



**ACU Access Controller Unit
V200R001C00**

Configuration Guide

Issue **01**
Date **2012-05-30**

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Email: support@huawei.com

About This Document

Intended Audience






This document provides the concepts, configuration procedures, and configuration examples supported by the SPU.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 01 (2012-05-30)

Initial commercial release.

Contents

About This Document.....	ii
1 WLAN Configuration.....	1
1.1 WLAN Overview.....	3
1.2 WLAN Features Supported by the SPU.....	6
1.3 Configuring Basic AC Attributes.....	8
1.4 Configuring Parameters for Communication Between the AC and APs.....	10
1.4.1 Establishing the Configuration Task.....	10
1.4.2 Adding an Offline AP and Configuring AP Attributes.....	11
1.4.3 Configuring AP Discovery.....	13
1.4.4 Configuring AP Discovery and Confirming the AP Identity.....	14
1.4.5 (Optional) Configuring an AC to Buffer AP Data.....	15
1.4.6 Checking the Configuration.....	15
1.5 Configuring the WLAN Radio Environment.....	16
1.5.1 Establishing the Configuration Task.....	16
1.5.2 Configuring a WMM Profile.....	17
1.5.3 Configuring a Radio Profile.....	18
1.5.4 Binding a Radio Profile to a Radio.....	20
1.5.5 (Optional) Configuring AP Radio Resource Management.....	21
1.5.6 (Optional) Configuring an AP Load Balancing Group.....	22
1.5.7 (Optional) Enabling the Traffic Scheduler.....	23
1.5.8 (Optional) Setting the Radio Working Mode.....	24
1.5.9 Checking the Configuration.....	24
1.6 Configuring the WLAN Service.....	25
1.6.1 Establishing the Configuration Task.....	25
1.6.2 Configuring a WLAN-ESS Interface.....	26
1.6.3 Configuring a Security Policy.....	28
1.6.4 Configuring a Traffic Profile.....	31
1.6.5 Configuring a WLAN Service Set.....	32
1.6.6 Configuring a VAP.....	34
1.6.7 Configuring a User Group.....	35
1.6.8 Configuring VLAN Mapping.....	36
1.6.9 Checking the Configuration.....	36
1.7 Managing APs.....	37

1.7.1 Configuring LLDP.....	37
1.7.2 Configuring Optical Module Alarm Thresholds on an AP.....	38
1.7.3 Configuring Dynamic Power Saving on an AP.....	39
1.7.4 Configuring Dual-Link Backup.....	40
1.7.5 Checking the Configuration.....	42
1.8 Maintaining the WLAN Service.....	42
1.8.1 Resetting an AP.....	42
1.8.2 Upgrading APs.....	43
1.8.3 Locating APs.....	44
1.8.4 Viewing Statistics.....	44
1.8.5 Deleting the Statistics.....	45
1.9 Configuration Examples.....	45
1.9.1 Example for Configuring the WLAN Service.....	45
1.9.2 Example for Configuring Dual-Link Backup on an AP.....	52
1.9.3 Example for Configuring Dual-Link Backup Globally.....	60
2 WLAN WDS Configuration.....	69
2.1 Introduction to WDS.....	70
2.2 WLAN WDS Features Supported by the SPU.....	72
2.3 Configuring the WDS Service.....	74
2.3.1 Configuring the Bridge Operation Mode.....	74
2.3.2 Configuring a Bridge Profile.....	75
2.3.3 Configuring a Bridge VAP.....	76
2.3.4 Checking the Configuration.....	77
2.4 Configuring the Bridge Whitelist.....	77
2.5 Configuring the AP Wired Interface.....	78
2.6 Configuring STP.....	79
2.7 Delivering Parameters to AP.....	80
2.8 Configuration Examples.....	80
2.8.1 Example for Configuring WLAN WDS.....	80
3 WLAN Security Configuration.....	88
3.1 WLAN Security Overview.....	89
3.2 WLAN Security Features Supported by the SPU.....	90
3.3 Configuring an Access Security Policy.....	91
3.4 Configuring the STA Blacklist and Whitelist.....	95
3.5 Configuring User Isolation.....	97
3.6 Configuration Examples.....	99
3.6.1 Example for Configuring Security Policies.....	99
4 WLAN QoS Configuration.....	108
4.1 WLAN QoS Overview.....	109
4.2 WLAN QoS Features Supported by the SPU.....	109
4.3 Configuring a Radio QoS Policy.....	111

4.4 Configuring a VAP QoS Policy.....	113
4.5 Configuring the User Priority and CAR.....	115
4.6 Configuring the User Priority and CAR in a QoS Profile.....	117
4.7 Configuration Examples.....	118
4.7.1 Example for Configuring a QoS Policy.....	118

1 WLAN Configuration

About This Chapter

This chapter describes how to configure the wireless local area network (WLAN) service in the AC + fit AP networking mode.

[1.1 WLAN Overview](#)

This section describes the concepts and application of WLAN.

[1.2 WLAN Features Supported by the SPU](#)

The SPU supports access controller (AC) management, access point (AP) management, Radio Frequency (RF) management, WLAN access security, and WLAN QoS management.

[1.3 Configuring Basic AC Attributes](#)

Before deploying WLAN services on an AC, configure basic attributes for the AC, including the AC ID, carrier ID, country code, and source interface.

[1.4 Configuring Parameters for Communication Between the AC and APs](#)

Before configuring WLAN services on an AC, ensure that the AC can communicate with APs. To enable an AP to go online, manually add the AP to the AC or configure the AC to discover APs and configure a whitelist. If the AP is in the whitelist, it can go online immediately after the AC discovers it. If the AP is not in the white list, confirm the AP identity and enable the AP to go online.

[1.5 Configuring the WLAN Radio Environment](#)

After an AP goes online, configure a radio profile for the AP. The SPU provides a maximum of four radios for APs. The radios are created by the system by default.

[1.6 Configuring the WLAN Service](#)

After an AP goes online, it provides different services for users based on parameters configured in the bound VAP.

[1.7 Managing APs](#)

This section describes how to configure LLDP, optical module alarm thresholds, dynamic power saving, and dual-link backup in the AC+Fit AP networking mode.

[1.8 Maintaining the WLAN Service](#)

This section describes how to reset, upgrade, and locate APs.

[1.9 Configuration Examples](#)

1.1 WLAN Overview

This section describes the concepts and application of WLAN.

Introduction to WLAN

A wireless local area network (WLAN) connects two or more computers or devices by using the wireless telecommunication technology to provide fast Ethernet access. It allows terminals, such as computers, to access a network through a wireless medium but not a physical cable. This facilitates network construction and allows users to move around without interrupting communication. Compared with a wired access network, a WLAN is easier to construct and requires lower maintenance cost. One or more access points (APs) can provide wireless access for a building or an area.

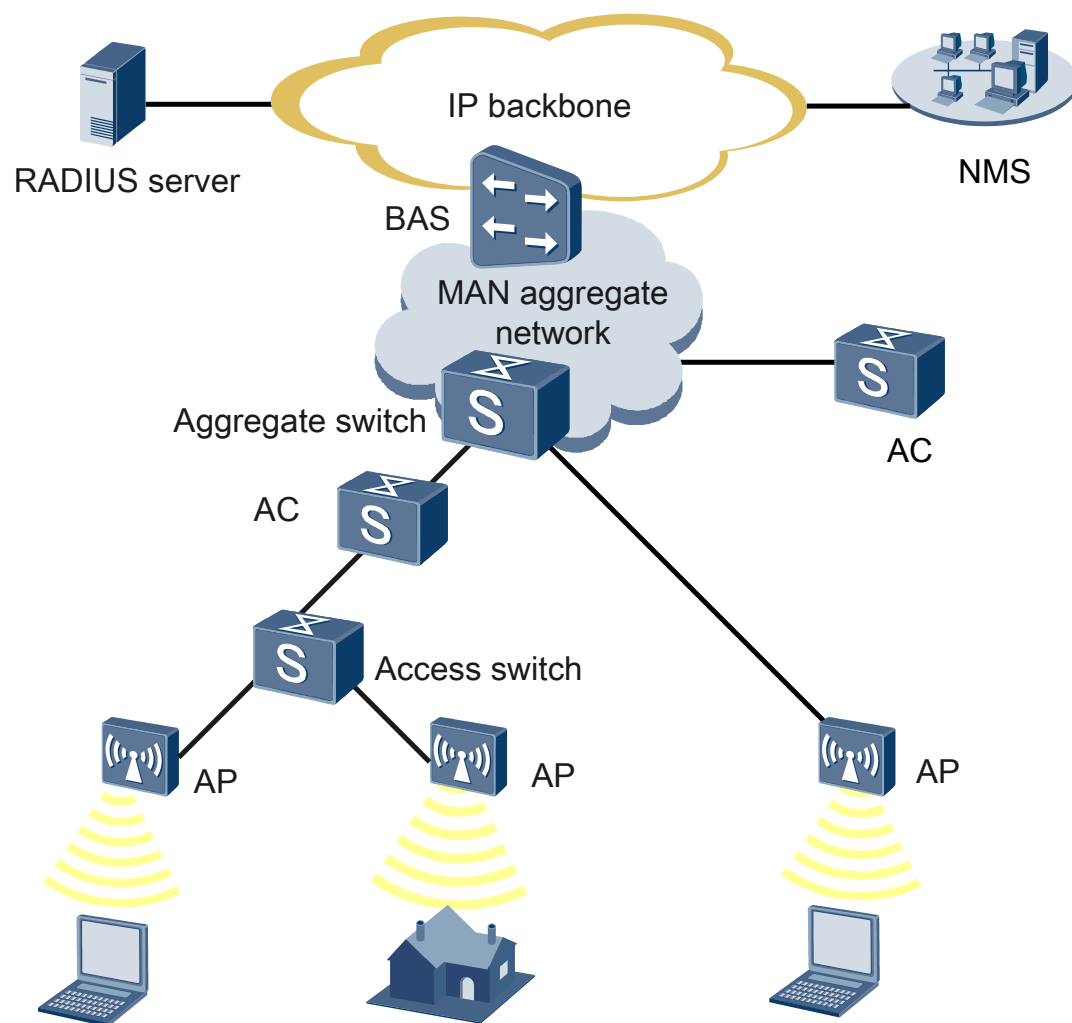
A WLAN uses wireless multiple access channels as the transmission media to provide LAN services. Data is transmitted by radio waves on the WLAN. WLANs are popular on campus and in business centers, airports, and other public areas.

WLAN Application

A WLAN system is not all wireless. The user access network is a wireless network, whereas servers and the backbone network are deployed on a wired network.

Figure 1-1 shows a WLAN with access controllers (ACs) and fit APs.

Figure 1-1 WLAN networking diagram



- AP
Encrypts and decrypts data on wireless channels.
An AP monitors wireless channels and converges wireless channel information to an AC. The AC manages wireless channels in a centralized manner.
- AC
Associates WLAN users with APs, controls wireless access, and guarantees access security.
An AC establishes management channels with APs to manage APs in a centralized manner. This reduces maintenance workload.
An SPU functions as an AC.
- BAS
Provides the authentication and accounting functions.
- NMS
Manages ACs.
- RADIUS Server
The RADIUS server performs authentication, authorization and accounting for access users.

Data traffic sent from wireless stations (STAs) to the Internet is transmitted over two types of media: wireless links between the wireless stations and APs and wired links between APs and ACs.

A wired link is established between an AP and an AC in the following process:

1. The AP starts and discovers the AC in unicast, multicast, or broadcast mode. In unicast mode, the AP discovers the AC by means of Dynamic Host Control Protocol (DHCP) discovery, Domain Name System (DNS) discovery, or static configuration.
 - DHCP discovery: The AP sends a DHCP request packet to apply for an IP address from the AC. The AC allocates an IP address to the AP by sending a DHCP reply packet carrying the Option 43 field that contains the AC's IP address. This allows the AP to discover the AC.
 - DNS discovery: The AP uses the DNS function to obtain the AC's IP address.
 - Static configuration: The AC's IP address is configured on the AP manually.
2. After the AP obtains the AC's IP address, it negotiates with the AC by sending a request message. After the AP receives a response message from the AC, it starts to establish a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel with the AC. The CAPWAP tunnel uses the Datagram Transport Layer Security (DTLS) protocol to encrypt and transmit User Datagram Protocol (UDP) packets.
3. After the CAPWAP tunnel is established, the AP sends a Join Request message to the AC. The AC determines whether to allow the AP to join the AC and sends a Join Response message to the AP.
4. The AP checks whether it is running the latest software version based on negotiation parameters. If the current version is not the latest version, the AP obtains the latest software version from the AC by using the CAPWAP tunnel. After the software version is updated, the AP restarts, discovers the AC, establishes a CAPWAP tunnel with the AC, and joins the AC again.
5. The AP sends a configuration status request message to the AC to notify the AC of the local configuration, including the antenna, radio, rate, channel, and power configurations. After receiving this message, the AC immediately sends a configuration status response message to the AP so that the AP can update the configuration.
6. After the configuration is updated, the AP sends a status change request message to the AC to notify the AC of the configuration update result. The AC then responds with a status change response message.
7. After the AP receives the status change response message, it enters the normal state and starts to function.

A wireless link is established between a STA and an AP in the following process:

1. Multiple APs on the WLAN periodically send Beacon frames. When a STA receives Beacon frames from multiple APs, it selects an AP as the access device.
2. The selected AP performs 802.11 authentication for the STA. After the STA is authenticated, it sends an association request to the AP. The AP forwards the association request to the AC. The AC determines whether to allow the STA to join itself. If the STA is allowed to join the AC, the AC sends a STA configuration request message to the AP.
3. The STA triggers 802.1x authentication by dialing. After the STA is authenticated by the AP, it is associated with the AP.

Terms

- STA
A STA is a computer with a wireless network adapter.
- AP
An AP is a bridge that connects STAs to a LAN and converts frames exchanged between STAs and the LAN.
- AC
An AC is a device that manages all APs in a WLAN. It can connect to an authentication server and allow WLAN users to be authenticated by the authentication server.
- SSID
A service set identifier (SSID) identifies a service set. A STA scans all wireless networks and selects a wireless network based on the SSID.
- Wireless medium
A wireless medium transmits frames between STAs. A WLAN system uses radios as transmission media.
- Service set
A service set is a combination of WLAN service parameters. You can configure multiple service sets and bind them to a radio of an AP to configure and deliver WLAN services quickly.
- VAP
A virtual access point (VAP) is a functional entity on an AP. You can create a VAP on a radio interface of an AP by binding a service set to the radio.

1.2 WLAN Features Supported by the SPU

The SPU supports access controller (AC) management, access point (AP) management, Radio Frequency (RF) management, WLAN access security, and WLAN QoS management.

AP Management

By default, an AP has no configuration after it is powered on. The SPU functions as an AC to deliver the WLAN configuration to APs.

When the SPU functions as an AC, it can set up connections with APs in the following modes:

- Adding APs offline: AP ID, AP attributes including the AP type, MAC address or serial number (SN), AP profile, and AP region are configured on the AC before APs go online. After an AP goes online, it uses the configured attributes.
- Discovering APs in the whitelist: The AP whitelist and AP authentication mode are configured on the AC. When an AP in the whitelist connects to the AC, the AC discovers the AP, and the AP functions properly.
- Discovering APs out of the whitelist: The AP whitelist and AP authentication mode are configured on the AC. When an AP out of the whitelist connects to the AC, the AC adds the AP to the list of unauthorized APs. After the AP identity is confirmed, the AP can function properly.

RF Management

On a WLAN, the network environment changes frequently, and mobile obstacles or interference from other radio frequencies (RFs) may affect transmission quality of radio signals.

The channels and transmit power of an AP must be adjusted to adapt to changes of the wireless network environment. Manual adjustment increases maintenance costs; therefore, RFs are managed by ACs in a WLAN system.

The SPU uses radio profiles to manage RFs.

WLAN Access Security

Channels of a WLAN are open to users, and malicious users can easily intercept, modify, and forward data of authorized users. The WLAN technology provides security policies to prevent access from unauthorized users. You can select security policies on a WLAN based on the security level.

The SPU uses security profiles to manage user access and supports four security policies: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and Wireless LAN Authentication and Privacy Infrastructure (WAPI).

WLAN QoS Management

The WLAN QoS feature provides services of different qualities for WLAN users.

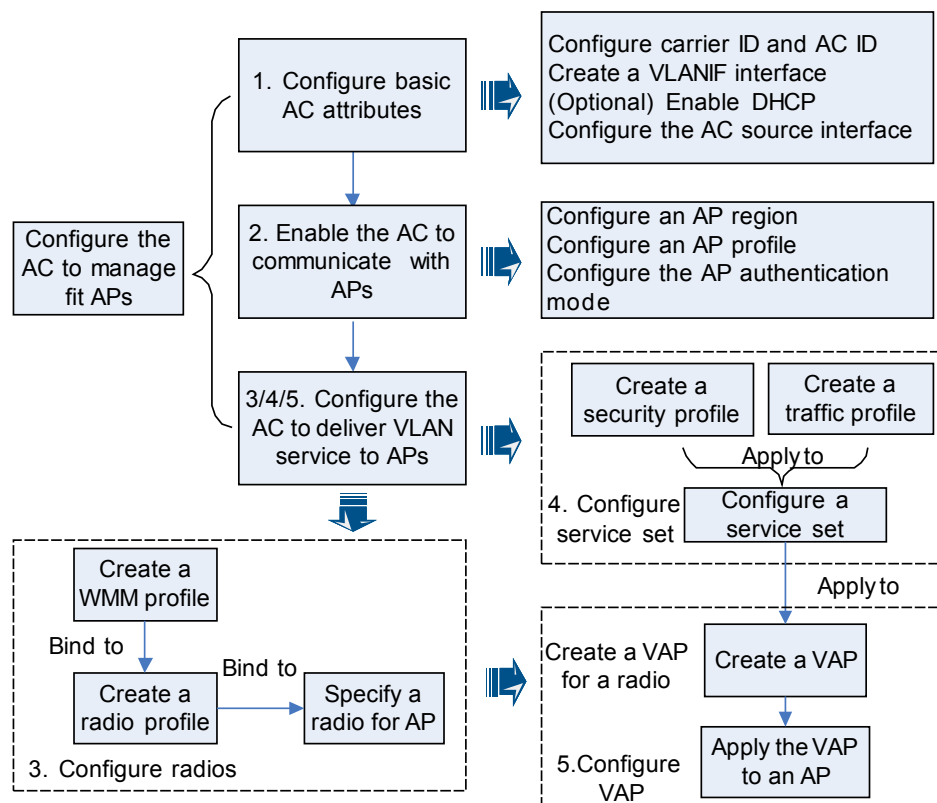
On the SPU, you can provide QoS of WLAN services by configuring Wi-Fi multimedia (WMM) profiles, QoS profiles, user priorities, and committed access rate (CAR).

WLAN Configuration Roadmap

As shown in [Figure 1-2](#), the WLAN configuration roadmap is as follows:

1. Configure basic AC attributes.
2. Configure parameters for communication between the AC and APs.
3. Configure radios for APs.
4. Configure service sets for APs.
5. Configure virtual APs (VAPs) and deliver VAP parameters to APs.

Figure 1-2 WLAN configuration roadmap



1.3 Configuring Basic AC Attributes

Before deploying WLAN services on an AC, configure basic attributes for the AC, including the AC ID, carrier ID, country code, and source interface.

Applicable Environment

An AC manages APs, controls WLAN user access, and guarantees security. APs can communicate with the AC only after the basic AC attributes are configured.

Data Preparation

To configure basic AC attributes, you need the following data.

No.	Data
1	AC ID, carrier ID, and country code
2	(Optional) VLANIF interface number and network segment in the address pool (when the AC functions as a DHCP server)
3	Source interface number

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan ac-global ac id ac-id [ carrier id { cmcc | ctc | cuc | other } ]
```

The AC ID and carrier ID are configured.

To facilitate AC management, configure an AC ID and a carrier ID on each AC.

By default, the AC ID is 0, and the carrier ID is **other**.

NOTE

If you configure a carrier ID in this step, skip [Step 3](#).

Step 3 Run:

```
wlan ac-global carrier id { cmcc | ctc | cuc | other } [ ac id ac-id ]
```

The AC ID and carrier ID are configured.

The supported carrier IDs are cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), and other.

Step 4 Run:

```
wlan ac-global country-code country-code
```

The country code is configured.

Step 5 (Optional) Configure the AC as a DHCP server to allocate IP addresses to APs.

1. Run:

```
dhcp enable
```

DHCP is enabled on the VLANIF interface.

2. Run:

```
interface vlanif vlan-id or interface loopback number
```

A VLANIF interface or loopback interface is created.

3. Run:

```
ip address
```

An IP address range is configured for APs.

4. Run:

```
quit
```

Return to the system view.

An AP can set up a connection with an AC only after obtaining an IP address from the AC, a broadband remote access server (BRAS), or a DHCP server. When the AC is configured as a DHCP server, it can allocate IP addresses to APs.

Step 6 Run:

```
wlan
```

The WLAN view is displayed.

Step 7 Run:

```
wlan ac source interface { LoopBack loopback-num | Vlanif vlanif-id }
```

The source interface of the AC is configured.

The AC uses the IP address of the specified source interface as the source IP address. All APs connected to the AC can learn this IP address.

---End

Result

Run the **display wlan ac-global** command. The AC configuration will be displayed.

1.4 Configuring Parameters for Communication Between the AC and APs

Before configuring WLAN services on an AC, ensure that the AC can communicate with APs. To enable an AP to go online, manually add the AP to the AC or configure the AC to discover APs and configure a whitelist. If the AP is in the whitelist, it can go online immediately after the AC discovers it. If the AP is not in the white list, confirm the AP identity and enable the AP to go online.

1.4.1 Establishing the Configuration Task

Before configuring parameters for communication between an AC and APs, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Before deploying WLAN services, ensure that APs can communicate with ACs. An AP can be connected to an AC directly or through a Layer 2 or Layer 3 network.

To enable an AP to go online, manually add the AP to the AC or configure the AC to discover APs and configure a whitelist. If the AP is in the whitelist, it can go online immediately after the AC discovers it. If the AP is not in the white list, confirm the AP identity and enable the AP to go online.

The difference between static AP configuration and automatic AP discovery is:

- When you add offline APs to the AC, you can modify the AP configurations. An AP uses the configured data to work after going online.
- When the AC is configured to automatically discover APs, an AP uses the default parameters to work after going online.

Pre-configuration Tasks

Before configuring parameters for communication between an AC and an AP, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)

- Connecting the AP to the AC correctly

Data Preparation

To configure parameters for communication between an AC and an AP, you need the following data.

No.	Data
1	(Optional) AP type name and AP type ID
2	AP upgrade file name and AP type ID matching the upgrade file
3	(Optional) FTP server's IP address, FTP user name, and password
4	AP ID, AP type ID or AP type name, AP's MAC address, and AP's serial number (SN)
5	(Optional) AP region ID
6	(Optional) AP profile name, AP profile ID, MTU, log server's IP address

1.4.2 Adding an Offline AP and Configuring AP Attributes

After you add an offline AP to an AC and configure AP attributes, the AP can go online and use the configured data to work.

Prerequisites

- Basic AC attributes have been configured according to [1.3 Configuring Basic AC Attributes](#).
- The AP is connected to the AC correctly.

Context

Before adding an AP to the AC, you can configure a radio and VAP for the AP. When the type and serial number (SN) or MAC address of an AP match those configured on the AC:

- If the AP is in the whitelist configured by using the **ap-whitelist** command, it starts to work and provides WLAN services immediately.
- If the AP is not in the whitelist, run the **ap-confirm** command to confirm the AP identity so that the AP can go online.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 (Optional) Run:

```
ap-license ap-license number
```

The number of AP licenses is set. An AP license controls the number of APs supported by an AC.

Step 4 (Optional) Run:

```
ap-type { id type-id | type ap-type } *
```

An AP type is added.

The system defines the following default AP types: WA601, WA631, WA651, WA602, WA632, WA652, WA603SN, WA603DN, WA653SN, WA633SN, WA603DE, WA653DE, AP6010SN-GN, WA615DN-AGN, AP6010DN-AGN, WA635SN-GN, AP6310SN-GN, WA655DN-AGN, AP6510DN-AGN, AP6610DN-AGN.

Step 5 Run:

```
ap-update mode { ftp-mode | ac-mode }
```

The AP upgrade mode is configured.

The system supports the AC mode and FTP mode. By default, the AC mode is used.

Step 6 Run:

```
ap-update update-filename filename ap-type type-id
```

The AP upgrade file is specified.

- If the AC mode is used, upload the upgrade file to the AC before specifying the AP upgrade file.
- If the FTP mode is used, run the **ap-update ftp-server server-ip-address [ftp-username ftpusername | ftp-password ftppassword] *** command to configure the FTP server's IP address, FTP user name, and password before specifying the AP upgrade file.

Step 7 Run:

```
ap-whitelist { mac ap-mac1 [ to ap-mac2 ] | sn ap-sn1 [ to ap-sn2 ] }
```

One or more AP MAC addresses or SNs are added to the whitelist.

Step 8 (Optional) Run:

```
ap-confirm { all | { mac ap-mac | sn ap-sn } [ id ap-id ] }
```

The AP identity is confirmed and the AP can go online.

After the AP identity is confirmed, the MAC address or SN of the AP is added to the whitelist.

Step 9 Run:

```
ap id ap-id [ { type-id type-id | ap-type ap-type } { mac ap-mac | sn ap-sn } * ]
```

An offline AP is added.

When adding an AP, specify the type and MAC address or SN for the AP.

Step 10 (Optional) Run:

```
region-id region-id
```

The AP is added to a region.

To create an AP region, run the **ap-region id** *region-id* command. If no AP region is created, the default AP region is used.

Step 11 (Optional) Run:

```
profile-id profile-id
```

The AP is bound to an AP profile.

To create an AP profile, run the **ap-profile** { **id** *profile-id* | **name** *profile-name* } * command. You can configure the MTU, log server's IP address, and backup mode for the AP profile.

If no AP profile is created, the default AP profile is used.

---End

Result

Run the **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* } command. The configuration of the newly added AP will be displayed.

1.4.3 Configuring AP Discovery

After you configure the AP whitelist and AP authentication mode on an AC, an AP can be discovered by the AC and go online if it is in the whitelist.

Prerequisites

- Basic AC attributes have been configured according to [1.3 Configuring Basic AC Attributes](#).
- The AP is connected to the AC correctly.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 (Optional) Run:

```
ap-type { id type-id | type ap-type } *
```

An AP type is added.

The system defines the following default AP types: WA601, WA631, WA651, WA602, WA632, WA652, WA603SN, WA603DN, WA653SN, WA633SN, WA603DE, WA653DE, AP6010SN-GN, WA615DN-AGN, AP6010DN-AGN, WA635SN-GN, AP6310SN-GN, WA655DN-AGN, AP6510DN-AGN, AP6610DN-AGN.

Step 4 Run:

```
ap-auth-mode auth-mode
```

The AP authentication mode is configured. The SPU supports MAC address authentication, SN authentication, and none authentication.

The default authentication mode is MAC address authentication.

Step 5 Run:

```
ap-whitelist { mac ap-mac1 [ to ap-mac2 ] | sn ap-sn1 [ to ap-sn2 ] }
```

One or more AP MAC addresses or SNs are added to the whitelist.

 **NOTE**

- If the AP authentication mode is set to **no-auth**, APs of the specified type can go online automatically. After an AP goes online, it is added to the default region and bound to the default AP profile, and its attributes are set to default values. The AP then enters the **normal** state.
- If the AP authentication mode is set to **sn-auth** or **mac-auth**, APs of the specified type can automatically go online if their MAC addresses or SNs are in the whitelist. After an AP goes online, it is added to the default region and bound to the default AP profile, and its attributes are set to default values. The AP then enters the **normal** state.

---End

Result

The MAC address or SN of the AP connected to the AC is in the whitelist, so the AP enters the **normal** state.

Run the **display ap { all | id ap-id | by-mac ap-mac | by-sn ap-sn }** command. The command output shows that the AP is in **normal** state.

1.4.4 Configuring AP Discovery and Confirming the AP Identity

After the AP authentication mode are configured on the AC, the AC adds an AP to the list of unauthorized APs if the AP is not in the whitelist. After you confirm the identity of the AP, the AP starts to work.

Prerequisites

- Basic AC attributes have been configured according to [1.3 Configuring Basic AC Attributes](#).
- The AP is connected to the AC correctly.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 (Optional) Run:

```
ap-type { id type-id | type ap-type } *
```

An AP type is added.

The system defines the following default AP types: WA601, WA631, WA603SN, WA603DN, WA633SN, WA603DE, WA653DE, WA653SN, AP6010SN-GN, AP6010DN-AGN, AP6310SN-GN, AP6510DN-AGN, AP6610DN-AGN.

Step 4 Run:

```
ap-auth-mode { mac-auth | no-auth | sn-auth }
```

The AP authentication mode is set to MAC address authentication or SN authentication.

The default authentication mode is MAC address authentication.

Step 5 Run:

```
ap-confirm { all | { mac ap-mac | sn ap-sn } [ id ap-id ] }
```

The AP identity is confirmed and the AP can go online.

After the AP identity is confirmed, the MAC address or SN of the AP is added to the whitelist. The AP is added to the default region and bound to the default AP profile, and its attributes are set to default values. The AP then enters the **normal** state.

----End

1.4.5 (Optional) Configuring an AC to Buffer AP Data

You can enable an AC to buffer AP data so that the NMS can obtain AP statistics from the AC.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 (Optional) Run:

```
ap-collect-time enable
```

An AC is enabled to buffer AP data.

By default, an AC is disabled from buffering AP data.

Step 4 Run:

```
ap collect-time timevalue
```

An AC is enabled to buffer AP data and the buffer duration is set.

By default, an AC buffers AP data every 15 minutes.

----End

1.4.6 Checking the Configuration

After configuring parameters for communication between an AP and an AC, you can use the following commands to verify the configuration.

Procedure

- Run the **display ap** { **all** | **id** *ap-id* | **by-mac** *ap-mac* | **by-sn** *ap-sn* } command to view AP information.
- Run the **display ap-auth-mode** command to view the AP authentication mode.
- Run the **display ap-profile** { **all** | **default** | **id** *profile-id* | **name** *profile-name* } command to view information about an AP profile.
- Run the **display ap-region** { **default** | **all** | **id** *region-id* } command to view information about an AP region.
- Run the **display ap-run-info id** *ap-id* command to view the AP running state.
- Run the **display ap-type** { **all** | **id** *type-id* | **type** *ap-type* } command to view information about an AP type.
- Run the **display ap-update mode** command to view the AP upgrade mode.
- Run the **display ap-update update-filename ap-type** *type-id* command to view the AP upgrade file name.
- Run the **display ap-update ftp-server** command to view information about the FTP server that stores the AP upgrade file.
- Run the **display ap-whitelist** { **mac** | **sn** } | [{ **begin** | **exclude** | **include** } *regular-expression*] command to view information about the AP whitelist.
- Run the **display wlan commit status** command to check whether the WLAN service configuration has been committed to an AP.

----End

1.5 Configuring the WLAN Radio Environment

After an AP goes online, configure a radio profile for the AP. The SPU provides a maximum of four radios for APs. The radios are created by the system by default.

1.5.1 Establishing the Configuration Task

Before configuring the WLAN radio environment, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This can help you complete the configuration task quickly and accurately.

Applicable Environment

A WLAN system uses radio frequencies as transmission media, and wireless devices compete for channels to transmit data. To guarantee quality of different wireless access services, create a Wi-Fi multimedia (WMM) profile and configure QoS parameters in the WMM profile. The WMM profile needs to be bound to a radio profile in which radio parameters are configured. The WMM profile is then applied to a radio together with the radio profile.

Pre-configuration Tasks

Before configuring the WLAN radio environment, complete the following tasks:

Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)

Data Preparation

To configure the WLAN radio environment, you need the following data.

No.	Data
1	WMM profile name and (optional) WMM profile ID
2	(Optional) WMM EDCA parameters for STAs: arbitration inter frame spacing number (AIFSN), minimum backoff time (ECWmin), maximum backoff time (ECWmax), and transmission opportunity limit (TXOPLimit)
3	(Optional) WMM EDCA parameters for APs: AIFSN, ECWmin, ECWmax, TXOPLimit, and ACK policy
4	Radio profile name and (optional) radio profile ID
5	AP ID, radio ID, name or ID of the radio profile bound to the radio
6	(Optional) Radio parameter calibration interval, ID of the AP whose parameters need to be calibrated, and calibration time
7	(Optional) Load balancing group name and ID, AP ID or radio ID, traffic threshold, session threshold, maximum number of association attempts

1.5.2 Configuring a WMM Profile

Different applications have different requirements on networks. The WMM profile provides access services with different quality to the applications.

Context

WMM provides QoS guarantee for wireless networks and enables high-priority packets to preempt the wireless channel first, providing better quality for voice and video services on WLANs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
wmm-profile { id profile-id | name profile-name } *
```

A WMM profile is created.

After a WMM profile is created, parameters in the profile use default values. To view the configuration of a WMM profile, run the **display wmm-profile { all | id profile-id | name profile-name }** command.

The following information shows the default configuration of the WMM profile **wp**.

```
[Quidway-wlan-view] display wmm-profile name wp
Profile ID       : 2
Profile name     : wp
WMM switch      : enable
Mandatory switch: disable
Client EDCA parameters:
-----
          ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO    3        2        2       47
AC_VI    4        3        2       94
AC_BE   10        4        3        0
AC_BK   10        4        7        0
-----
AP EDCA parameters:
-----
          ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO    3        2        1       47       normal
AC_VI    4        3        1       94       normal
AC_BE    6        4        3        0       normal
AC_BK   10        4        7        0       normal
-----
```

NOTE

A STA communicates with an AP by sending radio signals over a channel. Four queues are provided for radio packets. Packets in different queues have different opportunities to obtain transmission channels so that differentiated services can be provided for radio packets.

The queues are AC_VO (voice queue), AC_VI (video queue), AC_BE (best effort queue), and AC_BK (background queue) in descending order of priority.

You can change the priorities of the queues by modifying the Enhanced Distributed Channel Access (EDCA) parameters, including the AIFSN, ECWmin, ECWmax, TXOPLimit, and ACK policy:

- AIFSN: determines the channel idle time. A greater AIFSN value indicates a longer channel idle time. Different AIFSNs can be configured for ACs.
- ECWmin and ECWmax: ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They determine the average backoff time. A larger value indicates a longer average backoff time.
- TXOPLimit: determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. If this parameter is set to 0, a STA can send only one packet every time it occupies a channel.
- ACK policy: determines whether the packet receiver acknowledges received packets. Two policies are available: normal ACK and no ACK.

Before occupying a channel to send packets, STAs monitor the channel. If the channel idle time is longer than or equal to the AIFSN, each STA selects a random backoff time between ECWmin and ECWmax. The STA whose backoff timer expires the first occupies the channel and starts to send packets over the channel.

---End

1.5.3 Configuring a Radio Profile

You can configure the radio type, radio rate, radio power mode, and channel mode in a radio profile and bind a Wi-Fi multimedia (WMM) profile to the radio profile. A radio profile can be applied to a radio only after a WMM profile is bound to the radio profile.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

A radio profile is created.

After a radio profile is created, parameters in the profile use default values.

To view the configuration of a radio profile, run the **display radio-profile { all | id profile-id | name profile-name }** command.

```
[Quidway-wlan-radio-prof-radio-profile-1] display radio-profile name  
huawei
```

```
-----  
Profile ID                :1  
Profile name              :huawei  
Radio type                :802.11b/g  
Rate mode                 :auto  
Rate (Mbps)               :54  
Channel mode              :auto  
Power mode                :auto  
Calibrate interval (min)  :720  
PER threshold (%)         :30  
Conflict rate threshold (%) :60  
RTS/CTS threshold (Byte)  :2347  
Fragmentation threshold (Byte) :2346  
Short retry number limit  :7  
Long retry number limit   :4  
Support short preamble    :support  
DTIM interval (Beacon interval numbers) :3  
Beacon interval (ms)     :100  
WMM profile ID           :1  
WMM profile name         :huawei  
Interference detect switch :disable  
Calibrate switch         :enable  
Common frequency disturb threshold (%) :50  
Adjacent frequency disturb threshold (%) :50  
Station disturb threshold :32  
Radio device report duration (second) :60  
RTS/CTS mode             :CTS-TO-SELF  
Wifi-light mode          :traffic  
Beamforming Switch       :disable  
-----
```

Step 4 (Optional) Run:

```
radio-type { 80211a | 80211an | 80211gn | 80211b | 80211bg | 80211bgn | 80211g |  
80211n }
```

The radio type is configured.

When changing the radio type in a radio profile, ensure that all radios using the radio profile support the new radio type. Otherwise, the modification fails.

Step 5 (Optional) Run:

```
rate auto max-rate rate-value { rate_1 | rate_2 | rate_5_5 | rate_6 | rate_9 |  
rate_11 | rate_12 | rate_18 | rate_22 | rate_24 | rate_33 | rate_36 | rate_48 |  
rate_54 }
```

The radio rate is set.

Step 6 (Optional) Run:

```
power-mode { auto | fixed }
```

The radio power mode is set.

The default power mode is **auto**. In this mode, the power of radios using the radio profile is set automatically based on the WLAN radio environment.

Step 7 (Optional) Run:

```
channel-mode { auto | fixed }
```

The channel mode is set.

The default channel mode is **auto**. In this mode, channels are selected for radios using the radio profile automatically based on the WLAN radio environment.

Step 8 Run:

```
wmm-profile { id profile-id | name profile-name }
```

A WMM profile is bound to the radio profile.

 **NOTE**

A radio profile can be applied to a radio only after a WMM profile is bound to the radio profile.

Step 9 (Optional) Run:

```
wifi-light { signal-strength | traffic }
```

The meanings of Wi-Fi indicator on the AP are configured.

 **NOTE**

This command takes effect only when the AP is enabled with WDS. If the AP is not enabled with WDS, the Wi-Fi indicator always shows service traffic volume.

Step 10 (Optional) Run:

```
rts-cts-mode { cts-to-self | disable | rts-cts }
```

The RTS-CTS mode is set for the specified radio profile.

 **NOTE**

Enabling RTS-CTS reduces the transmission rate. To reduce the network delay, disable RTS-CTS.

----End

1.5.4 Binding a Radio Profile to a Radio

After a radio profile is bound to a radio, parameters defined in the radio profile are applied to the radio.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
ap ap-id radio radio-id
```

The radio view is displayed.

Step 4 Run:

```
radio-profile { id profile-id | name profile-name }
```

A radio profile is bound to the radio.

---End

1.5.5 (Optional) Configuring AP Radio Resource Management

An AP manages radio resources by selecting channels for radios, adjusting the radio transmission power, and calibrating radio parameters.

Context

A coverage hole is generated when an AP is removed or signals are blocked by an obstacle. An AC periodically checks for coverage holes. If the AC detects a coverage hole, it calibrates radios to eliminate the coverage hole.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

A radio profile is created.

After a radio profile is created, parameters in the profile use default values.

Step 4 Run:

```
channel-mode auto
```

The automatic channel mode is configured in the radio profile. In this mode, an AP can select a channel for a radio based on the WLAN radio environment.

An AC periodically triggers APs to check the network environment. The APs then determine whether to adjust channels and how to adjust channels based on the network environment.

Step 5 Run:

```
power-mode auto
```

The automatic power mode is configured in the radio profile. In this mode, an AP can set the transmit power for a radio based on the WLAN radio environment.

An AC periodically triggers APs to check the network environment. The APs then determine whether to adjust the transmit power so that the entire WLAN can be covered.



CAUTION

When the channel or antenna gain is manually changed or a radio calibration triggers change of the channel or power, an alarm may be generated, indicating that the transmit power exceeds the maximum value. If the gain of external antennas of an AP is too high, the transmit power of the AP may still exceed the value allowed by the local law even the AP software sets the transmit power to the minimum value.

Step 6 Run:

```
calibrate-interval calibrate-interval
```

Partial radio calibration is enabled and the calibration interval is set.

The calibration function ensures that the transmit power of a radio is not affected by interference from other radios. An AP checks the radio environment at the specified interval. If the radio environment deteriorates, the AP calibrates the radio parameters.

Step 7 Manually enable global radio calibration in an AP region.

- Run:

```
quit
```

Return to the WLAN view.

- Run:

```
calibrate startup region region-id [ listen-uncontrol-neighbor ]
```

Global radio calibration is enabled in an AP region.

- Run:

```
calibrate auto-startup region region-id time time [ listen-uncontrol-neighbor ]
```

Scheduled radio calibration is enabled in an AP region.

----End

1.5.6 (Optional) Configuring an AP Load Balancing Group

You can configure an AP load balancing group on an AC to implement load balancing between APs. The AC controls user access according to the policies configured in the load balancing group.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
load-balance-group { name group-name | id group-id } *
```

A load balancing group is created.

1. Run:

```
member ap-id ap-id radio-id radio-id
```

A radio is added to the load balancing group.

When a STA requests to associate with a radio, the AC compares traffic on this radio with traffic on other working radios to determine whether the STA can be associated with the radio.

2. (Optional) Run:

```
traffic gap gap-threshold
```

The load balancing mode is set to traffic mode.

If the difference between the traffic volume on one radio and that on another exceeds the value of *gap-threshold*, the AC considers that traffic is not balanced in the load balancing group. Subsequent STAs will be associated with radios with a lower traffic volume. The traffic of a radio refers to the sum of upstream traffic and downstream traffic.

By default, the session mode is used for load balancing.

3. (Optional) Run:

```
session gap gap-threshold
```

The load balancing mode is set to session mode.

If the difference between the number of STAs on one radio and that on another exceeds the value of *gap-threshold*, the AC considers that traffic is not balanced in the load balancing group. Subsequent STAs will be associated with radios used by fewer STAs.

4. Run:

```
associate-threshold associate-threshold
```

The threshold for the number of association requests is set.

If the number of times a STA requests to associate with a radio exceeds the threshold, the STA is allowed to associate with the radio regardless of whether the traffic is balanced in the load balancing group.

---End

1.5.7 (Optional) Enabling the Traffic Scheduler

Prerequisites

The VAP has been configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
ap ap-id radio radio-id
```

The radio view is displayed.

Step 4 Run:

```
users-traffic-scheduler enable
```

The traffic scheduler is enabled for users on a radio.

----End

1.5.8 (Optional) Setting the Radio Working Mode

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
ap ap-id radio radio-id
```

The radio view is displayed.

Step 4 Run:

```
work-mode {hybrid | monitor | normal}
```

The radio working mode is set.

Step 5 Run:

```
quit
```

Return to the WLAN view.

Step 6 Run:

```
commit ap ap-id
```

The radio working mode is delivered to the specified AP.

----End

1.5.9 Checking the Configuration

After configuring the WLAN radio environment, use the following commands to verify the configuration.

Procedure

- Run the **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to view information about a WMM profile.
- Run the **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to view information about a radio profile.
- Run the **display binding radio-profile** { **id** *profile-id* | **name** *profile-name* } command to view information about the radios bound to a radio profile.
- Run the **display load-balance-group** { **all** | **id** *group-id* | **name** *group-name* } command to view information about a load balancing group.
- Run the **display actual channel-power ap-id** *ap-id* **radio-id** *radio-id* command to view the channel and power of a radio.
- Run the **display calibrate auto-startup info region** *region-id* command to view the configuration of scheduled global calibration in an AP region.
- Run the **display radio config ap-id** *ap-id* **radio-id** *radio-id* command to view the configuration of a radio.

----End

1.6 Configuring the WLAN Service

After an AP goes online, it provides different services for users based on parameters configured in the bound VAP.

1.6.1 Establishing the Configuration Task

Before configuring the WLAN service, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This can help you complete the configuration task quickly and accurately.

Applicable Environment

If users need to access an Ethernet network by using wireless devices, the WLAN service must be configured. For the WLAN service configuration roadmap, see [1.2 WLAN Features Supported by the SPU](#).

Pre-configuration Tasks

Before configuring the WLAN service, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC
- Configuring the WLAN radio environment according to [1.5 Configuring the WLAN Radio Environment](#)

Data Preparation

To configure the WLAN service, you need the following data.

No.	Data
1	WLAN-ESS interface number, guest VLAN ID, restrict VLAN ID, and QoS CAR name
2	Security profile name or ID and security parameters required for the specified authentication mode: <ul style="list-style-type: none">● WEP shared key authentication: key value and key ID● WPA/WPA2 shared key authentication: key value● WAPI authentication: names of the AC certificate file, AC certificate issuer's certificate file, and authentication server unit (ASU) certificate, ASU IP address, and optional parameters, including: base key (BK) update interval or lifetime percentage, time-based interval or packet count-based interval for updating an MBMS service key (MSK), maximum number of retransmissions of MSK negotiation packets, and maximum number of retransmissions of certificate authentication packets
3	Traffic profile name or ID and optional parameters including the tunnel priority value, mappings from user priorities to 802.1p priorities, mapping from 802.1p priorities to user priorities, and packet rate limit
4	Service set name or ID, name or ID of the security profile bound to the service set, and name or ID of the traffic policy bound to the service set
5	AP ID, radio ID, name or ID of the service set bound to the radio, and (optional) WLAN index

1.6.2 Configuring a WLAN-ESS Interface

When an AP receives 802.11 radio packets, it converts the packets into 802.3 Ethernet packets and forwards them to an AC. The AC uses a WLAN-ESS interface to send the 802.3 Ethernet packets to the WLAN service module. The WLAN-ESS interface is configured with parameters such as the QoS profile, interface priority, and authentication mode.

Context

A WLAN-ESS interface is a virtual Layer 2 interface. Similar to a Layer 2 Ethernet interface of the hybrid type, a WLAN-ESS interface has Layer 2 attributes and supports multiple Layer 2 protocols.

After creating a WLAN-ESS interface, bind a service set to the interface.

Procedure

- Step 1** Run:
- ```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface wlan-ess wlan-ess-number
```

A WLAN-ESS interface is created.

**Step 3** Run:

```
port link-type hybrid
```

The link type of an interface .

**Step 4** Run:

```
port hybrid pvid vlan vlan-id
```

The default VLAN of a hybrid interface is specified.

By default, all ports are added to VLAN 1.

Indicates the default VLAN of user packets that an AC sends and receives. The PVID VLAN is manually configured by the administrator and valid only in CAPWAP tunnel forwarding mode.

**Step 5** Run:

```
port hybrid untagged vlan { { vlan-id1 [to vlan-id2] } <1-10> | all }
```

The port is added to VLANs in untagged mode.

By default, all ports are added to VLAN 1 in untagged mode.

**Step 6** Run:

```
{ dot1x-authentication | mac-authentication | web-authentication } enable
```

The authentication mode is configured on the WLAN-ESS interface.

 **NOTE**

- The **dot1x-authentication** keyword must be configured when WPA/WPA2-dot1x authentication is used.
- The **mac-authentication** keyword must be configured when WPA/WPA2-PSK authentication is used. In this authentication mode, MAC address authentication and WPA/WPA2-PSK authentication are performed in sequence for WLAN users.
- The **web-authentication** keyword must be configured when WEP authentication is used. In this authentication mode, WEP authentication is performed for WLAN users. After users are authenticated, they can access the Web server for service authentication.

**Step 7** Run:

```
dot1x authentication-method { chap | pap | eap }
```

The dot1x authentication method is configured.

By default, the Challenge Handshake Authentication Protocol (CHAP) authentication is used.

 **NOTE**

When the dot1x authentication method is set to **chap** or **pap**, no guest VLAN or restrict VLAN can be configured on the interface.

**Step 8** (Optional) Run:

```
dot1x guest-vlan vlan-id
```

A guest VLAN is configured on the WLAN-ESS interface.

To allow users on an interface to access certain network resources before dot1x authentication is performed, add the interface to a guest VLAN.

**Step 9** (Optional) Run:

```
dot1x restrict-vlan vlan-id
```

A restrict VLAN is configured on the WLAN-ESS interface.

To allow users on an interface to access certain network resources after they fail in dot1x authentication, add the interface to a restrict VLAN.

**Step 10** (Optional) Run:

```
qos car { inbound | outbound } car-name
```

A QoS CAR profile is applied to the WLAN-ESS interface.

**Step 11** (Optional) Run:

```
dot1x authentication domain domain-name
```

An AAA domain is bound to the WLAN-ESS interface.

**Step 12** (Optional) Run:

```
port-isolate enable
```

Port isolation is enabled.

**Step 13** (Optional) Run:

```
port priority
```

The default 802.1p priority that will be added to untagged packets on the WLAN-ESS interface is set.

**Step 14** (Optional) Run:

```
traffic-policy
```

A traffic policy is applied to the WLAN-ESS interface.

**Step 15** (Optional) Run:

```
trust
```

The priority to be mapped for packets is specified.

**Step 16** (Optional) Run:

```
trust upstream
```

A DiffServ domain is bound to the WLAN-ESS interface. The system then maps priorities of packets that pass through the interface to PHBs and colors according to the mappings in the DiffServ domain.

----End

### 1.6.3 Configuring a Security Policy

A security policy specifies the authentication mode for WLAN users.

#### Context

WLAN supports the following authentication modes: Wired Equivalent Privacy (WEP) authentication, Wi-Fi Protected Access (WPA) authentication, WPA2 authentication, and WLAN Authentication and Privacy Infrastructure (WAPI) authentication.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
security-profile { id profile-id | name profile-name } *
```

A security profile is created.

After a security profile is configured, its default settings are:

- Open system authentication and empty key if WEP is used
- 802.1x+PEAP authentication and TKIP encryption if WPA1 is used
- 802.1x+PEAP authentication and CCMP encryption if WPA2 is used
- WAI authentication and WPI encryption if WAPI is used

**Step 4** Configure security policies.

- WEP open system authentication

## 1. Run:

```
security-policy wep
```

The WEP security policy is configured.

## 2. Run:

```
wep authentication-method open-system [data-encrypt]
```

WEP open system authentication is configured.

- WEP shared key authentication

## 1. Run:

```
security-profile wep
```

The WEP security policy is configured.

## 2. Run:

```
wep authentication-method share-key
```

WEP shared key authentication is configured.

## 3. Run:

```
wep key { wep-40 | wep-104 } { pass-phrase | hex } key-id key-value
```

The WEP shared key is configured.


If WEP-40 is used, the WEP shared key is 10 hexadecimal characters or 5 ASCII characters. If WEP-104 is used, the WEP shared key is 26 hexadecimal characters or 13 ASCII characters.

## 4. Run:

```
wep default-key key-id
```

The WEP key ID is set.

A maximum of four WEP keys can be configured, but only one WEP key is used in authentication or encryption. This command specifies which key to use.

- WPA/WPA2 authentication
  1. Run:  
`security-policy wpa`  
The WPA security policy is configured.
  2. Run:  
`{ wpa | wpa2 } authentication-method dot1x { peap | tls } encryption-method { tkip | ccmp }`  
The dot1x authentication and corresponding encryption mode are configured for the WPA/WPA2 policy.  
 **NOTE**  
If WPA/WPA2 dot1x authentication is configured, run the **dot1x-authentication enable** command on a WLAN-ESS interface.
  3. Run:  
`{ wpa | wpa2 } authentication-method psk { pass-phrase | hex } key encryption-method { tkip | ccmp }`  
The shared key authentication and corresponding encryption mode are configured for the WPA/WPA2 policy.
- WAPI authentication
  1. Run:  
`security-policy wapi`  
The WAPI security policy is configured.
  2. Run:  
`wapi authentication-method { certificate | psk { pass-phrase | hex } key }`  
The authentication mode is set for the WAPI security policy.  
WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, the shared key must be configured.
  3. Run:  
`wapi import certificate { ac | asu | issuer } file-name file_name`  
The AC certificate file, certificate of the AC certificate issuer, and ASU certificate file are imported.
  4. Run:  
`wapi import private-key file-name file_name`  
The AC private key file is imported.
  5. Run:  
`wapi asu ip ip-address`  
The ASU server's IP address is configured.  
If WAPI certificate authentication is configured, an AC will send the certificate to the ASU server at the configured IP address.
  6. (Optional) Run the following commands to modify WAPI parameters:
    - Run:  
`wapi { bk-threshold bk-threshold | bk-update-interval bk-interval }`  
The interval for updating a base key (BK) and the BK lifetime percentage are set. By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.
    - Run:  
`wapi { msk-update-interval msk-interval | msk-update-packet msk-packet | msk-retrans-count msk-count }`

The interval for updating an MBMS service key (MSK), the number of packets that will trigger MSK update, and the number of retransmissions of MSK negotiation packets are set.

By default, the interval for updating an MSK is 86400s; the number of packets that will trigger MSK update is 10000; the number of retransmissions of MSK negotiation packets is 3.

- Run:

```
wapi cert-retrans-count cert-count
```

The number of retransmissions of certificate authentication packets is set.

By default, the number of retransmissions is 3.

- Run:

```
wapi { usk | msk } key-update { disable | time-based | packet-based |
timepacket-based }
```

The unicast session key (USK) or MSK update mode is set.

By default, USKs and MSKs are updated on the basis of time.

---End

## 1.6.4 Configuring a Traffic Profile

To apply the priority mapping and traffic suppression functions to a virtual access point (VAP), create a traffic profile and bind the traffic profile to a service set.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
traffic-profile { name profile-name | id profile-id } *
```

A traffic profile is created.

After a traffic profile is created, parameters in the profile use default values. To view the configuration of a traffic profile, run the **display traffic-profile { id profile-id | name profile-name }** command.

View attributes of the traffic profile **traffic-profile-1**.

```
[Quidway-wlan-view] display traffic-profile name traffic-
profile-1
Profile ID : 3
Profile name : traffic-profile-1
Client Limit Rate : 4294967295 Kbps (up)
 : 4294967295 Kbps (down)
VAP Limit Rate : 4294967295 Kbps (up)
 : 4294967295 Kbps (down)
802.1p Mapping Mode: mapping

User-priority 802.1p
0 0
```

```
1 1
2 2
3 3
4 4
5 5
6 6
7 7

802.1p to User-priority Mapping List:

802.1p User-priority
0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7

Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)

ToS(inner) ToS(outer)
0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7

Tunnel priority(down) Mapping Mode:ToS(inner) to ToS(outer)
```

** NOTE**

An AP converts the 802.11 packet sent from a STA into an 802.3 packet before sending it to an Ethernet network. The AP may retain the packet priority, change the packet priority according to the VAP configuration, or map the user priority to the 802.1p priority.

When receiving an 802.3 packet from the Ethernet network, the AP converts the 802.3 packet into an 802.11 packet and forwards it to the STA. The user priority in the packet is determined by DSCP-CoS mappings or set in a traffic classifier.

----End

## 1.6.5 Configuring a WLAN Service Set

A service set defines key service parameters. After creating a service set, bind a security profile and a traffic profile to the service set.

### Prerequisites

A security profile and a traffic profile have been created.

### Context

A service set defines key service parameters. After the service set is bound to a specified radio on an AP, the service parameters are applied to a WLAN service entity, namely, a virtual access point (VAP).

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
service-set { name service-set-name | id service-set-id } *
```

A service set is created.

**Step 4** Run:

```
ssid ssid
```

The SSID is specified the service set.

**Step 5** (Optional) Run:

```
ssid-hide
```

SSID hiding in a Beacon frame is enabled.

**Step 6** Run:

```
security-profile { name profile-name | id profile-id } *
```

A security profile is bound to the service set.

**Step 7** Run:

```
traffic-profile { name profile-name | id profile-id } *
```

A traffic profile is bound to the service set.

 **NOTE**

The security profile and traffic profile bound to a service set apply to all users using the service set.

**Step 8** Run:

```
wlan-ess wlan-ess-number
```

A WLAN-ESS interface is bound to the service set.

**Step 9** Run:

```
service-vlan
```

A VLAN is specified for the service set.

**Step 10** Run:

```
association-timeout association-timeout
```

The association aging time is set for STAs.

**Step 11** Run:

```
max-user-number max-user-number
```

The maximum number of access users is set for a service set.

**Step 12** (Optional) Run:



```
ip source guard enable
```

The IP source guard function is enabled for the AP.

By default, the IP source guard function is disabled.

**Step 13** (Optional) Run:

```
tunnel-forward protocol dot1x
```

EAP packets are forwarded over the tunnel.

By default, EAP packets are not forwarded over tunnels.

**Step 14** (Optional) Run:

```
dai enable
```

Dynamic ARP detection is enabled.

By default, dynamic ARP detection is disabled.

**Step 15** (Optional) Run:

```
arp-attack threshold threshold-value
```

The dynamic ARP detection threshold is set.

By default, the dynamic ARP detection threshold is 15.

**Step 16** (Optional) Run:

```
dhcp trust port
```

DHCP trusted port is configured on the AP.

By default, no DHCP trusted port is configured on the AP.

---End

## 1.6.6 Configuring a VAP

When a virtual access point (VAP) is delivered to an AP, the service set parameters in the VAP are delivered to the AP. The AP then provides services for users.

### Prerequisites

- A radio profile has been bound to the specified radio according to [1.5.4 Binding a Radio Profile to a Radio](#)
- A service set has been configured according to [1.6.5 Configuring a WLAN Service Set](#).

### Context

A VAP is a functional entity on an AP. You can create a VAP on a radio by binding a service set to the radio. To deliver a VAP to an AP, run the **commit { all | ap ap-id }** command.

#### NOTE

The WLAN service parameters configured on an AC take effect only after you run the **commit** command to deliver the VAP to an AP.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Create a single VAP.

1. Run:

```
ap ap-id radio radio-id
```

The radio view is displayed.

2. Run:

```
service-set { name service-set-name | id service-set-id } [wlan wlan-id]
```

A service set is bound to the radio.

3. Run:

```
quit
```

Return to the WLAN view.

4. Run:

```
commit { all | ap ap-id }
```

The VAP is delivered to an AP.

**Step 4** Create multiple VAPs at a time.

1. Run:

```
batch ap { ap-id [to ap-id] } &<0-1023> radio { radio-id [to radio-id] }
&<1-4> service-set { service-set-id [to service-set-id] } &<0-1023> [radio-
profile { id profile-id | name profile-name } *]
```

Multiple VAPs are created.

2. Run:

```
commit { all | ap ap-id }
```

The VAPs are delivered to APs.

----End

## 1.6.7 Configuring a User Group

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
user-group group-name
```

A user group is created and the user group interface view is displayed.

**Step 3** Run:

```
acl-id acl-id
```

An ACL is bound to the user group.

**Step 4** Run:

```
quit
```

Return to the system view.

**Step 5** Run:

```
aaa
```

The AAA view is displayed.

**Step 6** Run:

```
cut access-user user-group group-name
```

All online users in the user group are deleted.

----End

## 1.6.8 Configuring VLAN Mapping

This section describes how to configure VLAN mapping.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface eth-trunk trunk-id
```

An Eth-Trunk interface is created and the Eth-Trunk interface view is displayed.

**Step 3** Run:

```
port vlan-mapping VLAN vlan-id1 [to vlan-id2] inner-vlan vlan-id3 map-vlan vlan-id4 [to vlan-id5] delete-inner-vlan
```

VLAN mapping is configured on the Eth-Trunk interface.

 **NOTE**

The mapped VLAN ID must be different from the PVID on an interface.

----End

## 1.6.9 Checking the Configuration

After configuring the WLAN service, use the following commands to verify the configuration.

### Procedure

**Step 1** Run the `display vap { all [ type { service-set | bridge-profile } ] | ap ap-id [ radio radio-id | type { service-set | bridge-profile } ] | service-set { id service-set-id | name service-set-`

*name* } | **bridge-profile** { **id** *bridge-profile-id* | **name** *bridge-profile-name* } } command to view the VAP configuration.

**Step 2** Run the **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [ **detail** ] } command to view information about security profiles.

**Step 3** Run the **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to view information about traffic profiles.

**Step 4** Run the **display service-set** { **all** | **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* } command to view information about service sets.

**Step 5** Run the **display interface wlan-ess** [ *wlan-ess-number* ], to view the running status and configuration of a wlan-ess interface.

----End

## 1.7 Managing APs

This section describes how to configure LLDP, optical module alarm thresholds, dynamic power saving, and dual-link backup in the AC+Fit AP networking mode.

### 1.7.1 Configuring LLDP

The Link Layer Discovery Protocol (LLDP) is a Layer 2 discovery protocol defined in the IEEE 802.1ab standard. The LLDP protocol allows the NMS to rapidly obtain the Layer 2 network topology and topology changes when the network scale increases.

#### Context

As defined in LLDP, the local device organizes information such as device ID, interface number, system name, system description, interface description, device capability, and network management address into Type Length Values (TLVs), encapsulates these TLVs into a Link Layer Discovery Protocol Data Unit (LLDPDU), and sends the LLDPDU to neighbors. When receiving this LLDPDU, neighbors save the information carried in the LLDPDU to the Management Information Base (MIB) for an AC to query and determine the link status.

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
wlan ap lldp enable
```

LLDP is enabled globally.

By default, LLDP is disabled globally.

**Step 4** Run:

```
ap id ap-id
```

The AP view is displayed.

**Step 5** Run:

```
lldp enable
```

LLDP is enabled on the AP.

By default, LLDP is enabled on an AP.

**Step 6** Run:

```
lldp admin-status { rx | tx | txrx }
```

The AP is enabled to send or receive LLDP packets.

By default, an AP is enabled to send and receive LLDP packets.

**Step 7** (Optional) Run:

```
lldp tlv-enable basic-tlv { all | management-address | port-description | system-
capability | system-description | system-name }
```

The TLVs that an AP advertises in an LLDP packet are specified.

By default, an AP advertises all basic TLVs in an LLDP packet.

**Step 8** (Optional) Run:

```
lldp message-transmission { delay delay-time | hold-multiplier multiplier-id |
interval interval-time }
```

LLDP parameters are configured for the AP.

By default, LLDP parameter settings on an AP are as follows:

- **delay** *delay-time*: 2 seconds
- **hold-multiplier** *multiplier-id*: 4
- **interval** *interval-time*: 30 seconds

**Step 9** (Optional) Run:

```
lldp report-interval interval-time
```

The interval at which the AP reports LLDP neighbor information to an AC is configured.

By default, an AP reports LLDP neighbor information to an AC at an interval of 30 seconds.

**Step 10** (Optional) Run:

```
lldp restart-delay delay-time
```

The delay in re-enabling the LLDP function on the AP is configured.

The default delay is 2 seconds.

----End

## 1.7.2 Configuring Optical Module Alarm Thresholds on an AP

This section describes how to configure optical module alarm thresholds on an AP.

## Context

Optical module alarms include high/low receive power alarms, high/low temperature alarms, and corresponding clear alarms.

**NOTE**

Currently, only the WA653SN and AP6610DN-AGN can have optical modules installed.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
ap id ap-id
```

The AP view is displayed.

**Step 4** Run:

```
optical { high-rx-power | low-rx-power | high-temperature | low-temperature }
threshold value
```

Optical module alarm thresholds are configured on the AP.

By default, optical module alarm thresholds are as follows:

- high-rx-power: 100 uw
- low-rx-power: 2.5 uw
- high-temperature: 70°C
- low-temperature: -5°C

----End

## 1.7.3 Configuring Dynamic Power Saving on an AP

Dynamic power saving reduces power consumption on APs and therefore reduces operation and maintenance costs.

## Context

When dynamic power saving is enabled on an AP, the AP enters the power saving mode if no packet is transmitted on the AP. If packets need to be transmitted on the AP, the AP resumes working properly.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ap id ap-id
```

The AP view is displayed.

**Step 3** Run:

```
save-mode enable
```

Dynamic power saving is enabled on the AP.

By default, dynamic power saving is disabled on an AP.

----End

## 1.7.4 Configuring Dual-Link Backup

A maximum of 1024 APs can connect to an AC. If an AC becomes faulty, services of access users on all the APs connecting to the AC are interrupted. Dual-link backup can address this problem and ensure service stability.

### Context

APs must establish channels with two ACs to implement AC backup. The two ACs work in active/standby mode. The active AC provides services for APs, while the standby AC is a backup to the active AC. When an AP detects a fault on the link connected to the active AC, the AP instructs the standby AC to take the active role and sends data packets to the standby AC. This operation ensures service stability.



### CAUTION

When configuring dual-link backup, ensure that active and standby ACs deliver the same WLAN service configuration to an AP that connects to the two ACs. If different WLAN service configurations are delivered to the AP, the AP cannot work properly after an active/standby AC switchover.

---

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
wlan ac protect { enable | disable }
```

Dual-link backup is enabled globally.

By default, dual-link backup is disabled globally.

**Step 4** Run:

```
wlan ac protect { protect-ac | priority }
```

The AC priority or standby AC IP address is configured.

By default, no AC priority or standby AC IP address is configured.

 **NOTE**

If a parameter is configured in both the WLAN view and AP view, the parameter value configured in the AP view takes effect.

**Step 5** Run:

```
wlan ac protect restore { enable | disable }
```

Active/standby AC switchback is enabled globally.

By default, active/standby AC switchback is enabled globally.

 **NOTE**

If active/standby AC switchback is disabled globally, traffic of an AP cannot be switched back to the original active AC when the link between the original active AC and the AP restores.

**Step 6** Run:

```
ap id ap-id
```

The AP view is displayed.

**Step 7** Run:

```
protect-ac
```

The standby AC IP address is configured for the AP.

By default, no standby AC IP address is configured for an AP.

 **NOTE**

If a parameter is configured in both the WLAN view and AP view, the parameter value configured in the AP view takes effect.

**Step 8** Run:

```
priority
```

The AC priority is configured for the AP.

By default, no AC priority is configured for an AP.

 **NOTE**

- If a parameter is configured in both the WLAN view and AP view, the parameter value configured in the AP view takes effect.
- If priorities have been configured for the two ACs to which an AP connects, the AC with a higher priority becomes the active AC. If active/standby AC switchback has been enabled globally, the original active AC establishes a connection with the AP to become the active AC again after recovering from a failure.

----End



## 1.7.5 Checking the Configuration

### Prerequisites

Configurations of the LLDP function, AP optical module alarm thresholds, AP dynamic power saving, and dual-link backup are complete.

### Procedure

- Run the **display ap { all | id *ap-id* | by-mac *ap-mac* | by-sn *ap-sn* }** command to view AP configuration, including AC priority and standby AC IP address used in dual-link backup and whether AP dynamic power saving is enabled.
- Run the **display optical-info ap-id *ap-id*** command to view optical module information on a specified AP.
- Run the **display lldp ap-neighbor [ *ap-id* [ port *portnum* ] ]** command to view LLDP neighbor information on a specified AP.

---End

## 1.8 Maintaining the WLAN Service

This section describes how to reset, upgrade, and locate APs.

### 1.8.1 Resetting an AP

Reset an AP when it cannot work properly.

#### Context



#### CAUTION

Exercise caution when resetting an AP because services on the AP will be interrupted.

---

### Procedure

- Step 1** Run:  
**system-view**
- The system view is displayed.
- Step 2** Run:  
**wlan**
- The WLAN view is displayed.
- Step 3** Run:  
**ap-reset { all | id *ap-id* }**
- An AP is reset.
- End

## 1.8.2 Upgrading APs

An AP needs to negotiate with an AC about the software version after the AP goes online or the software version on the AC changes. If the software version on the AP is different from that on the AC, the AP starts to upgrade the software.

### Context

An AP supports the following upgrade modes:

- AC mode: An AP downloads the upgrade version file from an AC.
- FTP mode: After the FTP function is configured on an AC using the **ap-update ftp-server** command, an AP downloads the upgrade version file from the specified FTP server.

#### NOTE

- The AC or FTP upgrade mode must be pre-configured on the AC. The AC allows a maximum of 128 APs of the same type to simultaneously load the upgrade version file.
- If the FTP mode is used, ensure that the upgrade version file name matches the version number required by APs. Otherwise, APs will repeatedly restart.

### Procedure

- Configure the AC mode.

#### NOTE

When the AC mode is used, upload the AP upgrade version file to the AC using TFTP or FTP.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
wlan
```

The WLAN view is displayed.

3. Run:

```
ap-update mode { ftp-mode | ac-mode }
```

The AP upgrade mode is set to AC mode.

4. Run:

```
ap-update update-filename filename ap-type type-id
```

The AP upgrade version file is specified.

- Configure the FTP mode.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
wlan
```

The WLAN view is displayed.

3. Run:

```
ap-update ftp-server server-ip-address [ftp-username ftpusername | ftp-
password ftppassword] *
```

The FTP server's IP address, FTP user name, and password are configured.

 **NOTE**

The AP upgrade version file must be stored in the FTP working directory on the FTP server. Ensure that the AP and FTP are reachable to each other.

4. Run:

```
ap-update mode { ftp-mode | ac-mode }
```

The AP upgrade mode is set to FTP mode.

5. Run:

```
ap-update update-filename filename ap-type type-id
```

The AP upgrade version file is specified.

----End

## Follow-up Procedure

- Run the **ap-update multi-load ap-type type-id** command to upgrade APs of the specified type online.
- After the APs are upgraded, run the **ap-update multi-reset ap-type type-id** to reset the APs.

## 1.8.3 Locating APs

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

### Context

Signals of unauthorized APs on a WLAN may interfere with signals of authorized APs on the WLAN, deteriorating the signal transmission quality or even data loss. To remove unauthorized APs from the WLAN to ensure network security, you need to analyze the APs' locations and neighbor relationships and locate the APs in the network topology.

### Procedure

**Step 1** Run:

```
display neighbor ap-id ap-id radio-id radio-id
```

Information about neighbors of the specified radio is displayed.

You can learn the AP distribution information and neighbor relationships between APs according to the neighbor information.

----End

## 1.8.4 Viewing Statistics

You can run **display** commands to view statistics about users and packets.

## Procedure

- Run the **display statistics { arp | icmp } ap-id ap-id** command to view ARP or ICMP packet statistics on a specified AP.
- Run the **display statistics ssid ssid-name ap ap-id radio radio-id** command to view statistics about packets with the specified SSID on the radio of an AP.
- Run the **display statistics { mac | calibrate } ap-id ap-id radio-id radio-id** command to view statistics about the MAC layer, channel, or power calibration of a specified radio.
- Run the **display station assoc-info { sta mac-address | ap ap-id [ radio radio-id | radio radio-id service-set service-set-id ] }** command to view information about a specified STA or all STAs associated with an AP, a radio of an AP, or an extended service set (ESS) on a radio.
- Run the **display station assoc-num { service-set service-set-id | ap ap-id [ radio radio-id ] }** command to view the number of STAs associated with a specified service set or AP.
- Run the **display station statistics { sta mac-address | ap ap-id }** command to view traffic statistics on a specified STA, including the number of packets or bytes sent and received by the STA and rate of the STA. If an AP is specified, this command displays the number of STAs associated with, disassociated from, and reassociated with the AP.
- Run the **display station status sta mac-address** command to view status of an STA, including the SSID of the WLAN to which the STA connects, online duration, uplink signal noise ratio, and uplink receiving power of the STA.
- Run the **display statistics sta mac-address** command to view statistics about online STAs.

----End

## 1.8.5 Deleting the Statistics

This section describes how to delete the user statistics.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **reset aaa statistics authentication** command to delete the statistics on AAA user authentication.
- Step 3** Run the **reset access-user statistics** command to delete the statistics on access user authentication.

----End

## 1.9 Configuration Examples

### 1.9.1 Example for Configuring the WLAN Service

#### Networking Requirements

An Internet service provider (ISP) provides the WLAN service for two neighboring areas A and B. AP1 provides the WLAN service for area A, and AP2 provides the WLAN service for area B.

Figure 1-3 shows the networking diagram.

- The SPU in slot 1 of the Switch functions as an AC.
- The APs assign service VLANs to users; the Switch transparently transmits packets of all service VLANs and tags AP management packets with the management VLAN ID.
- The AC functions as a DHCP server to allocate IP addresses to APs.
- AP1 and AP2 directly forward service data.

Figure 1-3 Networking diagram of WLAN service configurations

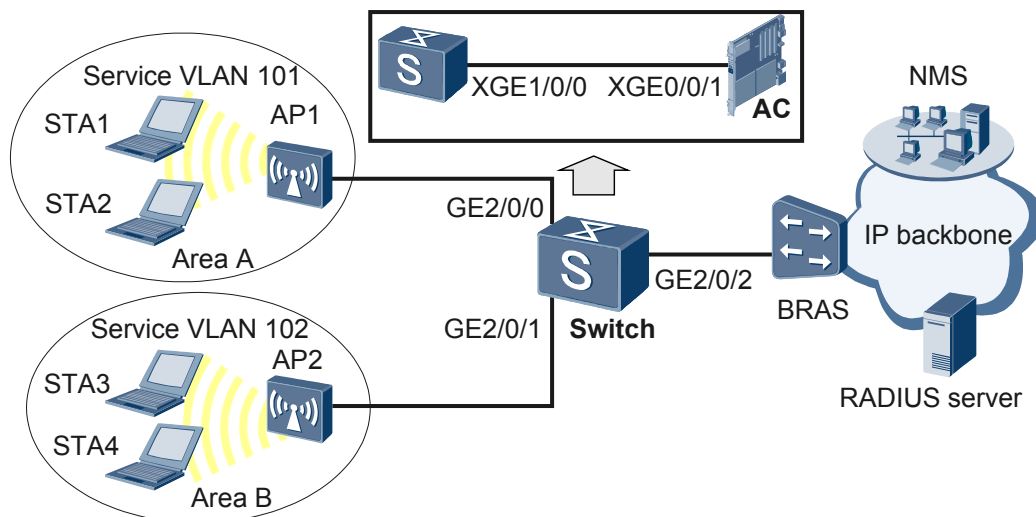


Table 1-1 WLAN service data plan

| Item                    | Data                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WLAN service            | WEP open system authentication and no encryption                                                                                                                                                                                                                                                                                                                                            |
| Management VLAN for APs | VLAN 100, which is assigned by the Switch                                                                                                                                                                                                                                                                                                                                                   |
| AP region               | AP1: 101<br>AP2: 102                                                                                                                                                                                                                                                                                                                                                                        |
| Service set             | <ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-1</li> <li>● WLAN virtual interface: WLAN-ESS 0</li> <li>● Data forwarding mode: direct forwarding</li> </ul> <ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-2</li> <li>● WLAN virtual interface: WLAN-ESS 1</li> <li>● Data forwarding mode: direct forwarding</li> </ul> |
| User VLAN               | AP1: VLAN 101<br>AP2: VLAN 102                                                                                                                                                                                                                                                                                                                                                              |
| VLANs on the Switch     | VLAN 100/101/102                                                                                                                                                                                                                                                                                                                                                                            |

| Item                            | Data                                     |
|---------------------------------|------------------------------------------|
| AC carrier ID/AC ID             | other/1                                  |
| Management IP address of the AC | VLANIF interface address: 192.168.0.1/24 |
| Address pool for APs            | 192.168.0.2–192.168.0.254/24             |
| Gateway address for APs         | 192.168.0.1/24 (IP address of the AC)    |
| DHCP server                     | AC                                       |

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Switch and the AC to enable APs to communicate with the AC.
2. Configure basic AC attributes, including the AC ID, carrier ID, countrycode and source interface that the AC uses to communicate with APs. Configure the AC as a DHCP server.
3. Set the AP authentication mode and add APs to an AP region.
4. Configure VAPs and deliver VAP parameters so that STAs can access the WLAN.

To configure a VAP:

- a. Configure a WLAN-ESS interface and bind it to a service set so that radio packets can be sent to the WLAN service module after reaching the AC.
- b. Configure a radio profile on the AC and bind it to a radio to enable STAs to communicate with the AP.
- c. Configure a service set and bind a security profile and a traffic profile to it to ensure wireless access security and QoS for STAs.
- d. Configure a VAP and deliver VAP parameters so that STAs can access the WLAN.

## Procedure

**Step 1** Configure the Switch and the AC to enable APs to communicate with the AC.

# Configure GE2/0/0 and GE2/0/1 of the Switch connected to APs as trunk interfaces, and set the PVID of the trunk interfaces to 100.

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] interface GigabitEthernet 2/0/0
[Quidway-GigabitEthernet2/0/0] port link-type trunk
[Quidway-GigabitEthernet2/0/0] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/0] port trunk allow-pass vlan 100 101
[Quidway-GigabitEthernet2/0/0] quit
[Quidway] interface GigabitEthernet 2/0/1
[Quidway-GigabitEthernet2/0/1] port link-type trunk
[Quidway-GigabitEthernet2/0/1] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 102
[Quidway-GigabitEthernet2/0/1] quit
```

# Configure XGE1/0/0 of the Switch connected to the AC to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 1/0/0
[Quidway-XGigabitEthernet1/0/0] port link-type trunk
[Quidway-XGigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 102
```

# Configure XGE0/0/1 of the AC connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC
[AC] vlan batch 100 to 102
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[AC-XGigabitEthernet0/0/1] quit
```

## Step 2 Configure basic AC attributes.

# Configure the AC ID, carrier ID, and country code.

```
[AC] wlan ac-global ac id 1 carrier id other
[AC] wlan ac-global country-code country-code
```

# Configure VLANIF interfaces, assign IP addresses to them for Layer 3 packet forwarding, and enable DHCP.

Configure an IP address pool on VLANIF 100 to assign IP addresses to APs, configure an IP address pool on VLANIF 101 to assign IP addresses to STAs in area A, and configure an IP address pool on VLANIF 102 to assign IP addresses to STAs in area B.

```
[AC] dhcp enable
[AC] interface vlanif100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

### NOTE

An AP can set up a connection with an AC only after obtaining an IP address from the AC, a broadband remote access server (BRAS), or a DHCP server. When the AC is configured as a DHCP server, it can allocate IP addresses to APs.

# Configure a source interface on the AC for tunnel communication between APs and the AC.

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
```

### NOTE

An AC uses the IP address of the specified source interface as the source IP address. All APs connected to the AC can learn this IP address.

## Step 3 Configure APs and enable them to go online.

# Set the AP authentication mode to **no-auth**.

```
[AC-wlan-view] ap-auth-mode no-auth
```

### NOTE

If the AP authentication mode is set to **no-auth**, APs of the specified type can go online automatically. After an AP goes online, it is added to the default region and bound to the default AP profile, and its attributes are set to default values. The AP then enters the normal state.

# Configure AP regions 101 and 102.

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```

# Add AP1 to AP region 101 and AP2 to AP region 102.

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

#### Step 4 Configure WLAN-ESS interfaces.

```
[AC] interface wlan-ess0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] dhcp enable
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] dhcp enable
[AC-WLAN-ESS1] quit
```

#### Step 5 Configure radios for APs.

# Create a WMM profile **wmm-1** and use the default settings.

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm-1 id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

# Create a radio profile **radio-1** and bind the WMM profile **wmm-1** to it.

```
[AC-wlan-view] radio-profile name radio-1
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[AC-wlan-radio-prof-radio-1] quit
```

# Bind the radio profile **radio-1** to radios of AP1 and AP2.

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] radio-profile name radio-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name radio-1
[AC-wlan-radio-1/0] quit
```

#### Step 6 Configure service sets for APs.

# Create a security profile.

Create a security profile **security-1**, and set the authentication mode to WEP open system authentication and the encryption mode to no encryption.

```
[AC-wlan-view] security-profile name security-1 id 1
[AC-wlan-sec-prof-security-1] wep authentication-method open-system
[AC-wlan-sec-prof-security-1] security-policy wep
[AC-wlan-sec-prof-security-1] quit
```

# Configure a traffic profile to specify the QoS policy.

Create a traffic profile **traffic-1** and use the default settings.

```
[AC-wlan-view] traffic-profile name traffic-1
[AC-wlan-traffic-prof-traffic-1] quit
```



# Create service sets for AP1 and AP2, and bind the traffic profile, security profile, and WLAN-ESS service to the service sets.

```
[AC-wlan-view] service-set name huawei-1
[AC-wlan-service-set-huawei-1] ssid huawei-1
[AC-wlan-service-set-huawei-1] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-1] security-profile name security-1
[AC-wlan-service-set-huawei-1] wlan-ess 0
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] forward-mode direct-forward
[AC-wlan-service-set-huawei-1] quit
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-2] security-profile name security-1
[AC-wlan-service-set-huawei-2] wlan-ess 1
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] forward-mode direct-forward
[AC-wlan-service-set-huawei-2] quit
```

**Step 7** Configure VAPs for APs and deliver VAP parameters.

# Bind radios of AP1 and AP2 to service sets **huawei-1** and **huawei-2**.

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] service-set name huawei-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
```

# Deliver VAP parameters to APs.

```
[AC-wlan-view] commit ap 0
[AC-wlan-view] commit ap 1
```

**Step 8** Verify the configuration.

Two WLANs with SSIDs **huawei-1** and **huawei-2** are available for STAs connected to AP1 and AP2, and these STAs can connect to the WLAN without authentication.

----End

## Configuration Files

- Configuration file of the AC

```
#
sysname
AC
#
vlan batch 100 to 102
#
dhcp
enable
#
wlan ac-global carrier id other ac id
1
#

interface
Vlanif100
ip address 192.168.0.1
255.255.255.0
dhcp select
interface
#
interface
```

```
Vlanif101
 ip address 192.168.1.1 255.255.255.0

 dhcp select
 interface
 #
 interface
 Vlanif102
 ip address 192.168.2.1
 255.255.255.0
 dhcp select
 interface
 #
 interface WLAN-ESS0
 port hybrid untagged vlan 101
 dhcp enable
 #
 interface WLAN-ESS1
 port hybrid untagged vlan 102
 dhcp enable
 #
 interface
 XGigabitEthernet0/0/1
 port link-type
 trunk
 undo port trunk allow-pass vlan
 1
 port trunk allow-pass vlan 100 to
 102
 #

wlan
 wlan ac source interface
 Vlanif100
 ap-region id
 101
 ap-region id
 102
 ap-auth-mode no-
 auth
 ap id 0 type-id 7 mac 80fb-0616-31d1 sn
 AB34002078
 region-id 101
 ap id 1 type-id 6 mac 5489-9849-8265 sn
 AB36015000
 region-id 102
 wmm-profile name wmm-1 id
 1
 traffic-profile name traffic-1 id
 1
 security-profile name security-1 id
 1
 service-set name huawei-1 id
 1
 wlan-ess
 0
 ssid
 huawei-1
 traffic-profile id
 1
 service-vlan
 101
 service-set name huawei-2 id
 2
 wlan-ess
 1
 ssid
 huawei-2
 traffic-profile id
```

```
2
 service-vlan
102
 radio-profile name radio-1 id
1
 wmm-profile id
1
 ap 0 radio
0
 radio-profile name
radio-1
 service-set id 0 wlan 1
 ap 1 radio
0
 radio-profile name
radio-1
 service-set id 1 wlan 1
#
return
```

- Configuration file of the Switch

```
#
vlan batch 100 to 102
#
interface GigabitEthernet2/0/0
 port link-type
trunk
 port trunk pvid vlan
100
 port trunk allow-pass vlan 100 to
101
#
interface GigabitEthernet2/0/1
 port link-type
trunk
 port trunk pvid vlan
100
 port trunk allow-pass vlan 100
102
#
interface
XGigabitEthernet1/0/0
 port link-type
trunk
 port trunk allow-pass vlan 100 to
102
#
```

## 1.9.2 Example for Configuring Dual-Link Backup on an AP

### Networking Requirements

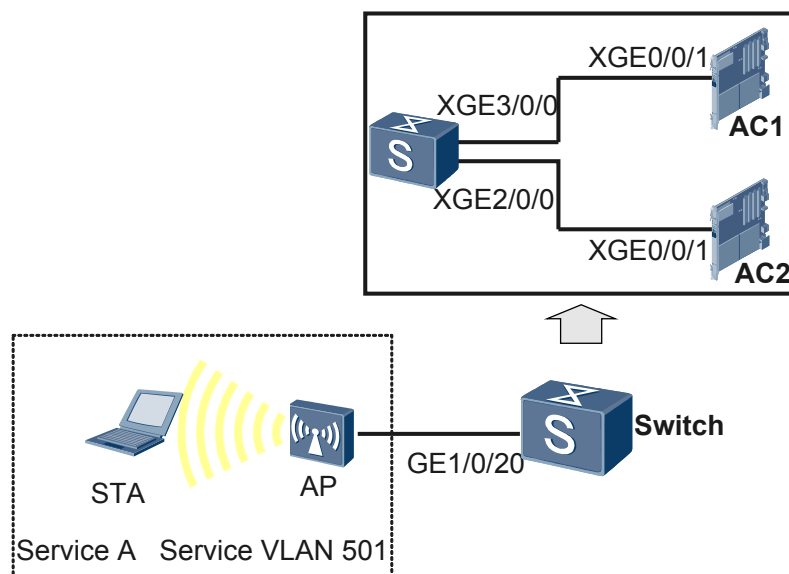
To implement dual-link backup on an AP, the AP needs to establish CAPWAP tunnels with two ACs (active and standby ACs). If the AP detects a fault on the tunnel established with the active AC, the AP instructs the standby AC to take the active role. This prevents service interruption caused by CAPWAP tunnel re-establishment.

**Figure 1-4** shows the networking diagram.

- The SPUs in slots 2 and 3 of the Switch function as AC1 and AC2.
- The APs assign service VLANs to users; the Switch transparently transmits packets of all service VLANs and tags AP management packets with the management VLAN ID.
- The Switch functions as a DHCP server to allocate IP addresses to APs and STAs.

- The AP directly forwards service data.

**Figure 1-4** Configuring dual-link backup on an AP



**Table 1-2** Data plan

| Item                       | Data                                                                                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WLAN service               | WEP open system authentication and no encryption                                                                                                                                          |
| Management VLAN of the AP  | VLAN 500, which is assigned by the Switch                                                                                                                                                 |
| AP region                  | 101                                                                                                                                                                                       |
| Service set                | <ul style="list-style-type: none"> <li>● Name: Huawei</li> <li>● SSID: Huawei</li> <li>● WLAN virtual interface: WLAN-ESS 0</li> <li>● Data forwarding mode: direct forwarding</li> </ul> |
| Service VLAN               | 501                                                                                                                                                                                       |
| Switch VLAN                | VLAN 500/501                                                                                                                                                                              |
| AC carrier ID/AC ID        | CTC (China Telecom)/1                                                                                                                                                                     |
| AC1 management IP address  | VLANIF interface address: 60.1.1.2/24                                                                                                                                                     |
| AC2 management IP address  | VLANIF interface address: 60.1.1.3/24                                                                                                                                                     |
| IP address pool for the AP | 60.1.1.4 to 60.1.1.254/24                                                                                                                                                                 |
| Gateway address for the AP | 60.1.1.1/24 (Switch)                                                                                                                                                                      |
| DHCP server                | The Switch functions as a DHCP server to allocate IP addresses to APs and STAs.                                                                                                           |

## Configuration Roadmap

1. Configure the Switch, AC1, and AC2 to enable the AP to communicate with AC1 and AC2.
2. Configure basic attributes for AC1, including the AC ID, carrier ID, and source interface that AC1 uses to communicate with the AP. Configure the Switch as a DHCP server.
3. Configure AC priority and standby AC IP address.
4. Set the AP authentication mode and add the AP to an AP region.
5. Configure VAPs and deliver VAP parameters so that STAs can access the WLAN.
  - a. Configure a WLAN-ESS interface and bind it to a service set so that radio packets can be sent to the WLAN service module after reaching an AC.
  - b. Configure a radio profile on the AP and bind it to a radio to enable STAs to communicate with the AP.
  - c. Configure a service set and bind a security profile and a traffic profile to it to ensure security and QoS for STAs.
  - d. Configure a VAP and deliver VAP parameters so that STAs can access the WLAN.
6. Configure AC2.

## Procedure

### Step 1 Configure the Switch.

# Set the link type of GE1/0/20 connected to the AP to trunk and PVID to 500.

```
<Quidway> system-view
[Quidway] vlan batch 500 501
[Quidway] interface GigabitEthernet 1/0/20
[Quidway-GigabitEthernet1/0/20] port link-type trunk
[Quidway-GigabitEthernet1/0/20] port trunk pvid vlan 500
[Quidway-GigabitEthernet1/0/20] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet1/0/20] quit
```

# Configure XGE3/0/0 connected to AC1 to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 3/0/0
[Quidway-XGigabitEthernet3/0/0] port link-type trunk
[Quidway-XGigabitEthernet3/0/0] port trunk allow-pass vlan 500 to 501
[Quidway-XGigabitEthernet3/0/0] quit
```

# Configure XGE2/0/0 connected to AC2 to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 2/0/0
[Quidway-XGigabitEthernet2/0/0] port link-type trunk
[Quidway-XGigabitEthernet2/0/0] port trunk allow-pass vlan 500 to 501
[Quidway-XGigabitEthernet2/0/0] quit
```

# Create VLANIF 500 and VLANIF 501, enable the DHCP server function, and configure IP address pools on the two VLANIF interfaces.

```
[Quidway] dhcp enable
[Quidway] interface vlanif500
[Quidway-vlanif500] ip address 60.1.1.1 255.255.255.0
[Quidway-vlanif500] dhcp select interface
[Quidway-vlanif500] quit
[Quidway] dhcp enable
[Quidway] interface vlanif501
[Quidway-vlanif501] ip address 60.1.2.1 255.255.255.0
```

```
[Quidway-vlanif501] dhcp select interface
[Quidway-vlanif501] quit
```

## Step 2 Configure AC1.

# Configure XGE0/0/1 connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC1
[AC1] interface XGigabitEthernet 0/0/1
[AC1-XGigabitEthernet0/0/1] port link-type trunk
[AC1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/1] quit
```

# Configure the AC ID, carrier ID, and country code.

```
[AC1] wlan ac-global ac id 1 carrier id ctc
[AC1] wlan ac-global country-code cn
```

# Configure a source interface on AC1 to communicate with the AP.

```
[AC1] interface vlanif500
[AC1-vlanif500] ip address 60.1.1.2 255.255.255.0
[AC1-vlanif500] quit
[AC1] wlan
[AC1-wlan-view] wlan ac source interface vlanif 500
[AC1-wlan-view] quit
```

# Configure the AC priority and standby AC IP address in the WLAN view to implement dual-link backup.

```
[AC1-wlan-view] wlan ac protect enable protect-ac 60.1.1.5 priority 2
[AC1-wlan-view] wlan ac protect restore
```

### NOTE

To differentiate the configurations in the WLAN view and AP view, ensure that the standby AC IP address configured in the WLAN view is not the source interface address of AC2.

# Configure the AC priority and standby AC IP address in the AP view to implement dual-link backup.

```
[AC1-wlan-view] ap id 0
[AC1-wlan-view] priority 3 protect 60.1.1.3
[AC1-wlan-view] quit
```

### NOTE

The AC priority and standby AC IP address configured in the AP view take effect on an AP. That is, AC priority 3 and standby AC IP address 60.1.1.3 take effect.

# Set the AP authentication mode to no-auth.

```
[AC1-wlan-view] ap-auth-mode no-auth
```

# Set the AP region ID to 101.

```
[AC1-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```

# Add the AP to AP region 101.

```
[AC-wlan-view] ap id 0
[AC1-wlan-ap-0] region-id 101
[AC1-wlan-ap-0] quit
```

# Configure a WLAN-ESS interface.

```
[AC1] interface wlan-ess 0
[AC1-WLAN-ESS1] quit
```

# Create a WMM profile named **wmm** and retain the default parameter settings.

```
[AC1] wlan
[AC1-wlan-view] wmm-profile name wmm id 1
[AC1-wlan-wmm-prof-wmm] quit

Create a radio profile named radio and bind the WMM profile wmm to it.

[AC1-wlan-view] radio-profile name radio
[AC1-wlan-radio-prof-radio] wmm-profile name wmm
[AC1-wlan-radio-prof-radio] quit

Bind the radio profile radio to the radio of the AP.

[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] radio-profile name radio
[AC1-wlan-radio-0/0] quit

Create a security profile named security, and set the authentication mode to WEP open system authentication and the encryption mode to no encryption.

[AC1-wlan-view] security-profile name security id 1
[AC1-wlan-sec-prof-security] wep authentication-method open-system
[AC1-wlan-sec-prof-security] security-policy wep
[AC1-wlan-sec-prof-security] quit

Configure a traffic profile named traffic and retain the default parameter settings.

[AC1-wlan-view] traffic-profile name traffic
[AC1-wlan-traffic-prof-traffic] quit

Create a service set for the AP, and bind the traffic profile, security profile, and WLAN-ESS service interface to the service set.

[AC1-wlan-view] service-set name huawei
[AC1-wlan-service-set-huawei] ssid huawei
[AC1-wlan-service-set-huawei] traffic-profile name traffic
[AC1-wlan-service-set-huawei] security-profile name security
[AC1-wlan-service-set-huawei] wlan-ess 0
[AC1-wlan-service-set-huawei] service-vlan 501
[AC1-wlan-service-set-huawei] forward-mode direct-forward
[AC1-wlan-service-set-huawei] quit

Bind the radio of the AP to service set huawei.

[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] service-set name huawei
[AC1-wlan-radio-0/0] quit

Deliver VAP parameters to the AP.

[AC1-wlan-view] commit ap 0
```

### Step 3 Configure AC2.

# Configure XGE0/0/1 connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC2
[AC2] interface XGigabitEthernet 0/0/1
[AC2-XGigabitEthernet0/0/1] port link-type trunk
[AC2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/1] quit
```

# Configure the AC ID, carrier ID, and country code.

```
[AC2] wlan ac-global ac id 2 carrier id ctc
[AC2] wlan ac-global country-code cn
```

# Configure a source interface on AC2 to communicate with the AP.

```
[AC2] interface vlanif500
[AC2-vlanif500] ip address 60.1.1.3 255.255.255.0
[AC2-vlanif500] quit
[AC2] wlan
[AC2-wlan-view] wlan ac source interface vlanif 500
[AC2-wlan-view] quit

Enable dual-link backup and active/standby AC switchback in the WLAN view.
[AC2-wlan-view] wlan ac protect enable
[AC2-wlan-view] wlan ac protect restore

Configure the AC priority and standby AC IP address in the AP view to implement dual-link
backup.
[AC1-wlan-view] ap id 0
[AC1-wlan-view] priority 6 protect 60.1.1.2
[AC1-wlan-view] quit
```

**NOTE**

Configure basic parameters for AC2 according to the configurations of AC1.

**Step 4** Verify the configuration.

Run the **display wlan ac protect** command to view the priority of AC1 and IP address of AC2 (a backup to AC1).

The WLAN with SSID **huawei** is available for STAs connected to the AP, and these STAs can connect to the WLAN without authentication.

When the AP detects a fault on the link connected to AC1, it instructs AC2 to take the active role. This ensures service stability.

----End

## Configuration File

- Configuration file of the Switch

```
#
vlan batch 500 to 501
#
dhcp
enable
#
interface
Vlanif500
ip address 60.1.1.1
255.255.255.0
dhcp select
interface
#
interface
Vlanif501
ip address 60.1.2.1
255.255.255.0
dhcp select
interface
#
interface
GigabitEthernet1/0/20
port link-type
trunk
port trunk pvid vlan
500
port trunk allow-pass vlan 500 to
501
#
interface
```



```
XGigabitEthernet2/0/0
 port link-type
 trunk
 port trunk allow-pass vlan 500 to 501
 #
 interface
 XGigabitEthernet3/0/0
 port link-type
 trunk
 port trunk allow-pass vlan 500 to
 501
 #
```

● Configuration file of the AC1

```
#
 sysname
 AC1
 #
 vlan batch 500 to
 501
 #
 wlan ac-global carrier id ctc ac id
 1
 #
 interface
 Vlanif500
 ip address 60.1.1.2
 255.255.255.0
 #
 interface
 XGigabitEthernet0/0/1
 port link-type
 trunk
 port trunk allow-pass vlan 500 to
 501
 #
 interface Wlan-
 Ess0
 #
 wlan
 wlan ac source interface
 vlanif500
 wlan ac protect enable protect-ac 60.1.1.5 priority 2
 ap-region id
 101
 ap-auth-mode no-
 auth
 ap id 0
 priority
 3
 protect-ac
 60.1.1.3
 region-id
 101
 wmm-profile name wmm id
 4
 traffic-profile name traffic id
 1
 security-profile name security id
 1
 service-set name huawei id
 6
 wlan-ess
 0
 ssid
 huawei
 traffic-profile id
 1
 security-profile id
 1
```

```

 service-vlan
501
 radio-profile name radio id
4
 wmm-profile id
4
 ap 0 radio
0
 radio-profile id
4
 service-set id 6 wlan
1

#
return

```

● Configuration file of the AC2

```

#
sysname
AC2
#
vlan batch 500 to
501
#
wlan ac-global carrier id ctc ac id
2
#
interface
Vlanif500
ip address 60.1.1.3
255.255.255.0
#
interface
XGigabitEthernet0/0/1
port link-type
trunk
port trunk allow-pass vlan 500 to
501
#
interface Wlan-
Ess0
#
wlan
wlan ac source interface
vlanif500
wlan ac protect enable
ap-region id
101
ap-auth-mode no-
auth
ap id 0
priority
6
protect-ac
60.1.1.2
region-id
101

wmm-profile name wmm id
4
traffic-profile name traffic id
1
security-profile name security id
1
service-set name huawei id
6
wlan-ess
0
ssid
huawei

```

```
 traffic-profile id
1
 security-profile id
1
 service-vlan
501
 radio-profile name radio id
4
 wmm-profile id
4
 ap 0 radio
0
 radio-profile id
4
 service-set id 6 wlan
1

#
return
```

## 1.9.3 Example for Configuring Dual-Link Backup Globally

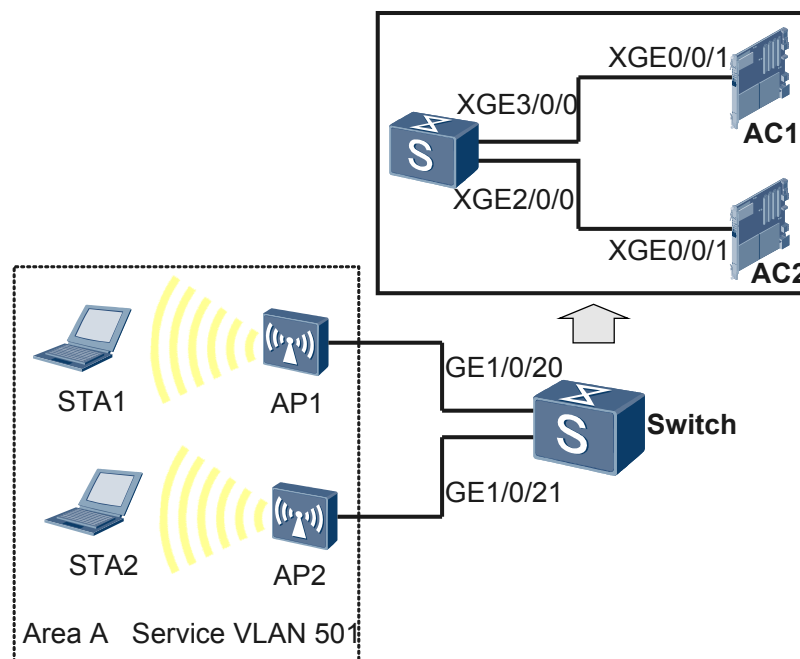
### Networking Requirements

To implement dual-link backup, an AP needs to establish CAPWAP tunnels with two ACs (active and standby ACs). If the AP detects a fault on the tunnel established with the active AC, the AP instructs the standby AC to take the active role. This prevents service interruption caused by CAPWAP tunnel re-establishment.

**Figure 1-5** shows the networking diagram.

- The SPUs in slots 2 and 3 of the Switch function as AC1 and AC2.
- The APs assign service VLANs to users; the Switch transparently transmits packets of all service VLANs and tags AP management packets with the management VLAN ID.
- The Switch functions as a DHCP server to allocate IP addresses to APs and STAs.
- AP1 and AP2 directly forward service data.

**Figure 1-5** Configuring dual-link backup globally



**Table 1-3** Data plan

| Item                      | Data                                                                                                                                                                                      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WLAN service              | WEP open system authentication and no encryption                                                                                                                                          |
| Management VLAN of APs    | VLAN 500, which is assigned by the Switch                                                                                                                                                 |
| AP region                 | 101                                                                                                                                                                                       |
| Service set               | <ul style="list-style-type: none"> <li>● Name: Huawei</li> <li>● SSID: Huawei</li> <li>● WLAN virtual interface: WLAN-ESS 0</li> <li>● Data forwarding mode: direct forwarding</li> </ul> |
| Service VLAN              | 501                                                                                                                                                                                       |
| Switch VLAN               | VLAN 500/501                                                                                                                                                                              |
| AC carrier ID/AC ID       | CTC (China Telecom)/1                                                                                                                                                                     |
| AC1 management IP address | VLANIF interface address: 60.1.1.2/24                                                                                                                                                     |
| AC2 management IP address | VLANIF interface address: 60.1.1.3/24                                                                                                                                                     |
| IP address pool for APs   | 60.1.1.4 to 60.1.1.254/24                                                                                                                                                                 |
| Gateway address for APs   | 60.1.1.1/24 (Switch)                                                                                                                                                                      |
| DHCP server               | The Switch functions as a DHCP server to allocate IP addresses to APs and STAs.                                                                                                           |

## Configuration Roadmap

1. Configure the Switch, AC1, and AC2 to enable APs to communicate with AC1 and AC2.
2. Configure basic attributes for AC1, including the AC ID, carrier ID, and source interface that AC1 uses to communicate with APs. Configure the Switch as a DHCP server.
3. Configure AC priority and standby AC IP address.
4. Set the AP authentication mode and add APs to an AP region.
5. Configure VAPs and deliver VAP parameters so that STAs can access the WLAN.
  - a. Configure a WLAN-ESS interface and bind it to a service set so that radio packets can be sent to the WLAN service module after reaching an AC.
  - b. Configure a radio profile on APs and bind it to a radio to enable STAs to communicate with the APs.
  - c. Configure a service set and bind a security profile and a traffic profile to it to ensure security and QoS for STAs.
  - d. Configure a VAP and deliver VAP parameters so that STAs can access the WLAN.
6. Configure AC2.

## Procedure

### Step 1 Configure the Switch.

# Set the link type of GE1/0/20 connected to AP1 to trunk and PVID to 500.

```
<Quidway> system-view
[Quidway] vlan batch 500 501
[Quidway] interface GigabitEthernet 1/0/20
[Quidway-GigabitEthernet1/0/20] port link-type trunk
[Quidway-GigabitEthernet1/0/20] port trunk pvid vlan 500
[Quidway-GigabitEthernet1/0/20] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet1/0/20] quit
```

# Set the link type of GE1/0/21 connected to AP2 to trunk and PVID to 500.

```
[Quidway] interface GigabitEthernet 1/0/21
[Quidway-GigabitEthernet1/0/21] port link-type trunk
[Quidway-GigabitEthernet1/0/21] port trunk pvid vlan 500
[Quidway-GigabitEthernet1/0/21] port trunk allow-pass vlan 500 to 501
[Quidway-GigabitEthernet1/0/21] quit
```

# Configure XGE3/0/0 connected to AC1 to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 3/0/0
[Quidway-XGigabitEthernet3/0/0] port link-type trunk
[Quidway-XGigabitEthernet3/0/0] port trunk allow-pass vlan 500 to 501
[Quidway-XGigabitEthernet3/0/0] quit
```

# Configure XGE2/0/0 connected to AC2 to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 2/0/0
[Quidway-XGigabitEthernet2/0/0] port link-type trunk
[Quidway-XGigabitEthernet2/0/0] port trunk allow-pass vlan 500 to 501
[Quidway-XGigabitEthernet2/0/0] quit
```

# Create VLANIF 500 and VLANIF 501, enable the DHCP server function, and configure IP address pools on the two VLANIF interfaces.

```
[Quidway] dhcp enable
[Quidway] interface vlanif500
```

```
[Quidway-vlanif500] ip address 60.1.1.1 255.255.255.0
[Quidway-vlanif500] dhcp select interface
[Quidway-vlanif500] quit
[Quidway] dhcp enable
[Quidway] interface vlanif501
[Quidway-vlanif501] ip address 60.1.2.1 255.255.255.0
[Quidway-vlanif501] dhcp select interface
[Quidway-vlanif501] quit
```

## Step 2 Configure AC1.

# Configure XGE0/0/1 connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC1
[AC1] interface XGigabitEthernet 0/0/1
[AC1-XGigabitEthernet0/0/1] port link-type trunk
[AC1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC1-XGigabitEthernet0/0/1] quit
```

# Configure the AC ID, carrier ID, and country code.

```
[AC1] wlan ac-global ac id 1 carrier id ctc
[AC1] wlan ac-global country-code cn
```

### NOTE

The default country code is CN.

# Configure a source interface on AC1 to communicate with APs.

```
[AC1] interface vlanif500
[AC1-vlanif500] ip address 60.1.1.2 255.255.255.0
[AC1-vlanif500] quit
[AC1] wlan
[AC1-wlan-view] wlan ac source interface vlanif 500
[AC1-wlan-view] quit
```

# Configure the AC priority and standby AC IP address in the WLAN view to implement dual-link backup.

```
[AC1-wlan-view] wlan ac protect enable protect-ac 60.1.1.3 priority 2
[AC1-wlan-view] wlan ac protect restore
```

# Set the AP authentication mode to no-auth.

```
[AC1-wlan-view] ap-auth-mode no-auth
```

# Set the AP region ID to 101.

```
[AC1-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```

# Add AP1 and AP2 to AP region 101.

```
[AC-wlan-view] ap id 0
[AC1-wlan-ap-0] region-id 101
[AC1-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC1-wlan-ap-1] region-id 101
[AC1-wlan-ap-1] quit
```

# Configure a WLAN-ESS interface.

```
[AC1] interface wlan-ess 0
[AC1-WLAN-ESS1] dhcp enable
[AC1-WLAN-ESS1] quit
```

# Create a WMM profile named **wmm** and retain the default parameter settings.

```
[AC1] wlan
[AC1-wlan-view] wmm-profile name wmm id 1
[AC1-wlan-wmm-prof-wmm] quit

Create a radio profile named radio and bind the WMM profile wmm to it.

[AC1-wlan-view] radio-profile name radio
[AC1-wlan-radio-prof-radio] wmm-profile name wmm
[AC1-wlan-radio-prof-radio] quit

Bind the radio profile radio to radios of AP1 and AP2.

[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] radio-profile name radio
[AC1-wlan-radio-0/0] quit
[AC1-wlan-view] ap 1 radio 0
[AC1-wlan-radio-1/0] radio-profile name radio
[AC1-wlan-radio-1/0] quit

Create a security profile named security, and set the authentication mode to WEP open system authentication and the encryption mode to no encryption.

[AC1-wlan-view] security-profile name security id 1
[AC1-wlan-sec-prof-security] wep authentication-method open-system
[AC1-wlan-sec-prof-security] security-policy wep
[AC1-wlan-sec-prof-security] quit

Configure a traffic profile named traffic and retain the default parameter settings.

[AC1-wlan-view] traffic-profile name traffic
[AC1-wlan-traffic-prof-traffic] quit

Create a service set for AP1 and AP2, and bind the traffic profile, security profile, and WLAN-ESS service interface to the service set.

[AC1-wlan-view] service-set name huawei
[AC1-wlan-service-set-huawei] ssid huawei
[AC1-wlan-service-set-huawei] traffic-profile name traffic
[AC1-wlan-service-set-huawei] security-profile name security
[AC1-wlan-service-set-huawei] wlan-ess 0
[AC1-wlan-service-set-huawei] service-vlan 501
[AC1-wlan-service-set-huawei] forward-mode direct-forward
[AC1-wlan-service-set-huawei] quit

Bind radios of AP1 and AP2 to service set huawei.

[AC1-wlan-view] ap 0 radio 0
[AC1-wlan-radio-0/0] service-set name huawei
[AC1-wlan-radio-0/0] quit
[AC1-wlan-view] ap 1 radio 0
[AC1-wlan-radio-1/0] service-set name huawei
[AC1-wlan-radio-1/0] quit

Deliver VAP parameters to the APs.

[AC1-wlan-view] commit ap 0
[AC1-wlan-view] commit ap 1
```

### Step 3 Configure AC2.

# Configure XGE0/0/1 connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC2
[AC2] interface XGigabitEthernet 0/0/1
[AC2-XGigabitEthernet0/0/1] port link-type trunk
[AC2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 500 to 501
[AC2-XGigabitEthernet0/0/1] quit
```

# Configure the AC ID, carrier ID, and country code.

```
[AC2] wlan ac-global ac id 2 carrier id etc
[AC2] wlan ac-global country-code cn
```

# Configure a source interface on AC2 to communicate with the APs.

```
[AC2] interface vlanif500
[AC2-vlanif500] ip address 60.1.1.3 255.255.255.0
[AC2-vlanif500] quit
[AC2] wlan
[AC2-wlan-view] wlan ac source interface vlanif 500
[AC2-wlan-view] quit
```

# Configure the AC priority and standby AC IP address in the WLAN view to implement dual-link backup.

```
[AC2-wlan-view] wlan ac protect enable protect-ac 60.1.1.2 priority 5
[AC2-wlan-view] wlan ac protect restore
```

#### NOTE

Configure basic parameters for AC2 according to the configurations of AC1.

#### Step 4 Verify the configuration.

Run the **display wlan ac protect** command to view the priority of AC1 and IP address of AC2 (a backup to AC1).

The WLAN with SSID **huawei** is available for STAs connected to AP1 and AP2, and these STAs can connect to the WLAN without authentication.

When an AP detects a fault on the link connected to AC1, it instructs AC2 to take the active role. This ensures service stability.

----End

## Configuration File

- Configuration file of the Switch

```
#
vlan batch 500 to 501
#
dhcp
enable
#
interface
Vlanif500
ip address 60.1.1.1
255.255.255.0
dhcp select
interface
#
interface
Vlanif501
ip address 60.1.2.1
255.255.255.0
dhcp select
interface
#
interface
GigabitEthernet1/0/20
port link-type
trunk
port trunk pvid vlan
500
port trunk allow-pass vlan 500 to
501
```



```
#
interface
GigabitEthernet1/0/21
 port link-type
 trunk
 port trunk pvid vlan
 500
 port trunk allow-pass vlan 500 to
 501
#
interface
XGigabitEthernet2/0/0
 port link-type
 trunk
 port trunk allow-pass vlan 500 to 501
#
interface
XGigabitEthernet3/0/0
 port link-type
 trunk
 port trunk allow-pass vlan 500 to
 501
#
```

- Configuration file of the AC1

```
#
sysname
AC1
#
vlan batch 500 to
501
#
wlan ac-global carrier id ctc ac id
1
#
interface
Vlanif500
 ip address 60.1.1.2
 255.255.255.0
#
interface
XGigabitEthernet0/0/1
 port link-type
 trunk
 port trunk allow-pass vlan 500 to
 501
#
interface Wlan-Ess0
 dhcp enable
#
wlan
 wlan ac source interface
 vlanif500
 wlan ac protect enable protect-ac 60.1.1.3 priority 2
 ap-region id
 101
 ap-auth-mode no-
 auth
 ap id 0
 region-id
 101
 wmm-profile name wmm id 4
 ap id 1
 region-id
 101
 wmm-profile name wmm id 4
 traffic-profile name traffic id
 1
 security-profile name security id 1
 service-set name huawei id
```

```

6
 wlan-ess
0
 ssid
huawei
 traffic-profile id
1
 security-profile id
1
 service-vlan
501
 radio-profile name radio id
4
 wmm-profile id
4
 ap 0 radio
0
 radio-profile id
4
 service-set id 6 wlan 1
 ap 1 radio
0
 radio-profile id
4
 service-set id 6 wlan
1

#
return

```

- Configuration file of the AC2

```

#
sysname
AC2
#
vlan batch 500 to
501
#
wlan ac-global carrier id ctc ac id
2
#
interface
Vlanif500
 ip address 60.1.1.3
255.255.255.0
#
interface
XGigabitEthernet0/0/1
 port link-type
trunk
 port trunk allow-pass vlan 500 to
501
#
interface Wlan-
Ess0
#
wlan
 wlan ac source interface
vlanif500
 wlan ac protect enable protect-ac 60.1.1.2 priority 5
 ap-region id
101
 ap-auth-mode no-
auth
 ap id 0
 region-id
101

 wmm-profile name wmm id 4
 ap id 1

```

```
 region-id
101
 wmm-profile name wmm id
4
 traffic-profile name traffic id
1
 security-profile name security id
1
 service-set name huawei id
6
 wlan-ess
0
 ssid
huawei
 traffic-profile id
1
 security-profile id
1
 service-vlan
501
 radio-profile name radio id
4
 wmm-profile id
4
 ap 0 radio
0
 radio-profile id
4
 service-set id 6 wlan 1
 ap 1 radio
0
 radio-profile id
4
 service-set id 6 wlan
1
#
return
```

# 2 WLAN WDS Configuration

---

## About This Chapter

This section describes the configuration procedures of WLAN Wireless Distribution System (WDS).

### [2.1 Introduction to WDS](#)

### [2.2 WLAN WDS Features Supported by the SPU](#)

The SPU, functioning as an AC, provides the wireless bridge management, bridge whitelist management, AP wired interface management, and WDS Spanning Tree Protocol (STP) management functions. After you configure AP parameters on the SPU, you must deliver the parameters to APs to make the configurations take effect.

### [2.3 Configuring the WDS Service](#)

This section describes the procedure for configuring the WLAN WDS service in the AC+Fit AP networking mode.

### [2.4 Configuring the Bridge Whitelist](#)

### [2.5 Configuring the AP Wired Interface](#)

### [2.6 Configuring STP](#)

### [2.7 Delivering Parameters to AP](#)

### [2.8 Configuration Examples](#)

## 2.1 Introduction to WDS

### Overview

WDS connects two or more wired or wireless LANs wirelessly to establish a large network.

On traditional WLAN, each AP must connect to a wired network to provide wireless services. To enlarge a WLAN, more APs and ACs are required. Therefore, a lot of cables, switches, and power supplies are used. This increases network costs and prolongs network construction period.

WDS allows APs to be connected wirelessly, so it facilitates WLAN construction in a complex environment. On a network constructed using WDS, APs set up wireless connections over multiple hops and connect to ACs wirelessly. WDS has the following notable advantages:

- Low cost, high performance.
- High extensibility: New APs can be added to the network without adding cables.
- Easy to deploy in complex environment, such as subway station, warehouse, large warehouse, manufacturer factory, and dock.

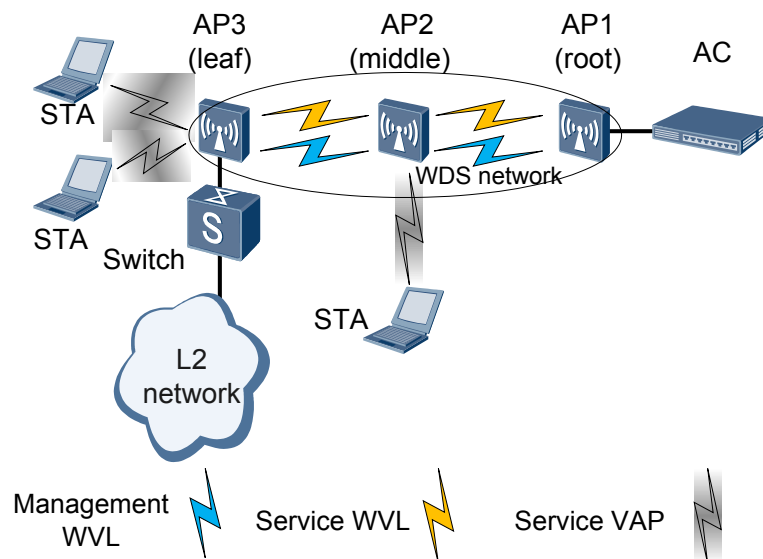
### Concepts

As shown in [Figure 2-1](#), WDS involves the following concepts:

1. On a traditional WLAN, service virtual access points (VAPs) are created on APs to provide access for wireless stations (STAs). On a WDS network, bridge VAPs are created on APs to provide access for neighboring bridges. The bridges then set up wireless links.
  - Bridge: a functional entity on an AP that provides WDS service.
  - Service VAP: a WLAN access point that an AP uses to provide WLAN service for STAs.
  - Bridge VAP: a wireless link access point that an AP uses to set up wireless links with neighboring bridges. A pair of bridge VAPs is created each time, in which one is called AP bridge and the other one is called STA bridge. The AP bridge provides a wireless access point for the STA bridge.
  - Wireless virtual link (WVL): a link set up between two bridge VAPs on different AP bridges.
  - Service WVL: a WVL used to transmit service data.
  - Management WVL: a WVL used to transmit management data. After the wireless bridge function is enabled on APs, the APs automatically set up management WVLs. Management WVLs transmit only management and configuration data.
2. Depending on the AP's location on the WDS network, a wireless bridge works in root, middle, or leaf mode.
  - Root: The AP functions as a root to connect to the AC through a wire, and functions as an AP bridge to connect to a STA bridge.
  - Middle: The AP functions as a middle node to connect to an AP bridge and an STA bridge. When connecting to an AP bridge, the AP is an STA bridge; when connecting to a STA bridge, the AP is an AP bridge.
  - Leaf: The AP connects to an AP bridge as an STA bridge.

3. The wired interfaces of APs on the WDS network can connect to ACs, switches, computers, or servers. Depending on an AP's location, a wired interface works in root or endpoint mode.
  - Root interface: connects to an AC.
  - Endpoint interface: connects to a switch, computer, or server.

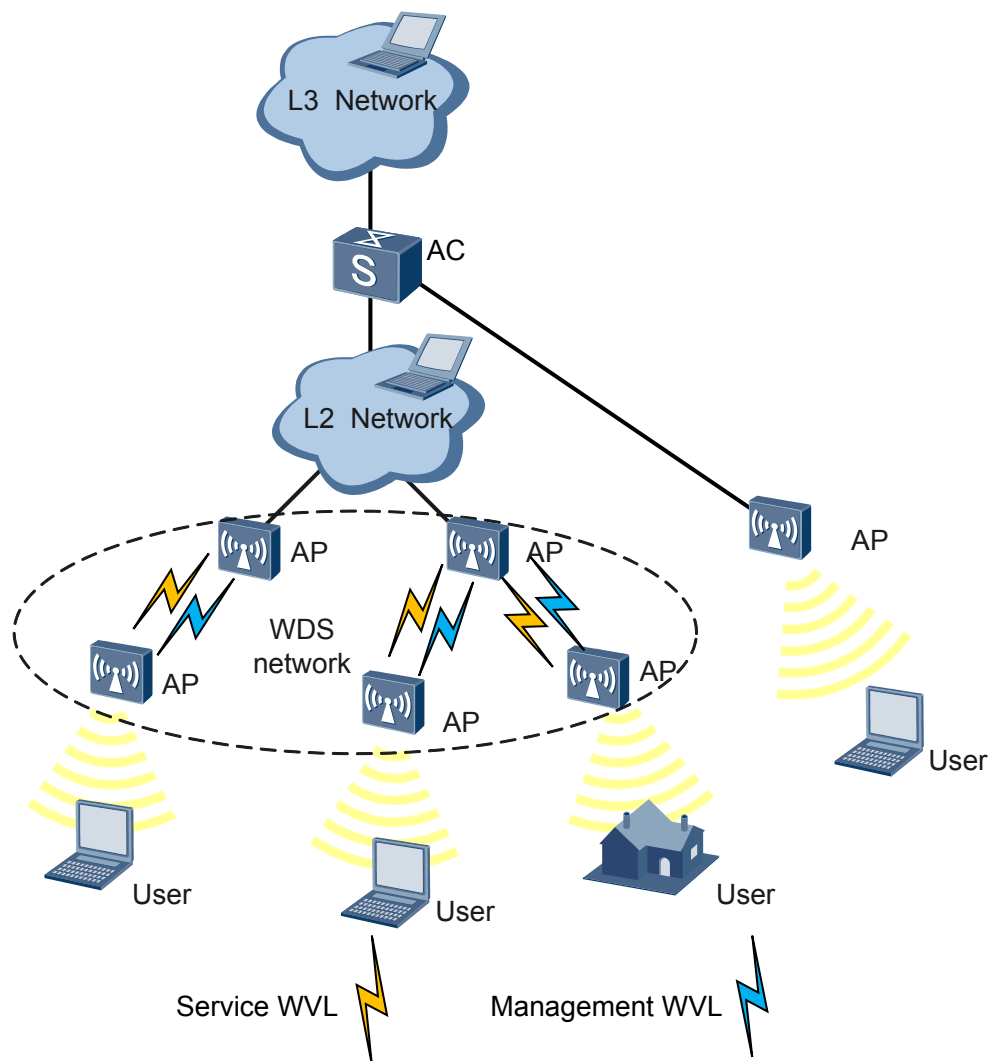
Figure 2-1 WDS network



## WDS Networking and Application

As shown in [Figure 2-2](#), a WDS network connects multiple APs, and APs connect to the AC wirelessly. Users are unaware of the differences between traditional WLAN and WDS networks because the only difference between them is the backbone layer.

**Figure 2-2** APs connecting to the AC through WDS



**NOTE**  
An SPU functions as an AC.

## 2.2 WLAN WDS Features Supported by the SPU

The SPU, functioning as an AC, provides the wireless bridge management, bridge whitelist management, AP wired interface management, and WDS Spanning Tree Protocol (STP) management functions. After you configure AP parameters on the SPU, you must deliver the parameters to APs to make the configurations take effect.

### Wireless Bridge Management

The SPU can configure operation modes for APs according to APs' locations.

A bridge profile contains the attributes of WVLs set up between APs. You can configure a bridge profile on the SPU and bind it to an AP radio so that the AP radio automatically creates a bridge VAP. Using different VAP parameters, the AP radio sets up and maintains the WVLs with neighboring APs.

## Bridge Whitelist Management

A bridge whitelist contains APs' MAC addresses on a WDS network. After a bridge whitelist is configured on the SPU for an AP radio, only the APs with the MAC addresses in the whitelist can associate with the AP radio.

## AP Wired Interface Management

The SPU can configure operation modes for AP wired interfaces according to APs' locations.

When an AP wired interface works in endpoint mode, you can configure allowed VLANs on the wired interface. Additionally, the SPU can configure the user isolation function on the AP wired interfaces.

## STP Management

The SPU can manage STP on wireless bridges and AP wired interfaces.

## WLAN WDS Service Configuration Process

The WLAN WDS service configuration procedure is as follows:

1. Set AP radio parameters and enable the bridge function on the AP radio.
2. Configure the bridge profile.
3. (Optional) Configure a bridge whitelist.
4. Configure a bridge VAP and deliver it to the AP.

### NOTE

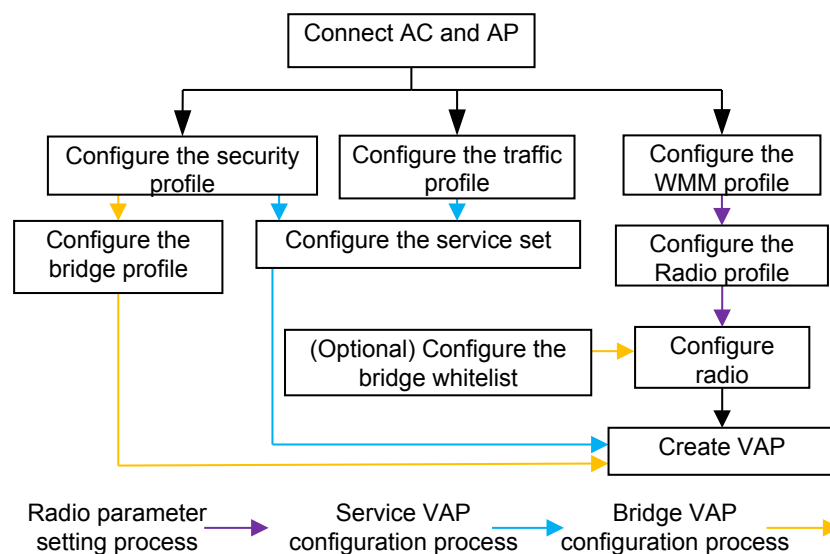
To connect an AP wired interface to a switch, computer, or server, set parameters for the wired interface. Configure STP to prevent loops between bridges and on the networks connected to AP wired interfaces.

**Figure 2-3** shows the WLAN WDS service configuration flowchart. The procedure for configuring bridge VAP is the procedure for configuring WLAN WDS; the procedure for configuring service VAP is the procedure for configuring traditional WLAN service. The configurations of the two VAPs have the following characteristics:

- Similar to service VAP, the bridge VAP is automatically created after a bridge profile is bound to an AP radio.
- The bridge profile is similar to the service set in traditional WLAN service except that the bridge profile only needs to be bound to a security profile.
- Both bridge VAP and service VAP are created based on radio; therefore, before you configure the VAPs, the radio configurations must be complete.
- The bridge whitelist configuration is optional. The bridge whitelist is bound to a radio, but not the bridge profile.



Figure 2-3 WLAN WDS service configuration flowchart



**NOTE**

It is strongly recommended that at most three wireless bridge APs are connected.  
Each AP in root, middle, or leaf mode can be connected to a maximum of six bridge APs.

## 2.3 Configuring the WDS Service

This section describes the procedure for configuring the WLAN WDS service in the AC+Fit AP networking mode.

### 2.3.1 Configuring the Bridge Operation Mode

#### Context

Enable the wireless bridge function and set the bridge operation mode for APs to set up WVLS. The APs can work in three modes: root, middle, and leaf.

#### Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`wlan`  
The WLAN view is displayed.
- Step 3** Run:  
`ap ap-id radio radio-id`  
The AP radio view is displayed.
- Step 4** Run:

```
bridge enable [mode { root | middle | leaf }]
```

The operation mode of the wireless bridge is set.

By default, a wireless bridge works is disabled.

 **NOTE**

The following AP models support WDS: AP6010SN-GN, AP6010DN-AGN, AP6510DN-AGN, AP6610DN-AGN, WA615DN-AGN, WA615DSN-GN, and WA655DN-AGN.

----End

## 2.3.2 Configuring a Bridge Profile

### Prerequisites

A security profile has been created.

### Context

A bridge profile has the same function as the service set in traditional WLAN service. The bridge profile is bound to the specified AP radio to create a bridge VAP.

A bridge profile contains the parameters of WVLS between APs. After a bridge profile is bound to a radio, the radio has all attributes of the bridge profile and automatically creates a bridge VAP. The radio uses different VAP parameters to set up and maintain WVLS between APs.

You can specify VLANs in the bridge profile to control the data allowed to be transmitted over a WVLS.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
bridge-profile {name profile-name | id profile-id } *
```

A bridge profile is created and the bridge profile view is displayed.

**Step 4** Run:

```
bridge-name name
```

The bridge profile identifier is set.

By default, a bridge profile does not have an identifier.

**Step 5** Run:

```
vlan tagged { vlan-id1 [to vlan-id2] } &<1-10>
```

A VLAN or a group of VLANs are added to the bridge profile in tagged mode.

By default, no VLAN is configured in a bridge profile.

 **NOTE**

A maximum of 256 VLANs can be added to a bridge profile.

**Step 6** Run:

```
security-profile { name profile-name | id profile-id }
```

A security profile is bound to the bridge profile.

By default, no security profile is bound to a bridge profile.

---End

## 2.3.3 Configuring a Bridge VAP

### Prerequisites

The specified AP radio has been bound to a radio profile. For details, see [1.5.4 Binding a Radio Profile to a Radio](#) in the *WLAN Configuration*.

A bridge profile has been created and configured. For details, see [2.3.2 Configuring a Bridge Profile](#).

Before binding an AP radio to a bridge profile, check the VAP WLAN IDs. The VAP WLAN IDs 13 and 14 must not be in use.

### Context

Similar to a service VAP, a bridge VAP is a logical unit on the AP's wireless interface. A bridge VAP has a unique MAC address (BSSID) and ID (bridge name). AP radios use the bridge VAP parameters to set up and maintain WVLs with other APs.

Each radio can only be bound to one bridge profile, generating two bridge VAPs. The system automatically allocates WLAN IDs 13 and 14 to the bridge VAPs.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
ap ap-id radio radio-id
```

The AP radio view is displayed.

**Step 4** Run:

```
bridge-profile { name profile-name | id profile-id }
```

The radio is bound to a bridge profile.

By default, a radio is not bound to any bridge profile.

----End

## 2.3.4 Checking the Configuration

### Context

After the WDS service configurations are complete, verify the configurations.

### Procedure

**Step 1** Run the **display bridge-profile** { **all** | **name** *profile-name* | **id** *profile-id* | **bridge-name** *name* } command to check information about a bridge profile.

**Step 2** Run the **display vap** { **all** | **ap** *ap-id* [ **radio** *radio-id* ] } **type bridge-profile** command to check information about a bridge VAP.

 **NOTE**

The **display vap** command can display information about service VAPs and bridge VAPs.

**Step 3** Run the **display bridge-link** command to view the wireless links between APs.

----End

## 2.4 Configuring the Bridge Whitelist

### Context

After a bridge whitelist is configured on an AP radio, only the APs with the MAC addresses in the whitelist can associate with the AP radio. After being authenticated, the APs set up WVLS with the AP radio.

If no whitelist is configured for an AP, all neighboring APs can associate with it.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Create and configure a bridge whitelist.

1. Run the **bridge-whitelist** { **name** *whitelist-name* | **id** *whitelist-id* } \* command to create a bridge whitelist and enter its view.

By default, no bridge whitelist is configured on an AP.

2. Run the **peer ap mac** *mac-address* command to add MAC addresses of neighboring APs to the whitelist.

3. Run the **quit** command to return to the WLAN view.

**Step 4** Bind the radio to a bridge whitelist.

1. Run the **ap** *ap-id* **radio** *radio-id* command to enter the AP radio view.
2. Run the **bridge-whitelist** { **name** *whitelist-name* | **id** *whitelist-id* } command to bind the radio to a bridge whitelist.

By default, no bridge whitelist is configured on an AP radio.

**Step 5** Run:

```
bridge whitelist enable
```

The bridge whitelist bound to the AP radio is enabled.

The bridge whitelist takes effect only after it is enabled.

By default, no bridge whitelist is enabled for wireless bridges.

----End

## Checking the Configuration

- Run the **display bridge-whitelist** { **all** | **id** *whitelist-id* | **name** *whitelist-name* } command to view the bridge whitelist configurations.

## 2.5 Configuring the AP Wired Interface

### Context

Among the APs on a WDS network, one AP must connect to the AC through a wired interface. This wired interface works in root mode. Other APs connect to the AC through WVLS, so their wired interfaces are idle. These wired interfaces can be configured to work in endpoint mode to connect to computers, servers, or Layer 2 networks. The wired interfaces working in endpoint mode have the same functions as switch's hybrid interfaces.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
ap id ap-id
```

The AP view is displayed.

**Step 4** Set parameters for the AP wired interface.

1. Run the **lineate-port mode** { **root** | **endpoint** } command to set the operation mode for the AP wired interface.

By default, an AP wired interface works in root mode.

 **NOTE**

After changing the operation mode, run the **ap-reset** command to reset the AP for the configuration to take effect.

2. Run the **lineate-port pvid vlan *vlan-id*** command to configure the PVID VLAN on the AP wired interface.

By default, no PVID VLAN is configured on an AP wired interface.

3. Run the **lineate-port vlan { tagged | untagged } { *vlan-id1* [ to *vlan-id2* ] }** &<1-10> command to add the AP wired interface to a VLAN.

An AP wired interface supports a maximum of 256 VLANs.

By default, an AP wired interface is not added to any VLAN.

4. Run the **lineate-port user-isolate enable** command to enable user isolation on the AP wired interface.

User isolation can be enabled only on the AP wired interfaces working in endpoint mode.

By default, user isolation is disabled on AP wired interfaces.

---End

## Checking the Configuration

- Run the **display ap { id *ap-id* | by-mac *ap-mac* | by-sn *ap-sn* }** command to view the AP wired interfaces' configurations.

## 2.6 Configuring STP

### Context

When an AP wired interface working in endpoint mode connects to a Layer 2 network, a loop may occur in the Layer 2 network. Network loops may also occur between the wireless bridges on a WDS network.

To prevent loops on the WDS network, enable STP on wireless bridges or AP wired interfaces.

### Procedure

#### Step 1 Enable STP on a wireless bridge.

1. Run the **system-view** command to enter the system view.
2. Run the **wlan** command to enter the WLAN view.
3. Run the **ap *ap-id* radio *radio-id*** command to enter the AP radio view.
4. Run the **bridge stp enable** command to enable STP on the wireless bridge.

By default, STP is disabled on wireless bridges.

5. Run the **quit** command to return to the WLAN view.

#### Step 2 Enable STP on an AP wired interface.

1. Run the **ap id *ap-id*** command to enter the AP view.
2. Run the **bridge stp enable** command to enable STP on the AP wired interface.

By default, STP is disabled on AP wired interfaces.

----End

## 2.7 Delivering Parameters to AP

### Context

All the AP parameters configured on the AC must be delivered to the AP using the **commit** command; otherwise, the parameters do not take effect.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
commit { all | ap ap-id }
```

The AP parameters configured on the AC are delivered to the AP.

----End

## 2.8 Configuration Examples

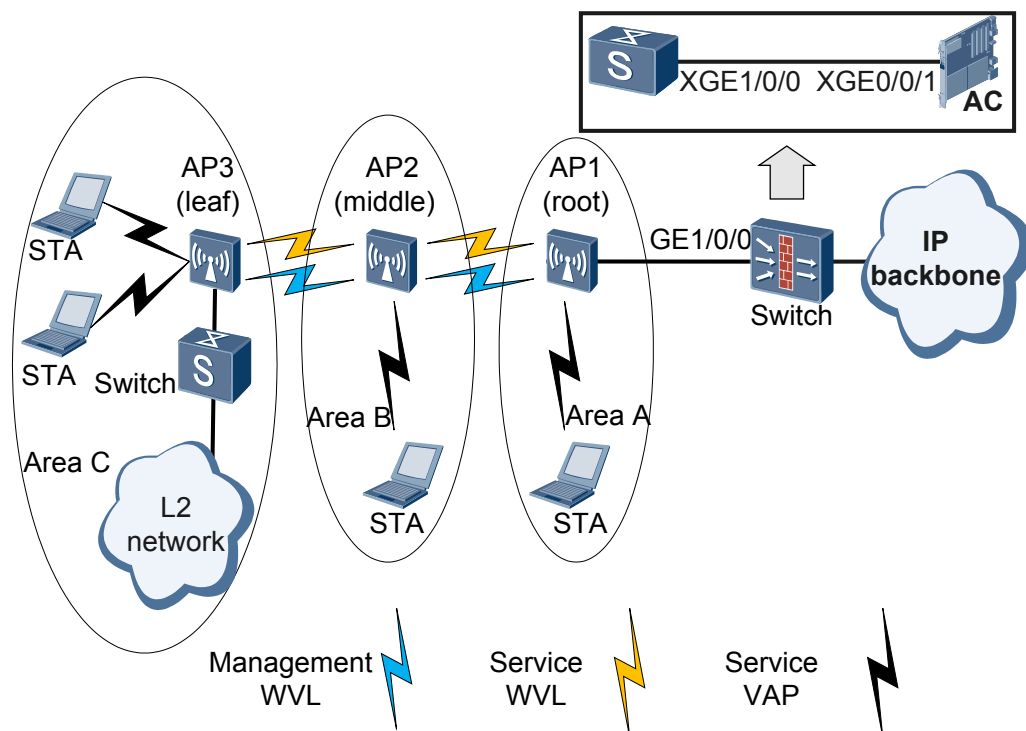
### 2.8.1 Example for Configuring WLAN WDS

#### Network Requirements

As shown in [Figure 2-4](#), a company needs to set up a WLAN for three office areas (area A, area B, and area C). The AC has only one available port to set up the WLAN. To reduce investment, the company decides to connect the APs in areas B and C to the AC wirelessly.

- The SPU provides the AC function and is installed in slot 1 of the S9300.
- The AC also functions as a DHCP server to allocate IP addresses to APs and STAs.
- AP1 connects to the AC through a wire, provides WLAN service for area A, and connects to AP2 as a bridge.
- AP2 connects to the AC through a wireless bridge (AP1), provides WLAN service for area B, and connects to AP3 as a bridge.
- AP3 connects to the AC through a wireless bridge (AP2), provides WLAN service for area C, and connects to a Layer 2 network.

Figure 2-4 WLAN WDS network diagram



## Data Preparation

To complete the configuration, you need the following data.

| AP  | Model   | MAC Address    |
|-----|---------|----------------|
| AP1 | WA603SN | 0025-9e12-6667 |
| AP2 | WA603SN | 5489-9845-9573 |
| AP3 | WA603SN | 80fb-0689-81c3 |

To complete the configuration, you need to plan the following data.

| Item                          | Data                                                                                                                                                                                                                                                                                                 |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN                          | Management VLAN: 100                                                                                                                                                                                                                                                                                 |
|                               | Service VLANs: 101, 102, 103, 104, 105, 106 <ul style="list-style-type: none"> <li>● Area A: VLAN 101 for WLAN service</li> <li>● Area B: VLAN 102 for WLAN service</li> <li>● Area C: VLAN 103 for WLAN service</li> <li>● Area C: VLANs 104, 105, and 106 on wireless interfaces of AP3</li> </ul> |
| Service forwarding mode on AP | Direct forwarding                                                                                                                                                                                                                                                                                    |



| Item                          | Data                                                                                                                                                                                           |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AC's source interface address | VLANIF 100: 192.168.0.1/24                                                                                                                                                                     |
| AP region                     | AP1: 101, AP2: 102, AP3: 103                                                                                                                                                                   |
| WMM profile                   | Name: wp01                                                                                                                                                                                     |
| Radio profile                 | Name: rp01                                                                                                                                                                                     |
| Security profile              | <ul style="list-style-type: none"><li>● Name: sp01</li><li>● Security and authentication policy: WPA2+PSK</li><li>● Authentication key: 12345678</li><li>● Encryption mode: CCMP</li></ul>     |
| Traffic profile               | Name: tp01                                                                                                                                                                                     |
| Bridge profile                | <ul style="list-style-type: none"><li>● Name: bp01</li><li>● Bridge identifier: ChinaNet01</li></ul>                                                                                           |
| Service set                   | <ul style="list-style-type: none"><li>● Name: ss01</li><li>● SSID: ChinaSer01</li><li>● WLAN virtual interface: WLAN-ESS 1</li><li>● Service data forwarding mode: direct forwarding</li></ul> |
|                               | <ul style="list-style-type: none"><li>● Name: ss02</li><li>● SSID: ChinaSer02</li><li>● WLAN virtual interface: WLAN-ESS 2</li><li>● Service data forwarding mode: direct forwarding</li></ul> |
|                               | <ul style="list-style-type: none"><li>● Name: ss03</li><li>● SSID: ChinaSer03</li><li>● WLAN virtual interface: WLAN-ESS 3</li><li>● Service data forwarding mode: direct forwarding</li></ul> |
| Bridge whitelist              | Name: bw01                                                                                                                                                                                     |

 **NOTE**

Before performing the tasks in this example, ensure that the radios on AP1, AP2, and AP3 are not configured with service VAPs with WLAN IDs 13, 14, 15, and 16.

## Configuration Roadmap

1. Configure the connection between AC and AP1.
2. Set parameters for the AP radio and set the operation mode for the wireless bridge.
3. Configure the bridge profile and service set.
4. Configure the bridge whitelist.
5. Create VAPs.

6. Set parameters for AP wired interfaces.
7. Deliver parameters to APs.

## Procedure

### Step 1 Configure the connection between AC and AP1.

1. Set parameters for Switch and AC so that the Switch can transparently transmit data to the AC.

# Set the link type of GE1/0/0 on the Switch connected to AP1 to trunk and PVID to 100.

```
<Quidway> system-view
[Quidway] vlan batch 100 to 106
[Quidway] interface GigabitEthernet 1/0/0
[Quidway-GigabitEthernet1/0/0] port link-type trunk
[Quidway-GigabitEthernet1/0/0] port trunk pvid vlan 100
[Quidway-GigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 106
[Quidway-GigabitEthernet1/0/0] quit
```

# Configure the XGE interface of the Switch connected to the AC to transparently transmit service and management data.

```
[Quidway] interface XGigabitEthernet 1/0/0
[Quidway-XGigabitEthernet1/0/0] port link-type trunk
[Quidway-XGigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 106
```

# Configure the XGE interface of the AC connected to the Switch to transparently transmit service and management data.

```
<Quidway> system-view
[Quidway] sysname AC
[AC] vlan batch 100 to 106
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 106
[AC-XGigabitEthernet0/0/1] quit
```

2. Configure basic AC attributes.

# Configure the AC ID, carrier ID, and country code.

```
[AC] wlan ac-global ac id 1 carrier id ctc
[AC] wlan ac-global country-code cn
```

# Configure VLANIF interfaces, assign IP addresses to them for Layer 3 packet forwarding, and enable the DHCP server function on them.

An AP can set up a connection with an AC only after obtaining an IP address from the DHCP server. In this example, the AC functions as a DHCP server.

Configure an IP address pool on VLANIF 100 to assign IP addresses to APs, configure an IP address pool on VLANIF 101 to assign IP addresses to STAs in area A, configure an IP address pool on VLANIF 102 to assign IP addresses to STAs in area B, and configure an IP address pool on VLANIF 103 to assign IP addresses to STAs in area C.

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
```

```
[AC] interface vlanif 102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
[AC] interface vlanif 103
[AC-Vlanif102] ip address 192.168.3.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

# Configure the AC's source interface and WLAN-ESS virtual interface.

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
[AC-wlan-view] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 101
[AC-WLAN-ESS1] quit
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port link-type hybrid
[AC-WLAN-ESS2] port hybrid untagged vlan 102
[AC-WLAN-ESS2] quit
[AC] interface wlan-ess 3
[AC-WLAN-ESS3] port link-type hybrid
[AC-WLAN-ESS3] port hybrid untagged vlan 103
[AC-WLAN-ESS3] quit
```

3. Add an AP offline, configure the AP region, and set the authentication mode.

# Add an AP offline.

```
[AC-wlan-view] ap id 1 ap-type WA603SN mac 0025-9e12-6667
[AC-wlan-ap-1] quit
[AC-wlan-view] ap id 2 ap-type WA603SN mac 5489-9845-9573
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3 ap-type WA603SN mac 80fb-0689-81c3
[AC-wlan-ap-3] quit
```

# Set the AP authentication mode to no-auth.

If the AP authentication mode is set to no-auth, AP1 can go online automatically. After AP1 goes online, it is added to the default region and bound to the default AP profile, and its attributes are restored to default settings. The AP then enters the normal state. After AP2 and AP3 set up management WVLs, they go online in the same way.

```
[AC-wlan-view] ap-auth-mode no-auth
```

#### NOTE

Some AP models automatically enable the wireless bridge function after being powered on. These APs can also set up management WVLs automatically. For the APs that cannot automatically enable wireless bridge, you must manually enable it.

# Create AP regions 101, 102, and 103.

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id
102
[AC-wlan-ap-region-102] quit
[AC-wlan-view] ap-region id
103
[AC-wlan-ap-region-103] quit
```

# Add AP1 to AP region 101, AP2 to AP region 102, and AP3 to AP region 103.

```
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 101
[AC-wlan-ap-1] quit
```

```
[AC-wlan-view] ap id 2
[AC-wlan-ap-2] region-id 102
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3
[AC-wlan-ap-3] region-id 103
[AC-wlan-ap-3] quit
```

**Step 2** Set parameters for the AP radio and set the operation mode for the wireless bridge.

# Create the WMM profile **wp01** and use the default settings.

```
[AC-wlan-view] wmm-profile name wp01
[AC-wlan-wmm-prof-wp01] quit
```

# Create the radio profile **rp01**, use the default settings, and bind it to the WMM profile **wp01**.

```
[AC-wlan-view] radio-profile name rp01
[AC-wlan-radio-prof-rp01] wmm-profile name wp01
[AC-wlan-radio-prof-rp01] quit
```

# Bind the radio profile **rp01** to each AP radio and set the operation modes for the wireless bridges.

1. Bind **ap1\_radio0** (radio 0 on AP 1) to the radio profile **rp01** and set the bridge operation mode to root.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name rp01
Warning: Modify the Radio type may cause some parameters of Radio resume
default
t value, are you sure to continue?[Y/N]: y
[AC-wlan-radio-1/0] bridge enable mode root
[AC-wlan-radio-prof-rp01] quit
```

2. Bind **ap2\_radio0** to the radio profile **rp01** and set the bridge operation mode to middle.

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] radio-profile name rp01
Warning: Modify the Radio type may cause some parameters of Radio resume
default
t value, are you sure to continue?[Y/N]: y
[AC-wlan-radio-2/0] bridge enable mode middle
[AC-wlan-radio-prof-rp01] quit
```

3. Bind **ap3\_radio0** to the radio profile **rp01** and set the bridge operation mode to leaf.

```
[AC-wlan-view] ap 3 radio 0
[AC-wlan-radio-3/0] radio-profile name rp01
Warning: Modify the Radio type may cause some parameters of Radio resume
default
t value, are you sure to continue?[Y/N]: y
[AC-wlan-radio-3/0] bridge enable mode leaf
[AC-wlan-radio-prof-rp01] quit
```

**Step 3** Configure the bridge profile and service set.

# Create the security profile **sp01**, set security and authentication policy to WPA2-PSK, set the authentication key to 12345678, and set the encryption mode to CCMP.

```
[AC-wlan-view] security-profile name sp01
[AC-wlan-sec-prof-sp01] security-policy wpa2
[AC-wlan-sec-prof-sp01] wpa2 authentication-method psk pass-phrase 12345678
encryption-method ccmp
[AC-wlan-sec-prof-sp01] quit
```

# Create the traffic profile **tp01** and use the default settings.

```
[AC-wlan-view] traffic-profile name tp01
[AC-wlan-traffic-prof-tp01] quit
```

# Create a bridge profile with the name **bp01** and identifier **ChinaNet01**, and bind the bridge profile to the security protocol **sp01**.

```
[AC-wlan-view] bridge-profile name bp01
[AC-wlan-bridge-prof-bp01] bridge-name ChinaNet01
[AC-wlan-bridge-prof-bp01] vlan tagged 100 to 106
[AC-wlan-bridge-prof-bp01] security-profile name sp01
[AC-wlan-bridge-prof-bp01] quit
```

# Configure a service set.

1. # Create and configure a service set with the name **ss01** and SSID **ChinaSer01**.

```
[AC-wlan-view] service-set name ss01
[AC-wlan-service-set-ss01] traffic-profile name tp01
[AC-wlan-service-set-ss01] security-profile name sp01
[AC-wlan-service-set-ss01] ssid ChinaSer01
[AC-wlan-service-set-ss01] service-vlan 101
[AC-wlan-service-set-ss01] wlan-ess 1
[AC-wlan-service-set-ss01] forward-mode direct-forward
[AC-wlan-service-set-ss01] quit
```

2. # Create and configure a service set with the name **ss02** and SSID **ChinaSer02**.

```
[AC-wlan-view] service-set name ss02
[AC-wlan-service-set-ss02] traffic-profile name tp01
[AC-wlan-service-set-ss02] security-profile name sp01
[AC-wlan-service-set-ss02] ssid ChinaSer02
[AC-wlan-service-set-ss02] service-vlan 102
[AC-wlan-service-set-ss02] wlan-ess 2
[AC-wlan-service-set-ss02] forward-mode direct-forward
[AC-wlan-service-set-ss02] quit
```

3. # Create and configure a service set with the name **ss03** and SSID **ChinaSer03**.

```
[AC-wlan-view] service-set name ss03
[AC-wlan-service-set-ss03] traffic-profile name tp01
[AC-wlan-service-set-ss03] security-profile name sp01
[AC-wlan-service-set-ss03] ssid ChinaSer03
[AC-wlan-service-set-ss03] service-vlan 103
[AC-wlan-service-set-ss03] wlan-ess 3
[AC-wlan-service-set-ss03] forward-mode direct-forward
[AC-wlan-service-set-ss03] quit
```

#### Step 4 Configure the bridge whitelist.

# Create the bridge whitelist **bw01**.

```
[AC-wlan-view] bridge-whitelist name bw01
[AC-wlan-br-whitelist-bw01] peer ap mac 0025-9e12-6667
[AC-wlan-br-whitelist-bw01] peer ap mac 5489-9845-9573
[AC-wlan-br-whitelist-bw01] peer ap mac 80fb-0689-81c3
[AC-wlan-br-whitelist-bw01] quit
```

#### Step 5 Create VAPs.

# Create a bridge VAP and service VAP on ap1\_radio0 and bind the radio to the bridge whitelist.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] bridge-profile name bp01
[AC-wlan-radio-1/0] bridge-whitelist name bw01
[AC-wlan-radio-1/0] bridge whitelist enable
[AC-wlan-radio-1/0] service-set name ss01
[AC-wlan-radio-prof-rp01] quit
```

# Create a bridge VAP and service VAP on ap2\_radio0 and bind the radio to the bridge whitelist.

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] bridge-profile name bp01
[AC-wlan-radio-2/0] bridge-whitelist name bw01
[AC-wlan-radio-2/0] bridge whitelist enable
```

```
[AC-wlan-radio-2/0] service-set name ss02
[AC-wlan-radio-prof-rp01] quit
```

# Create a bridge VAP and service VAP on ap3\_radio0 and bind the radio to the bridge whitelist.

```
[AC-wlan-view] ap 3 radio 0
[AC-wlan-radio-3/0] bridge-profile name bp01
[AC-wlan-radio-3/0] bridge-whitelist name bw01
[AC-wlan-radio-3/0] bridge whitelist enable
[AC-wlan-radio-3/0] service-set name ss03
[AC-wlan-radio-prof-rp01] quit
```

### Step 6 Set parameters for the AP wired interface.

# Set parameters for the wired interface of AP1.

```
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] lineate-port mode root
[AC-wlan-ap-1] quit
```

# Set parameters for the wired interface of AP3.

```
[AC-wlan-view] ap id 3
[AC-wlan-ap-3] lineate-port pvid vlan 104
[AC-wlan-ap-3] lineate-port vlan tagged 105
[AC-wlan-ap-3] lineate-port vlan untagged 106
[AC-wlan-ap-3] lineate-port stp enable
[AC-wlan-ap-3] lineate-port mode endpoint
[AC-wlan-ap-3] lineate-port user-isolate enable
[AC-wlan-ap-3] quit
```

#### NOTE

After changing the operation mode of AP wired interfaces, reset the APs to make the configurations effective.

### Step 7 Deliver parameters to APs.

The AP parameters configured on the AC take effect only after they are delivered to the APs.

```
[AC-wlan-view] commit ap 1
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
[AC-wlan-view] commit ap 2
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
[AC-wlan-view] commit ap 3
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
```

----End

# 3 WLAN Security Configuration

---

## About This Chapter

This chapter describes how to configure WLAN security in the AC + fit AP networking mode.

### [3.1 WLAN Security Overview](#)

### [3.2 WLAN Security Features Supported by the SPU](#)

The SPU supports a variety of WLAN security features, including access security policy management, station (STA) blacklist and whitelist management, and user isolation.

### [3.3 Configuring an Access Security Policy](#)

By configuring an access security policy, you specify the authentication mode to use when users access WLAN devices according to the network plan.

### [3.4 Configuring the STA Blacklist and Whitelist](#)

By configuring the STA blacklist and whitelist, you can control STA access.

### [3.5 Configuring User Isolation](#)

The user isolation function prevents wireless users associated with the same AP from forwarding Layer 2 packets to each other. These users cannot communicate directly. Instead, user traffic is aggregated to gateways, facilitating user management.

### [3.6 Configuration Examples](#)

## 3.1 WLAN Security Overview

The wireless security feature provided by 802.11 authentication can defend against common network attacks. However, 802.11 authentication cannot fully protect networks containing sensitive data because a few hackers can still access WLANs. To prevent unauthorized user access, a security mechanism more secure than 802.11 authentication is required. Link authentication, WLAN service data security, and user access authentication are used to provide higher security.

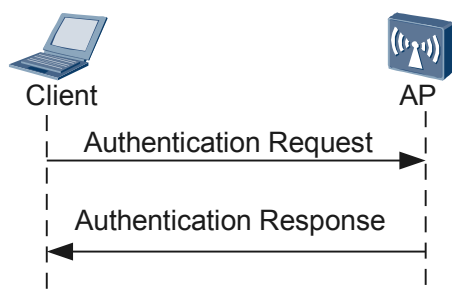
### Link Authentication

Open system authentication and shared key authentication are used for link authentication.

- Open system authentication

Open system authentication is the default and simplest authentication mode. Users do not need to be authenticated in this mode.

**Figure 3-1** Open system authentication



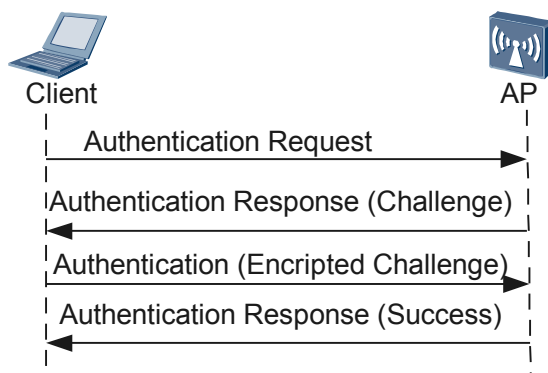
The open system authentication process is as follows:

1. A wireless client initiates an authentication request.
2. An access point (AP) confirms that the wireless client has passed link authentication and responds to the wireless client with an authentication success message.

- Shared key authentication

Shared key authentication requires a wireless client and an AP to be configured with the same shared key.

**Figure 3-2** Shared key authentication





The shared key authentication process is as follows:

1. A wireless client initiates an authentication request to an AP. The AP then generates a Challenge packet (a character string) and sends it to the wireless client.
2. The wireless client generates a new message based on the received character string, encrypts the message with a key, and then sends the message to the AP.
3. After receiving the message from the wireless client, the AP decrypts it with a key and then compares the decrypted character string with the original character string sent to the wireless client. If the two character strings are the same, the wireless client and AP have the same shared key and the wireless client passes shared key authentication. Otherwise, the wireless client fails to be authenticated.

## WLAN Service Data Security

Compared with wired networks, WLANs have data security risks. All the WLAN devices in an area share the same transmission medium, and any WLAN device can receive data from all the other WLAN devices. This makes WLAN access data vulnerable to attacks.

The 802.11 protocol is dedicated to addressing security threats on WLANs. In addition to authentication, it encrypts data packets and allows only specified devices to successfully decrypt the data packets. Other devices can receive data packets but fail to decrypt these packets because they lack the required key. This protects WLAN data.

Currently, the SPU supports RC4 encryption, Temporal Key Integrity Protocol (TKIP) encryption, and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption.

## User Access Authentication

Three types of user access authentication are used:

- Pre-shared key (PSK) authentication  
PSK authentication requires a wireless client and an AP to be configured with the same pre-shared key. If their pre-shared keys are the same, the wireless client passes PSK authentication; otherwise, the wireless client fails to be authenticated.
- 802.1x authentication  
The 802.1x protocol is a port-based network access control protocol. It authenticates and controls user devices connected to an interface on a WLAN access device. User devices connected to the interface can access WLAN resources only after they are authenticated.
- MAC address authentication  
MAC address authentication controls the network access authority of a user based on the access interface and MAC address of the user. The user does not need to install any client software. After detecting the MAC address of the user for the first time, a WLAN access device starts authenticating the user.

## 3.2 WLAN Security Features Supported by the SPU

The SPU supports a variety of WLAN security features, including access security policy management, station (STA) blacklist and whitelist management, and user isolation.

## Access Security Policy Management

Access security policy management allows you to configure an authentication mode for WLAN access users.

The SPU supports four access security policies: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WLAN Authentication and Privacy Infrastructure (WAPI).

## STA Blacklist and Whitelist Management

The SPU controls STA access by adding STAs to the blacklist or whitelist.

- After the blacklist function is enabled, a STA in the blacklist cannot be associated with an access point (AP) or access WLANs.
- After the whitelist function is enabled, a STA in the whitelist can be associated with an AP and access WLANs.

## User Isolation

The user isolation function prevents wireless users associated with the same AP from forwarding Layer 2 packets to each other, which prevents these users from communicating directly.

On the SPU, you can configure user isolation in a service set and configure port isolation on a WLAN-ESS interface to implement Layer 2 isolation between wireless users associated with the same AP.

# 3.3 Configuring an Access Security Policy

By configuring an access security policy, you specify the authentication mode to use when users access WLAN devices according to the network plan.

## Applicable Environment

WLAN channels are open to users, and malicious users can easily intercept, modify, and forward data of authorized users. The WLAN technology provides security policies to prevent unauthorized user access. Select a security policy based on the security level needed for your network.

- Wired Equivalent Privacy (WEP) is an old security policy and has security risks. It can be used in open scenarios that do not require high security, such as airports.
- Wi-Fi Protected Access (WPA) and WLAN Authentication and Privacy Infrastructure (WAPI) provide higher security for devices.

## Pre-configuration Tasks

Before configuring an access security policy, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC

## Data Preparation

To configure an access security policy, you need the following data.

| No. | Data                                                                                                                                                                                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Security profile name or security profile ID                                                                                                                                                                                                                                                      |
| 2   | WEP shared key and key ID                                                                                                                                                                                                                                                                         |
| 3   | WPA/WPA2 shared key                                                                                                                                                                                                                                                                               |
| 4   | <ul style="list-style-type: none"><li>● WAPI shared key if shared key authentication is used</li><li>● AC certificate file and private key file, certificate of the AC certificate issuer, ASU certificate file name, and ASU server's IP address if certificate authentication is used</li></ul> |
| 5   | (Optional) Interval for updating a base key (BK), BK lifetime percentage, time-based interval or packet count-based interval for updating an MBMS service key (MSK), number of retransmissions of MSK negotiation packets, and number of retransmissions of certificate authentication packets    |

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
wlan
```

The WLAN view is displayed.

### Step 3 Run:

```
security-profile { id profile-id | name profile-name } *
```

An access security profile is configured.

After an access security profile is configured, its default settings are:

- Open system authentication and empty key if WEP is used
- 802.1x+PEAP authentication and TKIP encryption if WPA1 is used
- 802.1x+PEAP authentication and CCMP encryption if WPA2 is used
- WAI authentication and WPI encryption if WAPI is used

### Step 4 Configure security policies.

- WEP open system authentication

#### 1. Run:


```
security-policy wep
```

The WEP security policy is configured.

#### 2. Run:

```
wep authentication-method open-system [data-encrypt]
```

WEP open system authentication is configured.

- WEP shared key authentication
  1. Run:  
`security-policy wep`  
The WEP security policy is configured.
  2. Run:  
`wep authentication-method share-key`  
WEP shared key authentication is configured.
  3. Run:  
`wep key { wep-40 | wep-104 } { pass-phrase | hex } key-id key-value`  
The WEP shared key is configured.  
If WEP-40 is used, the WEP shared key is 10 hexadecimal characters or 5 ASCII characters. If WEP-104 is used, the WEP shared key is 26 hexadecimal characters or 13 ASCII characters.
  4. Run:  
`wep default-key key-id`  
The WEP key ID is set.  
A maximum of four WEP keys can be configured, but only one WEP key is used in authentication or encryption. This command specifies which key to use.
- WPA/WPA2 authentication
  1. Run:  
`security-policy wpa`  
The WPA security policy is configured.
  2. Run:  
`{ wpa | wpa2 } authentication-method dot1x { peap | tls } encryption-method { tkip | ccmp }`  
The dot1x authentication and corresponding encryption mode are configured for the WPA/WPA2 policy.  
 **NOTE**  
If WPA/WPA2 dot1x authentication is configured, run the **dot1x-authentication enable** command on a WLAN-ESS interface.  
WPA authentication differs from WPA2 authentication in the protocol packet format.
  3. Run:  
`{ wpa | wpa2 } authentication-method psk { pass-phrase | hex } key encryption-method { tkip | ccmp }`  
The pre-shared key authentication and corresponding encryption mode are configured for the WPA/WPA2 security policy.
- WAPI authentication
  1. Run:  
`security-policy wapi`  
The WAPI security policy is configured.
  2. Run:  
`wapi authentication-method { certificate | psk { pass-phrase | hex } key }`  
The authentication mode is set for the WAPI security policy.  
WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, the shared key must be configured.

3. Run:  

```
wapi import certificate { ac | asu | issuer } file-name file_name
```

The AC certificate file, certificate of the AC certificate issuer, and ASU certificate file are imported.
4. Run:  

```
wapi import private-key file-name file_name
```

The AC private key file is imported.
5. Run:  

```
wapi asu ip ip-address
```

The ASU server's IP address is configured.  
If WAPI certificate authentication is configured, an AC will send the certificate to the ASU server at the configured IP address.
6. (Optional) Run the following commands to modify WAPI parameters:
  - Run:  

```
wapi { bk-threshold bk-threshold | bk-update-interval bk-interval }
```

The interval for updating a BK and the BK lifetime percentage are set.  
By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.
  - Run:  

```
wapi { msk-update-interval msk-interval | msk-update-packet msk-packet
| msk-retrans-count msk-count }
```

The interval for updating an MSK, number of packets that will trigger MSK update, and number of retransmissions of MSK negotiation packets are set.  
By default, the interval for updating an MSK is 86400s; the number of packets that will trigger MSK update is 10000; the number of retransmissions of MSK negotiation packets is 3.
  - Run:  

```
wapi cert-retrans-count cert-count
```

The number of retransmissions of certificate authentication packets is set.  
By default, the number of retransmissions is 3.
  - Run:  

```
wapi { usk | msk } key-update { disable | time-based | packet-based |
timepacket-based }
```

The unicast session key (USK) or MSK update mode is set.  
By default, USKs and MSKs are updated on the basis of time.

----End

## Checking the Configuration

Run the **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [ **detail** ] } command to view information about security profiles.

Check detailed information about a single security profile.

```
<Quidway> display security-profile id 0 detail
```

```

Profile name : lw
Profile ID : 0
Authentication : Share key
Encryption : WEP-40

```

```
Service-set ID SSID
0 100129796_9300
1 100129796_93002

WEP's configuration
Authentication : Share key
Encryption : WEP-40
Key 0 : *****
Key 1 : Empty
Key 2 : Empty
Key 3 : Empty
Default key ID : 0

WPA's configuration
Authentication : WPA 802.1x + PEAP
Encryption : TKIP

WPA2's configuration
Authentication : WPA2 802.1x + PEAP
Encryption : CCMP

WAPI's configuration
CA certificate filename : -
ASU certificate filename : -
AC certificate filename : -
AC private key filename : -
Authentication server IP : -
Authentication method : WAPI PSK
WAI timeout(s) : 60
BK update interval(s) : 43200
BK lifetime threshold(%) : 70
USK update interval(s) : 600
USK update packet(k) : 10
MSK update interval(s) : 86400
MSK update packet(k) : 10
Cert auth retrans count : 3
USK negotiate retrans count : 3
MSK negotiate retrans count : 3
USK update method : Time-based
MSK update method : Time-based

```

## 3.4 Configuring the STA Blacklist and Whitelist

By configuring the STA blacklist and whitelist, you can control STA access.

### Applicable Environment

To prevent some STAs from accessing a WLAN network, add them to the STA blacklist. To allow some STAs to access a WLAN, add them to the STA whitelist.

### Pre-configuration Tasks

Before configuring the STA blacklist and whitelist, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC

### Data Preparation

To configure the STA blacklist and whitelist, you need the following data.

| No. | Data                        |
|-----|-----------------------------|
| 1   | AP ID and STA's MAC address |

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
wlan
```

The WLAN view is displayed.

### Step 3 Configure the blacklist and whitelist.

- Configure the blacklist.

1. Run:

```
sta-access-mode ap ap-id { blacklist | whitelist | disable }
```

The STA access control mode is set to **blacklist**.

By default, the STA access control mode is **disable**.

2. Run:

```
sta-blacklist mac-address
```

The STA is added to the blacklist.

- Configure the whitelist.

1. Run:

```
sta-access-mode ap ap-id { blacklist | whitelist | disable }
```

The STA access control mode is set to **whitelist**.

By default, the STA access control mode is **disable**.

2. Run:

```
sta-whitelist mac-address
```

The STA is added to the whitelist.

----End

## Checking the Configuration

- Run the **display sta-access-mode ap ap-id** command to check the STA access control mode.

Check the STA access control mode.

```
<Quidway> display sta-access-mode ap 0
Station access control mode: disable
```

- Run the **display sta-blacklist** command to view the STA blacklist.

Check the STA blacklist.

```
<Quidway> display sta-blacklist
Station mac global black list
information:

```

```
 ID
 MAC

 0
0026-0000-90a1
 1
0026-0000-909f

```

```
Total number: 2
```

- Run the **display sta-whitelist** command to view the STA whitelist.

Check the STA whitelist.

```
<Quidway> display sta-whitelist
 Station mac global white list
information:
```

```
 ID
 MAC

 0 0025-9e26-
b9bd
 1 001e-907a-
b6a6
 2
0026-0000-90a1

```

```
Total number: 3
```

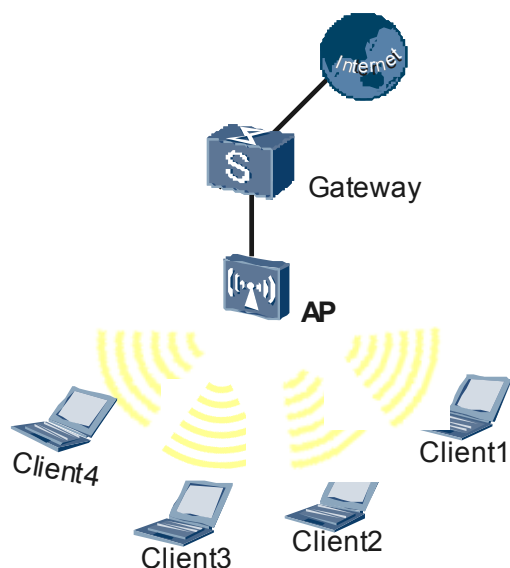
## 3.5 Configuring User Isolation

The user isolation function prevents wireless users associated with the same AP from forwarding Layer 2 packets to each other. These users cannot communicate directly. Instead, user traffic is aggregated to gateways, facilitating user management.

### Applicable Environment

In public places, carriers' networks, medium- and large-sized enterprises, and financial organizations, users may need to access the Internet using the wireless technology. If accurate and reliable user authentication is not performed, unauthorized users are able to use network resources, consuming bandwidth. This lowers the service quality of authorized users and brings unacceptable loss to wireless access service providers. Layer 2 wireless user isolation, together with IEEE802.11i, RADIUS user authentication, and user accounting can secure users.



**Figure 3-3** User isolation networking

As shown in [Figure 3-3](#), after user isolation is configured, clients 1 through 4 cannot communicate directly.

## Pre-configuration Tasks

Before configuring user isolation, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC

## Data Preparation

To configure user isolation, you need the following data.

| No. | Data                                       |
|-----|--------------------------------------------|
| 1   | Service set profile name or service set ID |
| 2   | (Optional) WLAN-ESS interface number       |

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Configure user isolation.

- If data is forwarded between the AP and AC through a common data link (direct forwarding), configure user isolation in a service set.
  1. Run:  

```
service-set { name service-set-name | id service-set-id } *
```

A service set is configured.
  2. Run:  

```
user-isolate
```

User isolation is configured.
- If data is forwarded between the AP and AC through a tunnel, configure user isolation in a service set and on a WLAN-ESS interface.
  1. Run:  

```
service-set { name service-set-name | id service-set-id } *
```

A service set is configured.
  2. Run:  

```
user-isolate
```

User isolation is configured.
  3. Run:  

```
quit
```

Return to the system view.
  4. Run:  

```
interface wlan-ess wlan-ess-number
```

The WLAN-ESS interface view is displayed.
  5. Run:  

```
port-isolate enable
```

Port isolation is enabled.

----End

## Checking the Configuration

Run the **display service-set { id service-set-id | name service-set-name }** command to check whether user isolation is enabled in service sets.

## 3.6 Configuration Examples

### 3.6.1 Example for Configuring Security Policies

#### Networking Requirements

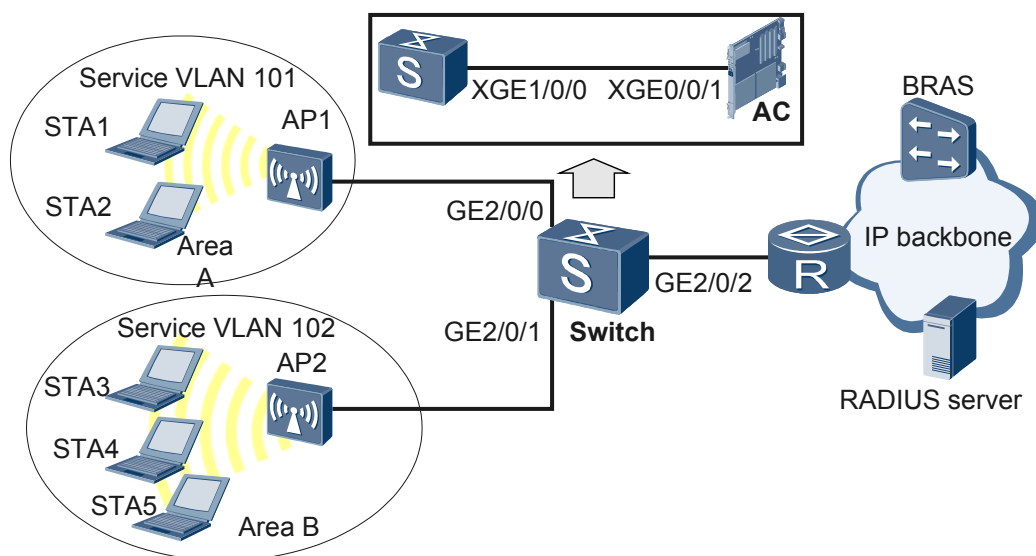
As shown in [Figure 3-4](#), the Switch functions as an AC; AP1 and AP2 provide WLAN services for access users. Five WLANs are available for the users, which provide different security policies. The requirements are:

- Open system authentication is used on the WLAN with the SSID huawei-1.

- Shared key authentication and WEP-40 encryption are used on the WLAN with the SSID huawei-2.
- WPA1 authentication and TKIP encryption are used on the WLAN with the SSID huawei-3.
- WPA2 authentication and CCMP encryption are used on the WLAN with the SSID huawei-4.
- WAPI authentication is used on the WLAN with the SSID huawei-5.

Before connecting to the Internet, STA3 and STA4 must be authenticated by the RADIUS server at 10.10.10.100. STA5 must be authenticated in WAPI mode by the ASU server at 10.10.10.1.

**Figure 3-4** Networking diagram of security policy configurations



**Table 3-1** Data plan

| Item              | Data                                                                                                                                                                                                                                         |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security policies | <ul style="list-style-type: none"> <li>● Security profile: security-1</li> <li>● SSID: huawei-1</li> <li>● Authentication mode: WEP open system authentication</li> </ul>                                                                    |
|                   | <ul style="list-style-type: none"> <li>● Security profile: security-2</li> <li>● SSID: huawei-2</li> <li>● Authentication mode: WEP shared key authentication</li> <li>● Encryption mode: WEP-40 encryption<br/>Key phrase: 12345</li> </ul> |
|                   | <ul style="list-style-type: none"> <li>● Security profile: security-3</li> <li>● SSID: huawei-3</li> <li>● Authentication mode: WPA1 authentication (802.1x +PEAP)</li> <li>● Encryption mode: TKIP encryption</li> </ul>                    |

| Item                       | Data                                                                                                                                                                                                                 |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <ul style="list-style-type: none"><li>● Security profile: security-4</li><li>● SSID: huawei-4</li><li>● Authentication mode: WPA2 authentication (802.1x +PEAP)</li><li>● Encryption mode: CCMP encryption</li></ul> |
|                            | <ul style="list-style-type: none"><li>● Security profile: security-5</li><li>● SSID: huawei-5</li><li>● Authentication mode: WAPI authentication (certificate authentication)</li></ul>                              |
| Radio profile              | radio-1 with the default configuration                                                                                                                                                                               |
| ASU server's IP address    | 10.10.10.1                                                                                                                                                                                                           |
| RADIUS server's IP address | 10.10.10.100                                                                                                                                                                                                         |

## Prerequisite

- There are reachable routes from the AC to ASU server and RADIUS server.
- Before configuring the policies of security-5, the AC certificate huawei-ac.cer, ASU server certificate huawei-asu.cer, Issuer certificate huawei-asu.cer, and AC private key certificate huawei-ac.cer have been stored on the AC.

## Configuration Roadmap

The configuration roadmap is as follows:

1. Create security profiles and configure security policies so that STAs access different WLANs by using different security policies.
2. Create service sets, bind security profiles to them, and specify SSIDs for them.
3. Create virtual APs (VAPs) and deliver VAP parameters so that STAs access different WLANs by using different security policies.

### NOTE

- Steps 1 to 3 are the same as the steps in WLAN service configuration. For details, see [1.9.1 Example for Configuring the WLAN Service](#).
- For security-3, WPA authentication must be used and 802.1x mode and encryption mode must be enabled.
- For security-4, WPA2 authentication must be used and 802.1x mode and encryption mode must be enabled.

## Procedure

**Step 1** Configure the Switch and the AC to enable APs to communicate with the AC. The configuration procedure is not provided here.

**Step 2** Configure basic AC attributes. The configuration procedure is not provided here.

**Step 3** Configure APs and enable them to go online. The configuration procedure is not provided here.

**Step 4** Configure radios for APs.

# Create a WMM profile named **wmm** and retain the default parameter settings.

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

# Create a radio profile named **radio** and bind the WMM profile **wmm** to it.

```
[AC-wlan-view] radio-profile name radio
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm
[AC-wlan-radio-prof-radio-1] quit
```

# Bind the radio profile **radio** to radios of AP1 and AP2.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-0/0] radio-profile name radio
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-1/0] radio-profile name radio
[AC-wlan-radio-1/0] quit
```

**Step 5** Configure the RADIUS server, AAA scheme, and domain name.

```
[AC] radius-server template peap.radius.com
[AC-radius-peap.radius.com] radius-server authentication 10.137.146.163 1812
[AC-radius-peap.radius.com] radius-server accounting 10.137.146.163 1813
[AC-radius-peap.radius.com] radius-server shared-key simple huawei
[AC-radius-peap.radius.com] quit
[AC] aaa
[AC-aaa] accounting-scheme radius
[AC-aaa-authen-radius] authentication-mode radius
[AC-aaa-authen-radius] quit
[AC-aaa] authentication-scheme radius
[AC-aaa-accounting-radius] accounting-mode radius
[AC-aaa-accounting-radius] quit
[AC-aaa] domain peap.radius.com
[AC-aaa-domain-peap.radius.com] authentication-scheme radius
[AC-aaa-domain-peap.radius.com] accounting-scheme radius
[AC-aaa-domain-peap.radius.com] radius-server peap.radius.com
[AC-aaa-domain-peap.radius.com] quit
```

**Step 6** Configure WLAN-ESS interfaces. Enable 802.1x authentication on WLAN-ESS 1.

```
[AC] dot1x enable
[AC] interface wlan-ess 0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid pvid vlan
101
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid pvid vlan 102
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] dot1x-authentication enable
[AC-WLAN-ESS1] dot1x authentication-method eap
[AC-WLAN-ESS1] quit
```

**Step 7** Create security profiles: security-1, security-2, security-3, security-4, and security-5.

```
<Quidway> system-view
[Quidway] sysname AC
[AC] wlan
[AC-wlan-view] security-profile name security-1
[AC-wlan-sec-prof-security-1] quit
[AC-wlan-view] security-profile name security-2
[AC-wlan-sec-prof-security-2] quit
```

```
[AC-wlan-view] security-profile name security-3
[AC-wlan-sec-prof-security-3] quit
[AC-wlan-view] security-profile name security-4
[AC-wlan-sec-prof-security-4] quit
[AC-wlan-view] security-profile name security-5
[AC-wlan-sec-prof-security-5] quit
```

### Step 8 Configure security profiles for WLAN users.

- Configure a security policy for security profile **security-1**.

# Configure WEP open system authentication.

```
[AC-wlan-view] security-profile name security-1
[AC-wlan-sec-prof-security-1] wep authentication-method open-system
[AC-wlan-sec-prof-security-1] security-policy wep
[AC-wlan-sec-prof-security-1] quit
```

- Configure a security policy for security profile **security-2**.

# Configure WEP shared key authentication, WEP-40 encryption, and key phrase 12345.

```
[AC-wlan-view] security-profile name security-2
[AC-wlan-sec-prof-security-2] wep authentication-method share-key
[AC-wlan-sec-prof-security-2] wep key wep-40 pass-phrase 0 12345
[AC-wlan-sec-prof-security-2] wep default-key 0
[AC-wlan-sec-prof-security-2] security-policy wep
[AC-wlan-sec-prof-security-2] quit
```

- Configure a security policy for security profile **security-3**.

# Configure 802.1x+PEAP for WPA1 authentication and configure TKIP encryption.

```
[AC-wlan-view] security-profile name security-3
[AC-wlan-sec-prof-security-3] wpa authentication-method dot1x peap encryption-
method tkip
[AC-wlan-sec-prof-security-3] security-policy wpa
[AC-wlan-sec-prof-security-3] quit
```

- Configure a security policy for security profile **security-4**.

# Configure 802.1x+PEAP for WPA2 authentication and configure CCMP encryption.

```
[AC-wlan-view] security-profile name security-4
[AC-wlan-sec-prof-security-4] wpa2 authentication-method dot1x peap encryption-
method ccmp
[AC-wlan-sec-prof-security-4] security-policy wpa2
[AC-wlan-sec-prof-security-4] quit
```

- Configure a security policy for security profile **security-5**.

# Configure certificate authentication for WAPI authentication.

```
[AC-wlan-view] security-profile name security-5
[AC-wlan-sec-prof-security-5] wapi authentication-method certificate
```

# Configure an ASU server's IP address 10.10.10.1, AC certificate file **huawei-ac.cer**, ASU certificate file **huawei-asu.cer**, issuer certificate file **huawei-asu.cer**, and AC private key certificate file **huawei-ac.cer**.

```
[Quidway-wlan-sec-prof-security-5] wapi asu ip 10.10.10.1
[Quidway-wlan-sec-prof-security-5] wapi import certificate ac file-name flash:/
huawei-ac.cer
[Quidway-wlan-sec-prof-security-5] wapi import certificate asu file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-security-5] wapi import certificate issuer file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-security-5] wapi import private-key file-name flash:/
huawei-ac.cer
[Quidway-wlan-sec-prof-security-5] security-policy wapi
[Quidway-wlan-sec-prof-security-5] quit
```

### Step 9 Create service sets, create VAPs, and deliver VAP parameters.

- # Create service set **ss-1**, specify SSID **huawei-1** for it, bind traffic profile **ctc** and security profile **security-1** to it, and deliver VAP parameters to radio 0 of AP1.

```
[AC-wlan-view] traffic-profile name ctc
[AC-wlan-traffic-prof-ctc] quit
[AC-wlan-view] service-set name ss-1
[AC-wlan-service-set-ss-1] ssid huawei-1
[AC-wlan-service-set-ss-1] traffic-profile name ctc
[AC-wlan-service-set-ss-1] security-profile name security-1
[AC-wlan-service-set-ss-1] service-vlan 101
[AC-wlan-service-set-ss-1] wlan-ess 0
[AC-wlan-service-set-ss-1] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name ss-1
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```

- # Create service set **ss-2**, specify SSID **huawei-2** for it, bind traffic profile **ctc** and security profile **security-2** to it, and deliver VAP parameters to radio 0 of AP1.

```
[AC-wlan-view] service-set name ss-2
[AC-wlan-service-set-ss-2] ssid huawei-2
[AC-wlan-service-set-ss-2] traffic-profile name ctc
[AC-wlan-service-set-ss-2] security-profile name security-2
[AC-wlan-service-set-ss-2] service-vlan 101
[AC-wlan-service-set-ss-2] wlan-ess 0
[AC-wlan-service-set-ss-2] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name ss-2
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```

- # Create service set **ss-3**, specify SSID **huawei-3** for it, bind traffic profile **ctc** and security profile **security-3** to it, and deliver VAP parameters to radio 0 of AP2.

```
[AC-wlan-view] service-set name ss-3
[AC-wlan-service-set-ss-3] ssid huawei-3
[AC-wlan-service-set-ss-3] traffic-profile name ctc
[AC-wlan-service-set-ss-3] security-profile name security-3
[AC-wlan-service-set-ss-3] service-vlan 102
[AC-wlan-service-set-ss-3] wlan-ess 1
[AC-wlan-service-set-ss-3] quit
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name ss-3
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

- # Create service set **ss-4**, specify SSID **huawei-4** for it, bind traffic profile **ctc** and security profile **security-4** to it, and deliver VAP parameters to radio 0 of AP2.

```
[AC-wlan-view] service-set name ss-4
[AC-wlan-service-set-ss-4] ssid huawei-4
[AC-wlan-service-set-ss-4] traffic-profile name ctc
[AC-wlan-service-set-ss-4] security-profile name security-4
[AC-wlan-service-set-ss-4] service-vlan 102
[AC-wlan-service-set-ss-4] wlan-ess 1
[AC-wlan-service-set-ss-4] quit
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name ss-4
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

- # Create service set **ss-5**, specify SSID **huawei-5** for it, bind traffic profile **ctc** and security profile **security-5** to it, and deliver VAP parameters to radio 0 of AP1.

```
[AC-wlan-view] service-set name ss-5
[AC-wlan-service-set-ss-5] ssid huawei-5
[AC-wlan-service-set-ss-5] traffic-profile name ctc
[AC-wlan-service-set-ss-5] security-profile name security-5
[AC-wlan-service-set-ss-5] service-vlan 101
[AC-wlan-service-set-ss-5] wlan-ess 0
[AC-wlan-service-set-ss-5] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-2/0] service-set name ss-5
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 1
```

**Step 10** Verify the configuration.

Five WLANs with SSIDs huawei-1, huawei-2, huawei-3, huawei-4, and huawei-5 are available for access users of AP1 and AP2.

- On the WLAN with the SSID huawei-1, users can use the WLAN service without being authenticated.
- On the WLAN with the SSID huawei-2, users can use the WLAN service only when they have the shared key.
- On the WLAN with the SSID huawei-3 or huawei-4, users can use the WLAN service only when they pass 802.1x authentication.
- On the WLAN with the SSID huawei-5, users can use the WLAN service only when they have the matching certificate.

---End

## Configuration Files

```
#
 sysname AC
#
 vlan batch 100 to 102
#
 wlan ac-global carrier id ctc ac id 1
#
 dhcp enable
#
 dot1x enable
#
 radius-server template
 peap.radius.com
 radius-server shared-key simple huawei
 radius-server authentication 10.10.10.100 1812
 radius-server accounting 10.10.10.100 1813
#
 aaa
 authentication-scheme radius
 authentication-mode radius
 accounting-scheme radius
 accounting-mode
 radius

 domain
 peap.radius.com
 authentication-scheme radius
 accounting-scheme radius
 radius-server
 peap.radius.com

#

 interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
 interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
 interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select
 interface
#
```



```
interface WLAN-ESS0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#

interface Wlan-Ess1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
 dot1x-authentication enable
 dot1x authentication-method
 eap

#
interface XGigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 to
 102
#
wlan
 wlan ac source interface vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 1 type-id 6 mac 5489-9849-8194 sn AB36014894
 region-id 101
 ap id 2 type-id 6 mac 5489-9849-8193 sn AB36014893
 region-id 102
 wmm-profile name wmm id 0
 traffic-profile name ctc id 1
 security-profile name security-1 id 0
 security-profile name security-2 id 1
 wep authentication-method share-key
 wep key wep-40 pass-phrase 0 12345
 security-profile name security-3 id 2
 security-policy wpa
 security-profile name security-4 id 3
 security-policy wpa2
 security-profile name security-5 id 4
 security-policy wapi
 wapi asu ip 10.10.10.1
 wapi import certificate ac file-name flash:/huawei-ac.cer
 wapi import certificate asu file-name flash:/huawei-asu.cer
 wapi import certificate issuer file-name flash:/huawei-issuer.cer
 wapi import private-key file-name flash:/huawei-ac.cer
 service-set name ss-1 id 0
 wlan-ess 0
 ssid huawei-1
 traffic-profile id 1
 security-profile id 1
 service-vlan 101
 service-set name ss-2 id 1
 wlan-ess 0
 ssid huwei-2
 traffic-profile id 1
 security-profile id 2
 service-vlan 102
 service-set name ss-3 id 2
 wlan-ess 1
 ssid huawei-3
 traffic-profile id 1
 security-profile id 3
 service-vlan 102
 service-set name ss-4 id 3
 wlan-ess 1
 ssid huawei-4
 traffic-profile id 1
 security-profile id 4
 service-vlan 102
```

```
service-set name ss-5 id 4
wlan-ess 0
ssid huawei-5
traffic-profile id 1
security-profile id 5
service-vlan 102
radio-profile name radio id 2
wmm-profile id 0
ap 1 radio 0
radio-profile name radio
service-set id 1 wlan 1
service-set id 2 wlan 1
service-set id 5 wlan 1
ap 2 radio 0
radio-profile name radio
service-set id 3 wlan 2
service-set id 4 wlan 2
```

# 4 WLAN QoS Configuration

---

## About This Chapter

This chapter describes how to configure the QoS service in the AC + fit AP networking mode.

### [4.1 WLAN QoS Overview](#)

The WLAN QoS feature provides services of different qualities for WLAN users.

### [4.2 WLAN QoS Features Supported by the SPU](#)

The SPU supports radio QoS policy management, VAP QoS policy management, and user priority and CAR management.

### [4.3 Configuring a Radio QoS Policy](#)

A radio QoS policy controls an AP's capability to compete for channels and determines the quality of services provided for the AP.

### [4.4 Configuring a VAP QoS Policy](#)

To apply the priority mapping and traffic suppression functions to a virtual AP (VAP), create a traffic profile and bind the traffic profile to a service set.

### [4.5 Configuring the User Priority and CAR](#)

You can control QoS of WLAN services by configuring user profiles, user priorities, and committed access rate (CAR).

### [4.6 Configuring the User Priority and CAR in a QoS Profile](#)

You can control QoS of WLAN services by configuring user priorities and committed access rate (CAR) in a QoS profile.

### [4.7 Configuration Examples](#)

## 4.1 WLAN QoS Overview

The WLAN QoS feature provides services of different qualities for WLAN users.

An 802.11 network provides the competition-based wireless access service. Different applications have different requirements for networks; however, traditional networks cannot provide access services of different qualities for different applications.

IEEE 802.11e defines the QoS feature for the 802.11-based WLAN system. The Wi-Fi Alliance defines the Wi-Fi Multimedia (WMM) standard for communication between QoS-supported devices of different WLAN vendors. WMM enables a WLAN network to provide QoS features.

### WMM

WMM provides QoS features for 802.11 networks and enables high-priority packets to be sent first. This provides better quality for voice and video services on WLANs.

### EDCA

Enhanced Distributed Channel Access (EDCA) is a channel preemption mechanism defined by WMM, enabling high-priority packets to be sent first and allocated more bandwidth.

### AC

WMM prioritizes queues of four access categories (ACs) in descending order: AC-voice (AC-VO), AC-video (AC-VI), AC-best effort (AC-BE), and AC-background (AC-BK). This ensures that packets in a high-priority queue have greater capabilities in channel preemption.

## 4.2 WLAN QoS Features Supported by the SPU

The SPU supports radio QoS policy management, VAP QoS policy management, and user priority and CAR management.

### Radio QoS Policy Management

In the 802.11 protocol, the distributed coordination function (DCF) defines the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) access mechanism for APs and STAs. Before occupying a channel to send packets, APs or STAs monitor the channel. If the channel idle time is longer than or equal to the arbitration inter frame spacing number (AIFSN), each AP or STA selects a random backoff time between exponent form of minimum contention window (ECWmin) and exponent form of maximum contention window (ECWmax). The first AP or STA whose backoff timer expires occupies the channel and starts to send packets over the channel.

WMM provides four AC queues: AC-VO for voice service flows, AC-VI for video service flows, AC-BE for best effort flows, and AC-BK for common data flows. Packets in a high-priority AC queue have greater capabilities in channel preemption. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of queues in channel preemption.

EDCA parameters are as follows:

- AIFSN: determines the channel idle time. A greater AIFSN value indicates a longer channel idle time.
- ECWmin and ECWmax: determine the average backoff time. A larger value indicates a longer average backoff time.
- Transmission opportunity limit (TXOPLimit): determines the maximum duration in which an AP or a STA can occupy a channel. A greater TXOPLimit value indicates a longer duration. If this parameter is set to 0, an AP or a STA can send only one packet each time it occupies a channel.
- ACK policy: determines whether to send an ACK packet to confirm the receiving of a unicast packet. In normal ACK mode, the receiver sends an ACK packet to confirm the receiving of a unicast packet from the sender. In no ACK mode, if the communication quality is good and interference is low, no ACK packet is sent to confirm the receiving of a unicast packet from the sender. This prevents packet retransmission and improves the transmission efficiency.

EDCA parameters and other WMM parameters are managed in a WMM profile. After a WMM profile is created, it is bound to a radio profile and then applied to a radio together with the radio profile.

## VAP QoS Policy Management

When an AP receives 802.11 packets from a STA, it converts the packets into 802.3 packets. The AP transmits the 802.3 packets to an AC directly or over a tunnel. After receiving the 802.3 packets, the AC forwards the packets to a network-side device. During packet transmission, the AC schedules the 802.3 packets based on the 802.1p priorities in the packets or tunnel priorities.

When the AC receives 802.3 packets from the network-side device, it forwards the 802.3 packets to the AP directly or over a tunnel. When being transmitted over a tunnel, the packets can be scheduled based on tunnel priorities. After receiving the 802.3 packets, the AP converts the packets into 802.11 packets and schedules the 802.11 packets into different AC queues based on user priorities before sending them to the STA.

VAP QoS policies are managed by using a traffic profile. [Table 4-1](#) lists parameters in a traffic profile.

**Table 4-1** Parameters in a traffic profile

| Parameter                        | Description                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client/VAP upstream rate limit   | Limits the upstream rate of a STA or VAP.                                                                                                                          |
| 802.1p priority in 802.3 packets | Specifies the 802.1p priority in 802.3 packets received by an AP. The 802.1p priority can be set or mapped from the user priority in 802.11 packets sent by a STA. |
| Upstream tunnel priority         | Specifies the outer tunnel priority in 802.3 packets received by an AP. The upstream tunnel priority can be set or mapped from the inner priority.                 |
| Priority in 802.11 packets       | Specifies the priority of 802.11 packets sent by an AP.                                                                                                            |

After a traffic profile is created, it is bound to a service set and applied to the corresponding VAP along with the service set.

## 4.3 Configuring a Radio QoS Policy

A radio QoS policy controls an AP's capability to compete for channels and determines the quality of services provided for the AP.

### Applicable Environment

A STA communicates with an AP by sending radio signals over a channel. To provide differentiated services for wireless users, configure a Wi-Fi multimedia (WMM) profile.

### Pre-configuration Tasks

Before configuring a radio QoS policy, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC

### Data Preparation

To configure a radio QoS policy, you need the following data.

| No. | Data                                                                                                                                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | WMM profile name or WMM profile ID                                                                                                                                                                                                                |
| 2   | (Optional) WMM EDCA parameters for STAs: arbitration inter frame spacing number (AIFSN), exponent form of minimum contention window (ECWmin), exponent form of maximum contention window (ECWmax), and transmission opportunity limit (TXOPLimit) |
| 3   | (Optional) WMM EDCA parameters for APs: AIFSN, ECWmin, ECWmax, and TXOPLimit                                                                                                                                                                      |

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```

The WLAN view is displayed.

**Step 3** Run:

```
wmm-profile { id profile-id | name profile-name } *
```

A WMM profile is configured.

After a WMM profile is created, parameters in the profile use default values. To view the configuration of a WMM profile, run the **display wmm-profile { all | id profile-id | name profile-name }** command.

The following information shows the default configuration of the WMM profile **wp**.

```
[Quidway-wlan-view] display wmm-profile name wp
Profile ID : 2
Profile name : wp
WMM switch : enable
Client EDCA parameters:

 ECWmax ECWmin AIFSN TXOPLimit
AC_VO 3 2 2 47
AC_VI 4 3 2 94
AC_BE 10 4 3 0
AC_BK 10 4 7 0

AP EDCA parameters:

 ECWmax ECWmin AIFSN TXOPLimit Ack-Policy
AC_VO 3 2 1 47 normal
AC_VI 4 3 1 94 normal
AC_BE 6 4 3 0 normal
AC_BK 10 4 7 0 normal

```

 **NOTE**

A STA communicates with an AP by sending radio signals over a channel. Four queues are provided for radio packets. Packets in different queues have different opportunities to obtain transmission channels so that differentiated services can be provided for radio packets.

The queues are AC\_VO (voice queue), AC\_VI (video queue), AC\_BE (best effort queue), and AC\_BK (background queue) in descending order of priority.

You can change the priorities of the queues by modifying the Enhanced Distributed Channel Access (EDCA) parameters, including the AIFSN, ECWmin, ECWmax, TXOPLimit, and ACK policy:

- **AIFSN**: determines the channel idle time. A greater AIFSN value indicates a longer channel idle time. Different AIFSNs can be configured for ACs.
- **ECWmin and ECWmax**: ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They determine the average backoff time. A larger value indicates a longer average backoff time.
- **TXOPLimit**: determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. If this parameter is set to 0, a STA can send only one packet every time it occupies a channel.
- **ACK policy**: determines whether the packet receiver acknowledges received packets. Two policies are available: normal ACK and no ACK.

Before occupying a channel to send packets, STAs monitor the channel. If the channel idle time is longer than or equal to the AIFSN, each STA selects a random backoff time between ECWmin and ECWmax. The STA whose backoff timer expires the first occupies the channel and starts to send packets over the channel.

**Step 4** (Optional) Run:

```
wmm edca client { ac-vo | ac-vi | ac-be | ac-bk } { aifsn aifsn-value | ecw ecwmin
ecwmin-value ecwmax ecwmax-value | txoplmit txoplmit-value } *
```

The EDCA parameters are configured for the four WMM queues of a STA.

**Step 5** (Optional) Run:

```
wmm edca ap { ac-vo | ac-vi | ac-be | ac-bk } { aifsn aifsn-value | ecw ecwmin
ecwmin-value ecwmax ecwmax-value | txoplmit txoplmit-value | ack-policy { normal
| noack } } *
```

The EDCA parameters are configured for the four WMM queues of an AP.

---End

## Checking the Configuration

Run the **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to view the configuration of a WMM profile.

## 4.4 Configuring a VAP QoS Policy

To apply the priority mapping and traffic suppression functions to a virtual AP (VAP), create a traffic profile and bind the traffic profile to a service set.

### Applicable Environment

To forward an 802.11 packet sent from a STA to an Ethernet network, an AP converts the 802.11 packet into an 802.3 packet. The AP may retain the packet priority or change the packet priority according to the VAP configuration to provide differentiated QoS services.

### Pre-configuration Tasks

Before configuring a VAP QoS policy, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC

### Data Preparation

To configure a VAP QoS policy, you need the following data.

| No. | Data                                                                                                                 |
|-----|----------------------------------------------------------------------------------------------------------------------|
| 1   | Traffic profile name or traffic profile ID                                                                           |
| 2   | (Optional) Mappings from user priorities to 802.1p priorities and mappings from 802.1p priorities to user priorities |
| 3   | (Optional) Packet rate limit                                                                                         |
| 4   | (Optional) Tunnel priority value                                                                                     |

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
wlan
```



The WLAN view is displayed.

**Step 3** Run:

```
traffic-profile { name profile-name | id profile-id } *
```

A traffic profile is configured.

After a traffic profile is created, parameters in the profile use default values. To view the configuration of a traffic profile, run the **display traffic-profile { all | id profile-id | name profile-name }** command.

View attributes of the traffic profile **traffic-profile-1**.

```
[Quidway-wlan-view] display traffic-profile name traffic-
profile-1
Profile ID : 3
Profile name : traffic-profile-1
Client Limit Rate : 4294967295 Kbps (up)
 : 4294967295 Kbps (down)
VAP Limit Rate : 4294967295 Kbps (up)
 : 4294967295 Kbps (down)
802.1p Mapping Mode: mapping

User-priority 802.1p
0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7

802.1p to User-priority Mapping List:

802.1p User-priority
0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7

Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)

ToS(inner) ToS(outer)
0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7

```

 **NOTE**

When receiving an 802.3 packet from the Ethernet network, the AP converts the 802.3 packet into an 802.11 packet and forwards it to the STA. The user priority in the packet is determined by DSCP-CoS mapping or set in a traffic classifier.

**Step 4** (Optional) Run:

```
8021p { designate value | up-mapping value0 value1 value2 value3 value4 value5
value6 value7 }
```

The 802.1p priority of 802.3 packets sent from an AP to an AC is set.

An AP terminates 802.11 packets sent from STAs, converts the 802.11 packets into 802.3 packets, and sends the 802.3 packets to an AC. To ensure the service quality for 802.3 packets, set packet priorities to ensure proper scheduling.

**Step 5** (Optional) Run:

```
8021p-map-up value0 value1 value2 value3 value4 value5 value6 value7
```

The mappings from 802.1p priorities to user priorities are set.

**Step 6** (Optional) Run:

```
rate-limit { client | vap } { up | down } ratelimit-value
```

The rate limit for upstream or downstream packets is set for a single STA or all STAs associated with a VAP.

**Step 7** (Optional) Run either of the following commands to set designated priorities or priority mappings for upstream tunnels:

- **tunnel-priority up designate** { tos | 8021p } priority-value
- **tunnel-priority up map** { tos-tos | tos-8021p | 8021p-tos | 8021p-8021p } value0 value1 value2 value3 value4 value5 value6 value7

---End

## Checking the Configuration

Run the **display traffic-profile** { all | id profile-id | name profile-name } command to view the configuration of a traffic profile.

# 4.5 Configuring the User Priority and CAR

You can control QoS of WLAN services by configuring user profiles, user priorities, and committed access rate (CAR).

## Applicable Environment

An AP terminates 802.11 packets sent from STAs, converts the 802.11 packets into 802.3 packets, and sends the 802.3 packets to an AC. To ensure the service quality for 802.3 packets, set user priorities and CAR for flow control.

## Pre-configuration Tasks

Before configuring the user priority and CAR, complete the following tasks:

- Configuring basic AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting an AP to an AC
- Configuring a QoS CAR profile

## Data Preparation

To configure the user priority and CAR, you need the following data.

| No. | Data                                 |
|-----|--------------------------------------|
| 1   | User profile name or user profile ID |
| 2   | User priority                        |
| 3   | QoS CAR profile name                 |

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
wlan
```

The WLAN view is displayed.

### Step 3 Run:

```
user-profile { name profile-name | id profile-id } *
```

A user profile is configured.

### Step 4 Run:

```
user-priority { downstream | upstream } user-priority
```

The priority is set for user packets reaching the AC.

### Step 5 Run:

```
qos car { inbound | outbound } car-name
```

A QoS CAR profile is specified for user packets.

---End

## Checking the Configuration

Run the **display user-profile { all | id profile-id | name profile-name }** command to view user profile information.

View information about all user profiles.

```
<Quidway> display user-profile all

ID Name

0 up
1 kk

Total: 2
```

View information about a specified user profile.

```
<Quidway> display user-profile name p1
Profile name : p1
Profile ID : 0
QoS CAR inbound CAR-profile : -
QoS CAR outbound CAR-profile : -
```

```
User-priority upstream : -
User-priority downstream : -
```

## 4.6 Configuring the User Priority and CAR in a QoS Profile

You can control QoS of WLAN services by configuring user priorities and committed access rate (CAR) in a QoS profile.

### Applicable Environment

An AP terminates 802.11 packets sent from STAs, converts the 802.11 packets into 802.3 packets, and sends the 802.3 packets to an AC. To ensure the service quality for 802.3 packets, set user priorities and CAR for flow control.

#### NOTE

- Similar as a user profile, a QoS profile controls QoS for users based on the user priority and CAR parameters. After a QoS profile is bound to a user group, the user priority and CAR parameters are applied to users in the user group. When a QoS profile and user profile are configured simultaneously on an AC, the AC prefers the QoS profile for QoS control.
- Modifications to a QoS profile take effect only for subsequent users and do not affect current online users.

### Pre-configuration Tasks

Before configuring the user priority and CAR, complete the following tasks:

- Configuring AC attributes according to [1.3 Configuring Basic AC Attributes](#)
- Connecting APs to the AC correctly
- Creating a user group and sending the user group configuration to the AP

### Data Preparation

To configure the user priority and CAR, you need the following data.

| No. | Data                               |
|-----|------------------------------------|
| 1   | Name of a QoS profile              |
| 2   | User priority                      |
| 3   | CAR parameter values               |
| 4   | (Optional) QoS profile description |

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
qos-profile name profile-name
```

A QoS profile is created and the QoS profile view is displayed.

**Step 3** Run:

```
description description
```

A description is configured for the QoS profile.

**Step 4** Run:

```
car { inbound | outbound } cir cir-value [pir pir-value [cbs cbs-value pbs pbs-
value]]
```

CAR parameters are configured.

**Step 5** Run:

```
remark local-precedence { local-precedence-name | local-precedence-value }
```

The user priority is configured.

**Step 6** Run:

```
commit { all | ap ap-id }
```

The QoS profile is delivered to a specified AP or all APs. The QoS configuration will apply to users after they go online and join the user group to which the QoS profile is bound.

----End

## Verifying the Configuration

Run the **display qos-profile { all | name profile-name }** command to check the QoS profile configuration.

# Check the configuration of QoS profile **name1**.

```
[Quidway] display qos-profile name name1
Name :name1
Description :global
Local Precedence :-
Inbound car cir - kbps, cbs - bytes, pir - kbps, pbs - bytes
Outbound car cir - kbps, cbs - bytes, pir - kbps, pbs - bytes
```

# Check the list of all QoS profiles.

```
[Quidway] display qos-profile all
index QoS Profile Name

0 name1

Total QoS Profile number is 1
```

## 4.7 Configuration Examples

### 4.7.1 Example for Configuring a QoS Policy

#### Networking Requirements

STA1 and STA2 are connected to the network through AP1. STA3, STA4, and STA5 are connected to the network through AP2. STA5 is a VIP customer. The requirements are:

- Voice service requirements of STA1 and STA2 connected to AP1 are met first.
- Video service requirements of STA3, STA4, and STA5 connected to AP2 are met first.
- Communication requirements of STA5 are met first when the network bandwidth is insufficient.

Figure 4-1 shows the networking diagram.

Figure 4-1 Networking diagram of WLAN service configurations

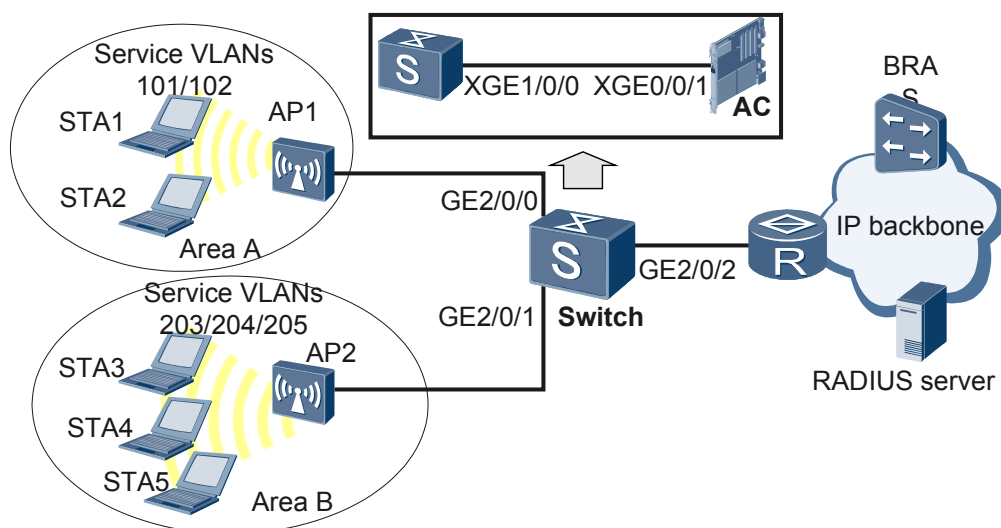


Table 4-2 Data plan

| Item         | Data                                                                                                                           |
|--------------|--------------------------------------------------------------------------------------------------------------------------------|
| WLAN service | <ul style="list-style-type: none"> <li>● SSID: huawei-1</li> <li>● Traffic profile: huawei</li> <li>● VLAN: 101</li> </ul>     |
|              | <ul style="list-style-type: none"> <li>● SSID: huawei-2</li> <li>● Traffic profile: huawei</li> <li>● VLAN: 102</li> </ul>     |
|              | <ul style="list-style-type: none"> <li>● SSID: huawei-3</li> <li>● Traffic profile: huawei</li> <li>● VLAN: 203</li> </ul>     |
|              | <ul style="list-style-type: none"> <li>● SSID: huawei-4</li> <li>● Traffic profile: huawei</li> <li>● VLAN: 204</li> </ul>     |
|              | <ul style="list-style-type: none"> <li>● SSID: huawei-5</li> <li>● Traffic profile: huawei-vip</li> <li>● VLAN: 205</li> </ul> |

| Item                       | Data                                                                                                                                                                      |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio profile of an AP     | <ul style="list-style-type: none"><li>● AP1 radio profile (huawei) and WMM profile (huawei)</li><li>● AP2 radio profile (huawei-vi) and WMM profile (huawei-vi)</li></ul> |
| Management VLAN of an AP   | VLAN 100, which is assigned by the Switch                                                                                                                                 |
| AP region                  | <ul style="list-style-type: none"><li>● AP1: 101</li><li>● AP2: 102</li></ul>                                                                                             |
| Service VLAN of an AP      | <ul style="list-style-type: none"><li>● AP1: VLAN 101 and VLAN 102</li><li>● AP2: VLAN 203, VLAN 204, and VLAN 205</li></ul>                                              |
| SwitchVLAN                 | VLAN 100/101/102/203/204/205                                                                                                                                              |
| AC's management IP address | VLANIF 100: 192.168.0.1/24                                                                                                                                                |
| AC carrier ID/AC ID        | other/1                                                                                                                                                                   |

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Switch and the AC to enable APs to communicate with the AC.
2. Configure basic AC attributes, including the AC ID, carrier ID, and source interface that the AC uses to communicate with APs.
3. Set the AP authentication mode and add APs to an AP region.
4. Configure VAPs and deliver VAP parameters. To configure a VAP:
  - Configure a WLAN-ESS interface and bind it to a service set so that radio packets can be sent to the WLAN service module after reaching the AC.
  - Create a WMM profile and set attributes for the profile. Create a radio profile and bind it to the WMM profile to first meet voice or video service requirements of users.
  - Create a traffic profile and set attributes for the profile to first meet communication requirements of the VIP customer when the network bandwidth is insufficient.
  - Create a security profile to control STA access.
  - Create a service set and bind the security profile and traffic profile to the service set.
  - Configure a VAP and deliver VAP parameters to implement QoS control for STAs.

## Procedure

**Step 1** Configure the Switch and the AC to enable APs to communicate with the AC.

# Configure GE2/0/0 and GE2/0/1 of the Switch connected to APs as trunk interfaces, and set the PVID of the trunk interfaces to 100.

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] vlan batch 203 to 205
[Quidway] interface GigabitEthernet 2/0/0
```

```
[Quidway-GigabitEthernet2/0/0] port link-type trunk
[Quidway-GigabitEthernet2/0/0] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/0] port trunk allow-pass vlan 100 101 102
[Quidway-GigabitEthernet2/0/0] quit
[Quidway] interface GigabitEthernet 2/0/1
[Quidway-GigabitEthernet2/0/1] port link-type trunk
[Quidway-GigabitEthernet2/0/1] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 203 to 205
[Quidway-GigabitEthernet2/0/1] quit
```

# Configure XGE1/0/0 of the Switch connected to the AC to transparently transmit packets of all service VLANs and the management VLAN.

```
[Quidway] interface XGigabitEthernet 1/0/0
[Quidway-XGigabitEthernet1/0/0] port link-type trunk
[Quidway-XGigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 102 203 to 205
```

# Configure XGE0/0/1 of the AC connected to the Switch to transparently transmit packets of all service VLANs and the management VLAN.

```
<Quidway> system-view
[Quidway] sysname AC
[AC] vlan batch 100 to 102
[AC] vlan batch 203 to 205
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102 203 to 205
[AC-XGigabitEthernet0/0/1] quit
```

## Step 2 Configure basic AC attributes.

# Configure the AC ID, carrier ID, and country code.

```
[AC] wlan ac-global ac id 1 carrier id other
[AC] wlan ac-global country-code country-code
```

# Configure a VLANIF interface and assign an IP address to it for Layer 3 packet forwarding.

```
[AC] interface vlanif100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] quit
```

# Configure a source interface on the AC to communicate with APs.

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
[AC-wlan-view] quit
```

### NOTE

An AC uses the IP address of the specified source interface as the source IP address. All APs connected to the AC can learn this IP address.

## Step 3 Configure APs and enable them to go online.

# Set the AP authentication mode to **no-auth**.

```
[AC-wlan-view] ap-auth-mode no-auth
```

### NOTE

If the AP authentication mode is set to **no-auth**, APs of the specified type can go online automatically. After an AP goes online, it is added to the default region and bound to the default AP profile, and its attributes are set to default values. The AP then enters the normal state.

# Create AP regions 101 and 102.

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```



```
Add AP1 to AP region 101 and AP2 to AP region 102.
```

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

#### Step 4 Configure WLAN-ESS interfaces.

```
[AC] interface wlan-ess1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 101
[AC-WLAN-ESS1] quit
[AC] interface wlan-ess2
[AC-WLAN-ESS2] port link-type hybrid
[AC-WLAN-ESS2] port hybrid untagged vlan 102
[AC-WLAN-ESS2] quit
[AC] interface wlan-ess3
[AC-WLAN-ESS3] port link-type hybrid
[AC-WLAN-ESS3] port hybrid untagged vlan 203
[AC-WLAN-ESS3] quit
[AC] interface wlan-ess4
[AC-WLAN-ESS4] port link-type hybrid
[AC-WLAN-ESS4] port hybrid untagged vlan 204
[AC-WLAN-ESS4] quit
[AC] interface wlan-ess5
[AC-WLAN-ESS5] port link-type hybrid
[AC-WLAN-ESS5] port hybrid untagged vlan 205
[AC-WLAN-ESS5] quit
```

#### Step 5 Configure profiles for APs.

- Create WMM profiles.

```
Create a WMM profile huawei and use the default settings, for example, the AC_VO queue has a higher priority than the AC_VI queue.
```

```
[AC-wlan-view] wmm-profile name huawei
[AC-wlan-wmm-prof-huawei] quit
```

```
Create a WMM profile huawei-vi and change the queue priority to enable the AC_VI queue to have a higher priority than the AC_VO queue.
```

```
[AC-wlan-view] wmm-profile name huawei-vi
[AC-wlan-wmm-prof-huawei-vi] wmm edca ap ac-vi ecw ecwmin 1 ecwmax 1 aifsn 1
txoplimit 36 ack-policy normal
[AC-wlan-wmm-prof-huawei-vi] wmm edca client ac-vi ecw ecwmin 1 ecwmax 3 aifsn
1 txoplimit 36
[AC-wlan-wmm-prof-huawei-vi] quit
```

- # Create radio profiles and bind WMM profiles to them.

```
[AC-wlan-view] radio-profile name huawei
[AC-wlan-radio-prof-huawei] wmm-profile name huawei
[AC-wlan-radio-prof-huawei] quit
[AC-wlan-view] radio-profile name huawei-vi
[AC-wlan-radio-prof-huawei-vi] wmm-profile name huawei-vi
[AC-wlan-radio-prof-huawei-vi] quit
```

- # Create a security profile **huawei**.

```
[AC-wlan-view] security-profile name huawei
[AC-wlan-sec-prof-huawei] quit
```

- Create traffic profiles.

```
Create a traffic profile huawei and limit the VAP downstream rate to 1024 kbit/s and STA upstream rate to 512 kbit/s.
```

```
[AC-wlan-view] traffic-profile name huawei
[AC-wlan-traffic-prof-huawei] rate-limit client up 512
[AC-wlan-traffic-prof-huawei] rate-limit vap down 1024
[AC-wlan-traffic-prof-huawei] quit
```

```
Create a traffic profile huawei-vip and limit the VAP upstream rate to 2048 kbit/s and
STA upstream rate to 1024 kbit/s.
```

```
[AC-wlan-view] traffic-profile name huawei-vi
[AC-wlan-traffic-prof-huawei-vi] rate-limit client up 1024
[AC-wlan-traffic-prof-huawei-vi] rate-limit vap up 2048
[AC-wlan-traffic-prof-huawei-vi] quit
```

### Step 6 Configure radios for APs.

- # Configure a radio for AP1 and bind it to a radio profile **huawei**.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name huawei
[AC-wlan-radio-1/0] quit
```

- # Configure a radio for AP2 and bind it to a radio profile **huawei-vi**.

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] radio-profile name huawei-vi
[AC-wlan-radio-2/0] quit
```

### Step 7 Configure service sets for APs.

- # Create service set **huawei-1**, specify SSID **huawei-1** for it, and bind traffic profile **huawei**, security profile **huawei**, and VLAN 101 to it.

```
[AC-wlan-view] service-set name huawei-1
[AC-wlan-service-set-huawei-1] ssid huawei-1
[AC-wlan-service-set-huawei-1] traffic-profile name Huawei
[AC-wlan-service-set-huawei-1] security-profile name Huawei
[AC-wlan-service-set-huawei-1] wlan-ess 1
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] quit
```

- # Create service set **huawei-2**, specify SSID **huawei-2** for it, and bind traffic profile **huawei**, security profile **huawei**, and VLAN 102 to it.

```
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name Huawei
[AC-wlan-service-set-huawei-2] security-profile name Huawei
[AC-wlan-service-set-huawei-2] wlan-ess 2
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] quit
```

- # Create service set **huawei-3**, specify SSID **huawei-3** for it, and bind traffic profile **huawei**, security profile **huawei**, and VLAN 203 to it.

```
[AC-wlan-view] service-set name huawei-3
[AC-wlan-service-set-huawei-3] ssid huawei-3
[AC-wlan-service-set-huawei-3] traffic-profile name Huawei
[AC-wlan-service-set-huawei-3] security-profile name Huawei
[AC-wlan-service-set-huawei-3] wlan-ess 3
[AC-wlan-service-set-huawei-3] service-vlan 203
[AC-wlan-service-set-huawei-3] quit
```

- # Create service set **huawei-4**, specify SSID **huawei-4** for it, and bind traffic profile **huawei**, security profile **huawei**, and VLAN 204 to it.

```
[AC-wlan-view] service-set name huawei-4
[AC-wlan-service-set-huawei-4] ssid huawei-4
[AC-wlan-service-set-huawei-4] traffic-profile name Huawei
[AC-wlan-service-set-huawei-4] security-profile name Huawei
[AC-wlan-service-set-huawei-4] wlan-ess 4
[AC-wlan-service-set-huawei-4] service-vlan 204
[AC-wlan-service-set-huawei-4] quit
```

- # Create service set **huawei-5**, specify SSID **huawei-5** for it, and bind traffic profile **huawei-vip**, security profile **huawei**, and VLAN 205 to it.

```
[AC-wlan-view] service-set name huawei-5
[AC-wlan-service-set-huawei-5] ssid huawei-5
[AC-wlan-service-set-huawei-5] traffic-profile name huawei-vip
[AC-wlan-service-set-huawei-5] security-profile name Huawei
[AC-wlan-service-set-huawei-5] wlan-ess 5
```

```
[AC-wlan-service-set-huawei-5] service-vlan 205
[AC-wlan-service-set-huawei-5] quit
```

**Step 8** Configure VAPs for APs and deliver VAP parameters.

# Bind the radio of AP1 to service sets **huawei-1** and **huawei-2** and deliver VAP parameters.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-1
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```

# Bind the radio of AP2 to service sets **huawei-3**, **huawei-4**, and **huawei-5** and deliver VAP parameters.

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] service-set name Huawei-3
[AC-wlan-radio-2/0] service-set name Huawei-4
[AC-wlan-radio-2/0] service-set name Huawei-5
[AC-wlan-radio-2/0] quit
[AC-wlan-view] commit ap 2
```

**Step 9** Verify the configuration.

Five WLANs with SSIDs huawei-1, huawei-2, huawei-3, huawei-4, and huawei-5 are available for STAs connected to AP1 and AP2. STA 1 to STA5 select WLANs with SSIDs huawei-1, huawei-2, huawei-3, huawei-4, and huawei-5 respectively.

- The maximum rate of STA1, STA2, STA3, and STA4 is 512 kbit/s. The maximum rate of STA5 is 1024 kbit/s, and the communication requirements of STA5 are met first when the network bandwidth is insufficient.
- Voice service requirements of STA1 and STA2 connected to AP1 are met first. Video service requirements of STA3, STA4, and STA5 connected to AP2 are met first.

----End

## Configuration Files

- Configuration file of the AC

```
#
sysname
AC
#
vlan batch 100 to 102
vlan batch 203 to 205
#
wlan ac-global carrier id other ac id 1
#
interface Vlanif100
ip address 192.168.0.1 255.255.255.0
#
interface Wlan-Ess1
port hybrid untagged vlan 101
#
interface Wlan-Ess2
port hybrid untagged vlan 102
#
interface Wlan-Ess3
port hybrid untagged vlan 203
#
interface Wlan-Ess4
port hybrid untagged vlan 204
#
interface Wlan-Ess5
```

```
port hybrid untagged vlan 205
#
wlan
wlan ac source interface
Vlanif100
ap-region id
101
ap-region id
102
ap-auth-mode no-
auth
ap id 0
ap id 1
wmm-profile name huawei id 0
wmm-profile name Huawei-vi id 1
wmm edca ap ac-vi aifsn 1 ecw ecwmin 1 ecwmax 1 txoplimit 36
wmm edca client ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
traffic-profile name huawei id 0
rate-limit client up 512
rate-limit vap down 1024
traffic-profile name huawei-vi
rate-limit client up 1024
rate-limit vap up 2048
security-profile name huawei id 0
service-set name huawei-1 id 0
wlan-ess 1
ssid huawei-1
traffic-profile id 0
security-profile id 0
service-vlan 101
service-set name huawei-2 id 1
wlan-ess 2
ssid huawei-2
traffic-profile id 0
security-profile id 0
service-vlan 102
service-set name huawei-3 id 2
wlan-ess 3
ssid huawei-3
traffic-profile id 0
security-profile id 0
service-vlan 203
service-set name huawei-4 id 3
wlan-ess 4
ssid huawei-4
traffic-profile id 0
security-profile id 0
service-vlan 204
service-set name huawei-5 id 4
wlan-ess 5
ssid huawei-5
traffic-profile id 1
security-profile id 0
service-vlan 205
radio-profile name huawei id 0
wmm-profile id 0
radio-profile name huawei-vi id 1
wmm-profile id 1
ap 1 radio
0
radio-profile name huawei
service-set name huawei-1 wlan 1
service-set name huawei-2 wlan 1
ap 0 radio
0
radio-profile name huawei-vi
service-set name huawei-3 wlan 2
service-set name huawei-4 wlan 2
service-set name huawei-5 wlan 2
```

- Configuration file of the Switch

```
#
interface GigabitEthernet2/0/0
 port link-type
 trunk
 port trunk pvid vlan
 100
 port trunk allow-pass vlan 100 101
 102
#
interface GigabitEthernet2/0/1
 port link-type
 trunk
 port trunk pvid vlan
 100
 port trunk allow-pass vlan 100 203 to
 205
#
interface GigabitEthernet1/0/0
 port link-type
 trunk
 port trunk allow-pass vlan 100 to 102 203 to
 205
```