

INTELBRAS WC 7060 Series Access Controllers

Web-Based Configuration Guide

INTELBRAS.
<http://www.intelbras.com.br>

Product version: E5457

Preface

The *INTELBRAS WC 7060 Series Access Controllers Web-Based Configuration Guide* describes the web functions of the INTELBRAS Access Controllers.

This preface includes the following topics about the documentation:

- [Audience.](#)
- [Conventions.](#)

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the INTELBRAS access controllers.

Conventions

The following information describes the conventions used in the documentation.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> 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 a minimum of one.
[x y ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.













GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window opens; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Logging in to the Web interface	2
Restrictions and guidelines	2
Web browser requirements	2
Default login settings	2
Concurrent login users	2
Logging in to the Web interface for the first time	3
Logging out of the Web interface	4

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 the following Web browsers:

- Internet Explorer 10 or higher.
- Mozilla Firefox 30.0.0.5269 or higher
- Google Chrome 35.0.1916.114 or higher.
- Safari 6.0 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 settings in [Table 1](#) for the first login.

Table 1 Default login settings

Item	Setting
Device IP (VLAN-interface 1)	192.168.0.100
IP address mask	255.255.0.0
Username	admin
Password	admin
User role	network-admin

Concurrent login users

The Web interface allows a maximum of 64 concurrent accesses. If this limit is reached, login attempts will fail.

Logging in to the Web interface for the first time



IMPORTANT:

For security purposes, change the login information and assign access permissions immediately after the first successful login.

NOTE:

- VLAN-interface 1 in the factory default configuration of the device obtains an IP address through DHCP. If the interface obtains an IP address through DHCP successfully, you must assign the login host an IP address in the same subnet as the interface. If the interface fails to obtain an IP address through DHCP, the interface uses default address 192.168.0.100.
- To obtain the current IP address of the device, log in to the device through the console, and then execute the **display interface vlan-interface 1** command.
- To view the factory default settings of the device, execute the **display default-configuration** command.

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. Assign the login host an IP address in the same subnet as the device.
3. Open the browser, and then enter login information:
 - a. In the address bar, enter the IP address of the device.
 - **HTTP access**—Enter `http://ip-address:80`.
 - **HTTPS access**—Enter `https://ip-address:443`.

ip-address is the IP address of the device. 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 default password (**admin**).
 - c. Click **Login**, change the login password as prompted on the page that opens, and then click **OK**.
4. Change the login information:
 - To change the IP address of the device, perform the following tasks:
 - Click the system view tab at the bottom of the page.
 - From the navigation tree, select **Network Configuration > Network Services > IP Services**. You are placed on the **IP** tab.
 - To change the password of the login user (**admin** at the first login) or add new administrator accounts, perform the following tasks:
 - Click the system view tab at the bottom of the page.
 - From the navigation tree, select **System > Administrators** to access the administrator configuration page.

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 directly closing the browser.
- Devices do 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.

To log out of the Web interface:

1. Use one of the following methods to save the current configuration:

Method 1:

Click **Save** in the upper right corner of the Web interface.

Method 2:

- a. Click the system view tab at the bottom of the page, select **System > Management** from the navigation tree.
 - b. Click the **Configuration** tab to access the configuration page.
 - c. Click **Save Running Configuration**.
2. Click the **admin** icon, and then click **Logout**.

Contents

Using the Web interface	1
Types of webpages	2
Using a feature page	2
Using a table page	2
Using a configuration page	3
Icons and buttons	3
Performing basic tasks	5
Saving the configuration	5
Displaying settings of a table entry	5
Rebooting the device	5

Using the Web interface

As shown in [Figure 1](#), the Web interface contains the following areas:


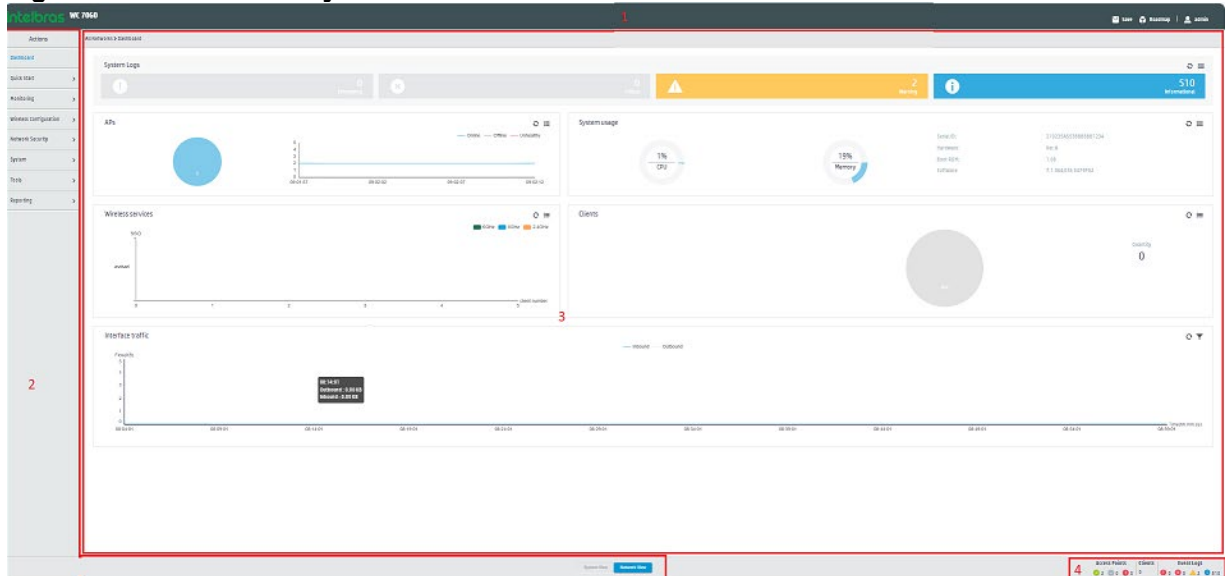
Area	Description
(1) Banner and auxiliary area	<p>Contains the following items:</p> <ul style="list-style-type: none"> The INTELBRAS logo. Device model. Icon for saving the current settings. Icon for displaying the roadmap. Admin icon  admin—Click this icon to select a language, change the login password, log out, or use the scan to follow feature.
(2) Navigation tree	Organizes feature menus in a tree in system view or in network view.
(3) Content pane	<p>Displays information and provides an area for you to configure features. Depending on the content in this pane, the webpages include the following types:</p> <ul style="list-style-type: none"> 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").
(4) Status area	Displays device status and statistics.

Figure 1 Web interface layout



- | | |
|------------------------------|---|
| 1) Banner and auxiliary area | 2) Navigation tree (in system view or network view) |
| 3) Content pane | 4) Status area |

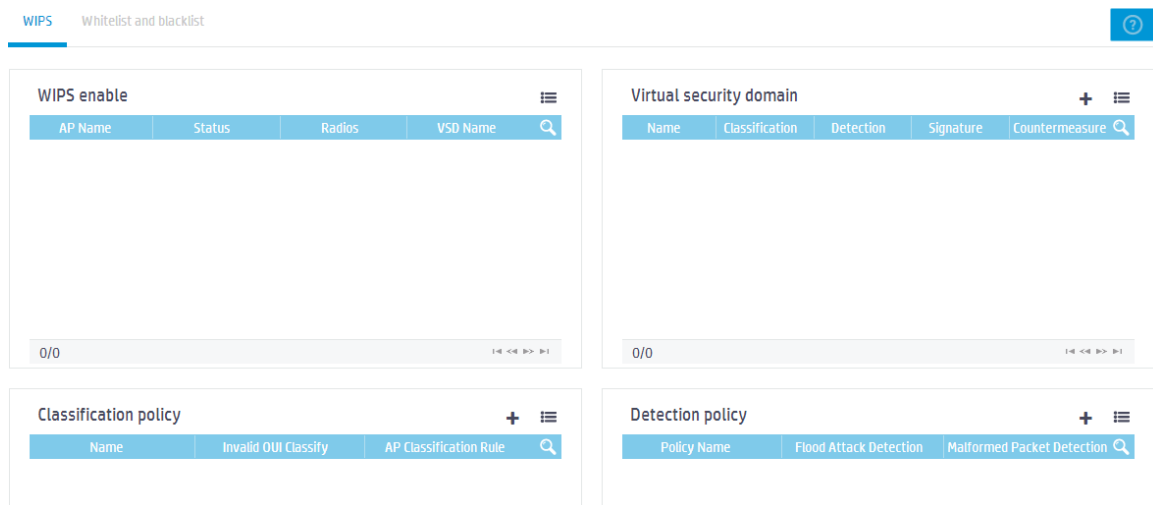
Types of webpages

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 **Interface** to sort entries by interfaces.

Figure 3 Sample table page

Interfaces Statistics


 All interfaces  Search  

 Interface 	Status	IP Address	Speed(Kb...	Duplex	Description	
 GE1/0/1	Down	-- --	0	Auto	GigabitEthernet1/0/1 Interf...	
 GE1/0/10	Down	-- --	0	Auto	GigabitEthernet1/0/10 Inte...	
 GE1/0/11	Down	-- --	0	Auto	GigabitEthernet1/0/11 Inte...	
 GE1/0/12	Down	-- --	0	Auto	GigabitEthernet1/0/12 Inte...	
 GE1/0/13	Down	-- --	0	Auto	GigabitEthernet1/0/13 Inte...	

Total 33 entries, 0 selected. Showing page 1 of 1. 

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.

Icons and buttons

[Table 1](#) describes icons and buttons you can use to configure and manage the device.

Table 1 Icons and buttons

Icon/button	Icon/button name	Task
General icons		
	Refresh	Refresh statistics or information manually.
	More	Display more contents.
	Add	Add a new configuration entry.
	Filter	Filter statistics or information by a specific field.
Help icons		
	Hint	Obtain help information for a function or parameter.
	Note	Display notes for a function or service.
Counter icon		
	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		
	Status control	Control the enable status of the feature. <ul style="list-style-type: none"> 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.
	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	<ul style="list-style-type: none"> Add a new entry. Confirm the addition of an entry and continue to add an additional entry.
	Export	Export an entry.
	Delete	Delete an entry. This icon appears at the end of an entry when you hover your mouse cursor over the entry.
	Modify	Modify an entry. This icon appears at the end of an entry when you hover your mouse cursor over the entry.

Icon/button	Icon/button name	Task
	Bulk-delete	Delete all entries.
	Details	Display detailed information for an entry. This icon appears at the end of an entry when you hover your mouse cursor over the entry.
	Field selector	Select fields to be displayed.
Advanced settings icon		
	Advanced settings	Access the advanced setting page.
Quick configuration icon		
	Quick configuration	Guide you through the quick configuration of a service.

Performing basic tasks


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

Saving the configuration

To prevent settings from being lost, save the configuration manually after configuring a device. To manually save the configuration, use either of the following methods:

- Click **Save** in the upper right corner.
- Perform the following tasks to access the configuration management page:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation tree, select **System > Management**.
 - c. Click the **Configuration** tab.
 - d. Click **Save Running Configuration**.

Displaying settings of a table entry

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

Rebooting the device

Reboot is required for some settings to take effect.

To reboot the device:

1. Save the configuration.
2. Click the system view tab at the bottom of the page.
3. From the navigation tree, select **System > Management**.
4. Click the **Reboot** tab.

5. On the reboot page, click the reboot button.

Contents

Feature navigator	1
Feature navigator in system view	1
Dashboard menu	1
Network configuration menu	1
Network security menu	5
System menu	6
Tools menu	7
Feature navigator in network view	7
Dashboard menu	7
Quick start menu	8
Monitoring menu	8
Wireless configuration menu	9
Network security menu	11
System menu	12
Tools menu	12
Reporting menu	12

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.

Top-level menus differ in system view and in network view. You can toggle between these two views by clicking the view tab at the bottom of the page. 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, perform the following tasks:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation tree, select **System > Management**. You are placed on the **Settings** tab.
- To delete an IPv4 ACL, perform the following tasks:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation tree, select **System > Resource**. You are placed on the **IPv4 ACL** tab.

NOTE:

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

Feature navigator in system view

Top-level menus in system view include **Dashboard**, **Network Configuration**, **Network Security**, **System**, and **Tools**.

Dashboard menu

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

- Event logs.
- AP statistics.
- System utilization information.
- Wireless service statistics.
- Client statistics.
- Interface traffic statistics.

This menu does not contain submenus.

Network configuration menu

Use [Table 1](#) to navigate to the tasks you can perform from the **Network Configuration** menu.

Table 1 Network configuration menu navigator

Menus	Tasks
Mobility Domain	

Menus	Tasks	
Roaming	<ul style="list-style-type: none">• Display WLAN client roaming information and roaming group information.• Configure WLAN client roaming settings.	
Roaming Centers	WLAN Roaming Center	<ul style="list-style-type: none">• Enable or disable WLAN roaming center• Configure a UDP port number, wait timer for user offline notification responses, maximum transmission attempts for user offline notification requests, and portal roaming center IP addresses.
	Portal Roaming Center	<ul style="list-style-type: none">• Enable or disable WLAN roaming center• Enable or disable the user packet access block feature.• Configure WLAN roaming center IP address, UDP port number, wait timer for responses from the WLAN roaming center, and maximum number of attempts to transmit a packet to the WLAN roaming center.
Network Interfaces		
Interfaces	<ul style="list-style-type: none">• Display interfaces and their attributes, including:<ul style="list-style-type: none">◦ Interface status.◦ IP address.◦ Speed and duplex mode.◦ Interface description.• Delete logical interfaces.• Modify interfaces.	
Link Aggregation	Create, modify, or delete Layer 2 aggregation groups.	
VLAN		
VLAN	<ul style="list-style-type: none">• Configure port-based VLANs.• Create VLAN-interfaces.	
MAC	<ul style="list-style-type: none">• Create or delete static MAC entries, dynamic MAC entries, and blackhole MAC entries.• Display existing MAC entries.	
STP	<ul style="list-style-type: none">• 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.	
Network Routing		
Routing Table	Display IPv4 and IPv6 routing table information, including brief routing table information and route statistics.	
Static Routing	<ul style="list-style-type: none">• Display IPv4 and IPv6 static routing entries.• Create, modify, or delete IPv4 and IPv6 static routing entries.	
Network Services-IP Services		
IP	<ul style="list-style-type: none">• 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
IPv6	<ul style="list-style-type: none"> 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.
Network Services-DHCP/DNS	
DHCP	<ul style="list-style-type: none"> Configure DHCP server functions, including: <ul style="list-style-type: none"> Configure DHCP services. Configure the interface to operate in the DHCP server mode. Configure DHCP address pools. Configure IP address conflict detection. Configure DHCP relay agent functions, including: <ul style="list-style-type: none"> Configure DHCP services. Configure the DHCP relay agent mode. Configure the IP address of the DHCP server. Configure settings for DHCP relay entry, include: <ul style="list-style-type: none"> Recording of DHCP relay entries. Periodic refreshing of DHCP relay entries. Interval for refreshing DHCP relay entries.
DHCP Snooping	<ul style="list-style-type: none"> Configure a port as a trusted or untrusted port. Record and back up DHCP snooping entries. Configure the following features for DHCP snooping ports: <ul style="list-style-type: none"> 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.
IPv4 DNS	<ul style="list-style-type: none"> Configure IPv4 static domain name resolution. Configure IPv4 dynamic domain name resolution. Configure the DNS proxy. Configure IPv4 domain name suffixes.
IPv6 DNS	<ul style="list-style-type: none"> Configure static and dynamic IPv6 domain name resolution. Configure the IPv6 DNS proxy. Configure IPv6 domain name suffixes.
Network Services-Multicast	
IGMP Snooping	<p>Configure IGMP snooping functions, including:</p> <ul style="list-style-type: none"> Enable or disable IGMP snooping in a VLAN. Query IGMP snooping entries. 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	<p>Configure MLD snooping functions, including:</p> <ul style="list-style-type: none"> Enable or disable MLD snooping in a VLAN. Query MLD snooping entries. Enable dropping unknown IPv6 multicast data. Configure the MLD snooping querier.

Menus	Tasks
	<ul style="list-style-type: none"> • Enable fast-leave processing. • Set the maximum number of IPv6 multicast groups on a port.
Network Services-ARP	
ARP	<ul style="list-style-type: none"> • Add static ARP entries. • Delete dynamic ARP entries and static ARP entries. • Configure the ARP proxy. • Configure gratuitous ARP. • Configure ARP attack protection.
Network Services-ND	
ND	<ul style="list-style-type: none"> • Add static ND entries. • Delete dynamic ND entries and static ND entries. • Configure the aging time for stale ND entries. • Enable or disable link local ND entry minimization. • Configure hop limit. • Configure RA prefix attributes, including: <ul style="list-style-type: none"> ◦ Address prefix. ◦ Prefix length. ◦ Valid lifetime. ◦ Preferred lifetime. • Configure RA settings for an interface, including: <ul style="list-style-type: none"> ◦ RA message suppression. ◦ Maximum and minimum intervals for sending RA messages. ◦ M-flag. ◦ MTU option. ◦ Hop limit. ◦ O-flag. ◦ Router lifetime. ◦ NS message retransmit interval. ◦ Router preference. ◦ Neighbor reachable time. • Enable common and local ND proxy on an interface. • Configure ND rules for the interface, including: <ul style="list-style-type: none"> ◦ Maximum number of dynamic neighbor entries. ◦ Maximum number of DAD attempts.
Network Services-NAT	
NAT	<ul style="list-style-type: none"> • Configure dynamic and static NAT, internal servers, and dynamic and static NAT444. • Configure NAT address groups, NAT444 address groups, port block groups, and server groups. • Configure PAT mode, DNS mappings, and NAT hairpin. • Enable NAT ALG. • Display NAT logs.
Management Protocols	
HTTP/HTTPS	<ul style="list-style-type: none"> • Enable or disable HTTP service. • Enable or disable HTTPS service. • Set the Web connection timeout. • Set the HTTP service port number. • Set the HTTPS service port number. • Specify Web access control ACLs.

Menus	Tasks
FTP	<ul style="list-style-type: none"> • Enable or disable FTP service. • Set the DSCP value for the device to use for outgoing FTP packets. • Specify FTP access control ACLs. • Set the FTP connection idle timeout. • Configure SSL service policies.
Telnet	<ul style="list-style-type: none"> • 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.
SSH	<ul style="list-style-type: none"> • Enable or disable the Stelnet, SFTP, and SCP services. • Configure SSH parameters.
NTP	<ul style="list-style-type: none"> • Enable or disable the NTP service. • Configure the IP address and stratum level of the local clock. • Set an NTP authentication key.
LLDP	<ul style="list-style-type: none"> • Enable or disable LLDP. • Enable or disable CDP compatibility. • Configure LLDP parameters. • Display interface status. • Configure the interface status. • Display LLDP neighbors. • Configure LLDP to advertise the specified TLVs.
Settings	<ul style="list-style-type: none"> • 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.

Network security menu

Use [Table 2](#) to navigate to the tasks you can perform from the **Network Security** menu.

Table 2 Network security menu navigator

Menus	Tasks
Packet Filter	
Packet Filter	<ul style="list-style-type: none"> • Create, modify, or delete a packet filter for an interface. • Configure the default action for the packet filter.
Traffic Policy	
QoS Policies	<ul style="list-style-type: none"> • Create, modify, or delete interface QoS policies.
Priority Mapping	<ul style="list-style-type: none"> • Query or configure the port priority. • Configure the priority trust mode for a port. • Query or modify the priority mapping table.
Access Control	
802.1X	<ul style="list-style-type: none"> • Enable or disable 802.1X. • Configure the 802.1X authentication method. • Configure the port access control method. • Configure the maximum number of concurrent 802.1X users on the port. • Configure advanced 802.1X features.

Menus	Tasks
Authentication	
ISP Domains	Configure ISP domains.
RADIUS	Configure RADIUS schemes.
User Management	
Local Users	<ul style="list-style-type: none"> Add, modify, or delete local users. Add, modify, or delete local user groups.

System menu

Use [Table 3](#) to navigate to the tasks you can perform from the **System** menu.

Table 3 System menu navigator

Menus	Tasks	
Event Logs		
Event Logs	Query, collect, or delete log information.	
Resource		
IPv4 ACL	<ul style="list-style-type: none"> Create, modify, or delete an IPv4 basic ACL. Create, modify, or delete an IPv4 advanced ACL. 	
IPv6 ACL	<ul style="list-style-type: none"> Create, modify, or delete an IPv6 basic ACL. Create, modify, or delete an IPv6 advanced ACL. 	
Layer 2 ACLs	Create, modify, or delete an Ethernet frame header ACL.	
Time range	Create, modify, or delete a time range.	
File Systems		
File System Management	Upload, download, or delete files.	
License Management	License configuration	Add license file.
	Obtain DID	Export DID.
	Licenses and features	View whether features are licensed.
	Compress	Compress license files.
	License guide	View license-related operation guides.
Administrators		
Administrators	<ul style="list-style-type: none"> Create, modify, or delete roles. Create, modify, or delete administrators. Configure the role of administrators. Control administrator access authority. Manage passwords. 	
Management		
Settings	<ul style="list-style-type: none"> Set the name, location, and contact information of the device. Set the system time. 	
Configuration	<ul style="list-style-type: none"> Save or export the running configuration. Import configuration. Display the running configuration. 	

Menus	Tasks
	<ul style="list-style-type: none"> Restore the settings to the factory defaults.
Upgrade	<ul style="list-style-type: none"> Upgrade system software. Display system software lists, including: <ul style="list-style-type: none"> List of software enabled at the current system startup. List of main software to be enabled at the next system startup.
Reboot	Reboot the device.
About	Display basic device information, including device name, serial number, model, description, location, contact information, version, electronic label, and statement.

Tools menu

Use [Table 4](#) to navigate to the tasks you can perform from the **Tools** menu.

Table 4 Tools menu navigator

Menus	Tasks	
Debug		
Diagnostics	Collect diagnostic information for locating problems.	
Ping	IPv4 Ping	Identify whether an IPv4 address is reachable.
	IPv6 Ping	Identify whether an IPv6 address is reachable.
Tracert	IPv4 Tracert	Trace the path of IPv4 packets from source to destination.
	IPv6 Tracert	Trace the path of IPv6 packets from source to destination.

Feature navigator in network view

Top-level menus in network view include **Dashboard**, **Quick Start**, **Monitoring**, **Wireless Configuration**, **Network Security**, **System**, **Tools**, and **Reporting**.

Dashboard menu

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

- Event logs.
- AP statistics.
- System utilization information.
- Wireless service statistics.
- Client statistics.
- Interface traffic statistics.

This menu does not contain submenus.

Quick start menu

Use [Table 5](#) to navigate to the tasks you can perform from the **Quick Start** menu.

Table 5 Quick start menu navigator

Menus	Tasks
Add New AP	
Add New AP	Add new APs manually.
Add New SSID	
Add New SSID	<ul style="list-style-type: none">• Configure wireless services.• Configure link layer authentication.• Enable or disable authorization.• Enable or disable intrusion detection.• Configure key management.• Bind APs.
Add New User	
Add New User	Add new users.

Monitoring menu

Use [Table 6](#) to navigate to the tasks you can perform from the **Monitoring** menu.

Table 6 Monitoring menu navigator

Menus	Tasks	
Wireless Networks		
Wireless Services	Display wireless services.	
Access Points		
APs	Display AP statistics.	
AP Groups	Display AP groups.	
Clients		
Clients	Display client statistics.	
Wireless Security		
WIPS	Display WIPS statistics.	
RRM		
RF Optimization	Display channel and power adjustment information.	
Spectrum Analysis	Display detailed information about spectrum analysis.	
Client Proximity Sensor		
Client Proximity Sensor	Display client proximity sensor information.	
DPI	IPv4	Display IPv4/IPv6 traffic and application statistics.
	IPv6	
Application Monitoring		

Menus	Tasks
Bonjour	<ul style="list-style-type: none"> • Display Bonjour service information discovered by Bonjour gateways. • Clear Bonjour service resource information.
Multicast Optimization	Display IPv4 and IPv6 multicast statistics.

Wireless configuration menu

Use [Table 7](#) to navigate to the tasks you can perform from the **Wireless Configuration** menu.

Table 7 Wireless configuration menu navigator

Menus	Tasks
Wireless Networks	
Wireless Networks	<ul style="list-style-type: none"> • Display wireless services. • Add, delete, or modify wireless services. • Configure link layer authentication. • Enable or disable authorization and intrusion detection. • Manage keys. • Bind APs. • Configure access control.
AP Management	
AP	Add, modify, delete, or query APs.
AP Groups	Create, query, modify, or delete AP groups.
AP Global Settings	<ul style="list-style-type: none"> • Configure AP region codes. • Enable or disable region code lock. • Enable or disable AP software upgrade. • Enable or disable auto AP. • Enable or disable auto-AP persistence.
AP Provisioning	Display or modify AP preprovisioned settings.
AP Group Provisioning	Display or modify AP group preprovisioned settings.
Wireless QoS	
Client Rate Limiting	<ul style="list-style-type: none"> • Display detailed information about client rate limit. • Configure client-type-based client rate limit. • Configure service-based client rate limit. • Configure AP radio or AP group radio-based client rate limit.
Bandwidth Guaranteeing	<ul style="list-style-type: none"> • Display detailed information about intelligent bandwidth guarantee. • Set the maximum radio bandwidth. • Configure intelligent bandwidth guarantee for an AP or AP group.
Wi-Fi Multimedia	<ul style="list-style-type: none"> • Display wireless QoS status and information. • Display radio EDCA parameters. • Display radio and client negotiation parameters. • Display WMM statistics for clients. • Display transport stream information.
Wireless Security	
WIPS	<ul style="list-style-type: none"> • Display detailed WIPS information. • Enable WIPS.

Menus	Tasks
	<ul style="list-style-type: none"> • Configure VSDs. • Configure classification policies. • Configure attack detection policies. • Configure signature policies. • Configure countermeasure policies. • Configure AP classification rules. • Configure signatures. • Add MAC addresses to the alarm-ignored device list.
Whitelist and blacklist	<ul style="list-style-type: none"> • Configure whitelists. • Configure static and dynamic blacklists.
Radio Management	
Radio Configuration	Display detailed model and radio information for all APs in an AP group.
RRM	<ul style="list-style-type: none"> • Display channel and power adjustment information. • One-key channel and power optimization. • Configure RRM for APs and AP groups: <ul style="list-style-type: none"> ◦ Configure RRM holddown groups. ◦ Configure radio baselines. • Display RRM adjustment history.
Spectrum Analysis	<ul style="list-style-type: none"> • Enable spectrum analysis. • Configure interference device type. • Import feature database files. • Configure the alarming feature.
Load Balancing	<ul style="list-style-type: none"> • Enable load balancing. • Configure the load balancing mode. • Configure load balancing groups. • Configure load balancing parameters.
Band Navigation	<ul style="list-style-type: none"> • Enable or disable global band navigation. • Enable or disable band navigation for APs and AP groups. • Configure band navigation parameters.
Client Proximity Sensor	
Client Proximity Sensor	<ul style="list-style-type: none"> • Enable or disable client proximity sensor. • Display client proximity sensor information.
Applications	
Mesh Services	Configure mesh settings.
Multicast Optimization	<ul style="list-style-type: none"> • Display IPv4 multicast optimization. • Configure IPv4 multicast optimization. • Display IPv6 multicast optimization. • Configure IPv6 multicast optimization.
Location Aware	<ul style="list-style-type: none"> • Configure global packet rate limit, packet filtering, and packet dilution. • Configure Aeroscout locating, bluetooth locating, CUPID locating, fingerprinting, and Internet of Things (IoT) locating.
Bonjour	<ul style="list-style-type: none"> • Enable or disable the Bonjour gateway feature. • Create and activate Bonjour service types. • Change the Bonjour gateway mode. • Configure Bonjour policies.

Network security menu

Use [Table 8](#) to navigate to the tasks you can perform from the **Network Security** menu.

Table 8 Network security menu navigator

Menus	Tasks
Packet Filter	
Packet Filter	<ul style="list-style-type: none">Create, modify, or delete a packet filter for an interface.Configure the default action for the packet filter.
Traffic Policy	
QoS Policies	<ul style="list-style-type: none">Create, modify, or delete interface QoS policies.
Priority Mapping	<ul style="list-style-type: none">Query and configure the port priority.Configure the priority trust mode for a port.Query and modify the priority mapping table.
Access Control	
802.1X	<ul style="list-style-type: none">Enable or disable 802.1X.Configure the 802.1X authentication method.Configure the port access control method.Configure the maximum number of concurrent 802.1X users on the port.Configure advanced 802.1X features.
Authentication	
ISP Domains	Configure ISP domains.
RADIUS	Configure RADIUS schemes.
BYOD	
BYOD DB	<ul style="list-style-type: none">Display DHCP rules, HTTP rules, and MAC rules.Configure DHCP rules, HTTP rules, and MAC rules.
BYOD Authorization	Query or modify BYOD authorization.
User Management	
Local Users	<ul style="list-style-type: none">Add, modify, or delete local users.Add or modify local user groups.
Guest Management	
Guest List	Query, add, or export guests.
Import Guests	Import guests.
Generate Guest Accounts	Generate guests in bulk.
Approve Guest	Approve guests.
Guest Configuration	Configure guest parameters.
Access Control	
MAC Authentication	Configure MAC authentication.
Port Security	Configure port security features.
Portal	Configure portal authentication.

System menu

Use [Table 9](#) to navigate to the tasks you can perform from the **System** menu.

Table 9 System menu navigator

Menus	Tasks
Resource	
IPv4 ACL	<ul style="list-style-type: none">Create basic or advanced IPv4 ACLs.Modify or delete ACLs on this page and other service module pages, such as the packet filtering page.
IPv6 ACL	<ul style="list-style-type: none">Create basic or advanced IPv6 ACLs.Modify or delete ACLs on this page and other service module pages, such as the packet filtering page.
Layer 2 ACLs	<ul style="list-style-type: none">Create Ethernet ACLs.Modify or delete ACLs on this page and other service module pages, such as the packet filtering page.
Time Range	Create, modify, or delete time ranges.
VLAN Groups	Create, modify, or delete VLAN groups.
SSL	<ul style="list-style-type: none">Create, modify, or delete server-end policiesCreate, modify, or delete client-end policies.Enable or disable SSL3.0.
Public Key	Manage local asymmetric keys and peer host public keys.
PKI	<ul style="list-style-type: none">Create, modify, and delete PKI domains.Create, modify, or delete PKI entities.Configure the storage path for certificates and CRLs.

Tools menu

Use [Table 10](#) to navigate to the tasks you can perform from the **Tools** menu.

Table 10 Tools menu navigator

Menus	Tasks
Wireless Capture	
Wireless Capture	Display captured wireless packets.
RF Ping	
RF Ping	Perform wireless link quality detection.
Debug	
Diagnostics	Collect diagnostic information for locating problems.

Reporting menu

Use [Table 11](#) to navigate to the tasks you can perform from the **Reporting** menu.

Table 11 Reporting menu navigator

Menus	Tasks
Client Statistics	
AC Frame	Display transmitted/received/dropped AC frames.
AC Bytes	Display transmitted/received/dropped AC bytes.
Total Frame	Display total transmitted, received, and dropped frames.
Total Bytes	Display total transmitted, received, and dropped bytes.
AP Statistics	
AP Statistics	Display AP statistics.
Wireless Service Statistics	
Wireless Service Statistics	Display wireless service statistics.

Contents

Network services features	1
WLAN roaming	1
Overview	1
Terminology	1
WLAN roaming mechanism	1
WLAN roaming center	2
Overview	2
WLAN roaming center UDP port number	3
Wait timer for user offline notification responses	3
Maximum transmission attempts for user offline notification requests	3
Portal roaming centers permitted by the WLAN roaming center	3
Portal roaming center	3
Overview	3
WLAN roaming center IP address	3
WLAN roaming center UDP port number	3
Response timeout timer for packets to the WLAN roaming center	4
Maximum number of transmission attempts for packets to the WLAN roaming center	4
Interfaces	4
Configuring the interface duplex mode and speed	4
Configuring the link mode of an Ethernet interface	4
Configuring jumbo frame support	5
Configuring generic flow control on an Ethernet interface	5
Storm suppression	5
Link aggregation	5
Aggregation group	6
Aggregation states of member ports in an aggregation group	6
Operational key	6
Attribute settings	6
Link aggregation modes	6
VLAN	10
Port-based VLANs	10
VLAN interface	10
MAC	10
Types of MAC address entries	11
Aging timer for dynamic MAC address entries	11
MAC address learning	11
STP	11
Spanning tree modes	12
MSTP basic concepts	12
Port roles	12
Port states	13
Routing table	13
Static routing	13
IP	14
IP address classes	14
Subnetting and masking	14
IP address configuration methods	15
MTU for an interface	15
IPv6	15
IPv6 address formats	15
IPv6 address types	15
EUI-64 address-based interface identifiers	16
IPv6 global unicast address configuration methods	17
IPv6 link-local address configuration methods	17
DHCP	17
DHCP server	17
DHCP relay agent	19

DHCP snooping	20
DNS	21
Dynamic domain name resolution	21
Static domain name resolution	21
DNS proxy	22
IGMP snooping	22
MLD snooping	22
ARP	22
Types of ARP table entries	22
Proxy ARP	23
Gratuitous ARP	23
ARP attack protection	24
ND	26
Neighbor entries	27
RA messages	27
ND proxy	28
NAT	29
Static NAT	29
Dynamic NAT	30
NAT Server	30
NAT444	31
Advanced settings	32
Restrictions and guidelines	34
HTTP/HTTPS	34
FTP	35
Telnet	35
SSH	35
NTP	36
LLDP	36
LLDP agent	36
Transmitting LLDP frames	36
Receiving LLDP frames	37
LLDP reinitialization delay	37
LLDP trapping	37
LLDP TLVs	37
CDP compatibility	37
Log	37
Log levels	37
Log destinations	38
Security features	39
Packet filter	39
QoS	39
QoS policies	39
Priority mapping	39
802.1X	40
802.1X architecture	40
802.1X authentication methods	40
Access control methods	40
Port authorization state	41
Periodic online user reauthentication	41
Online user handshake	41
Authentication trigger	41
EAD assistant	41
802.1X SmartOn	42
ISP domains	42
RADIUS	43
RADIUS protocol	43
Enhanced RADIUS features	43
Local users	44

System features	44
ACL	44
ACL types and match criteria	44
Match order	45
Rule numbering	46
Time range	46
File system management	47
File systems	47
Directories	47
Files	48
File system management restrictions and guidelines	48
File management	48
License management	49
Administrators	49
User account management	49
Role-based access control	49
Password control	54
Settings	57
System time sources	57
Clock synchronization protocols	57
NTP/SNTP operating modes	58
NTP/SNTP time source authentication	58
Tools	59
Diagnostics	59
Ping	59
Tracert	59

Network services features

WLAN roaming

Overview

WLAN roaming enables clients to seamlessly roam among APs in an ESS while retaining their IP address and authorization information during the roaming process.

INTELBRAS ACs also support fast roaming, which enables RSN + 802.1X clients to roam to a new AP without being authenticated again.

Terminology

- **Inter Access Device Tunneling Protocol**—IADTP is an INTELBRAS-proprietary protocol that provides a generic packet encapsulation and transport mechanism for devices to securely communicate with each other. Devices providing roaming services establish an IADTP tunnel with each other to exchange control messages and client information.
- **Home agent**—A home agent is an AC that manages the AP with which a wireless client associates for the first time. If the AC that authenticates a client is not the AC with which the client associates for the first time, the AC that authenticates the client is the HA.
- **Foreign agent**—A foreign agent is an AC that is other than the HA and with which a client currently associates.

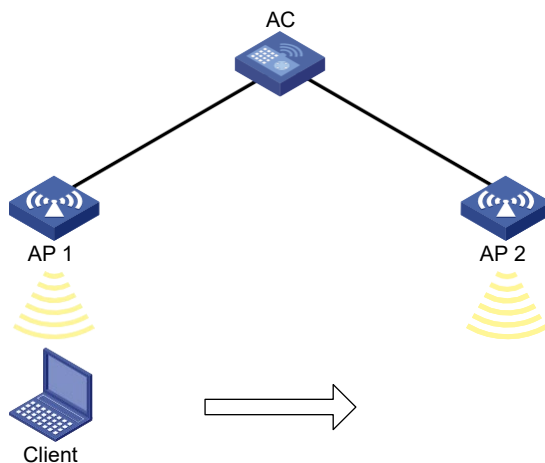
WLAN roaming mechanism

Clients can roam between APs managed by ACs in the same mobility group.

Intra-AC roaming

Intra-AC roaming enables clients to roam among APs that are managed by the same AC.

Figure 1 Intra-AC roaming



As shown in [Figure 1](#), intra-AC roaming uses the following procedure:

1. The client comes online from AP 1, and the AC creates a roaming entry for the client.

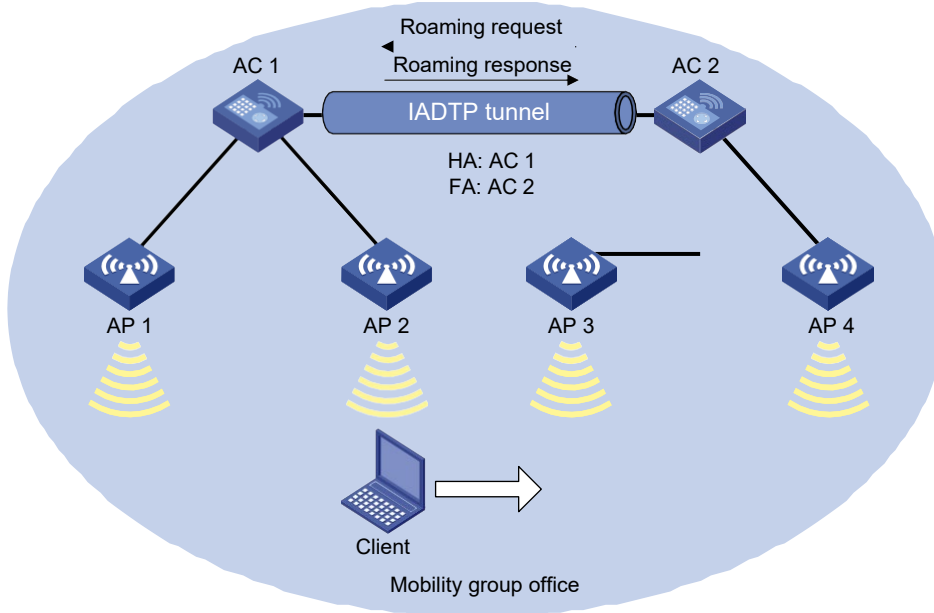
2. The client roams to AP 2. The AC examines the roaming entry for the client and determines whether to perform fast roaming.

Fast roaming is performed only if the client is an RSN + 802.1X client and the PMKID carried by the client is the same as that in the client's roaming entry on the AC.

Inter-AC roaming

Inter-AC roaming enables clients to roam among APs that are managed by different ACs. These ACs must be in the same mobility group and have established an IADTP tunnel with each other.

Figure 2 Inter-AC roaming



As shown in [Figure 2](#), inter-AC roaming uses the following procedure:

1. The client comes online from AP 2. AC 1 creates a roaming entry for the client and sends the information to AC 2 through the IADTP tunnel.
2. The client roams to AP 3. AC 2 examines the roaming entry for the client and determines whether to perform fast roaming.
Fast roaming is performed only if the client is an RSN + 802.1X client and the PMKID carried by the client is the same as that in the client's roaming entry on AC 2.
3. The client associates with AP 3. AC 2 sends a roaming request to AC 1.
4. AC 1 verifies the roaming request and performs either of the following operations:
 - Sends a roaming response that indicates roaming failure to AC 2 if the request is invalid. AC 2 logs off the client.
 - Saves the roaming trace and roam-out information and sends a roaming response that indicates roaming success to AC 2 if the request is valid. AC 2 saves roaming-in information for the client.

WLAN roaming center

Overview

A WLAN roaming center is an AC that manages information about wireless client authentication, authorization, and roaming to enable seamless inter-AC roaming. With the roaming center feature configured, clients can roam to another AC without being reauthenticated.

WLAN roaming center UDP port number

The WLAN roaming center uses a port number to communicate with portal roaming centers. Make sure the port specified for the WLAN roaming center is the same as the port specified for portal roaming centers.

Wait timer for user offline notification responses

After sending a user offline notification request to an AC, the WLAN roaming center resends the request if it fails to receive a response before the wait timer expires. If it fails to receive any response after the maximum transmission attempt limit is reached, the WLAN roaming center deletes the timeout timer and removes the AC from the access device list of the client.

Maximum transmission attempts for user offline notification requests

After sending a user offline notification request to an AC, the WLAN roaming center resends the request if it fails to receive a response before the wait timer expires. If it fails to receive any response after the maximum transmission attempt limit is reached, the WLAN roaming center deletes the timeout timer and removes the AC from the access device list of the client.

Portal roaming centers permitted by the WLAN roaming center

This feature enables the WLAN roaming center to process packets only from the permitted portal roaming centers, enhancing network security. If no permitted portal roaming centers are specified, the WLAN roaming center processes packets from all portal roaming centers.

Portal roaming center

Overview

A portal roaming center manages authentication, authorization, and roaming information for wireless portal users, stores and updates user information, sends request and response packets, and provides user query services.

WLAN roaming center IP address

The WLAN roaming center uses an IP address to communicate with portal roaming centers. The address can be any IP address used by the WLAN roaming center.

WLAN roaming center UDP port number

The WLAN roaming center uses a port number to communicate with portal roaming centers. Make sure the port specified for portal roaming centers is the same as the port specified for the WLAN roaming center.

Response timeout timer for packets to the WLAN roaming center

After the portal roaming center sends a packet to the WLAN roaming center, it starts a timer to wait for a response from the WLAN roaming center. If the portal roaming center does not receive a response before the timer expires, it retransmits the packet till the maximum number of transmission attempts is reached.

Maximum number of transmission attempts for packets to the WLAN roaming center

After the portal roaming center sends a packet to the WLAN roaming center, it starts a timer to wait for a response from the WLAN roaming center. If the portal roaming center does not receive a response before the timer expires, it retransmits the packet. If the maximum number of attempts is reached, it still does not receive a response from the WLAN roaming center, the process goes as follows:

- If the portal roaming center does not receive a user query response, the portal roaming center performs authentication on the user.
- If the portal roaming center does not receive a user deletion response, it determines that the WLAN roaming center does not delete the user.
- If the portal roaming center does not receive a user information update response, it determines that the WLAN roaming center does not update the user information.

Interfaces

You can view interface traffic statistics information and configure basic interface settings.

Configuring the interface duplex mode and speed

You can configure an Ethernet interface to operate in one of the following duplex modes:

- **Full-duplex mode**—The interface can send and receive packets simultaneously.
- **Half-duplex mode**—The interface can only send or receive packets at a given time.
- **Autonegotiation mode**—The interface negotiates a duplex mode with its peer.

You can set the speed of an Ethernet interface or enable it to automatically negotiate a speed with its peer.

Configuring the link mode of an Ethernet interface

Ethernet interfaces operate differently depending on the hardware structure of interface cards:

- Some Ethernet interfaces can operate only as Layer 2 Ethernet interfaces (in bridge mode).
- Some Ethernet interfaces can operate only as Layer 3 Ethernet interfaces (in route mode).
- Some Ethernet interfaces can operate either as Layer 2 or Layer 3 Ethernet interfaces. You can set the link mode to bridge or route for these Ethernet interfaces.

Configuring jumbo frame support

Jumbo frames are frames larger than a device-specific size and are typically received by an Ethernet interface during high-throughput data exchanges, such as file transfers. The device-specific size varies by device model.

The Ethernet interface processes jumbo frames in the following ways:

- When the Ethernet interface is configured to deny jumbo frames, the Ethernet interface discards jumbo frames.
- When the Ethernet interface is configured with jumbo frame support, the Ethernet interface performs the following operations:
 - Processes jumbo frames within the specified length.
 - Discards jumbo frames that exceed the specified length.

Configuring generic flow control on an Ethernet interface

To avoid dropping packets on a link, you can enable generic flow control at both ends of the link. When traffic congestion occurs at the receiving end, the receiving end sends a flow control (Pause) frame to ask the sending end to suspend sending packets. Generic flow control includes the following types:

- **TxRx-mode generic flow control**—With TxRx-mode generic flow control enabled, an interface can both send and receive flow control frames:
 - When congestion occurs, the interface sends a flow control frame to its peer.
 - When the interface receives a flow control frame from its peer, it suspends sending packets to its peer.
- **Rx-mode generic flow control**—With Rx-mode generic flow control enabled, an interface can receive flow control frames, but it cannot send flow control frames:
 - When congestion occurs, the interface cannot send flow control frames to its peer.
 - When the interface receives a flow control frame from its peer, it suspends sending packets to its peer.

Storm suppression

The storm suppression feature ensures that the size of a particular type of traffic (broadcast, multicast, or unknown unicast traffic) does not exceed the threshold on an interface. When the broadcast, multicast, or unknown unicast traffic on the interface exceeds this threshold, the system discards packets until the traffic drops below this threshold.

Both storm suppression and storm control can suppress storms on a Layer 2 interface. Storm suppression uses the chip to suppress traffic. Storm suppression has less impact on the device performance than storm control, which uses software to suppress traffic.

Link aggregation

Ethernet link aggregation bundles multiple physical Ethernet links into one logical link, called an aggregate link. Link aggregation provides 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 either 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 settings

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

Feature	Considerations
Port isolation	Whether a port is assigned to an isolation group and the isolation group to which the port is assigned.
VLAN	VLAN attribute settings include: <ul style="list-style-type: none">• Permitted VLAN IDs.• PVID.• Port link type.• VLAN tagging mode.

Link aggregation modes

An aggregation group operates in either 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.

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 settings as the reference port.

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

The candidate ports are sorted in the following order:

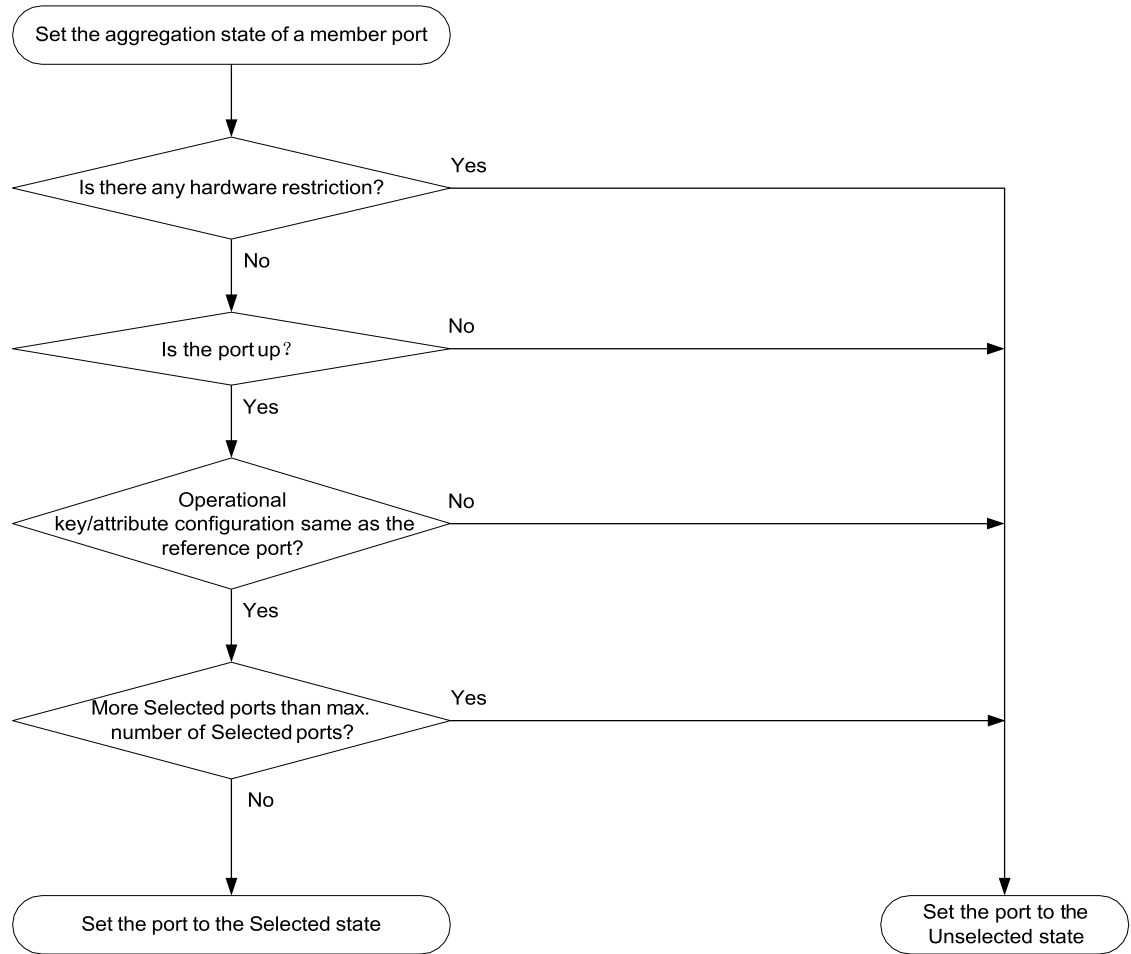
1. Port priority
2. Full duplex/high speed
3. Full duplex/low speed
4. Half duplex/high speed
5. Half duplex/low speed

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 3 Setting the aggregation state of a member port in a static aggregation group



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 Selected state.

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

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

1. 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.
 - a. 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 the next step.
 - b. The two systems compare their MAC addresses.

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

2. The system with the smaller system ID chooses the port with the smallest port ID as the reference port.

A port ID contains a port priority and a port number. The lower the port priority, the smaller the port ID.

- a. 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.

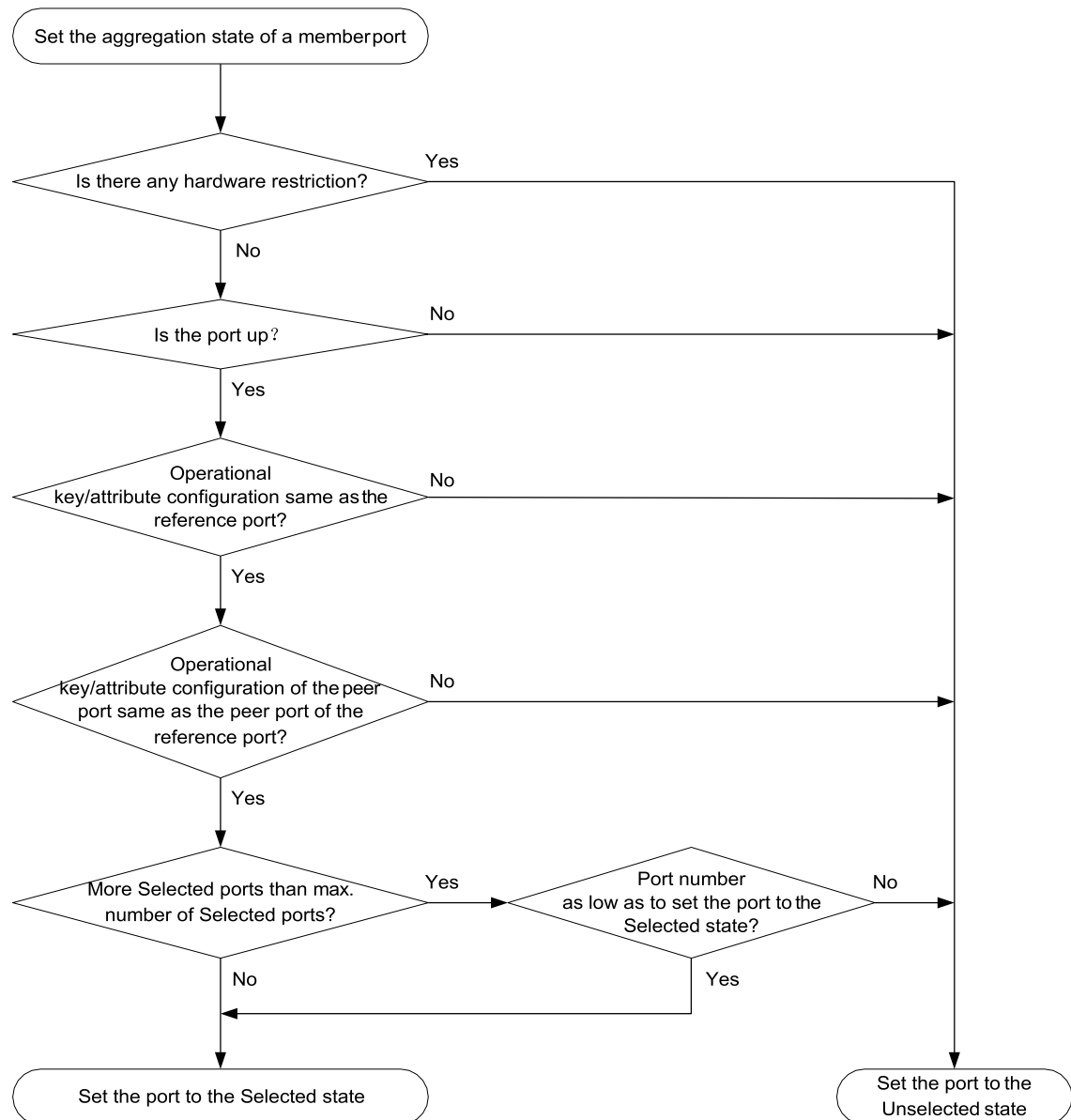
- b. The system compares their port numbers.

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

The port with the smallest port number and the same attribute settings 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 4 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.

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.

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. The blackhole entry of a MAC address has a higher priority than the dynamic entry of the MAC address.

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, PVST, 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. Because each VLAN runs RSTP independently, a spanning tree only serves its VLAN.
- **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 the following:

- **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**—On an access port, the PVST mode is compatible with other spanning tree modes in all VLANs. On a trunk port or hybrid port, the PVST mode is compatible with other spanning tree modes only in the default VLAN.
- **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**—Acts 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**—Acts 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**—Acts 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.

Routing table

You can display routing table information, including brief routing table information and route statistics.

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.

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 commonly 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 contains 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.

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

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 hexadecimal numbers 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 an Ethernet interface and 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:

- Insert the 16-bit binary number 1111111111111110 (hexadecimal value of FFFE) behind the 24th high-order bit of the MAC address.
- 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.

- **On a tunnel interface**—The lower 32 bits of the EUI-64 address-based interface identifier are the source IPv4 address of the tunnel interface. The higher 32 bits of the EUI-64 address-based interface identifier of an ISATAP tunnel interface are 0000:5EFE, whereas those of other tunnel interfaces are all zeros.
- **On an interface of another type**—The EUI-64 address-based interface identifier is generated randomly by the device.

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 to avoid link-local address conflicts, use the automatic generation method. If both methods are used, manual assignment takes precedence over automatic generation.

- 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.

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:

- 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 receives no response, the server continues to ping the IP address until a specific number of ping packets are sent. If still no response is received, 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 avoids deploying a DHCP server for each subnet to centralize management and reduce investment.

DHCP relay entry recording

This function 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.

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 contains no Option 82, DHCP snooping forwards it directly.

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.
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.

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 tasks:

- 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.

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.

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 when the output interface goes down. In addition, a dynamic ARP entry can be overwritten by a static ARP entry.

Dynamic ARP entries can be converted to static ARP entries. These static ARP entries cannot be converted back to dynamic entries.

To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn.

Static ARP entry

A static ARP entry is manually configured or converted from a dynamic ARP entry. 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.

To communicate with a host by using a fixed IP-to-MAC mapping, configure a 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, you must specify the VLAN and the output interface in the ARP entry. Make sure the IP address is on the same subnet as the IP address of the VLAN interface.

Proxy ARP

Proxy ARP enables a device on one network to answer ARP requests for an IP address on another network. With proxy ARP, hosts on different broadcast domains can communicate with each other as they would on the same broadcast domain.

Proxy ARP includes common proxy ARP and local proxy ARP.

- **Common proxy ARP**—Allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.
- **Local proxy ARP**—Allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

You can specify an IP address range for which local proxy ARP is enabled.

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

When this function 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.

Replying with gratuitous ARP packets

This function enables a device to send gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

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 are threatening LAN security. Although ARP is easy to implement, it provides no 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.

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 by 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 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.

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 1 describes the ICMPv6 messages used by ND.

Table 1 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 when certain conditions are met.

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 must be less than or equal to 0.75 times the maximum interval.

[Table 2](#) describes the configurable parameters in an RA message.

Table 2 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

Parameter	Description
	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	Notifies the hosts to not 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

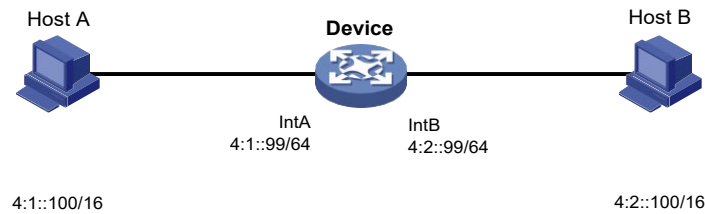
ND proxy enables a device to answer an NS message requesting the hardware address of a host on another network. With ND proxy, hosts in different broadcast domains can communicate with each other as they would on the same network.

ND proxy includes common ND proxy and local ND proxy.

Common ND proxy

As shown in [Figure 5](#), 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 B reside on the same network but in different broadcast domains.

Figure 5 Application environment of common ND proxy



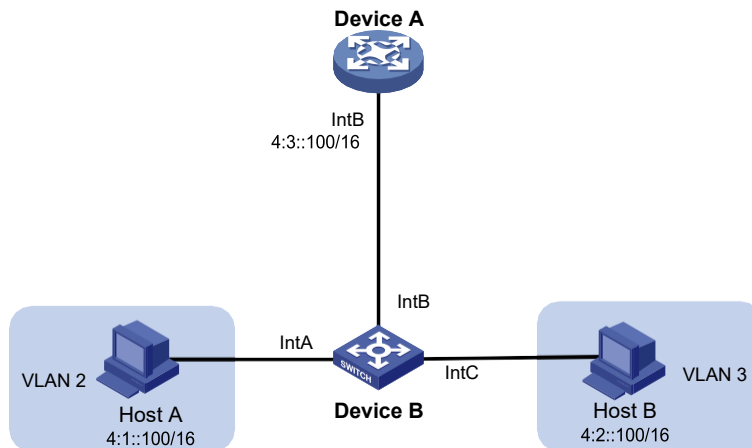
Because Host A's IPv6 address is on the same subnet as Host B's, Host A directly sends an NS message to obtain Host B's MAC address. However, Host B cannot receive the NS message because they belong to different broadcast domains.

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 6, 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 6 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.

NAT

Network Address Translation (NAT) translates an IP address in the IP packet header to another IP address. Typically, NAT is configured on gateways to enable private hosts to access external networks and external hosts to access private network resources such as a Web server.

Static NAT

Static NAT creates a fixed mapping between a private address and a public address. It supports connections initiated from internal users to the external network and from external users to the internal network. Static NAT applies to regular communications.

Dynamic NAT

Dynamic NAT uses an address pool to translate addresses. It applies to the scenario where a large number of internal users access the external network.

NO-PAT

Not Port Address Translation (NO-PAT) translates a private IP address to a public IP address by mapping the private IP address to the public IP address. The public IP address cannot be used by another internal host until it is released.

NO-PAT supports all IP packets and creates a NO-PAT entry for each IP address mapping.

PAT

Port Address Translation (PAT) translates multiple private IP addresses to a single public IP address by mapping the private IP addresses and source ports to the public IP address and a unique port.

PAT supports only TCP and UDP packets, and ICMP request packets.

NAT Server

The NAT Server feature maps a public address and port number to the private IP address and port number of an internal server. This feature allows servers in the private network to provide services for external users.

The following table describes the address-port mappings between an external network and an internal network for NAT Server.

Table 3 Address-port mappings for NAT Server

External network	Internal network
A public address	A private address.
A public address and a public port number	A private address and a private port number.
A public address and N consecutive public port numbers	A private address and a private port number.
	N consecutive private addresses and a private port number.
	A private address and N consecutive private port numbers.
N consecutive public addresses	A private address.
	N consecutive private addresses.
N consecutive public addresses and a public port number	A private address and a private port number.
	N consecutive private addresses and a private port number.
	A private address and N consecutive private port numbers.
A public address and a public port number	A private server group.
A public address and N consecutive public port numbers	
N consecutive public addresses and a public port number	

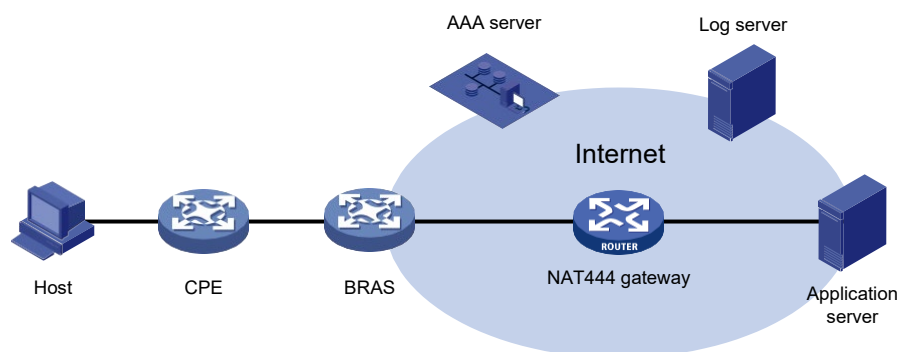
NAT444

NAT444 provides carrier-grade NAT. It is a preferred solution for carriers to mitigate IPv4 address exhaustion. It introduces a second layer of NAT on the carrier side, with few changes on the customer side and the application server side. Its user logging function provides the user tracing service.

As shown in Figure 7, the NAT444 architecture includes the following entities:

- **CPE**—Provides NAT services on the customer side.
- **BRAS**—Provides Internet access services.
- **NAT444 gateway**—Provides carrier-grade NAT services.
- **AAA server**—Cooperates with BRAS to provide user authentication, authorization, and accounting services.
- **Log server**—Records user access logs and responds to queries for user access information.

Figure 7 NAT444 application diagram



The NAT444 gateway provides port block-based PAT translation. It maps multiple private IP addresses to one public IP address and uses a different port block for each private IP address.

For example, the private IP address 10.1.1.1 of an internal host is mapped to the public IP address 202.1.1.1 and port block 10001 to 10256. When the internal host accesses public hosts, the source IP address 10.1.1.1 is translated to 202.1.1.1, and the source ports are translated to ports in the port block 10001 to 10256.

NAT444 includes static NAT444 and dynamic NAT444.

Static NAT444

The NAT444 gateway computes a static NAT444 mapping before address translation. The mapping is between a private IP address and a public IP address with a port block.

The NAT444 gateway uses private IP addresses, public IP addresses, a port range, and a port block size to compute static mappings:

1. Divides the port range by the port block size to get the number of available port blocks for each public IP address.
This value is the base number for mapping.
2. Sorts the port blocks in ascending order of the start port number in each block.
3. Sorts the private IP addresses and the public IP addresses separately in ascending order.
4. Maps the first base number of private IP addresses to the first public IP address and its port blocks in ascending order.

For example, the number of available port blocks of each public IP address is **m**. The first **m** private IP addresses are mapped to the first public IP address and the **m** port blocks in ascending order. The

next **m** private IP addresses are mapped to the second IP address and the **m** port blocks in ascending order. The other static NAT444 mappings are created by analogy.

Dynamic NAT444

Dynamic NAT444 works as follows:

1. Creates a mapping from the internal host's private IP address to a public IP address and a port block when the host initiates a connection to the public network.
2. Translates the private IP address to the public IP address, and the source ports to ports in the selected port block for subsequent connections from the private IP address.
3. Withdraws the port block and deletes the dynamic NAT444 mapping when all connections from the private IP address are disconnected.

Dynamic NAT444 uses ACLs to implement translation control. It processes only packets that match an ACL permit rule.

Dynamic NAT444 supports port block extending. If the ports in the port block for a private address are all occupied, dynamic NAT444 translates the source port to a port in an extended port block.

Advanced settings

NAT address group

A NAT address group is a set of address ranges. Dynamic NAT uses a NAT address group to translate a larger group of private IP addresses.

NAT444 address group

A NAT444 address group is used to perform dynamic NAT444. A NAT444 address group is similar to a NAT address group. The difference is that a NAT444 address group includes port block parameters, such as a port range, a port block size, and an extended port block number.

Port block group

A port block group is used to perform static NAT444. A port block group includes private IP addresses, public IP addresses, a port range, and a port block size. The NAT444 gateway uses these parameters to calculate static NAT444 mappings and performs NAT444 accordingly.

Internal server group

An internal server group is used to configure load-sharing NAT Server. The internal servers in the group provide the same service to external hosts. When an external host sends a request to the public IP address mapped to the internal server group, the NAT device chooses an internal server based on the weight and number of connections of the servers.

PAT

PAT supports the following mappings:

- **Endpoint-Independent Mapping**—Uses the same IP and port mapping (EIM entry) for packets from the same source IP and port to any destination. EIM allows external hosts to access the internal hosts by using the translated IP address and port. It allows internal hosts behind different NAT gateways to access each other.
- **Address and Port-Dependent Mapping**—Uses different IP and port mappings for packets from the same source IP and port to different destination IP addresses and ports. APDM allows an external host to access an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.

NAT with DNS mapping

NAT with DNS mapping allows an internal host to access an internal server on the same private network by using the domain name of the internal server when the DNS server is on the public network.

NAT with DNS mapping must operate with NAT Server. DNS mapping maps the domain name to the public IP address, public port number, and protocol type of the internal server. NAT Server maps the public IP and port to the private IP and port of the internal server.

DNS mapping can also be used by DNS ALG. The DNS reply from the external DNS server contains only the domain name and public IP address of the internal server in the payload. The NAT interface might have multiple internal servers configured with the same public IP address but different private IP addresses. DNS ALG might find an incorrect internal server by using only the public IP address. If a DNS mapping is configured, DNS ALG can obtain the public IP address, public port number, and protocol type of the internal server by using the domain name. Then it can find the correct internal server by using the public IP address, public port number, and protocol type of the internal server.

NAT hairpin

NAT hairpin allows internal hosts to access each other through NAT.

NAT hairpin includes P2P and C/S modes:

- **P2P**—Allows internal hosts to access each other through NAT.
To configure the P2P mode, you must configure outbound PAT on the interface connected to the external network and enable the EIM mapping mode. Internal hosts first register their public addresses to an external server. Then, the hosts communicate with each other by using the registered IP addresses.
- **C/S**—Allows internal hosts to access internal servers through NAT.
In C/S mode, the source and destination IP address of a packet are translated on the interface connected to the internal network. The destination IP address of the packet going to the internal server is translated by matching the NAT Server configuration. The source IP address is translated by matching the outbound dynamic or static NAT entries.

NAT hairpin typically operates with NAT Server, outbound dynamic NAT, or outbound static NAT. They must be configured on interfaces of the same interface card. Otherwise, NAT hairpin cannot function correctly.

NAT with ALG

NAT with ALG translates address or port information in the application layer payloads to ensure connection establishment.

NAT logging

- NAT session logging
NAT session logging records NAT session information, including translation information, access information, and flow information.
A NAT device generates NAT session logs for the following events:
 - NAT session establishment.
 - NAT session removal. This event occurs when you add a configuration with a higher priority, remove a configuration, and change ACLs, when a NAT session ages out, or when you manually delete a NAT session.
 - Active NAT session logging.
- NAT444 user logging
NAT444 user logs are used for user tracing. The NAT444 gateway generates a user log whenever it assigns or withdraws a port block. The log includes the private IP address, public IP address, and port block. You can use the public IP address and port numbers to locate the user's private IP address from the user logs.
A NAT444 gateway generates NAT user logs when one of the following events occurs:
 - A port block is assigned.
For static NAT444, the NAT444 gateway generates a user log when it translates the first connection from a private IP address.

For dynamic NAT444, the NAT444 gateway generates a user log when it assigns or extends a port block for a private IP address.

- A port block is withdrawn.

For static NAT444, the NAT444 gateway generates a user log when all connections from a private IP address are disconnected.

For dynamic NAT444, the NAT444 gateway generates a user log when all the following conditions are met:

- All connections from a private IP address are disconnected.
- The port blocks (including the extended ones) assigned to the private IP address are withdrawn.
- The corresponding mapping entry is deleted.

- NAT444 alarm logging

If the public IP addresses, port blocks, or ports in selected port blocks (including extended ones) are all occupied, the NAT444 gateway cannot perform address translation and packets will be dropped. To monitor the usage of public IP addresses and port block resources, you can configure NAT444 alarm logging.

A NAT444 gateway generates alarm logs when one of the following occurs:

- The ports in the selected port block of a static NAT444 mapping are all occupied.
- The ports in the selected port blocks (including extended ones) of a dynamic NAT444 mapping are all occupied.
- The public IP addresses and port blocks for dynamic NAT444 are all assigned.

Restrictions and guidelines

When you configure NAT, follow these restrictions and guidelines:

- Do not configure inbound static NAT alone. Typically, inbound static NAT functions with outbound dynamic NAT, NAT Server, or outbound static NAT to implement bidirectional NAT.
- The following shows the priorities of different NAT features in descending order:
 - NAT Server.
 - Static NAT.
 - Static NAT444.
 - Dynamic NAT and dynamic NAT444.

Dynamic NAT and dynamic NAT444 have the same priority. They are matched in the descending order of ACL numbers.
- The address ranges in a NAT address group cannot overlap with each other.
- The number of IP addresses in a NAT address group cannot be smaller than the number of security engines.
- In an internal server group, an internal server with a larger weight provides a larger percentage of service.
- Before configuring NAT444 user and alarm logging, you must configure the custom NAT444 log generation and outputting functions.

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 do 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 specified ACL has rules, only users permitted by the ACL can log in to the Web interface through HTTP or HTTPS.

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 do 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.

SSH

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.

The device can act as an SSH server and provide the following services for SSH clients:

- **Secure Telnet**—Stelnet provides secure and reliable network terminal access services.
- **Secure FTP**—SFTP uses SSH connections to provide secure file transfer based on SSH2.
- **Secure Copy**—SCP offers a secure method to copy files based on SSH2.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 provides better performance and security than SSH1. In non-FIPS mode, the device that acts as an SSH server supports both SSH2 and SSH1. In FIPS mode, it supports only SSH2.

When the device acts as an SSH server, it supports using local password authentication to examine the validity of the username and password of an SSH client. After the SSH client passes the authentication, the two parties establish a session for data exchange.

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.

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, port ID, and so on. The device stores the device information in LLDPDUs from the LLDP neighbors in a standard MIB. LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

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. When the TTL value in the Time To Live TLV carried in the LLDP frame becomes zero, the information ages out immediately.

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

$$\text{TTL} = \text{Min} (65535, (\text{TTL multiplier} \times \text{LLDP frame transmission interval} + 1))$$

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.

Log

Log levels

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

Table 4 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.

Security features

Packet filter

Packet filter uses ACLs to filter incoming or outgoing packets on interfaces. 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.

QoS

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 an 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 and SSH packets.

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 automatically resolves 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 and 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.

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 multiple priority maps. If a default priority map cannot meet your requirements, you can modify the priority map as required.

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.

802.1 X 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.

802.1 X 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.

EAD assistant

Endpoint Admission Defense (EAD) is an INTELBRAS 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.

802.1X SmartOn

The SmartOn feature is mutually exclusive with the 802.1X online user handshake feature.

When the device sends a unicast EAP-Request/Notification packet to the client, it starts the SmartOn client timeout timer.

- If the device does not receive any EAP-Response/Notification packets from the client within the timeout timer, it retransmits the EAP-Request/Notification packet to the client. After the device has made the maximum retransmission attempts but received no response, it stops the 802.1X authentication process for the client.
- If the device receives an EAP-Response/Notification packet within the timer or before the maximum retransmission attempts have been made, it starts the SmartOn authentication. If the SmartOn switch ID and the MD5 digest of the SmartOn password in the packet match those on the device, 802.1X authentication continues for the client. Otherwise, the device denies the client's 802.1X authentication request.

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 RADIUS authentication**—The device works with a remote RADIUS 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.
 - The working directory for FTP, SFTP, and SCP users is the root directory of the device. 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 RADIUS authorization**—The device works with a remote RADIUS 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. 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 RADIUS accounting**—The device works with a remote RADIUS 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 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 come 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 INTELBRAS INC to correctly log out users when a card reboots on the distributed device to which the users connect.

- **Session-control**—ARADIUS server running on INTELBRAS INC 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.

Local users

The device performs local authentication, authorization, and accounting based on the locally configured user information, including the username, password, and authorization attributes. Each local user is identified by the username.

User groups simplify local user configuration and management. A user group contains a group of local users and has a set of local user attributes. The user attributes of a user group apply to all users in this group.

System features

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 5](#) shows the ACL types available on the switch and the fields that can be used to filter or match traffic.

Table 5 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	<ul style="list-style-type: none">• Source IPv4 address.• Destination IPv4 address.• Packet priority.• Protocol number.• Other Layer 3 and Layer 4 header fields.
		IPv6	<ul style="list-style-type: none">• Source IPv6 address.• Destination IPv6 address.

Type	ACL number	IP version	Match criteria
			<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 6](#) lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

Table 6 Sort ACL rules in depth-first order

ACL category	Sequence of tie breakers
IPv4 basic ACL	<ol style="list-style-type: none"> VPN instance. More 0s in the source IPv4 address wildcard (more 0s means a narrower IPv4 address range). Rule configured earlier.
IPv4 advanced ACL	<ol style="list-style-type: none"> VPN instance. Specific protocol number. More 0s in the source IPv4 address wildcard mask. More 0s in the destination IPv4 address wildcard. Narrower TCP/UDP service port number range. Rule configured earlier.
IPv6 basic ACL	<ol style="list-style-type: none"> VPN instance. Longer prefix for the source IPv6 address (a longer prefix means a narrower IPv6 address range). Rule configured earlier.
IPv6 advanced ACL	<ol style="list-style-type: none"> VPN instance. Specific protocol number. Longer prefix for the source IPv6 address. Longer prefix for the destination IPv6 address. Narrower TCP/UDP service port number range. Rule configured earlier.
Ethernet frame header ACL	<ol style="list-style-type: none"> More 1s in the source MAC address mask (more 1s means a smaller MAC address). More 1s in the destination MAC address mask. 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 numbered 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**—Recurrs 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.

File system management

File systems

Each storage medium on the device has a file system.

File system naming conventions

The system supports the fixed flash memory and swappable USB disks. The name of a file system on the USB disk has the following parts:

- Storage medium type **usb**.
- Sequence number, a lower-case English letter such as a, b, or c.
- Partition number, an integer starting from 0.
- Colon (:).

For example, the file system on the first USB disk is named **usba0:**.



IMPORTANT:

File system names are case sensitive and must be entered in lower case.

Default file system

You are working with the default file system by default after you log in. To specify a file or directory on the default file system, you do not need to specify the file system name. For example, you do not need to specify any location information if you want to save the running configuration to the root directory of the default file system.

Directories

Directories in a file system are structured in a tree form.

Root directory

The root directory is represented by a forwarding slash (/).

Working directory

The working directory is also called the current directory.

The default working directory is the root directory of the flash memory.

Directory naming conventions

When you specify a name for a directory, follow these conventions:

- A directory name can contain letters, digits, and special characters except for asterisks (*), vertical bars (|), forward slashes (/), backward slashes (\), question marks (?), left angle brackets (<), right angle brackets (>), quotation marks ("), and colons (:).
- A directory whose name starts with a dot character (.) is a hidden directory. To prevent the system from hiding a directory, make sure the directory name does not start with a dot character.

Commonly used directories

The device has some factory-default directories. The system automatically creates directories during operation. These directories include:

- **diagfile**—Stores diagnostic information files.
- **license**—Stores license files.

- **logfile**—Stores log files.
- **seclog**—Stores security log files.
- **versionInfo**—Stores software version information files.

Files

File naming conventions

When you specify a name for a file, follow these conventions:

- A file name can contain letters, digits, and special characters except for asterisks (*), vertical bars (|), forward slashes (/), backward slashes (\), question marks (?), left angle brackets (<), right angle brackets (>), quotation marks ("), and colons (:).
- A file whose name starts with a dot character (.) is a hidden file. To prevent the system from hiding a file, make sure the file name does not start with a dot character.

Common file types

The device is shipped with some files. The system automatically creates files during operation. The types of these files include:

- **.ipe file**—Compressed software image package file.
- **.bin file**—Software image file.
- **.cfg file**—Configuration file.
- **.mdb file**—Binary configuration file.
- **.log file**—Log file.

Hidden files and directories

Some system files and directories are hidden. For correct system operation and full functionality, do not modify or delete hidden files or directories.

File system management restrictions and guidelines

To avoid file system corruption, do not install or remove storage media during file system management.

If you remove a storage medium while a directory or file on the medium is being accessed, the device might not recognize the medium when you reinstall it. To reinstall this kind of storage medium, perform one of the following tasks:

- If you were accessing a directory on the storage medium, change the working directory.
- If you were accessing a file on the storage medium, close the file.

Make sure a USB disk is not write protected before an operation that requires the write right on the disk.

Before managing file systems, directories, and files, make sure you know the possible impacts.

File management

You can manage files in the specified directory. The following shows the supported operations:

- **Upload**—The device supports uploading files, including software image files, configuration files, certificate files, local portal webpages, MAP files, customized AP software image files.
- **Download**—The device supports downloading files, including software image files, configuration files, diagnostic information files, and the previously uploaded files.

- **Delete**—The device supports deleting unhidden files. Delete a file with caution. Deleted files cannot be recovered.

License management

To use a license-based feature, you must purchase a formal license or obtain a trial license and install the license for the feature.

The license management feature supports the following operations on the webpages:

- Install licenses. The following installation methods are supported:
 - **Automatic installation**—Access the license management server from the device, and then enter the license key to automatically install the license.
 - **Manual installation**—Request an activation file on the license management platform (<http://www.intelbras.com.br/cn/License>), and then import the activation file to the device to install the license. For information about license request and activation, see *INTELBAS Comware 7 and Comware 9 WLAN Products Licensing Guide*.
- Obtain the DID file of the device.
- Identify features that have been licensed and view brief information about their licenses.
- Compress the license storage area.

Before registering an activation file, make sure the license storage area has sufficient space for installing the new activation file. If the license storage space is not sufficient, compress the license storage area. Compressing the license storage area changes the DID and deletes expired licenses and uninstalled license information. Before you compress the license storage area, back up Uninstall keys and make sure all activation files generated based on the old DID have been installed. These activation files cannot be installed after the compression.

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 HTTP, HTTPS, SSH, Telnet, FTP, PAD, or terminal. A terminal user can access the device through the console 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

This feature controls user access to items and system resources based on user role. Items include commands, features, feature groups, Web pages, XML elements, and MIB nodes. System resources include interfaces and VLANs.

On devices that support multiple users, this feature is used to assign access permissions to user roles that are created for different job functions. Users are given permission to access a set of items

and resources based on the users' user roles. Because user roles are persistent, in contrast to users, separating permissions from users enables easy permission authorization management. When the job responsibilities of a user changes, new users are added, or old users are removed, you only need to change the user roles or assign new user roles.

Permission assignment

Assigning permissions to a user role includes the following:

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

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

For example, a user role has a rule to permit VLAN 10 and has access permission to all VLANs. With this user role, you can create VLAN 10 and enter the view of VLAN 10. However, you cannot create any other VLAN or enter the view of any other VLAN. If the user role has access permission to all VLANs but does not have a rule to permit any VLAN, you cannot configure any VLAN.

User role rules

User role rules permit or deny access to commands, features, feature groups, Web pages, XML elements, or MIB nodes. You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type. All features and their commands are predefined.
- **Feature group rule**—Controls access to the commands of a feature group by command type. You can define a feature group and assign features to the group. The system has two predefined feature groups named L2 and L3. The L2 feature group includes all Layer 2 commands, and the L3 feature group includes all Layer 3 commands. These predefined feature groups are not user configurable. Features in feature groups can overlap.
- **Web menu rule**—Controls access to Web pages by Web type. A Web page is identified by the Web menu that can open the Web page.
- **XML element rule**—Controls access to XML elements by XML element type. An XML element is identified by its Xpath.
- **OID rule**—Controls SNMP access to a MIB node and its child nodes by node type. The path from the root node to that node is uniquely identified by OID.

The commands, features, feature groups, Web menus, XML elements, or MIB nodes are divided into the following types:

- **Read**—Commands, features, feature groups, Web menus, XML elements, or MIB nodes that display configuration and maintenance information.
- **Write**—Commands, features, feature groups, Web menus, XML elements, or MIB nodes that configure the feature in the system.
- **Execute**—Commands, features, feature groups, Web menus, XML elements, or MIB nodes that execute specific functions.

A user role can access the set of permitted commands, features, feature groups, Web pages, XML elements, and MIB nodes specified in the user role rules. The user role rules include predefined and user-defined user role rules. For more information about the user role rule priority, see "[Rule configuration guidelines](#)."

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.

ACLI login user can perform the following tasks on an accessible interface or VLAN:

- Create, remove, or configure the interface or VLAN.
- Enter the interface or VLAN view.
- Apply the interface or VLAN to other objects.

Resource access policies do not control access to the interface or VLAN options in the **display** commands. The CLI login user can specify these options in the **display** commands if the options are permitted by any user role rule.

A Web login user can perform the following tasks on an accessible interface or VLAN:

- Create, remove, or configure the interface or VLAN.
- Apply the interface or VLAN to other objects.

Predefined user roles

The system provides predefined user roles. These user roles have access to all system resources (interfaces and VLANs). However, their access permissions differ, as shown in [Table 7](#).

Among all of the predefined user roles, only the network-admin and level-15 user roles have the following access permissions:


- Access the RBAC feature.
- Modify settings on user lines, including the **user-role**, **authentication-mode**, **protocol inbound**, and **set authentication password** command settings.
- Create, modify, and delete local users and local user groups.

User roles except network-admin and level-15 can only modify their own passwords if they have permissions to configure local users and local user groups.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Table 7 Predefined roles and permissions matrix

User role name	Permissions
network-admin	Accesses all features and resources in the system, except for the display security-logfile summary , info-center security-logfile directory , and security-logfile save commands.
network-operator	<ul style="list-style-type: none"> • Accesses the display commands for features and resources in the system. To display all accessible commands of the user role, use the display role command. • Enables local authentication login users to change their own passwords. • Accesses the command used for entering XML view. • Accesses all read-type Web menu items. • Accesses all read-type XML elements. • Accesses all read-type MIB nodes.
level- <i>n</i> (<i>n</i> = 0 to 15)	<ul style="list-style-type: none"> • level-0—Has access to commands including ping, tracert, ssh2, telnet, and super. Level-0 access rights are configurable. • level-1—Has access to the display commands of features and

User role name	Permissions
	<p>resources in the system. The level-1 user role also has all access rights of the level-0 user role. Level-1 access rights are configurable.</p> <ul style="list-style-type: none"> • level-2 to level-8, and level-10 to level-14—Have no access rights by default. Access rights are configurable. • level-9—Has access to most of the features and resources in the system. If you are logged in with a local user account that has a level-9 user role, you can change the password in the local user account. The following are the major features and commands that the level-9 user role cannot access: <ul style="list-style-type: none"> ○ RBAC non-debugging commands. ○ Local users. ○ File management. ○ Device management. ○ The display history-command all command. • level-15—Has the same rights as network-admin.
security-audit	<p>Security log manager. The user role has the following access rights to security log files:</p> <ul style="list-style-type: none"> • Accesses the commands for displaying and maintaining securitylog files (for example, the dir, display security-logfile summary, and more commands). • Accesses the commands for managing security log files and security log file system (for example, the info-center security-logfile directory, mkdir, and security-logfile save commands). <p>For more information about security log management commands, see information center in <i>Network Management and Monitoring Command Reference</i>. For more information about file system management commands, see <i>Fundamentals Command Reference</i>.</p> <p> IMPORTANT:</p> <p>Only the security-audit user role has access to security log files.</p>
guest-manager	Accesses only guest-related Web pages, and has no access to commands.

User role assignment

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 that 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 items and resources accessible to all the user roles.

Rule configuration guidelines

When you specify a command string for a command line rule, follow the guidelines in [Table 8](#).

Table 8 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do

Rule	Guidelines
	<p>not use a semicolon to separate commands available in user view or any view, for example, display and dir.</p> <p>Each semicolon-separated segment must have a minimum of one printable character.</p> <p>To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon.</p> <p>For example, you must enter system view before you enter interface view. To specify all commands starting with the ip keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string.</p> <p>For another example, the "system ; radius scheme * ;" command string represents all commands that start with the radius scheme keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the radius scheme keywords in system view and all commands in RADIUS scheme view.</p>
Asterisk (*) is the wildcard.	<p>An asterisk represents zero or multiple characters.</p> <p>In a non-last segment, you can use an asterisk only at the end of the segment.</p> <p>In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk.</p> <p>For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.</p>
Keyword abbreviation is allowed.	<p>You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule.</p> <p>For example, "rule 1 deny command dis arp source *" denies access to the display arp source-mac interface and display arp source-suppression commands.</p>
To control the access to a command, you must specify the command immediately after the view that has the command.	<p>To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command.</p> <p>For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the acl basic 3000 command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl * ;".</p>
Do not include the vertical bar (), greater-than sign (>), or double greater-than sign (>>) when you specify display commands in a user role command rule.	<p>The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match.</p> <p>For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a display debugging command but not a display</p>

Rule	Guidelines
	<code>debugging > log</code> command.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
 - `rule 1 permit command ping.`
 - `rule 2 permit command tracert.`
 - `rule 3 deny command ping.`
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- If the MIB node specified in a rule is a child node of the MIB nodes specified in other rules, only this rule takes effect. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
 - `rule 1 permit read write oid 1.3.6.`
 - `rule 2 deny read write oid 1.3.6.1.4.1.`
 - `rule 3 permit read write oid 1.3.6.1.4.`
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, the user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
 - `rule 1 permit read write oid 1.3.6.`
 - `rule 2 deny read write oid 1.3.6.1.4.1.`
 - `rule 3 permit read write oid 1.3.6.1.4.1.`

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 two types: 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 9](#).

Table 9 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 10](#).

Table 10 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

In non-FIPS mode, all the combination levels are available for a password. In FIPS mode, only the level 4 combination is available for a password.

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 less complicated password such as a password containing the username or repeated characters is more likely to be cracked. For higher security, you can configure a password complexity checking policy to ensure that all user passwords are relatively complicated. With such a policy configured, when a user configures a password, the system checks the complexity of the 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 function 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.

Settings

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

System time sources

Correct system time settings are essential for the device to cooperate with other devices on the network. The system time is calculated based on the GMT, time zone, and daylight saving time.

You can use the following methods to obtain the GMT:

- Manually set the GMT.
- Configure NTP or SNTP to obtain the GMT.

The GMT obtained through NTP or SNTP is more secure than the GMT configured at the CLI.

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 provides lower time accuracy.

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 11 NTP/SNTP operating modes

Mode	Operating process	Principle	Application scenario
Client/server	<ol style="list-style-type: none">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. <p>You can configure multiple time servers for a client.</p> <p>This operating mode requires that you specify the IP addresses of the NTP servers on the client.</p>	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	<ol style="list-style-type: none">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. <p>This operating mode requires you to specify the IP address of the symmetric passive peer on the symmetric active peer.</p>	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 feature enables the device to authenticate the received NTP or SNTP packets. This feature ensures that the device obtains the correct GMT.

Tools

Diagnostics

The system provides an interface to collect diagnostics information to help users diagnose and locate issues.

Ping

Use the ping utility to determine if an address is reachable.

Ping sends ICMP echo requests (ECHO-REQUEST) to the destination device. Upon receiving the requests, the destination device responds with ICMP echo replies (ECHO-REPLY) to the source device. The source device outputs statistics about the ping operation, including the number of packets sent, number of echo replies received, and the round-trip time. You can measure the network performance by analyzing these statistics.

Tracert

Tracert enables retrieval of the IP addresses of Layer 3 devices in the path to a destination. In the event of network failure, use tracert to test network connectivity and identify failed nodes.

Contents

Wireless configuration	1
WLAN	1
WLAN access	1
Link layer authentication	2
Authentication mode	4
Authenticator	4
ACL-based access control	5
AP management	5
CAPWAP tunnel	5
AP groups	7
Global configuration	7
AP preprovisioning	7
Region code	8
Auto AP	8
AC backup	8
Hide SSIDs of overloaded 5 GHz radios	8
Configuration prerequisites	8
LED lighting mode	9
AP configuration file	9
Client rate limiting features	9
Client rate limit mode	9
Client rate limit methods	10
Bandwidth guaranteeing features	10
WMM features	10
WMM status	10
WMM settings	10
EDCA parameters and ACK policies	11
EDCA parameters of AC queues for clients	11
Client WMM statistics	11
Traffic statistics	11
WIPS	12
Enabling WIPS	12
Configuring a VSD	12
Configuring device classification	12
Configuring attack detection	15
User-defined attack detection based on signatures	19
Countermeasures	20
Configuring the alarm-ignored device list	20
Whitelist and blacklist features	20
Radio management	20
Radio mode	20
Channel	21
Transmit power	21
Transmission rate	22
MCS	22
VHT-MCS	23
HE-MCS	28
Basic radio functions	34
802.11n functions	36
802.11ac functions	39
802.11ax functions	39
WLAN optimization	40
Disabling a radio as scheduled	40
Configuration restrictions and guidelines	41
WLAN RRM	41
Dynamic frequency selection	41
Transmit power control	42

Bandwidth adjustment	42
WSA	42
Interference identification	42
Channel quality detection	43
RRM collaboration	43
WSA notifications	43
WLAN load balancing	43
Load balancing types	43
Load balancing modes	43
Load balancing parameters	43
Band navigation	44
WLAN mesh	44
MP roles	44
Mesh profile	44
Mesh policy	44
Probe request suppression	45
Mesh peer whitelist	45
WLAN multicast optimization	45
Overview	45
Aging time for multicast optimization entries	45
Multicast optimization policy	45
Multicast optimization entry limits	46
Rate limits for IGMP packets from clients	46
Client probing	46
Wireless locating	46
Locating system	46
Wireless locating mechanism	46
Wireless location common parameters	47
Aer Scout location	47
BLE location	49
CUPID location	50
RF fingerprinting	50
IoT location	51
Bonjour gateway	51
Bonjour service advertisement snooping and caching	51
Bonjour query snooping and response	52
Bonjour service type	53
Bonjour policy	54
Network security	1
Packet filtering	1
QoS	1
QoS policies	1
Priority mapping	1
Port priority	1
Priority map	2
802.1X	2
802.1X architecture	2
802.1X authentication methods	2
Access control methods	2
Port authorization state	3
Periodic online user reauthentication	3
Online user handshake	3
Authentication trigger	3
EAD assistant	3
802.1X SmartOn	4
ISP domains	4
RADIUS	5
RADIUS protocol	5
Enhanced RADIUS features	5
BYOD	6
BYOD endpoint identification rules	6

BYOD authorization	6
Local users	6
Guest management	7
Access control	7
MAC authentication	7
Port security	8
Portal	8
System	9
ACL	9
ACL types	9
Match order	9
Rule numbering	10
Time range	10
VLAN group	10
SSL	11
Overview	11
Restrictions and guidelines	11
Public key	11
Managing local key pairs	11
Managing peer public keys	12
PKI	12
Overview	12
Managing certificates	13
Restrictions and guidelines	14
Tools	15
Packet capture	15
Filter elements	15
Capture filter keywords	16
Capture filter operators	17
Building a capture filter	18
RF Ping	19
Debugging	19

Wireless configuration

WLAN

WLAN access

WLAN access provides access to WLANs for wireless clients.

Wireless service

A wireless service defines a set of wireless service attributes, such as SSID and authentication method.

SSID

A service set identifier is the name of a WLAN.

SSID hiding

APs advertise SSIDs in beacon frames. If the number of clients in a BSS exceeds the limit or the BSS is unavailable, you can enable SSID-hidden to prevent clients from discovering the BSS. When SSID-hidden is enabled, the BSS hides its SSID in beacon frames and does not respond to broadcast probe requests. A client must send probe requests with the specified SSID to access the WLAN. This feature can protect the WLAN from being attacked.

SSID-based user isolation

SSID-based user isolation is applicable to both local forwarding mode and centralized forwarding mode.

When SSID-based user isolation is enabled for a service, the device isolates all wireless users that access the network through the service in the same VLAN.

Traffic forwarding

The client traffic forwarder can be the AC (centralized forwarding) or APs (local forwarding). Using APs to forward client traffic releases the forwarding burden on the AC.

If APs forward client traffic, you can specify a VLAN or a VLAN range for the APs to forward traffic from the specified VLANs. The AC forwards data traffic from the other VLANs.

Wireless service binding

If you bind a wireless service to a radio, the AP creates a BSS that can provide wireless services defined in the wireless service.

You can perform the following tasks when binding a wireless service to a radio:

- Bind a VLAN group to the radio so that clients associated with the BSS will be assigned evenly to all VLANs in the VLAN group.
- Bind the NAS port ID or the NAS ID to the radio to identify the network access server.
- Enable the AP to hide SSIDs in beacon frames.

Quick association

Enabling load balancing or band navigation might affect client association efficiency. For delay-sensitive services or in an environment where load balancing and band navigation are not required, you can enable quick association for a service template.

Quick association disables load balancing or band navigation on clients associated with the service template. The device will not balance traffic or perform band navigation even if these two features are enabled in the WLAN.

Fast BSS transition

802.11r fast BSS transition (FT) minimizes the delay when a client roams from a BSS to another BSS within the same ESS.

FT provides the following message exchanging methods:

- **Over-the-air**—The client communicates directly with the target AP for pre-roaming authentication.
- **Over-the-DS**—The client communicates with the target AP through the current AP for pre-roaming authentication.

Link layer authentication

The original IEEE 802.11 is a Pre Robust Security Network Association (Pre-RSNA) mechanism. This mechanism is vulnerable to security attacks such as key exposure, traffic interception, and tampering. To enhance WLAN security, IEEE 802.11i (the RSNA mechanism) was introduced. You can select either of the Pre-RSNA or RSNA as needed to secure your WLAN.

IEEE 802.11i encrypts only WLAN data traffic. Unencrypted WLAN management frames are open to attacks on secrecy, authenticity, and integrity. IEEE 802.11w offers management frame protection based on the 802.11i framework to prevent attacks such as forged de-authentication and disassociation frames.

Pre-RSNA mechanism

The pre-RSNA mechanism uses the open system and shared key algorithms for authentication and uses WEP for data encryption. WEP uses the stream cipher RC4 for confidentiality and supports key sizes of 40 bits (WEP40), 104 bits (WEP104), and 128 bits (WEP128).

RSNA mechanism

The RSNA mechanism includes WPA and RSN security modes. RSNA provides the following features:

- 802.1X and PSK authentication and key management (AKM) for authenticating user integrity and dynamically generating and updating keys.
 - **802.1X**—802.1X performs user authentication and generates the pairwise master key (PMK) during authentication. The client and AP use the PMK to generate the pairwise transient key (PTK).
 - **Private PSK**—The MAC address of the client is used as the PSK to generate the PMK. The client and AP use the PMK to generate the PTK.
 - **PSK**—The PSK is used to generate the PMK. The client and AP use the PMK to generate the PTK.
- Temporal key integrity Protocol (TKIP) and Counter Mode CBC-MAC Protocol (CCMP) mechanisms for encrypting data.

Key types

802.11i uses the PTK and group temporary key (GTK). The PTK is used in unicast and the GTK is used in multicast and broadcast.

WPA key negotiation

WPA uses EAPOL-Key packets in the four-way handshake to negotiate the PTK, and in the two-way handshake to negotiate the GTK.

WPA3 security mode key negotiation

WPA3 supports the following security modes:

- **WPA3-SAE**—Uses Simultaneous Authentication of Equals (SAE), which replaces PSK in WPA2-Personal to provide more robust password-based authentication. It brings better protections to individual users.

- **WPA3-Enterprise**—Offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data. It ensures the right combination of cryptographic tools is used and sets a consistent baseline of security within a WPA3 network.

RSN key negotiation

RSN uses EAPOL-Key packets in the four-way handshake to negotiate the PTK and the GTK.

Key updates

Key updates enhance WLAN security. Key updates include PTK updates and GTK updates.

- **PTK updates**—Updates for the unicast keys using the four-way handshake negotiation.
- **GTK updates**—Updates for the multicast keys using the two-way handshake negotiation.

Authorization information ignoring

You can configure the device to ignore the authorization information received from the server (local or remote) after a client passes 802.1X or MAC authentication. Authorization information includes VLAN, ACL, and user profile.

Intrusion protection

When the authenticator detects an association request from a client that fails authentication, intrusion protection is triggered. The feature takes one of the following predefined actions on the BSS where the request is received:

- Adds the source MAC address of the request to the blocked MAC address list and drops the request packet. The client at a blocked MAC address cannot establish connections with the AP within a user-configurable block period.
- Temporarily disables wireless services where invalid packets are received. The system stops the BSS where the request is received for a user-configurable stop period.
- Permanently disables wireless services where invalid packets are received. The system stops the BSS where the request is received until the BSS is enabled manually on the radio interface.

Cipher suites

- **TKIP**—TKIP and WEP both use the RC4 algorithm. You can change the cipher suite from WEP to TKIP by updating the software without changing the hardware. TKIP has the following advantages over WEP:
 - TKIP provides longer initialization vectors (IVs) to enhance encryption security. Compared with WEP encryption, TKIP encryption uses the 128-bit RC4 encryption algorithm, and increases the length of IVs from 24 bits to 48 bits.
 - TKIP allows for dynamic key negotiation to avoid static key configuration. TKIP dynamic keys cannot be easily deciphered.
 - TKIP offers MIC and countermeasures. If a packet has been tampered with, it will fail the MIC. If two packets fail the MIC in a period, the AP automatically takes countermeasures by stopping providing services in a period to prevent attacks.
- **CCMP**—CCMP is based on the Counter-Mode/CBC-MAC (CCM) of the Advanced Encryption Standard (AES) encryption algorithm.

CCMP contains a dynamic key negotiation and management method. Each client can dynamically negotiate a key suite, which can be updated periodically to further enhance the security of the CCMP cipher suite. During the encryption process, CCMP uses a 48-bit packet number (PN) to make sure each encrypted packet uses a different PN. This improves WLAN security.

Authentication mode

PSK authentication

PSK authentication requires the same PSK to be configured for both an AP and a client. PSK integrity is verified during the four-way handshake. If PTK negotiation succeeds, the client passes the authentication.

802.1X authentication

The authenticator uses EAP relay or EAP termination to communicate with the RADIUS server.

- **Online user handshake**—The online user handshake feature examines the connectivity status of online 802.1X clients. The device periodically sends handshake messages to online clients. If the device does not receive any responses from an online client after it has made the maximum handshake attempts, the device sets the client to offline state.
- **Online user handshake security**—The online user handshake security feature adds authentication information in the handshake messages. This feature can prevent illegal clients from forging legal 802.1X clients to exchange handshake messages with the device. With this feature, the device compares the authentication information in the handshake response message from a client with that assigned by the authentication server. If no match is found, the device logs off the client.
- **Periodic online user reauthentication**—Periodic online user reauthentication tracks the connection status of online clients, and updates the authorization attributes assigned by the server. The attributes include the ACL, VLAN, and user profile-based QoS.

Dynamic WEP mechanism

IEEE 802.11 provides the dynamic WEP mechanism to ensure that each user uses a private WEP key. For unicast communications, the mechanism uses the WEP key negotiated by the client and server during 802.1X authentication. For multicast and broadcast communications, the mechanism uses the configured WEP key. If you do not configure a WEP key, the AP randomly generates a WEP key for broadcast and multicast communications.

After the client passes 802.1X authentication, the AP sends the client an RC4-EAPOL packet that contains the unicast WEP key ID, and the multicast and broadcast WEP key and key ID. The unicast WEP key ID is 4.

MAC authentication

You can perform MAC authentication on the authenticator (local authentication) or through a RADIUS server. The authenticator can be the AP or AC.

Portal authentication

Portal authentication controls user access to networks. Portal authenticates a user by the username and password the user enters on a portal authentication page. In a portal-enabled network, users can actively initiate portal authentication by visiting the authentication website provided by the portal Web server. Or, they are redirected to the portal authentication page for authentication when they visit other websites. Both IPv4 portal authentication and IPv6 portal authentication are supported.

Authenticator

You can specify the AC or AP to act as the authenticator to perform local or RADIUS-based authentication for WLAN clients. In an AC hierarchical network, the AC refers to a local AC. For information about AC hierarchy, see AC hierarchy configuration in *WLAN Advanced Features Configuration Guide*.

ACL-based access control

This feature controls client access by using ACL rules bound to an AP or a service template.

Upon receiving an association request from a client, the device performs the following actions:

- Allows the client to access the WLAN if a match is found and the rule action is permit.
- Denies the client's access to the WLAN if no match is found or the matched rule has a deny statement.

AP management

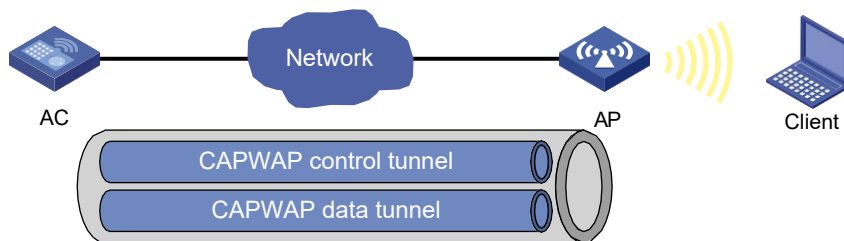
Managing a large number of APs is both time consuming and costly. The fit AP+AC network architecture enables an AC to establish Control And Provisioning of Wireless Access Points (CAPWAP) tunnels with a large number of APs for centralized AP management and maintenance.

CAPWAP tunnel

CAPWAP defines how an AP communicates with an AC. It provides a generic encapsulation and transport mechanism between AP and AC. CAPWAP uses UDP and supports both IPv4 and IPv6.

As shown in [Figure 1](#), an AC and an AP establish a data tunnel to forward data packets and a control tunnel to forward control packets.

Figure 1 CAPWAP tunnel



AC discovery

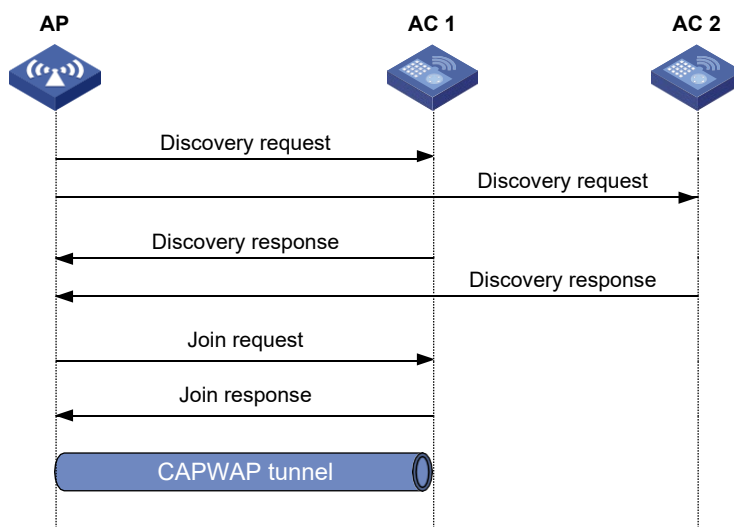
After starting up with zero configurations, an AP automatically creates VLAN-interface 1 and enables the DHCP client, DHCPv6 client, and DNS features on the interface. Then it obtains its own IP address from the DHCP server and discovers ACs by using the following methods in descending order:

- Static IP address:
If AC IP addresses have been manually configured for the AP, the AP sends a unicast discovery request to each AC IP address to discover ACs.
- DHCP options:
 - a. The AP obtains AC IPv4 addresses from Option 138 or Option 43 or AC IPv6 addresses from Option 52 that are sent from the DHCP server.
If the AP obtains IPv4 addresses of ACs from both Option 138 and Option 43, the AP uses the addresses in Option 138.
 - b. The AP sends a unicast discovery request to each received AC address to discover ACs.
For more information about DHCP options, see "DHCP" and "DNS."
- DNS:
 - a. The AP obtains the domain name suffix from the DHCP server.
 - b. The AP adds the suffix to the host name.

- c. The DNS server translates the domain name into IP addresses.
 - d. The AP sends a unicast discovery request to each IP address to discover ACs.
For more information about DNS, see *Layer 3—IP Services Configuration Guide*.
 - Broadcast:
The AP broadcasts discovery requests to IP address 255.255.255.255 to discover ACs.
 - IPv4 multicast:
The AP sends multicast discovery requests to IPv4 address 224.0.1.140 to discover ACs.
 - IPv6 multicast:
The AP sends multicast discovery requests to IPv6 address FF0E::18C to discover ACs.
- The AP does not stop AC discovery until it establishes a CAPWAP tunnel with one of the discovered ACs.

CAPWAP tunnel establishment

Figure 2 Establishing a CAPWAP tunnel



As shown in [Figure 2](#), the AP and an AC establish a CAPWAP tunnel by using the following process:

1. The AP sends a discovery request to each AC to discover ACs.
2. After receiving a discovery request, each AC determines whether to send a discovery response based on its local configuration and the information in the request. A discovery response contains the following information:
 - Whether the AC saves information about the AP.
 - AP connection priority.
 - Load information.
3. After receiving discovery responses, the AP compares information in the responses and selects the optimal AC.
4. The AP sends a join request to the AC.
5. After receiving the join request, the AC examines information in the request to determine whether to provide access services to the AP and sends a join response.
6. After receiving the join response, the AP examines the result code in the response:
 - If the result code represents failure, the AP does not establish a CAPWAP tunnel with the AC.
 - If the result code represents success, the AP establishes a CAPWAP tunnel with the AC.

AP groups

AP groups enable you to configure multiple APs in a batch to reduce configuration workload.

APs in an AP group use the configuration of the group. By default, all APs belong to the system-defined AP group **default-group**. The system-defined AP group cannot be created or deleted.

You can configure AP grouping rules by AP names, serial IDs, MAC addresses, and IP addresses to add APs to the specified AP group. Priorities of these grouping rules are in descending order. If an AP does not match any grouping rules, it is added to the system-defined AP group.

When you configure an AP group, follow these restrictions and guidelines:

- An AP can be added to only one AP group.
- You cannot delete an AP group that contains an AP.
- You cannot create grouping rules for the system-defined AP group.
- You cannot create the same grouping rule for different AP groups. If you do so, the most recent configuration takes effect.

An AP selects AP settings in the following order:

1. Settings configured exclusively for the AP.
2. Settings configured for the AP group where the AP belongs.
3. Global settings.
4. Default settings for global configuration.

Global configuration

Global configuration takes effect on APs in all AP groups.

Global configuration has a lower priority than AP configuration and AP group configuration. An AP uses global settings only when no settings are configured for the AP or the AP group.

AP preprovisioning

AP preprovisioning allows you to configure network settings for APs on an AC. The AC automatically assigns these settings to the APs in run state through CAPWAP tunnels in a batch. This reduces the work load in large WLAN networks.

You must save these settings in the preprovisioned configuration file **wlan_ap_prvs.xml** for the APs. These settings take effect after the APs restart.

This feature takes effect only on master ACs.

You can configure network settings in AP provision configuration or AP group provision configuration. Settings in AP provision configuration have a higher priority.

Preprovisioned settings include the following items:

- Host name of the AC with which the AP establishes a CAPWAP tunnel.
- AP IP address.
- AP gateway address.
- DNS domain name suffix that is used during AC discovery.
- DNS server IP address that is used during AC discovery.
- 802.1X client settings.

Region code

A region code determines characteristics such as available frequencies, available channels, and transmit power level. Set a valid region code before configuring an AP.

To prevent regulation violation caused by region code modification, lock the region code.

Auto AP

The auto AP feature enables APs to connect to an AC without manual AP configuration. The AC names auto APs by their MAC addresses. This feature simplifies configuration when you deploy a large number of APs in a WLAN.

During AC discovery, an AP first connects to an AC that saves information about the AP. If no AC has information about the AP, the AP selects the optimal AC with auto AP enabled to establish a CAPWAP tunnel.

To configure an auto AP, you must use auto AP persistence to convert the auto AP to a manual AP or configure it through an AP group.

For security purposes, use the auto AP feature in conjunction with the auto AP persistence feature. Disable the auto AP feature after all auto APs connect to the AC for the first time. Auto APs are converted to manual APs the first time they are connected to the AC.

AC backup

AC backup enables an AP to establish a CAPWAP tunnel with both the master AC and the backup AC in a VSRP group. In the VSRP group, the AC that is assigned a higher AP connection priority is the master AC. The AC whose IP address is configured on the master AC is the backup AC. The master AC synchronizes AP and client information to the backup in real time. When the master AC fails, the backup AC takes over to avoid service interruption.

Hide SSIDs of overloaded 5 GHz radios

With this feature enabled, the system hides a 5GHz radio's SSID to avoid client overloading if the following conditions are met:

- The number of online clients associated with the 5GHz radio reaches or exceeds the session threshold.
- The gap of online client quantity between the radio and the other 5GHz radio on the same AP reaches the gap threshold.

If the associated client quantity drops below the session threshold or the quantity gap drops below the gap threshold, the system shows the radio's SSID again.

When radar avoidance occurs on a 5 GHz radio, all clients on the radio will be transferred to the other 5 GHz radio of the same AP. As a result, the 5 GHz radio might be overloaded. To resolve this issue, you can enable **Log Off Clients** to force half of the clients on a 5 GHz radio to log off when the other 5 GHz radio is no longer used by the radar.

Hiding SSIDs of overloaded 5 GHz radios takes effect only on APs with multiple 5GHz radios.

Configuration prerequisites

Before you manage APs, complete the following tasks:

- Create a DHCP address pool on the DHCP server to assign IP addresses to APs.

- If DHCP options are used for AC discovery, perform either of the following tasks for the specified DHCP address pool on the DHCP server:
 - Configure Option 138 or Option 43 to specify AC IPv4 address.
 - Configure Option 52 to specify AC IPv6 address.
- If DNS is used for AC discovery, configure the IP address of the DNS server and the AC domain name suffix in the specified DHCP address pool on the DHCP server. Then configure the mapping between the domain name and the AC IP address on the DNS server.
- Make sure the APs and the AC can reach each other.

For more information about DHCP and DNS configuration, see "DHCP" and "DNS."

LED lighting mode

You can configure LEDs on an AP to flash in the following modes:

- **quiet**—All LEDs are off.
- **awake**—All LEDs flash once every minute. Support for this mode depends on the AP model.
- **always-on**—All LEDs are steady on. Support for this mode depends on the AP model.
- **normal**—How LEDs flash in this mode varies by AP model. This mode can identify the running status of an AP.

AP configuration file

Deploy a configuration file to an AP if you want to update its configuration file or configure features that require a configuration file. For example, to configure a user profile for an AP in local forwarding mode, you must write related commands to a configuration file and then deploy the configuration file to the AP. The configuration file takes effect when the CAPWAP tunnel to the AC is in Run state. It does not survive an AP reboot.

Make sure the configuration file is stored in the storage medium of the AC.

This feature takes effect every time the specified AP comes online.

An AP can only use its main IP address to establish a CAPWAP tunnel to the AC if the AP is configured by using a configuration file.

Client rate limiting features

Client rate limiting prevents aggressive use of bandwidth by one client and ensures fair use of bandwidth among clients associated with the same AP.

Client rate limit mode

The following modes are available for client rate limiting:

- **Dynamic mode**—Sets the total bandwidth shared by all clients. The rate limit for each client is the total rate divided by the number of online clients. For example, if the total rate is 10 Mbps and five clients are online, the rate limit for each client is 2 Mbps.
- **Static mode**—Sets the bandwidth that can be used by each client. When the rate limit multiplied by the number of associated clients exceeds the available bandwidth provided by the AP, the clients might not get the set bandwidth.

You can configure the client rate limit mode only for service-based and radio-based client rate limiting.

Client rate limit methods

You can use the following methods to limit the traffic rate:

- **Client-type-based client rate limiting**—The setting takes effect on all clients. Traffic rate of each client type cannot exceed the corresponding setting.
- **Service-based client rate limiting**—The setting takes effect on all clients associated with the same wireless service.
- **Radio-based client rate limiting**—The setting takes effects on all clients associated with the same radio or a group of radios.

If more than one method and mode are configured, all settings take effect. The rate for a client will be limited to the minimum value among all the client rate limiting settings.

Bandwidth guaranteeing features

Bandwidth guaranteeing provides the following functions:

- Ensures that traffic from all BSSs can pass through freely when the network is not congested.
- Ensures that each BSS can get the guaranteed bandwidth when the network is congested.

This feature improves bandwidth efficiency and maintains fair use of bandwidth among WLAN services. For example, you assign SSID1, SSID2, and SSID3 25%, 25%, and 50% of the total bandwidth. When the network is not congested, SSID1 can use all idle bandwidth in addition to its guaranteed bandwidth. When the network is congested, SSID1 is guaranteed with 25% of the bandwidth.

This feature applies only to AP-to-client traffic.

WMM features

An 802.11 network provides contention-based wireless access. To provide applications with QoS services, IEEE developed 802.11e for 802.11-based WLANs.

While IEEE 802.11e was being standardized, Wi-Fi Alliance defined the Wi-Fi Multimedia (WMM) standard to allow QoS provision devices of different vendors to interoperate. WMM enables a WLAN to provide QoS services, so that audio and video applications can have better performance in WLANs.

WMM status

You can view the WMM enabling status for each AP that is connected to the AC.

WMM settings

You can configure the maximum number of SVP mappings, CAC policies, and allowed clients.

SVP mapping assigns packets that have the protocol ID 119 in the IP header to the AC-VI or AC-VO queue to provide SVP packets with the specified priority. When SVP mapping is disabled, SVP packets are assigned to the AC-BE queue.

Connect Admission Control (CAC) limits the number of clients that can use high-priority ACs (AC-VO and AC-VI) to make sure there is enough bandwidth for these clients. If a high-priority AC (AC-VO or AC-VI) is required, a client must send a request to the AP. The AP returns a positive or negative response based on the channel-usage-based admission policy or client-based admission policy. If the request is rejected, the AP assigns AC-BE to clients.

EDCA parameters and ACK policies

You can view and modify the EDCA parameters and ACK policies.

EDCA is a channel contention mechanism defined by WMM to preferentially transmit packets with high priority and allocate more bandwidth to such packets.

WMM defines the following EDCA parameters:

- **Arbitration inter-frame spacing number**—In 802.11-based WLAN, each client has the same idle duration (DIFS), but WMM defines an idle duration for each AC. The idle duration increases as the AIFSN increases.
- **Exponent form of CWmin/Exponent form of CWmax**—ECWmin/ECWmax determines the backoff slots, which increase as the two values increase.
- **Transmission opportunity limit**—TXOP limit specifies the maximum time that a client can hold the channel after a successful contention. A larger value represents a longer time. If the value is 0, a client can send only one packet each time it holds the channel.

WMM defines the following ACK policies:

- **Normal ACK**—The recipient acknowledges each received unicast packet.
- **No ACK**—The recipient does not acknowledge received packets during wireless packet exchange. This policy improves the transmission efficiency in an environment where communication quality is strong and interference is weak. If communication quality deteriorates, this policy might increase the packet loss rate.

EDCA parameters of AC queues for clients

You can view and modify EDCA parameters, and enable or disable a CAC policy.

Client WMM statistics

You can view the following information:

- The device's basic information such as SSID.
- Data traffic statistics.
- APSD attribute for an AC queue.

U-APSD is a power saving method defined by WMM to save client power. U-APSD enables clients in sleep mode to wake up and receive the specified number of packets only after receiving a trigger packet. U-APSD improves the 802.11 APSD power saving mechanism.

U-APSD is automatically enabled after you enable WMM.

Traffic statistics

You can view the following information:

- User priority for packets from wired networks.
- Traffic Identifier.
- Traffic direction.
- Surplus bandwidth allowance.

WIPS

Wireless Intrusion Prevention System (WIPS) helps you monitor your WLAN, detect attacks and rogue devices, and take countermeasures. WIPS provides a complete solution for WLAN security.

WIPS contains the network management module, the AC, and sensors (APs enabled with WIPS). They provide the following functions:

- The sensors monitor the WLAN, collect channel information, and report the information to the AC for further analysis.
- The AC determines attacks and rogue devices, takes countermeasures, and triggers alarms.
- The network management module allows you to configure WIPS in the Web interface. It provides configuration management, report generation, and alarm management functions.

WIPS provides the following features:

- **Attack detection**—WIPS detects attacks by listening for 802.11 frames and triggers alarms to notify the administrator.
- **Signature-based attack detection**—WIPS provides signature-based attack detection. A signature contains a packet identification method and actions to take on the matching packets.
- **Device classification**—WIPS identifies wireless devices by listening for 802.11 frames and classifies the devices based on the classification rules.
- **Countermeasures**—WIPS enables you to take countermeasures against rogue devices.

Enabling WIPS

Before enabling WIPS for a radio of an AP, you must add the AP to a virtual security domain (VSD).

Configuring a VSD

You can apply a classification policy, attack detection policy, signature policy, or countermeasure policy to a VSD to enable the policy to take effect on the radios in the VSD.

Configuring device classification

Classification policy

You can enable WIPS to classify devices by using either of the following methods:

- **Automatic classification**—WIPS automatically classifies devices by adding the MAC addresses, OUIs, or SSIDs of the devices to the specified lists. WIPS also allows you to classify APs by using user-defined AP classification rules.
- **Manual classification**—You manually specify a category for a device. Manual classification is applicable only to APs.

If you configure both automatic classification and manual classification, manual classification takes effect.

AP classification

As shown in [Table 1](#), WIPS classifies detected APs according to the predefined classification rules.

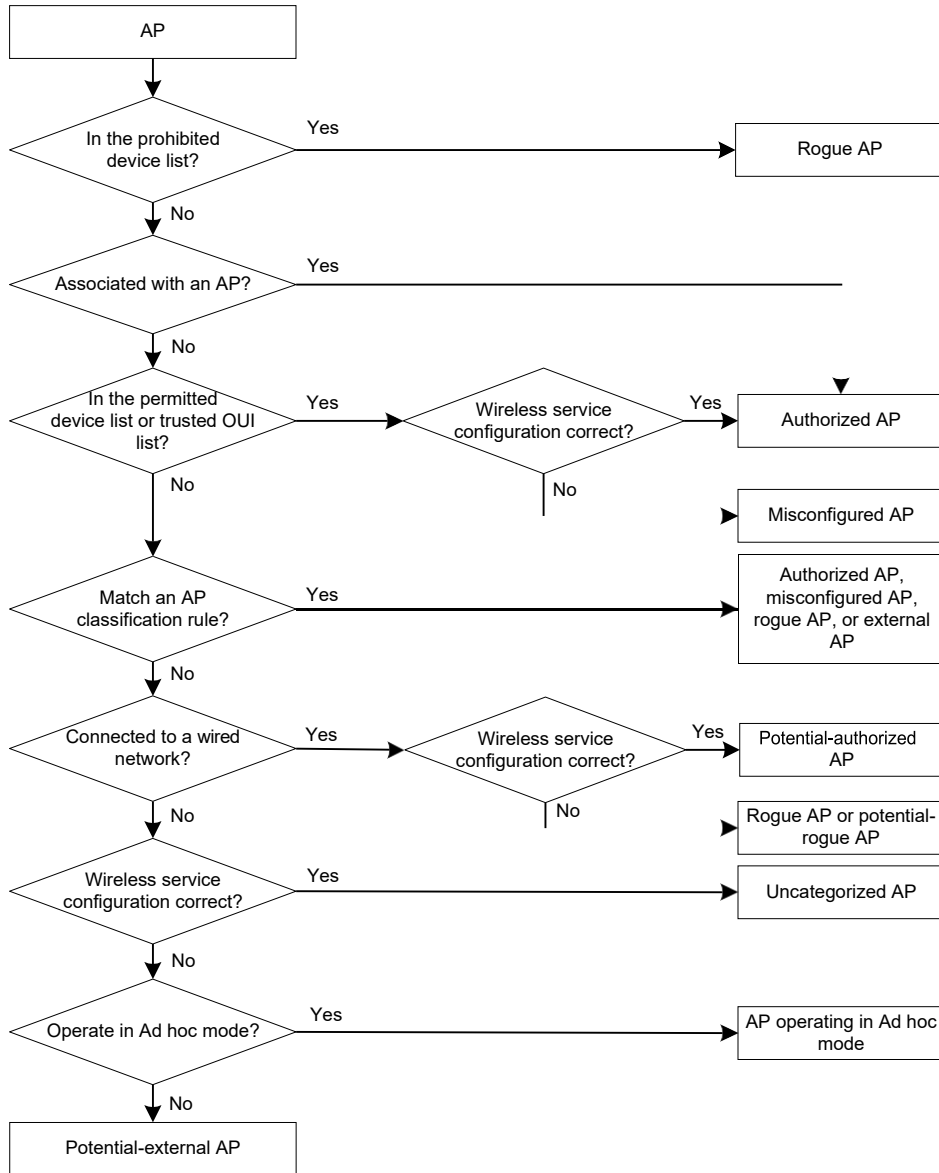
Table 1 AP classification

Category	Description	Classification rule
Authorized AP	An AP that is permitted in the WLAN.	<ul style="list-style-type: none">• Not in the prohibited device list.• Has been connected to the AC.

Category	Description	Classification rule
		<ul style="list-style-type: none"> Configured as an authorized AP.
Rogue AP	An AP that cannot be used in the WLAN.	<ul style="list-style-type: none"> In the prohibited device list. Not in the OUI configuration file. Configured as a rogue AP.
Misconfigured AP	An AP that can be used in the WLAN but has incorrect configuration.	<ul style="list-style-type: none"> In the permitted device list but with an incorrect SSID. Not in the prohibited device list but in the OUI configuration file. In the trusted OUI list or permitted device list but not connected to the AC.
External AP	An AP that is in an adjacent WLAN.	N/A
Ad hoc	An AP operating in Ad hoc mode. WIPS detects Ad hoc APs by listening to beacon frames.	N/A
Potential-authorized AP	An AP that is possibly authorized.	<p>Not in any of the following lists:</p> <ul style="list-style-type: none"> Permitted device list. Prohibited device list. Trusted OUI list.
Potential-rogue AP	An AP that is possibly a rogue AP.	<p>Has incorrect wireless configuration and is not in any of the following lists:</p> <ul style="list-style-type: none"> Permitted device list. Prohibited device list. Trusted OUI list. <p>If the wired port on an AP has been connected to the network, the AP is a rogue AP.</p>
Potential-external AP	An AP that is possibly an external AP.	<ul style="list-style-type: none"> Has incorrect wireless service configuration. The wired port has not been connected to the network. Not in any of the following lists: <ul style="list-style-type: none"> Permitted device list. Prohibited device list. Trusted OUI list.
Uncategorized AP	An AP whose category cannot be determined.	N/A

WIPS classifies detected APs by following the procedure shown in [Figure 3](#).

Figure 3 AP classification flow



Client classification

As shown in [Table 2](#), WIPS classifies detected clients according to the predefined classification rules.

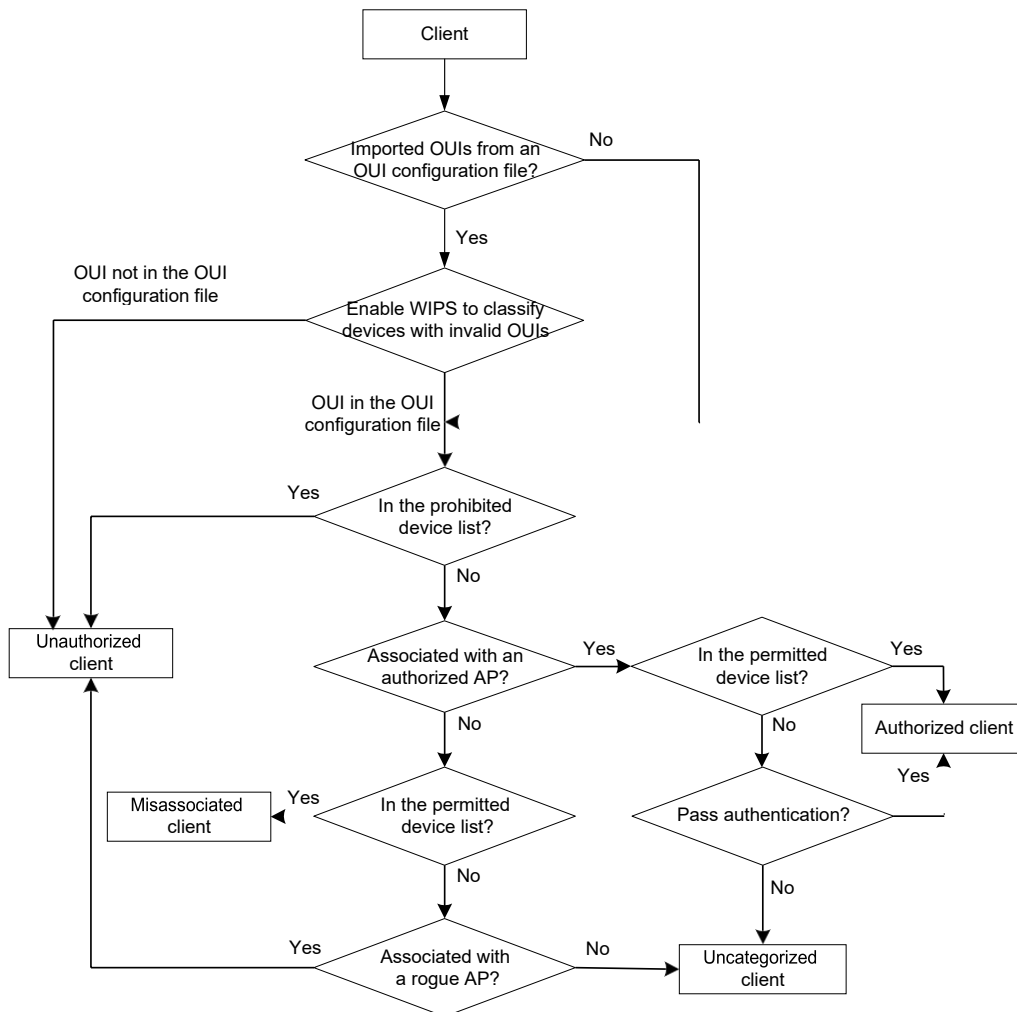
Table 2 Client classification

Category	Description	Classification rule
Authorized client	A client that is permitted in the WLAN.	<ul style="list-style-type: none"> In the permitted device list and associated with an authorized AP. Has passed authentication and is associated with an authorized AP.
Unauthorized client	A client that cannot be used in the WLAN.	<ul style="list-style-type: none"> In the prohibited device list. Associated with a rogue AP. Not in the OUI configuration file.
Misassociated client	A client that is associated with an unauthorized AP.	In the permitted device list but associated with an unauthorized AP. A misassociated client might

Category	Description	Classification rule
		bring security threats to the network.
Uncategorized client	A client whose category cannot be determined.	N/A

WIPS classifies detected clients by following the procedure shown in [Figure 4](#).

Figure 4 Client classification flow



Configuring attack detection

WIPS detects attacks by listening to 802.11 frames and triggers alarms to notify the administrator.

Device entry attack detection

Attackers can send invalid packets to WIPS to increase processing costs. WIPS periodically examines the learned device entries to determine whether to rate limit device entry learning. If the number of AP or client entries learned within the specified interval exceeds the threshold, WIPS triggers an alarm and stops learning new entries.

Flood attack detection

An AP might be facing a flood attack if it receives a large number of same-type frames within a short period of time. To prevent the AP from being overwhelmed, WIPS periodically examines incoming

packet statistics, and alarms when it detects a suspicious flood attack. WIPS can detect the following flood attacks:

- **Probe request/association request/reassociation request flood attack**—Floods the association table of an AP by imitating many clients sending probe requests/association requests/reassociation requests to the AP.
- **Authentication request flood attack**—Floods the association table of an AP by imitating many clients sending authentication requests to the AP.
- **Beacon flood attack**—Floods beacon frames imitating a large number of fake APs to interrupt client association.
- **Block Ack flood attack**—Floods Block Ack frames to the AP to interrupt the operation of the Block Ack mechanism.
- **RTS/CTS flood attack**—Floods RTS/CTS frames to reserve the RF medium and force other wireless devices sharing the RF medium to hold back their transmissions. This attack takes advantage of vulnerabilities of the virtual carrier mechanism.
- **Broadcast/unicast deauthentication flood attack**—Spoofs deauthentication frames from the AP to the associated clients to disassociate the clients from the AP. This attack can rapidly terminate wireless services to multiple clients.
- **Broadcast/unicast disassociation flood attack**—Spoofs disassociation frames from the AP to the associated clients to disassociate the clients from the AP. This attack can rapidly terminate wireless services to multiple clients.
- **EAPOL-start flood attack**—Exhausts the AP's resources by imitating many clients sending EAPOL-start frames defined in IEEE 802.1X to the AP.
- **Null data flood attack**—Spoofs null data frames from a client to the AP. The AP determines that the client is in power save mode and buffers frames for the client. When the aging time of the buffered frames expires, the AP discards the frames. This interrupts the client's communication with the AP.
- **EAPOL-logoff flood attack**—The IEEE 802.1X standard defines the authentication protocol using Extensible Authentication Protocol over LANs (EAPOL). A client needs to send an EAPOL-logoff frame to terminate the session with an AP. The EAPOL-logoff frames are not authenticated, and an attacker can spoof EAPOL-logoff frames to disassociate a client.
- **EAP-success/failure flood attack**—In a WLAN using 802.1X authentication, an AP sends an EAP-success or EAP-failure frame to a client to inform authentication success or failure. An attacker can spoof the MAC address of an AP to send EAP-success or EAP-failure frames to a client to disrupt the authentication process.

Malformed packet detection

WIPS determines that a frame is malformed if the frame matches the criteria shown in [Table 3](#), and then it triggers alarms and logs. WIPS can detect 16 kinds of malformed packets.

Table 3 Malformed frame match criteria

Detection type	Applicable frames	Match criteria
Duplicate IE detection	All management frames	Duplicate IE. This type of detection is not applicable to vendor-defined IEs.
FATA-Jack detection	Authentication frames	The value of the authentication algorithm number is 2.
Abnormal IBSS and ESS setting detection	<ul style="list-style-type: none"> • Beacon frames • Probe response frames 	Both IBSS and ESS are set to 1.
Invalid source address detection	All management frames	<ul style="list-style-type: none"> • The TO DS is 1, indicating that the frame is sent to the AP by a client. • The source MAC address of the frame is a multicast or broadcast

Detection type	Applicable frames	Match criteria
		address.
Malformed association request frame detection	Association request frames	The frame length is 0.
Malformed authentication request frame detection	Authentication request frames	<ul style="list-style-type: none"> The authentication algorithm number does not conform to the 802.11 protocol and is larger than 3. The authentication transaction sequence number is 1 and the status code is not 0. The authentication transaction sequence number is larger than 4.
Invalid deauthentication code detection	Deauthentication frames	The reason code is 0 or is in the range of 67 to 65535.
Invalid disassociation code detection	Disassociation frames	The reason code is 0 or is in the range of 67 to 65535.
Malformed HT IE detection	<ul style="list-style-type: none"> Beacon frames Probe responses Association responses Reassociation requests 	<ul style="list-style-type: none"> The SM power save value for the HT capabilities IE is 2. The secondary channel offset value for the HT operation IE is 2.
Invalid IE length detection	All management frames	The IE length does not conform to the 802.11 protocol.
Invalid packet length detection	All management frames	The remaining length of the IE is not zero after the packet payload is resolved.
Malformed probe response frame detection	Probe response frames	The frame is not a mesh frame and its SSID length is 0.
Oversized EAPOL key detection	EAPOL-Key frames	The TO DS is 1 and the length of the key is larger than 0.
Oversized SSID detection	<ul style="list-style-type: none"> Beacon frames Probe requests Probe responses Association request frames 	The SSID length is larger than 32.
Redundant IE detection	All management frames	The IE is not a necessary IE to the frame and is not a reserved IE.
Oversized duration detection	<ul style="list-style-type: none"> Unicast management frames Unicast data frames RTS, CTS, and ACK frames 	The packet duration value is larger than the specified threshold.

Attack detection

- Spoofing attack detection

In a spoofing attack, the attacker sends frames on behalf of another device to threaten the network. WIPS supports detection of the following spoofing attacks:

- **Frame spoofing**—A fake AP spoofs an authorized AP to send beacon or probe response frames to induce clients to associate with it.

- **AP MAC address spoofing**—A client spoofs an authorized AP to send deauthentication or disassociation frames to other clients. This can cause the clients to go offline and affect the correct operation of the WLAN.
- **Client MAC address spoofing**—A fake AP spoofs an authorized client to associate with an authorized AP.
- Weak IV detection

When the RC4 encryption algorithm, used by the WEP security protocol, uses an insecure IV, the WEP key is more likely to be cracked. Such an insecure IV is called a weak IV. WIPS prevents this kind of attack by detecting the IV in each WEP packet.
- Windows bridge detection

When a wireless client connected to a wired network establishes a Windows bridge through the wired NIC, the client can bridge an external AP with the internal network. This might bring security problems to the internal network. WIPS detects Windows bridges by analyzing data frames sent by associated clients.
- Detection on clients with the 40 MHz bandwidth mode disabled

802.11n devices support both the 20 MHz and 40 MHz bandwidth modes. If the 40 MHz bandwidth mode is disabled on a client, other clients associated with the same AP as the client must also use the 20 MHz bandwidth. This affects network throughput and efficiency.

WIPS detects such clients by detecting probe request frames sent by the clients.
- Omerta attack detection

Omerta is a DoS attack tool based on the 802.11 protocol. It sends disassociation frames with the reason code 0x01 to disassociate clients. Reason code 0x01 indicates an unknown disassociation reason. WIPS detects Omerta attacks by detecting the reason code of each disassociation frame.
- Unencrypted device detection

An authorized AP or client that is transmitting unencrypted frames might bring security problems to the network. WIPS detects unencrypted devices by analyzing the frames sent the by authorized APs or clients.
- Hotspot attack detection

An attacker sets up a rogue AP with the same SSID as a hotspot to lure the clients to associate with it. After the clients associate with the malicious AP, the attacker initiates further attacks to obtain client information.

You can configure a hotspot file to enable WIPS to detect hotspot attacks.
- HT-greenfield AP detection

An AP operating in HT-greenfield mode might cause collisions, errors, and retransmissions because it cannot communicate with 802.11a/b/g devices. WIPS detects HT-greenfield APs by analyzing the beacon frames or probe response frames sent by APs.
- Association/reassociation DoS attack detection

An association/reassociation DoS attack floods the association table of an AP by imitating many clients sending association requests to the AP. When the number of entries in the table reaches the upper limit, the AP cannot process requests from legitimate clients.
- MITM attack detection

In an MITM attack, the attacker sets up a rogue AP and lures a client to associate with it. Then the rogue AP spoofs the MAC address of the client to associate with the authorized AP. When the client and the authorized AP communicate, the rogue AP captures packets from both the client and the authorized AP. The rogue AP might modify the frames and obtain the frame information. WIPS detects MITM attacks by detecting clients that are disassociated from an authorized AP and associated with a honeypot AP.
- Wireless bridge detection

An attacker might intrude on the internal networks through a wireless bridge. When detecting a wireless bridge, WIPS generates an alarm. If the wireless bridge is in a mesh network, WIPS records the mesh link.

- AP channel change detection

WIPS detects the channel change events for APs in the WLAN.

- Broadcast disassociation/deauthentication attack detection

An attacker spoofs a legitimate AP to send a broadcast disassociation or deauthentication frame to log off all clients associated with the AP.

- AP impersonation attack detection

In an AP impersonation attack, a malicious AP that has the same BSSID and ESSID as a legitimate AP lures the clients to associate with it. Then this impersonating AP initiates hotspot attacks or fools the detection system.

WIPS detects AP impersonation attacks by detecting the interval at which an AP sends beacon frames.

- AP flood attack detection

WIPS detects the number of APs in the WLAN and triggers an alarm for an AP flood attack when the number of APs exceeds the specified threshold.

- Honeypot AP detection

In a honeypot AP attack, the attacker sets up a malicious AP to lure clients to associate with it. The SSID of the malicious AP is similar to the SSID of a legitimate AP. After a client associates with a honeypot AP, the honeypot AP initiates further attacks such as port scanning or fake authentication to obtain client information.

WIPS detects honeypot APs by detecting SSIDs of external APs. If the similarity between the SSID of an external AP and the SSID of a legitimate AP reaches the specified threshold, WIPS generates an alarm.

- Power save attack detection

An attacker spoofs the MAC address of a client to send power save on frames to an AP. The AP caches the frames for the client. The attacked client cannot receive data frames because the AP determines that the client is still in power save mode. When the aging time of the cached frames expires, the AP discards the frames. WIPS detects power save attacks by determining the ratio of power save on frames to power save off frames.

- Soft AP detection

A soft AP refers to a client that acts as an AP and provides wireless services. An attacker can access the internal network through a soft AP and then initiate further attacks. WIPS detects soft APs by detecting the interval at which a device switches its roles between client and AP.

- Permitted channel list and prohibited channel detection

After you configure a permitted channel list and enable prohibited channel detection, WIPS determines that channels that are not in the permitted channel list are prohibited channels.

User-defined attack detection based on signatures

WIPS provides user-defined attack detection based on signatures. A signature contains a packet identification method and actions to take on the matching packets. The sensor matches the detected packets against the signature, and takes actions defined in the signature if a packet matches the signature.

A signature can contain a maximum of six subsignatures, which can be defined based on the frame type, MAC address, serial ID, SSID length, SSID, and frame pattern. A packet matches a signature only when it matches all the subsignatures in the signature.

Countermeasures

Rogue devices are susceptible to attacks and might bring security problems to the WLAN. WIPS enables you to take countermeasures against rogue devices.

Configuring the alarm-ignored device list

For wireless devices in an alarm-ignored device list, WIPS only monitors them but does not trigger any alarms.

Whitelist and blacklist features

You can configure the whitelist or blacklists to filter frames from WLAN clients and implement client access control. Multicast and broadcast MAC addresses cannot be added to the whitelist or blacklists.

- **Whitelist**—Contains the MAC addresses of all clients allowed to access the WLAN. Frames from clients not in the whitelist are discarded. This list is manually configured.
- **Static blacklist**—Contains the MAC addresses of clients forbidden to access the WLAN. This list is manually configured.
- **Dynamic blacklist**—Contains the MAC addresses of clients forbidden to access the WLAN through specific APs within the specified aging time. A client is dynamically added to the list if an AP determines this client is a rogue client.

When an AP receives an association request and sends an add mobile message to the AC, the AC performs the following operations to determine whether to permit the client:

1. Searches the whitelist.
 - If the client MAC address does not match any entries in the whitelist, the client is rejected.
 - If there is a match, the client is permitted.
2. Searches the static and dynamic blacklists if no whitelist entries exist.
 - If the client MAC address matches an entry in either blacklist, the client is rejected.
 - If there is no match, or no blacklist entries exist, the client is permitted.

The static blacklist and whitelist configured on the AC apply to all APs connected to the AC, and the dynamic blacklist applies to APs that received attack packets.

Radio management

Radio frequency (RF) is a rate of electrical oscillation in the range of 300 kHz to 300 GHz. WLAN uses the 2.4 GHz band and 5 GHz band radio frequencies as the transmission media. The 2.4 GHz band includes radio frequencies from 2.4 GHz to 2.4835GHz. The 5 GHz band includes radio frequencies from 5.150 GHz to 5.350 GHz and from 5.725 GHz to 5.850 GHz.

The term "radio frequency" or its abbreviation RF is also used as a synonym for "radio" in wireless communication.

Radio mode



CAUTION:

Changing the mode of an enabled radio logs off all associated clients.

IEEE defines the 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax radio modes. [Table 4](#) provides a comparison of these radio modes.

Table 4 Comparison of 802.11 standards

IEEE standard	Frequency band	Maximum rate
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz or 5 GHz	600 Mbps
802.11ac	5 GHz	6900 Mbps
802.11ax	5 GHz	9600 Mbps

Different radio modes support different channels and transmit powers. When you edit the radio mode, the AP automatically selects a channel or transmit power if the new radio mode does not support the original channel or transmit power.

Available radio functions vary by radio mode:

- For 802.11a, 802.11b, and 802.11g radios, you can configure basic radio functions. For more information about basic radio functions, see "[Basic radio functions](#)."
- For 802.11n radios, you can configure basic radio functions and 802.11n functions. For more information about 802.11n functions, see "[802.11n functions](#)."
- For 802.11ac radios, you can configure basic radio functions, 802.11n functions, and 802.11ac functions. For more information about 802.11ac functions, see "[802.11ac functions](#)."
- For 802.11ax radios, you can configure basic radio functions, 802.11n functions, 802.11ac functions, and 802.11ax functions. For more information about 802.11ax functions, see "[802.11ax functions](#)."

NOTE:

[802.11q](#), [802.11n](#), [802.11ac](#), and [802.11ax](#) are backward compatible.

Channel

A channel is a range of frequencies with a specific bandwidth.

The 2.4 GHz band has 14 channels. The bandwidth for each channel is 20 MHz and each two channels are spaced 5 MHz apart. Among the 14 channels, four groups of non-overlapping channels exist and the most commonly used one contains channels 1, 6, and 11.

The 5 GHz band can provide higher rates and is more immune to interference. There are 24 non-overlapping channels designated to the 5 GHz band. The channels are spaced 20 MHz apart with a bandwidth of 20 MHz. The available channels vary by country.

Transmit power

Transmit power reflects the signal strength of a wireless device. A higher transmit power enables a radio to cover a larger area but it brings more interference to adjacent devices. The signal strength decreases as the transmission distance increases.

Transmission rate

Transmission rate refers to the speed at which wireless devices transmit traffic. It varies by radio mode and spreading, coding, and modulation schemes. The following are rates supported by different types of radios:

- **802.11a**—6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.
- **802.11b**—1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps.
- **802.11g**—1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.
- **802.11n**—Rates for 802.11n radios vary by channel bandwidth. For more information, see "[MCS](#)."
- **802.11ac**—Rates for 802.11ac radios vary by channel bandwidth and number of spatial streams (NSS). For more information, see "[VHT-MCS](#)."
- **802.11ax**—Rates for 802.11ax radios vary by channel bandwidth and number of spatial streams (NSS). For more information, see "[HE-MCS](#)."

MCS

Modulation and Coding Scheme (MCS) defined in IEEE 802.11n-2009 determines the modulation, coding, and number of spatial streams. An MCS is identified by an MCS index, which is represented by an integer in the range of 0 to 76. An MCS index is the mapping from MCS to a data rate.

[Table 5](#) and [Table 6](#) show sample MCS parameters for 20 MHz and 40 MHz.

When the bandwidth mode is 20 MHz, MCS indexes 0 through 15 are mandatory for APs, and MCS indexes 0 through 7 are mandatory for clients.

Table 5 MCS parameters for 20 MHz

MCS index	Number of spatial streams	Modulation	Data rate (Mbps)	
			800ns GI	400ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

Table 6 MCS parameters for 40 MHz

MCS index	Number of spatial streams	Modulation	Data rate (Mbps)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

MCS indexes are classified into the following types:

- **Mandatory MCS indexes**—Mandatory MCS indexes for an AP. To associate with an 802.11n AP, a client must support the mandatory MCS indexes for the AP.
- **Supported MCS indexes**—MCS indexes supported by an AP except for the mandatory MCS indexes. If a client supports both mandatory and supported MCS indexes, the client can use a supported rate to communicate with the AP.
- **Multicast MCS index**—MCS index for the rate at which an AP transmits multicast frames.

NOTE:

For all the MCS data rate tables, see *IEEE 802.11n-2009*.

VHT-MCS

802.11 ac uses Very High Throughput Modulation and Coding Scheme (VHT-MCS) indexes to indicate wireless data rates. A VHT-MCS is identified by a VHT-MCS index, which is represented by an integer in the range of 0 to 9. A VHT-MCS index is the mapping from VHT-MCS to a data rate.

802.11ac supports the 20 MHz, 40 MHz, 80 MHz, and 160 MHz bandwidth modes, and supports a maximum of eight spatial streams.

Table 7 through Table 18 show VHT-MCS parameters that are supported by an AP.

Table 7 VHT-MCS parameters (20 MHz, NSS=1)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	6.5	7.2
1	QPSK	13.0	14.4
2	QPSK	19.5	21.7
3	16-QAM	26.0	28.9
4	16-QAM	39.0	43.3
5	64-QAM	52.0	57.8
6	64-QAM	58.5	65.0
7	64-QAM	65.0	72.2
8	256-QAM	78.0	86.7
9	Not valid		

Table 8 VHT-MCS parameters (20 MHz, NSS=2)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	13.0	14.4
1	QPSK	26.0	28.9
2	QPSK	39.0	43.3
3	16-QAM	52.0	57.8
4	16-QAM	78.0	86.7
5	64-QAM	104.0	115.6
6	64-QAM	117.0	130.0
7	64-QAM	130.0	144.4
8	256-QAM	156.0	173.3
9	Not valid		

Table 9 VHT-MCS parameters (20 MHz, NSS=3)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	19.5	21.7
1	QPSK	39.0	43.3
2	QPSK	58.5	65.0
3	16-QAM	78.0	86.7
4	16-QAM	117.0	130.0
5	64-QAM	156.0	173.3
6	64-QAM	175.5	195.0

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
7	64-QAM	195.0	216.7
8	256-QAM	234.0	260.0
9	256-QAM	260.0	288.9

Table 10 VHT-MCS parameters (20 MHz, NSS=4)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	26.0	28.9
1	QPSK	52.0	57.8
2	QPSK	78.0	86.7
3	16-QAM	104.0	115.6
4	16-QAM	156.0	173.3
5	64-QAM	208.0	231.1
6	64-QAM	234.0	260.0
7	64-QAM	260.0	288.9
8	256-QAM	312.0	346.7
9	Not valid		

Table 11 VHT-MCS parameters (40 MHz, NSS=1)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	13.5	15.0
1	QPSK	27.0	30.0
2	QPSK	40.5	45.0
3	16-QAM	54.0	60.0
4	16-QAM	81.0	90.0
5	64-QAM	108.0	120.0
6	64-QAM	121.5	135.0
7	64-QAM	135.0	150.0
8	256-QAM	162.0	180.0
9	256-QAM	180.0	200.0

Table 12 VHT-MCS parameters (40 MHz, NSS=2)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	27.0	30.0

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
1	QPSK	54.0	60.0
2	QPSK	81.0	90.0
3	16-QAM	108.0	120.0
4	16-QAM	162.0	180.0
5	64-QAM	216.0	240.0
6	64-QAM	243.0	270.0
7	64-QAM	270.0	300.0
8	256-QAM	324.0	360.0
9	256-QAM	360.0	400.0

Table 13 VHT-MCS parameters (40 MHz, NSS=3)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	40.5	45.0
1	QPSK	81.0	90.0
2	QPSK	121.5	135.0
3	16-QAM	162.0	180.0
4	16-QAM	243.0	270.0
5	64-QAM	324.0	360.0
6	64-QAM	364.5	405.0
7	64-QAM	405.0	450.0
8	256-QAM	486.0	540.0
9	256-QAM	540.0	600.0

Table 14 VHT-MCS parameters(40 MHz, NSS=4)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	54.0	60.0
1	QPSK	108.0	120.0
2	QPSK	162.0	180.0
3	16-QAM	216.0	240.0
4	16-QAM	324.0	360.0
5	64-QAM	432.0	480.0
6	64-QAM	486.0	540.0
7	64-QAM	540.0	600.0
8	256-QAM	648.0	720.0

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
9	256-QAM	720.0	800.0

Table 15 VHT-MCS parameters (80 MHz, NSS=1)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	29.3	32.5
1	QPSK	58.5	65.0
2	QPSK	87.8	97.5
3	16-QAM	117.0	130.0
4	16-QAM	175.5	195.0
5	64-QAM	234.0	260.0
6	64-QAM	263.0	292.5
7	64-QAM	292.5	325.0
8	256-QAM	351.0	390.0
9	256-QAM	390.0	433.3

Table 16 VHT-MCS parameters (80 MHz, NSS=2)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	58.5	65.0
1	QPSK	117.0	130.0
2	QPSK	175.5	195.0
3	16-QAM	234.0	260.0
4	16-QAM	351.0	390.0
5	64-QAM	468.0	520.0
6	64-QAM	526.5	585.0
7	64-QAM	585.0	650.0
8	256-QAM	702.0	780.0
9	256-QAM	780.0	866.7

Table 17 VHT-MCS parameters (80 MHz, NSS=3)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	87.8	97.5
1	QPSK	175.5	195.0
2	QPSK	263.3	292.5

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
3	16-QAM	351.0	390.0
4	16-QAM	526.5	585.0
5	64-QAM	702.0	780.0
6	Not valid		
7	64-QAM	877.5	975.0
8	256-QAM	1053.0	1170.0
9	256-QAM	1170.0	1300.0

Table 18 VHT-MCS parameters (80 MHz, NSS=4)

VHT-MCS index	Modulation	Data rate (Mbps)	
		800ns GI	400ns GI
0	BPSK	117.0	130.0
1	QPSK	234.0	260.0
2	QPSK	351.0	390.0
3	16-QAM	468.0	520.0
4	16-QAM	702.0	780.0
5	64-QAM	936.0	1040.0
6	64-QAM	1053.0	1170.0
7	64-QAM	1170.0	1300.0
8	256-QAM	1404.0	1560.0
9	256-QAM	1560.0	1733.3

802.11ac NSSs are classified into the following types:

- **Mandatory NSSs**—Mandatory NSSs for an AP. To associate with an 802.11acAP, a client must support the mandatory NSSs for the AP.
- **Supported NSSs**—NSSs supported by an AP except for the mandatory NSSs. If a client supports both mandatory and supported NSSs, the client can use a supported rate to communicate with the AP.
- **Multicast NSS**—An AP uses a rate in the VHT-MCS data rate table for the NSS to transmit multicast frames.

NOTE:

For all the VHT-MCS data rate tables, see *IEEE 802.11ac-2013*.

HE-MCS

High Efficiency Modulation and Coding Scheme (HE-MCS) defined in IEEE 802.11ax determines the wireless data rates.

An HE-MCS is identified by an HE-MCS index, which is represented by an integer in the range of 0 to 11. An HE-MCS index is the mapping from HE-MCS to a data rate.

802.11ax supports the 20 MHz, 40 MHz, 80 MHz, and 160 MHz (80+80 MHz) bandwidth modes, and supports a maximum of eight spatial streams. Table 19 through Table 30 show HE-MCS parameters that are supported by an AP.

Table 19 HE-MCS parameters (20 MHz, NSS=1)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	8	8.6
1	QPSK	16	17.2
2	QPSK	24	25.8
3	16-QAM	33	34.4
4	16-QAM	49	51.6
5	64-QAM	65	68.8
6	64-QAM	73	77.4
7	64-QAM	81	86
8	256-QAM	98	103.2
9	256-QAM	108	114.7
10	1024-QAM	122	129
11	1024-QAM	135	143.4

Table 20 HE-MCS parameters (20 MHz, NSS=2)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	16	17.2
1	QPSK	32	34.4
2	QPSK	48	51.6
3	16-QAM	66	68.8
4	16-QAM	98	103.2
5	64-QAM	130	137.6
6	64-QAM	146	154.8
7	64-QAM	162	172
8	256-QAM	196	206.4
9	256-QAM	216	229.4
10	1024-QAM	244	258
11	1024-QAM	270	286.8

Table 21 HE-MCS parameters (20 MHz, NSS=3)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	24	25.8

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
1	QPSK	48	51.6
2	QPSK	72	77.4
3	16-QAM	99	103.2
4	16-QAM	147	154.8
5	64-QAM	195	206.4
6	64-QAM	219	232.2
7	64-QAM	243	258
8	256-QAM	294	309.6
9	256-QAM	324	344.1
10	1024-QAM	366	387
11	1024-QAM	405	430.2

Table 22 HE-MCS parameters (20 MHz, NSS=4)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	32	34.4
1	QPSK	64	68.8
2	QPSK	96	103.2
3	16-QAM	132	137.6
4	16-QAM	196	206.4
5	64-QAM	260	275.2
6	64-QAM	292	309.6
7	64-QAM	324	344
8	256-QAM	392	412.8
9	256-QAM	432	458.8
10	1024-QAM	488	516
11	1024-QAM	540	573.6

Table 23 HE-MCS parameters (40 MHz, NSS=1)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	16	17.2
1	QPSK	33	34.4
2	QPSK	49	51.6
3	16-QAM	65	68.8
4	16-QAM	98	103.2

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
5	64-QAM	130	137.6
6	64-QAM	146	154.9
7	64-QAM	163	172.1
8	256-QAM	195	206.5
9	256-QAM	217	229.4
10	1024-QAM	244	258.1
11	1024-QAM	271	286.8

Table 24 HE-MCS parameters (40 MHz, NSS=2)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	32	34.4
1	QPSK	66	68.8
2	QPSK	98	103.2
3	16-QAM	130	137.6
4	16-QAM	196	206.4
5	64-QAM	260	275.2
6	64-QAM	292	309.8
7	64-QAM	326	344.2
8	256-QAM	390	413
9	256-QAM	434	458.8
10	1024-QAM	488	516.2
11	1024-QAM	542	573.6

Table 25 HE-MCS parameters (40 MHz, NSS=3)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	48	51.6
1	QPSK	99	103.2
2	QPSK	147	154.8
3	16-QAM	195	206.4
4	16-QAM	294	309.6
5	64-QAM	390	412.8
6	64-QAM	438	464.7
7	64-QAM	489	516.3
8	256-QAM	585	619.5

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
9	256-QAM	651	688.2
10	1024-QAM	732	774.3
11	1024-QAM	813	860.4

Table 26 HE-MCS parameters (40 MHz, NSS=4)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	64	68.8
1	QPSK	132	137.6
2	QPSK	196	206.4
3	16-QAM	260	275.2
4	16-QAM	392	412.8
5	64-QAM	520	550.4
6	64-QAM	584	619.6
7	64-QAM	652	688.4
8	256-QAM	780	826
9	256-QAM	868	917.6
10	1024-QAM	976	1032.4
11	1024-QAM	1084	1147.2

Table 27 HE-MCS parameters (80 MHz, NSS=1)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	34	36
1	QPSK	68	72.1
2	QPSK	102	108.1
3	16-QAM	136	144.1
4	16-QAM	204	216.2
5	64-QAM	272	288.2
6	64-QAM	306	324.4
7	64-QAM	340	360.3
8	256-QAM	408	432.4
9	256-QAM	453	480.4
10	1024-QAM	510	540.4
11	1024-QAM	567	600.5

Table 28 HE-MCS parameters (80 MHz, NSS=2)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	68	72
1	QPSK	136	144.2
2	QPSK	204	216.2
3	16-QAM	272	288.2
4	16-QAM	408	432.4
5	64-QAM	544	576.4
6	64-QAM	612	648.8
7	64-QAM	680	720.6
8	256-QAM	816	864.8
9	256-QAM	906	960.8
10	1024-QAM	1020	1080.8
11	1024-QAM	1134	1201

Table 29 HE-MCS parameters (80 MHz, NSS=3)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	102	108
1	QPSK	204	216.3
2	QPSK	306	324.3
3	16-QAM	408	432.3
4	16-QAM	612	648.6
5	64-QAM	816	864.6
6	64-QAM	918	973.2
7	64-QAM	1020	1080.9
8	256-QAM	1224	1297.2
9	256-QAM	1359	1441.2
10	1024-QAM	1530	1621.2
11	1024-QAM	1701	1801.5

Table 30 HE-MCS parameters (80 MHz, NSS=4)

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
0	BPSK	136	144
1	QPSK	272	288.4
2	QPSK	408	432.4

HE-MCS index	Modulation	Data rate (Mbps)	
		1600ns GI	800ns GI
3	16-QAM	544	576.4
4	16-QAM	816	864.8
5	64-QAM	1088	1152.8
6	64-QAM	1224	1297.6
7	64-QAM	1360	1441.2
8	256-QAM	1632	1729.6
9	256-QAM	1812	1921.6
10	1024-QAM	2040	2161.6
11	1024-QAM	2268	2402

Basic radio functions

Working channel

Specify a working channel to reduce interference from both wireless and non-wireless devices.

You can manually specify a channel or configure the system to automatically select a channel for a radio.

When radar signals are detected on the working channel of a radio, one of the following events occurs:

- If the channel is a manually specified channel, the radio immediately changes its channel, and switches back to the specified channel after 30 minutes and then starts the quiet timer. If no radar signals are detected within the quiet time, the radio starts to use the channel. If radar signals are detected within the quiet time, the radio changes its channel.
- If the channel is an automatically assigned channel, the system automatically selects a new channel for the radio and the radio immediately changes its channel.

Maximum transmit power

The transmit power range supported by a radio varies by country code, channel, AP model, radio mode, antenna type, and bandwidth mode. If you change these attributes for a radio after you set the maximum transmit power, the configured maximum transmit power might be out of the supported transmit power range. If this happens, the system automatically adjusts the maximum transmit power to a valid value.

Power lock

If you enable TPC, and then enable power lock, the most recently selected power is locked for APs. After the AC restarts, the locked power still takes effect. If a radio enabled with power lock switches to a new channel that provides lower power than the locked power, the maximum power supported by the new channel takes effect.

For TPC to work, make sure the power is not locked before enabling TPC. For more information about TPC, see the **Network View > Wireless Configuration > Radio Resource > RF Optimization** page.

Transmission rates

Transmission rates are classified into the following types:

- **Prohibited rates**—Rates that cannot be used by an AP.
- **Mandatory rates**—Rates that the clients must support to associate with an AP.

- **Supported rate**—Rates that an AP supports. After a client associates with an AP, the client can select a higher rate from the supported rates to communicate with the AP. The AP automatically decreases the transmission rate when interference signals increase and increases the transmission rate when interference signals decrease.
- **Multicast rate**—Rate at which an AP transmits multicasts. The multicast rate must be selected from the mandatory rates.

Preamble type



IMPORTANT:

This feature is applicable only to 2.4 GHz band radios.

A preamble is a set of bits in a packet header to synchronize transmission signals between sender and receiver. A short preamble improves network performance and a long preamble ensures compatibility with all wireless devices of early models.

Transmission distance

The strength of wireless signals gradually degrades as the transmission distance increases. The maximum transmission distance of wireless signals depends on the surrounding environment and on whether an external antenna is used.

- **Without an external antenna**—About 300 meters (984.25 ft).
- **With an external antenna**—30 km (18.64 miles) to 50 km (31.07 miles).
- **In an area with obstacles**—35 m (114.83 ft) to 50 m (164.04 ft).

Beacon interval

An AP broadcasts beacon frames at a specified interval to allow itself to be detected by clients. A short beacon interval enables clients to easily detect the AP but consumes more system resources.

Access services for 802.11b clients

To prevent low-speed 802.11b clients from decreasing wireless data transmission performance, you can enable an 802.11g or 802.11n radio to disable access services for 802.11b clients.

RTS threshold

802.11 allows wireless devices to send Request to Send (RTS) or Clear to Send (CTS) packets to avoid collision. However, excessive RTS and CTS packets cost system resources and reduce transmission efficiency. You can configure an RTS threshold to resolve this problem. The system performs collision avoidance only for packets larger than the RTS threshold.

In a low-density WLAN, increase the RTS threshold to improve the network throughput and efficiency. In a high-density WLAN, decrease the RTS threshold to reduce collisions in the network.

802.11g protection

This feature is applicable only to 802.11g and 802.11n (2.4 GHz) radios.

When both 802.11b and 802.11g clients exist in a WLAN, transmission collision might occur because they use different modulation modes. 802.11g protection can avoid such avoidance. It enables 802.11g or 802.11n devices to send RTS/CTS or CTS-to-self packets to inform 802.11b clients to defer access to the medium.

802.11g or 802.11n devices send RTS/CTS or CTS-to-self packets before sending data only when 802.11b signals are detected on the channel.

802.11g protection automatically takes effect when 802.11b clients associate with an 802.11g or 802.11n (2.4 GHz) AP.

Fragment threshold

Frames larger than the fragment threshold are fragmented before transmission. Frames smaller than the fragment threshold are transmitted without fragmentation.

When a fragment is not received, only this fragment rather than the whole frame is retransmitted. In a WLAN with great interference, decrease the fragment threshold to improve the network throughput and efficiency.

Maximum number of retransmissions

In wireless networks, unicast packets require acknowledgements. If a device fails to receive the acknowledgement for a packet, it retransmits the packet. If the device fails to receive the acknowledgement when the maximum number of retransmissions is reached, it discards the packet and notifies upper layer protocols of the transmission failure.

You can set different values for the maximum number of retransmissions for large frames and small frames. Large frames refer to frames that are larger than the RTS threshold, and small frames refer to frames that are smaller than the RTS threshold.

Transmitting large frames requires more buffer and time because the system performs collision avoidance for large frames before transmission. Therefore, you can reduce the maximum number of retransmissions for large frames to save system buffer and transmission time.

802.11n functions

! IMPORTANT:

When you configure 802.11n functions for an AP, your configuration fails if another user is configuring 802.11n functions for the same AP.

IEEE 802.11n provides high-quality wireless services, and enables a WLAN to have the same network performance as Ethernet. 802.11n improves the throughput and transmission rate of WLAN by optimizing the physical layer and the MAC layer.

The physical layer of 802.11n is based on OFDM. This layer enables high throughput by using Multiple Input, Multiple Output (MIMO), 40 MHz bandwidth, short Guard Interval (GI), Space-Time Block Coding (STBC), and Low-Density Parity Check (LDPC).

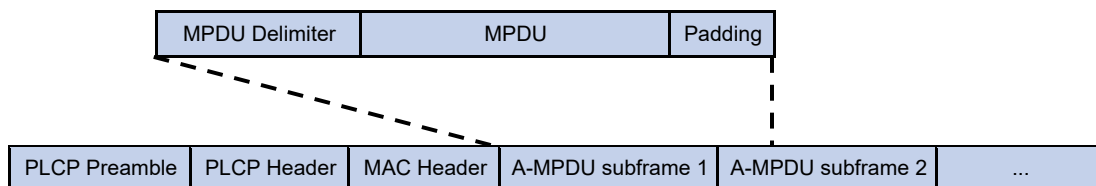
The MAC layer enables high transmission efficiency by using A-MPDU, A-MSDU, and Block Acknowledgment (BA).

MPDU aggregation

A MAC Protocol Data Unit (MPDU) is a data frame in 802.11 format. MPDU aggregation aggregates multiple MPDUs into one aggregate MPDU (A-MPDU) to reduce additional information, ACK frames, and Physical Layer Convergence Procedure (PLCP) header overhead. This improves network throughput and channel efficiency.

All MPDUs in an A-MPDU must have the same QoS priority, source address, and destination address.

Figure 5 A-MPDU format



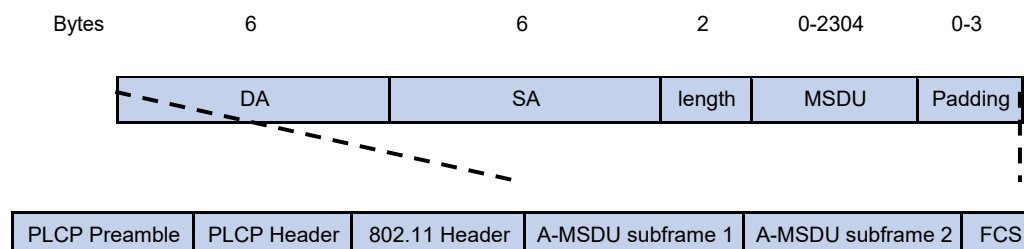
MSDU aggregation

An AP or client encapsulates a MAC Service Data Unit (MSDU) with an Ethernet header, and then converts the frame into 802.11 format for forwarding.

MSDU aggregation aggregates multiple MSDUs into one aggregate MSDU (A-MSDU) to reduce PLCP preamble, PLCP header, and MAC header overheads. This improves network throughput and frame forwarding efficiency.

All MSDUs in an A-MSDU must have the same QoS priority, source address, and destination address. When a device receives an A-MSDU, it restores the A-MSDU to multiple MSDUs for processing.

Figure 6 A-MSDU format



Short GI

<http://en.wikipedia.org/wiki/802.11> OFDM fragments frames to data blocks for transmission. It uses GI to ensure that the data block transmissions do not interfere with each other and are immune to transmission delays.

The GI used by 802.11a/g is 800 ns. <http://en.wikipedia.org/wiki/802.11n> supports a short GI of 400 ns, which provides a 10% increase in data rate.

Both the 20 MHz and 40 MHz bandwidth modes support short GI.

LDPC

802.11n introduces the Low-Density Parity Check (LDPC) mechanism to increase the signal-to-noise ratio and enhance transmission quality. LDPC takes effect only when both ends support LDPC.

STBC

The Space-Time Block Coding (STBC) mechanism enhances the reliability of data transmission and does not require clients to have high transmission rates.

MSC indexes

802.11n clients use the rate corresponding to the MCS index to send unicast frames. Non-802.11n clients use the 802.11a/b/g rate to send unicast frames.

The client dot11n-only feature

The client dot11n-only feature enables an AP to accept only 802.11n and 802.11ac clients. Use this feature to prevent low-speed 802.11a/b/g clients from decreasing wireless data transmission performance.

802.11 n bandwidth mode

802.11n uses the channel structure of 802.11a/b/g, but it increases the number of data subchannels in each 20 MHz channel to 52. This improves data transmission rate.

802.11n binds two adjacent 20 MHz channels to form a 40 MHz channel (one primary channel and one secondary channel). This provides a simple way to double the data rate.

The bandwidth for a radio varies by bandwidth mode configuration and chip capability.

MIMO modes

Multiple-input and multiple-output (MIMO) enables a radio to send and receive wireless signals through multiple spatial streams. This improves system capacity and spectrum usage without requiring higher bandwidth.

A radio can operate in one of the following MIMO modes:

- **1x1**—Sends and receives wireless signals through one spatial stream.
- **2x2**—Sends and receives wireless signals through two spatial streams.
- **3x3**—Sends and receives wireless signals through three spatial streams.
- **4x4**—Sends and receives wireless signals through four spatial streams.
- **5x5**—Sends and receives wireless signals through five spatial streams.
- **6x6**—Sends and receives wireless signals through six spatial streams.
- **7x7**—Sends and receives wireless signals through seven spatial streams.
- **8x8**—Sends and receives wireless signals through eight spatial streams.

Number of spatial streams supported by a radio varies by device model.

Energy saving

The energy saving feature enables an AP to automatically change the MIMO mode of a radio to **1x1** if no clients associate with the radio.

802.11 n protection

When both 802.11n and non-802.11n clients exist in a WLAN, transmission collision might occur because they use different modulation modes. 802.11n protection can avoid such avoidance. It enables 802.11n devices to send RTS/CTS or CTS-to-self packets to inform non-802.11n clients to defer access to the medium.

802.11n devices send RTS/CTS or CTS-to-self packets before sending data only when non-802.11n signals are detected on the channel.

802.11n protection automatically takes effect when non-802.11n clients associate with an 802.11n AP.

NOTE:

802.11n devices refer to 802.11n and 802.11ac devices.

The smart antenna feature

⚠ IMPORTANT:

- Support for this feature depends on the AP model.
 - This feature is applicable only to 802.11n and 802.11ac radios.
-

The smart antenna feature enables an AP to automatically adjust the antenna parameters based on the client location and channel information to improve signal quality and stability.

You can configure a radio to operate in one of the following smart antenna modes:

- **auto**—Uses the high availability mode for audio and video packets, and uses the high throughput mode for other packets.
- **high-availability**—Applicable to WLANs that require stable bandwidth, this mode reduces noise and interference impacts, and provides guaranteed bandwidth for clients.
- **high-throughput**—Applicable to WLANs that require high performance, this mode enhances signal strength and association capability.

802.11ac functions

! IMPORTANT:

When you configure 802.11ac functions for an AP, your configuration fails if another user is configuring 802.11ac functions for the same AP.

Based on 802.11n, 802.11ac further increases the data transmission rate and improves the network performance by providing higher bandwidth, more spatial streams, and more advanced modulation schemes.

NSSs

If the AP supports an NSS, it supports all VHT-MCS indexes for the NSS.

802.11ac clients use the rate corresponding to the VHT-MCS index for the NSS to send unicast frames. Non-802.11ac clients use the 802.11a/b/g/n rate to send unicast frames.

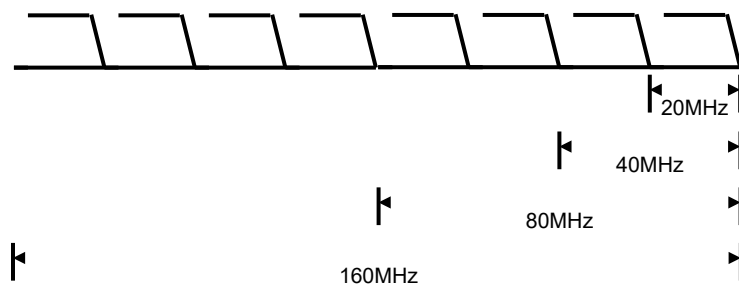
Client dot11ac-only

To prevent low-speed 802.11a/b/g/n clients from decreasing wireless data transmission performance, you can enable the client dot11ac-only feature for an AP to accept only 802.11ac and 802.11ax clients.

802.11ac bandwidth mode

802.11ac uses the channel structure of 802.11n and increases the maximum bandwidth from 40 MHz to 80 MHz. 802.11ac can bind two adjacent 20 MHz channels to form a 40 MHz channel, and bind two adjacent 40 MHz channels to form an 80 MHz channel.

Figure 7 802.11ac bandwidth modes



802.11ax functions

! IMPORTANT:

When you configure 802.11ax functions for an AP, your configuration fails if another user is configuring 802.11ax functions for the same AP.

802.11 ax uses the 1024-QAM, MU-MIMO, UL MU-MIMO, OFDMA, and spatial reuse technologies to improve the wireless transmission rate.

NSS

If an AP supports an NSS, it supports all HE-MCS indexes for the NSS. 802.11ax clients that use the rate corresponding to the HE-MCS index for the NSS to send unicast frames. Non-802.11ax clients use the 802.11a/b/g/n/ac rate to send unicast frames.

If you do not set a multicast NSS, 802.11ax clients and the AP use the 802.11a/b/g/n/ac multicast rate to send multicast frames. If you set a multicast NSS and specify an HE-MCS index, the following situations occur:

- The AP and clients use the rate corresponding to the HE-MCS index to send multicast frames if all clients are 802.11ax clients.
- The AP and clients use the 802.11a/b/g/n/ac multicast rate to send multicast frames if any non-802.11ax clients exist.

The maximum supported NSS cannot be smaller than the maximum mandatory NSS and the multicast NSS cannot be greater than the maximum mandatory NSS.

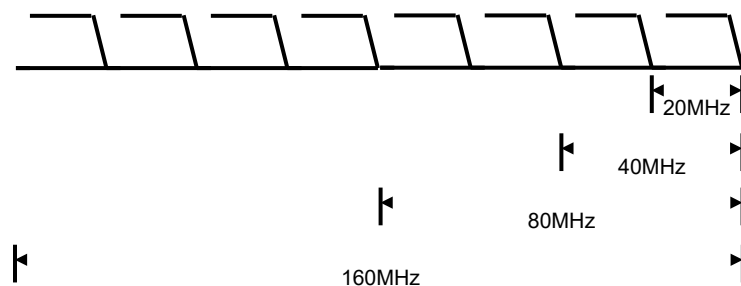
The maximum mandatory NSS or supported NSS determines a range of 802.11 rates. For example, if the maximum mandatory NSS is 5, rates corresponding to HE-MCS indexes for NSSs 1 through 5 will be 802.11ax mandatory rates.

802.11 ax bandwidth mode

802.11ax uses the channel structure of 802.11n and increases the maximum bandwidth from 40 MHz to 160 MHz. 802.11gax supports only the 20 MHz and 40 MHz bandwidth modes.

802.11ax can bind two adjacent 20/40/80 MHz channels to form a 40/80/160 MHz channel. An 802.11ax radio uses the specified 40/80/160 MHz bandwidth if adjacent channels can be bound to form a 40/80/160 channel.

Figure 8 802.11ax bandwidth modes



Client dot11ax-only

To prevent low-speed 802.11a/b/g/n/ac clients from decreasing wireless data transmission performance, you can enable the client dot11ax-only feature for an AP to accept only 802.11ax clients.

WLAN optimization

Hidden node protection

Enable this feature for clients to send RTS or CTS frames before transmitting frames to avoid interference from hidden nodes. This feature takes effect only on 802.11g, 802.11n, and 802.11ac clients.

AP-triggered client reassociation

Enable this feature for an AP to send unsolicited deauthentication frames to a client when the signal strength of the client is lower than the specified RSSI threshold. Then, the client can reassociate with the AP or roam to another AP.

Disabling a radio as scheduled

You can disable a radio in the specified time period to control client access.

The following tasks are supported to disable a radio:

- **Periodic**—Disables the radio on the specified days in a week.
- **One-off**—Disables the radio at the specified time.

Configuration restrictions and guidelines

When you configure radio management, follow these restrictions and guidelines:

- When you change the mode of a radio, the system automatically adjusts the channel and power parameters for the radio.
Modifying the mode of an enabled radio logs off all associated clients.
- When you set the maximum transmit power, make sure the maximum transmit power is within the transmit power range supported by a radio.
- When you set MCS indexes for an 802.11n AP, follow these restrictions and guidelines:
 - If you do not set a multicast MCS index, 802.11n clients and the AP use the 802.11a/b/g multicast rate to send multicast frames. If you set a multicast MCS index, one of the following events occurs:
 - The AP and clients use the rate corresponding to the multicast MCS index to send multicast frames if all clients are 802.11n clients.
 - The AP and clients use the 802.11a/b/g multicast rate to send multicast frames if any non-802.11n clients exist.
 - When you set the maximum mandatory or supported MCS index, you are specifying a range. For example, if you set the maximum mandatory MCS index to 5, rates corresponding to MCS indexes 0 through 5 are configured as 802.11n mandatory rates.
- When you set NSSs for an 802.11ac AP, follow these restrictions and guidelines:
 - If you do not set a multicast NSS, 802.11ac clients and the AP use the 802.11a/b/g/n multicast rate to send multicast frames. If you set a multicast NSS and specify a VHT-MCS index, the following situations occur:
 - The AP and clients use the rate corresponding to the VHT-MCS index for the NSS to send multicast frames if all clients are 802.11ac clients.
 - The AP and clients use the 802.11a/b/g/n multicast rate to send multicast frames if any non-802.11ac clients exist.
 - The maximum mandatory NSS or supported NSS determines a range of 802.11 rates. For example, if the maximum mandatory NSS is 5, rates corresponding to VHT-MCS indexes for NSSs 1 through 5 will be 802.11ac mandatory rates.

WLAN RRM

WLAN Radio Resource Management (RRM) provides an intelligent and scalable radio management solution. RRM enables an AC to monitor its associated radios and perform radio resource monitoring, dynamic frequency selection (DFS), and transmit power control (TPC). This allows a WLAN to adapt to environment changes and maintain the optimal radio resource condition.

Dynamic frequency selection

With DFS, the AC selects an optimal channel for each radio in real time to avoid co-channel interference and interference from other radio sources.

The following factors determine DFS:

- **Error code rate**—Physical layer error code rate and CRC errors.
- **Interference**—Influence of all wireless signals on wireless services.

- **Channel usage**—The capability of a radio to process a large number of packets.
- **Retransmission**—Data retransmission by radios if they do not receive ACK messages from the AC.
- **Radar signal**—Radar signals detected on the current channel. In this case, the AC selects a new channel and immediately notifies a radio to change its working channel.

Transmit power control

TPC enables an AC to dynamically control access point transmit power based on real-time WLAN conditions. It can achieve desired RF coverage while avoiding channel interference between radios.

Transmit power control is affected by the number of neighbor radios. The neighbor radios of a radio are the radios that are managed by the same AC as the radio and can be detected by the radio.

Bandwidth adjustment

The device detects the channel quality periodically and automatically increases or decreases the bandwidth of a radio if the number of neighbor radios for the radio meets the requirement.

WSA

Wireless devices in a WLAN share frequency bands with devices such as microwave ovens and cordless phones, and these devices might interfere with the operation of the wireless devices.

Wireless Spectrum Analysis (WSA) can resolve the problem by monitoring the spectrum environment and detecting interference.

WSA provides the following features:

- **Interference identification**—Identifies the types of interference devices and provides detailed information about interference devices.
- **Channel quality evaluation**—Provides channel quality reports, records the number of interference devices on each channel, and calculates the average channel quality and the worst channel quality.
- **Feature database management**—Deploys different feature databases to enable APs to identify different interference devices.
- **Channel adjustment**—Collaborates with Radio Resource Management (RRM) to adjust channels for APs based on channel quality.

You can view the interference device information on the AC and view the real-time WSA graphs on the NMS.

Interference identification

APs can detect only the types of interference devices in the feature database. After an AP receives a wireless signal, it performs the following operations:

1. Analyzes the frequency hopping interval and pulse interval.
2. Matches the analysis result against the interference device features in the feature database to determine whether interference devices exist in the WLAN.

You can view the interference device information on the **Network > Monitoring > RF Monitoring > Spectrum Analysis** page.

Channel quality detection

WSA can provide channel quality reports, record the number of interference devices on each channel, and calculate the average channel quality and the worst channel quality.

You can view the channel quality information on the **Network > Monitoring > RF Monitoring > Spectrum Analysis** page.

RRM collaboration

WSA can collaborate with RRM to adjust channels for APs based on channel quality.

WSA notifications

WSA supports the following notifications:

- **Interference device notifications**—The AC sends notifications to the NMS no matter when interference devices are detected or when they disappear.
- **Channel quality notifications**—The AC sends notifications to the NMS no matter when the channel quality falls below or rises above the specified threshold.

WLAN load balancing

WLAN load balancing dynamically loads balance clients across APs to ensure wireless service quality and adequate bandwidth for clients in high-density WLANs.

Load balancing types

The AC supports the following load balancing types:

- **Radio based**—The AC performs load balancing among all APs connected to the AC.
- **Load balancing group based**—You add the radios of desired APs to a load balancing group. The AC does not perform load balancing on radios that do not belong to the load balancing group.

Load balancing modes

The AC supports session-mode, traffic-mode, and bandwidth-mode load balancing. It performs load balancing of a specific mode when the following conditions are met:

- The specified session/traffic/bandwidth threshold is reached.
- The specified session/traffic/bandwidth gap threshold is reached.

Load balancing parameters

WLAN load balancing uses the following parameters:

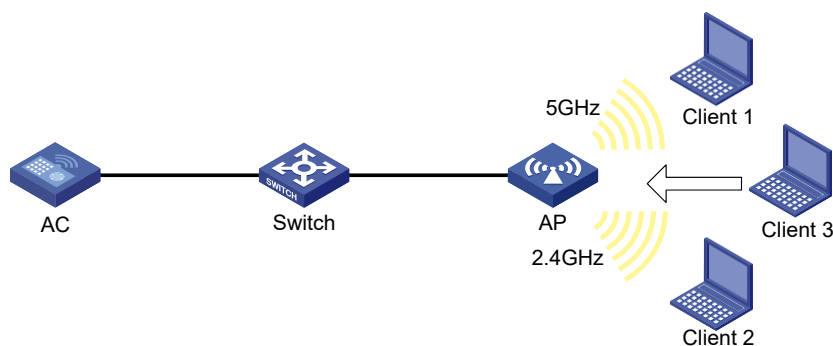
- **Load balancing RSSI threshold**—A client might be detected by multiple APs. An AP considers a client not detected if the client's RSSI is lower than the load balancing RSSI threshold. If only one AP can detect the client, the AP increases the access probability for the client even if it is overloaded.
- **Maximum number of denials for association requests**—If the number of times that an AP rejects a client reaches the specified maximum number of denials for association requests, the AP accepts the association request of the client.

Band navigation

Band navigation enables an AP to direct dual-band clients (2.4 GHz and 5 GHz) to the 5 GHz radio whenever possible to avoid typical congestion in the 2.4 GHz band. This can load balance the radios and improve network performance.

As shown in Figure 9, band navigation is enabled in the WLAN. Client 1 is associated with the 5 GHz radio and Client 2 is associated with the 2.4 GHz radio. When the dual-band Client 3 requests to associate with the 2.4 GHz radio, the AP rejects Client 3 and directs it to the 5 GHz radio.

Figure 9 Band navigation



WLAN mesh

WLAN mesh allows APs to be wirelessly connected. The APs on a WLAN mesh network can be connected directly or over multiple hops. When one AP fails, the remaining APs can still communicate with each other. For users, a WLAN mesh network can provide the same good user experience as a traditional WLAN.

MP roles

APs on a WLAN mesh network are mesh points (MPs). MPs play the following roles:

- Single-purpose MP—Provides only mesh services.
- **Mesh access point (MAP)**—Provides both mesh and access services.
- **Mesh portal point (MPP)**—Provides a wired connection to a wired network.

Mesh profile

A mesh profile is a set of mesh protocol processing capabilities for an AP to operate on a mesh network. A mesh profile contains a mesh ID, the Authentication and Key Management mode, and the keepalive interval.

Before MPs can establish a mesh link, they need to discover each other and establish a peer relationship. MPs establish a peer relationship with each other only when their mesh profiles match.

Mesh policy

A mesh policy contains a set of mesh link setup and maintenance attributes. These attributes are the mesh link initiation feature, the probe request interval, the link rate mode, and the maximum number of mesh links. Only one mesh policy can be bound to a radio of an MP, and the policy takes effect on all mesh links on the radio.

By default, a system-defined mesh policy is bound to each radio. This system-defined mesh policy cannot be deleted or modified. To change the link setup and maintenance settings on a radio, you can bind a user-defined mesh policy to the radio to replace the system-defined mesh policy.

Probe request suppression

As the point that connects the WLAN mesh network to a wired network, an MPP might need to establish a large number of mesh links. To maintain its performance, you can enable the probe request suppression feature on the MPP. The MPP will not send probe requests for neighbor discovery but only respond to the probe requests from other MPs.

Mesh peer whitelist

Use a mesh peer whitelist to ensure that an MP establishes mesh links only with legitimate MPs.

An MP can establish peer relationships with any MP neighbors if you do not configure a whitelist.

WLAN multicast optimization

Overview

Multicast transmission has limitations and cannot meet the requirements for applications that are not sensitive to time delay but sensitive to data integrity. To address this issue, you can configure WLAN multicast optimization to enable an AP to convert multicast packets to unicast packets.

WLAN multicast optimization uses multicast optimization entries to manage traffic forwarding. The multicast optimization entries use the clients' MAC addresses as indexes. A multicast optimization entry records information about multicast groups that clients join, multicast sources from which clients receive traffic, multicast group version, and multicast optimization mode.

Each time a client joins a multicast group, the AP creates a multicast optimization entry for the multicast group. If multicast sources have been specified for a client when the client joins the multicast group, the AP also creates a multicast optimization entry for each multicast source. When a client leaves a multicast group or rejects a multicast source, the AP deletes the relevant multicast optimization entry for the client.

Aging time for multicast optimization entries

Configure an appropriate aging timer for multicast optimization entries. A long aging time consumes more system resources and affects the creation of new entries and a short aging time causes frequent entries generation and aging.

Multicast optimization policy

A multicast optimization policy defines the maximum number of clients that WLAN multicast optimization supports and defines the following actions an AP takes when the limit is reached:

- **Unicast forwarding**—Sends unicast packets converted from a multicast packet to only n (n equal to the specified threshold) clients that are randomly selected.
- **Multicast forwarding**—Forwards the multicast packet to all clients.
- **Packet dropping**—Drops the multicast packet.

If you do not specify an action, an AP performs unicast forwarding.

Multicast optimization entry limits

Limit for multicast optimization entries

You can limit the number of multicast optimization entries to save system resources.

When the number of multicast optimization entries reaches the limit, the AP stops creating new entries until the number falls below the limit.

Limit for multicast optimization entries per client

You can limit the number of multicast optimization entries that an AP maintains for each client to prevent a client from occupying excessive system resources.

Rate limits for IGMP packets from clients

You can configure the maximum number of IGMP packets that an AP can receive from clients within the specified interval. The AP discards the excessive IGMP packets.

Client probing

After you enable client probing on the radio of an AP, the AP scans channels to collect client information. You can view the client information on the **Network > Monitoring > Client Proximity Sensor** page.

Do not enable WIPS and client probing simultaneously.

Wireless locating

Wireless location tracks 802.11 or Bluetooth Low Energy (BLE) devices for medical monitoring, asset management, and logistics management.

Locating system

A wireless locating system contains the following parts:

- **Devices to locate**—802.11 devices that can send wireless packets. 802.11 devices include Tags (small wireless devices that can only send 802.11 packets periodically) and MUs (all 802.11 devices except Tags).
- **Locating information receiver**—802.11 APs or other 802.11 devices that can receive wireless packets.
- **Locating server**—A server on which the locating software runs.

Wireless locating mechanism

Wireless locating operates as follows:

1. APs discover the locating server.
APs send locating packets to the specified locating server.
2. APs collect locating information.
3. Upon receiving packets from devices to locate, APs encapsulate the packets and the collected locating information in locating packets, and send them to the locating server.
4. The locating server calculates the locations of the devices.

Wireless location common parameters

Packet rate limiting

- **Client packet rate limiting**
This feature enables an AP to not report location information from excessive client packets when both the CIR and CBS are exceeded. This practice ensures that the location information for each client can be sent to the location server and prevents client packets from flooding the AP.
This feature takes effect only when AeroScout location or RF fingerprinting is configured. If packet dilution is enabled, this feature limits the rate for diluted packets.
- **Location packet rate limiting**
This feature enables an AP to discard excessive location packets when both the CIR and CBS are exceeded. This practice prevents location packets from flooding the location server.
This feature takes effect only when AeroScout location or RF fingerprinting is configured.

Wireless location keepalive

This feature enables an AP to send hello packets to the location server at an interval of 15 seconds. If the location server does not receive any packets from an AP within 30 seconds, the location server determines that the AP is offline.

Packet filtering

- **RSSI-based packet filtering**
When RSSI-based packet filtering is enabled, an AP does not report location information in packets with an RSSI lower than the RSSI threshold. This feature enables an AP to not locate clients far away from the AP.
This feature takes effect only when AeroScout location or RF fingerprinting is configured.
- **Ignoring beacon frames**
Ignoring beacon frames prevents traffic flood.
This feature takes effect only when AeroScout location or RF fingerprinting is configured.

Packet dilution

Packet dilution controls the number of locating packets from an AP to the locating server.

The dilution factor specifies wireless packet number threshold for sending a locating packet. For example, if you set the dilution factor to 100, the AP sends a locating packet every time it receives 100 wireless packets from a client (excluding management and broadcast packets).

To avoid affecting locating accuracy, you can set a dilution timeout timer. If the number of wireless packets does not reach the dilution factor when the dilution timeout timer expires, the AP sends the most recent frame it received to the locating server.

Aeroscout location

Enabling AeroScout location

This feature triggers an AP to scan all supported channels. Then, the AP encapsulates the detected device information in location packets and sends the packets to the AeroScout location server.

Timestamp

Upon receiving a wireless location packet, an AP adds either of the following timestamps to the location packet:

- **Absolute timestamp**—Represents the time elapsed since 1970.
- **Relative timestamp**—Represents the time elapsed since the AP started.

Tag packets can be encapsulated with only the relative timestamp. Whether MU packets are encapsulated with the relative time or absolute time depends on the location server vendor. The location servers of some vendors support only the absolute time for MU packets.

Listening port

The location server sends packets to a specific port during packet exchange with an AP. The AP must listen on the port to respond to the location server.

AeroScout location mode

The following AeroScout location modes are supported:

- **Dynamic location**—An AP negotiates with the location server to obtain the multicast MAC address for Tags, packet dilution attributes, and the IP address and port number of the location server. The location server obtains the AP's AeroScout version, MAC address, radio mode, and channel information. Then the location server notifies the AP to send location packets.
- **Static location**—An AP gets predefined location attributes from the AC and then starts to send location packets to the location server. Use static AeroScout location if the location server does not support dynamic negotiation with an AP. In this mode, you must configure location parameters on the AC, and an AP can send location packets after it obtains the IP address and port number of the location server.

In dynamic AeroScout location, an AP saves the IP address and port number of the location server in the flash memory. It uses the information to report its IP change or reboot events so that the server can respond in time. The AP maintains such information as follows:

- The AP starts a 10-minute timer after receiving a set configuration message that contains the server information. If it receives another set configuration message within 10 minutes, the AP only updates the configuration information in the cache. When the timer expires, the AP saves the information in the flash memory.
- If an IP change or reboot event occurs within 10 minutes after the AP receives the first configuration message, no server information is saved in the flash memory. The AP does not send an IP change or reboot message to the location server.

Forwarding mode

An AP can report location packets to the location server through either of the following modes:

- **Centralized**—The AP encapsulates location information in a location packet and sends the packet directly to the location server.
- **Local**—The AP encapsulates location information in a location packet and send the packets to the AC. The AC encapsulates location information received from multiple APs in a location packet and sends the packet to the location server.

Specifying a multicast MAC address for Tags

Both Tags and MUs send 802.11 packets. The destination MAC address of packets sent by Tags is the multicast MAC address defined by the manufacturer. Configure this feature to specify the multicast MAC address for an AP to identify Tags.

Perform this task when static AeroScout location is configured. This feature does not take effect when dynamic AeroScout location is used.

If you do not specify a multicast MAC address for Tags, an AP determines that all received 802.11 packets are from MUs.

Static server configuration

In static AeroScout location mode, you must specify the IPv4 address and port number of the AeroScout location server.

BLE location

Listening port

The location server sends packets to a specific port during packet exchange with an AP. The AP must listen on the port to response to the location server.

Static server configuration

Specify the IPv4 address and port number of the BLE location server for an AP to communicate with the location server.

Real-time BLE device information reporting

To locate BLE devices, you must enable an AP to send BLE device information to the location server in real time and configure manufacturer prefixes.

When an AP receives an advertisement from a BLE device with the specified manufacturer prefix, the AP sends the device information to the location server at the specified interval.

You can specify a maximum of 5 manufacturer prefixes and specify a location server and a report interval for each prefix.

If centralized report is enabled for BLE, and the location packet format is lightweight, the report interval is fixed at 1 second.

Neighbor list reporting

When an AP receives an advertisement from an iBeacon device, it adds the device to the neighbor list and periodically sends neighbor list reports to the location server. The neighbor list contains the UUID, major ID, minor ID, and the most recently collected transmit power and RSSI of iBeacon devices. You can enable neighbor list reporting and specify the report interval.

Forwarding mode

An AP can report location packets to the location server through either of the following modes:

- **Centralized**—The AP encapsulates location information in a location packet and sends the packet directly to the location server.
- **Local**—The AP encapsulates location information in a location packet and send the packets to the AC. The AC encapsulates location information received from multiple APs in a location packet and sends the packet to the location server.

Location packet format

BLE location supports the following location packet formats:

- **General**—This format is applicable to most scenarios. Most third-party location servers support only the general format.
- **Lightweight**—An AP encapsulates location information for several clients in one lightweight location packet to save bandwidth. This format is applicable to traffic-sensitive scenarios.

Password

An AP can send the configuration of the location server to an iBeacon device only when the password configured on the AP is the same as the password of the device. Therefore, before managing an iBeacon device through an AP, configure the factory default password of the device on the AP.

Device entry aging time

If an AP does not receive any packets from an iBeacon device within the aging time, the AP removes the device from the neighbor list, and notifies the location server of the device removal event. After receiving the notification, the location server deletes the device record.

CUPID location

Static server configuration

You can specify a remote location server or the AC as the CUPID location server. When the AC is used as the location server, only centralized forwarding is supported and only associated clients can be located.

Listening port

The location server sends packets to a specific port during packet exchange with an AP. The AP must listen on the port to response to the location server.

Client list reporting

A client can be located only when its associated AP is enabled with both CUPID location and client list reporting. After you enable client list reporting for an AP, the AP sends client list reports to the location server at the specified interval. The location server selects a group of location APs for each client based on the client list reports.

Unassociated client information reporting

This feature enables an AP to report information about unassociated clients to the location server. Unassociated client information includes client MAC address, RSSI, and location measurement result.

Forwarding mode

An AP can report location packets to the location server through either of the following modes:

- **Centralized**—The AP encapsulates location information in a location packet and sends the packet directly to the location server.
- **Local**—The AP encapsulates location information in a location packet and send the packets to the AC. The AC encapsulates location information received from multiple APs in a location packet and sends the packet to the location server.

Location packet format

CUPID location supports the following location packet formats:

- **General**—This format is applicable to most scenarios. Most third-party location servers support only the general format.
- **Lightweight**—An AP encapsulates location information for several clients in one lightweight location packet to save bandwidth. This format is applicable to traffic-sensitive scenarios.

RF fingerprinting

Static server configuration

Specify the IPv4 address and port number of the location server for an AP to communicate with the location server.

Listening port

The location server sends packets to a specific port during packet exchange with an AP. The AP must listen on the port to response to the location server.

Raw frame reporting

To enable the location server to obtain location information directly from the wireless packets of clients, enable raw frame reporting. This feature enables an AP to encapsulate both the raw frames and the location information obtained from the frames in location packets.

MU information reporting

This feature enables an AP to encapsulate MU information, including the IP address and the transmit rate of an MU in location packets.

Forwarding mode

An AP can report location packets to the location server through either of the following modes:

- **Centralized**—The AP encapsulates location information in a location packet and sends the packet directly to the location server.
- **Local**—The AP encapsulates location information in a location packet and send the packets to the AC. The AC encapsulates location information received from multiple APs in a location packet and sends the packet to the location server.

Location packet format

RF fingerprinting supports the following location packet formats:

- **CUPID-hybrid**—An AP encapsulates only clients' MAC addresses and RSSIs in location packets.
- **General**—This format is applicable to most scenarios. Most third-party location servers support only the general format.
- **Lightweight**—An AP encapsulates location information for several clients in one lightweight location packet to save bandwidth. This format is applicable to traffic-sensitive scenarios.

IoT location

IoT location can be used to locate bracelets and RFID tags.

Specify the IPv4 address and port number of the IoT location server for an AP to communicate with the location server.

Bonjour gateway

Bonjour is a set of zero configuration network protocols developed by Apple Inc based on Multicast DNS (mDNS) services. Bonjour is designed to make network configuration easier for users. It enables service devices to automatically advertise service information and enables clients to automatically discover service devices without obtaining information about the devices.

However, Bonjour supports only link-local multicast addresses. To address this issue, the AC can act as a Bonjour gateway to manage clients and service devices and forward mDNS packets across VLANs. This enables Bonjour to be applied in large scale networks.

Bonjour gateway provides the following benefits:

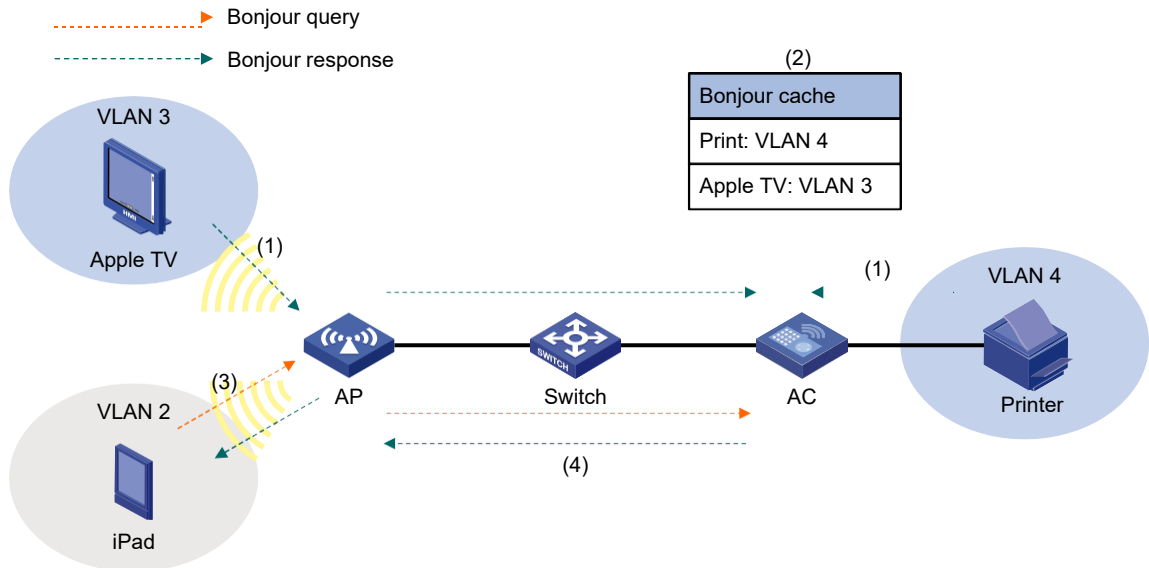
- mDNS traffic control.
- Inter-VLAN forwarding of mDNS packets.

Bonjour service advertisement snooping and caching

As shown in [Figure 10](#), Bonjour service advertisement snooping operates as follows:

1. Apple TV and Printer send service advertisements to advertise their service information.
2. Upon receiving the service advertisements, the Bonjour gateway caches all the service advertisements.
3. iPad requests the service of Apple TV or Printer.
4. The Bonjour gateway sends a response to iPad because the requested service is in the Bonjour cache.

Figure 10 Bonjour service advertisement snooping and caching

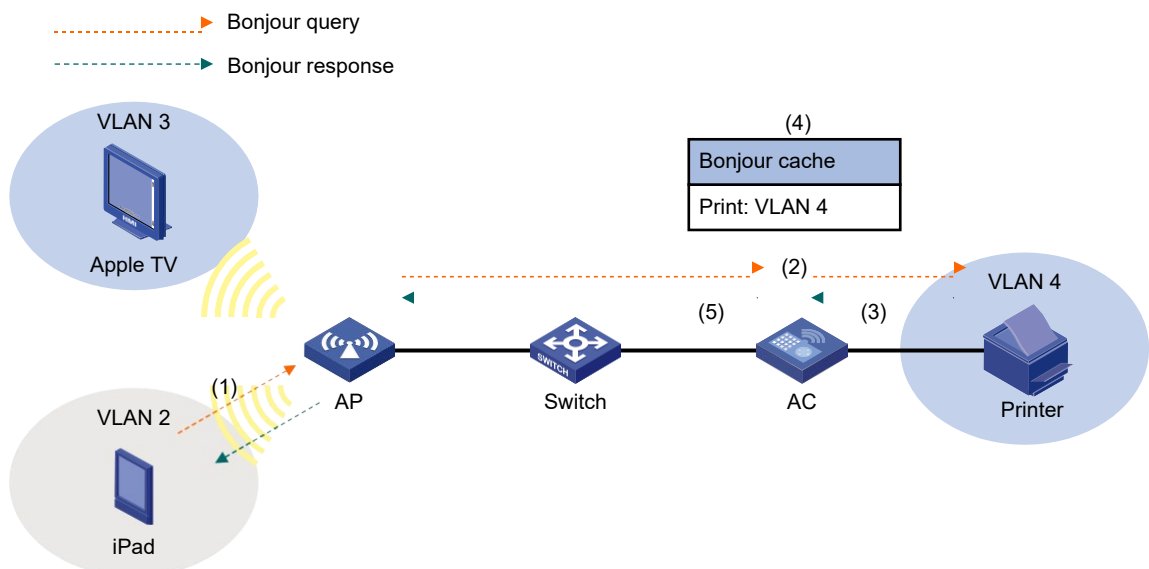


Bonjour query snooping and response

As shown in Figure 11, the Bonjour gateway performs the Bonjour query snooping and response operation by using the following process if the service query it receives is not in the Bonjour cache:

1. Upon receiving a query for the printing service from a client (iPad in the figure), the AP sends the query to the Bonjour gateway (AC) through the CAPWAP tunnel.
2. The Bonjour gateway forwards the query to the configured service VLANs because it does not find any printing service entry in the Bonjour cache.
3. The printer sends a response to the Bonjour gateway upon receiving the query.
4. The Bonjour gateway caches the response and forwards it to iPad.

Figure 11 Bonjour query snooping and response



Bonjour service type

You can use the default Bonjour service types or create new Bonjour service types to control the Bonjour services that can be queried by clients. To create a Bonjour service type, you need to specify the UDP or TCP protocol and specify a description for the service type. [Table 31](#) lists the default service types by their names and service type strings.

After you activate a Bonjour service type, the Bonjour gateway sends a query for each service of the service type if Bonjour gateway is enabled globally.

When you activate a Bonjour service type, you can specify the maximum number of service entries for the service type. If you do not specify this limit, the number of service entries for the service type is not limited.

When you deactivate a service type, all service entries of the service type are removed.

Table 31 Apple Bonjour protocols and service type strings

Name	Service type strings
afpovertcp	AppleTalkFiling Protocol
airplay	Airplay
airport	Airport Base Station
apple-sasl	Apple Password Server
daap	Digital Audio Access Protocol
dacp	Digital Audio Control Protocol
distcc	Distributed Compiler
dpap	Digital Photo Access Protocol
eppc	Remote AppleEvents
ftp	File Transfer Protocol
http	Hypertext Transfer Protocol
ica-networking	Image Capture Sharing
ichat	iChat Instant Messaging Protocol
ipp	Internet Printing Protocol over HTTP
ipps	Internet Printing Protocol over HTTPS
nfs	Network File System
pdl-stream	PDL Data Stream
printer	Line Printer Daemon
raop	Remote Audio Output Protocol
riousbprint	Remote I/O USB Printer Protocol
servermgr	Server Admin
ssh	Secure Shell
telnet	Remote Login
webdav	WebDav File System
workstation	Workgroup Manager
xserveraid	Xerver RAID

Bonjour policy

You can apply a Bonjour policy to a user profile, AP, AP group, interface, or wireless service to manage the service types and service VLANs.

Service type

This feature enables the Bonjour gateway to forward queries and service advertisements according to the following rules:

- For a query, if the service type in the query does not match the specified service type, the Bonjour gateway discards the query.
- For a service advertisement, the Bonjour gateway forwards it only when it matches all the configured options.

Service VLAN

The Bonjour gateway forwards queries and service advertisements only to the VLANs in the specified VLAN list.

You can also enable the Bonjour gateway to forward queries and responses to the VLANs to which the clients belong.

Network security

Packet filtering

You can apply an ACL to an interface to filter and take corresponding actions on incoming or outgoing packets. Packets not matching any ACL rules are processed based on the default action.

QoS

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 or PVC 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, routing, LDP, RSVP, and SSH packets.

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 and 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.

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 multiple priority maps. If a default priority map cannot meet your requirements, you can modify the priority map as required.

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.

802.1 X 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.

802.1 X 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 sends ciphertext passwords to the RADIUS server, and PAP sends plaintext passwords to the RADIUS server.
- **EAP relay**—The access device uses EAPOR packets to send authentication information to the RADIUS server.

Access control methods

The following access control methods are supported:

- **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, the other online users are not affected.

Port authorization state

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 to the authorized state to allow access to the network.

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.

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.

802.1X SmartOn

The SmartOn feature is mutually exclusive with the 802.1X online user handshake feature.

When the device sends a unicast EAP-Request/Notification packet to the client, it starts the SmartOn client timeout timer.

- If the device does not receive any EAP-Response/Notification packets from the client within the timeout timer, it retransmits the EAP-Request/Notification packet to the client. After the device has made the maximum retransmission attempts but received no response, it stops the 802.1X authentication process for the client.
- If the device receives an EAP-Response/Notification packet within the timer or before the maximum retransmission attempts have been made, it starts the SmartOn authentication. If the SmartOn switch ID and the MD5 digest of the SmartOn password in the packet match those on the device, 802.1X authentication continues for the client. Otherwise, the device denies the client's 802.1X authentication request.

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 RADIUS authentication**—The device works with a remote RADIUS 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 RADIUS authorization**—The device works with a remote RADIUS 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. 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 RADIUS accounting**—The device works with a remote RADIUS 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 come 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 INTELBRAS INC to correctly log out users when a card reboots on the distributed device to which the users connect.

- **Session-control**—ARADIUS server running on INTELBRAS INC 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.

BYOD

Bring Your Own Device (BYOD) allows employees to access privileged company data and applications by using personal mobile devices at the workplace, for example, laptops, tablets, and smart phones. BYOD solutions can provide different authentication and authorization services based on the user identities, endpoint types, and access scenarios.

BYOD endpoint identification rules

A BYOD endpoint identification rule defines the mapping between an endpoint type and a fingerprint string. The device obtains fingerprint information from the authentication request of an endpoint, and matches the fingerprint with the rules for the associated endpoint type.

BYOD authorization supports the following endpoint fingerprints:

- **DHCP Option 55 fingerprint**—Parameter request list option. The option is used by an endpoint to request specific configuration parameters.
- **HTTP user agent fingerprint**—Located in the header of HTTP requests to carry information about the endpoint operating system, Web browser, and versions.
- **MAC address fingerprint**—OUI of the endpoint or MAC address range to which the endpoint belongs.

The device matches fingerprint information for an endpoint in the following order:

1. DHCP Option 55 fingerprint.
2. HTTP user agent fingerprint.
3. MAC address fingerprint.

The system has predefined BYOD endpoint identification rules. You can also configure BYOD endpoint identification rules depending on the network requirements.

BYOD authorization

BYOD authorization attributes are assigned based on endpoint types to user groups and apply to users who have passed local authentication. After the device identifies the endpoint type of a user, it assigns BYOD authorization attributes to the user according to the settings of the user group for the user.

Local users

The device performs local authentication, authorization, and accounting based on the locally configured user information, including the username, password, and authorization attributes. Each local user is identified by the username.

User groups simplify local user configuration and management. A user group contains a group of local users and has a set of local user attributes. The user attributes of a user group apply to all users in this group.

Guest management

Guest management enables you to manage accounts and define access authorities for guests. It includes the following functions:

- **Creating a guest**—You can manually create a guest and configure attributes for the guest.
- **Importing guests**—You can import a .csv file that contains the guest information to enable the device to automatically generate guests.
- **Bulk generating guests**—You can configure the system to automatically generate multiple guests and assign usernames and passwords to the guests.
- **Exporting guests**—You can export the guest information to a .csv file.
- **Guest registration and approval**—The guest registration and approval process is as follows:
 - a. The guest enters the registration information including username, password, and email address on the pushed webpage.
 - b. Upon receiving the registration information, the device records the information and sends a notification to the guest administrator.
 - c. Upon receiving the notification, the guest administrator approves the guest on the webpage.
 - d. The device automatically creates the guest and generates related attributes.

The device creates the guest only if the guest administrator approves the guest within the timeout period. If the guest administrator does not approve the guest within the timeout period, the device deletes the guest information.
 - e. After creating the guest, the device sends a notification containing the guest password and validity period to the guest or receptionist.
 - f. Upon receiving the notification, the guest can use the registered account to access the network.
- **Deleting expired guests**—The device periodically checks the guests and deletes expired guests.
- **Email notifications**—The device can send notifications to guests, receptionist, and guest administrators.

Access control

MAC authentication

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 a username and password for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication-enabled port. If the MAC address passes authentication, the user can access authorized network resources. If the authentication fails, the device marks the MAC address as a silent MAC address, drops the packet, and starts a quiet timer. The device drops all subsequent packets from the MAC address within the quiet time. The quiet mechanism avoids repeated authentication during a short time.

MAC authentication performed by using a RADIUS server supports the following authentication methods:

- **PAP**—Requires a username and password for authentication. PAP authentication transmits usernames and passwords in plaintext mode, which is applicable to networks with low security requirements.
- **CHAP**—Requires clients and the server to exchange challenge messages to authenticate users. CHAP authentication transmits usernames in plaintext mode and passwords in ciphertext mode. Compared with PAP, CHAP provides better security performance.

Port security

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 address of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC address of outbound traffic.
- Controls MAC address learning and authentication on a port to ensure that 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.

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. When portal authentication is deployed on a network, an access device redirects unauthenticated users to the website provided by a portal Web server. The users can access the resources on the website without authentication. If the users want to access other network resources, they must pass authentication on the website.

Portal authentication is classified into the following types:

- **Active authentication**—Users visit the authentication website provided by the portal Web server and enter their username and password for authentication.
- **Forced authentication**—Users are redirected to the portal authentication website for authentication when they visit other websites.

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.

System

ACL

An access control list (ACL) is a set of rules for identifying traffic based on criteria such as source IP address, destination IP address, and port number. The rules are also called permit or deny statements.

ACL types

ACL type		Match criteria
IPv4 ACLs	Basic ACLs	Source IPv4 address.
	Advanced ACLs	Source IPv4 address, destination IPv4 address, source port number, destination port number, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
IPv6 ACLs	Basic ACLs	Source IPv6 address.
	Advanced ACLs	Source IPv6 address, destination IPv6 address, source port number, destination port number, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
Layer 2 ACLs		Layer 2 header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type.

Match order

The rules in an ACL are sorted in a specific order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule.

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.
- **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 32](#) lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL. User-defined ACLs do not support auto match order.

Table 32 Sort ACL rules in depth-first order

ACL type	Sequence of tie breakers
IPv4 basic ACL	<ol style="list-style-type: none">1. More 0s in the source IPv4 address wildcard (more 0s means a narrower IPv4 address range).2. Rule configured earlier.
IPv4 advanced ACL	<ol style="list-style-type: none">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	<ol style="list-style-type: none">1. Longer prefix for the source IPv6 address (a longer prefix means a narrower IPv6 address range).2. Rule configured earlier.

ACL type	Sequence of tie breakers
IPv6 advanced ACL	<ol style="list-style-type: none"> 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.
Layer 2 ACL	<ol style="list-style-type: none"> 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.

Rule numbering

ACL rules can be manually numbered or automatically numbered. The rule numbering step sets the increment by which the system automatically numbers rules. By introducing a gap between rules rather than contiguously numbering rules, you have the flexibility of inserting rules in an ACL. When you create an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15. Whenever the step changes, the rules are renumbered, starting from the 0. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step 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 takes effect only in 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 types of time ranges are available:

- **Periodic time range**—Recurrs 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 identified by a name. A time range can contain one or multiple periodic and absolute time ranges. In this case, 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.

VLAN group

A VLAN group includes a set of VLANs. You can add multiple VLAN lists to a VLAN group. Each VLAN list can contain a VLAN ID or a range of VLAN IDs.

SSL

Overview

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.

Restrictions and guidelines

- SSL versions include SSL 2.0, SSL 3.0, and TLS 1.0 (or SSL 3.1). When the device acts as the SSL server, it can communicate with clients running SSL 3.0 or TLS 1.0. When the server receives an SSL 2.0 Client Hello message from a client that supports both SSL 2.0 and SSL 3.0/TLS 1.0, it notifies the client to use SSL 3.0 or TLS 1.0 for communication.
- An SSL server policy contains a set of SSL parameters used by the SSL server. An SSL server policy takes effect only after it is associated with an application such as HTTPS.
- An SSL client policy contains a set of SSL parameters that the client uses to establish a connection to the server. An SSL client policy takes effect only after it is associated with an application such as the DDNS.

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 33](#) describes the peer public key configuration methods.

Table 33 Peer public key configuration methods

Method	Prerequisites	Remarks
Import the peer public key from a public key file (recommended).	<ol style="list-style-type: none"> 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.	<ul style="list-style-type: none"> • 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

Overview

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 IPsec and 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 the 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. Import certificates when the CRL repository is not specified, the CA server does not support SCEP, or 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.

Restrictions and guidelines

When you configure PKI, follow these restrictions and guidelines:

- Follow the CA policy to configure the PKI entity. If the PKI entity settings do not meet the CA policy requirements, the certificate request will fail. For example, if the CA policy requires the entity DN, but you configure only the IP address, the CA rejects the certificate request from the entity.
- The SCEP add-on on the Windows 2000 CA server has restrictions on the data length of a certificate request. If a request from a PKI entity exceeds the data length limit, the CA server does not respond to the certificate request. In this case, you can use an out-of-band means to submit the request. Other types of CA servers, such as RSA servers and OpenCA servers, do not have such restrictions.

Tools

Packet capture

The packet capture feature captures incoming packets that are to be forwarded in the CPU. The feature displays the captured packets in real time, and allows you to save the captured packets to a .pcap file for future analysis.

Packet capture uses the following modes:

- **Local packet capture**
Local packet capture saves the captured packets to a file on an FTP server.
- **Remote packet capture**
Remote packet capture displays the captured packets on a Wireshark client. Before using remote packet capture, you must install the Wireshark software on a PC and connect the PC to the RPCAP service port of the AP. Packets captured on the RPCAP port will be displayed on the Wireshark client.

Filter elements

Packet capture supports capture filters. You can use expressions to match packets to capture.

A capture filter contains a keyword string or multiple keyword strings that are connected by operators.

Keywords include the following types:

- **Qualifiers**—Fixed keyword strings. For example, you must use the **ip** qualifier to specify the IPv4 protocol.
- **Variables**—Values supplied by users in the required format. For example, you can set an IP address to 2.2.2.2 or any other valid values.

A variable must be modified by one or multiple qualifiers. For example, to capture any packets sent from the host at 2.2.2.2, use the filter **src host 2.2.2.2**.

Operators include the following types:

- **Logical operators**—Perform logical operations, such as the AND operation.
- **Arithmetic operators**—Perform arithmetic operations, such as the ADD operation.
- **Relational operators**—Indicate the relation between keyword strings. For example, the **=** operator indicates equality.

This document provides basic information about these elements. For more information about capture and display filters, go to the following websites:

- <http://wiki.wireshark.org/CaptureFilters>.
- <http://wiki.wireshark.org/DisplayFilters>.

Capture filter keywords

Table 34 and Table 35 describe the qualifiers and variables for capture filters, respectively.

Table 34 Qualifiers for capture filters

Category	Description	Examples
Protocol	Matches a protocol. If you do not specify a protocol qualifier, the filter matches any supported protocols.	<ul style="list-style-type: none">• arp—Matches ARP.• icmp—Matches ICMP.• ip—Matches IPv4.• ip6—Matches IPv6.• tcp—Matches TCP.• udp—Matches UDP.
Direction	Matches packets based on their source or destination location (an IP address or port number). If you do not specify a direction qualifier, the src or dst qualifier applies.	<ul style="list-style-type: none">• src—Matches the source IP address field.• dst—Matches the destination IP address field.• src or dst—Matches the source or destination IP address field. NOTE: The src or dst qualifier applies if you do not specify a direction qualifier. For example, port 23 is equivalent to src or dst port 23 .
Type	Specifies the direction type.	<ul style="list-style-type: none">• host—Matches the IP address of a host.• net—Matches an IP subnet.• port—Matches a service port number.• portrange—Matches a service port range. NOTE: The host qualifier applies if you do not specify any type qualifier. For example, src 2.2.2.2 is equivalent to src host 2.2.2.2 . To specify an IPv6 subnet, you must specify the net qualifier.
Others	Any other qualifiers than the previously described qualifiers.	<ul style="list-style-type: none">• broadcast—Matches broadcast packets.• multicast—Matches multicast and broadcast packets.• less—Matches packets that are less than or equal to a specific size.• greater—Matches packets that are greater than or equal to a specific size.• len—Matches the packet length.• vlan—Matches VLAN packets.

NOTE:

None of the protocol qualifiers and the **broadcast**, **multicast** qualifiers can modify variables.

Table 35 Variable types for capture filters

Variable type	Description	Examples
Integer	Represented in binary, octal,	The port 23 expression matches traffic sent to or

Variable type	Description	Examples
	decimal, or hexadecimal notation.	from port number 23.
Integer range	Represented by hyphenated integers.	The portrange 100-200 expression matches traffic sent to or from any ports in the range of 100 to 200.
IPv4 address	Represented in dotted decimal notation.	The src 1.1.1.1 expression matches traffic sent from the IPv4 host at 1.1.1.1.
IPv6 address	Represented in colon hexadecimal notation.	The dst host 1::1 expression matches traffic sent to the IPv6 host at 1::1.
IPv4 subnet	Represented by an IPv4 network ID or an IPv4 address with a mask.	Both of the following expressions match traffic sent to or from the IPv4 subnet 1.1.1.0/24: <ul style="list-style-type: none"> • src 1.1.1. • src net 1.1.1.0/24.
IPv6 network segment	Represented by an IPv6 address with a prefix length.	The dst net 1::/64 expression matches traffic sent to the IPv6 network 1::/64.

Capture filter operators

Capture filters support logical operators ([Table 36](#)), arithmetic operators ([Table 37](#)), and relational operators ([Table 38](#)). Logical operators can use both alphanumeric and nonalphanumeric symbols. Arithmetic and relational operators can use only nonalphanumeric symbols.

Logical operators are left associative. They group from left to right. The **not** operator has the highest priority. The **and** and **or** operators have the same priority.

Table 36 Logical operators for capture filters

Nonalphanumeric symbol	Alphanumeric symbol	Description
!	not	Reverses the result of a condition. Use this operator to capture traffic that matches the opposite value of a condition. For example, to capture non-HTTP traffic, use not port 80 .
&&	and	Joins two conditions. Use this operator to capture traffic that matches both conditions. For example, to capture non-HTTP traffic that is sent to or from 1.1.1.1, use host 1.1.1.1 and not port 80 .
	or	Joins two conditions. Use this operator to capture traffic that matches either of the conditions. For example, to capture traffic that is sent to or from 1.1.1.1 or 2.2.2.2, use host 1.1.1.1 or host 2.2.2.2 .

Table 37 Arithmetic operators for capture filters

Nonalphanumeric symbol	Description
+	Adds two values.
-	Subtracts one value from another.
*	Multiplies one value by another.

Nonalphanumeric symbol	Description
/	Divides one value by another.
&	Returns the result of the bitwise AND operation on two integral values in binary form.
	Returns the result of the bitwise OR operation on two integral values in binary form.
<<	Performs the bitwise left shift operation on the operand to the left of the operator. The right-hand operand specifies the number of bits to shift.
>>	Performs the bitwise right shift operation on the operand to the left of the operator. The right-hand operand specifies the number of bits to shift.
[]	Specifies a byte offset relative to a protocol layer. This offset indicates the byte where the matching begins. You must enclose the offset value in the brackets and specify a protocol qualifier. For example, ip[6] matches the seventh byte of payload in IPv4 packets (the byte that is six bytes away from the beginning of the IPv4 payload).

Table 38 Relational operators for capture filters

Nonalphanumeric symbol	Description
=	Equal to. For example, ip[6]=0x1c matches an IPv4 packet if its seventh byte of payload is equal to 0x1c.
!=	Not equal to. For example, len!=60 matches a packet if its length is not equal to 60 bytes.
>	Greater than. For example, len>100 matches a packet if its length is greater than 100 bytes.
<	Less than. For example, len<100 matches a packet if its length is less than 100 bytes.
>=	Greater than or equal to. For example, len>=100 matches a packet if its length is greater than or equal to 100 bytes.
<=	Less than or equal to. For example, len<=100 matches a packet if its length is less than or equal to 100 bytes.

Building a capture filter

This section provides the most commonly used expression types for capture filters.

Logical expression

Use this type of expression to capture packets that match the result of logical operations.

Logical expressions contain keywords and logical operators. For example:

- **not port 23 and not port 22**—Captures packets with a port number that is not 23 or 22.
- **port 23 or icmp**—Captures packets with a port number 23 or ICMP packets.

In a logical expression, a qualifier can modify more than one variable connected by its nearest logical operator. For example, to capture packets sourced from IPv4 address 192.168.56.1 or IPv4 network 192.168.27, use either of the following expressions:

- **src 192.168.56.1 or 192.168.27.**
- **src 192.168.56.1 or src 192.168.27.**

The *expr relop expr* expression

Use this type of expression to capture packets that match the result of arithmetic operations.

This expression contains keywords, arithmetic operators (*expr*), and relational operators (*relop*). For example, **len+100>=200** captures packets that are greater than or equal to 100 bytes.

The *proto [expr:size]* expression

Use this type of expression to capture packets that match the result of arithmetic operations on a number of bytes relative to a protocol layer.

This type of expression contains the following elements:

- *proto*—Specifies a protocol layer.
- *[]*—Performs arithmetic operations on a number of bytes relative to the protocol layer.
- *expr*—Specifies the arithmetic expression.
- *size*—Specifies the byte offset. This offset indicates the number of bytes relative to the protocol layer. The operation is performed on the specified bytes. The offset is set to 1 byte if you do not specify an offset.

For example, **ip[0]&0xf !=5** captures an IP packet if the result of ANDing the first byte with 0x0f is not 5.

To match a field, you can specify a field name for *expr:size*. For example, **icmp[icmptype]=0x08** captures ICMP packets that contain a value of 0x08 in the Type field.

The *vlan vlan_id* expression

Use this type of expression to capture 802.1Q tagged VLAN traffic.

This type of expression contains the **vlan vlan_id** keywords and logical operators. The *vlan_id* variable is an integer that specifies a VLAN ID. For example, **vlan 1 and ip6** captures IPv6 packets in VLAN 1.

To capture 802.1Q tagged traffic, you must use the **vlan vlan_id** expression prior to any other expressions. An expression matches untagged packets if it does not follow a **vlan vlan_id** expression. For example:

- **vlan 1 and !tcp**—Captures VLAN 1-tagged non-TCP packets.
- **icmp and vlan 1**—Captures untagged ICMP packets that are VLAN 1 tagged. This expression does not capture any packets because no packets can be both tagged and untagged.

RF Ping

RF Ping, which is also known as wireless link quality detection, enables an AP to test the quality of the link to a wireless client. The AP sends five empty data frames to the client at each supported rate. Then it calculates link quality information such as RSSI, packet retransmissions, and Round-trip Time (RTT) based on the responses from the client.

The wireless link quality detection timeout is 10 seconds.

Debugging

The system provides diagnostic information collection to help users in troubleshooting.

Contents

System features configuration examples	1
Network settings configuration examples	1
Intra-AC roaming configuration example	1
Inter-AC roaming configuration example	2
Layer 2 static aggregation configuration example	3
Layer 2 dynamic aggregation configuration example	4
Outbound dynamic NAT configuration example	5
Outbound static NAT configuration example	6
IPv4 static route configuration example	7
IPv6 static route configuration example	8
Static IPv6 address configuration example	9
DHCP server configuration example	10
DHCP relay agent configuration example	11
DHCP snooping configuration example	12
IPv4 static DNS configuration example	13
IPv4 dynamic DNS configuration example	14
IPv4 DNS proxy configuration example	15
IPv6 static DNS configuration example	16
IPv6 dynamic DNS configuration example	16
IPv6 DNS proxy configuration example	17
IGMP snooping configuration example	18
MLD snooping configuration example	20
Proxy ARP configuration example	21
ARP attack protection configuration example	22
Using the AC as the Stelnet server for password authentication configuration example	23
NTP configuration example	24
Network security configuration examples	25
ACL-based packet filter configuration example	25
System configuration examples	26
Administrators configuration example	26
Network configuration examples	28
Wireless configuration examples	28
CAPWAP tunnel establishment through DHCP configuration example	28
CAPWAP tunnel establishment through DNS configuration example	29
Auto AP configuration example	30
AP group configuration example	31
Radio management configuration example	32
Scheduled radio shutdown configuration example	33
AP configuration file deployment configuration example	34
AP group configuration file deployment configuration example	34
WIPS device classification and countermeasures configuration example	35
WIPS malformed packet and flood attack detection configuration example	37
Signature-based attack detection configuration example	38
Client rate limiting configuration example	39
Bandwidth guaranteeing configuration example	40
Shared key authentication configuration example	41
PSK authentication and bypass authentication configuration example	42
PSK authentication and MAC authentication configuration example	43
802.1X RADIUS authentication configuration example	44
802.1X local authentication configuration example	46
802.1X AKM configuration example	47
Direct IPv4 portal authentication configuration example	48
WLAN RRM DFS configuration example	49
WLAN RRM TPC configuration example	50
WLAN RRM bandwidth adjustment configuration example	51
Session-mode load balancing configuration example	51

Traffic-mode load balancing configuration example.....	53
Bandwidth-mode load balancing configuration example	54
Session-mode load balancing configuration example for a load balancing group	56
Traffic-mode load balancing configuration example for a load balancing group	57
Bandwidth-mode load balancing configuration example for a load balancing group.....	59
Band navigation configuration example	60
Wireless locating configuration example	61
WLAN mesh configuration example.....	63
Multicast optimization configuration example	64
Network security configuration examples.....	65
BYOD configuration example	65
Guest management configuration example	67
Tools configuration examples	69
Local packet capture configuration example	69
Remote packet capture configuration example.....	70

System features configuration examples

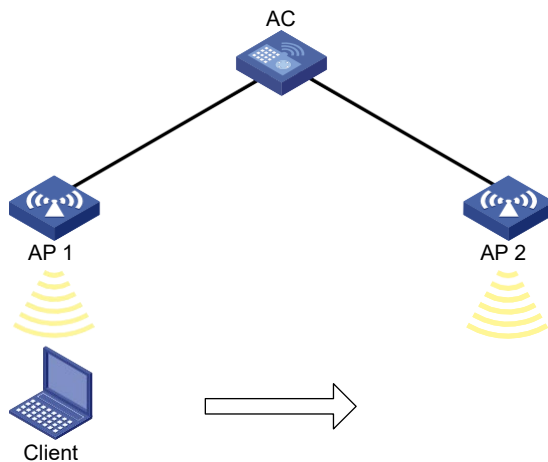
Network settings configuration examples

Intra-AC roaming configuration example

Network requirements

As shown in [Figure 1](#), configure intra-AC roaming to enable the client to roam from AP 1 to AP 2. The two APs are managed by the same AC.

Figure 1 Network diagram



Configuration procedures

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **roaming**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Configure AP 1:
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to the radio of AP 1.
 - c. Configure AP 2 in the same way AP 1 is configured.

Verifying the configuration

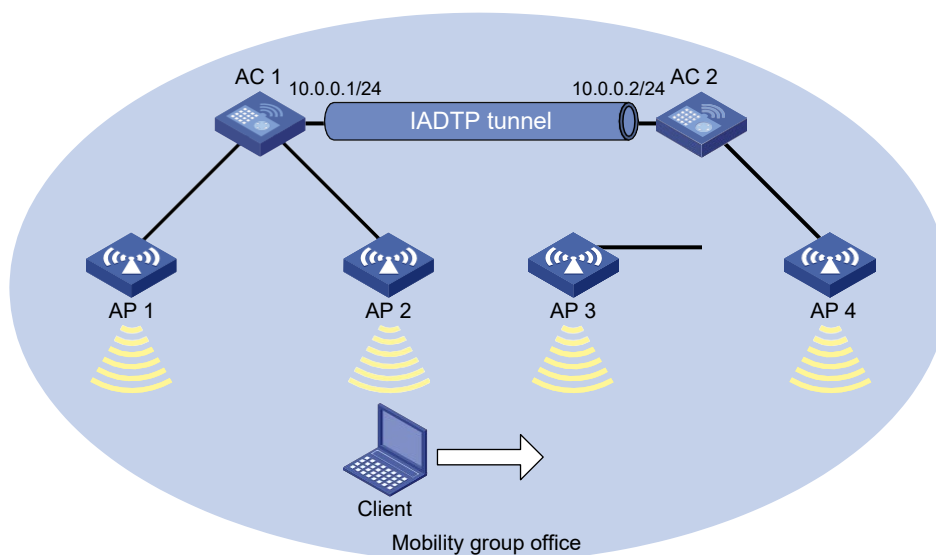
On the **System View > Network Configuration > Mobility Domain > Roaming** page, verify that the client associates with AP 1 before roaming and associates with AP 2 after roaming.

Inter-AC roaming configuration example

Network requirements

As shown in Figure 2, configure inter-AC roaming to enable the client to roam from AP 2 to AP 3 that are managed by different ACs.

Figure 2 Network diagram



Configuring AC 1

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **roaming**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Configure AP 1:
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to the radio of AP 1.
 - c. Configure AP 2 in the same way AP 1 is configured.
4. Click the system view tab at the bottom of the page.
5. Configure a mobility group:
 - a. From the navigation pane, select **Network Configuration > Mobility Domain**.
 - b. On the **Roaming** tab, perform the following tasks:
 - Create a mobility group named **office**.
 - Set the IP address type to **IPv4** for IADTP tunnels.
 - Specify **10.0.0.1** as the source IP address for establishing IADTP tunnels.
 - Add the member device whose IP address is **10.0.0.2** to the mobility group.

- Enable the mobility group.

Configuring AC 2

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **roaming**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Configure AP 3:
 - Click the edit icon in the operation column for AP 3.
 - Click the wireless service setting tab, and bind the wireless service **service** to the radio of AP 3.
 - c. Configure AP 4 in the same way AP 3 is configured.
4. Click the system view tab at the bottom of the page.
5. Configure a mobility group:
 - a. From the navigation pane, select **Network Configuration > Mobility Domain**.
 - b. On the **Roaming** tab, perform the following tasks:
 - Create a mobility group named **office**.
 - Set the IP address type to **IPv4** for IACTP tunnels.
 - Specify **10.0.0.2** as the source IP address for establishing IACTP tunnels.
 - Add the member device whose IP address is **10.0.0.1** to the mobility group.
 - Enable the mobility group.

Verifying the configuration

On the **System View > Network Configuration > Mobility Domain > Roaming** page, verify the following information:

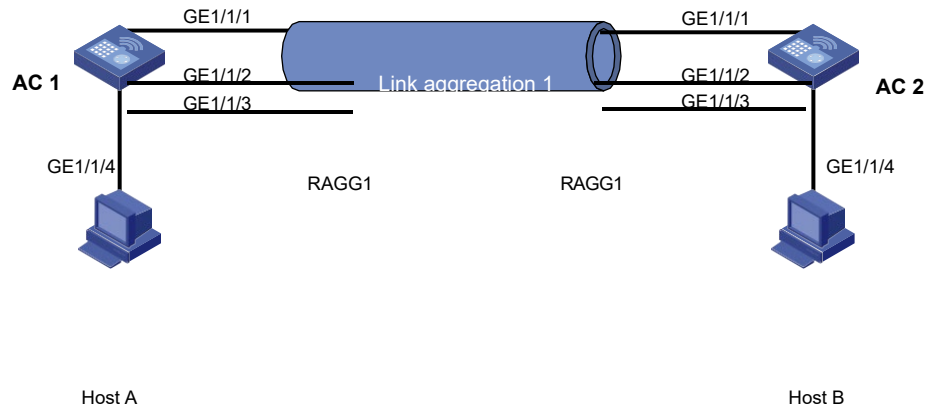
- The client associates with AP 2 managed by AC 1 before roaming.
- The client associates with AP 3 managed by AC 2 after roaming.

Layer 2 static aggregation configuration example

Network requirements

As shown in [Figure 3](#), configure a Layer 2 static aggregation group on both AC 1 and AC 2 to improve the link reliability.

Figure 3 Network diagram



Configuration procedure

1. Configure Ethernet link aggregation on AC 1:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Interfaces**.
 - c. Click the **Link Aggregation** tab.
 - d. Configure a Layer 2 aggregation group:
 - Add Layer 2 aggregation group 1.
 - Configure the aggregation mode as **Static**.
 - Assign ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 to the aggregation group.
2. Configure a VLAN on AC 1:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - c. Create VLAN 10.
 - d. Access the details page for VLAN 10 to perform the following tasks:
 - Add the port GigabitEthernet 1/1/4 (that connects to Host A) to the untagged portlist.
 - Add ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 and aggregate interface BAGG1 to the tagged port list.
3. Configure AC 2 in the same way AC 1 is configured. (Details not shown.)

Verifying the configuration

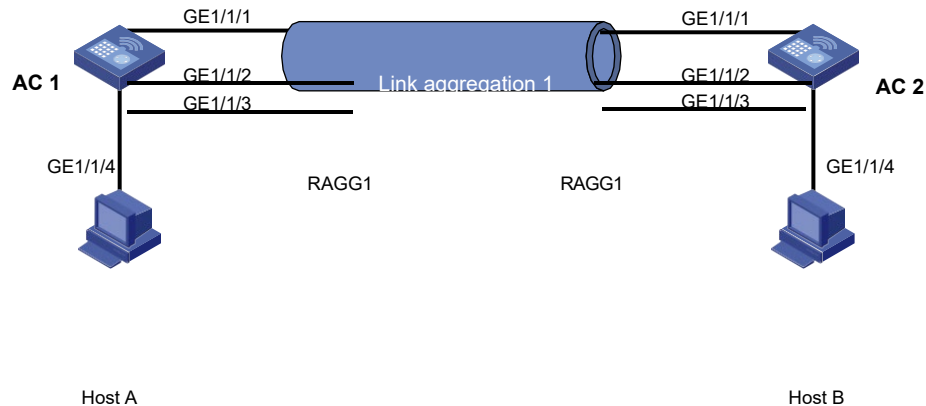
1. Access the link aggregation page, and verify that ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 have been assigned to link aggregation group 1.
2. Verify that Host A can ping Host B.
3. Verify that Host A can still ping Host B after a link between AC 1 and AC 2 fails.

Layer 2 dynamic aggregation configuration example

Network requirements

As shown in [Figure 4](#), configure a dynamic Layer 2 aggregation group on both AC 1 and AC 2 to improve the link reliability.

Figure 4 Network diagram



Configuration procedure

1. Configure Ethernet link aggregation on AC 1:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Interfaces**.
 - c. Click the **Link Aggregation** tab.
 - d. Configure a Layer 2 aggregation group:
 - Add Layer 2 aggregation group 1.
 - Configure the aggregation mode as **Dynamic**.
 - Assign ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 to the aggregation group.
2. Configure a VLAN on AC 1:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - c. Create VLAN 10.
 - d. Access the details page for VLAN 10 to perform the following tasks:
 - Add the port GigabitEthernet 1/1/4 (that connects to Host A) to the untagged portlist.
 - Add ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 and aggregate interface BAGG1 to the tagged port list.
3. Configure AC 2 in the same way AC 1 is configured. (Details not shown.)

Verifying the configuration

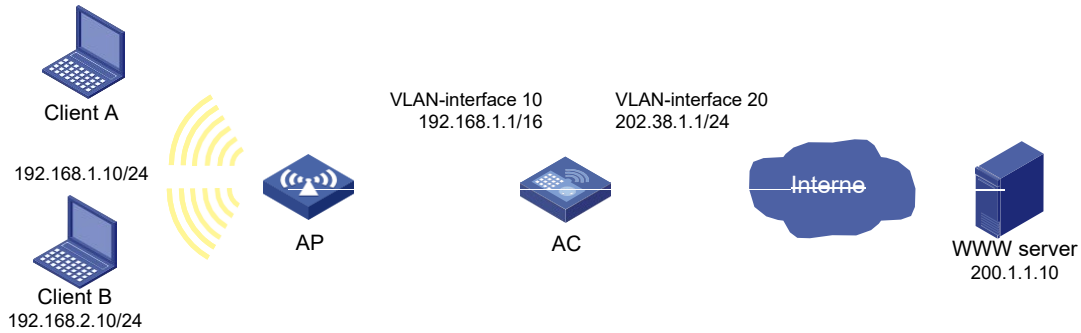
1. Access the link aggregation page, and verify that ports GigabitEthernet 1/1/1 through GigabitEthernet 1/1/3 have been assigned to link aggregation group 1.
2. Verify that Host A can ping Host B.
3. Verify that Host A can still ping Host B after a link between AC 1 and AC 2 fails.

Outbound dynamic NAT configuration example

Network requirements

As shown in Figure 5, a company has a private address 192.168.0.0/16 and two public IP addresses 202.38.1.2 and 202.38.1.3. Configure outbound dynamic NAT to allow only internal users on subnet 192.168.1.0/24 to access the Internet.

Figure 5 Network diagram



Configuration procedures

1. Click the system view tab at the bottom of the page.
2. From the navigation pane, select **Network Configuration > Network Services > NAT**.
3. Click **Dynamic NAT**.
4. Click the add icon.
5. On the **New Dynamic NAT Rule** page, perform the following tasks:
 - a. Add ACL 2000 to permit packets only from subnet 192.168.1.0/24 to pass through.
 - b. Add address group 0, and add an address range from 202.38.1.2 to 202.38.1.3 to the group.
6. Apply the dynamic NAT rule to VLAN-interface 20.

Verifying the configuration

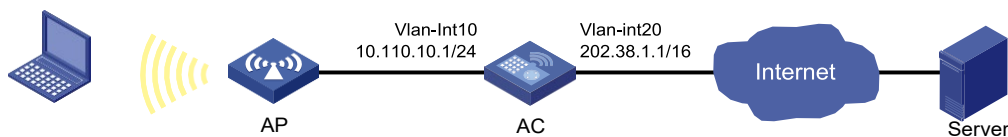
Verify that Client A can access the WWW server, but Client B cannot. (Details not shown.)

Outbound static NAT configuration example


Network requirements

Configure static NAT to enable the client to access the server on the external network.

Figure 6 Network diagram



Configuration procedures

1. Click the system view tab at the bottom of the page.
2. From the navigation pane, select **Network Configuration > Network Services > NAT**.
3. Click **Static NAT**.
4. Click the **Rules** tab.
5. Click the  icon.
6. Select the **Host to host** translation mode.
7. Enter 10.110.10.8 in the private address field and 202.38.1.100 in the public address field.
8. Click **Apply**.
9. Click the **Apply** tab.
10. Select interface VLAN-interface 20.

11. Click **Apply**.

Verifying the configuration

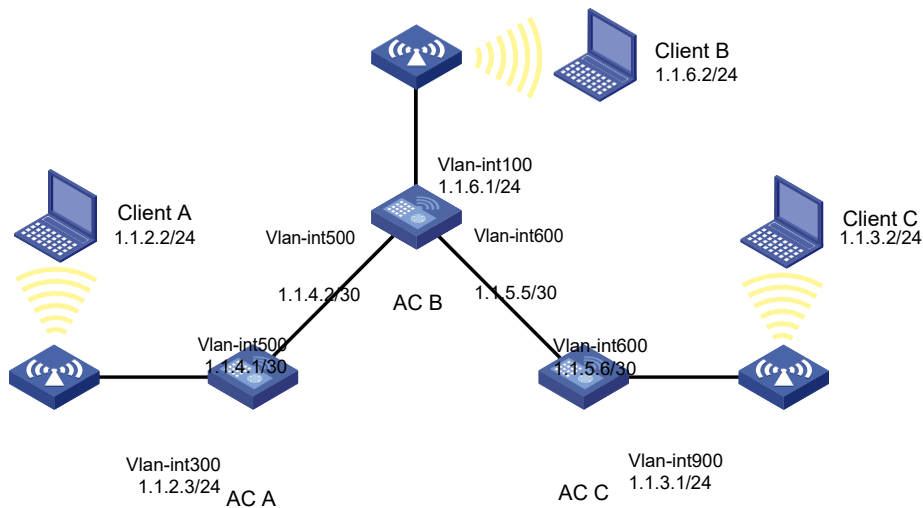
Verify that the client can access the server on the external network.

IPv4 static route configuration example

Network requirements

As shown in [Figure 7](#), configure IPv4 static routes on the ACs for the clients to communicate with each other.

Figure 7 Network diagram



Configuration procedure

1. On AC A, configure a default route:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv4 static routing**.
 - e. Configure the default route:
 - Set the destination IP address to **0.0.0.0**.
 - Set the mask length to **0**.
 - Set the next hop address to **1.1.4.2**.
2. On AC B, configure static routes to reach Client A and Client C:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv4 static routing**.
 - e. Configure a static route to the network that contains Client 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**.
 - f. Configure a static route to the network that contains Client 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**.
- 3. On AC C, configure a default route:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv4 static routing**.
 - e. Configure the 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**.

Verifying the configuration

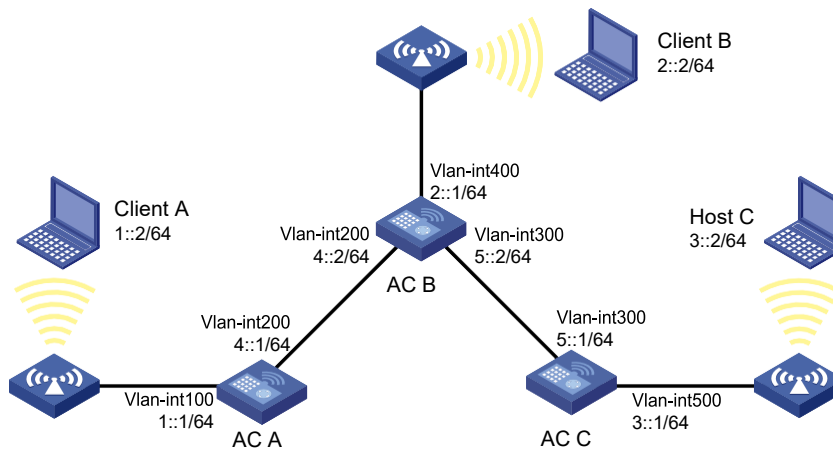
Verify that the clients can ping each other. (Details not shown.)

IPv6 static route configuration example

Network requirements

As shown in [Figure 8](#), configure IPv6 static routes on the ACs for the clients to communicate with each other.

Figure 8 Network diagram



Configuration procedure

1. On AC A, configure an IPv6 default route:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv6 static routing**.
 - e. Configure the IPv6 default route:
 - Set the destination IP address to **::**.
 - Set the mask length to **0**.
 - Set the next hop address to **4::2**.
2. On AC B, configure IPv6 static routes to reach Client A and Client C:
 - a. Click the system view tab at the bottom of the page.

- b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv6 static routing**.
 - e. Configure an IPv6 static route to the network that contains Client C:
 - Set the destination address to **3::2**.
 - Set the mask length to **64**.
 - Set the next hop address to **5::1**.
 - f. Configure an IPv6 static route to the network that contains Client A:
 - Set the destination address to **1::2**.
 - Set the mask length to **64**.
 - Set the next hop address to **4::1**.
3. On AC C, configure an IPv6 default route:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Routing**.
 - c. Click the **Static Routing** tab.
 - d. Click **IPv6 static routing**.
 - e. Configure the IPv6 default route:
 - Set the destination address to **::**.
 - Set the mask length to **0**.
 - Set the next hop address to **5::2**.

Verifying the configuration

Verify that the clients can ping each other successfully. (Details not shown.)

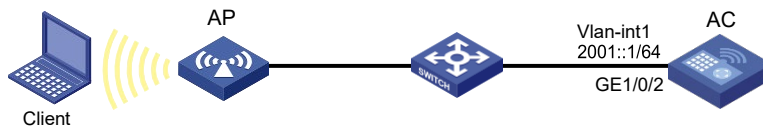
Static IPv6 address configuration example

Network requirements

As shown in [Figure 9](#), the client generates an IPv6 address through stateless address autoconfiguration.

Assign a global unicast IPv6 address to VLAN-interface 1 of the AC.

Figure 9 Network diagram



Configuration procedure

1. Configure wireless service and AP settings. (Details not shown.)
2. Configure an IPv6 address for VLAN-interface 1:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > IP Services**.
 - c. Click the **IPv6** tab.
 - d. Access the details page for VLAN-interface 1 to perform the following tasks:
 - Configure the IPv6 address of the interface as **2001::1**.

- Set the prefix length to **64**.
- 3. Configure VLAN-interface 1 to advertise RA messages.
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > ND**. You are placed on the **ND** tab.
 - c. Access the advanced settings page to configure the RA settings.
 - d. Configure VLAN-interface 1 to advertise RA messages.
- 4. Install IPv6 on the client. The client automatically generates an IPv6 address based on the address prefix information contained in the RA message.

Verifying the configuration

Verify that the client and the AC can ping each other successfully.

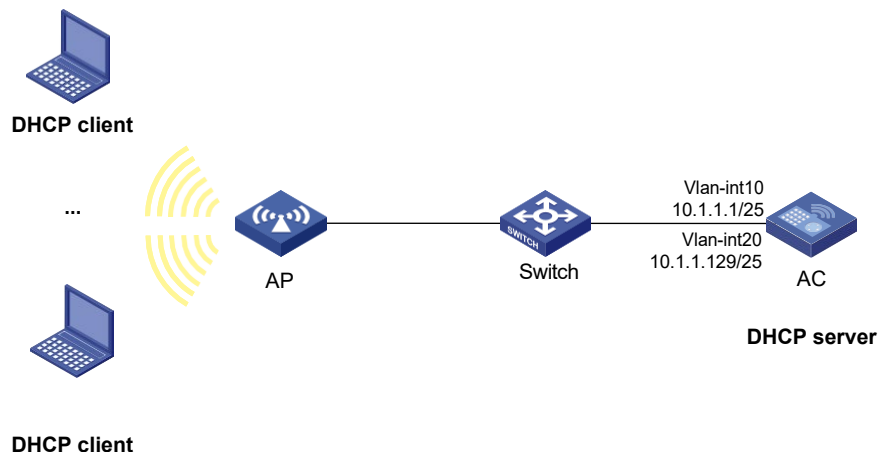
DHCP server configuration example

Network requirements

As shown in Figure 10, the DHCP server (AC) assigns IP addresses to the AP and DHCP clients on subnet 10.1.1.0/24, which is subnetted into 10.1.1.0/25 and 10.1.1.128/25. The AC is connected to the clients and the AP through two VLAN interfaces: VLAN-interface 10 at 10.1.1.1/25 and VLAN-interface 20 at 10.1.1.129/25.

Configure DHCP server on the AC to assign an IP address on subnet 10.1.1.0/25 to the AP and IP addresses on subnet 10.1.1.128/25 to DHCP clients.

Figure 10 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. Configure VLANs and VLAN interfaces:
 - a. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - b. Create VLANs and assign IP addresses to VLAN interfaces:
 - Create VLAN **10** and assign IP address **10.1.1.1/25** to VLAN-interface 10.
 - Create VLAN **20** and assign IP address **10.1.1.129/25** to VLAN-interface 20.
3. Configure the DHCP server:
 - a. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**. You are placed on the **DHCP** tab.
 - b. Enable DHCP.

- c. Specify VLAN-interface 10 and VLAN-interface 20 as DHCP servers.
- d. Click the address pool link and perform the following tasks:
 - Create the address pool **pool1**, specify **10.1.1.0/25** as the subnet for dynamic assignment, and specify **10.1.1.1** as the gateway.
 - Create the address pool **pool2**, specify **10.1.1.128/25** as the subnet for dynamic assignment, and specify **10.1.1.129** as the gateway.
- e. Access the advanced settings page to perform the following tasks:
 - Set the maximum number of ping packets to 1.
 - Set the ping response timeout time to 500 milliseconds.
4. Click the network view tab at the bottom of the page.
5. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **office**.
 - Specify the default VLAN **20**.
 - Enable the wireless service.
6. Configure the AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Add and configure the AP:
 - Set the AP name to **AP1**, and set the AP model and serialID.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to the 5 GHz radio of AP 1.
7. Configure the AP radio:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Set the status of the 5 GHz radio of AP 1 to **On**.

Verifying the configuration

1. Verify that the AP can obtain an IP address on subnet 10.1.1.0/25 and the gateway address from the DHCP server.
2. Verify that the DHCP clients can obtain IP addresses on subnet 10.1.1.128/25 and the gateway address from the DHCP server.

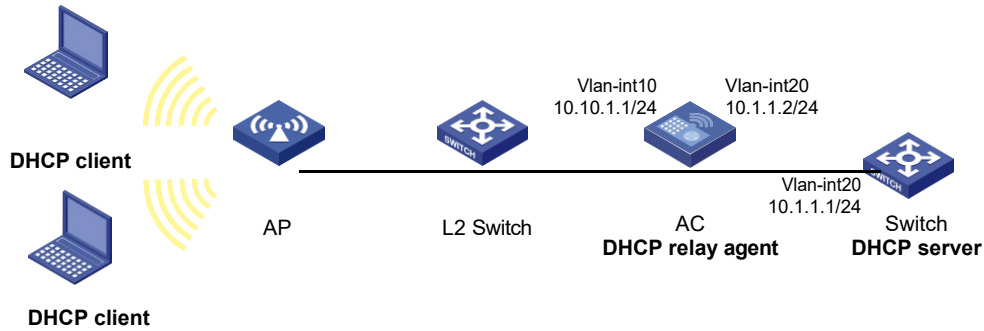
DHCP relay agent configuration example

Network requirements

As shown in [Figure 11](#), the DHCP clients and the DHCP server are in different subnets. The DHCP clients reside in subnet 10.10.1.0/24 and the DHCP server is at 10.1.1.1/24. An AC is deployed between the DHCP clients and the DHCP server. The AC is connected to the network in which the DHCP clients reside through VLAN-interface 10 at 10.10.1.1/24. The AC is connected to the DHCP server through VLAN-interface 20 at 10.1.1.2/24.

Configure the DHCP relay agent on the AC, so the DHCP clients can obtain IP addresses and other configuration parameters from the DHCP server.

Figure 11 Network diagram



Configuration procedure

1. Assign IP addresses to interfaces. (Details not shown.)
2. Configure the DHCP server. (Details not shown.)
3. Configure basic settings on the AC. (Details not shown.)
4. Configure the DHCP relay agent:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**. You are placed on the **DHCP** tab.
 - c. Perform the following tasks:
 - Enable DHCP.
 - Specify VLAN-interface 10 as the DHCP relay agent.
 - Specify the DHCP server address 10.1.1.1.

Verifying the configuration

Verify that the DHCP clients can obtain IP addresses and other configuration parameters from the DHCP server through the DHCP relay agent.

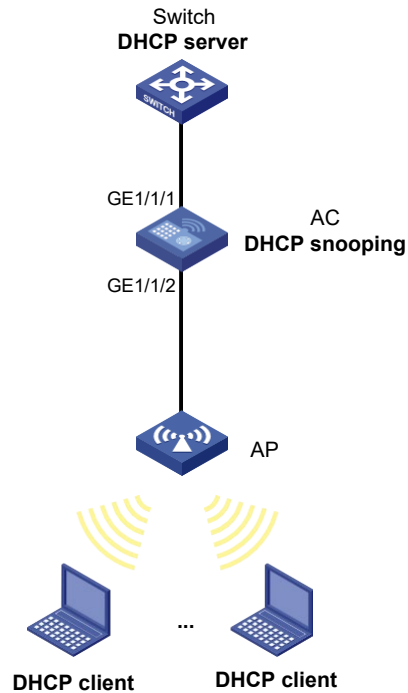
DHCP snooping configuration example

Network requirements

As shown in [Figure 12](#), the AC is connected to a DHCP server through GigabitEthernet 1/1/1 and to an AP through GigabitEthernet 1/1/2. Configure DHCP snooping on the AC to meet the following requirements:

- Allow only the interface connected to the authorized DHCP server to forward packets from the DHCP server.
- Record the clients' IP-to-MAC binding information in DHCP-REQUEST packets and in DHCP-ACK packets received by trusted ports.

Figure 12 Network diagram



Configuration procedure

1. Configure the DHCP server. (Details not shown.)
2. Configure basic settings on the AC. (Details not shown.)
3. Configure the DHCP snooping device:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
 - c. Click the **DHCP Snooping** tab.
 - d. Perform the following tasks:
 - Enable DHCP snooping.
 - Configure GigabitEthernet 1/1/1, the interface connected to the authorized DHCP server, as the trusted port.
 - Configure GigabitEthernet 1/1/2, the interface connected to the DHCP clients, to record DHCP snooping entries.

Verifying the configuration

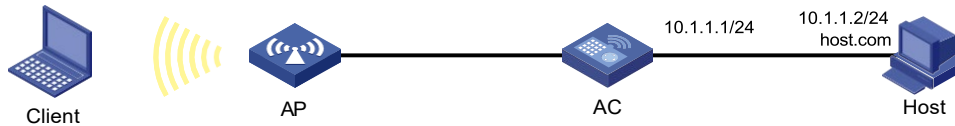
Verify that the AC maintains DHCP snooping entries for clients that have obtained IP addresses through DHCP.

IPv4 static DNS configuration example

Network requirements

As shown in [Figure 13](#), configure a static DNS entry on the AC, so the AC can use the domain name **host.com** to access the host at 10.1.1.2.

Figure 13 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
3. Click the **IPv4 DNS** tab.
4. 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 AC to verify the following items:

- The ping operation succeeds.
- The AC can use static domain name resolution to resolve the domain name **host.com** into the IPv4 address **10.1.1.2**.

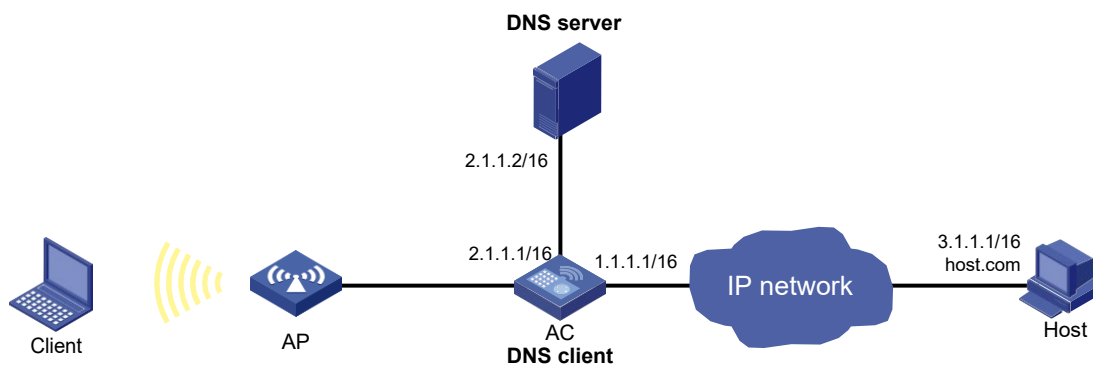
IPv4 dynamic DNS configuration example

Network requirements

As shown in Figure 14, the DNS server at 2.1.1.2/16 has a **com** domain that stores the mapping between the domain name **host** and the IPv4 address 3.1.1.1/16.

Configure dynamic DNS and the DNS suffix **com** on the AC that acts as a DNS client. The AC can use the domain name **host** to access the host whose domain name is **host.com** and IPv4 address is 3.1.1.1/16.

Figure 14 Network diagram



Configuration procedure

1. Map the domain name **host.com** to the IPv4 address 3.1.1.1 on the DNS server. (Details not shown.)
2. Configure static routes or dynamic routing protocols on the devices to make sure the devices can reach each other. (Details not shown.)
3. Configure DNS client on the AC:

- a. Click the system view tab at the bottom of the page.

- b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
- c. Click the **IPv4 DNS** tab.
- d. Specify the DNS server address **2.1.1.2**.
- e. Access the advanced settings page and add the domain name suffix **com**.

Verifying the configuration

Use the **ping host** command on the AC to verify the following items:

- The ping operation succeeds.
- The AC can resolve the domain name **host.com** into the IPv4 address **3.1.1.1** through the DNS server.

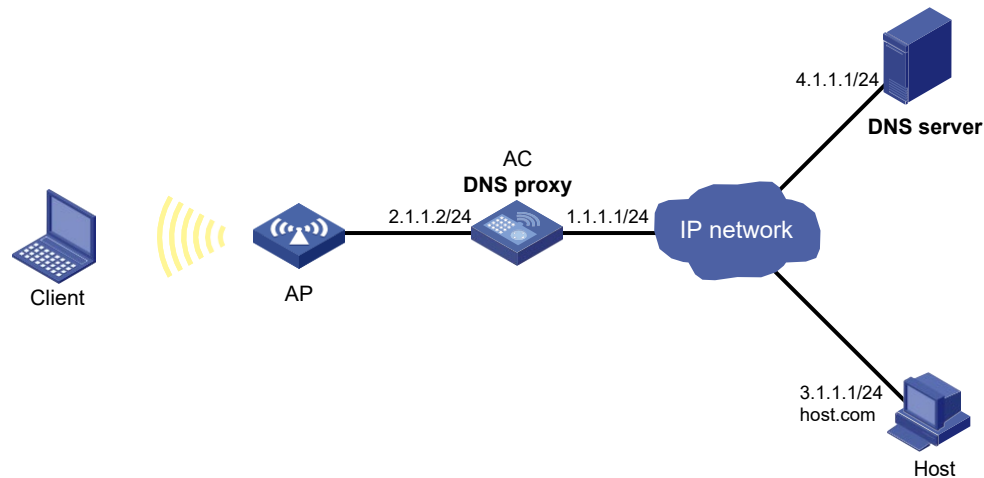
IPv4 DNS proxy configuration example

Network requirements

As shown in Figure 15, the LAN has a large number of devices deployed. The devices access the DNS server for domain name resolution. If the DNS server's IP address changes, the administrator must modify the DNS server address on each device, which takes a lot of time.

To simplify the configuration, configure the AC as the DNS proxy. Specify the real DNS server address on the AC. Specify the DNS proxy address as the DNS server address on the other devices. If the DNS server address changes, the administrator only needs to modify the DNS server address on the DNS proxy.

Figure 15 Network diagram



Configuration procedure

1. Configure static routes or dynamic routing protocols on the devices to make sure the devices can reach each other. (Details not shown.)
2. Configure the DNS server. (Details not shown.)
3. Configure DNS proxy on the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
 - c. Click the **IPv4 DNS** tab.
 - d. Specify the DNS server address **4.1.1.1**.

- e. On the advanced settings page, enable DNS proxy.
4. Configure DNS clients.
Specify the DNS proxy address **2.1.1.2** as the DNS server address on the other devices that act as DNS clients.

Verifying the configuration

Use the **ping host.com** command on a DNS client to verify the following items:

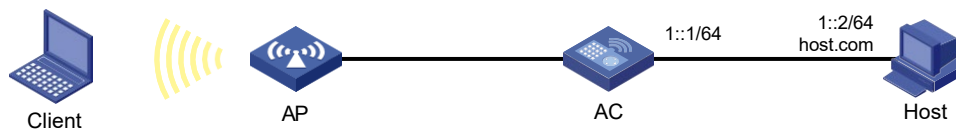
- The ping operation succeeds.
- The client can resolve the domain name **host.com** into the IPv4 address **3.1.1.1** through the DNS server.

IPv6 static DNS configuration example

Network requirements

As shown in [Figure 16](#), configure a static DNS entry on the AC, so the AC can use the domain name **host.com** to access the host at 1::2.

Figure 16 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
3. Click the **IPv6 DNS** tab.
4. Create a static DNS entry:
 - Configure the host name as **host.com**.
 - Configure the IPv6 address as **1::2**.

Verifying the configuration

Use the **ping ipv6 host.com** command on the AC to verify the following items:

- The ping operation succeeds.
- The AC can use static domain name resolution to resolve the domain name **host.com** into the IPv6 address **1::2**.

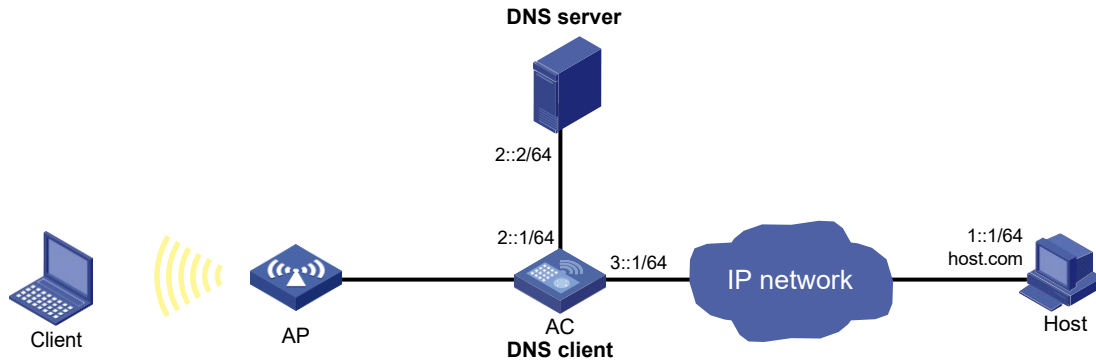
IPv6 dynamic DNS configuration example

Network requirements

As shown in [Figure 17](#), the DNS server at 2::2/64 has a **com** domain that stores the mapping between the domain name **host** and the IPv6 address 1::1/64.

Configure dynamic DNS and the DNS suffix **com** on the AC that acts as a DNS client. The AC can use the domain name **host** to access the host whose domain name is **host.com** and IPv6 address is 1::1/64.

Figure 17 Network diagram



Configuration procedure

1. Map the domain name **host.com** to the IPv6 address 1::1 on the DNS server. (Details not shown.)
2. Configure static routes or dynamic routing protocols on the devices to make sure the devices can reach each other. (Details not shown.)
3. Configure DNS client on the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
 - c. Click the **IPv6 DNS** tab.
 - d. Specify the DNS server address **2::2**.
 - e. Access the advanced settings page and add the domain name suffix **com**.

Verifying the configuration

Use the **ping ipv6 host** command on the AC to verify the following items:

- The ping operation succeeds.
- The AC can resolve the domain name **host.com** into the IPv6 address **1::1** through the DNS server.

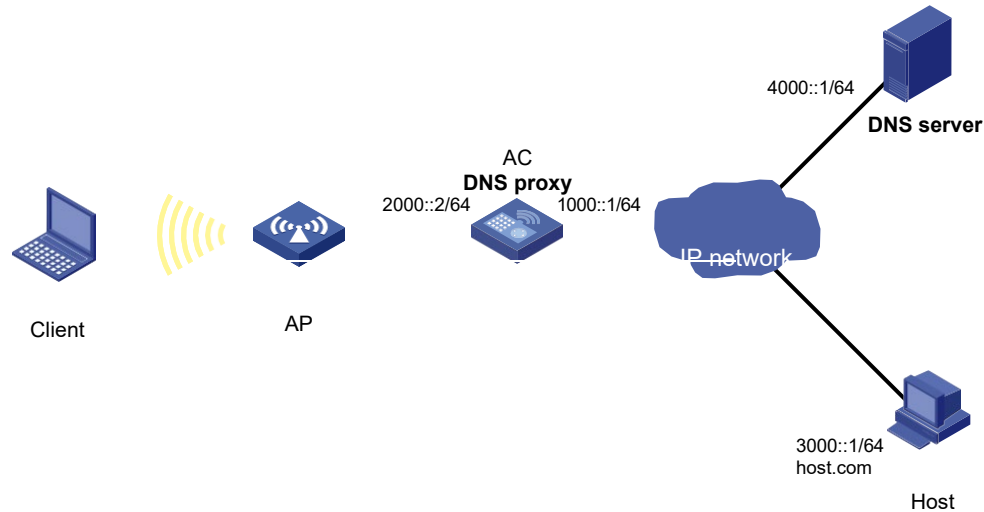
IPv6 DNS proxy configuration example

Network requirements

As shown in [Figure 18](#), the LAN has a large number of devices deployed. The devices access the DNS server for domain name resolution. If the DNS server's IPv6 address changes, the administrator must modify the DNS server address on each device, which takes a lot of time.

To simplify the configuration, configure the AC as the DNS proxy. Specify the real DNS server address on the AC. Specify the DNS proxy address as the DNS server address on the other devices. If the DNS server address changes, the administrator only needs to modify the DNS server address on the DNS proxy.

Figure 18 Network diagram



Configuration procedure

1. Configure static routes or dynamic routing protocols on the devices to make sure the devices can reach each other. (Details not shown.)
2. Configure the DNS server. (Details not shown.)
3. Configure DNS proxy on the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
 - c. Click the **IPv6 DNS** tab.
 - d. Specify the DNS server address **4000::1**.
 - e. On the advanced settings page, enable DNS proxy.
4. Configure DNS clients.

Specify the DNS proxy address **2000::2** as the DNS server address on the other devices that act as DNS clients.

Verifying the configuration

Use the **ping ipv6 host.com** command on a DNS client to verify the following items:

- The ping operation succeeds.
- The client can resolve the domain name **host.com** into the IPv6 address **3000::1** through the DNS server.

IGMP snooping configuration example

Network requirements

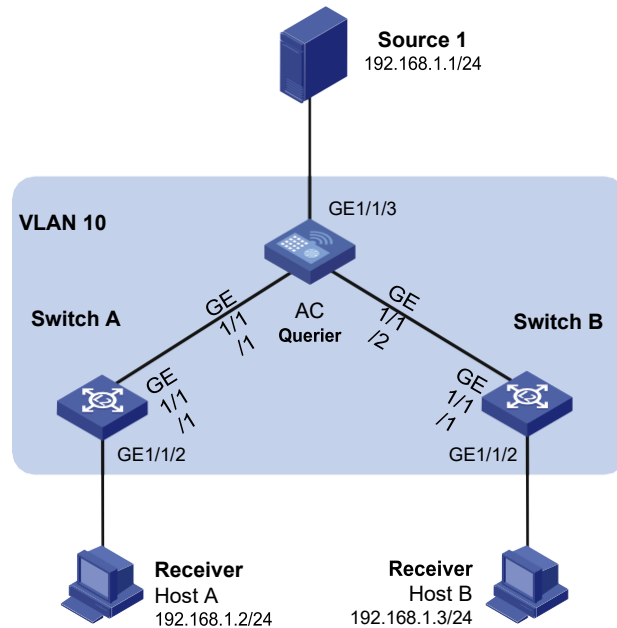
As shown in [Figure 19](#):

- The network is a Layer 2-only network.
- Source 1 sends multicast data to the multicast group 224.1.1.1, and Host A and Host B are receivers of the group.
- Host A and Host B run IGMPv2. The AC, Switch A, and Switch B run IGMPv2 snooping, and the AC acts as the IGMP querier.

Configure the devices to meet the following requirements:

- For IGMP snooping forwarding entries to be created, configure the source IP address of IGMP queries as a non-zero IP address on the AC.
- To prevent unknown multicast data from being flooded in VLAN 10, enable the devices to drop unknown multicast data.

Figure 19 Network diagram



Configuration procedure

1. Configure the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > Multicast**. You are placed on the **IGMP Snooping** tab.
 - c. Enable IGMP snooping.
 - d. Access the page for enabling IGMP snooping on a VLAN to perform the following tasks:
 - Set the VLAN ID to 10.
 - Set the IGMP snooping version to 2.
 - Enable dropping unknown multicast data.
 - Enable the AC to act as the IGMP querier.
 - Set the source IP address to 192.168.1.10 for IGMP general queries.
 - Set the source IP address to 192.168.1.10 for IGMP group-specific queries.
2. Configure Switch A:

Enable IGMP snooping for VLAN 10, set the IGMP snooping version to 2, and then enable dropping unknown multicast data. (Details not shown.)
3. Configure Switch B in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

1. Send IGMP reports from Host A and Host B to join the multicast group 224.1.1.1. (Details not shown.)
2. Send multicast data from the source to the multicast group. (Details not shown.)

3. Access the **Network Configuration > Network Services > Multicast > IGMP snooping > Entries** page to verify that GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 are host ports of VLAN 1.

MLD snooping configuration example

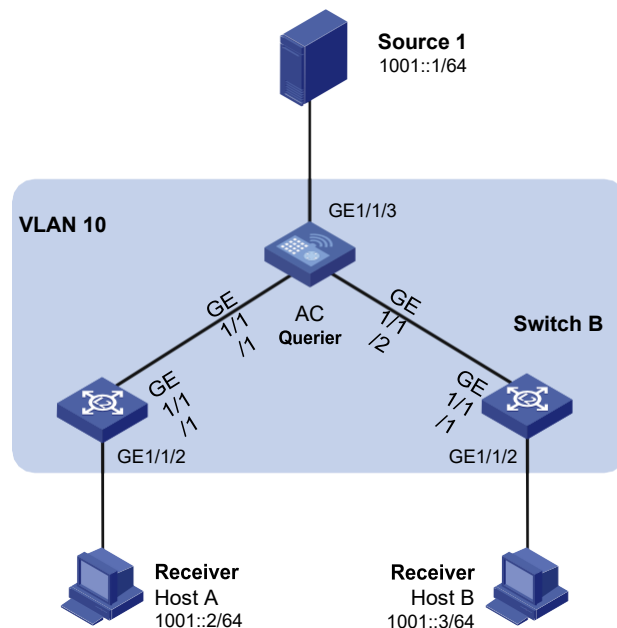
Network requirements

As shown in [Figure 20](#):

- The network is a Layer 2-only network.
- Source 1 sends IPv6 multicast data to the IPv6 multicast group FF1E::101. Host A and Host B are receivers of the group.
- Host A and Host B run MLDv1. The AC, Switch A, and Switch B run MLDv1 snooping, and the AC acts as the MLD querier.

To prevent unknown IPv6 multicast data from being flooded in VLAN 10, enable all the devices to drop unknown IPv6 multicast data.

Figure 20 Network diagram



Configuration procedure

1. Configure the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > Multicast**. You are placed on the **IGMP Snooping** tab.
 - c. Click the **MLD Snooping** tab, and then enable MLD snooping.
 - d. Access the page for enabling MLD snooping on a VLAN to perform the following tasks:
 - Set the VLAN ID to 10.
 - Set the MLD snooping version to 1.
 - Enable dropping unknown IPv6 multicast data.
 - Enable the AC to act as an MLD querier.
 - Apply the configuration.

2. Configure Switch A:
Enable MLD snooping for VLAN 10, set the MLD snooping version to 1, and then enable dropping unknown IPv6 multicast data. (Details not shown.)
3. Configure Switch B in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

1. Send MLD reports from Host A and Host B to join the IPv6 multicast group FF1E::101. (Details not shown.)
2. Send IPv6 multicast data from Source 1 to the IPv6 multicast group. (Details not shown.)
3. Access the **Network Configuration > Network Services > Multicast > MLD snooping > Entries** page to verify that GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 are host ports of VLAN 1.

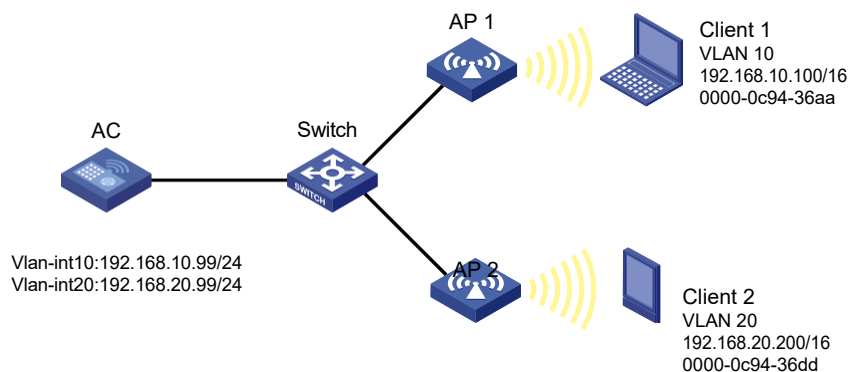
Proxy ARP configuration example

Network requirements

As shown in [Figure 21](#), Client 1 and Client 2 have the same IP prefix and mask, but they are located on different subnets separated by the AC. Client 1 belongs to VLAN 10, and Client 2 belongs to VLAN 20. No default gateway is configured on Client 1 and Client 2.

Configure proxy ARP on the AC to enable communication between the two clients.

Figure 21 Network diagram



Configuration procedure

1. Configure VLAN 10 and VLAN 20, and assign IP addresses to VLAN-interface 10 and VLAN-interface 20:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - c. Create VLAN 10, and assign IP address 192.168.10.99/24 to VLAN-interface 10.
 - d. Create VLAN 20, and assign IP address 192.168.20.99/24 to VLAN-interface 20.
2. Enable proxy ARP on VLAN-interface 10 and VLAN-interface 20.
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > ARP**. You are placed on the **ARP** tab.
 - c. Access the advanced settings page to configure proxy ARP.
 - Enable proxy ARP on VLAN-interface 10.
 - Enable proxy ARP on VLAN-interface 20.

Verifying the configuration

```
# Verify that Client 1 and Client 2 can ping each other successfully.
```

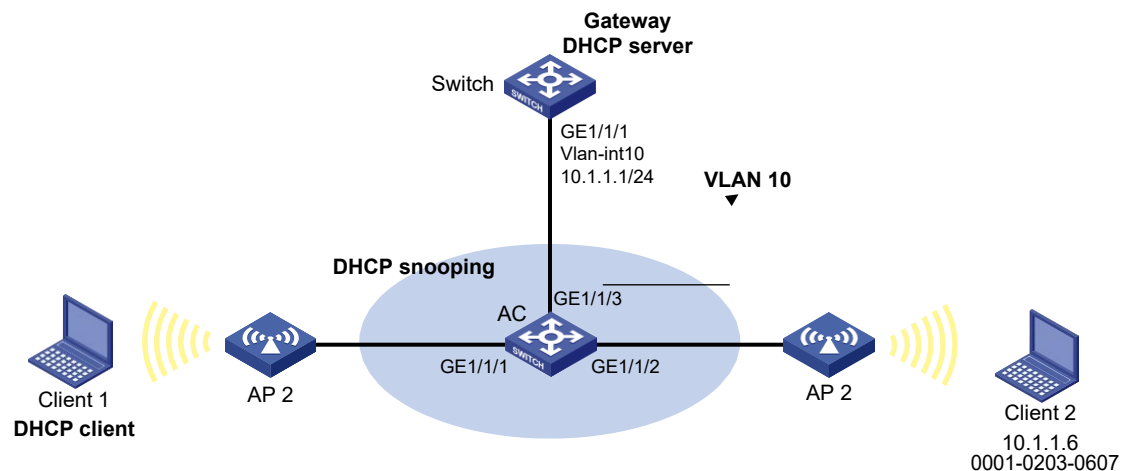
ARP attack protection configuration example

Network requirements

As shown in [Figure 22](#), Client 1 obtains an IP address from the switch (DHCP server). Client 2 is manually assigned IP address 10.1.1.6.

Configure the AC to perform ARP packet validity check and user validity check for connected clients.

Figure 22 Network diagram



Configuration procedure

1. Assign all interfaces to VLAN 10, and specify the IP address of VLAN-interface 10 on the switch. (Details not shown.)
2. Configure the DHCP server on the switch. (Details not shown.)
3. Configure Client 1 (the DHCP client) and Client 2. (Details not shown.)
4. Enable DHCP snooping on the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**.
 - c. Click the **DHCP Snooping** tab.
 - d. Enable DHCP snooping.
 - e. Configure GigabitEthernet 1/1/3 as a trusted port.
 - f. Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/1/1.
5. Configure ARP detection on the AC:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Network Services > ARP**. You are placed on the **ARP** tab.
 - c. Access the advanced settings page to configure ARP detection under ARP attack protection.
 - d. Enable ARP detection for VLAN 10.
 - e. Access the advanced settings page for ARP detection to perform the following tasks:
 - Configure GigabitEthernet 1/1/3 as a trusted interface.

By default, an interface is an untrusted interface.

- Enable ARP packet validity check by checking the sender MAC address, target MAC address, and IP addresses of ARP packets.

After the configurations are completed, the AC first checks the validity of ARP packets received on GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2. If the ARP packets are confirmed valid, the switch performs user validity check by using the DHCP snooping entries.

Verifying the configuration

Access the ARP page to verify that ARP entry for Client 1 is created and no ARP entry is created for Client 2.

Using the AC as the Stelnet server for password authentication configuration example

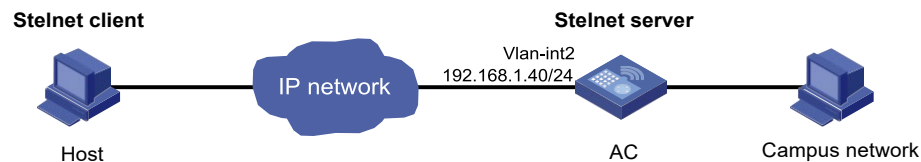
Network requirements

As shown in [Figure 23](#):

- The AC acts as the Stelnet server and uses password authentication.
- The username and password of the client are saved on the AC.

Establish an Stelnet connection between the host and the AC, so you can log in to the AC to configure and manage the AC.

Figure 23 Network diagram



Configuration procedure

1. Configure the Stelnet server:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Management Protocols**.
 - c. Click the **SSH** tab.
 - d. Enable the Stelnet service.
2. Configure the VLAN interface:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > VLAN**.
 - c. On the **VLAN** tab, create VLAN 2.
 - d. Click the edit icon for VLAN 2.
The **Edit VLAN** page opens.
 - e. Add GigabitEthernet 1/1/2 to the untagged port list.
 - f. Select **Configure VLAN interface**.
 - g. Set the IPv4 address/mask to 192.168.1.40/24.
3. Configure the administrator account:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **System > Administrators**.
 - c. Click the add icon.

- d. Set the username and password to **client** and **aabbcc**, respectively.
- e. Select **network-admin** from the user roles list.
- f. Select **SSH** for the permitted access types parameter.

Verifying the configuration

This example uses PuTTY0.58 to verify the configuration.

1. Execute PuTTY on the host.
2. Enter **192.168.1.40** in the **Host Name (or IP address)** field.
3. Click **Open**.
4. Verify that you can use username **client** and password **aabbcc** to log in to the configuration page of the AC.

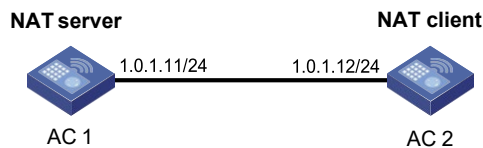
NTP configuration example

Network requirements

As shown in [Figure 24](#):

- Configure the local clock of AC 1 as a reference source, with the stratum level 2.
- Set AC 2 to client mode and use AC 1 as the NTP server for AC 2.

Figure 24 Network diagram



Configuration procedure

1. Configure AC 1 (NTP server):
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Configuration > Management Protocols**.
 - c. Click the **NTP** tab.
 - d. Enable the NTP service.
 - e. Specify the IP address of the local clock as **127.127.1.0**.
 - f. Configure the stratum level of the local clock as **2**.
2. Configure AC 2:
 - a. Click the system view tab at the bottom of the page.
 - b. From the navigation pane, select **System > Management**. You are placed on the **Settings** tab.
 - c. Select automatic time synchronization with a trusted time source, and then select NTP as the time protocol.
 - d. 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 AC 2 has synchronized to AC 1, and the clock stratum level is 3 on AC 2 and 2 on AC 1.

Network security configuration examples

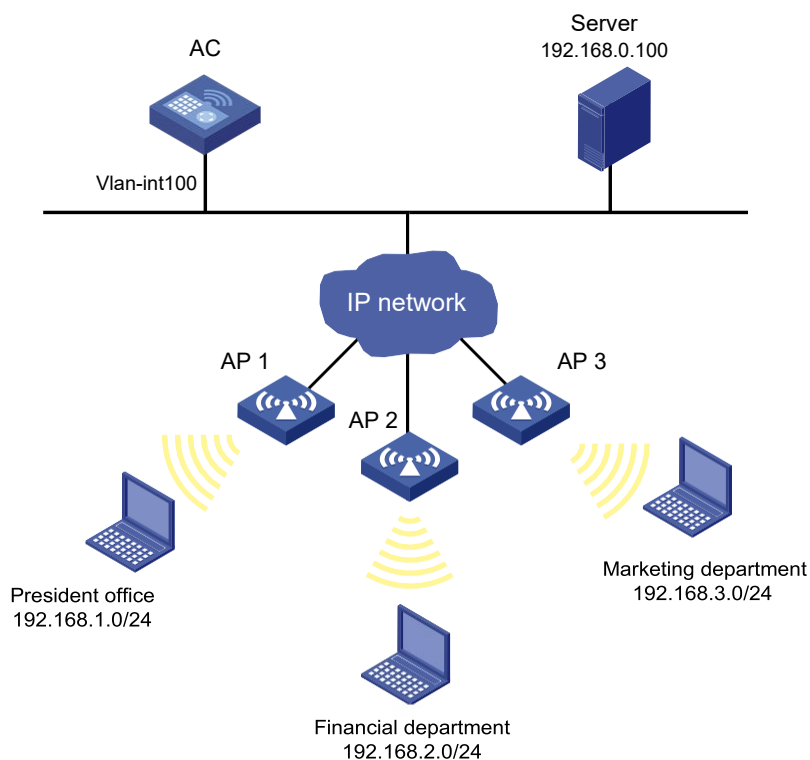
ACL-based packet filter configuration example

Network requirements

As shown in Figure 25, a company interconnects its departments through the AC. Configure the packet filter on the AC to meet the following requirements:

- Permit access from the President's office at any time to the financial database server.
- Permit access from the Financial Department to the financial database server only during working hours (from 8:00 to 18:00) on working days.
- Deny access from any other department to the financial database server.

Figure 25 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. From the navigation pane, select **Network Security > Packet Filter**.
3. Create a packet filter policy:
 - a. Select VLAN-interface 100.
 - b. Select the outbound application direction.
 - c. Select the IPv4 ACL type for packet filter.
4. 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: 192.168.1.0/0.0.0.255 Destination: 192.168.0.100/0	N/A
Permit	256	Source: 192.168.2.0/0.0.0.255 Destination: 192.168.0.100/0	Create a time range named work : <ul style="list-style-type: none"> Specify the start time as 08:00. Specify the end time as 18:00. Select Monday through Friday.
Deny	256	Destination: 192.168.0.100/0	N/A

5. Enable rule match counting for the ACL.

Verifying the configuration

1. Ping the database server from different departments to verify the following items:
 - o You can access the server from the President's office at any time.
 - o You can access the server from the Financial Department during the working hours on working days.
 - o You cannot access the server from the Marketing Department at any time.
2. Access the ACL rule Web interface, verify that the ACL rules are active and the number of matching packets is displayed.

System configuration examples

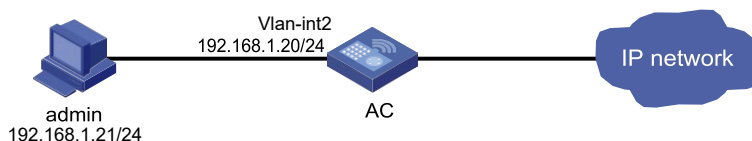
Administrators configuration example

Network requirements

As shown in [Figure 26](#), configure an administrator account with the username **webuser** and password **12345** on the AC to meet the following requirements:

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

Figure 26 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. Configure the VLAN and VLAN interface:
 - a. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - b. Create VLAN 2.
 - c. Access the edit 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.
- 3. Configure an administrator account:
 - a. From the navigation pane, select **System > Administrators**. You are placed on the **Administrators** tab.
 - b. Create and configure an administrator account:
 - Set the username and the password to **webuser** and **12345**, respectively.
 - Select the network-admin user role.
 - Specify HTTP and HTTPS as the permitted access types.

Verifying the configuration

1. Access the **System > Administrators** page to verify that the administrator account is successfully added.
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.

Network configuration examples

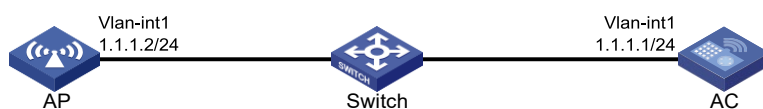
Wireless configuration examples

CAPWAP tunnel establishment through DHCP configuration example

Network requirements

As shown in [Figure 27](#), configure the AP to obtain its IP address and the AC's IP address from the DHCP server (the AC) through DHCP Option 43. The AP uses the IP address of the AC to establish a CAPWAP tunnel with the AC.

Figure 27 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. Set the AC IP address:
 - a. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - b. Click the edit icon in the operation column for VLAN-interface 1.
 - c. Set the IP address to **1.1.1.1/24**.
3. Configure DHCP:
 - a. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**. You are placed on the **DHCP** tab.
 - b. Enable the DHCP service.
 - c. Access the DHCP configuration page to select **DHCP server** from the **DHCP service** list for VLAN-interface 1.
 - d. Access the address pool configuration page. You are placed on the **Assigned Address** tab.
 - e. Click **Add Address Pool** and then perform the following tasks:
 - Create an address pool named **pool1**.
 - Specify subnet **1.1.1.0/24** for dynamic IP address assignment.
 - f. Click the **DHCP Options** tab.
 - g. Perform the following tasks:
 - Set the gateway address to **1.1.1.1**.
 - Configure DHCP Option 43 to specify the AC's IP address in the hexadecimal format. The option content is **800700000101010101** in this example.
4. Click the network view tab at the bottom of the page.
5. Configure the AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.

- b. Add and configure AP 1:
 - Set the AP name to **AP1**.
 - Set the AP model and serial ID.

Verifying the configuration

Access the **Wireless Configuration > AP Management > AP** page to verify that AP 1 has come online.

Access the AP details page to verify the following information:

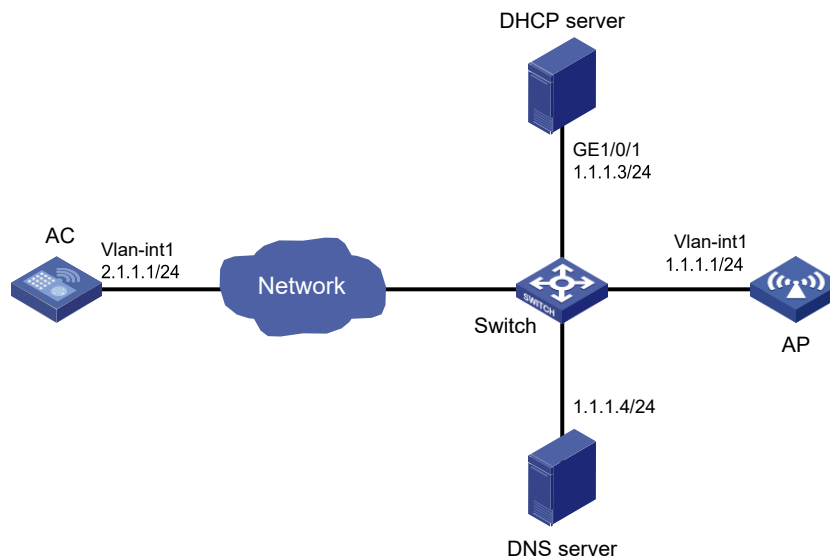
- The AP has obtained an IP address.
- The AC IP address is 1.1.1.1/24.
- The AC discovery type is DHCP.

CAPWAP tunnel establishment through DNS configuration example

Network requirements

As shown in [Figure 28](#), configure the AP to obtain the IP address of the AC through DNS to establish a CAPWAP tunnel with the AC.

Figure 28 Network diagram



Configuration procedure

1. On the DHCP server, specify subnet **1.1.1.0/24** for IP address assignment, set the domain name suffix of the AC to **abc**, and specify the DNS server address as **1.1.1.4/24**. (Details not shown.)
2. On the DNS server, configure a mapping between domain name **host.abc** and IP address **1.1.1.1/24**. (Details not shown.)
3. Click the system view tab at the bottom of the page.
4. Set the AC's IP address:
 - a. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - b. Click the edit icon in the operation column for VLAN-interface 1.
 - c. Set the IP address to **2.1.1.1/24**.

5. Click the network view tab at the bottom of the page.
6. Configure the AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**.
 - Set the AP model and serial ID.

Verifying the configuration

Access the **Wireless Configuration > AP Management > AP** page to verify that AP 1 has come online.

Access the AP details page to verify the following information:

- The AP has obtained an IP address.
- The AC's IP address is 1.1.1.1/24.
- The AC discovery type is DNS.

Auto AP configuration example

Network requirements

As shown in [Figure 29](#), enable the auto AP feature on the AC. The AP obtains the AC's IP address through DHCP Option 43 and establishes a CAPWAP tunnel with the AC.

Figure 29 Network diagram



Configuration procedure

1. Click the system view tab at the bottom of the page.
2. Set the AC IP address:
 - a. From the navigation pane, select **Network Configuration > VLAN**. You are placed on the **VLAN** tab.
 - b. Click the edit icon in the operation column for VLAN-interface 1.
 - c. Set the IP address to **1.1.1.1/24**.
3. Configure DHCP:
 - a. From the navigation pane, select **Network Configuration > Network Services > DHCP/DNS**. You are placed on the **DHCP** tab.
 - b. Enable the DHCP service.
 - c. Access the DHCP configuration page to select **DHCP server** from the **DHCP service** list for VLAN-interface 1.
 - d. Access the address pool configuration page. You are placed on the **Assigned Address** tab.
 - e. Click **Add Address Pool** and then perform the following tasks:
 - Create an address pool named **pool1**.
 - Specify subnet **1.1.1.0/24** for dynamic IP address assignment.
 - f. Click the **DHCP Options** tab.
 - g. Perform the following tasks:

- Set the gateway address to **1.1.1.1**.
 - Configure DHCP Option 43 to specify the AC's IP address in the hexadecimal format. The option content is **800700000101010101** in this example.
4. Click the network view tab at the bottom of the page.
 5. Configure the AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**.
 - b. Click the **AP Global Settings** tab.
 - c. Enable the auto AP feature.

Verifying the configuration

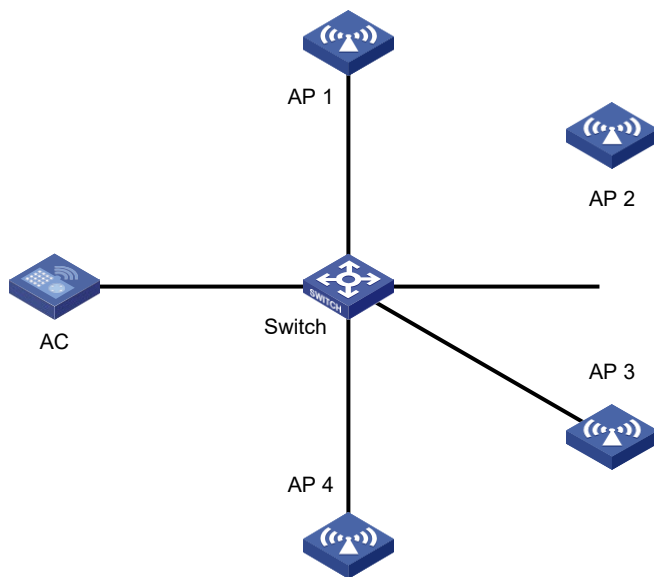
Access the **Wireless Configuration > AP Management > AP** page to verify that AP 1 has come online as an auto AP.

AP group configuration example

Network requirements

As shown in [Figure 30](#), configure AP groups and add AP 1 to the AP group **group1**, and AP 2, AP 3, and AP 4 to the AP group **group2**.

Figure 30 Network diagram



Configuration procedure

1. Configure APs to obtain their IP addresses and the AC's IP address from the DHCP server. (Details not shown.)
2. Click the network view tab at the bottom of the page.
3. Configure the AP groups:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**.
 - b. Click the **AP Groups** tab.
 - c. Add AP group **group1**, and create an AP name grouping rule to add AP **ap1** to the AP group.
 - d. Add AP group **group2**, and create an AP name grouping rule to add APs **ap2**, **ap3**, and **ap4** to the AP group.

Verifying the configuration

Access the AP groups page to verify the following information:

- The AP **ap1** is in the AP list of the AP group **group1**.
- The APs **ap 2**, **ap 3**, and **ap 4** are in the AP list of the AP group **group2**.

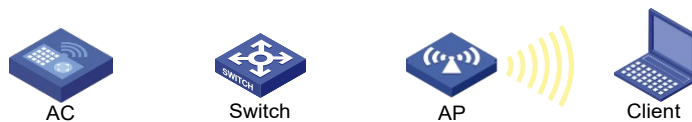
Radio management configuration example

Network requirements

As shown in [Figure 31](#), perform the following tasks to configure the 5 GHz radio of the AP:

- Set the radio type, working channel, and maximum transmit power to 802.11ac, 48, and 19 dBm, respectively.
- Set the maximum mandatory NSS, maximum supported NSS, multicast NSS, and VHT-MCS index to 2, 3, 2, and 5, respectively.
- Enable the A-MSDU and A-MPDU aggregation methods to improve network throughput.

Figure 31 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.
3. Access the details page for all AP radio configurations.
4. Click the edit icon in the operation column for the 5 GHz radio of the AP. You are placed on the **Basic** tab.
5. Perform the following tasks in the basic configuration area:
 - a. Enable the radio.
 - b. Set the radio type to **802.11ac (5GHz)**.
 - c. Set the channel to **48**.
 - d. Set the maximum transmit power to **19 dBm**.
6. Perform the following tasks in the rates configuration area:
 - a. Set the maximum mandatory NSS to **2**.
 - b. Set the maximum supported NSS to **3**.
 - c. Set the multicast NSS to **2**.
 - d. Set the VHT-MCS index to **5**.
7. Perform the following tasks in the 802.11n/802.11ac configuration area:
 - a. Enable the A-MSDU aggregation method.
 - b. Enable the A-MPDU aggregation method.
8. Apply the configuration.

Verifying the configuration

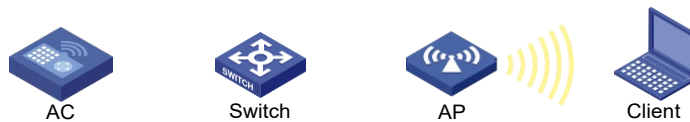
Access the **Wireless Configuration > Radio Management > Radio Configuration** page to verify that the configuration is correct.

Scheduled radio shutdown configuration example

Network requirements

As shown in [Figure 33](#), the AP connects to the AC through the switch. Configure the system to shut down radio 1 on the AP during non-working hours (including weekends and 00:00-08:00 and 22:00-24:00 on working days).

Figure 32 Network diagram



Configuration procedure

1. Configure a wireless service:
 - a. Click the network view tab at the bottom of the page.
 - b. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - c. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **service**.
 - Enable the wireless service.
2. Configure the AP:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure the AP:
 - Set the AP name to **AP**, and configure the AP model and serial number,.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 1 of the AP.
3. Configure scheduled radio shutdown:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the more icon in the scheduled radio shutdown area.
 - c. Select radio 1 of the AP.
 - d. Add the following periodic time ranges:
 - 00:00-08:00 from Monday to Friday.
 - 22:00-24:00 from Monday to Friday.
 - 00:00-24:00 for Saturday and Sunday.

Verifying the configuration

Access the **Wireless Configuration > Radio Management > Radio Configuration** page, and verify that the scheduled shutdown task has been added successfully.

Verify that the task is in effective during the radio-off time and clients cannot access the WLAN.

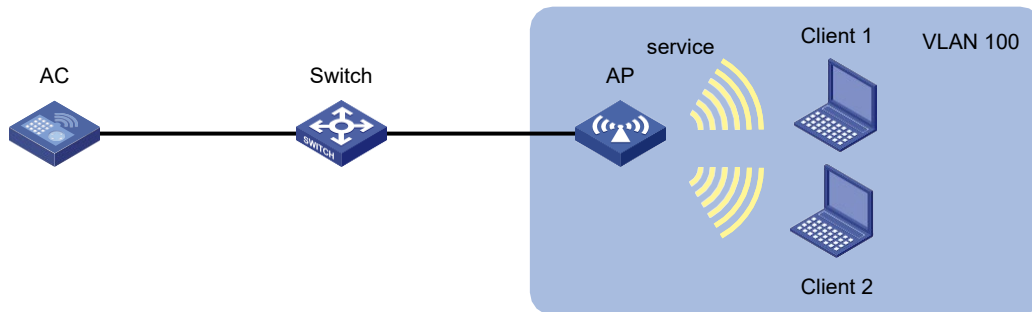
Verify that the radio is in up state if the system time is not within the radio-off time and clients can access the WLAN.

AP configuration file deployment configuration example

Network requirements

As shown in [Figure 33](#), the AP connects to the AC through the switch. Configure the AC to deploy a configuration file to the AP to isolate Client 1 and Client 2.

Figure 33 Network diagram



Configuration procedure

1. Configure the AP to obtain its IP address and the AC's IP address through DHCP, and configure wireless services and radio settings. (Details not shown.)
2. Edit the AP configuration file, add user isolation commands to the file, and name the file **apcfg.txt**.
3. Click the network view tab at the bottom of the page.
4. From the navigation pane, select **Wireless Configuration > AP Management**.
5. On the **AP** tab, click **Edit** for the target AP, select map file **apcfg.txt** for the AP, and then click **OK**.

Verifying the configuration

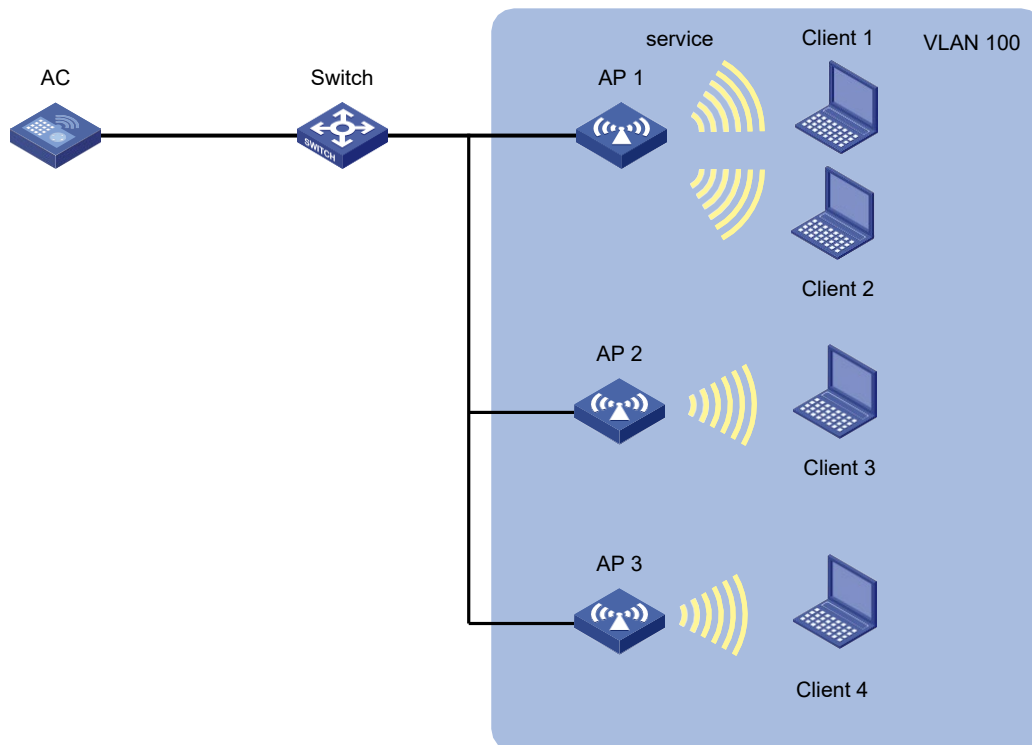
Verify that Client 1 and Client 2 can access the Internet, but cannot reach each other.

AP group configuration file deployment configuration example

Network requirements

As shown in [Figure 34](#), the APs connect to the AC through the switch. Add the APs to the same AP group and configure the AC to deploy a configuration file to the AP group to isolate clients associated with the same AP.

Figure 34 Network diagram



Configuration procedure

1. Configure the APs to obtain their IP addresses and the AC's IP address through DHCP, add the APs to the same AP group, and configure wireless services and radio settings. (Details not shown.)
2. Edit the AP group configuration file, add user isolation configuration commands to the file, and name the file **apcfg.txt**.
3. Click the network view tab at the bottom of the page.
4. From the navigation pane, select **Wireless Configuration > AP Management**.
5. Click the **AP Groups** tab.
6. Click **Edit** for the target AP group, select map file **apcfg.txt** for the AP group, and then click **OK**.

Verifying the configuration

Verify that Client 1 and Client 2 can access the Internet, but cannot reach each other.

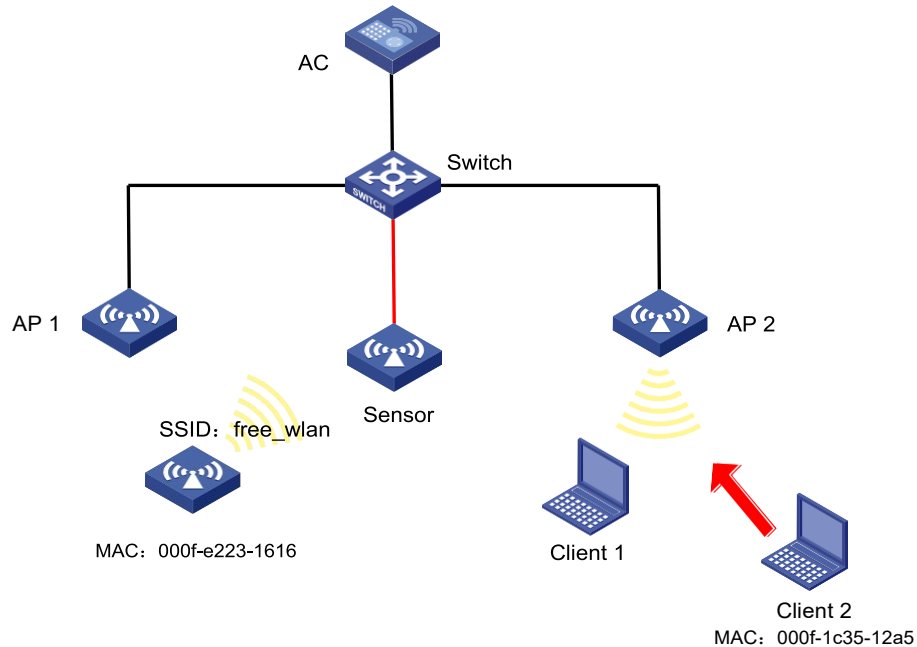
WIPS device classification and countermeasures configuration example

Network requirements

As shown in Figure 35, the sensor connects to the AC through the switch. AP 1 and AP 2 provide wireless services to clients through the SSID **abc**. Perform the following tasks:

- Enable WIPS for the sensor.
- Configure wireless device classification to add the MAC address **000f-1c35-12a5** to the static prohibited device list and the SSID **abc** to the trusted SSID list.
- Configure countermeasures to enable WIPS to take countermeasures against potential-external APs and unauthorized clients.

Figure 35 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Create a manual AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Perform the following tasks:
 - Add APs **ap1**, **ap2**, and **Sensor**.
 - Specify the AP models and serial IDs.
 - Bind a wireless service with SSID **abc** to APs **ap1** and **ap2**.
3. Configure WIPS:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Security > WIPS**.
 - b. Create VSD **VSD_1**.
 - c. Enable WIPS for AP **Sensor** and add the AP to VSD **VSD_1**.
 - d. Configure a classification policy:
 - Create the classification policy **class1**.
 - Add the MAC address of Client 2 to the prohibited device list.
 - Add the SSID **abc** to the trusted SSID list.
 - e. Configure a countermeasure policy:
 - Create the countermeasure policy **protect**.
 - Configure WIPS to take countermeasures against unauthorized clients and potential-external APs.
 - f. Modifying VSD **VSD_1**:
 - Apply the classification policy **class1** to the VSD **VSD_1**.
 - Apply the countermeasure policy **protect** to the VSD **VSD_1**.

Verifying the configuration

Verify that the AP with the MAC address **000f-e223-1616** is classified as a potential-external AP and the client with the MAC address **000f-1c35-12a5** is classified as an unauthorized client.

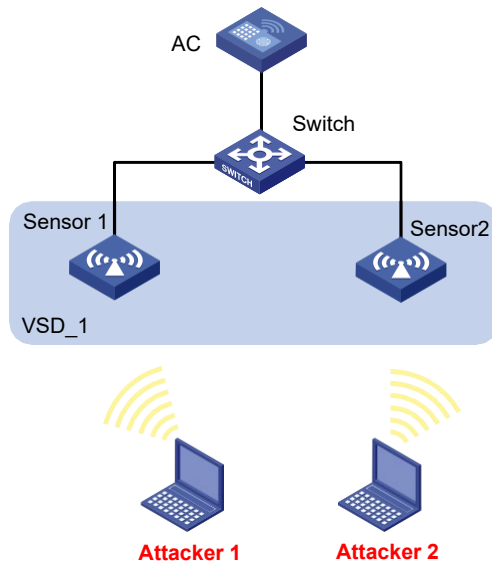
Verify that WIPS has taken countermeasures against the unauthorized client with the MAC address **000f-1c35-12a5** and the potential-external AP with the MAC address **000f-e223-1616**.

WIPS malformed packet and flood attack detection configuration example

Network requirements

As shown in [Figure 36](#), configure the two APs that connect to the AC through the switch as sensors. Add Sensor 1 and Sensor 2 to the VSD **VSD_1**. Configure malformed packet detection and flood attack detection to enable WIPS to trigger an alarm when it detects beacon flood attacks or malformed packets with duplicated IE.

Figure 36 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Create a manual AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Create two APs named **Sensor 1** and **Sensor 2**.
 - c. Specify the AP models and serial IDs.
3. Configure WIPS:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Security > WIPS**.
 - b. Create the VSD **VSD_1**.
 - c. Enable WIPS for the APs **Sensor 1** and **Sensor 2** and add the APs to the VSD **VSD_1**.
 - d. Add an attack detection policy:
 - Create an attack detection policy.
 - Enable detection on malformed packets with duplicated IE, and set the quiet time to 50 seconds.

- Enable beacon flood attack detection, and set the statistics interval, threshold, and quiet time to 100 seconds, 200, and 50 seconds, respectively.
- e. Modify VSD **VSD_1** to apply the attack detection policy to the VSD **VSD_1**.

Verifying the configuration

Verify that no malformed packets or flood attack messages exist when WIPS does not detect any attacks in the WLAN.

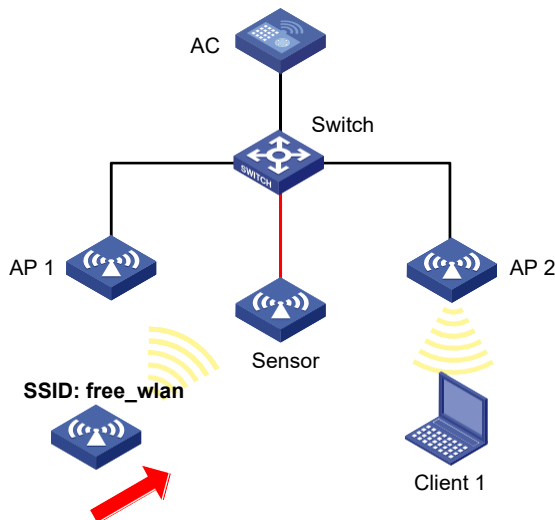
Verify that the number of malformed packets or flood attack messages is not zero when WIPS detects beacon flood attacks and malformed packets with duplicated IE.

Signature-based attack detection configuration example

Network requirements

As shown in [Figure 37](#), AP 1 and AP 2 provide wireless services for clients through the SSID **abc**. Enable WIPS for the sensor, and configure a signature to enable WIPS to trigger an alarm when it detects beacon frames whose SSIDs are not **abc**.

Figure 37 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Create a manual AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Access the page for adding an AP to perform the following tasks:
 - Add APs **AP1**, **AP2**, and **Sensor**.
 - Specify the AP models and serial IDs.
 - Bind a wireless service with SSID **abc** to APs **ap1** and **ap2**.
3. Configure WIPS:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Security > WIPS**.
 - b. Create VSD **VSD_1**.
 - c. Enable WIPS for the AP **Sensor** and add the AP to the VSD **VSD_1**.
 - d. Configure a signature rule:
 - Create signature 1.

- Configure a subsignature to match beacon frames.
- Configure a subsignature to match frames whose SSIDs are not **abc**.
- e. Configure a signature policy:
 - Create a signature policy named **sig1**.
 - Bind signature 1 to the signature policy **sig1**.
 - Set the detection interval, quiet time, and alarm threshold to 5 seconds, 60 seconds, and 60, respectively.
- f. Modify VSD **VSD_1** to apply the signature policy **sig1** to the VSD **VSD_1**.

Verifying the configuration

Verify that the AC receives an alarm from the sensor when the sensor detects the wireless service with the SSID **free_wlan**.

Verify that the number of detected messages for packets that match the signature is not zero.

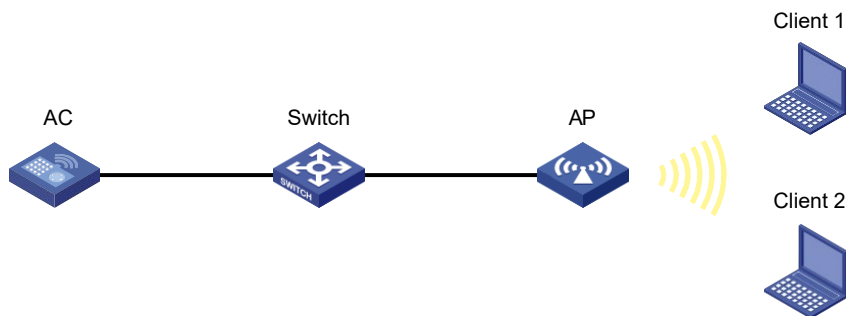
Client rate limiting configuration example

Network requirements

As shown in [Figure 38](#), the AC is in the same network as the AP. Perform the following tasks on the AC:

- Configure static mode client rate limiting to limit the rate of incoming client traffic.
- Configure dynamic mode client rate limiting to limit the rate of outgoing client traffic.

Figure 38 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **service**.
 - Enable the wireless service.
3. Configure the AP:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.

- Click the wireless service setting tab, and bind the wireless service **service** to radio 1 of AP 1.
4. Configure client rate limiting:
 - a. From the navigation pane, select **Wireless Configuration > Wireless QoS**. You are placed on the **Client Rate Limiting** tab.
 - b. Click the more icon in the service configuration area.
 - c. Select the service name **service**, and click the edit icon for the wireless service **service**.
 - d. On the edit page, perform the following tasks:
 - Set the limit mode to static mode for inbound traffic.
 - Set the per-client limit rate to **8000** for inbound traffic.
 - Set the limit mode to dynamic mode for outbound traffic.
 - Set the total limit rate to **8000** for outbound traffic.
 5. Enable radio 1 for AP 1:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.
 - b. Click the details icon in the all AP radio configuration area.
 - c. Select the combination of AP 1 and radio 1, and click the corresponding edit icon.
 - d. On the edit page, enable radio 1.

Verifying the configuration

Verify that the download rate and upload rate of each client do not exceed 8 Mbps and 4 Mbps, respectively.

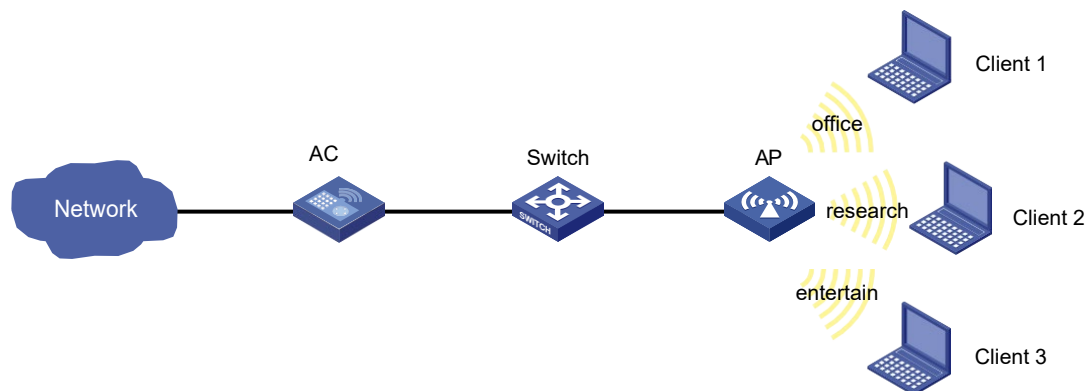
Bandwidth guaranteeing configuration example

Network requirements

As shown in [Figure 39](#), Clients 1, 2, and 3 access the network through the SSIDs **research**, **office**, and **entertain**, respectively.

For the network to operate correctly, guarantee 20% of the bandwidth for the SSID **office**, 80% for **research**, and none for **entertain**.

Figure 39 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.

- b. Add wireless services:
 - Create wireless services named **office**, **research**, and **entertain**.
 - Set their SSID to **office**, **research**, and **entertain**, respectively.
 - Enable the wireless services.
 3. Configure the AP:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless services **office**, **research**, and **entertain** to radio 1 of AP 1.
 4. Configure bandwidth guaranteeing:
 - a. From the navigation pane, select **Wireless Configuration > Wireless QoS**.
 - b. Click the **Bandwidth Guaranteeing** tab.
 - c. Click the more icon in the AP configuration area.
 - d. Select the combination of AP 1 and radio 1, and click the edit icon.
 - e. On the edit page, perform the following tasks:
 - Enable bandwidth guaranteeing.
 - Set the guaranteed bandwidth percentage to 20% for the wireless service **office**.
 - Set the guaranteed bandwidth percentage to 80% for the wireless service **research**.
 5. Enable radio 1 for AP 1:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.
 - b. Click the details icon in the all AP radio configuration area.
 - c. Select the combination of AP 1 and radio 1, and click the corresponding edit icon.
 - d. On the edit page, enable radio 1.

Verifying the configuration

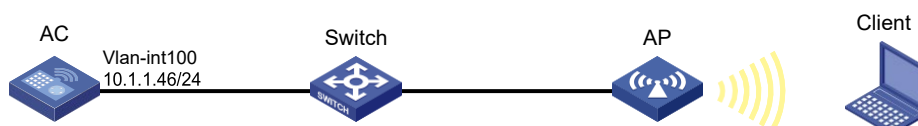
View details about AP configuration. Verify that clients accessing WLAN **office** and WLAN **research** can obtain a minimum of 20% and 80% of the total bandwidth, respectively. The system does not guarantee bandwidth for clients accessing WLAN **entertain**.

Shared key authentication configuration example

Network requirements

As shown in [Figure 40](#), the switch functions as a DHCP server to assign IP addresses to the AP and client. Configure shared key authentication to enable the client to access the network by using the WEP key **12345**.

Figure 40 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service1**.
 - Set the SSID to **service**.
 - Enable the wireless service.
3. Click **Apply and Set Advanced**, and then click the **Authentication** tab.
4. Configure static WEP authentication:
 - o Set the security type to static WEP.
 - o Set the key type to **Passphrase**.
 - o Select the WEP 40 cipher suite.
 - o Set the key to **12345**.
5. Apply the wireless service.
6. Bind the wireless service **service1** to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select **service1** and click **Bind to APs**.
 - c. Select the 5GHz radio of the AP and click **Quick Bind**.

Verifying the configuration

View details about the wireless service **service1** to verify that the configuration is correct.

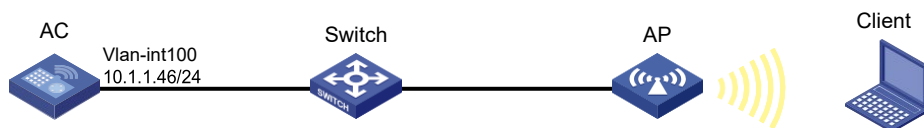
PSK authentication and bypass authentication configuration example

Network requirements

As shown in [Figure 41](#), the switch functions as a DHCP server to assign IP addresses to the AP and client.

- Configure open system authentication and bypass authentication.
- Configure the client to use the preshared key **12345678** to access the network.

Figure 41 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service1**.
 - Set the SSID to **service**.

- Enable the wireless service.
- 3. Click **Apply and Set Advanced**, and then click the **Authentication** tab.
- 4. Configure static PSK authentication:
 - Set the security type to static PSK.
 - Set the security mode to WPA.
 - Select the CCMP cipher suite.
 - Set the key type to **Passphrase** and the key to **12345678**.
- 5. Apply the wireless service.
- 6. Bind the wireless service **service1** to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select **service1** and click **Bind to APs**.
 - c. Select the 5GHz radio of the AP and click **Quick Bind**.

Verifying the configuration

View details about the wireless service **service1** to verify that the configuration is correct.

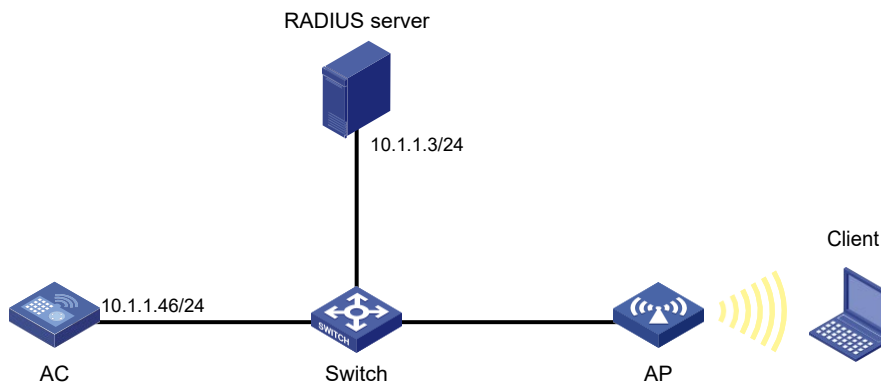
PSK authentication and MAC authentication configuration example

Network requirements

As shown in [Figure 42](#), the switch functions as a DHCP server to assign IP addresses to the AP and client.

- Configure open system authentication and MAC authentication for clients.
- Configure the client to use the preshared key **12345678** to access the network.

Figure 42 Network diagram



Configuration procedure

1. On the RADIUS server, configure the client's MAC address as the username and password used for authentication. The MAC address cannot contain hyphens and upper case letters.
2. Configure the RADIUS server correctly to provide authentication, authorization, and accounting functions.
3. Configure RADIUS and an authentication domain.
4. Click the network view tab at the bottom of the page.
5. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.

- b. Add a wireless service:
 - Create a wireless service named **service1**.
 - Set the SSID to **service**.
 - Enable the wireless service.
6. Click **Apply and Set Advanced**, and then click the **Authentication** tab.
7. Configure static PSK authentication and MAC authentication:
 - o Set the security type to static PSK and select MAC authentication.
 - o Set the security mode to WPA.
 - o Select the CCMP cipher suite.
 - o Set the key type to **Passphrase** and the key to **12345678**.
 - o Set the domain name to **dom1**.
8. Apply the wireless service.
9. Bind the wireless service **service1** to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select **service1** and click **Bind to APs**.
 - c. Select the 5GHz radio of the AP and click **Quick Bind**.

Verifying the configuration

View details about the wireless service **service1** to verify that the configuration is correct.

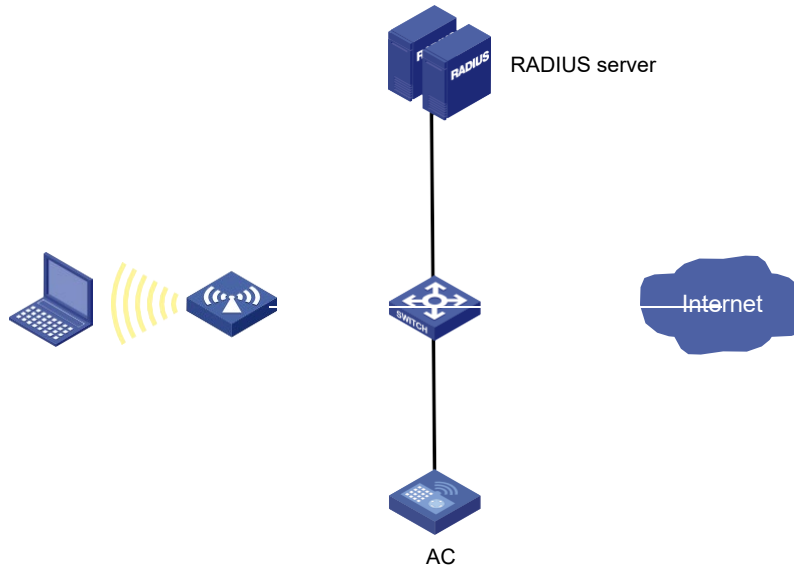
802.1 X RADIUS authentication configuration example

Network requirements

As shown in [Figure 43](#), configure the AC to meet the following requirements:

- Use the RADIUS server to perform authentication, authorization, and accounting for 802.1X users.
- Configure the AC to authenticate all 802.1X users in ISP domain **dm1X**.
- 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 AC and the RADIUS server.
- Use ports **1812** and **1813** for authentication and accounting, respectively.

Figure 43 Network diagram



Configuration procedure

1. Assign an IP address to each interface. (Details not shown.)
2. On the AC, click the system view tab at the bottom of the page.
3. Configure a RADIUS scheme on the AC:
 - a. From the navigation pane, select **Network Security > Authentication**.
 - b. Click the **RADIUS** tab.
 - c. Add and configure a RADIUS scheme:
 - Set the name of the RADIUS scheme to **802.1X**.
 - Configure the primary authentication server: set its IP address to **10.1.1.1**, set the port number to **1812**, set the shared key to **name**, and set the state to **Active**.
 - Configure the primary accounting server: set its IP address to **10.1.1.1**, set the port number to **1813**, set the shared key to **name**, and set the state to **Active**.
 - Set the format of usernames sent to the RADIUS server to **Excludes the domain name**.
4. Configure an ISP domain on the AC:
 - a. Click the **ISP domains** tab.
 - b. Add and configure an ISP domain:
 - Set the domain name to **dm1X**.
 - Set the ISP domain state to **Active**.
 - Set the service type to LAN access.
 - Set the method and scheme for authentication, authorization, and accounting to **RADIUS** and **802.1X**, respectively.
5. Configure 802.1X on the AC:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Click **Add**.
 - c. Specify the wireless service name and SSID.
 - d. Enable 802.1X authentication.
 - e. Set the domain to **dm1X**.

- f. Click **OK**.
6. Configure the RADIUS server:
 - o Add a user account on the server. (Details not shown.)
 - o Configure the authentication, authorization, and accounting settings. (Details not shown.)

Verifying the configuration

1. Access the **Network Security > Authentication > RADIUS** page to verify brief information of the RADIUS scheme **802.1X**.
2. Access the **Network Security > Authentication > ISP Domains** page to verify brief information of the ISP domain **dm1X**.
3. Verify that the user can use the configured username and password to come online.

802.1 X local authentication configuration example

Network requirements

As shown in Figure 44, add a user account with the username **dotuser** and password **12345** on the AC. Configure the AC to meet the following requirements:

- Perform local 802.1X authentication to control the network access of users.
- Authenticate the users in the ISP domain **abc**.

Figure 44 Network diagram



Configuration procedure

1. Assign an IP address to each interface, as shown in Figure 44. (Details not shown.)
2. Click the system view tab at the bottom of the page.
3. Configure a local user:
 - a. From the navigation pane, select **Network Security > User Management**. You are placed on the **Local Users** tab.
 - b. Add and configure a local user:
 - Set the username to **dotuser**.
 - Set the password to **12345**.
 - Set the service type to LAN access.
4. Configure an ISP domain:
 - a. From the navigation pane, select **Authentication**. You are placed on the **ISP Domains** tab.
 - b. Add and configure an ISP domain:
 - Set the ISP domain name to **abc**.
 - Set the ISP domain state to **Active**.
 - Set the service type to LAN access.
 - Configure the ISP domain to use local method for authentication and authorization of LAN users, and not perform accounting for LAN users.
5. Configure 802.1X:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Specify the wireless service name and SSID.

- c. Enable 802.1X authentication.
- d. Set the domain to **abc**.

Verifying the configuration

1. Access the **Network Security > User Management > Local Users** page to verify the configuration of the local user **dotuser**.
2. Access the **Network Security > Authentication > ISP Domains** page to verify brief information of the ISP domain **abc**.
3. Verify that the user can use the configured username and password to come online.

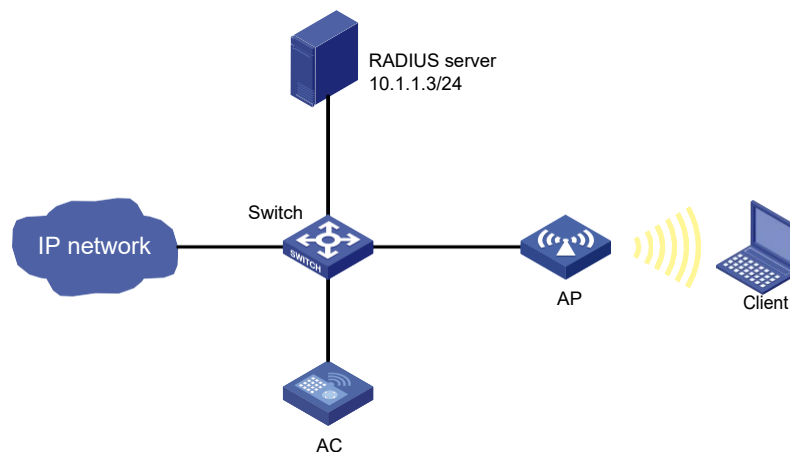
802.1 X AKM configuration example

Network requirements

As shown in [Figure 45](#), the switch functions as a DHCP server to assign IP addresses to the AP and client.

- Configure open system authentication and 802.1X authentication so that the client can access the network by using the login username **abcdef** and password **123456**.
- Configure 802.1X as the AKM mode.

Figure 45 Network diagram



Configuration procedure

1. Configure the username **abcdef** and the password **123456** on the RADIUS server and make sure the RADIUS server and AC can reach each other. (Details not shown.)
2. Configure RADIUS and an authentication domain.
3. Click the network view tab at the bottom of the page.
4. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service1**.
 - Set the SSID to **service**.
 - Enable the wireless service.
5. Click **Apply and Set Advanced**, and then click the **Authentication** tab.
6. Configure 802.1X authentication:
 - o Set the security type to 802.1X authentication.

- Set the security mode to WPA.
 - Select the CCMP cipher suite.
 - Set the domain name to **dom1**.
7. Apply the wireless service.
 8. Bind the wireless service **service1** to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select **service1** and click **Bind to APs**.
 - c. Select the 5GHz radio of the AP and click **Quick Bind**.

Verifying the configuration

View details about the wireless service **service1** to verify that the configuration is correct.

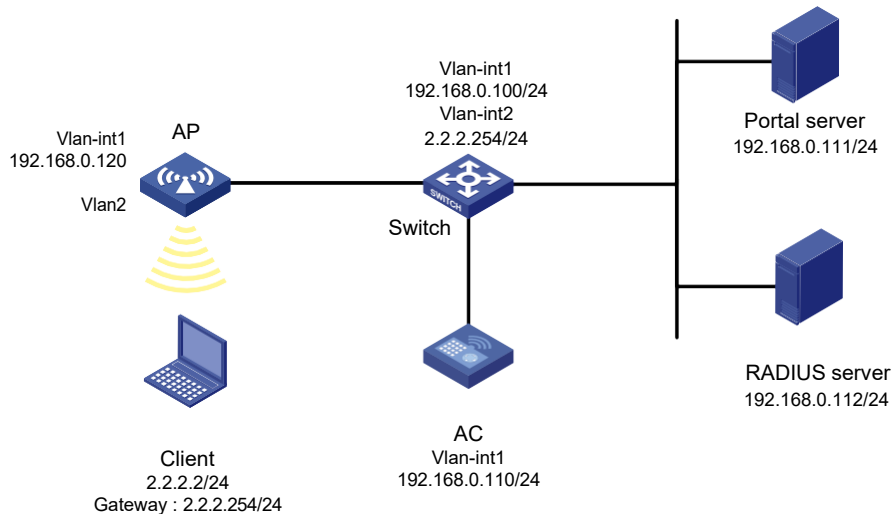
Direct IPv4 portal authentication configuration example

Network requirements

As shown in [Figure 46](#), the AP directly forwards user traffic from the client. The client is assigned with 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 client can access only the portal Web server before passing the authentication and access Internet resources after passing the authentication.

Figure 46 Network diagram



Configuration procedures

1. Configure IP addresses for the client, AC, and servers as shown in [Figure 46](#) and make sure they can reach each other.
2. Configure the RADIUS server correctly to provide authentication and accounting functions.
3. Configure the AP to make sure the AP can communicate with the AC.
4. Configure RADIUS and an authentication domain.
 - Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service1**.

- Set the SSID to **service**.
 - Enable the wireless service.
5. Configure the portal authentication mode:
 - a. Click the edit icon for wireless service **service1**.
The advanced settings page opens.
 - b. Click the **Authentication** tab.
 - c. Select **IPv4 Portal Authentication**.
 - d. Set the domain name to **dm1**.
 - e. Set the server URL to **newpt**.
 - f. Set the BAS-IP to **192.168.0.110**.
 - g. Click **Apply**.
 6. Bind the wireless **service1** to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select **service1** and click **Bind to APs**.
 - c. Select the 5GHz radio of the AP and click **Bind**.
The **Bind to AP window** opens.
 - d. Enter **2** in the **Bound VLAN** field.
 - e. Click **Apply**.

Verifying the configuration

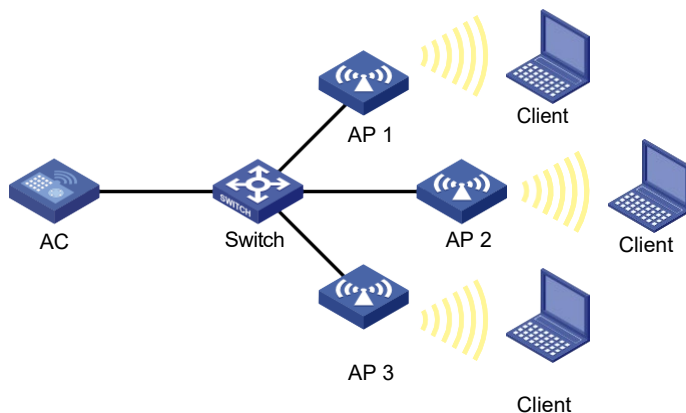
View details about the service **service1** to verify that the configuration is correct.

WLAN RRM DFS configuration example

Network requirements

As shown in [Figure 47](#), configure auto-DFS to adjust channels for the APs when a channel adjustment trigger condition is met.

Figure 47 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Specify a working channel for each AP:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.

- b. Access the details page for radio configuration and set the working channel to **Auto unlock** for AP 1, AP 2, and AP 3.
 3. Configure auto-DFS:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **RRM** tab.
 - c. Access the details page for AP configuration, and enable auto-DFS for AP 1, AP 2, and AP 3.

Verifying the configuration

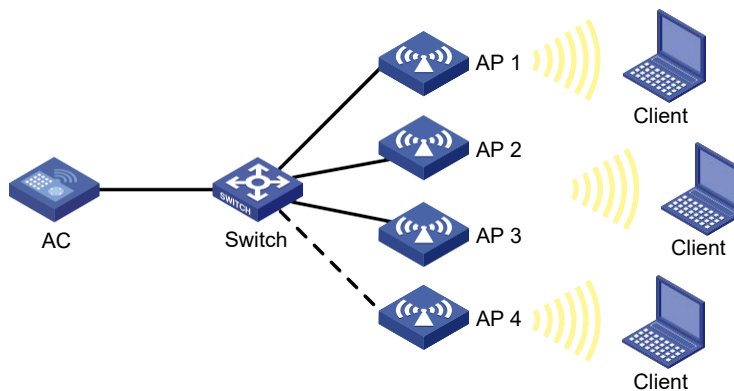
Access the **Monitoring > RF Monitoring > RRM** page. Verify that the working channels for the APs change when a channel adjustment trigger condition is met and the calibration interval is reached.

WLAN RRM TPC configuration example

Network requirements

As shown in [Figure 48](#), configure auto-TPC and set the neighbor number threshold as 3 to enable the AC to perform auto-TPC when AP 4 joins. Enable only radio 1 on each AP.

Figure 48 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Disable power lock for the APs:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.
 - b. Access the details page for radio configuration to disable power lock for AP 1, AP 2, AP 3, and AP 4.
3. Configure auto-TPC:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **RRM** tab.
 - c. Access the details page for AP configuration, and enable auto-TPC for AP 1, AP 2, AP 3, and AP 4.

Verifying the configuration

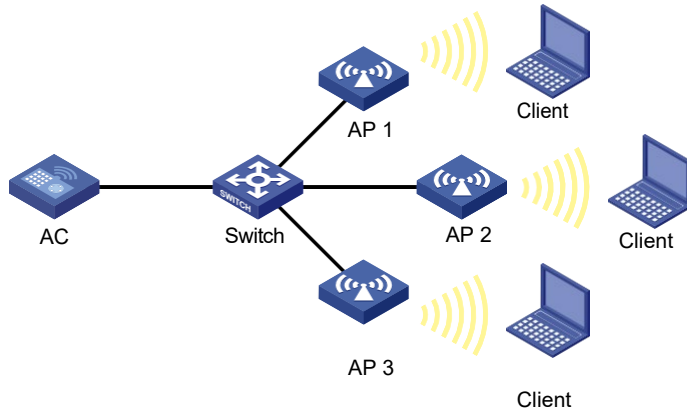
On the **Monitoring > RF Monitoring > RRM** page, verify that the power values for the APs change when the power adjustment threshold and the calibration interval are reached.

WLAN RRM bandwidth adjustment configuration example

Network requirements

As shown in [Figure 49](#), to ensure service quality for clients, configure the AC to adjust radio bandwidth automatically when the number of adjacent radios reaches the limit.

Figure 49 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. From the navigation pane, select **Wireless Configuration > Radio Management**. You are placed on the **Radio Configuration** tab.
3. Click the **RRM** tab.
4. Enable global bandwidth adjustment.
5. Click the more icon for fast adjustment, and set the adjustment interval to 10 minutes.

Verifying the configuration

On the **Wireless Configuration > Radio Management > RRM** page, click the more icon for AP RRM configuration.

Verify that radio bandwidth is adjusted when the number of adjacent radios reaches the threshold.

Session-mode load balancing configuration example

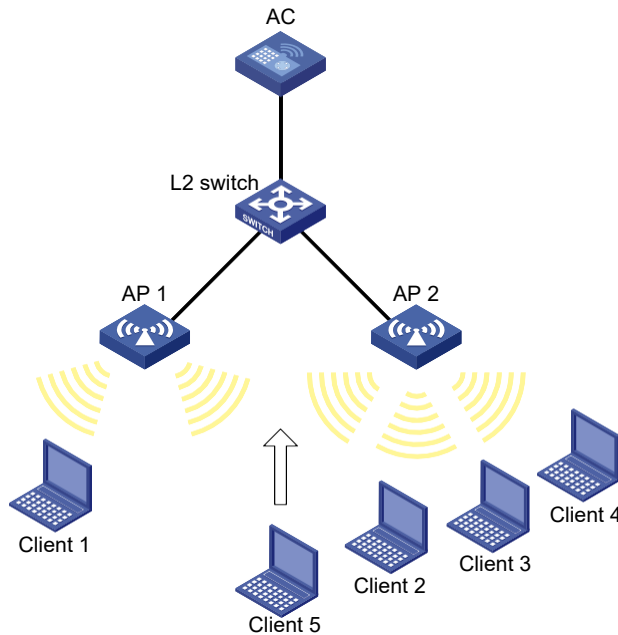
Network requirements

As shown in [Figure 50](#), AP 1 and AP 2 are managed by the AC and the clients can discover the APs.

Configure the AC to perform session-mode load balancing on AP 1 and AP 2 when the following conditions are met:

- The number of sessions on one AP reaches 3.
- The session gap between the APs reaches 2.

Figure 50 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **session-balance**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 in the same way AP 1 is added and configured.
4. Configure load balancing:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Session Mode**.
 - Set the session threshold to **3** and the session gap to **2**.

Verifying the configuration

- # Connect clients 2, 3, and 4 to radio 2 of AP 2, connect client 1 to radio 2 of AP 1, and then try to connect client 5 to AP 2.
- # Verify that AP 2 rejects client 5 and client 5 can access the WLAN only from AP 1.
- # On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Traffic-mode load balancing configuration example

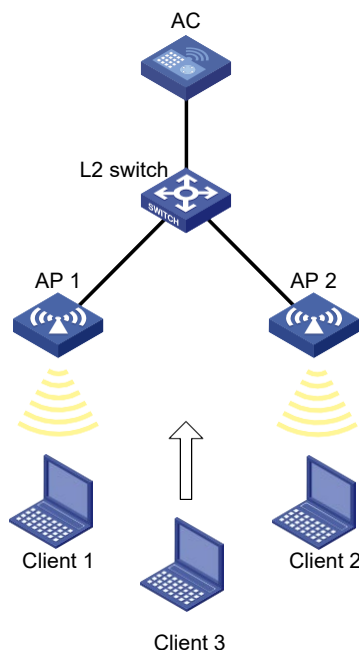
Network requirements

As shown in [Figure 51](#), AP 1 and AP 2 are managed by the AC and the clients can discover the APs. The maximum bandwidth for each AP is 250 Mbps. Configure 2.4 GHz radios on the APs to operate in 802.11gn mode.

Configure the AC to perform traffic-mode load balancing on AP 1 and AP 2 when the following conditions are met:

- The traffic on one AP reaches 50 Mbps (20% of the maximum bandwidth).
- The traffic gap between the APs reaches 25 Mbps (10% of the maximum bandwidth).

Figure 51 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **traffic-balance**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.

- b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 in the same way AP 1 is added and configured.
- 4. Configure load balancing:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Traffic Mode**.
 - Set the traffic threshold to **20** and the traffic gap to **10**.

Verifying the configuration

Verify that the AC performs session-mode load balancing for AP 1 and AP 2 when the following conditions are met:

- The traffic of radio 2 on AP 1 reaches 50 Mbps.
- The traffic gap between the APs reaches 25 Mbps.

On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Bandwidth-mode load balancing configuration example

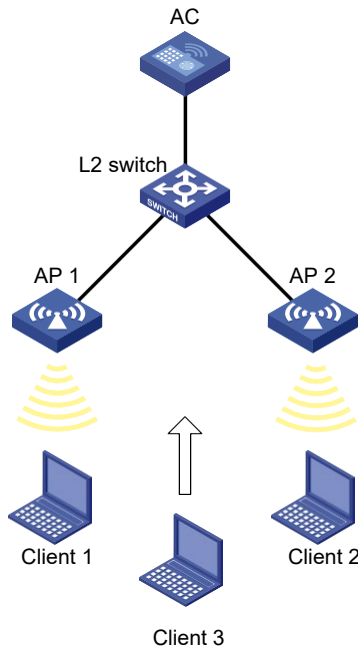
Network requirements

As shown in [Figure 52](#), AP 1 and AP 2 are managed by the AC and the clients can discover the APs.

Configure the AC to perform bandwidth-mode load balancing on AP 1 and AP 2 when the following conditions are met:

- The bandwidth of one AP reaches 12 Mbps.
- The bandwidth gap between the APs reaches 3 Mbps.

Figure 52 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **bandwidth-balance**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the SSID setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 in the same way AP 1 is added and configured.
4. Configure load balancing:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Bandwidth Mode**.
 - Set the bandwidth threshold to **12** and the bandwidth gap to **3**.

Verifying the configuration

Verify that the AC performs bandwidth-mode load balancing for AP 1 and AP 2 when the following conditions are met:

- The bandwidth of radio 2 on AP 1 reaches 12 Mbps.
- The bandwidth gap between the APs reaches 3 Mbps.

On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Session-mode load balancing configuration example for a load balancing group

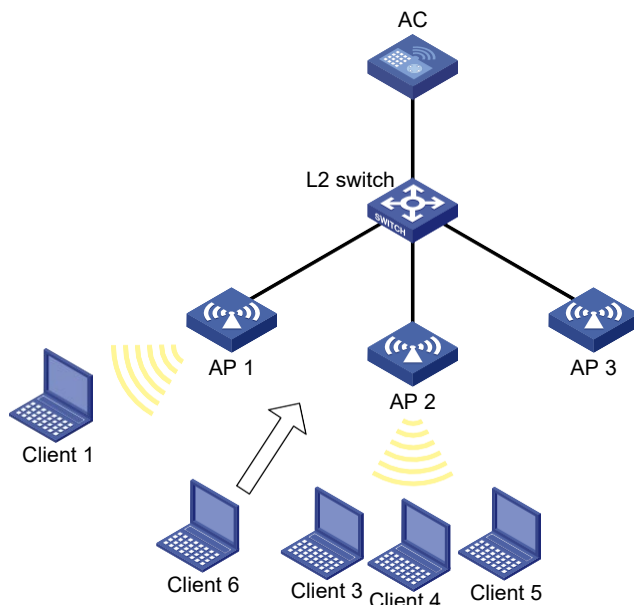
Network requirements

As shown in Figure 53, AP 1, AP 2, and AP 3 are managed by the AC and the clients can discover the APs.

Configure the AC to perform session-mode load balancing on radio 2 of AP 1 and radio 2 of AP 2 when the following conditions are met:

- The number of sessions on one radio reaches 3.
- The session gap between the radios reaches 2.

Figure 53 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **session-balance**.
 - Enable the wireless service.
3. Configure the APs:

- a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 and AP 3 in the same way AP 1 is added and configured.
4. Configure load balancing:
- a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Session Mode**.
 - Set the session threshold to **3** and the session gap to **2**.
 - d. Access the details page for load balancing group configuration to perform the following tasks:
 - Create a load balancing group.
 - Bind radio 2 of AP 1 and AP 2 to the load balancing group.

Verifying the configuration

- # Connect clients 3, 4, and 5 to radio 2 of AP 2, connect client 1 to radio 2 of AP 1, and then try to connect client 6 to AP 2.
- # Verify that AP 2 rejects client 6 and client 6 can access the WLAN only from AP 1.
- # On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Traffic-mode load balancing configuration example for a load balancing group

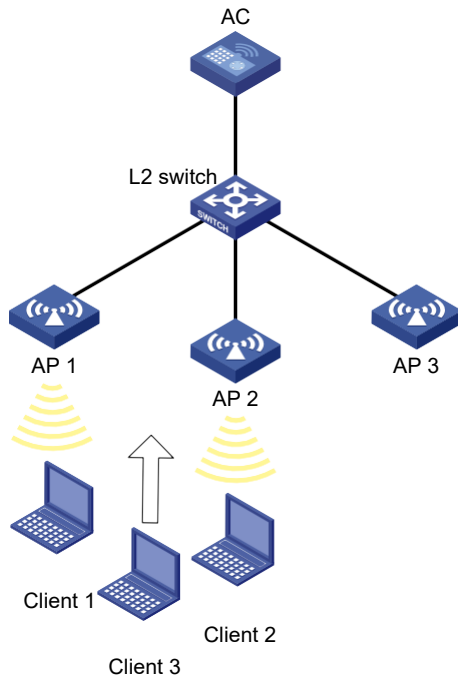
Network requirements

As shown in [Figure 54](#), AP 1, AP 2, and AP 3 are managed by the AC and the clients can discover the APs. The maximum bandwidth for each AP is 250 Mbps. Configure 2.4 GHz radios on the APs to operate in 802.11gn mode.

Configure the AC to perform traffic-mode load balancing on radio 2 of AP 1 and radio 2 of AP 2 when the following conditions are met:

- The traffic of one radio reaches 50 Mbps (20% of the maximum bandwidth).
- The traffic gap between the radios reaches 25 Mbps (10% of the maximum bandwidth).

Figure 54 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:
 - Create a wireless service named **service**.
 - Set the SSID to **traffic-balance**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 and AP 3 in the same way AP 1 is added and configured.
4. Configure load balancing:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Traffic Mode**.
 - Set the traffic threshold to **20** and the traffic gap to **10**.
 - d. Access the details page for load balancing group configuration to perform the following

tasks:

- Create a load balancing group.
- Bind radio 2 of AP 1 and AP 2 to the load balancing group.

Verifying the configuration

Verify that the AC performs traffic-mode load balancing for radio 2 of AP 1 and radio 2 of AP 2 when the following conditions are met:

- The traffic of radio 2 on AP 1 reaches 50 Mbps.
- The traffic gap between the radios reaches 25 Mbps.

On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Bandwidth-mode load balancing configuration example for a load balancing group

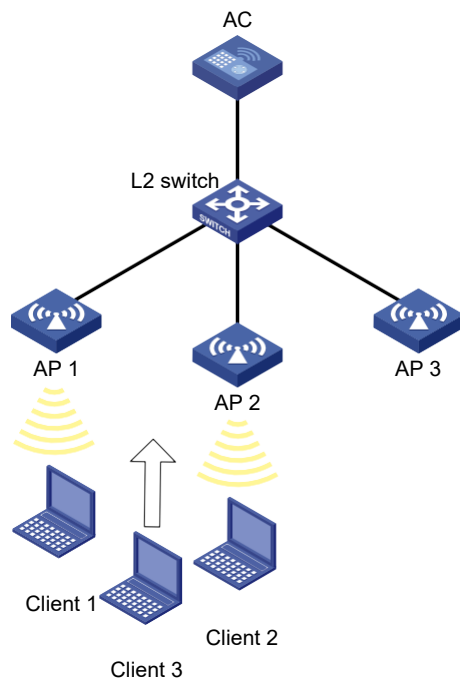
Network requirements

As shown in [Figure 55](#), AP 1, AP 2, and AP 3 are managed by the AC and the clients can discover the APs.

Configure the AC to perform bandwidth-mode load balancing on radio 2 of AP 1 and radio 2 of AP 2 when the following conditions are met:

- The bandwidth of one radio reaches 12 Mbps.
- The bandwidth gap between the radios reaches 3 Mbps.

Figure 55 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Add a wireless service:

- Create a wireless service named **service**.

- Set the SSID to **bandwidth-balance**.
 - Enable the wireless service.
3. Configure the APs:
 - a. From the navigation pane, select **AP Management**. You are placed on the **AP** tab.
 - b. Add and configure AP 1:
 - Set the AP name to **AP1**, configure the AP model and serial number, and then apply the configuration.
 - Click the edit icon in the operation column for AP 1.
 - Click the wireless service setting tab, and bind the wireless service **service** to radio 2 of AP 1.
 - c. Add and configure AP 2 and AP 3 in the same way AP 1 is added and configured.
 4. Configure load balancing:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Load Balancing** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable load balancing.
 - Select **Bandwidth Mode**.
 - Set the bandwidth threshold to **12** and the bandwidth gap to **3**.
 - d. Access the details page for load balancing group configuration to perform the following tasks:
 - Create a load balancing group.
 - Bind radio 2 of AP 1 and AP 2 to the load balancing group.

Verifying the configuration

Verify that the AC performs bandwidth-mode load balancing for radio 2 of AP 1 and radio 2 of AP 2 when the following conditions are met:

- The bandwidth of radio 2 of AP 1 reaches 12 Mbps.
- The bandwidth gap between the radios reaches 3 Mbps. (Details not shown.)

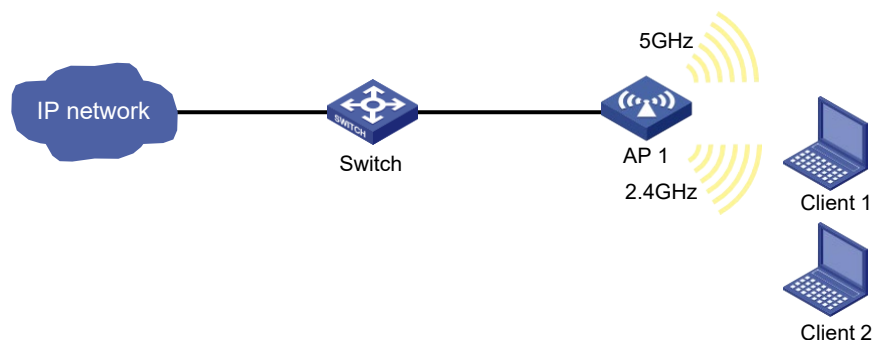
On the **Monitoring > Clients** page, verify that AP 1 and AP 2 are load balanced.

Band navigation configuration example

Network requirements

As shown in [Figure 56](#), both the 5 GHz radio and the 2.4 GHz radio are enabled on the AP. Configure band navigation for band navigation to load balance the radios.

Figure 56 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Access the page for adding a wireless network to perform the following tasks:
 - Set the name of the wireless service to **service**.
 - Set its SSID to **band-navigation**.
 - Disable fast association.
 - Enable the wireless service.
3. Configure AP 1:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**.
 - b. Click the **AP** tab.
 - c. Access the configuration page for AP 1 and click the wireless service setting tab.
 - d. Bind the wireless service **service** to both the 5 GHz and 2.4 GHz radios of AP 1.
4. Configure band navigation:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Click the **Band Navigation** tab.
 - c. Access the details page for global configuration to perform the following tasks:
 - Enable band navigation globally.
 - Set the session threshold to 5.
 - Set the session gap threshold to 2.
 - d. Access the band navigation configuration page for AP 1 to enable band navigation for AP 1.

Verifying the configuration

Verify that clients supporting both 2.4 GHz and 5 GHz prefer to access the 5 GHz radio. (Details not shown.)

Verify that the system rejects client access requests to the 5 GHz radio when the following conditions are met:

- The number of online clients on the 5 GHz radio reaches 5.
- The client quantity gap between the 5 GHz and 2.4 GHz radios reach 2. (Details not shown.)

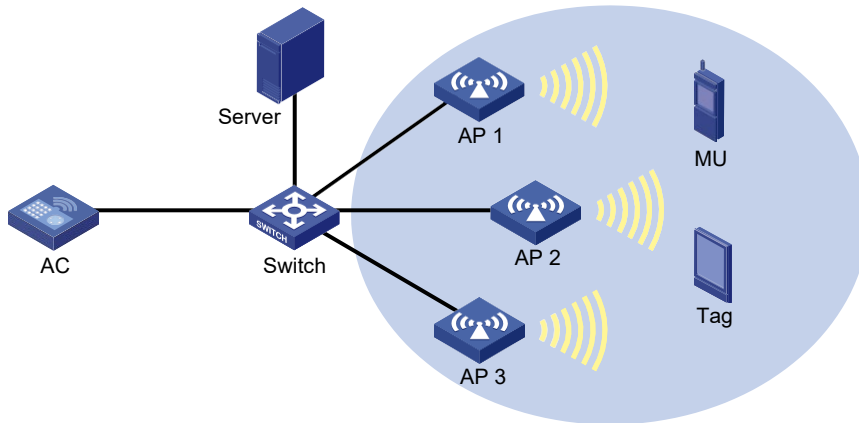
On the **Monitoring > Clients** page, verify that the 5 GHz radio and the 2.4 GHz radio of AP 1 are load balanced.

Wireless locating configuration example

Network requirements

As shown in [Figure 57](#), configure wireless locating on AP 1, AP 2, and AP 3 to locate the MU and the Tag.

Figure 57 Network diagram



Configuration procedure

1. Configure the locating server:
 - Set the IP addresses of the three APs on the locating server, or configure the locating server to discover APs through broadcast. (Details not shown.)
 - Configure wireless locating on the locating server. (Details not shown.)
2. Click the network view tab at the bottom of the page.
3. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Access the page for adding a wireless service to perform the following tasks:
 - Set the wireless service name to **market**.
 - Enable the wireless service.
4. Configure AP 1:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**. You are placed on the **AP** tab.
 - b. Access the page for adding an AP to perform the following tasks:
 - Set the AP name to **AP1**.
 - Select the AP model **WA4320i-ACN**.
 - Set the serial ID.
 - c. Click the edit icon in the operation column for AP 1 to perform the following tasks:
 - Click the wireless service setting tab.
 - Bind the wireless service **market** to radio 1 of the AP **AP1**.
 - d. From the navigation pane, select **Wireless Configuration > Applications**.
 - e. Click the **Location Aware** tab.
 - f. Access the details page for global configuration.
 - g. Click the **Aeroscout configuration** tab.
 - h. Enable Aeroscout locating.
 - i. Access the details page for AP configuration to perform the following tasks:
 - Access the edit page for the AP **AP1**. You are placed on the **Common** tab.
 - Enable ignoring beacon frames.
 - Click the **Aeroscout** tab.
 - Enable AeroScout locating.

- Enable radio 1.
 - Select both the MU and Tag.
5. Configure AP 2 and AP 3 in the same way AP 1 is configured.

Verifying the configuration

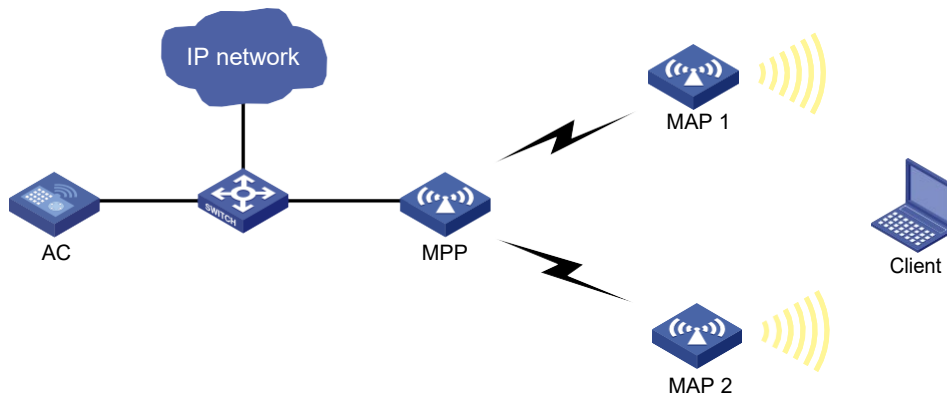
Verify that you can view the locating information about the MU and the Tag by using maps, forms, or reports provided by the graphics software. (Details not shown.)

WLAN mesh configuration example

Network requirements

As shown in [Figure 58](#), the MPP connects to the AC through a switch. Configure the MPP, MAP 1, and MAP 2 to use channel 149 and 5 GHz radios in 802.11n mode to establish mesh links for the client to access network resources.

Figure 58 Network diagram



Configuration procedure

1. Click the network view tab at the bottom of the page.
2. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Create a wireless service named **service**.
 - c. Set the SSID to **mesh-network**.
 - d. Enable the wireless service.
3. Configure APs:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**.
 - b. Create APs named **MPP**, **MAP1**, and **MAP2**.
 - c. Specify the AP models and serial IDs.
 - d. Bind wireless service **service** to radio 1 of each AP.
4. Configure a mesh profile:
 - a. From the navigation pane, select **Wireless Configuration > Applications**.
 - b. On the **Mesh Services** tab, click the **Add** icon + in the **Mesh Profile** area.
 - c. Set the profile number to 1.
 - d. Enable the mesh profile.
 - e. Set the mesh ID to 1.
 - f. Set the authentication and key management mode to **SAE** and specify the key to **12345678**.

- g. Retain the default settings for the other fields.
5. Bind the mesh profile to radios:
 - a. From the navigation pane, select **Wireless Configuration > Applications**.
 - b. On the **Mesh Services** tab, click the **More** icon in the **Binding Info** area.
 - c. Bind mesh profile 1 to MPP, MAP 1, and MAP 2.
6. Enable probe request suppression for the MPP:
 - a. From the navigation pane, select **Wireless Configuration > Applications**.
 - b. On the **Mesh Services** tab, click the **More** icon in the **Probe Request Suppression** area.
 - c. Disable probe request suppression for the MPP.
7. Configure the peer whitelist:
 - a. From the navigation pane, select **Wireless Configuration > Applications**.
 - b. On the **Mesh Services** tab, click the **More** icon in the **Mesh Peer Whitelist** area.
 - c. Add MPP to the whitelist of MAP 1 and MAP 2 for the MAPs to establish mesh links only with the MPP to avoid loops.
8. Configure the radio mode and channel:
 - a. From the navigation pane, select **Wireless Configuration > Radio Management**.
 - b. Configure the 5 GHz radio on each AP as follows in the **Radios for all APs** area:
 - Set the radio mode to 802.11n (5 GHz).
 - Set the channel to 149.
 - Enable the radio.

Verifying the configuration

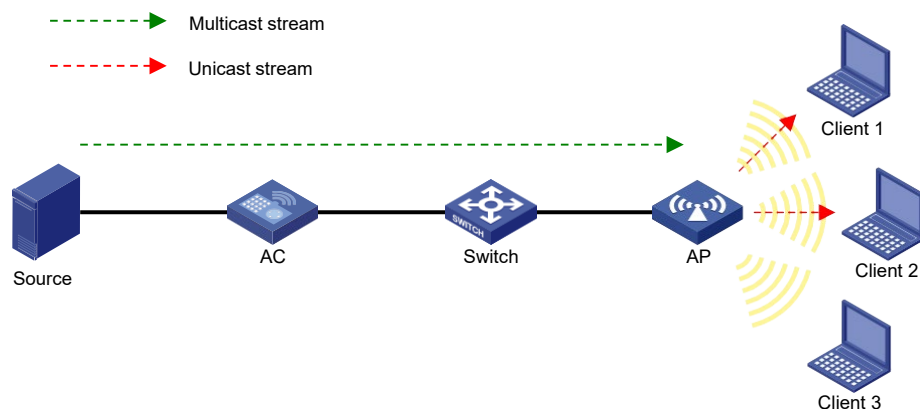
Verify that the client can access the network and you can view mesh link packet statistics from the Web interface.

Multicast optimization configuration example

Network requirements

As shown in [Figure 59](#), the source connected to the AC provides the IPv4 multicast service, and the AP provides wireless services to the clients through SSID **service**. Configure IPv4 multicast optimization to manage multicast packet forwarding.

Figure 59 Network diagram



Configuration procedure

1. Configure a wireless service:

- a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Create a wireless service named **service**.
 - c. Set the SSID to **service**.
 - d. Enable the wireless service.
2. Configure the AP:
 - a. From the navigation pane, select **Wireless Configuration > AP Management**.
 - b. Create APs named **AP1**.
 - c. Specify the AP model and serial ID.
 - d. Bind wireless service **service** to radio 1 of the AP.
3. Configure multicast optimization:
 - a. From the navigation pane, select **Wireless Configuration > Applications**.
 - b. Click the **More** icon for IPv4 multicast optimization.
 - c. Enable multicast optimization for wireless service **service**.
 - d. Click the **Advanced Configuration** tab and then perform the following tasks:
 - Set the entry aging time to 300 seconds.
 - Set the entry limit to 1024 and set the entry limit per client to 256.
 - Set the client limit per group to 2 and set the action to drop multicast packets.
 - Configure the device to learn a maximum of 100 IGMP packets every 60 seconds.

Verifying the configuration

- # Connect Client 1, Client 2, and Client 3 to the WLAN service with SSID **service**.
- # Send IGMP reports from Client 1 and Client 2 to join the IPv4 multicast group that the source uses to forward IPv4 multicast data. Both Client 1 and Client 2 can receive the IPv4 multicast data.
- # Send an IGMP report from Client 3 to join the IPv4 multicast group. None of the clients can receive the IPv4 multicast data.

Network security configuration examples

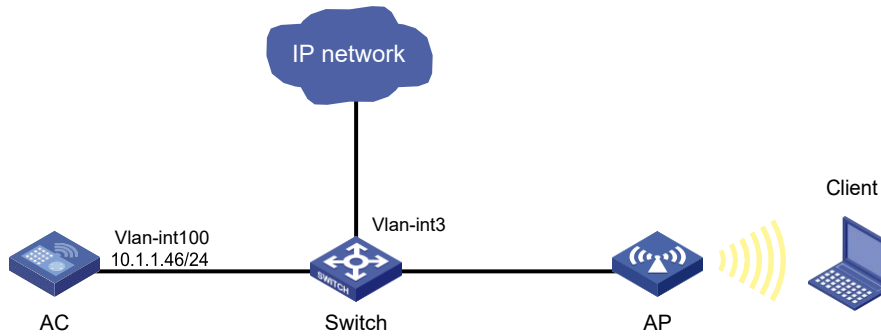
BYOD configuration example

Network requirements

As shown in [Figure 60](#), perform the following tasks for the AC to perform 802.1X authentication on the client:

- Set the username and password for 802.1X authentication to **dotuser** and **12345**, respectively.
- Set the authentication method to open system for the AC to perform local authentication and authorization for the client, and set the authentication domain name to **abc**.
- Allow the client that runs Microsoft Windows 8 to access VLAN 3 after passing the authentication.

Figure 60 Network diagram



Configuration procedure

1. Assign an IP address to each interface. (Details not shown.)
2. Click the network view tab at the bottom of the page.
3. Configure a wireless service:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Access the page for adding a wireless service to perform the following tasks:
 - Set the wireless service name to **service1**.
 - Set the SSID to **service**.
 - Enable the wireless service.
4. Configure 802.1X:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Access the advanced settings configuration page for the wireless service **service1** to perform the following tasks:
 - Set the security type to 802.1X authentication.
 - Set the security mode to WPA.
 - Select the CCMP cipher suite.
 - Set the domain name.
5. Bind the wireless service to the AP:
 - a. From the navigation pane, select **Wireless Configuration > Wireless Networks**.
 - b. Select the wireless service **service1**, and click the bind to APs button.
 - c. Select the 5 GHz radio of the AP, and then click the quick bind button.
6. Configure an ISP domain:
 - a. From the navigation pane, select **Network Security > Authentication**. You are placed on the **ISP Domains** tab.
 - b. Add an ISP domain, and then set its state to active.
 - c. Set the service type to **LAN Access**.
 - d. Set the authentication, authorization, and accounting methods to **Local**, **Local**, and **None**, respectively.
7. Configure a local user:
 - a. From the navigation pane, select **Network Security > User Management**. You are placed on the **Local Users** tab.
 - b. Click **User groups**.
 - c. Click the add icon.
 - d. Add a user group named **windows8**.

- e. Click **Apply**.
- f. On the **Local Users** tab, click **Users**.
- g. Click the add icon.
- h. Add a user named **dotuser**, and then set the password to **12345**.
- i. Set the service type to **LAN Access**.
- j. Specify the user group **windows8**.
- k. Click **Apply**.
8. Configure BYOD authorization:
 - a. From the navigation pane, select **Network Security > BYOD**.
 - b. Click the **BYOD Authorization** tab.
 - c. Set the terminal type to **Microsoft Windows 8**.
 - d. Set the ACL number to **2000**.
 - e. Set the authorization VLAN to **VLAN 3**.
 - f. Click **Apply**.
9. Configure BYOD rules:
 - a. From the navigation pane, select **Network Security > BYOD**. You are placed on the **BYOD Rules** tab.
 - b. Add a DHCP rule:
 - Set the DHCP Option 55 value to **1,15,3,6,44,46,47,31,33,121,249,252,43.33**.
 - Set the terminal type to **Microsoft Windows 8**.

Verifying the configuration

Verify that the client can access the resources in VLAN 3 after passing 802.1X authentication.

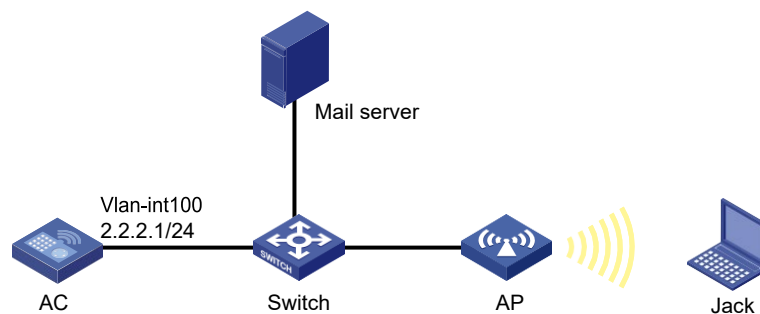
Guest management configuration example

Network requirements

Configure guest management on the AC as follows:

- Create a guest account **user1** for Jack, and set the password, user group, personal profiles, validity period, and receptionist information.
- Configure the SMTP server address, sender address, and guest administrator's email address that are used to send emails.
- Configure the subject and contents of the Emails to be sent to the guest, receptionist, and guest administrator.
- Configure the system to automatically delete expired guest accounts.

Figure 61 Network diagram



Configuration procedures

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure wireless services. (Details not shown.)
3. Add a guest account:
 - a. Click the network view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Security > Guest Management**.
 - c. On the **Guest List** tab, click the add icon.
 - d. On the **Add Guest** page, perform the following tasks:
 - Set the account and password to **user1** and **123456**, respectively.
 - Select a group for the guest.
 - Enter the full name, company, Email address, phone number, and description of the guest.
 - Enter the sponsor's full name, department, and Email address.
 - Set the validity period.
4. Configure the guest service parameters:
 - a. Click the network view tab at the bottom of the page.
 - b. From the navigation pane, select **Network Security > Guest Management**.
 - c. Click the **Guest Configuration** tab.
 - d. Select **Auto delete**.
 - e. Set the SMTP server address to **smtp://192.168.0.112/smtp**.
 - f. Set the email sender address to <mailto:bbb@ccc.com>.
 - g. Set the guest manager email address to <mailto:guest-manager@ccc.com>.
 - h. Set the subject of notifications to guests to **Guest account information**, and set the body to **A guest account has been created for your use. The username, password, and valid dates for the account are given below.**
 - i. Set the subject of notifications to guest managers to **Guest register information**, and set the body to **A guest account has been registered. The username for the account is given below. Please approve the register information.**
 - j. Set the subject of notifications to guest sponsors to **Guest account information**, and set the body to **A guest account has been created. The username, password, and valid dates for the account are given below.**

Verifying the configuration

- # Verify that guest Jack can access the network after passing local authentication by using username **user1** and password **123456**.
- # Verify that guests, guest managers, and guest sponsors can receive notifications with the specified subject and body upon guest creations.
- # Verify that the system can delete expired guest accounts automatically.

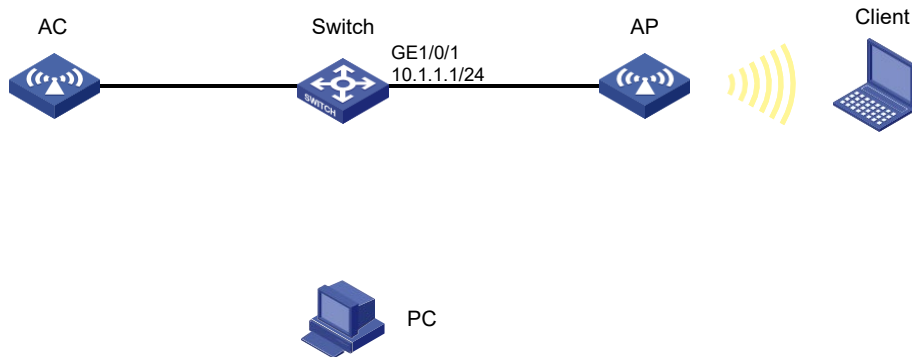
Tools configuration examples

Local packet capture configuration example

Network requirements

As shown in [Figure 62](#), enable local packet capture on radio 1 of the AP to capture 1 KB of TCP packets sourced from 192.168.20.173. The switch acts as the FTP server for storing the captured packets sent by the AP.

Figure 62 Network diagram



Restrictions and guidelines

Make sure the PC installed with the packet capture software and the AP can reach each other.

Configuration procedure

1. Configure the switch:
 - a. Create a device management user named **abc**.
 - b. Set the password for the user to **123456**.
 - c. Specify the user role for the user as **network-admin**.
 - d. Specify the working directory **flash:/** for the user.
 - e. Specify the service type for the user as **ftp**.
 - f. Enable the FTP server on the switch.
2. Configure local packet capture:
 - a. Click the network view tab at the bottom of the page.
 - b. From the navigation pane, select **Tools > Wireless Capture**.
 - c. Select radio 1 of the AP.
 - d. Configure wireless capture:
 - Select the local packet capture mode.
 - Specify the capture filter as **src 192.168.20.173 and tcp**.
 - Set the maximum frame size to **8000** bytes.
 - Set the file size to **1 KB**.
 - Set the FTP URL to **ftp://10.1.1.1**.
 - Set the FTP username to **abc**.
 - Set the FTP password to **123456**.

Verifying the configuration

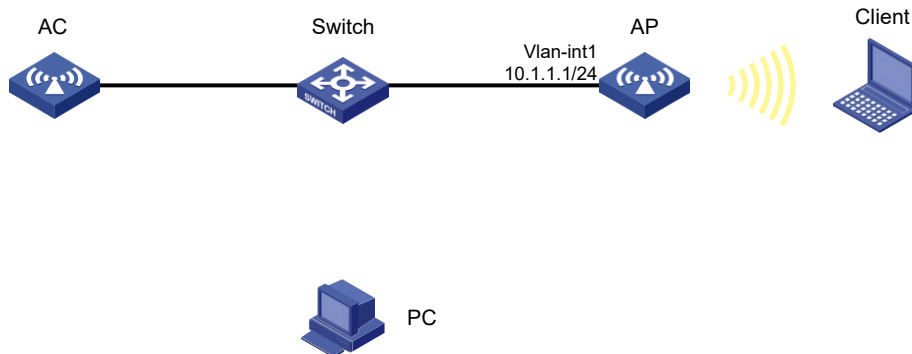
Verify that the captured packets can be displayed on the PC after the packet capture software is connected to the FTP server.

Remote packet capture configuration example

Network requirements

As shown in [Figure 63](#), enable remote packet capture on radio 1 of the AP and use packet capture software to display the captured packets.

Figure 63 Network diagram



Configuration procedure



IMPORTANT:

Make sure the packet capture software and the AP can reach each other.

1. Configure remote packet capture:
 - a. Click the network view tab at the bottom of the page.
 - b. From the navigation pane, select **Tools > Wireless Capture**.
 - c. Select radio 1 of the AP.
 - d. Select the remote packet capture mode.
 - e. Set the RPCAP port to **2014**.
2. Display captured packets on the PC:
 - a. Start packet capture software and select **Capture > Options**.
 - b. Select **Remote** from the **Interface** list.
 - c. Enter the IP address **10.1.1.1** and the port number **2014**, and click **OK**.
 - d. Click **Start**.

The captured packets are displayed on the page that appears.

Figure 64 Displaying the captured packets on the packet capture software

