements

As shown in Figure 142, 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 from VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

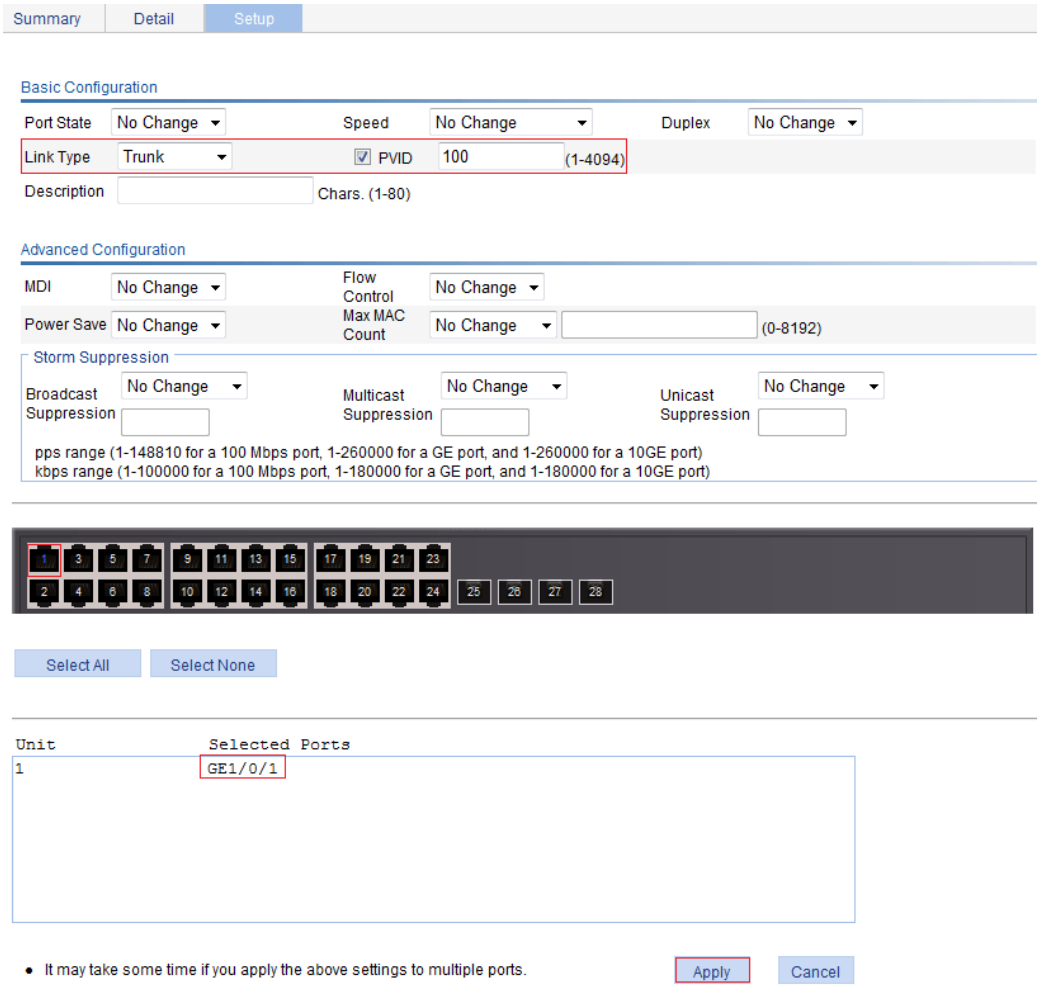
Figure 142 Network diagram



Configuring Switch A

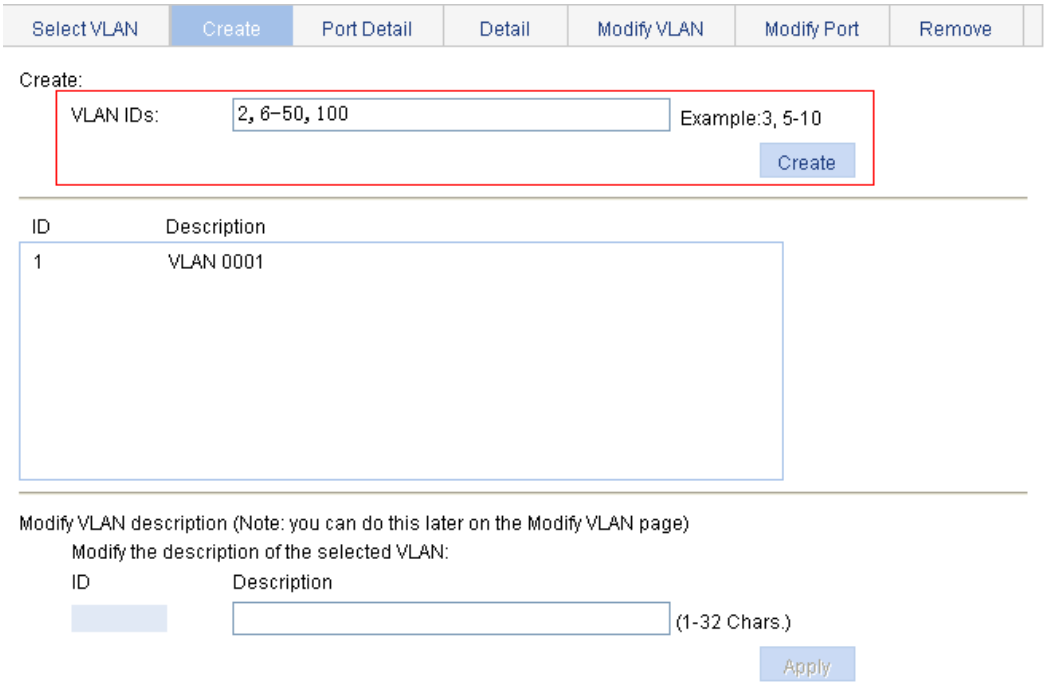
1. Configure GigabitEthernet 1/0/1 as a trunk port and configure VLAN 100 as the PVID:
   a. From the navigation tree, select **Device** > **Port Management**.
   b. Click **Setup** to enter the page for setting ports.
   c. Select **Trunk** in the **Link Type** list, select the **PVID** box, and then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

Figure 143 Configuring GigabitEthernet 1/0/1 as a trunk port and its PVID as 100



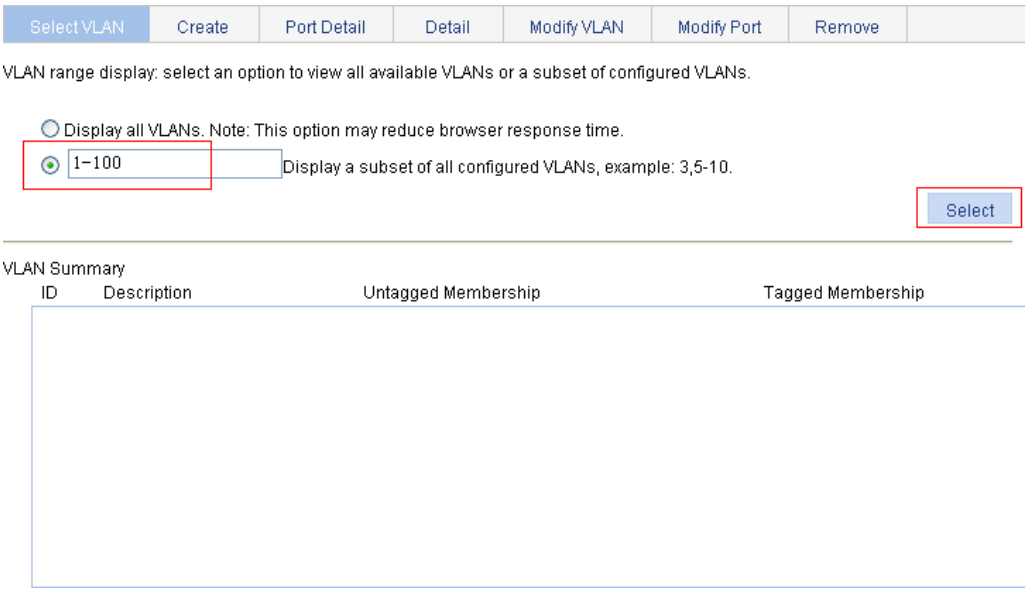
2. Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100:
   a. From the navigation tree, select **Network** > **VLAN**.
   b. Click **Create** to enter the page for creating VLANs.
   c. Enter VLAN IDs 2, 6-50, 100.
   d. Click **Apply**.

Figure 144 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 145 Setting a VLAN range

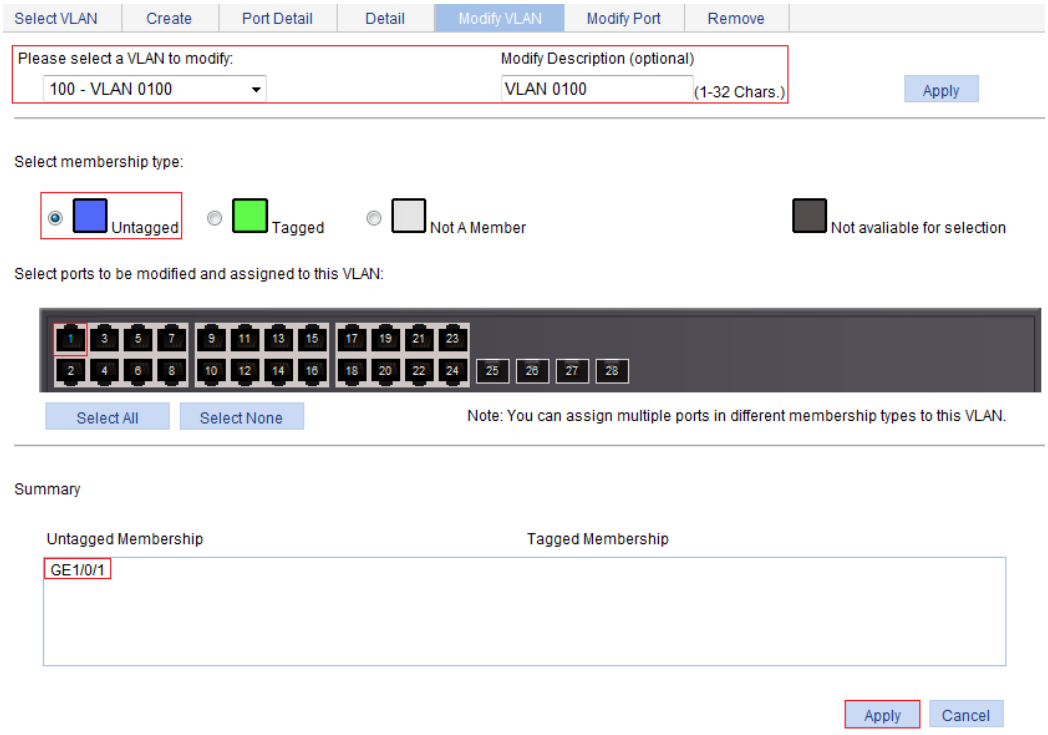


   d. Click **Modify VLAN** to enter the page for modifying the ports in a VLAN.
   e. Select **100 – VLAN 0100** in the **Please select a VLAN to modify:** list, select the **Untagged** option, and select GigabitEthernet 1/0/1 on the chassis front device panel.
   f. Click **Apply**.

A configuration progress dialog box appears.

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

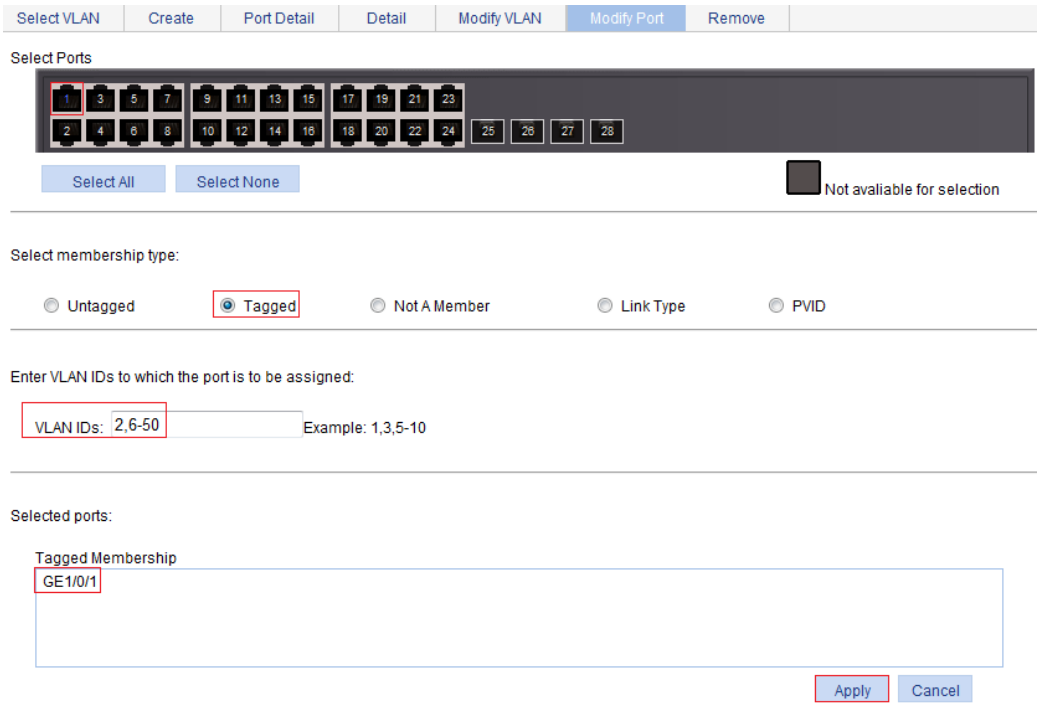
Figure 146 Assigning GigabitEthernet 1/0/1 to VLAN 100 as an untagged member



4. Assign GigabitEthernet 1/0/1 to VLAN 2, 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 147 Assigning GigabitEthernet 1/0/1 to VLAN 2 and to VLANs 6 through 50 as a tagged member



Configuring Switch B

Configure Switch B in the same way Switch A is configured. (Details not shown.)

Configuration guidelines

When you configure VLANs, follow these guidelines:

- 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.
- You cannot remove a VLAN that has referenced a QoS policy.

Configuring VLAN interfaces

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

Overview

For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, 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 it as the gateway of the VLAN to forward the traffic destined for an IP network segment different from that of the VLAN.

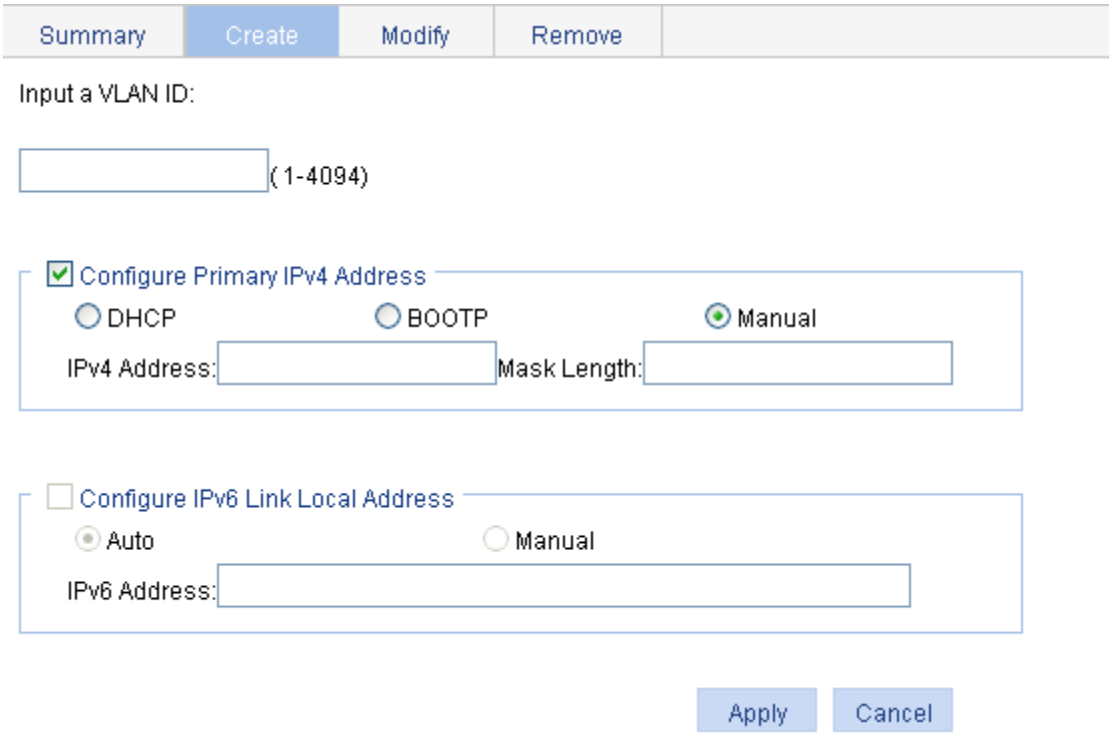
Creating a VLAN interface

When you create 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. From the navigation tree, select **Network** > **VLAN Interface**.
2. Click **Create** to enter the page for creating a VLAN interface.

Figure 148 Creating a VLAN interface



3. Configure the VLAN interface as described in Table 44.
4. Click **Apply**.

Table 44 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 the corresponding VLAN exists.	
Configure Primary IPv4 Address	DHCP	Configure the way in which the VLAN interface gets an IPv4 address. Allow the VLAN interface to get an IP address automatically by selecting the **DHCP** or **BOOTP** option. Otherwise, select the **Manual** option to manually assign the VLAN interface an IP address. After a VLAN interface fails to get an IP address through DHCP multiple times, the device stops IP address application and configures the default IP address for the interface.	These items are available after you select the **Configure Primary IPv4 Address** box.
	BOOTP		
	Manual		
	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	Configure the way in which the VLAN interface gets an IPv6 link-local address. Select the **Auto** or **Manual** option: • **Auto**—The device automatically assigns a link-local address to 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 Address** box.
	Manual		
	IPv6 Address	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.

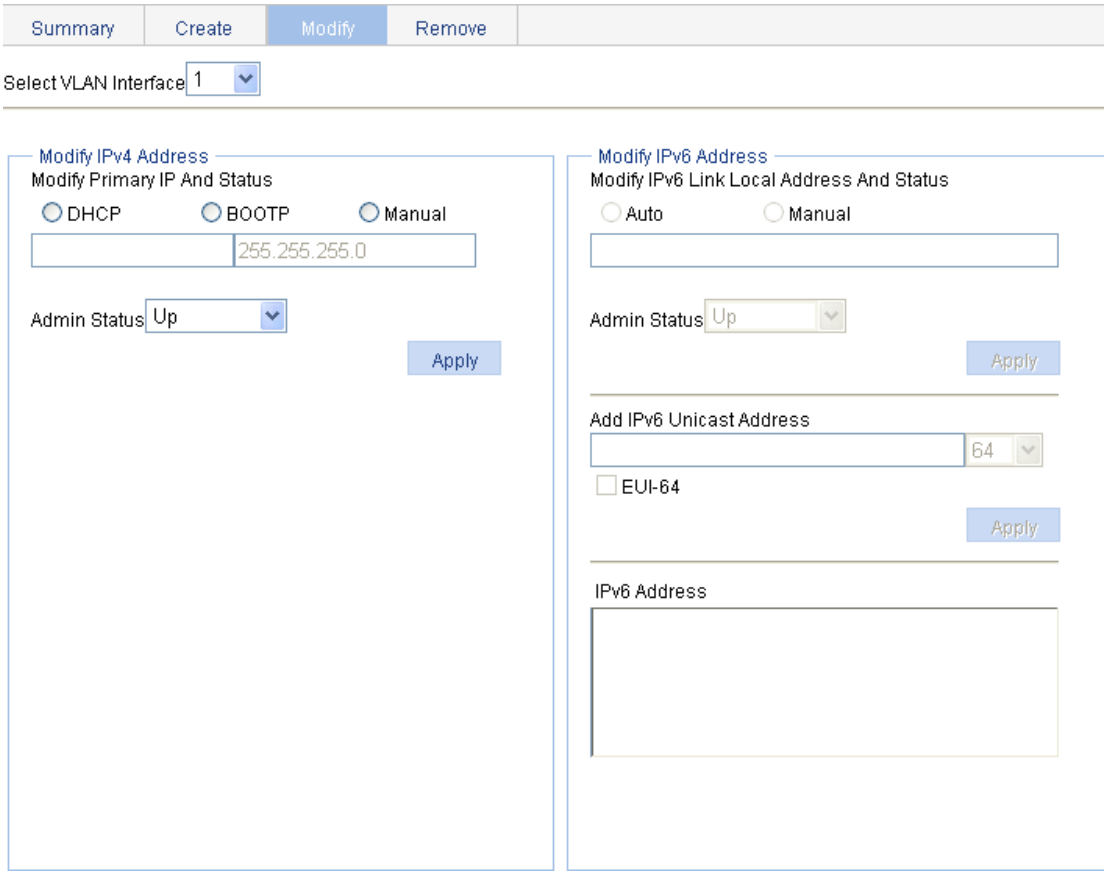
After you modify the IPv4 address and status or the IPv6 address and status, or add an IPv6 unicast address for a selected VLAN interface on the page for modifying VLAN interfaces, you must click the correct **Apply** button to submit the modification.

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.

To modify a VLAN interface:

1. From the navigation tree, select **Network** > **VLAN Interface**.
2. Click **Modify** to enter the page for modifying a VLAN interface.

Figure 149 Modifying a VLAN interface



3. Modify a VLAN interface as described in Table 45.
4. Click **Apply**.

Table 45 Configuration items

Item		Description
Select VLAN Interface		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.
Modify IPv4 Address	DHCP	Configure the way in which the VLAN interface gets an IPv4 address. Allow the VLAN interface to get 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 must set the mask length or enter a mask in dotted decimal notation format.
	BOOTP	
	Manual	
	Admin Status	Select **Up** or **Down** from the **Admin Status** list to bring up or shut down the selected VLAN interface. When the VLAN interface fails, shut down and then bring up the VLAN interface, which might restore the VLAN interface. By default, a VLAN interface is down if all Ethernet ports in the VLAN are down. Otherwise, the VLAN interface is up. When you set the admin status, follow these guidelines: • 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.

Item		Description
Modify IPv6 Address	Auto	Configure the way in which the VLAN interface gets an IPv6 link-local address. Select the **Auto** or **Manual** option: • **Auto**—The device automatically assigns a link-local address to 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.
	Manual	
	Admin Status	Select **Up** or **Down** from the **Admin Status** list to bring up or shut down the selected VLAN interface. When the VLAN interface fails, shut down and then enable the VLAN interface, which might restore the VLAN interface. By default, a VLAN interface is down if all Ethernet ports in the VLAN are down. Otherwise, the VLAN interface is up. When you set the admin status, follow these guidelines: • 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.
	Add IPv6 Unicast Address	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.
	EUI-64	Select the box to generate IPv6 site-local addresses or global unicast addresses in the 64-bit Extended Unique Identifier (EUI-64) format. If the **EUI-64** box is not specified, manually configured IPv6 site-local addresses or global unicast addresses are used.

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. However, 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 46 for voice traffic identification.

Table 46 The default OUI list

Number	OUI Address	Vendor
1	0003-6b00-0000	Cisco phone
2	00e0-7500-0000	Polycom phone

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."

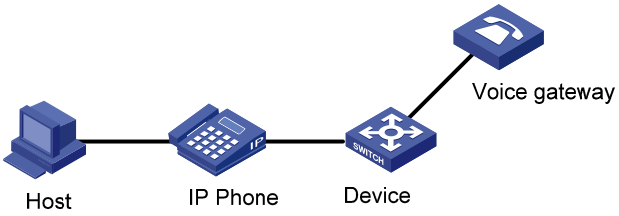
You can remove default OUI addresses and if needed, add them to the OUI list after their removal.

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:

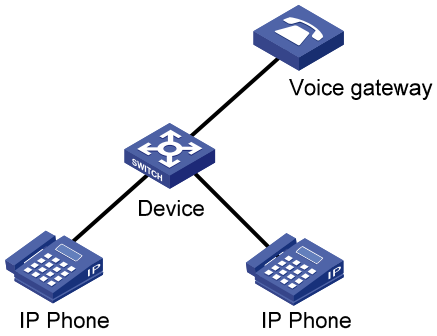
- **Automatic mode**—The system matches the source MAC addresses in the protocol packets (tagged packets) sent by the IP phone upon its power-on against the OUI list. If a match is found, the system automatically assigns the receiving port to a voice VLAN, issues ACL rules and configures the packet precedence. 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 150. 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 150 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 151. 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 151 Only IP phones access the network

Both modes forward tagged packets according to their tags.

Table 47 and Table 48 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 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 tagged voice traffic	Configuration requirements
Access	Manual	Configure the PVID of the port as the voice VLAN.
Trunk	Automatic and manual	In automatic mode, the PVID of the port cannot be the voice VLAN. In manual mode, 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, 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 48 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.

Hewlett Packard Enterprise recommends not transmitting 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 49 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	If the packet is a voice packet does not carry the voice VLAN tag or PVID tag, the packet is dropped. Otherwise, the packet is 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 8 OUI addresses. By default, the system is configured with two OUI addresses, as shown in Table 46.

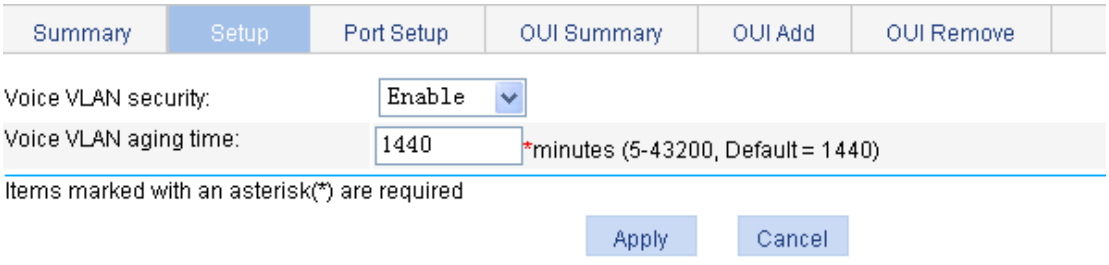
Recommended configuration procedure for a port in manual voice VLAN assignment mode

Step	Remarks
1. Configuring voice VLAN globally	(Optional.) Configure the voice VLAN to operate in security mode and configure the aging timer.
2. 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.
3. Adding OUI addresses to the OUI list	(Optional.) You can configure up to 8 OUI addresses. By default, the system is configured with the two OUI addresses shown in Table 46.

Configuring voice VLAN globally

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

Figure 152 Configuring voice VLAN



3. Configure the global voice VLAN settings as described in Table 50.
4. Click **Apply**.

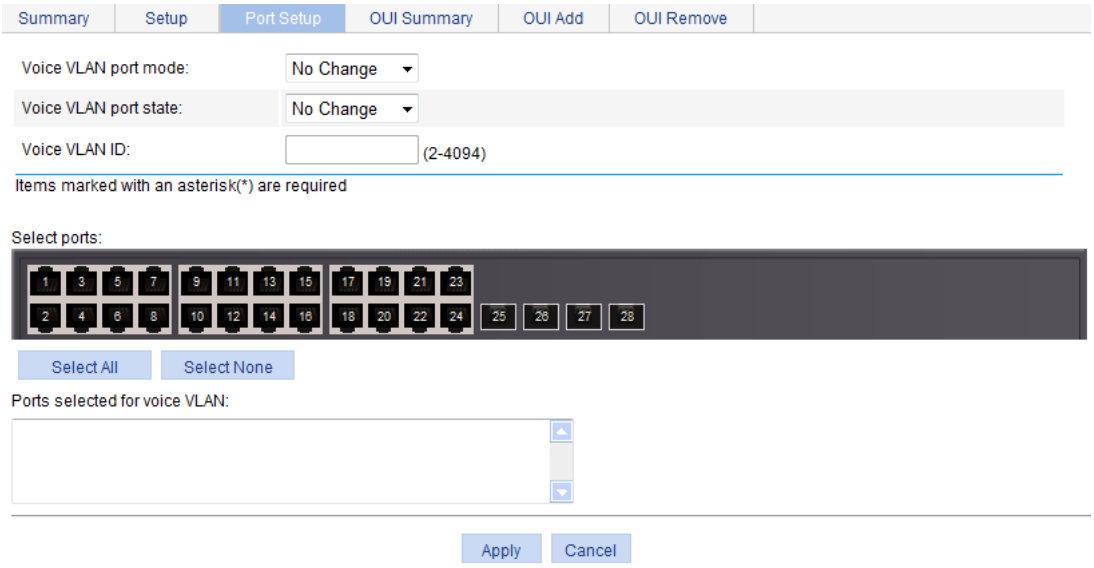
Table 50 Configuration items

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 153 Configuring voice VLAN on ports



3. Configure the voice VLAN function for ports as described in Table 51.
4. Click **Apply**.

Table 51 Configuration items

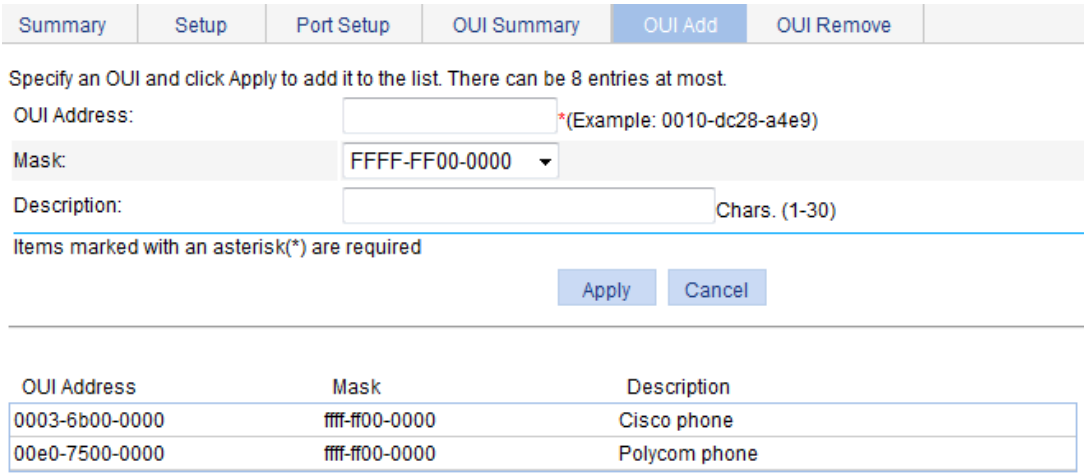
Item	Description
Voice VLAN port mode	Set the voice VLAN assignment mode of a port to: • **Auto**—Automatic voice VLAN assignment mode • **Manual**—Manual voice VLAN assignment mode
Voice VLAN port state	Select **Enable** or **Disable** in the list to enable or disable the voice VLAN function on the port.
Voice VLAN ID	Set the voice VLAN ID of a port when the voice VLAN port state is set to **Enable**.

Item	Description
Select Ports	Select the port on the chassis front panel. You can select multiple ports to configure them in bulk. The numbers of the selected ports will be displayed in the **Ports selected for voice VLAN** 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 154 Adding OUI addresses to the OUI list



3. Add an OUI address to the list as described in Table 52.
4. Click **Apply**.

Table 52 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

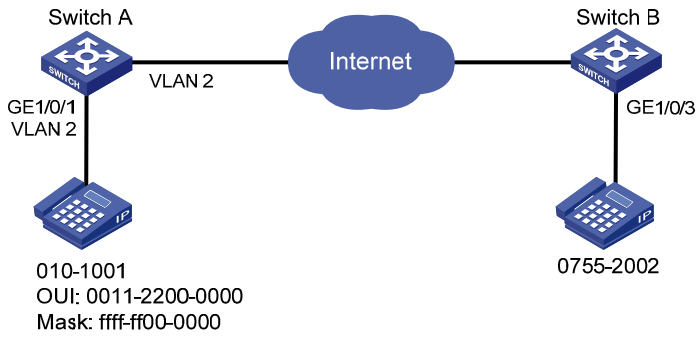
Configuring voice VLAN on a port in automatic voice VLAN assignment mode

Network requirements

As shown in Figure 155:

- 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**.

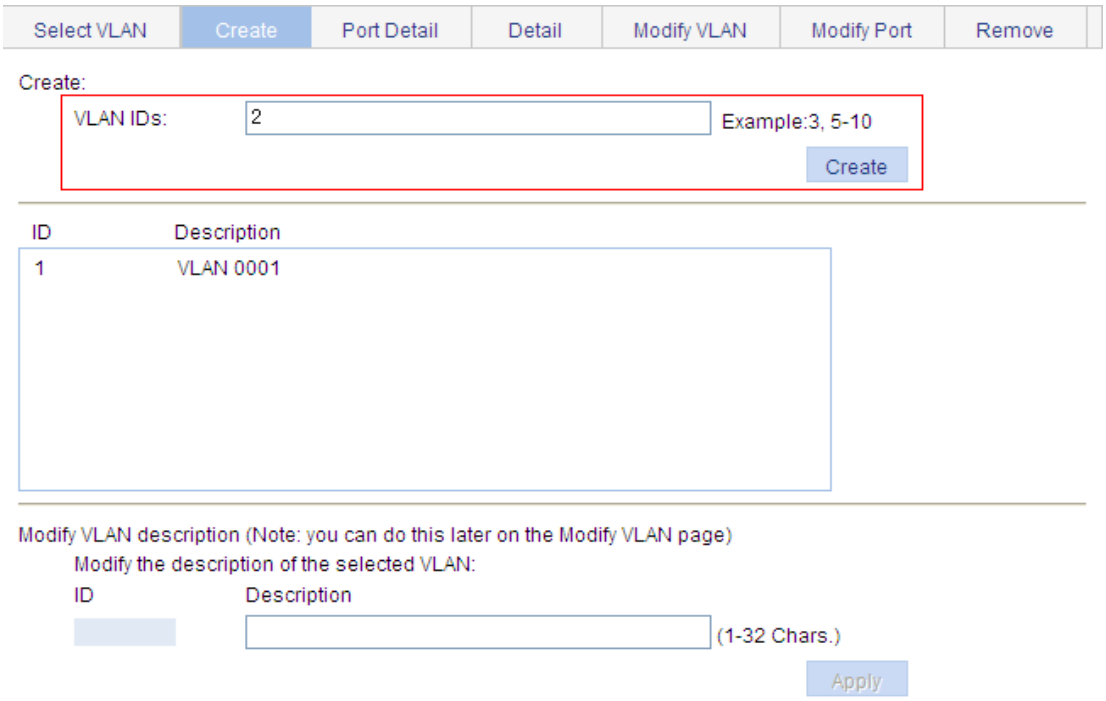
Figure 155 Network diagram



Configuring Switch A

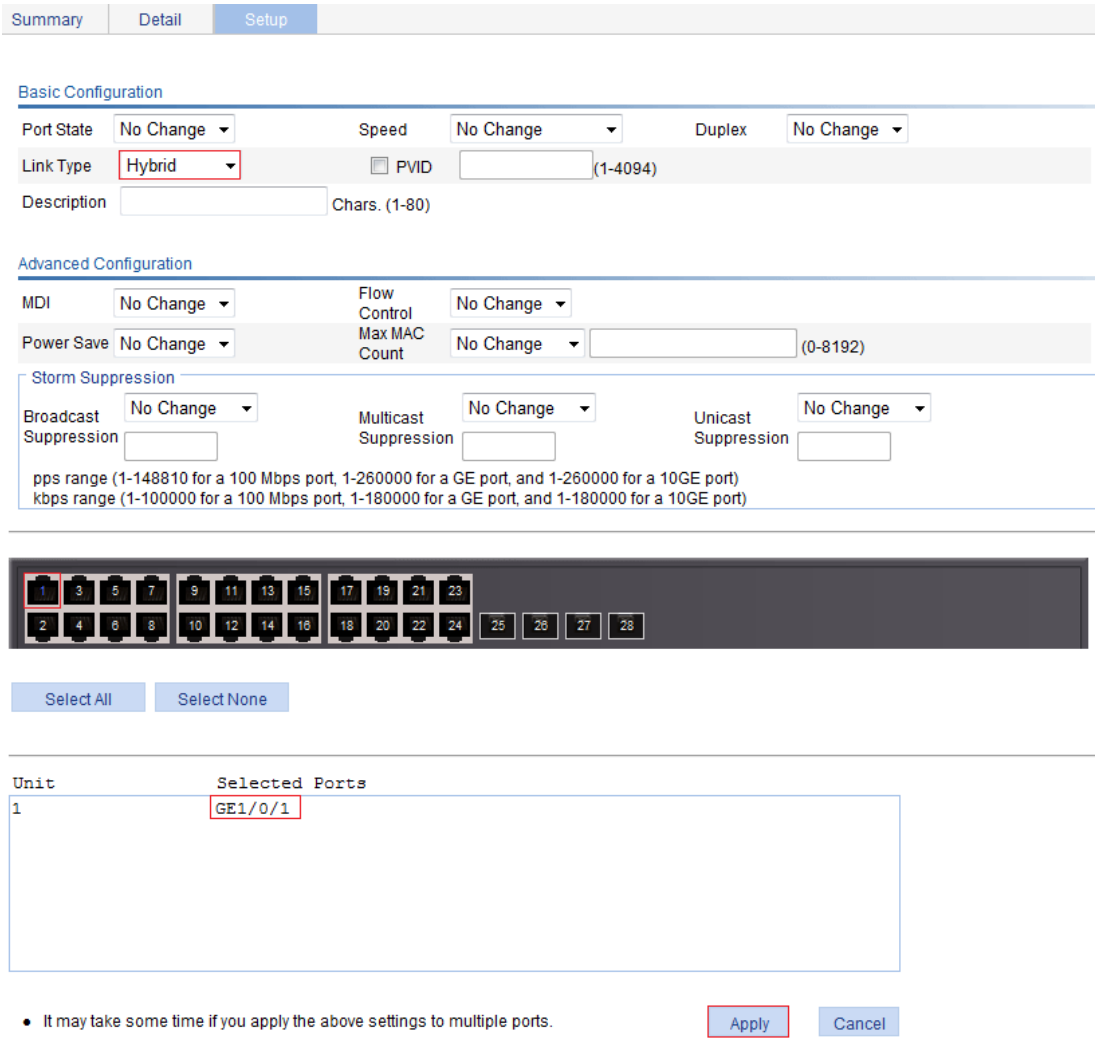
1. Create VLAN 2:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter VLAN ID 2.
   d. Click **Create**.

Figure 156 Creating VLAN 2



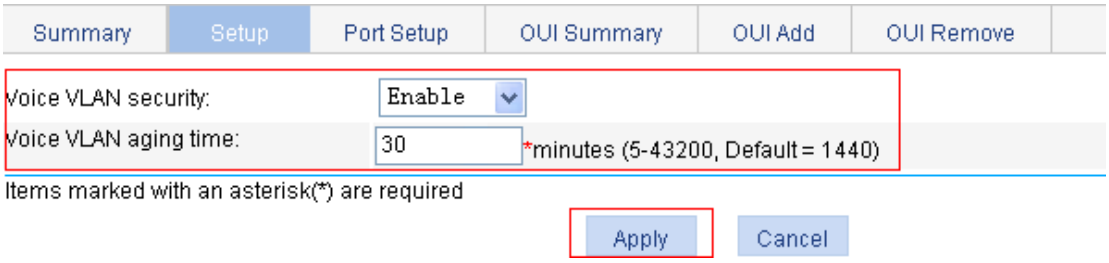
2. Configure GigabitEthernet 1/0/1 as a hybrid port:
   a. Select **Device** > **Port Management** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **Hybrid** from the **Link Type** list.
   d. Select GigabitEthernet 1/0/1 from the chassis front panel.
   e. Click **Apply**.

Figure 157 Configuring GigabitEthernet 1/0/1 as a hybrid port



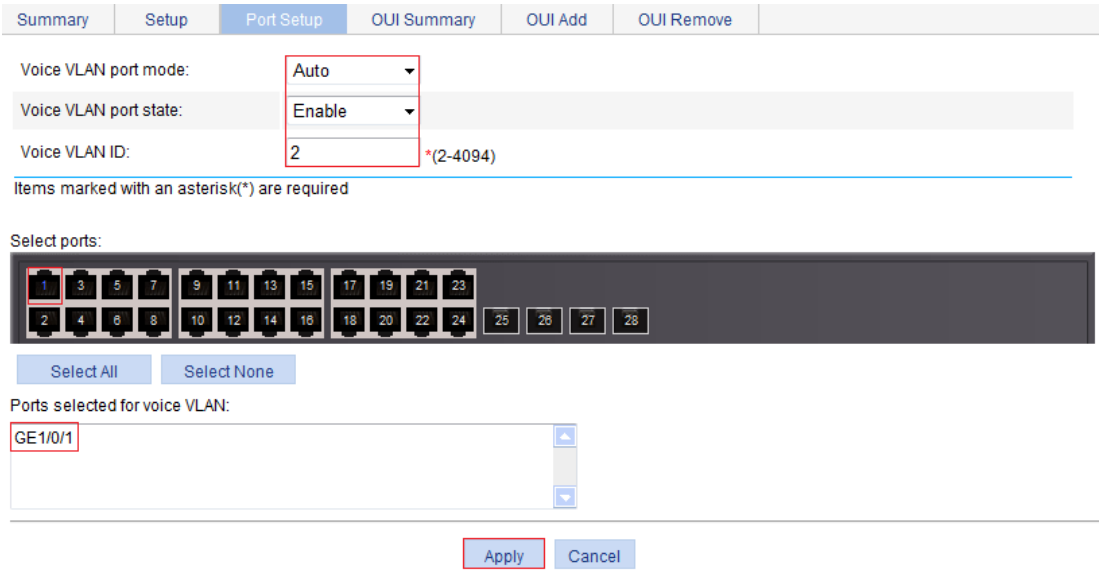
3. Configure the voice VLAN function globally:
   a. Select **Network** > **Voice VLAN** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **Enable** in the **Voice VLAN security** list.
   d. Set the voice VLAN aging timer to 30 minutes.
   e. Click **Apply**.

Figure 158 Configuring the voice VLAN function globally



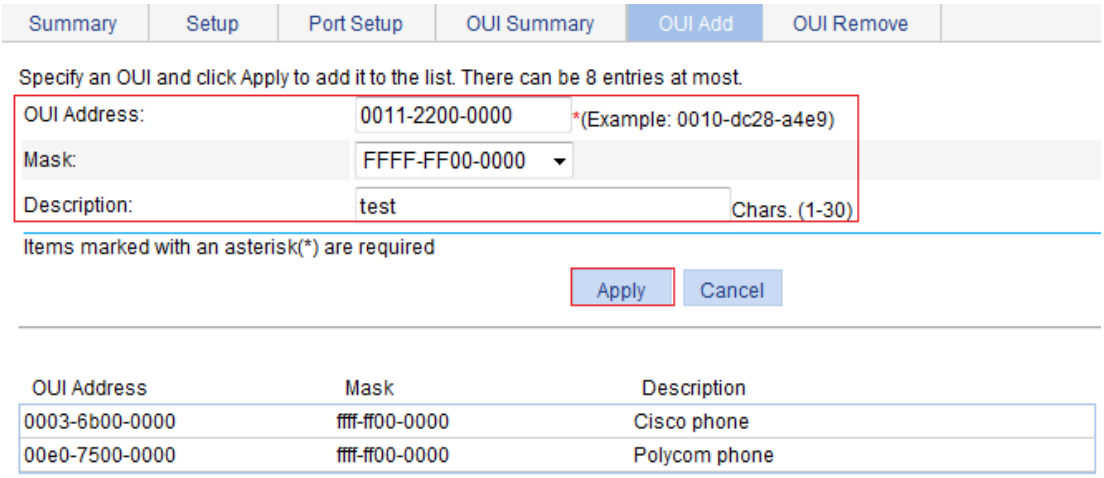
4. Configure voice VLAN on GigabitEthernet 1/0/1:
   a. Click the **Port Setup** tab.
   b. Select **Auto** in the **Voice VLAN port mode** list.
   c. Select **Enable** in the **Voice VLAN port state** list.
   d. Enter voice VLAN ID 2.
   e. Select GigabitEthernet 1/0/1 on the chassis front panel.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

Figure 159 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**.

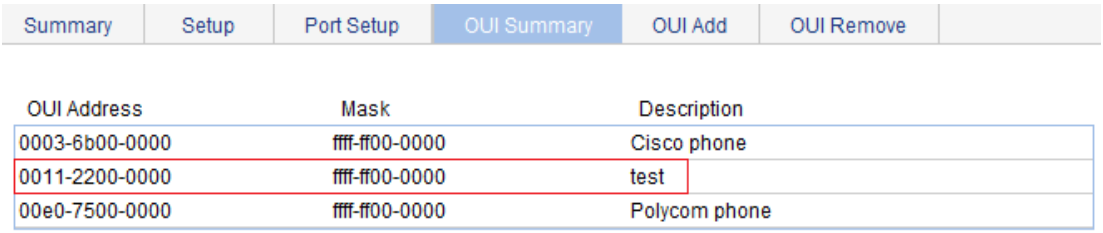
Figure 160 Adding OUI addresses to the OUI list



Verifying the configuration

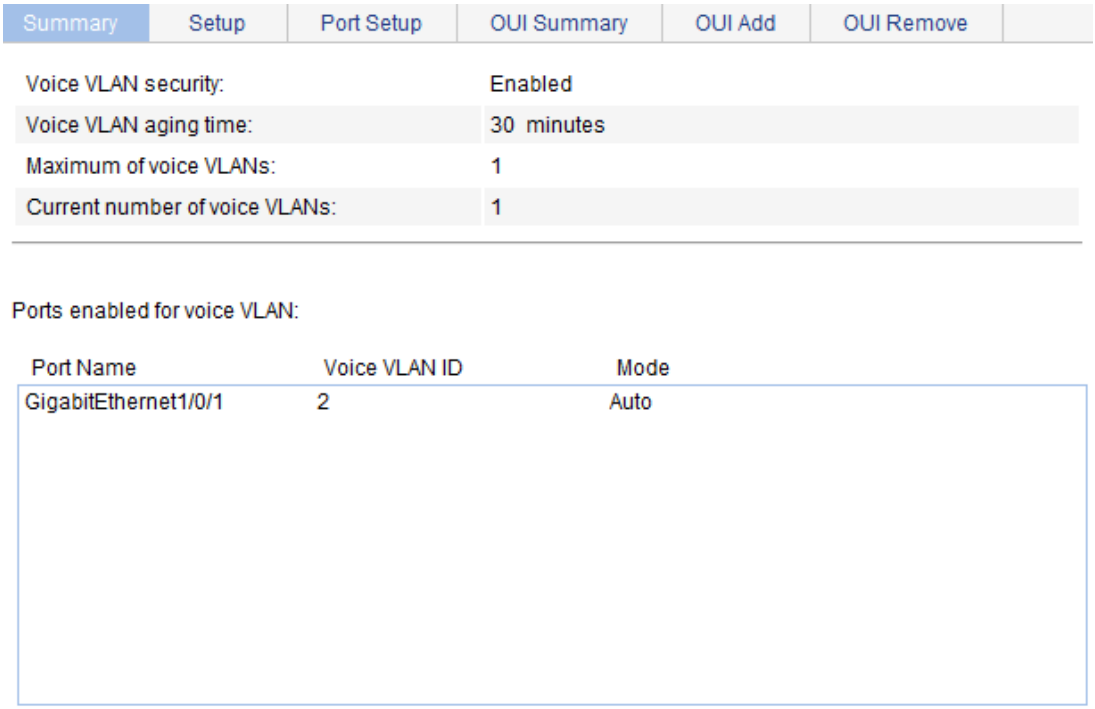
1. When the preceding configurations are completed, the **OUI Summary** tab is displayed by default, as shown in Figure 161. You can view the information about the newly-added OUI address.

   Figure 161 Displaying the current OUI list of the device



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

Figure 162 Displaying voice VLAN information



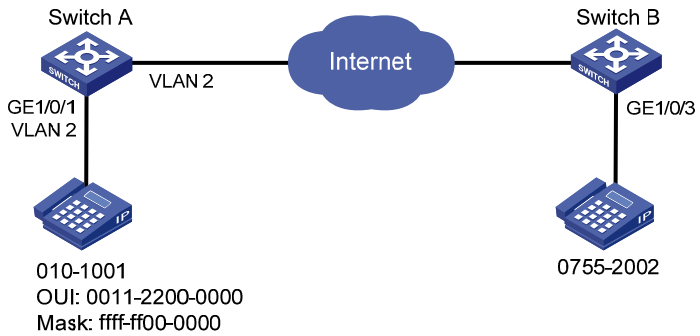
Configuring a voice VLAN on a port in manual voice VLAN assignment mode

Network requirements

As shown in Figure 163:

- 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**.

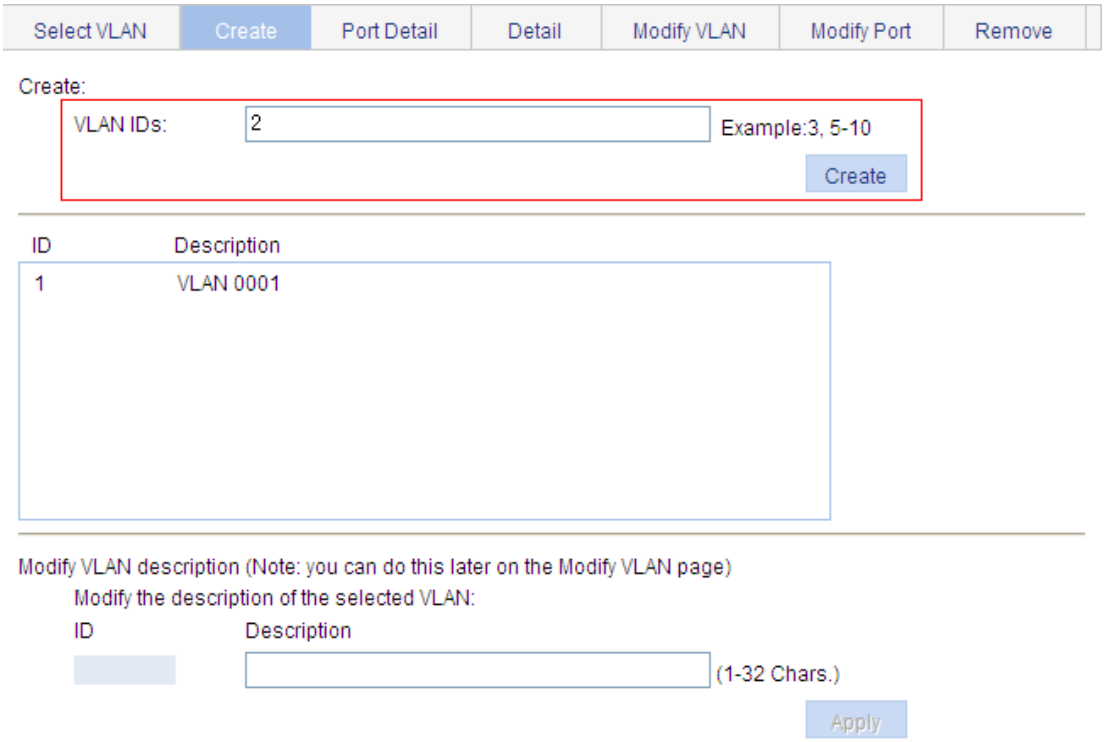
Figure 163 Network diagram



Configuring Switch A

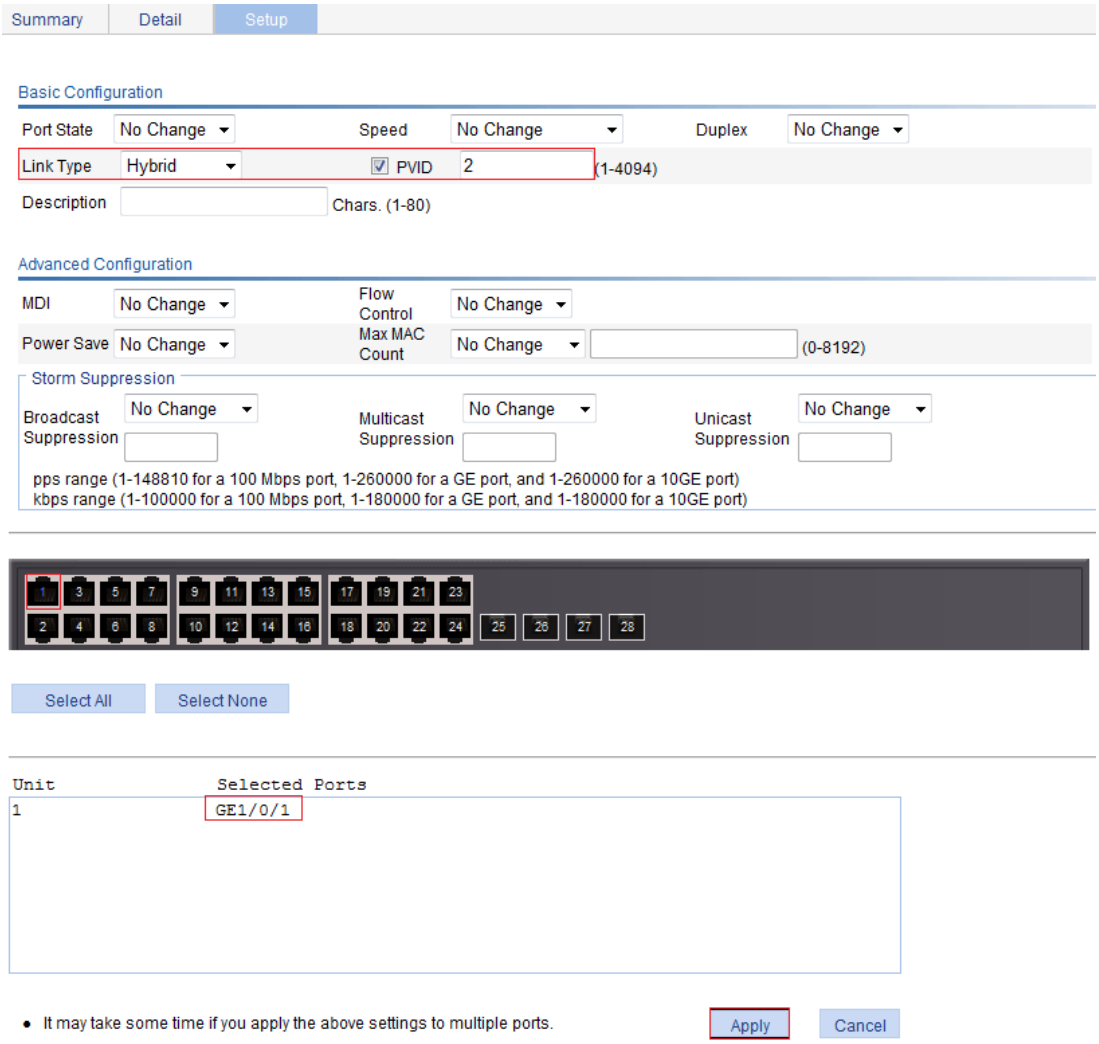
1. Create VLAN 2:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter VLAN ID 2.
   d. Click **Create**.

Figure 164 Creating VLAN 2



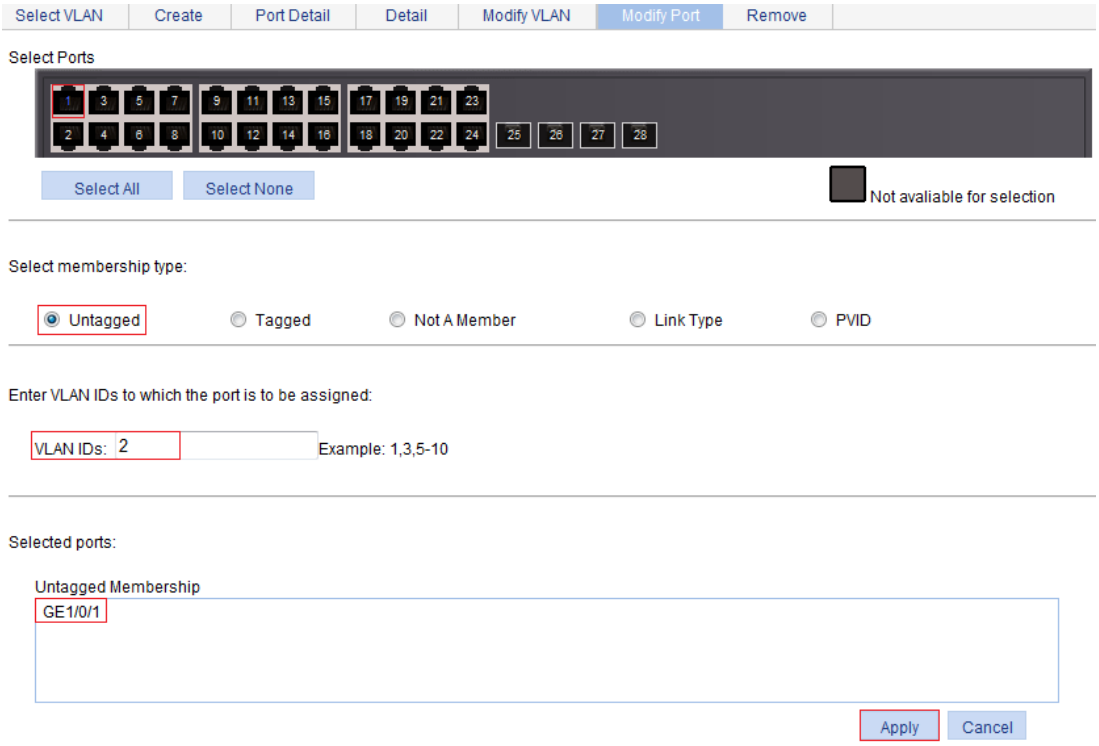
2. Configure GigabitEthernet 1/0/1 as a hybrid port and configure its PVID as VLAN 2:
   a. Select **Device** > **Port Management** from the navigation tree.
   b. Click the **Setup** tab.
   c. Select **Hybrid** from the **Link Type** list.
   d. Select the **PVID** box and enter 2 in the field.
  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

Figure 165 Configuring GigabitEthernet 1/0/1 as a hybrid port



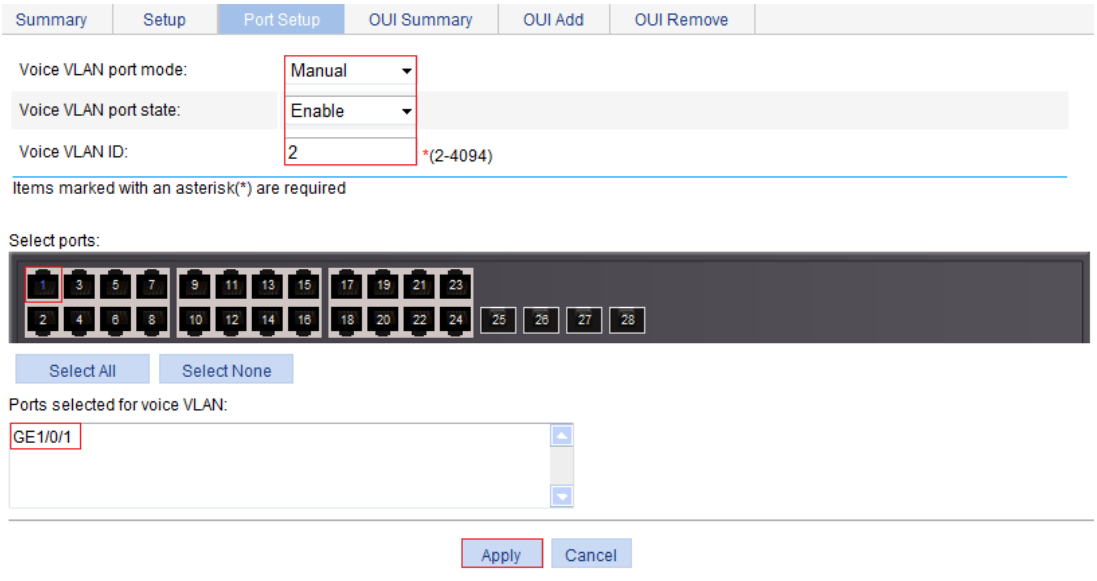
3. Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Modify Port** tab.
   c. Select GigabitEthernet 1/0/1 from the chassis front panel.
   d. Select the **Untagged** option.
   e. Enter VLAN ID 2.
   f. Click **Apply**.
      A configuration progress dialog box appears.
   g. After the configuration process is complete, click **Close**.

Figure 166 Assigning GigabitEthernet 1/0/1 to VLAN 2 as an untagged member



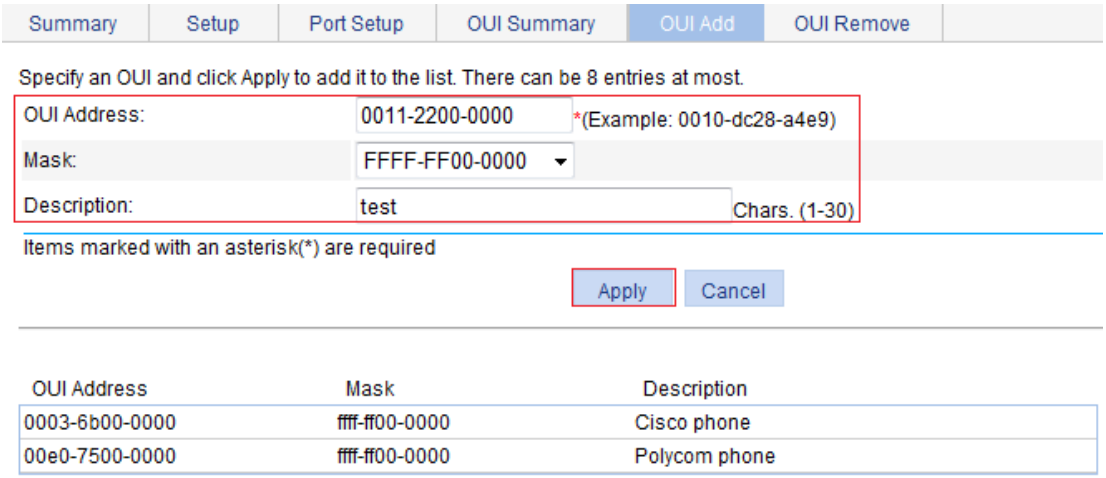
4. Configure voice VLAN on GigabitEthernet 1/0/1:
   a. Select **Network** > **Voice VLAN** from the navigation tree.
   b. Click the **Port Setup** tab.
   c. Select **Manual** in the **Voice VLAN port mode** list.
   d. Select **Enable** in the **Voice VLAN port state** list.
   e. Enter 2 in the **VLAN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

Figure 167 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**.

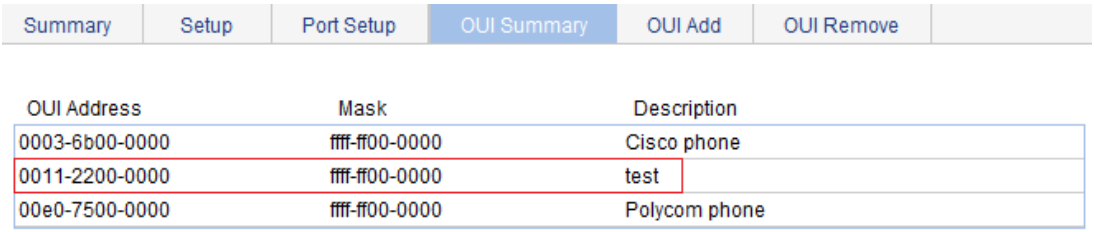
Figure 168 Adding OUI addresses to the OUI list



Verifying the configuration

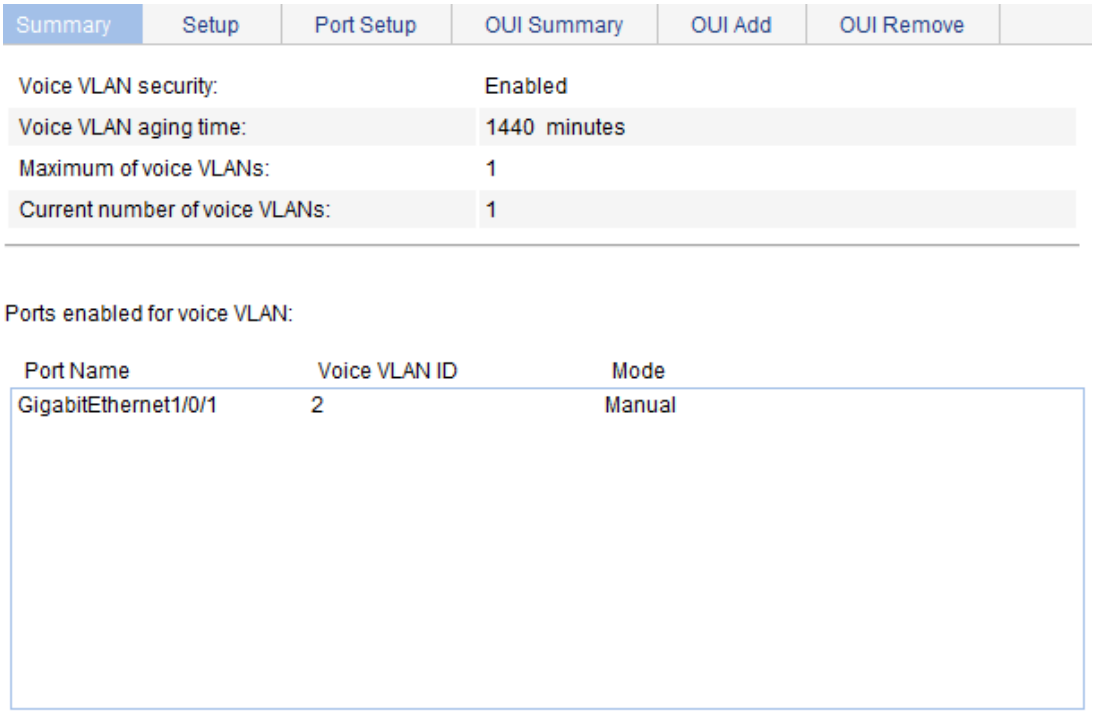
1. When the preceding configurations are complete, the **OUI Summary** tab is displayed by default, as shown in Figure 169. You can view the information about the newly-added OUI address.

Figure 169 Displaying the current OUI list of the device



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

Figure 170 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 the MAC address table

MAC address configurations related to interfaces apply to Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces only.

This document covers only the configuration of unicast MAC address entries, including static, dynamic, and blackhole entries.

Overview

To reduce single-destination packet flooding in a switched LAN, an Ethernet device uses a MAC address table to forward frames. This table describes from which port a MAC address (or host) can be reached. Upon receiving a frame, the device uses the destination MAC address of the frame to look for a match in the MAC address table. If a match is found, the device forwards the frame out of the outgoing interface in the matching entry. If no match is found, the device floods the frame out of all but the incoming port.

How a MAC address 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 (for example, Port A), 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.
   - If an entry is found, the device updates the entry.
   - If no entry is found, the device adds an entry for MAC-SOURCE and Port A.
3. When the device receives a frame destined for MAC-SOURCE after learning this source MAC address, the device finds the MAC-SOURCE entry in the MAC address table and forwards the frame out of 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.

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 with which the real MAC address is associated, 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 manually add MAC address entries to the MAC address table of the device to bind specific user devices to the port.

Types of MAC address 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. They are configured for filtering out frames with specific source or destination MAC addresses. For example, to block all frames destined for a specific user for security concerns, you can configure the MAC address of this user as a blackhole MAC address entry.

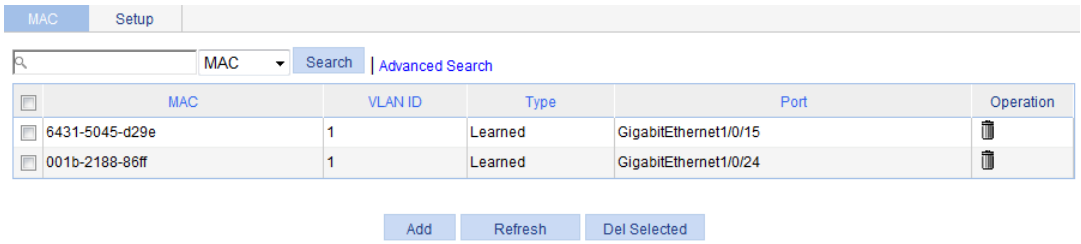
A static or blackhole MAC address entry can overwrite a dynamic MAC address entry, but not vice versa.

Displaying and configuring MAC address entries

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

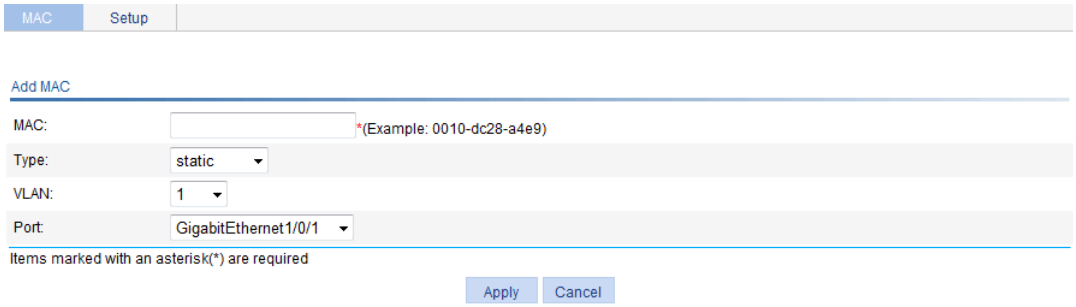
   The **MAC** tab automatically appears, which shows all the MAC address entries on the device.

   Figure 171 The MAC tab



2. Click **Add** in the bottom to enter the page for creating MAC address entries.

   Figure 172 Creating a MAC address entry



3. Configure a MAC address entry as described in Table 53.
4. Click **Apply**.

Table 53 Configuration items

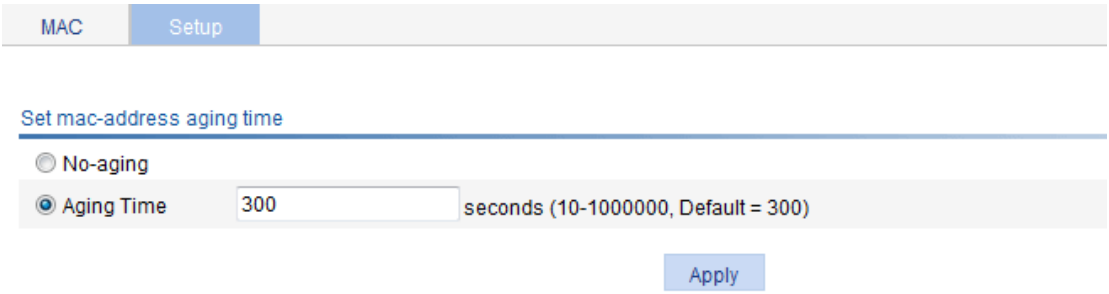
Item	Description
MAC	Set the MAC address to be added.
Type	Set the type of the MAC address entry: • **Static**—Static MAC address entries that never age out. • **Dynamic**—Dynamic MAC address entries that will age out. • **Blackhole**—Blackhole MAC address entries that never age out. The **MAC** tab (see Figure 171) displays the following types of MAC address entries: • **Config static**—Static 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 ID	Set the ID of the VLAN to which the MAC address belongs.

Item	Description
Port	Set the port to which the MAC address belongs. This port must belong to the specified VLAN.

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.

   Figure 173 Setting the aging time for MAC address entries



3. Configure the aging time for MAC address entries as described in Table 54.
4. Click **Apply**.

Table 54 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 table configuration example

Network requirements

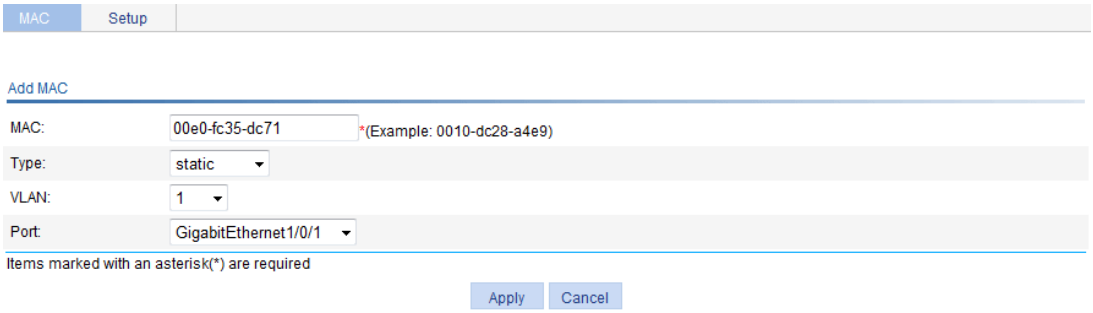
Use the Web-based NMS to configure the MAC address table of the device. Add a static MAC address 00e0-fc35-dc71 under GigabitEthernet 1/0/1 in VLAN 1.

Creating a static MAC address entry

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

   By default, the **MAC** tab is displayed.
2. Click **Add**.
3. Configure a MAC address entry:
   a. Type MAC address **00e0-fc35-dc71**.
   b. Select **static** from the **Type** list.
   c. Select **1** from the **VLAN** list.
   d. Select **GigabitEthernet1/0/1** from the **Port** list.
4. Click **Apply**.

Figure 174 Creating a static MAC address entry



Configuring MSTP

Overview

Spanning tree protocols eliminate loops in a physical link-redundant network by selectively blocking redundant links and putting them in a standby state.

The recent versions of STP include the Rapid Spanning Tree Protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP).

Introduction to STP

STP was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a LAN. Networks often have redundant links as backups in case of failures, but loops are a very serious problem. Devices running STP 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.

In the narrow sense, STP refers to 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. This chapter uses BPDUs to represent all types of spanning tree 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.

STP uses the following types of BPDUs:

- **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.

Configuration BPDUs contain sufficient information for the network devices to complete spanning tree calculation. Important fields in a configuration BPDU include the following:

- **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 denoted by the root identifier from the transmitting bridge.
- **Designated bridge ID**—Consisting of the priority and MAC address of the designated bridge.
- **Designated port ID**—Consisting of the priority and global port number of the designated port.
- **Message age**—Age of the configuration BPDU while it propagates in the network.
- **Max age**—Maximum age of the configuration BPDU stored on a device.
- **Hello time**—Configuration BPDU transmission interval.
- **Forward delay**—Delay that STP bridges use to transit port state.

The descriptions and examples in this chapter only use 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).

Basic concepts in STP

Root bridge

A tree network must have a root bridge. The entire network contains only one root bridge, and all the other bridges in the network are called "leaf nodes". The root bridge is not permanent, but can change with changes of the network topology.

Upon initialization of a network, each device generates and periodically sends configuration BPDUs, with itself as the root bridge. After network convergence, only the root bridge generates and periodically sends configuration BPDUs. The other devices only forward the BPDUs.

Root port

On a non-root bridge, the port nearest to the root bridge is the root port. The root port communicates with the root bridge. Each non-root bridge has only one root port. The root bridge has no root port.

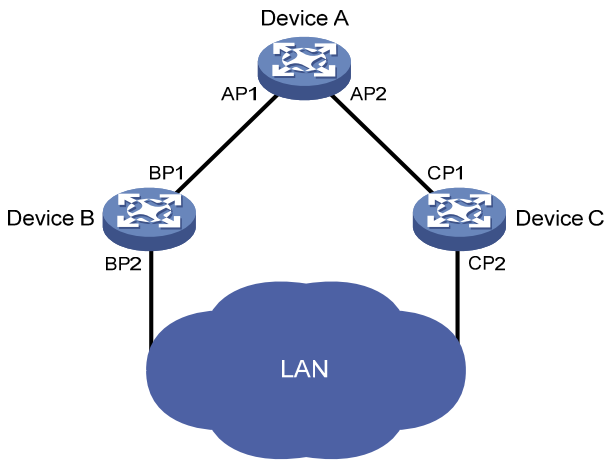
Designated bridge and designated port

Classification	Designated bridge	Designated port
For a device	Device directly connected with the local device and responsible for forwarding BPDUs to the local device.	Port through which the designated bridge forwards BPDUs to the local device.
For a LAN	Device responsible for forwarding BPDUs to this LAN segment.	Port through which the designated bridge forwards BPDUs to this LAN segment.

As shown in Figure 175, Device B and Device C are connected to the LAN. 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.
- 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 175 Designated bridges and designated ports



Path cost

Path cost is a reference value used for link selection in STP. STP calculates path costs to select the most robust links and block redundant links that are less robust, to prune the network into a loop-free tree.

All the ports on the root bridge are designated ports.

Calculation process of the STP algorithm

The spanning tree calculation process described in the following sections is a simplified process for example only.

Calculation process

The STP algorithm uses the following calculation process:

1. Network initialization.

   Upon initialization of a device, each port generates a BPDU with the port as the designated port, the device as the root bridge, 0 as the root path cost, and the device ID as the designated bridge ID.

2. Root bridge selection.

   Initially, each STP-enabled device on the network assumes itself to be the root bridge, with its own device ID as the root bridge 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.

3. Root port and designated ports selection on the non-root bridges.

Step	Description
1	A non-root-bridge device regards the port on which it received the optimum configuration BPDU as the root port. Table 55 describes how the optimum configuration BPDU is selected.
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 other 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 whose port role will be determined, and acts depending on the result of the comparison: • If the calculated configuration BPDU is superior, the device considers this port as the designated port, replaces the configuration BPDU on the port with the calculated configuration BPDU, and periodically sends the calculated configuration BPDU. • 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 it cannot send BPDUs or forward any data.

When the network topology is stable, only the root port and designated ports forward user traffic. Other ports are all in the blocked state to receive BPDUs but not to forward BPDUs or user traffic.

Table 55 Selecting the optimum configuration BPDU

Step	Actions
1	Upon receiving a configuration BPDU on a port, the device compares the priority of the received configuration BPDU with that of the configuration BPDU generated by the port. It takes one of the following actions: • If the former priority is lower, the device discards the received configuration BPDU and keeps the configuration BPDU the port generated. • If the former priority is higher, 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.

The following are the principles of configuration BPDU comparison:

a. The configuration BPDU with the lowest root bridge ID has the highest priority.

b. 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.

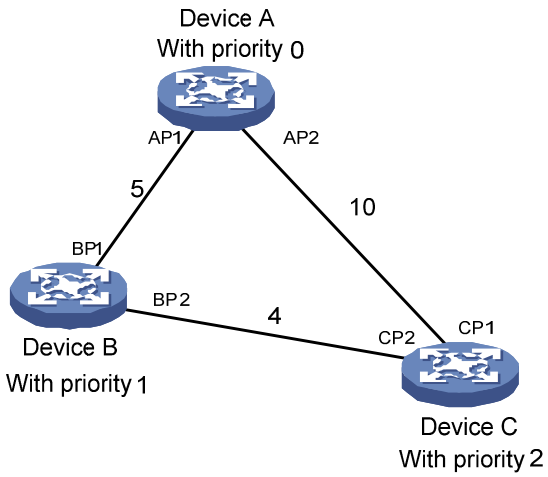
c. If all configuration BPDUs have the same root bridge ID and S value, their designated bridge IDs, designated port IDs, and the IDs of the receiving ports are compared in sequence. The configuration BPDU that contains a smaller designated bridge ID, designated port ID, or receiving port ID is selected.

A tree-shape topology forms when the root bridge, root ports, and designated ports are selected.

Example of STP calculation

Figure 176 provides an example showing how the STP algorithm works.

Figure 176 STP network



As shown in Figure 176, the priority values of Device A, Device B, and Device C are 0, 1, and 2, and the path costs of links among the three devices are 5, 10, and 4, respectively.

1. Device state initialization.

In Table 56, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

Table 56 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}

2. Configuration BPDUs comparison on each device.

   In Table 57, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

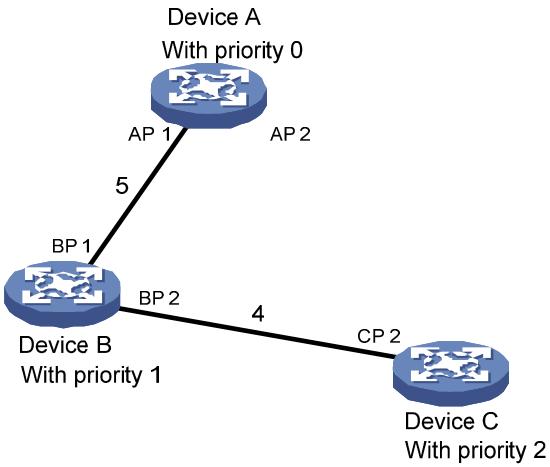
Table 57 Comparison process and result on each device

Device	Comparison process	Configuration BPDU on ports 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 it 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 it 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 it starts sending out configuration BPDUs periodically.	• AP1: {0, 0, 0, AP1} • AP2: {0, 0, 0, AP2}
Device B	• Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and it 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 it discards the received configuration BPDU.	• BP1: {0, 0, 0, AP1} • BP2: {1, 0, 1, BP2}
	• Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. • Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. • Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically.	• Root port BP1: {0, 0, 0, AP1} • Designated port BP2: {0, 5, 1, BP2}

Device	Comparison process	Configuration BPDU on ports after comparison
Device C	• Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and it 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 it updates the configuration BPDU of CP2.	• CP1: {0, 0, 0, AP2} • CP2: {1, 0, 1, BP2}
	After comparison: • The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. • Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU.	• Root port CP1: {0, 0, 0, AP2} • Designated port CP2: {0, 10, 2, CP2}
	• Then, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its own configuration BPDU, Device C launches a BPDU update process. • At the same time, port CP1 receives periodic configuration BPDUs from Device A. Device C does not launch an update process after comparison.	• CP1: {0, 0, 0, AP2} • CP2: {0, 5, 1, BP2}
	After comparison: • Because the root path cost of CP2 (9) (root path cost of the BPDU (5) plus path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. • After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new event, for example, the link from Device B to Device C going down.	• Blocked port CP2: {0, 0, 0, AP2} • Root port CP2: {0, 5, 1, BP2}

After the comparison processes described in Table 57, a spanning tree with Device A as the root bridge is established, and the topology is as shown in Figure 177.

Figure 177 The final calculated spanning tree



The configuration BPDU forwarding mechanism of STP

The configuration BPDUs of STP are forwarded according to 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 the root port 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 it starts a timer to time the configuration BPDU while sending 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 its own configuration BPDU in response.
- If a path becomes faulty, the root port on this path no longer receives new configuration BPDUs and the old configuration BPDUs will be discarded because of timeout. The device generates configuration BPDUs with itself as the root and sends the BPDUs and TCN BPDUs. This triggers a new spanning tree calculation process to establish a new path to restore the network connectivity.

However, the newly calculated configuration BPDU cannot 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 might occur.

STP timers

STP calculation involves the following timers:

- **Forward delay**—The delay time for device state transition. A path failure can cause spanning tree recalculation 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 immediately, 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 they transit to the forwarding state, which makes sure the new configuration BPDU has propagated throughout the network.
- **Hello time**—The time interval at which a device sends hello packets to the neighboring devices to make sure the paths are fault-free.
- **Max age**—A parameter used to determine whether a configuration BPDU held by the device has expired. The device discards the BPDU if the max age is exceeded.

Introduction to RSTP

Developed based on the 802.1w standard of IEEE, RSTP is an optimized version of STP. It achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much faster than STP.

If the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data, a newly elected RSTP root port rapidly enters the forwarding state.

A newly elected RSTP designated port rapidly enters the forwarding state if it is an edge port (a port that directly connects to a user terminal rather than to another network device or a shared LAN segment) or it connects to a point-to-point link. Edge ports directly enter the forwarding state. Connecting to a point-to-point link, a designated port enters the forwarding state immediately after the device receives a handshake response from the directly connected device.

Introduction to MSTP

MSTP overcomes the following STP and RSTP limitations:

- **STP limitations**—STP does not support rapid state transition of ports. A newly elected port must wait twice the forward delay time before it transits to the forwarding state, even if it connects to a point-to-point link or is an edge port.
- **RSTP limitations**—Although RSTP enables faster network convergence than STP, RSTP fails to provide load balancing among VLANs. As with STP, all RSTP bridges in a LAN share one spanning tree and forward packets from all VLANs along this spanning tree.

MSTP features

Developed based on IEEE 802.1s, MSTP overcomes the limitations of STP and RSTP. In addition to supporting rapid network convergence, it provides a better load sharing mechanism for redundant links by allowing data flows of different VLANs to be forwarded along separate paths.

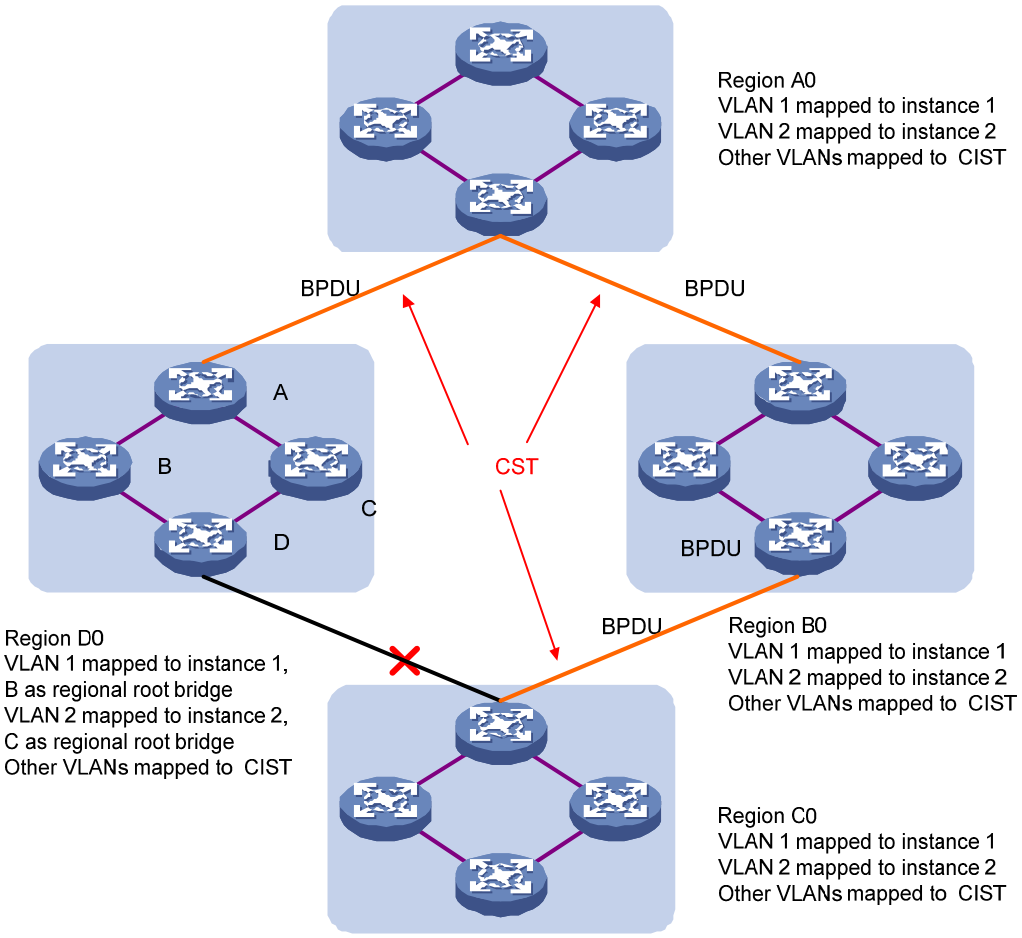
MSTP provides the following features:

- MSTP divides a switched network into multiple regions, each of which contains multiple spanning trees that are independent of one another.
- MSTP supports mapping VLANs to spanning tree instances by means of a VLAN-to-instance mapping table. MSTP can reduce communication overheads and resource usage by mapping multiple VLANs to one instance.
- MSTP prunes a loop network into a loop-free tree, which avoids proliferation and endless cycling of packets in a loop network. In addition, it supports load balancing of VLAN data by providing multiple redundant paths for data forwarding.
- MSTP is compatible with STP and RSTP.

MSTP basic concepts

Figure 178 shows a switched network that comprises four MST regions, each MST region comprising four MSTP devices.

Figure 178 Basic concepts in MSTP



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 with one another.

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region. In Figure 178, the switched network comprises four MST regions, MST region A0 through MST region D0, 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 a range of VLANs. Each spanning tree is referred to as a "multiple spanning tree instance (MSTI)".

In Figure 178, multiple MSTIs can exist in each MST region, each MSTI corresponding to the specified VLANs.

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 178, the VLAN-to-instance mapping table of region A0 is: VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to CIST. MSTP achieves load balancing by means of the VLAN-to-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 red lines in Figure 178 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 178, the CIST has a section in each MST region, and this section is the IST in the respective MST region.

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 178, the ISTs in all MST regions plus the inter-region CST constitute the CIST of the entire network.

Regional root bridge

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

As shown in Figure 178, the regional root of MSTI 1 in region D0 is device B, and that of MSTI 2 is device C.

Common root bridge

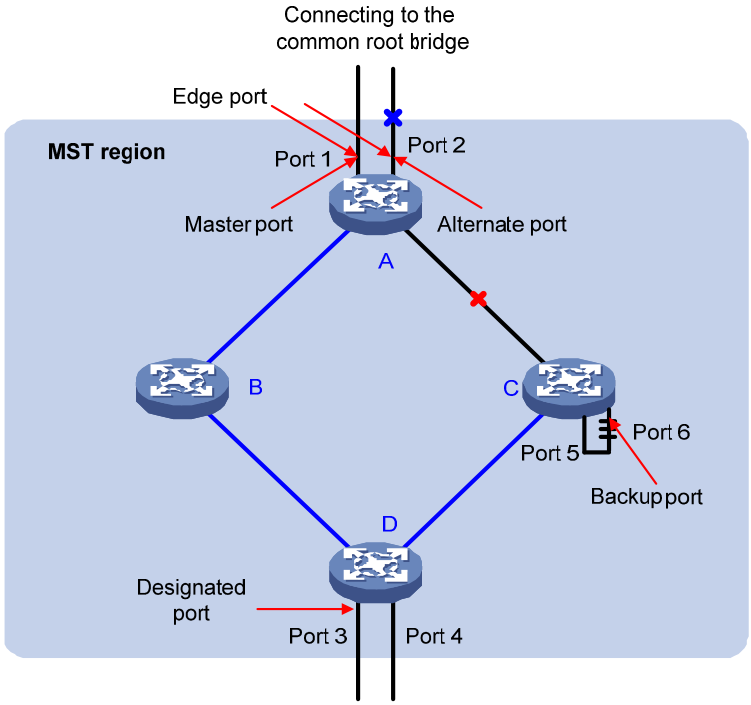
The common root bridge is the root bridge of the CIST.

In Figure 178, for example, the common root bridge is a device in region A0.

Port roles

A port can play different roles in different MSTIs. As shown in Figure 179, an MST region has device A, device B, device C, and device D. Port 1 and port 2 of device A are connected to the common root bridge, port 5 and port 6 of device C form a loop, and port 3 and port 4 of device D are connected downstream to the other MST regions.

Figure 179 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.
- **Master port**—Serves as 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.
- **Alternate port**—Serves as 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**—Serves as 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 connected, so the device blocks one of the ports. The blocked port acts as the backup.
- **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 learns MAC addresses and forwards user traffic.
- **Learning**—The port learns MAC addresses but does not forward user traffic.
- **Discarding**—The port does not learn MAC addresses or forwards user traffic.

A port can have different port states in different MSTIs. A port state is not exclusively associated with a port role. Table 58 lists the port states supported by each port role. (A check mark [√] indicates that the port state is available for the corresponding port role, and a dash [—] indicates that the port state is not available for the corresponding port role.)

Table 58 Ports states supported by different port roles

Port state	Port role				
	Root port/master port	Designated port	Boundary port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

How MSTP works

MSTP divides an entire Layer 2 network into multiple MST regions, which are connected by a calculated CST. Inside an MST region, multiple spanning trees, called MSTIs, are calculated. Among these MSTIs, MSTI 0 is the CIST.

Similar to RSTP, MSTP uses configuration BPDUs to calculate spanning trees. An important difference is that an MSTP BPDU carries the MSTP configuration of the bridge from which the 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. 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-instance mappings. For each spanning tree, MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP/RSTP. For more information, see "Calculation process of the STP algorithm"

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.

MSTP implementation 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.
- Support for the hot swapping of interface boards and switchover of the active and standby main boards.

Protocols and standards

MSTP is documented in the following protocols and standards:

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

Configuration guidelines

When you configure MSTP, follow these guidelines:

- Two or more spanning tree devices belong to the same MST region only if they are configured to have the same MST region name, MST region level, and the same VLAN-to-instance mapping entries in the MST region, and they are connected through a physical link.
- If two or more devices are selected as the root bridge in a spanning tree at the same time, the device with the lowest MAC address is chosen.
- If BPDU guard is disabled, a port set as an edge port becomes a non-edge port again if it receives a BPDU from another port. To restore its port role as an edge port, you must restart the port.
- If a port directly connects to a user terminal, configure it as an edge port and enable BPDU guard for it. This enables the port to quickly transit to the forwarding state when ensuring network security.

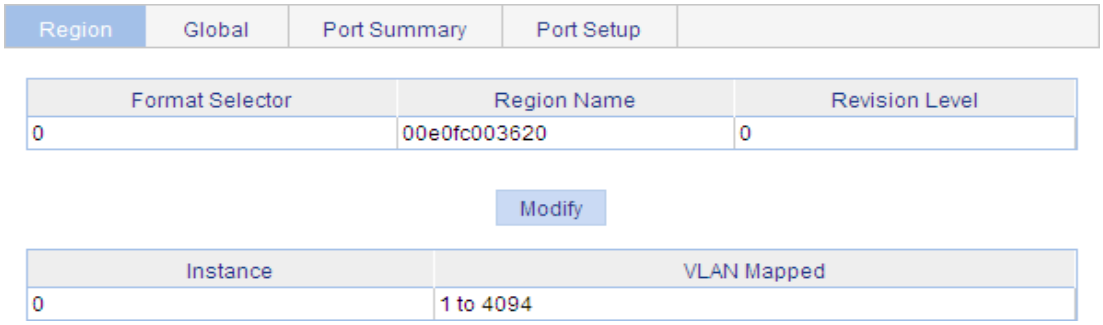
Recommended MSTP configuration procedure

Step	Remarks
1. Configuring an MST region.	Optional. Configure the MST region-related parameters and VLAN-to-instance 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. By default, STP is enabled globally. 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

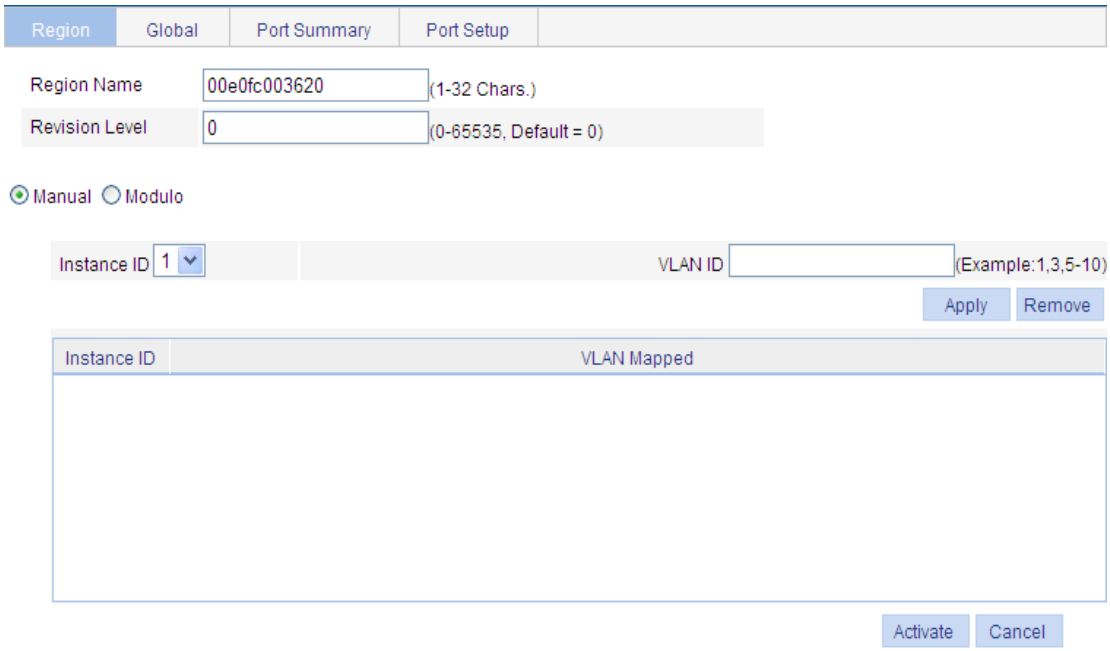
1. From the navigation tree, select **Network** > **MSTP**.
   By default, the **Region** tab is displayed.

Figure 180 MST region



2. Click **Modify**.

Figure 181 Configuring an MST region



3. Configure the MST region information as described in Table 59, and click **Apply**.

Table 59 Configuration items

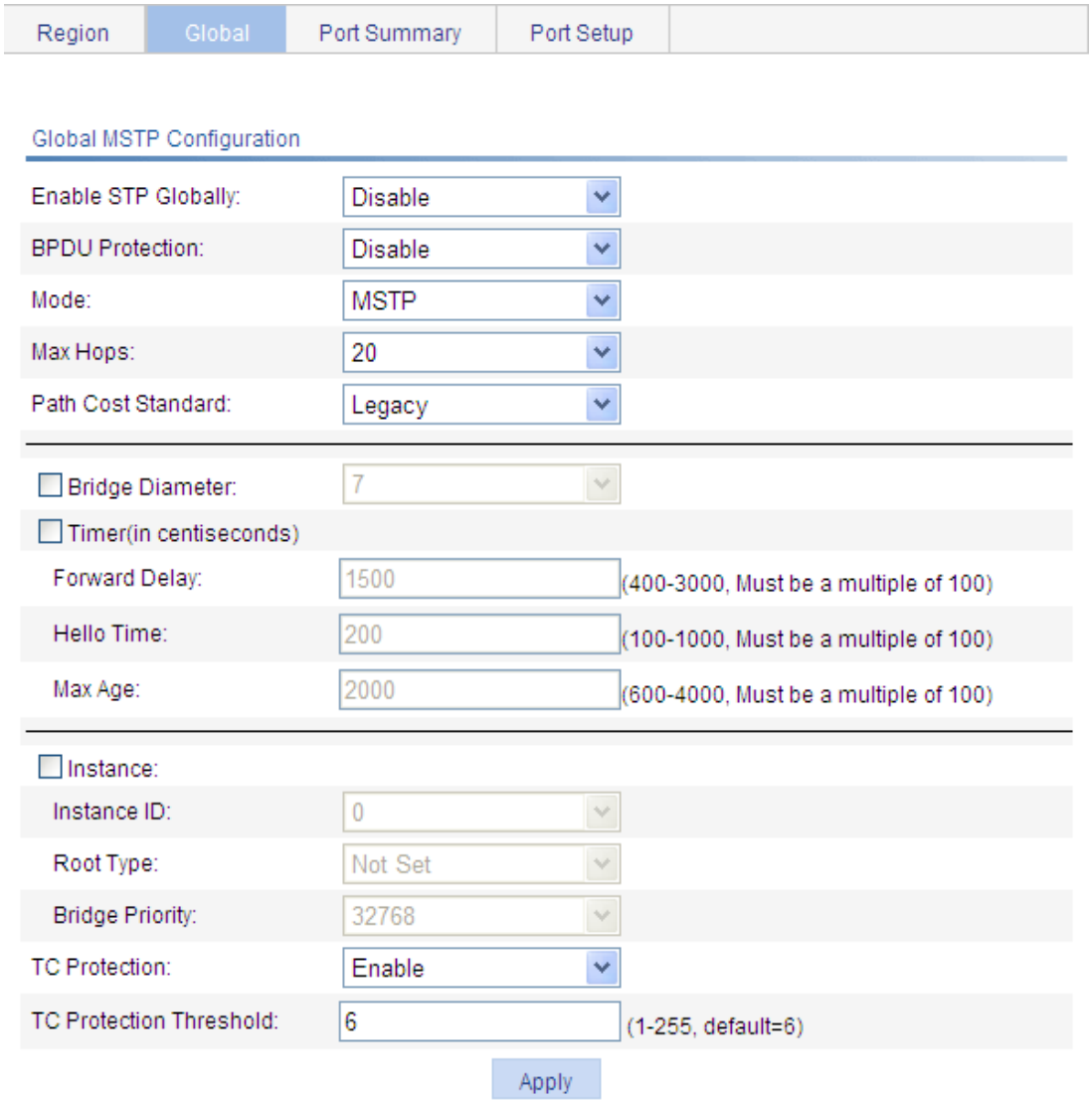
Item	Description
Region Name	MST region name. The MST region name is the bridge MAC address of the device by default.
Revision Level	Revision level of the MST region.
Manual (Instance ID and VLAN ID)	Manually add VLAN-to-instance mappings. Click **Apply** to add the VLAN-to-instance mapping entries to the list.
Modulo	The device automatically maps 4094 VLANs to the corresponding MSTIs based on the modulo value.

4. Click **Activate**.

Configuring MSTP globally

1. From the navigation tree, select **Network** > **MSTP**.
2. Click the **Global** tab.

Figure 182 Configuring MSTP globally



3. Configure the global MSTP configuration as described in Table 60, and then click **Apply**.

Table 60 Configuration items

Item	Description
Enable STP Globally	Selects whether to enable STP globally. Other MSTP configurations take effect only after you enable STP globally.
BPDU Guard	Selects whether to enable BPDU guard. BPDU guard can protect the device from malicious BPDU attacks, making the network topology stable.

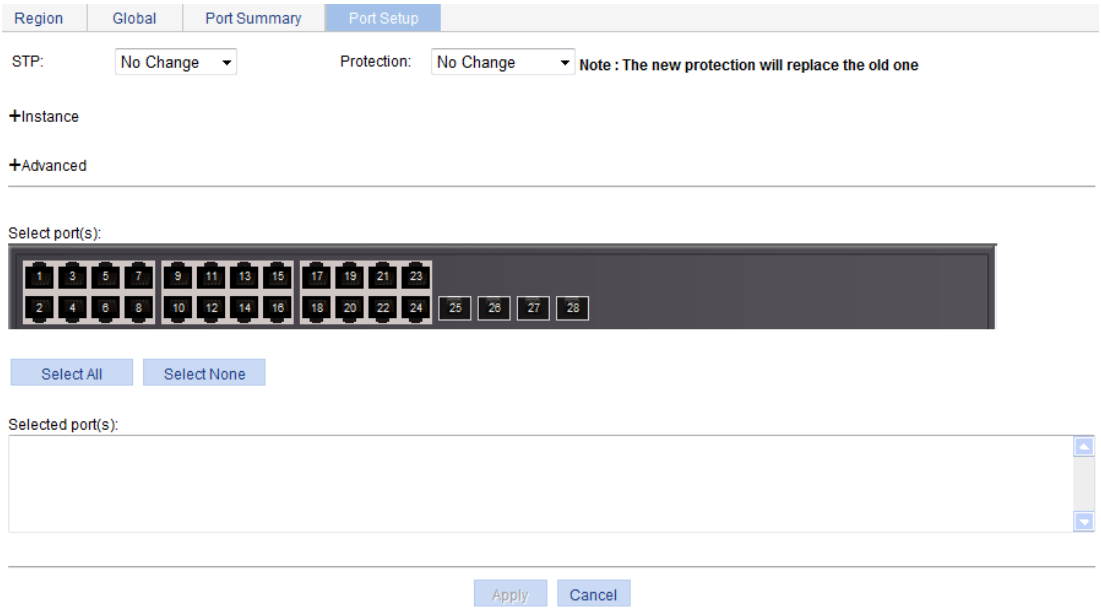
Item	Description
Mode	Sets the operating mode of STP: • **STP**—Each port on a device sends out STP BPDUs. • **RSTP**—Each port on a device sends out RSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP. • **MSTP**—Each port on a device sends out MSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP.
Max Hops	Sets the maximum number of hops in an MST region to restrict the region size. The setting can take effect only when it is configured on the regional root bridge.
Path Cost Standard	Specifies the standard for path cost calculation. It can be Legacy, IEEE 802.1D-1998, or IEEE 802.1T.
Bridge Diameter	Any two stations in a switched network are interconnected through a specific path composed of a series of devices. The bridge diameter (or the network diameter) is the number of devices on the path composed of the most devices. After you set the network diameter, you cannot set the timers. Instead, the device automatically calculates the forward delay, hello time, and max age. When you configure the bridge diameter, follow these guidelines: • The configured network diameter is effective on CIST only, not on MSTIs. • The bridge diameter cannot be configured together with the timers.
Timers	Configure the timers: • **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 the paths are fault-free. • **Max Age**—Set the maximum length of time a configuration BPDU can be held by the device. When you configure timers, follow these guidelines: • The settings of hello time, forward delay and max age must meet a certain formula. Otherwise, the network topology will not be stable. Hewlett Packard Enterprise recommends that you 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.
Instance (Instance ID, Root Type, and Bridge Priority)	Sets 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).

Item	Description
tc-protection	Selects 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. Hewlett Packard Enterprise recommends not disabling this function.
tc-protection threshold	Sets 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. From the navigation tree, select **Network** > **MSTP**.
2. Click the **Port Setup** tab.

Figure 183 MSTP configuration on a port



3. Configure MSTP for ports as described in Table 61, and then click **Apply**.

Table 61 Configuration items

Item	Description
STP	Selects whether to enable STP on the port.
Protection	Sets 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 62.

Item	Description
Instance (Instance ID, Port Priority, Auto Path Cost, and Manual Path Cost)	Sets the priority and path cost of the port in the current MSTI: • **Priority**—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**—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 Specifles whether the port is connected to a point-to-point link: ○ **Auto**—Configures 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. If a port is configured as connecting to a point-to-point link, the setting takes effect on 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 might incur a temporary loop. • **Transmit Limit**—Configures 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. Hewlett Packard Enterprise recommends that you use the default value. • **MSTP Mode**—Sets 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 might 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)	Selects 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 62 Protection types

Protection type	Description
Edged Port	Sets 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. Hewlett Packard Enterprise 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	Enables the root guard function. Configuration errors or attacks might 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.

Protection type	Description
Loop Protection	Enables 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 might get lost because of network congestion or unidirectional link failures. The device will re-elect a root port, and blocked ports might 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. From the navigation tree, select **Network** > **MSTP**.
2. Click the **Port Summary** tab.
3. Select a port on the chassis front panel.

   If you have configured aggregate interfaces 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 184 The port summary tab

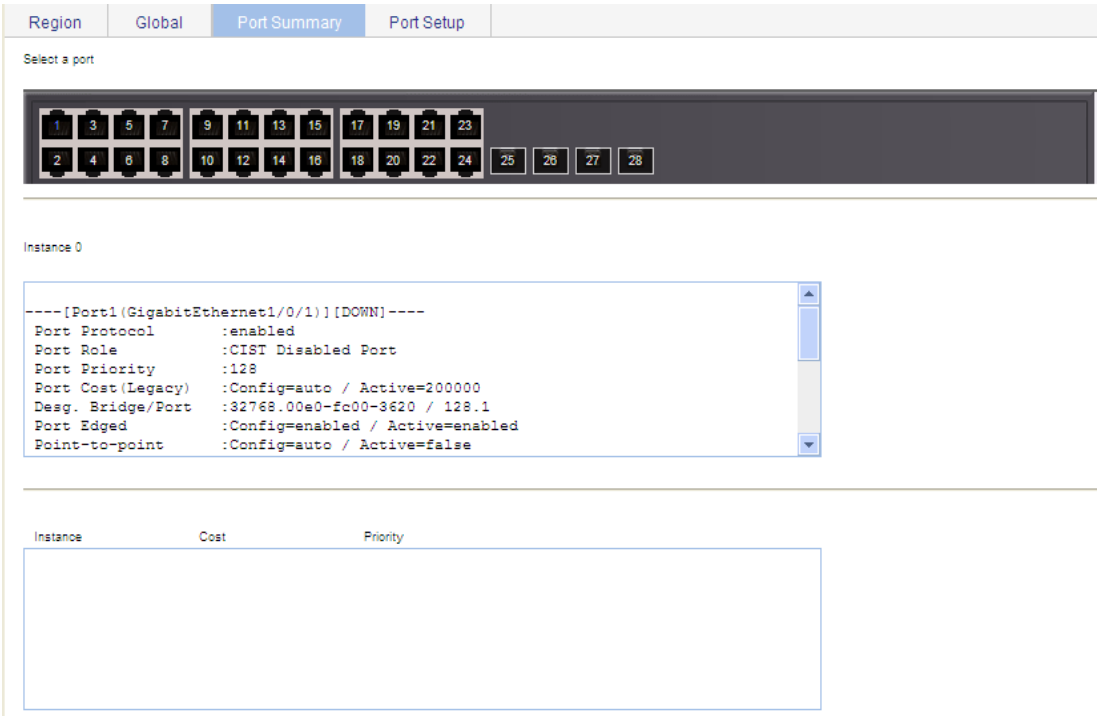


Table 63 Field description

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.

Field	Description
[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	Role of the port, which can be Alternate, Backup, Root, Designated, Master, or Disabled.
Port Priority	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**—The configured value. • **Active**—The actual value.
Point-to-point	Whether the port is connected to a point-to-point link: • **Config**—The configured value. • **Active**—The actual value.
Transmit Limit	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 transits 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.

Field	Description
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.

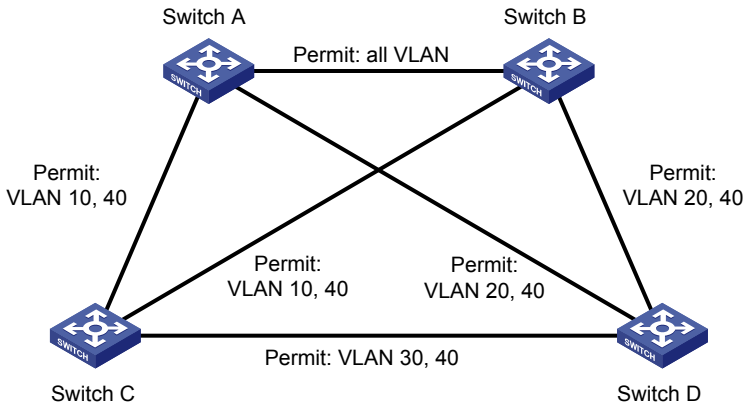
MSTP configuration example

Network requirements

As shown in Figure 185, configure MSTP as follows:

- All devices on the network are in the same MST region.
- Packets of VLAN 10, VLAN 20, VLAN 30, and VLAN 40 are forwarded along MSTI 1, MSTI 2, MSTI 3, and MSTI 0, respectively.
- Switch A and Switch B operate at the distribution layer. Switch C and Switch D operate at the access layer. VLAN 10 and VLAN 20 are terminated on the distribution layer devices, and VLAN 30 is terminated on the access layer devices, so the root bridges of MSTI 1 and MSTI 2 are Switch A and Switch B, respectively, and the root bridge of MSTI 3 is Switch C.

Figure 185 Network diagram



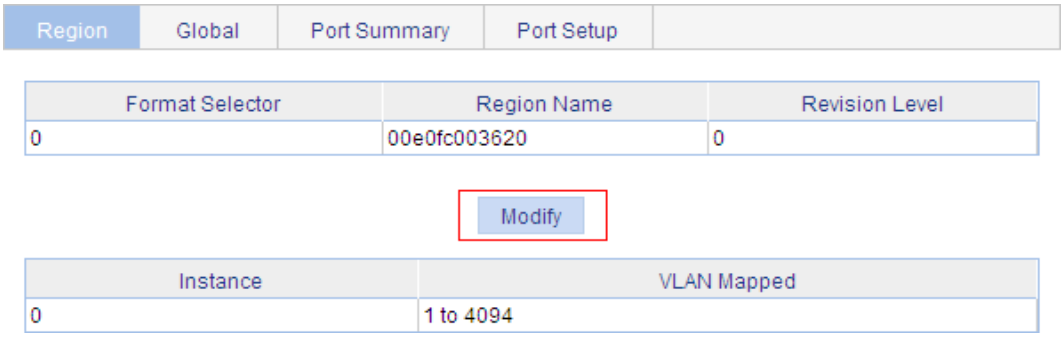
"Permit:" next to a link in the figure is followed by the VLANs the packets of which are permitted to pass this link.

Configuration procedure

Configuring Switch A

1. Configure an MST region:
   a. From the navigation tree, select **Network** > **MSTP**.
      By default, the **Region** tab is displayed.
   b. Click **Modify**.

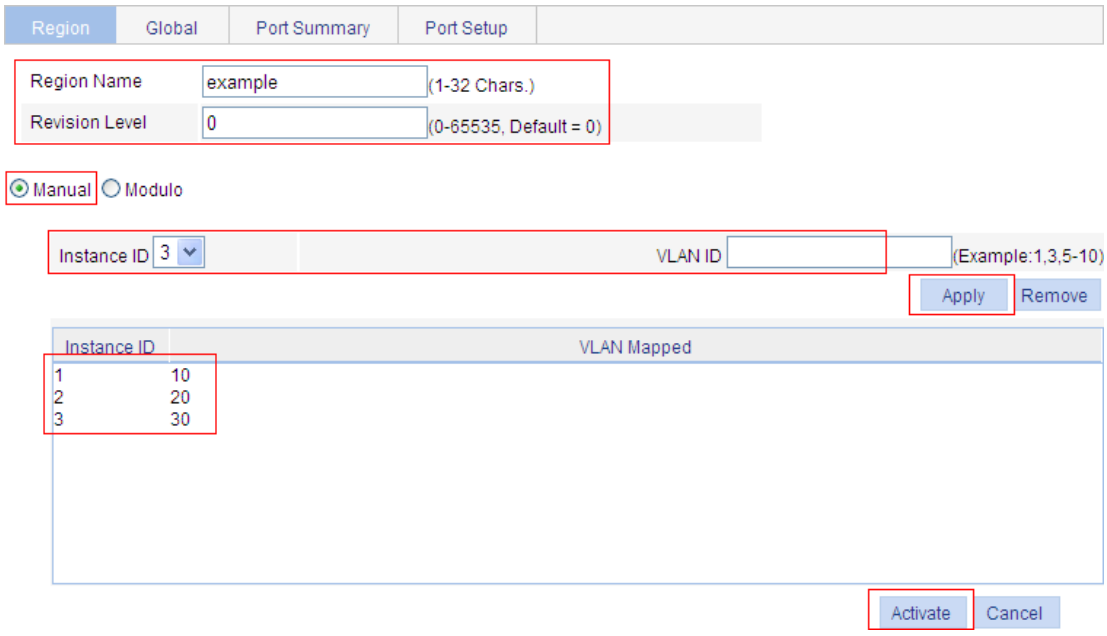
Figure 186 The region tab



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

   The system maps VLAN 10 to MSTI 1 and adds the VLAN-to-instance mapping entry to the VLAN-to-instance 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-instance mapping entries to the VLAN-to-instance mapping list.
j. Click **Activate**.

Figure 187 Configuring an MST region



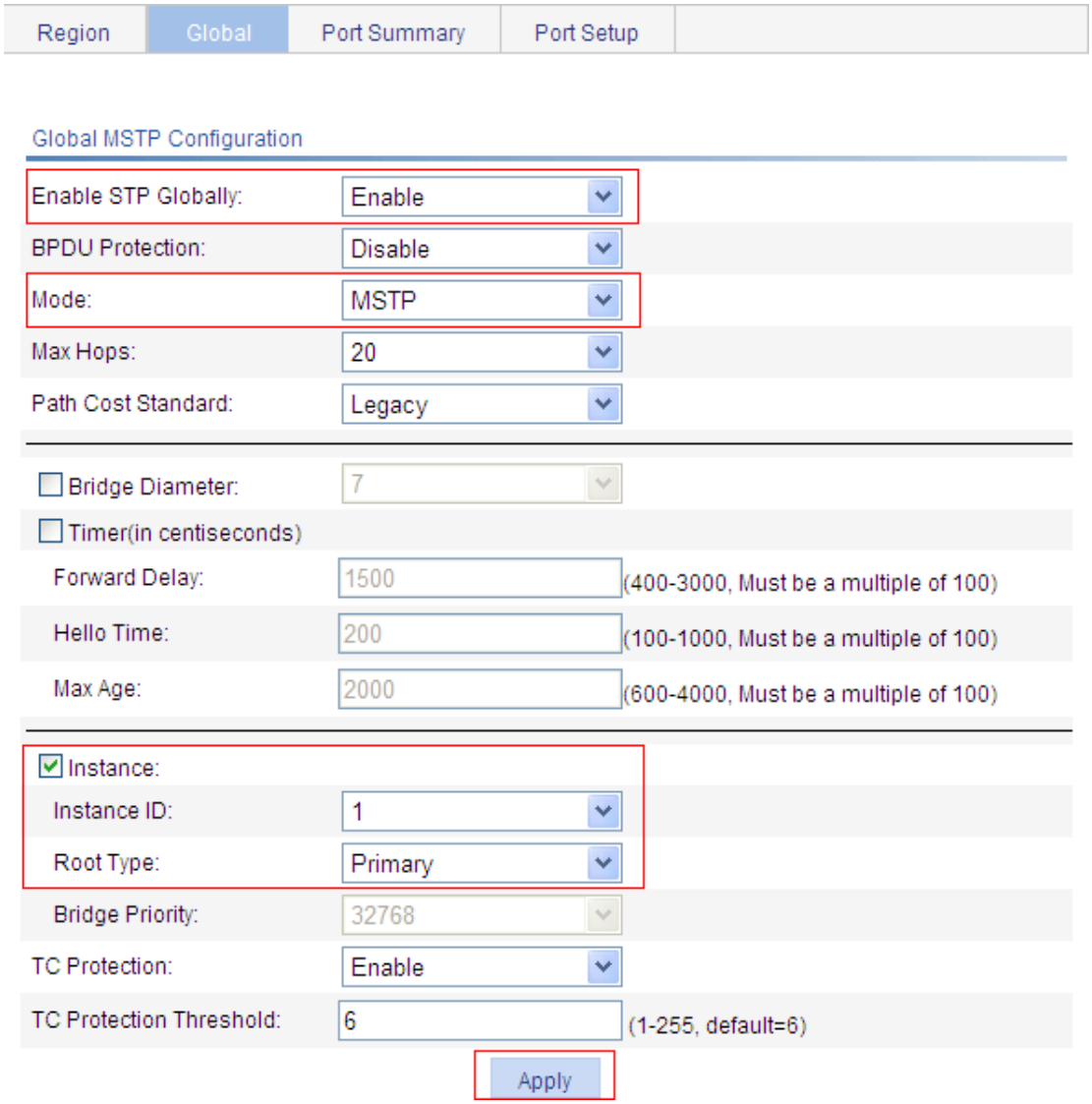
2. Configure MSTP globally:
   a. From the navigation tree, select **Network** > **MSTP**.
   b. Click the **Global** tab.
   c. Select **Enable** from the **Enable STP Globally** list.
   d. Select **MSTP** from the **Mode** list.
   e. Select the box before **Instance**.

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

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

h. Click **Apply**.

Figure 188 Configuring MSTP globally (on Switch A)



Configuring Switch B

1. Configure an MST region on the switch in the same way the MST region is configured on Switch A.
2. Configure MSTP globally:
   a. From the navigation tree, select **Network** > **MSTP**.
   b. Click the **Global** tab.
   c. Select **Enable** from the **Enable STP Globally** list.
   d. Select **MSTP** from 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**.

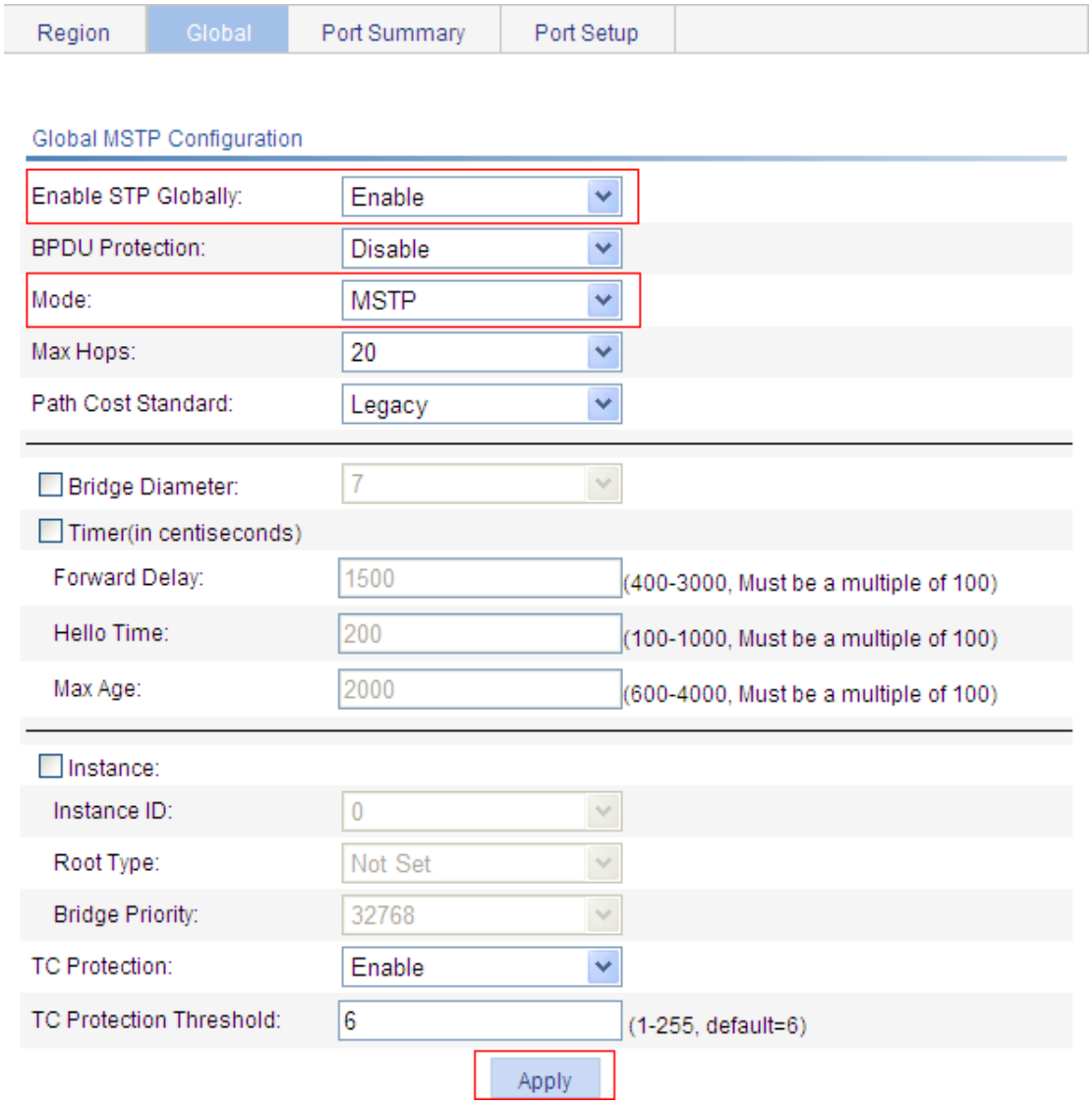
Configuring Switch C

1. Configure an MST region on the switch in the same way the MST region is configured on Switch A.
2. Configure MSTP globally:
   a. From the navigation tree, select **Network** > **MSTP**.
   b. Click **Global**.
   c. Select **Enable** from the **Enable STP Globally** list.
   d. Select **MSTP** from 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 on the switch in the same way the MST region is configured on Switch A.
2. Configure MSTP globally:
   a. From the navigation tree, select **Network** > **MSTP**.
   b. Click **Global**.
   c. Select **Enable** from the **Enable STP Globally** list.
   d. Select **MSTP** from the **Mode** list.
   e. Click **Apply**.

Figure 189 Configuring MSTP globally (on Switch D)



Configuring link aggregation and LACP

Overview

Ethernet link aggregation bundles multiple physical Ethernet links into one logical link, called an aggregate link. Link aggregation has the following benefits:

- Increased bandwidth beyond the limits of any single link. In an aggregate link, traffic is distributed across the member ports.
- Improved link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

Basic concepts

Aggregate interface

An aggregate interface is a logical interface.

Aggregation group

An aggregation group is a collection of Ethernet interfaces. When you create an aggregate interface, the switch automatically creates an aggregation group of the same number as the aggregate interface.

Aggregation states of the member ports in an aggregation group

A member port in an aggregation group can be in either of the following states:

- **Selected**—A Selected port can forward user traffic.
- **Unselected**—An Unselected port cannot forward user traffic.

The port rate of an aggregate interface equals the total rate of its member ports in Selected state, and its duplex mode is the same as that of the selected member ports.

For more information about the states of member ports in an aggregation group, see "Static aggregation mode" and "Dynamic aggregation mode."

LACP

The Link Aggregation Control Protocol (LACP) is defined in IEEE 802.3ad. It uses LACPDUs to exchange aggregation information between LACP-enabled devices.

LACP is automatically enabled on member ports in a dynamic aggregation group. An LACP-enabled port 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 peer port compares the received information with the information received on other member ports. In this way, the two systems reach an agreement on which ports are 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.

Configuration classes

Port configurations include the following classes:

- **Class-two configurations**—A member port can be placed in the Selected state only if it has the same class-two configurations as the aggregate interface.

Table 64 Class-two configurations

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

- **Class-one configurations**—Include settings that do not affect the aggregation state of the member port even if they are different from those on the aggregate interface. For example, MSTP, can be configured on aggregate interfaces and member ports. However, class-one configurations do not take effect in operational key calculation.

Any class-two configuration change might affect the aggregation state of link aggregation member ports and running services. To make sure you are aware of the risk, the system displays a warning message every time you attempt to change a class-two configuration setting on a member port.

Link aggregation modes

Based 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 the aggregation state of each member port according to the following rules:

1. Chooses a reference port from the member ports that are in up state and with the same class-two configurations as the aggregate interface. The candidate ports are sorted in the following order:
   - Full duplex/high speed.
   - Full duplex/low speed.
   - Half duplex/high speed.
   - Half duplex/low speed.

   If two ports have the same duplex mode/speed pair, the one with the lower port number is chosen.
2. Places the ports in up state with the same port attributes and class-two configurations as the reference port in the Selected state, and place all others in the Unselected state.
3. The number of Selected ports is limited in a static aggregation group. When the number of the Selected ports is under the limit, all the member ports become Selected ports. When the limit is exceeded, places the ports with smaller port numbers in the Selected state and those with greater port numbers in the Unselected state.
4. Places the member ports in the Unselected state if all the member ports are down.
5. Places the ports that cannot aggregate with the reference port in the Unselected state, for example, as a result of the inter-board aggregation restriction.

After a static aggregation group has reached the limit on Selected ports, any port that joins the group is placed in the Unselected state to avoid traffic interruption on the existing Selected ports. However, the state of link aggregation member ports might 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 send LACPDUs. An Unselected port can receive and send LACPDUs only when it is up, and has the same configurations as the aggregate interface.

In a dynamic aggregation group, the local system (the actor) negotiates with the remote system (the partner) to determine the aggregation state of each port in the following steps:

1. The systems compare the system IDs. (A system ID contains the system LACP priority and the system MAC address). The lower the LACP priority, the smaller the system ID. If LACP priority values are the same, the two systems compare their system MAC addresses. The lower the MAC address, the smaller the system ID.
2. The system with the smaller system ID chooses the port with the smallest port ID as the reference port. (A port ID contains a port priority and a port number.) The port with the lower priority value is chosen. If two ports have the same aggregation priority, the system compares their port numbers. The port with the smaller port number becomes the reference port.
3. 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, the port is placed in the Unselected state.

The number of Selected ports in an aggregation group is limited. When the number of Selected ports is under the limit, all the member ports are set to Selected state. When the limit is exceeded, the system sets the ports with smaller port IDs as the Selected ports, and place other ports in the Unselected state. At the same time, the peer device, being aware of the changes, sets the aggregation state of local member ports the same as their peer ports.

The system places the ports that cannot aggregate with the reference port in the Unselected state, for example, as the result of the inter-board aggregation restriction.

When you configure static and dynamic aggregation modes, follow these guidelines:

- In an aggregation group, a Selected port must have the same port attributes and class-two configurations as the reference port. To keep these configurations consistent, you should configure the port manually.
- Any port attribute or class-two configuration change might affect the aggregation state of all member ports and ongoing traffic. If you need to make this change, make sure you understand its impact on the live network.

Configuration procedures

Configuring a static aggregation group

Step	Remarks
1. Creating a link aggregation group.	Create a static aggregate interface and configure member ports for the static aggregation group. By default, no link aggregation group exists.
2. (Optional.) Displaying aggregate interface information.	Display detailed information of an existing aggregation group.

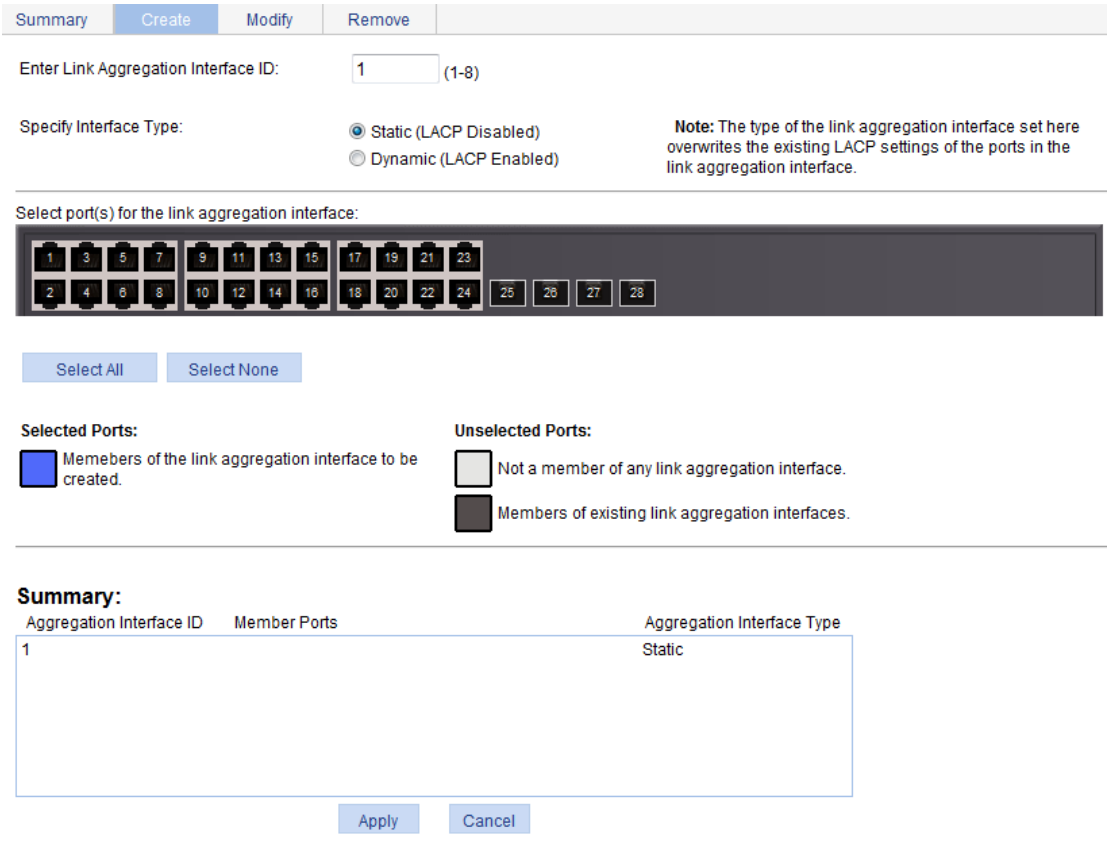
Configuring a dynamic aggregation group

Step	Remarks
1. Creating a link aggregation group.	Create a dynamic aggregate interface and configure member ports for the dynamic aggregation group automatically created. LACP is enabled automatically on all the member ports. By default, no link aggregation group exists.
2. (Optional.) Displaying aggregate interface information.	Display detailed information of an existing aggregation group.
3. (Optional.) Setting LACP priority.	Set LACP priority for the local system and link aggregation member ports. Changes of LACP priorities affect the aggregation state of the member ports. The default port LACP priority and system LACP priority are both 32768.
4. (Optional.) Displaying LACP-enabled port information.	Display detailed information of LACP-enabled ports and the corresponding remote (partner) ports.

Creating a link aggregation group

1. From the navigation tree, select **Network** > **Link Aggregation**.
2. Click **Create**.

Figure 190 Creating a link aggregation group



3. Configure a link aggregation group as described in Table 65.
4. Click **Apply**.

Table 65 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 is disabled. • **Dynamic**—LACP is 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 aggregate interface information

1. From the navigation tree, select **Network** > **Link Aggregation**.

   The default **Summary** tab appears. The list on the upper part of the page displays information about all the aggregate interfaces.
2. Choose 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 link aggregation group.

Figure 191 Displaying information of an aggregate interface

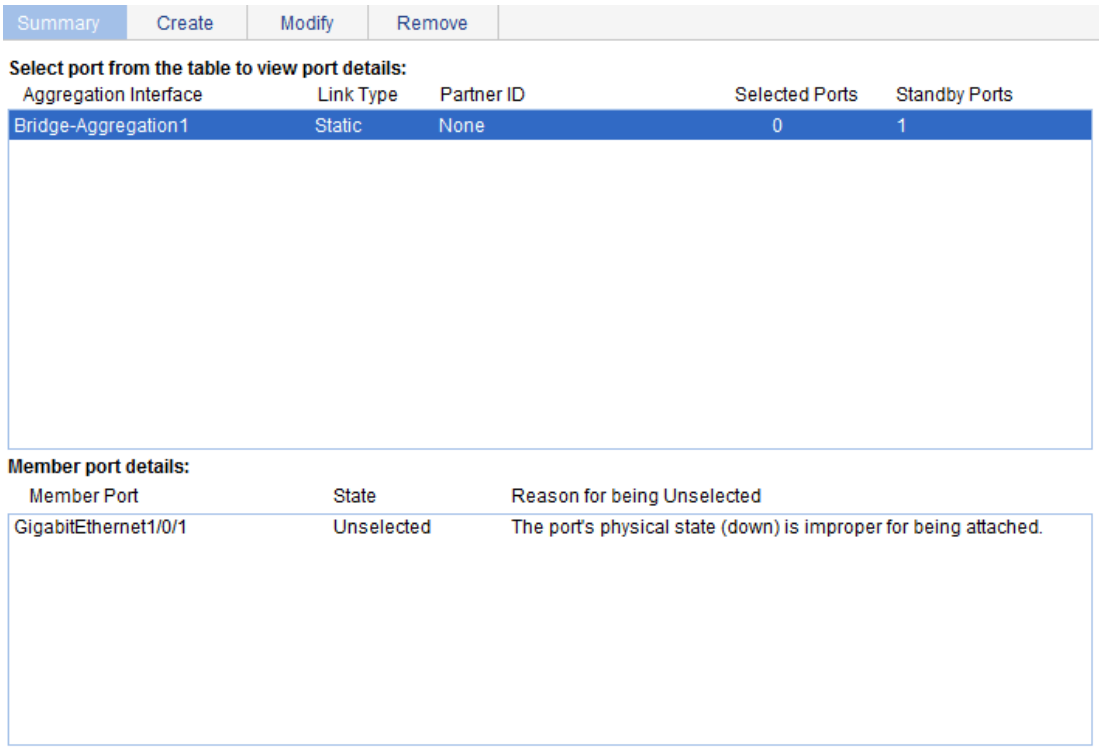


Table 66 Field description

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: 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 send and receive user data).
Standby Ports	Number of Unselected ports in each link aggregation group (Unselected ports cannot send or receive user data).
Member Port	A member port of the link aggregation group corresponding to the target aggregate interface.
State	Aggregation 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 port, this field displays a hyphen (-).

Setting LACP priority

1. From the navigation tree, select **Network** > **LACP**.
2. Click **Setup**.
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.

Figure 192 Setting the LACP priority

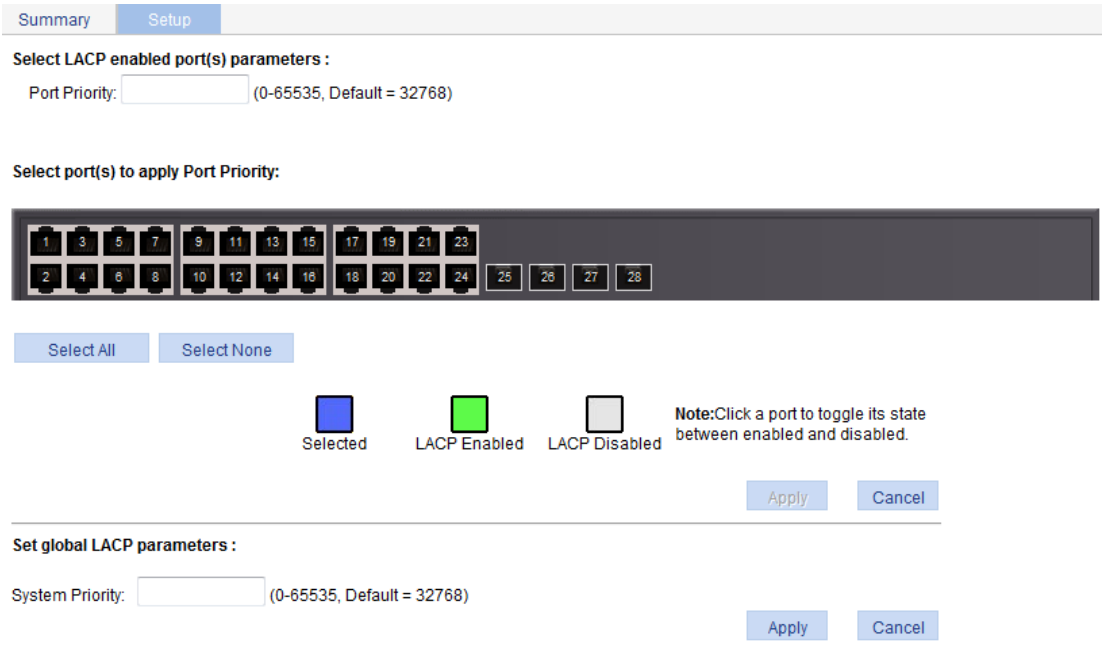


Table 67 Configuration items

Item	Description
Port Priority	Set a port LACP priority.
Select port(s) to apply Port Priority	Choose the ports where the port LACP priority you set will apply on the chassis front panel. You can set LACP priority on both LACP-enabled ports and LACP-disabled ports.

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

Displaying LACP-enabled port information

1. From the navigation tree, select **Network** > **LACP**.

   The default **Summary** tab appears. The upper part of the page displays a list of all LACP-enabled ports on the device and information about them. Table 68 describes the fields.
2. Select a port on the port list.
3. Click **View Details**.

   Detailed information about the peer port appears on the lower part of the page. Table 69 describes the fields.

Figure 193 Displaying the information of LACP-enabled ports

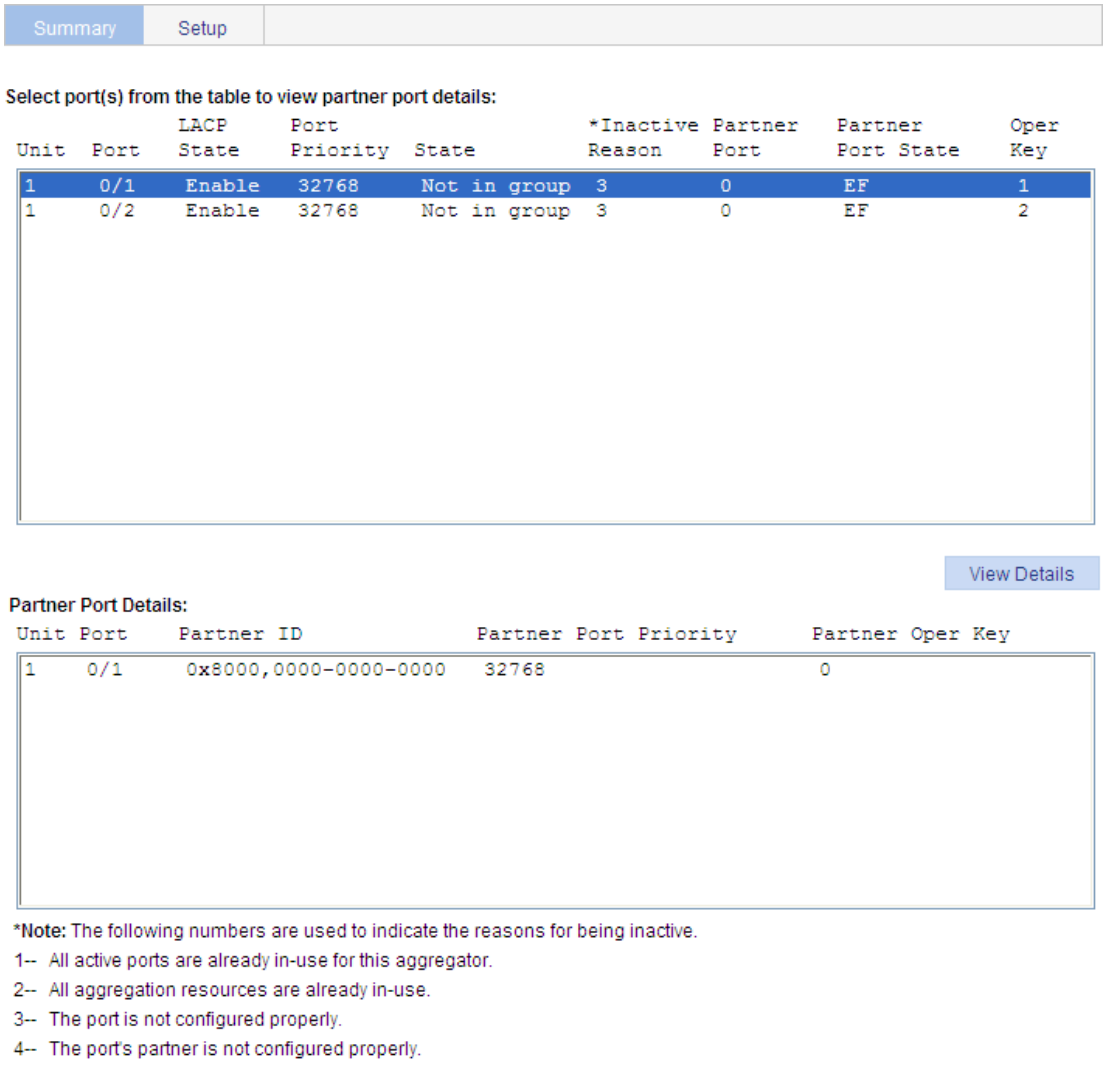


Table 68 Field description

Field	Description
Unit	ID of a device in a stack.
Port	Port where LACP is enabled.
LACP State	State of LACP on the port.
Port Priority	LACP priority of the port.
State	Aggregation state of the port. If a port is Selected, this field also displays the ID of the aggregation group it belongs to.
Inactive Reason	Reason code indicating why a port is Unselected for receiving or sending user data. For more information about the reason codes, see the bottom of the page shown in Figure 193.
Partner Port	ID of the peer port.

Field	Description
Partner Port State	States of the peer port: • **A**—LACP is enabled. • **B**—LACP short timeout. If B does not appear, it indicates LACP long timeout. • **C**—The sending system considers the link is aggregatable. • **D**—The sending system considers the link is synchronized. • **E**—The sending system considers the incoming frames are collected. • **F**—The sending system considers the outgoing frames are distributed. • **G**—The sending system receives frames in the default state. • **H**—The sending system receives frames in the expired state.
Oper Key	Operational key of the local port.

Table 69 Field description

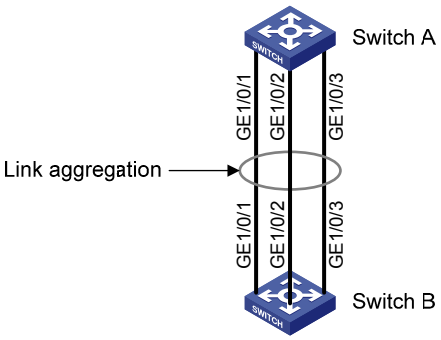
Field	Description
Unit	Number of the remote system.
Port	Name of the remote port.
Partner ID	LACP priority and MAC address of the remote system.
Partner Port Priority	LACP priority of the remote port.
Partner Oper Key	Operational key of the remote port.

Link aggregation and LACP configuration example

Network requirements

As shown in Figure 194, create a link aggregation group on Switch A and Switch B to load-share incoming and outgoing traffic across the member ports.

Figure 194 Network diagram



Method 1: Create static link aggregation group 1

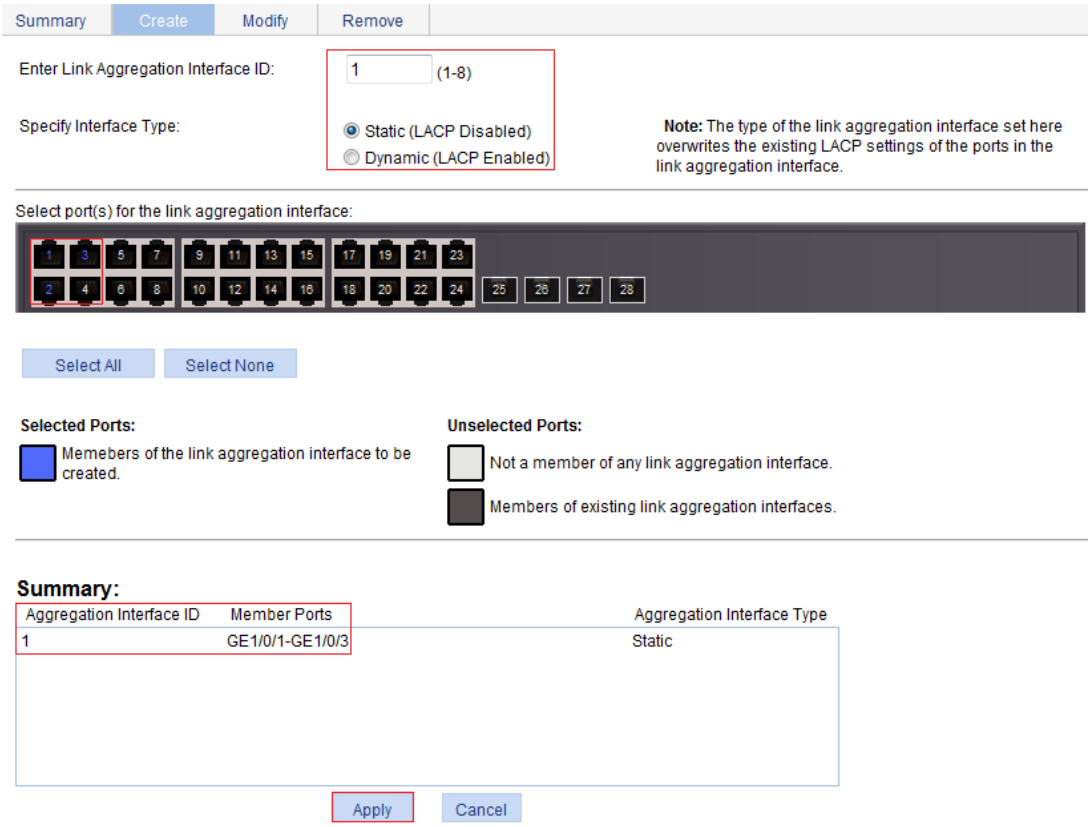
1. From the navigation tree, select **Network** > **Link Aggregation**.
2. Click **Create**.
3. Configure static link aggregation group 1:
   a. Enter link aggregation interface ID **1**.

b. Select **Static (LACP Disabled)** 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**.

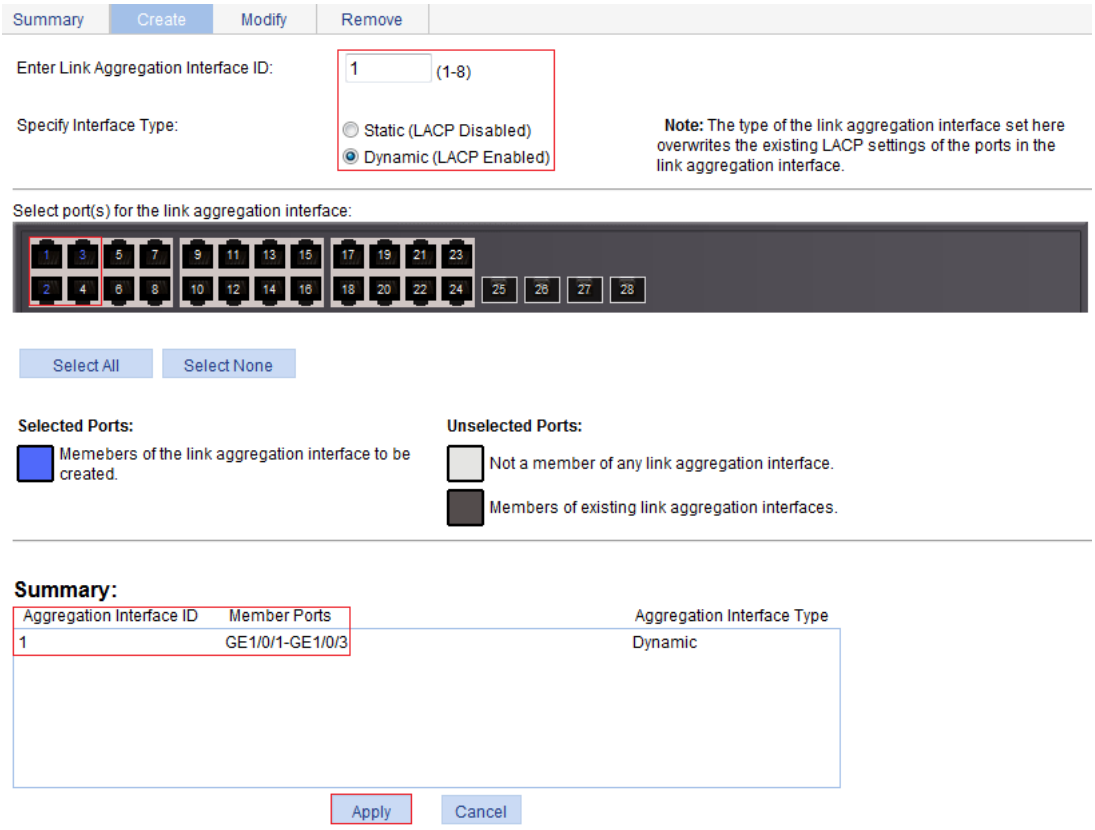
Figure 195 Creating static link aggregation group 1



Method 2: Create dynamic link aggregation group 1

1. From the navigation tree, select **Network** > **Link Aggregation**.
2. Click **Create**.
3. Configure dynamic aggregation group 1:
   a. Enter link aggregation interface ID **1**.
   b. Select **Dynamic (LACP Enabled)** 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 196 Creating dynamic link aggregation group 1



Configuration guidelines

When you configure a link aggregation group, follow these guidelines:

- In an aggregation group, a Selected port must have the same port attributes and class-two configurations as the reference port. To keep these configurations consistent, you should configure the port manually.
- Choose a reference port from the member ports that are in up state and with the same class-two configurations as the aggregate interface. The candidate ports are sorted in the following order:
- Full duplex/high speed.
- Full duplex/low speed.
- Half duplex/high speed.
- Half duplex/low speed.

  If two ports have the same duplex mode/speed pair, the one with the lower port number is chosen.
- Port attribute configuration includes the configuration of the port rate, duplex mode, and link state. For more information about class-two configurations, see "Configuration classes."
- To guarantee a successful static aggregation, make sure the ports at the two ends of each link to be aggregated are in the same aggregation state. To guarantee a successful dynamic aggregation, make sure the peer ports of the ports aggregated at one end are also aggregated. The two ends can automatically negotiate the aggregation state of each member port.
- Do not assign the following types of ports to Layer 2 aggregate groups:
- MAC address authentication-enabled ports.

- port security-enabled ports.
- packet filtering-enabled ports.
- Ethernet frame filtering-enabled ports.
- IP source guard-enabled ports.
- 802.1X-enabled ports.
- Deleting a Layer 2 aggregate interface also deletes its aggregation group and causes all member ports to leave the aggregation group.
- When a load sharing aggregation group becomes non-load-sharing because of insufficient load sharing resources, one of the following problems might occur:
- The number of Selected ports of the actor is inconsistent with that of the partner, which might result in incorrect traffic forwarding
- The peer port of a Selected port is Unselected, which might result anomalies in upper-layer protocol and traffic forwarding.

Configuring LLDP

Overview

In a heterogeneous network, a standard configuration exchange platform makes sure different types of network devices from different vendors can discover one another and exchange configuration.

The Link Layer Discovery Protocol (LLDP) is specified in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices. Local device information includes its system capabilities, management IP address, device ID, port ID, and so on. The device stores the device information in LLDPDUs from the LLDP neighbors in a standard MIB. LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

For more information about MIBs, see "Configuring SNMP."

Basic concepts

LLDP frame formats

LLDP sends device information in LLDP frames. LLDP frames are encapsulated in Ethernet II or SNAP frames.

- LLDP frames encapsulated in Ethernet II

  Figure 197 LLDP frame encapsulated in Ethernet II

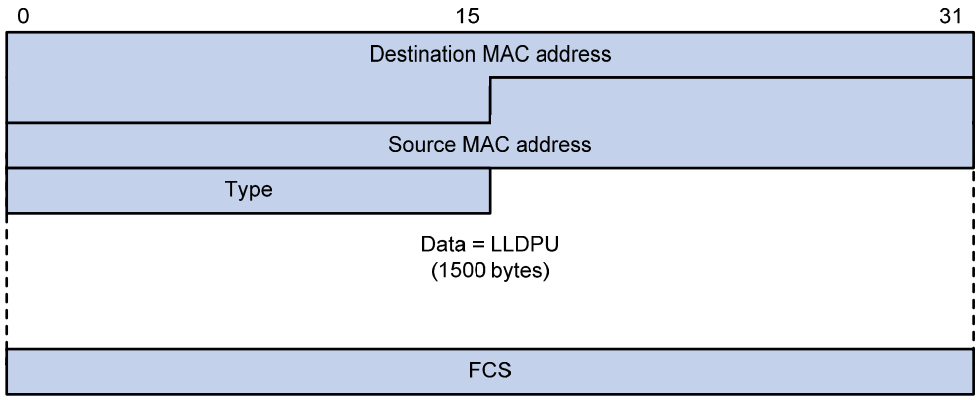


  Table 70 Fields in an Ethernet II encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	MAC address of the sending port.
Type	Ethernet type for the upper layer protocol. It is 0x88CC for LLDP.
Data	LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

- LLDP frames encapsulated in SNAP

Figure 198 LLDP frame encapsulated in SNAP

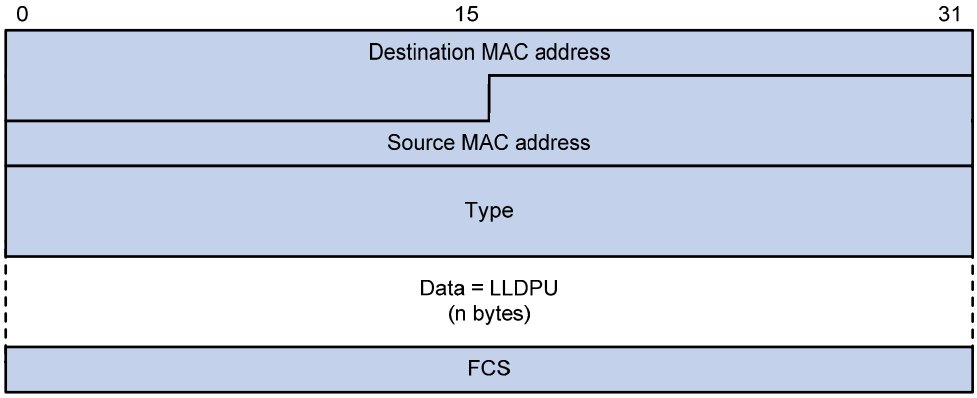


Table 71 Fields in a SNAP-encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame 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 type for the upper layer protocol. It is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDPDU.
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 TLVs. Each TLV carries a type of device information, as shown in Figure 199.

Figure 199 LLDPDU encapsulation format

An LLDPDU can carry up to 28 types of TLVs. Mandatory TLVs include Chassis ID TLV, Port ID TLV, Time to Live TLV, and End of LLDPDU TLV. Other TLVs are optional.

TLVs

A TLV is an information element that contains the type, length, and value fields.

LLDPDU TLVs include the following categories:

- Basic management TLVs.
- Organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs.
- LLDP-MED (media endpoint discovery) TLVs.

Basic management TLVs are essential to device management.

Organizationally specific TLVs and LLDP-MED TLVs are used for improved device management. They are defined by standardization or other organizations and are optional to LLDPDUs.

- Basic management TLVs

  Table 72 lists the basic management TLV types. Some of them are mandatory for LLDPDUs.

Table 72 Basic management 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 the LLDPDU carries LLDP-MED TLVs, 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. • Otherwise, 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 enabled primary functions.	
Management Address	Specifies the following elements: • The management address used to reach higher level entities to assist discovery by network management. • The interface number and OID associated with the address.	

- IEEE 802.1 organizationally specific TLVs

Table 73 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.
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:

HPE devices support only receiving protocol identity TLVs.

- IEEE 802.3 organizationally specific TLVs

Table 74 IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the rate and duplex capabilities of the sending port, support for autonegotiation, enabling status of auto negotiation, and the current rate and duplex mode.
Power Via MDI	Contains the power supply capability of the port: • Port class (PSE or PD). • Power supply mode. • Whether PSE power supply is supported. • Whether PSE power supply is enabled. • Whether pair selection can be 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 MTU of the port.
Power Stateful Control	Indicates the power state control configured on the sending port, including the following: • Power supply mode of the PSE/PD. • PSE/PD priority. • PSE/PD power.

The power stateful control TLV is defined in IEEE P802.3at D1.0. The later versions no longer support this TLV. HPE devices send this type of TLVs only after receiving them.

- LLDP-MED TLVs

  LLDP-MED TLVs provide multiple advanced applications for VoIP, such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs provide a cost-effective and easy-to-use solution for deploying voice devices in Ethernet. LLDP-MED TLVs are shown in Table 75.

Table 75 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.
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.

Type	Description
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.

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 network management system uses the management address of a device to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

LLDP operating modes

LLDP can operate in one of the following modes:

- **TxRx mode**—A port in this mode can send and receive LLDP frames.
- **Tx mode**—A port in this mode can only send LLDP frames.
- **Rx mode**—A port in this mode can only receive LLDP frames.
- **Disable mode**—A port in this mode cannot send or receive LLDP frames.

Each time the LLDP operating mode of a port changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, a port must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

Working mechanism

Transmitting LLDP frames

An LLDP-enabled port operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes. To prevent LLDP frames from overwhelming the network during times of frequent changes to local device information, an interval is introduced between two successive LLDP frames.

This interval is shortened to 1 second in either of the following cases:

- A new neighbor is discovered. A new LLDP frame is received carrying device information new to the local device.
- The LLDP operating mode of the port changes from Disable or Rx to TxRx or Tx.

This is the fast sending mechanism of LLDP. With this mechanism, the specified number of LLDP frames is sent successively at the 1-second interval. The mechanism helps LLDP neighbors discover the local device as soon as possible. Then, the normal LLDP frame transmission interval resumes.

Receiving LLDP frames

An LLDP-enabled port operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the information is saved and an aging timer is set. When the TTL value in the Time to Live TLV carried in the LLDP frame becomes zero, the information ages out immediately.

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 LLDP is also enabled globally, because LLDP can work on a port only when it is enabled both globally and on the port.
2. Setting LLDP parameters on ports.	Optional. LLDP settings include LLDP operating mode, packet encapsulation, CDP compatibility, device information polling, trapping, and advertisable TLVs. By default: • The LLDP operating mode is TxRx. • The encapsulation format is Ethernet II. • CDP compatibility is disabled. • Device information polling and trapping are disabled. • All TLVs except the Location Identification TLV are advertised.
3. Configuring LLDP globally.	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.

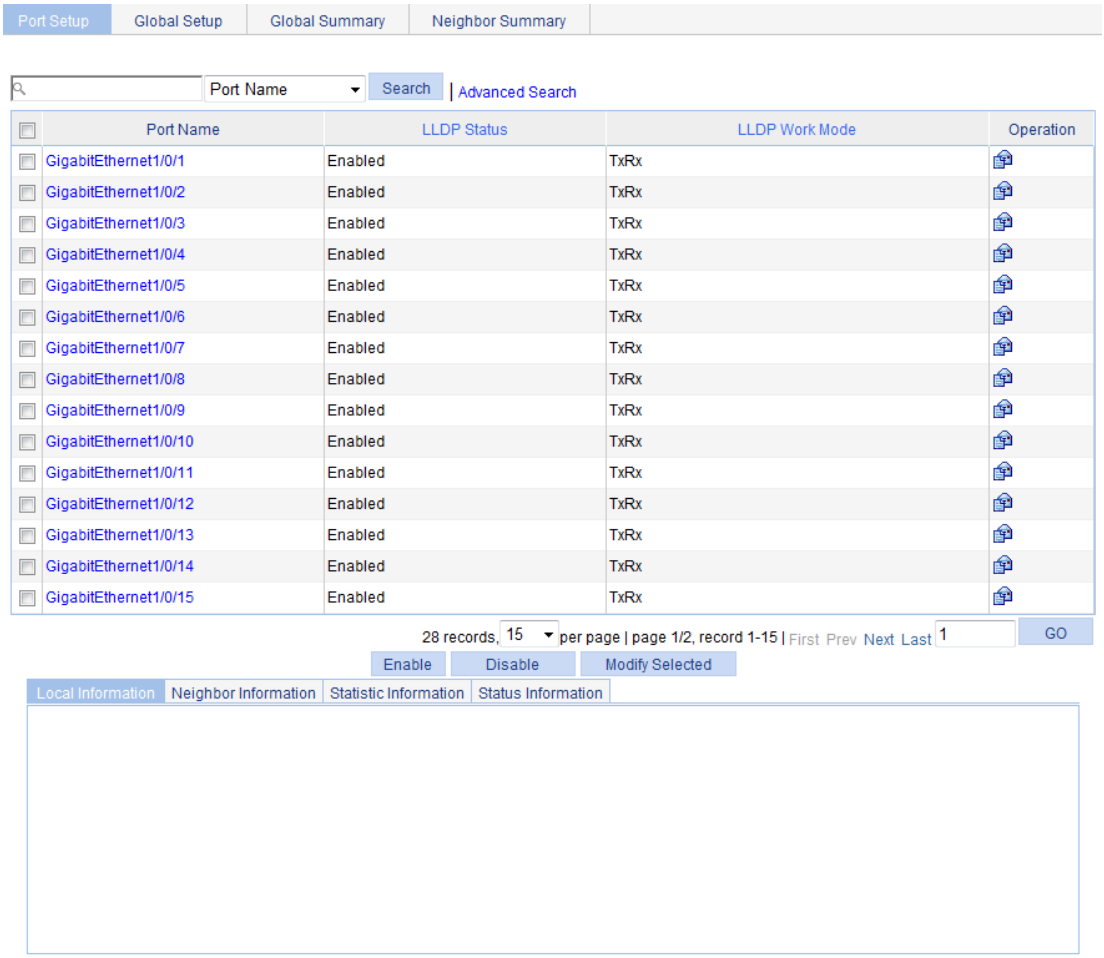
Enabling LLDP on ports

1. From the navigation tree, select **Network** > **LLDP**.

   By default, the **Port Setup** tab is displayed. This tab displays the enabling status and operating mode of LLDP on a port.
2. Select one or more ports and click **Enable**.

   To disable LLDP on a port, select the port and click **Disable**.

Figure 200 The port setup tab



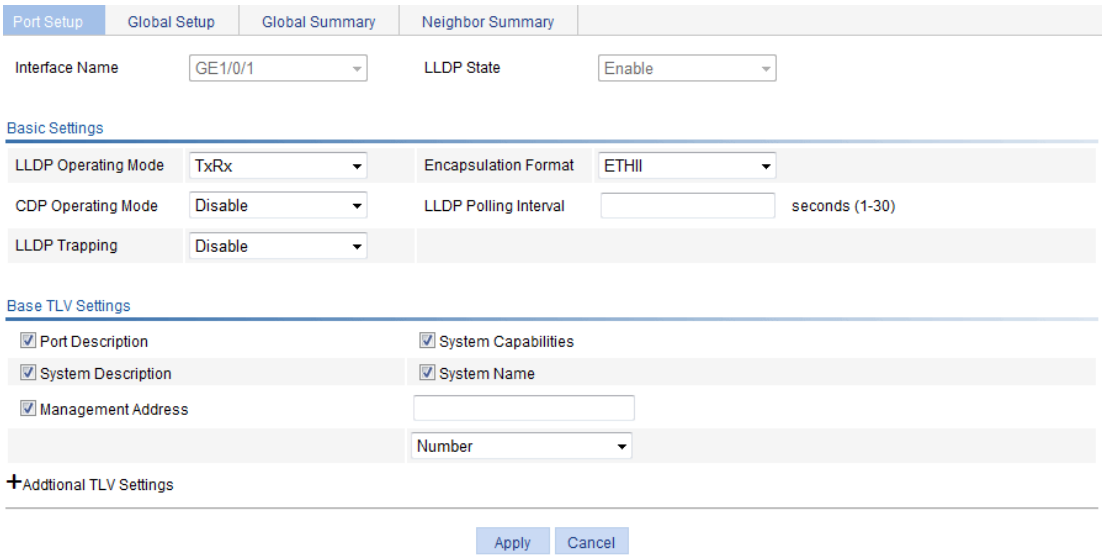
Setting LLDP parameters on ports

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

Setting LLDP parameters for a single port

1. From the navigation tree, select **Network** > **LLDP**.
   By default, the **Port Setup** tab is displayed.
2. Click the icon for the port.
   On the page as shown in Figure 201, the LLDP settings of the port are displayed.

Figure 201 Modifying LLDP settings on a port



3. Configure the LLDP parameters for the port as described in Table 76.
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 76 Configuration items

Item		Description
Interface Name		Displays the name of the port or ports you are configuring.
DLDP State		Displays the LLDP enabling status on the port you are configuring. This field is not available when you batch-configure ports.
Basic Settings	LLDP Operating Mode	Set the LLDP operating mode on the port or ports you are configuring: • **TxRx**—Sends and receives LLDP frames. • **Tx**—Sends but does not receive LLDP frames. • **Rx**—Receives but not does not send LLDP frames. • **Disable**—Neither sends nor receives LLDP frames.
	Encapsulation Format	Set the encapsulation for LLDP frames: • **ETHII**—Encapsulates outgoing LLDP frames in Ethernet II frames and processes an incoming LLDP frame only if its encapsulation is Ethernet II. • **SNAP**—Encapsulates outgoing LLDP frames in Ethernet II frames and processes an incoming LLDP frame only if its encapsulation is Ethernet II. LLDP-CDP PDUs use only SNAP encapsulation.
	CDP Operating Mode	Set the CDP compatibility of LLDP: • **Disable**—Neither sends nor receives CDP frames. • **TxRx**—Sends and receives CDP frames 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.

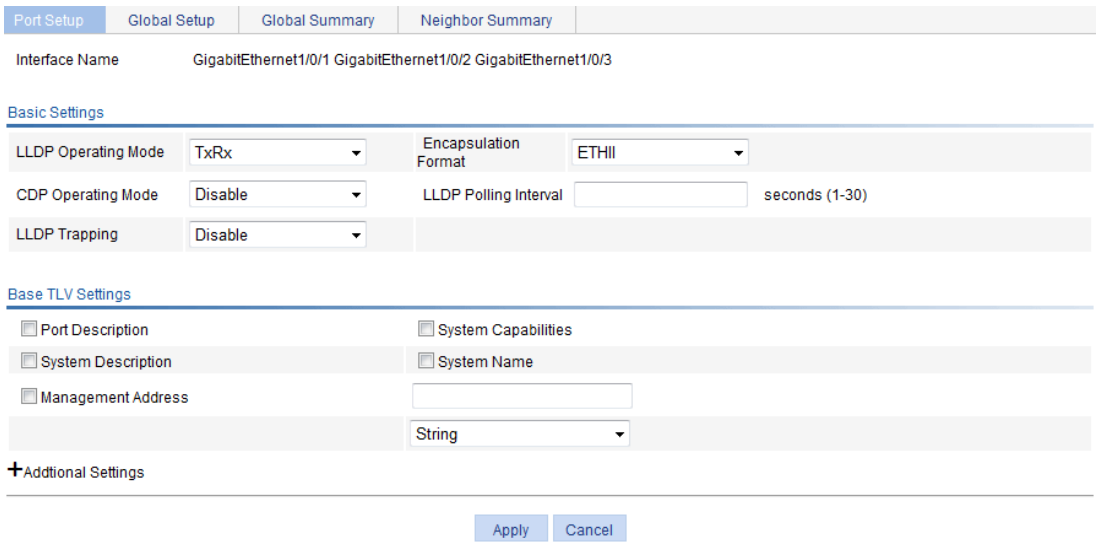
Item		Description
	LLDP Polling Interval	Enable LLDP polling and set the polling interval. If no polling interval is set, LLDP polling is disabled. With the polling mechanism, LLDP periodically detects local configuration changes. If a configuration change is detected, an LLDP frame is sent to inform 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. To avoid excessive traps from being sent when topology is instable, tune the minimum trap transmission interval on the **Global Setup** tab.
Base TLV Settings	Port Description	Select the box to include the port description TLV in transmitted LLDP frames.
	System Capabilities	Select the box to include the system capabilities TLV in transmitted LLDP frames.
	System Description	Select the box to include the system description TLV in transmitted LLDP frames.
	System Name	Select the box to include the system name TLV in transmitted LLDP frames.
	Management Address	Select the box to include the management address TLV in transmitted LLDP frames and, in addition, set the management address and its format (a numeric or character string in the TLV). If no management address is specified, the main IP address of the lowest VLAN carried on the port is used. If no main IP address is assigned to the VLAN, 127.0.0.1 is used.
DOT1 TLV Setting	Port VLAN ID	Select the box to include the PVID TLV in transmitted LLDP frames.
	Protocol VLAN ID	Select the box to include port and protocol VLAN ID TLVs in transmitted LLDP frames and specify the VLAN IDs to be advertised. If no VLAN is specified, the lowest protocol VLAN ID is transmitted.
	VLAN Name	Select the box to include VLAN name TLVs in transmitted LLDP frames, 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 the box to include the link aggregation TLV in transmitted LLDP frames.
	MAC/PHY Configuration/Status	Select the box to include the MAC/PHY configuration/status TLV in transmitted LLDP frames.
	Maximum Frame Size	Select the box to include the maximum frame size TLV in transmitted LLDP frames.
	Power via MDI	Select the box to include the power via MDI TLV and power stateful control TLV in transmitted LLDP frames.
MED TLV Setting	LLDP-MED Capabilities	Select the box to include the LLDP-MED capabilities TLV in transmitted LLDP frames.
	Inventory	Select the box 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 LLDP frames.
	Network Policy	Select the box to include the network policy TLV in transmitted LLDP frames.

Item		Description
	Extended Power-via-MDI Capability	Select the box to include the extended power-via-MDI TLV in transmitted LLDP frames.
	Emergency Number	Select the box to encode the emergency call number in the location identification TLV in transmitted LLDP frames and set the emergency call number.
	Address	Select Address to encode the civic address information of the network connectivity device in the location identification TLV in transmitted LLDP frames. In addition, set the device type (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, enter 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.
	Network Device Address	

Setting LLDP parameters for ports in batch

1. From the navigation tree, select **Network** > **LLDP**.
   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 202 Modifying LLDP settings on ports in batch

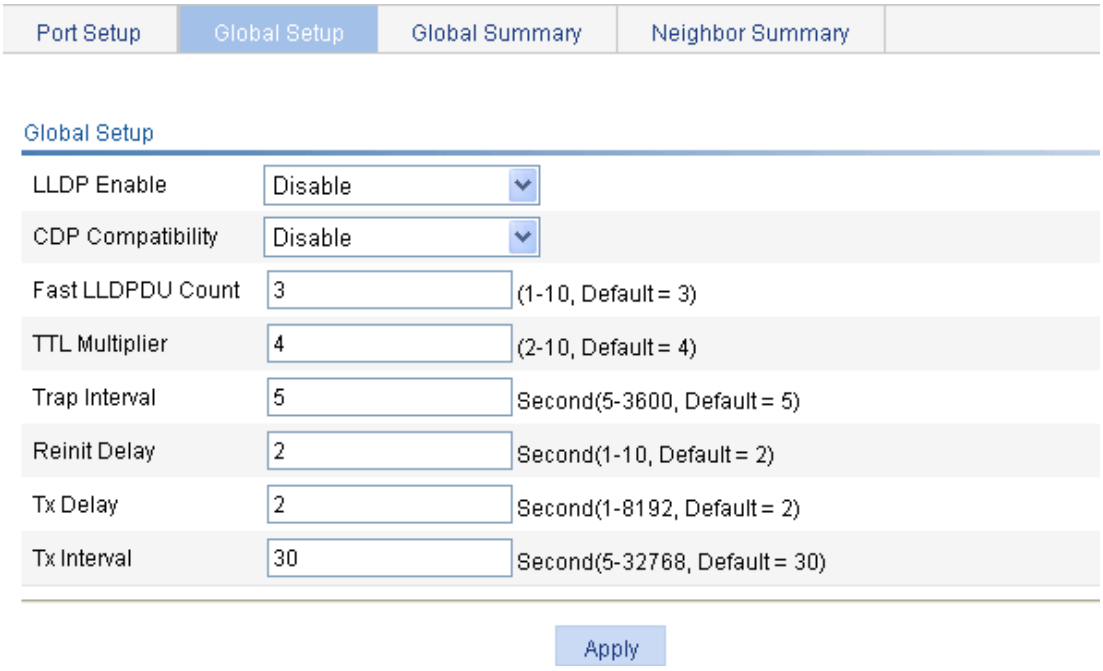


4. Set the LLDP settings for these ports as described in Table 76.
5. Click **Apply**.
   A progress dialog box appears.
6. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Configuring LLDP globally

1. From the navigation tree, select **Network** > **LLDP**.
2. Click the **Global Setup** tab.

Figure 203 The global setup tab



3. Set the global LLDP setup 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
LLDP Enable	Select from the list to enable or disable global LLDP.
CDP Compatibility	Select from the list to enable or disable CDP compatibility of LLDP. When you configure CDP compatibility, follow these guidelines: • To enable LLDP to be compatible with CDP on a port, you must set the CDP operating mode on the port to TxRx and enable CDP compatibility on the **Global Setup** tab. • Because the maximum TTL allowed by CDP is 255 seconds, you must make sure the product of the TTL multiplier and the LLDP frame transmission interval is less than 255 seconds for CDP-compatible LLDP to work correctly with Cisco IP phones.
Fast LLDPDU Count	Set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Item	Description
TTL Multiplier	Set the TTL multiplier. The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device. You can configure the TTL of locally sent LLDPDUs to determine how long information about the local device can be saved on a neighbor device by setting the TTL multiplier. The TTL is expressed as *TTL multiplier × LLDP frame transmission interval*. When you configure the TTL multiplier, follow these guidelines: • If the product of the TTL multiplier and the LLDP frame transmission interval is greater than 65535, the TTL carried in transmitted LLDP frames takes 65535 seconds. • Because the maximum TTL allowed by CDP is 255 seconds, you must make sure the product of the TTL multiplier and the LLDP frame transmission interval is less than 255 seconds for CDP-compatible LLDP to work correctly 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 reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, a port must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.
Tx Delay	Set LLDP frame transmission delay. With LLDP enabled, a port advertises LLDP frames to its neighbors both periodically and when the local configuration changes. To avoid excessive number of LLDP frames caused by frequent local configuration changes, an LLDP frame transmission delay is introduced. After sending an LLDP frame, the port must wait for the specified interval before it can send another one. LLDP frame transmission delay must be less than the TTL to make sure the LLDP neighbors can receive LLDP frames to update information about the device you are configuring before it is aged out.
Tx Interval	Set the LLDP frame transmission interval. If the product of the TTL multiplier and the LLDP frame transmission interval is greater than 65535, the TTL carried in transmitted LLDP frames takes 65535 seconds. The likelihood exists that the LLDP frame transmission interval is greater than TTL. You should avoid the situation, because the LLDP neighbors will fail to receive LLDP frames to update information about the device you are configuring before it is aged out.

Displaying LLDP information for a port

1. From the navigation tree, select **Network** > **LLDP**.
   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. Table 78 describes the fields.

Figure 204 The local information tab

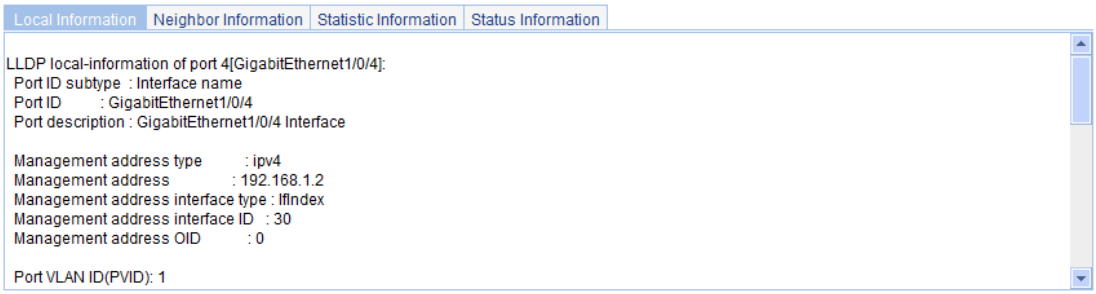


Table 78 Field description

Field	Description
Port ID subtype	Port ID subtype: • **Interface alias.** • **Port component.** • **MAC address.** • **Network address.** • **Interface name.** • **Agent circuit ID.** • **Locally assigned**—Locally-defined port ID type other than those listed above.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
Port power classification	Power class of the PD: • Unknown. • Class0. • Class1. • Class2. • Class3. • Class4.
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	PSE power source type: • Primary. • Backup.

Field	Description
Port PSE priority	PoE power supply priority of PSE ports: • **Unknown**—Unknown PSE 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 79 describes the fields.

Figure 205 The neighbor information tab

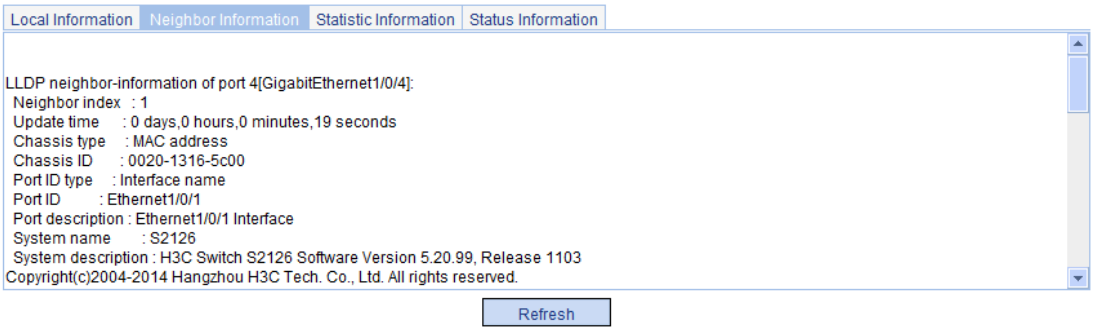


Table 79 Field description

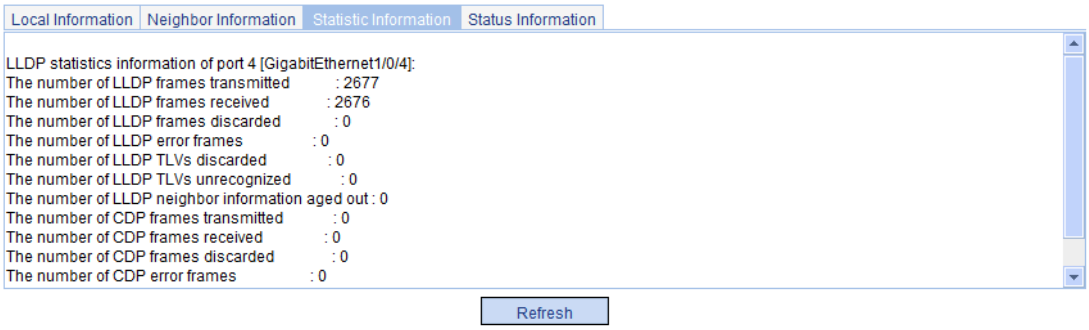
Field	Description
Chassis type	Chassis ID type: • **Chassis component**. • **Interface alias**. • **Port component**. • **MAC address**. • **Network address**. • **Interface name**. • **Locally assigned**—Locally-defined chassis type other than those listed above.
Chassis ID	Chassis ID depending on the 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**—Locally-defined port ID type other than those listed above.
Port ID	Port ID value.
System capabilities supported	Capabilities supported on the system: • Repeater. • Bridge. • Router.

Field	Description
System capabilities enabled	Capabilities enabled on the system: • Repeater. • Bridge. • Router.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
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	Maximum frame size supported on the neighbor port.
Device class	MED device class: • **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 and 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 value.
HardwareRev	Hardware version of the neighbor.
FirmwareRev	Firmware version of the neighbor.
SoftwareRev	Software version of the neighbor.
SerialNum	Serial number advertised by the neighbor.
Manufacturer name	Manufacturer name advertised by the neighbor.

Field	Description
Model name	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	PSE power source type: • Primary. • Backup.
Port PSE priority	PoE power supply priority of PSE ports: • **Unknown**—Unknown PSE priority. • **Critical**—Priority level 1. • **High**—Priority level 2. • **Low**—Priority level 3.

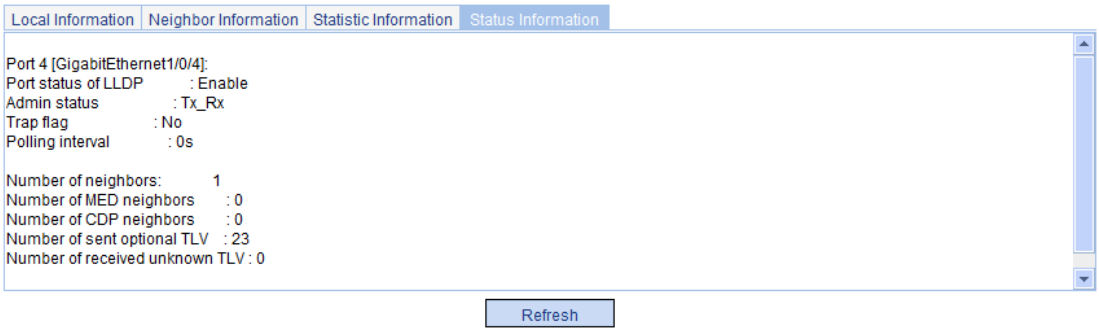
4. Click the **Statistics Information** tab to display the LLDP statistics.

Figure 206 The statistic information tab



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

Figure 207 The status information tab



Displaying global LLDP information

1. From the navigation tree, select **Network** > **LLDP**.
2. Click the **Global Summary** tab to display global local LLDP information and statistics. Table 80 describes the fields.

Figure 208 The global summary tab

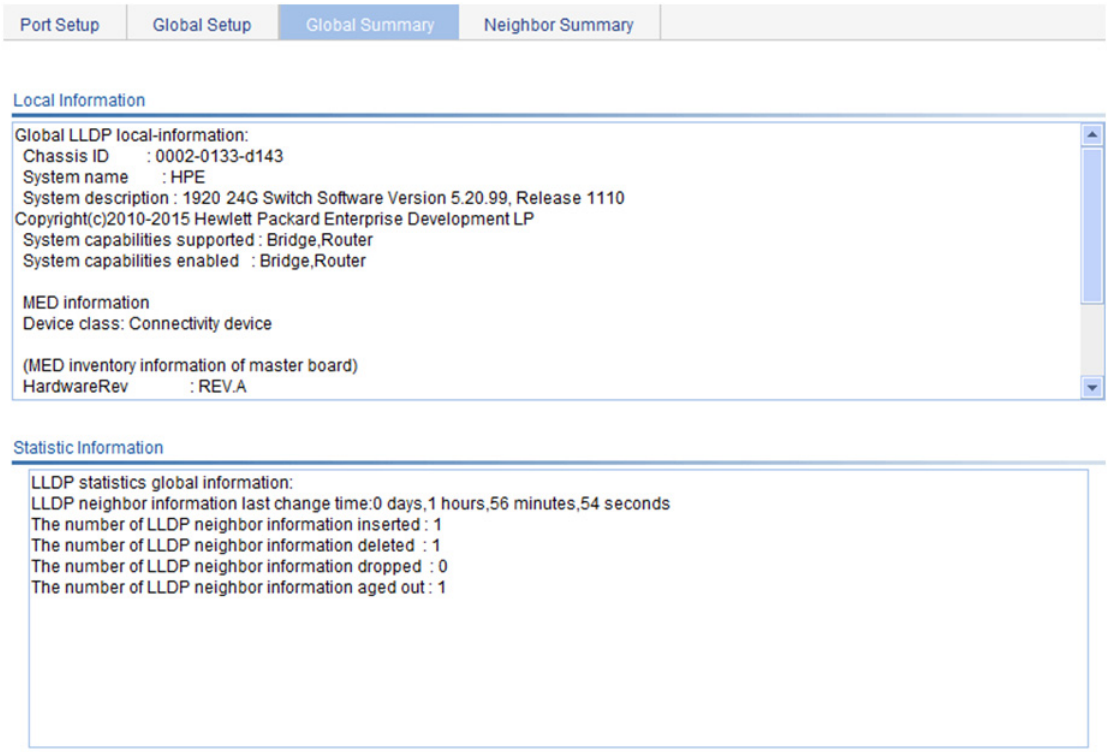


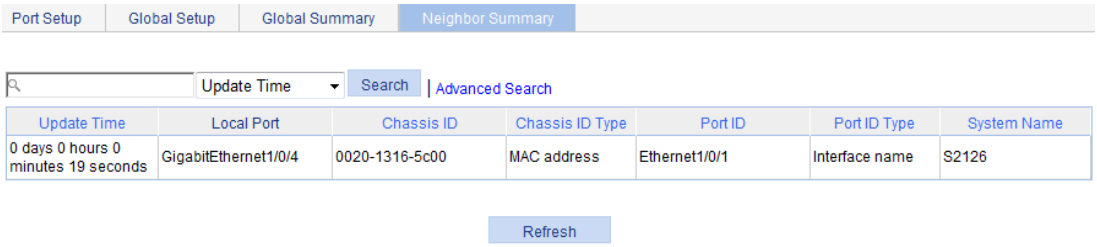
Table 80 Field description

Field	Description
Chassis ID	Local chassis ID depending on the chassis type defined.
System capabilities supported	Capabilities supported on the system: • Repeater. • Bridge. • Router.
System capabilities enabled	Capabilities enabled on the system: • Repeater. • Bridge. • Router.
Device class	MED device class: • **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 and 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. From the navigation tree, select **Network** > **LLDP**.
2. Click the **Neighbor Summary** tab to display the global LLDP neighbor information, as shown in Figure 209.

Figure 209 The neighbor summary tab

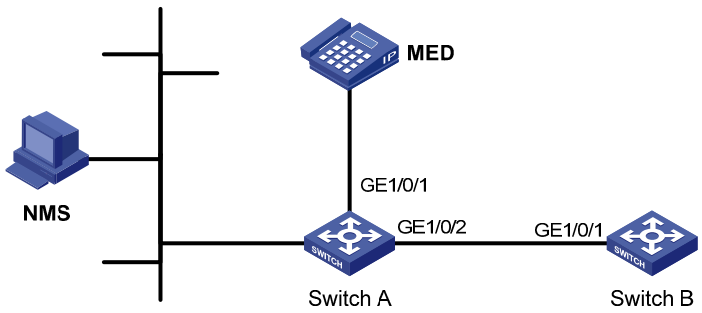


LLDP configuration example

Network requirements

As shown in Figure 210, configure LLDP on Switch A and Switch B so that the NMS can determine the status of the link between Switch A and MED and the link between Switch A and Switch B.

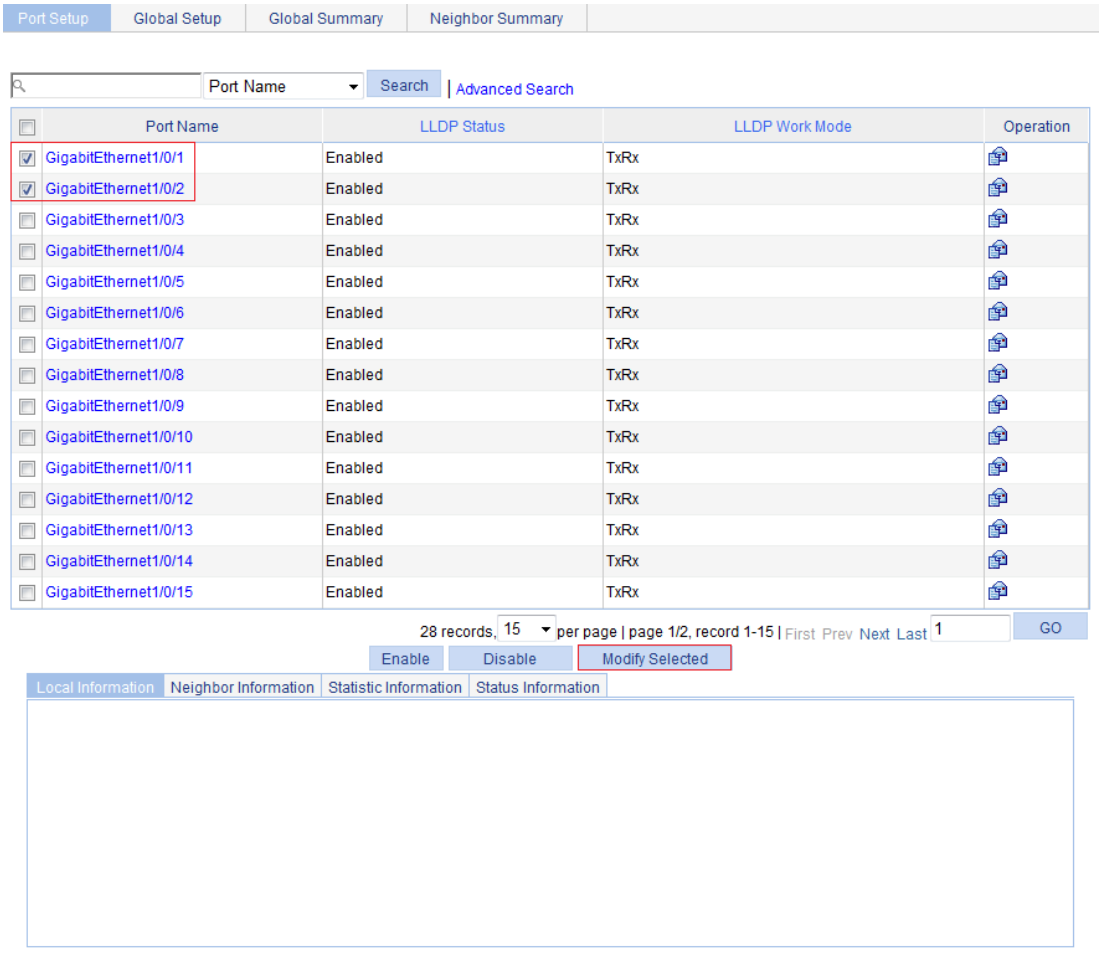
Figure 210 Network diagram



Configuring Switch A

1. (Optional.) Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. 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. From the navigation tree, select **Network** > **LLDP**.
      By default, the **Port Setup** tab is displayed, as shown in Figure 211.
   b. Select port **GigabitEthernet1/0/1** and **GigabitEthernet1/0/2**.
   c. Click **Modify Selected**.
      The page shown in Figure 212 appears.

Figure 211 The port setup tab



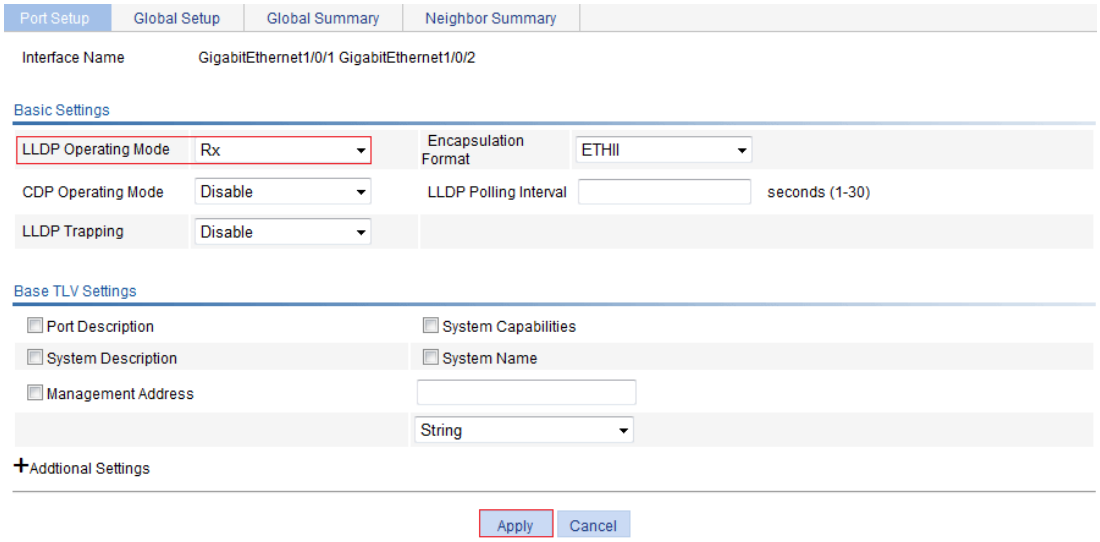
d. Select **Rx** from the **LLDP Operating Mode** list.

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.

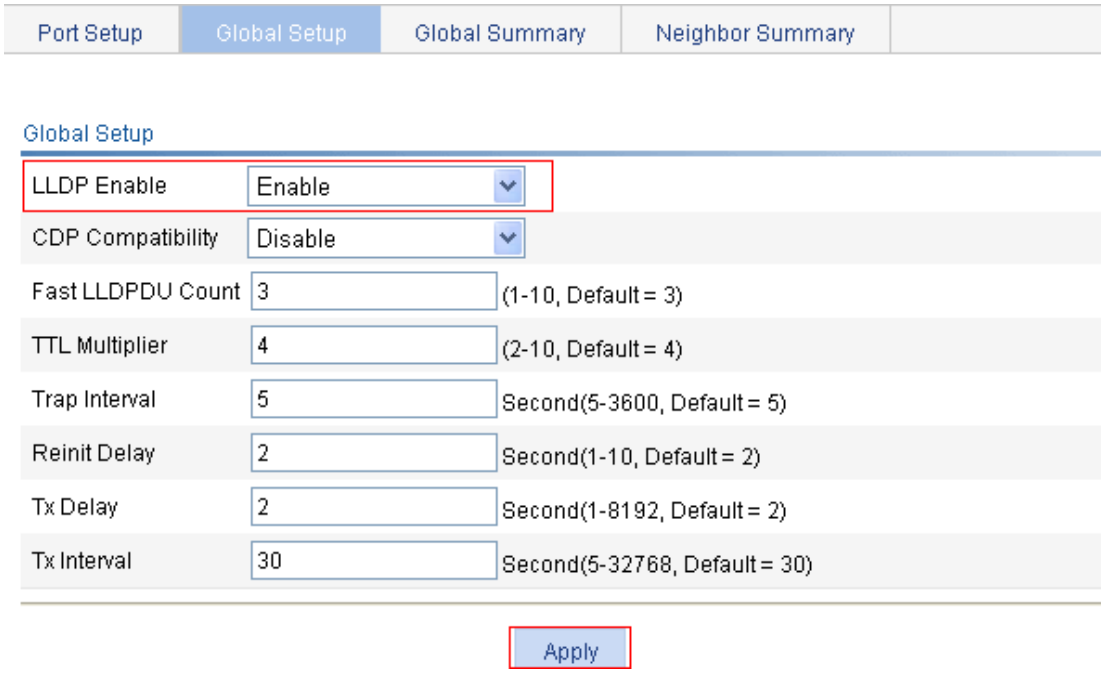
Figure 212 Setting LLDP on multiple ports



5. Enable global LLDP:
   a. Click the **Global Setup** tab, as shown in Figure 213.
   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.

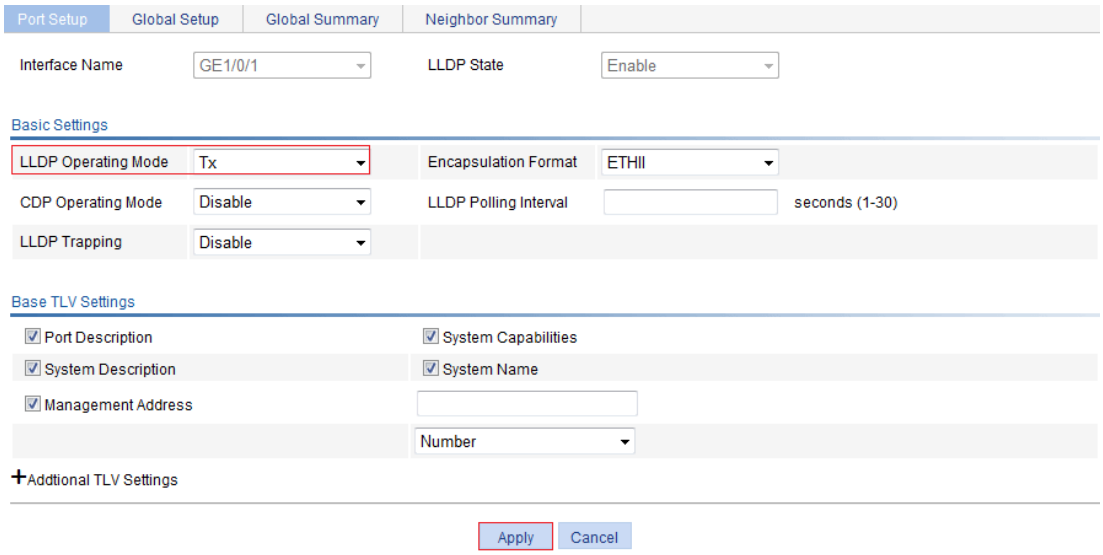
Figure 213 The global setup tab



Configuring Switch B

1. (Optional.) Enable LLDP on port GigabitEthernet 1/0/1. By default, LLDP is enabled on Ethernet ports.
2. Set the LLDP operating mode to Tx on GigabitEthernet 1/0/1:
   a. From the navigation tree, select **Network** > **LLDP**.
      By default, the **Port Setup** tab is displayed.
   b. Click the icon for port GigabitEthernet 1/0/1.
   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 214 Setting the LLDP operating mode to Tx

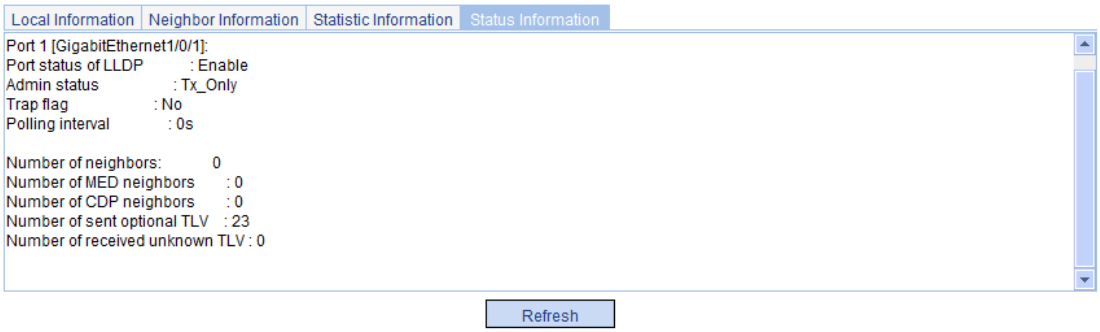


5. Enable global LLDP:
   a. Click the **Global Setup** tab.
   b. Select **Enable** from the **LLDP Enable** list.
6. Click **Apply**.
   A progress dialog box appears.
7. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Verifying the configuration

1. Display the status information of port GigabitEthernet 1/0/1 on Switch A:
   a. From the navigation tree, select **Network** > **LLDP**.
      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.

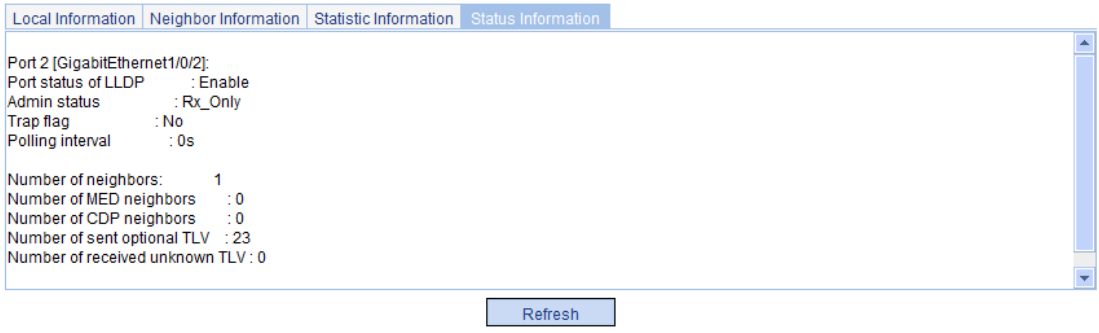
Figure 215 The status information tab (1)



2. Display the status information of port GigabitEthernet 1/0/2 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), as shown in Figure 216.

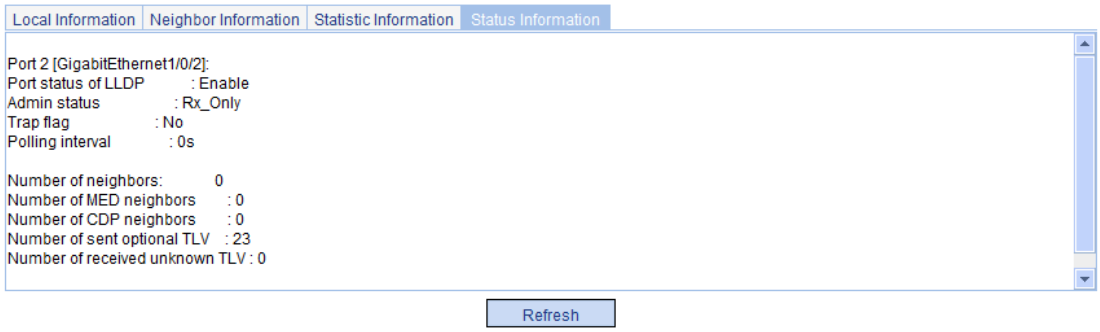
Figure 216 The status information tab (2)



3. Tear down the link between Switch A and Switch B.
4. Click **Refresh** to display the status information of port GigabitEthernet 1/0/2 on Switch A.

   The updated status information of port GigabitEthernet 1/0/2 shows that no neighbor device is connected to the port, as shown in Figure 217.

Figure 217 The status information tab displaying the updated port status information



LLDP configuration guidelines

When you configure LLDP, follow these guidelines:

- To make LLDP take effect on a port, enable LLDP both globally and on the port.

- To advertise LLDP-MED TLVs other than the LLDP-MED capabilities TLV, include the LLDP-MED capabilities TLV.
- To remove the LLDP-MED capabilities TLV, 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

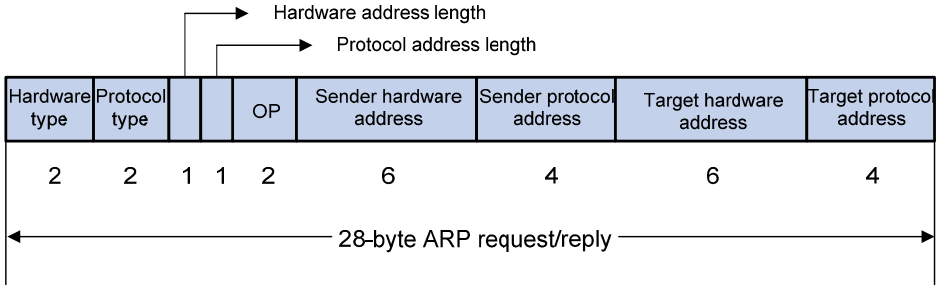
Overview

ARP resolves IP addresses into MAC addresses on Ethernet networks.

ARP message format

ARP uses two types of messages: ARP request and ARP reply. Figure 218 shows the format of the ARP request/reply messages. Numbers in the figure refer to field lengths.

Figure 218 ARP message format



- **Hardware type**—Hardware address type. The value 1 represents Ethernet.
- **Protocol type**—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. 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, which describes type of the ARP message. Value 1 represents an ARP request, and value 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 to which the message is being sent.
- **Target protocol address**—Protocol address of the device to which the message is being sent.

ARP operating mechanism

As shown in Figure 219, Host A and Host B are on the same subnet. Host A sends a packet to Host B as follows:

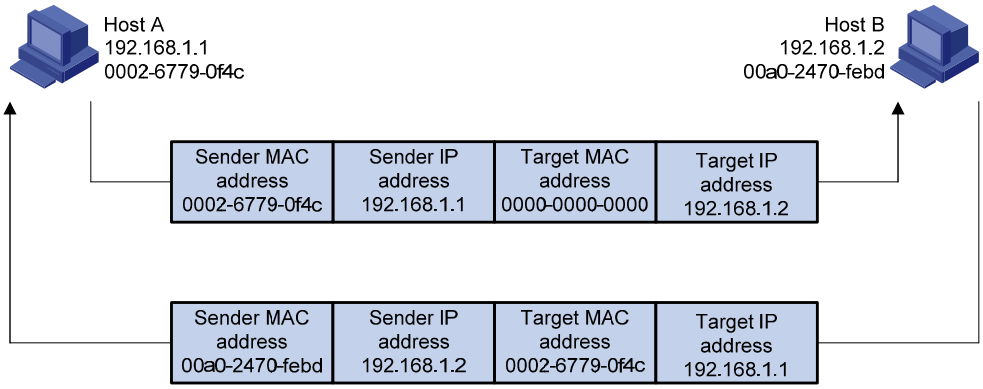
1. Host A looks through its ARP table for an ARP entry for Host B. If one entry is found, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame. Then Host A sends the frame to Host B.
2. If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request. The payload of the ARP request contains the following information:

- **Sender IP address and sender MAC address**—Host A's IP address and MAC address.
- **Target IP address**—Host B's IP address.
- **Target MAC address**—An all-zero MAC address.

All hosts on this subnet can receive the broadcast request, but only the requested host (Host B) processes 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 into 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 into its ARP table.
   b. Encapsulates the MAC address into the packet and sends the packet to Host B.

Figure 219 ARP address resolution process



If Host A and Host B are on different subnets, Host A sends a packet to Host B, as follows:

1. Host A broadcasts an ARP request to the gateway. The target IP address in the ARP request is the IP address of the gateway.
2. The gateway responds with its MAC address in an ARP reply to Host A.
3. Host A uses the gateway's MAC address to encapsulate the packet, and then sends the packet to the gateway.
4. If the gateway has an ARP entry for Host B, it forwards the packet to Host B directly. If not, the gateway broadcasts an ARP request, in which the target IP address is the IP address of Host B.
5. After the gateway gets the MAC address of Host B, it sends the packet to Host B.

ARP table

An ARP table stores 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 does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries protect communication between devices, because attack packets cannot modify the IP-to-MAC mapping in a static ARP entry.

Gratuitous ARP

In a gratuitous ARP packet, the sender IP address and the target IP address are the IP address of the sending device, the sender MAC address is the MAC address of the sending device, and the target MAC address is the broadcast address ff:ff:ff:ff:ff:ff.

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 is informed of the conflict by an ARP reply.
- Inform other devices of a MAC address change.

Gratuitous ARP packet learning

This feature enables a device to create or update ARP entries by using the sender IP and MAC addresses in received gratuitous ARP packets.

When this feature is disabled, the device uses the received gratuitous ARP packets to update existing ARP entries only.

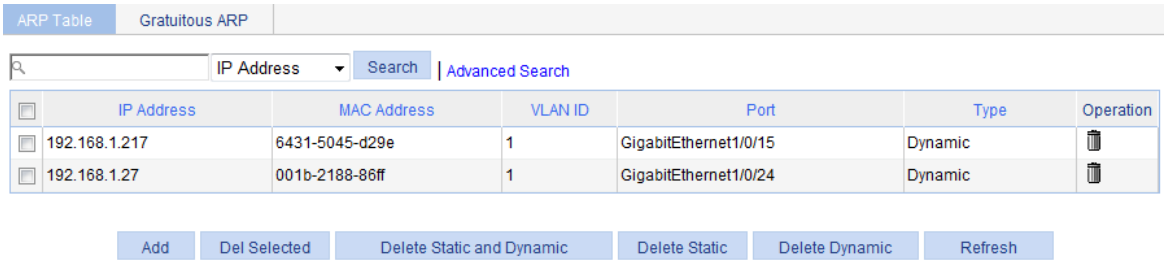
Configuring ARP entries

Displaying ARP entries

From the navigation tree, select **Network** > **ARP Management**. The default **ARP Table** page appears, as shown in Figure 220.

This page displays all ARP entries.

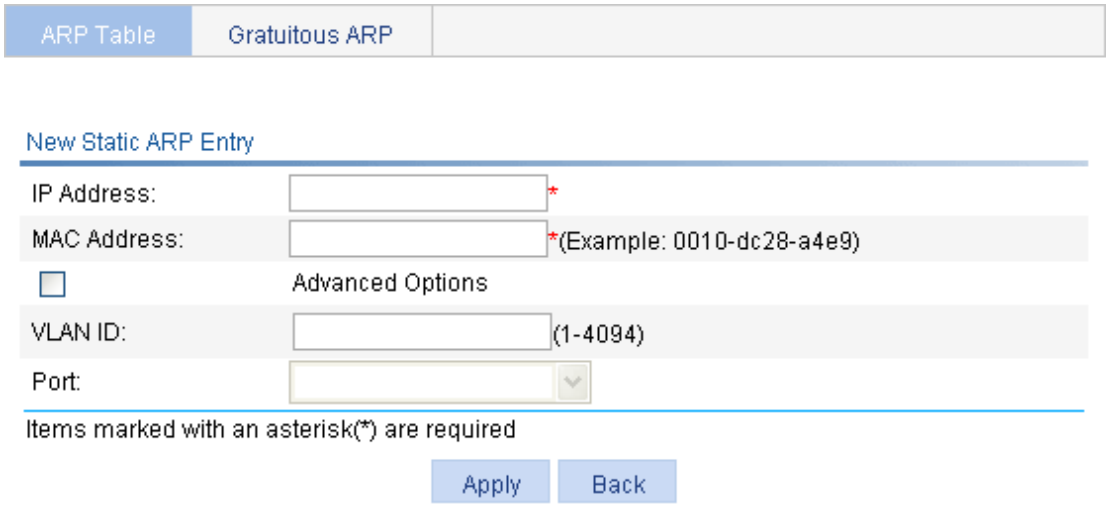
Figure 220 ARP Table configuration page



Creating a static ARP entry

1. From the navigation tree, select **Network** > **ARP Management**.
   The default **ARP Table** page appears, as shown in Figure 220.
2. Click **Add**.
   The **New Static ARP Entry** page appears.

Figure 221 Add a static ARP entry



3. Configure the static ARP entry as described in Table 81.
4. Click **Apply**.

Table 81 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

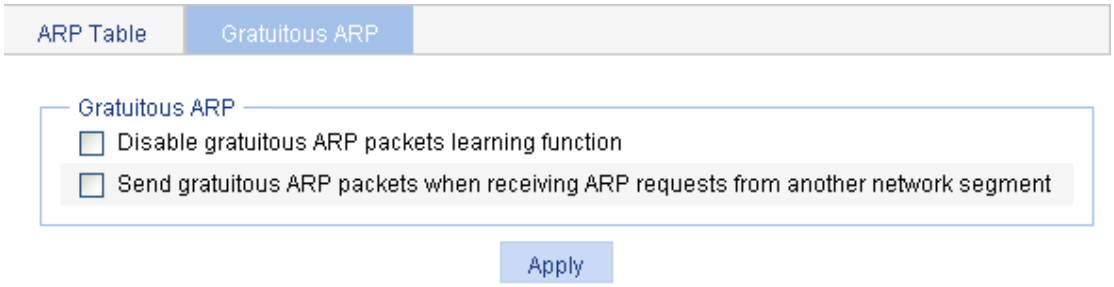
1. From the navigation tree, select **Network** > **ARP Management**.
   The default **ARP Table** page appears, as shown in Figure 220.
2. Remove ARP entries:

- 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. From the navigation tree, select **Network** > **ARP Management**.
2. Click the **Gratuitous ARP** tab.

Figure 222 Gratuitous Configuring ARP page



3. Configure gratuitous ARP as described in Table 82.
4. Click **Apply**.

Table 82 Configuration items

Item	Description
Disable gratuitous ARP packets learning function	Disable learning of ARP entries from gratuitous ARP packets. Gratuitous ARP packet learning is 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. By default, the device does not send gratuitous ARP packets upon receiving ARP requests from another network segment.

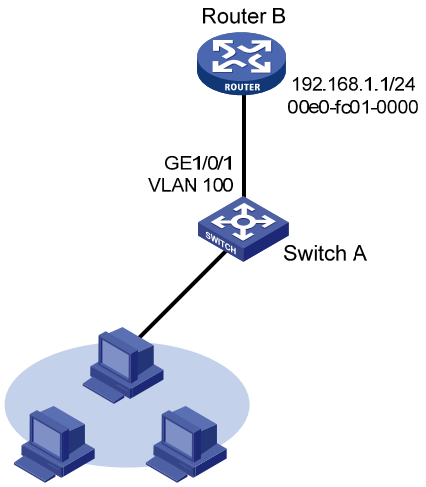
Static ARP configuration example

Network Requirements

As shown in Figure 223, hosts are connected to Switch A, and Switch A is connected to Router B through GigabitEthernet 1/0/1 in VLAN 100.

To ensure secure communications between Switch A and Router B, configure a static ARP entry on Switch A for Router B.

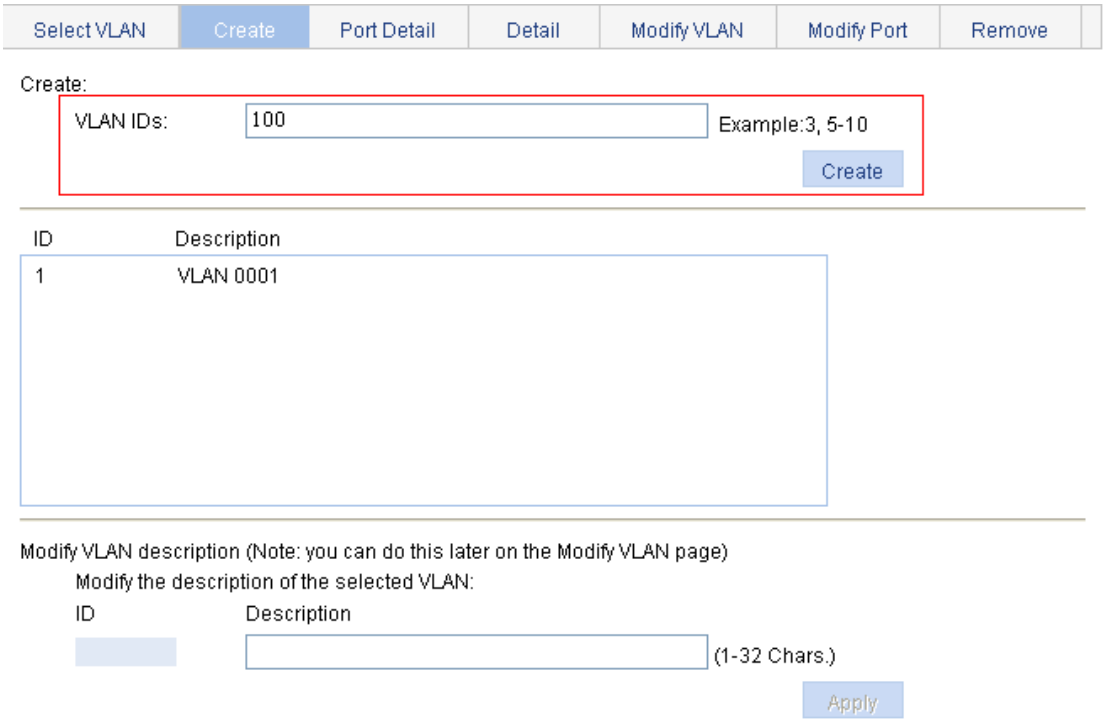
Figure 223 Network diagram



Configuring Switch A

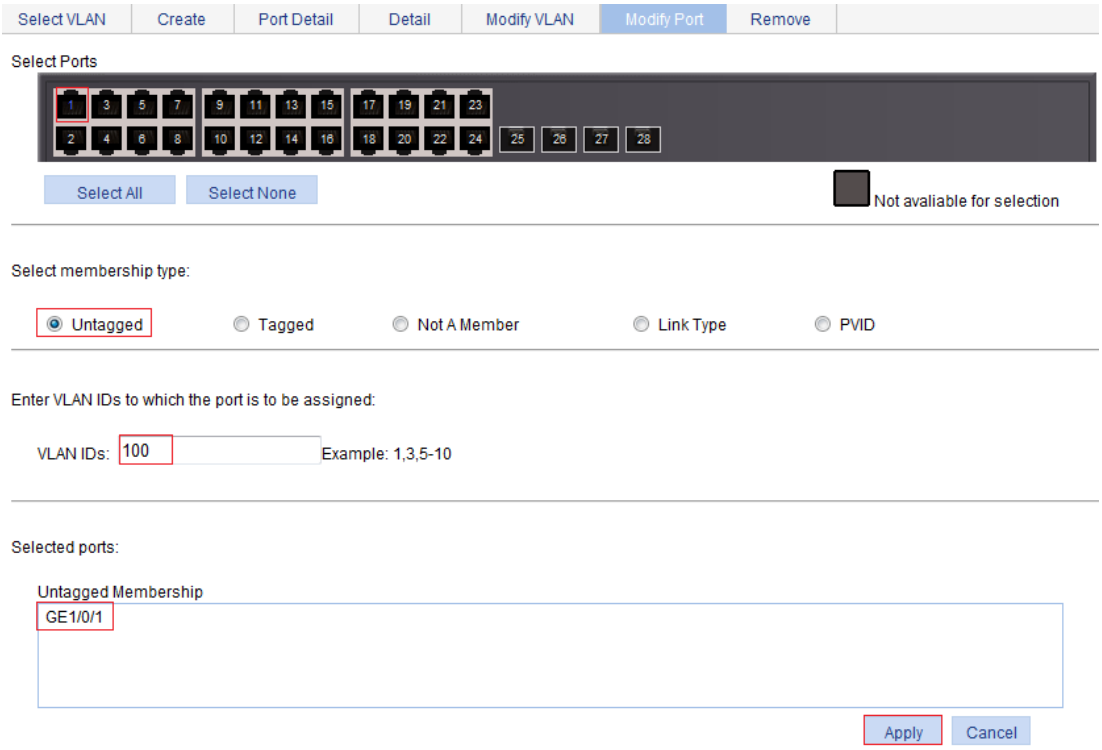
1. Create VLAN 100:
   a. From the navigation tree, select **Network** > **VLAN**.
   b. Click the **Add** tab.
   c. Enter **100** in the **VLAN ID** field.
   d. Click **Create**.

Figure 224 Creating VLAN 100



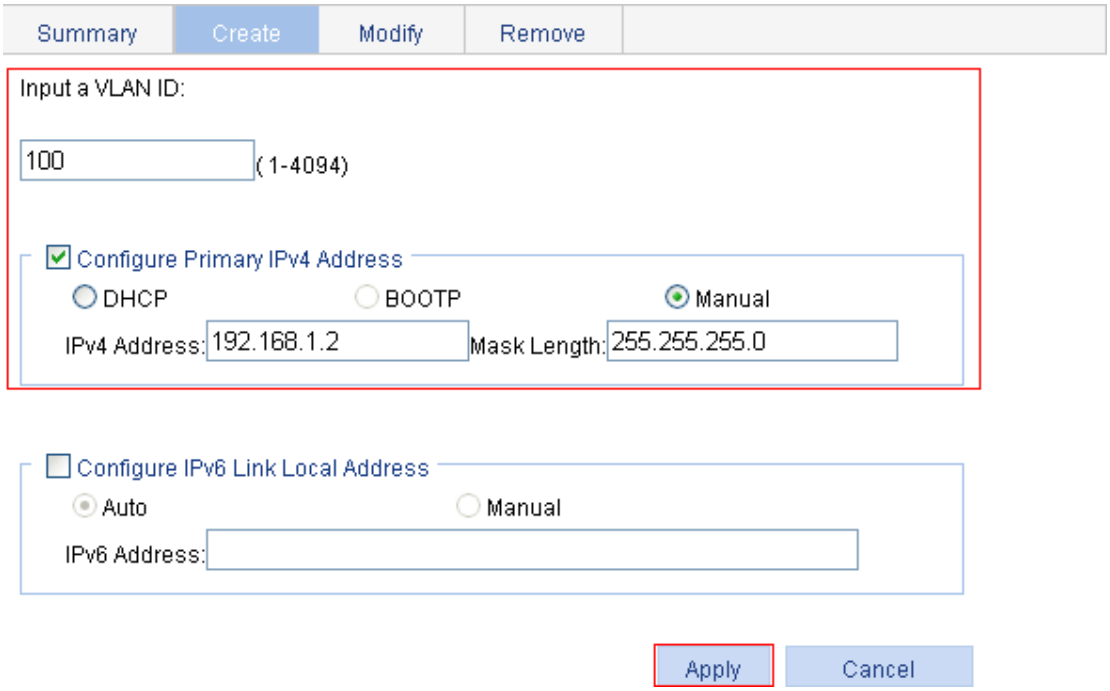
2. Add GigabitEthernet 1/0/1 to VLAN 100:
   a. Click the **Modify Port** tab.
   b. In the **Select Ports** area, select interface GigabitEthernet 1/0/1.
   c. Select **Untagged** for **Select membership type**.
   d. Enter **100** in the **VLAN IDs** field.
   e. Click **Apply**.
   A configuration process dialog box appears.
   f. After the configuration process is complete, click **Close**.

Figure 225 Adding GigabitEthernet 1/0/1 to VLAN 100



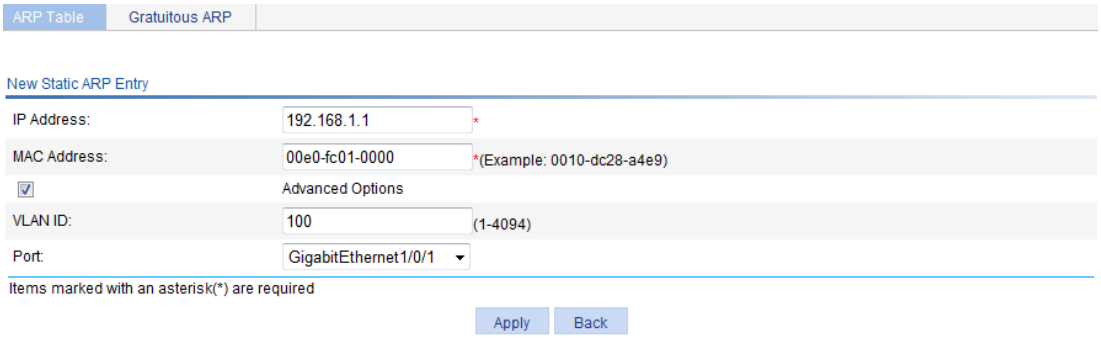
3. Create VLAN-interface 100:
   a. From the navigation tree, select **Network** > **VLAN Interface**.
   b. Click the **Create** tab.
   c. Enter **100** in the **VLAN ID** field.
   d. Select **Configure Primary IPv4 Address**.
   e. Select **Manual**.
   f. Enter **192.168.1.2** in the **IPv4 Address** field.
   g. Enter **24** or **255.255.255.0** in the **Mask Length** field.
   h. Click **Apply**.

Figure 226 Creating VLAN-interface 100



4. Create a static ARP entry:
   a. From the navigation tree, select **Network** > **ARP Management**.
      The default **ARP Table** page appears.
   b. Click **Add**.
   c. Enter **192.168.1.1** in the **IP Address** field.
   d. Enter **00e0-fc01-0000** in the **MAC Address** field.
   e. Select **Advanced Options**.
   f. Enter **100** in the **VLAN ID** field.
   g. Select **GigabitEthernet1/0/1** from the **Port** list.
   h. Click **Apply**.

Figure 227 Creating a static ARP entry



Configuring ARP attack protection

Overview

Although ARP is easy to implement, it provides no security mechanism and is vulnerable 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 user validity check and ARP packet validity check.

User validity check

This feature does not check ARP packets received from ARP trusted ports, but it checks ARP packets from ARP untrusted ports.

Upon receiving an ARP packet from an ARP untrusted interface, this feature compares the sender IP and MAC addresses against the DHCP snooping entries and 802.1X security entries. If a match is found from those entries, the ARP packet is considered valid and is forwarded. 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 ARP trusted ports. It checks ARP packets received from ARP untrusted ports based on the following objects:

- **src-mac**—Checks whether the sender MAC address in the message body 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 the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

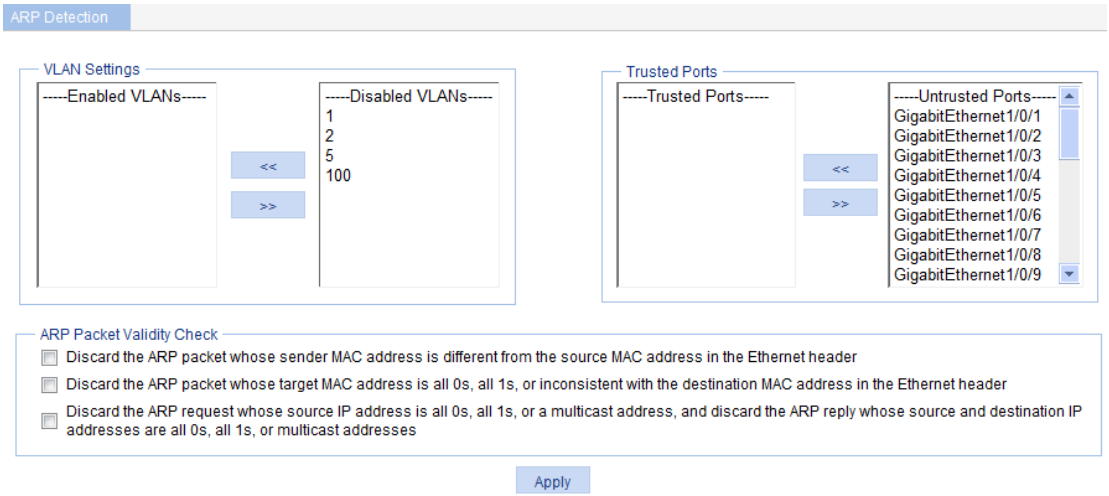
Configuring ARP detection

To check user validity, at least one among DHCP snooping entries and 802.1X security entries is available. Otherwise, all ARP packets received from ARP untrusted ports are discarded.

1. From the navigation tree, select **Network** > **ARP Anti-Attack**.

   The default **ARP Detection** page appears.

Figure 228 ARP detection configuration page



2. Configure ARP detection as described in Table 83.
3. Click **Apply**.

Table 83 Configuration items

Item	Description
VLAN Settings	Select VLANs on which ARP detection is to be enabled. To add VLANs to the **Enabled VLANs** list, select one or multiple VLANs from the **Disabled VLANs** list and click the **<<** button. To remove VLANs from the **Enabled VLANs** list, select one or multiple VLANs from the list and click the **>>** button.
Trusted Ports	Select trusted ports and untrusted ports. To add ports to the **Trusted Ports** list, select one or multiple ports from the **Untrusted Ports** list and click the **<<** button. To remove ports from the **Trusted Ports** list, select one or multiple ports from the list 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 sender IP address is all 1s or a multicast address, and discard the ARP reply whose sender and target IP addresses are all 1s or multicast addresses. If none 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 system performs the former first, and then the latter.

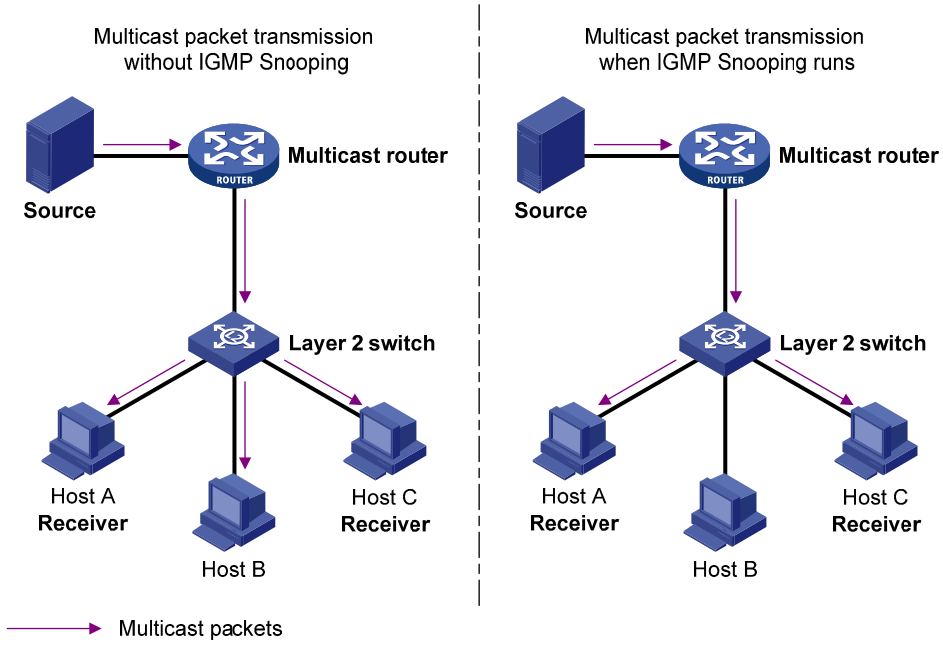
Configuring IGMP snooping

Overview

IGMP snooping runs on a Layer 2 switch as a multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from IGMP packets that are exchanged between the hosts and the router.

As shown in Figure 229, when IGMP snooping is not enabled, the Layer 2 switch floods multicast packets to all hosts. When IGMP snooping is enabled, the Layer 2 switch forwards multicast packets of known multicast groups to only the receivers of the multicast groups.

Figure 229 Multicast forwarding before and after IGMP snooping is enabled



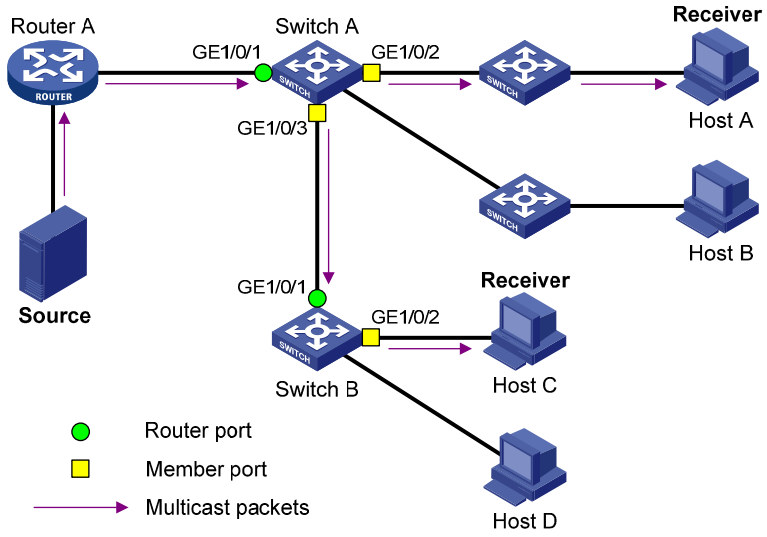
Basic IGMP snooping concepts

This section lists the basic IGMP snooping concepts.

IGMP snooping related ports

As shown in Figure 230, IGMP snooping runs on Switch A and Switch B, Host A and Host C are receivers in a multicast group.

Figure 230 IGMP snooping related ports



The following describes the ports involved in IGMP snooping:

- **Router port**—Layer 3 multicast device-side port. Layer 3 multicast devices include designated routers and IGMP queriers. In Figure 230, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. A switch records all its local router ports in its router port list.

  Do not confuse the "router port" in IGMP snooping with the "routed interface" commonly known as the "Layer 3 interface." The router port in IGMP snooping is the Layer 2 interface.
- **Member port**—Multicast receiver-side port. In Figure 230, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. A switch records all its member ports in the IGMP snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document include both dynamic and static ports.

NOTE:

When IGMP snooping is enabled, all ports that receive PIM hello messages or IGMP general queries with the source addresses other than 0.0.0.0 are considered dynamic router ports.

Aging timers for dynamic ports in IGMP snooping

Timer	Description	Message received before the timer expires	Action after the timer expires
Dynamic router port aging timer	When a port receives an IGMP general query with the source address other than 0.0.0.0 or PIM hello message, the switch starts or resets an aging timer for the port. When the timer expires, the dynamic router port ages out.	IGMP general query with the source address other than 0.0.0.0 or PIM hello message.	The switch removes this port from its router port list.
Dynamic member port aging timer	When a port dynamically joins a multicast group, the switch starts or resets 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.

How IGMP snooping works

The ports in this section are dynamic ports.

IGMP messages include general query, IGMP report, and leave message. An IGMP snooping-enabled switch performs differently depending on the message.

General query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to determine whether any active multicast group members exist on the subnet. The destination address of IGMP general queries is 224.0.0.1.

After receiving an IGMP general query, the switch forwards the query through all ports in the VLAN except the receiving port. The switch also performs one of the following actions:

- If the receiving port is a dynamic router port in the router port list, the switch restarts the aging timer for the port.
- If the receiving port is not in the router port list, the switch adds the port as a dynamic router port into the router port list and starts an aging timer for the port.

IGMP report

A host sends an IGMP report to the IGMP querier for the following purposes:

- Responds to IGMP queries if the host is a multicast group member.
- Applies for a multicast group membership.

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, and performs one of the following actions:

- If no forwarding entry matches the group address, the switch creates a forwarding entry for the group, adds the receiving port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.
- If a forwarding entry matches the group address, but the receiving port 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 the port.
- If a forwarding entry matches the group address and the receiving port is in the forwarding entry for the group, the switch restarts the aging timer for the port.

A switch does not forward an IGMP report through a non-router port. If the switch forwards a report message through a member port, the IGMP report suppression mechanism running on hosts causes all attached hosts that monitor the reported multicast address to suppress their own reports. In this case, the switch cannot determine whether the reported multicast group still has active members attached to that port.

Leave message

An IGMPv1 host silently leaves a multicast group and the switch is not notified of the leaving. However, because the host stops sending IGMP reports as soon as it leaves the multicast group, the switch removes the port that connects to the host from the forwarding entry for the multicast group when the aging timer for the port expires.

An IGMPv2 or IGMPv3 host sends an IGMP leave message to the multicast router when it leaves a multicast group.

When the switch receives an IGMP leave message on a dynamic member port, the switch first examines 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 message.
- If a forwarding entry matches the group address and the forwarding entry contains the port, the switch forwards the leave 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, it restarts the aging timer for the 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 the 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 of the multicast group. The switch also performs one of the following actions for the port that received the IGMP leave message:

- If the port (assuming that it is a dynamic member port) receives an IGMP report in response to the group-specific query before its aging timer expires, it means that some host attached to the port is receiving or expecting to receive multicast data for the multicast group. The switch restarts the aging timer for the port.
- If the port receives no IGMP report in response to the group-specific query before its aging timer expires, it means 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

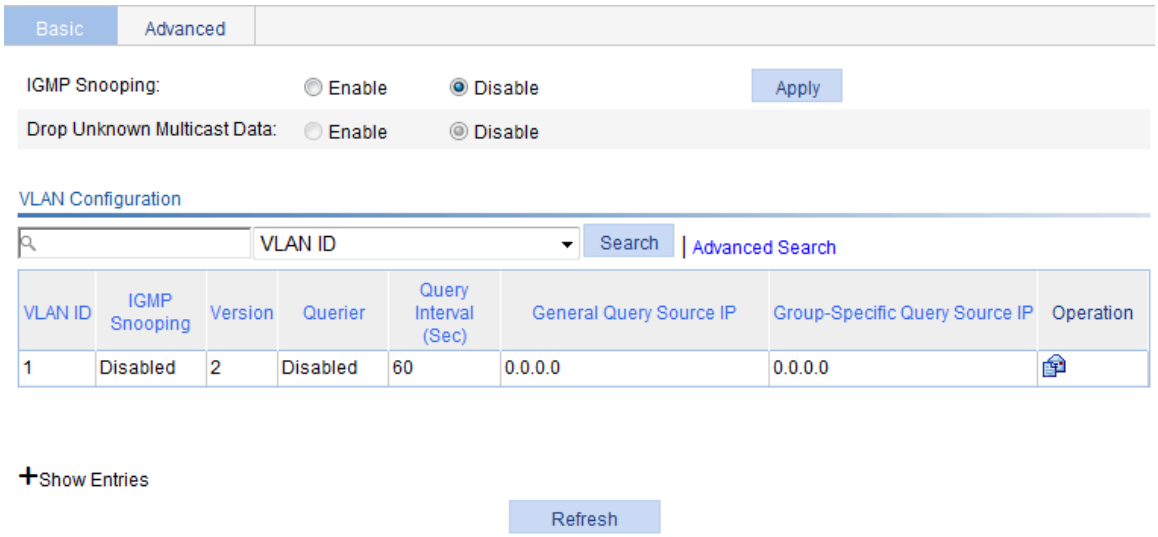
Step	Remarks
1. Enabling IGMP snooping globally	Required. Disabled by default.
2. Enabling dropping unknown multicast data globally	Optional. Unknown multicast data refers to multicast data for which no forwarding entries exist in the forwarding table. When the switch receives such multicast traffic, one of the following situations occurs: • If dropping unknown multicast data is disabled, the switch floods unknown multicast data in the VLAN. • If dropping unknown multicast data is enabled, the switch drops all received unknown multicast data. Disabled by default. Enable IGMP snooping globally before you enable dropping unknown multicast data globally.
3. Configuring IGMP snooping in a VLAN	Required. Enable IGMP snooping in the VLAN and configure the IGMP snooping version and querier feature. By default, IGMP snooping is disabled in a VLAN. When you enable IGMP snooping, follow these guidelines: • Enable IGMP snooping globally before you enable it for a VLAN. • IGMP snooping for a VLAN takes effect only on the member ports in that VLAN.

Step	Remarks
4. Configuring IGMP snooping port functions	Optional. Configure the maximum number of multicast groups and fast-leave processing on a port of the specified VLAN. When you configure IGMP snooping port functions, follow these guidelines: • Before you enable IGMP snooping on a port, enable multicast routing or IGMP snooping globally. • IGMP snooping enabled on a port takes effect only after IGMP snooping is enabled in the VLAN or IGMP is enabled on the VLAN interface.
5. Displaying IGMP snooping multicast forwarding entries	Optional.

Enabling IGMP snooping globally

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click **Enable** for IGMP snooping.
3. Click **Apply**.

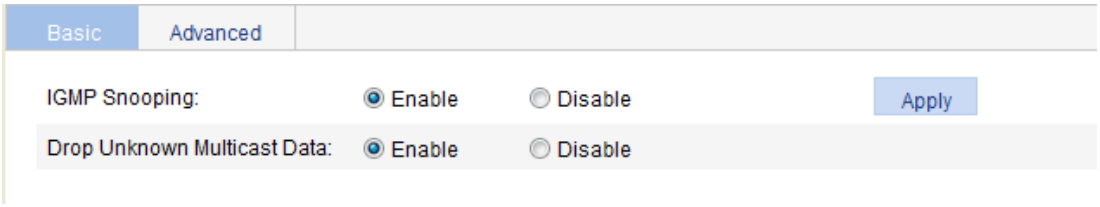
Figure 231 Enabling IGMP snooping globally



Enabling dropping unknown multicast data globally

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click **Enable** for **Drop Unknown Multicast Data**.

Figure 232 Enabling dropping unknown multicast data globally

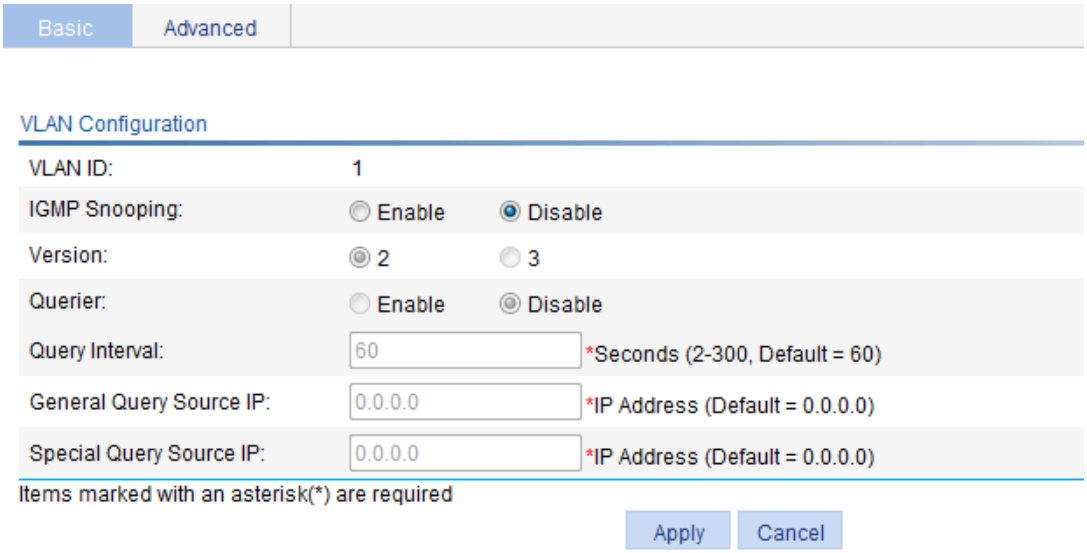


3. Click **Apply**.

Configuring IGMP snooping in a VLAN

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click the icon for the VLAN.

Figure 233 Configuring IGMP snooping in a VLAN



3. Configure the parameters as described in Table 84.
4. Click **Apply**.

Table 84 Configuration items

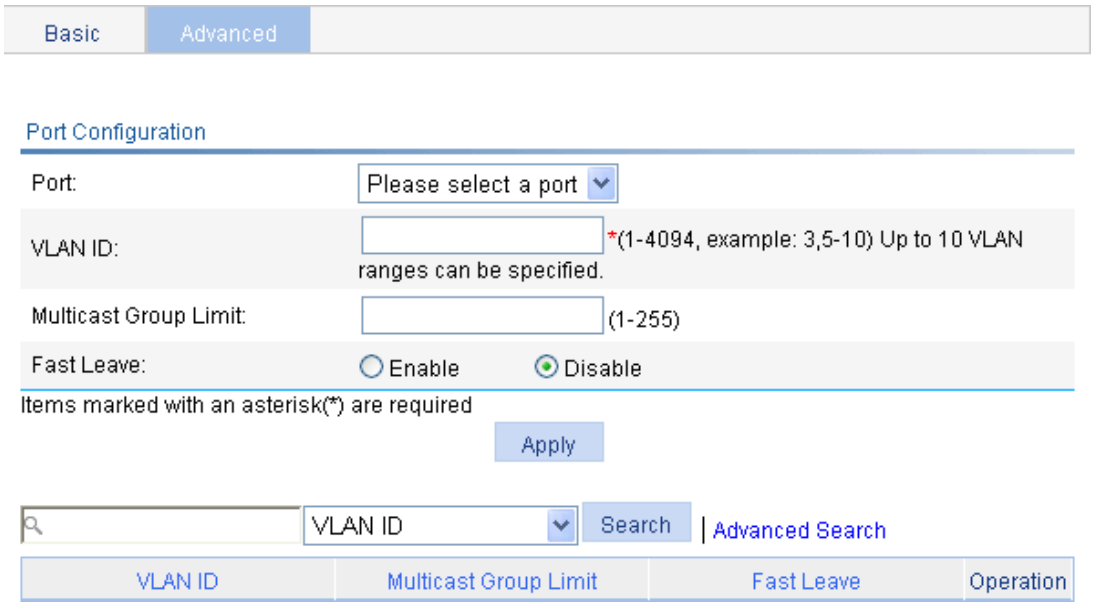
Item	Description
IGMP snooping	Enable or disable IGMP snooping in the VLAN. You can proceed with the subsequent configurations only if **Enable** is selected here.
Version	The default setting is IGMPv2. By configuring an IGMP snooping version, you actually configure the versions of IGMP messages that IGMP snooping can process. • IGMPv2 snooping can process IGMPv1 and IGMPv2 messages, but it floods IGMPv3 messages in the VLAN instead of processing them. • IGMPv3 snooping can process IGMPv1, IGMPv2, and IGMPv3 messages. **IMPORTANT:** If you change IGMPv3 snooping to IGMPv2 snooping, the system clears all IGMP snooping forwarding entries that are dynamically added.

Item	Description
Querier	Enable or disable the IGMP snooping querier function. On an IP multicast network that runs IGMP, a Layer 3 device acts as an IGMP querier to send IGMP queries and establish and maintain multicast forwarding entries, ensuring correct multicast traffic forwarding at the network layer. On a network without Layer 3 multicast devices, IGMP querier cannot work 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 the data link layer, providing IGMP querier functions.
Query interval	Configure the IGMP 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 port functions

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click the **Advanced** tab.

Figure 234 Configuring IGMP snooping port functions



3. Configure the parameters as described in Table 85.
4. Click **Apply**.

Table 85 Configuration items

Item	Description
Port	Select the port on which advanced IGMP snooping features will be configured. The port can be an GigabitEthernet port or Layer 2 aggregate interface. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. **TIP:** The advanced IGMP snooping configurations on a Layer 2 aggregate interface do not interfere with configurations on its member ports, nor do they participate in aggregation calculations. The configuration on a member port of the aggregate group does not take effect until the port leaves the aggregate group.
VLAN ID	Specify the ID of the VLAN in which the port functions are to be configured. The configurations made in a VLAN take effect on the ports only in this VLAN.
Group Limit	Configure the maximum number of multicast groups on a port. With this feature, you can limit multicast traffic on the port. **IMPORTANT:** If the number of multicast groups on a port exceeds the limit that you are setting, the system removes all the forwarding entries related to that port from the IGMP snooping forwarding table. The receiver hosts attached to that port can join multicast groups again before the number of multicast groups on the port reaches the limit.
Fast Leave	Enable or disable fast-leave processing on the port. When a port that is enabled with the IGMP snooping fast-leave processing feature receives an IGMP leave message, the switch immediately removes that port from the forwarding entry for the multicast group specified in the message. When the switch receives IGMP group-specific queries for that multicast group, it does not forward them to that port. You can enable IGMP snooping fast-leave processing on ports to save bandwidth and resources.

Displaying IGMP snooping multicast forwarding entries

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click **Show Entries** to display information about IGMP snooping multicast forwarding entries.

   Figure 235 Displaying entry information

3. To display detailed information about an entry, click the icon for the entry.

Figure 236 Displaying detailed information about the entry

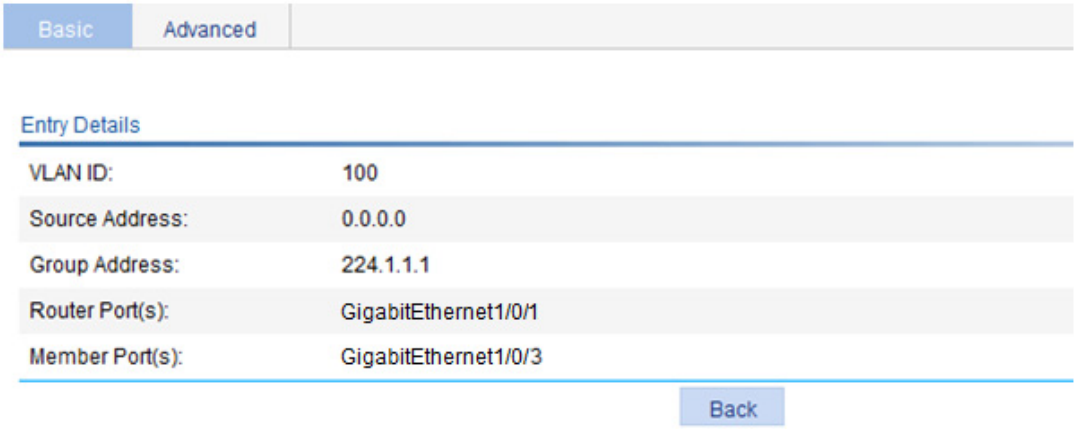


Table 86 Field description

Field	Description
VLAN ID	ID of the VLAN to which the entry belongs.
Source Address	Multicast source address. If no multicast sources are specified, this field displays **0.0.0.0**.
Group Address	Multicast group address.
Router Port(s)	All router ports.
Member Port(s)	All member ports.

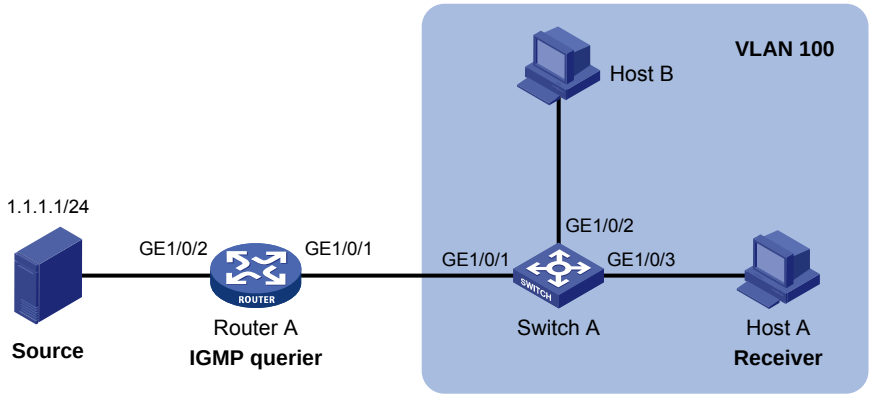
IGMP snooping configuration example

Network requirements

As shown in Figure 237, IGMPv2 runs on Router A and IGMPv2 snooping runs on Switch A. Router A acts as the IGMP querier.

Perform the configuration so Host A can receive the multicast data addressed to the multicast group **224.1.1.1**.

Figure 237 Network diagram



Configuration procedure

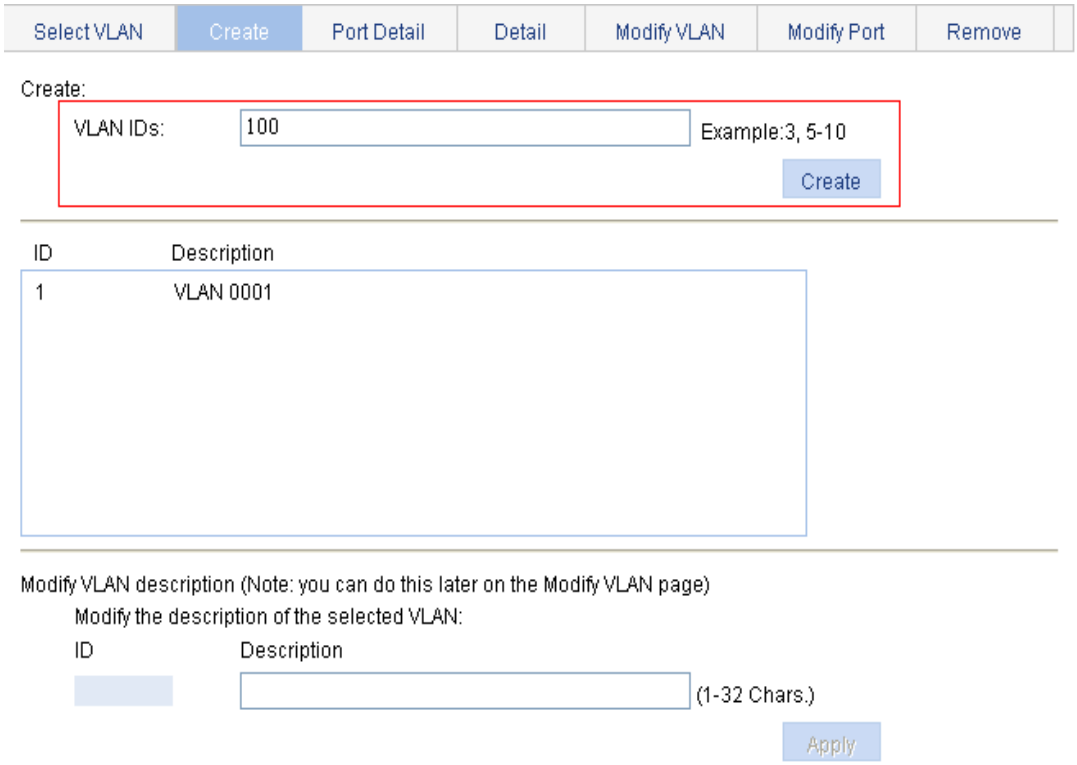
Configuring Router A

Enable IP multicast routing globally, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1. (Details not shown.)

Configuring Switch A

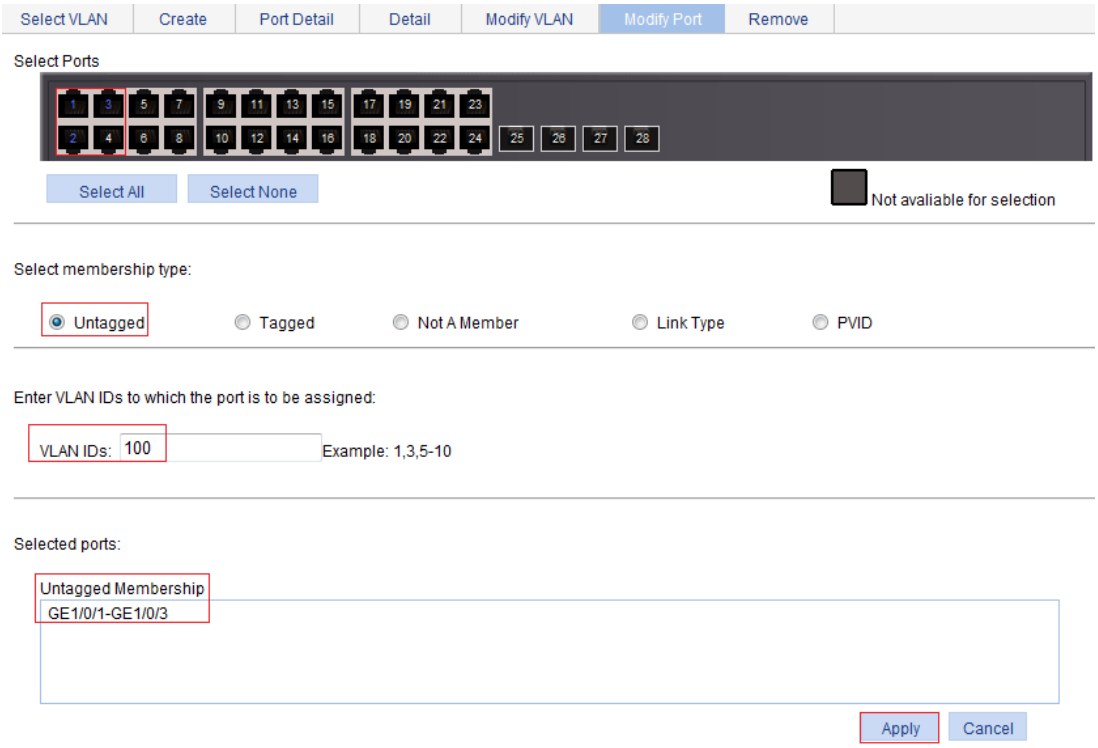
1. Create VLAN 100:
   a. From the navigation tree, select **Network** > **VLAN**.
   b. Click the **Create** tab.
   c. Enter **100** as the VLAN ID.
   d. Click **Apply**.

Figure 238 Creating VLAN 100



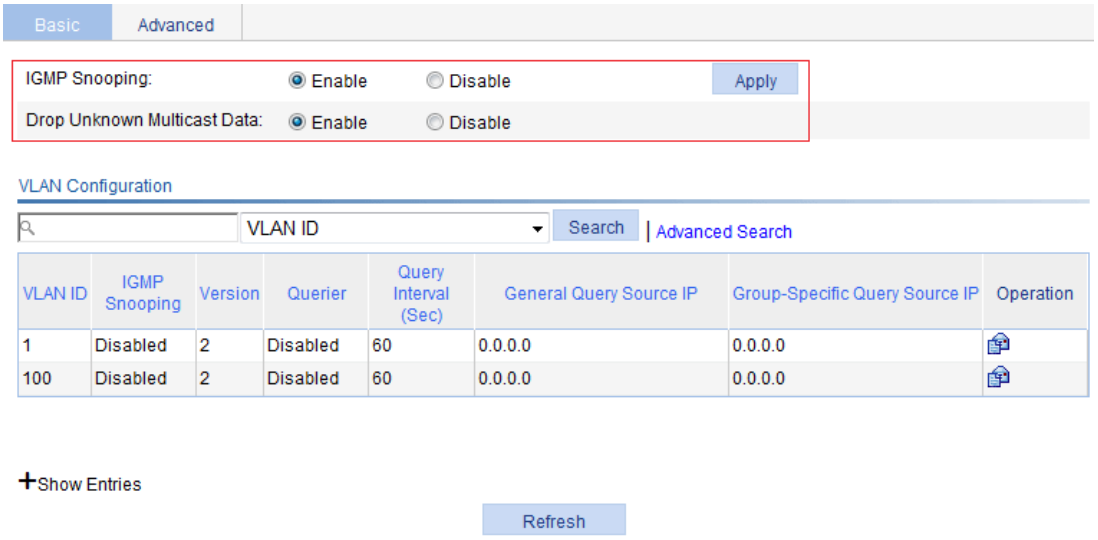
2. Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100:
   a. Click the **Modify Port** tab.
   b. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** area.
   c. Select **Untagged** for **Select membership type**.
   d. Enter **100** as the VLAN ID.
   e. Click **Apply**.

Figure 239 Assigning ports to the VLAN



3. Enable IGMP snooping and dropping unknown multicast data globally:
   a. From the navigation tree, select **Network** > **IGMP snooping**.
   b. Select **Enable**.
   c. Click **Apply**.

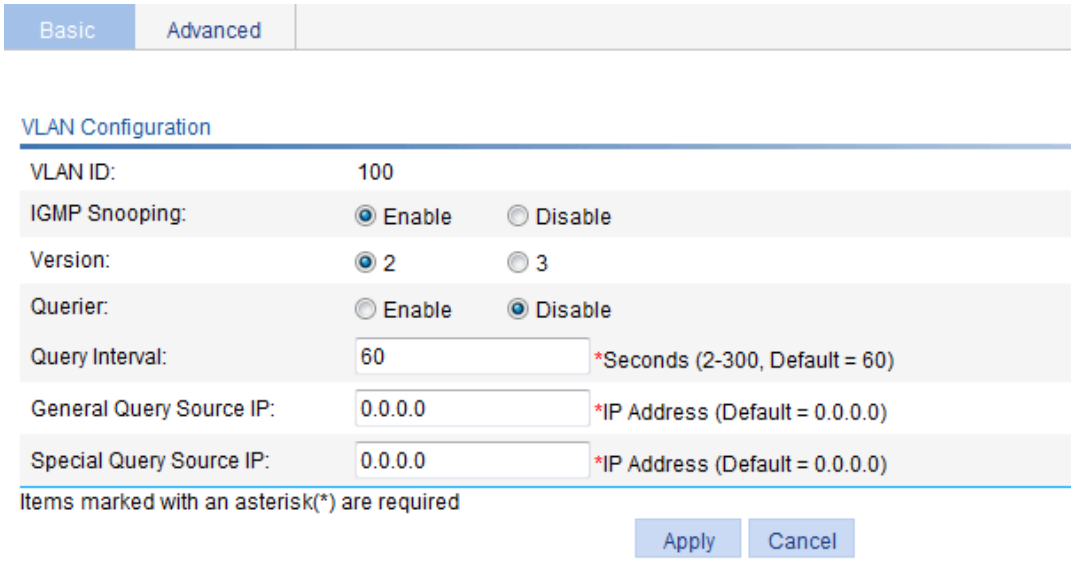
Figure 240 Enabling IGMP snooping and dropping unknown multicast data globally



4. Enable IGMP snooping for VLAN 100:
   a. Click the icon for VLAN 100.
   b. Select **Enable** for **IGMP snooping**.
   c. Select **2** for **Version**.

d. Click **Apply**.

Figure 241 Configuring IGMP snooping in VLAN 100



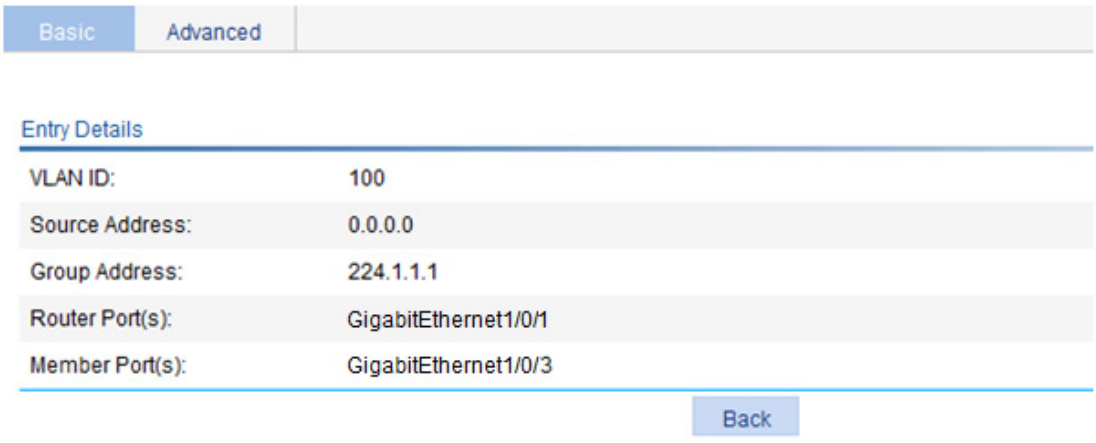
Verifying the configuration

1. From the navigation tree, select **Network** > **IGMP snooping**.
2. Click **Show Entries** in the basic VLAN configuration page to display information about IGMP snooping multicast forwarding entries.

Figure 242 Displaying IGMP snooping multicast forwarding entries

3. Click the icon for the multicast entry (**0.0.0.0**, **224.1.1.1**) to display detailed information about this entry.

Figure 243 Displaying detailed information about the entry



The output shows that GigabitEthernet 1/0/3 of Switch A is listening to the multicast streams destined for multicast group **224.1.1.1**.

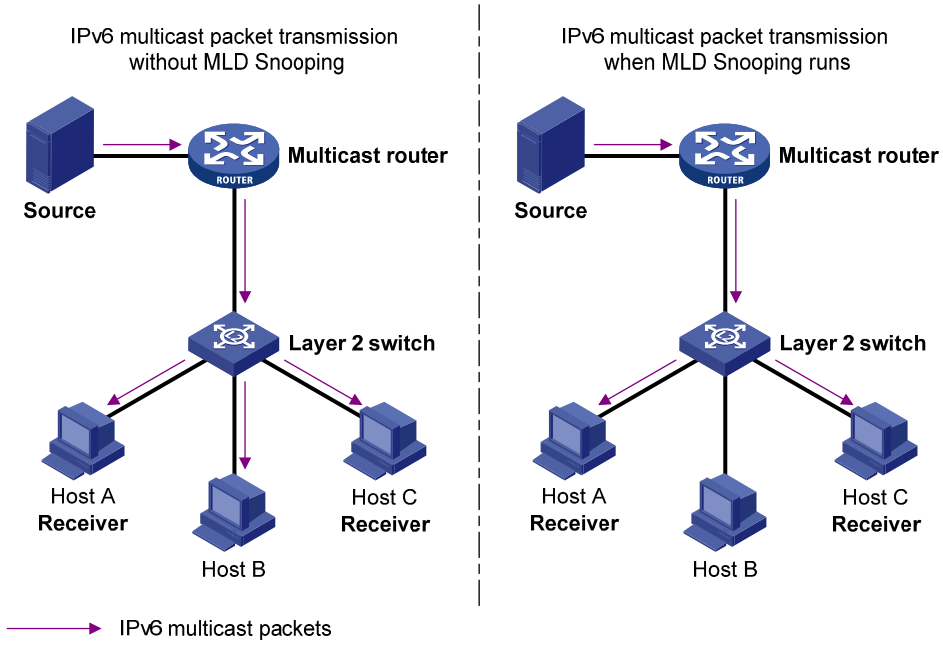
Configuring MLD snooping

Overview

MLD snooping runs on a Layer 2 switch as an IPv6 multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from MLD messages that are exchanged between the hosts and the router.

As shown in Figure 244, when MLD snooping is not enabled, the Layer 2 switch floods IPv6 multicast packets to all hosts. When MLD snooping is enabled, the Layer 2 switch forwards multicast packets of known IPv6 multicast groups to only the receivers of the multicast groups.

Figure 244 IPv6 multicast forwarding before and after MLD snooping is enabled



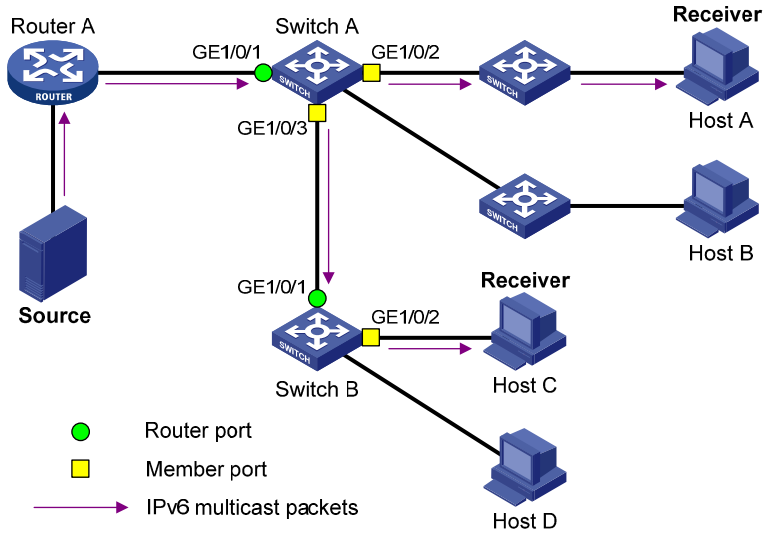
Basic MLD snooping concepts

This section lists the basic MLD snooping concepts.

MLD snooping related ports

As shown in Figure 245, MLD snooping runs on Switch A and Switch B. Host A and Host C are receivers in an IPv6 multicast group.

Figure 245 MLD snooping related ports



The following describes the ports involved in MLD snooping:

- **Router port**—Layer 3 multicast device-side port. Layer 3 multicast devices include designated routers and MLD queriers. As shown in Figure 245, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. A switch records all its local router ports in its router port list.

  Do not confuse the "router port" in MLD snooping with the "routed interface" commonly known as the "Layer 3 interface." The router port in MLD snooping is a Layer 2 interface.
- **Member port**—Multicast receiver-side port. As shown in Figure 245, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. A switch records all local member ports in its MLD snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document include both dynamic and static ports.

NOTE:

When MLD snooping is enabled, all ports that receive IPv6 PIM hello messages or MLD general queries with source addresses other than 0::0 are considered dynamic router ports.

Aging timers for dynamic ports in MLD snooping

Timer	Description	Message received before the timer expires	Action after the timer expires
Dynamic router port aging timer	When a port receives an MLD general query with the source address other than 0::0 or IPv6 PIM hello message, the switch starts or resets an aging timer. When the timer expires, the dynamic router port ages out.	MLD general query with the source address other than 0::0 or IPv6 PIM hello message.	The switch removes this port from its router port list.
Dynamic member port aging timer	When a port dynamically joins an IPv6 multicast group, the switch starts or resets 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.

How MLD snooping works

The ports in this section are dynamic ports.

MLD messages include general query, MLD report, and done message. An MLD snooping-enabled switch performs differently depending on the MLD message.

General query

The MLD querier periodically sends MLD general queries to all hosts and routers on the local subnet to check whether any active IPv6 multicast group members exist on the subnet. The destination IPv6 address of MLD general queries is FF02::1.

After receiving an MLD general query, the switch forwards the query to all ports in the VLAN except the receiving port. The switch also performs one of the following actions:

- If the receiving port is a dynamic router port in the router port list, the switch restarts the aging timer for the router port.
- If the receiving port is not in the router port list, the switch adds the port as a dynamic router port to the router port list and starts an aging timer for the port.

MLD report

A host sends an MLD report to the MLD querier for the following purposes:

- Responds to queries if the host is an IPv6 multicast group member.
- Applies for an IPv6 multicast group membership.

After receiving an MLD report, the switch forwards it through all the router ports in the VLAN and resolves the address of the reported IPv6 multicast group. The switch also performs one of the following actions:

- If no forwarding entry matches the IPv6 group address, the switch creates a forwarding entry for the group, adds the receiving port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.
- If a forwarding entry matches the IPv6 group address, but the receiving port 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 the port.
- If a forwarding entry matches the IPv6 group address and the receiving port is in the forwarding entry for the group, the switch resets an aging timer for the port.

A switch does not forward an MLD report through a non-router port. If the switch forwards a report through a member port, the MLD report suppression mechanism causes all attached hosts that monitor the reported IPv6 multicast group address to suppress their own reports. In this case, the switch cannot determine whether the reported IPv6 multicast group still has active members attached to that port.

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, the switch first examines whether a forwarding entry matches the IPv6 group address in the message, and, if a match is found, determines 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 one of the following actions for 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 means 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 means 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

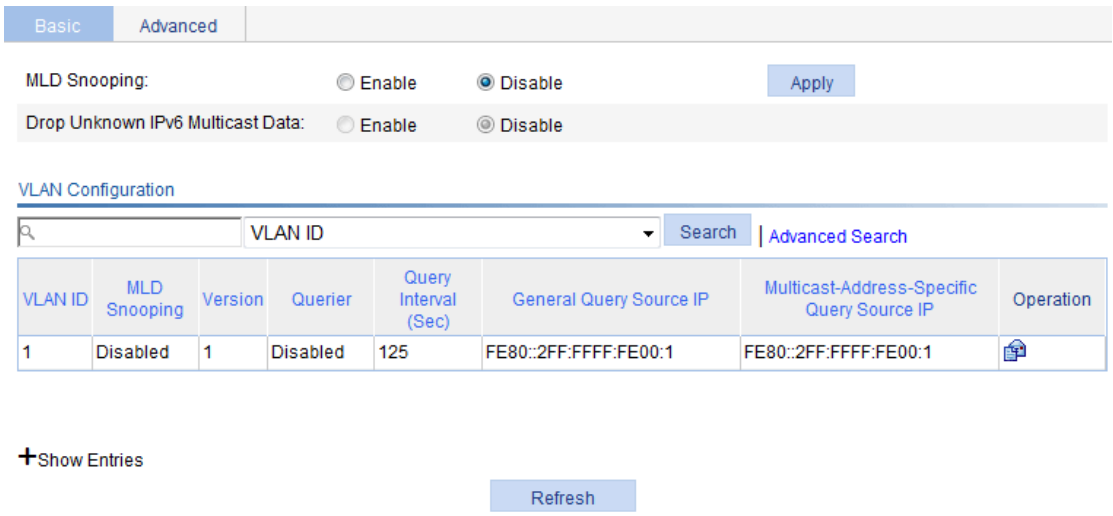
Step	Remarks
1. Enabling MLD snooping globally	Required. Disabled by default.
2. Enabling dropping unknown IPv6 multicast data globally	Optional. Unknown multicast data refers to multicast data for which no forwarding entries exist in the forwarding table. When the switch receives such multicast traffic, one of the following situations occurs: • If dropping unknown IPv6 multicast data is disabled, the switch floods unknown multicast data in the VLAN. • If dropping unknown IPv6 multicast data is enabled, the switch drops all received unknown multicast data. Disabled by default. Enable MLD snooping globally before you enable dropping unknown IPv6 multicast data globally.
3. Configuring MLD snooping in a VLAN	Required. Enable MLD snooping in the VLAN and configure the MLD snooping version and querier. By default, MLD snooping is disabled in a VLAN. When you enable MLD snooping, follow these guidelines: • Enable MLD snooping globally before you enable it for a VLAN. • MLD snooping for a VLAN takes effect only on the member ports in that VLAN.

Step	Remarks
4. Configuring MLD snooping port functions	Optional. Configure the maximum number of IPv6 multicast groups and fast-leave processing on a port of the specified VLAN. When you configure MLD snooping port functions, follow these guidelines: • Enable MLD snooping globally before you enable it on a port. • MLD snooping enabled on a port takes effect only after MLD snooping is enabled for the VLAN.
5. Displaying MLD snooping multicast forwarding entries	Optional.

Enabling MLD snooping globally

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Enable** for MLD snooping.
3. Click **Apply**.

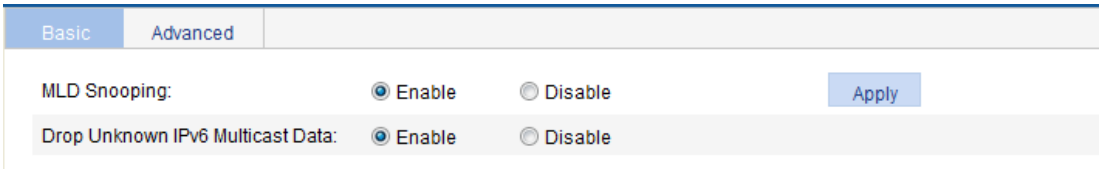
Figure 246 Enabling MLD snooping globally



Enabling dropping unknown IPv6 multicast data globally

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Enable** for **Drop Unknown IPv6 Multicast Data**.

Figure 247 Enabling dropping unknown IPv6 multicast data globally

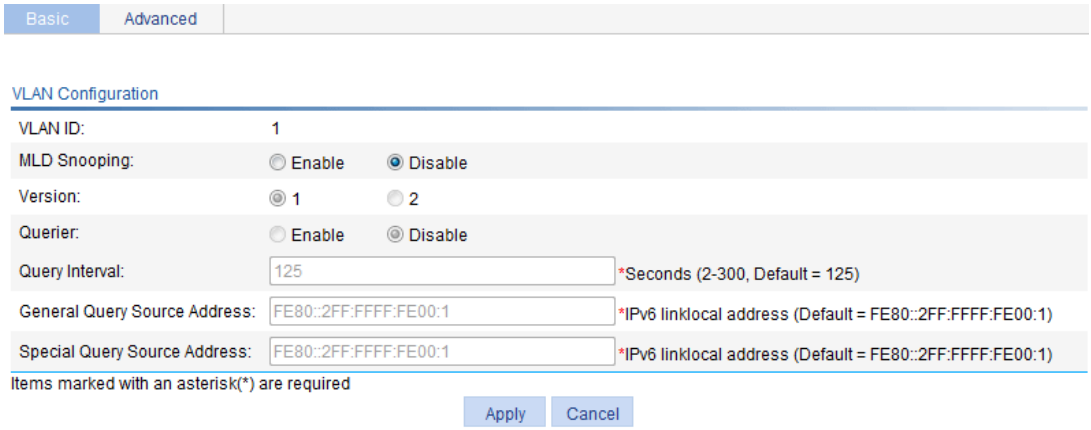


3. Click **Apply**.

Configuring MLD snooping in a VLAN

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click the icon for the VLAN.

Figure 248 Configuring MLD snooping in a VLAN



3. Configure the parameters as described in Table 87.
4. Click **Apply**.

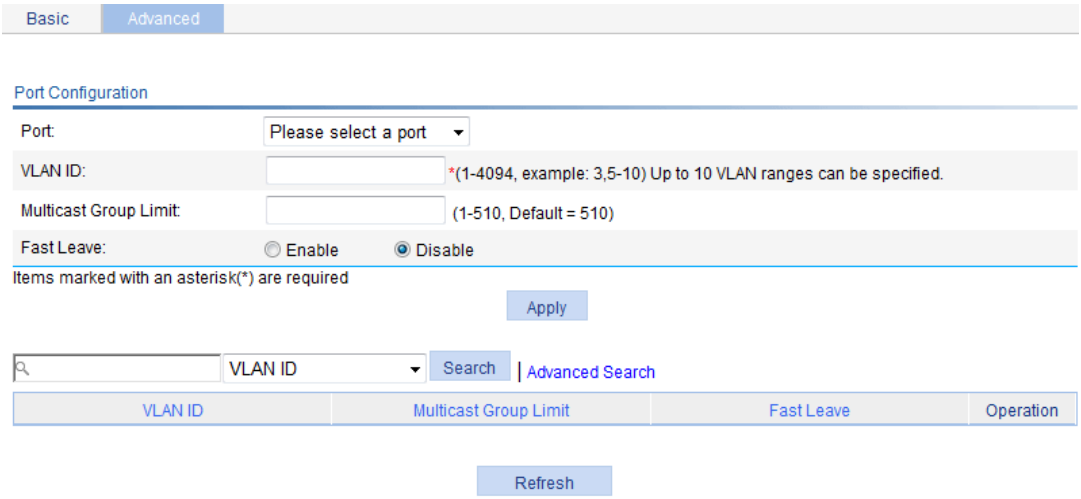
Table 87 Configuration items

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	The default setting is MLDv1. 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 it 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.
Querier	Enable or disable the MLD snooping querier function. In an IPv6 multicast network that runs MLD, a Layer 3 device acts as the MLD querier to send MLD queries and establish and maintain IPv6 multicast forwarding entries, ensuring correct IPv6 multicast traffic forwarding at the network layer. On an IPv6 network without Layer 3 multicast devices, MLD querier cannot work 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, providing MLD querier functions.
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 port functions

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click the **Advanced** tab.

Figure 249 Configuring MLD snooping port functions



3. Configure the parameters as described in Table 88.
4. Click **Apply**.

Table 88 Configuration items

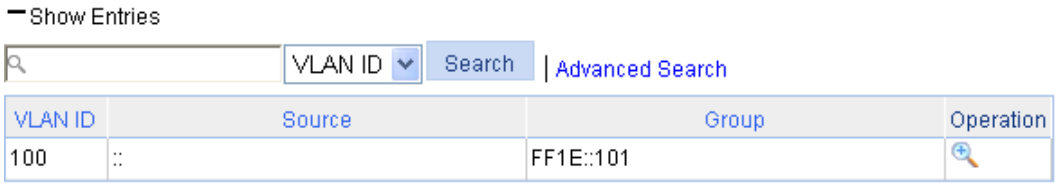
Item	Description
Port	Select the port on which advanced MLD snooping features will be configured. The port can be an GigabitEthernet port or Layer 2 aggregate interface. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. **TIP:** Advanced MLD snooping features configured on a Layer 2 aggregate interface do not interfere with configurations on its member ports, nor do they take part in aggregation calculations. The configuration on a member port of the aggregate group does not take effect until the port leaves the aggregate group
VLAN ID	Specify the ID of the VLAN in which port functions are to be configured. The configurations made in a VLAN take effect on the ports only in this VLAN.
Multicast Group Limit	Configure the maximum number of IPv6 multicast groups on a port. With this feature, you can regulate IPv6 multicast traffic on the port. **IMPORTANT:** When the number of IPv6 multicast groups on a port exceeds the limit that you are setting, the system deletes all the IPv6 forwarding entries related to that port from the MLD snooping forwarding table. The receiver hosts to that port can join the IPv6 multicast groups again before the number of IPv6 multicast groups on this port reaches the limit.

Item	Description
Fast Leave	Enable or disable fast-leave processing on the port. When a port that is enabled with the MLD snooping fast-leave processing feature receives an MLD done message, the switch immediately deletes that port from the IPv6 forwarding table entry for the multicast group specified in the message. When the switch receives MLD multicast-address-specific queries for that multicast group, it does not forward them to that port. You can enable MLD snooping fast-leave processing on ports to save bandwidth and resources.

Displaying MLD snooping multicast forwarding entries

1. Select **Network** > **MLD snooping** from the navigation tree.
2. Click **Show Entries** to display information about MLD snooping multicast forwarding entries.

Table 89 Displaying entry information



3. To view detailed information about an entry, click the icon for the entry.

Figure 250 Detailed information about an MLD snooping multicast entry

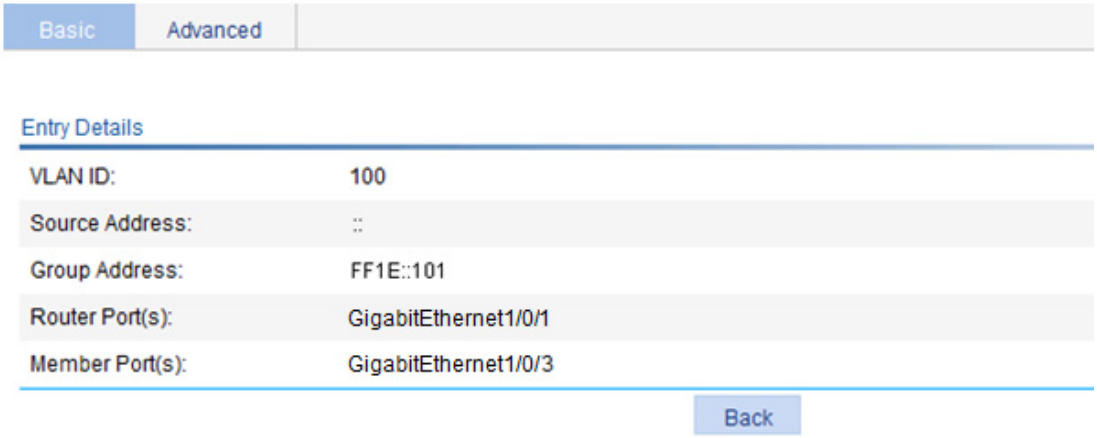


Table 90 Field description

Field	Description
VLAN ID	ID of the VLAN to which the entry belongs.
Source Address	Multicast source address. If no IPv6 multicast sources are specified, this field displays **::**.
Group Address	Multicast group address.
Router Ports	All router ports.
Member Ports	All member ports.

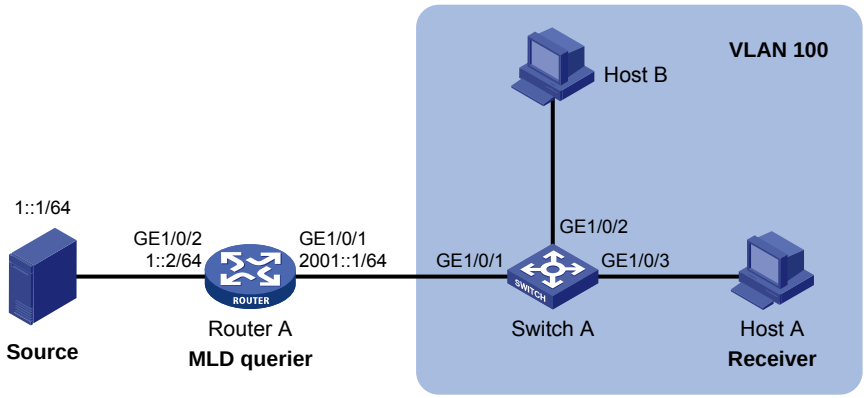
MLD snooping configuration example

Network requirements

As shown in Figure 251, 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**.

Figure 251 Network diagram



Configuration procedure

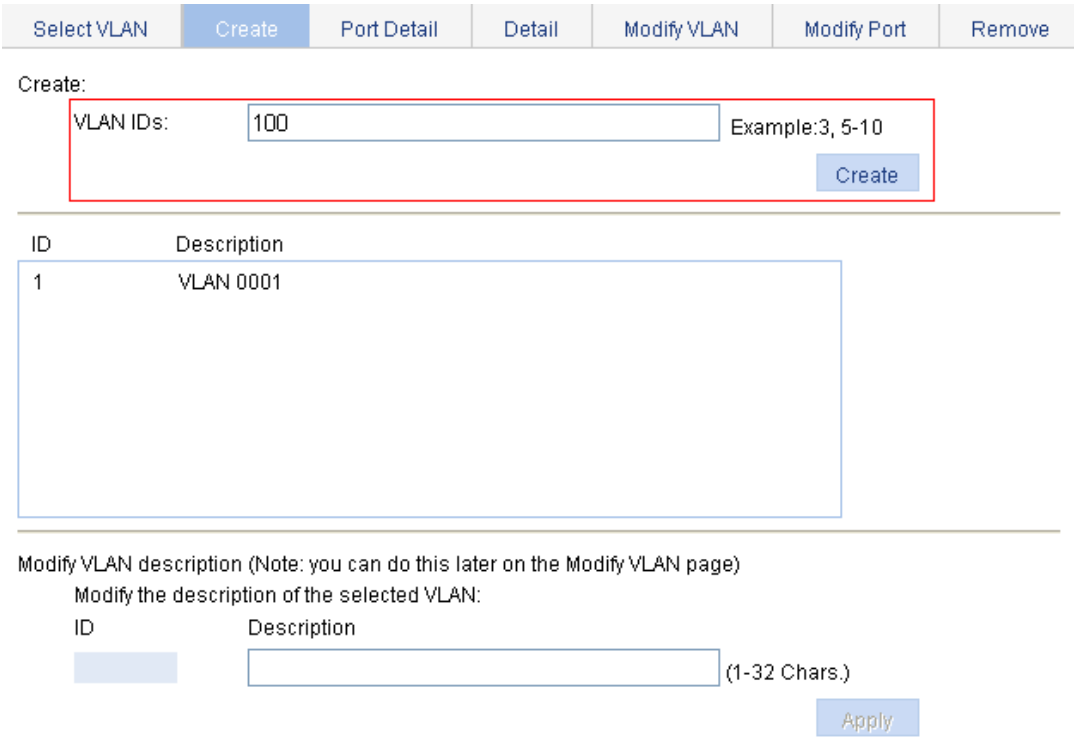
Configuring Router A

Enable IPv6 multicast routing, assign an IPv6 address to each interface, enable IPv6 PIM-DM on each interface, and enable MLD on GigabitEthernet 1/0/1. (Details not shown.)

Configuring Switch A

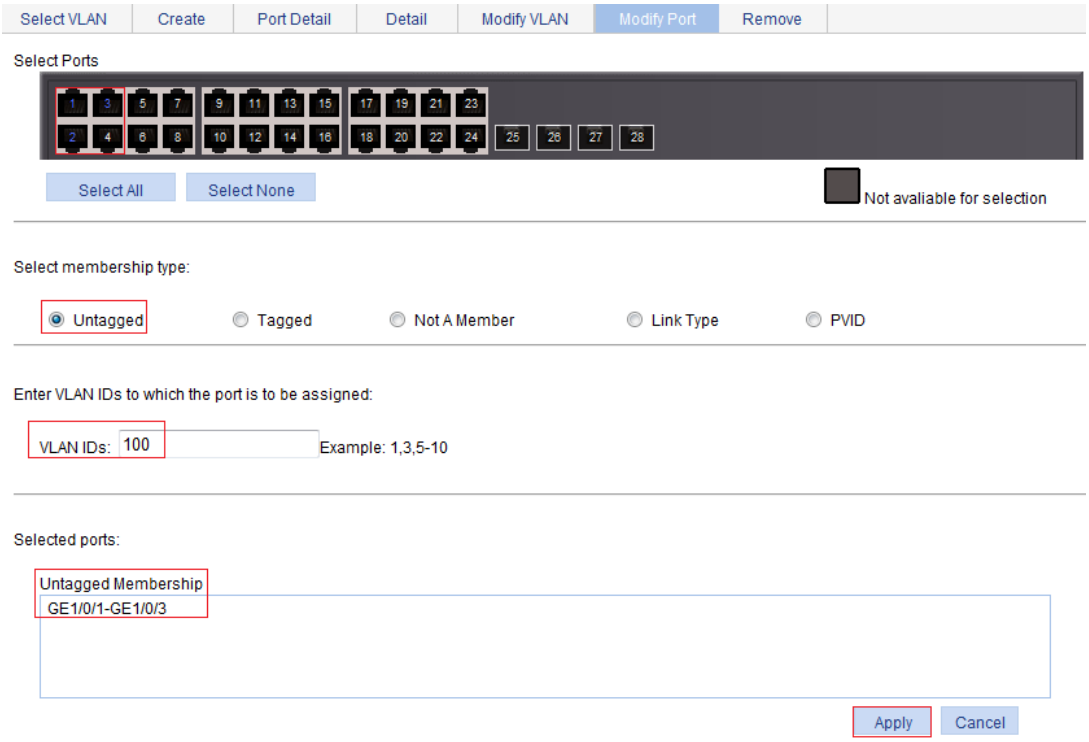
1. Create VLAN 100:
   a. Select **Network** > **VLAN** from the navigation tree.
   b. Click the **Create** tab.
   c. Enter **100** as the VLAN ID.
   d. Click **Apply**.

Figure 252 Creating VLAN 100



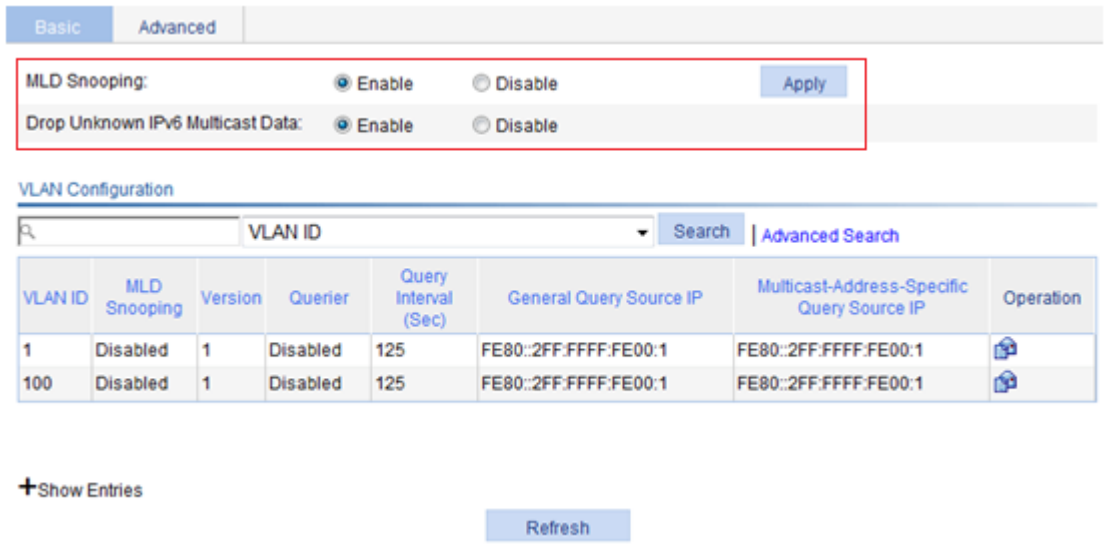
2. Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100:
   a. Click the **Modify Port** tab.
   b. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** area.
   c. Select **Untagged** for **Select membership type**.
   d. Enter **100** as the VLAN ID.
   e. Click **Apply**.

Figure 253 Assigning ports to VLAN 100



3. Enable MLD snooping and dropping unknown IPv6 multicast data globally:
   a. Select **Network** > **MLD snooping** from the navigation tree.
   b. Select **Enable**.
   c. Click **Apply**.

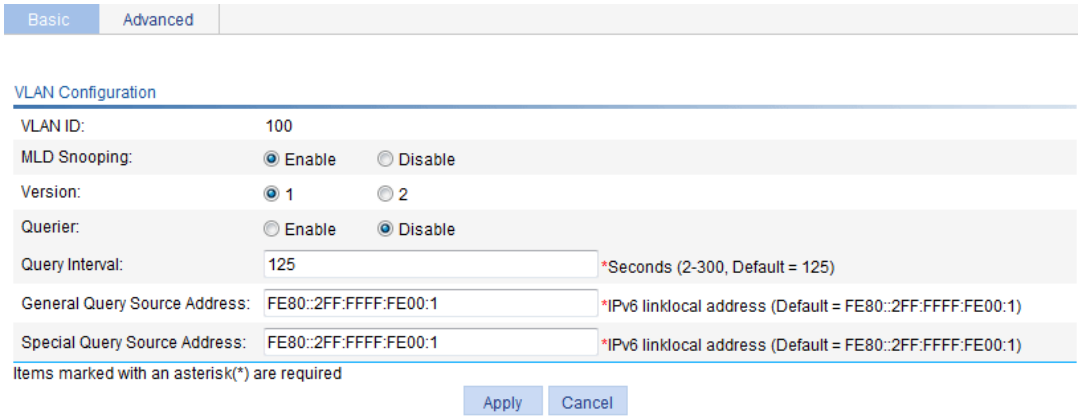
Figure 254 Enabling MLD snooping and dropping unknown IPv6 multicast data globally



4. Enable MLD snooping:
   a. Click the icon for VLAN 100.
   b. Select **Enable** for **MLD snooping**.
   c. Select **1** for **Version**.

d. Click **Apply**.

Figure 255 Enabling MLD snooping in VLAN 100



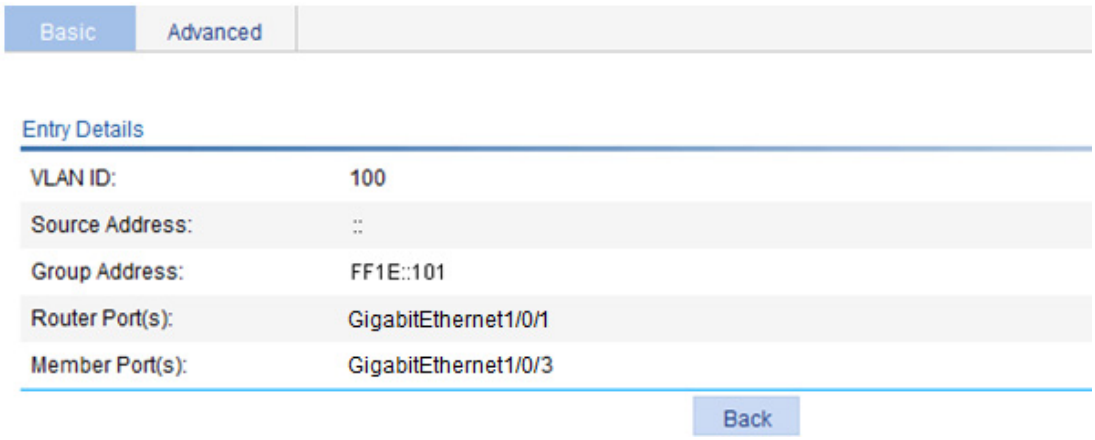
Verifying the configuration

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 forwarding entries.

   Figure 256 Displaying MLD snooping multicast forwarding entries

3. Click the icon for the multicast entry (::, FF1E::101) to display detailed information about this entry.

   Figure 257 Displaying detailed information about the entry



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

The term "router" in this chapter 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 includes 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 might 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 correctly.

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 do not match any specific routing entry in the routing table.

Without a default route, packets that do not match any routing entries are discarded.

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 258 IPv4 active route table

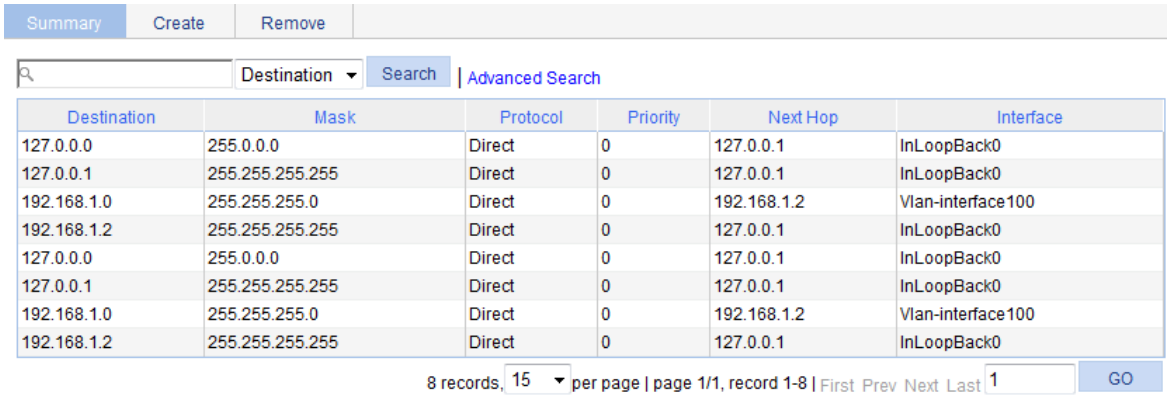


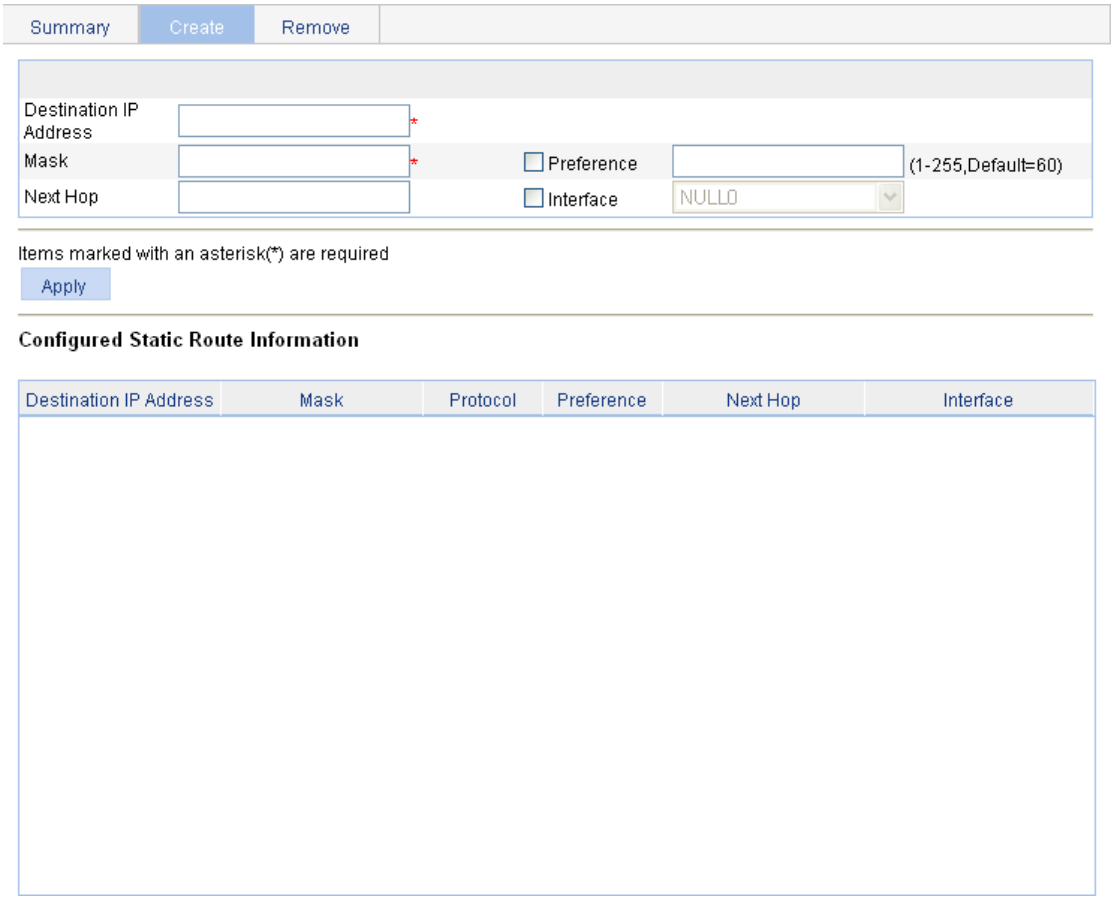
Table 91 Field description

Field	Description
Destination IP Address	Destination IP address and subnet mask of the IPv4 route.
Mask	
Protocol	Protocol that discovered the IPv4 route.
Preference	Preference value for the IPv4 route. The smaller the number, the higher the preference.
Next Hop	Next hop IP address of the IPv4 route.
Interface	Output interface of the IPv4 route. Packets destined for the specified network segment are 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 an IPv4 static route appears.

Figure 259 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.
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. Specifying different preferences enables route backup.
Next Hop	Enter the next hop IP address in dotted decimal notation.
Interface	Select the output 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 260 IPv6 active route table

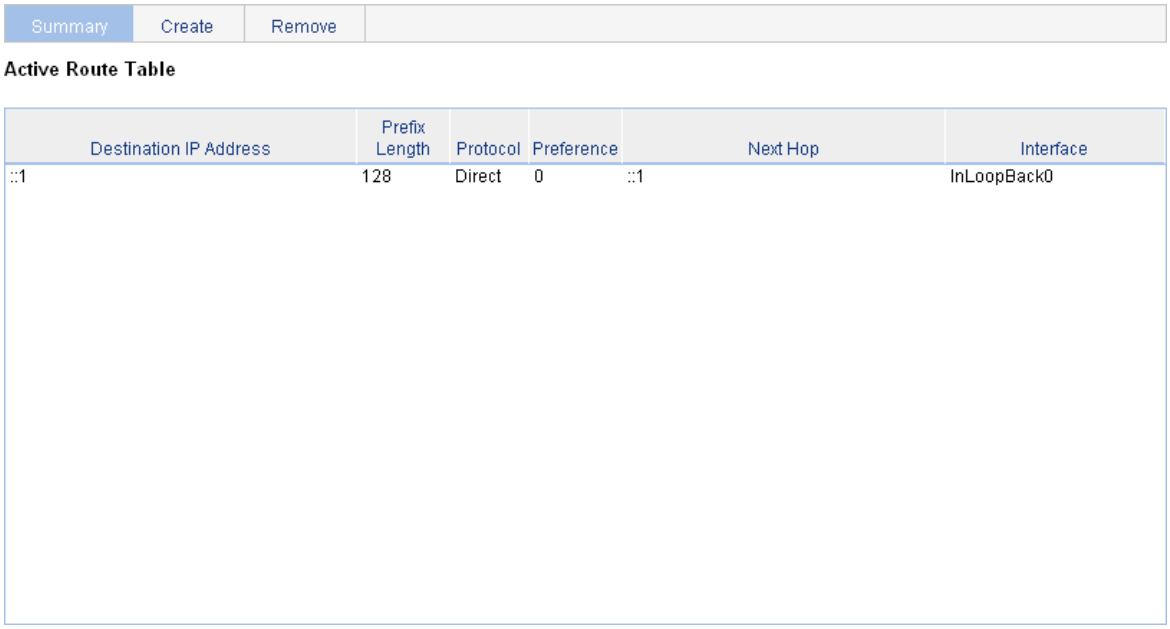


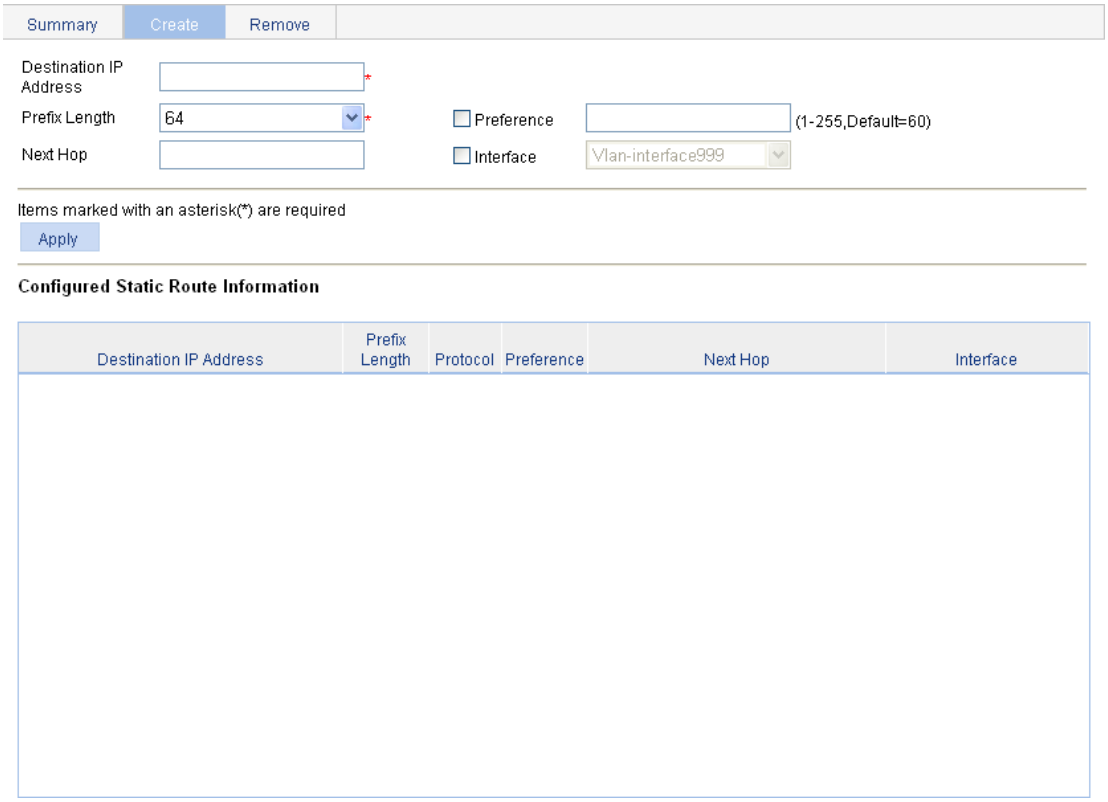
Table 93 Field description

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.
Next Hop	Next hop IP address of the IPv6 route.
Interface	Output interface of the IPv6 route. Packets destined for the specified network segment are 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 an IPv6 static route appears.

Figure 261 Creating an IPv6 static route



3. Create an IPv6 static route as described in Table 94.
4. Click **Apply**.

Table 94 Configuration items

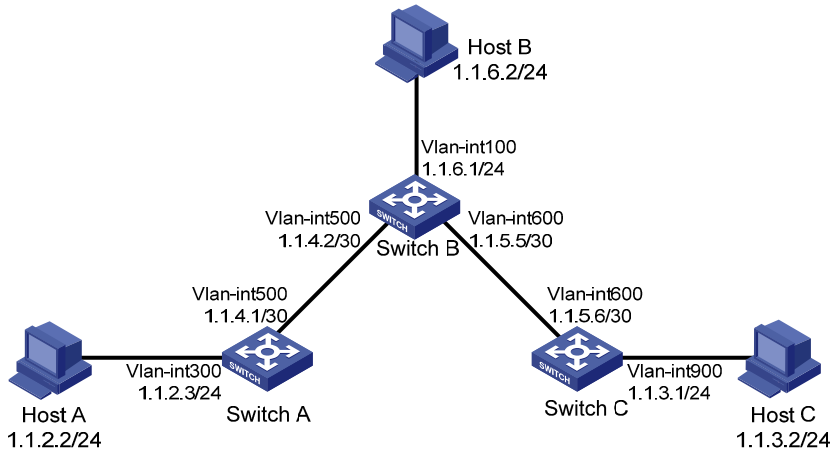
Item	Description
Destination IP Address	Enter the destination host or network IP address, in the X:X::X:X format. The 128-bit destination IPv6 address is a hexadecimal address with eight parts separated by colons (:). Each part is represented by a 4-digit hexadecimal integer.
Prefix Length	Enter or select the prefix length of the destination IPv6 address.
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. 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 output 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

As shown in Figure 262, configure IPv4 static routes on Switch A, Switch B, and Switch C for any two hosts to communicate with each other.

Figure 262 Network diagram



Configuration considerations

On Switch A, configure a default route with Switch B as the next hop.

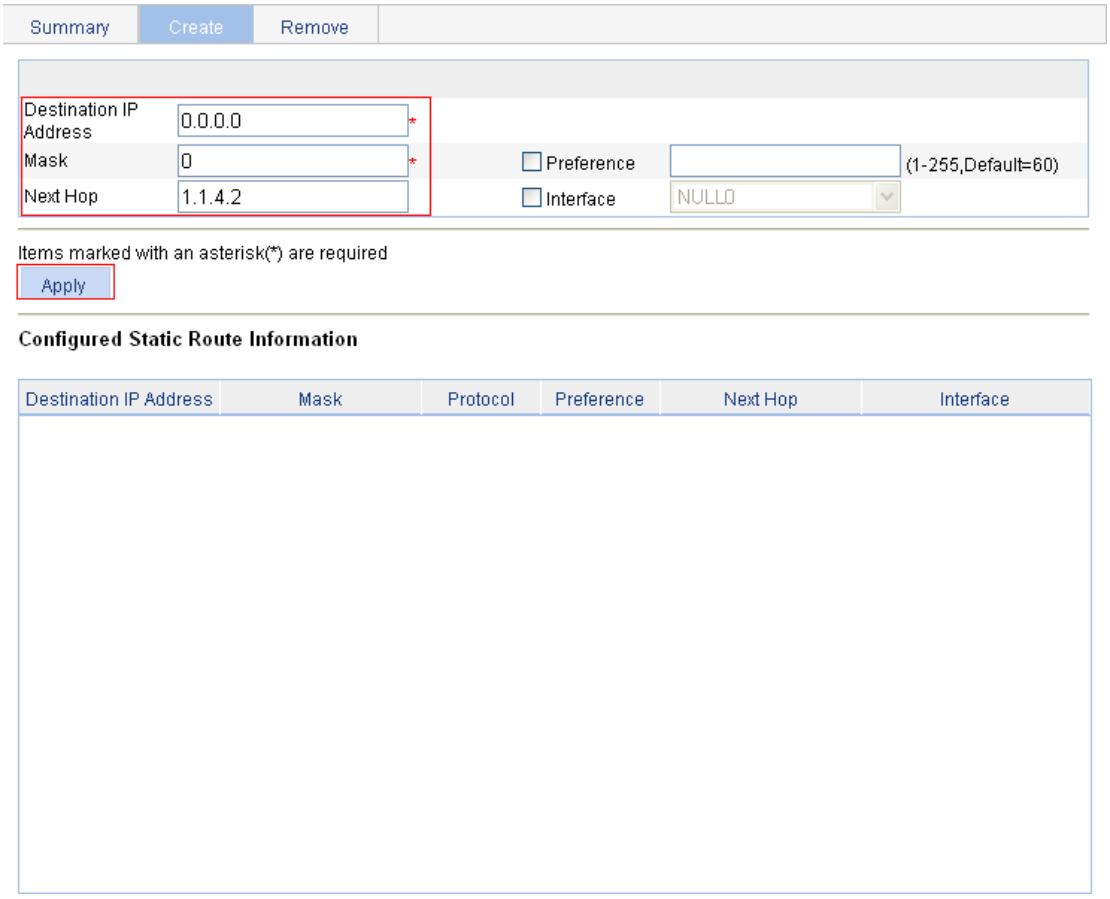
On Switch B, configure one static route with Switch A as the next hop and the other with Switch C as the next hop.

On Switch C, configure a default route with Switch B as the next hop.

Configuration procedure

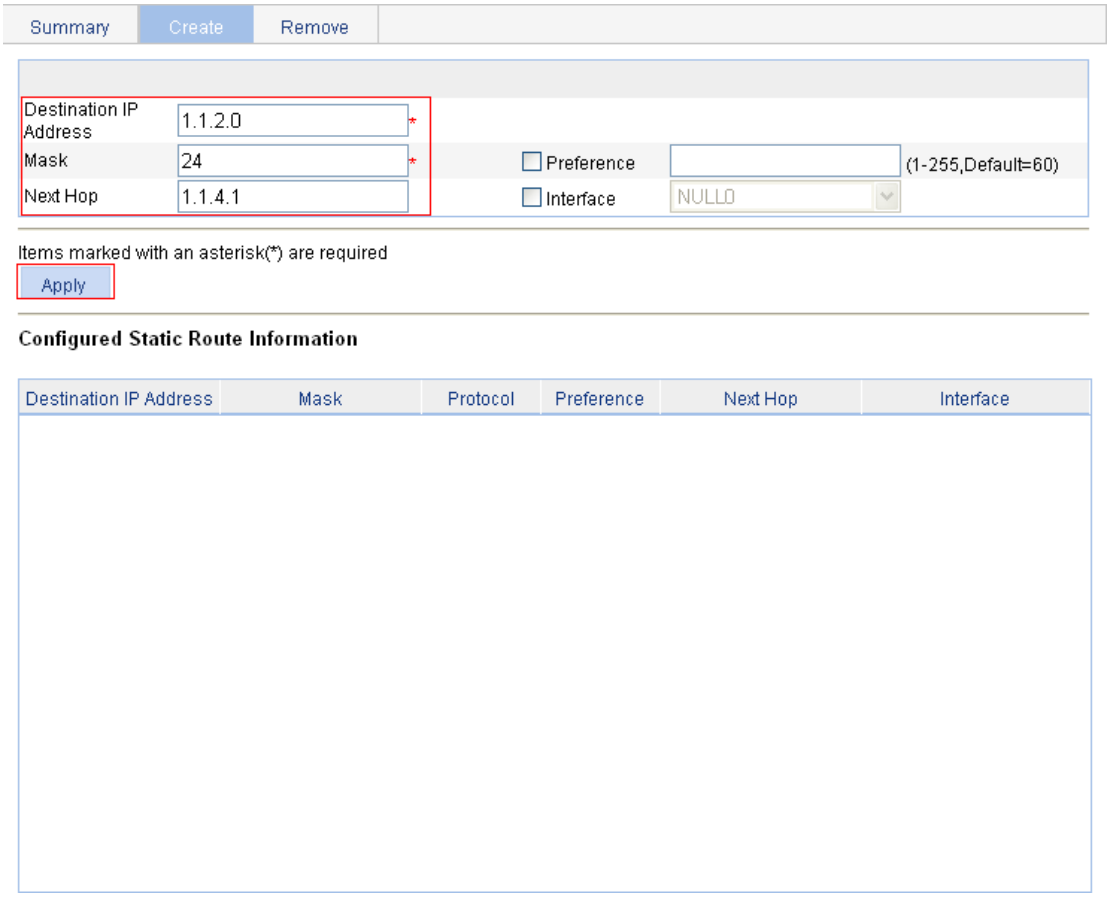
1. Configure a default route to Switch B on Switch A:
   a. Select **Network** > **IPv4 Routing** from the navigation tree of Switch A.
   b. Click the **Create** tab.
   c. Enter **0.0.0.0** for **Destination IP Address**, **0** for **Mask**, and **1.1.4.2** for **Next Hop**.
   d. Click **Apply**.

Figure 263 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 264 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:

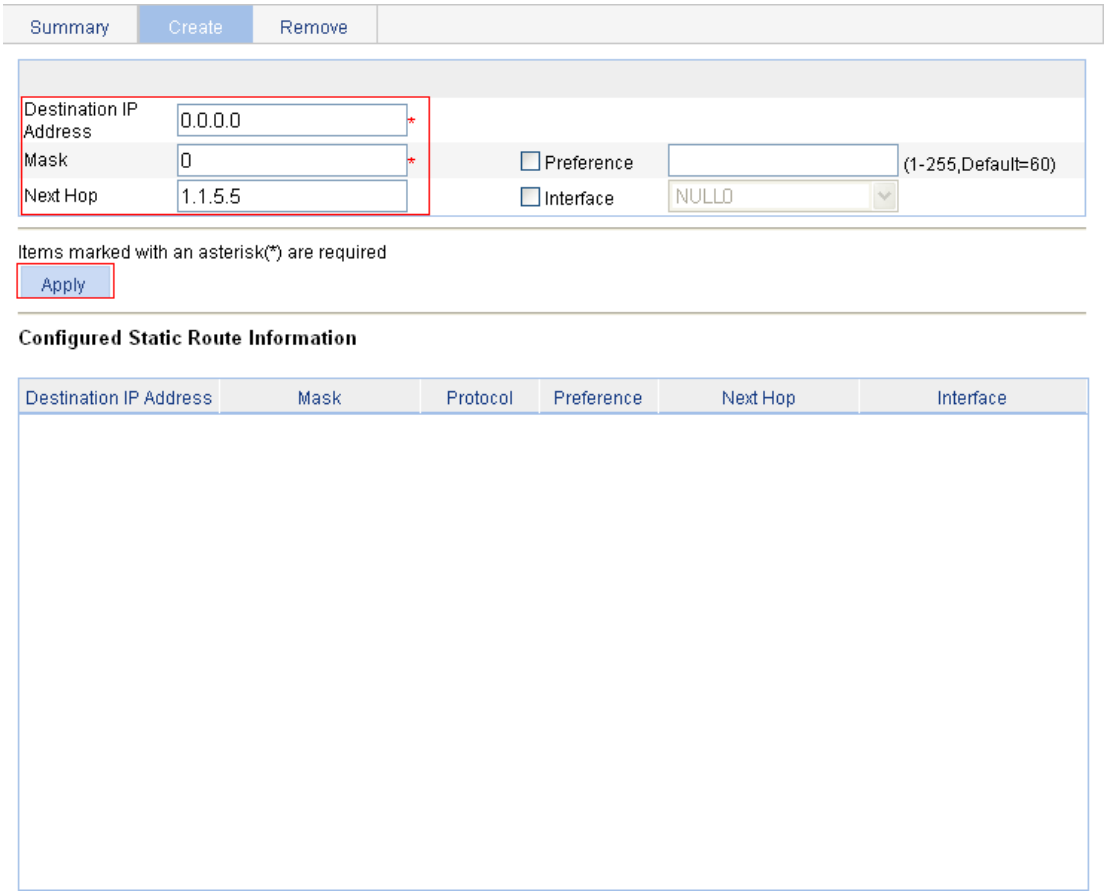
a. Select **Network** > **IPv4 Routing** from the navigation tree of Switch C.

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 265 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 pages.

2. Ping Host C from Host A (assuming both hosts run Windows XP):

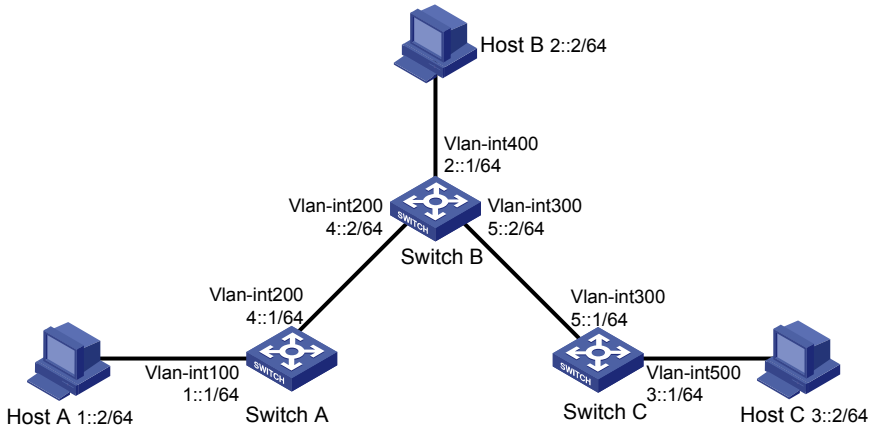
```
C:\Documents and Settings\Administrator>ping 1.1.3.2

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

As shown in Figure 266, configure IPv6 static routes on Switch A, Switch B, and Switch C for any two hosts to communicate with each other.

Figure 266 Network diagram



Configuration considerations

On Switch A, configure a default route with Switch B as the next hop.

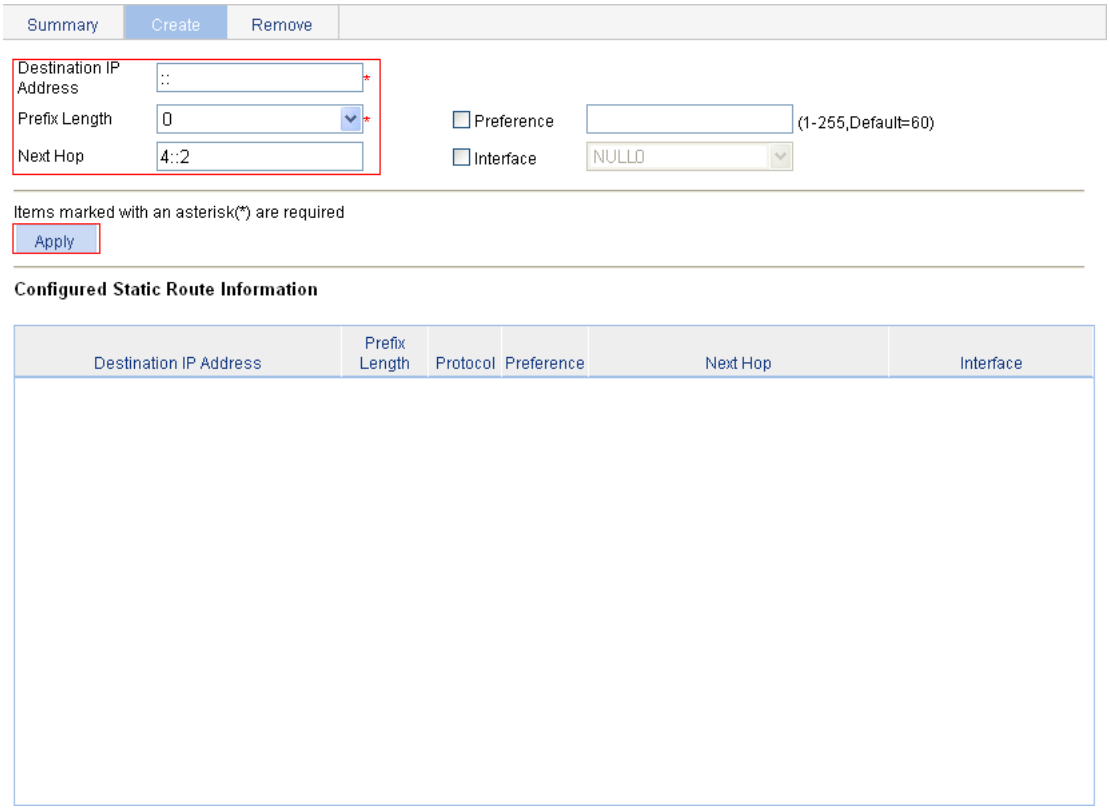
On Switch B, configure one static route with Switch A as the next hop and the other with Switch C as the next hop.

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**.

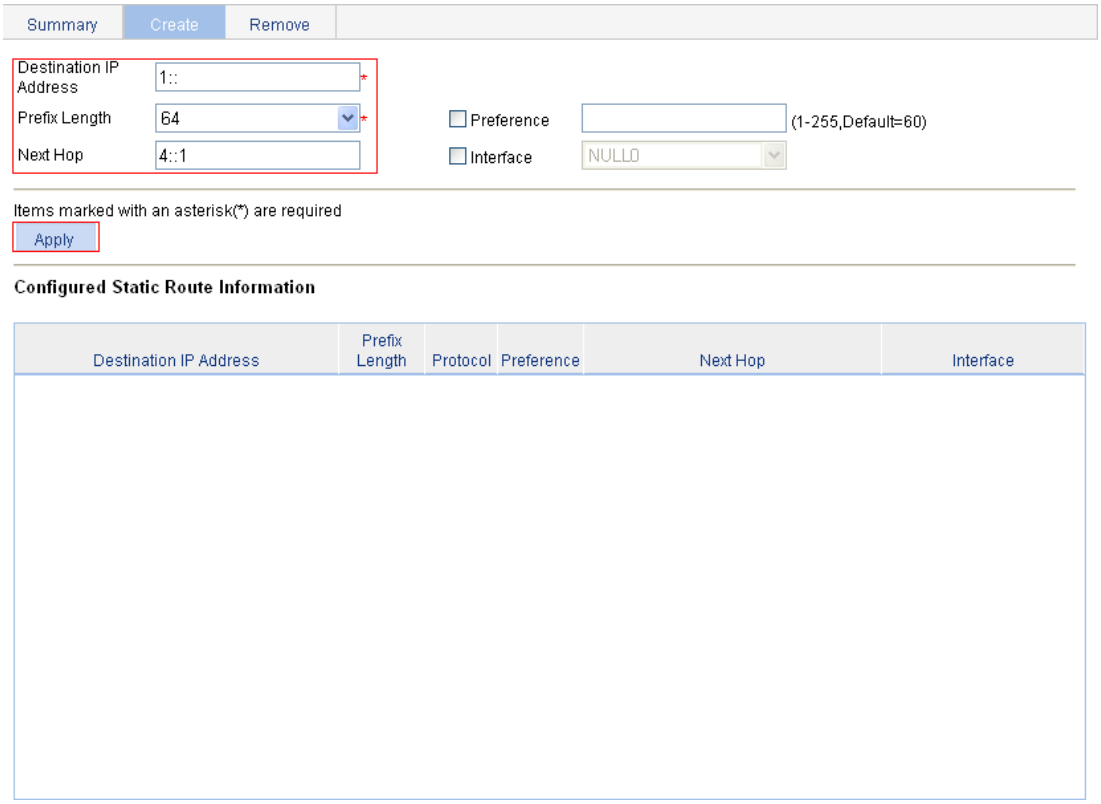
Figure 267 Configuring a default route



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 268 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:

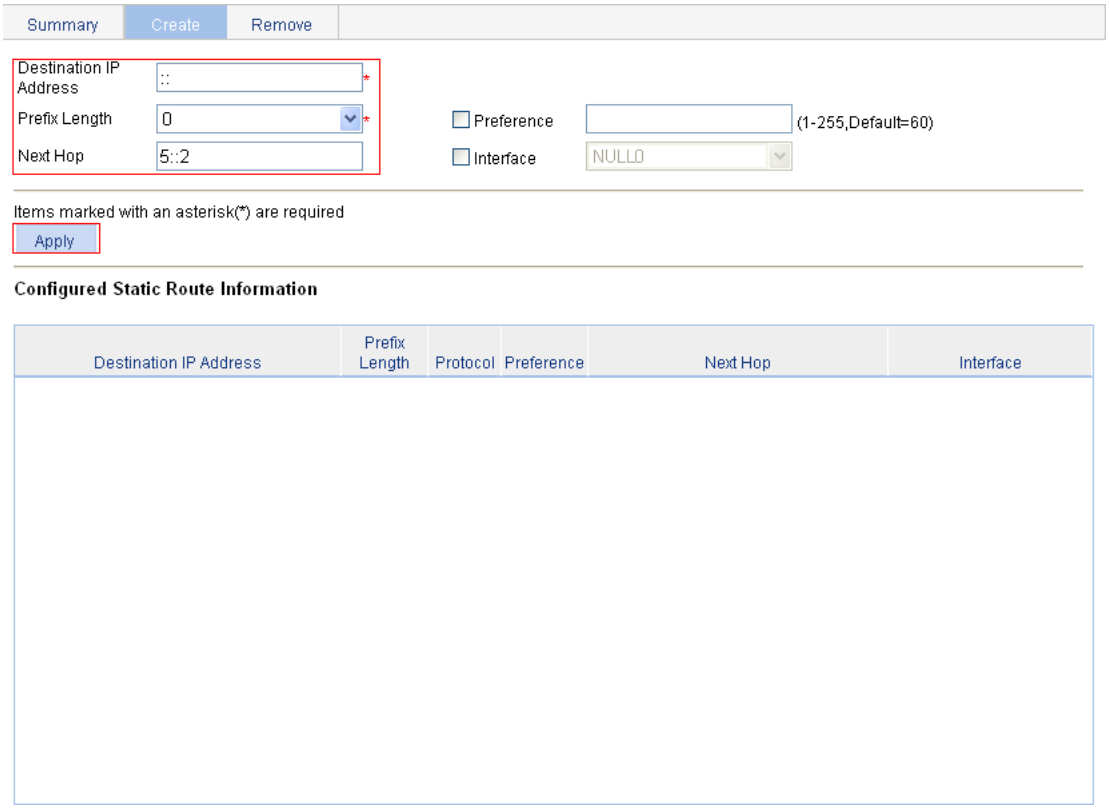
a. Select **Network** > **IPv6 Routing** from the navigation tree of Switch C.

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 269 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 to verify that the newly configured static routes are displayed as active routes on the pages.

2. Ping Host C from Switch A:

```
<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. 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 output interface, note the following:
- If the output interface is NULL 0 or a loopback interface, no next hop address is required.
- If the output interface is a broadcast interface (such as a VLAN interface), you must specify the output interface and the next hop at the same time.
- You can delete only IPv4/IPv6 static routes on the **Remove** tab.

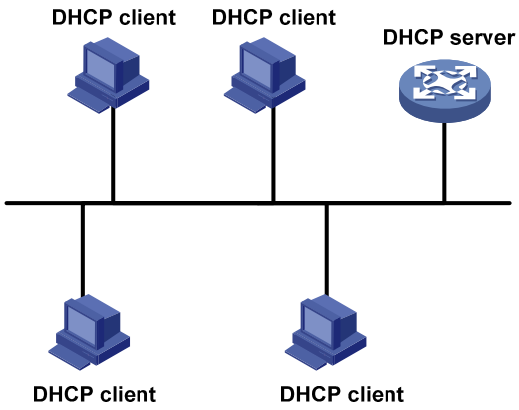
DHCP overview

The Dynamic Host Configuration Protocol (DHCP) provides a framework to assign configuration information to network devices.

DHCP uses the client-server model. Figure 270 shows a typical DHCP application.

A DHCP client can obtain an IP address and other configuration parameters from a DHCP server on another subnet through a DHCP relay agent. For more information about the DHCP relay agent, see "Configuring DHCP relay agent." You can enable the DHCP client on an interface. For more information about the DHCP client configuration, see "Configuring VLAN interface."

Figure 270 A typical DHCP application



DHCP address allocation

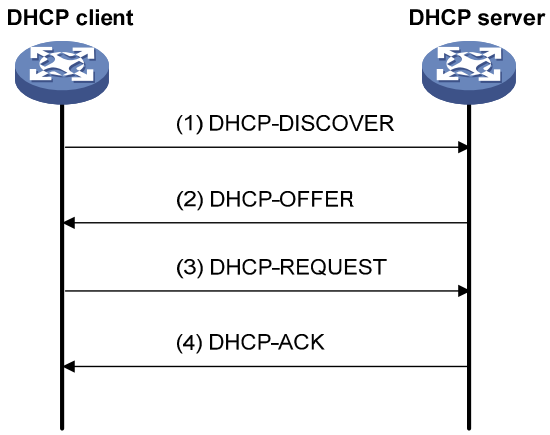
Allocation mechanisms

DHCP supports the following mechanisms for IP address allocation:

- **Static allocation**—The network administrator assigns an IP address to a client (for example, 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.

IP address allocation process

Figure 271 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. (IP addresses offered by other DHCP servers can be assigned to other clients.)
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.
   - 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 address lease extension

A dynamically assigned IP address has a lease. When the lease expires, the IP address is reclaimed by the DHCP server. To continue using the IP address, the client must extend the lease duration.

When half of the lease duration elapses, the DHCP client unicasts a DHCP-REQUEST to the DHCP server to extend the lease. Depending on the availability of the IP address, the DHCP server returns either 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 broadcasts another DHCP-REQUEST message for lease extension when seven eighths of the lease duration elapses. Again, depending on the availability of the IP address, the DHCP server returns either a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

DHCP message format

Figure 272 shows the DHCP message format. DHCP uses some of the fields in significantly different ways. The numbers in parentheses indicate the size of each field in bytes.

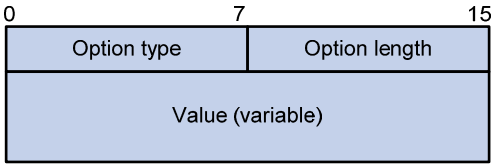
Figure 272 DHCP message format

- **op**—Message type defined in option field. 1 = REQUEST, 2 = REPLY
- **htype**, **hlen**—Hardware address type and length of the 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. 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 if the client has an IP address that is valid and usable. Otherwise, it is set to zero. (The client does not use this field to request a specific IP address to lease.)
- **yiaddr**—"Your" (client) IP address, assigned by the server.
- **siaddr**—Server IP address, from which the client obtained configuration parameters.
- **giaddr**—(Gateway) 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 duration, subnet mask, domain name server IP address, and WINS IP address.

DHCP options

DHCP defines the message format as an extension to BOOTP for compatibility. DHCP uses the Option field to carry information for dynamic address allocation and to provide additional configuration information to clients.

Figure 273 DHCP option format



Common DHCP options

The following are common DHCP options:

- **Option 3**—Router option. It specifies the gateway address.
- **Option 6**—DNS server option. It specifies the DNS server's IP address.
- **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 into 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 includes values that correspond to the parameters requested by the client.
- **Option 60**—Vendor class identifier option. It is used by a DHCP client to identify its vendor, and by a DHCP server to distinguish DHCP clients by vendor class and assign specific IP addresses to the DHCP clients.
- **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.

Option 82

Some options, such as Option 82, have no unified definitions in RFC 2132.

Option 82 is the relay agent option. It records the location information about 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 and sends it to the server.

The administrator can use Option 82 to locate the DHCP client and further implement security control and accounting. The DHCP server can use Option 82 to provide individual configuration policies for the clients.

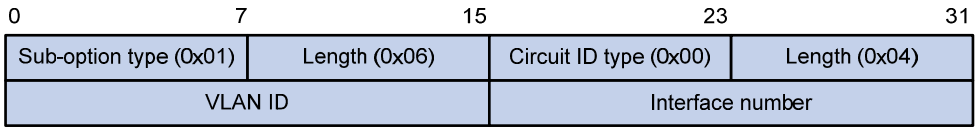
Option 82 can include up to 255 sub-options and must have one sub-option at least. Option 82 supports two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

Option 82 has no unified definition. Its padding formats vary with vendors.

By default, the normal padding format is used on the device. You can specify the code type for the sub-options as ASCII or HEX. The padding contents for sub-options in the normal padding format are as follows:

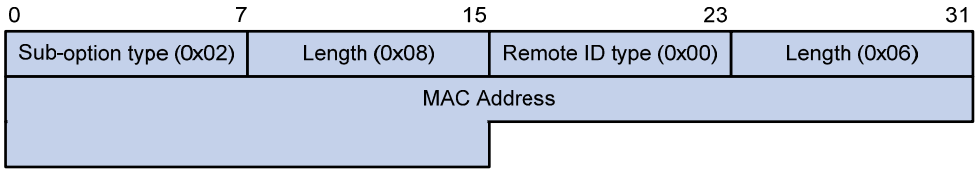
- **Sub-option 1**—Padded with the VLAN ID and interface number of the interface that received the client's request. The following figure gives its format. The value of the sub-option type is 1, and that of the circuit ID type is 0.

  Figure 274 Sub-option 1 in normal padding format



- **Sub-option 2**—Padded with the MAC address of the DHCP relay agent interface or the MAC address of the DHCP snooping device that received the client's request. The following figure gives its format. The value of the sub-option type is 2, and that of the remote ID type is 0.

  Figure 275 Sub-option 2 in normal padding format



Protocols and standards

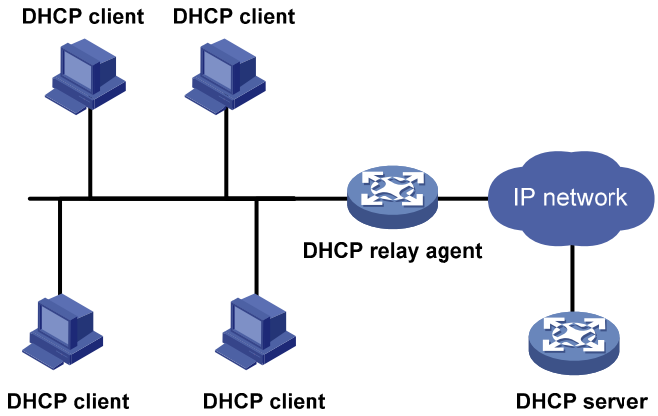
- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3442, *The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4.*

Configuring DHCP relay agent

Overview

Since the DHCP clients request IP addresses through broadcast messages, the DHCP server and clients must be on the same subnet. Through a DHCP relay agent, DHCP clients can get IP addresses from a DHCP server on another subnet. This feature avoids deploying a DHCP server for each subnet to centralize management and reduce investment. Figure 276 shows a typical application of the DHCP relay agent.

Figure 276 DHCP relay agent application

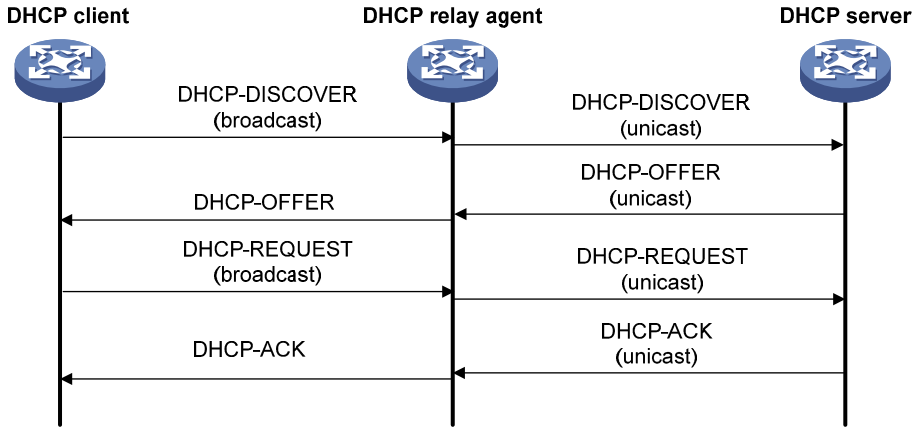


The DHCP server and client interact with each other in the same way regardless of whether the relay agent exists (see "DHCP overview"). For more information about DHCP packet exchange, see "IP address allocation process."

The following only describes steps related to the DHCP relay agent:

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 in a response.
3. The relay agent conveys the response to the client.

Figure 277 DHCP relay agent operation



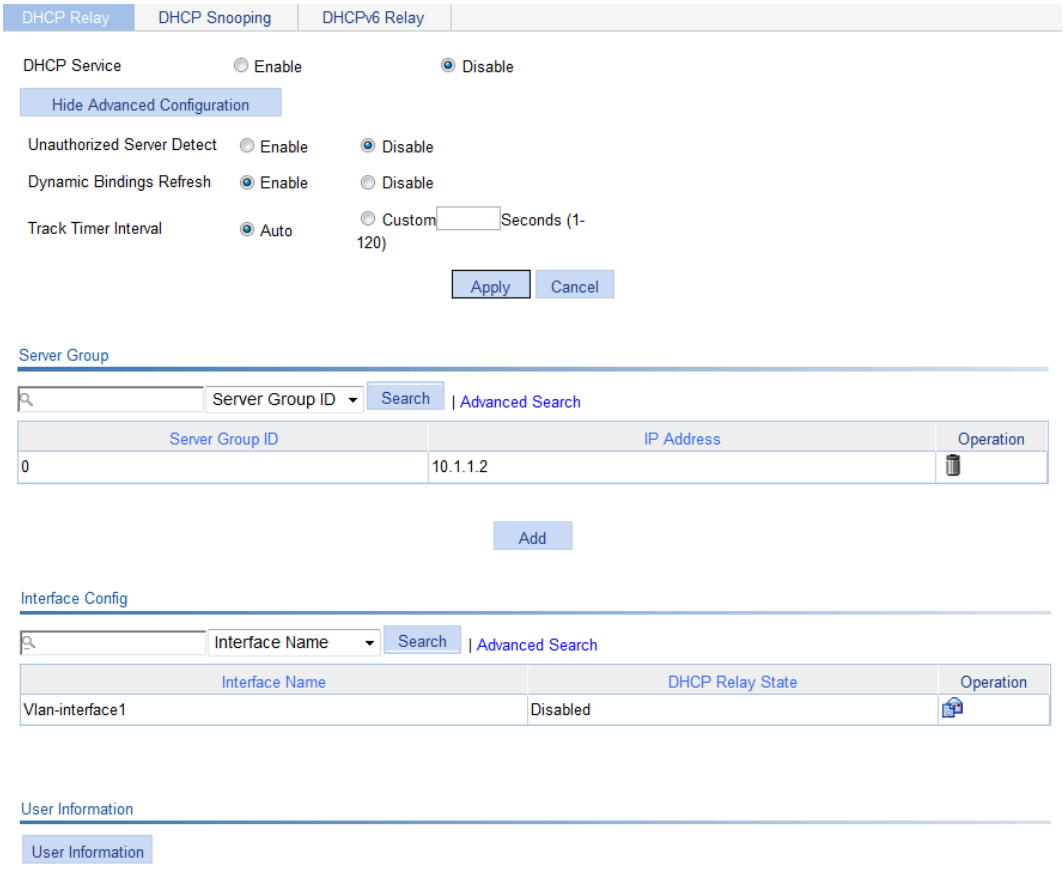
Recommended configuration procedure

Task	Remarks
Enabling DHCP and configuring advanced parameters for the DHCP relay agent	Required. Enable DHCP globally and configure advanced DHCP parameters. By default, global DHCP is disabled.
Creating a DHCP server group	Required. To improve reliability, you can specify several DHCP servers as a group on the DHCP relay agent and correlate a relay agent interface with the server group. When the interface receives requesting messages from clients, the relay agent forwards them to all the DHCP servers of the group.
Enabling the DHCP relay agent on an interface	Required. Enable the DHCP relay agent on an interface, and correlate the interface with a DHCP server group. **IMPORTANT:** The DHCP relay agent works on interfaces with IP addresses manually configured only.
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. From the navigation tree, select **Network** > **DHCP** to enter the default **DHCP Relay** page.
2. Click **Display Advanced Configuration** to expand the advanced DHCP relay agent configuration area, as shown in Figure 278.

Figure 278 DHCP relay agent configuration page



3. Enable DHCP service and configure advanced parameters for DHCP relay agent as shown in Table 95.
4. Click **Apply**.

Table 95 Configuration items

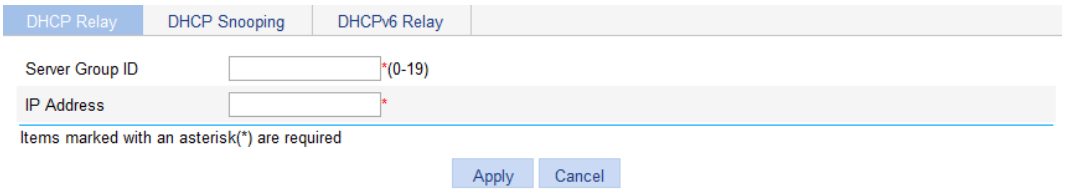
Item	Description
DHCP Service	Enable or disable global DHCP.
Unauthorized Server Detect	Enable or disable unauthorized DHCP server detection. There are unauthorized DHCP servers on networks, which reply DHCP clients with wrong IP addresses. With this feature enabled, upon receiving a DHCP request, the DHCP relay agent records 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 re-records server information following this mechanism.

Item	Description
Dynamic Bindings Refresh	Enable or disable periodic refresh of dynamic client entries, and set the refresh interval. A DHCP client sends a DHCP-RELEASE unicast message to the DHCP server through the DHCP relay agent to relinquish its IP address. In this case the DHCP relay agent simply conveys the message to the DHCP server, thus it does not remove the IP address from dynamic client entries. To solve this problem, the periodic refresh of dynamic client entries feature is introduced. With this feature, the DHCP relay agent uses the IP address of a client and the MAC address of the DHCP relay agent interface to periodically send a DHCP-REQUEST message to the DHCP server. • If the server returns a DHCP-ACK message or does not return any message within a specific interval, which means that the IP address is assignable now, the DHCP relay agent ages out the client entry. • If the server returns a DHCP-NAK message, which means the IP address is still in use, the relay agent does not age it out. If the **Auto** option is selected, the refresh interval is calculated by the relay agent according to the number of client entries.
Track Timer Interval	

Creating a DHCP server group

1. From the navigation tree, select **Network** > **DHCP** to enter the default **DHCP Relay** page shown in Figure 278.
2. In the **Server Group** area, click **Add** to enter the page shown in Figure 279.

   Figure 279 Create a server group

3. Configure the DHCP server group as shown in Table 96.
4. Click **Apply**.

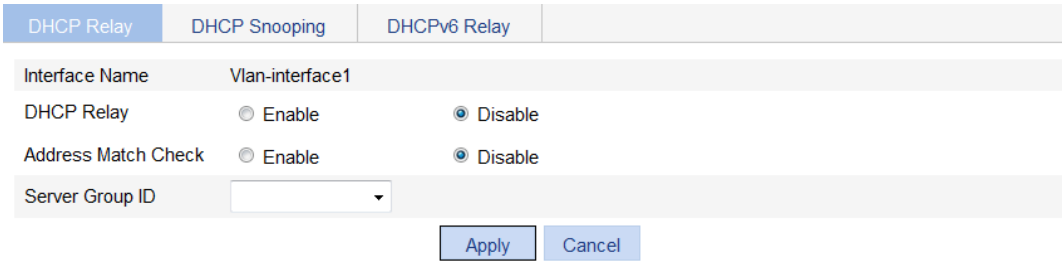
Table 96 Configuration items

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. From the navigation tree, select **Network** > **DHCP** to enter the default **DHCP Relay** page shown in Figure 278.
2. In the **Interface Config** field, click the icon of a specific interface to enter the page shown in Figure 280.

Figure 280 Configuring a DHCP relay agent interface



3. Configure the DHCP relay agent on the interface as shown in Table 97.
4. Click **Apply**.

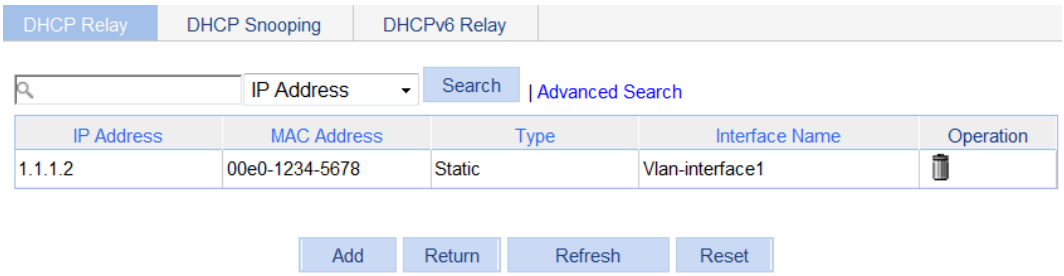
Table 97 Configuration items

Item	Description
Interface Name	This field displays the name of a specific interface.
DHCP Relay	Enable or disable the DHCP relay agent on the interface.
Address Match Check	Enable or disable IP address check. With this function enabled, the DHCP relay agent checks whether a requesting client's IP and MAC addresses match a binding (dynamic or static) on the DHCP relay agent. If not, the client cannot access outside networks through 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

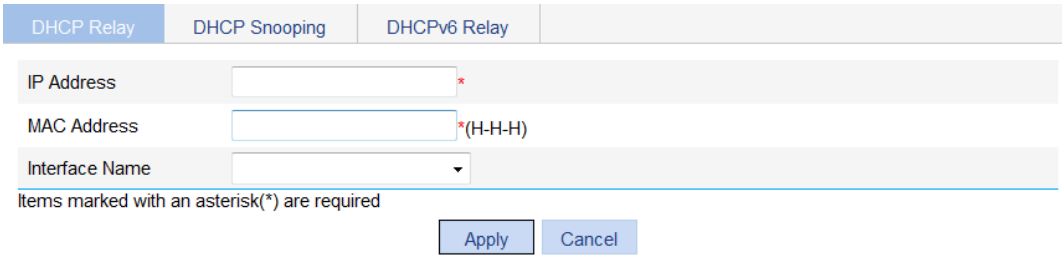
1. From the navigation tree, select **Network** > **DHCP** to enter the default **DHCP Relay** page shown in Figure 278.
2. In the **User Information** area, click **User Information** to view static and dynamic bindings, as shown in Figure 281.

Figure 281 Displaying clients' IP-to-MAC bindings



3. Click **Add** to enter the page as shown in Figure 282.

Figure 282 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 might occur.

DHCP relay agent configuration example

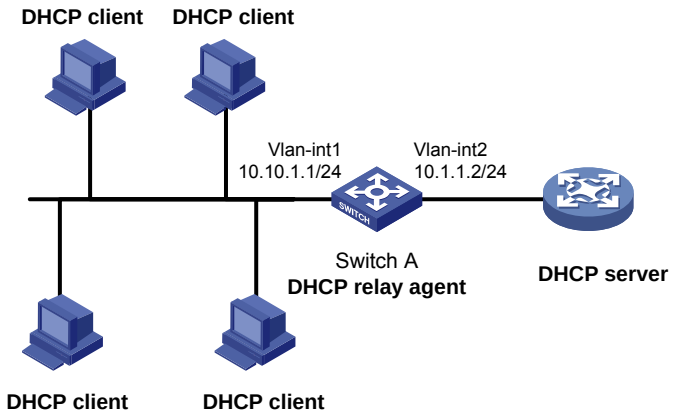
Network requirements

As shown in Figure 283, VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside.

The IP address of VLAN-interface 1 is 10.10.1.1/24 and the IP address of VLAN-interface 2 is 10.1.1.1/24. VLAN-interface 2 is connected to the DHCP server whose IP address is 10.1.1.1/24.

The switch forwards DHCP messages between DHCP clients and the DHCP server.

Figure 283 Network diagram



Configuring Switch A

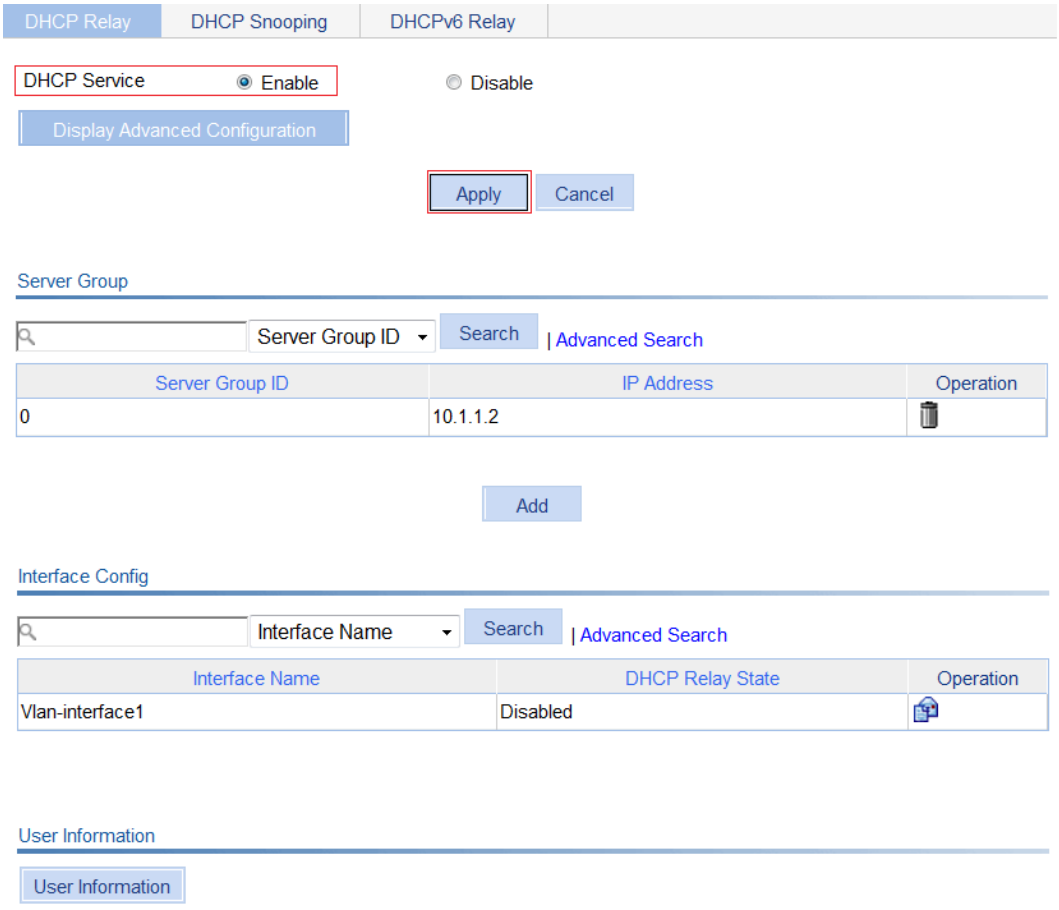
1. Enable DHCP:

a. From the navigation tree, select **Network** > **DHCP** to enter the default **DHCP Relay** page.

b. Select the **Enable** option next to **DHCP Service**, as shown in Figure 225.

c. Click **Apply**.

Figure 284 Enabling DHCP



2. Configure a DHCP server group:

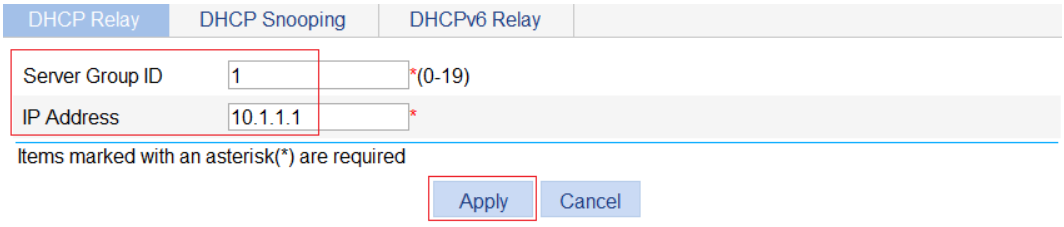
a. In the **Server Group** area, click **Add** and then perform the following operations, as shown in Figure 285.

b. Enter **1** for **Server Group ID**.

c. Enter **10.1.1.1** for **IP Address**.

d. Click **Apply**.

Figure 285 Adding a DHCP server group



3. Enable the DHCP relay agent on VLAN-interface 1:

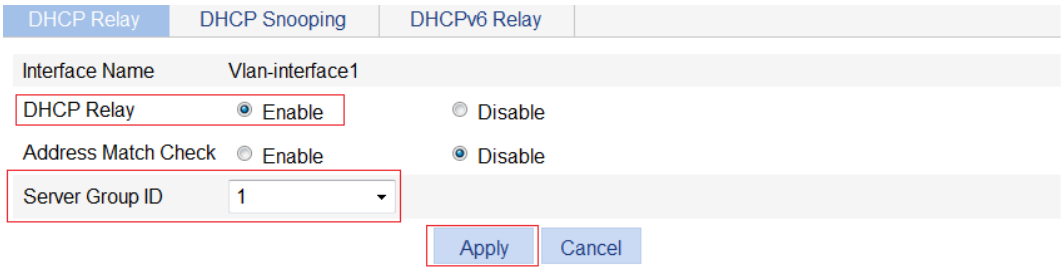
a. In the **Interface Config** field, click the icon of VLAN-interface 1, and then perform the following operations, as shown in Figure 286.

b. Select the **Enable** option next to **DHCP Relay**.

c. Select **1** for **Server Group ID**.

d. Click **Apply**.

Figure 286 Enabling the DHCP relay agent on an interface and correlate it with a server group



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

DHCP snooping works between the DHCP client and server, or between the DHCP client and DHCP relay agent. It guarantees that DHCP clients obtain IP addresses from authorized DHCP servers. Also, it records IP-to-MAC bindings of DHCP clients (called DHCP snooping entries) for security purposes.

DHCP snooping does not work between the DHCP server and DHCP relay agent.

Overview

DHCP snooping defines trusted and untrusted ports to make sure clients obtain IP addresses only from authorized DHCP servers.

- Trusted—A trusted port can forward DHCP messages correctly to make sure the clients get IP addresses from authorized DHCP servers.
- Untrusted—An untrusted port discards received DHCP-ACK and DHCP-OFFER messages to prevent unauthorized servers from assigning IP addresses.

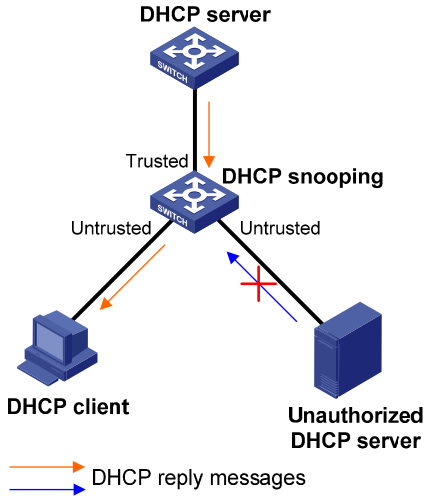
DHCP snooping reads DHCP-ACK messages received from trusted ports and DHCP-REQUEST messages to create DHCP snooping entries. A DHCP snooping entry includes the MAC and IP addresses of a client, the port that connects to the DHCP client, and the VLAN. The DHCP snooping entries can be used by ARP detection to prevent ARP attacks. For more information about ARP detection, see "Configuring ARP attack protection".

Application of trusted ports

Configure ports facing the DHCP server as trusted ports, and configure other ports as untrusted ports.

As shown in Figure 287, configure the DHCP snooping device's port that is connected to the DHCP server as a trusted port. The trusted port forwards response messages from the DHCP server to the client. The untrusted port connected to the unauthorized DHCP server discards incoming DHCP response messages.

Figure 287 Trusted and untrusted ports



In a cascaded network as shown in Figure 288, configure each DHCP snooping device's ports connected to other DHCP snooping devices as trusted ports. To save system resources, you can disable the untrusted ports that are not directly connected to DHCP clients from generating DHCP snooping entries.

Figure 288 Trusted and untrusted ports in a cascaded network

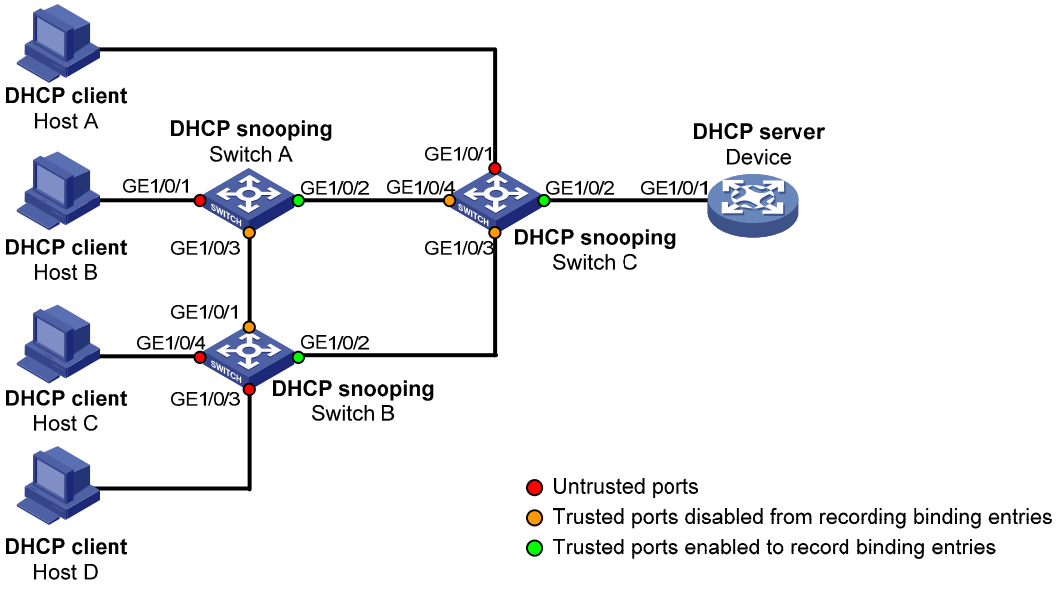


Table 99 describes roles of the ports shown in Figure 288.

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 about the DHCP client so the administrator can locate the DHCP client for security and accounting purposes. For more information, see "Option 82."

DHCP snooping uses the same strategies as the DHCP relay agent to handle Option 82 for DHCP request messages, as shown in Table 100. If a response returned by the DHCP server contains Option 82, DHCP snooping removes Option 82 before forwarding the response to the client. If the response contains no Option 82, DHCP snooping forwards it directly.

Table 100 Handling strategy

If a DHCP request has…	Handling strategy	The DHCP snooping device…
Option 82	Drop	Drops the message.
	Keep	Forwards the message without changing Option 82.
	Replace	Forwards the message after replacing the original Option 82 with the Option 82 padded in normal format.
No Option 82	N/A	Forwards the message after adding the Option 82 padded in normal format.

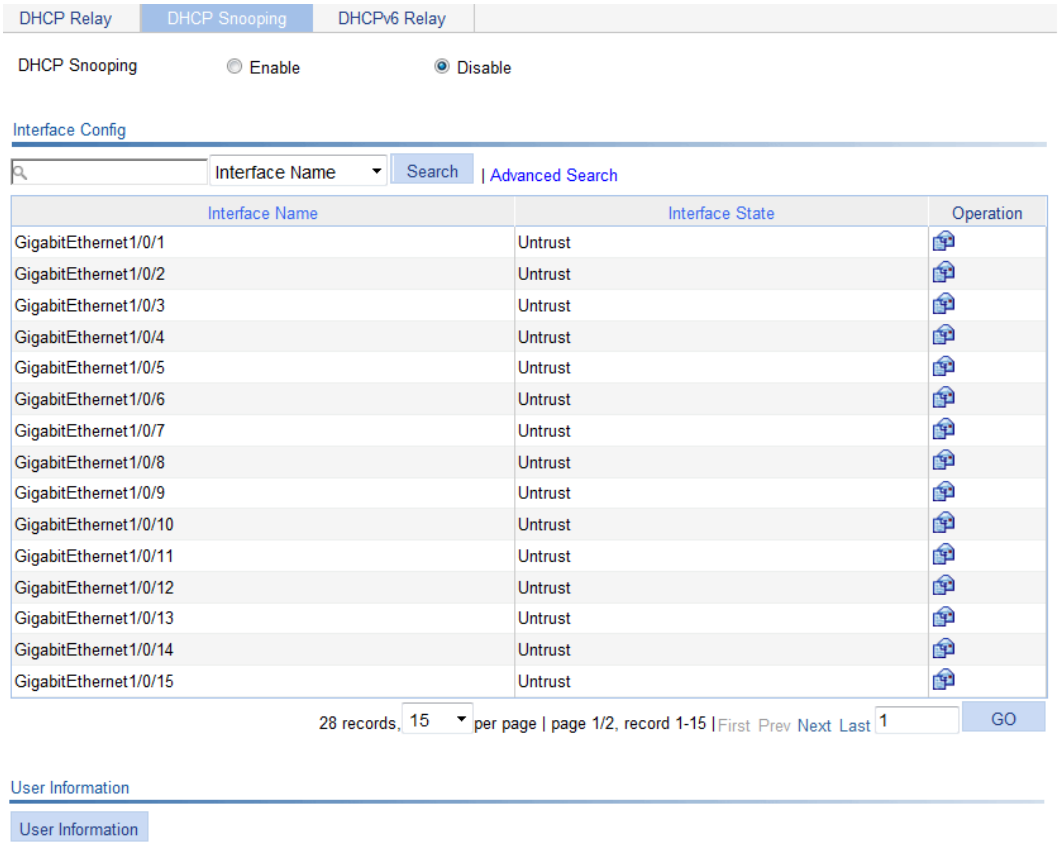
Recommended configuration procedure

Task	Remarks
Enabling DHCP snooping	Required. By default, DHCP snooping is disabled.
Configuring DHCP snooping functions on an interface	Required. Specify an interface as trusted and configure DHCP snooping to support Option 82. By default, an interface is untrusted and DHCP snooping does not support Option 82. **IMPORTANT:** You need to specify the ports connected to the authorized DHCP servers as trusted to make sure DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.
Displaying clients' IP-to-MAC bindings	Optional. Display clients' IP-to-MAC bindings recorded by DHCP snooping.

Enabling DHCP snooping

1. From the navigation tree, select **Network** > **DHCP**.
2. Click the **DHCP Snooping** tab to enter the page shown in Figure 289.
3. Select the **Enable** option next to **DHCP Snooping** to enable DHCP Snooping.

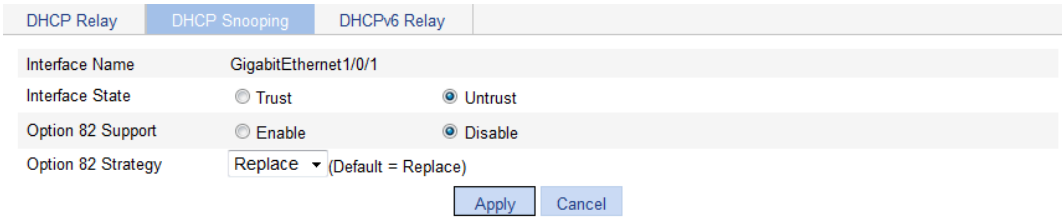
Figure 289 DHCP snooping configuration page



Configuring DHCP snooping functions on an interface

1. From the navigation tree, select **Network** > **DHCP**.
2. Click the **DHCP Snooping** tab to enter the page shown in Figure 289.
3. Click the icon of a specific interface in the **Interface Config** area to enter the page shown in Figure 290.

   Figure 290 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	This field displays the name of a specific interface.
Interface State	Configure the interface as trusted or untrusted.
Option 82 Support	Configure DHCP snooping to support Option 82 or not.
Option 82 Strategy	Select the handling strategy for DHCP requests containing Option 82. The strategies include: • **Drop**—The message is discarded if it contains Option 82. • **Keep**—The message is forwarded without its Option 82 being changed. • **Replace**—The message is forwarded after its original Option 82 is replaced with the Option 82 padded in normal format.

Displaying clients' IP-to-MAC bindings

1. From the navigation tree, select **Network** > **DHCP**.
2. Click the **DHCP Snooping** tab to enter the page shown in Figure 289.
3. Click **User Information** to enter the page as shown in Figure 291.

Figure 291 DHCP snooping user information

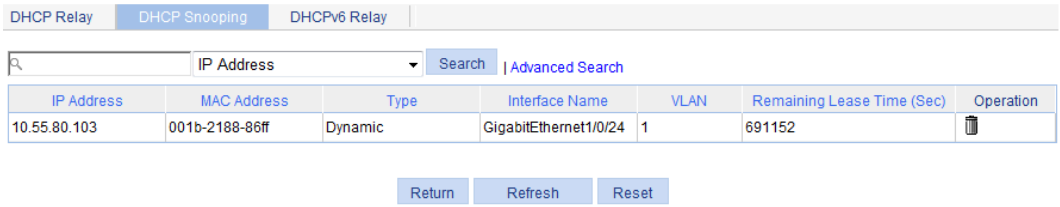


Table 102 describes the fields of DHCP snooping entries.

Table 102 Field description

Item	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: • **Dynamic**—The IP-to-MAC binding is generated dynamically. • **Static**—The IP-to-MAC binding is configured manually. 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.

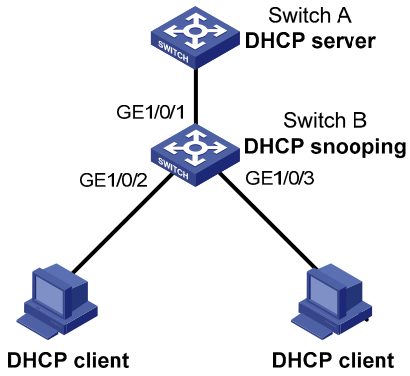
DHCP snooping configuration example

Network requirements

As shown in Figure 292, 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.

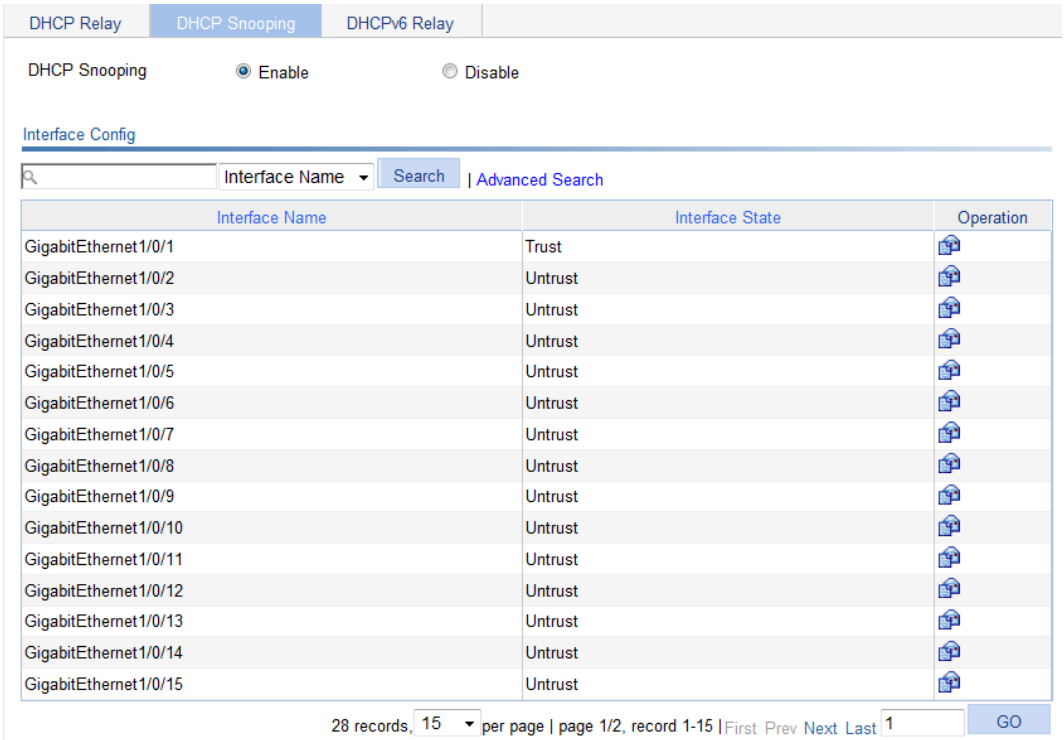
Figure 292 Network diagram



Configuring Switch B

1. Enable DHCP snooping:
   a. From the navigation tree, select **Network** > **DHCP**.
   b. Click the **DHCP Snooping** tab.
   c. As shown in Figure 293, select the **Enable** option next to **DHCP Snooping** to enable DHCP snooping.

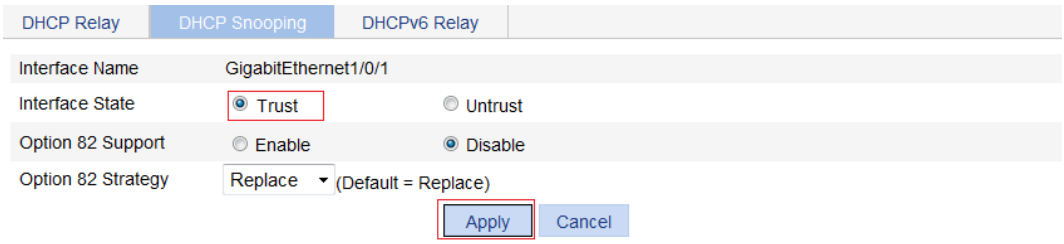
Figure 293 Enabling DHCP snooping



2. Configure DHCP snooping functions on GigabitEthernet 1/0/1:

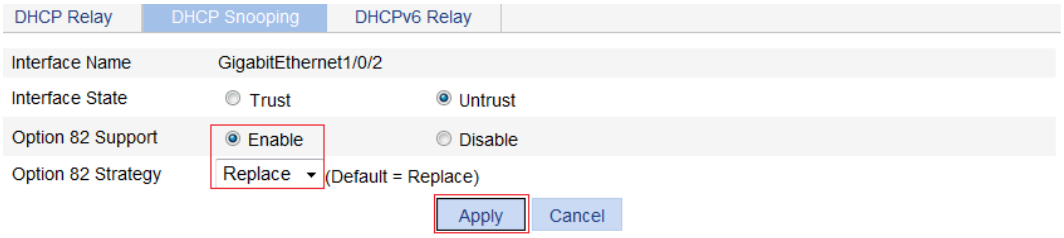
a. Click the icon of GigabitEthernet 1/0/1 on the interface list.
b. Select the **Trust** option next to **Interface State** as shown in Figure 294.
c. Click **Apply**.

Figure 294 Configuring DHCP snooping functions on GigabitEthernet 1/0/1



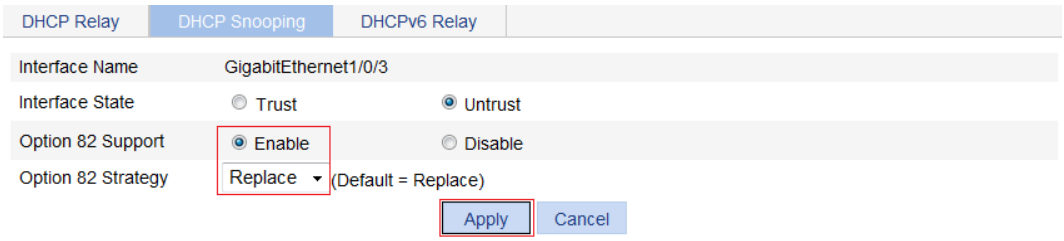
3. Configure DHCP snooping functions on GigabitEthernet 1/0/2:
   a. Click the icon of GigabitEthernet 1/0/2 on the interface list.
   b. Select the **Untrust** option for **Interface State** shown in Figure 295.
   c. Select the **Enable** option next to **Option 82 Support**.
   d. Select **Replace** for **Option 82 Strategy**.
   e. Click **Apply**.

Figure 295 Configuring DHCP snooping functions on GigabitEthernet 1/0/2



4. Configure DHCP snooping functions on GigabitEthernet 1/0/3:
   a. Click the icon of GigabitEthernet 1/0/3 on the interface list.
   b. Select the **Untrust** option for **Interface State** as shown in Figure 296.
   c. Select the **Enable** option next to **Option 82 Support**.
   d. Select **Replace** for **Option 82 Strategy**.
   e. Click **Apply**.

Figure 296 Configuring DHCP snooping functions on GigabitEthernet 1/0/3

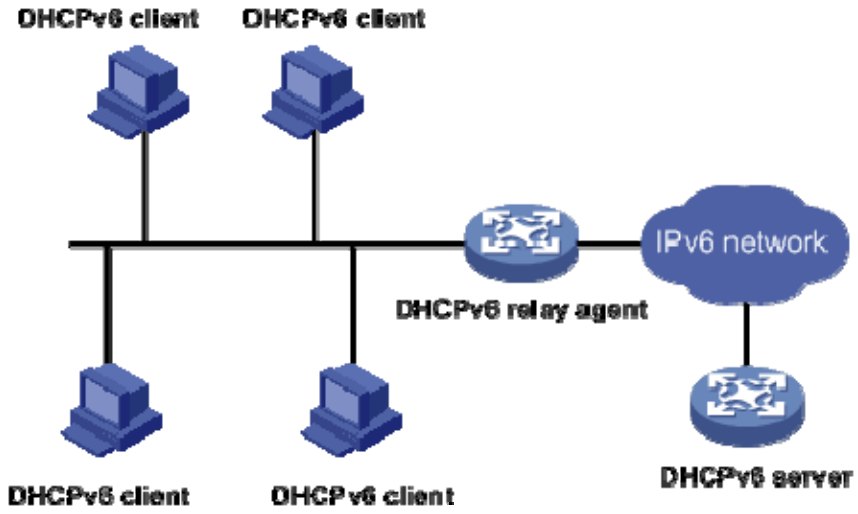


Configuring DHCPv6 relay agent

Overview

A DHCPv6 client usually uses a multicast address to contact the DHCPv6 server on the local link to obtain an IPv6 address and other configuration parameters. As shown in Figure 297, if the DHCPv6 server resides on another subnet, the DHCPv6 clients need a DHCPv6 relay agent to contact the server. The relay agent feature avoids deploying a DHCPv6 server on each subnet.

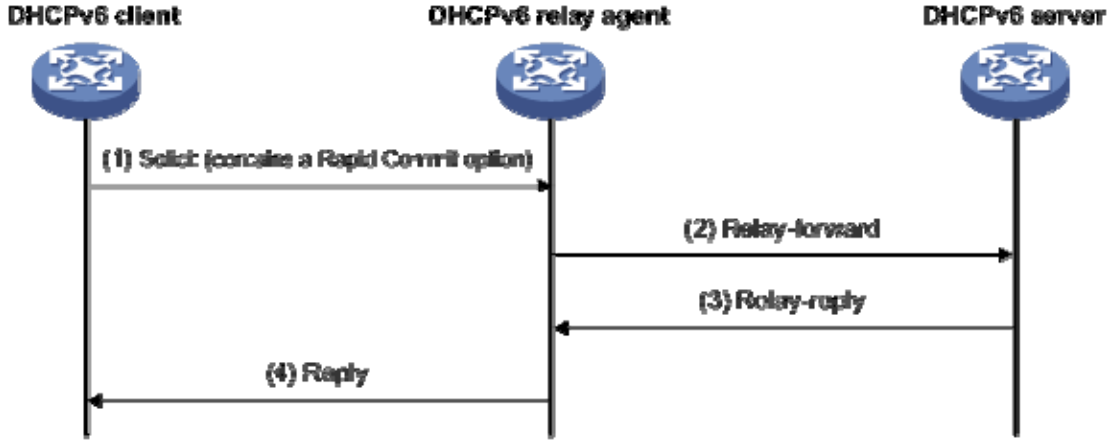
Figure 297 DHCPv6 relay agent application



As shown in Figure 298, a DHCPv6 client obtains an IPv6 address and other network configuration parameters from a DHCPv6 server through a DHCPv6 relay agent. The following example uses rapid assignment to describe the process:

- The DHCPv6 client sends a Solicit message containing the Rapid Commit option to the multicast address FF02::1:2 of all the DHCPv6 servers and relay agents.
- After receiving the Solicit message, the DHCPv6 relay agent encapsulates the message into the Relay Message option of a Relay-forward message, and sends the message to the DHCPv6 server.
- After obtaining the Solicit message from the Relay-forward message, the DHCPv6 server performs the following tasks:
  - Selects an IPv6 address and other required parameters.
  - Adds them to a reply that is encapsulated within the Relay Message option of a Relay-reply message.
  - Sends the Relay-reply message to the DHCPv6 relay agent.
- The DHCPv6 relay agent obtains the reply from the Relay-reply message and sends the reply to the DHCPv6 client.
- The DHCPv6 client uses the IPv6 address and other network parameters assigned by the DHCPv6 server to complete network configuration.

Figure 298 Operating process of a DHCPv6 relay agent



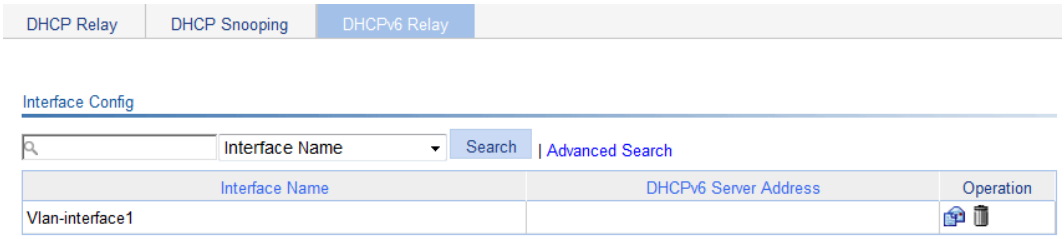
Recommended configuration procedure

Task	Remarks
Specifying a DHCPv6 server on the relay agent	Required. By default, no DHCPv6 server is specified.

Specifying a DHCPv6 server on the relay agent

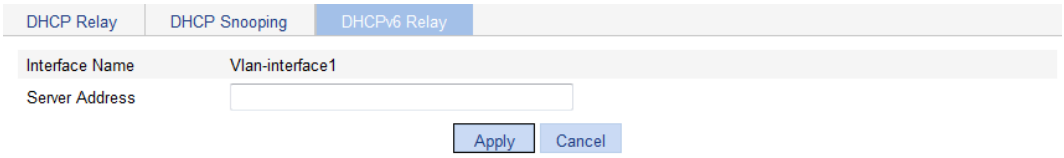
1. From the navigation tree, select **Network** > **DHCP**.
2. On the page that appears, click the **DHCPv6 Relay** tab.
   The page for configuring the DHCPv6 relay agent appears, as shown in Figure 299.

   Figure 299 Configuring the DHCPv6 relay agent interface



3. In the **Interface Config** area, locate the interface that acts as the DHCPv6 relay agent, and click the **Operation** icon for the interface.
   The page for configuring the DHCPv6 server address appears, as shown in Figure 300.

   Figure 300 Configuring the DHCPv6 server address



4. Specify the DHCPv6 server address, as shown in Table 103.

5. Click **Apply**.

Table 103 Configuration items

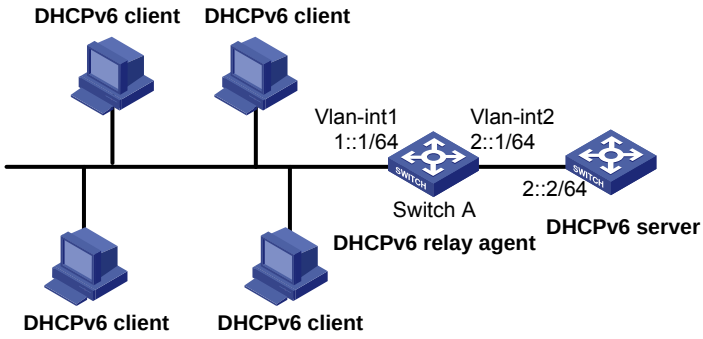
Item	Description
Server Address	Specify the DHCPv6 server address.

DHCPv6 relay agent configuration example

Network requirements

As shown in Figure 301, configure the DHCPv6 relay agent on Switch A to relay DHCPv6 packets between DHCPv6 clients and the DHCPv6 server.

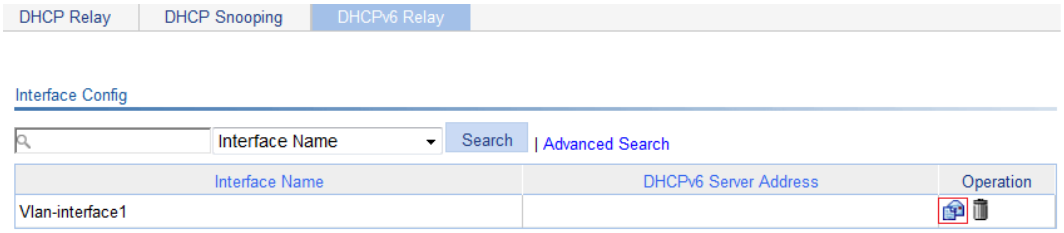
Figure 301 Network diagram



Configuration procedure

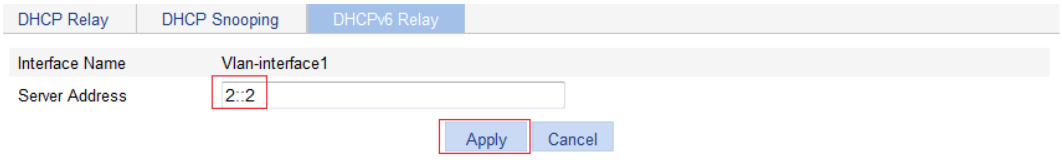
1. In the **Interface Config** area, click the **Operation** icon for VLAN-interface 1.

Figure 302 Configuring the DHCPv6 relay agent



2. Specify the DHCPv6 server address as **2::2**.

Figure 303 Specifying the DHCPv6 server address



3. Click **Apply**.

Managing services

Overview

Service management allows you to manage the following types of services: FTP, Telnet, SSH, SFTP, HTTP and HTTPS.

You can enable or disable the services, modify HTTP and HTTPS port numbers, and associate the FTP, HTTP, or HTTPS service with an ACL to block illegal users.

FTP service

FTP is an application layer protocol for sharing files between server and client over a TCP/IP network.

Telnet service

Telnet is an application layer protocol that provides remote login and virtual terminal functions.

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

HTTP is used for transferring webpage information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite.

You can log in to the device by 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.

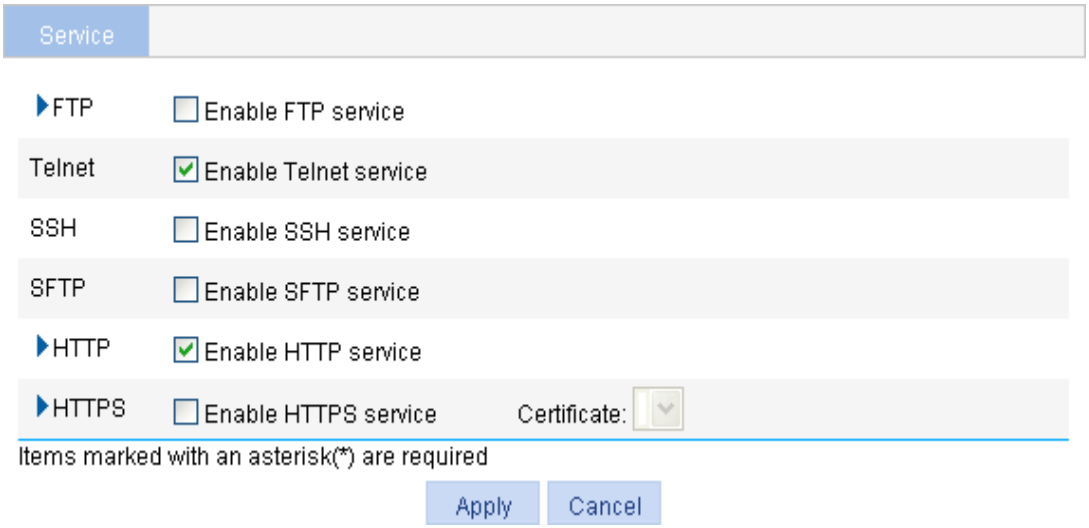
The SSL protocol of HTTPS enhances the security of the device in the following ways:

- 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.
- Defines certificate attribute-based access control policy for the device to control user access.

Managing services

1. Select **Network** > **Service** from the navigation tree to enter the service management configuration page, as shown in Figure 304.

Figure 304 Service management



2. Enable or disable services on the page. Table 104 describes the detailed configuration items.
3. Click **Apply**.

Table 104 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.
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 the port is not used by any other service.

Item		Description
	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.
	Certificate	Select a local certificate for the HTTPS service from the **Certificate** dropdown list. You can configure the certificates available in the dropdown list in **Authentication** > **Certificate Management.** For more information, see "Managing certificates." **IMPORTANT:** If no certificate is specified, the HTTPS service generates its own certificate.
	Port Number	Set the port number for 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 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**.

Using diagnostic tools

This chapter describes how to use the ping and traceroute utilities.

Ping

Use the ping utility to determine if a specific address is reachable.

A ping operation involves the following steps:

1. The source device sends ICMP echo requests to the destination device.
2. The destination device responds by sending ICMP echo replies to the source device after receiving the ICMP echo requests.
3. The source device displays related statistics after receiving the replies.

You can ping the IP address or the host name of a device. A prompt appears if the host name cannot be resolved.

If the source device does not receive an ICMP echo reply within the timeout time, it displays:

- A prompt.
- Ping statistics.

If the source device receives ICMP echo replies within the timeout time, it displays:

- Number of bytes for each echo reply.
- Message sequence number.
- Time to Live (TTL).
- Response time.
- Ping statistics.

Ping statistics include:

- Number of echo requests sent.
- Number of echo replies received.
- Percentage of echo replies not received.
- Minimum, average, and maximum response time.

Traceroute

Traceroute retrieves the IP addresses of Layer 3 devices in the path to a specific destination. You can use traceroute to test network connectivity and identify failed nodes.

You can traceroute the IP address or the host name of a destination device. If the target host name cannot be resolved, a prompt appears.

A traceroute operation involves the following steps:

1. The source device sends a packet with a Time to Live (TTL) value of 1 to the destination device.
2. The first hop device responds with an ICMP TTL-expired message to the source. In this way, the source device gets the address of the first device.
3. The source device sends a packet with a TTL value of 2 to the destination device.
4. The second hop responds with an ICMP TTL-expired message. In this way, the source device gets the address of the second device.

5. The destination device responds with an ICMP port-unreachable message because the packet from the source has an unreachable port number. In this way, the source device gets the address of the destination device.

In this way, the source device can get the addresses of all Layer 3 devices on the path.

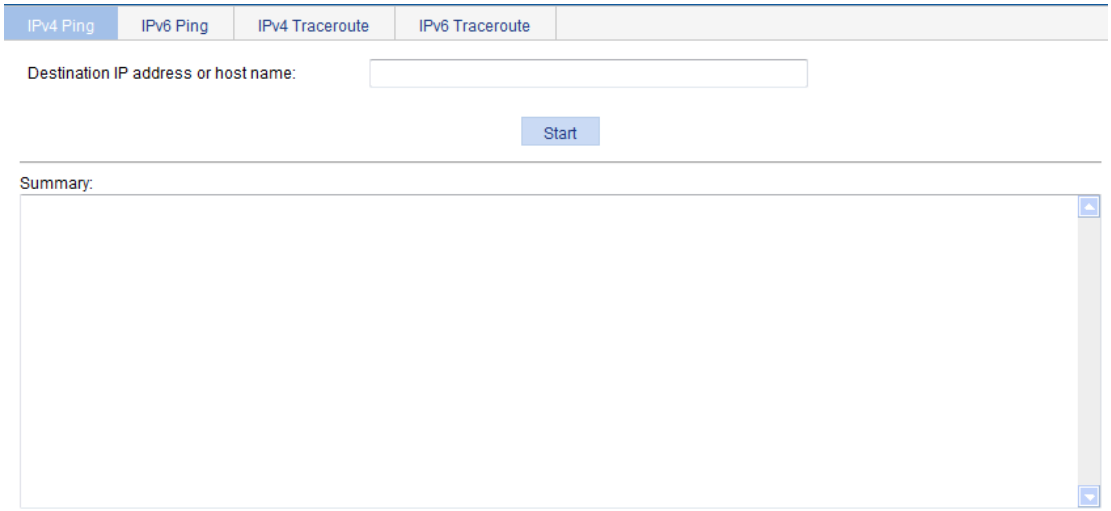
Ping operation

Configuring IPv4 Ping

1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv4 Ping** tab.

   The ping configuration page appears.

   Figure 305 Ping configuration page



3. Enter the IP address or the host name of the destination device in the **Destination IP address or host name** field.
4. Click **Start**.

   The output is displayed in the **Summary** area.

   Figure 306 IPv4 ping output

Summary:

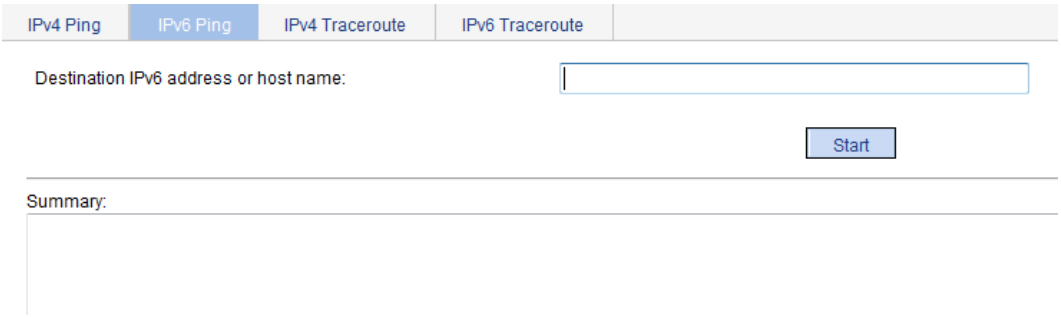
```
PING 192.168.1.16: 56  data bytes
  Reply from 192.168.1.16: bytes=56 Sequence=1 ttl=128 time=4 ms
  Reply from 192.168.1.16: bytes=56 Sequence=2 ttl=128 time=4 ms
  Reply from 192.168.1.16: bytes=56 Sequence=3 ttl=128 time=3 ms
  Reply from 192.168.1.16: bytes=56 Sequence=4 ttl=128 time=3 ms
  Reply 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
```

Configuring IPv6 Ping

1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv6 Ping** tab.

   The ping configuration page appears.

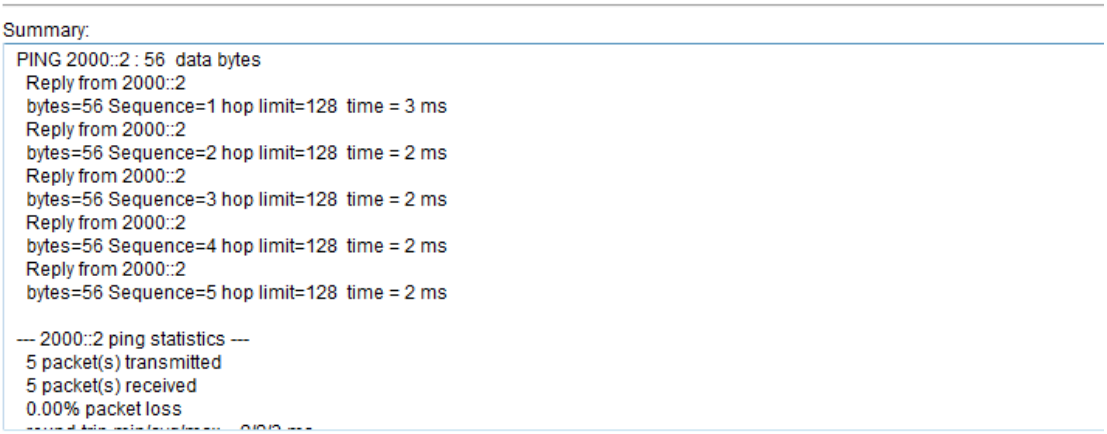
   Figure 307 Ping configuration page



3. Enter the IP address or the host name of the destination device in the **Destination IPv6 address or host name** field.
4. Click **Start**.

   The output is displayed in the **Summary** area.

   Figure 308 IPv6 ping output



Traceroute operation

Before performing a traceroute operation, perform the following tasks:

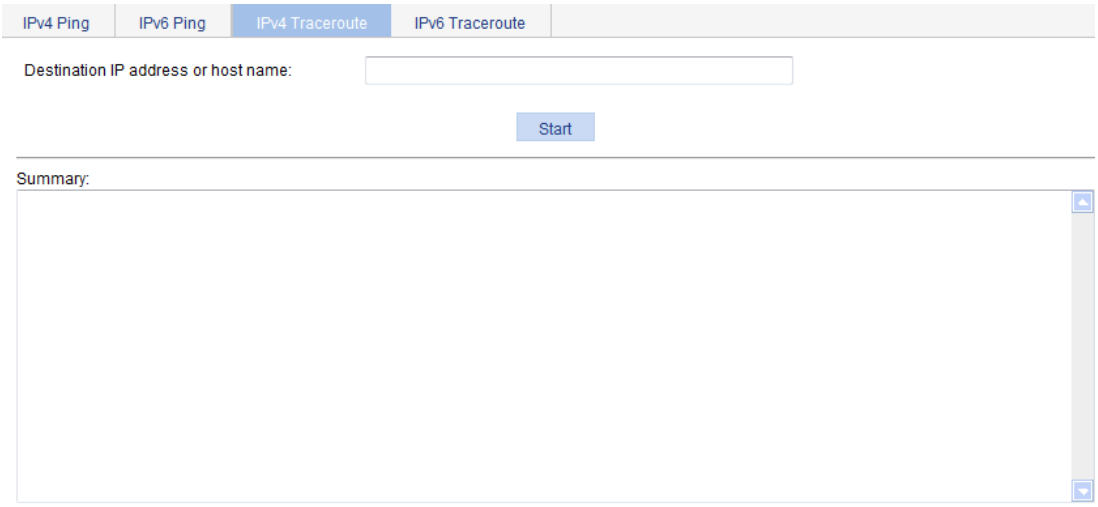
- Enable sending of ICMP timeout packets by executing the **ip ttl-expires enable** command on intermediate devices.
- Enable sending of ICMP destination unreachable packets by executing the **ip unreachables enable** command on the destination device.

Configuring IPv4 traceroute

1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv4 Traceroute** tab.

The traceroute configuration page appears.

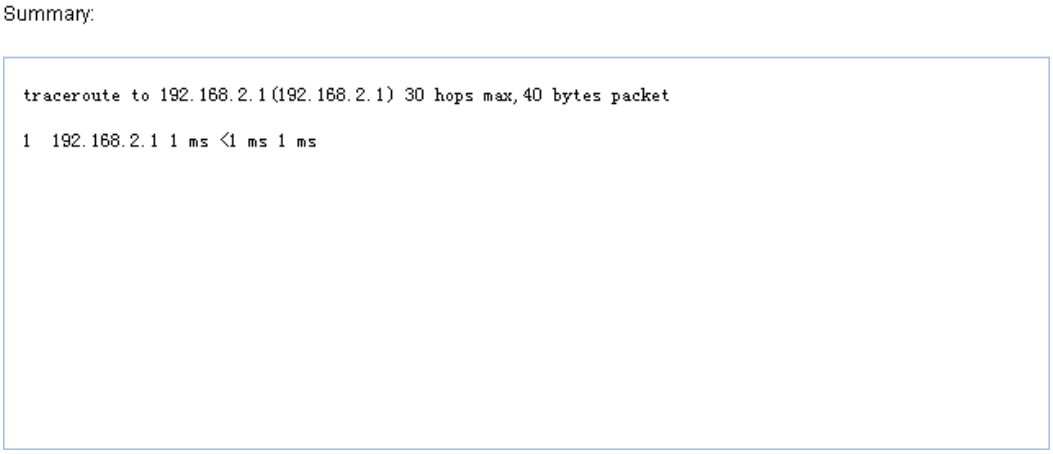
Figure 309 Traceroute configuration page



3. Enter the IP address or host name of the destination device in the **Destination IP address or host name** field.
4. Click **Start**.

   The output is displayed in the **Summary** area.

Figure 310 IPv4 traceroute output

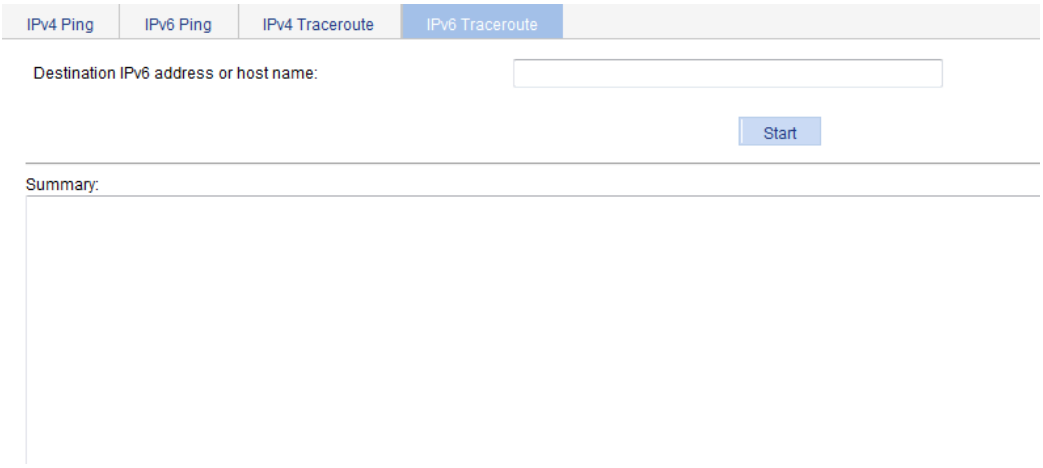


Configuring IPv6 traceroute

1. Select **Network** > **Diagnostic Tools** from the navigation tree.
2. Click the **IPv6 Traceroute** tab.

   The traceroute configuration page appears.

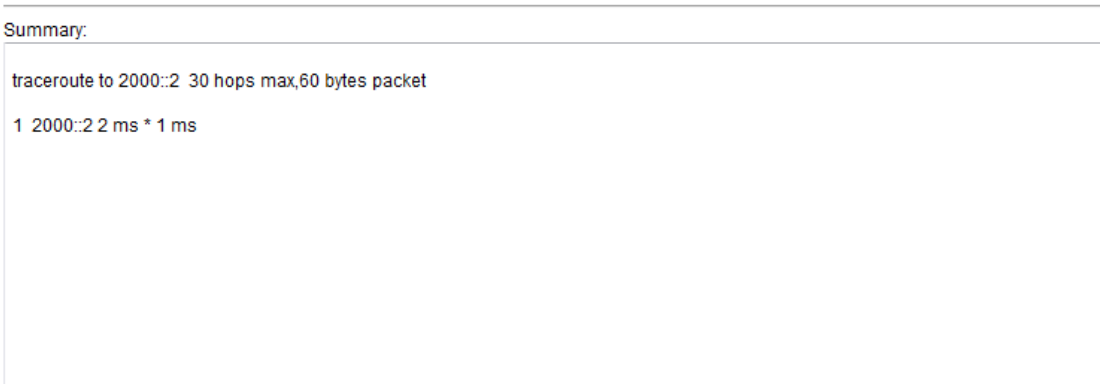
Figure 311 Traceroute configuration page



3. Enter the IP address or host name of the destination device in the **Destination IPv6 address or host name** field.
4. Click **Start**.

   The output is displayed in the **Summary** area.

Figure 312 IPv6 traceroute output



Configuring 802.1X

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 WLANs. It has been widely used on Ethernet for access control.

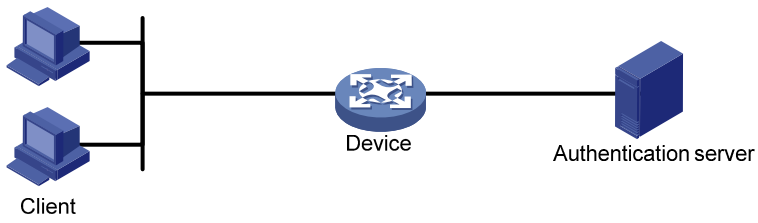
802.1X controls network access by authenticating the devices connected to 802.1X-enabled LAN ports.

This chapter describes how to configure 802.1X on an HPE device. You can also configure the port security feature to perform 802.1X. Port security combines and extends 802.1X and MAC authentication. It applies to a network (for example, a WLAN) that requires different authentication methods for different users on a port. For more information, see "Configuring port security."

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 313 802.1X architecture



- **Client**—A user terminal seeking access to the LAN. It must have 802.1X software to authenticate to the network access device.
- **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.
- **Authentication server**—Provides authentication services for the network access device. The authentication server authenticates 802.1X clients by using the data sent from the network access device, and returns the authentication results to the network access device to make access decisions. The authentication server is typically a RADIUS server. In a small LAN, you can also use the network access device as the authentication server.

Access control methods

Hewlett Packard Enterprise implements port-based access control as defined in the 802.1X protocol, and extends the protocol to support MAC-based access control.

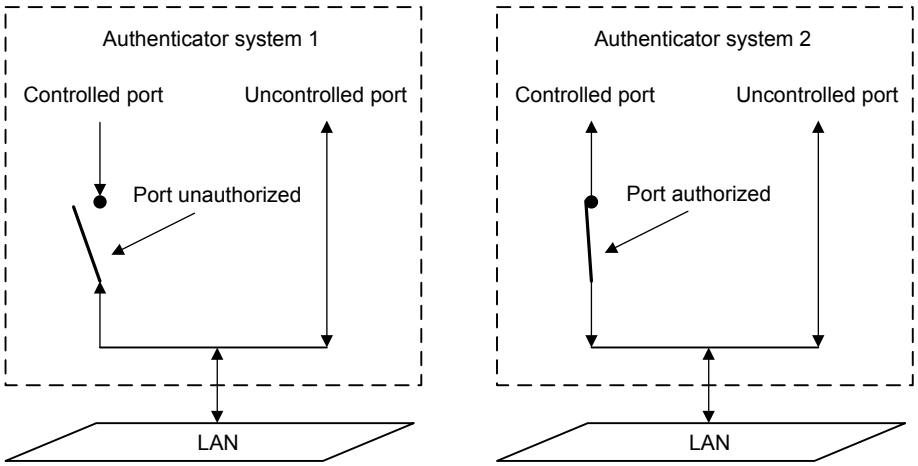
- **Port-based access control**—Once an 802.1X user passes authentication on a port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.
- **MAC-based access control**—Each user is separately authenticated 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.

- **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 314. The controlled port is set in authorized state if the client has passed authentication, and in unauthorized state, if the client has failed authentication.
- **Uncontrolled port**—Is always open to receive and transmit EAPOL frames.

Figure 314 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.

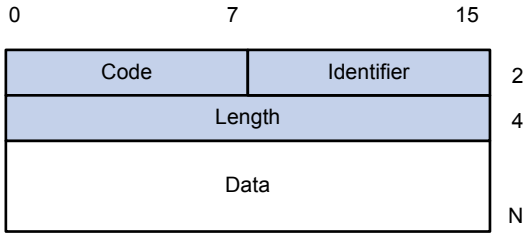
The device supports only unidirectional traffic control.

Packet formats

EAP packet format

Figure 315 shows the EAP packet format.

Figure 315 EAP packet format



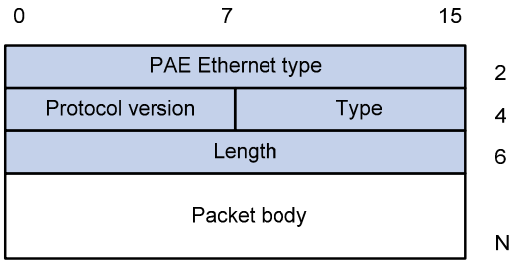
- **Code**—Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- **Identifier**—Used for matching Responses with Requests.
- **Length**—Length (in bytes) of the EAP packet. The length is the sum of the Code, Identifier, Length, and Data fields.

- **Data**—Content of the EAP packet. This field appears only in a Request or Response EAP packet. The Data 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 316 shows the EAPOL packet format.

Figure 316 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 105 lists the types of EAPOL packets supported by Hewlett Packard Enterprise implementation of 802.1X.

  Table 105 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.
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.

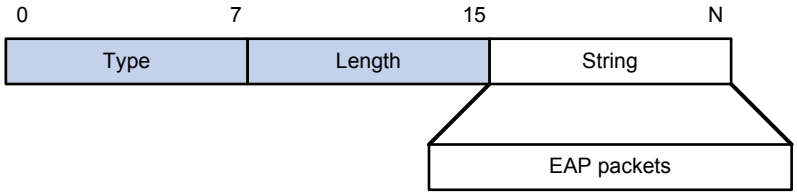
EAP over RADIUS

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 317. 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.

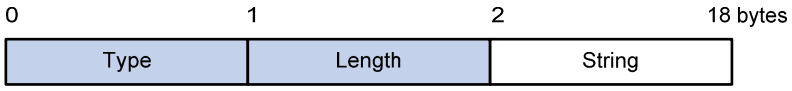
Figure 317 EAP-Message attribute format



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 from the Message-Authenticator attribute value. The Message-Authenticator prevents EAP authentication packets from being tampered with during EAP authentication.

Figure 318 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 (for example, the HPE iNode 802.1X client) that can send broadcast EAPOL-Start packets.

Access device as the initiator

The access device initiates authentication, if a client cannot send EAPOL-Start packets. One example is the 802.1X client available with Windows XP.

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 provides the following methods for authentication:

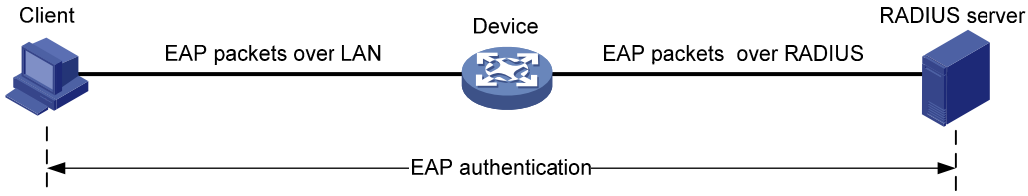
- EAP relay.
- EAP termination.

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 319.

Figure 319 EAP relay



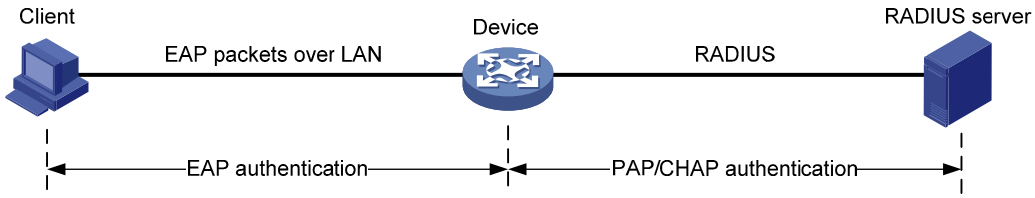
In EAP relay mode, the client must use the same authentication method as the RADIUS server. On the network access device, you only need to enable EAP relay.

Some network access devices provide the EAP server function so you can use EAP relay even if the RADIUS server does not support any EAP authentication method or no RADIUS server is available.

- 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 PAP or CHAP to authenticate to the RADIUS server, as shown in Figure 320.

  Figure 320 EAP termination



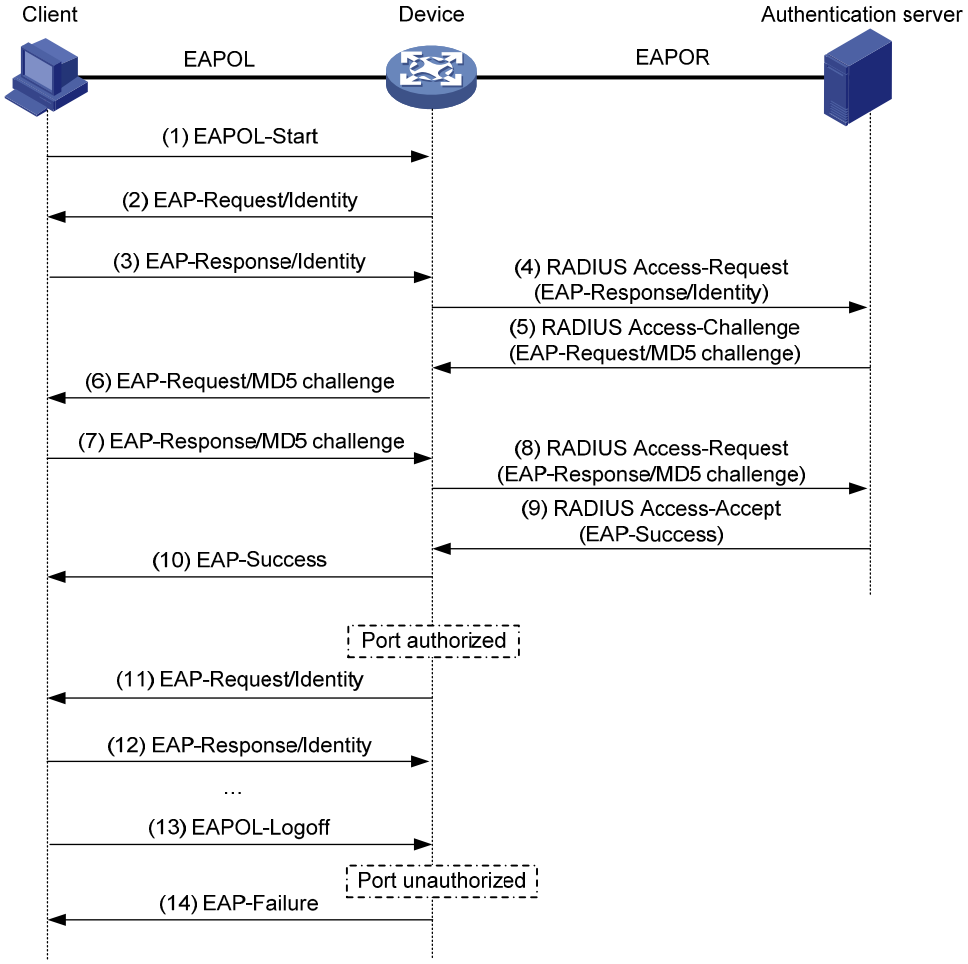
Comparing EAP relay and EAP termination

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 HPE iNode 802.1X client. • The processing is complex on the network access device.

EAP relay

Figure 321 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

Figure 321 802.1X authentication procedure in EAP relay mode



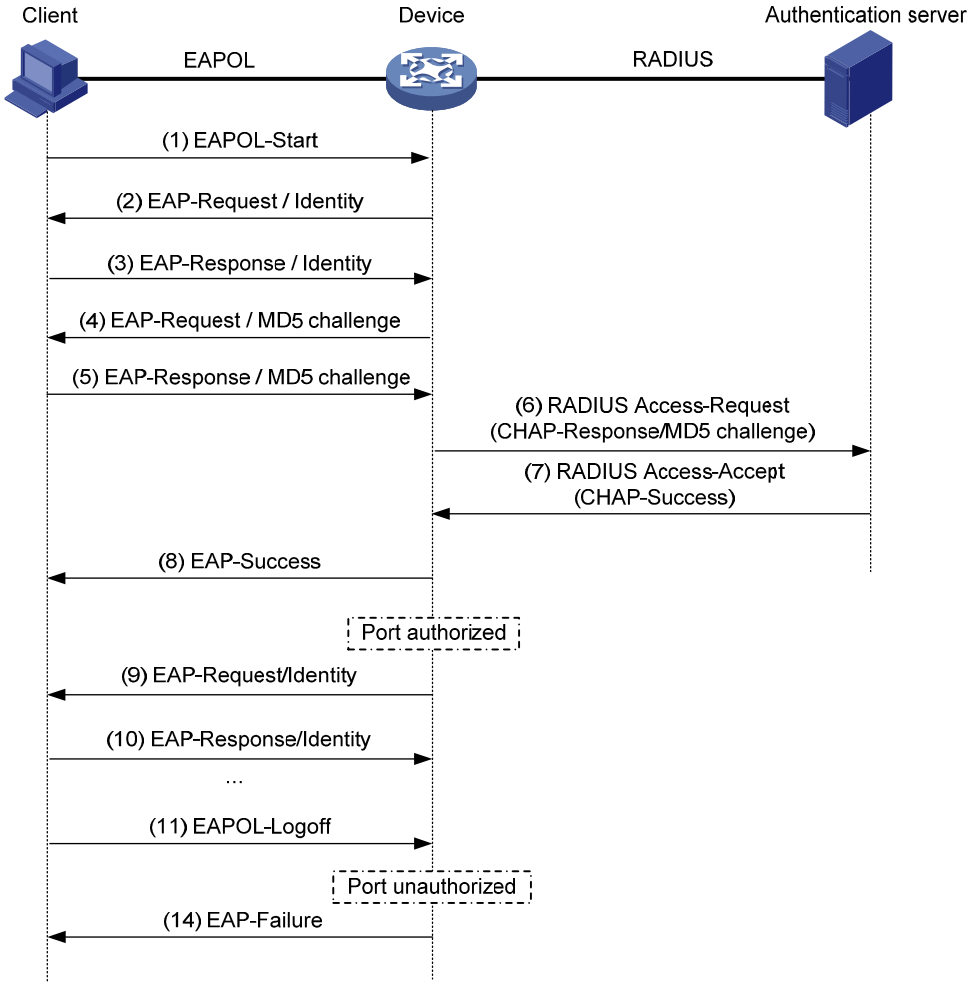
1. When a user launches the 802.1X client software and enters a registered username and password, the 802.1X client software sends an EAPOL-Start packet to the network access device.
2. The network access device responds with an Identity EAP-Request packet to ask for the client username.
3. In response 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 322 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 322 802.1X authentication procedure in EAP termination mode



In EAP termination mode, 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 correctly.

- **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. For information about how to enable the online user handshake function, see "Configuring 802.1X on a port."
- **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. For information about how to enable periodic online user re-authentication on a port, see "Configuring 802.1X on a port."

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 a hybrid port with MAC-based VLAN enabled, the device maps the MAC address of each user to the VLAN assigned by the authentication server. The PVID of the port does not change. When a user logs off, the MAC-to-VLAN mapping for the user is removed. • If the port is an access, trunk, or MAC-based VLAN disabled hybrid port, the device 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.

With 802.1X authentication, a hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

On a periodic online user re-authentication enabled port, if a user has been online before you enable the MAC-based VLAN function, the access device does not create a MAC-to-VLAN mapping for the user unless the user passes re-authentication and the VLAN for the user has changed.

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. Once a user in the guest VLAN passes 802.1X authentication, it is removed from the guest VLAN and can access authorized network resources. The way that the network access device handles VLANs on the port differs by 802.1X access control mode.

- On a port that performs port-based access control:

Authentication status	VLAN manipulation
No 802.1X user has performed authentication within 90 seconds after 802.1X is enabled.	The device 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, the device 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.	• The device 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 PVID. After the user logs off, the PVID remains unchanged.

- On a port that performs MAC-based access control:

Authentication status	VLAN manipulation
A user has not passed 802.1X authentication yet.	The device creates a mapping between the MAC address of the user and the 802.1X guest VLAN. The user can access resources in the guest VLAN.
A user in the 802.1X guest VLAN fails 802.1X authentication.	If an 802.1X Auth-Fail VLAN is available, the device remaps the MAC address of the user to the Auth-Fail VLAN. The user can access only resources in the Auth-Fail VLAN. If no 802.1X Auth-Fail VLAN is configured, the user is still in the guest VLAN.
A user in the 802.1X guest VLAN passes 802.1X authentication.	The device remaps the MAC address of the user to the authorized VLAN. If the authentication server assigns no authorized VLAN, the device remaps the MAC address of the user to the initial PVID on the port.

To use the 802.1X guest VLAN function on a port that performs MAC-based access control, make sure the port is a hybrid port, and enable MAC-based VLAN on the port.

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 way that the network access device handles VLANs on the port differs by 802.1X access control mode.

- On a port that performs port-based access control:

Authentication status	VLAN manipulation
A user fails 802.1X authentication.	The device 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.	• The device 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.

- On a port that performs MAC-based access control:

Authentication status	VLAN manipulation
A user fails 802.1X authentication.	The device remaps the MAC address of the user to the Auth-Fail VLAN. The user can access only resources in the Auth-Fail VLAN.
A user in the Auth-Fail VLAN fails 802.1X re-authentication.	The user is still in the Auth-Fail VLAN.
A user in the Auth-Fail VLAN passes 802.1X authentication.	The device remaps the MAC address of the user to the server-assigned VLAN. If the authentication server assigns no VLAN, remaps the MAC address of the user to the initial PVID on the port.

To perform the 802.1X Auth-Fail VLAN function on a port that performs MAC-based access control, you must ensure that the port is a hybrid port, and enable MAC-based VLAN on the port.

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

When you configure 802.1X, follow these restrictions and guidelines:

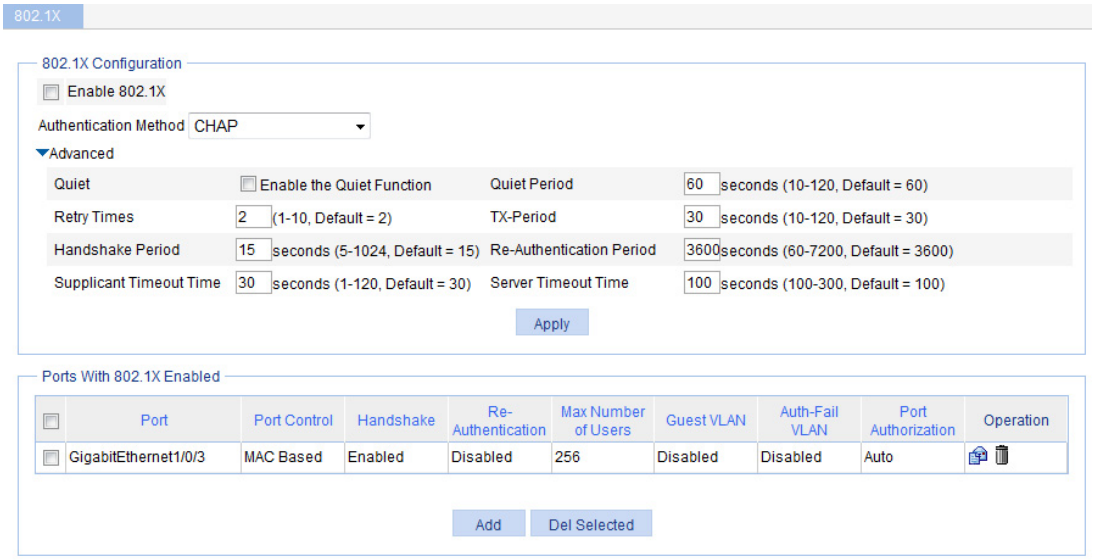
- Configure an ISP domain and AAA scheme (local or RADIUS authentication) for 802.1X users. For more information, see "Configuring AAA" and "Configuring RADIUS."
- If RADIUS authentication is used, create user accounts on the RADIUS server.
- If local authentication is used, create local user accounts on the access device and specify the LAN access service for the user accounts. For more information, see "Configuring users."

Recommended configuration procedure

Step	Remarks
1. Configuring 802.1X globally	Required. This function enables 802.1X authentication globally. It also configures the authentication method and advanced parameters.By default, 802.1X authentication is disabled globally.
2. Configuring 802.1X on a port	Required. This function enables 802.1X authentication on the specified port and configures 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**.
   The **802.1X** page appears.
   Figure 323 Configuring 802.1X



2. In the **802.1X Configuration** area, select **Enable 802.1X**.
3. Select an authentication method from the **Authentication Method** list.

   Authentication Method list

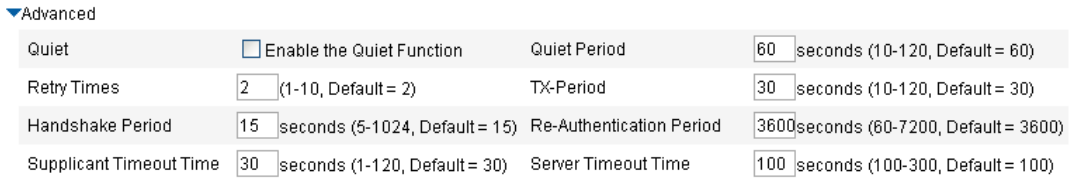
- **CHAP**—Sets the access device to perform EAP termination and use CHAP to communicate with the RADIUS server.
- **PAP**—Sets the access device to perform EAP termination and use PAP to communicate with the RADIUS server.
- **EAP**—Sets the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

  When you configure 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.

4. Click **Advanced** to expand the advanced 802.1X configuration area.

Figure 324 Configuring advanced 802.1X parameters



5. Configure advanced 802.1X settings as described in Table 106, and then click **Apply**.

Table 106 Configuration items

Item	Description
Quiet	Sets whether to enable the quiet timer.
Quiet Period	Sets the value of the quiet timer.
Retry Times	Sets the maximum number of authentication request attempts. The network access device retransmits an authentication request if it does not receive a response to the request it has sent to the client within a period of time (set by the **TX Period** or the **Supplicant Timeout Time** value). 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	Sets the username request timeout timer.
Handshake Period	Sets the handshake timer.
Re-Authentication Period	Sets the periodic online user re-authentication timer.
Supplicant Timeout Time	Sets the client timeout timer.
Server Timeout Time	Sets 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

1. From the navigation tree, select **Authentication** > **802.1X**.
2. In the **Ports With 802.1X Enabled** area, click **Add**.
3. Configure 802.1X features on a port as shown in Figure 325, and then click **Apply**.

Figure 325 Configuring 802.1X on a port

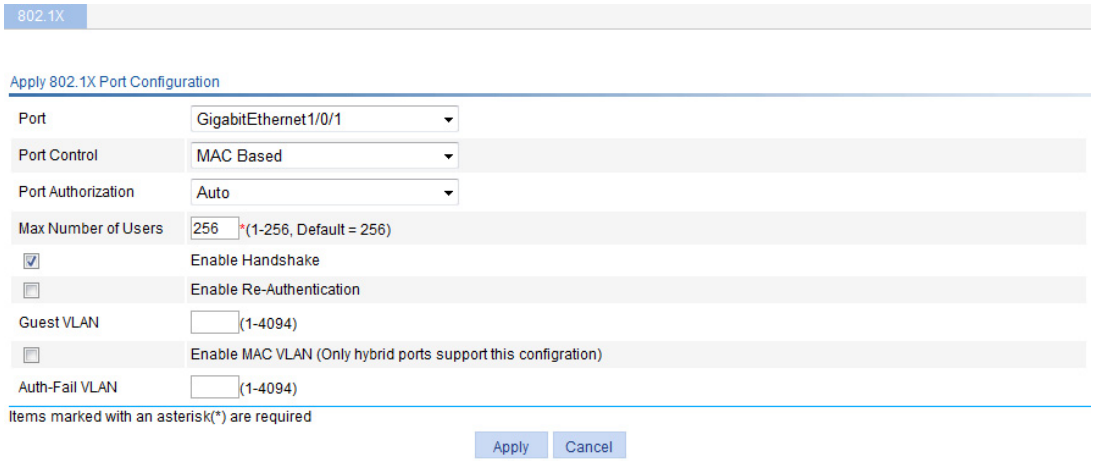


Table 107 describes the configuration items.

Table 107 Configuration items

Item	Description
Port	Selects a port where you want to enable 802.1X. Only ports not enabled with 802.1X authentication are available. 802.1X configuration takes effect on a port only after 802.1X is enabled both globally and on the port.
Port Control	Selects an access control method for the port, **MAC Based** or **Port Based**.
Port Authorization	Selects a port authorization state for 802.1X: • **Auto**—Places the port 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 port in the authorized state, enabling users on the port to access the network without authentication. • **Force-Unauthorized**—Places the port in the unauthorized state, denying any access requests from users on the port.
Max Number of Users	Sets the maximum number of concurrent 802.1X users on the port.
Enable Handshake	Specifies whether to enable the online user handshake function. This function enables the network access device to send handshake messages to online users at the interval set by the **Handshake Period** setting. If no response is received from an online user after the maximum number of handshake attempts (set by the **Retry Times** setting) has been made, the network access device sets the user in the offline state. For information about the timers, see "Configuring 802.1X globally." **NOTE:** If the network has 802.1X clients that cannot exchange handshake packets with the network access device, disable the online user handshake function to prevent their connections from being inappropriately torn down.

Item	Description
Enable Re-Authentication	Specifies whether 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** setting in Table 106. **NOTE:** • The periodic online user re-authentication timer can also be set by the authentication server in the session-timeout attribute. The server-assigned timer overrides the timer setting on the access device, and it enables periodic online user re-authentication, even if the function is not configured on the access device. Support for the server assignment of re-authentication timer and the re-authentication timer configuration on the server vary with servers. • The VLAN assignment status must be consistent before and after re-authentication. If the authentication server has assigned a VLAN before re-authentication, it must also assign a VLAN at re-authentication. If the authentication server has assigned no VLAN before re-authentication, it must not assign one at re-authentication. Violation of either rule can cause the user to be logged off. The VLANs assigned to an online user before and after re-authentication can be the same or different.
Guest VLAN	Specifies an existing VLAN as the guest VLAN. For more information, see "Configuring an 802.1X guest VLAN."
Enable MAC VLAN	Specifies whether to enable MAC-based VLAN. Required when **MAC Based** is selected for **Port Control**. NOTE: Only hybrid ports support the feature.
Auth-Fail VLAN	Specifies 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.
- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the 802.1X guest VLAN as an untagged member.

Configuration guidelines

- The 802.1X guest VLANs on different ports can be different.
- Assign different IDs to the port VLAN 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 reconfigure the port as a tagged member in the VLAN.
- Use Table 108 when you configure multiple security features on a port.

Table 108 Relationships of the 802.1X guest VLAN and other security features

Feature	Relationship description
MAC authentication guest VLAN on a port that performs MAC-based access control	Only the 802.1X guest VLAN take effect. A user that fails MAC authentication will not be assigned to the MAC authentication guest VLAN.
802.1X Auth-Fail VLAN on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN has a higher priority.
Port intrusion protection on a port that performs MAC-based access control	The 802.1X guest VLAN function has higher priority than the block MAC action, but it has lower priority than the shutdown port action of the port intrusion protection feature.

Configuring an Auth-Fail VLAN

Configuration prerequisites

- Create the VLAN to be specified as the 802.1X Auth-Fail VLAN.
- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the Auth-Fail VLAN as an untagged member.

Configuration guidelines

- The 802.1X Auth-Fail VLANs on different ports can be different.
- Assign different IDs to the port VLAN and the 802.1X Auth-Fail VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.
- Use Table 109 when configuring multiple security features on a port.

Table 109 Relationships of the 802.1X Auth-Fail VLAN with other features

Feature	Relationship description
MAC authentication guest VLAN on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN has a high priority.
Port intrusion protection on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN function has higher priority than the block MAC action, but it has lower priority than the shutdown port action of the port intrusion protection feature.

802.1X configuration examples

MAC-based 802.1X configuration example

Network requirements

As shown in Figure 326, 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.

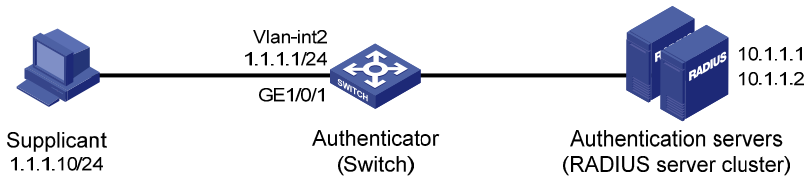
Configure the host at 10.1.1.1 as the primary authentication and secondary accounting servers, and the host at 10.1.1.2 as the secondary authentication and primary accounting servers. Assign all users to the ISP domain **test**.

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 5 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 326 Network diagram



Configuring IP addresses

Assign an IP address to each interface as shown in Figure 326. Make sure the supplicant, switch, and servers can reach each other. (Details not shown.)

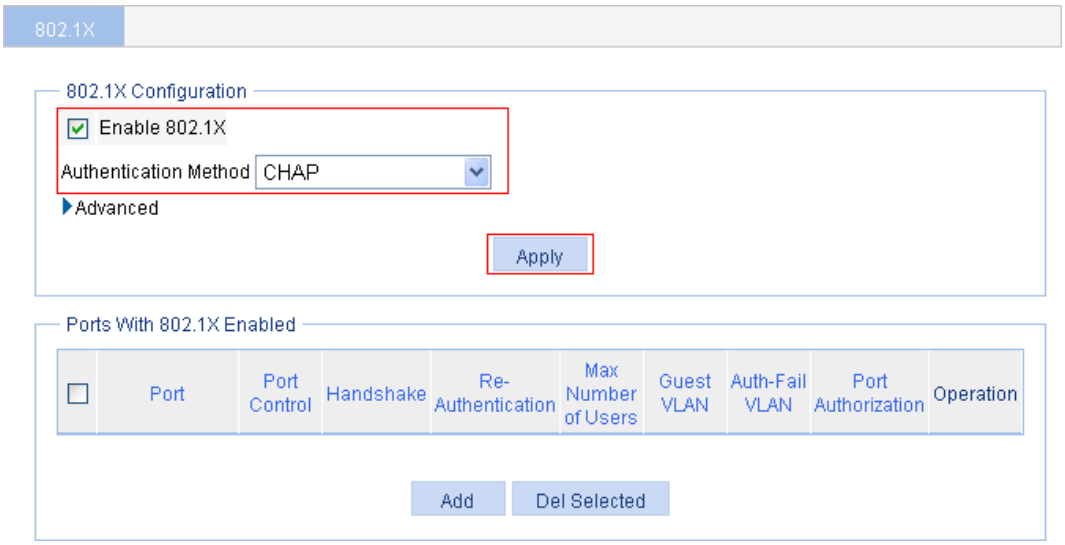
Configuring the RADIUS servers

For more information about the RADIUS configuration, see "Configuring RADIUS."

Configuring 802.1X for the switch

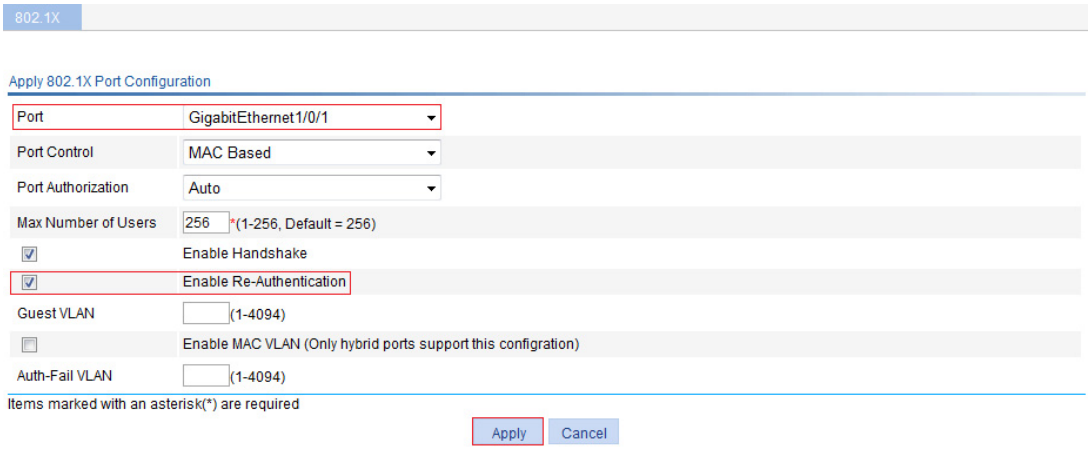
1. Configure global 802.1X:
   a. From the navigation tree, select **Authentication** > **802.1X**.
   b. Select **Enable 802.1X**, select the authentication method as **CHAP**, and click **Apply**.

   Figure 327 Configuring 802.1X globally



2. Configure 802.1X for GigabitEthernet 1/0/1:
   a. In the **Ports With 802.1X Enabled** area, click **Add**.
   b. Select **GigabitEthernet1/0/1** from the **Port** list, select **Enable Re-Authentication**, and click **Apply**.

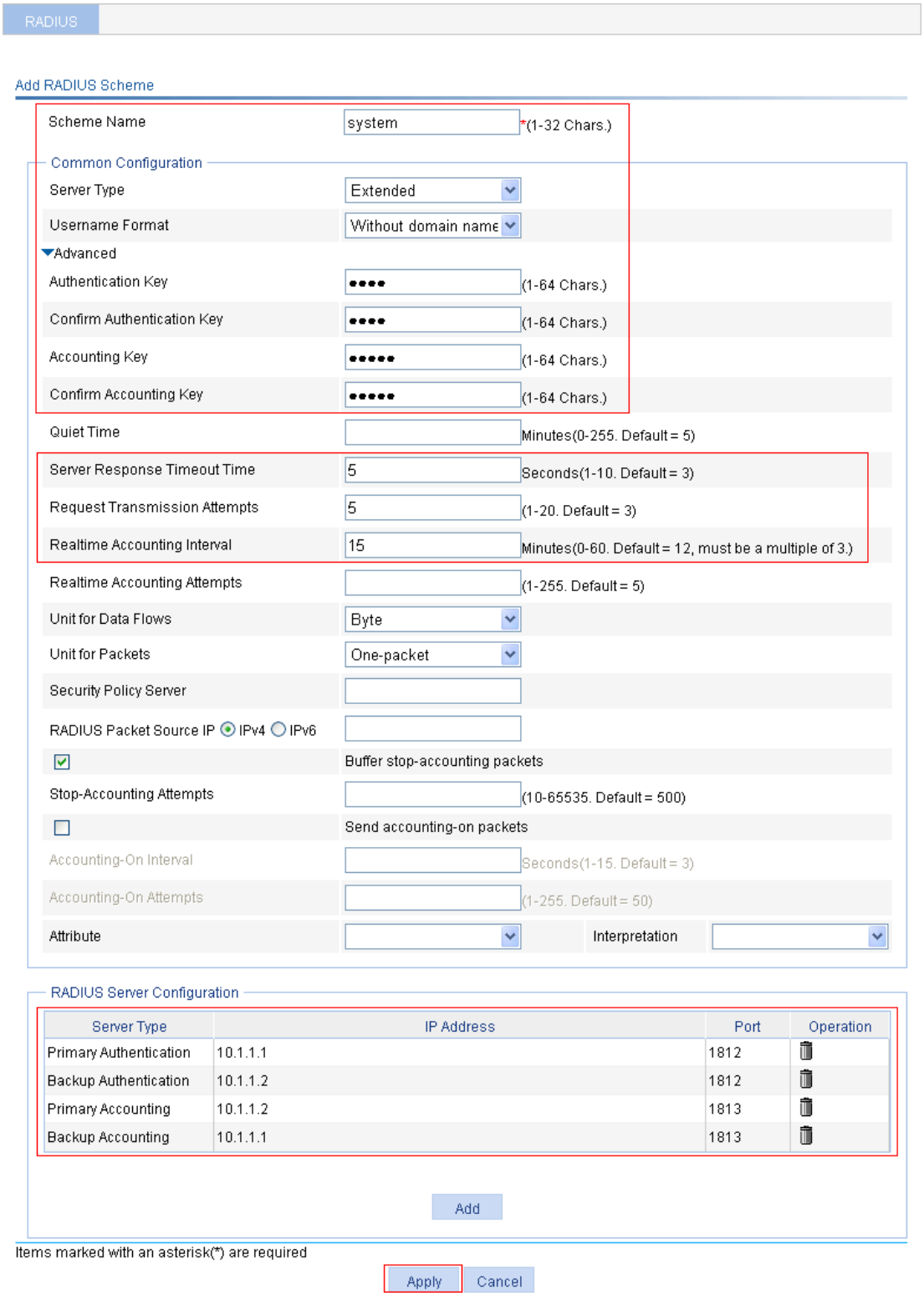
Figure 328 Configuring 802.1X for GigabitEthernet 1/0/1



Configuring the RADIUS scheme for the switch

1. Configure authentication and accounting attributes for the RADIUS scheme:
   a. From the navigation tree, select **Authentication** > **RADIUS,** and click **Add**.
   b. Enter the scheme name **system**.
   c. Select the server type **Extended**, and select **Without domain name** from the **Username Format** list.
   d. Click **Advanced**.
   e. Enter **name** in the **Authentication Key** and **Confirm Authentication Key** fields.
   f. Enter **money** in the **Accounting Key** and **Confirm Accounting Key** fields.
   g. Enter **5** as the server timeout timer.
   h. Enter **5** as the maximum number of request transmission attempts.
   i. Enter **15** as the realtime accounting interval.

Figure 329 Configuring the RADIUS scheme



2. Configure the primary authentication server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Primary Authentication**.
   c. Enter the IP address **10.1.1.1**, and enter the port number **1812**.

d. Click **Apply**.

   The **RADIUS Server Configuration** area displays the primary authentication server you have configured.

3. Configure the backup authentication server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Backup Authentication**.
   c. Enter the IP address **10.1.1.2**, and enter the port number **1812**.
   d. Click **Apply**.

      The **RADIUS Server Configuration** area displays the backup authentication server you have configured.
4. Configure the primary accounting server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Primary Accounting**.
   c. Enter the IP address **10.1.1.2**, and enter the port number **1813**.
   d. Click **Apply**.

      The **RADIUS Server Configuration** area displays the accounting server you have configured.
5. Configure the secondary accounting server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Backup Accounting**.
   c. Enter the IP address **10.1.1.1**, and enter the port number **1813**.
   d. Click **Apply**.

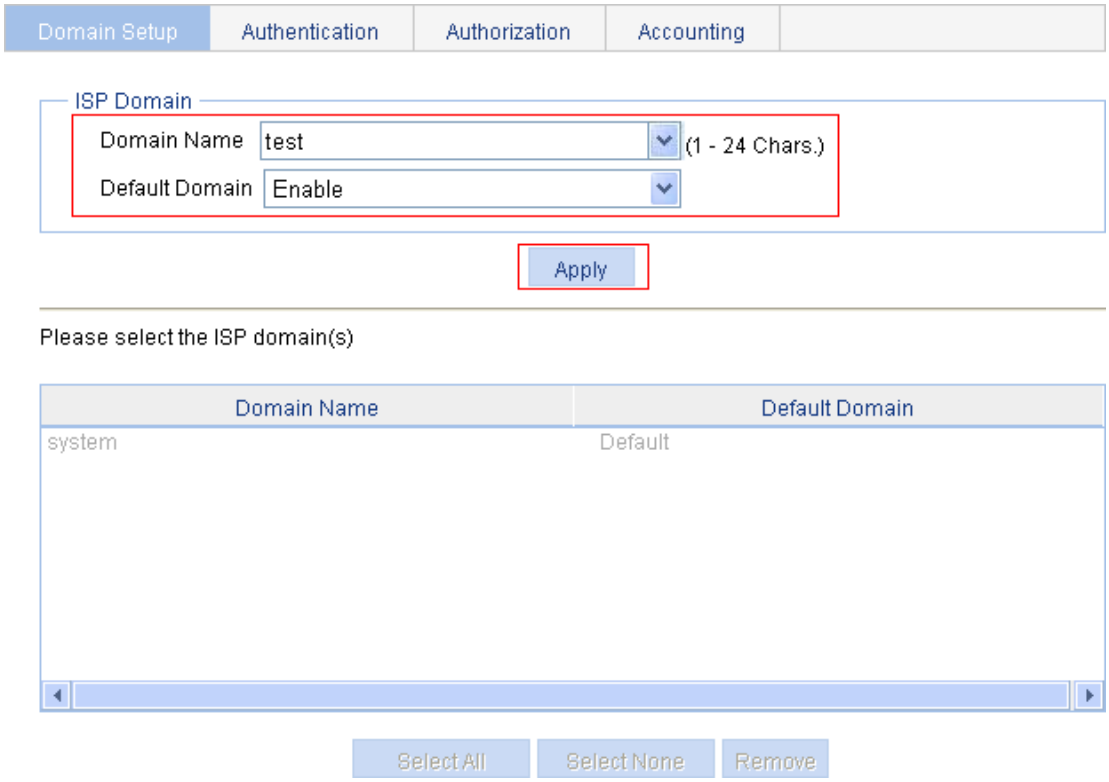
      The **RADIUS Server Configuration** area displays the backup accounting server you have configured.
6. On the RADIUS configuration page, click **Apply**.

Configuring AAA for the scheme

1. Create an ISP domain:
   a. From the navigation tree, select **Authentication** > **AAA**.

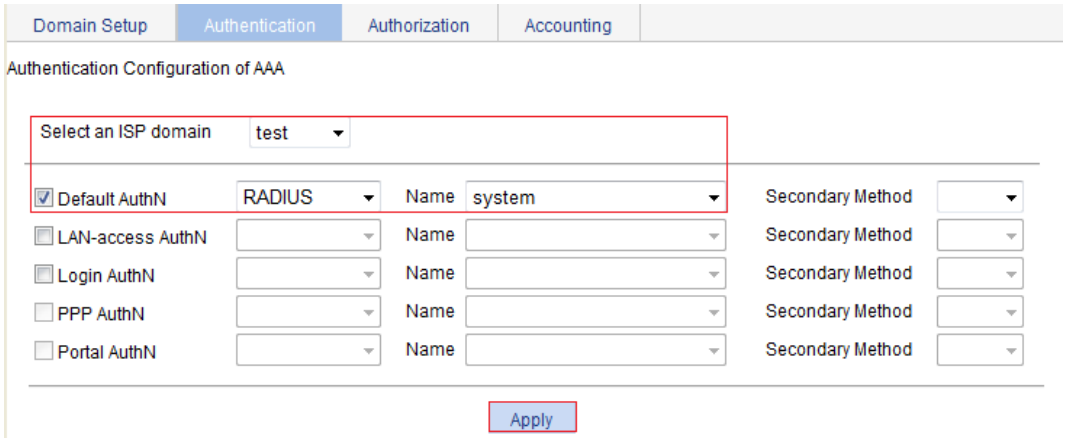
      The **Domain Setup** page appears.
   b. Select **test** from the **Domain Name** list, and select **Enable** from the **Default Domain** list.
   c. Click **Apply**.

Figure 330 Creating an ISP domain



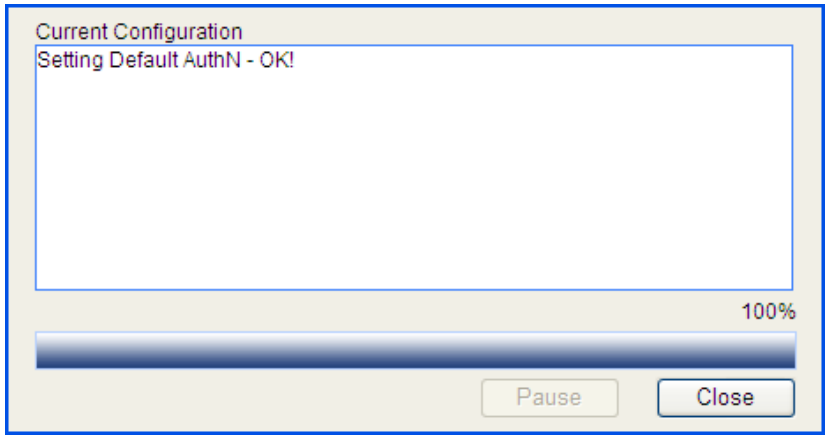
2. Configure AAA authentication method for the ISP domain:
   a. Click the **Authentication** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Default AuthN**, select authentication method **RADIUS** from the **Default AuthN** list, and select the authentication scheme **system** from the **Name** list, as shown in Figure 331.

Figure 331 Configuring AAA authentication method for the ISP domain



   d. Click **Apply**.
   A configuration progress dialog box appears, as shown in Figure 332.

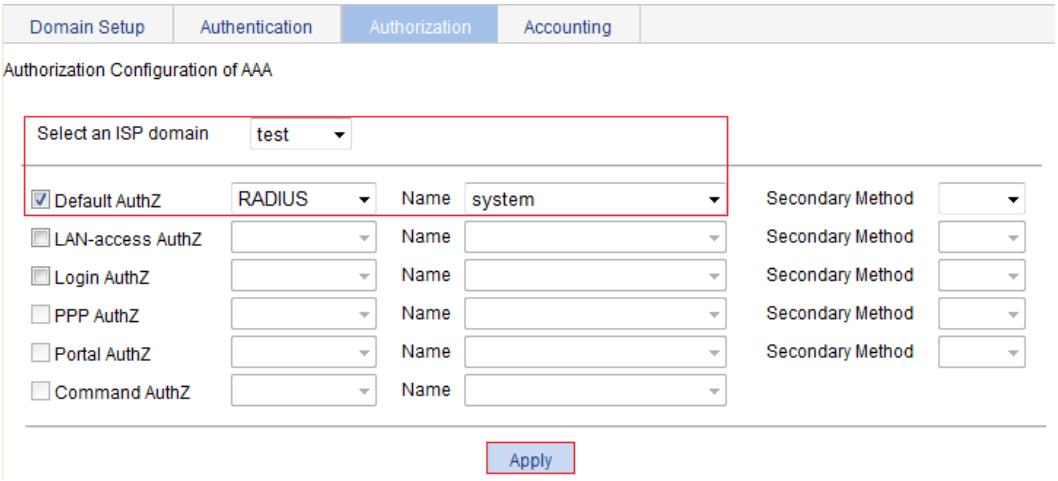
Figure 332 Configuration progress dialog box



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

3. Configure AAA authorization method for the ISP domain:
   a. Click the **Authorization** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Default AuthZ**, select the authorization method **RADIUS** from the **Default AuthZ** list, and select the authorization scheme **system** from the **Name** list, as shown in Figure 333.

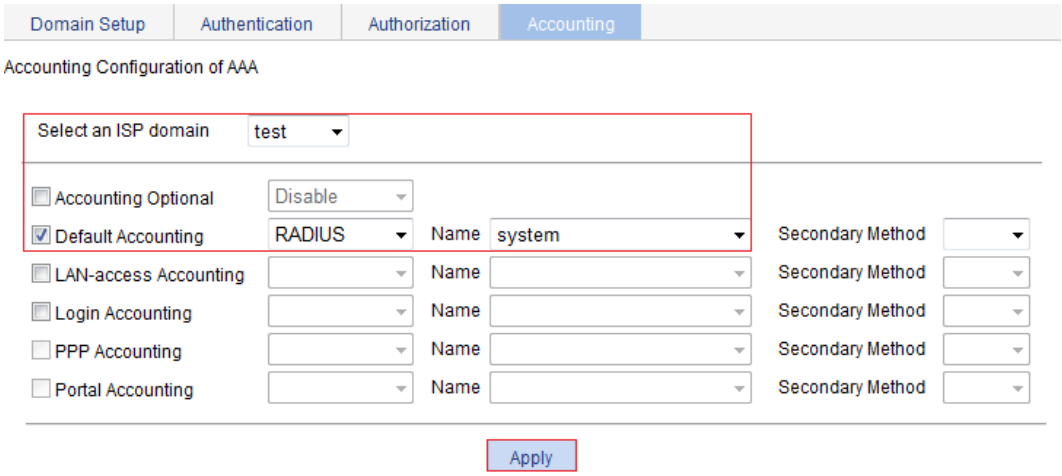
Figure 333 Configuring the AAA authorization method for the ISP domain



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

4. Configure AAA accounting method for the ISP domain:
   a. Click the **Accounting** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Default Accounting**, select the accounting method **RADIUS** as the default accounting method, and select the accounting scheme **system** from the **Name** list, as shown in Figure 334.

Figure 334 Configuring the AAA accounting method for the ISP domain



d. Click **Apply**.

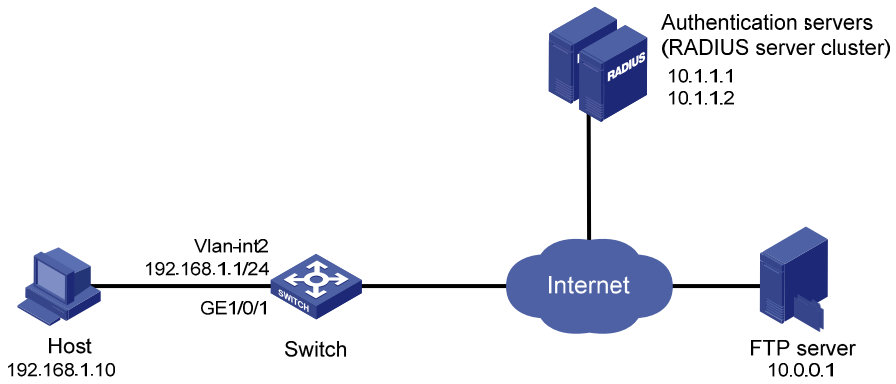
e. After the configuration process is complete, click **Close**.

802.X with ACL assignment configuration example

Network requirements

As shown in Figure 335, perform 802.1X authentication on port GigabitEthernet 1/0/1. 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 335 Network diagram



Configuring IP addresses

Assign an IP address to each interface as shown in Figure 335. (Details not shown.)

Configuring a RADIUS scheme

1. Create a RADIUS scheme:

a. From the navigation tree, select **Authentication** > **RADIUS**, and then click **Add**.

b. Enter the scheme name **system**.

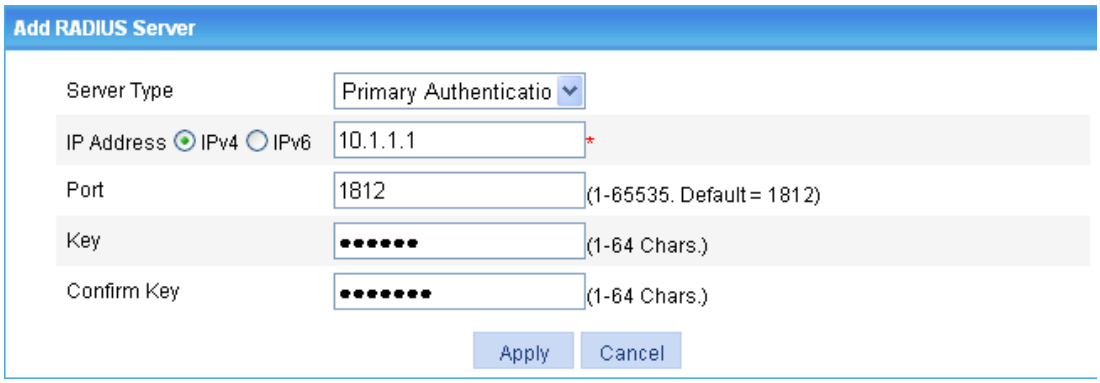
c. Select the server type **Extended**.

d. Select **Without domain name** from the **Username Format** list.

e. Click **Apply**.

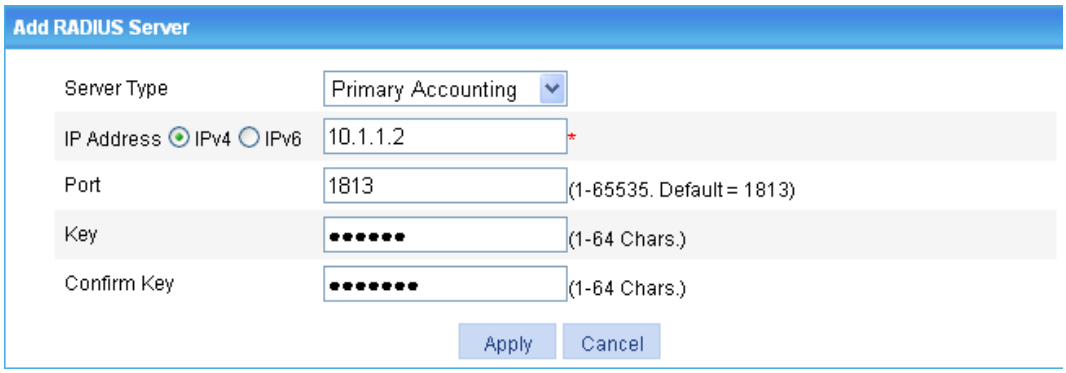
2. Configure the primary authentication server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Primary Authentication**.
   c. Enter the IP address **10.1.1.1**, and enter the port number **1812**.
   d. Enter **expert** in the **Key** and **Confirm Key** fields.
   e. Click **Apply**.

Figure 336 Configuring the RADIUS authentication server



3. Configure the primary accounting server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Select the server type **Primary Accounting**.
   c. Enter the IP address **10.1.1.2**, and enter the port number **1813**.
   d. Enter **expert** in the **Key** and **Confirm Key** fields.

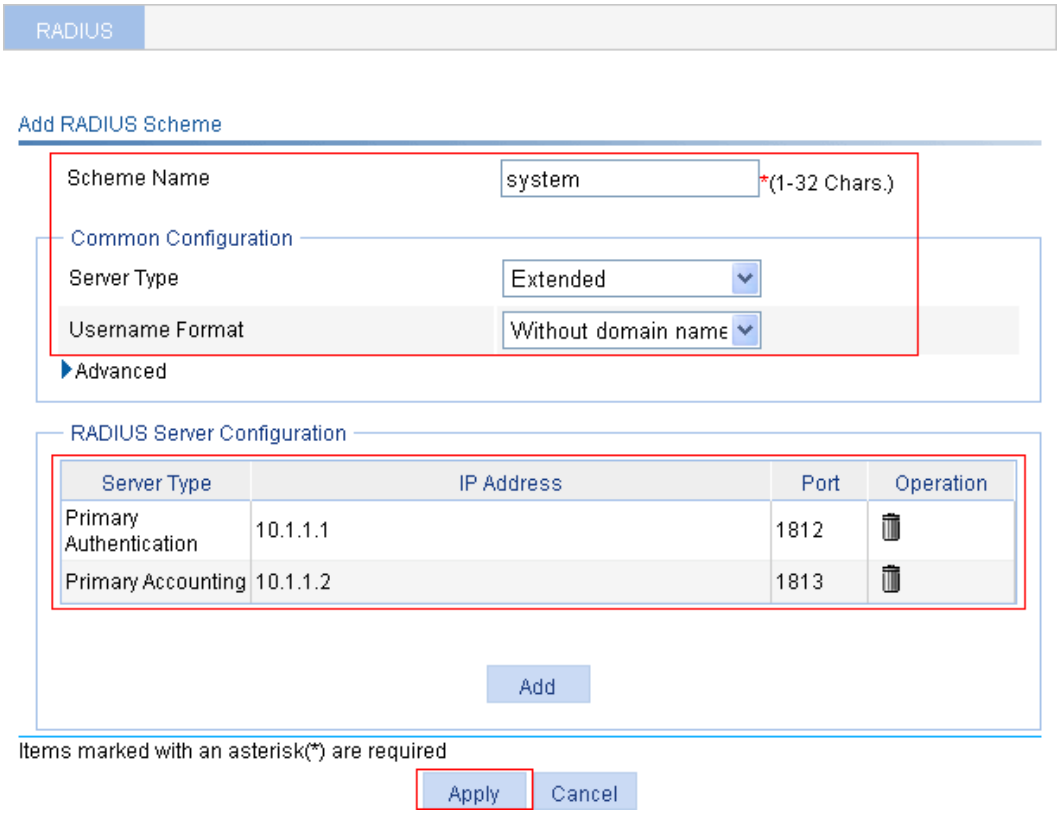
Figure 337 Configuring the RADIUS accounting server



   e. Click **Apply**.

   The **RADIUS Server Configuration** area displays the accounting server you have configured, as shown in Figure 338.

Figure 338 Configuring the RADIUS scheme

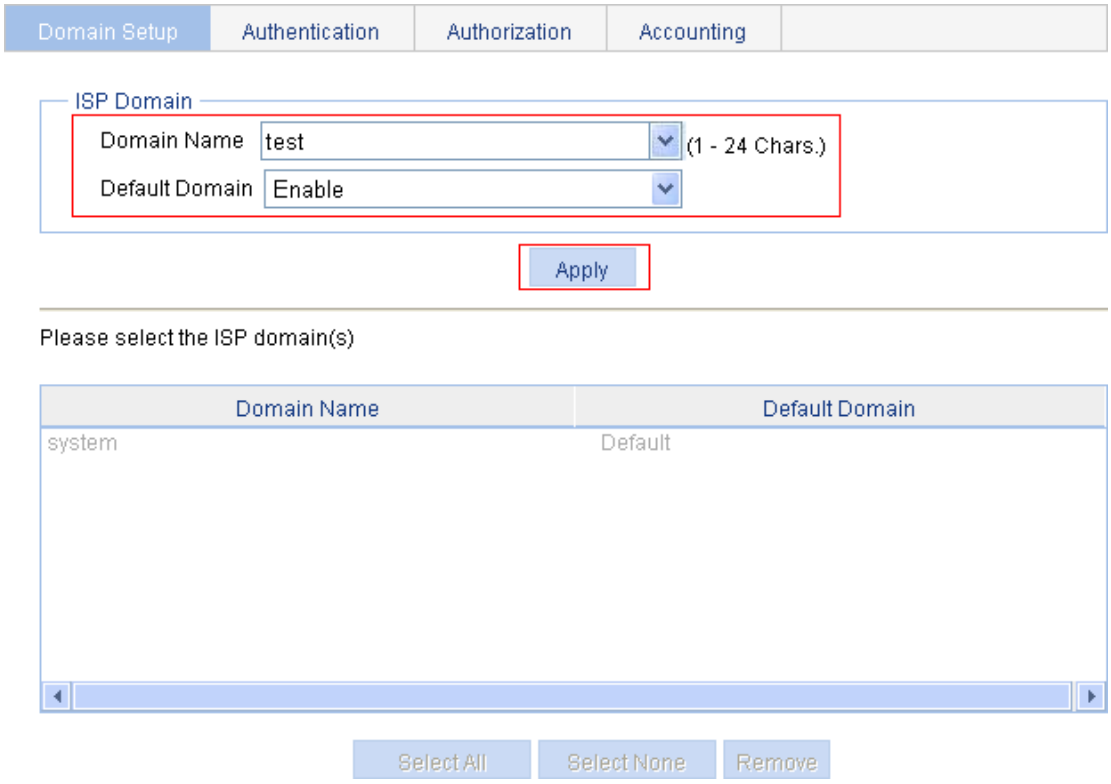


4. Click **Apply**.

Configuring AAA

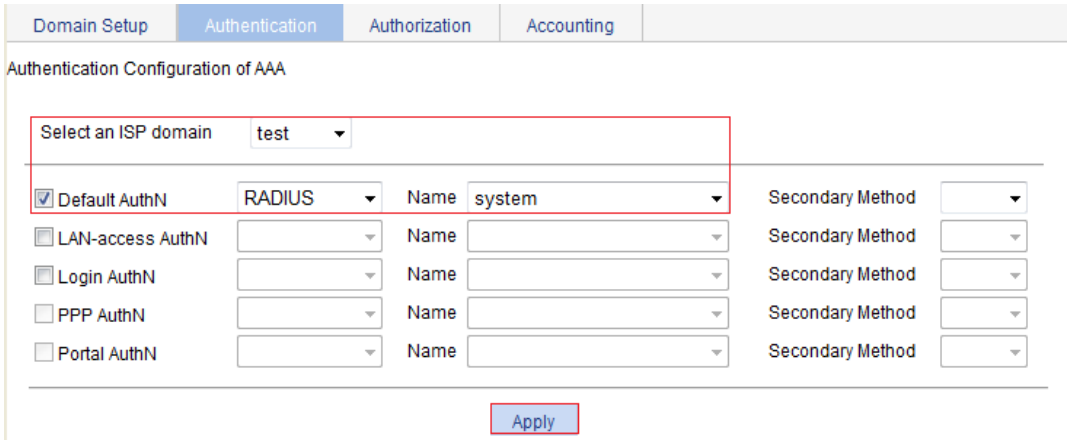
1. Create an ISP domain:
   a. From the navigation tree, select **Authentication** > **AAA**.
      The **Domain Setup** page appears.
   b. Enter **test** from the **Domain Name** list, and select **Enable** from the **Default Domain** list.
   c. Click **Apply**.

Figure 339 Creating an ISP domain



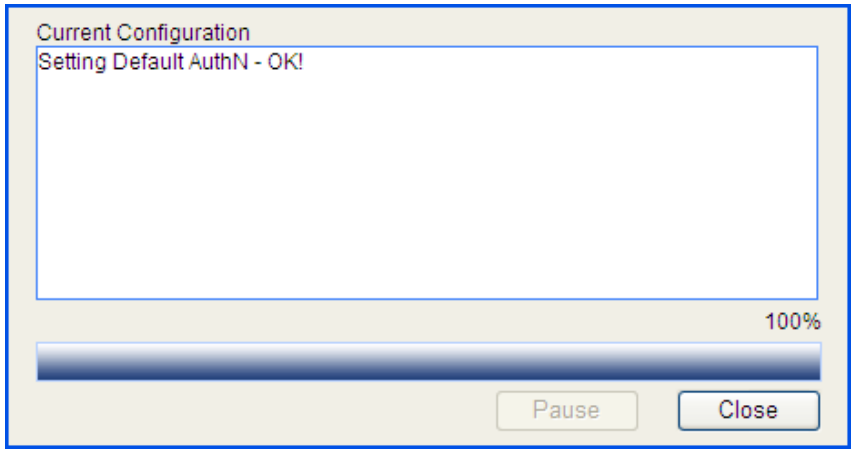
2. Configure AAA authentication method for the ISP domain:
   a. Click the **Authentication** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Default AuthN**, select **RADIUS** as the default authentication method, and select the authentication scheme **system** from the **Name** list, as shown in Figure 340.

Figure 340 Configuring the AAA authentication method for the ISP domain



   d. Click **Apply**.
   A configuration progress dialog box appears, as shown in Figure 341.

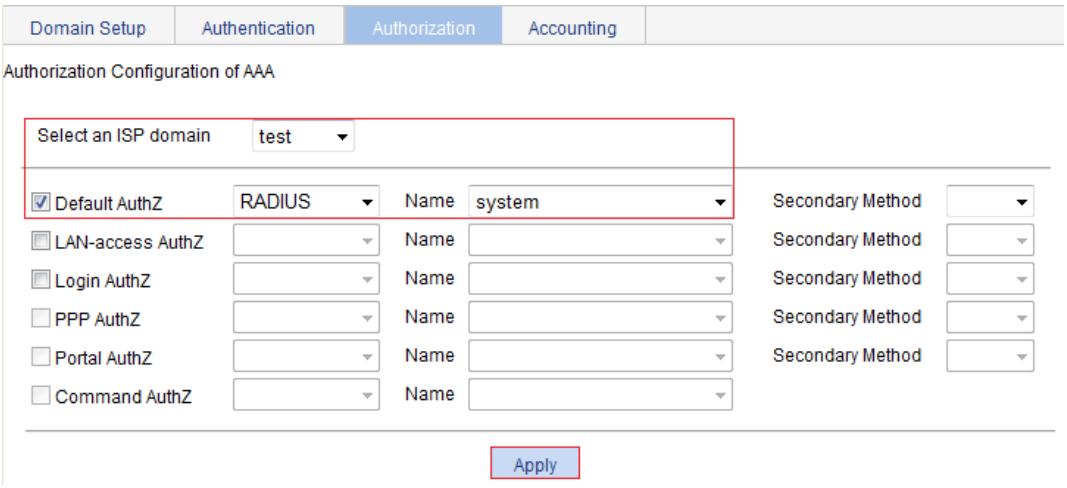
Figure 341 Configuration progress dialog box



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

3. Configure AAA authorization method for the ISP domain:
   a. Click the **Authorization** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Default AuthZ**, select **RADIUS** as the default authorization method, and select the authorization scheme **system** from the **Name** list, as shown in Figure 342.

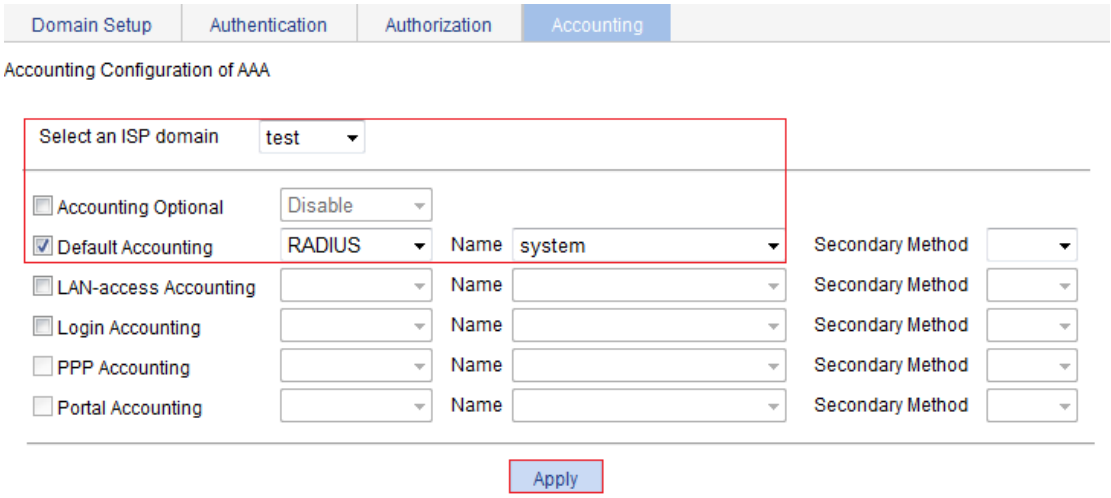
Figure 342 Configuring the AAA authorization method for the ISP domain



   d. Click **Apply**.
   e. After the configuration process is complete, click **Close**.

4. Configure AAA accounting method for the ISP domain:
   a. Click the **Accounting** tab.
   b. Select **test** from the **Select an ISP domain** list.
   c. Select **Accounting Optional** and select **Enable** from the list.
   d. Select **Default Accounting**, select the accounting method **RADIUS**, and select the accounting scheme **system** from the **Name** list.
   e. Click **Apply**.

Figure 343 Configuring the AAA accounting method for the ISP domain

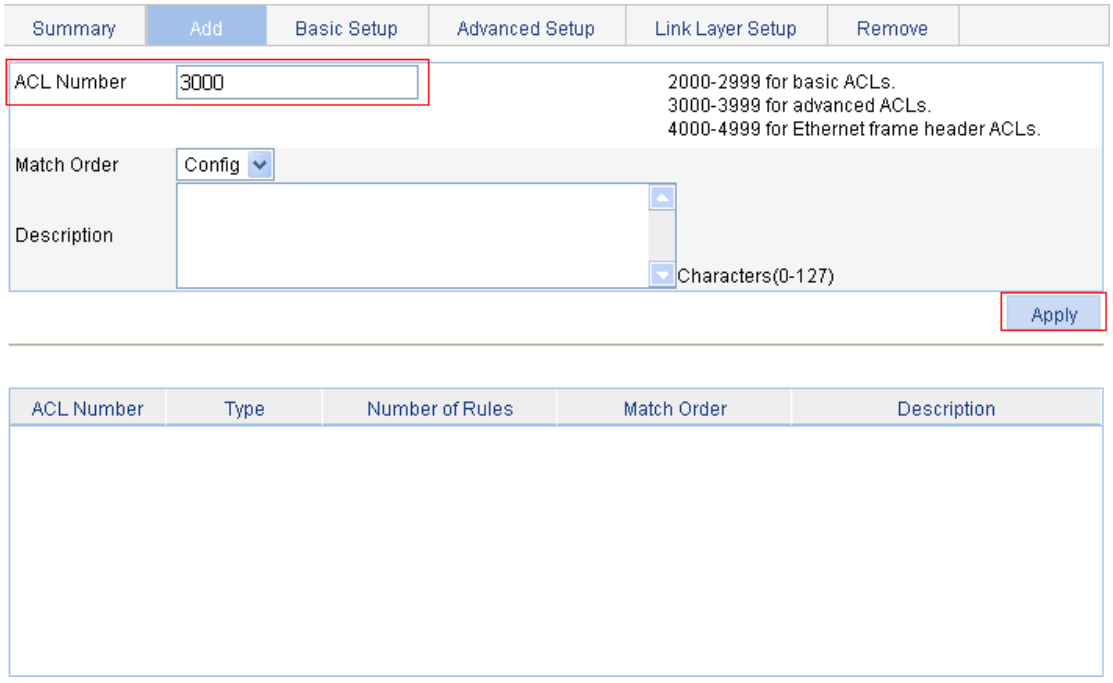


f. After the configuration process is complete, click **Close**.

Configuring an ACL

1. From the navigation tree, select **QoS** > **ACL IPv4**.
2. Click the **Add** tab.
3. Enter the ACL number **3000**, and click **Apply**.

Figure 344 Creating ACL 3000

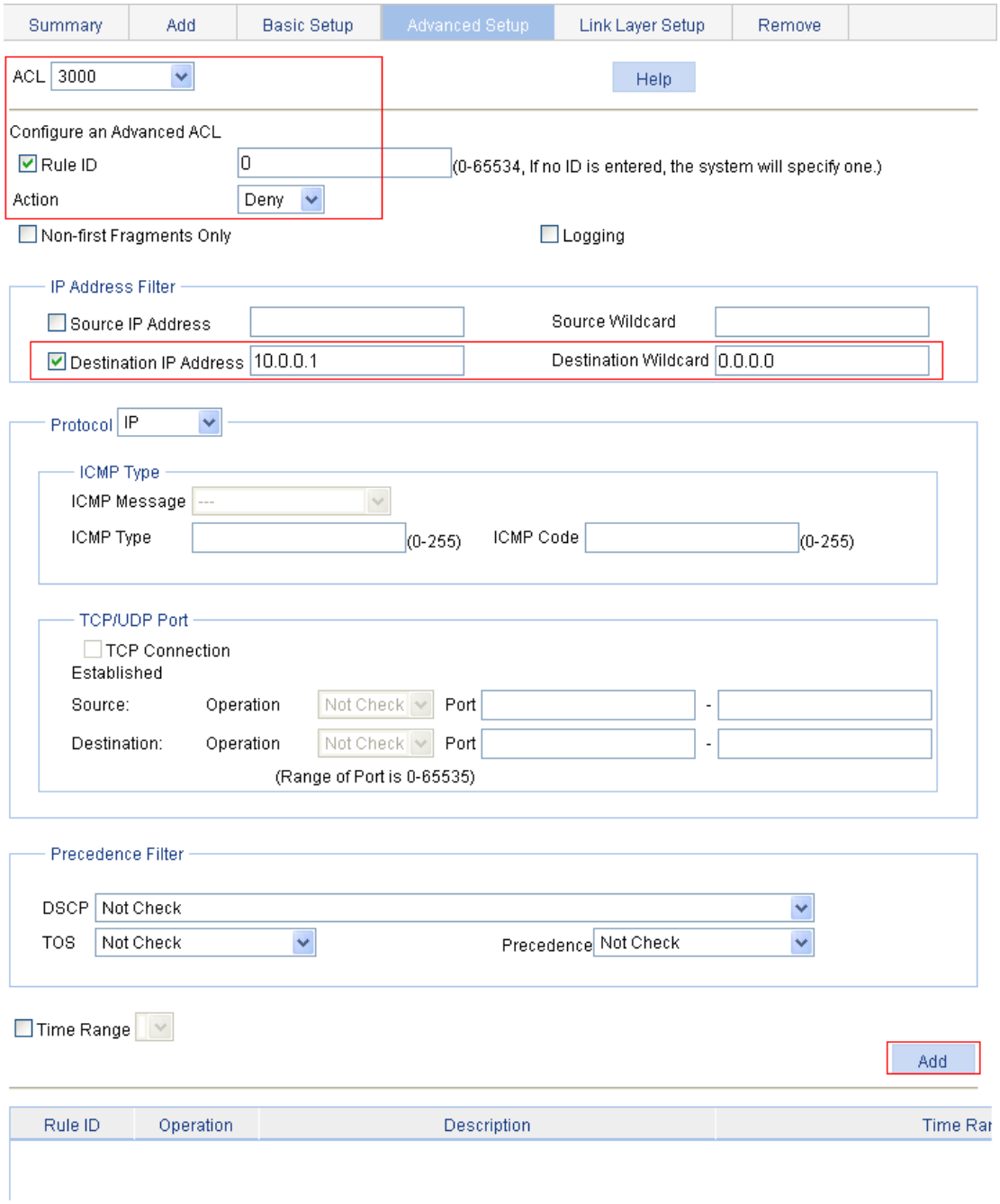


4. Click the **Advanced Setup** tab.
5. Configure the following parameters:
   a. Select **3000** from the **ACL** list.
   b. Select **Rule ID**, enter the rule ID **0**, and select the action **Deny**.
   c. In the **IP Address Filter** area, select **Destination IP Address**:
      – Enter **10.0.0.1** as the destination IP address.

– Enter **0.0.0.0** as the destination IP address wildcard.

d. Click **Add**.

Figure 345 ACL rule configuration



Configuring 802.1X

1. Configure 802.1X globally:

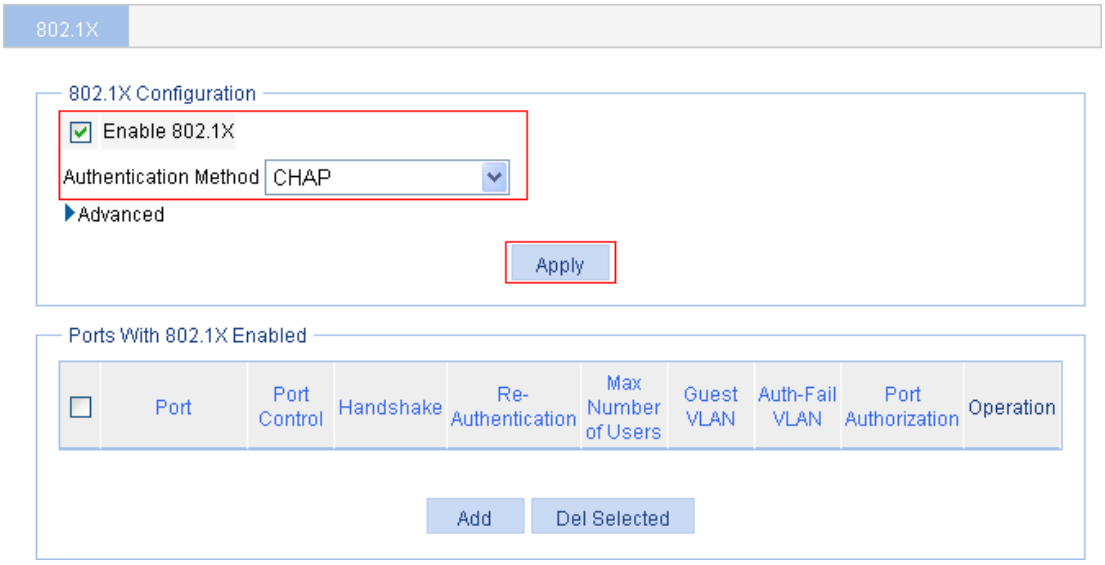
a. From the navigation tree, select **Authentication** > **802.1X**.

b. Select **Enable 802.1X**.

c. Select the authentication method **CHAP**.

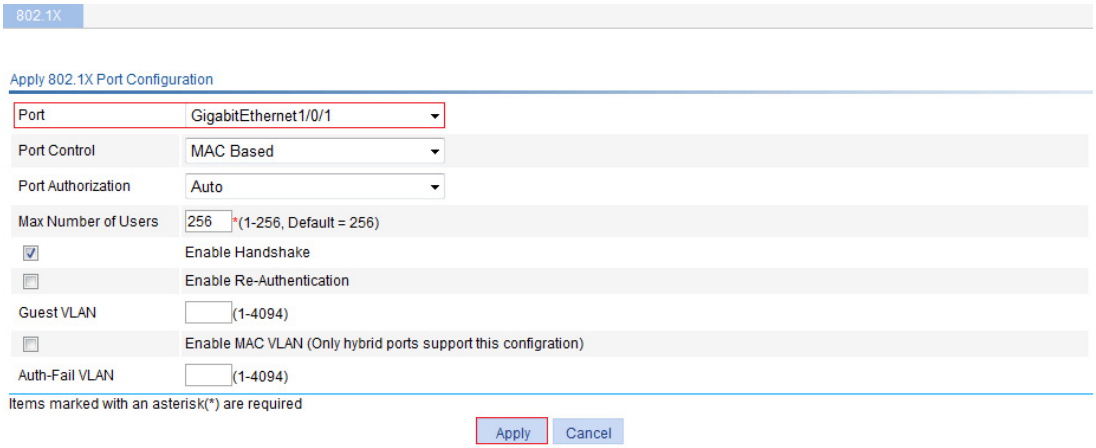
d. Click **Apply**.

Figure 346 Configuring 802.1X globally



2. Configure 802.1X for GigabitEthernet 1/0/1:
   a. In the **Ports With 802.1X Enabled** area, click **Add**.
   b. Select **GigabitEthernet1/0/1** from the **Port** list.
   c. Click **Apply**.

Figure 347 Configuring 802.1X for 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**.
   Figure 348 shows the ping operation summary.

Figure 348 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

Overview

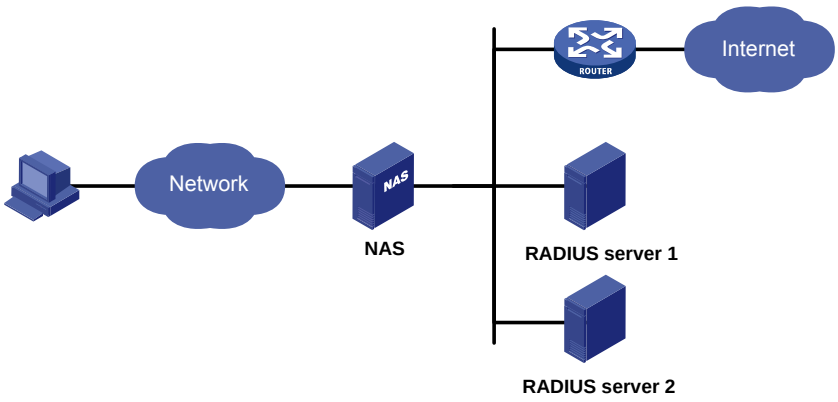
Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. It provides the following security functions:

- **Authentication**—Identifies users and determines whether a user is valid.
- **Authorization**—Grants user rights and controls user access to resources and services. For example, a user who has successfully logged in to the device can be granted read and print permissions to the files on the device.
- **Accounting**—Records all network service usage information, including service type, start time, and traffic. The accounting function provides information required for charging, and allows for network security surveillance.

AAA application

AAA typically uses a client/server model, as shown in Figure 349. The client runs on the network access server (NAS), which is also called the access device. The server maintains user information centrally. In an AAA network, the NAS is a server for users but a client for AAA servers.

Figure 349 AAA application scenario



The NAS uses the authentication server to authenticate any user who tries to log in, use network resources, or access other networks. The NAS transparently transmits authentication, authorization, and accounting information between the user and the servers. The RADIUS protocol defines how a NAS and a remote server exchange user information.

The network shown in Figure 349 contains two RADIUS servers. You can choose different servers to implement different security functions. For example, you can use RADIUS server 1 for authentication and authorization, and RADIUS server 2 for accounting.

You can implement any of the three security functions provided by AAA as needed. For example, if your company wants employees to be authenticated before they access specific resources, configure an authentication server. If network usage information is needed, you must also configure an accounting server.

AAA can be implemented through multiple protocols. The device supports RADIUS, which is most often used. For more information about RADIUS, see "Configuring RADIUS."

Domain-based user management

A NAS manages users based on ISP domains. On a NAS, each user belongs to one ISP domain. A NAS determines the ISP domain for a user by the username entered by the user at login. For a username in the *userid@isp-name* format, the access device considers the *userid* part the username for authentication and the *isp-name* part the ISP domain name.

In a networking scenario with multiple ISPs, a NAS can connect users of different ISPs. Different ISP users can have different user attributes (such as username and password structure), different service type, and different rights. To manage these ISP users, you need to create ISP domains and then configure AAA methods and domain attributes for each ISP domain

On the NAS, each user belongs to an ISP domain. If a user provides no ISP domain name at login, the NAS considers the user belongs to the default ISP domain.

AAA allows you to manage users based on their access types:

- **LAN users**—Users on a LAN who must pass 802.1X or MAC address authentication to access the network.
- **Login users**—Users who want to log in to the device, including SSH users, Telnet users, Web users, FTP users, and terminal users.

In addition, AAA provides command authorization for login users to improve device security. Command authentication enables the NAS to defer to the authorization server to determine whether a command entered by a login user is permitted for the user, and allows login users to execute only authorized commands.

Configuration prerequisites

To deploy local authentication, configure local users on the access device. See "Configuring users."

To deploy remote authentication, authorization, or accounting, configure the RADIUS schemes to be referenced. See "Configuring RADIUS."

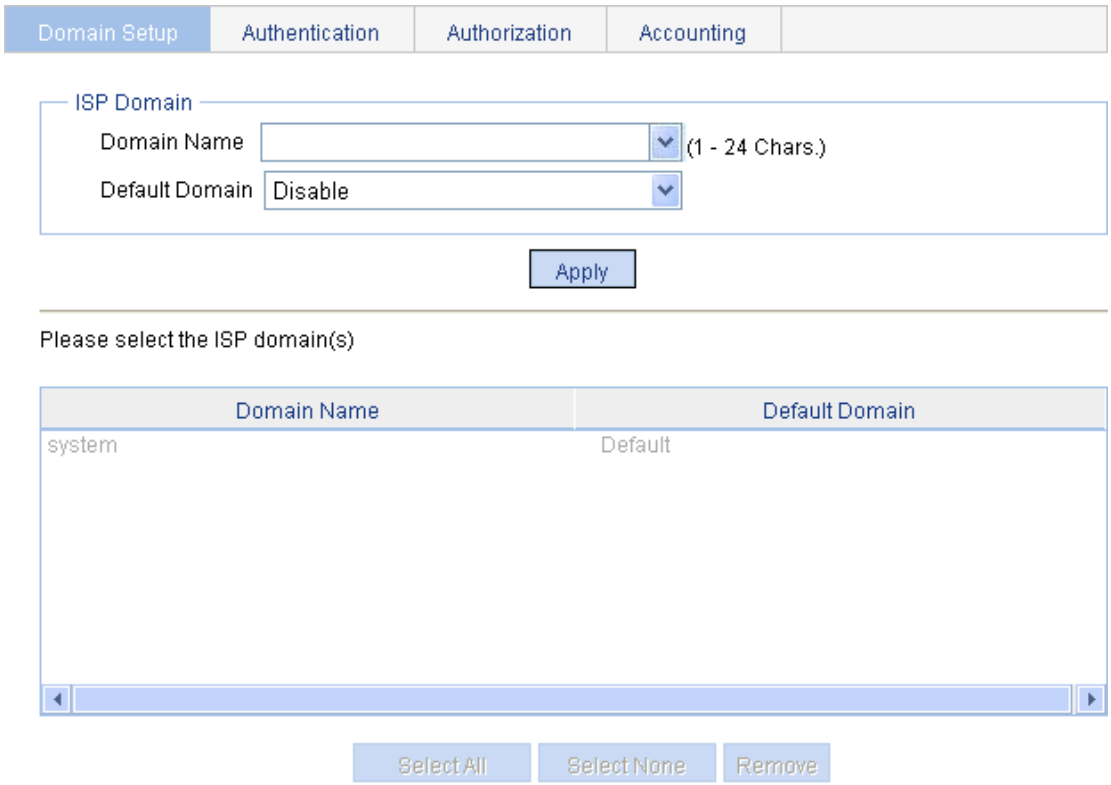
Recommended configuration procedure

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.
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	Required. 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 350 Domain Setup page



2. Create an ISP domain, as described in Table 110.
3. Click **Apply**.

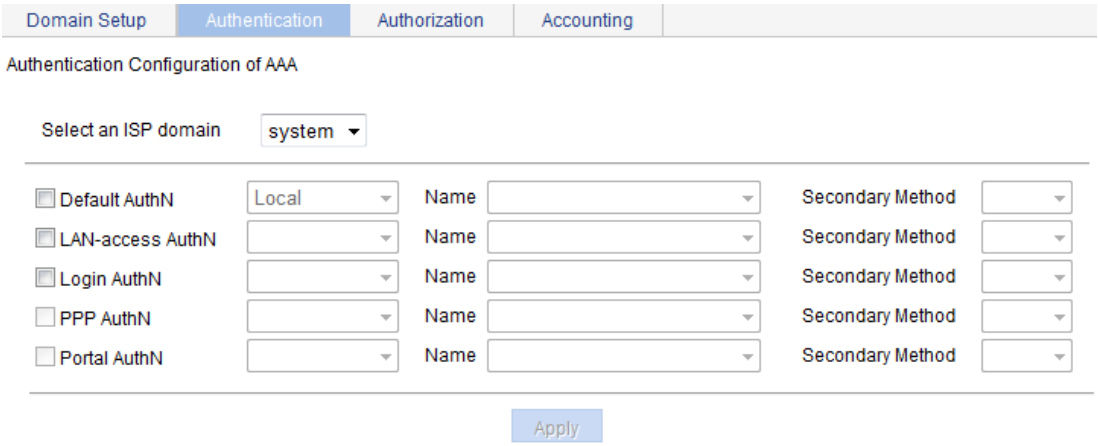
Table 110 Configuration items

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).
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 another 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 351 Authentication method configuration page



3. Select the ISP domain and specify authentication methods for the domain, as described in Table 111.
4. Click **Apply**.

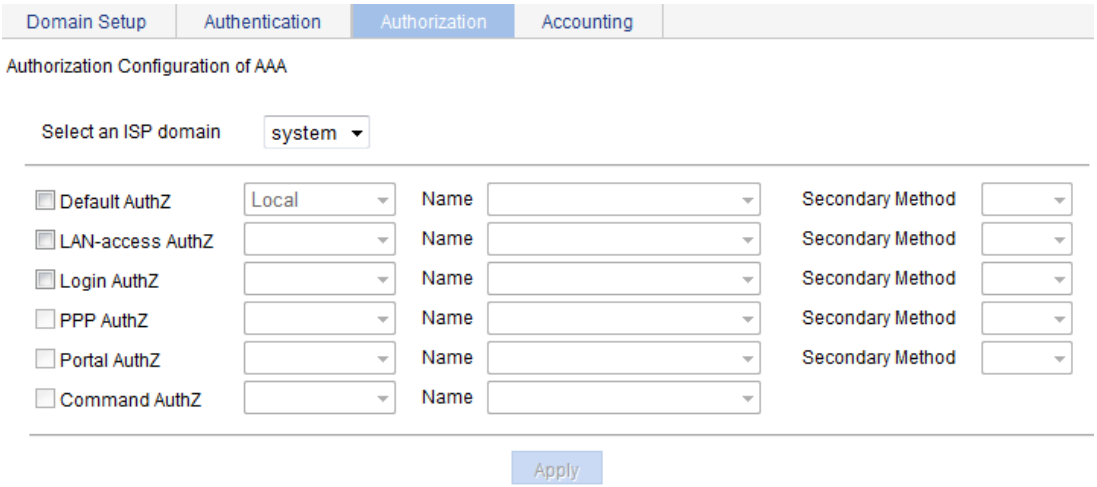
Table 111 Configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthN Name Secondary Method	Configure the default authentication method and secondary authentication method for all types of users. Options include: • **HWTACACS**—HWTACACS authentication. You must specify the HWTACACS scheme to be used. • **Local**—Local authentication. • **None**—No authentication. This method trusts all users and is not for general use. • **RADIUS**—RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the default authentication setting, which is local authentication.
LAN-access AuthN Name Secondary Method	Configure the authentication method and secondary authentication method for LAN access users. Options include: • **Local**—Local authentication. • **None**—No authentication. This method trusts all users and is not for general use. • **RADIUS**—RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default AuthN** area for LAN access users.
Login AuthN Name Secondary Method	Configure the authentication method and secondary authentication method for login users. Options include: • **HWTACACS**—HWTACACS authentication. You must specify the HWTACACS scheme to be used. • **Local**—Local authentication. • **None**—No authentication. This method trusts all users and is not for general use. • **RADIUS**—RADIUS authentication. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default AuthN** area for login users.

Configuring authorization methods for the ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
2. Click the **Authorization** tab.

Figure 352 Authorization method configuration page



3. Select the ISP domain and specify authorization methods for the ISP domain, as described in Table 112.
4. Click **Apply**.

Table 112 Configuration items

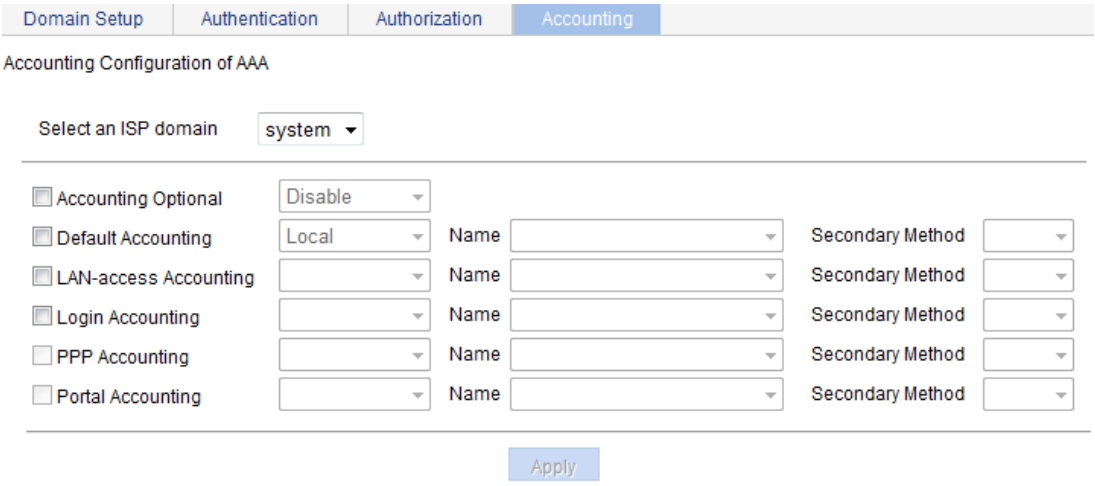
Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthZ Name Secondary Method	Configure the default authorization method and secondary authorization method for all types of users. Options include: • **HWTACACS**—HWTACACS authorization. You must specify the HWTACACS scheme to be used. • **Local**—Local authorization. • **None**—This method trusts all users and assigns default rights to them. • **RADIUS**—RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the default authorization setting, which is local authorization.
LAN-access AuthZ Name Secondary Method	Configure the authorization method and secondary authorization method for LAN access users. Options include: • **Local**—Local authorization. • **None**—This method trusts all users and assigns default rights to them. • **RADIUS**—RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default AuthZ** area for LAN access users.

Item	Description
Login AuthZ Name Secondary Method	Configure the authorization method and secondary authorization method for login users. Options include: • **HWTACACS**—HWTACACS authorization. You must specify the HWTACACS scheme to be used. • **Local**—Local authorization. • **None**—This method trusts all users and assigns default rights to them. • **RADIUS**—RADIUS authorization. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default AuthZ** area for login users.

Configuring accounting methods for the ISP domain

1. Select **Authentication** > **AAA** from the navigation tree.
2. Click the **Accounting** tab.

Figure 353 Accounting method configuration page



3. Select the ISP domain and specify accounting methods for the ISP domain, as described in Table 113.
4. Click **Apply**.

Table 113 Configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Accounting Optional	Specify whether to enable the accounting optional feature. The feature enables a user who would otherwise be disconnected to use network resources even if there is no accounting server available or communication with the current accounting server fails. If accounting for the user fails, the device no longer sends real-time accounting updates for the user.

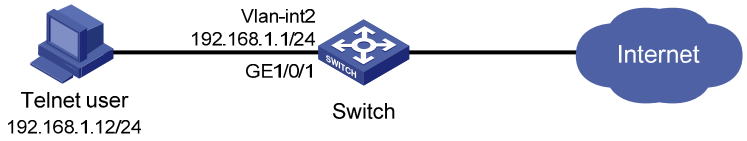
Item	Description
Default Accounting Name Secondary Method	Configure the default accounting method and secondary accounting method for all types of users. Options include: • **HWTACACS**—HWTACACS accounting. You must specify the HWTACACS scheme to be used. • **Local**—Local accounting. • **None**—No accounting. • **RADIUS**—RADIUS accounting. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the default accounting setting, which is local accounting.
LAN-access Accounting Name Secondary Method	Configure the accounting method and secondary accounting method for LAN access users. Options include: • **Local**—Local accounting. • **None**—No accounting. • **RADIUS**—RADIUS accounting. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default Accounting** area for LAN access users.
Login Accounting Name Secondary Method	Configure the accounting method and secondary accounting method for login users. Options include: • **HWTACACS**—HWTACACS accounting. You must specify the HWTACACS scheme to be used. • **Local**—Local accounting. • **None**—No accounting. • **RADIUS**—RADIUS accounting. You must specify the RADIUS scheme to be used. • **Not Set**—The device uses the settings in the **Default Accounting** area for login users.

AAA configuration example

Network requirements

As shown in Figure 354, configure the switch to perform local authentication, authorization, and accounting for Telnet users.

Figure 354 Network diagram

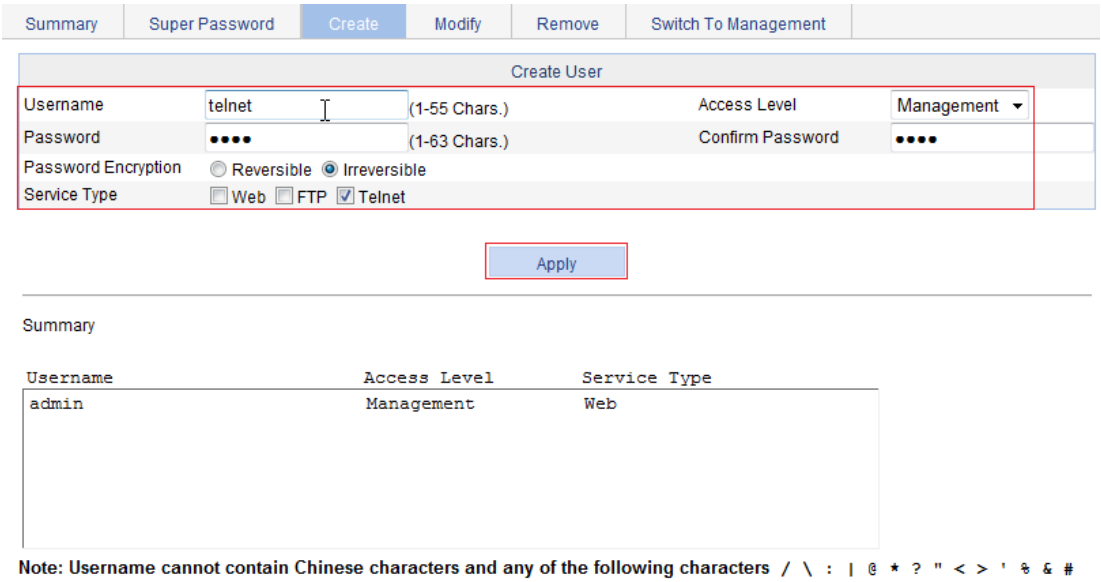


Configuration procedure

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:

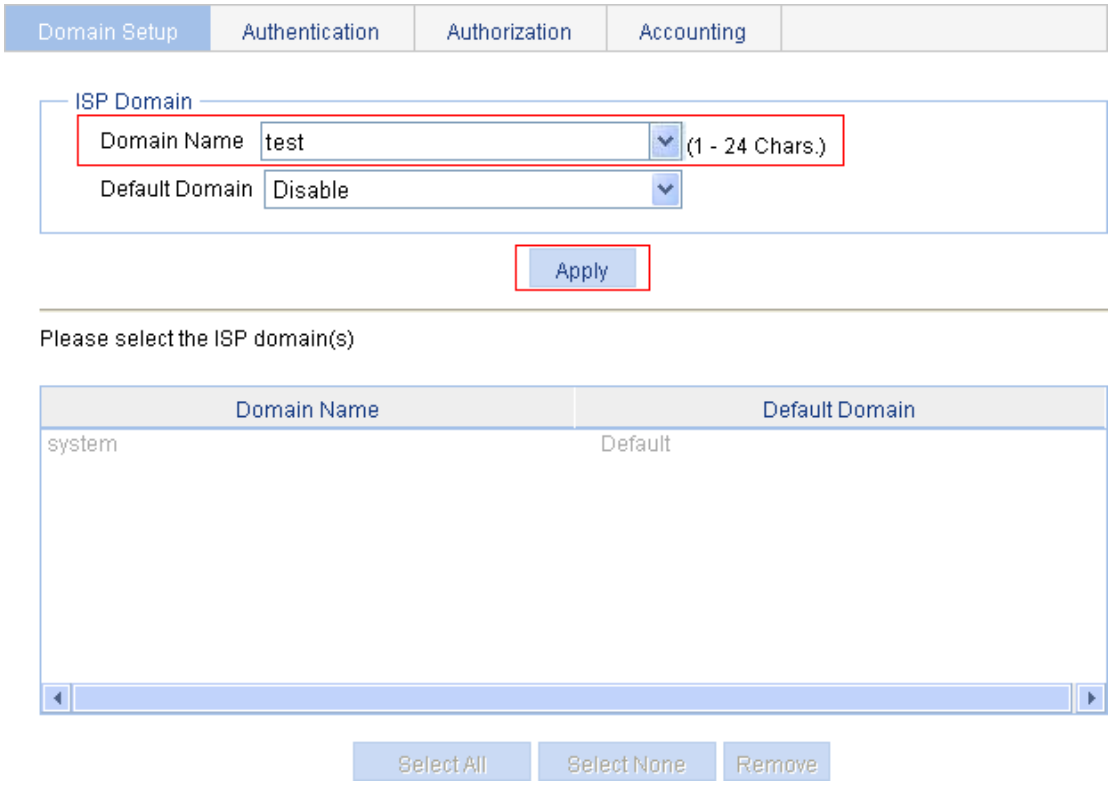
a. Select **Device** > **Users** from the navigation tree.
b. Click the **Create** tab.
c. Enter the username **telnet**.
d. Select the access level **Management**.
e. Enter the password **abcd** and confirm the password.
f. Select the password encryption method **Irreversible**.
g. Select the service type **Telnet Service**.
h. Click **Apply**.

Figure 355 Configuring a local user



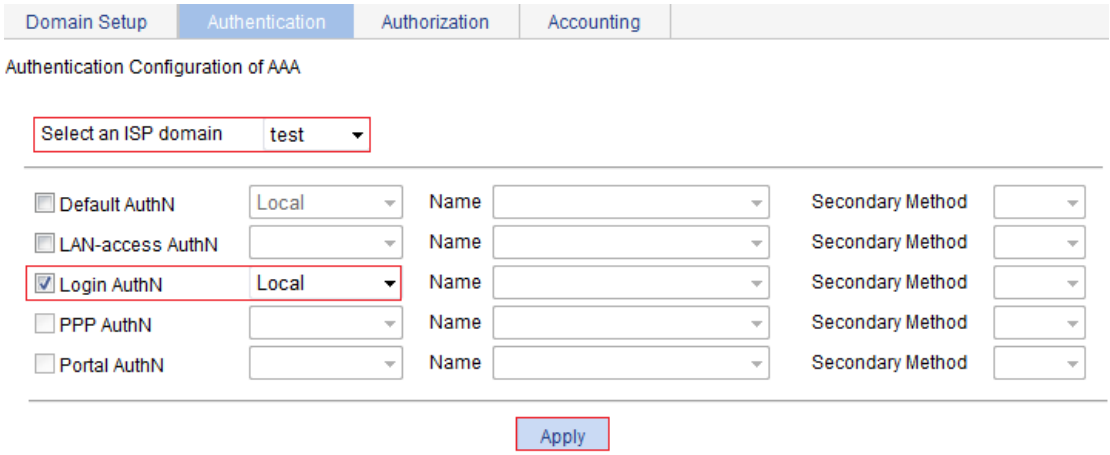
4. Configure ISP domain **test**:
   a. Select **Authentication** > **AAA** from the navigation tree.
      The domain configuration page appears.
   b. Enter the domain name **test**.
   c. Click **Apply**.

Figure 356 Configuring ISP domain test



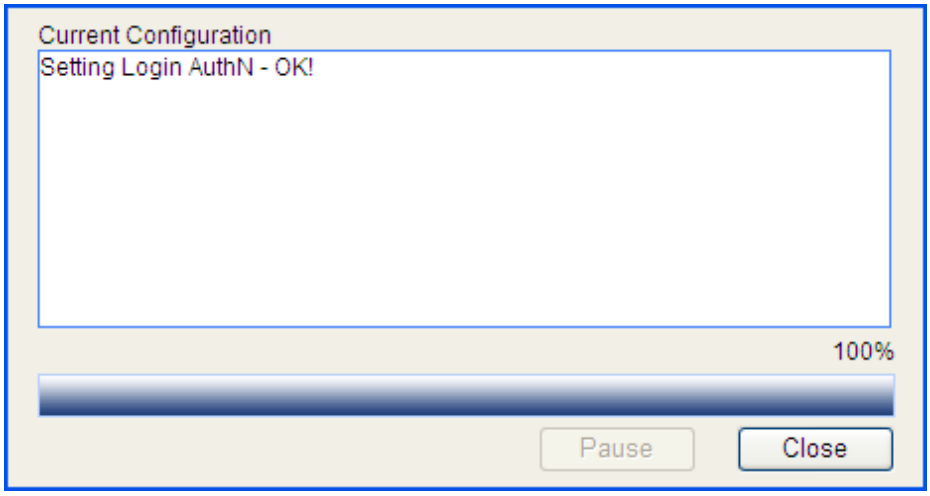
5. Configure the ISP domain to use local authentication:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. Click the **Authentication** tab.
   c. Select the domain **test**.
   d. Select **Login AuthN** and select the authentication method **Local**.

Figure 357 Configuring the ISP domain to use local authentication



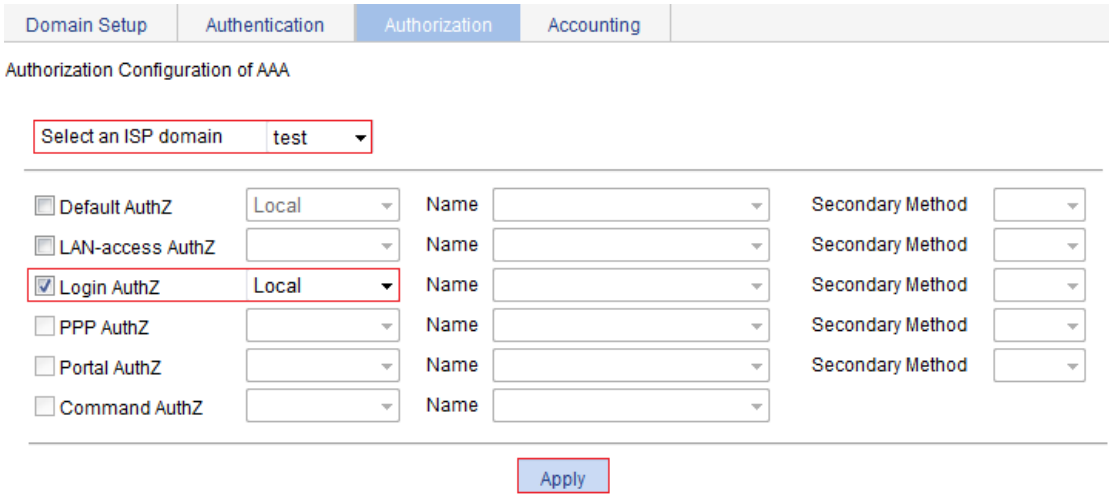
   e. Click **Apply**.
      A configuration progress dialog box appears, as shown in Figure 358.
   f. After the configuration process is complete, click **Close**.

Figure 358 Configuration progress dialog box



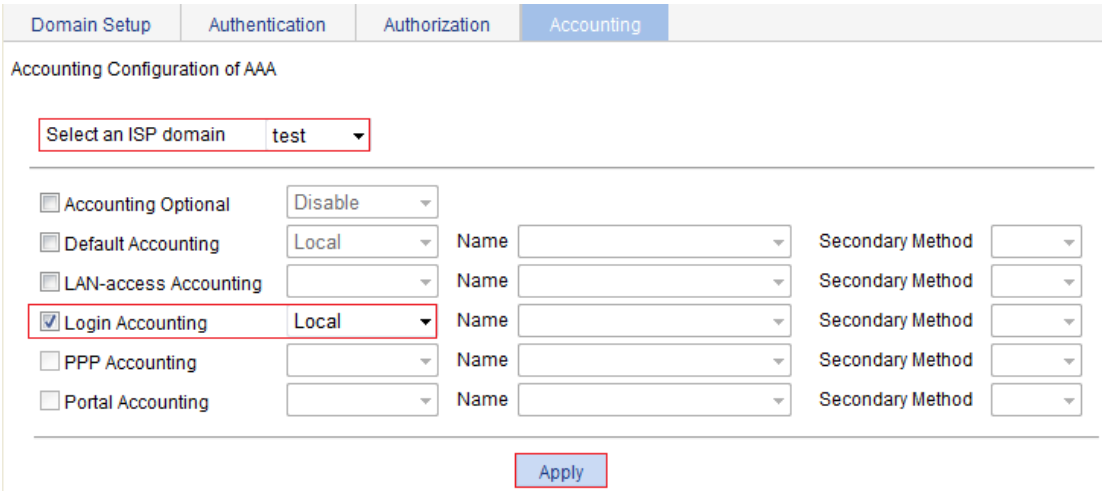
6. Configure the ISP domain to use local authorization:
   a. Select **Authentication** > **AAA** from the navigation tree.
   b. Click the **Authorization** tab.
   c. Select the domain **test**.
   d. Select **Login AuthZ** and select the authorization method **Local**.
   e. Click **Apply**.
      A configuration progress dialog box appears.
   f. After the configuration progress is complete, click **Close**.

Figure 359 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 360 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 will be serviced as a user in domain **test**.

Configuring RADIUS

Overview

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model to implement AAA. It can protect networks against unauthorized access and is often used in network environments that require both high security and remote user access. For more information about AAA, see "Configuring AAA."

RADIUS 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, including Ethernet and ADSL. RADIUS provides access authentication, authorization, and accounting services. The accounting function collects and records network resource usage information.

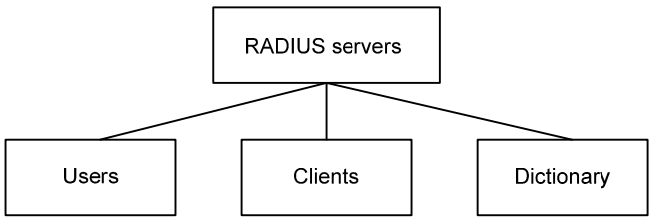
Client/server model

RADIUS clients run on NASs located throughout the network. NASs pass user information to RADIUS servers, and determine to reject or accept user access requests depending on the responses from RADIUS servers.

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 receives connection requests, authenticates users, and returns access control information (for example, rejecting or accepting the user access request) to the clients.

The RADIUS server typically maintains the following databases: Users, Clients, and Dictionary. See Figure 361.

Figure 361 RADIUS server databases



- **Users**—Stores user information such as 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

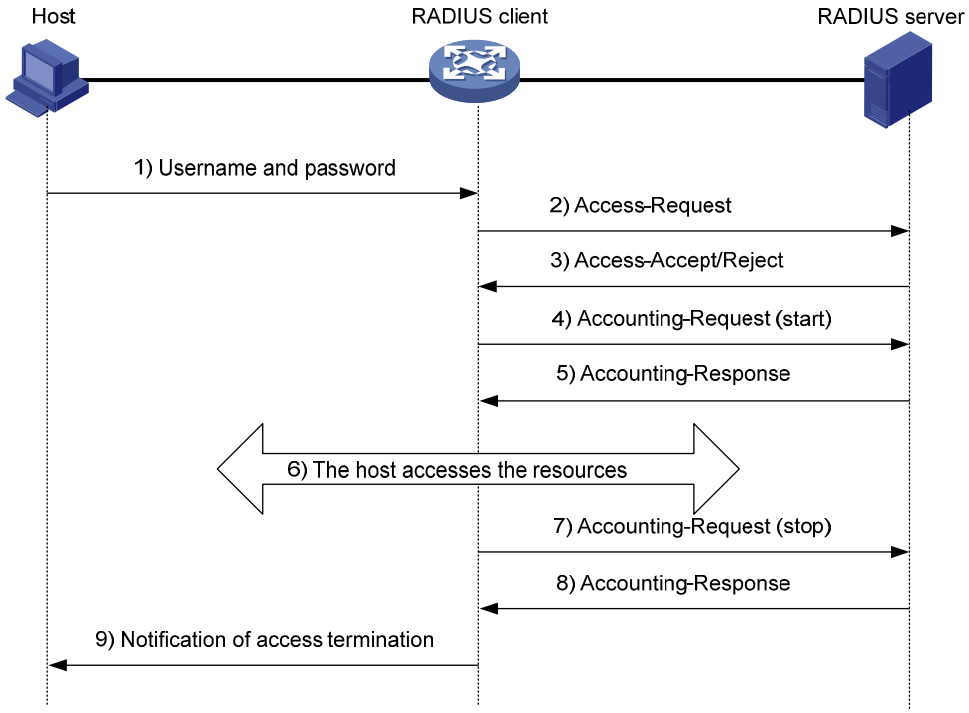
The RADIUS client and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords exchanged between them. For security, this key must be manually configured on the client and the server.

RADIUS servers support multiple authentication protocols, including PPP PAP and CHAP. A RADIUS server can act as the client of another AAA server to provide authentication proxy services.

Basic RADIUS message exchange process

Figure 362 illustrates the interactions between the host, the RADIUS client, and the RADIUS server.

Figure 362 Basic RADIUS message exchange process



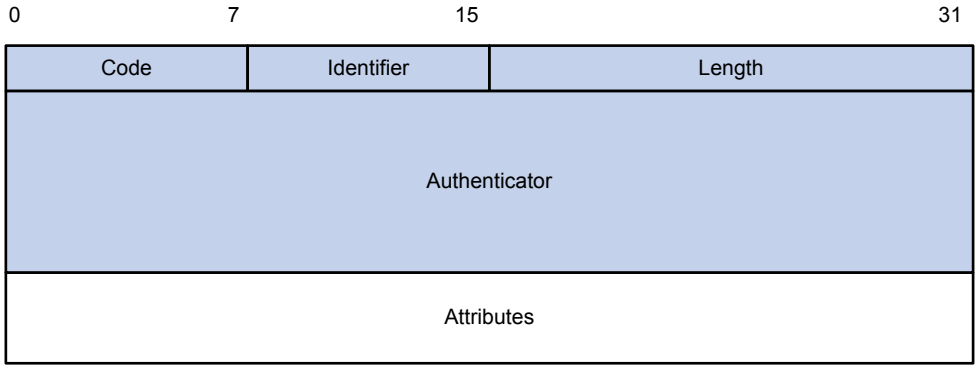
RADIUS operates in the following manner:

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 using the MD5 algorithm and the shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, the server returns 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 timer management mechanism, a retransmission mechanism, and a backup server mechanism. Figure 363 shows the RADIUS packet format.

Figure 363 RADIUS packet format



The following describes the fields of a RADIUS packet:

- The Code field (1 byte long) indicates the type of the RADIUS packet.

  Table 114 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 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 Attribute fields. Bytes beyond this length are considered padding and are neglected upon reception. 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 replies 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 1 to 255. Commonly used attributes for RADIUS authentication, authorization and accounting are listed in Table 115.

- **Length**—(1 byte long) Length of the attribute in bytes, including the Type, Length, and Value fields.
- **Value**—(Up to 253 bytes) Value of the attribute. Its format and content depend on the Type and Length fields.

Table 115 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
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

No.	Attribute	No.	Attribute
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

NOTE:

This table lists the attribute types, which are defined by RFC 2865, RFC 2866, RFC 2867, and RFC 2568.

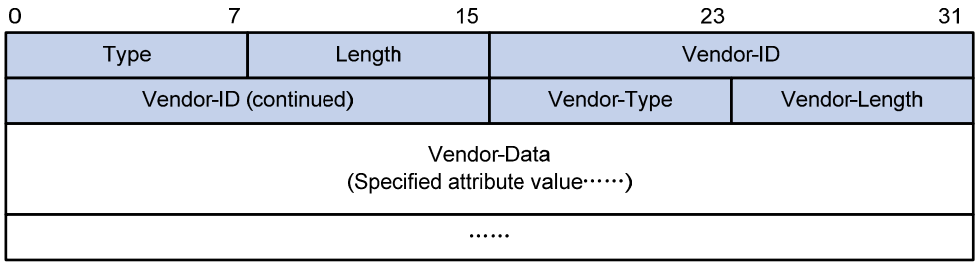
Extended RADIUS attributes

Attribute 26 (Vendor-Specific), an attribute defined by 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 as TLVs in attribute 26 to provide extended functions. As shown in Figure 364, a sub-attribute encapsulated in Attribute 26 consists of the following parts:

- **Vendor-ID**—ID of the vendor. Its most significant byte is 0. The other three bytes contains a code that is compliant to RFC 1700.
- **Vendor-Type**—Type of the sub-attribute.
- **Vendor-Length**—Length of the sub-attribute.
- **Vendor-Data**—Contents of the sub-attribute.

Figure 364 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*

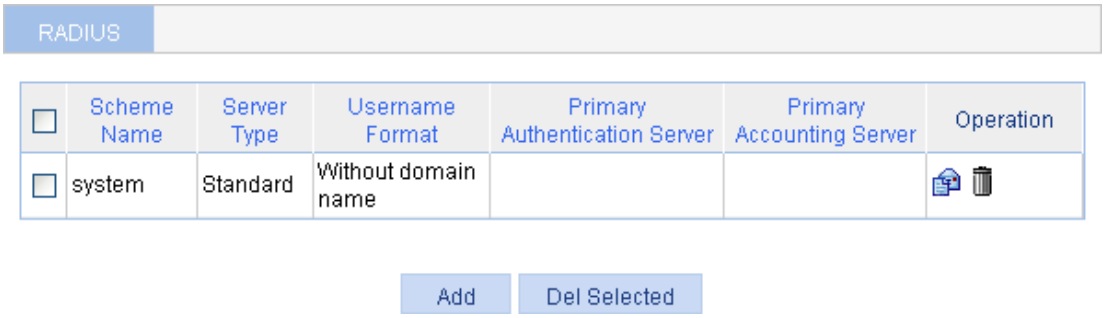
Configuring a RADIUS scheme

A RADIUS scheme defines a set of parameters that the device uses to exchange information with the RADIUS servers. There might be authentication servers and accounting servers, or primary servers and secondary servers. The parameters mainly include the IP addresses of the servers, the shared keys, and the RADIUS server type. By default, no RADIUS scheme exists.

To configure a RADIUS scheme:

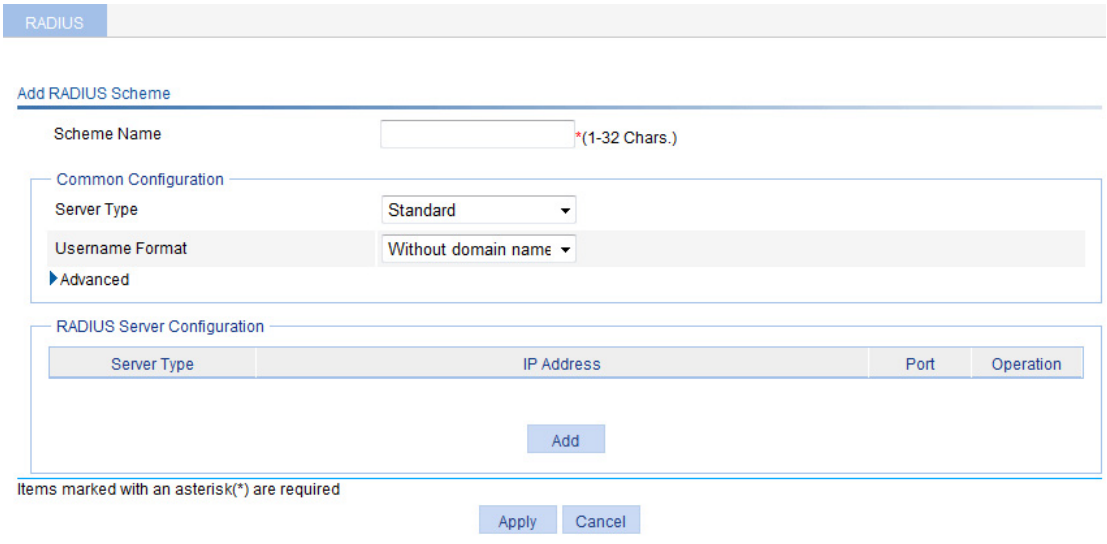
1. Select **Authentication** > **RADIUS** from the navigation tree.

   Figure 365 RADIUS scheme list

2. Click **Add**.

   Figure 366 RADIUS scheme configuration page

3. Configure the parameters as described in Table 116.
4. Click **Apply**.

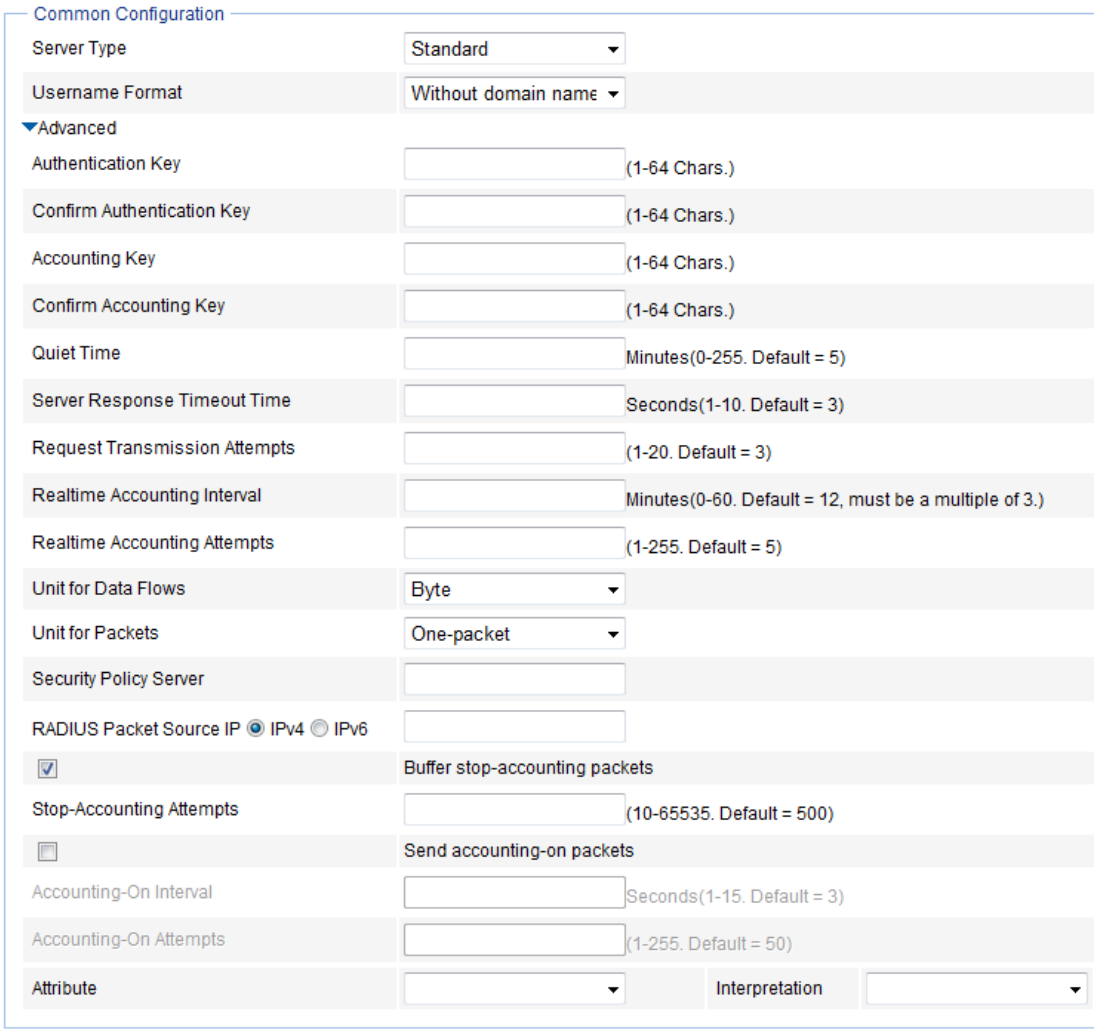
Table 116 Configuration items

Item	Description
Scheme Name	Enter a name for the RADIUS scheme.
Common Configuration	Configure the common parameters for the RADIUS scheme, including the server type, the username format, and the shared keys for authentication and accounting packets. For more information about common configuration, see "Configuring common parameters."
RADIUS Server Configuration	Configure the parameters of the RADIUS authentication servers and accounting servers. For more information about RADIUS server configuration, see "Adding RADIUS servers."

Configuring common parameters

1. Click the expand button before **Advanced** in the **Common Configuration** area to expand the advanced configuration area.

   Figure 367 Common configuration



2. Configure the parameters, as described in Table 117.

Table 117 Configuration items

Item	Description
Server Type	Select the type of the RADIUS servers supported by the device, which can be: • **Standard**—Standard RADIUS servers. The RADIUS client and RADIUS server communicate by using the standard RADIUS protocol and packet format defined in RFC 2138/2139 or later. • **Extended**—Extended RADIUS servers, usually running on CAMS or IMC. The RADIUS client and the RADIUS server communicate by using the proprietary RADIUS protocol and packet format.
Username Format	Select the format of usernames to be sent to the RADIUS server. Typically, a username is in the format of *userid@isp-name*, of which *isp-name* is used by the device to determine the ISP domain for the user. If a RADIUS server (such as a RADIUS server of some early version) does not accept a username that contains an ISP domain name, you can configure the device to remove the domain name of a username before sending it to the RADIUS server. The options include: • **Original format**—Configure the device to send the username of a user on an "as is" basis. • **With domain name**—Configure the device to include the domain name in a username. • **Without domain name**—Configure the device to remove any domain name of a username.
Authentication Key Confirm Authentication Key Accounting Key Confirm Accounting Key	Set the shared key for RADIUS authentication packets and that for RADIUS accounting packets. The RADIUS client and the RADIUS authentication/accounting server use MD5 to encrypt RADIUS packets. They verify packets through the specified shared key. The client and the server can receive and respond to packets from each other only when they use the same shared key. **IMPORTANT:** • The shared keys configured on the device must be consistent with those configured on the RADIUS servers. • The shared keys configured in the common configuration part are used only when no corresponding shared keys are configured in the RADIUS server configuration part.
Quiet Time	Set the time the device keeps an unreachable RADIUS server in blocked state. If you set the quiet time to 0, when the device needs to send an authentication or accounting request but finds that the current server is unreachable, it does not change the server's status that it maintains. It simply sends the request to the next server in the active state. As a result, when the device needs to send a request of the same type for another user, it still tries to send the request to the server because the server is in the active state. You can use this parameter to control whether the device changes the status of an unreachable server. For example, if you determine that the primary server is unreachable because the device's port for connecting the server is out of service temporarily or the server is busy, you can set the time to 0 so that the device uses the primary server as much.

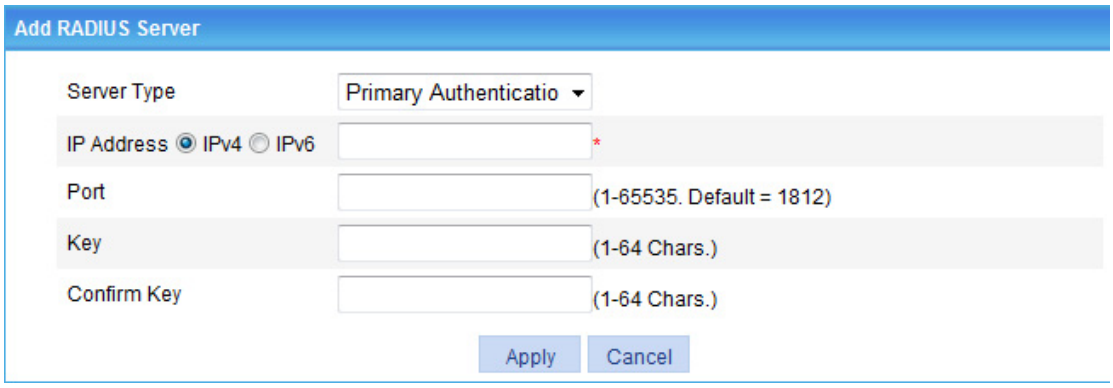
Item	Description
Server Response Timeout Time	Set the RADIUS server response timeout time. If the device sends a RADIUS request to a RADIUS server but receives no response in the specified server response timeout time, it retransmits the request. Setting a proper value according to the network conditions helps in improving the system performance.
Request Transmission Attempts	Set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server. If the device does not receive a response to its request from the RADIUS server within the response timeout period, it retransmits the RADIUS request. If the number of transmission attempts exceeds the limit but the device still does not receive a response from the RADIUS server, the device considers the request a failure. **IMPORTANT:** The server response timeout time multiplied by the maximum number of RADIUS packet transmission attempts must not exceed 75.
Realtime Accounting Interval	Set the interval for sending real-time accounting information. The interval must be a multiple of 3. To implement real-time accounting, the device must send real-time accounting packets to the accounting server for online users periodically. Different real-time accounting intervals impose different performance requirements on the NAS and the RADIUS server. A shorter interval helps achieve higher accounting precision but requires higher performance. Use a longer interval when a large number of users (1000 or more) exist. For more information about the recommended real-time accounting intervals, see "Configuration guidelines."
Realtime Accounting Attempts	Set the maximum number of attempts for sending a real-time accounting request.
Unit for Data Flows	Specify the unit for data flows sent to the RADIUS server, which can be: • Byte. • Kilo-byte. • Mega-byte. • Giga-byte.
Unit for Packets	Specify the unit for data packets sent to the RADIUS server, which can be: • One-packet. • Kilo-packet. • Mega-packet. • Giga-packet.
Security Policy Server	Specify the IP address of the security policy server.
RADIUS Packet Source IP	Specify the source IP address for the device to use in RADIUS packets sent to the RADIUS server. Hewlett Packard Enterprise recommends that you use a loopback interface address instead of a physical interface address as the source IP address. If the physical interface is down, the response packets from the server cannot reach the device.
Buffer stop-accounting packets	Enable or disable buffering of stop-accounting requests for which no responses are received.

Item	Description
Stop-Accounting Attempts	Set the maximum number of stop-accounting attempts. The maximum number of stop-accounting attempts, together with some other parameters, controls how the NAS deals with stop-accounting request packets. Suppose that the RADIUS server response timeout period is three seconds, the maximum number of transmission attempts is five, and the maximum number of stop-accounting attempts is 20. For each stop-accounting request, if the device receives no response within three seconds, it retransmits the request. If it receives no responses after retransmitting the request five times, it considers the stop-accounting attempt a failure, buffers the request, and makes another stop-accounting attempt. If 20 consecutive attempts fail, the device discards the request.
Send accounting-on packets	Enable or disable the accounting-on feature. The accounting-on feature enables a device to send accounting-on packets to RADIUS servers after it reboots, making the servers forcedly log out users who logged in through the device before the reboot. **IMPORTANT:** When enabling the accounting-on feature on a device for the first time, you must save the configuration so that the feature takes effect after the device reboots.
Accounting-On Interval	Set the interval for sending accounting-on packets. This field is configurable only after you select the **Send accounting-on packets** box.
Accounting-On Attempts	Set the maximum number of accounting-on packets transmission attempts. This field is configurable only after you select the **Send accounting-on packets** box.
Attribute Interpretation	Enable or disable the device to interpret the RADIUS class attribute as CAR parameters.

Adding RADIUS servers

1. In the **RADIUS Server Configuration** area, click **Add**.

Figure 368 RADIUS server configuration page



2. Configure the parameters, as described in Table 118.
3. Click **Apply**.

Table 118 Configuration items

Item	Description
Server Type	Select the type of the RADIUS server to be configured. Options include primary authentication server, primary accounting server, secondary authentication server, and secondary accounting server.
IP Address	Specify the IPv4 or IPv6 address of the RADIUS server. The IP addresses of the primary and secondary servers for a scheme must be different. Otherwise, the configuration fails. RADIUS server addresses in the same scheme must use the same IP version.
Port	Specify the UDP port of the RADIUS server.
Key Confirm Key	Specify the shared key for communication with the RADIUS server. If no shared key is specified, the shared key specified in the common configuration part is used.

RADIUS configuration example

Network requirements

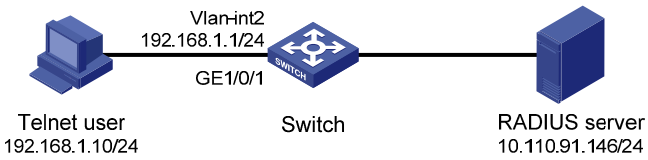
As shown in Figure 369, an 802.1X user logs in to the switch from the host. Configure the switch to implement RADIUS authentication and accounting for the 802.1X user. RADIUS accounting records the online duration of the 802.1X user.

Configure RADIUS servers on CAMS or IMC to use the default port for authentication and accounting. The 802.1X user's username and password and the shared key **expert** are configured for packet exchange with the switch.

On the switch, configure the shared key for packet exchange with the RADIUS server as **expert**, and configure the system to remove the domain name of a username before sending it to the RADIUS server.

On the switch, enable the Telnet server function, and configure the switch to use AAA for authentication, authorization and accounting of Telnet users.

Figure 369 Network diagram



Configuration prerequisites

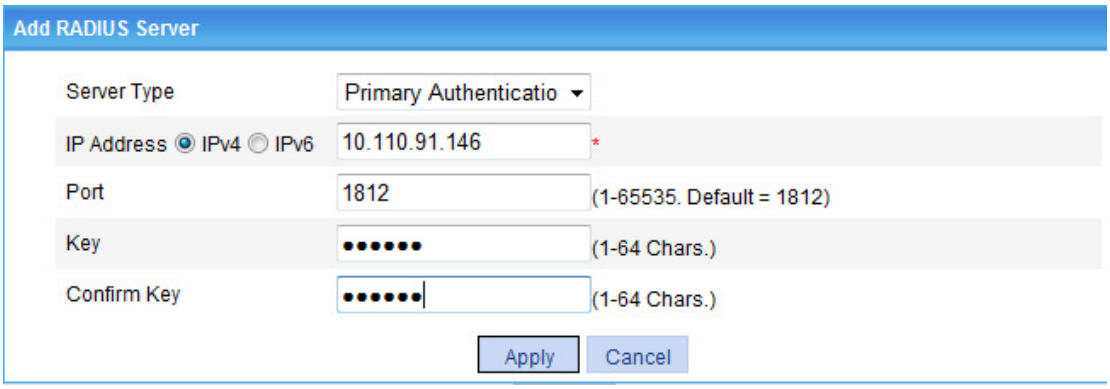
Enable 802.1X globally and on the specified port. Configure network access control based on MAC addresses. (Details not shown.)

Configuring a RADIUS scheme

1. Select **Authentication** > **RADIUS** from the navigation tree.
2. Click **Add** to add a RADIUS scheme:
   a. Enter **system** as the scheme name.
   b. Select **Extended** as the server type.
   c. Select **Without domain name** for the username format.
3. In the **RADIUS Server Configuration** area, click **Add** to configure the primary authentication server:

a. Select **Primary Authentication** as the server type.
b. Enter **10.110.91.146** as the IP address.
c. Enter **1812** as the port.
d. Enter **expert** as the key and enter **expert** again to confirm the key.
e. Click **Apply**.

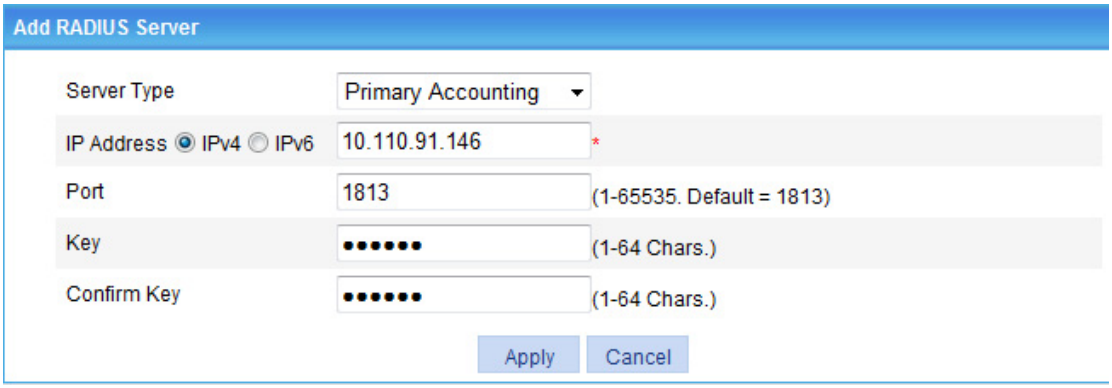
Figure 370 RADIUS authentication server configuration page



4. In the **RADIUS Server Configuration** area, click **Add** again to configure the primary accounting server:
   a. Select **Primary Accounting** as the server type.
   b. Enter **10.110.91.146** as the IP address.
   c. Enter **1813** as the port.
   d. Enter **expert** as the key and enter **expert** again to confirm the key.
   e. Click **Apply**.

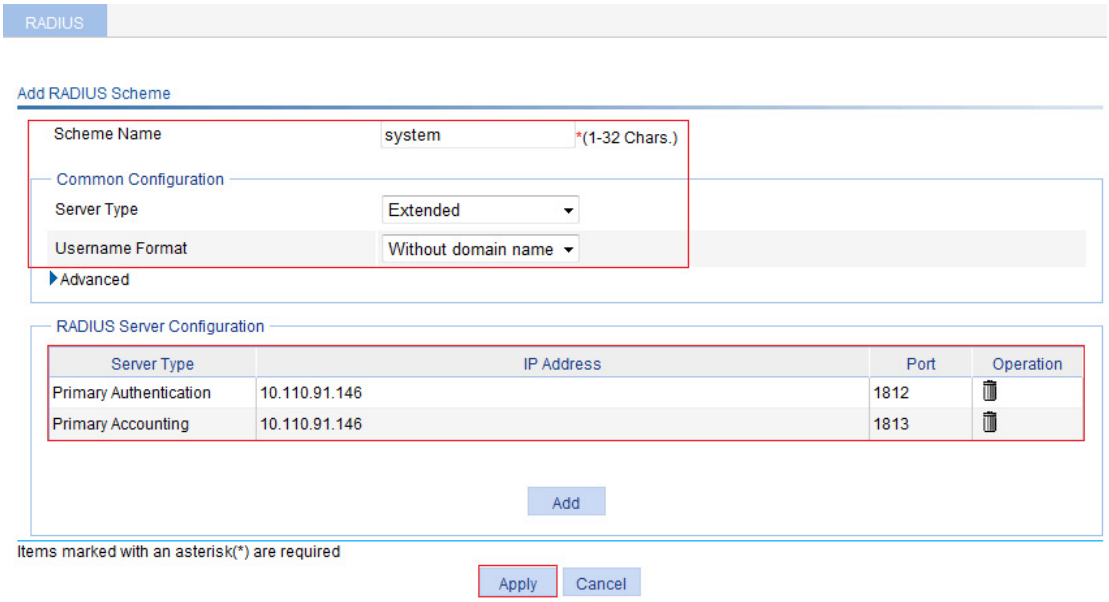
   The RADIUS scheme configuration page refreshes. The added servers appear in the server list.

Figure 371 RADIUS accounting server configuration page



5. Click **Apply**.

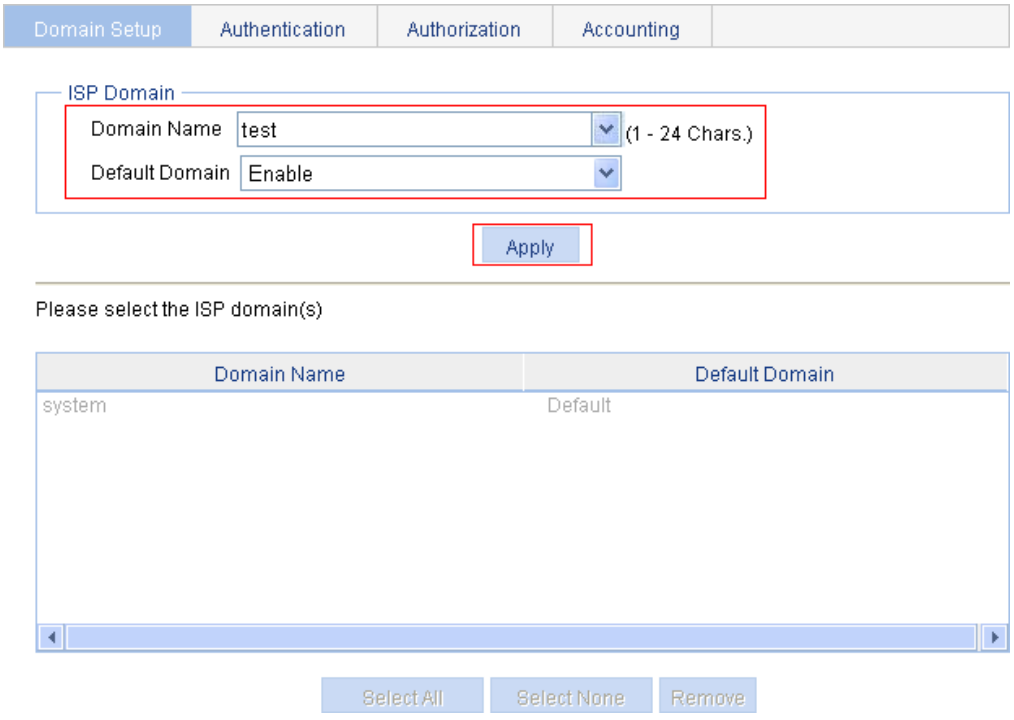
Figure 372 RADIUS scheme configuration



Configuring AAA

1. Select **Authentication** > **AAA** in the navigation tree.
   The domain setup page appears.
2. On the domain setup page, configure a domain:
   a. Enter **test** for **Domain Name**.
   b. Click **Enable** to use the domain as the default domain.
   c. Click **Apply**.

Figure 373 Creating an ISP domain



3. Select the **Authentication** tab to configure the authentication scheme:
   a. Select the domain name **test**.
   b. Select **Default AuthN** and select **RADIUS** as the authentication mode.
   c. Select **system** from the **Name** list to use it as the authentication scheme.
   d. Click **Apply**.
      A configuration progress dialog box appears.
   e. After the configuration process is complete, click **Close**.

Figure 374 Configuring the AAA authentication method for the ISP domain

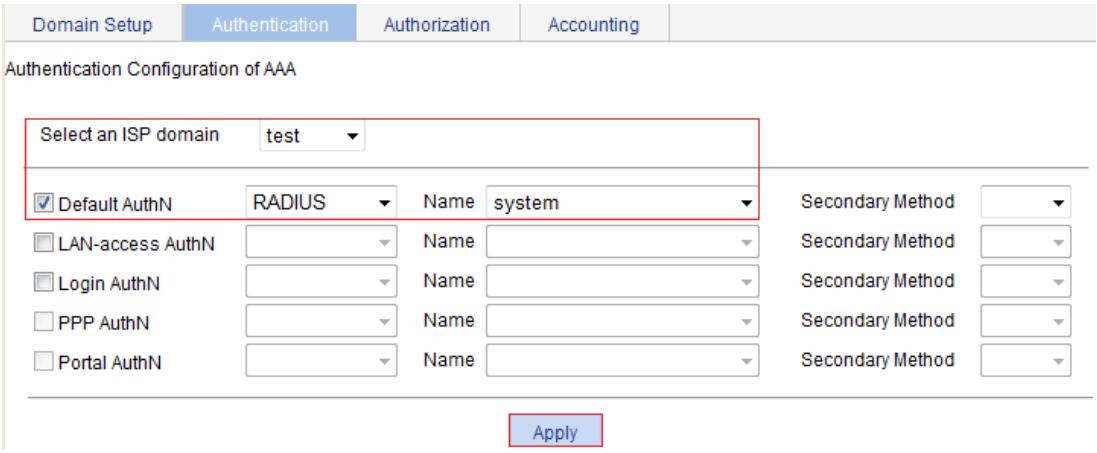
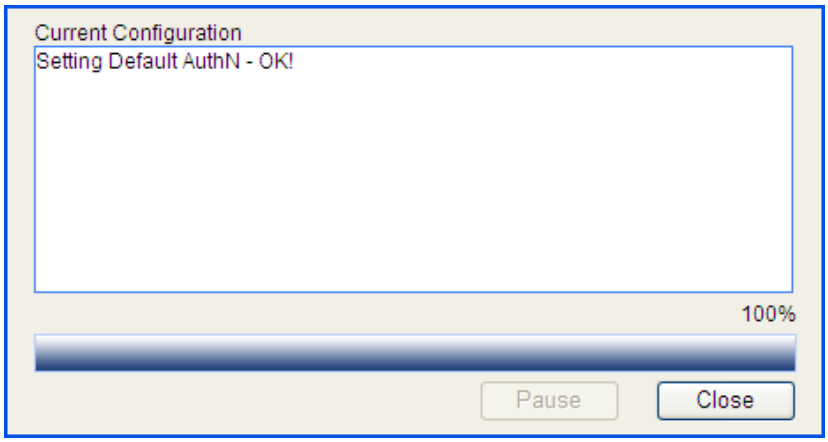
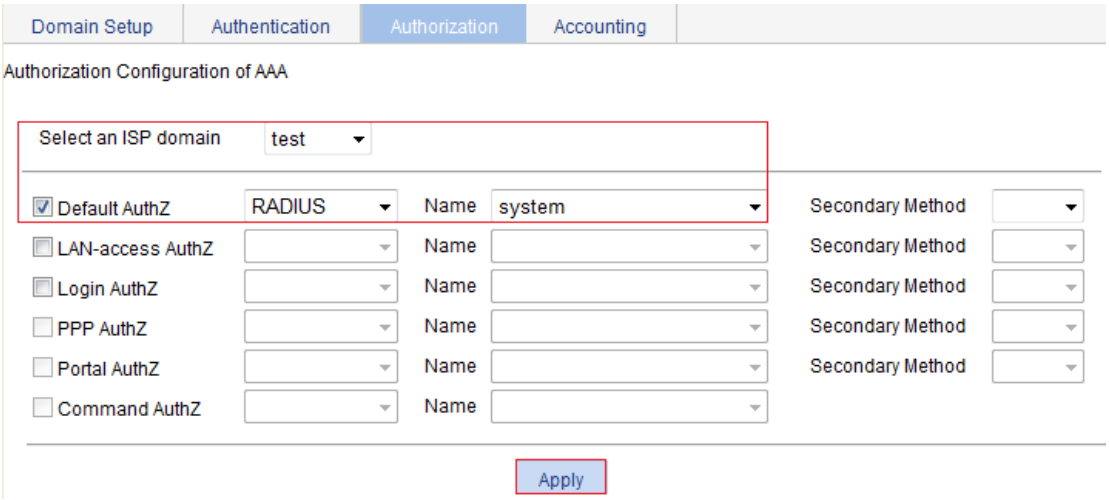


Figure 375 Configuration progress dialog box



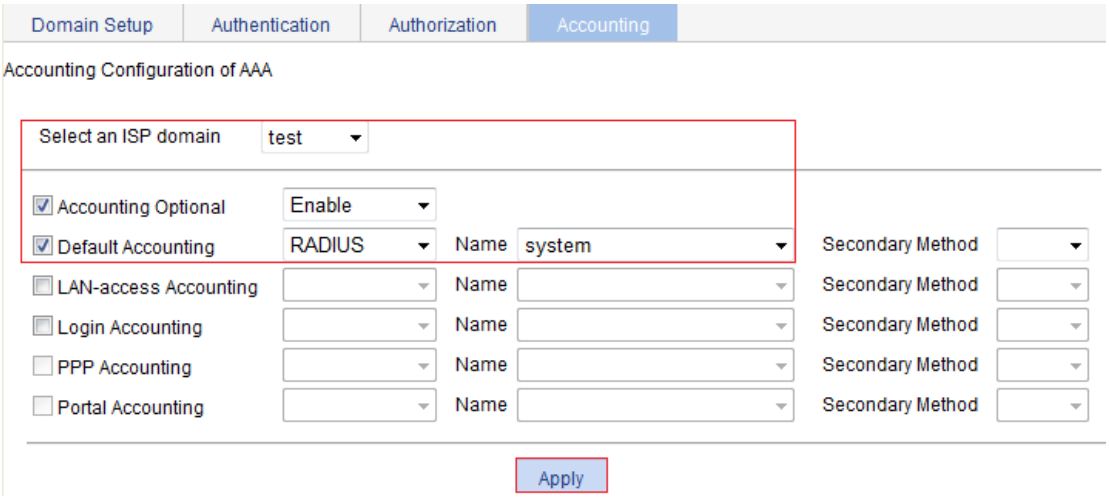
4. Select the **Authorization** tab to configure the authorization scheme:
   a. Select the domain name **test**.
   b. Select **Default AuthZ** and select **RADIUS** as the authorization mode.
   c. Select **system** from the **Name** list to use it as the authorization scheme.
   d. Click **Apply**.
      A configuration progress dialog box appears.
   e. After the configuration process is complete, click **Close**.

Figure 376 Configuring the AAA authorization method for the ISP domain



5. Select the **Accounting** tab to configure the accounting scheme:
   a. Select the domain name **test**.
   b. Select **Accounting Optional** and select **Enable** from the list.
   c. Select **Default Accounting** and select **RADIUS** as the accounting mode.
   d. Select **system** from the **Name** list to use it as the accounting scheme.
   e. Click **Apply**.
      A configuration progress dialog box appears.
   f. After the configuration process is complete, click **Close**.

Figure 377 Configuring the AAA accounting method for the ISP domain



Configuration guidelines

When you configure the RADIUS client, follow these guidelines:

- Accounting for FTP users is not supported.
- If you remove the accounting server used for online users, the device cannot send real-time accounting requests and stop-accounting messages for the users to the server, and the stop-accounting messages are not buffered locally.

- The status of RADIUS servers, blocked or active, determines which servers the device will communicate with or turn to when the current servers are not available. In practice, you can specify one primary RADIUS server and multiple secondary RADIUS servers, with the secondary servers that function as the backup of the primary servers. Typically, the device chooses servers based on these rules:
- When the primary server is in the active state, the device communicates with the primary server. If the primary server fails, the device changes the state of the primary server to blocked, starts a quiet timer for the server, and turns to a secondary server in the active state (a secondary server configured earlier has a higher priority). If the secondary server is unreachable, the device changes the state of the secondary server to blocked, starts a quiet timer for the server, and continues to check the next secondary server in the active state. This search process continues until the device finds an available secondary server or has checked all secondary servers in the active state. If the quiet timer of a server expires or an authentication or accounting response is received from the server, the status of the server changes back to active automatically, but the device does not check the server again during the authentication or accounting process. If no server is found reachable during one search process, the device considers the authentication or accounting attempt a failure.
- Once the accounting process of a user starts, the device keeps sending the user's real-time accounting requests and stop-accounting requests to the same accounting server. If you remove the accounting server, real-time accounting requests and stop-accounting requests for the user can no longer be delivered to the server.
- If you remove an authentication or accounting server in use, the communication of the device with the server will soon time out, and the device will look for a server in the active state by checking any primary server first and then the secondary servers in the order they are configured.
- When the primary server and secondary servers are all in the blocked state, the device communicates with the primary server. If the primary server is available, its statues changes to active. Otherwise, its status remains to be blocked.
- If one server is in the active state but all the others are in the blocked state, the device only tries to communicate with the server in the active state, even if the server is unavailable.
- After receiving an authentication/accounting response from a server, the device changes the status of the server identified by the source IP address of the response to active if the current status of the server is blocked.
- Set a proper real-time accounting interval based on the number of users.

Table 119 Recommended real-time accounting intervals

Number of users	Real-time accounting interval (in minutes)
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

Configuring users

You can configure local users and create groups to manage them.

A local user represents a set of user attributes configured on a device (such as the user password, use type, service type, and authorization attribute), and is uniquely identified by the username. For a user to pass local authentication, you must add an entry for the user in the local user database of the device. For more information about local authentication, see "Configuring AAA."

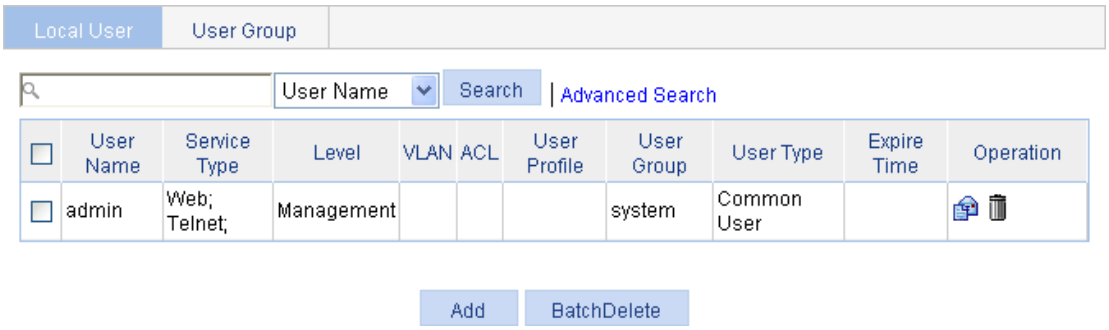
A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. All local users in a user group inherit the user attributes of the group. However, if you configure user attributes for a local user, the settings for 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 created automatically 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.

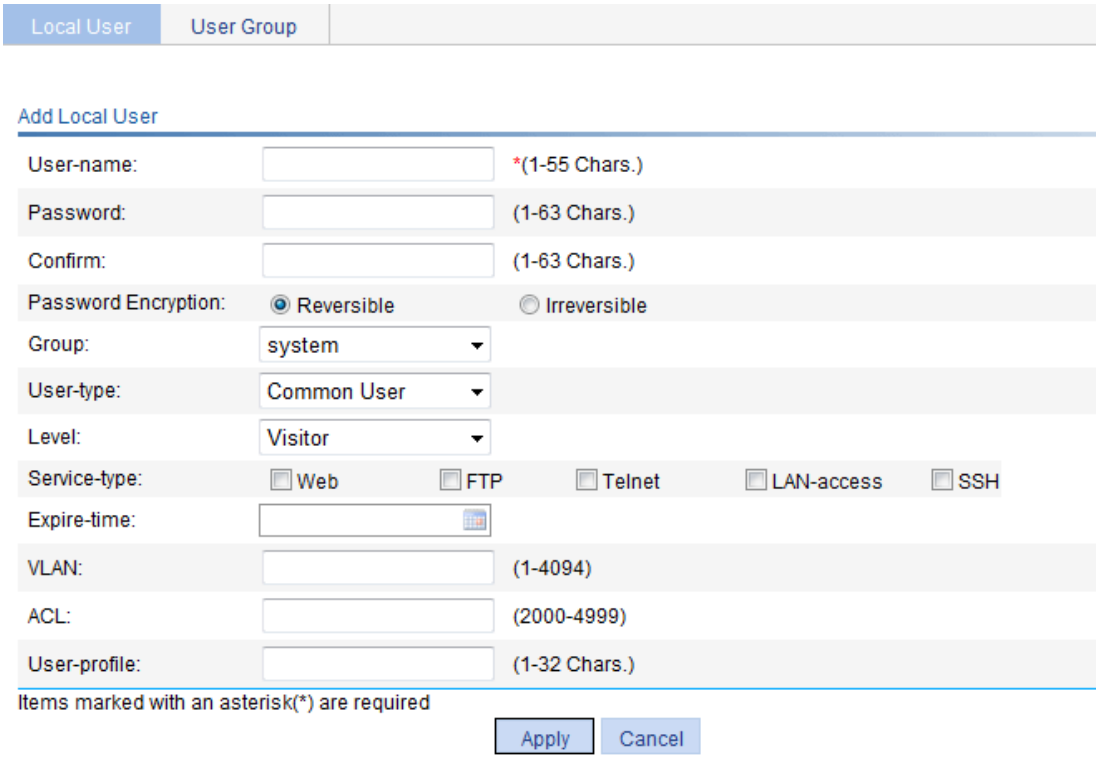
   Figure 378 Local user list

2. Click **Add**.

   The page for adding a local user appears.

Figure 379 Local user configuration page



3. Configure the local user as described in Table 120.
4. Click **Apply**.

Table 120 Configuration items

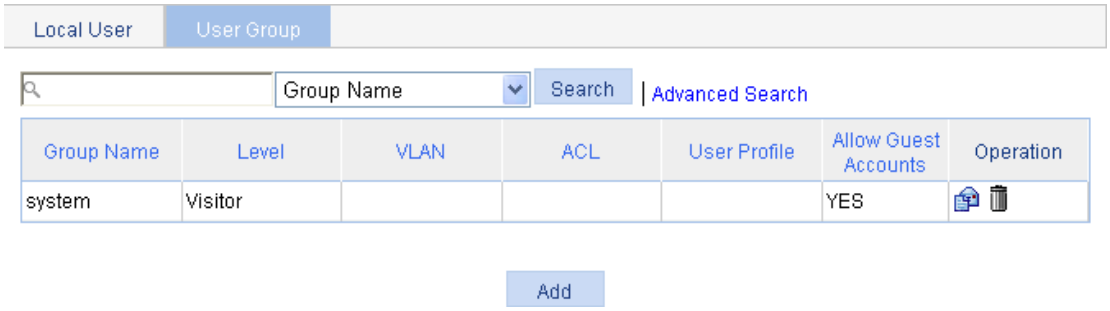
Item	Description
Username	Specify a name for the local user.
Password Confirm	Specify and confirm the password of the local user. The settings of these two fields must be the same. Do not specify a password starting with spaces because the spaces will be ignored.
Password Encryption	Select a password encryption method: **Reversible** or **Irreversible**.
Group	Select a user group for the local user. For information about user group configuration, see "Configuring a user group."
User-type	Select a user type for the local user: **Common User**, **Security Log Administrator**, or **Guest Administrator**. Only the **Common User** option takes effect on this software version.
Level	Select an authorization level for the local user: **Visitor**, **Monitor**, **Configure**, or **Management**, in ascending order of priority. This option takes effect on only Web, FTP, Telnet, and SSH users.
Service-type	Select the service types for the local user to use, including **Web**, **FTP**, **Telnet**, **LAN access** (Ethernet access service such as 802.1X), and **SSH**. 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. The service type of the guest administrator and security log administrator is **Web**.

Item	Description
Expire-time	Specify an expiration time for the local user, in the HH:MM:SS-YYYY/MM/DD format. To authenticate a local user with the expiration time configured, the access device checks whether the expiration time has passed. If it has not passed, the device permits the user to log in.
VLAN	Specify the VLAN to be authorized to the local user after the user passes authentication. This option takes effect on only LAN users.
ACL	Specify the ACL to be used by the access device to restrict the access of the local user after the user passes authentication. This option takes effect on only LAN users.
User-profile	Specify the user profile for the local user. This option takes effect on only LAN users, but it does not take effect on this software version.

Configuring a user group

1. Select **Authentication** > **Users** from the navigation tree.
2. Click the **User Group** tab to display the existing user groups.

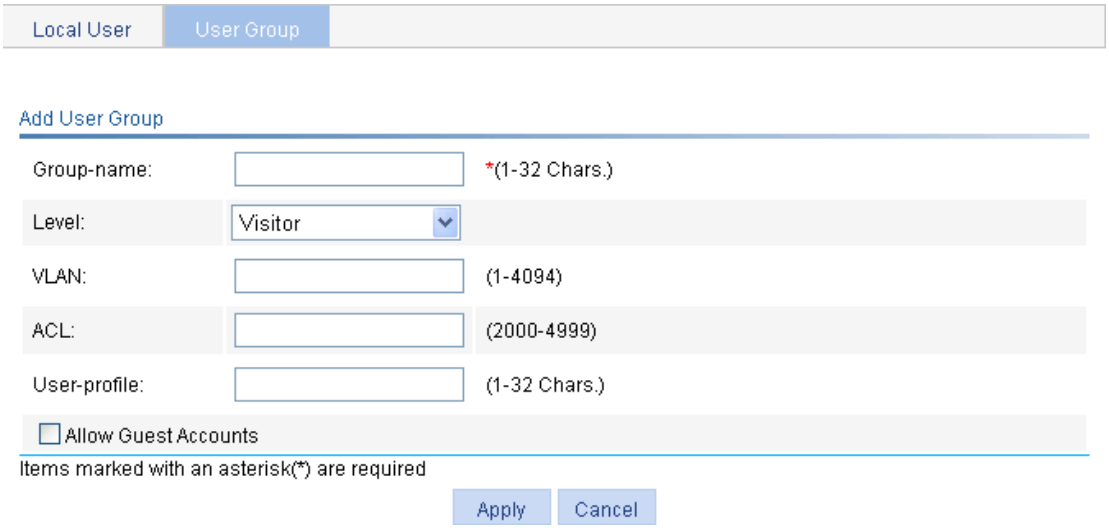
   Figure 380 User group list



3. Click **Add**.

   The page for configuring a user group appears.

Figure 381 User group configuration page



4. Configure the user group as described in Table 121.
5. Click **Apply**.

Table 121 Configuration items

Item	Description
Group-name	Specify a name for the user group.
Level	Select an authorization level for the user group: **Visitor**, **Monitor**, **Configure**, or **Management**, in ascending order of priority.
VLAN	Specify the VLAN to be authorized to users of the user group after the users pass authentication.
ACL	Specify the ACL to be used by the access device to control the access of users of the user group after the users pass authentication.
User-profile	Specify the user profile for the user group. This option does not take effect on this software version.
Allow Guest Accounts	Select this option to allow guest accounts to be added to the user group. This option is selected for the system-defined user group **system** and cannot be modified. However, this option does not take effect on this software version.

Managing certificates

Overview

The Public Key Infrastructure (PKI) offers an infrastructure for securing network services through public key technologies and digital certificates, and for verifying the identities of the digital certificate owners.

A digital certificate is a binding of certificate owner identity information and a public key. Users can get certificates, use certificates, and revoke certificates. By leveraging digital certificates and relevant services like certificate and blacklist distribution, PKI supports authenticating the entities involved in communication, and therefore guarantees 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 username 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). When 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.

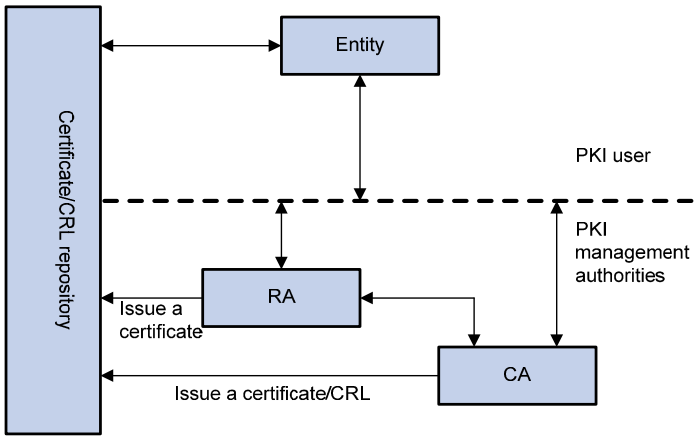
CA policy

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. Because different CAs might use different methods to examine the binding of a public key with an entity, make sure 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 382 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 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

An 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 an 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.

How PKI works

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificate. The following describes how it works:

1. An entity submits a certificate request to the CA.
2. The RA verifies the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.
3. The CA verifies the digital signature, approves the application, and issues a certificate.
4. The RA receives the certificate from the CA, sends it to the LDAP server to provide directory navigation service, and notifies the entity that the certificate is successfully issued.
5. The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.

6. The entity makes a request to the CA when it needs to revoke its certificate. The CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

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 VPN is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for example, 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 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 an 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.

Recommended configuration procedures

The device supports the following PKI certificate request modes:

- **Manual**—In manual mode, you need to manually 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 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 distinguished name (DN) shows the identity information of the entity. A CA identifies a certificate applicant uniquely by an entity DN. The DN settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request might be rejected. You must know the policy to determine which entity parameters are mandatory or optional.
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 called a PKI domain. A PKI domain is intended only for convenience of reference by other applications like IKE and SSL, and has only local significance.

Step	Remarks
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 must remove the CA certificate and local certificate first.
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 must 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 must 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 must 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.

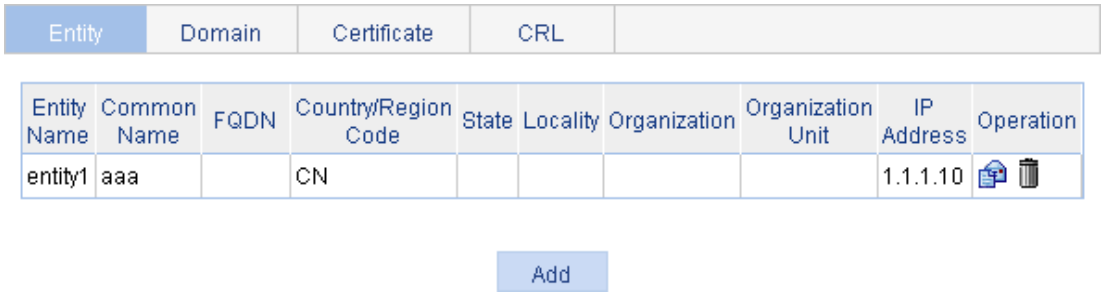
Recommended configuration procedure for automatic request

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 the identity information of an entity, where the DN shows the identity information of the entity. A CA identifies a certificate applicant uniquely by an entity DN. The DN settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request might be rejected. You must know the policy to determine which entity parameters are mandatory or optional.
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 called a PKI domain. A PKI domain is intended only for convenience of reference by other applications like IKE and SSL, and has only local significance.
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 must 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

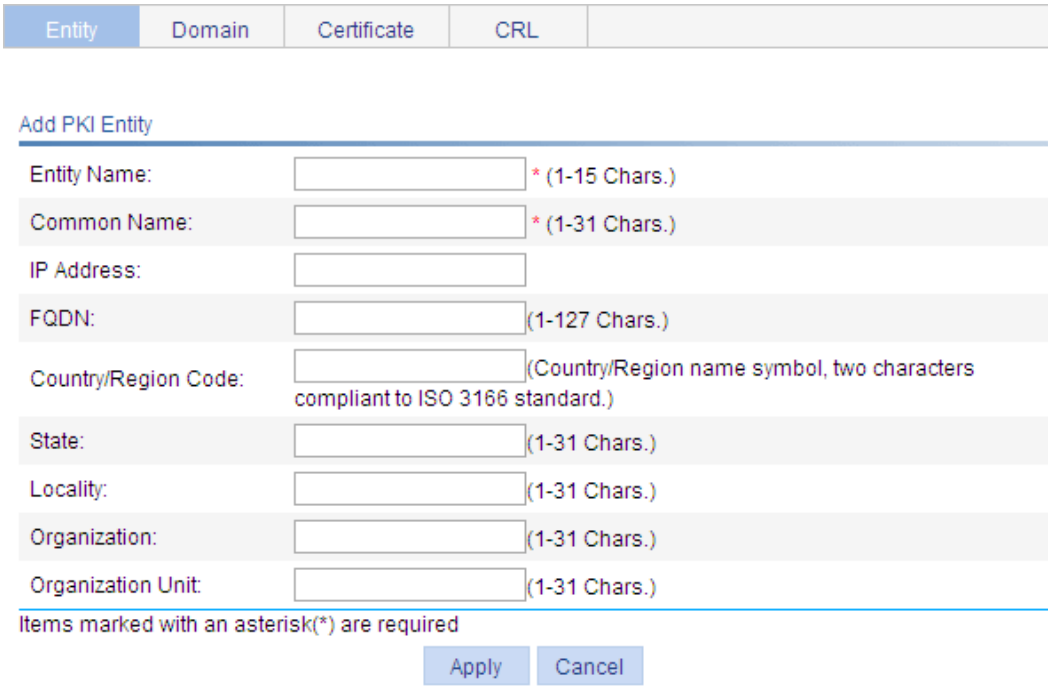
1. From the navigation tree, select **Authentication** > **Certificate Management**.
   The PKI entity list page is displayed by default.

   Figure 383 PKI entity list



2. Click **Add** on the page.

Figure 384 PKI entity configuration page



3. Configure the parameters, as described in Table 122.
4. Click **Apply**.

Table 122 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 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.

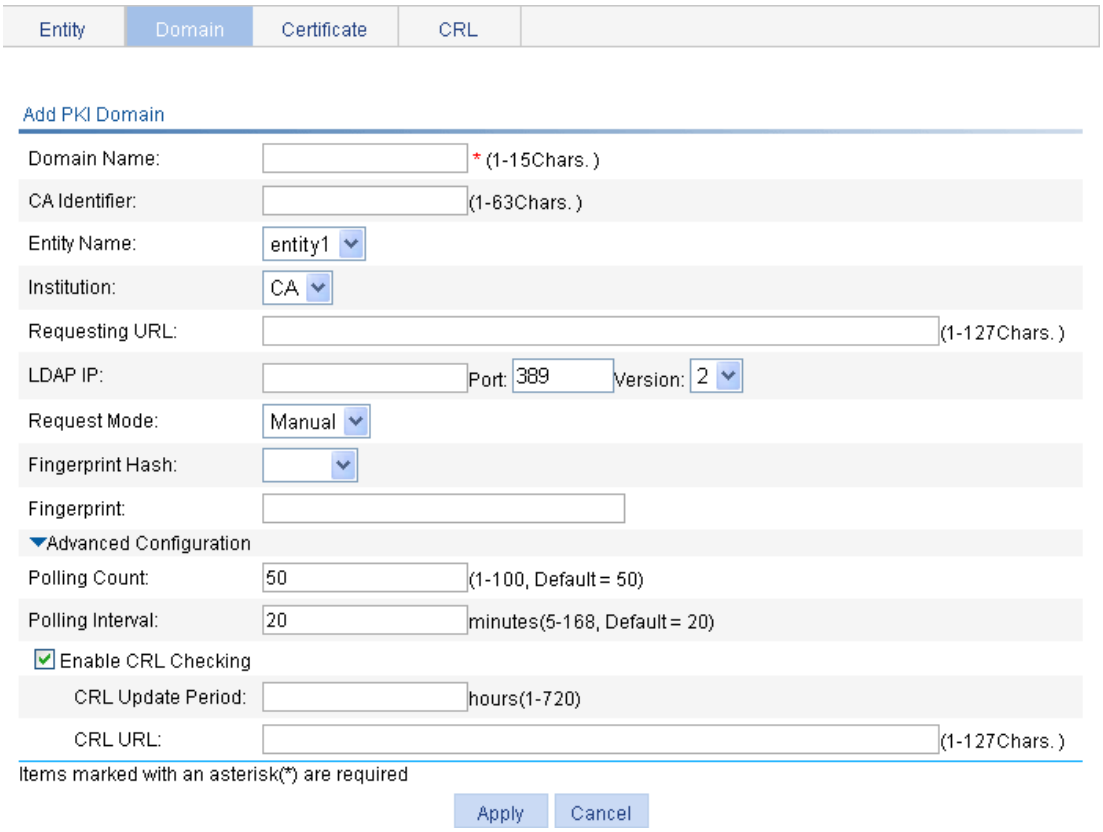
Creating a PKI domain

1. From the navigation tree, select **Authentication** > **Certificate Management**.
2. Click the **Domain** tab.

Figure 385 PKI domain list

3. Click **Add**.
4. Click **Display Advanced Config** to display the advanced configuration items.

Figure 386 PKI domain configuration page



5. Configure the parameters, as described in Table 123.
6. Click **Apply**.

Table 123 Configuration items

Item	Description
Domain Name	Enter the name for the PKI domain.
CA Identifier	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.

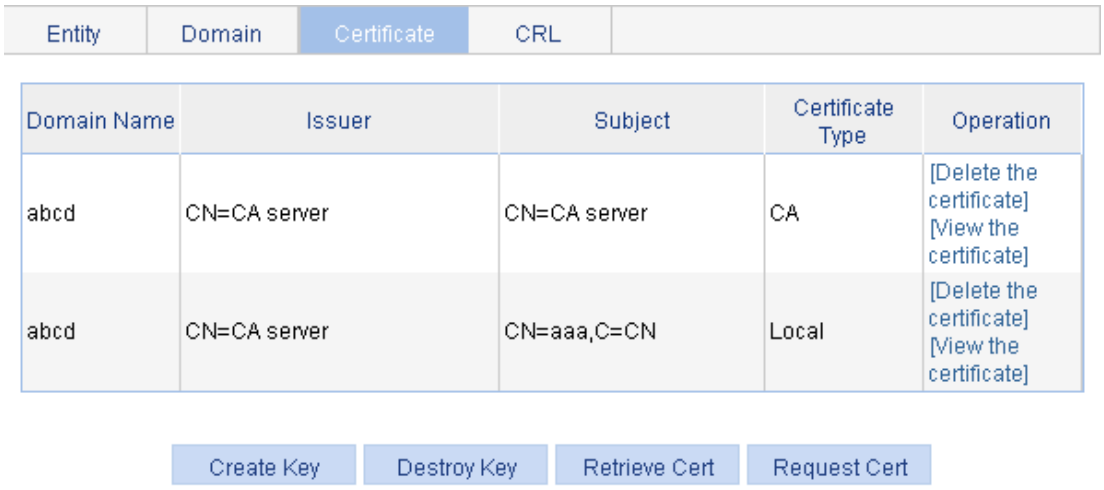
Item	Description
Entity Name	Select the local PKI entity. When submitting a certificate request to a CA, an entity needs to show its identity information. Available PKI entities are those that have been configured.
Institution	Select the authority for certificate request. • **CA**—Indicates that the entity requests a certificate from a CA. • **RA**—Indicates that the entity requests a certificate from an RA. RA is recommended.
Requesting URL	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.
LDAP IP	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..
Port	
Version	
Request Mode	Select the online certificate request mode, which can be auto or manual.
Password	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**..
Confirm Password	
Fingerprint Hash	Specify the fingerprint used for verifying the CA root certificate.
Fingerprint	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. • If you do not specify the fingerprint hash, do not enter any fingerprint. The entity will not verify the CA root certificate, and you yourself must make sure the CA server is trusted. **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 the CA server is trusted.
Polling Count	Set the polling interval and attempt limit for querying the certificate request status. 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..
Polling Interval	
Enable CRL Checking	Select this box to specify that CRL checking is required during certificate verification.

Item	Description
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. The URL can be an IP address or a domain name. This item is available after you click the **Enable CRL Checking** box. If the URL of the CRL distribution point is not set, you should get the CA certificate and a local certificate, and then get a CRL through SCEP.

Generating an RSA key pair

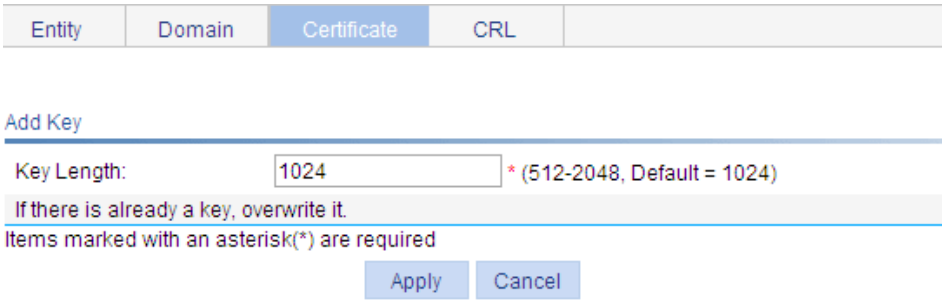
1. From the navigation tree, select **Authentication** > **Certificate Management**.
2. Click the **Certificate** tab.

Figure 387 Certificate configuration page



3. Click **Create Key**.
4. Set the key length.
5. Click **Apply**.

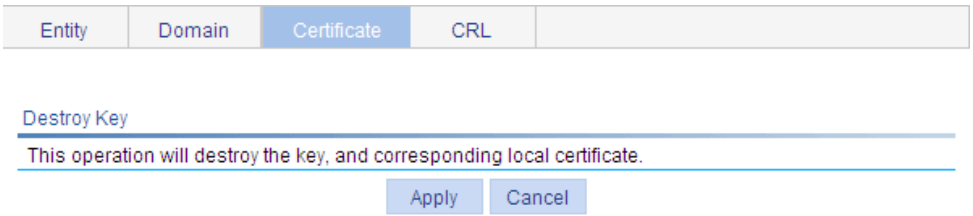
Figure 388 Key pair parameter configuration page



Destroying the RSA key pair

1. From the navigation tree, select **Authentication** > **Certificate Management**.
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 389 Key pair destruction page



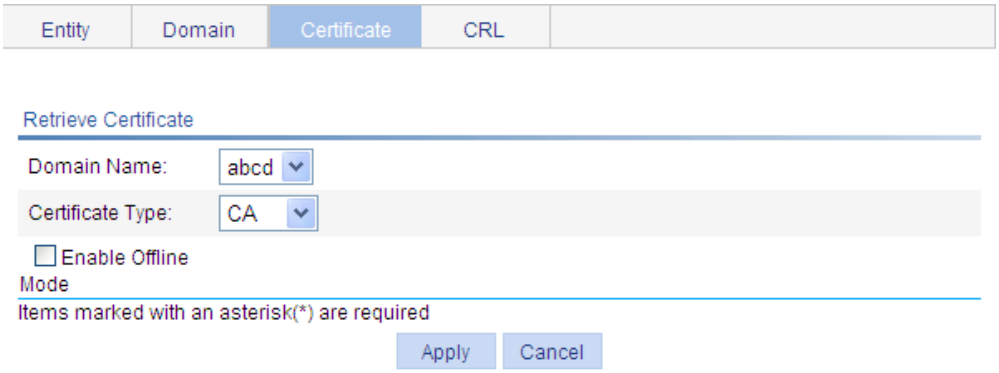
Retrieving and displaying a certificate

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. From the navigation tree, select **Authentication** > **Certificate Management**.
2. Click the **Certificate** tab.
3. Click **Retrieve Cert**.

Figure 390 PKI certificate retrieval page



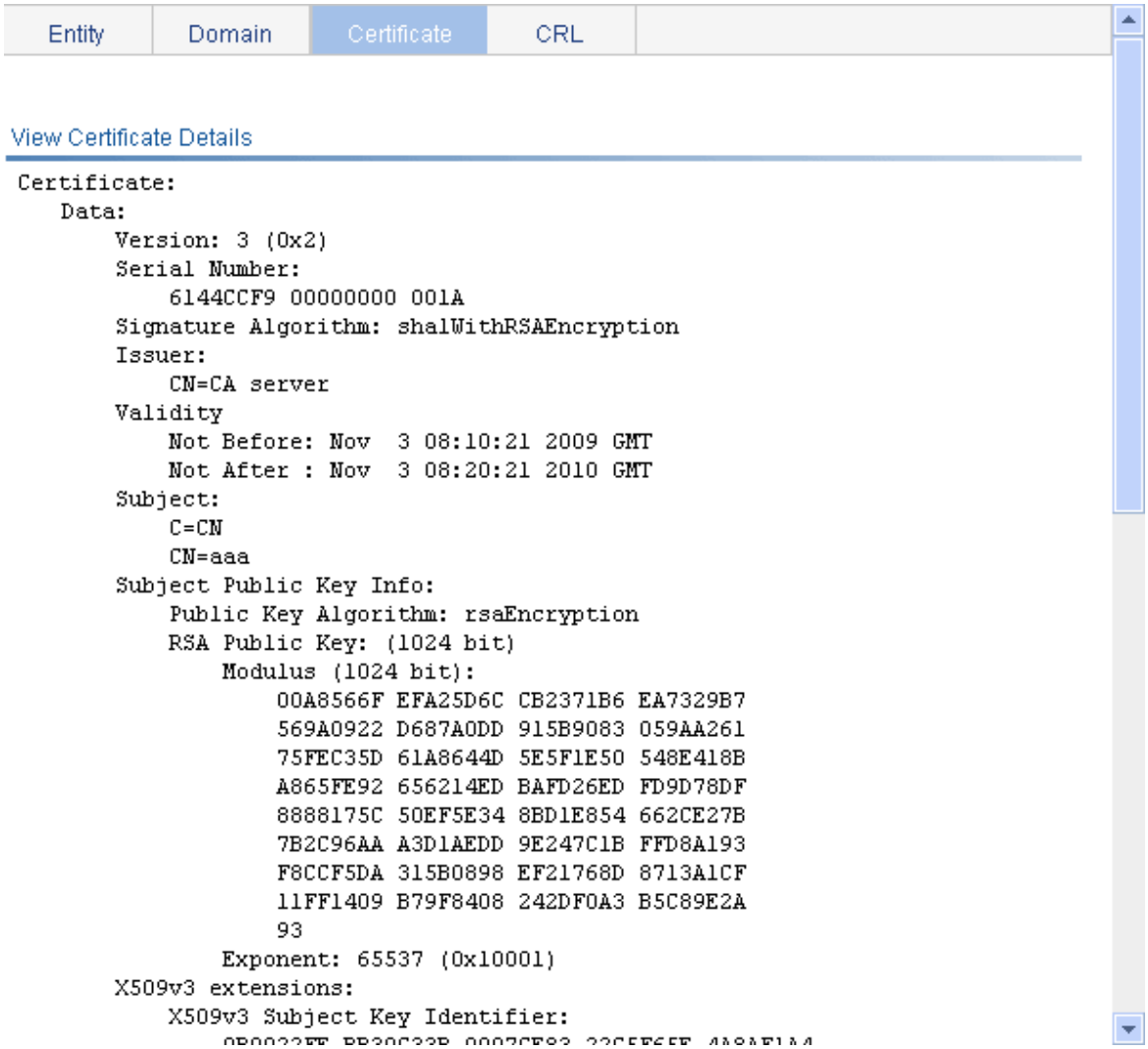
4. Configure the parameters, as described in Table 124.
5. Click **Apply**.

Table 124 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 Get File From PC	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. • 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.

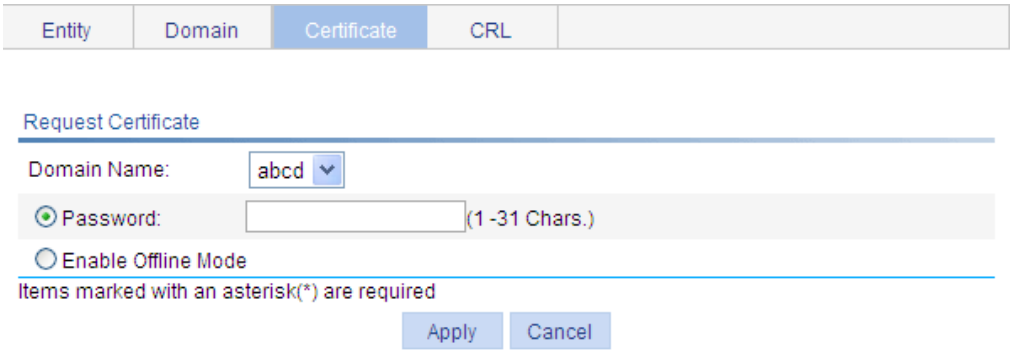
Figure 391 Certificate information



Requesting a local certificate

1. From the navigation tree, select **Authentication** > **Certificate Management**.
2. Click the **Certificate** tab.
3. Click **Request Cert**.

   Figure 392 Local certificate request page



4. Configure the parameters, as described in Table 125.

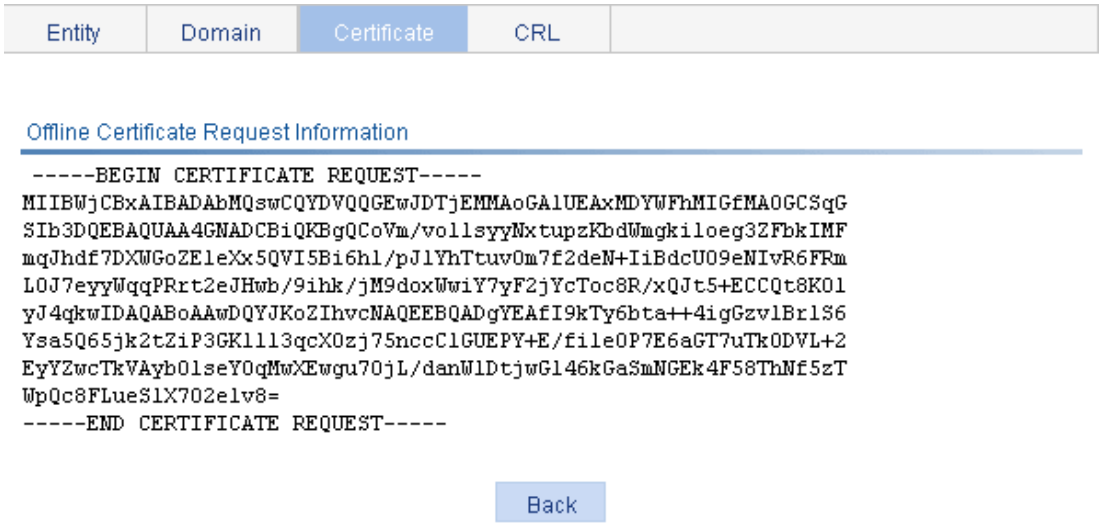
Table 125 Configuration items

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 shows a prompt that the 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.

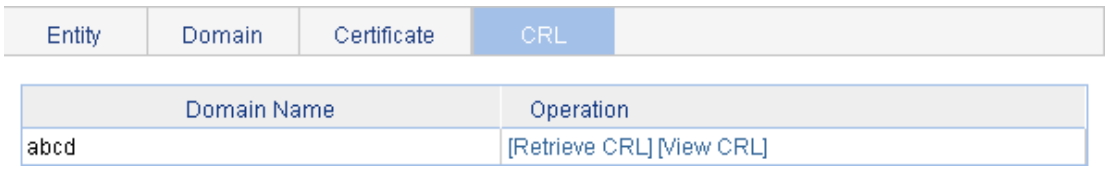
Figure 393 Offline certificate request information page



Retrieving and displaying a CRL

1. From the navigation tree, select **Authentication** > **Certificate Management**.
2. Click the **CRL** tab.

Figure 394 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 395 CRL information

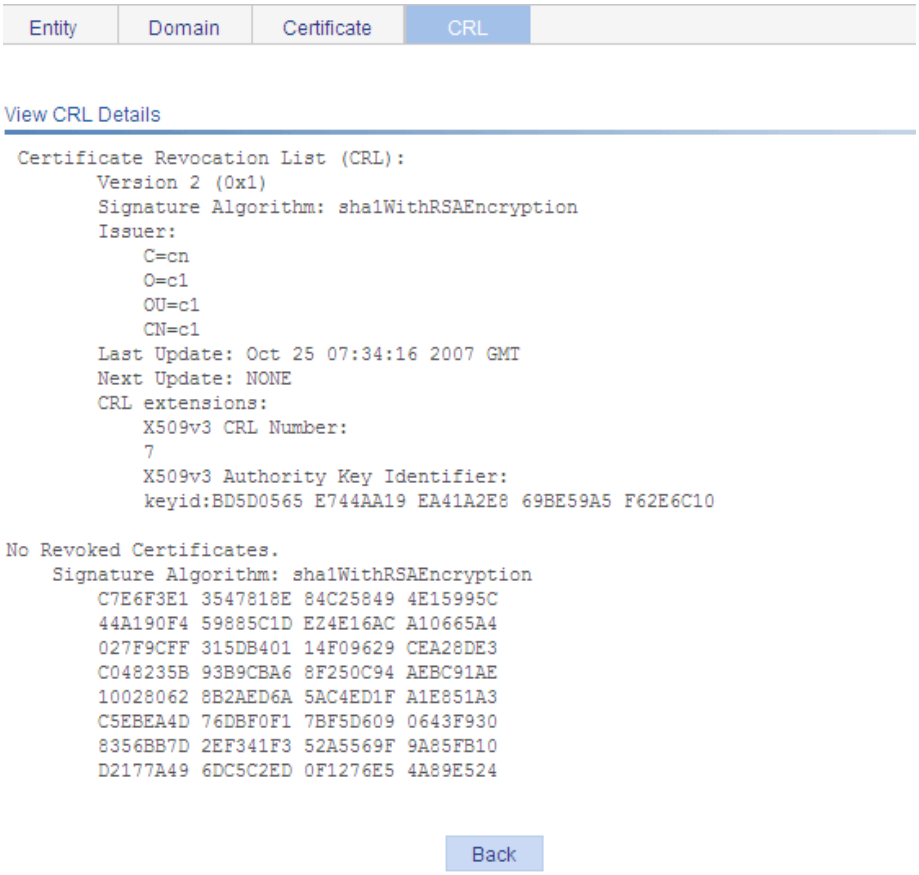


Table 126 Field description

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 CRL Number	CRL sequence number
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.

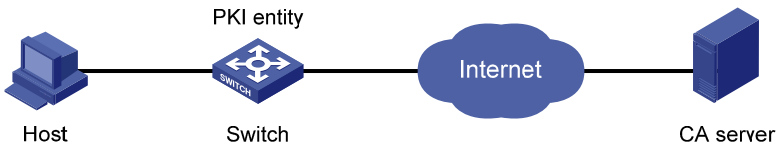
PKI configuration example

Network requirements

As shown in Figure 396, configure the switch working as the PKI entity, so that:

- The switch submits a local certificate request to the CA server, which runs the RSA Keon software.
- The switch retrieves CRLs for certificate verification.

Figure 396 Network diagram



Configuring the CA server

1. Create a CA server named **myca**:

   In this example, 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, organization unit, organization, and country. Leave the default values of the other attributes.

2. Configure extended attributes:

   After configuring the basic attributes, configure the parameters 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, 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 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

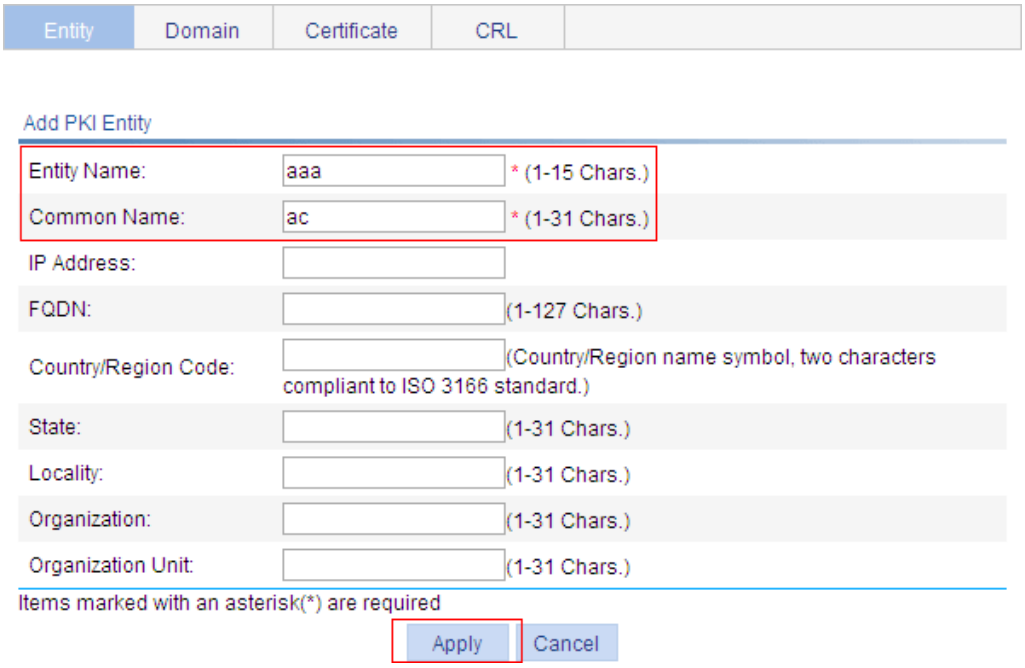
1. Create a PKI entity:
   a. From the navigation tree, select **Authentication** > **Certificate Management**.

      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 397 Creating a PKI entity

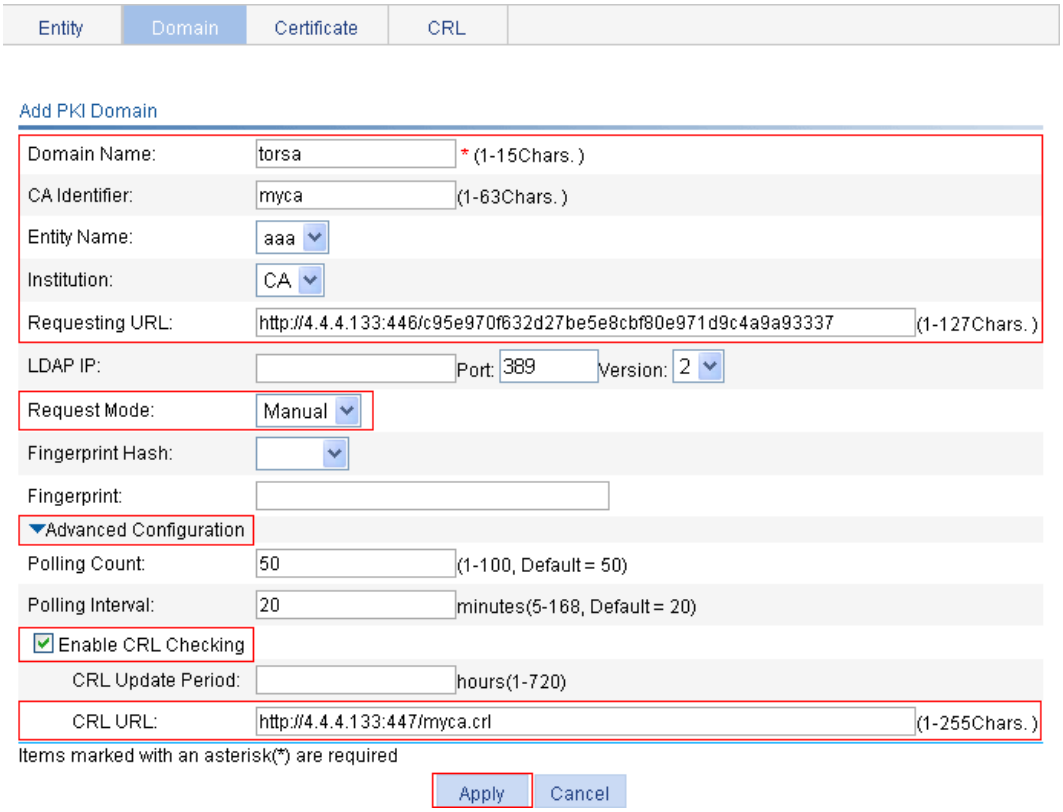


2. Create a PKI domain:
   a. Click the **Domain** tab.
   b. Click **Add**.

      The page in Figure 398 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**.

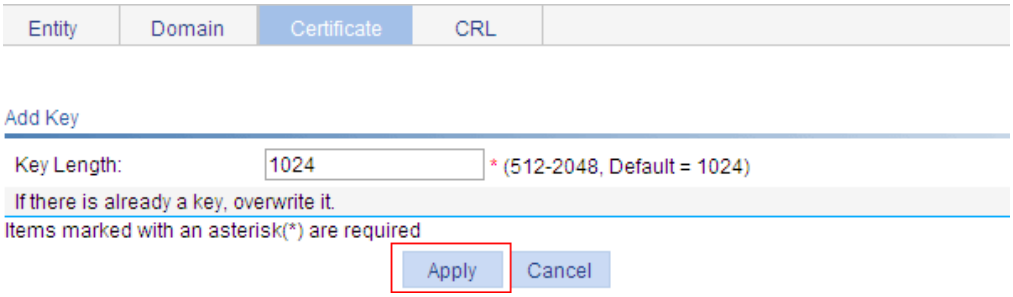
      A dialog box appears, asking "Fingerprint of the root certificate not specified. No root certificate validation will occur. Continue?"
   g. Click **OK**.

Figure 398 Creating a PKI domain



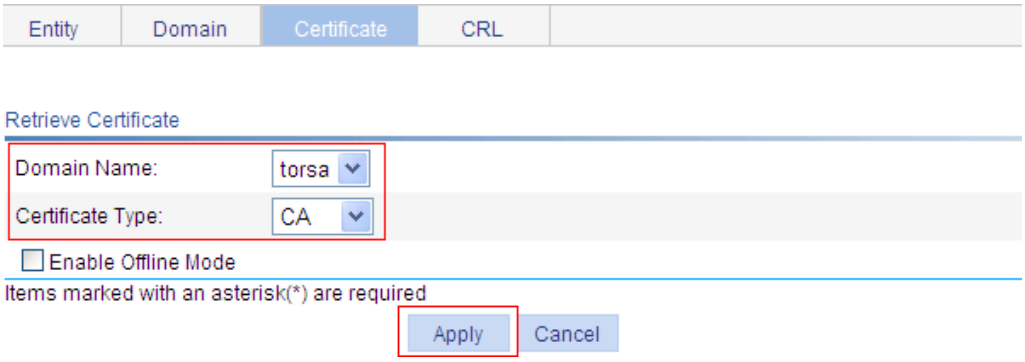
3. Generate an RSA key pair:
   a. Click the **Certificate** tab.
   b. Click **Create Key**.
   c. Enter **1024** as the key length, and click **Apply** to generate an RSA key pair.

   Figure 399 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**.

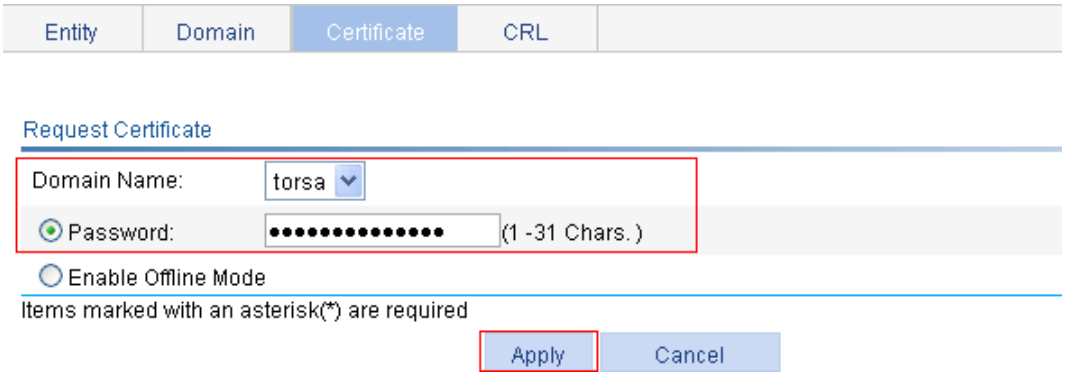
Figure 400 Retrieving the CA certificate



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 401 Requesting a local certificate



6. Retrieve the CRL:
   a. Click the **CRL** tab.
   b. Click **Retrieve CRL** of the PKI domain of **torsa**.

Figure 402 Retrieving the CRL

Verifying the configuration

After the configuration, select **Authentication** > **Certificate Management** > **Certificate** from the navigation tree to view detailed information about the retrieved CA certificate and local certificate, or select **Authentication** > **Certificate Management** > **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, 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, specify **CA** as the authority for certificate request when you configure the PKI domain.

Configuring MAC authentication

Overview

MAC authentication controls network access by authenticating source MAC addresses on a port. It does not require client software. A user does not need to enter a username and password for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication enabled port. If the MAC address passes authentication, the user can access authorized network resources. If the authentication fails, the device marks the MAC address as a silent MAC address, drops the packet, and starts a quiet timer. The device drops all subsequent packets from the MAC address within the quiet time. This quiet mechanism avoids repeated authentication during a short time.

If the MAC address that has failed authentication is a static MAC address or a MAC address that has passed any security authentication, the device does not mark the MAC address as a silent address.

User account policies

MAC authentication supports the following user account policies:

- **One MAC-based user account for each user**—The access device uses the source MAC addresses in packets as the usernames and passwords of users for MAC authentication. This policy is suitable for an insecure environment.
- **One shared user account for all users**—You specify one username and password, which are not necessarily a MAC address, for all MAC authentication users on the access device. This policy is suitable for a secure environment.

Local authentication and remote authentication

You can perform MAC authentication on the access device (local authentication) or through a RADIUS server.

Local authentication:

- If you configure MAC-based accounts, the access device uses the source MAC address of the packet as the username and password to search its local account database for a match.
- If you configure a shared account, the access device uses the shared account username and password to search its local account database for a match.

RADIUS authentication:

- If you configure MAC-based accounts, the access device sends the source MAC address as the username and password to the RADIUS server for authentication.
- If you configure a shared account, the access device sends the shared account username and password to the RADIUS server for authentication.

Authentication methods

RADIUS-based MAC authentication supports the following authentication methods:

- **Password Authentication Protocol (PAP)**—Transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security.
- **Challenge Handshake Authentication Protocol (CHAP)**—Transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.

MAC authentication timers

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before it regards the user idle. If a user connection has been idle for two consecutive intervals, the device logs the user out and stops accounting for the user.
- **Quiet timer**—Sets the interval that the device must wait before it can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- **Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before it regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Using MAC authentication with other features

VLAN assignment

You can specify a VLAN in the user account for a MAC authentication user to control its access to network resources. After the user passes MAC authentication, the authentication server, either the local access device or a RADIUS server, assigns the VLAN to the port as the default VLAN. After the user logs off, the initial default VLAN, or the default VLAN configured before any VLAN is assigned by the authentication server, restores. If the authentication server assigns no VLAN, the initial default VLAN applies.

A hybrid port is always assigned to a server-assigned VLAN as an untagged member. After the assignment, do not re-configure the port as a tagged member in the VLAN.

If MAC-based VLAN is enabled on a hybrid port, the device maps the server-assigned VLAN to the MAC address of the user. The default VLAN of the hybrid port does not change.

ACL assignment

You can specify an ACL in the user account for a MAC authentication user to control its access to network resources. After the user passes MAC authentication, the authentication server, either the local access device or a RADIUS server, assigns the ACL to the access port to filter the traffic from this user. You must configure the ACL on the access device for the ACL assignment function. You can change ACL rules while the user is online.

Auth-Fail VLAN

You can configure an Auth-Fail VLAN on a port to accommodate MAC authentication users that have failed MAC authentication on the port. 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. If no MAC Auth-Fail VLAN is configured, the user that fails MAC authentication cannot access any network resources.

If a user in the Auth-Fail VLAN passes MAC authentication, it is removed from the Auth-Fail VLAN and can access all authorized network resources. If not, the user is still in the Auth-Fail VLAN.

A hybrid port is always assigned to an Auth-Fail VLAN as an untagged member. After the assignment, do not re-configure the port as a tagged member in the VLAN.

Configuration prerequisites

Before you configure MAC authentication, complete the following tasks:

1. Configure an ISP domain and specify an AAA method. For more information, see "Configuring AAA."

- For local authentication, you must also create local user accounts (including usernames and passwords), and specify the **lan-access** service for local users.
- For RADIUS authentication, make sure the device and the RADIUS server can reach each other, and create user accounts on the RADIUS server. If you are using MAC-based accounts, make sure the username and password for each account are the same as the MAC address of each MAC authentication user.

2. Make sure the port security feature is disabled. For more information about port security, see "Configuring port security."

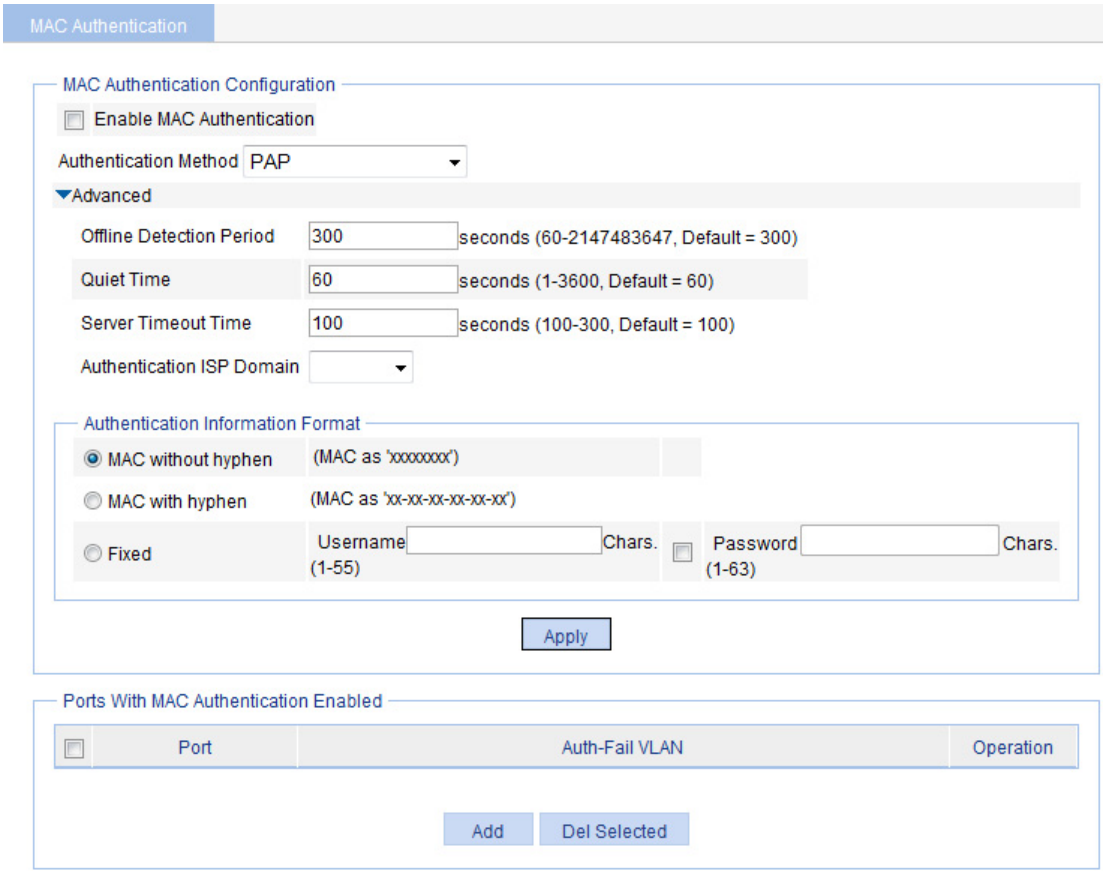
Recommended configuration procedure

Step	Remarks
1. Configuring MAC authentication globally	Required. This function enables MAC authentication globally and configures the authentication method and advanced parameters. By default, MAC authentication is disabled globally.
2. Configuring MAC authentication on a port	Required. This function enables MAC authentication on a port. MAC authentication can take effect on a port only when it is enabled globally and on the port. You can configure MAC authentication on ports first. By default, MAC authentication is disabled on a port.

Configuring MAC authentication globally

1. From the navigation tree, select **Authentication** > **MAC Authentication**.
2. Select **Enable MAC authentication**.
3. Select an authentication method, which can be CHAP or PAP.
4. In the **MAC Authentication Configuration** area, click **Advanced**.

Figure 403 MAC authentication configuration page



5. Configure MAC authentication global settings as described in Table 127, and then click **Apply**.

Table 127 Configuration items

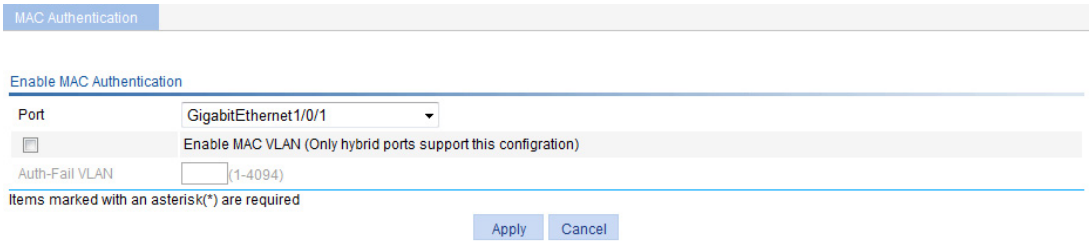
Item	Description
Enable MAC Authentication	Specifies whether to enable MAC authentication globally.
Authentication Method	Specifies the authentication method for MAC authentication, which can be PAP or CHAP. By default, the device uses PAP for MAC authentication.
Offline Detection Period	Specifies the period that the device waits for traffic from a user before it regards the user idle.
Quiet Time	Specifies the interval that the device must wait before it can perform MAC authentication for a user that has failed MAC authentication.
Server Timeout Time	Specifies the interval that the device waits for a response from a RADIUS server before it regards the RADIUS server unavailable.
Authentication ISP Domain	Specifies the ISP domain for MAC authentication users. If no ISP domain is specified, the system default authentication domain is used for MAC authentication users.

Authentication Information Format	Configures the properties of MAC authentication user accounts. • **MAC without hyphen**—Uses MAC-based accounts, and excludes hyphens from the MAC address, for example, xxxxxxxxxxxx. • **MAC with hyphen**—Uses MAC-based accounts, and hyphenates the MAC address, for example, xx-xx-xx-xx-xx-xx. • **Fixed**—Uses a shared account. You must specify a username and password for the account.

Configuring MAC authentication on a port

1. From the navigation tree, select **Authentication** > **MAC Authentication**.
2. In the **Ports With MAC Authentication Enabled** area, click **Add**.

Figure 404 Configuring MAC authentication on a port



3. Configure MAC authentication for a port as described in Table 128, and then click **Apply**.

Table 128 Configuration items

Item	Description
Port	Selects a port on which you want to enable MAC authentication.
Enable MAC VLAN	Specifies whether to enable MAC-based VLAN on the port. **IMPORTANT:** You can enable MAC authentication only on hybrid ports.
Auth-Fail VLAN	Specifies an existing VLAN as the MAC authentication Auth-Fail VLAN. **IMPORTANT:** • The MAC authentication Auth-Fail VLAN has a lower priority than the 802.1X guest VLAN on a port that performs MAC-based access control. If a user fails both types of authentication, the access port adds the user to the 802.1X guest VLAN. For more information about 802.1X guest VLANs, see "Configuring 802.1X." • The MAC authentication Auth-Fail VLAN function has higher priority than the quiet function of MAC authentication. • The MAC authentication Auth-Fail VLAN function has higher priority than the block MAC action, but it has lower priority than the shutdown port action of the port intrusion protection feature. For more information about port intrusion protection, see "Configuring port security."

MAC authentication configuration examples

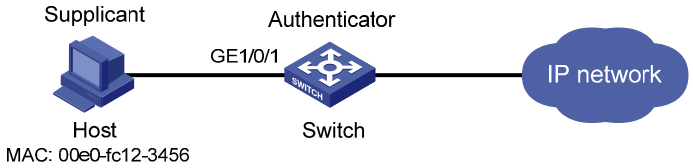
Local MAC authentication configuration example

Network requirements

As shown in Figure 405, configure local MAC authentication on port GigabitEthernet 1/0/1 to control Internet access, as follows:

- Configure all users to belong to the domain **aabbcc.net**, and specify local authentication for users in the domain.
- Use the MAC address of each user as the username and password for authentication, and require that the MAC addresses is hyphenated and in lower case.
- Configure the access device to detect whether a user has gone offline every 180 seconds. When a user fails authentication, the device does not authenticate the user within 180 seconds.

Figure 405 Network diagram



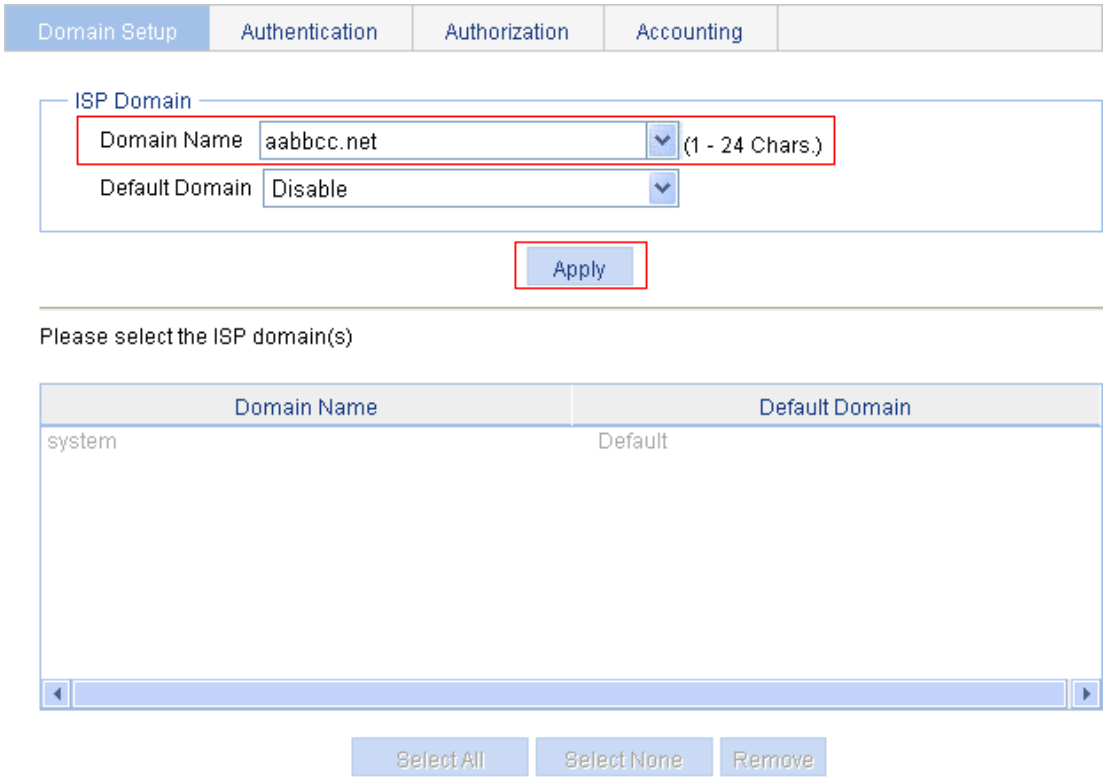
Configuring a local user

Add a local user. Set the username and password as **00-e0-fc-12-34-56**, the MAC address of the user. Set the service type to LAN access. (Details not shown.)

Configuring AAA

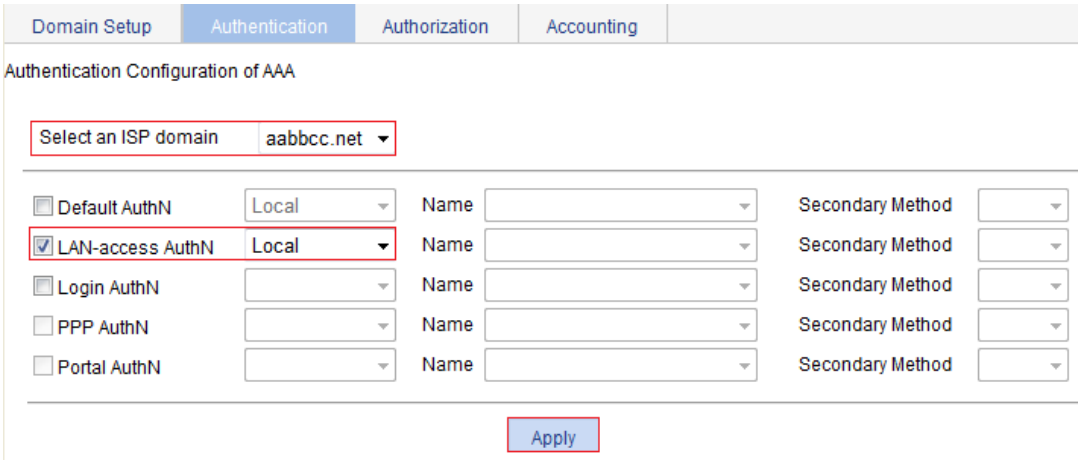
1. From the navigation tree, select **Authentication** > **AAA**.
2. On the **Domain Setup** page, enter the domain name **aabbcc.net** and click **Apply**.

Figure 406 Creating an ISP domain



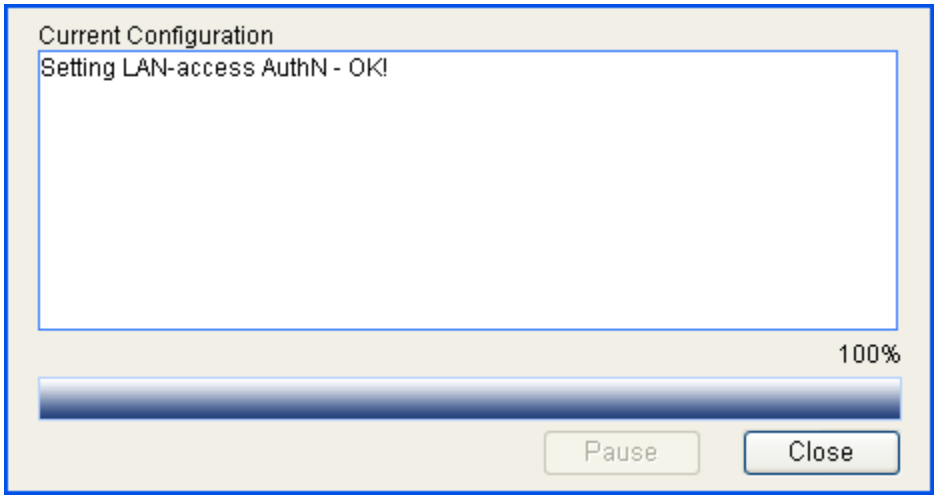
3. Click the **Authentication** tab.
4. Select the ISP domain **aabbcc.net**.
5. Select **LAN-access AuthN**, and select **Local** from the list.

Figure 407 Configuring the authentication method for the ISP domain



6. Click **Apply**.
   A configuration progress dialog box appears, as shown in Figure 408.

Figure 408 Configuration progress dialog box

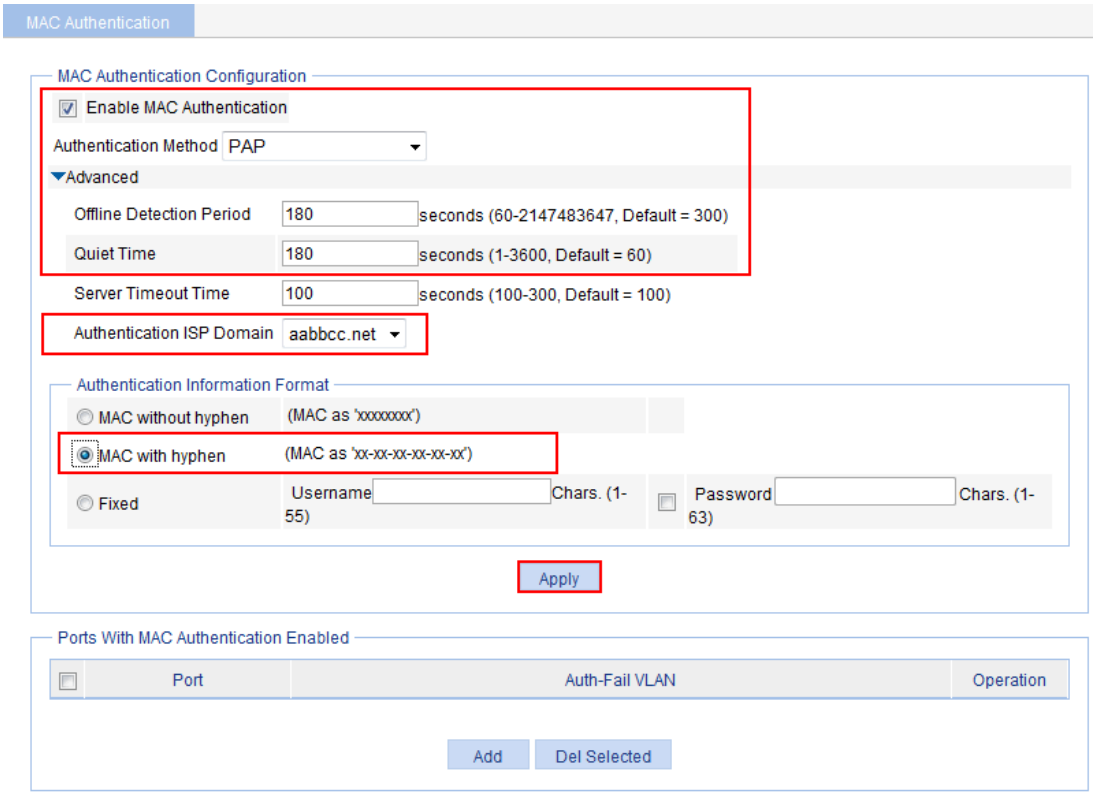


7. After the configuration process is complete, click **Close**.

Configuring MAC authentication

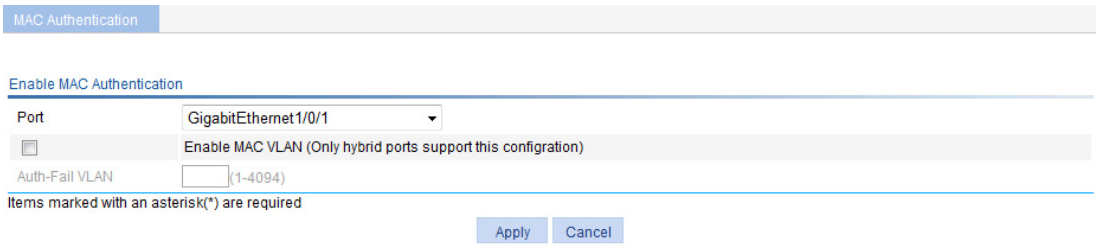
1. Configure MAC authentication globally:
   a. From the navigation tree, select **Authentication** > **MAC Authentication**.
   b. Select **Enable MAC Authentication**.
   c. Select **PAP** from the **Authentication Method** list.
   d. Click **Advanced**, and configure advanced MAC authentication.
   e. Set the offline detection period to **180** seconds.
   f. Set the quiet timer to **180** seconds.
   g. Select **aabbcc.net** from the **Authentication ISP Domain** list.
   h. Select **MAC with hyphen** from the **Authentication Information Format** area.
   i. Click **Apply**.

Figure 409 Configuring MAC authentication globally



2. Configure MAC authentication for GigabitEthernet 1/0/1:
   a. In the **Ports With MAC Authentication Enabled** area, click **Add**.
   b. Select **GigabitEthernet1/0/1** from the **Port** list, and click **Apply**.

Figure 410 Enabling MAC authentication for port GigabitEthernet 1/0/1



ACL assignment configuration example

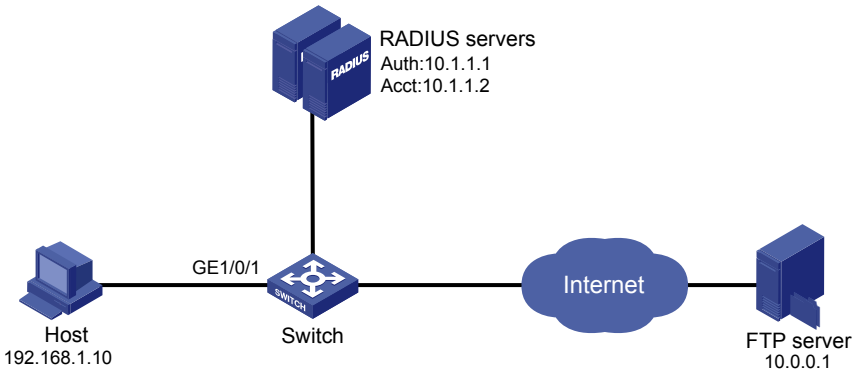
Network requirements

As shown in Figure 411, the switch uses RADIUS servers to perform authentication, authorization, and accounting.

Configure MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Make sure an authenticated user can access the Internet but not the FTP server at 10.0.0.1.

Use MAC-based user accounts for MAC authentication users. The MAC addresses are not hyphenated.

Figure 411 Network diagram



Configuring IP addresses

Assign an IP address to each interface. Make sure the RADIUS servers, host, and switch can reach each other. (Details not shown.)

Configuring the RADIUS servers

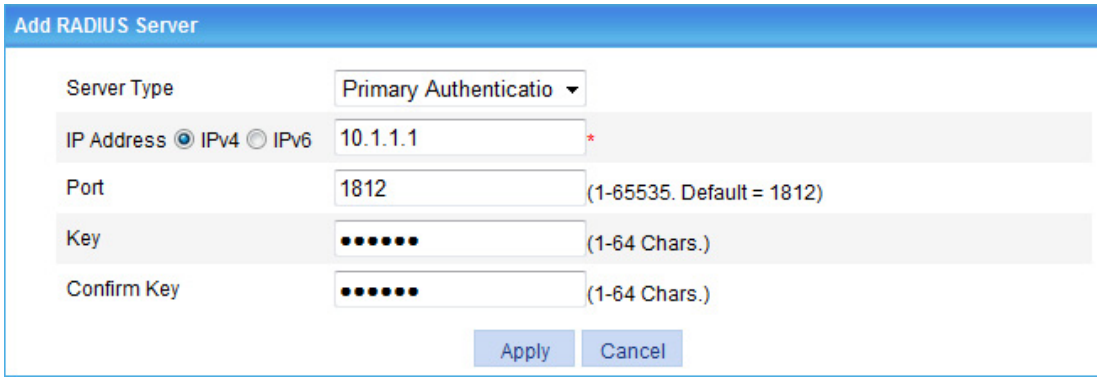
Add a user account with the host MAC address unhyphenated as both the username and password, and specify ACL 3000 as the authorization ACL for the user account. (Details not shown.)

For information about the RADIUS server configuration, see "Configuring RADIUS."

Configuring a RADIUS scheme for the switch

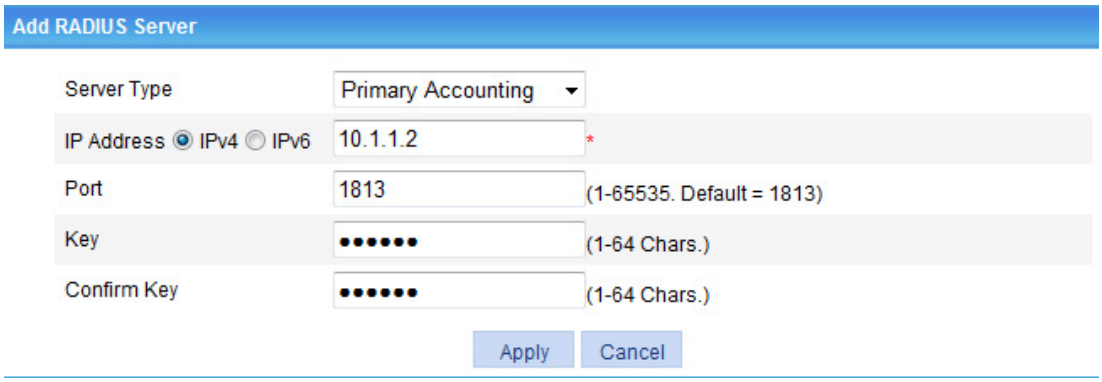
1. Create a RADIUS scheme:
   a. From the navigation tree, select **Authentication** > **RADIUS**.
   b. Click **Add**.
   c. Enter the scheme name **system**.
   d. Select the server type **Extended**.
   e. Select **Without domain name** from the **Username Format** list.
   f. Click **Apply**.
2. Configure the primary authentication server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Configure the RADIUS authentication server:
      – Select **Primary Authentication** from the **Server Type** list.
      – Enter **10.1.1.1** in the **IP Address** field, and enter the port number **1812**.
      – Enter **expert** in the **Key** field and the **Confirm Key** field.
   c. Click **Apply**.

Figure 412 Configuring a RADIUS authentication server



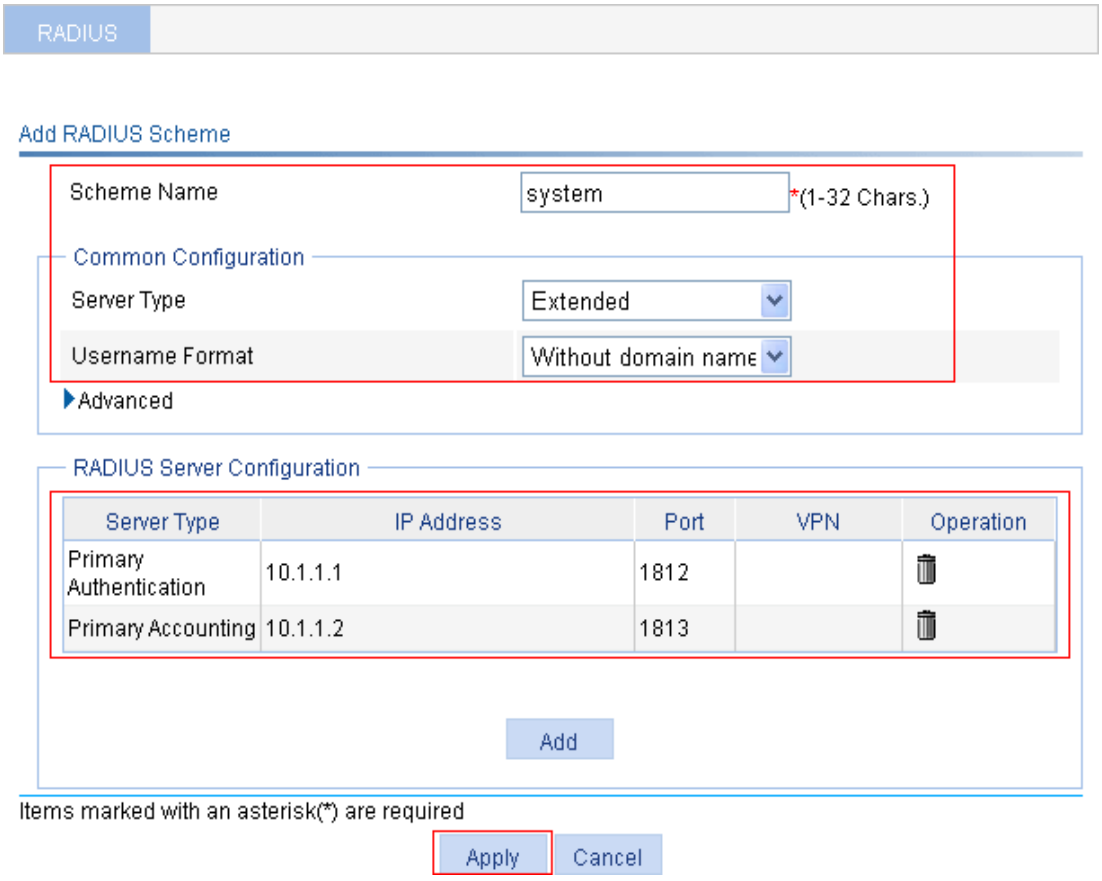
3. Configure the primary accounting server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Configure the primary accounting server:
      - Select the server type **Primary Accounting**.
      - Enter the IP address **10.1.1.2**, and enter the port number **1813**.
      - Enter **expert** in the **Key** field and the **Confirm Key** field.
   c. Click **Apply**.

Figure 413 Configuring a RADIUS accounting server



4. On the RADIUS configuration page, click **Apply**.

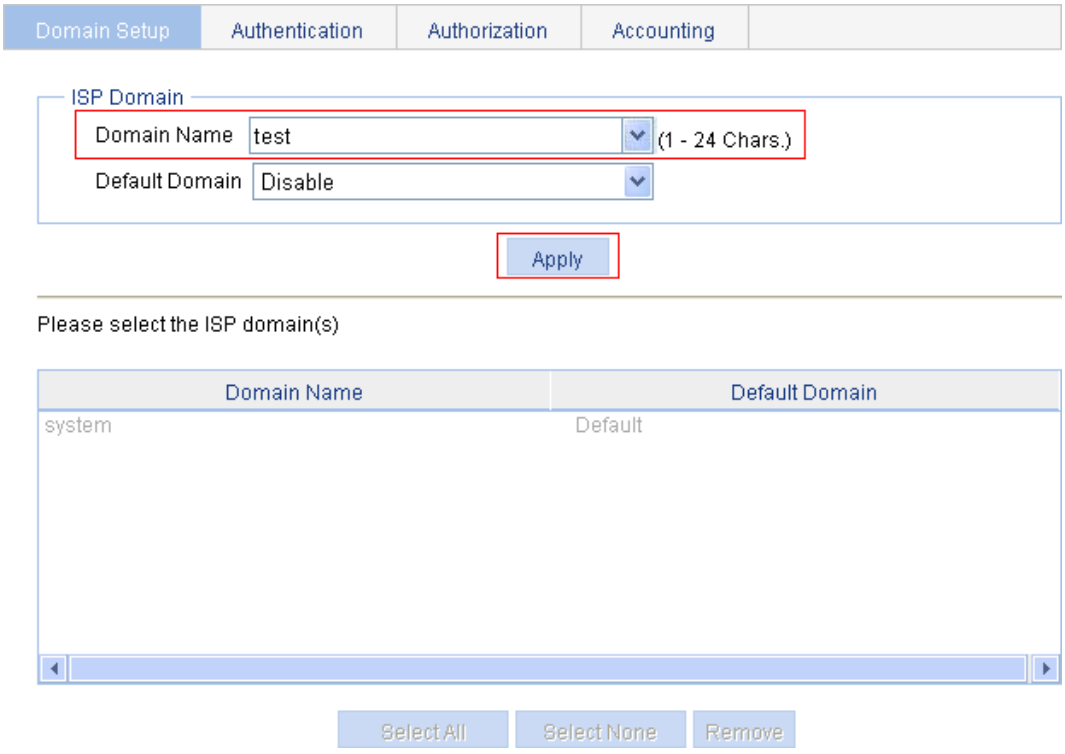
Figure 414 RADIUS configuration



Configuring AAA for the scheme

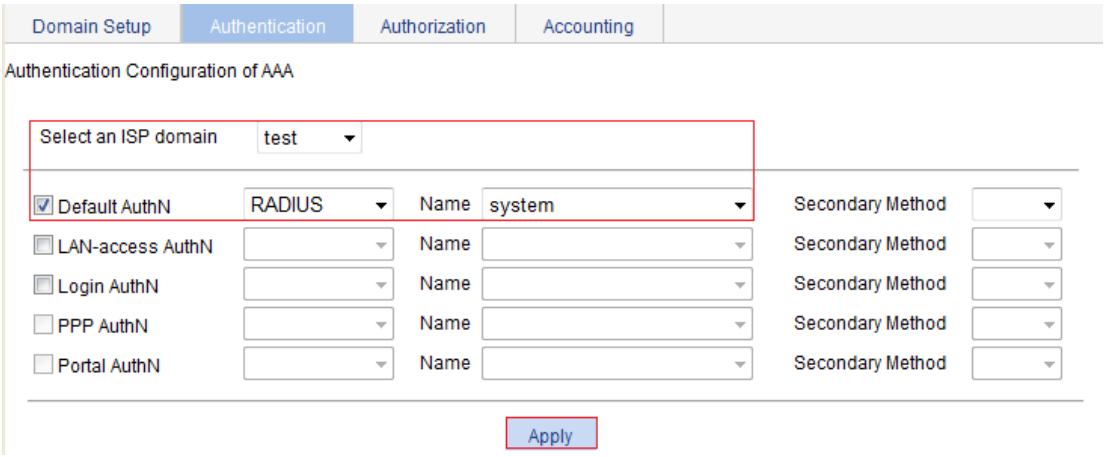
1. Create an ISP domain:
   a. From the navigation tree, select **Authentication** > **AAA**.
   b. On the **Domain Setup** page, enter **test** in the **Domain Name** field and click **Apply**.

Figure 415 Creating an ISP domain



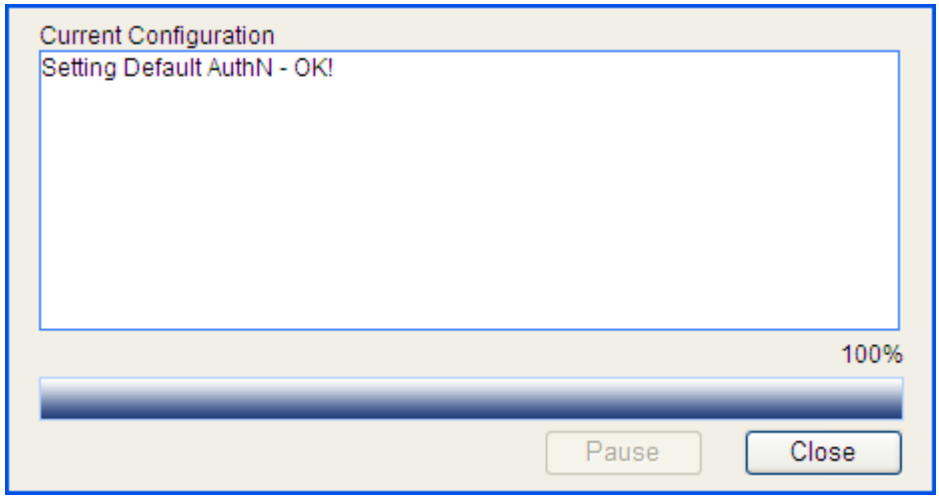
2. Configure AAA authentication method for the ISP domain:
   a. Click the **Authentication** tab.
   b. Select the ISP domain **test**.
   c. Select **Default AuthN**, select the authentication method **RADIUS**, and select the authentication scheme **system** from the **Name** list.

Figure 416 Configuring the authentication method for the ISP domain



   d. Click **Apply**.
   A configuration progress dialog box appears, as shown in Figure 417.

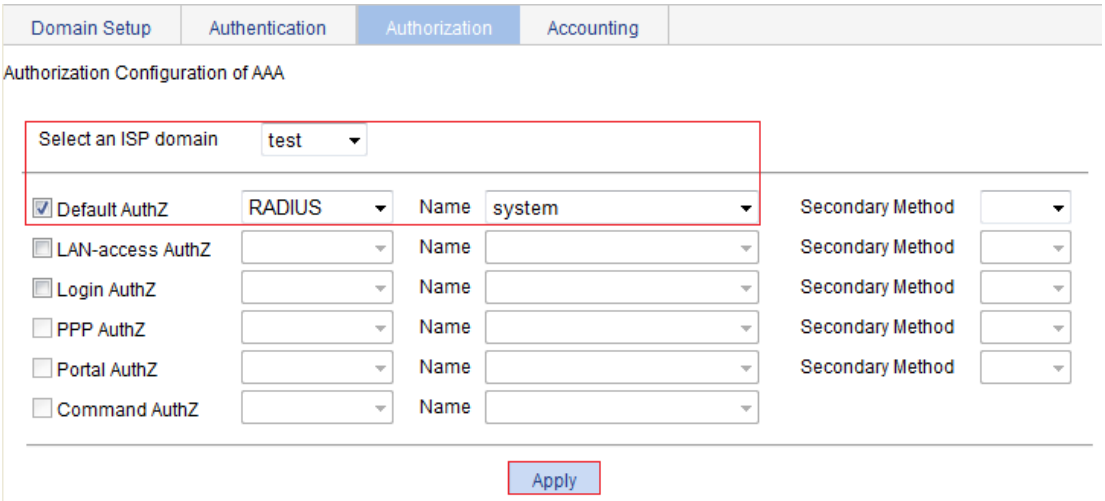
Figure 417 Configuration progress dialog box



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

3. Configure AAA authorization method for the ISP domain:
   a. Click the **Authorization** tab.
   b. Select the ISP domain **test**.
   c. Select **Default AuthZ**, select the authorization mode **RADIUS**, and select the authorization scheme **system** from the **Name** list.
   d. Click **Apply**.

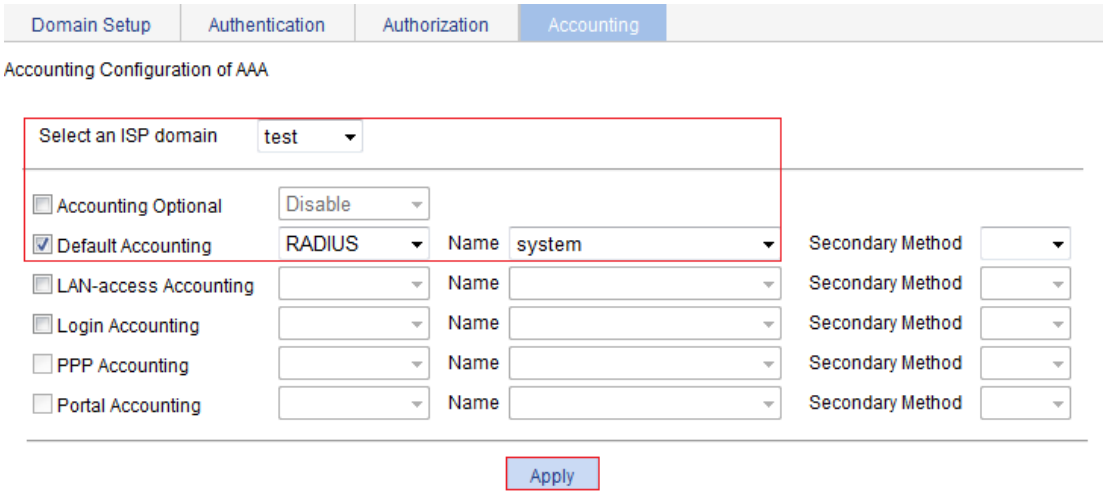
Figure 418 Configuring the authorization method for the ISP domain



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

4. Configure AAA accounting method for the ISP domain:
   a. Click the **Accounting** tab.
   b. Select the ISP domain **test**.
   c. Select **Default Accounting**, select the accounting method **RADIUS**, and select the accounting scheme **system** from the **Name** list.
   d. Click **Apply**.

Figure 419 Configuring the accounting method for the ISP domain

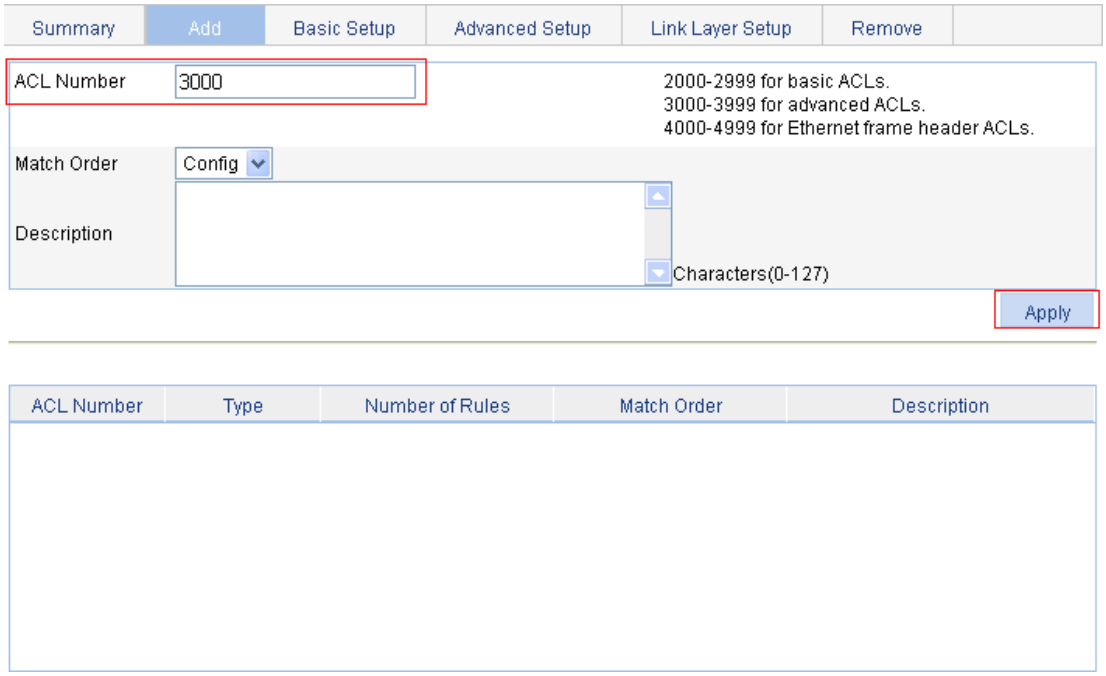


e. After the configuration process is complete, click **Close**.

Configuring an ACL

1. From the navigation tree, select **QoS** > **ACL IPv4**.
2. Click the **Add** tab.
3. Enter the ACL number **3000**, and then click **Apply**.

Figure 420 Adding ACL 3000

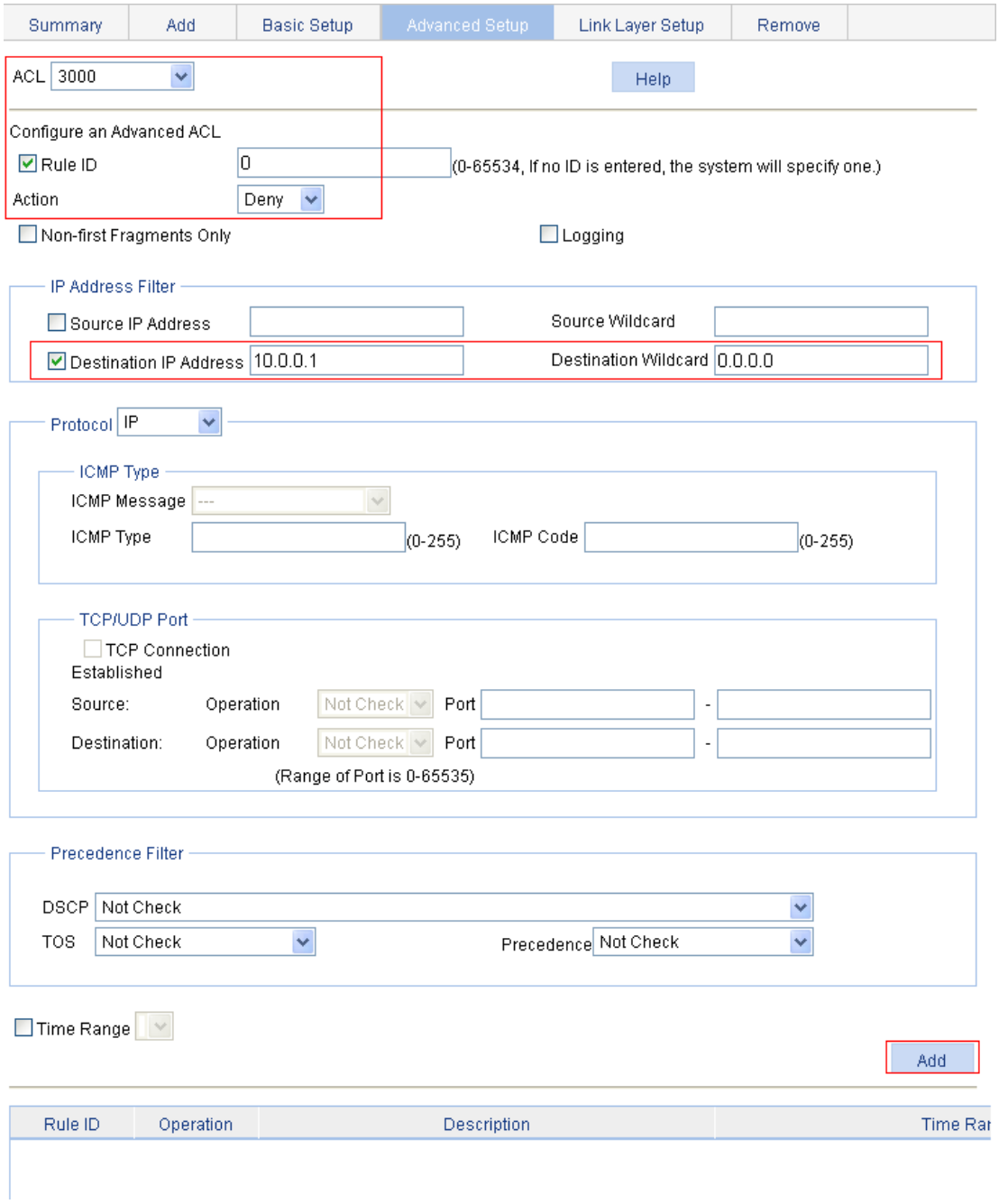


4. Click the **Advanced Setup** tab.
5. Configure the following parameters:
   a. Select the ACL **3000**.
   b. Select **Rule ID**, and enter the rule ID **0**.
   c. Select the action **Deny**.
   d. In the **IP Address Filter** area, select **Destination IP Address**:

- Enter the destination IP address **10.0.0.1**.
- Enter the destination address wildcard **0.0.0.0**.

e. Click **Add**.

Figure 421 Configuring an ACL rule

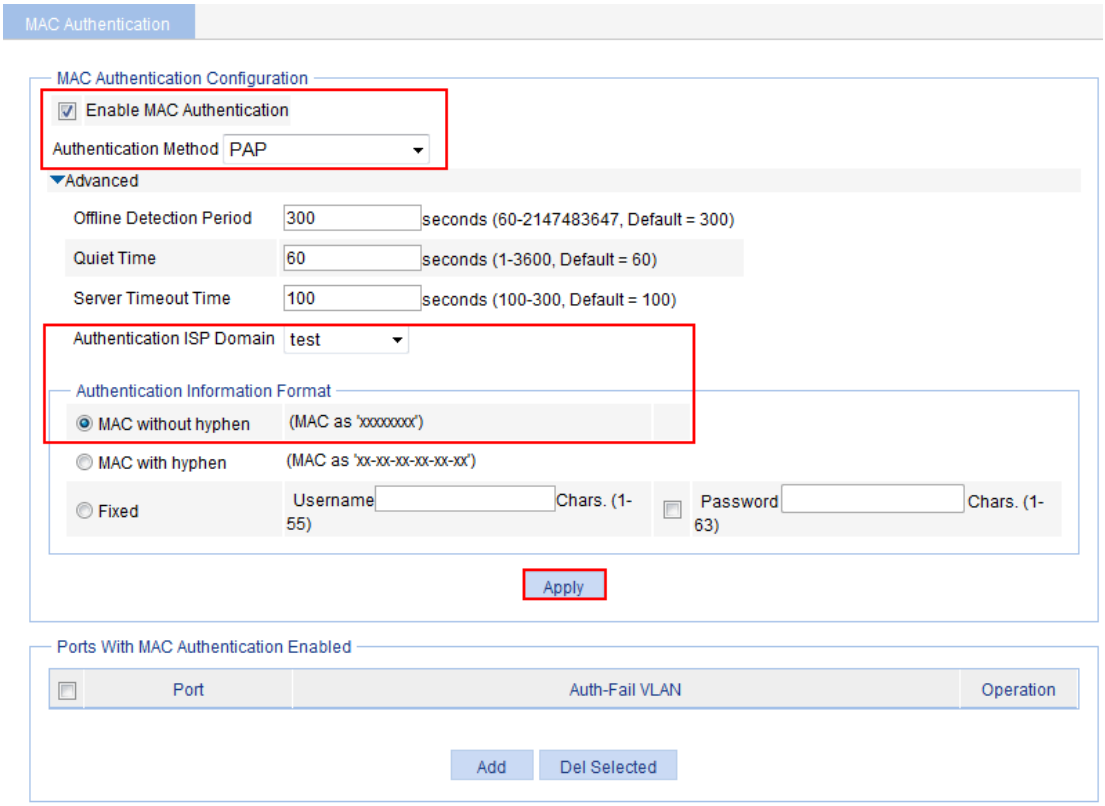


Configuring MAC authentication

1. Configure MAC authentication globally:
   a. From the navigation tree, select **Authentication** > **MAC Authentication**.
   b. Select **Enable MAC Authentication**.
   c. Select **PAP** from the **Authentication Method** list.
   d. Click **Advanced**.

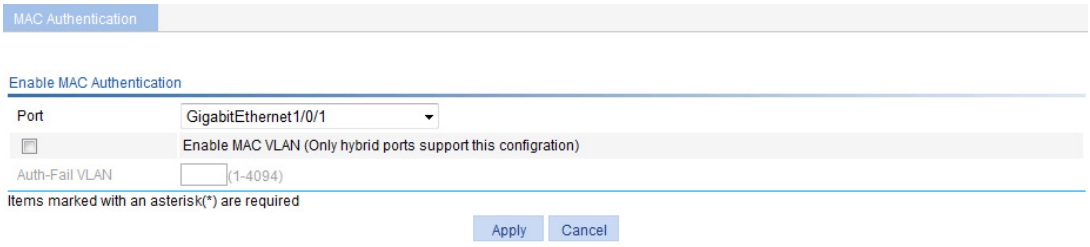
e. Select the authentication ISP domain **test**, select the authentication information format **MAC without hyphen**, and click **Apply**.

Figure 422 Configuring MAC authentication globally



2. Configure MAC authentication for GigabitEthernet 1/0/1:
   a. In the **Ports With MAC Authentication Enabled** area, click **Add**.
   b. Select the port **GigabitEthernet1/0/1**, and click **Apply**.

Figure 423 Enabling MAC authentication for port GigabitEthernet 1/0/1



Verifying the configuration

After the host passes authentication, ping the FTP server from the host to see whether ACL 3000 assigned by the authentication server takes effect.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

```
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Configuring port security

Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. It applies networks that require different authentication methods for different users on a port.

Port security prevents unauthorized access to a network by checking the source MAC address of inbound traffic and prevents access to unauthorized devices by checking the destination MAC address of outbound traffic.

Port security can control MAC address learning and authentication on a port to make sure the port learns only source trusted MAC addresses.

A frame is illegal if its source MAC address cannot be learned in a port security mode or if it is from a client that has failed 802.1X or MAC authentication. The port security feature automatically takes a predefined action on illegal frames. This automatic mechanism enhances network security and reduces human intervention.

For scenarios that require only 802.1X authentication or MAC authentication, Hewlett Packard Enterprise recommends that you configure 802.1X authentication or MAC authentication rather than port security for simplicity.

For more information about 802.1X and MAC authentication, see "Configuring 802.1X" and "Configuring MAC authentication."

Port security features

Outbound restriction

The outbound restriction feature is not supported in this release.

The outbound restriction feature prevents traffic interception by checking the destination MAC addresses in outbound frames. The feature guarantees that frames are sent only to devices that have passed authentication or whose MAC addresses have been learned or configured on the access device.

Intrusion protection

The intrusion protection feature checks the source MAC addresses in inbound frames for illegal frames and takes a predefined action on each detected illegal frames. The action can be disabling the port temporarily, disabling the port permanently, or blocking frames from the illegal MAC address for 3 minutes (not user configurable).

Port security traps

You can configure the port security module to send traps for port security events such as login, logoff, and MAC authentication. These traps help you monitor user behaviors.

Port security modes

Port security supports the following categories of security modes:

- **Basic mode**—In this mode, a port can learn the specified number of MAC addresses and save those addresses as secure MAC addresses. It permits only frames whose source MAC addresses are secure MAC addresses or configured static MAC addresses. When the number of secure MAC addresses reaches the upper limit, no more secure MAC addresses can be added.

- **Advanced mode**—Port security supports 802.1X and MAC authentication. Different port security modes represent different combinations of the two methods.

  Table 129 describes the advanced security modes.

  Table 129 Advanced security modes

Advanced mode	Description
MAC-Auth	A port performs MAC authentication for users. It services multiple users.
802.1X Port Based	A port performs 802.1X authentication and implements port-based access control. In this mode, a port can service multiple 802.1X users. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication. In this mode, neither outbound restriction nor intrusion protection will be triggered.
802.1X Single Host	A port performs 802.1X authentication and implements MAC-based access control. It services only one user passing 802.1X authentication.
802.1X MAC Based	A port performs 802.1X authentication of users and implements MAC-based access control. The port in this mode supports multiple online 802.1X users.
802.1X MAC Based Or OUI	Similar to the 802.1X Single Host mode, a port in this mode performs 802.1X authentication of users and allows only one 802.1X user to access at a time. • The port also permits frames from a wired terminal whose MAC address contains a specific OUI. • For frames from a wireless user, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication.
MAC-Auth Or 802.1X Single Host	This mode is the combination of the 802.1X Single Host and MAC-Auth modes, with 802.1X authentication having higher priority. • For wired users, the port performs MAC authentication upon receiving non-802.1X frames and performs 802.1X authentication upon receiving 802.1X frames. • For wireless users, 802.1X authentication is performed first. If 802.1X authentication fails, MAC authentication is performed.
MAC-Auth Or 802.1X MAC Based	Similar to the MAC-Auth Or 802.1X Single Host mode, except that it supports multiple 802.1X and MAC authentication users on the port.
MAC-Auth Else 802.1X Single Host	This mode is the combination of the MAC-Auth and 802.1X Single Host modes, with MAC authentication having higher priority. • A port in this mode performs only MAC authentication for non-802.1X frames. • For 802.1X frames, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.
MAC-Auth Else 802.1X MAC Based	Similar to the MAC-Auth Else 802.1X Single Host mode, except that it supports multiple 802.1X and MAC authentication users on the port.

The maximum number of users a port supports equals the maximum number of secure MAC addresses that port security allows or the maximum number of concurrent users the authentication mode in use allows, whichever is smaller.

An OUI is a 24-bit number that uniquely identifies a vendor, manufacturer, or organization. In MAC addresses, the first three octets are the OUI.

Configuration guidelines

When you configure port security, follow these restrictions and guidelines:

- Before you enable port security, disable 802.1X and MAC authentication globally.
- Only one port security mode can be configured on a port.
- The outbound restriction feature is not supported in this release.

Recommended configuration procedure

To configure basic port security mode:

Step	Remarks
1. Configuring global settings for port security	Required. This function enables port security globally and configures intrusion protection actions. By default, port security is disabled globally.
2. Configuring basic port security control	Required. This function configures the basic port security mode, maximum secure MAC addresses, intrusion protection, and outbound restriction for a port. By default, port security is disabled on all ports, and access to the ports is not restricted.
3. Configuring secure MAC addresses	Optional. Secure MAC addresses never age out or get lost if saved before the device restarts. One secure MAC address can be added to only one port in the same VLAN. You can bind a MAC address to one port in the same VLAN. Secure MAC addresses can be learned by a port in basic port security mode or manually configured in the Web interface. When the maximum number of secure MAC addresses is reached, no more can be added. The port allows only packets sourced from a secure MAC address to pass through. By default, no secure MAC addresses are configured.

To configure advanced port security mode:

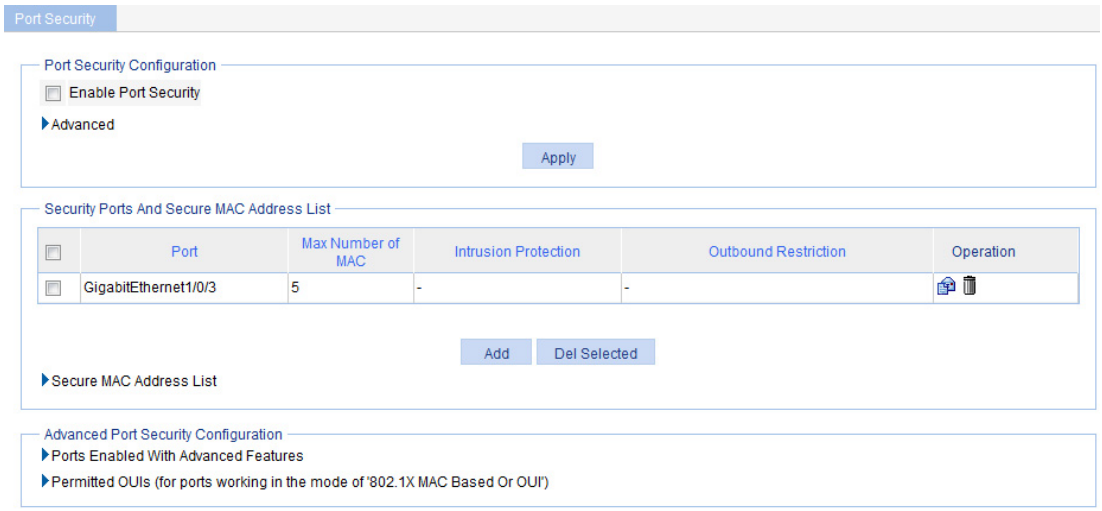
Step	Remarks
1. Configuring global settings for port security	Required. This function enables port security globally and configures intrusion protection actions. By default, port security is disabled globally.
2. Configuring advanced port security control	Required. This function configures the advanced port security mode, intrusion protection action, or outbound restriction, and selects whether to ignore the authorization information from the RADIUS server. By default, port security is disabled on all ports, and access to the ports is not restricted.

Step	Remarks
3. Configuring permitted OUIs	Optional. This setting is available only for the 802.1X MAC Based Or OUI mode. You can configure up to 16 permitted OUI values. A port in this mode allows only one 802.1X user and one user whose MAC address contains the specified OUI to pass authentication at the same time. By default, no OUI values are configured.

Configuring global settings for port security

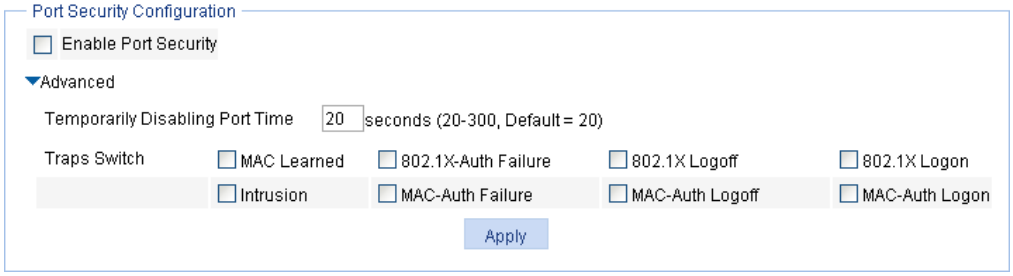
1. From the navigation tree, select **Authentication** > **Port Security**.

   Figure 424 Port security configuration page



2. In the **Port Security Configuration** area, click **Advanced**.

   Figure 425 Port security configuration



3. Configure global port security settings as described in Table 130.
4. Click **Apply**.

Table 130 Configuration items

Item	Description
Enable Port Security	Specifies whether to enable the port security feature globally. By default, port security is disabled.

Advanced	Configures intrusion protection actions globally.
	Intrusion protection actions:
	• **Temporarily Disabling Port Time**—Sets the time length for how long the port is disabled temporarily upon receiving illegal frames. **Traps Switch**—Selects one or more events to trigger trap sending. The following is the available events:
	  ○ **MAC Learned**.
	  ○ **802.1X-Auth Failure**.
	  ○ **8021X Logoff**.
	  ○ **802.1X Logon**.
	  ○ **Intrusion**.
	  ○ **MAC-Auth Failure**.
	  ○ **MAC-Auth Logoff**.
	  ○ **MAC-Auth Logon**.

Configuring basic port security control

1. From the navigation tree, select **Authentication** > **Port Security**.

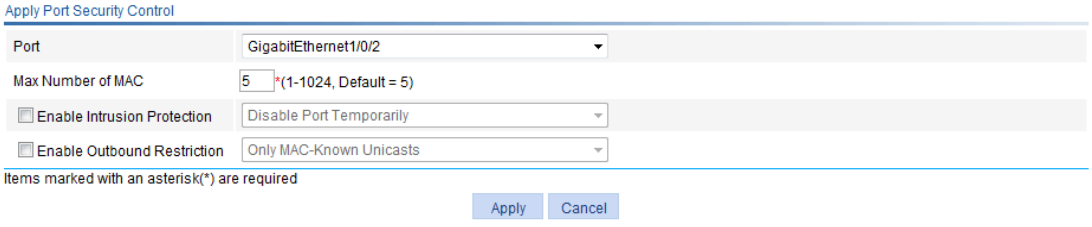
   On the **Port Security** page, the **Security Ports And Secure MAC Address List** area displays the port security control settings, as shown in Figure 426.

   Figure 426 Security Ports And Secure MAC Address List area

2. Click **Add**.

   The page for applying port security control appears.

   Figure 427 Configuring basic port security control



3. Configure basic port security control settings as described in Table 131.
4. Click **Apply**.

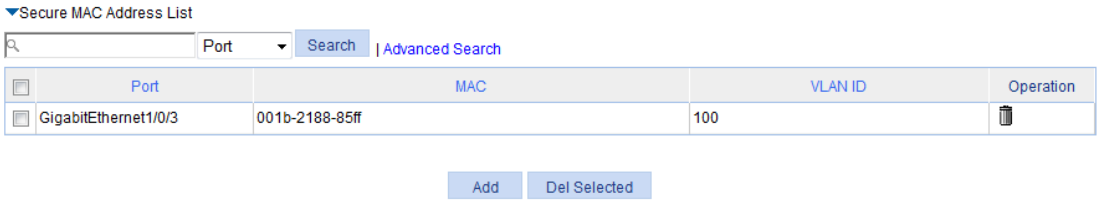
Table 131 Configuration items

Item	Description
Port	Selects a port where you want to configure port security. By default, port security is disabled on all ports, and access to the ports is not restricted.
Max Number of MAC	Sets the maximum number of secure MAC addresses on the port. The number of authenticated users on the port cannot exceed the specified upper limit. You can set the maximum number of MAC addresses that port security allows on a port for the following purposes: • Control the maximum number of concurrent users on the port. • Control the number of secure MAC addresses that can be added with port security. **NOTE:** The port security's limit on the maximum number of MAC addresses on a port is independent of the MAC learning limit in MAC address table management.
Enable Intrusion Protection	Specifies whether to enable intrusion protection, and selects an action to be taken on illegal frames. Available actions: • **Disable Port Temporarily**—Disables the port for a period of time. The period can be configured in the global settings. For more information, see "Configuring global settings for port security." • **Disable Port Permanently**—Disables the port permanently upon detecting an illegal frame received on the port. The port does not come up unless you bring it up manually. • **Block MAC**—Adds the source MAC addresses of illegal frames to the blocked MAC addresses list and discards the frames. All subsequent frames sourced from a blocked MAC address will be dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is not user configurable.
Enable Outbound Restriction	Specifies whether to enable outbound traffic control, and selects a control method. Available control methods: • **Only MAC-Known Unicasts**—Allows only unicast frames with their destination MAC addresses being authenticated to pass through. • **Only Broadcasts and MAC-Known Unicasts**—Allows only broadcast and unicast packets with their destination MAC addresses being authenticated to pass through. • **Only Broadcasts, Multicasts, and MAC-Known Unicasts**—Allows only broadcast, multicast, and known unicast packets with their destination MAC addresses being authenticated to pass through.

Configuring secure MAC addresses

1. From the navigation tree, select **Authentication** > **Port Security**.
   The **Port Security** page appears.
2. In the **Security Ports And Secure MAC Address List** area, click **Secure MAC Address List**.
   The secure MAC address configuration area displays the secure MAC addresses that have been learned or configured.

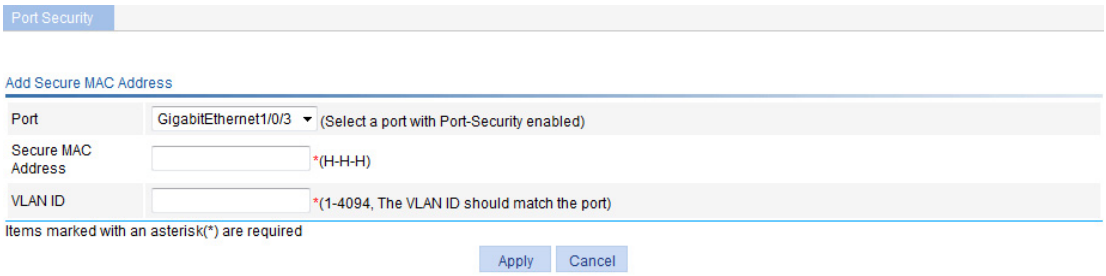
Figure 428 Secure MAC address list



3. Click **Add**.

   The page for adding a secure MAC address appears.

Figure 429 Adding secure MAC address



4. Configure a secure MAC address as described in Table 130.
5. Click **Apply**.

Table 132 Configuration items

Item	Description
Port	Selects a port where the secure MAC address is configured.
Secure MAC Address	Enters the MAC address that you want to configure as a secure MAC address.
VLAN ID	Enters the ID of the VLAN in which the secure MAC address is configured. The VLAN must already exist on the selected port.

Configuring advanced port security control

1. From the navigation tree, select **Authentication** > **Port Security**.

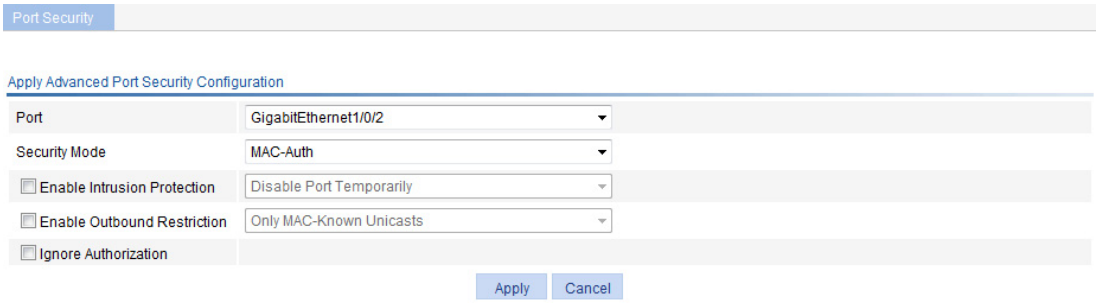
   The **Port Security** page appears.
2. In the **Advanced Port Security Configuration** area, click **Ports Enabled With Advanced Features**.

Figure 430 Ports Enabled With Advanced Features area

3. Click **Add**.

   The page for configuring advanced port security control appears.

Figure 431 Configuring advanced port security control



4. Configure advanced port security control as described in Table 133.
5. Click **Apply**.

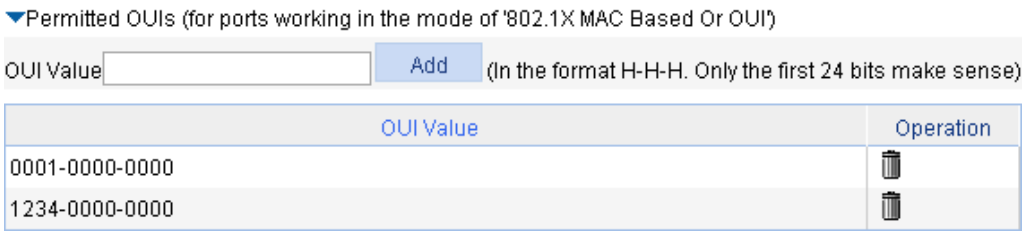
Table 133 Configuration items

Item	Description
Port	Selects a port where you want to configure port security. By default, port security is disabled on all ports, and access to the ports is not restricted.
Security Mode	Selects a port security mode. For more information about advanced security modes, see Table 129.
Enable Intrusion Protection	Specifies whether to enable intrusion protection, and selects an action to be taken upon detection of illegal frames. Available actions: • **Disable Port Temporarily**—Disables the port for a period of time. The period can be configured in the global settings. For more information, see "Configuring global settings for port security." • **Disable Port Permanently**—Disables the port permanently upon detecting an illegal frame received on the port. The port does not come up unless you bring it up manually. • **Block MAC**—Adds the source MAC addresses of illegal frames to the blocked MAC addresses list and discards the frames. All subsequent frames sourced from a blocked source MAC address will be dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is fixed and cannot be changed.
Enable Outbound Restriction	Specifies whether to enable the outbound traffic control, and selects a control method. Available control methods: • **Only MAC-Known Unicasts**—Allows only unicasts frames with their destination MAC addresses being authenticated to pass through. • **Only Broadcasts and MAC-Known Unicasts**—Allows only broadcast and unicasts packets with their destination MAC addresses being authenticated to pass through. • **Only Broadcasts, Multicasts, and MAC-Known Unicasts**—Allows only broadcast, multicast, and unicasts packets with their destination MAC addresses being authenticated to pass through.
Ignore Authorization	Specifies whether to configure the port to ignore the authorization information from the authentication server. The authorization information is delivered by the authentication server to the device after an 802.1X user or MAC authenticated user passes authentication.

Configuring permitted OUIs

1. From the navigation tree, select **Authentication** > **Port Security**.
   The **Port Security** page as shown in Figure 424 appears.
2. In the **Advanced Port Security Configuration** area, click **Permitted OUIs**.

Figure 432 Permitted OUIs



3. Enter the 48-bit MAC address in the format of H-H-H in the **OUI Value** field.
4. Click **Add**.
   The system automatically saves the first 24 bits as an OUI value.

Port security configuration examples

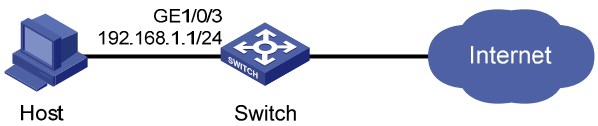
Basic port security mode configuration example

Network requirements

As shown in Figure 433, configure port GigabitEthernet 1/0/3 of the switch as follows:

- Allow up to three users to access the port without authentication, and permit the port to learn the MAC addresses of the users as secure MAC addresses.
- After the number of secure MAC addresses reaches 3, the port stops learning MAC addresses. If an unknown MAC address frame arrives, intrusion protection is triggered and the port is disabled and stays silence for 30 seconds.

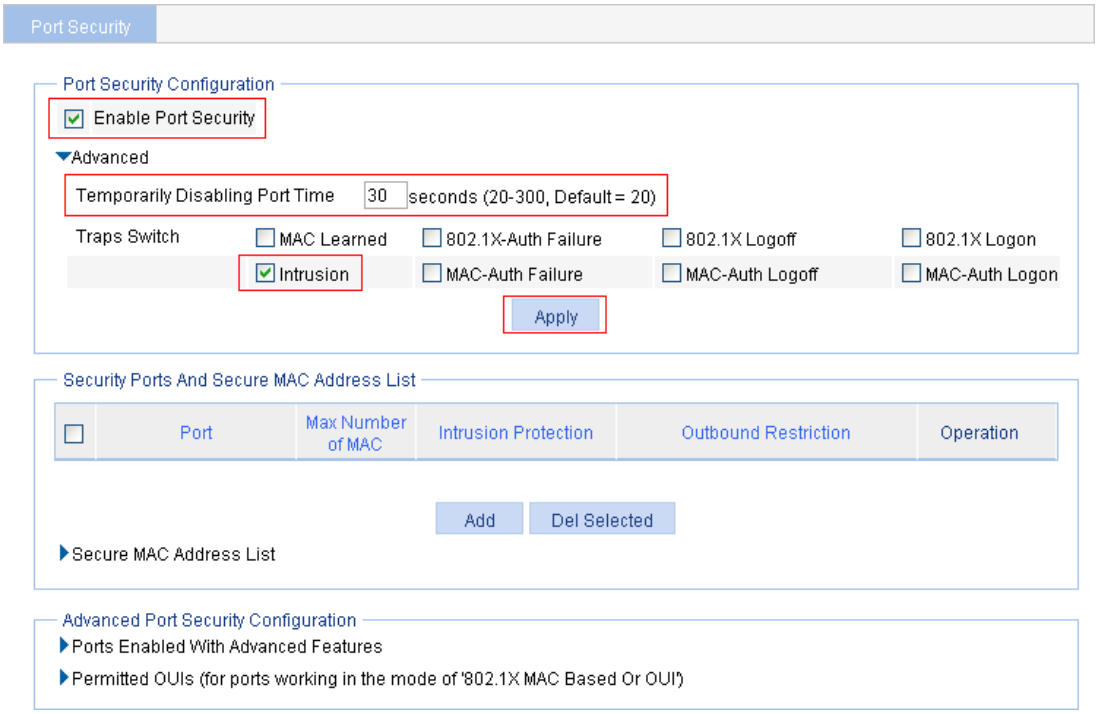
Figure 433 Network diagram



Configuring global port security settings

1. From the navigation tree, select **Authentication** > **Port Security**.
2. In the **Port Security Configuration** area, configure global port security settings:
   a. Select **Enable Port Security**.
   b. Click **Advanced**.
   c. Specify the system to disable the port temporarily for **30** seconds.
   d. Select **Intrusion** from the **Trap Switch** area.
   e. Click **Apply**.

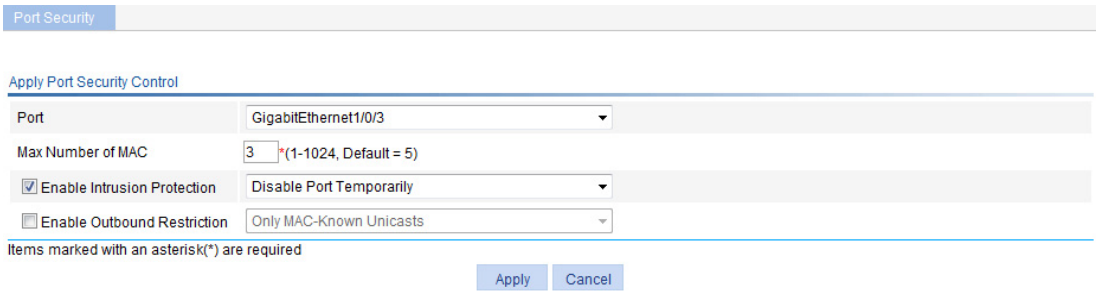
Figure 434 Configuring port security



Configuring the basic port security control

1. In the **Security Ports And Secure MAC Address List** area, click **Add**.
2. On the page that appears, select **GigabitEthernet1/0/3**.
3. Enter **3** as the maximum number of MAC addresses.
4. Select **Enable Intrusion Protection**, and select **Disable Port Temporarily** from the list.
5. Click **Apply**.

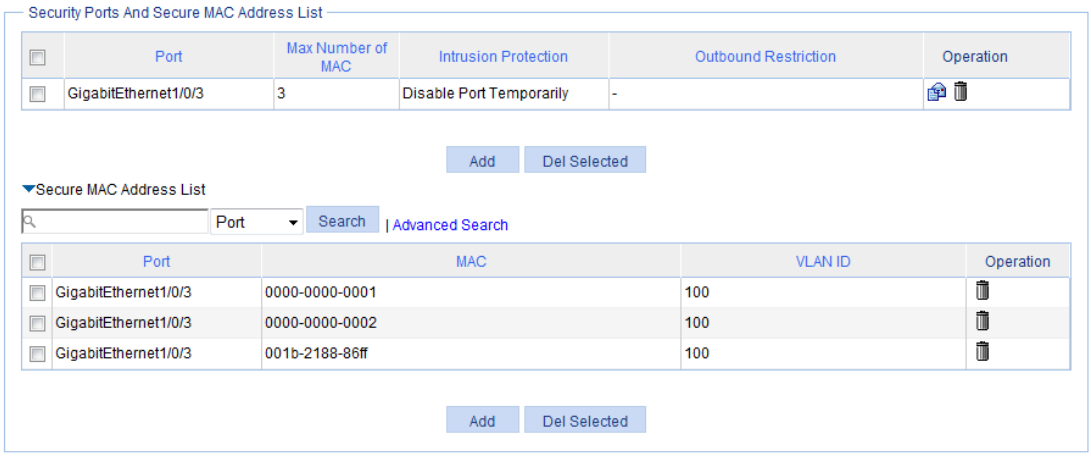
Figure 435 Applying the port security feature



Verifying the configuration

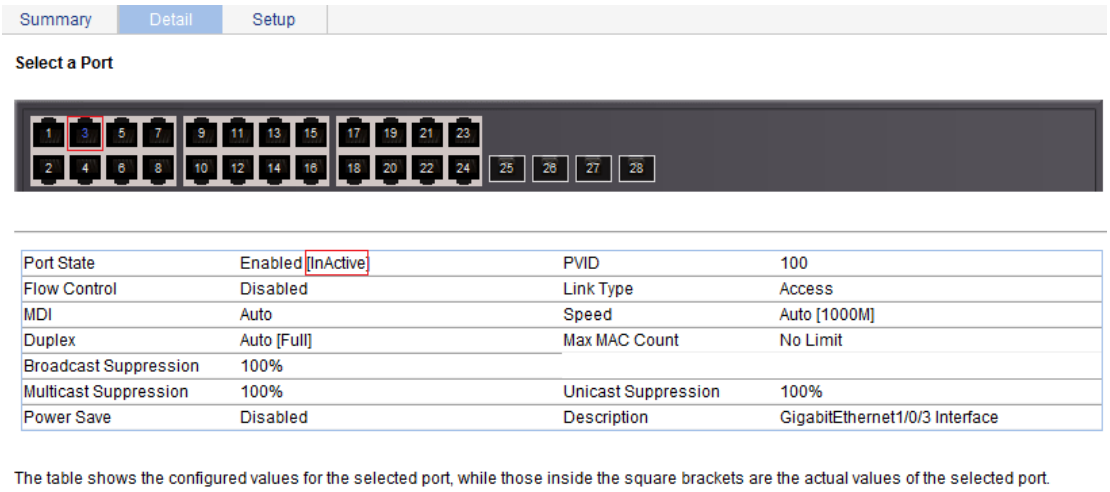
1. Display the secure MAC address entries learned and manually configured on port GigabitEthernet 1/0/3. The maximum number of secure MAC is configured as 3, so up to 3 MAC addresses can be learned and added as secure MAC addresses, as shown in Figure 436.

Figure 436 Secure MAC address list



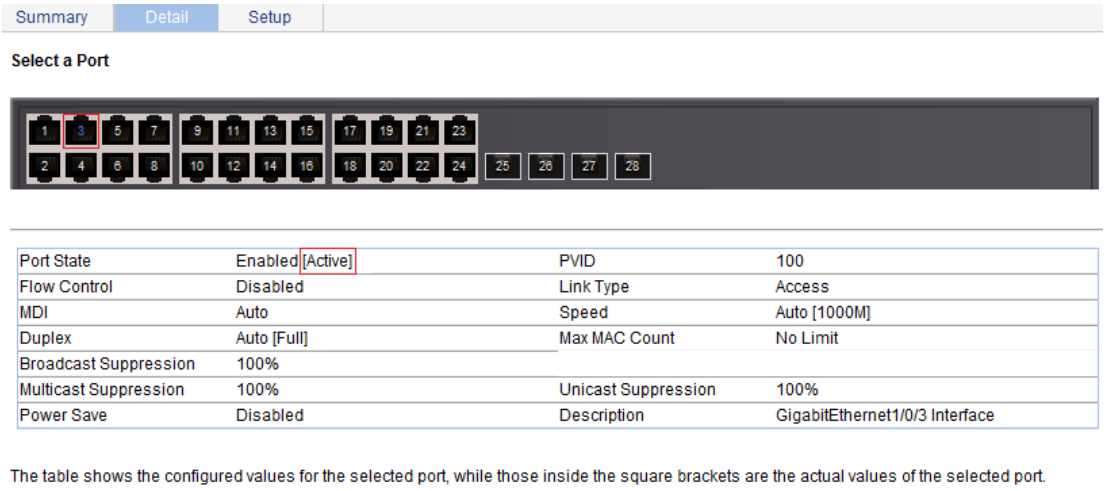
2. When the maximum number of MAC addresses is reached, intrusion protection is triggered. Select **Device** > **Port Management** from the navigation tree, and then select the **Detail** tab. On the page, click the target port (GigabitEthernet 1/0/3 in this example) to view details. Figure 437 shows that the port state is inactive.

Figure 437 Displaying port state



3. Re-select GigabitEthernet 1/0/3 to refresh its data 30 seconds later. Figure 438 shows that the port state is active.

Figure 438 Displaying port state



If you remove MAC addresses from the secure MAC address list, the port can continue to learn MAC addresses.

Advanced port security mode configuration example

Network requirements

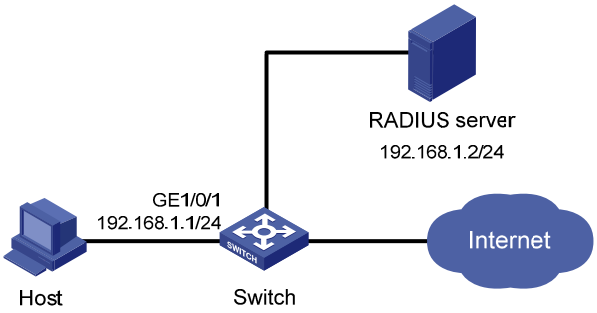
As shown in Figure 439, the switch authenticates the client with a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

- The RADIUS server at 192.168.1.2 functions as the primary authentication server and the secondary accounting server, and the RADIUS server at 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is **name**, and the shared key for accounting is **money**.
- All users use the default authentication, authorization, and accounting methods of ISP domain **system**.
- The switch sends usernames without domain names to the RADIUS server.

Configure port GigabitEthernet 1/0/1 of the switch to perform the following operations:

- Allow only one 802.1X user to be authenticated.
- Allow up to three OUI values to be configured, and allow one terminal that uses any of the OUI values to access the port.

Figure 439 Network diagram



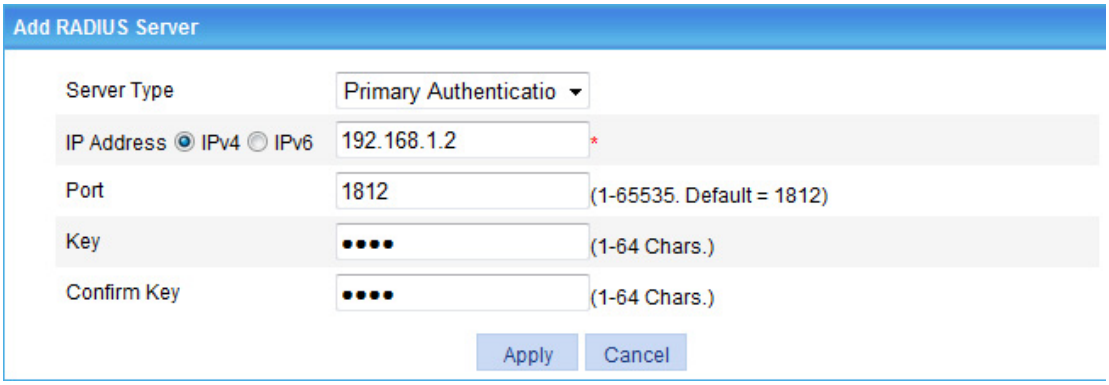
NOTE:

Configurations on the host and RADIUS servers are not shown.

Configuring a RADIUS scheme

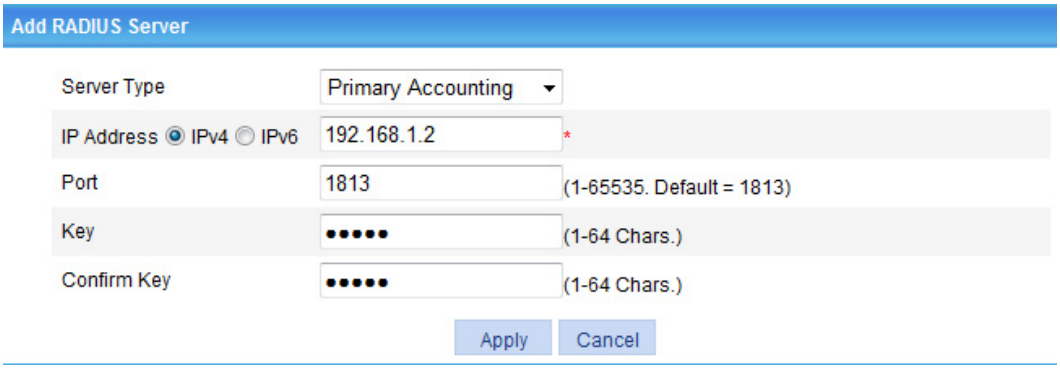
1. Create a RADIUS scheme:
   a. From the navigation tree, select **Authentication** > **RADIUS**.
   b. Click **Add**.
   c. On the page that appears, configure a RADIUS scheme:
      – Enter the scheme name **system**.
      – Select the service type **Extended**.
      – Select **Without domain name** from the **Username Format** list.
   d. Click **Apply**.
2. Configure the primary authentication server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Configure the primary authentication server:
      – Select the server type **Primary Authentication**.
      – Enter the IP address **192.168.1.2**, and enter the port number **1812**.
      – Enter **name** in both the **Key** field and the **Confirm Key** field.
   c. Click **Apply**.

Figure 440 Configuring the RADIUS authentication server



3. Configure the primary accounting server in the RADIUS scheme:
   a. In the **RADIUS Server Configuration** area, click **Add**.
   b. Configure the primary accounting server:
      – Select the server type **Primary Accounting**.
      – Enter the IP address **192.168.1.2**, and enter the port number **1813**.
      – Enter **money** in both the **Key** field and the **Confirm Key** field.

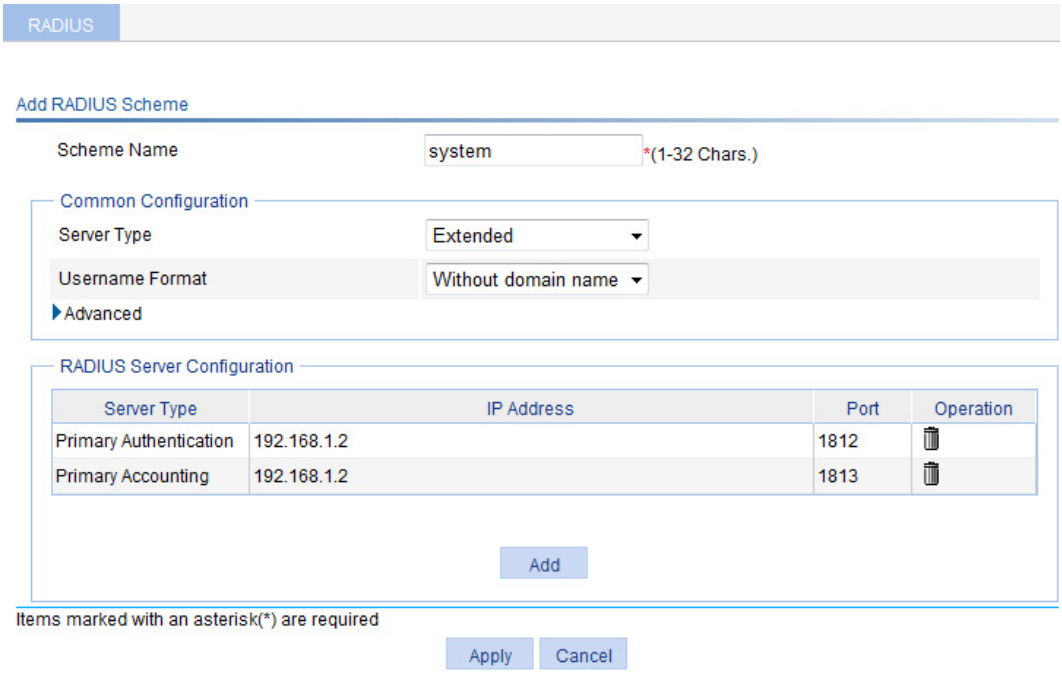
Figure 441 Configuring the RADIUS accounting server



c. Click **Apply**.

The **RADIUS Server Configuration** area displays the servers you have configured, as shown in Figure 442.

Figure 442 Configuring the RADIUS scheme

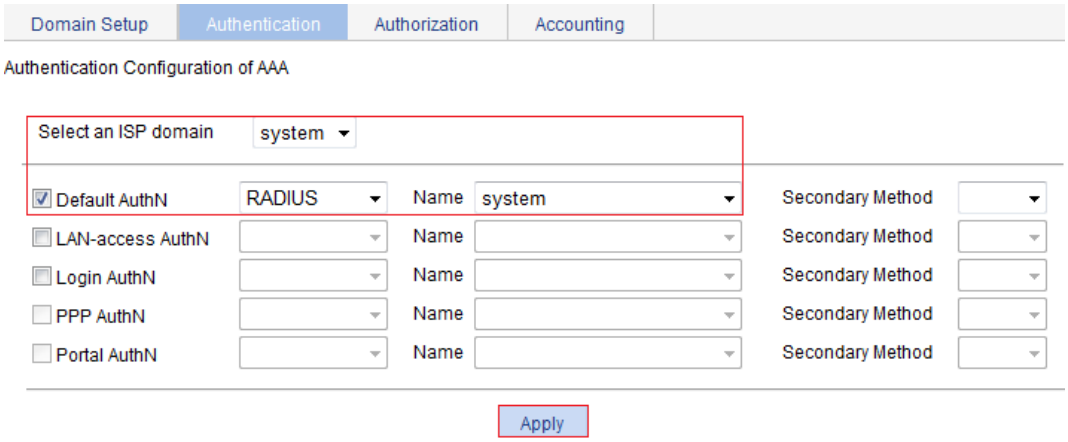


4. Click **Apply**.

Configuring AAA

1. Configure AAA authentication method:
   a. From the navigation tree, select **Authentication** > **AAA**.
   b. Click the **Authentication** tab.
   c. Select the ISP domain **system**.
   d. Select **Default AuthN**, select the authentication method **RADIUS** from the list, and select authentication scheme **system** from the **Name** list.

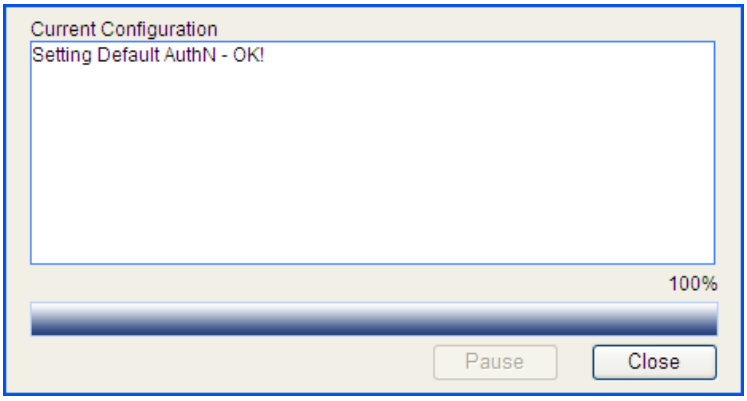
Figure 443 Configuring AAA authentication



e. Click **Apply**.

A dialog box appears, displaying the configuration progress, as shown in Figure 444.

Figure 444 Configuration progress dialog box



f. When the configuration process is complete, click **Close**.

2. Configure AAA authorization method:

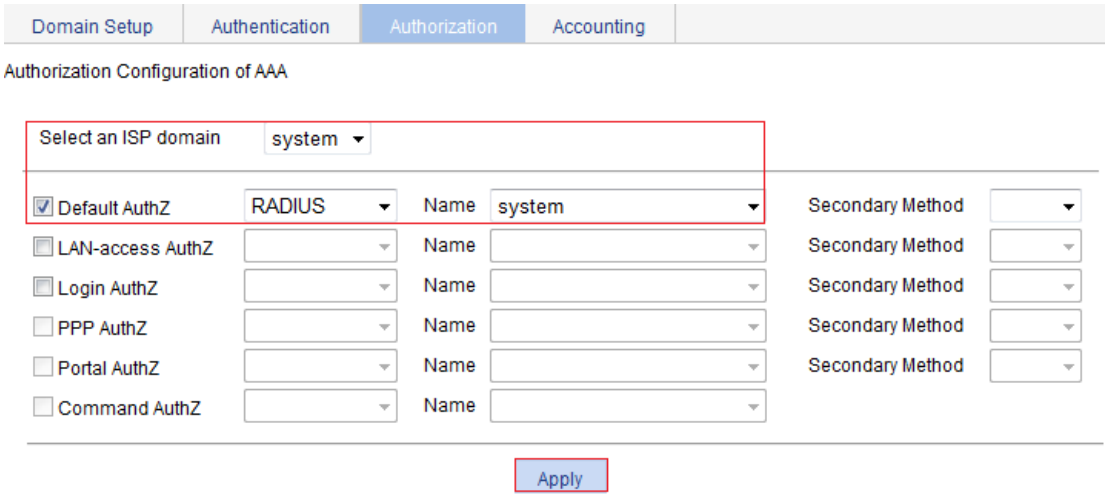
a. Click the **Authorization** tab.

b. Select the ISP domain **system**.

c. Select **Default AuthZ**, select authorization method **RADIUS** from the list, and select the authorization scheme **system** from the **Name** list.

d. Click **Apply**.

Figure 445 Configuring AAA authorization



e. When the configuration process is complete, click **Close**.

3. Configure AAA accounting method:

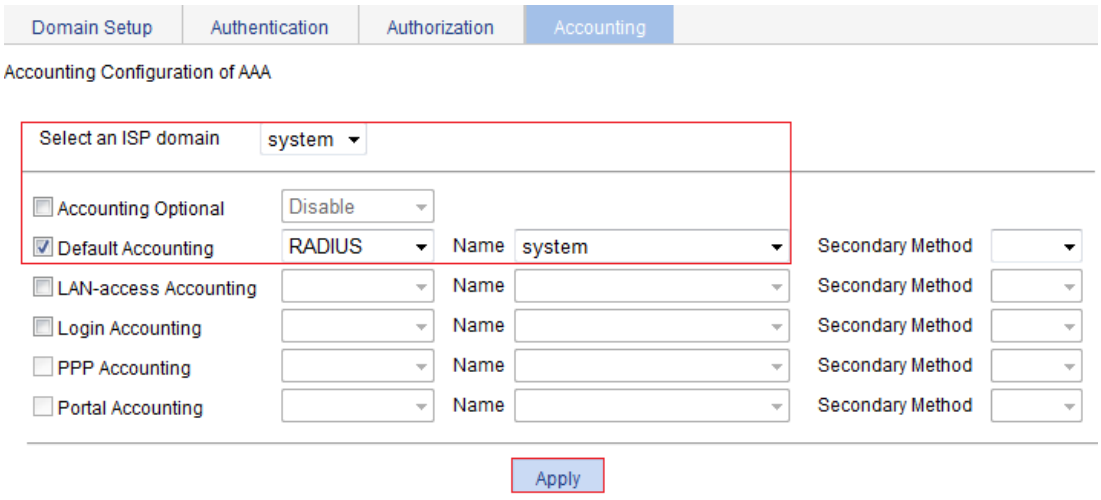
a. Click the **Accounting** tab.

b. Select the ISP domain **system**.

c. Select **Default Accounting**, select the accounting method **RADIUS** from the list, and select the accounting scheme **system** from the **Name** list.

d. Click **Apply**.

Figure 446 Configuring AAA accounting



e. When the configuration process is complete, click **Close**.

Configuring port security

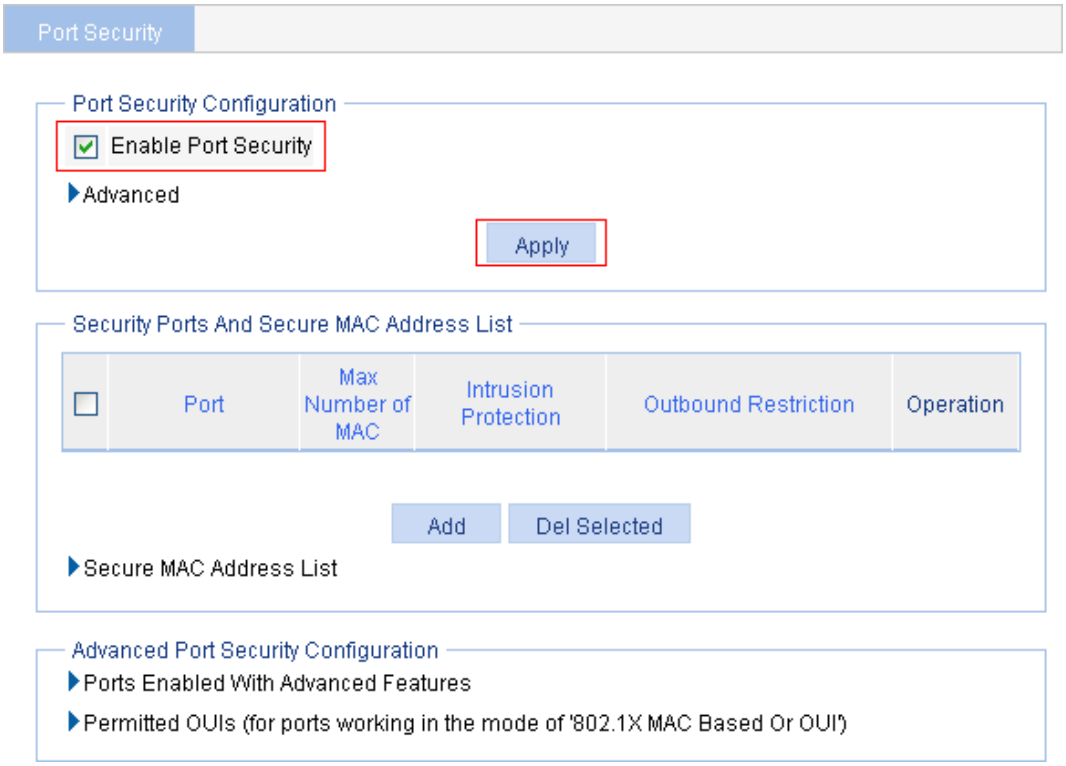
1. Enable port security:

a. From the navigation tree, select **Authentication** > **Port Security**.

b. Select **Enable Port Security**.

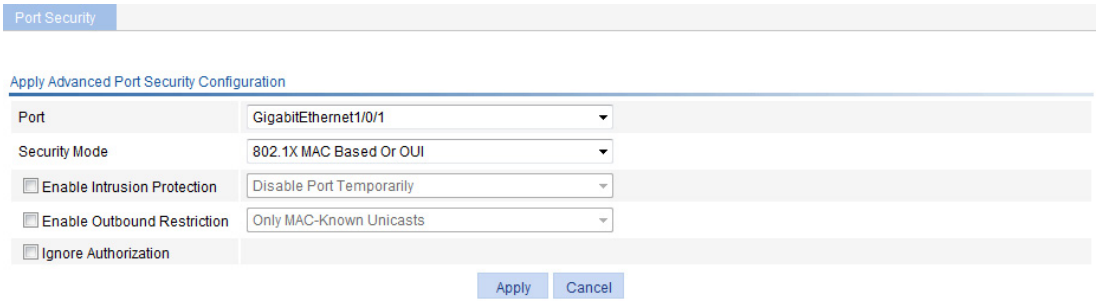
c. Click **Apply**.

Figure 447 Configuring global port security settings



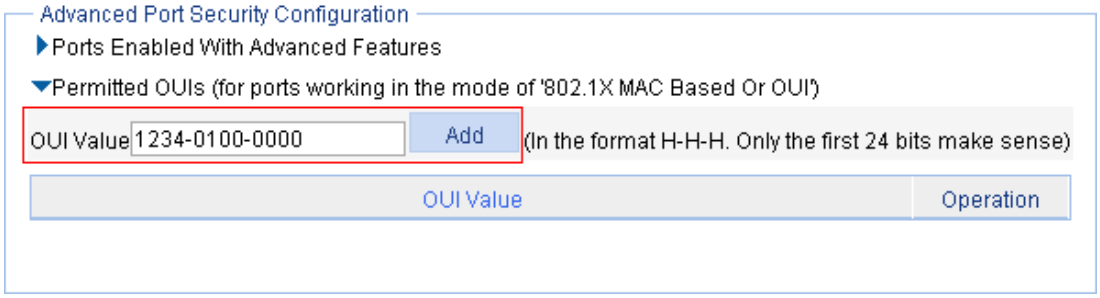
2. Configure advanced port security control:
   a. In the **Advanced Port Security Configuration** area, click **Ports Enabled With Advanced Features**, and then click **Add**.
   b. Select **GigabitEthernet1/0/1** from the **Port** list, and select **802.1X MAC Based Or OUI** from the **Security Mode** list.
   c. Click **Apply**.

Figure 448 Configuring advanced port security control settings on GigabitEthernet 1/0/1



3. Add permitted OUIs:
   a. In the **Advanced Port Security Configuration** area, click **Permitted OUIs**.
   b. Enter **1234-0100-0000** in the **OUI Value** field.
   c. Click **Add**.

Figure 449 Configuring permitted OUI values



d. Repeat previous three steps to add the OUI values of the MAC addresses **1234-0200-0000** and **1234-0300-0000**.

Configuring port isolation

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs. You can also use this feature to isolate the hosts in a VLAN from one another.

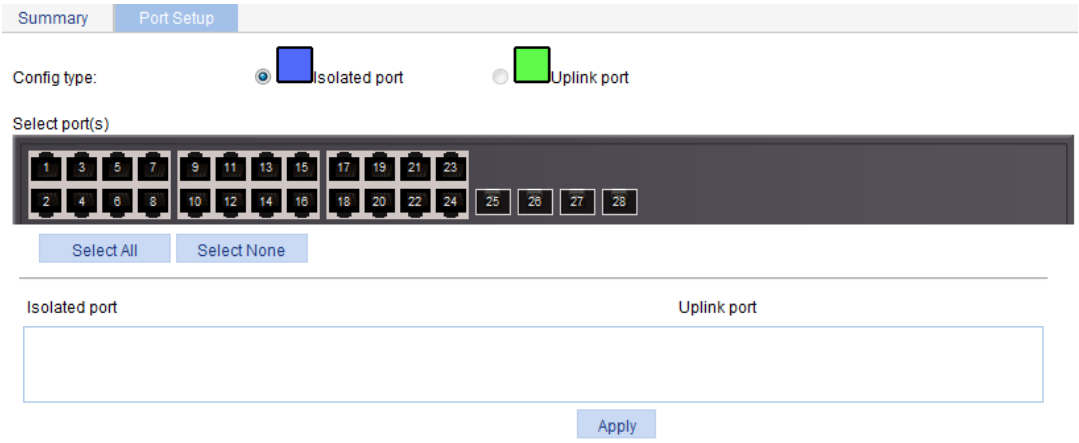
The switch supports only one isolation group that is automatically created as isolation group 1. You cannot remove the isolation group or create other isolation groups on the device. The number of ports assigned to the isolation group is not limited.

Within the same VLAN, ports in an isolation group can communicate with those outside the isolation group at Layer 2.

Configuring the isolation group

1. Select **Security** > **Port Isolate Group** from the navigation tree.
2. Click the **Port Setup** tab.

Figure 450 Configuring the port isolation group



3. Configure the port isolation group as described in Table 134.
4. Click **Apply**.

Table 134 Configuration items

Item	Description
Config type	Specify the role of the ports to be assigned to the isolation group: • **Isolated port**—Assign the ports to the isolation group as isolated ports. • **Uplink port**—Assign the port to the isolation group as the uplink port. The switch does not support the **Uplink port** config type.
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 be listed under the chassis panel for selection.

Port isolation configuration example

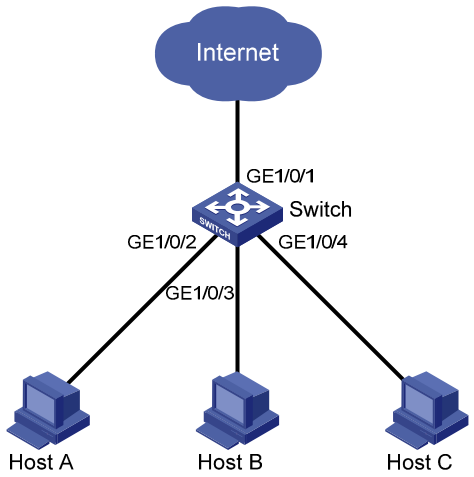
Network requirements

As shown in Figure 451:

- 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 so that they can access the external network but are isolated from one another at Layer 2.

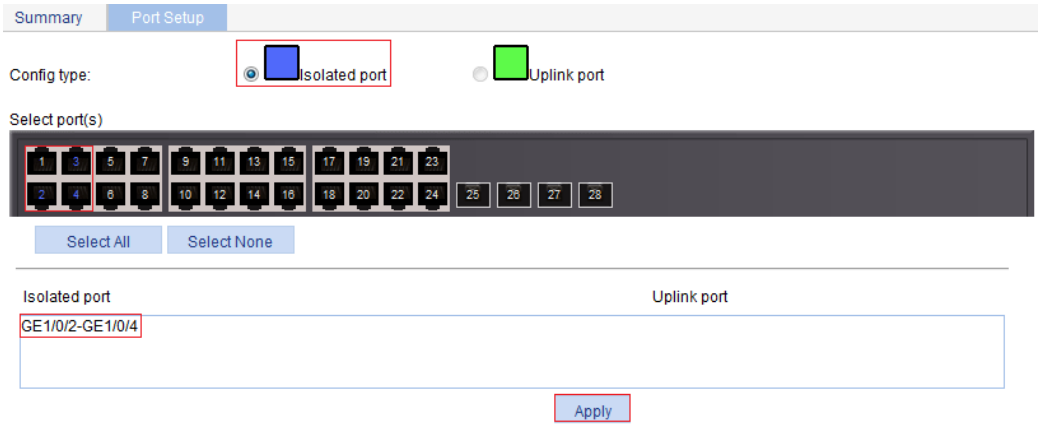
Figure 451 Networking diagram



Configuring the switch

1. Assign ports 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.
   c. Select **Isolated port** for **Config Type**.
   d. Select **2**, **3**, **4** on the chassis front panel. **2**, **3**, **4** represent ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4, respectively.

Figure 452 Assigning ports to the isolation group



e. Click **Apply**.

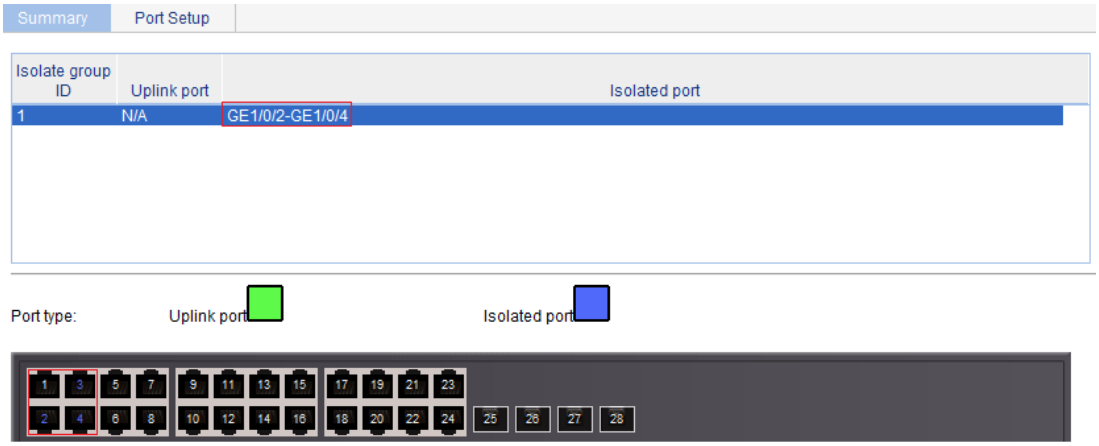
A configuration progress dialog box appears.

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

Viewing information about the isolation group

1. Click **Summary**.
2. Display port isolation group 1, which contains ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.

Figure 453 Viewing information about port isolation group 1



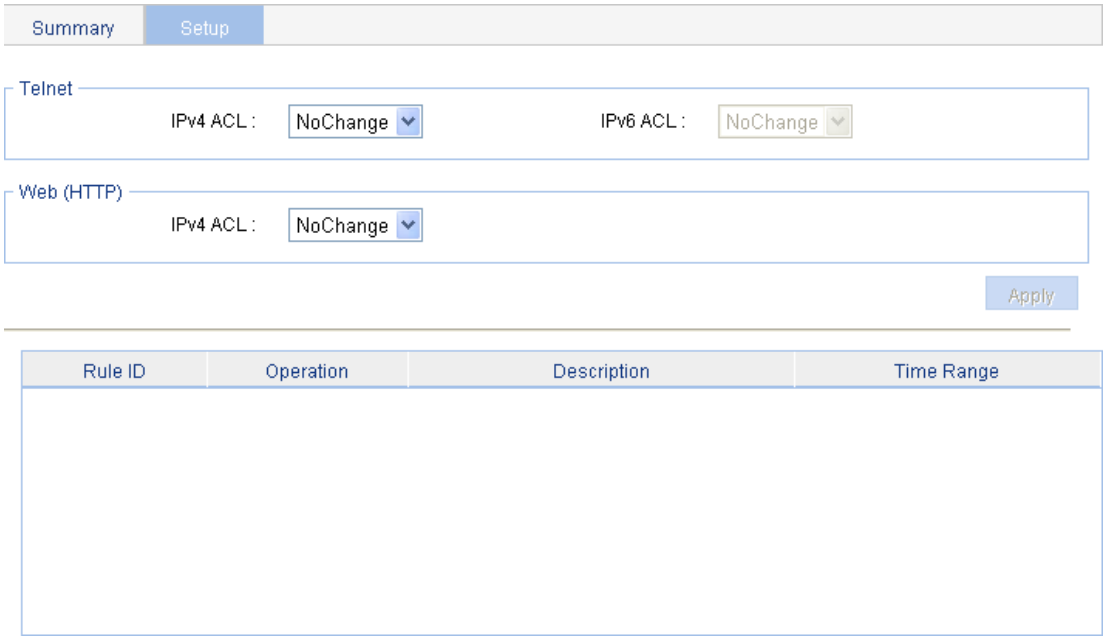
Configuring authorized IP

The authorized IP function associates 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.

Configuration procedure

1. From the navigation tree, select **Security** > **Authorized IP**.
2. Click **Setup** to enter the authorized IP configuration page.

Figure 454 Authorized IP configuration page



3. Configure authorized IP as described in Table 135.
4. Click **Apply**.

Table 135 Configuration items

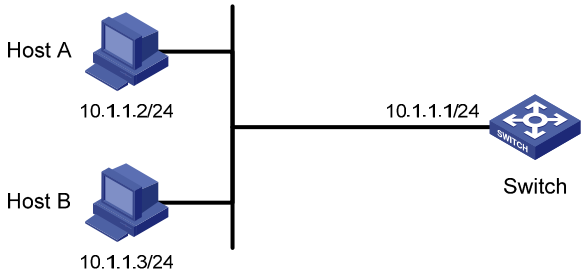
Item		Description
Telnet	IPv4 ACL	Associate the Telnet service with an IPv4 ACL. To configure the IPv4 ACL to be selected, select **QoS** > **ACL IPv4**.
	IPv6 ACL	Associate the Telnet service with an IPv6 ACL. To configure the IPv6 ACL to be selected, select **QoS** > **ACL IPv6**.
Web (HTTP)	IPv4 ACL	Associate the HTTP service with an IPv4 ACL. To configure the IPv4 ACL to be selected, select **QoS** > **ACL IPv4**.

Authorized IP configuration example

Network requirements

In Figure 455, configure Switch to deny Telnet and HTTP requests from Host A, and permit Telnet and HTTP requests from Host B.

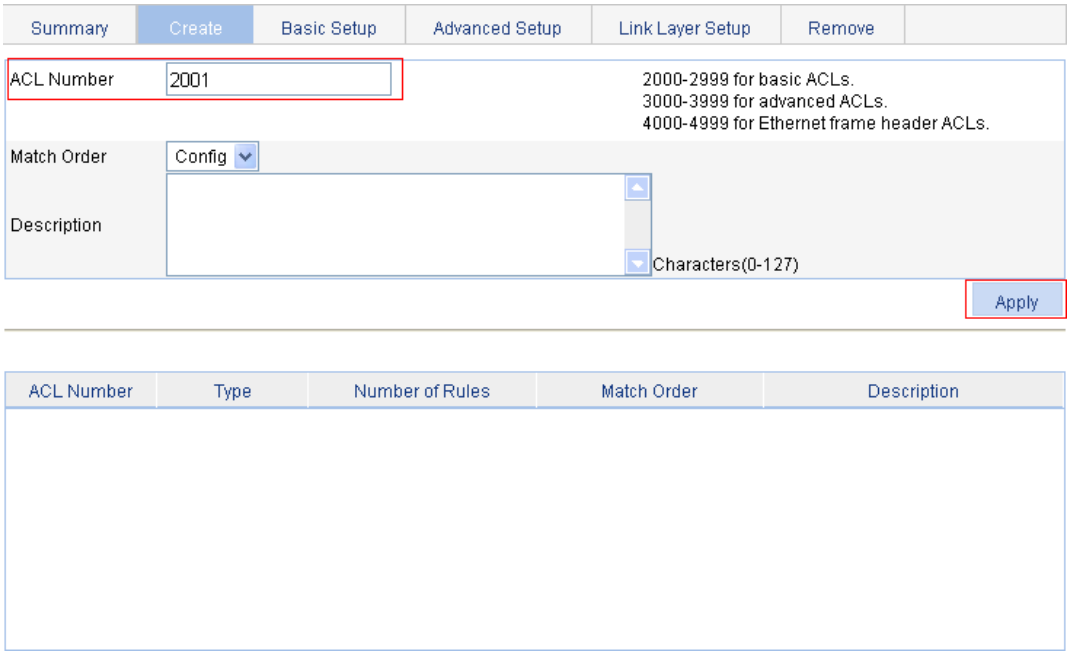
Figure 455 Network diagram



Configuration procedure

1. Create an ACL:
   a. From the navigation tree, select **QoS** > **ACL IPv4**.
   b. Click **Create**.
   c. Enter **2001** for **ACL Number**.
   d. Click **Apply**.

   Figure 456 Creating an ACL

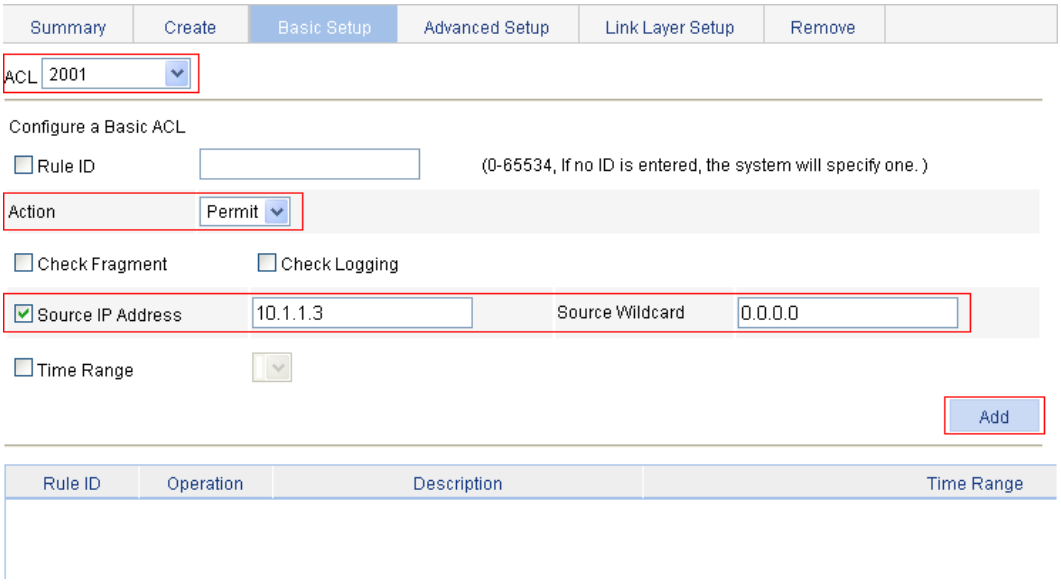


2. Configure an ACL rule to permit Host B:
   a. Click **Basic Setup**.
      The page for configuring an ACL rule appears.

b. Select 2001 from the **ACL** list, select **Permit** from the **Action** list, select the **Source IP Address** box and enter **10.1.1.3**, and then enter **0.0.0.0** in the **Source Wildcard** field.

c. Click **Add**.

Figure 457 Configuring an ACL rule to permit Host B



3. Configure authorized IP:

a. From the navigation tree, select **Security** > **Authorized IP**.

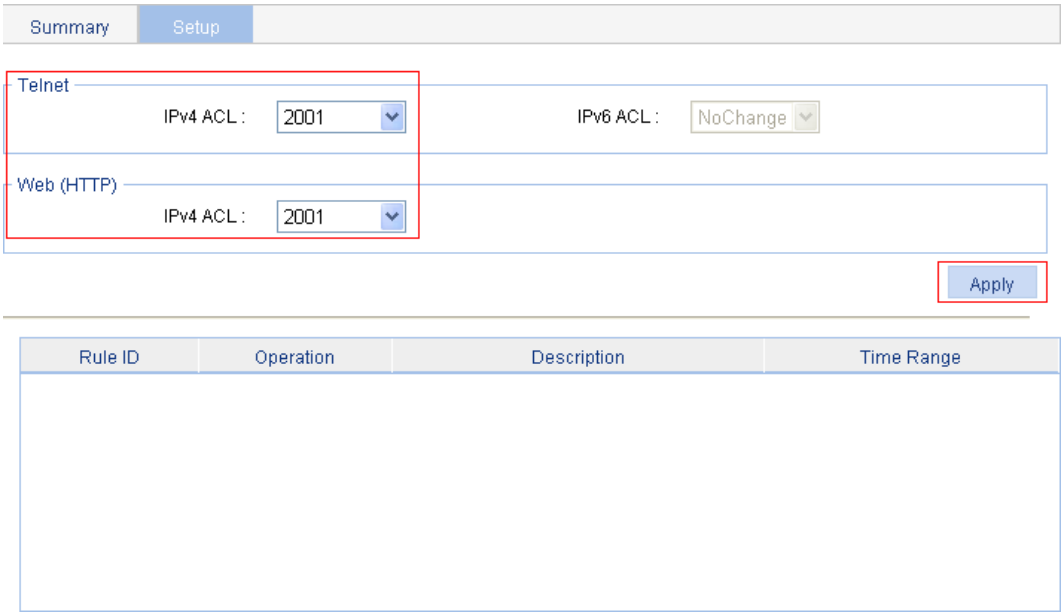
b. Click **Setup**.

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 458 Configuring authorized IP



Configuring loopback detection

A loop occurs when a port receives a packet sent by itself. Loops might cause broadcast storms. The purpose of loopback detection is to detect loops on ports.

With loopback detection enabled on an Ethernet port, the device periodically checks for loops on the port. If the device detects a loop on the port, it operates on the port according to the preconfigured loopback detection actions.

When the device detects a loop on an access port, it disables the port from forwarding data packets, sends a trap message to the terminal, and deletes the corresponding MAC address forwarding entry.

When the device detects a loop on a trunk port or a hybrid port, it sends a trap message to the terminal. If loopback detection control is also enabled on the port, the device disables the port from forwarding data packets, sends a trap message to the terminal, and deletes the corresponding MAC address forwarding entry.

Recommended configuration procedure

Step	Remarks
1. Configuring loopback detection globally	Required. By default, loopback detection is disabled globally.
2. Configuring loopback detection on a port	Required. By default, loopback detection is disabled on a port.

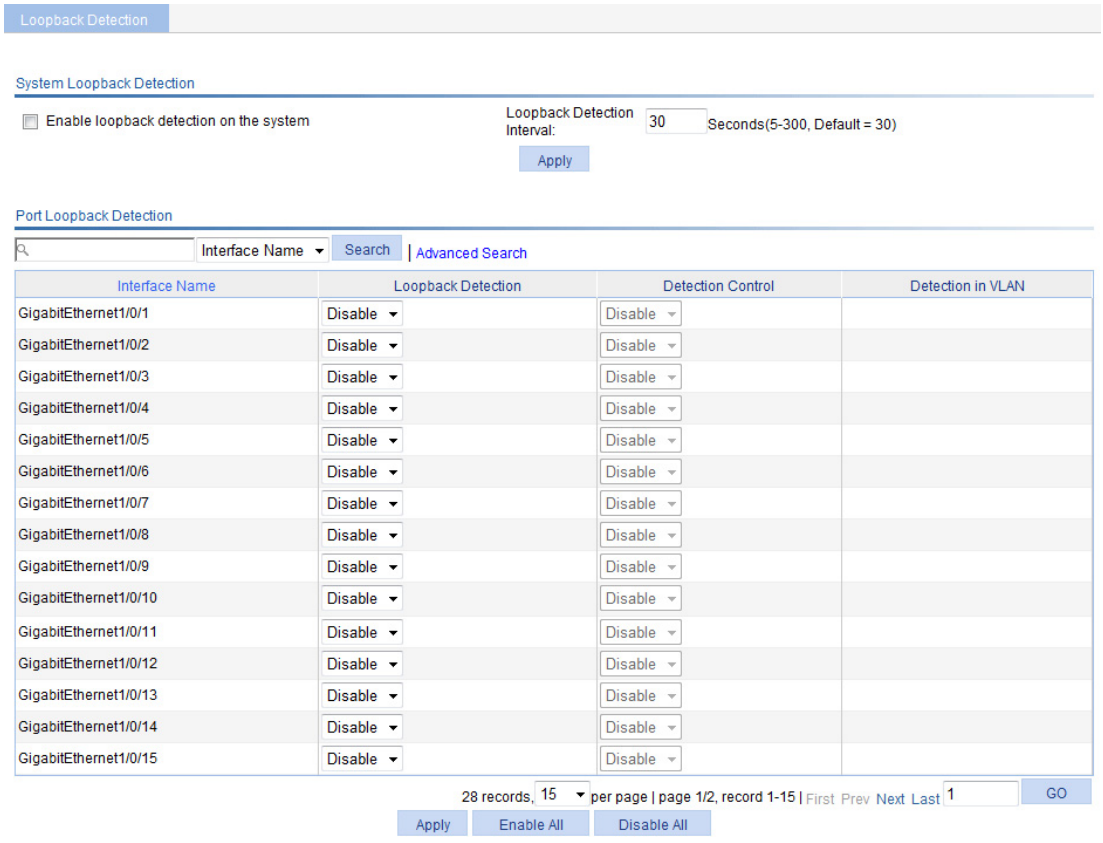
NOTE:

Loopback detection takes effect on a port only after you enable loopback detection both globally and on the port.

Configuring loopback detection globally

1. From the navigation tree, select **Security** > **Loopback Detection**.
   The **System Loopback Detection** area appears.

Figure 459 Loopback detection configuration page



2. Configure the global loopback detection settings as described in Table 136, and then click **Apply**.

Table 136 Configuration items

Item	Description
Enable loopback detection on the system	Sets whether to enable loopback detection globally.
Loopback Detection Interval	Sets the loopback detection interval.

Configuring loopback detection on a port

1. From the navigation tree, select **Security** > **Loopback Detection**.

   The **Port Loopback Detection** area appears.
2. Configure loopback detection on a port as described on Table 137, and then click **Apply**.

Table 137 Configuration items

Item	Description
Loopback Detection	Sets whether to enable loopback detection on the target port.
Detection Control	Sets whether the system disables the target trunk or hybrid port from forwarding data packets when the device detects a loop on it. This configuration item is available only for a trunk or hybrid port.

Item	Description
Detection in VLAN	Sets whether the system performs loopback detection in all VLANs for the target trunk or hybrid port. If you select **Disable**, the system performs loopback detection only in the default VLAN of the target trunk or hybrid port. This configuration item is available only for a trunk or hybrid port.

Configuring ACLs

Unless otherwise stated, ACLs refer to both IPv4 and IPv6 ACLs throughout this document. Grayed-out options on Web configuration pages cannot be configured.

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

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, protocol number, and other Layer 3 and Layer 4 header fields
		IPv6	Source/destination IPv6 address, protocol number, 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 method, check the rule content and order carefully.
- **Auto**—Sorts ACL rules in depth-first order. Depth-first ordering makes sure any subset of a rule is always matched before the rule. Table 138 lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

Table 138 Depth-first match for ACLs

ACL category	Sequence of tie breakers
IPv4 basic ACL	1. More 0s in the source IP address wildcard (more 0s means a narrower IP address range). 2. Smaller rule ID.
IPv4 advanced ACL	1. Specific protocol number. 2. More 0s in the source IP address wildcard mask. 3. More 0s in the destination IP address wildcard. 4. Narrower TCP/UDP service port number range. 5. Smaller ID.
IPv6 basic ACL	1. Longer prefix for the source IP address (a longer prefix means a narrower IP address range). 2. Smaller ID.
IPv6 advanced ACL	1. Specific protocol number. 2. Longer prefix for the source IPv6 address. 3. Longer prefix for the destination IPv6 address. 4. Narrower TCP/UDP service port number range. 5. Smaller ID.
Ethernet frame header ACL	1. More 1s in the source MAC address mask (more 1s means a smaller MAC address). 2. More 1s in the destination MAC address mask. 3. Smaller ID.

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.

Rule numbering

ACL rules can be manually numbered or automatically numbered. This section describes how automatic ACL rule numbering works.

Rule numbering step

If you do not assign an ID to the rule you are creating, 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 creating, they are automatically 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 renumbering

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 there are five ACL rules numbered 0, 5, 9, 10, and 12, the newly defined rule is numbered 15. If the ACL does not contain any rule, the first rule is numbered 0.

Whenever the step changes, the rules are renumbered, starting from 0. For example, if there are five rules numbered 5, 10, 13, 15, and 20, 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 improve network security, ACL filters all packets by default, including fragments and non-fragmented packets. Meanwhile, to improve match efficiency, you can modify ACL rules. For example, you can configure ACL rules to filter non-first fragments only.

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 can choose to change just some of the settings, in which case the other settings remain the same.

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.	

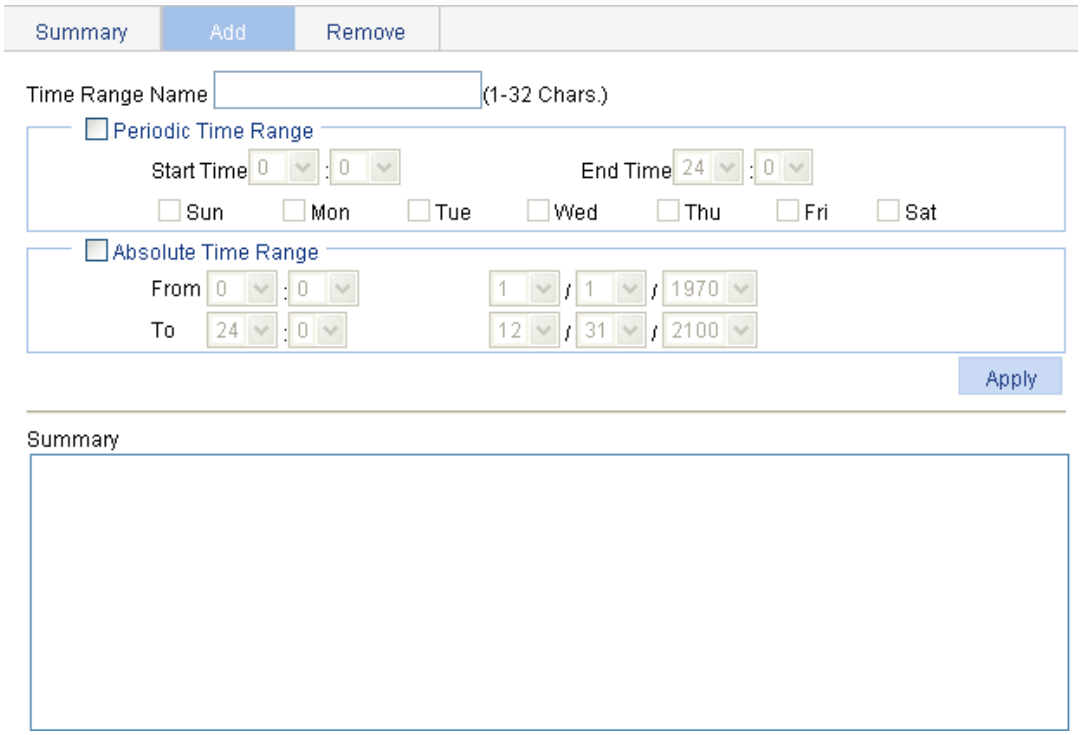
Recommended IPv6 ACL configuration procedure

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.
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 **Add** tab.

Figure 460 Adding a time range



3. Configure a time range as described in Table 139.
4. Click **Apply**.

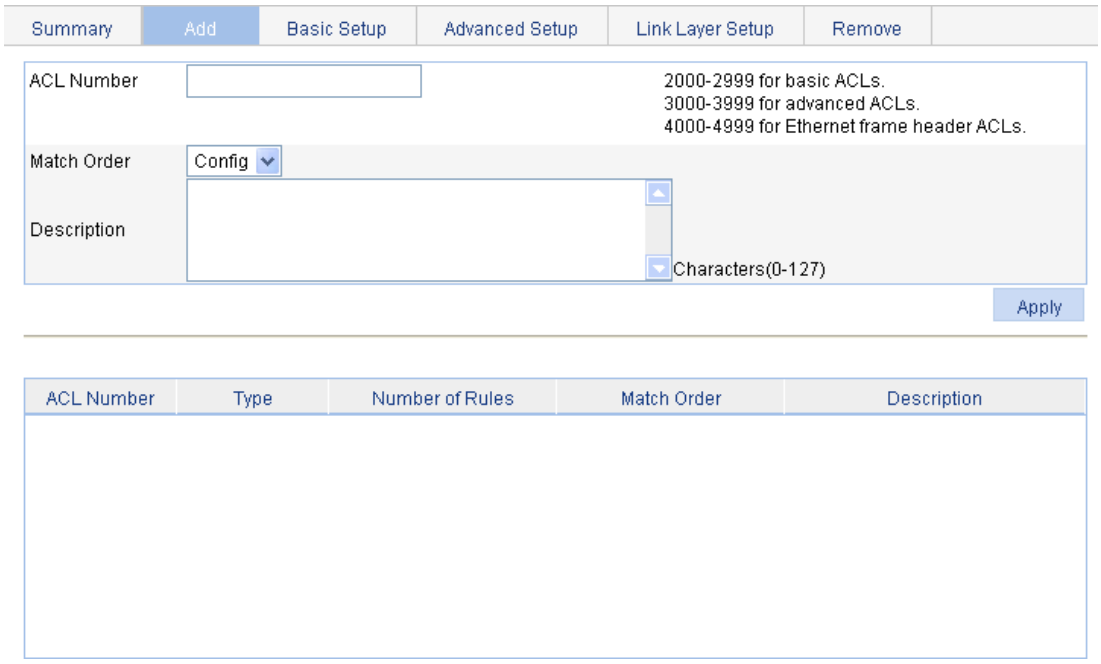
Table 139 Configuration items

Item		Description	
Time Range Name		Set the name for the time range.	
Periodic Time Range	Start Time	Set the start time of the periodic time range.	You can define both a periodic time range and an absolute time range to 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 **Add** tab.

Figure 461 Adding an IPv4 ACL



3. Add an IPv4 ACL as described in Table 140.
4. Click **Apply**.

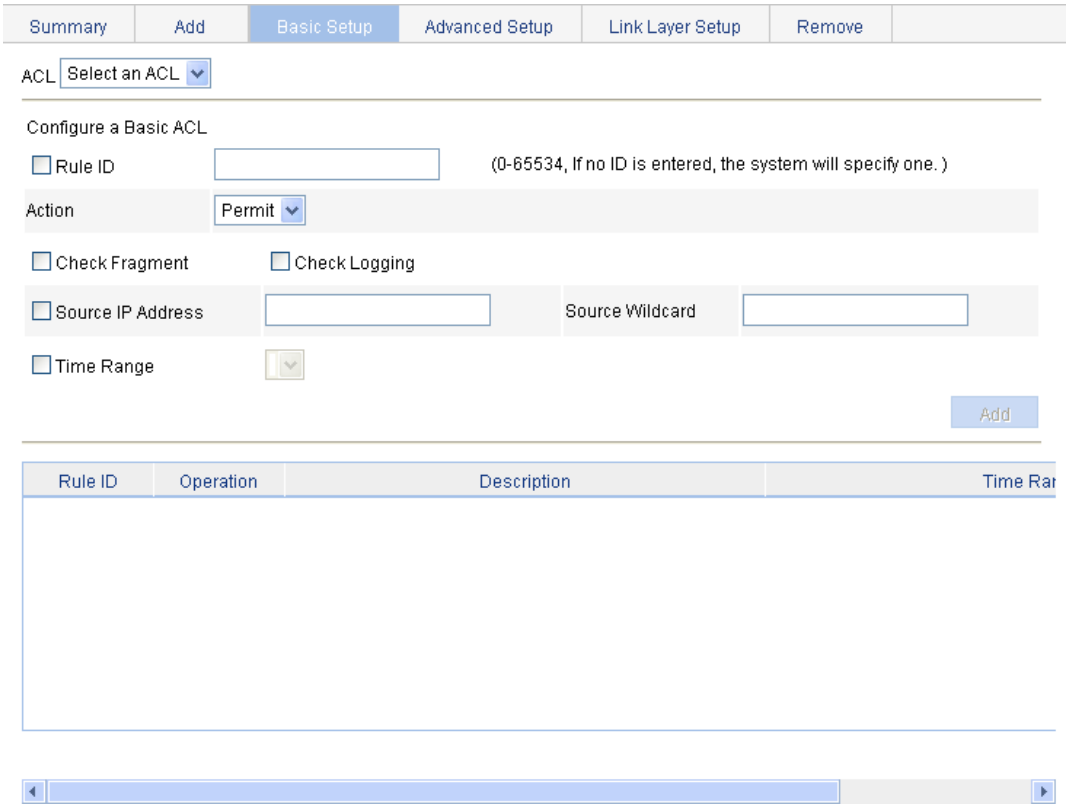
Table 140 Configuration items

Item	Description
ACL Number	Set the number of the IPv4 ACL.
Match Order	Set the match order of the ACL. Available values are: • **Config**—Packets are compared against ACL rules in the order that the rules are configured. • **Auto**—Packets are compared against ACL rules in the depth-first match order.
Description	Set the description for the ACL.

Configuring a rule for a basic IPv4 ACL

1. Select **QoS** > **ACL IPv4** from the navigation tree.
2. Click the **Basic Setup** tab.
   The rule configuration page for a basic IPv4 ACL appears.

   Figure 462 Configuring a basic IPv4 ACL



3. Configure a rule for a basic IPv4 ACL.
4. Click **Add**.

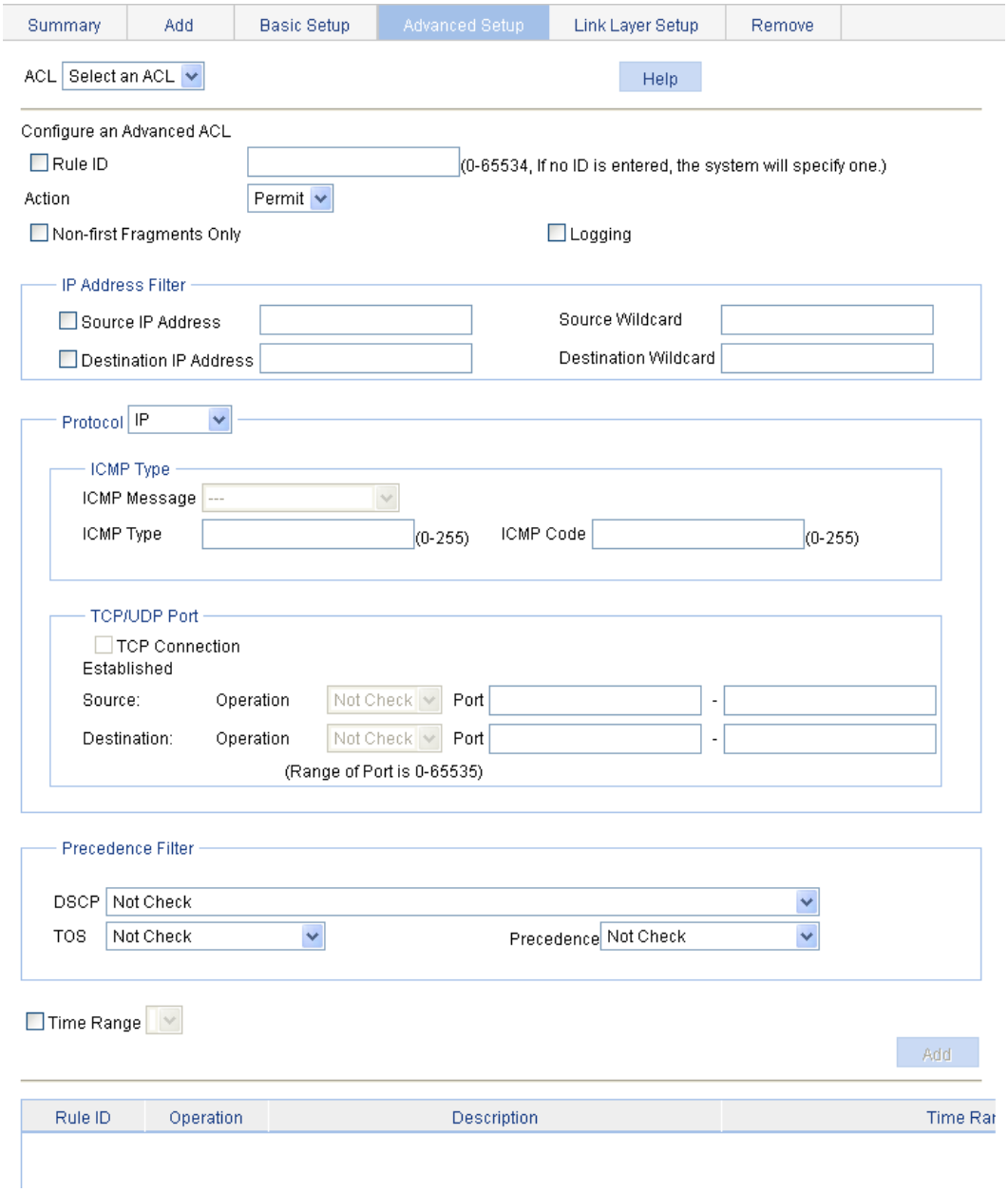
Table 141 Configuration items

Item	Description
ACL	Select the basic IPv4 ACL for which you want to configure rules. Available ACLs are basic 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. 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 number, source/destination address, source/destination port number, and number of matched packets. This function is not supported.
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.
   The rule configuration page for an advanced IPv4 ACL appears.

Figure 463 Configuring an advanced IPv4 ACL



3. Configure a rule for an advanced IPv4 ACL as described in Table 142.
4. Click **Add**.

Table 142 Configuration items

Item	Description
ACL	Select the advanced IPv4 ACL for which you want to configure rules. Available ACLs are advanced 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. If the rule number you specify already exists, the following operations modify the configuration of the rule.

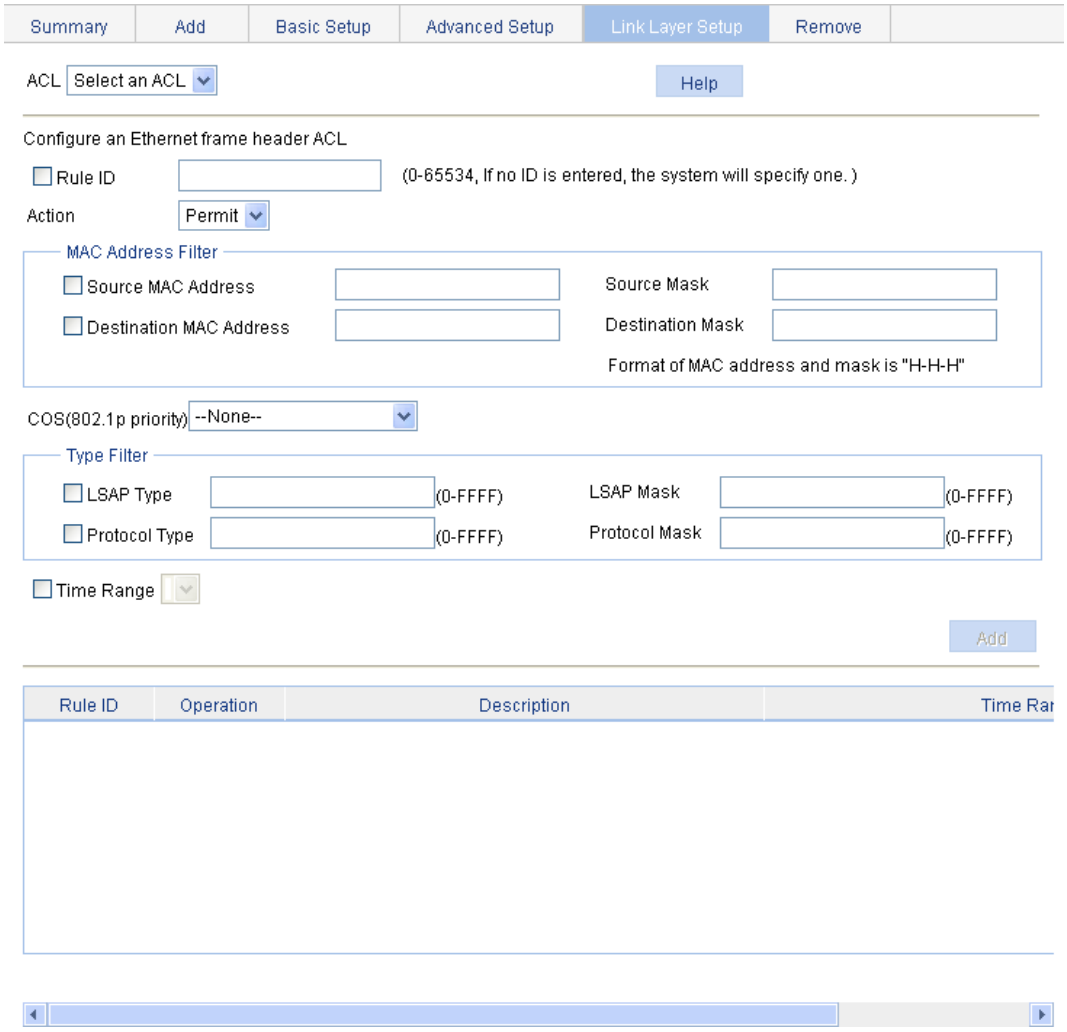
Item			Description
Action			Select the action to be performed for packets matching the rule: • **Permit**—Allows matched packets to pass. • **Deny**—Drops matched packets.
Non-First Fragments Only			Select this box to apply the rule to only non-first fragments. If you do no select this box, the rule applies to all fragments and non-fragments.
Logging			Select this box to keep a log of matched packets. A log entry contains the ACL rule number, operation for the matched packets, protocol number, source/destination address, source/destination port number, and number of matched packets. This function is not supported.
IP Address Filter	Source IP Address		Select the **Source IP Address** box and enter a source IPv4 address and a source wildcard mask, in dotted decimal notation.
	Source Wildcard		
	Destination IP Address		Select the **Source IP Address** box and enter a source IP address and a source wildcard mask, in dotted decimal notation.
	Destination Wildcard		
Protocol			Select the protocol number. If you select **1 ICMP**, you can configure the ICMP message type and code. If you select **6 TCP** or **17 UDP**, you can configure the TCP or UDP port.
ICMP Type	ICMP Message		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.
	ICMP Type		
	ICMP Code		
TCP/UDP Port	TCP Connection Established		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.
	Source	Operator	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. Only **Not Check** and **Other values** are supported.
		Port	
	Destination	Operator	
		Port	

Item		Description	
Precedence Filter	DSCP	Specify the DSCP value.	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.
	TOS	Specify the ToS preference.	
	Precedence	Specify the IP precedence.	
Time Range		Select the time range during which the rule takes effect.	

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.
   The rule configuration page for an Ethernet frame header IPv4 ACL appears.

   Figure 464 Configuring a rule for an Ethernet frame header ACL



3. Configure a rule for an Ethernet frame header IPv4 ACL as described in Table 143.
4. Click **Add**.

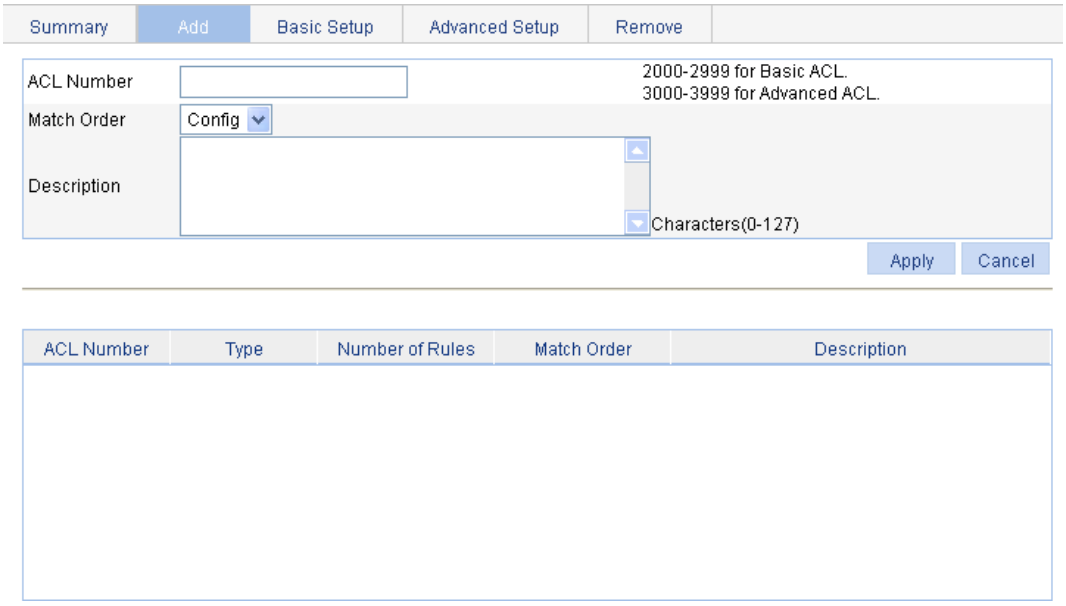
Table 143 Configuration items

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. 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 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**—Frame encapsulation format. • **LSAP Mask**—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**—Frame type. It corresponds to the type-code field of Ethernet_II and Ethernet_SNAP frames. • **Protocol Mask**—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 **Add** tab.
   The IPv6 ACL configuration page appears.

Figure 465 Adding an IPv6 ACL



3. Add an IPv6 ACL.
4. Click **Apply**.

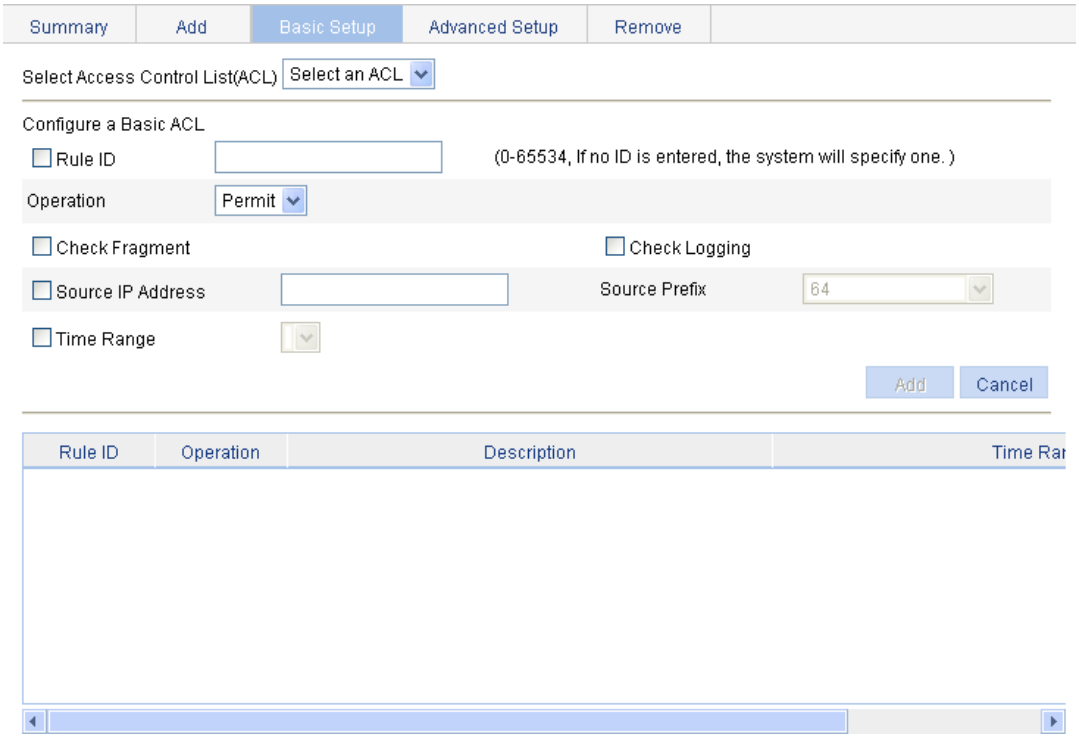
Table 144 Configuration items

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.
Description	Set the description for the ACL.

Configuring a rule for a basic IPv6 ACL

1. Select **QoS** > **ACL IPv6** from the navigation tree.
2. Click the **Basic Setup** tab.
   The rule configuration page for a basic IPv6 ACL appears.

Figure 466 Configuring a rule for a basic IPv6 ACL



3. Add a rule for a basic IPv6 ACL.
4. Click **Add**.

Table 145 Configuration items

Item	Description
Select Access Control List (ACL)	Select the basic 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. 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 number, source/destination address, source/destination port number, and number of matched packets. This function is not supported.
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	

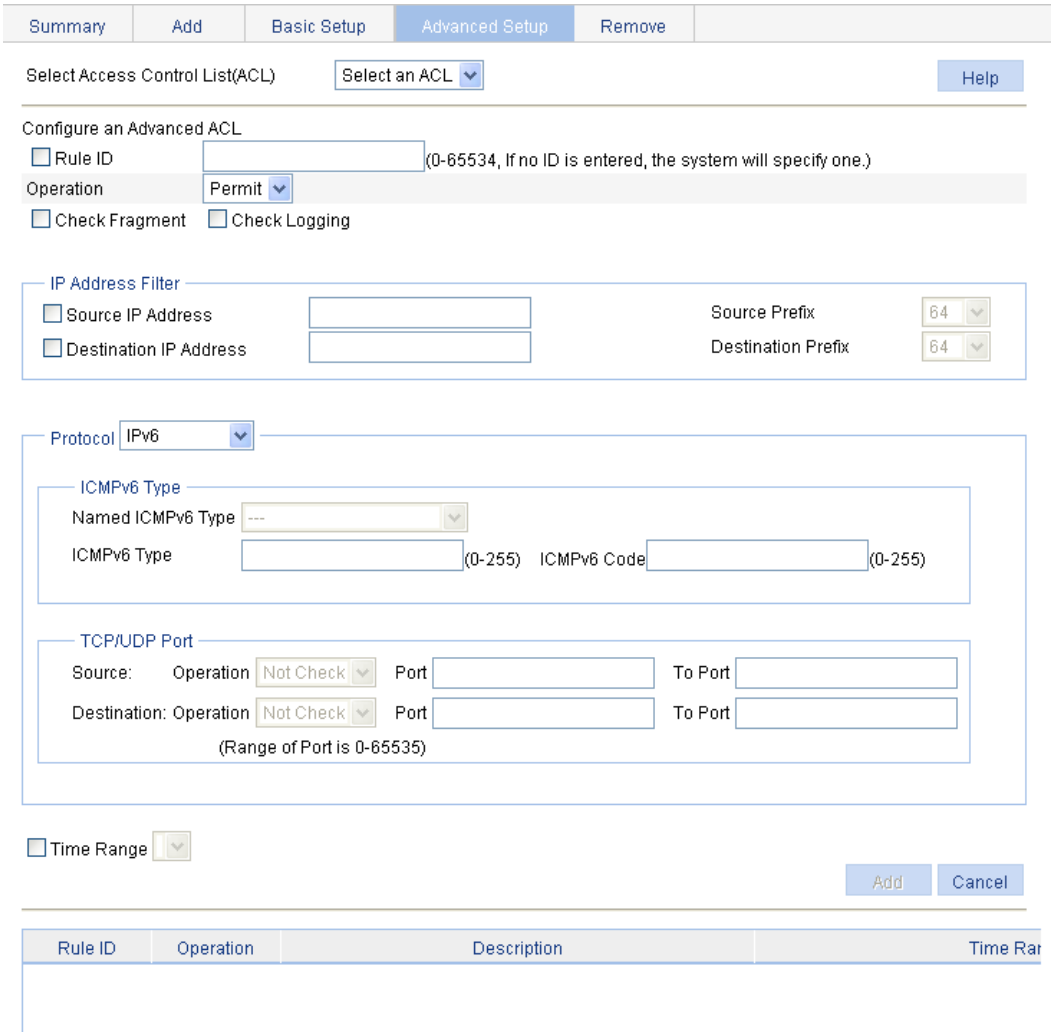
Item	Description
Time Range	Select the time range during which the rule takes effect.

Configuring a rule for an advanced IPv6 ACL

1. Select **QoS** > **ACL IPv6** from the navigation tree.
2. Click the **Advance Setup** tab.

   The rule configuration page for an advanced IPv6 ACL appears.

   Figure 467 Configuring a rule for an advanced IPv6 ACL



3. Add a rule for an advanced IPv6 ACL as described in Table 146.
4. Click **Add**.

Table 146 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. 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 number, source/destination address, source/destination port number, and number of matched packets. This function is not supported.
IP Address Filter	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	
	Destination IP Address	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 (:).
	Destination Prefix	
Protocol		Select the protocol number. 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.
ICMPv6 Type	Named ICMPv6 Type	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.
	ICMPv6 Type	
	ICMPv6 Code	

<table>
<tr><th colspan="3">Item</th><th>Description</th></tr>
<tr><td rowspan="6">TCP/UDP Port</td><td rowspan="3">Source</td><td>Operator</td><td rowspan="3">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.</td></tr>
<tr><td>Port</td></tr>
<tr><td>To Port</td></tr>
<tr><td rowspan="3">Destination</td><td>Operator</td><td rowspan="3">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.
Only Not Check and Other values are supported.</td></tr>
<tr><td>Port</td></tr>
<tr><td>To Port</td></tr>
<tr><td colspan="3">Time Range</td><td>Select the time range during which the rule takes effect.</td></tr>
</table>

Configuring QoS

Grayed-out options on Web configuration pages cannot be configured.

Overview

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 might 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 might 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.

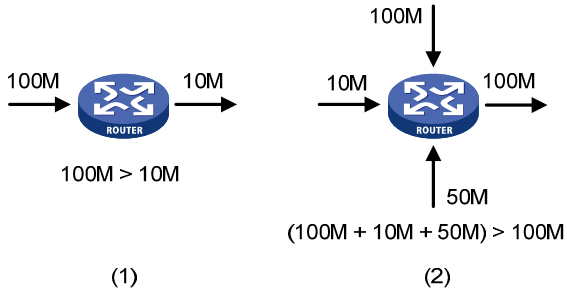
Congestion: causes, impacts, and countermeasures

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 468 shows two common cases:

Figure 468 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 might 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.

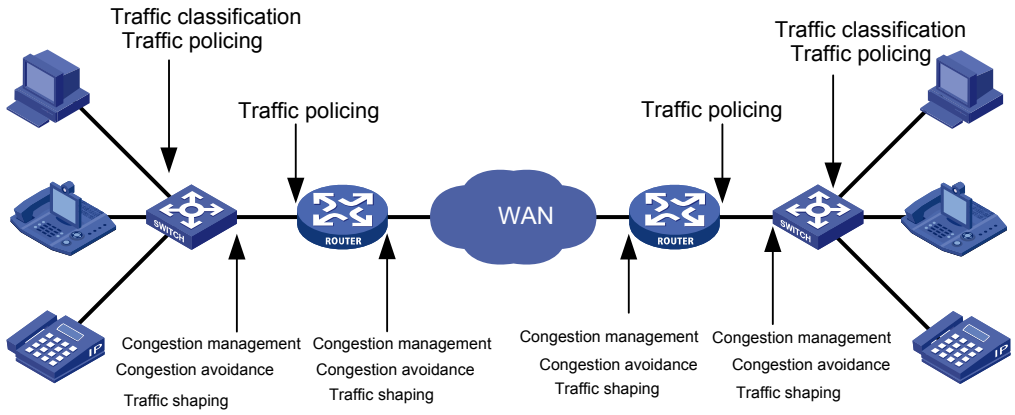
Countermeasures

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 469 End-to-end QoS model



As shown in Figure 469, 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.

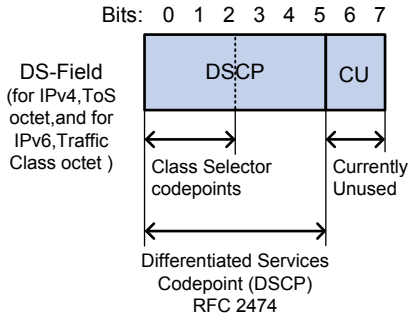
When packets are classified on the network boundary, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be directly used to classify the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream 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 470 ToS field and DS field



As shown in Figure 470, the ToS field of the IP header contains 8 bits. 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 6 bits (0 to 5) and is in the range of 0 to 63. The remaining 2 bits (6 and 7) are reserved.

Table 147 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 148 Description on DSCP values

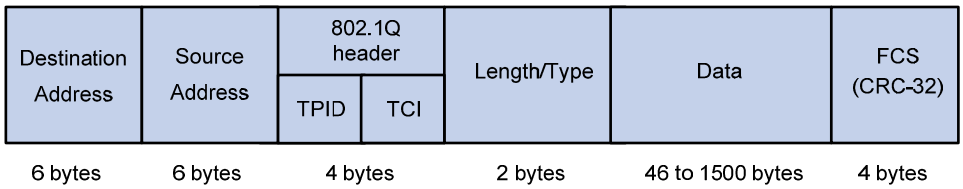
DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11

DSCP value (decimal)	DSCP value (binary)	Description
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 471 An Ethernet frame with an 802.1Q tag header



As shown in Figure 471, 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 472 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 149 presents the values for 802.1p priority.

Figure 472 802.1Q tag header

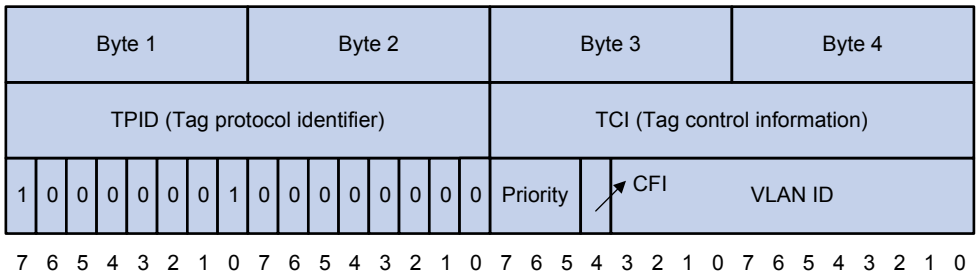


Table 149 Description on 802.1p priority

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

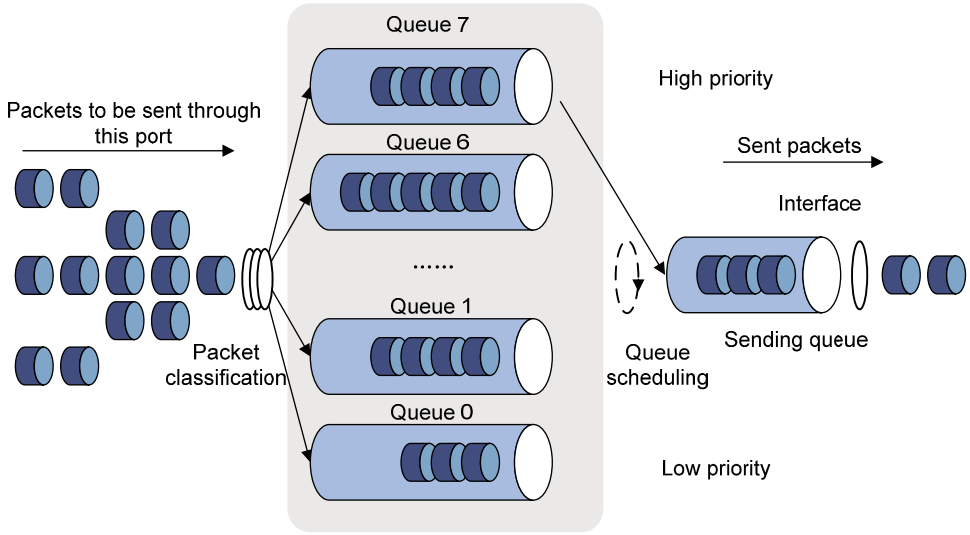
In general, congestion management uses queuing technology. The system uses a certain queuing algorithm for traffic classification, and then uses a certain precedence algorithm to send the traffic. Each queuing algorithm handles a particular network traffic problem and has significant impacts on bandwidth 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 473 SP queuing



A typical switch provides eight queues per port. As shown in Figure 473, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

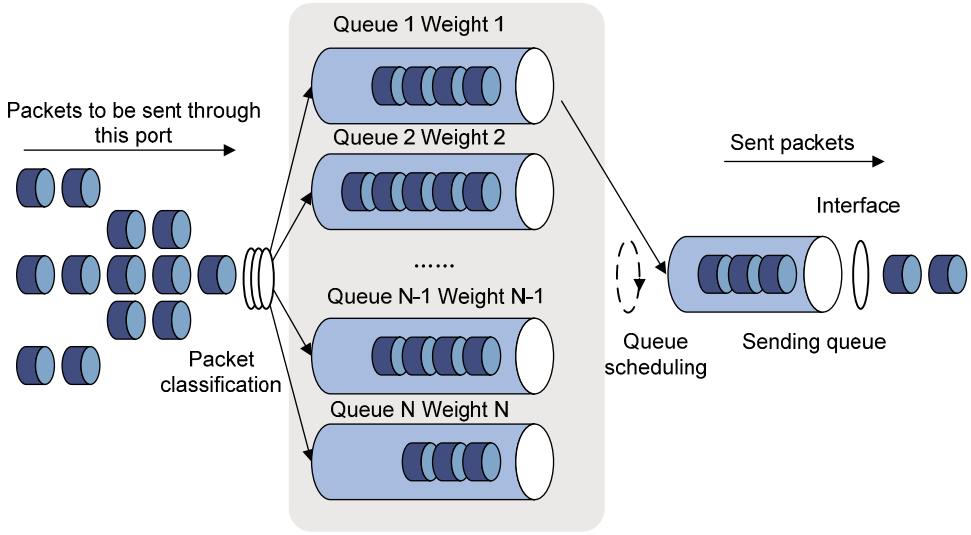
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. You can assign mission-critical packets to the high priority queue to make sure 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 might cause lower priority traffic to starve to death.

WRR queuing

WRR queuing schedules all the queues in turn to make sure every queue can be served for a certain time, as shown in Figure 474.

Figure 474 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 25, 25, 15, 15, 5, 5, 5, and 5 (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 might 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.

Basic WRR queuing contains multiple queues. You can configure the weight, percentage (or byte count) for each queue, and WRR schedules these queues based on the user-defined parameters in a round robin manner.

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.

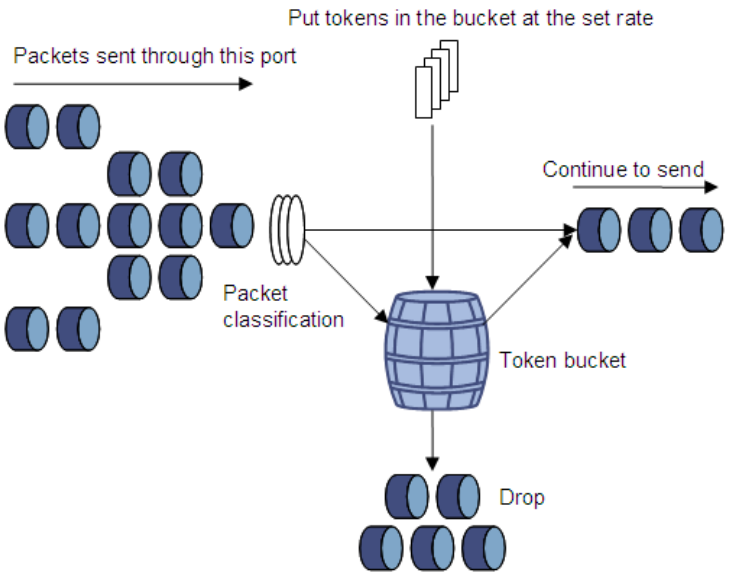
Rate limit

Rate limit is a traffic control method using token buckets. The rate limit of a physical interface specifies the maximum rate for forwarding packets (including critical packets). Rate limit can limit all the packets passing a physical interface.

Traffic evaluation and token bucket

A token bucket can be considered as a container holding a certain number of tokens. The system puts tokens into the bucket at a set rate. When the token bucket is full, the extra tokens will overflow.

Figure 475 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:

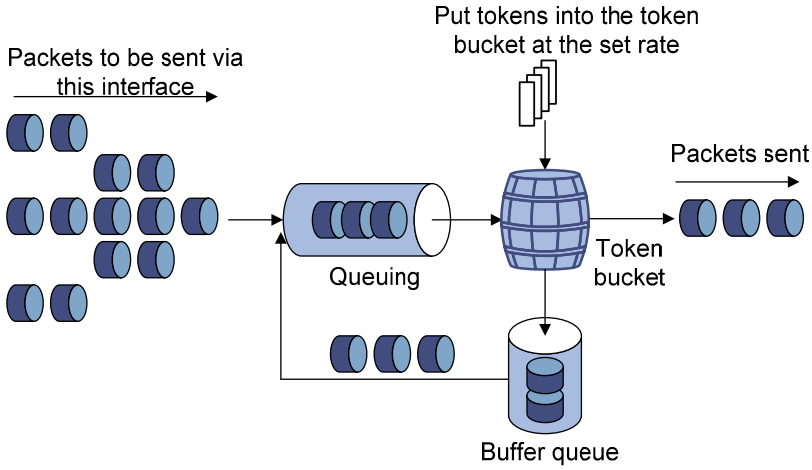
- **Mean rate**—Rate at which tokens are put into the bucket, or the permitted average rate of traffic. It is usually set to the committed information rate (CIR).
- **Burst size**—The capacity of the token bucket, or the maximum traffic size permitted in each burst. It is usually set to the committed 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.

Working mechanism of rate limit

With rate limit configured on an interface, all packets to be sent through the interface are firstly handled by the token bucket of rate limit. 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 476 Rate limit implementation



With a token bucket used for traffic control, when the token bucket has tokens, the bursty packets can be transmitted. When 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, and local precedence).

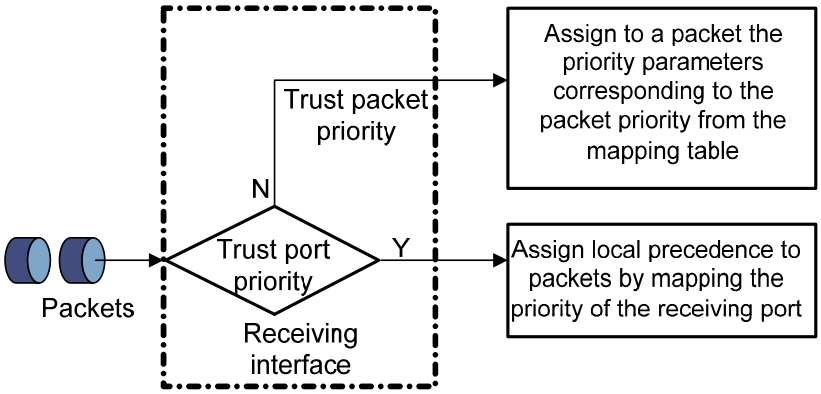
- For more information about 802.1p priority and DSCP values, see "Packet precedences."
- Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to an output queue. Packets with the highest local precedence are processed preferentially.

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 477 shows the process of priority mapping on a device.

Figure 477 Priority mapping process



Introduction to priority mapping tables

The device provides the following types of priority mapping tables:

- **CoS to Queue**—802.1p--to-local mapping table.
- **DSCP to Queue**—DSCP-to-local mapping table, which applies to only IP packets.

Table 150 through Table 151 list the default priority mapping tables.

Table 150 Default CoS to Queue mapping table

Input CoS value	Local precedence (Queue)
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Table 151 Default DSCP to Queue mapping table

Input DSCP value	Local precedence (Queue)
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3

Input DSCP value	Local precedence (Queue)
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Configuration guidelines

When an ACL is referenced by a QoS policy for traffic classification, the action (permit or deny) in the ACL is ignored, and the actions in the associated traffic behavior are performed.

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. A QoS policy can be applied to only the inbound direction of one port.

Perform the tasks in Table 152 to configure a QoS policy:

Table 152 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: o Configuring traffic mirroring and traffic redirecting for a traffic behavior o Configuring other actions for a traffic behavior	Use either method. Configure various actions for the traffic behavior.

Step	Remarks
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 GTS configuration procedure

Step	Remarks
1. Configuring GTS on ports	Optional. Configure GTS parameters on ports.

Recommended rate limit configuration procedure

Step	Remarks
1. Configuring rate limit 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	Required. Set priority mapping tables.

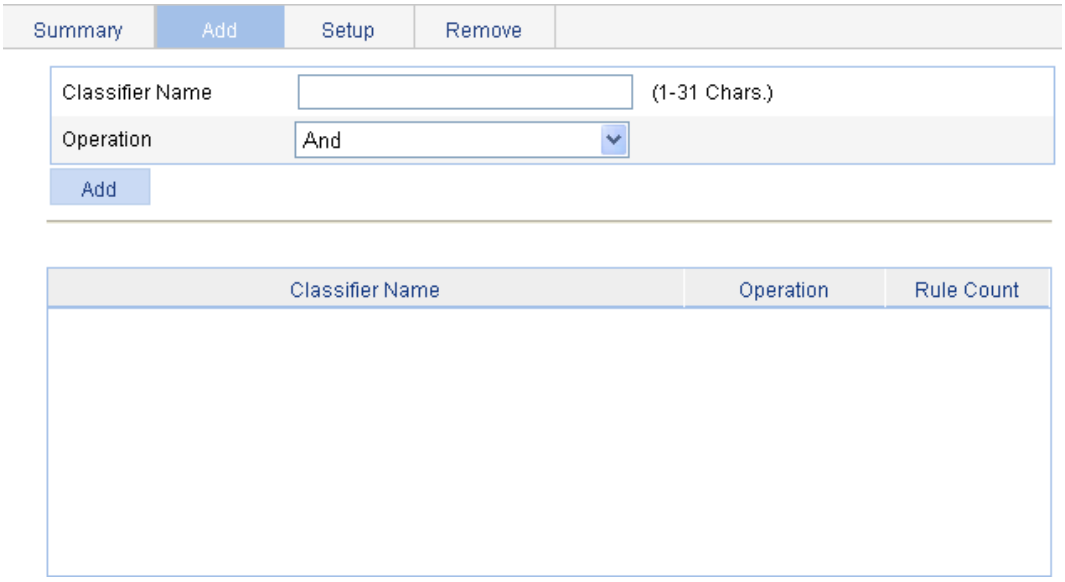
Recommended priority trust mode configuration procedure

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 **Add** tab to enter the page for adding a class.

Figure 478 Adding a class



3. Add a class as described in Table 153.
4. Click **Add**.

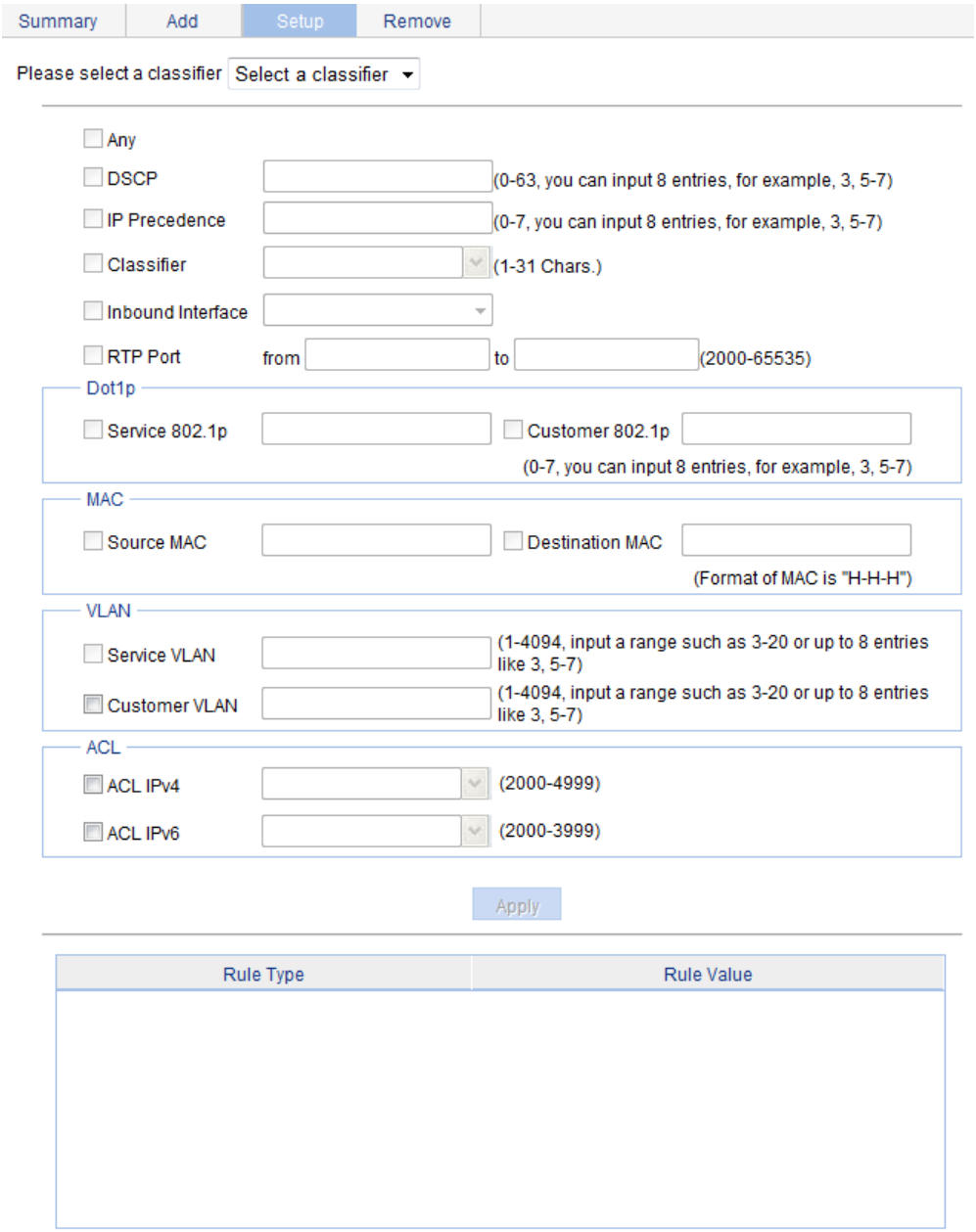
Table 153 Configuration items

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. The device does not support this operator.

Configuring classification rules

1. Select **QoS** > **Classifier** from the navigation tree.
2. Click **Setup** to enter the page for setting a class.

Figure 479 Configuring classification rules



3. Configure classification rules for a class as described in Table 154.
4. Click **Apply**.

Table 154 Configuration items

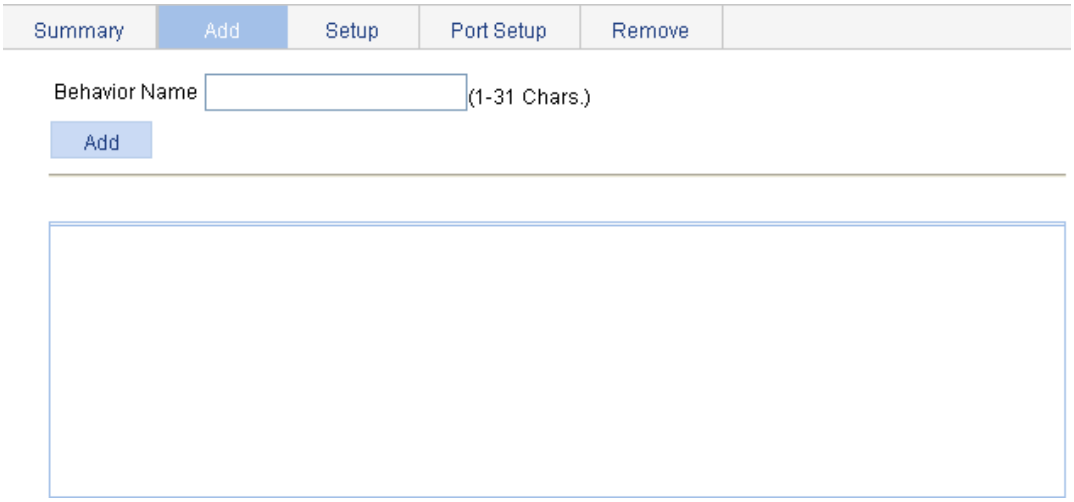
Item		Description
VLAN	Customer VLAN	Define a rule to match customer VLAN IDs. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure only one VLAN ID at a time. Otherwise, the relevant QoS policy fails to be applied. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**.

Item		Description
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 **Add** tab to enter the page for adding a traffic behavior.

Figure 480 Adding a traffic behavior



3. Add a traffic behavior as described in Table 155.
4. Click **Add**.

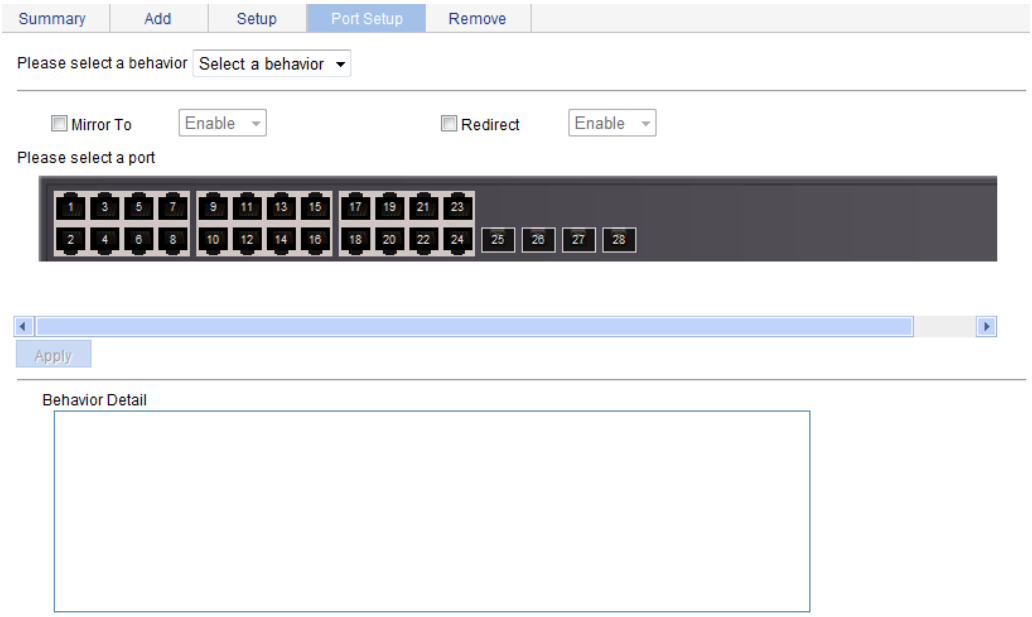
Table 155 Configuration items

Item	Description
Behavior name	Specify a name for the behavior to be added.

Configuring traffic mirroring and 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 481 Port setup page for a traffic behavior



3. Configure traffic mirroring and traffic redirecting as described in Table 156.
4. Click **Apply**.

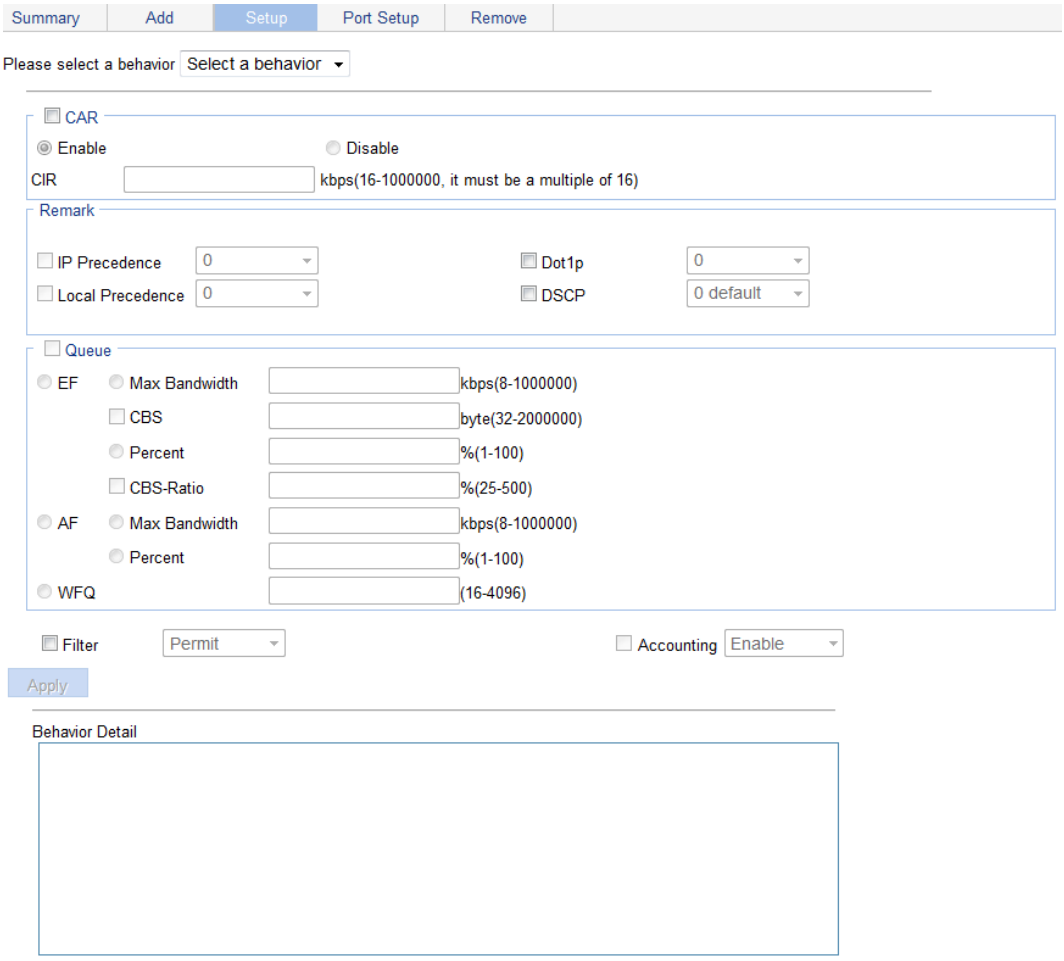
Table 156 Configuration items

Item	Description
Please select a behavior	Select an existing behavior in the list.
Mirror To	Set the action of mirroring traffic to the specified destination port.
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 482 Setting a traffic behavior



3. Configure other actions for a traffic behavior as described in Table 157.
4. Click **Apply**.

Table 157 Configuration items

Item		Description
Please select a behavior		Select an existing behavior in the list.
CAR	Enable/Disable	Enable or disable CAR.
	CIR	Set the committed information rate (CIR), the average traffic rate.
Filter		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.

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.

Figure 483 Adding a policy

3. Add a policy as described in Table 158.
4. Click **Add**.

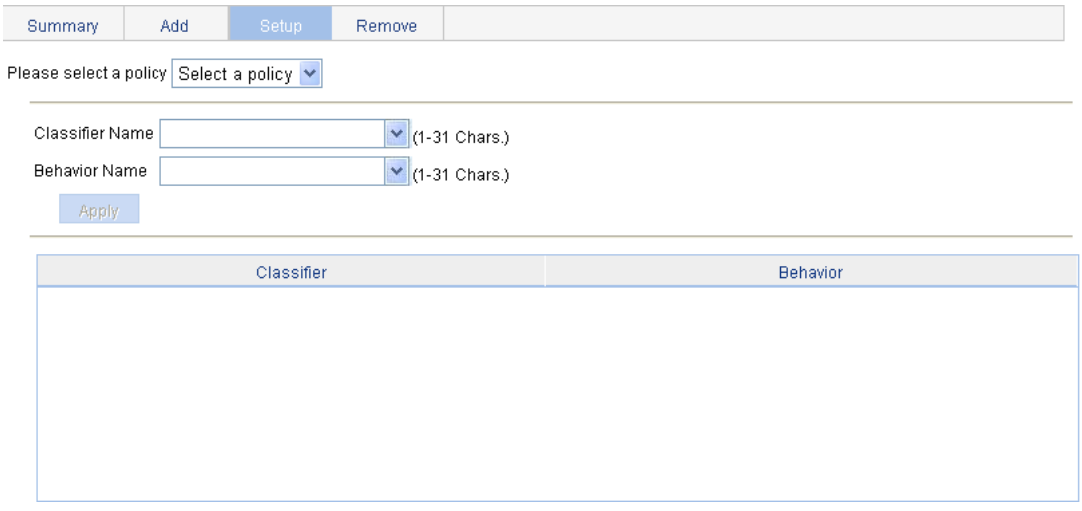
Table 158 Configuration items

Item	Description
Policy Name	Specify a name for the policy to be added. Some devices have their own system-defined policies. The policy name you specify cannot overlap with system-defined ones. The system-defined policy is the policy **default**.

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 484 Setting a policy



3. Configure a classifier-behavior association for a policy as described in Table 159.

4. Click **Apply**.

Table 159 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 485 Applying a policy to a port

3. Apply a policy to a port as described in Table 160.
4. Click **Apply**.

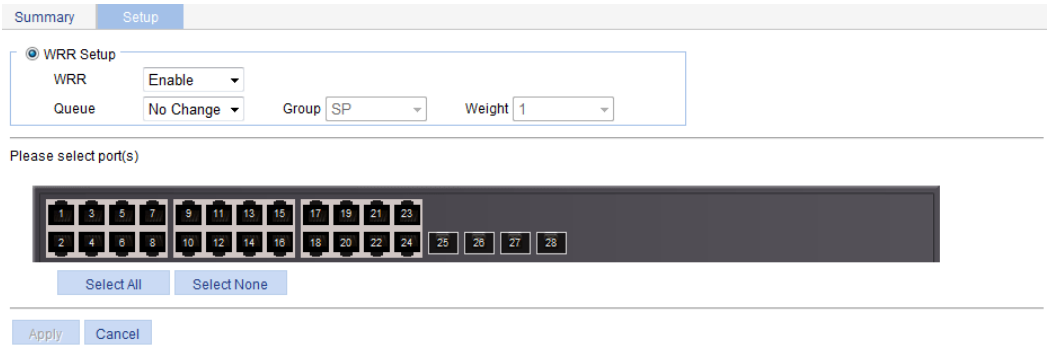
Table 160 Configuration items

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**—Applies the policy to the incoming packets of the specified ports. • **Outbound**—Applies the policy to the outgoing packets of the specified ports.
Please select port(s)	Select one port 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 486 Configuring queue scheduling



3. Configure queue scheduling on a port as described in Table 161.
4. Click **Apply**.

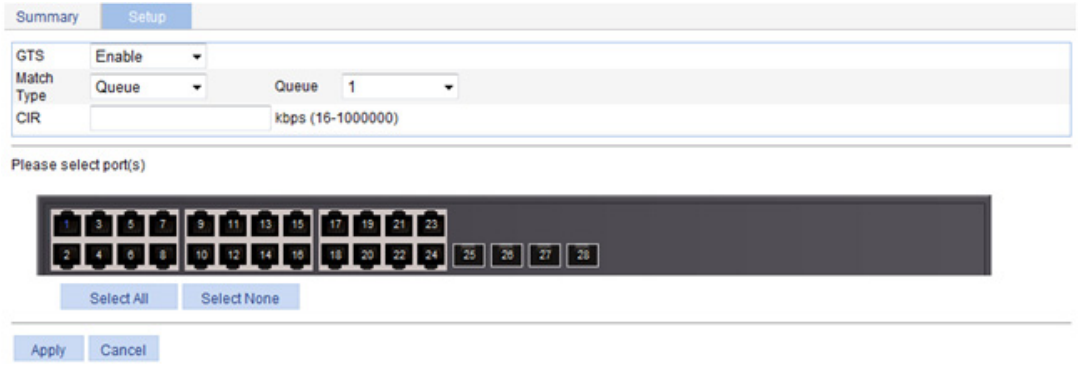
Table 161 Configuration items

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. The value range for a queue ID is 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.
	Weight	Set a weight for the current queue. This list is available when group 1 is selected.
Please select port(s)		Click to select ports to be configured with queuing on the chassis front panel.

Configuring GTS on ports

1. From the navigation tree, select **QoS** > **GTS**.
2. Click the **Setup** tab, as shown in Figure 487.

Figure 487 GTS



3. Configure GTS parameters as described in Table 162.
4. Click **Apply**.

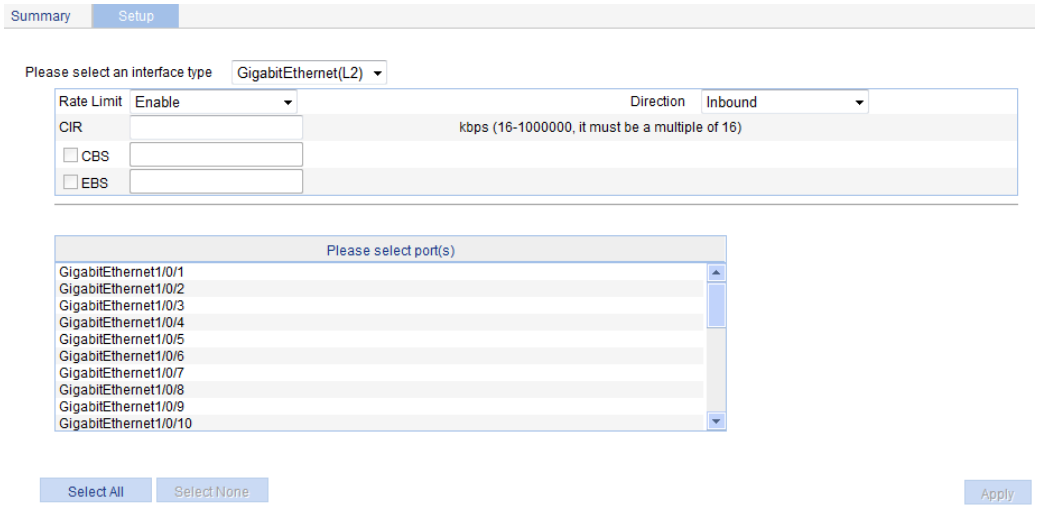
Table 162 Configuration items

Item	Description
GTS	Enable or disable GTS.
Match Type	Select the GTS type. Only queue-based GTS is supported.
Queue	Select a queue by its number in the range of 0 to 7.
CIR	Specify the CIR, which is the average traffic rate.
Please select port(s)	Select one or more ports by clicking them on the chassis front panel.

Configuring rate limit on a port

1. Select **QoS** > **Line rate** from the navigation tree.
2. Click the **Setup** tab to enter the rate limit configuration page.

Figure 488 Configuring rate limit on a port



3. Configure rate limit on a port as described in Table 163.
4. Click **Apply**.

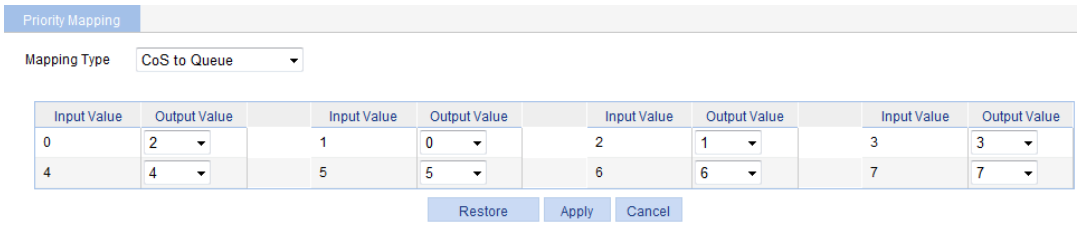
Table 163 Configuration items

Item	Description
Please select an interface type	Select the types of interfaces to be configured with rate limit.
Rate Limit	Enable or disable rate limit on the specified port.
Direction	Select a direction in which the rate limit is to be applied. • **Inbound**—Limits the rate of packets received on the specified port. • **Outbound**—Limits the rate of packets sent by the specified port. • **Both**—Limits the rate of packets received and sent by the specified port.
CIR	Set the committed information rate (CIR), the average traffic rate.
Please select port(s)	Specify the ports to be configured with rate limit. Click the ports to be configured with rate limit in the port list. You can select one or more ports.

Configuring priority mapping tables

1. Select **QoS** > **Priority Mapping** from the navigation tree.

   Figure 489 Configuring priority mapping tables



2. Configure a priority mapping table as described in Table 164.
3. Click **Apply**.

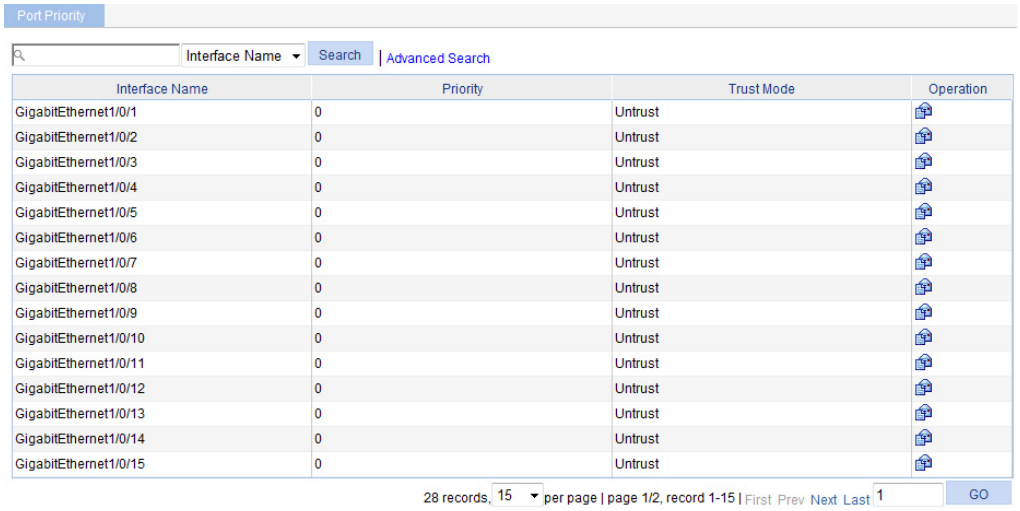
Table 164 Configuration items

Item	Description
Mapping Type	Select the priority mapping table to be configured: • **CoS to Queue**. • **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

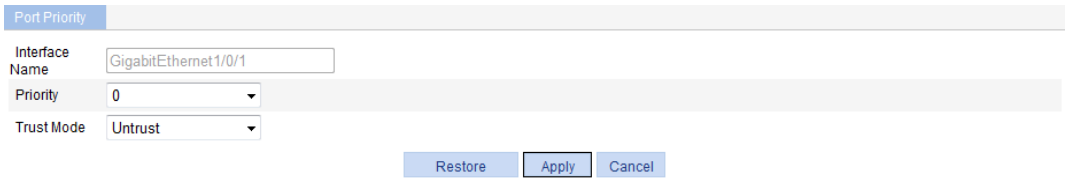
1. Select **QoS** > **Port Priority** from the navigation tree.

Figure 490 Configuring port priorities



2. Click the icon for a port.

Figure 491 Modifying the port priority



3. Configure the port priority for a port as described in Table 165.
4. Click **Apply**.

Table 165 Configuration items

Item	Description
Interface	Interface to be configured.
Priority	Set a local precedence value for the port.
Trust Mode	Select a priority trust mode for the port: • **Untrust**—Packet priority is not trusted. • **Dot1p**—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.

ACL and QoS configuration example

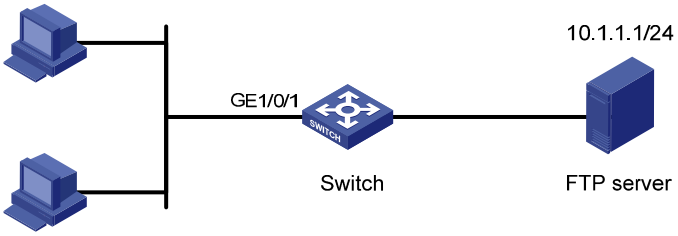
Network requirements

As shown in Figure 492, 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.

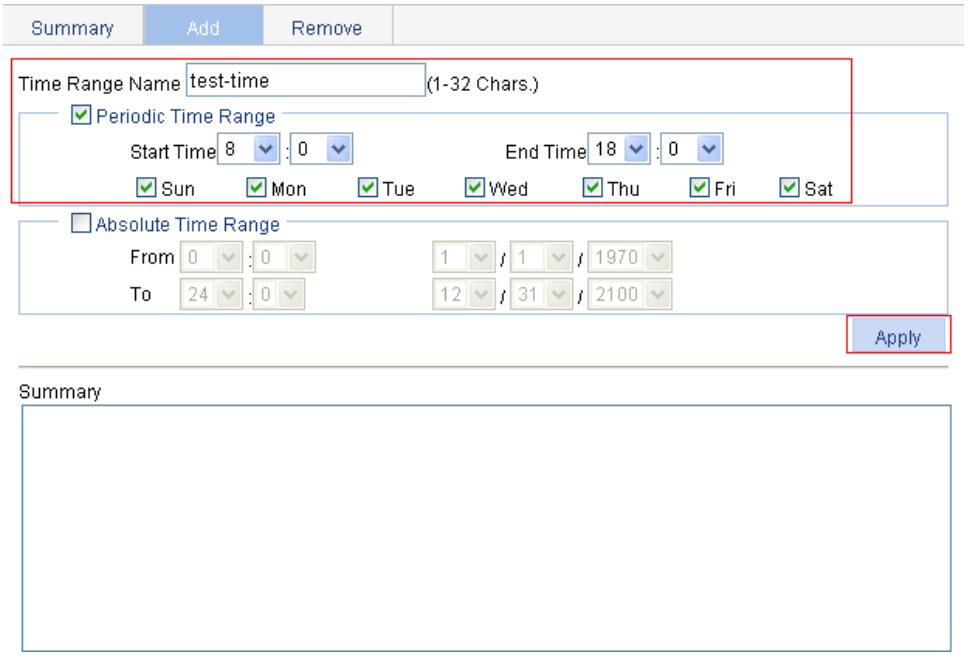
Figure 492 Network diagram



Configuring Switch

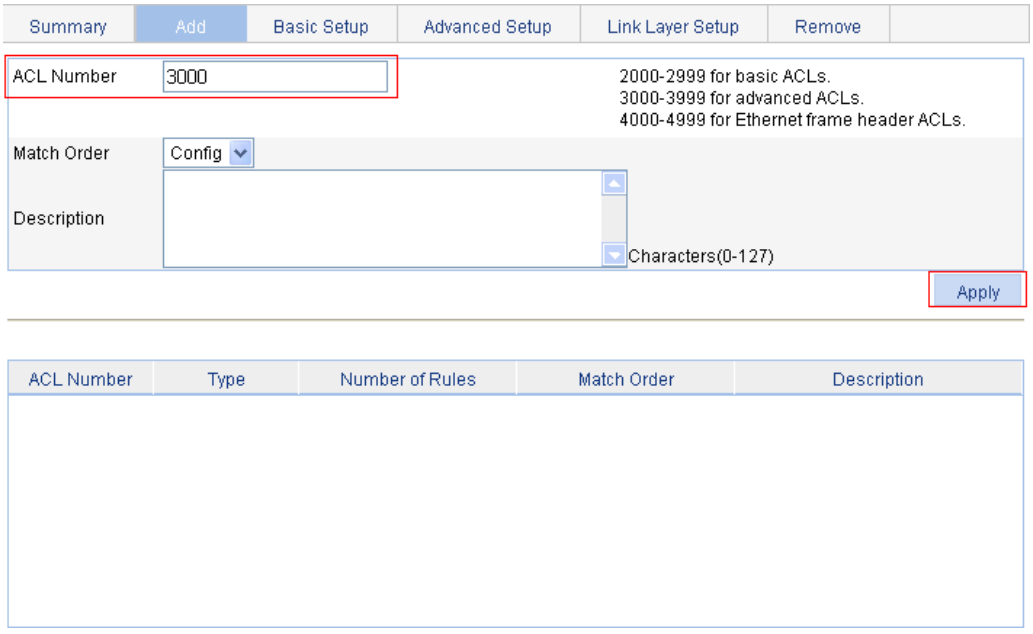
1. Define a time range to cover the time range from 8:00 to 18:00 every day:
   a. Select **QoS** > **Time Range** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the time range name **test-time**.
   d. Select the **Periodic Time Range** box.
   e. Set the **Start Time** to 8:00 and the **End Time** to 18:00.
   f. Select the options **Sun** through **Sat**.
   g. Click **Apply**.

Figure 493 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 **Add** tab.
   c. Enter the ACL number 3000.
   d. Click **Apply**.

Figure 494 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** in the **ACL** list.
   c. Select the **Rule ID** box, and enter rule ID 2.

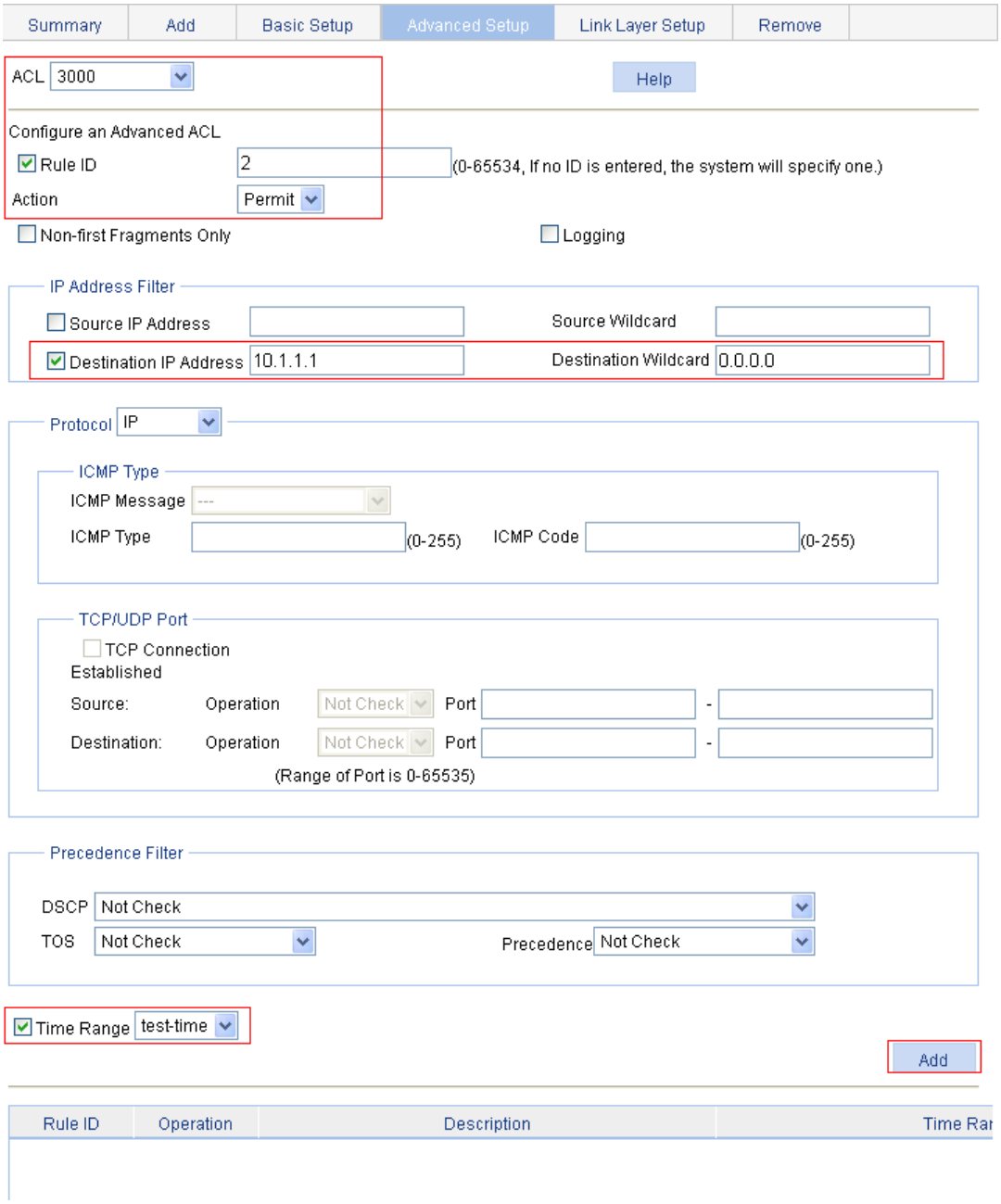
d. Select **Permit** in the **Action** list.

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** in the **Time Range** list.

g. Click **Add**.

Figure 495 Defining an ACL rule for traffic to the FTP server



4. Add a class:

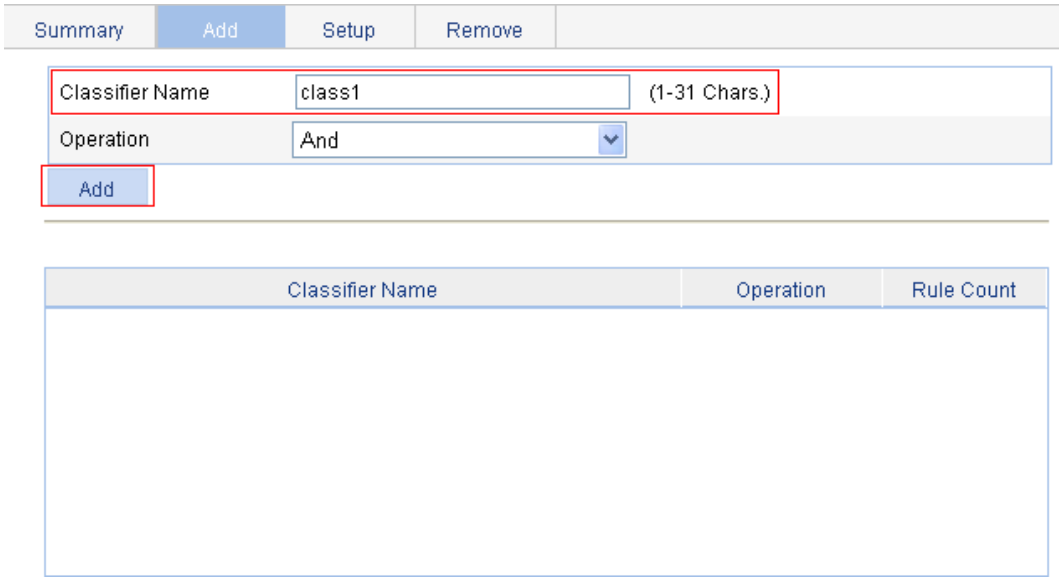
a. Select **QoS** > **Classifier** from the navigation tree.

b. Click the **Add** tab.

c. Enter the class name **class1**.

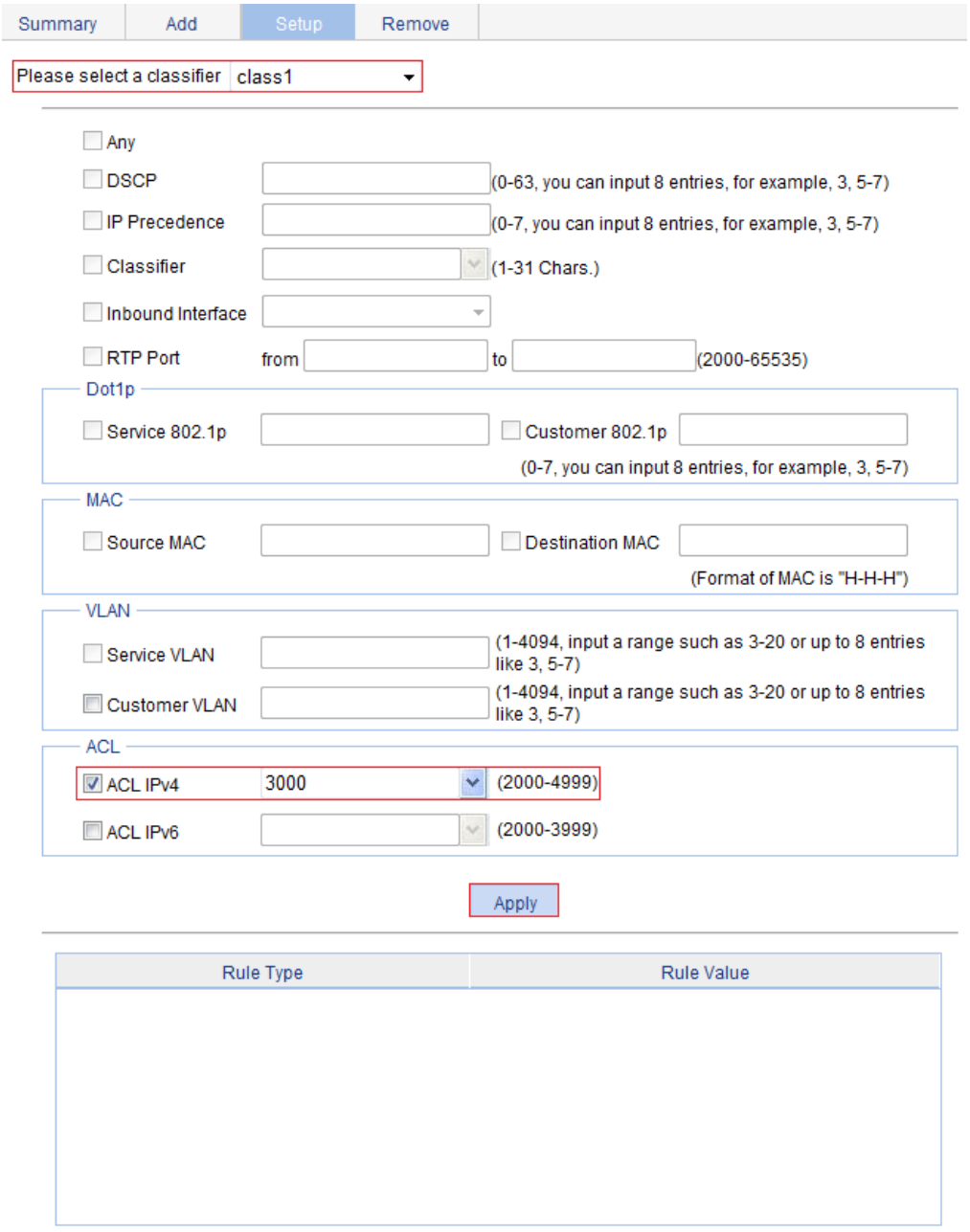
d. Click **Add**.

Figure 496 Adding a class



5. Define classification rules:
   a. Click the **Setup** tab.
   b. Select the class name **class1** in the list.
   c. Select the **ACL IPv4** box, and select ACL 3000 in the following list.

Figure 497 Defining classification rules

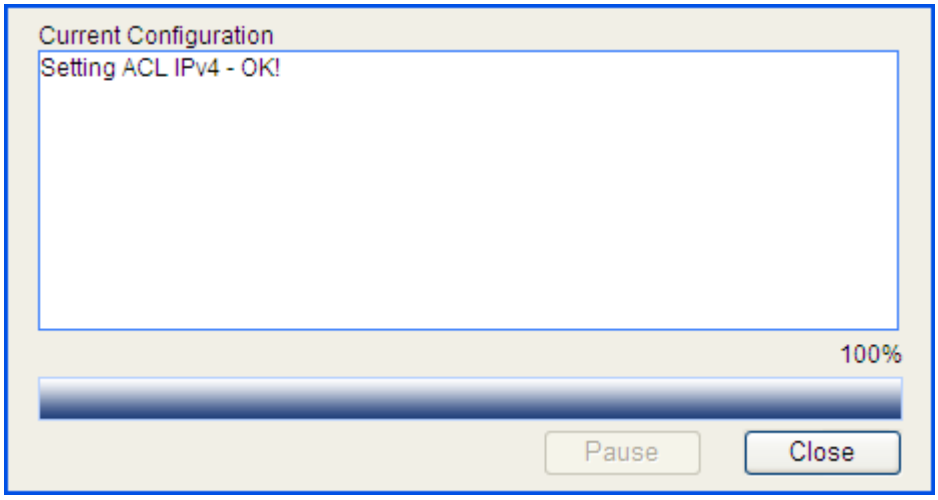


d. Click **Apply**.

A progress dialog box appears, as shown in Figure 498.

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

Figure 498 Configuration progress dialog box

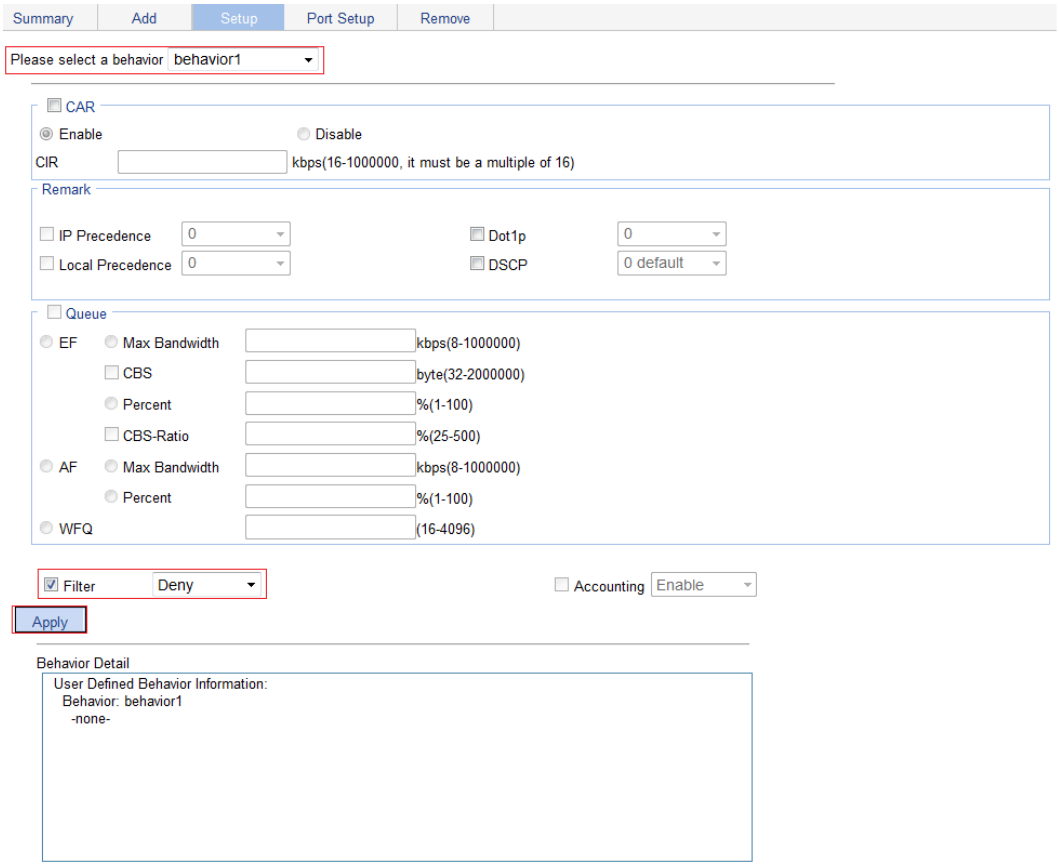


6. Add a traffic behavior:
   a. Select **QoS** > **Behavior** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the behavior name **behavior1**.
   d. Click **Add**.

Figure 499 Adding a traffic behavior

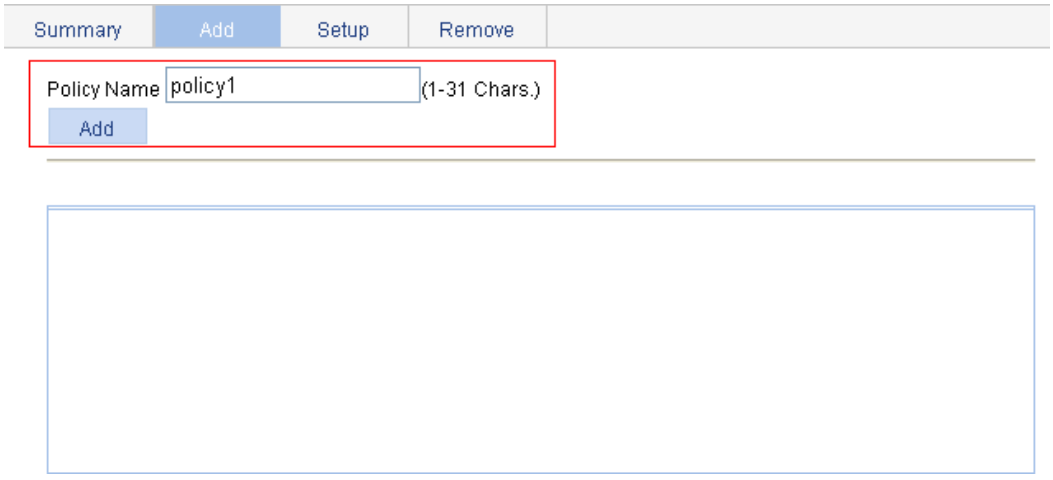
7. Configure actions for the traffic behavior:
   a. Click the **Setup** tab.
   b. Select **behavior1** in the list.
   c. Select the **Filter** box, and then select **Deny** in the following list.
   d. Click **Apply**.
      A progress dialog box appears.
   e. Click **Close** when the progress dialog box prompts that the configuration succeeds.

Figure 500 Configuring actions for the behavior



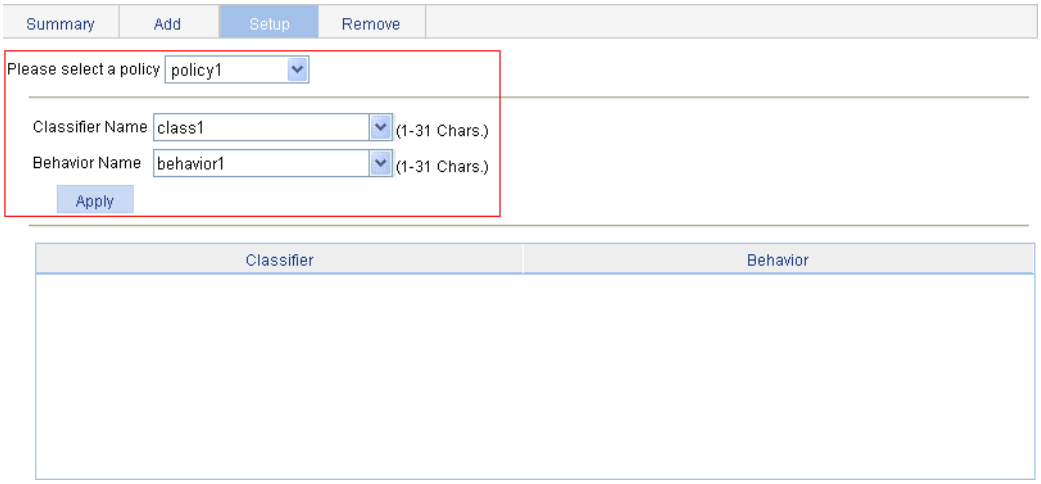
8. Add a policy:
   a. Select **QoS** > **QoS Policy** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the policy name **policy1**.
   d. Click **Add**.

Figure 501 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 502 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 503 Applying the QoS policy in the inbound direction of GigabitEthernet 1/0/1

Configuring PoE

Only a device with a mark of PoE supports the PoE feature.

Overview

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 straight-through 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.

As shown in Figure 504, a PoE system comprises the following elements:

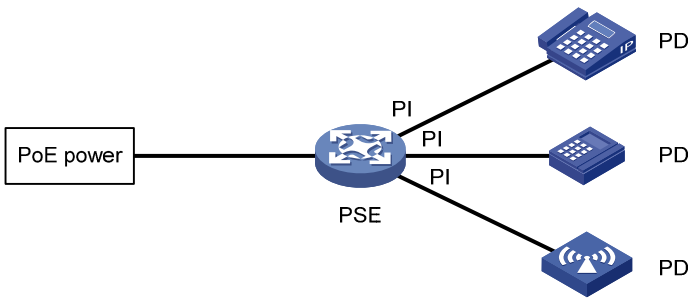
- **PoE power**—The entire PoE system is powered by the PoE power.
- **PSE**—The PSE supplies power for PDs. A PSE can examine the Ethernet cables connected to PoE interfaces, search for PDs, classify them, and supply power to them. When detecting that a PD is removed, the PSE stops supplying power to the PD. A PSE can be built-in (Endpoint) or external (Midspan). A built-in PSE is integrated into a switch or router, and an external PSE is independent of a switch or router. The HPE PSEs are built-in. Only one PSE is available on the device, so the entire device is considered as a PSE.
- **PI**—An Ethernet interface with the PoE capability is called PoE interface. A PoE interface can be an FE or GE interface.
- **PD**—A PD receives power from the PSE. You can also connect a PD to a redundant power source for reliability.

The PSE supplies power over category 3/5 twisted pair cable for a PoE interface in the following two modes:

- **Over signal wires**—The PSE uses data pairs (pins 1, 2 and 3, 6) to supply DC power to PDs.
- **Over spare wires**—The PSE uses spare pairs (pins 4, 5 and 7, 8) to supply DC power to PDs.

A PSE can supply power to a PD only when the selected power supply mode is supported by both the PSE and PD. If the PSE and PD support different power supply modes (for example, the PSE does not support power over spare wires, while the PD supports power over spare wires), you have to change the order of the lines in the twisted pair cable to supply power to the PD.

Figure 504 PoE system diagram



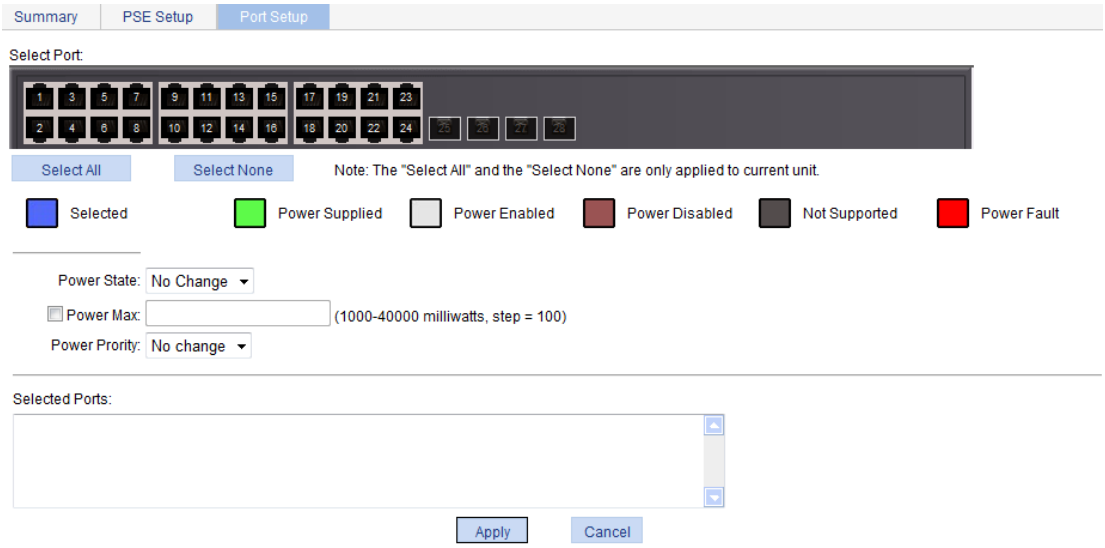
Configuring PoE

Before configuring PoE, make sure the PoE power supply and PSE are operating correctly. Otherwise, either you cannot configure PoE or the PoE configuration does not take effect.

Configuring PoE ports

1. Select **PoE** > **PoE** from the navigation tree.
2. Click the **Port Setup** tab.

Figure 505 Port Setup tab



3. Configure the PoE ports as described in Table 166.
4. Click **Apply**.

Table 166 Configuration items

Item	Description
Select Port	Select ports to be configured and they are displayed in the **Selected Ports** area.
Power State	Enable or disable PoE on the selected ports. • The system does not supply power to or reserve power for the PD connected to a PoE port if the PoE port is not enabled with the PoE function. • You can enable PoE for a PoE port if the PoE port does not result in PoE power overload. Otherwise, you cannot enable PoE for the PoE port. By default, PoE is enabled on a PoE port. **IMPORTANT:** When the sum of the power consumption of all ports exceeds the maximum power of PSE, the system considers the PSE as overloaded.
Power Max	Set the maximum power for the PoE port. The maximum PoE interface power is the maximum power that the PoE interface can provide to the connected PD. If the PD requires more power than the maximum PoE interface power, the PoE interface does not supply power to the PD. By default, the maximum power of a PoE port is 30 watts.

Item	Description
Power Priority	Set the power supply priority for a PoE port. In descending order, the power-supply priority levels of a PoE port are critical, high, and low. • When the PoE power is insufficient, power is first supplied to PoE ports with a higher priority level. • If the PoE power is overloaded and a PSE power-management-priority policy is enabled, the PSE that has a lower priority is first disconnected to guarantee the power supply to a new PSE that has a higher priority. • The guaranteed remaining PoE power is the maximum PoE power minus the power allocated to the critical PSE, regardless of whether PoE is enabled for the PSE. If this is lower than the maximum power of the PSE, you cannot set the power priority of the PSE to **critical**. Otherwise, you can set the power priority to **critical**, and this PSE preempts the power of the PSE that has a lower priority level. In this case, the PSE whose power is preempted is disconnected, but its configuration remains unchanged. If you change the priority of the PSE from **critical** to a lower level, other PSEs have an opportunity to be powered. By default, the power priority of a PoE port is **low**. **IMPORTANT:** • A guard band of 20 watts is reserved for each PoE interface on the device to prevent a PD from being powering off because of a sudden increase of power. If the remaining power of the PSE is lower than 20 watts, the PoE interface with higher priority can preempt the power of a PoE interface with lower priority to supply power to a new PD. In this way, you can ensure normal operation of the PoE interface with higher priority. If the power of the PoE interface with lower priority is lower than 20 watts, for the PoE interface to operate correctly, it supplies power again. • If a sudden increase of the PD power results in PSE power overload, power supply to the PD on the PoE interface that has a lower priority is stopped to ensure power supply to the PD that has a higher priority.

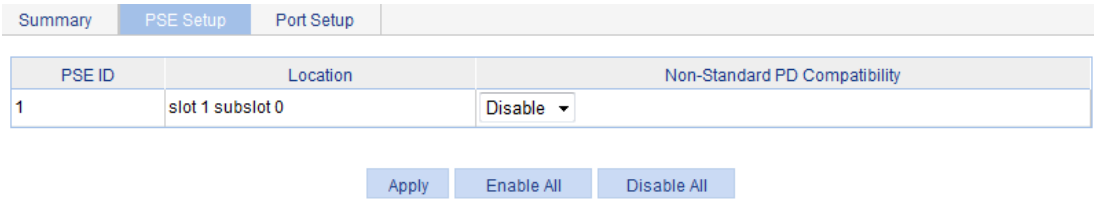
Configuring non-standard PD detection

There are standard PDs and nonstandard PDs. 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 if you enable the PSE to detect nonstandard PDs.

1. Select **PoE** > **PoE** from the navigation tree.
2. Click the **PSE Setup** tab.

   The page displays the location of all PSEs, and the status of the non-standard PD detection function.

   Figure 506 PSE Setup tab



Enabling the non-standard PD detection function for a PSE

1. Select **Enable** in the corresponding **Non-Standard PD Compatibility** column.
2. Click **Apply**.

Disabling the non-standard PD detection function for a PSE

1. Select **Disable** in the corresponding **Non-Standard PD Compatibility** column.
2. Click **Apply**.

Enabling the non-standard PD detection for all PSEs

Click **Enable All**.

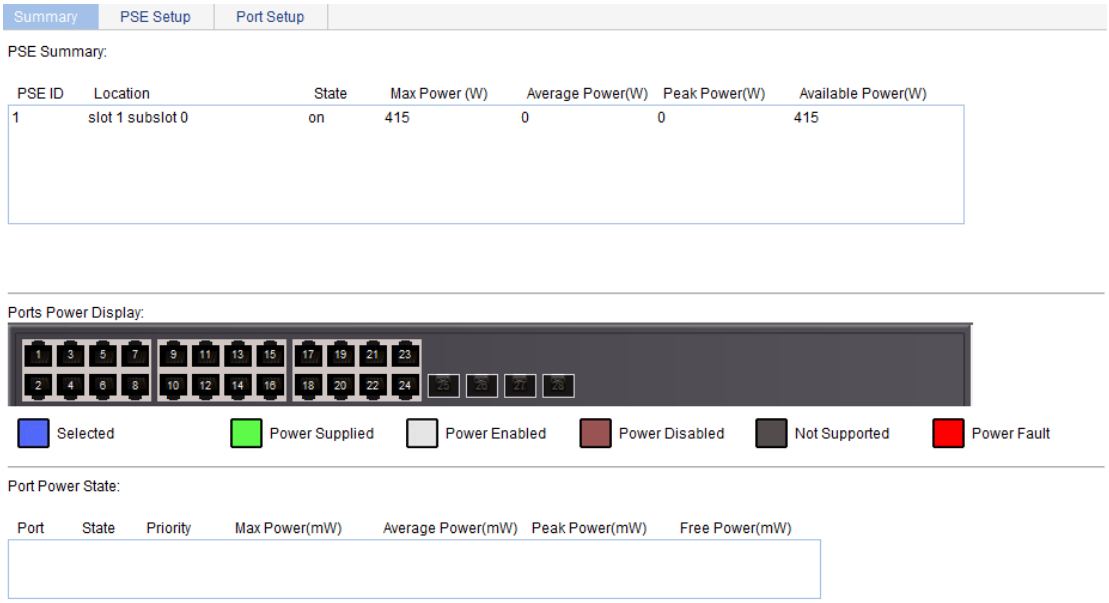
Disabling the non-standard PD detection for all PSEs

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 507 PoE summary (with GigabitEthernet 1/0/1 selected)



PoE configuration example

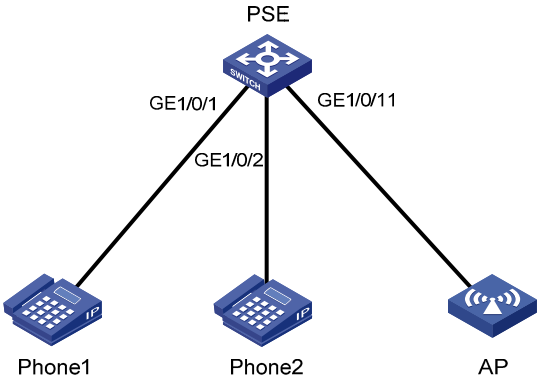
Network requirements

As shown in Figure 508, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are connected to IP telephones.

GigabitEthernet 1/0/11 is connected to AP whose maximum power does not exceed 9000 milliwatts.

The IP telephones have a higher power supply priority than the AP so the PSE supplies power to the IP telephones first if the PSE power is overloaded.

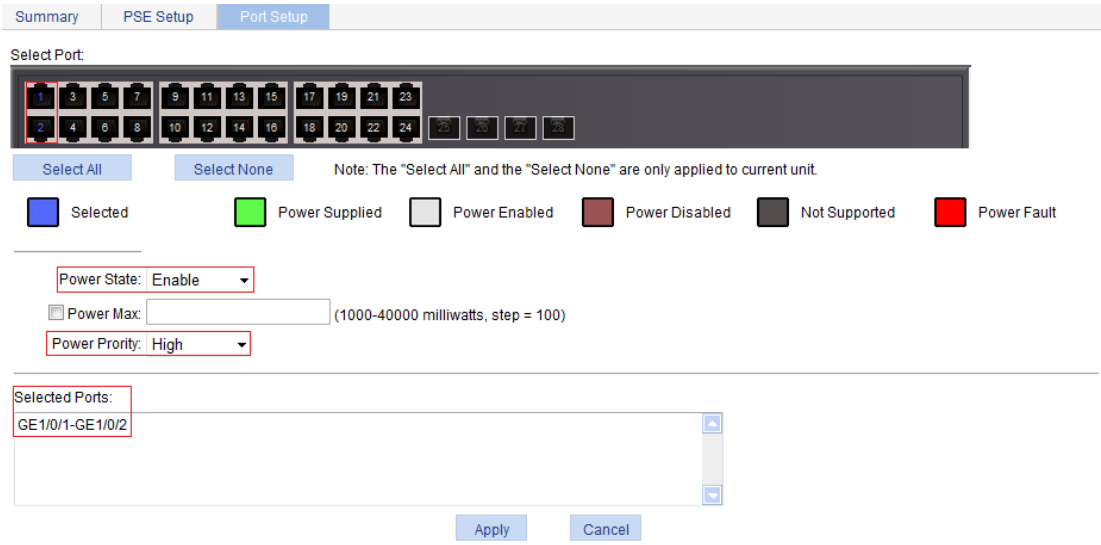
Figure 508 Network diagram



Configuring PoE

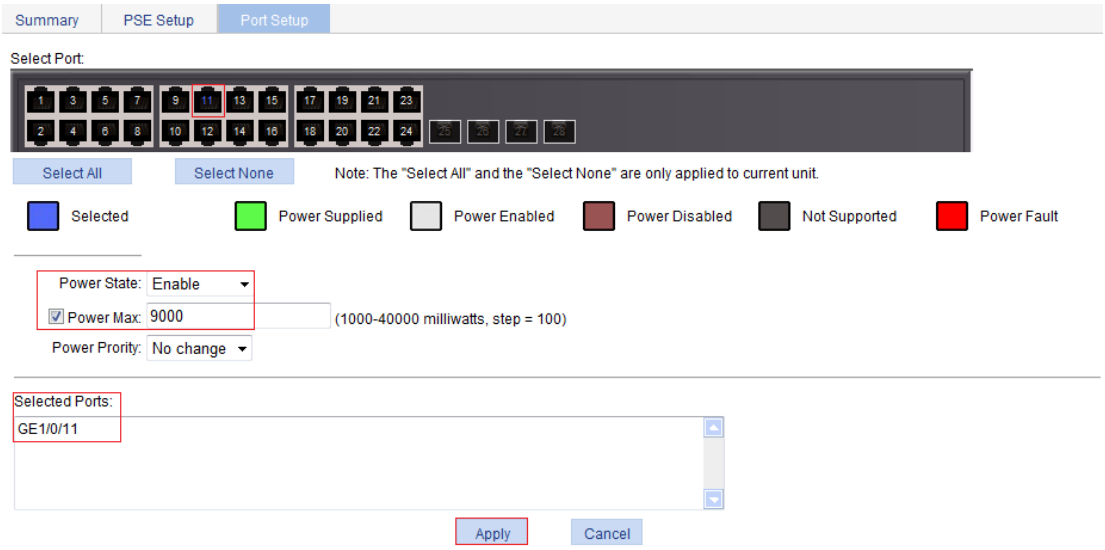
1. Enable PoE on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, and set their power supply priority to **critical**:
   a. Select **PoE** > **PoE** from the navigation tree.
   b. Click the **Setup** tab.
   c. On the tab, click to select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel, select **Enable** from the **Power State** list, and select **Critical** from the **Power Priority** list.
   d. Click **Apply**.

   Figure 509 Configuring the PoE ports supplying power to the IP telephones



2. Enable PoE on GigabitEthernet 1/0/11 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 1/0/11 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 510 Configuring the PoE port supplying power to AP



After the configuration takes effect, the IP telephones and AP are powered and can operate correctly.

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; 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

Convention	Description
	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.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

D

N

Q

S

T