Switch HPE OfficeConnect JG961A

O switch HPE série 1950 é uma família de switches Gigabit com gerenciamento inteligente pela Web e uplinks 10GbE para clientes de pequenas empresas que precisam de conexões avançadas de alto desempenho.

Hewlett Packard Enterprise

HPE OfficeConnect 1950 Switch Series

User Guide

Part number: 5998-8111b
Document version: 6W104-20190520

Acknowledgments

Contents

Overview

This user guide provides the following information:

Information	Section
How to log in to the Web interface for the first time.	Logging in to the Web interface for the first time
How to use the Web interface.	Using the Web interface
What features you can configure from the Web interface. How to access the page for a feature or task.	Feature navigator
How to use features in typical scenarios.	Configuration examples
How to manage the device from the CLI.	Appendix A Managing the device from the CLI

This user guide does not include step-by-step configuration procedures, because the webpages are task oriented by design. A configuration page typically provides links to any pages that are required to complete the task. Users do not have to navigate to multiple pages. For tasks that require navigation to multiple pages, this user guide provides configuration examples.

This user guide also does not provide detailed information about parameters. You can obtain sufficient online help, feature information, and parameter information from the webpages.

Restrictions: Applicable hardware platforms and software versions

Product code	HPE description	Software version
JG960A	HPE OfficeConnect 1950 24G 2SFP+ 2XGT Switch	Release 3111P02 Release 3113P05
JG961A	HPE OfficeConnect 1950 48G 2SFP+ 2XGT Switch	
JG962A	HPE OfficeConnect 1950 24G 2SFP+ 2XGT PoE+(370W) Switch	
JG963A	HPE OfficeConnect 1950 48G 2SFP+ 2XGT PoE+(370W) Switch	
JH295A	HPE OfficeConnect 1950 12XGT 4SFP+ Switch	Release 5103P03

Logging in to the Web interface

Log in to the Web interface through HTTP or HTTPS.

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.

Web browser requirements

As a best practice, use one of the following Web browsers to log in:

- Internet Explorer 8 or higher.
- Google Chrome 10 or higher.
- Mozilla Firefox 4 or higher.
- Opera 11.11 or higher.
- Safari 5.1 or higher.

To access the Web interface, you must use the following browser settings:

- Accept the first-party cookies (cookies from the site you are accessing).
- To ensure correct display of webpage contents after software upgrade or downgrade, clear data cached by the browser before you log in.
- Enable active scripting or JavaScript, depending on the Web browser.
- If you are using a Microsoft Internet Explorer browser, you must enable the following security settings:
  - Run ActiveX controls and plug-ins.
  - Script ActiveX controls marked safe for scripting.

Default login settings

Use the settings in Table 1 for the first login.

Table 1 Default login settings

Item	Setting
Device IP (VLAN-interface 1)	See "Logging in to the Web interface for the first time."
IP address mask	
Username	**admin**
Password	None
User role	network-admin

NOTE:

If the network has a DHCP server, you must use the DHCP assigned IP address to access the device. For more information, see "Logging in to the Web interface for the first time."

Concurrent login users

The Web interface allows a maximum of 32 concurrent accesses. If this limit is reached, login attempts will fail.

Logging in to the Web interface for the first time

IMPORTANT:

As a best practice, change the login information and assign access permissions immediately after the first successful login for security purposes.

By default, HTTP and HTTPS are enabled.

To log in to the Web interface:

1. Use an Ethernet cable to connect the configuration terminal to an Ethernet port on the device.
2. Identify the IP address and mask of the device.
   - If the device is not connected to the network, or no DHCP server exists on the network, the device uses the default IP address and mask. The default mask is 255.255.0.0. The default IP address is 169.254.*xxx*.*xxx*, where *xxx*.*xxx* depends on the last two bytes of the MAC address. Find the MAC address label on the device and use the following rules to determine the last two bytes for the IP address:

Last two bytes of the MAC address	Last two bytes for the IP address
All 0s	0.1
All Fs	255.1
Not all 0s or all Fs	Decimal values of the last two bytes of the MAC address

     For example:

MAC address	IP address
08004E080000	169.254.0.1
08004E08FFFF	169.254.255.1
08004E082A3F	169.254.42.63 (The decimal value of 2A is 42. The value of 3F is 63.)

   - If a DHCP server is available, the device obtains an IP address from the server. To identify the address, log in to the device through the console port, and then execute the **summary** command. The following is the sample output:

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

     For more information about console login, see the getting started guide for the device.
3. Assign the login host an IP address in the same subnet as the device.
4. Open the browser, and then enter login information:

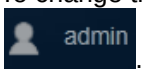
a. In the address bar, enter the IP address of the device.
   - **HTTP access**—Enter the address in the **http://***ip-address***:***port* or *ip-address***:***port* format.
   - **HTTPS access**—Enter the address in the **https://***ip-address***:***port* format.

   The *ip-address* argument represents the IP address of the device. The *port* argument represents the HTTP or HTTPS service port. The default port number is 80 for HTTP and 443 for HTTPS. You do not need to enter the port number if you have not changed the service port setting.

b. On the login page, enter the default username (**admin**) and the verification code.

   You do not need to enter a password at the first login.

c. Click **Login**.

5. Change the login information:
   - To change the password of the login user (**admin** at the first login), click the **Admin** icon 

.
   - To add new user accounts and assign access permissions to different users, select **Device** > **Maintenance** > **Administrators**.

Logging out of the Web interface

IMPORTANT:

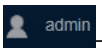
- For security purposes, log out of the Web interface immediately after you finish your tasks.
- You cannot log out by closing the browser.
- The device does not automatically save the configuration when you log out of the Web interface. To prevent the loss of configuration when the device reboots, you must save the configuration.

1. Use one of the following methods to save the current configuration.
   - Click the **Save** icon  in the left corner.
   - Select **Device** > **Maintenance** > **Configuration** to access the configuration management page.
2. Click **Logout** in the upper-left corner of the Web interface.

Using the Web interface

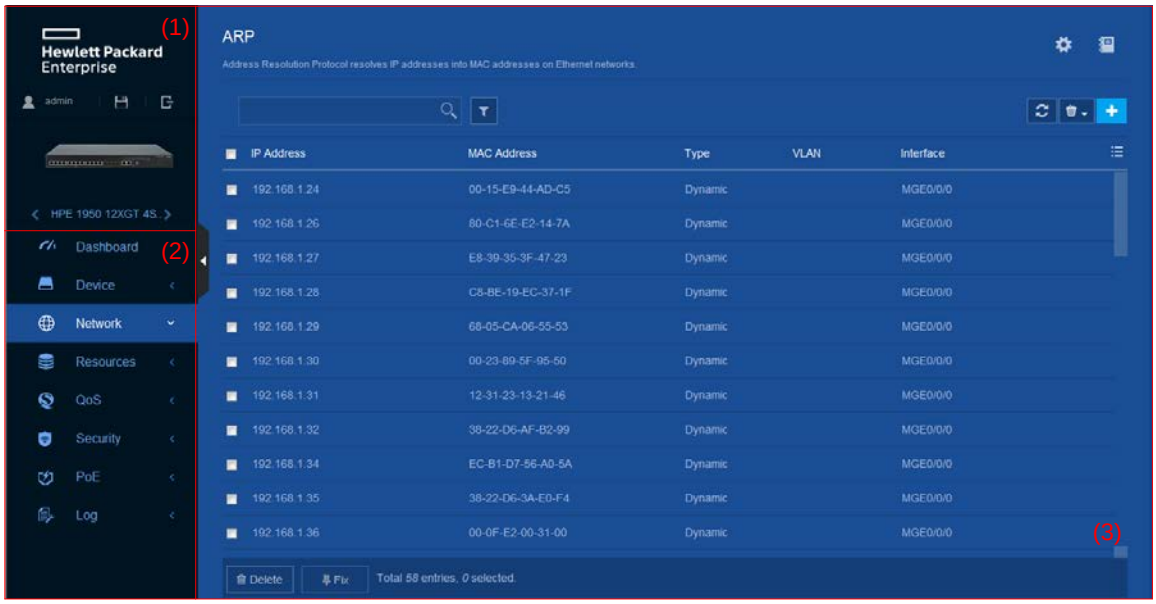
The Web interface contains the following areas:

Area	Description

(1) Banner and auxiliary area	Contains the following items:
	• Basic information, including the Hewlett Packard Enterprise logo, device name, and information about the current login user.
	• Basic management icons:
	  ○ **Admin icon**  —Click this icon to change the login password.
	  ○ **Logout icon**  —Click this icon to log out.
	  ○ **Save icon**  —Click this icon to save the configuration.

(2) Navigation tree	Organizes feature menus in a tree.
(3) Content pane	Displays information and provides an area for you to configure features. Depending on the content in this pane, the webpages include the following types: • **Feature page**—Contains functions or features that a feature module can provide (see "Using a feature page"). • **Table page**—Displays entries in a table (see "Using a table page"). • **Configuration page**—Contains parameters for you to configure a feature or function (see "Using a configuration page").

Figure 1 Web interface layout



1) Banner and auxiliary area	2) Navigation tree	3) Content pane

Types of webpages

Webpages include feature, table, and configuration pages. This section provides basic information about these pages. For more information about using the icons and buttons on the pages, see "Icons and buttons."

Using a feature page

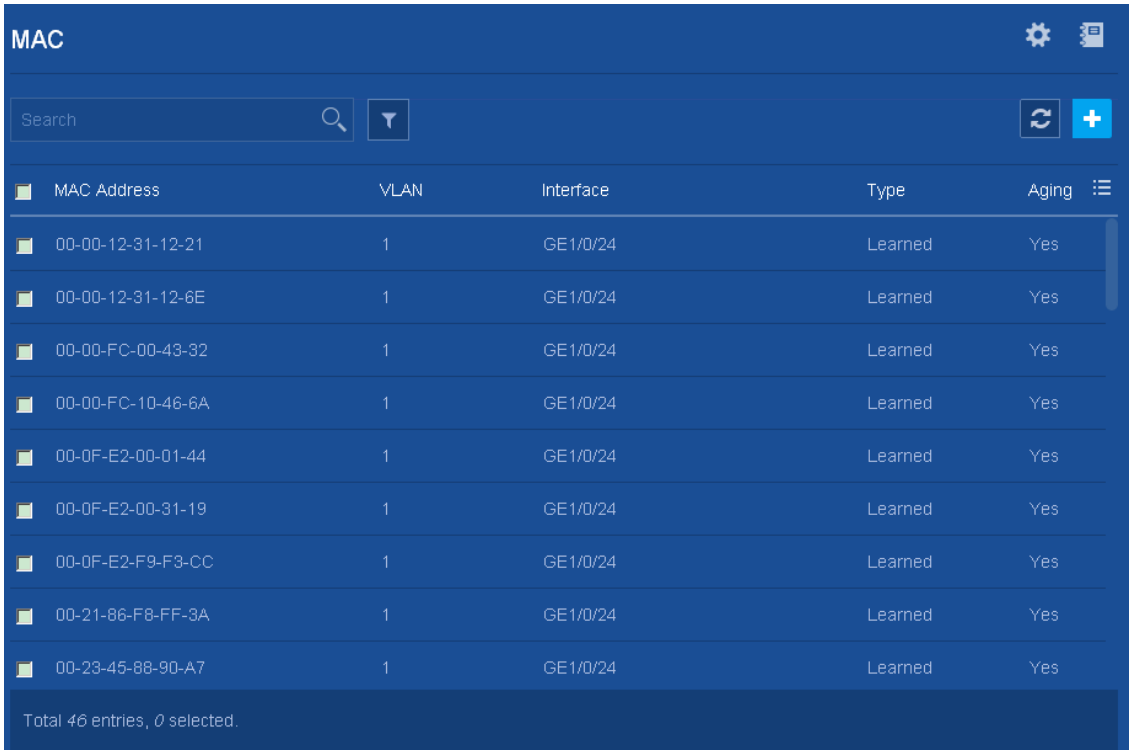
As shown in Figure 2, a feature page contains information about a feature module, including its table entry statistics, features, and functions. From a feature page, you can configure features provided by a feature module.

Figure 2 Sample feature page

Using a table page

As shown in Figure 3, a table page displays entries in a table. To sort entries by a field in ascending or descending order, click the field. For example, click **MAC Address** to sort entries by MAC address.

Figure 3 Sample table page



Using a configuration page

As shown in Figure 4, one configuration page contains all parameters for a configuration task. If a parameter must be configured on another page, the configuration page typically provides a link. You do not need to navigate to the destination page.

For example, you must use an ACL when you configure a packet filter. If no ACLs are available when you perform the task, you can click the **Add** icon to create an ACL. In this situation, you do not need to navigate to the ACL management page.

Figure 4 Sample configuration page

Icons and buttons

Table 2 describes icons and buttons you can use to configure and manage the device.

Table 2 Icons and buttons

Icon/button	Icon/button name	Task
Help icons		
	Help	Obtain help information for a feature.
	Hint	Obtain help information for a function or parameter.
Counter icon		
1	Counter	Identify the total number of table entries.
Navigation icon		
	Next	Access the lower-level page to display information or configure settings.
Status control icon		
OFF	Status control	Control the enable status of the feature. • If **ON** is displayed, the feature is enabled. To disable the feature, click the button. • If **OFF** is displayed, the feature is disabled. To enable the feature, click the button.
Search icons		
	Search	Enter a search expression in the search box, and then click this icon to perform a basic search.

Icon/button	Icon/button name	Task
	Advanced search	Click this icon, and then enter a combination of criteria to perform an advanced search.
Entry management icons		
	Refresh	Refresh table entries manually.
	Add	• Add a new entry. • Confirm the addition of an entry and continue to add an additional entry.
	Detail	Display or modify settings of an entry. This icon appears at the end of an entry when you hover over the entry.
	Delete	Delete an entry. This icon appears at the end of an entry when you hover over the entry.
	Bulk-delete	Select one or multiple entries, and then click this icon to delete the selected entries.
	Field selector	Select fields to be displayed.
Advanced settings icon		
	Advanced settings	Access the configuration page to configure settings.

Performing basic tasks

This section describes the basic tasks that must be frequently performed when you configure or manage the device.

Saving the configuration

Typically, settings take effect immediately after you create them. However, the system does not automatically save the settings to the configuration file. They are lost when the device reboots.

To prevent settings from being lost, use one of the following methods to save the configuration:

- Click the **Save** icon  in the left corner.
- Select **Device** > **Maintenance** > **Configuration** to access the configuration management page.

Displaying or modifying settings of a table entry

1. Hover over the entry.
2. Click the **Detail** icon  at the end of the entry.

Rebooting the device

Reboot is required for some settings (for example, the stack setup) to take effect.

To reboot the device:

1. Save the configuration.
2. Select **Device** > **Maintenance** > **Reboot**.
3. On the reboot page, click the reboot button.

Feature navigator

Menu items and icons available to you depend on the user roles you have. By default, you can use any user roles to display information. To configure features, you must have the **network-admin** user role.

This chapter describes all menus available for the **network-admin** user role. The top-level menu includes **Dashboard**, **Device**, **Network**, **Resources**, **QoS**, **Security**, **PoE**, and **Log**. For each top menu, a navigator table is provided. Use the navigator tables to navigate to the pages for the tasks you want to perform.

For example:

- To change the default device name, select **Device** > **Maintenance** > **Settings** from the navigation tree.
- To delete an IPv4 ACL, select **Resources** > **ACL** > **IPv4** from the navigation tree.

NOTE:

In the navigator tables, a menu is in boldface if it has submenus.

Dashboard menu

The dashboard menu provides an overview of the system and its running status, including:

- System logs.
- System utilization.
- System info.

This menu does not contain submenus.

Device menu

Use Table 3 to navigate to the tasks you can perform from the **Device** menu.

Table 3 Device menu navigator

Menus	Tasks
Maintenance	
Settings	• Configure basic device settings, including the device name, location, and contact. • Configure the system time settings. You can manually set the system time, or configure the device to obtain the UTC time from a trusted time source and calculate the system time.
Administrators	• Create, modify, or delete user roles. • Create, modify, or delete user accounts. • Assign user roles to administrators for access control. • Manage passwords.

Menus	Tasks
Configuration	• Save the running configuration. • Import configuration and export the running configuration. This task is not supported in Release 3111P02. • Display the running configuration. • Restore the factory-default configuration.
File System	• Display storage medium information. • Display file and folder information. • Delete files. • Download and upload files

Upgrade	• Upgrade software images.
	• Display software image lists, including:
	  ○ Current software images.
	  ○ Main and backup startup software images.

Diagnostics	Collect diagnostic information used for system diagnostics and troubleshooting.
Reboot	Reboot the device.
About	Display basic device information, including: • Device name. • Serial number. • Version information. • Electronic label. • Legal statement.
Virtualization	

IRF	• Configure the following settings to set up an HPE OfficeConnect 1950 stack:
	  ○ Member ID.
	  ○ Priority.
	  ○ Domain ID.
	  ○ Stack port bindings.
	• Display the stack topology.

Network menu

Use Table 4 to navigate to the tasks you can perform from the **Network** menu.

Table 4 Network menu navigator

Menus	Tasks
Probe	
Ping	• Test the connectivity to a device in an IPv4 network. • Test the connectivity to a device in an IPv6 network.
Tracert	• IPv4 Tracert. • IPv6 Tracert.
Interfaces	

Menus	Tasks

Interfaces	• Display interfaces and their attributes, including:
	  ○ Interface status.
	  ○ IP address.
	  ○ Speed and duplex mode.
	  ○ Interface description.
	• Change interface settings.
	• Delete logical interfaces.

Link Aggregation	Create, modify, or delete Layer 2 aggregation groups.
Storm Constrain	• Set the statistics polling interval. • Set storm control parameters. • Display storm control information.
Isolation	• Create isolation groups. • Modify isolation groups.
Links	
VLAN	• Configure port-based VLANs. • Create VLAN-interfaces.
Voice VLAN	• Assign ports to voice VLANs. • Set the port mode to manual or automatic. • Set the voice VLAN mode to normal or security. • Configure the QoS settings for voice packets. • Add OUI addresses.
MAC	• Create or delete static MAC entries, dynamic MAC entries, and blackhole MAC entries. • Display existing MAC entries.
STP	• Enable or disable STP globally. • Enable or disable STP on interfaces. • Configure the STP operating mode as STP, RSTP, PVST, or MSTP. • Configure instance priorities. • Configure MST regions.
LLDP	• Enable or disable LLDP. • Modify the LLDP operating mode. • Modify the interface mode. • Configure LLDP to advertise the specified TLVs.

DHCP Snooping	• Configure a port as a trusted or untrusted port.
	• Record and back up DHCP snooping entries.
	• Configure the following features for DHCP snooping ports:
	  ○ MAC address check.
	  ○ DHCP-REQUEST check.
	  ○ DHCP packet rate limit.
	  ○ Max DHCP snooping entries.
	• Enable support for Option 82. If Option 82 is enabled, you can configure the handling strategy, the padding format, and the padding contents for Option 82.

IP	
IP	• Configure the method to obtain an IP address (DHCP or static). • Configure the IP address or MTU of an interface. • Create a loopback interface.

Menus	Tasks
ARP	• Manage dynamic ARP entries and static ARP entries. • Configure ARP proxy. • Configure gratuitous ARP. • Configure ARP attack protection.
DNS	• Configure IPv4 static domain name resolution. • Configure IPv4 dynamic domain name resolution. • Configure the DNS proxy. • Configure IPv4 domain name suffixes.
Dynamic DNS	• Manage dynamic DNS policies. • Configure an interface to be associated with the dynamic DNS policy.
IPv6	
IPv6	• Configure the method to obtain an IPv6 address (manual assignment, dynamic assignment, or auto generation). • Configure the IPv6 address of an interface. • Create a loopback interface.

ND	• Manage dynamic ND entries and static ND entries.
	• Configure the aging time for stale ND entries.
	• Minimize link-local ND entries.
	• Configure hop limit.
	• Configure RA prefix attributes, including:
	  ○ Address prefix.
	  ○ Prefix length.
	  ○ Valid lifetime.
	  ○ Preferred lifetime.
	• Configure RA settings for an interface, including:
	  ○ RA message suppression.
	  ○ Maximum and minimum intervals for sending RA messages.
	  ○ Hop limit.
	  ○ M-flag.
	  ○ O-flag.
	  ○ Router lifetime.
	  ○ NS retransmission interval.
	  ○ Router preference.
	  ○ Neighbor reachable time.
	• Enable common and local ND proxy on an interface.
	• Configure ND rules for the interface.

DNS	• Configure static and dynamic IPv6 domain name resolution. • Configure the IPv6 DNS proxy. • Configure IPv6 domain name suffixes.
Mirroring	
Port Mirroring	• Configure local mirroring groups. • Configure remote mirroring groups.
Routing	
Routing Table	Display IPv4 and IPv6 routing table information, including brief routing table information and route statistics.

Menus	Tasks
Static Routing	• Display IPv4 and IPv6 static route entries. • Create, modify, and delete IPv4 and IPv6 static route entries.
Policy-Based Routing	• Create, modify, and delete IPv4 and IPv6 policies. • Configure interface PBR. • Configure local PBR.
Multicast	

IGMP Snooping	• Configure IGMP snooping functions, including:
	  ○ Enable dropping unknown multicast data.
	  ○ Configure the IGMP snooping querier.
	  ○ Enable fast-leave processing.
	  ○ Set the maximum number of multicast groups on a port.

MLD Snooping	• Configure MLD snooping functions, including:
	  ○ Enable dropping unknown IPv6 multicast data.
	  ○ Configure the MLD snooping querier.
	  ○ Enable fast-leave processing.
	  ○ Set the maximum number of IPv6 multicast groups on a port.

Service	

DHCP	• Configure DHCP server functions, including:
	  ○ Configure DHCP services.
	  ○ Configure the interface to operate in the DHCP server mode.
	  ○ Configure DHCP address pools.
	  ○ Configure the IP address conflict detection.
	• Configure DHCP relay agent functions, including:
	  ○ Configure DHCP services.
	  ○ Configure the DHCP relay agent mode
	  ○ Configure the IP address of the DHCP server
	• Configure settings for DHCP relay entry, include:
	  ○ Recording of DHCP relay entries.
	  ○ Periodic refreshing of DHCP relay entries.
	  ○ Interval for refreshing DHCP relay entries.

HTTP/HTTPS	• Enable or disable HTTP service. • Enable or disable HTTPS service. • Set the Web connection idle timeout. • Set the HTTP service port number. • Set the HTTPS service port number. • Specify Web access control ACLs.
SSH (not available in Release 3111P02)	• Enable the Stelnet, SFTP, and SCP services. • Set the DSCP in packets sent by the device. • Filter SSH clients by using an ACL. • Set the SFTP connection idle timeout time.
FTP	• Enable or disable FTP service. • Set the DSCP value for the device to use for outgoing FTP packets. • Specify the FTP access control ACL. • Set the FTP connection idle timeout.

Menus	Tasks
Telnet	• Enable or disable Telnet service. • Set the DSCP values for the device to use for outgoing IPv4 or IPv6 Telnet packets. • Specify Telnet access control ACLs.
NTP	Configure the device to use the local clock as the reference clock.
SNMP	• Enable SNMP. • Configure SNMP parameters such as version, community name, group, and users. • Configure the notification sending function.

Resources menu

The **Resources** menu contains common resources that can be used by multiple features. For example, you can use an ACL both in a packet filter to filter traffic and in a QoS policy to match traffic.

Use Table 5 to navigate to the tasks you can perform from the **Resources** menu.

Table 5 Resources menu navigator

Menus	Tasks
ACLs	
IPv4	• Create, modify, or delete an IPv4 basic ACL. • Create, modify, or delete an IPv4 advanced ACL.
IPv6	• Create, modify, or delete an IPv6 basic ACL. • Create, modify, or delete an IPv6 advanced ACL.
Ethernet	Create, modify, or delete an Ethernet frame header ACL.
Time Range	
Time Range	
SSL	
SSL	• Create, modify, or delete an SSL client policy. • Create, modify, or delete an SSL server policy.
Public key	
Public key	• Manage local asymmetric key pairs. • Manage peer host public keys.
PKI	
PKI	• Manage CA and local certificates. • Create, modify, or delete a PKI domain or PKI entity.
Certificate Access Control	• Create, modify, or delete a certificate access control policy. • Create, modify, or delete a certificate attribute group.

NOTE:

You can create ACLs from ACL pages or during the process of configuring a feature that uses ACLs. However, to modify or delete an ACL, you must access the **ACL** menu.

QoS menu

Use Table 6 to navigate to the tasks you can perform from the **QoS** menu.

Table 6 QoS menu navigator

Menus	Tasks
QoS	
QoS Policies	• Create, modify, or delete interface QoS policies. • Create, modify, or delete VLAN QoS policies. • Create, modify, or delete global QoS policies.
Hardware Queuing	Modify hardware queuing configuration.

Priority Mapping	• Configure the port priority.
	• Configure the priority trust mode for a port.
	• Configure priority maps:
	  ○ Apply and reset the 802.1p-to-local priority map.
	  ○ Apply and reset the DSCP-to-802.1p priority map.
	  ○ Apply and reset the DSCP-to-DSCP priority map.

Rate Limit	Create, modify, or delete rate limit.

Security menu

Use Table 7 to navigate to the tasks you can perform from the **Security** menu.

Table 7 Security menu navigator

Menus	Tasks
Packet Filter	
Packet Filter	• Create, modify, or delete a packet filter for an interface, a VLAN, or the system. • Configure the default action for the packet filter.
IP Source Guard	Configure an interface-specific static IPv4 source guard binding.
Access Control	
802.1X	• Enable or disable 802.1X. • Configure the 802.1X authentication method. • Configure the port access control method. • Configure the port authorization state. • Configure the authentication ISP domain on a port.
MAC Authentication	• Enable or disable MAC authentication. • Configure the username format. • Configure the MAC authentication ISP domain.
Port Security	• Enable or disable port security • Configure the port security mode. • Configure the intrusion protection action. • Configure the NTK mode. • Configure secure MAC aging mode.

Menus	Tasks
Portal	• Configure a portal authentication server. • Configure a portal Web server. • Configure a local portal Web server. • Create portal-free rules. • Create interface policies.
Authentication	
ISP Domains	Configure ISP domains.
RADIUS	Configure RADIUS schemes.
TACACS	Configure TACACS schemes.
Local Users	Configure local users.

PoE menu

Use Table 8 to navigate to the tasks you can perform from the **PoE** menu.

Table 8 PoE menu navigator

Menus	Tasks
PoE	• Configure the maximum PoE power and power alarm threshold for the device. • Enable or disable PoE on an interface. • Configure the maximum PoE power, power supply priority, PD description, and fault description for an interface.

Log menu

Use Table 9 to navigate to the tasks you can perform from the **Log** menu.

Table 9 Log menu navigator

Menus	Tasks
Log	
System Log	• Display log information. • Query, collect, and delete log information.
Settings	• Enable or disable log output to the log buffer, and configure the maximum number of logs in the log buffer. • Configure the address and port number of log hosts.

Device management

Settings

Access the **Settings** page to change the device name, location, and system time.

System time sources

Correct system time is essential to network management and communication. Configure the system time correctly before you run the device on the network.

The device can use the manually set system time, or obtain the UTC time from a time source on the network and calculate the system time.

- When using the locally set system time, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.
- If you change the time zone or daylight saving settings without changing the date or time, the device adjusts the system time based on the new settings.
- After obtaining the UTC time from a time source, the device uses the UTC time and the time zone and daylight saving settings to calculate the system time. Then, the device periodically synchronizes the UTC time and recalculates the system time.
- If you change the time zone or daylight saving settings, the device recalculates the system time.

The system time calculated by using the UTC time from a time source is more precise.

Make sure the time zone and daylight saving setting are the same as the parameters of the place where the device resides.

If the system time does not change accordingly when the daylight saving period ends, refresh the Web interface.

Clock synchronization protocols

The device supports the following clock synchronization protocols:

- **NTP**—Network Time Protocol. NTP is typically used in large networks to dynamically synchronize time among network devices. It provides higher clock accuracy than manual system time configuration.
- **SNTP**—Simple NTP, a simpler implementation of NTP. SNTP uses the same packet formats and exchange procedures as NTP. However, SNTP simplifies the clock synchronization procedure. Compared with NTP, SNTP uses less resources and implements clock synchronization in shorter time, but it is not as accurate as NTP.

NTP/SNTP operating modes

NTP supports two operating modes: client/server mode and symmetric active/passive mode. The device can act only as a client in client/server mode or the active peer in symmetric active/passive mode.

SNTP supports only the client/server mode. The device can act only as a client.

Table 10 NTP/SNTP operating modes

Mode	Operating process	Principle	Application scenario
Client/server	1. A client sends a clock synchronization message to the NTP servers. 2. Upon receiving the message, the servers automatically operate in server mode and send a reply. 3. If the client is synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source. You can configure multiple time servers for a client. This operating mode requires that you specify the IP address of the NTP server on the client.	A client can synchronize to a server, but a server cannot synchronize to a client.	This mode is intended for scenarios where devices of a higher stratum synchronize to devices with a lower stratum.
Symmetric active/passive	1. A symmetric active peer periodically sends clock synchronization messages to a symmetric passive peer. 2. The symmetric passive peer automatically operates in symmetric passive mode and sends a reply. 3. If the symmetric active peer can be synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source. You must specify the IP address of the symmetric passive peer on the symmetric active peer.	A symmetric active peer and a symmetric passive peer can be synchronized to each other. If both of them are synchronized, the peer with a higher stratum is synchronized to the peer with a lower stratum.	This mode is most often used between servers with the same stratum to operate as a backup for one another. If a server fails to communicate with all the servers of a lower stratum, the server can still synchronize to the servers of the same stratum.

NTP/SNTP time source authentication

The time source authentication function enables the device to authenticate the received NTP or SNTP packets. This feature ensures that the device obtains the correct GMT.

Administrators

An administrator configures and manages the device from the following aspects:

- **User account management**—Manages user account information and attributes (for example, username and password).
- **Role-based access control**—Manages user access permissions by user role.
- **Password control**—Manages user passwords and controls user login status based on predefined policies.

The service type of an administrator can be SSH, Telnet, FTP, HTTP, HTTPS, PAD, or terminal. A terminal user can access the device through the console, Aux, or Async port.

User account management

A user account on the device manages attributes for users who log in to the device with the same username. The attributes include the username, password, services, and password control parameters.

Role-based access control

Assign users user roles to control the users' access to functions and system resources. Assigning permissions to a user role includes the following:

- Defines a set of rules to determine accessible or inaccessible functions for the user role.
- Configures resource access policies to specify which interfaces and VLANs are accessible to the user role.

To configure a function related to a resource (an interface or VLAN), a user role must have access to both the function and the resource.

Resource access policies

Resource access policies control access of user roles to system resources and include the following types:

- **Interface policy**—Controls access to interfaces.
- **VLAN policy**—Controls access to VLANs.

You can perform the following tasks on an accessible interface, VLAN:

- Create or remove the interface or VLAN.
- Configure attributes for the interface or VLAN.
- Apply the interface or VLAN to other parameters.

Predefined user roles

The system provides predefined user roles. These user roles have access to all system resources (interfaces and VLANs). Their access permissions differ.

If the predefined user roles cannot meet the access requirements, you can define new user roles to control the access permissions for users.

IMPORTANT:

The security-audit user role has access only to security log menus. Security log menus are not supported on the current Web interface, so do not assign the security-audit user role to any users.

Assigning user roles

Depending on the authentication method, user role assignment has the following methods:

- **Local authorization**—If the user passes local authorization, the device assigns the user roles specified in the local user account.
- **Remote authorization**—If the user passes remote authorization, the remote AAA server assigns the user roles specified on the server.

A user who fails to obtain a user role is logged out of the device.

If multiple user roles are assigned to a user, the user can use the collection of functions and resources accessible to all the user roles.

Password control

Password control allows you to implement the following features:

- Manage login and super password setup, expirations, and updates for device management users.
- Control user login status based on predefined policies.

Local users are divided into device management users and network access users. This feature applies only to device management users.

Minimum password length

You can define the minimum length of user passwords. If a user enters a password that is shorter than the minimum length, the system rejects the password.

Password composition policy

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters. See Table 11.

Table 11 Special characters

Character name	Symbol	Character name	Symbol
Ampersand sign	&	Apostrophe	'
Asterisk	*	At sign	@
Back quote	`	Back slash	\
Blank space	N/A	Caret	^
Colon	:	Comma	,
Dollar sign	$	Dot	.
Equal sign	=	Exclamation point	!
Left angle bracket	<	Left brace	{
Left bracket	[	Left parenthesis	(
Minus sign	-	Percent sign	%
Plus sign	+	Pound sign	#
Quotation marks	"	Right angle bracket	>
Right brace	}	Right bracket	]
Right parenthesis	)	Semi-colon	;
Slash	/	Tilde	~
Underscore	_	Vertical bar	|

Depending on the system's security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters for each type, as shown in Table 12.

Table 12 Password composition policy

Password combination level	Minimum number of character types	Minimum number of characters for each type
Level 1	One	One
Level 2	Two	One
Level 3	Three	One
Level 4	Four	One

When a user sets or changes a password, the system checks if the password meets the combination requirement. If the password does not meet the requirement, the operation fails.

Password complexity checking policy

A weak password such as a password that contains the username or repeated characters is easy to be cracked. For higher security, you can configure a password complexity checking policy to ensure that all user passwords are complex enough to be secure. With such a policy configured, the system checks password complexity when a user configures a password. If the password is complexity-incompliant, the configuration will fail.

You can apply the following password complexity requirements:

- A password cannot contain the username or the reverse of the username. For example, if the username is abc, a password such as abc982 or 2cba is not complex enough.
- A character or number cannot be included three or more times consecutively. For example, password a111 is not complex enough.

Password updating

This feature allows you to set the minimum interval at which users can change their passwords. If a user logs in to change the password but the time passed since the last change is less than this interval, the system denies the request. For example, if you set this interval to 48 hours, a user cannot change the password twice within 48 hours.

The set minimum interval is not effective when a user is prompted to change the password at the first login or after its password aging time expires.

Password expiration

Password expiration imposes a lifecycle on a user password. After the password expires, the user needs to change the password.

If a user enters an expired password when logging in, the system displays an error message. The user is prompted to provide a new password and to confirm it by entering it again. The new password must be valid, and the user must enter exactly the same password when confirming it.

Telnet users, SSH users, and console users can change their own passwords. The administrator must change passwords for FTP users.

Early notice on pending password expiration

When a user logs in, the system checks whether the password will expire in a time equal to or less than the specified notification period. If so, the system notifies the user when the password will expire and provides a choice for the user to change the password. If the user sets a new password that is complexity-compliant, the system records the new password and the setup time. If the user chooses not to change the password or the user fails to change it, the system allows the user to log in using the current password.

Telnet users, SSH users, and console users can change their own passwords. The administrator must change passwords for FTP users.

Login with an expired password

You can allow a user to log in a certain number of times within a period of time after the password expires. For example, if you set the maximum number of logins with an expired password to 3 and the time period to 15 days, a user can log in three times within 15 days after the password expires.

Password history

With this feature enabled, the system stores passwords that a user has used. When a user changes the password, the system checks the new password against the current password and those stored in the password history records. The new password must be different from the current one and those stored in the history records by at least four characters. The four characters must be different from one another. Otherwise, the system will display an error message, and the password will not be changed.

You can set the maximum number of history password records for the system to maintain for each user. When the number of history password records exceeds your setting, the most recent record overwrites the earliest one.

Current login passwords of device management users are not stored in the password history, because a device management user password is saved in cipher text and cannot be recovered to a plaintext password.

Login attempt limit

Limiting the number of consecutive login failures can effectively prevent password guessing.

Login attempt limit takes effect on FTP and VTY users. It does not take effect on the following types of users:

- Nonexistent users (users not configured on the device).
- Users logging in to the device through console ports.

If a user fails to use a user account to log in after making the maximum number of consecutive attempts, login attempt limit takes the following actions:

- Adds the user account and the user's IP address to the password control blacklist. This account is locked for only this user. Other users can still use this account, and the blacklisted user can use other user accounts.
- Limits the user and user account in any of the following ways:
  - Disables the user account until the account is manually removed from the password control blacklist.
  - Allows the user to continue using the user account. The user's IP address and user account are removed from the password control blacklist when the user uses this account to successfully log in to the device.
  - Disables the user account for a period of time.

    The user can use the account to log in when either of the following conditions exist:

    - The locking timer expires.
    - The account is manually removed from the password control blacklist before the locking timer expires.

Maximum account idle time

You can set the maximum account idle time for user accounts. When an account is idle for this period of time since the last successful login, the account becomes invalid.

HPE OfficeConnect 1950 stacking (IRF)

Intelligent Resilient Framework (IRF) is true stacking technology that creates a large virtual stack from multiple devices to provide high availability and scalability. This stacking technology offers

processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

A stack provides a single point of management. You can access the stack from any member device to configure and manage all the members as if they were interface modules on one node. Settings will be issued to all member devices in the stack.

The following information describes the concepts that you might encounter when you use stacking.

NOTE:

Stacking and stack are called IRF on the webpages and in online help.

Stack member roles

HPE OfficeConnect 1950 stacking uses two member roles: master and standby (also called subordinate).

When devices form a stack, they elect a master to manage and control the stack. All the other members process services while backing up the master. When the master device fails, the other devices automatically elect a new master.

Stack port

A stack port is a logical interface for the connection between stack member devices. Every stackable device supports two stack ports. The stack ports are referred to as IRF-port 1 and IRF-port 2.

To use a stack port, you must bind a minimum of one physical interface to it. The physical interfaces assigned to a stack port automatically form an aggregate stack link.

When you connect two neighboring stack members, connect the physical interfaces of IRF-port 1 on one member to the physical interfaces of IRF-port 2 on the other.

Stack physical interfaces

Stack physical interfaces connect stack member devices and must be bound to a stack port. They forward stack protocol packets and data packets between stack member devices.

You can use 10GBase-T or SFP+ ports for stack links.

To connect the 10GBase-T Ethernet ports in a short distance, you can use Category 6A (or above) twisted-pair cables.

To connect the SFP+ ports in a short distance, you can use SFP+ DAC cables.

To connect the SFP+ ports in a long distance, you must use SFP+ transceiver modules and fibers.

You can assign fiber and copper ports to the same stack port. However, the ports at the two ends of a stack link must be the same type.

Stack domain ID

One stack forms one stack domain. Stack domain IDs uniquely identify stacks and prevents stacks from interfering with one another.

Stack split and stack merge

A stack split occurs when a virtual stack breaks up into two or more virtual stacks because of stack link failures.

A stack merge occurs when two split virtual stacks reunite or when two independent stacks are united.

Member priority

Member priority determines the possibility of a member device to be elected the master. A member with higher priority is more likely to be elected the master.

The default member priority is 1. You can change the member priority of a device to affect the master election result.

Network services features

Link aggregation

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.

Aggregation group

Link bundling is implemented through interface bundling. An aggregation group is a group of Ethernet interfaces bundled together. These Ethernet interfaces are called member ports of the aggregation group. Each aggregation group has a corresponding logical interface (called an aggregate interface).

When you create an aggregate interface, the device automatically creates an aggregation group of the same type and number as the aggregate interface. For example, when you create Layer 2 aggregate interface 1, Layer 2 aggregation group 1 is created.

You can assign Layer 2 Ethernet interfaces only to a Layer 2 aggregation group.

The port rate of an aggregate interface equals the total rate of its Selected member ports. Its duplex mode is the same as that of the Selected member ports.

Aggregation states of member ports in an aggregation group

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

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

Operational key

When aggregating ports, the system automatically assigns each port an operational key based on port information, such as port rate and duplex mode. Any change to this information triggers a recalculation of the operational key.

In an aggregation group, all Selected ports have the same operational key.

Attribute configurations

To become a Selected port, a member port must have the same attribute configurations as the aggregate interface.

Feature	Considerations
Port isolation	Indicates whether the port has joined an isolation group, and the isolation group to which the port belongs.
VLAN	VLAN attribute configurations include: • Permitted VLAN IDs. • PVID. • VLAN tagging mode.

Link aggregation modes

An aggregation group operates in one of the following modes:

- **Static**—Static aggregation is stable. An aggregation group in static mode is called a static aggregation group. The aggregation states of the member ports in a static aggregation group are not affected by the peer ports.
- **Dynamic**—An aggregation group in dynamic mode is called a dynamic aggregation group. The local system and the peer system automatically maintain the aggregation states of the member ports, which reduces the administrators' workload.

An aggregation group in either mode must choose a reference port and then set the aggregation state of its member ports.

1. Aggregating links in static mode

When setting the aggregation states of the ports in an aggregation group, the system automatically picks a member port as the reference port. A Selected port must have the same operational key and attribute configurations as the reference port.

The system chooses a reference port from the member ports that are in up state and have the same attribute configurations as the aggregate interface.

The candidate ports are sorted in the following order:

a. Highest port priority.

b. Full duplex/high speed.

c. Full duplex/low speed.

d. Half duplex/high speed.

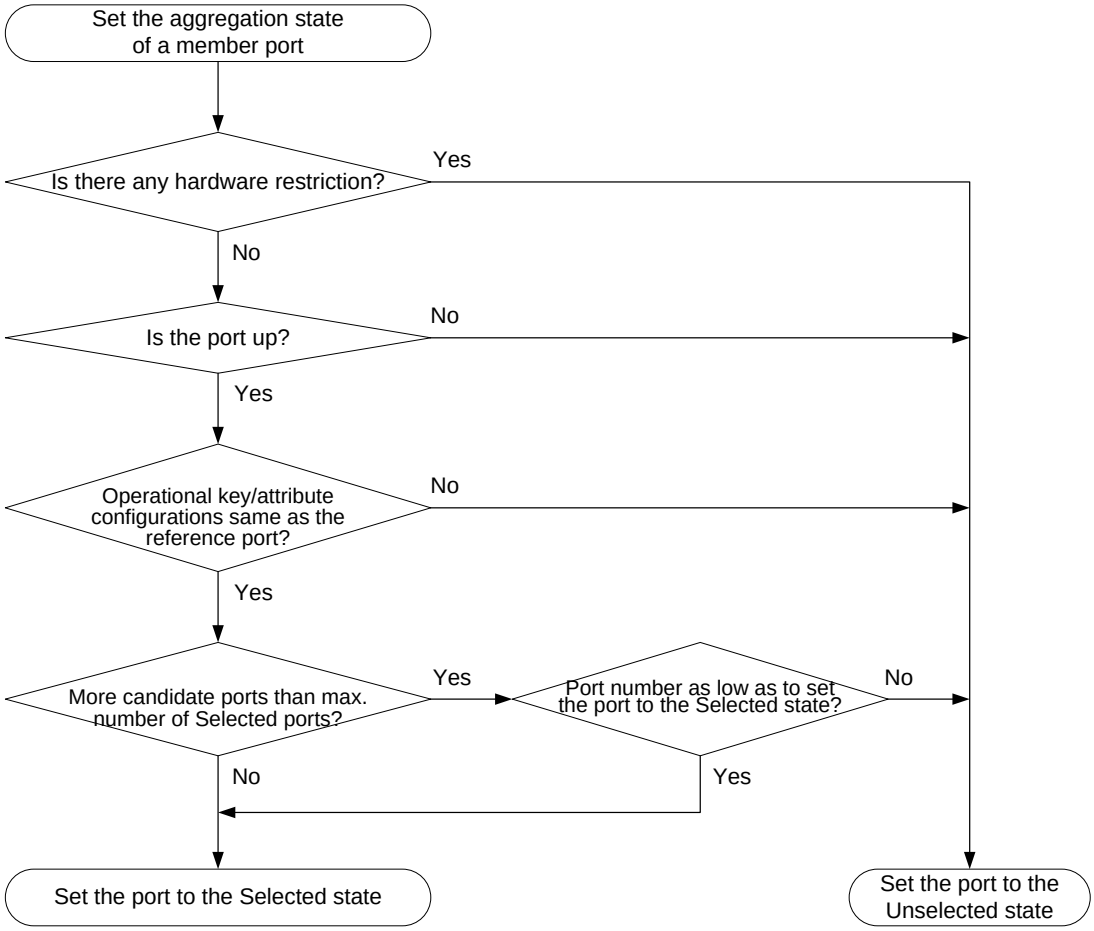
e. Half duplex/low speed.

The candidate port at the top is chosen as the reference port.

- If multiple ports have the same port priority, duplex mode, and speed, the port that has been a Selected port (if any) is chosen. If multiple ports have been Selected ports, the one with the smallest port number is chosen.
- If multiple ports have the same port priority, duplex mode, and speed and none of them has been a Selected port, the port with the smallest port number is chosen.

After the reference port is chosen, the system sets the aggregation state of each member port in the static aggregation group.

Figure 5 Setting the aggregation state of a member port in a static aggregation group



2. Aggregating links in dynamic mode

Dynamic aggregation is implemented through IEEE 802.3ad Link Aggregation Control Protocol (LACP).

LACP uses LACPDUs to exchange aggregation information between LACP-enabled devices.

Each member port in an LACP-enabled aggregation group exchanges information with its peer. When a member port receives an LACPDU, it compares the received information with information received on the other member ports. In this way, the two systems reach an agreement on which ports are placed in the Selected state.

The system chooses a reference port from the member ports that are in up state and have the same attribute configurations as the aggregate interface. A Selected port must have the same operational key and attribute configurations as the reference port.

The local system (the actor) and the peer system (the partner) negotiate a reference port by using the following workflow:

a. The two systems compare their system IDs to determine the system with the smaller system ID.

A system ID contains the system LACP priority and the system MAC address.

- The two systems compare their LACP priority values.

  The lower the LACP priority, the smaller the system ID. If LACP priority values are the same, the two systems proceed to compare their MAC addresses.

- The two systems compare their MAC addresses.

  The lower the MAC address, the smaller the system ID.

b. 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 lower the port priority, the smaller the port ID.

- The system chooses the port with the lowest priority value as the reference port.

  If ports have the same priority, the system proceeds to the next step.

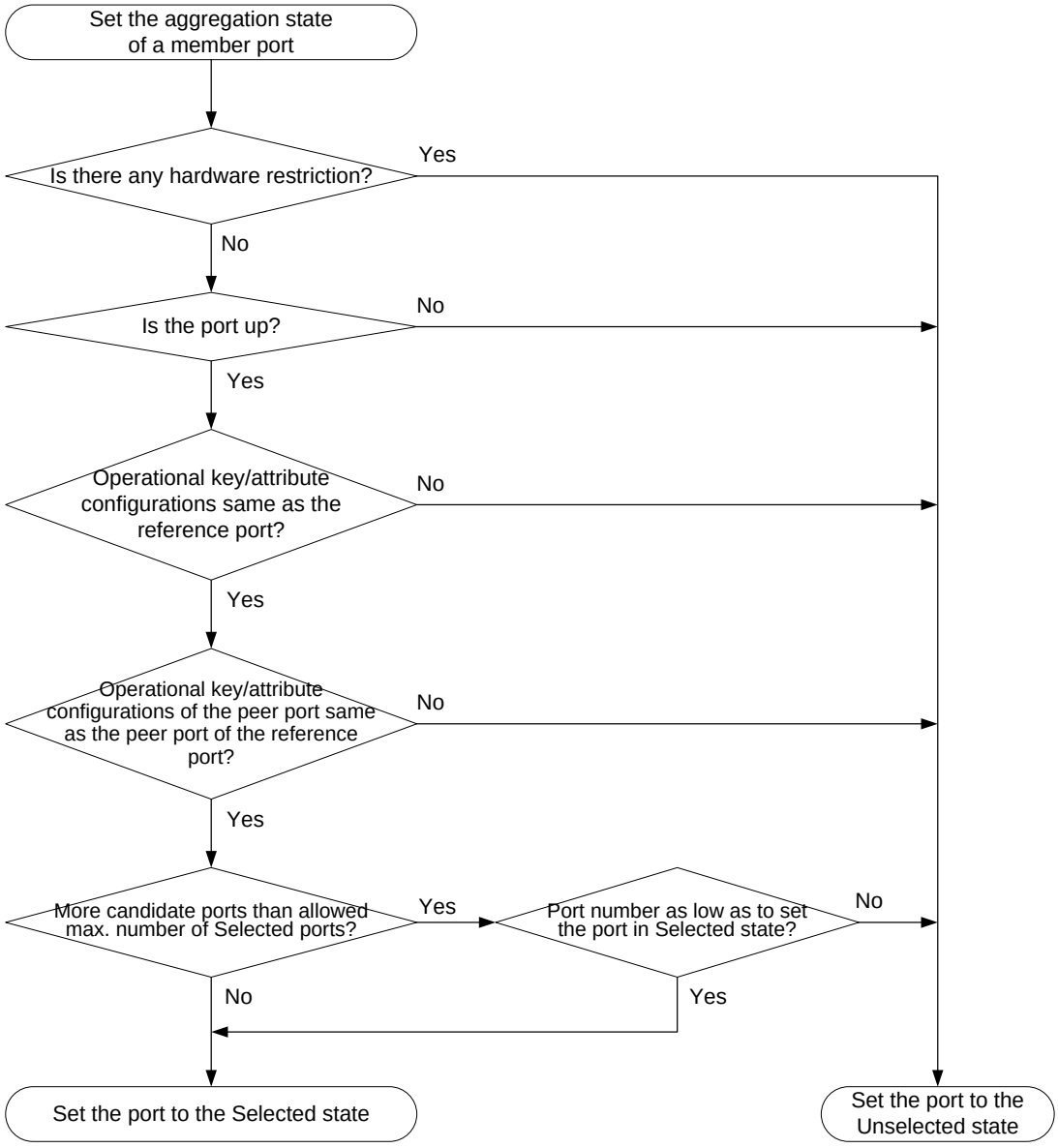
- The system compares their port numbers.

  The smaller the port number, the smaller the port ID.

  The port with the smallest port number and the same attribute configurations as the aggregate interface is chosen as the reference port.

After the reference port is chosen, the system with the smaller system ID sets the state of each member port on its side.

Figure 6 Setting the state of a member port in a dynamic aggregation group



Meanwhile, the system with the higher system ID is aware of the aggregation state changes on the peer system. The system sets the aggregation state of local member ports the same as their peer ports.

Storm control

Storm control compares broadcast, multicast, and unknown unicast traffic regularly with their respective traffic thresholds on an Ethernet interface. For each type of traffic, storm control provides a lower threshold and an upper threshold.

Depending on your configuration, when a particular type of traffic exceeds its upper threshold, the interface performs either of the following tasks:

- **No action**—Does not perform any actions on the interface.
- **Block**—Blocks this type of traffic and forwards other types of traffic. Even though the interface does not forward the blocked traffic, it still counts the traffic. When the blocked traffic drops below the lower threshold, the interface begins to forward the traffic.
- **Shutdown**—The interface goes down automatically and stops forwarding any traffic. When the blocked traffic drops below the lower threshold, the interface does not automatically come up. To bring up the interface, manually bring up the interface or disable the storm control function.

You can configure an Ethernet interface to output threshold event traps and log messages when monitored traffic meets one of the following conditions:

- Exceeds the upper threshold.
- Drops below the lower threshold.

Port isolation

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs.

Ports in an isolation group cannot communicate with each other. However, they can communicate with ports outside the isolation group.

VLAN

The Virtual Local Area Network (VLAN) technology breaks a LAN down into multiple logical LANs, which is called VLANs. Each VLAN is a broadcast domain. Hosts in the same VLAN can directly communicate with one another. Hosts in different VLANs are isolated from one another at Layer 2.

Port-based VLANs

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

You can configure a port as an untagged or tagged port of a VLAN.

- To configure the port as an untagged port of a VLAN, assign it to the untagged port list of the VLAN. The untagged port of a VLAN forwards packets from the VLAN without VLAN tags.
- To configure the port as a tagged port of a VLAN, assign it to the tagged port list of the VLAN. The tagged port of a VLAN forwards packets from the VLAN with VLAN tags.

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

- **Access**—An access port can forward packets from only one VLAN and send them untagged. Assign an access port to only the untagged port list of a VLAN.

- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. Assign a trunk port to the untagged port list of the PVID of the port, and to the tagged port lists of other VLANs.
- **Hybrid**—A hybrid port can forward packets from multiple VLANs. You can assign a hybrid port to the untagged port lists of some VLANs, and to the tagged port lists of other VLANs. An untagged hybrid port of a VLAN forwards packets from the VLAN without VLAN tags. A tagged hybrid port of a VLAN forwards packets from the VLAN with VLAN tags.

VLAN interface

For hosts of different VLANs to communicate at Layer 3, you can use VLAN interfaces. VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface and assign an IP address to it. The VLAN interface acts as the gateway of the VLAN to forward packets destined for another IP subnet.

Voice VLAN

A voice VLAN is used for transmitting voice traffic. The device can configure QoS parameters for voice packets to ensure higher transmission priority of the voice packets.

OUI addresses

A device identifies voice packets based on their source MAC addresses. A packet whose source MAC address complies with an Organizationally Unique Identifier (OUI) address of the device is regarded as a voice packet. OUI addresses are the logical AND results of MAC addresses and OUI masks.

The following table shows the default OUI addresses.

Number	OUI address	Vendor
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	000F-E200-0000	H3C Aolynk phone
5	0060-B900-0000	Philips/NEC phone
6	00D0-1E00-0000	Pingtel phone
7	00E0-7500-0000	Polycom phone
8	00E0-BB00-0000	3Com phone

QoS priority setting mode for voice traffic

The QoS priority settings carried in voice traffic include the CoS and DSCP values. You can configure the device to trust or modify the QoS priority settings for voice traffic. If the device trusts the QoS priority settings in incoming voice VLAN packets, the device does not modify their CoS and DSCP values.

Voice VLAN assignment modes

A port can be assigned to a voice VLAN automatically or manually.

Automatic mode

When an IP phone is powered on, it sends out protocol packets. After receiving these protocol packets, the device uses the source MAC address of the protocol packets to match its OUI addresses. If the match succeeds, the device performs the following operations:

- Assigns the receiving port of the protocol packets to the voice VLAN.
- Issues ACL rules and sets the packet precedence.
- Starts the voice VLAN aging timer.

If no voice packet is received from the port before the aging timer expires, the device will remove the port from the voice VLAN. The aging timer is also configurable.

Manual mode

You must manually assign the port that connects to the IP phone to a voice VLAN. The device uses the source MAC address of the received voice packets to match its OUI addresses. If the match succeeds, the device issues ACL rules and sets the packet precedence.

Security mode and normal mode of voice VLANs

Depending on the incoming packet filtering mechanisms, a voice VLAN-enabled port can operate in one of the following modes:

- **Normal mode**—The port receives voice-VLAN-tagged packets and forwards them in the voice VLAN without examining their MAC addresses. If the PVID of the port is the voice VLAN and the port operates in manual VLAN assignment mode, the port forwards all the received untagged packets in the voice VLAN.
- **Security mode**—The port uses the source MAC addresses of the received packets to match the OUI addresses of the device. Packets that fail the match will be dropped.

MAC

An Ethernet device uses a MAC address table to forward frames. A MAC address entry includes a destination MAC address, an outgoing interface (or egress RB), and a VLAN ID. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.

- The device forwards the frame out of the outgoing interface in the matching entry if a match is found.
- The device floods the frame in the VLAN of the frame if no match is found.

Types of MAC address entries

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

- **Dynamic entries**—A dynamic entry can be manually configured or dynamically learned to forward frames with a specific destination MAC address out of the associated interface. A dynamic entry might age out. A manually configured dynamic entry has the same priority as a dynamically learned one.
- **Static entries**—A static entry is manually added to forward frames with a specific destination MAC address out of the associated interface, and it never ages out. A static entry has higher priority than a dynamically learned one.

- **Blackhole entries**—A blackhole entry is manually configured and never ages out. A blackhole entry is configured for filtering out frames with a specific source or destination MAC address. For example, to block all frames destined for or sourced from a user, you can configure the MAC address of the user as a blackhole MAC address entry.
- **Security entries**—A security entry can be manually configured or dynamically learned to forward frames with a specific MAC address out of the associated interface. A security entry never ages out.

Aging timer for dynamic MAC address entries

For security and efficient use of table space, the MAC address table uses an aging timer for dynamic entries learned on all interfaces. If a dynamic MAC address entry is not updated before the aging timer expires, the device deletes the entry. This aging mechanism ensures that the MAC address table can promptly update to accommodate latest network topology changes.

A stable network requires a longer aging interval, and an unstable network requires a shorter aging interval.

An aging interval that is too long might cause the MAC address table to retain outdated entries. As a result, the MAC address table resources might be exhausted, and the MAC address table might fail to update its entries to accommodate the latest network changes.

An interval that is too short might result in removal of valid entries, which would cause unnecessary floods and possibly affect the device performance.

To reduce floods on a stable network, set a long aging timer or disable the timer to prevent dynamic entries from unnecessarily aging out. Reducing floods improves the network performance. Reducing flooding also improves the security because it reduces the chances for a data frame to reach unintended destinations.

MAC address learning

MAC address learning is enabled by default. To prevent the MAC address table from being saturated when the device is experiencing attacks, disable MAC address learning. For example, you can disable MAC address learning to prevent the device from being attacked by a large amount of frames with different source MAC addresses.

When global MAC address learning is enabled, you can disable MAC address learning on a single interface.

You can also configure the MAC learning limit on an interface to limit the MAC address table size. A large MAC address table will degrade forwarding performance. When the limit is reached, the interface stops learning any MAC addresses. You can also configure whether to forward frames whose source MAC address is not in the MAC address table.

STP

Spanning tree protocols perform the following tasks:

- Prune the loop structure into a loop-free tree structure for a Layer 2 network by selectively blocking ports.
- Maintain the tree structure for the live network.

Spanning tree protocols include STP, RSTP, and MSTP:

- **STP**—Defined in IEEE 802.1d.
- **RSTP**—Defined in IEEE 802.1w. RSTP achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much faster than STP.

- **PVST**—**PVST** allows every VLAN to have its own spanning tree, which increases usage of links and bandwidth.
- **MSTP**—Defined in IEEE 802.1s. MSTP overcomes the limitations of STP and RSTP. It supports rapid network convergence and allows data flows of different VLANs to be forwarded along separate paths. This provides a better load sharing mechanism for redundant links.

Spanning tree modes

The spanning tree modes include:

- **STP mode**—All ports of the device send STP BPDUs. Select this mode when the peer device of a port supports only STP.
- **RSTP mode**—All ports of the device send RSTP BPDUs. A port in this mode automatically transits to the STP mode when it receives STP BPDUs from a peer device. The port does not transit to the MSTP mode when it receives MSTP BPDUs from a peer device.
- **PVST** mode—All ports of the device send PVST BPDUs. Each VLAN maintains a spanning tree. In a network, the number of spanning trees maintained by all devices equals the number of PVST-enabled VLANs multiplied by the number of PVST-enabled ports. If the number of spanning trees exceeds the capacity of the network, device CPUs become overloaded, packet forwarding is interrupted, and the network becomes unstable. The number of spanning trees that a device can maintain varies by device model.
- **MSTP mode**—All ports of the device send MSTP BPDUs. A port in this mode automatically transits to the STP mode when it receives STP BPDUs from a peer device. The port does not transit to the RSTP mode when it receives RSTP BPDUs from a peer device.

MSTP basic concepts

MSTP divides a switched network into multiple spanning tree regions (MST regions). MSTP maintains multiple independent spanning trees in an MST region, and each spanning tree is mapped to specific VLANs. Such a spanning tree is referred to as a multiple spanning tree instance (MSTI). The common spanning tree (CST) is a single spanning tree that connects all MST regions in the switched network. 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. The common and internal spanning tree (CIST) is a single spanning tree that connects all devices in the switched network. It consists of the ISTs in all MST regions and the CST.

Devices in an MST region have the following characteristics:

- A spanning tree protocol enabled.
- Same region name.
- Same VLAN-to-instance mapping configuration.
- Same MSTP revision level.
- Physically linked together.

Port roles

Spanning tree calculation involves the following port roles:

- **Root port**—Forwards data for a non-root bridge to the root bridge. The root bridge does not have any root port.
- **Designated port**—Forwards data to the downstream network segment or device.
- **Alternate port**—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.
- **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.

STP calculation involves root ports, designated ports, and alternate ports. RSTP calculation involves root ports, designated ports, alternate ports, and backup ports. MSTP calculation involves all port roles.

Port states

RSTP and MSTP define the following port states:

State	Description
Forwarding	The port receives and sends BPDUs, and forwards user traffic.
Learning	The port receives and sends BPDUs, but does not forward user traffic. Learning is an intermediate port state.
Discarding	The port receives and sends BPDUs, but does not forward user traffic.

STP defines the following port states: Disabled, Blocking, Listening, Learning, and Forwarding. The Disabled, Blocking, and Listening states correspond to the Discarding state in RSTP and MSTP.

LLDP

The Link Layer Discovery Protocol (LLDP) 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, and port ID. 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.

LLDP agent

An LLDP agent is a mapping of an entity where LLDP runs. Multiple LLDP agents can run on the same interface.

LLDP agents are divided into the following types:

- Nearest bridge agent.
- Nearest customer bridge agent.
- Nearest non-TPMR bridge agent.

LLDP exchanges packets between neighbor agents and creates and maintains neighbor information for them.

Transmitting LLDP frames

An LLDP agent 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, LLDP uses the token bucket mechanism to rate limit LLDP frames.

LLDP automatically enables the fast LLDP frame transmission mechanism in either of the following cases:

- A new LLDP frame is received and carries device information new to the local device.
- The LLDP operating mode of the LLDP agent changes from Disable or Rx to TxRx or Tx.

The fast LLDP frame transmission mechanism successively sends the specified number of LLDP frames at a configurable fast LLDP frame transmission 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 agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging timer. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, the saved information ages out.

By setting the TTL multiplier, you can configure the TTL of locally sent LLDPDUs. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds. TTLs greater than 65535 will be rounded down to 65535 seconds.

LLDP reinitialization delay

When the LLDP operating mode changes on a port, the port initializes the protocol state machines after an LLDP reinitialization delay. By adjusting the delay, you can avoid frequent initializations caused by frequent changes to the LLDP operating mode on a port.

LLDP trapping

LLDP trapping notifies the network management system of events such as newly detected neighboring devices and link failures.

LLDP 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 enhanced device management. They are defined by standardization or other organizations and are optional for LLDPDUs.

CDP compatibility

CDP compatibility enables your device to receive and recognize CDP packets from a Cisco IP phone and respond with CDP packets.

DHCP snooping

DHCP snooping works between the DHCP client and server, or between the DHCP client and DHCP relay agent. DHCP snooping provides the following functions:

- Ensures that DHCP obtain IP addresses only from authorized DHCP servers.

  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.

  Configure ports facing the DHCP server as trusted ports, and configure other ports as untrusted ports.
- Records DHCP snooping entries.

  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. ARP detection uses DHCP snooping entries to filter ARP packets from unauthorized clients.
- Backs up DHCP snooping entries automatically.

  The auto backup function saves DHCP snooping entries to a backup file, and allows the DHCP snooping device to download the entries from the backup file at device reboot. The entries on the DHCP snooping device cannot survive a reboot. The auto backup helps some other features provide services if these features must use DHCP snooping entries for user authentication.
- Supports 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. Option 82 contains two sub-options: Circuit ID and Remote ID.

  If the DHCP relay agent supports Option 82, it handles DHCP requests by the strategies described in the following table.

  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 does not contain Option 82, DHCP snooping forwards it immediately.

  The following table shows the Option 82 handling strategies for DHCP requests:

If a DHCP request has…	Handling strategy	DHCP snooping…
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 according to the configured padding format, padding content, and code type.

If a DHCP request has…	Handling strategy	DHCP snooping…
No Option 82	N/A	Forwards the message after adding the Option 82 padded according to the configured padding format, padding content, and code type.

IP

IP address classes

IP addressing uses a 32-bit address to identify each host on an IPv4 network. To make addresses easier to read, they are written in dotted decimal notation, each address being four octets in length. For example, address 00001010000000010000000100000001 in binary is written as 10.1.1.1.

Each IP address breaks down into the following sections:

- **Net ID**—Identifies a network. The first several bits of a net ID, known as the class field or class bits, identify the class of the IP address.
- **Host ID**—Identifies a host on a network.

IP addresses are divided into five classes. The following table shows IP address classes and ranges. The first three classes are most typically used.

Class	Address range	Remarks
A	0.0.0.0 to 127.255.255.255	The IP address 0.0.0.0 is used by a host at startup for temporary communication. This address is never a valid destination address. Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link.
B	128.0.0.0 to 191.255.255.255	N/A
C	192.0.0.0 to 223.255.255.255	N/A
D	224.0.0.0 to 239.255.255.255	Multicast addresses.
E	240.0.0.0 to 255.255.255.255	Reserved for future use, except for the broadcast address 255.255.255.255.

Subnetting and masking

Subnetting divides a network into smaller networks called subnets by using some bits of the host ID to create a subnet ID.

Masking identifies the boundary between the host ID and the combination of net ID and subnet ID.

Each subnet mask comprises 32 bits that correspond to the bits in an IP address. In a subnet mask, consecutive ones represent the net ID and subnet ID, and consecutive zeros represent the host ID.

Before being subnetted, Class A, B, and C networks use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

Subnetting increases the number of addresses that cannot be assigned to hosts. Therefore, using subnets means accommodating fewer hosts.

For example, a Class B network without subnetting can accommodate 1022 more hosts than the same network subnetted into 512 subnets.

- **Without subnetting**—65534 (2^{16} – 2) hosts. (The two deducted addresses are the broadcast address, which has an all-one host ID, and the network address, which has an all-zero host ID.)
- **With subnetting**—Using the first nine bits of the host-id for subnetting provides 512 (2^{9}) subnets. However, only seven bits remain available for the host ID. This allows 126 (2^{7} – 2) hosts in each subnet, a total of 64512 (512 × 126) hosts.

IP address configuration methods

You can use the following methods to enable an interface to obtain an IP address:

- Manually assign an IP address to the interface.
- Configure the interface to obtain an IP address through DHCP.

MTU for an interface

When a packet exceeds the MTU of the output interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Because fragmentation and reassembling consume system resources, set an appropriate MTU for an interface based on the network environment to avoid fragmentation.

ARP

ARP resolves IP addresses into MAC addresses on Ethernet networks.

Types of ARP table entries

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.

The device supports the following types of static ARP entries:

- **Long static ARP entry**—It contains the IP address, MAC address, VLAN, and output interface. It is directly used for forwarding packets.
- **Short static ARP entry**—It contains only the IP address and MAC address.
    - If the output interface is a VLAN interface, the device sends an ARP request whose target IP address is the IP address in the short entry. If the sender IP and MAC addresses in the received ARP reply match the short static ARP entry, the device performs the following operations:

- Adds the interface that received the ARP reply to the short static ARP entry.
- Uses the resolved short static ARP entry to forward IP packets.

To communicate with a host by using a fixed IP-to-MAC mapping, configure a short static ARP entry on the device. To communicate with a host by using a fixed IP-to-MAC mapping through an interface in a VLAN, configure a long static ARP entry on the device.

Gratuitous ARP

In a gratuitous ARP packet, the sender IP address and the target IP address are the IP address of the sending device.

A device sends a gratuitous ARP packet for either of the following purposes:

- Determine whether its IP address is already used by another device. If the IP address is already used, the device is informed of the conflict by an ARP reply.
- Inform other devices of a MAC address change.

Gratuitous ARP packet learning

This functionfeature 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 received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Periodic sending of gratuitous ARP packets

Enabling periodic sending of gratuitous ARP packets helps downstream devices update ARP entries or MAC entries in a timely manner.

This feature can implement the following functions:

- Prevent gateway spoofing.

  Gateway spoofing occurs when an attacker uses the gateway address to send gratuitous ARP packets to the hosts on a network. The traffic destined for the gateway from the hosts is sent to the attacker instead. As a result, the hosts cannot access the external network.

  To prevent such gateway spoofing attacks, you can enable the gateway to send gratuitous ARP packets at intervals. Gratuitous ARP packets contain the primary IP address and manually configured secondary IP addresses of the gateway, so hosts can learn correct gateway information.
- Prevent ARP entries from aging out.

  If network traffic is heavy or if the host CPU usage is high, received ARP packets can be discarded or are not promptly processed. Eventually, the dynamic ARP entries on the receiving host age out. The traffic between the host and the corresponding devices is interrupted until the host re-creates the ARP entries.

  To prevent this problem, you can enable the gateway to send gratuitous ARP packets periodically. Gratuitous ARP packets contain the primary IP address and manually configured secondary IP addresses of the gateway, so the receiving hosts can update ARP entries in a timely manner.

ARP attack protection

ARP attacks and viruses threaten LAN security. Although ARP is easy to implement, it does not provide a security mechanism and is vulnerable to network attacks. Multiple features are used to detect and prevent ARP attacks.

- The gateway supports the following features:
  - ARP blackhole routing.

    - ARP source suppression.
    - ARP packet source MAC consistency check.
    - ARP active acknowledgement.
    - Source MAC-based ARP attack detection.
    - Authorized ARP.
- ARP scanning and fixed ARP.
- The access device supports the following features:
    - ARP packet rate limit.
    - ARP gateway protection.
    - ARP filtering.
    - ARP detection.

Unresolvable IP attack protection

If a device receives a large number of unresolvable IP packets from a host, the following situations can occur:

- The device sends a large number of ARP requests, overloading the target subnets.
- The device keeps trying to resolve the destination IP addresses, overloading its CPU.

To protect the device from such IP attacks, you can configure the following features:

- **ARP source suppression**—Stops resolving packets from a host if the number of unresolvable IP packets from the host exceeds the upper limit within 5 seconds. The device continues ARP resolution when the interval elapses. This feature is applicable if the attack packets have the same source addresses.
- **ARP blackhole routing**—Creates a blackhole route destined for an unresolvable IP address. The device drops all matching packets until the blackhole route ages out. This feature is applicable regardless of whether the attack packets have the same source addresses.

ARP packet source MAC consistency check

This feature enables a gateway to filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body. This feature allows the gateway to learn correct ARP entries.

ARP active acknowledgement

Configure this feature on gateways to prevent user spoofing.

ARP active acknowledgement prevents a gateway from generating incorrect ARP entries.

In strict mode, a gateway performs more strict validity checks before creating an ARP entry:

- Upon receiving an ARP request destined for the gateway, the gateway sends an ARP reply but does not create an ARP entry.
- Upon receiving an ARP reply, the gateway determines whether it has resolved the sender IP address:
    - If yes, the gateway performs active acknowledgement. When the ARP reply is verified as valid, the gateway creates an ARP entry.
    - If not, the gateway discards the packet.

Source MAC-based ARP attack detection

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device adds the MAC address to an ARP attack entry. Before the entry is aged out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.

- **Filter**—Generates log messages and filters out subsequent ARP packets from that MAC address.

You can exclude the MAC addresses of some gateways and servers from this detection. This feature does not inspect ARP packets from those devices even if they are attackers.

Authorized ARP

Authorized ARP entries are generated based on the DHCP clients' address leases on the DHCP server or dynamic client entries on the DHCP relay agent.

With authorized ARP enabled, an interface is disabled from learning dynamic ARP entries. This feature prevents user spoofing and allows only authorized clients to access network resources.

ARP scanning and fixed ARP

ARP scanning is typically used together with the fixed ARP feature in small-scale networks.

ARP scanning automatically creates ARP entries for devices in an address range. The device performs ARP scanning using the following steps:

1. Sends ARP requests for each IP address in the address range.
2. Obtains their MAC addresses through received ARP replies.
3. Creates dynamic ARP entries.

Fixed ARP converts existing dynamic ARP entries (including those generated through ARP scanning) to static ARP entries. This feature prevents ARP entries from being modified by attackers.

ARP packet rate limit

The ARP packet rate limit feature allows you to limit the rate of ARP packets delivered to the CPU. An ARP detection enabled device will send all received ARP packets to the CPU for inspection. Processing excessive ARP packets will make the device malfunction or even crash. To solve this problem, configure the ARP packet rate limit.

Configure this feature when ARP detection is enabled, or when ARP flood attacks are detected.

If logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules.

ARP gateway protection

Configure this feature on interfaces not connected with a gateway to prevent gateway spoofing attacks.

When such an interface receives an ARP packet, it checks whether the sender IP address in the packet is consistent with that of any protected gateway. If yes, it discards the packet. If not, it handles the packet correctly.

ARP filtering

The ARP filtering feature can prevent gateway spoofing and user spoofing attacks.

An interface enabled with this feature checks the sender IP and MAC addresses in a received ARP packet against permitted entries. If a match is found, the packet is handled correctly. If not, the packet is discarded.

ARP detection

ARP detection enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks. ARP detection does not check ARP packets received from ARP trusted ports.

ARP detection provides the following functions:

- User validity check

If you only enable ARP detection for a VLAN, ARP detection provides only the user validity check.

Upon receiving an ARP packet from an ARP untrusted interface, the device matches the sender IP and MAC addresses with the following entries:

- Static IP source guard binding entries.
- DHCP snooping entries.

If a match is found, 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

  Enable validity check for ARP packets received on untrusted ports and specify the following objects to be checked:

  - **Sender 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.
  - **Target 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.

- ARP restricted forwarding

  ARP restricted forwarding controls the forwarding of ARP packets that are received on untrusted interfaces and have passed user validity check as follows:

  - If the packets are ARP requests, they are forwarded through the trusted interface.
  - If the packets are ARP replies, they are forwarded according to their destination MAC address. If no match is found in the MAC address table, they are forwarded through the trusted interface.

ARP does not have security mechanisms and is vulnerable to network attacks. To protect the network from ARP attacks, the device provides the ARP scanning and fixed ARP features.

ARP scanning is typically used together with the fixed ARP feature in small-scale networks.

ARP scanning automatically creates ARP entries for devices in an address range. The device performs ARP scanning in the following steps:

1. Sends ARP requests for each IP address in the address range.
2. Obtains their MAC addresses through received ARP replies.
3. Creates dynamic ARP entries.

Fixed ARP converts existing dynamic ARP entries (including those generated through ARP scanning) to static ARP entries. This feature prevents ARP entries from being modified by attackers.

DNS

Domain Name System (DNS) is a distributed database used by TCP/IP applications to translate domain names into IP addresses. IPv4 DNS translates domain names into IPv4 addresses. IPv6 DNS translates domain names into IPv6 addresses. The domain name-to-IP address mapping is called a DNS entry.

Dynamic domain name resolution

To use dynamic domain name resolution, you must specify a DNS server address for a device. The device sends DNS queries to the DNS server for domain name resolution.

You can configure a domain name suffix list so that the resolver can use the list to supply the missing part of an incomplete name. For example, you can configure **com** as the suffix for aabbcc.com. The user only needs to enter **aabbcc** to obtain the IP address of **aabbcc.com**. The resolver adds the suffix and delimiter before passing the name to the DNS server.

The name resolver handles the queries based on the domain names that the user enters:

- If the user enters a domain name without a dot (.) (for example, aabbcc), the resolver considers the domain name as a host name. It adds a DNS suffix to the host name before performing the query operation. If no match is found for any host name and suffix combination, the resolver uses the user-entered domain name (for example, aabbcc) for the IP address query.
- If the user enters a domain name with a dot (.) among the letters (for example, www.aabbcc), the resolver directly uses this domain name for the query operation. If the query fails, the resolver adds a DNS suffix for another query operation.
- If the user enters a domain name with a dot (.) at the end (for example, aabbcc.com.), the resolver considers the domain name an FQDN and returns the successful or failed query result. The dot at the end of the domain name is considered a terminating symbol.

Static domain name resolution

Static domain name resolution means manually creating mappings between domain names and IP addresses. For example, you can create a static DNS mapping for a device so that you can Telnet to the device by using the domain name.

After a user specifies a name, the device checks the static name resolution table for an IP address. If no IP address is available, it contacts the DNS server for dynamic name resolution, which takes more time than static name resolution. To improve efficiency, you can put frequently queried name-to-IP address mappings in the local static name resolution table.

DNS proxy

The DNS proxy performs the following operations:

- Forwards the request from the DNS client to the designated DNS server.
- Conveys the reply from the DNS server to the client.

The DNS proxy simplifies network management. When the DNS server address is changed, you can change the configuration on only the DNS proxy instead of on each DNS client.

DDNS

DNS provides only the static mappings between domain names and IP addresses. When the IP address of a node changes, your access to the node fails.

Dynamic Domain Name System (DDNS) can dynamically update the mappings between domain names and IP addresses for DNS servers.

To use DDNS, a user must access the website of a DDNS service provider and register an account. When its IP address changes, the user, as a DDNS client, sends a DDNS update request to the DDNS server to update the mapping between its domain name and IP address. When receiving the update request, the DDNS server verifies the following:

- The account information is correct.
- The domain name to be updated belongs to the account.

If the DDNS client passes the verification, the DDNS server tells the DNS server to re-map the domain name and the IP address of the DDNS client.

A DDNS policy contains the DDNS server address, login ID, password, associated SSL client policy, and update time interval. After creating a DDNS policy, you can apply it to multiple interfaces to simplify DDNS configuration.

DDNS is supported by only IPv4 DNS, and it is used to update the mappings between domain names and IPv4 addresses.

IPv6

IPv6, also called IP next generation (IPng), was designed by the IETF as the successor to IPv4. One significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

IPv6 address formats

An IPv6 address is represented as a set of 16-bit hexadecimals separated by colons (:). An IPv6 address is divided into eight groups, and each 16-bit group is represented by four hexadecimal numbers, for example, 2001:0000:130F:0000:0000:09C0:876A:130B.

To simplify the representation of IPv6 addresses, you can handle zeros in IPv6 addresses by using the following methods:

- The leading zeros in each group can be removed. For example, the above address can be represented in a shorter format as 2001:0:130F:0:0:9C0:876A:130B.
- If an IPv6 address contains one or more consecutive groups of zeros, they can be replaced by a double colon (::). For example, the above address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.

An IPv6 address consists of an address prefix and an interface ID, which are equivalent to the network ID and the host ID of an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation. The prefix-length is a decimal number indicating how many leftmost bits of the IPv6 address are in the address prefix.

IPv6 address types

IPv6 addresses include the following types:

- **Unicast address**—An identifier for a single interface, similar to an IPv4 unicast address. A packet sent to a unicast address is delivered to the interface identified by that address.
- **Multicast address**—An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Broadcast addresses are replaced by multicast addresses in IPv6.
- **Anycast address**—An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to the nearest interface among the interfaces identified by that address. The nearest interface is chosen according to the routing protocol's measure of distance.

The type of an IPv6 address is designated by the first several bits, called the format prefix. The following table shows mappings between address types and format prefixes:

Type		Format prefix (binary)	IPv6 prefix ID	Remarks
Unicast address	Unspecified address	00...0 (128 bits)	::/128	It cannot be assigned to any node. Before acquiring a valid IPv6 address, a node fills this address in the source address field of IPv6 packets. The unspecified address cannot be used as a destination IPv6 address.
	Loopback address	00...1 (128 bits)	::1/128	It has the same function as the loopback address in IPv4. It cannot be assigned to any physical interface. A node uses this address to send an IPv6 packet to itself.
	Link-local address	1111111010	FE80::/10	Used for communication among link-local nodes for neighbor discovery and stateless autoconfiguration. Packets with link-local source or destination addresses are not forwarded to other links.
	Global unicast address	Other forms	N/A	Equivalent to public IPv4 addresses, global unicast addresses are provided for Internet service providers. This type of address allows for prefix aggregation to restrict the number of global routing entries.
Multicast address		11111111	FF00::/8	N/A
Anycast address		Anycast addresses use the unicast address space and have the identical structure of unicast addresses.		N/A

EUI-64 address-based interface identifiers

An interface identifier is 64-bit long and uniquely identifies an interface on a link. Interfaces generate EUI-64 address-based interface identifiers differently.

On an IEEE 802 interface (such as a VLAN interface), the interface identifier is derived from the link-layer address (typically a MAC address) of the interface. The MAC address is 48-bit long.

To obtain an EUI-64 address-based interface identifier, follow these steps:

1. Insert the 16-bit binary number 1111111111111110 (hexadecimal value of FFFE) behind the 24th high-order bit of the MAC address.
2. Invert the universal/local (U/L) bit (the seventh high-order bit). This operation makes the interface identifier have the same local or global significance as the MAC address.

IPv6 global unicast address configuration methods

Use one of the following methods to configure an IPv6 global unicast address for an interface:

- **EUI-64 IPv6 address**—The IPv6 address prefix of the interface is manually configured, and the interface identifier is generated automatically by the interface.
- **Manual configuration**—The IPv6 global unicast address is manually configured.

- **Stateless address autoconfiguration**—The IPv6 global unicast address is generated automatically according to the address prefix information contained in the RA message and the EUI-64 address-based interface identifier.
- **Stateful address autoconfiguration**—Enables a host to acquire an IPv6 address from a DHCPv6 server.

You can configure multiple IPv6 global unicast addresses on an interface.

IPv6 link-local address configuration methods

Configure IPv6 link-local addresses by using one of the following methods for an interface:

- **Automatic generation**—The device automatically generates a link-local address for an interface according to the link-local address prefix (FE80::/10) and the EUI-64 address-based interface identifier.
- **Manual assignment**—An IPv6 link-local address is manually configured.

An interface can have only one link-local address. As a best practice, use the automatic generation method to avoid link-local address conflicts. If both methods are used, manual assignment takes precedence.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated one.
- If you first use manual assignment and then automatic generation, both of the following occur:
  - The link-local address is still the manually assigned one.
  - The automatically generated link-local address does not take effect. If you delete the manually assigned address, the automatically generated link-local address takes effect.

ND

The IPv6 Neighbor Discovery (ND) protocol uses ICMPv6 messages to provide the following functions:

- Address resolution
- Neighbor reachability detection
- DAD
- Router/prefix discovery
- Stateless address autoconfiguration
- Redirection

Table 13 describes the ICMPv6 messages used by ND.

Table 13 ICMPv6 messages used by ND

ICMPv6 message	Type	Function
Neighbor Solicitation (NS)	135	Acquires the link-layer address of a neighbor.
		Verifies whether a neighbor is reachable.
		Detects duplicate addresses.
Neighbor Advertisement (NA)	136	Responds to an NS message.
		Notifies the neighboring nodes of link layer changes.
Router Solicitation (RS)	133	Requests an address prefix and other configuration information for autoconfiguration after startup.
Router Advertisement (RA)	134	Responds to an RS message.
		Advertises information, such as the Prefix Information options and flag bits.
Redirect	137	Informs the source host of a better next hop on the path to a particular destination.

Neighbor entries

A neighbor entry stores information about a neighboring node on the link. Neighbor entries can be dynamically configured through NS and NA messages or manually configured.

You can configure a static neighbor entry by using one of the following methods:

- **Method 1**—Associate a neighbor's IPv6 address and link-layer address with the local Layer 3 interface.

  If you use Method 1, the device automatically finds the Layer 2 port connected to the neighbor.
- **Method 2**—Associate a neighbor's IPv6 address and link-layer address with a Layer 2 port in a VLAN.

  If you use Method 2, make sure the corresponding VLAN interface exists and the Layer 2 port belongs to the VLAN.

RA messages

An RA message is advertised by a router to all hosts on the same link. The RA message contains the address prefix and other configuration information for the hosts to generate IPv6 addresses through stateless address autoconfiguration.

You can enable an interface to send RA messages, specify the maximum and minimum sending intervals, and configure parameters in RA messages. The device sends RA messages at random intervals between the maximum and minimum intervals. The minimum interval should be less than or equal to 0.75 times the maximum interval.

Table 14 describes the configurable parameters in an RA message.

Table 14 Parameters in an RA message and their descriptions

Parameter	Description
IPv6 prefix/prefix length	The IPv6 prefix/prefix length for a host to generate an IPv6 global unicast address through stateless autoconfiguration.
Valid lifetime	Specifies the valid lifetime of a prefix. The generated IPv6 address is valid within the valid lifetime and becomes invalid when the valid lifetime expires.
Preferred lifetime	Specifies the preferred lifetime of a prefix used for stateless autoconfiguration. After the preferred lifetime expires, the node cannot use the generated IPv6 address to establish new connections, but can receive packets destined for the IPv6 address. The preferred lifetime cannot be greater than the valid lifetime.
No-autoconfig flag	Tells the hosts not to use the address prefix for stateless autoconfiguration.
Off-link flag	Specifies the address with the prefix to be indirectly reachable on the link.
MTU	Guarantees that all nodes on the link use the same MTU.
Unlimited hops flag	Specifies unlimited hops in RA messages.
M flag	Determines whether a host uses stateful autoconfiguration to obtain an IPv6 address. If the M flag is set, the host uses stateful autoconfiguration (for example, from a DHCPv6 server) to obtain an IPv6 address. If the flag is not set, the host uses stateless autoconfiguration to generate an IPv6 address according to its link-layer address and the prefix information in the RA message.
O flag	Determines whether a host uses stateful autoconfiguration to obtain configuration information other than IPv6 address. If the O flag is set, the host uses stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 address. If the flag is not set, the host uses stateless autoconfiguration.
Router Lifetime	Advertises the lifetime of an advertising router. If the lifetime is 0, the router cannot be used as the default gateway.
Retrans Timer	Specifies the interval for retransmitting the NS message after the device does not receive a response for an NS message within a time period.
Router Preference	Specifies the router preference in an RA message. A host selects a router as the default gateway according to the router preference. If router preferences are the same, the host selects the router from which the first RA message is received.
Reachable Time	Specifies the reachable period for a neighbor after the device detects that a neighbor is reachable. If the device needs to send a packet to the neighbor after the reachable period, the device reconfirms whether the neighbor is reachable.

ND proxy

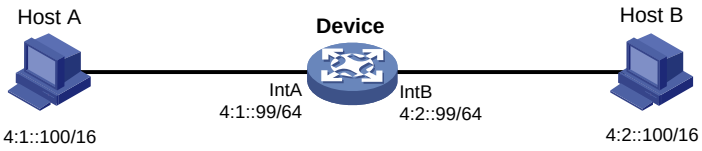
ND proxy enables a device to answer an NS message requesting the hardware address of a host on another network. With ND proxy, hosts in different broadcast domains can communicate with each other as they would on the same network.

ND proxy includes common ND proxy and local ND proxy.

Common ND proxy

As shown in Figure 7, Interface A with IPv6 address 4:1::96/64 and Interface B with IPv6 address 4:2::99/64 belong to different subnets. Host A and Host reside on the same network but in different broadcast domains.

Figure 7 Application environment of common ND proxy



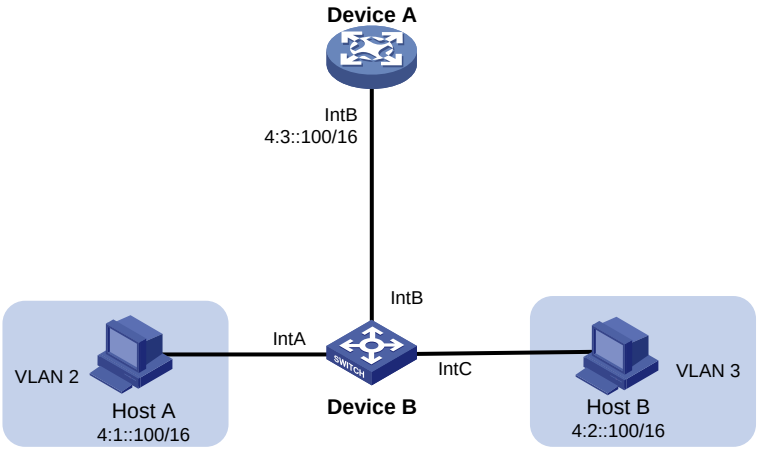
Because Host A's IPv6 address is on the same subnet as Host B's, Host A directly sends an NS message to obtain Host B's MAC address. However, Host B cannot receive the NS message because they belong to different broadcast domains.

To solve this problem, enable common ND proxy on Interface A and Interface B of the Device. The Device replies to the NS message from Host A, and forwards packets from other hosts to Host B.

Local ND proxy

As shown in Figure 8, Host A belongs to VLAN 2 and Host B belongs to VLAN 3. Host A and Host B connect to Interface A and Interface C, respectively.

Figure 8 Application environment of local ND proxy



Because Host A's IPv6 address is on the same subnet as Host B's, Host A directly sends an NS message to obtain Host B's MAC address. However, Host B cannot receive the NS message because they are in different VLANs.

To solve this problem, enable local ND proxy on Interface B of the router so that the router can forward messages between Host A and Host B.

Port mirroring

Port mirroring copies the packets passing through a port to the destination port that connects to a data monitoring device for packet analysis. The copies are called mirrored packets.

Port mirroring includes the following terms:

- **Source port**—Monitored port on the device. Packets of the monitored port will be copied and sent to the destination port.
- **Source device**—Device where a source port resides.
- **Destination port**—Port that connects to the data monitoring device. Packets of the source port will be copied and sent to the destination port.
- **Destination device**—Device where the destination port resides.
- **Mirroring group**—Includes local mirroring group and remote mirroring group.
  - **Local mirroring group**—The source port and the destination port are on the same device. A local mirroring group is a mirroring group that contains the source ports and the destination port on the same device.
  - **Remote port mirroring**—The source port and the destination port are on different devices. A remote source group is a mirroring group that contains the source ports. A remote destination group is a mirroring group that contains the destination port. In remote port mirroring, mirrored packets are transmitted by the remote probe VLAN from the source device to the destination device.

Static routing

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.

A default route is used to forward packets that do not match any specific routing entry in the routing table. You can configure a default IPv4 route with destination address 0.0.0.0/0 and configure a default IPv6 route with destination address ::/0.

Policy-based routing

Policy-based routing (PBR) uses user-defined policies to route packets. A policy can specify next hops for packets that match specific criteria such as ACLs.

Policy

A policy includes match criteria and actions to be taken on the matching packets. A policy can have one or multiple nodes as follows:

- Each node is identified by a node number. A smaller node number has a higher priority.
- A node contains the following elements:
  - **Match criterion**—Uses an ACL to match packets.
  - **Action**—Sets a next hop for the permitted packets. You can associate a next hop with a track entry, and specify whether the next hop is directly connected.
- A node has a match mode of **permit** or **deny**.

A policy matches nodes in priority order against packets. If a packet matches the criteria on a node, it is processed by the action on the node. If the packet does not match the criteria on the node, it goes to the next node for a match. If the packet does not match the criteria on any node, it is forwarded according to the routing table.

PBR and Track

PBR can work with the Track feature to dynamically adapt the status of an action to the availability status of a tracked next hop.

- When the track entry changes to **Negative**, the action is invalid.
- When the track entry changes to **Positive** or **NotReady**, the action is valid.

IGMP snooping

IGMP snooping runs on a Layer 2 device as a multicast constraining mechanism. It creates Layer 2 multicast forwarding entries from IGMP packets that are exchanged between the hosts and the Layer 3 device.

The Layer 2 device forwards multicast data based on Layer 2 multicast forwarding entries. A Layer 2 multicast forwarding entry contains the VLAN, multicast group address, multicast source address, and host ports. A host port is a multicast receiver-side port on the Layer 2 multicast device.

MLD snooping

MLD snooping runs on a Layer 2 device as an IPv6 multicast constraining mechanism. It creates Layer 2 IPv6 multicast forwarding entries from MLD packets that are exchanged between the hosts and the Layer 3 device.

The Layer 2 device forwards multicast data based on Layer 2 IPv6 multicast forwarding entries. A Layer 2 IPv6 multicast forwarding entry contains the VLAN, IPv6 multicast group address, IPv6 multicast source address, and host ports. A host port is a multicast receiver-side port on the Layer 2 multicast device.

DHCP

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

A typical DHCP application scenario has a DHCP server and multiple DHCP clients deployed on the same subnet. DHCP clients can also obtain configuration parameters from a DHCP server on another subnet through a DHCP relay agent.

DHCP server

The DHCP server is well suited to networks where the following conditions exist:

- Manual configuration and centralized management are difficult to implement.
- IP addresses are limited. For example, an ISP limits the number of concurrent online users, and users must acquire IP addresses dynamically.
- Most hosts do not need fixed IP addresses.

The DHCP server selects IP addresses and other parameters from an address pool and assigns them to DHCP clients. A DHCP address pool contains the following items:

- Assignable IP addresses.

- Lease duration.
- Gateway addresses.
- Domain name suffix.
- DNS server addresses.
- WINS server addresses.
- NetBIOS node type.
- DHCP options.

Before assigning an IP address, the DHCP server performs IP address conflict detection to verify that the IP address is not in use.

DHCP address pool

The DHCP server supports the following address assignment mechanisms:

- **Static address allocation**—Manually bind the MAC address or ID of a client to an IP address in a DHCP address pool. When the client requests an IP address, the DHCP server assigns the IP address in the static binding to the client.
- **Dynamic address allocation**—Specify IP address ranges in a DHCP address pool. Upon receiving a DHCP request, the DHCP server dynamically selects an IP address from the matching IP address range in the address pool.

You can specify the lease duration for IP addresses in the DHCP address pool.

The DHCP server observes the following principles to select an address pool for a client:

- If there is an address pool where an IP address is statically bound to the MAC address or ID of the client, the DHCP server selects this address pool and assigns the statically bound IP address and other configuration parameters to the client.
- If no static address pool is configured, the DHCP server selects an address pool depending on the client location.
    - **Client on the same subnet as the server**—The DHCP server compares the IP address of the receiving interface with the subnets of all address pools. If a match is found, the server selects the address pool with the longest-matching subnet.
    - **Client on a different subnet than the server**—The DHCP server compares the IP address in the **giaddr** field of the DHCP request with the subnets of all address pools. If a match is found, the server selects the address pool with the longest-matching subnet.

IP address allocation sequence

The DHCP server selects an IP address for a client in the following sequence:

1. IP address statically bound to the client's MAC address or ID.
2. IP address that was ever assigned to the client.
3. IP address designated by the Option 50 field in the DHCP-DISCOVER message sent by the client. Option 50 is the Requested IP Address option. The client uses this option to specify the wanted IP address in a DHCP-DISCOVER message. The content of Option 50 is user defined.
4. First assignable IP address found in the way of selecting an address pool.
5. IP address that was a conflict or passed its lease duration. If no IP address is assignable, the server does not respond.

DHCP options

DHCP uses the options field to carry information for dynamic address allocation and provide additional configuration information for clients.

You can customize options for the following purposes:

- Add newly released DHCP options.

- Add options for which the vendor defines the contents, for example, Option 43. DHCP servers and clients can use vendor-specific options to exchange vendor-specific configuration information.
- Add options for which the Web interface does not provide a dedicated configuration page. For example, you can use Option 4 to specify the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration page. For example, on the DNS server configuration page, you can specify up to eight DNS servers. To specify more than eight DNS servers, you can use Option 6 to specify all DNS servers.

The following table shows the most commonly used DHCP options.

Option number	Option name	Recommended padding format
3	Router	IP address
6	Domain Name Server	IP address
15	Domain Name	ASCII string
44	NetBIOS over TCP/IP Name Server	IP address
46	NetBIOS over TCP/IP Node Type	Hexadecimal string
66	TFTP server name	ASCII string
67	Bootfile name	ASCII string
43	Vendor Specific Information	Hexadecimal string

IP address conflict detection

Before assigning an IP address, the DHCP server pings the IP address.

- If the server receives a response within the specified period, it selects and pings another IP address.
- If it does not receive a response, the server continues to ping the IP address until a specific number of ping packets are sent. If it still does not receive a response, the server assigns the IP address to the requesting client.

DHCP relay agent

The DHCP relay agent enables clients to get IP addresses from a DHCP server on another subnet. This feature centralizes management and reduces investment by not deploying a DHCP server for each subnet.

DHCP relay entry recording

This feature enables the DHCP relay agent to automatically record clients' IP-to-MAC bindings (relay entries) after they obtain IP addresses through DHCP.

Some security functions use the relay entries to check incoming packets and block packets that do not match any entry. In this way, illegal hosts are not able to access external networks through the relay agent. Examples of the security functions are ARP address check, authorized ARP, and IP source guard.

Periodic refreshing of dynamic DHCP relay entries

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses the following information to periodically send a DHCP-REQUEST message to the DHCP server:

- The IP address of a relay entry.
- The MAC address of the DHCP relay interface.

The relay agent maintains the relay entries depending on what it receives from the DHCP server:

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent removes the relay entry. In addition, upon receiving the DHCP-ACK message, the relay agent sends a DHCP-RELEASE message to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the relay entry.

HTTP/HTTPS

The device provides a built-in Web server. After you enable the Web server on the device, users can log in to the Web interface to manage and monitor the device.

The device's built-in Web server supports both Hypertext Transfer Protocol (HTTP) (version 1) and Hypertext Transfer Protocol Secure (HTTPS). HTTPS is more secure than HTTP because of the following items:

- HTTPS uses SSL to ensure the integrity and security of data exchanged between the client and the server.
- HTTPS allows you to define a certificate attribute-based access control policy to allow only legal clients to access the Web interface.

You can also specify a basic ACL for HTTP or HTTPS to prevent unauthorized Web access.

- If you does not specify an ACL for HTTP or HTTPS, or the specified ACL does not exist or does not have rules, the device permits all HTTP or HTTPS logins.
- If the specifies ACL has rules, only users permitted by the ACL can log in to the Web interface through HTTP or HTTPS.

SSH

SSH is not available in Release 3111P02.

Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.

SSH uses the typical client-server model to establish a channel for secure data transfer based on TCP.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 is better than SSH1 in performance and security.

The device can act as an SSH server to provide the following SSH applications to SSH clients:

- **Secure Telnet**—Stelnet provides secure and reliable network terminal access services. Through Stelnet, a user can securely log in to a remote server. Stelnet can protect devices against attacks, such as IP spoofing and plain text password interception. The device can act as an Stelnet server or an Stelnet client.
- **Secure File Transfer Protocol**—Based on SSH2, SFTP uses SSH connections to provide secure file transfer.
- **Secure Copy**—Based on SSH2, SCP offers a secure method to copy files.

When acting as an Stelnet, SFTP, or SCP server, the device supports both SSH2 and SSH1 in non-FIPS mode and only SSH2 in FIPS mode.

FTP

File Transfer Protocol (FTP) is an application layer protocol for transferring files from one host to another over an IP network. It uses TCP port 20 to transfer data and TCP port 21 to transfer control commands.

The device can act as the FTP server.

Telnet

The device can act as a Telnet server to allow Telnet login. After you configure Telnet service on the device, users can remotely log in to the device to manage and monitor the device.

To prevent unauthorized Telnet logins, you can use ACLs to filter Telnet logins.

- If you does not specify an ACL for Telnet service, or the specified ACL does not exist or does not have rules, the device permits all Telnet logins.
- If the specified ACL has rules, only users permitted by the ACL can Telnet to the device.

NTP

Synchronize your device with a trusted time source by using the Network Time Protocol (NTP) or changing the system time before you run it on a live network.

NTP uses stratum to define the accuracy of each server. The value is in the range of 1 to 15. A smaller value represents a higher accuracy.

If the devices in a network cannot synchronize to an authoritative time source, you can perform the following tasks:

- Select a device that has a relatively accurate clock from the network.
- Use the local clock of the device as the reference clock to synchronize other devices in the network.

You can configure the local clock as a reference clock in the Web interface.

SNMP

Simple Network Management Protocol (SNMP) is an Internet standard protocol widely used for a network management station (NMS) to access and manage the devices (agents) on a network. After you enable SNMP on the device, the device acts as an SNMP agent.

SNMP enables an NMS to read and set the values of the variables on an agent. The agent sends traps to report events to the NMS.

MIB

Management Information Base (MIB) is a collection of objects. It defines hierarchical relations between objects and object properties, including object name, access privilege, and data type.

An NMS manages a device by reading and setting the values of variables (for example, interface status and CPU usage) on the device. These variables are objects in the MIB.

OID and subtree

A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a dotted numeric string that uniquely identifies the path from the root node to a leaf node. For example, the object **internet** is uniquely identified by the OID {1.3.6.1}.

A subtree is like a branch in the tree hierarchy. It contains a root node and the lower-level nodes of the root node. A subtree is identified by the OID of the root node.

MIB view

A MIB view is a subset of a MIB. You can control NMS access to MIB objects by specifying a MIB view for the username or community name that the NMS uses. For a subtree included in a MIB view, all nodes in the subtree are accessible to the NMS. For a subtree excluded in a MIB view, all nodes in the subtree are inaccessible to the NMS.

Subtree mask

A subtree mask is in hexadecimal format. It identifies a MIB view collectively with the subtree OID.

To determine whether an MIB object is in a MIB view, convert the subnet mask to binary bits (0 and 1) and match each bit with each node number of the object OID from left to right. If the 1-bit corresponded node numbers of the object OID are the same as those of the subtree OID, the MIB object is in the MIB view. The 0-bit corresponded node numbers can be different from those of the subtree OID.

For example, the view determined by the subtree OID 1.3.6.1.6.1.2.1 and the subtree mask 0xDB (11011011 in binary) includes all the nodes under the subtree OID 1.3.*.1.6.*.2.1, where * represents any number.

NOTE:

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

SNMP versions

You can enable SNMPv1, SNMPv2c, or SNMPv3 on a device. For an NMS and an agent to communicate, they must run the same SNMP version.

- SNMPv1 and SNMPv2c use community name for authentication. An NMS can access a device only when the NMS and the device use the same community name.
- SNMPv3 uses username for authentication and allows you to configure an authentication key and a privacy key to enhance communication security. The authentication key authenticates the validity of the packet sender. The privacy key is used to encrypt the packets transmitted between the NMS and the device.

SNMP access control

SNMPv1 and SNMPv2 access control

SNMPv1 and SNMPv2 uses community name for authentication. To control NMS access to MIB objects, configure one or both of the following settings on the community name that the NMS uses:

- Specify a MIB view for the community. You can specify only one MIB view for a community.

- If you grant read-only permission to the community, the NMS can only read the values of the objects in the MIB view.
- If you grant read-write permission to the community, the NMS can read and set the values of the objects in the MIB view.

- Specify a basic IPv4 ACL or a basic IPv6 ACL for the community to filter illegitimate NMSs from accessing the agent.
  - Only NMSs with the IPv4/IPv6 address permitted in the IPv4/IPv6 ACL can access the SNMP agent.
  - If you do not specify an ACL, or the specified ACL does not exist, all NMSs in the SNMP community can access the SNMP agent. If the specified ACL does not have any rules, no NMS in the SNMP community can access the SNMP agent.

SNMPv3 access control

SNMPv3 uses username for authentication. To control NMS access to MIB objects, configure one or both of the following settings on the username that the NMS uses:

- Create an SNMPv3 group and assign the username to the group. The user has the same access right as the group.

  When you create the group, specify one or more MIB views for the group. The MIB views include read-only MIB view, read-write MIB view, or notify MIB view. You can specify only one MIB view of a type for a group.
  - Read-only MIB view only allows the group to read the values of the objects in the view.
  - Read-write MIB view allows the group to read and set the values of the object in the view.
  - Notify MIB view automatically sends a notification to the NMS when the group accesses the view.
- Specify a basic IPv4 ACL or a basic IPv6 ACL for both the user and group to filter illegitimate NMSs from accessing the agent.
  - Only the NMSs permitted by ACLs specified for both the user and group can access the agent.
  - If you do not specify an ACL, or the specified ACL does not exist, all NMSs in the SNMP community can access the SNMP agent. If the specified ACL does not have any rules, no NMS in the SNMP community can access the SNMP agent.

Resources features

Resource features are common resources that can be used by multiple features. For example, you can use an ACL both in a packet filter to filter traffic and in a QoS policy to match traffic.

The Web interface provides access to the resource creation page for features that might use the resources. When you configure these features, you can create a resource without having to navigate to the **Resources** menu. However, to modify or remove a resource, you must access the **Resources** menu.

ACL

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 primarily used for packet filtering. You can use ACLs in QoS, security, routing, and other feature modules for identifying traffic. The packet drop or forwarding decisions depend on the modules that use ACLs.

ACL types and match criteria

Table 15 shows the ACL types available on the switch and the fields that can be used to filter or match traffic.

Table 15 ACL types and match criteria

Type	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 IPv4 address. • Destination IPv4 address. • Packet priority. • Protocol number. • Other Layer 3 and Layer 4 header fields.
		IPv6	• Source IPv6 address. • Destination IPv6 address. • Packet priority. • Protocol number. • Other Layer 3 and Layer 4 header fields.
Ethernet frame header ACLs	4000 to 4999	IPv4 and IPv6	Layer 2 header fields, including: • Source and destination MAC addresses. • 802.1p priority. • Link layer protocol type.

Match order

The rules in an ACL are sorted in a specific 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 rules and their 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 16 lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

Table 16 Sort ACL rules in depth-first order

ACL category	Sequence of tie breakers
IPv4 basic ACL	**1.** More 0s in the source IPv4 address wildcard (more 0s means a narrower IPv4 address range). **2.** Rule configured earlier.
IPv4 advanced ACL	**1.** Specific protocol number. **2.** More 0s in the source IPv4 address wildcard mask. **3.** More 0s in the destination IPv4 address wildcard. **4.** Narrower TCP/UDP service port number range. **5.** Rule configured earlier.
IPv6 basic ACL	**1.** Longer prefix for the source IPv6 address (a longer prefix means a narrower IPv6 address range). **2.** Rule configured earlier.
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.** Rule configured earlier.
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.** Rule configured earlier.

NOTE:

A wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. In contrast to a network mask, the 0 bits in a wildcard mask represent "do care" bits, and the 1 bits represent "don't care" bits. If the "do care" bits in an IP address are 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 or automatically numbered.

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.

Time range

You can implement a service based on the time of the day by applying a time range to it. A time-based service only takes effect in any time periods specified by the time range. For example, you can implement time-based ACL rules by applying a time range to them. If a time range does not exist, the service based on the time range does not take effect.

The following basic types of time ranges 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.

A time range is uniquely identified by the time range name. A time range can include multiple periodic statements and absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

SSL

Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security for TCP-based application layer protocols such as HTTP. SSL has been widely used in applications such as e-business and online banking to provide secure data transmission over the Internet.

SSL provides the following security services:

- **Privacy**—SSL uses a symmetric encryption algorithm to encrypt data. It uses the asymmetric key algorithm RSA to encrypt the key used by the symmetric encryption algorithm.
- **Authentication**—SSL uses certificate-based digital signatures to authenticate the SSL server and client. The SSL server and client obtain digital certificates through PKI.
- **Integrity**—SSL uses the message authentication code (MAC) to verify message integrity.

Public key

The device supports the following asymmetric key algorithms:

- Revest-Shamir-Adleman Algorithm (RSA).
- Digital Signature Algorithm (DSA).
- Elliptic Curve Digital Signature Algorithm (ECDSA).

Many security applications, including SSH, SSL, and PKI, use asymmetric key algorithms to secure communications. Asymmetric key algorithms use two separate keys (one public and one private) for encryption and decryption.

The device manages both local asymmetric key pairs and peer public keys for data encryption, decryption, and digital signature.

Managing local key pairs

Generating local key pairs

You can generate RSA, DSA, or ECDSA key pairs on the device.

Distributing the public key of a local key pair

You can distribute the public key of a local key pair to a peer device by using one of the following methods:

- Display the public key, record the key, and then import the key to the peer device through copy-and-paste.
- Export the public key in a specific format to a file, and then import the public key file to the peer device.
- Display the public key in a specific format, save it to a file, and import the public key file to the peer device.

Destroying a local key pair

To avoid key compromise, destroy the local key pair and generate a new pair after any of the following conditions occurs:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The local certificate has expired.

Managing peer public keys

To encrypt information sent to a peer device or authenticate the digital signature of the peer device, you must configure the peer device's public key on the local device.

You can import, view, and delete peer public keys on the local device.

Table 17 describes the peer public key configuration methods.

Table 17 Peer public key configuration methods

Method	Prerequisites	Remarks
Import the peer public key from a public key file (recommended)	1. Save the host public key in a file on the peer device. 2. Get the file from the peer device, for example, by using FTP or TFTP in binary mode.	The system automatically converts the imported public key to a string in the Public Key Cryptography Standards (PKCS) format.
Manually enter (type or copy) the peer public key	Display and record the public key on the peer device.	• Be sure to enter the key in the format in which the key is displayed on the peer device. If the key is not in the correct format, the system discards the key. • Always use the first method if you are not sure of the format of the recorded public key.

PKI

Public Key Infrastructure (PKI) is an asymmetric key infrastructure to encrypt and decrypt data for securing network services.

PKI uses digital certificates to distribute and employ public keys, and provides network communication and e-commerce with security services such as user authentication, data confidentiality, and data integrity.

PKI provides certificate management for SSL.

Digital certificate and CRL

- **Digital certificate**—An electronic document signed by a CA that binds a public key with the identity of its owner.

  A digital certificate includes the following information:

  - Issuer name.
  - Subject name (name of the individual or group to which the certificate is issued).
  - Subject's public key.
  - Signature of the CA.
  - Validity period.

  A digital certificate must comply with the international standards of ITU-T X.509, of which X.509 v3 is the most commonly used.

  This help covers the following types of certificates:

  - **CA certificate**—Certificate of a CA. Multiple CAs in a PKI system form a CA tree, with the root CA at the top. The root CA generates a self-signed certificate, and each lower level CA holds a CA certificate issued by the CA immediately above it. The chain of these certificates forms a chain of trust.
  - **Local certificate**—Digital certificate issued by a CA to a PKI entity, which contains the entity's public key.
- **CRL**—A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked. A CRL is created and signed by the CA that originally issued the certificates.

  The CA publishes CRLs periodically to revoke certificates. Entities that are associated with the revoked certificates should not be trusted.

  The CA must revoke a certificate when any of the following conditions occurs:

  - The certificate subject name is changed.
  - The private key is compromised.
  - The association between the subject and CA is changed. For example, when an employee terminates employment with an organization.

PKI architecture

A PKI system consists of PKI entities, CAs, RAs and a certificate/CRL repository.

- **PKI entity**—An end user using PKI certificates. The PKI entity can be an operator, an organization, a device like a router or a switch, or a process running on a computer. A valid PKI entity must include one or more of following identity categories:
  - Distinguished name (DN) of the entity, which further includes the common name, county code, locality, organization, unit in the organization, and state. If you configure the DN for an entity, a common name is required.
  - FQDN of the entity.
  - IP address of the entity.

- **CA**—Certification authority that issues and manages certificates. A CA issues certificates, defines the certificate validity periods, and revokes certificates by publishing CRLs.
- **RA**—Registration authority, which offloads the CA by processing enrollment requests. The RA accepts certificate requests, verifies user identity, and determines whether to forward the certificate requests to the CA.
- **Certificate/CRL repository**—A certificate distribution point that stores certificates and CRLs, and distributes these certificates and CRLs to PKI entities. It also provides the query function. A PKI repository can be a directory server using the LDAP or HTTP protocol, of which LDAP is commonly used.

Managing certificates

The device manages certificates in PKI domains. A PKI domain contains enrollment information for a PKI entity. It is locally significant and is intended only for reference by other applications like IKE and SSL.

Importing certificates

You can import CA certificates and local certificates related to a PKI entity to a PKI domain. You must import certificates in the following situations:

- The CRL repository is not specified on the device.
- The CA server does not support SCEP.
- The CA server generates the key pair for the certificates.

Before you import certificates, perform the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device.
- Obtain the CA certificate chain if it is neither available in the PKI domain nor contained in the certificate to be imported.

When you import local certificates, follow these guidelines:

- If the certificate to be imported contains the CA certificate chain, you also import the CA certificate by importing the local certificate.
- You can directly import the local certificate if its associated CA certificate already exists on the device.
- If the certificate file to be imported contains the root CA certificate, you must verify the fingerprint of the root certificate during the import. Contact the CA administrator to obtain the fingerprint of the root CA certificate.
- To import a local certificate containing an encrypted key pair, you must provide the challenge password. Contact the CA administrator to obtain the password. During the import, the system searches the PKI domain for the key pair settings and saves the key pair accordingly. If the domain already contains the key pair, the system prompts whether you want to overwrite the existing key pair. If the PKI domain does not contain settings for the key pair, the system generates the key pair locally based on the algorithm and usage of the key pair in the certificate.

You can import the following CA certificates:

- Root CA certificate.
- Non-root CA certificate that contains the complete certificate chain.
- Non-root CA certificate that contains partial certificate chain and can form complete certificate chain with existing CA certificates on the device.

Exporting certificates

You can export the CA certificate and the local certificates in a PKI domain to certificate files. The exported certificate files can then be imported back to the device or other PKI applications.

Requesting certificates

To request a certificate, a PKI entity must provide its identity information and public key to a CA.

You can first generate the certificate request on the device, and then send the request to the CA by using an out-of-band method such as phone and email.

Before you submit a certificate request, make sure the CA certificate exists in the PKI domain and a key pair is specified for the PKI domain.

- The CA certificate is used to verify the authenticity and validity of the obtained local certificate.
- The key pair is used for certificate request. Upon receiving the public key and the identity information, the CA signs and issues a certificate.

When generating the certificate request, the system automatically creates a key pair if the key pair specified in the PKI domain does not exist. The name, algorithm, and length of the key pair are configured in the PKI domain.

Certificate access control

Certificate access control policies

Certificate access control policies allow you to authorize access to a device (for example, an HTTPS server) based on the attributes of an authenticated client's certificate.

A certificate access control policy is a set of access control rules (permit or deny statements). Each access control rule associates an action with an attribute group.

- **Action**—Determines whether a certificate is considered valid (**Permit**) or invalid (**Deny**).
- **Attribute group**—Contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field.

If a certificate matches all attribute rules in a certificate attribute group associated with an access control rule, the system determines that the certificate matches the access control rule. In this scenario, the match process stops, and the system performs the access control action defined in the access control rule.

The following conditions describe how a certificate access control policy verifies the validity of a certificate:

- The system matches a certificate with the access control rules (statements) in a policy in ascending order of the rule ID.
- If a certificate matches a permit statement, the certificate passes the verification.
- If a certificate matches a deny statement or does not match any statements in the policy, the certificate is regarded invalid.
- If a statement is associated with a non-existing attribute group, or the attribute group does not have attribute rules, the certificate matches the statement.
- If the certificate access control policy referenced by a security application (for example, HTTPS) does not exist, all certificates in the application pass the verification.

Attribute groups

A certificate attribute group contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field.

An attribute rule is a combination of an attribute-value pair with an operation keyword, as listed in Table 18.

Table 18 Combinations of attribute-value pairs and operation keywords

Operation	DN	FQDN/IP
ctn	The DN contains the specified attribute value.	Any FQDN or IP address contains the specified attribute value.
nctn	The DN does not contain the specified attribute value.	None of the FQDNs or IP addresses contains the specified attribute value.
equ	The DN is the same as the specified attribute value.	Any FQDN or IP address is the same as the specified attribute value.
nequ	The DN is not the same as the specified attribute value.	None of the FQDNs or IP addresses are the same as the specified attribute value.

A certificate matches an attribute rule only if it contains an attribute that matches the criterion defined in the rule.

A certificate matches an attribute group if it matches all attribute rules in the group.

QoS features

QoS policies

In data communications, Quality of Service (QoS) provides differentiated service guarantees for diversified traffic in terms of bandwidth, delay, jitter, and drop rate, all of which can affect QoS.

By associating a traffic behavior with a traffic class in a QoS policy, you apply QoS actions in the traffic behavior to the traffic class.

Traffic class

A traffic class defines a set of match criteria for classifying traffic.

Traffic behavior

A traffic behavior defines a set of QoS actions to take on packets.

QoS policy

A QoS policy associates traffic classes with traffic behaviors and performs the actions in each behavior on its associated traffic class.

Applying a QoS policy

You can apply a QoS policy to the following destinations:

- **Interface**—The QoS policy takes effect on the traffic sent or received on the interface. The QoS policy applied to the outgoing traffic on an interface does not regulate local packets. Local packets refer to critical protocol packets sent by the local system for operation maintenance. The most common local packets include link maintenance packets.
- **VLAN**—The QoS policy takes effect on the traffic sent or received on all ports in the VLAN. QoS policies cannot be applied to dynamic VLANs, for example, VLANs created by GVRP.
- **Globally**—The QoS policy takes effect on the traffic sent or received on all ports.

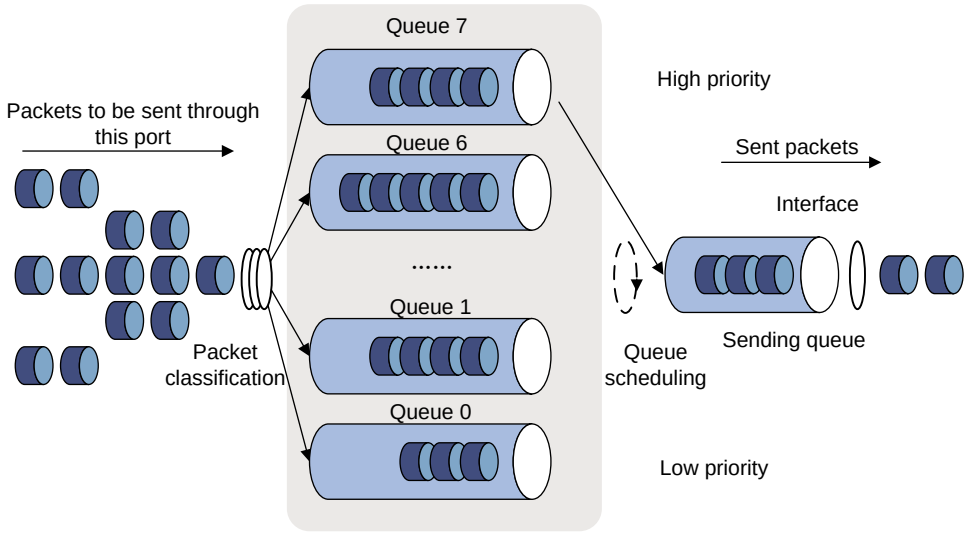
Release 3111P02 does not support applying a QoS policy to the outbound direction of an interface, a VLAN, or globally.

Hardware queuing

Congestion occurs on a link or node when the traffic size exceeds the processing capability of the link or node. Congestion is unavoidable in switched networks or multiuser application environments. To improve the service performance of your network, implement congestion management policies. Queuing is a typical congestion management technique. SP, WRR, and WFQ are typical queuing methods.

SP queuing

Figure 9 SP queuing



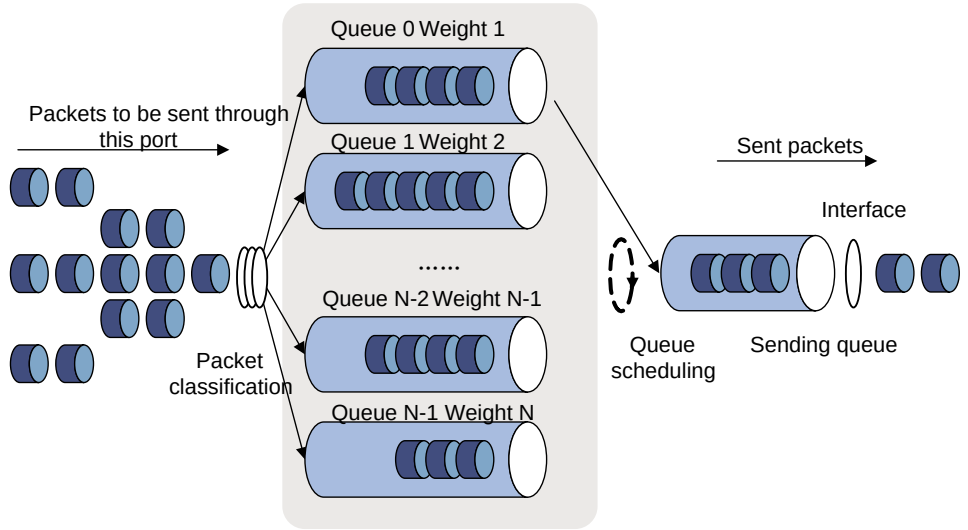
SP queuing is designed for mission-critical applications that require preferential service to reduce the response delay when congestion occurs. SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

SP queuing schedules the eight queues in the descending order of priority. SP queuing 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 a high priority queue to make sure they are always serviced first. Common service packets can be assigned to low priority queues to be transmitted when high priority queues are empty.

The disadvantage of SP queuing is that packets in the lower priority queues cannot be transmitted if packets exist in the higher priority queues. In the worst case, lower priority traffic might never get serviced.

WRR queuing

Figure 10 WRR queuing



WRR queuing schedules all the queues in turn to ensure every queue is serviced. For example, a port provides eight output queues. WRR assigns each queue a weight value (represented by w7, w6, w5, w4, w3, w2, w1, or w0). The weight value of a queue decides the proportion of resources assigned to the queue. On a 1 Gbps port, you can set the weight values to 50, 30, 10, 10, 50, 30, 10, and 10 for w7 through w0. In this way, the queue with the lowest priority can get a minimum of 50 Mbps bandwidth. In comparison, SP queuing might fail to service packets in low-priority queues for a long period of time.

Another advantage of WRR queuing is that when 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.

WRR queuing includes the following types:

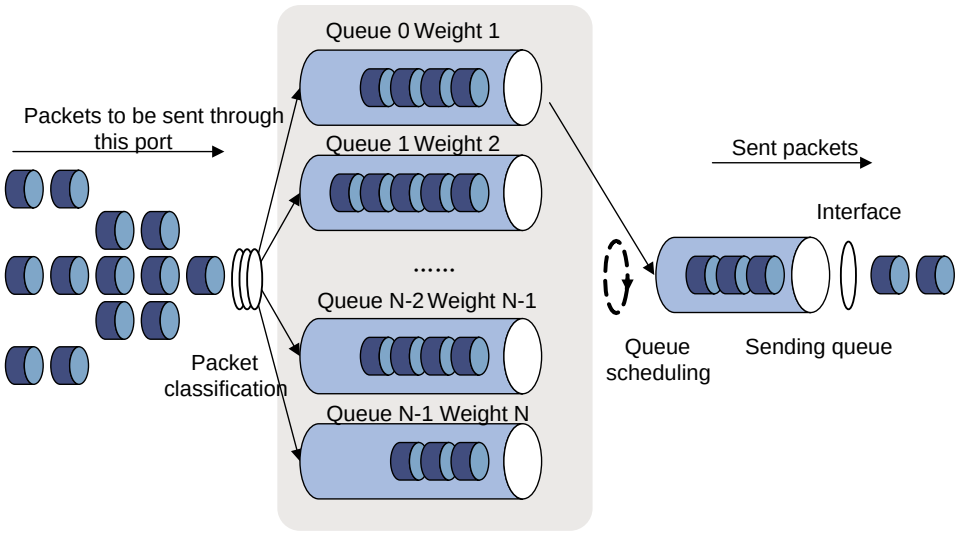
- **Basic WRR queuing**—Contains multiple queues. You can configure the weight for each queue, and WRR schedules these queues based on the user-defined parameters in a round robin manner.
- **Group-based WRR queuing**—All the queues are scheduled by WRR. You can divide output queues to WRR group 1 and WRR group 2. Round robin queue scheduling is performed for group 1 first. When group 1 is empty, round robin queue scheduling is performed for group 2.

On an interface enabled with group-based WRR queuing, you can assign queues to the SP group. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR groups.

Only group-based WRR queuing is supported in the current software version, and only WRR group 1 is supported.

WFQ queuing

Figure 11 WFQ queuing



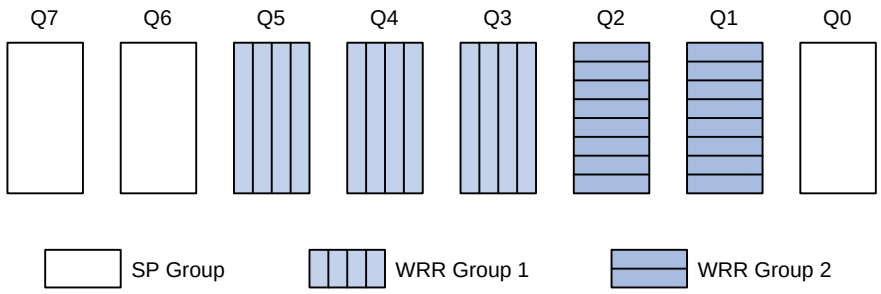
WFQ automatically classifies traffic based on packet fields including protocol type, TCP or UDP source/destination port numbers, source/destination IP addresses, and IP precedence bits in the ToS field. To ensure proportional scheduling fairness, WFQ provides as many queues as possible so that each traffic flow has a separate queue When dequeuing packets, WFQ assigns the outgoing interface bandwidth to each traffic flow by precedence. The higher precedence value a traffic flow has, the more bandwidth it gets.

For example, five flows exist in the current interface with precedence 0, 1, 2, 3, and 4. The total bandwidth quota is the sum of all the (precedence value + 1): 1 + 2 + 3 + 4 + 5 = 15. The bandwidth percentage assigned to each flow is (precedence value of the flow + 1)/total bandwidth quota. The bandwidth percentages for the flows are 1/15, 2/15, 3/15, 4/15, and 5/15.

WFQ is similar to WRR. On an interface with group-based WFQ queuing enabled, you can assign queues to the SP group. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WFQ groups. The difference is that WFQ enables you to set guaranteed bandwidth that a WFQ queue can get during congestion.

Queue scheduling profile

Queue scheduling profiles support three queue scheduling algorithms: SP, WRR, and WFQ. In a queue scheduling profile, you can configure SP + WRR or SP + WFQ. When the three queue scheduling algorithms are configured, SP queues, WRR groups, and WFQ groups are scheduled in descending order of queue ID. In a WRR or WFQ group, queues are scheduled based on their weights. When SP and WRR groups are configured in a queue scheduling profile, the following figure shows the scheduling order.



- Queue 7 has the highest priority. Its packets are sent preferentially.
- Queue 6 has the second highest priority. Packets in queue 6 are sent when queue 7 is empty.
- Queue 3, queue 4, and queue 5 are scheduled according to their weights. When both queue 6 and queue 7 are empty, WRR group 1 is scheduled.
- Queue 1 and queue 2 are scheduled according to their weights. WRR group 2 is scheduled when queue 7, queue 6, queue 5, queue 4, and queue 3 are all empty.
- Queue 0 has the lowest priority, and it is scheduled when all other queues are empty.

Priority mapping

When a packet arrives, a device assigns values of priority parameters to the packet for the purpose of queue scheduling and congestion control.

Priority mapping allows you to modify the priority values of the packet according to priority mapping rules. The priority parameters decide the scheduling priority and forwarding priority of the packet.

Port priority

When a port is configured with a priority trust mode, the device trusts the priorities included in incoming packets. The device can automatically resolve the priorities or flag bits included in packets. The device then maps the trusted priority to the target priority types and values according to the priority maps.

When a port is not configured with a priority trust mode but is configured with a port priority, the device does not trust the priorities included in incoming packets. The device uses its port priority to look for priority parameters for the incoming packets.

Configuring the port priority

After you configure a port priority for a port, the device uses its port priority to look for priority parameters for incoming packets.

Configuring the priority trust mode

After you configure a priority trust mode for a port, the device maps the trusted priority in incoming packets to the target priority types and values according to the priority maps.

The available priority trust modes include the following types:

- **Untrust**—Does not trust any priority included in packets.
- **Dot1p**—Trusts the 802.1p priorities included in packets.
- **DSCP**—Trusts the DSCP priorities included in IP packets.

Priority map

The device provides three priority maps: 802.1p-lp, DSCP-802.1p, and DSCP-DSCP. If a default priority map cannot meet your requirements, you can modify the priority map as required.

Rate limit

Rate limit uses token buckets for traffic control. If there are tokens in the token bucket, bursty traffic is allowed. Otherwise, packets are not forwarded until new tokens are generated. In this way, packets are limited to the token generation rate while bursty traffic is allowed.

A token bucket has the following configurable parameters:

- Mean rate at which tokens are put into the bucket, which is the permitted average rate of traffic. It is typically set to the committed information rate (CIR).
- Burst size or the capacity of the token bucket. It is the maximum traffic size permitted in each burst. It is typically set to the committed burst size (CBS). The set burst size must be greater than the maximum packet size.

Each arriving packet is evaluated. 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, the traffic is excessive.

When rate limit is configured on an interface, a token bucket handles all packets to be sent through the interface for rate limiting. If enough tokens are in the token bucket, packets can be forwarded. Otherwise, packets are put into QoS queues for congestion management. In this way, the traffic passing the interface is controlled.

Security features

Packet filter

Packet filter uses ACLs to filter incoming or outgoing packets on interfaces, VLANs, or globally. An interface permits packets that match permit statements to pass through, and denies packets that match deny statements. The default action applies to packets that do not match any ACL rules.

The packet filter feature does not support displaying the hardwarecounting result.

The packet filter feature does not support applying an ACL to VLANs to filter packets.

IP source guard

Overview

IP source guard (IPSG) prevents spoofing attacks by using an IPSG binding table to match legitimate packets. It drops all packets that do not match the table.

The IPSG binding table can include the following bindings:

- IP-interface.
- MAC-interface.
- IP-MAC-interface.
- IP-VLAN-interface.
- MAC-VLAN-interface.
- IP-MAC-VLAN-interface.

Interface-specific static IPv4SG bindings

Interface-specific static IPv4SG bindings are configured manually and take effect only on the interface. They are suitable for scenarios where a few hosts exist on a LAN and their IP addresses are manually configured. For example, you can configure a static IPv4SG binding on an interface that connects to a server. This binding allows the interface to receive packets only from the server.

Static IPv4SG bindings on an interface implements the following functions:

- Filter incoming IPv4 packets on the interface.
- Cooperate with ARP detection for user validity checking.

You can configure the same static IPv4SG binding on different interfaces.

802.1X

802.1X is a port-based network access control protocol that controls network access by authenticating the devices connected to 802.1X-enabled LAN ports.

802.1X architecture

802.1X includes the following entities:

- **Client**—A user terminal seeking access to the LAN. The terminal must have 802.1X software to authenticate to the access device.
- **Access device**—Authenticates the client to control access to the LAN. In a typical 802.1X environment, the access device uses an authentication server to perform authentication.
- **Authentication server**—Provides authentication services for the access device. The authentication server first authenticates 802.1X clients by using the data sent from the access device. Then, the server returns the authentication results to the access device to make access decisions. The authentication server is typically a RADIUS server. In a small LAN, you can use the access device as the authentication server.

802.1X authentication methods

The access device can perform EAP relay or EAP termination to communicate with the RADIUS server.

- **EAP termination**—The access device performs the following operations in EAP termination mode:
  a. Terminates the EAP packets received from the client.
  b. Encapsulates the client authentication information in standard RADIUS packets.
  c. Uses PAP or CHAP to authenticate to the RADIUS server.
  CHAP does not send plaintext password to the RADIUS server, and PAP sends plaintext password to the RADIUS server.
- **EAP relay**—The access device uses EAPOR packets to send authentication information to the RADIUS server.

Access control methods

Comware 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, all subsequent users 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.

Port authorization state

The port authorization state determines whether the client is granted access to the network. You can control the authorization state of a port by using the following options:

- **Authorized**—Places the port in the authorized state, enabling users on the port to access the network without authentication.
- **Unauthorized**—Places the port in the unauthorized state, denying any access requests from users on the port.
- **Auto**—Places the port initially in unauthorized state to allow only EAPOL packets to pass. 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.

Periodic online user reauthentication

Periodic online user reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the server. The attributes include the ACL, VLAN, and user profile-based QoS. The reauthentication interval is user configurable.

Online user handshake

The online user handshake feature checks the connectivity status of online 802.1X users. The access device sends handshake messages to online users at the handshake interval. If the device does not receive any responses from an online user after it has made the maximum handshake attempts, the device sets the user to offline state.

You can also enable the online user handshake security feature to check authentication information in the handshake packets from clients. With this feature, the device prevents 802.1X users who use illegal client software from bypassing iNode security check such as dual network interface cards (NICs) detection.

Authentication trigger

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:

- **Unicast trigger mode**—Upon receiving a frame from an unknown MAC address, the access device sends an Identity EAP-Request packet out of the receiving port to the MAC address. The device retransmits the packet if no response has been received within the specified interval.
- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets periodically (every 30 seconds by default) to initiate 802.1X authentication.

Auth-Fail VLAN

The 802.1X Auth-Fail VLAN on a port accommodates users who have failed 802.1X authentication because of the failure to comply with the organization's security strategy. For example, the VLAN accommodates users who have entered a wrong password. The Auth-Fail VLAN does not accommodate 802.1X users who have failed authentication for authentication timeouts or network connection problems.

The access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method.

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 802.1X Auth-Fail VLAN fails 802.1X reauthentication	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 authorization VLAN of the user to the port as the PVID, and it removes the port from the Auth-Fail VLAN. After the user logs off, the guest VLAN is assigned to the port as the PVID. If no guest VLAN is configured, the initial PVID of the port is restored. • If the authentication server does not authorize a VLAN, the initial PVID of the port applies. The user and all subsequent 802.1X users are

Authentication status	VLAN manipulation
	assigned to the initial PVID. After the user logs off, the PVID remains unchanged.

Guest VLAN

The 802.1X guest VLAN on a port accommodates users who have not performed 802.1X authentication. 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 access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method.

On a port that performs port-based access control:

Authentication status	VLAN manipulation
A user has not passed 802.1X authentication.	The device assigns the 802.1X guest VLAN to the port as the PVID. All 802.1X users on this port can access resources only 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 authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X guest VLAN. After the user logs off, the initial PVID of the port is restored. • If the authentication server does not authorize a VLAN, the initial PVID applies. The user and all subsequent 802.1X users are assigned to the initial port VLAN. After the user logs off, the port VLAN remains unchanged. NOTE: The initial PVID of an 802.1X-enabled port refers to the PVID used by the port before the port is assigned to any 802.1X VLANs.

Critical VLAN

The 802.1X critical VLAN on a port accommodates 802.1X users who have failed authentication because none of the RADIUS servers in their ISP domain is reachable. The critical VLAN feature takes effect when 802.1X authentication is performed only through RADIUS servers. If an 802.1X user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

The access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method.

On a port that performs port-based access control:

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are	The device assigns the critical VLAN to the port as the PVID. The 802.1X user and all subsequent 802.1X users on this port can access resources only in the 802.1X critical VLAN.

Authentication status	VLAN manipulation
unreachable.	
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The critical VLAN is still the PVID of the port, and all 802.1X users on this port are in this VLAN.
A user in the 802.1X critical VLAN fails authentication for any other reasons except for unreachable servers.	If an 802.1X Auth-Fail VLAN has been configured, the PVID of the port changes to the Auth-Fail VLAN ID, and all 802.1X users on this port are moved to the Auth-Fail VLAN. If no 802.1X Auth-Fail VLAN is configured, the initial PVID of the port is restored.
A user in the 802.1X critical VLAN passes 802.1X authentication.	• The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X critical VLAN. After the user logs off, the guest VLAN ID changes to the PVID. If no 802.1X guest VLAN is configured, the initial PVID of the port is restored. • If the authentication server (either the local access device or a RADIUS server) does not authorize a VLAN, the initial PVID of the port applies. The user and all subsequent 802.1X users are assigned to this port VLAN. After the user logs off, the PVID remains unchanged.
A user in the 802.1X guest VLAN fails authentication because all the RADIUS servers are unreachable.	The device assigns the 802.1X critical VLAN to the port as the PVID, and all 802.1X users on this port are in this VLAN.
A user in the 802.1X Auth-Fail VLAN fails authentication because all the RADIUS servers are unreachable.	The PVID of the port remains unchanged. All 802.1X users on this port can access resources only in the 802.1X Auth-Fail VLAN.
A user who has passed authentication fails reauthentication because all the RADIUS servers are unreachable, and the user is logged out of the device.	The device assigns the 802.1X critical VLAN to the port as the PVID.

Mandatory authentication domain

You can place all 802.1X users in a mandatory authentication domain for authentication, authorization, and accounting on a port. No user can use an account in any other domain to access the network through the port. The implementation of a mandatory authentication domain enhances the flexibility of 802.1X access control deployment.

EAD assistant

Endpoint Admission Defense (EAD) is an integrated endpoint access control solution to improve the threat defensive capability of a network. The solution enables the security client, security policy server, access device, and third-party server to operate together. If a terminal device seeks to access an EAD network, it must have an EAD client, which performs 802.1X authentication.

The EAD assistant feature enables the access device to redirect a user who is seeking to access the network to download and install an EAD client. This feature eliminates the administrative task to deploy EAD clients.

MAC authentication

Overview

MAC authentication controls network access by authenticating source MAC addresses on a port. The feature does not require client software, and users do not have to enter usernames and passwords for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication-enabled port.

Silent MAC address information

When a user fails MAC authentication, the device marks the user's MAC address as a silent MAC address, drops the packet, and starts a quiet timer. The device drops all subsequent packets from the silent MAC address within the quiet time. The quiet mechanism avoids repeated authentication during the quiet time.

Username format

MAC authentication supports the following username formats:

- **Individual** MAC **address**—The device uses the MAC address of each user as the username and password for MAC authentication. This format is suitable for an insecure environment.
- **Shared username**—You specify one username and password, which is not necessarily a MAC address, for all MAC authentication users on the device. This format is suitable for a secure environment.

MAC authentication domain

By default, MAC authentication users are in the system default authentication domain. To implement different access policies for users, you can use one of the following methods to specify authentication domains for MAC authentication users:

- Specify a global authentication domain. This domain setting applies to all ports enabled with MAC authentication.
- Specify an authentication domain for an individual port.

MAC authentication chooses an authentication domain for users on a port in the following order: the port-specific domain, the global domain, and the default domain.

Offline detect timer

This timer sets the interval that the device waits for traffic from a user before the device regards the user idle. If a user connection has been idle within the interval, the device logs the user out and stops accounting for the user.

Quiet timer

This timer sets the interval that the device must wait before the device can perform MAC authentication for a user who has failed MAC authentication. All packets from the MAC address are dropped during the quiet time.

Server timeout timer

This timer sets the interval that the device waits for a response from a RADIUS server before the device regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

MAC authentication configuration on a port

For MAC authentication to take effect on a port, you must enable this feature globally and on the port.

Authentication delay

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered.

If no 802.1X authentication is triggered or 802.1X authentication fails within the delay period, the port continues to process MAC authentication.

Do not set the port security mode to **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** when you use MAC authentication delay. The delay does not take effect on a port in either of the two modes.

Multi-VLAN mode

The MAC authentication multi-VLAN mode prevents an authenticated online user from service interruption caused by VLAN changes on a port. When the port receives a packet sourced from the user in a VLAN that does not match the existing MAC-VLAN mapping, the device does not logs off the user or reauthenticates the user. The device creates a new MAC-VLAN mapping for the user, and traffic transmission is not interrupted. The original MAC-VLAN mapping for the user remains on the device until it dynamically ages out.

This feature improves transmission of data that is vulnerable to delay and interference. It is typically applicable to IP phone users.

Periodic MAC reauthentication

Periodic MAC reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the RADIUS server. The attributes include the ACL, VLAN, and user profile-based QoS.

The device reauthenticates an online MAC authentication user periodically only after it receives the termination action **Radius-request** from the authentication server for this user. The Session-Timeout attribute (session timeout period) assigned by the server is the reauthentication interval. To display the server-assigned Session-Timeout and Termination-Action attributes, use the **display mac-authentication connection** command. Support for the server configuration and assignment of Session-Timeout and Termination-Action attributes depends on the server model.

When no server is reachable for MAC reauthentication, the device keeps the MAC authentication users online or logs off the users, depending on the keep-online feature configuration on the device.

Keep-online

By default, the device logs off online MAC authentication users if no server is reachable for MAC reauthentication. The keep-online feature keeps authenticated MAC authentication users online when no server is reachable for MAC reauthentication.

In a fast-recovery network, you can use the keep-online feature to prevent MAC authentication users from frequently coming online and going offline.

Port security

Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. Port security provides the following functions:

- Prevents unauthorized access to a network by checking the source MAC addresses of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC addresses of outbound traffic.
- Controls 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 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.

Authorization-fail-offline

The authorization-fail-offline feature logs off port security users who fail ACL or user profile authorization.

A user fails ACL or user profile authorization in the following situations:

- The device fails to authorize the specified ACL or user profile to the user.
- The server assigns a nonexistent ACL or user profile to the user.

If this feature is disabled, the device does not log off users who fail ACL or user profile authorization.

Aging timer for secure MAC addresses

When secure MAC addresses are aged out, they are removed from the secure MAC address table.

The aging timer applies to all configured sticky secure MAC addresses and those automatically learned by a port. To disable the aging timer, set the timer to 0.

Silence period

This period sets the duration during which a port remains disabled when the port receives illegal frames. The intrusion protection action on the port must be **Disable port temporarily**.

Authentication OUI

The configured OUI value takes effect only when the port authentication mode is **userLoginWithOUI**.

In userLoginWithOUI mode, the port allows a maximum of two users to pass through, including:

- One user who passes 802.1X authentication.
- One user whose MAC address matches any one of the OUIs configured on the device.

Port security settings

Port security modes

Port security supports the following categories of security modes:

- **MAC learning control**—Includes two modes: autoLearn and secure. MAC address learning is permitted on a port in autoLearn mode and disabled in secure mode.
- **Authentication**—Security modes in this category implement MAC authentication, 802.1X authentication, or a combination of these two authentication methods.

Upon receiving a frame, the port in a security mode searches the MAC address table for the source MAC address. If a match is found, the port forwards the frame. If no match is found, the port learns the MAC address or performs authentication, depending on the security mode. If the frame is illegal, the port takes the predefined NTK or intrusion protection action. Outgoing frames are not restricted by port security's NTK action unless they trigger the NTK feature.

Table 19 describes the port security modes and the security features.

Table 19 Port security modes

Purpose	Security mode	Features that can be triggered
Turning off the port security feature	noRestrictions (the default mode) In this mode, port security is disabled on the port	N/A

Purpose	Security mode		Features that can be triggered
	and access to the port is not restricted.		
Control MAC address learning:	autoLearn		NTK/intrusion protection
	secure		
Perform 802.1X authentication:	userLogin		N/A
	userLoginSecure		NTK/intrusion protection
	userLoginSecureExt		
	userLoginWithOUI		
Perform MAC authentication:	macAddressWithRadius		NTK/intrusion protection
Perform a combination of MAC authentication and 802.1X authentication:	Or	macAddressOrUserLoginSecure	NTK/intrusion protection
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

- Control MAC address learning:
  - autoLearn.

    A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, these MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also manually add secure MAC addresses.

    A port in autoLearn mode allows frames sourced from the following MAC addresses to pass:

    - Secure MAC addresses.
    - Manually configured static and dynamic MAC addresses.

    When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.
  - secure.

    MAC address learning is disabled on a port in secure mode. A port in secure mode allows only frames sourced from the following MAC addresses to pass:

    - Secure MAC addresses.
    - Manually configured static and dynamic MAC addresses.
- Perform 802.1X authentication:
  - userLogin.

    A port in this mode performs 802.1X authentication and implements port-based access control. The port can service multiple 802.1X users. Once an 802.1X user passes authentication on the port, any subsequent 802.1X users can access the network through the port without authentication.
  - userLoginSecure.

    A port in this mode performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.
  - userLoginSecureExt.

    This mode is similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.

- userLoginWithOUI.

  This mode is similar to the userLoginSecure mode. The difference is that a port in this mode also permits frames from one user whose MAC address contains a specific OUI.

  In this mode, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

- Perform MAC authentication:

  macAddressWithRadius: A port in this mode performs MAC authentication, and services multiple users.

- Perform a combination of MAC authentication and 802.1X authentication:
  - macAddressOrUserLoginSecure.

    This mode is the combination of the macAddressWithRadius and userLoginSecure modes. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

    In this mode, the port performs 802.1X authentication first. If 802.1X authentication fails, MAC authentication is performed.

  - macAddressOrUserLoginSecureExt.

    This mode is similar to the macAddressOrUserLoginSecure mode, except that this mode supports multiple 802.1X and MAC authentication users.

  - macAddressElseUserLoginSecure.

    This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority as the **Else** keyword implies. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

    In this mode, the port performs MAC authentication upon receiving non-802.1X frames. Upon receiving 802.1X frames, the port performs MAC authentication and then, if the authentication fails, 802.1X authentication.

  - macAddressElseUserLoginSecureExt.

    This mode is similar to the macAddressElseUserLoginSecure mode except that this mode supports multiple 802.1X and MAC authentication users as the **Ext** keyword implies.

Port security features

Intrusion protection mode

The intrusion protection feature checks the source MAC addresses in inbound frames for illegal frames, and takes one of the following actions in response to illegal frames:

- **Block MAC**—Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards the frames. All subsequent frames sourced from a blocked MAC address are dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is fixed and cannot be changed.
- **Disable port**—Disables the port until you bring it up manually.
- **Disable port temporarily**—Disables the port for a period of time. The silence period is user configurable.

NTK mode

The NTK feature checks the destination MAC addresses in outbound frames to make sure frames are forwarded only to authenticated devices.

The NTK feature supports the following modes:

- **ntkonly**—Forwards only unicast frames with authenticated destination MAC addresses.

- **ntk-withbroadcasts**—Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.
- **ntk-withmulticasts**—Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

The NTK feature drops any unicast frame with an unknown destination MAC address.

Secure MAC addresses

Secure MAC addresses are configured or learned in autoLearn mode. Secure MAC addresses include static, sticky, and dynamic secure MAC addresses.

Aging mode for secure MAC addresses

Secure MAC addresses can be aged out when you use one of the following aging modes:

- **Timeout**—Secure MAC addresses age out when the aging timer expires. The aging timer counts up regardless of whether traffic data has been sent from secure MAC addresses. By default, this mode is used.
- **Inactivity**—Secure MAC addresses age out only when no traffic is detected during the aging interval. The device detects whether traffic data has been sent from a secure MAC address when the aging timer expires for the secure MAC address. If traffic is detected, the aging timer restarts. This feature prevents the unauthorized use of a secure MAC address when the authorized user is offline.

Dynamic secure MAC

This feature converts sticky MAC addresses to dynamic and disables saving them to the configuration file.

When this feature is enabled, you cannot manually configure sticky MAC addresses. All dynamic MAC addresses are lost at reboot. Use this feature when you want to clear all sticky MAC addresses after a device reboot.

When this feature is disabled, all dynamic secure MAC addresses on the port are converted to sticky MAC addresses, and you can manually configure sticky MAC addresses.

Authorization information ignore

A port can be configured to ignore the authorization information received from the server (local or remote) after an 802.1X or MAC authentication user passes authentication.

Max users

This function specifies the maximum number of secure MAC addresses that port security allows on a port. The maximum number is configured for the following purposes:

- Control the number of concurrent users on the port.

  For a port operating in a security mode (except for autoLearn and secure), the upper limit equals the smaller of the following values:

  - The limit of the secure MAC addresses that port security allows.
  - The limit of concurrent users allowed by the authentication mode in use.
- Control the number of secure MAC addresses on the port in autoLearn mode.

Portal

Portal authentication controls user access to networks. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Allows users to perform authentication through a Web browser without installing client software.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.
- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assignment scheme and saves public IP addresses. Cross-subnet authentication can authenticate users who reside in a different subnet than the access device.

A typical portal system consists of the following components:

- **Authentication client**—A Web browser that runs HTTP/HTTPS or a user host that runs a portal client application.
- **Access device**—Broadband access device such as a switch or a router.
- **Portal authentication server**—Receives authentication requests from authentication clients and interacts user authentication information with the access device.
- **Portal Web server**—Pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server.

  The portal authentication server and the portal Web server are usually the same device, but they can also be separate devices.
- **AAA server**—Interacts with the access device to implement authentication, authorization, accounting for portal users.

Portal authentication server

A portal authentication server receives authentication requests from authentication clients and interacts user authentication information with the access device.

Portal authentication server detection

During portal authentication, if the communication between the access device and portal authentication server is broken, both of the following occur:

- New portal users are not able to log in.
- The online portal users are not able to log out normally.

To address this problem, the access device needs to be able to detect the reachability changes of the portal server quickly and take corresponding actions to deal with the changes.

With the detection feature enabled, the device periodically detects portal login, logout, or heartbeat packets sent by a portal authentication server to determine the reachability of the server. If the device receives a portal packet within a detection timeout and the portal packet is valid, the device determines the portal authentication server to be reachable. Otherwise, the device determines the portal authentication server to be unreachable.

You can configure the device to take one or more of the following actions when the server reachability status changes:

- Sending a trap message to the NMS. The trap message contains the name and current state of the portal authentication server.
- Sending a log message, which contains the name, the current state, and the original state of the portal authentication server.

Portal user synchronization

Once the access device loses communication with a portal authentication server, the portal user information on the access device and the server might be inconsistent after the communication

resumes. To address this problem, the device provides the portal user synchronization feature. This feature is implemented by sending and detecting portal synchronization packets, as follows:

1. The portal authentication server sends the online user information to the access device in a synchronization packet at the user heartbeat interval.

   The user heartbeat interval is set on the portal authentication server.

2. Upon receiving the synchronization packet, the access device compares the users carried in the packet with its own user list and performs the following operations:
   - If a user contained in the packet does not exist on the access device, the access device informs the portal authentication server to delete the user.
   - If the user does not appear in any synchronization packet within a synchronization detection interval, the access device determines the user does not exist on the server and logs the user out.

Portal Web server

A portal Web server pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server.

The portal authentication server and the portal Web server are usually the same device, but they can also be separate devices.

Redirection URL parameters

This feature configure the parameters to be carried in the redirection URL. Commonly required parameters include the user IP address, user MAC address, and the URL that the user originally visits.

After you configure the URL parameters, the access device sends the portal Web server URL with these parameters to portal users. Assume that the URL of a portal Web server is http://www.test.com/portal, the originally visited URL of the user whose IP address 1.1.1.1 is http://www/abc.com/welcome, and you configure the user IP address and original URL parameters. Then, the access device sends to the user whose IP address is 1.1.1.1 the URL http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome.

Portal Web server detection

A portal authentication process cannot complete if the communication between the access device and the portal Web server is broken. To address this problem, you can enable portal Web server detection on the access device.

With the portal Web server detection feature, the access device simulates a Web access process to initiate a TCP connection to the portal Web server. If the TCP connection can be established successfully, the access device considers the detection successful, and the portal Web server is reachable. Otherwise, it considers the detection to have failed. Portal authentication status on interfaces of the access device does not affect the portal Web server detection feature.

You can configure the following detection parameters:

- **Detection interval**—Interval at which the device detects the server reachability.
- **Maximum number of consecutive failures**—If the number of consecutive detection failures reaches this value, the access device considers that the portal Web server is unreachable.

You can configure the device to take one or more of the following actions when the server reachability status changes:

- Sending a trap message to the NMS. The trap message contains the name and current state of the portal Web server.
- Sending a log message, which contains the name, the current state, and the original state of the portal Web server.

Local portal Web server

Using this feature, the access device also acts as the portal Web server and the portal authentication server to perform local portal authentication on portal users. In this case, the portal system consists of only three components: authentication client, access device, and AAA server.

Client and local portal Web server interaction protocols

HTTP and HTTPS can be used for interaction between an authentication client and a local portal Web server. If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text. If HTTPS is used, secure data transmission is ensured because HTTP packets are secured by SSL.

Portal page customization

To perform local portal authentication, you must customize a set of authentication pages that the device will push to users. You can customize multiple sets of authentication pages, compress each set of the pages to a .zip file, and upload the compressed files to the storage medium of the device. On the device, you must specify one of the files as the default authentication page file.

Authentication pages are HTML files. Local portal authentication requires the following authentication pages:

- Logon page
- Logon success page
- Logon failure page
- Online page
- System busy page
- Logoff success page

You must customize the authentication pages, including the page elements that the authentication pages will use, for example, **back.jpg** for authentication page **Logon.htm**.

Follow the authentication page customization rules when you edit the authentication page files.

File name rules

The names of the main authentication page files are fixed (see Table 20). You can define the names of the files other than the main authentication page files. File names and directory names are case insensitive.

Table 20 Main authentication page file names

Main authentication page	File name
Logon page	logon.htm
Logon success page	logonSuccess.htm
Logon failure page	logonFail.htm
Online page Pushed after the user gets online for online notification	online.htm
System busy page Pushed when the system is busy or the user is in the logon process	busy.htm
Logoff success page	logoffSuccess.htm

Page request rules

The local portal Web server supports only Get and Post requests.

- **Get requests**—Used to get the static files in the authentication pages and allow no recursion. For example, if file **Logon.htm** includes contents that perform Get action on file **ca.htm**, file **ca.htm** cannot include any reference to file **Logon.htm**.
- **Post requests**—Used when users submit username and password pairs, log in, and log out.

Post request attribute rules

1. Observe the following requirements when editing a form of an authentication page:
   - An authentication page can have multiple forms, but there must be one and only one form whose action is **logon.cgi**. Otherwise, user information cannot be sent to the local portal Web server.
   - The username attribute is fixed as **PtUser**. The password attribute is fixed as **PtPwd**.
   - The value of the **PtButton** attribute is either **Logon** or **Logoff**, which indicates the action that the user requests.
   - A logon Post request must contain **PtUser**, **PtPwd**, and **PtButton** attributes.
   - A logoff Post request must contain the **PtButton** attribute.
2. Authentication pages **logon.htm** and **logonFail.htm** must contain the logon Post request.

   The following example shows part of the script in page **logon.htm**.

   ```
   <form action=logon.cgi method = post >
   <p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px"
   maxlength=64>
   <p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px"
   maxlength=32>
   <p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
   onclick="form.action=form.action+location.search;">
   </form>
   ```
3. Authentication pages **logonSuccess.htm** and **online.htm** must contain the logoff Post request.

   The following example shows part of the script in page **online.htm**.

   ```
   <form action=logon.cgi method = post >
   <p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
   </form>
   ```

Page file compression and saving rules

You must compress the authentication pages and their page elements into a standard zip file.

- The name of a zip file can contain only letters, numbers, and underscores.
- The authentication pages must be placed in the root directory of the zip file.
- Zip files can be transferred to the device through FTP or TFTP and must be saved in the root directory of the device.

  Examples of zip files on the device:

  ```
  <Sysname> dir
  Directory of flash:
     0     -rw-      1405  Feb 28 2008 15:53:31   ssid2.zip
     1     -rw-      1405  Feb 28 2008 15:53:20   ssid1.zip
     2     -rw-      1405  Feb 28 2008 15:53:39   ssid3.zip
     3     -rw-      1405  Feb 28 2008 15:53:44   ssid4.zip
  2540 KB total (1319 KB free)
  ```

Redirecting authenticated users to a specific webpage

To make the device automatically redirect authenticated users to a specific webpage, do the following in logon.htm and logonSuccess.htm:

1. In logon.htm, set the target attribute of Form to _**blank**.

   See the contents in gray:

   ```
   <form method=post action=logon.cgi target="_blank">
   ```

2. Add the function for page loading pt_init() to logonSucceess.htm.

   See the contents in gray:

   ```
   <html>
   <head>
   <title>LogonSuccessed</title>
   <script type="text/javascript" language="javascript"
   src="pt_private.js"></script>
   </head>
   <body onload="pt_init();" onbeforeunload="return pt_unload();">
   ... ...
   </body>
   </html>
   ```

Portal-free rules

A portal-free rule allows specified users to access specified external websites without portal authentication.

- IP-based portal-free rules

  The matching items for an IP-based portal-free rule include the IP address and TCP/UDP port.

- Source-based portal-free rules

  The matching items for an IP-based portal-free rule include source MAC address, access interface, and VLAN.

Packets matching a portal-free rule will not trigger portal authentication, so users sending the packets can directly access the specified external websites.

Interface policy

An interface policy is a set of portal features configured on an interface.

Portal fail-permit feature

This feature allows users on an interface to have network access without portal authentication when the access device detects that the portal authentication server or portal Web server is unreachable.

If you enable fail-permit for both a portal authentication server and a portal Web server on an interface, the interface performs the following operations:

- Disables portal authentication when either server is unreachable.
- Resumes portal authentication when both servers are reachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

BAS-IP attribute

This feature allows you to configure the BAS-IP or BAS-IPv6 attribute on a portal-enabled interface. The device uses the configured BAS-IP or BAS-IPv6 address as the source IP address of the portal notifications sent from the interface to the portal authentication server.

If you do not configure this feature, the BAS-IP/BAS-IPv6 attribute of a portal notification packet sent to the portal authentication server is the IPv4/IPv6 address of the packet output interface. The BAS-IP/BAS-IPv6 attribute of a portal reply packet is the source IPv4/IPv6 address of the packet.

User detection

This feature implements quick detection of abnormal logouts of portal users. It supports ARP or ICMP detection for IPv4 portal users and ND or ICMPv6 detection for IPv6 portal users.

ARP and ND detections apply only to direct and re-DHCP portal authentication. ICMP detection applies to all portal authentication modes.

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMP or ICMPv6 detection**—Sends ICMP or ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it determines that the user is online and stops sending detection packets. Then, the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ARP or ND detection**—Sends ARP or ND requests to the user and detects the ARP or ND entry status of the user at configurable intervals.
  - If the ARP or ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops the detection. Then the device resets the idle timer and repeats the detection process when the timer expires.
- If the ARP or ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

ISP domains

The device manages users based on ISP domains. An ISP domain includes authentication, authorization, and accounting methods for users. The device determines the ISP domain and access type of a user. It also uses the methods configured for the access type in the domain to control the user's access.

The device supports the following authentication methods:

- **No authentication**—This method trusts all users and does not perform authentication. For security purposes, do not use this method.
- **Local authentication**—The device authenticates users by itself, based on the locally configured user information including the usernames, passwords, and attributes. Local authentication allows high speed and low cost, but the amount of information that can be stored is limited by the size of the storage space.
- **Remote authentication**—The device works with a remote RADIUS server or TACACS server to authenticate users. The server manages user information in a centralized manner. Remote authentication provides high capacity, reliable, and centralized authentication services for multiple devices. You can configure backup methods to be used when the remote server is not available.

The device supports the following authorization methods:

- **No authorization**—The device performs no authorization exchange. The following default authorization information applies after users pass authentication:
  - Non-login users can access the network.
  - FTP, SFTP, and SCP users have the root directory of the device set as the working directory. However, the users do not have permission to access the root directory.

    - Other login users obtain the default user role.
- **Local authorization**—The device performs authorization according to the user attributes locally configured for users.
- **Remote authorization**—The device works with a remote RADIUS server or TACACS server to authorize users. RADIUS authorization is bound with RADIUS authentication. RADIUS authorization can work only after RADIUS authentication is successful, and the authorization information is included in the Access-Accept packet. TACACS authorization is separate from TACACS authentication, and the authorization information is included in the authorization response after successful authentication. You can configure backup methods to be used when the remote server is not available.

The device supports the following accounting methods:

- **No accounting**—The device does not perform accounting for the users.
- **Local accounting**—Local accounting is implemented on the device. It counts and controls the number of concurrent users who use the same local user account, but does not provide statistics for charging.
- **Remote accounting**—The device works with a remote RADIUS server or TACACS server for accounting. You can configure backup methods to be used when the remote server is not available.

On the device, each user belongs to one ISP domain. The device determines the ISP domain to which a user belongs based on the username entered by the user at login.

AAA manages users in the same ISP domain based on the users' access types. The device supports the following user access types:

- **LAN**—LAN users must pass 802.1X authentication to come online.
- **Login**—Login users include Telnet, FTP, and terminal users who log in to the device. Terminal users can access through a console or AUX port.
- **Portal**—Portal users.

In a networking scenario with multiple ISPs, the device can connect to users of different ISPs. The device supports multiple ISP domains, including a system-defined ISP domain named **system**. One of the ISP domains is the default domain. If a user does not provide an ISP domain name for authentication, the device considers the user belongs to the default ISP domain.

The device chooses an authentication domain for each user in the following order:

- The authentication domain specified for the access module (for example, 802.1X).
- The ISP domain in the username.
- The default ISP domain of the device.

RADIUS

RADIUS protocol

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model. The protocol can protect networks against unauthorized access and is often used in network environments that require both high security and remote user access.

The RADIUS client runs on the NASs located throughout the network. It passes user information to RADIUS servers and acts on the responses to, for example, reject or accept user access requests.

The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access.

RADIUS uses UDP to transmit packets. The RADIUS client and server exchange information with the help of shared keys.

When AAA is implemented by a remote RADIUS server, configure the RADIUS server settings on the device that acts as the NAS for the users.

Enhanced RADIUS features

The device supports the following enhanced RADIUS features:

- **Accounting-on**—This feature enables the device to automatically send an accounting-on packet to the RADIUS server after a reboot. Upon receiving the accounting-on packet, the RADIUS server logs out all online users so they can log in again through the device. Without this feature, users cannot log in again after the reboot, because the RADIUS server considers them to be online.

  You can configure the interval for which the device waits to resend the accounting-on packet and the maximum number of retries.

  The RADIUS server must run on IMC to correctly log out users when a card reboots on the distributed device to which the users connect.
- **Session-control**—A RADIUS server running on IMC can use session-control packets to inform disconnect or dynamic authorization change requests. Enable session-control on the device to receive RADIUS session-control packets on UDP port 1812.

Log features

Log levels

Logs are classified into eight severity levels from 0 through 7 in descending order.

Table 21 Log levels

Severity value	Level	Description
0	Emergency	The system is unusable. For example, the system authorization has expired.
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.
3	Error	Error condition. For example, the link state changes or a storage card is unplugged.
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.
6	Informational	Informational message. For example, a command or a ping operation is executed.
7	Debugging	Debug message.

Log destinations

The system outputs logs to destinations such as the log buffer and log host. Log output destinations are independent and you can configure them in the Web interface.

Configuration examples

Device maintenance examples

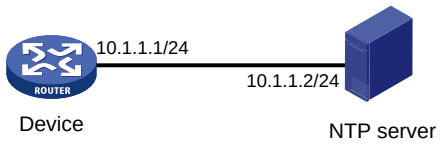
System time configuration example

Network requirements

As shown in Figure 12:

- Configure the device to obtain the UTC time from the NTP server.
- Configure NTP authentication on both the device and NTP server.

Figure 12 Network diagram



Configuration procedure

1. Configure the NTP client:
   a. From the navigation tree, select **Device** > **Maintenance** > **Settings**.
   b. Click the **Date & time** link.
   c. On the date and time settings page, perform the following tasks:
      – Select automatic time synchronization, and then select NTP.
      – Select NTP server authentication.
      – Enter the authentication key ID and the key value.
      – Enter the IP address of the NTP server, select the unicast server mode, and enter the authentication key ID.
2. Configure the NTP server:

   On the NTP server, enable the NTP service, and configure NTP authentication on the NTP server. For more information about the configuration procedure, see the NTP server documentation. (Details not shown.)

Verifying the configuration

Verify that the system clock is in synchronized state, and the device has synchronized to the NTP server. (Details not shown.)

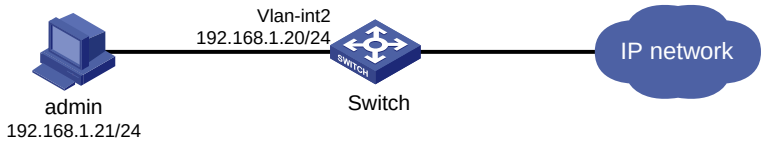
Administrators configuration example

Network requirements

As shown in Figure 13, configure an administrator account to meet the following requirements:

- Allow the user to use the account to log in to the switch through HTTP.
- Perform local authentication for the user that uses the administrator account to log in to the switch.
- Assign the network-admin user role to the authenticated user.

Figure 13 Network diagram



Configuration procedure

1. Configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **2**.
   c. Access the details page for VLAN 2 to perform the following tasks:
      – Add the interface that connects to the admin's PC to the tagged port list.
      – Create VLAN-interface **2**.
      – Assign the IP address **192.168.1.20/24** to VLAN-interface 2.
2. Configure an administrator account:
   a. From the navigation tree, select **Device** > **Maintenance** > **Administrators**.
   b. Create an administrator account:
      – Set the username and the password.
      – Select the network-admin user role.
      – Select HTTP as the permitted access type.
3. Enable the HTTP and HTTPS services:
   a. From the navigation tree, select **Network** > **Service** > **HTTP/HTTPS**.
   b. Enable the HTTP service.
   c. Enable the HTTPS service.

Verifying the configuration

1. Verify that the administrator account is successfully added. (Details not shown.)
2. Enter **http://192.168.1.20** in the address bar to verify the following items:
   ○ You can use the administrator account to log in to the Web interface.
   ○ After login, you can configure the device.

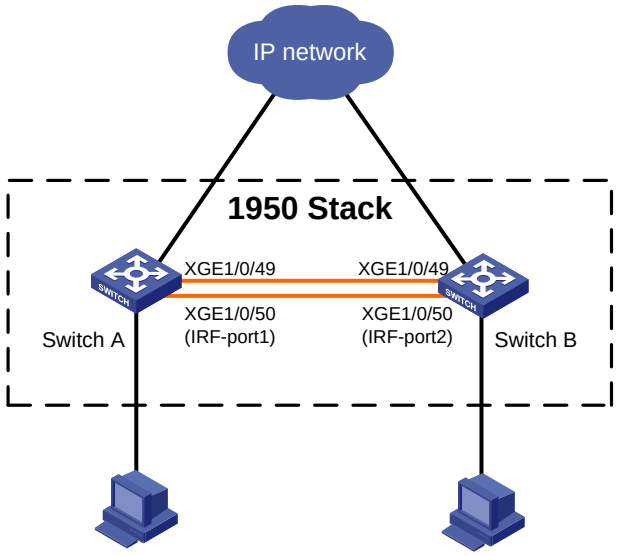
Stack configuration example

Network requirements

As shown in Figure 14, combine Switch A and Switch B into a virtual stack.

- Connect ports XGE 1/0/49 and XGE 1/0/50 on Switch A to ports XGE 1/0/49 and XGE 1/0/50 on Switch B to create stack links.
- Use Switch A as the master.

Figure 14 Network diagram



Configuration procedure

IMPORTANT:

- When you connect two neighboring stack members, you must connect the physical interfaces of IRF-port 1 on one member to the physical interfaces of IRF-port 2 on the other.
- On the webpages, stack and stacking are referred to as IRF, and stack port is referred to as IRF port.

1. Configure Switch A:
   a. From the navigation tree, select **Device** > **Virtualization** > **IRF**.
   b. Click the basic settings link, and then access the details page for member device 1 to perform the following tasks:
      – Assign a new member ID of **2** to the device.
      – Set the priority to **10**.

        For Switch A to become the master, assign it a higher priority than Switch B.
   c. Click the IRF port bindings link, and then access the details page for IRF-port 1 to assign **XGE 1/0/49** and **XGE 1/0/50** to IRF-port 1.
   d. Click the advanced link to perform the following tasks:
      – Set the domain ID to **10**.
      – If the software version is Release 3111P02, save the running configuration, and then reboot the device.

        If the software version is Release 5103P03, activate IRF port configuration, save the running the configuration, and then reboot the device.

        The new member ID takes effect after the reboot.
2. Configure Switch B:
   a. From the navigation tree, select **Device** > **Virtualization** > **IRF**.
   b. Click the basic settings link, and then access the details page for member device 1 to perform the following tasks:
      – Assign a new member ID of **3** to the device.

        The IDs of member devices must be unique.
      – Use the default priority for the device.

c. Click the IRF port bindings link, and then access the details page for IRF-port 2 to assign **XGE 1/0/49** and **XGE 1/0/50** to IRF-port 2.

d. Click the advanced link to perform the following tasks:

   – Set the domain ID to be the same as Switch A.

     The domain ID must be the same across stack member devices.

   – If the software version is Release 3111P02, save the running configuration.

     If the software version is Release 5103P03, activate IRF port configuration and save the running configuration.

3. Connect physical interfaces of IRF-port 2 on Switch B to physical interfaces of IRF-port 1 on Switch A. For more information about connecting IRF ports, see "Stack physical interfaces."

   If the software version is Release 3111P02, reboot Switch B.

   If the software version is Release 5103P03, Switch B automatically reboots to form a stack with Switch A.

Verifying the configuration

1. Log in to the Web interface of Switch A.
2. From the navigation tree, select **Device** > **Virtualization** > **IRF**.
3. Access the topology information page to verify the following items:
   - The stack contains member device 2 (Switch A) and member device 3 (Switch B).
   - The stack ports are connected.

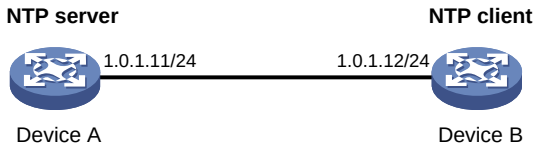
NTP configuration example

Network requirements

As shown in Figure 15:

- Configure the local clock of Device A as a reference source, with the stratum level 2.
- Set Device B to client mode and use Device A as the NTP server for Device B.

Figure 15 Network diagram



Configuration procedure

1. Configure Device A (NTP server):
   a. From the navigation tree, select **Network** > **Service** > **NTP**.
   b. Enable the NTP service.
   c. Specify the IP address of the local clock as **127.127.1.0**.
   d. Configure the stratum level of the local clock as **2**.
2. Configure Device B:
   a. From the navigation tree, select **Device** > **Maintenance** > **Settings**.
   b. Access the date and time page to select automatic time synchronization with a trusted time source, and then select NTP as the time protocol.
   c. Specify the IP address of Device A as **1.0.1.11**, and configure Device B to operate in server mode.

Verifying the configuration

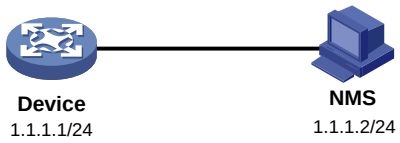
Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A. (Details not shown.)

SNMP configuration example

Network requirements

As shown in Figure 16, the NMS (1.1.1.2/24) uses SNMPv2c to manage the SNMP agent (1.1.1.1/24), and the agent automatically sends notifications to report events to the NMS.

Figure 16 Network diagram



Configuration procedure

1. Configure the device
   a. From the navigation tree, select **Network** > **Service** > **SNMP**.
   b. Click **Enable SNMP** to enable the SNMP service.
   c. Specify SNMPv2c.
   d. Create a read and write community named **readandwrite**, which can access all nodes in the default MIB view. Configure an IPv4 basic ACL to allow only the SNMPv2c NMS at 1.1.1.2/24 to use community name **readandwrite** to access the device.
   e. Enable traps, and set the destination host to 1.1.1.2, with the security string **readandwrite** and security model **v2c**.
2. Configure the SNMP NMS:
   a. Specify SNMPv2c.
   b. Create read and write community **readandwrite**.

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

Verifying the configuration

Verify that the NMS can get the value of the sysName node and can receive linkDown notifications when an interface on the device is shut down.

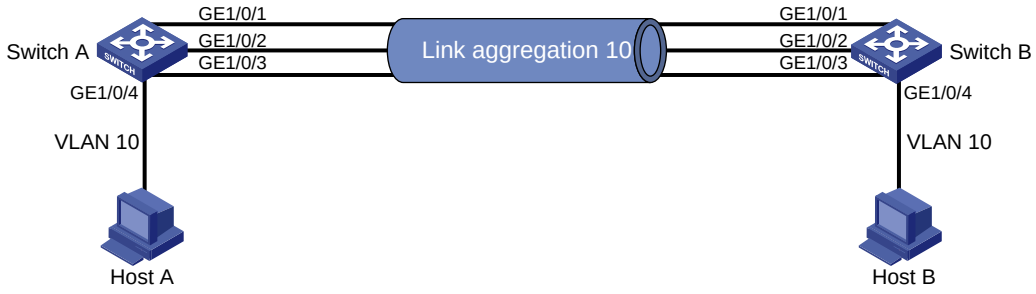
Network services configuration examples

Ethernet link aggregation configuration example

Network requirements

As shown in Figure 17, configure static Layer 2 link aggregation on Switch A and Switch B to improve the link reliability.

Figure 17 Network diagram



Configuration procedure

1. Configure Ethernet link aggregation on Switch A:
   a. From the navigation tree, select **Network** > **Interfaces** > **Link Aggregation**.
   b. Configure a Layer 2 aggregation group on Switch A as follows:
      – Configure the aggregation mode as static.
      – Assign ports to the aggregation group.
2. Configure the VLAN on Switch A.
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN 10.
   c. Access the details page for VLAN 10 to perform the following tasks:
      – Add the port that connects to Host A to the untagged port list.
      – Add ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the tagged port list.
3. Configure Switch B in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

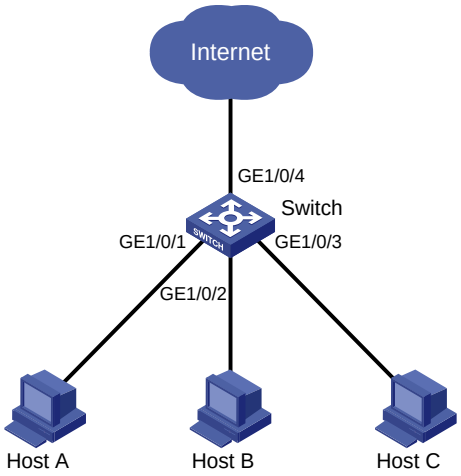
1. Access the link aggregation page, and verify that ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 have been assigned to the link aggregation group. (Details not shown.)
2. Verify that Host A can ping Host B. (Details not shown.)
3. Verify that Host A can still ping Host B after a link between Switch A and Switch B fails. (Details not shown.)

Port isolation configuration example

Network requirements

As shown in Figure 18, configure the switch to provide Internet access for all the hosts and isolate them from one another.

Figure 18 Network diagram



Configuration procedure

1. From the navigation tree, select **Network** > **Interfaces** > **Isolation**.
2. Create an isolation group.
3. Access the details page for the isolation group.
4. Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the isolation group.

Verifying the configuration

Verify that Host A, Host B, and Host C cannot ping each other. (Details not shown.)

VLAN configuration example

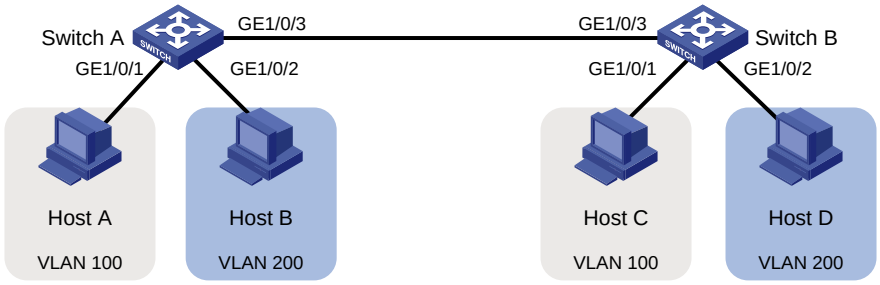
Network requirements

As shown in Figure 19:

- Host A and Host C belong to Department A. VLAN 100 is assigned to Department A.
- Host B and Host D belong to Department B. VLAN 200 is assigned to Department B.

Configure VLANs so that only hosts in the same department can communicate with each other.

Figure 19 Network diagram



Configuration procedure

1. Configure Switch A:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN 100 and VLAN 200 on Switch A.
   c. Access the details page for VLAN 100 to perform the following tasks:

- Add GigabitEthernet 1/0/1 to the untagged port list (Host A cannot recognize VLAN tags).
- Add GigabitEthernet 1/0/3 to the tagged port list (Switch B needs to identify the VLAN tags of packets).

d. Access the details page for VLAN 200 to perform the following tasks:

- Add GigabitEthernet 1/0/2 to the untagged port list (Host B cannot recognize VLAN tags).
- Add GigabitEthernet 1/0/3 to the tagged port list (Switch B needs to identify the VLAN tags of packets).

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

Verifying the configuration

1. Verify that Host A and Host C can ping each other, but neither of them can ping Host B or Host D. (Details not shown.)

2. Verify that Host B and Host D can ping each other, but neither of them can ping Host A or Host C. (Details not shown.)

Voice VLAN configuration example

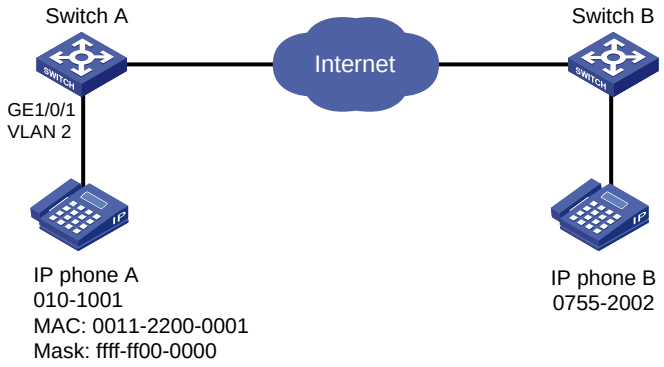
Network requirements

As shown in Figure 20, IP phone A sends and recognizes only untagged voice packets.

To enable GigabitEthernet 1/0/1 to transmit only voice packets, perform the following tasks on Switch A:

- Create VLAN 2. This VLAN will be used as a voice VLAN.
- Add GigabitEthernet 1/0/1 to VLAN 2.
- Add the OUI address of IP phone A to the OUI list of Switch A.

Figure 20 Network diagram



Configuration procedure

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

2. Set the PVID of GigabitEthernet 1/0/1 as 2.

3. From the navigation tree, select **Network** > **Links** > **VLAN**.

a. Create VLAN 2.

b. Access the details page for VLAN 2, and add GigabitEthernet 1/0/1 to the untagged port list.

4. From the navigation tree, select **Network** > **Links** > **Voice VLAN**.

a. Access the page for selecting ports, assign GigabitEthernet 1/0/1 to VLAN 2, and set the port mode to manual.

b. Access the advanced settings page, and set the mode to security.

c. Access the page for adding an OUI address, and add the OUI address **0011-2200-0000**, the mask **ffff-ff00-0000**, and the description **OUI address of IP phone A**.

Verifying the configuration

1. View the OUI summary to verify that the OUI address 0011-2200-0000 has been added.
2. View the port summary to verify that GigabitEthernet 1/0/1 has been assigned to voice VLAN 2.

MAC address entry configuration example

Network requirements

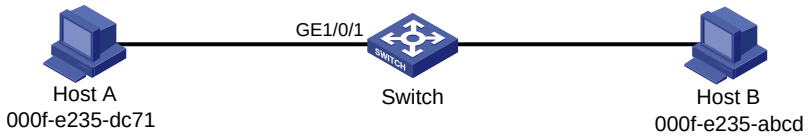
As shown in Figure 21:

- Host A at MAC address 000f-e235-dc71 is connected to GigabitEthernet 1/0/1 of the switch and belongs to VLAN 1.
- Host B at MAC address 000f-e235-abcd, which behaved suspiciously on the network, also belongs to VLAN 1.

Configure the MAC address table on the switch as follows:

- To prevent MAC address spoofing, add a static entry for Host A.
- To drop all frames destined for Host B, add a blackhole MAC address entry for Host B.
- Set the aging timer to 500 seconds for dynamic MAC address entries.

Figure 21 Network diagram



Configuration procedure

1. From the navigation tree, select **Network** > **Links** > **MAC**.
2. Add a static MAC address entry for the MAC address 000f-e235-dc71. The outgoing interface is GigabitEthernet 1/0/1, and the VLAN is 1.
3. Add a blackhole MAC address entry for the MAC address 000f-e235-abcd. The VLAN is 1.
4. Access the MAC advanced settings page, and then set the MAC aging timer to 500 seconds.

Verifying the configuration

Verify that the created MAC address entries exist in the MAC address table, and Host B cannot ping Host A. (Details not shown.)

MSTP configuration example

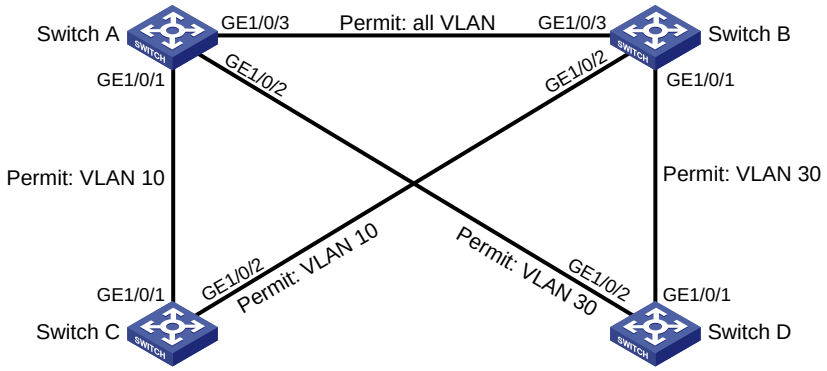
Network requirements

As shown in Figure 22, all devices in the network are in the same MST region. Switch A and Switch B work at the aggregation layer. Switch C and Switch D work at the access layer.

Configure MSTP so that packets from different VLANs are forwarded along different spanning trees.

- Packets from VLAN 10 are forwarded along MSTI 1.
- Packets from VLAN 30 are forwarded along MSTI 2.

Figure 22 Network diagram



Configuration procedure

1. Configure VLANs:
   a. Configure VLANs on Switch A:
      - From the navigation tree, select **Network** > **Links** > **VLAN**.
      - Create VLAN 10 and VLAN 30.
      - Access the details page for VLAN 10. Add ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to the tagged port list.
      - Access the details page for VLAN 30. Add ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to the tagged port list.
   b. Configure VLANs on Switch B:
      - From the navigation tree, select **Network** > **Links** > **VLAN**.
      - Create VLAN 10 and VLAN 30.
      - Access the details page for VLAN 10. Add ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to the tagged port list.
      - Access the details page for VLAN 30. Add ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to the tagged port list.
   c. Configure VLANs on Switch C:
      - From the navigation tree, select **Network** > **Links** > **VLAN**.
      - Create VLAN 10.
      - Access the details page for VLAN 10. Add ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the tagged port list.
   d. Configure VLANs on Switch D:
      - From the navigation tree, select **Network** > **Links** > **VLAN**.
      - Create VLAN 30.
      - Access the details page for VLAN 30. Add ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the tagged port list.
2. Configure MSTP on Switch A through Switch D:
   a. From the navigation tree, select **Network** > **Links** > **STP**.
   b. Enable STP, and configure the operating mode as MSTP.
   c. Access the MST region configuration page to perform the following tasks:
      - Configure the MST region name as Web.
      - Map VLAN 10 and VLAN 30 to MSTI 1 and MSTI 2, respectively.
      - Set the MSTP revision level to 0.

Verifying the configuration

Verify that the port roles and port states in the spanning tree status are as expected. (Details not shown.)

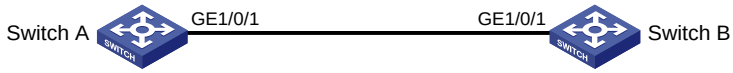
LLDP configuration example

Network requirements

As shown in Figure 23, configure LLDP on Switch A and Switch B to meet the following requirements:

- Switch A can discover Switch B and obtain system and configuration information from Switch B.
- Switch B cannot discover Switch A.

Figure 23 Network diagram



Configuration procedure

1. Configure LLDP on switch A:
   a. From the navigation tree, select **Network** > **Links** > **LLDP**.
   b. Enable LLDP globally.
   c. Access the interface status page, and enable LLDP on GigabitEthernet 1/0/1.
   d. Access the interface configuration page of advanced settings to perform the following tasks:
      – Enable the nearest bridge agent function on GigabitEthernet 1/0/1.
      – Configure the interface to only receive LLDP frames.

      Then, Switch A can discover neighbors.
2. Configure LLDP on Switch B:
   a. From the navigation tree, select **Network** > **Links** > **LLDP**.
   b. Enable LLDP globally on Switch B.
   c. Access the interface status page, and enable LLDP on GigabitEthernet 1/0/1.
   d. Access interface configuration page of advanced settings to perform the following tasks:
      – Enable the nearest bridge agent function on GigabitEthernet 1/0/1.
      – Configure the interface to only transmit LLDP frames.

      Then, Switch B cannot discover neighbors.

Verifying the configuration

1. Verify that you can see information about Switch B on the LLDP neighbor information page of Switch A. (Details not shown.)
2. Verify that the LLDP neighbor information page of Switch B does not contain an entry for Switch A. (Details not shown.)

DHCP snooping configuration example

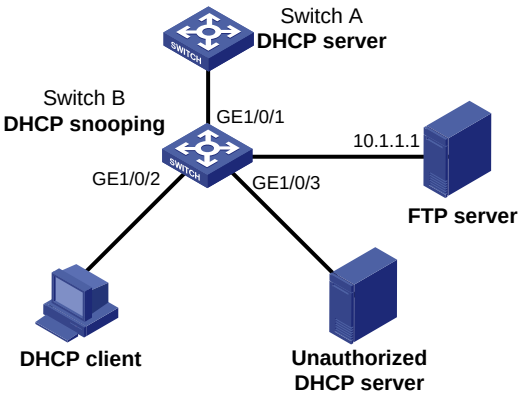
Network requirements

As shown in Figure 24, configure DHCP snooping on Switch B to meet the following requirements:

- Allow only the interface that connects to the authorized DHCP server, GigabitEthernet 1/0/1 on Switch B, can forward packets from the DHCP server.

- Record the client IP-MAC binding information in DHCP-REQUEST packets and in DHCP-ACK packets received by GigabitEthernet 1/0/1.
- Save the bindings to the FTP server.

Figure 24 Network diagram



Configuration procedure

1. Configure the DHCP server. (Details not shown.)
2. Configure the FTP server:

   Enable the FTP service, and configure the login username and password. (Details not shown.)
3. Configure the DHCP snooping device:
   a. From the navigation tree, select **Network** > **Links** > **DHCP Snooping**.
   b. Perform the following tasks:
      - Enable the DHCP snooping feature.
      - Configure GigabitEthernet 1/0/1, the interface that connects to the authorized DHCP server, as the trusted port.
      - Configure GigabitEthernet 1/0/2, the interface that connects to the client, to record DHCP snooping entries.
4. Access the advanced settings page to perform the following tasks:
   - Save the DHCP snooping entries to a remote server.
   - Specify the URL as **ftp://10.1.1.1/database.dhcp**.
   - Specify the username and password for logging into the remote server.

Verifying the configuration

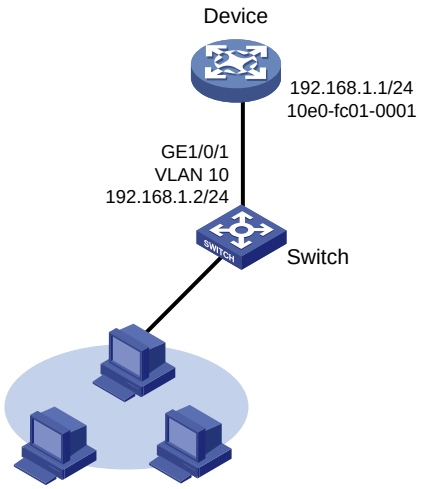
1. Verify that the DHCP client can obtain an IP address and configuration parameters only from the authorized DHCP server. (Details not shown.)
2. Verify that the DHCP snooping device records the snooping entries. (Details not shown.)
3. Verify that the DHCP database file on the FTP server saves the DHCP snooping entries. (Details not shown.)

Static ARP entry configuration example

Network requirements

As shown in Figure 25, configure a static ARP entry for the device on the switch. The static ARP entry prevents spoofing attacks to modify the IP-MAC mapping of the device.

Figure 25 Network diagram



Configuration procedure

1. Configure the VLAN and the VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.
   c. Access the details page for VLAN 10 to perform the following tasks:
      – Add GigabitEthernet 1/0/1 to the tagged port list.
      – Create VLAN-interface **10**.
      – Assign the IP address **192.168.1.2/24** to VLAN-interface 10.
2. Configure the static ARP entry:
   a. From the navigation tree, select **Network** > **IP** > **ARP**.
   b. Access the page for adding a static ARP entry to perform the following tasks:
      – Configure the IP as **192.168.1.1**.
      – Configure the MAC address as **10-e0-fc-01-00-01**.
      – Configure VLAN 10 for the entry.
      – Select GigabitEthernet 1/0/1 for the entry.

Verifying the configuration

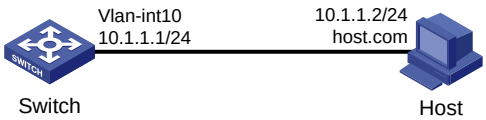
Verify that the static ARP entry is successfully added. (Details not shown.)

Static DNS configuration example

Network requirements

As shown in Figure 26, configure a static DNS entry on the device, so the device can use the domain name **host.com** to access the host at 10.1.1.2.

Figure 26 Network diagram



Configuration procedure

1. Configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.
   c. Access the details page for VLAN 10 to perform the following tasks:
      – Add GigabitEthernet 1/0/1 to the tagged port list.
      – Create VLAN-interface **10**.
      – Assign the IP address **10.1.1.1/24** to VLAN-interface 10.
2. Create a static DNS entry:
   a. From the navigation tree, select **Network** > **IP** > **DNS**.
   b. Create a static DNS entry:
      – Configure the host name as **host.com**.
      – Configure the IPv4 address as **10.1.1.2**.

Verifying the configuration

Use the **ping host.com** command on the switch to verify the following items:

- The ping operation succeeds.
- The switch can use static domain name resolution to resolve domain name **host.com** into IP address **10.1.1.2**.

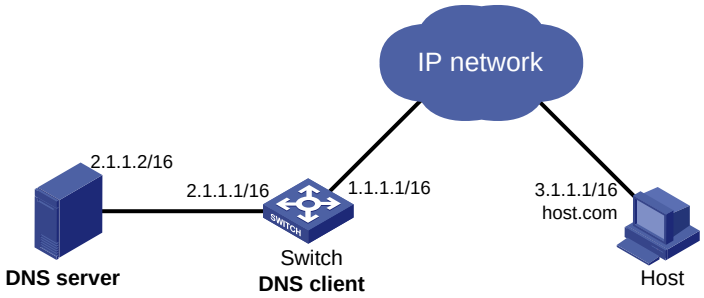
Dynamic DNS configuration example

Network requirements

As shown in Figure 27, the DNS server at 2.1.1.2/16 has a com domain that stores the mapping between domain name **host** and IP address 3.1.1.1/16.

Configure dynamic DNS and the DNS suffix com on the device that acts as a DNS client. The device can use the domain name **host** to access the host with the domain name **host.com** and the IP address 3.1.1.1/16.

Figure 27 Network diagram



Configuration procedure

1. Configure network routes:

   Configure static routes or dynamic routing protocols on each device to make sure the devices can reach each other. (Details not shown.)
2. Configure the DNS server:

   Create a mapping between **host.com** and **3.1.1.1**. (Details not shown.)
3. On the switch, configure dynamic DNS:

a. From the navigation tree, select **Network** > **IP** > **DNS**.
b. Configure the IP address of the DNS server as **2.1.1.2**.
c. On the advanced settings page, configure the domain name suffix as **com**.

Verifying the configuration

Use the **ping host** command on the switch to verify the following items:

- The ping operation succeeds.
- The switch can resolve the domain name **host.com** into the IP address **3.1.1.1**.

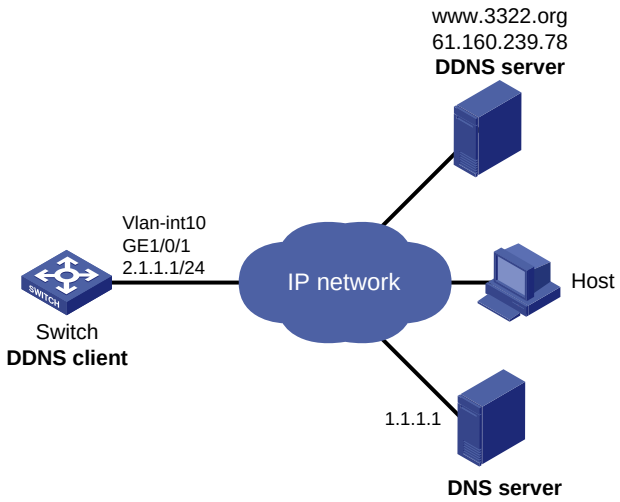
DDNS configuration example with www.3322.org

Network requirements

As shown in Figure 28, the switch is a Web server with the domain name **whatever.3322.org**.

- Configure a DDNS policy on the switch. The switch can then update its domain name-IP address mapping on the DDNS server, and the DDNS server can update the mapping on the DNS server.
- Configure DNS on the switch so that the switch can resolve **www.3322.org** into the IP address 61.160.239.78.

Figure 28 Network diagram



Configuration procedure

1. On the DDNS server, create an account:

   Access the website at **http://www.3322.org**, and set the account name to **abc** and the password to **123**. (Details not shown.)
2. On the DNS server, create the mappings between domain names and IP addresses:

   Create a mapping between **3322.org** and **61.160.239.18**, and a mapping between **whatever.3322.org** and **2.1.1.1**. (Details not shown.)
3. Configure network routes:

   Configure static routes or dynamic routing protocols on each device to make sure the devices can reach each other. (Details not shown.)
4. On the switch, configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.

c. Access the details page for VLAN 10 to perform the following tasks:
   - Add GigabitEthernet 1/0/1 to the tagged port list.
   - Create VLAN-interface **10**.
   - Assign the IP address **2.1.1.1/24** to VLAN-interface 10.

5. On the switch, configure DDNS:
   a. From the navigation tree, select **Network** > **IP** > **Dynamic DNS**.
   b. Create a DDNS policy:
      - Configure the policy name as **3322**.
      - Select the service provider **www.3322.org**.
      - Configure the username as **abc**.
      - Configure the password as **123**.
      - Configure the switch to send DDNS update requests every 15 minutes.
      - Select the associated interface VLAN-interface 10.
      - Configure the FQDN as **whatever.3322.org**.
   c. From the navigation tree, select **Network** > **IP** > **DNS**.
   d. Configure the IP address of the DNS server as **1.1.1.1**.

Verifying the configuration

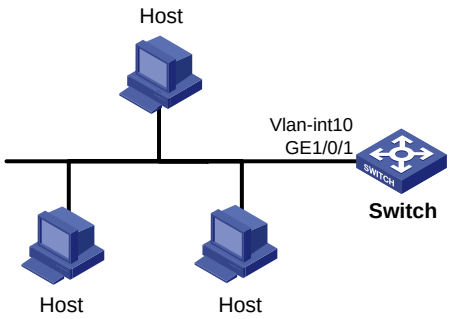
1. Change the IP address of the VLAN-interface 10 on the switch to **2.1.1.2/24**.
2. After a period, ping the domain name **whatever.3322.org** from the host to verify that the domain name is resolved to the IP address **2.1.1.2**.

Static IPv6 address configuration example

Network requirements

As shown in Figure 29, configure VLAN-interface 10 on the switch to generate an EUI-64 address with the prefix 2001::/64.

Figure 29 Network diagram



Configuration procedure

1. Configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.
   c. Access the details page for VLAN 10 to perform the following tasks:
      - Add GigabitEthernet 1/0/1 to the tagged port list.
      - Create VLAN-interface **10**.

2. Configure an IPv6 address for VLAN-interface 10:
   a. From the navigation tree, select **Network** > **IPv6** > **IPv6**.
   b. Access the details page for VLAN-interface 10 to perform the following tasks:
      – Configure the IPv6 address of the interface as **2001::**.
      – Set the prefix length to **64**.
      – Select the EUI-64 type.

Verifying the configuration

Verify that the IPv6 addresses of the VLAN-interface:

- The IPv6 global unicast address is **2001::5EDD:70FF:FEB1:86D0**.
- A link-local IPv6 address **FE80::5EDD:70FF:FEB1:86D0** is automatically generated for the interface.

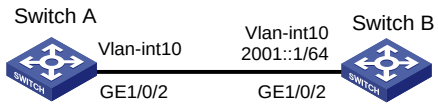
ND configuration example

Network requirements

As shown in Figure 30, configure IPv6 ND to meet the following requirements:

- VLAN-interface 10 on Switch B sends RA messages to advertise its address prefix.
- VLAN-interface 10 on Switch A generates an IPv6 global unicast addresses through stateless address autoconfiguration.

Figure 30 Network diagram



Configuration procedure

1. Configure Switch B:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.
   c. Access the details page for VLAN 10 to perform the following tasks:
      – Add GigabitEthernet 1/0/2 to the tagged port list.
      – Create VLAN-interface **10**.
      – Assign the IP address **2001::1/64** to VLAN-interface 10.
   d. From the navigation tree, select **Network** > **IPv6** > **ND**.
   e. On the advanced settings page, add an RA prefix:
      – Select the interface VLAN-interface 10.
      – Configure the prefix address as **2001::1**.
      – Set the prefix length to **64**.
      – Set the valid lifetime to **2592000** seconds.
      – Set the preferred lifetime to **604800** seconds.
      – Select the stateless autoconfiguration method.
   f. On the advanced settings page, modify the RA settings:
      – Suppress the interface from advertising RA messages.
      – Set the maximum interval to **600** seconds for sending RA messages.

- Set the minimum interval to **200** seconds for sending RA messages.
- Set the router lifetime to **1800** seconds.

2. Configure Switch A:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **10**.
   c. Access the details page for VLAN 10 to perform the following tasks:
      - Add GigabitEthernet 1/0/2 to the tagged port list.
      - Create VLAN-interface **10**.
   d. From the navigation tree, select **Network** > **IPv6** > **IPv6**.
   e. On the details page for VLAN-interface 10, configure the interface to obtain an IPv6 global unicast address through stateless autoconfiguration.

Verifying the configuration

Verify that VLAN-interface 10 of Switch A has generated an IPv6 global unicast address **2001::EDA:41FF:FE5A:2AC8**, and the address prefix is the same as that advertised by Switch B.

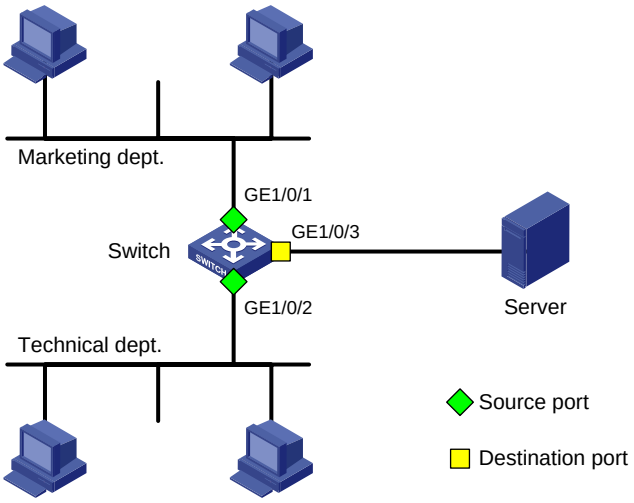
Port mirroring configuration example

Network requirements

As shown in Figure 31, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of the switch are connected to the marketing department and the technical department, respectively. The switch is connected to the server through GigabitEthernet 1/0/3.

Configure local port mirroring for the server to monitor the incoming and outgoing traffic of the two departments.

Figure 31 Network diagram



Configuration procedure

1. From the navigation tree, select **Network** > **Mirroring** > **Port Mirroring**.
2. Create a local mirroring group.
3. Configure the local port mirroring group to monitor the incoming and outgoing traffic of ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
4. Configure GigabitEthernet 1/0/3 as the destination port of the local mirroring group.

Verifying the configuration

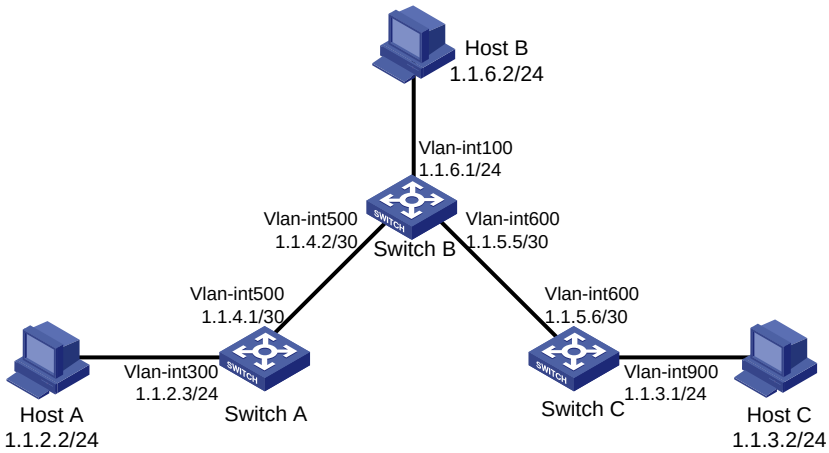
Verify that the server can monitor the incoming and outgoing traffic of the marketing department and the technical department. (Details not shown.)

IPv4 static route configuration example

Network requirements

As shown in Figure 32, configure IPv4 static routes on the switches for the hosts to communicate with each other.

Figure 32 Network diagram



Configuration procedure

In this example, Switch A is a 1950 switch.

1. On Switch A, configure a default route:
   a. From the navigation tree, select **Network** > **Routing** > **Static Routing**.
   b. Configure the route:
      – Set the destination address to **0.0.0.0**.
      – Set the mask length to **0**.
      – Set the next hop address to **1.1.4.2** (Switch B).

   NOTE:

   If the switch has only one uplink port, you only need to configure a default route that points to the upstream device.

2. On Switch B, configure static routes to reach Host A and Host C:
   a. Configure a static route to the network that contains Host A:
      – Set the destination address to **1.1.2.0**.
      – Set the mask length to **24**.
      – Set the next hop address to **1.1.4.1**.
   b. Configure a static route to the network that contains Host C:
      – Set the destination address to **1.1.3.0**.
      – Set the mask length to **24**.
      – Set the next hop address to **1.1.5.6**.

3. On Switch C, configure a default route:
   - Set the destination address to **0.0.0.0**.
   - Set the mask length to **0**.
   - Set the next hop address to **1.1.5.5** (Switch B).

Verifying the configuration

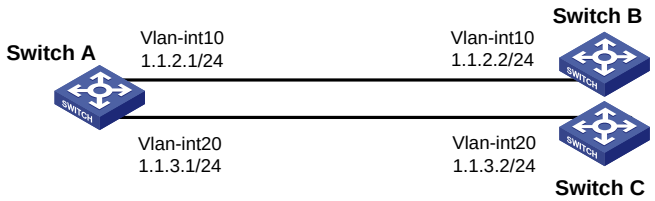
Verify that the hosts can ping each other. (Details not shown.)

IPv4 local PBR configuration example

Network requirements

As shown in Figure 33, configure PBR on Switch A to forward all TCP packets to the next hop 1.1.2.2. Switch A forwards other packets according to the routing table.

Figure 33 Network diagram



Configuration procedure

In this example, Switch A is a 1950 switch.

1. From the navigation tree, select **Network** > **Routing** > **Policy-based Routing**.
2. Click **IPv4 PBR policies**.
3. On the **New IPv4 PBR Policy** page, perform the following tasks:
   a. Enter the policy name **pbr**, and node number **5**.
   b. Set the match mode to permit.
   c. Select the IPv4 ACL match criterion.
   d. Create an IPv4 advanced ACL 3001 and configure a rule to permit TCP packets.
   e. Select IPv4 ACL 3001 as the match criterion for the policy **pbr**.
   f. Set the next hop address to 1.1.2.2 for matching packets.
4. Click **Forwarding policy of locally generated IP packets** and choose **pbr** to apply the policy to the local device.

Verifying the configuration

1. Verify that Switch A forwards TCP packets to Switch B by using PBR:
   - Telnet to Switch B from Switch A. The operation succeeds.
   - Telnet to Switch C from Switch A. The operation fails.
2. Verify that Switch A forwards other packets (ICMP packets, for example) to Switch C according to the routing table:
3. Ping Switch C from Switch A. The operation succeeds.

IGMP snooping configuration example

Network requirements

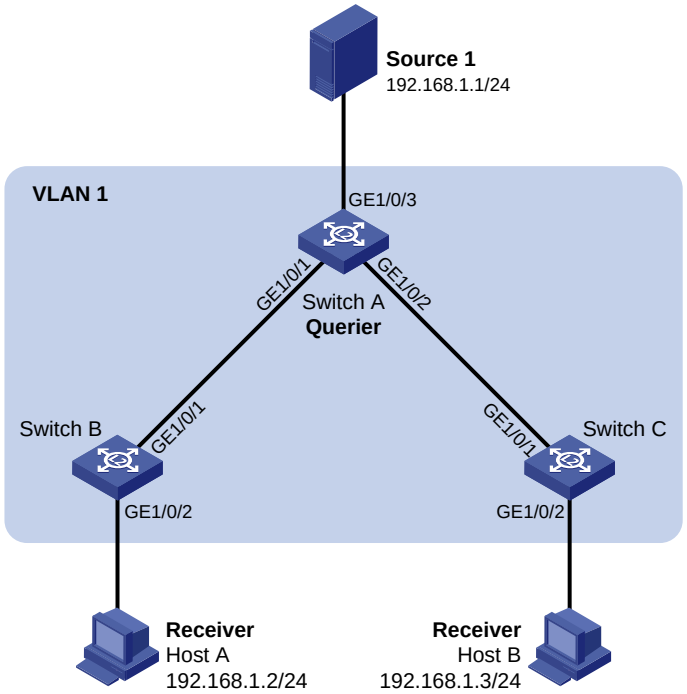
As shown in Figure 34:

- The network is a Layer 2-only network.
- Host A and Host B are receivers of multicast group 224.1.1.1.
- All host receivers run IGMPv2, and all switches run IGMPv2 snooping. Switch A (which is close to the multicast source) acts as the IGMP querier.

Configure the switches to meet the following requirements:

- To prevent the switches from flooding unknown packets in the VLAN, enable dropping unknown multicast packets on all the switches.
- A switch does not mark a port that receives an IGMP query with source IP address 0.0.0.0 as a dynamic router port. This adversely affects the establishment of Layer 2 forwarding entries and multicast traffic forwarding. To avoid this situation, configure the source IP address of IGMP queries as a non-zero IP address.

Figure 34 Network diagram



Configuration procedure

1. Configure Switch A:
   a. From the navigation tree, select **Network** > **Multicast** > **IGMP Snooping**.
   b. Enable IGMP snooping for VLAN 1.
   c. Specify the IGMP snooping version as 2.
   d. Enable dropping unknown multicast data.
   e. Enable the switch to act as the IGMP querier.
   f. Set the source IP address to 192.168.1.10 for IGMP general queries and IGMP group-specific queries.
2. Configure Switch B:
   a. From the navigation tree, select **Network** > **Multicast** > **IGMP Snooping**.
   b. Enable IGMP snooping for VLAN 1.
   c. Specify the IGMP snooping version as 2.
   d. Enable dropping unknown multicast data.
3. Configure Switch C:

a. From the navigation tree, select **Network** > **Multicast** > **IGMP Snooping**.
b. Enable IGMP snooping for VLAN 1.
c. Specify the IGMP snooping version as 2.
d. Enable dropping unknown multicast data.

Verifying the configuration

1. Send IGMP reports from Host A and Host B to join the multicast group 224.1.1.1.
2. Send multicast data from the source to the multicast group.
3. On the configuration page, click **Entries** to check that the forwarding entry for the multicast group exists.

MLD snooping configuration example

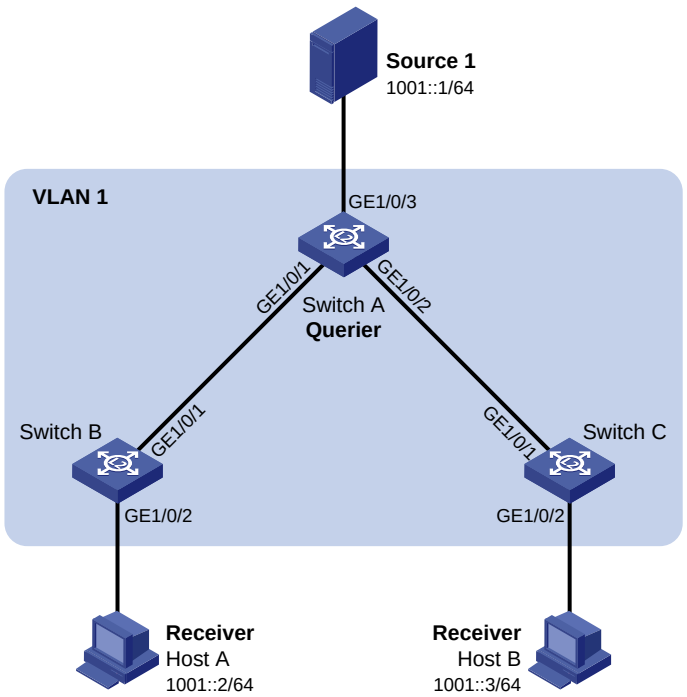
Network requirements

As shown in Figure 35:

- The network is a Layer 2-only network.
- Host A and Host B are receivers of IPv6 multicast group FF1E::101.
- All host receivers run MLDv1, and all switches run MLDv1 snooping. Switch A (which is close to the multicast source) acts as the MLD querier.

To prevent the switches from flooding unknown packets in the VLAN, enable all the switch to drop unknown IPv6 multicast packets.

Figure 35 Network diagram



Configuration procedure

1. Configure Switch A:
   a. From the navigation tree, select **Network** > **Multicast** > **MLD Snooping**.
   b. Enable MLD snooping for VLAN 1.
   c. Specify the MLD snooping version as 1.

d. Enable dropping unknown IPv6 multicast data.
e. Enable the switch to act as the MLD querier.

2. Configure Switch B:
   a. From the navigation tree, select **Network** > **Multicast** > **MLD Snooping**.
   b. Enable MLD snooping for VLAN 1.
   c. Specify the MLD snooping version as 1.
   d. Enable dropping unknown IPv6 multicast data.
3. Configure Switch C:
   a. From the navigation tree, select **Network** > **Multicast** > **MLD Snooping**.
   b. Enable MLD snooping for VLAN 1.
   c. Specify the MLD snooping version as 1.
   d. Enable dropping unknown IPv6 multicast data.

Verifying the configuration

1. Send MLD reports from Host A and Host B to join the IPv6 multicast group FF1E::101.
2. Send multicast data from the source to the IPv6 multicast group.
3. On the configuration page, click **Entries** to check that the forwarding entry for the IPv6 multicast group exists.

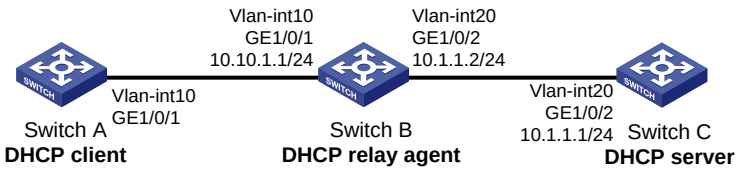
DHCP configuration example

Network requirements

As shown in Figure 36, the DHCP client and the DHCP server are on different subnets.

Configure the DHCP relay agent on switch B so that the DHCP client can obtain IP addresses through DHCP.

Figure 36 Network diagram



Configuration procedure

1. Configure the DHCP server:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **20**.
   c. Access the details page for VLAN 20 to perform the following tasks:
      – Add GigabitEthernet 1/0/2 to the tagged port list.
      – Create VLAN-interface **20**.
      – Assign the IP address **10.1.1.1/24** to VLAN-interface 20.
   d. From the navigation tree, select **Network** > **Service** > **DHCP**.
   e. On the basic setting page, perform the following tasks:
      – Enable DHCP.
      – Configure VLAN-interface 20 to operate in the DHCP server mode.
   f. Access the address pool configuration page to perform the following tasks:

- Specify the pool name as **pool1**.
- Specify the subnet as **10.10.1.0/24** for dynamic allocation.
- Specify the gateway IP address as **10.10.1.1**.

g. Access the advanced settings page to perform the following tasks:

- Configure the conflict detection feature to send a maximum of one ping packet.
- Specify the timeout time for the response as 500 milliseconds.

2. Configure the DHCP relay agent:

a. From the navigation tree, select **Network** > **Links** > **VLAN**.

b. Create VLAN **10** and VLAN **20**.

c. Access the details page for VLAN 10 to perform the following tasks:

- Add GigabitEthernet 1/0/1 to the tagged port list.
- Create VLAN-interface **10**.
- Assign the IP address **10.10.1.1/24** to VLAN-interface 10.

d. Access the details page for VLAN 20 to perform the following tasks:

- Add GigabitEthernet 1/0/2 to the tagged port list.
- Create VLAN-interface **20**.
- Assign the IP address **10.1.1.2/24** to VLAN-interface 20.

e. From the navigation tree, select **Network** > **Service** > **DHCP**.

f. Perform the following tasks:

- Enable the DHCP service.
- Configure VLAN-interface 10 to operate in DHCP relay agent mode.
- Specify the IP address of the DHCP server as **10.1.1.1**.

g. Access the advanced settings page to perform the following tasks:

- Enable the DHCP relay agent to record client information.
- Enable the relay agent to fresh relay entries periodically.
- Set the refresh internal to 100 seconds.

3. Configure the DHCP client:

a. From the navigation tree, select **Network** > **Links** > **VLAN**.

b. Create VLAN **10**.

c. Access the details page for VLAN 10 to perform the following tasks:

- Add GigabitEthernet 1/0/1 to the tagged port list.
- Create VLAN-interface **10**.

d. From the navigation tree, select **Network** > **IP** > **IP**.

e. Access the details page for VLAN-interface 10 and configure the interface to obtain an IP address through DHCP.

Verifying the configuration

1. Access the Web interface of the DHCP server to verify that an IP address has been assigned to the DHCP client. (Details not shown.)

2. Access the Web interface of the DHCP relay agent to verify that a relay entry exists for the assigned IP address. (Details not shown.)

3. On the DHCP client, verify that the client has obtained the IP address assigned by the DHCP server. (Details not shown.)

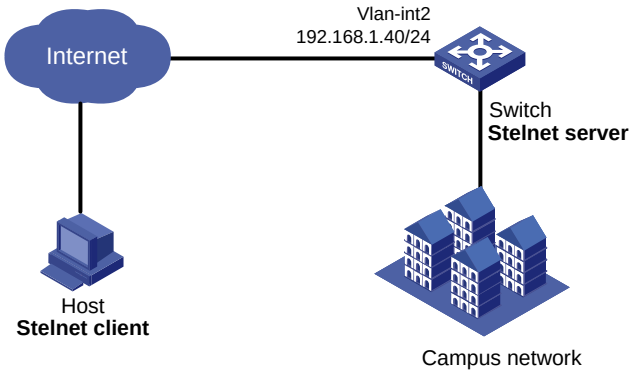
Password authentication enabled Stelnet server configuration example

Network requirements

As shown in Figure 37, the switch acts as the Stelnet server and uses password authentication. The username (**client**) and password (**aabbcc**) of the client are saved on the switch.

Establish an Stelnet connection between the host and the switch, so the client can log in to the switch to configure and manage the switch as a network administrator.

Figure 37 Network diagram



Configuration procedure

1. Configure the Stelnet server to generate RSA, DSA, and ECDSA key pairs:

From the navigation tree, select **Resources** > **Public key** > **Public key**.

2. Configure the Stelnet server feature:
   a. From the navigation tree, select **Network** > **Service** > **SSH**.
   b. Enable the Stelnet service.
3. Configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN 2.
   c. Add port GigabitEthernet 1/0/2 to the untagged port list of VLAN 2.
   d. Create VLAN-interface 2 and configure its IP address as 192.168.1.40/24.
4. Configure the Stelnet client login authentication method as **scheme**:
   a. Log in to the switch through the console port.
   b. Configure the Stelnet client login authentication method as **scheme**.
5. Configure the administrator account:
   a. From the navigation tree, select **Device** > **Maintenance** > **Administrators**.
   b. Add an administrator account.
   c. Configure the username as **client** and password as **aabbcc**.
   d. Select the user role as **network-admin**.
   e. Specify the available service as **SSH**.

Verifying the configuration

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

To establish a connection to the Stelnet server:

1. Launch PuTTY.exe to enter the interface.
2. In the **Host Name (or IP address)** field, enter the IP address **192.168.1.40** of the Stelnet server.
3. Click **Open** to connect to the server.

If the connection is successfully established, the system notifies you to enter the username and password. After entering the username (**client** in this example) and password (**aabbcc** in this example), you can enter the CLI of the switch.

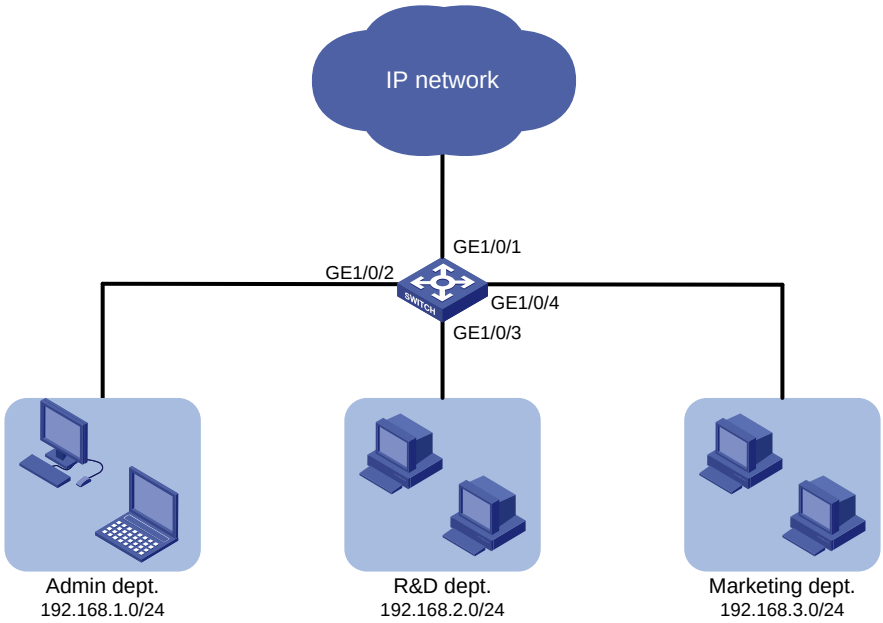
QoS configuration example

Network requirements

As shown in Figure 38, configure QoS to meet the following requirements:

- The traffic of the Administration department, R&D department, and Marketing department is scheduled in the ratio of 2:1:1.
- The rate of traffic for accessing the Internet is limited to 15 Mbps.

Figure 38 Network diagram



Configuration procedure

1. Configure QoS policies:
   a. From the navigation tree, select **QoS** > **QoS** > **QoS Policy**.
   b. Apply a QoS policy to the incoming traffic of GigabitEthernet 1/0/2.
   c. Access the details page for the QoS policy to modify the applied QoS policy as follows:
      – Create IPv4 ACL 2000, and add a rule to permit packets with source IP address 192.168.1.0 and mask 0.0.0.255.
      – Configure the ACL as a match criterion of a class, and specify the associated behavior to mark the matched packets with 802.1p priority 0.
   d. Apply a QoS policy to the incoming traffic of GigabitEthernet 1/0/3.
   e. Access the details page for the QoS policy to modify the applied QoS policy as follows:

- Create IPv4 ACL 2002, and add a rule to permit packets with source IP address 192.168.2.0 and mask 0.0.0.255.
- Configure the ACL as a match criterion of a class, and specify the associated behavior to mark the matched packets with 802.1p priority 1.

f. Apply a QoS policy to the incoming traffic of GigabitEthernet 1/0/4.

g. Access the details page for the QoS policy to modify the applied QoS policy as follows:

- Create IPv4 ACL 2003, and add a rule to permit packets with source IP address 192.168.3.0 and mask 0.0.0.255.
- Configure the ACL as a match criterion of a class, and specify the associated behavior to mark the matched packets with 802.1p priority 2.

2. Configure priority mapping:

a. From the navigation tree, select **QoS** > **QoS** > **Priority Mapping**.

b. Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to trust the 802.1p priority.

c. Configure the 802.1p-to-local priority map to map 802.1p priority values 0, 1, and 2 to local precedence values 0, 1, and 2, respectively.

3. Configure hardware queuing:

a. From the navigation tree, select **QoS** > **QoS** > **Hardware Queuing**.

b. Access the details page for GigabitEthernet 1/0/1 to perform the following tasks:

- Configure the queuing algorithm as WRR (byte-count).
- Modify the byte counts of queues 0, 1, and 2 as 2, 1, and 1, respectively.

4. Configure rate limit:

a. From the navigation tree, select **QoS** > **QoS** > **Rate Limit**.

b. Set the CIR to 15360 kbps for the incoming traffic of GigabitEthernet 1/0/1.

Verifying the configuration

Verify that the QoS application status on the QoS policy page and the queuing configuration on the hardware queuing page are as expected. (Details not shown.)

Security configuration examples

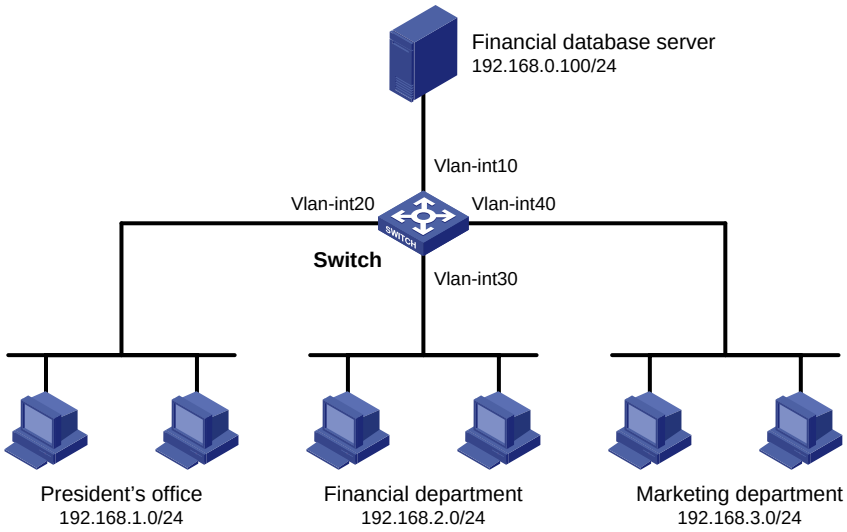
ACL-based packet filter configuration example

Network requirements

As shown in Figure 39, a company interconnects its departments through the switch.

Configure the packet filter to permit access from the Financial department to the database server only during working hours (from 8:00 to 18:00) on working days.

Figure 39 Network diagram



Configuration procedure

1. From the navigation tree, select **Security** > **Packet Filter** > **Packet Filter**.
2. Create a packet filter policy:
   a. Select VLAN-interface 30.
   b. Select the inbound application direction.
   c. Select the IPv4 ACL type for packet filter.
3. Create an advanced IPv4 ACL and configure the following rules in the order they are described:

Action	Protocol type	IP/wildcard mask	Time range
Permit	256	Source: 192.168.2.0/0.0.0.255 Destination: 192.168.0.100/0	Create a time range named **work**: • Specify the start time as **08:00**. • Specify the end time as **18:00**. • Select Monday through Friday.

4. Enable rule match counting for the ACL.

Verifying the configuration

1. You can access the server from the Financial department during the working hours.
2. Access the ACL rule Web interface, verify that the ACL rules are active. (Details not shown.)

Static IPv4 source guard configuration example

Network requirements

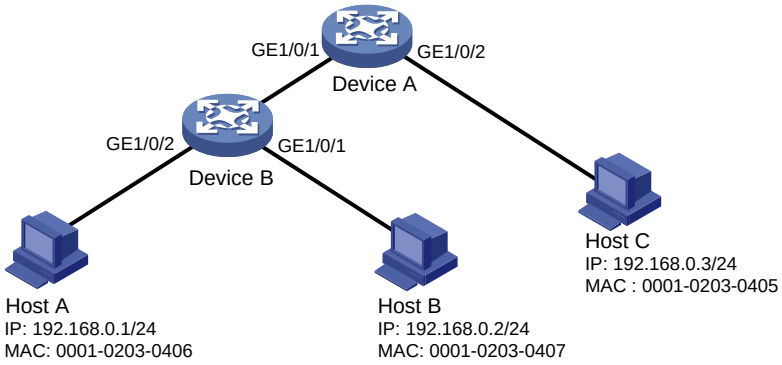
As shown in Figure 40, all hosts use static IP addresses.

Configure static IPv4 source guard entries on Device A and Device B to meet the following requirements:

- GigabitEthernet 1/0/2 of Device A allows only IP packets from Host C to pass.

- GigabitEthernet 1/0/1 of Device A allows only IP packets from Host A to pass.
- GigabitEthernet 1/0/2 of Device B allow only IP packets from Host A to pass.
- GigabitEthernet 1/0/1 of Device B allows only IP packets from Host B to pass.

Figure 40 Network diagram



Configuration procedure

1. Configure Device A:
   a. Configure IP addresses for the interfaces. (Details not shown.)
   b. From the navigation tree, select **Security** > **Packet Filter** > **IP Source Guard**.
   c. Add an IP source guard entry for Host A.

      The entry contains interface GigabitEthernet 1/0/1, IP address 192.168.0.1, and MAC address 00-01-02-03-04-06.
   d. Add an IP source guard entry for Host C.

      The entry contains interface GigabitEthernet 1/0/2, IP address 192.168.0.3, and MAC address 00-01-02-03-04-05.
2. Configure Device B:
   a. Configure IP addresses for the interfaces. (Details not shown.)
   b. From the navigation tree, select **Security** > **Packet Filter** > **IP Source Guard**.
   c. Add an IP source guard entry for Host B.

      The entry contains interface GigabitEthernet 1/0/1, IP address 192.168.0.2, and MAC address 00-01-02-03-04-07.
   d. Add an IP source guard entry for Host A.

      The entry contains interface GigabitEthernet 1/0/2, IP address 192.168.0.1, and MAC address 00-01-02-03-04-06.

Verifying the configuration

1. From the navigation tree, select **Security** > **Packet Filter** > **IP Source Guard** on Device A.
2. Verify that the static IPv4 source guard entries are configured successfully on the IP source guard configuration page.
3. Repeat step 1 and 2 on Device B to verify that the static IPv4 source guard entries are configured successfully.

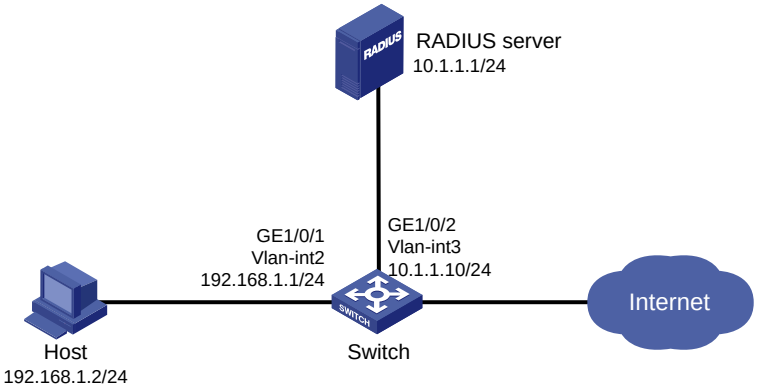
802.1X RADIUS authentication configuration example

Network requirements

As shown in Figure 41, configure the switch to meet the following requirements:

- Use the RADIUS server to perform authentication, authorization, and accounting for 802.1X users.
- Authenticate all 802.1X users who access the switch through GigabitEthernet 1/0/1 in ISP domain **dm1X**.
- Use MAC-based access control on GigabitEthernet 1/0/1 to authenticate all 802.1X users on the port separately.
- Exclude domain names from the usernames sent to the RADIUS server.
- Use **name** as the authentication and accounting shared keys for secure RADIUS communication between the switch and the RADIUS server.
- Use ports **1812** and **1813** for authentication and accounting, respectively.

Figure 41 Network diagram



Configuration procedure

1. Configure IP addresses for the interfaces, as shown in Figure 38. (Details not shown.)
2. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **802.1X**.
   c. Configure the primary authentication server:
      – Set the IP address to **10.1.1.1**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **name**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **10.1.1.1**.
      – Set the accounting port number to **1813**.
      – Set the shared key to **name**.
      – Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
3. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **dm1X**, and set the domain state to **Active**.
   c. Set the access service to LAN access.
   d. Configure the ISP domain to use RADIUS scheme **802.1X** for authentication, authorization, and accounting of LAN users.

4. Configure 802.1X on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **802.1X**.
   b. Enable 802.1X globally.
   c. Enable 802.1X on GigabitEthernet 1/0/1, and set the access control method to MAC-based.
   d. On the advanced settings page for GigabitEthernet 1/0/1, set the port authorization state to **Auto** and set the mandatory ISP domain to **dm1X**.
5. Configure the RADIUS server:
   a. # Add a user account on the server. (Details not shown.)
   b. # Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **802.1X**. (Details not shown.)
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **dm1X**. (Details not shown.)
5. Use the configured user account to pass authentication.
6. From the navigation tree, select **Security** > **Access Control** > **802.1X**.
7. Verify that the number of online users is not **0** on GigabitEthernet 1/0/1. (Details not shown.)

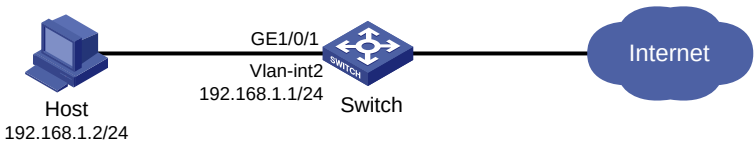
802.1X local authentication configuration example

Network requirements

As shown in Figure 42, add a user account with username **dotuser** and password **12345** on the switch. Configure the switch to meet the following requirements:

- Perform local 802.1X authentication to control the network access of users on GigabitEthernet 1/0/1.
- Authenticate the users in ISP domain **abc**.
- Specify port-based access control on GigabitEthernet 1/0/1. After a user passes authentication on the port, all subsequent users can access the network without authentication.

Figure 42 Network diagram



Configuration procedure

1. Configure IP addresses for the interfaces, as shown in Figure 42. (Details not shown.)
2. Configure the local user account:
   a. From the navigation tree, select **Security** > **Authentication** > **Local Users**.
   b. Add user account **dotuser** and set the password to **12345**.
   c. Set the service type to LAN access.
3. Configure the ISP domain:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **abc** and set the state to **Active**.
   c. Set the access service to LAN access.

d. Configure the ISP domain to use local method for authentication and authorization of LAN users, and not perform accounting for LAN users.

4. Configure 802.1X:
   a. From the navigation tree, select **Security** > **Access Control** > **802.1X**.
   b. Enable 802.1X globally.
   c. Enable 802.1X on GigabitEthernet 1/0/1, and set the access control method to port-based.
   d. On the advanced settings page for GigabitEthernet 1/0/1, set the port authorization state to **Auto** and set the mandatory ISP domain to **abc**.

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **Local Users**.
2. Verify the configuration of local user **dotuser**. (Details not shown.)
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **abc**. (Details not shown.)
5. Use the user account **dotuser** and password **12345** to pass authentication.
6. From the navigation tree, select **Security** > **Access Control** > **802.1X**.
7. Verify that the number of online users is not **0** on GigabitEthernet 1/0/1. (Details not shown.)

RADIUS-based MAC authentication configuration example

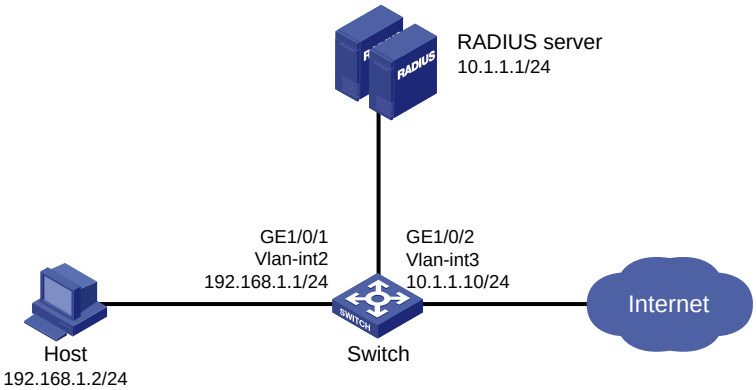
Network requirements

As shown in Figure 43, the switch uses MAC authentication to control Internet access of users on GigabitEthernet 1/0/1.

Configure the switch to meet the following requirements:

- Use the RADIUS server to perform authentication, authorization, and accounting for all users.
- Authenticate all users in ISP domain **macauth**.
- Use an account with username **aaa** and password **qaz123wdc** to identify all users.
- Exclude domain names from the usernames sent to the RADIUS server.
- Use **name** as the authentication and accounting shared keys for secure RADIUS communication between the switch and the RADIUS server.
- Use ports **1812** and **1813** for authentication and accounting, respectively.

Figure 43 Network diagram



Configuration procedure

1. Configure IP addresses for the interfaces, as shown in Figure 43. (Details not shown.)

2. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **macauth**.
   c. Configure the primary authentication server:
      - Set the IP address to **10.1.1.1**.
      - Set the authentication port number to **1812**.
      - Set the shared key to **name**.
      - Set the server state to **Active**.
   d. Configure the primary accounting server:
      - Set the IP address to **10.1.1.1**.
      - Set the accounting port number to **1813**.
      - Set the shared key to **name**.
      - Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
3. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **macauth**, and set the domain state to **Active**.
   c. Set the access service to LAN access.
   d. Configure the ISP domain to use RADIUS scheme **macauth** for authentication, authorization, and accounting of LAN users.
4. Configure MAC authentication on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **MAC Authentication**.
   b. Enable MAC authentication globally.
   c. Enable MAC authentication on GigabitEthernet 1/0/1.
   d. On the advanced settings page, configure the following parameters:
      - Set all users to use the same username and password.
      - Configure the username as **aaa** and password as **qaz123wdc**.
      - Specify the authentication domain as **macauth**.
5. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **macauth**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **macauth**.
5. Use the user account **aaa** and password **qaz123wdc** to pass MAC authentication.
6. From the navigation tree, select **Security** > **Access Control** > **MAC Authentication**.
7. Verify that the number of online users is not **0** on GigabitEthernet 1/0/1.

RADIUS-based port security configuration example

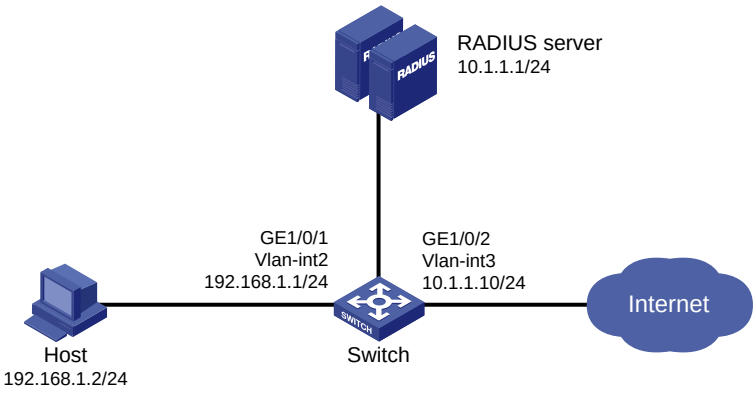
Network requirements

As shown in Figure 44, GigabitEthernet 1/0/1 operates in userLoginWithOUI mode to control Internet access of users.

Configure the switch to meet the following requirements:

- Use the RADIUS server to perform authentication, authorization, and accounting for users.
- Use **name** as the authentication and accounting shared keys for secure RADIUS communication between the switch and the RADIUS server.
- Use ports **1812** and **1813** for authentication and accounting, respectively.
- Authenticate all 802.1X users in ISP domain **portsec**, and exclude domain names from the usernames sent to the RADIUS server.
- Allow only one 802.1X user and one user whose OUI matches one of the following OUIs to come online on GigabitEthernet 1/0/1:
  - 1234-0100-1111
  - 1234-0200-1111
  - 1234-0300-1111
  - 1234-0400-1111
  - 1234-0500-1111

Figure 44 Network diagram



Configuration procedure

1. Configure IP addresses for the interfaces, as shown in Figure 44. (Details not shown.)
2. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **portsec**.
   c. Configure the primary authentication server:
      – Set the IP address to **10.1.1.1**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **name**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **10.1.1.1**.
      – Set the accounting port number to **1813**.

- Set the shared key to **name**.
- Set the server state to **Active**.

e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.

3. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **portsec**, and set the domain state to **Active**.
   c. Set the access service to LAN access.
   d. Configure the ISP domain to use RADIUS scheme **portsec** for authentication, authorization, and accounting of LAN users.
4. Configure port security on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **Port Security**.
   b. Enable port security.
   c. On the advanced settings page for GigabitEthernet 1/0/1, set the port security mode to **userLoginWithOUI**.
   d. On the 802.1X tab of the advanced settings page for GigabitEthernet 1/0/1, set the 802.1X mandatory domain to **portsec**.
   e. On the advanced settings page for port security, add five OUI values to the OUI list. The OUI values include 1234-0100-1111, 1234-0200-1111, 1234-0300-1111, 1234-0400-1111, and 1234-0500-1111.
5. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **portsec**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **portsec**.
5. Use the configured user account to pass authentication.
6. From the navigation tree, select **Security** > **Access Control** > **Port Security**.
7. Verify that the number of online users is not **0** on GigabitEthernet 1/0/1.

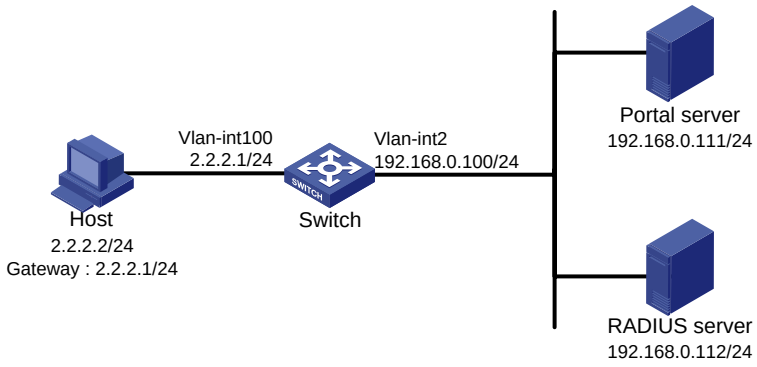
Direct portal authentication configuration example

Network requirements

As shown in Figure 45, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication, so the host can access only the portal server before passing the authentication and access other network resources after passing the authentication.

Figure 45 Network diagram



Configuration procedure

1. Configure the portal server. (Details not shown.)
2. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **rs1**.
   c. Configure the primary authentication server:
      – Set the IP address to **192.168.0.112**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **192.168.0.112**.
      – Set the accounting port number to **1813**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
   f. Click the **Advanced settings** icon on the **RADIUS** page.
   g. Enable the session-control feature.
3. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **dm1**, and set the domain state to **Active**.
   c. Set the access service to **Portal**.
   d. Configure the ISP domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting of portal users.
   e. Click the **Advanced settings** icon on the **ISP Domain** page.
   f. Specify **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
4. Configure the VLAN and the VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **100**.

c. Open the details page for VLAN 100.
d. Create VLAN-interface 100 and assign IP address **2.2.2.1** to it.

5. Configure portal authentication on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **Portal**.
   b. Add a portal authentication server:
      - Specify the server name as **newpt**.
      - Specify the IP address as **192.168.0.111**.
      - Specify the shared key as **portal**.
      - Set the server listening port to **50100**.
   c. Add a portal Web server:
      - Specify the server name as **newpt**.
      - Specify the URL.

        The URL must be the same as the URL of the portal Web server used in the network. This example uses **http://192.168.0.111:8080/portal**.
   d. Add an interface policy:
      - Select interface VLAN-interface 100.
      - In the IPv4 configuration area, enable portal authentication and select the **Direct** method.
      - Select portal Web server **newpt**.
      - Configure the BAS-IP address as **2.2.2.1**.
6. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **rs1**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **dm1**.
5. Use the configured user account to pass portal authentication.
6. From the navigation tree, select **Security** > **Access Control** > **Portal**.
7. Verify that the number of online users is not 0 on VLAN-interface 100.

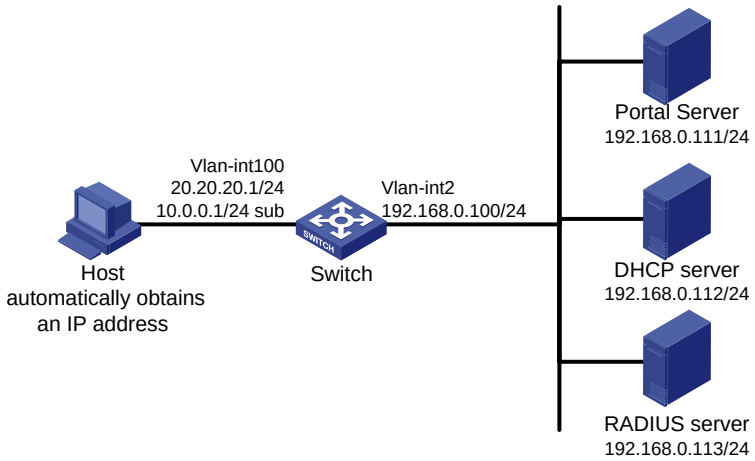
Re-DHCP portal authentication configuration example

Network requirements

As shown in Figure 46, the host is directly connected to the switch (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure re-DHCP portal authentication. Before passing the authentication, the host is assigned a private IP address. After passing the authentication, the host gets a public IP address and can access network resources.

Figure 46 Network diagram



Configuration procedure

1. Configure the portal server. (Details not shown.)
2. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **rs1**.
   c. Configure the primary authentication server:
      – Set the IP address to **192.168.0.113**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **192.168.0.113**.
      – Set the accounting port number to **1813**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
   f. Click the **Advanced settings** icon on the **RADIUS** page.
   g. Enable the session-control feature.
3. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **dm1**, and set the domain state to **Active**.
   c. Set the access service to **Portal**.
   d. Configure the ISP domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting of portal users.
   e. Click the **Advanced settings** icon on the **ISP Domain** page.
   f. Specify **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
4. Configure the VLAN and the VLAN interface:

a. From the navigation tree, select **Network** > **Links** > **VLAN**.
b. Create VLAN **100**.
c. Open the details page for VLAN 100.
d. Create VLAN-interface 100.
e. Configure the primary IP address as **20.20.20.1** and secondary IP address as **10.0.0.1** for the VLAN interface.

5. Configure DHCP relay on the switch:
   a. From the navigation tree, select **Network** > **Service** > **DHCP**.
   b. Click **Enable DHCP**.
   c. Create VLAN-interface 100 to operate in **DHCP relay agent** mode.
   d. Configure the IP address of the DHCP server as **192.168.0.112**.
   e. Open the DHCP server advanced settings page and enable the **Record DHCP relay client information** feature.
6. Configure authorized ARP on the switch:
   a. From the navigation tree, select **Network** > **IP** > **ARP**.
   b. Open the advanced settings page.
   c. Open the ARP attack protection page.
   d. Enable authorized ARP on VLAN-interface 100.
7. Configure portal authentication on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **Portal**.
   b. Add a portal authentication server:
      - Specify the server name as **newpt**.
      - Specify the IP address as **192.168.0.111**.
      - Specify the shared key as **portal**.
      - Set the server listening port to **50100**.
   c. Add a portal Web server:
      - Specify the server name as **newpt**.
      - Specify the URL.

        The URL must be the same as the URL of the portal Web server used in the network. This example uses **http://192.168.0.111:8080/portal**.
   d. Add an interface policy:
      - Select interface VLAN-interface 100.
      - In the IPv4 configuration area, enable portal authentication and select the **Redhcp** method.
      - Select portal Web server **newpt**.
      - Configure the BAS-IP address as **20.20.20.1**.
8. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **rs1**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **dm1**.

5. Use the configured user account to pass portal authentication.
6. From the navigation tree, select **Security** > **Access Control** > **Portal**.
7. Verify that the number of online users is not 0 on VLAN-interface 100.

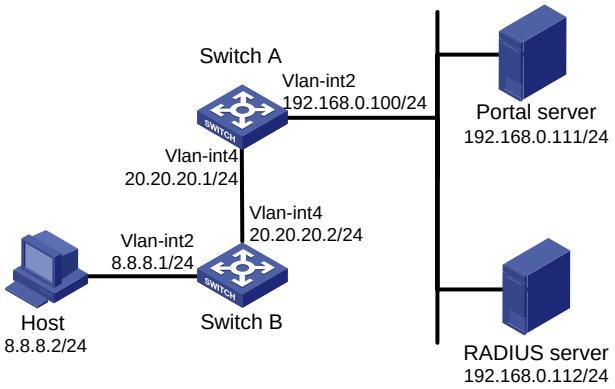
Cross-subnet portal authentication configuration example

Network requirements

As shown in Figure 47, Switch A supports portal authentication. The host accesses Switch A through Switch B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Switch A for cross-subnet portal authentication. Before passing the authentication, the host can access only the portal Web server. After passing the authentication, the user can access other network resources.

Figure 47 Network diagram



Configuration procedure

1. Configure the portal server. (Details not shown.)
2. Configure a RADIUS scheme on Switch A:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **rs1**.
   c. Configure the primary authentication server:
      – Set the IP address to **192.168.0.112**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **192.168.0.112**.
      – Set the accounting port number to **1813**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
   f. Click the **Advanced settings** icon on the **RADIUS** page.
   g. Enable the session-control feature.

3. Configure an ISP domain on Switch A:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **dm1**, and set the domain state to **Active**.
   c. Set the access service to **Portal**.
   d. Configure the ISP domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting of portal users.
   e. Click the **Advanced settings** icon on the **ISP Domain** page.
   f. Specify **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
4. Configure the VLAN and the VLAN interface on Switch A:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **4**.
   c. Open the details page for VLAN 4.
   d. Create VLAN-interface 4 and assign IP address **20.20.20.1** to it.
5. Configure portal authentication on Switch A:
   a. From the navigation tree, select **Security** > **Access Control** > **Portal**.
   b. Add a portal authentication server:
      - Specify the server name as **newpt**.
      - Specify the IP address as **192.168.0.111**.
      - Specify the shared key as **portal**.
      - Set the server listening port to **50100**.
   c. Add a portal Web server:
      - Specify the server name as **newpt**.
      - Specify the URL.

        The URL must be the same as the URL of the portal Web server used in the network. This example uses **http://192.168.0.111:8080/portal**.
   d. Add an interface policy:
      - Select interface VLAN-interface 4.
      - In the IPv4 configuration area, enable portal authentication and select the **Layer3** method.
      - Select portal Web server **newpt**.
      - Configure the BAS-IP address as **20.20.20.1**.
6. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **rs1**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **dm1**.
5. Use the configured user account to pass portal authentication.
6. From the navigation tree, select **Security** > **Access Control** > **Portal**.
7. Verify that the number of online users is not 0 on VLAN-interface 4.

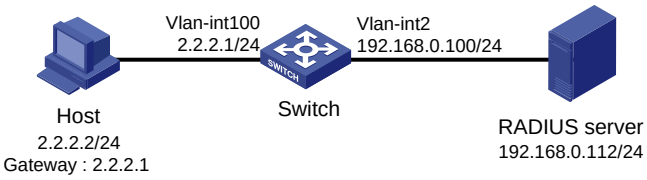
Direct portal authentication using local portal Web server configuration example

Network requirements

As shown in Figure 48, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. The switch acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the switch. Before a user passes portal authentication, the user can access only the local portal Web server. After passing portal authentication, the user can access other network resources.

Figure 48 Network diagram



Configuration procedure

1. Configure a RADIUS scheme on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
   b. Add RADIUS scheme **rs1**.
   c. Configure the primary authentication server:
      – Set the IP address to **192.168.0.112**.
      – Set the authentication port number to **1812**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   d. Configure the primary accounting server:
      – Set the IP address to **192.168.0.112**.
      – Set the accounting port number to **1813**.
      – Set the shared key to **radius**.
      – Set the server state to **Active**.
   e. Configure the switch to not include domain names in the usernames sent to the RADIUS server.
   f. Click the **Advanced settings** icon on the **RADIUS** page.
   g. Enable the session-control feature.
2. Configure an ISP domain on the switch:
   a. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
   b. Add ISP domain **dm1**, and set the domain state to **Active**.
   c. Set the access service to **Portal**.
   d. Configure the ISP domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting of portal users.
   e. Click the **Advanced settings** icon on the **ISP Domain** page.

f. Specify **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

3. Configure the VLAN and the VLAN interface on Switch A:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN **100**.
   c. Open the details page for VLAN 100.
   d. Create VLAN-interface 100 and assign IP address **2.2.2.1** to it.
4. Configure portal authentication on the switch:
   a. From the navigation tree, select **Security** > **Access Control** > **Portal**.
   b. Add a portal Web server:
      – Specify the server name as **newpt**.
      – Specify the URL as **http://2.2.2.1:2331/portal**.

        The URL can be the IP address of the interface enabled with portal authentication or a loopback interface's address other than 127.0.0.1.
   c. Add a local portal Web server:
      – Select **HTTP**.
      – Select the default logon page **abc.zip**.

        The default logon page file must have existed in the root directory of the switch's storage medium.
      – Set the TCP port to **2331**.
   d. Add an interface policy:
      – Select interface VLAN-interface 100.
      – In the IPv4 configuration area, enable portal authentication and select the **Direct** method.
      – Select portal Web server **newpt**.
5. Configure the RADIUS server:
   a. Add a user account on the server. (Details not shown.)
   b. Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. From the navigation tree, select **Security** > **Authentication** > **RADIUS**.
2. Verify the configuration of RADIUS scheme **rs1**.
3. From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
4. Verify the configuration of ISP domain **dm1**.
5. Use the configured user account to pass portal authentication.
6. From the navigation tree, select **Security** > **Access Control** > **Portal**.
7. Verify that the number of online users is not 0 on VLAN-interface 100.

AAA for SSH users by a TACACS server configuration example

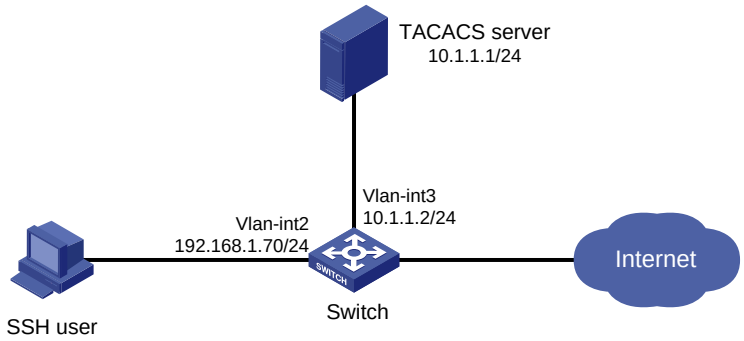
Network requirements

As shown in Figure 49, configure the switch to meet the following requirements:

- Use the TACACS server for SSH user authentication, authorization, and accounting.

- Assign the default user role **network-admin** to SSH users after they pass authentication.
- Exclude domain names from the usernames sent to the TACACS server.
- Use **expert** as the shared keys for secure TACACS communication.

Figure 49 Network diagram



Configuration procedure

1. Configure the Stelnet server to generate local key pairs for SSH:
   a. From the navigation tree, select **Resources** > **Public key** > **Public key**.
   b. Add local DSA, ECDSA, and RSA key pairs.
2. Configure the SSH server:
   a. From the navigation tree, select **Network** > **Service** > **SSH**.
   b. Enable the Stelnet service.
3. Configure the VLAN and VLAN interface:
   a. From the navigation tree, select **Network** > **Links** > **VLAN**.
   b. Create VLAN 2.
   c. Access the details page for VLAN 2 to perform the following tasks:
      – Add interface GigabitEthernet 1/0/2 to the tagged port list.
      – Create VLAN-interface 2.
      – Assign IP address 192.168.1.70/24 to VLAN-interface 2.
      – Configure a TACACS scheme on the switch:
      – From the navigation tree, select **Security** > **Authentication** > **TACACS**.
      – Add TACACS scheme **tac**.
      – Configure the primary authentication, authorization, and accounting servers:
      – Set the IP address to **10.1.1.1**.
      – Set the port number to **49**.
      – Set the shared key to **expert**.
      – In advanced settings, configure the switch to exclude domain names in the user names sent to the TACACS server.
      – Configure an ISP domain on the switch:
      – From the navigation tree, select **Security** > **Authentication** > **ISP Domains**.
      – Add ISP domain **bbb** and set the domain state to **Active**.
      – Select **Login** as the service type.
      – Configure the ISP domain to use TACACS scheme **tac** for authentication, authorization, and accounting of login users.
      – Configure the user lines for the Stelnet client:

- Log in to the switch through the console port.
- Set the login authentication mode to scheme. (Details not shown.)
- Configure the TACACS server:
- Add a user account on the server. (Details not shown.)
- Configure the authentication, authorization, and accounting settings. (Details not shown.)
- Configure the user role feature to assign authenticated SSH users the network-admin user role. (Details not shown.)
- Verifying the configuration
- Initiate an SSH connection to the switch and enter the correct username and password. The user logs in to the switch.
- Verify that the user can use the commands permitted by the network-admin user role.

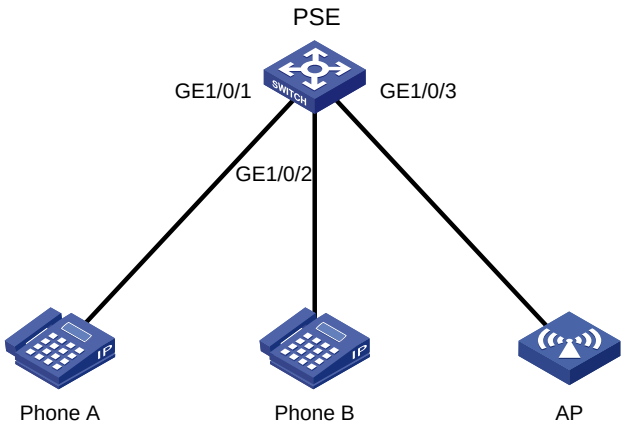
PoE configuration example

Network requirements

As shown in Figure 50, configure PoE to meet the following requirements:

- Enable the device to supply power to IP telephones and the AP.
- Enable the device to supply power to IP telephones first when overload occurs.
- Allocate AP a maximum power of 9000 milliwatts.

Figure 50 Network diagram



Configuration procedure

1. From the navigation tree, select **PoE** > **PoE**.
2. Enable PoE for GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, set the power supply priority to critical.
3. Enable PoE for GigabitEthernet 1/0/3 and set the maximum PoE power for the interface to 9000 milliwatts.

Appendix A Managing the device from the CLI

Commands are available for you to perform basic device management when the Web interface is not available.

To manage the device from the CLI, access the device through the console port or Telnet. You are placed in user view immediately after you log in to the CLI.

Table 22 provides a command summary. All these commands are available in user view. However, the commands you can use depend on the user roles you have. By default, a command is available for the predefined user roles. You can use the RBAC feature to assign a command to additional user roles from the Web interface.

Table 22 Command summary

Command	Description
display poe pse [*pse-id*]	Display PSE information.
initialize	Initializes the device.
ipsetup dhcp	Enables VLAN-interface 1 to obtain an IPv4 address from a DHCP server.
ipsetup ip-address *ip-address* { *mask-length* | *mask* } [**default-gateway** *ipv4-gateway-address*]	Assigns an IPv4 address to VLAN-interface 1.
ipsetup ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } [**default-gateway** *ipv6-gateway-address*]	Assigns an IPv6 global unicast address to VLAN-interface 1.
ipsetup ipv6 auto	Enables VLAN-interface 1 to obtain an IPv6 global unicast address through stateless autoconfiguration.
password	Modifies the login password for a user.
ping *host*	Identifies whether the destination IPv4 address is reachable and display related statistics.
ping ipv6 *host*	Identifies whether the destination IPv6 address is reachable and display related statistics.
poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]	Upgrade a PSE firmware when the device is operating.
quit	Logs out of the system.
reboot [**slot** *slot-number*] [**force**]	Reboots stack member devices.
summary	Displays summary information for the device.
telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]	Telnets to a host in an IPv4 network.
telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*]	Telnets to a host in an IPv6 network.
transceiver phony-alarm-disable **undo transceiver phony-alarm-disable**	Disables transceiver module source alarm. Restores the default. These commands are not available in Release 3111P02.

Command	Description
upgrade { *tftp-server* | **ipv6** *ipv6-tftp-server* } **bootrom** *bootrom-filename* **upgrade** { *tftp-server* | **ipv6** *ipv6-tftp-server* } **runtime boot** *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] **upgrade** { *tftp-server* | **ipv6** *ipv6-tftp-server* } **runtime file** *ipe-filename*	Downloads the specified file from a TFTP server and specify the file as the file to be used at the next startup. If the device is a stack member device, the setting of this command applies to all member devices in the stack.
xtd-cli-mode **undo xtd-cli-mode**	Switches to extended CLI mode. Extended CLI is for the use of Hewlett Packard Enterprise support personnel when troubleshooting an issue. This is not a supported feature for operation in customer networks. Restores the default.

display poe pse

Use **display poe pse** to display PSE information.

Syntax

display poe pse [*pse-id*]

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

pse-id: Specifies a PSE by its ID.

Usage guidelines

If you do not specify a PSE, this command displays information about all PSEs.

Examples

Display detailed information about PSE 7.

```
<Sysname> display poe pse 7
 PSE ID                              : 7
 Slot No.                           : 1
 SSlot No.                          : 0
 PSE Model                          : LSP7POEB
 PSE Status                         : Enabled
 Power Priority                     : Low
 Current Power                      : 0.0      W
 Average Power                      : 0.0      W
 Peak Power                         : 0.0      W
 Max Power                          : 370.0    W
 Remaining Guaranteed Power       : 370.0    W
 PSE CPLD Version                   : -
 PSE Software Version              : 130
```

```
PSE Hardware Version              : 57633
Legacy PD Detection               : Disabled
Power Utilization Threshold      : 80
PD Power Policy                    : Disabled
PD Disconnect-Detection Mode     : AC
```

Table 23 Command output

Field	Description
PSE ID	ID of the PSE.
Slot No.	Slot number of the PSE.
SSlot No.	Subslot number of the PSE.
PSE Status	PoE status of the PSE: • **Enabled.** • **Disabled**.
Power Priority	Power priority of the PSE.
Current Power	Current power of the PSE.
Average Power	Average power of the PSE.
Peak Power	Peak power of the PSE.
Max Power	Maximum power of the PSE.
Remaining Guaranteed Power	Remaining guaranteed power of the PSE = Maximum guaranteed power of the PSE – Total maximum power of all critical PIs of the PSE.
PSE CPLD Version	PSE CPLD version number.
PSE Software Version	PSE software version number.
PSE Hardware Version	PSE hardware version number.
Legacy PD Detection	Nonstandard PD detection status: • **Enabled.** • **Disabled**.
Power Utilization Threshold	PSE power alarm threshold.
PD Power Policy	PD power management policy mode.
PD Disconnect Detection Mode	PD disconnection detection mode.

initialize

Use **initialize** to initialize the device.

Syntax

initialize

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command deletes the next-startup configuration file from the storage medium, and then reboots the device with the factory-default configuration.

Make sure you understand the impact on the network when you use this command.

Examples

Initialize the device.

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

ipsetup dhcp

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

Syntax

ipsetup dhcp

Default

No IPv4 address for VLAN-interface 1 can be obtained through DHCP.

Views

User view

Predefined user roles

network-admin

Usage guidelines

You can use either of the following methods to assign an IPv4 address to VLAN-interface 1:

- **DHCP**—VLAN-interface 1 acts as a DHCP client to dynamically obtain an IPv4 address from the DHCP server.
- **Manual**—Allows you to use the **ipsetup ip address** command to assign an IPv4 address to this interface.

Whichever method is used, the newly obtained IPv4 address overwrites the existing IPv4 address.

Examples

Configure VLAN-interface 1 to obtain an IPv4 address through DHCP.

```
<Sysname> ipsetup dhcp
```

Related commands

ipsetup ip address

ipsetup ip address

Use **ipsetup ip address** to assign an IPv4 address to VLAN-interface 1.

Syntax

ipsetup ip-address *ip-address* { *mask-length* | *mask* } [**default-gateway** *ipv4-gateway-address*]

Default

No IPv4 address is assigned to VLAN-interface 1.

Views

User view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IPv4 address for the interface, in dotted decimal notation.

mask-length: Specifies the subnet mask length, the number of consecutive 1s in the mask. The value range for this argument is 1 to 31.

mask: Specifies the subnet mask in dotted decimal notation.

default-gateway *ipv4-gateway-address*: Specifies the IPv4 address of the default gateway, in dotted decimal notation. If you specify this option, the command not only assigns an IPv4 gateway address to the interface, but also specifies a default route for the device. For this option to take effect, make sure the *ipv4-gateway-address* setting is in the same segment with the *ip-address* setting.

Usage guidelines

You can use either of the following methods to assign an IPv4 address to VLAN-interface 1:

- **DHCP**—VLAN-interface 1 acts as a DHCP client to dynamically obtain an IPv4 address from the DHCP server.
- **Manual**—Allows you to use the **ipsetup ip address** command to assign an IPv4 address to this interface.

Whichever method is used, the newly obtained IPv4 address overwrites the existing IPv4 address.

Examples

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
```

Related commands

ipsetup dhcp

ipsetup ipv6 address

Use **ipsetup ip address** to assign an IPv6 global unicast address to VLAN-interface 1.

Syntax

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

Default

No IPv6 global unicast address is assigned to VLAN-interface 1.

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 global unicast address for the interface.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 1 to 128.

default-gateway *ipv6-gateway-address*: Specifies the IPv6 address of the default gateway. If you specify this option, the command not only assigns an IPv6 gateway address to the interface, but also specifies a default route for the device. For this option to take effect, make sure the *ipv6-gateway-address* setting is in the same segment with the *ipv6-address* setting.

Usage guidelines

You can use either of the following methods to assign an IPv6 global unicast address to VLAN-interface 1:

- **Auto**—Automatically generates an IPv6 global unicast address through stateless autoconfiguration by using the **ipsetup ipv6 auto** command.
- **Manual**—Allows you to use the **ipsetup ipv6 address** command to assign an IPv6 global unicast address to this interface.

Whichever method is used, the newly obtained IPv6 address overwrites the existing IPv6 address.

Examples

Assign 2::2 with prefix length 64 to VLAN-interface 1, and specify 2::3 as the default gateway.

```
<Sysname> ipsetup ipv6 address 2::2 64 default-gateway 2::3
```

Related commands

ipsetup ipv6 auto

ipsetup ipv6 auto

Use **ipsetup ipv6 auto** to configure VLAN-interface 1 to obtain an IPv6 global unicast address through stateless autoconfiguration.

Syntax

ipsetup ipv6 auto

Default

No IPv6 global unicast address can be obtained for VLAN-interface 1 through stateless autoconfiguration.

Views

User view

Predefined user roles

network-admin

Usage guidelines

You can use either of the following methods to assign an IPv6 global unicast address to VLAN-interface 1:

- **Auto**—Automatically generates an IPv6 global unicast address through stateless autoconfiguration by using the **ipsetup ipv6 auto** command.
- **Manual**—Allows you to use the **ipsetup ipv6 address** command to assign an IPv6 global unicast address to this interface.

Whichever method is used, the newly obtained IPv6 address overwrites the existing IPv6 address.

Examples

Configure VLAN-interface 1 to obtain an IPv6 global unicast address through stateless autoconfiguration.

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

Related commands

ipsetup ipv6 address

password

Use **password** to modify the login password for a user.

Syntax

password

Views

User view

Predefined user roles

network-admin

Examples

Modify the login password for user **aaa**.

```
<Sysname> password
Change password for user: aaa
Old password:
Enter new password:
Confirm:
The password has been successfully changed.
```

ping

Use **ping** to identify whether the destination IPv4 address is reachable and display related statistics.

Syntax

ping *host*

Views

User view

Predefined user roles

network-admin

Parameters

host: Specifies the destination IPv4 address or host name. The host name must be a case-insensitive string of 1 to 253 characters that can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

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 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
```

```
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 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, maximum, and standard deviation roundtrip intervals are 1.963 millisecond, 2.028 milliseconds, 2.137 milliseconds, and 0.062 milliseconds, respectively.

ping ipv6

Use **ping ipv6** to identify whether the destination IPv6 address is reachable and display related statistics.

Syntax

ping ipv6 *host*

Views

User view

Predefined user roles

network-admin

Parameters

host: Specifies the destination IPv6 address or host name. The host name must be a case-insensitive string of 1 to 253 characters that can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

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

Examples

Ping IPv6 address 2001::2.

```
<Sysname> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

The output shows that IPv6 address 2001::2 is reachable and the echo replies are all returned from the destination. The minimum, average, maximum, and standard deviation round trip intervals are 4 milliseconds , 25 milliseconds, 62 milliseconds, and 20 milliseconds, respectively.

poe update

Use **poe update** to upgrade a PSE firmware when the device is operating.

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

Views

User view

Predefined user roles

network-admin

Parameters

full: Upgrades the PSE firmware in full mode.

refresh: Upgrades the PSE firmware in refresh mode.

filename: Specifies the name of the upgrade file, a case-sensitive string of 1 to 64 characters. The specified file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

You can upgrade the PSE firmware in service in either of the following modes:

- **Refresh mode**—Updates the PSE firmware without deleting it. You can use the refresh mode in most cases.
- **Full mode**—Deletes the current PSE firmware and reloads a new one. Use the full mode if the PSE firmware is damaged and you cannot execute any PoE commands.

Examples

Upgrade the firmware of PSE 7 in service.

```
<Sysname> poe update refresh POE-168.bin pse 7
```

quit

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

Syntax

quit

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Executing this command in user view disconnects you from the device.

Examples

Log out of the system.

```
<Sysname> quit
```

reboot

Use **reboot** to reboot stack member devices.

Syntax

reboot [**slot** *slot-number*] [**force**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a stack member device by its member ID. If you do not specify a member ID, this command reboots all member devices in the stack.

force: Reboots the device immediately without performing software or hard disk check. If you do not specify this keyword, the system first examines whether the reboot might result in data loss or a system failure. For example, the system examines whether the main system software image file exists and whether a write operation is in progress on a storage medium. If the reboot might cause these problems, the system does not reboot the device.

Usage guidelines

Use the command with caution because a device reboot might interrupt network services.

If the main startup software images are corrupted or missing, the device cannot be rebooted with the **reboot** command. Specify a new main configuration file to reboot the device.

For data security, the device does not reboot if you reboot the device while the device is performing file operations.

Use the **force** keyword only when the device fails or a **reboot** command without the **force** keyword cannot perform a reboot task correctly. A **reboot** command with the **force** keyword might result in file system corruption because it does not perform data protection.

Examples

Reboot all stack member devices.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration may be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Reboot the device immediately without performing software check.

```
<Sysname> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

summary

Use **summary** to display summary information for the device.

Syntax

summary

Views

User view

Predefined user roles

network-admin

Usage guidelines

The summary information includes the following items:

- IP address of VLAN-interface 1.
- Network management information.
- Device version.
- Software version information.
- Startup software images.

Examples

Display summary information for the device.

```
<Sysname> summary
Select menu option:             Summary
IP Method:                      Manual
IP address:                     192.168.1.82
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:

Software images on slot 1:
Current software images:
  flash:/1950-cmw710-boot-r3111p02.bin
  flash:/1950-cmw710-system-r3111p02.bin
Main startup software images:
  flash:/1950-cmw710-boot-r3111p02.bin
  flash:/1950-cmw710-system-r3111p02.bin
Backup startup software images:
  flash:/1950-cmw710-boot-a0007-ft.bin
  flash:/1950-cmw710-system-a0007-ft.bin
  flash:/1950-cmw710-manufacture-a0007-ft.bin

HPE Comware Platform Software
HPE Comware Software, Version 7.1.045, Release 3111P02
Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP
HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ uptime is 0 weeks, 0 days, 0 hours, 1
```

```
0 minutes



Slot 1:
Uptime is 0 weeks,0 days,0 hours,10 minutes
HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ JG962A with 1 Processor
BOARD TYPE:         1950-24G-2SFP+-2XGT-PoE+
DRAM:               1024M bytes
FLASH:              512M bytes
PCB 1 Version:      VER.B
Bootrom Version:    142
CPLD 1 Version:     001
Release Version:    HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ JG962A-3111P02
Patch Version  :    None
Reboot Cause   :    UserReboot
[SubSlot 0] 24GE+2SFP-Plus+2XGT
```

telnet

Use **telnet** to Telnet to a host in an IPv4 network.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters that can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535, and the default is 23.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets. If you do not specify this keyword, the command uses the primary IPv4 address of the routing outbound interface as the source IPv4 address for outgoing Telnet packets.

interface *interface-type interface-number*: Specifies the source interface by its type and number. 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.

Usage guidelines

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

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

Use **telnet ipv6** to Telnet to a host in an IPv6 network.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv6 address or host name of a remote host. A host name is a case-insensitive string of 1 to 253 characters that can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

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

port-number: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535, and the default is 23.

Usage guidelines

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
```

transceiver phony-alarm-disable

Use **transceiver phony-alarm-disable** to disable transceiver module source alarm.

Use **undo transceiver phony-alarm-disable** to enable transceiver module source alarm.

Syntax

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Default

Transceiver module source alarm is disabled.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command is not available in Release 3111P02.

The device regularly checks transceiver modules for their vendor names. If a transceiver module does not have a vendor name or the vendor name is not HPE, the device repeatedly outputs traps and log messages.

Transceiver module source alarm is disabled by default. If you want to view the traps and log messages, execute the **undo transceiver phony-alarm-disable** command.

Examples

Disable transceiver module source alarm.

```
<Sysname> system-view
[Sysname] transceiver phony-alarm-disable
```

upgrade

Use **upgrade** to download the specified file from a TFTP server and specify the file as the file to be used at the next startup. If the device is a stack member, the setting of this command applies to all member devices in the stack.

Syntax

upgrade { *tftp-server* | **ipv6** *ipv6-tftp-server* } **bootrom** *bootrom-filename*

upgrade { *tftp-server* | **ipv6** *ipv6-tftp-server* } **runtime boot** *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>]

upgrade { *tftp-server* | **ipv6** *ipv6-tftp-server* } **runtime file** *ipe-filename*

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IP address or host name for a TFTP server. The host name is a string of 1 to 253 characters.

ipv6-address: Specifies the IPv6 address or host name for a TFTP server. The host name is a string of 1 to 253 characters.

bootrom *bootrom-filename*: Specifies the Boot ROM file in the software image to be used at the next startup.

runtime: Specifies the Comware image file to be used at the next startup.

boot *boot-package*: Specifies the file path of a .bin boot image file, a case-insensitive string. The file must be stored in the root directory of a storage medium in the system. The value range is 1 to 63 characters for the storage-medium:/base-filename.bin segments of the file path. This length limit does not include the stack member ID or slot number in front of the storage medium segment.

system *system-package*: Specifies the file path of a .bin system image file, a case-insensitive string. The file must be stored in the root directory of a storage medium in the system. The value range is 1 to 63 characters for the storage-medium:/base-filename.bin segments of the file path. This length limit does not include the stack member ID or slot number in front of the storage medium segment.

feature *feature-package*: Specifies a space-separated list of up to 30 .bin feature image file paths. The file paths are case insensitive. The files must be stored in the root directory of a storage medium in the system. The value range is 1 to 63 characters for the storage-medium:/base-filename.bin segments of a file path. This length limit does not include the stack member ID or slot number in front of the storage medium segment.

file *ipe-filename*: Specifies the file path of an .ipe image file, a case-insensitive string. The file must be stored in the root directory of a storage medium in the system. The value range is 1 to 63 characters for the storage-medium:/base-filename.ipe segments of the file path. This length limit does not include the stack member ID or slot number in front of the storage medium segment.

Usage guidelines

For the system to operate correctly, you must specify Boot ROM image, boot image, and system image. You can specify feature images as needed. Boot images, system images, and feature images are all Comware images.

Comware images can be released separately as a .bin file or as a whole in one .ipe package file. If a .ipe file is used, the system automatically decompresses the file into multiple .bin files and uses them to upgrade the device.

For the downloaded image to take effect, reboot the device.

After you execute the **upgrade runtime** command, the system replaces the existing software images with the specified images. If you do not specify a feature image, no feature image will be included in the software image list.

When an .ipe image package file is used for upgrade, you must choose whether to delete the file after the system decompresses the file.

Examples

Download file **bootrom.bin** from the root directory of the TFTP server and use the Boot ROM file at the next startup.

```
<Sysname> upgrade 192.168.8.2 bootrom bootrom.bin
The file flash:/bootrom.bin already exists.Overwrite?[Y/N]y
Verifying server file...
Downloading file boot.bin from remote TFTP server, please
wait.............................................................. Done.
This command will upgrade the Boot ROM file on the specified board(s), Continue?
 [Y/N]:y
Now Upgrade the Boot ROM of slot 1, please wait.........................Done.
```

Download file **all.ipe** from the root directory of the TFTP server and use the .ipe file at the next startup.

```
<Sysname> upgrade 192.168.8.2 runtime file all.ipe
The file flash:/all.ipe already exists.Overwrite?[Y/N]y
Verifying server file...
Downloading file all.ipe from remote TFTP server, please
wait.....................................................................Done.
Verifying the file flash:/all.ipe on slot 1..................Done.
HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file boot.bin to flash:/ boot.bin...................Done.
Decompressing file system.bin to
flash:/system.bin.....................................................Do
ne.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
Decompression completed.
```

```
Do you want to delete flash:/all.ipe now? [Y/N]:y
```

Download files **boot.bin** and **system.bin** from the root directory of the TFTP server and use these files at the next startup.

```
<Sysname>upgrade 192.168.8.2 runtime boot boot.bin system system.bin
The file flash:/boot.bin already exists.Overwrite?[Y/N]y
Verifying server file...
Downloading file boot.bin from remote TFTP server, please
wait.....................................Done.
The file flash:/system.bin already exists.Overwrite?[Y/N]y
Verifying server file...
Downloading file system.bin from remote TFTP server, please
wait.....................Done.
This command will set the main startup software images. Continue? [Y/N]:y
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

xtd-cli-mode

Use **xtd-cli-mode** to switch to extended CLI mode.

Use **undo xtd-cli-mode** to restore the default.

Syntax

xtd-cli-mode

undo xtd-cli-mode

Default

You can display and execute part of the commands on the device.

Views

User view

Predefined user roles

network-admin

Usage guidelines

Extended CLI is for the use of Hewlett Packard Enterprise support personnel when troubleshooting an issue. This is not a supported feature for operation in customer networks.

You enter extended CLI mode after executing this command and entering a correct password. In extended CLI mode, you can execute all commands on the device.

This command takes effect only on the current login. It restores to the default setting after you log in to the device again.

Examples

Switch to extended CLI mode.

```
<Sysname> xtd-cli-mode
All commands can be displayed and executed in extended CLI mode. Switch to extended CLI
mode? [Y/N]: y
Password:
```

Warning: Extended CLI mode is intended for developers to test the system. Before using commands in extended CLI mode, contact the Technical Support and make sure you know the potential impact on the device and the network.

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

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 appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.

Convention	Description
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 card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

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

E

M

Q

T