Huawei WLAN Certification Training

HCIA-WLAN

Lab Guide

ISSUE:3.0

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

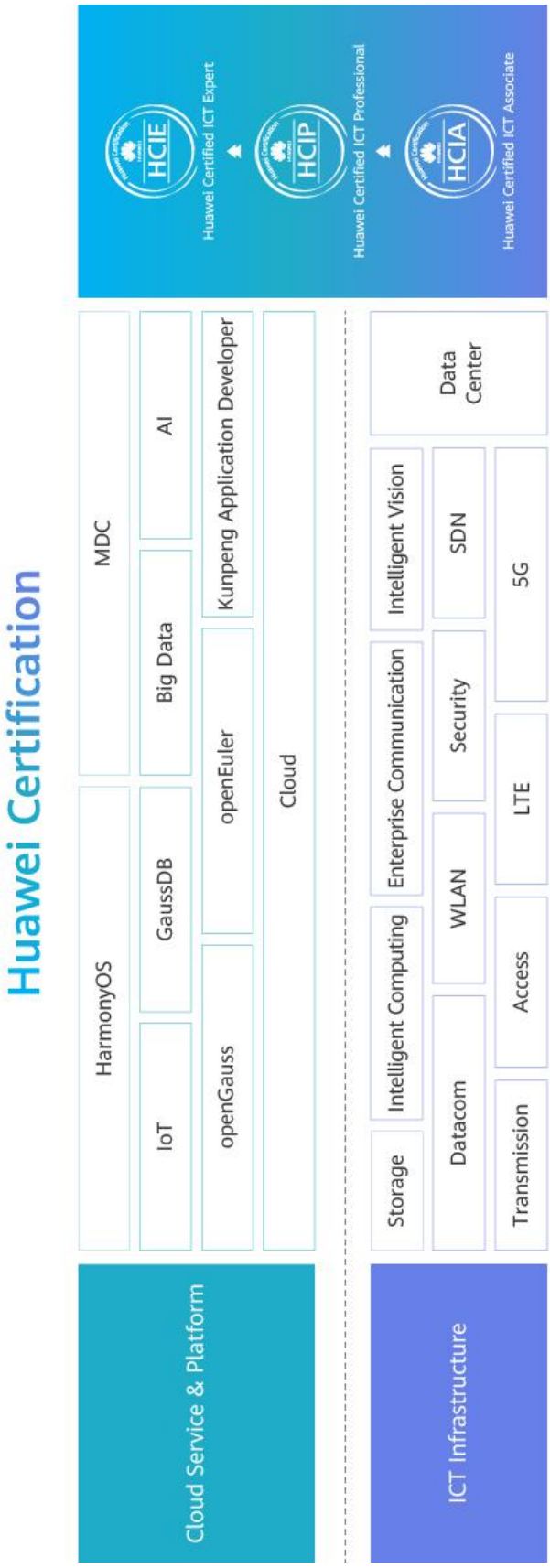
Huawei Certificate System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, Platform and Service certification and ICT vertical certification, and grants Huawei certification the only all-range technical certification in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

Huawei Certified Network Associate-Wireless Local Area Network (HCIA-WLAN) is designed for Huawei local offices, online engineers in representative offices, and readers who want to understand Huawei WLAN products and technology. HCIA-WLAN covers WLAN basics, Control and Provisioning of Wireless Access Points (CAPWAP) protocol, WLAN networking, Huawei WLAN product features, security configuration, WLAN advanced technology, antennas, WLAN network planning and optimization, and WLAN fault troubleshooting.

The HCIA-WLAN certificate system introduces you to the industry and market, helps you in innovation, and enables you to stand atop the WLAN frontiers.


Huawei Certification
Cloud Service & Platform
ICT Infrastructure
HarmonyOS
IoT
GaussDB
MDC
Big Data
AI
openGauss
openEuler
Kunpeng Application Developer
Cloud
Storage
Intelligent Computing
Enterprise Communication
Intelligent Vision
Data Center
Datacom
WLAN
Security
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This document is an HCIA-WLAN certification training course. It is intended for trainees who are preparing for the HCIA-WLAN exam or readers who want to understand Huawei WLAN basics, implementation, CAPWAP protocol, networking modes, features and security configurations of Huawei WLAN products, advanced WLAN technologies, antenna technology, WLAN troubleshooting, and project deployment.

Description

This document contains six experiments, including basic VRP configuration, WLAN device upgrade, WLAN Layer 2 off-path networking, WLAN Layer 3 off-path networking, and WLAN radio resource management and troubleshooting.

- Experiment 1 is about basic VRP configurations. This exercise helps you familiarize yourself with the operations and commands related to Huawei wireless controllers.
- Experiment 2: WLAN device upgrade. This exercise describes how to upgrade Huawei WLAN devices, helping readers get familiar with the upgrade procedures and commands related to AC and AP upgrade.
- Experiment 3 is a Layer 2 bypass networking experiment. This experiment describes how to configure Huawei WLAN Layer 2 networking and how to deploy a small-scale WLAN.
- Experiments 4 describe how to configure Huawei WLAN Layer 3 networking in bypass mode using the CLI and web. This chapter helps readers learn how to configure Huawei WLAN Layer 3 networking and configure medium- and large-sized WLANs.
- Experiment 5 is an experiment on WLAN radio resource management. This experiment introduces basic configurations of Huawei WLAN radio resource management, helping readers to master basic WLAN network optimization methods.
- Experiment 6 is a WLAN troubleshooting experiment. This experiment describes the basic WLAN troubleshooting process and methods, helping readers to master basic WLAN troubleshooting methods.

Background Knowledge Required

This course is for Huawei's basic certification. To better understand this course, familiarize yourself with the following requirements:

- Basic knowledge about WLAN and data communication.

Common Icons


AC


AP


Core switch


Access switch


Router


PC


STA

Experiment Environment Overview

Networking Introduction

This experiment environment is intended for WLAN engineers who are preparing for the HCIA-WLAN exam. Each lab environment includes two ACs, two APs, one core switch, one access switch, and one router. Each lab environment is applicable to two groups of trainees. Router, core switch, access switch, and APs are shared by two groups of trainees. Each group of trainees uses one AC. Trainees need to prepare test PCs by themselves.

Device Introduction

The following table lists the recommended device configurations in each lab environment of HCIA-WLAN.

Device Type	Device Model	Software Version
Switch	S5731-H24P4XC	V200R019C10SPC500
AC	AirEngine 9700-M	V200R019C10SPC300
AP	AirEngine 5760-51	V200R019C10SPC300
Router	AR2220E	V200R010C10SPC700

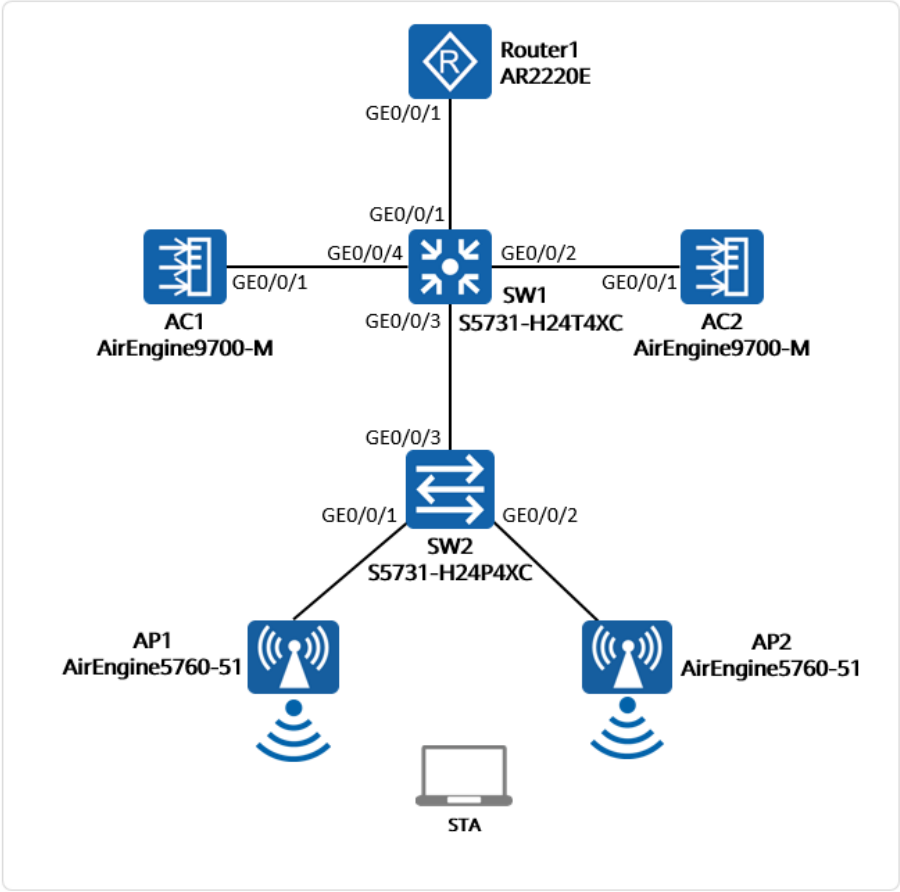
Experiment Environment Preparation

Checking Whether All Devices Are Available

Before starting a lab, ensure that the devices listed in the following table are ready.

Device Name	Quantity	Remarks
S5731-H24P4XC	2/group	PoE power supply required
AirEngine 9700-M	1/group	
AirEngine 5760-51	2/group	
AR2220E	1/group	
Test Laptop	1/group	

Experiment topology



Contents

1 Basic VRP Configurations

1.1 Introduction

1.1.1 About This Lab

In this lab activity, you will learn the basic commands of Huawei devices by configuring an AC to communicate with a switch.

1.1.2 Objectives

Understand the basic configuration of Huawei devices.

1.1.3 Networking Topology

The following uses AC1 as an example to describe the topology. If you use AC2, pay attention to the interface numbers of SW1. In this document, AC1 and AC2 are collectively referred to as ACs.

Figure 1-1 Lab topology for basic VRP configurations

1.1.4 Lab Planning

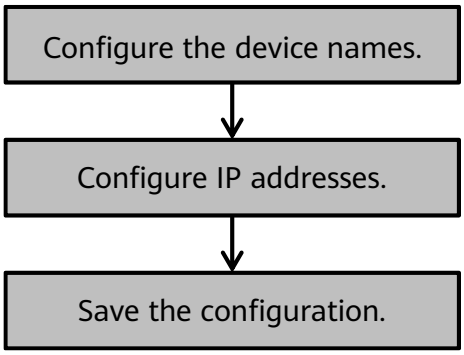
This lab aims to achieve communication between an AC and a switch, help you get familiar with basic configurations of Huawei devices and help information.

Table 1-1 IP address design

Device	Interface	IP Address
SW1	Vlanif 1	192.168.1.1
AC	Vlanif 1	192.168.1.2

1.2 Lab Procedure

1.2.1 Configuration Roadmap



1.2.2 Configuration Procedure

Step 1 Configure the device names.

Configure names for the switch and AC.

On the switch, enter the system view from the user view. Enter the first letters of a keyword in a command, and enter a question mark (?) or press **Tab** to display a complete keyword.

```
<Huawei> sys?                 // You can use “?” to view the command line prompt.
  system-view   SystemView from terminal
<Huawei> sys                  // You can use “Tab” to complete configuration commands.
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

After entering the system view, run the **sysname** command to change the device name to **SW**.

```
[Huawei] sysname SW
[SW]
```

On the AC, enter the system view from the user view. Enter the first letters of a keyword in a command, and enter a question mark (?) or press **Tab** to display a complete keyword.

```
<AirEngine9700-M> sys?
  system-view     SystemView from terminal
<AirEngine9700-M> sys
<AirEngine9700-M> system-view
Enter system view, return user view with Ctrl+Z.
[AirEngine9700-M]
```

After entering the system view, run the **sysname** command to change the device name to **AC**.

```
[AirEngine9700-M] sysname AC
[AC]
```

Step 2 Configure IP addresses for the devices.

Configure IP addresses for the interfaces connecting the switch and AC according to the IP address design.

Set the IP address of **Vlanif 1** on the SW to 192.168.1.1 and the mask length to 24.

```
[SW] interface Vlanif 1
[SW-Vlanif1] ip address 192.168.1.1 24
```

Display IP address information.

```
[SW] display ip int brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 1

Interface                         IP Address/Mask      Physical   Protocol
NULL0                             unassigned           up         up(s)
Vlanif1                           192.168.1.1/24       up         up
```

Set the IP address of **Vlanif 1** on the AC to 192.168.1.2 and the mask length to 24.

```
[AC] interface Vlanif 1
[AC-Vlanif1] ip address 192.168.1.2 24
```

Run the **display this** command on the AC's interface to verify the configuration result.

```
[AC-Vlanif1] display this
#
interface Vlanif1
 ip address 192.168.1.2 255.255.255.0
#
return
```

Run the **ping** command on SW to test the connectivity between the AC and SW. The command output shows that SW can ping the AC.

```
[SW] ping 192.168.1.2
  PING 192.168.1.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.2: bytes=56 Sequence=1 ttl=255 time=90 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 192.168.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 192.168.1.2: bytes=56 Sequence=4 ttl=255 time=10 ms
```

```
  Reply from 192.168.1.2: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 192.168.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/28/90 ms
```

Step 3 Save the configuration.

In the production environment, to prevent the configuration from becoming invalid after power-off or fault recovery, save the device configuration.

Run the **save** command in the user view of the AC and SW to save the device configurations. If the message "saved successfully" is displayed, the configuration is saved successfully.

```
[SW] quit
<SW> save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]: y
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<SW>
[AC] quit
<AC> save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]: y
  It will take several minutes to save configuration file, please wait.....
  Configuration file has been saved successfully
  Note: The configuration file will take effect after being activated
<AC>
```

----End

1.3 Verification

1.3.1 Checking the Device Configuration After a Device Is Restarted

Run the **reboot** command to restart a device.

```
<SW> reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue? [y/n]: y
Info: system is rebooting, please wait...
```

After the device restarts, run the **display current-configuration** command to check the device configuration.

```
<SW> display current-configuration
#
 sysname SW
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
#
return
```

1.4 Configuration Reference

1.4.1 Configuration on the SW1

```
#
 sysname SW
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
#
return
```

1.4.2 Configuration on the AC

```
#
 sysname AC
#
interface Vlanif1
 ip address 192.168.1.2 255.255.255.0
#
Return
```

2 WLAN Device Upgrade

2.1 Introduction

2.1.1 About This Lab

An enterprise has been using Huawei devices to build its WLAN. The enterprise wants to upgrade ACs and APs to fix bugs in some versions and obtain new functions.

2.1.2 Objectives

- Understand the reason why WLAN devices need an upgrade.
- Learn how to upgrade the WLAN devices.

2.1.3 Networking Topology

In the following experiment, an AC and an AP are directly connected to the PC and AP. In this document, AC1 and AC2 are collectively referred to as ACs, and AP1 and AP2 are collectively referred to as APs.

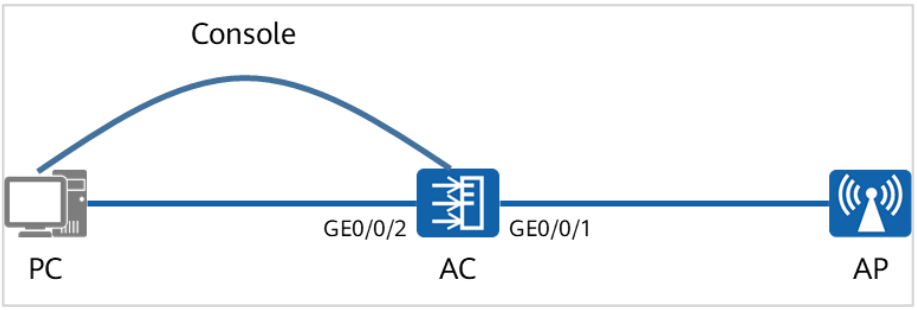


Figure 2-1 WLAN device upgrade topology

2.1.4 Lab Planning

This lab aims to upgrade WLAN devices by connecting a PC directly to an AC to upgrade the AC and upgrading an AP in AC mode.

Table 2-1 VLAN port types and parameters

Device	Port	Port Type	VLAN Settings
AC	GE0/0/1	Access	PVID: VLAN 10
	GE0/0/2	Access	PVID: VLAN 1

Table 2-2 IP address plan

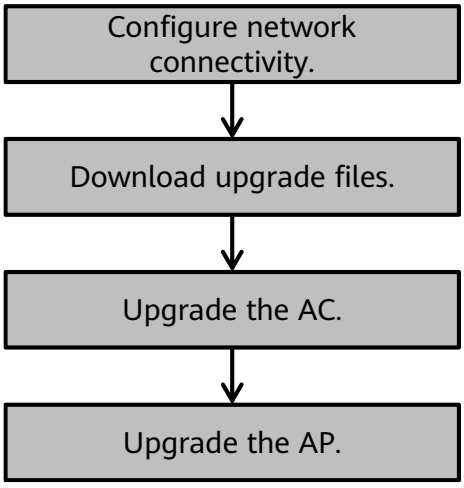
Device	Interface	IP Address
PC	Ethernet interface	192.168.1.1/24
AC	Vlanif 1	192.168.1.2/24
	Vlanif 10	10.1.10.1/24

Table 2-3 WLAN data plan

Item	Configuration
DHCP server	The AC functions as a DHCP server to assign IP addresses to APs and as the gateway of APs.
IP address pool for APs	10.1.10.2–10.1.10.254/24
AC's source interface address	VLAN 10

2.2 Lab Procedure

2.2.1 Configuration Roadmap



2.2.2 Configuration Procedure

Step 1 Configure network connectivity.

Create VLAN 10 on the AC.

```
<AirEngine9700-M> system-view
[AirEngine9700-M] sysname AC
[AC] vlan batch 10
```

Configure interface types on the AC and configure the AC to allow packets from the corresponding VLANs to pass through according to Table 2-1.

```
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type access
[AC-GigabitEthernet0/0/1] port default vlan 10
[AC-GigabitEthernet0/0/1] quit
```

Configure IP addresses on devices to ensure network connectivity.

Create Vlanif interfaces on the AC and configure IP addresses for them.

```
[AC] interface Vlanif 1
[AC-Vlanif1] ip address 192.168.1.2 24
[AC-Vlanif1] quit
[AC] interface Vlanif 10
[AC-Vlanif10] ip address 10.1.10.1 24
[AC-Vlanif10] quit
```

Ping the PC from the AC. The ping operation succeeds.

```
<AC> ping 192.168.1.1
  PING 192.168.1.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=128 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=128 time=1 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=128 time=1 ms
    Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=128 time=1 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Step 2 Download upgrade files.

Download the required AC and AP software packages to the AC through FTP.

Run the **display version** command to check the running device version.

```
<AC> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine9700-M V200R019C00SPC300)
Copyright (C) 2011-2019 HUAWEI TECH CO., LTD
Huawei AirEngine9700-M Router uptime is 0 week, 5 days, 17 hours, 59 minutes

MPU 0(Master) : uptime is 0 week, 5 days, 17 hours, 59 minutes
SDRAM Memory Size      : 16384     M bytes
Flash Memory Size      : 2048      M bytes
MPU version information :
1. PCB          Version   : H852V26S VER.B
2. MAB          Version   : 0
3. Board        Type      : AirEngine9700-M
4. CPLD0        Version   : 273
```

```
5. CPLD1      Version   : 277
6. CPLD2      Version   : 273
7. BootROM    Version   : 1080

PWRCARD I information
PCB          Version : PWR VER   VER.NC
```

The running device version is V200R019C00SPC300. To support new functions, upgrade the device to V200R019C10SPC300.

Download the software package of the corresponding version from Huawei official website to the local PC. Configure the local PC as the FTP server so that the AC downloads the software package through FTP.

The FTP server is the local PC, with the user name and password of **admin** and **huawei**, respectively. Run the **ftp 192.168.1.1** command to log in to the FTP server.

```
<AC> ftp 192.168.1.1
Trying 192.168.1.1 ...
Press CTRL+K to abort
Connected to 192.168.1.1.
220 3Com 3CDaemon FTP server 2.0
User(192.168.1.1:(none)):admin
331 Correct user name. Enter the password.
Enter password:
230 You have successfully logged in.

[AC-ftp]
```

Run the **dir** command to check the files in the current directory.

```
[AC-ftp] dir
200 PORT The command is executed successfully.
150 The file status is normal. Ready to start the data connection.
-rwxrwxrwx 1 owner group    89296660 May 25 17:32 AirEngine9700-M_V200R019C10SPC300.cc
-rwxrwxrwx 1 owner group    21255580 May 22 17:07 FitAirEngine5760-51_V200R019C10SPC300.bin
226 The data connection is being closed.
FTP: 1858 byte(s) received in 0.134 second(s) 13.86Kbyte(s)/sec.
```

Run the **get** command to download the software packages of the AC and AP to the AC.

```
[AC-ftp] get AirEngine9700-M_V200R019C10SPC300.cc
200 PORT The command is executed successfully.
150 The file status is normal. Ready to start the data connection.
226 Closing the data connection. The file is successfully transferred.
FTP: 89296660 byte(s) received in 515.622 second(s) 173.18Kbyte(s)/sec.
Now begins to save file, please
wait.....................................................................................................................
.....................
File has been saved successfully.
[AC-ftp] get FitAirEngine5760-51_V200R019C10SPC300.bin
200 PORT The command is executed successfully.
150 The file status is normal. Ready to start the data connection.
226 Closing the data connection. The file is successfully transferred.
```

```
FTP: 21255580 byte(s) received in 14.445 second(s) 1471.48Kbyte(s)/sec.
Now begins to save file, please
wait.....................................................................................................................................
.....................................................................
File has been saved successfully.
```

Step 3 Upgrade the AC.

Configure the downloaded AC software package as the startup configuration software package to upgrade the AC.

Run the **display startup** command to check the startup software package of the AC.

```
<AC> display startup
  Configed startup system software:        flash:/AirEngine9700-M_V200R019C10SPC300.cc
  Startup system software:                  flash:/AirEngine9700-M_V200R019C10SPC300.cc
  Next startup system software:            flash:/AirEngine9700-M_V200R019C10SPC300.cc
  Startup saved-configuration file:         flash:/vrpcfg.zip
  Next startup saved-configuration file:   flash:/vrpcfg.zip
  Startup patch package:                    NULL
  Next startup patch package:               NULL
```

Run the **startup system-software** AirEngine9700-M_V200R019C10SPC300.cc command to update the startup software package.

```
<AC> startup system-software AirEngine9700-M_V200R019C10SPC300.cc
Info: Verifying the file, please wait....
Info: Succeeded in setting the software for booting system.
```

Run the **save** command to save the configuration.

```
<AC> save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n) [n]: y
  It will take several minutes to save configuration file, please wait.....
  Configuration file has been saved successfully
  Note: The configuration file will take effect after being activated
```

Run the **reboot fast** command to restart the AC.

```
<AC> reboot fast
System will reboot! Continue ? [y/n]: y
```

After the AC restarts, run the **display version** command to check the running device version.

```
<AC> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine9700-M V200R019C10SPC300)
Copyright (C) 2011-2020 HUAWEI TECH CO., LTD
Huawei AirEngine9700-M Router uptime is 0 week, 0 day, 0 hour, 0 minute

MPU 0(Master) : uptime is 0 week, 0 day, 0 hour, 0 minute
```

```
SDRAM Memory Size      : 16384     M bytes
Flash Memory Size      : 2048      M bytes
MPU version information :
1. PCB          Version   : H852V26S VER.B
2. MAB          Version   : 0
3. Board        Type      : AirEngine9700-M
4. CPLD0        Version   : 273
5. CPLD1        Version   : 277
6. CPLD2        Version   : 273
7. BootROM    Version   : 1080

PWRCARD I information
PCB          Version : PWR VER    VER.NC
```

The command output shows that the AC version is V200R019C10SPC300, indicating that the upgrade is successful.

Step 4 Upgrade the AP.

Configure the DHCP service on the AC to assign IP addresses to APs.

```
[AC] dhcp enable
[AC] interface Vlanif 10
[AC-Vlanif10] dhcp select interface
[AC-Vlanif10] quit
```

Configure Vlanif 10 as the AC's source interface.

```
[AC] capwap source interface Vlanif 10
```

Configure the AP authentication mode to non-authentication.

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

Run the **display ap all** command to check the AP status.

```
[AC-wlan-view] display ap all
Total AP information:
vmiss : ver-mismatch      [1]
ExtraInfo : Extra information
P       : insufficient power supply
------------------------------------------------------------------------------------------------------------
ID      MAC                 Name      Group     IP              Type               State   STA Uptime
ExtraInfo
------------------------------------------------------------------------------------------------------------
0       b4fb-f9b7-de40      AP1       default   10.1.10.231     AirEngine5760-51     vmiss   0     -
-
------------------------------------------------------------------------------------------------------------
Total: 1
```

The AP status is **vmiss**, indicating an AP version mismatch. If the major version numbers are the same (for example, V200R019C10SPC300 and V200R019C10SPC500), **vmiss** is not displayed and the AP can go online normally.

```
[AC-wlan-view] ap-group name Huawei
```

Change the AP upgrade mode to AC mode.

```
[AC-wlan-view] ap update mode ac-mode
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The
FTP or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

Specify the AP upgrade version to upgrade the AP.

```
[AC-wlan-view] ap update update-filename FitAirEngine5760-51_V200R019C10SPC300.bin ap-type
115
Warning: If an AP is performing the automatic upgrade, the AP will be upgraded to the latest version.
Continue? [Y/N]: y
Warning: If AP update mode is AC-mode, update-file's default path is sdcard:/. Continue? [Y/N]: y
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The
FTP or SFTP upgrade mode is recommended. Continue? [Y/N]: y
Info: This operation may take a few seconds. Please wait for a moment.
done.
```

Run the **ap-reset all** command to restart all APs.

```
[AC-wlan-view] ap-reset all
Warning: Reset AP(s), continue? [Y/N]: y
```

Run the **display ap all** command to check the AP status.

```
<AC> display ap all
Total AP information:
dload : download            [1]
ExtraInfo : Extra information
P       : insufficient power supply
------------------------------------------------------------------------------------------------------
ID      MAC                 Name      Group     IP              Type        State   STA Uptime ExtraInfo
------------------------------------------------------------------------------------------------------
0       b4fb-f9b7-de40      AP1       default   10.1.10.231     AirEngine5760-51 dload   0     -       -
------------------------------------------------------------------------------------------------------
Total: 1
```

The AP status is **dload**, indicating that the AP is downloading the software package.

Run the d**isplay ap update status all** command to check the AP upgrade status.

```
<AC> display ap update status all
FT   : File Type
------------------------------------------------------------------------------------------------------
--------------
ID      Name AP Type   AP Group AP MAC            FT          Update Version      Last Update Time
Update Status
```

```
------------------------------------------------------------------------------------------------------------------------
--------------
0       AP1   AirEngine5760-51 default   b4fb-f9b7-de40 FIT          V200R019C10SPC300 XXXX-XX-
29/09:53:09       downloading(progress: 100%/47%)
------------------------------------------------------------------------------------------------------------------------
--------------
Total: 1
```

Wait for a period of time, and run the **display ap all** command again to check the AP status.

```
<AC> display ap all
Total AP information:
nor    : normal              [1]
ExtraInfo : Extra information
P      : insufficient power supply
-------------------------------------------------------------------------------------------
ID      MAC                 Name      Group     IP              Type        State  STA Uptime
ExtraInfo
-------------------------------------------------------------------------------------------
0       b4fb-f9b7-de40      AP1       default   10.1.10.231     AirEngine5760-51 nor     0    23S -
-------------------------------------------------------------------------------------------
Total: 1
```

The AP status is **nor**, indicating that the AP is online.

----End

2.3 Verification

2.3.1 Verifying the AC and AP Upgrade Results

Run the **display version** command on the AC to check the AC version. The command output shows that the AC has been successfully upgraded.

```
<AC> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine9700-M V200R019C10SPC300)
Copyright (C) 2011-2020 HUAWEI TECH CO., LTD
Huawei AirEngine9700-M Router uptime is 0 week, 0 day, 0 hour, 0 minute

MPU 0(Master) : uptime is 0 week, 0 day, 0 hour, 0 minute
SDRAM Memory Size      : 16384     M bytes
Flash Memory Size      : 2048      M bytes
MPU version information :
1. PCB          Version   : H852V26S VER.B
2. MAB          Version   : 0
3. Board        Type      : AirEngine9700-M
4. CPLD0        Version   : 273
5. CPLD1        Version   : 277
6. CPLD2        Version   : 273
7. BootROM      Version   : 1080
```

```
PWRCARD I information
PCB         Version : PWR VER    VER.NC
```

Run the **display ap run-info ap-id 0** command on the AC to check the AP version. The command output shows that the AP has been upgraded successfully.

```
<AC> display ap run-info ap-id 0
Info: Waiting for AP response.
-------------------------------------------------------------------------------------------------
AP type                          : AirEngine5760-51
Country code                     : CN
Software version                 : V200R019C10SPC300
Hardware version                 : Ver.A
BIOS version                     : 627
BOM version                      : 000
Memory size(MB)                  : 256
Flash size(MB)                   : 64
SD Card size(MB)                 : -
Manufacture                      : Huawei Technologies Co., Ltd.
Software vendor                  : Huawei Technologies Co., Ltd.
Online time(ddd:hh:mm:ss)        : 16H:57M:1S
Run time(ddd:hh:mm:ss)           : 16H:58M:12S
IP address                       : 10.1.10.231
IP mask                          : 255.255.255.0
Gateway                          : 10.1.10.1
DNS server                       : 0.0.0.0
AP mode                          : campus
GigabitEthernet port 0
  Port speed(Mbps)               : 1000
  Port speed mode                : auto
  Port duplex                    : full
  Port duplex mode               : auto
  Port state                     : up
  STP down recovery time(ddd:hh:mm:ss)          : -
Card status                      :
-------------------------------------------------------------------------------------------------
```

2.4 Configuration Reference

2.4.1 Configuration on the AC

```
#
 sysname AC
#
vlan batch 10
#
dhcp enable
#
interface Vlanif1
 ip address 192.168.1.2 255.255.255.0
```

```
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
capwap source interface vlanif10
#
wlan
ap auth-mode no-auth
#
return
```

3 WLAN Layer 2 Off-Path Networking

3.1 Introduction

3.1.1 About This Lab

On a Layer 2 WLAN, network traffic is usually sent to the upper-layer network through a switch, without passing through an AC. This networking mode applies to small- and medium-scale centralized WLANs.

3.1.2 Objectives

- Understand the Layer 2 networking mode.
- Understand the advantages of off-path networking.
- Learn how to configure WLAN services.

3.1.3 Networking Topology

The following uses AC2 as an example to describe the topology. If you use AC1, pay attention to the interface numbers of SW1. In this document, AC1 and AC2 are collectively referred to as ACs.

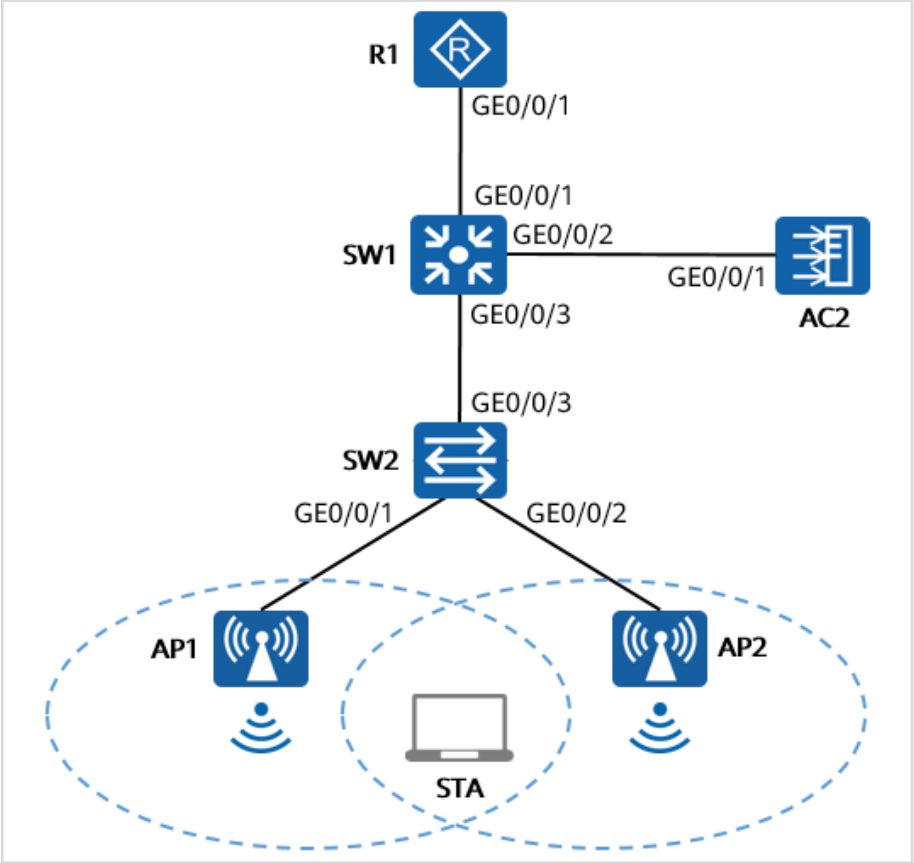


Figure 3-1 WLAN Layer 2 off-path networking topology

3.1.4 Lab Planning

This lab aims to instruct how to configure Layer 2 off-path networking, with the AC as the AP gateway and SW1 as the STA gateway. The two APs can both cover PC1, and STA traffic does not pass through the AC.

Table 3-1 VLAN port types and parameters

Device	Port	Port Type	VLAN Settings
SW1	GE0/0/1	Access	PVID: VLAN 30
	GE0/0/2	Trunk	PVID: 1 Allow-pass: VLAN 10
	GE0/0/3	Trunk	PVID: 1 Allow-pass: VLANs 10 and 20
SW2	GE0/0/1	Trunk	PVID: VLAN 10 Allow-pass: VLANs 10 and 20
	GE0/0/2	Trunk	PVID: VLAN 10 Allow-pass: VLANs 10 and 20

	GE0/0/3	Trunk	PVID: 1 Allow-pass: VLANs 10 and 20
AC	GE0/0/1	Trunk	PVID: VLAN 1 Allow-pass: VLAN 10

Table 3-2 IP Address Plan

Device	Interface	IP Address
R1	GE0/0/1	10.1.30.1/24
SW1	Vlanif 20	10.1.20.1/24
	Vlanif 30	10.1.30.2/24
AC	Vlanif 10	10.1.10.1/24

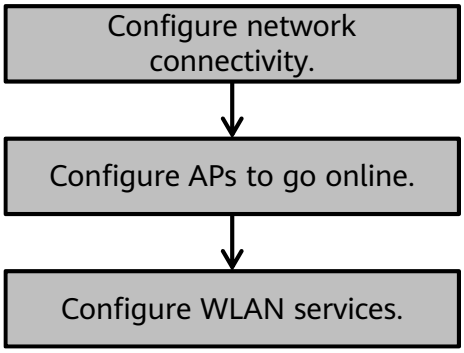
Table 3-3 WLAN Data Plan

Item	Configuration
DHCP server	The AC functions as a DHCP server to assign IP addresses to APs and as the gateway of APs. SW1 functions as a DHCP server to assign IP addresses to STAs and as the gateway of STAs.
IP address pool for APs	10.1.10.2–10.1.10.254/24
IP address pool for STAs	10.1.20.2–10.1.20.254/24
AC's source interface address	10.1.10.1/24
AP group	Name: Huawei Referenced profiles: VAP profile and regulatory domain profile
Regulatory domain profile	Name: Huawei Country code: CN
SSID profile	Name: Huawei SSID name: Huawei
Security profile	Name: Huawei Security policy: WPA-WPA2+PSK+AES Password: a1234567
VAP profile	Name: Huawei

	Forwarding mode: direct forwarding Service VLAN: VLAN 20 Referenced profiles: SSID profile and security profile

3.2 Lab Procedure

3.2.1 Configuration Roadmap



3.2.2 Configuration Procedure

Step 1 Configure network connectivity.

Configure VLANs and interface types on the devices to ensure that services can be transparently transmitted at Layer 2.

Create VLAN 10, VLAN 20, and VLAN 30 on SW1.

```
<Huawei> system-view
[Huawei] sysname SW1
[SW1] vlan batch 10 20 30
```

Configure interface types on SW1 and configure SW1 to allow packets from the corresponding VLANs to pass through according to Table 3-1.

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 30
[SW1-GigabitEthernet0/0/1] quit
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[SW1-GigabitEthernet0/0/2] quit
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SW1-GigabitEthernet0/0/3] quit
```

Create VLAN 10 and VLAN 20 on SW2.

```
<Huawei> system-view
[Huawei] sysname SW2
[SW2] vlan batch 10 20
```

Configure interface types on SW2 and configure SW2 to allow packets from the corresponding VLANs to pass through according to Table 3-1.

```
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk
[SW2-GigabitEthernet0/0/1] port trunk pvid vlan 10
[SW2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
[SW2-GigabitEthernet0/0/1] quit
[SW2] interface GigabitEthernet 0/0/2
[SW2-GigabitEthernet0/0/2] port link-type trunk
[SW2-GigabitEthernet0/0/2] port trunk pvid vlan 10
[SW2-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 20
[SW2-GigabitEthernet0/0/2] quit
[SW2] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type trunk
[SW2-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SW2-GigabitEthernet0/0/3] quit
```

Create VLAN 10 on the AC.

```
<AC6508> system-view
[AC6508] sysname AC
[AC] vlan batch 10
```

Configure interface types on the AC and configure the AC to allow packets from the corresponding VLANs to pass through according to Table 3-1.

```
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[AC-GigabitEthernet0/0/1] quit
```

Configure IP addresses and routing information on the devices to ensure network connectivity.

Create Vlanif 20 and Vlanif 30 on SW1 and assign IP addresses to them.

```
[SW1] interface Vlanif 20
[SW1-Vlanif20] ip address 10.1.20.1 24
[SW1-Vlanif20] quit
[SW1] interface Vlanif 30
[SW1-Vlanif30] ip address 10.1.30.2 24
[SW1-Vlanif30] quit
```

Create Vlanif 10 on the AC and configure an IP address for the Vlanif interface.

```
[AC] interface Vlanif 10
[AC-Vlanif10] ip address 10.1.10.1 24
[AC-Vlanif10] quit
```

On R1, configure an IP address for the interface connected to SW1 and create a static route destined for the STA network segment.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1] ip address 10.1.30.1 24
[R1-GigabitEthernet0/0/1] quit
[R1] ip route-static 10.1.20.0 24 10.1.30.2
```

Ping the IP address 10.1.20.1 on R1 from SW1. The ping operation succeeds.

```
[SW1] ping -a 10.1.20.1 10.1.30.1
  PING 10.1.30.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.30.1: bytes=56 Sequence=1 ttl=255 time=90 ms
    Reply from 10.1.30.1: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 10.1.30.1: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 10.1.30.1: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.1.30.1: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.1.30.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 10/38/90 ms
```

Step 2 Configure APs to go online.

Configure DHCP servers to assign IP addresses to APs and STAs.

Enable DHCP and configure an interface address pool on SW1.

```
[SW1] dhcp enable
[SW1] interface Vlanif 20
[SW1-Vlanif20] dhcp select interface
[SW1-Vlanif20] quit
```

Enable DHCP and configure an interface address pool on the AC.

```
[AC] dhcp enable
[AC] interface Vlanif 10
[AC-Vlanif10] dhcp select interface
[AC-Vlanif10] quit
```

Configure the AC's source interface address and configure a proper AP authentication mode so that the APs can go online normally.

Set the AC's source interface to 10.1.10.1.

```
[AC] capwap source ip-address 10.1.10.1
```

Create an AP group named **Huawei** on the AC.

```
[AC] wlan
```

```
[AC-wlan-view] ap-group name Huawei
[AC-wlan-ap-group-Huawei] quit
```

Set the AP authentication mode to non-authentication and wait for APs to go online.

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

Run the **display ap all** command to check the AP online status. The command output shows that the two APs have gone online.

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor   : normal              [2]
------------------------------------------------------------------------------------------------
ID         MAC             Name      Group      IP              Type        State      STA  Uptime
------------------------------------------------------------------------------------------------
0      00e0-fc1f-4ee0  00e0-fc1f-4ee0  default  10.1.10.177  AirEngine5760-51  nor  0     22S
1      00e0-fc54-64a0  00e0-fc54-64a0  default  10.1.10.122  AirEngine5760-51  nor  0     3S
------------------------------------------------------------------------------------------------
Total: 2
```

Name the two APs **AP1** and **AP2**, and add them to the AP group **Huawei**.

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] ap-name AP1
[AC-wlan-ap-0] ap-group Huawei
Warning: This operation may cause AP reset. If the country code changes, it will
 clear channel, power and antenna gain configurations of the radio, Whether to c
ontinue? [Y/N]: y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1
[AC-wlan-ap-1] ap-name AP2
[AC-wlan-ap-1] ap-group Huawei
Warning: This operation may cause AP reset. If the country code changes, it will
 clear channel, power and antenna gain configurations of the radio, Whether to c
ontinue? [Y/N]: y
[AC-wlan-ap-1] quit
```

Run the **display ap all** command to check whether the configuration takes effect. The command output shows that the configuration has taken effect.

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment. done.
Total AP information:
nor   : normal              [2]
------------------------------------------------------------------------------------
0      00e0-fc1f-4ee0  AP1      Huawei  10.1.10.177  AirEngine5760-51  nor  0     49S
1      00e0-fc54-64a0  AP2      Huawei  10.1.10.122  AirEngine5760-51  nor  0     36S
------------------------------------------------------------------------------------
Total: 2
```

To prevent unauthorized APs from accessing the network, change the AP authentication mode to MAC address authentication.

```
[AC-wlan-view] ap auth-mode mac-auth
```

Step 3 Configure WLAN services.

Configure the SSID profile, security profile, and VAP profile according to the WLAN data plan to ensure that the APs can emit signals for STAs to access.

Create the SSID profile **Huawei** and set the SSID to **Huawei**.

```
[AC-wlan-view] ssid-profile name Huawei
[AC-wlan-ssid-prof-Huawei] ssid Huawei
[AC-wlan-ssid-prof-Huawei] quit
```

Create the security profile **Huawei** and set the password.

```
[AC-wlan-view] security-profile name Huawei
[AC-wlan-sec-prof-Huawei] security wpa-wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-Huawei] quit
```

Create the VAP profile **Huawei**, bind the SSID profile and security profile to the VAP profile, and configure the service VLAN and forwarding mode.

```
[AC-wlan-view] vap-profile name Huawei
[AC-wlan-vap-prof-Huawei] ssid-profile Huawei
[AC-wlan-vap-prof-Huawei] security-profile Huawei
[AC-wlan-vap-prof-Huawei] service-vlan vlan-id 20
[AC-wlan-vap-prof-Huawei] forward-mode direct-forward
[AC-wlan-vap-prof-Huawei] quit
```

Create the regulatory domain profile **Huawei** and set the country code to **CN**.

```
[AC-wlan-view] regulatory-domain-profile name Huawei
[AC-wlan-regulate-domain-Huawei] country-code CN
[AC-wlan-regulate-domain-Huawei] quit
```

Enter the AP group **Huawei**, and bind the regulatory domain profile **Huawei** and VAP profile **Huawei** to the AP group.

```
[AC-wlan-view] ap-group name Huawei
[AC-wlan-ap-group-Huawei] regulatory-domain-profile Huawei
Warning: Modifying the country code will clear channel, power and antenna gain c
onfigurations of the radio and reset the AP. Continue?[Y/N]: y
[AC-wlan-ap-group-Huawei] vap-profile Huawei wlan 1 radio all
[AC-wlan-ap-group-Huawei] quit
```

----End

3.3 Verification

3.3.1 Verifying that the APs Emit Signals

Run the **display vap ssid Huawei** command on the AC. The command output shows that both APs send dual-band signals.

```
[AC-wlan-view] display vap ssid Huawei
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID              Status  Auth type       STA  SSID
--------------------------------------------------------------------------------
0     AP1     0    1    00E0-FC1F-4EE0 ON        WPA/WPA2-PSK    0    Huawei
0     AP1     1    1    00E0-FC1F-4EF0 ON        WPA/WPA2-PSK    0    Huawei
1     AP2     0    1    00E0-FC54-64A0 ON        WPA/WPA2-PSK    0    Huawei
1     AP2     1    1    00E0-FC54-64B0 ON        WPA/WPA2-PSK    0    Huawei
--------------------------------------------------------------------------------
Total: 4
```

3.3.2 Testing STA Connections and Network Connectivity

Connect a STA to an AP and ping R1 from the STA to test network connectivity.

```
STA> ping 10.1.30.1
Ping 10.1.30.1: 32 data bytes, Press Ctrl_C to break
From 10.1.30.1: bytes=32 seq=1 ttl=254 time=157 ms
From 10.1.30.1: bytes=32 seq=2 ttl=254 time=171 ms
From 10.1.30.1: bytes=32 seq=3 ttl=254 time=157 ms
From 10.1.30.1: bytes=32 seq=4 ttl=254 time=156 ms
From 10.1.30.1: bytes=32 seq=5 ttl=254 time=156 ms
--- 10.1.30.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 156/159/171 ms
```

3.4 Configuration Reference

3.4.1 Configuration on SW1

```
#
sysname SW1
#
vlan batch 10 20 30
#
dhcp enable
#
interface Vlanif20
 ip address 10.1.20.1 255.255.255.0
```

```
 dhcp select interface
#
interface Vlanif30
 ip address 10.1.30.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

3.4.2 Configuration on SW2

```
#
sysname SW2
#
vlan batch 10 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 20
return
```

3.4.3 Configuration on the AC

```
#
 sysname AC
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
 dhcp select interface
```

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
capwap source ip-address 10.1.10.1
#
wlan
security-profile name Huawei
  security wpa-wpa2 psk pass-phrase %^%#6z\~7+HUhK[FjBC!)3gUEvFu>@],Y)]H))N.RiI@
%^%# aes
ssid-profile name Huawei
  ssid Huawei
vap-profile name Huawei
  service-vlan vlan-id 20
  ssid-profile Huawei
  security-profile Huawei
regulatory-domain-profile name Huawei
ap-group name Huawei
  regulatory-domain-profile Huawei
  radio 0
   vap-profile Huawei wlan 1
  radio 1
   vap-profile Huawei wlan 1
  radio 2
   vap-profile Huawei wlan 1
ap-id 0 type-id 61 ap-mac 00e0-fc1f-4ee0 ap-sn 210235448310CE11E816
  ap-name AP1
  ap-group Huawei
 ap-id 1 type-id 61 ap-mac 00e0-fc54-64a0 ap-sn 21023544831065281D1F
  ap-name AP2
  ap-group Huawei
#
return
```

3.4.4 Configuration on R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.1.30.1 255.255.255.0
#
ip route-static 10.1.20.0 255.255.255.0 10.1.30.2
#
return
```

4 WLAN Layer 3 Off-Path Networking (CLI)

4.1 Introduction

4.1.1 About This Lab

In WLAN Layer 3 networking, the off-path deployment is an overlay networking mode, which requires little reconstruction on the live network and is easy to deploy. You can select the direct or tunnel forwarding mode according to networking requirements.

4.1.2 Objectives

- Understand the Layer 3 networking mode.
- Understand the advantages of off-path networking.
- Learn how to configure WLAN services.

4.1.3 Networking Topology

The following uses AC2 as an example to describe the topology. If you use AC1, pay attention to the interface numbers of SW1. In this document, AC1 and AC2 are collectively referred to as ACs.

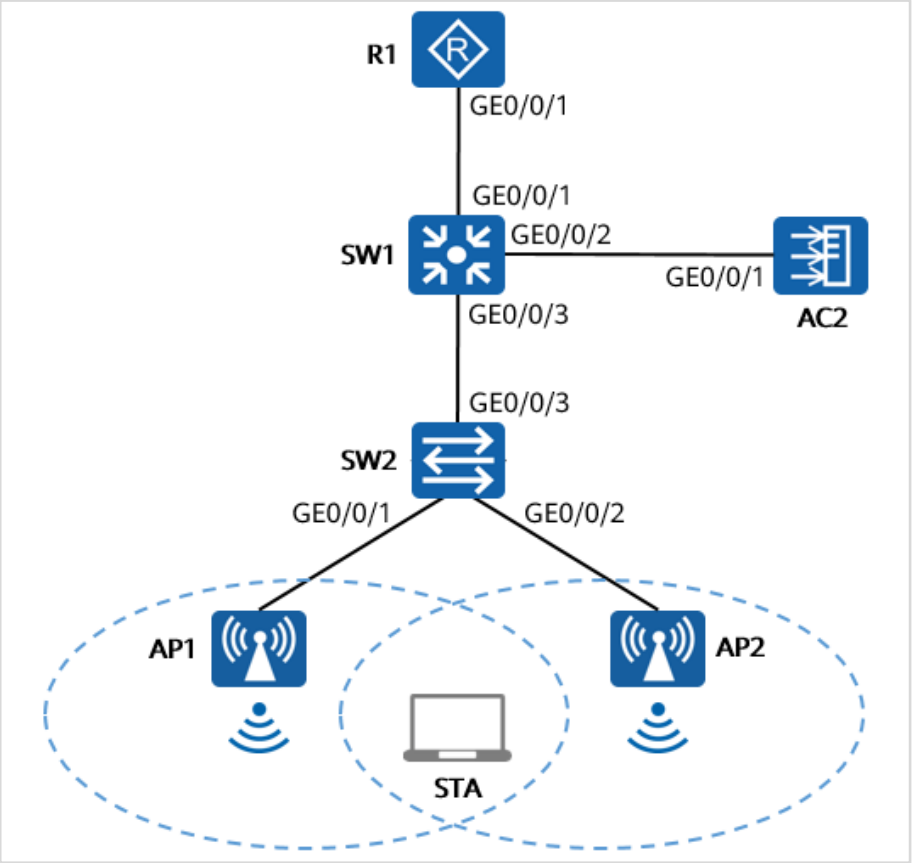


Figure 4-1 WLAN Layer 3 off-path networking topology

4.1.4 Lab Planning

This lab aims to deploy Layer 3 bypass networking, with SW1 as the gateway of both APs and STAs. Enterprise employees and guests are provided network services.

Table 4-1 VLAN Port Types and Parameters

Device	Port	Port Type	VLAN Settings
SW1	GE0/0/1	Access	PVID: VLAN 50
	GE0/0/2	Trunk	PVID: 1 Allow-pass: VLANs 20 and 60
	GE0/0/3	Trunk	PVID: 1 Allow-pass: VLANs 10 and 30
SW2	GE0/0/1	Trunk	PVID: VLAN 10 Allow-pass: VLANs 10 and 30
	GE0/0/2	Trunk	PVID: VLAN 10 Allow-pass: VLANs 10 and 30
	GE0/0/3	Trunk	PVID: 1

			Allow-pass: VLANs 10 and 30
AC	GE0/0/1	Trunk	PVID: VLAN 1 Allow-pass: VLANs 20 and 60

Table 4-2 IP Address Plan

Device	Interface	IP Address
R1	GE0/0/1	10.1.50.1/24
SW1	Vlanif 10	10.1.10.1/24
	Vlanif 20	10.1.20.1/24
	Vlanif 30	10.1.30.2/24
	Vlanif 50	10.1.50.2/24
	Vlanif 60	10.1.60.2/24
AC	Vlanif 60	10.1.60.1/24
	Loopback 0	10.10.10.10/32

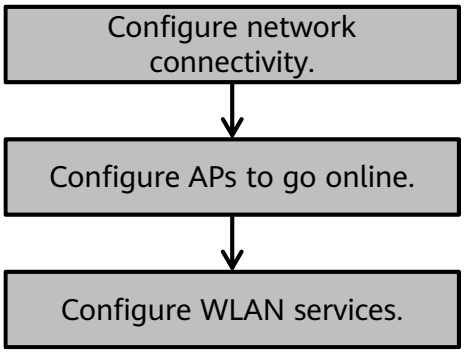
Table 4-3 WLAN Data Plan

Item	Configuration	
DHCP server	SW1 functions as a DHCP server to assign IP addresses to APs and STAs and as their gateway.	
IP address pool for APs	10.1.10.2–10.1.10.254/24	
IP address pool for STAs	Employee: 10.1.20.2–10.1.20.254/24 Guest: 10.1.30.2–10.1.30.254/24	
AC's source interface address	Loopback 0	
AP group	Name: Huawei Referenced profiles: VAP profile and regulatory domain profile	
Regulatory domain profile	Name: Huawei Country code: CN	
SSID profile	Name: Employee SSID name: Employee	Name: Guest SSID name: Guest

Security profile	Name: Employee Security policy: WPA2+PSK+AES Password: a1234567	Name: Guest Security policy: open system
VAP profile	Name: Employee Forwarding mode: tunnel forwarding Service VLAN: VLAN 20 Referenced profiles: SSID profile and security profile	Name: Guest Forwarding mode: direct forwarding Service VLAN: VLAN 30 Referenced profiles: SSID profile and security profile

4.2 Lab Procedure

4.2.1 Configuration Roadmap



4.2.2 Configuration Procedure

Step 1 Configure network connectivity.

Configure VLANs and interface types on the devices to ensure that services can be transparently transmitted at Layer 2.

Create VLANs 10, 20, 30, 50, and 60 on SW1.

```
<Huawei> system-view
[Huawei] sysname SW1
[SW1] vlan batch 10 20 30 50 60
```

Configure interface types on SW1 and configure SW1 to allow packets from the corresponding VLANs to pass through according to Table 4-1.

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 50
[SW1-GigabitEthernet0/0/1] quit
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
```

```
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 20 60
[SW1-GigabitEthernet0/0/2] quit
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 30
[SW1-GigabitEthernet0/0/3] quit
```

Create VLAN 10 and VLAN 30 on SW2.

```
<Huawei> system-view
[Huawei] sysname SW2
[SW2] vlan batch 10 30
```

Configure interface types on SW2 and configure SW2 to allow packets from the corresponding VLANs to pass through according to Table 4-1.

```
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk
[SW2-GigabitEthernet0/0/1] port trunk pvid vlan 10
[SW2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 30
[SW2-GigabitEthernet0/0/1] quit
[SW2] interface GigabitEthernet 0/0/2
[SW2-GigabitEthernet0/0/2] port link-type trunk
[SW2-GigabitEthernet0/0/2] port trunk pvid vlan 10
[SW2-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 30
[SW2-GigabitEthernet0/0/2] quit
[SW2] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type trunk
[SW2-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 30
[SW2-GigabitEthernet0/0/3] quit
```

Create VLAN 20 and VLAN 60 on the AC.

```
<AirEngine9700-M> system-view
[AirEngine9700-M] sysname AC
[AC] vlan batch 20 60
```

Configure interface types on the AC and configure the AC to allow packets from the corresponding VLANs to pass through according to Table 4-1.

```
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 60
[AC-GigabitEthernet0/0/1] quit
```

Configure IP addresses and routing information on the devices to ensure network connectivity.

Create Vlanif interfaces on SW1 and configure IP addresses for them.

```
[SW1] interface Vlanif 10
[SW1-Vlanif10] ip address 10.1.10.1 24
[SW1-Vlanif10] quit
```

```
[SW1] interface Vlanif 20
[SW1-Vlanif20] ip address 10.1.20.1 24
[SW1-Vlanif20] quit
[SW1] interface Vlanif 30
[SW1-Vlanif30] ip address 10.1.30.1 24
[SW1-Vlanif30] quit
[SW1] interface Vlanif 50
[SW1-Vlanif50] ip address 10.1.50.2 24
[SW1-Vlanif50] quit
[SW1] interface Vlanif 60
[SW1-Vlanif60] ip address 10.1.60.2 24
[SW1-Vlanif60] quit
```

Create Vlanif 60 and loopback 0 on the AC and configure IP addresses for them.

```
[AC] interface Vlanif 60
[AC-Vlanif60] ip address 10.1.60.1 24
[AC-Vlanif60] quit
[AC] interface LoopBack 0
[AC-LoopBack0] ip address 10.10.10.10 32
[AC-LoopBack0] quit
```

On R1, configure an IP address for the interface connected to SW1 and create a static route destined for the STA network segment.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1] ip address 10.1.50.1 24
[R1-GigabitEthernet0/0/1] quit
[R1] ip route-static 10.1.20.0 24 10.1.50.2
[R1] ip route-static 10.1.30.0 24 10.1.50.2
```

Ping the IP address 10.1.20.1 on R1 from SW1. The ping operation succeeds.

```
[SW1] ping -a 10.1.20.1 10.1.50.1
  PING 10.1.50.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.50.1: bytes=56 Sequence=1 ttl=255 time=90 ms
    Reply from 10.1.50.1: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.1.50.1: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 10.1.50.1: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.1.50.1: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 10.1.50.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/46/90 ms
```

Step 2 Configure APs to go online.

Configure a DHCP server to assign IP addresses to APs and STAs.

Enable DHCP and create an IP address pool for APs on SW1.

```
[SW1] dhcp enable
[SW1] ip pool ap
[SW1-ip-pool-ap] network 10.1.10.0 mask 24
[SW1-ip-pool-ap] gateway-list 10.1.10.1
[SW1-ip-pool-ap] option 43 sub-option 2 ip-address 10.10.10.10
[SW1-ip-pool-ap] quit
```

Create an address pool for employees and guests on SW1.

```
[SW1] ip pool employee
[SW1-ip-pool-employee] network 10.1.20.0 mask 24
[SW1-ip-pool-employee] gateway-list 10.1.20.1
[SW1-ip-pool-employee] dns-list 114.114.114.114
[SW1-ip-pool-employee] quit
[SW1] ip pool guest
[SW1-ip-pool-guest] network 10.1.30.0 mask 24
[SW1-ip-pool-guest] gateway-list 10.1.30.1
[SW1-ip-pool-guest] dns-list 114.114.114.114
[SW1-ip-pool-guest] quit
```

Enable the global address pool function on the Vlanif interfaces of SW1.

```
[SW1] interface Vlanif 10
[SW1-Vlanif10] dhcp select global
[SW1-Vlanif10] quit
[SW1] interface Vlanif 20
[SW1-Vlanif20] dhcp select global
[SW1-Vlanif20] quit
[SW1] interface Vlanif 30
[SW1-Vlanif30] dhcp select global
[SW1-Vlanif30] quit
```

Configure the AC's source interface address and configure a proper AP authentication mode so that the APs can go online normally.

Configure loopback 0 as the AC's source interface.

```
[AC] capwap source interface LoopBack 0
```

Create an AP group named **Huawei** on the AC.

```
[AC] wlan
[AC-wlan-view] ap-group name Huawei
[AC-wlan-ap-group-Huawei] quit
```

Set the AP authentication mode to MAC address authentication, add APs to the AP group, and name them **AP1** and **AP2**.

```
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-mac 00e0-fc41-6340
[AC-wlan-ap-0] ap-name AP1
[AC-wlan-ap-0] ap-group Huawei
Warning: This operation may cause AP reset. If the country code changes, it will
```

```
 clear channel, power and antenna gain configurations of the radio, Whether to c
ontinue? [Y/N]: y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-mac 00e0-fca2-5970
[AC-wlan-ap-1] ap-name AP2
[AC-wlan-ap-1] ap-group Huawei
Warning: This operation may cause AP reset. If the country code changes, it will
 clear channel, power and antenna gain configurations of the radio, Whether to c
ontinue? [Y/N]: y
[AC-wlan-ap-1] quit
```

Run the **display ap all** command to check the AP online status. The command output shows that the two APs are not online.

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
idle : idle              [2]
------------------------------------------------------------------------------
ID   MAC            Name      Group     IP    Type      State      STA  Uptime
------------------------------------------------------------------------------
0    00e0-fc41-6340 AP1       Huawei    -     -         idle       0    -
1    00e0-fca2-5970 AP2       Huawei    -     -         idle       0    -
------------------------------------------------------------------------------
Total: 2
```

Troubleshoot the fault and find that the reason is that the APs fail to communicate with the AC's source address.

On SW1, add a route to the AC's source address. On the AC, add a route to the AP network segment.

```
[SW1] ip route-static 10.10.10.10 32 10.1.60.1
[AC] ip route-static 10.1.10.0 24 10.1.60.2
```

Wait for a period of time, and then run the **display ap all** command to check the AP online status. The command output shows that the two APs have gone online.

```
[AC] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal            [2]
------------------------------------------------------------------------------------------------------------------
ID   MAC            Name      Group     IP            Type                State      STA  Uptime
------------------------------------------------------------------------------------------------------------------
0    00e0-fc41-6340 AP1       Huawei    10.1.10.253   AirEngine5760-51    nor        0    9S
1    00e0-fca2-5970 AP2       Huawei    10.1.10.254   AirEngine5760-51    nor        0    10S
------------------------------------------------------------------------------------------------------------------
Total: 2
```

Step 3 Configure WLAN services.

Configure the SSID profile, security profile, and VAP profile according to the WLAN data plan to ensure that the APs can emit signals for STAs to access.

Create SSID profiles **Employee** and **Guest**, and set the SSIDs to **Employee** and **Guest**, respectively.

```
[AC-wlan-view] ssid-profile name Employee
[AC-wlan-ssid-prof-Employee] ssid Employee
[AC-wlan-ssid-prof-Employee] quit
[AC-wlan-view] ssid-profile name Guest
[AC-wlan-ssid-prof-Guest] ssid Guest
[AC-wlan-ssid-prof-Guest] quit
```

Create security profiles **Employee** and **Guest**, and configure their security policies.

```
[AC-wlan-view] security-profile name Employee
[AC-wlan-sec-prof-Employee] security wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-Employee] quit
[AC-wlan-view] security-profile name Guest
[AC-wlan-sec-prof-Guest] security open
[AC-wlan-sec-prof-Guest] quit
```

Create VAP profiles **Employee** and **Guest**, and configure them according to the WLAN data plan.

```
[AC-wlan-view] vap-profile name Employee
[AC-wlan-vap-prof-Employee] ssid-profile Employee
[AC-wlan-vap-prof-Employee] security-profile Employee
[AC-wlan-vap-prof-Employee] service-vlan vlan-id 20
[AC-wlan-vap-prof-Employee] forward-mode tunnel
[AC-wlan-vap-prof-Employee] quit
[AC-wlan-view] vap-profile name Guest
[AC-wlan-vap-prof-Guest] ssid-profile Guest
[AC-wlan-vap-prof-Guest] security-profile Guest
[AC-wlan-vap-prof-Guest] service-vlan vlan-id 30
[AC-wlan-vap-prof-Guest] forward-mode direct-forward
[AC-wlan-vap-prof-Guest] quit
```

Create the regulatory domain profile **Huawei** and set the country code to **CN**.

```
[AC-wlan-view] regulatory-domain-profile name Huawei
[AC-wlan-regulate-domain-Huawei] country-code CN
[AC-wlan-regulate-domain-Huawei] quit
```

Enter the AP group **Huawei**, and bind the regulatory domain profile **Huawei** and VAP profiles **Employee** and **Guest** and to the AP group.

```
[AC-wlan-view] ap-group name Huawei
[AC-wlan-ap-group-Huawei] regulatory-domain-profile Huawei
Warning: Modifying the country code will clear channel, power and antenna gain c
onfigurations of the radio and reset the AP. Continue?[Y/N]: y
[AC-wlan-ap-group-Huawei] vap-profile Employee wlan 1 radio all
[AC-wlan-ap-group-Huawei] vap-profile Guest wlan 2 radio all
[AC-wlan-ap-group-Huawei] quit
```

----End

4.3 Verification

4.3.1 Verifying that the APs Emit Signals

Run the **display vap ssid Employee** command on the AC. The command output shows that both APs send dual-band signals.

```
[AC-wlan-view] display vap ssid Employee
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID              Status  Auth type   STA   SSID
--------------------------------------------------------------------------------
0     AP1     0    1    00E0-FC41-6340 ON      WPA2-PSK    0     Employee
0     AP1     1    1    00E0-FC41-6350 ON      WPA2-PSK    0     Employee
1     AP2     0    1    00E0-FCA2-5970 ON      WPA2-PSK    0     Employee
1     AP2     1    1    00E0-FCA2-5980 ON      WPA2-PSK    0     Employee
--------------------------------------------------------------------------------
Total: 4

[AC-wlan-view] display vap ssid Guest
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID              Status  Auth type   STA   SSID
--------------------------------------------------------------------------------
0     AP1     0    2    00E0-FC41-6341 ON      Open        0     Guest
0     AP1     1    2    00E0-FC41-6351 ON      Open        0     Guest
1     AP2     0    2    00E0-FCA2-5971 ON      Open        0     Guest
1     AP2     1    2    00E0-FCA2-5981 ON      Open        0     Guest
--------------------------------------------------------------------------------
Total: 4
```

4.3.2 Testing STA Connections and Network Connectivity

Connect a STA to the two SSIDs, and ping R1 from the STA to test network connectivity.

```
STA> ping 10.1.50.1
Ping 10.1.50.1: 32 data bytes, Press Ctrl_C to break
From 10.1.50.1: bytes=32 seq=1 ttl=254 time=234 ms
From 10.1.50.1: bytes=32 seq=2 ttl=254 time=172 ms
From 10.1.50.1: bytes=32 seq=3 ttl=254 time=203 ms
From 10.1.50.1: bytes=32 seq=4 ttl=254 time=188 ms
From 10.1.50.1: bytes=32 seq=5 ttl=254 time=203 ms
--- 10.1.50.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 172/200/234 ms
```

4.4 Configuration Reference

4.4.1 Configuration on SW1

```
#
sysname SW1
#
vlan batch 10 20 30 50 60
#
dhcp enable
#
ip pool ap
 gateway-list 10.1.10.1
 network 10.1.10.0 mask 255.255.255.0
 option 43 sub-option 2 ip-address 10.10.10.10
#
ip pool employee
 gateway-list 10.1.20.1
 network 10.1.20.0 mask 255.255.255.0
 dns-list 114.114.114.114
#
ip pool guest
 gateway-list 10.1.30.1
 network 10.1.30.0 mask 255.255.255.0
 dns-list 114.114.114.114
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
 dhcp select global
#
interface Vlanif20
 ip address 10.1.20.1 255.255.255.0
 dhcp select global
#
interface Vlanif30
 ip address 10.1.30.1 255.255.255.0
 dhcp select global
#
interface Vlanif50
 ip address 10.1.50.2 255.255.255.0
#
interface Vlanif60
 ip address 10.1.60.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 50
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 60
#
interface GigabitEthernet0/0/3
 port link-type trunk
```

```
 port trunk allow-pass vlan 10 30
#
ip route-static 10.10.10.10 255.255.255.255 10.1.60.1
#
return
```

4.4.2 Configuration on SW2

```
#
sysname SW2
#
vlan batch 10 30
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 30
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 30
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 30
#
return
```

4.4.3 Configuration on the AC

```
#
 sysname AC
#
vlan batch 20 60
#
interface Vlanif60
 ip address 10.1.60.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 60
#
interface LoopBack0
 ip address 10.10.10.10 255.255.255.255
#
ip route-static 10.1.10.0 255.255.255.0 10.1.60.2
#
capwap source interface loopback0
#
wlan
security-profile name Guest
security-profile name Employee
```

```
  security wpa2 psk pass-phrase %^%#AD:[8l4P;UxL2B9*`b4H+Bj}AXMFiI+mr-,nFy|D%^%#
 aes
ssid-profile name Guest
  ssid Guest
 ssid-profile name Employee
  ssid Employee
 vap-profile name Guest
  service-vlan vlan-id 30
  ssid-profile Guest
  security-profile Guest
vap-profile name Employee
  forward-mode tunnel
  service-vlan vlan-id 20
  ssid-profile Employee
  security-profile Employee
regulatory-domain-profile name Huawei
ap-group name Huawei
  regulatory-domain-profile Huawei
  radio 0
   vap-profile Employee wlan 1
   vap-profile Guest wlan 2
  radio 1
   vap-profile Employee wlan 1
   vap-profile Guest wlan 2
  radio 2
   vap-profile Employee wlan 1
   vap-profile Guest wlan 2
ap-id 0 type-id 61 ap-mac 00e0-fc41-6340 ap-sn 210235448310B37A293B
  ap-name AP1
  ap-group Huawei
 ap-id 1 type-id 61 ap-mac 00e0-fca2-5970 ap-sn 210235448310FD475B70
  ap-name AP2
  ap-group Huawei
#
return
```

4.4.4 Configuration on R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.1.50.1 255.255.255.0
#
ip route-static 10.1.20.0 255.255.255.0 10.1.50.2
ip route-static 10.1.30.0 255.255.255.0 10.1.50.2
#
return
```

5 WLAN RRM

5.1 Introduction

5.1.1 About This Lab

An enterprise deploys a WLAN at its reception hall and requires the WLAN service for both employees and guests. To ensure good Internet access experience for users, simple radio calibration on the WLAN is required.

5.1.2 Objectives

- Understand the basic principles of radio calibration.
- Know how to configure RRM.

5.1.3 Networking Topology

The following uses AC2 as an example to describe the topology. If you use AC1, pay attention to the interface numbers of SW1. In this document, AC1 and AC2 are collectively referred to as ACs.

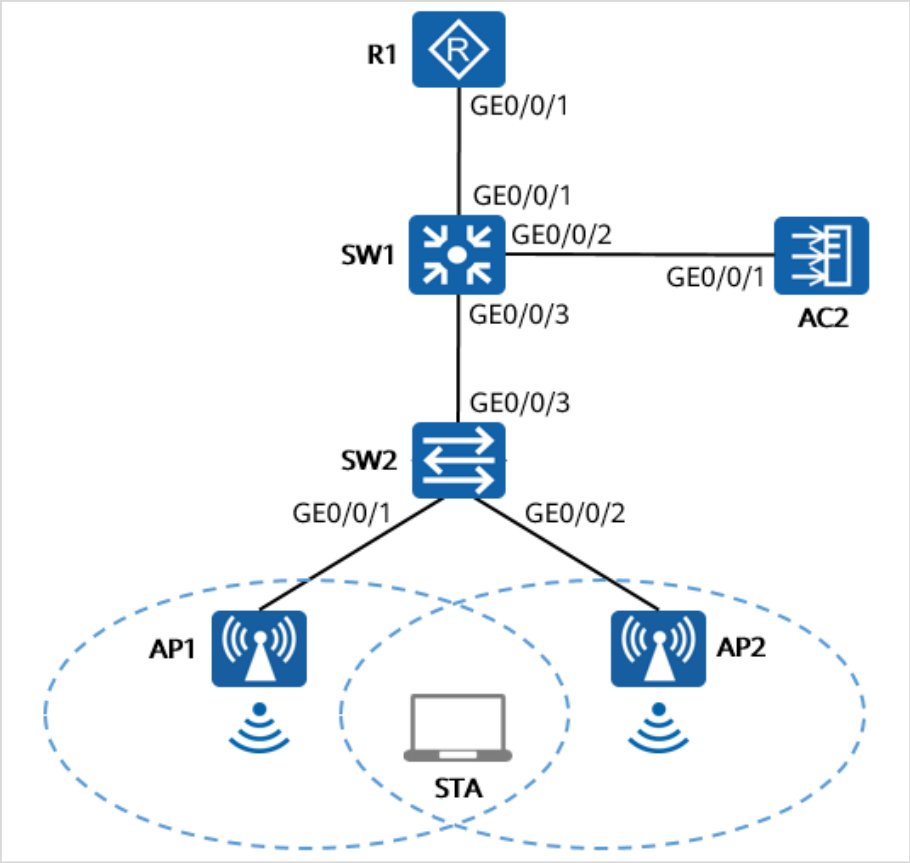


Figure 5-1 WLAN RRM topology

5.1.4 Lab Planning

Table 5-1 Radio parameters

Item	Parameter
Channel	2.4 GHz AP1: 1; AP2: 6
Channel bonding	5 GHz AP1: 40 MHz; AP2: 40 MHz

5.2 Lab Procedure

5.2.1 Configuration Roadmap

Perform radio calibration.

5.2.2 Configuration Procedure

Step 1 Perform radio calibration.

Adjust the radio parameters according to Table 5-1.

For the 2.4 GHz radio, set AP1's channel to 1 and AP2's channel to 6.

```
[AC] wlan
[AC-wlan-view] ap-name AP1
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] channel 20mhz 1
Warning: This action may cause service interruption. Continue?[Y/N] y
[AC-wlan-radio-0/0] quit
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-name AP2
[AC-wlan-ap-1] radio 0
[AC-wlan-radio-1/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N] y
[AC-wlan-radio-1/0] quit
[AC-wlan-ap-1] quit
```

Run the **display radio all** command to check the channel status of the APs.

```
[AC-wlan-view] display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
--------------------------------------------------------------------------
AP ID Name   RfID  Band  Type     ST  CH/BW          CE/ME   STA    CU
--------------------------------------------------------------------------
0     AP1    0     2.4G  bgn      on  1/20M          -/-     0      0%
0     AP1    1     5G    an11ac   on  149/20M        -/-     0      0%
1     AP2    0     2.4G  bgn      on  6/20M          -/-     0      0%
1     AP2    1     5G    an11ac   on  149/20M        -/-     0      0%
--------------------------------------------------------------------------
Total:4
```

To improve user experience and network throughput, bond channels on the 5 GHz frequency band.

```
[AC-wlan-view] ap-name AP1
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] channel 40mhz-plus 36
Warning: This action may cause service interruption. Continue?[Y/N] y
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-name AP2
[AC-wlan-ap-1] radio 1
[AC-wlan-radio-1/1] channel 40mhz-plus 44
Warning: This action may cause service interruption. Continue?[Y/N] y
[AC-wlan-radio-1/1] quit
[AC-wlan-ap-1] quit
```

5.3 Verification

5.3.1 Checking AP Radio Information

Run the **display radio all** command to check radio information about the APs.

```
[AC-wlan-view] display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
------------------------------------------------------------------------------
AP ID Name   RfID  Band  Type     ST  CH/BW          CE/ME   STA     CU
------------------------------------------------------------------------------
0     AP1    0     2.4G  bgn      on  1/20M          -/-     0       0%
0     AP1    1     5G    an11ac   on  36/40M+        -/-     0       0%
1     AP2    0     2.4G  bgn      on  6/20M          -/-     0       0%
1     AP2    1     5G    an11ac   on  44/40M+        -/-     0       0%
------------------------------------------------------------------------------
Total:4
```

5.4 Configuration Reference

5.4.1 Configuration on the AC

```
ap-id 0 type-id 61 ap-mac 00e0-fcbe-1fd0 ap-sn 210235448310181CFE48
  ap-name AP1
  ap-group Huawei
  radio 0
   channel 20mhz 1
  radio 1
   channel 40mhz-plus 36
 ap-id 1 type-id 61 ap-mac 00e0-fc5a-7fd0 ap-sn 210235448310CF70816B
  ap-name AP2
  ap-group Huawei
  radio 0
   channel 20mhz 6
  radio 1
   channel 40mhz-plus 44
```

6 WLAN Troubleshooting Basics

6.1 Introduction

6.1.1 About This Lab

Wired LANs are expensive and lack mobility. The increasing demand for portability and mobility requires WLAN technologies. As the most cost-efficient and convenient network access mode nowadays, WLAN allows users to freely move within the covered area.

Common faults on a WLAN include AP join failures, STA access faults, and other faults caused by incorrect configurations. This lab aims to introduce the basic WLAN troubleshooting process and configuration based on typical AC + Fit AP networking.

6.1.2 Objectives

- Understand the basic WLAN troubleshooting process.
- Know common WLAN troubleshooting commands.

6.1.3 Networking Topology

The following uses AC1 as an example to describe the topology. If you use AC2, pay attention to the interface numbers of SW1. In this document, AC1 and AC2 are collectively referred to as ACs.

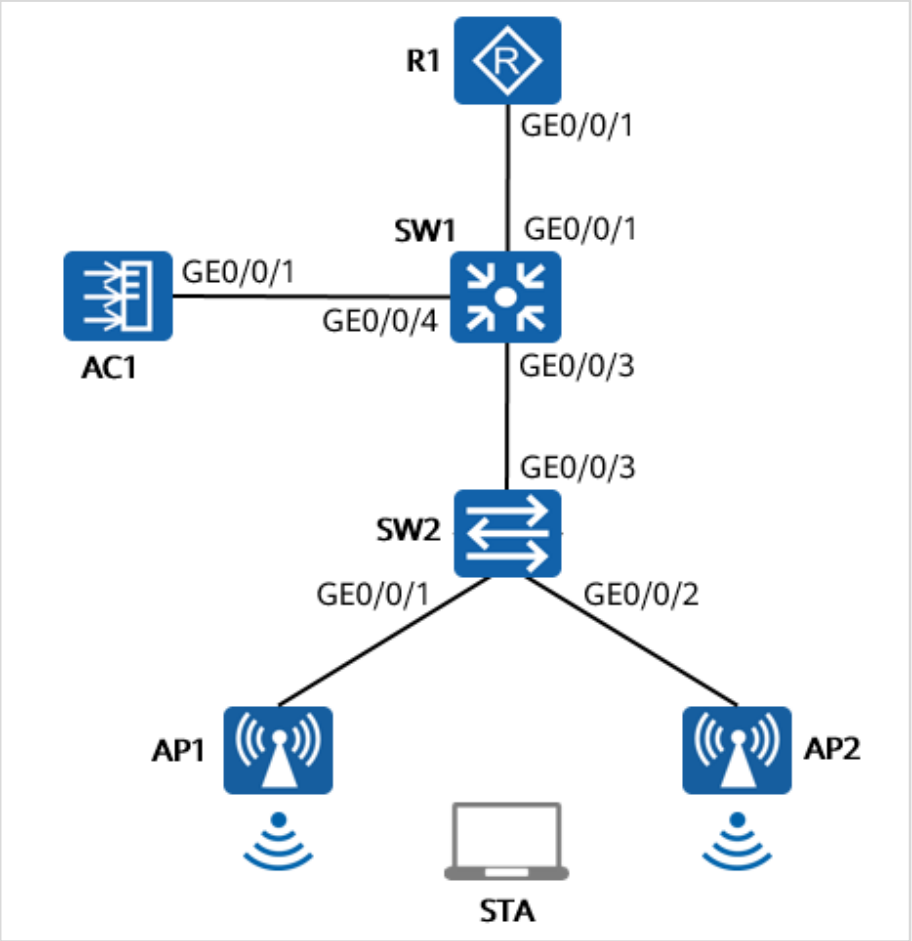


Figure 6-1 WLAN troubleshooting basic topology

6.1.4 Data Planning

In this experiment, Layer 2 bypass networking is used. The management VLAN of the AC and AP is VLAN 100. The AC functions as the DHCP server to assign IP addresses to APs. The service VLAN is planned as VLAN 200. SW1 functions as the DHCP server to allocate IP addresses to STAs. Data is forwarded in direct forwarding mode.

Table 6-1 VLAN planning

Device	Port	Port Type	VLAN Settings
SW1	GE0/0/1	Access	PVID: VLAN 50
	GE0/0/3	Trunk	PVID:1 Allow-pass: VLAN 100 200
	GE0/0/4	Trunk	PVID:1 Allow-pass: VLAN 100 200
SW2	GE0/0/1	Trunk	PVID: VLAN 100 Allow-pass: VLAN 100 200

	GE0/0/2	Trunk	PVID: VLAN 100 Allow-pass: VLAN 100 200
	GE0/0/3	Trunk	PVID:1 Allow-pass: VLAN 100 200
AC	GE0/0/1	Trunk	PVID: VLAN 1 Allow-pass: VLAN 100 200

Table 6-2 IP address planning

Device	Port	IP Address
R1	GE0/0/1	10.1.50.1/24
SW1	Vlanif 100	192.168.100.254/24
	Vlanif 200	192.168.200.254/24
	Vlanif 50	10.1.50.2/24
AC	Vlanif 100	192.168.100.1/24

Table 6-3 AC data planning

Item	Configuration
Management VLAN for APs	VLAN 100
Service VLAN for STAs	VLAN 200
DHCP server	The AC functions as a DHCP server to assign IP addresses to APs.
	SW1 functions as a DHCP server to assign IP addresses to STAs. The default gateway address of STAs is 192.168.200.254.
IP address pool for APs	192.168.100.1-192.168.100.253/24
IP address pool for STAs	192.168.200.1-192.168.200.253/24
AC's source interface address	Vlanif 100: 192.168.100.1/24
AP group	Name: ap-group1
	Referenced profiles: VAP profile HCIA-WLAN and regulatory domain profile default
Regulatory domain profile	Name: default

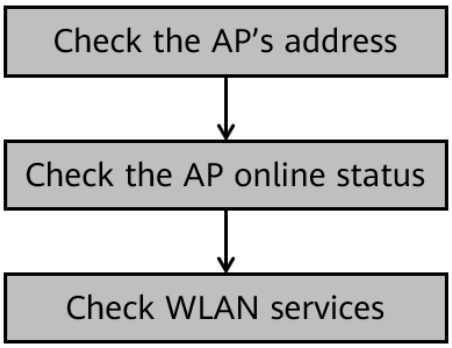
	Country code: CN
SSID profile	Name: HCIA-WLAN
	SSID name: HCIA-WLAN
Security profile	Name: HCIA-WLAN
	Security policy: WPA-WPA2+PSK+AES
	Password: a12345678
VAP profile	Name: HCIA-WLAN
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 200
	Referenced profiles: SSID profile HCIA-WLAN and security profile HCIA-WLAN

6.1.5 Fault Symptom

After the preceding configurations are complete, AP1 and AP2 cannot go online, and STAs cannot search for SSID signals and access the wireless network.

6.2 Lab Procedure

6.2.1 Configuration Roadmap



6.2.2 Configuration Procedure

Step 1 Import the pre-configuration.

Import the pre-configuration of SW1.

```
#
sysname SW1
#
```

```
vlan batch 50 100 200
#
interface Vlanif50
 ip address 10.1.50.2 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
#
interface Vlanif200
 ip address 192.168.200.254 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 50
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

Import the pre-configuration of SW2.

```
#
sysname SW2
#
vlan batch 100 200
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

Import the pre-configuration of AC.

```
#
 sysname AC1
```

```
#
vlan batch 100 200
#
dhcp enable
#
ip pool ap
 gateway-list 192.168.100.1
 network 192.168.100.0 mask 255.255.255.0
 excluded-ip-address 192.168.100.254
#
interface Vlanif100
 shutdown
 ip address 192.168.100.1 255.255.255.0
 #
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
#
capwap source interface vlanif100
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase a12345678 aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
 vap-profile name default
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 200
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-system-profile name default
 ap-group name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap blacklist mac f09b-b861-3a70
 ap-id 0 type-id 130 ap-mac f09b-b861-3a70 ap-sn 2102353GES6RM6019261
  ap-name AP1
  ap-group ap-group1
#
return
```

Import the pre-configuration of R1.

```
#
 sysname R1
#
interface GigabitEthernet0/0/0
#
```

```
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 10.1.50.1 255.255.255.0
#
ip route-static 192.168.0.0 255.255.0.0 10.1.50.2
#
return
```

Step 2 Troubleshoot the AP fails to obtain an IP address.

Log in to the AC and check whether the AP goes online.

```
[AC1] display ap all
--------------------------------------------------------------------------------
ID  MAC                 Name  Group  IP  Type  State  STA  Uptime ExtraInfo
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Total: 0
```

The AP is offline. Before an AP goes online, the AP must obtain an IP address. Therefore, check whether the AP obtains an IP address first. According to the plan, the management VLAN of the AP is 100, and the AC functions as the DHCP server to assign IP addresses to the AP. The following figure shows the DHCP address pool of the AC.

```
[AC1] display ip pool
 --------------------------------------------------------------------------------
  Pool-name            : ap
  Pool-No              : 0
  Lease                : 1 Days 0 Hours 0 Minutes
  Position             : Local
  Status               : Unlocked
  Gateway-0            : 192.168.100.1
  Network              : 192.168.100.0
  Mask                 : 255.255.255.0
  Conflicted address recycle interval: -
  Address Statistic: Total          :253          Used           :0
                     Idle           :252          Expired        :0
                     Conflict       :0            Disabled       :1

  IP address Statistic
    Total          :253
    Used           :0            Idle           :252
    Expired        :0            Conflict       :0             Disabled   :1
```

The name of the DHCP address pool on the AC is **ap**, and the address range is 192.168.100.0/24. The configuration is correct. Check the address allocation status, as shown in the following figure.

```
[AC1] display ip pool name ap used
  Pool-name            : ap
  Pool-No              : 0
  Lease                : 1 Days 0 Hours 0 Minutes
  Domain-name          : -
```

```
  DNS-server0         : -
  NBNS-server0        : -
  Netbios-type        : -
  Position            : Local
  Status              : Unlocked
  Gateway-0           : 192.168.100.1
  Network             : 192.168.100.0
  Mask                : 255.255.255.0
  Logging             : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253          Used          :0
                     Idle           :252          Expired       :0
                     Conflict       :0            Disabled      :1

 ------------------------------------------------------------------------------
  Network section
          Start           End           Total     Used Idle(Expired) Conflict Disabled
 ------------------------------------------------------------------------------
    192.168.100.1 192.168.100.254       253        0          252(0)        0        1
 ------------------------------------------------------------------------------
```

The query result shows that the DHCP server does not assign any IP address. The network configuration of the queried interface is as follows:

```
[AC1] display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 1

Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/47                    169.254.3.1/24       up         up
NULL0                             unassigned           up         up(s)
Vlanif1                           169.254.1.1/24       up         up
Vlanif100                         192.168.100.1/24     *down      down
```

```
[AC1] display current-configuration interface vlan100
#
interface Vlanif100
 shutdown
 ip address 192.168.100.1 255.255.255.0
```

The command output shows that Vlanif100 is shut down by the administrator and the DHCP service is not enabled on the interface. You need to manually enable the interface and enable the DHCP service. The configuration is as follows:

```
[AC1] interface vlan100
```

```
[AC1-Vlanif100] dhcp select global
[AC1-Vlanif100] undo shutdown
[AC1-Vlanif100] quit
```

Check the address allocation of the DHCP server.

```
[AC1] display ip pool name ap used
  Pool-name            : ap
  Pool-No              : 0
  Lease                : 1 Days 0 Hours 0 Minutes
  Domain-name          : -
  DNS-server0          : -
  NBNS-server0         : -
  Netbios-type         : -
  Position             : Local
  Status               : Unlocked
  Gateway-0            : 192.168.100.1
  Network              : 192.168.100.0
  Mask                 : 255.255.255.0
  Logging              : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253          Used          :1
                     Idle           :251          Expired       :0
                     Conflict       :0            Disabled      :1

--------------------------------------------------------------------------------
 Network section
         Start            End          Total      Used Idle(Expired) Conflict Disabled
--------------------------------------------------------------------------------
   192.168.100.1 192.168.100.254       253          1          251(0)          0        1
--------------------------------------------------------------------------------
Client-ID format as follows:
   DHCP   : mac-address                    PPPoE    : mac-address
   IPSec : user-id/portnumber/vrf          PPP      : interface index
   L2TP   : cpu-slot/session-id            SSL-VPN : user-id/session-id
--------------------------------------------------------------------------------
 Index                IP                Client-ID      Type          Left     Status
--------------------------------------------------------------------------------
     95   192.168.100.96          f4de-af36-acc0      DHCP         86303    Used
--------------------------------------------------------------------------------
```

It is found that only one AP obtains an IP address and the MAC address is AP2's MAC address, but AP1 still does not obtain an IP address. Therefore, the DHCP server is not faulty. Check the configuration of the interface connecting SW2 to AP1, as shown in the following figure.

```
[SW2] display current-configuration interface g0/0/1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
```

The command output shows that the PVID of GigabitEthernet0/0/1 is not set to VLAN 100. The manual configuration is as follows:

```
[SW2] interface GigabitEthernet0/0/1
[SW2-GigabitEthernet0/0/1] port trunk pvid vlan 100
[SW2-GigabitEthernet0/0/1] quit
```

Check the address allocation. Both APs have obtained IP addresses.

```
[AC1] display ip pool name ap used
...
Client-ID format as follows:
    DHCP   : mac-address                    PPPoE    : mac-address
    IPSec : user-id/portnumber/vrf        PPP       : interface index
    L2TP   : cpu-slot/session-id           SSL-VPN : user-id/session-id
 ------------------------------------------------------------------------------
  Index                IP              Client-ID      Type         Left    Status
 ------------------------------------------------------------------------------
     95   192.168.100.96          f4de-af36-acc0     DHCP        86356    Used
     99   192.168.100.100         f09b-b861-3a70     DHCP        86325    Used
 ------------------------------------------------------------------------------
```

Step 3 Troubleshoot the APs' onboarding failures.

After the AP obtains the IP address, check whether the AP is online on the AC.

```
[AC1] display ap all
Total AP information:
idle   : idle                [1]
unauth: unauthed            [1]
ExtraInfo : Extra information
P       : insufficient power supply
-------------------------------------------------------------------------------------------
ID      MAC                Name Group       IP Type                State   STA   Uptime ExtraInfo
-------------------------------------------------------------------------------------------
-       f4de-af36-acc0 -      -            -   AirEngine5760-51       unauth  -     -        -
0       f09b-b861-3a70 AP1    ap-group1 -   AirEngine5760-51       idle      0     -        -
-------------------------------------------------------------------------------------------
Total: 2
```

Two APs are offline and their states are **unauth** and **idle**. Therefore, You need to further query the detailed reasons for APs' onboarding failures, as shown in the following figure:

```
[AC1] display ap online-fail-record all
Info: This operation may take a few seconds. Please wait for a moment.done.
------------------------------------------------------------------------------
MAC                 Last fail time              Reason
------------------------------------------------------------------------------
f09b-b861-3a70   XXXX-XX-XX/17:40:38        The AP is added to the AP blacklist
f4de-af36-acc0   XXXX-XX-XX /17:40:11       The AP is not in the MAC whitelist
------------------------------------------------------------------------------
Total APs: 2 Total records: 2
```

The AP with the MAC address f09b-b861-3a70 (AP1) is added to the blacklist, and the AP with the MAC address f4de-af36-acc0 (AP2) is not added to the whitelist.

Remove AP1 from the blacklist.

```
[AC1] wlan
[AC1-wlan-view] undo ap blacklist mac f09b-b861-3a70
```

Manually add AP2 to the MAC address authentication list and configure the AP name and AP group.

```
[AC1-wlan-view] ap-id 1 ap-mac f4de-af36-acc0
[AC1-wlan-ap-1] ap-name AP2
[AC1-wlan-ap-1] ap-group ap-group1
[AC1-wlan-ap-1] quit
[AC1-wlan-view] quit
```

Check the APs' onboarding status again.

```
[AC1] display ap all
Total AP information:
nor    : normal              [2]
ExtraInfo : Extra information
P      : insufficient power supply
------------------------------------------------------------------------------------------------------
ID      MAC                Name Group       IP                Type                State  STA  Uptime
ExtraInfo
------------------------------------------------------------------------------------------------------
0       f09b-b861-3a70 AP1   ap-group1 192.168.100.100 AirEngine5760-51 nor     0     3M:48S P
1       f4de-af36-acc0 AP2   ap-group1 192.168.100.96  AirEngine5760-51 nor     0     1M:20S -
------------------------------------------------------------------------------------------------------
Total: 2
```

The command output shows that AP1 and AP2 have gone online and are in the **normal** state.

Step 4 Troubleshoot STAs' failures to detect radio signals.

After the AP goes online successfully, use the STA to search for the **HCIA-WLAN** signal nearby. However, the STA fails to search for the **HCIA-WLAN** signal. Log in to the AC and check the VAP status.

```
[AC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
------------------------------------------------------------------------------
AP ID AP name   RfID WID   BSSID             Status   Auth type       STA    SSID
------------------------------------------------------------------------------
0     AP1       0    1     F09B-B861-3A70 ON       WPA/WPA2-PSK   0      HUAWEI-WLAN
0     AP1       1    1     F09B-B861-3A80 ON       WPA/WPA2-PSK   0      HUAWEI-WLAN
1     AP2       0    1     F4DE-AF36-ACC0 ON       WPA/WPA2-PSK   0      HUAWEI-WLAN
1     AP2       1    1     F4DE-AF36-ACD0 ON       WPA/WPA2-PSK   0      HUAWEI-WLAN
------------------------------------------------------------------------------
Total: 4
```

The SSID associated with the VAP is **HUAWEI-WLAN**. Check the VAP configuration.

```
[AC1] wlan
[AC1-wlan-view] display this
...
 ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 200
  security-profile HCIA-WLAN
...
```

Check the configuration. It is found that the VAP does not reference the SSID profile. Therefore, the manual configuration is as follows:

```
[AC1-wlan-view] vap-profile name HCIA-WLAN
[AC1-wlan-vap-prof-HCIA-WLAN] ssid-profile HCIA-WLAN
Warning: This action may cause service interruption. Continue?[Y/N] y
Info: This operation may take a few seconds, please wait.....done.
[AC1-wlan-vap-prof-HCIA-WLAN] quit
```

Check the VAP status again. The SSID is changed to **HCIA-WLAN**.

```
[AC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name   RfID WID  BSSID              Status  Auth type       STA   SSID
--------------------------------------------------------------------------------
0     AP1       0    1    F09B-B861-3A70 ON       WPA/WPA2-PSK    0     HCIA-WLAN
0     AP1       1    1    F09B-B861-3A80 ON       WPA/WPA2-PSK    0     HCIA-WLAN
1     AP2       0    1    F4DE-AF36-ACC0 ON       WPA/WPA2-PSK    0     HCIA-WLAN
1     AP2       1    1    F4DE-AF36-ACD0 ON       WPA/WPA2-PSK    0     HCIA-WLAN
--------------------------------------------------------------------------------
Total: 4
```

Use the STA to associate with the **HCIA-WLAN** and enter the password **a12345678**. The STA is successfully associated.

Although the STA is successfully associated, it is found that the STA does not obtain an IP address. The WLAN service gateway is located on SW1, and SW1 functions as the DHCP server to assign IP addresses to STAs. Therefore, check the DHCP configuration on SW1, as shown in the following figure.

```
[SW1] display current-configuration | include dhcp
...
[SW1]
```

The command output shows that the DHCP service is not configured on SW1. The manual configuration is as follows:

```
[SW1] dhcp enable
[SW1] interface Vlanif 200
```

```
[SW1-Vlanif200] dhcp select interface
[SW1-Vlanif200] quit
```

Disconnect the STA and re-associate the STA. The STA has obtained an IP address, as shown in the following figure.

```
C:\Users\admin> ipconfig
Wireless LAN adapter WLAN:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.200.232
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.200.254
```

Test the connectivity between the STA and the WLAN service gateway. The **ping** operation is successful, as shown in the following figure.

```
C:\Users\admin> ping 192.168.200.254

Pinging 192.168.200.254 with 32 bytes of data:
Reply from 192.168.200.254: bytes=32 time=6ms TTL=252
Reply from 192.168.200.254: bytes=32 time=5ms TTL=252
Reply from 192.168.200.254: bytes=32 time=5ms TTL=252
Reply from 192.168.200.254: bytes=32 time=6ms TTL=252

Ping statistics for 192.168.200.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss);
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

6.3 Verification

6.3.1 Checking the AP Onboarding Status

Check the AP status on the AC. The AP status is **normal**, indicating that the AP goes online successfully and one STA is associated with AP1, as shown in the following figure.

```
[AC1] display ap all
Total AP information:
nor    : normal              [2]
ExtraInfo : Extra information
P      : insufficient power supply
-------------------------------------------------------------------------------------------------
ID   MAC          Name Group      IP             Type            State STA  Uptime      ExtraInfo
-------------------------------------------------------------------------------------------------
0    f09b-b861-3a70 AP1   ap-group1 192.168.100.100 AirEngine5760-51 nor   1   1H:8M:18S P
1    f4de-af36-acc0 AP2   ap-group1 192.168.100.96  AirEngine5760-51 nor   0   1H:5M:50S -
-------------------------------------------------------------------------------------------------
Total: 2
```

6.3.2 Checking VAP Information

Check the VAP status on the AC. One STA is associated with AP1, as shown in the following figure.

```
[AC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name   RfID WID  BSSID           Status  Auth type       STA   SSID
--------------------------------------------------------------------------------
0     AP1       0    1    F09B-B861-3A70 ON      WPA/WPA2-PSK    0     HCIA-WLAN
0     AP1       1    1    F09B-B861-3A80 ON      WPA/WPA2-PSK    1     HCIA-WLAN
1     AP2       0    1    F4DE-AF36-ACC0 ON      WPA/WPA2-PSK    0     HCIA-WLAN
1     AP2       1    1    F4DE-AF36-ACD0 ON      WPA/WPA2-PSK    0     HCIA-WLAN
--------------------------------------------------------------------------------
Total: 4
```

6.3.3 Checking the STA Access Status

Check the STA access status on the AC.

```
[AC1] display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------------------------
STA MAC      AP ID Ap name   Rf/WLAN  Band  Type  Rx/Tx     RSSI  VLAN  IP address     SSID
--------------------------------------------------------------------------------------------------
081f-7153-906f  0  AP1  1/1  5G  11ac  24/115  -52  200  192.168.200.232  HCIA-WLAN
--------------------------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

6.3.4 Testing Network Connectivity

Ping the service IP address of R1 from the STA. The ping is successful, as shown in the following figure.

```
C:\Users\admin> ping 10.1.50.1

Pinging 10.1.50.1 with 32 bytes of data:
Reply from 10.1.50.1: bytes=32 time=6ms TTL=252
Reply from 10.1.50.1: bytes=32 time=5ms TTL=252
Reply from 10.1.50.1: bytes=32 time=5ms TTL=252
Reply from 10.1.50.1: bytes=32 time=6ms TTL=252

Ping statistics for 10.1.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss);
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

6.4 Configuration Reference

6.4.1 SW1 Configuration

```
#
sysname SW1
#
vlan batch 50 100 200
#
dhcp enable
#
interface Vlanif50
 ip address 10.1.50.2 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
#
interface Vlanif200
 ip address 192.168.200.254 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 50
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

6.4.2 SW2 Configuration

```
#
sysname SW2
#
vlan batch 100 200
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

6.4.3 AC Configuration

```
#
 sysname AC1
#
vlan batch 100 200
#
dhcp enable
#
ip pool ap
 gateway-list 192.168.100.1
 network 192.168.100.0 mask 255.255.255.0
 excluded-ip-address 192.168.100.254
#
interface Vlanif100
 ip address 192.168.100.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
#
capwap source interface vlanif100
#
wlan
 traffic-profile name default
 security-profile name default
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase %^%#Qt8(LipCzL)\84Z-T#&WX_Rt-s00|'G!>`D3$EiG%^%# aes
 security-profile name default-wds
  security wpa2 psk pass-phrase %^%#qNfI(V#y8:b/W|/(mY81#Z\D8~!8Y*#IO1RwV);+%^%# aes
 security-profile name default-mesh
  security wpa2 psk pass-phrase %^%#o[7"I"t]\4xd-e7_BV:3&kdR~nCGO!El4DSuB>~E%^%# aes
 ssid-profile name default
 ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
 vap-profile name default
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 200
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-system-profile name default
```

```
 ap-group name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 0 type-id 130 ap-mac f09b-b861-3a70 ap-sn 2102353GES6RM6019261
  ap-name AP1
  ap-group ap-group1
 ap-id 1 type-id 115 ap-mac f4de-af36-acc0 ap-sn 2102352UBR10L6001245
  ap-name AP2
  ap-group ap-group1
#
return
```

6.4.4 R1 Configuration

```
#
 sysname R1
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 10.1.50.1 255.255.255.0
#
ip route-static 192.168.0.0 255.255.0.0 10.1.50.2
#
return
```

6.5 Quiz

If both the AP and STA support dual radios, the STA always associates with the 2.4 GHz radio but cannot associate with the 5 GHz radio, what are the possible causes?

Reference answer:

The possible causes are as follows:

1. A VAP profile is applied only to the 2.4 GHz radio but not to the 5 GHz radio. As a result, only the 2.4 GHz frequency band releases SSID signals, and the STA can associate with only the 2.4 GHz radio.

2. A VAP profile is applied to both 2.4 GHz and 5 GHz radios on the AP, but the administrator manually disables the 5 GHz radio using the **radio disable** command.

3. The power of the AP's 5 GHz radio is low, and the STA is far away from the AP. As a result, the RSSI signal is weak and the STA cannot associate with the 5 GHz radio.